# NetWitness Platform Known Issues

To find out if any known issue is fixed, refer to the Fixed Issues section in the Release Notes for the appropriate release.

| Components | Title, Problem and Workaround | Found In / Exists In | Fixed Version | Tracking Number |
|---|---|---|---|---|
| Context Hub | **Title:** Custom Feeds may enter a failed state after a restore operation during the S6 to S7 data migration.<br><br>**Problem:** This issue occurs because some files were not restored correctly during the data migration process for Custom Feeds, leading to the following functional loss impact on the end users:<br>Recurring Custom Feeds will stop working and remain failed.<br>Unable to edit the existing Custom Feeds (AdHoc and Recurring feeds).<br>Unable to push AdHoc Custom Feeds to the new/different decoder service.<br><br>**Workaround:** Perform the following steps:<br>1. Extract tar.gz file and move missing .xml and .csv files manually on AdminServer Host,<br>a. from backup<br>location: /var/netwitness/<backup_folder>/files/var/lib/netwitness/uax.tgz/uax.tar/./uax/backup/custom-feeds.tar.gz/custom-feeds.tar/var/lib/netwitness/uax/<custom_feed_uuid><br>b. to /var/lib/netwitness/uax/scheduler/<custom_feed_uuid><br>2. Run service jetty restart on AdminServer Host<br>3. Run service rsa-nw-contexthub-server restart on ESAprimary Host<br>4. Refresh Configure → Custom Feeds page. | 12.5.1 | | SADOC S-2580 |
| Endpoint | **Title:** Agent installation time is less than command creation time<br><br>**Problem:** When initiating an upgrade via the UI, an error message stating “Agent install time is less than the command time” is displayed. This error typically occurs during agent upgrades through the UI, even though the upgrade completes successfully. The issue causes the command to be marked as expired with the agent install time being less than the command creation time.<br><br>**Workaround:**<br>This issue may or may not occur. If the agent upgrade does not succeed, the user must manually upgrade the agent. | 12.5.1 | | ASOC-151558 |

| | | | | |
|---|---|---|---|---|
| Endpoint | **Title:** Cannot run offline standalone scan on an air-gapped Linux machine<br><br>**Problem:** When attempting to run the standalone scan, an error was encountered stating "Couldn't get scan progress message," possibly due to a problem with the standalone scan functionality in this version.<br><br>**Workaround:** There is no workaround. The agent must be connected to a network to communicate with the server. | 12.5.1 | | ASOC- 158518 |
| Endpoint | **Title:** Incorrect display of tags count<br><br>**Problem:** The tag count is not displaying correctly, even though the tags are being assigned as expected.<br><br>**Workaround:** Currently, there's no workaround. However, there is no functional impact, and the system will perform similar as before. | 12.5.1 | | ASOC-158576 |
| Home Page Widgets | **Title:** Multiple Delete and Reset confirmation modals are displayed at the same time when the user tries to delete or reset the widgets in Edit Layout mode.<br><br>**Problem:** In Edit Layout mode, the following issues occur:<br>When a user attempts to delete a widget and then cancels the action, trying to delete another widget causes two confirmation modals to appear.<br>Similarly, if the user tries to reset the layout, both the reset and delete confirmation modals appear at the same time.<br>This issue occurs because the cancel state is not cleared in the UI.<br><br>**Workaround:** To fix the issue, the user needs to perform one of the following actions:<br>While in Edit Layout mode on the Home page, click the Cancel button.<br>Refresh the Home page. | 12.5.1 | | ASOC-157893 |
| Home Page Widgets | **Title:** NetWitness Hosts/Devices widget fails to update host status due to a cache refresh issue.<br><br>**Problem:** When a new host is added or an existing host goes offline, the NetWitness Hosts/Devices widget does not update to reflect the new status or show the newly added host. This issue occurs because the cache does not refresh automatically.<br><br>**Workaround:** To resolve the issue, perform the following steps:<br>1. Go to<br>(Admin) > Services page.<br>2. In the Services list, select the Admin Server service.<br>3. Click<br>> Restart.<br>4. A dialog requests confirmation. To restart the service, click Yes. | 12.5.1 | | ASOC- 158458 |

| | | | | |
|---|---|---|---|---|
| UEBA | **Title:** Incorrect display of None Feedback option in the Users > Alerts > Filters panel.<br><br>**Problem:** The Feedback option for None is incorrectly displayed in the Filters panel on the Users > Alerts page. Currently, it shows as Missing Translation "investigateUsers.feedback.none" for locale "en-us".<br>**Note:** This issue does not impact the functionality of UEBA. The filter functionality is working properly and on selecting this option, the corresponding alerts are displayed correctly.<br><br>**Workaround:** None | 12.5.1 | | ASOC-158455 |
| UEBA | **Title:** A high volume of Non-Standard Activity alerts generated on the Users > Alerts page after the UEBA upgrade.<br><br>**Problem:** After upgrading UEBA to versions 12.5 or 12.5.1, a high volume of Non-Standard Activity alerts is generated on the Users > Alerts page for the Abnormal Activity for JA4 indicator, typically within the first two days. This issue occurs because new UEBA models introduced in version 12.5 require time to learn user behavior patterns. During this initial learning phase, the system may temporarily misclassify normal activities as anomalies, leading to an increase in alerts.<br><br>**Important:** This learning period will be completed within two to three days, and the UEBA models will be updated. As a result, you will not see such high number of alerts.<br><br>**Note:** This issue occurs only in environments with the TLS schema enabled and does not affect the UEBA functionality.<br><br>**Workaround:** None | 12.5 and later versions | | ASOC-158458 |
| Endpoint | **Title:** Cannot run offline standalone scan on an air-gapped Linux machine<br><br>**Problem:** When attempting to run the standalone scan, an error was encountered stating "Couldn't get scan progress message," possibly due to a problem with the standalone scan functionality in this version.<br><br>**Workaround:** There is no workaround. The agent must be connected to a network to communicate with the server. | 12.5 | | ASOC-158518 |

| | | | | |
|---|---|---|---|---|
| UEBA | **Title:** Users have encountered a persistent issue with the presidio configserver while upgrading the NetWitness UEBA server from the older versions to 12.5.<br><br>**Problem:** From 12.5, UEBA no longer uses the presidio config server for communication. Instead, uses a new service called UEBA-server. The presidio configserver service keeps restarting and the service file references to a non-existent jar file.<br><br>For more information, refer to the following figure displaying the activating error log.<br>  <br>  <br>**Note:** This issue does not impact the functionality of UEBA.<br><br>**Workaround:**<br>To resolve the issue, perform the following steps:<br>1. SSH to the UEBA server.<br>2. Run the following commands to stop and disable the presidio-configserver service:<br>systemctl stop presidio-configserver<br>systemctl disable presidio-configserver | 12.5 | 12.5.1 | ASOC-158028 |
| Admin Server | **Title:** Users are unable to log in to NetWitness using AD and AD SSO with Primary Group Mapping.<br><br>**Problem:** NetWitness login failures occur for users whose primary Active Directory (AD) group is mapped to any NetWitness external group. This issue affects both AD login and AD Single Sign-On (SSO) authentication methods. For example, if a user's primary AD group is Test123 and they are assigned the Administrator role within that group in NetWitness, login attempts fail. However, users with the same group as a secondary AD group can log in successfully.<br><br>**Workaround:**<br>As a temporary solution for this issue, users can change their primary group in Active Directory (e.g. Test123) to a secondary group, allowing users to log in using this group. | 12.5 | 12.5.1 | ASOC-154386 |
| Core | **Title:** raidNew fails when using preferSecure=1 to configured PVs with SEDs.<br><br>**Problem:** When configuring raid on a Series 7 appliance with attached PowerVault and encryption Key set on the raid controller, raidNew is executed with preferSecure=1 parameter. The raidNew command execution fails with preferSecure=1.<br><br>**Workaround:** Use preferSecure=0 when creating raid using raidNew and complete the storage configuration. Use encryptSedVd.py script to enable encryption post storage configuration. *Refer to Appendix B. Encrypt a Series 6E or Series 7 Core or Hybrid Host (encryptSedVd.py).* | 12.4.2 and 12.5 | 12.5.1 | ASOC-157333 |

| | | | | |
|---|---|---|---|---|
| UEBA | **Title:** Unable to add a large number of entities to the watchlist on the Users > Entities page due to size limit.<br><br>**Problem:** When you try to add all entities to the watchlist from the Users > Entities page using the Add All To Watchlist button, the system fails to add them if the environment contains an exceptionally high number of entities. The issue occurs due to exceeding the payload size limit when processing a very high number of entities.<br>**Note:** Adding individual users to the watchlist remains unaffected by this issue. To add a user, navigate to the Users page, select a username, and then click Watch Profile in the user's profile view.<br><br>**Workaround:** None | 12.5 | 12.5.1 | ASOC- 156298 |
| Home Page Widgets | **Title:** Unable to view the Mitre ATT&CK Overview widget data in the Analyst UI after a fresh installation of the 12.5 version.<br><br>**Problem:** The Mitre ATT&CK Overview widget displays a "Widget Data Retrieve Error" upon logging into the Analyst UI. This issue occurs due to the absence of the mitre-explorer-content.js file in the Analyst node.<br><br>**Workaround:**<br>To resolve this issue, perform the following steps:<br>1.SSH to the Admin Server.<br>2. Copy this file /var/netwitness/common/repo/mitre-data/mitre-explorer-content.js from the admin node to the analyst node.<br>3. After the file is copied to the same location on the analyst node, all data for the Mitre ATT&CK Overview widget will load without any errors. | 12.5 and later versions | | ASOC-157114 |
| Home Page Widgets | **Title:** An unhandled exception error occurs in the Resource Usage per Content Type widget when switching to an offline device. This error persists even after the device is reconnected or switched to another online device.<br><br>**Problem:** The Resource Usage per Content Type widget within the Admin view of the Home page displays an unhandled exception error when an offline device is selected from the drop-down list. This issue continues to occur even after the device is back online or switched to another online device.<br><br>**Workaround:** Refresh the Home page to view the data for the selected device. | 12.5 and later versions | | ASOC-152916 |
| Home Page Widgets | **Title:** Home page widgets display an additional day on the x-axis usage trend due to UTC time zone mismatch.<br><br>**Problem:** A few of the widgets on the Home page are displaying an extra day at the beginning of the usage trend on the x-axis graph. This is because the widgets are using UTC time instead of the time zone specified in the user's preferences panel.<br><br>**Workaround:** Currently, there is no workaround. However, there is no functional impact on the widgets. | 12.5 and later versions | | ASOC-154383 |

| | | | | |
|---|---|---|---|---|
| Platform | **Title:** Bubblewrap and Flatpak security update<br><br>**Problem:** CVE-2024-42472 is getting reported in Bubblewrap version installed in Netwitness.<br><br>**Workaround:** None<br>The sandbox escape vulnerability in Flatpak is not applicable to NetWitness, as the Flatpak library is not installed in the environment. Therefore, the bubblewrap update aimed at addressing this vulnerability does not impact the system and will not influence the security. | 12.5 and earlier versions | | |
| UEBA | **Title:** Node.js Multiple Vulnerabilities for UEBA service<br><br>**Problem:** The version of Node.js installed on UEBA reports multiple vulnerabilities<br><br>**Workaround:** None<br><br>The NW Platform is not affected by the multiple security vulnerabilities related to Node.js. The vulnerable version of Node.js is installed as part of Kibana, but no vulnerable functions or activities are associated with it. | 12.5 and earlier versions | 12.5.1. 0 | |
| Reporting Engine | **Title:** Reporting Engine is down after fresh Installation of the NetWitness Platform 12.5<br><br>**Problem:** After Fresh Installation of the the NetWitness Platform 12.5, the Reporting Engine service attempts to restart continuously without success. The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted.<br><br>**Workaround:**<br>Follow the **Resolution** mentioned in the KB Article - **Reporting Engine restarts After upgrade to RSA NetWitness Platform 11.4 - NetWitness Community - 676705** | 12.5 and earlier versions | | ASOC-157136 |
| Endpoint | **Title:** All blocked hashes are showing source as Investigate after upgrade<br><br>**Problem:** After an upgrade, all the blocked hashes display "Investigate" as the source.<br>Unable to delete the import hashes using the UI. Filtering by source is also ineffective.<br><br>**Workaround:**<br>If the customer is on version 12.3 or higher and has imported blocked hashes into the deployment:<br>Before the Upgrade:<br>Navigate to the Blocked Hashes User Interface.<br>Filter the list by selecting "Import" as the source.<br>Delete all the listed entries.<br>After the upgrade, re-import the same set of checksums either via CSV or individually.<br>If the Upgrade has already been completed:<br>Connect to the context-hub collection on the ESA primary node.<br>Locate the ds_entries collection related to fileStatus.<br>Filter the checksums using the import comment or review them one by one.<br>(eg:<br>db.getCollection('ds_entries_65a0e7aa22f4dd07f02d3125').find({"data_lower.comment"<br>: " blocked files via import in 12.4.1"}))<br>Delete the relevant entries from the database.<br>Re-import the CSV file containing the blocked hashes through the UI. | 12.5 | 12.5.1 | ASOC-155882 |

| | | | | |
|---|---|---|---|---|
| Endpoint | **Title:** Event summary for agent last seen is displayed as N/A.<br><br>**Problem:** The event summary is not generated for offline agents last seen in the events list view on the Investigate > Events page. It appears as N/A.<br><br>**Workaround:** The summary is displayed in the Endpoint Event Details screen and will be displayed in the events list view on the Investigate > Events page in the upcoming release. | 12.5 | 12.5.1 | ASOC-154866 |
| Home Page Widgets | **Title:** The Default layout is not displayed automatically after the Reset<br><br>**Problem:** In the Manager, Admin and Analyst view, after you reset the layout in the landing page, the default layout is not automatically displayed.<br><br>**Workaround:** Refresh the page to view the default layout. | 12.5 | 12.5.1 | ASOC-154993 |
| Home Page Widgets | **Title:** Service Unavailable Error on the Home pages<br><br>**Problem:** In the Home tab, while trying to view the widgets, some of them may show as service unavailable or not configured even if the service is running in the Admin -> Services page.<br><br>**Workaround:** Verify If the hostname for admin-server is default admin-node IP and domain-name in url used, to access the NetWitness setup, is different than admin-node IP. Then update the domain-name in hostname. (To check Admin -> HOSTS -> select admin-server and edit) | 12.5 | 12.5.1 | ASOC-157181 |
| Warehouse Connector (WC) | **Title:** Incorrect Service Version number for Warehouse Connector in 12.5<br><br>**Problem:** The version of the Warehouse Connector (WC) displayed on the Admin > Services page and Warehouse Connector > System page is shown as 12.4 instead of 12.5.<br><br>**Workaround:** Currently, there's no workaround to rectify the version display discrepancy. However, there is no functional impact, and the system will perform similar as before. | 12.5 | 12.6 | ASOC-155376 |
| Log Collector | **Title:** The JDBC pipeline name with encrypted password of the DB are added under Logstash->Keystore management post service restart.<br><br>**Problem:** When creating JDBC pipelines, the user ID and password are automatically added under Logstash> Keystore management after the service is restarted.<br><br>**Workaround:** Currently, there's no workaround. However, there is no functional impact, and the system will perform similar as before. | 12.5 | 12.5.1 | ASOC- 155356 |

| | | | | |
|---|---|---|---|---|
| Respond | **Title:** Default Respond Syslog and Email Template does not work accurately for Created Incidents<br><br>**Problem:** When configuring Syslog or email notifications for incidents, the Default Respond Syslog or Email Template sends an notification that states UPDATED instead of CREATED, even for a new incident.<br><br>**Workaround:** Fixed in NetWitness 12.5.X. | 12.4.2 | 12.5.X | SACE-22219 |
| Platform | **Title:** Default almalinux repositories are not cleared as part of NetWitness upgrade<br><br>**Problem:** Upgrade to NetWitness 12.4.2.0 fails as it cannot reach the default alma repository (mirrors.almalinux.org or a mirror).<br><br>**Workaround:** Remove the default repos using rm -f /etc/yum.repos.d/almalinux*.repo and re-trigger the upgrade. | 12.4.2 | | SACE-21856<br>SACE-21878<br>ASOC-156451 |
| Admin Server | **Title:** Users on NetWitness 12.4 or later versions using Single Sign-On (SSO) and accessing Legacy UI pages encounter an error when attempting to log out.<br><br>**Problem:** When users log in through SSO and navigate to legacy UI pages (such as Admin or Reporting), they encounter an error when attempting to log out from these Legacy pages. This occurs when the Enable Global Logout option is disabled on the Admin > Security > Single Sign-On Settings page.<br><br>**Workaround:**<br>To resolve this issue, try one of the following steps:<br>1. Try turning on the Enable Global Logout option:<br>Go to Admin > Security > Single Sign-On Settings.<br>Enable the Enable Global Logout option.<br>Log out of the UI.<br>2. Access NetWitness Classic UI:<br>Go to the Classic UI pages (e.g., Investigate or Respond).<br>Log out of the UI.<br>In case these steps do not resolve the issue, it is recommended to contact NetWitness Customer Support as there is a hotfix available for this issue. | 12.4 and later versions | 12.5.1 | SACE- 21794 |
| Centralized Content Management | **Title:** Duplicate Application/Network Rules getting added to the policy following the service migration after upgrading to version 12.4.0.0 or above.<br><br>**Problem:** After upgrading to version 12.4.0.0 or above, if service contents are migrated, then assigned Policy may contain duplicate Application/Network rules. This may cause duplicate alerts to be generated.<br><br>**Workaround:** Remove duplicate rules from Policy which got updated with content migration and publish the policy. | 12.4 and later versions | | ASOC-148918 |

| | | | | |
|---|---|---|---|---|
| Endpoint | **Title:** Endpoint Respond Alert Workflow Error<br><br>**Problem:** When the alerts are generated from the Log Decoder, errors appear while attempting to analyze the process of an endpoint alert on the Respond page.<br>This issue is detected in NetWitness Platform 12.4.0 and later versions.<br><br>**Workaround:** Customers should continue to use Event Stream Analytics (ESA) rules to generate alerts instead of notifications within application rules. | 12.4.0 and later versions | | ASOC-150954 |
| Platform | **Title:** "No media devices detected" While deploying from rsa-nw-12.4.0.0.20806.iso from OVA.<br><br>**Problem:** Fails to detect Media (ISO) while running nwsetup-tui.<br><br>**Workaround:** On the host where failure is seen, Perform the following steps to update /usr/bin/bootstrap and usr/bin/nwsetup-tui<br>vi usr/bin/bootstrap<br>Update the following:<br>cp -a "$mountPoint/Packages/"* "$NW_REPO_LOCAL_BASE/" to cp -a "$mountPoint/Minimal/Packages/"* "$NW_REPO_LOCAL_BASE/"<br>local blockDeviceDetect=$(blkid \| grep '"OEMDRV"\|"CentOS 7 x86_64"') to local blockDeviceDetect=$(blkid \| grep '"OEMDRV"\|"AlmaLinux-8-9-x86_64-dvd"')<br>local blockDeviceCount=$(blkid \| grep -c '"OEMDRV"\|"CentOS 7 x86_64"') to local blockDeviceCount=$(blkid \| grep -c '"OEMDRV"\|"AlmaLinux-8-9-x86_64-dvd"')<br>elif [[ "${blockDeviceDetect}" == *"CentOS 7 x86_64"* ]]; then to elif [[ "${blockDeviceDetect}" == *"AlmaLinux-8-9-x86_64-dvd"* ]]; then<br>vi /usr/bin/nwsetup-tui<br>if [ "$(blkid \| grep -ci '"OEMDRV"\|"CentOS')" -gt 0 ]; then to if [ "$(blkid \| grep -ci '"OEMDRV"\|"Alma')" -gt 0 ]; then | 12.4 | 12.4.1 | SADOC S-2543 |
| Platform | **Title:** The network interface fails to start after rebooting the 12.4.0.0 host.<br><br>**Problem:** The host with the 12.4.0.0 version does not retain its IP after rebooting. This issue occurs because the NM_CONTROLLED parameter is set to no on the host.<br><br>**Workaround:**<br>To resolve the issue, you must update the NM_CONTROLLED parameter to yes on the host where the failure occurs. You can do this by following these steps:<br>1. vi /etc/sysconfig/network-scripts/ifcfg-<INTERFACE><br>For example, vi /etc/sysconfig/network-scripts/ifcfg-em1<br>2. Set the NM_CONTROLLED parameter to yes (NM_CONTROLLED=yes)<br>3. Restart the NetworkManager and network services by running the following command:<br>systemctl restart NetworkManager && systemctl restart network | 12.4 | 12.4.1 | ASOC-149880 |

| | | | | |
|---|---|---|---|---|
| Platform | **Title:** STIG disabled with all the control groups failed on all the node-x on 12.4.0.0.<br><br>**Problem:** When STIG is disabled with all the control groups, chronyd configuration parser misinterprets the line server <%= ntp_server %> iburst # maxpoll 10, incorrectly parsing maxpoll 10 as part of the server directive, causing chronyd service start failure.<br><br>**Workaround:** To resolve the issue, do the following:<br>1. SSH to the NW server.<br>2. Run the following command to update "# maxpoll" in the next line on all the nodes in the chrony.conf.erb file:<br>salt '*' cmd.run "sed -i 's/server <%= ntp_server %> iburst # maxpoll 10/server <%= ntp_server %> iburst\\n# maxpoll 10/' /var/netwitness/config-management/cookbooks/platform/nw-ntp/templates/default/chrony.conf.erb" | 12.4 | | SADOC S-2540 |
| Source Server | **Title:**Source-server Service Crashes Following Upgrade to Version 12.4.0.0<br><br>**Problem:** After upgrading to version 12.4, if custom LogDevices were uploaded by customers via the CCM-UI page in a previous 12.x version, the upgrade process will search for .xml and -custom.xml files. If any of these files do not adhere to a specific format, it will result in a crash of the source-server.<br><br>**Workaround:** The users have to recreate .envision file with the proper structure:<br>envision File Structure: /etc/devices/<LogDevice Name>/<LogDevice>.xml<br>For example: /etc/devices/accurev/accurevmsg.xml<br>Reference: **Import Content to Content Library** | 12.4 and 12.4.1 | | SACE-21327, ASOC-151331, ASOC-151326 |
| ESA Correlation Server | **Title:**Java Exceptions for Memory usage, CPU % in the legacy page, and computation values set to 0 in the Deployment stats page.<br><br>**Problem:** After the Deployment is successfully deployed, some of the ESA Rules containing annotations and Windows are throwing Java exception errors for memory and CPU usage in the ESA rules service or showing up blank in the new Deployment stats page. This does not affect performance or functionality of ESA, however rule performance stats collection does not work.<br><br>**Workaround:** None | 12.4 | | ASOC-148285 |

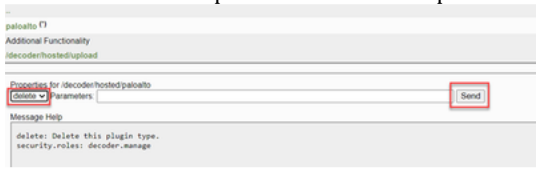
| | | | | |
|---|---|---|---|---|
| Admin Server | **Title:** Logs are not writing to /var/log/messages on all the nodes after the upgrade to 12.4.0.0.<br><br>**Problem:** After the upgrade to 12.4.0.0, /var/log/messages are empty and logs are not generating to "/var/log/messages".<br><br>**Workaround:** To resolve the issue, perform the following steps:<br>1. SSH to the NW Admin server.<br>2. Run the following three commands to update new configuration file of rsyslog that aligns to new log rotate call:<br>1. salt "*" cmd.run "sed -i 's@/bin/kill -HUP \`cat /var/run/syslogd.pid 2> /dev/null\` 2> /dev/null \|\| true@/usr/bin/systemctl -s HUP kill rsyslog.service >/dev/null 2>\&1 \|\| true@g' /var/netwitness/config-management/cookbooks/platform/rsa-audit/files/default/syslog.conf"<br><br>2. salt "*" cmd.run "chef-client -r "recipe[rsa-audit::config]" --config /var/lib/netwitness/config-management/client.rb --json-attributes /etc/netwitness/config-management/node.json"<br><br>3. salt "*" cmd.run "systemctl restart rsyslog"<br><br>3. Check if the log message file is available at the NW Admin server and hosts: /var/log/messages | 12.4 | | SACE- 21282, ASOC-150684 |
| Reporting Engine | **Title:** Duplicate Report emails are generated after the failback from the standby NW server to the primary NW server.<br><br>**Problem:** When a user performs failover or failback, the Reporting Engine service in the standby NW server is still online, executing reports and producing duplicate reporting emails or reports.<br><br>**Workaround:**<br>To resolve the issue, perform the following steps:<br><br>1. SSH to the Standby NW server.<br>2. Run the following command to stop the Reporting Engine service: systemctl stop rsasoc_re | 12.4 and earlier versions | | SACE- 20721, ASOC-147783 |
| Ember UI - Home Page | **Title** : Home Page is blank and visible as landing page option in 12.4<br><br>**Problem** : Under the user preference, in default landing page, there is a new option visible-"Home Page".<br>On selecting that option and relogging in, the user lands onto a blank page.<br><br>**Workaround:** Respective user can click on the User Preference option and change the default landing page to Springboard, Investigate etc. [except for home page] and then relog in. | 12.4 | 12.5 | ASOC-148336 |

| | | | | |
|---|---|---|---|---|
| Response Action | **Title:** Same keys can be entered multiple times in the Parameter Key field in Add Parameter window (<br>(CONFIGURE) > More > Response Actions ><br>> Create<br>Response Action ><br>)<br><br>**Problem:** You can enter the same keys multiple times in the Parameter Key field in Add Parameter window while creating Response Actions in (<br><br>(CONFIGURE) > More > Response Actions ><br>> Create Response Action. As a<br>result, the duplicate keys entered in the Parameter key field are sent to the connector after executing the Response Action.<br>**Workaround:** None. | 12.4 | | ASOC- 146230 |
| Endpoint | **Title:** Endpoint server upgrade failed during the upgrade from 12.3.1 to 12.4<br><br>**Problem:** During the upgrade from 12.3.1 to 12.4, the Endpoint Server upgrade failed since the relay server was enabled in the Endpoint server before configuring the IP, which gave a null value.<br><br>**Workaround:** The current workaround is to delete the relay configuration from monogdb. | 12.4 | | ASOC-146805 |
| UEBA | **Title:** Unable to view data on the Users page after upgrading to version 12.4.<br><br>**Problem:** When you upgrade the UEBA server to version 12.4 from lower versions, you may encounter an issue where red banner errors are displayed on the Users page. This issue occurs because presidio-ui fails to connect with presidio-output for fetching the data required to be displayed on the Users page.<br><br>**Workaround:**<br>To resolve this issue, perform the following steps:<br>1. SSH to the UEBA server.<br>2. Run the following commands to restart the presidio-output and presidio-ui services:<br>systemctl restart presidio-output<br>systemctl restart presidio-ui | 12.4 | 12.4.1 | ASOC-145668 |
| Investigate | **Title:** [Timeline-Chart] Selecting the first/last bar from the chart doesn't show the proper event count in the timeline text<br><br>**Problem:** When selecting the date and time range for the first and last bar in the chart, the correct event count in the timeline text is not displayed.<br><br>**Workaround:** Select a minimal time range between start and end to view the correct data. | 12.4 and later versions | | ASOC-145468 |

| | | | | |
|---|---|---|---|---|
| Platform | **Title:** Leapp upgrade fails due to Insufficient disk requirements<br><br>**Problem:** In some instances, the leapp upgrade fails due to the following error.<br>Error Summary Disk Requirements: At least x MB more space needed on the /<br>filesystem.<br><br>**Workaround:**<br>Run the following command to update the default value for LEAPP_OVL_SIZE variable,<br>so that it creates overlay mounts with size 4GB instead of 2GB.<br><br>sed -i 's/2048/4096/g' /usr/share/leapp-<br>repository/repositories/system_upgrade/common/libraries/overlaygen.py<br>Run the following command to update the default base directory for leapp<br>to /var/netwitness which has more available space.<br>sed -i s#/var/lib/leapp#/var/netwitness#g /usr/share/leapp-<br>repository/repositories/system_upgrade/common/actors/targetuserspacecrea<br>tor/libraries/constants.py<br>Proceed to re-trigger the upgrade for the respective host from the Admin Server. | 12.4 | 12.4.1 | ASOC-150789 |
| Platform | **Title:** /decoder/devices/message=prune failing with icap interface<br><br>**Problem:** If you run the optional Prune command as part of the DPDK migration, you might<br>see continuous failure messages related to some interfaces on the logs.<br><br>**Workaround:** It has no functional impact, and a Decoder service restart fixes the issue. Refer<br>to the KB Article "PF_RING Capture Devie KB Article" for more information. | 12.4 | | ASOC-147188 |
| Platform | **Title:** Edge Case Scenario - Host fails to boot OS with EL8 Kernel 4.x<br><br>**Problem:** In some instances, during upgrade to NW Version 12.4, the host fails to boot into<br>el8 kernel after OS Migration is complete.<br><br>**Workaround:** Check the logs in/var/log/salt/minion log file for "NodeRecovery" logs and if<br>found, please refer the KB Article "Edge Case Scenario - Host fails to boot OS with EL8<br>Kernel 4.x" for more details. | 12.4 | | ASOC-146908 |
| Platform | **Title:** SHA1 deprecated setting for SSH<br><br>**Problem:** SHA1 algorithm is deprecated, SHA1 algorithm is enabled on core services node-x<br>sshd config. It will be flagged for any Security scan.<br><br>**Workaround:**<br>1. Open file "/etc/ssh/sshd_config"<br>2. Comment out the following entry by adding "#" as prefix to below line<br>a. HostKey /etc/ssh/ssh_host_rsa_key<br>3. systemctl restart sshd | 12.4 | | ASOC-142946 |

| | | | | |
|---|---|---|---|---|
| Platform | **Title:** Secure UEFI boot causes leapp alma migration to fail<br><br>**Problem:** In some instances, after executing the leapp upgrade command during Alma migration and rebooting the appliance, a GRUB menu appears and attempts to boot to an 'elevate' kickstart.<br><br>**Workaround:** The current workaround is to just disable secure boot via BIOS settings. | 12.4 | | ASOC-123786 |
| UEBA | **Title:** Data collected for versions 12.2 or lower are not displayed in the Adapter dashboard after upgrading the UEBA server to version 12.4 or later.<br><br>**Problem:** After upgrading the UEBA server to version 12.4 or later from version 12.2 or older, the data collected before the upgrade are not visible in the Adapter dashboard. This issue occurs because, in version 12.2 or lower, the application name in the filter panel of the dashboard is the adapter. However, from version 12.3 or later, the application name is changed to presidio-adapter.<br><br>**Workaround:** In the Adapter dashboard, perform the following steps:<br><br>To view the older data collected before 12.2, you need to edit the visualization of the dashboard and update the application name in the filter panel of the dashboard as an adapter.<br>To view the newly collected data in the Adapter dashboard, you need to update the application name to presidio-adapter. | 12.4 and later versions | | ASOC-145667 |

| | | | | |
|---|---|---|---|---|
| SASE - CCM | **Title:** The decoder is unable to process the latest configuration updates (for example, invalid bucket names) made in the Palo Alto instances.<br><br>**Problem:** When you edit configurations for the Palo Alto instance, such as fixing a previously invalid bucket name to the correct one, the decoder fails to identify the latest changes. This issue occurs because the decoder does not recognize the recent updates made in the configuration.<br><br>**Workaround:** The instance needs to be restarted after applying decoder configuration changes to consider the latest configuration changes.<br>To update the Palo Alto instance properties manually using RestAPI, perform the following steps:<br>1. Connect to the Decoder host by using the Decoder IP address and Port 50104 as follows: <decoder-ip>:50104<br>2. Enter the username and password for the decoder host.<br>3. Navigate to the following path: /decoder/hosted/paloalto<br>4. Click Instances, and under the Properties section, select stop from the drop-down list. In the parameters field, type name=paloalto and click the Send button.<br>5. In the Properties section, select start from the drop-down list, and in the parameters field, type name=paloalto and click the Send button.<br>6. To verify that the instance state is Running, navigate to the following path: /decoder/hosted/paloalto/instances/paloalto<br>  | 12.4 | | ASOC-145406 |
| SASE | **Title:** Hosted Plugin Framework - Delete command deletes the plugin type only from the UI<br><br>**Problem:** The hosted plugin framework supports a delete command that deletes the plugin type from the UI. However, the associated filesystems are not deleted through this command as expected and require a separate cleanup.<br><br>**Workaround:** The leftover filesystems from the previously deleted plugin type are located at /etc/netwitness/ng/hosted and /var/netwitness/decoder/hosted on the decoder. These need to be manually deleted to ensure the plugin type is completely uninstalled. | 12.4 | | ASOC-142526 |
| SASE | **Title:** Hosted plugin reload deletes the plugin instance from the decoder/hosted tree.<br><br>**Problem:** On Hosted plugin reload, the plugin instance is getting deleted instead of reloading. On all future reloads, the user needs to add an instance and then reconfigure the plugin, which is not feasible for users.<br><br>**Workaround:** The current workaround is to stop the plugin instances before reloading the plugin or uploading an updated version of the plugin. After performing this step, the plugin instance will not be deleted from the Decoder config tree. | 12.4 | | ASOC-144467 |

| | | | | |
|---|---|---|---|---|
| SASE | **Title:** The decoder fails to remove Palo Alto Prisma Integration plugin details even after deleting the policy.<br><br>**Problem:** Deleting a policy with the Palo Alto Prisma Integration plugin type does not remove the plugin from the Decoder due to the current system behavior.<br><br>**Workaround:**<br>To remove the Palo Alto Prisma Integration Plugin from the Decoder, perform the following steps:<br>1. SSH to the Packet Decoder Host.<br>2. Run the following command to stop the Decoder service:<br>systemctl stop nwdecoder<br>3. Navigate to the following path:<br>/etc/netwitness/ng/hosted<br>4. Delete the paloalto folder.<br>5. Run the following command to start the Decoder service:<br>systemctl start nwdecoder<br>6. Connect to the Decoder host by using the Decoder IP address and Port 50104 as follows:<br><decoder-ip>:50104<br>7. Navigate to the following path:<br>/decoder/hosted/paloalto<br>8. Select the delete operation from the drop-down list and click Send.<br>  <br><br>The plugin details are removed from the decoder. | 12.4 | | ASOC-144688 |
| CCM | **Title:** Application rules are assigned incorrect order numbers during service content migration.<br><br>**Problem:** Application rules have incorrect entries, where several Application rules on service migration have been tagged with an order value of 1. This problem occurs when the service content is deployed using RPM. By default, application rules of this type are assigned an order value of 1, leading to incorrect entries.<br><br>**Workaround:**<br>If the user redeploys the same content from NetWitness Live or redeploys any one of the contents, the correct order is placed. | 12.4 and later versions | | ASOC-146940 |

| | | | | |
|---|---|---|---|---|
| CCM | **Title:** Policy updated with re-migration might fail to publish due to duplicate application rule.<br><br>**Problem:** If a user migrates and creates policy in 12.3 or 12.3.1 version and post upgrade to 12.4 they re-migrate the same service and update the pre-existing policy, there could be chances of getting duplicate application rule in the policy which can lead to a policy publication failure.<br><br>**Workaround:** If there are duplicate application rules, they get pushed to the bottom of the application rule list on Policy Details page. Remove these duplicate application rules manually to proceed with the publication. Follow these steps to remove the duplicate application rules:<br>1. Identify the duplicate rules in the Policy Details page by checking the orders.<br>2. Click Edit Policy to edit the policy.<br>3. Navigate to the Define Policy section.<br>4. Remove the duplicate contents from selected content list by searching the contents by name. | 12.4 | | ASOC-145770 |
| CCM | **Title:** While importing a Custom Log Device, there is no control on content update if CL has multiple flavors of same content.<br><br>**Problem:** When the user tries to import a Custom Log Device with Overwrite option selected and CL already has multiple flavors of same Custom Log Device, it is hard to predict which flavor of content will get overwritten. This import can lead to loss of customization made to Custom Log Device.<br><br>**Workaround:** Follow these steps to update specific flavor content.<br>1. Search specific flavor of content in Content Library collection in mongoDB and copy its path.<br>2. ssh to SA node and navigate to path copied from mongo.<br>3. Replace XML present in this location with updated XML.<br>4. Restart the source server. | 12.4 | | ASOC-143403 |
| Respond | **Title:** Service Unavailable Error When Trying to Incident Reports from Respond<br><br>**Problem:** In the Respond tab, while trying to create/schedule an incident report, the below error message is displayed:<br>The Reporting Engine service may be offline or inaccessible. Try starting the service.<br>This occurs when you have a domain name configured to access Netwitness and not via its IP.<br><br>**Workaround:**<br>If a domain name is used instead of the node-zero's IP, update the domain-name in "hostname" of the node-zero host. To update, go to Admin -> HOSTS -> select admin-server and edit, change to the domain name and save. Log out and log back in. | 12.3.1 | 12.5.1 | ASOC-157181 |

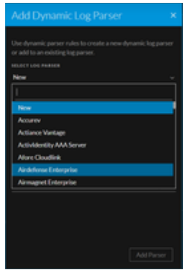
| | | | | |
|---|---|---|---|---|
| Reporting Engine | **Title**: Report generation fails on the **Investigate** > **Events** page due to mismatched service names.<br><br>**Problem**: If a user changes the name of a service on the **Services** page (for example., "Log Decoder" to "Log Decoder_new") but does not update the corresponding data source name used on the **Services** > **Reporting Engine** > > **View** > **Config** > **Sources** page, they will encounter issues when creating or scheduling reports from the **Investigate** > **Events** page. This is because the data source name used in the report configuration no longer matches the actual name of the data source. As a result, the reports cannot be generated, and an error message will be displayed indicating that the data source is not configured.<br><br>**Workaround**: To prevent this issue, ensure that the service name used as a data source in the Reporting Engine always matches the service name displayed on the **Services** page.<br>**Note**: Before re-adding the renamed data source in Reporting Engine, ensure to delete the current data source by navigating to **(Admin)** > **Services > Reporting Engine** > > **View** > **Config** > **Sources**.<br>Follow these steps to re-add the renamed data source in the Reporting Engine:<br>1. Go to **(Admin)** > **Services**.<br>2. In the **Services** list, select the Reporting Engine service.<br>3. Click > **View** > **Config**.<br>The Services Config View of the Reporting Engine is displayed.<br>4. Select the **Sources** tab.<br>5. Click and select **Available Services**.<br>The Available Services dialog is displayed.<br>6. Select the renamed service (for example, Log Decoder_new) and click **OK**.<br>The service authentication dialog box is displayed.<br>**Note**:<br>The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.<br>7. Enter the Username and Password for the service.<br>8. Click OK | 12.3.1, 12.4, 12.4.1 | | ASOC-129464 |

| | | | | |
|---|---|---|---|---|
| CCM, ESA, Source server | **Title:** The feed does not have an associated ID in the configured parameters of the policy.<br><br>**Problem:** The ESA rules were unable to be saved on editing or updating the ESA rule. Furthermore, a run time exception was shown in UI and SA logs while saving the rule. Further troubleshooting found that feed "RSA OSINT Non-IP Threat Intel Feed "did not have a unique ID associated with the policy and showed in multiple documents in the content policy collections.<br><br>**Workaround:** N/A | 12.3, 12.3.1 | | ASOC-141524 |
| CCM | **Title:** Log Devices are not getting disabled when content deletion is performed from CCM.<br><br>**Problem:** The Log Device contents published from CCM are not getting disabled when contents are deleted for a service. This is observed when a different policy is again published on the same service.<br><br>**Workaround:** Navigate to the Log Decoder Service Config view and disable Log Device contents that are not required. | 12.3.1 | | ASOC-142018 |
| Health-Wellness, Metric Server, Security | **Title:** RabbitMQ Warning Messages in All the Nodes<br><br>**Problem:** All the nodes encounter an error [warn] <0.16195.0> HTTP access denied: user 'guest' - invalid credentials every 5 minutes in the rabbitMQ logs. The NetWitness application services use the default guest account with the guest password or listening to the guest user in RabbitMQ.<br><br>**Workaround:** There is no impact on the system due to the error message. You can ignore the message. | 12.3.1 | | ASOC-141840 |
| Admin server | **Title:** Users cannot deploy or modify custom feeds when one or more decoders in the deployment group are offline.<br><br>**Problem:** When you are using the Groups option to deploy custom feeds, you may encounter an error message stating, "Failed to Retrieve Meta keys." This error occurs when one or more decoders in the group are offline, preventing the feeds from being deployed to that specific group. This issue occurs while creating new feeds or modifying an existing custom feed.<br><br>**Workaround:** When configuring custom feeds, do not use the Groups tab. Instead, use the Services tab. Unselect the offline decoder and select all the required decoders. Then, proceed with the configuration settings. | 11.7.x, and 12.x | | SACE-20424 |
| UEBA | **Title:** Increased JA3 entities due to JA3 randomization caused DAGs delay on the UEBA server.<br><br>**Problem:** The implementation of JA3 randomization in applications such as Chrome has resulted in a significant increase in the number of JA3 entities on the UEBA server, causing delays in the DAGs.<br><br>**Workaround:** To resolve this issue, please contact your NetWitness Customer Support team. | 11.7.x, 12.0, 12.1, 12.2, 12.3 | 12.3.1 | ASOC-138953 |

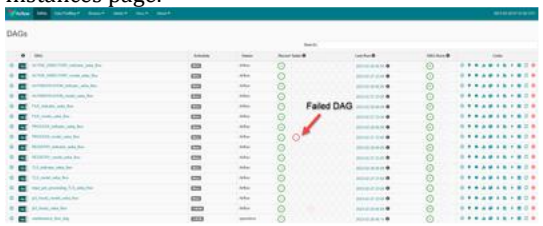
| | | | | |
|---|---|---|---|---|
| Correlation -Server | **Title:** InMemoryTable Adhoc Enrichment windows are not getting uploaded with data.<br><br>**Problem:** When the user adds the Adhoc In-Memory table enrichment under CONFIGURE > ESA > Enrichment Sources, the CSV file gets uploaded via UI, but upon using the enrichment in an ESA Rule and deployment, the contents are not read to the named window, and thus are not accessible for the rule to enrich the rule/alerts. There might be an impact of alerts not getting enriched, or the rule condition (if in-memory table enrichment reference is added to the rule) might not work as expected.<br><br>**Workaround:** Re-import the CSV file post-enrichment creation and deploy the rules again. Basically, the CSV file must be imported twice upon enrichment creation/update for the content to be reflected in the named window. Users can confirm if the data is uploaded to the named window under the "Named Windows" section of CONFIGURE > ESA Rules > Settings Page. | 12.1.x, 12.2 and, 12.3 | | ASOC-138145 |
| Central Content Management | **Title:** Content Migration Failing for Logdevice Contents<br><br>**Problem:** When service contents are migrated from services to Centralized Content Management, if the syntax of one of the custom log device is invalid, it fails to migrate.<br><br>**Workaround:**<br><br>1. Make sure there are no syntax errors inside the XML file of the custom base parser and deploy it again on the service.<br>2. Import Logdevice directly into Content-Library.<br>a) Navigate to CONFIGURE > POLICIES > CONTENT > Content Library > Log Device.<br>b) Click on the "Import" button and select Logdevice, which fails to migrate. | 12.3, 12.3.1 | | ASOC-138255 |
| UEBA | **Title:** Red banner errors are displayed on the Users page after the UEBA host upgrade<br><br>**Problem:** When you upgrade the UEBA host, you may encounter an issue where red banner errors are displayed on the Users page. A communication delay between the UEBA server and the Presidio UI service usually causes this issue.<br><br>**Workaround:** To resolve this issue, perform the following steps.<br><br>1. SSH to the UEBA server.<br>2. Run the following command:<br>systemctl restart presidio-ui | 12.2, 12.3 | 12.3.1 | ASOC- 134234 |
| UEBA | **Title:** Airflow shows a warning message that the scheduler task is not running<br><br>**Problem:** Airflow UI warning message "The scheduler does not appear to be running. Last heartbeat was received xx seconds ago. The DAGs list may not update, and new tasks will not be scheduled". This issue could occur due to a delayed response from the UEBA server.<br>**Note:** This warning message does not affect any functionality.<br><br>**Workaround:** To resolve the issue, try refreshing the page a couple of times. If the issue persists, connect to the UEBA server to check the airflow scheduler services. | 12.3, | 12.3.1 | ASOC-133835 |

| | | | | |
|---|---|---|---|---|
| Reporting Engine | **Title:** Generic error message is displayed for duplicate report names in Investigate > Events Page<br><br>**Problem:** When you create or schedule a report from the Investigate > Events page using a report name that already exists, an error message will be displayed. However, the error message displayed is generic and provides limited information. The error message states, "Error generating report. Please check respond-server.log/investigate-server.log and sa.log"<br><br>**Workaround:** To resolve this issue, always create or schedule the reports with a unique name. | 12.3 | 12.3.1 | ASOC-134996 |
| Reporting Engine | **Title:** Generic error message is displayed when you create or schedule reports on the Investigate > Events page when the data source is not configured in Reporting Engine.<br><br>**Problem:** When you create or schedule a report from the Investigate > Events page, an error message is displayed if the data source is not configured in the reporting engine. However, the error message displayed is generic and provides limited information. The error message states, "Error generating report. Please check respond-server.log/investigate-server.log and sa.log"<br><br>**Workaround:** To resolve this issue, perform the following steps:<br>1. Go to **(Admin)** > **Services**.<br>2. In the **Services** list, select the **Reporting Engine** service.<br>3. Click > **View** > **Config**.<br>The Services Config View of Reporting Engine is displayed.<br>4. Select the **Sources** tab.<br>5. Click the and select **Available Services**.<br>The Available Services dialog is displayed.<br>6. Select the required service (for example, Log Decoder) and click **OK**.<br>The service authentication dialog box is displayed.<br>**Note**: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.<br>7. Enter the Username and Password for the service.<br>8. Click **OK**.<br>The selected service is listed in the Aggregate Services pane. | 12.3 | 12.3.1 | ASOC-134996 |
| Reporting Engine | **Title:** Use of future dates in the Custom date range option for Adhoc reports will result in incorrect date ranges in the output report.<br><br>**Problem:** If you choose future dates using the Custom date range option to create Adhoc reports from the Investigate > Events page, the report generated will display an invalid date range. This issue occurs whenever a future date is detected. The system recognizes it as an invalid date.<br><br>**Workaround:** NetWitness recommends avoiding the use of future dates when configuring the Adhoc reports. | 12.3 | 12.3.1 | ASOC-135074 |

| | | | | |
|---|---|---|---|---|
| Investigate | **Title:** Use of Enter as a shortcut key to select a query suggestion in Advanced Query mode.<br><br>**Problem:** When you construct a query in Advanced Query Bar mode in the Investigate > Events view, pressing Enter key will select and execute the query instead of only selecting a suggestion from the query suggestions list. This action is not in line with the Guided Query Mode, where pressing Enter key selects a suggestion from the query suggestions list but does not execute the query.<br><br>**Workaround:** Use the Tab key to select a suggestion from the query suggestions list while you are in the Advanced Query Bar mode. | 12.3 | 12.3.1 | ASOC-134482 |
| Investigate | **Title:** Unable to load a saved query to the query bar in Advanced Query Bar mode.<br><br>**Problem:** When you select a saved query while you are in Advanced Query Bar mode in the Investigate > Events view, the selected saved query is not loaded into the query bar and is not applied to the executed query either.<br><br>**Workaround:** NetWitness recommends you use Guided Mode if you want to execute a saved query in Investigate > Events view. | 12.3 | 12.3.1 | ASOC-133508 |
| Investigate | **Title:** Unable to execute a query when a service is updated to Decoder/Log decoder in Advanced Query Bar mode.<br><br>**Problem:** When you update a service to decoder/log decoder while you are in Advanced Query Bar mode in the Investigate > Events view, the search button is enabled but, clicking the search button does not execute the query or show an error. This happens because of unindexed keys in the query for the selected service which is the expected behavior with any unindexed keys. In Guided Mode, an error is displayed as soon as the service is updated using the service selection drop-down.<br><br>**Workaround:** You need to remove the unindexed keys from the query before executing it. | 12.3 | 12.3.1 | ASOC-134481 |
| CCM | **Title:** Publish and Restart pop-up does not appear while publishing policy from Policy listing page.<br><br>**Problem:** When any configuration which requires service restart, is updated in Policy and it is being published from Policy listing page, pop-up does not appear for “Publish and Restart Now” option. Policy is being published with “Publish and Restart Later” option automatically and services need to be restarted later.<br><br>**Workaround:**<br>a. Restart service(s) from Groups page<br>1. Go to Groups listing page.<br>2. Select Group in which service(s) require restart.<br>3. Click “Restart Service” button.<br>or<br>b. Publish and restart from Edit Policy view.<br>1. Edit the Policy.<br>2. Click “Save and Publish” button.<br>3. Click “Publish and Restart Now” button. | 12.3 | | ASOC-134862 |

| | | | | |
|---|---|---|---|---|
| Investigate | **Title:** The most recent query is not populated while creating a new saved query in Advanced Query mode.<br><br>**Problem:** Usually, the most recently executed query is auto-populated in the Pre-Query Conditions field when you try to save a new query. But, while you are in Investigate > Events > Event Preferences > Advanced Query mode, the most recently executed query is not auto-populated in the Pre-Query Conditions field when you try to save the query (Saved Queries > New Saved Query).<br><br>**Workaround:** We recommend you switch to Guided Mode, run the same query, and then proceed with saving a new query. | 12.3 | 12.3.1 | ASOC-135221 |
| Log Parser Configuration | **Title:** Missing list of Logparsers in Dropdown when trying to Add new Parser<br><br>**Problem:** The dropdown does not list existing Out of box (OOTB) Logparsers because UI is not able to sync with the previously synced Log Decoder service to fetch those OOTB Logparsers.<br><br>**Workaround:**<br>1. Go to Admin > Services page<br>2. Click on the Service name of a Log Decoder in a working state to open its System View.<br>3. Now, Copy the UUID of that service from the URL of the service's System page.<br>Example - UUID of service will look like this in URL:<br>https://<AdminServerIP>/admin/services/e099b4bb-a7f6-4149-ae31-a453797d8c25/info<br>4. Go to Admin > Services page, open the explore view of content-server.<br>5. Go to > content > parser.<br>6. Update the value of "previously-synced-log-decoder-id" with the UUID of the new Log decoder.<br>7. Go to CONFIGURE > LOG PARSER RULES page.<br>8. Click the [+ADD] button.<br>The dropdown list will start getting populated.<br><br>  | 12.3 | | ASOC-135320 |

| | | | | |
|---|---|---|---|---|
| CCM | **Title:** Unable to Access ESA Deployments<br><br>**Problem:** Users will not be able to access ESA deployments configurations in the Unified deployment view or policy details. Due to stale or invalid entries in source server mongo.<br><br>**Workaround:**Clean up the source-server mongo of invalid entries. Refer to KB article NetWitness ESA Deployments are not accessible in the Policies tab | 12.1 | | ASOC-131743 |
| Decoder | **Title:** The database stagger operation takes a long time to complete, resulting in a timeout from the UI Explore page.<br><br>**Problem:** If you perform the database stagger operation from the UI Explore page, it takes a long time to complete the operation based on the data and results in a timeout.<br><br>**Workaround:** To perform the database stagger operation, you must run the command using the RESTful API or NwConsole. | 11.7.x,<br>12.0,<br>12.1,<br>12.2 | | ASOC-<br>124339 |

| | | | | |
|---|---|---|---|---|
| UEBA | **Title:** When UEBA receives a high volume of events, the root DAG becomes unresponsive as it awaits the completion of other associated DAGs.<br><br>**Problem:** Upon receiving a high volume of events, the root DAG of UEBA becomes unresponsive as it awaits the completion of other associated DAGs, resulting in failures in the model_ueba_flow DAGs for their respective schemas. These failures are followed by errors related to java.heap.memory, as shown below.<br>1. [2023-02-19 08:02:09,178] {bash_operator.py:126} INFO - java.lang.OutOfMemoryError: Java heap space<br>2. [2023-02-19 08:02:09,178] {bash_operator.py:126} INFO - java.lang.OutOfMemoryError: Java heap space<br>3. [2023-02-19 08:02:09,179] {bash_operator.py:126} INFO - at java.base/java.util.concurrent.ConcurrentHashMap$KeySetView.iterator(ConcurrentHashMap.java:4625)<br>4. [2023-02-19 08:02:09,179] {bash_operator.py:126} INFO - at java.base/java.util.Collections$UnmodifiableCollection$1.<init>(Collections.java:1044)<br>5. [2023-02-19 08:02:09,179] {bash_operator.py:126} INFO - at java.base/java.util.Collections$UnmodifiableCollection.iterator(Collections.java:1043)<br>6. [2023-02-19 08:02:09,179] {bash_operator.py:126} INFO - at org.apache.http.impl.nio.reactor.BaseIOReactor.validate(BaseIOReactor.java:210)<br>7. [2023-02-19 08:02:09,179] {bash_operator.py:126} INFO - at org.apache.http.impl.nio.reactor.AbstractIOReactor.execute(AbstractIOReactor.java:280)<br><br>**Workaround:**<br>1. In the DAGs tab, click the failed Dag (circle with red) that takes you to Task Instances page.<br>  <br><br>2. Click the DAG ID and then click Tree View.<br>3.  <br>3. In the Tree View, click the failed task instance and click View Log.<br>**Note:** Hover over the failed task instance to view the operator of the task instance.<br>4.  <br>The log view is displayed.<br>You will see the executed jar in the logs in the running command section. | 12.2 and later versions | | ASOC-128667 |

| | | | | |
|---|---|---|---|---|
| | For example, presidio -output processor.jar .<br>4. SSH to the UEBA server.<br>5.<br>Open /etc/netwitness/presidio/configserver/configurations/airflow/workflows-default.json file.<br>6. Increase the heap memory size of respective failing DAGs with their respective operator by two times. For example, if it is 2048, make it 4096.<br>7. In the Tree View, click the failed task instance and click Clear.<br>This solution will help to run the DAGs successfully. | | | |

| | | | | |
|---|---|---|---|---|
| Source Server | **Title:** Unable to load the Content Library.<br><br>**Problem:** After upgrade to 12.1, user will not be able to load Content Library for the created policies. The issue is due to the source-server not able to connect to Live CMS , even though the Live is configured and the source server is not able to resolve cms.netwitness.com. Following error is seen in the source server logs path /var/log/netwitness/sourceserver/source-server.log<br>ERROR CentralContent\|Failed to authenticate with CMS Server. 2org.springframework.web.client.ResourceAccessException: I/O error on POST request for "https://cms.netwitness.com:443/authlive/authenticate/CMS": cms.netwitness.com; nested exception is java.net.UnknownHostException: cms.netwitness.com<br><br>**Workaround:**<br><br>1. If the affected netwitness environment can reach out to any of the DNS servers internal or external, then the user could add the DNS IP entry as nameserver to /etc/resolve.conf on Node-Zero.<br>2. If the above workaround is not feasible, then the user can add a manual entry of the "<ip-address> cms.netwitness.com" into /etc/hosts.user file and refresh the host using the "nw-manage -r --host-key <admin-server-ip>". The IP address of cms.netwitness.com can be found by pinging cms.netwitness.com from a system that can be connected to cms.netwitness.com.<br>3. Restart the source server using the command service rsa-nw-source-server restart. | 12.2 | | ASOC-124473 |
| ESA Correlation Server | **Title:** Enable / Disable of rules in Endpoint Risk Scoring bundle applies to all deployments.<br><br>**Problem:** When a rule in the Endpoint Risk Scoring Bundle is either enabled / disabled from the ESA Service Stats UI it throws an error on UI. However, in the backend, the rule gets enabled / disabled.<br>The disabled list of rules is saved in the keyValueRuleSettings as a generic setting without any associated engine ID. As it doesn't have any engine id associated with it, the config acts like a global configuration.<br>In all the deployments, wherever the Endpoint Risk Scoring Bundle is deployed, the rules disabled in any one deployment get automatically disabled in all deployments.<br><br>**Workaround:** N/A | 11.7.x, 12.0, 12.1, 12.2 | | ASOC-127949 |
| Endpoint Investigation | **Title:** Event overview panel error or infinite loading.<br><br>**Problem:** The event overview panel throws an error or loads infinitely for endpoint events.<br><br>**Workaround:** Restart the investigating server to properly load the overview panel to display endpoint events. On re-enabling the meta forwarding, the issue will get resolved. | 12.2 | N/A | ASOC-123671 |

| | | | | |
|---|---|---|---|---|
| SA Server | **Title:** Floating Save button on Decoder Stats page in UI.<br><br>**Problem:** Whenever a user opens the Decoder Stats page, a Save button, originally under the Key Stats Settings, toggles on the top left corner of the screen, covering part of NetWitness branding. A click on the gear icon beside the Key Stats Settings will take the Save button to appear in its original place.<br><br>**Workaround:** N/A<br><br>**Note:** This cosmetic issue does not interfere with the service functionally. | 12.2 | N/A | ASOC-114414 |
| Platform | **Title:** Logback and Spring Warning Message is displayed while upgrading to 12.5.2.0.<br><br>**Issue:** While upgrading to 12.5.2.0 using CLI, a warning message related to the Logback and Spring appears once across all the Node-0 and Node-x systems. The warning message is displayed also when you run the data sync job and when you run the Security CLI command.<br><br>**Workaround: N/A** | 12.5.2.0 | | PLATFORM-62 |
| UEBA | **Title**: After upgrade, the UEBA Server component version is displayed incorrectly on the **ADMIN** > **Services** page.<br><br>**Issue:** After upgrading from 12.5.1.3 or any other older version to 12.5.2.0, the **ADMIN** > **Services** page displays the respective older version as the upgraded version of the UEBA-server component. However, the **ADMIN > Hosts** page displays the upgraded version as 12.5.2.0.<br><br>**workaround:** Run the following command and restart Jetty.<br>**service jetty restart** | 12.5.2.0 | | UI-19 |