# NetWitness® Platform

Version 12.4.0.0

# Upgrade Guide

NETWITNESS

Platform

## 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.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

## 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.

## Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.



April, 2024

# Contents

# Upgrade NetWitness Platform

This document provides information about the benefits and process of upgrading NetWitness Platform to 12.4. Ensure you go through the pre-requisites and pre-upgrade tasks before you upgrade NetWitness Platform. You can upgrade NetWitness Platform using four different options depending upon your Internet connectivity. After upgrading, you should also perform certain post upgrade tasks and post upgrade sanity checks listed in this guide to complete the upgrade process successfully. The instructions in this document apply to both physical and virtual hosts (including AWS, Azure Public Cloud, and Google Cloud Platform) unless stated to the contrary.

**IMPORTANT:** The versions 11.7.x, 12.0, and 12.1 reached the End of Life (EOL) on 31st December 2023. For more information, see https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. If you want to upgrade from 11.7.x (Service packs) or 11.7.x.x (Patches) versions to 12.4.0.0 version, you must first upgrade to 12.2.0.0 or 12.3.0.0 version before upgrading to 12.4.

**IMPORTANT:** The custom search patterns you created using the **search.ini** file in version 12.3.1 or earlier will not be migrated to the new **search.xml** file format used in version 12.4 and later. As a result, those custom search patterns will not be available from the **Content Library** > **More** > **Search Pattern Rule** tab after you upgrade to version 12.4 or later. For more information, see **Manage Search Pattern Rules** topic in the Centralized Content Management Guide for NetWitness.

**IMPORTANT:** NetWitness 12.4 and later versions (AlmaLinux) do not support numeric usernames. This means that customers who use Pam Securid with only numbers as usernames cannot be added to the groups after upgrading to 12.4. For more information on this limitation, see https://www.webconn.tech/kb/are-all-numeric-usernames-allowed-in-almalinux-8.

**Note:** NetWitness Platform now supports installing multiple servers of UEBA in your environment. For more information, see **Configure Multiple UEBA Servers** topic in the *NetWitness UEBA Configuration Guide*.

There are many exciting new features that you can enable after you have upgraded to 12.4. For a detailed description of the new features in this release, see the *Release Notes for NetWitness Platform 12.4*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues. For more information on the new features released in the previous releases, see https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-x-to-12-x/ta-p/695650.

## Upgrade Paths Supported for 12.4

The following upgrade paths are supported for NetWitness 12.4:

- NetWitness 12.3.1.0 to 12.4
- NetWitness 12.3.0.0 to 12.4
- NetWitness 12.2.0.1 to 12.4
- NetWitness 12.2.0.0 to 12.4

# Running in Mixed Mode Environment

NetWitness Platform supports mixed mode during upgrade. Mixed mode occurs when some services are upgraded to the latest version and some services are still on the older versions.

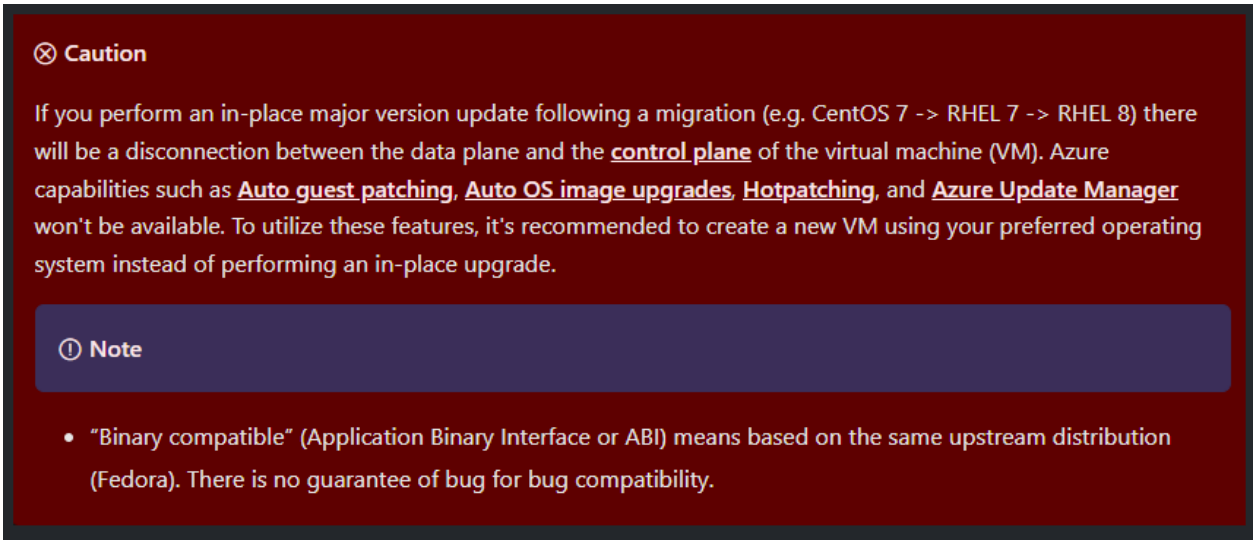
For more information, see **Running in Mixed Mode** in the *NetWitness Hosts and Services Getting Started Guide*.

**Note:**
- If it takes a longer duration for upgrading all the hosts in your environment, contact NetWitness support to avoid encountering any issues.
- If you are running Endpoint Log Hybrid in mixed mode, make sure Endpoint Broker is on the same version as one of the Endpoint Servers.
- Mixed mode is not supported for ESA hosts in NetWitness Platform.

# NetWitness Upgrade Guidelines for Azure

In-place upgrades on Azure VMs are supported when followed by the Standard Configuration outlined in the Azure Installation Guide. The customer is responsible for ensuring that no VM policies at the Azure Subscription level interfere with the VM's operating system, such as configurations related to the Azure Control Plane.

If you follow the Azure Installation Guide correctly, you should experience a smooth upgrade process without encountering any warnings. However, deviating from these guidelines or adding extra configurations, such as those involving the Azure Control Plane, can lead to errors, as shown below:




# Upgrade Guidelines for Managing Users

When adding users at the OS level during or after an upgrade to NetWitness version 12.4.0.0 or later, the admin server may encounter issues with new users or groups related to the following NetWitness accounts:

- `nw-integration-server:x:3001:`
- `nw-response-actions-server:x:3002:`
- `nw-integration-server:x:3001:3001:RSA nw-integration-server service account:/home/nw-integration-server:/usr/sbin/nologin`
- `nw-response-actions-server:x:3002:3002:RSA nw-response-actions-server service account:/home/nw-response-actions-server:/usr/sbin/nologin`

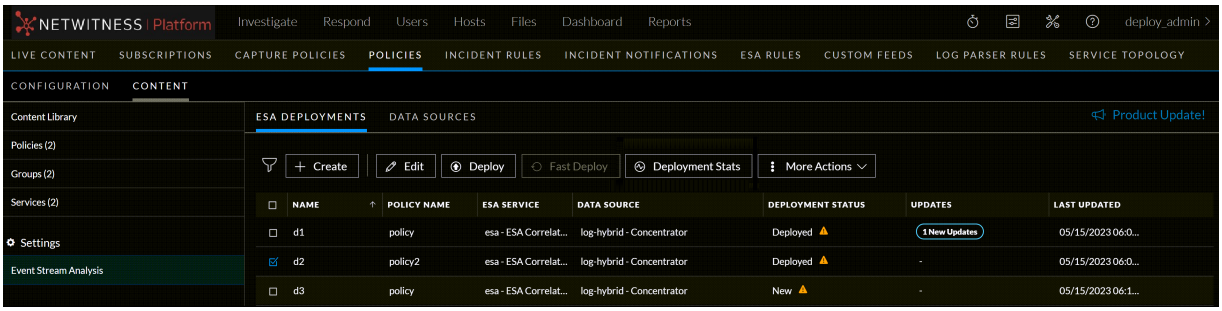
This results in incorrect LDAP mapping IDs for the users and causes their LDAP logins to stop working after the upgrade.

To avoid this issue, NetWitness recommends not to add any users at the OS level while the upgrade is in progress or after it is finished.

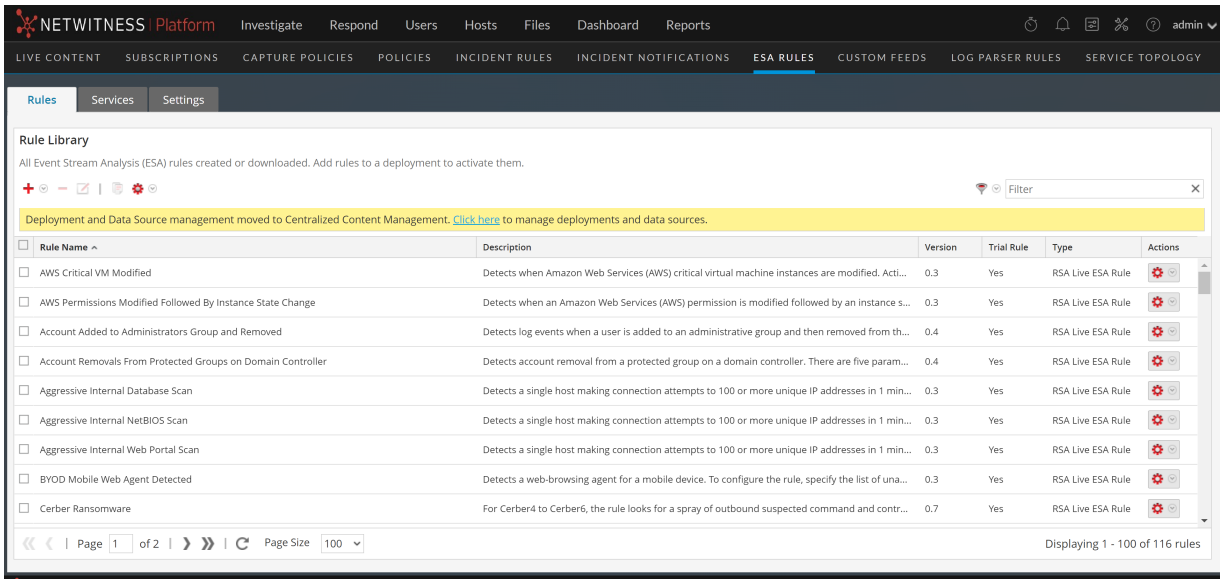
## Upgrade Considerations for ESA Hosts

**IMPORTANT:** The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

- 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 figure.




- You can only manage the ESA Rules in the **ESA Rules** page. Refer the following figure.




- After upgrading to the 12.4 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 12.4 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 Content Management Guide for NetWitness.

## Upgrade or Install Windows Legacy Collection

Refer to Windows Legacy Collection Guide for NetWitness for NetWitness Legacy Windows Collection Upgrade & Installation Instructions.

**Note:** After you upgrade or install Windows Legacy Collection, reboot the system to ensure that Log Collection functions correctly.

## Terminologies

| Name | Description |
|---|---|
| AVX | Advanced Vector Extensions |
| VMX | Virtual Machine Extension |
| NFS | Network File System |
| BTRFS | B-Tree File System |

| Name | Description |
| --- | --- |
| DPDK | Data Plane Development Kit |

# Run Pre-Upgrade Checks

You must run the pre-upgrade checks before you upgrade to NetWitness Platform 12.4 to identify any issues that may result in upgrade failure.

### Before you begin

You must first download the Standalone RPM using https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-platform-standalone-precheck-tool/ta-p/709096 and refer to the read me file for instructions on how to install the Standalone RPM and then run the pre-check.

### To run the pre-upgrade checks:

1. SSH to Admin Server.
2. Using the Upgrade Precheck tool, run the following commands in sequence:
   a. `nw-precheck-tool-standalone os-migration-checklist`: This command allows the Upgrade Precheck tool to perform sanity checks for the list of probes in the OS Migration Checklist.
   b. `nw-precheck-tool-standalone upgrade-checklist`: This command allows the Upgrade Precheck tool to perform sanity checks for the list of probes in the Upgrade Checklist.
   c. `nw-precheck-tool-standalone network-checklist`: This command allows the Upgrade Precheck tool to perform sanity checks for the list of probes in the Network Checklist.
   d. `nw-precheck-tool-standalone cert-checklist`: This command allows the Upgrade Precheck tool to perform sanity checks for the list of probes in the Certificate Checklist.

## OS Migration Checklist

The Upgrade Precheck tool performs the sanity checks for the following list of probes in the OS Migration checklist:

- **Version Check Probe**: Checks whether the NetWitness version of the system is the later version of 12.2.0.0 or not.
- **AVX / VMX Probe**: Checks if the AVX / VMX flags are enabled or not for the nodes that require them.
- **NFS Mount Probe**: Checks if NFS type mount point is active on any of the nodes.
- **Multiple kernel-devel Package Probe**: Checks if Decoder and PacketHybrid have multiple versions of kernel-devel package or not.
- **PF Ring Capture Device Probe**: Checks for PF_ring capture device on decoders and raises a warning to change PF_ring capture device to DPDK capture device.
- **BTRFS mount Probe**: Check if BTRFS partition is mounted.

  **Note:** LEAPP and Alma OS doesn't support BTRFS partition.
- **Disk space check**: Checks to ensure that enough disk is free in the / partition on each node.

- **Fips Mode Check**: Checks to ensure that the Fips mode is disabled (set to false) on all nodes.
- **Mountcheck probe**: Checks if all the partitions or file directories are mounted properly.

## Upgrade Checklist

The Upgrade Precheck tool performs the sanity checks for the following list of probes in the upgrade checklist:

- **Security Client File Check**: Ensures `security-client-amqp.yml` file is not present.
- **Node-0 NW Service-id Status Check**: Ensures all the service-id is intact with all the different services in Node 0.
- **Broker Service Trustpeer Symlink File Check**: Ensures Broker Service Trustpeer Symlink file `(/etc/netwitness/ng/broker/trustpeers/)` is not broken.
- **Node-0 NW Services Status Check**: Checks the status of all the services in Node 0.
- **Yum External Repo Check**: Ensures external repos are not available and not enabled.
- **Node-0 RPM DB Index Check**: Checks if the RPM DB is corrupted or not.
- **Salt Master Communication Check**: Verifies the salt communication from Node 0 to all the Nodes.
- **Node-0 Certificates Check**: Checks if any certificates are missing, expired, or invalid issuer type.
- **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.
- **(Component Hosts) Node X NW Service Status Check**: Verifies the status of services (Active or Inactive) on all the Node X.
- **(Component Hosts) Node X Certificates Check**: Checks the certificate expiry, missing, corrupted, and issuer mismatch in all the categories of Node X.
- **Provide Nodes CPU-Memory Info**: Provides CPU and Memory details of all the nodes along with the real-time available memory.
- **(Admin Server) Node 0 File System Utilization Check**: Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness`, and `root` on Node 0.
- **(Component Hosts) Node X File System Utilization Check**: Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness`, and `root` for ESA Primary and Endpoint Log Hybrid services on Node X.

- **Mongo File (ESAPrimary) Permission Mode Check**: Checks the ESA Primary node in the system or stack and verifies the permission mode of Mongo file.
- **Orchestration Server Normal Mode Check**: Checks if the orchestration service is running in normal or safe mode.
- **(Admin Server) Node 0 Init status Check**: Checks if there are any issues that might fail init process.
- **Fips Mode Check**: Checks to ensure that the Fips mode is disabled (set to false) before and after upgrade.
- **Node-X RPM DB Index Check**: Checks for the status of RPM DB on Node-X to make sure it is not corrupted.
- **Node-Z Yum Proxy Check**: Checks for the existence of yum.conf file and availability of proxy within the file on Node -Z.
- **Node-X Yum Proxy Check**: Checks for the existence of yum.conf file and availability of proxy within the file on Node -X.
- **Host Info Check Probe**: Checks if the required fields of information of all the hosts in the system (Host IP, Hostname, Installed Services, and Raw Version) are available.
- **Node-Z Cipher Check Probe**: Checks if the required ciphers are available in the location `/etc/rabbitmq/rabbitmq.config` on Node-0.
- **Node-X Cipher Check Probe**: Checks if the required ciphers are available in the location `/etc/rabbitmq/rabbitmq.config` on all Node-X.
- **Node-X Hardware Version Check Probe**: Checks for the hardware version of all reachable Node-X.
- **Node-Z Hardware Version Check Probe**: Checks for the hardware version of the Admin server.
- **PuppetCA Certificates Check Probe**: Checks if the stale puppet CA certificates are present in the location `/etc/pki/nw/trust/truststore.pem`.
- **AdminCertCheck Probe**: Verifies if the admin-certs across all the nodes are the same as the admin-certs on the Admin Server.
- **NTP Probe**: Checks all the nodes to ensure they are in sync with the NTP server.
- **StaleCerts Check Probe**: Checks the mongo and warns if there are any unused stale certificates in it.
- **NodeCertIDCheck Probe**: Checks the subject field of the node-cert and ensures that it is the same as the node-ID of the host.
- **Deploy Admin password expiry check Probe**: Verifies if the deploy_admin password is expired on Node-0.
- **File / Folder permission check**: This probe checks if the files / folders have the appropriate permissions.

## Network Checklist

The Upgrade Precheck tool performs the sanity checks for the following list of probes in the network checklist:

- **(Admin Server) Node 0 closed ports Check**: Checks if the service ports required for NetWitness services are open and listening on Node 0.
- **(Component Hosts) Node X closed ports Check**: Checks if the service ports required for NetWitness services are open and listening on Node X.

## Certificate Checklist

The Upgrade Precheck tool performs the sanity checks for the following list of probes in the Certificate checklist:

- **Node 0 Service Certificates Validity Check**: Checks the validity of service certificates in the location `/etc/pki/nw/service/` on Node-0.
- **Node X Service Certificates Validity Check**: Checks the validity of service certificates in the location `/etc/pki/nw/service/` on Node-X.
- **Node Certificates Validity Check on Node-0**: Checks the validity of node certificates in the location `/etc/pki/nw/service` on Node-0.
- **Root CA Certificates Validity Check**: Checks the validity of Root CA certificates in the location `/etc/pki/nw/ca`.

# Prepare to Upgrade NetWitness Platform

Complete the following tasks to prepare for the upgrade to NetWitness Platform 12.4.

## Task 1. (Important) Prepare to Upgrade AlmaLinux OS

### Unsupported File System

#### Unmount and Remove BTRFS

BTRFS is a copy-on-write (CoW) filesystem for Linux that aims to implement advanced filesystem features while focusing on fault tolerance, repair, and easy administration. The BTRFS file system is deprecated from Red Hat Enterprise Linux 8, and AlmaLinux OS does not support the BTRFS file system. NetWitness does not use BTRFS by default, but in some categories like network decoder, network hybrid, etc., BTRFS module exists and is loaded. If BTRFS is mounted as a filesystem, perform the below steps to unmount the BTRFS partition manually (If BTRFS is not mounted, skip the below steps):

a. Relocate the data.

b. Unmount the BTRFS partition using the following command.

c. umount <btrfs partition path>. You can get the btrfs partition info from `/etc/fstab or df -hT` commands.

d. Remove the BTRFS partition from `/etc/fstab`.

e. Verify if the kernel moduleis still loaded using `lsmod | grep btrfs`. If the kernel module is still loaded , use `modprobe -r btrfs` to unload the btrfs kernel module.

f. Trigger/Retrigger the Upgrade.

For more information, refer the KB article “Upgrade to Alma OS when BTRFS file system is mounted.”

#### Unmount NFS

NFS type file systems active on the nodes cause the upgrade to fail for the nodes. You should manually unmount these mount points from the CLI of each node where it is found. Perform the below steps to unmount the NFS manually:

a. SSH to the nodes where NFS mount point is detected.

b. In each node, run `mount | grep 'type nfs'` and get the directory path of the NFS mount point.

> **Note:** Before unmounting NFS, you must stop the NetWitness services that rely upon NFS.
> For example: If Archiver and Warehouse Connector service is running on NFS, you must run the following commands to stop the services before unmounting NFS.
> `systemctl stop nwarchiver`
> `systemctl stop nwwarehouseconnector`

c. Execute umount <dir_path> from the terminal, where <dir_path> is the directory path from Step b.

d. Open `/etc/fstab` file in an editor of choice and comment out the line(s) that pertain to NFS mount point(s).

e. Run the NetWitness upgrade.

f. After upgrade has completed successfully, un-comment the respective entry from `/etc/fstab` and execute `mount -a` from the terminal to add the NFS mount point(s) back.

## AVX/VMX CPU Instruction Set Check

AVX/VMX CPU flag needs to be enabled for NetWitness Platform 12.4. Run the command `salt '*' cmd.run "lscpu | grep -E 'avx|vmx'"` to check if AVX/VMX CPU instruction set is enabled. Refer the KB Article "Use AVX Instruction Set for MongoDB 5.0 Platform Support" for more information.

**Note:** For NetWitness hardware appliance, AVX/VMX CPU instruction set is enabled by default.

## PF_RING to DPDK Migration Support

The decoder capture config will not be valid for customers using PF_RING capture (CentOS) and directly upgrading to 12.4 (AlmaLinux). First, they must migrate PF_RING devices to DPDK and then upgrade.

Refer to Migrate PF_RING Devices to DPDK for migration instructions.

# Task 2. (Optional). Remove Legacy Package Repositories

You can free up the disk space by removing obsolete repositories from previous releases.

**To remove the obsolete repositories:**

1. Determine the version of the oldest NetWitness Platform host in your environment by using the NetWitness Repo tool. Do the following:

- SSH to the Admin Server as a `root` user.
- Run the following command.

  ```
  nw-repo-tool --list-obsolete
  ```

  After running this command, you will get a list of all the obsolete repositories.

2. Run the following command to remove all the obsolete repositories.

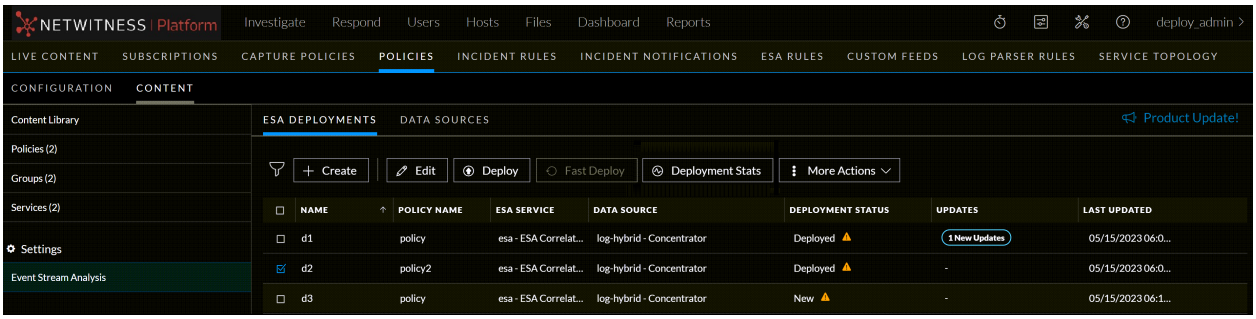
   ```
   nw-repo-tool --purge-obsolete
   ```

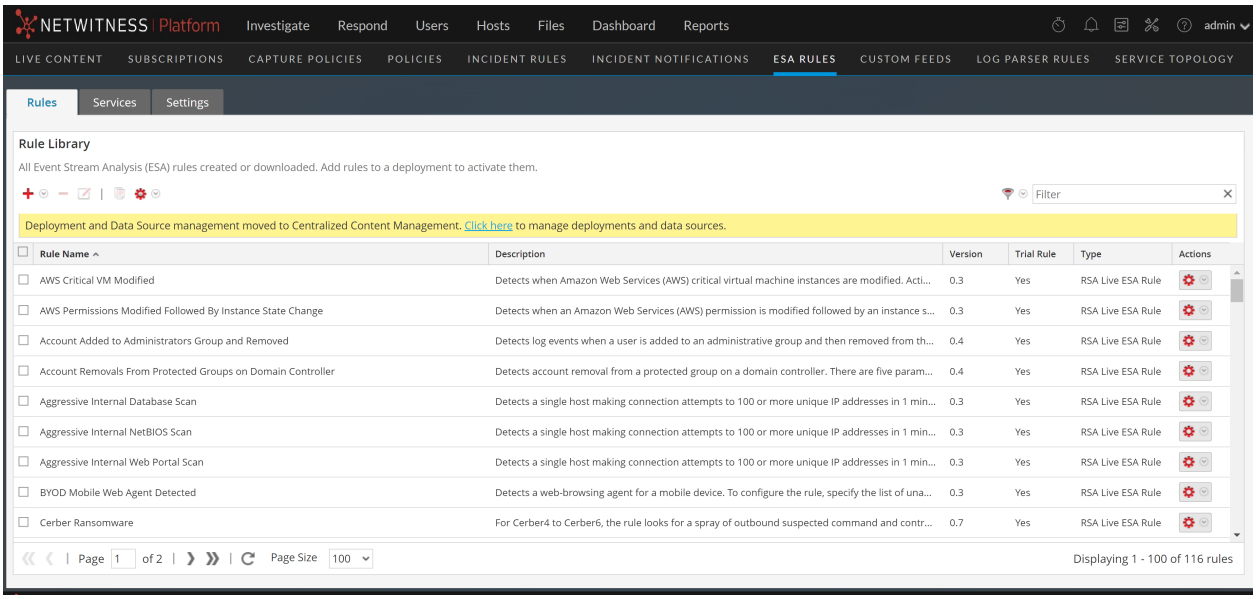
# Task 3. Prepare ESA Deployments for Migration to 12.4

Before upgrading to 12.4, NetWitness recommends that all the ESA deployments maintain an error-free state. You must remove any unused ESA deployments, as ESA deployments will be migrated to policies and groups after upgrading to 12.4. 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 12.4 version.

# Manage ESA Deployments and Data Sources

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. You can only manage the ESA Rules in the **ESA Rules** page. Refer the following figures.




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 Content Management Guide for NetWitness.

**IMPORTANT:** If there is any need to import ESA Rules and enrichments, NetWitness recommends importing those missing rules and enrichments before the upgrade.

The pre-upgrade and post-upgrade states of deployments are represented in the following table.

| SINo | Pre-upgrade Deployment State | Post-upgrade Deployment State | | |
|---|---|---|---|---|
| | | Creates Policy | Creates Group | The policy will be Published |
| 1 | Healthy deployment | Yes | Yes | Yes |
| 2 | Deployment with errors | Yes | Yes | Yes |
| 3 | Deployment with only rules | Yes | No | No |
| 4 | Deployment with no rules | No | No | No |

Healthy deployment contains no errors, and the required resources such as ESA Server, Data source, and ESA rules are added.

**Note:** NetWitness recommends that all the deployments maintain an error-free state. You must remove any unnecessary or unused ESA deployments.

## Task 4. Third-Party Package Removal

Any third-party packages installed on hosts out of the NetWitness repository are subjected to removal based on the Upgrade dependencies as part of OS migration.

## Task 5. Single Sign-on (SSO): Enable SAML Response Signing in Microsoft Azure ADFS

The following configuration is only applicable to cases where the SAML response from Microsoft Azure ADFS was only encrypted by not signed. If your Microsoft Azure ADFS is already configured to sign and encrypt SAML responses, you can ignore this configuration and proceed with the upgrade process.

If you are not signing the SAML response, NetWitness recommends you to configure Microsoft Azure ADFS to encrypt and sign the SAML responses before upgrading your NetWitness Platform to version 12.4 for a successful Single Sign-on (SSO) login. To enable response signing in Active Directory Federation Service (AD FS), run the following command in ***powershell***:

```
Set-AdfsRelyingPartyTrust -TargetName <<relying-party-name>> -
SamlResponseSignature MessageAndAssertion
```

**IMPORTANT:** It is mandatory to configure Microsoft Azure ADFS to sign SAML responses before upgrading to version 12.4 of the NetWitness Platform. Without complying with these requirements, you may not be able to log in using SSO.

## Task 6. (Optional). Disable STIG-based FIPS Kernel Controls

If you enabled STIG-based FIPS Kernel controls, you must disable them before initiating the NetWitness Platform upgrade process to avoid boot errors. To disable STIG-based FIPS Kernel controls, run the following commands:

```
manage-stig-controls --disable-control-groups 3 --host-all
grub2-mkconfig -o /boot/grub2/grub.cfg
```

After you upgrade NetWitness Platform, ensure that you enable STIG-based FIPS Kernel controls.

**Note:** STIG-based FIPS Kernel controls which require modifications to kernel boot options are not enabled by NetWitness out-of-the-box.

## Task 7. (Optional). Verify Connection for Live Server

**Note:** This optional task is applicable to you only if you are upgrading NetWitness Platform through live.

Go to `admin/system/live services` and do a test connection to verify if you are able to connect to the live server as this is essential for the source-server from 12.x and above. This is an optional step and applicable only for customers who have configured live.

## Task 8. Synchronize Time on Component Hosts with NW Server Host

Before you upgrade hosts, make sure that the time on each host is synchronized with the time on the NetWitness Server.

**To synchronize the time, do one of the following:**

1. Configure the NTP Server.

For more information, see **Configure NTP Servers** in the System Configuration Guide.

2. Perform the following steps:

a. SSH to the Admin Server host.

b. Run the following commands.

```
salt \* service.stop chronyd
salt \* cmd.run "chronyc makestep"
salt \* service.start chronyd
```

# Perform Upgrade Tasks

**IMPORTANT:** You must run the pre-upgrade checks before performing the upgrade tasks. For more information on how to run the pre-upgrade checks, see Run Pre-Upgrade Checks

Upgrade the systems in your environment in the following order:

1. NW Server hosts
2. Analyst UI hosts
3. ESA Primary hosts
4. ESA Secondary hosts
5. Standalone Broker hosts
6. Concentrator hosts
7. Archiver hosts
8. Packet Decoder hosts
9. Log Decoder hosts
10. Log Collector / VLC hosts
11. The rest of your component hosts

**IMPORTANT:** NW Server, Analyst UI, and ESA Primary and Secondary hosts must all be upgraded on the same day. The rest of your component hosts can be upgraded on the same day or later. Make sure that you plan the upgrade process so that Correlation servers are upgraded immediately after the Admin Server is done. For more information, see "**Task 3. Prepare ESA Deployments for Migration to 12.4**" in the topic Prepare to Upgrade NetWitness Platform. Mixed mode is not supported for ESA hosts in NetWitness Platform. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

For information about all the host types in NetWitness, see the *NetWitness Hosts and Services Getting Started Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

**IMPORTANT:** After upgrading the primary NW Server (including the Respond Server service), the Respond Server service is not automatically re-enabled until after the Primary ESA host is also upgraded to same version. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

**Note:** For 12.4 version with Legacy Windows Log Collector, you should perform few additional post upgrade tasks. Refer to Legacy Windows Log Collection section in Perform Post Upgrade Tasks for these additional post upgrade tasks.

# Select Upgrade Options

You can select one of the following upgrade options based on your Internet connectivity. They are listed in the order recommended by NetWitness Platform.

- Option 1: Upgrade NetWitness Platform using Live Services
- Option 2: Upgrade NetWitness Platform Offline
- Option 3: Upgrade NetWitness Platform using CLI (Offline)
- Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages

The following rules apply when you are upgrading hosts using any of the 4 upgrade methods:

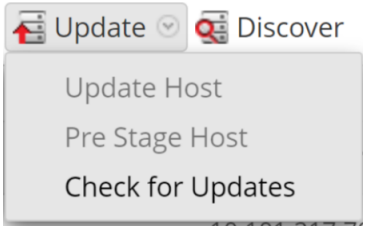
- You must upgrade the NW Server host first.
- You can only apply a version that is compatible with the existing host version.
- The NW Server, ESA primary, ESA secondary, and Analyst UI hosts must all be on the same NetWitness Platform version.

# Option 1: Upgrade NetWitness Platform using Live Services

You can use this method if the NW Server host is connected to Live Services.

**Caution:** You must review your network policy before downloading the upgrade package which is around 11.7 GB. If you have set up any policy that disallows file download beyond 10GB, the upgrade package download fails.

**Note:** You can pre-stage the upgrade repository using the **Pre Stage Host** feature. Refer the following figure. For more information, see Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages.

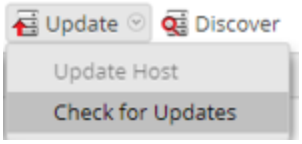



### Prerequisites

1. The **Automatically download information about new upgrades every day** option is selected and is applied in **(Admin) > System > Updates**.
2. Updates are available. Go to **(Admin) > Hosts > Update > Check for Updates** to check for updates. The Host view displays the **Update Available** status.
3. 12.4 is available in the **Update Version** column.

**To upgrade from 12.2.0.0, 12.2.0.1, 12.3.0.0, and 12.3.1.0 to 12.4:**

1. Go to **(Admin) > Hosts**.
2. Select the NW Server (`nw-server`) host.
3. Check for the latest updates.




Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.

4. Select **12.4** from the **Update Version** column.

**Note:**
- If you want to view a dialog with the major features in the upgrade and information on the updates, click the information icon ( ) to the right of the upgrade version number.

- If you cannot find the version you want, select **Update > Check for Updates** to check the repository for any available updates. If an update is available, the message "New updates are available" is displayed and the **Status** column updates automatically to show Update Available. By default, only supported updates for the selected host are displayed.

5. Click **Update** > **Update Host** from the toolbar.
6. Click **Begin Update**.
7. Click **Reboot Host**.
8. Repeat steps 5 to 7 for other hosts.

**Note:** You can select multiple hosts to upgrade at the same time only after updating and rebooting the NW Server host. All ESA, Endpoint, and Malware Analysis hosts should be upgraded to the same version as that of the NW Server host.

# Option 2: Upgrade NetWitness Platform Offline

You can manually upgrade NetWitness Platform by performing the following tasks.

## Task 1. Populate Staging Folder (`/var/netwitness/common/update-stage/`) with Version Upgrade Files. Do the following.

1. Download the upgrade package `netwitness-12.4.0.0.zip` from NetWitness Community (https://community.netwitness.com/) > **Downloads** > **NetWitness Platform** > **Version 12.4** to a local directory:
   - If you are upgrading from 12.2.0.0, 12.2.0.1, 12.3.0.0, and 12.3.1.0, download `netwitness-12.4.0.0.zip`.

2. SSH to the NW Server host.
3. Upload `netwitness-12.4.0.0.zip` to `/var/netwitness/common/update-stage/` on the NW Server Host.
   For example:

   ```
   mv /var/netwitness/tmp/netwitness-12.4.0.0.zip
   /var/netwitness/common/update-stage/
   ```

**Note:** NetWitness Platform unzips the file automatically.

## Task 2. Apply Upgrades from the Staging Area to Each Host. Do the following.

**Caution:** You must upgrade the NW Server host before upgrading any non-NW Server host.

1. Log in to NetWitness.
2. Go to  **(Admin) > Hosts**.

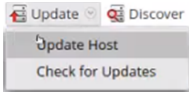
   **Note:** If you are already on the  **(Admin) > Hosts** page and the **Check for Updates** option (**Update** > **Check for Updates**) is grayed out, refresh the page from the browser to check for the updates.
3. Check for updates and wait for the upgrade packages to be copied, validated, and ready to be initialized.

   "Ready to initialize packages" is displayed if:

   - NetWitness Platform can access the upgrade package.
   - The package is complete and has no errors.

   Refer to Troubleshooting Version Installations and Updates for instructions on how to troubleshoot errors (for example, "Error deploying version <version-number>" and "Missing the following update package(s)," are displayed in the **Initiate Update Package for RSA NetWitness Platform** dialog.)
4. Click **Initialize Update**.

   It takes some time to initialize the packages because the files are large and need to be unzipped. The time varies depending on how the host is configured.
   After the initialization is successful, the **Status** column displays Update Available.
5. Click **Update** > **Update Hosts** from the toolbar.

   
   
6. Click **Begin Update** from the **Update Available** dialog.
   After the host is upgraded, it prompts you to reboot the host.
7. Click **Reboot Host** from the toolbar.

# Option 3: Upgrade NetWitness Platform using CLI (Offline)

You can use this option if the NW Server host is not connected to Live Services.

### Before you begin

Make sure that you have downloaded the following file from NetWitness Community (https://community.netwitness.com/) > **Products > NetWitness Platform** > **Downloads** to a local directory:

- If you are upgrading from 12.2.0.0, 12.2.0.1, 12.3.0.0, and 12.3.1.0 to 12.4, download:

  `netwitness-12.4.0.0.zip`

- If you are using external repository, you can update the external repository with the latest upgrade content. For more information, see External Repo Instructions for CLI upgrade.

### To upgrade NW Server Hosts and component servers:

**Note:** If you copy and paste the commands from PDF to Linux SSH terminal, the characters do not work. However, you can copy the commands from the HTML page https://community.netwitness.com/t5/netwitness-platform-online/upgrade-tasks-for-12-1-1/ta-p/695018#Option3 and paste them to Linux SSH terminal.

1. Stage the 12.4.0.0 files to prepare them for the upgrade. Consider the following scenarios.
   - **Option 1 (Manual)** : Log into the NetWitness Server and create the following directory:

     `/var/netwitness/tmp/upgrade/12.4.0.0/`
     Then copy the package zip file to the `/var/netwitness/tmp/` directory of the NW Server and extract the package files from `/var/netwitness/tmp/` to the appropriate directory using the following command:

     `unzip netwitness-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
     Make sure you remove the update zip file from the staging directory after it is extracted.

   - **Option 2 (Automated)** : Log into the NetWitness Server and create the following directory:
     `/var/netwitness/tmp/upgrade/`
     Then copy the NetWitness 12.4.0.0 package zip files to the `/var/netwitness/tmp/` directory on the NetWitness Server.
     After this, run the below command to extract, validate, and initialize the 12.4.0.0 zip files:
     `[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.4.0.0`
     Once the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed** is displayed in the console of the admin server, only then the initialization process will begin.

   **Note:** If you do not receive the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed**, run the previous command again.

   **IMPORTANT:** After staging 12.4.0.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`. If the initialization succeeds, ignore the step 2 Initialize the upgrade below and proceed with the further steps 3-6.

2. Initialize the upgrade using the following command:
   `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`
3. Upgrade the NW Server host, using the following command:
   `upgrade-cli-client --upgrade --version 12.4.0.0 --host-key <ID / display name / (hostname/ IP address)>`

   **Note:** Once the upgrade is triggered, NW Server will reboot automatically ~10 mins into the upgrade process. It will boot into the new kernel (4.18 for Alma Linux 8.9).

   **Caution:** Users are advised to wait until the UI is up and running, which may take up to an hour to complete. After 20 to 30 minutes of the migration, you can SSH and check if the OS is migrated. Once the OS migration is complete, it may take at least 30 minutes for the UI to appear as the NW Upgrade runs in the background.

   The above upgrade process can be tracked through a virtual console for VMs or remote console for servers with iDRACs.

   Once the OS is migrated and able to SSH to Admin Node, run the following command on the host to confirm successful OS migration:

   - `cat /etc/redhat-release`
   - `AlmaLinux release 8.9 (Midnight Oncilla)`

   **Caution:** After the OS migration, reinstall any third-party RPMs you have previously installed.
4. Once the orchestration-server is up, it will automatically trigger the NW Upgrade through chef to the desired NW Version. To check the progress of this, please SSH to the Admin Server and run the following command:

   - `orchestration-cli-client --check-admin-upgrade-status`

   **Note:** Run the above command only for NW Admin Server.
5. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
6. (Conditional) If Warm Standby Server is deployed, repeat steps 1 to 5 on the Warm Standby Server host.
7. Repeat steps 3 and 5 for each component host, changing the IP address to the component host which is being upgraded.

**Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on the NW Server host. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

## External Repo Instructions for CLI upgrade

For information about setting up an external repository, see **Appendix A. Set Up External Repo** in the *12.4Upgrade Guide for NetWitness Platform*. The following instructions assume that you already have an external repository set up. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

1. Stage the 12.4.0.0 files to prepare them for the upgrade. Consider the following scenarios.

   - **If you are upgrading from 12.2.0.0**, **12.2.0.1**, **12.3.0.0**, and **12.3.1.0**, you only need to stage 12.4.0.0.
     - **Option 1 (Manual)** : Log into the NetWitness Server and create the following directory:

       `/var/netwitness/tmp/upgrade/12.4.0.0/`
       Then copy the package zip file to the `/var/netwitness/tmp/` directory of the NW Server and extract the package files from `/var/netwitness/tmp/` to the appropriate directory using the following command:

       `unzip netwitness-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
       Make sure you remove the update zip file from the staging directory after it is extracted.
     - **Option 2 (Automated)** : Log into the NetWitness Server and create the following directory:
       `/var/netwitness/tmp/upgrade/`
       Then copy the NetWitness 12.4.0.0 package zip files to the `/var/netwitness/tmp/` directory on the NetWitness Server.
       After this, run the below command to extract, validate, and initialize the 12.4.0.0 zip files:
       `[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.4.0.0`
       Once the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed** is displayed in the console of the admin server, only then the initialization process will begin.

   **Note:** If you do not receive the message **(INFO) Download and extraction of all the necessary NetWitness zips are completed**, run the previous command again.

   **IMPORTANT:** After staging 12.4.0.0 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`. If the initialization succeeds, ignore the step 2 Initialize the upgrade below and proceed with the further steps 3-6.

2. Initialize the upgrade using the following command:
   `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`

3. Upgrade the NW Server host, using the following command:
   `upgrade-cli-client --upgrade --version 12.4.0.0 --host-key <ID / display name / (hostname/ IP address)>`

   **Note:** Once the upgrade is triggered, NW Server will reboot automatically ~10 mins into the upgrade process. It will boot into the new kernel (4.18 for Alma Linux 8.9).

**Caution:** Users are advised to wait until the UI is up and running, which may take up to an hour to complete. After 20 to 30 minutes of the migration, you can SSH and check if the OS is migrated. Once the OS migration is complete, it may take at least 30 minutes for the UI to appear as the NW Upgrade runs in the background.

The above upgrade process can be tracked through a virtual console for VMs or remote console for servers with iDRACs.

Once the OS is migrated and able to SSH to Admin Node, run the following command on the host to confirm successful OS migration:

- `cat /etc/redhat-release`
- `AlmaLinux release 8.9 (Midnight Oncilla)`

**Caution:** After the OS migration, reinstall any third-party RPMs you have previously installed.

4. Once the orchestration-server is up, it will automatically trigger the NW Upgrade through chef to the desired NW Version. To check the progress of this, please SSH to the Admin Server and run the following command:
   - `orchestration-cli-client --check-admin-upgrade-status`

   **Note:** Run the above command only for NW Admin Server.
5. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
6. (Conditional) If Warm Standby Server is deployed, repeat steps 1 to 5 on the Warm Standby Server host.
7. Repeat steps 3 and 5 for each component host, changing the IP address to the component host which is being upgraded.

**Note:** You can check versions of all the hosts, using the command `upgrade-cli-client --list` on the NW Server host. If you want to view the help content of `upgrade-cli-client`, use the command `upgrade-cli-client --help`.

# Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages

You can pre-stage the upgrade repository by downloading the required packages (.zip) without affecting the system. This minimizes the upgrade downtime and ensures the upgrade is completed within the planned time.

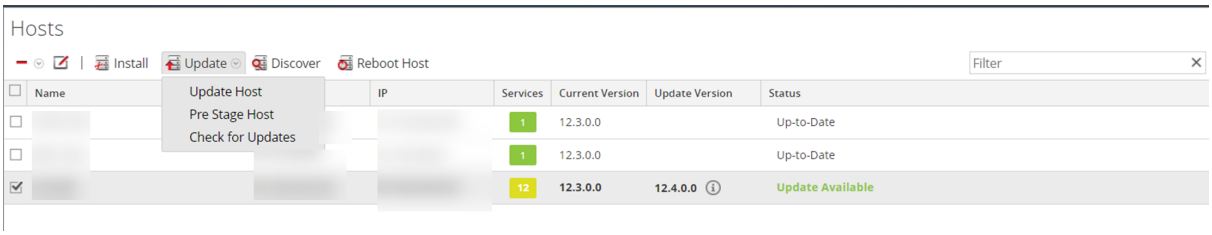
### To pre-stage the upgrade repository and update the hosts:

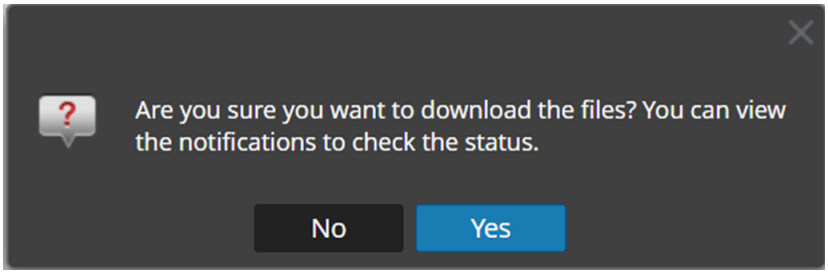
1. Go to  **(Admin) > Hosts**.
2. Click **Update > Check for Updates** from the toolbar.

   All possible update versions will be displayed in the Versions drop-down list.

3. Click **Update** > **Pre Stage Host** and select the version in the update version column.

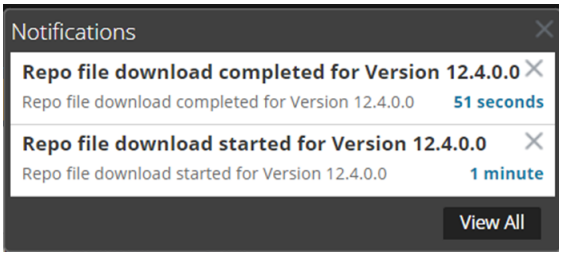
   A confirmation message for downloading the files is displayed.




4. Click **Yes** to download the upgrade packages to the repo.
5. Verify the status of the download in the notifications tray as shown below.

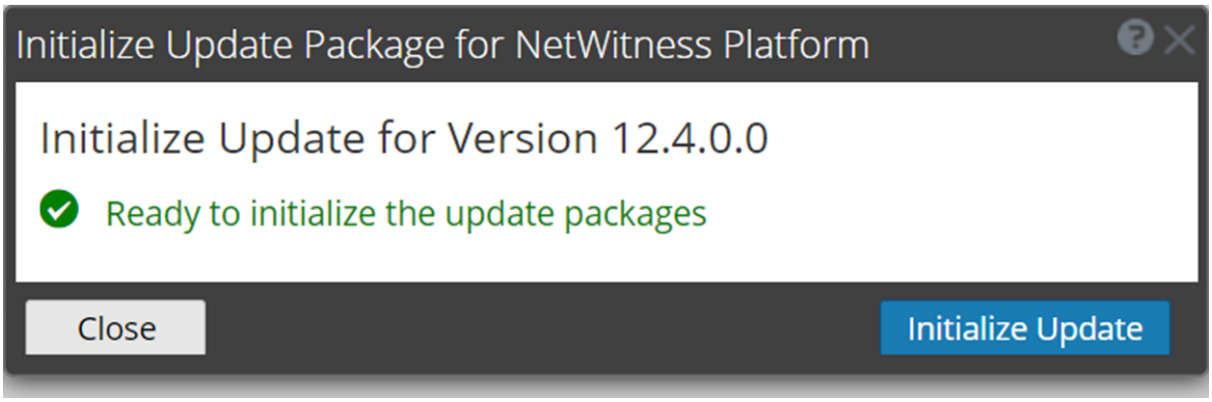
   The **Pre Stage Host** and **Upgrade Host** will be disabled until pre stage is completed.




> **Note:** The current version and the update version in the UI will be the same during the pre stage as it is not the actual update. This is because only the repo files are downloaded and no actual upgrade is done. The version will change only after upgrade.

6. If the download is successful, **Check for Updates** again to start the initialization.
7. Click **Initialize Update**.

   The initialization of the package will take some time as the files are large and will need to be unzipped.




**IMPORTANT:** Pre Stage Repo preparation steps from 1 to 4 can be performed at any time. However, from steps 5 to 8 the upgrade process begins and you must NOT reboot the host or restart the jetty server during this time as it will corrupt the .ZIP files.

8. Check the status of initialization in the notifications tray.
9. After the initialization is completed successfully, click **Update** > **Update Host**.

   After the host is updated, you will be prompted to reboot the host.
10. Set up the host and reboot the host.

# Perform Post Upgrade Tasks

This topic lists the tasks you must perform after upgrading NetWitness Platform. Complete the tasks that apply to the hosts in your environment.



## General

You must configure Jetty, restore the core services contents, and also start Network capture, Log capture, and aggregation after upgrading NetWitness Platform.

### Configure Jetty

For Jetty Configuration and related information, see **Manage Custom Host Entries** topic in the System Maintenance Guide.

### Make Sure Services Have Restarted and Are Capturing and Aggregating Data

Make sure that services have restarted and are capturing data (this depends on whether or not you have auto-start enabled).

If required, restart data capture and aggregation for the following services:

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

#### To Start Network Capture:

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.
   The **Services** view is displayed.
2. Select each **Decoder** service.

3. Under  (actions), select **View** > **System**.
4. In the toolbar, click 


**To Start Log Capture:**

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.
   The **Services** view is displayed.
2. Select each **Log Decoder** service.
3. Under  (actions), select **View** > **System**.
4. In the toolbar, click 


**To Start Aggregation:**

1. In the NetWitness Platform menu, go to  (Admin) > **Services**.
   The **Services** view is displayed.
2. For each **Concentrator**, **Broker**, and **Archiver** service:
   a. Select the service.
   b. Under  (actions), select **View** > **Config**.
   c. In the toolbar, click 

3. For Event Stream Analysis (ESA):

   **Note:** Mixed mode is not supported for ESA hosts. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

   There are no required post-upgrade tasks for ESA. For ESA troubleshooting, see ESA Troubleshooting Information.

   If you want to add support for Endpoint, UEBA, and Live content rules, you must update the `multi-valued` and `single-valued` parameter meta keys on the ESA Correlation service to include all the required meta keys. It is not necessary to make these adjustments during the upgrade; you can make the adjustments later at a convenient time. For detailed information and instructions, see **Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys** in the ESA Configuration Guide.

## Restore the Core Services Contents

Once you upgrade to 12.4, the Core services Contents such as Configuration files (.cfg), Feeds, Parsers, and Log Devices are copied to the **.tar** location of the respective components such as Decoder, Log Hybrid, Network Hybrid, and Log Decoder.

The following table lists the Core Services Contents paths and the **.tar** location of the respective components where the Core Services Contents are copied.

| Core Services Contents Paths | Components | .tar location of the Components |
|---|---|---|
| /etc/netwitness/ng/feeds (Feeds) | Decoder | /var/netwitness/decoder/decoder_backupcontent_ccm.tar |
| /etc/netwitness/ng/parsers (Parsers) | Log Hybrid | /var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar |
| /etc/netwitness/ng/envision/etc/devices (Log Devices) | Network Hybrid | /var/netwitness/decoder/decoder_backupcontent_ccm.tar |
| /etc/netwitness/ng/NwDecoder.cfg (Configuration files (.cfg)) | Log Decoder | /var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar |

By default, CCM option is disabled. After upgrading to 12.4, if you enable CCM and encounter the loss of the Core Services Contents, you can use the backup tar files to recover the lost data. For more information, see https://community.netwitness.com/t5/netwitness-knowledge-base/automatic-backup-of-core-service-content-after-upgrading-core/ta-p/694527.

## Event Stream Analysis (ESA)

After upgrading to the 12.4 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 12.4 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. Verify if all the ESA deployments are in a healthy state. For more information, see **View a Deployment** topic in the *Live Services Management Guide*.

**Note:** Analysts must have appropriate permissions to view the ESA rules under (**CONFIGURE**) > **ESA Rules** and (**CONFIGURE**) > **Policies** pages. For more information, see the **Source-server** section in the **Role Permissions** topic in the *System Security and User Management Guide*.

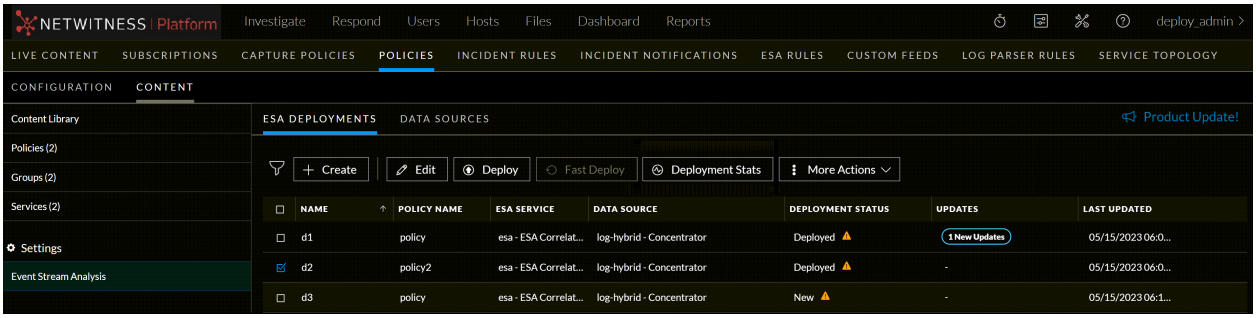
The pre-upgrade and post-upgrade states of deployments are represented in the following table.

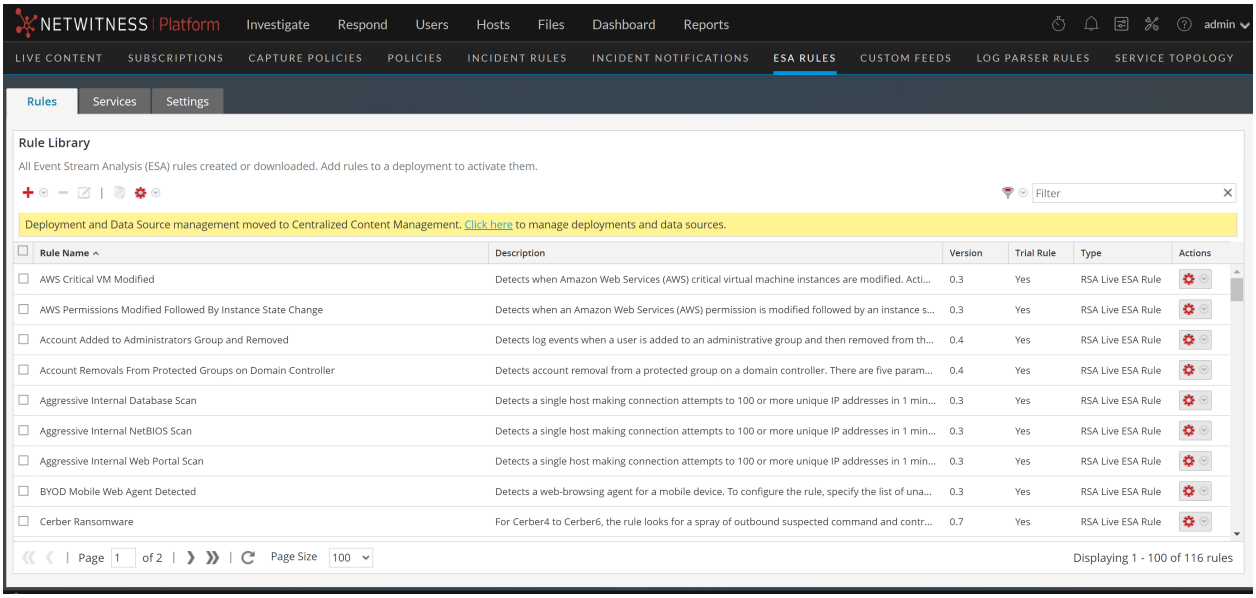
| SINo | Pre-upgrade Deployment State | Post-upgrade Deployment State | | |
|---|---|---|---|---|
| | | Creates Policy | Creates Group | The policy will be Published |
| 1 | Healthy deployment | Yes | Yes | Yes |
| 2 | Deployment with errors | Yes | Yes | Yes |
| 3 | Deployment with only rules | Yes | No | No |
| 4 | Deployment with no rules | No | No | No |

(Optional) Using the **Merge Policy** button, you can merge a policy having ESA content with a policy with no ESA content. For more information, see **Merge Policy with ESA Content** topic in the *Live Services Management Guide*.

## Manage ESA Deployments and Data Sources

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. You can only manage the ESA Rules in the **ESA Rules** page. Refer the following figures.




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

## Migrate custom scripts for notifications

- Since there are a wide range of changes regarding the file permissions and ownership attributes of custom script files of the **Script Notifications** feature (**ADMIN** > **System** > **Global Notifications** > **Script**), Netwitness suggests having a backup of the custom scripts before the system is upgraded to 12.4
- Once the upgrade is completed, each script needs to be revisited for syntactic/semantic changes that have to be done.

- Even if the custom script in NetWitness versions prior to 12.4 is accessing any file resources in the /tmp or /var/tmp folder, they cannot be accessed further since the ownership with which the custom script executes has been changed. The suggestion for this scenario is to tweak/modify the custom script to create/read from a new file in **/tmp** or **/var/tmp** directory.

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

# Respond

The Primary ESA server must be upgraded to 12.4 before you can complete the following task.

**Note:** After upgrading the primary NW Server (including the Respond Server service), the Respond Server service is not automatically re-enabled until after the Primary ESA host is also upgraded to 12.4. The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

## (Conditional) Restore Any Respond Service Custom Keys in the custom_normalize_alerts.js and support new datasource

**Note:** If you did not manually customize the custom_normalize_alerts.js, you can skip this task. We attempt to automatically migrate the custom keys. However in case of failures, use this step to verify the custom data's integrity.

If you added custom keys in the `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` file for use in custom normailization, modify the `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` file and add the custom normalized keys from the automatic backup file. The backup file is located in `/var/netwitness/respond-server/scripts` and it is in the following format:

`custom_normalize_alerts.js.bak-<time of the backup>`

In case of automatic update of the script fails, add support for Netwitness Core and NetWitness Insight by updating the `custom_normalize_alerts.js` file manually to support these new sources in respond.

# User and Entity Behavior Analytics

Complete the following tasks after upgrading UEBA to 12.4.

1. Update the UEBA configuration using the following command from the UEBA machine.
   - `source /etc/sysconfig/airflow`
   - `source $AIRFLOW_VENV/bin/activate`
   - `python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio_workflows-1.0-py3.9.egg/presidio/resources/rerun_ueba_server_config.py`
   - `deactivate`

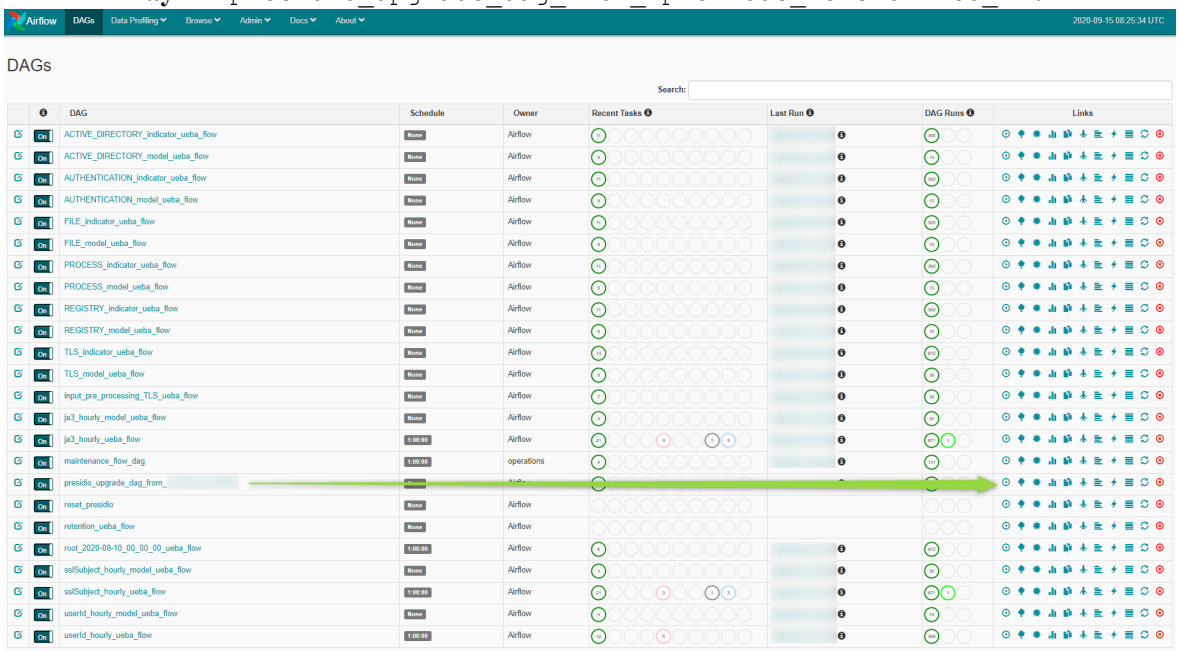
2. (Optional) Update the UEBA processing schema, if needed.

   NetWitness recommends that the UEBA start date is set to 28 days earlier than the current date. For UEBA systems that intend to process TLS data, you must make sure that the start date is set to no later than 14 days earlier than the current date.

   For more information, see the "reset-presidio script" section in the *UEBA Configuration Guide*.

3. Run the airflow upgrade DAG.

   - Go to Airflow main page `https://<UEBA-host-name>/admin`
   - Enter the admin username and password.
   - Click the **Play** in `presidio_upgrade_dag_from_<previous_version> to_12.4`.



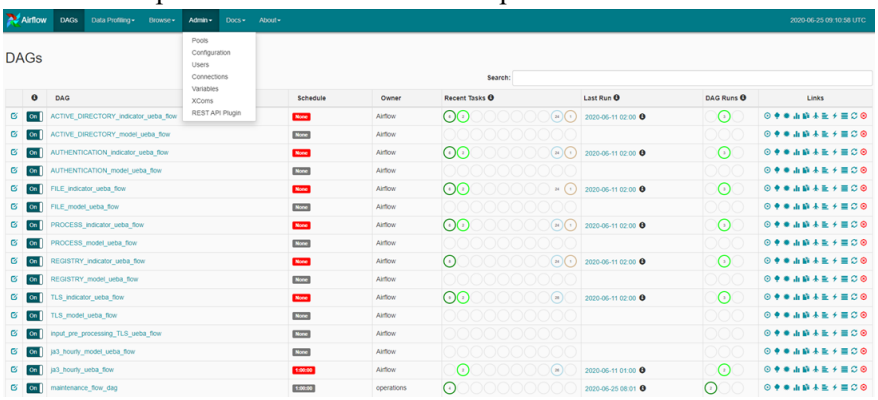

   **Note:** A light green circle will appear next to the upgrade DAG row during the upgrade. If the upgrade process is completed successfully the light green circle changes to green. If the upgrade process fails, the light green circle changes to red.

4. Set the appropriate "Boot Jar Pools" slots:

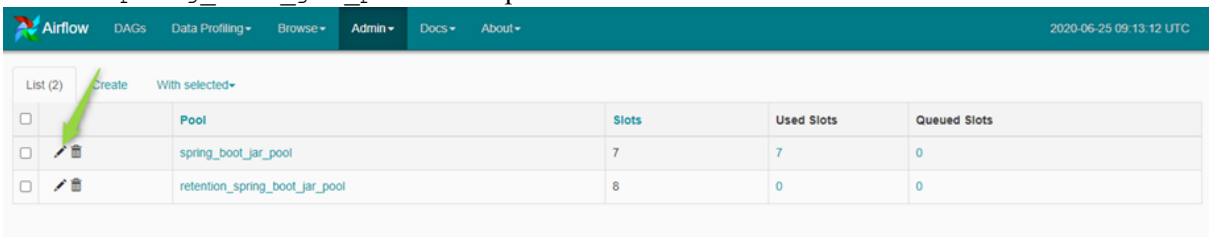
   - **Physical Appliance**: Update the `spring_boot_jar_pool` slot value be 18.
   - **Virtual Appliance**: Update the `spring_boot_jar_pool` slot value to 22.
     To update the **Spring Boot Jar Pools** slots, go to the Airflow main page, tap the **Admin** tab at the top bar and tap **Pools**.

   a. To access the Airflow UI, go to `https://<UEBA_host>/admin` and enter the credentials.
      User: admin
      Password: The environment deploy admin password.

b. Click on the pencil mark of the Pools to update the slot values.




5. Edit the `spring_boot_jar_pool` and update the slots amount to 22.




# Legacy Windows Log Collector

## Refresh Legacy Windows Log Collector Certificates with Updated SA Certificates

**Post Upgrade Steps:**

1. Execute the following command in SA:

   a. `wlc-cli-client --host-display-name` **`hostDisplayName`** `--service-display-name` **`serviceDisplayName`** `--host` **`WLChostIPAddress`** `--port 50101 --use-ssl false`

   Enter following information:

   i. **Legacy Windows Log Collector REST Username and Legacy Windows Log Collector REST Password**: Enter the admin credentials for the Legacy Windows Log Collector.

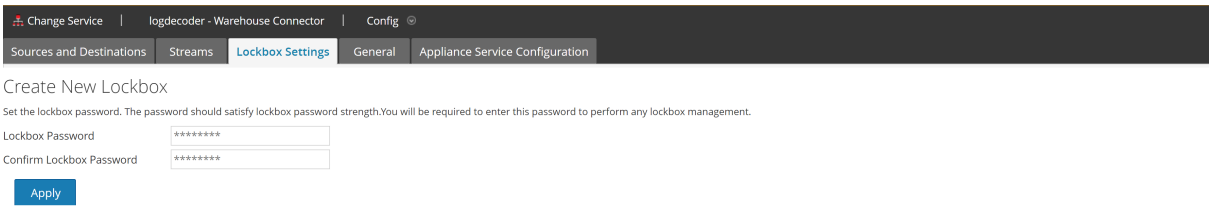
   ii. **Security Server Username and Security Server Password**: Enter admin credentials for NetWitness.

2. Restart the system.

# Warehouse Connector

The Warehouse connector uses a lockbox to store credentials securely for data integration sources and destinations. However, users upgrading from earlier versions to the 12.4 version cannot start the configured streams without migrating their existing credentials in the new lockbox. As a result, users must manually create a new lockbox key and then refresh the password for their sources and destinations configured in Warehouse Connector, wherever applicable, using the following steps :

1. Log in to the NetWitness Platform.
2. Navigate to **(Admin)** > **Services**.
3. In the **Services** view, select the added Warehouse Connector service, and select > **View** > **Config**.
4. In the Services Config view of Warehouse Connector, click the **Lockbox Settings** tab and create a fresh lockbox key.




5. Reauthorize the user account in source configurations using **Explore** or **REST API**. Reauthorization of source user account is not available in UI. The command to reauthorize the user account from **Explore** is given below:

   ```
   > /warehouseconnector/sources/<source:port> ---> setPass property with password=<password of the configured user in source>
   ```

6. Reauthorize the user account in SFTP destination configuration from **UI**, **Explore** or **REST API**. The command to reauthorize the password from **Explore** is given below:

   ```
   > /warehouseconnector/destinations/<sftp_destination> ---> setPass property with password=<password of the configured user in SFTP destination>
   ```

7. If NFS directory mount was removed as part of pre-upgrade step, mount back the same configuration. Additionally, enable back the mount entry in */etc/fstab*.

```
> mount -t nfs -o nolock,tcp,hard,intr <IP_Address_for_SAW>:/mapr/<cluster-name> /<directory_name>
```

Where **<IP_Address_for_SAW>** is the IP address of the primary Warehouse appliance in the cluster and **<cluster-name>** is the name provided in the template file.

# Setting Recovery Password for Lockbox

After upgrading all the Log Collectors and WLC in the NW deployment to 12.4.0.0, administrator should execute the **Recovery Password Utility** using SATools. This tool sets the Lockbox recovery password for all the log collector services (version 12.4 or above) within the deployment. Administrators are advised to keep a note of the Lockbox recovery password as required during disaster recover scenarios.

To set the recovery password, the administrator should SSH into **Admin Server(Node 0)** and execute the utility **set-lockbox-password** from the path `/opt/rsa/saTools/bin/set-lockbox-password`. Administrators should enter the new password to be set as recovery password for the Lockbox available in all the Log Collectors.

**Note:** On re-executing the utility and setting an updated Lockbox, the recovery password will reset the password for all the applicable log collector services (version 12.4 and above).

```
[root@adminserver ~]# cd /opt/rsa/saTools/bin
[root@adminserver bin]# ll
total 68
-rwx------. 1 root root  3224 Dec 10 11:38 category-toggle
-rwx------. 1 root root   699 Dec 10 11:38 dkms-recompile
-rwx------. 1 root root  4719 Dec 10 11:38 external-repo-creator
-rwx------. 1 root root 12029 Dec 10 11:38 schedule-standby-admin-data-sync
-rwx------. 1 root root  5037 Dec 10 11:38 set-deploy-admin-password
-rwxrwxrwx. 1 root root  3071 Dec 21 13:28 set-lockbox-password
-rwx------. 1 root root 18074 Dec 10 11:38 sosreport-select-plugins
-rwx------. 1 root root  4762 Dec 10 11:38 ueba-server-config
[root@adminserver bin]# ./set-lockbox-password
Enter the Lockbox password to be set:
Please re-enter the password
Lockbox operation in progress...
Setting lockbox password for 10.125.245.116 : Success
Setting lockbox password for 10.125.245.105 : Success
Setting lockbox password for 10.125.245.114 : Success
Lockbox password is already set for log-collector :
'"logcollector":10.125.245.116'
'"logdecoder":10.125.245.105'
'"endpointloghybrid1":10.125.245.114'
[root@adminserver bin]#
```

# Perform Sanity Checks After Upgrade

You must perform the following sanity checks after upgrading to NetWitness 12.4.

1. Go to (Admin) > **Services** view to verify that all the services are active (appearing in green) after upgrade.
2. Verify that the services are upgraded to match the host version. The service version in (Admin) > **Services** view must match the host version in (Admin) > **Hosts** view after upgrade.
3. In the (Admin) > **Services** view, do the following.
   - Select a Log Collector service and go to (actions) > **View** > **System** view to verify if the required logs collection is started. You should click the Collection drop-down option and go to the right collection protocol to check if the logs collection is started. If the required collection is not started, select Start next to the required collection protocol from the list to start the collection.
   - Select a Log Decoder service and go to (actions) > **View** > **System** view to verify if the Log Decoder is capturing the logs properly.
   - Select a Packet Decoder service and go to (actions) > **View** > **Config** view to check if the capture interface is configured under **Decoder Configuration** section. If the capture interface is not configured, you must select the required capture interface from the drop-down list to configure it. If the capture interface is already configured, go to the (actions) > **View** > **System** view of the Packet Decoder and check if the capture is started. If the capture is not started, click Start Capture to start the packet capture.
4. Go to (Admin) > **Services** > Select a Log Decoder or Packet Decoder service > (actions) > **View** > **Stats** > **General** view to analyze the current capture rate.
5. Verify that the Concentrators, Archivers, and Brokers are aggregating the data. Make sure that you can investigate from each Concentrator, Archiver, and Broker to validate that it is operational.
6. Go to **Respond** > **Alerts** view to verify if the alerts are triggering from different sources.
7. Go to (Admin) > **Health & Wellness** > **Alarms** view and verify if the SMS server is up and running.
8. Go to (Admin) > **Event Sources** > **Monitoring Policies** view and verify if the policies configured before upgrade are appearing.
9. Go to (Admin) > **Health & Wellness** > **New Health & Wellness** > **Pivot to Dashboard** > **Elastic** > **Dashboard** view and ensure the following.
   - The visualizations you created before upgrade still exist.

- The metric server is up and running.
- Alerts are generated properly for the monitors you have configured before upgrade.

# Install the 12.4 Relay Server

**IMPORTANT:** Post upgrading EPLH from 12.2.x.x and 12.3.x.x versions to 12.4, you must re-install the relay server on EL 8 (Alma Linux) box since relay server is a standalone server.

### Before you begin

- Make sure you have the EL 8 box.
- Perform the following tasks before installing the 12.4 Relay server:
  1. Upgrade NetWitness Platform XDR.
  2. Once the EPLH is upgraded, download the relay packager.
  3. Copy the packager to EL 8 box.
  4. Turn off the existing Relay server.
  5. Configure the IP address of EL 8 by re-using the IP address of the existing Relay server.

     Once you configure the IP address of EL 8, install the Relay server. For more information, see **(Optional) Installing and Configuring Relay Server** section in the Endpoint Configuration Guide. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

**Note:** You must keep the security patches up to date on the Relay Server.

# Upgrade Endpoint Agents

See **Upgrade Agents** in the Endpoint Agent Installation Guide for NetWitness Platform for instructions on how to upgrade the agents.

# Troubleshoot Upgrade Issues

This section describes the error messages displayed in the Hosts view when it encounters problems updating host versions and installing services on hosts in the Hosts view. If you cannot resolve an upgrade or installation issue using the following troubleshooting solutions, contact Customer Support.

Troubleshooting instructions for the following errors that may occur during the upgrade are described in this section.

- AlmaLinux OS Troubleshooting Information
- deploy_admin Password Expired Error
- Downloading Error
- Error Deploying Version <version-number> Missing Update Packages
- Upgrade Failed Error
- External Repo Update Error
- Host Update Failed Error
- Missing Update Packages Error
- Patch Update to Non-NW Server Error
- Reboot Host After Update from Command Line Error
- Reporting Engine Restarts After Upgrade

Troubleshooting instructions are also provided for errors for the following hosts and services that may occur during or after an upgrade.

- Log Collector Service
- NW Server
- Orchestration
- Reporting Engine
- Event Stream Analysis
- Legacy Windows Log Collector

| | |
|---|---|
| **Problem** | Unable to boot the appliance after upgrading |
| **Wokaround** | 1. Manually modify the GRUB boot line to `FIPS=0` to get it to boot.<br>2. From here, disable FIPS using the following command:<br>`manage-stig-controls --disable-control-groups 3 --host-all`<br>3. Verify the line `FIPS=1` is removed from `/boot/grub2/grub.cfg`<br>• If not, run the following command: |

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reboot.
5. Run the following command to enable FIPS:

   ```
   manage-stig-controls --enable-control-groups 3 --host-all
   ```

6. Reboot again.

## AlmaLinux OS Troubleshooting Information

For better understanding, AlmaLinux OS Upgrade can be divided into 4 parts:

1. Running the precheck utility to ensure the health of the system and detect any upgrade issues. This can be done any time before the upgrade using the standalone precheck-tool rpm. (required only on NW Server)

   Logs are recorded here - `/var/log/netwitness/precheck-tool/checklist.log`

2. Initialization or init phase (happens only on NW Server)

   For any issues during init phase, check these logs.

   - salt minion logs - `/var/log/salt/minion`
   - deployment-upgrade logs - `/var/log/netwitness/deployment-upgrade/chef-solo.log`

   **Note:** Please perform the init only when you plan to do the actual upgrade. It is not recommended to perform an init without upgrading the system in the same change window.

3. OS Upgrade from CentOS to AlmaLinux

   As the first step of OS Upgrade, salt gets upgraded. You can execute the below command to see that salt is upgraded to version 3006:

   ```
   cat /var/log/yum.log | grep salt
   ```

   You can view similar to the below update where xxx represents the current datetime stamp:

   ```
   xxx Updated: salt-master-3006.2-0.x86_64
   xxx Updated: salt-api-3006.2-0.x86_64
   xxx Updated: salt-minion-3006.2-0.x86_64
   ```

   For any issues, with salt-upgrade, please check:

   - /var/log/netwitness/node-infra-server/node-infra-server.log
   - /var/log/salt/master
   - /var/log/salt/minion

   Once salt has been upgraded, the leapp process will begin.

   The logs can be viewed in `/var/log/salt/minion`:

   ```
   xxx [salt.loaded.ext.module.nw_platform:445 ][INFO ][139407] [1/5]
   Searching for leapp config for version: 12.4.0.0
   ```

```
xxx [salt.loaded.ext.module.nw_platform:453 ][INFO ][139407] [2/5]
Retrieving leapp config for version: 12.4.0.0

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'config/12.4.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:467 ][INFO ][139407] [3/5] Running
pre-requisites required to perform leapp upgrade

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/actor.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/libraries/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/addupgradebootentry.py'

xxx [salt.loaded.ext.module.nw_platform:500 ][INFO ][139407] [4/5] Running
leapp pre-upgrade

xxx [salt.loaded.ext.module.nw_platform:503 ][INFO ][139407] [5/5] Running
leapp upgrade
```

For any issues encountered during OS Upgrade, the logs below will be helpful in troubleshooting.

- `/var/log/salt/minion`
- If Preupgrade fails - `/var/log/leapp/leapp-preupgrade.log`
- If Leapp upgrade fails - `/var/log/leapp/leapp-upgrade.log`

If leapp fails, then `/var/log/leapp/leapp-report.txt` will provide you with details about inhibitors.

A few minutes after this log “Running leapp upgrade” in /var/log/salt/minion, the system will reboot and may take 20 to 30 minutes to return.

Once it is up, you can confirm the OS using the command cat `/etc/almalinux-release`. If it does not show Alma Linux release, please call Customer Support before taking any action.

Also, if you have triggered the upgrade through UI and see the status "`Performing OS Migration`" on any NodeX for more than an hour, please check the leapp logs and reach out to Customer Support.

4. NW Software upgrade to 12.4

   Once the OS Migration has completed, The NW software upgrade begins and takes up to 30 min before the UI is functional.

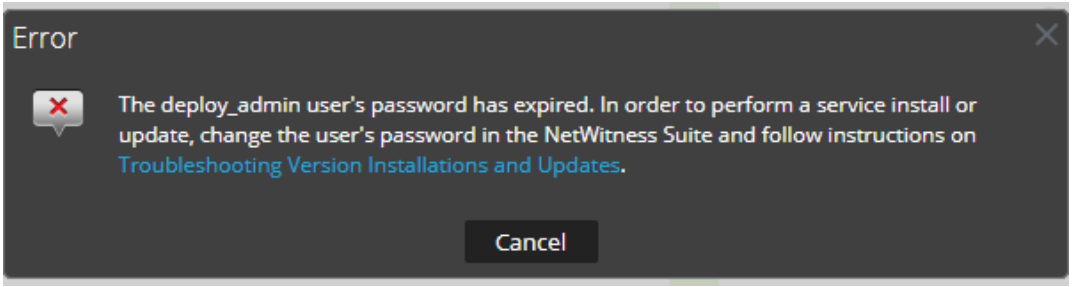
   You can see these logs in `/var/log/salt/minion` when NW software upgrade starts:

```
xxx [salt.loaded.ext.module.nw_platform:276 ][INFO ][14035] Preparing node
for upgrade to 12.4.0.0

xxx [salt.loaded.ext.module.nw_platform:280 ][INFO ][14035] [1/2] Searching
for yum config for version: 12.4.0.0

xxx [salt.loaded.ext.module.nw_platform:287 ][INFO ][14035] [2/2]
Retrieving yum config for version: 12.4.0.0
```

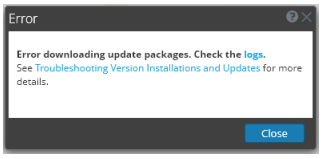
```
xxx [salt.fileclient :1333][INFO ][14035] Fetching file from saltenv
'base', ** done ** 'config/12.4.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading chef
package

xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading rsa-
nw-config-management package
```

You can also refer to config management logs at `/var/log/netwitness/config-management/chef-solo.log` or UI logs `/var/netwitness/uax/logs/sa.log`

# deploy_admin User Password Has Expired Error

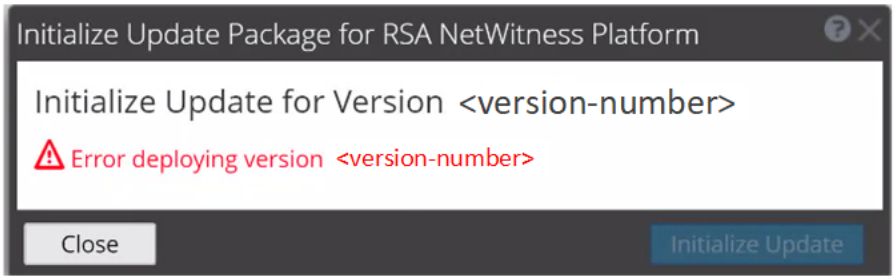
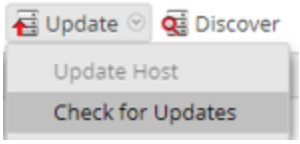
| | |
|---|---|
| **Error Message** |  |
| **Cause** | The `deploy_admin` user password has expired. |
| **Solution** | Reset your `deploy_admin` password password. Do the following.<br>1. On the NW Server host only, run the following command.<br>`nw-manage --update-deploy-admin-pw`<br>`Please enter the new deploy_admin account password: <new-deploy-admin-password>`<br>`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`<br>2. Review the output of the `nw-manage --update-deploy-admin-pw` command to verify the `deploy_admin` password was successfully updated on all hosts. If an NW host is down or fails for any reason as displayed by the output of the `nw-manage --update-deploy-admin-pw` command, run `nw-manage --sync-deploy-admin-pw --host-key <host-identifier>` to synchronize the password between the NW Server and the host that failed once the communication failure is resolved.<br>3. On the host that failed installation or orchestration, run the `nwsetup-tui` command and use the new **deploy_admin** password in response to the **Deployment Password** prompt. |

# Downloading Error

| | |
|---|---|
| **Error Message** |  |
| **Problem** | When you select an update version and click **Update** >**Update Host**, the download starts but fails to complete. |
| **Cause** | Version download files can be large and take a long time to download. If there are communication issues during the download it will fail. |
| **Solution** | 1. Try to update again.<br>2. If it fails again with the same error, try to update using the offline methods as described in "Offline Method from Hosts View" or "Offline Method Using Command Line Interface" in the *Upgrade Guide for NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.<br>3. If you are still not able to update, contact Customer Support. |

| | |
|---|---|
| **Error Message** | If you are upgrading the NetWitness Platform to the latest version, offline UI upgrade fails with the Download error message. |
| **Solution** | 1. In the Command Line Interface (CLI), do the following:<br>a. SSH to NW Server.<br>b. Run the following command:<br>`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version <version number>`<br>**`For example:`**<br>`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 12.4.0.0`<br>2. After the NW Server is successfully updated, log in to the NW Server user interface and go to **(Admin) > Hosts**, where you are prompted to reboot the host.<br>3. Click **Reboot Host** from the toolbar.<br>**To upgrade all the other hosts directly from the user interface:**<br>1. Click **Begin Update** from the **Update Available** dialog.<br>After the host is upgraded, it prompts you to reboot the host.<br>2. Click **Reboot Host** from the toolbar. |

## Error Deploying Version <version-number> Missing Update Packages

| | |
|---|---|
| **Error Message** |  |
| **Problem** | Error deploying version <version-number> is displayed in the **Initialize Update Package for NetWitness Platform** dialog after you click on **Initialize Update** if the update package is corrupted. |
| **Solution** | 1. Click **Close** to close the dialog.<br>2. Remove the version folder from staging folder.<br>3. Make sure that the salt-master service is running.<br>4. Recopy the update package zip file to the staging folder.<br>5. In the **Hosts** view toolbar, select **Check for Updates** again.<br>  <br>6. Click **Initialize Update**.<br>7. Click **Update** > **Update Hosts** from the toolbar.<br>8. Click **Begin Update** from the **Update Available** dialog.<br>After the host is updated, it prompts you to reboot the host.<br>9. Click **Reboot** from the toolbar. |

## Upgrade Failed Error

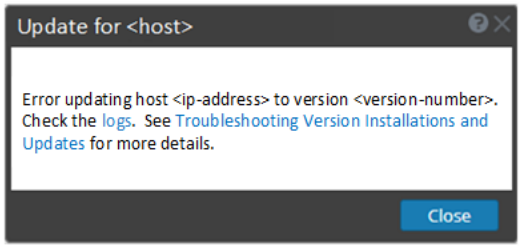
| | |
|---|---|
| **Error Message** | You will receive an error in the error log similar to the following while trying to update to version 11.6 or later:<br>`FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt` |
| **Cause** | Custom builds/rpms installed for certain components installed on hosts, such as in the case of installing Hotfixes. |

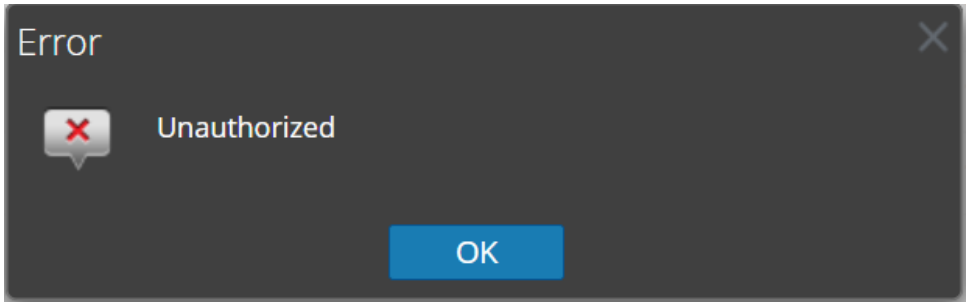
| | |
|---|---|
| **Solution** | **To resolve the issue:**<br>1. SSH to Admin Server.<br>2. Locate the component descriptor file by running the following command.<br>`cd /etc/netwitness/component-descriptor/`<br>3. Open the component descriptor file by running the following command.<br>`vi nw-component-descriptor. json`<br>4. Search for "packages" section for the component you have custom build/rpm. For example, below shown is the package details for "concentrator" host that has custom build/rpm.<br>`"concentrator": {`<br>`"cookbook_name": "rsa-concentrator",`<br>`"service_names": ["rsa-nw-concentrator"],`<br>`"family": "launch",`<br>`"default_port": xxxx, "description": "Concentrator",`<br>`"packages":[{ "name": "rsa-nw-concentrator",`<br>`"version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"`<br>`},`<br>5. Delete the complete version details including (,) character in the packages section. For example, it should look like as shown below after you delete the version details.<br>`"packages": [{`<br>`"name": "rsa-nw-concentrator"`<br>`},`<br>**Note:** You must delete the version details for all the host that has custom builds/rpms in the component descriptor of the admin server.<br>6. Run the upgrade process again. |

## External Repo Update Error

| | |
|---|---|
| **Error Message** | You will receive an error similar to the following error while trying to update to a new version from the :<br>`.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""` |
| **Cause** | Incorrect path specified. |
| **Solution** | Make sure that:<br>• the URL does exist on the NW Server host.<br>• you used the correct path and remove any spaces from it. |

# Host Update Failed Error

| | |
|---|---|
| **Error Message** |  |
| **Problem** | When you select an update version and click **Update** > **Update Host**, the download process is successful, but the update process fails. |
| **Solution** | 1. Try to apply the version update to the host again.<br>Often this is all you need to do.<br>2. If you still cannot apply the new version update:<br>Monitor the following logs on NW Server as it progresses (for example, run the `tail -f` command from the command line):<br>`/var/netwitness/uax/logs/sa.log`<br>`/var/log/netwitness/orchestration-server/orchestration-server.log`<br>`/var/log/netwitness/deployment-upgrade/chef-solo.log`<br>`/var/log/netwitness/config-management/chef-solo.log`<br>`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`<br>The error appears in one or more of these logs.<br>3. If you still cannot apply the update, gather the logs from **step 2** above and contact Customer Support. |

| | |
|---|---|
| **Error Message** |  |
| **Problem** | When you select an update version and click **Update** > **Check for Updates**, the **Unauthorized** error message is displayed. As a result, the connection to the live service fails. |
| **Solution** | 1. Make sure the Live test connection passes.<br>2. Update https://update.netwitness.com/RSA-netwitness in **(Admin)** > **System** > **Updates**. |

| | |
|---|---|
| | 3. SSH to the Admin Server and backup `/etc/default/jetty`.<br>4. Update the following entry at the end of the JAVA_OPTIONS in the `/etc/default/jetty`.<br>`JAVA_OPTIONS="${JAVA_OPTIONS} -Drsa.nw.legacy.web.server.system.update.repo.url=https://update.netwitness.com/RSA-netwitness/ -Drsa.nw.legacy.system.update.auth.url=https://update.netwitness.com/authenticate "`<br>5. Restart the jetty service. Run the following command.<br>`service jetty restart` |

## Missing Update Packages Error

| | |
|---|---|
| **Error Message** | **Initialize Update for Version xx.x.x.x**<br>Missing the following update package(s)<br>Download Packages from NetWitness Link |
| **Problem** | Missing the following update package(s) is displayed in the **Initialize Update Package for NetWitness Platform** dialog when you are updating a host from the **Hosts** view offline and there are packages missing in the staging folder. |
| **Solution** | 1. Click Download Packages from NetWitness Community in the **Initialize Update Package for NetWitness Platform** dialog.<br>The NetWitness Community page that contains the update files for the selected version is displayed.<br>2. Select the missing packages from the staging folder.<br>The **Initialize Update Package for NetWitness Platform** dialog is displayed telling you that it is ready to initialize the update packages. |

## Patch Update to Non-NW Server Error

| | |
|---|---|
| **Error Message** | The `/var/log/netwitness/orchestration-server/orchestration-server.log` has an error similar to the following error:<br>**`API\|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`** |
| **Problem** | After you update the NW Server host to a version, you must update all non-NW Server hosts to the same version. For example, if you update the NW Server from 11.4.0.0 to 11.6.0.0 or later, the only update path for the non-NW Server hosts is the same version (that is, 11.6.0.0). If you try to update any non-NW Server host to a different version (for example, from 11.4.0.0 to an 11.4.x.x) you will get this error. |
| **Solution** | Do any of the following:<br>• Update the non-NW Server host to 11.6.0.0 or later, or |

| | |
|---|---|
| | • Do not update the non-NW Server host (keep it at its current version) |

## Reboot Host After Update from Command Line Error

| | |
|---|---|
| **Error Message** | You will receive a message in the User Interface to reboot the host after you update and reboot the host offline.<br>  |
| **Cause** | The above error occurs when you use CLI to reboot the host. You must use the User Interface to reboot the host. |
| **Solution** | Reboot the host in the **Host** View in the User Interface. |

## Reporting Engine Restarts After Upgrade

| | |
|---|---|
| **Problem** | In some cases, after you upgrade to 11.6 or later from versions of 11.x, such as 11.4, the Reporting Engine service attempts to restart continuously without success. |
| **Cause** | The database files for live charts, alert status, or report status may not be loaded successfully as the files may be corrupted. |
| **Solution** | **To resolve the issue:**<br>1. Check which database files are corrupted:<br>Navigate to the file located at `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` and check the following blocks:<br>• If the live charts db file is corrupted, the following logs are displayed:<br>Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:<br>org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]<br>at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)<br>at org.h2.message.DbException.get(DbException.java:168)<br>org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database!<br>• If the alert status db file is corrupted, the following logs are displayed: |

Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:

org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]

at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)

at org.h2.message.DbException.get(DbException.java:168)

org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl'

- If the report status db file is corrupted, the following logs are displayed:

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading
record: null. Possible solution: use the recovery tool
[90030-196]
```

2. To resolve the live charts database file corruption, do the following:
   a. Stop the Reporting Engine service.
   b. Move the `livechart.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` folder to a temporary location.
   c. Restart the Reporting Engine service.

   **Note:** Some live charts data may be lost on performing the above steps.
3. To resolve the alert status or report status database file corruption, perform the following steps:
   a. Stop the Reporting Engine service.
   b. Replace the corrupted db file with the latest `alertstatusmanager.mv.db` or `reportstatusmanager.mv.db` file from `/var/netwitness/reserver/rsa/soc/reporting-engine/archives` folder.
   c. Restart the Reporting Engine service.

For more information, see the Knowledge Base article Reporting Engine restarts After upgrade to NetWitness Platform 11.4.

| | |
|---|---|
| **Problem** | After you upgrade to NetWitness latest version, the Reporting Engine service does not restart. |
| **Cause** | The Reporting Engine service may not start due to any of the following reasons.<br>- workspace.xml not updated.<br>- Time is not converted properly in livechart h2 database.<br>- JCR (Jackrabbit repository) is corrupted with primary key violation. |
| **Solution** | To resolve the issue, run the Reporting Engine Migration Recovery tool (`rsa-nw-re-migration-recovery.sh`) on the Admin Server where the Reporting Engine service |

| | |
|---|---|
| | is installed.<br><br>**Note:** You can find the Reporting Engine Migration Recovery tool in the below location.<br>`/opt/rsa/soc/reporting-engine-<version number>-<Tag>/nwtools`<br>For example:<br>`/opt/rsa/soc/reporting-engine-12.4.0.0-<Tag>/nwtools`<br><br>1. SSH to Admin Server.<br><br>2. Untar the RE (Reporting Engine) tool, run the following command.<br>`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`<br><br>3. (Optional) If you want to untar the RE tool file in some other directory, you can create a directory and untar the RE tool. Run the following commands.<br>`mkdir <NAME OF THE DIRECTORY>`<br>`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`<br><br>4. Run the script, run the following command.<br>`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`<br><br>For more information, see the Knowledge Base article **Reporting Engine Migration Recovery Tool**. |

## Log Collector Service (`nwlogcollector`)

Log Collector installation logs posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

| | |
|---|---|
| **Error Message** | `<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.` |
| **Cause** | The Log Collector Lockbox failed to open after the update. |
| **Solution** | Log in to NetWitness and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the **Reset the Stable System Value** topic under **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*. |

| | |
|---|---|
| **Error Message** | `<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found` |
| **Cause** | The Log Collector Lockbox is not configured after the update. |
| **Solution** | If you use a Log Collector Lockbox, log in to NetWitness and configure the Lockbox as described in the **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*. |

| | |
|---|---|
| **Error Message** | `<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.` |
| **Cause** | You need to reset the stable value threshold field for the Log Collector Lockbox. |
| **Solution** | Log in to NetWitness and reset the stable system value password for the Lockbox as described in the **Reset the Stable System Value** topic under **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*. |

| | |
|---|---|
| **Error Message** | Decoder tries to start capture events but fails.<br>`Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.` |
| **Cause** | The decoder capture config will not be valid for customers using PF_RING capture (CentOS) and directly upgrading to 12.4 (AlmaLinux). First, they must migrate PF_RING devices to DPDK and then upgrade. |
| **Solution** | **To resolve the issue:**<br>Refer to Migrate PF_RING Devices to DPDK for migration instructions. |

## NW Server

These logs are posted to `/var/netwitness/uax/logs/sa.log` on the NW Server Host.

| | |
|---|---|
| **Problem** | After upgrade, you will notice one of the following:<br>• Audit logs are not getting forwarded to the configured Global Audit Setup.<br>• The following message seen in the `sa.log`.<br>`Syslog Configuration migration failed. Restart jetty service to fix this issue` |
| **Cause** | NW Server Global Audit setup migration failed to migrate from 11.4.x.x or 11.5.x.x. to 11.6.0.0 or later. |
| **Solution** | 1. SSH to the NW Server.<br>2. Submit the following command.<br>`orchestration-cli-client --update-admin-node` |

# Orchestration

The orchestration server logs are posted to `/var/log/netwitness/orchestration-server/orchestration-server.log` on the NW Server Host.

| | |
|---|---|
| **Problem** | 1. Tried to upgrade a non-NW Server host and it failed.<br>2. Retried the upgrade for this host and it failed again.<br><br>You will see the following message in the `orchestration-server.log`.<br>`"'file' _virtual_ returned False: cannot import name HASHES""` |
| **Cause** | Salt minion may have been upgraded and never restarted on failed non-NW Server host |
| **Solution** | 1. SSH to the non-NW Server host that failed to upgrade.<br>2. Submit the following commands.<br>`systemctl unmask salt-minion`<br>`systemctl restart salt-minion`<br>3. Retry the upgrade of the non-NW Server host. |

| | |
|---|---|
| **Problem** | When you install and orchestrate a fresh 12.4 core Node-X to the Admin server (Node-0) upgraded from 12.0 or older versions to 12.4, the core services such as Concentrator, Log Decoder, Log Collector, Archiver, Decoder, Appliance, Workbench, Warehouse Connector, and Broker appear inactive under the **Services** column in the **Admin** > **Hosts** view. As a result, you cannot access the core services in the UI.<br>This is not applicable if you are orchestrating a fresh 12.4 core Node-X to the fresh-Installed 12.4 Admin Server (not upgraded from 12.0 or older versions to 12.4). |
| **Cause** | The 12.4 core Node-X uses a dedicated SA-server certificate instead of the common Node-0 node certificate under its trustpeers if it is orchestrated directly to an upgraded 12.4 Admin Server host. |
| **Solution** | 1. Before you bootstrap and orchestrate the 12.4 core Node-X host, run the following commands.<br>`mkdir -p /etc/netwitness/platform`<br>`touch /etc/netwitness/platform/nw-upgrade-mode`<br>2. Perform this workaround only if you skip the above workaround (Workaround 1). Run the following commands after you bootstrap and orchestrate the 12.4 core Node-X host.<br>`touch /etc/netwitness/platform/nw-upgrade-mode`<br>`nw-manage --refresh-host --host-key <core-node-x-salt-minion-uuid>`<br>`systemctl restart <core-service-name>`<br>**Note:**<br>- Refer the file `/etc/salt/minion` to find `<core-node-x-salt-minion-uuid>`. |

| | |
|---|---|
| | - You must enter the core service name such as **nwarchiver** (Archiver), **nwdecoder** (Decoder), **nwlogcollector** (Log Collector), **nwappliance** (Appliance), **nwconcentrator** (Concentrator), **nwlogdecoder** (Log Decoder), **nwbroker** (Broker), **nwworkbench** (Workbench), and **nwwarehouseconnector** (Warehouse Connector) in `<core-service-name>`. |

## Reporting Engine Service

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

| | |
|---|---|
| **Error Message** | `<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]` |
| **Cause** | Update of the Reporting Engine failed because you do not have enough disk space. |
| **Solution** | Free up the disk space to accommodate the required space shown in the log message. See the **Add Additional Space for Large Reports** topic in the *Reporting Engine Configuration Guide* for instructions on how to free up disk space. |

## Event Stream Analysis

| | |
|---|---|
| **Problem** | After upgrading to version 12.4 or later, the ESA correlation server does not aggregate events from the configured data sources. |
| **Error Message** | `Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)` |
| **Solution** | **To resolve the issue:**<br>In the NetWitness user interface,<br>1. Go to (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** > **Data Sources**.<br>The **Data Sources** panel is displayed.<br>2. Select the data source and click **Edit Datasource** in the toolbar.<br>The **Edit Datasource** dialog is displayed.<br>3. In the **Edit Datasource** dialog, do one of the following:<br>• Select **Trusted Authentication**.<br>• Select **Use Credentials** and enter the Username and Password.<br>4. Click **Test Connection** to make sure that it can communicate with the ESA service and then click **OK**.<br>**Note:** Do the above procedure for all the configured data sources. |

| | |
|---|---|
| | 5. Deploy all the deployments associated with the edited data sources in the **Data Sources** panel after you finish making changes to the data sources. |

# Legacy Windows Log Collector

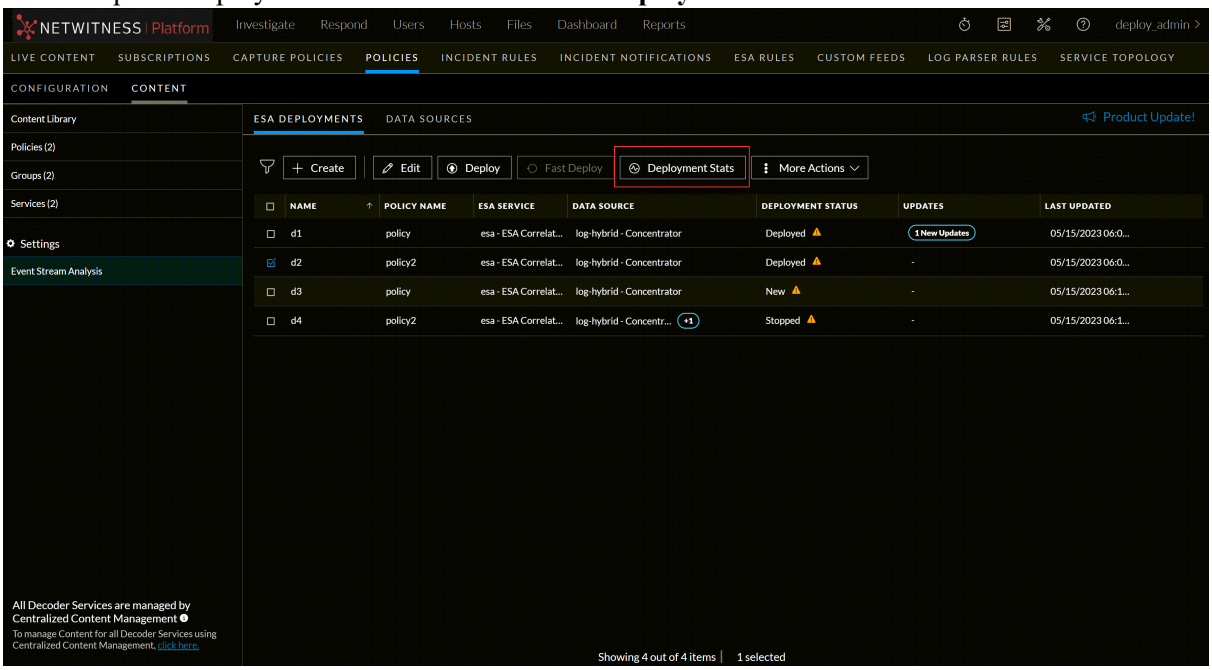
| | |
|---|---|
| **Problem** | • Legacy Windows Log Collector appears as inactive post upgrade of SA to 12.4 version and Legacy Windows Log Collector to 11.6.x or 11.7.x versions.<br>• Legacy Windows Log Collector appears as inactive when the stack is upgraded to 12.4. |
| **Cause** | Certificate update in the SA node. |
| **Solution** | Refer Legacy Windows Log Collector section in the Perform Post Upgrade Tasks. |

# ESA Troubleshooting Information

## ESA Rules are Not Creating Alerts

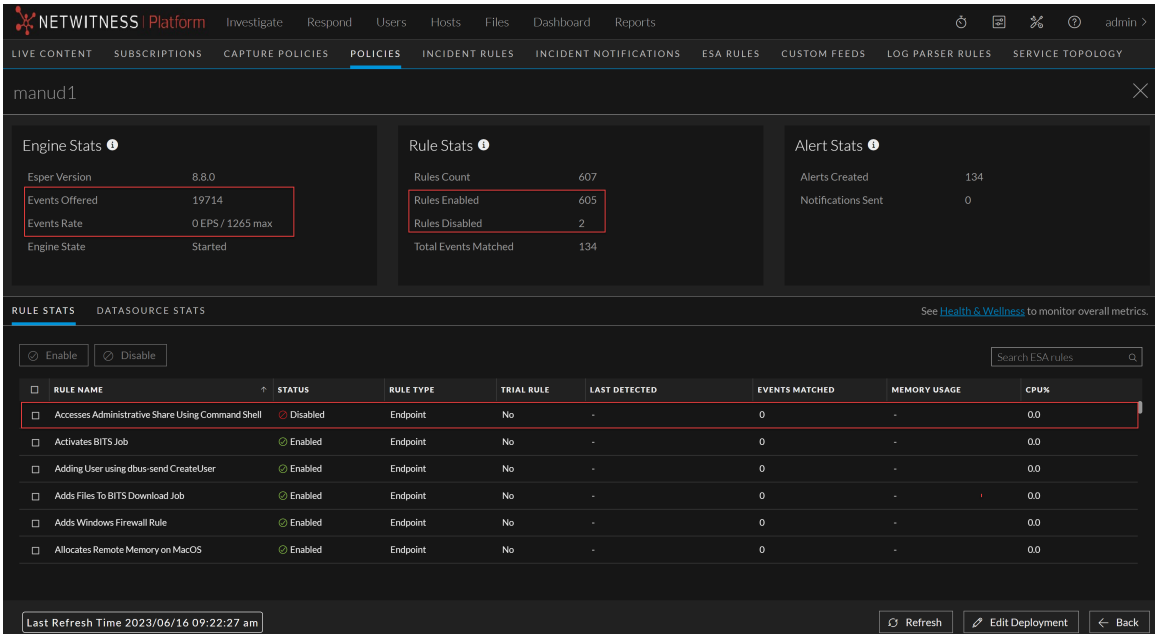
If you are not seeing any alerts, check the status of the ESA rule deployments.

1. Go to (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** > **ESA Deployments**. The **ESA Deployment** panel is displayed.
2. Select required deployment from the list and click **Deployment Stats** tab.




3. Deployment Stats page is displayed, which shows the status of your ESA services and deployments.

4. For each ESA rule deployment:
   a. In the **Engine Stats** section, look at the **Events Offered** and the **Offered Rate**. They confirm that the data is being aggregated and analyzed properly. If you see 0 for Events Offered, nothing is coming in for the deployment.
   b. In the **Rule Stats** section, look at the **Rules Enabled** and **Rules Disabled**. If there are any disabled rules, look in the **Deployed Rule Stats** section below to view the details of the disabled rules. Disabled rules show a white circle. Enabled rules show a green circle.




5. If you notice any disabled rules that should be enabled:
   a. Go to  **(Configure) > ESA Rules > Rules** tab and redeploy the ESA rule deployments that contain disabled rules.
   b. Go back to the **Services** tab and check to see if the rules are still disabled. If the rules are still disabled, check the ESA Correlation service log files, which are located at `/var/log/netwitness/correlation-server/correlation-server.log`.

**Note:** To avoid unnecessary processing overhead, the Ignore Case option has been removed from the ESA Rule Builder - Build a Statement dialog for meta keys that do not contain text data values. During the upgrade to 11.4 or later, NetWitness Platform does not modify existing rules for the Ignore Case option. If an existing Rule Builder rule has the Ignore Case option selected for a meta key that no longer has the option available, an error occurs if you try to edit the statement and try to save it again without clearing the checkbox.

## Example ESA Correlation Server Warning Message for Missing Meta Keys

If you see a warning message in the ESA Correlation server error logs that means there is a difference between the `default-multi-valued` parameter and `multi-valued parameter` meta key values, the new Endpoint, UEBA, and Live content rules will not work. Completing the **Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules** procedure in the *ESA Configuration Guide* should fix the issue.

**Multi-Valued Warning Message Example**

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id,
browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_
src, client_all, content, context, context_all, context_dst, context_src, dir_
path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst,
directory_src, email_dst, email_src, feed_category, feed_desc, feed_name,
file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter,
function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_
orig, OS, param, param_dst, param_src, registry_key, registry_value, risk,
risk_info, risk_suspicious, risk_warning, threat_category, threat_desc,
threat_source, user_agent] are still MISSING from multi-valued
```

**Single Value Warning Message Example**

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target,
file_attributes, logon_type_desc, packets] are still MISSING from single-
valued
```

# Use NetWitness Community Portal for Assistance

You can use NetWitness Community Portal to search for specific documents, find information related to End of Life of appliances, and read blogs.

## 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<br>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 |

# Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.