Installing the Cisco Nexus 1000V Software

This chapter contains the following sections:

Installation Workflow

Steps to Install Cisco Nexus 1000V Manually

You can install Cisco Nexus 1000V manually. Use these high-level steps and the workflow diagram in the section to guide you through the installation process.

Procedure

Step 1 Make sure that all of the VMware prerequisites have been met.

For details, see the following sections:

- Supported VMware vSphere ESXi Hypervisor Versions, on page 3
- ESXi Host Prerequisites, on page 4

Step 2 Make sure that all of the Cisco Nexus 1000V prerequisites have been met.

For details, see the following sections:.

- VSM Prerequisites, on page 5
- VEM Prerequisites, on page 6
- Upstream Switch Prerequisites, on page 7

Step 3 Read and follow the guidelines and limitations for the Cisco Nexus 1000V.

For details, see Guidelines and Limitations for Installing the Cisco Nexus 1000V, on page 7.

Step 4 Make topology decisions and gather any necessary information.

For details, see Information Required for Installation, on page 9.

Step 5 Download the Cisco Nexus 1000V software.

Step 6 (Optional) Verify the authenticity of the Cisco Nexus 1000V image.

For details, see Verifying the Authenticity of the Cisco-Signed Image (Optional), on page 9

Step 7 Install the Virtual Supervisor Module (VSM) software from an ISO image, OVA image, or on a Cisco Nexus Cloud Services Platform.

For details, see one of the following sections:

- Installing the Software from the ISO Image, on page 10
- Installing the Software from an OVA Image, on page 14
- Installing a VSM on the Cisco Nexus Cloud Services Platform , on page 40

Step 8 If you installed the VSM software on a CSP, proceed to the next step. If you installed the VSM software on a VM using an ISO or OVA image, you need to establish the SVS connection and configure the VM startup and shutdown parameters.

For details, see Establishing the SVS Connection, on page 22 and Setting Virtual Machine Startup and Shutdown Parameters, on page 24.

Step 9 Add the VEM hosts to the Distributed Virtual Switch.

For details, see Adding VEM Hosts to the Cisco Nexus 1000V Distributed Virtual Switch, on page 25.

Step 10 If you want to install the VEM software on a stateless ESXi host, proceed to the next step. Otherwise, install the VEM software using VUM, the Cisco Nexus 1000VCLI, or the VMware ESXi CLI.

For details, see one of the following sections:

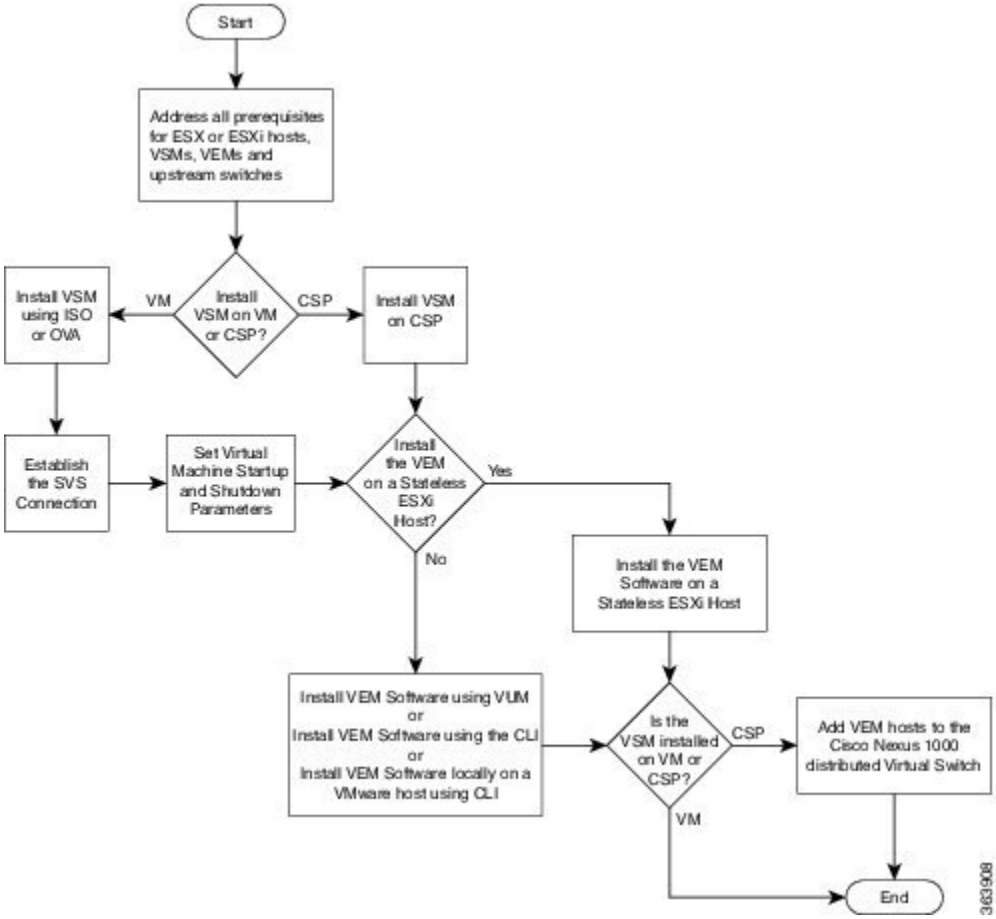
- Installing the VEM Software Using VUM, on page 29
- Installing the VEM Software Using the CLI, on page 29
- Installing the VEM Software Locally on a VMware Host Using the CLI, on page 29

Step 11 Install the VEM software on a stateless ESXi host.

For more details, see Installing the VEM Software on a Stateless ESXi Host, on page 31.

Process Flowchart for Installing the Cisco Nexus 1000V Manually

Use the procedures in this chapter and the following workflow as a guide to install the Cisco Nexus 1000V for VMware manually.



Supported VMware vSphere ESXi Hypervisor Versions

Cisco Nexus 1000V supports the following VMware vSphere ESXi Hypervisor versions:

- 6.5a
- 6.0
- 5.5

For information about installing or upgrading the VMware software, see Installing and Upgrading VMware.

See the following table for detailed compatibility information.

Note Do not install VMware vSphere 5.5 Patch 2702864 with Cisco Nexus 1000V. The VMware vSphere 5.5 Patch 2702864 is not supported on Cisco Nexus 1000V.

Table 1: VMware vSphere ESXi Hypervisor Software Compatibility Versions

VMware [1]	VIB [2]	VEM Bundle [3]	Windows VC Installer	Linux vCenter Server Appliance	VMware vSphere CLI	PowerShell CLI
ESXi 6.5a	cross_cisco-vem-v390-5.2.1.3.3.1.0-6.5.1.vib	VEM650-201903522119-BG-release.zip (Offline) VEM650-201903522119-BG (Online)	6.5a	6.5a	6.5a	6.5a
ESXi 6.0	cross_cisco-vem-v390-5.2.1.3.3.1.0-6.0.1.vib	VEM600-201903522113-BG-release.zip (Offline) VEM600-201903522113-BG (Online)	6.0	6.0	6.0	6.0
ESXi 5.5 [4]	cross_cisco-vem-vv390-5.2.1.3.3.1.0-3.2.1.vib	VEM550-201903522107-BG-release.zip (Offline) VEM550-201903522107-BG (Online)	5.5	5.5	5.5	5.5

1 Includes patches and updates.
2 VIB files are available at http://www.vmware.com/patch/download.
3 VMware bundled software updates require placing the host in maintenance mode.
4 Do not install the VMware vSphere 5.5 Patch 2702864. The VMware vSphere 5.5 Patch 2702864 is not supported on Cisco Nexus 1000V.

Prerequisites for Installing the Cisco Nexus 1000V

ESXi Host Prerequisites

ESX or ESXi hosts have the following prerequisites:

- You have already installed and prepared vCenter Server for host management using the instructions from VMware.
- You should have VMware vSphere Client installed.
- You have already installed the VMware Enterprise Plus license on the hosts.
- All VEM hosts must be running ESXi 5.0 or later releases.
- You have two physical NICs on each host for redundancy. Deployment is also possible with one physical NIC.
- If you are using a set of switches, make sure that the interswitch trunk links carry all relevant VLANs, including control and packet VLANs. The uplink should be a trunk port that carries all VLANs that are configured on the host.
- You must configure control and management VLANs on the host to be used for the VSM VM.

- Make sure that the VM to be used for the VSM meets the minimum requirements listed in the following table.
- All the vmnics should have the same configuration upstream.

Caution

- VSM hardware version 11 is not supported. See table below for supported versions.
- The VSM VM might fail to boot if RAM and CPU are not properly allocated. This document includes procedures for allocating RAM and setting the CPU speed.

The VSM VM might fail to boot if RAM and CPU are not properly allocated. This document includes procedures for allocating RAM and setting the CPU speed.

This table lists the minimum requirements for hosting a VSM.

Table 2: Minimum Requirements for a VM Hosting a VSM

VSM VM Component	Minimum Requirement
VSM Hardware Version	7 **Note** VSM hardware versions 7, 8, 9, and 10 are supported. VSM hardware version 11 is not supported.
Platform	64 bit
Type	Other 64-bit Linux (recommended)
Processor	2
RAM (configured and reserved)	4 GB[5]
NIC	3
SCSI Hard Disk	3 GB with LSI Logic Parallel adapter
CPU speed	2048 MHz[6]

[5] If you are installing the VSM using an OVA file, the correct RAM setting is made automatically during the installation of this file. If you are using the CD ISO image, see Installing the Software from the ISO Image, on page 10 to reserve RAM and set the memory size.

[6] If you are installing the VSM using an OVA file, the correct CPU speed setting is made automatically during the installation. If you are using the CD ISO image, see Installing the Software from the ISO Image, on page 10 to reserve CPU and set the CPU reservation.

VSM Prerequisites

The Cisco Nexus 1000V VSM software has the following are prerequisites:

- You have the VSM IP address.

- You have installed the appropriate vCenter Server and VMware Update Manager (VUM) versions.
- If you are installing redundant VSMs, make sure that you first install and set up the software on the primary VSM before installing and setting up the software on the secondary VSM.
- If you are using the OVA file for installation, make sure that the CPU speed is 2048 MHz or greater. If the CPU speed is less than 2048 MHz, then use ISO image for installation.
- You have already identified the HA role for this VSM from the list in the following table.

Table 3: HA Roles

HA Role	Single Supervisor System	Dual Supervisor System
Standalone (test environment only)	X	
HA		X

Note A standalone VSM is not supported in a production environment.

- You are familiar with the Cisco Nexus 1000V topology diagram that is shown in Topology for Layer 3 Control Mode.

VEM Prerequisites

The Cisco Nexus 1000V VEM software has the following prerequisites:

Note If VMware vCenter Server is hosted on the same ESXi host as a Cisco Nexus 1000V VEM, a VUM-assisted upgrade on the host will fail. You should manually VMotion the vCenter Server VM to another host before you perform an upgrade.

- When you perform any VUM operation on hosts that are a part of a cluster, ensure that VMware fault tolerance (FT) and VMware distributed power management (DPM) features are disabled for the entire cluster. Otherwise, VUM cannot install the hosts in the cluster.
- If the hosts are in ESXi stateless mode, enable the PXE booted ESXi host settings under **Home** > **Update Manager** > **Configuration** > **ESXi host/cluster**.
- You have a copy of your VMware documentation available for installing software on a host.
- You have already obtained a copy of the VEM software file.
- You have already downloaded the correct VEM software based on the current ESXi host patch level. For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.
- For a VUM-based installation, you must deploy VUM and make sure that the VSM is connected to vCenter Server.

Upstream Switch Prerequisites

The upstream switch from the Cisco Nexus 1000V has the following prerequisites:

- If you are using a set of switches, make sure that the interswitch trunk links carry all relevant VLANs, including the control and packet VLANs. The uplink must be a trunk port that carries all the VLANs that are configured on the host.
- The following spanning tree prerequisites apply to the upstream switch from the Cisco Nexus 1000V on the ports that are connected to the VEM.
  - On upstream switches, the following configuration is mandatory:

    On your Catalyst series switches with Cisco IOS software, enter the **spanning-tree portfast trunk** or **spanning-tree portfast edge trunk** command.

    On your Cisco Nexus 5000 series switches with Cisco NX-OS software, enter the **spanning-tree port type edge trunk** command.
  - On upstream switches we highly recommend that you enable Global BPDU Filtering and Global BPDU Guard globally.
  - On upstream switches, where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the **spanning-tree bpdu filter** and **spanning-tree bpdu guard**commands.

  For more information about spanning tree and its supporting commands, see the documentation for your upstream switch.
- Enter the following commands on the upstream switch:

```
show running interface interface number
interface GigabitEthernet interface number
 description description of interface
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN native VLAN
switchport trunk allowed vlan list of VLANs
switchport mode trunk

end
```

Guidelines and Limitations for Installing the Cisco Nexus 1000V

The Cisco Nexus 1000V software installation has the following configuration guidelines and limitations:

- Virtual machine hardware version 11 is not supported.
- Do not enable VMware fault tolerance (FT) for the VSM VM because it is not supported. Instead, Cisco NX-OS HA provides high availability for the VSM.
- The VSM VM supports VMware HA. However, we strongly recommend that you deploy redundant VSMs and configure Cisco NX-OS HA between them. Use the VMware recommendations for the VMware HA.
- Do not enable VM monitoring for the VSM VM because it is not supported, even if you enable the VMware HA on the underlying host. Cisco NX-OS redundancy is the preferred method.

- When you move a VSM from the VMware vSwitch to the Cisco Nexus 1000V DVS, the connectivity between the active and standby VSM might get temporarily lost. In that situation, both active and standby VSMs assume the active role.

  The reboot of the VSM is based on the following conditions:

  1. The number of modules attached to the VSM
     - If more modules are attached on one of the VSMs and there is no virtual channel (VC) connectivity on both VSMs, the VSM that has the smaller number of modules is rebooted.
     - If modules are attached to both VSMs and one of the VSMs has VC connectivity, the VSM without connectivity is rebooted.
  2. VC connectivity

     Note This option is invoked when the previous condition is not met.

     - If both VSMs have the same number of modules, the software makes a selection that is based on the VC connectivity status.

       For example, this action is taken if both VSMs have two modules attached or both VSMs have no modules attached.
  3. Last configuration change

     Note This condition is invoked when the previous two conditions are not met.

     - If both VSMs have the same number of modules and no VC connectivity, the VSM with the latest configuration remains active and the other VSM is rebooted.
  4. Last active VSM
     - If the previous three conditions are not met, the VSM that became active most recently is rebooted.

- If the VSM is moved from the VMware vSwitch to the Cisco Nexus 1000V DVS, we recommend that you configure port security on the VSM vEthernet interfaces to secure control/packet MAC addresses.
- To improve redundancy, install primary and secondary VSM VMs on separate hosts that are connected to different upstream switches.
- The Cisco Nexus 1000V VSM always uses the following three network interfaces in the same order as specified below:
  1. Control Interface
  2. Management Interface
  3. Packet Interface
- There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

- We recommend that you deploy the VMware vCenter server and VSM in the same physical data center. If you choose to deploy the vCenter server and VSM in different physical data centers, be aware of the following guidelines and limitations:
  - The VSM HA pair must be located in the same site as their storage and the active vCenter Server.
  - Layer 3 control mode is preferred.
  - If you are using Link Aggregation Control Protocol (LACP) on the VEM, use LACP offload.
  - Quality of Service bandwidth guarantees for control traffic over the DCI link.
  - Limit the number of physical data centers to two.
  - A maximum latency of 10 ms is supported for VSM-VSM control traffic when deployed across datacenters.
  - A maximum latency of 100 ms is supported for VSM-VEM control traffic for both L2 and L3 mode of deployments.
  - Cisco Nexus 1000V Release 5.2(1)SV3(1.1) and later supports deployments where vCenter and VSM are in different data centers, provided the number of hosts does not exceed 35 and the link latency does not exceed 200 ms. In these types of deployments, we recommend that you do not edit port profiles when the VSM and the vCenter are disconnected.
- We recommend that you monitor and install all the relevant patch applications from VMware ESX host server.

Information Required for Installation

Before installing the software, make topology decisions and gather any necessary information, as follows:

- Decide whether to deploy the VSM as a VM on a vSphere host or cluster or on a CSP.
- Decide whether to deploy in Layer 2 or Layer 3 control mode (Layer 3 control mode is recommended).
- For Layer 2 control mode, determine the control or packet VLANs that will be used.
- For Layer 3 control mode, decide whether the management and Layer 3 control ports will be unified or separate. If they will be separate, determine the IP address of the Layer 3 control port for each ESXi host.
- Determine the domain ID.
- Determine the management, subnet, and gateway IP addresses for the VSM.
- Determine the administrative password for the VSM.

Verifying the Authenticity of the Cisco-Signed Image (Optional)

- openssl
- base64

Before you install the Nexus1000v.5.2.1.SV3.4.1a.zip image, you have the option to validate the authenticity of it. In the zip file, there is a signature.txt file that contains a SHA-512 signature and an executable script that can be used to verify the authenticity of the Nexus1000v.5.2.1.SV3.4.1a.zip image.

Note Verifying the authenticity of an image is optional. You can still install the image without validating its authenticity.

Before you begin

You need to be running a Linux machine with the following utilities installed:

Procedure

Step 1 Copy the following files to a directory on the Linux machine:

- Nexus1000v.5.2.1.SV3.4.1a.zip

  signature.txt file
- cisco_n1k_image_validation_v_1_1 script

Step 2 Ensure that the script is executable.

Step 3 Run the script.

Nexus1000v.5.2.1.SV3.4.1a.zip

Step 4 Check the output. If the validation is successful, the following message displays:

Installing the Cisco Nexus 1000V Software Using ISO or OVA Files

Installing the VSM Software

Installing the Software from the ISO Image

Before you begin

- Know the location and image name of the ISO image you require for the installation.
- You have already read the Prerequisites for Installing the Cisco Nexus 1000V, on page 4.
- You have already manually provisioned the VM to be used for the VSM. For more information, see the *VMware vSphere Virtual Machine Administration Guide*.

- The VSM VM requires the following and this procedure includes steps for updating these properties:
  - We recommend 4 Gigabit of RAM reserved and allocated.
  - We recommend 2048 MHz of CPU speed.

Procedure

Step 1 Using your VMware documentation, attach the VSM ISO image to the virtual CD-ROM and copy the software to a virtual machine (VM).

Step 2 Make sure that the VSM VM is powered off.

Step 3 In the **vSphere client Virtual Machine Properties** window **Hardware** tab, choose **Memory.**

Step 4 In the **Memory Size** field, choose 4 GB.

Step 5 In the **Resources** tab, choose **Memory.**

The Resource Allocation settings display in the right-hand pane.

Step 6 In the **Reservation** field, choose 4096 MB.

Step 7 In the **Resources** tab, choose CPU.

The Resource Allocation settings display in the right-hand pane.

Step 8 In the **Reservation** field, choose 2048 MHz.

Note For optimum performance, we recommend minimum 2048 MHz of CPU speed. You may change the value as per availability.

Step 9 Click **OK.**

The VSM VM memory and CPU speed settings are saved in VMware vSphere Client.

Step 10 Right-click the VSM and choose **Open Console**.

Step 11 Choose **Install Nexus1000V and bring up the new image** entry and press **Enter**.

Step 12 Enter and confirm the Administrator password.

Note All alphanumeric characters and symbols on a standard US keyboard are allowed except for these three: $ \ ?

Step 13 Enter the domain ID.

```
Enter the domain id<1-1023>: 152
```

Step 14 Enter the HA role.

If you do not specify a role, standalone is assigned by default.

This example shows the HA role as primary.

```
Enter HA role[standalone/primary/secondary]: primary

[########################################] 100%

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
```

```
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

Step 15 Do one of the following:

- If you are setting up the primary/active VSM, go to Step 18.
- If you are setting up the secondary/standby VSM, then continue with the next step.

Step 16 If you have set up the VSM virtual machine (VM) to boot from the CD-ROM, and are installing the secondary VSM from the ISO image attached to your CD-ROM, remove the virtual CD-ROM now so that the VSM does not boot from the CD.

This step is necessary if you have set up the VSM VM to boot from the CD-ROM before the hard drive.

Step 17 If you are setting up the secondary or standby VSM, do the following:

a) Enter the HA role at the following prompt:

```
Enter HA role[standalone/primary/secondary]:
```

b) Enter **yes** at the following prompt about rebooting the VSM:

```
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? :
```

c) Enter the domain ID at the following prompt:

```
Enter the domain id<1-1023>:
```

The secondary VSM VM is rebooted and brought up in standby mode. The password on the secondary VSM is synchronized with the password on the active/primary VSM. Any configuration made on the active/primary VSM is now automatically synchronized with the standby.

This example shows the system rebooting when the HA role is set to secondary.

```
Enter HA role[standalone/primary/secondary]: secondary

Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? : y

Enter the domain id<1-1023>: 1020
[########################################] 100%
HA mode set to secondary. Rebooting now...
```

You have completed this procedure for the secondary VSM.

Step 18 Enter **yes** to enter the basic configuration dialog.

```
Would you like to enter the basic configuration dialog (yes/no): yes
```

Step 19 Enter **no** to create another Login account.

```
Create another login account (yes/no) [n]: no
```

Step 20 Enter **no** to configure a read-only SNMP community string.

```
Configure read-only SNMP community string (yes/no) [n]: no
```

Step 21 Enter **no** to configure a read-write SNMP community string.

```
Configure read-write SNMP community string (yes/no) [n]: no
```

Step 22 Enter a name for the switch.

```
Enter the switch name: n1000v
```

Step 23 Enter **yes** to configure out-of-band management and then enter the mgmt0 IPv4 address and subnet mask.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: yes
Mgmt0 IPv4 address: 172.28.15.152
Mgmt0 IPv4 netmask: 255.255.255.0
```

Step 24 Enter **yes** to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes
IPv4 address of the default gateway : 172.23.233.1
```

Step 25 Enter **no** to configure advanced IP options.

```
Configure Advanced IP options (yes/no)? [n]: no
```

Step 26 Enter **yes** to enable the Telnet service.

```
Enable the telnet service? (yes/no) [y]: yes
```

Step 27 Enter **yes** to enable the SSH service and then enter the key type and number of key bits.

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of  key bits <768-2048> : 1024
```

For more information, see the document, *Cisco Nexus 1000V Security Configuration Guide*.

Step 28 Enter **yes** to enable the HTTP server.

```
Enable the http-server? (yes/no) [y]: yes
```

Step 29 Enter **no** to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: no
```

Step 30 Enter **yes** to configure the SVS domain parameters and then enter the mode (L2 or L3), and the control and packet VLAN IDs.

```
Configure svs domain parameters? (yes/no) [y]: yes
Enter SVS Control mode (L2 / L3) [L3] : Press Return
```

Step 31 Enter **yes** to configure the VEM feature level and then enter 0 or 1.

```
Vem feature level will be set to 5.2.1.SV3.4.1a,
Do you want to reconfigure? (yes/no) [n] yes
          Current vem feature level is set to 5.2.1.SV3.4.1a
          You can change the feature level to:
                      vem feature level is set to the highest value possible
```

Note The feature level is the least VEM release that the VSM can support. For example, if the feature level is set to the 5.2(1)SV3(4.1a) release, any VEMs with an earlier release are not attached to the VSM.

The system now summarizes the complete configuration and asks if you want to edit it.

```
The following configuration will be applied:
 Switchname n1000v
interface Mgmt0
ip address 172.28.15.152 255.255.255.0
no shutdown
no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  feature http-server
  svs-domain
    no control vlan
    no packet vlan
    svs mode L3 interface mgmt0
```

Step 32 Do one of the following:

- If you do not want to edit the configuration enter no and continue with the next step.
- If you want to edit the configuration, enter yes and return to Step 19 to revisit each command.

```
Would you like to edit the configuration? (yes/no) [n]:no
```

Step 33 Enter **yes** to use and save this configuration, answer **yes.**

Caution If you do not save the configuration now, none of your changes will be part of the configuration the next time that the switch is rebooted. Enter **yes** to save the new configuration and to ensure that the kickstart and system images are also automatically configured.

```
Use this configuration and save it? (yes/no) [y]: yes
[########################################] 100%
```

The new configuration is saved into nonvolatile storage.

Note You can use the setup routine to update the configuration done in Step 18 through Step 33 at any time by entering the setup command in EXEC mode. Once setup begins, press **Enter** to skip a command. Press **Ctrl-C** to skip the remaining commands.

If you are installing redundant VSMs, make sure that you configure the software on the primary VSM before installing the software on the secondary VSM.

Step 34 Create the SVS connection manually or go to Establishing the SVS Connection, on page 22.

Installing the Software from an OVA Image

Before you begin

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

- Know the location and image name of the OVA image you require for the installation.
- You have already read the Prerequisites for Installing the Cisco Nexus 1000V, on page 4.
- You have a copy of the following Cisco Nexus 1000V software image files on your local drive, depending on the installation type you are using:
- For detailed information about using the Deploy OVF Template wizard, see the *vSphere Virtual Machine Administration Guide*.

- You have the following information available for creating a VM for the VSM and mapping the required port groups:
  - A name for the new VSM that is unique within the inventory folder and up to 80 characters.
  - The name of the host where the VSM will be installed in the inventory folder.
  - The name of the datastore in which the VM files will be stored.
  - The names of the network port groups used for the VM.
  - The Cisco Nexus 1000V VSM IP address.
- If you are using the OVA file for installation, make sure that you have the following information available for creating and saving an initial configuration file on the VSM:
  - VSM domain ID
  - Admin password
  - Management IP address, subnet mask, and gateway
- The VSM VM requires the CPU speed to be 2048 MHz or greater. If the CPU speed is less than 2048 MHz, then do not proceed with this procedure. Instead perform Installing the Software from the ISO Image, on page 10.

Procedure

Step 1 From the vSphere Client, choose **File > Deploy OVF Template**.

Step 2 In the **Source** screen, specify the location of the OVA file and click **Next.**

The OVF Template Details screen opens displaying product information, including the size of the file and the size of the VM disk.

Step 3 Click **Next.**

Step 4 Read the Cisco Nexus 1000V License Agreement.

Step 5 Click **Accept** and then click **Next.**

Step 6 In the **Name:** field, add the VSM name, choose the folder location within the inventory where it will reside, and click **Next.**

The name for the VSM must be unique within the inventory folder and less than 80 characters.

Step 7 From the **Configuration** drop-down list, choose **Nexus 1000V Installer**.

This choice configures the primary VSM using the GUI setup dialog.

Step 8 If you want to configure a secondary VSM, select **Nexus 1000V Secondary**.

Step 9 Click **Next**.

Step 10 Choose the data center or cluster on which to install the VSM.

Step 11 Click **Next**.

Step 12 Choose the datastore in which to store the file if one is available.

On this page, you choose from datastores already configured on the destination cluster or host. The virtual machine configuration file and virtual disk files are stored on the datastore. Choose a datastore large enough to accommodate the virtual machine and all of its virtual disk files.

Step 13 Click **Next**.

Step 14 Choose one of the following disk formats for storing virtual machine virtual disks, and click **Next.**

Format	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. In this format, the space required for the virtual disk is allocated when the disk is created. The data remaining on the physical device is not erased during creation. The data is zeroed out on demand at a later time on first write from the virtual machine. Virtual machines do not read stale data from the physical device.
Thick Provision Eager Zeroed	Creates a virtual disk that supports clustering features such as Fault Tolerance. In this format, the space required for the virtual disk is allocated when the disk is created. The data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks.
Thin Provision	Creates a virtual disk in thin provision format. This format is useful for saving storage space. In this format, storage blocks are allocated and zeroed out when they are first accessed. Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it.

Step 15 In the **Network Mapping** screen, choose the networks (the control, management, and packet port groups) that are present in your inventory.

Step 16 Click **Next**

Step 17 Do one of the following:

- If you are installing software on a primary VSM, specify the following properties for your primary VSM:
  - VSM domain ID
  - Admin password
  - Management IP address
  - Management IP subnet mask
  - Management IP gateway

- If you are installing software on a secondary VSM, specify only the following properties for your secondary VSM (all other properties are acquired on synchronization with the primary VSM), and then click Next:
  - VSM domain ID (use the same domain ID entered for the primary).
  - Admin password (use the same password entered for the primary).

Step 18 Click **Next.**

Step 19 In the **Ready to Complete** screen, if the configuration is correct, click **Finish**.

A status bar displays as the VM installation progresses.

Step 20 Click **Close.**

You have completed installing the Cisco Nexus 1000V software.

Step 21 Right-click the VSM and choose **Open Console**.

Step 22 Click the **green arrow** to power on the VSM.

Step 23 Enter the following commands at the VSM prompt.

```
switch# configure terminal
switch(config)# setup
```

Step 24 Enter the HA role.

If you do not specify a role, standalone is assigned by default.

This example shows the HA role as primary.

```
Enter HA role[standalone/primary/secondary]: primary

[########################################] 100%

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

Step 25 Do one of the following:

- If you are setting up the primary/active VSM, go to Step 18.
- If you are setting up the secondary/standby VSM, then continue with the next step.

Step 26 If you have set up the VSM virtual machine (VM) to boot from the CD-ROM, and are installing the secondary VSM from the ISO image attached to your CD-ROM, remove the virtual CD-ROM now so that the VSM does not boot from the CD.

This step is necessary if you have set up the VSM VM to boot from the CD-ROM before the hard drive.

Step 27 If you are setting up the secondary or standby VSM, do the following:

a) Enter the HA role at the following prompt:

```
Enter HA role[standalone/primary/secondary]:
```

b) Enter **yes** at the following prompt about rebooting the VSM:

```
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? :
```

c) Enter the domain ID at the following prompt:

```
Enter the domain id<1-1023>:
```

The secondary VSM VM is rebooted and brought up in standby mode. The password on the secondary VSM is synchronized with the password on the active/primary VSM. Any configuration made on the active/primary VSM is now automatically synchronized with the standby.

This example shows the system rebooting when the HA role is set to secondary.

```
Enter HA role[standalone/primary/secondary]: secondary

Setting HA role to secondary will cause a system reboot. Are you sure (yes/no) ? : y

Enter the domain id<1-1023>: 1020
[########################################] 100%
HA mode set to secondary. Rebooting now...
```

You have completed this procedure for the secondary VSM.

Step 28 Enter **yes** to enter the basic configuration dialog.

```
Would you like to enter the basic configuration dialog (yes/no): yes
```

Step 29 Enter **no** to create another Login account.

```
Create another login account (yes/no) [n]: no
```

Step 30 Enter **no** to configure a read-only SNMP community string.

```
Configure read-only SNMP community string (yes/no) [n]: no
```

Step 31 Enter **no** to configure a read-write SNMP community string.

```
Configure read-write SNMP community string (yes/no) [n]: no
```

Step 32 Enter a name for the switch.

```
Enter the switch name: n1000v
```

Step 33 Enter **yes** to configure out-of-band management and then enter the mgmt0 IPv4 address and subnet mask.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: yes
Mgmt0 IPv4 address: 172.28.15.152
Mgmt0 IPv4 netmask: 255.255.255.0
```

Step 34 Enter **yes** to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes

    IPv4 address of the default gateway : 172.23.233.1
```

Step 35 Enter **no** to configure advanced IP options.

```
Configure Advanced IP options (yes/no)? [n]: no
```

Step 36 Enter **yes** to enable the Telnet service.

```
Enable the telnet service? (yes/no) [y]: yes
```

Step 37 Enter **yes** to enable the SSH service and then enter the key type and number of key bits.

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of  key bits <768-2048> : 1024
```

For more information, see the document, *Cisco Nexus 1000V Security Configuration Guide*.

Step 38 Enter **yes** to enable the HTTP server.

```
Enable the http-server? (yes/no) [y]: yes
```

Step 39 Enter **no** to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: no
```

Step 40 Enter **yes** to configure the SVS domain parameters and then enter the mode (L2 or L3), and the control and packet VLAN IDs.

```
Configure svs domain parameters? (yes/no) [y]: yes
Enter SVS Control mode (L2 / L3) : L2
Enter control vlan <1-3967, 4048-4093> : 100
Enter packet vlan <1-3967, 4048-4093> : 101
```

Step 41 Enter **yes** to configure the VEM feature level and then enter **0** or **1**.

```
Vem feature level will be set to 5.2.1.SV3.4.1a,
Do you want to reconfigure? (yes/no) [n] yes
          Current vem feature level is set to 5.2.1.SV3.4.1a
          You can change the feature level to:
                      vem feature level is set to the highest value possible
```

The system now summarizes the complete configuration and asks if you want to edit it.

```
The following configuration will be applied:
 Switchname n1000v
interface Mgmt0
ip address 172.28.15.152 255.255.255.0
no shutdown
no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  feature http-server
  svs-domain
    svs mode L2
    control vlan 100
    packet vlan 101
    domain id 101
vlan 100
vlan 101
```

Step 42 Do one of the following:

- If you do not want to edit the configuration enter **no** and continue with the next step.
- If you want to edit the configuration, enter **yes** and return to Step 19 to revisit each command.

```
Would you like to edit the configuration? (yes/no) [n]:no
```

Step 43 Enter **yes** to use and save this configuration.

Caution If you do not save the configuration now, none of your changes will be part of the configuration the next time that the switch is rebooted. Enter yes to save the new configuration and to ensure that the kickstart and system images are also automatically configured.

```
Use this configuration and save it? (yes/no) [y]: yes
[########################################] 100%
```

The new configuration is saved into nonvolatile storage.

Note You can use the setup routine to update the configuration done in Step 18 through Step 33 at any time by entering the **setup** command in EXEC mode. Once setup begins, press **Enter** to skip a command. Press **Ctrl-C** to skip the remaining commands.

Note If you are installing redundant VSMs, make sure that you configure the software on the primary VSM before installing the software on the secondary VSM.

Step 44 Register the vCenter extension file in VMware vCenter. See Registering a vCenter Extension File in VMware vCenter, on page 20 for more information.

Step 45 Create the SVS connection manually or go to Establishing the SVS Connection, on page 22.

Registering a vCenter Extension File in VMware vCenter

In VMware vCenter , the vCenter extension files are called plug-ins.

Before you begin

- You know the IP address of the active VSM.
- You have already downloaded a copy of the following file from the VSM home page.
  - cisco_nexus1000v_extension.xml

Note To go to your VSM home page, point your browser to the IP address of the active VSM.

Procedure

Step 1 Start the vSphere Client.

Step 2 From the Plug-Ins menu, choose **Manage Plug-Ins**. The Plug-In Manager dialog box opens.

Step 3 Right-click the white space within the dialog box, and choose **New Plug-In** from the popup menu. The Register Plug-In dialog box opens.

Step 4 Click **Browse** and choose the cisco_nexus1000v_extension.xml file that you downloaded from the VSM home page.

Step 5 Click **Register Plug-In**.

Step 6 In the Security Warning dialog box, click **Ignore** to continue using the certificate.

Step 7 In the Register Plug-in dialog box, click **OK**. After the plug-in is registered on vCenter, a dialog box appears stating that it has successfully registered.

Registering a vCenter Extension File in VMware vCenter 6.5a

Note This procedure applies for VMware vCenter 6.5a.

Before you begin

- You know the IP address of the active VSM.
- You have already downloaded a copy of the following file from the VSM home page.
  - cisco_nexus1000v_extension.xml

Note To go to your VSM home page, point your browser to the IP address of the active VSM.

Procedure

Step 1 Log in to Cisco Nexus 1000V VSM.

Step 2 Enter the terminal configuration mode.

configure terminal

Step 3 Configure VSM to vCenter Server connection.

svs connection vc

Step 4 Configure the protocol.

protocol vmware-vim

Step 5 Configure the DVS datacenter.

vmware dvs datacenter-name

Step 6 Configure the IP address of the remote vCenter server.

remote ip address

Step 7 Register the vCenter plugin.

register-plugin remote username password

Step 8 Establish VSM to vCenter Server connection.

connect

The following example shows how to install VEM software locally on a VMware 6.5a host using the CLI.

```
vsm# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
vsm(config)# svs connection vc
vsm(config-svs-conn)# 2017 Mar 28 08:38:42 sv331-ip-171 vms[2751]: %VMS-5-CONN_CREATE:
Connection 'vc' created.
vsm(config-svs-conn)# protocol vmware-vim
vsm(config-svs-conn)# vmware dvs datacenter-name dc1
vsm(config-svs-conn)# remote ip address 10.197.135.64
vsm(config-svs-conn)# register-plugin remote username administrator@vsphere.local password
 N1k@12345
vsm(config-svs-conn)# connect
```

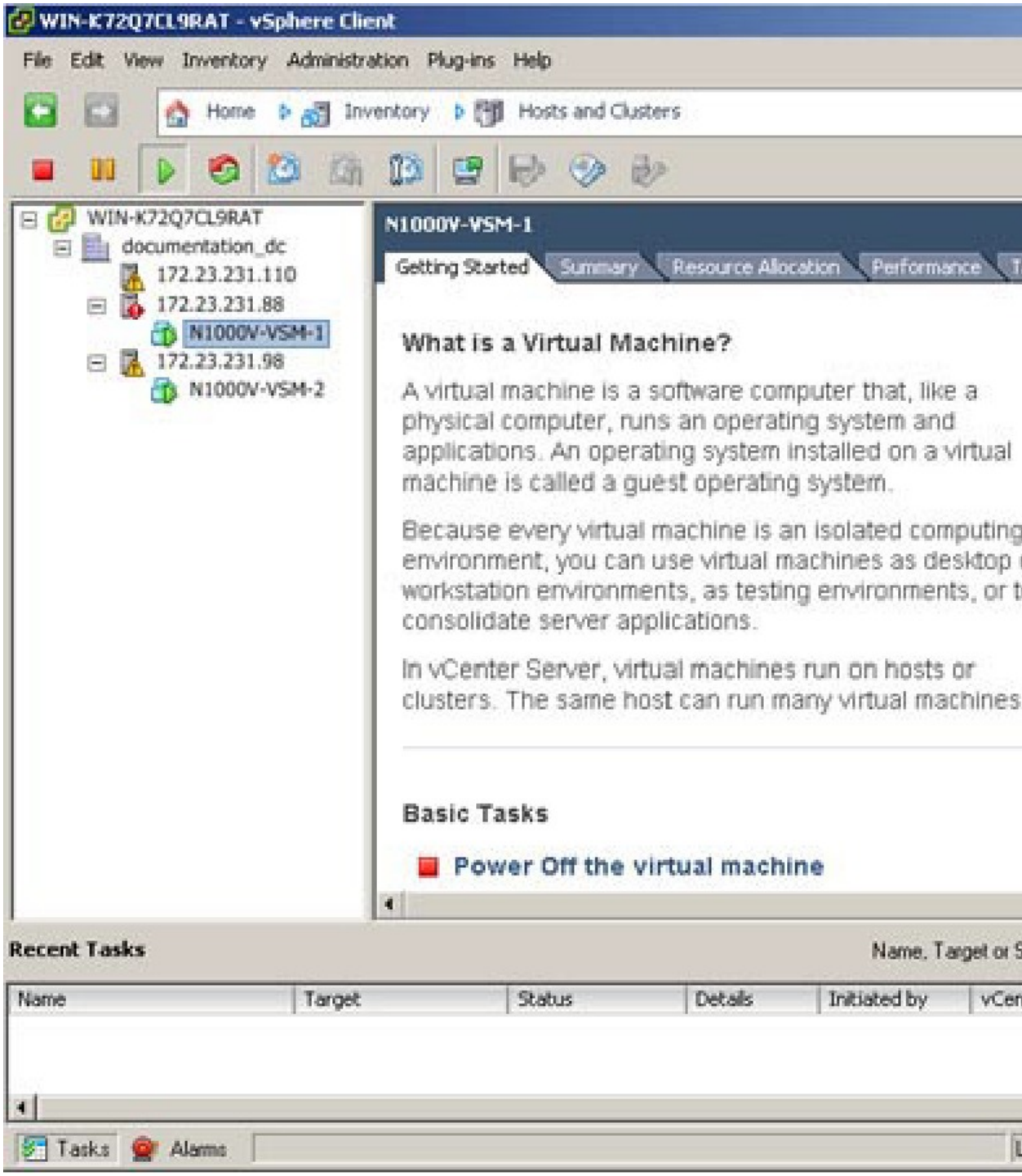
Establishing the SVS Connection

Procedure

Step 1 Open the vSphere Client.

Step 2 Choose the primary VSM.

Figure 1: vSphere Client Window



Step 3 Choose the **Console** tab.

Step 4 Enter the **show svs connections** command to confirm that there is not an SVS connection.

Step 5 Open a command window.

Step 6 In the **VSM Console**, enter the following command:

```
svs connection <name of the connection>
  protocol vmware-vim
  remote ip address
<vc ip address> port 80
  transport type <ipv4/ipv6>
  vmware dvs datacenter-name <name>
  max-ports 50000
  vmware dvs-version <4.0.0/5.0.0/5.5.0/6.0.0>
  connect
```

Step 7 In the **vSphere Console** window, enter the **show svs connections** command.

The operational status is Connected.

Note The VMware vCenter, version 6.5, requires the DVS UUID field to be populated before establishing a connection after the DVS has been created and UUID has been allocated. When you run **no connect** and **connect** commands under **svs connection** to re-establish the connection, you need to make sure that you have already configured UUID using the **vmware dvs uuid <> datacenter-name <>** command.

You have completed establishing the SVS connection.

Setting Virtual Machine Startup and Shutdown Parameters

Before you begin

- You have the following information:
  - Number of seconds for the default startup delay
  - Number of seconds for the default shutdown delay

Procedure

Step 1 In the **vSphere Client** window, choose a host and click the **Configuration** tab.

Step 2 In the **Configuration** pane, choose **Virtual Machine Startup/Shutdown**.

Step 3 In the **Virtual Machine Startup and Shutdown** pane, click the **Properties** link.

Step 4 In the **System Settings** dialog box, do the following:

a) Check the **Allow virtual machines to start and stop automatically with the system** check box.

b) In the System Settings pane, do the following:
   - Enter the number of seconds in the **Default Startup Delay seconds** field.
   - Enter the number of seconds in the **Default Shutdown Delay seconds** field.

c) In the **Startup Order** pane, do the following:
   - Choose the VM.

- Click the **Move Up** button until the VM is under Automatic Startup.

d) Click **OK**.
e) Repeat Step 2 through Step 4 for the other VM.

Startup and shutdown settings are complete.

Adding VEM Hosts to the Cisco Nexus 1000V Distributed Virtual Switch

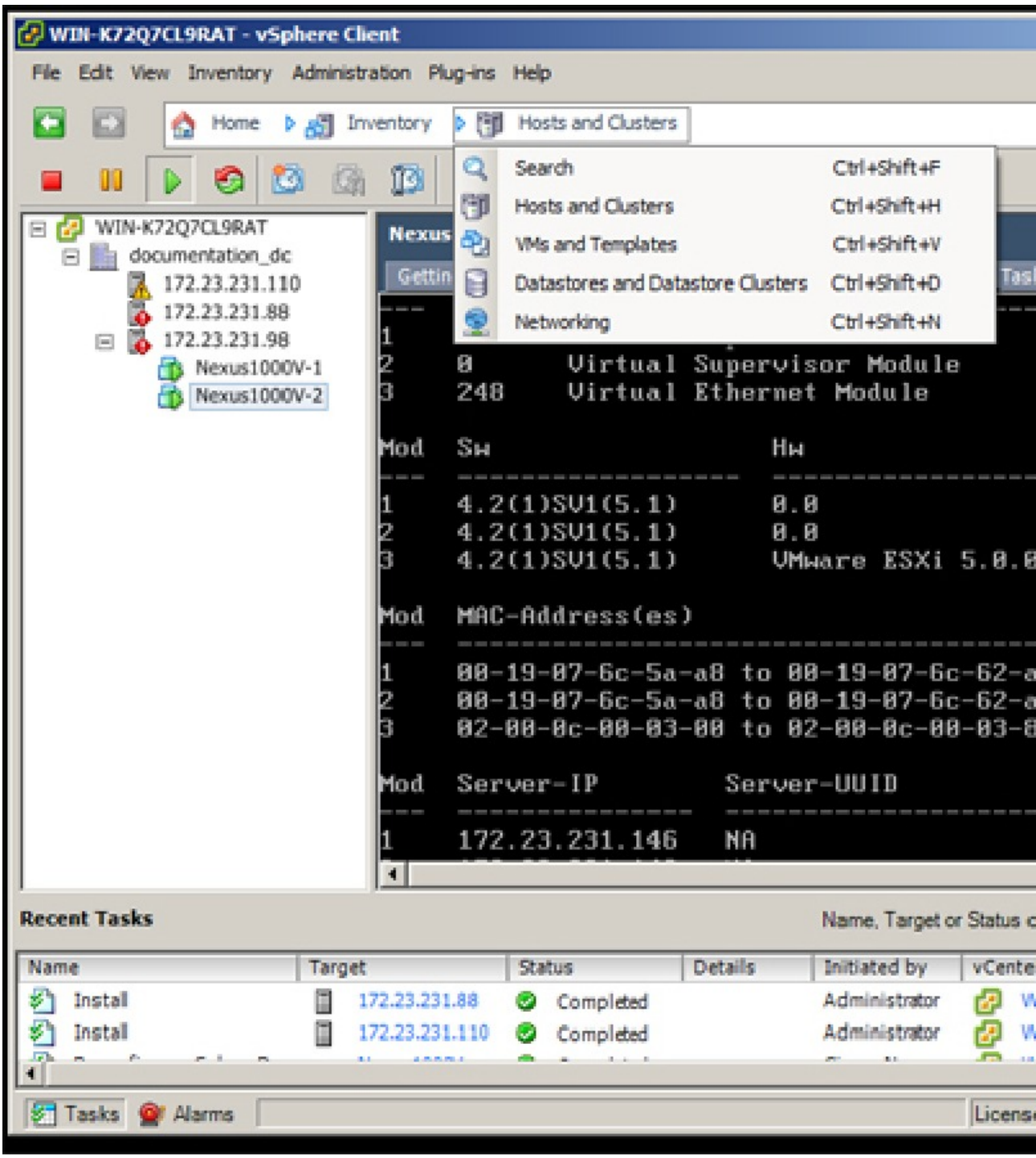
Before you begin

- You have the following information:
  - Physical adapters
  - Uplink port groups

Procedure

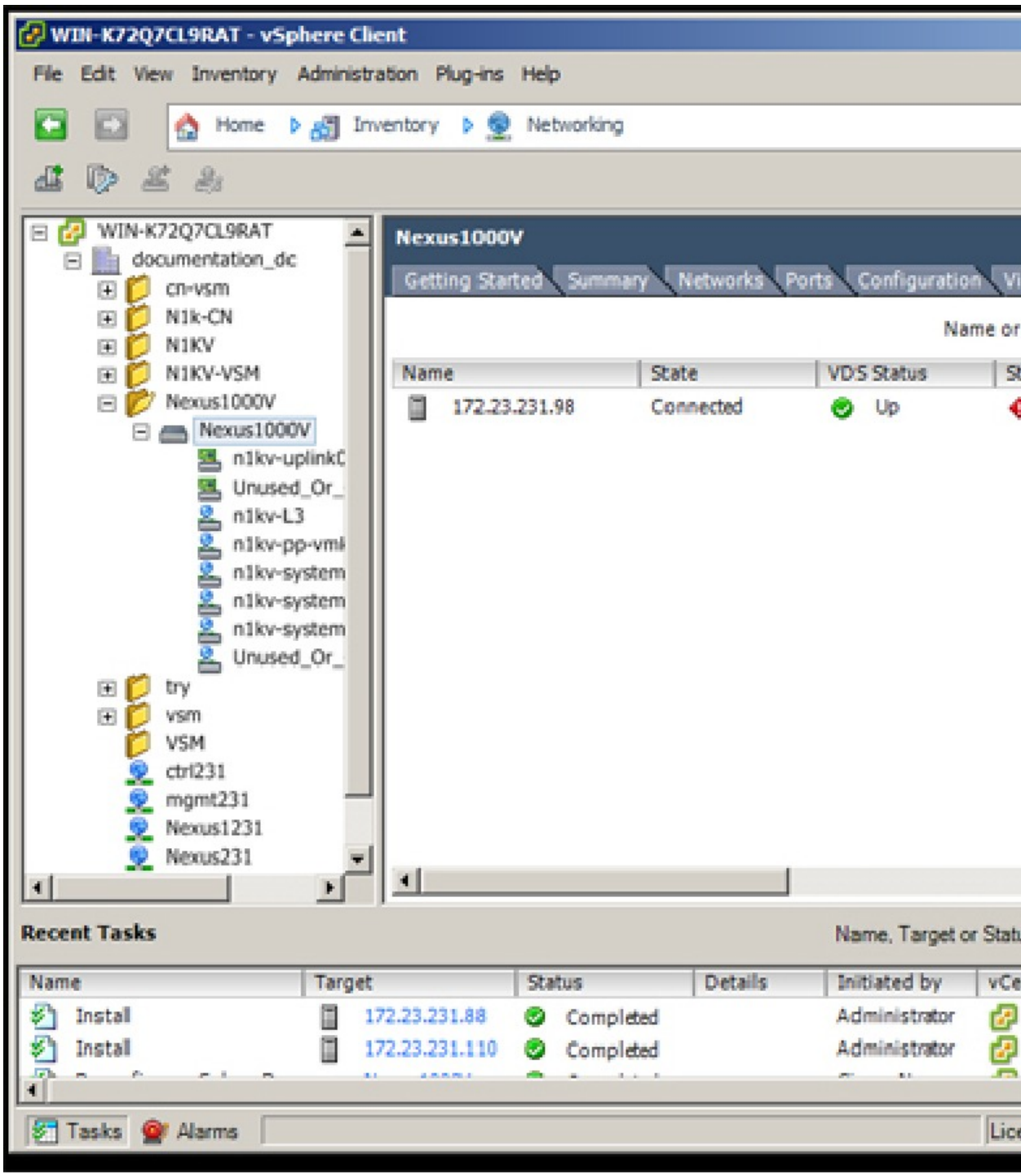
Step 1 In the **vSphere Client** window, choose **Hosts and Clusters** > **Networking**.

Figure 2: vSphere Client WIndow



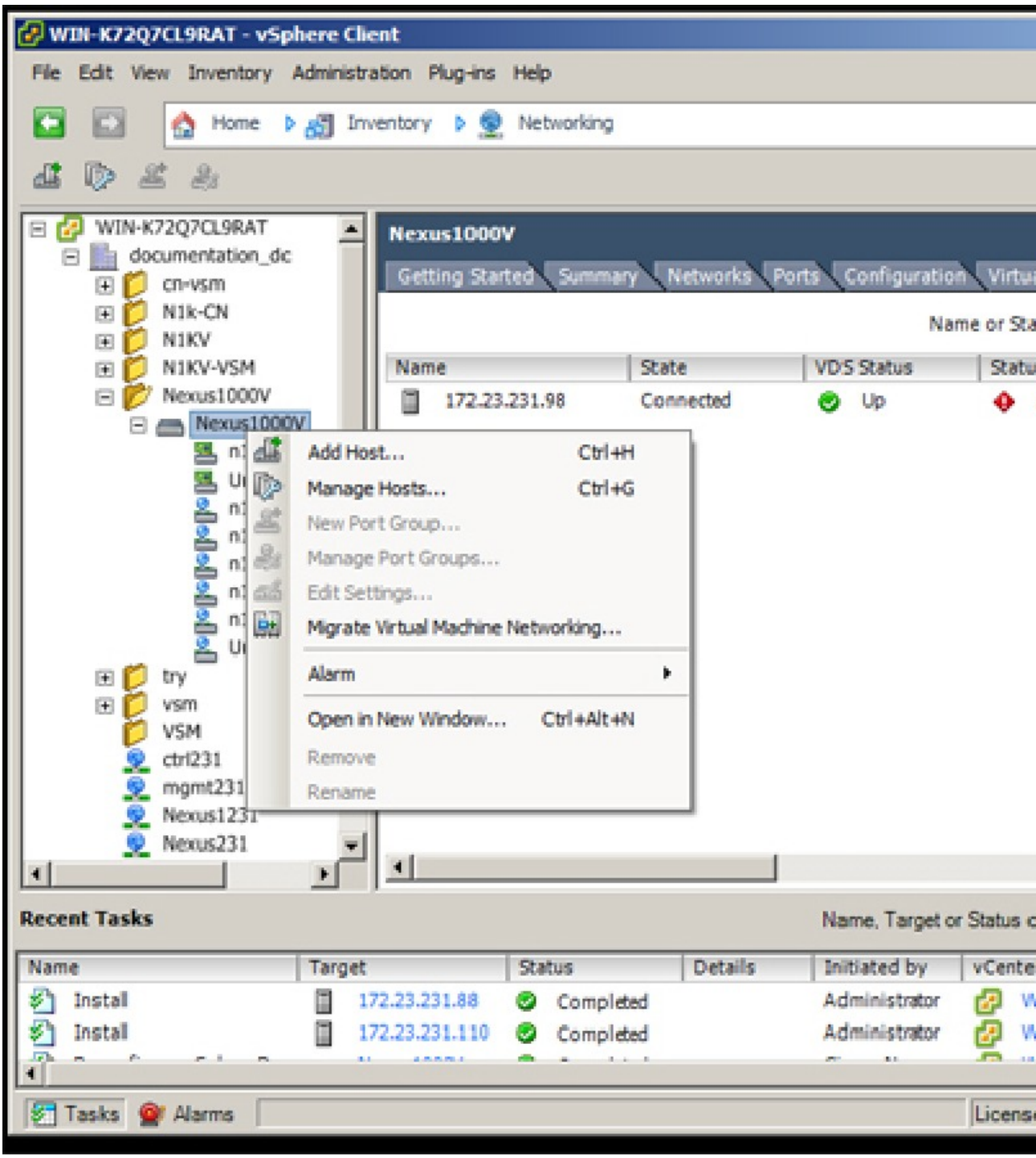
Step 2 In the **vSphere Client Hosts** window, choose the DVS and click the **Hosts** tab.

Figure 3: vSphere Client Hosts Window



Step 3 In the **Add Hosts to DVS** window, right-click the DVS and from the drop-down list, choose **Add Host**.

Figure 4: Add Hosts to DVS



Step 4 In the **Select Hosts and Physical Adapters** screen, choose the hosts and the uplink port groups, and click **Next.**

Step 5 In the **Network Connectivity** screen, do the following tasks:

Note For Layer 3 communication, you must migrate or create a new Layer 3 vmkernel interface. Migrate your management vmkernel interface into the Layer 3 capable port-profile. Do not use multiple vmkernel interfaces on the same subnet.

a) Highlight the vmkernel interface that you want to migrate, and choose the destination port group that you created for management traffic earlier.
b) Click **Next**.

Step 6 In the **Virtual Machine Networking** screen, click **Next**.

Step 7 In the **Ready to Complete** screen, click **Finish**.

Step 8 In the **vSphere Client Hosts** window, confirm that the hosts are in the Connected state.

The host connection process is complete.

Installing the VEM Software Using VUM

VMware Update Manager (VUM) automatically selects the correct VEM software to be installed on the host when the host is added to the DVS.

Note When the Nexus 1000V is configured with svs mode l3 control0 and the VMKNics are configured on a different subnet than the control0, the modules may flap as the ARP reachability will fail between these subnets. This happens for the networks where proxy ARP is not configured. If the proxy ARP not enabled in the setup, configure the network specific route to VMK network to route via the control0 interface in the default VRF.

Note Make sure that you read the VEM Prerequisites, on page 6 to ensure that the VUM operation proceeds without failure.

Installing the VEM Software Using the CLI

Based on the version of VMware ESX/ESXi software that is running on the server, there are different installation paths.

Installing the VEM Software Locally on a VMware Host Using the CLI

Note This procedure applies for VMware 5.0 host and later ESXi versions.

Procedure

Step 1 Copy the VEM software to the `/tmp` directory.

Step 2 ~ # **esxcli software vib install -v /tmp/***VIB_FILE*

Begin the VEM installation procedure.

Step 3 Verify that the installation was successful by checking for the “VEM Agent (vemdpa) is running” statement in the output of the **vem status -v** command.

Step 4 Verify that the VIB has installed by entering the following command:

esxcli software vib list | grep cisco

Step 5 Verify VEM and VSM version by entering the following command:

vem show version

Step 6 Verify the VSM to check that the module is online by entering the following command:

vem vesion -v

Step 7 Do one of the following:

- If the installation was successful, the installation procedure is complete.
- If the installation was not successful, see the "Recreating the Cisco Nexus 1000V Installation" section in the *Cisco Nexus 1000V Troubleshooting Guide*.

The following example shows how to install VEM software locally on a VMware 6.5 host using the CLI.

```
~ # esxcli software vib install -v /Cisco_bootbank_cisco-vem-v390-5.2.1.3.1.4.0-6.5.1.vib
esxcli software vib install -v /Cisco_bootbank_cisco-vem-v390
-esx_5.2.1.3.1.4.0-6.5.1.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v390-esx_5.2.1.3.1.4.0-6.5.1
   VIBs Removed:
   VIBs Skipped:

~ # vem status -v
[root@localhost:~] vem status -v
Package vssnet-esxesx2016-release
Version 5.2.1.3.1.4.0-6.5.1
Build 1
Date Fri Feb 24 23:22:23 PST 2017

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         2432        4           128               1500    vmnic0

VEM Agent (vemdpa) is running

~ #
```

```
~ # esxcli software vib list | grep cisco
cisco-vem-v390-esx           5.2.1.3.1.4.0-6.5.1                Cisco   PartnerSupported
  2017-03-01
~ #

~ # vemcmd show version
 vemcmd show version
VEM Version: 5.2.1.3.1.4.0-6.5.1
VSM Version: 5.2(1)SV3(1.4)
System Version: VMware ESXi 6.5.0 Releasebuild-4887370
ESX Version Update Level: 0
~ #
```

Installing the VEM Software on a Stateless ESXi Host

The following list outlines the VEM installation process on a stateless ESXi host.

Note Stateless 6.5a ESXi host is not supported with Nexus1000V.

Procedure

Step 1 See the procedure for Adding the Cisco Nexus 1000V to an ESXi Image Profile, on page 32.

Step 2 Installing the VEM software using one of the two following procedures:

- Installing the VEM Software on a Stateless ESXi Host Using esxcli, on page 36
- Installing the VEM Software on a Stateless ESXi Host Using VUM, on page 38

Step 3 See the procedure for Configuring Layer 2 Connectivity, on page 39.

Stateless ESXi Host

Note For stateless ESXi, the VLAN that you use for the Preboot Execution Environment (gPXE) and Management must be a native VLAN in the Cisco Nexus 1000V management uplink. It must also be a system VLAN on the management VMkernel NIC and on the uplink.

VMware vSphere 5.5 introduces the VMware Auto Deploy, which provides the infrastructure for loading the ESXi image directly into the host's memory. The software image of a stateless ESXi is loaded from the Auto Deploy Server after every boot. In this context, the image with which the host boots is identified as the image profile.

An image profile is a collection of vSphere Installation Bundles (VIBs) required for the host to operate. The image profile includes base VIBs from VMware and additional VIBs from partners.

On a stateless host, you can install or upgrade the VEM software using either the VUM or CLI.

In addition, you should bundle the new or modified VEM in the image profile from which the stateless host boots. If it is not bundled in the image profile, the VEM does not persist across reboots of the stateless host.

For more information about the VMware Auto Deploy Infrastructure and stateless boot process, see the "Installing ESXi using VMware Auto Deploy" chapter of the *vSphere Installation and Setup, vSphere 5.5* document.

Adding the Cisco Nexus 1000V to an ESXi Image Profile

Before you begin

- Install and set up the VMware Auto Deploy Server. See the *vSphere Installation and Setup* document.
- Install the VMware PowerCLI on a Windows platform. This step is required for bundling the VEM into the image profile. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform where VMware PowerCLI is installed, do the following:
  - Download the image profile offline bundle, which is a ZIP file, to a local file path.
  - Download the VEM offline bundle, which is a ZIP file, to a local file path.

Procedure

Step 1 Start the vSphere PowerCLI application.

Step 2 Connect to vCenter Server by entering the following command:

Connect-VIServer *IP_address* **–User Administrator –Password** *XXXXX*.

Step 3 Load the image profile offline bundle by entering the following command:

Add-ESXSoftwareDepot *image_profile_bundle*

Note Each image profile bundle can include multiple image profiles.

Step 4 List the image profiles by entering the following command:

[vSphere PowerCLI] > **Get-EsxImageProfile**

Step 5 Choose the image profile into which the VEM is to be bundled by entering the following command:

New-EsxImageProfile -CloneProfile *image_profile_name* **-Name n1kv-Image**

Note The image profiles are in read-only format. You must clone the image profile before adding the VEM into it. The n1kv-Image is the cloned image profile of the ESXi-5.0.0-standard.

Step 6 change to Load the Cisco Nexus 1000V offline bundle by entering the following command:

Add-EsxSoftwareDepot *VEM_bundle*

Note The offline bundle is a zip file that includes the n1kv-vib file.

Step 7 Confirm that the n1kv-vib package is loaded by entering the following command:

Get-EsxSoftwarePackage -Name *cisco**

Step 8 Bundle the n1kv-package into the cloned image profile by entering the following command:

Add-EsxSoftwarePackage -ImageProfile n1kv-Image -SoftwarePackage *n1kv_package_name*

Step 9 List all the VIBs into the cloned image profile by entering the following command:

a) **$img = Get-EsxImageProfile n1kv-Image**
b) **$img.vibList**

Step 10 Export the image profile to a depot file for future use by entering the following command:

Export-EsxImageProfile –ImageProfile n1kv-Image –FilePath C:\n1kv-Image.zip –ExportToBundle

Step 11 Set up the rule for the host to bott with the image profile by entering the following commands

Note Any of the host parameters, such as the MAC address, IPV4 IP address, or domain name, can be used to associate an image profile with the host.

a) **New-deployrule -item $img -name rule-test –Pattern "mac=00:50:56:b6:03:c1"**
b) **Add-DeployRule -DeployRule rule-test**

Step 12 Display the configured rule to make sure that the correct image profile is associated with the host by entering the following command:

Get-DeployRuleSet

Step 13 Reboot the host.

The host contacts the Auto-Deploy Server and presents the host boot parameters. The Auto Deploy server checks the rules to find the image profile associated with this host and loads the image to the host's memory. The host boots from the image.

Example

This example shows how to add the Cisco Nexus 1000V to an ESXi image profile:

Note The examples in the procedure may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
vSphere PowerCLI> Set-ExecutionPolicy unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks described
in the about_Execution_Policies help topic. Do you want to change the execution
 policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
vSphere PowerCLI>  Connect-VIServer 10.105.231.40 -User administrator -Password 'xxxxxxxx'

Working with multiple default servers?

    Select [Y] if you want to work with more than one default servers. In this
case, every time when you connect to a different server using Connect-VIServer,
```

```
 the new server connection is stored in an array variable together with the
previously connected servers. When you run a cmdlet and the target servers
cannot be determined from the specified parameters, the cmdlet runs against all
 servers stored in the array variable.
    Select [N] if you want to work with a single default server. In this case,
when you run a cmdlet and the target servers cannot be determined from the
specified parameters, the cmdlet runs against the last connected server.

    WARNING: WORKING WITH MULTIPLE DEFAULT SERVERS WILL BE ENABLED BY DEFAULT
IN A FUTURE RELEASE. You can explicitly set your own preference at any time by
using the DefaultServerMode parameter of Set-PowerCLIConfiguration.

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Name                           Port  User
----                           ----  ----
10.105.231.40                  443   administrator


vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\VEM650-201703390111-BG-release.zip'

Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\VMware-ESXi-...


vSphere PowerCLI>  Get-EsxImageProfile

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.1.0-20121201001s-no-... VMware, Inc.    12/7/2015 7:... PartnerSupported
CN1-CY                         CISCO           4/22/2015 11... PartnerSupported
ESXi-5.1.0-20121204001-stan... VMware, Inc.    12/7/2015 7:... PartnerSupported
ESXi-5.1.0-20121201001s-sta... VMware, Inc.    12/7/2015 7:... PartnerSupported
ESXi-5.1.0-799733-no-tools     VMware, Inc.    8/12/2015 3:0... PartnerSupported
ESXi-5.1.0-20121204001-no-t... VMware, Inc.    12/7/2015 7:... PartnerSupported
ESXi-5.1.0-799733-standard     VMware, Inc.    8/12/2015 3:0... PartnerSupported


vSphere PowerCLI> New-EsxImageProfile -CloneProfile ESXi-5.1.0-799733-standard -Name FINAL

cmdlet New-EsxImageProfile at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Vendor: CISCO

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           09/09/2016 3:0... PartnerSupported


vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\VEM650-201703390111-BG-release.zip
Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\cisco-vem-v1...


vSphere PowerCLI> Get-EsxSoftwarePackage cisco*

Name                           Version                        Vendor
Creation Date
----                           -------                        ------
```

```
------------
cisco-vem-v390-esx             5.2.1.3.3.1.0-6.5.1            Cisco PartnerSupported
2017-03-01
~ #


vSphere PowerCLI> Add-EsxSoftwarePackage -SoftwarePackage cisco-vem-v300-esx -ImageProfile
 FINAL

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           12/07/2016 3:... PartnerSupported


vSphere PowerCLI> $img = Get-EsxImageProfile FINAL


Name                     Version                        Vendor     Creation Date
----                     -------                        ------     ------------
scsi-bnx2i               1.9.1d.v50.1-5vmw.510.0.0.7... VMware     8/12/2015 ...
sata-sata-promise        2.12-3vmw.510.0.0.799733       VMware     8/12/2015 ...
net-forcedeth            0.61-2vmw.510.0.0.799733       VMware     8/12/2015 ...
esx-xserver              5.1.0-0.0.799733               VMware     8/12/2015 ...
misc-cnic-register       1.1-1vmw.510.0.0.799733        VMware     8/12/2015 ...
net-tg3                  3.110h.v50.4-4vmw.510.0.0.7... VMware     8/12/2015 ...
scsi-megaraid-sas        5.34-4vmw.510.0.0.799733       VMware     8/12/2015 ...
scsi-megaraid-mbox       2.20.5.1-6vmw.510.0.0.799733   VMware     8/12/2015 ...
scsi-ips                 7.12.05-4vmw.510.0.0.799733    VMware     8/12/2015 ...
net-e1000e               1.1.2-3vmw.510.0.0.799733      VMware     8/12/2015 ...
sata-ahci                3.0-13vmw.510.0.0.799733       VMware     8/12/2015 ...
sata-sata-svw            2.3-3vmw.510.0.0.799733        VMware     8/12/2015 ...
net-cnic                 1.10.2j.v50.7-3vmw.510.0.0.... VMware     8/12/2015 ...
net-e1000                8.0.3.1-2vmw.510.0.0.799733    VMware     8/12/2015 ...
ata-pata-serverworks     0.4.3-3vmw.510.0.0.799733      VMware     8/12/2015 ...
scsi-mptspi              4.23.01.00-6vmw.510.0.0.799733 VMware     8/12/2015 ...
ata-pata-hpt3x2n         0.3.4-3vmw.510.0.0.799733      VMware     8/12/2015 ...
net-s2io                 2.1.4.13427-3vmw.510.0.0.79... VMware     8/12/2015 ...
esx-base                 5.1.0-0.0.799733               VMware     8/12/2015 ...
net-vmxnet3              1.1.3.0-3vmw.510.0.0.799733    VMware     8/12/2015 ...
net-bnx2                 2.0.15g.v50.11-7vmw.510.0.0... VMware     8/12/2015 ...
cisco-vem-v320-esx       5.2.1.3.3.1.0-3.2.1            Cisco      9/09/2016 ...
scsi-megaraid2           2.00.4-9vmw.510.0.0.799733     VMware     8/12/2015 ...
ata-pata-amd             0.3.10-3vmw.510.0.0.799733     VMware     8/12/2015 ...
ipmi-ipmi-si-drv         39.1-4vmw.510.0.0.799733       VMware     8/12/2015 ...
scsi-lpfc820             8.2.3.1-127vmw.510.0.0.799733  VMware     8/12/2015 ...
ata-pata-atiixp          0.4.6-4vmw.510.0.0.799733      VMware     8/12/2015 ...
esx-dvfilter-generic-... 5.1.0-0.0.799733               VMware     8/12/2015 ...
net-sky2                 1.20-2vmw.510.0.0.799733       VMware     8/12/2015 ...
scsi-qla2xxx             902.k1.1-9vmw.510.0.0.799733   VMware     8/12/2015 ...
net-r8169                6.011.00-2vmw.510.0.0.799733   VMware     8/12/2015 ...
sata-sata-sil            2.3-4vmw.510.0.0.799733        VMware     8/12/2015 ...
scsi-mpt2sas             10.00.00.00-5vmw.510.0.0.79... VMware     8/12/2015 ...
sata-ata-piix            2.12-6vmw.510.0.0.799733       VMware     8/12/2015 ...
scsi-hpsa                5.0.0-21vmw.510.0.0.799733     VMware     8/12/2015 ...
ata-pata-via             0.3.3-2vmw.510.0.0.799733      VMware     8/12/2015 ...
scsi-aacraid             1.1.5.1-9vmw.510.0.0.799733    VMware     8/12/2015 ...
scsi-rste                2.0.2.0088-1vmw.510.0.0.799733 VMware     8/12/2015 ...
ata-pata-cmd64x          0.2.5-3vmw.510.0.0.799733      VMware     8/12/2015 ...
ima-qla4xxx              2.01.31-1vmw.510.0.0.799733    VMware     8/12/2015 ...
net-igb                  2.1.11.1-3vmw.510.0.0.799733   VMware     8/12/2015 ...
scsi-qla4xxx             5.01.03.2-4vmw.510.0.0.799733  VMware     8/12/2015 ...
block-cciss              3.6.14-10vmw.510.0.0.799733    VMware     8/12/2015 ...
scsi-aic79xx             3.1-5vmw.510.0.0.799733        VMware     8/12/2015 ...
tools-light              5.1.0-0.0.799733               VMware     8/12/2015 ...
```

```
uhci-usb-uhci            1.0-3vmw.510.0.0.799733        VMware     8/12/2015 ...
sata-sata-nv             3.5-4vmw.510.0.0.799733        VMware     8/12/2015 ...
sata-sata-sil24          1.1-1vmw.510.0.0.799733        VMware     8/12/2015 ...
net-ixgbe                3.7.13.6iov-10vmw.510.0.0.7... VMware     8/12/2015 ...
ipmi-ipmi-msghandler     39.1-4vmw.510.0.0.799733       VMware     8/12/2015 ...
scsi-adp94xx             1.0.8.12-6vmw.510.0.0.799733   VMware     8/12/2015 ...
scsi-fnic                1.5.0.3-1vmw.510.0.0.799733    VMware     8/12/2015 ...
ata-pata-pdc2027x        1.0-3vmw.510.0.0.799733        VMware     8/12/2015 ...
misc-drivers             5.1.0-0.0.799733               VMware     8/12/2015 ...
net-enic                 1.4.2.15a-1vmw.510.0.0.799733  VMware     8/12/2015 ...
net-be2net               4.1.255.11-1vmw.510.0.0.799733 VMware     8/12/2015 ...
net-nx-nic               4.0.558-3vmw.510.0.0.799733    VMware     8/12/2015 ...
esx-xlibs                5.1.0-0.0.799733               VMware     8/12/2015 ...
net-bnx2x                1.61.15.v50.3-1vmw.510.0.0.... VMware     8/12/2015 ...
ehci-ehci-hcd            1.0-3vmw.510.0.0.799733        VMware     8/12/2015 ...
ohci-usb-ohci            1.0-3vmw.510.0.0.799733        VMware     8/12/2015 ...
net-r8168                8.013.00-3vmw.510.0.0.799733   VMware     8/12/2015 ...
esx-tboot                5.1.0-0.0.799733               VMware     8/12/2015 ...
ata-pata-sil680          0.4.8-3vmw.510.0.0.799733      VMware     8/12/2015 ...
ipmi-ipmi-devintf        39.1-4vmw.510.0.0.799733       VMware     8/12/2015 ...
scsi-mptsas              4.23.01.00-6vmw.510.0.0.799733 VMware     8/12/2015 ...
```

```
vSphere PowerCLI> Export-EsxImageProfile -ImageProfile FINAL -FilePath 'C:\Documents and
Settings\Administrator\Desktop\FINAL.zip' -ExportToBundle
vSphere PowerCLI>  New-deployrule -item $img -name rule-test –Pattern “mac=00:50:16:26:13:c2”
vSphere PowerCLI] > Add-DeployRule -DeployRule rule-test
[vSphere PowerCLI] > Get-DeployRuleSet
Name : rule-test
PatternList : {mac=00:50:16:26:13:c2}
ItemList : {FINAL}
```

Installing the VEM Software on a Stateless ESXi Host Using esxcli

Before you begin

- When you enter the **esxcli software vib install** command on an ESXi 5.0.0 host, note that the following message appears:

  Message: WARNING: Only live system was updated, the change is not persistent.

Procedure

Step 1 Display the VMware version and build number by entering the following commands:

- **vmware -v**
- **vmware -l**

Step 2 Log in to the ESXi stateless host.

Step 3 Copy the offline bundle to the host by entering the the following command:

esxcli software vib install -d *file_path/offline_bundle*

Note If the host is an ESXi 5.0.0 stateful host, the “Message: Operation finished successfully” line appears.

Step 4 Verify that the VIB has installed by entering the following command:

esxcli software vib list | grep cisco

Step 5 Change to Check that the VEM agent is running by entering the following command:

vem status -v

Step 6 Display the VEM version, VSM version, and ESXi version by entering the following command:

vemcmd show version

Step 7 Display the ESXi version and details about passthrough NICs by entering the following command:

vem version -v

Step 8 Add the host to the DVS by using the vCenter Server.

Step 9 On the VSM, verify that the VEM software has been installed by entering the following command:

show module

Example

This example shows how to install VEM software on a stateless host using esxcli.

Note The examples in the procedure may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
~ # vmware -v
VMware ESXi 6.5.0 build-4887370
~ #
~ # vmware -l
VMware ESXi 6.5.0 GA

~ # esxcli software vib install -d
/vmfs/volumes/newnfs/MN-VEM/VEM550-201703390101-BG-release.zip
Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v390-esx_5.2.1.3.1.4.0-6.5.1
   VIBs Removed:
   VIBs Skipped:


~ # esxcli software vib list | grep cisco
cisco-vem-v390-esx           5.2.1.3.1.4.0-6.5.1                 Cisco   PartnerSupported
  2017-03-01

vem status -v
vem status -v
Package vssnet-esxesx2016-release
Version 5.2.1.3.1.4.0-6.5.1
Build 1
Date Fri Feb 24 23:22:23 PST 2017

VEM modules are loaded
```

```
Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         2432        59          128               1500    vmnic0
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
daotocrystal1    1024       296        1024             1500    vmnic4,vmnic5,vmnic2,vmnic3

VEM Agent (vemdpa) is running

~ # vemcmd show version
vemcmd show version
VEM Version: 5.2.1.3.1.4.0-6.5.1
VSM Version:
System Version: VMware ESXi 6.5.0 Releasebuild-4887370
ESX Version Update Level: 0


~(config)# show module

 show module
Mod  Ports  Module-Type                      Model               Status
---  -----  -------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module        Nexus1000V          active *
2    0      Virtual Supervisor Module        Nexus1000V          ha-standby
4    1022   Virtual Ethernet Module          NA                  ok
5    1022   Virtual Ethernet Module          NA                  ok
6    1022   Virtual Ethernet Module          NA                  ok
7    1022   Virtual Ethernet Module          NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    5.2(1)SV3(1.4)      0.0
2    5.2(1)SV3(1.4)      0.0
4    5.2(1)SV3(1.4)      VMware ESXi 6.0.0 Releasebuild-3620759 (6.0)
5    5.2(1)SV3(1.4)      VMware ESXi 6.5.0 Releasebuild-4887370 (6.5)
6    5.2(1)SV3(1.4)      VMware ESXi 6.0.0 Releasebuild-3620759 (6.0)
7    5.2(1)SV3(1.4)      VMware ESXi 6.5.0 Releasebuild-4887370 (6.5)

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.197.132.57    NA                                    NA
2    10.197.132.57    NA                                    NA
4    10.197.132.43    e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba  10.197.132.43
5    10.197.132.44    7b1a5e63-bcd0-11e0-bd1d-30e4dbc2c3ae  10.197.132.44
6    10.197.132.45    8d8ff0e8-b565-11e0-bd1d-30e4dbc297da  10.197.132.45
7    10.197.132.46    db8b80ac-af1d-11e0-a4e7-30e4dbc26b82  10.197.132.46

* this terminal session

~#
```

Installing the VEM Software on a Stateless ESXi Host Using VUM

Before you begin

- Make sure that the VUM patch repository has the VEM software downloaded.

Note Stateless 6.5a ESXi host is not supported with Cisco Nexus1000V.

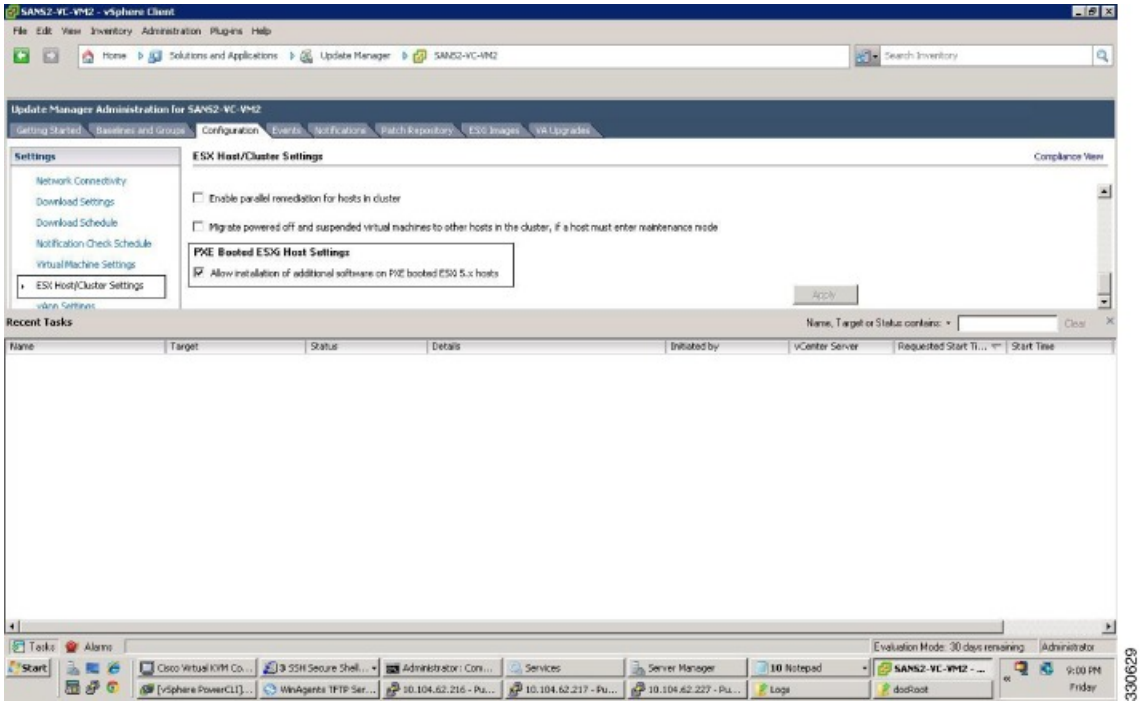
Procedure

Step 1 In vCenter Server, choose **Home** > **Update Manager** > **Configuration** > **ESX host/Cluster** settings.

The ESX Host/Cluster Settings window opens.

Step 2 Check the **PXE Booted ESXi Host Settings** check box.

Figure 5: ESX Host/Cluster Settings Window



Step 3 Add the host to the DVS by using vCenter Server.

Configuring Layer 2 Connectivity

Note Layer 3 connectivity is the preferred method.

You can configure a different VMware vSwitch port group for each VSM network adapter.

Procedure

Step 1 In the **Configure Networking** screen click **L2: Configure port groups for L2**.

Step 2 In the **Configure Networking** screen, do the following:

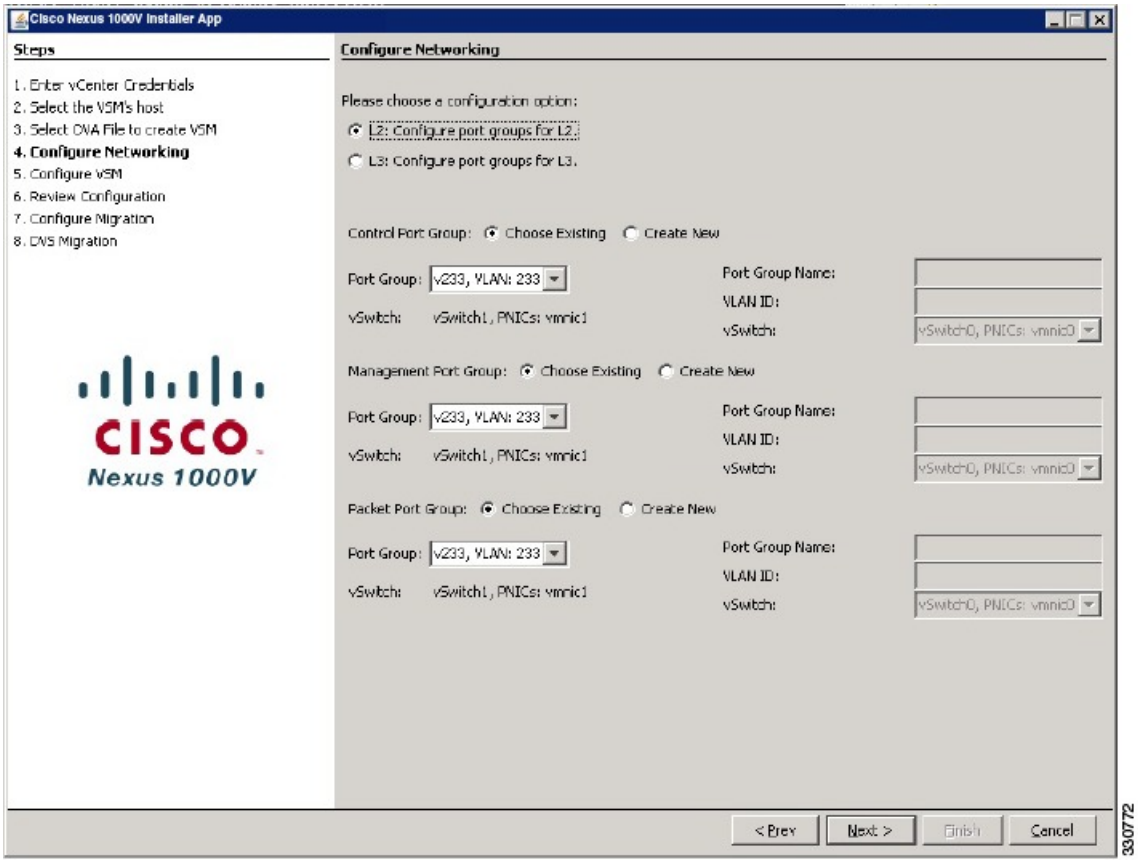
- From the **Port Group** drop-down list, choose your port groups.

- (Optional) In the **VLAN ID** field, enter the VLAN ID.

  Note The VLAN ID is only needed if you choose to create a new port group.

- Click **Next**. The Configure Networking screen opens.

Figure 6: Configure Networking Screen



Step 3 If desired, return to your Standard or Custom installation to enter the remaining Layer 2 configuration information.

Installing a VSM on the Cisco Nexus Cloud Services Platform

You can install the VSM on the Cisco Nexus Cloud Services Platform and move from Layer 2 to Layer 3 connectivity.

Note VEMs do not register to the VSM before a vmkernel interface (vmk) is migrated to a Layer 3 control-capable port profile. You must migrate a vmk to the Layer 3 port profile after migrating host vmnics to Ethernet port profiles.

The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

Before you begin

Copy the OVA file to the bootflash:repository/ of the Cisco Nexus Cloud Services Platform.

Procedure

Step 1 Create a virtual service blade.

```
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  1000v-dk9.5.2.1.SV3.1.4.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
vsm-1       SECONDARY     NONE          VSB NOT PRESENT          SECONDARY

switch(config-vsb-config)#
```

Step 2 Configure the control, packet, and management interface VLANs for static and flexible topologies.

```
switch(config-vsb-config)# interface management vlan 100
switch(config-vsb-config)# interface control vlan 101
switch(config-vsb-config)# interface packet vlan 101
```

Step 3 Configure the Cisco Nexus 1000V on the Cisco Nexus 1010.

```
switch(config-vsb-config)# enable
Enter vsb image:  [1000v-dk9.5.2.1.SV3.1.4.iso]
Enter domain id[1-1023]: 127
Enter SVS Control mode (L2 / L3): [L3] L2
Management IP version [V4/V6]: [V4]
Enter Management IP address: 192.0.2.79
Enter Management subnet mask: 255.255.255.0
IPv4 address of the default gateway: 192.0.2.1
Enter HostName: n1000v
Enter the password for 'admin': ********
Note: VSB installation is in progress, please use show virtual-service-blade commands to
check the installation status.
switch(config-vsb-config)#
```

Step 4 Display the primary and secondary VSM status.

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

--------------------------------------------------------------------------------
Name        HA-Role       HA-Status     Status                   Location
--------------------------------------------------------------------------------
vsm-1       PRIMARY       NONE          VSB POWER ON IN PROGRESS PRIMARY
vsm-1       SECONDARY     ACTIVE        VSB POWERED ON           SECONDARY
```

Step 5 Log in to the VSM.

```
switch(config)# virtual-service-blade vsm-1
switch(config-vsb-config)# login virtual-service-blade vsm-1
Telnet escape character is '^\'.
Trying 192.0.2.18...
Connected to 192.0.2.18.
Escape character is '^\'.

Nexus 1000v Switch
n1000v login: admin
Password:
Cisco Nexus operating System (NX-OS) Software
TAC support: http://www/cisco.com/tac
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

Step 6 Change svs mode from Layer 2 to Layer 3 in the Cisco Nexus 1000V.

Note The configuration in the highlighted code is optional.

```
switch(config)# svs-domain
switch(config-svs-domain)# no control vlan
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
switch(config-svs-domain)# no packet vlan
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
switch(config-svs-domain)# svs mode L3 interface mgmt0
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
switch(config-svs-domain)# show svs domain
switch(config-svs-domain)# show svs domain
SVS domain config
Domain id: 101
Control vlan: NA
Packet vlan:  NA
L2/L3 Control mode: L3
L3 control interface: mgmt0
Status: Config push to VC successful.
switch(config-svs-domain)#
```

Feature History for Installing the Cisco Nexus 1000V

The following table lists the release history for installing the Cisco Nexus 1000V.

Feature Name	Releases	Feature Information
VEM Installation 5.1	4.2(1)SV2(2.1)	Installing VEM software remotely or locally on a VMware 5.1 host using the CLI is now supported.
Standard and Custom installation application	4.2(1)SV2(1.1)	Installation Application updated with a Standard and Custom version
Updated installation application	4.2(1)SV1(5.2)	Added screens to the Java application.
VSM and VEM Installation	4.2(1)SV1(5.1)	Java applications introduced for VSM and VEM installation.
Installing the Cisco Nexus 1000V	4.0(1)SV1(1)	Introduced in this release.