Enable Geo Redundancy Solution

This chapter contains the following topics:

Geo Redundancy Workflow (Day 0)

This topic explains the workflow to enable geo redundancy on day 0. The workflow give a high level description of the tasks necessary to install and enable geo redundancy in Crosswork Network Controller.

Note The recommended day-0 setup for enabling geo redundancy is an empty Crosswork cluster (without any applications, devices or data gateways onboarded).

The following table describes the stages to install and enable the geo redundancy mode on Crosswork Network Controller.

Table 1: Geo Redundancy Workflow (Day 0)

Step	Action
1. Install the Active Crosswork cluster.	Install using your preferred method: • *Using cluster installer tool:* Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool • *Manual Installation:* Manual Installation of Cisco Crosswork using vCenter vSphere UI Verify if the installation was successful, and log into the Cisco Crosswork UI. • Monitor Cluster Activation • Log into the Cisco Crosswork UI

Step	Action
2. Install the Standby Crosswork cluster.	Install using your preferred method: • *Using cluster installer tool:* Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool • *Manual Installation:* Manual Installation of Cisco Crosswork using vCenter vSphere UI Verify if the installation was successful, and log into the Cisco Crosswork UI. • Monitor Cluster Activation • Log into the Cisco Crosswork UI
3. Validate the Crosswork Inventory. In case of manual installation of Crosswork Cluster, you must import a cluster inventory file (.yaml file) to the Crosswork UI. **Important** If you fail to ensure this step, the geo redundancy enablement will fail.	For more information, see the *Import Cluster Inventory* topic in the *Crosswork Network Controller 6.0 Administration Guide*.
4. (Recommended) Create a backup of your Crosswork cluster.	Follow the instructions in *Manage Backups* chapter in *Cisco Crosswork Network Controller 6.0 Administration Guide*.
5. Perform the connectivity checks.	Follow the instructions in Connectivity Checks, on page 3 topic.
6. Prepare and upload the cross cluster inventory template in the Active and Standby clusters to enable geo redundancy.	Follow the instructions in Enable Geo Redundancy, on page 5 topic.
7. Verify that the geo redundancy was successfully enabled on the active and standby clusters.	Follow the instructions in View Cross Cluster Status, on page 9 topic.
8. Configure the cross cluster settings	Follow the instructions in below topics: • Storage settings: Configure Cross Cluster Storage Settings, on page 10 • Sync settings: Configure Cross Cluster Sync Settings, on page 11 • DNS settings: Configure Cross Cluster DNS Settings, on page 12 • Arbitration settings: Configure Cross Cluster Arbitration Settings, on page 14 • Notification settings: Configure Cross Cluster Notification Settings, on page 15

Step	Action
9. Validate if geo redundancy is enabled	Check the following: • In the Cross Cluster Health Status, ensure the operational state is **Connected**. • In the Cross Cluster Health Status, ensure that Active cluster state is **Healthy**. • In the Cross Cluster Health Status, ensure that Standby cluster state is **Healthy**. • In the Cross Cluster Health Status, ensure the High Availability state is **AVAILABLE**. • Verify if the heartbeat count between the clusters is incrementing and no failures are observed for over a 30-minute period. • Confirm the completion of one successful sync between the clusters.

Connectivity Checks

Perform the following connectivity checks before enabling geo redundancy:

- Copy (using `SCP)` a file from Availability Zone 1 (AZ1) to Availability Zone 2 (AZ2), and from AZ2 to AZ1 in corresponding Crosswork VMs and Crosswork Orchestrator pods to ensure connectivity between both clusters.

```
# Perform the below steps from AZ1 to AZ2, and from AZ2 to AZ1:

root@dev4-jump:~# ssh cw-admin@192.168.6.100
Password:
Last login: Sat Jul  1 16:50:21 2023 from 192.168.6.6
Cisco Crosswork


Copyright (c) 2023 by Cisco Systems, Inc.
Version: release-6.0.0 (Build 182)
Built on: Jul-01-2023 01:27 AM UTC

cw-admin@192-168-6-101-hybrid:~$ sudo su
[sudo] password for cw-admin:
root@192-168-6-101-hybrid:/home/cw-admin# kubectl exec -it -n=kube-system
robot-orch-76856487-562w6 -- bash
robot-orch-76856487-562w6:~# touch t.txt
robot-orch-76856487-562w6:~# scp t.txt cw-admin@YOUR_PEER_CLUSTER_MGMT_VIP:/home/cw-admin/
(cw-admin@192.168.5.100) Password:
t.txt

robot-orch-76856487-562w6:~# scp t.txt cw-admin@YOUR_PEER_CLUSTER_DATA_VIP:/home/cw-admin/
(cw-admin@192.168.5.100) Password:
t.txt
```

- Static routes are not required for cross cluster connectivity.

- Mesh connectivity is required between Crosswork Network Controller, Crosswork Data Gateway, NSO, and data interface components across the AZs.
- L2/L3 connectivity is supported.
- Test the DNS resolution on system wide DNS server.

```
### Internal Authortative  resolution

dig @your_dns_server_ip  your_name.cw.cisco

; <<>> DiG 9.10.6 <<>> @172.28.122.84 geomanagement.cw.cisco
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8167
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;your_name.cw.cisco.        IN  A

;; ANSWER SECTION:
your_name.cw.cisco. 5   IN  A   192.168.6.100

;; Query time: 126 msec
;; SERVER: 172.28.122.84#53(172.28.122.84)
;; WHEN: Fri Jun 30 23:47:51 PDT 2023
;; MSG SIZE  rcvd: 67

### External forwarding and resolution

 dig @your_dns_server_ip  ntp.esl.cisco.com

; <<>> DiG 9.10.6 <<>> @172.28.122.84 ntp.esl.cisco.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43986
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;ntp.esl.cisco.com.     IN  A

;; ANSWER SECTION:
ntp.esl.cisco.com.  1   IN  A   171.68.38.66

;; Query time: 311 msec
;; SERVER: 172.28.122.84#53(172.28.122.84)
;; WHEN: Fri Jun 30 23:46:37 PDT 2023
;; MSG SIZE  rcvd: 62
```

- Verify if the DNS TTL in your VM is lesser than 60 seconds (< 60s).

```
# DNS TTL with 5s for FQDN entry

cw-user@admin-M-C2EM ~ %  dig +nocmd +noall +answer @your_dns_server_ip  your_fqdn
geomanagement.cw.cisco. 60  IN  A   192.168.6.100
```

Enable Geo Redundancy

This topic explains the procedure to enable geo redundancy from Crosswork UI.

> **Tip** Click on **How it works?** link to view a visual representation of how geo redundancy is enabled.

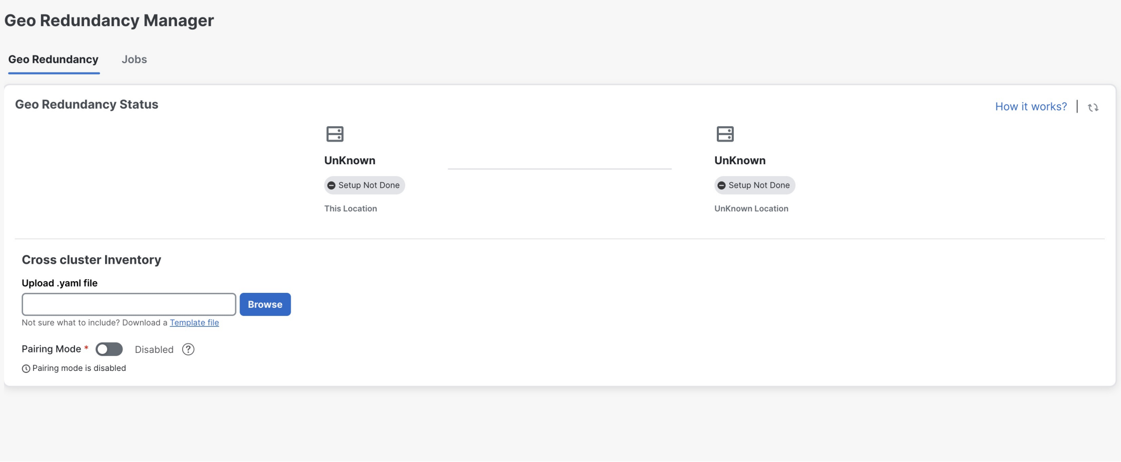
Before you begin

Ensure you have met all the requirements specified in Geo Redundancy Requirements.

Step 1 Log in to the Crosswork cluster that will function as the active cluster.

Step 2 From the main menu, choose **Administration** > **Geo Redundancy Manager**. The **Geo Redundancy Manager** window is displayed.

Figure 1: Geo Redundancy Manager



UnKnown
Setup Not Done
This Location

UnKnown
Setup Not Done
UnKnown Location

Not sure what to include? Download a Template file

Pairing Mode * Disabled

Pairing mode is disabled

Step 3 Click on **Download a Template file** to download the sample template (.yaml file) for the cross cluster inventory (for more details, see Sample Cross Cluster Inventory Template). Fill the template file with the relevant information for active and standby clusters and the unified cross cluster.

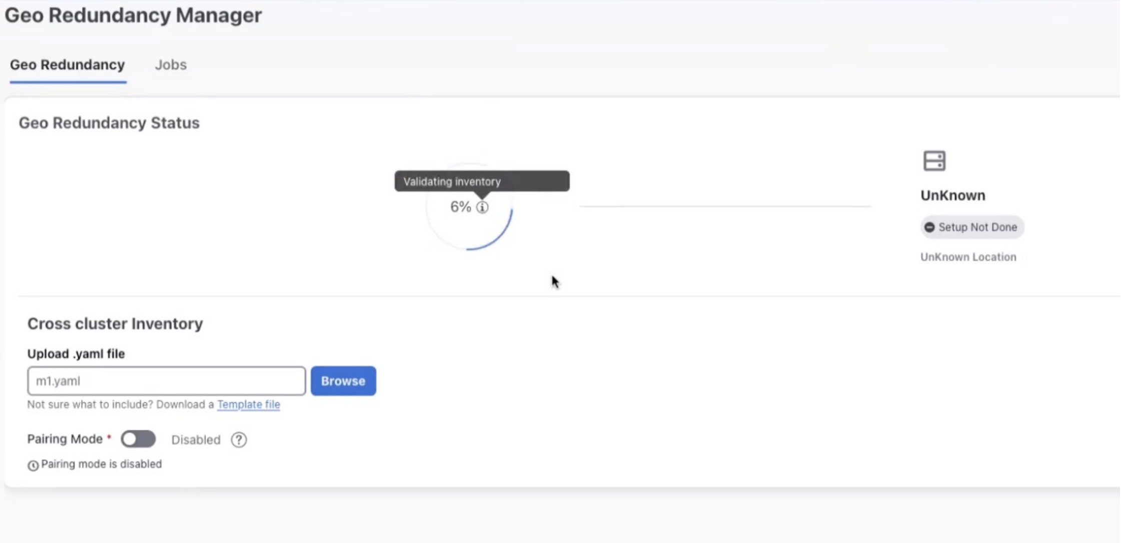
Step 4 Click **Browse** and select the cross cluster inventory file that you prepared. The **Import Inventory File** dialog box is displayed. Verify the contents of the template file.

Step 5 After you have verified, click **Setup**. A service interruption alert is displayed. Click **Proceed** to continue.

> **Important** This is the final step to enable geo redundancy. It cannot be undone.

The progress can be viewed from the **Jobs** window, or by clicking the ⓘ icon.

Figure 2: Inventory import



Geo Redundancy Manager

Geo Redundancy | Jobs

Geo Redundancy Status

Validating inventory
6% ⓘ

UnKnown
Setup Not Done
UnKnown Location

Cross cluster Inventory

Upload .yaml file: m1.yaml Browse

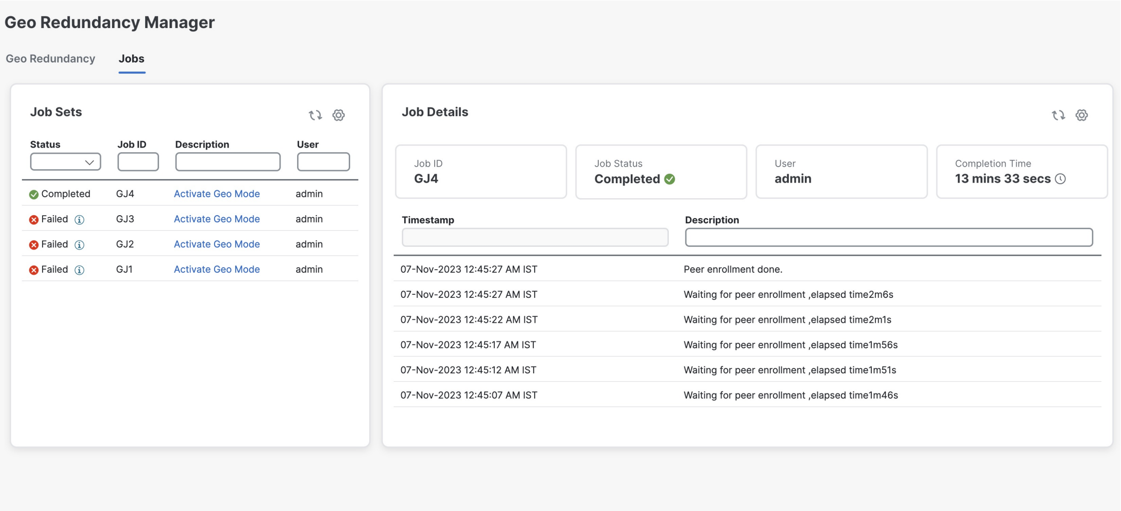
Not sure what to include? Download a Template file

Pairing Mode *: Disabled ?

Pairing mode is disabled

After the standby cluster is created, the setup status will be displayed as **Completed** on both clusters.

Figure 3: Geo Redundancy Jobs



Geo Redundancy Manager

Geo Redundancy | Jobs

Job Sets

Status	Job ID	Description	User
✓ Completed	GJ4	Activate Geo Mode	admin
✗ Failed ⓘ	GJ3	Activate Geo Mode	admin
✗ Failed ⓘ	GJ2	Activate Geo Mode	admin
✗ Failed ⓘ	GJ1	Activate Geo Mode	admin

Job Details

Job ID: GJ4
Job Status: Completed ✓
User: admin
Completion Time: 13 mins 33 secs ⓘ

Timestamp	Description
07-Nov-2023 12:45:27 AM IST	Peer enrollment done.
07-Nov-2023 12:45:27 AM IST	Waiting for peer enrollment ,elapsed time2m6s
07-Nov-2023 12:45:22 AM IST	Waiting for peer enrollment ,elapsed time2m1s
07-Nov-2023 12:45:17 AM IST	Waiting for peer enrollment ,elapsed time1m56s
07-Nov-2023 12:45:12 AM IST	Waiting for peer enrollment ,elapsed time1m51s
07-Nov-2023 12:45:07 AM IST	Waiting for peer enrollment ,elapsed time1m46s

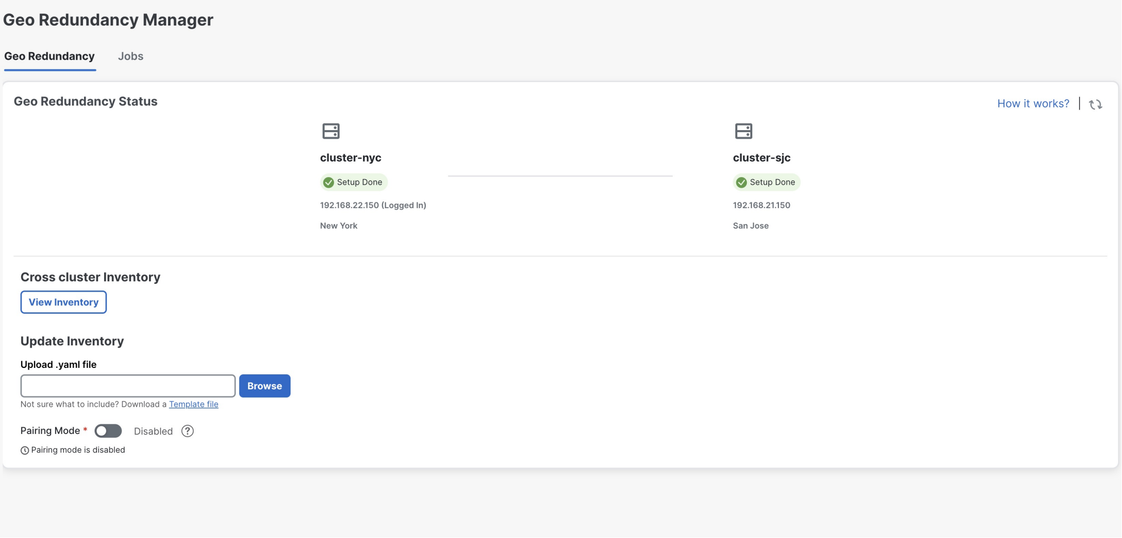
Step 6 After inventory upload is completed in the first cluster, the same process must be repeated in the second cluster.

Step 7 Log in to the Crosswork cluster that will function as the standby cluster, and repeat the actions in steps 4 and 5.

Important Please activate **Pairing mode** if the standby cluster is activated more than 6 hours after the active cluster.

Once the inventory upload is successfully completed on both clusters, the status will be updated in the **Geo Redundancy Manager** window.

Figure 4: Geo Redundancy Status Update



Geo Redundancy Manager

Geo Redundancy Status

cluster-nyc
Setup Done
192.168.22.150 (Logged In)
New York

cluster-sjc
Setup Done
192.168.21.150
San Jose

Cross cluster Inventory

Update Inventory

Upload .yaml file

Not sure what to include? Download a Template file

Pairing Mode * Disabled

Pairing mode is disabled

Sample Cross Cluster Inventory Template

Here is an example of the cross cluster inventory file (.yaml) that you need to prepare to enable geo redundancy:

```
############## Crosswork Multi cluster yaml for enabling Geo Redundancy ##########
## meta version of yaml ###
meta_version: 1.0.0
## Crosscluster name , mutable
crosscluster_name: mycnc-geo-cluster
### Unified endpoint of multi cluster for management and data endpoint across clusters
crosscluster_unified_connectivity:
  unified_end_point:
    unified_endpoint_type:
      #### fqdn_type,ip_type are options , only fqdn_type is supported.
      fqdn_type: {}
    #### DNS,BGP,NLB are options, only DNS is supported for now.
    unified_endpoint_implementation: DNS
     ### The below is needed if fqdn_type is chosen,else data_vip,mgmt_vip could be used
for ip_type endpoint type
  management_fqdn:
    ## cnc domain zone, DNS server would be checked for resolution
    domain_name: your-name.domain
    host_name: your-unified-cnc-mgmt-hostname
  data_fqdn:
    ## cnc domain zone name, DNS server would be checked for resolution
    domain_name: your-name.domain
    host_name: your-unified-cnc-data-hostname

### Constituent clusters ####
clusters:
##### Mutable cluster name
  - cluster_name: cluster-sjc
    connectivity:
      ### Intra cluster (within a cluster) unified endpoint  ###
      ### Endpoint type is ip_type,fqdn_type , Implementation could be VRRP,NLB,BGP.
      unified_end_point:
        unified_endpoint_type:
```

```
     ip_type: {}
    #### VRRP,BGP,NLB are options, only VRRP,ip_type is supported for now in on prem.
For cloud NLB,
    ### fqdn_type could be used.
    unified_endpoint_implementation: VRRP
   ### The below is needed if ip_type is chosen,else data_fqdn,mgmt_fqdn could be used
for fqdn_type endpoint type
   ## Your intra cluster data vip
   data_vip: 10.10.10.11
   ## data vip subnet mask
   data_vip_mask: 0
   ## Your intra cluster management vip
   management_vip: 20.20.20.11
   ## management vip subnet mask
   management_vip_mask: 0
   ## management and data fqdn for crosscluster instance
   ## management and data fqdn is applicable for only for unified crosscluster instance
  ## STANDBY or ACTIVE for leadership state
  initial_preferred_leadership_state: ACTIVE
  ### DC location , needs to be unique per cluster, For cloud region-az could be used
  site_location:
   location: San Jose
   #Mutable credentials
  cluster_credential:
   ## This is the https credential post first time cluster login
   https_credential:
    username: admin
    #### pwd/secrets are within single quotes,if special chars are used
    password: your-password
   ssh_credential:
    username: admin
    #### pwd/secrets are within single quotes,if special chars are used
    password: your-password
##### Mutable cluster name
 - cluster_name: cluster-nyc
  ## STANDBY or ACTIVE for leadership state
  initial_preferred_leadership_state: STANDBY
  connectivity:
   ### Intra cluster (within a cluster) unified endpoint  ###
   ### Endpoint type is ip_type,fqdn_type , Implementation could be VRRP,NLB,BGP.
   unified_end_point:
    unified_endpoint_type:
     ip_type: {}
    #### VRRP,BGP,NLB are options, only VRRP,ip_type is supported for now in on prem.
For cloud NLB,
    ### fqdn_type could be used.
    unified_endpoint_implementation: VRRP
   ### The below is needed if ip_type is chosen,else data_fqdn,mgmt_fqdn could be used
for fqdn_type endpoint type
   ## Your intra cluster data vip
   data_vip: 30.30.30.11
   ## data vip subnet mask
   data_vip_mask: 0
   ## Your intra cluster management vip
   management_vip: 40.40.40.11
   ## management vip subnet mask
   management_vip_mask: 0
   ## management and data fqdn for crosscluster instance
   ## management and data fqdn is applicable for only for unified crosscluster instance
  ### DC location , needs to be unique per cluster, For cloud region-az could be used
  site_location:
   location: New York City
  #Mutable credentials
  cluster_credential:
      ## This is the https credential post first time cluster login
      https_credential:
        username: admin
        #### pwd/secrets are within single quotes if special chars are used
        password: your-password
      ssh_credential:
        username: admin
        #### pwd/secrets are within single quotes if special chars are used
        password: your-password
#### Mutable secret are within single quotes if special chars are used, used to kick-start
 inter cluster mTLS
### needs to be >= 10 chars with at-least 1 special,upper,numerical characters
secret: Your-secret1
### Set this to true , if one is enabling geo mode on a system post migration setup, rather
 than a fresh first time
## install
is_post_migration_activation: false
### Set this to true , if one is enabling geo mode on a system post Disaster Recovery when
 both the clusters are down
is_skip_peer_check_enabled: false
```

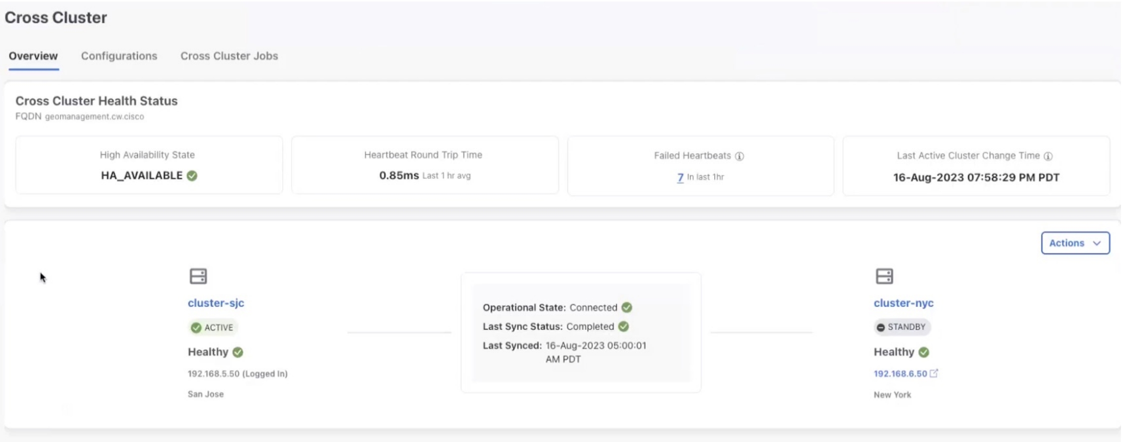
View Cross Cluster Status

This topic explains how to view the cross cluster status after successfully enabling geo redundancy.

Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed.

The cross cluster health status is displayed along with the high availability state, heartbeats round trip time, failed heartbeats, and last active cluster change time. You can also view the status of the active and standby clusters along with the operational state and last sync status.

Figure 5: Cross Cluster Overview



Cross Cluster Health Status
FQDN geomanagement.cw.cisco

High Availability State: HA_AVAILABLE ✓
Heartbeat Round Trip Time: 0.85ms Last 1 hr avg
Failed Heartbeats ⓘ: 7 In last 1hr
Last Active Cluster Change Time ⓘ: 16-Aug-2023 07:58:29 PM PDT

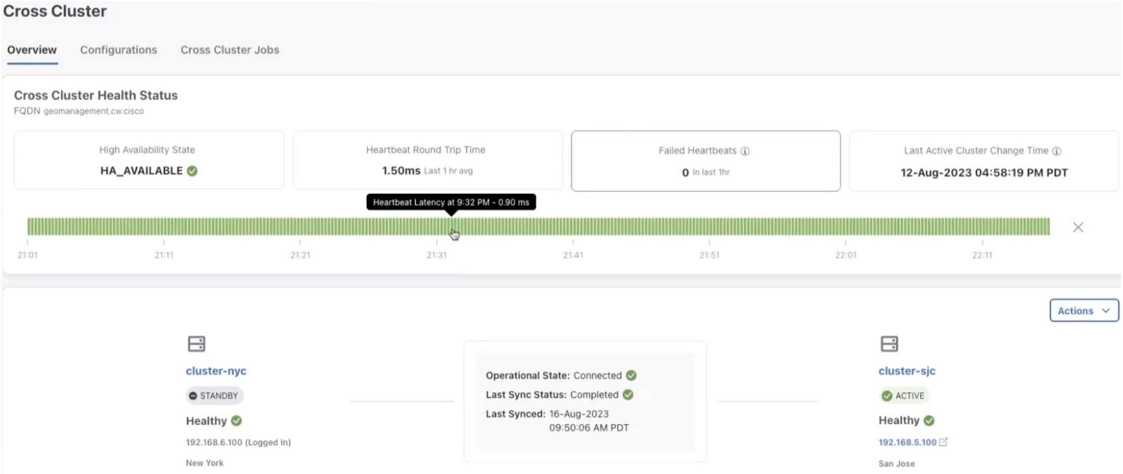
cluster-sjc
✓ ACTIVE
Healthy ✓
192.168.5.50 (Logged In)
San Jose

Operational State: Connected ✓
Last Sync Status: Completed ✓
Last Synced: 16-Aug-2023 05:00:01 AM PDT

cluster-nyc
● STANDBY
Healthy ✓
192.168.6.50
New York

Step 2 (Optional) Click ⓘ next to failed heartbeats to see a visual representation of the heartbeat count.

Figure 6: Cross Cluster Overview



Cross Cluster Health Status

FQDN geomanagement.cw.cisco

High Availability State: HA_AVAILABLE ✓

Heartbeat Round Trip Time: 1.50ms Last 1 hr avg

Failed Heartbeats: 0 In last 1hr

Last Active Cluster Change Time: 12-Aug-2023 04:58:19 PM PDT

Heartbeat Latency at 9:32 PM - 0.90 ms

cluster-nyc

STANDBY

Healthy ✓

192.168.6.100 (Logged In)

New York

Operational State: Connected ✓

Last Sync Status: Completed ✓

Last Synced: 16-Aug-2023 09:50:06 AM PDT

cluster-sjc

ACTIVE

Healthy ✓

192.168.5.100

San Jose

Step 3 (Optional) Click **Actions** > **Showtech Request** to download the showtech logs.

Configure Cross Cluster Storage Settings

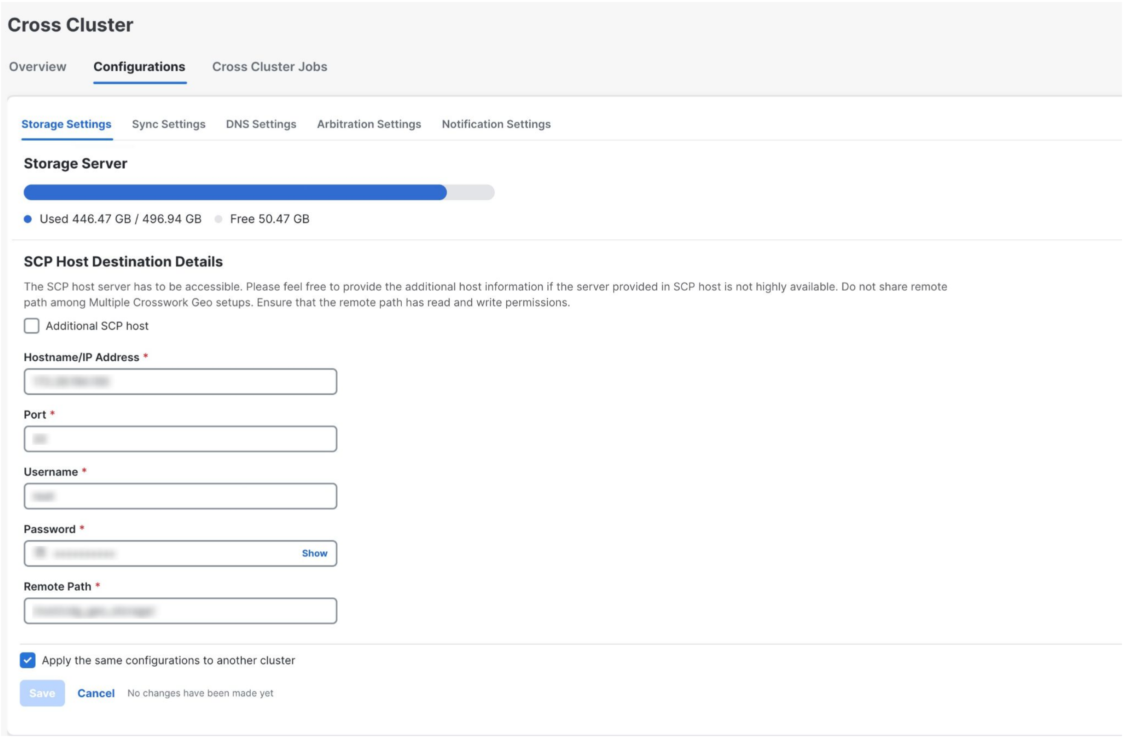
This topic explains how to configure the cross cluster storage settings.

Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed. Click on the **Configurations** tab.

The **Storage Settings** window is displayed.

Note After a SCP host is configured, you can view the used and free space available in the server.

Figure 7: Storage Settings



Cross Cluster

Storage Server

● Used 446.47 GB / 496.94 GB ● Free 50.47 GB

SCP Host Destination Details

The SCP host server has to be accessible. Please feel free to provide the additional host information if the server provided in SCP host is not highly available. Do not share remote path among Multiple Crosswork Geo setups. Ensure that the remote path has read and write permissions.

□ Additional SCP host

Hostname/IP Address * [redacted]

Port * [redacted]

Username * [redacted]

Password * [redacted] Show

Remote Path * [redacted]

☑ Apply the same configurations to another cluster

Save Cancel No changes have been made yet

Step 2 Fill all the fields provided for the SCP Host server.

To add additional SCP host, select the **Additional SCP host** checkbox. Additional SCP host is needed only when the current SCP host is not highly available across both AZs.

Step 3 (Optional) Select the checkbox to apply the same configuration to the other cluster.

Step 4 Click **Save** to save the changes.

Note **Save** is enabled only after all cross cluster settings are completed.

Configure Cross Cluster Sync Settings

This topic explains how to configure the cross cluster sync settings.

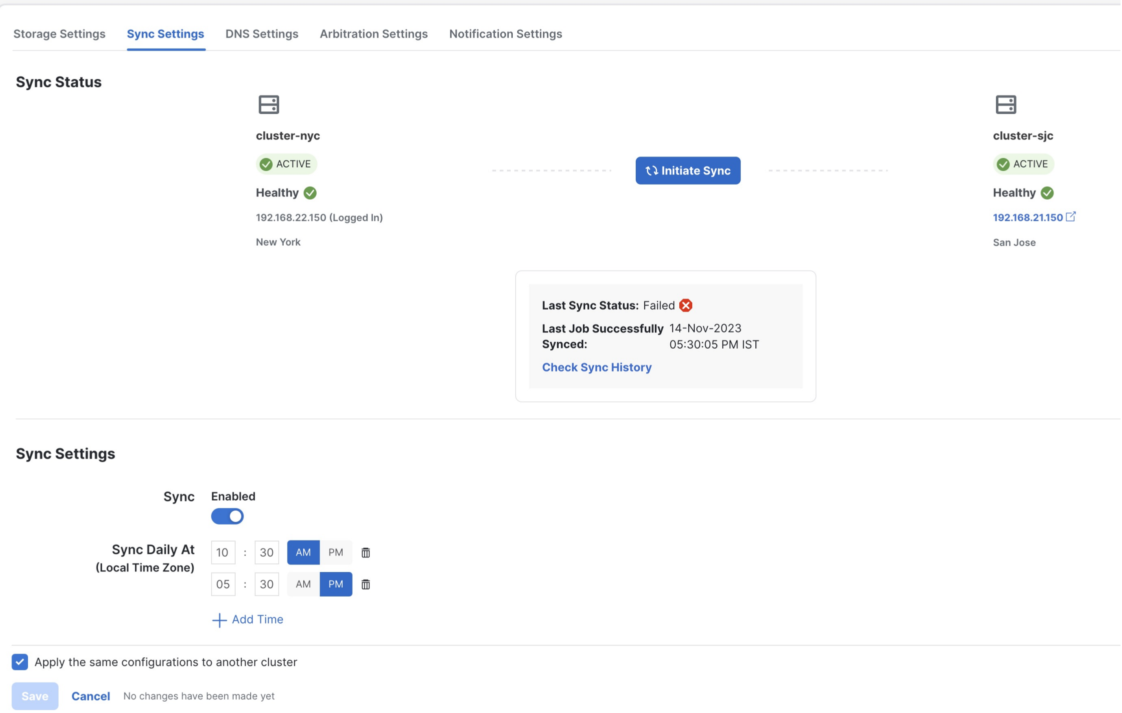
Note During the sync, the system will automatically go in to maintenance mode and can result in service disruptions. It is recommended to schedule the sync accordingly to minimize disruption to other users.

Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed. Click on the **Configurations** tab.

Step 2 Click on the **Configurations** tab, and click on the **Sync Settings**.

The **Sync Settings** window is displayed. The **Sync Status** will display the current status of the clusters. the last sync status, and the last successful sync job time.

Figure 8: Sync Settings



Sync Status

cluster-nyc
ACTIVE
Healthy ✓
192.168.22.150 (Logged In)
New York

cluster-sjc
ACTIVE
Healthy ✓
192.168.21.150
San Jose

Last Sync Status: Failed ☒
Last Job Successfully Synced: 14-Nov-2023 05:30:05 PM IST
Check Sync History

Sync Settings

Sync: Enabled
Sync Daily At (Local Time Zone): 10 : 30 AM; 05 : 30 PM

☑ Apply the same configurations to another cluster

No changes have been made yet

Step 3 (Optional) Click **Initiate Sync** to start the sync immediately. A confirmation prompt is displayed. Click **Proceed** to continue.

Important
- Do not click **Initiate Sync** without completing all other sync configurations (such as storage, DNS, and sync settings).
- Once a sync is initiated, it cannot be stopped midway.

Step 4 (Optional) To set a auto-sync schedule, toggle the **Sync Enabled** button, and set the sync times.

Note It is recommended to sync at least once every 12 hours.

Step 5 (Optional) Select the check box to apply the same configuration to the other cluster.

Step 6 Click **Save** to save the changes.

Note **Save** is enabled only after all cross cluster settings are completed.

Configure Cross Cluster DNS Settings

This topic explains how to configure the cross cluster DNS settings.

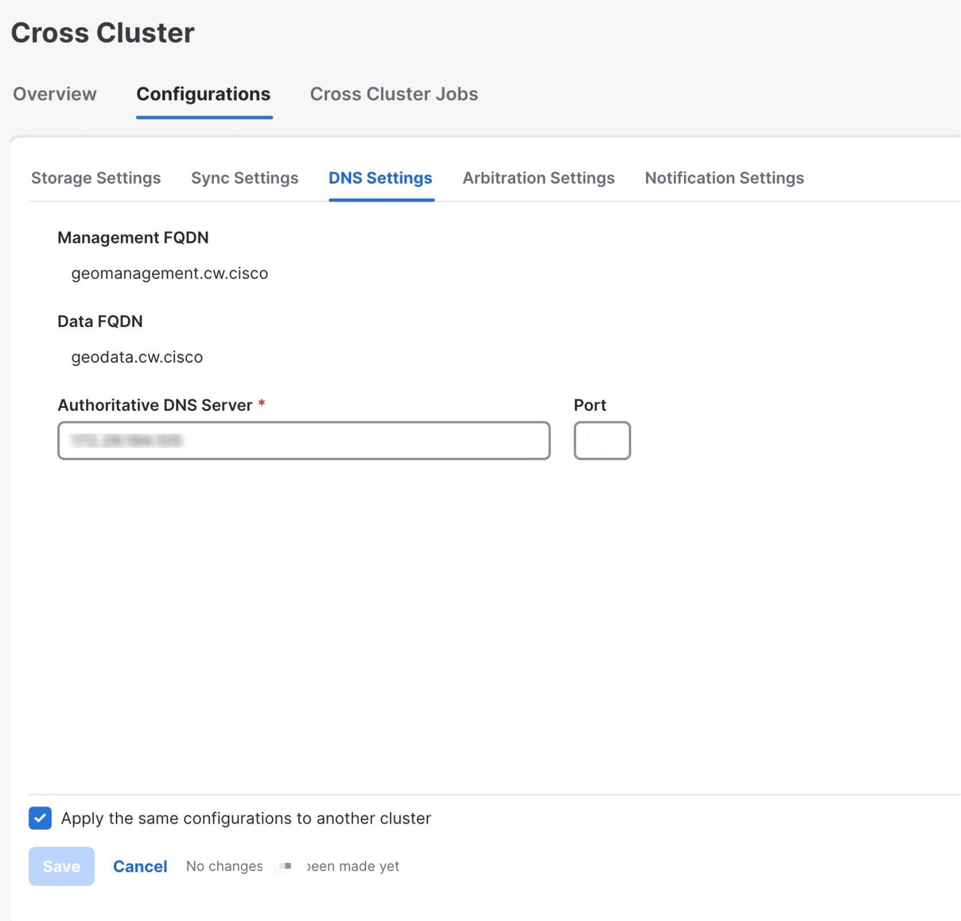
Note The DNS record TTL for FQDN must be lesser than 60 seconds (< 60s).

Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed. Click on the **Configurations** tab.

Step 2 Click on the **Configurations** tab, and click on the **DNS Settings**.

The **DNS Settings** window is displayed. The management FQDN and data FQDN details are displayed.

Figure 9: DNS Settings



Management FQDN

geomanagement.cw.cisco

Data FQDN

geodata.cw.cisco

Authoritative DNS Server *

[redacted]

Port

☑ Apply the same configurations to another cluster

No changes ▪ ›een made yet

Note The DNS server should be configured with the same management FQDN and data FQDN shown on the UI.

Step 3 Add the details for the **Authoritative DNS Server** and **Port**.

Step 4 (Optional) Select the checkbox to apply the same configuration to the other cluster.

Step 5 Click **Save** to save the changes.

Note **Save** is enabled only after all cross cluster settings are completed.

Configure Cross Cluster Arbitration Settings

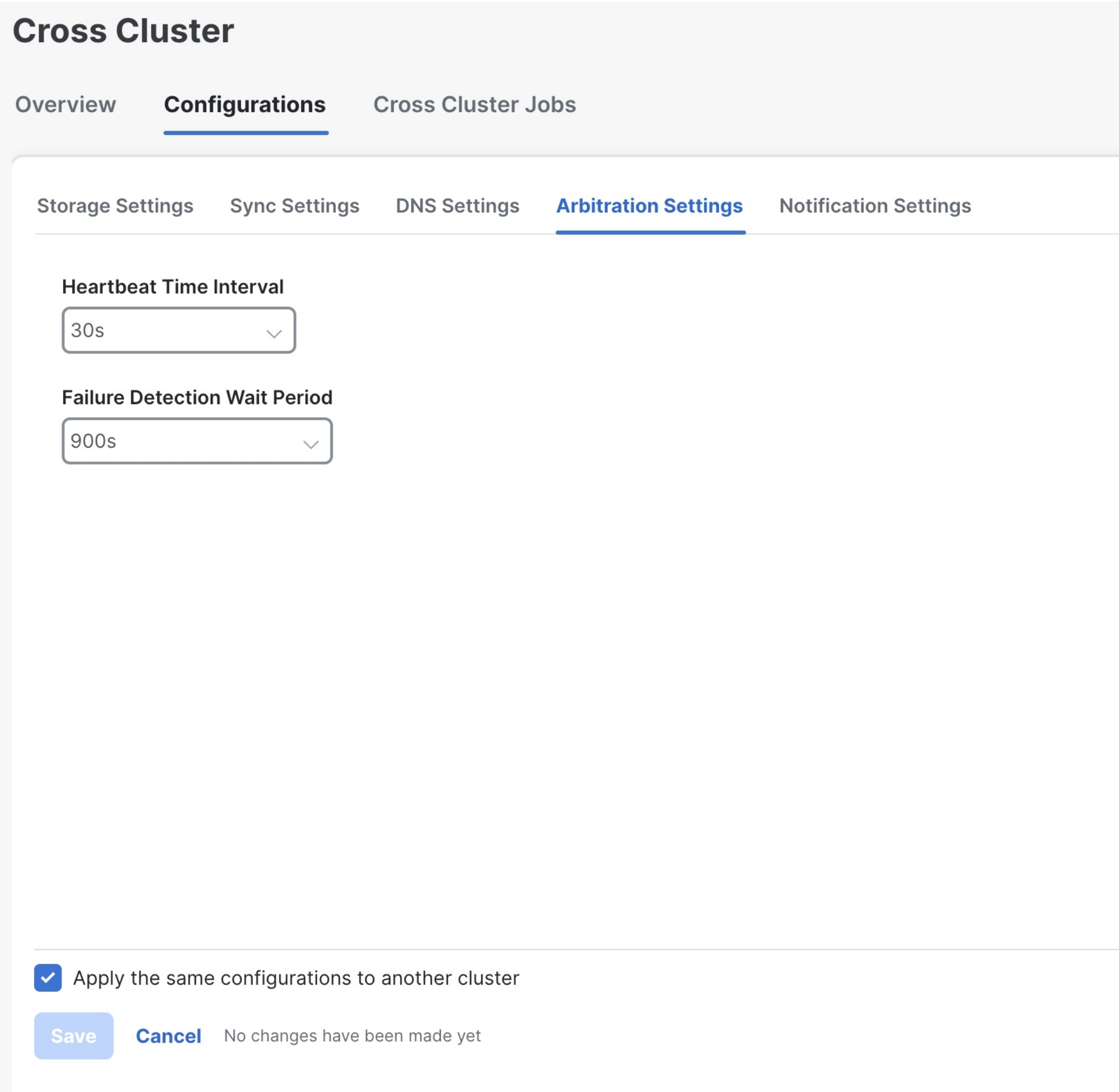
This topic explains how to configure the cross cluster arbitration settings.

Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed. Click on the **Configurations** tab.

Step 2 Click on the **Configurations** tab, and click on the **Arbitration Settings**.

The **Arbitration Settings** window is displayed.

Figure 10: Arbitration Settings



Heartbeat Time Interval: 30s

Failure Detection Wait Period: 900s

☑ Apply the same configurations to another cluster

No changes have been made yet

Step 3 Set relevant values for the **Heartbeat Time Interval** and **Failure Detection Wait Period** fields.

Step 4 (Optional) Select the checkbox to apply the same configuration to the other cluster.

Step 5 Click **Save** to save the changes.

Note **Save** is enabled only after all cross cluster settings are completed.

Configure Cross Cluster Notification Settings

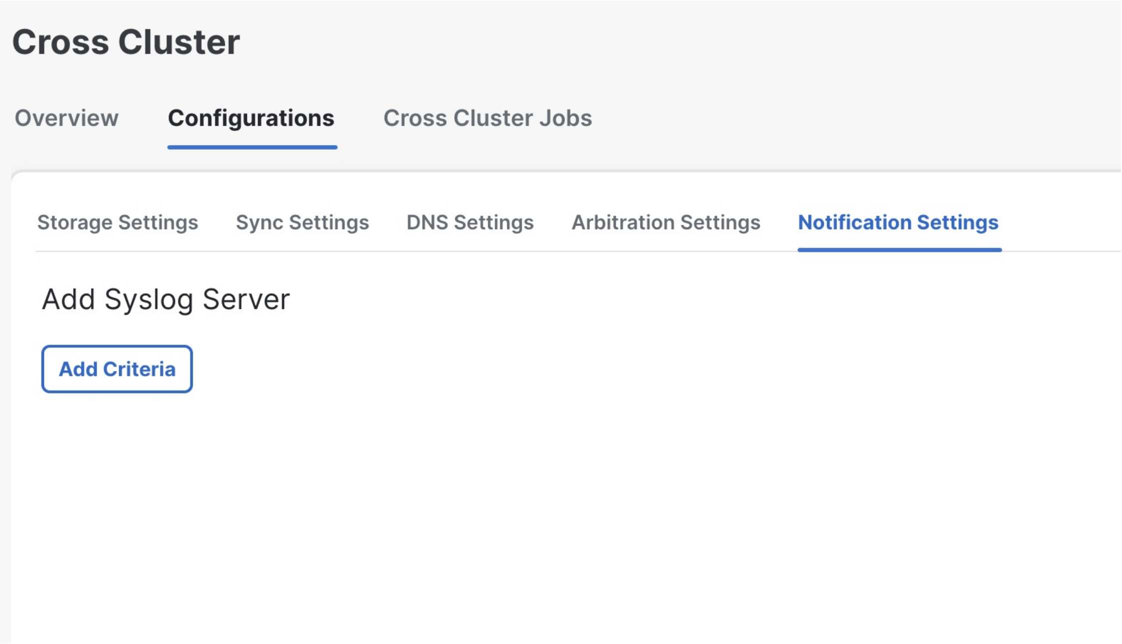
This topic explains how to configure the cross cluster notification settings.

Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed. Click on the **Configurations** tab.

Step 2 Click on the **Configurations** tab, and click on the **Notification Settings**.

The **Notification Settings** window is displayed.

Figure 11: Notification Settings



Step 3 (Optional) Click **Add Criteria** to add a syslog server.

Step 4 Once the syslog server is added, provide the relevant information for the notification settings.

Step 5 (Optional) Select the checkbox to apply the same configuration to the other cluster.

Step 6 Click **Save** to save the changes.

Note **Save** is enabled only after all cross cluster settings are completed.

Geo Redundancy Scenarios

This topic explains the expected system behavior for certain geo redundancy scenarios.

Application Installation

Table 2: Application Installation Scenarios

Scenario	Expected System Behavior
Application or version mismatch between active and standby clusters prior to enabling geo redundancy.	An equivalency check done prior to the geo redundancy enablement will identify any mismatch between the active and standby clusters (in terms of applications or versions), and prevent enablement. To proceed, please ensure that applications and versions match on both clusters.
Application or version mismatch between active and standby cluster after enabling geo redundancy.	Any configured sync operation will fail until the mismatch is corrected.
Installing an application or patch while a sync is in progress.	A sync operation can be configured as a periodic event or initiated on demand. While a sync operation is in progress, application installation will not be allowed.
Installing an application or patch when sync is not happening.	When sync is not happening, application installation is allowed.

Backup and Restore

Table 3: Backup and Restore Scenarios

Scenario	Expected System Behavior
Taking a data only backup on the active crosswork cluster.	This operation is allowed. You are recommended to make data only backup of the active cluster for the following reasons: • In case the data sync is corrupted between clusters or in the event of a disaster, you will have a point in time to roll back. • If you want to restore the cluster to a previous point in time.
Taking a data only backup on the standby crosswork cluster.	This operation is not permitted.

Scenario	Expected System Behavior
Disaster recovery from a corrupted data sync between the clusters.	This operation is allowed. In case the data sync is corrupted between clusters, you can restore the data only backup made on the active cluster and allow the normal sync flow to sync the standby cluster.
Disaster recovery where both clusters need to recovered	In the rare case that the active and standby clusters are unrecoverable or unusable, please redeploy the active and standby clusters and apply the data only backup on the active cluster. The standby will sync in the normal sync flow.
Perform restore operation on the standby cluster.	This operation is not permitted.
Perform restore operation on the active cluster.	This operation is allowed. If you want to restore a previous backup, perform the restore only on the active cluster, and allow the standby cluster will sync on the next sync cadence.

The following combinations are supported:

Table 4: Supported Backup Restore Combinations

Backup Type	From Deployment	To Deployment	Support
Data only	Geo redundant	Geo redundant	Supported
Data only	Non-geo redundant	Non-geo redundant	Supported

Any other combination is not supported.

Password Update

Follow the below sequence while updating password on a geo redundant cluster:

1. Update the password on the active cluster.
2. Wait for the sync operation to complete, and the password update is pushed to the standby cluster.
3. Update the inventory file on the active cluster.

Install Geo HA Crosswork Data Gateway

Cisco Crosswork Data Gateway is installed as a base VM that contains only enough software to register itself with Cisco Crosswork.

Note If you are redeploying the same Cisco Crosswork Data Gateway with Cisco Crosswork, delete the previous Crosswork Data Gateway entry from the Virtual Machine table under Data Gateway Management. For information on how to delete a Crosswork Data Gateway VM, see Delete Crosswork Data Gateway from the Crosswork Cluster.

To install Crosswork Data Gateway VM for use with Cisco Crosswork, follow these steps:

1. Choose the deployment profile for the Crosswork Data Gateway VM.

   For the VM requirements, see Crosswork Cluster VM Requirements.

2. Review the installation parameters and make sure that you have all the required information to install Crosswork Data Gateway using your the preferred deployment scenario. For the parameter information, see Cisco Crosswork Data Gateway Parameters and Deployment Scenarios.

3. Install Cisco Crosswork Data Gateway using yours preferred method:

   Table 5: Crosswork Data Gateway installation options

VMware	Install Cisco Crosswork Data Gateway using vCenter vSphere Client
	Install Cisco Crosswork Data Gateway via OVF Tool

4. Complete the post-installation tasks mentioned in the section Crosswork Data Gateway Post-installation Tasks.

5. Verify that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork. For information on how to verify the enrollment process, see Cisco Crosswork Data Gateway Authentication and Enrollment.

After verifying that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the Crosswork Data Gateway for collection by creating a Crosswork Data Gateway pool. For more information, see the *Create a Crosswork Data Gateway Pool* section in *Cisco Crosswork Network Controller 6.0 Administration Guide*.