NetWitness® Platform XDR

Version 12.1.1.0

Release Notes

NETWITNESS

Platform XDR

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 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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

January 2023

Contents

What's New

The NetWitness 12.1.1.0 Release Notes describe new features, enhancements, security fixes, upgrade paths, fixed issues, known issues, end-of-life functionality, build numbers, and self-help resources.

Enhancement: Policy-based Centralized Content Management (CCM)

The following enhancements are made for Policy-based Centralized Content Management in 12.1.1.0 version.

- Administrator can clone Application Rules and Network Rules with a unique rule name and same rule value.

> **IMPORTANT:**
> - The **Rule Name** is the unique title of the rule, which is used as a reference to the rule within the Content Library.
> - The **Rule Value** is a string or text which is registered to a meta key when the rule is triggered with an "alert" output. It may be the same as the rule name, but it is not unique within the Content Library.
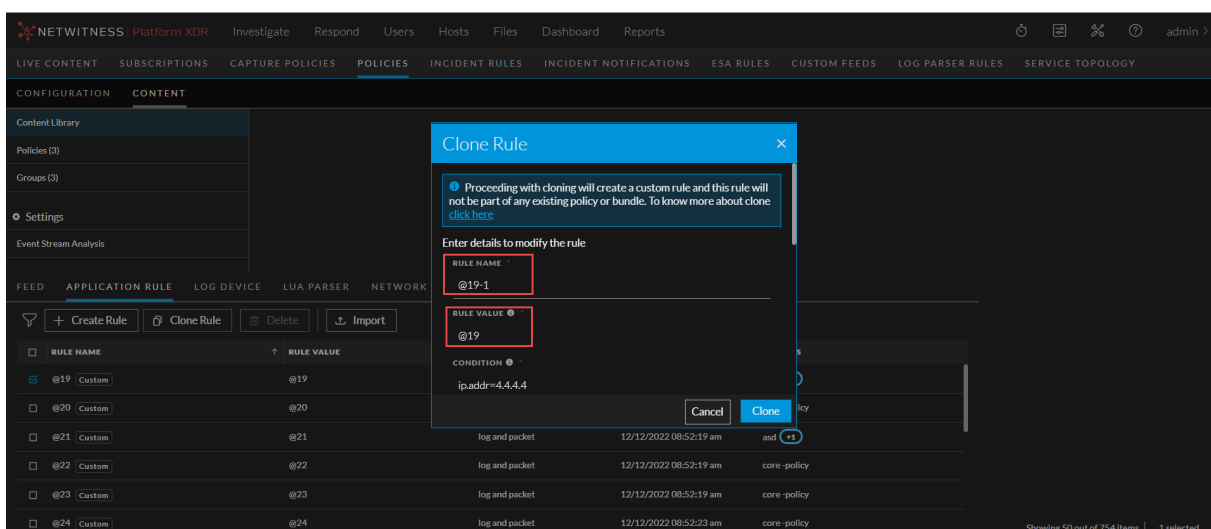

- Single CCM toggle is introduced to enable or disable CCM for all 12.0+ Decoders and Log Decoders at once. The toggle button is available via backend of source-server.

- When you upgrade a Decoder or Log Decoder from 11.x, 12.0 or 12.1 version to 12.1.1 version, a backup of all the content is created automatically. Backup file will be available on Core Services' host under the following path:

  ○ For Log Decoder - `/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar`

  ○ For Network Decoder - `/var/netwitness/decoder/decoder_backupcontent_ccm.tar`

- In 12.1 and later versions, you can only manage the ESA deployments and Data Sources through **Centralized Content Management**.

  Go to ▣ (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** page to manage the ESA deployments and Data Sources.

  Refer the following screenshot.
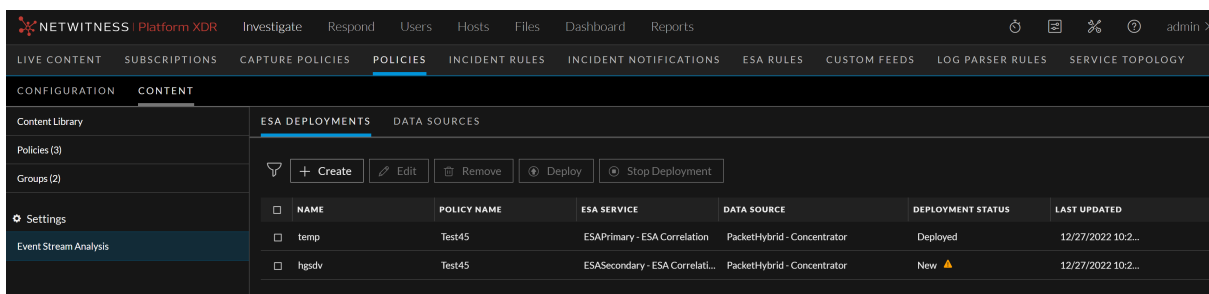
- A new unified deployment view **(ESA DEPLOYMENTS)** tab is created to manage deployments from a single view across all policies within CCM.
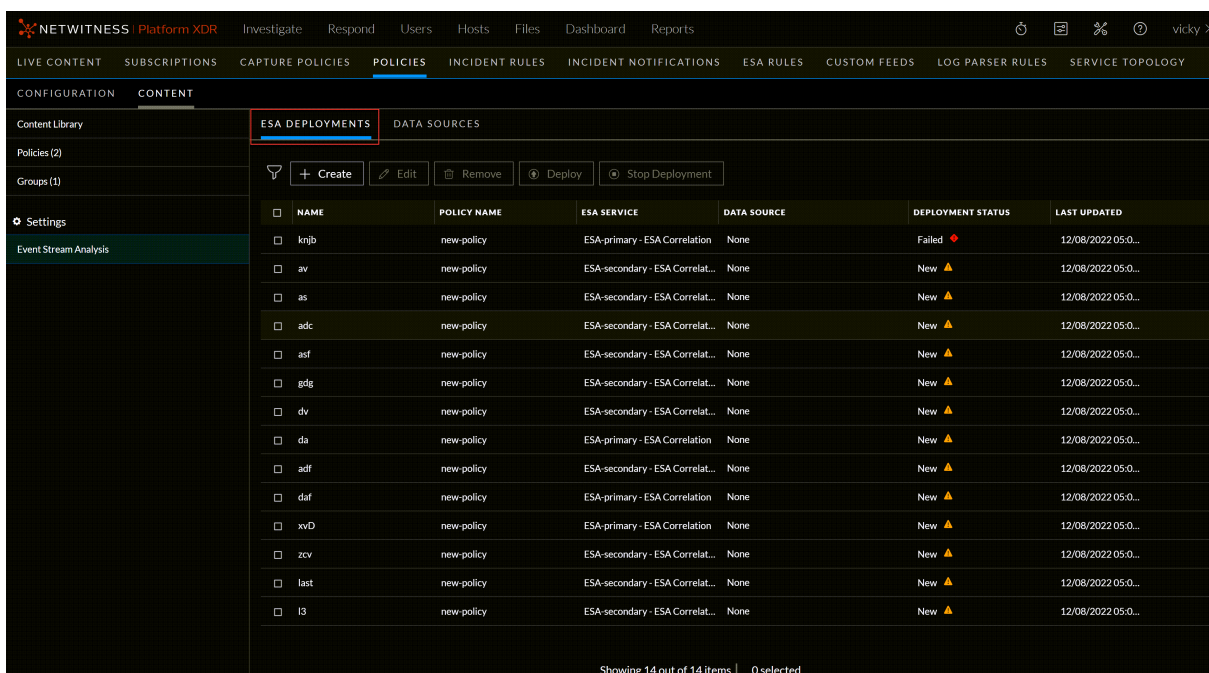
- Navigation is made simple to edit policy wizard from the **Edit deployment** view > **View rules**.

  ○ The edit deployment screen will save the current state and close. The user will be redirected to the **edit policy** wizard on the new tab.

- A new search option is created from the listed ESA rules in the **View ESA rules** modal in the edit and create deployment views.

- Caution banners are created to convey the customer about the requirement of a deployment while creating ESA related policies.

- After upgrading to 12.1 and later versions, you can only manage the ESA Rules in the **ESA Rules** page. Refer the following screenshot.
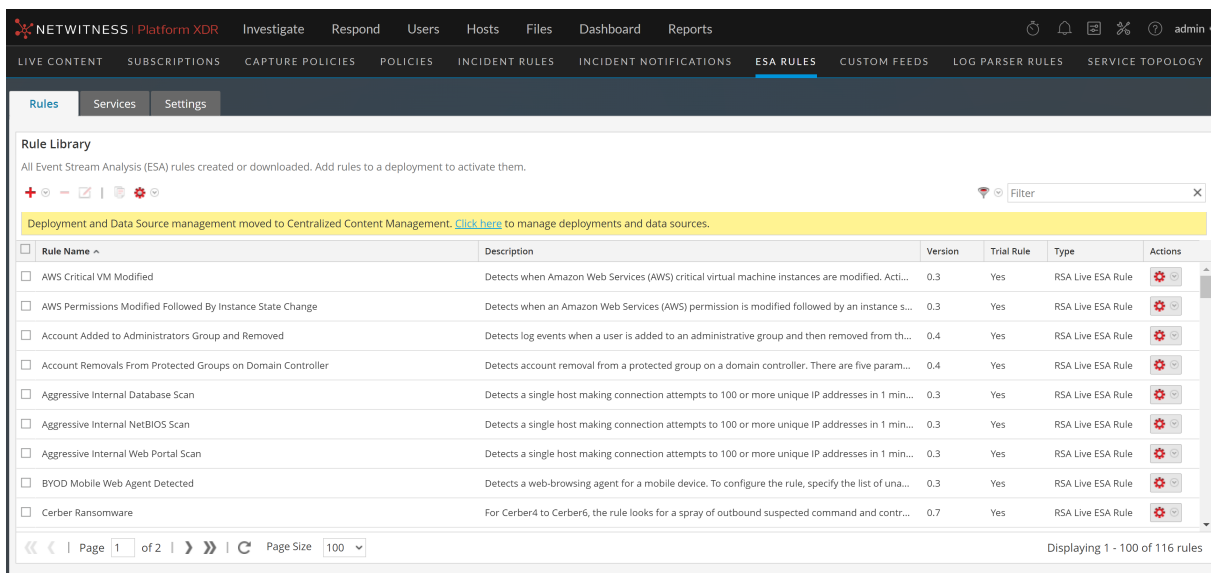
- After upgrading to the 12.1.1.0 version, all the ESA deployments will be migrated to ▣ (**CONFIGURE**) > **Policies** page. Each deployment will be converted into a policy and group and will be available to manage only after the upgrade of the Correlation servers to the 12.1.x.x version. Make sure that you plan the upgrade process so that Correlation servers are upgraded immediately after the Admin Server is done. The deployments will not be accessible until the corresponding Correlation servers are upgraded. However, the correlation servers will still continue to process the Alerts and Events.

- You must upgrade the ESA hosts immediately after upgrading the Admin Server.

  For more information on **Centralized Content Management** and managing the deployments, see Centralized Management Guide for 12.1.1.

Security Fixes

The following ciphers in the NetWitness Platform XDR are disabled and removed.

- DHE-RSA-AES128-SHA

- DHE-RSA-AES256-SHA

- ECDHE-RSA-AES128-SHA

- ECDHE-RSA-AES256-SHA

- DHE-RSA-AES128-SHA256

- DHE-RSA-AES256-SHA256

- ECDHE-RSA-AES128-SHA256

- ECDHE-RSA-AES256-SHA384

- RSA-AES128-SHA256

- RSA-AES128-SHA256(AES-GCM)

- RSA-AES256-SHA384

- AES128-SHA

- AES256-SHA

- RSA-AES128-SHA256(AES-CBC)

- RSA-AES256-SHA256

> **IMPORTANT:** If the communication between the external integrated devices and the NetWitness Platform XDR is interrupted, you must disable the use of the above ciphers on the external integrated devices.

> **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 12.1.1.0 patch upgrade. In this case, 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 and install the updated plugins, see Post-Upgrade Tasks.
> - 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 12.1.1.0 patch upgrade.

For more information on the various vulnerabilities fixed in this release, see https://community.netwitness.com/t5/netwitness-platform-product/nw-2023-01-multiple-components-within-netwitness-platform/ta-p/694185.

Upgrade Paths

The following upgrade paths are supported for NetWitness 12.1.1.0:

- NetWitness 11.6.x.x to 12.1.1.0

- NetWitness 11.7.x.x to 12.1.1.0

- NetWitness 12.0.x.0 to 12.1.1.0

- NetWitness 12.1.0.0 to 12.1.1.0

- NetWitness 12.1.0.1 to 12.1.1.0

Product Version Life Cycle for NetWitness Platform

For information about versions that reach End of Primary Support (EOPS), see Product Version Life Cycle for NetWitness Platform XDR.

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 (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) on NetWitness Community Portal

SMS Fixes

Tracking Number	Description
ASOC-124645	After upgrading or installing 11.6, 11.6.1 and 11.7 versions, the logs are not written to sms.log and instead written to wrapper.log. This is because multiple libraries were updated in these versions. In 12.1.1 version, the logs are written to sms.log file.

Endpoint Fixes

Tracking Number	Description
ASOC-127217	Process Tree is not displayed in the **Respond** Service for high and critical Endpoint alerts (**Host**> **Event Details** > **View alert Details**). This issue occurs when the session ID of the event exceeds the integer limit of 32 bits. As a result, you cannot investigate the events.
ASOC-125221	The **Cancel** and **Reset** options in the **Reset Risk Score** window (**Files** > **select a file** > **More Actions** > **Reset Risk Score**) cannot be accessed. As a result, you can neither cancel the Risk score reset operation nor you can reset the Risk score of the selected file.

CCM Fixes

Tracking Number	Description
ASOC-125896	Automatic rule name assignment for clone rule is getting wrong value after filtering. When you clone a rule after filtering, the rule name is assigned according to the filtered list. Hence, the error occurs while validating the rule name. In 12.1.1 version, the rule name is assigned according to the content present in the Content Library.
ASOC-125838	Alert meta are not populating while editing Application or Network Rules for the first time. But, the alert meta are populating after creating a rule. The issue occurs as the API was being called only for creating the rule. In 12.1.1 version, API is called for both creating and editing the rule.
ASOC-125810	Explicit message is not displayed on deletion of content when the first policy is published to a service. In 12.1.1 version, the warning message is displayed to the user.
ASOC-125808	No proper visual notification in the Live content UI regarding the services managed by CCM. In 12.1.1 version, there is a notification banner added in the **Live** page, **Subscription** page and **Content Deployment** wizard with a CCM link. The link will redirect the user to **CCM** page.
ASOC-125258	The user cannot remove or toggle off Log Decoder from central policy. THe issue occurs due to the settings in the NTP server and Global audit log server. In 12.1.1 version, the user is able to remove or toggle off Log Decoder with the settings.
ASOC-125321	When the user filters the policy using **Unpublished** filter and then publishes the policy and removes the **Unpublished** filter, the policy status changes to **In-progress** state. The issue occurs due to state calculation. In 12.1.1 version, the state calculation is done even after filtering the policy. Hence, the issue is fixed.
ASOC-125530	Error while importing zip file in Log Devices. The issue occurs due to zip file structure. In 12.1.1 version, the user is able to import or deploy all content without any issues.
ASOC-125735	Importing content with same zip file name does not display correct error message. The issue occurs when the recent file name does not get validated if the file names are same and importing happens in the same session. In 12.1.1 version, correct number of error messages are displayed for any Log Device .zip file with duplicate contents since the recent file is also validated even if the names are same.

Tracking Number	Description
ASOC-124473	Source-server cannot load up the basic meta information when it is unable to connect to Live. The issue occurs when the source-server cannot connect to Live CMS, event though the Live is configured. As a result, the source-server cannot fetch the content-related information such as resource types and mediums on the first start up and the user cannot view the Content Library and the migrated policy details information. From 12.1.1 onwards, the user can download or deploy content from CCM when: • HTTP proxy configured with SSL disabled, Localhost DNS disabled • HTTP proxy configured with SSL disabled, Localhost DNS enabled • HTTP proxy configured with SSL enabled, localhost DNS disabled • HTTP proxy configured with SSL enabled, Localhost DNS enabled • HTTP proxy not configured, Localhost DNS enabled
ASOC-124429	In Content Library, custom content tag is not visible in light theme. This issue occurs due to light theme color issue. In 12.1.1 version, the light theme color is changed to make the custom content visible in light theme.
ASOC-124423	Content deployment fails for all the Live contents from Legacy Live content UI and CCM. In 12.1.1 version, a KB article is created and published which provides detailed steps on the resolution. For details on the KB article, click here.
ASOC-124402	The user is able to upload duplicate Log Device contents in the zip file without selecting the **Overwrite** option. The issue occurs since the duplicate content is not validated inside zip. In 12.1.1 version, the duplicate content inside zip is validated before it is uploaded.

Known Issues

For information on known issues, see NetWitness® Platform Known Issues list (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872).

End of Life Functionality

The following table provides information on end of life functionality, features and hardware in NetWitness 12.1.1.0 or later releases.

End of Life Functionality and Features in 12.1.1.0

Feature	Notes
ECAT Integration	In 12.0 and later versions, the ECAT Integration such as the RSA Endpoint (ECAT Data Sources) in the ContextHub Server is not supported by NetWitness Platform XDR. Before you upgrade from 11.7 and older versions to 12.0, 12.1, and 12.1.x.x versions, you must manually delete the RSA Endpoint (ECAT Data Sources) from the Context Hub Server . For more information, see the *12.1.1 Upgrade Guide for NetWitness Platform XDR*. **IMPORTANT:** RSA Endpoint is the ECAT Data Source used in the ContextHub Server and not the Endpoint Agent.

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness Platform XDR All Versions Documents	https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246
NetWitness Platform XDR 12.1 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform XDR 12.1.1 Upgrade Guide	https://community.netwitness.com/t5/netwitness-platform-online/upgrade-guide-for-12-1/ta-p/687965

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 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 NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW Update	https://update.netwitness.com
LiveUI	https://live.netwitness.com

Build Numbers

The following table lists the build numbers for various components of NetWitness 12.1.1.0.

Component	Version Number
NetWitness Admin Server	rsa-nw-admin-server-12.1.1.0-221205030723.5.a0a61ec.el7.centos.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Appliance Nonfips	rsa-nw-appliance-nonfips-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Audit Plugins	rsa-audit-plugins-12.1.1.0-4808.5.3953722a3.el7.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.1.1.0-4808.5.3953722a3.el7.x86_64.rpm
NetWitness Bootstrap	rsa-nw-bootstrap-12.1.1.0-2211211034.5.74485a3.el7.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Broker Nonfips	rsa-nw-broker-nonfips-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.1.1.0-2732.5.f57309d89.el7.x86_64.rpm
NetWitness Collectd	rsa-collectd-12.1.1.0-4808.5.3953722a3.el7.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.1.1.0-4808.5.3953722a3.el7.x86_64.rpm
NetWitness Cloud Connector Server	rsa-nw-cloud-connector-server-12.1.1.0-221201125530.5.4ce9d94.el7.centos.noarch.rpm
NetWitness Cloud Link Server	rsa-nw-cloud-link-server-12.1.1.0-230102014709.5.8088477.el7.centos.noarch.rpm
NetWitness Component Descriptor	rsa-nw-component-descriptor-12.1.1.0-2301090955.5.6f26ac5.el7.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Concentrator Nonfips	rsa-nw-concentrator-nonfips-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.1.1.0-2301050846.5.2426ef3.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-12.0.0.0-220531042629.5.b236ead.el7.centos.noarch.rpm
NetWitness Console	rsa-nw-console-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm

NetWitness Content Server	rsa-nw-content-server-12.1.1.0-221205032018.5.718f599.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-12.1.1.0-221202103000.5.f8fc365.el7.centos.noarch.rpm
NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.1.1.0-230109030938.5.57800a8.el7.centos.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Decoder Nonfips	rsa-nw-decoder-nonfips-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Decoder Content	rsa-nw-decodercontent-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-12.1.1.0-2211211037.5.587bcea.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-12.1.1.0-2301052015.5.8455277.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-12.1.1.0-230103012037.5.b500311.el7.centos.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-12.1.1.0-230117100203.5.45d088c.el7.centos.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.1.1.0-221209044723.5.2ae8391.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-12.1.1.0-221206034843.5.23a7fe8.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-12.1.1.0-230102110937.5.5e62d94.el7.centos.noarch.rpm
NetWitness License Server	rsa-nw-license-server-12.1.1.0-221205035951.5.d045cfa.el7.centos.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.1.1.0-15044.5.12b44204e.el7.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.1.1.0-15044.5.12b44204e.el7.x86_64.rpm
NetWitness Log Collector Tools	rsa-nw-logcollector-tools-12.1.1.0-15044.5.12b44204e.el7.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.1.1.0-12608.5.fdd27c6f2.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-12.1.1.0-221212100621.5.93aa5c3.el7.centos.x86_64.rpm

NetWitness Metrics Server	rsa-nw-metrics-server-12.1.1.0-221206042657.5.925045d.el7.centos.noarch.rpm
NetWitness Orchestration CLI	rsa-nw-orchestration-cli-12.1.1.0-2212060924.5.6a3f991.el7.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-server-12.1.1.0-221202063703.5.5af5235.el7.centos.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.1.1.0-2301020953.5.55358f0.el7.noarch.rpm
NetWitness Presidio Config Server	rsa-nw-presidio-configserver-12.1.1.0-2301020953.5.55358f0.el7.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.1.1.0-2301020953.5.55358f0.el7.noarch.rpm
NetWitness Presidio Elastic Search Init	rsa-nw-presidio-elasticsearch-init-12.1.1.0-2301020953.5.55358f0.el7.noarch.rpm
NetWitness Presidio Ext	rsa-nw-presidio-ext-netwitness-12.1.1.0-2301021008.5.870b8fb.el7.noarch.rpm
NetWitness Presidio Flume	rsa-nw-presidio-flume-12.1.1.0-2301021006.5.9ae9356.el7.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.1.1.0-2301020953.5.55358f0.el7.noarch.rpm
NetWitness Presidio Output	rsa-nw-presidio-output-12.1.1.0-2301020953.5.55358f0.el7.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-12.1.1.0-2301021010.5.1f8d431.el7.noarch.rpm
NetWitness Recovery Tools	rsa-nw-recovery-tool-12.1.1.0-2301020759.5.84e1f73.el7.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-12.1.1.0-5957.5.c4a512515.el7.x86_64.rpm
NetWitness Relay Server	rsa-nw-relay-server-12.1.1.0-230103011944.5.c19c2f6.el7.centos.noarch.rpm
NetWitness Respond Server	rsa-nw-respond-server-12.1.1.0-230117075903.5.9b085ac.el7.centos.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-12.1.1.0-2212121755.5.eed8093.el7.noarch.rpm
NetWitness SA Tools	rsa-sa-tools-12.1.1.0-2301020753.5.992cdd4.el7.noarch.rpm
NetWitness Security CLI	rsa-nw-security-cli-12.1.1.0-2212150738.5.2763b08.el7.noarch.rpm
NetWitness Security Server	rsa-nw-security-server-12.1.1.0-221220012824.5.19db193.el7.centos.noarch.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-12.1.1.0-4808.5.3953722a3.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.1.1.0-4810.5.4a36b38ae.el7.x86_64.rpm

NetWitness Source Server	rsa-nw-source-server-12.1.1.0-230102064618.5.42ea9ed.el7.centos.noarch.rpm
NetWitness User Interface	rsa-nw-ui-12.1.1.0-230103094425.5.43aebff0c3.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.1.1.0-12601.5.20a1c0b68.el7.x86_64.rpm

Revision History

Date	Description
January 2023	Release for GA