Release Notes

for RSA NetWitness® Platform 11.5.1

Contact Information

RSA Link at https://community.rsa.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

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.

December 2020

Contents

What's New

The RSA NetWitness® Platform 11.5.1 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 11.5.1.0:

- RSA NetWitness® Platform 11.3.x.x to 11.5.1.0*
- RSA NetWitness® Platform 11.4.x.x to 11.5.1.0
- RSA NetWitness® Platform 11.5.0.0 to 11.5.1.0
- RSA NetWitness® Platform 11.5.0.1 to 11.5.1.0

* If you are upgrading from 11.3.0.0, or 11.3.0.1, you must upgrade to 11.3.1.1 before you can upgrade to 11.5.1.0.

If you are upgrading from NetWitness Platform version (10.6.6.x) or (11.2.x.x or below), you must upgrade to 11.3.0.2 before you can upgrade to 11.5.1.0. For more information, see the guides that apply to your environment.

For more information on upgrading to 11.5.1.0, see Upgrade Guide for RSA NetWitness Platform 11.5.1.

Enhancements

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

- Investigation - SIEM and Network Detection & Response
- Endpoint Investigation
- User Entity Behavior Analytics
- Incident Response
- Endpoint Configuration
- Broker, Concentrator, Decoder and Log Decoder Services
- Administration and Configuration
- Log Collection
- Logstash Integration
- 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.

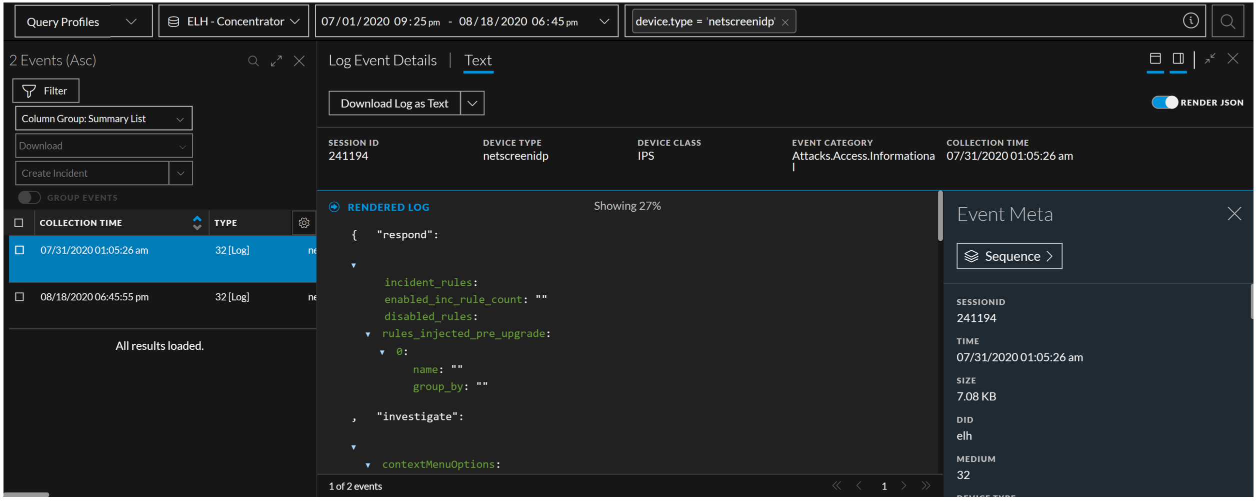
Investigation - SIEM and Network Detection & Response

JSON Viewer for Logs

The JSON log data in the Events page renders in an easy-to-read JSON format instead of the raw block format using the Render JSON toggle switch. It allows analysts to identify nodes, node values, and position of the node in the tree. By default, the switch is enabled, and JSON snippets in a log event are detected and displayed in an expanded tree format. The system supports rendering of logs with a mix of text and JSON to display in both Respond and Investigate views.

For more information, see the "View a JSON String in Tree Format in the Text Tab" topic in the NetWitness Investigate User Guide.

Below is an example of the Render JSON switch enabled.



07/01/2020 09:25 pm - 08/18/2020 06:45 pm

device.type = 'netscreenidp'

□	COLLECTION TIME	TYPE
□	07/31/2020 01:05:26 am	32 [Log]
□	08/18/2020 06:45:55 pm	32 [Log]

All results loaded.

SESSION ID	DEVICE TYPE	DEVICE CLASS	EVENT CATEGORY	COLLECTION TIME
241194	netscreenidp	IPS	Attacks.Access.Informational	07/31/2020 01:05:26 am

Showing 27%

```
{   "respond":

▾
      incident_rules:
      enabled_inc_rule_count: ""
      disabled_rules:
    ▾ rules_injected_pre_upgrade:
      ▾ 0:
          name: ""
          group_by: ""

,   "investigate":

▾
    ▾ contextMenuOptions:
```

SESSIONID
241194

TIME
07/31/2020 01:05:26 am

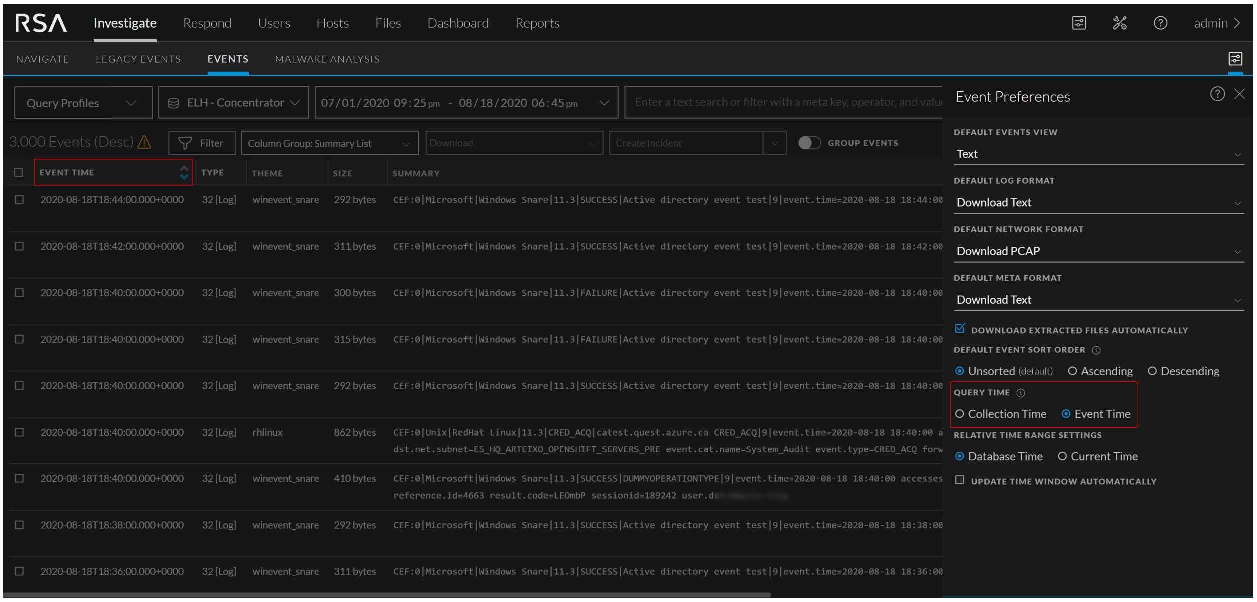
SIZE
7.08 KB

DID
elh

MEDIUM
32

Investigation Using the Event Time

Analysts can directly query and sort events using event time (the time the event occurred) instead of collection time (the time the Decoder received the event). This eliminates the need to find the log or the Endpoint events relevant to the actual time range, thus, saving time and effort of the analyst as the events are displayed as they happen. For more information, see the NetWitness Investigate User Guide.



07/01/2020 09:25 pm - 08/18/2020 06:45 pm

3,000 Events (Desc)

Column Group: Summary List

☐	EVENT TIME	TYPE	THEME	SIZE	SUMMARY
☐	2020-08-18T18:44:00.000+0000	32 [Log]	winevent_snare	292 bytes	CEF:0|Microsoft|Windows Snare|11.3|SUCCESS|Active directory event test|9|event.time=2020-08-18 18:44:00
☐	2020-08-18T18:42:00.000+0000	32 [Log]	winevent_snare	311 bytes	CEF:0|Microsoft|Windows Snare|11.3|SUCCESS|Active directory event test|9|event.time=2020-08-18 18:42:00
☐	2020-08-18T18:40:00.000+0000	32 [Log]	winevent_snare	300 bytes	CEF:0|Microsoft|Windows Snare|11.3|FAILURE|Active directory event test|9|event.time=2020-08-18 18:40:00
☐	2020-08-18T18:40:00.000+0000	32 [Log]	winevent_snare	315 bytes	CEF:0|Microsoft|Windows Snare|11.3|FAILURE|Active directory event test|9|event.time=2020-08-18 18:40:00
☐	2020-08-18T18:40:00.000+0000	32 [Log]	winevent_snare	292 bytes	CEF:0|Microsoft|Windows Snare|11.3|SUCCESS|Active directory event test|9|event.time=2020-08-18 18:40:00
☐	2020-08-18T18:40:00.000+0000	32 [Log]	rhlinux	862 bytes	CEF:0|Unix|RedHat Linux|11.3|CRED_ACQ|catest.quest.azure.ca CRED_ACQ|9|event.time=2020-08-18 18:40:00 a dst.net.subnet=ES_HQ_ARTEIXO_OPENSHIFT_SERVERS_PRE event.cat.name=System_Audit event.type=CRED_ACQ forw
☐	2020-08-18T18:40:00.000+0000	32 [Log]	winevent_snare	410 bytes	CEF:0|Microsoft|Windows Snare|11.3|SUCCESS|DUMMYOPERATIONTYPE|9|event.time=2020-08-18 18:40:00 accesses reference.id=4663 result.code=LEOmbP sessionid=189242 user.d[redacted]
☐	2020-08-18T18:38:00.000+0000	32 [Log]	winevent_snare	292 bytes	CEF:0|Microsoft|Windows Snare|11.3|SUCCESS|Active directory event test|9|event.time=2020-08-18 18:38:00
☐	2020-08-18T18:36:00.000+0000	32 [Log]	winevent_snare	311 bytes	CEF:0|Microsoft|Windows Snare|11.3|SUCCESS|Active directory event test|9|event.time=2020-08-18 18:36:00

Event Preferences

DEFAULT EVENTS VIEW
Text

DEFAULT LOG FORMAT
Download Text

DEFAULT NETWORK FORMAT
Download PCAP

DEFAULT META FORMAT
Download Text

☑ DOWNLOAD EXTRACTED FILES AUTOMATICALLY

DEFAULT EVENT SORT ORDER
● Unsorted (default) ○ Ascending ○ Descending

QUERY TIME
○ Collection Time ● Event Time

RELATIVE TIME RANGE SETTINGS
● Database Time ○ Current Time

☐ UPDATE TIME WINDOW AUTOMATICALLY

Manual Column Width Adjustments Automatically Apply

When analysts manually adjust the width of a column in the Events panel, the column width is preserved as a personal preference and is applied every time the column is used in the Events list, overriding any default column width. For more information, see the NetWitness Investigate User Guide.

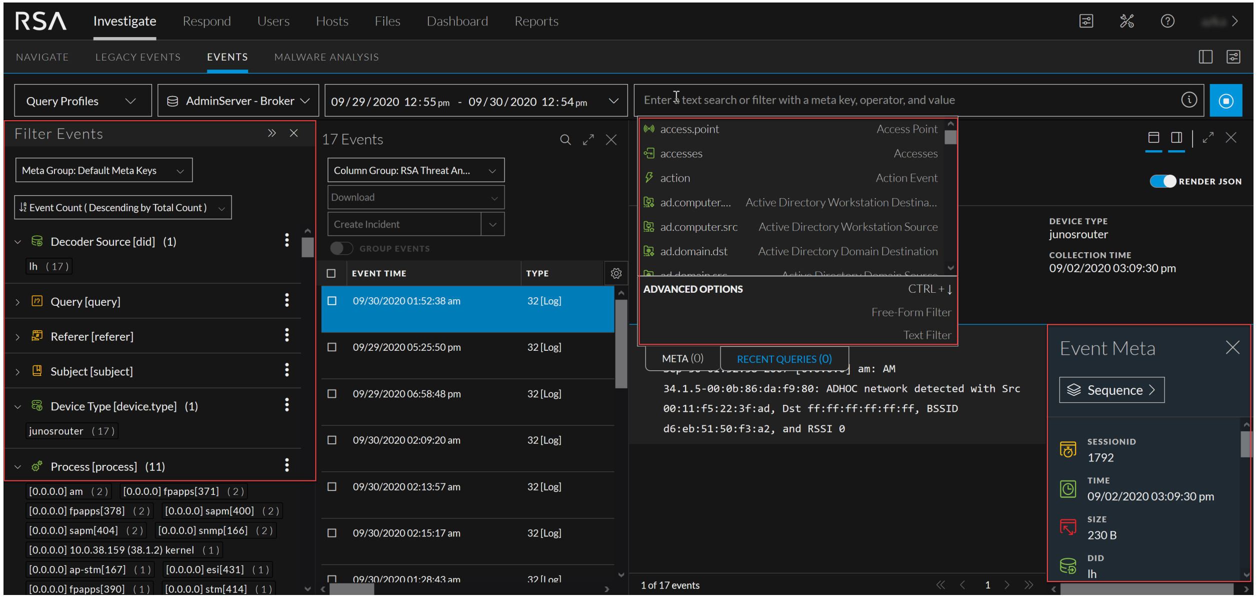
Option to Add Multiple Filters Prior to Query

An analyst can build a query with multiple filters pivoting through the meta available in the Events Filter panel. For more information, see “Drill into Meta Values” in the *NetWitness Investigate User Guide*.

New Icons for Meta Keys

The Events page includes new unique icons for every meta key displayed in the Events query bar, Filter Events panel, and Event Meta reconstruction panel to help analysts recognize items while visually scanning the data available on the page. The icons use color to indicate meta key search capability and are categorized based on the family of metadata. For more information, see the NetWitness Investigate User Guide.

Below is an example of the new icons.



```
am: AM
34.1.5-00:0b:86:da:f9:80: ADHOC network detected with Src
00:11:f5:22:3f:ad, Dst ff:ff:ff:ff:ff:ff, BSSID
d6:eb:51:50:f3:a2, and RSSI 0
```

Springboard Panel Enhancements

- The panel rendering time is improved and the memory usage is reduced. For example, when the administrator adds or scroll across the panel, only the displayed panels are loaded and not the hidden panels.
- Includes User's Trending Data (24 hours) and Trending Data (7 days) options in the UEBA panels.
- Clicking on a Springboard panel row name or clicking > at the top of the panel, takes you to a new tab for quick hunting and investigation.
- Includes drop-down filter options for menus such as Data Source and Meta key.

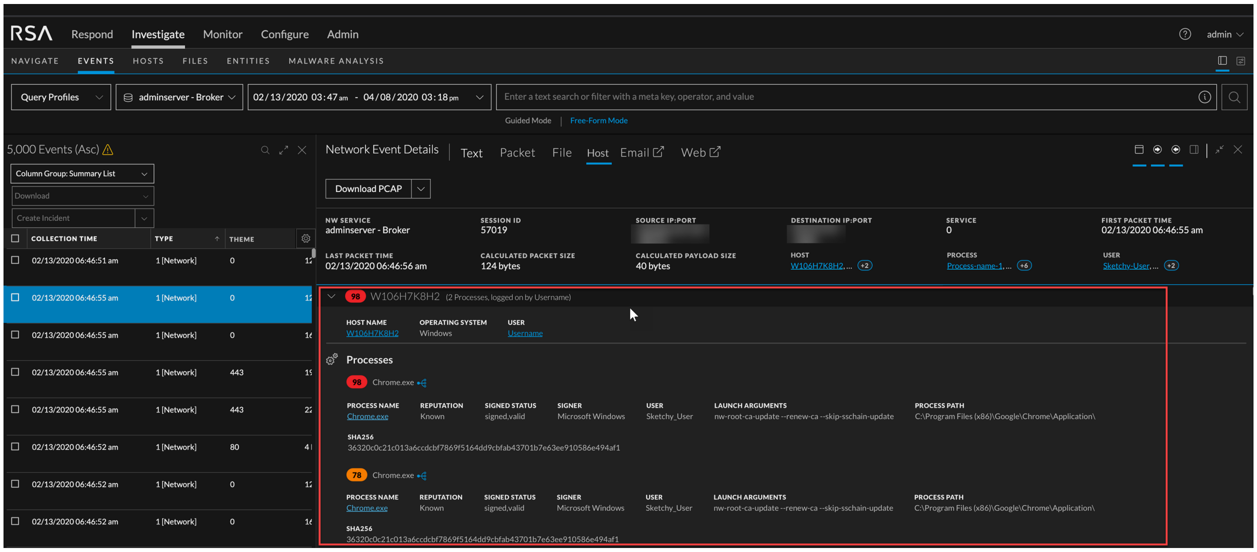
  For more information, see the "Managing the Springboard" topic in the *NetWitness Platform Getting Started Guide*.

Expanded Network Visibility with Endpoint Data Enrichment

Network events are further enriched with additional host information. It includes alerts and process details associated with the enriched host values. This additional data enables an analyst to investigate an event more efficiently.

Example 1

An analyst can use the Process Tree option to see the origin of a process and associated process information.



02/13/2020 03:47 am - 04/08/2020 03:18 pm

5,000 Events (Asc)

☐	COLLECTION TIME	TYPE	THEME	
☐	02/13/2020 06:46:51 am	1 [Network]	0	12
☐	02/13/2020 06:46:55 am	1 [Network]	0	12
☐	02/13/2020 06:46:55 am	1 [Network]	0	16
☐	02/13/2020 06:46:55 am	1 [Network]	443	19
☐	02/13/2020 06:46:55 am	1 [Network]	443	22
☐	02/13/2020 06:46:52 am	1 [Network]	80	4
☐	02/13/2020 06:46:52 am	1 [Network]	0	12
☐	02/13/2020 06:46:52 am	1 [Network]	0	16

NW SERVICE adminserver - Broker
SESSION ID 57019
SOURCE IP:PORT [redacted]
DESTINATION IP:PORT [redacted]
SERVICE 0
FIRST PACKET TIME 02/13/2020 06:46:55 am
LAST PACKET TIME 02/13/2020 06:46:56 am
CALCULATED PACKET SIZE 124 bytes
CALCULATED PAYLOAD SIZE 40 bytes
HOST W106H7K8H2, ... +2
PROCESS Process-name-1, ... +6
USER Sketchy-User, ... +2

98 W106H7K8H2 (2 Processes, logged on by Username)

HOST NAME W106H7K8H2
OPERATING SYSTEM Windows
USER Username

98 Chrome.exe

PROCESS NAME	REPUTATION	SIGNED STATUS	SIGNER	USER	LAUNCH ARGUMENTS	PROCESS PATH
Chrome.exe	Known	signed,valid	Microsoft Windows	Sketchy_User	nw-root-ca-update --renew-ca --skip-sschain-update	C:\Program Files (x86)\Google\Chrome\Application\

SHA256
36320c0c21c013a6ccdcbf7869f5164dd9cbfab43701b7e63ee910586e494af1

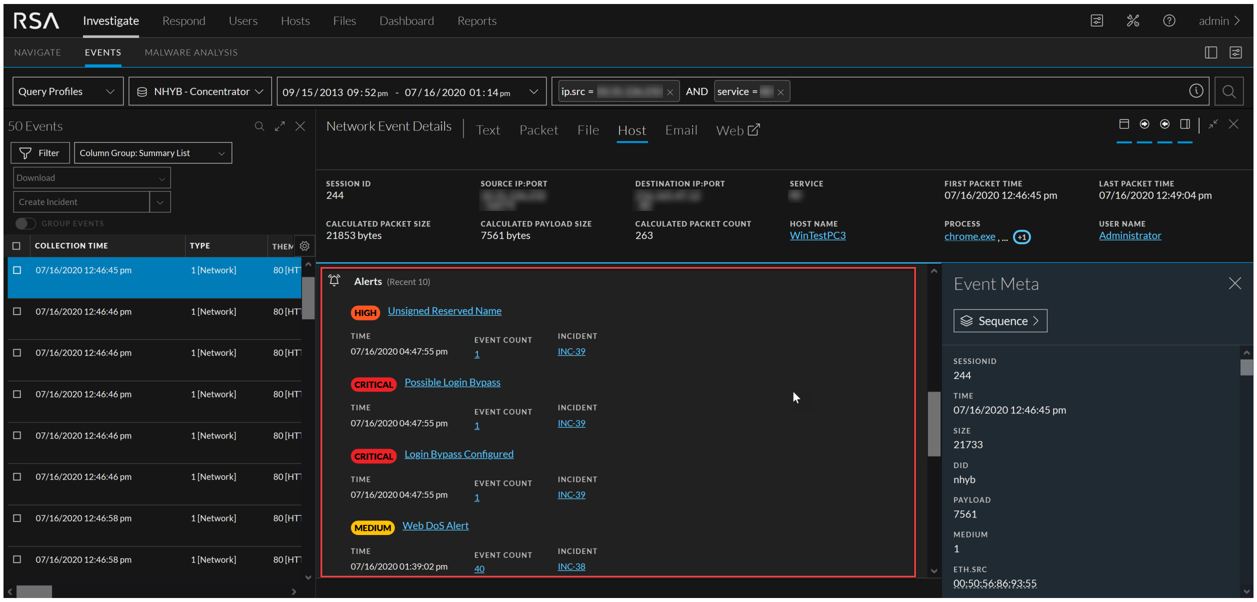
78 Chrome.exe

PROCESS NAME	REPUTATION	SIGNED STATUS	SIGNER	USER	LAUNCH ARGUMENTS	PROCESS PATH
Chrome.exe	Known	signed,valid	Microsoft Windows	Sketchy_User	nw-root-ca-update --renew-ca --skip-sschain-update	C:\Program Files (x86)\Google\Chrome\Application\

SHA256
36320c0c21c013a6ccdcbf7869f5164dd9cbfab43701b7e63ee910586e494af1

Example 2

An analyst can see the Alerts section to see the alerts triggered on a host. This section provides information on alerts, incidents, and events count associated with the host.



09/15/2013 09:52 pm - 07/16/2020 01:14 pm

ip.src = [redacted] AND service = [redacted]

50 Events

☐	COLLECTION TIME	TYPE	THEM
☐	07/16/2020 12:46:45 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:46 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:46 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:46 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:46 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:46 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:58 pm	1 [Network]	80 [HT
☐	07/16/2020 12:46:58 pm	1 [Network]	80 [HT

SESSION ID 244
SOURCE IP:PORT [redacted]
DESTINATION IP:PORT [redacted]
SERVICE [redacted]
FIRST PACKET TIME 07/16/2020 12:46:45 pm
LAST PACKET TIME 07/16/2020 12:49:04 pm
CALCULATED PACKET SIZE 21853 bytes
CALCULATED PAYLOAD SIZE 7561 bytes
CALCULATED PACKET COUNT 263
HOST NAME WinTestPC3
PROCESS chrome.exe , ... +1
USER NAME Administrator

Alerts (Recent 10)

HIGH Unsigned Reserved Name
TIME 07/16/2020 04:47:55 pm
EVENT COUNT 1
INCIDENT INC-39

CRITICAL Possible Login Bypass
TIME 07/16/2020 04:47:55 pm
EVENT COUNT 1
INCIDENT INC-39

CRITICAL Login Bypass Configured
TIME 07/16/2020 04:47:55 pm
EVENT COUNT 1
INCIDENT INC-39

MEDIUM Web DoS Alert
TIME 07/16/2020 01:39:02 pm
EVENT COUNT 40
INCIDENT INC-38

SESSIONID 244
TIME 07/16/2020 12:46:45 pm
SIZE 21733
DID nhyb
PAYLOAD 7561
MEDIUM 1
ETH.SRC 00:50:56:86:93:55

For more information, see "Examine Event Details in the Events View" in the *NetWitness Investigate User Guide*.

> **Note:** Expanded Network Visibility is a policy setting that enables Insights and Advanced agents to monitor the network events. It can optimize the frequency of sending endpoint events for network (packet) correlation. For more information on how to enable the Expanded Network Visibility policy, see Creating Groups and Policies in the NetWitness Endpoint Configuration Guide.

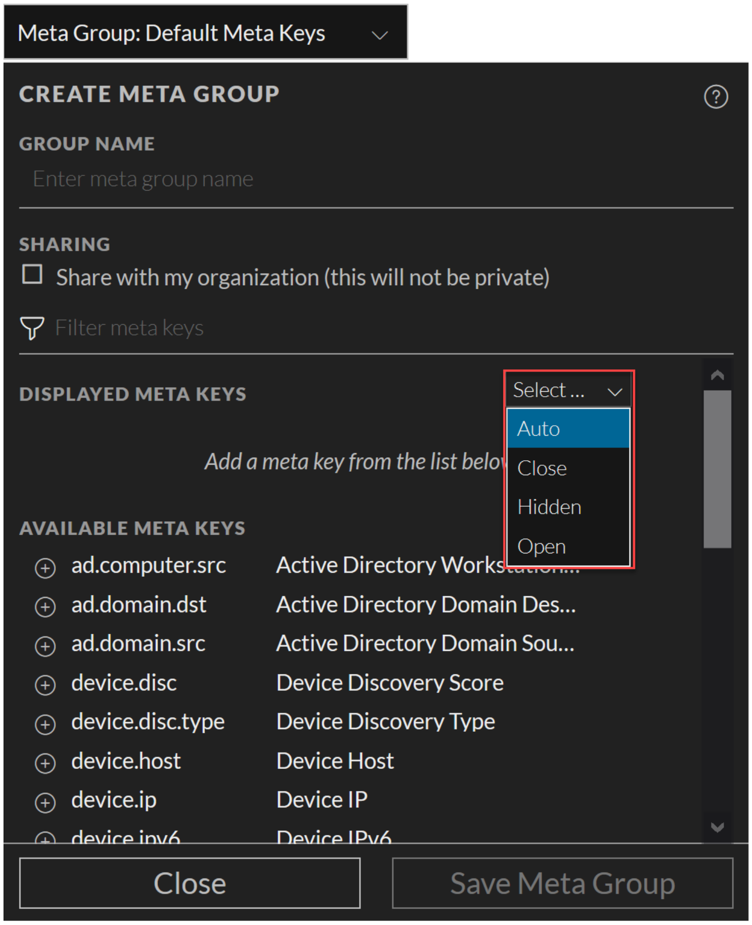
Improved Meta Group Usage while Filtering Events

Analysts can efficiently use meta groups to control the options available in the Filter Events panel. It includes the following enhancements:

- The last meta group is used instead of resetting to the default meta key group.
- Ability to change the default view (AUTO, OPEN, CLOSE, or HIDDEN) for all the meta keys at once.
- The default meta group displays the list of meta keys and can be cloned.

For more information, see the NetWitness Investigate User Guide.

Below is an example showing the option to change the default view for all meta keys.



⊕ ad.computer.src	Active Directory Works...
⊕ ad.domain.dst	Active Directory Domain Des...
⊕ ad.domain.src	Active Directory Domain Sou...
⊕ device.disc	Device Discovery Score
⊕ device.disc.type	Device Discovery Type
⊕ device.host	Device Host
⊕ device.ip	Device IP
⊕ device.ipv6	Device IPv6

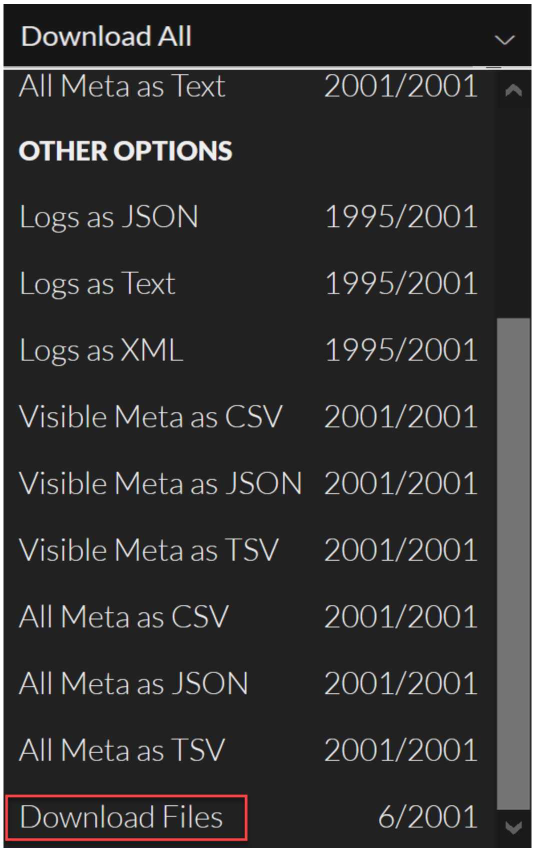
Performance Improvements while Filtering Events

To decrease the time taken to load the panel, estimations for the events count (>) and size (~) are enabled by default. Analysts can also view the debug information that provides the time it takes for the services to present the meta key values. It helps analysts to identify the services that might be causing the latency. For more information, see the NetWitness Investigate User Guide.

Option to Download Files from Multiple Events

In the Events view, analysts can securely download bulk files for multiple events versus per individual event. The downloaded files are present in a password protected zip file to limit exposure to potentially malicious files. For more information, see the NetWitness Investigate User Guide.

Below is an example showing the new **Download Files** option.


Download All
All Meta as Text 2001/2001
OTHER OPTIONS
Logs as JSON 1995/2001
Logs as Text 1995/2001
Logs as XML 1995/2001
Visible Meta as CSV 2001/2001
Visible Meta as JSON 2001/2001
Visible Meta as TSV 2001/2001
All Meta as CSV 2001/2001
All Meta as JSON 2001/2001
All Meta as TSV 2001/2001
Download Files 6/2001

Enhanced Events Query Experience

Analysts can resume a canceled query, to load more meta keys in the Events Filter panel. When the Filter Events panel is being loaded, new messages indicate which meta keys are going to load next. It will also indicate if the query is canceled. For more information, see the NetWitness Investigate User Guide.

User Experience Improvements while Filtering Events

During review of meta key values, analysts can see the unit of measure when the values are sorted based on the event size. If analysts want to shift focus to one specific meta key, they can change their view so all other meta keys in the meta group are closed. For more information, see the NetWitness Investigate User Guide.

Endpoint Investigation

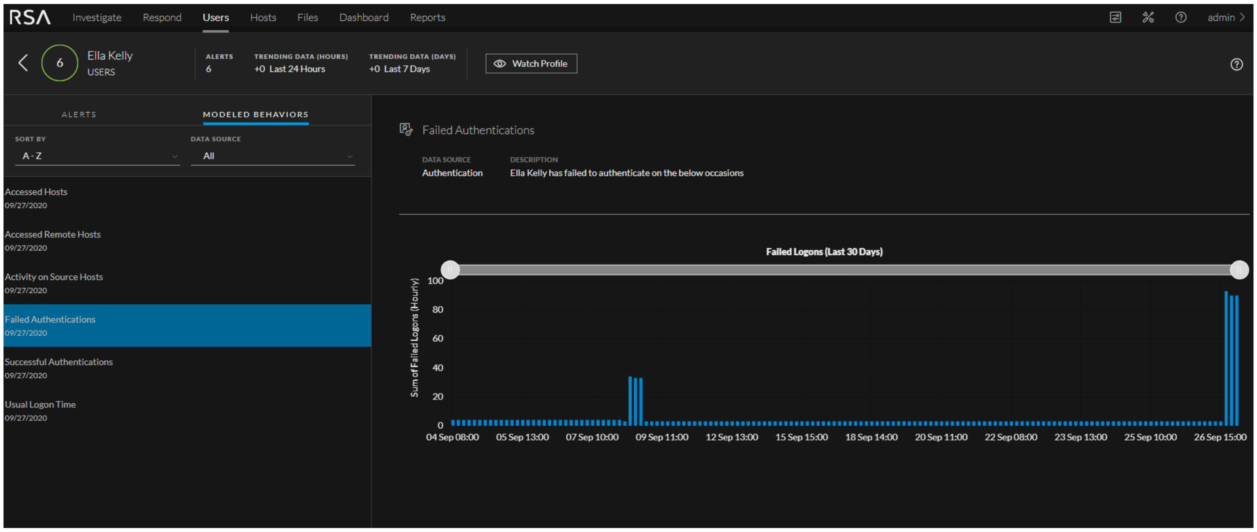
Extended Linux Agent Support with SUSE

Introduced agent support for SUSE Linux Enterprise Server 12 SP5 and later. This enables RSA NetWitness to detect threats on resources running on SUSE Linux Enterprise Server. For more information, see the *NetWitness Endpoint Agent Installation Guide*.

User Entity Behavior Analytics

User Profile Baselines

Modeled Behaviors for users provides analysts with insights on the usual daily activities of users monitored by UEBA. UEBA monitors abnormal user behaviors to identify risky users and this requires data to be processed over a certain period of time during which the usual behavior is captured. Unlike alerts for users, Modeled Behaviors reflect the activities of the user within a day of the service configuration. For example, if a user fails multiple times by logging in with incorrect credentials within an hour, analysts can view these behaviors as Failed Authentications for the user, even if an anomaly was not triggered. This allows Analysts to explore user behaviors, even if they don't rise to a critical level. For more information, refer to “View Modeled Behaviors” in the NetWitness UEBA User Guide.



6 Ella Kelly
USERS

ALERTS 6
TRENDING DATA (HOURS) +0 Last 24 Hours
TRENDING DATA (DAYS) +0 Last 7 Days

SORT BY A - Z
DATA SOURCE All

Accessed Hosts
09/27/2020

Accessed Remote Hosts
09/27/2020

Activity on Source Hosts
09/27/2020

Failed Authentications
09/27/2020

Successful Authentications
09/27/2020

Usual Logon Time
09/27/2020

Failed Authentications

DATA SOURCE Authentication
DESCRIPTION Ella Kelly has failed to authenticate on the below occasions

Incident Response

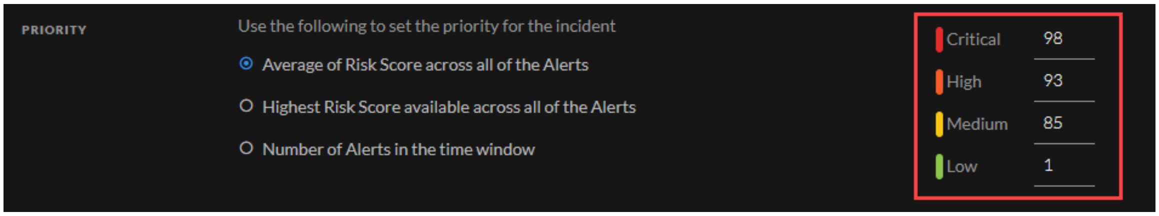
Improved the User Entity Behavior Analytics Incident Rule

The User Entity Behavior Analytics incident rule captures user entity behavior grouped by both UEBA Classifier ID and UEBA Entity Name. The incident name automatically created by the rule contains the a user-friendly UEBA Entity Name instead of UEBA Classifier ID.

In addition, the User Entity Behavior Analytics incident rule default priority threshold ranges are consistent with the severity ranges in NetWitness UEBA.

Priority Threshold	Default Value
Critical	98
High	93
Medium	85
Low	1

For example, with the Critical priority set to 98, incidents with a risk score of 98 or higher are assigned a Critical priority for this rule.



PRIORITY

Use the following to set the priority for the incident

● Average of Risk Score across all of the Alerts

○ Highest Risk Score available across all of the Alerts

○ Number of Alerts in the time window

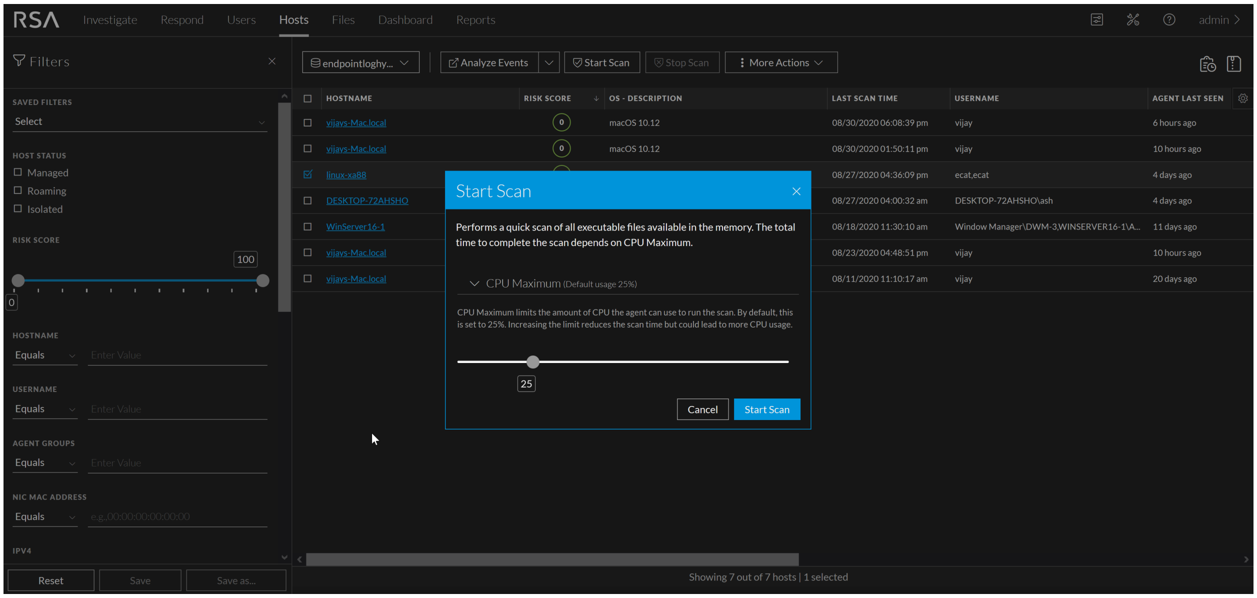
Critical	98
High	93
Medium	85
Low	1

For more information, see "Update the User Entity Behavior Analytics Incident Rule Priority Thresholds, Grouping Options, and Title" in Set Up and Verify Default Incident Rules.

Endpoint Configuration

Added Option to Select CPU Utilization for Manual Scans

On-demand host scans provide analysts the flexibility of choosing the CPU utilization. Analysts can use the CPU Maximum slider to select the CPU percentage so that the agent can limit the usage within the specified range. The Endpoint agents use the selected CPU percentage to get the latest snapshot. It ensures a quick snapshot creation and optimal CPU performance. For more information, see "Scan Hosts" in the NetWitness Endpoint User Guide.



SAVED FILTERS: Select

HOST STATUS

☐ Managed
☐ Roaming
☐ Isolated

RISK SCORE: 0 – 100

HOSTNAME: Equals Enter Value

USERNAME: Equals Enter Value

AGENT GROUPS: Equals Enter Value

NIC MAC ADDRESS: Equals e.g.,00:00:00:00:00:00

IPV4

Reset | Save | Save as...

☐	HOSTNAME	RISK SCORE	OS - DESCRIPTION	LAST SCAN TIME	USERNAME	AGENT LAST SEEN
☐	vijays-Mac.local	0	macOS 10.12	08/30/2020 06:08:39 pm	vijay	6 hours ago
☐	vijays-Mac.local	0	macOS 10.12	08/30/2020 01:50:11 pm	vijay	10 hours ago
☑	linux-xa88			08/27/2020 04:36:09 pm	ecat,ecat	4 days ago
☐	DESKTOP-72AHSHO			08/27/2020 04:00:32 am	DESKTOP-72AHSHO\ash	4 days ago
☐	WinServer16-1			08/18/2020 11:30:10 am	Window Manager\DWM-3,WINSERVER16-1\A...	11 days ago
☐	vijays-Mac.local			08/23/2020 04:48:51 pm	vijay	10 hours ago
☐	vijays-Mac.local			08/11/2020 11:10:17 am	vijay	20 days ago

Showing 7 out of 7 hosts | 1 selected

Start Scan

Performs a quick scan of all executable files available in the memory. The total time to complete the scan depends on CPU Maximum.

CPU Maximum (Default usage 25%)

CPU Maximum limits the amount of CPU the agent can use to run the scan. By default, this is set to 25%. Increasing the limit reduces the scan time but could lead to more CPU usage.

25

Cancel | Start Scan

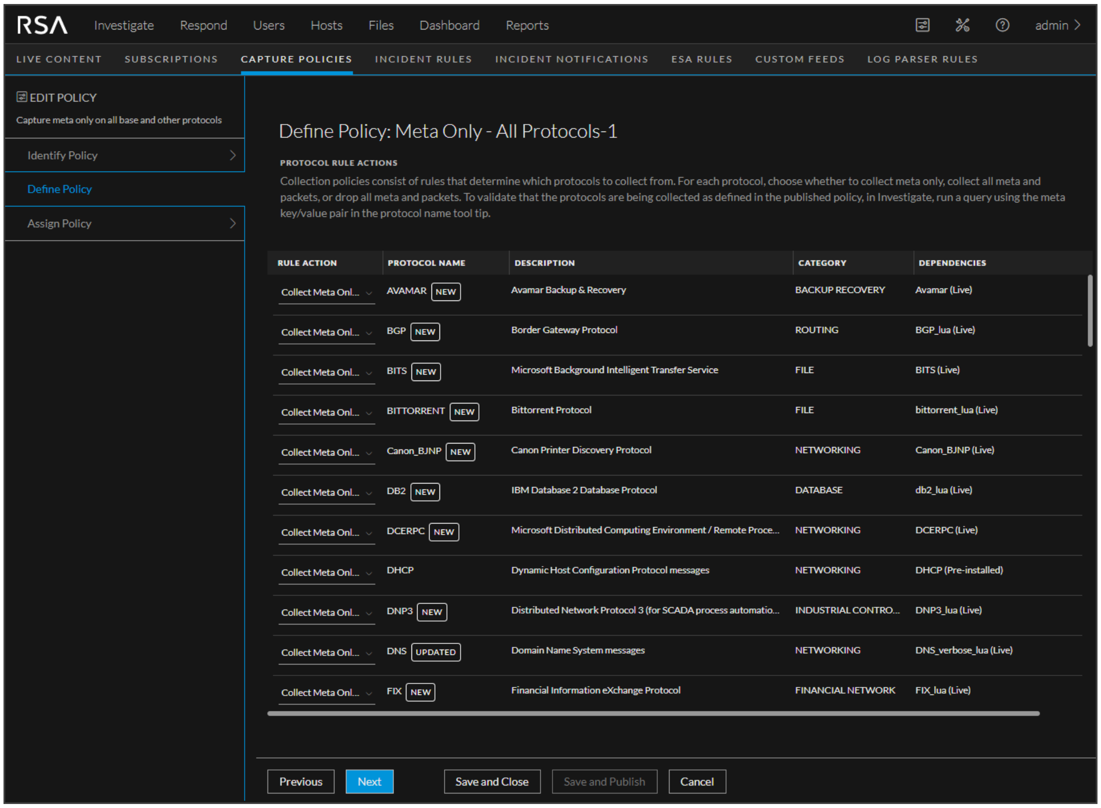
Broker, Concentrator, Decoder and Log Decoder Services

Expanded Selective Network Data Collection

Administrators can choose to collect from 41 new protocols available in the collection policies. A new detail panel displays a preview of the policy with the following information:

- Decoders that received the policy
- Protocol rules in the policy
- Last policy update (time and user)

For more information, see "Supported Protocols for Selective Network Data Collection" topic in *Decoder Configuration Guide for RSA NetWitness Platform*.



Capture meta only on all base and other protocols

Define Policy: Meta Only - All Protocols-1

PROTOCOL RULE ACTIONS

Collection policies consist of rules that determine which protocols to collect from. For each protocol, choose whether to collect meta only, collect all meta and packets, or drop all meta and packets. To validate that the protocols are being collected as defined in the published policy, in Investigate, run a query using the meta key/value pair in the protocol name tool tip.

RULE ACTION	PROTOCOL NAME	DESCRIPTION	CATEGORY	DEPENDENCIES
Collect Meta Onl...	AVAMAR NEW	Avamar Backup & Recovery	BACKUP RECOVERY	Avamar (Live)
Collect Meta Onl...	BGP NEW	Border Gateway Protocol	ROUTING	BGP_lua (Live)
Collect Meta Onl...	BITS NEW	Microsoft Background Intelligent Transfer Service	FILE	BITS (Live)
Collect Meta Onl...	BITTORRENT NEW	Bittorrent Protocol	FILE	bittorrent_lua (Live)
Collect Meta Onl...	Canon_BJNP NEW	Canon Printer Discovery Protocol	NETWORKING	Canon_BJNP (Live)
Collect Meta Onl...	DB2 NEW	IBM Database 2 Database Protocol	DATABASE	db2_lua (Live)
Collect Meta Onl...	DCERPC NEW	Microsoft Distributed Computing Environment / Remote Proce...	NETWORKING	DCERPC (Live)
Collect Meta Onl...	DHCP	Dynamic Host Configuration Protocol messages	NETWORKING	DHCP (Pre-installed)
Collect Meta Onl...	DNP3 NEW	Distributed Network Protocol 3 (for SCADA process automatio...	INDUSTRIAL CONTRO...	DNP3_lua (Live)
Collect Meta Onl...	DNS UPDATED	Domain Name System messages	NETWORKING	DNS_verbose_lua (Live)
Collect Meta Onl...	FIX NEW	Financial Information eXchange Protocol	FINANCIAL NETWORK	FIX_lua (Live)

Improved search experience with N-gram free-text search

The N-gram functionality is enabled by default to improve the free-text search experience. It allows analysts to search sub-strings of text providing more accurate results with a minimal index size increase compared to previous N-gram implementations. By default, this only applies to unparsed logs that are processed by the log tokenizer on the Log Decoder to generate word metadata.

For more information, see "ngrams" in the *Core Database Tuning Guide for RSA NetWitness Platform*.

Administration and Configuration

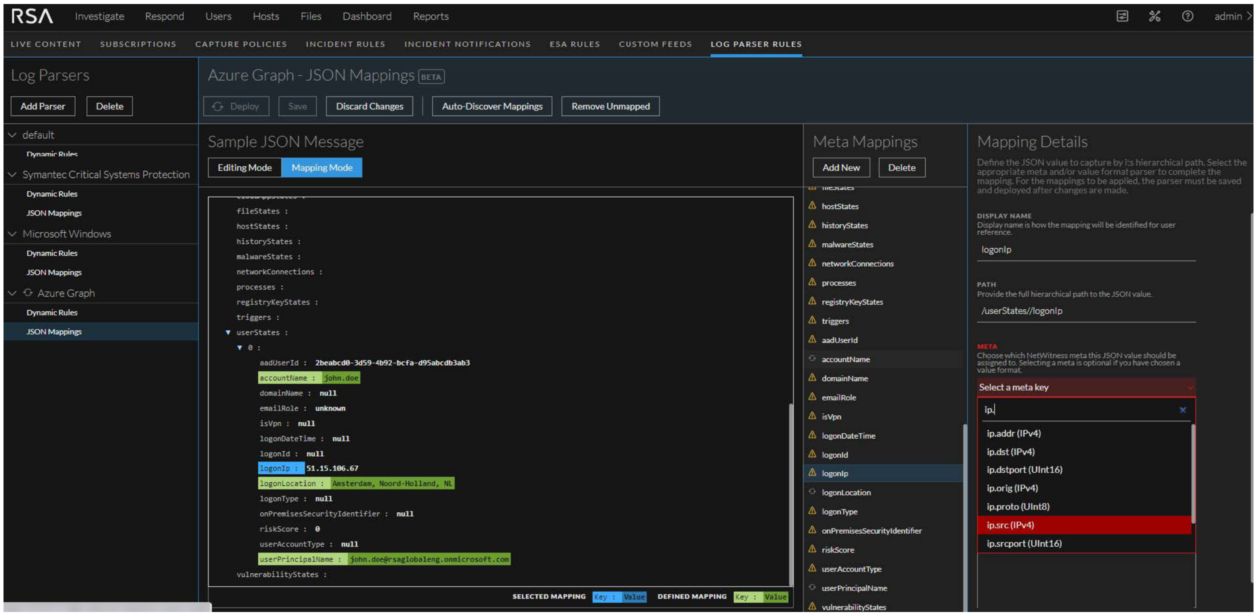
RAID Configuration for PowerVault and DACs

When allocating PowerVault storage to a Decoder / Log Decoder, users have a configuration option to include a hot-spare. For more information see "Storage Configuration Tasks" topic in Storage Guide for RSA NetWitness Platform .

Log Collection

Enhanced JSON Log Mapping (BETA)

JSON Log Mapping is enhanced to automatically add mappings for the JSON nodes in a log. You only have to choose the meta value and no longer have to manually enter the name and the path of the mapping.



```
fileStates :
hostStates :
historyStates :
malwareStates :
networkConnections :
processes :
registryKeyStates :
triggers :
▼ userStates :
  ▼ 0 :
      aadUserId :  2beabcd0-3d59-4b92-bcfa-d95abcdb3ab3
      accountName :  john.doe
      domainName :  null
      emailRole :  unknown
      isVpn :  null
      logonDateTime :  null
      logonId :  null
      logonIp :  51.15.106.67
      logonLocation :  Amsterdam, Noord-Holland, NL
      logonType :  null
      onPremisesSecurityIdentifier :  null
      riskScore :  0
      userAccountType :  null
      userPrincipalName :  john.doe@rsaglobaleng.onmicrosoft.com
vulnerabilityStates :
```

Define the JSON value to capture by its hierarchical path. Select the appropriate meta and/or value format parser to complete the mapping. For the mappings to be applied, the parser must be saved and deployed after changes are made.

DISPLAY NAME
Display name is how the mapping will be identified for user reference.
logonIp

PATH
Provide the full hierarchical path to the JSON value.
/userStates//logonIp

META
Choose which NetWitness meta this JSON value should be assigned to. Selecting a meta is optional if you have chosen a value format.
ip.
- ip.addr (IPv4)
- ip.dst (IPv4)
- ip.dstport (UInt16)
- ip.orig (IPv4)
- ip.proto (UInt8)
- ip.src (IPv4)
- ip.srcport (UInt16)

After you complete the JSON log mappings, the JSON nodes and values are highlighted in green in the JSON tree, this allows you to identify which nodes are mapped. Once you map the JSON nodes that are needed, you can quickly remove the unmapped JSON nodes. For more information see "Auto Discover JSON Mappings" topic in Log Parser Customization Guide for RSA NetWitness Platform

Logstash Integration

NetWitness Export Connector

NetWitness Platform version 11.5.1 introduces "NetWitness Export Connector 1.0", an input plugin for Logstash that can be used to export NetWitness Platform events and routes the data where you want, in a streaming fashion that gives you the flexibility to unlock a variety of downstream use cases. For more information, see *NetWitness Export Connector - Installation and Configuration Guide for RSA NetWitness Platform*.

Licensing

Enhanced License Details

- Admins can check the compliance status of newly introduced Meta-only licenses.
- Usage data for Throughput license is consolidated and organized to show details of multiple statistics that are used to measure the compliance of the network throughput licenses. For more information, see the Licensing Management Guide.

Throughput License Calculation Changes

NetWitness Platform version 11.5.1 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 temporarily adjusted to delay the display of the license violation banner by 45-days. 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

Administration Fixes

Tracking Number	Description
SACE-13731/ ASOC-101328	In NetWitness Platform 11.4.0.1, Single Sign-On does not work even after implementing it.
SACE-13668/ ASOC-98036	NwLogPlayer time stamp converted into milliseconds for LogDecoder processing.
SACE-13256/ ASOC-91953	PAM is not enabled, but the PAM displays a warning message.

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

Tracking Number	Description
SACE-13400/ ASOC-102074	Unable to query on the content of the emails in the network (packets) data.
SACE-14165/ ASOC-102072	The Broker service is not able to retrieve the meta keys and the user interface hangs when a query is run.
SACE-14051/ ASOC-101846	Issue with deployment of Non-IP feeds with IPv6 values (non CIDR) on Decoders or Log Decoders. The first entry on the feed fails to load.
ASOC-101087/ ASOC-101107	Issue with logging UUID's or obsolete IP addresses in core services system log files.

Log Decoder Fixes

Tracking Number	Description
SACE-13928/ ASOC-101847	In the Investigate > Explore view, the `capture.appfilter.bytes` parameters does not display the correct count.
SACE-13985/ ASOC-101191	Index customizations for Retention Log Hybrid service not reflecting on updating entities from Index definition files on Decoder.
SACE-13350/ ASOC-95972	Log Decoder service crashes if changes are done to the log forwarding configuration fields `logs.forwarding.enabled` and `logs.forwarding.destination`.
ASOC-95972	Log Decoder service crashes if changes are done to the log forwarding configuration fields `logs.forwarding.enabled` and `logs.forwarding.destination`.

Log Collection Fixes

Tracking Number	Description
SACE-13403	The bookmarking file failed to update the correct bookmark time as the NwVmwareCollector PERL script execution failed because of linefeeds and exception (starttime and userName field) errors.

Investigate Fixes

Tracking Number	Description
SACE-13887/ ASOC-101526	Unable to export the PCAP files from the **ADMIN > System > Jobs** panel.
ASOC-100133	Filter Events Panel Shows Unexpected Results for Query Containing an Unwrapped OR.
ASOC-97975	Permissions to manage meta groups and column groups in Investigate do not apply in Investigate.

Event Stream Analysis (ESA) Fixes

Tracking Number	Description
SACE-12773	While creating a Rule with subquery using is `OneOfIgnoreCase/isNotOneOfIgnoreCase` functions for array comparison with context hub list, the functions `OneOfIgnoreCase/isNotOneOfIgnoreCase` are not called by Esper.
ASOC-101423	Position tracking does not get migrated for data sources with a deployment name that contains @ or _ characters at the end of the deployment name.
SACE-12736/ ASOC-102521	When multiple users make changes (adding or removing rules) to ESA Deployment groups, the user who clicks "deploy" first will overwrite the changes of other users.
ASOC-103097	After upgrading to version 11.5, the ESA correlation server does not aggregate events from the configured data sources.

Health and Wellness Fixes

Tracking Number	Description
SACE-13666	The Historical Graph does not show the graph, instead it shows only the tooltip when checking for data other than current day.

Malware Fixes

Tracking Number	Description
SACE-14144/ ASOC-101768	The MD5SUM hash value and the file in `spectrum/repository/files` directory does not match.

Context Hub Fixes

Tracking Number	Description
SACE-12733/ ASOC-93550	RSA NetWitness Platform Admin server is not stable because the RabbitMQ service is overloaded.

UEBA Fixes

Tracking Number	Description
ASOC-102780	The User Profile view displays data for inactive users.
ASOC-101686	When performing a rerun, UEBA deployments with the TLS schema will not trigger alerts for two weeks.
ASOC-100389	After upgrading UEBA from 11.3 to 11.5, the saved filters in the UI do not work.
ASOC-100310	After upgrade from 11.2 or 11.3 to 11.5, adapter logs are not written.

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 11.5.1 Upgrade Guide	https://community.rsa.com/docs/DOC-114927

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 11.5.1.0.

Component	Version Number
NetWitness Platform Audit Plugins	11.5.1.0-4633.5.dfa234a96.el7.noarch.rpm
NetWitness Platform Admin Server	11.5.1.0-200903125045.5.1cd2430.el7.centos.noarch.rpm
NetWitness Platform Appliance	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Archiver	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Broker	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Concentrator	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Config Management	11.5.1.0-2009221219.5.1c258d2.el7.noarch.rpm
NetWitness Platform Config Server	11.5.1.0-201013040027.5.8d3f3f2.el7.centos.noarch.rpm
NetWitness Platform Console	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Content Server	11.5.1.0-200916084613.5.5a128a8.el7.centos.noarch.rpm
NetWitness Platform ContextHub Server	11.5.1.0-200916100907.5.76183ab.el7.centos.noarch.rpm
NetWitness Platform Correlation Server (ESA)	11.5.1.0-200918140811.5.1b32a0f.el7.centos.noarch.rpm
NetWitness Platform Decoder	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Deployment Upgrade	11.5.1.0-2007011851.5.22cec34.el7.noarch.rpm
NetWitness Platform Endpoint Agents	11.5.1.0-2009242046.5.0f8aec7.el7.x86_64.rpm
NetWitness Platform Endpoint Broker Server	11.5.1.0-200930080320.5.9cf34b8.el7.centos.noarch.rpm

NetWitness Platform Endpoint Server	11.5.1.0-200930063035.5.5c24860.el7.centos.noarch.rpm
NetWitness Platform Integration Server	11.5.1.0-200902030748.5.10b7da8.el7.centos.noarch.rpm
NetWitness Platform Investigate Server	11.5.1.0-200915161133.5.ab796ca.el7.centos.noarch.rpm
NetWitness Platform Legacy Web Server	11.5.1.0-201027134652.5.0304ffd.el7.centos.noarch.rpm
NetWitness Platform License Server	11.5.1.0-201027025739.5.311661f.el7.centos.noarch.rpm
NetWitness Platform Log Decoder	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Log Player	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform Malware Analytics Server	11.5.1.0-201016050512.5.eac5558.el7.centos.x86_64.rpm
NetWitness Platform Metrics Server	11.5.1.0-200924101236.5.3d0f70c.el7.centos.noarch.rpm
NetWitness Platform Orchestration Server	11.5.1.0-200917124122.5.1ce9338.el7.centos.noarch.rpm
NetWitness Platform Reporting Engine Server	11.5.1.0-5872.5.75cab0c7b.el7.x86_64.rpm
NetWitness Platform Respond Server	11.5.1.0-200903125113.5.cea9b59.el7.centos.noarch.rpm
NetWitness Platform Root CA Update	11.5.1.0-2010201838.5.eca3a4a.el7.noarch.rpm
NetWitness Platform SDK	11.5.1.0-11324.5.81ea008ea.el7.x86_64.rpm
NetWitness Platform Security Server	11.5.1.0-200917013306.5.5b864f4.el7.centos.noarch.rpm
NetWitness Platform Source Server	11.5.1.0-200902084940.5.0bbc763.el7.centos.noarch.rpm
NetWitness Platform User Interface	11.5.1.0-200925113323.5.f27563d4a0.el7.centos.noarch.rpm
NetWitness Platform Workbench	11.5.1.0-11382.5.07bae7f5f.el7.x86_64.rpm
NetWitness Platform SMS Runtime	11.5.1.0-4633.5.dfa234a96.el7.x86_64.rpm
NetWitness Platform SMS Server	11.5.1.0-4633.5.dfa234a96.el7.x86_64.rpm

Revision History

Date	Description
November 2020	Release to Operations