RSA NETWITNESS® PLATFORM

Release Notes

for RSA NetWitness® Platform 11.5

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.

September 2020

Contents

What's New

The RSA NetWitness® Platform 11.5 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 11.5.0.0:

- RSA NetWitness® Platform 11.3.x.x to 11.5.0.0 *
- RSA NetWitness® Platform 11.4.x.x to 11.5.0.0

* If you are upgrading from 11.2.x.x, 11.3.0.0, or 11.3.0.1, you must upgrade to 11.3.1.1 before you can upgrade to 11.5.

For more information on upgrading to 11.5.0.0, see Upgrade Guide for RSA NetWitness Platform 11.5.

Enhancements

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

- Investigation - SIEM and Network Traffic Analysis
- User Entity Behavior Analytics
- Incident Response
- Health and Wellness
- Endpoint Investigation
- Endpoint Configuration
- Broker, Concentrator, Decoder and Log Decoder Services
- Event Stream Analysis (ESA)
- Administration and Configuration
- Context Hub
- Log Collection
- Licensing

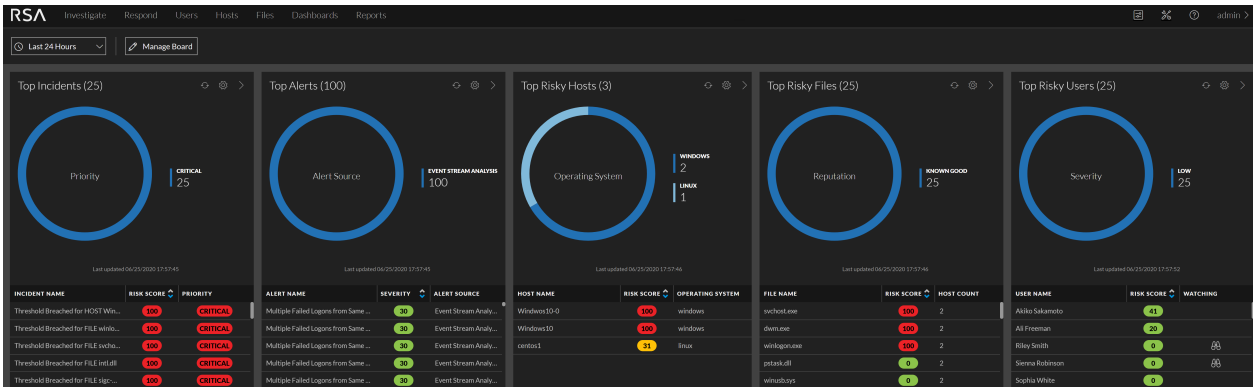
To locate the documents referred to in this section, go to the RSA NetWitness Platform 11.x Master Table of Contents: https://community.rsa.com/docs/DOC-81328. Product Documentation has links to the documentation for this release.

Investigation - SIEM and Network Traffic Analysis

Springboard - Unified View for Detections and Signals

RSA NetWitness Platform introduces the Springboard, an easy-to-use landing page that presents platform-wide detections and signals in a single view. On the Springboard, analysts can see panels for prioritized alerts, incidents, risky hosts, risky users, risky files, and focused event data to help hunt and investigate faster than ever before.

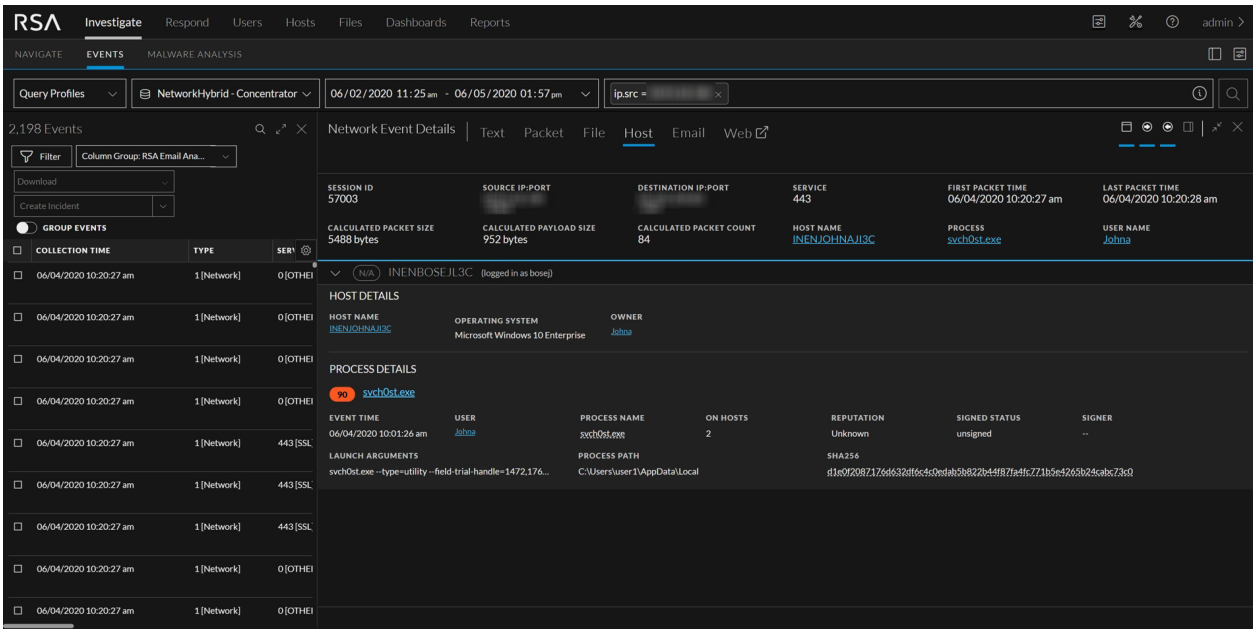
Springboard is customizable by administrators, allowing for editing of the built-in panels, and creation of new panels showing focused event metadata based on predefined query conditions. For additional information, refer to "Managing the Springboard" in the NetWitness Platform Getting Started Guide.



Expanded Network Visibility with Endpoint Data Enrichment

Expanded network visibility enables network events in your network (packet) deployment to be enriched with host and process data collected from the Endpoint agent. This empowers an analyst with improved coverage of threat landscape with enhanced detection and enriched network analysis. The enrichment will attach host, user, and process information from endpoint to any correlated network (packet) events collected from the network. Analysts can also drill from this correlated view into associated details, including user, reputation, risk score, and other endpoint details. For more information, see "Examine Event Details in the Events View" in the *NetWitness Investigate User Guide*.

Expanded Network Visibility is a policy setting that enables Insights and Advanced agents to track and monitor network events and optimize the frequency of sending endpoint network events for network (packet) correlation. For more information to enable the Expanded Network Visibility policy, see Creating Groups and Policies.

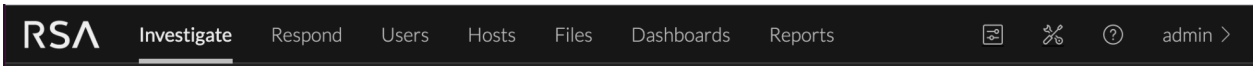


Improved Navigation to Help Analysts Quickly Detect and Respond to Threats

When logged in to NetWitness Platform, analysts can easily see the most common ways to extract value from the product.

- The top-level navigation promotes the key methods that analysts use to detect and respond to threats. Previously, analysts had to go to Investigate to access the Hosts, Files, and Users views.
- Administrative tasks are consolidated as icons in the upper right corner to keep administration, configuration, notifications, jobs, and user preferences together.

The following figure illustrates the top-level navigation for views that include notifications and jobs. For additional information, refer to NetWitness Platform Basic Navigation.

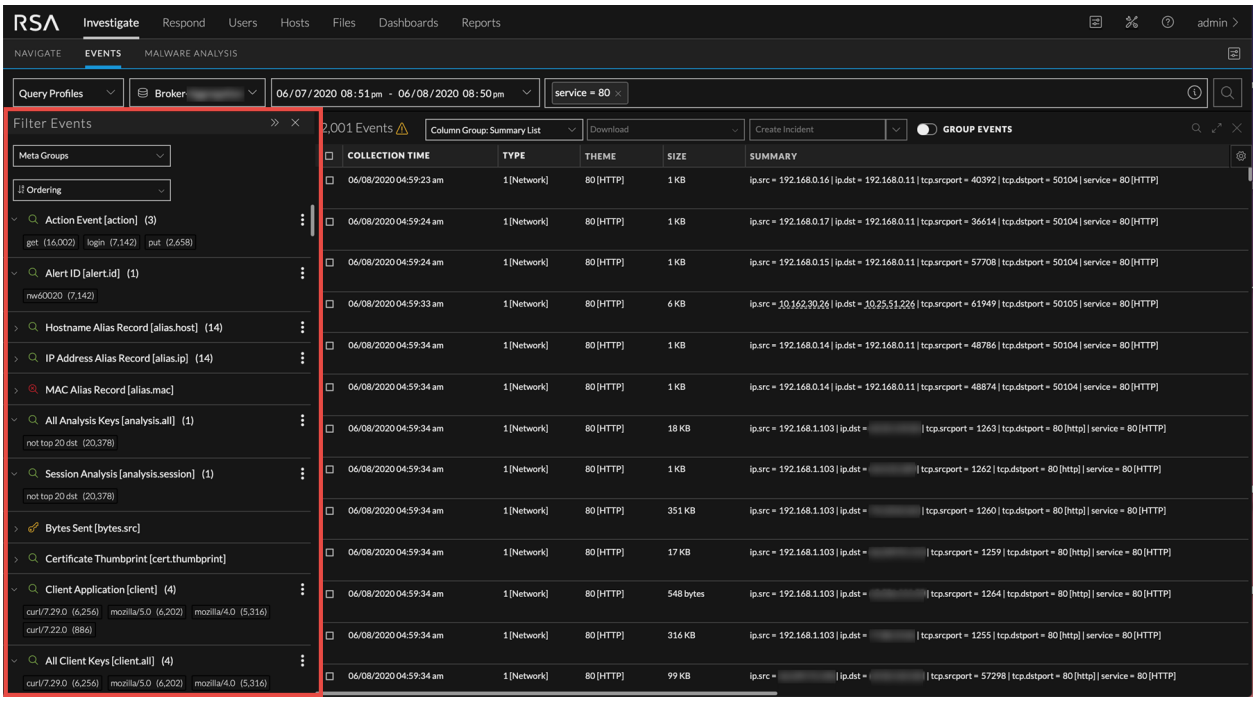


A Powerful New Way to Filter Events in the Events View by Pivoting Through the Associated Metadata (BETA)

In the Events view, analysts can pivot through metadata to filter down to a subset of events in a new Filter Events panel, which is side-by-side with the sequential list of events in the Events panel. The Filter Events panel allows analysts to:

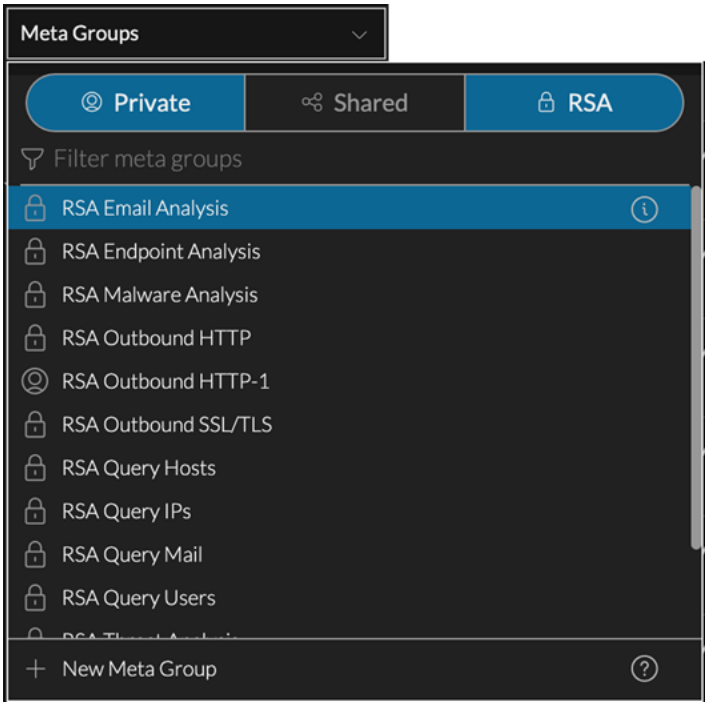
- Click meta values and immediately see the resulting events in the Events panel.
- Expand the panel to do further exploration of the metadata before examining the results.

The feature is enabled by default for all user roles except existing custom roles, Operators, UEBA Analysts, and Content Administrators. When upgrading to version 11.5, the administrator needs to add the `investigate-server.event.filter` permission for any existing custom roles as described in "Change Permissions Assigned to a Role" in (Optional) Add a Role and Assign Permissions. For additional information, refer to "Pivot Through Metadata in the Events View (Beta)" in the NetWitness Investigate User Guide.



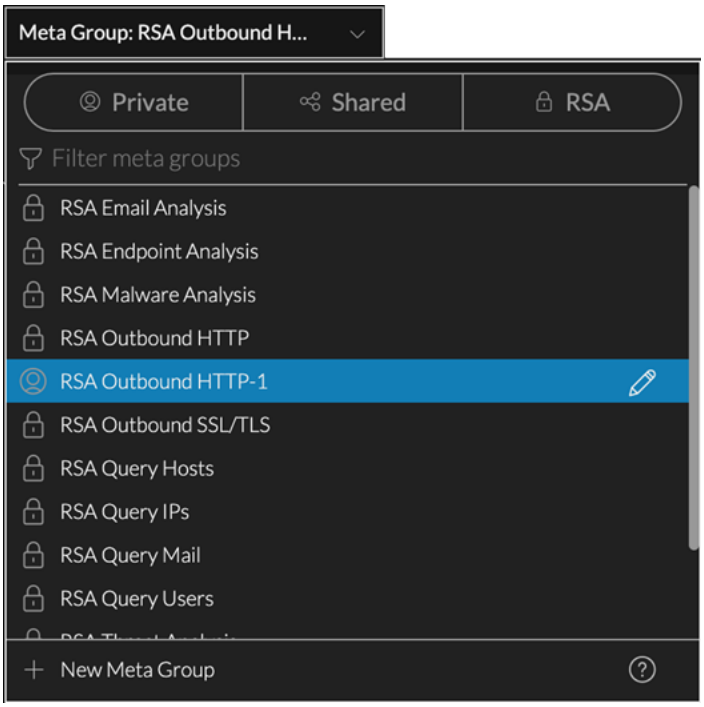
Separation of Each User's Private Investigate Content and Content That Is Shared between Users

Each user can have their own private set of profiles, meta groups, and column groups inside the Events view that no other user can view or modify. The user interface for managing content is uncluttered because users can limit the types of content that are visible by selecting one or more types to be displayed: shared, private, and RSA built-in. Cloning any type of content allows users to edit any profiles, meta groups, or column groups to share or make private. For additional information, refer to Use Meta Groups to Focus on Relevant Meta Keys, Use Columns and Column Groups in the Events List, and Use Query Profiles to Encapsulate Common Areas for Investigation.



Meta Groups Allow Analysts to Optimize the Attributes per Event in the Events View

When investigating and looking over thousands of events in the Events view, analysts can optimize the sequence and number of attributes (meta keys) per event using meta groups to identify patterns and to determine if further investigation is warranted. Analysts can create, clone, edit, and delete meta groups. The built-in meta groups and shared meta groups are the same meta groups used in the Navigate and Legacy Events view, while private meta groups are available only to a single user in the Events view. For additional information, refer to Use Meta Groups to Focus on Relevant Meta Keys.



Added Protection When Downloading Email Attachments and Files

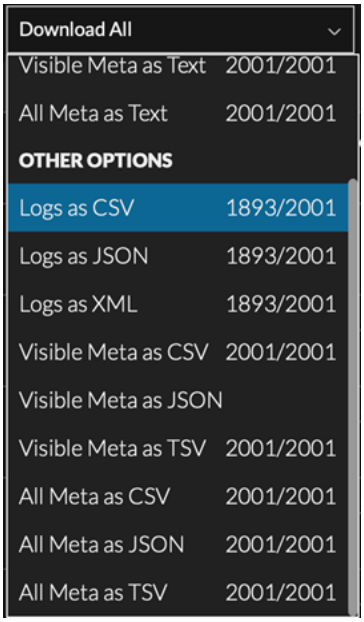
When downloading email attachments and files, users are protected from automatic opening of files that are potentially malicious. The password-protected zip archive limits downloads of malicious files from being quarantine by anti-virus software; you need to enter the password, `netwitness`, in order to open the file. For additional information see Download Data in the Events View.

Updated Context Menu Actions When Right-Clicking a Meta Value in the Events View

Context menu action options and labels in the Events view are updated to include Apply Equals Drill, Apply Equals Drill in New Tab, and refocus submenu options. For additional information, refer to Look Up Additional Context for Results.

Added Ability to Download All Metadata in the Events View for Further Analysis or Evidence

A new download option (All Meta) downloads all metadata in the Events panel, not just the visible columns downloaded with the Visible Meta option. The Download All Meta option is also available in reconstructions. The resulting download includes all metadata for the events selected, regardless of what columns are visible in the Events list. For example, if an event has 40 meta keys in the meta database, even if the column group in the Events list has 20 columns with 10 columns visible, all 40 meta keys for that event are included in the downloaded file. For additional information, refer to "Download Events or Metadata in the Events Panel" in the NetWitness Investigate User Guide.

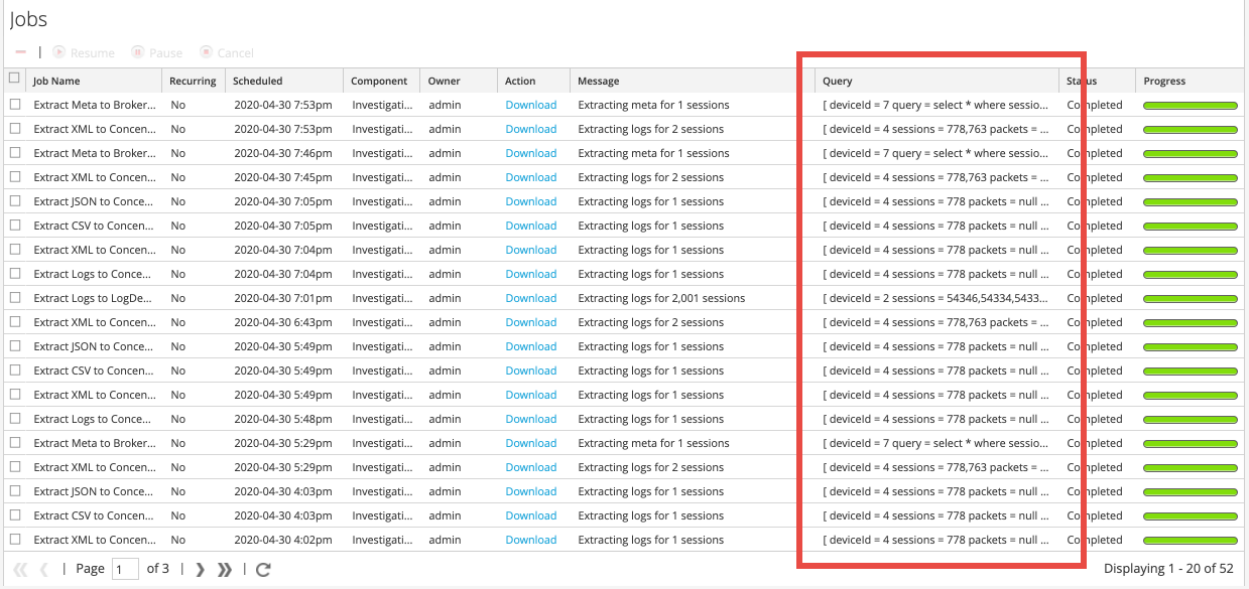


Added Convenience with Optional Human-Readable Time Format in Downloads from the Events View

Downloads previously used the Epoch format for the date, which needs some form of conversion to be understandable. Now the administrator can set the time format for downloads to an easily readable representation similar to the presentation in the Events panel. This is an example of the time on the 12-hour clock as it appears in the user interface: `04/13/2020 09:17:36 am - 07:00 pm`. In the download, Epoch format would represent the time as `61547519856000`. If the administrator set the time format for downloads to the easily readable representation, the same time would be represented as follows: `04-13-2020T09:17:36AM-07:00`. For additional information, refer to "Select a Time Range" in the NetWitness Investigate User Guide.

Details in the Jobs Queue Identify the Action or Query That Initiated a Failed Job

When viewing their failed jobs in the job queue, users can see details about the query or action that generated the job so they do not have to look through logs to find the action or query that initiated that job. It is easier to determine why the job failed and re-run it. For additional information, refer to Managing Jobs.



User Entity Behavior Analytics

Pivot from UEBA to view Network Events

Analysts can now pivot and further investigate network events in the Events view by selecting an indicator and clicking one of the pivot links in the events table under the indicator. For more information, see the NetWitness UEBA User Guide.

Support for new data source and additional indicators for VPN Logs and Azure Active Directory Logs

UEBA has introduced support for new data sources and additional indicators to help analysts perform analysis on VPN Logs and Azure Active directory logs to investigate and monitor potentially risky behaviors across all users in your environment. For example, Multiple Failed Authentications - External Access alert can be triggered when anomalous activity is identified for multiple failed authentication attempts in both Azure Active directory and VPN. For more information, see the NetWitness UEBA User Guide.

New network indicators

New network indicators are available for new occurrences of external destinations such as Domains, SSL Subjects, Destination Organizations, Destination Ports,as well as for new JA3 hashes. For more information, see the NetWitness UEBA User Guide.

Enhanced Performance For Physical Deployments

Analysts can now experience enhanced performance in the processing of historical data that is required to create baselines for UEBA models. For more information, see the NetWitness UEBA User Guide.

Incident Response

Saved Filters are Available for the Incidents and Alerts Lists in the Respond View

Analysts can save their filters for the Respond incident and alerts lists (Respond > Incidents and Respond > Alerts). For example, analysts may want to create an incidents filter to show only critical incidents over the last 24 hours. They may also want to create an alerts filter to show only alerts from a specific source and severity level over the last 24 hours. Saved filters provide the following benefits:

- Analysts can save and quickly apply specific filter conditions to the incident and alert lists.
- Since saved filters are global, all analysts have access to the saved filters.
- Saved Respond filters can be used to customize Springboard landing page panels.

Filters used in the Springboard cannot be deleted. For more information on the Respond saved filter, see the NetWitness Respond User Guide.

The Analysts role has the required Respond filter permissions by default. For information on the required permissions, see “Respond Saved Filter Permissions” in the System Security and User Management Guide.

Health and Wellness

Enhanced Health Monitoring

New Health and Wellness provides improved and intuitive dashboards, monitors, and visualizations.

This reduces the complexity of monitoring by providing visibility into the complete NetWitness Platform deployment with various statistics and details around the health parameters.

Customization of these dashboards, monitors, and visualizations is simple, flexible, and easy to use.

Below are some of the new and improved dashboards:

- **ESA Correlation Overview Dashboard** - This dashboard provides health statistics and trends on the ESA deployment.

- **Hosts Dashboard** – This dashboard provides the resource utilization and health statistics of the selected NetWitness host in your deployment.
- **Logs Dashboard** - This dashboard provides insights on logs deployment in the NetWitness Platform.

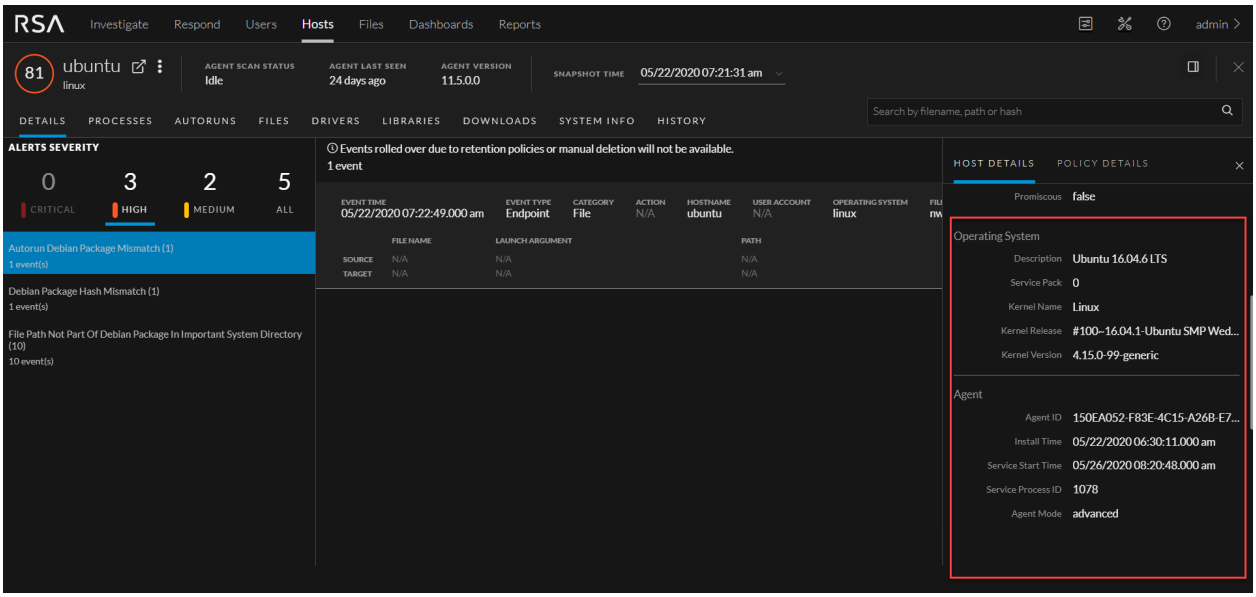
Administrators can add health alerts using alert notifications (for example, Email and Syslog notifications). They can also suppress notifications for a time period as required.

For more information, see “Monitor New Health and Wellness” section in the System Maintenance Guide.

Endpoint Investigation

Extended Linux Agent Support with Ubuntu

Introduced agent support for Ubuntu versions 16.04 LTS, 18.04 LTS, and 20.04 LTS. This enables RSA NetWitness to detect threats present on Ubuntu-based assets in the network. For more information, see the NetWitness Endpoint Agent Installation Guide.



Extended Windows Agent Support for Windows 10, version 2004

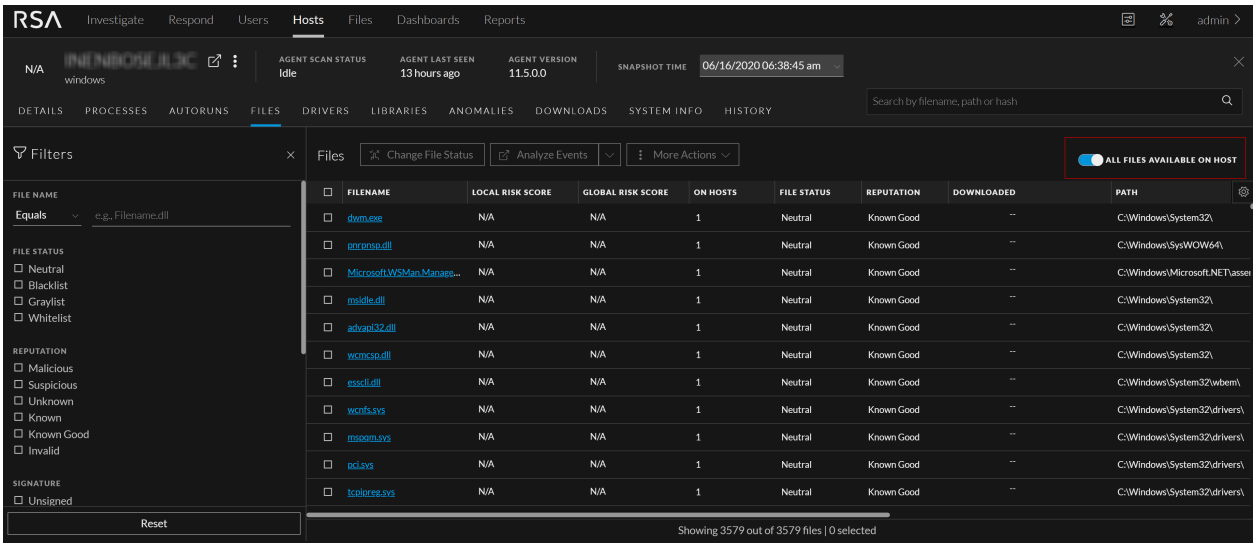
Extended agent support for Windows 10, version 2004 (32 and 64-bit) from 19041.329 onwards. For more information, see the NetWitness Endpoint Agent Installation Guide.

Improved Visibility within Host View

For faster investigation, **All files Available on Host** option option allows an analyst to view files reported on a specific host. It includes:

- All files reported as part of the scan and tracking
- Deleted files

Available on Host and **Deleted from Host** filters are also added to help analysts narrow down files for analysis. For more information, see Investigating Hosts.



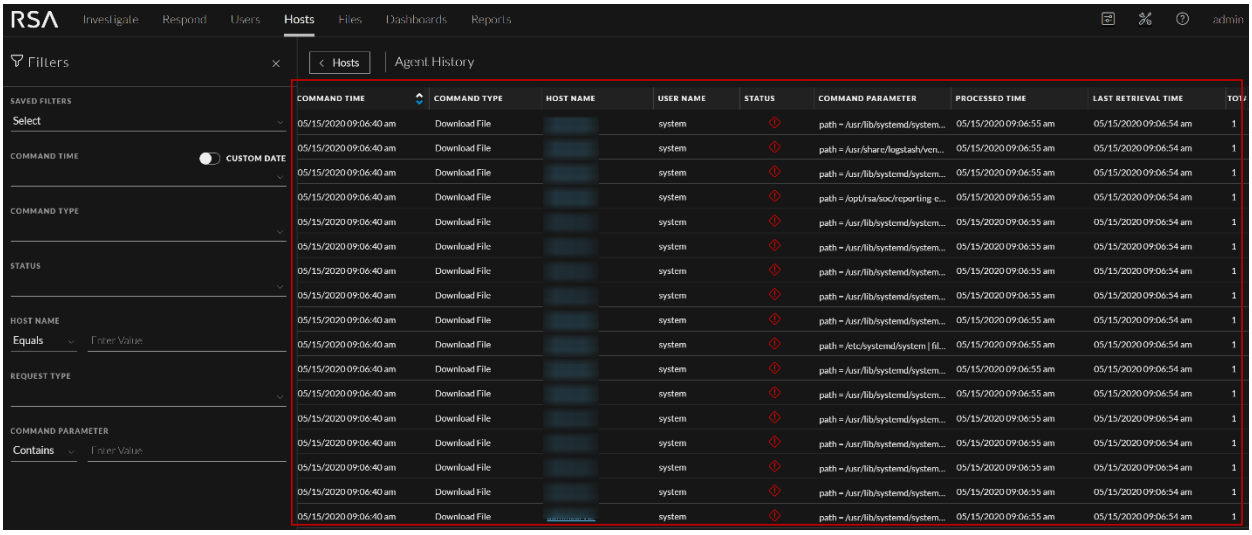
Ability to View Agent History

Agent History lists and details the commands issued to the agent (by the server or actions performed by any analyst) that is running on the host. This assist analysts in viewing the status (such as Success, Pending, Error and so on) of the commands issued.

For example, Analyst can view the status of commands issued such as MFT, file download, system dump and so on across the hosts.

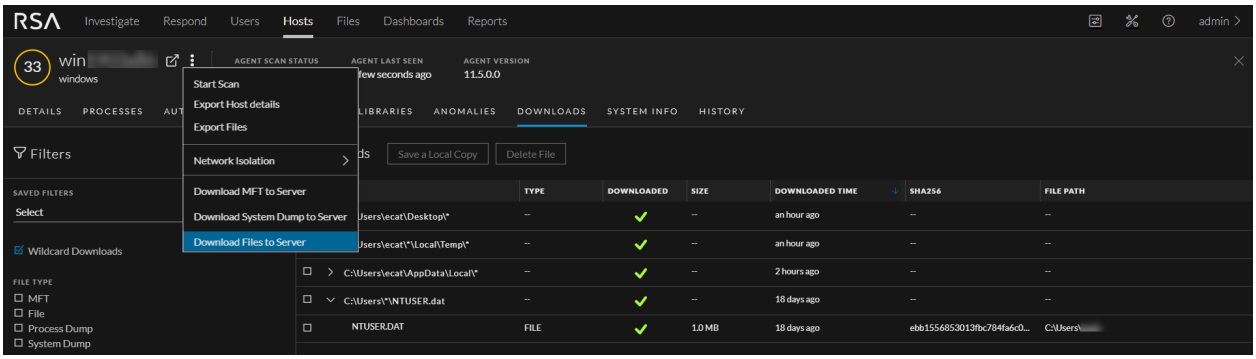
Analyst can choose to view agent history for the selected host or global agent history that contain commands issued across the different hosts along with details like command types, command status, command parameters and so on.

Filtering capabilities are supported to view selective command history details so the analyst can focus on specific information and take necessary actions. For more information, see Investigating Hosts.



Support to Download Any Files

For detailed investigation, an analyst can now download any files present on a host regardless of whether or not they are reported as part of scan or tracking, for example, registry hives, documents, or any other arbitrary file. Analysts can specify the full path of a file, file name, or wildcards to download files, and also request file download from multiple hosts at the same time. For more information, see Performing Host Forensics.



Endpoint Configuration

Throttle Network Bandwidth Parameter

For File Log policies and Windows policies, use the new **Throttle Network Bandwidth** parameter to limit network bandwidth that the Agent uses to connect to NetWitness Platform.

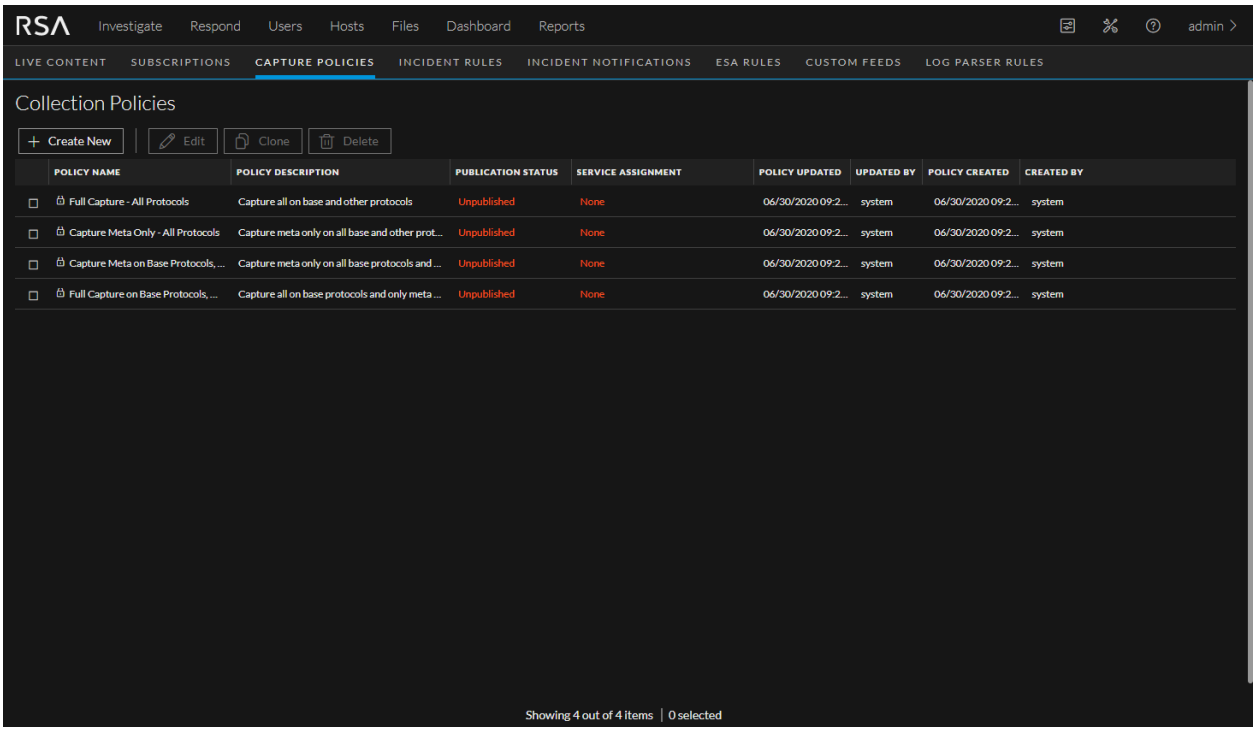
Broker, Concentrator, Decoder and Log Decoder Services

Selective Network Data Collection

Selective network data collection gives administrators the ability to apply centrally-managed capture policies across their Network Decoders. This results in better use of Decoder resources, including hard drive space, which leads to more predictable costs and lessens the burden of managing multiple Decoders. Administrators use policies to determine which traffic is stored and how it is stored. Inside each policy is a list of supported base protocols and definitions for how to handle any other protocols that are detected. A base set of protocols are available, allowing administrators to choose what level of capture they prefer on a per-protocol basis.

Note: An optional license is available that can be used for configuring a Decoder to capture metadata only.

Administrators can deploy predefined policies or create custom policies to give further control over the deployment. For more information, see "Configure Selective Network Data Collection" in the Decoder Configuration Guide.



Expanded Coverage of Snort Rules

NetWitness Platform now supports a wider variety of Snort rules, which enables you to use detection rules that are community-available that were not previously supported. Some of the new rule parameters that are now supported are:

- `nocase`
- `byte-extract`
- `byte-jump`
- `threshold`
- `depth`
- `offset`

For more information, see "Decoder Snort Detection" in the Decoder Configuration Guide.

Network and Log Decoders Import Data While Capturing

Administrators can now import data while capturing real-time on Network and Log Decoders, eliminating downtime when analyzing data that is collected off the network.

Multiple Adapter Packet Capture

The Network Decoder can now capture from multiple interfaces simultaneously. This functionality allows Network Decoders to capture from multiple physical Network Interface Cards (NICs) while leveraging the same network rules, application rules, and parsers for each NIC.

For more information, see "(Optional) Multiple Adapter Packet Capture" in the Decoder Configuration Guide.

User Account and Aggregation Account Information Available in Audit Logs

Previously, when a user performed a query that required searching upstream devices, for example, a query on a Broker, the audit logging on the upstream devices only showed the aggregation account username. In version 11.5, audit logging now provides information about the aggregation account and the actual user who submitted the query. For example, the information is displayed as follows in the audit log:

`User aggAccount (session 478, [::1]:1133, on behalf of <`*`username of submitter`*`>) has requested the SDK transforms.`

This information is available through multiple levels of Brokers and Concentrators. For more information, see Verify Global Audit Logs.

Decoders Include the Decoder Identifier Value in Session Metadata Lists

The Decoder Identifier value (`did`) denotes which Decoder generated metadata. The `did` value is now available in each Decoder session's metadata list. This is important for environments that do not have a Concentrator, and where a Decoder does its own indexing.

Note: Early versions of 11.4 in a mixed environment do not detect when the `did` value is already part of a session, and may duplicate an existing `did` value.

Configure Meta-Only Decoders

Administrators can configure Log and Network Decoders so that logs and packets can be processed, and then dropped before they are written to disk. This is called a Meta-Only Decoder and can save a lot of storage space (however, the traffic that generated the metadata cannot be reconstructed when you use this option). With this feature, all logs and packets are dropped after parsing, so they are never written to the database. The logs and packets flow through the system normally so that parsing and other operations are not impacted. For more information, see "(Optional) Configure Meta-Only Decoders" in the Decoder Configuration Guide.

Event Stream Analysis (ESA)

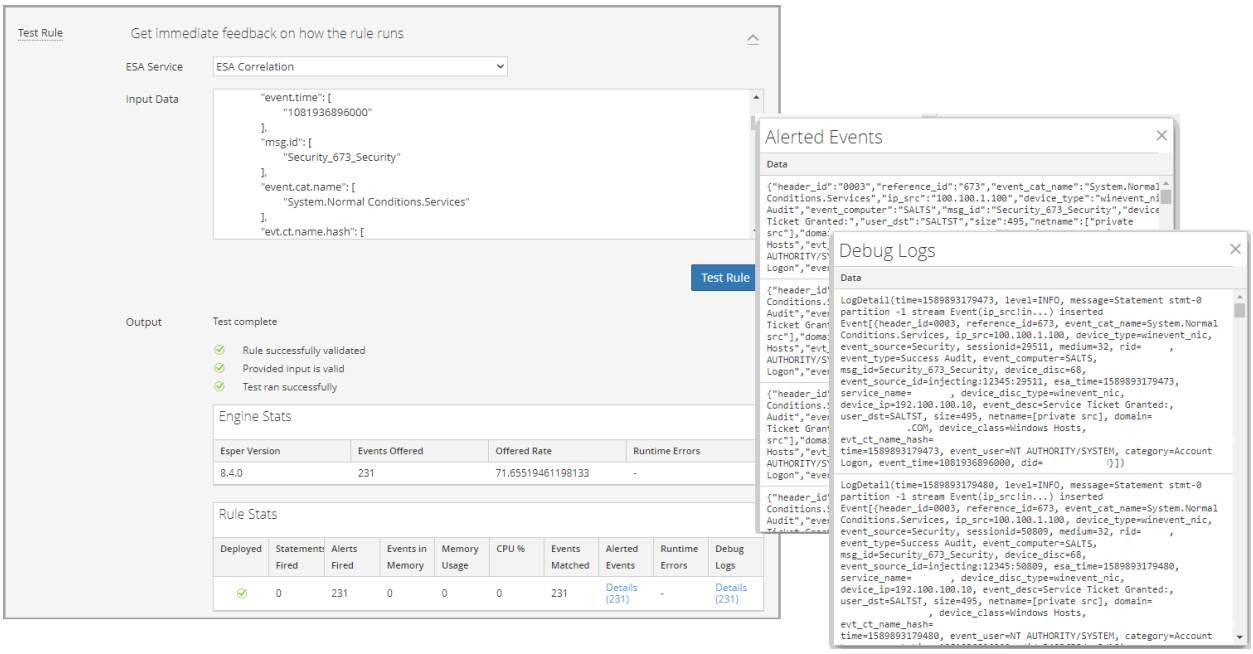
Configure Memory Thresholds Individually for Each ESA Rule

To prevent ESA rules from using too much memory, users can now add Memory Thresholds to individual ESA rules. If an ESA rule uses memory, such as a rule that contains windows or pattern matching, configure a memory threshold for that rule. The Memory Threshold option works for trial rules as well as non-trial rules. New rules default to a 100 MB memory threshold. Rules that existed before version 11.5 do not have a default value and a memory threshold is not set.

If an ESA rule goes over the allotted memory threshold, it gets disabled individually and an error is displayed for that rule on the  (Configure) > ESA Rules > Services tab in the Deployed Rule Stats section. Users can also view the CPU%, which is the percentage of the ESA rule deployment CPU used by the rule. For more information, see "Change Memory Threshold for Individual Trial Rules and Non-Trial Rules" in Change Memory Threshold for ESA Rules.

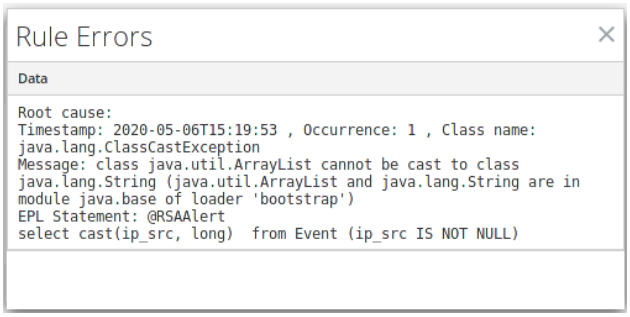
Validate ESA rules within the Rule Builder or Advanced EPL Rule Builder

Within the ESA rule builders, users can validate an ESA rule to determine if the rule logic is working as expected before deploying the rule. Instead of testing the rule on an external website, it is possible to download events from the Investigate view to a file in JSON format, copy the events, and paste them in the Input Data field in the Test Rule section of the rule builder.



Looking at the test rule output, rule writers can determine if the results meet the rule requirements.

The output shows ESA Correlation service processing statistics as well as individual statistics for each rule including Alerts Fired, Events in Memory, Memory Usage, CPU %, and Events Matched. Depending on the rule, links to Alerted Events, Runtime Errors, and Debug logs may be available.



By clicking the link to Alerted Events Details, users can quickly view the events that caused the alerts. The Debug logs are useful when troubleshooting ESA rules.

Note: You can view the alerts in the output, but this test does not send any alert notifications.

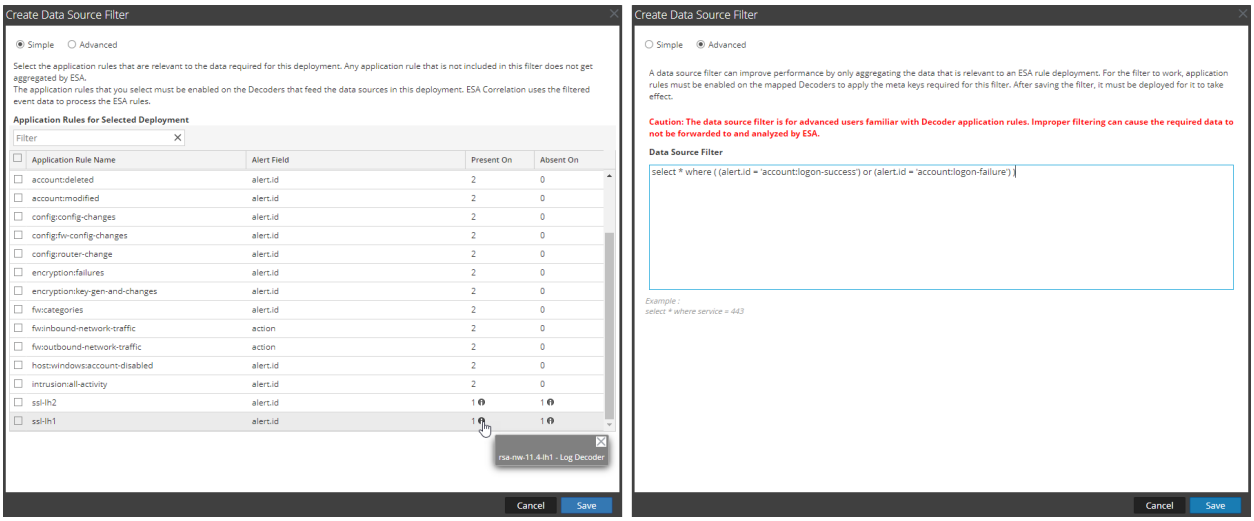
For more information, see “Validate an ESA Rule” and “Validate an Advanced EPL Rule” in the Alerting with ESA Correlation Rules User Guide.

Esper Version Upgraded from version 8.2.0 to 8.4.0

In NetWitness Platform 11.5, ESA Correlation supports Esper version 8.4.0.

A Filter Option is Available for ESA Rule Deployment Data Sources

To improve performance, users can add an optional data source filter to their ESA rule deployment so that only the data relevant to the deployment is forwarded to ESA. The filter is comprised of application rules, which are applied to the Decoders mapped to your selected data sources.



Caution: The data source filter is intended for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

For more information, see "(Optional) Add a Data Source Filter" in the Alerting with ESA Correlation Rules User Guide.

Advanced EPL Rules Can Dynamically Update Context Hub Lists

The @RSAContext annotation can be used in advanced rules to dynamically add or remove data from a Context Hub list after the rule fires. For example, users can create a rule that automatically adds an IP address to a blacklist and removes it from a whitelist.

Users can update a single-column or a multi-column Context Hub list. The @RSAContext annotation also performs error handling when the Context Hub list cannot be reached.

For more information, see "@RSAContext Annotation (11.5 and later)" in the Alerting with ESA Correlation Rules User Guide.

Administration and Configuration

New Permissions for Investigate to Filter Events and Manage Meta Groups in the Events View

Three new `investigate-server` permissions allow administrators to control new features in the Events view. Analysts can use the Filter Events view, a BETA feature for the Events view, and they can view and manage meta groups in the Events view. The new permissions, are enabled by default for most roles. When upgrading to version 11.5, the administrator needs to add these permissions for any existing custom roles: `investigate-server.event.filter`, `investigate-server.metagroup.read`, and `investigate-server.metagroup.manage` For additional information, refer to "Change Permissions Assigned to a Role" in (Optional) Add a Role and Assign Permissions.

Manage Permissions for the New Respond Saved Filters for Incidents and Alerts Lists

The following permissions are required for the incidents and alerts saved filters in the Respond view (Respond > Incidents and Respond > Alerts): `respond-server.incident.manage`, `respond-server.incident.read`, `respond-server.alert.manage`, and `respond-server.alert.read`. The Analysts role has the required Respond filter permissions by default. For more information, see "Respond-server" in Role Permissions.

Reporting Engine Content Administrator Role for Deploying Reporting Engine Content

RSA NetWitness® Platform introduces a new role "Reporting Engine Content Administrators" for deploying Reporting Engine content from Live. Users with the Reporting Engine Content Administrators role can search and deploy Reporting Engine content (rules, reports, charts, schedule and lists) from Live and view or modify the deployed content, thus eliminating the need of asking the administrator to add permissions to the deployed content. For more information, see the System Security and User Management Guide.

New Tool for Reporting Engine Service Auto-Recovery

RSA NetWitness® Platform introduces a new Reporting Engine Migration Recovery Tool for restoring the Reporting Engine service when the Reporting Engine service fails to restart after an upgrade. For more information, see Reporting Engine Migration Recovery Tool.

Option to Stop a Running Scheduled Reporting Engine Report

Previously if multiple scheduled executions of a report are running at the same time without completing, there was no ability to stop them manually. Now, if there are multiple Reporting Engine schedules executing at the same time for any scheduled report, the analyst can stop these individually if needed. For more information, see the Reporting User Guide.

Improved Process for Changing IP Addresses

Administrators can now change an IP address, netmask, or gateway for any host within their environments with minimal interruption of operations. The nwsetup-tui script has been updated to streamline the process of changing the network configuration of NW Server and component hosts. For more information, see “Change Host Network Configuration” in the System Maintenance Guide.

Warm Standby NW Server Can Have Different IP Address Than Active NW Server

Administrators now have the capability to deploy a standby NW Server into different network zones and geographical locations. A different IP address (than the primary) can be assigned to the NW Standby Server, giving administrators added disaster recovery capabilities. For more information, see “Fail Over Primary NW Server to Secondary NW Server with Different IP Address” in Warm Standby NW Server Host.

Context Hub

Expand Threat Detection With Improved Threat Intel (Via STIX) Integrations

NetWitness Platform’s integration with Structured Threat Intelligence Expression (STIX) enhances the threat detection capabilities with improved threat intel information to detect and respond to attacks in a timely manner. Now, when an analyst investigates threat intelligence information retrieved from a STIX data source, the context for each indicator is displayed. The context information includes viewing the adversary and the attack details directly from Context Hub, in both Investigate and Respond views.

For the analyst to use this capability, an administrator configures the STIX data sources to retrieve the threat intelligence data from the specified STIX source.

For more information, see the Investigate User Guide and the NetWitness Respond User Guide.

After the configuration, the analyst can push the custom feeds using the custom feed workflow. The supported data sources are TAXII Server, REST Server and File. For more information, see the Context Hub Configuration Guide.

Log Collection

More and more log event sources are making logs available via non-standardized APIs rather than traditional methods such as syslog or SNMP. This has resulted in each source requiring a client, or plugin, be written for each API in order to collect these logs. The upside is that these logs are usually offered in a structured format, such as JSON. In NetWitness 11.5 we have added features to make it much easier to collect and parse log event sources in an open manner.

Logstash Support

Logstash is an open source data collection engine with real-time pipelining capabilities and a thriving, open community. Dozens of plugins are supported for collection, parsing, and transformation of logs. NetWitness can now accept logs collected from Logstash allowing collection from event sources that do not have any other native NetWitness collection or parsing support. As part of the process, the logs are forwarded as JSON and, using the new JSON mapping UI within the NetWitness platform, the parsed Logstash data can be easily mapped to NetWitness meta. For more information, see the Logstash and NetWitness Integration Guide.

Native JSON Log Support & BETA UI

NetWitness 11.5 introduces the ability to parse logs in a JSON format. This allows analysts to view the logs in their native format which allows them to understand the original context and correlate that data to indicators of compromise from threat intelligence sites. A new user interface (BETA) within the NetWitness UI allows admins to map JSON keys in a log to the appropriate meta keys in NetWitness. This mapping removes the need to transform the log and build a parser. For more information, see the Log Parser Customization Guide.

Raw Pass-through Options for Log Collector Plugins

As NetWitness can now parse JSON event data directly on the Log Decoder, there is no longer a need to transform most cloud logs into CEF. Previously, plugins had to be tailored to each JSON schema individually to transform them to CEF. Now, all of the raw JSON event data can be sent straight to the Log Decoder. This allows NetWitness to keep the logs in their native format for correlation with threat intelligence sites. It also enables NetWitness plugins to accomplish API based log collection in a universal manner, such as having many source types forward logs through AWS CloudWatch without needing a new plugin created.

Note: The Proofpoint and Azure Monitor collector plugins are updated to use JSON-formatted parsers. These parsers must be deployed from RSA Live to support the JSON format.

Licensing

RSA NetWitness® Platform introduces a Network Meta-Only license in addition to the Network Full Packet license. The Network Meta-Only license captures and analyzes packet payloads and discards the packet payload data after analysis. Using this license, NetWitness Platform can be deployed in an environment where full packet capture is not required. This helps to optimally manage the storage space and easily detect threats without the need to retain the full payload of the sessions. The Network Meta-Only license measures the bytes analyzed for the network packets and can be used with or without the Network Full Packet license. For more information, see the Licensing Management Guide.

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

Log Collection Fixes

Tracking Number	Description
ASOC-94276	Improved TCP Syslog Performance.

Administration Fixes

Tracking Number	Description
SACE-13620	In version 11.4, unable to deploy recursive feeds on the Decoder group.
SACE-13572	When querying using the msearch option, it displays "Year is out of valid range: 1400..9999" error.
SACE-13278	After upgrading to 11.4, the Login Banner does not display while logging in to the NetWitness Platform.
SACE-13124	Raid Tool Script fails if a disk in a 15 drive Viper Shelf is in a 'UBad' state.
SACE-13060	In the Define Email Notifications panel, unable to enter an email address with domain name, if the domain name has letters after (.) symbol. For example, XXX@innotec.security.com

Audit Logging

Tracking Number	Description
ASOC-85468 / ASOC-86055	Logstash does not reconnect to RabbitMQ, if RabbitMQ is reset.

Tracking Number	Description
ASOC-77307	Audit Logs do not have enough context when an ESA rule is created, duplicated, or deleted on the Rule Builder. In NetWitness Platform 11.5, in addition to the audit logs available on ESA Correlation-server, new audit logs on the NW Server show when users add, modify, filter, delete, export, and import ESA rules in the Rule Library. The NW Server audit logs also show when users add, modify, and deploy ESA rule deployments. Modifications to an ESA rule deployment include adding, deleting, or updating a rule in a deployment as well as adding a data source or an ESA Correlation service to a deployment.

Investigate Fixes

Tracking Number	Description
ASOC-92642	Refocusing a value that contains the backslash (\) character in the Events view does not return results.
ASOC-92534	In the email reconstruction, the Download button for attachments is not enabled due to a filename mismatch.
ASOC-85375	Unable to query meta keys with values and meta values are truncated for some characters like ®.
ASOC-50412	When initiating a download, Investigate fails to connect to the browser job tray and the download spinner remains indefinitely.

Respond Fixes

Tracking Number	Description
ASOC-83210	Incident email notifications are missing "Changed by" fields. In NetWitness Platform 11.4, when an automatically generated incident was updated, the email notification failed to display the "Change By" field showing the timestamp and user associated with the update. This is fixed in 11.5.
ASOC-80896	Incidents generated by Reporting Engine alerts display cleartext values despite Data Privacy being enabled. Previously, in deployments where data privacy is enabled, incidents aggregated from Reporting Engine alerts were displaying cleartext metadata due to both cleartext and hashed values getting published. Now, when data privacy is enabled, the Reporting Engine only sends hashed / obfuscated values to Respond, which maintains data privacy when analysts view incidents.

Tracking Number	Description
ASOC-73173	Matching files are not displayed in the Files tab if the file name in the event does not match the global file name. Previously, when you pivoted to the Investigate > Hosts or Files tab from the Nodal Graph to analyze a file, if the file name in the event did not match the case of the global file name, no results were displayed. Now, case sensitivity is no longer an issue when pivoting to the Investigate > Hosts or Files tab.

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

Tracking Number	Description
ASOC-90740	Log Decoder service was core-dumping at restart.
SACE-13702	When querying the Broker through Rest API, it displays incorrect results.
SACE-13597	For a TLS session, the meta keys for Ja3/Ja3s and cert.thumbprint are generated.

Event Stream Analysis (ESA) Fixes

Tracking Number	Description
ASOC-87778	An ESA Rule Deployment name with a colon (:) throws a failed to start stream error. If an ESA rule deployment name contains a colon (:), data aggregation fails to start during deployment. This is not an issue in NetWitness Platform 11.5.
ASOC-77307	Audit Logs do not have enough context when an ESA rule is created, duplicated, or deleted on the Rule Builder. In NetWitness Platform 11.5, in addition to the audit logs available on ESA Correlation-server, new audit logs on the NW Server show when users add, modify, filter, delete, export, and import ESA rules in the Rule Library. The NW Server audit logs also show when users add, modify, and deploy ESA rule deployments. Modifications to an ESA rule deployment include adding, deleting, or updating a rule in a deployment as well as adding a data source or an ESA Correlation service to a deployment.

Tracking Number	Description
SACE-12736	Multiple users can edit an ESA rule deployment at the same time and overwrite changes. If two users modify the same ESA rule deployment by adding or removing rules, whoever clicks **Deploy Now** first overwrites the changes of the other user. In NetWitness Platform 11.5, multiple users can edit an ESA rule deployment at the same time and not overwrite changes.

Reporting Engine Fixes

Tracking Number	Description
SACE-12893	Reports > Alert tab, does not display all the alerts when queried for a custom time range.

Endpoint Fixes

Tracking Number	Description
ASOC-86942	Endpoint server is often found in Unhealthy state after a day of deployment.
SACE-13763	Unable to install NetWitness Endpoint Agent on Redhat 8.x system.
SACE-13529	Test connection fails for Relay Server with Endpoint Log Hybrid.

Upgrade Fixes

Tracking Number	Description
SACE-12658	When running the nwsetup-tui command on the CLI for configuring the static IP address , it fails.
SADOCS-1883	Request for pre-upgrade steps to clear out repositories from previous releases. These instructions have been added to the *Upgrade Guide for RSA NetWitness Platform 11.5*.

Known Issues

Issues that remain unresolved in this release are documented in the RSA NetWitness® Platform Known Issues list on RSA Link:
https://community.rsa.com/community/products/netwitness/documentation/known-issues

Wherever a workaround is available, it is noted or referenced in detail.

End of Life Functionality

The following table provides information on end of life functionality and features in RSA NetWitness® Platform 11.5 or later releases.

End of Life Functionality and Features in 11.5.0.0 or later releases

Note: Event Stream Analysis (ESA) is not end of life. The ESA Correlation service (ESA Correlation Rules) is supported. The Event Stream Analytics Server service (ESA Analytics), which is used for Automated Threat Detection, is EOL. In its place, you can use ESA Correlation as it offers more functional capabilities and better performance.

Feature	Notes
ESA Analytics / Automated Threat Detection	The Event Stream Analytics Server (ESA Analytics) service is end of life (EOL) and not supported in NetWitness Platform version 11.5 and later. The ESA Analytics Mapping panel is no longer in the user interface (Admin > System).
WhoIs Lookup Service	The WhoIs Lookup Configuration panel, used for ESA Analytics, is no longer in the user interface (Admin > System).
Warehouse Analytics	Legacy Warehouse Analytics is not supported in NetWitness Platform 11.0 or later releases and is no longer in the user interface.

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 Upgrade Guide	https://community.rsa.com/docs/DOC-112676

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 11.5.0.0.

Component	Version Number
NetWitness Platform Audit Plugins	11.5.0.0-4615.5.3fd9584cb.el7.noarch.rpm
NetWitness Platform Appliance	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Archiver	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Broker	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Concentrator	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Config Management	11.5.0.0-2008111220.5.ff9e424.el7.noarch.rpm
NetWitness Platform Config Server	11.5.0.0-200710072900.5.bd6a63c.el7.centos.noarch.rpm
NetWitness Platform Console	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Content Server	11.5.0.0-200630183429.5.512a4b8.el7.centos.noarch.rpm
NetWitness Platform ContextHub Server	11.5.0.0-200728093949.5.488ccfe.el7.centos.noarch.rpm
NetWitness Platform Correlation Server (ESA)	11.5.0.0-200806185527.5.4bcdaf3.el7.centos.noarch.rpm
NetWitness Platform Decoder	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Deployment Upgrade	11.5.0.0-2006261254.5.22cec34.el7.noarch.rpm
NetWitness Platform Endpoint Agents	11.5.0.0-2006151822.5.4bdbb4a.el7.x86_64.rpm
NetWitness Platform Endpoint Broker Server	11.5.0.0-200619040007.5.686adbd.el7.centos.noarch.rpm
NetWitness Platform Endpoint Server	11.5.0.0-200619014840.5.8b18a0a.el7.centos.noarch.rpm

NetWitness Platform Integration Server	11.5.0.0-200710042756.5.4e8cb86.el7.centos.noarch.rpm
NetWitness Platform Investigate Server	11.5.0.0-200708104951.5.5091482.el7.centos.noarch.rpm
NetWitness Platform Legacy Web Server	11.5.0.0-200810151928.5.9b5bd42.el7.centos.noarch.rpm
NetWitness Platform License Server	11.5.0.0-200709025209.5.da37a84.el7.centos.noarch.rpm
NetWitness Platform Log Decoder	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Log Player	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Malware Analytics Server	11.5.0.0-200723090201.5.461916c.el7.centos.x86_64.rpm
NetWitness Platform Metrics Server	11.5.0.0-200724014709.5.4d136f3.el7.centos.noarch.rpm
NetWitness Platform Orchestration Server	11.5.0.0-200805133852.5.bc285ed.el7.centos.noarch.rpm
NetWitness Platform Reporting Engine Server	11.5.0.0-5866.5.ddb451a8b.el7.x86_64.rpm
NetWitness Platform Respond Server	11.5.0.0-200731030842.5.f45aff7.el7.centos.noarch.rpm
NetWitness Platform Root CA Update	11.5.0.0-2006261255.5.470ba8b.el7.noarch.rpm
NetWitness Platform SDK	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Security Server	11.5.0.0-200722041910.5.50e951c.el7.centos.noarch.rpm
NetWitness Platform Source Server	11.5.0.0-200624103220.5.1add390.el7.centos.noarch.rpm
NetWitness Platform User Interface	11.5.0.0-200804200134.5.b715e6362d.el7.centos.noarch.rpm
NetWitness Platform Workbench	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform SA Tools	11.5.0.0-2006261246.5.4688bd1.el7.noarch.rpm
NetWitness Platform SMS Runtime	11.5.0.0-4615.5.3fd9584cb.el7.x86_64.rpm
NetWitness Platform SMS Server	11.5.0.0-4615.5.3fd9584cb.el7.x86_64.rpm

Revision History

Date	Description
August 2020	Release to Operations
September 2020	Initial Release