RSA NetWitness

Version 11.7.1

Release Notes

Contact Information

NetWitness Community at https://community.netwitness.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 NetWitness Community. 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.

April 2022

Contents

What's New

The NetWitness 11.7.1.0 release provides new features and enhancements for every role in the Security Operations Center.

Security Fixes

The Log4j vulnerability recently discovered in the commonly used open source logging library has been addressed. This applies to CVE-2021-44228. For more information, see the Security Advisory for Log4j.

Note: This patch release of NetWitness addresses log4j vulnerabilities reported till date. The following CVEs were validated and found to be not exploitable.
- CVE-2021-44228
- CVE-2021-44832
- CVE-2021-4104
- CVE-2021-45105
- CVE-2021-45046

NetWitness will continuously monitor this issue for new developments and provide periodic updates.

Note: If you have the Export Connector plugin in your deployment, you must do the following:
- If you have Logstash installed separately, not as part of the NetWitness installation, you must uninstall the Export Connector plugin and install the updated Export Connector plugin after 11.7.0.1 patch upgrade. For more information to install the updated plugin, see *Post-Upgrade Tasks* on the Upgrade Guide for 11.7.1.0
- If you have Logstash installed as part of the NetWitness installation on the Log Collector service, the updated Export Connector plugin will be automatically installed during the 11.7.0.1 patch upgrade.

In both the above cases, the old Export Connector plugin files are not automatically removed after upgrade. You must remove the old plugin files, so the scans do not list them as vulnerabilities. For more information on how to remove the old plugin files, see see *Post-Upgrade Tasks* on the Upgrade Guide for 11.7.1.0

Upgrade Paths

The following upgrade paths are supported for NetWitness 11.7.1.0:

- NetWitness 11.5.3.2 to 11.7.1.0
- NetWitness 11.5.3.3 to 11.7.1.0
- NetWitness 11.6.0.0 to 11.7.1.0
- NetWitness 11.6.1.0 to 11.7.1.0
- NetWitness 11.6.1.1 to 11.7.1.0
- NetWitness 11.6.1.2 to 11.7.1.0
- NetWitness 11.6.1.3 to 11.7.1.0
- NetWitness 11.7.0.0 to 11.7.1.0

- NetWitness 11.7.0.1 to 11.7.1.0
- NetWitness 11.7.0.2 to 11.7.1.0

For more information on upgrading to 11.7.1.0, see Upgrade Guide for RSA NetWitness Platform 11.7.1.0

Enhancements

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

- Upgrade
- Investigation - SIEM and Network Traffic Analysis
- Endpoint Investigation
- Concentrator, Decoder, and Log Decoder Services
- Event Stream Analysis (ESA)
- Configuration Updates
- Platform

To locate the documents referred to in this section, go to the NetWitness Platform 11.x - All Documents. Product Documentation has links to the documentation for this release.

Upgrade

Pre-stage the upgrade repo to minimize downtime

Administrators can pre-stage the upgrade repository by downloading the required packages (.zip) without affecting the system. This minimizes the upgrade downtime and ensures the upgrade is completed within the planned time. The Pre-Stage Host option is available on the NetWitness UI and requires the NetWitness Server Host to be connected to Live Services. For more information, see Hosts and Services Maintenance Procedures topic in the Hosts and Services Getting Started Guide.

Note: You can use this feature only if you upgrade from 11.7.1.0 to a higher version.

Support for Additional Pre-Upgrade Check Utility

Additional health-check utility is introduced for Administrators to analyze the current NetWitness setup and identify conditions that may impact the upgrade. If any issues are detected, the issues can be resolved before proceeding with the upgrade.

The pre-upgrade check verifies the following:

- **(Component Hosts) Node X Service Status** - Verifies the status of services (Active or In Active) on all the Node X.
- **(Component Hosts) Node X Certificates Check** - Checks the certificate expiry, missing, corrupted, and issuer mismatch in all categories of Node X.

- **CPU-Memory Info** - Provides CPU and Memory details along with the real-time available memory.
- **(Admin Server) Node 0 File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness` and `root` on Node 0.
- **(Component Hosts) Node X File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness` and `root` for ESA Primary, Endpoint Log Hybrid, and UEBA services on Node X.
- **Mongo File (ESAPrimary)** - Checks the ESA Primary node in the system and verifies the permission mode of mongo file.
- **Orchestration Server Normal Mode** - Checks if the orchestration service is running in normal or safe mode.
- **(Admin Server) Node 0 Init status** - Checks if there are any issues that might fail init process.
- **(Admin Server) Node 0 closed ports** - Checks if the service ports required for NetWitness services are open and listening on Node 0.
- **(Component Hosts) Node X closed ports** - Checks if the service ports required for NetWitness services are open and listening on Node X.

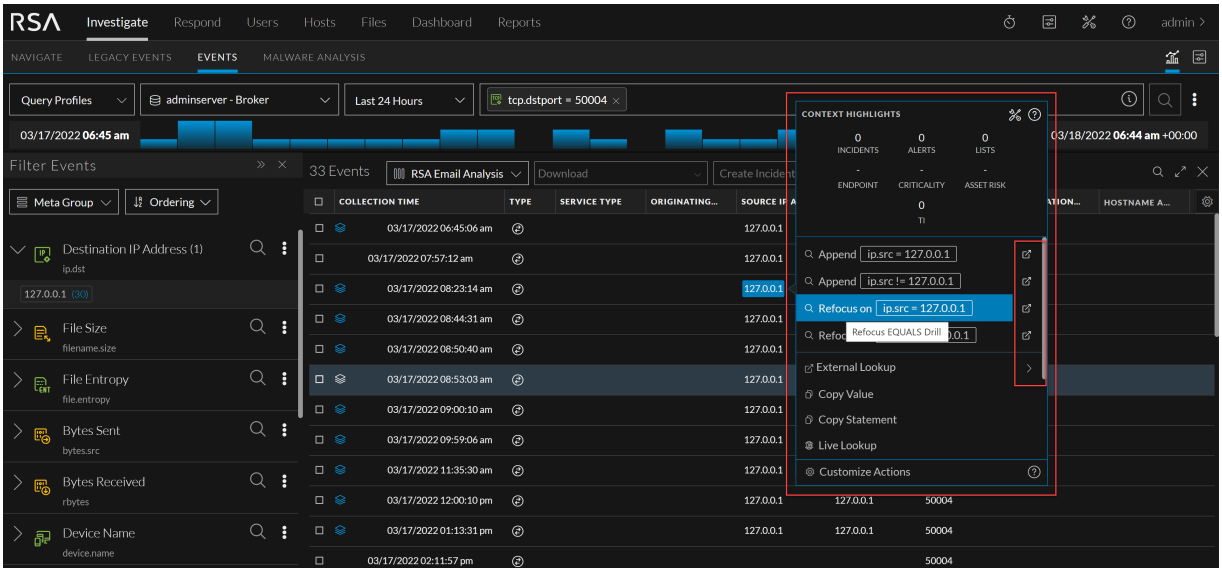
  For more information, see Upgrade Guide for NetWitness 11.7.1.0.

Investigation - SIEM and Network Traffic Analysis

Investigation Enhancements

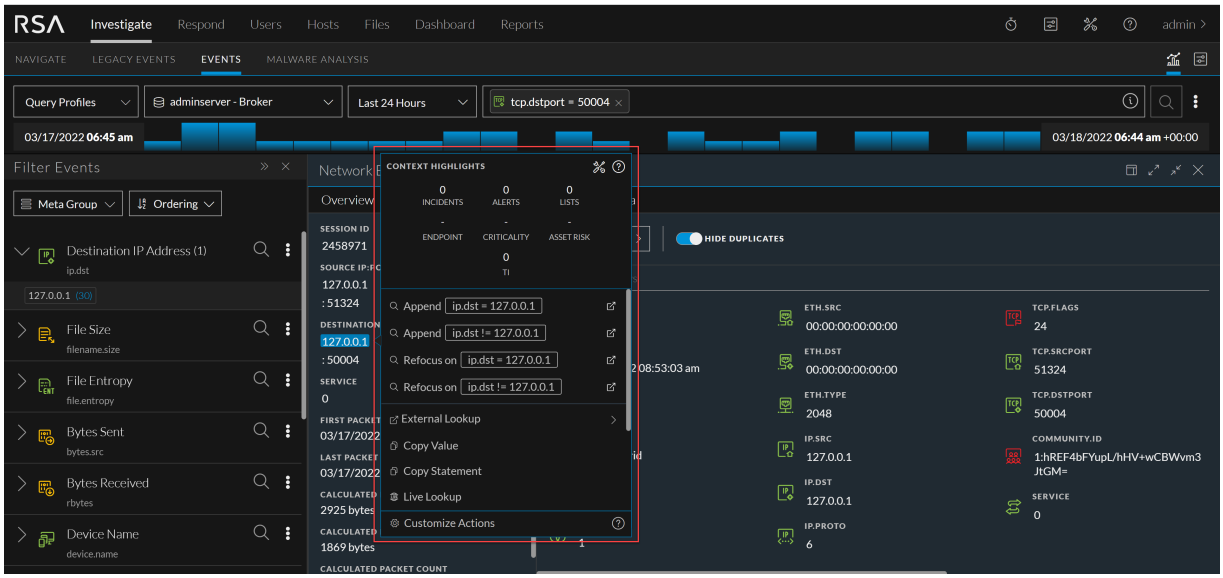
Unified Discovery and Interaction of Investigate Metadata - Analysts have a unified way to interact with metadata presented in the Events view to perform actions or review contextual information.

- Analysts can perform actions and view the context data for a selected meta in the same window or a separate window that will enable the display of data in an optimized manner, and easily carry out further investigation.



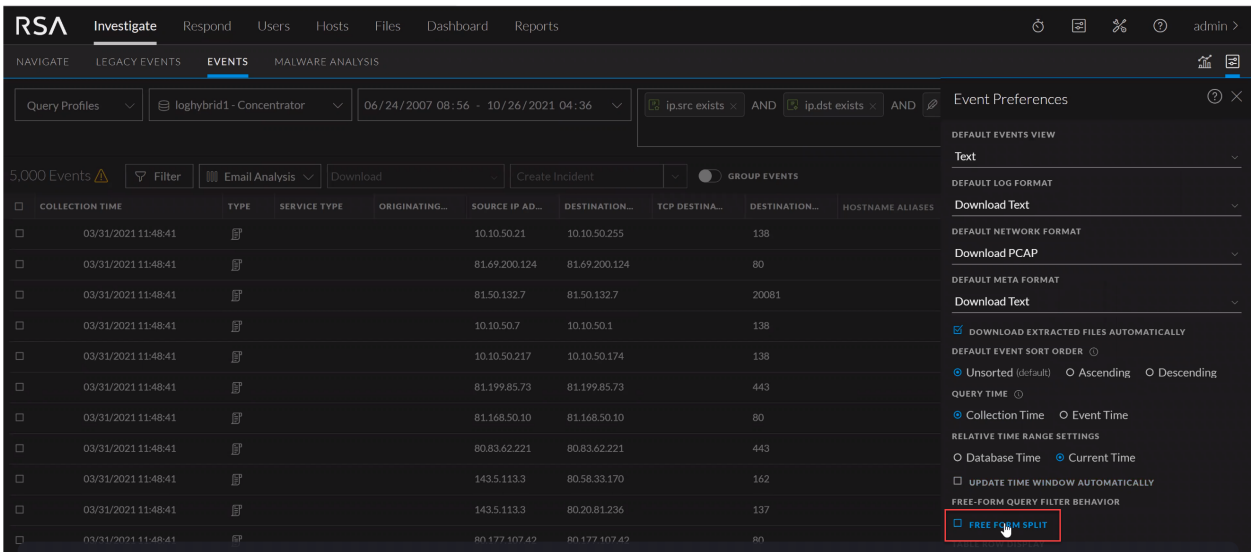
For more information, see the Use Columns and Column Groups in the Events List topic in *Investigate User Guide*.

- In the Overview and Event Meta panel, analysts can use the right and left click options to view the unified panel or run a query on a selected meta.



For more information, see the Use Columns and Column Groups in the Events List topic in *Investigate User Guide*.

Free-form Query Preference - With the new preference, analysts can choose to split the free-form queries into multiple guided filters or a single free-form query. Analysts can switch the modes using the Free Form Split checkbox.



Light Theme Overhaul – The existing light theme primary and secondary colors on the UI has been enhanced to provide better contrast and shading for improved user experience.

For more information, see the Investigate User Guide.

Endpoint Investigation

Capabilities for Detecting Ransomware that Use the Registry

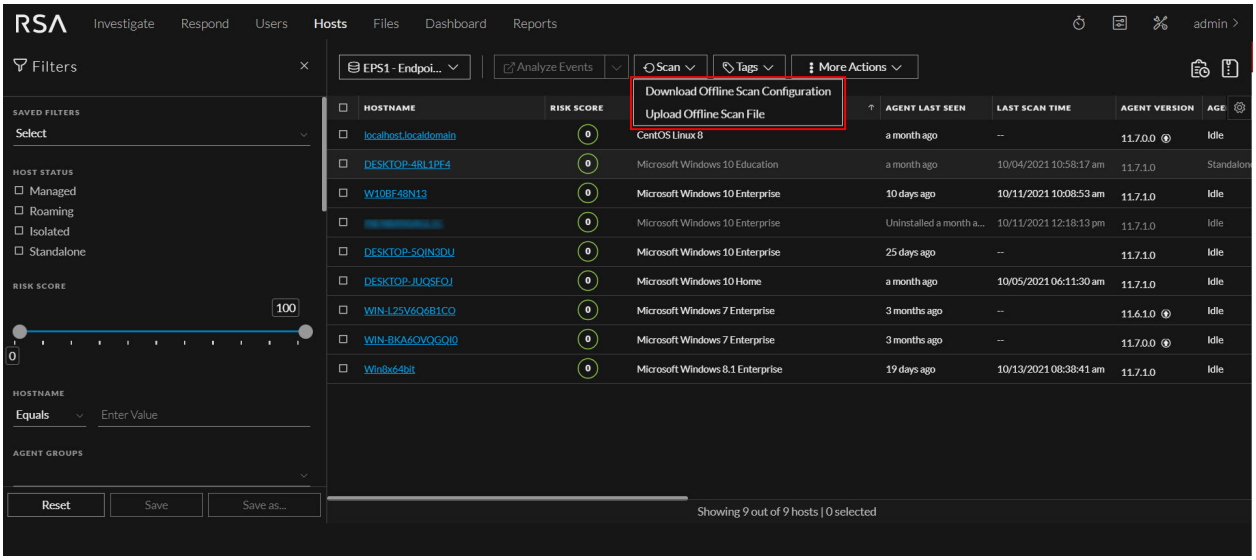
Endpoint agents can detect ransomware that uses the registry to perform actions such as forcing Windows machines to reboot in safe mode, encrypting files, and deleting volume shadow copies.

Endpoint Agent Support for macOS Monterey and Windows 11

Endpoint Agents are enhanced to support macOS Monterey (12.0.1) and Windows 11. To view the list of supported operation systems, see Introduction to Endpoint Agent Installation on the *NetWitness Endpoint Agent Installation Guide*.

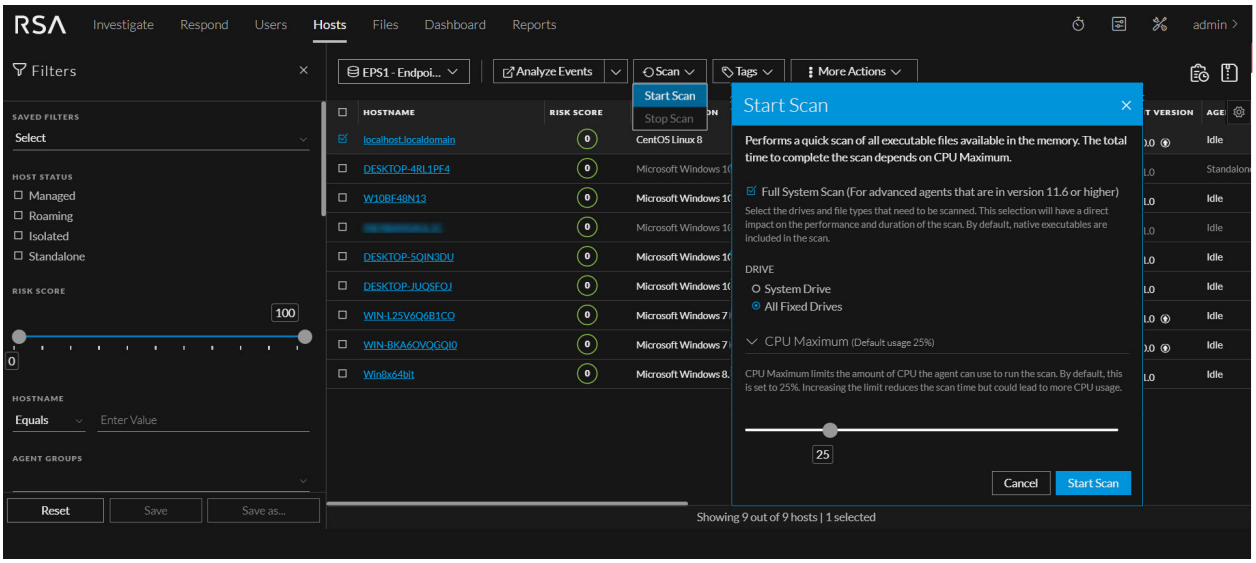
Support for Offline or Standalone Scans on Air-gapped Windows Hosts

Administrators can execute offline or standalone scans on air-gapped Windows hosts to perform threat analysis on the Windows hosts disconnected from the network. Administrators can download the Offline Scan Configuration file from UI and execute it on multiple air-gapped hosts. Then, the Offline Scan File (scan results file) can be transferred to the UI and uploaded to the Endpoint server for processing. See Standalone Scan on Air-gapped Windows Hosts topic on NetWitness Endpoint User Guide for more information.



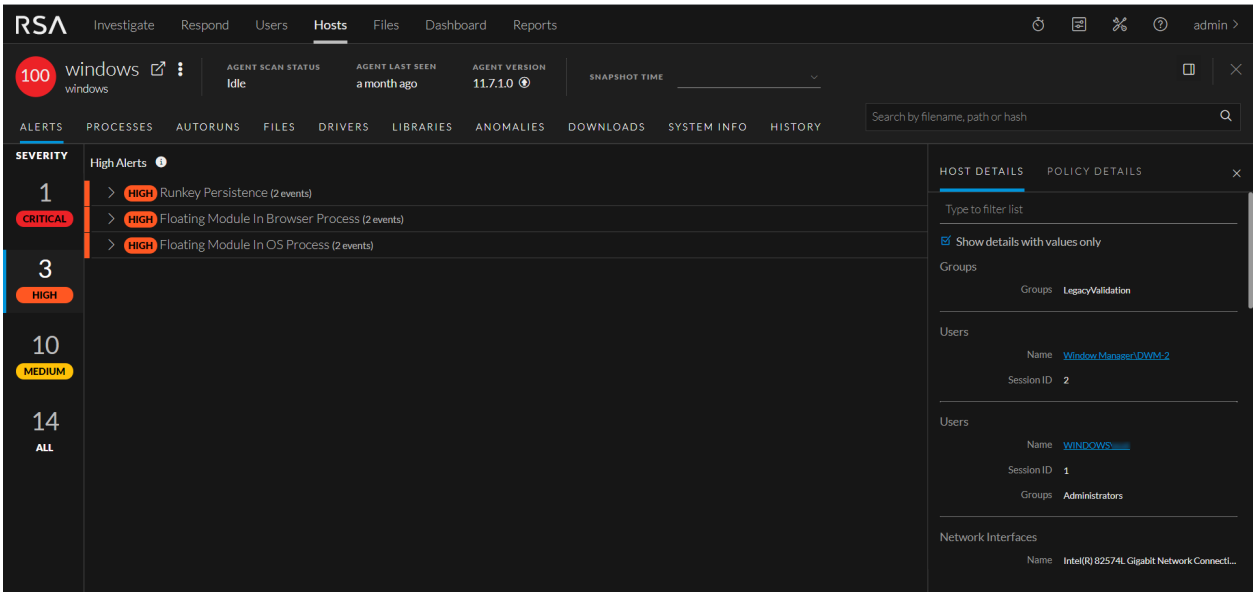
Support for Full System Scan

Analysts can perform a full system scan on system drives and all fixed drives in addition to the quick scan of executable files in memory. For more information, see Scan Hosts topic on NetWitness Endpoint User Guide.



Redesigned Alerts Tab for Optimized Navigation

Analyst can use the redesigned alerts tab to conveniently access all alert information and the associated events for optimized navigation on Host details view. For more information, see NetWitness Endpoint User Guide.



Concentrator, Decoder, and Log Decoder Services

Centralized Configuration Management Enhancements

The enhanced centralized configuration management allows administrators to:

- Reconfigure 10G Network Decoders from the Policy UI. Administrators can quickly create 10G policies for each Decoder group based on the hardware profile.

- Clone policy from an existing service to save policy transition time for existing users.
- Restart only specific services within a service group that require changes. This minimizes potential downtime.

For more information, see Host and Services Getting Started Guide.

Enhanced Network Decoder to Support Load Balancing Deployments

When you shut down the Decoders, the network interfaces connected to the Decoders are automatically shut down. Then, the load balancers divert the traffic to other available Decoders. This enhancement will protect customers from data loss when they use load balancers to distribute traffic between several Decoders. For more information, see *Configure the Decoder Capture Failover in Load Balance Deployments* topic on Decoder and Log Decoder Configuration Guide.

Event Stream Analysis (ESA)

Enhanced Performance when Retaining Incident Network Data Artifacts

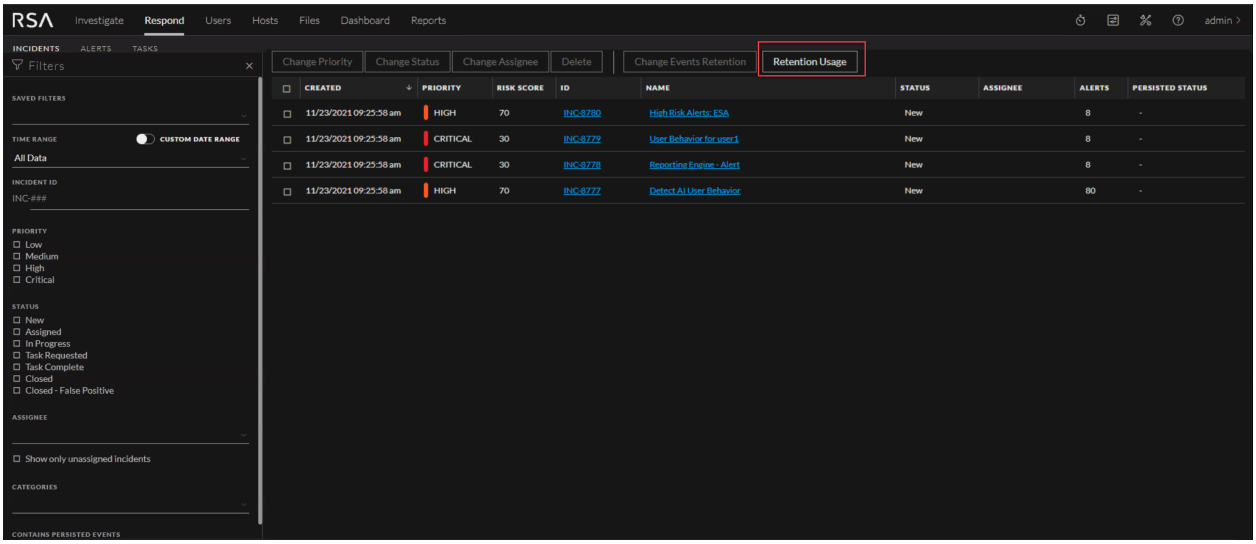
Respond analysts saving artifacts of an incident will notice improved feedback for the tasks running and swifter completion of those tasks.

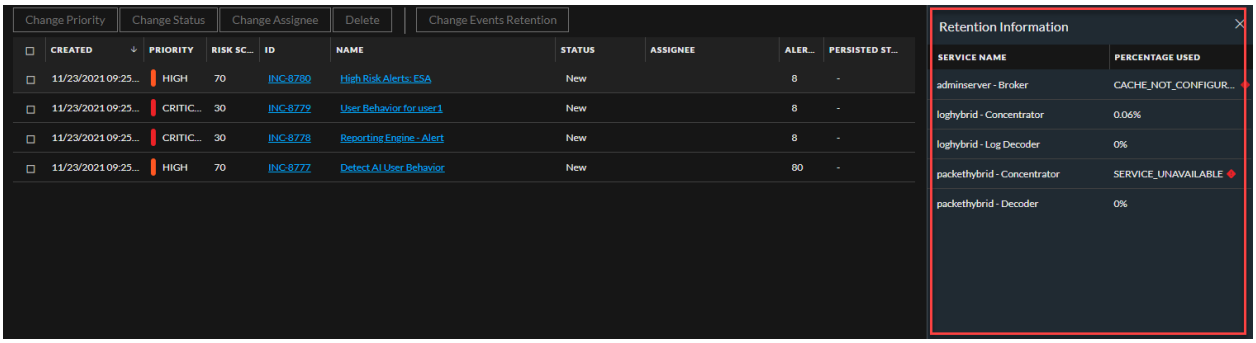
Analyst can use the new Retention Usage tab to view the statistics of all configured services and the percentage used by the pinned cache directories.

With this information, the analyst can:

- Determine if the disk is running out of space and if additional space needs to be added or the persistence needs to be suspended for the existing events in an incident.
- Obtain insights on the space requirements for retention functions.

In Respond > Incidents tab, analyst can click the Retention Usage tab to fetch all the statistics of all the configured services and the percentage used by the pinned cache directories.





For more information, see Escalate or Remediate the Incident topic the Respond User Guide.

Configuration Updates

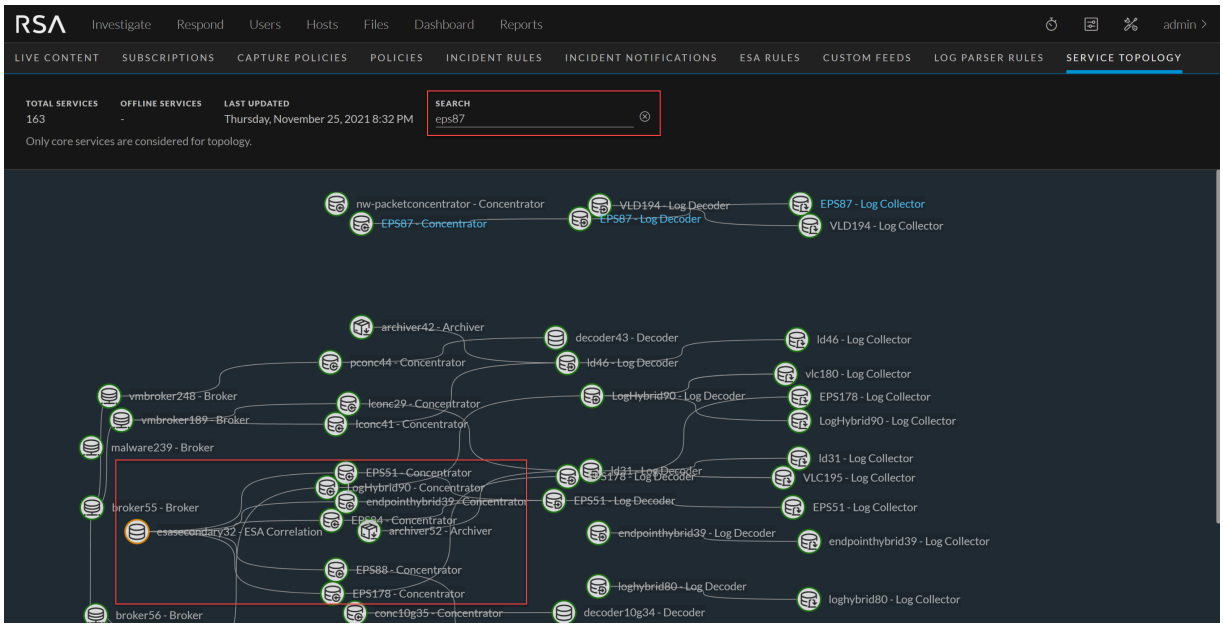
Feed Case Sensitivity

Administrators can configure to ignore the case sensitivity of values a feed uses as part of the feed wizard in the UI. This allows the administrator to avoid converting the feed into an XML format or perform additional steps during deployment. For more information, see Creating a Custom Feed in the Live Services Management Guide.

NetWitness Topology Feature

The following enhancements help administrators and analysts to:

- **Obtain quick insights using the Search Option** – The search option helps locate a specific service, without having to look at the entire hierarchical layout.
- **View ESA hosts**: ESA service and the connected services can be viewed in the hierarchical layout.



For more information, see the Hosts and Services Getting Started Guide.

Platform

Backup and Restore CLI Improvements

Administrators can take advantage of the following improvements:

- Back up Mongo databases for Endpoint and ESA instances.
- Include Broker index for NetWitness node in which Broker service is running.
- Back up custom files and folders provided by user.

For more information, see the Recovery Tool User Guide.

Better Error Handling for Core Services Messages

Improved error messaging to include the source string and target format when an unrecognized string format exception is generated to help users determine the root cause.

Support for new internal RAID controller (PERC H750) on Series 6 Appliances

The existing internal controller (PERC H740 Mini) on S6 Dell PowerEdge 640/740 based appliances are replaced with PERC H750. All S6 appliances will have the new ISO to support PERC H750. All future S6 appliances and RMA will have PERC H750. Before adding a new appliance with PERC H750 to your existing deployment (For example, 11.7.0.0 or 11.7.0.1), you must first upgrade the Admin Server and Standby Admin Server to version 11.7.0.2 or higher.

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 NetWitness Platform Known Issues list on NetWitness Community portal.

Log Collection Fixes

Tracking number	Description
ASOC-112586	NwLogCollector Service is frequently respawning with 9/KILL Signals leading the service to enter into a bad state and failure.
ASOC-80137	'Last modified' column on an ESA Rule Deployment does not allow sorting because the UI sends DateModified and looking for this value in DataBase. However, the DB has DateLastModified field, not DateModified.

ESA Fixes

Tracking number	Description
ASOC-113649	ESA Rule deployment fails because API calls time out when there are lots of rules in the deployment.
ASOC-114216	ECDHE cipher does not support syslog TLS connection, while establishing connection between the server and client.

Context Hub Fixes

Tracking number	Description
ASOC-113605	List located at **Admin** > **Service** > **Context Hub** > **Config** > **List** displays the previously loaded data from the CSV file data even if an empty CSV file is uploaded to overwrite it into Context Hub.

Reporting Engine Fixes

Tracking number	Description
ASOC-113286	In reporting Engine, scheduled weekly report is not generating properly. It runs on a different day of the week even when a specific time zone is selected and converted to UTC, it flows into the previous or the next day.

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

Tracking number	Description
SACE-16772	After setting the Parse Transaction Mode (`parse.transaction.mode`) to **on** in **Admin** > **Services**> **View**> **Config**> **Explore**> **Decoder**> **Parsers**> **Config**, and try to Filter or Truncate incoming packets via App Rule in the Rule Editor window (**Explore**> **Config**> **App Rules**), the sessions are not processed, and the packets are not displayed in the Investigate page.

NetWitness Server Fixes

Tracking number	Description
ASOC - 113390	The build-in exit command (Run nw-shell > admin) couldn't exit from the NwShell gracefully because the spring application context is not closed properly.
ASOC-113848	Deleted Machine records were not removed from mongoDB though the delete operation was performed on the UI. This happens because of an error in deleting documents containing null / empty array in machinefile collection.

Tracking number	Description
SACE-13643 SACE-16473 SACE-17131 SACE-16786 SACE-16766 ASOC-49262	Installation of a service on a host fails as the service may already be installed on the host. There is no message to indicate the same. This is fixed by displaying a message listing the services installed on the host before installation.

Endpoint Fixes

Tracking number	Description
ASOC-113850	Failed to upload a file to the Endpoint-server when automatic file download is enabled as the hash of the file to be downloaded has changed. This caused high CPU usage in the machine.

SA Classic Web Application Fixes

Tracking number	Description
ASOC-113766	NetWitness service topology tab is visible with the 'False' feature tag in extjs pages. Login to **NetWitness Platform** > **SA Source Server**> **Explorer** > **features**> feature tag.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness Platform 11.x Master Table of Contents	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 11.7 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 11.7 Upgrade Guide	https://community.netwitness.com//t5/rsa-netwitness-platform-staged/upgrade-guide-for-11-7-1/ta-p/658666

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on 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:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here:https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- See Troubleshooting section in the guides.
- See also RSA NetWitness® Platform Blog Posts.
- If you need further assistance, contact NetWitness Support.

Contact NetWitness Support

If you contact NetWitness Support, you should be at your computer. Be prepared to provide the following information:

- The version number of the 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.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact RSA NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Build Numbers

The following table lists the build numbers for various components of NetWitness 11.7.1.0.

Component	Version Number
NetWitness Audit Plugins	rsa-audit-plugins-11.7.1.0-4759.5.c9d173e37.el7.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Broker	rsa-nw-broker-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Concentrator	rsa-nw-concentrator-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-11.7.1.0-2203281719.5.a6607a9.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-11.7.1.0-211027104203.5.6db321b.el7.centos.noarch.rpm
NetWitness Console	rsa-nw-console-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Content Server	rsa-nw-content-server-11.7.1.0-210928060352.5.97a0904.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-11.7.1.0-211207101137.5.a34943b.el7.centos.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-11.7.1.0-220201033229.5.40fc434.el7.centos.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-11.7.1.0-2109210631.5.286995c.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-11.7.1.0-2111042134.5.811d099.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-11.7.1.0-211115061143.5.a777eb9.el7.centos.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-11.7.1.0-220111053722.5.c8c3c14.el7.centos.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-11.7.1.0-220131065448.5.a0217e7.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-11.7.1.0-211029100157.5.7638003.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-11.7.1.0-220331150244.5.3dc0de3.el7.centos.noarch.rpm

NetWitness Log Decoder	rsa-nw-logdecoder-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-11.7.1.0-220316032229.5.3497c84.el7.centos.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-11.7.1.0-211123040334.5.a64cd77.el7.centos.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-11.7.1.0-210913095434.5.6b579d0.el7.centos.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-11.7.1.0-5918.5.a9ca1da4a.el7.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-11.7.1.0-220324045201.5.880e2bf.el7.centos.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-11.7.1.0-220118025727.5.c12703a.el7.centos.noarch.rpm
NetWitness Source Server	rsa-nw-source-server-11.7.1.0-220118035623.5.ff5109d.el7.centos.noarch.rpm
NetWitness User Interface	rsa-nw-ui-11.7.1.0-211115045702.5.f44042a38a.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-11.7.1.0-12265.5.1ffba5e11.el7.x86_64.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-11.7.1.0-4759.5.c9d173e37.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-11.7.1.0-4759.5.c9d173e37.el7.x86_64.rpm

Revision History

Date	Description
March 2022	General Availability