Upgrade to Geo Redundancy Solution

This chapter contains the following topics:

Upgrade from Crosswork Network Controller 5.0 to 6.0 (Geo Redundant)

This topic explains the high level description of the tasks necessary to upgrade from Crosswork Network Controller version 5.0 to version 6.0 (geo redundant enabled).

Note Any day N activity will yield the system ineligible to migrate to a geo redundant solution. You will need to re-install the Crosswork cluster to enable geo redundancy.

Table 1: Upgrade from Crosswork 5.0 to 6.0 Geo Redundancy (Day 0)

Step	Action
1. Convert single instance NSO to NSO HA	Follow the instructions in Convert Single Instance NSO to NSO HA, on page 2 topic. **Note** Crosswork Network Controller 6.0 supports NSO version 6.1.4. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation.
2. Deploy SR-PCE	Deploy SR-PCE in a Point of Presence (PoP) site closer to the Crosswork's Availability Zone. For more information, refer to the relevant install instructions in the Cisco IOS XRv 9000 Router Installation Guide. **Note** Crosswork Network Controller 6.0 supports IOS XR 7.11.1.

Step	Action
3. Create backup of the Crosswork 5.0 cluster.	Follow the instructions in Create Backup of the Cisco Crosswork Cluster, on page 3 topic.
4. Shut down the Crosswork 5.0 cluster	Shut down the Cisco Crosswork 5.0 cluster by powering down the VMs hosting each node (start with the Hybrid VMs). **1.** Gather following information before shutting down the cluster. • All IP addresses of the cluster. • All IP addresses of the Crosswork Data Gateways **2.** Shut down the VMs of the Crosswork cluster. For vcenter shutdown all the VMs using vcenter UI **3.** Log into the VMware vSphere Web Client. In the **Navigator** pane, right-click the VM that you want to shut down. **4.** Choose **Power** > **Power Off**. Wait for the VM status to change to **Off**. **5.** Wait for 30 seconds and repeat the steps for each of the remaining VMs. **6.** (Optional) Put NSO in read-only mode using `ncs_cmd -c maapi_read_only` command.
4. Install the Crosswork Network Controller 6.0 cluster and applications.	Follow the instructions in Install the Cisco Crosswork 6.0 Cluster and Applications, on page 5 topic.
5. Perform the migration.	Follow the instructions in Run Migration, on page 6 topic.
6. Install the standby cluster and enable geo redundancy solution.	Follow the instructions in Install the Standby Cluster and Enable Geo Redundancy, on page 7 topic.
7. Upgrade Crosswork Data Gateway 5.0 to 6.0 (geo Redundant)	Follow the instructions in Upgrade Crosswork Data Gateway 5.0 to 6.0 Geo Redundancy, on page 8 topic.
8. Update the providers.	Follow the instructions in Update Providers, on page 9 topic.
9. Complete the geo enablement operation.	Follow the instructions in Complete Geo Redundancy Enablement, on page 9 topic.

Convert Single Instance NSO to NSO HA

This topic explains the procedure to convert a single instance NSO to NSO HA (High Availability). For detailed instructions, please refer to the NSO Administration Guide on HA.

Attention Make a backup and upgrade your NSO setup to the compatible version before executing the below steps.

Follow the below guidelines to create a HA setup from a standalone NSO.

Step 1 Determine the High Availability topology to follow: L2 or L3
Step 2 Make a backup of the original NSO system.
Step 3 Clone the original NSO to a new instance.
Step 4 Install the hcc package on both nodes.
Step 5 Configure the high availability and hcc as per the selected network topology.
Step 6 Request to enable high availability on both nodes.
Step 7 Verify the changes made.

Create Backup of the Cisco Crosswork Cluster

Creating a backup is a prerequisite when upgrading your current version of Cisco Crosswork to a new version.

Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Cisco Crosswork while the backup operation is running.

Before you begin

Follow these guidelines whenever you create a backup:

- Cisco Crosswork will back up the configuration of the system to an external server using SCP. Before you begin you need to have the following configuration in place and information about the SCP server available:
  - The hostname or IP address and the port number of a secure SCP server.
  - A preconfigured path on the SCP server where the backup will be stored.
  - User credentials with file read and write permissions to the directory.
  - The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
- Ensure that you have configured a destination SCP server to store the backup files. This configuration is a one-time activity.
- After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.
- 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.
- Keep a record of the list of Crosswork applications you have installed in the current version of Cisco Crosswork, as you can only install those applications after migrating to the new version of Cisco Crosswork.

- If you have onboarded a custom MIB package in the current version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete migrating to new version of Cisco Crosswork.
- If you have modified the current version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to the new version of Cisco Crosswork. The device configuration file is located on the cluster node (at `/mnt/cw_glusterfs/bricks/brick3/sys-oids.yaml`) and on the pod (at `/mnt/backup/sys-oids.yaml`).
- If Cisco Crosswork Optimization Engine has feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) that are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM or BWOpt (**Traffic Engineering > Local Congestion Mitigation > Domain Identifier <domain_id> > Interface Thresholds > Export** OR **Traffic Engineering > Bandwidth Optimization > Interface Thresholds > Export** icon).

Step 1 Login to the Crosswork UI by navigating to https://<VIP>:30603.

The VIP refers to the Management Virtual IP of the cluster.

Step 2 Check and confirm that all the VMs are healthy and running in your cluster.

Step 3 **Configure an SCP backup server:**

a) From the Cisco Crosswork 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 4 **Create a backup:**

a) From the Cisco Crosswork 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 any of the VMs or applications are not in **Healthy** state, but you want to create the backup, check the **Force** check box.

Note The **Force** option must be used only after consultation with the Cisco Customer Experience team.

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** section in the *Cisco Crosswork Network Controller 6.0 Administration Guide* 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 verifications are successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.

If the verification is unsuccessful, please contact the Cisco Customer Experience team for assistance.

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.

Note You can also perform a data backup (backup using rest-api). The data backup is faster as it does not include application binaries. To perform, do the following:

- Get JWT (using sso apis)
- API to take the data backup (https://<VIP>:30603/crosswork/platform/v1/platform/backup/dataonly)
- Payload for the api {"jobName": "jobname","force": false}

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 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.

Note After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.

Note If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

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 Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task **`uploadBackupToRemote`**). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Install the Cisco Crosswork 6.0 Cluster and Applications

This install the latest version of the Cisco Crosswork cluster and applications.

Important While the cluster installation is in progress, you must upgrade your NSO setup to the compatible version. Please monitor actively to ensure that the NSO leader is in the same site as Crosswork.

Before you begin

- Make sure that your environment meets all the installation prerequisites (see Installation Prerequisites for VMware vCenter).

Step 1 Install Cisco Crosswork 6.0 cluster (see Install Crosswork Cluster on VMware vCenter) using the same IP addresses and same number of nodes as in old cluster.

Step 2 After the installation is completed, log into the Cisco Crosswork UI (using https://<VIP>:30603) and check if all the nodes are up and running in the cluster.

Step 3 Install the Cisco Crosswork applications which were installed in the old cluster. Ensure that you install the latest versions that are compatible with the 6.0 cluster. For installation instructions, please refer to the Install Crosswork Applications chapter.

Note The applications binaries and versions are not updated in the migration job.

Step 4 After the applications are successfully installed, check the health of the new Cisco Crosswork cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Run Migration

After successfully installing the new versions of the Cisco Crosswork applications, proceed to migrate the Cisco Crosswork backup taken earlier to the new Cisco Crosswork cluster.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure destination SCP server used in Create Backup of the Cisco Crosswork Cluster, on page 3.
- The name and path of the backup file created in Create Backup of the Cisco Crosswork Cluster, on page 3.
- User credentials with file read and write permissions to the directory.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 **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.

c) Make the relevant entries in the fields provided.

Note In the **Remote Path** field, please provide the location of the backup created in Create Backup of the Cisco Crosswork Cluster, on page 3.

d) Click **Save** to confirm the backup server details.

Step 3 **Migrate the previous Cisco Crosswork backup on the new Cisco Crosswork cluster:**

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

b) Click **Actions** > **Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.

c) Provide the name of the data migration backup (created in Create Backup of the Cisco Crosswork Cluster, on page 3) in the **Backup File Name** field.

d) If you want to perform the data migration backup despite any Cisco Crosswork application or microservice issues, check the **Force** check box.

e) Click **Start Migration** to start the data migration operation. Cisco Crosswork creates the corresponding data migration 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.

Note If you do not see your job in the list, please wait for a few minutes and refresh the **Backup and Restore Job Sets** table.

f) To view the progress of a data migration 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.

Note Crosswork UI might become temporarily unavailable during the data migration operation. When the Crosswork UI is down, you can view the job status in the Grafana dashboard. The Grafana link is available as *View Data Migration Process Dashboard* option on the right side of the Job Details window.

g) If the data migration fails in between, you need to restart the procedure from step 1.

Step 4 After the data migration is successfully completed, check the health of the new Cisco Crosswork cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Install the Standby Cluster and Enable Geo Redundancy

After completing the migration on the active cluster, install the standby cluster and enable geo redundancy.

Note When you are enabling geo redundancy after the 5.0 to 6.0 migration, you must set the following flag in the inventory file:

```
## install
is_post_migration_activation: true
```

Step 1 In the second site, install the standby cluster. For more information, refer to the installation instructions in Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool or Manual Installation of Cisco Crosswork using vCenter vSphere UI.

Step 2 Install the applications (that were installed on the active cluster) on the standby cluster.

Note Migration is not required in the standby cluster, as the changes would be taken from the active cluster during the periodic sync operation.

Step 3 Ensure DNS connectivity on both sites. Perform DNS server update on both sites if needed to ensure that Crosswork cluster is using the right DNS server.

Step 4 Ensure unified cross cluster endpoint is resolved on *site 1* (active site).

Step 5 Create and upload the inventory file on *site 1* to create the active cluster, and verify the operation. For more information, refer to the instructions in Enable Geo Redundancy.

Upgrade Crosswork Data Gateway 5.0 to 6.0 Geo Redundancy

This topic explains the procedure to upgrade from Crosswork Data Gateway version 5.0 to version 6.0 (geo redundant enabled).

For the 6.0 Crosswork Network Controller release, it is mandatory to deploy Crosswork Data Gateway using the FQDN. When Crosswork undergoes an upgrade, the existing data gateways transition to the ERROR state because of their enrollment using the VIP address, resulting in a discrepancy in the enrollment information.

To install Crosswork Data Gateway after an upgrade:

Before you begin

Ensure that you are aware of the following:

- After Crosswork is upgraded, the data gateways, virtual data gateways, HA pool, and device-mapping configuration are restored.
- The Data Gateway Manager automatically assigns the active Crosswork site as the default site for all existing data gateways.

Step 1 Redeploy the Crosswork Data Gateway instance by removing the old instance and replacing it with a new installation. During the redeployment, use the unified management FQDN for ControllerIP in the OVF deployment script.

For information on removing a data gateway instance, see Delete Crosswork Data Gateway from the Crosswork Cluster and installing a new instance, see Install Geo HA Crosswork Data Gateway.

If the data gateways are redeployed using the same name and hostname attribute provided in the OVF script, the Data Gateway Manager considers them as existing gateways and automatically enrolls them with the upgraded Crosswork during the migration process.

Important It is recommended to initiate a sync operation to enhance the accuracy of the data after the addition of a new device or the deployment of a new gateway. See Configure Cross Cluster Sync Settings for information on how to perform a sync operation.

Step 2 Modify the high availability Crosswork Data Gateway pools as following:

- If a new data gateway instance is added to a high availability pool from the Standby site, which is currently the Active site, and a switchover occurs. The data gateway's role changed from Spare to Assigned.
- By default, the existing pools will be tagged as imbalanced, as there are no data gateways connected to the standby site. For preserving the data gateway balance, deploy new data gateways on the standby site.
- The SBConfig is configured to the Shared option. You must configure it to be Site-specific.
- Configure the VIP or FQDNs for the standby site.

Step 3 Accept an upgrade acknowledgment message that appears on the Crosswork UI when all the data gateways with the Assigned role are in the UP state and the Spare gateways in the NOT_READY state.

Data gateways with the Assigned role start the data collection.

What to do next

If the data gateways cannot connect with the Active cluster, re-enroll the gateway from the interactive menu. See the *Re-enroll Crosswork Data Gateway* section in the *Cisco Crosswork Network Controller 6.0 Administration Guide* for more information.

Update Providers

After enabling geo redundancy on the active cluster, update the providers.

Note Skip this step if you are not planning to enable geo redundancy.

Step 1 Add the RBAC JWT token on the Cisco NSO VMs.

Step 2 Upload and update the JWT package on the Cisco NSO High Availability VMs.

Step 3 Reload the NCS packages on both VMs.

Step 4 Update the **JWT auth file** with *geo-CW FQDN cnc-host* value on both VMs.

Step 5 Update the *cert.pem* on both VMs.

Step 6 Update NSO with unified cluster endpoint in the **Manage Providers** window.

Step 7 (Optional) Update SR-PCE IP address in the **Manage Providers** window.

Step 8 (Optional) While upgrading from a non-HA setup to geo redundant mode, Crosswork Data Gateway will end with multiple VIPs for southbound devices. These devices need to be set up for syslogs, traps and MDT. In case of MDT, you can use admin DOWN/UP to push the configuration changes to the devices.

Note Any other external destination needs to be in HA mode with its own unified endpoint in the form of VIP or FQDN.

Complete Geo Redundancy Enablement

After updating the providers, activate geo redundancy on the standby cluster.

Note Skip this step if you are not planning to enable geo redundancy.

Step 1 Create and upload the cluster inventory file on site 2, to create the standby cluster. Verify the operation. For more information, refer to the instructions in Enable Geo Redundancy.

Step 2 Configure the cross cluster settings. For more information, see step 7 in the Geo Redundancy Workflow (Day 0) topic.

Step 3 Perform a on-demand sync to sync the data from active to standby cluster.