Cluster Management

Table 1: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Persona-based Cluster Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	Simplifies adding Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

- Information About Cluster Management, on page 1
- Manage the configuration database backup for a Cisco SD-WAN Manager cluster using the CLI, on page 2
- Guidelines for a Cisco Catalyst SD-WAN Manager Cluster, on page 4
- View Available Cluster Services, on page 5
- Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 5
- Add a Cisco Catalyst SD-WAN Manager Server to a Cluster, on page 7
- View Cisco Catalyst SD-WAN Manager Service Details, on page 9
- Edit Cisco Catalyst SD-WAN Manager Parameters, on page 10
- Update Configuration Database Login, on page 11
- Downgrade Cisco Catalyst SD-WAN Manager, on page 12
- Upgrade a Cisco SD-WAN Manager Cluster, on page 12
- Manually Restart Cisco Catalyst SD-WAN Manager Processes, on page 16
- Remove Cisco Catalyst SD-WAN Manager Nodes from a Cluster, on page 18

Information About Cluster Management

A Cisco SD-WAN Manager cluster consists of at least three Cisco SD-WAN Manager servers. These servers manage the Cisco Catalyst SD-WAN edge devices in a network. Cisco SD-WAN Manager servers in a cluster perform specific functions based on the services that are running on them. In this way, a cluster distributes the workload among Cisco SD-WAN Manager servers while sharing information between these servers. For scaling recommendations, see *Server Recommendations* for your release in Cisco Catalyst SD-WAN Controller Compatibility Matrix and Server Recommendations.

Use the **Administration** > **Cluster Management** window to create a Cisco SD-WAN Manager cluster and perform related tasks.

From Cisco vManage Release 20.6.1, each Cisco SD-WAN Manager server has a *persona*. The persona is determined when the Cisco SD-WAN Manager server first boots up after Cisco SD-WAN Manager is installed and defines which services run on the server. The persona of a server lasts for the lifetime of the server and cannot be changed. A server must have a persona before it can be added to a cluster. For more information on personas, see Cisco Catalyst SD-WAN Manager Persona and Storage Device.

The role that a server has in a cluster depends on its persona. A Cisco SD-WAN Manager server can have any of the following personas:

- Compute+Data: Includes all services that are required for Cisco SD-WAN Manager, including services that are used for the application, statistics, configuration, messaging, and coordination
- Compute: Includes services that are used for the application, configuration, messaging, and coordination
- Data: Includes services that are used for the application and statistics

Encryption

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, cluster traffic for all services is encrypted.

Reserved IP Addresses

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, a WAN edge device or Cisco SD-WAN Control Components in a Cisco SD-WAN Manager cluster reserve IP addresses with the 172.30.0.0/16 prefix. These reserved IP addresses cannot be used as a system IP address by a WAN edge device or Cisco SD-WAN Control Components. If the reserved IP address is already in use by a WAN edge device or Cisco SD-WAN Control Components, open a TAC case to replace the IP addresses.

Manage the configuration database backup for a Cisco SD-WAN Manager cluster using the CLI

From Cisco Catalyst SD-WAN Control Components Release 20.18.1, you can use CLI commands to manage configuration database backups. These commands allow you to capture a config-db backup, list available backups, download backups, restore backups and add metadata to the config-db backup file.

Procedure

Step 1 Capture a configuration database backup in the online mode.

a) Use this command to generate a config-db backup on demand:

```
request nms configuration-db backup path VM12_Leader_Online
```

The following example demonstrates how to back up the configuration database in the online mode.

```
Device:~# confd_cli
Welcome to Viptela CLI
User root last logged in 2024-05-10T21:11:20.924041+00:00, to vm12, from 127.0.0.1 using cli-console
root connected from 127.0.0.1 using console on vm12
vm12# request nms configuration-db backup path VM12_Leader_Online
```

```
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/VM12_Leader_Online.tar.gz
sha256sum: 5c1b0db8518b29c99af856eca0e47f42b262ade13520fbebec7bb9224cebace6
Removing the temp staging dir :/opt/data/backup/staging
Device#
```

Step 2 Capture a configuration database backup in the offline mode.

a) Use the following command to access the internal network namespace:

```
tools internal ip_netns options "exec default bash"
```

b) Dump the configuration database:

Use the following command to dump the configuration database to a .tar.gz file:

```
configuration_db_cmd configuration_db_dump /opt/data/backup/VM12_Leader_Offline.tar.gz
```

This command will create a compressed archive of the database in the specified directory.

The following example demonstrates how to back up the configuration database in the offline mode.

```
vm12# request nms configuration-db stop
Successfully stopped NMS configuration database
vm12# tools internal ip_netns options "exec default bash"
vm12:~# configuration_db_cmd configuration_db_dump /opt/data/backup/VM12_Leader_Offline.tar.gz
Configuration-db dump to /backup/VM12_Leader_Offline.tar.gz
```

Step 3 **View Metadata Information During Restore**

a) Extract the Contents of the Backup File:

Use the following command to extract the contents of the `.tar.gz` file:

```
tar -zxf VM12_Leader_Offline.tar.gz
```

b) View the Metadata Information:

View the contents of the `neo4j_backup_info.json` file:

```
vi neo4j_backup_info.json
```

Note

- The `neo4j_backup_info.json` file contains critical information (metadata) about the backup. Review this information carefully before proceeding with the restore process.

  The metadata includes details such as the backup ID, start time, end time, database version, and system information.

Example

Note The system prompts for confirmation before proceeding with the restore if the backup is older than 24 hours.

Guidelines for a Cisco Catalyst SD-WAN Manager Cluster

The following guidelines apply to a Cisco SD-WAN Manager cluster:

- We recommend that all members of a Cisco SD-WAN Manager cluster be located in the same data center.
- We recommend that the IP addresses of all members of the Cisco SD-WAN Manager cluster be in the same subnet.

Note

- In a multi-node Cisco SD-WAN Manager cluster, the SD-WAN Manager system-ip is the system IP designated by the SD-WAN Manager cluster itself, which may differ from the individual device's system IP.
- The device system-ip is the unique identifier for each device, while the SD-WAN Manager system-ip represents the cluster node managing the control connections.

- We recommend that Cisco SD-WAN Manager cluster interface should not be the same as transport interface. Beginning with Cisco vManage Release 20.9.1, this is enforced. If you attempt to configure this, Cisco SD-WAN Manager displays an error message.
- The cluster interface should not be accessible externally.
- Access to Cisco SD-WAN Manager cluster IP addresses is restricted to Cisco SD-WAN Manager instances in the same cluster.
- The members of a Cisco SD-WAN Manager cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, if you need to change the clock time of a Cisco SD-WAN Manager server in a cluster, make the same change on every Cisco SD-WAN Manager server in the cluster.
- In a three node cluster deployment, only one node can have a systematic failure. When one node fails, the Cisco SD-WAN Manager Graphical User Interface (GUI) of two remaining nodes are reachable and can communicate with remaining nodes through SSH. If two nodes fail, the GUI of an active node on which a user is already logged in allows read-only operations, but new logins to the GUI are not permitted.
- When the guest node has factory default credentials configured on it and a host node tries to add it to the cluster, the cluster management fails. You must modify the password on new node same as that of the other nodes in the cluster.
- When logged in using a single sign-on (SSO) user with netadmin privilege, user cannot perform any of the cluster or disaster recovery operations using the SSO user. For any cluster operations like add, delete node, or enable SD-AVC, Cisco SD-WAN Manager expects any local username and password part of the net-admin group. In case of multitenancy, only admin user can update the SD-AVC. Other users even with netadmin privileges cannot update SD-AVC.
- On devices without dedicated mgmt-intf, VPN 512 gets mapped to custom VRF 512, instead of VRF mgmt-intf. In the back end, this VRF is not mapped to same namespace as other platforms. You cannot download the image as there is a platform difference.

View Available Cluster Services

To view the services that are available in and reachable on all the members in a Cisco SD-WAN Manager cluster, choose **Administration** > **Cluster Management** > **Service Reachability**.

Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server

When you start Cisco SD-WAN Manager for the first time, the default IP address of the Cisco SD-WAN Manager server is shown as localhost. Before you can add a new Cisco SD-WAN Manager server to a cluster, you must change the localhost address of the primary Cisco SD-WAN Manager server to an out-of-band IP address. (From Cisco vManage Release 20.6.1, the primary Cisco SD-WAN Manager server has the Compute+Data persona.) Servers in the cluster use this out-of-band IP address to communicate with each other.

If you need to change the out-of-band IP address in the future, contact your Cisco support representative.

Cluster interconnection between Cisco SD-WAN Manager servers requires that each of the servers be assigned a static IP address. We recommend that you do not use DHCP to assign IP addresses to Cisco SD-WAN Manager servers that are to be a part of a cluster. Configure the IP address on a nontunnel interface in VPN 0.

Before you configure the cluster IP address of a Cisco SD-WAN Manager server, ensure that out-of-band IP addresses have been configured on VPN0 for its server interfaces. This configuration typically is done when the server is provisioned. The port type for an out-of-band IP address must be **service** for the IP address to be available for assigning to a Cisco SD-WAN Manager server.

Note From Cisco vManage Release 20.11.1, some alarms display the hostname as **localhost** during the cluster setup for the first time as the system-ip/hostname is not configured in Cisco SD-WAN Manager. When the system-ip/hostname is configured, the alarms display the correct hostname.

Configure the IP Address for Releases Before Cisco vManage Release 20.6.1

Configure the IP address of a Cisco SD-WAN Manager server before you add the server to the cluster. To do so for releases before Cisco vManage Release 20.6.1, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add vManage**.

   The **Edit vManage** dialog box opens.
3. From the **vManage IP Address** drop-down list, choose an IP address to assign to the Cisco SD-WAN Manager server.
4. Enter the user name and password for logging in to the Cisco SD-WAN Manager server.
5. Click **Update**.

The Cisco SD-WAN Manager server reboots and displays the **Cluster Management** window.

Configure the IP Address for Cisco vManage Release 20.6.1 and Later Releases

Configure the IP address of a Cisco SD-WAN Manager server before you add the server to the cluster. To do so from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on the primary Cisco SD-WAN Manager server (which has the Compute+Data persona).

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management** window is displayed. The table on this window lists the Cisco SD-WAN Manager servers that are in the cluster.

2. Click **...** adjacent to the Cisco SD-WAN Manager server to configure and click **Edit**.

   The **Edit vManage** dialog box is displayed.

3. In the **Edit vManage** dialog box, perform the following actions.

Note You cannot change the persona of a server. So the Node Persona options are disabled.

   a. From the **vManage IP Address** drop-down list, choose an out-of-band static IP address to assign to the server.

   b. In the **Username** field, enter the user name for logging in to the server.

   c. In the **Password** field, enter the password for logging in to the server.

   d. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

      Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on only one Cisco SD-WAN Manager server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

Note If Cisco SD-WAN Manager is set up as a cluster and the cluster crashes as a result of a reboot or upgrade, the connection to the edge device is reset and the custom app ceases to function.

To resolve this and to resume operation, redefine the custom application name with a new, unique name. For more information to define custom applications, see the Define Custom Applications Using Cisco Catalyst SD-WAN Manager chapter of the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

   e. Click **Update**.

      The server reboots and displays the **Cluster Management** window.

Add a Cisco Catalyst SD-WAN Manager Server to a Cluster

Table 2: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Persona-based Cluster Configuration	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	Simplifies adding Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

The following sections provide information about adding a Cisco SD-WAN Manager server to a cluster in various Cisco SD-WAN Manager releases.

Add a Cisco SD-WAN Manager Server to a Cluster for Releases Before Cisco vManage Release 20.6.1

To add a new Cisco SD-WAN Manager server to a cluster for releases before Cisco vManage Release 20.6.1, perform the following steps on the primary Cisco SD-WAN Manager server.

Before you begin, ensure that the default IP address of the Cisco SD-WAN Manager server has been changed to an out-of-band IP address as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 5.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add Manager**.

   The **Edit Manager** window opens.
3. In the **Manager IP Address** field, select an IP address to assign to the Cisco SD-WAN Manager server.
4. Enter the username and password for logging in to the Cisco SD-WAN Manager server.
5. Enter the IP address of the Cisco SD-WAN Manager server that you are adding to the cluster.
6. Specify the username and password for the new Cisco SD-WAN Manager server.
7. Select the services to be run on the Cisco SD-WAN Manager server. You can select from the services listed below. Note that the **Application Server** field is not editable. The Cisco SD-WAN Manager Application Server is the local Cisco SD-WAN Manager HTTP web server.
   - Statistics Database: Stores statistics from all the Cisco Catalyst SD-WAN devices in the network.
   - Configuration Database: Stores all the device and feature templates and configurations for all the Cisco Catalyst SD-WAN devices in the network.
   - Messaging Server: Distributes messages and shares state among all the Cisco SD-WAN Manager cluster members.
8. Click **Add**.

   The Cisco SD-WAN Manager server that you just added reboots before joining the cluster.

Note

- In a cluster, we recommend that you run at least three instances of each service.
- When you add the first two compute or compute+data nodes to the cluster, the host node's application-server is unavailable. The following message is displayed on the host node's GUI, before the application-server shuts down in the host node: `\Node added to the cluster. The operation may take up to 30 minutes and may cause application-server to restart in between. Once the application server is back online, the post cluster operation progress can be viewed under tasks pop-up\.`
- Starting Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, ensure that you disable the **HTTP/HTTPs Proxy** option in the Cisco SD-WAN Manager settings, before adding a node to the cluster.

Add a Cisco SD-WAN Manager Server to a Cluster for Cisco vManage Release 20.6.1 and Later Releases

From Cisco vManage Release 20.6.1, a cluster supports any of the following deployments of nodes:

- Three Compute+Data nodes
- Three Compute+Data nodes and three Data nodes

Note DATA nodes should be added only after 3 node cluster with CONFIG+DATA is added.

- Three Compute nodes and three Data nodes (supported only in an upgrade from an existing deployment)

If you require a different combination of nodes, contact your Cisco representative.

To add a Cisco SD-WAN Manager server to a cluster from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on a Compute+Data node or a Compute node. Performing this procedure on a Data node is not supported because a Data node does not run all the services that are required for the addition.

Do not add a server that was a member of the cluster and then removed from the cluster. If you need to add that server to the cluster, bring up a new VM on that server to be used as the node to add.

Before you begin, ensure that the default IP address of the Cisco SD-WAN Manager server has been changed to an out-of-band IP address, as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 5. This operation must happen only once on the Cisco SD-WAN Manager server and then the same is used to add other servers to form a cluster.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management page** window appears. The table on this window shows the Cisco SD-WAN Manager servers that are in the cluster.

2. Click **Add Manager**.

   The **Add Manager** dialog box opens.

Note If the **Edit Manager** dialog box opens, configure an out-of-band IP address for the server, as described in Configure the Cluster IP Address of a Cisco Catalyst SD-WAN Manager Server, on page 5, and then repeat this procedure for adding a server.

3. In the **Add Manager** dialog box, perform the following actions:
   a. Click the **Node Persona** option (**Compute+Data**, **Compute**, or **Data**) that corresponds to the persona that has been configured for the server.

      You can determine the persona of a server by logging in to the server and looking at the persona display on the **Administration** > **Cluster Management** window. If you choose an incorrect persona, a message displays the persona that you should choose.

   b. From the **Manager IP Address** drop-down list, choose the IP address of the server to be added to the cluster.

   c. In the **Username** field, enter the user name for logging in to the server.

   d. In the **Password** field, enter the password for logging in to the server.

   e. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

      Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on one Cisco SD-WAN Manager server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

      If you enabled Cisco SD-AVC for this server when you changed its IP address, the **Enable SD-AVC** check box is checked by default.

   f. Click **Add**.

   g. To confirm, click **OK**.

      The dialog box indicates that the services will restart, and that the existing metadata and other information that is not required when the server joins the cluster will be deleted from the server.

      When you click **OK**, the system starts the server add operation. The **Cluster Management** window displays the tasks that the system performs as it adds the server.

      As part of this operation, the system checks the compatibility of the server that you are adding. This check ensures that the server has sufficient disk space, and that the persona that you specified matches the persona of the node.

      After the server is added, the system performs a cluster sync operation, which rebalances the services in the cluster. Then the Cisco SD-WAN Manager servers in the cluster restart.

View Cisco Catalyst SD-WAN Manager Service Details

The following sections describe how to view detailed information about services that are running on a Cisco SD-WAN Manager server and how to view devices that are connected to Cisco SD-WAN Manager.

View Detailed Information about Services

To view detailed information about the services running on a Cisco SD-WAN Manager server:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click the hostname of the Cisco SD-WAN Manager server.

   The **vManage Details** window opens, displaying the process IDs of all the Cisco SD-WAN Manager services that are enabled on Cisco SD-WAN Manager.
3. Click **Cluster Management** in the breadcrumb in the title bar to return to the **Cluster Management** window.

View Devices Connected to Cisco SD-WAN Manager

To view the list of devices connected to Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click the hostname of the Cisco SD-WAN Manager server.
3. Click **Managed Devices**.

Alternatively:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **...** adjacent to the Cisco SD-WAN Manager server and choose **Device Connected**.
3. If a device is connected to Cisco SD-WAN Manager from a cluster, ensure that you do not configure the data stream hostname to the Cisco SD-WAN Manager system IP address. However, you can configure the management IP address on VPN 512 or the internet public IP address on VPN 0. For information about data stream troubleshooting tools, see Data Stream Troubleshooting Tools FAQ.

Edit Cisco Catalyst SD-WAN Manager Parameters

You can edit various parameters for a Cisco SD-WAN Manager server that has been added to a cluster. To do so, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **...** adjacent to the Cisco SD-WAN Manager server to edit, and click **Edit**.

   The **Edit vManage** window opens.
3. Select an IP address to edit.
4. Enter the username and password, and edit parameters for the selected Cisco SD-WAN Manager server.
   - For releases before Cisco vManage Release 20.6.1, you can edit the cluster services.

- From Cisco vManage Release 20.6.1, you can change the IP address to another IP address that appears in the **vManage IP Address** drop-down list, change the Cisco SD-AVC setting, or change the username and password if the server credentials have changed.

5. Click **Update**.

Update Configuration Database Login

The default username of the configuration database is **neo4j** and the default password is **password**. To update the default login credentials of the configuration database, access Cisco SD-WAN Manager using a terminal and run the following commands. Do not use the SSH terminal option in Cisco SD-WAN Manager to run these commands. Doing so causes you to lose access to Cisco SD-WAN Manager.

1. Use **request nms application-server stop** to stop application servers on all the Cisco SD-WAN Manager servers whether configuration-db is enabled or not.

   .

2. Use one of the following commands to reset the user name and password for the configuration database on all the Cisco SD-WAN Manager servers:

   - For Cisco SD-WAN Release 20.1.1 and earlier:

     request nms configuration-db update-admin-user username *username* **password** *password* **newusername** *newadminuser* **newpassword** *newpassword*

   - For releases from Cisco SD-WAN Release 20.1.2:

     request nms configuration-db update-admin-user

     When prompted, enter your current username and password, and your new username and password.

     When you run one of these commands, Cisco SD-WAN Manager restarts the application server

Note

- If you do not know the default credentials of the configuration database, contact your Cisco support representative to retrieve the credentials.
- You cannot use a previous username.
- Passwords can include only a mix of characters A to Z (upper or lowercase), digits 0 to 9, and special characters @, #, and *.

Example

- For Cisco SD-WAN Release 20.1.1 and earlier:

```
request nms configuration-db update-admin-user username neo4j
password ******** newusername myusername newpassword mypassword
```

- For releases from Cisco SD-WAN Release 20.1.2:

```
request nms configuration-db update-admin-user

Enter current user name: neo4j
```

```
Enter current user password: password
Enter new user name: myusername
Enter new user password: mypassword
```

Note After a configuration database admin user update, if you are unable to view a specific Cisco SD-WAN Manager instance, use the **request nms application-server restart** command to restart the application server on that Cisco SD-WAN Manager instance again.

Note Starting from Cisco SD-WAN Release 20.6.1, when using the **request nms configuration-db update-admin-user** command to update the admin user credentials, provide the same inputs (old username, password and the new username, password) across all the nodes in the Cisco SD-WAN Manager cluster. You must execute the **request nms configuration-db update-admin-user** command one node at a time. We recommend that you do not push the CLI to all the nodes at the same time because the NMS services will restart for the new configuration to take effect.

Downgrade Cisco Catalyst SD-WAN Manager

You cannot downgrade Cisco SD-WAN Manager (install a version of Cisco SD-WAN Manager that is lower than the current version), either through Cisco SD-WAN Manager or by using CLI commands.

Note This restriction applies for single Cisco SD-WAN Manager instances and for Cisco SD-WAN Manager clusters. This restriction is not related to software upgrades or downgrades on network devices.

To downgrade your Cisco SD-WAN Manager version, contact your Cisco support representative.

Upgrade a Cisco SD-WAN Manager Cluster

Table 3: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Manager Cluster Upgrade	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature outlines the upgrade procedure for Cisco SD-WAN Manager servers in a cluster.

Feature Name	Release Information	Description
Check for Database Schema Violation	Cisco Catalyst SD-WAN Manager Release 20.13.1	Updated the **request nms application-server status** command to indicate whether there is a schema violation in the configuration database. You can check for violations before upgrading a cluster.
Cisco SD-WAN Manager Cluster Upgrade Compatibility Check	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature helps to upgrade a Cisco SD-WAN Manager cluster, performing a pre-upgrade software compatibility check and a post-upgrade check to ensure a successful upgrade. The feature helps to ensure a successful upgrade and helps to troubleshoot any problems in case of an unsuccessful upgrade.

Information About Cluster Upgrade

This section describes how to upgrade Cisco SD-WAN Manager in a cluster.

You can upgrade directly from Cisco vManage 20.3.1 or later releases to Cisco vManage Release 20.6.1. To upgrade from earlier releases, first upgrade to Cisco vManage 20.4.2 or Cisco vManage Release 20.5.1.

If you are upgrading a Cisco SD-WAN Manager cluster deployment from Cisco vManage Release 20.3.1 or later to Cisco vManage Release 20.5.1 or later, you must do it through the CLI.

If you are upgrading to Cisco vManage Release 20.6.1 or later releases from a six-node Cisco SD-WAN Manager cluster deployment in which not all services are running on all nodes, contact your Cisco support representative before performing the upgrade.

Starting with Cisco vManage Release 20.6.1, 6-node cluster deployments support only 3 Compute+Data nodes and 3 Data nodes. If your 6-node cluster is still configured with 3 Compute nodes and 3 Data nodes, **contact your Cisco support representative for assistance** in migrating it to 3 Compute+Data nodes and 3 Data nodes before performing any further upgrades.

Checking Software Compatibility Before Upgrade

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

In a cluster deployment, Cisco SD-WAN Manager services such as the configuration database, coordination service, and messaging services operate in a cluster mode.

We recommend using Cisco SD-WAN Manager to perform cluster upgrade, rather than CLI methods. Cisco SD-WAN Manager performs an important pre-upgrade check before proceeding with an upgrade. The pre-upgrade check includes items such as certificate expiration dates, the configuration database, CPU, disk, memory, and the status of services such as the coordination service and messaging service. If the cluster is not ready for upgrade, Cisco SD-WAN Manager notifies you.

After an upgrade, Cisco SD-WAN Manager performs a post-upgrade check, which includes checking the functionality of services to ensure a successful upgrade. If an upgrade fails, you can use Cisco SD-WAN Manager to troubleshoot and run the upgrade again.

While a cluster upgrade is in progress, at a given time, some nodes in the cluster continue to run an older software release while others have been upgraded to the newer release. Consequently, during the upgrade, there may be incompatibilities between services of the older and newer releases, preventing them from functioning properly.

For information about how to upgrade Cisco SD-WAN Manager clusters using Cisco SD-WAN Manager, see the Software Upgrade section in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide.*

Encryption

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1

For a multitenant cluster upgrade from Cisco Catalyst SD-WAN Manager Release 20.13.1 to Cisco Catalyst SD-WAN Manager Release 20.14.1 using Cisco SD-WAN Manager, the upgrade coordinator sometimes fails due to the encryption keys. The upgrade coordinator service uses the encryption keys to encrypt the service credentials.

To re-encrypt the service credentials, reboot the Cisco SD-WAN Manager and trigger the software activation.

Prerequisites for Cluster Upgrade

Before you upgrade Cisco SD-WAN Manager nodes to Cisco vManage Release 20.6.1 or later releases, verify the following:

- Ensure that the internal user account vmanage-admin is not locked for any server that you are upgrading.

  You can check the status of this admin account by pushing a template to the devices that are connected to the server. The push fails if the account is locked. In such a scenario, you can unlock the account by using the **request aaa unlock-user vmanage-admin** command.

- Ensure that PKI keys have been exchanged between the servers that you are upgrading.

  To do so, ensure that the control connections are in the UP state on the servers and restart the application server.

- Ensure that the out-of-band IP address of each server is reachable.
- Ensure that the Cisco SD-WAN Manager is accessible on all servers in the cluster.
- Ensure that DCA is running on all nodes in the cluster.

  To do so, use the **request nms data-collection-agent status** command and ensure that the status value shows **running** for each node.

  To start DCA, if needed, use the **request nms data-collection-agent start** command.

- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Use the **request nms application-server status** command to verify that there is no schema violation in the configuration database. If the command output indicates a violation, contact Cisco Customer Support to resolve the issue.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.12.3, the compute and data check is a prerequisite for disaster recovery (DR) replications to work. DR is not supported, if you run three compute nodes and three data nodes for DR replication.

If these prerequisites are not met or if another error occurs during the upgrade the activation of the image fails and a file named upgrade-context.json is created in the /opt/data/extra-packages/*image-version* folder on each node in the cluster. You can provide this file to your Cisco representative for assistance with resolving the issue.

Upgrade a Cluster Using CLI

1. Take snapshots of all the Cisco SD-WAN Manager servers. Take a backup of the configuration database and save it in a location outside of the Cisco SD-WAN Manager server using the following command:

   request nms configuration-db backup path *path_and_filename*
2. Ensure that Cisco vManage Release 18.3 or later is installed.
3. For upgrades from Cisco vManage Release 20.3.1 or later, copy the current image to each Cisco SD-WAN Manager server in the cluster and install the image on each Cisco SD-WAN Manager server by using the following command. Do not activate the image at this time.

   request software install *path*

Note The copy to Cisco SD-WAN Manager can be done using SCP using CLI using the VPN 512 interface.

4. For upgrades from Cisco vManage Release 20.3.1 or later, activate the current image on each Cisco SD-WAN Manager server using the following command. All servers reboot simultaneously.

   request software activate *version*
5. You must upgrade the configuration database when upgrading from one of the following:
   - Cisco vManage Release 18.4.x or 19.2.x to Cisco vManage 20.3.x or 20.4.x
   - Cisco vManage Release 20.3.x or 20.4.x to Cisco vManage Release 20.5.x or 20.6.x
   - Any Cisco SD-WAN Manager release to Cisco vManage Release 20.10.1 or later

Note
- Starting from Cisco vManage Release 20.1.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command:

  request nms *configuration-db diagnostics*
- When you upgrade the configuration database, ensure that you have activated the current image on each Cisco SD-WAN Manager server in the cluster as described in the previous step. In addition, ensure that all services except the application server and configuration-db services are running on these servers by entering the **request nms all status** command on each server.

To upgrade the configuration database, do the following:

a. To determine which node to upgrade, enter the **request nms configuration-db status** command on each node. In the output look for the following:

```
Enabled: true
Status: not running
```

Note After activating a new image on a Cisco SD-WAN Manager host server, the server reboots. After the reboot, for approximately 30 minutes, the output of the **request nms configuration-db status** command shows **Enabled: false** even on a node that has the configuration database enabled, while NMS services are being migrated to a containerized form.

b. On the node to upgrade, as determined in the previous step, enter the following:

request nms configuration-db upgrade

Note
- Enter this command on one node only.
- Do not enter this command if you are upgrading from Cisco vManage Release 20.5.x to Cisco vManage Release 20.6.1 or later.

6. Enter your login credentials, if prompted. Login credentials are prompted in releases earlier than Cisco vManage Release 20.3.1 if all the Cisco SD-WAN Manager servers establish control connection with each other. After a successful upgrade, all the configuration database services are UP across the cluster, and the application server is started.

You can check the database upgrade logs at the following location: *vmanage-server*:/var/log/nms/neo4j-upgrade.log.

Manually Restart Cisco Catalyst SD-WAN Manager Processes

If the cluster is malfunctioning and requires restart, you can manually restart the Cisco SD-WAN Manager processes. Do one of the following:

- (Cisco vManage Release 20.6.1 and later) Use the request nms all restart command to restart all processes.
- (Releases earlier than Cisco vManage Release 20.6.1) Restart the processes one at a time in an orderly manner using the procedure that follows. The manual restart order may vary for your cluster, depending on what services you are running on the Cisco SD-WAN Manager instances in the cluster. The following order is based on a basic cluster with three Cisco SD-WAN Manager devices.

Note It is not recommended to restart the NMS services immediately after the software upgrade. You must wait for at least 45 minutes. Beginning with Cisco vManage Release 20.9.1, you can check the status of the NMS service containers using the command **docker ps-a** in the root shell of Cisco SD-WAN Manager before restarting the NMS services. You can contact Cisco TAC for assistance.

1. On each Cisco SD-WAN Manager device, stop all the NMS services:

```
request nms all stop
```

2. Verify that all the services have stopped. It is normal for the **request nms all stop** command to display a message about failing to stop a service if it takes too long. So use the following command to verify that everything is stopped before proceeding further:

   ```
   request nms all status
   ```

3. Start the Statistics database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms statistics-db start
   ```

4. Verify that the service is started before proceeding to start it on the next Cisco SD-WAN Manager. After the service starts, perform step 3 to start the Statistics database on the next Cisco SD-WAN Manager device. After all the Cisco SD-WAN Manager devices have the Statistics database running, proceed to the next step.

   ```
   request nms statistics-db status
   ```

5. Start the Configuration database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms configuration-db start
   ```

6. For releases earlier than Cisco vManage Release 20.3.1, verify that the service has started before proceeding to start it on the next Cisco SD-WAN Manager device. Go to vshell and tail a log file to look for a message that the database is online. After confirming, go to step 5 to start the Configuration database on the next Cisco SD-WAN Manager device. After all the Cisco SD-WAN Manager devices have the Configuration database running, proceed to the next step.

   ```
   tail -f -n 100 /var/log/nms/vmanage-neo4j-out.log
   ```

7. Start the Coordination server on each device. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms coordination-server start
   ```

8. Verify that the service is started before proceeding to start it on the next Cisco SD-WAN Manager device. After verifying, go to step 7 to start the Coordination server on the next Cisco SD-WAN Manager device. After the Coordination server runs on all the Cisco SD-WAN Manager devices, proceed to the next step.

   ```
   request nms coordination-server status
   ```

9. Start the Messaging server on each device. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

   ```
   request nms messaging-server start
   ```

10. Verify that the service has started before proceeding to start the service on the next Cisco SD-WAN Manager device. After verifying, go to step 9 to start the Messaging server on the next Cisco SD-WAN Manager device. After the Messaging server runs on all the Cisco SD-WAN Manager devices, proceed to the next step.

    ```
    request nms messaging-server status
    ```

11. Start the Application server on each device. Wait for the service to start each time before proceeding to the next Cisco SD-WAN Manager device.

    ```
    request nms application-server start
    ```

12. For Cisco vManage Release 20.3.1 and later releases, start the server-proxy service on each Cisco SD-WAN Manager device:

```
request nms server-proxy start
```

To verify that the service is fully started, open the GUI of that Cisco SD-WAN Manager device. After the GUI is fully loaded and you are able to log in, start the server-proxy service on the next Cisco SD-WAN Manager device.

13. Restart the NMS cloud services on each device. Wait for the services to start each time before proceeding to the next Cisco SD-WAN Manager device.

    You can verify that the cloud services are running by entering the following commands:

    ```
    request nms cloud-agent status
    request nms cloud-agent-v2 status
    ```

    Verify that the service has started before proceeding to start it on the next Cisco SD-WAN Manager device. After verifying, start the cloud services on the next Cisco SD-WAN Manager device. After the cloud services run on all the Cisco SD-WAN Manager devices, continue to the next step.

14. To verify that there are no errors and everything has loaded cleanly, tail the log files.

If you experience issues when upgrading to Cisco vManage Release 20.6.1 or later, contact your Cisco support representative for assistance.

Note Consider bringing up the services manually as described in this section whenever you have to reboot a Cisco SD-WAN Manager device, or after an upgrade.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, a **device-data-collector** service container is added. The following is a sample output for the command, **`request nms device-data-collector`**.

```
Device# request nms device-data-collector
Possible completions:
  diagnostics   Run diagnostics on NMS component
  jcmd          Run jcmd on NMS component
  restart       Restart NMS component
  start         Start NMS component
  status        Status of NMS component
  stop          Stop NMS component
```

Remove Cisco Catalyst SD-WAN Manager Nodes from a Cluster

You can remove a Cisco SD-WAN Manager node from a cluster, if necessary.

In releases earlier than Cisco vManage Release 20.6.1, you can only remove *n* - 2 Cisco SD-WAN Manager nodes from a cluster of *n* nodes. You must retain at least two Cisco SD-WAN Manager nodes in a cluster.

From Cisco vManage Release 20.6.1, you must retain at least two Cisco SD-WAN Manager nodes that include the compute capability and at least one node that includes the data capability. That is, the cluster must retain any of the following:

- At least two Cisco SD-WAN Manager nodes that include the Compute+Data persona
- At least one Cisco SD-WAN Manager nodes that includes the Compute+Data persona and one Cisco SD-WAN Manager node that includes the Compute persona

- At least two Cisco SD-WAN Manager nodes that include the Compute persona and one Cisco SD-WAN Manager node that includes the Data persona

From Cisco vManage Release 20.6.1, if a Cisco SD-WAN Manager node is reachable when you remove it from a cluster, Cisco SD-WAN Manager automatically performs a factory reset operation on the removed node to ensure that the node does not join the cluster again. If a Cisco SD-WAN Manager node is unreachable when you remove it from a cluster, a factory reset operation is not performed on the node. In this situation, the node is added back to the cluster automatically when the node becomes reachable. To prevent the node from being added back to the cluster, enter the command **request software reset** from the CLI of the node after the node is removed from the cluster.

To remove a Cisco SD-WAN Manager node from a cluster, follow these steps:

1. From the Cisco SD-WAN Manager, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **…** adjacent to the Cisco SD-WAN Manager instance that you want to remove and click **Remove**.

   The **Remove Manager** dialog box opens.
3. Enter the username and password to confirm the removal of the device from the network.
4. Click **Remove**.

The Cisco SD-WAN Manager instance is removed from the cluster, the certificates for that Cisco SD-WAN Manager are deleted, and Cisco SD-WAN Manager undergoes a factory reset.