Troubleshooting TechNotes

First Published: 2023-08-01

Last Modified: 2023-08-10

CHAPTER 1

Recover Cisco Catalyst SD-WAN Manager

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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.

Information About Cisco SD-WAN Manager Recovery

This document is valid for Cisco SD-WAN Release 20.3.1 and later.

Cisco SD-WAN Manager recovery includes procedures for configuring and restoring a Cisco SD-WAN Manager instance or data center failure that occurs due to unforeseen circumstances.

The procedures in this document apply only to deployments with Cisco vEdge Cloud that are configured with **WAN Edge Cloud Certification Authorization** set to **Automated (vManage – signed)**.

Note   The term *Cisco SD-WAN Manager instance* refers either to a standalone Cisco SD-WAN Manager instance or a cluster of Cisco SD-WAN Manager instances.

Prerequisites for Cisco SD-WAN Manager Recovery

- Ensure that the number and configuration of the active Cisco SD-WAN Manager instances are identical to the number and configuration of the standby Cisco SD-WAN Manager instances.

- Ensure that all the active and standby Cisco SD-WAN Manager instances run the same software version.

- Ensure that all the active and standby Cisco SD-WAN Manager instances are able to reach the management IP address of the Cisco SD-WAN Validator.

- Ensure that all the active and standby Cisco SD-WAN Manager instances are able to connect to the WAN transport IP address of the Cisco SD-WAN Validator for disaster recovery with virtual routers.

- Ensure that certificates have been installed on the standby Cisco SD-WAN Manager instances.

- Ensure that you certify the standby Cisco SD-WAN Manager instances.

- Ensure that the clocks on all Cisco Catalyst SD-WAN devices, including the standby Cisco SD-WAN Manager instances, are synchronized.

Best Practices

- Do not interrupt any of the services that are running on a Cisco SD-WAN Manager node during the backup process.

Prepare for Cisco SD-WAN Manager Recovery

1. Deploy and configure the standby Cisco SD-WAN Manager instance.

   The standby Cisco SD-WAN Manager instance is inactive and does not participate in the overlay network.

2. Perform regular backups of the configuration database on the active Cisco SD-WAN Manager instance.

   If the active Cisco SD-WAN Manager instance fails, you can restore and activate the latest configuration database on the standby Cisco SD-WAN Manager instance. Ensure that you delete the previously active Cisco SD-WAN Manager instance in the overlay network.

Configure a Standby Cisco SD-WAN Manager Instance

1. Configure the standby Cisco SD-WAN Manager instance with its own running configuration and locally installed certificate.

The running configuration on the standby Cisco SD-WAN Manager instance is identical to that of the active Cisco SD-WAN Manager instance except for configurations such as the system IP address, tunnel interface IP address, and so on.

2. On the standby Cisco SD-WAN Manager instance, add the **shutdown** command to the transport interface configuration to place the transport interface in VPN 0 in shutdown mode.

With this configuration, the standby Cisco SD-WAN Manager instance is not visible to the Cisco Catalyst SD-WAN network.

Verify the Configuration of a Standby Cisco SD-WAN Manager Instance After the Data Center Becomes Operational

1. Ensure that the standby Cisco SD-WAN Manager instance has its own running configuration and locally installed certificate.

   The running configuration on standby is identical to that of the active Cisco SD-WAN Manager instance except for configurations such as the system IP address, tunnel interface IP address, and so on.

2. On the standby Cisco SD-WAN Manager instance, add the **shutdown** command to the transport interface configuration to place the transport interface in VPN 0 in shutdown mode.

With this configuration, the standby Cisco SD-WAN Manager instance is not visible to the Cisco Catalyst SD-WAN network.

Back Up the Active Cisco SD-WAN Manager

On a regular basis, make backup snapshots (full, not incremental) of the active Cisco SD-WAN Manager configuration database. Additionally, make virtual machine snapshots of active Cisco SD-WAN Manager virtual machines.

To backup the active Cisco SD-WAN Manager instance, follow these steps:

1. Enter the following command to generate a backup of the configuration database of the active Cisco SD-WAN Manager instance:

   device# **request nms configuration-db backup path** *path*.

   This command backs up the database to a `.tar.gz` file that is located at *path*. In the following example, 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
   ```

2. Copy the generated configuration database to an external server.

Restore a Cisco SD-WAN Manager Instance from Backup

If the active Cisco SD-WAN Manager instance, or the data center hosting it, becomes unavailable, restore the most recent copy of the configuration database to the standby Cisco SD-WAN Manager instance.

The restore operation does not restore all information that is included in the database, such as users and the repository. All running configurations of Cisco SD-WAN Manager instances, such as users and repositories, must be manually configured again after the restore procedure completes.

Note This restore procedure is irreversible and the previously active Cisco SD-WAN Manager instances cannot be reused without further steps that are beyond the scope of this document.

To restore a Cisco SD-WAN Manager instance from a backup, follow these steps:

1. Enter the following command to restore the configuration database from the active Cisco SD-WAN Manager instance:

   device# **request nms configuration-db restore path**.

   This command restores the configuration database from the file located at *path*.

2. Enter the following command on the standby Cisco SD-WAN Manager instance to verify that all services are running on the standby Cisco SD-WAN Manager instance:

   device# **request nms all status**

3. On the standby Cisco SD-WAN Manager instance, choose **Configuration** > **Devices** > **Controllers** and verify that the page displays all active and standby Cisco SD-WAN Manager instances.

4. On the Cisco SD-WAN Validator, from the CLI, use the **show orchestrator valid-vmanage-id** command. This displays the chassis number of the active Cisco SD-WAN Manager instance.

5. On a vEdge Cloud router, from the CLI, use the **show control valid-vmanage-id** command. This displays the chassis number of the active Cisco SD-WAN Manager instance.

6. Add the **no shutdown** command to the configuration to bring up the transport interface on the standby Cisco SD-WAN Manager instance:

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

7. Add the standby Cisco SD-WAN Controllers to the overlay network:

   a. Log in to the standby Cisco SD-WAN Manager instance.

   b. From Cisco SD-WAN Manager menu, click **Configuration** > **Devices**.

   c. Click the **Controllers** tab.

   d. In the table of controllers, click **...** adjacent to the Cisco SD-WAN Controller instance and click **Edit**.

   e. In the **Edit** window, enter the Cisco SD-WAN Controller WAN transport IP address, the username **admin**, and the password of this **admin** user, and then click **Save**.

   f. Repeat the steps a through e for all the Cisco SD-WAN Controllers in the network.

8. Add the standby Cisco SD-WAN Manager instance to the overlay network:

   a. Log in to the standby Cisco SD-WAN Manager instance.

    b. From the Cisco SD-WAN Manager menu, click **Configuration** > **Devices** .

    c. Click the **Controllers** tab.

    d. In the table of controllers, click **...** adjacent to the Cisco SD-WAN Validator and click **Edit**..

    e. In the **Edit** window, enter the Cisco SD-WAN Validator's WAN transport IP address, the username **admin**, and the password of this **admin** user, and then click **Save**.

    f. Repeat the steps a through e for all the Cisco SD-WAN Validators in the network.

9. Disconnect the active Cisco SD-WAN Manager instance from the overlay network by using one of these two methods.

Perform this step in a lab environment, where you are simulating a disaster scenario. However, if you cannot reach the Cisco SD-WAN Manager instances, as in an actual disaster scenario, you may not be able make this configuration change.

- Add the **shutdown** command to the configuration to shut down the transport interface in VPN 0:

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

- Enter the **no tunnel-interface configuration** command to deactivate the tunnel interface in VPN 0:

```
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
```

10. On any Cisco SD-WAN Manager server in the newly active cluster, perform the following actions:

    a. Enter the following command to synchronize the root certificate with all Cisco Catalyst SD-WAN devices in the newly active cluster:

```
Standby-vManage#
https://newly_active_vManage_IP_address/dataservice/system/device/sync/rootcertchain
```

    b. Enter the following command to synchronize the Cisco SD-WAN Manager UUID with the Cisco SD-WAN Validator:

```
Standby-vManage# https://newly_active
_vManage_IP_address/dataservice/certificate/syncvbond
```

11. From the newly active Cisco SD-WAN Manager instance, send the updated device list to the Cisco SD-WAN Validator:

    a. From the Cisco SD-WAN Manager menu, click **Configuration** > **Certificates** .

    b. Click the **Controllers** tab.

    c. Click **Send to vBond**.

    d. Wait for the task to complete.

        The following messages appear after the task is complete:

        - Failure message for the previously active Cisco SD-WAN Manager instances.

- Success message for the newly active Cisco SD-WAN Manager instances and the Cisco SD-WAN Validators.

   Wait for the control to be fully established before proceeding. After control is established:

   - The Cisco SD-WAN Manager instances are up to date with the most recent database backup.

   - Each instance begins to establish control connections with the other instances in the network. The previously active Cisco SD-WAN Manager instances are not part of the overlay network anymore.

   e. On the Cisco SD-WAN Validator, open the CLI and run the **show orchestrator valid-manage-id** command. This displays the chassis number of both the active and the standby Cisco SD-WAN Manager instances.

   f. From the Cisco SD-WAN Manager menu, click **Configuration** > **Certificates**.

   g. Click the **vEdge List** tab.

   h. Click **Send to Controllers**.

12. On a newly active Cisco SD-WAN Manager server, from the CLI, use the **show control valid-vedges** command. The output displays the chassis number and serial numbers of Cisco vEdge devices.

13. Verify that the following items appear as expected:

   - Templates

   - Policies

   - Device page (both tabs) **WAN vEdge List** and **Controllers**

14. Perform these actions to verify the valid Cisco SD-WAN Manager instances:

   a. Log in to each Cisco SD-WAN Validator and enter the following command:

   show orchestrator valid-manage-id

   b. Verify that the output lists the chassis number of all the Cisco SD-WAN Manager instances for the previously active and the newly active systems.

   c. Log in to a Cisco vEdge device and enter the following command:

   show control valid-manage-id

   d. Verify that the output lists the chassis number of all the Cisco SD-WAN Manager instances for the previously active and the newly active systems.

   e. Verify that control is up with the newly active Cisco SD-WAN Manager instances and with the Cisco SD-WAN Controllers.

The standby Cisco SD-WAN Manager instance is now the active Cisco SD-WAN Manager instance.

Restore a Cisco SD-WAN Manager from Backup After the Data Center Becomes Operational

If the active Cisco SD-WAN Manager instance, or the data center hosting it, becomes unavailable, restore the most recent copy of the configuration database to the standby Cisco SD-WAN Manager instance.

The restore operation does not restore all information included in the database, such as users and the repository. All running configurations in Cisco SD-WAN Manager instances, such as users and repositories, must be manually configured again after the restore procedure completes.

✎

Note This restored procedure is irreversible and the previously active Cisco SD-WAN Manager instances cannot be reused without further steps that are beyond the scope of this document.

1. Copy the saved configuration database backup that was taken from the active Cisco SD-WAN Manager instance to /home/admin/db_backup.tar.gz on the standby Cisco SD-WAN Manager instance.

2. Enter the following command to restore the configuration database:

   device# **request nms configuration-db restore /home/admin/db_backup.tar.gz**

3. Enter the following command to verify that all services are running on the standby Cisco SD-WAN Manager instance:

   device# **request nms all status**

4. On the standby Cisco SD-WAN Manager instance, choose **Configuration** > **Devices** > **Controllers** and verify that the page displays all active and standby Cisco SD-WAN Manager instances.

5. Add the standby Cisco SD-WAN Manager instance to the overlay network:

   a. Log in to the standby Cisco SD-WAN Manager instance.

   b. From the Cisco SD-WAN Manager menu, click **Configuration** > **Devices** .

   c. Click the **Controllers** tab.

   d. In the table of controllers, click **...** adjacent to the Cisco SD-WAN Controller instance and click **Edit**.

   e. In the **Edit** window, enter the Cisco SD-WAN Validator's management IP address, username and password, and then click **Save**.

   f. Repeat substeps d through e for all Cisco SD-WAN Validators in the network.

6. If any Cisco SD-WAN Manager instances are still accessible, disconnect the instances from the overlay network.

7. Enter the following commands to bring up the transport interface on the standby Cisco SD-WAN Manager instances:

   • Add the **no shutdown** command to the configuration:

   ```
   Standby-vManage# config
   Standby-vManage(config)# vpn 0 interface interface-name
   ```

```
Standby-vManage(config)# no shutdown
Standby-vManage(config-interface)# commit and-quit
```

- Add the **tunnel-interface** command to the configuration:

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

8. From the standby Cisco SD-WAN Manager instance, send the updated device list to the Cisco SD-WAN Validator:

   a. From the Cisco SD-WAN Manager menu, click **Configuration** > **Certificates**.

   b. Click the **Controllers** tab.

   c. Click **Send to vBond**.

   d. Wait for the task to complete.

      The following messages appear after the task is complete:

      - Failure message for the previously active Cisco SD-WAN Manager instances.

      - Success message for the standby Cisco SD-WAN Manager instances and the Cisco SD-WAN Validators.

      Wait for the control to be fully established before proceeding. After control is established:

      - The standby Cisco SD-WAN Manager instance becomes the active Cisco SD-WAN Manager instance.

      - The Cisco SD-WAN Manager instances are up to date with the most recent database backup.

      - Each instance begins to establish control connections with the other instances in the network. The previously active Cisco SD-WAN Manager instances are not part of the overlay network anymore.

   e. From the Cisco SD-WAN Manager menu, click **Configuration** > **Certificates**.

   f. Click the **vEdge List** tab.

   g. Click **Send to Controllers**.

9. Verify that the items appear as expected:

   - Templates

   - Policies

   - Device page (both tabs) **WAN vEdge List** and **Controllers**

10. Verify the valid Cisco SD-WAN Manager instances:

   a. Log in to each Cisco SD-WAN Validator and enter the following command:

      device# **show orchestrator valid-vmanage-id**

b. Verify that the output lists the chassis number of all the Cisco SD-WAN Manager instances for the previously active and the newly active systems.

c. Log in to a Cisco vEdge device and enter the following command:

From the CLI, run the command **show control valid-vmanage-id**.

d. Verify that the output lists the chassis number of all the Cisco SD-WAN Manager instances for the previously active and the newly active systems.

e. Verify that the control is up with the newly active Cisco SD-WAN Manager instances and with the Cisco SD-WAN Controllers.

The standby Cisco SD-WAN Manager instance is now the active Cisco SD-WAN Manager instance.