RSA NETWITNESS® PLATFORM

Recovery Tool User Guide

for Version 11.2

Contents

Disaster Recovery (Backup and Restore Instructions)

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 Respond, Health and Wellness, and Reporting Engine)

- **Malware** Malware Analysis (stand-alone)

- **Archiver** Log Archiver

- **Broker** Stand-alone Broker

- **Concentrator** Network or Log

- **Decoder** Network Decoder

- **Endpoint Hybrid**

- **Endpoint Log Hybrid**

- **Event Stream Analysis (ESA) Primary** Including Context Hub and Incident Management database

- **ESA Secondary**

- **Gateway** Cloud Gateway

- **Log Collector** Including Virtual Log Collector if installed

- **Log Decoder** Including Local Log Collector and Warehouse Connector, if installed.

- **Log Hybrid**

- **Network Hybrid**

- **UEBA** User Entity and Behavior Analytics

- **Warehouse**

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`, `Archiver`, `Broker`, `Concentrator`, `Decoder`, `EndpointHybrid`, `EndpointLogHybrid`, `ESAPrimary`, `ESASecondary`, `Gateway`, `LogCollector`, `LogDecoder`, `LogHybrid`, `Malware`, `NetworkHybrid`, `UEBA`, and `Warehouse`. You can specify a single category or multiple categories. For example: `--category AdminServer` for the Admin Server exclusively. `--category AdminServer --category Gateway` for the Admin Server and the Cloud Gateway.
`-p, --deploy-password <pwd>`	Specify deployment password. This is only needed if the selected category or component includes Mongo (for hosts such as AdminServer, Endpoint, or ESA Primary).

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. Log and packet collection is not stopped.

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).

Backup (Export) Workflow

Back up (export) NW Server host data. → Back up (export) Component hosts data → Move back up from local host to external location.
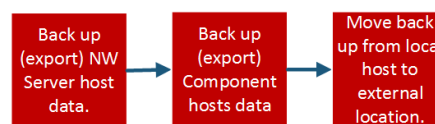
Restore (Export) Workflow

For NW Server host that has failed.

Re-image NW Server host. → Reconfigure NW Server host. → Import NW Server host data. → Reboot NW Server host.

For any component host or hosts that have failed.

Re-image Each Component host. → Reconfigure Each Component host. → Import Component hosts data. → Reboot Each Component host.
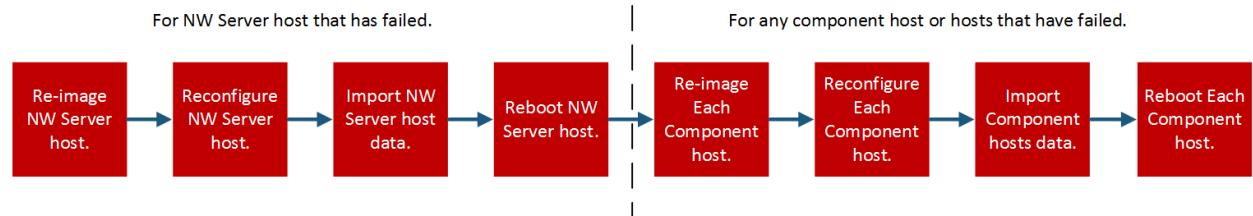
Back Up and Restore Data for 11.x Hosts

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. 3.) Make sure that you record your master password and store it in a safe location so you can access the system in the case of Disaster Recovery.

Back Up and Restore Data on the 11.x 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 11.x 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 (for example Cloud Gateway) is co-located on the NW Server with the Admin Server rather than on its own, dedicated host, you must include it in the command string. For example.
   > ```
   > nw-recovery-tool--export --dump-dir /var/netwitness/backup --category
   > AdminServer --category Gateway
   > ```

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.

3. When you are prompted for the deployment administration password, enter the password, or include the following additional argument for the `nw-recovery-tool` command:

   ```
   --deploy-password <password>
   ```

   > **Note:** Use the existing `deploy_admin` password that was used when you first installed the host.

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

4. 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 11.2 on the NetWitness Server Host" in the *Physical Host Installation Guide for Version 11.2 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 11.x on this host.

3. When you are prompted, select install type option **3: 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 11.x 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/patch version for which data was backed up).

   - If the data was on a major release version (for example, 11.x) 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 on the NW Server with the Admin Server rather than on its own, dedicated host, you must include it in the command string. For example.
> ```
> nw-recovery-tool--import--dump-dir /var/netwitness/backup --category
> AdminServer --category Gateway
> ```

6. (Conditional) For customers using 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.

7. Reboot the NetWitness Server host.

Back Up and Restore Data on Other Component Hosts

Perform these procedures on each existing, functional 11.x 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:
   ```
   Archiver, Broker, Concentrator, Decoder, EndpointHybrid, EndpointLogHybrid,
   ESAPrimary, ESASecondary, LogCollector, LogDecoder, LogHybrid, Malware,
   NetworkHybrid, UEBA
   ```

   > **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 **EndpointHybrid**, **EndpointLogHybrid**, and **ESAPrimary** systems, 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 **EndpointHybrid**, **EndpointLogHybrid**, or **ESAPrimary** host data and Mongo database in a single command string. For example, `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category EndpointHybrid --component mongo`

   When you are prompted for the deployment administration password, enter the password, or include the following additional argument for the `nw-recovery-tool` command:
   ```
   --deploy-password <password>
   ```

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 11.x on Other Component Hosts" in the *Physical Host Installation Guide for Version 11.x 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 11.x on this host.

4. When you are prompted, select install type option **3: Recover (Reinstall)**, click **OK**, and then enter the path to the directory containing the backup data.

5. After completing the `nwsetup-tui` command setup, you must re-install the appropriate services (except EndpointHybrid and EndpointLogHybrid) on the host using the Install command from the Hosts View in the NetWitness Platform User Interface.
For EndpointHybrid and EndpointLogHybrid, you must use the orchestration-cli-client on the Admin Server to install the Endpoint services. Run the following command:

```
orchestration-cli-client --hostaddr-as-id -i -o <host IP Address> --
category <EndpointHybrid or EndpointLogHybrid> --version <version>
```

For example:

```
 orchestration-cli-client --hostaddr-as-id -i -o 192.168.200.83 --category
EndpointLogHybrid --version 11.2.0.0
```

> **Note:** The version number must match the version of the media that was used to re-image the host.

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 an 11.x 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/patch version for which data was backed up).

   - If the data was on a major release version (for example, 11.x) 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 **EndpointHybrid**, **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
```

When you are prompted for the deployment administration password, enter the password, or include the following additional argument for the `nw-recovery-tool` command:
```
 --deploy-password <password>
```

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
```

Disaster Recovery (Backup and Restore Instructions)

10. For a Decoder, Log Decoder , Concentrator, Archiver, Network Hybrid, or Log Hybrid configured with external storage (JBOD / SAN /Unity / 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.

    b. 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.

    c. Run the following command on each host.

       `mount -a`

11. From ASOC-59466) (Conditional) For customers using 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.

12. Reboot the component host.

Hardware Refresh Only - Use Additional Space in New Hardware Hosts

Refer to the *RSA NetWitness Platform Core Tuning Guide* (https://community.rsa.com/docs/DOC-95938) for instructions on how to use all the space you have available on your new hardware.

Disaster Recovery in Azure Deployment

The section tells you how to back up and restore NetWitness Platform 11.x deployed on Azure virtual hosts (also referred to as VMs in this section). The two major tasks to back up and restore 11.x 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 Disaster Recovery (Backup and Restore Instructions).

Task 2 - · Restore and Import Data

You need to refer to the *10.6.5 to 11.2 Azure Upgrade Guide* to complete this task. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

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 AdminServer host, Broker host, ESA host, Endpoint host, and LogCollector host (where host = `--category`).

   a. Delete the all the resources except the network interface card of the older 11.2 VM.

   b. Deploy the fresh 11.2 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 *11.2 Azure Deployment Guide*.

   c. Run the `azure-mac-retention.ps1` from the local machine.
   See the *10.6.5 to 11.2Azure 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 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` from the `<dump-dir>/unmanaged` folder

3. Complete the following steps for the LogDecoder 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 11.2 VM.

b. Deploy the fresh 11.2 VM with the same disk and resources listed in the *11.2 Azure Deployment 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 *10.6.5 to 11.2Azure 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

The section tells you how to back up and restore NetWitness Platform 11.x deployed on AWS virtual hosts (also referred to as VMs in this section). The two major tasks to back up and restore 11.x 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 Disaster Recovery (Backup and Restore Instructions).

2. Record the IP addresses. You need to refer to them later in the Disaster Recovery process.
   Refer to the *10.6.5 to 11.2 AWS Upgrade Guide* for instructions on how retain the IP addresses. Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

Task 2 - · Restore and Import Data

You need to refer to the *10.6.5 to 11.2 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 AdminServer host, Broker host, ESA (Primary/Seconday) host, Endpoint Hybrid host, Endpoint Log Hybrid host, and LogCollector host (where host = `--category`).

   a. Delete the all the resources of the older 11.2 VM.

   b. Deploy the fresh 11.2 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 *11.2 AWS Deployment 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 LogDecoder 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 11.2 VM.

   b. Deploy the fresh 11.2 VM with the same IP address, disk and resources listed in the *11.2 AWS Deployment 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`