Upgrading Cisco Nexus 1000V

This chapter describes the prerequisites, guidelines and limitations, and the process to upgrade Cisco Nexus 1000V.

Prerequisites for Upgrading the VSM Software

Complete this section before upgrading the VSM software.

Before You Begin

- A pair of VSMs in an HA pair is required in order to support a nondisruptive upgrade.
- A system with a single VSM can only be upgraded in a disruptive manner.

The upgrade process is irrevocable. After the software is upgraded, you can downgrade by removing the current installation and reinstalling the software.

Prerequisites

Upgrading VSMs has the following prerequisites:

- Close any active configuration sessions before upgrading the Cisco Nexus 1000V software.
- Save all changes in the running configuration to the startup configuration.
- Save a backup copy of the running configuration in external storage.

Caution In Cisco Nexus 1000V for Microsoft Hyper-V Release 5.2(1)SM3(2.1), the VEM MSI cannot be installed on Windows Server 2012. Hence, you must update the operating system of the host to Windows Server 2016 before you upgrade to Cisco Nexus 1000V for Microsoft Hyper-V Release 5.2(1)SM3(2.1). The VEM software version 5.2(1)SM3(1.1c) can run on Windows server 2016 during upgrade path.

Licensing

Determine the edition of the Cisco Nexus 1000V by using the **show switch edition** command. Based on the edition, see the following sections:

- Essential Edition, page 2-2

Essential Edition

The upgrade to a current release is supported in the Essential edition. For more information, see the *Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide*.

Advanced Edition

If you are upgrading the Cisco Nexus 1000V software from Release 5.2(1)SM1(5.1) to the current release:

- Install the Cisco Nexus 1000V platform-specific licenses (evaluation or permanent) before you upgrade to the current release, or the upgrade might fail.
- Platform-specific licenses are checked in and the Cisco Nexus 1000V Multi-Hypervisor Licenses are checked out with the license socket count changed to 1024 and the evaluation period changed to 60 days after a successful VSM upgrade.

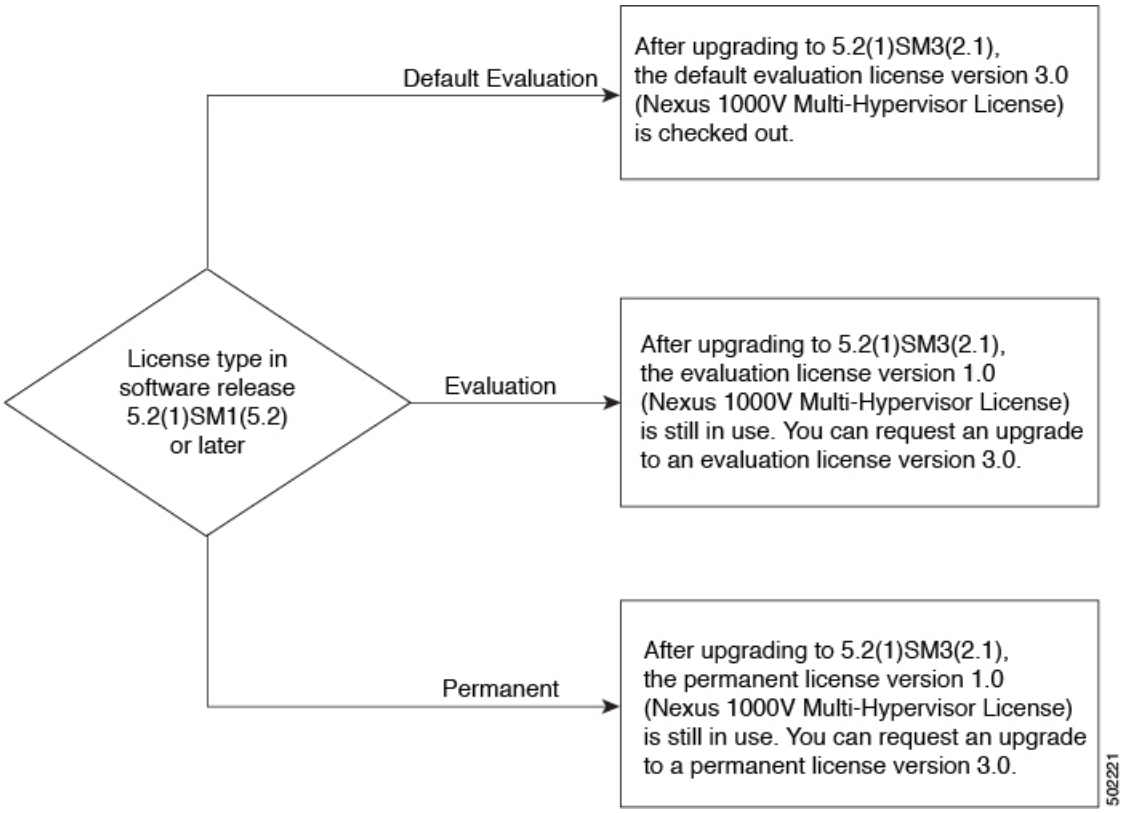
Licensing and Upgrade

If you are upgrading the software from Release 5.2(1)SM1(5.2) or later, see Figure 2-1 to check the license details after the upgrade.

Note For information on obtaining a replacement for the Cisco Nexus 1000V Multi-Hypervisor licenses, see "Rehosting a License on a Different VSM" in the *Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide.*

Note The license count is counted as one for each CPU socket.

Figure 2-1 Licensing and Upgrade



Prerequisites for Upgrading the VEM Software

Upgrading the VEM software has the following prerequisites:

1. The VSM and virtual switch extension manager (VSEM) need to be upgraded to the current release before you upgrade the VEM software.
   - To upgrade the VSM, see Upgrading the VSM to the Current Release, page 2-5.
   - To upgrade the VSEM, see Upgrading the Cisco VSEM to the Current Release, page 2-13.
2. You have already obtained a copy of the VEM software file.
3. You have Windows Server 2012 R2 or Windows Server 2016 hosts with Microsoft Hotfix KB3014795 applied. For more information, see http://support.microsoft.com/kb/3014795/en-us.
4. Ensure that the SCVMM version is higher or the same version as that of the host version. If not higher or the same, you cannot add the host of the SCVMM.

Upgrade Procedures

Table 2-1 lists the upgrade paths from the Cisco Nexus 1000V software releases.

Table 2-1 Upgrade Paths from Cisco Nexus 1000V Releases

If you are running this configuration	Follow these steps
Release 5.2(1)SM3(1.1) and later with the following: • SCVMM 2012 R2 UR4 and later • Windows Server 2012 R2 hosts	Upgrade workflow: • Preparing SCVMM and Windows Server Hosts • Upgrading the VSM to the Current Release • Upgrading the Cisco VSEM to the Current Release • Upgrading the VEM Software to the Current Release • Performing Post Upgrade Operations
• Release 5.2(1)SM1(5.2) and later with the following:SCVMM 2012 R2 UR4 and later – Upgrade to Release 5.2(1)SM3(1.1c) • Windows Server 2012 R2 hosts	
Release 5.2(1)SM1(5.2) and later with the following: • SCVMM 2012 R2 UR4 and later • Windows Server 2012 R2 hosts – Upgrade to Release 5.2(1)SM3(1.1c)	
Release 5.2(1)SM1(5.1) and later with the following: • SCVMM 2012 (SP1) UR3 and later • Windows Server 2012 hosts – Upgrade to Release 5.2(1)SM3(1.1c)	

Preparing SCVMM and Windows Server Hosts

Before you upgrade Cisco Nexus 1000V to Release 5.2(1)SM3(2.1), ensure that the Cisco Nexus 1000V software version is 5.2(1)SM3(1.1c) with minimum Windows set to 2012.

For example, see the following:

- If the SCVMM 2012 is installed, you must upgrade to SCVMM 2012 R2 UR4

  To upgrade to SCVMM 2012 R2 UR4 or SCVMM 2016, see Upgrading SCVMM 2012 SP1 to SCVMM 2012 R2 UR4, page 2-4.

If the target setup includes Windows Server 2012 or Windows Server 2016 host, you must uninstall VEM before you begin upgrading the SCVMM. To upgrade the host to the Windows Server, see Upgrading Windows Server 2012 R2 to Windows Server 2016, page 2-5.

Upgrading SCVMM 2012 SP1 to SCVMM 2012 R2 UR4

Refer to http://technet.microsoft.com/en-us/library/dn469609.aspx for additional details.

Preparing the Cisco Nexus 1000V

Step 1 Uninstall the existing Cisco Nexus 1000V VSEM provider.

Note The uninstallation restarts the SCVMM service.

Step 2 Reinstall the new Cisco Nexus 1000V VSEM provider.

Note The installation restarts the SCVMM service.

Step 3 Verify that the Cisco provider is installed correctly:

a. Open the SCVMM console.

b. Navigate to **Settings workspace**.

c. On the Settings pane, click **Configuration Providers**.

d. Verify that the **Cisco Systems Nexus 1000V extension** is displayed.

Step 4 Refresh the Cisco Nexus 1000V Extension Manager:

a. Open the SCVMM console.

b. Navigate to **Fabric workspace**. On the **Fabric** pane, expand **Networking**, and click **Switch Extension Manager**. If the SCVMM version is 2012 R2, click **Network Service** instead of **Switch Extension Manager**.

c. In the results pane, right-click **Cisco Systems Nexus 1000V extension** and choose **Refresh**.

Upgrading Windows Server 2012 R2 to Windows Server 2016

Microsoft does not support an upgrade of the third-party extension—for example, Cisco Nexus 1000V VEM, while upgrading Windows Server 2012 to Windows Server 2012 R2. Therefore, you must uninstall Cisco Nexus 1000V VEM before upgrading the host. Later, add the upgraded host to the logical switch after upgrading VSM and VSEM to the current release.

Refer to http://technet.microsoft.com/en-us/library/dn303416.aspx for additional details.

Upgrading the VSM to the Current Release

For prerequisites to upgrade the VSM, see Prerequisites for Upgrading the VSM Software, page 2-1. This section includes the following topics:

Software Images

The software image install procedure depends 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 1000V software prompt.
- Image version—Each image file has a version.
- Disk—The bootflash: resides on the VSM.

In-Service Software Upgrades on Systems with Dual VSMs

Note Performing an In-Service Software Upgrade (ISSU) from Cisco Nexus 1000V Release 5.2(1)SM1(5.1) to the current release of Cisco Nexus 1000V using ISO files is not supported. You must use the kickstart and system files to perform an ISSU upgrade to the current release of Cisco Nexus 1000V.

The Cisco Nexus 1000V 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 1000V 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.

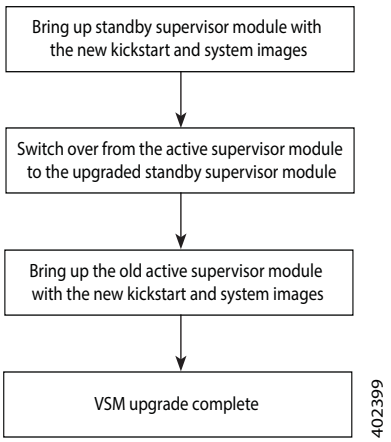
An ISSU updates the following images:

- Kickstart image
- System image

ISSU Process for the Cisco Nexus 1000V

Figure 2-2 displays the ISSU process.

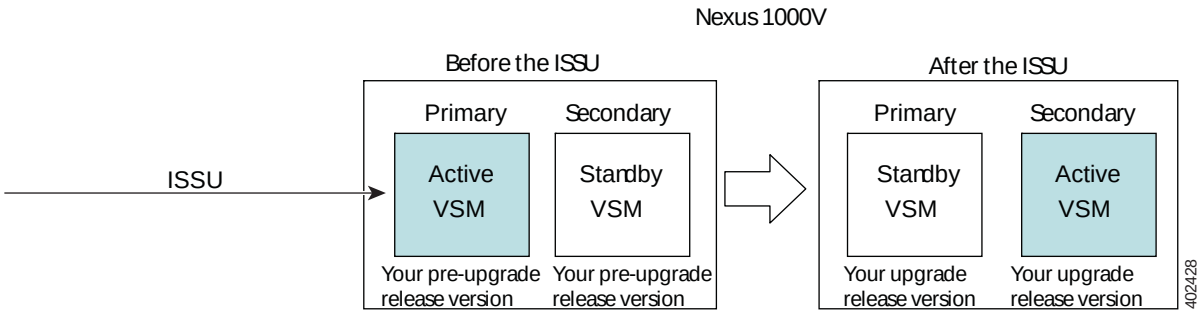
Figure 2-2 ISSU Process



ISSU VSM Switchover

Figure 2-3 provides an example of the VSM status before and after an ISSU switchover.

Figure 2-3 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.
- Sets the kickstart and system boot variables.
- Reloads the standby VSM with the new Cisco Nexus 1000V 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 VSMs Using Kickstart and System Images

Depending on the redundancy status of the VSM, the upgrade procedure differs. The redundancy status of VSM can be determined by the **show system redundancy status** command.

Upgrading VSMs in an HA Pair

To upgrade the VSMs in an HA pair using the ISSU process, perform the following steps:

Step 1 Choose and download the Cisco Nexus 1000V zip file and extract the kickstart and system software files to a server.

Step 2 Log in to the active VSM.

Step 3 Ensure that the required space is available for the image file(s) to be copied.

```
switch# dir bootflash:
...
Usage for bootflash://
485830656 bytes used
1109045248 bytes free
1594875904 bytes total
```

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

Step 4 Verify that there is space available on the standby VSM by entering the **dir bootflash://sup-standby/** command.

Step 5 Verify that there is space available on the standby VSM.

```
switch# dir bootflash://sup-standby/
...
Usage for bootflash://
485830656 bytes used
1109045248 bytes free
1594875904 bytes total
```

Step 6 Delete any unnecessary files to make space available if you need more space on the standby VSM.

Step 7 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V kickstart and system images 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 tftp:.

```
switch# copy tftp://10.106.196.163/n1000vh-dk9.5.2.1.SM3.2.1.bin
bootflash:n1000vh-dk9.5.2.1.SM3.2.1.bin
switch# copy tftp://10.106.196.163/n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin
bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin
```

Step 8 Verify the ISSU upgrade for the **kickstart** and **system** images

```
switch# show install all impact kickstart
bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin system
bootflash:n1000vh-dk9.5.2.1.SM3.2.1.bin
```

Step 9 Determine if the Cisco PNSC is configured in the deployment using the **show nsc-pa status** command.

```
VSM# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1c)-vsm
```

Note If the VSM version is 5.2(1)SM1(5.1), use the command **show vnm-pa status** instead of **show nsc-pa status**.

Note If the output shows a successful installation, the Cisco VSG is configured. You must follow the upgrade procedure in the *Cisco VSG for Microsoft Hyper-V, Release 5.2(1)VSG2(1.2b) and Cisco Prime NSC, Release 3.4 Installation and Upgrade Guide* and later continue to next step. If the output shows that the policy agent did not install, continue to next step.

Step 10 Save the running configuration to startup configuration, bootflash:, and to an external location.

a. Save the running configuration to a startup configuration using **copy running-config startup-config**.

b. Save the running configuration to bootflash: using **copy running-config bootflash:run-cfg-backup**.

c. Save the running configuration to external location using **copy running-config tftp://external_backup_location**.

Step 11 Perform the upgrade on the active VSM by using the following command:

```
switch# install all kickstart bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin system
bootflash:n1000vh-dk9.5.2.1.SM3.2.1.bin
```

Step 12 Continue with the installation by pressing **Y**.

Note If you press N, the installation exits gracefully.

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

Step 13 After the installation operation completes, log in and verify that the switch is running the required software version by using the **show version** and the s**how module** commands.

Step 14 Copy the running configuration to the startup configuration by using the **copy running-config startup-config** command.

Step 15 Display the log for the last installation by entering the following commands.

```
switch# show install all status
switch# attach module <module_number>
switch# show install all status
```

Note If the command **show install all** status does not exit automatically while the installation is in progress, use Ctrl+C to exit.

Upgrading a Standalone VSM

The system with a single/standalone VSM can only be upgraded in a disruptive manner using the **install all** command.

To upgrade the standalone VSM, perform the following steps:

Step 1 Choose and download the Cisco Nexus 1000V zip file and extract the kickstart and system software files to a server. For more information, see Downloading the Cisco Nexus 1000V Package, page 1-6.

Step 2 Log in to the VSM.

Step 3 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V kickstart and system images to the active VSM by using a transfer protocol. You can use ftp, tftp, scp, or sftp. The examples in this procedure copy a kickstart and system image using tftp.

```
switch# copy tftp://10.106.196.163/n1000vh-dk9.5.2.1.SM3.2.1.bin
bootflash:n1000vh-dk9.5.2.1.SM3.2.1.bin
switch# copy tftp://10.106.196.163/n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin
bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin
```

Step 4 Determine the VSM status using the **show system redundancy status** command.

Step 5 Verify the ISSU upgrade for the **kickstart** and **system** images.

```
switch# show install all impact kickstart
bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin system
bootflash:n1000vh-dk9.5.2.1.SM3.2.1.bin
```

Step 6 Determine if the Cisco VSG is configured in the deployment using the **show nsc-pa status** command.

```
VSM# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1c)-vsm
```

Note If the VSM version is 5.2(1)SM1(5.1), use the command **show vnm-pa status** instead of **show nsc-pa status**.

Note If the output shows a successful installation, the Cisco VSG is configured. You must follow the upgrade procedure in the *Cisco VSG for Microsoft Hyper-V, Release 5.2(1)VSG2(1.2b) and Cisco Prime NSC, Release 3.4 Installation and Upgrade Guide* and later continue to next step. If the output shows that the policy agent did not install, continue to next step.

Step 7 Save the running configuration to startup configuration, bootflash:, and to an external location.

a. Save the running configuration to a startup configuration using **copy running-config startup-config** command.

b. Save the running configuration to bootflash: using the **copy running-config bootflash:run-cfg-backup** command.

c. Save the running configuration to external location using the **copy running-config tftp://external_backup_location** command.

Step 8 Perform the upgrade on the standalone VSM using the following command:

```
switch# install all kickstart bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.2.1.bin system
bootflash:n1000vh-dk9.5.2.1.SM3.2.1.bin
```

Step 9 Continue with the installation by pressing **Y**.

Note If you press N, the installation exits gracefully.

Step 10 After the installation operation completes, log in and verify that the switch is running the required software version by using the **show version** and the **show module** command.

Step 11 Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

Step 12 Enter the following commands to display the log of the previous installation:

```
switch# show install all status
switch# attach module <module_number>
switch# show install all status
```

Note If the command **show install all status** does not exit automatically while the installation is in progress, use Ctrl+C to exit.

Reregistering the Policy Agent of the Upgraded VSM

This section applies only if the VSG is configured in deployment. To determine whether VSG is deployed, run the command **show nsc-pa status**.

```
switch# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1a)-vsm
```

Note If the VSM version is 5.2(1)SM1(5.1), use the command **show vnm-pa status** instead of **show nsc-pa status**.

If the output displays a successful installation, you must reregister the policy agent after upgrading the Cisco VSM.

Step 1 Log in to the active VSM.

Step 2 Check the current policy agent version.

```
switch# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1a)-vsm
```

Step 3 Copy the PNSC-PA file to bootflash.

```
switch# copy tftp://10.106.196.163/vsmhv-pa.3.2.1e.bin bootflash:vsmhv-pa.3.2.1e.bin
```

Note Determine the file version from the filename and if it is a higher version than the currently installed version, proceed to next step.

Step 4 Enter the configuration mode.

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#
```

Step 5 Unregister the old policy agent from VSG.

```
switch(config)# nsc-policy-agent
switch(config-nsc-policy-agent)# no policy-agent-image
```

Step 6 Register the new policy agent.

```
switch(config-nsc-policy-agent)# policy-agent-image bootflash: vsmhv-pa.3.2.1e.bin
switch(config-nsc-policy-agent)# exit
switch(config)#
```

Step 7 Copy the current running configuration to the startup configuration.

```
switch(config)# copy running startup
[########################################] 100%
```

Step 8 Verify the updated policy agent version.

```
switch(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1e)-vsm
switch(config)#
```

Refreshing Network Service and Remediate a Logical Switch

After the VSM is upgraded, you must refresh the network service and remediate the logical switch on the SCVMM so that the VSM version is displayed in the VEM.

To refresh the network service, perform the following steps:

Step 1 Launch the SCVMM console.

Step 2 In the SCVMM user interface, navigate to **Fabric > Network Service > <*network_service_name*>** and right-click **Refresh**.

In the **Jobs** section, verify that the refresh is successful.

To remediate the logical switch, perform the following steps:

Step 1 Navigate to the **Fabric** workspace. On the **Fabric** pane, expand **Networking** and select **Logical Switches**.

Step 2 In the **Home** tab, select **Hosts**.

Step 3 Select the corresponding host and select the Cisco Nexus 1000V on the same host.

Step 4 Right-click the switch and select **Remediate**.

In the **Jobs** section, verify that the remediate is successful

Step 5 Enter the *vemcmd show version* command in the VEM to verify if the new version of the VSM is displayed.

Upgrading the Cisco VSEM to the Current Release

This section describes the procedure for upgrading the Cisco VSEM Provider MSI package on the SCVMM server.

To upgrade the Cisco VSEM, perform the following steps:

Step 1 Install the Nexus1000V-NetworkServiceProvider-5.2.1.SM3.2.1.0.msi from the Cisco Nexus1000V zip location on the SCVMM Server.

The installation restarts the SCVMM service.

- After a successful installation, it places the PowerShell scripts that are used to upgrade the Cisco VSEM in the following folder of the SCVMM server: **%ProgramFiles%\Cisco\Nexus1000V\V2\Scripts\ProviderUpgrade**. For example, C:\Program Files\Cisco\Nexus1000V\V2\Scripts\ProviderUpgrade.
- The powershell scripts needed to upgrade VEM are placed in **%ProgramFiles%\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade** on the SCVMM server. For example, C:\Program Files\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade.

Step 2 Verify that the Cisco VSEM provider is installed correctly:

a. Open the SCVMM console.

b. Navigate to **Settings workspace**.

c. On the **Settings** pane, click **Configuration Providers**.

d. Verify that the **Cisco Systems Nexus 1000V - version 2** extension is displayed.

Step 3 Execute the Upgrade-Nexus1000V-Provider.ps1 script to upgrade the Cisco VSEM. On the SCVMM server, the script is located at %ProgramFiles%\Cisco\Nexus1000V\V2\Scripts\ProviderUpgrade. For example, C:\Program Files\Cisco\Nexus1000V\V2\Scripts\ProviderUpgrade. It requires the following inputs as parameters:

- IP address for the Cisco Nexus 1000V VSM
- Username for the Cisco Nexus 1000V VSM
- Password for the Cisco Nexus 1000V VSM

Below is a sample snapshot of the VEM upgrade script:

```
PS C:\Program Files\Cisco\Nexus1000V\V2\Scripts\ProviderUpgrade>
.\Upgrade-Nexus1000V-Provider.ps1
Enter IP Address for the Nexus1000V VSM: 10.105.225.123
Enter Username for the Nexus1000V VSM: admin
Enter Password for the Nexus1000V VSM:
Found the NetworkService vsem connected to the VSM 10.105.225.123
The NetworkService model: Nexus 1000V Chassis
The NetworkService is linked to the old provider. Start upgrading...
Upgrade the provider for the NetworkService: vsem
Upgrade completed
Performing VSEM Refresh with extension ip ==> '10.105.225.123'
```

```
-----------------------------------------------------
Retrieve Cisco Extension with IP = 10.105.225.123
-----------------------------------------------------
Cisco Switch Extension Manager with ip '10.105.225.123' is detected on this VMM server.
Reading Cisco Switch Extension Manager now...
This may take a while depending on VSM configuration Size...
Saving the configs  of VSM ==> '10.105.225.123'
Upgrade Script Execution Complete
```

Step 4 Verify that the Cisco VSEM provider is upgraded correctly:

a. Open the SCVMM console.

b. Navigate to the **Fabric** workspace. On the **Fabric** pane, expand **Networking**, and click **Network Service**.

c. In the **Results** pane, click the corresponding **Cisco Systems Nexus 1000V extension** and verify that **Cisco Systems Nexus 1000V – Version 2** is displayed in the **Provider** column.

Step 5 Refresh the Cisco Nexus 1000V Extension Manager:

a. Open the SCVMM console.

b. Navigate to the **Fabric** workspace. On the **Fabric** pane, expand **Networking**, and click **Network Services**.

c. In the **Results** pane, right-click **Cisco Systems Nexus 1000V extension** and choose **Refresh**.

Step 6 Install CiscoVmmService which runs as a Windows service.

The MSI file (*Nexus1000V-NetworkServiceProvider-5.2.1.SM3.2.1.0.msi)* also contains **CiscoVmmService** which is required for the automatic refresh of the network service and remediate at SCVMM. The files are located at the **%ProgramFiles%\Cisco\Nexus1000V\V2\CiscoVmmService** directory. For more information, see Installation of CiscoVmmService, page 1-22.

Note that the CiscoVmmService is supported only from Release 5.2(1)SM3(2.1) and later.

Upgrading the VEM Software to the Current Release

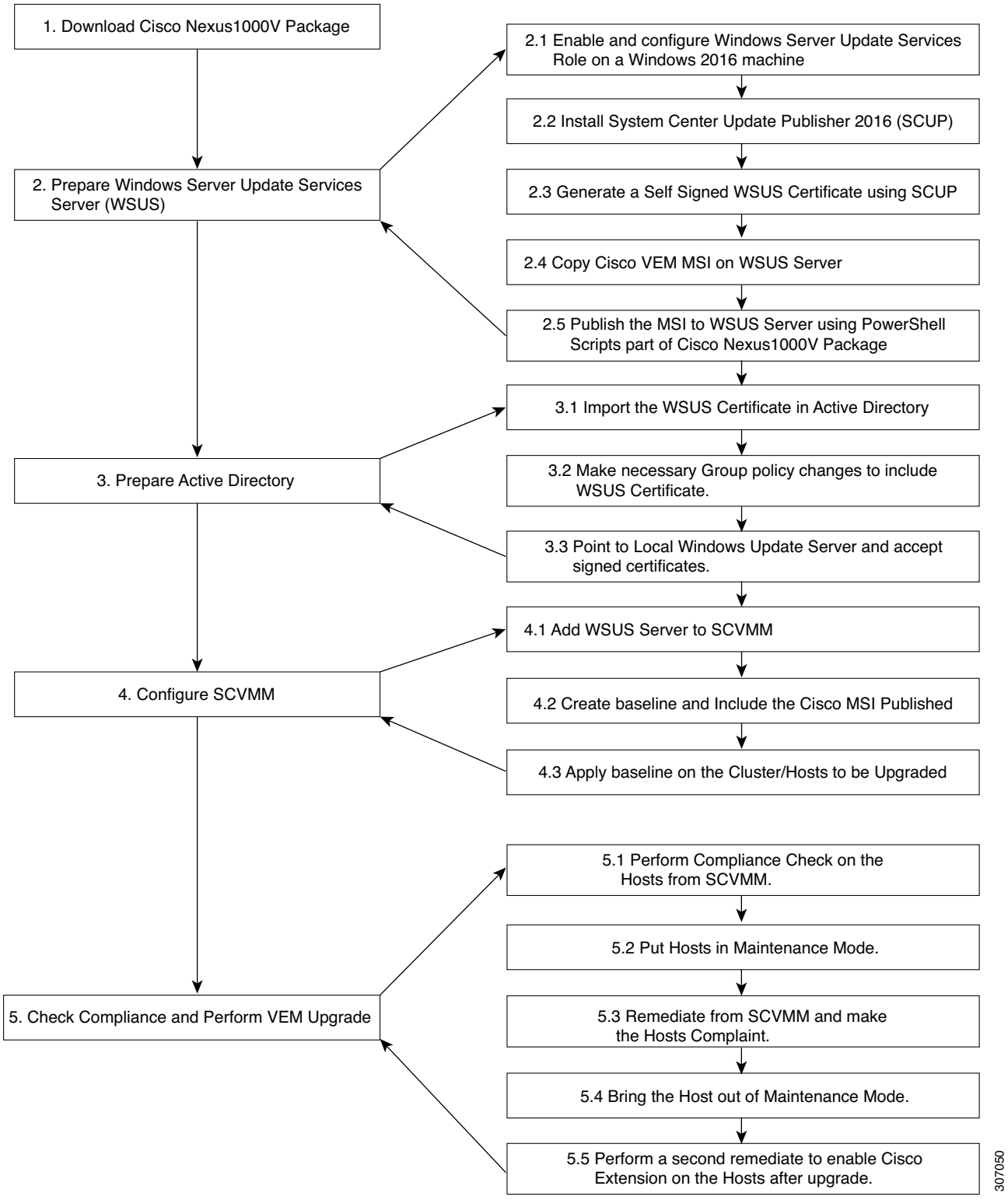
For prerequisites to upgrade the VEM, see Prerequisites for Upgrading the VEM Software, page 2-3. You must complete the following procedures before upgrading the VEM software:

- Upgrade the VSM—see Upgrading the VSM to the Current Release, page 2-5.
- Upgrade the VSEM—see Upgrading the Cisco VSEM to the Current Release, page 2-13.

Upgrade Workflow

Figure 2-4 displays the VEM upgrade workflow using the WSUS server.

Figure 2-4 Cisco Nexus 1000V VEM Upgrade Workflow



Upgrading the VEM Software Using WSUS Server

Summary Steps

1. Downloading the Cisco Nexus 1000V package, page 2-16.
2. Preparing the Windows Server Update Services (WSUS) Server, page 2-16.
3. Preparing the Active Directory, page 2-17.
4. Configuring SCVMM, page 2-18.
5. Checking Compliance and Performing the VEM Upgrade, page 2-19.

Downloading the Cisco Nexus 1000V package

See Downloading the Cisco Nexus 1000V Package, page 1-6.

Preparing the Windows Server Update Services (WSUS) Server

To prepare the WSUS, perform the following steps:

Step 1 Enable and configure the WSUS role on a Windows Server 2016 machine.

For more information, see http://technet.microsoft.com/en-us/library/hh852340.aspx.

Step 2 Install the System Center Update Publisher 2011 (SCUP) version 6.0.283.0 on the WSUS server.

For more information, see https://www.microsoft.com/en-us/download/details.aspx?id=55543.

Step 3 Generate a self-signed WSUS certificate via the SCUP:

a. Run the SCUP as a network administrator.
b. Click the **Options** icon in the upper left corner and then click **Options**.
c. Check the **Enable publishing to an update server** check box for Updates Publisher 2011 to publish all software updates.
d. Click the **Connect to a local update server** radio button as the SCUP was installed locally on the WSUS server.
e. Click **Test Connection** to validate that the WSUS server name and the port settings are valid.
f. If the connection succeeded, click **Create**. This creates a new certificate.
g. In the **Test Connection** dialog box, click **OK**.
h. In the **System Center Updates Publisher Options** dialog box, click **OK**.

Step 4 Configure the certificate store on the WSUS server using the following steps:

For more information, see http://technet.microsoft.com/en-us/library/hh134732.aspx.

a. On the WSUS server, click **Start**, click **Run**, and then enter **MMC** in the text box.
b. Click **OK** to open the Microsoft Management Console (MMC).
c. Click **File** and then click **Add/Remove Snap-in**.
d. In the **Add or Remove Snap-ins** dialog box, select **Certificates** and click **Add**.
e. In the **Certificates snap-in** dialog box, select **Computer account** and click **Next**.
f. Click the **Local computer radio** button and click **Finish**.

g. Click **OK** on the **Add or Remove Snap-ins** dialog box.

h. On MMC, expand **Certificates (Local Computer)**, expand **WSUS**, and click **Certificates**.

i. In the results pane, right-click the desired certificate, click **All Tasks**, and click **Export**.

j. In the **Certificate Export** wizard, use the default settings to create an export file with the name and location specified in the wizard.

k. Right-click **Trusted Publishers**, click **All Tasks**, and click **Import**. Complete the **Certificate Import** wizard using the exported file from step j.

l. Right-click **Trusted Root Certification Authorities**, click **All Tasks**, and click **Import**. Complete the **Certificate Import** wizard using the exported file from step j.

Step 5 Copy the VEM MSI file to the local directory on the WSUS server.

Step 6 Publish the VEM MSI file to the WSUS server using the provided PowerShell script.

```
PS C: .\Get-CiscoUpdates.ps1
Script to retrive Cisco Products installed in WSUS Server.
1 packages found in WSUS Server.
-----------------------------------------------------
Company : Cisco Systems, Inc.
Product : Cisco-Nexus1000V
Title : Cisco Nexus 1000V Series Switch [MSI: 3.00.400] [Driver: 302.100.0.0]
GUID : 70fa6867-ba86-48b5-bfe6-ad0462f9c131
Description : [PC: {C999F283-0B3B-495F-85AE-F3F205E08F9E}] [UC:
{D1099B98-17BE-40F2-A10E-29D48B9A5829}] \n
Creation Date : 11/1/2018 4:03:41 AM
Arrival Date : 11/1/2018 4:03:44 AM
version : Nexus1000V-VEM-5.2.1.SM3.2.1.0
```

Step 7 Verify that the MSI published correctly using the following script:

```
PS C:> Get-CiscoUpdate.ps1

    Script to retrieve Cisco Products installed in WSUS Server.
    1 packages found in WSUS Server.
    -----------------------------------------------------
    Company : Cisco Systems, Inc.
    Product : Cisco-Nexus1000V
    Title : Cisco Nexus 1000V Series Switch [MSI: 3.00.000] [Driver: 301.100.0.0]
    GUID : 9b0c5728-debe-4223-960f-8511e7cc7f19
    Description : [PC: {1C17F17E-34F5-4E6B-901C-FA229EB367E4}] [UC:
    {D1099B98-17BE-40F2-A10E-29D48B9A5829}] \n
    Creation Date : 12/10/2014 11:06:09 AM
    Arrival Date : 12/10/2014 11:06:12 AM
    -----------------------------------------------------
```

Preparing the Active Directory

Step 1 Copy the previously exported certificate that was exported earlier (see step 4j) to the local directory of the active directory (AD) server.

Step 2 On the AD server, click the **Tools** tab of the **Server Manager**, and select **Group Policy Management**.

Step 3 Do the following to create a new Group Policy Object:

a. In the console tree, navigate to **<Forest name>/Domains/<Domain name>/Group Policy Objects** and right-click to select **New**.

b. In the New GPO dialog box, enter a name for the new GPO, and click **OK**.

c. To link the newly created GPO, navigate to **<Forest name>/Domains/<Domain name>** and select **Link and Existing GPO**.

d. From the results pane of the Group Policy Objects in the **Select GPO** dialog box, select the **GPO**, and click **OK**.

Step 4 Navigate to the newly created GPO in **<Forest name>/Domains/<Domain name>** and right-click to select **Edit** to open a policy in tje Group Policy Management Editor. Modify the following settings:

a. Windows Update Group Policy settings:

Navigate to **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update** location and modify the following settings for:

1. Specify intranet Microsoft update service location:

– Select **Specify intranet Microsoft update service** location and right-click to select **Edit**. Click the **Enabled** radio button. Navigate to **Options>Set the intranet update service for detecting updates and Options>Set the intranet statistics server** and enter the location of local update server; for example, http://wsus-2016. Click **Apply** and click **OK**.

2. Allow signed updates from an intranet Microsoft update service location:

– Select **Allow signed updates from an intranet Microsoft update service location** and right-click to select **Edit**. Click the **Enabled** radio button. Click **Apply** and click **OK**.

b. Public Key Policies Group Policy settings:

Deploy the **WSUS Publishers Self-signed** certificate to **Trusted Publishers** and **Trusted Root Certification Authorities certificate** stores of **Public Key Policies** of the newly created GPO.

1. On the AD server, using the **Group Policy Management Editor**, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key policies** of the newly created GPO.

2. Right-click **Trusted Publishers**, click **All Tasks**, and click **Import**. Complete the **Certificate Import** wizard using the file from Step 1.

3. Right-click **Trusted Root Certification Authorities**, click **All Tasks**, and click **Import**. Complete the **Certificate Import** wizard using the file from Step 1.

Step 5 Identify the hosts on which the VEM upgrade is needed and enter the **gpupdate** command using an elevated command prompt. This applies the group policy settings to the hosts immediately.

Configuring SCVMM

Step 1 Add the WSUS server to the VMM:

a. On the VMM console, in the **Fabric** workspace, choose the **Home** tab. Click **Add Resources** and click **Update Server**.

b. In the **Add Windows Server Update Services Server** dialog box, enter the name of the Update server in the **Computer name** field. Specify the WSUS TCP/IP port in the **TCP/IP port** field. The default value is 8530.

c. Use or create a **Run As account** that has administrative rights on the WSUS server.

d. In the **Add Windows Server Update Services Server** dialog wizard, select **Add**.

Step 2 Create a new baseline for the Cisco Nexus 1000V:

a. In the Library workspace, on the Library pane, expand **Update Catalog and Baselines** and right-click **Update Baselines** to select **Create Baseline**.

b. In **Update Baseline** wizard, select the **General** tab to enter a name and description for the baseline.

c. Click **Next** to move to the Updates tab. Click **Add**. Search for the string “Cisco” to select an update for the Cisco Nexus 1000V.

d. Click **Next** to move to the Assignment Scope tab and select infrastructure servers to add to the baseline.

e. Click **Next** and then **Finish**.

Checking Compliance and Performing the VEM Upgrade

Step 1 Navigate to **Host > Launch Hyperv Manager > select Virtual Switch Manager**. Click **Logical Switch** and then click **Extension**. Uncheck the Cisco Nexus 1000v Series switch.

Note Step 1 is only applicable for the Windows 2016 hosts.

Step 2 Scan servers to check compliance with the previously created baseline for the Cisco Nexus 1000V:

a. In the **Fabric** workspace, on the **Fabric** pane, expand **Servers**.

b. Select the **Home** tab and click **Compliance**.

c. From the Compliance view, select the host to scan.

d. Right-click the host and select **Scan**.

After the scan is complete, identify the hosts that are noncompliant.

Step 3 Put the non-compliant host to maintenance mode and perform remediation:

a. Put the non-compliant host in maintenance mode by referring to the following link:

http://technet.microsoft.com/en-us/library/hh882398.aspx

b. In the **Fabric** workspace, on the **Fabric** pane, expand **Servers**.

c. Select the **Home** tab and click **Compliance**.

d. From the Compliance view, select the host to remediate.

e. Right-click the host and select **Remediate**.

f. In the **Update remediation wizard**, check the **Do not restart servers after remediation** check box.

g. Click **Remediate**.

Step 4 Bring the host out of maintenance mode. See http://technet.microsoft.com/en-us/library/hh882398.aspx.

Step 5 Perform another remediation to bring the host online in VSM:

a. Navigate to the **Fabric** workspace. On the **Fabric** pane, expand **Networking** and select **Logical Switches**.

b. In the **Home** tab, select **Hosts**.

c. Select the corresponding host and select the Cisco Nexus 1000V on the same host.

d. Right-click the switch and select **Remediate**.

Step 6 Use the **show module** command in VSM to verify whether the VEM modules were upgraded. After the upgrade, the software version of the corresponding VEM in the **show module** output should be 5.2(1)SM3(2.1).

This completes the upgrade process for the Cisco Nexus 1000V.

Upgrading the VEM Software Using a Script

Step 5 of Upgrade Workflow, page 2-14 is performed by this script.

Note Steps 1 to 4 of Upgrade Workflow, page 2-14 must be done manually.

Prerequisites

Execute the script from the PowerShell console of the SCVMM server. Additionally, complete the following prerequisites before running the script:

- Add the Windows Update server to the SCVMM.
- Create the upgrade baselines.
- Verify that the Cisco Nexus 1000V baseline has only one upgrade.

Running the VEM Upgrade Script

On the SCVMM server, the Upgrade-Nexus1000V-VEM.ps1 script is located at %Program Files%\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade. For example, C:\Program Files\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade.

The script requires the following inputs as parameters:

- Baseline name
- Cluster name
- Logical switch name

Note For Windows 2016 hosts, navigate to **Host > Launch Hyperv Manager > select Virtual Switch Manager**. Click **Logical Switch** and then click **Extension**. Uncheck the Cisco Nexus 1000v Series switch.

Below is a sample snapshot of the VEM upgrade script:

```
**********************
Windows PowerShell transcript start
Start time: 20181024222117
Username: N1KQA\administrator
RunAs User: N1KQA\administrator
Machine: 2016 (Microsoft Windows NT 10.0.14393.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoExit
-Command $ep = Get-ExecutionPolicy; if ( $ep -eq
([Microsoft.PowerShell.ExecutionPolicy]::Restricted) ) { Set-ExecutionPolicy
```

```
RemoteSigned -Scope Process -Force } Import-Module 'C:\Program Files\Microsoft System
Center 2016\Virtual Machine
Manager\Bin\psModules\virtualmachinemanager\virtualmachinemanager.psd1'; cd $home;
$host.UI.RawUI.WindowTitle = 'Windows PowerShell - Virtual Machine
Manager';$credential = Get-Credential;$vmmserver_VAR=Get-SCVMMServer 2016.n1kqa.com
-UserRoleName 'Administrator' -Credential $credential;
Process ID: 7820
PSVersion: 5.1.14393.2515
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.2515
BuildVersion: 10.0.14393.2515
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
Transcript started, output file is C:\Program
Files\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade\Upgrade-Nexus1000V-VEM-logs\Upgrade-Nexus
1000V-VEM-10-24-18_10-17.log
C:\Program
Files\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade\Upgrade-Nexus1000V-VEM-logs\Upgrade-Nexus
1000V-VEM-10-24-18_10-17.log
################################################################################
## SCRIPT NAME: Upgrade-Nexus1000V-VEM.ps1 ##
## VERSION: 1.1 ##
## DESCRIPTION: This script is applicable to all releases . ##
## ##
## =============== ##
## PREREQUISITES: ##
## =============== ##
## 1: WINDOWS UPDATE SERVER SHOULD ALREADY BE ADDED to SCVMM. ##
## 2: UPGRADE BASELINES SHOULD BE PRE-CREATED. ##
## 3: NEXUS1000V BASELINE SHOULD HAVE ONLY ONE UPGRADE. ##
################################################################################

Importing Virtual Machine Manager Libraries ..
-----------------------------------------------------
Fetching Baseline Info for Baseline - 'bld-255'
-----------------------------------------------------
Update 1 => Cisco Nexus 1000V Series Switch [MSI: 3.00.400] [Driver: 302.100.0000.0]

-------------------------------------------------------------------------------------
-----------
Starting Compliance Scan on Cluster before Upgrade 'cluster' with baseline 'bld-255'
-------------------------------------------------------------------------------------
-----------
HOSTNAME = hyperv-109 : STATUS = NonCompliant : Nexus1000V Version = 3.00.300
HOSTNAME = hypev-108 : STATUS = NonCompliant : Nexus1000V Version = 3.00.300

-------------------------------------------------------------------------------
STARTING UPGRADE ON HOST: hyperv-109
-------------------------------------------------------------------------------
STEP 1.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster

If you proceed with this operation, above listed VM's will be put to 'saved' state .


STEP 1.2 : Starting Update Remediation

STEP 1.3 : Stopping Maintenance Mode

-------------------------------------------------------------------------------
STARTING UPGRADE ON HOST: hypev-108
-------------------------------------------------------------------------------
```

```
STEP 2.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster


If you proceed with this operation, above listed VM's will be put to 'saved' state .


STEP 2.2 : Starting Update Remediation

STEP 2.3 : Stopping Maintenance Mode

--------------------------------------------------------------------------------
-----------
Starting Compliance Scan on Cluster after Upgrade 'cluster' with baseline 'bld-255'
--------------------------------------------------------------------------------
-----------
HOSTNAME = hyperv-109 : STATUS = Compliant : Nexus1000V Version = 3.00.400
HOSTNAME = hypev-108 : STATUS = Compliant : Nexus1000V Version = 3.00.400

------------------------------
Nexus1000V VEM Upgrade Complete
------------------------------
**********************
Windows PowerShell transcript end
End time: 20181024222750
**********************
```

Verify whether the VEM modules were upgraded using the **show module** command in VSM. After the upgrade, the software version in the **show module** output should be 5.2(1)SM3(2.1).

Upgrading the VEM Software Manually from Cisco Nexus 1000V Release 5.2(1)SM1(5.2) or Later to Release 5.2(1)SM3(2.1)

Step 1 Navigate to **Host > Launch Hyperv Manager > select Virtual Switch Manager**. Click **Logical Switch** and then click **Extension**. Uncheck the Cisco Nexus 1000v Series switch.

Note Step 1 is only applicable for the Windows 2016 hosts.

Step 2 Put the Windows Server host in maintenance mode. See http://technet.microsoft.com/en-us/library/hh882398.aspx.

Step 3 Copy the VEM MSI file (for example, Nexus1000V-VEM-5.2.1.SM3.2.1.0.msi) to the host.

Step 4 Run the MSI file to install.

Step 5 Remediate the host to make it available online in VSM:

a. Launch the SCVMM.

b. Navigate to the **Fabric** workspace. On the **Fabric** pane, expand **Networking** and select **Logical Switches**.

c. In the **Home** tab, click **Hosts** to list all hosts configured on the server.

d. Navigate to the host where you installed the MSI. Select the Cisco Nexus 1000V on the same host and right-click it.

e. Choose **Remediate** to make it online in VSM.

Note If the switch status is compliant, the **Remediate** option is not available. Refresh the corresponding host from the SCVMM console to get the **Remediate** option.

Step 6 Bring the host out of maintenance mode. See http://technet.microsoft.com/en-us/library/hh882398.aspx.

Step 7 Verify that the VEM module on the corresponding host is upgraded using the **show module** command in VSM. After the upgrade, the software version in the **show module** output should be 5.2(1)SM3(2.1).

Performing Post Upgrade Operations

This section contains:

Changing the Feature Support Level

After all VEMs are upgraded, complete the following procedure so the VSM can support all of the new features in the new software version.

Prerequisites

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- After an upgrade, the VSM default is to support only features in the previous software version. Features added in the new software version are only supported and functional after the network administrator explicitly upgrades the feature support level. This procedure upgrades the feature support level.
- Before upgrading the feature support level, all VEMs in the VSM domain must be upgraded to the new software version.
- After the VSM feature support level is upgraded, VEMs with other software versions are not allowed to connect with the VSM.
- After the VSM feature support level is upgraded, it cannot be downgraded.

Changing the Feature Level Support

Step 1 Display the current level of feature support using the command **show system vem feature level**. For example:

```
n1000v# show system vem feature level
current feature level: 5.2(1)SM3(1.1c)
n1000v#
```

Step 2 Display the current VEM feature and the version of the VEMs using the command **system update vem feature level**. For example:

```
n1000v# system update vem feature level
Feature      Version
Level        String
--------------------
1            5.2(1)SM3(1.1c)
2            5.2(1)SM3(2.1)
```

Note If all VEMs are upgraded to the new software version, the feature support can be upgraded to the new software version. If an instance of VEM is running an earlier software version, the feature support level cannot be upgraded, and the list is empty.

Step 3 Change the feature level using the command **system update vem feature level** *level_number*. For example:

```
n1000v# System update vem feature level 2
```

Note After the feature-level upgrade, VEMs with versions older than the feature level can no longer connect to the VSM.

Step 4 Display the updated level of feature support using the command **show system vem feature level**. For example:

```
n1000v# show system vem feature level
current feature level: 5.2(1)SM3(2.1)
n1000v#
```

Installing the Windows Patch

Install Microsoft hotfix KB3014795 on Windows Server 2012 R2 UR4 or Windows Server 2016 hosts. For more information, see http://support.microsoft.com/kb/3014795/en-us.