RSA NETWITNESS®
PLATFORM

Release Notes

for RSA NetWitness Platform 11.3 (Version 11.3.0.2)

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.

October 2019

Contents

Introduction

RSA NetWitness® Platform 11.3 provides new features and enhancements for every role in the Security Operation Center. These are a few examples: additional capabilities for analyzing hosts and files, usability enhancements to make work easier for incident responders and threat hunters, policy and licensing enhancements to help administrators manage their environments, and performance enhancements for Event Stream Analysis (ESA).

Note: NetWitness Platform 11.3, version 11.3.0.2 contains all the 11.3 and 11.3.0.1 features, with significant improvements for Event Stream Analysis (ESA). This version fully replaces version 11.3.0.0. For information about ESA, see Event Stream Analysis. For information about upgrades, see Upgrade Notes.

Note: The only supported upgrade path for 11.3.0.2 is from Security Analytics 10.6.6.x. 11.3.0.2 is not intended for customers who have already upgraded to any 11.x release.
- If you are running a version that is prior to 10.6.6.x, you must update to 10.6.6.x before you can upgrade to 11.3.0.2. See the RSA Security Analytics 10.6.6 Update Guide (https://community.rsa.com/docs/DOC-95880) on RSA Link.
- If you are already running 11.1.x.x, 11.2.x.x or 11.3.x.x, you must upgrade to 11.3.1.1 to make sure that you are running the latest version of the 11.3.x.x platform.

These sections provide the complete list of enhancements to specific capabilities:

- Endpoint Investigation
- Incident Response
- User and Entity Behavior Analytics
- Network Data and Log Investigation
- Event Stream Analysis
- Log Collection
- Core Services (Broker, Concentrator, Decoder, Archiver)
- Administration
- License Management
- Threat Aware Authentication

Endpoint Investigation

Endpoint Agent

The agent supports Endpoint Detection and Response (EDR) capabilities along with Windows Log Collection.

The Advanced (licensed) agent provides EDR capabilities with continuous monitoring of activities on the host for deep visibility, and analysis of all behavior and processes on the endpoint. The agent records data about every critical action, such as process, file, registry modification, and network connections, and posts them as events, in near real-time, to the server. The agent can detect anomalies such as image hooks, kernel hooks, registry discrepancies, and suspicious threads. In addition, it collects Windows logs. For more information, see the *NetWitness Endpoint User Guide*.

The following are key capabilities:

- User console interactions that are crucial for investigating malware attacks that use Windows legitimate files, such as `cmd.exe` or `powershell.exe`, to execute commands on a compromised host.
- Visibility into complete command line argument strings that are important for forensics and investigations.
- Detection of file or file-less based scripts by reporting scripts directly on process events instead of script engines. Currently supported engines include `powershell`, `cmd`, `cscript`, `wscript`, `rundll32`, `mshtml`, and `javascript`.
- Tamper Proof Agent - Registry keys, `exe` and `sys` files of both user-mode and kernel-mode agents are protected.

Endpoint agents can operate in an Insights or Advanced mode depending on the policy configuration. For more information on policies, see the *NetWitness Endpoint Configuration Guide*.

Key Improvements in Agents over Legacy NetWitness Endpoint Agents

- Decoupled dependencies with kernel internal structures.
- Performance improvements in file blocking with huge increase in number of hashes that can be blocked.
- Increased event capture limits. Events are no longer tied to executable-hash but to the entire creation chain.
- Better compatibility and interoperability with third-party applications.

Supported Agent Operating Systems

The following operating systems are now supported:

- Windows 2019 Server
- Windows 10 (32 and 64-bit) (up to version 1809)
- Red Hat Linux 7.x
- macOS 10.13 (High Sierra)
- macOS 10.14 (Mojave)

Agents can also be installed on Virtual Desktop Infrastructure (VDI) on VMware environments. For more information, see the *NetWitness Endpoint Agent Installation Guide*.

Scalable and Distributed Deployments

You can scale your deployment by adding multiple Endpoint Log Hybrids, depending on the number, location, distribution of agents, and data collected from endpoints. Install Endpoint Broker to get a consolidated view of all Endpoint servers in your deployment. For more information, see the *NetWitness Endpoint User Guide* and the *NetWitness Endpoint Configuration Guide*.

Groups and Policies

To efficiently manage and update endpoint agent configurations, administrators can group agents and manage their behavior using policies. Administrators can either use default or customized policies. You can enable Windows Log configuration through the Windows Log policy instead of generating it through the agent packager. For more information, see the *NetWitness Endpoint Configuration Guide*.

Analyze Files and Hosts Using Risk Score

Analysts can investigate a file or host using risk scores ranging from 1 to 100. Detailed context of risk contributors (alerts and events) is available to help you rapidly investigate suspicious or malicious activity. For more information, see the *NetWitness Endpoint User Guide*.

Process Visualization

For a better analyst experience during process investigation, an intuitive user interface is introduced to:

- Understand the entire process event chain, process parent-child relationships, and all associated events in a timeline view.
- Analyze important process attributes, such as username, launch arguments, reputation, file status, signer, signature, and file path.

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

File Analysis and Response

Analysts can:

- Analyze files using file reputation (such as known good, invalid, suspicious) from the Context Hub, risk score, and certificate status.
- Perform external lookup using Google or VirusTotal.
- Download a file and perform deeper file analysis, such as string search and text content for scripts.

After investigation, analysts can:

- Assign statuses to files to categorize them as blacklist, whitelist, and so on.
- Remediate threats by blocking malicious or infected files.

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

Application Rules for Existing IIOCs

The existing IIOCs from NetWitness Endpoint 4.4.0.x are available as out-of-the-box application rules in NetWitness Platform. For more information, see the *NetWitness Endpoint Configuration Guide*.

Added Endpoint Risk Scoring Rules for ESA

In addition to the ESA sample rules, NetWitness Platform now includes an Endpoint Risk Scoring Bundle with approximately 400 rules. These rules generate alerts that are used to calculate risk scores for suspicious files and hosts that cross defined risk score thresholds. If you have NetWitness Endpoint, you can add this rule bundle to an ESA rule deployment in the same way that you would add any ESA rule. However, you must specify endpoint data sources (Concentrators) during ESA rule deployments. For more information, see the *ESA Configuration Guide*.

Updates to the Investigate > Event Analysis View for Endpoint Events

- Text Analysis for Endpoint events provides meaningful text explaining the event. You can also view metadata with values greater than 255 characters.
- For each session, you can view the event in the Process Analysis, or view the details of the host associated with the event by pivoting to the Hosts details view.

Incident Response

Redesigned the Events List for NetWitness Endpoint Events

To improve the analyst experience and incorporate Endpoint events into NetWitness Respond, the redesigned Events List has a flexible layout that better renders diverse data. The redesigned list empowers analysts to quickly understand and triage events with a more scannable event preview, which is customized for NetWitness Endpoint and inline event details. For more information, see the *NetWitness Respond User Guide*.

Improved the Alerts List Filter for NetWitness Endpoint

When you filter the alerts list for the Endpoint source, it includes both NetWitness Endpoint 4.4.x and NetWitness Endpoint 11.x alerts.

Added a UEBA Incident Rule

A new User Entity Behavior Analytics (UEBA) default incident rule is available, which captures user entity behavior grouped by Classifier ID to create incidents from alerts.

Updated the NetWitness Endpoint Incident Rule

If you have NetWitness Endpoint, the High Risk Alerts: NetWitness Endpoint default incident rule captures alerts generated by NetWitness Endpoint with a risk score of High or Critical. This rule now groups alerts into incidents by Host Name. For more information, see the *NetWitness Respond Configuration Guide*.

Added the Ability to Automatically Create Endpoint Risk Scoring Incidents

If you have NetWitness Endpoint, you can configure Endpoint Risk Score Threshold settings to automatically create risk scoring incidents for suspicious files and hosts that cross the defined risk score thresholds. For more information about configuring risk score threshold settings, see the *NetWitness Respond Configuration Guide*. For more information about NetWitness Endpoint, see the *NetWitness Endpoint Configuration Guide*.

Pivot to the Investigate > Hosts and Files Views from the Respond View

For a detailed investigation of an incident, analysts can access the Investigate > Hosts and Files views through context tooltips in the Respond view.

Look Up File Reputation Status and Information From the Respond View

In the Respond view and Investigate views where Context Hub is integrated into NetWitness Platform, analysts can hover over a file hash entity to open a context tooltip, which shows the reputation status of the file. Analysts can also click a View Context button, which opens a Context Lookup panel with additional file information.

User and Entity Behavior Analytics

Advanced Analytics Using RSA NetWitness Endpoint

UEBA is integrated with NetWitness Endpoint to enhance the current detection coverage on NetWitness Platform. The purpose of this integration is to identify potential attacker activity. This focuses on two primary data sources:

- Process Executions
- Registry Changes

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

Access Host Details or Analyze Process Views from the User Profile View

An analyst can pivot to the Host Details view or the Analyze Process view from the User Profile view to look for more detailed information about an anomalous process or a host that is associated with the user risk. For more information, see the *NetWitness UEBA User Guide*.

Support for Additional Data Source

NetWitness UEBA now supports the RSA SecurID data source.

Network Data and Log Investigation

Analysts Can View a Large Number of Events Simultaneously in the Event Analysis View Events List

Up to 50,000 events are loaded in the Events list in ascending order based on collection time. A row number indicator every 100 rows helps with navigation through the list. User interface features help you to understand what is being displayed and the sorting order. For detailed information, see "Analyzing Events in the Event Analysis View" in the *NetWitness Investigate User Guide*.

Analysts Can See Detailed Status of a Query in the Event Analysis View

Clicking the information icon (ⓘ) in the Event Analysis view query builder opens the query console, a new user interface feature that provides a status bar, warnings, errors, and other details about what is occurring as a query is being executed. When a query is complete, the query console displays the time range, the query, the services queried, any services that could not be queried, and the amount of time each service took to find results and retrieve events based on the query. You can copy the complete query as text. For detailed information, see "Filtering Data in the Event Analysis View" in the *NetWitness Investigate User Guide*.

Improved Analyst Workflow in the Navigate View, Events View, and Event Analysis View

To make it easier for analysts to conduct investigations, these improvements have been implemented:

- When you are switching between pages in the Events view, log events load faster due to caching of query results.
- The time range used in Navigate is used when transitioning to the Events view.
- In the Navigate view, an easily understood meta key description is displayed next to the meta key name. For detailed information, see "Navigate View" in the *NetWitness Investigate User Guide*.
- Custom time range input has been added in the Event Analysis view. In addition to the predefined time windows, you can enter a custom time range, and then click the month, day, year, hour, and minute to edit the time range directly in the breadcrumb. For detailed information, see "Filtering Data in the Event Analysis View" in the *NetWitness Investigate User Guide*.

Detailed Information about Loaded Events in the Events View is Displayed in the Footer

The message in the footer helps analysts to understand what they are viewing in the Events view. If no events are loaded, this message is displayed: "0 event matches." Other messages let you know if the scan limit or results limit set by the administrator has been met and which services have results displayed. For example, the following message lets you know that the scan limit has been reached and further data is available to scan: "Displaying 1-25 of 100000+ event matches (scan limit of 100000 events has been reached)." For detailed information, see "Events View" in the *NetWitness Investigate User Guide*.

Faster Search and Query Speed in the Navigate View and Events View

When analysts working in the Navigate view query a Broker or Concentrator, subsequent queries that share all or some of a previous query's criteria return results faster by using a new caching built into the services. In the Events view, queries using complex operations with text values are cached so subsequent queries that share all or some of a previous query's criteria return results quicker.

New Query Builder Capabilities in the Event Analysis View

- You can create complex filters in the Guided Mode query builder using the Free Form Filter in the Advanced Options submenu, which is in all of the Guided Mode drop-down menus. Free-Form Mode is still available if you want to paste a long, complex query.
- When you submit a query that contains free-form filters, the free-form filters are validated on the server side before execution. If any of the filters are invalid the query is not executed.
- While a query is executing, you can cancel the query in progress. When a query is canceled, the Events panel event count, the footer message, and the query console reflect the number of events retrieved rather than the total number of events found.

For detailed information, see "Filtering Events in the Event Analysis View" in the *NetWitness Investigate User Guide*.

Updated Meta Keys in the Endpoint Analysis Column Group

The Endpoint Analysis column group is updated to include new meta keys for endpoint investigation, which are displayed when viewing an Endpoint event in the Events view and the Event Analysis view.

New Preference Option to Control Automatic Update of Time Range in Breadcrumb

In the Event Analysis view, a new preference in the Event Preference dialog controls automatic update of the time range in the breadcrumb. While you are viewing results for a specific time range, the service is being polled at one minute intervals to detect if there are new results, but any new results are not loaded to the current view. By default, the time range window in the breadcrumb stays synchronized with the current search. You can choose to automatically update the time range window in the breadcrumb when the service indicates that it has the latest updated results by selecting the **Update Time Window Automatically** checkbox. When the time range is updated and the Submit Query button is activated, you can get the latest updated results.

Access UEBA from the Investigate > Host Details View

If you have NetWitness UEBA installed, you can analyze risks associated with users logged-in on the host by pivoting to the Users view. For more information, see the *NetWitness UEBA User Guide*.

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.

Log Collection

Sorted List of Log Collectors and Virtual Log Collectors

For Log Collector services, Local Collectors, and Remote Collectors, drop-down menus are sorted alphabetically to make it easier to locate the collector you want to view:

- On a Local Collector, in the Remote Collectors tab, the Remote Collectors field in the Add Source dialog box is sorted.
- On a Virtual Log Collector, the Local Collectors tab has sorted fields for Destinations and Sources.

Sorted List of Log Collectors and Log Decoders

In the ADMIN > Health & Wellness > Event Source Monitoring view, the Log Collectors and Log Decoders drop-down menus are sorted alphabetically to make it easier to locate the items you want to view.

Local Log Collectors Syslog Ports

Local Log Collectors (Log Collectors residing on Log Decoder appliances) are capable of receiving syslog on ports other than 514 and 6514 in order to support receiving syslog messages with different encodings, such as EUC-KR, ISO8897-9, and so on. The Log Decoder service is still the collection point for receiving ASCII/UTF-8 logs on port 514 and 6514.

Improved "Pass-Through-Logic" for Non-conformant Syslog

Remote Log Collectors now accept all non-conformant syslog messages except for those with an empty message header or body. Unwanted messages should be filtered out at syslog collection using event filters. For details, see the "Configure Event Filters for a Collector" section in the *Log Collection Guide*. Refer to syslog RFC3164 and RFC5424 for details about syslog format (https://www.ietf.org/standards/rfcs/).

Core Services (Broker, Concentrator, Decoder, Archiver)

Snort Parser with UDM Support

Snort parser support has been updated with a new option, `udm=true`, that uses the aligned Unified Data Model (UDM) key set. For more information, see "Snort Parsers" in the *Decoder and Log Decoder Configuration Guide*.

Decryption of Secure SMTP

NetWitness Platform supports opportunistic SSL/TLS decryption, which addresses RFC 3207 (https://tools.ietf.org/html/rfc3207). You can add an HTTPS parser option that provides a comma-separated-values (.csv) formatted list of destination ports of the session where the STARTTLS command will be searched, with at least one encryption key that has been uploaded. This enables the STARTTLS functionality. For more information, see "Decryption of Secure SMTP" in the *Decoder and Log Decoder Configuration Guide*.

GeoIP Parser No Longer Supported, Replaced With GeoIP2 Parser

The original GeoIP parser is no longer supported. The new GeoIP2 parser that was introduced in 11.2 fully replaces it. The GeoIP2 parser supports all the previous functionality, as well as the new Maxmind package including IPv4 and IPv6 conversions.

Limit Query Memory Usage with the SDK max.query.memory Parameter

The `max.where.clause.sessions` parameter is used to impose a limit on how many sessions can be scanned by a single query. For example, if a user selects all meta from the database, the database stops processing results once the number of sessions read for the query reaches this configuration value. This parameter will be deprecated in a future release. Use the `max.query.memory` parameter to limit overall query memory usage.

PowerVault SEDs Can Be Used for External Storage

You can now configure PowerVault SEDs (self-encrypted drives) for use as external storage to store logs and packets data for retrieval.

N-Gram Indexes Have Better Performance than in 11.2, Improving Full-text Searches

There have been improvements to the insert rate of N-Gram indexes for full-text searches. N-Gram mode indexes are approximately twice as fast for updates, which means that they can be leveraged in more Concentrators without having as much of an impact on aggregation performance. This feature is disabled by default. For information about N-gram indexes, see "Index Customization" in the *NetWitness Platform Core Database Tuning Guide*.

New `avglen` Function in Database Query Syntax

The `avglen` function has been added to query syntax. It returns a single value, which is the average length of a meta value within a function.

Administration

Ability to Configure Hybrid Components onto Core Appliances (allows use of multiple PowerVaults for Hybrid components)

You can install Hybrid categories, such as Log Hybrid and Network (Packet) Hybrid service categories, on a Series 6 (R640) Physical host. This gives you the ability to attach multiple PowerVault external storage devices to the Series 6 (R640) physical host.

Public Key Infrastructure (PKI) Authentication

PKI Authentication enables users to authenticate and access the NetWitness Platform UI using digital certificates. For more information, see PKI Authentication in *System Security and User Management Guide*.

DISA STIG Support

RSA supports all Audit Rules in the DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide) Control Group. For detailed information on STIG support, refer to the *System Maintenance Guide*.

Certificate Reissue Command

RSA added the `cert-reissue` command and its arguments so that you can reissue host certificates. After you update all your hosts to 11.3.0.2, you should reissue certificates for all of them as soon as possible to avoid having them expire. If the certificates expire, your NetWitness deployment is placed in an unrecoverable state. For detailed information on how to reissue certificates, refer to the *Security Configuration Guide*.

Warm, Standby NW Server Host (For FailOver/High Availability) - Physical Host Only

The Warm Standby NW Server duplicates the critical components and configurations of your active NW Server Host to increase reliability. The Warm Standby NW Server can be configured to remain in standby mode and receive backups of the Active NW Server Host at regular intervals. If the Active NW Server fails (goes offline), the failover procedure can be executed and the Standby NW Server becomes active. For detailed information on how to set up and manage a Warm Standby NW Server, refer to the NetWitness Platform *Deployment Guide*.

New Tool for Consolidating Hosts and Services Configuration Data into a Single Instance

The NW-Consolidator tool is available for selective 10.6.6 customers who want to migrate the configuration and data from 10.6.6 to NetWitness Platform 11.3.0.2. This tool can be used if your deployment has multiple Security Analytics and Reporting Engine instances and you want to consolidate the Hosts and Services configuration and data into a single instance. You can also consolidate the data related to users, groups, roles, feeds and reports.

License Management

Support for Endpoint and ESA Correlation Server Licensing and Consolidation of all Entitlements for Throughput Licenses

The enhanced licensing user interface make it easy for administrators to view the license information. The Licensing Details page displays the aggregated throughput usage for different entitlements with throughput usage trends. Administrators can view all the licenses in the deployment, including those for Endpoint and the ESA Correlation Server. In addition, administrators can configure the licenses for multiple NetWitness servers and hot and warm servers. For more information, see the *Licensing Management Guide*.

Threat Aware Authentication

NetWitness Platform Integration with RSA SecureID Access

NetWitness Platform Integration with RSA SecureID Access enables you to identify suspicious users in Netwitness Platform and elevate the access levels or block the users in RSA Secure ID Access based on the assurance level and policies defined in Secure ID. The NetWitness Respond server sends email identifiers of suspicious users from incidents to RSA SecureID Access. To configure this integration on the Respond Server, see the *Respond Configuration Guide*.

Fixed Issues

This section lists issues fixed since the last major release.

Issues Fixed in 11.3.0.2

Event Stream Analysis (ESA)

Tracking Number	Description
ASOC-82690	The maximum memory for the ESA Correlation server has been changed to 164 GB.
ASOC-81823	Converting arrays `toLowerCase` for use in `GROUP BY` or `PARTITION BY` function in Esper/ESA causes partitioning to malfunction.
ASOC-81752	Health & Wellness shows that ESA Correlation is Unhealthy after a notification failure and does not resolve itself over time.
ASOC-81672 ASOC-76364	Unable to delete an endpoint bundle from an ESA deployment.

Tracking Number	Description
ASOC-81375	If the rules memory threshold is set to 60%, it needs tuning to avoid false Health & Wellness alerts.
ASOC-81373	ESA rules with Context Hub lists get disabled during upgrade when there are duplicate Context Hub data sources.

Issues Fixed in 11.3 or 11.3.0.1

Security

Tracking Number	Description
ASOC-59254	Kernel Security Update https://access.redhat.com/errata/RHSA-2018:1965.
ASOC-58383	policycoreutils Security Update https://access.redhat.com/errata/RHSA-2018:0913.
ASOC-58382	Openssl Security Update https://access.redhat.com/errata/RHSA-2018:0998.

Core Services (Broker, Concentrator, Decoder, Archiver)

Tracking Number	Description
ASOC-74691	When you included a meta value in the Archiver configuration, the metakey `word` was also added.
ASOC-41902	SSL FIPS Mode (Checkbox) for Broker, Concentrator and Archiver needs to be disabled.
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.

Endpoint

Tracking Number	Description
ASOC-74735	Owner information is now available on the Hosts > Details > Process tab.
ASOC-74199	On Windows, the agent driver stopped when the agent mode was changed multiple times from `Advanced` to `Insights`.

Tracking Number	Description
ASOC-74025	The Endpoint agent was not able to communicate to the server using UDP when it went back to HTTP mode.
ASOC-73742	A complete list of Loaded Libraries was not displayed when investigating the process.
ASOC-72823	The default scan schedule is now set to 1 week for improved performance of the Endpoint Server.

Event Stream Analysis

Tracking Number	Description
ASOC-60511	ESA rules with Context Hub lists get disabled during upgrade or ESA host reboot.
ASOC-60367	ESA Rules with custom meta keys do not deploy on the ESA Server.
ASOC-26481	Cannot set ESA compression level as in other appliances.
ASOC-14157	ESA displays warning for array operators.
SACE-11668 ASOC-79640	Disabled ESA rules get enabled after restarting the ESA Correlation service. (After the fix, disabled ESA rules remain disabled after restarting the ESA Correlation service.)

Health and Wellness

Tracking Number	Description
SACE-10840	The following NetWitness Database (NW DB) retention statistics are available in 11.3.0.2. • Overall Meta Oldest File Time Retention • Overall Session Oldest File Time Retention • Overall Packet Oldest File Time Retention

Investigate

Tracking Number	Description
ASOC-61230	When you import Profiles to the Navigate view or the Events view using the Manage Profiles dialog, the newly imported profiles are not added to the Profiles drop-down menu.
ASOC-60941	Network and log events are interleaved and sorted in time order in the Events view, but in the Event Analysis view, events are sorted differently. In the Event Analysis view, the events are not interleaved as they should be; instead all log events sorted in time order are displayed before all network events sorted in time order.
ASOC-50196	If the URL for a drill point is very long and you use the query in the Event Analysis view, an error (414 Request error) is returned.
ASOC-49427	The query builder in the Event Analysis view is unresponsive for filters that contain a space.

Respond

Tracking Number	Description
ASOC-59243	When all alerts are deleted for an alert rule, the filter for the rule is not properly removed.
ASOC-37533	When a custom In-memory table is created and added as an enrichment source in ESA, that information is not displayed for ESA alerts.
ASOC-75674	When you upgrade to 11.3.0.2, Respond's primary host property (`/rsa/primary/host`) was set to `false` by default, which had an adverse effect on some of the critical functionality. This is now set as `true`.

UEBA

Tracking Number	Description
ASOC-75673	The cache size for MongoDB is set to 20 GB for better performance.
ASOC-73271	The OOTB UEBA Incident Rule was missing UEBA values in the `Source` and `GroupBy` fields.

Upgrade

Tracking Number	Description
ASOC-49843	Audit log templates are not getting updated in Logstash output conf file while upgrading to 11.x.
ASOC-42136	Post-upgrade, the investigation links are disabled for static charts.
SACE-11250	In cases where systems have gone through multiple kernel updates, the `/boot` directory contained multiple kernel images, which consumed the `/boot` partition.

Upgrade Notes

The only upgrade path that is supported for RSA NetWitness® Platform 11.3.0.2 is 10.6.6.x to 11.3.0.2.

Note: If you are upgrading from 11.1.x.x, 11.2.x.x, or 11.3.x.x, you must upgrade to 11.3.1.1.

For more information on installing and upgrading to 11.3.0.2, see the Installation and Upgrade Guides in https://community.rsa.com/community/products/netwitness/113 > Installation and Upgrade Guides.

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
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 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).

Features Not Supported

The following tables provide information on features no longer supported in RSA NetWitness® Platform 11.1 or later releases.

Features Not Supported in 11.1.0.0 or later releases

No.	Feature	Notes
1	Malware Colo	Malware co-located is not supported in 11.1.0.0 and later releases. Malware Analysis is supported using a standalone Malware Analysis.
2	All-In-One (AIO) Deployment	All-in-one deployment is not supported. Fresh Install AIO has been removed.
3	Standalone Warehouse Connector	Standalone Warehouse Connector is not supported.
4	Administration Features	1. Forgot my password. 2. Email Notification to user when password expires. 3. Test/Search AD user.
5.	Pivotal	Pivotal is not supported.
6.	Warehouse Analytics	Warehouse Analytics is not supported.

No.	Feature	Notes
7.	Some Event Stream Analysis service features from 11.2 and earlier	Event Stream Analysis service features (11.2 and earlier) that are not in the 11.3 ESA Correlation service: 1. Memory snapshot for trial rules 2. ESA SNMP notification method 3. Database as an enrichment source (replaced by Context Hub list) 4. Warehouse Analytics as an enrichment source (replaced by Context Hub list) 5. Database Connection as an enrichment source (replaced by Context Hub list) 6. Capture time ordering 7. Memory pool
8.	Endpoint Hybrid	Endpoint Hybrid host type is not supported in 11.3.0.0 and later releases.