Multitenancy: Disaster Recovery

Disaster recovery for a multitenant Cisco SD-WAN Manager cluster

Summary

If a Multitenant Cisco SD-WAN Manager cluster or the data center hosting the SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby SD-WAN Manager cluster. You can perform disaster recovery as follows:

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Managercluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active CSD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

What’s next

To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

Prerequisites for a multitenant disaster recovery

Follow these prerequisites for a successful migration.

- The number of SD-WAN Manager nodes in the active and standby clusters must match.
- Each SD-WAN Manager node in the active and standby clusters must run the same SD-WAN Manager software release.
- Each SD-WAN Manager node in the active and standby clusters must connect to the WAN transport IP address of the SD-WAN Validator in the overlay network.
- Initially, disable the tunnel interfaces of the SD-WAN Manager nodes in the standby cluster.
- Certify the SD-WAN Manager nodes in the standby cluster.
- Synchronize the clock of every SD-WAN Manager node in the standby cluster with the clocks of the SD-WAN Controller and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby SD-WAN Manager nodes.
- Use identical Neo4j credentials on the SD-WAN Manager nodes in the active and standby clusters.

Restrictions for a multitenant disaster recover

Defines restrictions to backup and restore process during disaster recovery of a SD-WAN Manager cluster.

- Do not interrupt any active processes while backing up the configuration database.
- Enable SD-AVC before restoring the configuration database on the standby SD-WAN Manager node.

Configure a standby SD-WAN Manager cluster

To prepare standby SD-WAN Manager nodes with a unique yet synchronized configuration for disaster recovery without impacting the active overlay network.

Procedure

Step 1 Configure the standby SD-WAN Manager nodes with a running configuration similar to the active SD-WAN Manager nodes and install local certificates.

The running configuration on a standby node is usually identical to an active node, but ensure settings such as system IP address and tunnel interface IP address are unique.

Step 2 On the standby nodes, shut down the transport interface in VPN 0 using the CLI shutdown command in the transport interface configuration.

Step 3 Create a standby cluster using the configured standby SD-WAN Manager nodes.

Step 4 With this configuration, the overlay network remains unaware of the standby SD-WAN Manager cluster.

Back up the active SD-WAN Manager cluster configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active SD-WAN Manager virtual machines.

Procedure

Step 1 Choose an active SD-WAN Manager node that hosts the configuration database service.

Step 2 On the CLI of the selected node, run the following command to back up the configuration database: **request nms configuration-db backup path <file-path>**

The command saves the configuration database as a `.tar.gz` file in the specified file path.

Example:

In the example below, the database is backed up to a file named db_backup.tar.gz in the /home/admin/ directory.

```
Active-vManage#
request nms configuration-db backup path /home/admin/db_backup
Successfully saved database to /home/admin/db_backup.tar.gz
```

Step 3 Choose a standby SD-WAN Manager node that hosts the configuration database service and copy the configuration database backup to this node.

Example:

In the following example, db_backup.tar.gz is copied from the active SD-WAN Managernode to the /home/admin/ directory of a standby SD-WAN Manager node.

```
Active-vManage#
request execute vpn 512 scp /home/admin/db_backup.tar.gz admin@10.126.93.92:/home/admin
The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
Are you sure you want to continue connecting (yes/no)?
yes
Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
viptela 18.4.5

admin@10.126.93.92's password:
db_backup.tar.gz                                100%  399KB   4.4MB/s   00:00
```

Restore SD-WAN Manager cluster using the configuration database backup

Restore the most recent backup of the configuration database from the active SD-WAN Manager cluster on the standby SD-WAN Manager node to which the backup was copied.

- The restore operation does not restore all configuration details. Settings such as users and repositories must be configured on the standby SD-WAN Manager node after restoring the backup.

- When you complete the steps that follow, the previously active SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

Procedure

Step 1 On the CLI of the standby SD-WAN Manager node, run the following command: r**equest nms configuration-db restore path** *file-path*.

Example:

In the following example, the configuration database is restored using the backup file db_backup.tar.gz.

```
Standby-vManage#
request nms configuration-db restore path /home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

Step 2 Verify standby SD-WAN Manager nodes.

a) Verify that all appropriate services are running on each standby SD-WAN Manager node.

   On the CLI of each standby node, run: **request nms all status**

   From the command output, confirm that the necessary services are active.

b) Verify that every standby node maintains a list of all active and standby SD-WAN Manager nodes:

   1. From the SD-WAN Manager, navigate to **Configuration** > **Devices** > **Controllers**.
   2. Confirm that the page displays all active and standby SD-WAN Manager nodes.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed **Control Components** to align with Cisco Catalyst SD-WAN rebranding.

Step 3 On the standby SD-WAN Manager nodes, enable the transport interface on VPN 0 using one of these two methods:

a) Enable the transport interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **no shutdown** command.

   Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Activate the tunnel interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **tunnel-interface** command.

   Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

Step 4 Add each standby SD-WAN Manager node to the overlay network.

a) From the Cisco SD-WAN Manager menu, choose **Configuration >** > **Devices**.
b) Click **Controllers**.
c) For a SD-WAN Validator, click **...** and click **Edit**.
d) In the **Edit** dialog box, enter the following details of the SD-WAN Validator: WAN transport IP address, username, and password.

e) Repeat **Step 4c** and **Step 4d** for every SD-WAN Validator.

Step 5 Disconnect the active SD-WAN Manager nodes from the overlay network using one of these methods.

a) Shut down the transport interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Deactivate the tunnel interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **no tunnel-interface** command.ste

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach SD-WAN Manager instances in an actual disaster scenario, you may not be able to perform this step and can omit the step.

Step 6 From the standby SD-WAN Manager send the updated controller and device list to the SD-WAN Validator, including the list of controllers:

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) Click **Send to Validator**.

Wait for the configuration task to complete. When the task is complete,

- The standby SD-WAN Manager nodes become the active Cisco SD-WAN Manager nodes.
- The previously active SD-WAN Manager nodes are no longer part of the overlay network.
- The active SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

d) Click **WAN Edge List.**
e) Click **Send to Controllers**.

Step 7 Verify configuration and connectivity

a) Verify that policies, templates, and the controller and WAN edge device lists are intact.
b) Verify valid SD-WAN Manager nodes:

1. On each SD-WAN Validator, log in to the CLI and run: **show orchestrator** *valid-vmanage-id*.
2. Confirm that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.
3. On a WAN edge device, log in to the CLI and run: **show control** *valid-vmanage-id*.
4. Confirm that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.

5. Check that the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Step 8 Invalidate the previously active SD-WAN Manager nodes.

After you invalidate the SD-WAN Manager, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) For each previously active SD-WAN Manager node, click **...** and click **Invalidate**.

Verify the valid SD-WAN Manager nodes

Procedure

Step 1 Log in to the CLI of each SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active SD-WAN Manager nodes are listed.

Step 2 Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Disaster recovery in an overlay network with virtual routers

The following disaster recovery procedure applies to an overlay network in which Cisco vEdge Cloud routers are deployed at branch locations.

Summary

If a Multitenant SD-WAN Manager cluster or the data center hosting the SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby SD-WAN Manager cluster. You can perform disaster recovery as follows:

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active SD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

5. To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

What's next

See these sections, before you proceed.

- Restrictions for a multitenant disaster recover
- Prerequisites for a multitenant disaster recovery
- Configure a standby SD-WAN Manager cluster
- Back up the active SD-WAN Manager cluster configuration

Restore SD-WAN Manager cluster using the configuration database backup

Restore the most recent backup of the configuration database from the active SD-WAN Manager cluster on the standby SD-WAN Manager node to which you copied this backup.

- The restore operation does not restore all the information included in the configuration database. SD-WAN Manager configurations such as users and repositories must be configured on the standby SD-WAN Manager node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

Procedure

Step 1 On the CLI of the standby SD-WAN Manager node, run the following command: **request nms configuration-db restore path** *file-path*

Example:

In the following example, the configuration database is restored using the backup file db_backup.tar.gz.

```
Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
Configuration database is running in a standalone mode
Importing database...Successfully restored database
```

Step 2 Verify services and node list on the standby SD-WAN Manager nodes

a) Verify that the appropriate services are running on the standby SD-WAN Manager nodes: On the CLI of each standby SD-WAN Manager node, run the **request nms all status** command.

   From the command output, verify the services running on the node.

b) Verify that every standby SD-WAN Manager node has a list of all the active and standby SD-WAN Manager nodes.

1. From the SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**.
2. Verify that the page displays all active and standby SD-WAN Manager nodes.

Step 3 Run the these commands:

a) Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

b) Log in to the CLI of Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.

Step 4 Enable the transport interface on VPN 0 on the standby SD-WAN Manager nodes using either of the following methods:

a) Enable the transport interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **no shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Activate the tunnel interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **tunnel-interface** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

Step 5 Add each standby SD-WAN Manager node to the overlay network.

a) From the SD-WAN Manager menu, choose **Configuration > > Devices**.

b) Click **Controllers**.

c) For a Cisco SD-WAN Validator, click **...** and click **Edit**.

a) In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.

b) Repeat **Step 5c** and **Step 5d** for every Cisco SD-WAN Validator.

Step 6 Disconnect the active SD-WAN Manager nodes from the overlay network using one of the following two methods.

a) Shut down the transport interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **shutdown** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

b) Deactivate the tunnel interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **no tunnel-interface** command.

Example:

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

Step 7 From the standby SD-WAN Manager, send the updated controller and device list to the Cisco SD-WAN Validator.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates** .
b) Click **Controllers**.
c) Click **Send to Validator**.

Wait for the configuration task to complete. When the task is complete,

- The standby SD-WAN Manager nodes become the active SD-WAN Manager nodes.
- The previously active SD-WAN Manager nodes are no longer part of the overlay network.
- The active SD-WAN Manager nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

d) Click **WAN Edge List**.
e) Click **Send to Controllers**.

Step 8 Verify configuration and connectivity.

a) Verify that policies, templates, and the controller and WAN edge device lists are intact.
b) Verify valid SD-WAN Manager nodes:

1. Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.
2. Log in to the CLI of a Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.
3. In the command output, verify that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.
4. Check whether the device is connected to the active SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Step 9 Invalidate the previously active SD-WAN Manager nodes.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) For each previously active SD-WAN Manager node, click **...** and click **Invalidate**.

a. The previously active SD-WAN Manager is the certificate issuer for the cloud WAN edge devices. The active SD-WAN Manager issues certificates to the cloud WAN edge devices only after the previously active SD-WAN Manager nodes are invalidated.

b. After you invalidate the SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

c. When you invalidate the previously active SD-WAN Manager nodes, SD-WAN Manager marks the nodes as invalid and sends an update to all controllers. However, SD-WAN Manager does not send an updated list of valid SD-WAN Manager UUIDs to Cisco SD-WAN Validator immediately because the previously active SD-WAN Manager is the CA for the cloud WAN edge devices. So, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator includes the UUIDs of the invalidated SD-WAN Manager nodes.

d. SD-WAN Manager has a scheduled task that runs every 24 hours and checks to see if all the cloud WAN edges have been moved to the active SD-WAN Manager. SD-WAN Manager sends the updated list of valid SD-WAN Manager UUIDs to Cisco SD-WAN Validator only after the cloud WAN edge devices have been moved to the active SD-WAN Manager. After this list is received, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator does not include the UUIDs of the invalidated SD-WAN Manager nodes.

What to do next

To verify SD-WAN Manager nodes, see Verify the valid SD-WAN Manager nodes.

Disaster recovery after a failed data center becomes operational

This procedure applies to a scenario in which an initially active SD-WAN Manager cluster or the data center hosting the cluster failed and the standby SD-WAN Manager cluster was configured to be the active SD-WAN Manager cluster. If the cluster that was initially active becomes operational again, it serves as a standby cluster. By completing the following procedure, you can turn this standby cluster into the active cluster.

Summary

If a Multitenant SD-WAN Manager cluster or the data center hosting the SD-WAN Manager nodes in the cluster fail, you can recover from the failure by activating a standby SD-WAN Manager cluster. You can perform disaster recovery as follows:

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active SD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

5. To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

What's next

- Back Up the Active Cisco SD-WAN Manager Cluster Configuration
- Restore Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

Replace faulty SD-WAN Controller

To replace a faulty SD-WAN Controller with a new instance, follow these steps:

Procedure

Step 1 Create a SD-WAN Controller instance. See Deploy the Cisco SD-WAN Controller.

Step 2 Add the Cisco SD-WAN Controller to the overlay network.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 4 Click **Controllers**.

Step 5 For the faulty SD-WAN Controller, click **...** and click **Invalidate**.

The **Invalidate** dialog box appears.

If you have not added a new SD-WAN Controller that can replace the faulty SD-WAN Controller, Cisco SD-WAN Manager indicates this through an error message. Click **Cancel** in the **Invalidate** dialog box and add a new SD-WAN Controller before invalidating the faulty instance.

Step 6 In the **Invalidate** dialog box, do the following:

a) Check the **Replace Controller** check box.
b) From the **Select Controller** drop-down list, choose the new SD-WAN Controller that should replace the faulty instance.
c) Click **Invalidate**.

Cisco SD-WAN Manager launches the Invalidate Device and Push CLI Tempalte Configuration task. When these tasks are completed, the faulty SD-WAN Controller is invalidated and removed from the overlay network.

The tenants that were served by the faulty SD-WAN Controller are now served by the new SD-WAN Controller that you chose as the replacement.