Manage Backups

This section contains the following topics:

Backup and Restore Overview

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

Cisco Crosswork 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 Cisco Crosswork Backup and Restore, on page 2 for details)	Preserves the Cisco Crosswork configuration data. The backup file can be used with the data disaster restore (Restore Cisco Crosswork After a Disaster, on page 5) to recover from a serious outage. Among the backup options, you can also choose to **Backup with NSO**. This option preserves the Cisco NSO data along with the Cisco Crosswork configuration. See Backup Cisco Crosswork with Cisco NSO, on page 10 for details.

Menu option	Description
Actions > Data Disaster Restore (See Restore Cisco Crosswork After a Disaster, on page 5 for details)	Restores the Cisco Crosswork configuration data after a natural or human-caused disaster has destroyed a Crosswork cluster. You must deploy a new cluster first, following the instructions in *Cisco Crosswork Network Controller 6.0 Installation Guide*, and must install the exact versions of the applications that were present in your old Crosswork cluster (when you made the data backup) in your new Crosswork cluster. Any mismatch in the build versions of the applications can result in data loss and failure of the restore job.
Actions > Data Migration (See Migrate Data Using Backup and Restore, on page 13 for details)	Migrates data from an older version of Cisco Crosswork to a newer version.

Manage Cisco Crosswork Backup and Restore

This section explains how to perform a data backup and restore operation from the Cisco Crosswork 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, to know the credentials for the server, and to have a target directory with adequate space for the backups in place.
- Crosswork does not manage the backups. It is up to the operator to periodically delete old backups from the target server to make room for future backups.
- Cisco Crosswork backup process depends on having SCP access to a server with sufficient amount of storage space. The storage required each backup will vary based on the your cluster size, applications in the cluster, and the scale requirements.
- The time taken for the backup or restore processes will vary based on the the type of backup, your cluster size and the applications in the cluster.

When you create backups for a Crosswork cluster, or restore a cluster from a backup, follow these guidelines:

- During your first login, configure a destination SCP server to store backup files. This configuration is a one-time activity. You can't take a backup or initiate a restore operation until you complete this task.
- We recommend that you perform backup or restore operations during a scheduled maintenance window only. Users shouldn't attempt to access Cisco Crosswork while these operations are running. Backups will take the system offline for about 10 minutes, but restore operations can be lengthy. Both will pause other applications until they are complete. These pauses can affect data-collection jobs.
- When performing a *data disaster* restore, you must use the same Cisco Crosswork software image that you used when creating the backup. You can't perform a disaster restore using a backup created using a different version of the software.

- Use the dashboard to monitor the progress of the backup or restore process, until the process completes. If you attempt to use the Cisco Crosswork system during the process, you may see incorrect content or errors, since various services pause and restart frequently.
- You can run only one backup or restore operation at a given time.
- Both the Crosswork cluster and the SCP server must be in the same IP environment. For example, if Crosswork is communicating over IPv6, so must the backup server.
- To save space on your backup server, you can delete older backups, but they may still appear in the job list in this version.
- Operators that make more changes should back up more often (possibly daily) while others might be comfortable with doing a backup once a week or before major system upgrades.
- By default, Cisco Crosswork will not allow you to make a backup of a system that it does not consider as healthy. However, there are provisions to override this protection to facilitate the sharing of an image with Cisco for additional analysis or other troubleshooting efforts.
- We recommend that you export the cluster inventory file when you perform a data backup.
- If Crosswork is installed (fresh install or reinstalled) after a disaster or failure and the data gateways are enrolled or integrated to the new Crosswork instance before the restore operation, it results in a certificate mismatch and the data gateways are moved to an error state. To correct the certificate issue, navigate to the Crosswork Data Gateway VM's interactive menu and re-import the certificates from the **Change Current System Settings** menu. For information on how to import the certificate, see Change Current System Settings.

Before you begin

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 the data restore, you must install the exact versions of those applications. Any mismatch in the build versions of the applications can result in data loss and failure of the data restore job.

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 Cisco Crosswork application or microservice issues, check the **Force** check box.

e) Uncheck the **Backup NSO** checkbox if you don't want to include Cisco NSO data in the backup.

   If you do want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in Backup Cisco Crosswork with Cisco NSO, on page 10 instead of the instructions here.

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 Cisco Crosswork has enough free resources to complete the backup. If the check is successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK** to continue.

h) Click **Start Backup** to start the backup operation. Cisco Crosswork 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. Cisco Crosswork 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 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 NSO (only possible if the backup was created with NSO).
   - Move the devices associated with MDT collection DOWN and UP in Device Management.
   - Detach and attach devices to the Crosswork Data Gateway pool.

Restore Cisco Crosswork After a Disaster

A disaster recovery is a restore operation that you use after a natural or human-caused disaster has destroyed a Cisco Crosswork cluster. You must deploy a new cluster first, following the instructions in *Cisco Crosswork Network Controller 6.0 Installation Guide*.

If your cluster only has one malfunctioning hybrid node, or one or more malfunctioning worker nodes, don't perform a disaster recovery. Instead, use cluster management features to redeploy these nodes, or replace them with new nodes, as explained in the Manage the Crosswork Cluster chapter in this guide.

If you have more than one malfunctioning hybrid node, the system will not be in a functional state. Even if you replace or reboot the failed hybrid nodes, there is no guarantee that the system will recover correctly. In this case, you can deploy a new cluster, and then recover the entire system using a recent backup taken from the old cluster.

For more information, see the Manage the Crosswork Cluster chapter in this guide.

When conducting a data disaster recovery, note the following:

- Before performing the **Data Disaster Restore**, the exact versions of the applications that were present in your old Crosswork cluster (when you made the data backup) must be installed and available in your new Crosswork cluster. Any mismatch in the build versions of the applications can result in data loss and failure of the restore job.
- The new Cisco Crosswork cluster to which you restore the backup must use the same IP addresses as the one where you took the backup. This guideline is important, as internal certificates use the IP addresses of the original cluster.
- The new cluster must have the same number and types of nodes as the cluster where you took the backup.
- The new cluster must use the same Cisco Crosswork software image that you used when creating the backup. You can't restore the cluster using a backup that was created using a different version of the software.
- Keep your backups current, so that you can recover the true state of your system as it existed before the disaster. The restore operation restores all applications that are installed at the time the backup was made. If you have installed more applications or patches since your last backup, take another backup.
- If the disaster recovery fails, contact Cisco Customer Experience.
- Smart licensing registration for Crosswork applications are not restored during a disaster restore operation, and must be registered again.

To perform a disaster recovery:

Before you begin

Get the full name of the backup file you want to use in your disaster recovery from the SCP backup server. This file is normally the most recent backup file you have made. Cisco Crosswork backup filenames have the following format:

```
backup_JobName_CWVersion_TimeStamp.tar.gz
```

Where:

- *JobName* is the user-entered name of the backup job.

- *CWVersion* is the Cisco Crosswork platform version of the backed-up system.
- *TimeStamp* is the date and time when Cisco Crosswork created the backup file.

For example: `backup_Wednesday_4-0_2021-02-31-12-00.tar.gz`.

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 CrossworkData Gateways after Cisco Crosswork recovers from a disaster.

Cisco Crosswork's disaster recovery process restores the CrossworkData Gateways in the network automatically. The following procedures are required only in case the CrossworkData Gateway VMs have been deleted from Cisco Crosswork.

- Crosswork Data Gateway Disaster Recovery with High Availability, on page 6: All active and standby Crosswork Data Gateway VMs in a pool have the **Operational state** as **Error**.
- Crosswork Data Gateway Disaster Recovery without High Availability, on page 7: A pool that has only one Crosswork Data Gateway VM, or a pool that has multiple active Crosswork 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 Crosswork Data Gateway pool with active and standby CrossworkData 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 no redeploy the data gateways before verifying that Crosswork is fully restored and all the pods are healthy.

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

The newly installed CrossworkData 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 Manage a Crosswork Data Gateway Pool

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

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="2023-03-18 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:

```
2021-02-11T21:25:32.373 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
2021-02-11T21:25:32.373 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 7 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 CrossworkData Gateway VM without high availability by using one of the following methods (**Steps**):

- 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 Crosswork Data Gateway VMs and pools will be available in Cisco Crosswork once the Crosswork disaster recovery process is complete.

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 Cisco Crosswork Data Gateway Instance.
e) Install a new Crosswork 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 the CrossworkData Gateway has the **Operational State** as **Up**

h) Attach devices to the Data Gateway. See Attach Devices to a Crosswork 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 Cisco 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 Cisco Crosswork Data Gateway Instance.
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 the CrossworkData Gateway has the **Operational State** as **Up**.
i) Attach devices or move devices back to this Data Gateway. See Manage Cisco 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 CrossworkData 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 Manage a Crosswork 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 Cisco Crosswork Data Gateway Instance.

   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 CrossworkData 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 and *after* the last cluster data synchronization. After a switchover in a High Availability setup, Crosswork automatically checks for any orphaned TE policies. Orphaned policies/tunnels may also happen after a backup/restore operation. You will be able to view policy details, but not modify them since they were not included as part of the last data synchronization. Crosswork will display an alarm when it finds orphan TE policies (**Administration > Alarms**).

Crosswork 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 (**Crosswork Optimization Engine APIs > 6.0 Release APIs**).

Backup Cisco Crosswork with Cisco NSO

You have the option to create backup of only Crosswork or create a backup that also captures a copy of the NSO CDB (the default data store for configuration data in NSO). The ability to backup the CDB requires your Crosswork user account to meet specific requirements detailed here and in the Add Cisco NSO Providers section.

Note While the backup can be automated (as described), the restore of the NSO CDB is a manual process (see Restore Cisco Crosswork with Cisco NSO, on page 11).

Before you begin

Before you begin, be sure:

- 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.

Also ensure that the NSO provider, the Cisco Crosswork credential profile that is 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 NSO server has NCT (NSO Cluster Tools) installed, and the user in the credential profile for the NSO provider can execute `nct` commands.
- 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 full read and write access to the NSO server's `/var/opt/ncs/backups/` folder.

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

In addition to these special requirements, the normal guideliness for backups discussed in Manage Cisco Crosswork Backup and Restore, on page 2 also apply to backups containing NSO data.

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 Cisco Crosswork and Cisco NSO backups:**

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 Cisco Crosswork 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. Cisco Crosswork 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 Cisco Crosswork with Cisco NSO

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

- We recommend that you perform restore operations during a scheduled maintenance window only. Users shouldn’t attempt to access Cisco Crosswork or Cisco NSO while these operations are running. Cisco Crosswork restore operations are lengthy, and will pause other Cisco Crosswork applications until they are complete. Cisco NSO must be stopped completely during restores.

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

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 Cisco Crosswork and Cisco NSO backups. Backup filenames have the following format:

```
backup_JobName_CWVersion_TimeStamp.tar.gz
```

Where:

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

For example: `backup_Wed_4-0_2021-02-31-12-00.tar.gz`.

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 Cisco NSO information that you want to restore. For example:

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar.gz
```

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

```
[root@localhost~]# tar -xzvf backup_Wed_4-0_2021-02-31-12-00.tar.gz
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar.gz
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar.gz
```

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

```
tar -xvsf 468c4715-ea09-4c2b-905e-98999d.tar.gz
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 Cisco NSO backup file. In the example in the previous step, the file name is highlighted.

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

```
[root@localhost nsol21]# ls
log ncs-5.4.2@backup_Wed_nso121.backup.gz NS0_REST0RE_PATH_nso121
[root@localhost nso121]# more NS0_REST0RE_PATH_nso121
/var/opt/ncs/backups/
[root@localhost nso121]#
...
```

Step 6 You can perform Cisco NSO restore operations only while NSO is not running. At the Cisco NSO cluster command line, run the following command to stop Cisco 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 Cisco 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 Cisco 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 Cisco Crosswork and Cisco NSO clusters from backups, re-add the Cisco NSO provider to Cisco Crosswork.

Migrate Data Using Backup and Restore

Using data migration backup and restore is a prerequisite when upgrading your Cisco Crosswork 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 Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.
- We recommend that you create a data migration backup only when upgrading your Cisco Crosswork installation, and that you do so during a scheduled upgrade window only. Users shouldn’t attempt to access Cisco Crosswork while the data migration backup or restore operations are running.
- Ensure that you capture a screenshot of the 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.

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 Cisco Crosswork 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 Cisco Crosswork 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. Cisco Crosswork 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 Cisco Crosswork 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. Cisco Crossworkcreates 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 the data gateway is complete, and the gateway is registered with Crosswork Network Controller.

e. Verify that the 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 the 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.