Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide, Release 5.2(1)SM3(1.1)

First Published: December 19, 2014
Last Updated: May 27, 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
CONTENTS

CHAPTER 1

Installing the Cisco Nexus 1000V  1-1
Prerequisites for Installing the VSM Software  1-1
Before You Begin  1-1
Guidelines and Limitations  1-1
System Requirements  1-1
Hardware Requirements  1-1
Software Requirements  1-2
VSM NIC Ordering  1-2
Basic Topology  1-3
Installation Workflow  1-4
Installing the VSM Software  1-6
  Downloading the Cisco Nexus 1000V Package  1-6
  Configuring SCVMM and VSM  1-6
    Installing SCVMM Components  1-7
    Installing and Configuring the VSM Workflow  1-8
    Configuring the SCVMM Fabric Workflow  1-12
  Installing the VSM Certificate  1-16
    Installing the VSM Certificate Manually  1-16
    Installing the VSM Certificate Using a Script  1-16
  PowerShell Scripts for Configuring the SCVMM Fabric Workflow  1-17
Preparing the Microsoft Hyper-V Hosts (Optional)  1-20
  Configuring the MTU with the Cisco Nexus 1000V  1-20
  VMQ Processor Configuration with the Cisco Nexus 1000V  1-20
  Changing the RSS Registry  1-21
Adding Hosts to a Logical Switch  1-21
Connecting the VM Network Adapter to the Logical Switch  1-22

CHAPTER 2

Upgrading the Cisco Nexus 1000V  2-1
Prerequisites for Upgrading the VSM Software  2-1
  Before You Begin  2-1
Prerequisites  2-1
  Licensing  2-1
Prerequisites for Upgrading the VEM Software  2-3
Upgrade Procedures  2-3
Preparing SCVMM and Windows Server Hosts 2-3
  Upgrading SCVMM 2012 SP1 to SCVMM 2012 R2 2-4
    Preparing the Cisco Nexus 1000V 2-4
  Upgrading Windows Server 2012 Hosts to 2012R2 2-4
Upgrading the VSM to the Current Release 2-4
  Software Images 2-5
  In-Service Software Upgrades on Systems with Dual VSMs 2-5
  ISSU Process for the Cisco Nexus 1000V 2-6
  ISSU VSM Switchover 2-6
  ISSU Command Attributes 2-6
  Upgrading VSMs Using Kickstart and System Images 2-7
    Upgrading VSMs in an HA Pair 2-7
    Upgrading a Standalone VSM 2-9
    Reregistering the Policy Agent of the Upgraded VSM 2-11
Upgrading the Cisco VSEM to the Current Release 2-12
Upgrading the VEM Software to the Current Release 2-13
  Upgrade Workflow 2-13
  Upgrading the VEM Software Using WSUS Server 2-15
    Downloading the Cisco Nexus 1000V package 2-15
    Preparing the Windows Server Update Services (WSUS) Server 2-15
    Preparing the Active Directory 2-17
    Configuring SCVMM 2-18
    Checking Compliance and Performing the VEM upgrade 2-18
  Upgrading the VEM Software Using a Script 2-19
    Prerequisites 2-19
    Running the VEM Upgrade Script 2-19
  Upgrading the VEM Software Manually from Cisco Nexus 1000V Release 5.2(1)SM1(5.2) or Later to 5.2(1)SM3(1.1) 2-21
Performing Post Upgrade Operations 2-22
  Changing the Feature Support Level 2-22
    Prerequisites 2-22
    Changing the Feature Level Support 2-22
  Installing the Windows Patch 2-23

CHAPTER 3
Installing a VSM on the Cisco Cloud Services Platform 3-1
  Before You Begin 3-1
  Procedure 3-1
Installing the Cisco Nexus 1000V

Prerequisites for Installing the VSM Software

For information about your software and platform compatibility, see the *Cisco Nexus 1000V and Microsoft Hyper-V Compatibility Information* document.

Before You Begin

Ensure that you have installed and configured the following components on the target setup:

- Windows Active Directory service.
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2 UR4 or later.
- For the hosts that are running the Virtual Ethernet Module (VEM), you should enable the Hyper-V module for Windows PowerShell.

Guidelines and Limitations

It is your responsibility to monitor and install all the relevant patches from Microsoft on the Windows hosts.

System Requirements

This section describes the hardware and software requirements.

Hardware Requirements

The hardware must meet the requirements set by Microsoft to run the Hyper-V role. The Cisco Nexus 1000V Virtual Supervisor Module (VSM) requires VMs with the following configuration:

- 4 GB minimum of hard disk space
- 4 GB minimum of RAM
As a best practice, we recommend that you have four network adapters (network interface cards—NICs) on the host where Microsoft Hyper-V is installed. You can have various combinations depending on the hardware that you have. For example, you can have one NIC with four ports or four NICs with one port each.

**Software Requirements**

To install and bring up a Cisco Nexus 1000V, you need the following server setup:

- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2 UR4 or later
- Windows 2012 R2 hosts
- Active Directory server

To configure the VSM, you need the following information:

- VSM IP address.
- VSM domain ID (1–1023)—This ID is used for high availability (HA).
- Layer 3 connectivity between a VSM and the hosts that run a VEM is required.
  - Layer2 mode is not supported.
  - Layer3 UDP port number 4785.
- Communication between the VSM and VEM occurs over UDP port number 4785 that uses the Cisco Nexus Control Protocol (CNCP).
- TCP port 80 is open on the network for communication from the SCVMM to VSM. With the HTTPS protocol, the TCP port is 443.

**VSM NIC Ordering**

The VSM creates interfaces in an ascending MAC address order of the virtual NIC offered by Microsoft Hyper-V. Currently, Microsoft Hyper V provides no guarantees that this order is the same as displayed at the VSM VM Settings panel. The VSM always uses its first interface as control0 and its second interface as mgmt0. The network profiles for these two interfaces might need different VLANs. Therefore, you should verify that the interfaces are selected by the VSM in the same order that are displayed in the Settings panel.

Enter the following command on the VSM to verify the order of the management and control MAC addresses:

```
Nexus1000V# show interface mac-address
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Mac-Address</th>
<th>Burn-in Mac-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt0</td>
<td>001d.d8b7.1e61</td>
<td>001d.d8b7.1e61</td>
</tr>
<tr>
<td>control0</td>
<td>001d.d8b7.1e60</td>
<td>001d.d8b7.1e60</td>
</tr>
</tbody>
</table>

If the order is not the same, use the following commands to specify the preferred MAC-to-control0/mgmt0 interface mappings:

```
system internal control-mac XXXX.XXXX.XXXX
system internal mgmt-mac XXXX.XXXX.XXXX
```

These commands require that you enter the `copy running-config startup-config` command afterwards to make the change persistent and effective after the next VSM reload.
switch# show system internal interface mac-address
Sample output:
Interface Preferred MAC
sh interface mac-address
--------- --------------
mgmt0 cccc.bbbb.aaaa
control0 aaaa.bbbb.cccc

If any of the preferred MACs are not available at VSM bootup, the driver picks another interface instead (following MAC ascending order). The system logs an error with a syslog as follows:
%KERN-3-SYSTEM_MSG: Preferred MAC (aaaa.bbbb.cccc) for control0 not found – kernel

Basic Topology

Figure 1-1 displays the basic Hyper-V topology on a Cisco Nexus 1000V VEM.

Note
The management NIC is actually on the Microsoft switch. The management VM cluster is for infra VMs. The data VM cluster is for workload VMs. The minimum topology is three servers with four NICs each.
Figure 1-1 displays the Cisco Nexus 1000V deployment on two servers with the following network configuration:

- Management NIC—This network adapter is connected to an external network for the host OS connectivity.
- Microsoft virtual switch—The Microsoft virtual switch has one physical network adapter for the VSM connectivity.
- Two physical network adapters—These adapters are connected to the Cisco Nexus 1000V logical switch instance of the Hyper-V host.

**Installation Workflow**

Figure 1-2 displays the Cisco Nexus 1000V installation process on Microsoft SCVMM.
Figure 1-2  Cisco Nexus 1000V Installation Workflow

1. Download Cisco Nexus 1000V Package
   - 2.1 Install Cisco Provider MSI
   - 2.2 Install Cisco Template Files
   - 2.3 Copy VEM to SCVMM Repository
   - 2.4 Copy VSM ISO to SCVMM Library

2. Install SCVMM Components
   - 3.1 Create Microsoft Switch for VSM Connectivity
   - 3.2 Install VSM VM using VM Template
   - 3.3 Configure VSM

3. Install and Configure VSM
   - 4.1 Add Switch Extension Manager (Connect to VSM)
   - 4.2 Create Logical Switch
   - 4.3 Create VM Networks

4. Configure SCVMM Fabric and VM Network
   - 5.1 Configure PNIC MTU Settings
   - 5.1 Configure VMQ RSS Settings

5. Prepare Hyper-V Hosts
   - Management PNIC Workflow
   - Non-MGMT PNIC Workflow

6. Create Nexus 1000V Logical Switch Instance on hosts
   - 6.1.1 Select Host
   - 6.1.2 Select the MGMT PNIC
   - 6.1.3 Create MGMT Host Virtual Network Adapter
   - 6.1.4 Deploy Logical Switch
   - 6.1.5 Add Remaining PNICs to Logical Switch

7. Connect VMs to Cisco Nexus 1000V
   - 7.1 Select VM Network Adapter
   - 7.2 Connect VM Network Adapter to Logical Switch
   - 7.3 Select VM Network and Port Classification for the Network Adapter
Installing the VSM Software

To install the VSM software, perform the following steps:

1. **Downloading the Cisco Nexus 1000V Package**, page 1-6.
2. **Configuring SCVMM and VSM**, page 1-6.
3. **Installing the VSM Certificate**, page 1-16.
4. **Preparing the Microsoft Hyper-V Hosts (Optional)**, page 1-20.
5. **Adding Hosts to a Logical Switch**, page 1-21.
6. **Connecting the VM Network Adapter to the Logical Switch**, page 1-22.

**Downloading the Cisco Nexus 1000V Package**

The Cisco Nexus 1000V for Microsoft Hyper-V package (a zip file) is available at the download URL location provided with the software.

To download the Cisco Nexus 1000V package, download the Cisco Nexus 1000V package for Microsoft System Center Virtual Machine Manager (SCVMM) 2012 SP1. This package contains the following files:

- VSM ISO (Nexus1000V.5.2.1.SM3.1.1\VSM\install\Nexus-1000V.5.2.1.SM3.1.1.iso)
- VEM MSI package (Nexus1000V.5.2.1.SM3.1.1\VEM\Nexus1000V-VEM-5.2.1.SM3.1.1.0.msi)
- Cisco VSEM Provider MSI package (Nexus1000V.5.2.1.SM3.1.1\VMM\Nexus1000V-VSEMProvider-5.2.1.SM3.1.10.msi)
- Kickstart file (Nexus1000V.5.2.1.SM3.1.1\VSM\Upgrade\Nexus-1000V-kickstart.5.2.1.SM3.1.10.bin)
- System file (Nexus1000V.5.2.1.SM3.1.1\VSM\Upgrade\Nexus-1000V.5.2.1.SM3.1.1.bin)
- PNSC-PA (Nexus1000V.5.2.1.SM3.1.1\PNSC-PA\vsmhv-pa.3.2.1e.bin)
- WSUS scripts (Nexus1000V.5.2.1.SM3.1.1\WSUS\)
  - Publish-CiscoUpdate.ps1
  - Remove-CiscoUpdates.ps1
  - Get-CiscoUpdates.ps1
  - Get-MSIDetails.ps1

**Configuring SCVMM and VSM**

This section describes how to install the Cisco Nexus 1000V for Microsoft Hyper-V VSM software and includes the following topics:

- **Installing SCVMM Components**, page 1-7
- **Installing and Configuring the VSM Workflow**, page 1-8
- **Configuring the SCVMM Fabric Workflow**, page 1-12
Installing SCVMM Components

To install the SCVMM components, perform the following steps:

---

**Step 1**  
Install the Cisco Provider MSI.

- Install the *Nexus1000V-VSEMProvider-5.2.1.SM3.1.1.0.msi* from the Cisco Nexus1000V zip location on the SCVMM server in order to establish communication between SCVMM and the Cisco Nexus1000V VSM.

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

- Verify that the Cisco Provider is installed properly:
  - Open the SCVMM console.
  - Navigate to the Settings Pane.
  - Click **Configuration Providers**.
  - Verify that the Cisco Nexus 1000V extension is displayed.

---

**Step 2**  
Install the Cisco VSM template files.

After downloading the Cisco Nexus 1000V for Microsoft Hyper-V package, complete the following steps to install the VSM template:

- On the SCVMM server, open the PowerShell console from the SCVMM console.
- Run the script *Register-Nexus1000VVSMTemplate.ps1* from the following location:
  
  \%ProgramFiles\%Cisco\%Nexus1000V\%V2\Nexus1000V-VSMTemplate.

  This script imports the Cisco VSM template in the SCVMM library.

- To verify the template, do the following:
  - Navigate to the **Templates** tab.
  - Choose **Templates**. On the right pane, the Nexus 1000V-VSM-Template is listed.

---

**Step 3**  
Copy the VEM to the SCVMM repository.

The VEM is an MSI file that needs to be placed in the following location on the SCVMM server:

\%ALLUSERSPROFILE\%Switch Extension Drivers. For example, C:\ProgramData\Switch Extension Drivers. SCVMM uses the MSI file during Add host operation.

**Caution**  
Do not install the VEM on the SCVMM server. Only copy the file to the location specified.

---

**Step 4**  
Copy the VSM ISO file. For example, copy Nexus-1000V.5.2.1.SM3.1.1.iso to the SCVMM library in the following location on SCVMM server: 

\VMName\MSSCVVMLibrary. After copying the ISO file, make sure to refresh the SCVMM library so that SCVMM detects the copied ISO.
Installing and Configuring the VSM Workflow

To install and configure the VSM workflow, use an existing Microsoft Switch with external connectivity or create a new one, for the VSM connectivity.

1. Installing the VSM using a VM Template, page 1-8
2. Configuring the VSM, page 1-9
3. Deploying the VSM, page 1-9
4. Configuring the VSM, page 1-11

Installing the VSM using a VM Template

To install the VSM using a VM template, perform the following steps:

---

**Step 1**
From the left navigation pane in the SCVMM user interface, click the VMs and Services icon and from the top menu bar, choose Create Virtual Machine. The Create Virtual Machine wizard opens.

**Step 2**
In the Select Source panel, choose the Use an existing virtual machine, VM template, or virtual hard disk option and click Browse.

**Step 3**
Choose the Nexus1000V_VSM_Template file listed under the Type: VM Template header.

**Step 4**
Click OK and click Next.

**Step 5**
In the Specify Virtual Machine Identity panel, enter the name of the virtual machine and click Next.

**Step 6**
In the Configure Hardware panel, configure the hardware settings for the virtual machine. If you are using a template, most of the settings have already been configured (For example, the hard drive is set to 4 GB and there are three network adapters). The only item that you have to manually configure is the ISO image.

**Step 7**
Click Virtual DVD drive below the Bus Configuration header in the center pane.

**Step 8**
Click Existing ISO image file and click Browse.

**Step 9**
Choose the ISO image from the SCVMM library, click OK, and click Next.

**Step 10**
In the Select Destination panel, keep the default settings of Place the virtual machine on a host; Destination: All Hosts and click Next.

**Step 11**
After the host is displayed in the Select Host panel, chose it, and click Next.

**Step 12**
In the Configure Settings panel, review the settings and click Next.

**Step 13**
In the Select Networks panel, choose the virtual switches that are used for the virtual machine. For each network adapter, select the type of the virtual switch. For example, choose Standard Switch or Logical Switch and click Next.

**Step 14**
In the Add Properties panel, keep the default settings of the Automatic Actions and click Next.

**Step 15**
In the Confirm the Settings panel in the final Summary window, review and confirm the settings.

**Step 16**
Click Create to begin the virtual machine creation. A progress bar is displayed in the Job Status column in the VM window.

**Step 17**
After the virtual machine creation is complete, right-click the Name of the virtual machine in the SCVMM user interface and choose Power On.

**Step 18**
Right-click the Name of the virtual machine again, click Connect or View, and choose Connect via Console.

See Table 1-1 for more information about the Cisco Nexus 1000V ISO boot options.
Installing the VSM Software

After installing VSM using a VM template, connect to a VM console and configure the VSM. We recommend that the VSM is deployed using the template provided by Cisco. After the deployment is complete, power on the VSM. The following basic inputs are required for the VSM configuration:

1. Switch name
2. Domain ID
3. Management address
4. Subnet mask
5. Gateway address

Note: Make sure that you eject the virtual ISO image from the CD ROM.

Deploying the VSM

To deploy the VSM, perform the following steps:

Step 1: When the Virtual Machine Viewer window opens, the message “Do you want to format it? (y/n)” appears. Enter Y (yes).
Step 2  At the command prompt, when the message “Perform r/w tests (takes very long time) on target disks? (y/n)” appears, enter Y (yes).

Note  The default action is taken if you do not immediately respond to the message prompts.

Step 3  After the software is copied and the CD-ROM drive is mounted, you are prompted to enter the System Administrator Account Setup. At the Enter the password for “admin”: prompt, enter the password. At the Confirm the password for “admin”: prompt, reenter the password.

Step 4  Enter the HA role at the prompt Enter HA role [standalone/primary/secondary].

Note  We recommend that you create a VSM HA pair. Configure the first VM as the primary VSM and install the second VM as the secondary VSM.

If you set the HA role as secondary, the following question is displayed at the prompt: Setting HA role to secondary will cause a system reboot. Are you sure (yes/no)?: Enter Yes if you want to set the HA role to Secondary.

Step 5  At the prompt, enter the domain ID: Enter the domain ID[1-1023]; for example, 199. A domain ID is required for the VSMs to communicate with each other. While installing the secondary VSM, enter the same domain ID that was specified for the primary VSM.

Step 6  After step 5 for secondary VSM, the message is displayed: saving boot configuration and the system reloads.

Step 7  At the prompt, the Basic System Configuration Dialog is displayed. Enter Yes at the prompt.

Step 8  At the command prompt, the following message is displayed: Create another login account? [yes/no] (n). Select No to skip creating another login account.

Note  The defaults are used if you do not change the values.

Step 9  Enter the switch name; for example, Nexus1000V-Eng.

Step 10 Press Y for yes when prompted to continue with the out-of-band management configuration.

Step 11 Enter the Mgmt0 IPv4 address for the VSM; for example, 10.10.10.4.

Step 12 Enter the Mgmt0 IPv4 netmask; for example, 255.255.255.0.

Step 13 At the command prompt, the following message is displayed: Configure the default gateway? Enter Y for yes.

Step 14 Enter the IPv4 address of the default gateway; for example, 10.10.10.5.

Step 15 At the command prompt, the following message is displayed: Vem feature level will be set to 5.2(1)SM3(1.1). Do you want to reconfigure? (yes/no) [n]: Press Enter at the prompt to enter the default value.

Step 16 Enter n when the following command prompt message is displayed: Configure Advanced Options? (yes/no)[n]:.

Step 17 The following message is displayed: Would you like to edit the configuration? (yes/no) [n]: Press Enter at the prompt to enter the default value.

Step 18 Enter y when the following command prompt message is displayed: Use this configuration and save it? (yes/no) [y]:.

Step 19 Complete steps 1 to 5 to configure the secondary VSM with an HA role.
Step 20 Verify the HA role using the command `show system redundancy status` on primary and secondary VSMs.

Configuring the VSM

After completing these steps, you are prompted to log into the VSM. Access the VSM via SSH using the IP address configured in the VSM installation section. The following minimal objects need to be created on the VSM:

- Logical network
- Network segment pool
- IP pool template
- Network segment
- Virtual Ethernet port profile
- Ethernet port profile
- Network uplink

To configure the VSM, perform the following steps:

Step 1 Enter the configuration mode using the command `config t`.

Step 2 Create a logical network using the command `nsm logical network <name>` at the prompt to configure the SCVMM networking fabric; for example, `nsm logical network Intranet`. Type `exit`. You can enter any name for the logical network.

Step 3 Create a network segment pool using the command `nsm network segment pool <name>`; for example, `nsm network segment pool IntranetSJ`.

Step 4 Associate the network segment pool to the logical network using the command `member-of logical-network <name>`; for example, `member-of logical-network Intranet`. Type `exit`.

Step 5 Create an IP pool template using the command `nsm ip pool template <name>`; for example, `nsm ip pool template pool10`.

Step 6 Configure the IP address range and network IP address range using the commands, for example, `ip address <30.0.0.2> <30.0.0.100>` and `network <30.0.0.2> <255.255.255.0>`. Type `exit`.

Step 7 Create a network segment using the command `nsm network segment <name>`; for example, `nsm network segment VMNetworkA`.

Step 8 Create a VLAN inside the network segment using the command `switchport access vlan <number>`; for example, `switchport access vlan 100`.

Step 9 Associate the network segment pool to the network segment using the command `member-of network segment pool <name>`; for example, `member-of network segment pool IntranetSJ`.

Step 10 (Optional) Import the IP pool template to the network segment. Specify the IP subnet using the commands `ipsubnet [CIDR notation]` and `ip pool import template [name]`. For example:

`ip subnet 30.30.30.0/24`;
`ip pool import template pool10`

Note The IP subnet should be the same as the network specified in the `ip pool template` command.
Step 11  Publish the network segment using the command `publish network segment <name>`; for example, `publish network segment VMNetworkA`. Type `exit`.

Step 12  Create a virtual Ethernet port profile using the command `port-profile type vethernet <name>`; for example, `port-profile type vethernet Veth-policy`.

Step 13  Enter the `no shutdown` command to keep the system in a power-on state. Enter `state enabled` at the prompt.

Step 14  Publish the port profile using the command `publish port-profile` and type `exit`. The port profile is imported for publishing the network uplink.

Step 15  Create a virtual Ethernet port profile using the command `port-profile type ethernet <name>`; for example, `port-profile type ethernet eth-pp-policy`.

Step 16  Enter the `no shutdown` command to keep the system in a power-on state. Enter `state enabled` at the prompt.

Step 17  Create a network uplink using the command `nsm network uplink NexusUplink`.

Step 18  Associate the network segment pool using the command `allow network segment pool IntranetSJ`; for example, `allow network segment pool IntranetSJ`.

Step 19  Import the port profile that was created earlier using the command `import port-profile <name>`; for example, `import port-profile eth-pp-policy`.

Step 20  Publish the network uplink using the command `publish network uplink <name>`; for example, `publish network uplink NexusUplink`. Type `exit`.

Step 21  Copy the running configuration to the start-up configuration using the command `copy running-config startup-config`. The following message is displayed in the window: “Copy complete, now saving to disk (please wait)"

Step 22  Enter the command `show running-config` to verify the configuration.

**Note**  The setup script configures the VSM to function in L3 control mode. L2 control mode is not supported with Cisco Nexus 1000V for Microsoft Hyper-V. When configuring L3 control with Microsoft Hyper-V, you do not need to create a port profile with L3 control.

---

### Configuring the SCVMM Fabric Workflow

**Note**  The entire workflow to configure the SCVMM fabric can also be performed using scripts. For more information, see [PowerShell Scripts for Configuring the SCVMM Fabric Workflow](#).

To install and configure the VSM workflow, create a Microsoft switch for VSM connectivity and then perform the following steps:

1. Connecting SCVMM to VSM, page 1-12.

### Connecting SCVMM to VSM

Once the VSM is up, configure the SCVMM networking fabric for the Cisco Nexus 1000V.
Chapter 1 Installing the Cisco Nexus 1000V

Installing the VSM Software

**Note** Check and turn off the proxy server settings for your LAN in the Internet Options settings window of Internet Explorer before proceeding to the next steps.

**Connecting SCVMM 2012-R2 to VSM**

To retrieve the objects from the VSM to SCVMM 2012 R2, perform the following steps:

**Step 1** When the VSM is up, log in to the VSM using SSH and the IP address configured in the previous section.

**Step 2** From the SCVMM administrator console, navigate to the **Fabric** pane.

**Step 3** Under **Networking**, select **Network Service**.

**Step 4** Right-click to add a **Add Network Service**. The **Add Network Service** wizard is displayed.

**Step 5** Enter a name for the Network Service and click **Next**. In the description, mention that it is a virtual switch extension.

**Step 6** Step 6: In the **Manufacturer and Model** window, select the settings as outlined in the following steps:

a. Select a manufacturer, for example, *Cisco Systems, Inc*.

b. Select the model type, for example, *Nexus 1000V Chassis 2.0*.

**Step 7** Step 7: In the next window, select **Run As Account**.

**Step 8** In the **Run As account** field, click **Browse**. The **Select a Run As Account window** opens.

a. In the **Select a Run As Account** window, select an account from the available options or click the **Create Run As account** tab to create an account for the VSM. A **Create Run As account** window opens.

b. In the **Create Run As account** window, enter the following VSM credentials:

   - Enter the name of the account in the **Name** field as *VSM_admin*.

   - Enter the description of the account in the **Description** field.

   - Enter the user name in the **User Name** field and the password in the **Password** field.

   - Confirm the password in the **Confirm password** field.

   - Uncheck the **Validate Domain Credentials** box as the Active Directory cannot be validated with the credentials.

   - Click **OK**.

   - The new account, for example, *VSM_admin* is displayed in the **Select a Run As Account** window. This is a one-time procedure for the VSM.

   - Select the new account and click **OK** in the **Select a Run As Account** window.

**Step 9** Enter the IP address of the VSM in the connection string, for example, http://10.10.10.4. To use HTTPS, see **Installing the VSM Certificate**, page 1-16.

**Step 10** In the Providers window, choose the provider as *Cisco Systems Nexus 1000V* and click **Test**. This verifies the communication between the Cisco VSM and the SCVMM.

**Step 11** In the Host Groups panel, select a few or all the host groups that can use the virtual switch extension manager and click **Next**.

**Step 12** In the Summary panel, confirm the settings and click **Finish**.
Once the Virtual Network Service has been successfully added, it is listed in the main window in the SCVMM user interface at the path: Fabric > Networking > Network Service.

Creating a Logical Switch in SCVMM

Once the Virtual Switch Extension Manager has been added, create a logical switch on VMM. Define the extensions and port profiles for the logical switch, create classifications that contain the native port profile and a port profile for each extension as outlined in the following steps.

To create a logical switch, perform the following steps:

**Step 1**

In the SCVMM user interface, under Networking, right-click Logical Switches and then click Create Logical Switch. The Create Logical Switch wizard appears.

**Step 2**

The Getting Started panel opens. Review the instructions and click Next.

**Step 3**

In the General panel, add a name and the description for the logical switch in the Name and Description fields; for example, N1000V_Test.

**Step 4**

Click Next.

**Step 5**

In the Extensions panel, the virtual switch extensions are listed. Choose the extension that you created in the previous steps. This is listed as a forwarding extension. Do not change any selections of the auto-selected extensions.

**Step 6**

Click Next.

**Step 7**

In the Uplink panel, specify the uplink port profiles that are part of this logical switch. The uplink port profiles are available for use on the hosts where an instance of the logical switch is created.

- Choose Team in the Uplink mode field to select multiple uplinks.

**Note**

Even if you use a single uplink or multiple uplinks, the mode should always be Team.

- In the Uplink port profiles field, click Add. The Add Uplink Port Profile window opens. Select a port profile that is available for use by the host physical adapter that connects to this logical switch.

- Click Next.

**Step 8**

In the Virtual Port panel, click Add. The Add Virtual Port window opens.

- Choose the VSM by checking the name that was created earlier; for example, Nexus 1000v-Test.

- Select the port profile from the drop-down menu.

- Select a port profile classification for the port profile; for example, AllAccess1.

- Click Browse in the Port Classification field. Assign the selected port profile to a port classification in the Select a Port Profile Classification window.

- Click Create Port Classification. The Create Port Classification wizard opens. Enter the name for the port profile classification in the Name field; for example, AllAccess1. Enter the description for the port profile classification in the Description field.

- Click OK. The selected port classification is displayed in the Select a Port Profile Classification window.

- Choose the port classification from the table.
Installing the VSM Software

Step 9 Click OK to finish adding the Virtual Port.

Step 10 Click Next to close the Create Logical Switch wizard.

Step 11 In the Summary panel, confirm the settings and click Finish. Now the logical switch is created.

The defined configuration is available on every host that uses the logical switch and the hosts, virtual switches, and virtual machines remain in compliance with their associated logical switch.

Note If you want to add more port profiles to the VSM, you must configure the properties again. All the hosts should be configured for multiple uplinks. To update the properties and add more uplink port profiles, right-click the logical switch in the SCVMM user interface and click Properties.

Configuring the VM Network

Once the logical switch and the hosts are configured, complete the following steps to configure the VMs and associate the network segments to the VMs.

Step 1 Click VMs and Services in the left navigation panel of the SCVMM user interface.

Step 2 Click VM Networks. Right-click and select the Create VM Network option. The Create VM Network wizard opens.

Step 3 In the Name panel, specify the name for the VM network in the Name field. Enter the description for the VM network in the Description field. For example, add a name for the VM network as VM_network. If the name is same as the network-segment name, it is easy for the customers to do the mapping.

Step 4 Select the Logical Network which is created on the VSM.

Step 5 Click Next.

Step 6 To configure VM network in SCVMM 2012 R2, do the following:

a. In the Isolation panel, select the Network manager in which is the logical switch was created.

b. Click Next.

c. In the Isolation options panel, select Specify an externally supplied VM network to configure the isolation externally. Confirm the External VM Network that was previously created; for example, VM_Network.

Step 7 Click Next.

Step 8 In the Summary panel, confirm the settings, and click Finish.

The new VM network is displayed in the VM Networks and IP Pools panel in the SCVMM user interface.
Installing the VSM Certificate

To enable HTTPS communication between the Cisco Nexus 1000V for Microsoft Hyper-V VSM software and the SCVMM server, you must first install the Cisco Nexus 1000V for Microsoft Hyper-V VSM certificate. You can install this certificate either manually or using a script.

Installing the VSM Certificate Manually

To install the Cisco Nexus 1000V for Microsoft Hyper-V VSM software certificate, perform the following steps:

**Step 1** From the SCVMM Server, open Internet Explorer, and connect to the VSM using https://vsm-ip. The Certificate Error window opens.

**Step 2** Choose the Continue to this website option. The Cisco Nexus 1000V window opens.

**Step 3** Select the Certificate Error link that is available on the address bar of the same window.

**Step 4** From the Untrusted Certificate dialog box click View Certificates. The Cisco Nexus 1000V VSM certificate appears.

**Step 5** Click the Install Certificate button. The Certificate Import wizard opens.

**Step 6** Choose Local Machine as the installation location and click Next.

**Step 7** Based on the VM settings, a popup window for the User Account Control (UAC) may open.

**Step 8** On the next window, select the Place all certificates in the following store option and click Browse.

**Step 9** Choose the Trusted Root Certification Authorities option available on the certificate store and click OK.

**Step 10** Click Next on the Certificate Import wizard.

**Step 11** Review the summary on the final window and Select Finish. This completes the importing of the certificate.

**Step 12** Press OK on the Certificate Import wizard.

**Step 13** Press OK on the Certificate window.

Installing the VSM Certificate Using a Script

Use the following PowerShell script to install the VSM certificate:

```
Install-Nexus1000V-VSMCertificate.ps1
```

This script is available at the following location on the SCVMM server:

```
%ProgramFiles%\Cisco\Nexus1000V\V2\Scripts\VMMConfig example "C:\Program Files\Cisco\Nexus1000V\V2\Scripts\VMMConfig"
```
PowerShell Scripts for Configuring the SCVMM Fabric Workflow

After the Cisco VSM Provider (Nexus1000V-NetworkServiceProvider-5.2.1.SM3.1.1.0.msi) is installed from the download package on the SCVMM server, the following scripts are available in %ProgramFiles%\Cisco\Nexus1000V\V2\Scripts\VMMConfig example "C:\Program Files\Cisco\Nexus1000V\V2\Scripts\VMMConfig":

- Deploy-Nexus1000V-VSEM.ps1
- Refresh-Nexus1000V-VSEM.ps1
- Install-Nexus1000V-VSMCertificate.ps1
- Cleanup-Nexus1000V-VSEM.ps1

Deploy-Nexus1000V-VSEM.ps1

This script handles the following operations that you would need to do on the SCVMM server:

a. Add extension manager/network service.

b. Create a logical switch.

c. Associate Cisco uplink port profiles with the logical switch (created in step b).

d. Associate virtual port profiles with the logical switch (created in step b).

e. Create VM networks from Cisco published network segments.

Below is a sample run:

```
PS C:\Program Files\Cisco\Nexus1000V\Scripts\VMMConfig> .\Deploy-Nexus1000V-VSEM.ps1
### SCRIPT NAME: Deploy-Nexus1000V-VSEM.ps1
### VERSION: 1.1
### DESCRIPTION: This script will add a new Cisco Nexus1000V Extension to SCVMM and create the following SCVMM objects:
### 1. Extension Manager / Network Service.
### 2: Logical Switch.
### 3: Associate Uplink Port Profiles with Logical Switch.
### 4: Associate Virtual Port Profile with Logical Switch.
### 5: Create VMNetworks from Cisco published Network Segments.

Enter IP Address for the Nexus1000V VSM: 10.105.234.211
Enter Username for the Nexus1000V VSM: admin
Enter Password for the Nexus1000V VSM: ********
Enter Name of Logical Switch to be Created on SCVMM: Nexus-Logical-Switch
Enter Mode of communication between SCVMM and VSM (http/https): https
Importing Virtual Machine Manager Libraries ..

Deploying Cisco Nexus1000V Logical Switch:

VSM IP : 10.105.234.211
RUN-AS-ACCOUNT: CiscoVSM-10.105.234.211-1-23-14_12-44
HOSTGROUP: All Hosts
NAME: Cisco Systems Nexus 1000V
LOGICAL SWITCH NAME: Nexus-Logical-Switch
SCVMM VERSION: 3.2.7510.0

Adding Cisco Extension over 'https' with IP = 10.105.234.211
```
Installing the VSM Software

This may take a while depending on VSM configuration Size...
Cisco Switch Extension Manager Added Successfully to VMM-Server.

Creating Logical Switch 'Nexus-Logical-Switch'.
Logical Switch 'Nexus-Logical-Switch' Created Successfully

Populating Uplink Port Profile Sets for Logical Switch 'Nexus-Logical-Switch'.
1 : Uplink Port Profile Set ==> 'NexusUplink'

Populating Virtual Port Profile Sets and Classifications for Logical Switch 'Nexus-Logical-Switch'.
1 : Port Classification ==> 'Veth-policy'

Populating VM Networks for Logical Switch 'Nexus-Logical-Switch'.
INFO : List of VMNetworks Created (1):
1 : 'VMNetworkA'

Execution Complete!

Transcript stopped, output file is C:\Program Files\Cisco\Nexus1000V\Scripts\VMMConfig\Deploy-Nexus1000V-VSEM-logs\Deploy-Nexus1000V-VSEM-1-23-14_12-44.log
PS C:\Program Files\Cisco\Nexus1000V\Scripts\VMMConfig>

Refresh-Nexus1000V-VSEM.ps1

Use this script if the Cisco VSEM is already added to the SCVMM server and you need to configure new objects such as port profiles, network segments, or uplink networks on the VSM. You may also need to refresh the Cisco VSEM to associate the Cisco Nexus 1000V objects on the SCVMM and make them available for usage.

This script helps you refresh the VSEM and make the necessary associations.

The following example creates a new VM network (VMNetworkB), a new port classification (Veth-policy-new), and a new uplink network (NexusUplink-New) on the Cisco VSM.

Note

The following were already created on the Cisco VSM as shown in Deploy-Nexus1000V-VSEM.ps1:

- Existing VM network (VMNetworkA)
- Existing port classification (Veth-policy)
- Existing uplink network (NexusUplink)

Below is a sample run:

PS C:\Program Files\Cisco\Nexus1000V\Scripts\VMMConfig> .\Refresh-Nexus1000V-VSEM.ps1
-VsmIP 10.105.234.211 -LogicalSwitch Nexus-Logical-Switch
############################################################################
## SCRIPT NAME: Refresh-Nexus1000V-VSEM.ps1
##
## VERSION: 1.1
## DESCRIPTION: This script will refresh an existing Cisco Nexus1000V Extension to SCVMM and create the following SCVMM objects:
## 1: Associate Uplink Port Profiles with Logical Switch.
## 2: Associate Virtual Port Profile with Logical Switch.
## 3: Create VMNetworks from Cisco published Network Segments.

Importing Virtual Machine Manager Libraries ..

---

Refresh Cisco Nexus1000V VSEM :
---

VSM IP : 10.105.234.211
HOSTGROUP: All Hosts
NAME: Cisco Systems Nexus 1000V
LOGICAL SWITCH NAME: Nexus-Logical-Switch
SCVMM VERSION: 3.2.7510.0

---

Retrieve Cisco Extension with IP = 10.105.234.211
---

Cisco Switch Extension Manager with ip '10.105.234.211' is detected on this VMM server.
Reading Cisco Switch Extension Manager now...

---

Retrieving Logical Switch 'Nexus-Logical-Switch'.
---

Logical Switch 'Nexus-Logical-Switch' with extension ip '10.105.234.211' was detected on this VMM server.

---

Populating Uplink Port Profile Sets for Logical Switch 'Nexus-Logical-Switch'.
---

1 : Uplink Port Profile Set ==> 'NexusUplink-New'

---

Populating Virtual Port Profile Sets and Classifications for Logical Switch 'Nexus-Logical-Switch'.
---

1 : Port Classification ==> 'Veth-policy-new'

---

Populating VM Networks for Logical Switch 'Nexus-Logical-Switch'.
---

INFO : List of VMnetworks Created (1):

1 : 'VMNetworkB'

---

Execution Complete!
---

Transcript stopped, output file is C:\Program Files\Cisco\Nexus1000V\Scripts\VMMConfig\Refresh-Nexus1000V-VSEM-logs\Refresh-Nexus1000V-VSEM-1-23-14_12-54.log

Install-Nexus1000V-VSMCertificate.ps1
This script is used to install the Cisco Nexus1000V VSM certificate on the SCVMM server. This certificate is required to establish an HTTPS connection between the SCVMM server and the VSM.
Installing the VSM Software

Below is a sample run:

```
PS C:\Program Files\Cisco\Nexus1000V\Scripts\VMMConfig>.
\Install-Nexus1000V-VSMCertificate.ps1 -ip 10.105.234.211
True
```

The script returns "True" for a successful install.

**Cleanup-Nexus1000V-VSEM.ps1**

This script is used to perform a cleanup of the Cisco Nexus 1000V components available on the SCVMM server.

This script exits if it encounters any Cisco Nexus 1000V objects.

**Preparing the Microsoft Hyper-V Hosts (Optional)**

Before you add hosts to the logical switch, you can prepare the Microsoft Hyper-V hosts. This step is optional.

**Configuring the MTU with the Cisco Nexus 1000V**

In Microsoft Hyper-V, the VSM does not manage the Maximum Transmission Unit (MTU) setting of VM NIC or physical adapters. All physical adapters added to the Cisco Nexus 1000V switch should have the same MTU configured and the PNIC MTU should not be changed after it is added to the switch.

To configure the MTU, perform the following steps:

1. **Step 1** Open *View Network Connections* from the Server Manager or Control Panel or by typing ncpa.cpl from a command line.
2. **Step 2** Right-click the adapter and choose *Properties*.
3. **Step 3** Click *Configure* under the *adapter properties* window.
4. **Step 4** Click the *Advanced* tab.
5. **Step 5** Under *Property*, click *Jumbo Packet* and set the desired value.

Repeat this procedure for all adapters that are added to Cisco Nexus 1000V logical switch.

---

**Note** Certain adapters allow the MTU change only through their own adapter manager. For example, the MTU of the Cisco VIC cards can be changed through the UCSM or ILO.

---

**VMQ Processor Configuration with the Cisco Nexus 1000V**

VMQ allows the network traffic received on an adapter to be spread over multiple CPU cores which provides better performance. The following two factors are important in determining if the VMQ operates correctly:

- The receive side scaling (RSS) CPU number determines the lowest CPU core that can be used by RSS.
**Note** Changing the RSS registry is a disruptive operation and causes the Ethernet adapter to flap.

The Cisco Nexus 1000V supports the following port-channel operational modes: Link Aggregation Control Protocol (LACP) and vPC.

The LACP utilizes the same Subgroup id for all the members of a port-channel. The RSS Base CPU and Max RSS Processors should be configured with same value for all member ports.

MAC pinning/manual pinning port-channel use multiple subgroup IDs within the members of the port-channel. Therefore, the RSS Base CPU and Max RSS processors should be configured so that the same CPU core is not used by multiple NICs.

**Changing the RSS Registry**

To change the RSS registry, perform the following steps:

1. Open **View Network Connections** from the Server Manager or Control Panel or by typing ncpa.cpl from a command line.
2. Right-click the adapter and choose **properties**.
3. Under the **Adapter Properties** window, click **Configure**.
4. Click the **Advanced** tab.
5. Click **Maximum Number of RSS Processor** and enter a value.
6. Click **Starting RSS CPU** and enter a value.

Repeat this procedure for all the adapters that you want VMQ to be enabled on.

The RSS setting cannot be modified through the network connections for certain adapters. For those adapters, you must set the registry keys directly using the registry editor. Check the Microsoft documentation for information about changing the registry.

**Adding Hosts to a Logical Switch**

After a logical switch is created, you can update the properties of the logical switch.

1. In the left navigation pane, choose the server, under **Fabric** > **Servers** > **All Hosts**, right-click and choose **Properties**. The **Properties** window opens.
2. In the left navigation pane of the **Properties** window, click **Virtual Switches**.
3. In the **Virtual Switches** pane, in the **New Virtual Switches** field, click **New Logical Switch**. Choose the correct logical switch and physical adapters to assign to the logical switch. The module is added to Cisco Nexus1000V VSM.
Installing the Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide, Release 5.2(1)SM3(1.1)

Chapter 1  Installing the Cisco Nexus 1000V

Installing the VSM Software

Note
The MGMT PNIC can be added to the logical switch only when the switch is created. Adding it later results in a loss of host connectivity.

Step 4  Under the Physical Adapter header, choose a network adapter from the drop-down list in the Adapter field. In the Uplink Port Profile field, confirm the uplink port profile for the adapter.

Step 5  For port-channeling, click Add to add a second network adapter. Choose a different network adapter, confirm the uplink port profile, and click OK.

Note
Do not use the same port profile for both adapters. If you have configured the port channels, then you can use the same port-profile on both the adapters. Refer the NSM Configuration Guide for more details.

The Cisco Nexus 1000V package that was copied on the SCVMM is installed on the host.
We recommend that you create one logical switch per VSM.

Connecting the VM Network Adapter to the Logical Switch

To connect the VM network adapter to the Logical Switch, perform the following steps:

Step 1  Choose the VM network adapter.

Step 2  Choose the server on which the VM is installed in the SCVMM user interface. In the left navigation pane under VMs and Services > All Hosts, click the Hyper-V server. In the main window, right-click the virtual machine that you have created, and choose Properties.

Step 3  In the properties file, click Hardware Configuration in the left navigation pane.

Step 4  In the Hardware Configuration panel, choose NetWork Adapter.

Step 5  In the Network Adapter 1 pane on the right, choose Connected to a VM Network.

Step 6  Browse to find the VM network created in an earlier section.

Step 7  Click OK.

Step 8  In the Hardware Configuration pane, under Virtual Switch, choose the logical switch in the Logical Switch field. For the classification, choose the previously created port profile in the Classification field.

Note
If you set the default port profile earlier as outlined in Step 8 of Creating a Logical Switch in SCVMM, page 1-14. If you do not select a port classification for the logical switch in this window, the default port classification is applied to the logical switch.

Step 9  Click OK.

The Cisco Nexus 1000V for Microsoft Hyper-V installation is now complete.
Upgrading the 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.

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 2-1
- Licensing and Upgrade, 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**

- After upgrading to 5.2(1)SM3(1.1), the default evaluation license version 3.0 (Nexus 1000V Multi-Hypervisor License) is checked out.

- After upgrading to 5.2(1)SM3(1.1), the evaluation license version 1.0 (Nexus 1000V Multi-Hypervisor License) is still in use. You can request an upgrade to an evaluation license version 3.0.

- After upgrading to 5.2(1)SM3(1.1), the permanent license version 1.0 (Nexus 1000V Multi-Hypervisor License) is still in use. You can request an upgrade to a permanent license version 3.0.
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 2-4.
   - To upgrade the VSEM, see Upgrading the Cisco VSEM to the Current Release, page 2-12.
2. You have already obtained a copy of the VEM software file.
3. You have Windows Server 2012 R2 hosts with Microsoft Hotfix KB3014795 applied. For more information, see http://support.microsoft.com/kb/3014795/en-us.

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

<table>
<thead>
<tr>
<th>If you are running this configuration</th>
<th>Follow these steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2(1)SM1(5.2) and later with the following:</td>
<td></td>
</tr>
<tr>
<td>- SCVMM 2012 R2 UR4 and later</td>
<td></td>
</tr>
<tr>
<td>- Windows Server 2012 R2 hosts</td>
<td></td>
</tr>
<tr>
<td>Release 5.2(1)SM1(5.2) and later with the following:</td>
<td></td>
</tr>
<tr>
<td>- SCVMM 2012 R2 UR4 and later</td>
<td></td>
</tr>
<tr>
<td>- Windows Server 2012 R2 hosts or Windows Server 2012 hosts</td>
<td></td>
</tr>
<tr>
<td>Release 5.2(1)SM1(5.1) and later with the following:</td>
<td></td>
</tr>
<tr>
<td>- SCVMM 2012 (SP1) UR3 and later</td>
<td></td>
</tr>
<tr>
<td>- Windows Server 2012 hosts</td>
<td></td>
</tr>
</tbody>
</table>

Preparation SCVMM and Windows Server Hosts

Before upgrading to Cisco Nexus 1000V Release 5.2(1)SM3(1.1), ensure that the target environment has Windows 2012 R2 hosts managed by SCVMM 2012 R2. Additionally, make sure that all relevant patches from Microsoft are installed on Windows hosts.

If SCVMM 2012 SP1 is installed, then you need to upgrade it to SCVMM 2012 R2.

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

If the target setup consists of Windows Server 2012 host, you must uninstall VEM before proceeding.

- To upgrade host to Windows Server 2012 R2, see Upgrading Windows Server 2012 Hosts to 2012R2, page 2-4.
Upgrading SCVMM 2012 SP1 to SCVMM 2012 R2

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


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 previous 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 Hosts to 2012R2

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.


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**

- 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
- VSM upgrade complete

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.

```bash
switch# dir bootflash:
...
Usage for bootflash://
485830656 bytes used
1109045248 bytes free
1594875904 bytes total
```
Upgrading VSM to the Current Release

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.SM3.1.1.bin
bootflash:n1000vh-dk9.5.2.1.SM3.1.1.bin
switch# copy tftp://10.106.196.163/n1000vh-dk9-kickstart.5.2.1.SM3.1.1.bin
bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.1.1.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.SM3.1.1.bin system
bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.1.1.bin
```

Step 9
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 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.SM3.1.1.bin system bootflash:n1000vh-dk9.5.2.1.SM3.1.1.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` command.

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.SM3.1.1.bin bootflash:n1000vh-dk9.5.2.1.SM3.1.1.bin
switch# copy tftp://10.106.196.163/n1000vh-dk9-kickstart.5.2.1.SM3.1.1.bin bootflash:n1000vh-dk9-kickstart.5.2.1.SM3.1.1.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.SM3.1.1.bin system
bootflash:n1000vh-dk9.5.2.1.SM3.1.1.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.SM3.1.1.bin system
bootflash:n1000vh-dk9.5.2.1.SM3.1.1.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` 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)#
```
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.SM3.1.1.0.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.
   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.
   c. In the Results pane, right-click Cisco Systems Nexus 1000V extension and choose Refresh.

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 2-4.
- Upgrade the VSEM—see Upgrading the Cisco VSEM to the Current Release, page 2-12.

Upgrade Workflow

Figure 2-4 displays the VEM upgrade workflow using the WSUS server.
Upgrading the VEM Software to the Current Release

Chapter 2  Upgrading the Cisco Nexus 1000V

Figure 2-4  Cisco Nexus 1000V VEM Upgrade Workflow

1. Download Cisco Nexus1000V Package

2. Prepare Windows Server Update Services Server (WSUS)
   2.1 Enable and configure Windows Server Update Services Role on a Windows 2012 machine
   2.2 Install System Center Update Publisher 2012 (SCUP)
   2.3 Generate a Self Signed WSUS Certificate using SCUP
   2.4 Copy Cisco VEM MSI on WSUS Server
   2.5 Publish the MSI to WSUS Server using PowerShell Scripts part of Cisco Nexus1000V Package

3. Prepare Active Directory
   3.1 Import the WSUS Certificate in Active Directory
   3.2 Make necessary Group policy changes to include WSUS Certificate.
   3.3 Point to Local Windows Update Server and accept signed certificates.

4. Configure SCVMM
   4.1 Add WSUS Server to SCVMM
   4.2 Create baseline and Include the Cisco MSI Published
   4.3 Apply baseline on the Cluster/Hosts to be Upgraded

5. Check Compliance and Perform VEM Upgrade
   5.1 Perform Compliance Check on the Hosts from SCVMM.
   5.2 Put Hosts in Maintenance Mode.
   5.3 Remediate from SCVMM and make the Hosts Complaint.
   5.4 Bring the Host out of Maintenance Mode.
   5.5 Perform a second remediate to enable Cisco Extension on the Hosts after upgrade.
Upgrading the VEM Software Using WSUS Server

**Summary Steps**


**Upgrading the VEM Software Using WSUS Server**

**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 2012 machine.

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

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

a. Run the SCUP 2011 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:

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.

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

```powershell
PS C: > \Publish-CiscoUpdate.ps1 .\Nexus1000V-VEM-5.2.1.SM3.1.1.0.msi
Starting Publish-CiscoUpdate...
-------------- MSI File Info --------------
Pkg File Name : Nexus1000V-VEM-5.2.1.SM3.1.1.0.msi
Pkg Full Path : C:\Users\Administrator.LAB\Desktop\WSUS\Nexus1000V-VEM-5.2.1.SM3.1.1.0.msi
Pkg Dir : C:\Users\Administrator.LAB\Desktop\WSUS
Pkg Name : Nexus1000V-VEM-5.2.1.SM3.1.1.0
--------------
Reading MSI Properties...
------------- MSI Details ---------------
MSI : C:\Users\Administrator.LAB\Desktop\WSUS\Nexus1000V-VEM-5.2.1.SM3.1.1.0.msi
ProductName : Cisco Nexus 1000V Series Switch
Description : Cisco Nexus 1000V Series Switch
Manufacturer : Cisco Systems, Inc.
ProductVersion : 3.00.000
ProductCode : {1C17F17E-34F5-4E6B-901C-FA229EB367E4}
UpgradeCode : {D1099B98-17BE-40F2-A10E-29D48B9A5829}
DriverID : {9C8ED422-F33A-4F34-B771-EBB8D0539FD3}
DriverVersion : 301.100.0.0
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.SM3.1.1.0.msi to WSUS Server.
```

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

```powershell
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
```
Preparing the Active Directory

**Step 1**  Copy the previously exported certificate that was exported earlier (see step 4)) 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 the 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-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**. 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** 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 2** Put the noncompliant host to maintenance mode and perform remediation:

a. Put the noncompliant host in maintenance mode by referring to the following link:


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

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

Step 4 Perform another remediation to bring the host online in VSM:

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 5 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(1.1).

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

Upgrading the VEM Software Using a Script

Step 5 of Upgrade Workflow, page 2-13 is performed by this script.

Note Steps 1 to 4 of Upgrade Workflow, page 2-13 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

Below is a sample snapshot of the VEM upgrade script:
Chapter 2  Upgrading the Cisco Nexus 1000V

Upgrading the VEM Software to the Current Release

PS C:\Program Files\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade> .\Upgrade-Nexus1000V-VEM.ps1 -BaseLineName b190 -ClusterName infraset5 -LogicalSwitchName nexus1000v

###############################################################################
## 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 - 'b190'

-------------------------------------------------------

Update 1 => Cisco Nexus 1000V Series Switch [MSI: 3.00.000] [Driver: 301.100.0.0]

Starting Compliance Scan on Cluster before Upgrade 'infraset5' with baseline 'b190'

HOSTNAME = hyperv04: STATUS = NonCompliant: Nexus1000V Version = 1.01.200
HOSTNAME = hyperv05: STATUS = NonCompliant: Nexus1000V Version = 1.01.200
HOSTNAME = hyperv09: STATUS = NonCompliant: Nexus1000V Version = 1.01.200
HOSTNAME = hyperv10: STATUS = NonCompliant: Nexus1000V Version = 1.01.200

STARTING UPGRADE ON HOST: hyperv04

STEP 1.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster
NOTE: This may take a while, '0' 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: hyperv05

STEP 2.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster
NOTE: This may take a while, '14' 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 UPGRADE ON HOST: hyperv09

STEP 3.1 : Enabling Maintenance Mode and migrating VM's to suitable host in Cluster
NOTE: This may take a while, '13' VM's are being migrated, and 0 VM's are being saved!!
STEP 3.2: Starting Update Remediation

STEP 3.3: Stopping Maintenance Mode

---------------------------------------------------------------------------
STARTING UPGRADE ON HOST: hyperv10
---------------------------------------------------------------------------
STEP 4.1: Enabling Maintenance Mode and migrating VM’s to suitable host in Cluster
NOTE: This may take a while, '13' VM's are being migrated, and 0 VM's are being saved!!

STEP 4.2: Starting Update Remediation

STEP 4.3: Stopping Maintenance Mode

---------------------------------------------------------------------------
Starting Compliance Scan on Cluster after Upgrade 'infraset5' with baseline 'b190'
---------------------------------------------------------------------------
HOSTNAME = hyperv04 : STATUS = Compliant : Nexus1000V Version = 3.00.000
HOSTNAME = hyperv05 : STATUS = Compliant : Nexus1000V Version = 3.00.000
HOSTNAME = hyperv09 : STATUS = Compliant : Nexus1000V Version = 3.00.000
HOSTNAME = hyperv10 : STATUS = Compliant : Nexus1000V Version = 3.00.000

---------------------------------------------------------------------------
Nexus1000V VEM Upgrade Complete
---------------------------------------------------------------------------
Windows PowerShell transcript end
End time: 20141201111052
**********************************************************

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(1.1).

Upgrading the VEM Software Manually from Cisco Nexus 1000V Release 5.2(1)SM1(5.2) or Later to 5.2(1)SM3(1.1)

---


Step 2 Copy the VEM MSI file (for example, Nexus1000V-VEM-5.2.1.SM3.1.1.0.msi) to the host.

Step 3 Run the MSI file to install.

Step 4 RemEDIATE the host to make it available online in VSM:
   a. Launch the SCVMM.
   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.
---
Performing Post Upgrade Operations

This section contains:

- Changing the Feature Support Level, page 2-22
- Installing the Windows Patch, page 2-23

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(1.1)
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)SM1(5.2)
2 5.2(1)SM3(1.1)
```

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(1.1)
n1000v#
```

### Installing the Windows Patch

Install Microsoft hotfix KB3014795 on Windows Server 2012 R2 hosts. For more information, see [http://support.microsoft.com/kb/3014795/en-us](http://support.microsoft.com/kb/3014795/en-us).
Installing a VSM on the Cisco Cloud Services Platform

You can install the Cisco Nexus 1000V VSM on the Cisco Cloud Services Platform. For more information, see the documentation at http://www.cisco.com/en/US/products/ps12752/index.html.

**Note**

Layer 3 mode is supported for the Cisco Nexus 1000V for Hyper-V.

**Before You Begin**

Copy the ISO file to the boot flash:repository/ of the virtual service blade as displayed in the following example:

```
switch(config)# dir boot flash:repository
16384 Feb 21 11:31:10 2013 lost+found/
169932800 May 08 20:20:09 2013 Nexus-1000V.5.2.1.SM3.1.1.iso
653 May 08 20:28:24 2013 vmpresults.txt
Usage for bootflash://sup-local
326832128 bytes used
3664547840 bytes free
3991379968 bytes total
switch(config)#
```

**Procedure**

Complete the following steps to install the VSM on the Cloud Services Platform:

**Step 1**

Create a virtual service blade by entering the following commands:

```
switch(config)# show virtual-service-blade summary
Name        HA-Role       HA-Status     Status               Location
---------------------------------------------------------------------------------
switch(config)# virtual-service-blade vsm-1
switch(config-vsb-config)# virtual-service-blade-type new Nexus-1000V.5.2.1.SM3.1.1.iso
switch(config-vsb-config)# show virtual-service-blade summary
Name        HA-Role       HA-Status     Status               Location
---------------------------------------------------------------------------------
vsm-1        PRIMARY       NONE          VSB NOT PRESENT          PRIMARY
```

```
### Step 2
Configure the control and packet VLANs for static and flexible topologies. Note that no provisioning is allowed for a management VLAN because the management class interface uses the management VLAN of the Cisco Cloud Services Platform.

```console
switch(config-vsb-config)# interface control vlan 391
switch(config-vsb-config)# interface packet vlan 392
```

### Step 3
Configure the Cisco Nexus 1000V on the Cisco Cloud Services Platform.

```console
switch(config-vsb-config)# enable
Enter vsb image: [Nexus-1000V.5.2.1.SM3.1.1.iso]
Enter domain id[1-1023]: 391
Management IP version [V4/V6]: [V4]
Enter Management IP address: 172.16.5.5
Enter Management subnet mask: 255.255.255.0
IPv4 address of the default gateway: 172.16.5.1
Enter HostName: vsm-1
Enter the password for 'admin': ********
Note: VSB installation is in progress, please use show virtual-service-blade commands to check the installation status.
```

### Step 4
Display the primary and secondary VSM status.

```console
switch(config-vsb-config)# show virtual-service-blade summary
```

### Step 5
Log in to the VSM.

```console
switch(config)# virtual-service-blade vsm-1
switch(config-vsb-config)# login virtual-service-blade vsm-1
Telnet escape character is '^\'.
Trying 172.1.0.18...
Connected to 172.1.0.18.
Escape character is '^\'.
```

---

<table>
<thead>
<tr>
<th>VSM-1</th>
<th>HA-Role</th>
<th>HA-Status</th>
<th>Status</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIMARY</td>
<td>none</td>
<td>VSB DEPLOY IN PROGRESS</td>
<td>PRIMARY</td>
<td></td>
</tr>
<tr>
<td>SECONDARY</td>
<td>none</td>
<td>VSB NOT PRESENT</td>
<td>SECONDARY</td>
<td></td>
</tr>
</tbody>
</table>

---

| switch# show system redundancy status
---

Redundancy role

```
administrative: primary
operational: primary
```
Redundancy mode
-------------
  administrative: HA
  operational: HA

This supervisor (sup-1)
----------------------
  Redundancy state: Active
  Supervisor state: Active
  Internal state: Active with HA standby

Other supervisor (sup-2)
-----------------------
  Redundancy state: Standby
  Supervisor state: HA standby
  Internal state: HA standby

switch#