Upgrading the Cisco Nexus 1000VE

This chapter contains the following sections:

Pre-requisites and Usage Guidelines

Follow these prerequisites and usage guidelines before upgrading Cisco Nexus 1000VE to release 5.2(1)SV5(1.3):

- Ensure that the current Nexus 1000VE release instance is up and running in the existing setup.
- Cisco Nexus 1000VE release 5.2(1)SV5(1.3) supports VMware vCenter v6.7. If you are upgrading ESXi hosts and VMWare vCenter Server to release v6.7, we recommend you to follow the upgrade steps in the specified sequence.
- Ensure that you have sufficient maintenance period during the upgrade process because a service disruption is expected during the upgrade process.

Upgrading the Cisco Nexus 1000VE VSMs

Software Images

The software image install procedure is dependent on the following factors:

- Software images—The kickstart and system image files reside in directories or folders that you can access from the Cisco Nexus 1000VE software prompt.
- Image version—Each image file has a version.
- Disk—The bootflash: resides on the VSM.

- ISO file—If a local ISO file is passed to the **install all** command, the kickstart and system images are extracted from the ISO file.

In-Service Software Upgrades on Systems with Dual VSMs

The Cisco Nexus 1000VE software supports in-service software upgrades (ISSUs) for systems with dual VSMs. An ISSU can update the software images on your switch without disrupting data traffic. Only control traffic is disrupted. If an ISSU causes a disruption of data traffic, the Cisco Nexus 1000VE software warns you before proceeding so that you can stop the upgrade and reschedule it to a time that minimizes the impact on your network.

Note On systems with dual VSMs, you should have access to the console of both VSMs to maintain connectivity when the switchover occurs during upgrades. If you are performing the upgrade over Secure Shell (SSH) or Telnet, the connection will drop when the system switchover occurs, and you must reestablish the connection.

An ISSU updates the following images:

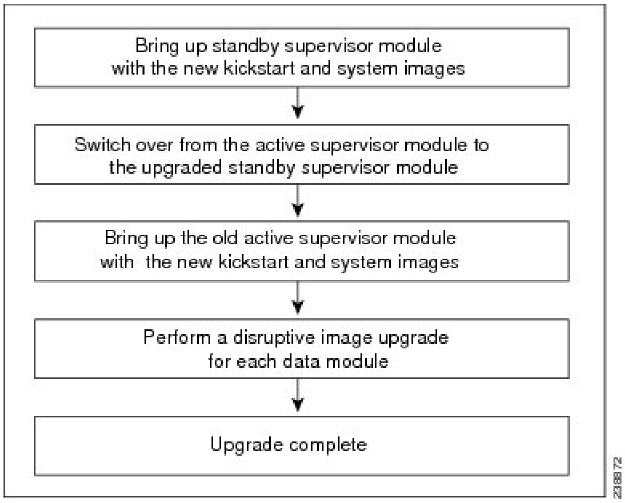
- Kickstart image
- System image
- VEM images

All of the following processes are initiated automatically by the upgrade process after the network administrator enters the **install all** command.

ISSU Process for Cisco Nexus 1000VE

The following figure shows the ISSU process.

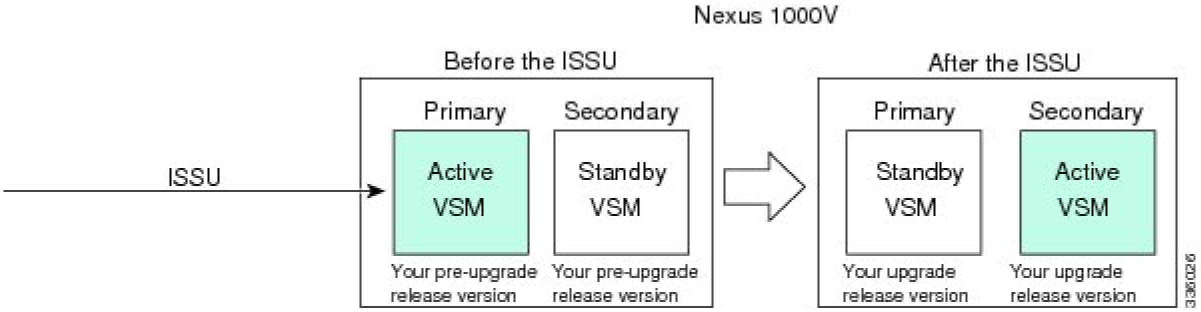
Figure 1: ISSU Process


Bring up standby supervisor module with the new kickstart and system images
Switch over from the active supervisor module to the upgraded standby supervisor module
Bring up the old active supervisor module with the new kickstart and system images
Perform a disruptive image upgrade for each data module
Upgrade complete
238872

ISSU VSM Switchover

The following figure provides an example of the VSM status before and after an ISSU switchover.

Figure 2: Example of an ISSU VSM Switchover



ISSU Command Attributes

Support

The **install all** command supports an in-service software upgrade (ISSU) on dual VSMs in an HA environment and performs the following actions:

- Determines whether the upgrade is disruptive and asks if you want to continue.
- Copies the kickstart and system images to the standby VSM. Alternatively, if a local ISO file is passed to the **install all** command instead, the kickstart and system images are extracted from the file.
- Sets the kickstart and system boot variables.
- Reloads the standby VSM with the new Cisco Nexus 1000VE software.
- Causes the active VSM to reload when the switchover occurs.

Benefits

The **install all** command provides the following benefits:

- You can upgrade the VSM by using the **install all** command.
- You can receive descriptive information on the intended changes to your system before you continue with the installation.
- You have the option to cancel the command. Once the effects of the command are presented, you can continue or cancel when you see this question (the default is no):

```
Do you want to continue (y/n) [n]: y
```

- You can upgrade the VSM using the least disruptive procedure.
- You can see the progress of this command on the console, Telnet, and SSH screens:
  - After a switchover process, you can see the progress from both the VSMs.
  - Before a switchover process, you can see the progress only from the active VSM.

- The **install all** command automatically checks the image integrity, which includes the running kickstart and system images.
- The **install all** command performs a platform validity check to verify that a wrong image is not used.
- The Ctrl-C escape sequence gracefully ends the **install all** command. The command sequence completes the update step in progress and returns to the switch prompt. (Other upgrade steps cannot be ended by using Ctrl-C.)
- After running the **install all** command, if any step in the sequence fails, the command completes the step in progress and ends.

Upgrading VSM from Release 5.2(1)SV5(1.2) to Release 5.2(1)SV5(1.3)

Unregistered Cisco.com users cannot access the links provided in this document.

Procedure

Step 1 Log in to the active VSM.

Step 2 Log in to Cisco.com to access the links provided in this document. To log in to Cisco.com, go to the URL http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.

Step 3 Access the Software Download Center by using this URL:

http://www.cisco.com/public/sw-center/index.shtml

Step 4 Navigate to the download site for your system.

You see links to the download images for your switch.

Step 5 Choose and download the Cisco Nexus 1000VE zip file and extract the kickstart and system software files to a server.

Step 6 Ensure that the required space is available for the image file(s) to be copied by entering the **dir bootflash:** command.

Tip We recommend that you have the kickstart and system image files for at least one previous release of the Cisco Nexus 1000VE software on the system to use if the new image files do not load successfully.

Step 7 Verify that there is space available on the standby VSM by entering the **dir bootflash://sup-standby/** command .

Step 8 Delete any unnecessary files to make space available if you need more space on the standby VSM.

Step 9 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000VE kickstart and system images or the ISO image to the active VSM by using a transfer protocol. You can use ftp:, tftp:, scp:, or sftp:. The examples in this procedure copies a kickstart and system image using scp:.

Note When you download an image file, change to your FTP environment IP address or DNS name and the path where the files are located.

a) switch# **copy scp://***filepath/kickstart_filename* **bootflash:***kickstart_filename*

Copy the ISO image.

b) switch# **copy scp://***filepath/system_filename* **bootflash:***system_filename*

Copy kickstart and system images.

Step 10 switch# **show install all impact kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename*

Verify the ISSU upgrade for the kickstart and system images or the ISO image. The example in this procedure shows the kickstart and system images.

Step 11 Read the release notes for the related image file. See the *Cisco Nexus 10000VE Release Notes*.

Step 12 Determine if the Cisco Virtual Security Gateway (Cisco VSG) is configured in the deployment by using the **show vnm-pa status** command .

Note If an output displaying a successful installation is displayed as in the example, the Cisco VSG is configured in the deployment. You must follow the upgrade procedure in the *Cisco Virtual Security Gateway and Cisco Virtual Network Management Center Installation and Upgrade Guide*. If an output displaying that the policy agent has not installed is displayed, continue to Step 13.

Step 13 Save the running configuration to the startup configuration by using the **copy running-config startup-config** command.

Step 14 Save the running configuration on the bootflash and externally.

Note You can also run a VSM backup. See the “Configuring VSM Backup and Recovery” chapter of the *Cisco Nexus 1000V System Management Configuration Guide*.

a) Save the running configuration on the bootflash by using the **copy running-config bootflash:run-cfg-backup** command.
b) Save the running configuration externally by using the **copy running-config scp://***external_backup_location* command.

Step 15 Perform the upgrade on the active VSM using the ISO or kickstart and system images by using the **install all kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename* command. The example in this procedure shows the kickstart and system images.

Step 16 Continue with the installation by pressing **`Y`**.

If you press **`N`**, the installation exits gracefully.

Note As part of the upgrade process, the standby VSM is reloaded with new images. Once it becomes the HA standby again, the upgrade process initiates a switchover. The upgrade then continues from the new active VSM.

Step 17 After the installation operation completes, log in and verify that the switch is running the required software version by using the switch# **show version** command

Step 18 Copy the running configuration to the startup configuration to adjust the startup-config size by using the switch# **copy running-config startup-config** command

Step 19 Display the log for the last installation by entering the following commands.

a) switch# **show install all status**
b) switch# **attach** *module_name*
c) switch# **show install all status**

Step 20 Review information about reserving memory and CPU on the VSM VM at the following URL: Reserving the Memory and CPU on the Virtual Supervisor Module Virtual Machine.

Note You must review this information, to accommodate the new scalability limits.

Upgrading Cisco Nexus 1000VE Manager vCenter Plugin

To upgrade the Cisco Nexus 1000VE Manager vCenter Plugin, see Installing the Cisco Nexus 1000VE Manager vCenter Plugin.

Upgrading the Cisco Nexus 1000VE VSEs

You can upgrade the Cisco Nexus 1000VE VSEs using two methods:

- Using Cisco Nexus 1000VE Manager vCenter Plugin
- Manually

Upgrading VSE using Cisco Nexus 1000VE Manager vCenter Plugin

Complete these steps to upgrade VSE using Cisco Nexus 1000VE Manager vCenter Plugin.

Before you begin

Make sure that new plugin corresponding to 5.2(1)SV5(1.3) is installed on vCenter.

Procedure

Step 1 Download the new VSE images, cisco-vse-5.2.1.SV5.1.3.ovf and cisco-vse-5.2.1.SV5.1.3-disk1.vmdk, to VMware vCenter content library.

Step 2 Navigate to **Home** on VMware vCenter Web Client. If a content library has already been created with the required VSE image, go to Step 6. If not, proceed to step 2.

Step 3 On the **Navigator** pane, click **Content Libraries** to open the **Content Libraries** page.

Step 4 On the **Getting Started** tab, click **Create new content library**.

Step 5 In the **New Content Library** dialog box, do the following:

a) On the **Name and Location** page, enter the content library name in the **Name** text field and select vCenter Server IP address from the **vCenter Server** drop-down list

b) Click **Next**.

c) On the **Configure content library** page, verify that the default option, Local content library is selected.

d) Click **Next**.

e) On the **Add Storage** page, choose the **Select a datastore** option and from the **Filter** tab, select a storage location.

f) Click **Next**.

g) On the **Ready to complete** page, click **Finish**.

h) On the **Navigator** tab, select the new content library that you just created.

i) On the **Getting Started** tab, under **Basic Tasks** section, click **Import Item** to open **New Content Library – Import Library Item** dialog box.

j) Choose Local file option and click **Browse** and navigate to the location of the VSE OVF file. Select the VSE OVF file and click **Open**.

k) In the **Select referenced files** dialog box, select the OVF referenced files and click **Open**.

l) On the **Select referenced files** dialog box, click **Ok**.

m) On the **New Content Library – Import Library Item** dialog-box, click **Ok**.

n) On the **Home** page, click **Recent Tasks** tab at the bottom to check VSE file upload progress.

Step 6 Navigate to **Home** tab on **VMware vSphere Web Client**.

Step 7 Click **N1KVE Manager**, and enter the VMware vCenter password and click **Login**. The **N1KVE Manager** page opens.

Step 8 On the **Installation** tab, select a Data Center from the **Select a DC** drop-down list.

Step 9 Select N1KVE vDS from the **Select a VDS** drop-down list to list the available Hosts.

Step 10 Select a Host to upgrade from the list of **Hosts**.

Step 11 Select an OVF file from the **OVF File** drop-down list.

Step 12 Enter VSM IP address for **VSM IP** text-field.

Step 13 Enter domain Id for **Domain ID** text-field.

Step 14 Select an uplink port profile from the **Uplink Port Profile** drop-down list.

Step 15 Select a management port group from the **Management Port Group** drop-down list.

Step 16 Select **Auto** or choose from **Datastore** drop-down list for all hosts.

Step 17 Enter VSM and VSE credentials in respective fields.

Step 18 Click **Upgrade**.

Step 19 In the **Upgrade** dialog box, click **Yes** to complete the VSE upgrade process.

Step 20 Log in to Cisco N1KVE VSM and reload the system using the **reload** command. After the VSM boots up, you should be able to see the modules are up with new version.

Note Module indices change after upgrading VSE.

Example:

```
N1KVE-VSM# show module
Mod Ports Module-Type Model Status
--- ----- -------------------------------- ------------------ ------------
1 0 Virtual Supervisor Module Nexus1000V active *
2 0 Virtual Supervisor Module Nexus1000V ha-standby
5 332 Virtual Service Engine NA ok
6 332 Virtual Service Engine NA ok

Mod Sw Hw
--- ------------------ ------------------------------------------------
1 5.2(1)SV5(1.3) 0.0
2 5.2(1)SV5(1.3) 0.0
5 5.2(1)SV5(1.3) NA
6 5.2(1)SV5(1.3) NA

Mod Server-IP Server-UUID Server-Name
--- --------------- ------------------------------------ --------------------
1 10.XXX.XXX.XXX NA NA
2 10.XXX.XXX.XXX NA NA
9 10.XXX.XXX.XXX XXXXXXXX-YYYY-ZZZZ-XXXX-YYYYYYYYYYYY localhost.localdomain
10 10.XXX.XXX.XXX AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE localhost.localdomain
```

```
Mod VSE-IP Host-IP
--- -------------- -----------------------------------
9 10.XXX.XXX.XXX 10.XXX.XXX.XXX
10 10.XXX.XXX.XXX 10.XXX.XXX.XXX
```

Upgrading VSE Manually

Complete the following steps to upgrade VSE manually. You need to manually upgrade all the VSEs.

Procedure

Step 1 Download the new VSE image, cisco-vse-5.2.1.SV5.1.3.ova, to the local system.

Step 2 Login to VSM.

Step 3 Use the **show module** command to identify the module to upgrade.

Step 4 Log into VMware vCenter using VMWare vSphere Web Client. For each host under the VSM complete the following steps:

a) Browse over **Hosts and Clusters** tab and Select a **Host**.

b) Select the **VSE Virtual Machine**, under the **Host**. Typically the VSE VMs are named as *N1KVE_VSE_<HOST_IP_ADDRESS>*.

c) Right-click the VSE and select **Edit Settings**. Note down the port-profiles for following network adapters required in future steps: Network Adapter 1 (Management), Network Adapter 2 (inside-trunk1), Network Adapter 3 (inside-trunk2), and Network Adapter 4 (Outside).

d) Right-click **Power** and select **Power-off**.

e) Right-click and select **Delete from the disk**.

Note Module will go offline in VSM.

Step 5 Login to VSM using administrator credentials and delete VSE module using the **no vse** command.

Example:

```
#no vse module_no
// for deleted VSE module
```

Step 6 Reboot the VSM to clear the stale VSE entry.

Step 7 Deploy the new VSE VM with the saved configuration settings. Login to VMware vCenter using VMWare vSphere Web Client.

a) In the **VMware vCenter WebClient**, select the **Host**.

b) Right-click the host and select **Deploy OVF Template** > **Local file** > **Browse**.

c) In the **Browse** dialog box, choose the cisco-vse-5.2.1.SV5.1.3.ova file from local system and click **Next**.

d) Enter VSE VM name, follow the standard naming convention, *N1KVE_VSE_<HOST_IP_ADDRESS>*.

e) Choose the same datacentre and click **Next**.

f) Choose the host and click **Next**.

g) Click **Next**.

h) In the **Select Networks** window, select **Destination Network** corresponding to inside-trunk1, inside-trunk2, Management and Outside Network Adapters as noted in Step 4c.

i) Enter the details in the **Customize Template** window:

- **Admin password**: Provide VSE administrator password.
- **Controller DomainId**: Provide domain id. Use **show svs domain** command to get domain Id.
- **DNS**: Provide DNS server IP address.
- **DNS Domain**: Provide DNS domain if required.
- **Default Gateway**: Default gateway IP Address.
- **ESX Host IP Address**: Host IP Address.
- **IP Setting(static/dhcp)**: Enter dhcp or static.
- **L3-Control IP Address**: Provide VSM IP address.
- **Network 1 IP Address**: Provide VSE IP Address. This IP address should be unused and available.
- **Network 1 Netmask**: Subnet mask for VSE adapter.
- **Uplink Port-Profile**: Provide the outside-trunk. Use the **show runnning-config port-profile outside-trunk** command on VSM to verify.

j) Click **Next**.
k) Review the detail of custom template and click **Finish** to deploy VSE on the selected host.
l) After deployment is completed, power on the VSE. Wait for some time to allow VSE to bootup.
m) Reload Cisco N1KVE VSM using the **reload** command and verify whether VSE is online.

Step 8 Verify the updated VSE using the **show module** command on VSM.

Example:

```
N1KVE-VSM# show module
Mod Ports Module-Type Model Status
--- ----- -------------------------------- ------------------ ------------
1 0 Virtual Supervisor Module Nexus1000V active *
2 0 Virtual Supervisor Module Nexus1000V ha-standby
5 332 Virtual Service Engine NA ok
6 332 Virtual Service Engine NA ok

Mod Sw Hw
--- ------------------ ------------------------------------------------
1 5.2(1)SV5(1.3) 0.0
2 5.2(1)SV5(1.3) 0.0
5 5.2(1)SV5(1.3) NA
6 5.2(1)SV5(1.3) NA

Mod Server-IP Server-UUID Server-Name
--- --------------- ------------------------------------ --------------------
1 10.XXX.XXX.XXX NA NA
2 10.XXX.XXX.XXX NA NA
9 10.XXX.XXX.XXX XXXXXXXX-YYYY-ZZZZ-XXXX-YYYYYYYYYYYY localhost.localdomain
10 10.XXX.XXX.XXX AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE localhost.localdomain

Mod VSE-IP Host-IP
--- --------------- ------------------------------------
9 10.XXX.XXX.XXX 10.XXX.XXX.XXX
10 10.XXX.XXX.XXX 10.XXX.XXX.XXX
```

Changing the VSE Feature Level

After upgrading to Release 5.2(1)SV5(1.3), you must update the VSE feature level.

Before you begin

- VSM and VSE have been upgraded to Release 5.2(1)SV5(1.3) .

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **show system VSE feature level**

Displays the current VSE feature level. The current feature level should be 5.2(1)SV5(x).

Step 3 switch(config)# **system update VSE feature level** *value*

Configures the VSE feature level.

Note When you run the **system update VSE feature level** command after upgrading from Release 5.2(1)SV5(1.2) to Release 5.2(1)SV5(1.3), it displays the following versions:

- 5.2(1)SV5(1.3)

You must select 5.2(1)SV5(1.3) to update the VSE feature level to Release 5.2(1)SV5(1.3).

Step 4 (Optional) switch(config)# **copy running-config startup-config**

Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to update the VSE feature level after upgrading to Release 5.2(1)SV5(1.3).

```
N1KVE-VSM#
N1KVE-VSM# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    332    Virtual Service Engine            NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
2    5.2(1)SV5(1.3)      0.0
3    5.2(1)SV5(1.3)      NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
2    10.126.129.80    NA                                    NA
```

```
3    10.126.129.63    4206ECC3-9820-CF49-4778-31BEF6680657  localhost.localdomain

Mod  VSE-IP           Host-IP
---  ---------------  ------------------------------------
3    10.126.129.63    10.126.129.109

* this terminal session
N1KVE-VSM#
N1KVE-VSM# module vse 3 execute vemcmd show feature level
VSE Feature Level: 5.2(1)SV5(1.2)
N1KVE-VSM#
N1KVE-VSM# show system vse feature level
Current feature level: 5.2(1)SV5(1.2)
N1KVE-VSM# configure
Enter configuration commands, one per line.  End with CNTL/Z.
N1KVE-VSM(config)#
N1KVE-VSM(config)# system update vse feature level
Feature      Version
Level        String
--------------------
1            5.2(1)SV5(1.3)
N1KVE-VSM(config)# system update vse feature level 1
 Note: Run the command 'enable l3sec' under svs-domain for robust VSM-VSE
 security
 Note: Run following commands under 'vdc <switch-name>' to take full advantage
 of scale offered by this release:
 'limit-resource port-channel minimum <min-value> maximum <max-value>'
 'limit-resource vlan minimum <min-value> maximum <max-value>'
N1KVE-VSM(config)# end
N1KVE-VSM#
N1KVE-VSM# show system vse feature level
Current feature level: 5.2(1)SV5(1.3)
N1KVE-VSM#
N1KVE-VSM# system update vse feature level
Current feature level is the only one compatible with the inserted VSEs
N1KVE-VSM#
N1KVE-VSM# module vse 3 execute vemcmd show feature level
VSE Feature Level: 5.2(1)SV5(1.3)
N1KVE-VSM#
```

Upgrading VMware ESXi Hosts

Refer to VMware documentation to upgrade VMware ESXi host from release 6.5 to 6.7. For more information, see https://www.vmware.com/support/pubs/