Software Image Management for Cluster Components and SWIM

Manage VM Catalog and Repository

Table 1: Feature History

Feature Name	Release Information	Description
Support for Cisco VM Image Upload in qcow2 Format	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature allows you to upload a virtual machine image to Cisco SD-WAN Manager in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.

Cisco SD-WAN Manager supports uploading a prepackaged Cisco virtual machine image, tar.gz, or an image in qcow2 format. It is mandatory to upload a scaffold file if you choose a qcow2 image file. Similarly, you can now select either an image package file or a qcow2 image file with a scaffold file when configuring a Virtual Network Function (VNF) during service chain creation.

A scaffold file contains the following components:

- VNF metadata (image_properties.xml)
- System-generated variables from cluster resource pools for service chaining (system_generated_propeties.xml)
- Tokenized Day-0 configuration files
- Package manifest file (package.mf)

Alternatively, you can package the VM image by providing a root disk image in any of the supported formats (qcow2). Use the linux command-line NFVIS VM packaging tool, **nfvpt.py** to package the qcow2 or alternatively create a customized VM image using Cisco SD-WAN Manager. See Create Customized VNF Image, on page 4.

A VM is SR-IOV capable means sriov_supported is set to true in image_properties.xml in the vm package *.tar.gz. Also, the service chain network is automatically connected to SR-IOV network. If sriov_supported is set to false, an OVS network is created on the data port channel. It's attached to VM VNICs for service chaining by using the OVS network. For the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, a VM uses homogeneous type of network in service chains. This type of network means it's either OVS or SR-IOV, and not a combination of SR-IOV and OVS.

Only two data VNICs are attached to any VM–one for inbound traffic and the other for outbound traffic. If more than two data interfaces are required, use subinterfaces configuration within the VM. The VM packages are stored in the VM catalog.

Note Each VM type such as firewall can have multiple VM images that are uploaded to Cisco SD-WAN Manager from same or different vendors and added to a catalog. Also, different versions that are based on the release of the same VM can be added to a catalog. However, ensure that the VM name is unique.

The Cisco VM image format can be bundled as *.tar.gz and can include:

- Root disk images to boot the VM.
- Package manifest for checksum validation of the file listing in the package.
- Image properties file in XML format that lists the VM meta data.
- (Optional) Day-0 configuration, other files that are required to bootstrap the VM.
- (Optional) HA Day-0 configuration if VM supports stateful HA.
- System-generated properties file in XML format that lists the VM system properties.

VM images can be hosted on both HTTP server local repository that Cisco SD-WAN Manager hosts or on the remote server.

If VM is in Cisco NFVIS supported VM package format such as, tar.gz, Cisco SD-WAN Manager performs all the processing and you can provide variable key and values during VNF provisioning.

Note Cisco SD-WAN Manager manages the Cisco VNFs, and the Day-1 and Day-N configurations within VNF aren't supported for other VNFs. See the Cisco NFVIS Configuration Guide, VM Image Packaging for more information about VM package format and content, and samples on image_properties.xml and manifest (package.mf).

To upload multiple packages for the same VM, same version, communication manager (CM) type, ensure that one of the three values (name, version, VNF type) are different. Then, you can repackage the VM *.tar.gz to be uploaded.

VNF Image Format

Cisco vbond Orchestrator doesn't distinguish between Cisco VNFs and third-party VNFs. All VNFs are categorized based on the services that are provided by the VNF such as router, firewall, load balancer, and others. The package metadata has VM-specific attributes. Based on HA NICs and management NICs specified in the package metadata file, Cisco vBond orchestrator attaches management NIC and HA NIC. By default, management NIC is zero and HA NIC is one. The number of HA NICs that is specified is attached during VNF provisioning.

Upload VNF Images

The VNF images are stored in the Cisco SD-WAN Manager software repository. These VNF images are referenced during service chain deployment, and then they are pushed to Cisco NFVIS during service chain attachment.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 To add a prepackaged VNF image, click **Virtual Images**, and then click **Upload Virtual Image**.

Step 3 Choose the location to store the virtual image.

- To store the virtual image on the local Cisco SD-WAN Manager server and download it to CSP devices over a control plane connection, click **Manager**. The **Upload VNF’s Package to Manager** dialog box appears.

  a. Drag and drop the virtual image file or the qcow2 image file to the dialog box or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server. For example, CSR.tar.gz, ASAv.tar.gz, or ABC.qcow2

  b. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

  c. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

  - Description of the image
  - Version number of the image
  - Checksum
  - Hash algorithm

  You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

  Note

  - It is mandatory to upload a scaffold file if you choose a qcow2 image file.
  - The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

  d. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it available for installing on the CSP devices.

- To store the image on a remote Cisco SD-WAN Manager server and then download it to CSP devices, click **Remote Server - Manager**. The **Upload VNF's Package to Remote Server-Manager** dialog box appears.

  a. In the **Manager Hostname/IP Address** field, enter the IP address of an interface on Cisco SD-WAN Manager server that is in the management VPN (typically, VPN 512).

  b. Drag and drop the virtual image file or the qcow2 image file to the dialog box, or click **Browse** to choose the virtual image from the local Cisco SD-WAN Manager server.

  c. If you upload a file, specify the type of the uploaded file: **Image Package** or **Scaffold**. Optionally, specify a description of the file and add custom tags to the file. The tags can be used to filter images and scaffold files when creating a service chain.

  d. If you upload a qcow2 image file, specify the service or VNF type: **FIREWALL** or **ROUTER**. Optionally, specify the following:

  - Description of the image
  - Version number of the image
  - Checksum
  - Hash algorithm

  You can also add custom tags to the file that can be used to filter images and scaffold files when creating a service chain.

  Note
  - It is mandatory to upload a scaffold file if you choose a qcow2 image file.
  - The option to select a qcow2 image file is available from Cisco vManage Release 20.7.1. In Cisco vManage Release 20.6.1 and earlier releases, you can select only a tar.gz file.

  e. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

You can have multiple VNF entries such as a firewall from same or from different vendors. Also, you can add different versions of VNF that are based on the release of the same VNF. However, ensure that the VNF name is unique.

Create Customized VNF Image

Before you begin

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

- Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.

- Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

- Root disk image for a VNF–qcow2
- Day-0 configuration files–system and tokenized custom variables
- VM configuration–CPU, memory, disk, NICs
- HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link.
- Additional Storage–If more storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .

Step 2 Click **Virtual Images** > **Add Custom VNF Package**.

Step 3 Configure the VNF with the following VNF package properties and click **Save**.

Table 2: VNF Package Properties

Field	Mandatory or Optional	Description
Package Name	Mandatory	The filename of the target VNF package. It's the Cisco NFVIS image name with .tar or .gz extensions.
App Vendor	Mandatory	Cisco VNFs or third-party VNFs.
Name	Mandatory	Name of the VNF image.
Version	Optional	Version number of a program.
Type	Mandatory	Type of VNF to choose. Supported VNF types are: Router, Firewall, Load Balancer, and Other.

Step 4 To package a VM qcow2 image, click **File Upload**, and browse to choose a qcow2 image file.

Step 5 To choose a bootstrap configuration file for VNF, if any, click **Day 0 Configuration** and click **File Upload** to browse and choose the file.

Include the following Day-0 configuration properties:

Table 3: Day-0 Configuration

Field	Mandatory or Optional	Description
Mount	Mandatory	The path where the bootstrap file gets mounted.

Field	Mandatory or Optional	Description
Parseable	Mandatory	A Day-0 configuration file can be parsed or not. Options are: **Enable** or **Disable**. By default, **Enable** is chosen.
High Availability	Mandatory	High availability for a Day-0 configuration file to choose. Supported values are: Standalone, HA Primary, HA Secondary.

Note
If any bootstrap configuration is required for a VNF, create a *bootstrap-config* or a *day0-config* file.

Step 6 To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** next to the desired Day-0 configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

Note
The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. For a shared VNF, see the Custom Packaging Details for Shared VNF for the list of system variables that must be added for different VNF types..

a) To add a system variable, in the **CLI configuration** dialog box, select, and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.
b) Choose a system variable from the **Variable Name** drop-down list, and click **Done**. The highlighted property is replaced by the system variable name.
c) To add a custom variable, in the **CLI configuration** dialog box, choose and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.
d) Enter the custom variable name and choose a type from **Type** drop-down list.
e) To set the custom variable attribute, do the following:

   - To ensure that the custom variable is mandatory when creating a service chain, click **Type** next to **Mandatory**.
   - To ensure that a VNF includes both primary and secondary day-0 files, click **Type** next to **Common**.

f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

Step 7 To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an extra qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

Note
Ensure that you don’t combine ephemeral disks and storage volumes when uploading extra VM images.

Step 8 To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

Table 4: Storage Properties

Field	Mandatory or Optional	Description
Size	Mandatory	The disk size that is required for the VM operation. If the size unit is GiB, the maximum disk size can be 256 GiB.
Size Unit	Mandatory	Choose size unit. The supported units are: MIB, GiB, TiB.
Device Type	Optional	Choose a disk or CD-ROM. By default, disk is chosen.
Location	Optional	The location of the disk or CD-ROM. By default, it's local.
Format	Optional	Choose a disk image format. The supported formats are: qcow2, raw, and vmdk. By default, it's raw.
Bus	Optional	Choose a value from the drop-down list. The supported values for a bus are: virtio, scsi, and ide. By default, it's virtio.

Step 9 To add VNF image properties, expand **Image Properties** and enter the following image information.

Table 5: VNF Image Properties

Field	Mandatory or Optional	Description
SR-IOV Mode	Mandatory	Enable or disable SR-IOV support. By default, it's enabled.
Monitored	Mandatory	VM health monitoring for those VMs that you can bootstrap. The options are: enable or disable. By default, it's enabled.
Bootup Time	Mandatory	The monitoring timeout period for a monitored VM. By default, it's 600 seconds.
Serial Console	Optional	The serial console that is supported or not. The options are: enable or disable. By default, it's disabled.

Field	Mandatory or Optional	Description
Privileged Mode	Optional	Allows special features like promiscuous mode and snooping. The options are: enable or disable. By default, it’s disabled.
Dedicate Cores	Mandatory	Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. The options are: enable or disable. By default, it’s enabled.

Step 10 To add VM resource requirements, expand **Resource Requirements** and enter the following information.

Table 6: VM Resource Requirements

Field	Mandatory or Optional	Description
Default CPU	Mandatory	The CPUs supported by a VM. The maximum numbers of CPUs supported are 8.
Default RAM	Mandatory	The RAM supported by a VM. The RAM can range 2–32.
Disk Size	Mandatory	The disk size in GB supported by a VM. The disk size can range 4–256.
Max number of VNICs	Optional	The maximum number of VNICs allowed for a VM. The number of VNICs can from range 8–32 and by default, the value is 8.
Management VNIC ID	Mandatory	The management VNIC ID corresponding to the management interface. The valid range is from 0 to maximum number of VNICs.
Number of Management VNICs ID	Mandatory	The number of VNICs.
High Availability VNIC ID	Mandatory	The VNIC IDs where high availability is enabled. The valid range is from 0–maximum number of VNICs. It shouldn’t conflict with management VNIC Id. By default, the value is 1.

Field	Mandatory or Optional	Description
Number of High Availability VNICs ID	Mandatory	The maximum number of VNIC IDs where high availability is enabled. The valid range is 0–(maximum number of VNICs-number of management VNICs-2) and by default, the value is 1.

Step 11 To add day-0 configuration drive options, expand **Day 0 Configuration Drive options** and enter the following information.

Table 7: Day-0 Configuration Drive Options

Field	Mandatory or Optional	Description
Volume Label	Mandatory	The volume label of the Day-0 configuration drive. The options are: V1 or V2. By default, the option is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.
Init Drive	Optional	The Day-0 configuration file as a disk when mounted. The default drive is CD-ROM.
Init Bus	Optional	Choose an init bus. The supported values for a bus are: virtio, scsi, and ide. By default, it's ide.

The Software Repository table displays the customized VNF image, and image is available for choosing when creating a custom service chain.

View VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**.

Step 3 To filter the search results, use the filter option in the search bar.

The Software Version column provides the version of the software image.

The Software Location column indicates where the software images are stored. Software images can be stored either in the repository on the Cisco SD-WAN Manager server or in a repository in a remote location.

The **Version Type Name** column provides the type of firewall.

The **Available Files** column lists the names of the VNF image files.

The **Update On** column displays when the software image was added to the repository.

Step 4 For the desired VNF image, click **...** and choose **Show Info**.

Delete VNF Images

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 2 Click **Virtual Images**. The images in the repository are displayed in a table.

Step 3 For the desired image, click **...** and choose **Delete**.

Note If you're downloading a VNF image to a device, you can't delete the VNF image until the download process completes.

Note If the VNF image is referenced by a service chain, it can't be deleted.

Upgrade Cisco NFVIS Using Cisco SD-WAN Manager

To upload and upgrade Cisco NFVIS, the upgrade image must be available as an archive file that can be uploaded to the Cisco SD-WAN Manager repository using Cisco SD-WAN Manager. After you upload the Cisco NFVIS image, the upgraded image can be applied to a CSP device by using the **Software Upgrade** window in Cisco SD-WAN Manager. You can perform the following tasks when upgrading Cisco NFVIS software using Cisco SD-WAN Manager:

- Upload Cisco NFVIS upgrade image. See Upload NFVIS Upgrade Image, on page 11.
- Upgrade a CSP device with the uploaded image. See Upgrade a CSP Device with a Cisco NFVIS Upgrade Image, on page 11.
- View the upgrade status for the CSP device by clicking the **Tasks** icon located in the Cisco SD-WAN Manager toolbar.

Upload NFVIS Upgrade Image

Procedure

Step 1 Download the Cisco NFVIS upgrade image from a prescribed location to your local system. You can also download the software image to an FTP server in your network.

Step 2 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .

Step 3 Click **Add New Software** > **Remote Server/Remote Server - Manager**.

You can either store the software image on a remote file server, on a remote Cisco SD-WAN Manager server, or on a Cisco SD-WAN Manager server.

Cisco SD-WAN Manager server: Saves software images on a local Cisco SD-WAN Manager server.

Remote server: Saves the URL pointing to the location of the software image and can be accessed using an FTP or HTTP URL.

Remote Cisco SD-WAN Manager server: Saves software images on a remote Cisco SD-WAN Manager server and location of the remote Cisco SD-WAN Manager server is stored in the local Cisco SD-WAN Manager server.

Step 4 To add the image to the software repository, browse and choose the Cisco NFVIS upgrade image that you had downloaded in Step1.

Step 5 Click **Add|Upload**.

The Software Repository table displays the added NFVIS upgrade image, and it's available for installing on the CSP devices. See the Manage Software Upgrade and Repository topic in the Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide.

Upgrade a CSP Device with a Cisco NFVIS Upgrade Image

Before you begin

Ensure that the Cisco NFVIS software versions are the files that have `.nfvispkg` extension.

Procedure

Step 1 From theCisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade** > **WAN Edge**.

Step 2 Check one or more CSP device check boxes for the devices you want to choose.

Step 3 Click **Upgrade**. The **Software Upgrade** dialog box appears.

Step 4 Choose the Cisco NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.

Step 5 To automatically upgrade and activate with the new Cisco NFVIS software version and reboot the CSP device, check the **Activate and Reboot** check box.

If you don't check the **Activate and Reboot** check box, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new Cisco NFVIS software version by choosing the device again and clicking the **Activate** button in the **Software Upgrade** window.

Step 6 Click **Upgrade**.

The **Task View** window displays a list of all running tasks along with total number of successes and failures. The window periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status window by clicking the **Task View** icon located in the Cisco SD-WAN Manager toolbar.

Note
If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happens in a sequence.

Note
The **Set the Default Software Version** option isn't available for the Cisco NFVIS images.

The CSP device reboots and the new NFVIS version is activated on the device. This reboot happens during the **Activate** phase. The activation can either happen immediately after upgrade if you check the **Activate and Reboot** check box, or by manually clicking **Activate** after choosing the CSP device again.

To verify if CSP device has rebooted and is running, use the task view window. Cisco SD-WAN Manager polls your entire network every 90 seconds up to 30 times and shows the status on th task view window.

Note You can delete a Cisco NFVIS software image from a CSP device if the image version isn't the active version that is running on the device.

Upgrade Cisco Catalyst 9500 Switches

You can perform a software upgrade for both Cisco Catalyst 9500-40X and Cisco Catalyst 9500-48Y4C switches.

Before you begin

- Back up the running configuration in both the switches
- Ensure that you download the Cisco Catalyst 9500 upgrade software (.bin file) from cisco.com website and it is available as an archive file.

Procedure

Step 1 To copy the upgraded software from Trivial File Transfer Protocol (TFTP) to the flash of switch1, use the following commands:

a) **conf t**

Enters the configuration mode one per line. Ends with CNTL/Z.

Example:

```
c9500-1#conf t
```

b) **blocksize** *value*

Manually changes the block size in the global configuration to speed up the transfer process.

Example:

```
c9500-1(config)#ip tftp blocksize 8165
c9500-1(config)#end
```

c) **copy scp**

Securely copies switch image files to the flash of switch1.

Example:

```
c9500-1#copy scp://<cec-id>@172.16.0.151//auto/tftp-xxx-users2/yyyy/Switch_Image/
cat9k_iosxe.17.03.01.SPA.bin flash: vrf Mgmt-vrf
```

Step 2 To copy the upgraded software from one switch to another switch when they are in the SVL mode, use the following commands.

If both the switches are not in SVL mode, repeat Step 1 for switch2.

- Cisco Catalyst 9500-40X

  copy

  Copies from flash of switch1 to flash of switch2.

  ```
  c9500-1#copy flash-1:cat9k_iosxe.17.03.01.SPA.bin flash-2:
  ```

- Cisco Catalyst 9500-48Y4C

  copy

  Copies to bootflash of switch2 from switch1

  ```
  switch1#copy bootflash:cat9k_iosxe.17.03.01.SPA.bin stdby-bootflash:
  cat9k_iosxe.17.03.01.SPA.bin
  ```

Step 3 To remove the startup switch software specification, use the **no** form of the **boot system** command on Catalyst 9500 switches.

a) **config t**

Enters the configuration mode.

b) **no boot system**

Clears all startup software configuration.

Step 4 To configure the switch and reload the copied software, use the following commands:

- Cisco Catalyst 9500-40X

  a. boot system switch all flash

  Configures the boot variable to boot the switch with the newly copied software.

  ```
  c9500-1(config)#boot system switch all flash:
  cat9k_iosxe.17.03.01.SPA.bin
  ```

  b. end

  Exits global configuration mode of the switch

```
c9500-1(config)#end
```

c. **wr mem**

Copies the switch configuration changes that you have made and save it to the configuration in flash.

```
c9500-1#wr mem
```

- Cisco Catalyst 9500-48Y4C

a. **boot system bootflash**

Installs the upgraded software, saves the configuration, and reloads the copied software.

```
switch1(config)#boot system bootflash:
cat9k_iosxe.17.03.01.SPA.bin
```

b. **end**

Exits global configuration mode of the switch

```
switch1(config)#end
```

c. **wr mem**

Copies the switch configuration changes that you have made and save it to the configuration in bootflash.

```
switch1#wr mem
```

- Switches without SVL configuration. Configure both the switches to reload the copied software. Use the following commands on both the switches:

a. **boot system flash**

Configures the switches to boot the image from flash memory.

```
Switch(config)#boot system flash:
cat9k_iosxe.17.03.01.SPA.bin
```

b. **end**

Exits global configuration mode of the switch

```
Switch(config)#end
```

c. **wr mem**

Copies the switch configuration changes that you have made and save it to the configuration in flash.

```
Switch#wr mem
```

Step 5 To verify only one boot system configuration exists in the running configuration, use the following commands:

a) **show run | i boot**

Verifies that the upgraded software is the first boot image.

Example:

```
c9500-1#show run | i boot
```

b) **license boot level**

Boots a new software license on a switch with the DNA essentials

Example:

```
c9500-1#license boot level network-advantage addon dna-advantage
```

c) **diagnostic bootup level**

Configures the bootup diagnostic level to trigger diagnostics when the switch boots up.

Example:

```
c9500-1#diagnostic bootup level minimal
```

Step 6 To reload and apply the switch configuration change, use the following command. It applies for both Cisco Catalyst 9500-40X and Cisco Catalyst 9500-48Y4C switches.:

Example:

```
c9500-1#reload
```

Supported Upgrade Scenarios and Recommended Connections

The following are the various upgrade scenarios and cluster states that determine the use of prescriptive or flexible connections.

Table 8: Supported Connections

Cisco SD-WAN Manager	Cisco NFVIS	Cluster State	Supported Connections
Upgrade from Releases 19.3 or 20.1.1.1 to Release 20.3.1	Upgrade from Releases 3.12 or 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Releases 19.3 or 20.1.1.1	Use prescriptive connections
Use the latest Release, 20.3.1	Use the latest Release, 4.2.1	Cluster created and active in Cisco vManage Release 20.3.1	Can use prescriptive or flexible connections
Upgrade from Release 20.1.1.1 to Release 20.3.1	Upgrade from Release 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Release 20.1.1.1	Use prescriptive connections
Upgrade from Release 20.1.1.1 to Release 20.3.1	Upgrade from Release 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Release 20.1.1.1. To add a new Cisco CSP device after upgrade, see Add Cisco CSP Device to Cluster After Upgrading Cisco SD-WAN Manager and Cisco NFVIS.	Use prescriptive connections
Upgrade from Release 20.1.1.1 to Release 20.3.1	Upgrade from Release 4.1 to Releases 4.1.1 or 4.2.1	Cluster created and active in Cisco vManage Release 20.3.1	Can use prescriptive or flexible connections

Add Cisco CSP Device to Cluster After Upgrading Cisco SD-WAN Manager and Cisco NFVIS

To add a Cisco CSP device to a cluster if the cluster was created before upgrading Cisco SD-WAN Manager to Release 20.3.1, perform the following steps:

1. Connect the cables for the newly added Cisco CSP device according to prescriptive connections.
2. Upgrade Cisco NFVIS to Release 4.2.1
3. Use the following commands on the newly added Cisco CSP device by logging into Cisco NFVIS:
    - **request csp-prescriptive-mode**

      Requests the newly added Cisco CSP device to run in prescriptive mode.
    - **request activate chassis-number** *chassis number* **token** *serial number*

      Activates the Cisco CSP device

      Example

      ```
      request activate chassis-number 71591a3b-7d52-24d4-234b-58e5f4ad0646 token
      e0b6f073220d85ad32445e30de88a739
      ```

Recommendations Prior to Updating a Cluster

- To use an already active cluster when you upgrade to the latest release of the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, ensure that you upgrade Cisco SD-WAN Manager and Cisco NFVIS to the latest releases.
- To create a new cluster when you upgrade to the latest release of the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, ensure that you upgrade Cisco SD-WAN Manager and Cisco NFVIS to the latest releases for flexible connections.