Disaster Recovery

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

Feature Name	Release Information	Description
Disaster Recovery for Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco vManage Release 19.2.1	This feature helps you configure Cisco SD-WAN Manager in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances.
Disaster Recovery for a 6 Node Cisco SD-WAN Manager Cluster.	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature provides support for disaster recovery for a 6 node Cisco SD-WAN Manager cluster.
Disaster Recovery for a Single Node Cisco SD-WAN Manager Cluster	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature provides support for disaster recovery for a Cisco SD-WAN Manager deployment with a single primary node.
Disaster Recovery User Password Change	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature lets you change the disaster recovery user password for disaster recovery components from the Cisco SD-WAN Manager **Disaster Recovery** window.

Feature Name	Release Information	Description
Disaster Recovery Alerts	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 Also: Cisco IOS XE Release 17.6.4 and later 17.6.x releases Cisco SD-WAN Manager Release 20.6.4 and later 20.6.x releases	You can configure Cisco SD-WAN Manager alerts to generate an alarm and a syslog message for any disaster recovery workflow failure or event that occurs.
Disaster Recovery Reliability Improvements Phase 1	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature removes the **Pause Replication** button from the **Disaster Recovery** screen. Replication pauses automatically when you pause disaster recovery and resumes when you resume disaster recovery.

Information About Disaster Recovery

Of the three controllers that make up the Cisco Catalyst SD-WAN solution (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator), Cisco SD-WAN Manager is the only one that is stateful and cannot be deployed in an active/active mode. The goal of the disaster recovery solution is to deploy Cisco SD-WAN Manager across two data centers in primary/secondary mode.

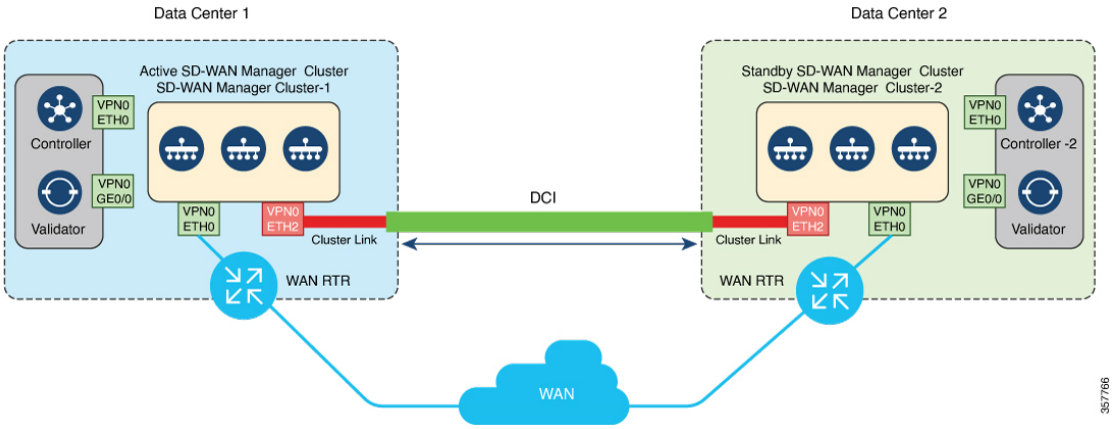
Disaster recovery provides an administrator-triggered failover process. When disaster recovery is registered, data is replicated automatically between the primary and secondary Cisco SD-WAN Manager clusters. You manually perform a failover to the secondary cluster if needed.

Disaster recovery is validated as follows:

- For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco SD-WAN Release 20.4.1, disaster recovery is validated for a three-node cluster.
- In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco SD-WAN Release 20.4.1, disaster recovery is validated for a six-node cluster.
- In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco SD-WAN Release 20.5.1, disaster recovery is validated for a deployment with a single primary node.

Architecture Overview

The following figure illustrates the high-level architecture of the disaster recovery solution.



Prerequisites

Before registering disaster recovery, ensure that you have met the following requirements:

- Ensure that you have two Cisco SD-WAN Manager clusters that contain the specific number of nodes as validated for your release. (The validated number of nodes for each release is described earlier in this chapter.)
- Ensure that the primary and the secondary cluster are reachable by HTTPS on a transport VPN (VPN 0).
- Ensure that Cisco Catalyst SD-WAN Controllers and Cisco Catalyst SD-WAN Validators on the secondary cluster are connected to the primary cluster.
- Ensure that the Cisco SD-WAN Manager nodes in the primary cluster and secondary cluster are running the same Cisco SD-WAN Manager version.
- Configure an out-of-band or cluster interface on the VPN 0 of each Cisco SD-WAN Manager node that is to be used for disaster recovery. This interface is the same one that Cisco SD-WAN Manager uses to communicate with its peers in a cluster.
- Ensure you change the localhost address of the primary Cisco SD-WAN Manager server to an out-of-band IP address. This is necessary even if the Cisco SD-WAN Manager is a standalone node.

Note For information on configuring the cluster IP address, see Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server.

- Ensure that all Cisco SD-WAN Manager nodes can reach each other through the out-of-band interface.
- Ensure that all services (application-server, configuration-db, messaging server, coordination server, and statistics-db) are enabled on all Cisco SD-WAN Manager nodes in the cluster.
- Ensure that all Cisco SD-WAN Manager nodes in a cluster reside on the same LAN segment.
- To allow Cisco SD-WAN Manager clusters to communicate with each other across data centers, enable TCP ports 8443 and 830 on your data center firewalls.
- Distribute all controllers, including Cisco Catalyst SD-WAN Validators, across both primary and secondary data centers. Ensure that these controllers are reachable by Cisco SD-WAN Manager nodes that are distributed across these data centers. The controllers connect only to the primary Cisco SD-WAN Manager cluster.
- Distribute each Cisco SD-WAN Manager VM on a separate physical server so that a single physical server outage does not affect the Cisco SD-WAN Manager cluster in a data center.
- Make sure that no other operations are in process in the active (primary) and the standby (secondary) Cisco SD-WAN Manager cluster. For example, make sure that no servers are in the process of upgrading or no templates are in the process of attaching templates to devices.
- Disable the Cisco SD-WAN Manager HTTP/HTTPS proxy server if it is enabled. See HTTP/HTTPS Proxy Server for Cisco SD-WAN Manager Communication with External Servers. If you do not disable the proxy server, Cisco SD-WAN Manager attempts to establish disaster recovery communication through the proxy IP address, even if Cisco SD-WAN Manager out-of-band cluster IP addresses are directly reachable. You can re-enable the Cisco SD-WAN Manager HTTP/HTTPS proxy server after disaster recovery registration completes.
- Ensure the Cisco Catalyst SD-WAN Validator has the tunnel-interface configuration in place and it allows the SSH connectivity.
- Before you start the disaster recovery registration process, go to the **Tools** > **Rediscover Network** window on the primary Cisco SD-WAN Manager node and rediscover the Cisco Catalyst SD-WAN Validators.

Best Practices and Recommendations

- Ensure that you use a netadmin user privilege for Disaster Recovery registration. We recommend that you modify the factory-default password, admin before you start the registration process.
- When you configure the IP address that the Cisco SD-WAN Validator uses for Disaster Recovery authentication, specify the VPN 0 interface IP address of the Cisco SD-WAN Validator that is reachable by both the primary and secondary Cisco SD-WAN Manager clusters. If tunnel-interface is configured NETCONF must be allowed on the tunnel-interface.
- To change user credentials, we recommend that you use the Cisco SD-WAN Manager GUI, and not use the CLI of a Cisco Catalyst SD-WAN device.

- If Cisco SD-WAN Manager is configured using feature templates, ensure that you create separate feature templates for both the primary cluster and the secondary cluster. Create these templates in the primary cluster. After templates replicate to the secondary cluster, you can attach devices to templates in the secondary cluster.
- For an on-premises deployment, ensure that you regularly take backup of the Configuration database from the active Cisco SD-WAN Manager instance.
- Ensure that you use only a bulit-in admin user privilege to restore config DB and to onboard controllers.
- To configure new Cisco SD-WAN Validators, deregister disaster recovery on Cisco SD-WAN Manager. Then, add the new Cisco SD-WAN Validator on the active cluster and then re-register with the new Cisco SD-WAN Validator.

Enable Disaster Recovery

You need to bring up two separate clusters with no devices being shared, which means do not share any Cisco SD-WAN Controller, or Cisco SD-WAN Validator or Cisco SD-WAN Manager device.

Perform these actions:

- Bring up the secondary Cisco SD-WAN Manager cluster.
- Ensure reachability between the primary cluster, secondary cluster, and Cisco SD-WAN Validator instances.

Register Disaster Recovery

Disaster Recovery must be registered on the primary Cisco SD-WAN Manager cluster. You can use the out-of-band IP address of a reachable Cisco SD-WAN Manager node in the cluster for disaster recovery registration.

The registration can take up to 30 minutes to complete. After the registration starts, the message “No Data Available” may display for a short time in the Disaster Registration Task View. During the registration process, the message “In-progress” displays.

In releases before Cisco Catalyst SD-WAN Manager Release 20.13.1, Cisco SD-WAN Manager nodes restart after registration. If you see the message "Error occurred retrieving status for action disaster_recovery_registration," click the **Reload** button in your browser after the last active Cisco SD-WAN Manager node restarts.

Beginning with Cisco Catalyst SD-WAN Manager Release 20.13.1, nodes do not restart after registration.

If you need to upgrade your Cisco SD-WAN Manager software in the future, pause disaster recovery, perform the upgrade, and then resume disaster recovery. When upgrading Cisco SD-WAN Manager, follow the best practices as described in Cisco SD-WAN Manager Cluster Creation and Troubleshooting.

Before a Cisco SD-WAN Manager maintenance window starts, pause disaster recovery. When the maintenance is complete, resume disaster recovery and ensure that all Cisco SD-WAN Manager nodes are up and running.

1. Log in to Cisco SD-WAN Manager as the netadmin user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Disaster Recovery**.

3. Click **Manage Disaster Recovery**.
4. To configure the primary and secondary cluster, on the Cisco SD-WAN Manager Disaster Recovery screen, select an IP address for any Cisco SD-WAN Manager node within the respective cluster.

   If a cluster is behind a load balancer, specify the IP address of the load balancer.
5. Specify the following: **Start Time**, **Replication Interval**, and **Delay Threshold** for replicating data from the primary to the secondary cluster.

   The default value for **Delay Threshold** is 30 minutes.

   The default value for **Replication Interval** is 15 minutes.
6. From the Cisco SD-WAN Manager menu, choose **Administration > Disaster Recovery**, and for Cluster 2 (Secondary), click **Make Primary**.

   It can take 10 to 15 minutes to push all changes from all the devices.
7. You can also decide to pause disaster recovery by clicking **Pause Disaster Recovery**, pause replication by clicking **Pause Replication** (in releases before Cisco Catalyst SD-WAN Manager Release 20.13.1), or delete your disaster recovery registration.

   After disaster recovery is registered and you have replicated data, you can view the following:

   - When your data was last replicated, how long it took to replicate, and the size of the data that was replicated.
   - When the primary cluster was switched over to the secondary cluster and the reason for the switchover.
   - The replication schedule and the delay threshold.

Verify Disaster Recovery Registration

After you register disaster recovery, do the following:

- Verify that replication from the primary cluster to the secondary cluster happens at the configured intervals.
- Perform a status check by choosing **Administration > Disaster Recovery**.

If disaster recovery registration fails, verify the following:

- Reachability to the Cisco SD-WAN Validator from all cluster members on the secondary cluster.
- Reachability between the secondary cluster and primary cluster on the transport interface (VPN 0).
- Check that you have the correct user name and password.

Delete Disaster Recovery

If you want to delete disaster recovery, we recommend that you initiate the delete operation on the primary cluster. Before deleting, make sure that there is no data replication session in pending state, and make sure that the secondary cluster is not importing data.

If the primary Cisco SD-WAN Manager cluster is down, you can perform the delete operation on the secondary Cisco SD-WAN Manager cluster.

If any Cisco SD-WAN Manager cluster that was offline during the disaster recovery delete operation come on line, execute the following POST request on that cluster to complete the delete disaster recovery operation:

POST /dataservice/disasterrecovery/deleteLocalDC

After you delete disaster recovery, makes sure that the primary and secondary clusters are operating correctly. To do so, go to the **Administration** > **Cluster Management** window and make sure that all Cisco SD-WAN Manager nodes are present in the cluster. If the nodes are not present, restart the application server. Also go to the **Administration** > **Disaster Recovery** window and make sure that no nodes appear.

Data centers must be deleted from disaster recovery before you can reregister disaster recovery for the data centers.

Perform an Administrator-Triggered Failover

To perform an administrator-triggered failover, perform the following these steps.

Note When a standby cluster becomes active, it does not inherit ZTP settings from the other cluster. After the failover completes, enable ZTP for the new active cluster as described in Start the Enterprise ZTP ServerStart the Enterprise ZTP Server.

1. Detach templates from Cisco SD-WAN Manager devices in the primary cluster.
2. Shut off the tunnel interfaces on the primary Cisco SD-WAN Manager cluster to prevent devices from toggling during the switchover.
3. From a Cisco SD-WAN Manager system on the secondary cluster, choose **Administration** > **Disaster Recovery**.
4. Wait for data replication to complete, then click **Make Primary**.

   Devices and controllers converge to the secondary cluster and that cluster assumes the role of the primary cluster. When this process completes, the original primary cluster assumes the role of the secondary cluster. Then data replicates from the new primary cluster to the new secondary cluster.

To move back to the original primary cluster, repeat these steps.

Disaster Recovery Operations

This sections explains how to perform disaster recovery in a variety of situations.

Loss of Primary Cisco SD-WAN Manager Cluster

If your primary Cisco SD-WAN Manager cluster goes down, follow these steps for disaster recovery:

1. From a Cisco SD-WAN Manager system on the secondary cluster, choose **Administration** > **Disaster Recovery**.
2. Click **Make Primary**.

Devices and controllers converge to the secondary cluster and that cluster assumes the role of the primary cluster.

When the original primary cluster recovers and is back on line, it assumes the role of the secondary cluster and begins to receive data from the primary cluster.

Loss of Primary Data Center

If your primary data center cluster goes down, follow these steps for disaster recovery:

1. From a Cisco SD-WAN Manager system on the secondary cluster, choose **Administration** > **Disaster Recovery**.
2. Click **Make Primary**.

   The switchover process begins. During the process, only the Cisco SD-WAN Validators in the secondary data center are updated with a new valid Cisco SD-WAN Manager list. Devices and controllers that are on line converge to the secondary cluster and that cluster assumes the role of the primary cluster.

   After the original primary data center recovers and all VMs, including controllers, are back on line, the controllers are updated with a new valid Cisco SD-WAN Manager and converge to the new primary Cisco SD-WAN Manager cluster. The original primary cluster assumes the role of secondary cluster and begins to receive data from the primary cluster.

Partial Loss of Primary Cisco SD-WAN Manager Cluster

If you experience a partial loss of the primary Cisco SD-WAN Manager cluster, we recommend that you try to recover that cluster instead of switching over to the secondary cluster.

A cluster with N nodes is considered to be operational if (N/2)+1 nodes are operational.

A cluster with N nodes becomes read only if (N/2)+1 or more nodes are lost.

Loss of Enterprise Network Between Data Centers

If a link failure occurs between your data centers but the WAN in the primary data center is operational, data replication fails. In this situation, attempt to recover the link so that data replication can resume.

To avoid a possible split brain scenario, do not perform a switchover operation.

Changing the Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Validator Administrator Password

For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you use Cisco SD-WAN Manager to change a user password that you entered during disaster recovery registration, first deregister disaster recovery from the Cisco SD-WAN Manager cluster, change the password, and then reregister disaster recovery on the cluster.

Changing the Disaster Recovery User Password for Disaster Recovery Components

During disaster recovery registration, you provide the user name and password of a Cisco SD-WAN Manager or a Cisco SD-WAN Validator user for the following disaster recovery components. You can provide the name and password of the same user for each of these components, or you can provide the names and passwords of different users for various components. The user names and passwords that you provide for a component identify the *disaster recovery user* who can access disaster recovery operations on the component.

- Cisco SD-WAN Manager servers in the active (primary) and standby (secondary) clusters. These components use the password of a Cisco SD-WAN Manager user.
- Each Cisco SD-WAN Validator. This component uses the password of a Cisco SD-WAN Validator user.

If you change the Cisco SD-WAN Manager or Cisco SD-WAN Validator password of a disaster recovery user, you must change the disaster recovery component password for this user to the new password.

To change a password for the disaster recovery user, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Disaster Recovery**.
2. Click **Pause Disaster Recovery**, and then click **OK** in the **Pause Disaster Recovery** dialog box that is displayed.

   Data replication between the primary and secondary data centers stops and this option changes to **Resume Disaster Recovery**.
3. Click **Manage Password**.
4. In the **Manage Password** window, perform these actions:
   a. Click **Active Cluster**, and in the **Password** field that appears, enter the new active cluster password for the disaster recovery user.
   b. Click **Standby Cluster**, and in the **Password** field that appears, enter the same password that you entered in the **Active Cluster** field for the disaster recovery user.
   c. Click **Validator**, and in each **Password** field that appears, enter the new Cisco Catalyst SD-WAN Validator password for the disaster recovery user. There is one **Password** field for each Cisco SD-WAN Validator.
   d. Click **Update**.

      The passwords are updated and the **Manage Password** window closes.
5. Click **Resume Disaster Recovery**, and then click **OK** in the **Resume Disaster Recovery** dialog box that is displayed.

   Data replication between the primary and secondary data centers restarts.

Configure Disaster Recovery Alerts

Minimum supported releases:
Cisco vManage Release 20.9.1
Cisco vManage Release 20.6.4 and later 20.6.x releases

You can configure Cisco SD-WAN Manager alerts to generate an alarm and a syslog message for any disaster recovery workflow failure or event that occurs. You can then monitor disaster recovery workflows and events through syslog notifications, event notifications, and webhooks.

To configure disaster recovery alerts, follow these steps:

1. On any Cisco SD-WAN Manager server in the primary cluster, pause Disaster Recovery by choosing **Administation** > **Disaster Recovery** and clicking **Pause Disaster Recovery**.
2. On any Cisco SD-WAN Manager server in the primary cluster and any Cisco SD-WAN Manager server in the secondary cluster, enable **Alarm Notifications** in the **Administation** > **Settings** window.

   See “Enable Email Notifications” in Alarms in *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.
3. Perform the following actions on any Cisco SD-WAN Manager server in the primary cluster and any Cisco SD-WAN Manager server in the secondary cluster to define a disaster recovery alarm notification rule:
   a. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs**.
   b. Click **Alarms**.
   c. Click **Alarm Notifications**.
   d. Click **Add Alarm Notification**.
   e. From the **Severity** drop-down list, choose the severity of the events for which an alarm is generated.
   f. From the **Alarm Name** drop-down list, choose **Disaster Recovery**.
   g. Configure other options for the rule as needed.

      For detailed instructions, see “Send Alarm Notifications” in Alarms in *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.
   h. In the **Select Devices** area, click **Custom**.
   i. Choose the Cisco SD-WAN Manager servers for which the disaster recovery alarms are generated by clicking the corresponding devices in the **Available Devices** list and then clicking the arrow to move them to the **Selected Devices** list.
   j. Click **Add**.
4. On any Cisco SD-WAN Manager server in the primary cluster, restart Disaster Recovery by choosing **Administration** > **Disaster Recovery** and clicking **Resume Disaster Recovery**.

After you configure disaster recovery alerts, from each Cisco SD-WAN Manager server in the primary cluster and secondary cluster, configure logging of syslog messages to a local device and remote device, if needed. For instructions, see "Log Syslog Messages to a Local Device" and "Log Syslog Messages to a Remote Device"

in Configure System Logging Using CLI in *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide*.