
# Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V

This chapter includes the following sections:



# Prerequisites for Upgrading the VSM Software

This section includes the following sections:



## Before You Begin

- A pair of VSMs in a high availability (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.
- Perform a VSM backup. For more information, see the *Configuring VSM Backup and Recovery* chapter in the *Cisco Nexus 1000V System Management Configuration Guide, Release 5.2(1)SM1(5.2)*.

## Licensing

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

- Advanced Edition, page 2-2
- Essential Edition, page 2-2
- Licensing and Upgrade, page 2-3

### Advanced Edition

- Install the Nexus1000V Multi-Hypervisor based licenses (evaluation or permanent) before you upgrade to the current release.
- If an upgrade is performed with a default license, the upgrade will fail.
- Platform-specific licenses are checked in and the Nexus1000V Multi-Hypervisor Licenses are checked out after a VSM upgrade.
- After a successful upgrade, the License Socket count is changed to 1024 with the evaluation period changed to 60 days.

### Essential Edition

- The upgrade to a current release is supported in the Essential edition with a default license.
- After a successful upgrade, the license socket count is changed to 1024 and the evaluation period is changed to 60 days.

For more information, see the *Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide*.

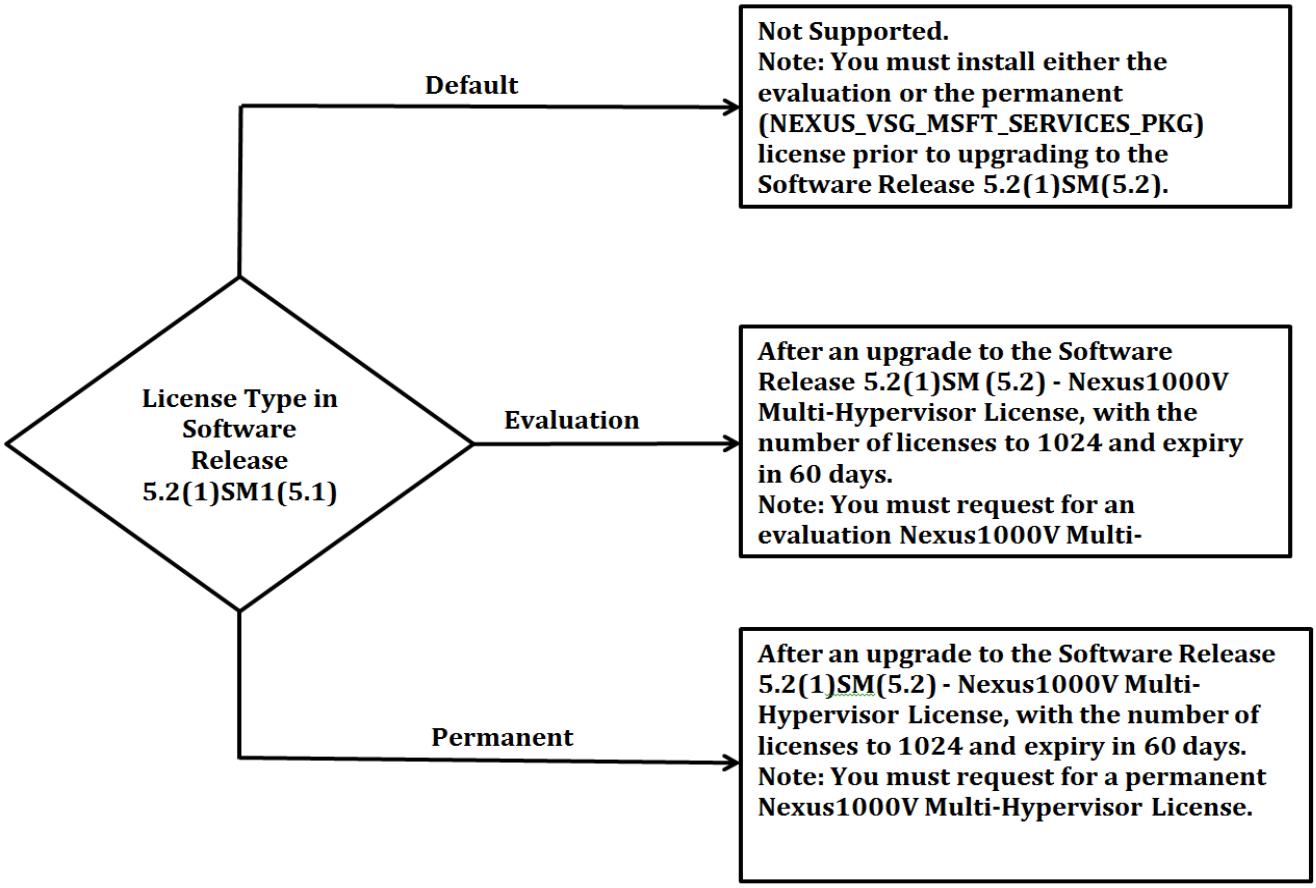
### Licensing and Upgrade

If you are upgrading the software from Release 5.2(1)SM1(5.1), and the switch edition is advanced, then you need to follow the Figure 2-1 to check on the license details after the upgrade.

**Note** For information on availing a replacement for the Nexus 1000V Multi-Hypervisor licenses, see the Rehosting a License on a Different VSM section in the Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide, Release 5.2(1)SM1(5.2).

**Note** The License count is counted as one for each of the 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 the "Upgrading the VSM" section on page 2-4.
- To upgrade the VSEM, see the "Upgrading the Cisco VSEM" section on page 2-12.

2. You have already obtained a copy of the VEM software file.

# Upgrade Procedures

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

**Note** For the SCVMM upgrade from SP1 to R2, see the "Upgrade SCVMM 2012 SP1 to SCVMM 2012 R2" section on page 2-21. For the host upgrade to Windows Server 2012 R2, see the "Upgrade Windows Server 2012 Hosts to 2012R2" section on page 2-22.

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

| If you are running this configuration | Follow these steps |
|---|---|
| Release 5.2(1)SM1(5.1) with the following:<br>• SCVMM 2012 (SP1) UR2 build version 3.1.6020.0 and later)<br>• Windows Server 2012 Hosts | • Upgrade Cisco Nexus 1000V to the current release<br>– Upgrade the VSM to current release.<br>– Upgrade the VSEM to current release.<br>– Upgrade the VEM to current release. |

# Upgrading the VSM

This section includes the following topics:



## 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 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.

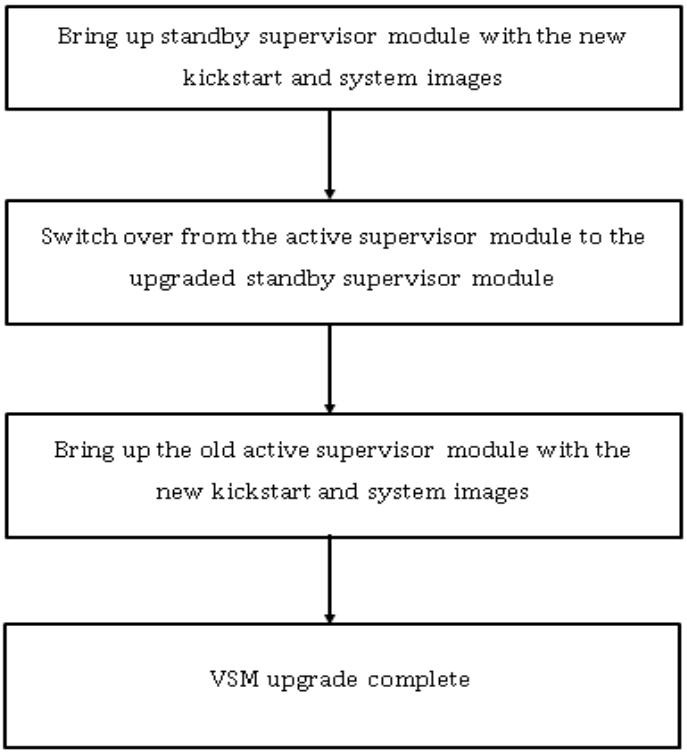
An ISSU updates the following images:

- Kickstart image
- System image

# ISSU Process for the Cisco Nexus 1000V

Figure 2-2 displays the ISSU process.

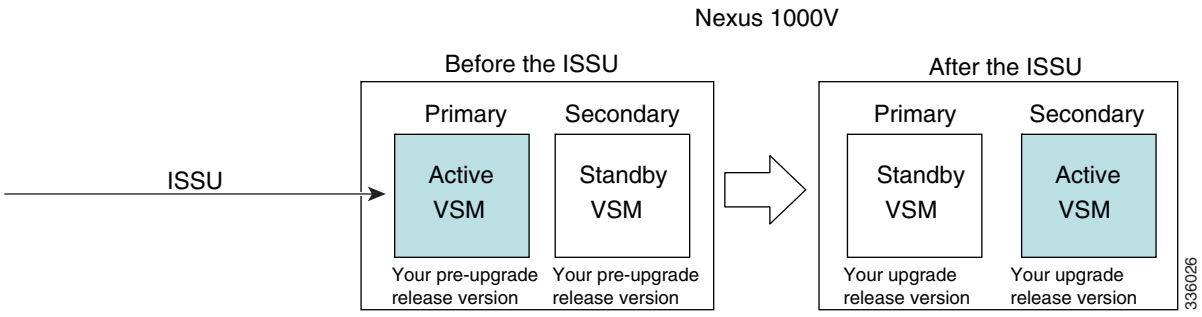
***Figure 2-2 ISSU Process***




# 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 from Releases 5.2(1)SM1(5.1) to Release 5.2(1)SM1(5.2) 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.

This section includes the following topics:

- Upgrading VSMs in a High Availability (HA) pair, page 2-8
- Upgrading a standalone VSM, page 2-9

## Upgrading VSMs in a High Availability (HA) pair

To upgrade the VSMs in a 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. For more information, see the "Downloading the Cisco Nexus 1000V Package" section on page 1-7.

**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.SM1.5.2.bin bootflash:
n1000vh-dk9.5.2.1.SM1.5.2.bin
switch# copy tftp://10.106.196.163/n1000vh-dk9-kickstart.5.2.1.SM1.5.2.bin
bootflash:n1000vh-dk9-kickstart.5.2.1.SM1.5.2.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.SM1.5.2.bin system bootflash: n1000vh-dk9.5.2.1.SM1.5.2.bin
```

**Step 9** Save the running configuration to startup configuration, bootflash:, and to an external location.

**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, Release 5.2(1) SM1 (5.2)*.

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 10** Perform the upgrade on the active VSM by using the following command:

```
install all kickstart bootflash: n1000vh-dk9-kickstart.5.2.1.SM1.5.2.bin system
bootflash: n1000vh-dk9.5.2.1.SM1.5.2.bin
```

**Step 11** 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 again, the upgrade process initiates a switchover. The upgrade then continues from the new active VSM.

**Step 12** After the installation operation completes, log in and verify that the switch is running the required software version by using the **show version** command.

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

**Step 14** 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** In case the command **show install all** status does not exit automatically while the installation is in progress, use Ctrl+C to exit from the command.

**Step 15** Perform the Refresh operation of the Cisco Nexus 1000V Virtual Switch Extension Manager, if you have added the Cisco Nexus 1000V as the Virtual Switch Extension Magager in SCVMM. To perform the refresh operation, do the following:

a. Open the SCVMM console.

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

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

## 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 the "Downloading the Cisco Nexus 1000V Package" section on page 1-7.

**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 copies a kickstart and system image using tftp.

```
switch# copy tftp://10.106.196.163/n1000vh-dk9.5.2.1.SM1.5.2.bin bootflash:
n1000vh-dk9.5.2.1.SM1.5.2.bin
switch# copy tftp://10.106.196.163/n1000vh-dk9-kickstart.5.2.1.SM1.5.2.bin
bootflash:n1000vh-dk9-kickstart.5.2.1.SM1.5.2.bin
```

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

**Step 5** Save the running configuration to startup configuration using the **copy running-config startup-config** command.

**Step 6** Verify the ISSU upgrade for the **kickstart** and **system** images

```
switch# show install all impact kickstart bootflash:
n1000vh-dk9-kickstart.5.2.1.SM1.5.2.bin system bootflash:
n1000vh-dk9.5.2.1.SM1.5.2.bin
```

**Step 7** Update the boot variables and module images on the VSM using the following command:

```
install all kickstart bootflash: n1000vh-dk9-kickstart.5.2.1.SM1.5.2.bin system
bootflash: n1000vh-dk9.5.2.1.SM1.5.2.bin
```

**Step 8** Continue with the installation by pressing **Y**.

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

**Step 9** After the installation operation completes, log in and verify that the switch is running the required software version by using the **show version** command.

**Step 10** Copy the running configuration to the startup configuration using the **copy running-config startup-config** command.

**Step 11** 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** In case the command **show install all status** does not exit automatically while the installation is in progress, use Ctrl+C to exit from the command.

**Step 12** If you have added the Cisco Nexus 1000V as the Virtual Switch Extension Magager in the SCVMM, then perform Refresh operation of Cisco Nexus 1000V Virtual Switch Extension Manager

a. Open the **SCVMM** console.

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

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

# Performing an ISSU Upgrade using an ISO Image File

To do an ISSU upgrade using an ISO image file, perform the following steps:

**Step 1** Log in to Cisco.com to access the Software Download Center. To log in to Cisco.com, go to http://www.cisco.com/ and click **Log In** at the top of the page. Enter your Cisco username and password.

You see links to the download images for the switch.

**Step 2** Select and download the ISO file to bootflash:.

**Step 3** Verify that the required space is available in the bootflash: directory for the image file(s) to be copied.

**Step 4** Copy the ISO to the bootflash using a transfer protocol such as ftp:, tftp:, scp:, or sftp:. The examples in this procedure use scp:.

**Step 5** Enter the **install all iso bootflash:<iso_filename>** command.

```
switch# install all iso bootflash:n1000vh-dk9.5.2.1.SM1.5.2.iso

Verifying image bootflash:/n1000vh-dk9-kickstart.5.2.1.SM1.5.2.gbin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/n1000vh-dk9.5.2.1.SM1.5.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/n1000vh-dk9.5.2.1.SM1.5.2.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/n1000vh-dk9-kickstart.5.2.1.SM1.5.2.gbin.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive         reset
     2       yes  non-disruptive         reset

Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system          5.2(1)SM1(5.1)        5.2(1)SM1(5.2)           yes
     1   kickstart          5.2(1)SM1(5.1)        5.2(1)SM1(5.2)           yes
     2      system          5.2(1)SM1(5.1)        5.2(1)SM1(5.2)           yes
     2   kickstart          5.2(1)SM1(5.1)        5.2(1)SM1(5.2)           yes
```

```
Module Running-Version ESX Version       VSM Compatibility       ESX Compatibility
------  -------------- ------------ ----------------------  ----------------------

Do you want to continue with the installation (y/n)?  [n] y<<<<<<<<<<<<compatibility
matrix (Press Ctrl + C here)
```

This step extracts the kickstart and system images to boot flash:. After issuing the **install all iso bootflash:<iso_filename>**, the installer executes and displays the compatibility matrix.

**Step 6** Exit (press Ctrl +C) @ compatibility matrix and run the command **install all kickstart bootflash:<kickstart_filename> system bootflash:<system_filename>**.

This initiates the installer for the ISSU to start and the upgrade completes.

The switch reboots and restarts with the new image.

# Upgrading the Cisco VSEM

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-VSEMProvider-5.2.1.SM1.5.2.0.msi from the Cisco Nexus1000V zip location on the SCVMM Server.

**Note** The installation restarts the SCVMM service.

- This uninstalls the existing Cisco VSEM Provider MSI and installs a new version.
- After a successful installation, it establishes communication between the SCVMM and the Cisco Nexus1000V VSM.
- It places the PowerShell scripts that are used to upgrade the Cisco Nexus 1000V VEM in the following folder of the SCVMM server: **%ProgramFiles%\Cisco\Nexus1000V\Scripts**. For example, C:\Program Files\Cisco\Nexus1000V\Scripts.

**Step 2** Verify that the Cisco VSEM Provider is installed correctly by completing the following steps:

**a.** Open SCVMM console.

**b.** Navigate to **Settings workspace**.

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

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

**Step 3** Refresh the Cisco Nexus 1000V Extension Manager

**a.** Open the SCVMM console.

**b.** Navigate to **Fabric workspace**. On **Fabric** pane, expand **Networking**, and then click **Switch Extension Manager**.

If the SCVMM version is 2012 R2, then click **Network Service** instead of **Switch Extension Manager**.

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

# Upgrading the VEM Software

You must complete the following procedures before upgrading the VEM software.

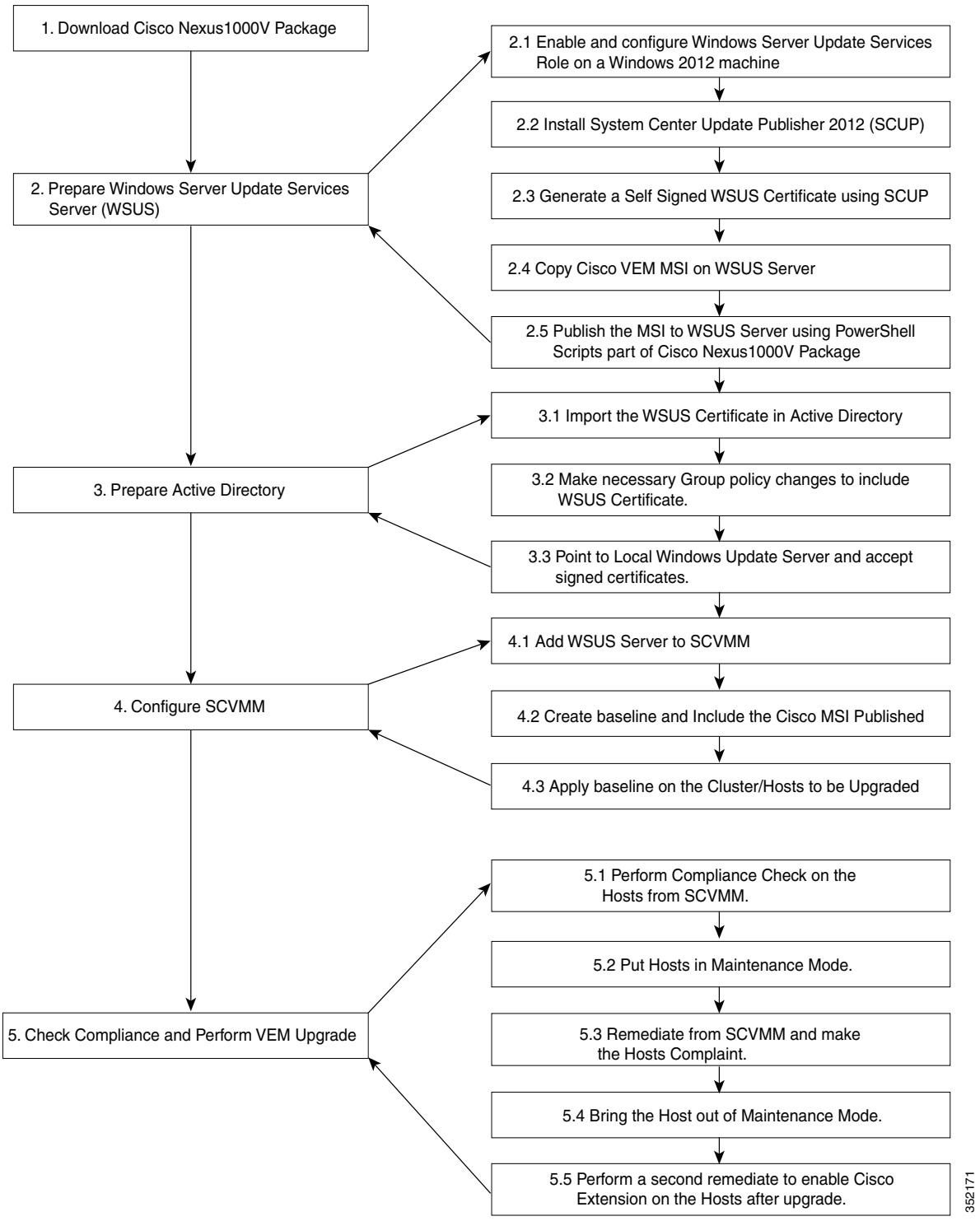
- Upgrade the VSM. For information, see the "Upgrading the VSM" section on page 2-4.
- Upgrade the VSEM. For information, see the "Upgrading the Cisco VSEM" section on page 2-12.

This section includes the following:

# Upgrade Workflow

Figure 2-4 displays the Cisco Nexus 1000V VEM upgrade workflow.

***Figure 2-4 Cisco Nexus 1000V VEM upgrade Workflow***



# Upgrading the VEM Software Manually

**Summary Steps**

1. Download Cisco Nexus 1000v package, page 2-15
2. Prepare the Windows Server Update Services (WSUS) Server, page 2-15
3. Prepare the Active Directory (AD), page 2-17
4. Configure SCVMM, page 2-18
5. Check Compliance and Perform VEM upgrade, page 2-19

# Download Cisco Nexus 1000v package

For information to download the Cisco Nexus 1000v package, see the "Downloading the Cisco Nexus 1000V Package" section on page 1-7.

# Prepare 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 2012 machine.

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

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

For more information, see http://technet.microsoft.com/en-us/library/hh134775.aspx.

**Step 3** Generate a self-signed WSUS certificate via the SCUP using the following steps:.

a. Run the SCUP 2011 as a network administrator.
b. Click the **Options** icon in the upper left corner and then click **Options**.
c. Select the **Enable publishing to an update server** check box for Updates Publisher 2011 to publish all software updates.
d. Select 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 is successful, 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 available 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 that appears, select **Certificates** and then click **Add**.

e. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.

f. Select the **Local computer radio** button and click **Finish** to close the **Certificates snap-in** dialog box.

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

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

i. In the results pane, right-click the desired certificate, click **All Tasks**, and then 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 then 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 then click **Import**. Complete the **Certificate Import Wizard** using the exported file from step j.

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

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

PS C: Publish-CiscoUpdate.ps1 <location of VEM MSI file on Update Server>

```
PS C: > .\Publish-CiscoUpdate.ps1 .\Nexus1000V-VEM-5.2.1.SM1.5.1.73.msi
Starting Publish-CiscoUpdate...
------------------ MSI File Info -----------------------
Pkg File Name : Nexus1000V-VEM-5.2.1.SM1.5.1.73.msi
Pkg Full Path : C:\Nexus1000V-VEM-5.2.1.SM1.5.1.73.msi
Pkg Dir : C:
Pkg Name : Nexus1000V-VEM-5.2.1.SM1.5.1.73
-------------------------------------------------------
Reading MSI Properties...
------------------ MSI Details -----------------------
MSI : C:\Nexus1000V-VEM-5.2.1.SM1.5.1.73.msi
ProductName :  Cisco Nexus 1000V Series Switch
Description :  Cisco Nexus 1000V Series Switch
Manufacturer :  Cisco Systems, Inc.
ProductVersion :  1.01.000
ProductCode :  {7D54B9CA-9DDA-4E67-94B4-695679F48539}
UpgradeCode :  {D1099B98-17BE-40F2-A10E-29D48B9A5829}
DriverID :  {9C8ED422-F33A-4F34-B771-E8B8D0539FD3}
DriverVersion :  105.200.0.73
ExtensionType :  Forwarding
-------------------------------------------------------
Connecting to WSUS Server ...
------------- Update Server Details ------------------
Name : WSUS
Version : 6.2.9200.16384
-------------------------------------------------------
Loading MSI in Software Distribution package...
Loaded MSI installer in SDP.
Configuring Software Distribution Package...
Configuration Complete.
Preparing Update Catalog XML...
Update Catalog Creation complete.
Publishing package to WSUS Server...
Published .\Nexus1000V-VEM-5.2.1.SM1.5.1.73.msi to WSUS Server.
```

**Step 7** Verify if the msi was published correctly using the script.

PS C: Get-CiscoUpdate.ps1

```
PS C: >Nexus1000v.5.2.1.SM1.5.2\WSUS\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: 1.01.000] [Driver: 105.200.0.73]
GUID : add6924f-2989-4143-bd46-bd16e919f32a
Description : [PC: {7D54B9CA-9DDA-4E67-94B4-695679F48539}] [UC:
{D1099B98-17BE-40F2-A10E-29D48B9A5829}] \n
Creation Date : 12/12/2013 7:07:24 PM
Arrival Date : 12/12/2013 7:07:42 PM
--------------------------------------------------
```

# Prepare the Active Directory (AD)

To prepare the AD, perform the following steps:

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

**Step 2** On the AD server, click the **Tools** tab of the **Server Manager**, and then 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 then right-click to select **New**.

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

**Step 4** Navigate to the newly created GPO in **<Forest name>/Domains/<Domain name>** and right-click to select **Edit** to open policy in 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**. Check 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-2012. 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**. Check the **Enabled** radio button. Click **Apply** and then 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 newly created GPO.

1. On AD server, using the **Group Policy Managament 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 then click **Import**. Complete the **Certificate Import Wizard** using the file from Step 1.
3. Right-click **Trusted Root Certification Authorities**, click **All Tasks**, and then 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 elevated command prompt, to enforce the group policy settings to be applied to the hosts immediately.

# Configure SCVMM

To configure the SCVMM, perform the following steps:

**Step 1** Add the WSUS server to the VMM using the following steps:

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

b. In the **Add Windows Server Update Services Server** dialog box, enter the name of the Update server in **Computer name** field and 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 Series Switch, using the following steps:

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**, and search for string "Cisco" to select an update for the Cisco Nexus 1000V.

d. Click **Next** to move to the Assignment Scope tab and then select infrastructure servers that need to be added to the baseline.

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

# Check Compliance and Perform VEM upgrade

To check compliance and perform a VEM upgrade, perform the following steps:

**Step 1** Scan servers to check compliance with respect to previously created baseline for Cisco Nexus 1000v Series Switch

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

b. Select the **Home** tab, and click **Compliance** on ribbon.

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

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

Once the scan is completed, identify the hosts that are non-compliant.

**Step 2** Put the non-compliant host to maintenance mode and perform Remediation.

a. Put the Non-compliant host in maintanence mode by refering to below link:

For more information, see http://technet.microsoft.com/en-us/library/hh882398.aspx

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

c. Select **Home** tab, and click **Compliance** on ribbon.

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

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

f. In the **Update remediation wizard**, select the **Do not restart servers after remediation** checkbox.

g. Click **Remediate** to start update remediation.

**Step 3** Bring the host out of Maintenance Mode.

For more information, see http://technet.microsoft.com/en-us/library/hh882398.aspx

**Step 4** Perform another remediation, to bring the Host online in VSM

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

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

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

d. Right-click on the switch to select **Remediate**.

**Step 5** Verify whether the VEM modules got upgraded using the **show module** command in VSM. After upgrade, the software version in the **show module** output should reflect as **5.2(1)SM1(5.2)**.

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

# Upgrading the VEM Software Using a Script

Step 5 of the "Upgrade Workflow" section on page 2-14 are performed by this script.

**Note** Steps 1 to 4 of "Upgrade Workflow" section on page 2-14 needs to be done manually.

## Prerequisites

The script needs to be executed from the PowerShell console of the SCVMM server. Additionally, ensure that the following prerequisites with respect to configuration are followed before running the script:

- Windows Update server should already be added to SCVMM.
- Upgrade baselines should be pre-created.
- Nexus1000v baseline should have only one upgrade.

## Runnning VEM upgrade script

On SCVMM server, the script is located at %ProgramFiles%\Cisco\Nexus1000V\Scripts\VEMUpgrade. For example, :\Program Files\Cisco\Nexus1000V\Scripts\VEMUpgrade.

It requires the following three inputs as parameters:

- BaseLine name
- Cluster name
- Logical Switch name.

Below is the sample snapshot of VEM upgrade script:

```
PS C:\Program Files\Cisco\Nexus1000V\Scripts\VEMUpgrade> .\Upgrade-Nexus1000V-VEM.ps1
-BaseLineName build_73 -ClusterName infraset4 -LogicalSwitchName nexus1000v

################################################################################
## COMPANY NAME: Cisco Systems Inc                                            ##
## Copyright © 2013 Cisco Systems, Inc. All rights Reserved.                  ##
##                                                                            ##
## 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 - 'build_73'
------------------------------------------------------
Update 1 => Cisco Nexus 1000V Series Switch [MSI: 1.01.000] [Driver: 105.200.0.73]

------------------------------------------------------------------------------------------
Starting Compliance Scan on Cluster before Upgrade 'infraset4' with baseline
'build_73'
------------------------------------------------------------------------------------------
HOSTNAME =  hyperv01 : STATUS = NonCompliant : Nexus1000V Version =  1.00.000
HOSTNAME =  hyperv06 : STATUS = NonCompliant : Nexus1000V Version =  1.00.000

------------------------------------------------------------------------------
STARTING UPGRADE ON HOST: hyperv01
------------------------------------------------------------------------------
STEP 1.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster
NOTE: This may take a while, '9' VM's are being migrated, and 0 VM's are being saved!!
```

```
STEP 1.2 : Starting Update Remediation

STEP 1.3 : Stopping Maintenance Mode

--------------------------------------------------------------------------------
STARTING UPGRADE ON HOST: hyperv06
--------------------------------------------------------------------------------
STEP 2.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster
NOTE: This may take a while, '9' VM's are being migrated, and 0 VM's are being saved!!

STEP 2.2 : Starting Update Remediation

STEP 2.3 : Stopping Maintenance Mode


--------------------------------------------------------------------------------
Starting Compliance Scan on Cluster after Upgrade 'infraset4' with baseline 'build_73'
--------------------------------------------------------------------------------
HOSTNAME =  hyperv01 : STATUS = Compliant : Nexus1000V Version =  1.01.000
HOSTNAME =  hyperv06 : STATUS = Compliant : Nexus1000V Version =  1.01.000
-------------------------------
Nexus1000V VEM Upgrade Complete
-------------------------------
Transcript stopped, output file is C:\Program
Files\Cisco\Nexus1000V\Scripts\VEMUpgrade\Upgrade-Nexus1000V-VEM-logs\Upgrade-Nexus100
0V-VEM-12-14-13_5-40.log
```

Verify whether VEM modules got upgraded using the **show module** command in VSM. After the upgrade, the software version in the **show module** output should reflect as 5.2(1)SM1(5.2).

# Upgrade SCVMM 2012 SP1 to SCVMM 2012 R2

Upgrade SCVMM 2012 SP1 to SCVMM 2012 R2 by retaining the VMM database from the System Center 2012 SP1 deployment.

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

## Preparing Cisco Nexus 1000V

After upgrading SCVMM to 2012 R2, install the Cisco Provider MSI using the following steps:

**Step 1** Uninstall existing Cisco Nexus 1000V VSEM Provider.

**Step 2** Install the Nexus1000V-VSEMProvider-5.2.1.SM1.5.2.0.msi from the Cisco Nexus1000V zip location on SCVMM Server.

**Note** The installation restarts the SCVMM service.

**Step 3** Verify that the Cisco Provider is installed corectly by completing the following steps:

a. Open the SCVMM console.

b. Navigate to **Settings workspace**.

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

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

**Step 4** Do the following to refresh the Cisco Nexus 1000V Extension Manager:

a. Open the SCVMM console.

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

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

# Upgrade Windows Server 2012 Hosts to 2012R2

Microsoft does not support an upgrade of the third party extension, for example, Cisco Nexus 1000V VEM, while upgrade of Windows Server 2012 to Windows Server 2012 R2. Therefore, you must uninstall Cisco Nexus 1000V VEM before the host upgrade, and re-install it after the upgrade.