RSA® NetWitness

Version 11.7

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

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

November 2021

Contents

What's New

The NetWitness 11.7 release provides new features and enhancements for every role in the Security Operations Center.

Upgrade Paths

The following upgrade paths are supported for NetWitness 11.7.0.0:

- NetWitness 11.5.3.2 to 11.7.0.0
- NetWitness 11.6.0.0 to 11.7.0.0
- NetWitness 11.6.0.1 to 11.7.0.0
- NetWitness 11.6.1.0 to 11.7.0.0
- NetWitness 11.6.1.1 to 11.7.0.0

For more information on upgrading to 11.7.0.0, see Upgrade Guide for NetWitness 11.7

Security Fixes

For more information on Security Fixes, see Security Advisories.

Enhancements

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

- Investigation
- Endpoint Investigation
- Concentrator, Decoder, and Log Decoder Services
- Event Stream Analysis (ESA)
- Platform
- Upgrades
- NetWitness Services

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

Investigation

Meta Only Event Reconstruction

As analysts review events, the new compact and expanded metadata views provide an alternative workflow to only view the high-level details of the event and in use cases where no raw data is present.
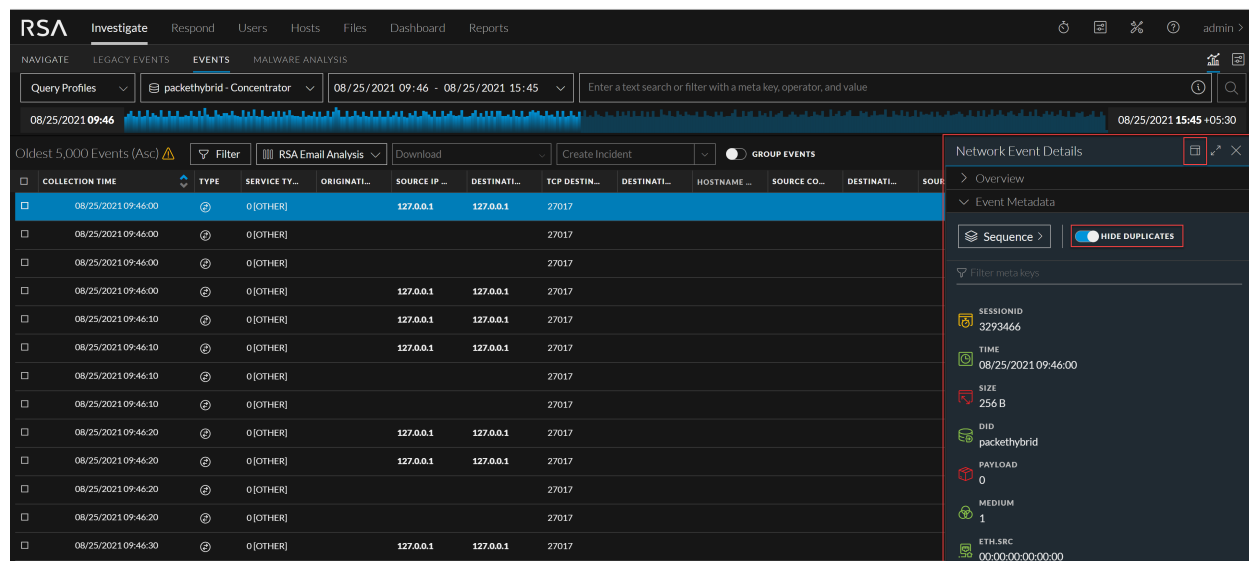
Improved Broker Query Experience

Analyst queries at the top-level Broker now by default provide partial results when one of the sub-services loses connectivity or times out. In addition, a hierarchical view of what is attached to the Broker is available to analysts to exclude certain sub-services prior to query if necessary.
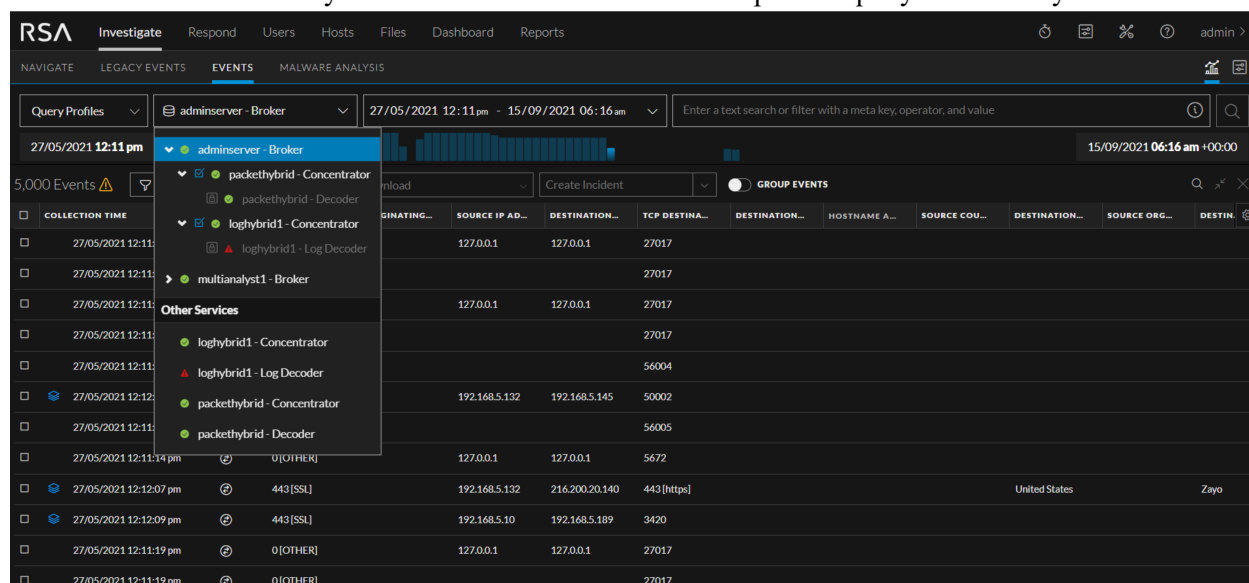
Email Reconstruction Improvement

Analyst can view the content of all the emails in a single session using the Expand All Emails option available on the Email view.
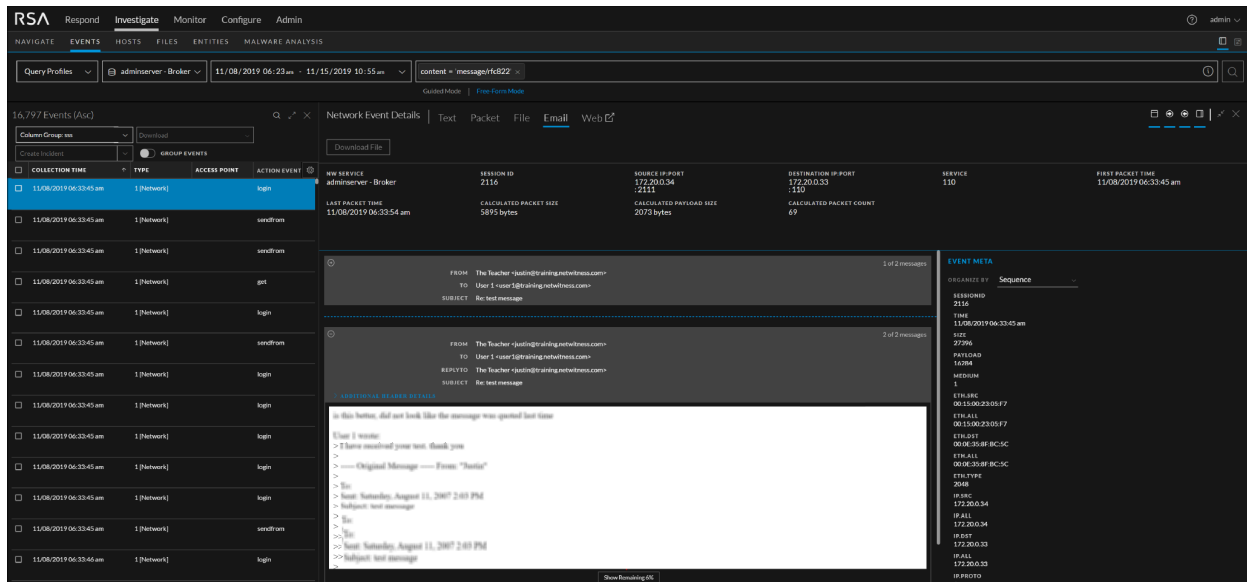
Direct Query Interaction with Meta Keys in Event Filter Panel

Analyst steps to create a query have been streamlined by clicking directly on the meta key name to generate a query with only the meta key. Alternatively, searches with combination of key value pairs are available inside the Event Filter panel without requiring direct interaction with the query bar.
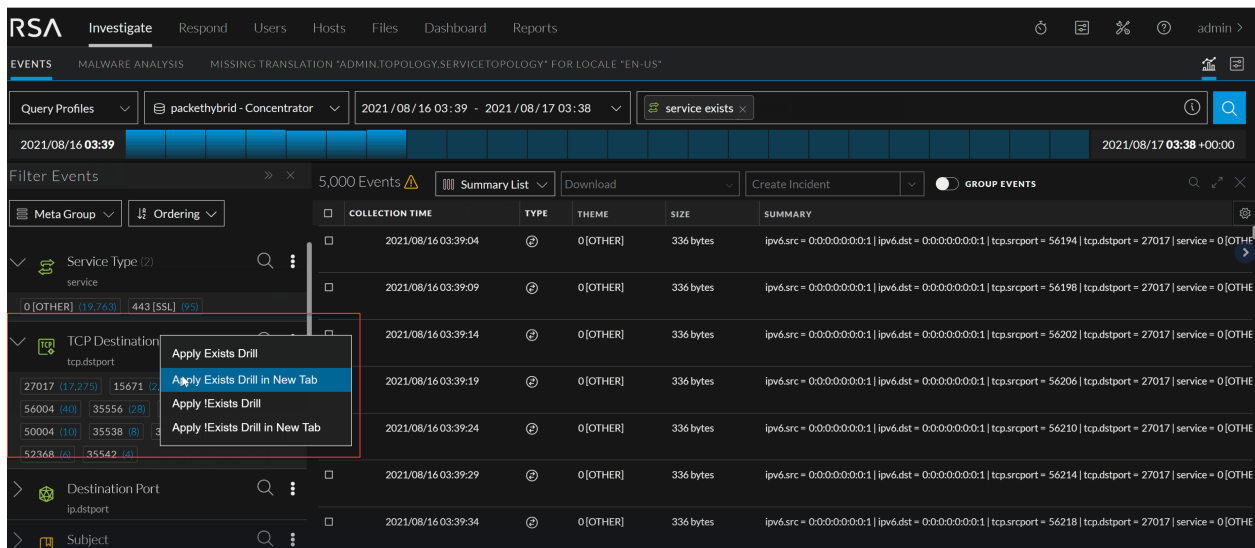
Network Fragment Identification

Analysts can view the related sessions for an event for analysis and investigation by hovering over the icon for the event.
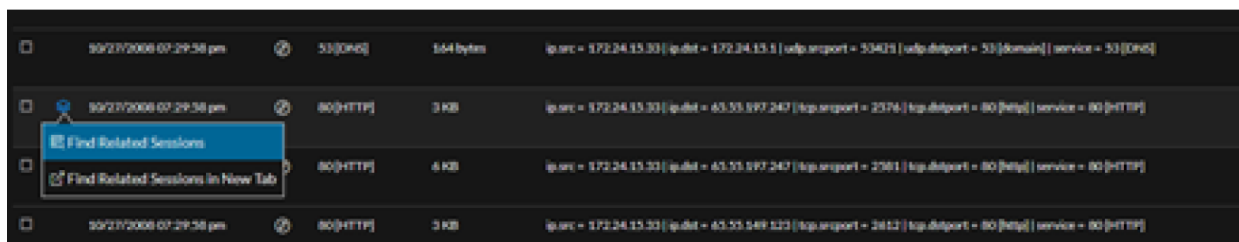
Saved Time Ranges

Analysts can take advantage of the last five recently used time ranges for future searches saving the investigation time. The saved time ranges are displayed under the Recent Time Ranges section.
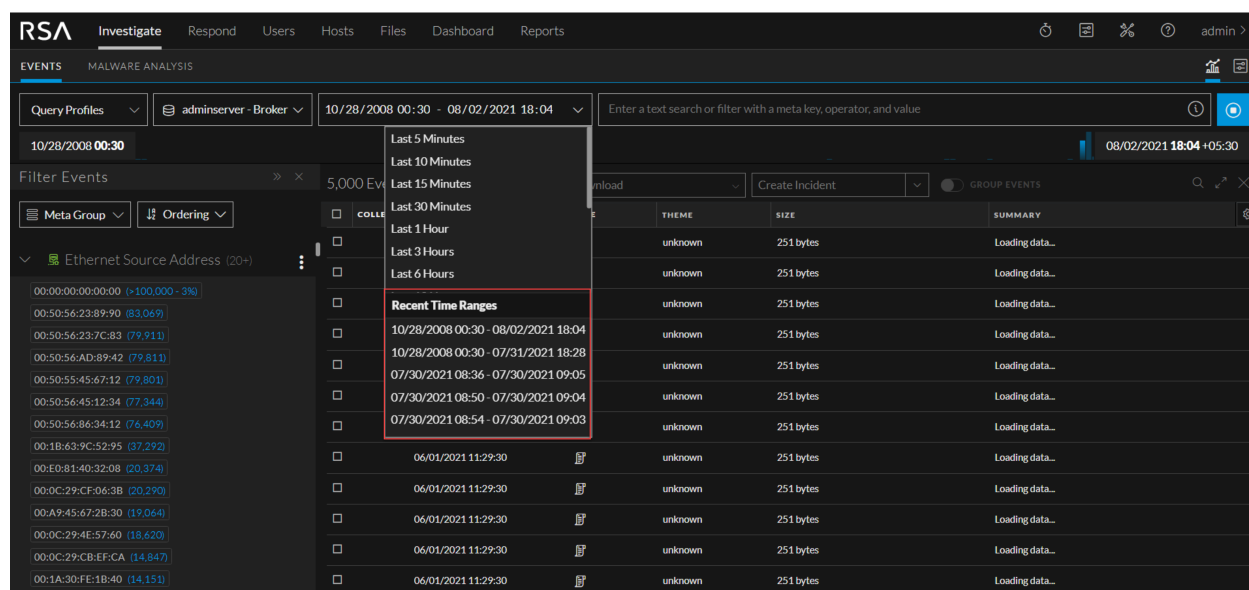
For more information, see the Investigation User Guide.

Endpoint Investigation

Granular Role Based Access Control for Endpoint Server

With the enhanced RBAC (Role-Based Access Control), administrators can grant or revoke access to specific Endpoint servers rather than all. And the addition of new permissions called endpoint-server.file.analyze and endpoint-server.tag.manage, adds flexibility in managing user privileges. For more information on managing permissions for an individual Endpoint server, see NetWitness Endpoint Configuration Guide.

Few Privileges Removed From *endpoint-server.agent.manage* And Added to *endpoint-server.file.analyze*

Analyze File, Save Local Copy and Scan with OPSWAT privileges are removed from *endpoint-server.agent.manage* and added to a new permission called *endpoint-server.file.analyze*. For more information see the System Security and User Management Guide.

Manage Hosts Using Tags

Analysts can create Tags to manage the hosts. Tags are custom texts (can combine alphanumeric and special characters) that you can create and assign to hosts. You can create host groups based on tags, and on the Hosts view, you can filter hosts by tags using the filters pane. Administrators can create and assign tags while generating the agent packager, and these are added to the hosts by default when the Endpoint agent is installed. For more information on managing tags, see NetWitness Endpoint User Guide.

Enhanced Windows Agent to Support Detecting the Persistence Techniques Targeting the Registry

The enhanced Windows agents detects persistence techniques that use the Windows registry. The registry monitor is more reliable now as it detects suspicious activity in an enhanced manner. For more information, see the NetWitness Endpoint User Guide.

Enhanced Suspicious Thread Detection

This enhancement to the suspicious thread detection helps detect and report suspicious threads more effectively using different methods. This enhancement enables analysts to have access to all the details and capabilities related to the suspicious threads as before. For more information, refer NetWitness Endpoint User Guide.

Delete Blocked Files Through Elevated Command Prompt

You can delete the blocked files on the host using the delete command on the elevated command prompt on the host.

Concentrator, Decoder, and Log Decoder Services

Introduction of Centralized Configuration Management

The management of general NetWitness core services namely Concentrator, Decoder, and Log Decoder configurations can be administered centrally from a single policy-based interface and distributed to multiple services. With centralized configuration management, administrators can:

- Create a group of the same service type based on similar hardware profiles or other criteria

- Add configuration items to policies in order to customize settings. Any settings which are not in the policy will be left as default

- Apply customized settings to any number of services in one step

- Restart all services within a group to apply changes

- View when an action is required, such as service restart, unpublished policies or out-of-compliance services indicated by the icon.

- Revert changes to a policy or group quickly

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

Enhanced Query Accuracy

An optional index configuration is available on a per meta key basis to extend the default key-value search into an N-gram layout. In addition to enabling query and reporting capabilities, this combination also provides complete and accurate search results, even if a maximum value threshold has been met.

For more information, see N-grams in the Core Database Tuning Guide.

Event Stream Analysis (ESA)

Enhancements for persisting Events and Incidents

Analysts can persist events encompassed in an incident, thus enabling to view the incident in the future, regardless of its age. Analysts can:

- Pin or unpin multiple events at an incident and alert level

- View details on when the events were persisted.

- Check the status of the persisted events, whether it is Completed, Partial, or None.

- Administrators can set up permissions for users to persist raw data associated with a particular incident.

For more information, see the Respond User Guide.

Platform

Backup and Restore Improvements

A new NetWitness Recovery Wrapper tool is introduced to centrally back up and restore individual or multiple hosts. This tool allows custom files to be incorporated in restorations and handles all supported deployment installations (Physical, Virtual, and Cloud).

With NetWitness Recovery Tool administrators can:

- Back up (export) an individual, a specific, or all hosts at a time

- Restore (import) an individual host at a time

- Customize files or folders during backup and restore

- Copy backup data to remote host location from NetWitness hosts and vice versa

For more information, see "Disaster Recovery (Back Up and Restore)" topic in the NetWitness Recovery Tool User Guide *for NetWitness*.

```
[root@adminserver ~]# nw-recovery-wrapper export -d /var/netwitness/backup/ --host-all --include /home/ /home/deep.txt --remote-ip              --remote-location /home/ --remote-password ne
twitness
2021-09-22 08:39:38,180 INFO  nw-recovery-wrapper|Running command: export
2021-09-22 08:39:38,180 INFO  nw-recovery-wrapper|Performing NRT remote operation on: *
2021-09-22 08:39:38,180 INFO  nw-recovery-wrapper|*** Export data/configuration ***
2021-09-22 08:39:38,180 INFO  nw-recovery-wrapper|Creating backup on: /var/netwitness/backup/
2021-09-22 08:39:38,180 INFO         __init__|Validating salt communication...
2021-09-22 08:39:38,684 INFO         __init__|Reachable Hosts: *
2021-09-22 08:39:38,687 INFO         __init__|Validating remote host connection with provided credentials...
2021-09-22 08:39:46,829 INFO         __init__|Updated custom path ['/home/', '/home/deep.txt'] in specified host's nw-base.nrt
2021-09-22 08:39:46,831 INFO         __init__|Scheduling backup for reachable target...'*'
2021-09-22 08:43:08,138 INFO         __init__|host              'esaprimary'                                  -> backup success
2021-09-22 08:43:08,138 INFO         __init__|host              'archiver'                                     backup success
2021-09-22 08:43:08,139 INFO         __init__|host              'adminserver'                                -> backup success
2021-09-22 08:43:08,139 INFO         __init__|host              'endpointloghybrid'                              -> backup success
2021-09-22 08:43:08,139 INFO         __init__|Scheduling remote copy on successfully backed up Netwitness host ['                                              ]
2021-09-22 08:43:28,782 INFO         __init__|host              'esaprimary'                                 -> remote copy success
2021-09-22 08:43:28,782 INFO         __init__|host              'archiver'                                    remote copy success
2021-09-22 08:43:28,782 INFO         __init__|host              'adminserver'                               -> remote copy success
2021-09-22 08:43:28,782 INFO         __init__|host              'endpointloghybrid'                          -> remote copy success
2021-09-22 08:43:28,782 INFO         __init__|Summarizing results...
2021-09-22 08:43:28,782 INFO         __init__|IP               HOSTNAME          ID          STATUS    MESSAGE
2021-09-22 08:43:28,783 INFO         __init__|--               --------          --          ------    -------
2021-09-22 08:43:28,783 INFO         __init__|                  esaprimary                    success
2021-09-22 08:43:28,783 INFO         __init__|                  archiver                      success
2021-09-22 08:43:28,783 INFO         __init__|                  adminserver                   success
2021-09-22 08:43:28,783 INFO         __init__|                  endpointloghybrid             success
2021-09-22 08:43:29,098 INFO         __init__|Reverted nw-base.nrt on reachable nodes
2021-09-22 08:43:29,406 INFO  nw-recovery-wrapper|*** Requested operation completed successfully ***
[root@adminserver ~]#
```

Upgrades

Introduction of Pre-Upgrade Check Utility

A new 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:

- **Security Client File Check** - Ensures `security-client-amqp.yml` file is not present

- **Node-0 NW Service-id Status** - Ensures all the service-ids are intact with the services in Node 0

- **Broker Service Trustpeer Symlink** - Ensures Broker symlink file (`/etc/netwitness/ng/broker/trustpeers/`) is not broken

- **Node-0 NW Services Status** - Checks the status of all the services in Node 0

- **Yum External Repo Check** - Ensures external repos are not available

- **RPM DB Index Check** - Checks if the RPM DB is corrupted

- **Salt Master Communication** - Verifies the salt communication from Node 0 to all the Nodes

- **Node-0 Certificates Check** - Checks if any certificates are missing, expired, or invalid

- **Mongo Authentication** - Validates the `deploy_admin` credentials fetched from `security-cli-client` using Mongo client

- **RabbitMQ Authentication** - Validates the `deploy_admin` credentials fetched from `security-cli-client` using RabbitMQ

For more information, see Upgrade Guide for NetWitness 11.7.

```
2021-09-22 06:33:30,575 DEBUG          mongo_shell|Executing mongo-shell
2021-09-22 06:33:30,845 INFO           UpgradeProbes|MongoAuthenticationProbe: *** completed verification of mongo authentication
sing deploy_admin creds***
2021-09-22 06:33:31,067 DEBUG          UpgradeProbes|FetchDeployAdminCreds: *** successfully fetched deploy_admin password ***
2021-09-22 06:33:31,067 DEBUG          UpgradeProbes|RabbitmqAuthenticationProbe: *** verifying rabbitmq authentication using dep
oy_admin creds***
2021-09-22 06:33:32,332 INFO           UpgradeProbes|RabbitmqAuthenticationProbe: *** completed verification of rabbitmq authentic
tion using deploy_admin creds ***
2021-09-22 06:33:32,333 INFO     nw-precheck-tool|Security Client File Check -> Success
2021-09-22 06:33:32,333 INFO     nw-precheck-tool|Broker Service Trustpeer Symlink -> Success
2021-09-22 06:33:32,334 INFO     nw-precheck-tool|Node-0 NW Service-id Status -> Success
2021-09-22 06:33:32,334 INFO     nw-precheck-tool|Node-0 NW Services Status -> Success
2021-09-22 06:33:32,334 INFO     nw-precheck-tool|RPM DB Index Check -> Success
2021-09-22 06:33:32,334 INFO     nw-precheck-tool|Yum External Repo Check -> Success
2021-09-22 06:33:32,334 INFO     nw-precheck-tool|Salt Master Communication -> Success
2021-09-22 06:33:32,335 INFO     nw-precheck-tool|Node-0 Certificates Check -> Success
2021-09-22 06:33:32,335 INFO     nw-precheck-tool|Mongo Authentication -> Success
2021-09-22 06:33:32,335 INFO     nw-precheck-tool|Rabbitmq Authentication -> Success
2021-09-22 06:33:32,335 INFO     nw-precheck-tool|*** completed running check-list for upgrade-cli-client ***


     PROBES                         STATUS        KB-ARTICLE      MESSAGE
     -----                          ------        ----------      -------
     Security Client File Check     Success
     Broker Service Trustpeer Symlink   Success
     Node-0 NW Service-id Status    Success
     Node-0 NW Services Status      Success
     RPM DB Index Check             Success
     Yum External Repo Check        Success
     Salt Master Communication      Success
     Node-0 Certificates Check      Success
     Mongo Authentication           Success
     Rabbitmq Authentication        Success

2021-09-22 06:33:32,336 INFO     nw-precheck-tool|*** Requested operation completed ***
[root@PrimarySA ~]#
```

NetWitness Services

Introduction of NetWitness Service Topology Map

A view of the hierarchical layout of all NetWitness core services depicting the collection and aggregation of services provides administrators and analysts quick insights into their deployment and the services that are online or offline. This topology displays only the Broker, Concentrator, Log Decoder, Packet Decoder, Hybrids, and Log Collector services. For more information, see the System and Security User Management Guide.

Note: Reporting Engine, Malware Analysis, UEBA, Endpoint Server, Cloud Link service, and Warehouse Connectors are not supported.

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.

Administration Fixes

Tracking Number	Description
ASOC-105322, SACE 14678	NetWitness Active Directory External Group Mapping does not support the same group name for different domains of the same name.

Security Fixes

Administration Fixes

Tracking Number	Description
ASOC-112493	Capture Policy deployment fails, when you try to create a new Capture Policy in **Configure** > **Capture Policies**. As a result, the status is displayed as **Failed** under **Publication Status** and **Service Assignment**.
ASOC-112805	Administrators are not permitted to download **Events** or **Jobs** created by other users in **Admin**>**System**>**Jobs**.

Context Hub Fixes

Tracking Number	Description
ASOC-112636	While configuring a STIX custom feed in **Config** > **Custom Feeds** > **Feeds**, Sightings data (*sightings_count=1* in the STIX xml file) such as Sources, Timestamps, Confidence, and References are not available under **Define Columns** preview.

Log Collection Fixes

Tracking Number	Description
ASOC-112547	When you add more than 50 Remote Destination Log Collectors under **Local Collectors** > **Destination Groups** in the **Config** window, pagination does not work. As a result, Destination Log Collectors above 50 are not displayed on the UI.

Endpoint Fixes

Tracking Number	Description
ASOC-112285	After downloading a file (present across different Endpoint servers) in one of the Endpoint servers, when you try to save a local copy of it from any other Endpoint server (where it was not downloaded), an error message **Download failed. Check the audit logs for more details.** is displayed. The download status of the file is changed from **Downloaded** to **File Deleted on server**.

Respond Fixes

Tracking Number	Description
ASOC-111459	When you edit any incident rule in **Configure** > **Incident Rules** page and save the changes, after sometime these changes are reverted. Consequently, incidents associated with these incident rules are not created with the new changes.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness 11.x Master Table of Contents	https://community.rsa.com/t5/netwitness-platform-online/rsa-netwitness-platform-11-x-master-table-of-contents/ta-p/567788
NetWitness 11.7 Product Documentation	https://community.rsa.com/t5/netwitness-platform/ct-p/netwitness-documentation
NetWitness 11.7 Upgrade Guide	https://community.rsa.com/t5/netwitness-platform-online/upgrade-to-netwitness-platform-11-7/ta-p/655210

Feedback on Product Documentation

You can send an email to nwdocsfeedback@rsa.com to provide feedback on NetWitness 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.rsa.com/community/products/netwitness/documentation

- Use the **Search** field in RSA Link to find specific information here: https://community.rsa.com/

- See the NetWitness Knowledge Base:
  https://community.rsa.com/community/products/netwitness/knowledge-base

- See Troubleshooting the NetWitness:
  https://community.rsa.com/community/products/netwitness/documentation/troubleshooting

- See also NetWitness 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 **Support > Case Portal > Manage My Cases**.
International Contacts (How to Contact RSA Support)	https://community.rsa.com/t5 https://community.rsa.com/t5/support-information/how-to-contact-rsa-support/ta-p/563897-information/how-to-contact-rsa-support/ta-p/563897
Community	https://community.rsa.com/t5/rsa-Community/ct-p/support

Build Numbers

The following table lists the build numbers for various components of NetWitness 11.7.0.0.

Component	Version Number
NetWitness Audit Plugins	rsa-audit-plugins-11.7.0.0-4695.5.36a93c8d9.el7.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Broker	rsa-nw-broker-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Concentrator	rsa-nw-concentrator-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-11.7.0.0-2109091739.5.be0ffac.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-11.7.0.0-210908042413.5.a52e0dc.el7.centos.noarch.rpm
NetWitness Console	rsa-nw-console-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Content Server	rsa-nw-content-server-11.7.0.0-210906060842.5.022d0d1.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-11.7.0.0-210908050143.5.589ec75.el7.centos.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-11.7.0.0-210914062311.5.730e55a.el7.centos.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-11.7.0.0-2105111629.5.286995c.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-11.7.0.0-2109081645.5.da02ba9.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-11.7.0.0-210928085116.5.ad9d4df.el7.centos.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-11.7.0.0-210908061251.5.fc23872.el7.centos.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-11.7.0.0-210908043046.5.db06a9d.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-11.7.0.0-210908094032.5.dd152ed.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-11.7.0.0-210909082049.5.751fea3.el7.centos.noarch.rpm

NetWitness License Server	rsa-nw-license-server-11.7.0.0-210908100642.5.3aee2de.el7.centos.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-11.7.0.0-14991.5.3a09b7b7d.el7.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-11.7.0.0-210830055027.5.a674232.el7.centos.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-11.7.0.0-210907081327.5.411da23.el7.centos.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-cli-11.7.0.0-2107281202.5.da1fa1d.el7.noarch.rpm
NetWitness Recovery Tools	rsa-nw-recovery-tool-11.7.0.0-2109201121.5.407f9ac.el7.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-11.7.0.0-5903.5.a09535ea0.el7.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-11.7.0.0-210914062602.5.b62650d.el7.centos.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-11.7.0.0-2105111632.5.7e09f04.el7.noarch.rpm
NetWitness SDK	
NetWitness Security Server	rsa-nw-security-server-11.7.0.0-210816032325.5.c946840.el7.centos.noarch.rpm
NetWitness Source Server	rsa-nw-source-server-11.7.0.0-210906022225.5.12e033b.el7.centos.noarch.rpm
NetWitness User Interface	rsa-nw-ui-11.7.0.0-210907091711.5.65a67f4557.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness SA Tools	rsa-sa-tools-11.7.0.0-2109140601.5.680134e.el7.noarch.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-11.7.0.0-4695.5.36a93c8d9.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-11.7.0.0-4695.5.36a93c8d9.el7.x86_64.rpm

Revision History

Date	Description
November 2021	Release to Operations