



Upgrade to Geo Redundancy Solution

This chapter contains the following topics:

- [Upgrade from Crosswork Network Controller 7.0.x \(non-geo redundant\) to 7.1 \(geo redundant\), on page 1](#)
- [Upgrade from Crosswork Network Controller 7.0.2 \(geo redundant\) to 7.1 \(geo redundant\), on page 13](#)

Upgrade from Crosswork Network Controller 7.0.x (non-geo redundant) to 7.1 (geo redundant)

This topic provides a high-level description of the tasks required to upgrade from Crosswork Network Controller version 7.0.x (non-geo redundant) to version 7.1 (geo redundant).



Important 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. For more information about enabling geo redundancy on day N, see [Geo redundancy workflow \(Day N\)](#).

Prerequisites

You have installed Crosswork Network Controller version [7.0.1](#) or [7.0.2](#), including the geo-redundancy patch file. For more information about the patch releases, please refer to the corresponding release notes.

Upgrade workflow



Important While the cluster installation is in progress, you must upgrade NSO and SR-PCE. Please see the [Release Notes for Crosswork Network Controller 7.1.0](#) to know the NSO and SR-PCE versions compatible with Crosswork Network Controller. The process to upgrade NSO or SR-PCE is not covered in this document. For install instructions, please refer to the relevant product documentation.

- Cisco NSO: [Cisco NSO documentation](#)
 - Cisco SR-PCE: [Cisco IOS XRv 9000 Router Installation Guide](#).
-

Table 1: Upgrade from Crosswork Network Controller 7.0.x (non-geo redundant) to 7.1 (geo redundant) on 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 3 topic.
2. Deploy SR-PCE	<p>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.</p> <p>After you have upgraded to the compatible version of SR-PCE, configure gRPC on SR-PCE. Ensure that your credentials in the CSV file include those for a gRPC connection, which should match your SSH credentials. In your provider settings, include gRPC as a connection option for SR-PCE</p>
3. Create backup of the Crosswork 7.0.x cluster.	Follow the instructions in Create backup of the Cisco Crosswork cluster , on page 4 topic.
4. Shut down the Crosswork 7.0.x cluster	<p>Shut down the Crosswork Network Controller 7.0.x cluster by powering down the VMs hosting each node (start with the Hybrid VMs).</p> <ol style="list-style-type: none"> Gather following information before shutting down the cluster. <ul style="list-style-type: none"> All IP addresses of the cluster. All IP addresses of the Crosswork Data Gateways Shut down the VMs of the Crosswork cluster. For vcenter shutdown all the VMs using vcenter UI Log into the VMware vSphere Web Client. In the Navigator pane, right-click the VM that you want to shut down. Choose Power > Power Off. Wait for the VM status to change to Off. Wait for 30 seconds and repeat the steps for each of the remaining VMs. (Optional) Put NSO in read-only mode using <code>ncs_cmd -c maapi_read_only</code> command.
5. Install the Crosswork Network Controller 7.1 cluster and applications.	<p>Follow the instructions in Install the Crosswork Network Controller Cluster and Applications, on page 6 topic.</p> <p>After the cluster installation, ensure that the Crosswork inventory is onboarded before proceeding with the migration.</p>

Step	Action
6. Perform the migration.	Follow the instructions in Run Migration, on page 7 topic. After the migration, ensure that the Crosswork inventory is onboarded before proceeding with geo enablement.
7. Install the standby cluster and enable geo redundancy solution.	Follow the instructions in Install the standby cluster and enable geo redundancy, on page 8 topic.
8. Update the providers.	Follow the instructions in Update Providers, on page 9 topic.
9. Upgrade Crosswork Data Gateway 7.0.x to 7.1 with Geo Redundancy	Follow the instructions in Upgrade Crosswork Data Gateway 7.0 to 7.1 Geo Redundancy, on page 10 topic.
10. Configure the Controller IP for Crosswork Data Gateway	Follow the instructions in Configure Controller IP for Crosswork Data Gateway, on page 11 topic.
12. Complete the geo enablement operation.	Follow the instructions in Complete Geo Redundancy Enablement, on page 12 topic. Optionally, you can complete the geo enablement operation for a three cluster inventory (active, standby, and arbiter). In this case, the arbiter cluster is added as a day-N scenario. For more information, see Geo redundancy workflow (Day N) .

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.

Procedure

-
- 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 Crosswork Network Controller to a new version.



Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Crosswork Network Controller 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 Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller is communicating over IPv6, so must the backup server.
- 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).

Procedure

- 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:**
- From the Crosswork Network Controller main menu, choose **Administration > Backup and Restore**.
 - Click **Destination** to display the **Edit Destination** drawer panel. Make the relevant entries in the fields provided.
 - Click **Save** to confirm the backup server details.
- Step 4** **Create a backup:**
- From the Crosswork Network Controller main menu, choose **Administration > Backup and Restore**.
 - Click **Actions > Backup** to display the **Backup** drawer panel with the destination server details prefilled.
 - Provide a relevant name for the backup in the **Job Name** field.
 - 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.
 - Uncheck the **Backup NSO** checkbox if you don't want to include Cisco NSO data in the backup.
Note
To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. Follow the instructions given in *Backup Cisco Crosswork with Cisco NSO* section in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#) instead of the instructions here.
 - Complete the remaining fields as needed.
If you want to specify a different remote server upload destination: Edit the prefilled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.
 - (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. If the verifications are successful, Crosswork Network Controller 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.
 - Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.
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 Crosswork Network Controller Cluster and Applications

This install the latest version of the Crosswork Network Controller 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](#)).

Procedure

- Step 1** Install the new version of the Crosswork Network Controller 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 Crosswork Network Controller UI (using <https://<VIP>:30603>) and check if all the nodes are up and running in the cluster.
- Step 3** After the cluster installation, ensure that the Crosswork inventory is onboarded.

Step 4 Install the Crosswork Network Controller applications which were installed in the old cluster. Ensure that you install the latest versions that are compatible with the new version of the 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 5 After the applications are successfully installed, check the health of the new cluster. From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager**.

- Click the **System summary** tile to view the health of the cluster nodes.
- Click the **Crosswork health** tab to view the health of the pods of all installed applications.

Run Migration

After successfully installing the new versions of the Crosswork Network Controller applications, proceed to migrate the Crosswork Network Controller backup taken earlier to the new Crosswork Network Controller 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 4](#).
- The name and path of the backup file created in [Create backup of the Cisco Crosswork cluster, on page 4](#).
- User credentials with file read and write permissions to the directory.

Procedure

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** drawer panel.
- 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 4](#).

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

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

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

- b) Click **Actions > Data Migration** to display the **Data Migration** drawer panel 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 4](#)) in the **Backup File Name** field.
- d) If you want to perform the data migration backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
- e) Click **Start Migration** to start the data migration operation. Crosswork Network Controller 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 cluster. From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager**.

- Click the **System summary** tile to view the health of the cluster nodes.
- Click the **Crosswork health** tab to view the health of the pods of all installed applications.

Step 5

After the migration, ensure that the Crosswork inventory is onboarded before proceeding with geo enablement.

Install the standby cluster and enable geo redundancy

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

Before you begin

Ensure inventory file is prepared as per the instructions in [Geo redundancy inventory file guidelines](#). For reference, see [Day 0: Geo inventory for active cluster deployed with peer cluster \(standby\)](#).

- Set `is_skip_peer_check_enabled` parameter to `false`.
- Set `is_post_migration_activation` parameter to `true`.

Procedure

Step 1 Install the standby cluster in Site 2.

Install using your preferred method:

- *Using Docker installer tool:* [Install Cisco Crosswork on VMware vCenter using the Docker installer tool](#)
- *Manual Installation:* [Manual Installation of Cisco Crosswork using vCenter vSphere UI](#)

Step 2 After the cluster installation, ensure that the Crosswork inventory is onboarded.

Step 3 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 4 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 5 Ensure unified cross cluster endpoint is resolved on Site 1 (active site).

Step 6 Enable geo redundancy on Site 1 (set as active) and Site 2 (set as standby), in that order.

- Log in to Site 1 (set as active). From the main menu, choose **Administration > Geo Redundancy Manager**. The **Geo Redundancy Manager** window is displayed.
- Click **Import inventory file**, and the **Import Inventory File** drawer panel is displayed. Click **Browse** and select the cross cluster inventory file that you prepared. Verify the contents of the template file.
- In this step you will be configuring the server to be used with Geo Redundancy. **This step cannot be undone**. You should have already made a backup of you cluster before proceeding with this action. To activate Geo Redundancy on the server, click **Enroll**.
- A service interruption alert is displayed. Click **Proceed** to continue.

The progress can be viewed from the **Jobs** window

- Wait until the job is completed, geo-redundancy is enabled on Site 1, and it is set as the active cluster.
- Log in to Site 2 (set as standby), and repeat steps 5a to 5d.

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.

Procedure

- 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.

Upgrade Crosswork Data Gateway 7.0 to 7.1 Geo Redundancy

You must upgrade the Data Gateway when transitioning Crosswork Network Controller from a non-geo-redundant to a geo-redundant deployment.

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 the existing Data Gateways.
- The Data Gateway must be enrolled using the FQDN. Enrolling with a Virtual IP (VIP) address can cause the Data Gateway to enter an error state after a Crosswork upgrade, due to a mismatch in enrollment details.

Procedure

- Step 1** Redeploy the 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 the Data Gateway VM from Cisco Crosswork](#) and installing a new instance, see **Step 9** in [Geo redundancy workflow \(Day 0\)](#).

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

We recommend that you 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 [View Cross Cluster Status](#) for information on how to perform a sync operation.

Step 2 Modify the high availability Data Gateway pools:

- 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 Migrate Data Gateway from a single stack that is IPv4 or IPv6 to a dual stack:

- Update the pool information by including the dual stack configuration's VIP IPs and gateway details. For instance, if you have configured IPv4 address when creating a pool, you must add the IPv6 information.

Step 4 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, reenroll the gateway from the interactive menu. See the *Reenroll Crosswork Data Gateway* section in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#) for more information.

Configure Controller IP for Crosswork Data Gateway

This topic explains the procedure for configuring the controller IP or FQDN for the data gateway after enabling the geo redundancy feature.

When a data gateway is deployed with an invalid controller IP, it may get stuck in the enrollment process. To address this, reconfigure the controller IP. Also, if a data gateway is enrolled to a Crosswork and there is a change in controller virtual IP or the IP is changed to FQDN due to the enabled geo redundancy feature, it must be reconfigured.

To configure the controller IP for a new enrollment or change the controller IP of an existing Crosswork that the data gateway is enrolled with:

Navigate to the data gateway on the active cluster before the geo redundancy feature is enabled.

Procedure

-
- Step 1** Log in to the data gateway VM on the active cluster before the geo redundancy feature is enabled.
- Step 2** In the data gateway VM interactive menu, select **3 Change Current System Settings**.
- Step 3** Select **Configure Controller IP/FQDN**.
- Step 4** Enter the SCP URI for the controller signing certificate file.
- Step 5** Enter the SCP passphrase or the SCP user password for the controller signing certificate file.
- Step 6** Enter the controller IP.
- A message appears to confirm that Crosswork has updated the controller's IP or FQDN, and the VM is rebooted.
-

The data gateway connects to Crosswork and progresses to the UP state. If the data gateways are in the Assigned state with devices attached, they resume data collection.

Complete Geo Redundancy Enablement

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

Optionally, you can complete the geo enablement operation for a three cluster inventory (active, standby, and arbiter). In this case, the arbiter cluster is added as a day-N scenario. For more information, see [Geo redundancy workflow \(Day N\)](#)



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

Before you begin

Ensure inventory file is prepared as per the instructions in [Geo redundancy inventory file guidelines](#). For reference, see [Day 0: Geo inventory for active cluster deployed with peer clusters \(standby and arbiter\)](#).

- Since both clusters are already deployed, set `is_skip_peer_check_enabled` parameter to `false`.
- Since this is a migration flow, set `is_post_migration_activation` parameter to `true`.

Procedure

-
- Step 1** Enable geo redundancy on the standby cluster.
- Log in to Site 2 (set as standby). From the main menu, choose **Administration > Geo Redundancy Manager**. The **Geo Redundancy Manager** window is displayed.
 - Click **Import inventory file**, and the **Import Inventory File** drawer panel is displayed. Click **Browse** and select the cross cluster inventory file that you prepared. Verify the contents of the template file.

- c) In this step you will be configuring the server to be used with Geo Redundancy. **This step cannot be undone.** You should have already made a backup of you cluster before proceeding with this action. To activate Geo Redundancy on the server, click **Enroll**.
- d) A service interruption alert is displayed. Click **Proceed** to continue.

The progress can be viewed from the **Jobs** window

Step 2 Configure the cross cluster settings. For more information, see [Configure Cross Cluster Settings](#).

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

Once geo redundancy is enabled, a **Geo Redundancy** tile is automatically added to the **Application management** window. This tile is built-in and cannot be upgraded, uninstalled, or deactivated.

Step 4 (Optional) Add an arbiter VM and enable geo redundancy. For more information, see [Geo redundancy workflow \(Day N\)](#).

Upgrade from Crosswork Network Controller 7.0.2 (geo redundant) to 7.1 (geo redundant)

This topic provides a high-level description of the tasks required to upgrade the geo redundant clusters in Crosswork Network Controller version [7.0.2](#) to version 7.1 (geo redundant). This migration is performed in geo redundant clusters across two sites while ensuring reduced migration downtime.



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. For more information about enabling geo redundancy on day N, see [Geo redundancy workflow \(Day N\)](#).

Prerequisites

- You have installed Crosswork Network Controller version 7.0.2 and enabled geo redundancy on both active and standby cluster sites. For more information about the 7.0.2 release, please refer to the [release notes](#).
- While the cluster installation is in progress, you must upgrade NSO and SR-PCE. Please see the [Release Notes for Crosswork Network Controller 7.1.0](#) to know the NSO and SR-PCE versions compatible with Crosswork Network Controller. The process to upgrade NSO or SR-PCE is not covered in this document. For install instructions, please refer to the relevant product documentation.
 - Cisco NSO: [Cisco NSO documentation](#)
 - Cisco SR-PCE: [Cisco IOS XRv 9000 Router Installation Guide](#).
- Geo synchronization must be disabled and avoided during the upgrade from version 7.0.2 to 7.1. It should only be performed after all clusters have been upgraded to version 7.1.0 and geo enablement has been fully completed.

- Ensure the inventory file (.yaml) is prepared without errors. For more information, see [Geo redundancy inventory file guidelines](#).

Upgrade workflow

Table 2: Upgrade from Crosswork Network Controller 7.0.2 (geo redundant) to 7.1 (geo redundant)

Step	Action
1. Upgrade and deploy SR-PCE	<p>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.</p> <p>After you have upgraded to the compatible version of SR-PCE, configure gRPC on SR-PCE. Ensure that your credentials in the CSV file include those for a gRPC connection, which should match your SSH credentials. In your provider settings, include gRPC as a connection option for SR-PCE</p>
2. Upgrade the secondary NSO (Site 2).	<p>If your NSO is running an older version, perform these steps:</p> <ol style="list-style-type: none"> 1. Set the primary NSO (Site 1) to read-only mode. 2. Disable HA on the secondary NSO (Site 2). 3. Upgrade the secondary NSO (Site 2) as per instructions in Cisco NSO documentation. <p>Follow instructions on converting single instance NSO to NSO HA, see Convert Single Instance NSO to NSO HA, on page 3 topic.</p>
3. (Optional) Create backup of the Crosswork Network Controller 7.0.2 cluster.	<p>Follow the instructions in Create backup of the Cisco Crosswork cluster, on page 4 topic.</p>

Step	Action
4. Shut down the Crosswork Network Controller 7.0.2 cluster on Site 2.	<p>Shut down the Crosswork Network Controller 7.0.2 cluster by powering down the VMs hosting each node (start with the Hybrid VMs).</p> <ol style="list-style-type: none"> 1. Gather following information before shutting down the cluster. <ul style="list-style-type: none"> • All IP addresses of the cluster. • All IP addresses of the Crosswork Data Gateways 2. Shut down the VMs of the Crosswork Network Controller 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 <code>ncs_cmd -c maapi_read_only</code> command.
5. Install the Crosswork Network Controller 7.1 cluster and applications on Site 2.	<p>Follow the instructions in Install the Crosswork Network Controller Cluster and Applications, on page 6 topic.</p> <p>Note Site 2 cluster will be non-geo redundant after installation of Crosswork Network Controller 7.1.</p> <p>After the cluster installation, ensure that the Crosswork inventory is onboarded before proceeding with the upgrade.</p>
6. Trigger the multi-cluster upgrade from the Site 2 cluster.	Follow the instructions in Multi cluster upgrade, on page 21 topic.
7. Upgrade Crosswork Data Gateway on Site 2 to version 7.1.	Follow the instructions in Upgrade Crosswork Data Gateway 7.0 to 7.1 Geo Redundancy on a Standby Site, on page 21 topic.
8. Update the providers.	Follow the instructions in Update Providers, on page 9 topic.
9. Enable geo redundancy on the Site 2 cluster.	Follow the instructions in Enable geo redundancy on the Site 2 cluster, on page 24 topic.
(Optional) 10. Shut down Crosswork Data Gateway on Site 1.	Follow the instructions in Shut down Crosswork Data Gateway in the active site, on page 24 topic.

Step	Action
11. Perform switchover from Site 1 to Site 2.	<p>For the instructions in the Perform switchover between sites, on page 25 topic.</p> <p>Attention Do not perform a sync operation from Site 1 to Site 2 during the switchover.</p>
12. Upgrade Crosswork Data Gateway on Site 1 to version 7.1.	<p>Follow the instructions in Upgrade Crosswork Data Gateway 7.0 to 7.1 Geo Redundancy, on page 10 topic.</p>
13. Upgrade the primary NSO (Site 1).	<p>Since the primary NSO (Site 1) is running an older version, perform these steps:</p> <ol style="list-style-type: none"> 1. Disable HA on the primary NSO (Site 1) before HA is enabled on the upgraded secondary NSO (Site 2). 2. Upgrade the primary NSO (Site 1) as per instructions in Cisco NSO documentation. 3. After primary NSO (Site 1) is upgraded, enable HA with node as secondary. This will sync all the data from the primary. <p>Follow instructions on converting single instance NSO to NSO HA, see Convert Single Instance NSO to NSO HA, on page 3 topic.</p>
14. Shut down the Crosswork Network Controller 7.0.2 cluster on Site 1.	<p>Shut down the Crosswork Network Controller 7.0.2 cluster by powering down the VMs hosting each node (start with the Hybrid VMs).</p> <ol style="list-style-type: none"> 1. Gather following information before shutting down the cluster. <ul style="list-style-type: none"> • All IP addresses of the cluster. • All IP addresses of the Crosswork Data Gateways 2. Shut down the VMs of the Crosswork Network Controller 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 <code>ncs_cmd -c maapi_read_only</code> command.

Step	Action
15. Install the Crosswork Network Controller 7.1 cluster and applications on Site 1.	<p>Follow the instructions in Install the Crosswork Network Controller Cluster and Applications, on page 6 topic.</p> <p>Note Site 1 cluster will be non-geo redundant after installation of Crosswork Network Controller 7.1.</p> <p>After the cluster installation, ensure that the Crosswork inventory is onboarded before proceeding.</p>
16. Complete the geo enablement operation on the Site 1 cluster.	Follow the instructions in Enable geo redundancy on the Site 1 cluster, on page 28
17. Enable and initiate sync in Site 2 (sync from Site 2 to Site 1)	<p>Perform these steps:</p> <ol style="list-style-type: none"> 1. Log in to the Site 2 cluster (currently, the active cluster). 2. Verify that the geo mode status is completed and the cross-cluster operational status is healthy. 3. Click on Configurations > Sync settings, and enable the Sync slider button. 4. Initiate a sync or wait for a configured periodic sync to complete. 5. After completing the sync, verify that both Site 1 and Site 2 are healthy and running Crosswork Network Controller version 7.1.
(Optional) 18. Perform the second switchover (Site 2 to Site 1)	If you need to make the original site active again, perform a switchover from Site 2 to Site 1 . Follow the instructions in Perform switchover between sites, on page 25 , but ensure that you reverse the site roles accordingly.
(Optional) 19. Complete the geo enablement operation with the arbiter node. Note You can skip this step if you do not wish to deploy an arbiter node.	Follow the instructions in Geo redundancy workflow (Day N) .

Create backup of the Cisco Crosswork cluster

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



Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Crosswork Network Controller 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 Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller is communicating over IPv6, so must the backup server.
- 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).

Procedure

-
- 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 Crosswork Network Controller main menu, choose **Administration > Backup and Restore**.
- b) Click **Destination** to display the **Edit Destination** drawer panel. 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 Crosswork Network Controller main menu, choose **Administration > Backup and Restore**.
- b) Click **Actions > Backup** to display the **Backup** drawer panel 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.

Note

To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. Follow the instructions given in *Backup Cisco Crosswork with Cisco NSO* section in the [Cisco Crosswork Network Controller 7.1 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 prefilled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.
- g) (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. If the verifications are successful, Crosswork Network Controller 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. Crosswork Network Controller creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.

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 Crosswork Network Controller Cluster and Applications

This install the latest version of the Crosswork Network Controller 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](#)).

Procedure

- Step 1** Install the new version of the Crosswork Network Controller 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 Crosswork Network Controller UI (using <https://<VIP>:30603>) and check if all the nodes are up and running in the cluster.
- Step 3** After the cluster installation, ensure that the Crosswork inventory is onboarded.
- Step 4** Install the Crosswork Network Controller applications which were installed in the old cluster. Ensure that you install the latest versions that are compatible with the new version of the 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 5** After the applications are successfully installed, check the health of the new cluster. From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager**.
- Click the **System summary** tile to view the health of the cluster nodes.

- Click the **Crosswork health** tab to view the health of the pods of all installed applications.
-

Multi cluster upgrade

This section explains how to perform the multi-cluster upgrade in Crosswork Network Controller.

Before you begin

Ensure you have downloaded and prepared the inventory file (.yaml).

Procedure

- Step 1** From the Crosswork Network Controller main menu, choose **Administration > Geo Redundancy Manager**. The **Geo Redundancy Manager** window is displayed.
- Step 2** Click on the **Multi-cluster upgrade** tab.
- Step 3** Click on **Import upgrade inventory**. The **Multi-Cluster Upgrade** drawer panel is displayed.
- Step 4** (Optional) Click **sample file** to download a sample inventory file (.yaml) file for multi-cluster upgrade.
- Step 5** Click **Browse** to select and upload the inventory file (.yaml) file from your machine. Ensure the `cluster_id` value in the inventory file matches with the value specified in regular geo inventory.

Important

The upgrade job storage path settings in the inventory file must be different from the configured path in the Cross Cluster storage settings.

- Step 6** Click the **Jobs** tab to view the progress of the upgrade job.
- The multi-cluster upgrade job creates a data backup backup job on site 1, and a data migration job on site 2. Navigate to the **Backup and Restore** window (**Administration > Backup and Restore**) in each site to view the jobs.

Note

Once the upgrade job starts on site 2, the UI will be unavailable for some time. You can check the upgrade alarm on site 1 for the Grafana dashboard URL, which can be opened in a browser to monitor the upgrade job's progress.

- Step 7** Once the job is completed, check the health of all applications and ensure that they are in a healthy state.
- The data from Crosswork Network Controller 7.0.2 on site 1 is now migrated to site 2 running Crosswork Network Controller 7.1.
-

Upgrade Crosswork Data Gateway 7.0 to 7.1 Geo Redundancy on a Standby Site

You must upgrade the Data Gateways on the standby site when transitioning Crosswork Network Controller from version 7.0 to 7.1.

Before you begin

Ensure that you are aware of the following:

- Data Gateways from the standby site must not be in the maintenance mode on the active site.
- The collection downtime occurs during this procedure. The total downtime includes the Data Gateway upgrade duration and delays in receiving jobs from northbound.
- The Data Gateways upgrade behavior on standby site:
 - The Data Gateways that are on the standby site, when connected to the active site, have the role as Spare.
 - Upgrading these Data Gateways does not impact data collection on the active site.
 - After redeployment, the upgraded Data Gateways enter the error state on the active site because a reenrollment is required.



Note The Data Gateways automatically enroll with the Crosswork on the standby site after the first switchover.

Procedure

-
- Step 1** Redeploy the 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 the Data Gateway VM from Cisco Crosswork](#) and installing a new instance, see **Step 9** in [Geo redundancy workflow \(Day 0\)](#).
- Note**
- If the Data Gateways are redeployed using the same name and hostname that is specified in the OVF script, the DG-Manager considers them as existing gateways. It automatically enrolls them with the upgraded Crosswork during the migration process.
 - We recommend that you 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 [View Cross Cluster Status](#) for information on how to perform a sync operation.
- Step 2** After the Crosswork cluster switchover when the standby site becomes active, the Data Gateways on standby site take over the roles of the active site-assigned Data Gateways. These Data Gateways are upgraded to version 7.1, and it may take a few minutes for them to enter either the **NOT_READY** or **UP** state. For more information, see [Geo Redundancy Switchover](#).
- Step 3** After you log in to the Crosswork Network Controller UI, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.
- Step 4** After the switchover is complete, modify the high availability Data Gateway pools:
- 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 5 Migrate Data Gateway from a single stack that is IPv4 or IPv6 to a dual stack:

- Update the pool information by including the dual stack configuration's VIP IPs and gateway details. For instance, if you have configured an IPv4 address when creating a pool, you must add the IPv6 information.

Step 6 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.

After the switchover to the standby site, the following occurs:

- The Data Gateways in the standby site enter the Assigned role to take over collections from the active site.
- Each Data Gateway begins downloading the Crosswork 7.1.0 version images.
- Once the 7.1.0 containers are deployed:
 - The Data Gateways in the Assigned role resume data collection.
 - Inventory and collection jobs are retransmitted from the northbound interface.

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.

Procedure

- 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.

Enable geo redundancy on the Site 2 cluster

After updating the providers, activate geo redundancy on the Site 2 cluster.

Before you begin

Kindly ensure

- the connectivity checks work for east-west communication.
- DNS connectivity checks work from both clusters.
- the unified cross-cluster endpoint resolves to the Site 1 cluster (active cluster).
- inventory file is prepared as per the instructions in [Geo redundancy inventory file guidelines](#). For reference, see [Day N: Geo inventory for active cluster deployed without peer cluster \(standby\)](#).
 - Set `is_skip_peer_check_enabled` parameter to `true`.
 - Set `is_post_migration_activation` parameter to `true`.
- the `cluster_id` parameter value matches with the value in the upgrade inventory yaml in [Multi cluster upgrade, on page 21](#). Any mismatch would cause the geo redundancy pairing to fail.

Procedure

-
- Step 1** Log in to the Site 1 cluster (currently, the active cluster), and navigate to the **Geo Redundancy Manager** window. Enable the **pairing mode** slider. This ensures the active cluster accepts the newly upgraded cluster for multi-cluster upgrade.
 - Step 2** Create and upload the cluster inventory file on Site 2, to create the standby cluster.
 - Step 3** Verify that the geo mode status is completed and the cross-cluster operational status is healthy on both Sites.

At the end of this procedure, Site 1 will serve as the active cluster with Crosswork Network Controller version 7.0.2, while Site 2 will function as the standby cluster with Crosswork Network Controller version 7.1 installed.

Attention

Do not perform a sync operation from Site 1 to Site 2 after this step.

Shut down Crosswork Data Gateway in the active site

Before initiating the Crosswork cluster switchover, shut down the Data Gateway on the active site. This action preserves the 7.0 configuration and prevents the automatic download of the 7.1 version.

Before you begin

Ensure that you are aware of the following:

- Shutting down the Data Gateway in the active site interrupts data collections. To minimize the downtime, shutdown Data Gateway only when you are ready to initiate the switchover.
- If you choose not to shut down the Data Gateway:
 - After a switchover, the Data Gateway in the active site connects to the standby site.
 - When the Data Gateway in the active site downloads the 7.1 configuration, its operational state changes to NOT_READY.

Procedure

- Step 1** Shut down all the Data Gateway VMs in the active site.
- a) Log in to the Data Gateway VM. For information, see [Log in and Log out of the Data Gateway VM](#). Crosswork Data Gateway launches an Interactive Console after your login.
 - b) Choose **5 Troubleshooting**.
 - c) From the **Troubleshooting** menu, choose **5 Shutdown VM** to shut down the VM.

- Step 2** Perform Crosswork cluster switchover. For more information, see [Geo Redundancy Switchover](#).

Note

If an issue occurs on the standby site before completing the switchover, and you need to revert to the active site, which is still running version 7.0:

- Make the now standby site active again
- Power on the Data Gateways in that site

Once powered on, the Data Gateways should resume data collection as expected.

After the switchover to the standby site, the Data Gateways enters the ERROR state. This behavior is expected and has no impact on active data collection, as the affected Data Gateways function only as spares. These Data Gateways are currently running version 7.0 and are re-deployed with version 7.1 in a later step.

Perform switchover between sites

This topic explains how to perform the first switchover between the cluster sites.

Before you begin

To initiate a switchover via the UI, perform these checks on each site *before the switchover*.

1. On Site 2

- Ensure that the completion time of the geo upgrade job has not exceeded 18 hours.

2. On Site 1

- Verify that the geo upgrade job is successfully completed.
- Confirm that the Crosswork Network Controller version in Site 1 is older than the version in Site 2.

If any of these checks fail, you must initiate the switchover using the API instead of the UI.

Skipping these checks and performing the switchover via the UI may result in a dampening period and at least one "sync required" error.

Procedure

Step 1 **Perform switchover via UI:** Initiate switchover from the Crosswork Network Controller UI. For more information, see [Perform switchover manually](#).

Step 2 **Perform switchover via API:** Execute these APIs from the local terminal.

Note

You can get cross cluster name and id from the **view inventory** option in the **Geo Redundancy Manager** window.

a) Set Site 2 to active using the `SetRole` API.

```
curl --insecure --location 'https://<site-2-managementvip>:30603/crosswork/crosscluster/v1/role'
--header 'Content-Type: application/json' --header 'Authorization: <your bearer token>'
--data '{
  "cross_cluster_component": {
    "id": "<cross cluster id of site2 mentioned in inventory file>",
    "name": "<cross cluster name of site2 mentioned in inventory file>",
    "component_type": "CROSSWORK_CLUSTER"
  },
  "preferred_cluster_leadership_state": "ACTIVE",
  "force": true
}'
```

b) Update DNS to point to Site 2 (Active).

c) Set Site 1 to standby using the `SetRole` API.

```
curl --insecure --location 'https://<site-1-managementvip>:30603/crosswork/crosscluster/v1/role'
--header 'Content-Type: application/json' --header 'Authorization: <your bearer token>'
--data '{
  "cross_cluster_component": {
    "id": "<cross cluster id of site1 mentioned in inventory file>",
    "name": "<cross cluster name of site1 mentioned in inventory file>",
    "component_type": "CROSSWORK_CLUSTER"
  },
  "preferred_cluster_leadership_state": "STANDBY",
  "force": true
}'
```

Step 3 Post switchover, verify that all services are healthy and the cross cluster is operationally healthy.

Step 4 In Site 2, disable the cross cluster sync setting.

Upgrade Crosswork Data Gateway 7.0 to 7.1 Geo Redundancy

You must upgrade the Data Gateway when transitioning Crosswork Network Controller from a non-geo-redundant to a geo-redundant deployment.

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 the existing Data Gateways.
- The Data Gateway must be enrolled using the FQDN. Enrolling with a Virtual IP (VIP) address can cause the Data Gateway to enter an error state after a Crosswork upgrade, due to a mismatch in enrollment details.

Procedure

- Step 1** Redeploy the 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 the Data Gateway VM from Cisco Crosswork](#) and installing a new instance, see **Step 9** in [Geo redundancy workflow \(Day 0\)](#).
- 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**
We recommend that you 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 [View Cross Cluster Status](#) for information on how to perform a sync operation.
- Step 2** Modify the high availability Data Gateway pools:
- 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** Migrate Data Gateway from a single stack that is IPv4 or IPv6 to a dual stack:
- Update the pool information by including the dual stack configuration's VIP IPs and gateway details. For instance, if you have configured IPv4 address when creating a pool, you must add the IPv6 information.

- Step 4** 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, reenroll the gateway from the interactive menu. See the *Reenroll Crosswork Data Gateway* section in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#) for more information.

Enable geo redundancy on the Site 1 cluster

After updating the providers, activate geo redundancy on the Site 1 cluster.

Before you begin

- Ensure connectivity checks work for east-west communication.
- Ensure DNS connectivity checks work from both clusters.
- Ensure the unified cross-cluster endpoint resolves to the Site 2 cluster (active cluster).
- Ensure you prepare the inventory file as per the instructions in [Geo redundancy inventory file guidelines](#). For reference, see [Day 0: Geo inventory for active cluster deployed with peer cluster \(standby\)](#).
 - Set `is_skip_peer_check_enabled` parameter to `false`.
 - Set `is_post_migration_activation` parameter to `true`.
 - As Site 2 cluster is already up and in ACTIVE state, set the `initial_preferred_leadership_state` parameter for Site 1 to `STANDBY`.

Procedure

- Step 1** Log in to the Site 2 cluster (currently, the active cluster), and navigate to the **Geo Redundancy Manager** window. Enable the **pairing mode** slider. This ensures the active cluster accepts the newly upgraded cluster for multi-cluster upgrade.
- Step 2** Create and upload the cluster inventory file on Site 1, to create the standby cluster.

Attention

If you accidentally activate Site 1 with `initial_preferred_leadership_state` parameter as `ACTIVE`, perform these recovery steps:

- Reset the geo mode using the `geo_reset` command from one of the Hybrid nodes in the cluster.

```
geo_reset -h
Usage: /usr/local/bin/geo_reset -r ORCH_REPLICAS
```

Options:

```
-r ORCH_REPLICAS | Specify the number of robot-orchestrator replicas between 1 and 2
: For SVM replicas is 1
: For Cluster replicas is 2
-h Show this help message
```

- Uninstall the geo redundancy CAPP file, and ensure the cross cluster pod is not running.
- Update the inventory file with the correct configurations, and perform the geo activation again.

Step 3 Verify that the geo mode status is completed and the cross-cluster operational status is healthy on both Sites.

At the end of this procedure, Site 2 will serve as the active cluster while Site 1 will function as the standby cluster, with both running Crosswork Network Controller version 7.1.

Step 4 Configure the cross cluster settings with SCP host over data network.
