NetWitness® Platform XDR

Version 12.0

Recovery Tool User 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

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

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

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

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

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

July, 2022

Contents

Disaster Recovery (Backup and Restore Instructions)

You can take a backup and restore of NetWitness Hosts using any of the following:

- (Recommended) NetWitness Recovery Wrapper Tool
- NetWitness Recovery Tool (NRT)

(Recommended) NetWitness Recovery Wrapper Tool

Note: NetWitness Recovery Wrapper tool is supported from NetWitness 11.6.1.4 and Later. In case of host with large volume of data (>500GB), NetWitness recommends to use NetWitness Recovery Tool (`nw-recovery-tool`) for backup.

NetWitness Recovery Wrapper Tool (NRWT) provides centralized backup and restore that makes it easy for you to take a backup of all the supported installation options (Physical Host, Virtual Host, AWS, and Azure). With NRWT you can:

- Backup (export) an individual, a specific, or all hosts at a time.
- Restore (import) an individual host at a time.
- Customize files or folders during backup and restore.
- Copy back up data to/from remote host location from/to Netwitness hosts provided:
  - Remote host is reachable via SSH from each NetWitness hosts.
  - The credentials are correct.
  - The location specified has sufficient space to take a backup in case of export.
  - The location specified should contain valid backup data in case of import.
- (For version 11.7.1 and Later) Back up Mongo databases for Endpoint and ESA instances
- (For version 11.7.1 and Later) Include Broker index for NetWitness node in which Broker service is running
- (For version 11.7.1 and Later) Back up custom files and folders provided by user

For details on previous run, check NRWT logs at `/var/log/netwitness/recovery-tool/nw-recovery-wrapper.log` on Admin Server.

Basic Usage of the NetWitness Recovery Wrapper Tool

You can use the NRWT to back up data by using the `export` option. To restore data, use the `import` option. The basic usage of the tool is to run the following command from the root directory level:

```
nw-recovery-wrapper [command] [option]
```

The commands and options that you can use with this tool are described in the following tables.

Commands and Options	Description
`-h --help`	Display help on commands and option. For example, specify: `nw-recovery-wrapper --help` to get a list of supported operations and arguments.
`-e, --export`	Export data or configuration.
`-i, --import`	Import data or configuration.
`-d, --dump-dir <path>`	Path for the where data will be exported or imported from (for example, `/var/netwitness/backup`).
`--host-key HOST_KEY [HOST_KEY ...]`	Host IP, ID or display name.
`--host-all`	specify for all hosts - supported only for export
`--include CUSTOM_PATH [CUSTOM_PATH ...]`	Custom path or file.
`--remote-location REMOTE_LOCATION`	Remote host path for remote host configuration.
`--remote-ip REMOTE_IP`	Remote host IP for remote host configuration.
`--remote-password REMOTE_PASSWORD`	Remote host password for remote host configuration.
`--remote-user REMOTE_USER`	User for remote host configuration.

Required Conditions

- Make sure that there is adequate disk space on dump directory to take the backup on each NetWitness Hosts.
- Valid Host key is entered. Host key can be Host ID, IP address or display name.

Back Up using NRT wrapper:

1. Backup NetWitness Hosts and store on local dump directory of each hosts:
   ```
   nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name> <Host 2 IP/ID/Name>......<Host N IP/ID/Name>

   nw-recovery-wrapper export --dump-dir <dir> --host-all
   ```
2. (Optional) Add custom files or folders during backup and restore other than what is predefined in recovery tool:

   Note: Make sure the custom files or directories are available on NetWitness Hosts, if not, the files or directories will be ignored.

   ```
   nw-recovery-wrapper export --dump-dir <dir> --include-file <custom files>/--include-dir --host-key <Host 1 IP/ID/Name> <Host 2 IP/ID/Name>......<Host N IP/ID/Name>
   nw-recovery-wrapper export --dump-dir <dir> --include-file <custom files>/--include-dir --host-all
   ```
3. (Optional) Copy backup data to remote Location:

   Note: Make sure that:
   - You specify valid values for `--remote-ip`, `--remote-location`, `--remote-password` arguments for remote copy operation.
   - Remote Host IP is valid and reachable via SSH from all NetWitness Hosts.
   - Remote Host location (`--remote-location`) has adequate space to take backup.

   ```
   nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name> <Host 2 IP/ID/Name>......<Host N IP/ID/Name> --remote-ip <IP ADDRESS of remote host> --remote-password <ssh-password> --remote-location <remote-location-where-backups-should-be-copied-to>
   nw-recovery-wrapper export --dump-dir <dir> --host-all --remote-ip <IP ADDRESS of remote host> --remote-password <ssh-password> --remote-location <remote-location-where-backups-should-be-copied-to>
   ```

   Note: Optional argument `--remote-user` defaults to root if you do not specify any value.

   Example:

   For adminserver, the backup folder name will be adminserver-backup-2021-09-08-12:48:13

4. Backup (export) including custom files or folders and copy to remote location:

> **Note:** Make sure that:
> - the custom files or directories are available on NetWitness Hosts, if not, the files or directories will be ignored.
> - You specify valid values for `--remote-ip`, `--remote-location`, `--remote-password` arguments for remote copy operation.
> - Remote Host IP is valid and reachable via SSH from all NetWitness Hosts.
> - Remote Host location (`--remote-location`) has adequate space to take backup.

```
nw-recovery-wrapper export --dump-dir <dir> --include <custom files/folder>
--host-key <Host 1 IP/ID/Name> <Host 2 IP/ID/Name>......<Host N IP/ID/Name>
--remote-ip <IP ADDRESS of remote host> --remote-password <ssh-password> --
remote-location <remote-location-where-backups-should-be-copied-to>
```

```
nw-recovery-wrapper export --dump-dir <dir> --include <custom files/folder>
--host-all --remote-ip <IP ADDRESS of remote host> --remote-password <ssh-
password> --remote-location <remote-location-where-backups-should-be-
copied-to>
```

```
optional argument: --remote-user defaults to root if argument is not
specified.
```

Example:

For Admin server, the backup folder name will be adminserver-backup-2021-09-08-12:48:13

5. (For version 11.7.1 and Later) (Optional) Include Mongo service.

> **Note:** Make sure that:
> - Mongo service is running on the NetWitness host.
> - `--host-all and --host-key` with multiple values are not supported for include Mongo operation.

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-mongo
```

6. (For version 11.7.1 and Later) (Optional) Include Broker index.

> **Note:** Make sure that:
> - Broker service is running on the NetWitness host.

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
<Host 2 IP/ID/Name>......<Host N IP/ID/Name> --include-broker-index
```

```
nw-recovery-wrapper export --dump-dir <dir> --host-all --include-broker-
index
```

7. (For version 11.7.1 and Later) (Optional) Backup (export) including Mongo and Broker index.

> **Note:** Make sure that:
> - Mongo service is running on the NetWitness host.
> - Broker service is running on the NetWitness host.
> - `--host-all and --host-key` with multiple values are not supported for include Mongo operation.

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-mongo --include-broker-index
```

8. (For version 11.7.1 and Later) (Optional) Backup (export) including custom files or folders, copying to remote location, Broker index and Mongo.

> **Note:** Make sure that:
> - Custom files or directories are present on NetWitness hosts to be backedup, if it is not present it skips the files or directory.
> - Fields such as `--remote-ip`, `--remote-location`, `--remote-password` are mandatory for remote copy operation.
> - Remote host IP credentials should be valid and reachable via SSH from all NetWitness hosts.
> - Remote host location (`--remote-location`) should have sufficient space to contain backups.
> - Mongo service is running on the NetWitness host.
> - Broker service is running on the NetWitness host.
> - `--host-all and --host-key` with multiple values are not supported for include Mongo operation.

```
nw-recovery-wrapper export --dump-dir <dir> --include-broker-index --
include-mongo ---include-file <custom files>/--include-dir <custom folders>
--host-key <Host 1 IP/ID/Name> --remote-ip <IP ADDRESS of remote host> --
remote-password <ssh-password> --remote-location <remote-location-where-
backups-should-be-copied-to>
```

Restore (import) options supported in NRT Wrapper

> **Caution:** Use import commands carefully as it performs system level changes.

1. Restore (import) single host at a time (using IP address, Host name, or Host ID).
   ```
   nw-recovery-wrapper import --dump-dir <dir> --host-key <Host IP/ID/Name>
   ```
2. Restore custom files or folders (if any).

   > **Note:** Make sure the custom files or directories are available on NetWitness Hosts, if not, the files or directories will be ignored.

   ```
   nw-recovery-wrapper import --dump-dir <dir> --include-file <custom files>/-
   -include-dir --host-key <Host IP/ID/Name>
   ```
3. Restore from a remote location.

   > **Note:** Make sure that:
   > - `--remote-location` contains remote host location in which data is backedup.
   > - Remote Host IP is valid and reachable via SSH from all NetWitness Hosts.
   > - Remote Host location (`--remote-location`) has adequate space to take backup.

   ```
   nw-recovery-wrapper import --remote-ip <IP address of remote host> --
   remote-password <SSH password of remote host> --remote-location <location-
   of-backup-on-remote-host> --dump-dir <dir> --host-key <Host IP/ID/Name>
   ```
   Optional argument: `--remote-user` defaults to root if argument is not specified.
   Example, for adminserver, the backup folder name should be adminserver-backup-2021-09-08-12:48:13
   ```
   nw-recovery-wrapper import --dump-directory <dir> --host-key <host-1> --
   remote-ip <remote-ip> --remote-password <password> --remote-location
   /home/adminserver-backup-2021-09-08-12:48:13
   ```

4. Restore data from remote location including custom files or folders.

   Note: Make sure that:
   - The custom files or directories are available on NetWitness Hosts, if not, the files or directories will be ignored.
   - `--remote-location` contains remote host location in which data is backedup.
   - Remote Host IP is valid and reachable via SSH from all NetWitness Hosts.
   - Remote Host location (`--remote-location`) has adequate space to take backup.

   ```
   nw-recovery-wrapper import --dump-dir <dir> --include <custom files/folder>
   --host-key <host1> --remote-ip <IP ADDRESS of remote host> --remote-
   password <ssh-password> --remote-location <remote-location-where-backups-
   should-be-copied-to>
   ```

   Optional argument: `--remote-user` defaults to root if argument is not specified.

   Example, for Admin Server, the backup folder name will be adminserver-backup-2021-09-08-12:48:13

5. (For version 11.7.1 and Later) (Optional) Restore Mongo service.

   Note: Make sure that:
   - Mongo service is running on the NetWitness host.
   - `--host-all and --host-key` with multiple values are not supported for include Mongo operation.

   ```
   nw-recovery-wrapper import --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
   --include-mongo
   ```

6. (For version 11.7.1 and Later) (Optional) Restore Broker index.

   Note: Make sure that:
   - Broker service is running on the NetWitness host.
   - `--host-all option is not support for include broker index operation.`

   ```
   nw-recovery-wrapper import --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
   --include-broker-index
   ```

7. (For version 11.7.1 and Later) (Optional) Restore Mongo and Broker index.

   Note: Make sure that:
   - Mongo service is running on the NetWitness host.
   - Broker service is running on the NetWitness host.
   - `--host-all and --host-key` with multiple values are not supported for include Mongo operation.

   ```
   nw-recovery-wrapper import --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
   --include-mongo --include-broker-index
   ```

8. (For version 11.7.1 and Later) (Optional) Restore custom files or folders, copying to remote location, Broker index, and Mongo.

Note: Make sure that:
- Custom files or directories are present on NetWitness hosts to be backedup, if it is not present the files or directory is skipped for backup.
- Fields such as `--remote-ip`, `--remote-location`, `--remote-password` are mandatory for remote copy operation.
- Remote host IP credentials should be valid and reachable via SSH from all NetWitness hosts.
- Remote host location (`--remote-location`) should have sufficient space to contain backups.
- Mongo service is running on the NetWitness host.
- Broker service is running on the NetWitness host.
- `--host-all and --host-key` with multiple values are not supported for include Mongo operation.

```
nw-recovery-wrapper import --dump-dir <dir> --include-file <custom files>/-
-include-dir <custom folders> --include-mongo --include-broker-index --
host-key <host1> --remote-ip <IP ADDRESS of remote host> --remote-password
<ssh-password> --remote-location <remote-location-where-backups-should-be-
copied-to>
```

Status Check

You can check the Backup or Restore status using the below command.

`/var/log/netwitness/recovery-tool/recovery.log`

Troubleshooting

Error Message	NRT Wrapper fails during backup or restore.
Solution	Do any one of the following: • Log in to host where backup is failing and check `/var/log/netwitness/recovery-tool/recovery.log`. • Run in debug mode (`nw-recovery-wrapper -l debug`) on Node 0 to get recovery logs of each host.

Error Message	NRT Wrapper fails due to incorrect password for remote copy operation (`--remote-password`).
Cause	NRWT

	fails if you enter wrong password multiple times during remote copy. Since SFTP uses SSH, it locks the system SSH for a while.
Solution	You must retry after sometime.

Error Message	NRT Wrapper fails after running for long hours for a particular host but the backup is still in progress. For example, Endpoint or ESA node.
Cause	NRT architecture is designed to take a backup of configuration and not user data. It uses salt to communicate between admin server(SA) and nodex. Due to large volume of data in the particular host, this issue is caused when salt communication times out.
Solution	SSH to the particular host and check the backup status at `/var/log/netwitness/recovery-tool/recovery.log`. If the data to be backed up is huge, recommend using "nw-recovery-tool" by logging into particular host.

NetWitness Recovery Tool (NRT)

You can use the NetWitness Recovery Tool (NRT) to back up and restore data from the NetWitness Server and component host systems. The NRT is a script that you run from the command line to back up and restore data on hosts for RMAs, hardware refreshes, and general backup and restore requirements. Refer to Disaster Recovery in Azure Deployment for specific steps on how to perform disaster recovery for hosts deployed in Azure VMs.

Note: You must run the NRT on each host system locally. You cannot run it from remote hosts or an external host.

The following types of hosts can be backed up and restored.

Note: In the NRT script, the following terms in bold are referred to as categories.

- **NetWitness Admin Server** (may include Broker, Investigate, Respond, Health and Wellness, and Reporting Engine)
- **AnalystUI** (may include Broker, Investigate, Respond, Reporting Engine)
- **Archiver** Log Archiver (Workbench and Archiver)
- **Broker** Stand-alone Broker
- **Concentrator** Network or Log Concentrator
- **Decoder** Network Decoder (Packets)
- **Endpoint** Endpoint Agents
- **Endpoint Broker** Endpoint Broker
- **Endpoint Log Hybrid** Log Collector, Log Decoder, Endpoint Server, and Concentrator
- **Event Stream Analysis (ESA) Primary** Contexthub, ESA Correlation, and Incident Management database
- **ESA Secondary** ESA Correlation
- **Gateway** Cloud Gateway
- **Log Hybrid Retention** Log Hybrid-Retention Optimized (for RSA Series 6 Hybrid hardware with Log Hybrid-Retention Optimization)
- **Log Collector** Log Collector including Virtual Log Collector if installed
- **Log Decoder** Log Decoder including Local Log Collector and Warehouse Connector, if installed
- **Log Hybrid** Log Collector, Log Decoder, and Concentrator
- **Malware** Malware Analysis and Broker
- **Network Hybrid** Concentrator and Decoder
- **Search** (for Health & Wellness Beta Host)
- **UEBA** User Entity and Behavior Analytics
- **Warehouse** Warehouse Connector

Basic Usage of the NetWitness Recovery Tool

You can use the NRT to back up data by using the `export` option. To restore data, use the `import` option. The basic usage of the tool is to run the following command from the root directory level:

```
nw-recovery-tool [command] [option]
```

The commands and options that you can use with this tool are described in the following tables.

Commands and Options	Description
`-h, --help`	Display help on commands and option. For example, specify: `nw-recovery-tool --help-categories` to get a list of all the valid category names.
`-e, --export`	Export data or configuration.
`-i, --import`	Import data or configuration.
`-d, --dump-dir <path>`	Path for the where data will be exported or imported from (for example, `/var/netwitness/backup`).
`-C, --category <name>`	Select components by category. Valid category names are `AdminServer`, `AnalystUI`, `Archiver`, `Broker`, `Concentrator`, `Decoder`, `Endpoint`, `EndPointBroker`, `EndpointLogHybrid`, `ESAPrimary`, `ESASecondary`, `Gateway`, `LogHybridRetention`, `LogCollector`, `LogDecoder`, `LogHybrid`, `Malware`, `NetworkHybrid`, `Search`, `UEBA`, and `Warehouse`. You can specify a single category or multiple categories if multiple categories are co-located on the same host. For example: • `--category AdminServer` for the Admin Server exclusively. `--category AdminServer --category Gateway` for the Admin Server and the Cloud Gateway. • `--category ESAPrimary` for the ESA Primary exclusively. • `--category Broker` for the Broker exclusively. `--category Broker --category EndpointBroker` for the Broker and the Endpoint Broker.

Required Conditions

Make sure that the following conditions are met:

- Read the entire document before backing up any data. The document covers all deployment scenarios, so you want to make sure you have all the information required to back up and restore your implementation of NetWitness Platform before going through this process.
- Run the NRT for both backup and recovery locally, on each system being backed up or restored. You cannot run the NRT on an external host, or back up or restore several hosts simultaneously. However, you can back up several components on the same host system simultaneously.
- Export and import data on the same host. If a host fails and you need to build a new system, the new system must have the same identity parameters (i.e., the same IP address), and must be on the same version of NetWitness Suite
- Make sure that there is adequate disk space in the backup location (`/var/netwitness/backup` is the recommended directory) before the export command in the nw-recovery tool is executed. Do not use a `tmp` directory because it fills up quickly and may cause the system to crash.
- Check the sizing of the Malware disks and adjust them before you back them up. The following table shows you the maximum size of Malware databases that you can back up by hardware type with the actions you can take to reduce them to the maximum size.

Host	Source Hardware	Target Hardware	Database	Maximum Size for Backup	Actions to Reduce Size to Backup Maximum
Malware	Series 4S Hybrid	Series 6 Core	`/var/netwitness`	2.5TB	Configure a rollover. Purge data that you do not need from the database.

- Restore to the exact ISO Image that each host had at the time of backup.
- If you have multiple services co-located on a single host, include all the services in a single command string for the `import` and `export` commands in the nw-recovery tool.

Note: 1.) When you run the NRT, the Malware , Reporting Engine, and Postgresql services are stopped and restarted during both the backup (export) and restore (import) processes.

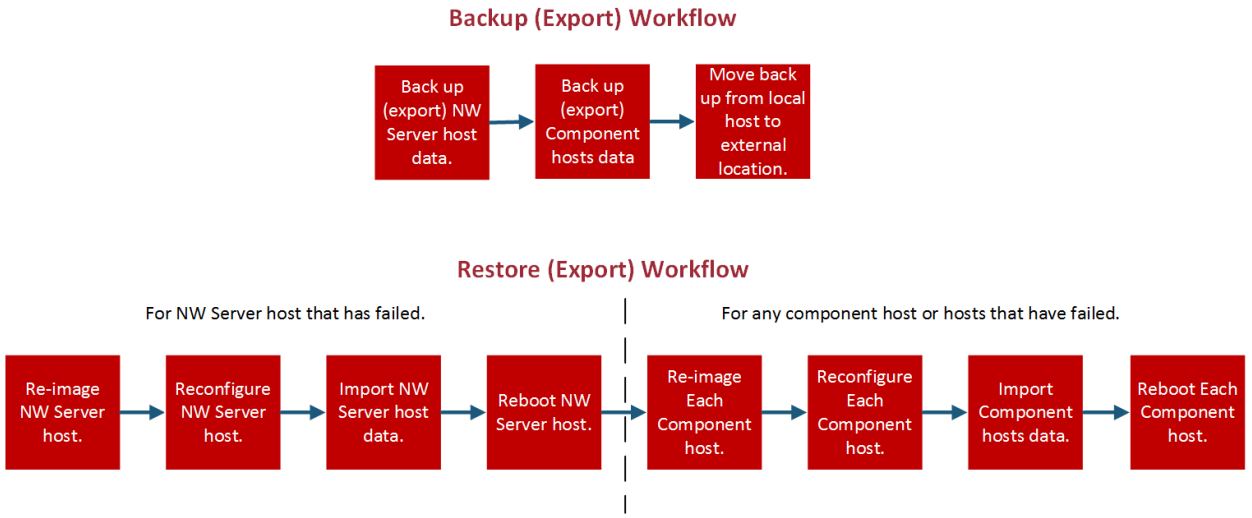
Disaster Recovery Workflow

The following diagram shows the high-level Disaster Recovery tasks.

Note: You only need to recover a host if it failed. This means that you can recover a single host, or any combination of hosts depending on which host or hosts failed.

The following diagram shows the tasks for:

- Backup (perform as soon as possible and as frequently as possible).
- Restore (only required if you need to restore your data).



Back Up and Restore Data for Hosts

The procedures for backing up and restoring data are different for NetWitness Server host systems and for component systems.

Caution: 1.) Do not remove component hosts (that is any host other than the NW Server host) from the Hosts View (**Admin** > **Hosts**) from the user interface when you are performing the following disaster recovery procedure. 2.) You must retain (restore) the 'Host name' that existed prior to performing the disaster recovery procedure.

Back Up and Restore Data on the NetWitness Server

Note: If you are using shared storage to export data from multiple hosts (for example, a shared mount or drive), use host-specific subfolders for the path to the location of the exported files for each host, to avoid overwriting one host's exported data with another. For example, you could use a path similar to `--dump-dir /mnt/storage/<host-specific-name>` for the path to the location of the exported files.

Back Up Data on a NetWitness Server Host

Perform this procedure on an existing, functional NetWitness Server host system.

1. At the root level, type the following command:

   ```
   nw-recovery-tool --export --dump-dir /var/netwitness/backup --category
   AdminServer
   ```

   Note: If a service is co-located with another category on the same host rather than on its own, dedicated host, you must include it in the command string. The `Gateway` and `EndpointBroker` can be co-located as show in the following examples:

   ```
   nw-recovery-tool--export --dump-dir /var/netwitness/backup --category
   AdminServer --category Gateway
   nw-recovery-tool--export --dump-dir /var/netwitness/backup --category
   Broker --category EndpointBroker
   ```

2. Replace `/var/netwitness/backup` with the path to the location to which the data should be exported.

   a. Ensure that this location has sufficient space to store the backup data.

   b. The backup directory path should be located on the local host. However, the backup files could be located on a network mount or an external device.

The data is backed up on the NetWitness Server host in the location you set up in step 2.

3. Move the backed up data from the local host to an external server or a USB stick.

Restore Data on a NetWitness Server Host

1. Re-image the NetWitness Server host using the same network configuration settings of the original host. For information about re-imaging the NetWitness Server host, see "Task 1 - Install 12.0 on the NetWitness Server Host" in the *Physical Host Installation Guide for Version 12.0 Guide*

   a. **Optional** If you need to establish network connectivity before you can fetch backup data, for example, if it is on a remote host, run the following script using the same IP address, subnet, gateway, DNS and domain information as the original host:

   ```
   netconfig --static --interface <name> --ip <address> --netmask <netmask>
   --gateway <gateway>
   ```

   For example:

   ```
   netconfig --static --interface eth0 --ip 192.168.1.100 --netmask
   255.255.255.0 --gateway 192.168.1.1
   ```

   Optional: To specify DNS server(s), include the following additional parameter:

   ```
   --dns <address>
   ```

   Optional: To set the local domain name, include the following additional parameter:

   ```
   --domain <name>
   ```

   b. (**Optional**) If you are using DHCP, run the following script:

   ```
   netconfig --dhcp --interface <name>
   ```

   For example:

   ```
   netconfig --dhcp --interface eth0
   ```

   c. Add the backup data to the backup directory path on the local host, for example:

   ```
   /var/netwitness/backup
   ```

2. Run the `nwsetup-tui` command. This initiates the Setup program.

   Note: During the Setup program, when you are prompted for the network configuration of the host, be sure to specify the same identical network configuration that was used for the original installation of the host.

3. When you are prompted, select install type option **2: Recover (Reinstall)**, click **OK**, and then enter the path to the backup directory containing the backup data.
4. After the installation completes successfully, ensure that the host is running the exact same release and patch version of the data that was backed up:

   - If the data was on an system that was updated to a later patch release, update the host by following the instructions for updating systems offline in the update guide for the same patch version as what was previously running on the host (the exact release or patch version for which data was backed up).
   - If the data was on a major release version (for example, 12.0) that had not been updated to a later patch version, you do not need to update the host system.

5. When the host is running at the correct version, run the following command on the NetWitness Server to restore data:

```
nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
AdminServer
```

Note: If a service is co-located with another category on the same host rather than on its own, dedicated host, you must include it in the command string. The `Gateway` and `EndpointBroker` can be co-located as show in the following examples:

```
nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
AdminServer --category Gateway
nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
Broker --category EndpointBroker
```

6. (Conditional) If you use custom firewall rules or custom entries in `/etc/hosts`:
   a. (Conditional) If you use custom firewall rules (that is, replied "Yes" to the "Disable Firewall" nwsetup-tui prompt during installation), restore the `/etc/sysconfig/iptables` file from the backup copy located in the `<dump-dir>/unmanaged/etc/sysconfig/iptables` file.
   b. (Conditional) If you use custom entries in `/etc/hosts`, restore the `/etc/hosts.users` file from the backup copy located at `<dump-dir>/unmanaged/etc/hosts.user` to `/etc` on the host.
   c. If you performed step 6a or 6b, refresh the host by running the following command:
   `nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>`
7. Reboot the NetWitness Server host.

Note: If you want to add any more custom entries to `/etc/host`, you must add them to the `/etc/hosts.users` file and then refresh the host as described in step 6c.

Back Up and Restore Data on Other Component Hosts

Perform these procedures on each existing, functional component host system.

Back Up Data on a Component Host

1. At the root level, type the following command:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category <category name>`
   where the category name is one of the following:
   `AdminServer`, `AnalystUI`, `Archiver`, `Broker`, `Concentrator`, `Decoder`, `Endpoint`, `EndPointBroker`, `EndpointLogHybrid`, `ESAPrimary`, `ESASecondary`, `Gateway`, `LogHybridRetention`, `LogCollector`, `LogDecoder`, `LogHybrid`, `Malware`, `NetworkHybrid`, `Search`, `UEBA`,or `Warehouse`

   Note: 1.) Use the category that matches the host type. 2.) If services are co-located on a Component Host rather than on its own dedicated host, you must include it in the command string. For example, a Warehouse Connector resides on a Log Decoder host. The following is an example of this command string.
   `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category LogDecoder --category Warehouse`

2. **(Optional)** Replace `/var/netwitness/backup` with the path to the location to which the data should be exported
   a. Ensure that this location has sufficient space to store the backup data.
   b. The backup directory path should be located on the local host. However, the backup files could be located on a network mount or an external device.

3. For **Endpoint Log Hybrid** and **ESA Primary** hosts, you can export application data that is stored in the database by running the following command:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component mongo`
   You can replace `/var/netwitness/backup` with the path to the location to which the data should be exported.

   Note: 1.) Make sure that there is enough space in the export location for the files from the Mongo database. 2.) You can back up the **Endpoint Log Hybrid** or **ESA Primary** host data and Mongo database in a single command string. For example, `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category EndpointLogHybrid --component mongo`

4. For **Malware**, you can export application data from the Malware application database by running the following command:
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component postgresql`
   You can replace `/var/netwitness/backup` with the path to the location to which the data should be exported.

Note: Ensure that there is enough space in the export location for the files from the Malware database.

5. Move the backed up data from the local host to an external server or a USB stick.

Restore Data on a Component Host

1. Re-image the component host using the same network configuration settings of the original host. For information about re-imaging a component host, see "Task 2 - Install 12.0 on Other Component Hosts" in the *Physical Host Installation Guide for Version 12.0 Guide*
2. **Optional** If you need to establish network connectivity before you can fetch backup data, for example, if it is on a remote host, run the following script using the same IP address, subnet, gateway, DNS and domain information as the original host:
   `netconfig --static --interface <name> --ip <address> --netmask <netmask> --gateway <gateway>`
   For example:
   `netconfig --static --interface eth0 --ip 192.168.1.100 --netmask 255.255.255.0 --gateway 192.168.1.1`
   Optional: To specify DNS server(s), include the following additional parameter:
   `--dns <address>`
   Optional: To set the local domain name, include the following additional parameter:
   `--domain <name>`
   a. (**Optional**) If you are using DHCP, run the following script:
      `netconfig --dhcp --interface <name>`
      For example:
      `netconfig --dhcp --interface eth0`
   b. Add the backup data to the backup directory path on the local host, for example, `/var/netwitness/backup`.
3. Run the `nwsetup-tui` command. This initiates the Setup program.

   Note: During the Setup program, when you are prompted for the network configuration of the host, be sure to specify the same identical network configuration that was used for the original installation of the host.
4. When you are prompted, select install type option **2: Recover (Reinstall)**, click **OK**, and then enter the path to the directory containing the backup data.

5. After you complete the `nwsetup-tui` command setup, you must re-install the appropriate services on the host using the **Install** command from the Hosts View in the NetWitness Platform User Interface.
6. After the service installation completes, ensure that the host is running the exact same release and patch version of the data that was backed up:
   - If the data was on system that was updated to a later patch release, update the host by following the instructions for updating systems offline for the same patch version as what was previously running on the host (the exact release or patch version for which data was backed up).
   - If the data was on a major release version (for example, 12.0) that had not been updated to a later patch version, you do not need to update the host system.
7. When the host is running at the correct version, return to the root level of the component host and run the following command to restore data:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   <category name>
   ```

   Note: If services are co-located on a Component Host rather than on its own dedicated host, you must include it in the command string. For example, a Warehouse Connector resides on a Log Decoder host. The following is an example of this command string.
   ```
   nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
   LogDecoder --category Warehouse
   ```
8. For **EnpointLogHybrid** and **ESAPrimary** systems, you can import application data to be restored by running the following command:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   mongo
   ```
9. For **Malware**, you can import application data from the Malware application database to be restored by running the following command:
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   postgresql
   ```

10. For a Decoder, Log Decoder , Concentrator, Archiver, Network Hybrid, or Log Hybrid configured with external storage (that is, DAC, SAN, Unity or Powervault):

    a. Scan the `<dump-dir>/unmanaged/etc/fstab` file for devices with mount points that do not exist in the system `/etc/fstab` file.

    IMPORTANT: If you are migrating to new host hardware (that is a new Decoder, Log Decoder, Concentrator, Archiver, Network Hybrid, or Log Hybrid host), before you proceed to the next step you must:
    1. Power off the old hardware host and the external storage device attached to it.
    2. Attach the external storage device to the new host hardware.
    3. Power on both the new host hardware and the external storage device attached to it.

    a. Complete the following steps for each device in the backup copy of `<dump-dir>/unmanaged/etc/fstab`.

        i. Verify that the corresponding device is present and attached. If it not attached, attach it. If the device is no longer applicable, skip it and go to the next device.

        ii. Verify that the mount point directory exists on the file system. If it does not exist, create the directory with the `mkdir <path>` command.

        iii. Add the `fstab` entry from the backup copy to the system `/etc/fstab` file.

        Caution: For a Series 5 or 6 Hybrid, you must restore backed up data to the `/etc/fstab` directory according to the instructions in Appendix A. Modify fstab for Series 5 and 6 Hybrid Storage After Recovery.

    b. Run the following command on each host.

    ```
    mount -a
    ```

11. (Conditional) If you use custom firewall rules or custom entries in `/etc/hosts`:

    a. (Conditional) If you use custom firewall rules (that is, replied "Yes" to the "Disable Firewall" nwsetup-tui prompt during installation), restore the `/etc/sysconfig/iptables` file from the backup copy located in the `<dump-dir>/unmanaged/etc/sysconfig/iptables` file.

    b. (Conditional) If you use custom entries in `/etc/hosts`, restore the `/etc/hosts.users` file from the backup copy located at `<dump-dir>/unmanaged/etc/hosts.user` to `/etc` on the host.

    c. If you performed step 11a or 11b, refresh the host by running the following command:

    ```
    nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
    ```

12. Reboot the component host.

Hardware Refresh Only - Use Additional Space in New Hardware Hosts

Refer to the *Core Database Tuning Guide for NetWitness Platform* for instructions on how to use all the space you have available on your new hardware. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Disaster Recovery in Azure Deployment

This section tells you how to back up and restore NetWitness Platform deployed on Azure virtual hosts (also referred to as VMs in this section). The two major tasks to back up and restore data in an Azure deployment are:

- Task 1 - Backup and Export Data
- Task 2 - Restore and Import Data

Task 1 - Backup and Export Data

1. Export the data by running the `nw-recovery-tool --export` commands as described in the Disaster Recovery (Backup and Restore Instructions) section of this document.

Task 2 - Restore and Import Data

You need to refer to the *10.6.6.x to 11.3 Azure Upgrade Guide* to complete this task. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

1. Delete the VM.

   Caution: Do not delete the resources (for example, do not delete Disks, Network Interface, and so on).

2. Complete the following steps for the NW Server host, Broker host, ESA host, Endpoint Log Hybrid host, and Log Collector host (where host = `--category`).

   a. Delete all the resources except the network interface card of the older 12.0 VM.

   b. Deploy the fresh 12.0 VM with the same disk and resources and power it off.
   For detailed instructions on how to deploy a virtual host in Azure, see the *Azure Installation Guide*.

   c. Run the `azure-mac-retention.ps1` from the local machine.
   See the *10.6.6 to 11.3 Azure Upgrade Guide* for instructions on how to run this script.

   d. Follow the procedure for the NRT restoration for the respective host as described in Disaster Recovery (Backup and Restore Instructions).

   e. After you restore NRT the component host, restore the following files.

   - `/etc/fstab`
   - `/etc/hosts` (if hostname is not changed)
   - `/etc/waagent.conf`
   - `/etc/logrotate.d/waagent.logrotate`
   - `/etc/krb5.conf` from the `<dump-dir>/unmanaged` folder

3. Complete the following steps for the Log Decoder host, Concentrator host, and Archiver host (where host = `--category`.

   a. Delete all the resources except the disks that are named **external** and the network interface card of the older 12.0 VM.

   b. Deploy the fresh 12.0 VM with the same disk and resources listed in the *Azure Installation Guide* and power it off.

   > **Note:** Do not create the **external** disk. Only create the **nwhome** disks.

   c. Run the `azure-mac-retention.ps1` from the local machine.
   See the *10.6.6 to 11.3 Azure Upgrade Guide* for instructions on how to run this script.

   d. Follow the procedure for the NRT restoration for the respective hosts as described in Restore Data on a Component Host.

   e. After you restore NRT the component host, restore the following files.

   - `etc/fstab`
   - `/etc/hosts` (if hostname is not changed)
   - `/etc/waagent.conf`
   - `etc/logrotate.d/waagent.logrotate`
   - `/etc/krb5.conf`

Disaster Recovery in AWS Deployment

This section tells you how to back up and restore NetWitness Platform deployed on AWS virtual hosts (also referred to as VMs in this section). The two major tasks to back up and restore data in an AWS deployment are:

- Task 1 - Backup and Export Data
- Task 2 - Restore and Import Data

Task 1 - Backup and Export Data

1. Export the data by running the `nw-recovery-tool --export` commands as described in the Disaster Recovery (Backup and Restore Instructions) section of this document.
2. Record the IP addresses. You need to refer to them later in the Disaster Recovery process. Refer to the *10.6.6 to 11.3 AWS Upgrade Guide* for instructions on how retain the IP addresses. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Task 2 - Restore and Import Data

You need to refer to the *10.6.6 to 11.3 AWS Upgrade Guide* to complete this task.

1. Delete the VM.

   Caution: Do not delete the resources (for example, do not delete Disks).

2. Complete the following steps for the NW Server host, Broker host, ESA (Primary/Seconday) host, Endpoint Log Hybrid host, and Log Collector host (where host = `--category`).
   a. Delete all the resources of the older 12.0 VM.
   b. Deploy the fresh 12.0 VM with the same IP address, disk and resources and power it off. For detailed instructions on how to deploy a virtual host in AWS, see the *AWS Installation Guide*.
   c. Follow the procedure for the NRT restoration for the respective host as described in Restore Data on a Component Host.
   d. After you restore NRT the component host, restore the following files.
      - `/etc/fstab`
      - `/etc/hosts` (if hostname is not changed)
3. Complete the following steps for the Log Decoder host, Decoder (Network Decoder) host, Concentrator host, and Archiver host (where host = `--category`.
   a. Delete all the resources except the **external disks** of the older 12.0 VM.
   b. Deploy the fresh 12.0 VM with the same IP address, disk, and resources listed in the *AWS Installation Guide* and power it off.

Note: Do not create the **external** disk. Only create the **nwhome** disks.

c. Follow the procedure for the NRT restoration for the respective hosts as described in Restore Data on a Component Host.

d. After you restore NRT the component host, restore the following files.

- `etc/fstab`
- `/etc/hosts` (if hostname is not changed)
- `/etc/krb5.conf`

Appendix A. Modify fstab for Series 5 and 6 Hybrid Storage After Recovery

Note: The procedures in this Appendix do not apply if the hybrid was an 11.4 fresh installation and you had a disaster.

You must modify the `/etc/fstab` file for a Series5 or Series 6 Hybrid if a Series 5 or Series 6 Network Hybrid was upgraded from 11.2.x.x or 11.3.x.x to 11.4 and a disaster occurred.

These are the tasks to recovery from this disaster scenario.

1. Image a new Series 5 or Series 6 Hybrid as Network Hybrid using an 11.4 ISO.
2. Import the backed up data or configuration (`nw-recovery-tool --import`).
3. Modify the recovered `/etc/fstab` file.

Sample etc/fstab File Before Disaster

The following data is an example of the external storage configuration backup for a Series 5 or 6 Hybrid that was upgraded to 11.4.

The data highlighted in yellow corresponds to internal storage on an upgraded system. This configuration is carried over from prior releases during upgrade process. This lay out changed in 11.4 (Fresh Install). You must only copy the entries corresponding to external storage (highlighted in green) to the new `etc/fstab` file as part of a disaster recovery.

When you export data or configuration using the `nw-recovery-tool --export` command, the storage configuration details are saved to `<back-location>/unmanaged/etc/fstab`. The `fstab` file contains both internal storage (highlighted in yellow) and external storage configuration (highlighted in green). The contents on a upgraded (10.6 or 11.x -> 11.4) Series 5 or Series 6 Network Hybrid look similar to the following storage configuration.

```
/dev/mapper/netwitness_vg00-root / xfs defaults 0 0 UUID=906e2a3d-3b59-46d1-
975d-fa2b8467d009
/boot xfs defaults 0 0 /dev/mapper/netwitness_vg00-usrhome
/home xfs nosuid 0 0
/dev/mapper/netwitness_vg00-varlog /var/log xfs defaults 0 0
/dev/mapper/netwitness_vg00-nwhome /var/netwitness xfs nosuid,noatime 0 0
/dev/mapper/concentrator-vlnwc /var/netwitness/concentrator xfs noatime,nosuid
0 0
/dev/mapper/index-vlnwci /var/netwitness/concentrator/index xfs noatime,nosuid
0 0
/dev/mapper/concentrator-vlnwcm /var/netwitness/concentrator/metadb xfs
noatime,nosuid 0 0
/dev/mapper/concentrator-vlnwcs /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwd /var/netwitness/decoder xfs noatime,nosuid 0 0
```

```
/dev/mapper/decoderpacket-vlnwdi /var/netwitness/decoder/index xfs
noatime,nosuid 0 0
/dev/mapper/decodermeta-vlnwdm /var/netwitness/decoder/metadb xfs
noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwdp /var/netwitness/decoder/packetdb xfs
noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwds /var/netwitness/decoder/sessiondb xfs
noatime,nosuid 0 0
/dev/mapper/netwitness_vg00-swap swap swap defaults 0 0
/var/netwitness/decoder /var/netwitness/logdecoder none defaults,rbind 0 0
/dev/concentrator0/sessiondb /var/netwitness/concentrator/sessiondb0 xfs
noatime,nosuid 1 2
/dev/concentrator0/metadb /var/netwitness/concentrator/metadb0 xfs
noatime,nosuid 1 2
/dev/decoder0/packetdb /var/netwitness/decoder/packetdb0 xfs noatime,nosuid 1
```

Sample etc/fstab File After Recovery - Before Modification

After you install 11.4 with the 11.4 ISO and execute the recovery tool execution to restore all previous configurations, the `/etc/fstab` file appears looks like the following example.

```
#
# /etc/fstab
# Created by anaconda on Thu Dec 5 17:31:26 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/netwitness_vg00-root / xfs defaults 0 0
UUID=d84db66c-fce6-4fec-9f84-b3449861f664 /boot xfs defaults 0 0
/dev/mapper/netwitness_vg00-usrhome /home xfs nosuid 0 0
/dev/mapper/netwitness_vg00-varlog /var/log xfs defaults 0 0
/dev/mapper/netwitness_vg00-nwhome /var/netwitness xfs nosuid,noatime 0 0
/dev/mapper/netwitness_vg00-swap swap swap defaults 0 0
/dev/hybrid-decoder-meta/decoroot /var/netwitness/decoder xfs noatime,nosuid 1
2
/dev/packet/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
/dev/hybrid-concentrator/root /var/netwitness/concentrator xfs noatime,nosuid
1 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
```

Note: You can see that it is missing the external storage configurations. You must add the external storage configurations highlighted in green above) to the `/etc/fstab` file on the newly built Hybrid.

Sample etc/fstab File After Recovery - After Modification

After you make this updater, the `/etc/fstab` looks like the following example.

```
#
# /etc/fstab
# Created by anaconda on Thu Dec 5 17:31:26 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/netwitness_vg00-root / xfs defaults 0 0
UUID=d84db66c-fce6-4fec-9f84-b3449861f664 /boot xfs defaults 0 0
/dev/mapper/netwitness_vg00-usrhome /home xfs nosuid 0 0
/dev/mapper/netwitness_vg00-varlog /var/log xfs defaults 0 0
/dev/mapper/netwitness_vg00-nwhome /var/netwitness xfs nosuid,noatime 0 0
/dev/mapper/netwitness_vg00-swap swap swap defaults 0 0
/dev/hybrid-decoder-meta/decoroot /var/netwitness/decoder xfs noatime,nosuid 1
2
/dev/packet/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
/dev/hybrid-concentrator/root /var/netwitness/concentrator xfs noatime,nosuid
1 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
/dev/concentrator0/sessiondb /var/netwitness/concentrator/sessiondb0 xfs
noatime,nosuid 1 2
/dev/concentrator0/metadb /var/netwitness/concentrator/metadb0 xfs
noatime,nosuid 1 2
/dev/decoder0/packetdb /var/netwitness/decoder/packetdb0 xfs noatime,nosuid 1
```