Manage Backup and Restore

Use this chapter for guidance on protecting your Crosswork Network Controller data and system configurations. Find essential procedures and reference information for backing up, restoring, and recovering your environment.

- Backup and restore features, on page 1
- Embedded NSO backups, on page 2
- Requirements for backup and restore, on page 3
- Best practices for backup and restore, on page 3
- Back up data, on page 4
- Restore data, on page 5
- Restore data after a disaster, on page 6
- Back up data using external NSO, on page 7
- Restore data using an external NSO, on page 9
- Migrate data using backup and restore, on page 11
- Orphaned SR-TE policies and RSVP-TE tunnels, on page 12
- Crosswork Data Gateway disaster recovery scenarios, on page 13

Backup and restore features

Backup and restore features are application functions that

- help prevent data loss,
- preserve installed applications and settings, and
- provide options to back up external data.

To access these features, from the main menu, click **Administration** > **Backup and Restore** to open the **Backup and Restore** window.

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.

Backup and restore options

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

Table 1: Backup and restore options

Menu option	Description
Actions > **Data Backup** (See Back up data, on page 4 for details)	Preserves the Crosswork Network Controller configuration data. The backup file can be used with the data disaster restore (Restore data after a disaster, on page 6) to recover from a serious outage.
Actions > **Data Disaster Restore** (See Restore data 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 7.2 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 11 for details)	Migrates data from an older version of Crosswork Network Controller to a newer version.

Supported backup and restore combinations

Crosswork Network Controller supports these backup and restore combinations.

Table 2: Supported backup and restore combinations

Backup type	From deployment	To deployment	Support
Data only	Geo redundant	Geo redundant	Supported only on the active cluster
Data only	Non-geo redundant	Non-geo redundant	Supported

Any other combination is not supported.

Embedded NSO backups

An embedded NSO backup is a data protection mechanism that

- is automatically included when the Crosswork Network Controller Advantage package is deployed on a single VM,
- always backs up the embedded NSO as part of the main backup operation without separate workflows or exclusion options, and

- includes the embedded NSO data within the primary backup tar file.

Additional information

- The embedded NSO cannot be excluded during backup or restore operations, unlike an external NSO.
- There is no specific option in the UI to enable/disable Backup NSO for embedded NSO.
- Embedded NSO is currently not included during the data migration between different Crosswork Network Controller release versions.
- When installed, the embedded NSO automatically onboards an NSO provider entry and an SSO service provider entry with cross-launch support, which cannot be edited or deleted; if removed, the system reinstates them upon restart.
- 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.

Requirements for backup and restore

These items define the mandatory conditions and limitations that must be met for successful backup and restore operations for a Crosswork Network Controller cluster.

- 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.
- Use the same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- 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).
- 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.
- 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.

Best practices for backup and restore

These items outline suggested actions that help ensure smoother, safer, and more efficient backup and restore processes for a Crosswork Network Controller cluster.

- 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 dashboard to monitor the progress of backup or restore processes. Avoid using the system during these processes to prevent errors or incorrect content.
- Operators are responsible for periodically deleting older backups from the target server to ensure adequate storage for new backups, as Crosswork Network Controller does not manage them. Deleted backups 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.

Back up data

This task describes how to perform a data backup operation from the Crosswork Network Controller UI.

The backup process depends on having SCP access to a server with sufficient storage space. The storage required for each backup varies based on your cluster size, applications in the cluster, and scale requirements. The time taken for the backup process also varies based on the type of backup, cluster size, and applications.

Note 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.

Before you begin

Before you begin:

- Ensure you have a secure SCP server in place, with adequate space for backups. Building the target machine is out of scope for this document.
- Obtain the hostname or IP address and port number of the SCP server, a file path on the server for backup files, and user credentials with read and write permissions to that path.
- If you want to include external NSO data in the backup process, follow the instructions in Back up data using external NSO, on page 7 instead of the instructions in this topic.

Procedure

Step 1 Go to **Administration** > **Backup and Restore**.

Step 2 Configure the SCP backup server destination:

a) Click **Destination**.
b) In the **Add Destination** dialog box, enter the hostname, port, destination path, and credentials for the SCP server.
c) Click **Save** to confirm the configuration.

Step 3 Create a backup job:

a) Click **Actions** > **Data Backup**.
b) In the **Data Backup** dialog box, Provide a relevant name in the **Job name** field.
c) (Optional) Check the **Force** checkbox to create the backup despite any application or microservice issues.
d) (Optional) Uncheck the **Backup NSO** checkbox if you do not want to include external NSO data in the backup.

To use the **Backup NSO** option, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. This option is not applicable for single VM deployments.

e) Complete any remaining fields as needed. To specify a different remote server upload destination, edit the **Host name**, **Port**, **Username**, **Password**, and **Path** fields.
f) (Optional) Click **Verify backup readiness** to confirm sufficient resources for the backup. If successful, click **OK** to acknowledge the warning about the operation's duration.
g) Click **Backup** to start the backup.

Step 4 Monitor the backup progress in the **Job details** panel.

The system creates a backup job set and adds it to the job list. The **Job details** panel reports the status of each backup step.

If the backup fails during upload to the remote server, investigate and resolve the issue (e.g., incorrect credentials, invalid destination directory, or lack of space). Then, in the **Job details** panel, click the **Upload backup** button to retry the upload.

The system creates and uploads a backup to the specified SCP destination. The backup job appears in the job list with status detail.

What to do next

Keep the build versions and backup files in a safe location for future restores.

Restore data

This task describes how to perform a data restore operation from the Crosswork Network Controller UI.

The time taken for the restore process varies based on the type of backup, your cluster size, and the applications in the cluster.

Before you begin

Before you begin:

- Ensure you have a backup file available for restore.
- You must install the exact build versions of the applications that were present when the backup was created. Any mismatch can result in data loss and failure of the data restore job.

Procedure

Step 1 Go to **Administration** > **Backup and Restore**.

Step 2 Select the backup file for restore:

a) In the **Backup and Restore Job Sets** table, select the data backup file you want to use for the restore. The **Job details** panel displays information about the selected backup file.
b) Click the **Data restore** button to start the restore operation.

Step 3 Monitor the restore progress:

The system creates a restore job set and adds it to the job list. To view the progress, click the link to the progress dashboard.

Attention
If MDT (Model-driven Telemetry) collection jobs were deleted after the backup, the restore operation will fail to recover them, leaving them in an error state due to missing device configurations. To rectify this, perform ONE of the following actions:

- Restore the backup taken for external NSO (only applicable if the original backup included 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, restoring the backup file may result in stale certificate expiry alarms. These alarms must be manually cleared.

The system initiates the restore operation from the selected backup file. The restore job appears in the job list with status detail.

Restore data after a disaster

Use this task when the original Cisco Crosswork cluster has been destroyed due to a natural or human-caused disaster. A new cluster must be deployed with the same configuration as the original before restoring data.

Before you begin

Before you begin:

- Obtain the full name of the backup file from the SCP backup server (typically the most recent backup). Backup filenames follow this format: `backup_JobName_CWVersion_TimeStamp.tar`.
  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the platform version of the backed-up system.
  - *TimeStamp* is the date and time when backup file was created.

  Example: `backup_Wednesday_7-2_2026-01-25-12-00.tar`.
- Ensure the new cluster uses the exact versions of all applications and the platform as the original cluster. Any mismatch can cause data loss or restore failure.
- Use the same IP addresses, number and types of nodes, and software image as the original cluster. Internal certificates depend on these details.
- Keep backups current. If you installed new applications or patches since the last backup, create a new backup.
- If only a single hybrid node or one or more worker nodes are malfunctioning, do not perform disaster recovery. Use cluster management features to replace or redeploy these nodes. If multiple hybrid nodes are malfunctioning and the system is nonfunctional, deploy a new cluster and restore using a recent backup.

- Smart licensing registration for applications is not restored and must be registered again after the restore.
- If recovery fails, contact Cisco Customer Experience for assistance.
- After restore, use the Configuration Database CLI tool to identify and reload any missing SR policies or RSVP-TE tunnels. See Orphaned SR-TE policies and RSVP-TE tunnels, on page 12 for more details.

Procedure

Step 1 Deploy a new cluster as described in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

Step 2 From the main menu, go to **Administration** > **Backup and Restore**.

Step 3 Click **Actions** > **Data Disaster Restore** to open the **Data Disaster Restore** dialog.

Step 4 In the **Backup File Name** field, enter the backup file name to restore.

Step 5 Click **Start Restore**.

To monitor progress, use the progress dashboard link.

The new cluster restores its data from the specified backup file. The configuration and data state return to the point of the last backup.

What to do next

- Re-register smart licensing for all restored applications.
- Use the Configuration Database CLI to identify and reload any missing SR policies or RSVP-TE tunnels.

Back up data using external NSO

Create a backup of your Crosswork data, optionally including the NSO CDB, to a remote SCP server.

Backing up Crosswork and NSO data ensures you can recover configurations in case of system issues. NSO backups can be automated, but restoring the NSO CDB is a manual process. For restore instructions, see Restore data using an external NSO, on page 9.

Before you begin

Ensure that you:

- Install a compatible version of NSO in system default mode.
- Install 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 7.2 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/
```

- Collect the hostname or IP address, port number, and file path for your SCP server.
- Ensure you have SCP server credentials with read and write access to the backup folder.
- Configure SSH as the connectivity protocol in the NSO provider, with an appropriate credential profile.
- Ensure the user associated with the credential profile has sudo permissions and full access to `/var/opt/ncs/backups/` on the NSO server.
- See general backup guidelines in Back up data, on page 4 for additional requirements.

Note If any prerequisite is not met, the backup job may fail.

Procedure

Step 1 Configure the SCP backup server.

a) Go to **Administration** > **Backup and Restore**.
b) Select **Destination** and enter the required backup server details.
c) Click **Save** to confirm the configuration.

Step 2 Create a backup job for Crosswork and external NSO data.

a) In **Administration** > **Backup and Restore**, select **Actions** > **Backup**.
b) Enter a job name in the **Job Name** field.
c) (Optional) Select **Force** to allow backup if there are application or microservice issues.
d) Ensure **Backup NSO** is checked.
e) Complete remaining fields as needed. To change the upload destination, edit the **Destination** settings.
f) Click **Start Backup** to begin the operation.

Step 3 Monitor the backup job.

a) View the job in the **Backup Restore Job Sets** table. Click on the job set to see status and details in the **Job Details** panel.
b) If an upload to the SCP server fails, click **Upload backup** in the **Job Details** panel to retry. To change the destination, edit **Destination** settings before retrying.

A backup of Crosswork and (optionally) NSO data is created and stored on the SCP server. The job status and any errors are displayed in the Job Details panel.

What to do next

- For restoration, see Restore data using an external NSO, on page 9.
- Review backup jobs to confirm successful completion.

Restore data using an external NSO

Restore a Crosswork cluster and its associated NSO from a backup file located on an SCP server.

Use this task to recover your Crosswork cluster and NSO in the event of data loss or system migration. Perform this operation during a scheduled maintenance window only. Do not allow users to access Crosswork or NSO while the restore is in progress. The operation may be lengthy and will pause other Crosswork applications until complete. NSO must be completely stopped during the restore process.

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

Before you begin

Before you begin:

- Obtain the full name of the backup file from the SCP backup server (typically the most recent backup). Backup filenames follow this format: `backup_`*`JobName`*`_`*`CWVersion`*`_`*`TimeStamp`*`.tar`.
  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the platform version of the backed-up system.
  - *TimeStamp* is the date and time when backup file was created.

  Example: `backup_Wed_7-2_2026-01-25-12-00.tar`.
- Ensure that NSO is not running before you begin the restore operation.

Procedure

Step 1 Log in to the remote SCP backup server. Access the backup destination directory and locate the backup file containing external NSO information.

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_7-2_2026-01-25-12-00.tar
```

Step 2 Extract the NSO backup from the main backup file using `tar -xvf`.

```
[root@localhost~]# tar -xvf ackup_Wed_7-2_2026-01-25-12-00.tar
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_7-2_2026-01-25-12-00.tar
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar
```

Step 3 Extract the NSO backup file in the destination folder.

This will create a folder structure under `/nso/ProviderName/`, where *ProviderName* is the configured NSO provider name.

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.

Step 5 Log in to NSO as a user with root privileges. Copy or move the generated NSO backup file from the SCP server to the restore path location of the NSO cluster.

```
[root@localhost nso121]# more NSO_RESTORE_PATH_nso121/var/opt/ncs/backups/

[root@localhost nso121]# 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 Stop NSO before starting the restore operation.

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

Step 7 Restore NSO using the backup file.

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

If you encounter issues running this command, ensure you have `sudo su` permission.

Step 8 Restart NSO after the restore completes.

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

Step 9 Re-add the NSO provider to Crosswork after restoring both Crosswork and NSO clusters from backups.

Complete the NSO configuration to ensure provisioning services function properly. For more information, see Add a Cisco NSO provider.

The Crosswork and NSO clusters are restored from backup and ready for continued operation. Services and provisioning can now resume as normal.

What to do next

- Verify that all NSO provisioning services are operational.
- Complete any additional configuration as required for your deployment.

Migrate data using backup and restore

Migrate your data to a new installation or software version using backup and restore operations.

Use this task when upgrading your Crosswork installation to a new software version or moving data to a new installation. Data migration using backup and restore ensures that your configuration and operational data are preserved during transition. Perform these actions during a scheduled maintenance or upgrade window, and ensure users do not access the system during migration.

Before you begin

Before you begin, ensure you have:

- Configured a destination SCP server for storing data migration files (a one-time setup).
- 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 SCP server.
- Ensured that the Crosswork cluster and SCP server use the same IP environment (IPv4 or IPv6 as required).
- Captured a screenshot of Data Gateways and recorded their assigned IP addresses and names for redeployment.

Procedure

Step 1 Configure the SCP backup server as your migration destination.

a) In the Crosswork UI, go to **Administration > Backup and Restore**.
b) Open **Destination** and enter the required server details.
c) Save the backup server configuration.

Step 2 Create a migration backup.

a) Log in as an administrator to the Crosswork installation you want to migrate.
b) Go to **Administration > Backup and Restore**.
c) Select **Actions > Data backup** and enter the necessary details, including a job name for the backup.
d) (Optional) Select **Force** to allow backup in case of application or microservice issues.
e) Complete any remaining required fields and adjust the destination if needed.
f) Start the backup operation.
g) Monitor backup progress in the **Backup and Restore Job Sets** table. Review job status and details as needed.
h) If the upload fails, retry using **Upload backup**. Update the destination if required before retrying.

Step 3 Migrate the backup to the new installation.

a) Log in as an administrator on the target Crosswork installation.
b) Go to **Administration > Backup and Restore**.
c) Select **Actions > Data migration** and enter the backup file name to restore from.
d) Click **Start migration**. Monitor progress in the job list or dashboard.

Step 4 Deploy and verify Crosswork Data Gateways.

a) Log out and log in to the Crosswork UI at `https://<new_crosswork_ip>:30603`. Acknowledge the **Action to be taken** pop-up after redeploying Data Gateways.
b) Delete old Data Gateway VMs and install new gateways with identical IPs and names as previously recorded.
c) Verify that each Data Gateway is deployed and registered with Crosswork.
d) Check Data Gateway status in **Administration > Data Gateway Management > Virtual Machines**. Ensure **Operation** and **Administration** state are UP.
e) After all gateways are active, confirm pool migration at **Administration > Data Gateway Management > Pools** and that Data Gateways are automatically enrolled.
f) Log out and log back in again to Crosswork UI to trigger the **Action to be taken** pop-up, then click **Acknowledge** to complete migration.

   Do not use browser history links with a child path to access the UI; this prevents the pop-up from appearing.

g) If NSO is set to read-only mode, disable it.

Data and configuration are successfully migrated to the new Crosswork installation. Data Gateways are redeployed and operational in the target environment.

What to do next

- Verify all migrated services and Data Gateways are operational.
- Go to **Device Management** > **Network Devices** and ensure that all devices are reachable and all the nodes are active. Then, select **Actions**, and choose **Detailed sync all devices**.

  This initiates a synchronization of all devices, ensuring their configurations and operational status reflect the most recent migration.
- Perform any required post-migration configuration.

Orphaned SR-TE policies and RSVP-TE tunnels

An orphaned SR-TE policy or RSVP-TE tunnel is a network path instance that:

- is initiated by the PCE within Crosswork Network Controller after the most recent cluster data synchronization,
- is not included in the current HA data set, and
- cannot be modified through the user interface until properly synchronized.

Additional reference information

- Orphaned policies and tunnels may appear after a cluster HA switchover or a backup/restore operation.
- Crosswork Network Controller displays an alarm when orphaned TE policies or RSVP-TE tunnels are detected (**Alerts** > **Alarms and Events**).
- You can view details of orphaned policies/tunnels, but cannot modify them until they are properly synchronized.

How to manage orphaned policies and tunnels

Crosswork Network Controller provides APIs to help clear orphans. To list orphaned SR-TE policies or RSVP-TE tunnels, use the following:

- **cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** (for SR-TE policies)
- **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** (for RSVP-TE tunnels)

Set **is-orphan=True** and use the GET action to retrieve the list. To make orphaned items manageable again, use the SAVE action for the corresponding policy or tunnel type.

Counter-examples

SR-TE policies or RSVP-TE tunnels that were synchronized before the last cluster data sync are not considered orphaned.

References

For more information, see API documentation on Devnet (**API Reference** > **Crosswork Optimization Engine**).

Crosswork Data Gateway disaster recovery scenarios

A disaster recovery scenario is a operational scenario that:

- addresses the re-establishment of Crosswork Data Gateway services after a system-wide disaster,
- involves steps that may vary depending on the number and types of Data Gateway VMs present, and
- determines whether additional manual procedures are required if Data Gateway VMs were deleted during the disaster.

Types of disaster recovery scenarios

- When all active and standby Data Gateway VMs in a pool have the **Operational state** set to **Error** after recovery. For recovery steps, see Restore Data Gateways after a disaster (with high availability), on page 14.
- When a pool contains only one Data Gateway VM, or multiple active Data Gateway VMs in the **Error** state without any standby VMs. For recovery steps, see Restore Data Gateways after a disaster (without high availability), on page 15.

Additional information

The disaster recovery process for Cisco Crosswork Network Controller automatically restores Data Gateway services in most cases. Manual procedures are only required if Data Gateway VMs have been deleted from the system during the disaster.

Restore Data Gateways after a disaster (with high availability)

Restore a Data Gateway pool with active and standby VMs after a disaster event, ensuring high availability and continued data collection.

Use this task after a disaster, when a Data Gateway pool with high availability is in the **Error** state and Cisco Crosswork disaster recovery is complete. This procedure returns the pool and devices to normal operation.

Before you begin

Before you begin:

- Complete the Cisco Crosswork disaster recovery operation.
- Ensure Crosswork data is restored and all pods are healthy and operational.
- Do not redeploy Data Gateways until Crosswork is fully restored.

Procedure

Step 1 Install new Data Gateway VMs using the same profile, hostname, and management interface as before the disaster.

The newly installed Data Gateway VMs will appear in the **Error** state because Crosswork restores data from the old VMs.

Step 2 Log in to Cisco Crosswork.

Step 3 Navigate to the **Administration > Data Gateway Management > Pools** page (or the equivalent for your environment).

Step 4 Select and edit the pool. Remove (unassign) the standby VM from the pool.

Step 5 Change the **Administration State** of the standby VM to **Maintenance** mode.

Note
If you redeploy the Data Gateway without first moving it to **Maintenance** mode, enrollment with Crosswork fails and errors appear in the logs. To resolve, switch to **Maintenance** mode or manually re-enroll the 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 4–6 to restore the (now) standby VM that is still in the **Error** state.

Step 8 Verify the following:

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

The Data Gateway pool is restored with high availability, and normal operation of devices and collection jobs resumes.

What to do next

- Monitor Data Gateway and device status to ensure continued normal operation.
- Address any remaining error states by reviewing logs or following troubleshooting procedures.

Related Topics

Change the Administration State of a Data Gateway
Attach devices to a Data Gateway
Detach devices from a Data Gateway
Device assignment management
Edit a Data Gateway pool
Re-enroll Crosswork Data Gateway

Restore Data Gateways after a disaster (without high availability)

Restore Data Gateway VMs and pools after a disaster in environments without high availability, so that device management and data collection can continue.

Use this task when you lose a Data Gateway VM during a disaster and your deployment does not use high availability. Choose the recovery option that fits your situation: replacing a VM, detaching or moving devices, or adding a standby VM. Each option restores device management and data collection capabilities.

Before you begin

Before you begin:

- Complete the Cisco Crosswork disaster recovery operation.
- Ensure all Data Gateway VM and pool information is restored and available in Cisco Crosswork.

Procedure

Step 1 Replace a lost Data Gateway VM with a new VM (same configuration as the original).

a) Log in to Cisco Crosswork and go to **Administration** > **Data Gateway Management** > **Data gateways**.
b) Delete the existing pool associated with the lost VM.
c) Set the Administration State of the VM to Maintenance.
d) Install a new Data Gateway VM with the same profile, hostname, and management interface as the lost VM.
e) Set the Administration State of the VM to Up.

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

f) Create a new pool with the same name as the original, and add the VM to this pool.

Verify the Data Gateway has Operational State as Up.

g) Attach devices to the Data Gateway as needed.
h) Verify that collection jobs are running as expected.

Step 2 Detach devices or move devices to another operational Data Gateway.

a) Log in to Cisco Crosswork and go to **Administration** > **Data Gateway Management** > **Data gateways**.
b) Detach devices from the affected VM or move devices to another Data Gateway that is Operational State Up.

c) Delete the existing pool. (Note: This action does not unassign the VM from the pool; it will still appear assigned.)
d) Set the Administration State of the VM to Maintenance.
e) Reboot the VM to unassign it from the pool.

After reboot, the VM enrolls with Cisco Crosswork automatically. Wait about 5 minutes, then verify the VM is administratively Up and in Not Ready state.

Note
You can also manually re-enroll the VM from the Interactive Console of the Data Gateway VM, if required.

f) Create a new pool with the same name and add the VM.
g) Verify Data Gateway has Operational State as Up.
h) Reattach devices or move devices back to this Data Gateway as needed.
i) Verify that collection jobs are running as expected.

Step 3 Add a standby VM to the pool (restore a pool with only one active VM or multiple VMs without standby).

Note
To restore multiple active VMs in a pool without standby VMs, repeat these steps for each active VM.

a) Install a new Data Gateway VM.
b) Log in to Cisco Crosswork and go to **Administration** > **Data Gateway Management** > **Pools**.
c) Add the new VM to the pool.

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

d) Edit the pool, remove the now-standby VM, and set its Administration State to Maintenance.

After about 5 minutes, the standby VM enrolls with Cisco Crosswork automatically and should be operationally Up and in Not Ready state.

Note
You can manually re-enroll the VM if necessary from the Interactive Console of the Data Gateway VM.

e) Add the standby VM back to the pool. Verify both active and standby VMs are operationally Up.
f) Verify the following:

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

Data Gateways and pools are restored, devices are reattached, and collection jobs resume as expected in a non-high availability deployment after a disaster.

What to do next

- Monitor Data Gateway and collection job status to confirm normal operation.
- Review logs and troubleshoot if any VM remains in Error or Not Ready state.

Related Topics

Change the Administration State of a Data Gateway
Attach devices to a Data Gateway

Detach devices from a Data Gateway
Device assignment management
Edit a Data Gateway pool
Re-enroll Crosswork Data Gateway