RSA® NetWitness Platform

Version 11.6

Release Notes

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.

May 2021

Contents

What's New

The RSA NetWitness Platform 11.6 release provides new features and enhancements for every role in the Security Operations Center.

Upgrade Paths

The following upgrade paths are supported for NetWitness Platform 11.6.0.0:

- RSA NetWitness Platform 11.4.x.x to 11.6.0.0 *
- RSA NetWitness Platform 11.5.x.x to 11.6.0.0

* If you are upgrading from 11.2.x.x, 11.3.x.x, you must upgrade to 11.4.x.x before you can upgrade to 11.6.

For more information on upgrading to 11.6.0.0, see Upgrade Guide for RSA NetWitness Platform 11.6

If you are upgrading from version below 11.4.x.x, you must first upgrade to 11.4.x.x before you upgrade to 11.6.0. For more information, see the *Upgrade Guide for RSA NetWitness Platform 11.4.1.1*. This guide applies to both physical and virtual hosts (including AWS and Azure Public Cloud).

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
- Endpoint Investigation
- Broker, Concentrator, Decoder, and Log Decoder Services
- Event Stream Analysis (ESA)
- Administration and Configuration
- Context Hub
- Log Collection
- Licensing
- Platform

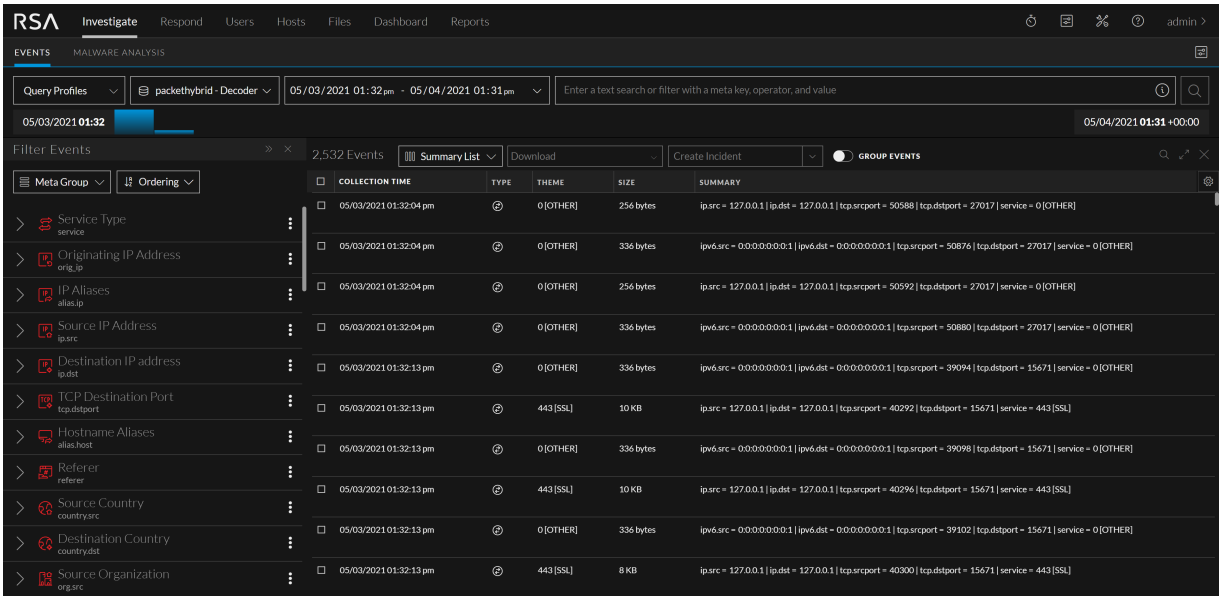
To locate the documents referred to in this section, go to the RSA NetWitness Platform 11.x Master Table of Contents. Product Documentation has links to the documentation for this release.

Investigation - SIEM and Network Traffic Analysis

Investigation Enhancements

- ### Faceted Search

  The new faceted search layout of the default Events view makes interacting with large amounts of data collected from the enterprise a more familiar experience and efficient workflow. By combining the functions of the Navigate and Event views, analysts can apply filters by interacting with any metadata generated by the platform which in turn creates the query and automatically executes a search to fetch the resulting events.



Organize Investigate Content (Column groups, Meta groups and Query Profiles)

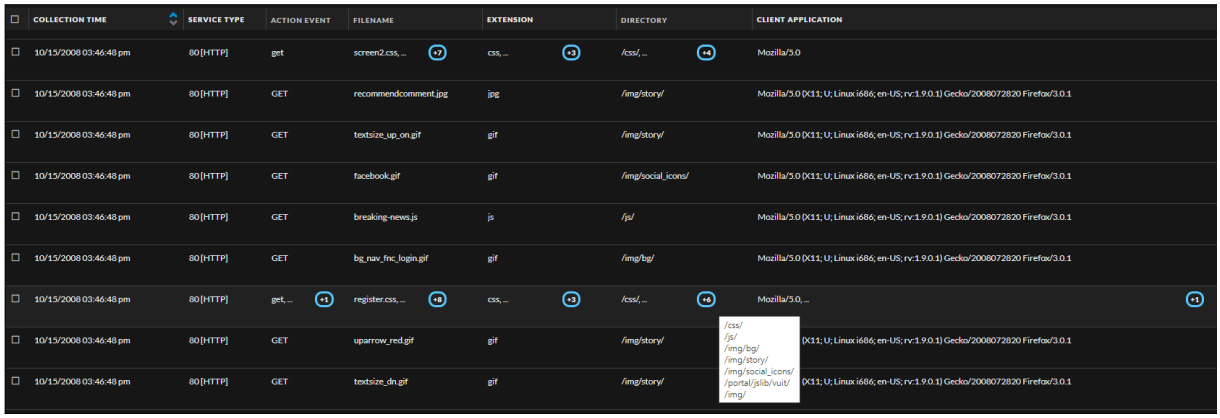
All Investigate content is displayed in a folder structure to help analysts organize their views depending on use cases. The RSA Groups (RSA Live content and RSA OOTB groups), and Shared group folders are available to all analysts. All Private groups, folders and sub-folders are displayed only to the analysts who created them. You can create, edit, copy, and delete Shared and Private folders and sub-folders.

Deliver Investigate Content (Column groups, Meta groups and Query Profiles) using RSA Live

Investigate content can be deployed using RSA Live providing updates outside the NetWitness release cycle. Analysts now have the ability to utilize the latest Investigate content to focus their view into the data based on use cases. All the RSA generated content is now contained in a RSA specific folder.

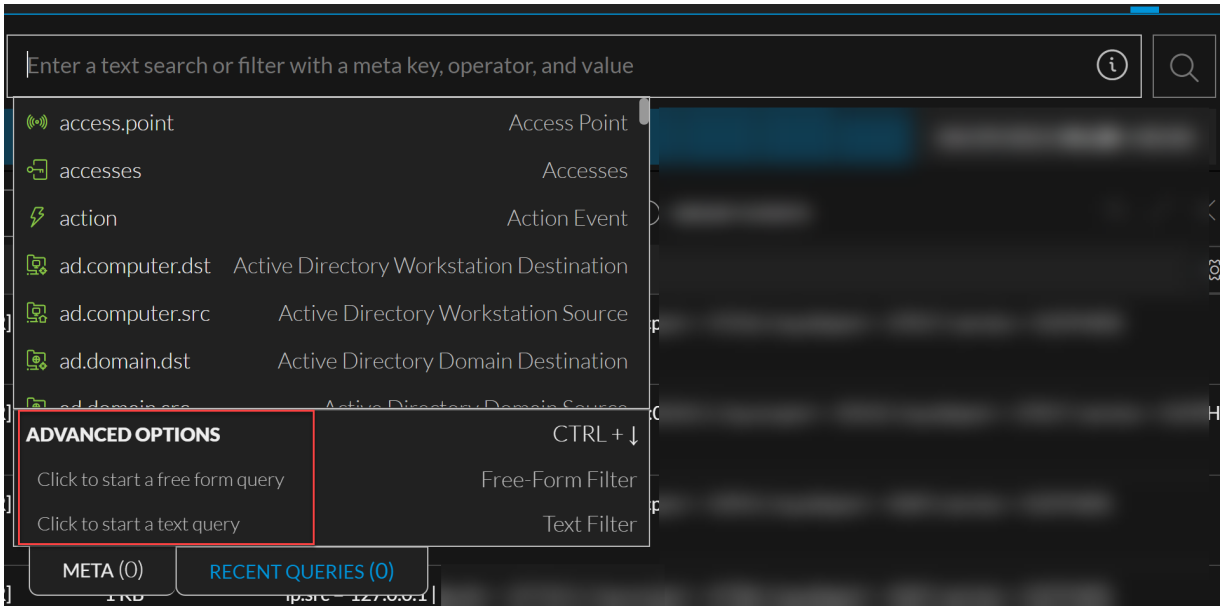
Multiple values

When investigating a list of events an analyst can see that an event has multiple values for a meta key in that specific session. A hover over indicator shows a list of multiple values that can be further investigated without requiring to drill into the reconstruction of the event.



Direct Free-form query or text search

To immediately create a blank free-form filter, an advanced user can select the option "**Click to start a free form query**" from the Advanced Options panel. In the same manner an analyst can choose "**Click to start a text search**" to create a new text search. In both scenarios, the analysts can bypass the auto-completion input logic and save some time in generating a query format.



Query filter enhancements

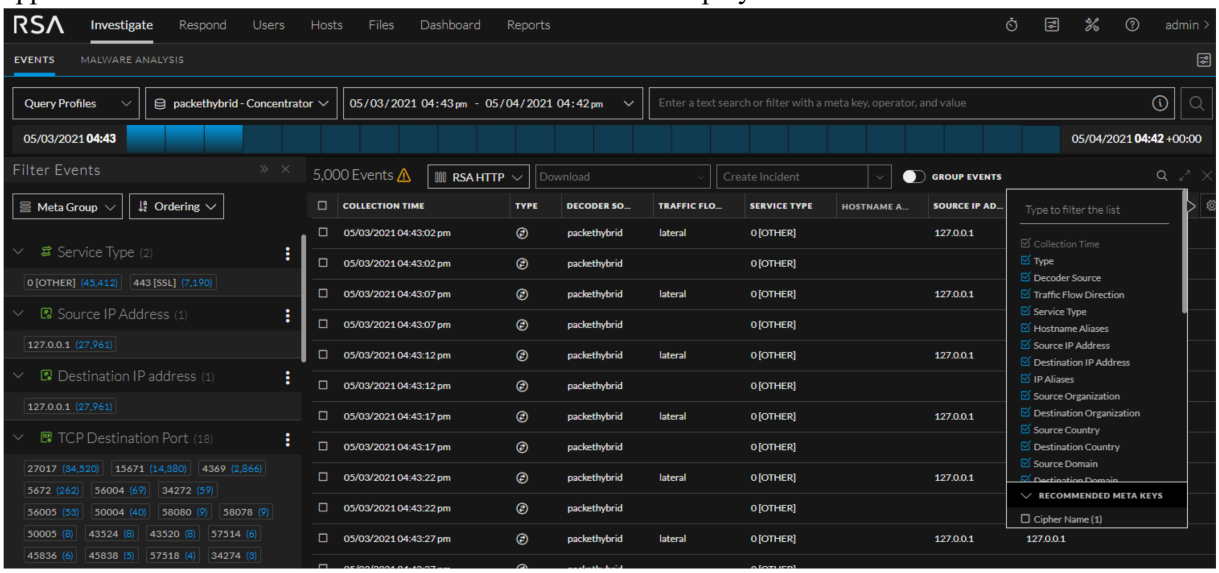
When a query is added in the Events, any filter that is selected will have a red highlighted border, so the analyst knows which filter is selected. When you edit a filter, the border will be in blue color to indicate that the analyst needs to provide some input in case they move their focus away from the query input.

Custom Column group enhancements

Metadata such as `custom.logdata` that are defined in Legacy Events or defined in OOTB Summary List column group can be used to combine the raw logs as a customized column of additional metadata. List of recommended metas that contain data are displayed. An analyst can create custom column groups using the summary and raw log (`custom.logdata`) meta keys.

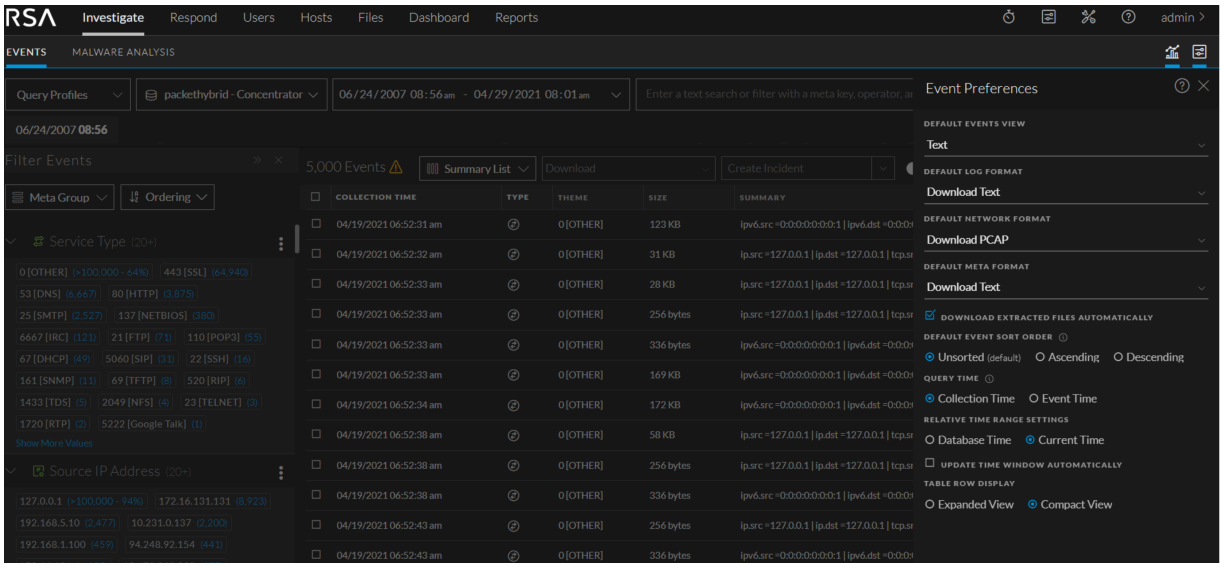
Column Group Meta Key Recommendations

While reviewing query results in the Events table with a selected column group, analysts have the option to view recommended columns that may have data for those events but are not part of the current column group. These suggested meta keys help analysts to have the best column groups applied so that no relevant data is missed for the events displayed.



Investigate Screen Layout Options

A new user preference allows analysts to choose between a Compact or Expanded format to determine how close the rows of data are to be displayed in the Event table on a single page. The following image is an example where Event Preference view is displayed with the Compact view selected.



Meta Panel Enhancements

The meta panel on the Events investigation page has been enhanced with a **Hide Duplicate Entries** radio button to limit the display of metadata only if they are a unique key value pair. A filter field is also introduced so analysts can search, and filter based on meta keys or values.

IndexNone Meta keys

As analysts create meta groups with multiple meta keys, the Open option is disabled for all non-indexed meta keys to avoid adverse effects on query performance.

Reconstruction Enhancements (view content and copy option)

The pagination of the **Text** tab has been enhanced to make it more obvious when there is further content available than can be displayed on a single page. Also, if required analysts can copy selected content to the clipboard using keyboard shortcut (in addition to menu option) for further investigation.

Search Indicator

When analysts do a free-text search a message is displayed on top of the Events page to make it clear that only indexed metadata is being searched. This message contains a link that helps in further search if the analysts requires to search more extensively beyond what is indexed. In case the maximum search limit has been reached, a message is displayed at the bottom to indicate there are no more results available.

Investigate Timeout Setting

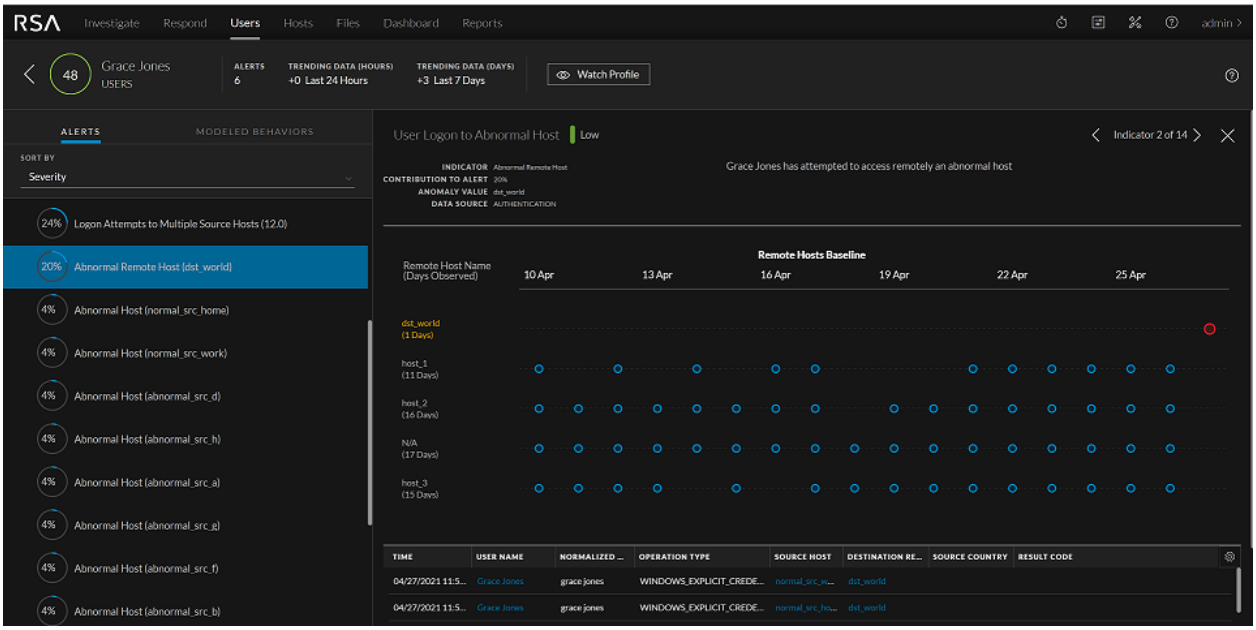
The Extraction timeout setting helps an administrator to increase or decrease the time available to retrieve the required sessions or events or files from Investigate. This can be configured by navigating to **Admin** > **System** > **Investigation** > **Common Settings.**

For more information on all the Investigation Enhancements, see *NetWitness Investigate User Guide*.

User Entity Behavior Analytics

New and Enhanced Chart

A new and enhanced dotted chart is introduced in version 11.6. The dotted chart, provides the analyst with the entities baseline values over time to better understand the context of the modeled behavior and the anomaly in case of an indicator. In version 11.6, the pie chart is replaced with a dotted chart to provide analysts with additional visibility to the entities activity over time. For more information, see *NetWitness UEBA User Guide*.



Incident Response

Respond Persist Data (BETA)

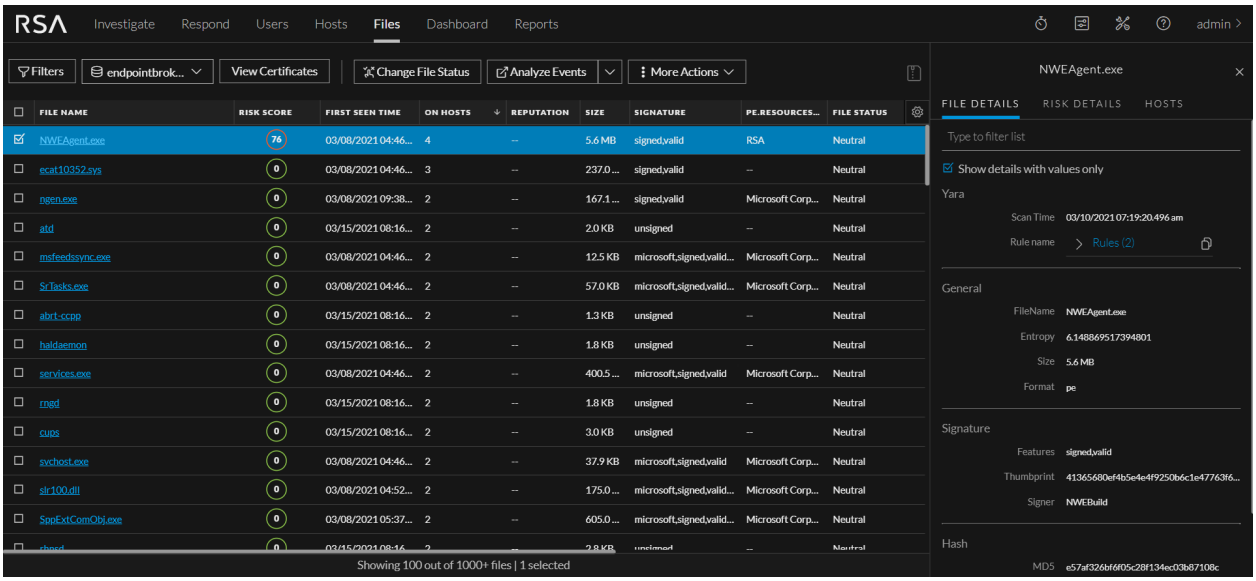
Analysts and Administrators can pin events that are associated with particular incidents, thereby enabling you to view the evidence related to an incident in the future. Once you pin an event, data is copied from the regular database into a long term storage cache within the data source. Event retention depends upon the available space in the directory (10 GB is offered by default). The roll over in the meta database does not impact the events that already saved in the pin directory. The BETA version comes with the limitation where you cannot download the pinned events, which will be enabled and notified in the subsequent releases.

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

Endpoint Investigation

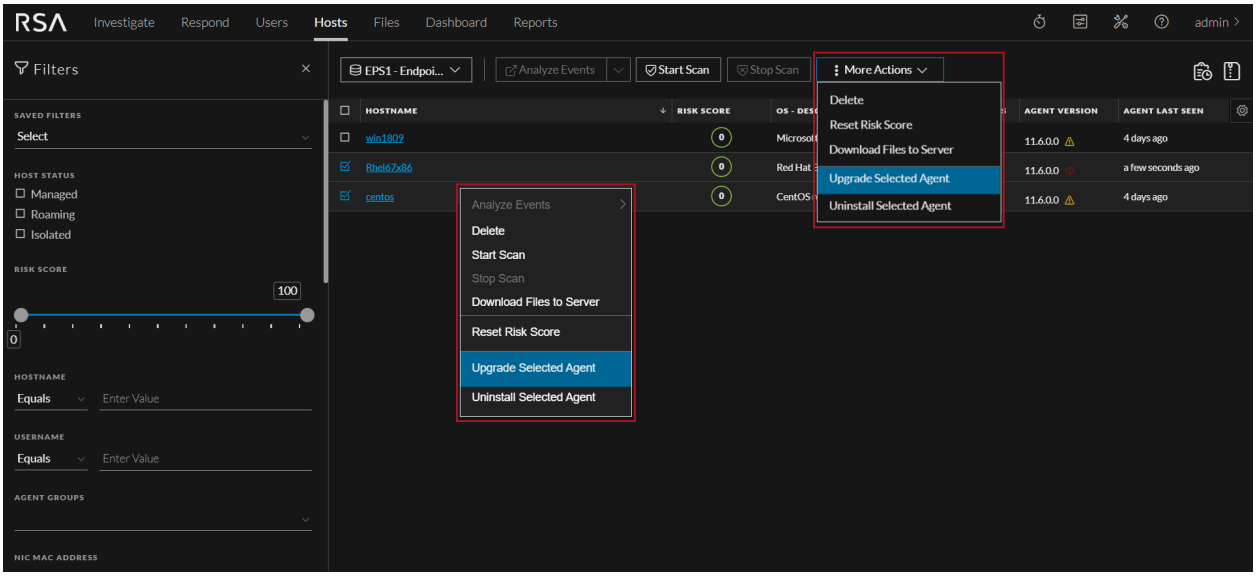
Support for YARA scans

YARA helps analysts with rule-based detection capabilities in identifying and classifying malware. You can easily create malware descriptions, called YARA rules, that are robust in detecting malware. YARA automatically scans downloaded files at regular intervals and increases the file's risk score if it matches any rule. Thus, helps analysts quickly respond to a threat. For more information, see *NetWitness Endpoint User Guide*. To learn how to enable and configure YARA, see *NetWitness Endpoint Configuration Guide*.



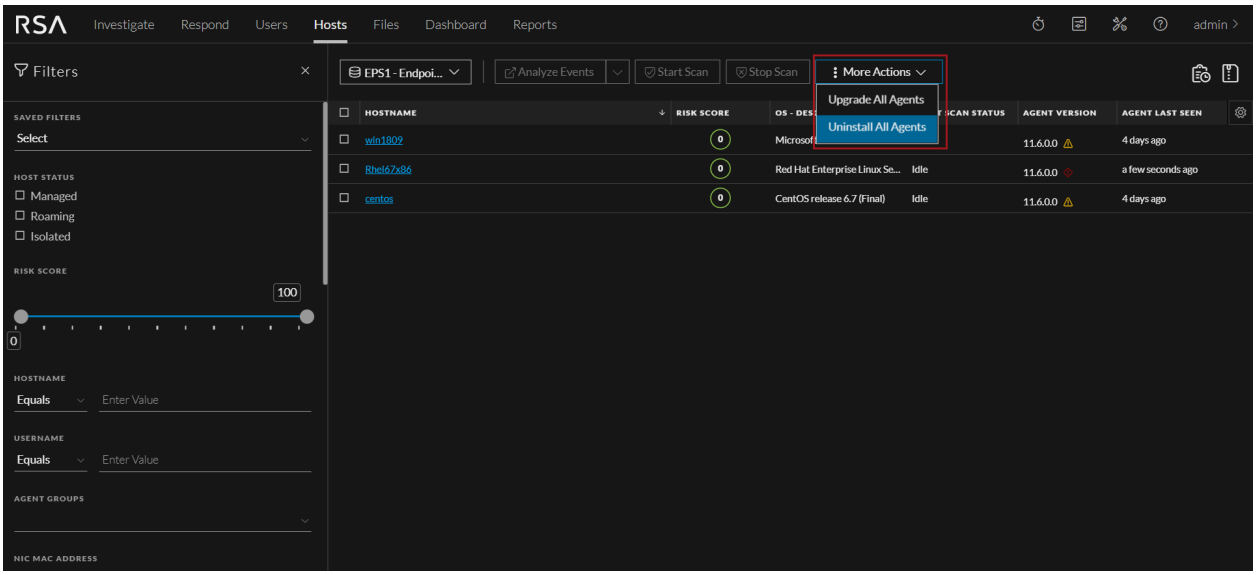
Centralized agent upgrade options using UI

Administrators can now upgrade and uninstall selected or all agents using the UI and thus helping you manage NetWitness agents with a lot of ease. For more information, see *NetWitness Endpoint Agent Installation Guide*.



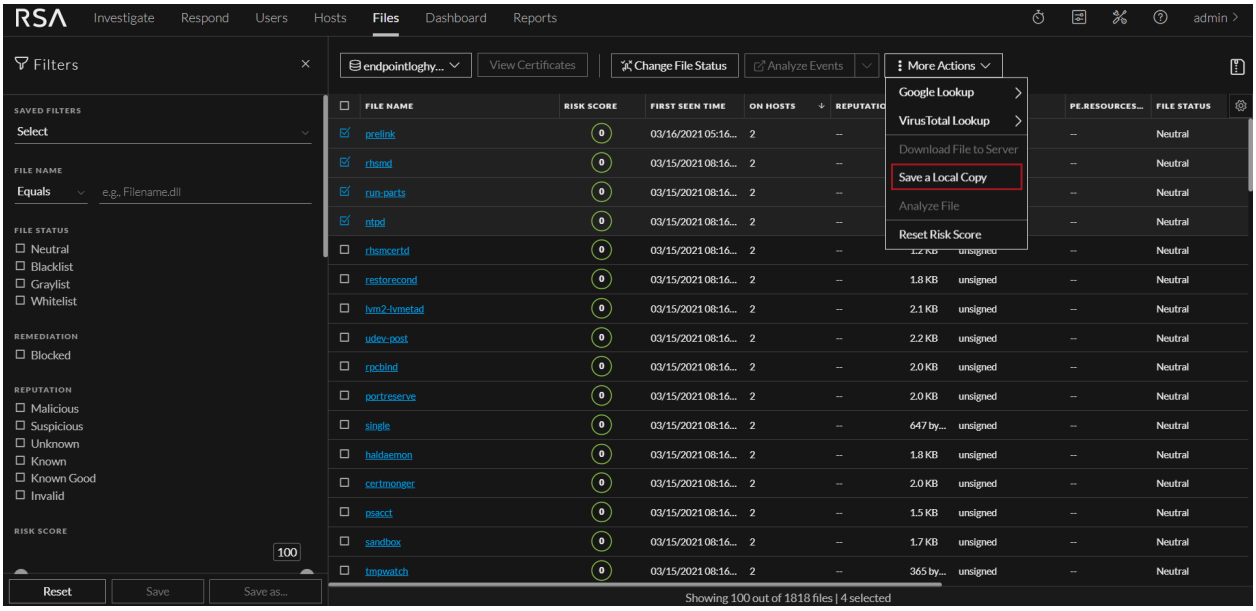
Centralized agent uninstall options using UI

Administrators can uninstall selected agents or all the agents easily using the UI. Bulk uninstall can be performed without even selecting any hosts. This enhancement will save time and help to focus more on responding to threats. To qualify for bulk uninstall, the agents must be on version 11.5.1 or later. For more information, see *NetWitness Endpoint Agent Installation Guide*.



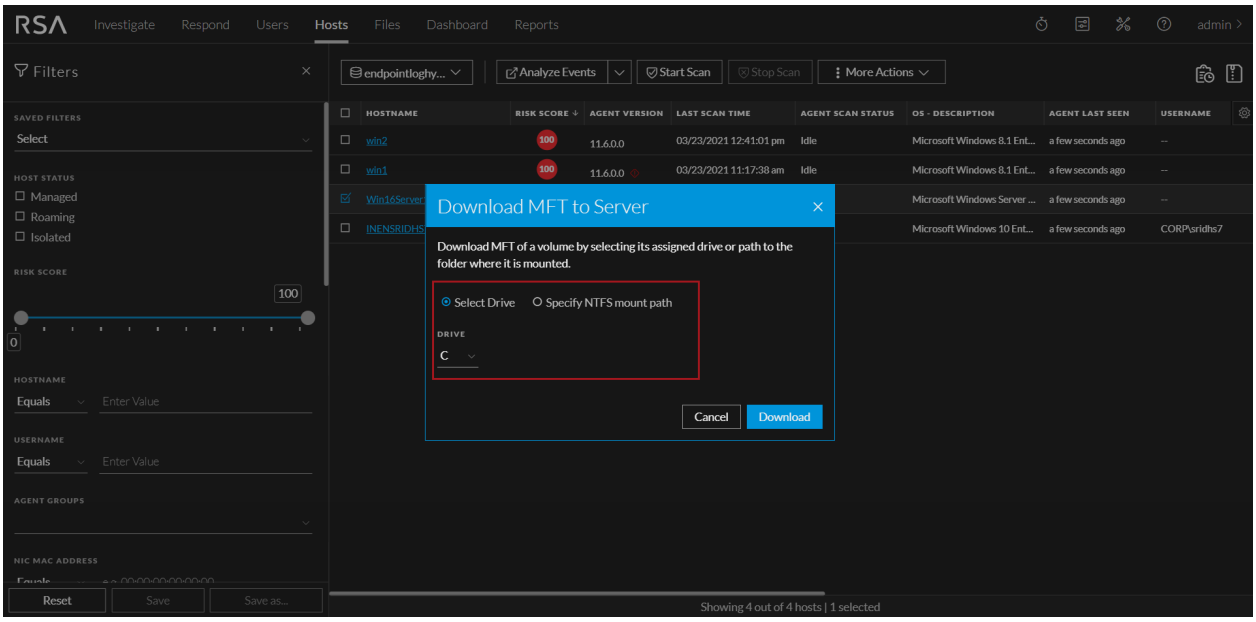
Support for Saving Local Copies of Multiple Downloaded Files

Now analysts can perform detailed investigations and forensics quickly and easily by saving copies of downloaded system dump, process dump, MFT, etc.



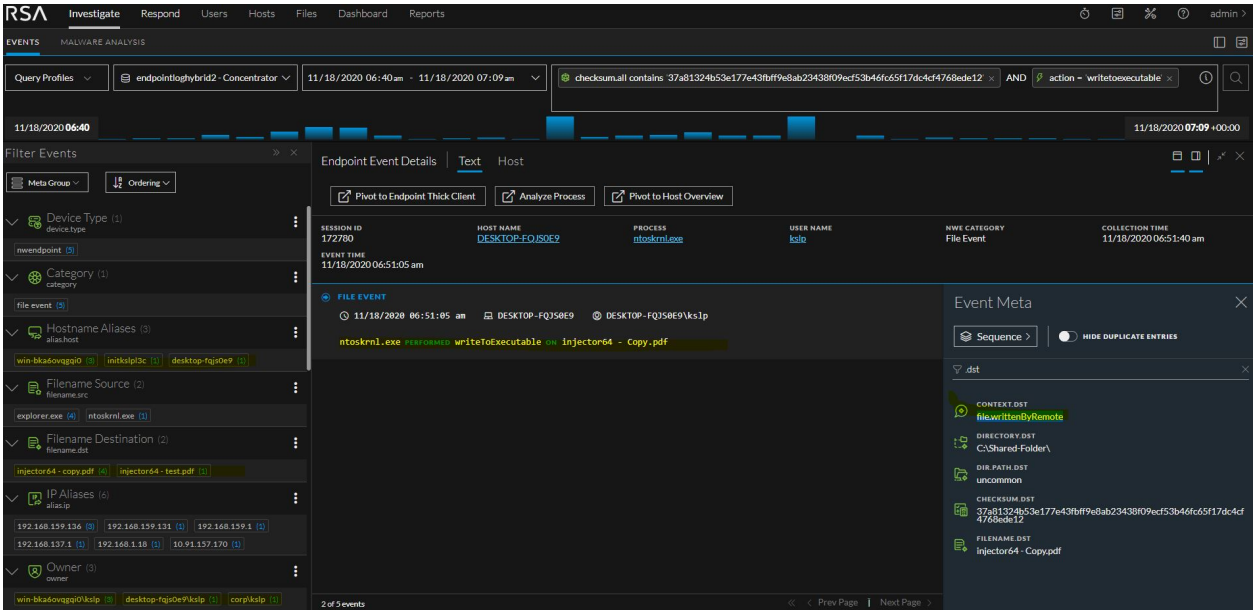
Support to Download MFT From Any Windows Drive

Analysts can now download MFT for any drive and can also download it on the NTFS mount path. This can help analysts perform critical investigation, analysis, and forensics on files in addition to the system volume.



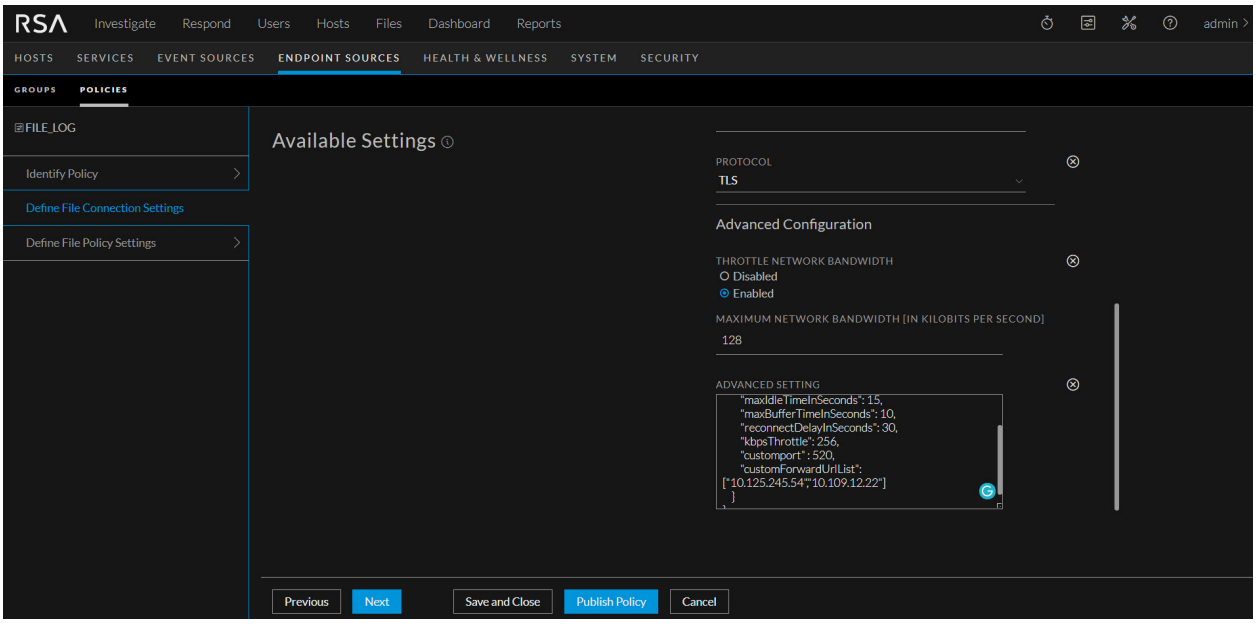
Expanded Lateral Movement Visibility

Enhanced Windows agent to report executable write events on the target machine when copied to network shares. Analysts can now have deeper visibility into lateral movement activities on Windows around files that are being copied to network shares.



Support for Forwarding Windows/File Logs to Custom Systems

Administrators can now collect the Windows and File logs on a non-VLC system by forwarding them to a custom system.



New rules added to detect Persistence tactic

New rules have been added to the Endpoint rules bundle to detect threats that follow the Persistence tactic. When such a threat is detected, these rules will trigger alerts and increase the risk score.

Broker, Concentrator, Decoder, and Log Decoder Services

Assembler Threading Modes

To enhance the throughput at which a Decoder can analyze data, the assembler is enhanced to perform further parallel processing. The process that reassembles captured packets into streams is known as the assembler. You can now customize the assembler operation using its two modes. These modes can be configured by setting the value of `assembler.threading.enabled` to `on` or `off`. The default value is `off`. The `on` mode enables higher throughput as each assembler instance operates on a dedicated processor.

The assembler modes work only when Multi Adapter Packet Capture is enabled. For more information on Multi Adapter Packet Capture and Assembler Modes, see the "(Optional) Multiple Adapter Packet Capture" topic in the *Decoder and Log Decoder Configuration Guide*.

High Speed Packet Capture

You can now analyze network data (packets) from higher speed networks and optimize your Network Decoder to capture network traffic up to 40 Gbps. In order to understand what capabilities are supported at different network speeds, the Decoder now operates in the following three modes:

1. **Normal:** For capture speeds less than 5 Gbps with large amounts of deep packet inspection while storing network sessions. This is the default mode.
2. **10G:** For capture speeds up to 10 Gbps with medium amounts of deep packet inspection while storing network sessions.
3. **NDR:** For capture speeds greater than 10 Gbps but less than 40 Gbps with small amounts of deep packet inspection while only storing metadata.

For more information on high speed capture and how to configure it, see the "Configure High Speed Packet Capture Capability (Version 11.6 and Later)" topic in the *Decoder and Log Decoder Configuration Guide*.

Support for Brotli Decompression

Decoder now detects and decompresses the Brotli payload in the HTTP/HTTPS session parsing. Brotli is a data format specification that compresses data streams with a specific combination of the general-purpose LZ77 lossless compression algorithm, Huffman coding, and 2nd order context modelling. Brotli encoding is supported by most web browsers, major web servers, and some CDNs.

To enable Brotli decompression, perform the following steps:

- For information on the HTTP decompression configuration, see the "HTTP Parsers" topic in the Decoder and Log Decoder Configuration Guide.
- For information on the HTTP_lua decompression configuration, see the "HTTP Lua Parser Options" topic in the RSA NetWitness® Platform Threat Intelligence Guide.

Support for OpenApp ID

Decoder can identify applications using the OpenApp ID detectors generating new metadata (`app.id`). It helps analysts to identify applications in a session. OpenApp ID from Cisco is an application-layer network security plug-in for Snort (an open source network intrusion detection system). It is a set of open source Lua libraries (detectors) that identifies applications in the network traffic.

For more information on OpenApp ID and how to configure detectors, see the "(Optional) Configure Decoder to Support OpenApp ID" topic in the *Decoder and Log Decoder Configuration Guide*.

Support for Receive Side Scaling

To enhance the throughput at which a Decoder can analyze data, the pipeline to create sessions is enhanced to use Receive side scaling (RSS). RSS enables the efficient distribution of network receive processing across multiple CPUs in multiprocessor systems. RSS ensures that the processing that is associated with a given connection stays on the assigned CPU. RSS is supported on DPDK devices only using ixgbe or i40e device drivers.

For more information, see the "(Optional) Data Plane Development Kit Packet Capture" topic in the *Decoder and Log Decoder Configuration Guide*.

Simultaneous Ingestion of the Encrypted and Decrypted Traffic Streams to Decoder

Decoder with multi-adapter capture and multi-thread assembler features enabled, can receive encrypted and decrypted streams of the same traffic when on separate adapters. This supports the use case when both the encrypted and decrypted versions of the same traffic are traversing the same Decoder. The multi-thread assembler feature allows Decoder to assemble packets from its corresponding capture work thread. It keeps the packets from encrypted and decrypted sessions separate during assembly to avoid inaccuracies in session parsing and content extraction.

For more information, see the "Decrypt Incoming Packets" topic in the *Decoder and Log Decoder Configuration Guide*.

Trusted Authentication for Aggregation Hosts

When configuring aggregation connections, you can use trusted authentication to perform this task instead of using service account credentials. The trusted authentication reduces administrator overhead by eliminating the need to manage service account password changes.

Make a note that this authentication method change requires the device to be offline. Also, once you switch to Trusted Authentication, you cannot switch back to the login method using the user credentials.

Event Stream Analysis (ESA)

Support for Meta Entities

Meta Entities provide a way to link similar meta keys together. Once they are defined, an entity can be used the same way as a key, so that analysts can use them as regular keys to get to multiple, similar concepts. From 11.6 release, meta key entities are configured to be a part of the event schema and can enable the string [] meta keys entities. Analysts can create rules and configure alerts based on the meta key entities selected. You can also add meta entities to create rules. The meta entities retrieve data from the data sources to trigger alerts.

- To view the list of meta entities, see Viewing the List of Meta Entities
- To enable meta entities in the ESA Correlation server, see Enabling Meta Entity in the ESA Correlation Server
- To build rules with custom meta entities, see Building Rules with Custom Meta Entities

For more information, see *NetWitness ESA Alerting User guide*.

Import and Edit Position Tracking Information

When you deploy a data source, by default, ESA starts processing information from the latest available session. Position tracking information enables the administrator to visualize the progress of the sessions that ESA has processed and provides information on the session IDs and the time or date when the events were processed.

- The edit function enables you to visualize the number of sessions that a particular ESA data source analyzes after you edit the position tracking, review the number of processed sessions, and plan your work. To edit position tracking information, see Editing Position Tracking Information.
- The import function enables you to migrate the settings of position tracking for one or more data sources at the same time from an existing deployment. To import position tracking information, see Importing Position Tracking Information.
- To review a use case scenario, see Use Case Scenario.

Leverage Trusted Authentication

While working with data sources, you can use trusted authentication to perform tasks, instead of logging in with the admin credentials. You need not log in using your admin credentials, every time you want to access the data sources.

For more information, see Trusted Authentication in the *NetWitness Getting Started Guide*.

Support for Detect AI

Detect AI has been added as an alert source in the Respond view. It captures the alerts from the cloud based user behavior analytics to create incidents from alerts.

You can filter the alerts list to show the alerts of interest using filters such as, alert name, alert source, and specific time range.

For more information, see View a Summary of Alerts

Administration and Configuration

Remove Unwanted Dashboards

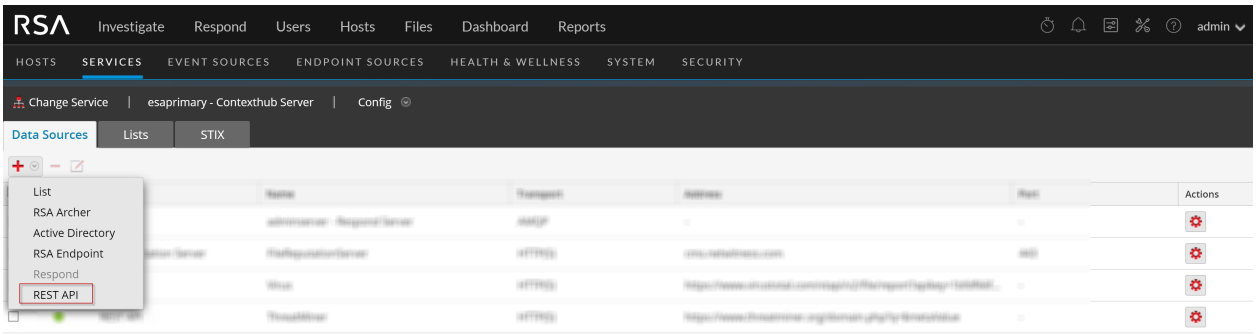
You can remove redundant dashboards (dashboards that are not owned, not shared, and duplicate default dashboards) by enabling the dashboard cleaning job.

For more information, see Removing Unwanted Dashboards

Context Hub

Support for REST API Data Source

NetWitness Platform 11.6 introduces the ability to add any RESTful API data source to Context Hub.



REST API allows analysts to query third-party applications by providing a meta value as a query parameter and rendering results in the Context Hub Panel in real-time. The results can be rendered in JSON or HTML format depending on the preference and capabilities of the third-party application. An analyst can now gain additional context about IPs, users, hosts, or files faster during an investigation without requiring them to leave the NetWitness Platform.

Improvements to Context Highlighting

Some additional configurations are introduced to the Context Highlighting feature to make the capability more usable and efficient in specific environments. Administrators can now configure specific Context Hub sources (For example, specific lists, Respond, Endpoint, and so on) for context highlighting. If the context highlighting is disabled for a Context Hub source, analysts can view results from all sources while opening the Context Panel for a meta value, but the values are not highlighted in the **Investigate** > **Navigate**, **Event**, and **Respond** views. Administrators can also disable the context highlighting globally for all sources.

For more information, see Configure REST API as a Data Source topic in the *Context Hub Configuration Guide*.

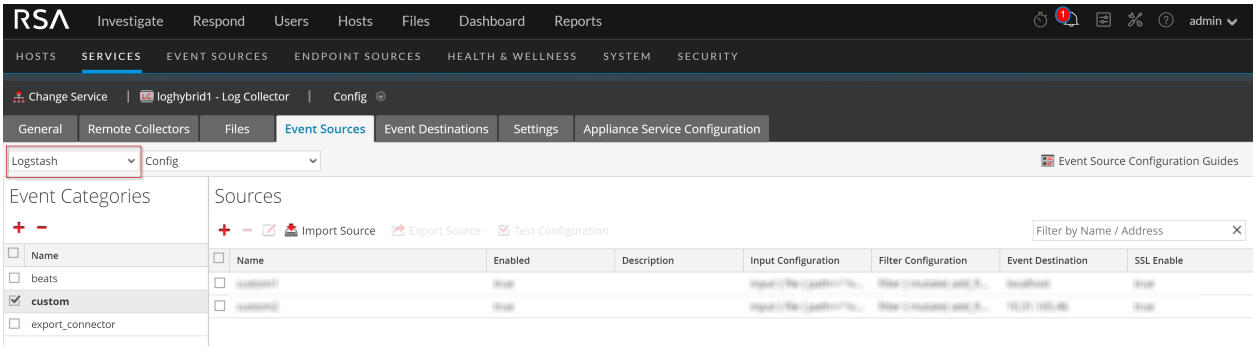
Log Collection

Support for Managed Logstash

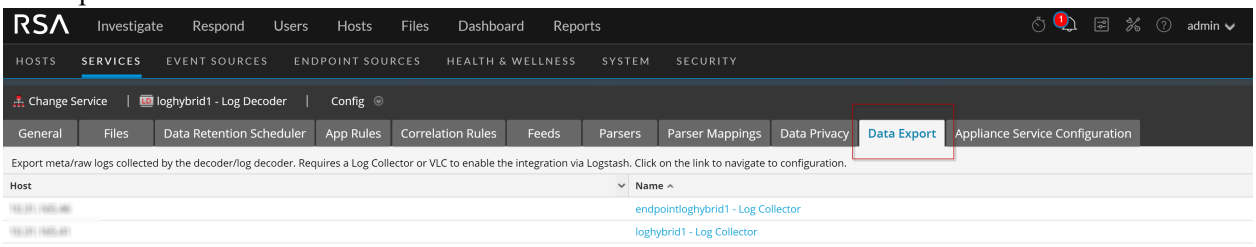
In 11.5, the NetWitness Output Codec for Logstash was introduced, making Logstash integrations possible with a customer-managed Logstash server. From 11.6 onwards, the Logstash server is packaged and supported along with the NetWitness Log Collector or Virtual Log Collector (VLC) service to provide easy access to Logstash. This is referred to as Managed Logstash and it eliminates the need for a separate Logstash server outside of the NetWitness Platform.

You can create Logstash pipelines (for example beats, export connector and so on) in the Event Sources tab within the Log Collector service. The custom category allows for a fully-custom Logstash pipeline configuration.

The following is an example of Logstash Event Source.



A new Data Export tab is added to the Decoder or Log Decoder configuration view. It lists the available Log Collector services in your environment. Once you select a Log Collector service, you can configure the Export Connector in the Event Sources tab.

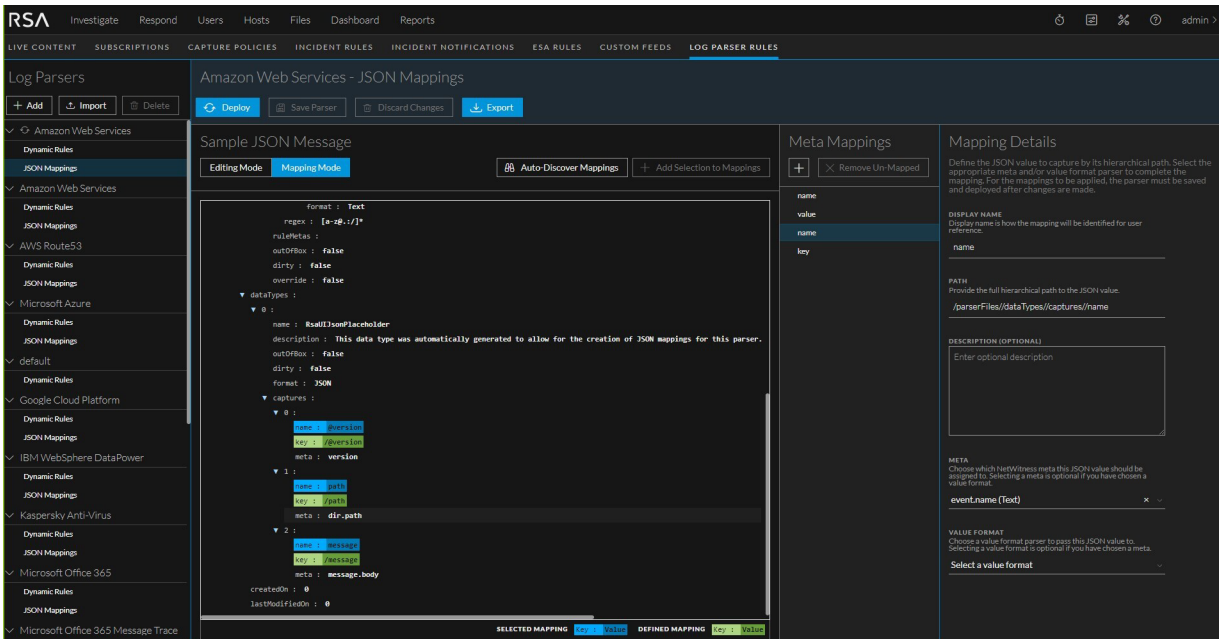


Also, New stats for both legacy and New Health and Wellness are introduced to monitor the health and throughput for each Logstash pipeline. Logstash Input Plugin Overview dashboard is added to showcase the new stats.

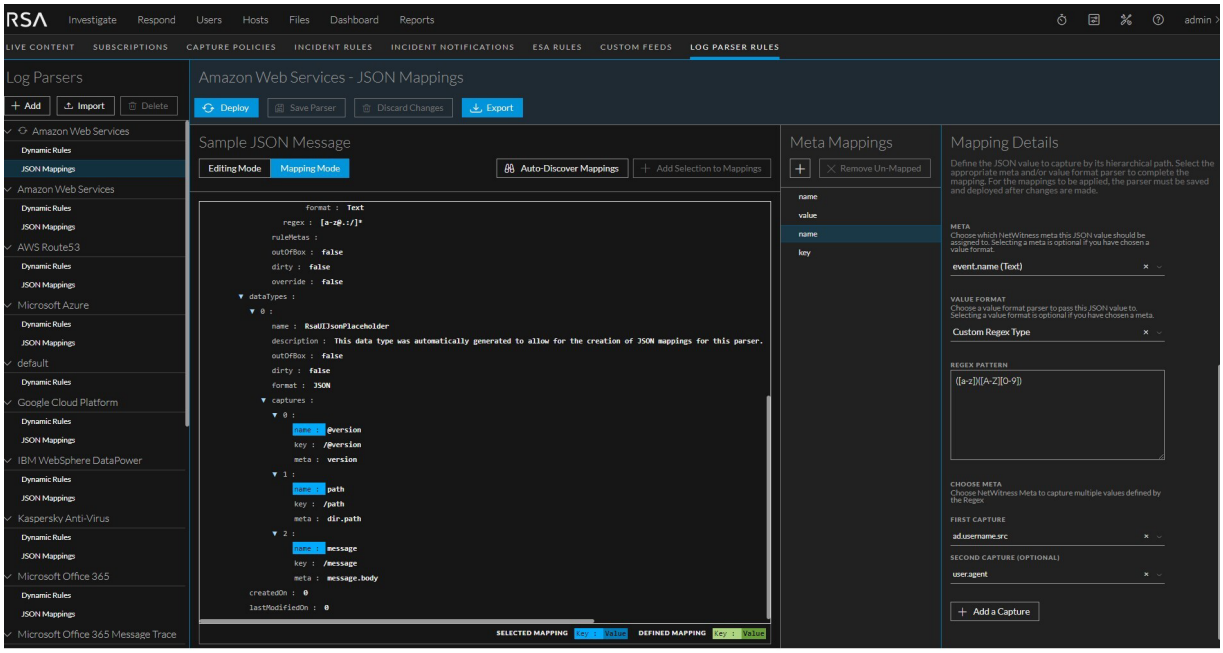
For more information, see Configure Logstash Event Sources in NetWitness Platform in the *Log Collection Configuration Guide*.

Parse Rules UI Improvements

- **JSON Mapping Usability Improvements** - In the tree view of a JSON sample, the corresponding RAW node or Mapping entry is highlighted when either is selected if the match exists. The highlighting indicates whether a match is successful in the current sample; that is, the value should parse correctly, including the node path and any DataType or RegEx.



- **Custom Regex for JSON mappings** - For fine-parsing JSON values (for example, ip:port), the user can create a custom RegEx pattern for each mapping within the UI. Multiple values (captures) can be extracted and assigned to separate meta keys.



- **Import or Export for custom UI Rules (Dynamic Rules or JSON mappings)** - Custom Dynamic Rules and JSON mappings that are created in the UI can now be easily imported or exported right from the UI. This enables customers to develop parse rules in one environment (For example, Lab) and move them to another (For example, Production).

For more information see *Log Parser Customization Guide*.

Note: Import or Export for custom UI rules does not export or import any "parser.XML" or "parser_custom.XML" that correspond to the Parse Rules.

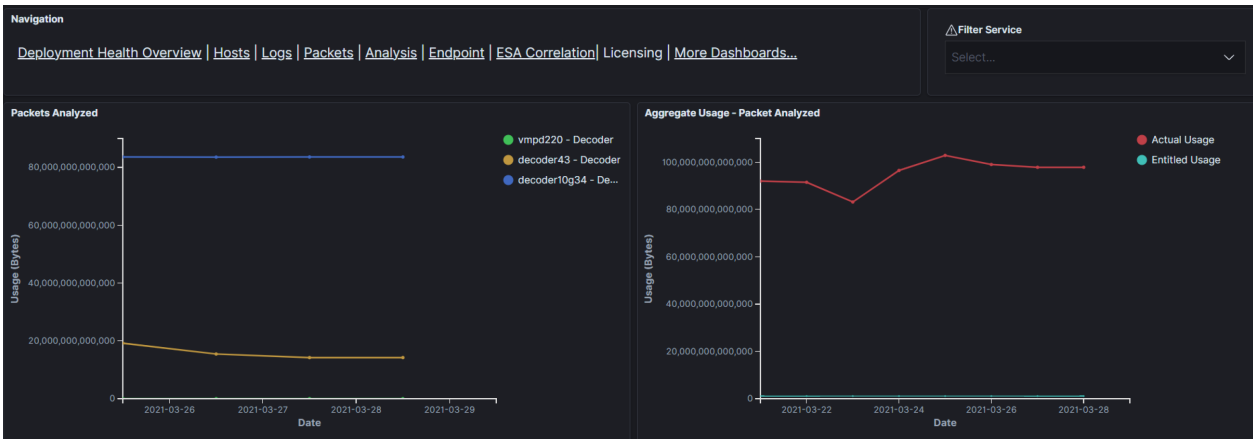
Licensing

Introducing License Usage Dashboard

A new license dashboard is introduced in New Health & Wellness to manage licenses efficiently. This dashboard provides insights on the license usage of all the Throughput licenses in your deployment. Administrators can do the following on this dashboard:

- Track daily license usage for individual hosts
- Track daily usage of Throughput licenses for all the hosts in your deployment
- Download license usage reports

For more information, see License Usage Dashboard in the System Maintenance Guide.



Throughput License Calculation Changes

NetWitness Platform versions 11.5.1 to 11.6, includes fixes to the metrics used in reporting for Network (Packet) Throughput usage. License metrics includes the overall network traffic analyzed and the raw network data stored after the analysis. Your Network Throughput License usage may increase, which may cause license violation banners in some situations. The Out-of-Compliance notifications for Network Throughput licenses has been adjusted to delay the display of the license violation banner by 45-days. For more information, see the *Licensing Management Guide*.

Platform

Support for Third Party Server Hardware

This allows you to use any third party server hardware to run NetWitness Platform. The kickstart wizard provides a list of available block devices, and prompts you to select the device to install the OS and NetWitness Platform application. For more information, see Installation Tasks topic in the *Physical host installation 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.

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 a domain name, if the domain name has letters after (.) symbol. For example, XXX@abc.xyz.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 NetWitness Server show when users add, modify, filter, delete, export, and import ESA rules in the Rule Library. The NetWitness 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	In the Events view, refocusing a value that contains the backslash (\) character 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	When querying meta keys with values with special characters like ® are truncated.
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-80896	Incidents generated by Reporting Engine alerts display cleartext values despite Data Privacy being enabled. Previously, in deployments where data privacy is enabled, incidents generated 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.
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 for count distinct.
SACE-13597	For a TLS session, the meta keys for JA3/JA3s and cert.thumbprint are not 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.
ASOC-77307	Audit Logs do not have enough context when an ESA rule is created, duplicated, or deleted on the Rule Builder.
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.

Reporting Engine Fixes

Tracking Number	Description
SACE-12893	The **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.

Springboard Fixes

Tracking Number	Description
ASOC-106211 / ASOC-106350	Risky Users information will not be displayed in the Top Risky Users panel and custom panels in the Springboard.

Upgrade Fixes

Tracking Number	Description
SACE-12658	The configuration fails when running the nwsetup-tui command on the CLI for static IP address.

Threat Intelligence Fixes

Tracking Number	Description
ASOC-100727	Recurring Custom Feeds are not pushed to core on failover.

End of Life Functionality

The following table provides information on end of life functionality and features in RSA NetWitness Platform 11.6 or later releases.

End of Life Functionality and Features in 11.6.0.0 or later releases

Feature	Notes
Live Connect Data Source	Live Connect Data Source is not supported in NetWitness Platform 11.6 or later releases.

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/t5/rsa-netwitness-platform/ct-p/netwitness-documentation
RSA NetWitness Platform 11.6 Product Documentation	https://community.rsa.com/
RSA NetWitness Platform 11.6 Upgrade Guide	https://community.rsa.com/t5/rsa-netwitness-platform-online/tkb-p/netwitness-online-documentation

Feedback on Product Documentation

You can send an email to nwdocsfeedback@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 11.6.0.0.

Component	Version Number
NetWitness Platform Audit Plugins	rsa-audit-plugins-11.6.0.0-4671.5.25a824322.el7.noarch.rpm
NetWitness Platform Appliance	rsa-nw-appliance-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Archiver	rsa-nw-archiver-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Broker	rsa-nw-broker-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Concentrator	rsa-nw-concentrator-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Config Management	rsa-nw-config-management-11.6.0.0-2104212116.5.d60ffff.el7.noarch.rpm
NetWitness Platform Config Server	rsa-nw-config-server-11.6.0.0-210331045328.5.6fe2c5e.el7.centos.noarch.rpm
NetWitness Platform Console	rsa-nw-console-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Content Server	rsa-nw-content-server-11.6.0.0-210318023955.5.2647b0c.el7.centos.noarch.rpm
NetWitness Platform ContextHub Server	rsa-nw-contexthub-server-11.6.0.0-210331043419.5.3d6abd0.el7.centos.noarch.rpm
NetWitness Platform Correlation Server (ESA)	rsa-nw-correlation-server-11.6.0.0-210415073028.5.3610f9b.el7.centos.noarch.rpm
NetWitness Platform Decoder	rsa-nw-decoder-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Deployment Upgrade	rsa-nw-deployment-upgrade-11.6.0.0-2103151416.5.f557d92.el7.noarch.rpm
NetWitness Platform Endpoint Agents	rsa-nw-endpoint-agents-11.6.0.0-2103311945.5.bd1280b.el7.x86_64.rpm
NetWitness Platform Endpoint Broker Server	rsa-nw-endpoint-broker-server-11.6.0.0-210331080032.5.2bc8f1d.el7.centos.noarch.rpm
NetWitness Platform Endpoint Server	rsa-nw-endpoint-server-11.6.0.0-210406104611.5.4c9695b.el7.centos.noarch.rpm

NetWitness Platform Integration Server	rsa-nw-integration-server-11.6.0.0-210331043939.5.385a853.el7.centos.noarch.rpm
NetWitness Platform Investigate Server	rsa-nw-investigate-server-11.6.0.0-210430143448.5.fb23b39.el7.centos.noarch.rpm
NetWitness Platform Legacy Web Server	rsa-nw-legacy-web-server-11.6.0.0-210504044611.5.9ec73de.el7.centos.noarch.rpm
NetWitness Platform License Server	rsa-nw-license-server-11.6.0.0-210503080758.5.619d23a.el7.centos.noarch.rpm
NetWitness Platform Log Decoder	rsa-nw-logdecoder-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Log Player	rsa-nw-logplayer-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform Malware Analytics Server	rsa-nw-malware-analytics-server-11.6.0.0-210325105147.5.293bed9.el7.centos.x86_64.rpm
NetWitness Platform Metrics Server	rsa-nw-metrics-server-11.6.0.0-210421095948.5.37b59af.el7.centos.noarch.rpm
NetWitness Platform Orchestration Server	rsa-nw-orchestration-server-11.6.0.0-210316174042.5.c0a599c.el7.centos.noarch.rpm
NetWitness Platform Reporting Engine Server	rsa-nw-re-server-11.6.0.0-5893.5.6eab5cd2a.el7.x86_64.rpm
NetWitness Platform Respond Server	rsa-nw-respond-server-11.6.0.0-210428102736.5.64efcea.el7.centos.noarch.rpm
NetWitness Platform Root CA Update	rsa-nw-root-ca-update-11.6.0.0-2011031833.5.745f08a.el7.noarch.rpm
NetWitness Platform SDK	rsa-nw-sdk-11.6.0.0-11374.5.fe9457e29.el7.x86_64.rpm
NetWitness Platform Security Server	rsa-nw-security-server-11.6.0.0-210330025250.5.ab7b8b1.el7.centos.noarch.rpm
NetWitness Platform Source Server	rsa-nw-source-server-11.6.0.0-210414045818.5.348fe73.el7.centos.noarch.rpm
NetWitness Platform User Interface	rsa-nw-ui-11.6.0.0-210503011255.5.5f8590a66a.el7.centos.noarch.rpm
NetWitness Platform Workbench	rsa-nw-workbench-11.6.0.0-12002.5.7a8a57058.el7.x86_64.rpm
NetWitness Platform SA Tools	rsa-sa-tools-11.6.0.0-2102240502.5.fea248a.el7.noarch.rpm
NetWitness Platform SMS Runtime	rsa-sms-runtime-rt-11.6.0.0-4671.5.25a824322.el7.x86_64.rpm
NetWitness Platform SMS Server	rsa-sms-server-11.6.0.0-4671.5.25a824322.el7.x86_64.rpm

Revision History

Date	Description
June 2021	Release to Operations