Implement Disaster Recovery

Overview

Disaster recovery adds another layer of redundancy to safeguard against network downtime. It responds to a cluster failure by handing off network management duties to a connected cluster (referred to as a site going forward). Disaster recovery implementation on Catalyst Center consists of three components: the main site, the recovery site, and the witness site. At any given time, the main and recovery sites are operating in either the active or standby role. The active site manages your network while the standby site maintains a continuously updated copy of the active site's data and managed services. Whenever an active site goes down, Catalyst Center automatically initiates a failover, completing the tasks necessary to designate the former standby site as the new active site.

The following topics provide information about how to set up and use disaster recovery in your production environment.

Key Terms

The following terms are key for understanding disaster recovery implementation on Catalyst Center:

- **Main Site**: The first site you configure when setting up your disaster recovery system. By default, it operates as the active site that manages your network. For information about how to configure the sites in your system, see Set Up Disaster Recovery, on page 14.

- **Recovery Site**: The second site you configure when setting up your disaster recovery system. By default, it acts as your system's standby site.

- **Witness Site**: The third site you configure when setting up your disaster recovery system. This site, which resides on a virtual machine or separate server, is not involved with the replication of data or managed services. Its role is to give the current active site the quorum it needs to carry out disaster recovery tasks. If a site fails, this site prevents the split brain scenario from taking place. This scenario can occur in a two-member system when the sites cannot communicate with each other. Each site believes that it should become active, creating two active sites. Catalyst Center uses the witness site to arbitrate between the active and standby sites, allowing only one active site at any given time. For information about witness site requirements, see Prerequisites, on page 6.

- **Register**: To add a site to a disaster recovery system, you must first register it with the system by providing information such as your main site's VIP. When registering your recovery or witness site, you will also need to provide the token that is generated when you register your main site. For more information, see Set Up Disaster Recovery, on page 14.

- **Configure Active**: The process of establishing a site as the active site, which involves tasks such as exposing the appropriate managed service ports.

- **Active site**: The site that is currently managing your network. Catalyst Center continuously replicates its data to your standby site.

- **Configure Standby**: The process of establishing a site as the standby site, which involves tasks such as configuring the replication of the active site's data and disabling the services which manage the network on the standby site.

- **Standby Ready**: When an isolated site meets the prerequisites to become a standby site, Catalyst Center moves it to this state. To establish this site as your system's standby site, click **Rejoin** in the **Action** area.

- **Standby site**: The site that maintains an up-to-date copy of your active site's data and managed services. If your active site goes down, your system initiates a failover and your standby site takes over as the active site.

> **Note** A message will indicate when you are currently viewing your system's standby site. You need to initiate all disaster recovery tasks from the active site.

- **Failover**: Catalyst Center supports two types of failover:

  - System-triggered: As soon as Catalyst Center recognizes that your active site has gone down, it automatically carries out the tasks required to establish your standby site as the new active site. You can monitor these tasks from the Monitor the Event Timeline.

  - Manual: You can initiate a manual failover to designate the current standby site as the new active site. For more information, see Initiate a Manual Failover, on page 30.

☞

Important

- After a failover, Assurance restarts and processes a fresh set of data on the new active site. Historical Assurance data from the former active site is *not* migrated over.

- After a failover, the Catalyst Center inventory service triggers a full device sync. This can take anywhere from a few minutes to a few hours, depending on the number of devices that are managed. As is the case when Catalyst Center's normally scheduled device sync is running, you will not be able to provision devices on the newly activated cluster until the device sync triggered by a failover completes.

- **Isolate**: During a failover, the former active site is separated from the disaster recovery system. Catalyst Center suspends its services and stops advertising its virtual IP address (VIP). From here, Catalyst Center completes the tasks necessary to establish the former standby site as the new active site.

- **Pause**: Temporarily suspend your disaster recovery system in order to separate the sites that make up your system and stop data and service replication. For more information, see Pause Your Disaster Recovery System, on page 25.

- **Rejoin**: From the **Disaster Recovery** > **Monitoring** tab, click this button in the **Action** area in order to add a Standby Ready or Paused site back into a disaster recovery system as the new standby site (after a failover has taken place). You would also click this button in order to restart a disaster recovery system that is currently paused.

- **Activate DR**: User-initiated operation that creates your system's active and standby sites. This operation entails setting up intracluster communication, verifying that the sites meet disaster recovery prerequisites, and replicating data between the two sites.

- **Deregister**: Click this button in the **Action** area to remove the three sites you have configured for your disaster recovery system. You must do so in order to make changes to any of the site settings you have entered previously.

- **Retry**: In the **Action** area, click this button in order to reinitiate any action that failed previously.

- **VIP Promotion**: When this option is enabled, the Enterprise interface VIP configured for your Catalyst Center deployment is promoted for use as your system's disaster recovery VIP. For more information, see the "VIP Promotion" section in Main Site Registration Considerations, on page 14.

Data Replication Overview

The data replication process syncs data between your disaster recovery system's main site and recovery site. Its duration depends on a few factors: the amount of data that needs to be replicated, your network's effective bandwidth, and the amount of latency that exists between the main and recovery sites. When disaster recovery is active for your Catalyst Center deployment, data replication will *not* impact any operations or application use on the current active site (which is managing your network).

☞

Important

After a failover takes place, Assurance data from the site that failed is *not* replicated. The site that takes over as your system's active site will collect a new set of Assurance data.

Either a full or incremental replication of data takes place, depending on which of the following scenarios is applicable:

- **After initial activation**: After the initial configuration and activation of your disaster recovery system, the recovery site does not have any data. In this scenario, a full replication of data between the main and recovery sites happens.

- **After a failover**: Whenever the current active site fails, the disaster recovery system triggers a failover. In this scenario, a full data replication between the main and recovery sites occurs after the failed site rejoins the system.

- **During normal operation**: This scenario will typically apply to your system. During its day-to-day operation, changes that take place on the current active site are continuously synced with the current standby site.

Navigate the Disaster Recovery GUI

The following table describes the components that make up Catalyst Center's disaster recovery GUI and their function.

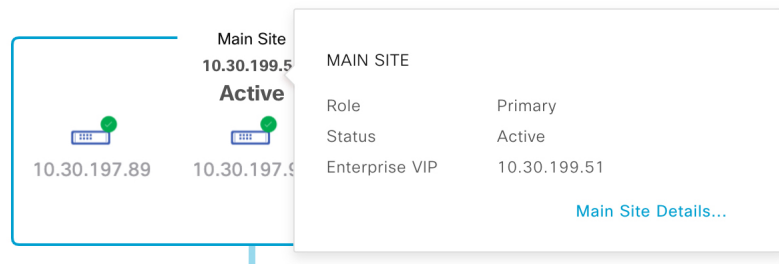| Callout	Description
1	**Monitoring** tab: Click to do the following: • View a topology of the sites that make up your system. • Determine the current status of your system. • Perform disaster recovery tasks. • View a listing of the tasks that have been completed to date.
2	**Show Detail Information** link: Click to open the **Disaster Recovery System** slide-in pane. See View Disaster Recovery System Status, on page 5 for more information.
3	**Topology**: Displays either a logical or physical topology of your system that indicates the current status of your sites and their members. • In both the logical and physical topologies, a blue box indicates the site that's currently acting as your system's active site. • In the logical topology, a blue line indicates that the IPSec tunnel connecting two sites is operational, and a red line indicates that the tunnel is currently down. • To view a description of the possible site states, see System and Site States, on page 41.
4	**Event Timeline**: Lists every disaster recovery task that is currently in progress or has been completed for your system. For more information, see Monitor the Event Timeline, on page 38.
5	**Configure** tab: Click to enter the settings necessary to establish a connection between your disaster recovery system's sites. See Set Up Disaster Recovery, on page 14 for more information.
6	**Logical** and **Physical** tabs: Click the appropriate tab to toggle between a logical and physical topology of your system.
7	**Status** area: Indicates the current status of your system. To view a description of the possible system states, see System and Site States, on page 41.
8	**Legend**: Indicates what the topology icons represent. To view the legend, click ⊙ in the bottom right corner of the **Disaster Recovery** window.
9	**Interactive Help** button: Click to open a slide-in pane that provides links to walkthroughs that provide on-screen guidance to help you complete specific tasks in Catalyst Center.
10	**Action** area: Displays the disaster recovery tasks that are currently available for you to initiate. The tasks you can choose from vary, depending on whether you have configured your sites and your system's status.

View Disaster Recovery System Status

The topology provides a graphical representation of your disaster recovery system's current status. If you want to view this information in a tabular format, you can do so in the **Disaster Recovery System** slide-in pane. To open this pane, do one of the following:

• Click the **Show Detail Information** link. Then expand the site for which you want to view the status in the slide-in pane.

• In the topology, place your cursor over a site's Enterprise virtual IP address or a particular node's icon. In the dialog box that opens, click the link in the bottom-right corner of the window.

Main Site
10.30.199.5
Active

10.30.197.89   10.30.197.9

MAIN SITE

Role	Primary
Status	Active
Enterprise VIP	10.30.199.51

Main Site Details...

The slide-in pane opens and displays the relevant site information.

Disaster Recovery System

| Status | Up and Running |

Main Site

Role	Primary
Status	Active
Enterprise VIP	10.30.199.51

IPSEC STATUS

| Tunnel Main-Recovery | 🔒 Up |
| Tunnel Main-Witness | 🔒 Up |

NODE

Status	✅ Up	✅ Up	✅ Up
Enterprise IP	10.30.197.89	10.30.197.90	10.30.197.99
Cluster IP	29.30.197.89	29.30.197.90	29.30.197.99

Prerequisites

Before you enable disaster recovery in your production environment, ensure that the following prerequisites have been met.

Witness Prerequisites

☞

Important

- If you plan to upgrade to Catalyst Center 2.3.7.5, you must complete several steps to ensure that disaster recovery works properly after the upgrade. See Configure Disaster Recovery on an Upgraded Catalyst Center Appliance, on page 10.

- Note that disaster recovery does not support IPv6.

General Prerequisites

- Catalyst Center supports two disaster recovery setups:

  - **1+1+1 setup**: One Catalyst Center appliance functions as your Main Site, a second appliance serves as your Recovery Site, and a third system (residing on a virtual machine) acts as your Witness Site. The following appliances and versions support this setup:

    - DN2-HW-APL (44-core second-generation appliance): Catalyst Center 2.2.2.x and later

    - DN3-HW-APL (32-core third-generation appliance): Catalyst Center 2.2.2.x and later

    - DN2-HW-APL-L (56-core second-generation appliance): Catalyst Center 2.2.1.x and later

    - DN3-HW-APL-L (56-core third-generation appliance): Catalyst Center 2.2.1.x and later

    - DN2-HW-APL-XL (112-core second-generation appliance): Catalyst Center 2.2.1.x and later

    - DN3-HW-APL-XL (80-core third-generation appliance): Catalyst Center 2.2.1.x and later

  - **3+3+1 setup**: One three-node Catalyst Center cluster functions as your Main Site, a second three-node cluster serves as your Recovery Site, and a third system (residing on a virtual machine) acts as your Witness Site. The following appliances and versions support this setup:

    - DN2-HW-APL (44-core second-generation appliance): Catalyst Center 2.2.2.x and later

    - DN3-HW-APL (32-core third-generation appliance): Catalyst Center 2.2.2.x and later

    - DN2-HW-APL-L (56-core second-generation appliance): Catalyst Center 2.1.2.x and later

    - DN3-HW-APL-L (56-core third-generation appliance): Catalyst Center 2.1.2.x and later

    - DN2-HW-APL-XL (112-core second-generation appliance): Catalyst Center 2.1.2.x and later

    - DN3-HW-APL-XL (80-core third-generation appliance): Catalyst Center 2.1.2.x and later

- You have configured a VIP for the Enterprise port interface on your Catalyst Center appliances. This is required because disaster recovery uses the Enterprise network for intrasite communication. In the Catalyst Center Second-Generation Appliance Installation Guide, refer to the following:

  - For more information about the Enterprise port, see the "Interface Cable Connections" topic.

  - For more information about Enterprise port configuration, see either the "Configure the Primary Node Using the Maglev Wizard" or "Configure the Primary Node Using the Advanced Install Configuration Wizard" topic.

- You have assigned a super-admin user to carry out disaster recovery tasks. Only users with this privilege level can access this functionality.

- You have confirmed that the links connecting the following sites are 1 Gbps with at most 350 ms RTT latency.

  - Main and recovery sites

  - Main and witness sites

  - Recovery and witness sites

- You have generated one third-party certificate and installed the same certificate on both the main and recovery sites. Otherwise, site registration will fail.

> **Note** Catalyst Center copies this certificate to the witness site automatically during the registration process.

  Ensure that all of the IP addresses (especially the Enterprise port's virtual IP address) and fully qualified domain names (**FQDN**) that the main and recovery sites use are included in this certificate. Also ensure that **nonRepudiation** and **digitalSignature** are specified for the certificate's **keyUsage** parameter. For a description of how to generate a third-party certificate, see Generate a Certificate Request Using Open SSL in the *Catalyst Center Security Best Practices Guide*.

- You have opened all of the ports listed in the Catalyst Center Security Best Practices Guide's "Disaster Recovery Ports" topic.

- If you are using an FQDN-only certificate, ensure that the same **cluster_hostname**—that is, the FQDN for Catalyst Center (set in the Catalyst Center configuration wizard)—is configured on both the main and recovery sites, as well as Disaster Recovery's VIP.

Main and Recovery Site Prerequisites

- Both your main and recovery site must consist of the same number of nodes. Catalyst Center will not allow you to register and activate a disaster recovery system that does not meet this requirement.

- Both your main and recovery site must consist of Catalyst Center appliances that have the same hardware profile. For example, a site can consist of second-generation 112-core and third-generation 80-core appliances. The following table lists the appliances that support disaster recovery and their corresponding Cisco part number:

Table 1: Supported Catalyst Center Appliances

Hardware Profile	Cisco Part Numbers

Regular	• Second-generation 44-core appliance:
	    • DN2-HW-APL
	    • DN2-HW-APL-U
	
	• Third-generation 32-core appliance: DN3-HW-APL

Hardware Profile	Cisco Part Numbers

Large	• Second-generation 56-core appliance:
	
	   • DN2-HW-APL-L
	
	   • DN2-HW-APL-L-U
	
	• Third-generation 56-core appliance: DN3-HW-APL-L

Extra Large	• Second-generation 112-core appliance:
	
	   • DN2-HW-APL-XL
	
	   • DN2-HW-APL-XL-U
	
	• Third-generation 80-core appliance: DN3-HW-APL-XL

Also ensure that your main and recovery site are running the same Catalyst Center version.

- You have configured and enabled high availability (HA) on both your main and recovery site. Otherwise, the registration of these sites will fail. For more information, see the latest Catalyst Center High Availability guide.

☞

Important   This is applicable to three-node setups only.

- Ensure that the main and recovery site have the same Federal Information Processing Standards (FIPS) mode setting. If FIPS mode is enabled on one site and disabled on the other, the registration of your disaster recovery system will fail due to a validation error. For more information on FIPS mode, see the description of the **IP addressing mode used for the services** screen (located in the Catalyst Center Second-Generation Appliance Installation Guide's "Configure the Primary Node Using the Maglev Wizard" topic).

- If you want to use Border Gateway Protocol (BGP) to advertise your system's virtual IP address routes, you need to configure your system's Enterprise virtual IP address on each of the main and recovery site's neighbor routers. The configuration you need to enter will look similar to one the following examples:

Interior BGP (iBGP) Configuration Example

```
router bgp 64555
 bgp router-id 10.30.197.57
 neighbor 172.25.119.175 remote-as 64555
 neighbor 172.25.119.175 update-source 10.30.197.57
 neighbor 172.25.119.175 next-hop-self
```

where:

- `64555` is the neighbor router's local and remote AS number.

- `10.30.197.57` is the neighbor router's IP address.

- `172.25.119.175` is your system's Enterprise virtual IP address.

Exterior BGP (eBGP) Configuration Example

```
router bgp 62121
 bgp router-id 10.30.197.57
 neighbor 172.25.119.175 remote-as 64555
 neighbor 172.25.119.175 update-source 10.30.197.57
 neighbor 172.25.119.175 next-hop-self
 neighbor 172.25.119.175 ebgp-multihop 255
```

where:

- `62121` is the neighbor router's local AS number.

- `64555` is the neighbor router's remote AS number.

- `10.30.197.57` is the neighbor router's IP address.

- `172.25.119.175` is your system's Enterprise virtual IP address.

- If you enable BGP route advertisement (as described in the previous bullet), we recommend that you filter routes towards Catalyst Center in order to improve its performance. To do so, enter the following configuration:

```
neighbor system's-Enterprise-virtual-IP-address route-map DENY_ALL out
!
ip prefix-list DENY_ALL seq 5 deny 0.0.0.0/0 le 32
!
route-map DENY_ALL permit 10
match ip address prefix-list DENY_ALL
```

Witness Site Prerequisites

- You have confirmed that the virtual machine that hosts your witness site is running (at a minimum) VMware ESXi hypervisor version 7.0 or later with a 2.1-GHz core and two virtual CPUs, 4 GB of RAM, and 10 GB of hard drive space.

- Witness site deployment in a public cloud is not supported.

- You have set up your witness site in a different location than your main and recovery sites and confirmed that it is reachable from both of these sites.

- You have configured an NTP server that is accessible by the witness site. You must synchronize this NTP server with the NTP servers that are used by the main and recovery sites.

- The witness site utilizes approximately 50 Mbps of actual bandwidth. This bandwidth is used primarily for monitoring the connections (WAN, LAN, private circuits) between the witness site and the primary/standby sites.

Configure Disaster Recovery on an Upgraded Catalyst Center Appliance

To successfully configure disaster recovery after upgrading your system to the latest Catalyst Center version, complete the following steps:

Step 1   Install the Witness Site, on page 12.

Step 2   Set Up Disaster Recovery, on page 14.

Add the Disaster Recovery Certificate

Catalyst Center supports the import and storage of an X.509 certificate and private key into Catalyst Center. The disaster recovery certificate is used for intracluster communications.

You must obtain a valid X.509 certificate that is issued by your internal CA and the certificate must correspond to a private key in your possession.

Note

- If you want your disaster recovery system to use the same certificate that Catalyst Center uses, you can skip this procedure. When you configure the certificate, make sure that you check the **Use system certificate for Disaster Recovery as well** check box (see Update the Catalyst Center Server Certificate).

- For more information about the disaster recovery certificate requirements, reference the Security Best Practices Guide.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **Certificates** > **Disaster Recovery**.

Step 2 In the **Add Certificate** area, choose the file format type for the certificate that you are importing into Catalyst Center:

- **PEM**: Privacy-enhanced mail file format

- **PKCS**: Public-Key Cryptography Standard file format

Step 3 If you chose **PEM**, perform the following tasks:

a) Import the certificate by dragging and dropping the PEM file into the highlighted area.

Note A PEM file must have a valid PEM format extension (.pem). The maximum file size for the certificate is 10 MB.

After the upload succeeds, the system certificate is validated.

b) In the **Private Key** area, import the private key by dragging and dropping it into the highlighted area.

Note Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 10 MB.

After the upload succeeds, the private key is validated.

c) Specify whether the private key will be encrypted by clicking the appropriate radio button.

d) If the private key will be encrypted, enter its password in the **Password** field.

Step 4 If you chose **PKCS**, perform the following tasks:

a) Import the certificate by dragging and dropping the PKCS file into the highlighted area.

Note A PKCS file must have a valid PKCS format extension (.pfx or .p12). The maximum file size for the certificate is 10 MB.

After the upload succeeds, the system certificate is validated.

b) In the **Password** field, enter the certificate's password (a PKCS requirement).

c) Specify whether the private key will be encrypted by clicking the appropriate radio button.

     d)   If the private key will be encrypted, enter its password in the **Password** field.

Step 5   Click **Save**.

After the Catalyst Center server's SSL certificate is replaced, you are automatically logged out and you must log in again.

Install the Witness Site

Complete the following procedure to set up the virtual machine that will serve as the witness site for your disaster recovery system.

Step 1   Download the OVF package that's specific to the Catalyst Center version that the witness site is running:

     a)   Open https://software.cisco.com/download/home/286316341/type.

        Note   You need a Cisco.com account to access this URL. See the following page for a description of how to create an account: https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html

     b)   In the **Select a Software Type** area, click the Catalyst Center software link.

The **Software Download** page updates, listing the software that's available for the latest Catalyst Center release.

     c)   Do one of the following:

          • If the OVF package (*.ova) you need is already listed, click its **Download** icon.

          • Enter the relevant version number in the **Search** field, click its link in the navigation pane, and then click the **Download** icon for that version's OVF package.

Step 2   Copy this package to a local machine running VMware vSphere 7.0 or later.

Step 3   From the vSphere client, choose **File** > **Deploy OVF Template**.

Step 4   Complete the **Deploy OVF Template** wizard:

     a)   Do the following in the wizard's **Source** screen:

         1.   Click **Browse**.

         2.   Navigate to the witness site's OVF package (.ova).

         3.   Click **Open**.

         4.   In the **Deploy from a file or URL** field, verify that the package's path is displayed and then click **Next**.

The wizard's **OVF Template Details** screen opens.

     b)   Click **Next >**.

     c)   Do the following in the wizard's **Name and Location** screen:

          • In the **Name** field, enter the name you want to set for the package.

          • In the **Inventory Location** field, select the folder that you want the package to reside in.

          • Click **Next >**.

The wizard's **Host/Cluster** screen opens.

d) Click the host or cluster on which you want to run the deployed template and then click **Next >**.

The wizard's **Storage** screen opens.

e) Click the storage drive that the virtual machine files will reside on and then click **Next >**.

The wizard's **Disk Format** screen opens.

f) Click the **Thick Provision** radio button and then click **Next** .

g) Do the following in the wizard's **Network Mapping** screen and then click **Next** :

1. Click the IP address that is listed in the **Destination Networks** column.

2. In the resulting drop-down list, choose the network that the deployed template should use.

The wizard's **Ready to Complete** screen opens, displaying all of the settings that you have entered.

h) Check the **Power on after deployment** check box and then click **Finish**.

i) When the **Deployment Completed Successfully** dialog box opens, click **Close**.

Step 5   Enter the network settings for your witness site:

a) Open a console to the virtual machine you just created by doing one of the following:

• Right-click the virtual machine from the vSphere Client list and choose **Open Console**.

• Click the **Open Console** icon in the vSphere Client menu.

The **Witness User Configuration** window opens.

b) Enter and confirm the desired password for the admin user (*maglev*), then press **N** to proceed.

c) Enter the following settings, then press **N** to proceed:

• Its IP address

• The netmask associated with the virtual machine's IP address

• The IP address of your default gateway

• **(Optional)** The IP address of the preferred DNS server

d) Enter one or more NTP server addresses or hostnames (separated by spaces), then press **S** to submit your settings and begin the configuration of the witness site.

At least one NTP address or hostname is required.

e) Verify that configuration has completed by using SSH port 2222 to log in to the IP address you configured for the witness site.

Note   Later, if you need to change the password configured for the **maglev** user on the witness site's VM, use the standard Linux **passwd** utility. You don't need to pause the disaster recovery system before doing this, and the password change will have no functional impact on disaster recovery operation.

Set Up Disaster Recovery

Setting up disaster recovery in your Catalyst Center deployment is a two-step process. The first step is to register the sites that will comprise your disaster recovery system. The second step is to activate your system, enabling disaster recovery. Refer to this section's topics for a description of the steps you need to complete, as well as information on the errors you may encounter during this process and how to deal with them.

Main Site Registration Considerations

Before you register your disaster recovery system's main site, you'll need to decide how to make use of the following features.

VIP Promotion

You'll need to decide is whether you want to use the Enterprise interface VIP configured for your Catalyst Center deployment as your system's disaster recovery VIP. VIP promotion is suitable only if all of the following items are applicable:

- You have a brownfield deployment, where an existing Catalyst Center instance is managing the network and all devices are configured with the instance's Enterprise VIP. This instance will act as your disaster recovery system's main site.

- The existing Enterprise interface VIP address is allowed to float between the two data centers where your main and recovery sites will reside. This is usually applicable in the case of an extended L2 network that spans multiple data centers.

- You don't want the existing devices to be reconfigured when the new disaster recovery system's Enterprise interface VIP.

If you want to use VIP promotion, complete Steps 2b through 2e in , clicking the **Yes** radio button in Step 2b.

Route Advertisement Options

You'll then need to decide the route advertisement option your deployment will use. One of disaster recovery's main objectives is to enable continuous network operation after a failover takes place without the need for device reprovisioning. This is achieved by specifying a floating VIP that's automatically configured on the disaster recovery system's current active site. Whenever a failover occurs, this VIP (referred to as the disaster recovery VIP in this chapter) is cleared from the previous active site and set on the new active site. This ensures that your network's devices can continue to communicate with Catalyst Center, regardless of which site is currently active. There are three route advertisement option to choose from when you complete Step 2g in :

- **Border Gateway Protocol (BGP)**: This option, which is recommended for most disaster recovery systems, is selected by default. BGP route advertisement ensures that you can access your system's current active site, which is critical after a failover takes place.

☞

Important If you want to use this option, first complete the steps described in the last two bullets of the "Main and Recovery Site Prerequisites" section (which can be found in the topic).

- **Disaster recovery VIPs without route advertisement**: Choose this option if you want to configure virtual IP addresses for your system whose routes are not advertised using BGP. This option is suitable for data centers where both the main and recovery sites can access the subnet that the system's global virtual IP addresses reside within.

- **No disaster recovery VIPs**: When this option is selected, the virtual IP address that's configured for a site is automatically configured on the devices that belong to that site. Each time a failover takes place, this virtual IP address is reconfigured on the devices.

Register the Main Site

Complete the following procedure to register your system's main site.

Before you begin

- Ensure that you've reviewed Main Site Registration Considerations, on page 14.

- On the Catalyst Center appliances or clusters where your disaster recovery system's main and recovery site will reside, do the following:

    - Configure the same backup schedule and proxy server. If you don't take care of this before you activate your system, you'll need to specify these two settings again after a failover occurs and the recovery site becomes the active site.

    - Configure an NFS backup configuration where each site points to a different NFS device.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default.

Step 2 Register your main site:

a) Click the **Configure** tab.

The **Main Site** radio button should already be selected.

Monitoring | Configure

Set up this cluster to be the ● Main Site ○ Recovery Site

Convert the cluster VIPs to the disaster recovery VIPs >
● Yes ⓘ [Recommended]   ○ No ⓘ

⚠ Reverting to the original state after cluster VIPs are promoted is a lengthy process involving manual steps. Make sure that the replacement VIP addresses are unique and are in the same enterprise and management subnets as the original VIPs respectively.

Turn the cluster enterprise VIP, [_____] to the disaster recovery enterprise VIP

New main site enterprise VIP*
Enter replacement enterprise VIP of main site

☑ Turn the cluster management VIP, [_____] to the disaster recovery management VIP

New main site management VIP*
Enter replacement management VIP of main site

Status: Unconfigured

Please complete registration for all three sites in the order of Main, Recovery, and Witness. Then configure/activate the disaster recovery system from the Main Site.

Promote

b) In the **Convert the cluster VIPs to the disaster recovery VIPs** area, click one of the following radio buttons:

- Click **Yes** to set up a cluster as the main site and automatically propagate virtual IP address changes to the devices that are connected to this cluster. This is accomplished by promoting the virtual IP addresses that are currently configured for the cluster and assigning them as your disaster recovery system's global virtual IP addresses. We recommend choosing this option if you are enabling disaster recovery on a cluster that has a lot of connected devices. Otherwise, these devices will need to be reconfigured to communicate with the new disaster recovery virtual IP address. If you choose this option, do the following:

   1. In the **New main site enterprise VIP** field, enter a new virtual IP address for the site's Enterprise network. This will replace the address that is going to be promoted. Ensure that it is a unique address that is not already used and that it resides in the same subnet as the previous virtual IP address.

   2. (Optional) Check the **Turn the cluster management VIP, <IP-address>, to the disaster recovery management VIP** check box.

   3. (Optional) In the **New main site management VIP** field, enter a new virtual IP address for the site's Management network. This will replace the address that is going to be promoted. Ensure that it is a unique address that is not already used and that it resides in the same subnet as the previous virtual IP address.

- Click **No** to set up a cluster as the main site without propagating virtual IP address changes to connected devices. We recommend this option for a brand-new cluster that isn't connected to any devices yet or is only connected to a few devices. If you choose this option, skip ahead to Step 2f.

c) In the **Action** area, click **Promote**.

The **Disaster Recovery VIP Promotion** dialog opens.

d) Click **Continue**.

Catalyst Center validates the virtual IP addresses you entered.

e) In the **Details** area, view the validation status:

- If any of the addresses you entered are invalid (likely because it doesn't reside in the same subnet as the address it's replacing), make the necessary corrections and repeat Step 2c.

- If the addresses you entered are successfully validated, the **Details** area lists all of the virtual IP addresses that will be configured for your disaster recovery system. Proceed to the next step.

f) Enter the following information in the **Site VIP/IPs** area:

- **Main Site VIP**: The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network. Catalyst Center prepopulates this field, based on your system's information.

- **Recovery Site VIP**: The Enterprise virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network.

- **Witness Site IP**: The IP address that manages traffic between the witness site's virtual machine and your Enterprise network.

Important   Ensure that the addresses that you enter are currently reachable. Otherwise, the registration of your system's sites will fail.

Note   At any point between Steps 2f and Step 2j, you can click **Reset** to clear all of the settings that you have entered. You will then need to repeat Step 2f and enter the correct settings before you register the main site.

g) Click one of the following radio buttons in the **Route advertisement** area:

- **Border Gateway Protocol (BGP)**

- **Disaster recovery VIPs without route advertisement**

- **No disaster recovery VIPs**: Skip ahead to Step 2k if you click this radio button.

h) If you clicked either of the first two radio buttons in the previous step, enter a value in the **Enterprise VIP for Disaster Recovery** field.

When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Enterprise network.

Note
- If you clicked the **Border Gateway Protocol (BGP)** radio button and don't want to configure a Management virtual IP address, skip ahead to Step 2j.

- If you clicked the **Disaster recovery VIPs without route advertisement** radio button and don't want to configure a Management virtual IP address, skip ahead to Step 2k.

i) (Optional) Enter a value in the **Management VIP for Disaster Recovery** field.

When configured, this floating virtual IP address automatically moves to and operates on the site that is currently acting as your network's active site. This address manages traffic between your disaster recovery system and your Management network.

j) If you clicked the **Border Gateway Protocol (BGP)** radio button, enter the information required to enable route advertisement:

- In the **Border Gateway Protocol Type** area, specify whether your BGP peers will establish exterior (**Exterior BGP (eBGP)**) or interior (**Interior BGP (iBGP)**) sessions with one another.

- In the **Main Site Router Settings for Enterprise Network** and **Recovery Site Router Settings for Enterprise Network** areas, enter the IP address of the remote router that Catalyst Center will use to advertise the Enterprise virtual IP address that's configured for the disaster recovery system's Main and Recovery sites. Also enter the router's remote and local AS numbers.

  Note the following points:

  - Click the **Add** (+) icon if you want to configure an additional remote router. You can configure a maximum of two routers for each site.

  - When entering an AS number, ensure that it's a 32-bit unsigned number that falls within the 1–4,294,967,295 range.

  - When the **iBGP** option is selected, Catalyst Center will automatically set the local AS number to the value you enter as the remote AS number.

  - If you configured a Management virtual IP address in the previous step, the **Main Site Router Settings for Management Network** and **Recovery Site Router Settings for Management Network** areas are also displayed. Enter the appropriate information for the remote router that Catalyst Center will use to advertise this virtual IP address.

k) From the **Action** area, click **Register**.

   The **Disaster Recovery Registration** dialog opens.

l) Click **Continue**.

   The token that your recovery and witness sites need to use in order to register with your main site is generated.

Step 3   In the **Details** area, click **Copy Token**.

Main Site Registration Errors

You may encounter errors when registering your system's main site. This topic describes these errors and how to deal with them.

Validation Type	Validation Made	Error Resolution
VIP reachability	Checks whether a TCP socket can be opened on the recovery site's port 443.	Make sure the recovery site's VIP matches the Enterprise VIP configured for the recovery site's Catalyst Center instance and that it's reachable from the main site.
	Checks whether a TCP socket can be opened on the witness site's port 2222.	Make sure the witness site's IP address is configured correctly and reachable from the main site.
Enterprise and Management interface VIP reachability	Confirms whether the disaster recovery system's VIP can be reached via the Enterprise interface by looking for the following items: • A static route defined on the Enterprise interface for the disaster recovery system's VIP • A default gateway configured on the Enterprise interface If neither of these items are present, the validation fails.	Define either a static route on the Enterprise interface for the disaster recovery system's Enterprise VIP or a default gateway on the Enterprise interface.
	Confirms whether the disaster recovery system's VIP can be reached via the Management interface by looking for the following items: • A static route defined on the Management interface for the disaster recovery system's VIP • A default gateway configured on the Management interface If neither of these items are present, the validation fails.	Define either a static route on the Management interface for the disaster recovery system's Management VIP or a default gateway on the Management interface.

Validation Type	Validation Made	Error Resolution
Certificate upload	Confirms whether a third-party certificate has been uploaded. If so, Catalyst Center also confirms that the certificate is not self-signed.	
	In the **System Certificates** page (**System** > **Settings** > **Certificates** > **System Certificates**), checks that one of the following is true: • The **Use System Certificate for Disaster Recovery as well** option is selected. • A certificate that's specific to disaster recovery has been uploaded. In both cases, the certificate must have a nonwildcard DNS name specified as the first entry in its **SAN** field.	

For errors not described above, their cause will be identified in the Status area. Make the necessary corrections and proceed by choosing one of the following options from the **Action** area:

- **Retry**: If the cause of the error is fixed or the error was caused by an intermittent issue (such as the restart of a dependent service during the registration process), try this option to continue registration.

- **Deregister**: If you want to change any configuration or start over with the registration, use this option so that you can enter the details and options from the beginning.

Register the Recovery Site

Complete the following steps to register the recovery site.

Note   At any point before Step 4, you can click **Reset** to clear all of the settings that you have entered. You will then need to repeat this procedure from the beginning and enter the correct settings before you register the recovery site.

Before you begin

View the Prerequisites, on page 6 topic and ensure that the requirements described in the "Main and Recovery Site Prerequisites" section have been met.

Step 1   From the **Details** area, right-click the **Recovery Site** link and open the resulting page in a new browser tab.

Step 2   If necessary, enter the appropriate username and password to log in to your recovery site.

The **Disaster Recovery** page's **Configure** tab opens, with the **Recovery Site** radio button already selected.

Monitoring Configure

Set up this cluster to be the ◯ Main Site ⦿ Recovery Site

Main Site VIP*

Enter enterprise VIP of main site

Recovery Site VIP

Enter enterprise VIP of recovery site

Registration Token*

Enter registration token from main site

Username*

Enter username for main site

Password*

Enter password for main site

Status: Unconfigured

Please complete registration for all three sites in the order of Main, Recovery, and Witness. Then configure/activate the disaster recovery system from the Main Site.

Reset   Register

Step 3 Enter the following information:

- **Main Site VIP**: The virtual IP address that manages traffic between the active site's cluster nodes and your Enterprise network.

- **Recovery Site VIP**: The virtual IP address that manages traffic between the recovery site's cluster nodes and your Enterprise network. Catalyst Center prepopulates this field, based on your system's information.

  Note   After a IPSec tunnel has been configured between the main and recovery sites, Enterprise traffic on the node(s) hosting the VIP will be sourced via the Enterprise VIP (UDP/TCP/ICMP).

- The registration token that you generated while registering the main site.

- The username and password configured for your active site's super-admin user.

Step 4 From the **Action** area, click **Register**.

The **Disaster Recovery Registration** dialog opens.

Step 5 Click **Continue**.

The topology updates the status for the main and recovery sites after they have been connected.

Register the Witness Site

Complete the following steps to register the witness site.

Before you begin

Ensure that the following conditions are true before you register your disaster recovery system's witness site:

- The witness site is reachable from both the main and recovery site.

- The VIPs configured for the main and recovery site are reachable from the witness site.

Step 1   Return to the main site's browser tab.

Monitoring   Configure

Disaster Recovery Topology   Logical   Physical
Show Detail Information

Main Site
Recovery Site Connected

Recovery Site
Main Site Connected

Witness Site
Unregistered
W1

Status: Registering

The system is in the middle of registration process. Note that the registration must be done in the order of Main, Recovery, and Witness.

Details

The third and final step of registration is to register the Witness Site. Use the following command to login to witness:

`ssh -p 2222`

Copy Witness Login Cmmd.

then register via CLI:

`witness register -w        -m        -t        -u <main_admin_user>`

Copy Witness Register Cmmd.

Or opt for copy the token only:

Copy Token

Deregister

Step 2   From the **Details** area, click **Copy Witness Login Cmmd**.

Step 3   Open an SSH console to the witness site, paste the command you just copied, and then run it to log in.

Step 4   When prompted, enter the default (maglev) user's password.

Step 5   Return to the **Details** area and click **Copy Witness Register Cmmd**.

Step 6   In the SSH console, paste the command you just copied.

Step 7   Replace `<main_admin_user>` with the super-admin user's username and then run the command.

Step 8   When prompted, enter the super-admin user's password.

Witness Site Registration Errors

This topic describes errors you may encounter when registering the witness site and how to deal with them.

Error Type	Validation Made	Resolution
IP validation	Validates that the witness site IP address entered during main site registration matches the IP address entered during witness site registration.	Ensure that you enter the same IP address for the witness site when registering the main and witness sites.
Version validation	Validates that the witness site's OVA package is the correct version for the Catalyst Center version that's installed on your system's main and recovery sites. Each Catalyst Center version supports only one OVA version.	Deploy the witness site OVA package version listed in the error message.

For errors that don't involve validation checks, their cause is identified in the **Status** area. Make the necessary corrections and proceed by doing one of the following:

- After logging in to the witness site, run the **witness reset** command.

- To make any registration setting changes or restart the process from the beginning, click **Deregister** from the **Action** area.

Activate Your Disaster Recovery System

After registering your system's sites, complete the following procedure to activate the system for use in your Catalyst Center deployment.

Step 1 Verify that your main, recovery, and witness sites have been registered successfully:

a) Return to the main site's browser tab and click **Monitoring** to view the Disaster Recovery **Monitoring** tab.
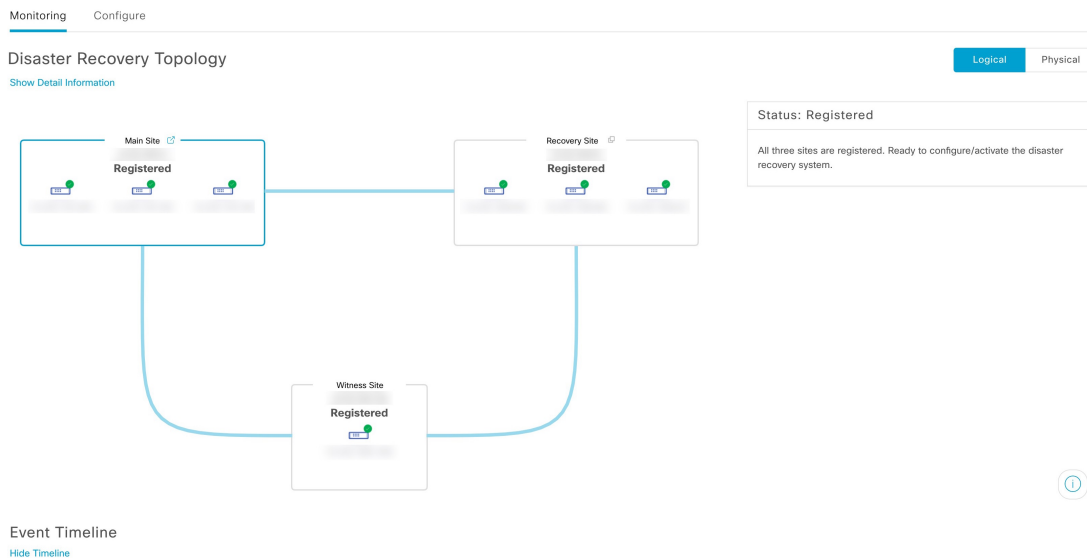
b) In the **Logical Topology** area, confirm that the three sites are displayed and their status is **Registered**.

c) In the **Event Timeline** area, confirm that the registration of each site is listed as an event and that each task completed successfully.

Step 2   In the **Action** area, click **Activate**.

A dialog box opens, indicating that all the data that currently resides in your recovery site will be erased.

Step 3   To begin the configuration of your disaster recovery system and the replication of your main site's data to the recovery site, click **Continue**.

Note   The activation process may take some time to complete. View the Event Timeline in order to monitor its progress.

Step 4   After Catalyst Center has completed the necessary tasks, verify that your system is operational:

a.   View its topology and confirm that the following status is displayed for your respective sites:
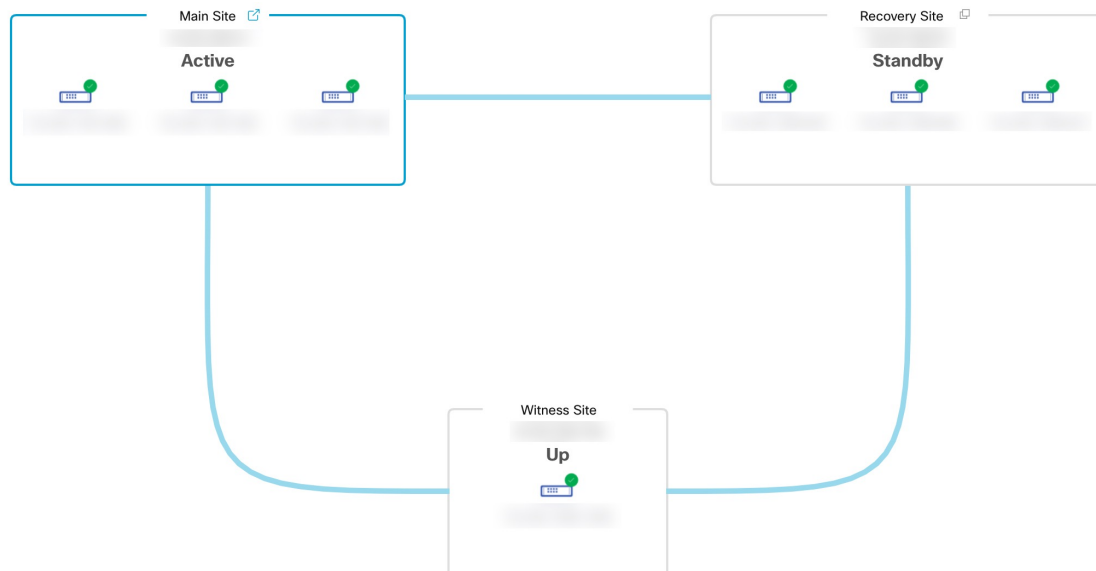
b.   View the Event Timeline and confirm that the **Activate Disaster Recovery System** task completed successfully.

Event Timeline

Hide Timeline

End   Last Update: 7/13/2021, 1:13:46 PM UTC-7

> Activate Disaster Recovery System –   7/13/2021, 1:13:39 PM UTC-7

Start Time   7/13/2021, 1:03:17 PM UTC-7
Status Message   Successfully setup disaster recovery
End Time   7/13/2021, 1:13:39 PM UTC-7

View Details

> Witness site registration –   7/13/2021, 12:59:30 PM UTC-7

> Recovery site registration –   7/13/2021, 12:49:37 PM UTC-7

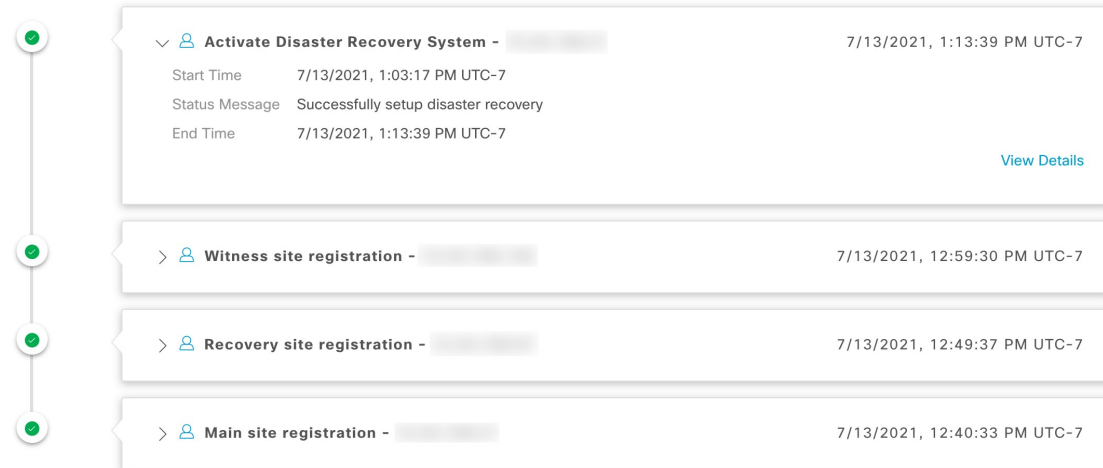> Main site registration –   7/13/2021, 12:40:33 PM UTC-7

c. Verify that your sites are reachable by pinging them from the main site.

Disaster Recovery System Validations

The following table describes the validations that the disaster recovery system makes after the **Activate** and **Rejoin** operations have been initiated.

Validation	Description
Package match	Confirms whether the packages installed on both the main and recovery sites are the same version.
Key services health	Checks the health of managed services and other key services that are critical for disaster recovery operations.
IPsec status and transmission	Confirms whether the IPSec tunnel is up for all of the disaster recovery system's sites.
Consul connectivity	Determines if the consul (the distributed database shared by the main, recovery and witness sites) is able to communicate with all of the sites.

Pause Your Disaster Recovery System

By pausing your main and recovery sites, you are effectively breaking up your disaster recovery system. The sites will no longer be connected and instead will act as standalone clusters. You would want to pause your system to temporarily disable the replication of data from the active site to the standby site if you plan to break up your system for an extended period of time. You would also pause the disaster recovery system to do one of the following:

• Complete any administrative tasks, such as upgrade the clusters or install additional packages.

- Replace the system or disaster recovery certificate.

- Perform maintenance on the main, recovery, or witness site clusters.

- Prepare for a planned network or power outage.

Place Your System on Pause

To pause your disaster recovery system temporarily, which you would typically do before performing maintenance on a system component, complete the following procedure:

Step 1 From the top-left corner, click the menu icon and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology.

Step 2 In the **Action** area, click **Pause**.

Step 3 In the resulting dialog, click **Continue** to proceed.

A message is displayed in the bottom-right corner of the page, indicating that the process to pause your system has started. To pause your system, Catalyst Center disables data and service replication. It also reinstates the services that were suspended on your recovery site. As this is taking place, the status for your main and recovery sites is set to **Pausing** in the topology.

After Catalyst Center completes the necessary tasks, the topology updates and sets the status for your main, recovery, and witness sites as **Paused**.
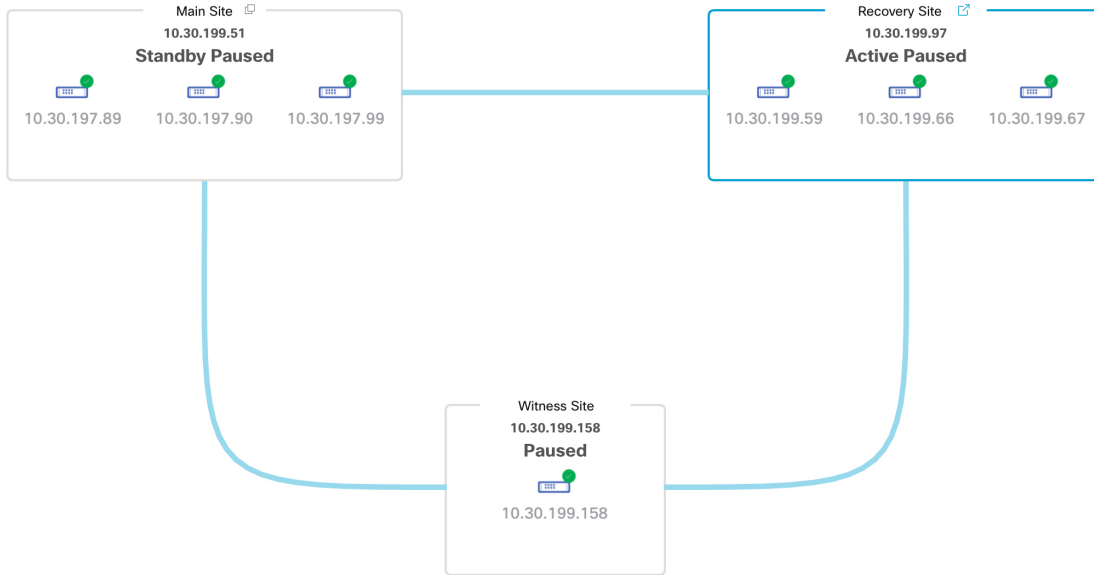
Step 4 Confirm that your disaster recovery system has been paused:

a. In the top right corner of the **Monitoring** tab, verify that its status is listed as **Paused**.

b. In the Event Timeline, verify that the **Pause Disaster Recovery System** task completed successfully.

Rejoin Your System

Complete the following procedure to restart a disaster recovery system that is currently on pause.

Step 1   From the top-left corner, click the menu icon and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology.
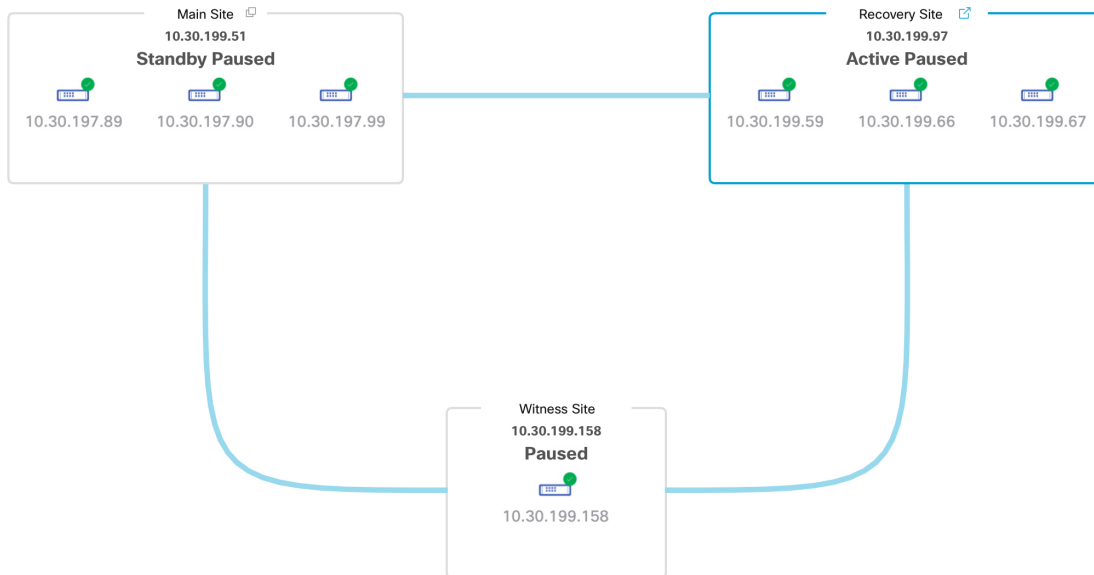

Step 2   In the **Action** area, click **Rejoin**.

A dialog opens, indicating that all the data on your standby site will be erased.

Step 3   Click **Continue** to proceed.

A message is displayed in the bottom-right corner of the page, indicating that the process to reconnect your main, recovery, and witness sites has started. As this is taking place, the status for your main and recovery sites is set to **Configuring** in the topology.
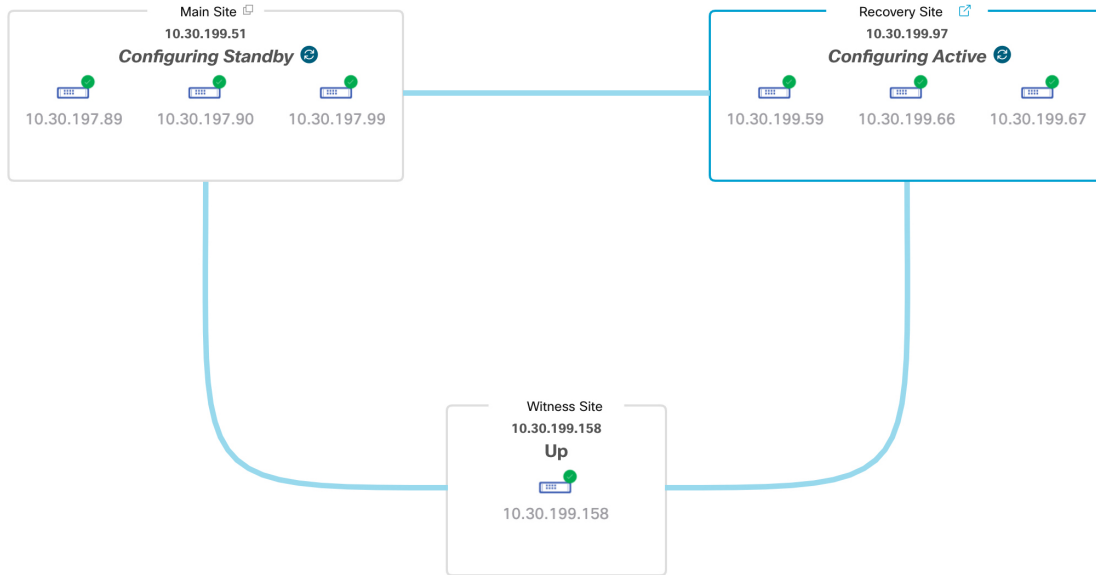
After Catalyst Center completes the necessary tasks, the topology updates the status for your main, recovery, and witness sites.
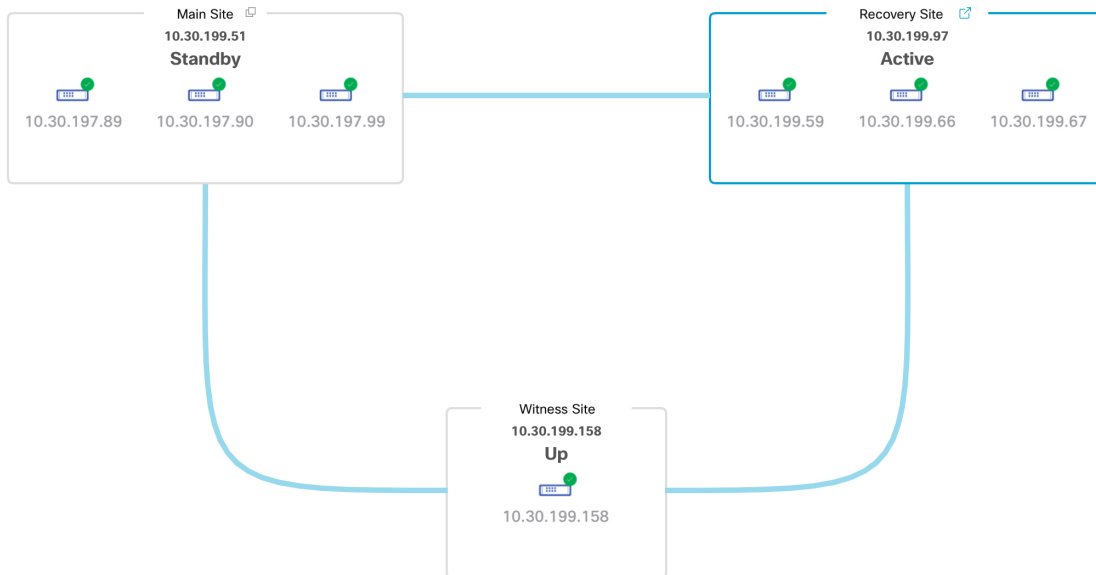
Step 4   Confirm that your disaster recovery system is operational again by verifying that its status is listed as **Up and Running** in the top-right corner of the **Monitoring** tab.

Failovers: An Overview

A failover takes place when your disaster recovery system's standby site takes over the responsibilities of the former active site and becomes the new active site. Catalyst Center supports two types of failover:

- System-triggered: Occurs when your system's active site experiences an issue that brings it offline (such as a hardware failure or network outage). When Catalyst Center recognizes that the active site has not been able to communicate with the rest of the Enterprise network (and the standby and witness sites) for seven minutes, it completes the tasks necessary for your standby site to assume its role so that network operations can continue without interruption.

- Manual: Occurs when a super-admin user instructs Catalyst Center to swap the roles that are currently held by your system's active and standby sites. You would typically do this before you update the Catalyst Center software that is installed on a site's appliances or perform routine site maintenance.

After either type of failover has taken place and the former active site has come back online, your disaster recovery system automatically moves the site to the **Standby Ready** state. To establish this site as the new standby site, click **Rejoin** in the **Action** area of the **Monitoring** tab.

Initiate a Manual Failover

When you manually initiate a failover, you instruct Catalyst Center to swap the roles that are currently assigned to your disaster recovery system's main and recovery site. Manual failover is useful if you know that the current active site is experiencing issues and you want to proactively designate the standby site as the new active site. Complete the following procedure to initiate a manual failover.

Note You cannot initiate a manual failover from your witness site. You can only do so from the current active site.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

The **Monitoring** tab is selected, by default, and displays your disaster recovery system's topology. In the following example, the user is logged in to the current active site.
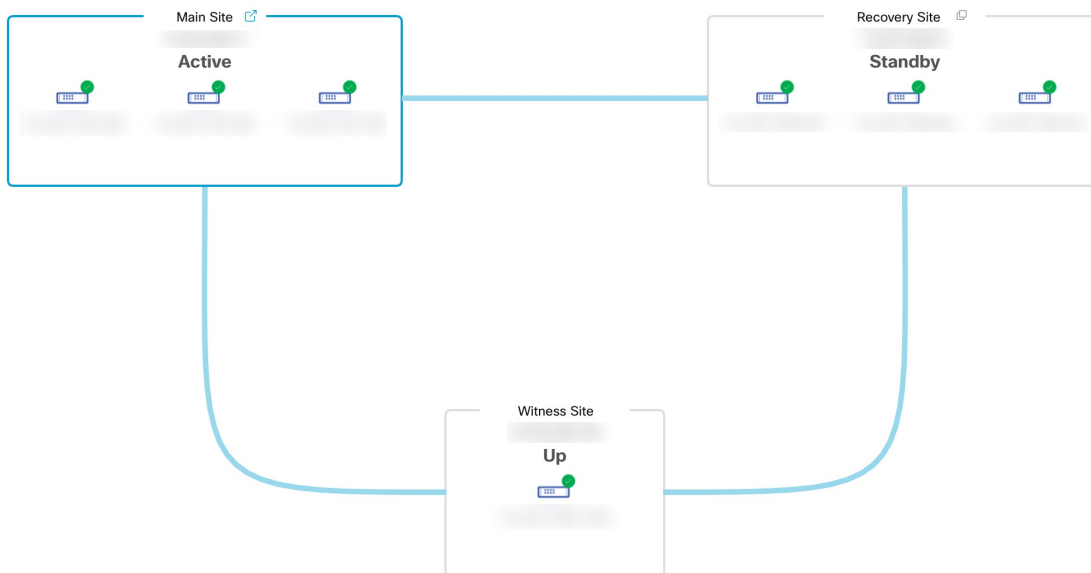
Step 2   In the **Action** area, click **Manual Failover**.

The **Disaster Recovery Manual Failover** dialog opens, indicating that the standby site will assume the **Active** role.

Step 3   Click **Continue** to proceed.

A message is displayed in the bottom-right corner of the page, indicating that the failover process has started. The site previously acting as the active site is isolated from the system and enters the **Standby Ready** state.

```
        Main Site  ⧉                                          Recovery Site  ⧉
        10.30.199.51                                          10.30.199.97
        Standby Ready                                            Active

  ▦       ▦        ▦                                    ▦        ▦        ▦
10.30.197.89  10.30.197.90  10.30.197.99        10.30.199.59  10.30.199.66  10.30.199.67


                          Witness Site
                          10.30.199.158
                               Up

                              ▦
                          10.30.199.158
```
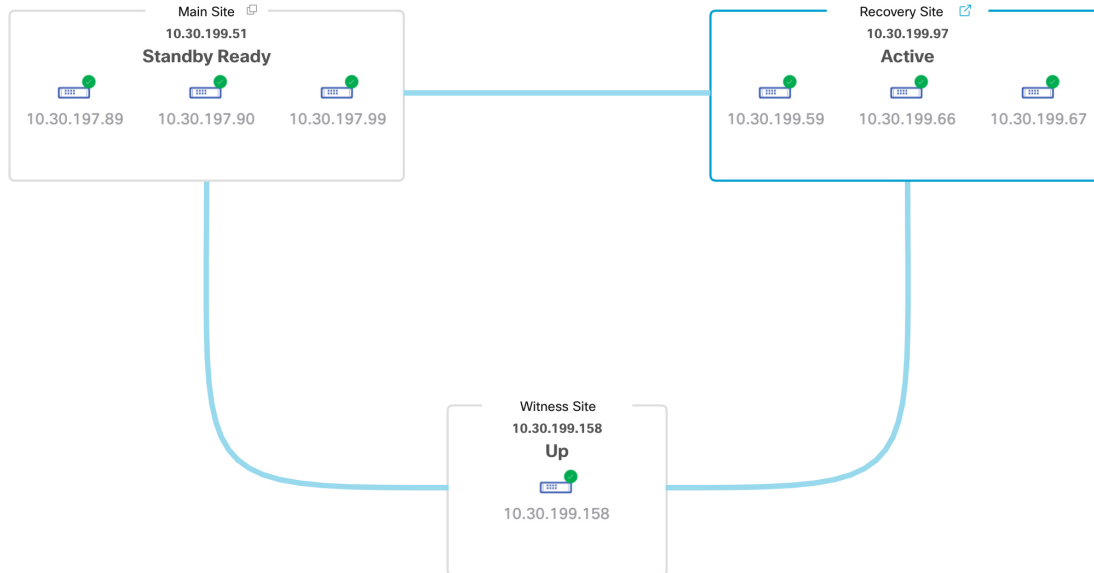
At this point, the main and recovery sites are not connected and data replication is not taking place. If the former active site is experiencing issues, now is a good time to resolve those issues.

A subsequent failover (initiated by either the system or a user) cannot take place until you add the former active site back to your disaster recovery system.

Step 4   Reconnect the main and recovery sites and reconfigure your disaster recovery system:

a.   Log in to your recovery site.

b.   In the **Action** area, click **Rejoin**.

A dialog opens, indicating that data on the standby site will be erased.

Step 5   Click **Continue** to proceed and restart data replication.

After Catalyst Center completes the relevant workflows, the manual failover completes. The main site, which was currently serving as the active site, is now the standby site.

Step 6   Confirm that your disaster recovery system is operational again:

    a.   In the top-right corner of the **Monitoring** tab, verify that its status is listed as **Up and Running**.

    b.   In the Event Timeline, verify that the **Rejoin** task completed successfully.

Deregister Your System

After your disaster recovery system is activated, you may need to update the settings that you entered for a particular site. If you find yourself in this situation, complete the following procedure.

Note   When you deregister your system, the settings that are currently set for all the sites in your system will be cleared.

Step 1   From the **Action** area, click **Pause** to suspend the operation of your system.

For more information, see Place Your System on Pause, on page 26.

Step 2   From the **Action** area, click **Deregister**.

Catalyst Center deletes all the settings that you configured previously for your system's sites.

Step 3   Complete the tasks described in Set Up Disaster Recovery, on page 14 to enter the appropriate settings for your sites, reregister them, and reactivate your system.

Disaster Recovery System Considerations

This section describes things to be aware of when managing your disaster recovery system.

Backup and Restore Considerations

- A backup can only be scheduled from your system's active site.

- You cannot restore a backup file when disaster recovery is enabled. You must first pause your system temporarily. For more information, see Place Your System on Pause, on page 26.

- You should only restore a backup file on the site that was the active site prior to pausing your system. After you restore the backup file, you then need to rejoin your system's sites. Doing so will reinstate disaster recovery and initiate the replication of the active site's data to the standby site. For more information, see Rejoin Your System, on page 28.

- You can only restore a backup file on cluster nodes that have the same Catalyst Center version installed as the other nodes in your system.

- After a failover takes place, your deployment's backup and restore settings and schedule are not replicated to the new active site. You will need to configure them again.

- If applicable to your deployment, we recommend that you upgrade the TLS version for incoming TLS connections to Catalyst Center. In the Catalyst Center Security Best Practices Guide, see the "Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)" topic. If you have already upgraded your main site, we recommend that you also upgrade your recovery site (ideally before you activate your disaster recovery system or after a failover occurs).

Node or Cluster Replacement Considerations

You cannot do either of the following without breaking your disaster recovery system's configuration:

- Replace one of the nodes in a 1+1+1 setup.

- Replace all of one site's nodes in a 3+3+1 setup.

If you need to do so, ensure that you then complete the steps described in to get your system up and running again.

Reconfiguration Considerations

- Any data present on the appliances that reside at the recovery site will be deleted in the following scenarios:

  - When setting up your disaster recovery system for the first time and you activate the system.

  - When the recovery site is the current active site, you pause your system, deregister it, and then reregister it as the recovery site.

- When you reconfigure an existing disaster recovery system, make sure you know which site is the current active site and register it as your system's main site. Alternatively, you can make a backup of the recovery site's data (if it's currently active) and restore this data on your system's main site prior to the system's reconfiguration.

- The following changes cannot be made without reconfiguring your system:

  - Changing the IP addresses and static/default routes configured for your disaster recovery system's Enterprise and Management interfaces.

  - Updating a site's **cluster_hostname** setting.

Complete the steps described in to configure new IP addresses and routes. If you updated the **cluster_hostname** value, complete these same steps after doing so.

HA Considerations

You cannot convert the main and recovery sites from single-node clusters to HA clusters without breaking your disaster recovery system's configuration. If you need to do so, do the following:

1. .

2. Convert both sites to HA clusters.

3. Reregister and reactivate disaster recovery (see).

Site Failure Considerations

By default, the disaster recovery system waits seven minutes before recognizing that a site has failed and taking one of the following actions:

- When the active site goes down, it starts the failover process.

- When either the standby or witness site goes down, the system marks that site as down and disables the ability to start any tasks from the **Action** area.

If you try to initiate a task before the seven minutes have passed, the **Details** area will display a message that indicates why it cannot be completed.

Certificate Replacement Considerations

The **Status** area indicates when the certificate configured for your disaster recovery system is set to expire. If the certificate will expire within 90 days, a warning message is displayed:

Status: Up and Running

The disaster recovery system is up and running. It will perform replication as needed.

CERTIFICATE STATUS

⚠ **The Disaster Recovery Certificates will expire in 89 days.** One day before the expiration, the disaster recovery system will automatically pause and discontinue replicating data. To avoid any interruption in service, please follow the steps below for the certificate renewal.

If the certificate will expire in 30 days or less, an error message is displayed instead:

Status: Up and Running

The disaster recovery system is up and running. It will perform replication as needed.

CERTIFICATE STATUS

✖ **The Disaster Recovery Certificates will expire in 29 days.** One day before the expiration, the disaster recovery system will automatically pause and discontinue replicating data. To avoid any interruption in service, please follow the steps below for the certificate renewal.

If the certificate is set to expire in a day, and the disaster recovery system is operational, Catalyst Center automatically pauses your system:

Status: Paused

The disaster recovery system is now paused. Main and Recovery Sites are two standalone clusters. There is no replication between these two sites. Click 'Re-Join' to form the disaster recovery system again and resume replication.

CERTIFICATE STATUS

✖ **The Disaster Recovery Certificates will expire in 1 day.** The disaster recovery system has paused and the data replication stopped. To avoid any interruption in service, please follow the steps below for the certificate renewal.

To configure a new certificate and restore the operation of your system, you'll need to do the following:

1. Place Your System on Pause (unless Catalyst Center has already done so).

2. Replace your system's certificate by completing the steps described in the Add the Disaster Recovery Certificate, on page 11 topic.

3. Rejoin Your System to restart it.

Administer Your Disaster Recovery System

This section describes how to complete the various tasks you may need to carry out while managing your deployment's disaster recovery system.

Replace the Current Witness Site

Complete the following procedure to replace your disaster recovery system's current witness site with a new site.

Step 1   Log in to the current witness site:

    a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev@***witness-site's-IP-address* command.

    b) Enter the default (maglev) user's password.

Note   Before you proceed to the next step, note the witness site's IP address. You'll need to configure the same address after you replace the witness site. Otherwise, the witness site won't work as expected.

Step 2   Run the **witness reset** command.

Step 3   Delete the current witness site's virtual machine.

Step 4   Install the new witness site's virtual machine, as described in Install the Witness Site, on page 12.

Step 5   Log in to the new witness site:

    a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev@***witness-site's-IP-address* command.

    b) Enter the default (maglev) user's password.

Step 6   Run the **witness reconnect -w** *witness-site's-IP-address* **-m** *main-site's-Enterprise-virtual-IP-address* **-u** *admin-username* command.

Note the following points:

- Regardless of the main site's current disaster recovery status, use the main site's Enterprise VIP when reconnecting the witness site.

- To verify that the witness site is operational after running this command, do the following:

    a. From the Disaster Recovery Topology, click the **Show Detail Information** link to open the **Disaster Recovery System** slide-in pane.

    b. In the **Witness Site** section, confirm that the status for the witness site and configured IPSec links is `Up`.

- To view all of the available options for this command, run the **witness reconnect --help** command.

Upgrade the Current Witness Site

Complete the following procedure to upgrade the witness site that's currently configured for your disaster recovery system.

Step 1 Download the witness site upgrade bundle that's specific to the Catalyst Center version that the witness site is running:

a) Open https://software.cisco.com/download/home/286316341/type.

Note You need a Cisco.com account to access this URL. See the following page for a description of how to create an account: https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html

b) In the **Select a Software Type** area, click the Catalyst Center software link.

The **Software Download** page updates, listing the software that's available for the latest Catalyst Center release.

c) Do one of the following:

- If the upgrade bundle (CC-witness-2.3.7.5-upgrade.tar.gz) you need is already listed, click its **Download** icon.

- Enter the relevant version number in the **Search** field, click its link in the navigation pane, and then click the **Download** icon for that version's upgrade bundle.

Step 2 In an SCP client, copy the upgrade bundle from the host on which it was downloaded to the current witness site's virtual machine by running the following command: **scp -P 2222** *upgrade-bundle-filename witness-site's-admin-username*

Refer to the following example:

```
$ scp -P 2222 CC-witness-2.3.7.5-upgrade.tar.gz
maglev@10.30.197.96:/tmp/CC-witness-2.3.7.5-upgrade.tar.gz
maglev@10.30.197.96's password:
CC-witness-2.3.7.5-upgrade.tar.gz    100%  242MB 138.4MB/s  00:01
```

Step 3 In an SSH client, log in to the witness site's virtual machine and run the **witness upgrade** command, supplying values for the following arguments:

- **-p, --password** (TEXT): Admin password for the main system

- **-u, --username** (TEXT): Admin username for the main system (required)

- **-m, --main_ip** (IPV4_ADDRESS): Virtual IP address of the main system (required)

- **-w, --witness_ip** (IPV4_ADDRESS): Witness site's IP address (required)

- **-b, --upgrade-bundle** (TEXT): File system path to the upgrade bundle (required)

Refer to the following example of what you'll see during an upgrade:

```
$ witness upgrade -b release_dr_witness_scapa-patch2_devtest_837
-2.1.714.837024_upgrade.tar.gz -m 10.30.199.53 -w 10.30.197.96 -u admin
password for admin:
Retrieving information from the Disaster Recovery service on 10.30.199.53...
Inspecting upgrade bundle release_dr_witness_scapa-patch2_devtest_837
```

```
-2.1.714.837024_upgrade.tar.gz...
Launching upgrade process in tmux session 'upgrade'...
Tailing the upgrade log /var/log/witness_upgrade.log...
upgrade_witness INFO witness upgrade process starting
[snip]
upgrade_witness INFO ***** Witness upgraded from version 2.1.714.837023 to
2.1.714.837024 *****
upgrade_witness INFO ***** Please reboot the witness VM ($ sudo reboot) to
insure all updates are applied *****
upgrade_witness INFO ***** Then use the 'witness reconnect' command to
re-establish witness connectivity *****
upgrade_witness INFO witness upgrade process completed successfully
Terminated
Witness upgrade invocation succeeded
```

Step 4   Do one of the following:

- If the upgrade completes successfully, reboot the witness site's virtual machine to pick up all of the updated packages that were applied by running the **sudo reboot** command.

- If you get an error during the upgrade, retry the operation.

Step 5   Log in to the new witness site:

a) Open an SSH console to the witness site and run the **ssh -p 2222 maglev**@*witness-site's-IP-address* command.

b) Enter the default (maglev) user's password.

Step 6   Run the **witness reconnect -w** *witness-site's-IP-address* **-m** *main-site's-Enterprise-virtual-IP-address* **-u** *admin-username* command.

Note the following points:

- Regardless of the main site's current disaster recovery status, use the main site's Enterprise VIP when reconnecting the witness site.

- To verify that the witness site is operational after running this command, do the following:

  a. From the Disaster Recovery Topology, click the **Show Detail Information** link to open the **Disaster Recovery System** slide-in pane.

  b. In the **Witness Site** section, confirm that the status for the witness site and configured IPSec links is Up.

- To view all of the available options for this command, run the **witness reconnect --help** command.

Monitor the Event Timeline

From the Event Timeline, you can track the progress of disaster recovery tasks that are currently running and confirm when these tasks have completed. To view the timeline, do the following:

1. From the top-left corner, click the menu icon and choose **System** > **Disaster Recovery** to open the **Disaster Recovery** page.

   The **Monitoring** tab is selected, by default.

2. Scroll to the bottom of the page.

Every task that is in progress or has completed for your system is listed here (in descending order based on their completion timestamp), starting with the most recent task. Catalyst Center indicates whether each task was initiated by the system (⌨) or a user (👤).

Say you want to monitor the restoration of your system after it was paused. Catalyst Center updates the Event Timeline as each task in the restoration process is started and then completed. To view a summary of what took place during a particular task, click >.

If the **View Details** link is displayed for a task, click it to view a listing of the relevant subtasks that were completed.

Event Timeline
Hide Timeline

End   Last Update: 7/13/2021, 3:12:07 PM UTC-7

✓   ⌄ 👤 **Re-Join - 10.30.199.51**   7/13/2021, 3:02:11 PM UTC-7

        Start Time   7/13/2021, 2:54:00 PM UTC-7
        Status Message   Successfully setup disaster recovery
        End Time   7/13/2021, 3:02:11 PM UTC-7

                                                                                            Hide Details

        ✓   > **Configure active - 10.30.199.51**   7/13/2021, 2:58:10 PM UTC-7

        ✓   > **Configure standby - 10.30.199.97**   7/13/2021, 3:02:04 PM UTC-7

✓   > 👤 **Manual failover - 10.30.199.97**   7/13/2021, 2:53:02 PM UTC-7

As with tasks, you can click **>** to view summary information for a particular subtask.

Event Timeline
Hide Timeline

End   Last Update: 7/13/2021, 3:12:07 PM UTC-7

✓   ⌄ 👤 **Re-Join - 10.30.199.51**   7/13/2021, 3:02:11 PM UTC-7

        Start Time   7/13/2021, 2:54:00 PM UTC-7
        Status Message   Successfully setup disaster recovery
        End Time   7/13/2021, 3:02:11 PM UTC-7

                                                                                            Hide Details

        ✓   ⌄ **Configure active - 10.30.199.51**   7/13/2021, 2:58:10 PM UTC-7

                   Start Time   7/13/2021, 2:54:08 PM UTC-7
                   Status Message   Successfully configured active system
                   End Time   7/13/2021, 2:58:10 PM UTC-7

                                                                                        Hide Details

              ✓   > **Configure standby to active services - 10.30.199.51**
                                                            7/13/2021, 2:58:04 PM UTC-7

              ✓   > **Add other cluster metadata - 10.30.199.51**   7/13/2021, 2:57:18 PM UTC-7

              ✓   > **File system migration - 10.30.199.51**   7/13/2021, 2:55:29 PM UTC-7

              ✓   > **Save cluster metadata - 10.30.199.51**   7/13/2021, 2:55:18 PM UTC-7

              ✓   > **Validate active cluster - 10.30.199.51**   7/13/2021, 2:54:09 PM UTC-7

See for a description of the issues that you may encounter while monitoring the Event Timeline and how to remedy them.

Monitor Managed Services Replication

After you activate your disaster recovery system, Catalyst Center begins monitoring the data replication status of the GlusterFS, MongoDB, and Postgres services. Whenever the replication of these services is taking place, the **Status** area displays one of the following four messages:

- Replication is completing as expected.

  ONGOING DATA REPLICATION

  ✔ Ongoing data replication is proceeding within the normal range of latency.

- Replication is completing, but the data sync lag between your system's main and recovery site is currently 20 minutes or more.

  ONGOING DATA REPLICATION

  ⚠ Ongoing data replication is slowing down. You may want to be on the lookout for the status of network and/or system.

- Replication is completing, but the data sync lag between your system's main and recovery site is 30 minutes or more.

  ONGOING DATA REPLICATION

  ✖ Ongoing data replication is slowing down significantly. **Please check the system and network. Contact Cisco support if the issue persists.**

- Replication has stopped.

  ONGOING DATA REPLICATION

  ✖ Ongoing data replication has stopped. It is critical to keep the data of the secondary site in-sync with the primary site. **Please check the system and network. Contact Cisco support immediately to prevent data loss.**

These messages allow you to keep tabs on the replication of managed services, pointing out when network or system issues are impacting the sync of these services' data between your system's sites.

System and Site States

In the disaster recovery GUI, the **Status** area indicates the current state of your system. The following tables explain the various states that you may see for the individual sites in your system Topology.

Table 2: Active Site States

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Initializing	The site is preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.

State	Description
Initialized	The site has successfully prepared the data that it will transmit to the other sites in order to set up the disaster recovery cluster during the registration process.
Failed to Initialize	The site encountered an error while preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Connecting Recovery	The main site is contacting the recovery site to retrieve the initialized data required to set up secure communication with the main site.
Connecting Witness	The main site is contacting the witness site to retrieve the initialized data required to set up secure communication with the main site.
Recovery Site Connected	The main site successfully established secure communication with the recovery site.
Failed to Connect Recovery	The main site encountered an error while establishing a secure channel with the recovery site.
Failed to Connect Witness	The main site encountered an error while establishing a secure channel with the witness site.
Registered	The active site successfully established secure communication with the other two sites.
Deregistering	Removing the current disaster recovery configuration from the system.
Deregister Failed	An error occurred while removing the current disaster recovery configuration from the system.
Validating	Validating the state of the system before starting the disaster recovery configuration.
Validated	Successfully validated the state of the system before starting the disaster recovery configuration.
Validation Failed	An error occurred while validating the state of the system before starting the disaster recovery configuration.
Configuring Active	Executing the workflows to establish this site as the active site.
Failed to Configure	An error occurred while running the workflows to enable disaster recovery on this site.
Syncing Config Data	Syncing the data required from the other sites to set up the disaster recovery system.
Config Data Synced	Successfully synced the data required from the other sites to set up the disaster recovery system.
Active Sync Failed	An error occurred while the pending active site was syncing the data required from the other sites to set up the disaster recovery system.
Waiting Standby Configuration	Successfully completed the workflows to establish this site as the active site; waiting for the standby site's workflows to complete.
Active	The site is successfully managing the network as the active site.
Failed to Configure	The site failed to execute some of the workflows that would enable itself as the active site in the disaster recovery cluster.
Isolating	The site is executing the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).

State	Description
Isolated	The site has successfully executed the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Failed to Isolate	The site encountered an error while executing the workflows to isolate itself because it either lost connectivity with the other two sites or is preparing to become standby-ready (as part of a manual failover).
Configuring Active	Configuring a previous standby site as the active site (as part of a system-triggered or manual failover).
Failed during Failover	An error occurred while executing the workflows to establish this site as the active site (as part of a failover or recovery from a two-system failure).
Pausing Active	Executing the workflows that disable disaster recovery operations on the active site (in order to prepare for an administrative operation or a planned outage).
Active Paused	Successfully disabled disaster recovery operations on the active site.
Failed to Pause Active	An error occurred while disabling disaster recovery operations on the active site.
Active Stand Alone	Executing the workflows to establish a previous active site that lost connectivity with the other two sites as an independent system by removing all disaster recovery configurations.
Down	The active site has lost connectivity with the other two sites.

Table 3: Standby Site States

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Initializing	The site is preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Initialized	The site has successfully prepared the data that it will transmit to the other sites in order to set up the disaster recovery cluster during the registration process.
Failed to Initialize	The site encountered an error while preparing to transmit the data required by the other sites in order to set up the disaster recovery cluster during the registration process.
Connecting Main	The recovery site is contacting the main site to retrieve the initialized data required to set up secure communication with the main site.
Connecting Witness	The recovery site is contacting the witness site to retrieve the initialized data required to set up secure communication with the main site.
Main Site Connected	The recovery site successfully established secure communication with the main site.
Failed to Connect Main	The recovery site encountered an error while establishing a secure channel with the main site.

State	Description
Failed to Connect Witness	The recovery site encountered an error while establishing a secure channel with the witness site.
Registered	The standby site successfully established secure communication with the other two sites.
Deregistering	Removing the current disaster recovery configuration from the system.
Deregister Failed	An error occurred while removing the current disaster recovery configuration from the system.
Validating	Validating the state of the system before starting the disaster recovery configuration.
Validated	Successfully validated the state of the system before starting the disaster recovery configuration.
Validation Failed	An error occurred while validating the state of the system before starting the disaster recovery configuration.
Configuring Standby	Executing the workflows to establish this site as the standby site.
Failed to Configure	An error occurred while running the workflows to enable disaster recovery on this site.
Syncing Config Data	Syncing the data required from the other sites to set up the disaster recovery system.
Config Data Synced	Successfully synced the data required from the other sites to set up the disaster recovery system.
Standby Sync Failed	An error occurred while the pending standby site was syncing the data required from the other sites to set up the disaster recovery system.
Waiting Active Configuration	Successfully completed the workflows to establish this site as the standby site; waiting for the active site's workflows to complete.
Standby	The site is successfully configured as the standby site in the disaster recovery cluster.
Failed to Configure	The site failed to execute some of the workflows that would enable itself as the standby site in the disaster recovery cluster.
Isolating	The site is executing the workflows to isolate itself because it lost connectivity with the other two sites.
Isolated	The site has successfully executed the workflows to isolate itself because it lost connectivity with the other two sites.
Failed to Isolate	The site encountered an error while executing the workflows to isolate itself because it lost connectivity with the other two sites.
Configuring Standby	Configuring a previous active site as the standby-ready site (as part of a manual failover).
Standby Ready	A previous active system is ready to be configured as a standby system (as a result of a failover).
Pausing Standby	Executing the workflows that disable disaster recovery operations on the standby site (in order to prepare for an administrative operation or a planned outage).
Standby Paused	Successfully disabled disaster recovery operations on the standby site.
Failed to Pause Standby	An error occurred while disabling disaster recovery operations on the standby site.

State	Description
Standby Stand Alone	Executing the workflows to establish a previous standby site that lost connectivity with the other two sites as an independent system by removing all disaster recovery configurations.
Down	The site has lost connectivity with the other two sites.

Table 4: Witness Site States

State	Description
Unregistered	Newly installed site. Disaster recovery information is not available yet.
Registered	This site has been designated as the witness site and the validation checks have completed successfully.
Up	Configuration of the witness site has completed successfully.
Down	The site has lost connectivity with the other two sites.

Upgrade a Disaster Recovery System

In this scenario, the first Catalyst Center version installed on your appliances was an earlier 2.1.x version and now you want to upgrade to the latest version. Also, disaster recovery is enabled and operational on these appliances. Complete the following steps to complete the upgrade:

Step 1 Place Your System on Pause, on page 26.

Step 2 Upgrade the appliances at your main and recovery sites to the latest Catalyst Center version (see the *Cisco Catalyst Center Upgrade Guide*).

Step 3 Do one of the following:

- Replace the Current Witness Site, on page 36

- Upgrade the Current Witness Site, on page 37

Step 4 Rejoin Your System, on page 28.

Note After upgrading to Catalyst Center 2.3.7 from version 2.3.4 or earlier, data migration takes place the first time a Rejoin operation is initiated. As a result, it will take longer for this operation to complete. The migration may add minutes or even hours to the completion time, depending on the amount of Catalyst Center data that's present. Keep in mind that this data migration only happens after an upgrade. This will not impact subsequent Rejoin operations.

Disaster Recovery Event Notifications

You can configure Catalyst Center to send a notification whenever a disaster recovery event takes place. See the "Work with Event Notifications" topic in the *Cisco Catalyst Center Platform User Guide* for a description of how to configure and subscribe to these notifications. When completing this procedure, ensure that you select and subscribe to the SYSTEM-DISASTER-RECOVERY event in the **Platform** > **Developer Toolkit** > **Events** table.

After you subscribe, Catalyst Center sends a notification indicating that the IPsec session is down because the system's certificate has expired. Do the following to update this certificate:

1. .

2. On both your main and recovery site, replace the current system certificate. From the top-left corner, click the menu icon and choose **System** > **Settings** > **Certificates** > **System Certificates**.

3. .

Supported Events

The following table lists the disaster recovery events that Catalyst Center generates notifications for when they take place.

System Health Status	Event	Notification
OK	The disaster recovery system is operational.	`Activate DR (Disaster Recovery Setup Successful)`
OK	Failover to either the main or recovery site has completed successfully.	`Failover Successful`
OK	Registration of the main site has completed successfully.	`Successfully Registered Main Site`
OK	Registration of the recovery site has completed successfully.	`Successfully Registered Recovery Site`
OK	Registration of the witness site has completed successfully.	`Successfully Registered Witness Site`
OK	The disaster recovery system has been paused successfully.	`DR Pause Success`
OK	The standby site is operational.	`Standby Site Up`
OK	The witness site is operational.	`Witness Site Up`
OK	The disaster recovery system has been unregistered successfully.	`Unregister Success`
Degraded	Failover to either the main or recovery site has failed.	`Failover Failed`
Degraded	Automated failover is not available because the standby site is currently down.	`Standby Cluster Down`
Degraded	Automated failover is not available because the witness site is currently down.	`Witness Cluster Down`

System Health Status	Event	Notification
Degraded	Unable to place the disaster recovery system on pause.	`Pause Failure`
Degraded	BGP route advertisement failed.	`BGP Failure`
Degraded	The IPsec tunnel connecting your system's sites is operational.	`IPsec Up`
Degraded	The IPsec tunnel connecting your system's sites is currently down.	`IPsec Down`
NotOk	Disaster recovery system configuration failed.	`Activate DR Failure`
NotOk	The site that is currently in the **Standby Ready** state is unable to rejoin the disaster recovery system.	`Activate DR Failure`
NotOk	Unregistration of the disaster recovery system failed.	`Unregistration Failed`
NotOk	Registration of the main site failed.	`Main Registration Failed`
NotOk	Registration of the recovery site failed.	`Recovery Registration Failed`
NotOk	Registration of the witness site failed.	`Witness Registration Failed`

Troubleshoot Your Disaster Recovery System

The following table describes the issues that your disaster recovery system may present and how to deal with them.

✎

Note   If a disaster recovery operation fails or times out, click **Retry** to perform the operation again. If the problem persists and its solution is not provided in the following table, contact Cisco TAC for assistance.

Table 5: Disaster Recovery System Issues

Error Code	Message	Solution
SODR10007	`Token does not match.`	The token provided during recovery site registration does not match the token generated during main site registration. From the main site's **Disaster Recovery** > **Configuration** tab, click **Copy Token** to ensure that you copy the correct token.
SODR10048	`Packages (package names) are mandatory and not installed on the main site.`	Install the listed packages before registering the system.
SODR10056	`Invalid credentials.`	Confirm that you entered the correct credentials for the main site during recovery and witness site registration.
SODR10062	`() site is trying to () with invalid IP address. Expected is (); actual is ().`	The main site IP address provided during recovery and witness site registration is different from the IP address that was provided during main site registration.

Error Code	Message	Solution
SODR10067	`Unable to connect to (recovery or witness site).`	Verify that the main site is up.
SODR10072	`All the nodes are not up for (main or recovery site).`	Check whether all three of the site's nodes are up.
SODR10076	`High availability should be enabled on (main or recovery) site cluster.`	Enable high availability (HA): 1. Log in to the site you need to enable HA on. 2. From the top-left corner, click the menu icon and choose **System** > **Settings** > **System Configuration** > **High Availability**. 3. Click **Activate High Availability**.
SODR10100	`(Main or recovery) site has no third party certificate.`	Replace the default certificate that Catalyst Center is currently using with a third-party certificate. See Update the Catalyst Center Server Certificate for more information.
SODR10113	`Save cluster metadata failed.`	Contact Cisco TAC for help with completing the appropriate recovery procedure.
SODR10118	`Appliance mismatch between main () and recovery ().`	Different appliances are used by the main and recovery sites. To successfully register disaster recovery, both sites must use the same 56 or 112 core appliance.
SODR10121	`Failed to advertise BGP. Reason: ().`	See Troubleshoot BGP Route Advertisement Issues, on page 54 for more information.
SODR10122	`Failed to stop BGP advertisement. Reason: ().`	See Troubleshoot BGP Route Advertisement Issues, on page 54 for more information.
SODR10123	`Failed to establish secure connection between main () and ()().`	No solution is available for this issue. Contact Cisco TAC for assistance.
SODR10124	`Cannot ping VIP: (main, recovery, or witness site's VIP or IP address).`	Do the following: • Verify that the address specified is correct. • Check whether the address is reachable from the other addresses.
SODR10129	`Unable to reach main site. ()`	Check whether the Enterprise virtual IP address configured for the main site is reachable from the recovery and witness sites.
SODR10132	`Unable to check IP addresses are on the same interface. Retry the operation. ()`	Retry the operation you just attempted.

Error Code	Message	Solution
SODR10133	`The disaster recovery enterprise VIP () and the IP addresses () are not configured or reachable via the same interface. Check the gateway or static routes configuration.`	Communication between a disaster recovery system's sites relies on the Enterprise network. The main and recovery site's Enterprise virtual IP address, and the witness site's IP address, need to be reachable via the Enterprise interface. This error indicates that the IP address/virtual IP address configured for one or multiple sites uses an interface other than the Enterprise interface for communication.
SODR10134	`The disaster recovery management VIP (VIP address) and the IPs (IP addresses) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration.`	The disaster recovery system's Management virtual IP address needs to be configured on the Management interface. This error indicates that the virtual IP address is currently configured on an interface where the Management cluster's virtual IP address has not been configured. Add a /32 static route to the Management virtual IP address that's configured on the Management interface.
SODR10136	`Certificates required to establish IPsec session not found.`	From the **System Certificate** page (**System** > **Settings** > **Certificates** > **System Certificates**), try uploading the third-party certificate again and then retry registration. If the problem persists, contact Cisco TAC for assistance.
SODR10138	`Self-signed certificate is not allowed. Upload a third-party certificate and retry.`	—
SODR10139	`Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate.`	The third-party certificate installed on your main and recovery sites has different DNS names specified for your disaster recovery system. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites. **Note** Ensure that the DNS name does *not* use a wildcard.
SODR10140	`Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.`	The third-party certificate installed on your main and recovery sites does not specify a DNS name for your disaster recovery system. Catalyst Center uses this name to configure the IPsec tunnel that connects your system's sites. Generate a third-party certificate that specifies a DNS name for your system and upload this certificate to both sites. **Note** Ensure that the DNS name does *not* use a wildcard.
—	—	When all three of your system's sites are not connected due to network partitioning or another condition, Catalyst Center sets the status of the sites to **Isolated**. Contact Cisco TAC for help with completing the appropriate recovery procedure.

Error Code	Message	Solution
—	External postgres services does not exists to check service endpoints.	Do the following: 1. Log in to the site that the error occurred on. 2. Run the following commands: • **Kubectl get sep -A** • **kubectl get svc -A | grep external** 3. In the resulting output, search for external-postgres. 4. If present, run the following command: **kubectl delete sep external-postgres -n fusion** 5. Retry the operation that failed previously.
—	Success with errors.	If you see this message after initiating a failover or pausing your disaster recovery system, it indicates that the operation completed successfully even though one or multiple services encountered minor errors. You can go ahead and click **Rejoin** to restart your system. These errors will be resolved after you do so.
—	Failed.	This message indicates that a disaster recovery operation failed because one or multiple services encountered a critical error. To troubleshoot the failure, we recommend that you view the Event Timeline and drill down to the relevant error. When you see this message, click **Retry** to perform the operation again.
—	Cannot ping VIP: (*VIP address*).	Verify that the Enterprise VIP address configured for your system is reachable.
—	VIP drop-down list is empty.	Confirm that your system's VIP addresses and intracluster link are configured properly.
—	Cannot perform (*disaster recovery operation*) due to ongoing workflow: BACKUP. Please try again at a later time.	A disaster recovery operation was triggered while a scheduled backup was running. Retry the operation after the backup finishes.

Error Code	Message	Solution
—	The GUI indicates that the standby site is still down after it has come back online.	If the standby site goes down and Catalyst Center's first attempt to isolate it from your disaster recovery system fails, it may not automatically initiate a second attempt. When this happens, the GUI will indicate that the site is down, even if it is operational again. In addition, you will not be able to restart your system as the standby site is stuck in maintenance mode. To restore the standby site, do the following: 1. In an SSH client, log in to the standby site. 2. Run the **maglev maintenance disable** command to take the site out of maintenance mode. 3. Log in to Catalyst Center. 4. From the top-left corner, click the menu icon and choose **System** > **Disaster Recovery**. The **Monitoring** tab is selected by default. 5. In the **Action** area, click **Rejoin** in order to restart your disaster recovery system.

—	Multiple services exists for MongoDB to check node-port label.	For debugging, the MongoDB node port is exposed as a service. Run the following commands to identify this port and hide it:
		
		    • **kubectl get svc --all-namespaces | grep mongodb**
		
		    • **magctl service unexpose mongodb** *<port-number>*

—	Multiple services exist for Postgres to check node-port label.	For debugging, the Postgres node port is exposed as a service. Run the following commands to identify this port and hide it:
		
		    • **kubectl get svc --all-namespaces | grep postgres**
		
		    • **magctl service unexpose postgres** *<port-number>*

Two-Site Failure Scenarios

A two-site failure occurs when at least two of your disaster recovery system's three sites go down at the same time or the sites have been partitioned. Refer to the following table for a description of how Catalyst Center responds to the various failure scenarios and any user actions that need to be taken.

Failure Scenario	System and User Response

Scenario 1: Two of your system's sites go down.	1. The system isolates the site that's still online.
	
	Important Even if this operation fails, complete the first task described in Step 3 if you plan to operate this site as a standalone site.
	
	2. Log in to this site.
	
	3. If you want the site to operate as a standalone site, click **Standalone** and then click **Continue** in the resulting dialog box.
	
	Note If you choose this option and want to reestablish your disaster recovery system later, you'll need to do the following:
	
	    a. Reset the witness site by running the **witness reset** command.
	
	    b. Log in to the other site that failed and click **Standalone** so that it also operates as a standalone site for the time being.
	
	    c. Log in to the site that's still online and reconfigure your Set Up Disaster Recovery. When you set this site to operate in standalone mode, the VIP configured for your system is deleted from the sites that went down. This step is key since it will reconfigure your system's VIP on these sites.
	
	If you don't want the site to operate as a standalone site, first bring the two sites that went down back up. Then do one of the following:
	
	• If the witness site remains offline, refer to the Scenario 3 system and user response.
	
	• If the standby site remains offline, refer to the Scenario 4 system and user response.
	
	• If the active site remains offline, refer to the Scenario 5 system and user response.
	
	When a site enters standalone mode, the system automatically configures its virtual IP address for that site. It also advertises its virtual IP address routes to prevent network reprovisioning.

Scenario 2: The active, standby, and witness sites go down and come back online about the same time.	1. The system isolates the active and standby sites. 2. The system restores the active site and the standby site enters the **Standby Ready** state. 3. You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Monitor the Event Timeline. 4. Set Up Disaster Recovery, on page 14.

Failure Scenario	System and User Response

Scenario 3: The active, standby, and witness sites go down. The active and standby sites come back online while the witness site remains offline.	**1.** The system isolates the active and standby sites.
	
	2. The system restores the active site and the standby site enters the **Standby Ready** state.
	
	3. You are notified that the system has recovered from a two-system failure.
	
	For confirmation, refer to the Monitor the Event Timeline.
	
	4. Do one of the following:
	
	   • After the witness site comes back online, Set Up Disaster Recovery, on page 14.
	
	   • Place Your System on Pause, on page 26.

Scenario 4: The active, standby, and witness sites go down. The active and witness sites come back online while the standby site remains offline.	**1.** The system isolates and then restores the active site. **2.** You are notified that the system has recovered from a two-system failure. For confirmation, refer to the Monitor the Event Timeline. **3.** After the former active site comes back online and enters the **Standby Ready** state, Set Up Disaster Recovery, on page 14. If you've determined that you need to replace the nodes at the standby site, do the following instead: **a.** Log in to the witness site and run the **witness reset** command. **b.** Log in to the active site, click **Standalone**, and then click **Continue**. **c.** Replace the nodes at the standby site. **d.** If the witness site will use a virtual machine that's newer than the one that was used previously, complete the steps described in Install the Witness Site, on page 12. Otherwise, proceed to the next step. **e.** Set Up Disaster Recovery, on page 14.

Failure Scenario	System and User Response

Scenario 5: The active, standby, and witness sites go down. The standby and witness sites come back online while the active site remains offline.	1. The system isolates the standby site and then establishes it as the new active site.
	
	2. You are notified that the system has recovered from a two-system failure.
	
	For confirmation, refer to the Monitor the Event Timeline.
	
	3. After the former active site comes back online and enters the **Standby Ready** state, Set Up Disaster Recovery, on page 14.
	
	If you've determined that you need to replace the nodes at the standby site, do the following instead:
	
	  a. Log in to the witness site and run the **witness reset** command.
	
	  b. Log in to the active site, click **Standalone**, and then click **Continue**.
	
	  c. Replace the nodes at the standby site.
	
	  d. If the witness site will use a virtual machine that's newer than the one that was used previously, complete the steps described in Install the Witness Site, on page 12. Otherwise, proceed to the next step.
	
	  e. Set Up Disaster Recovery, on page 14.

Troubleshoot BGP Route Advertisement Issues

If you receive a BGP route advertisement error, complete the following procedure to troubleshoot the cause.

Step 1 From the Catalyst Center cluster, validate the BGP session's status:

a) In the Event Timeline, confirm whether the **Starting BGP advertisement** task completed successfully (**Activate Disaster Recovery System** > **View Details** > **Configure active** > **View Details**).

If the task failed, do the following before proceeding to Step 1b:

1. Check whether the neighbor router indicated in the error message is up.

2. Confirm whether the neighbor router has connectivity with Catalyst Center. If it doesn't, restore connectivity and then retry activating the new disaster recovery system or restarting an existing system that was paused.

b) In the Catalyst Center GUI, view the disaster recovery system's Logical Topology and determine whether the neighbor router is currently active.

If it's down, check whether the Catalyst Center cluster is configured as a BGP neighbor from the router's perspective. If it's not, configure the cluster as a neighbor and then retry activating the new disaster recovery system or restarting an existing system that was paused.

c) Run the following commands to view the bgpd and bgpmanager log files:

    • **sudo vim /var/log/quagga/bgpd.log**

    • **magctl service logs -rf bgpmanager | lql**

When viewing the log files, look for error messages. If you can't find any, this indicates that the BGP session is functioning properly.

d) Check the status of the BGP session between Catalyst Center and its neighbor router by running the following command: **echo** *admin-password*| **sudo VTYSH_PAGER=more -S -i vtysh -c 'show ip bgp summary'**

In the command output, look for the neighbor router's IP address. At the end of the same line, confirm that the router's connection state is listed as **0**. If this is the case, this indicates that the BGP session is active and functioning properly.

Step 2   From the neighbor router indicated in the error message, validate the BGP session's status:

a) Run the **show ip bgp summary** command.

b) In the command output, look for the Catalyst Center cluster's virtual IP address. At the end of the same line, confirm that the cluster's connection state is listed as **0**. If this is the case, this indicates that the BGP session is active and functioning properly.

c) Run the **show ip route** command.

d) View the command's output and confirm whether the disaster recovery system's Enterprise virtual IP address is being advertised.

For example, say your system's Enterprise virtual IP address is 10.30.50.101. If this is the first IP address that you see in the output, this confirms that it is being advertised.