

NetWitness[®] Platform XDR

Version 12.2.0.1

Release Notes

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 and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

July, 2023

Contents

What's New	5
Security Fixes	5
Upgrade Paths	6
Fixed Issues	7
Reporting Engine Fixes	7
Administration Fixes	7
Endpoint Fixes	8
Upgrade Instructions	9
Running in Mixed Mode	9
Upgrade Tasks	10
Important Notes	10
Synchronize Time on Component Hosts with NW Server Host	10
Mixed Mode Unsupported for ESA Hosts	10
Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 12.2.0.1	10
Task 1: Upgrade External Repository	10
Task 2: Disable Decoder Services	11
Task 3: Upgrade the Patch	11
Upgrade Options	13
Option 1: Upgrade NetWitness Platform XDR	13
Prerequisites	13
To Upgrade NetWitness Platform XDR:	14
Option 2: Upgrade NetWitness Platform XDR Offline	15
Download the 12.2.0.1 Patch	15
Option 3: Upgrade NetWitness Platform XDR using CLI (Offline)	16
Download the 12.2.0.1 Patch	16
Procedure	17
External Repo Instructions for CLI Upgrade	19
Option 4 (Optional): Pre-Stage Upgrade Repository by Downloading Packages	20
Post-Upgrade Tasks	22
Post Upgrade Tasks for Customers Upgrading from versions 11.6.1.3 or 11.6.1.4	22
Task 1 (Optional) - Move the Custom Certificates	22
Task 2 - Enable Decoder Services	22
Task 3 (Optional) - Remove Old Plugins and Reinstall Export Connector Plugin	22
Getting Help with NetWitness Platform	24
Self-Help Resources	24
Contact NetWitness Support	24

Product Documentation	24
Feedback on Product Documentation	25
Build Numbers	26
Firmware and BIOS Updates	27

What's New

This release notes provides information about the changes in NetWitness Platform 12.2.0.1.

Security Fixes

This patch release of NetWitness addresses the following vulnerability:

- CVE-2022-2132
- CVE-2022-37434
- CVE-2022-4378
- CVE-2022-42703
- CVE-2023-0286
- CVE-2023-0767
- CVE-2023-21930
- CVE-2023-21939
- CVE-2023-21954
- CVE-2023-21967
- CVE-2023-21937
- CVE-2023-21938
- CVE-2023-21968

For more information, refer the following security advisories:

- <https://community.netwitness.com/t5/netwitness-platform-security/nw-2023-05-multiple-components-within-netwitness-platform-xdr/ta-p/698474>.
- <https://community.netwitness.com/t5/netwitness-platform-security/nw-2023-03-multiple-components-within-netwitness-platform-xdr/ta-p/697207>.

Note: If you have the Export Connector plugin in your deployment, you must do the following:

- If you have Logstash installed separately, not as part of the NetWitness installation, you must uninstall the Export Connector plugin and install the updated Export Connector plugin after 12.2.0.1 patch upgrade. In this case, the old Export Connector plugin files are not automatically removed after upgrade. You must remove the old plugin files, so the scans do not list them as vulnerabilities. For more information on how to remove the old plugin files and install the updated plugins, see [Post-Upgrade Tasks](#).

- If you have Logstash installed as part of the NetWitness installation on the Log Collector service, the updated Export Connector plugin will be automatically installed during the 12.2.0.1 patch upgrade.

Upgrade Paths

The following upgrade paths are supported for NetWitness 12.2.0.1:

- 12.2.0.0 to 12.2.0.1
- 12.1.1.0 to 12.2.0.1
- 12.1.0.1 to 12.2.0.1
- 12.1.0.0 to 12.2.0.1
- 12.0.0.0 to 12.2.0.1
- 11.7.3.0 to 12.2.0.1
- 11.7.2.0 to 12.2.0.1
- 11.7.1.2 to 12.2.0.1
- 11.7.1.1 to 12.2.0.1
- 11.7.1.0 to 12.2.0.1
- 11.7.0.2 to 12.2.0.1
- 11.7.0.1 to 12.2.0.1
- 11.7.0.0 to 12.2.0.1
- 11.6.1.4 to 12.2.0.1
- 11.6.1.3 to 12.2.0.1

Warning: Before upgrading the UEBA host to 12.2.0.1, 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 *NetWitness UEBA Configuration Guide for 12.2*.


Fixed Issues

This section lists issues fixed after the last major release. For additional information on fixed issues, see the Fixed Version column in the [NetWitness® Platform Known Issues list](#) on NetWitness Community.

Reporting Engine Fixes

Tracking Number	Description
ASOC-131062	When you select any time range except Custom for the first time and click Run Test in Reports > Manage > Charts > Select and Edit a chart > Test Chart to test the chart, the error message Cannot request the chart test is displayed. As a result, the charts cannot be tested.
ASOC-131063	When you create and then schedule the Reports or Alerts using the SFTP Output action, the data is not sent to the configured SFTP Output action in the form of PDF or CSV. The status of the report schedule or alert schedule is displayed as Partial in the Report Schedule view or Alert Schedule view.

Administration Fixes

Tracking Number	Description
ASOC-130883	When you update or delete any group mapping in  (Admin) > Event Sources > Manage , the changes are not pushed to Log Decoders. This happens even though the ESM Feed file uploaded to the Log Decoder captures the updated information. This is due to the connection failure between SMS and Log Decoder. Consequently, the accurate information about the group mappings is not displayed in the Investigate page.
ASOC-130904	When the Jetty service runs for a longer duration without a restart, the Metaspace memory exhausts and the error message nw-jetty-wrapper.sh: java.lang.RuntimeException: java.lang.OutOfMemoryError: Metaspace is displayed.

Endpoint Fixes

Tracking Number	Description
ASOC-131058	While fetching the metas for fileProperties , the Endpoint Server memory usage increases. This issue occurs when multiple queries are made on the Mongo DB to fetch the metas.

Upgrade Instructions

You need to read the information and follow these procedures for upgrading NetWitness version 12.2.0.1.

Upgrade Path	Downloads Required
From 11.6.1.3, 11.6.1.4, 11.7.0.0, 11.7.0.1, 11.7.0.2, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 11.7.3.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, and 12.1.1.0 to 12.2.0.1	<ul style="list-style-type: none">• 12.2.0.0 base pack• 12.2.0.1 patch release
From 12.2.0.0 to 12.2.0.1	<ul style="list-style-type: none">• 12.2.0.1 patch release

You can upgrade 12.2.0.1 patch using one of the following options:

- If the NetWitness Server has internet connectivity to Live Services, the NetWitness Platform User Interface can be used to apply the patch.
- If the NetWitness Server does not have internet connectivity to Live Services, the Command Line Interface (CLI) or the NetWitness Platform User Interface can be used to apply the patch.

Note: If you are using S4s device that utilizes SD cards, SSH to NW Server and run the following command before starting the upgrade process.
`manage-stig-controls --disable-control-groups 7 --host-id <node uuid>.`

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. For more information see the topic "Running in Mixed Mode" in the [NetWitness Platform Hosts and Services Getting Started Guide](#).

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

Upgrade Tasks

Important Notes

This section lists few important notes you must read before proceeding with the upgrade tasks.

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

Respond Server Service Not Enabled Until NW Server and Primary ESA Host Upgraded to 12.2.0.1

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

Task 1: Upgrade External Repository

Note: Perform the below steps only if you are using an external repository for 12.2.0.1.

To upgrade the external repository which is an externally managed server, do the following:

1. Upgrade the external repository with the latest upgrade content for the NetWitness Platform XDR `netwitness-12.2.0.1.zip`.



The following is the structure after upgrading the external repository:

```
|-12.2.0.0
|---OS
|-----repodata
|---RSA
|-----repodata
|-12.2.0.1
|---OS
|-----repodata
|---RSA
|-----repodata
|-cloud-extras
|---RSA
|-----repodata
```

Task 2: Disable Decoder Services

Before upgrading to 12.2.0.1, you must disable **Capture AutoStart** option on Network Decoder and Network Hybrid Services.

To disable Capture Autostart:

1. Go to  (Admin) > Services.
The Administration Services view is displayed.
2. Select a Network Decoder or Network Hybrid service and select  > **View** > **Config**.
The services config view for the selected Network Decoder or Network Hybrid is displayed.
3. In the **Decoder Configuration** panel, deselect the **Capture Autostart** and click **Apply**.

Task 3: Upgrade the Patch

You can choose one of the following upgrade methods based on your internet connectivity.

- [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](#)

Upgrade Options



Option 1: Upgrade NetWitness Platform XDR

You can use this method if the NetWitness Server host is connected to Live Services and can obtain the package.

Note: If the NetWitness Server does not have access to Live Services, use [Option 2: Upgrade NetWitness Platform XDR Offline](#) or [Option 3: Upgrade NetWitness Platform XDR using CLI \(Offline\)](#)

Prerequisites


Make sure that:

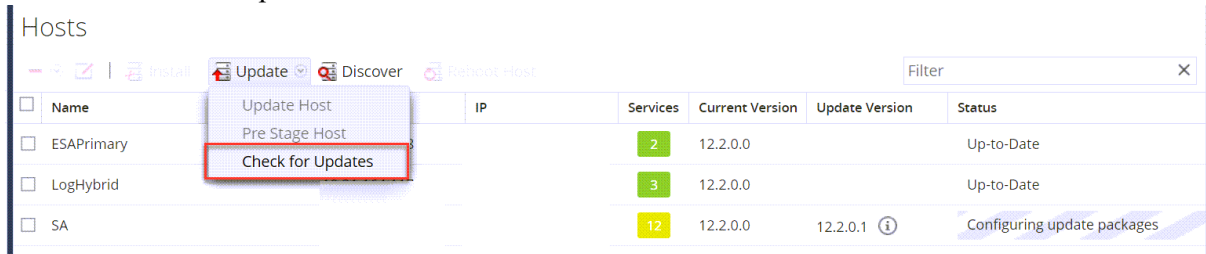
1. The **Automatically download information about new upgrades every day** option is selected and is applied in  **(Admin) > System > Updates**.
2. Go to  **(Admin) > Hosts > Update > Check for Updates** to check for upgrades. The Host page displays the **Update Available** status.
3. **12.2.0.1** is available under **Update Version** column.

Note: If you have custom certificates, move any custom certificates from `/etc/pki/nw/trust/import/` directory to `/root/cert`. Follow these steps to move the certificates:

- `mkdir /root/cert`
- `mv /etc/pki/nw/trust/import/* /root/cert`

To Upgrade NetWitness Platform XDR:

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



The screenshot shows the 'Hosts' management page. The 'Update' dropdown menu is open, showing three options: 'Update Host', 'Pre Stage Host', and 'Check for Updates'. The 'Check for Updates' option is highlighted with a red box. Below the menu is a table with columns: Name, IP, Services, Current Version, Update Version, and Status.

Name	IP	Services	Current Version	Update Version	Status
ESAPrimary		2	12.2.0.0		Up-to-Date
LogHybrid		3	12.2.0.0		Up-to-Date
SA		12	12.2.0.0	12.2.0.1 ⓘ	Configuring update packages

Note: In 11.7.1.0 and later versions, the (optional) **Pre Stage Host** option is added in the **Update** drop-down list. For more information, see [Option 4 \(Optional\): Pre-Stage Upgrade Repository by Downloading Packages](#).

4. **Update Available** is displayed in the **Status** column if you have a version upgrade in your Local Update Repository for the selected host.
5. Select **12.2.0.1** 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 upgrades automatically to show **Update Available**. By default, only supported upgrades for the selected host are displayed.
6. Click **Update > Update Host** from the toolbar.
7. Click **Begin Update**.
8. Click the **Reboot Host** when prompted.
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 NetWitness Server host. All ESA, Endpoint, and Malware Analysis hosts should be upgraded to the same version as that of NW Admin Server or NetWitness Server host.
- Not all components have been changed for 12.2.0.1, so after you perform the upgrade steps, it is normal to see some components with different version numbers. For a list of the components that were upgraded for this release, see [Build Numbers](#).

Option 2: Upgrade NetWitness Platform XDR Offline

When you apply version upgrades:

- You must upgrade the NW Server host first.
- You can only apply a version that is compatible with the existing host version.

Download the 12.2.0.1 Patch

Download the NetWitness Platform XDR 12.2.0.1 Upgrade Pack file (`netwitness-12.2.0.1.zip`), which contains all the NetWitness Platform 12.2.0.1 upgrade files, from the NetWitness Community <https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads> to a local directory.

Upgrading from	Download and Stage file
11.6.1.3, 11.6.1.4, 11.7.0.0, 11.7.0.1, 11.7.0.2, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 11.7.3.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, and 12.1.1.0	<code>netwitness-12.2.0.0.zip</code> and <code>netwitness-12.2.0.1.zip</code>
12.2.0.0	<code>netwitness-12.2.0.1.zip</code>

Note: If you get the **Download Error**, see the [Troubleshooting](#) information for resolution.

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

- If you are upgrading from 11.6.1.3, 11.6.1.4, 11.7.0.0, 11.7.0.1, 11.7.0.2, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 11.7.3.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, or 12.1.1.0 to 12.2.0.1, download the `netwitness-12.2.0.0.zip` and `netwitness-12.2.0.1.zip`, upgrade package from NetWitness Community to a local directory.
- If you are upgrading from 12.2.0.0 to 12.2.0.1, download the `netwitness-12.2.0.1.zip`, upgrade package from NetWitness Community to a local directory.

1. SSH to the NW Server host.
2. If you are upgrading from 11.6.1.3, 11.6.1.4, 11.7.0.0, 11.7.0.1, 11.7.0.2, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 11.7.3.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, or 12.1.1.0 to 12.2.0.1, copy `netwitness-12.2.0.0.zip` and `netwitness-12.2.0.1.zip` from the local directory to the `/var/netwitness/common/update-stage/` staging folder. For example:

```
mv/var/netwitness/tmp/netwitness-12.2.0.0.zip
/var/netwitness/common/update-stage/
mv/var/netwitness/tmp/netwitness-12.2.0.1.zip
```


```
/var/netwitness/common/update-stage/
```

- If you are upgrading from 12.2.0.0 to 12.2.0.1, copy `netwitness-12.2.0.1.zip` from the local directory to the `/var/netwitness/common/update-stage/` staging folder. For example:

```
mv/var/netwitness/tmp/netwitness-12.2.0.1.zip
/var/netwitness/common/update-stage/
```

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

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

- Log in to NetWitness.
- Go to  (Admin) > Hosts.
- Check for updates and wait for the update packages to be copied, validated, and ready to be initialized.

"Ready to initialize packages" is displayed if:

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

Refer to [Troubleshooting Version Installations and upgrades](#) 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.)

- Click **Initialize Update**.

It takes some time to initialize the packages because the files are large and need to be unzipped. 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 update of the host.

- Click **Update** > **Update Hosts** from the toolbar.
- Click **Begin Update** from the **Update Available** dialog.
After the host is upgraded, it prompts you to reboot the host.
- Click **Reboot** from the toolbar.

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

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

Note: Alternatively, you can upgrade using the [Option 2: Upgrade NetWitness Platform XDR Offline](#).

Download the 12.2.0.1 Patch

Download the NetWitness 12.2.0.1 Upgrade Pack file (`netwitness-12.2.0.1.zip`), which contains all the NetWitness 12.2.0.1 upgrade files, from the NetWitness Community <https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads> to a local directory.

Upgrading from	Download and Stage file
11.6.1.3, 11.6.1.4, 11.7.0.0, 11.7.0.1, 11.7.0.2, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 11.7.3.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, and 12.1.1.0	netwitness-12.2.0.0.zip and netwitness-12.2.0.1.zip
12.2.0.0	netwitness-12.2.0.1.zip

Note: If you are using external repository, you can upgrade the external repository with the latest upgrade content. For more information see, [Task 1: Upgrade External Repository](#).

Procedure

You need to perform the upgrade steps for NetWitness Server host and for component hosts.

Note:

- If you copy paste the commands from PDF to Linux SSH terminal, the characters do not work. It is recommended to type the commands.
- Make sure you remove the update zip file from the staging directory after it is extracted.

- **If you are upgrading from 11.6.1.3, 11.6.1.4, 11.7.0.0, 11.7.0.1, 11.7.0.2, 11.7.1.0, 11.7.1.1, 11.7.1.2, 11.7.2.0, 11.7.3.0, 12.0.0.0, 12.1.0.0, 12.1.0.1, or 12.1.1.0,** you must stage 12.2.0.0 and 12.2.0.1. Log into the NW Server as `root` and create the following directory:
 - **Option 1 (Manual)** : Log into the NetWitness Server and create the following directories:


```
/var/netwitness/tmp/upgrade/12.2.0.0/
/var/netwitness/tmp/upgrade/12.2.0.1/
```

 and 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 commands:


```
unzip netwitness-12.2.0.0.zip -d /var/netwitness/tmp/upgrade/12.2.0.0/
unzip netwitness-12.2.0.1.zip -d /var/netwitness/tmp/upgrade/12.2.0.1/
```

 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/
```

 and then copy the NetWitness 12.2.0.0 and 12.2.0.1 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 12.2.0.1 zip files:


```
[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness
/tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.2.0.1
```

 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 12.2.0.1 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 12.2.0.1 --stage-dir /var/netwitness/tmp/upgrade`. If the initialization succeeds, ignore the [first step](#) under **Upgrading the NetWitness Server and component hosts** and proceed with the further steps 2-4.

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


```
/var/netwitness/tmp/upgrade/12.2.0.1/
```

 and 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-12.2.0.1.zip -d /var/netwitness/tmp/upgrade/12.2.0.1
```

 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/
```

 and then copy the NetWitness 12.2.0.1 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 12.2.0.1 zip files:


```
[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.2.0.1
```

 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 command `[root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness/tmp/upgrade --download-path /var/netwitness/tmp --version 12.2.0.1` again to stage 12.2.0.1.

IMPORTANT: After staging 12.2.0.1 (using the Option 2), if the initialization fails, run the command `upgrade-cli-client --init --version 12.2.0.1 --stage-dir /var/netwitness/tmp/upgrade`. If the initialization succeeds, ignore the [first step](#) under **Upgrading the NetWitness Server and component hosts** and proceed with the further steps 2-4.

Upgrading the NetWitness Server and component hosts

1. Initialize the upgrade using the following command:


```
upgrade-cli-client --init --version 12.2.0.1 --stage-dir /var/netwitness/tmp/upgrade
```

IMPORTANT: Once `init` is performed, do not reboot the NW Admin server or restart jetty.

2. Upgrade Netwitness Server using the following command:


```
upgrade-cli-client --upgrade --version 12.2.0.1 --host-key <ID / display name / (hostname/ IP address)>
```
3. When the component host upgrade is successful, reboot the host from NetWitness UI.

IMPORTANT: This is a mandatory step. Ensure that you reboot the host from the NetWitness UI.

4. Change the IP address to the component host being upgraded and repeat the steps 2 and 3 for each component host.

Note: You can check versions of all the hosts, using the command `upgrade-cli-client --list` on the NetWitness Server. 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 patch will install correctly. No action is required. If you encounter additional errors when upgrading a host to a new version, contact [Getting Help with NetWitness Platform](#).

External Repo Instructions for CLI Upgrade

Note: The external repo should have separate directories for 12.2.0.0 and 12.2.0.1, as described in [Option 3: Upgrade NetWitness Platform XDR using CLI \(Offline\)](#).

Note: Make sure you remove the update zip file from the staging directory after it is extracted.

1. Stage 12.2.0.1 by creating a directory on the NetWitness Server at `/var/netwitness/tmp/upgrade/12.2.0.1` and extract the zip package.
`unzip netwitness-12.2.0.1.zip -d /var/netwitness/tmp/upgrade/12.2.0.1`
2. Initialize the upgrade using the following command:
`upgrade-cli-client --init --version 12.2.0.1--stage-dir /var/netwitness/tmp/upgrade`
3. Upgrade Netwitness Server using the following command:
`upgrade-cli-client --upgrade --version 12.2.0.1 --host-addr <IP of Netwitness Server>`
4. When the component host upgrade is successful, reboot the host from NetWitness UI.
5. Change the IP address to the component host being upgraded and repeat the steps 3 and 4 for each component.


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

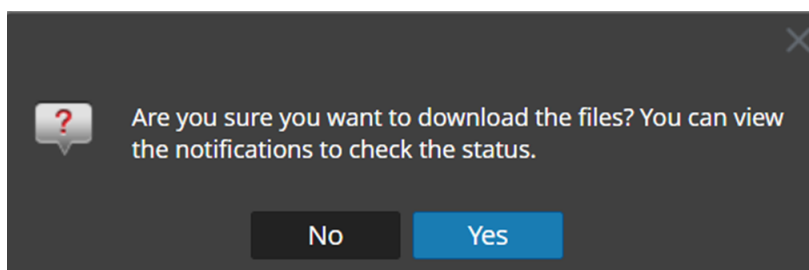
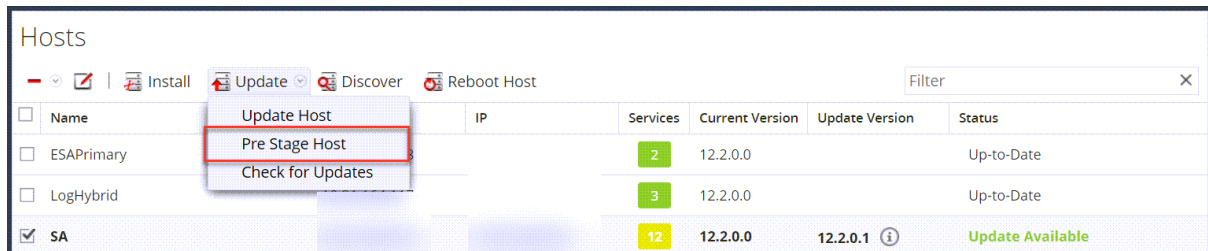
Note: If the following error displays during the upgrade process:
 2017-11-02 20:13:26.580 ERROR 7994 - [127.0.0.1:5671]
 o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
 protocol method: #method<connection.close>(reply-code=320, reply-
 text=CONNECTION_FORCED - broker forced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

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

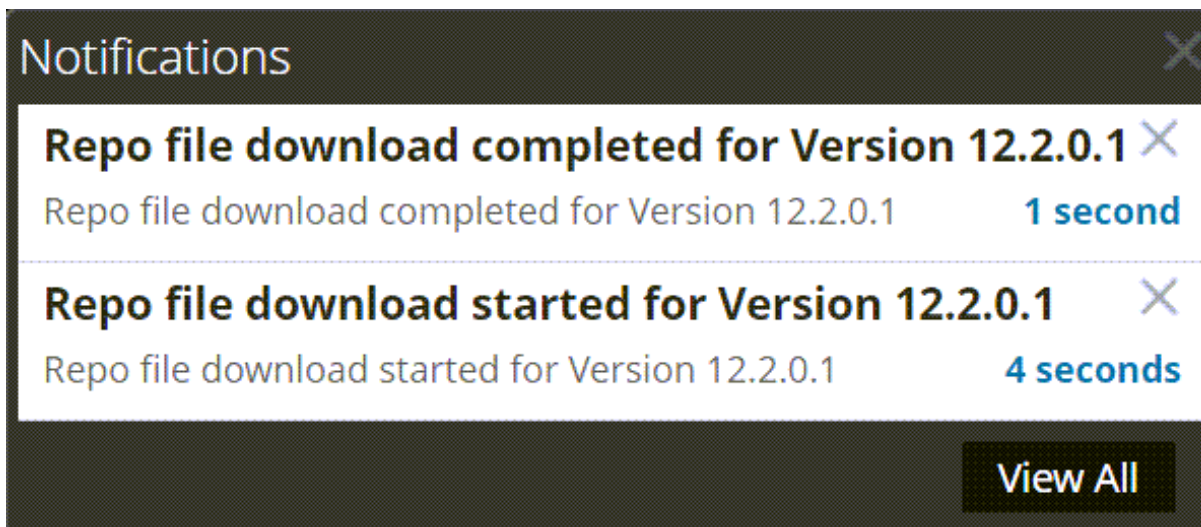
You can pre-stage the upgrade repository by downloading the required packages (.zip) without affecting the system. This minimizes the upgrade downtime and ensures the upgrade is completed within the planned time.

To Pre-Stage the Upgrade Repository

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.



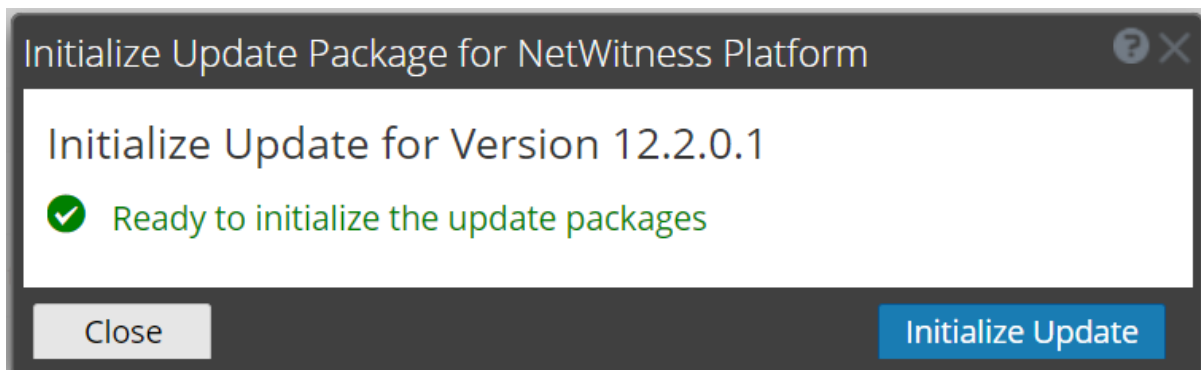
4. Click **Yes** to download the upgrade packages to the repo.
5. Verify the status of the download in the notifications tray as shown below.
The **Pre Stage Host** and **Upgrade Host** will be disabled until pre stage is completed.



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 and reboot the host.

Post-Upgrade Tasks

This topic provides information about the tasks performed after upgrading from 11.6.1.3 or 11.6.1.4 to 12.2.0.1.

Post Upgrade Tasks for Customers Upgrading from versions 11.6.1.3 or 11.6.1.4



Task 1 (Optional) - Move the Custom Certificates

Move the custom certificates from external directory to `/etc/pki/nw/trust/import` directory.

Task 2 - Enable Decoder Services

After you upgrade to 12.2.0.1, you must enable Capture AutoStart on Network Decoder and Network Hybrid Services.

To enable the Capture Autostart field:

1. Go to  **(Admin) > Services**.
The Administration Services view is displayed.
2. Select a Network Decoder or Network Hybrid service and select  **> View > Config**.
The services Config view for the selected Network Decoder or Network Hybrid is displayed.
3. In the **Decoder Configuration** panel, select the **Capture Autostart** field and click **Apply**.

Task 3 (Optional) - Remove Old Plugins and Reinstall Export Connector Plugin

Follow the below procedure only if you have export connector plugin in your deployment and logstash installed separately.

Remove the old plugin

You must remove the old plugin, so the scans do not list them as vulnerabilities.

1. Remove old Export Connector Plugin files. Do the following.

```
rm -rf /usr/share/logstash/vendor/bundle/jruby/2.5.0/logstash-
inputnetwitness_export_connector-1.x.x
rm -rf /usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/logstash-
inputnetwitness_export_connector-1.x.x
```

Note: 1.x.x can be 1.1.0 or 1.0.0

Install the updated plugin

If you have Logstash installed separately, not as part of the NetWitness installation, you must install the updated Export Connector plugin after 12.2.0.1 patch upgrade. For more information to install the updated plugin, see <https://community.netwitness.com/t5/netwitness-platform-online/install-netwitness-logstash-input-plugin/ta-p/669115>.

Restart the Log Collector

```
service nwlogcollector restart
```

Note: In case you have installed Logstash separately, outside NetWitness installation, the path and version of the plugin will be different. Restarting of the Log Collector service may not be required.

Getting Help with NetWitness Platform

Self-Help Resources

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

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, contact NetWitness Support.

Contact NetWitness Support

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

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

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

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

Product Documentation

The following documentation is provided with this release.

Documentation	Location URL
NetWitness Platform XDR All Versions Documents	https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246
NetWitness Platform XDR 12.2 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform XDR 12.2 Upgrade Guide	https://community.netwitness.com/t5/netwitness-platform-online/upgrade-guide-for-12-2/ta-p/696583

Feedback on Product Documentation

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

Build Numbers

The following table lists the build numbers for various components of NetWitness 12.2.0.1.

Component	Version Number
NetWitness Audit Plugins	12.2.0.1-4852.5
NetWitness Audit RT	12.2.0.1-4852.5
NetWitness Collectd	12.2.0.1-4852.5
NetWitness Collectd SMS	12.2.0.1-4852.5
NetWitness Bootstrap	12.2.0.1-2304050607.5
NetWitness Component Descriptor	12.2.0.1-2304240644.5
NetWitness Config Management	12.2.0.1-2304050608.5
NetWitness Deployment Upgrade	12.2.0.1-2304050610.5
NetWitness Endpoint Server	12.2.0.1-230414103313.5
NetWitness Legacy Web Server	12.2.0.1-230411132523.5
NetWitness RE Server	12.2.0.1-5969.5
NetWitness SMS Server	12.2.0.1-4852.5
NetWitness SMS Runtime RT	12.2.0.1-4852.5
NetWitness UI	12.2.0.1-230420080854.5
NetWitness Presidio Airflow	12.2.0.1-2304121254.5
NetWitness Presidio ConfigServer	12.2.0.1-2304121254.5
NetWitness Presidio Core	12.2.0.1-2304121254.5
NetWitness Presidio ElasticSearch Init	12.2.0.1-2304121254.5
NetWitness Presidio EXT NetWitness	12.2.0.1-2304121313.5
NetWitness Presidio Flume	12.2.0.1-2304121312.5
NetWitness Presidio Manager	12.2.0.1-2304121254.5
NetWitness Presidio Output	12.2.0.1-2304121254.5
NetWitness Presidio UI	12.2.0.1-2304121317.5

Firmware and BIOS Updates

NetWitness recommends updating the firmware to obtain the latest security fixes and enhancements. The recommended firmware versions have been tested and verified by NetWitness and will not affect the operation of the various hosts.

To update the firmware, you must download the Update Package for Microsoft Windows 64-Bit and refer to the recommended firmware levels. Some firmware versions may require a reboot to be effective. For more information, see [About Firmware and BIOS Updates](#).