Manage Backups

This section contains the following topics:

- Backup and Restore Overview, on page 1
- Embedded NSO backup, on page 2
- Manage Crosswork Network Controller Backup and Restore, on page 3
- Restore Crosswork Network Controller After a Disaster, on page 6
- Crosswork Data Gateway disaster recovery scenarios, on page 7
- Resolve SR-TE policies and RSVP-TE tunnels, on page 10
- Backup Crosswork Network Controller with external NSO, on page 11
- Restore Crosswork Network Controller with external NSO, on page 13
- Migrate data using backup and restore, on page 14

Backup and Restore Overview

Crosswork Network Controller's backup and restore features help prevent data loss and preserve your installed applications and settings.

Among the backup options, you can also choose to **Backup NSO**. This option preserves the external NSO data along with the Crosswork Network Controller configuration. See Backup Crosswork Network Controller with external NSO, on page 11 for details.

Crosswork Network Controller offers multiple menu options to backup and restore your data.

From the main menu, click **Administration** > **Backup and Restore** to access the **Backup and Restore** window.

Table 1: Backup and Restore options

Menu option	Description
Actions > Data Backup (See Manage Crosswork Network Controller Backup and Restore, on page 3 for details)	Preserves the Crosswork Network Controller configuration data. The backup file can be used with the data disaster restore (Restore Crosswork Network Controller After a Disaster, on page 6) to recover from a serious outage.

Menu option	Description
Actions > Data Disaster Restore (See Restore Crosswork Network Controller After a Disaster, on page 6 for details)	Restores the Crosswork Network Controller configuration data after a natural or human-caused disaster has required you to rebuild a Crosswork cluster. First, deploy a new cluster by following the instructions in the *Cisco Crosswork Network Controller 7.1 Installation Guide*. Ensure you install the exact versions of the applications that were in your old Crosswork cluster when you made the data backup. Any version mismatch can lead to data loss and restore job failure.
Actions > Data Migration (See Migrate data using backup and restore, on page 14 for details)	Migrates data from an older version of Crosswork Network Controller to a newer version.

Table 2: Supported Backup Restore Combinations

Backup Type	From Deployment	To Deployment	Support
Data only	Geo redundant	Geo redundant	Supported
Data only	Non-geo redundant	Non-geo redundant	Supported

Any other combination is not supported.

Embedded NSO backup

Crosswork Network Controller, deployed on a single VM with the Advantage package, uses an embedded NSO instead of an external NSO. The embedded NSO is part of the Advantage package and is automatically installed when the Crosswork Network Controller Advantage package is deployed on a single VM.

Backing up embedded NSO

- Embedded NSO is always included in the data backup and restore operation. Unlike an external NSO, the embedded NSO cannot be excluded during a backup operation, meaning there is no separate workflow specifically for backing up or restoring embedded NSO information.
- In case of embedded NSO, there is no specific option in the UI to enable/disable Backup NSO.
- The embedded NSO tar file is included as part of the primary backup tar file.
- Embedded NSO is currently not included during the data migration between different Crosswork Network Controller release versions.
- When the embedded NSO is installed on the Crosswork Network Controller:
  - An NSO provider entry is automatically onboarded on the Providers page.
  - An SSO service provider entry with NSO cross-launch support is automatically added on the SSO page.

The embedded NSO provider and the SSO service provider entries cannot be edited or deleted. If the SSO configuration is removed, restarting the embedded NSO automatically adds it back to the system.

Note Any data configured on a device after a backup operation will not be in sync with NSO once the restore operation is completed. You must perform a check sync on the device to obtain the correct status before initiating the restore operation.

Manage Crosswork Network Controller Backup and Restore

This section explains how to perform a data backup and restore operation from the Crosswork Network Controller UI.

Attention

- Building a target machine for the backup is out of scope for this document. The operator is expected to have the server in place, know the server credentials, and have a target directory with adequate space for the backups.
- Crosswork Network Controller does not manage the backups. It is the operator's responsibility to periodically delete old backups from the target server to make room for future backups.
- Crosswork Network Controller backup process depends on having SCP access to a server with sufficient storage space. The storage required for each backup will vary based on your cluster size, applications in the cluster, and scale requirements.
- The time taken for the backup or restore processes will vary based on the type of backup, your cluster size, and the applications in the cluster.
- If you want to include the external NSO data in the Crosswork Network Controller backup process, follow the instructions given in Backup Crosswork Network Controller with external NSO, on page 11 instead of the instructions in this topic.

Before you begin

Ensure that you have:

- The hostname or IP address and the port number of the secure SCP server. Ensure that the server has sufficient storage available.
- A file path on the SCP server, to use as the destination for your backup files.
- User credentials for an account with file read and write permissions to the remote path on the destination SCP server.
- Made a note of the build version of the installed applications. Before performing a data restore, you must install the exact versions of those applications. Any mismatch in build versions can result in data loss and failure of the data restore job.

When creating or restoring backups for a Crosswork Network Controller cluster, follow these guidelines:

- Configure a destination SCP server for storing backup files during your first login. This is a one-time setup and must be completed before taking backups or initiating restore operations.
- Perform backup or restore operations during a scheduled maintenance window. Users should not access the system during these operations. Backups will take the system offline for about 10 minutes, while restore operations can be lengthy and pause other applications, affecting data-collection jobs.
- Use the same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- Use the dashboard to monitor the progress of backup or restore processes. Avoid using the system during these processes to prevent errors or incorrect content.
- Only one backup or restore operation can run at a time.
- Ensure both the Crosswork Network Controller cluster and the SCP server are in the same IP environment (e.g., both using IPv6).
- Delete older backups to save space on the backup server, though they may still appear in the job list.
- Operators making frequent changes should back up more often (possibly daily), while others might back up weekly or before major system upgrades.
- By default, backups are not allowed if the system is not considered healthy, but this can be overridden for troubleshooting purposes.
- Export the cluster inventory file when performing a data backup. For more information, see Export Cluster Inventory.
- If Crosswork Network Controller is reinstalled after a disaster and Data Gateways are enrolled before the restore, a certificate mismatch may occur. To fix this, re-import the certificates from the **Change Current System Settings** menu on the Crosswork Data Gateway VM. For information on how to import the certificate, see Change the system settings.

Procedure

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create a backup:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data Backup** to display the **Data Backup** dialog box with the destination server details pre-filled.
c) Provide a relevant name for the backup in the **Job Name** field.
d) If you want to create the backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
e) Uncheck the **Backup NSO** checkbox if you don't want to include external NSO data in the backup.

Important

- You must configure the SSH connectivity protocol in the NSO provider to use the **Backup NSO** option; otherwise, the backup will fail.

- The **Backup NSO** option is not applicable for single VM deployments.

f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

g) (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. If the check is successful, Crosswork Network Controller displays a warning about the time-consuming nature of the operation. Click **OK** to continue.

h) Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.

i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

j) *If the backup fails during upload to the remote server:* In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note
The upload can fail due to multiple problems such as incorrect credentials, invalid destination directory, or lack of space in server. Investigate the problem and fix it (for example, clean old backups to free up space or use the **Destination** button to specify a different remote server and path) before clicking the **Upload backup** button.

Step 3 **To restore from a backup file:**

a) From the main menu, choose **Administration** > **Backup and Restore**.

b) In the **Backup and Restore Job Sets** table, select the data backup file to be used for the restore. The **Job Details** panel shows information about the selected backup file.

c) With the backup file selected, click the **Data Restore** button shown on the **Job Details** panel to start the restore operation. Crosswork Network Controller creates the corresponding restore job set and adds it to the job list.

To view the progress of the restore operation, click the link to the progress dashboard.

Attention
If the MDT (Model-driven Telemetry) collection jobs are deleted after a backup, the restore operation will fail to recover the MDT collection tasks. The MDT collection tasks will be in an error state as the associate devices will not have the required configurations.

This situation can be rectified using any ONE of the following actions:

- Restore the backup taken for external NSO (only possible if the backup was created with external NSO).
- Move the devices associated with MDT collection DOWN and UP in Device Management.
- Detach and attach devices to the Crosswork Data Gateway pool.

Note
In a geo redundant setup, if external destinations are added and Data Gateway is re-enrolled after a backup is taken, restoring the backup file may result in stale certificate expiry alarms. These alarms must be manually cleared.

Restore Crosswork Network Controller After a Disaster

A disaster recovery is a restore operation used after a natural or human-caused disaster destroys a Cisco Crosswork cluster. First, deploy a new cluster by following the instructions in the *Cisco Crosswork Network Controller 7.1 Installation Guide*.

Note If your cluster has only one malfunctioning hybrid node or one or more malfunctioning worker nodes, do not perform a disaster recovery. Instead, use cluster management features to redeploy or replace these nodes. If more than one hybrid node is malfunctioning, the system will not be functional. Replacing or rebooting the failed hybrid nodes may not guarantee recovery. In this case, deploy a new cluster and recover the entire system using a recent backup from the old cluster. For more information, see the Manage the Crosswork Cluster chapter in this guide.

To perform a disaster recovery:

Before you begin

Before performing a Data Disaster Restore, ensure the following:

- Obtain the full name of the backup file you want to use from the SCP backup server. Typically, this will be the most recent backup file you have created. Crosswork Network Controller backup filenames typically follow this format:

  `backup_JobName_CWVersion_TimeStamp.tar`

  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the Crosswork Network Controller platform version of the backed-up system.
  - *TimeStamp* is the date and time when Crosswork Network Controller created the backup file.

  For example: `backup_Wednesday_7-0_2024-08-31-12-00.tar`.

- Install the exact versions of the applications that were present in your old Crosswork Network Controller cluster when the data backup was made. Any version mismatch can lead to data loss and restore job failure.
- The new Crosswork Network Controller cluster must use the same IP addresses as the original cluster where the backup was taken. This is crucial because internal certificates rely on these IP addresses.
- The new cluster must have the same number and types of nodes as the original cluster.
- Use the same Crosswork Network Controller software image that was used when creating the backup. You cannot restore the cluster using a backup created with a different software version.
- Keep your backups up-to-date to ensure you can recover the system's true state as it existed before the disaster. If you have installed new applications or patches since your last backup, take another backup.
- If the disaster recovery fails, contact Cisco Customer Experience for assistance.
- Smart licensing registration for Crosswork Network Controller applications is not restored during a disaster restore operation and must be registered again.

Procedure

Step 1 From the main menu of the newly deployed cluster, choose **Administration** > **Backup and Restore**.

Step 2 Click **Actions** > **Data Disaster Restore** to display the **Data Disaster Restore** dialog box with the remote server details pre-filled.

Step 3 In the **Backup File Name** field, enter the file name of the backup from which you want to restore.

Step 4 Click **Start Restore** to initiate the recovery operation.

To view the progress of the operation, click the link to the progress dashboard.

Crosswork Data Gateway disaster recovery scenarios

This section explains the various scenarios to restore the Data Gateways after Cisco Crosswork Network Controller recovers from a disaster.

The Crosswork Network Controller disaster recovery process automatically restores the Data Gateways in the network. You only need to follow additional procedures if the Data Gateway VMs have been deleted from Crosswork Network Controller.

- Crosswork Data Gateway disaster recovery with high availability, on page 7: All active and standby VMs in a pool have the **Operational state** as **Error**.
- Crosswork Data Gateway disaster recovery without high availability, on page 8: A pool that has only one Data Gateway VM, or a pool that has multiple active Data Gateway VMs in the **Error** state without any standby VMs.

Crosswork Data Gateway disaster recovery with high availability

Follow these steps to restore a Data Gateway pool with active and standby Data Gateway VMs in the **Error** state. For the purpose of these instructions, we use a pool with one active and one standby VM.

Before you begin

Ensure that you have completed the Cisco Crosswork disaster recovery operation before you proceed with this procedure. This implies that the Crosswork backed up data before the disaster is restored and all the Crosswork's pods are healthy and operational.

Note Do not redeploy the Data Gateways before verifying that Crosswork is fully restored and all the pods are healthy.

Procedure

Step 1 Install new Data Gateway VMs with same information (profile, hostname, management interface) as the VMs in the pool prior to the disaster.

The newly installed Data Gateway VMs have the operational state as **Error** since Cisco Crosswork's disaster recovery process restores data from the older VMs.

Step 2 Log in to Cisco Crosswork.

Step 3 Navigate to **Administration** > **Data Gateway Management** > **Pools**.

Step 4 Select and edit the pool to remove (unassign) the standby VM from the pool. See Edit or delete a Data Gateway pool

Step 5 Change the **Administration State** of the standby VM to the **Maintenance** mode. See Change the administration state of Crosswork Data Gateway.

Note
If the Data Gateway is redeployed without moving it to the **Maintenance** mode, the enrollment with Crosswork fails and the following errors appear in the logs:

In the dg-manager logs:

```
time="2025-03-18 06:44:54.305973" level=error msg="[re-installing dg requires admin state to be in
maintenance mode and role "+\n"to be unassigned]" tag=ROBOT_dg-manager_dg-manager-0 - DG re-installed
```

In the controller-gateway logs:

```
2025-02-11T21:25:32.373 ERROR - Received Error from AutoEnroll Challenge Token Response call
re-installing dg requires admin state to be in maintenance mode and role to be unassigned
2025-02-11T21:25:32.373 ERROR - Error while posting sendTokenResponse re-installing dg requires admin
 state to be in maintenance mode and role to be unassigned
```

To rectify the problem, you can switch the Data Gateway to the **Maintenance** mode or manually re-enroll the gateway. For more information, Re-enroll Crosswork Data Gateway.

Step 6 Edit the pool again and add the standby VM to the pool.

Adding the standby VM triggers a failover and the newly added VM becomes the active VM in the pool.

Step 7 Repeat steps 4 to 6 to restore the (now) standby VM that has the **Operational State** as **Error**.

Step 8 Verify the following:

- The pool has an active and standby VM as before.
- Devices are attached to active VM in the pool.
- Collection jobs are running as expected.

Crosswork Data Gateway disaster recovery without high availability

In case of a disaster, you can restore the Data Gateway VM without high availability by using one of these methods:

- Replace the old VM with a newly installed VM that is installed with the same information as the old VM

- Detach devices or move devices to another Data Gateway in the network
- Add a standby VM to the pool (install an additional VM and add it as a standby in the pool)

Before you begin

Ensure that you have completed the Cisco Crosswork disaster recovery operation before you proceed with this procedure. All information about the Data Gateway VMs and pools will be available in Cisco Crosswork once the Crosswork disaster recovery process is complete.

Procedure

Step 1 **Replace the old VM with a newly installed VM that is installed with the same information as the old VM**

a) Log in to Cisco Crosswork.
b) Navigate to **Administration** > **Data Gateway Management** > **Data gateways**.
c) Delete the existing pool.
d) Change the **Administration State** of the VM to the **Maintenance** mode. See Change the administration state of Crosswork Data Gateway.
e) Install a new Data Gateway VM with the same information as the older VM.
f) Change the **Administration State** of the VM to **Up** from **Maintenance**.

The **Operational State** of the VM changes from **Error** to **Not Ready**.

g) Create a new pool with the same name as the older pool and add the VM to the pool.

Verify that Data Gateway has the **Operational State** as **Up**

h) Attach devices to Data Gateway. See Attach devices to Data Gateway.
i) Verify that collection jobs are running as expected.

Step 2 **Detach devices or move devices to another Data Gateway in the network**

a) Log in to Cisco Crosswork.
b) Navigate to **Administration** > **Data Gateway Management** > **Data gateways**.
c) Detach devices from the VM or move devices to another Data Gateway that is operationally **Up**. See Manage Crosswork Data Gateway device assignments.
d) Delete the existing pool.

This step will not unassign the VM from the pool. The VM will continue to show as assigned to the pool.

e) Change the **Administration State** of the VM to the **Maintenance** mode. See Change the administration state of Crosswork Data Gateway.
f) Reboot the VM. With this step, the VM is unassigned from the pool.

Wait for about 5 minutes. The VM enrolls with Cisco Crosswork automatically. Verify that the VM is in the administratively UP and is in the **Not Ready** state.

Note
You can also manually re-enroll the VM with Cisco Crosswork from the Interactive Console of the Data Gateway VM. See Re-Enroll Crosswork Data Gateway.

g) Create a new pool with the same name as the older pool and add the VM to the pool.
h) Verify that Data Gateway has the **Operational State** as **Up**.

i) Attach devices or move devices back to this Data Gateway. See Manage Crosswork Data Gateway device assignments.
j) Verify that collection jobs are running as expected.

Step 3 **Add a standby VM to the pool (install an additional VM and add it as a standby in the pool)**

Note
The following steps list the procedure to restore a pool that has a single active VM in the **Error** state. To restore multiple active VMs in a pool in the **Error** state without any standby VMs, ensure that you add an additonal VM for each active VM in the pool.

a) Install a new Data Gateway VM.
b) Log in to Cisco Crosswork.
c) Navigate to **Administration** > **Data Gateway Management** > **Pools**.
d) Select and edit the pool to add the newly installed VM to the pool. See Edit or delete a Data Gateway pool

   Adding the VM triggers a failover and the newly added VM become the active VM in the pool.

e) Edit the pool and remove the (now) standby VM from the pool.
f) Change the **Administration state** of the standby VM to **Maintenance** mode. See Change the administration state of Crosswork Data Gateway.

   Wait for about 5 minutes. The VM enrolls with Cisco Crosswork automatically. Verify that the VM is operationally UP and is in the **Not Ready** state.

   Note
   You can also manually re-enroll the VM with Cisco Crosswork from the Interactive Console of the Data Gateway VM. See Re-Enroll Crosswork Data Gateway.

g) Edit the pool again and add the standby VM to the pool.
h) Verify the Data Gateway is operationally **Up** and the pool has an active and standby VM.
i) Verify the following:

   - Devices are attached to active VM in the pool.
   - Collection jobs are running as expected.

Resolve SR-TE policies and RSVP-TE tunnels

Orphaned TE policies are any PCE initiated SR-TE policies (SRv6, SR-MPLS, and Tree-SID) or RSVP-TE tunnels that were created within Crosswork Network Controller and *after* the last cluster data synchronization. After a switchover in a High Availability setup, the system automatically checks for any orphaned TE policies. Orphaned policies/tunnels may also happen after a backup/restore operation. You can view policy details but not modify them since they were not included in the last data synchronization. Crosswork Network Controller will display an alarm when it finds orphan TE policies (**Alerts > Alarms and Events**).

Crosswork Network Controller provides APIs to help clear these orphans. To get a list of orphan SR-TE policies or RSVP-TE tunnels, use **cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** or **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** where **is-orphan=True** and default action is GET. To make the orphans manageable again, use a SAVE action for the corresponding URL per policy type. For more information, see API documentation on Devnet (**API Reference > Crosswork Optimization Engine**).

Backup Crosswork Network Controller with external NSO

You can create a backup of just the Crosswork Network Controller or include a copy of the NSO CDB (the default data store for configuration data in NSO). To back up the CDB, your Crosswork Network Controller user account must meet specific requirements detailed in the Add a Cisco NSO provider section.

Note While the backup can be automated, the restore of the NSO CDB is a manual process. For detailed instructions, see Restore Crosswork Network Controller with external NSO, on page 13).

Before you begin

Ensure that:

- You have installed the compatible version of NSO in system default mode.
- You have installed the latest version of the Crosswork Network Controller Transport SDN function pack using the **NSO deployment manager** window. For more information, see *Install Cisco NSO Function Pack Bundles from Crosswork UI* in the *Crosswork Network Controller 7.1 Installation Guide*.
  - If you did not install the Transport SDN Function Pack using the **NSO deployment manager** window and instead installed it manually, you must manually copy the `ncs_backup.sh` script into the `/var/opt/ncs/scripts` folder. Otherwise, the backup operation will fail.
    1. Get the NCS run directory using the command: `vi $NCS_DIR/../installdirs`

       Example: `NCS_RUN_DIR="/var/opt/ncs"`
    2. Copy the scripts to the NCS run directory.

       ```
       $ cd tsdn-<RELEASE-VERSION>-nso-<NSO-VERSION>/
       $ sudo cp ncs_backup.sh <NCS_RUN_DIR>/scripts/
       $ sudo cp ncs_restore.sh <NCS_RUN_DIR>/scripts/
       ```

       Example:

       ```
       $ sudo cp ncs_backup.sh /var/opt/ncs/scripts/
       $ sudo cp ncs_restore.sh /var/opt/ncs/scripts/
       ```
- You have the hostname or IP address and the port number of a secure SCP server.
- You have a file path on the SCP server, to use as the destination for your backup files.
- You have the user credentials for an account with read and write permissions to the storage folder on the destination SCP server.
- In order to select the **Backup NSO** option, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail.
- The NSO provider, the Crosswork Network Controller credential profile associated with the NSO provider, and the NSO server meet the following prerequisites:
  - Ensure that SSH is enabled on the NSO provider configuration.

- The user ID associated with the SSH connectivity type in the credential profile assigned to the NSO provider has sudo permissions.
- The user in the NSO provider's credential profile has full access to the NSO server's backup folder and the files in it. This requirement usually means proper file permissions (full read and write access) to the NSO server's `/var/opt/ncs/backups/` folder.

Failure to meet any of these requirements means that all or part of the backup job will fail.

In addition to these special requirements, the normal guidelines for backups discussed in Manage Crosswork Network Controller Backup and Restore, on page 3 also apply to backups containing external NSO data.

Procedure

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create the backups of Crosswork Network Controller and external NSO:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Backup** to display the **Backup** dialog box with the destination server details prefilled.
c) Provide a relevant name for the backup in the **Job Name** field.
d) If you want to create the backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
e) Leave the **Backup NSO** check box checked.
f) Complete the remaining fields as needed.

   If you want to use a different remote server upload destination, click **cancel**, then select the destination tab and edit the values.

g) Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set adds it to the job list, and begins processing the backup. The Job Details pane reports the status of each backup step as it is completed.
h) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup Restore Job Sets** table. Then click on the job set you want.

   The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

i) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

   If the upload failed due to problems with the remote server, use the **Destination** button to specify a different remote server and path before clicking **Upload backup**.

Restore Crosswork Network Controller with external NSO

When you restore a Crosswork Network Controller cluster and its associated NSO from a backup, follow these guidelines:

- We recommend performing restore operations during a scheduled maintenance window only. Users should not attempt to access Crosswork Network Controller or NSO while these operations are running. The restore operations are lengthy and will pause other Crosswork Network Controller applications until they are complete. NSO must be completely stopped during restore operation.

Note Restore from the external NSO backup file is a manual process.

Before you begin

Get the full name of the backup file you want to restore from the SCP server. This file will contain both the Crosswork Network Controller and NSO backups. Backup filenames have the following format:

`backup_`*`JobName_CWVersion_TimeStamp`*`.tar`

Where:

- *JobName* is the user-entered name of the backup job.
- *CWVersion* is the Crosswork Network Controller version of the backed-up system.
- *TimeStamp* is the date and time when Crosswork Network Controller created the backup file.

For example: `backup_Wed_7-1_2024-08-31-12-00.tar`.

Procedure

Step 1 Log in (if needed) to the remote SCP backup server. Using the Linux command line, access the backup destination directory and find the backup file containing external NSO information that you want to restore. For example:

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_7-0_2024-08-31-12-00.tar
```

Step 2 Use `tar -xvf` to extract the NSO backup from the Crosswork Network Controller backup file in the destination folder. For example:

```
[root@localhost~]# tar -xvf backup_Wed_7-0_2024-08-31-12-00.tar
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_7-0_2024-08-31-12-00.tar
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar
```

Step 3 Un-tar the NSO backup file in the destination folder. You will see NSO files being extracted to a folder structure under `/nso/`*`ProviderName`*`/`, where `/nso/`*`ProviderName`*`/` is the name of the NSO provider as configured in Crosswork Network Controller. In the following example, the NSO provider is named `nso121`:

```
tar -xvf 468c4715-ea09-4c2b-905e-98999d.tar
468c4715-ea09-4c2b-905e-98999d/nso/
```

```
468c4715-ea09-4c2b-905e-98999d/nso/nso121/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/nso_backup_result_nso121_Wed.log
468c4715-ea09-4c2b-905e-98999d/nso/nso121/NSO_RESTORE_PATH_nso121
468c4715-ea09-4c2b-905e-98999d/nso/nso121/ncs-5.4.2@backup_Wed_nso121.backup.gz
...
```

Step 4 Locate the file with a backup.gz extension in the `/nso/ProviderName/` folder. This is the generated NSO backup file. In the example in the previous step, the file name is highlighted.

Step 5 Log in to NSO as a user with root privileges and access the command line. Then copy or move the generated NSO backup file from the SCP server to the specified restore path location of the NSO cluster. For example:

```
[root@localhost nso121]# ls
log ncs-5.4.2@backup_Wed_nso121.backup.gz NSO_RESTORE_PATH_nso121
[root@localhost nso121]# more NSO_RESTORE_PATH_nso121
/var/opt/ncs/backups/
[root@localhost nso121]#
...
```

Step 6 You can perform NSO restore operations only while NSO is not running. At the NSO cluster command line, run the following command to stop NSO:

```
$/etc/init.d/ncs stop
```

Step 7 Once NCS has stopped, start the restore operation using the following command and the name of the generated NSO backup file. For example:

```
#ncs-backup --restore ncs-5.4.2@backup_Wed_nso121.backup.gz
```

If you have trouble running this command, first give yourself `sudo su` permission.

Step 8 Once the restore completes, restart NSO using the following command. This command may take a few minutes to complete.

```
$/etc/init.d/ncs start
```

Step 9 Once you have restored both Crosswork Network Controller and NSO clusters from backups, re-add the NSO provider to Crosswork Network Controller.

Step 10 Complete the NSO configuration to ensure that the provisioning services function properly. For more information, see Configure Standalone NSO.

Migrate data using backup and restore

Using data migration backup and restore is a prerequisite when upgrading your Crosswork Network Controller installation to a new software version, or moving your existing data to a new installation.

Follow these guidelines whenever you create a data migration backup:

- Ensure that you have configured a destination SCP server to store the data migration files. This configuration is a one-time activity.
- Both the Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller is communicating over IPv6, so must the backup server.
- We recommend that you create a data migration backup only when upgrading your Crosswork Network Controller installation, and that you do so during a scheduled upgrade window only. Users shouldn't

attempt to access Crosswork Network Controller while the data migration backup or restore operations are running.

- Ensure that you capture a screenshot of Data Gateways to keep a record of the assigned IP addresses and names. You need this information when you deploy the new Data Gateways.

Before you begin

Ensure that you have:

- The hostname or IP address and the port number of a secure SCP server.
- A file path on the SCP server, to use as the destination for your data migration backup files.
- User credentials for an account with file read and write permissions to the remote path on the destination SCP server.

Procedure

Step 1 **Configure a SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create a backup:**

a) Log in as an administrator to the Crosswork Network Controller installation whose data you want to migrate to another installation.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data Backup** to display the **Data Backup** dialog box with the destination server details prefilled.
d) Provide a relevant name for the backup in the **Job Name** field.
e) If you want to create the backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
f) Complete the remaining fields as needed.

   If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.
g) Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.
h) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

   The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.
i) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

   If the upload failed due to problems with the remote server, use the **Destination** button to specify a different remote server and path before clicking **Upload backup**.

Step 3 **Migrate the backup to the new installation:**

a) Log in as an administrator on the Crosswork Network Controller installation to which you want to migrate data from the backup.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data Migration** to display the **Data Migration** dialog box with the remote server details pre-filled.
d) In the **Backup File Name** field, enter the file name of the backup from which you want to restore.
e) Click **Start Migration** to initiate the data migration. Crosswork Network Controllercreates the corresponding migration job set and adds it to the job list.

To view the progress of the data migration operation, click the link to the progress dashboard.

Step 4 **Deploy Crosswork Data Gateway:**

a. After the migration is complete, log out from the Crosswork UI and log in again to the UI using https://<new_crosswork_ip>:30603.

The **Action to be taken** pop-up appears with the message **Please Acknowledge once redeploy of the CDGs is done**.

b. In the **Action to be taken** pop-up, click **Cancel**.

c. Delete the old Data Gateway VMs and install new gateways. Ensure that they have the identical IPs and names as the previous gateway VMs.

d. Verify that the deployment of Data Gateway is complete, and the gateway is registered with Crosswork Network Controller.

e. Verify that Data Gateway is in the same state as it was before the upgrade by choosing **Administration > Data Gateway Management > Virtual Machines**. The **Operation** and **Administration** state of Data Gateways should be UP.

f. After all the Data Gateways are active, navigate to **Administration > Data Gateway Management > Pools** page to verify the successful migration of all pools from the previous cluster version and ensure that Data Gateways are automatically enrolled with Crosswork Network Controller.

g. Log out from the Crosswork UI and log in back to the UI using https://<new_crosswork_ip>:30603. The **Action to be taken** pop-up appears.

Note
Do not click on the browser history links that have a child path to access the UI. This prevents the **Action taken** pop-up from appearing.

h. In the pop-up, click **Acknowledge**. With this step, the migration should be complete.

i. If the NSO is set to the read-only mode, disable it.