NetWitness® Platform XDR

Version 12.2.0.0

Upgrade Guide

NETWITNESS

Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

March, 2023

Contents

Upgrade Overview

NetWitness 12.2.0.0 provides enhancements and fixes for all products in NetWitness Platform. The instructions in this guide apply to both physical and virtual hosts (including AWS, Azure Public Cloud, and Google Cloud Platform) unless stated to the contrary.

In 12.2.0.0, NetWitness has several new features in the user interface.

Warning: Before upgrading the UEBA host from 12.0 and older versions to 12.2, you must perform the backup of your Elasticsearch data such as Users, Entities, Alerts, and Indicators to retain them post upgrade. For more information, see Upgrade Preparation Tasks. This action is not required if you are upgrading the UEBA host from 12.1 to 12.2.

Upgrade Paths

The following upgrade paths are supported for NetWitness 12.2.0.0:

- NetWitness 11.6.x.x to 12.2.0.0
- NetWitness 11.7.0.0 to 12.2.0.0
- NetWitness 11.7.0.1 to 12.2.0.0
- NetWitness 11.7.0.2 to 12.2.0.0
- NetWitness 11.7.1.0 to 12.2.0.0
- NetWitness 11.7.1.1 to 12.2.0.0
- NetWitness 11.7.1.2 to 12.2.0.0
- NetWitness 11.7.2.0 to 12.2.0.0
- NetWitness 12.0.0.0 to 12.2.0.0
- NetWitness 12.1.0.0 to 12.2.0.0
- NetWitness 12.1.0.1 to 12.2.0.0
- NetWitness 12.1.1.0 to 12.2.0.0

This guide applies to both physical and virtual hosts (including AWS and Azure Public Cloud).

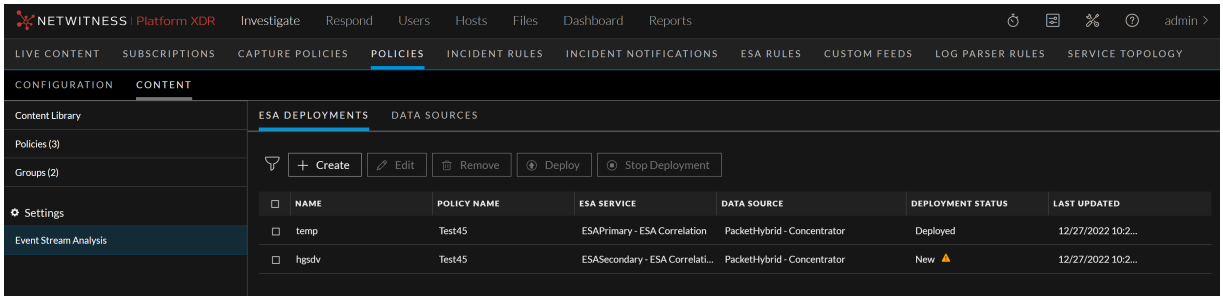
Running in Mixed Mode

Running in mixed mode occurs when some services are upgraded to the latest version and some services are on older versions. See "Running in Mixed Mode" in the *NetWitness Platform Hosts and Services Getting Started Guide* for further information.

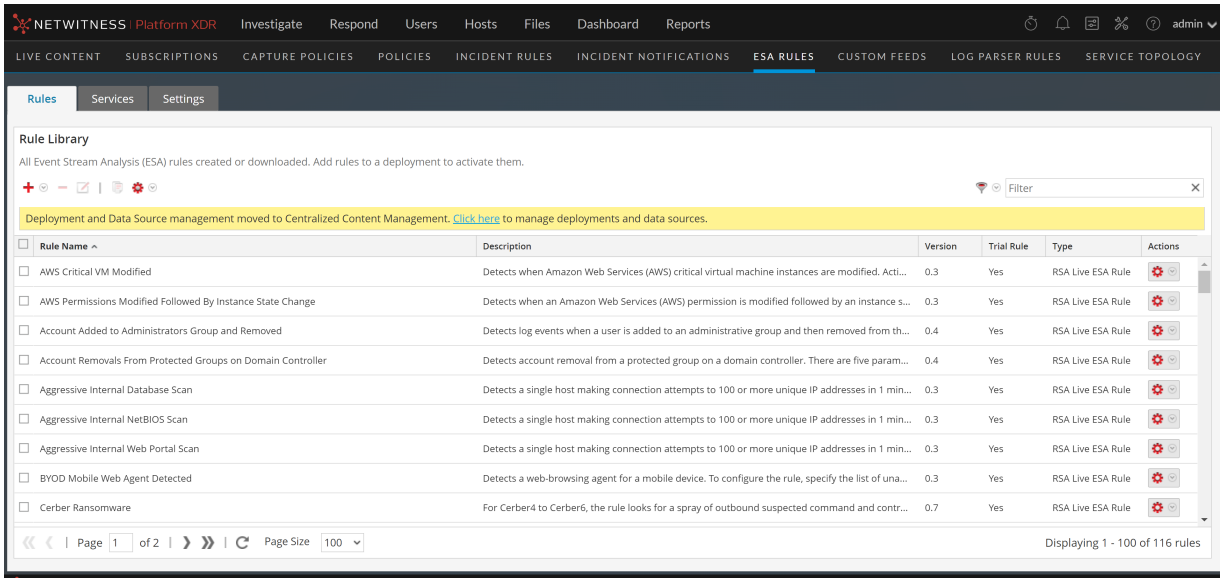
Note: If you are running Endpoint Log Hybrid in mixed mode, make sure Endpoint Broker is on the same version as one of the Endpoint Servers.

Upgrade Considerations for ESA Hosts

- Mixed mode is not supported for ESA hosts in NetWitness Platform XDR.
- In 12.1 and later versions, you can only manage the ESA deployments and Data Sources through **Centralized Content Management**. Go to (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** page to manage the ESA deployments and Data Sources. Refer the following screenshot.



- After upgrading to 12.1 and later versions, you can only manage the ESA Rules in the **ESA Rules** page. Refer the following screenshot.



- After upgrading to the 12.2 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 12.2.x.x version. Make sure that you plan the upgrade process so that Correlation servers are upgraded immediately after the Admin Server is done. The deployments will not be accessible until the corresponding Correlation servers are upgraded. However, the correlation servers will still continue to process the Alerts and Events.
- You must upgrade the ESA hosts immediately after upgrading the Admin Server.

  For more information on **Centralized Content Management** and managing the deployments, see https://community.netwitness.com/t5/rsa-netwitness-platform-staged/centralized-content-management-guide-for-12-1-1/ta-p/694426.

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

Upgrade or install Legacy Windows Log Collection

Refer to the Legacy Windows Log Collection Guide for NetWitness.

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

Feedback on Product Documentation

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

Pre Upgrade Checks

You must run the pre-upgrade checks before you upgrade to NetWitness 12.2.0.0 to identify any issues that may result in upgrade failure.

To run the pre-upgrade checks, perform the following:

1. Log in to Admin console.
2. Run the following command:
   `nw-precheck-tool upgrade-checklist`

   The pre-upgrade checks verifies the following:

Upgrade Checklist

- **Security Client File Check** - Ensures `security-client-amqp.yml` file is not present.
- **Node-0 NW Service-id Status** - Ensures all the service-id is intact with all the different services in Node 0.
- **Broker Service Trustpeer Symlink** - Ensures Broker symlink file `(/etc/netwitness/ng/broker/trustpeers/)` is not broken.
- **Node-0 NW Services Status** - Checks the status of all the services in Node 0.
- **Yum External Repo Check** - Ensures external repos are not available and not enabled.
- **Node-0 RPM DB Index Check** - Checks if the RPM DB is corrupted or not.
- **Salt Master Communication** - Verifies the salt communication from Node 0 to all the Nodes.
- **Node-0 Certificates Check** - Checks if any certificates are missing, expired, or invalid 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** - Verifies the status of services (Active or In Active) on all the Node X.
- **(Component Hosts) Node X Certificates Check** - Checks the certificate expiry, missing, corrupted, and issuer mismatch in all categories of Node X.

- **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** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness`, and `root` on Node 0.
- **(Component Hosts) Node X File System Utilization** - Verifies the disk partition utilization of `/var/netwitness/mongo`, `/var/netwitness`, and `root` for ESA Primary and Endpoint Log Hybrid services on Node X.
- **Mongo File (ESAPrimary)** - Checks the ESA Primary node in the system or stack and verifies the permission mode of Mongo file.
- **Orchestration Server Normal Mode** - Checks if the orchestration service is running in normal or safe mode.
- **(Admin Server) Node 0 Init status** - Checks if there are any issues that might fail init process.
- **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.

Network Checklist

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

Certificate Checklist

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

Upgrade Preparation Tasks

Complete the following tasks to prepare for the upgrade to NetWitness 12.2.0.0

Warning: The Dell S4 and S4s appliances reached the End of Life (EOL) in June 2021. We recommend that you discontinue installation or upgrade activities on these and upgrade to new hardware. For more information on End of Life hardware support, see https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitnessplatform/ta-p/569875.

Task 1 (Optional). Remove Legacy Package Repositories

Perform this task to free up space by removing unused repositories from previous releases.

1. Determine the version of the oldest NetWitness Platform host in your environment by doing one of the following:
   - Review the host list in the Admin user interface.
   - Run the following command on the NW Server:

     ```
     upgrade-cli-client --list
     ```
2. You can safely remove all legacy package repository folders located at `/var/netwitness/common/repo/<version>` on the NW Server for all versions prior the baseline major release version of the oldest active host in the environment.
   - If the oldest host version is 11.6.x.x (for example, 11.6.1.0), you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, 11.3.x.x, and 11.4.x.x, and 11.5.x.x repository folders. **However, do not remove repository versions greater than or equal to 11.7.0.0.**
   - If the oldest host version is 11.7.x.x, you can safely remove 11.0.x.x, 11.1.x.x, 11.2.x.x, 11.3.x.x, 11.4.x.x, 11.5.x.x, and 11.6.x.x repository folders. **However, do not remove repository versions greater than or equal to 11.7.0.0.**

Task 2. Backup and Remove the Rotated RabbitMQ Logs

Before upgrading from 11.6.x or 11.7.x to 12.2.0.0, you must remove the old RabbitMQ logs and free up the space in /var/log mount disk. Follow the below procedure to free up the space in /var/log mount disk.

1. Backup the rotated RabbitMQ logs into var/netwitness directory. Do the following.

   ```
   mkdir /var/netwitness/rabbitmq_logsbkp
   scp -r /var/log/rabbitmq/ /var/netwitness/rabbitmq_logsbkp
   ```
2. Remove the rotated RabbitMQ logs from /var/log/rabbitmq pre-upgrade. Do the following.

   ```
   cd /var/log/rabbitmq
   rm -f rabbit\@<sa-uuid>.log.*
   rm -f rabbit\@<sa-uuid>_upgrade.log.*
   ```

```
rm -f *.gz
rm -f rabbit@<sa-uuid>.log-*
```

Note:
- This procedure must be performed only once before upgrading to 12.2.0.0 Post-upgrade, the RabbitMQ service automatically handles the log rotation.
- The command `rm -f rabbit\@<sa-uuid>.log.*` is used to clean up the old uncompressed logs such as log.1, log.2, and log.3.
- The command `rm -f rabbit\@<sa-uuid>_upgrade.log.*` is used to clean up the old uncompressed upgrade logs.
- The command `rm -f *.gz` is used to clean up the old compressed logs.
- The command `rm -f rabbit@<sa-uuid>.log-*` is used to clean up the old uncompressed logs rotated with logrotate.

Task 3. Uninstall the Security Analytics l10n language pack

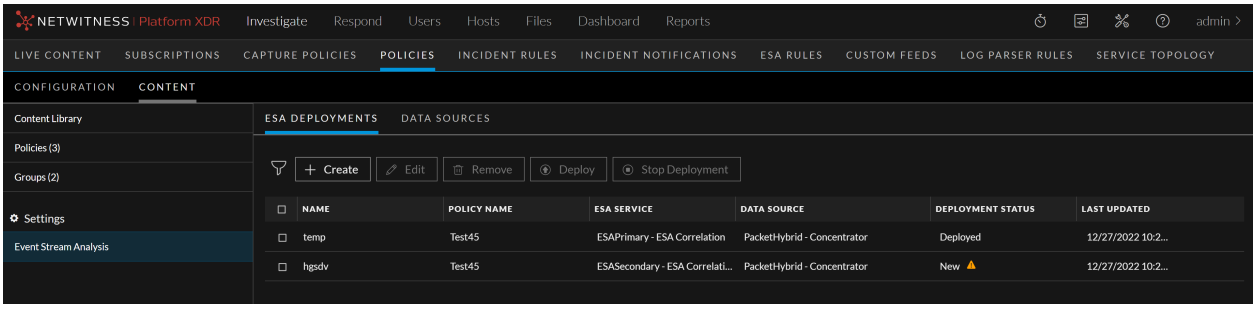
Before you upgrade from 11.6.x.x to 11.7.x.x or 12.2.0.0 version, you must uninstall the Security Analytics l10n language pack.

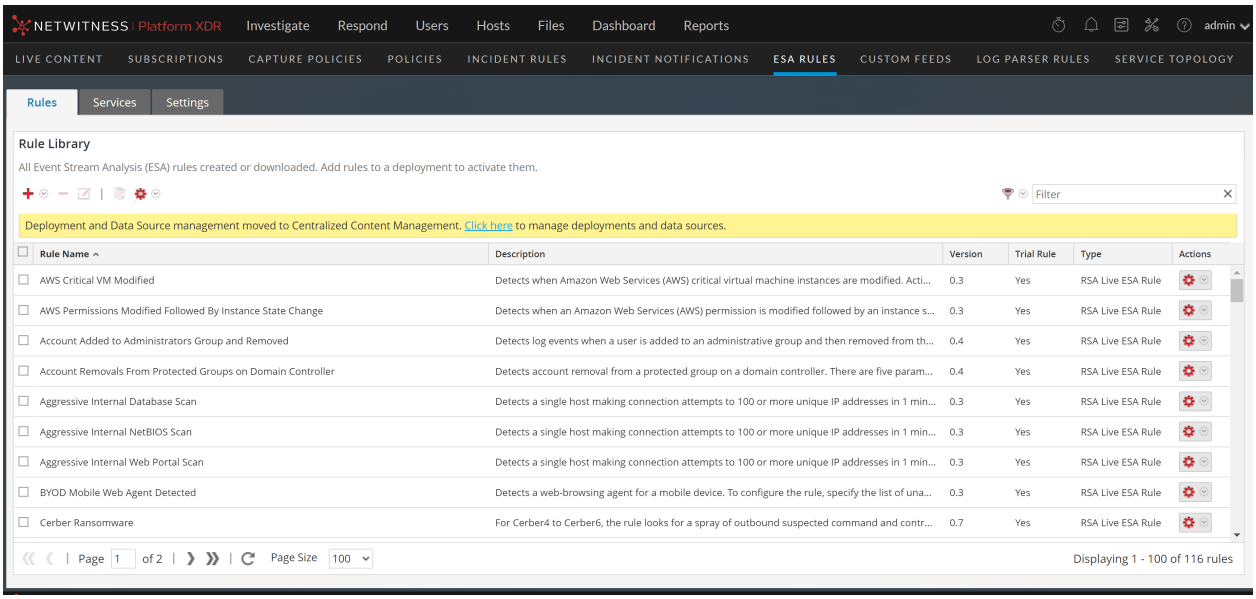
Task 4. Preparing ESA Deployments for Migration to 12.2.0.0

Before upgrading to 12.2.0.0, NetWitness recommends that all the ESA deployments maintain an error-free state and remove any unused ESA deployments, as ESA deployments will be migrated to policies and groups after upgrading to 12.2.0.0. 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 12.2.x.x version.

Manage ESA Deployments and Data Sources

In 12.1 and later versions, you can only manage the ESA deployments and Data Sources through **Centralized Content Management**. Go to (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** page to manage the ESA deployments and Data Sources. You can only manage the ESA Rules in the **ESA Rules** page. Refer the following screenshots.





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 https://community.netwitness.com/t5/rsa-netwitness-platform-staged/centralized-content-management-guide-for-12-1-1/ta-p/694426.

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.

SlNo	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 rule are added.

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

Task 5. Backup Elasticsearch Data (Users, Entities, Alerts, and Indicators)

Before upgrading the UEBA host from 12.0.0.0 and older versions to 12.2.0.0, you must perform the backup of your Elasticsearch data such as Users, Entities, Alerts, and Indicators (using the Elasticsearch migration tool) to retain them post upgrade.

Prerequisites

Make sure the following prerequisites are met before you perform data backup:

- The current Elasticsearch version must be 5.5.0.
- Presidio rpms version must be less than or equal to 12.0.0.0.
- `ueba_es_migration_tool.zip` file must be downloaded.

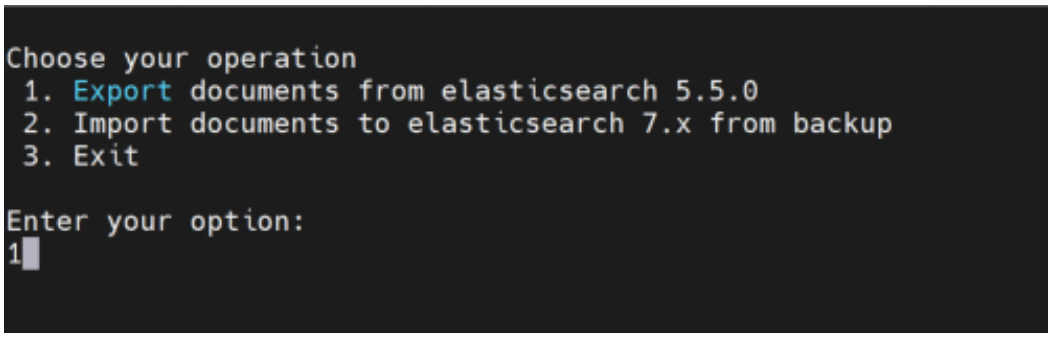
> **Note: ueba_es_migration_tool** allows you to migrate presidio Elasticsearch data from Elasticsearch version 5.5.0 to 7.17.6 while upgrading the UEBA host to 12.2.0.0 from 12.0.0.0 and older versions. This tool contains `elk-migration-script.sh` script file and `presidio-elk-migration-1.0.0.jar` file and it can be downloaded from https://community.netwitness.com/t5/rsa-netwitness-platform-staged/ueba-elasticsearch-migration-tool-fof-nw-12-2/ta-p/696519.

To backup the Elasticsearch data:

1. Select the available directory and unzip the `ueba_es_migration_tool.zip` file.
2. Go to `cd ueba_es_migration_tool`. Run the following command.

   ```
   sh elk-migration-script.sh
   ```

   The Elasticsearch migration tool guide is displayed.

3. Select **Export documents from elasticsearch 5.5.0** and enter **yes** when prompted to stop the airflow scheduler.

   > **Note:** When you enter **yes**, the airflow scheduler stops consuming the fresh incoming data such as Users, Entities, and Alerts. This avoids data loss during the export process.

4. In the next step, select **Fresh Export** to export the existing data.

```
Export documents from elasticsearch 5.5.0
 1. Fresh Export
 2. Resume Export
 3. Main menu
 4. Exit

Enter your option:
1

Destination dir path:
/root/elasticsearch_export_backup
Please wait processing your export request...

+----------------------------------------+----------+--------+----------+
| Index                                  | Exported | Total  | Took     |
+----------------------------------------+----------+--------+----------+
| presidio-monitoring-2023.02.07         | 39612    | 39612  | 1641 ms. |
| presidio-monitoring-2023.02.09         | 5628     | 5628   | 204 ms.  |
| presidio-output-indicator              | 4294     | 4294   | 703 ms.  |
| presidio-output-entity                 | 672      | 672    | 27 ms.   |
| presidio-output-feature                | 2091     | 2091   | 321 ms.  |
| presidio-output-entity-severities-range | 3        | 3      | 11 ms.   |
| presidio-output-alert                  | 1279     | 1279   | 57 ms.   |
| presidio-output-event                  | 41335    | 41335  | 2070 ms. |
| presidio-monitoring-2023.02.08         | 112617   | 112617 | 3999 ms. |
+----------------------------------------+----------+--------+----------+

Total: 207531, Exported: 207531, Dropped: 0, Started: 2023-02-10 02:08:56, Ends: 2023-02-10 02:09:05, Took: 9483 ms.
[root@ueba ~]#
```

Note:
- If the Export operation fails due to some technical issue, select **Resume Export** once the issue is resolved, to resume the Export operation.
- Go to `<backup_directory_path>/log/log/es-migration-export.log` if you want to view the log for the succeeded or failed processes.

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

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.

Upgrade Tasks

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

Note: 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.

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

Note: 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 4. Preparing ESA Deployments for Migration to the 12.2 Version**" in topic Upgrade Preparation Tasks.

Important Notes - Read This First

Synchronize Time on Component Hosts with NW Server Host

Before upgrading your 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:

- Configure the NTP Server. For more information, see"Configure NTP Servers" in the *System Configuration Guide*.
- Perform the following steps on each host:
  a. SSH to the Admin Server host.
  b. Run the following commands.

```
salt \* service.stop ntpd
salt \* cmd.run 'ntpdate nw-node-zero'
salt \* service.start ntpd
```

Mixed Mode Unsupported for ESA Hosts

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

Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 12.2.0.0

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 12.2.0.0 The Respond post-upgrade tasks only apply after the Respond Server service is upgraded and is in the enabled state.

Deploy_Admin Password Guidelines

In NetWitness Platform version 11.6 or Later, deployment account password (only on node-zero) must contain at least one number, one upper and lower case letter, and one special characters (!@#%^,+ .) along with the existing policy. The same password policy applies while updating deploy_admin password using `nw-manage script`.

If `deploy_admin` password is changed on Primary NW Server, it must be changed in the Warm Standby Server if it exists

Removal of DNSMasq in 12.1 and 12.2 Versions

After upgrading to 12.1 and 12.2 versions, the package, service, and the configuration files associated with DNSMasq are removed. However, this will not impact the system.

Additional Post Upgrade Steps for 12.2.0.0 Version with Legacy Windows Log Collector

For 12.2.0.0 version with Legacy Windows Log Collector, you should perform few additional post upgrade tasks. Refer to Legacy Windows Log Collection section in Post Upgrade Tasks for these additional post upgrade tasks.

Upgrade Options

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

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

The following rules apply when you are upgrading hosts for all of these 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.
- Add Warm Standby (if exists) to the list of hosts and it must be on same version as NetWitness Platform.

Option 1: Upgrade NetWitness Platform XDR

You can use this method if the NW Server host is connected to Live Services and if you are able to obtain the package.

Prerequisites

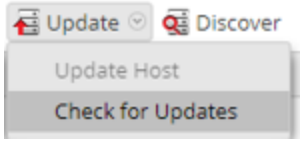
Make sure that:

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. 12.2.0.0 is available in the **Update Version** column.

Procedure

To upgrade from 11.6.x.x, 11.7.0.x, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, and 12.1.1.0 to 12.2.0.0, follow the steps below:

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

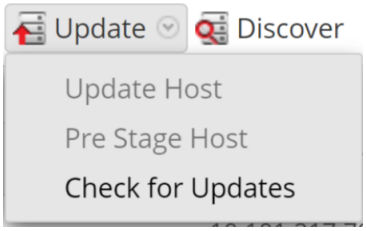


4. Update Available is displayed in the **Status** column if you have a version update in your Local Update Repository for the selected host.

5. Select **12.2.0.0** from the **Update Version** column. 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.
   - 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.
6. Click **Update** > **Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click **Reboot Host**.
9. Repeat steps 6 to 8 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.

Note: In 11.7.1.0 or later versions, you can pre-stage the upgrade repository using the **Pre Stage Host** feature. Refer the following screenshot. For more information, see Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages.



Option 2: Upgrade NetWitness Platform XDR Offline

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

1. Download the upgrade package `netwitness-12.2.0.0.zip` from NetWitness Community (https://community.netwitness.com/) > **Downloads** > **NetWitness Platform** > **Version 12.2** to a local directory:
2. SSH to the NW Server host.
3. Copy `netwitness-12.2.0.0.zip` from the local directory to the `/var/lib/netwitness/common/update-stage/` staging folder.
   For example:

```
sudo cp /tmp/netwitness-12.2.0.0.zip /var/lib/netwitness/common/update-stage/
```

If you are logged as a root user you can ignore sudo in the command, for example,

```
cp /tmp/netwitness-12.2.0.0.zip /var/lib/netwitness/common/update-stage/
```

Note: NetWitness Platform unzips the file automatically.

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

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**.

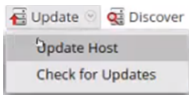
   Note: If you are already on the  **(Admin) > Hosts** page and the **Check for Updates** option (**Update** > **Check for Updates**) is grayed out, refresh the page from the browser to check for the updates.
3. Check for updates and wait for the upgrade packages to be copied, validated, and ready to be 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 and you complete the rest of the steps in this procedure to finish the upgrade of the host.
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 XDR using CLI (Offline)

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

Prerequisites

Make sure that you have downloaded the `netwitness-12.2.0.0.zip` file from NetWitness Community (https://community.netwitness.com/) > **Products > NetWitness Platform** > **Downloads** > **Version 12.2** > **Full Product Downloads** to a local directory:

Procedure

You must perform the upgrade steps for NW Server hosts and for 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 12.2.0.0 files to prepare them for the upgrade.
   - Log into the NW Server as `root` and create the following directory:
     `/var/netwitness/tmp/upgrade/12.2.0.0`
     and then copy the package zip files to the `/var/netwitness/tmp/` directory of the NW Server and extract the package files from `/var/netwitness/tmp/` to the appropriate directories using the following command:
     `unzip netwitness-12.2.0.0.zip -d /var/netwitness/tmp/upgrade/12.2.0.0/`

     Make sure you remove the update zip file from the staging directory after it is extracted.
2. Initialize the upgrade, using the following command:
   `upgrade-cli-client --init --version 12.2.0.0 --stage-dir /var/netwitness/tmp/upgrade`
3. Upgrade the NW Server host, using the following command:
   `upgrade-cli-client --upgrade --version 12.2.0.0 --host-key <ID / display name / (hostname/ IP address)>`
4. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
5. Repeat steps 3 and 4 for other component hosts.

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`.

Note: If the following error is displayed during the upgrade process:

```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support for assistance.

External Repo Instructions for CLI upgrade

1. Stage the 12.2.0.0 files to prepare them for the upgrade.
   - Log into the NW Server as `root` and create the following directory:
     `/var/netwitness/tmp/upgrade/12.2.0.0`
     and then copy the package zip files to the `/var/netwitness/tmp/` directory of the NW Server and extract the package files from `/var/netwitness/tmp/` to the appropriate directories using the following command:
     ```
     unzip netwitness-12.2.0.0.zip -d /var/netwitness/tmp/upgrade/12.2.0.0/
     ```
     Make sure you remove the update zip file from the staging directory after it is extracted.
2. Initialize the upgrade, using the following command:
   ```
   upgrade-cli-client --init --version 12.2.0.0 --stage-dir
   /var/netwitness/tmp/upgrade
   ```
3. Upgrade the NW Server host, using the following command:
   ```
   upgrade-cli-client --upgrade --version 12.2.0.0 --host-key <ID / display
   name / (hostname/ IP address)>
   ```
4. When the NW Server host upgrade is successful, reboot the host from NetWitness Platform user interface in the Hosts view.
5. Repeat steps 3 and 4 for other component hosts.

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`.

Note: If the following error displays during the upgrade process:
```
2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```
the service pack will install correctly. No action is required. If you encounter additional errors when updating a host to a new version, contact Customer Support for assistance.

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.

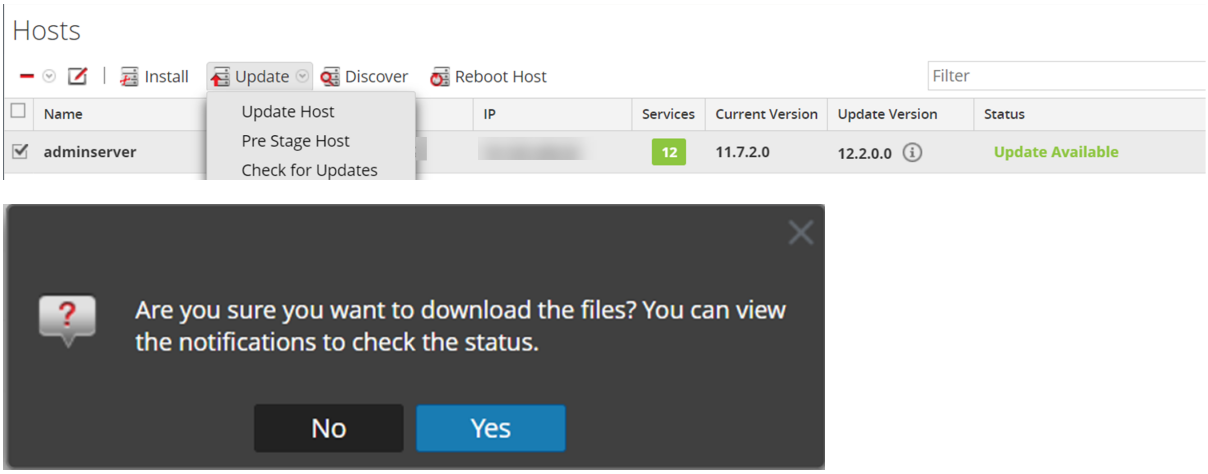
Note: Pre Stage Host feature is supported from version 11.7.1.0 or later.

Procedure

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

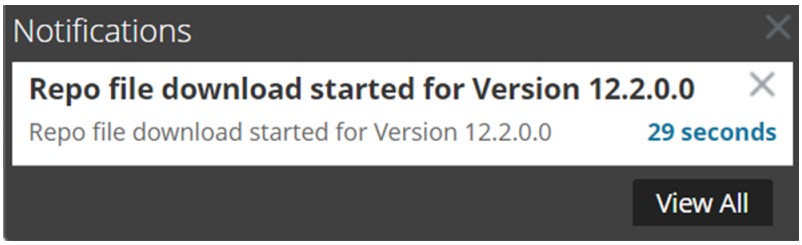
   All possible update versions will be displayed in the Versions drop-down list.
3. Click **Update** > **Pre Stage Host** and select the version in the update version column.

   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.

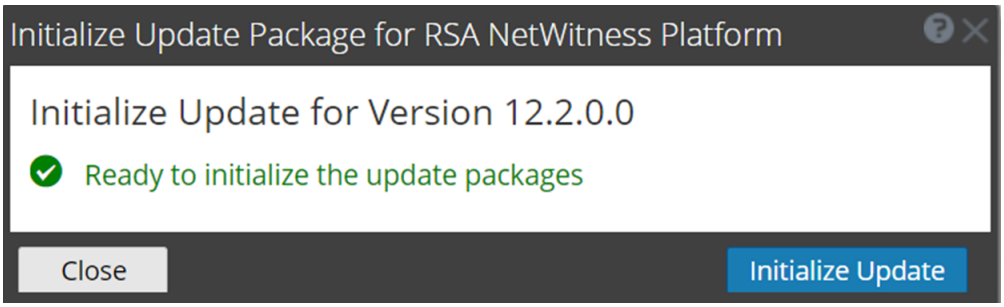
   The **Pre Stage Host** and **Upgrade Host** will be disabled until pre stage is completed.



> **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.

Post Upgrade Tasks

After you upgrade to 12.2.0.0, NetWitness has several new features in the user interface. Complete the tasks that apply to the hosts in your environment.

General

Jetty Configuration

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

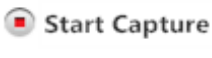
Make Sure Services Have Restarted and Are Capturing and Aggregating Data

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

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 

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 Start Capture

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 Start Aggregation
3. Event Stream Analysis (ESA)

Note: Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.6 and later. 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 12.2, 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

Core Services Contents Paths	Components	.tar location of the Components
/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 12.2, 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 12.2 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 12.2 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*.

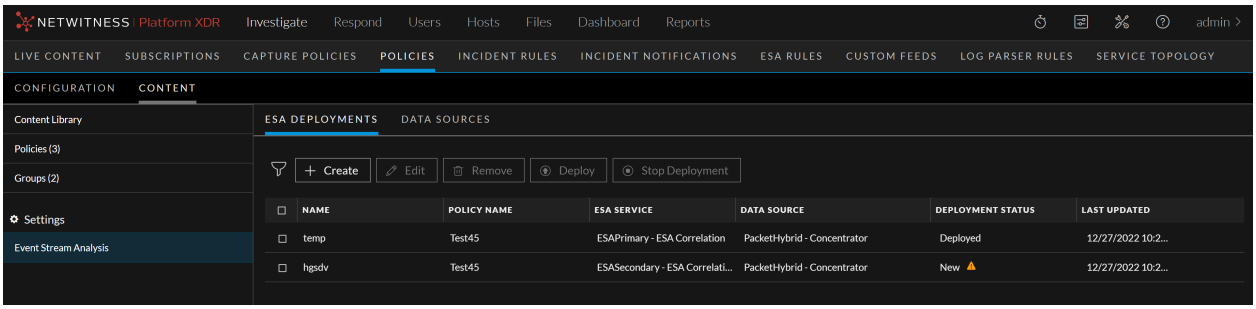
The pre-upgrade and post-upgrade states of deployments are represented in the following table.

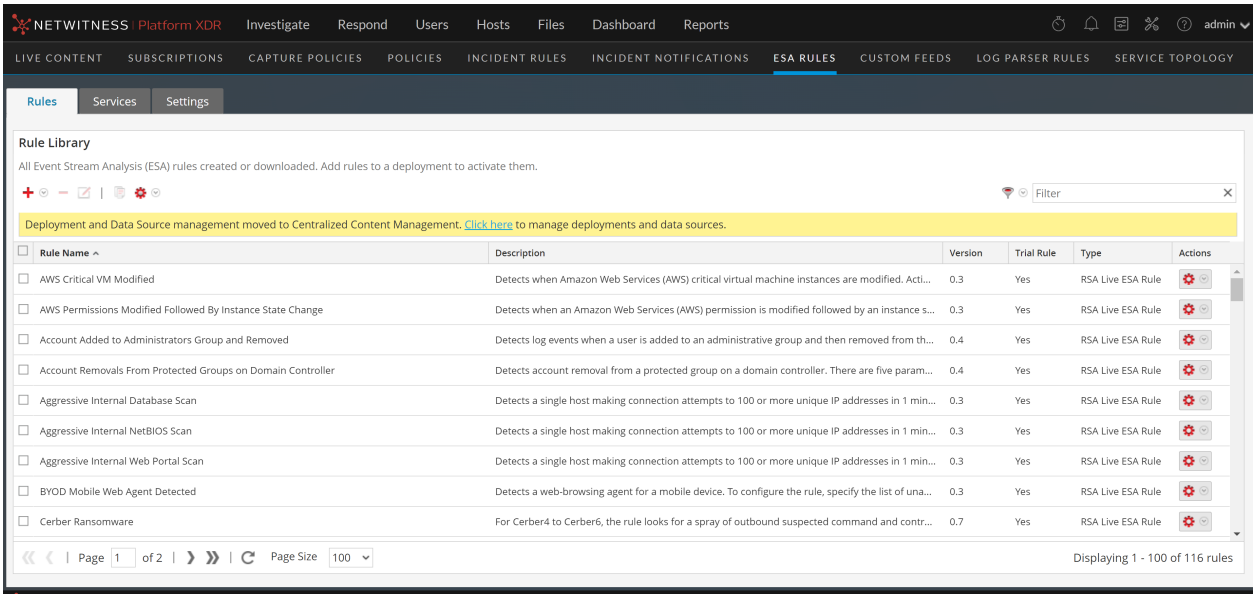
SINo	Pre-upgrade Deployment State	Post-upgrade Deployment State		
		Creates Policy	Creates Group	The policy will be Published
1	Healthy deployment	Yes	Yes	Yes
2	Deployment with errors	Yes	Yes	Yes
3	Deployment with only rules	Yes	No	No
4	Deployment with no rules	No	No	No

(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

In 12.1 and later versions, you can only manage the ESA deployments and Data Sources through **Centralized Content Management**. Go to (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** page to manage the ESA deployments and Data Sources. You can only manage the ESA Rules in the **ESA Rules** page. Refer the following screenshots.





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

For more information on **Centralized Content Management** and managing the deployments, see https://community.netwitness.com/t5/rsa-netwitness-platform-staged/centralized-content-management-guide-for-12-1-1/ta-p/694426.

Respond

The Primary ESA server must be upgraded to 12.2.0.0 before you can complete these tasks.

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 12.2.0.0 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 Aggregation Rule Schema

Note: If you did not manually customize the incident aggregation rule schema, you can skip this task.

If you added custom keys in the `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file for use in the `groupBy` clause for 12.2.0.0, modify the `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` file and add the custom keys from the automatic backup file.

The backup file is located in `/var/lib/netwitness/respond-server/data` and it is in the following format:
`aggregation_rule_schema.json.bak-<time of the backup>`

Legacy Windows Log Collector

Update the Legacy Windows Log Collector UUID

After upgrading to 12.2.0.0, for each Legacy Windows Log Collector configured in your environment, run the following command on the NW Server:

```
wlc-cli-client --update-to-uuid --host <WLC host address>
```

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.

User Entity Behavior Analytics

IMPORTANT: Every UEBA deployment when upgraded requires additional steps to complete the upgrade process. When you upgrade from 11.6.x to 11.6.x.x, you must follow UEBA instructions in the Upgrade Guide for 11.6.x.x, before you upgrade to 11.7.x.

Note: When you upgrade to 12.2.0.0 from 11.6.x.x, you don't need to rerun the UEBA system for the last 28 days, if you don't update the current processing schemas. When you upgrade to 12.2.0.0 from a version prior to 11.7.x, the UEBA system runs a rerun automatically.

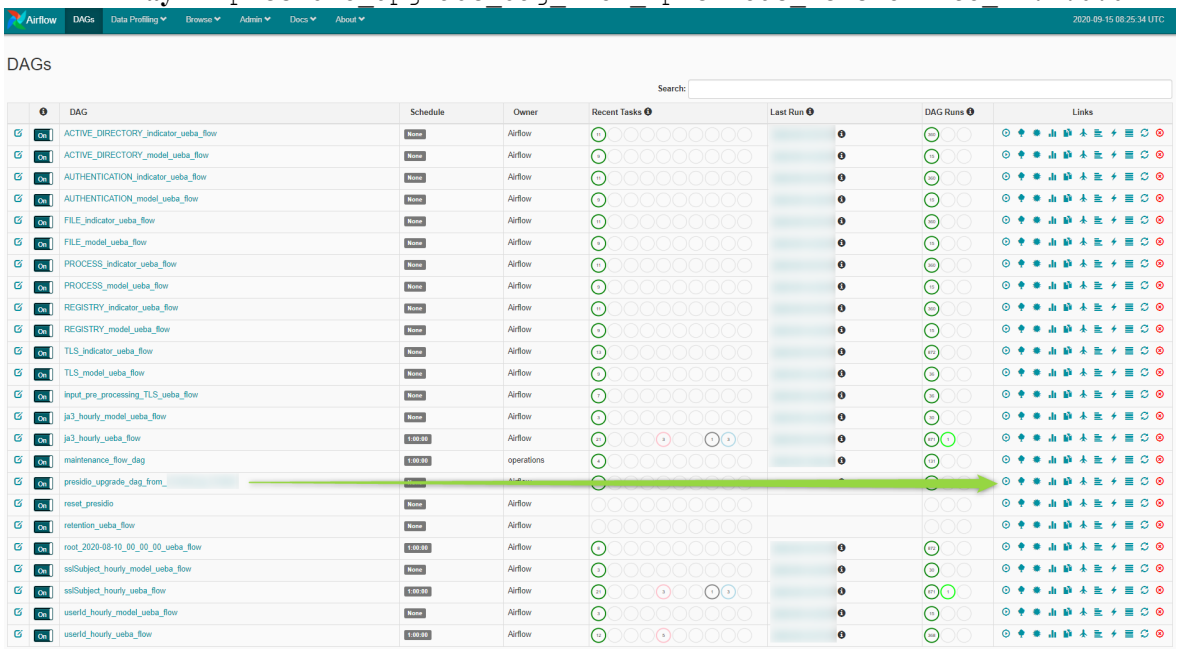
1. Update the UEBA configuration using the following command from the UEBA machine.
   ```
   source /etc/sysconfig/airflow

   source $AIRFLOW_VENV/bin/activate

   OWB_ALLOW_NON_FIPS=on python
   /var/netwitness/presidio/airflow/venv/lib/python2.7/site-packages/presidio_
   workflows-1.0-py2.7.egg/presidio/resources/rerun_ueba_server_config.py
   ```
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_12.2.0.0`.



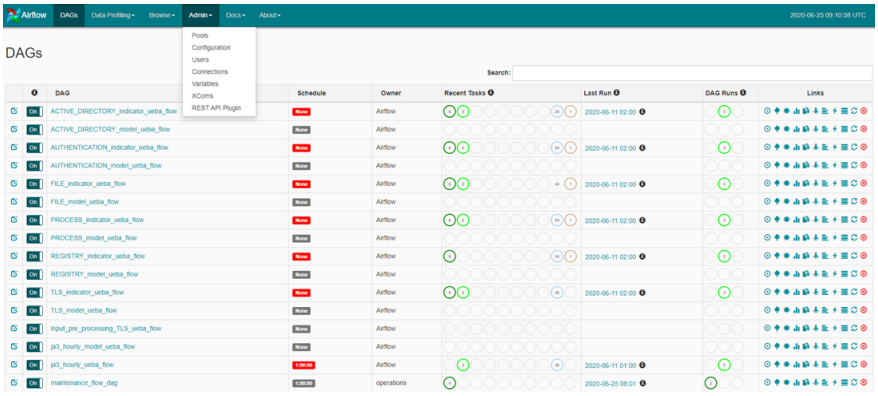
Note: A light green circle will appear next to the upgrade DAG row during the upgrade. If the upgrade process is completed successfully the light green circle changes to green. If the upgrade process fails, the light green circle changes to red.

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

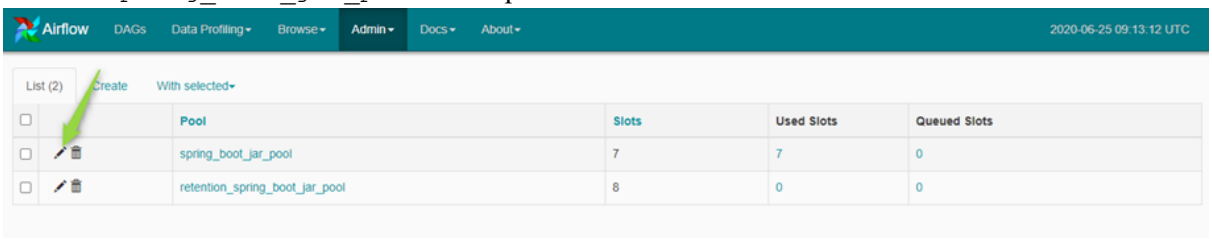
- **Physical Appliance**: Update the `spring_boot_jar_pool` slot value be 18.
- **Virtual Appliance**: Update the `spring_boot_jar_pool` slot value to 22.
  To update the **Spring Boot Jar Pools** slots, go to the Airflow main page, tap the **Admin** tab at the top bar and tap **Pools**.

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.



6. Import the Elasticsearch presidio data after upgrading the UEBA host from 12.0 and older versions to 12.2.0.0. Make sure the following prerequisites are met before you import the Elasticsearch presidio data:

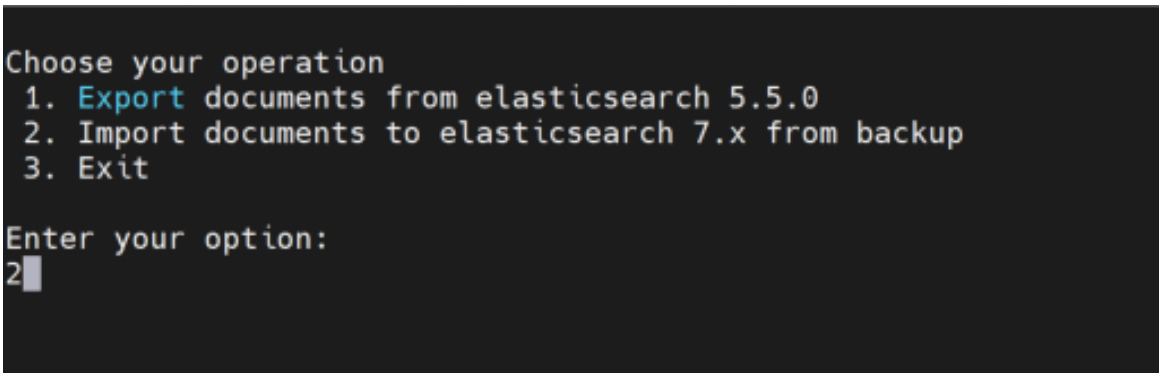
- Elasticsearch version must be upgraded to 7.17.6 from 5.5.0.
- UEBA host must be upgraded to 12.2.0.0
- UEBA rpm version must be 12.2.0.0.
- Elasticsearch data in 12.0.0.0 or older versions must be exported and stored in the Elasticsearch data backup folder located in the `/root/` directory.

To import the Elasticsearch data:

a. Go to `cd ueba_es_migration_tool`. Run the following command.

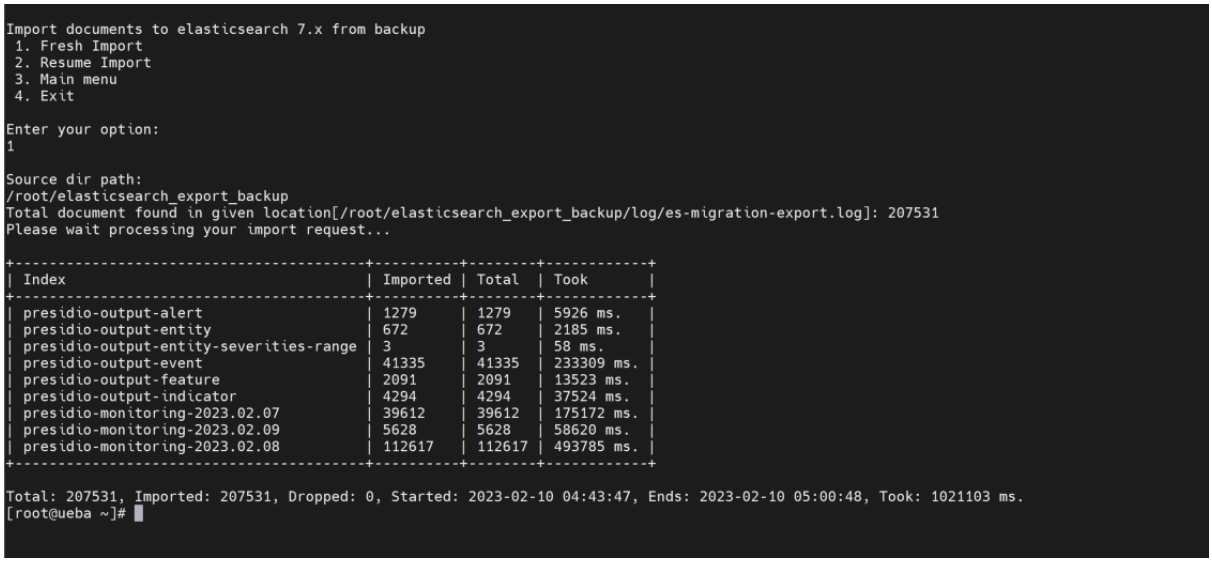
```
sh elk-migration-script.sh
```

The Elasticsearch migration tool guide is displayed.



b. Select **Import documents to elasticsearch 7.x from backup**.

c. In the next step, select **Fresh Import** to import the backup data.



d. Restart the Presidio UI service once the Import operation is completed. Run the following command.

```
systemctl restart presidio-ui
```

e. Go to the NetWitness Platform XDR **Users** tab and verify if all the Elasticsearch data is imported.

> **Note:**
> - Go to `<backup_directory_path>/log/log/es-migration-import.log` if you want to view the log for any exceptions.
> - If the Import operation fails due to some technical issue, select **Resume Import** once the issue is resolved, to resume the Import operation.

Endpoint Upgrade Tasks

Install the 12.2.0.0 Relay Server

If you have configured Relay Server, perform the following:

1. You must upgrade the Relay Server to 12.2.0.0 by downloading the Relay Server installer from the upgraded Endpoint 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.
2. Restart the Endpoint Server using the command:

   ```
   systemctl restart rsa-nw-endpoint-server
   ```

Upgrade Endpoint Agents

See "Upgrade Agents" in the *Endpoint Agent Installation Guide for NetWitness Platform 12.2* for instructions on how to upgrade agents.

Start Using New Features

There are many exciting new features that you can enable after you have upgraded to 12.2. For a detailed description of the new features in this release, see the *Release Notes for NetWitness Platform 12.2*. 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-11-7-to-12-1-1/ta-p/695650.

Appendix A. Set Up External Repo

Complete the following procedure to set up an external repository (Repo).

Note: 1.) You need an unzip utility installed on the host to complete this procedure. 2.) You must know how to create a web server before you complete the following procedure.

1. (Conditional) Complete this step if you have an external repo and you want to override it.
   - Case 1: You bootstrapped the host from an external repo and you want to upgrade using a local repo on the Admin Server.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/netwitness/platform/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://nw-node-zero/nwrpmrepo`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool.
   - Case 2: You bootstrapped the host from local repo on the Admin server (NW Server host) and you want to use an external repo for the upgrade.
     a. Create the `/etc/netwitness/platform/repobase` file.
        `vi /etc/netwitness/platform/repobase`
     b. Edit the `repobase` file so that the only information in the file is the following URL.
        `https://<webserver-ip>/<alias-for-repo>`
     c. Complete the instructions on how to run the upgrade using the `upgrade-cli-client` tool. The instructions are in "Option 3: Upgrade NetWitness Platform XDR using CLI (Offline)" in the Upgrade Tasks topic in the *Upgrade Guide for NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.
2. Set up the external repo.
   a. Log in to the web server host.
   b. Create directory to host the NW repository (`netwitness-12.2.0.0.zip`), for example `ziprepo` under `web-root` of the web server. For example, /var/netwitness is the web-root, run the following command string.
      `mkdir -p /var/netwitness/<your-zip-file-repo>`
   c. Create the 12.2.0.0 directory under `/var/netwitness/<your-zip-file-repo>`.
      `mkdir -p /var/netwitness/<your-zip-file-repo>/12.2.0.0`
   d. Create the `OS` and `RSA` directories under `/var/netwitness/<your-zip-file-repo>/12.2.0.0`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/12.2.0.0/OS`
      `mkdir -p /var/netwitness/<your-zip-file-repo>/12.2.0.0/RSA`

e. Unzip the `netwitness-12.2.0.0.zip` file into the `/var/netwitness/<your-zip-file-repo>/12.2.0.0` directory.
`unzip netwitness-12.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/12.2.0.0`

Unzipping `netwitness-12.2.0.0.zip` results in two zip files (`OS-12.2.0.0.zip` and `RSA-12.2.0.0.zip`)
and some other files.

f. Unzip the:
`OS-12.2.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/12.2.0.0/OS` directory.
`unzip /var/netwitness/<your-zip-file-repo>/12.2.0.0/OS-12.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/12.2.0.0/OS`

The external url for the repo is `http://<web server IP address>/<your-zip-file-repo>`.

g. Unzip the:
`RSA-12.2.0.0.zip` into the `/var/netwitness/<your-zip-file-repo>/12.2.0.0/RSA` directory.
`unzip /var/netwitness/<your-zip-file-repo>/12.2.0.0/RSA-12.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/12.2.0.0/RSA`

h. (Conditional - For Azure) Follow these steps for Azure update.

i. `mkdir -p /var/netwitness/<your-zip-file-repo>/12.2.0.0/OS/other`

ii. `unzip nw-azure-12.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/12.2.0.0/OS/other`

iii. `cd /var/netwitness/<your-zip-file-repo>/12.2.0.0/OS`

iv. `createrepo`

i. Use the `http://<web server IP address>/<your-zip-file-repo>` in response to **Enter the base URL of the external update repositories** prompt from NW 12.2.0.0 Setup program (`nwsetup-tui`) prompt.

Troubleshooting Installation and 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 update 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.

- 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
- OpenSSL 1.1.x 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. 2. From here, disable FIPS using the following command: `manage-stig-controls --disable-control-groups 3 --host-all` 3. Verify the line `FIPS=1` is removed from `/boot/grub2/grub.cfg` • If not, run the following command:

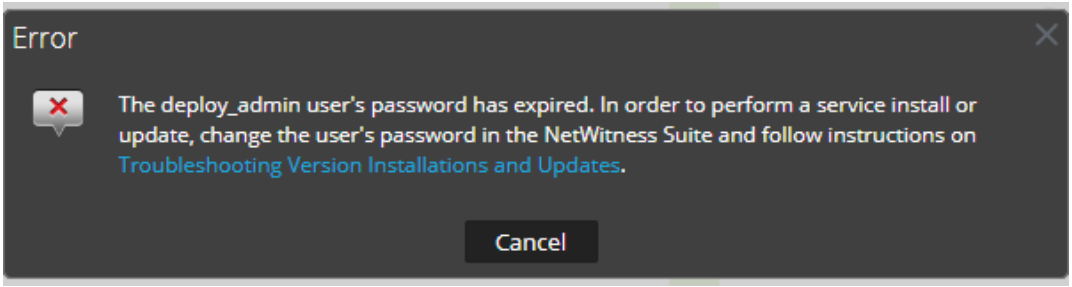
```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

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

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

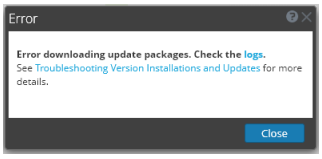
6. Reboot again.

deploy_admin User Password Has Expired Error

Error Message	
Cause	The `deploy_admin` user password has expired.

Solution	Reset your `deploy_admin` password password.
	1. On the NW Server host only, run the following command.
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	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.
	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.

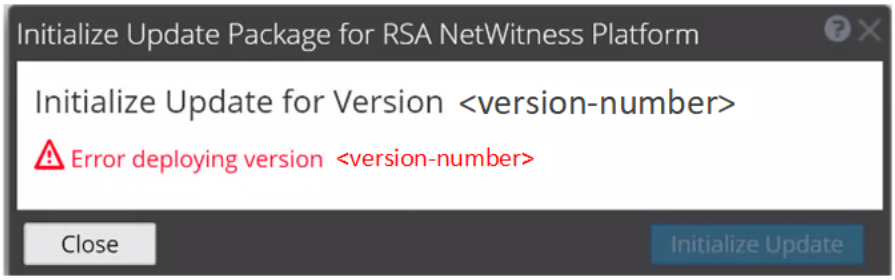
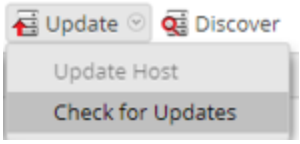
Downloading Error

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. 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. 3. If you are still not able to update, contact Customer Support.

Error Message	If you are upgrading from NetWitness Platform 11.x.x.x to 11.6.x.x or later, offline UI upgrade fails with the Download error message.

Solution	1. In the Command Line Interface (CLI):
	a. SSH to NW Server.
	b. Run the following command:
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version <version number>`
	For example:
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.6.0.0`
	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.
	3. Click **Reboot Host** from the toolbar.
	You can upgrade all the other hosts directly from the user interface:
	1. Click **Begin Update** from the Update Available dialog.
	After the host is upgraded, it prompts you to reboot the host.
	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. 2. Remove the version folder from staging folder. 3. Make sure that the salt-master service is running. 4. Recopy the update package zip file to the staging folder. 5. In the Hosts view toolbar, select Check for Updates again.  6. Click **Initialize Update**. 7. Click **Update** > **Update Hosts** from the toolbar. 8. Click **Begin Update** from the **Update Available** dialog. After the host is updated, it prompts you to reboot the host. 9. Click **Reboot** from the toolbar.

Upgrade Failed Error

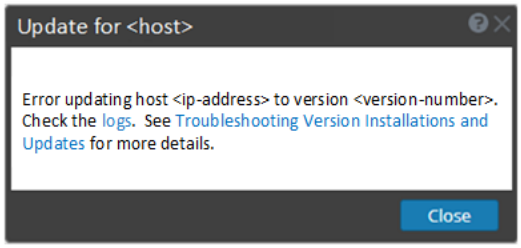
Error Message	Received an error in the error log similar to the following when trying to update to version 11.6 or later: `FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version 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, follow the below steps.
	1. SSH to Admin Server.
	2. Locate the component descriptor file by running the following command.
	`cd /etc/netwitness/component-descriptor/`
	3. Open the component descriptor file by running the following command.
	`vi nw-component-descriptor. json`
	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.
	`"concentrator": {`
	`"cookbook_name": "rsa-concentrator",`
	`"service_names": ["rsa-nw-concentrator"],`
	`"family": "launch",`
	`"default_port": xxxx, "description": "Concentrator",`
	`"packages":[{ "name": "rsa-nw-concentrator",`
	`"version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"`
	`},`
	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.
	`"packages": [{`
	`"name": "rsa-nw-concentrator"`
	`},`
	Note: You must delete the version details for all the host that has custom builds/rpms in the component descriptor of the admin server.
	6. Run the upgrade process again.

External Repo Update Error

Error Message	Received an error similar to the following error when trying to update to a new version from the : `.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	There is an error the path you specified.
Solution	Make sure that: • the URL does exist on the NW Server host. • 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.
	Often this is all you need to do.
	2. If you still cannot apply the new version update:
	Monitor the following logs on NW Server as it progresses (for example, run the `tail -f` command from the command line):
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	The error appears in one or more of these logs.
	3. If you still cannot apply the update, gather the logs from step 2 and contact Customer Support.

Missing Update Packages Error

Error Message	**Initialize Update for Version xx.x.x.x** Missing the following update package(s) 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. The NetWitness Community page that contains the update files for the selected version is displayed. 2. Select the missing packages from the staging folder. The **Initialize Update Package for NetWitness Platform** dialog is displayed telling

	you that it is ready to initialize the update packages.

OpenSSL 1.1.x

Error Message	The following example illustrates an ssh error that can occur when the ssh client is run from a host with OpenSSL 1.1.x installed: `$ ssh root@10.1.2.3` **`ssh_dispatch_run_fatal: Connection to 10.1.2.3 port 22: message authentication code incorrect`**

Problem	Advanced users who want to ssh to a NetWitness Platform host from a client that is using OpenSSL 1.1.x encounter this error because of incompatibility between CENTOS 7.x and OpenSSL 1.1.x. For example:
	`$ rpm -q openssl`
	`openssl-1.1.1-8.el8.x86_64`

Solution	Specify the compatible cipher list on the command line. For example:
	`$ ssh -oCiphers=aes128-ctr,aes192-ctr,aes256-ctr root@10.1.2.3`
	`I've read & consent to terms in IS user agreement.`
	`root@10.1.2.3's password:`
	`Last login: Mon Oct 21 19:03:23 2019`

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: **`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	You have two options: • 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 receive a message in the User Interface to reboot the host after you update and reboot the host offline.

Cause	You cannot use CLI to reboot the host. You must use the User Interface.
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, do the following: 1. Check which database files are corrupted: Navigate to the file located at `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` and check the following blocks: • If the live charts 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.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! • 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, perform the following steps:

	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. 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 version 11.6 or later, the Reporting Engine service does not restart.
Cause	The Reporting Engine service may not start due to any of the following reasons. - workspace.xml not updated. - Time is not converted properly in livechart h2 database. - 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.
	Note: You can find the Reporting Engine Migration Recovery tool in the below location.
	`/opt/rsa/soc/reporting-engine-<version number>-<Tag>/nwtools`
	For example:
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	1. SSH to Admin Server.
	2. Untar the RE (Reporting Engine) tool, run the following command.
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	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.
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	4. Run the script, run the following command.
	`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`

	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 "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. `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`

Solution	To resolve the issue, do the following steps,
	1. SSH to the Decoder host.
	2. Run the following commands.
	`yum reinstall pfring*`
	`systemctl restart nwdecoder`

NW Server

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

Problem	After upgrade, you notice that Audit logs are not getting forwarded to the configured Global Audit Setup; or, The following message seen in the `sa.log`. `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. 2. Submit the following command. `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. 2. Retried the upgrade for this host and it failed again. You will see the following message in the `orchestration-server.log`. `"'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.
	2. Submit the following commands.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Retry the upgrade of the non-NW Server host.

Problem	When you install and orchestrate a fresh 12.2 core Node-X to the Admin server (Node-0) upgraded from 12.0 or older versions to 12.2, 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. This is not applicable if you are orchestrating a fresh 12.2 core Node-X to the fresh-Installed 12.2 Admin Server (not upgraded from 12.0 or older versions to 12.2).
Cause	The 12.2 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 12.2 Admin Server host.

Solution	1. Before you bootstrap and orchestrate the 12.2 core Node-X host, run the following commands.
	`mkdir -p /etc/netwitness/platform`
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	2. Perform this workaround only if you skip the above workaround (Workaround 1). Run the following commands after you bootstrap and orchestrate the 12.2 core Node-X host.
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	`nw-manage --refresh-host --host-key <core-node-x-salt-minion-uuid>`
	`systemctl restart <core-service-name>`
	Note:
	- 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 12.1.1 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, do the following steps. In the NetWitness user interface, 1. Go to (**CONFIGURE**) > **Policies** > **Content** > **Event Stream Analysis** > **Data Sources**. The **Data Sources** panel is displayed. 2. Select the data source and click **Edit Datasource** in the toolbar. The **Edit Datasource** dialog is displayed. 3. In the **Edit Datasource** dialog, do one of the following: • Select **Trusted Authentication**. • Select **Use Credentials** and enter the Username and Password. 4. Click **Test Connection** to make sure that it can communicate with the ESA service and then click **OK**. **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

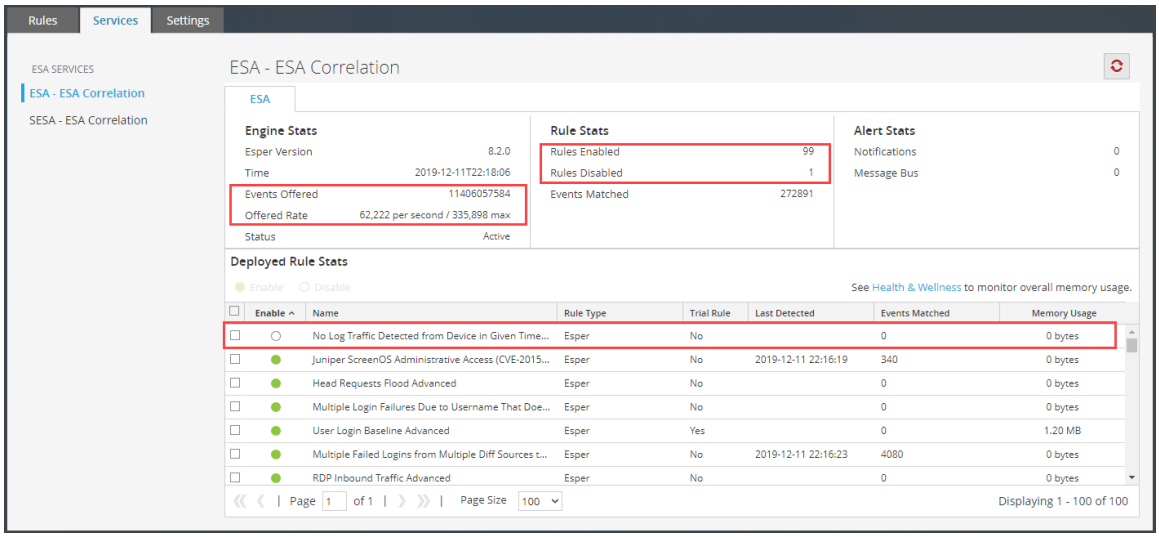
Problem	• Legacy Windows Log Collector appears as inactive post upgrade of SA to 12.2.0.0 version and Legacy Windows Log Collector to 11.6.x or 11.7.x versions. • Legacy Windows Log Collector appears as inactive when the stack is upgraded to 12.2.0.0.
Cause	Certificate update in the SA node.
Solution	Refer Legacy Windows Log Collector section in the 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) > ESA Rules > Services** tab.
   The Services view is displayed, which shows the status of your ESA services and deployments.
2. In the options panel on the left, select an ESA service.
3. For each service listed, look at the deployment tabs in the panel on the right. Each tab represents a separate ESA rule deployment.
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 deploymIent.
   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.

Endpoint, UEBA, and Live Content Rules are Not Working

To support Endpoint and UEBA content as well as changes to ESA rules from Live, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service. In NetWitness Platform 11.4 or later, ESA automatically adjusts the operator in the rule statement when there is a change from string to string array, but you still may need to make manual adjustments to adjust for the string array changes.

To change the string type meta keys to string array type meta keys manually in 11.4 or later, see “Configure Meta Keys as Arrays in ESA Correlation Rule Values” in the *ESA Configuration Guide*.

To use the latest Endpoint, UEBA, and Live content rules, the following default **multi-valued** meta keys are required on the ESA Correlation service in NetWitness Platform version 11.4 or later:

```
action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file
, analysis.service , analysis.session , boc , 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 , email.dst , email.src , eoc , 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 ,
inv.category , inv.context , ioc , ip.orig , ipv6.orig , netname , 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 , username
```

The following default **single-valued** meta keys are also required on the ESA Correlation service in NetWitness Platform 11.4 or later:

```
accesses , context.target , file.attributes , logon.type.desc , packets
```

To update your meta keys, see "Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules" in the *ESA Configuration Guide*.

If you used any meta keys in the ESA rule notification templates from the Required String Array or String Meta Keys list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Note: Advanced EPL rules may get disabled and are not automatically updated so they must be fixed manually.

For additional troubleshooting information, see “Troubleshoot ESA” in the *Alerting with ESA Correlation Rules User Guide for NetWitness Platform*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

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
```

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- See Troubleshooting section in the guides.
- See https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875 for information related to the End of Life (EOL) of appliances and the products.
- See also https://community.netwitness.com/t5/netwitness-community-blog/bg-p/netwitness-blog.
- If you need further assistance, contact NetWitness Support.

Contact NetWitness Support

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

- The version number of the NetWitness Platform product or application you are using.
- The type of hardware you are using.

Use the following contact information if you have any questions or need assistance.

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