

Disaster Recovery

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 six 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 six 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.
Multitenancy Support for Disaster Recovery	Cisco IOS XE Release 17.6.x Cisco vManage Release 20.6.x	This feature provides support for multitenancy in disaster recovery.
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, on page 2
- Architecture Overview, on page 3
- Prerequisites for Registering Disaster Recovery, on page 4
- Guidelines for Registering Disaster Recovery, on page 6
- Workflow for Disaster Recovery, on page 6
- Disaster Recovery Operations, on page 9
- Changing the Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Validator Administrator Password Used for Disaster Recovery, on page 10
- Configure Disaster Recovery Alerts, on page 12
- Upgrade Disaster Recovery Overlays, on page 13
- Add or Delete Cisco SD-WAN Control Components from the Disaster Recovery Overlays, on page 14
- How Features Operate When Disaster Recovery is Enabled, on page 14

Information About Disaster Recovery

In the Cisco Catalyst SD-WAN solution, which includes Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator, only the Cisco SD-WAN Manager is stateful and can't be deployed in an active/active mode. The disaster recovery solution aims to deploy Cisco SD-WAN Manager across two data centers in primary/secondary mode.

The user account used for disaster recovery supports only local authentication and does not support remote authentication methods such as TACACS+ or RADIUS. This user must be dedicated solely to disaster recovery tasks and must not be used for any other functions, such as cluster management because of the following reasons:

- Reliability: Using dedicated accounts for DR sync minimizes configuration errors and reduces operational risks.

- Resilience: Prevents issues related to user lockouts or account overrides, ensuring DR processes are not impacted by administrative changes to other accounts.
- Audit and compliance: Dedicated users provide clear separation for auditing purposes, making it easier to track and log DR-related activities.
- Industry standard: All our customers, including those in highly regulated sectors such as finance, follow this model. It is the recommended and supported deployment standard.
- Avoid remote authentication issues: TACACS-based users are prone to disruptions due to potential latency or connectivity issues with remote authentication servers. Using local accounts eliminates these risks, ensuring uninterrupted DR sync and cluster operations.
- Password rotation: Capabilities are provided via API/GUI on active cluster and through CLI on standby cluster.

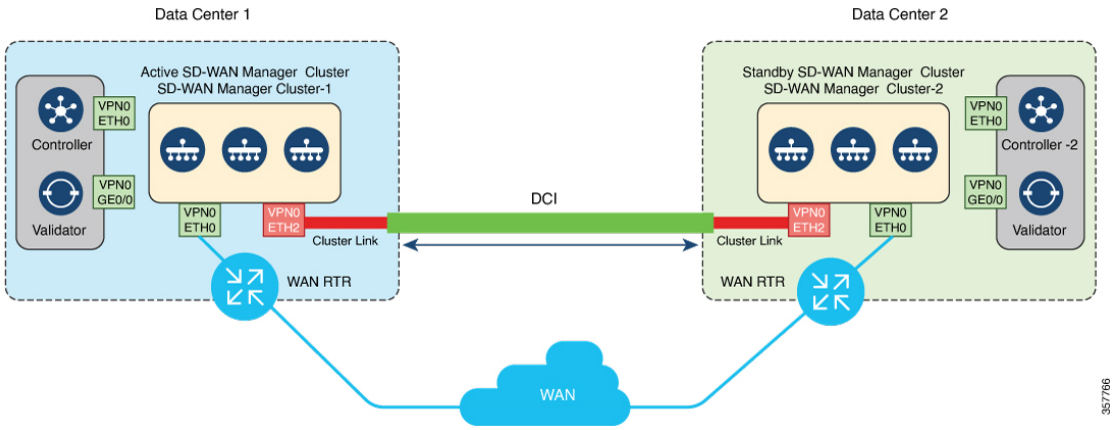
Disaster recovery provides an administrator-triggered failover process. When disaster recovery is registered, data is replicated automatically between the primary and secondary Cisco SD-WAN Manager clusters. If necessary, you can manually initiate a failover to the secondary cluster.

Disaster recovery is validated for these setups.

Release	Validated for
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco SD-WAN Release 20.4.1, and earlier	Three-node cluster
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and Cisco SD-WAN Release 20.4.1	Six-node cluster
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco SD-WAN Release 20.5.1	Deployment with a single primary node

Architecture Overview

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



Prerequisites for Registering Disaster Recovery

Cluster 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 in the *Information About Disaster Recovery* section.
- 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.
- Ensure that no operations are currently running on either the active or standby 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.

Node Specifications

- Ensure that services such as 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.
- Ensure that both the active and standby Cisco SD-WAN Manager nodes are not in managed mode for disaster recovery to operate effectively.
- 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.

IP Address Configurations

- 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 is the same interface that Cisco SD-WAN Manager uses to communicate with other nodes in a cluster.
- Ensure that you change the local host address of the primary Cisco SD-WAN Manager 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.

User Configurations

Create a new local netadmin username and password that are identical on both the active and standby Cisco SD-WAN Manager nodes. Use this newly created user exclusively for disaster recovery registration instead of the default admin user. This user must be dedicated solely to disaster recovery tasks and must not be used for any other functions, such as cluster management.

Control Components Configurations

- 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 located in these data centers. The controllers connect only to the primary Cisco SD-WAN Manager cluster.
- 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.
- Ensure the Cisco Catalyst SD-WAN Validator has the tunnel-interface configuration in place and it allows SSH connectivity.

Device Switchover

- Enable TCP ports 8443 and 830 on your data center firewalls to allow Cisco SD-WAN Manager clusters to communicate with each other across data centers.

  During a device switchover, active Cisco SD-WAN Manager interacts with Cisco SD-WAN Validator or Cisco SD-WAN Controller through Netconf (port 830) for initial connection. To connect the cluster, shutdown the tunnel interface and configure controller serial list to controller components through Netconf (port 830). If port 830 is unavailable, the Cisco SD-WAN Manager fails.. and shuts down the tunnel interface.

Proxy Configuration

- To configure an HTTP/HTTPS proxy before setting up disaster recovery, rnsure that the Cisco SD-WAN Manager's HTTP/HTTPS proxy server is disabled if it is currently active. See HTTP/HTTPS Proxy Server for Cisco SD-WAN Manager Communication with External Servers. If you don't disable the proxy server, Cisco SD-WAN Manager attempts to establish disaster recovery communication through the proxy IP address, even when the out-of-band cluster IP addresses are reachable.

  You can re-enable the Cisco SD-WAN Manager HTTP/HTTPS proxy server after disaster recovery registration is complete.

SD-AVC Configuration

- If you wish to enable Cisco Software-Defined Application Visibility and Control (SD-AVC) and disaster recovery is already configured, first delete the existing disaster recovery. Next, enable Cisco SD-AVC on both the primary and secondary nodes. Re-register Disaster Recovery to proceed.

Cisco SD-WAN Validator Configurations

For a successful disaster recovery registration, configure a tunnel interface with netconf service enabled on a VPN 0 interface.

This is an example of a Cisco SD-WAN Validator configuration:

```
vpn 0
interface ge0/0
ip address 10.0.46.6/24
tunnel-interface
encapsulation ipsec
allow-service netconf
```

Guidelines for Registering Disaster Recovery

IP Address and Configurations

- Specify the VPN 0 interface IP address when you configure the IP address that the Cisco SD-WAN Validator uses for disaster recovery authentication. Ensure that the IP address is reachable by both the primary and secondary Cisco SD-WAN Manager clusters. If a tunnel interface is configured, make sure that NETCONF is permitted on it.
- Before you configure a new Cisco SD-WAN Validator, deregister disaster recovery on Cisco SD-WAN Manager. Then, add the new Cisco SD-WAN Validator on the active cluster and re-register with the new Cisco SD-WAN Validator.
- The system configurations on Cisco SD-WAN Manager should be identical on all the active and standby nodes.

Disaster Recovery Operations

- Regularly take backup of the configuration database from the active Cisco SD-WAN Manager instance. See, request nms configuration-db command. Use only a system administrator user to restore configuration database and to onboard Cisco Catalyst SD-WAN Control Components.
- Pause disaster recovery before initiating manual disaster recovery. Performing manual switchover operation while disaster recovery is active can lead to cluster failure.
- Configuration changes via Command Line Interface is not recommended on standby nodes.

Replication history

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) The replication logs are retained for one year. Any historical data older than one year is automatically pruned.

Workflow for Disaster Recovery

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 two separate Cisco SD-WAN Manager clusters without devices and Cisco Catalyst SD-WAN Control Components.
- The active cluster is onboarded with Cisco Catalyst SD-WAN Control Components and edge devices that are not shared with the standby cluster.
- For disaster recovery on a single node Cisco SD-WAN Manager, configure both the primary and secondary nodes with cluster IP address on the **Cluster Management** page.
- Ensure that there is connectivity between the primary and secondary clusters through the cluster IP interface.

Register Disaster Recovery

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 registration task view on Cisco SD-WAN Manager. During the registration process, the message **In-progress** is displayed.

For Cisco Catalyst SD-WAN Manager Release 20.13.1 and earlier releases, 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.

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

Before you begin

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.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the netadmin user.

Step 2 Use the netadmin user, which was specifically created for disaster recovery, for the registration. Use the same user for all disaster recovery operations.

Step 3 From the Cisco SD-WAN Manager menu, choose **Administration > Disaster Recovery**.

Step 4 Click **Manage Disaster Recovery**.

Step 5 To configure the primary and secondary clusters, on the **Manage Disaster Recovery** > **Connectivity Info** page, enter the cluster IP address of any primary and secondary Cisco SD-WAN Manager node and the netadmin user from step 2.

If a cluster is behind a load balancer, specify the IP address of the load balancer.

Step 6 On the **Validator Info** page, enter all the Cisco SD-WAN Validator IP addresses. If you miss adding any Cisco SD-WAN Validator details, it can be added after you delete disaster recovery and enable it again.

Step 7 Choose **Manual** as the type of recovery in the **Recovery Mode**.

Step 8 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.

Note
When there is a failure in data replication, disaster recovery waits for six times the configured replication interval before initiating the next replication cycle. For example, if the replication interval is set to one hour and a failure occurs, disaster recovery waits for an additional 6 hours, resulting in a total wait time of 7 hours before attempting the next replication.

Verify Disaster Recovery Registration

Successful Registration

After successfully registering for disaster recovery, perform status checks as follows:

- Registration Task: Confirm that the registration task is successful.
- Monitor alarms: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**. Check for the **DR Registration Success** alarm.
- Node health: From the Cisco SD-WAN Manager menu, choose **Administration** > **Disaster Recovery**. Confirm that all nodes of both the primary and secondary clusters are displayed. Also verify the health status of the nodes.
- Replication: Verify that replication from the primary cluster to the secondary cluster happens at the configured intervals. Check the delay threshold, the time of last replication, and size of the data that is replicated. Choose **Monitor** > **Logs** > **Alarms** and check for **Primary Successfully Exported** and **Secondary Successfully Imported** alarms.
- Switchover: Verify the time when the primary cluster switched over to the secondary cluster. Additionally, check the reason for the switchover.

Registration Failure

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 cluster interface (VPN 0).
- Check that you have provided the correct user name and password during registration.

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 in progress.

We recommend that you pause disaster recovery to prevent the replication from restarting before a deletion attempt.

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

If any Cisco SD-WAN Manager in an active or standby cluster that was offline during the disaster recovery delete operation comes back online, execute the following POST request on that cluster to complete the delete disaster recovery operation:

POST /dataservice/disasterrecovery/deleteLocalDataCenter

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. Choose **Monitor** > **Logs** > **Alarms** and check for the DR De-Registration Success alarm.

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

Perform an Administrator-Triggered Failover

Procedure

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

Step 2 Choose **Make Primary**.

Step 3 If replication is in progress and the standby cluster is not ready to switchover, **Make Primary** option is not available to trigger the failover.

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.

Disaster Recovery Operations

Loss of Primary Cisco SD-WAN Manager Cluster

Procedure

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

Step 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

Procedure

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

Step 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 online converge to the secondary cluster which assumes the role of the primary cluster.

After the original primary data center recovers and all VMs, including controllers, are back online, 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 there is a link failure between data centers but the WAN in the primary data center is operational, data replication fails. You can attempt to recover the link to resume the data replication.

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 Used for Disaster Recovery

For releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, if you use the 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.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Disaster Recovery**.

Step 2 Click **Pause Disaster Recovery**, and then click **OK**.

Data replication between the primary and secondary data centers stops and this option changes to **Resume Disaster Recovery**.

Step 3 To change the Cisco SD-WAN Manager or Cisco SD-WAN Validator password used for disaster recovery:

- To update the password of Cisco SD-WAN Manager in an active cluster, navigate to **Administration**>**Manage Users** and modify the user's password. For information, refer to the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.
- For a standby cluster, the password must be updated individually on each node. This can be done using the CLI on all Cisco SD-WAN Manager nodes in the standby cluster. For information, refer to the sections about users and access in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Step 4 Click **Manage Password**.

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. There is one **Password** field for each Cisco SD-WAN Validator.
d) Click **Update**.

The passwords are updated and the **Manage Password** window closes.

Step 5 Click **Resume Disaster Recovery**, and then click **OK**.

Data replication between the primary and secondary data centers restarts.

Change the Cisco SD-WAN Manager Password Used to Create the Cisco SD-WAN Manager Cluster with Disaster Recovery Configured

Procedure

Step 1 To change the password of the Cisco SD-WAN Manager cluster that is used to create the active cluster, login to any of the Cisco SD-WAN Manager of the active cluster and navigate to **Administration**> **Manage Users** to edit the user password.

For information, refer to the information about users and access in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Step 2 To change the password of the Cisco SD-WAN Manager cluster that is used to create the standby cluster:

a) Perform switchover to make the standby cluster as the new active cluster. After a successful switchover, ensure that the status of all the services in the **Cluster Management** page is healthy or reachable.

b) Login to any of the Cisco SD-WAN Manager of the new active cluster and navigate to **Administration** > **Manage Users** and edit the user password. For information, refer to the information about users and access in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Configure Disaster Recovery Alerts

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

Procedure

Step 1 On any Cisco SD-WAN Manager server in the primary cluster, pause Disaster Recovery by choosing **Administration** > **Disaster Recovery** and clicking **Pause Disaster Recovery**.

Step 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 **Administration** > **Settings** window.

See Enable Email Notifications section in Alarms in *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 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.

Step 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**.

What to do next

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*.

Upgrade Disaster Recovery Overlays

Upgrade both the active and standby Cisco SD-WAN Manager clusters.

Before you begin

- Use the Command Line Interface method to upgrade both the active and standby Cisco SD-WAN Managers.
- Ensure that the replication status on the **Administration** > **Disaster Recovery** page is stable and not in a transient state such as **Import Pending**, **Export Pending**, or **Download Pending**.
- Pause the disaster recovery before the upgrade using **Pause Disaster Recovery**. For Cisco Catalyst SD-WAN Manager Release 20.13.1 and earlier releases, do not use **Pause Replication**.

  If you upgrade Cisco SD-WAN Manager without pausing disaster recovery the following error occurs: Error: error-reason 'Disaster Recovery is not Paused. Terminating Activation.

Procedure

Step 1 Upgrade the active Cisco SD-WAN Manager nodes. See, Upgrade and Activate procedure described in the *Cisco Catalyst SD-WAN Monitor and Maintain* guide.

Step 2 Upgrade the standby Cisco SD-WAN Manager nodes.

Step 3 Upgrade the Cisco SD-WAN Validators and Cisco SD-WAN Controllers nodes accordingly.

Step 4 Upgrade the WAN edge devices if required.

What to do next

Once upgrade is complete, **UnPause Disaster Recovery** and verify that disaster recovery has resumed. See, Verify Disaster Recovery Registration, on page 8.

Add or Delete Cisco SD-WAN Control Components from the Disaster Recovery Overlays

To add or remove any node in the active or standby Cisco SD-WAN Control Components, perform the following steps:

Before you begin

Cisco SD-WAN Control Components

Procedure

Step 1 Delete disaster recovery.

Step 2 Add or remove the Cisco SD-WAN Control Components.

Step 3 Register disaster recovery.

How Features Operate When Disaster Recovery is Enabled

Zero Touch Provisioning (ZTP)

When a standby cluster becomes active, it does not inherit Zero Touch Provisioning (ZTP) settings from the other cluster. After the failover is complete, enable ZTP for the new active cluster. See, Start the Enterprise ZTP Server.

SD-AVC

It's important to maintain the classification of SD-AVC custom applications, especially during a switchover from a primary to a secondary Cisco SD-WAN Manager.

- Any custom application configured in the primary Cisco SD-WAN Manager under **Configuration**> **Policies**> **Centralized Policy**> **Lists**> **Custom Applications** is automatically replicated to the secondary Cisco SD-WAN Manager.
- After a switchover, a new Cisco SD-WAN Manager becomes primary. You can edit each custom application on the new primary Cisco SD-WAN Manager and save each custom application to ensure a continuity in classification.
- Any new custom applications configured after the switchover does not require an additional edit and save action for continuity in classification.

Note Starting with Cisco Catalyst SD-WAN Manager Release 20.18.1 for single-node deployments and Cisco Catalyst SD-WAN Manager Release 20.13.1 for cluster deployments, SD-AVC custom applications are automatically replicated to the secondary Cisco SD-WAN Manager as part of the disaster recovery process.

From these versions onward, SD-AVC custom applications are backed up within the configuration database and synchronized across the disaster recovery setup, ensuring continuity and consistency of application classification after failover.

User Management

When managing user accounts on a Cisco SD-WAN Manager, it's important to understand the replication behavior between the primary and the secondary Cisco SD-WAN Managers.

- Adding a new user or modifying an existing user on the primary Cisco SD-WAN Manager is automatically replicated to the secondary Cisco SD-WAN Manager when done using the Cisco SD-WAN Manager.
- Deleting a user on the primary Cisco SD-WAN Manager is not replicated to the secondary Cisco SD-WAN Manager. The user account still exists on the secondary Cisco SD-WAN Manager and may need to be deleted manually for consistency across both the Cisco SD-WAN Managers.
- Adding, modifying and deleting the user using the Command Line Interface is not replicated.

HTTP Proxy

When managing HTTP proxy settings in relation to disaster recovery on Cisco Catalyst SD-WAN, perform the following steps:

1. Remove the HTTP proxy from the configuration before proceeding with the disaster recovery registration to avoid any conflicts.
2. HTTP proxy configuration is automatically replicated to the standby Cisco SD-WAN Manager.
3. After a switchover, edit and save the proxy configurations for the HTTP proxy settings to take effect on the new primary Cisco SD-WAN Manager.

Admin-tech Collection and Management

When managing admin-tech data on Cisco SD-WAN Manager, consider the following guidelines:

- Admin-tech data for the primary Cisco SD-WAN Manager can be collected and downloaded using both the Cisco SD-WAN Manager and Command Line Interface (CLI).
- Admin-tech data for the standby Cisco SD-WAN Manager can only be collected and downloaded using the CLI.
- Admin-tech entries are replicated to the standby Cisco SD-WAN Manager but the actual admin-tech files are not transferred.
- After a switchover to the standby Cisco SD-WAN Manager, the replicated admin-tech entries become dummy entries.
- You must manually clean up these dummy entries post-switchover to ensure data integrity and system cleanliness.

Cisco SD-WAN Manager Software Repository

When managing software repository on Cisco SD-WAN Manager, consider the following guidelines:

- Software repository entries are replicated to the standby Cisco SD-WAN Manager. The actual software files are not transferred.
- After a switchover to the standby Cisco SD-WAN Manager, the replicated software repository entries becomes dummy entries.
- You must manually clean up these dummy entries after switchover to ensure data integrity and system cleanliness.

Cisco SD-WAN Manager, Validator, Controller Certificate Renewal

Certificate renewal of primary Cisco SD-WAN Manager, secondary Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Controller should be performed using the following steps when Disaster Recovery (DR) is enabled:

1. Delete Disaster recovery.
2. Renew the necessary certificates for the respective Cisco SD-WAN Manager components using the Control Components Certificate Management workflow available in Cisco SD-WAN Manager.

   This workflow supports both automatic and manual renewal methods.
3. After successful certificate renewal, register the DR again to resume disaster recovery operations.

For Cisco IOS XE Catalyst SD-WAN device certificate renewal, certificates can be renewed while DR is enabled.

However, an administrator triggered failover should only be performed after at least one successful replication to ensure that the edge device certificate renewals are up to date on the standby Cisco SD-WAN Manager.