Manage Backups

This section contains the following topics:

Manage Cisco Crosswork Backup and Restore

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

Crosswork offers multiple ways to perform a backup:

1. **Backup:** Preserves the Crosswork configuration
2. **Data Backup:** Preserves the data only. Application binaries are not backed up.
3. **Backup with NSO:** Preserves NSO data along with the Crosswork configuration.

The process for the first and second options (**Backup** and **Data Backup**) are mostly similar and is explained in this topic. The third option (Backup with NSO) is explained in detail in Backup Cisco Crosswork with Cisco NSO, on page 6.

Attention

- Bulding 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.
- If you are making a **Data Backup**, note down the build version of the installed applications in your cluster. Before performing the **Data Restore**, the exact versions of those applications must be installed and available in your cluster. Any mismatch in the build versions of the applications can result in data loss and failure of the data restore job.

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

- 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.
- 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 normal restore, Cisco Crosswork applications and data are restored to the same version as when you took the backup. When performing a *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 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.
- To save space on your backup server, you may delete older backups, but they will 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, 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.

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.
- If you are making a data backup, note down 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** > **Backup** to display the **Backup** dialog box with the destination server details prefilled.

Note To create a Data Backup, click **Actions** > > **Data Backup**. The rest of the procedure in Step 2 remains the same.

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 6 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.

If the upload failed due to problems with the remote server, either fix the issue with the remote server (for example, clean old backups to free up space) or use the **Destination** button to specify a different remote server and path before clicking **Upload backup**.

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 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 **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.

Note The procedure to restore a data backup is similar. Select the data backup file in the **Backup and Restore Job Sets** table. With the data backup file selected, click the **Data Restore** button shown on the **Job Details** panel to start the data restore operation.

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 the *Cisco Crosswork Infrastructure and Applications Installation Guide*.

If your cluster only has one malfunctioning hybrid node, or one or more 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 disaster recovery, note the following:

- 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.
- If you have made a data backup (**Actions** > > **Data Backup)** instead of a full backup, you can perform a **Data Disaster Restore** which is quicker than a regular disaster restore. 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.
- 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 from the SCP backup server the full name of the backup file you want to use in your disaster recovery. 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 **To perform a disaster restore:**

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

Step 3 **To perform a data disaster restore:**

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

Step 4 In the **Backup File Name** field, enter the file name of the backup from which you want to restore.

Step 5 Click **Start Restore** to initiate the recovery operation.

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

Resolve Missing SR-TE (SR-MPLS and SRv6) Policies and RSVP-TE Tunnels

The information in this topic is applicable only when Cisco Crosswork Optimization Engine is installed.

The Configuration Database contains all SR-TE policies and RSVP-TE tunnels of which Cisco Crosswork is aware. Cisco Crosswork updates the Configuration Database whenever you provision, modify or delete an SR-TE policy or RSVP-TE tunnel. You can use the Configuration Database CLI tool to do the following:

- Read and write CSV files to the Configuration Database.
- Populate SR-TE policy and RSVP-TE tunnel information from the Configuration Database to create a CSV file.

The Configuration Database CLI tool is especially useful when trying to recover missing SR-TE policies and RSVP-TE tunnels after a restore operation. For example, the `--dump-missing` option produces a CSV file which lists the SR-TE policies and RSVP-TE tunnels that are missing. Use this CSV file to determine which

SR-TE policies and RSVP-TE tunnels are missing. Then load them back into the topology using the `--load` option. See the CLI tool help for more information.

Step 1 Enter the **optima-pce-dispatcher** container:

```
kubectl exec -it optima-pce-dispatcher-XXXXXXX-XXXX bash
```

Step 2 You can run the following commands:

a) Show CLI tool help text.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --help
```

b) Save all SR-TE policies and RSVP-TE tunnels that are in the Configuration Database to a CSV file.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --dump /<PathToFile>/dump_file.csv
```

c) Load the contents from the provided CSV file and write policies to the Configuration Database.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --load /<PathToFile>/load_file.csv
```

Note This command overwrites any duplicate SR-TE policies or RSVP-TE tunnels that it finds, and adds only valid TE tunnels to the Configuration Database. Duplicate SR-TE policies have the same combination of headend, endpoint, and color. Duplicate RSVP-TE tunnels have the same combination of headend and tunnel name.

d) After the CSV load completes, synchronize the Cisco Crosswork Optimization Engine UI with the Configuration Database by restarting Optimization Engine, as follows:

1. From the main menu, select **Administration** > > **Crosswork Manager** > **Crosswork Health** > **Optimization Engine**.
2. Select **optima-ui-service** > > **Action** > **Restart**. Restart takes approximately five minutes.

e) After the restart, compare SR-TE policies and RSVP-TE tunnels that are currently in the topology with the Configuration Database contents. Save the missing SR policies and RSVP-TE tunnels to a CSV file. You can then use this CSV file and the following command to load the missing policies into the Configuration Database:

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py -dump-missing /<PathToFile>/dump_file.cs
```

Backup Cisco Crosswork with Cisco NSO

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

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:

- The NSO provider configuration includes an SSH connection. If you don't enable SSH on the provider, Cisco Crosswork displays a warning alarm. Cisco Crosswork creates a backup for its own data, but not for NSO.
- The NSO provider's credential profile contains the user ID and password of a user with `sudo` privileges on the NSO server.
- 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 NSO server has Python version 3.x installed, and the user in the credential profile for the NSO provider can execute `python3` 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 1 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 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 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.
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.

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 cluster 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.
- You can run both a Cisco Crosswork and a Cisco NSO restore operation at the same time.

Before you begin

Get from the SCP server the full name of the backup file you want to restore. 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 pre-requisite when upgrading your Cisco Crosswork installation to a new software version, or moving your existing data to a new installation.

As with normal backups, 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.

Before you begin

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 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) 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** > **Backup** to display the **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.