Revised: September 28, 2026

Cluster Management

Cluster Management

Feature History for Cluster Management

This table describes the developments of this feature, by release.

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 vManage Release 20.6.1 Cisco SD-WAN 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. You can add Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

Cluster Management

A SD-WAN Manager cluster is a group of at least three SD-WAN Manager servers that collectively manage Cisco Catalyst SD-WAN edge devices and distribute workloads.

- Consists of a minimum of three SD-WAN Manager servers.
- Distributes workload and shares information among servers.
- Each server in the cluster has a persona that determines its role and services.

Cluster Management Details and Server Personas

Cluster management involves creating and managing a SD-WAN Manager cluster, where each server is assigned a persona that defines its role and the services it runs.

- Compute+Data: Includes all services required for SD-WAN Manager, such as application, statistics, configuration, messaging, and coordination.
- Compute: Includes services for application, configuration, messaging, and coordination.
- Data: Includes services for application and statistics.

To create a cluster, use the **Administration** > **Cluster Management** window.

From Cisco vManage Release 20.6.1 , each SD-WAN Manager server has a *persona* determined at first boot after installation, which defines the services running on the server and cannot be changed.

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

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, a WAN edge device or SD-WAN Control Component in a SD-WAN Manager cluster reserves IP addresses with the 169.254.x.0/24 prefix. These reserved IP addresses cannot be used as a system IP address by a WAN edge device or SD-WAN Control Component. If the reserved IP address is already in use, open a TAC case to replace the IP addresses.

For scaling recommendations, see Cisco Catalyst SD-WAN Controller Compatibility Matrix and Server Recommendations .

For more information on personas, see Cisco Catalyst SD-WAN Manager Persona and Storage Device .

Restrictions for cluster management

Describes restrictions, limitations, and important notes concerning cluster management.

Cluster interface restrictions

- The cluster interface is exclusively for internal communication between SD-WAN Manager instances. Ensure that this interface remains inaccessible to the public. In case of a disaster recovery (DR) topology, the cluster interface can be accessed over the public network, but only through a specific route to connect the active and standby data centers.
- Cluster traffic must be directed to the cluster interface. Any cluster-related traffic received on other interfaces will be dropped. In such cases, the SD-WAN Manager cluster may become unhealthy and nonoperational.

Back Up the configuration database for a 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 online config-db backup and view config-db backup metadata.

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 <path_and_filename>
```

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

```
Device:~# 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
```

Step 2 (Optional) View Backup Metadata Information

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.

Guidelines for a SD-WAN Manager cluster

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

- Ensure that all members of a SD-WAN Manager cluster is located in the same data center.
- Ensure that the IP addresses of all members of the SD-WAN Manager cluster is in the same subnet.
  - In a multi-node 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.
- The members of a 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 SD-WAN Manager server in a cluster, make the same change on every 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 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 a new 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.
- In clustered environments, when the HTTP proxy is enabled or disabled, restart the application-server on the other nodes for them to pick up latest proxy configuration.

The following restrictions apply to SD-WAN Manager 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, 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.
- The cluster interface should not be accessible externally.
- Access to SD-WAN Manager cluster IP addresses is restricted to SD-WAN Manager instances in the same cluster.

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

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

Cluster interconnection between 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 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 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 SD-WAN Manager server.

Note

Some alarms might display the hostname as **localhost** during the cluster setup for the first time as the system-ip/hostname is not configured in SD-WAN Manager. When the system-ip/hostname is configured, the alarms display the correct hostname.

Before you begin

- When you start SD-WAN Manager for the first time, the default IP address of the SD-WAN Manager server is shown as localhost. Before you can add a new SD-WAN Manager server to a cluster, you must change the localhost address of the primary SD-WAN Manager server to an out-of-band IP address. Servers in the cluster use this out-of-band IP address to communicate with each other.
- Before you configure the cluster IP address of a 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 SD-WAN Manager server.

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

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

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

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

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

Step 3 In the **Edit Manager** dialog box, perform the following actions:

Note You cannot change the persona of a server. Therefore, 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) From SD-WAN Manager 20.18.1, to enable **Enable SD-AVC** navigate to **Administrator** > **Settings** > **SD-AVC** and toggle the **SD-AVC** button, 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 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.

e) Click **Add**.

f) 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 SD-WAN Manager servers in the cluster restart.

Add a SD-WAN Manager server to a cluster for Cisco SD-WAN Release 20.6.1 and later releases

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

From Cisco SD-WAN 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 must be added only after three node cluster with CONFIG+DATA is added.

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

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 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. 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.

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

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

Step 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, and then repeat this procedure for adding a server.

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

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 SD-WAN Manager servers in the cluster restart.

View service details on SD-WAN Manager

This section describes how to view detailed information about services that are running on a SD-WAN Manager server.

Follow these steps to view detailed information about the services running on a SD-WAN Manager server.

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

Step 2 Click the hostname of the SD-WAN Manager server.

The **vManage Details** window opens, displaying the process IDs of all the SD-WAN Manager services that are enabled on SD-WAN Manager.

Step 3 Click **Cluster Management** in the breadcrumb in the title bar to return to the **Cluster Management** window.

Viewing SD-WAN Manager service details

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

- View detailed information about services.
- View devices connected to SD-WAN Manager.

View service details on SD-WAN Manager

This section describes how to view detailed information about services that are running on a SD-WAN Manager server.

Follow these steps to view detailed information about the services running on a SD-WAN Manager server.

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

Step 2 Click the hostname of the SD-WAN Manager server.

The **vManage Details** window opens, displaying the process IDs of all the SD-WAN Manager services that are enabled on SD-WAN Manager.

Step 3 Click **Cluster Management** in the breadcrumb in the title bar to return to the **Cluster Management** window.

View list of devices connected to SD-WAN Manager

This section describes how to view devices that are connected to SD-WAN Manager.

Follow these steps to view the list of devices connected to SD-WAN Manager.

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

Step 2 Click the hostname of the SD-WAN Manager server.

Step 3 Click **Managed Devices**.

Step 4 Alternatively, follow these steps.

a) From the SD-WAN Manager menu, choose **Administration** > **Cluster Management** and click **Service Configuration** .

b) Click **...** adjacent to the SD-WAN Manager server and choose **Device Connected** .

c) If a device is connected to SD-WAN Manager from a cluster, ensure that you do not configure the data stream hostname to the 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 SD-WAN Manager Parameters

You can edit various parameters for a SD-WAN Manager server that has been added to a cluster.

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

Step 2 Click **...** adjacent to the SD-WAN Manager server to edit, and click **Edit** .

The **Edit Manager** window opens.

Step 3 Select an IP address to edit.

Step 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 **Manager IP Address** drop-down list, change the Cisco SD-AVC setting, or change the username and password if the server credentials have changed.

Step 5 Click **Update** .

Update the configuration database login credentials

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 SD-WAN Manager using a terminal and run the following commands. Do not use the SSH terminal option in SD-WAN Manager to run these commands. Doing so causes you to lose access to SD-WAN Manager .

Note

When connecting to the SD-WAN Manager through SSH, use the same URL that you use to access the SD-WAN Manager's web interface. Do not use the local IP address listed under **Configuration** > **Devices** to ensure a secure and successful connection.

Reset the user name and password for the configuration database on all the Cisco SD-WAN Manager servers using one of the following commands:

```
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, 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 *.

Note After a configuration database admin user update, if you are unable to view a specific 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 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 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.

```
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
```

SD-WAN Manager cluster upgrade

SD-WAN Manager upgrade in a cluster is a procedure that

- enables direct upgrades from previous versions, and
- requires intermediate upgrades when starting from older releases.

Upgrade paths

Check the Cisco Catalyst SD-WAN Upgrade Matrix for information about upgrading, including upgrade paths and recommended methods.

Some individual points:

- Cisco vManage 20.3.1 or later releases to Cisco vManage Release 20.6.1

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 .

- Cisco vManage Release 20.3.1 or later to Cisco vManage Release 20.5.1 or later

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

- From a 6-node cluster in which not all services are running on all nodes

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

- Support for compute+data nodes and data nodes

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

One-time boot-up delay

Starting Cisco Catalyst SD-WAN Manager Release 26.2.1, there is a security enhancement to the coordination server used by SD-WAN Manager cluster operations. During the upgrade to 26.2.1 release, additional validation steps results in a one-time boot-up delay immediately after the upgrade. The delay occurs only during the first startup after the upgrade. Regular operations and subsequent reboots do not require the same validation steps.

Prerequisites for cluster upgrade

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

- 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 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.

Note

In certain cases, the existing data-collection-agent container may remain in the Created state without being removed when a new container is launched. However, only one container with the intended name will be active at any given time. Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.18.1a , the data-collection-agent (DCA) runs as a host service instead of a container, which prevents this behavior.

Encryption key requirements for SD-WAN Manager cluster upgrade

This section provides required information about encryption key handling when performing a multitenant cluster upgrade in SD-WAN Manager.

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 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 SD-WAN Manager and trigger the software activation.

Manually restart 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.

Follow these steps to manually restart SD-WAN Manager processes.

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

Example:

```
request nms all stop
```

Step 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. Use the following command to verify that everything is stopped before proceeding further:

```
request nms all status
```

Step 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 SD-WAN Manager device.

Example:

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

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

Example:

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

Step 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 SD-WAN Manager device.

Example:

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

Step 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 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 SD-WAN Manager device. After all the 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
```

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

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

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

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

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

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

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

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

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

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

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

Example:

```
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.

Step 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.

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

What to do next

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.

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

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
```

Upgrade a Cluster Using CLI

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

Example:

```
request nms configuration-db backup path <path_and_filename>
```

Step 2 For upgrades from Cisco vManage Release 20.3.1 or later, copy the current image to each SD-WAN Manager server in the cluster and install the image on each 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 SD-WAN Manager can be done using SCP using CLI using the VPN 512 interface.

Step 3 For upgrades from Cisco vManage Release 20.3.1 or later, activate the current image on each SD-WAN Manager server using the following command. All servers reboot simultaneously.

Example:

request software activate *version*

Step 4 You must upgrade the configuration database when upgrading a cluster.

For more information about compatible upgrade path for configuration-DB upgrade, see Cisco Catalyst SD-WAN Upgrade Matrix.

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 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 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. If you are upgrading from vManage 20.4.x or earlier, then on the node to upgrade, as determined in the previous step, enter this:

request nms configuration-db upgrade

Note

- Enter this command on one node only.
- Check the Cisco Catalyst SD-WAN Upgrade Matrix for information about upgrading from vManage 20.5.x or later.

Step 5 Enter your login credentials, if prompted. Login credentials are prompted in releases earlier than Cisco vManage Release 20.3.1 if all the 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` .

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.

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

Step 2 Click **…** adjacent to the Cisco SD-WAN Manager instance that you want to remove and click **Remove** .

The **Remove Manager** dialog box opens.

Step 3 Enter the username and password to confirm the removal of the device from the network.

Step 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.