Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.2)

First Published: January 31, 2012

Last Modified: February 05, 2014

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

Text Part Number: OL-26891-02

CONTENTS

Preface

This preface contains the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco Nexus devices .

This guide is for network administrators and server administrators with the following experience and knowledge:

- An understanding of virtualization
- Using VMware software to create a virtual machine and configure a VMware vSwitch

Note Knowledge of VMware vNetwork Distributed Switch is not required.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.

Convention	Description
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element(keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation for Nexus 1000V Series NX-OS Software

This section lists the documents used with the Cisco Nexus 1000V and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V Documentation Roadmap

Cisco Nexus 1000V Release Notes

Cisco Nexus 1000V and VMware Compatibility Information

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V Interface Configuration Guide

Cisco Nexus 1000V Layer 2 Switching Configuration Guide

Cisco Nexus 1000V License Configuration Guide

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide

Cisco Nexus 1000V Port Profile Configuration Guide

Cisco Nexus 1000V Quality of Service Configuration Guide

Cisco Nexus 1000V Security Configuration Guide

Cisco Nexus 1000V System Management Configuration Guide

Cisco Nexus 1000V VXLAN Configuration Guide

Programming Guide

Cisco Nexus 1000V XML API Configuration Guide

Reference Guides

Cisco Nexus 1000V Command Reference

Cisco Nexus 1000V MIB Quick Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide

Cisco Nexus 1000V Password Recovery Procedure

Cisco NX-OS System Messages Reference

Virtual Services Appliance Documentation

The *Cisco Nexus Virtual Services Appliance* documentation is available at http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html.

Virtual Security Gateway Documentation

The *Cisco Virtual Security Gateway for Nexus 1000V Series Switch* documentation is available at http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html.

Virtual Wide Area Application Services (vWAAS) Documentation

The *Virtual Wide Area Application Services* documentation is available at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

ASA 1000V Cloud Firewall Documentation

The *ASA 1000V Cloud Firewall* documentation is available at http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html.

Documentation Feedback

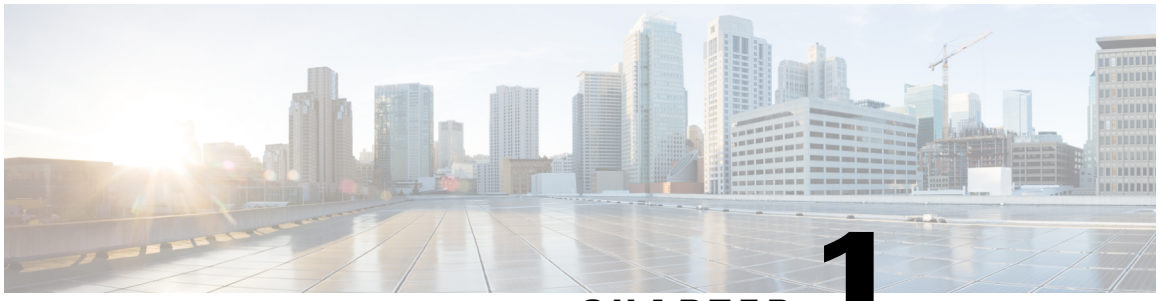
To provide technical feedback on this document, or to report an error or omission, please send your comments to . We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Overview

This chapter includes the following sections:

Information About Virtualization

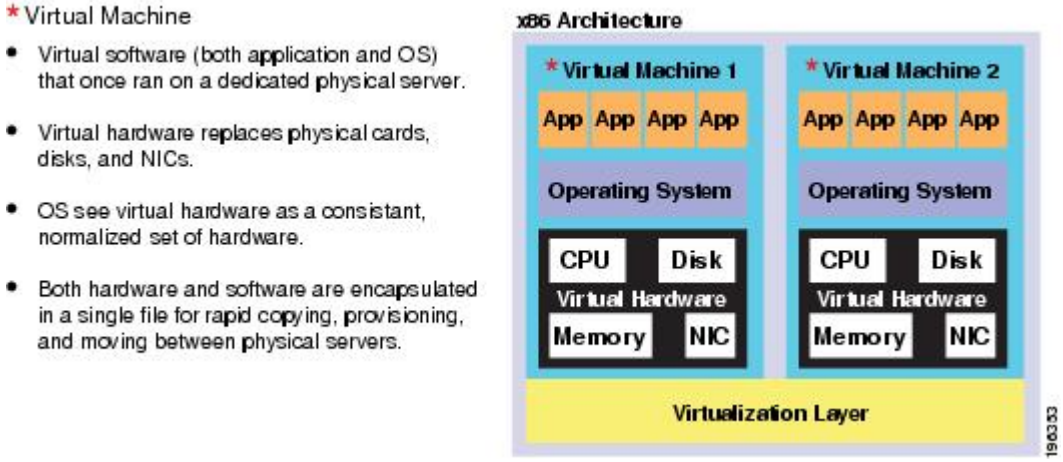
Virtualization allows multiple virtual machines to run in isolation, side by side on the same physical machine.

Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and applications are loaded. The operating system detects a consistent, normalized set of hardware regardless of the actual physical hardware components.

Virtual machines are encapsulated into files for rapid saving of the configuration, copying, and provisioning. You can move full systems (fully configured applications, operating systems, BIOS and virtual hardware) within seconds from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

The following figure shows two virtual machines (VMs) side by side on a single host.

Figure 1: Two Virtual Machines Running on the Same Physical Machine



The following table lists the documents and videos that you need to use when performing a new installation or upgrade to Release 4.2(1)SV1(5.2).

Procedure	Document	Video
New Installation	Installing the Cisco Nexus 1000V, on page 15	Cisco Nexus 1000V Release 4.2(1)SV1(5.1) Installation
Upgrading from Release 4.0(1)SV1(3) through Release 4.0(1)SV1(3d) to Release 4.2(1)SV1(5.2).	Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.2), on page 123	Upgrading from Release 4.0(4)SV1(3, 3a, 3b) to Release 4.2(1)SV1(4)
Upgrading from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.2)	Upgrading from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2)	Upgrading the Cisco Nexus 1000V VSMs from Release 4.2(1)SV1(4) to Release 4.2(1)SV1(4a)

Information About the Cisco Nexus 1000V

The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is Ethernet standard compliant, including the Catalyst 6500 series switch, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000V is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL).

Cisco and VMware jointly designed APIs that produced the Cisco Nexus 1000V. The Cisco Nexus 1000V is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. This solution offloads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy.

Cisco Nexus 1000V and Its Components

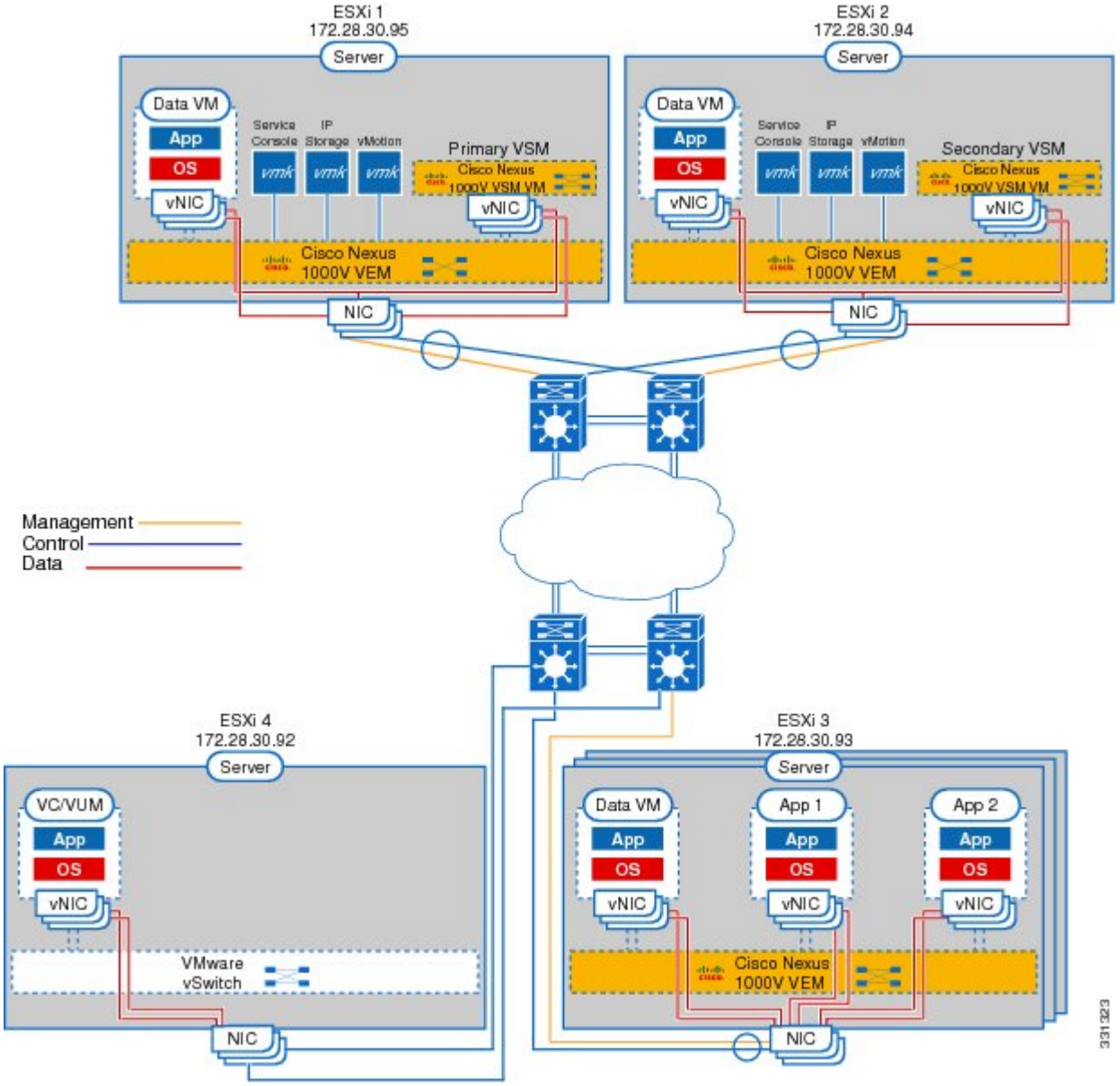
Note A list of terms used with the Cisco Nexus 1000V can be found in Glossary, on page 175.

The Cisco Nexus 1000V is a virtual access software switch that works with VMware vSphere and has the following components:

- Virtual Supervisor Module (VSM)—The control plane of the switch and a virtual machine that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)—A virtual line card embedded in each VMware vSphere (ESX) host. The VEM is partly inside the kernel of the hypervisor and partly in a user-world process, called the VEM Agent.

The following figure shows the relationship between the Cisco Nexus 1000V components.

Figure 2: Cisco Nexus 1000V Installation Diagram for Layer 3



Information About the Virtual Supervisor Module

The VSM is a virtual appliance that can be installed in either a standalone or active/standby HA pair. The VSM, with the VEMs that is controls, performs the following functions for the Cisco Nexus 1000V system:

- Configuration
- Management

- Monitoring
- Diagnostics
- Integration with VMware vCenter Server

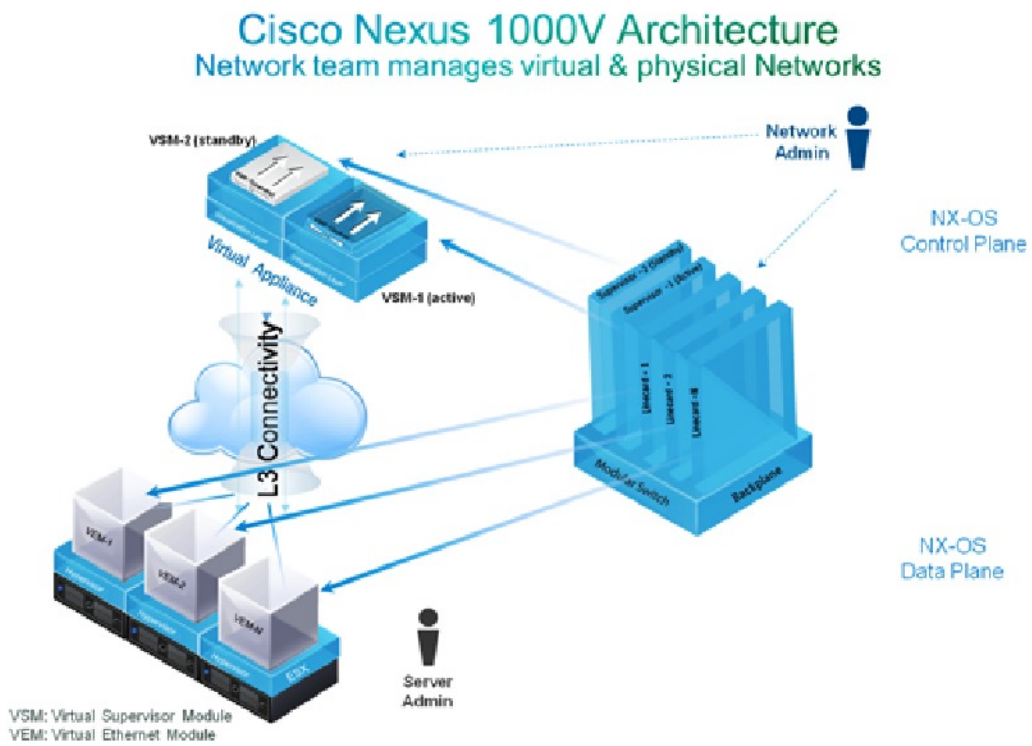
A single VSM can manage up to 64 VEMs.

Note We recommend an active/standby HA pair configuration.

The VSM uses an external network fabric to communicate with the VEMs. The physical NICs on the VEM server are uplinks to the external fabric. VEMs switch traffic between the local virtual Ethernet ports connected to VM vNICs, but do not switch traffic to other VEMs. Instead, a source VEM switches packets to uplinks that the external fabric delivers to the target VEM. The VSM runs the control plane protocols and configures the state of each VEM, but it never actually forwards packets.

A single VSM can control up to 64 VEMs. We recommend that you install two VSMs in an active-standby configuration for high availability. With the 64 VEMs and the redundant supervisors, the Cisco Nexus 1000V 1000V can be viewed as a 66-slot modular switch. See the following figure.

Figure 3: Cisco Nexus 1000V Architecture



A single Cisco Nexus 1000V instance, including dual-redundant VSMs and managed VEMs, forms a switch domain. Each Cisco Nexus 1000V domain within a VMware vCenter Server must be distinguished by a unique integer called the domain identifier.

Information About the Virtual Ethernet Module

Each hypervisor is embedded with one VEM, which is a lightweight software component that replaces the virtual switch by performing the following functions:

- Advanced networking and security
- Switching between directly attached virtual machines
- Uplinking to the rest of the network

Note Only one version of VEM can be installed on an ESX/ESXi host at any given time.

In the Cisco Nexus 1000V, traffic is switched between virtual machines locally at each VEM instance. Each VEM also interconnects the local virtual machine with the rest of the network through the upstream access-layer network switch (blade, top-of-rack, end-of-row, and so forth). The VSM runs the control plane protocols and configures the state of each VEM accordingly, but it never forwards packets.

In the Cisco Nexus 1000V, the module slots are for the primary module 1 and secondary module 2. Either module can act as active or standby. The first server or host is automatically assigned to Module 3. The Network Interface Card (NIC) ports are 3/1 and 3/2 (vmnic0 and vmnic1 on the ESX/ESXi host). The ports to which the virtual NIC interfaces connect are virtual ports on the Cisco Nexus 1000V where they are assigned a global number.

Information About Port Profiles

A port profile is a set of interface configuration commands that can be dynamically applied to either the physical (uplink) or virtual interfaces. A port profile specifies a set of attributes that can include the following:

- VLAN
- Private VLAN (PVLAN)
- Virtual Extensible LAN (VXLAN)
- Access Control List (ACL)
- Quality of Service (QoS)
- Catalyst Integrated Security Features (CISF)
- Virtual Service Domain (VSD)
- Port channel
- Port security
- Link Aggregation Control Protocol (LACP)
- LACP Offload

- NetFlow
- Virtual Router Redundancy Protocol (VRRP)
- Unknown Unicast Flood Blocking (UUFB)

The network administrator defines port profiles in the VSM. When the VSM connects to vCenter Server, it creates a Distributed Virtual Switch (DVS), and each port profile is published as a port group on the DVS. The server administrator can then apply those port groups to specific uplinks, VM vNICs, or management ports, such as virtual switch interfaces or VM kernel NICs.

A change to a VSM port profile is propagated to all ports associated with the port profile. The network administrator uses the Cisco NX-OS CLI to change a specific interface configuration from the port profile configuration applied to it. For example, a specific uplink can be shut down or a specific virtual port can have ERSPAN applied to it without affecting other interfaces using the same port profile.

For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide*.

Information About Administrator Roles

The Cisco Nexus 1000V enables network and server administrators to collaborate in managing the switch. The network administrator is responsible for the VSM, including its creation, configuration and maintenance. The server administrator manages the hosts and the VMs, including the connection of specific VM ports and host uplinks to specific port groups, which are published in the vCenter Server by the network administrator. The VEMs are part of the network administrator's domain, but the server administrator is responsible for the installation, upgrade, or deletion of a VEM.

The following table compares the roles of the network administrator and server administrator.

Network Administrator	Server Administrator
• Creates, configures, and manages virtual switches (VMware vSwitches). • Creates, configures, and manages port profiles, including the following: ◦ Security ◦ Port channels ◦ QoS policies	• Assigns the following to port groups: ◦ vNICs ◦ VMkernel interfaces ◦ Service console interfaces • Assigns physical NICs (also called PNICs).

Differences Between the Cisco Nexus 1000V and a Physical Switch

The following are the differences between the Cisco Nexus 1000V and a physical switch:

- Joint management by network and server administrators

- External fabric—The supervisor(s) and line cards in a physical switch have a shared internal fabric over which they communicate. The Cisco Nexus 1000V uses the external fabric.
- No switch backplane—Line cards in a physical switch can forward traffic to each other on the switch's backplane. Because the Cisco Nexus 1000V lacks this backplane, a VEM cannot directly forward packets to another VEM. Instead, it has to forward the packet using an uplink to the external fabric, which then switches it to the destination.
- No Spanning Tree Protocol—The Cisco Nexus 1000V does not run STP because STP deactivates all but one uplink to an upstream switch, preventing full utilization of uplink bandwidth. Instead, each VEM is designed to prevent loops in the network topology.
- Port channels only for uplinks—The uplinks in a host can be bundled in a port channel for load balancing and high availability. The virtual ports cannot be bundled into a port channel.

Layer 3 and Layer 2 Control Modes

VSM to VEM Communication

The VSM and the VEM can communicate over a Layer 2 network or a Layer 3 network. These configurations are respectively referred to as Layer 2 or Layer 3 control mode.

Layer 3 Control Mode

The VEMs can be in a different subnet than the VSM and also from each other in the Layer 3 control mode. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs.

Each VEM needs a designated VMkernel NIC interface that is attached to the VEM that communicates with the VSM. This interface, which is called the L3 Control vmknic, must have a system port profile applied to it (see the Information About System Port Profiles, on page 10 and Information About System VLANs, on page 10), so the VEM can enable it before contacting the VSM.

For more information on the Layer 3 control mode, see the "Configuring the Domain" chapter in the *Cisco Nexus 1000V System Management Configuration Guide*.

Layer 2 Control Mode

The VSM and VEM are in the same subnet in the Layer 2 control mode.

For more information on Layer 2 control mode, see Configuring Layer 2 Connectivity, on page 74 and Migrating from Layer 2 to Layer 3.

Management, Control, and Packet VLANs

Information About the Control VLAN

The control VLAN is used for communication between the VSM and the VEMs within a switch domain. The control interface is the first interface on the VSM and is labeled “Network Adapter 1” in the virtual machine network properties.

- The control VLAN is used for the following:
  - VSM configuration commands to each VEM and their responses.
  - VEM notifications to the VSM. For example, a VEM notifies the VSM of the attachment or detachment of ports to the Distributed Virtual Switch (DVS).
  - VEM NetFlow exports that are sent to the VSM, where they are forwarded to a NetFlow Collector.
  - VSM active to standby synchronization for high availability.

Management VLANs

A management VLAN, which is used for system login and configuration, corresponds to the mgmt0 interface. The mgmt0 interface appears as the mgmt0 port on a Cisco switch, and is assigned an IP address. Although the management interface is not used to exchange data between the VSM and VEM, it is used to establish and maintain the connection between the VSM and VMware vCenter Server in Layer 2 mode. In (default) Layer 3 mode, when the (default) mgmt0 interface is used for Layer 3 connectivity on the VSM, the management interface communicates with the VEMs and the VMware vCenter Server.

The management interface is the second interface on the VSM and is labeled “Network Adapter 2” in the virtual machine network properties.

Information About the Packet VLAN

Note The packet VLAN is not a component of the Layer 3 control mode.

The packet VLAN is also used for communication between the VSM and the VEMs within a switch domain.

The packet interface is the third interface on the VSM and is labeled “Network Adapter 3” in the virtual machine network properties.

The packet VLAN is used to tunnel network protocol packets between the VSM and the VEMs such as the Cisco Discovery Protocol (CDP), Link Aggregation Control Protocol (LACP), and Internet Group Management Protocol (IGMP).

You can use the same VLAN for control, packet, and management, but you can also use separate VLANs for flexibility. Make sure that the network segment has adequate bandwidth and latency.

For more information about VLANs, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide*.

System Port Profiles and System VLANs

Information About System Port Profiles

System port profiles can establish and protect ports and VLANs that need to be configured before the VEM contacts the VSM.

When a server administrator adds a host to the DVS, its VEM must be able to contact the VSM. Because the ports and VLANs used for this communication are not yet in place, the VSM sends a minimal configuration, including system port profiles and system VLANs, to the vCenter Server, which then propagates it to the VEM.

When configuring a system port profile, you assign VLANs and designate them as system VLANs. The port profile becomes a system port profile and is included in the Cisco Nexus 1000V opaque data. Interfaces using the system port profile, which are members of one of the defined system VLANs, are automatically enabled and forwarding traffic when the VMware ESX starts even if the VEM does not have communication with the VSM. The critical host functions are enabled even if the VMware ESX host starts and cannot communicate with the VSM.

Caution VMkernel connectivity can be lost if you do not configure the relevant VLANs as system VLANs.

Information About System VLANs

A system VLAN must be defined in both the Ethernet and vEthernet port profiles to automatically enable a specific virtual interface to forward traffic outside the ESX host. If the system VLAN is configured only on the port profile for the virtual interface, the traffic will not be forwarded outside the host. Conversely, if the system VLAN is configured only on the Ethernet port profile, the VMware VMkernel interface that needs that VLAN is not enabled by default and does not forward traffic.

The following ports must use system VLANs:

- Control and packet VLANs in the uplinks that communicate with the VSM.
- Management VLAN in the uplinks and port profiles (that is, the Ethernet and vEthernet ports) and VMware kernel NICs used for VMware vCenter Server connectivity or Secure Shell (SSH) or Telnet connections.
- VLAN used for remote storage access (iSCSI or NFS).

Caution You must use system VLANs sparingly and only as described in the section. Only 32 system port profiles are supported.

After a system port profile has been applied to one or more ports, you can add more system VLANs, but you can only delete a system VLAN after removing the port profile from service. This action prevents accidentally deleting a critical VLAN, such as a host management VLAN or a VSM storage VLAN.

Note One VLAN can be a system VLAN on one port and a regular VLAN on another port in the same ESX host.

To delete a system VLAN, see the *Cisco Nexus 1000V Port Profile Configuration Guide*.

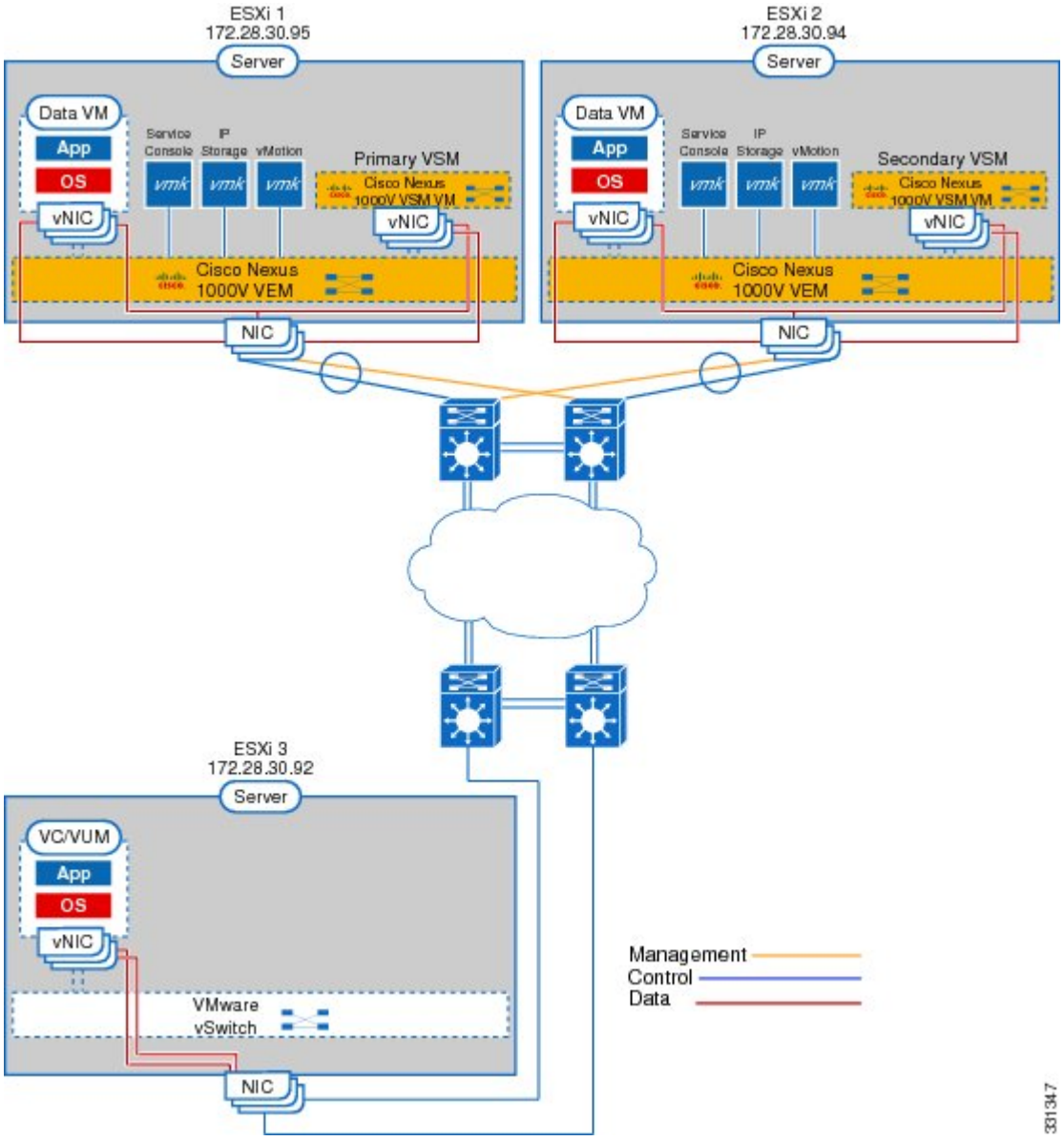
Recommended Topologies

Layer 3 Topology

The Cisco Nexus 1000V software installation installs the VSM software required to create the VSM VM.

The following figure shows an example of redundant VSM VMs, where the software for the primary VSM is installed on ESXi 1, and the software for the secondary VSM is installed on ESXi 2 for Layer 3 connectivity.

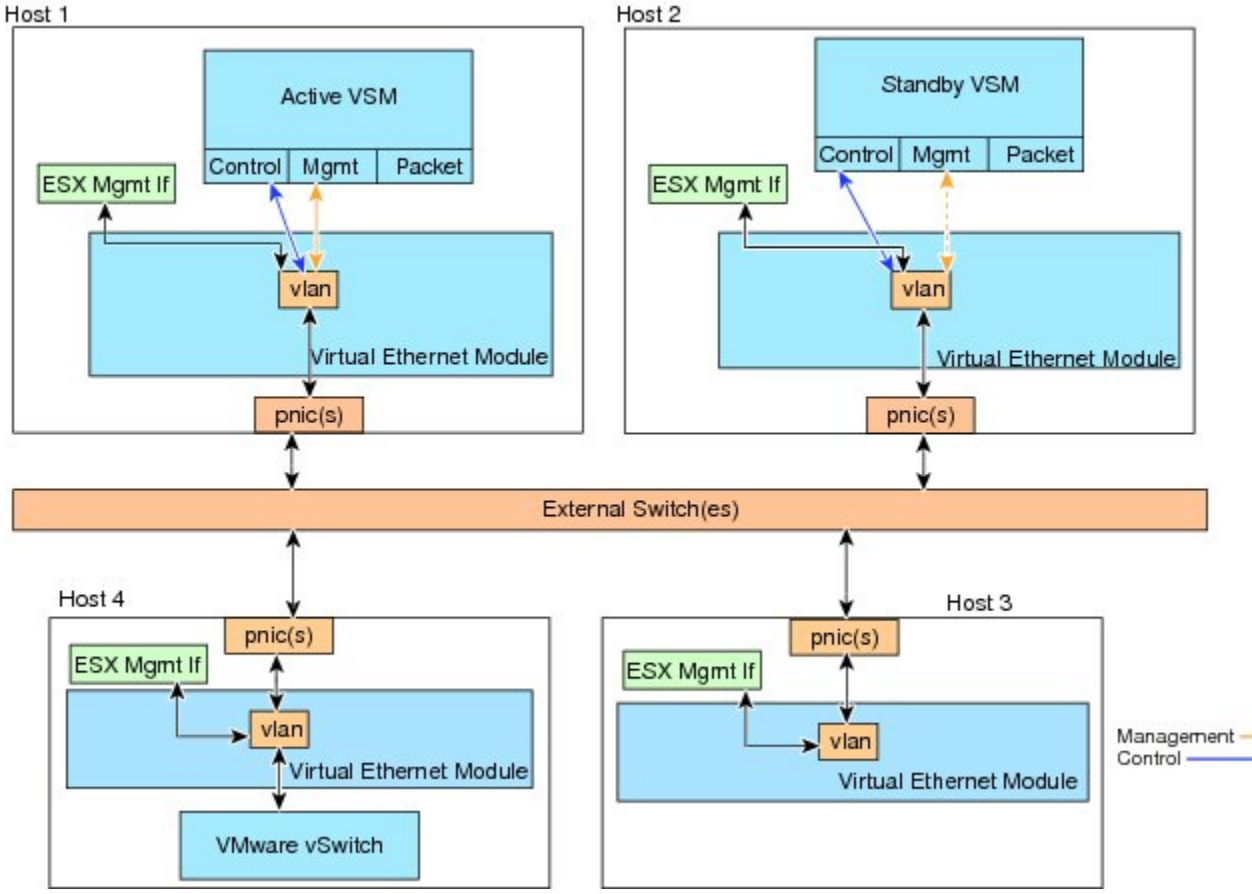
Figure 4: Cisco Nexus 1000V Installation Diagram for Layer 3



Control and Management on the Same VLAN Topology

The following figure shows a VSM and VEM that run on the same host in Layer 3 mode with the management and control interfaces on the same VLAN.

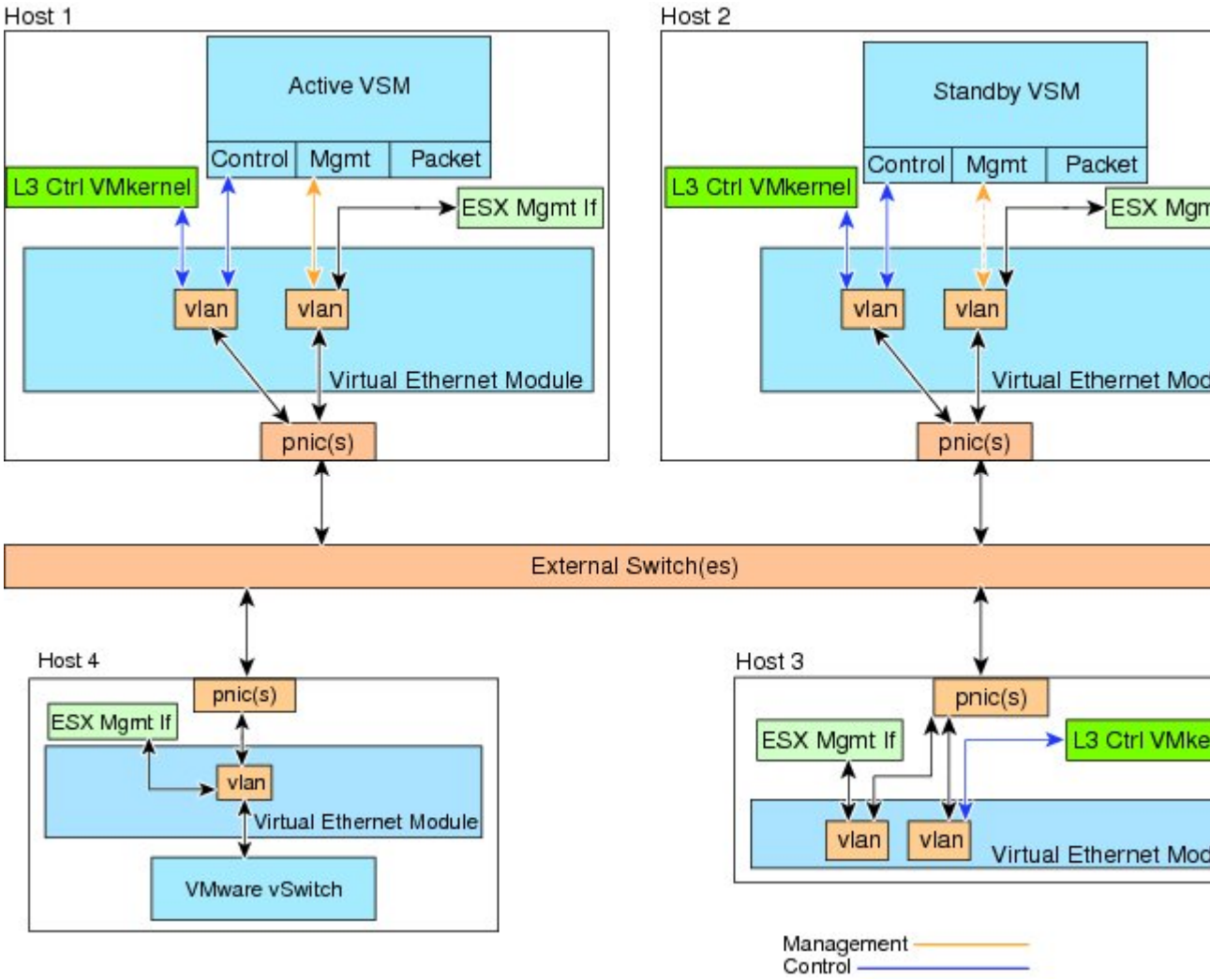
Figure 5: Control and Management on Same VLAN



Control and Management on Separate VLANs Topology

The following figure shows a VSM and VEM that run on the same host in Layer 3 mode with the management and control interfaces on different VLANs.

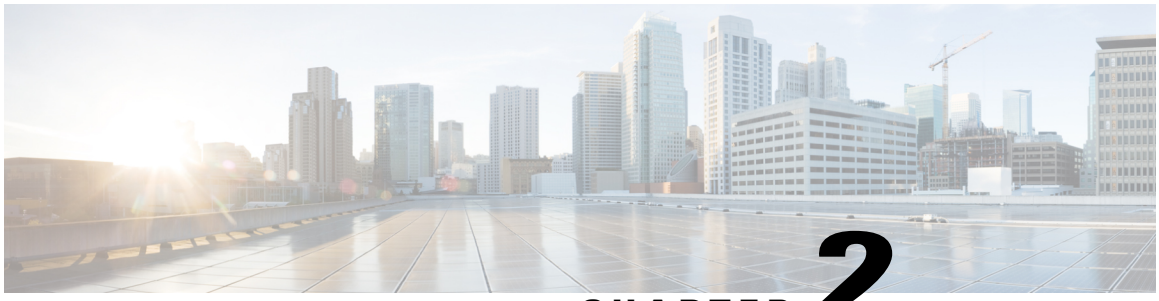
Figure 6: Control and Management on Separate VLAN



VMware Interaction

You can use a Cisco Nexus 1000V VSM as a virtual machine in ESX/ESXi 4.1 or later releases. (requires Enterprise Plus license edition of vSphere 4).

For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.



CHAPTER 2

Installing the Cisco Nexus 1000V

This chapter includes the following sections:

Information About Installing the Cisco Nexus 1000V

VSM Software

You can obtain the Cisco Nexus 1000V software from the Cisco Nexus 1000V Series switches web page:

Cisco Nexus 1000V Download Software page

The filename is `Nexus1000v.4.2.1.SV1.5.2.zip`.

VEM Software

You can obtain the Virtual Ethernet Module (VEM) software from the sources listed in the following table:

Table 1: VEM Software Sources

Source	Description
VSM	After the VSM has been installed as a Virtual Machine (VM), copy the file that contains the VEM software from the Virtual Supervisor Module (VSM) home page located at the following URL: http://*VSM_IP_Address*/
Cisco	Download the VEM software from the Cisco Nexus 1000V Download Software page.

Information About the Nexus 1000V Installation Management Center

The Nexus 1000V Installation Management Center is the graphical user interface (GUI) for installing the VSMs in high availability (HA) mode and the VEMs on ESX/ESXi hosts.

To prevent a disruption in connectivity, all port profiles are created with a system VLAN. You can change this after migration if needed.

The host and adapter migration process moves all physical network interface cards (PNICs) used by the VSM from the VMware vSwitch to the Cisco Nexus 1000V Distributed Virtual Switch (DVS).

The migration process supports Layer 2 and Layer 3 topologies.

The installer does the following:

- Creates port profiles for the control, management, and packet port groups.
- Creates uplink port profiles.
- Creates port profiles for VMware kernel NICs.
- Specifies a VLAN to be used for system login and configuration, and control and packet traffic.

Note You can use the same VLAN for control, packet, and management port groups, but you can also use separate VLANs for flexibility. If you use the same VLAN, make sure that the network segment where the VLAN resides has adequate bandwidth and latency.

- Enables Telnet and Secure Shell (SSH) and configures an SSH connection.
- Creates a Cisco Nexus 1000V plug-in and registers it on the vCenter Server.
- Migrates each VMware port group or kernel NIC to the correct port profile.
- Migrates each physical network interface card (PNIC) from the VMware vSwitch to the correct uplink on the DVS.
- Adds the host to the DVS.

Prerequisites for Installing the Cisco Nexus 1000V

Nexus 1000V Installation Management Center Prerequisites

Note The Installation Management Center requires you to satisfy all the prerequisites.

If you migrate the host and adapters from the VMware vSwitch to the Cisco Nexus 1000V DVS:

- The host must have one or more physical NICs on each VMware vSwitch in use.
- The VMware vSwitch must not have any active VMs.

  To prevent a disruption in connectivity during migration, any VMs that share a VMware vSwitch with port groups used by the VSM must be powered off.
- You must also configure the VSM connection to the vCenter server datacenter where the host resides.
- Host should have only one VMware vSwitch.
- Make sure no VEMs were previously installed on the host where the VSM resides.
- You must have administrative credentials for the vCenter Server.

Host Prerequisites

The ESX or ESXi hosts to be used for the Cisco Nexus 1000V have the following prerequisites:

- You have already installed and prepared the vCenter Server for host management using the instructions from VMware.
- SSH has been enabled.
- You should have the VMware vSphere Client installed.

- You have already installed the VMware Enterprise Plus license on the hosts.
- All VEM hosts must be running ESX/ESXi 4.1 or later releases.
- You have two physical NICs on each host for redundancy.
- All hosts must have Layer 2 connectivity to each other.
- If you are using a set of switches, make sure that the inter-switch trunk links carry all relevant VLANs, including control and packet VLANs. The uplink should be a trunk port that carries all VLANs configured on the host.
- The control and management VLANs must already be configured 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 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 following table lists the minimum requirements for hosting a VSM.

Table 2: Minimum Requirements for a VM Hosting a VSM

VSM VM Component	Minimum Requirement
Platform	64-bit
Type	Other 64-bit Linux (recommended)
Processor	1
RAM (configured and reserved)	2 GB[1]
NIC	3
SCSI Hard Disk	3 GB with LSI Logic Parallel adapter
CPU speed	1500 MHz[2]

1 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 149 to reserve RAM and set the memory size.

2 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 149 to reserve RAM and set the memory size.

Upstream Switch Prerequisites

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

- If you are using a set of switches, make sure that the inter-switch 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 switch upstream from the Cisco Nexus 1000V on the ports connected to the VEM.
  - On upstream switches, the following configuration is mandatory:

    On your Catalyst series switches with Cisco IOS software, enter the following command:

    (config-if) **spanning-tree portfast trunk**

    or

    (config-if) **spanning-tree portfast edge trunk**

    On your Cisco Nexus 5000 series switches with Cisco NX-OS software, enter the following command:

    (config-if) **spanning-tree port type edge trunk**
  - On upstream switches we highly recommend that you enable the following globally:

    Global BPDU Filtering

    Global BPDU Guard
  - On upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:

    (config-if) **spanning-tree bpdu filter**

    (config-if) **spanning-tree bpdu guard**

  For more information about spanning tree and its supporting commands, see the documentation for your upstream switch.
- Run 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
```

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.
- 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 Layer 3 Topology, on page 11.

VEM Prerequisites

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

Note If the VMware vCenter Server is hosted on the same ESX/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 HA, 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.
- 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 from one of the sources listed in VEM Software, on page 16.
- You have already downloaded the correct VEM software based on the current ESX/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 the vCenter Server.

Guidelines and Limitations

Guidelines and Limitations of the Nexus 1000V Installation Management Center

Configuring the software using the Nexus 1000V Installation Management Center has the following guidelines and limitations:

- For a complete list of port profile guidelines and limitations, see the *Cisco Nexus 1000V Port Profile Configuration Guide*.

Caution Host management connectivity might be interrupted if the management vmknic or vswif are migrated and the uplink's native VLAN is not correctly specified in the setup process.

- If you are installing a Cisco Nexus 1000V in an environment where the upstream switch does not support static port channels, such as the Cisco Unified Computing System (UCS), you must use the **channel-group auto mode** on the **mac-pinning** command instead of the **channel-group auto mode** command.
- We recommend that you install redundant VSMs on the Cisco Nexus 1000V. For information about high availability and redundancy, see the *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide*.
- If the Installation Management Center fails, check the vCenter Server event status. If an event shows failure due to a timeout, then it could be because of a vCenter Server overload. Please consult the VMware website to address a vCenter Server overload event.

Guidelines and Limitations for Installing the Cisco Nexus 1000V

Use the following guidelines and limitations when installing the Cisco Nexus 1000V software:

- Do not enable VMware 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 a user moves a VSM from the VMware vSwitch to the Cisco Nexus 1000V DVS, it is possible that the connectivity between the active and standby VSM is temporarily lost. In that situation, both active and standby VSMs assume the active role. Once the connectivity is restored between the VSMs, the VSM configured with the role of primary reloads itself and comes back as standby.
- If the VSM is moved from the VMware vSwitch to the Cisco Nexus 1000V DVS, it is recommended that you configure the port-security on the VSM vethernet interfaces to secure control/packet MACs.
- 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

- To improve redundancy, install primary and secondary VSM virtual machines in separate hosts that are connected to different upstream switches.

Installing a VSM HA Pair with L3 Mode Behind a VEM Using the Nexus 1000V Installation Management Center

The procedure to install a VSM HA pair behind a VEM is as follows:

Procedure

Step 1 Installing VSM Software Using the Nexus 1000V Installation Management Center
Step 2 Installing VEM Software Using the Nexus 1000V Installation Management Center, on page 33
Step 3 Adding VEM Hosts to the Distributed Virtual Switch, on page 39
Step 4 Moving the Secondary VSM to a Different Host, on page 47
Step 5 Setting Virtual Machine Startup and Shutdown Parameters, on page 56

Installing a VSM HA Pair Using the Nexus 1000V Installation Management Center

Before You Begin

- You have the following information:
  - Control VLAN ID
  - Management VLAN ID
  - Domain ID
  - Management IP address
  - Subnet mask
  - Gateway IP address
  - SVS datacenter name
  - VLAN ID of the untagged traffic
- You have the JDK version 1.6 or later installed.

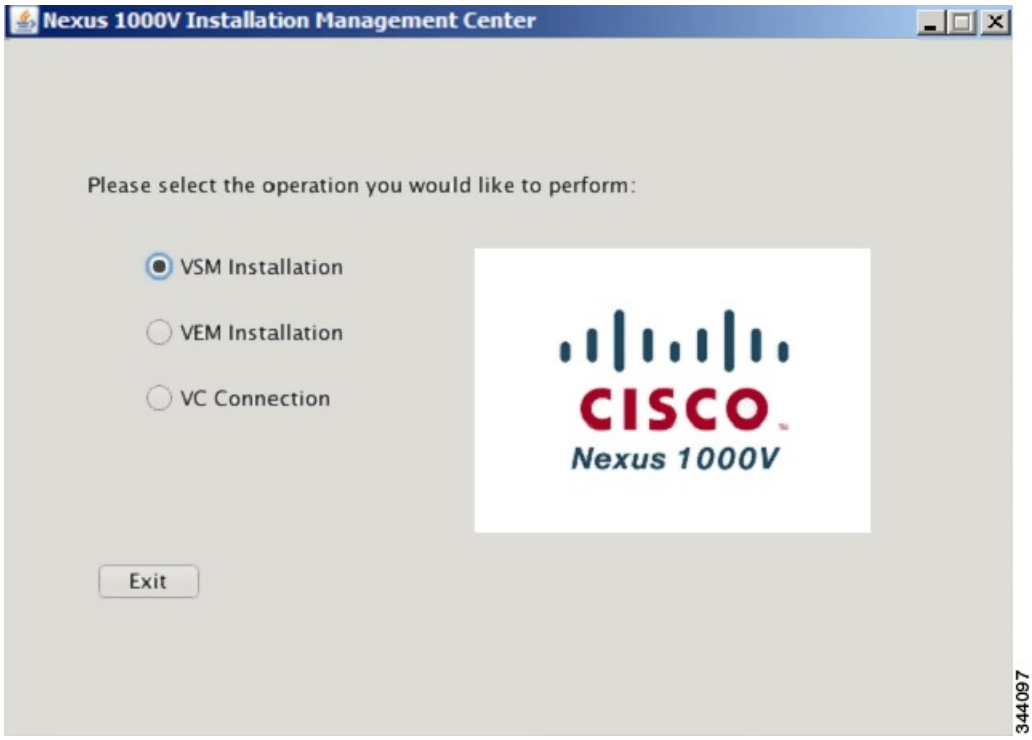
Procedure

Step 1 Download the `Nexus1000v.4.2.1.SV1.5.2.zip` file.
Step 2 Enter the following command from a Windows, Linux, or Mac command prompt.

java -jar zip_file_location/Nexus1000v.4.2.1.SV1.5.2/VSM/Installer_App/Nexus1000V-install.jar

Step 3 In the **Nexus 1000V Installation Management Center** window, click the **VSM Installation** radio button.

Figure 7: Nexus 1000V Installation Management Center Window



Step 4 In the **Enter vCenter Credentials** screen, do the following:

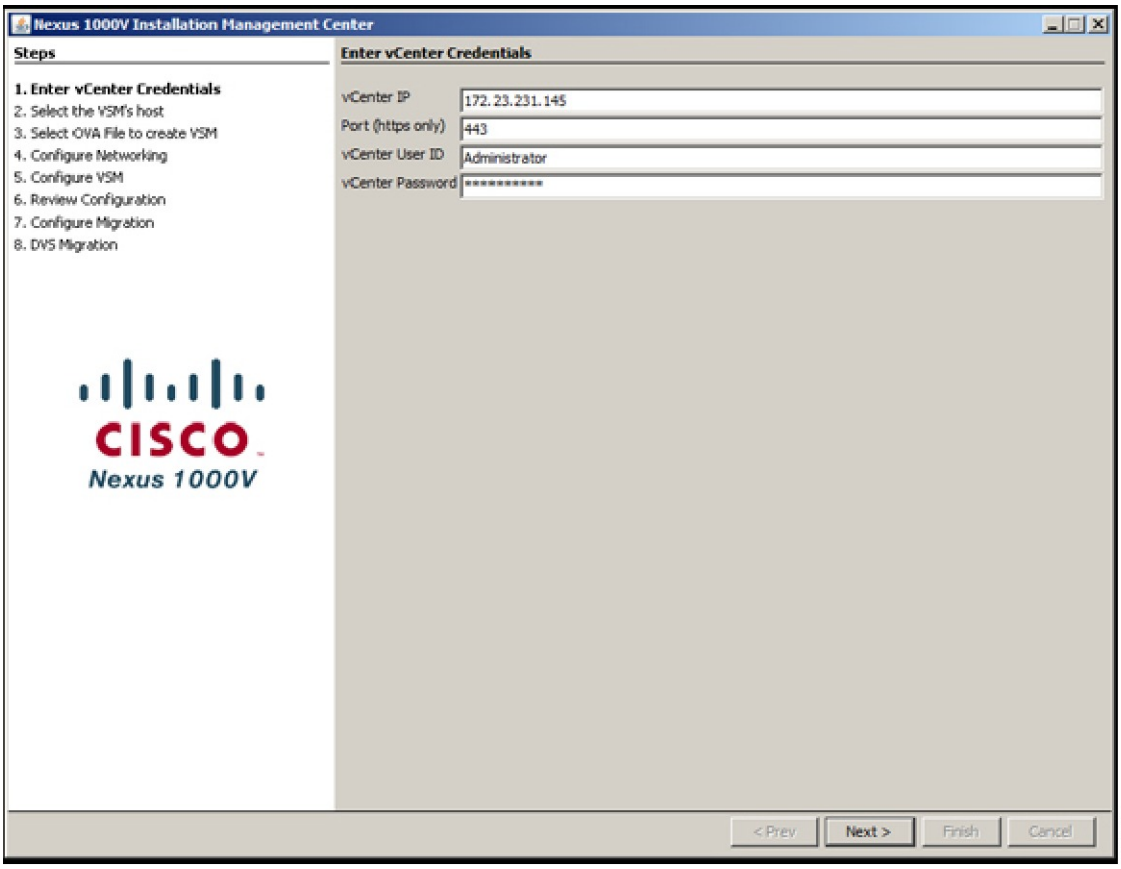
a) Enter the following vCenter credentials:

- vCenter IP address
- Secure HTTP port

  Port 443 is configured by default, but you can change the port if needed.
- vCenter User ID (for a vCenter user with administrator-level privileges)
- vCenter Password (for a vCenter user with administrator-level privileges)

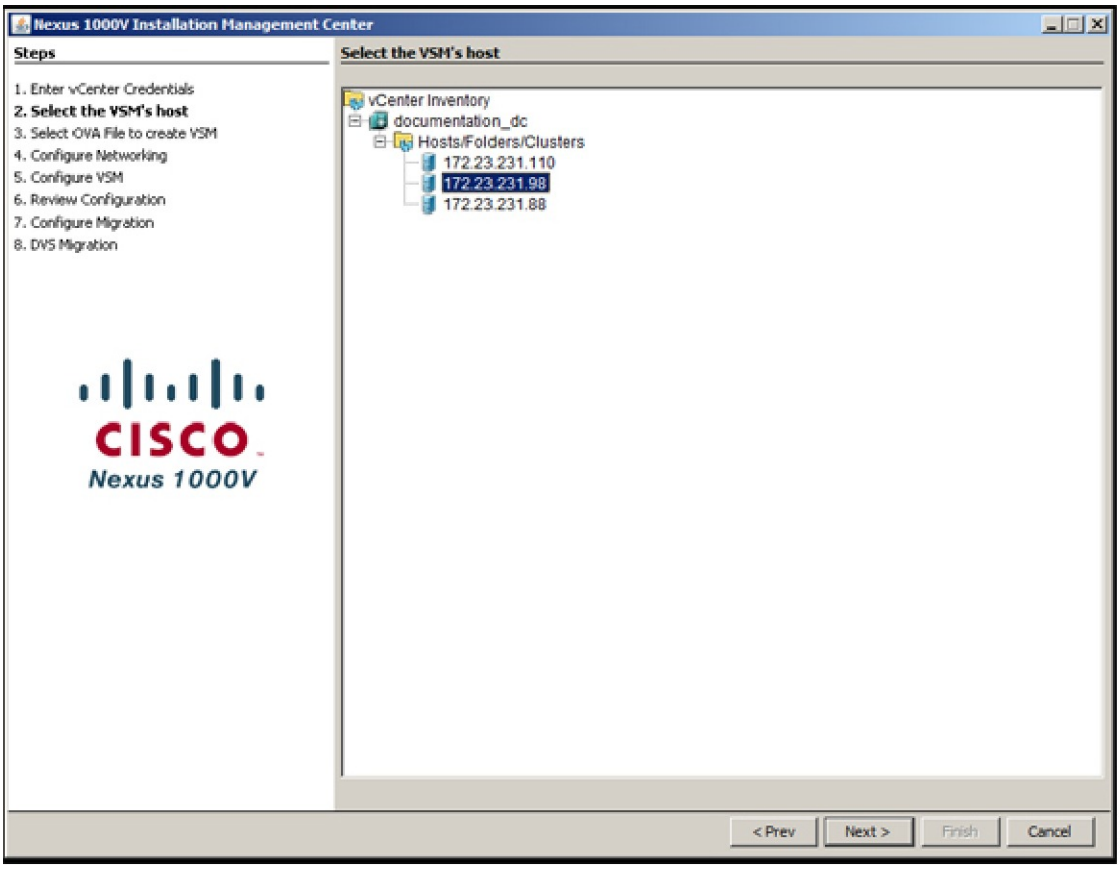
b) Click **Next**.

Figure 8: Enter vCenter Credentials Screen



Step 5 In the **Select the VSM's host** screen, Choose a host where the VSM will be deployed and click **Next**.

Figure 9: Select the VSM's host Screen



Step 6 In the **Select OVA File to create VSM** screen, do the following:

a) Click **Browse OVA** and browse to the location of the OVA file.

b) From the **System Redundancy** drop-down list, choose a System Redundancy value.

Note If you choose a System Redundancy value of HA, a primary and secondary VSM is created.

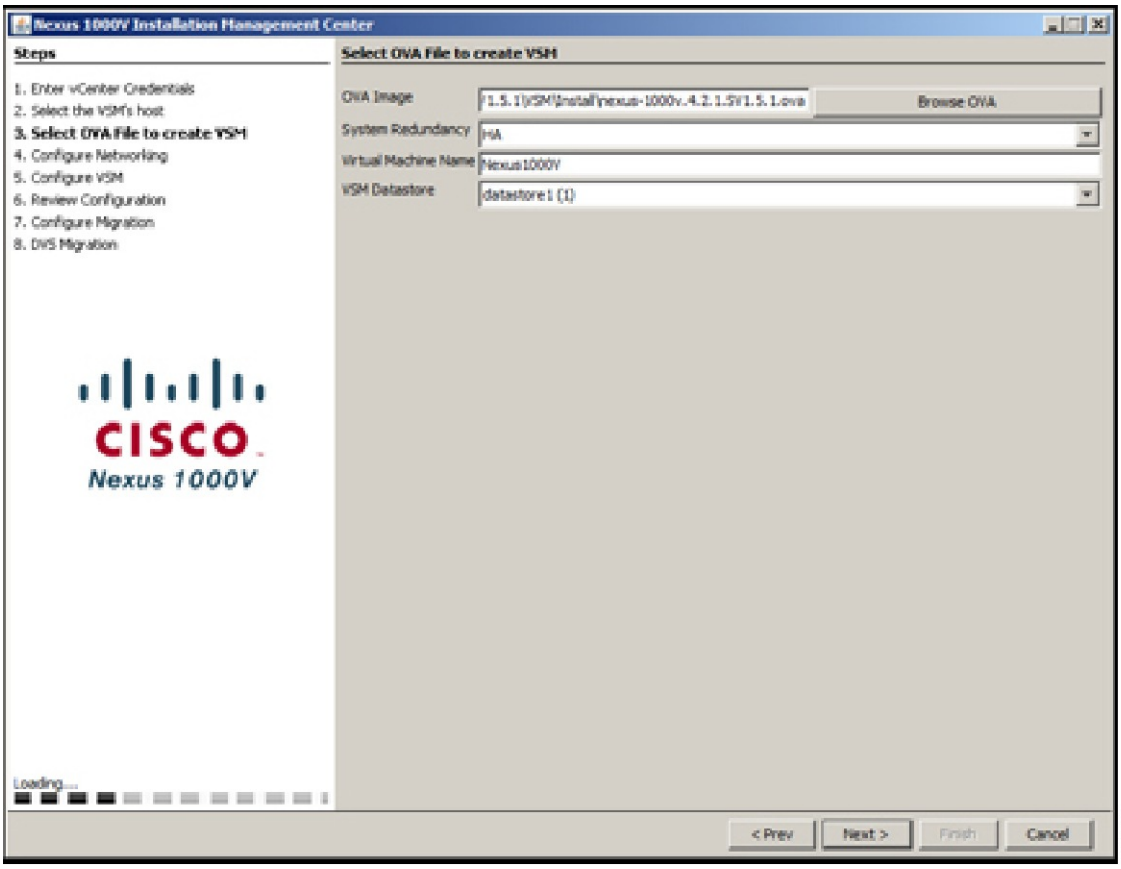
c) In the **Virtual Machine Name** field, enter a name for the virtual machine.

Note The application appends "-1" to the primary VSM and "-2" to the secondary VSM.

d) From the **VSM Datastore** drop-down list, choose a datastore.

e) Click **Next**.

Figure 10: Select OVA File to create VSM Screen



Step 7 To configure Layer 3 connectivity, click the **L3: Configure port groups for L3** radio button in the **Configure Networking** screen.

Note To configure Layer 2 connectivity, see Configuring Layer 2 Connectivity, on page 74.

Step 8 For the control port group, do the following:

a) Click the **Create New** radio button.
b) In the **Port Group Name** field, enter a port group name.
c) In the **VLAN ID** field, enter a VLAN.
d) From the **vSwitch** drop-down list, choose a VMWare vSwitch value.

Step 9 For the management port group, do the following.

a) Click the **Create New** radio button.
b) In the **Port Group Name** field, enter a port group name.
c) In the **VLAN ID** field, enter a VLAN.
d) From the **vSwitch** drop-down list, choose a VMWare vSwitch value.

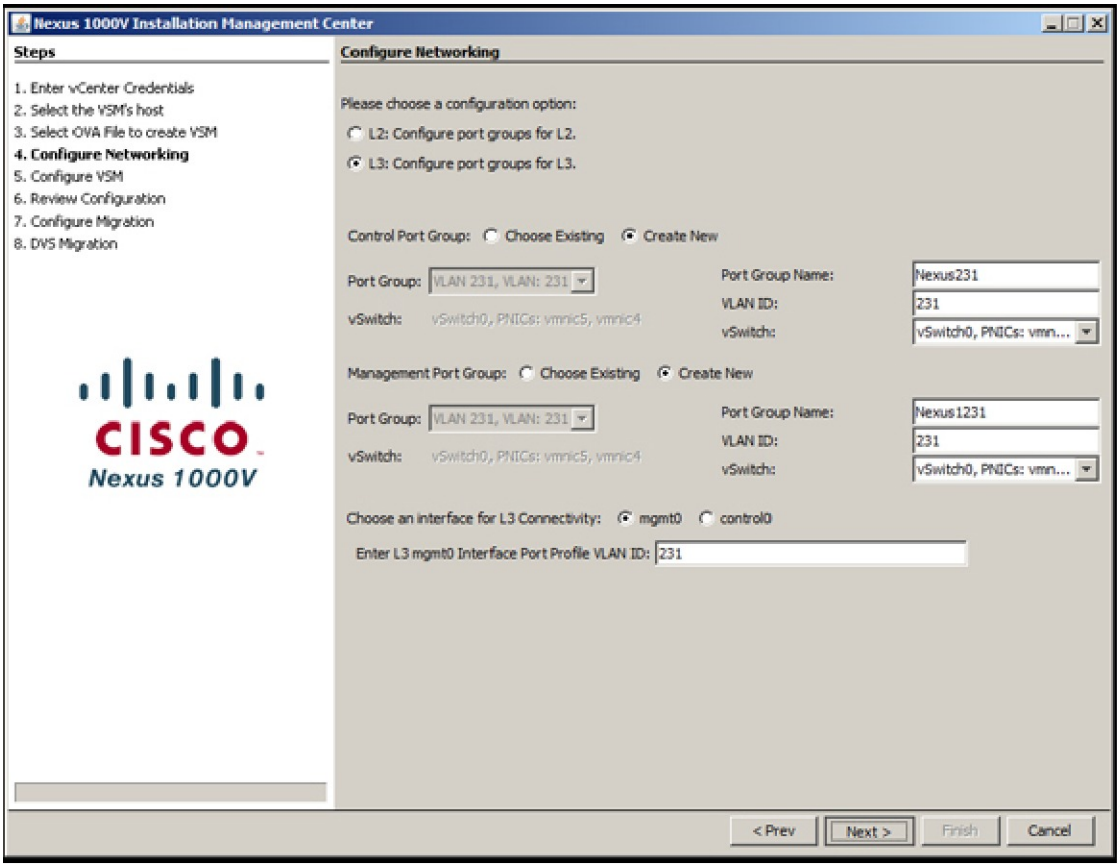
Note You can also use existing port groups for the control and management port groups.

Step 10 For Layer 3 connectivity, choose the **mgmt0** radio button and do the following:

a) In the **Enter L3 mgmt0 Interface Port Profile VLAN ID** field, enter the VLAN of your management network.

b) Click **Next.**

Figure 11: Configure Networking Screen



Note For Layer 3 control0 mode, control and management IP addresses must be in different subnets. Step 10 will fail if the control and management IP addresses are not in different subnets.

Step 11 In the **Configure VSM** screen, enter the following information:

a) In the **Switch Name** field, enter the switch name.

b) In the **Enter Admin Password** field, enter the admin password.

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

c) In the **Confirm Admin Password** field, enter the admin password.

d) In the **Mgmt IP Address** field, enter the mgmt0 IP address of the VSM VM.

e) In the **Subnet Mask** field, enter the subnet mask.

f) In the **Gateway IP address** field, enter the gateway IP address.

g) In the **Domain ID** field, enter the domain ID.

h) From the **SVS Datacenter Name** drop-down list, choose a data center name.

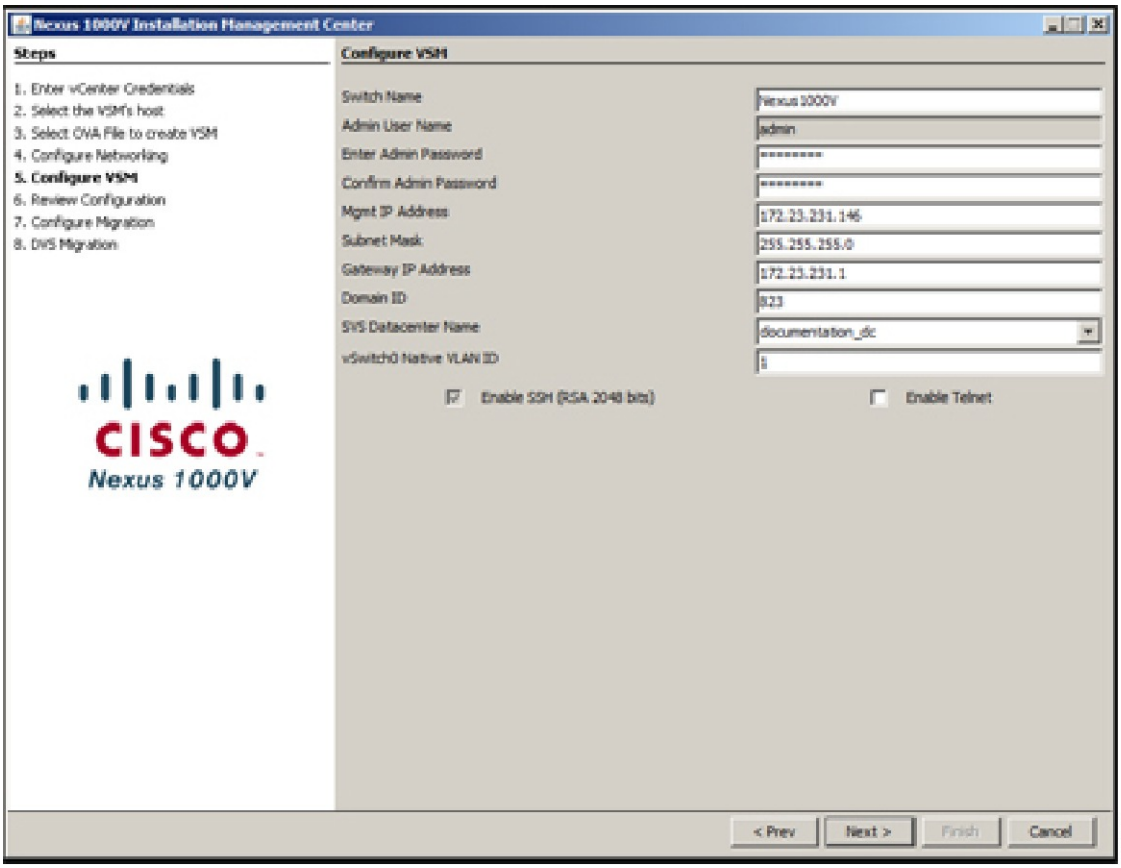
i) In the **vSwitch0 Native VLAN ID** field, enter the native VLAN ID.

Caution Host management connectivity might be interrupted if VMware kernel 0 and the VMware vSwitch interface 0 are migrated and the native VLAN is not correctly specified.

Step 12 (Optional) Click **Enable Telnet** if you want to enable Telnet or click **Enable SSH** if you want to enable SSH.

Step 13 Click **Next.**

Figure 12: Configure VSM Screen

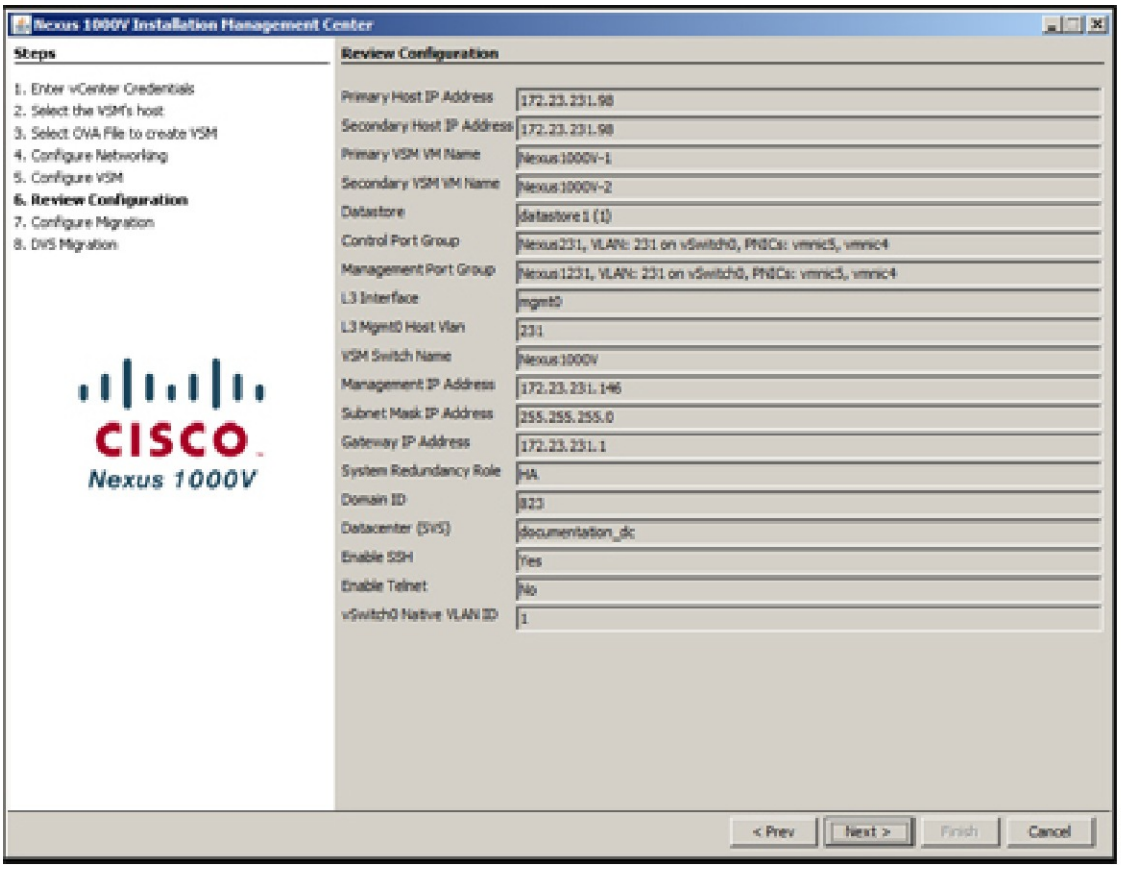


Step 14 In the **Review Configuration** screen, do one of the following:

- To make corrections, click **Prev**, go back to the previous screens, and make corrections.
- If the configuration is correct, continue with Step 14.

Step 15 In the **Review Configuration** screen, click **Next.**

Figure 13: Review Configuration Screen



If you chose a redundancy value of HA, the primary and secondary VSMs are being created.

Step 16 In the **Configure Migration** screen, do the following:

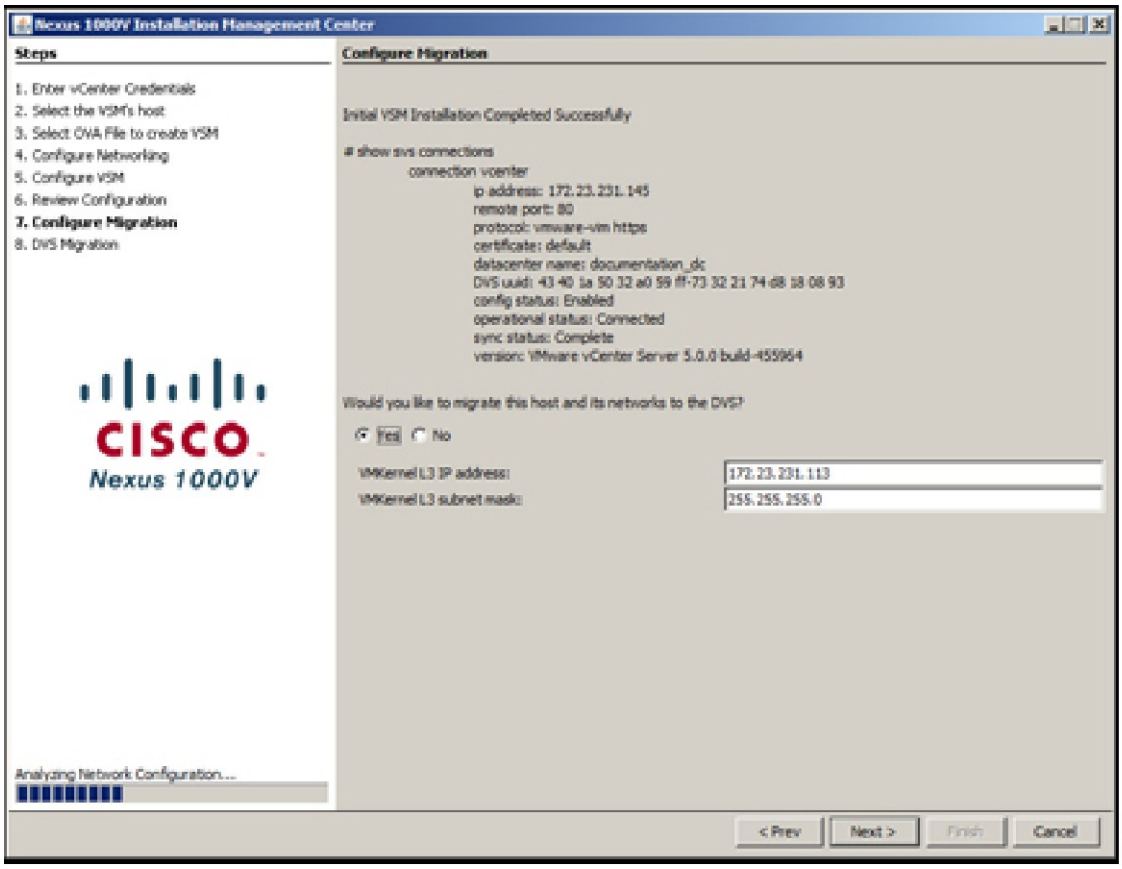
a) Click the **Yes** radio button.
b) In the **VMkernel L3 IP Address** field, enter an IP address.
c) In the **VMkernel L3 subnet mask** field, enter the subnet mask.
When you click **Yes**, one of the channel-group commands in the following table is applied to the uplink port profile during migration.

Port Channel created during migration	For VMware vSwitch Teaming policy in use
A static port channel **channel-group auto mode on**	Route based on IP hash or route based on the originating virtual port ID
A vPC host mode port channel with mac-pinning **channel-group auto mode on mac-pinning**	MAC hash

Note If VUM is not installed, the VSM installer installs the vSphere Installation Bundles (VIBs) as a part of the VSM installation.

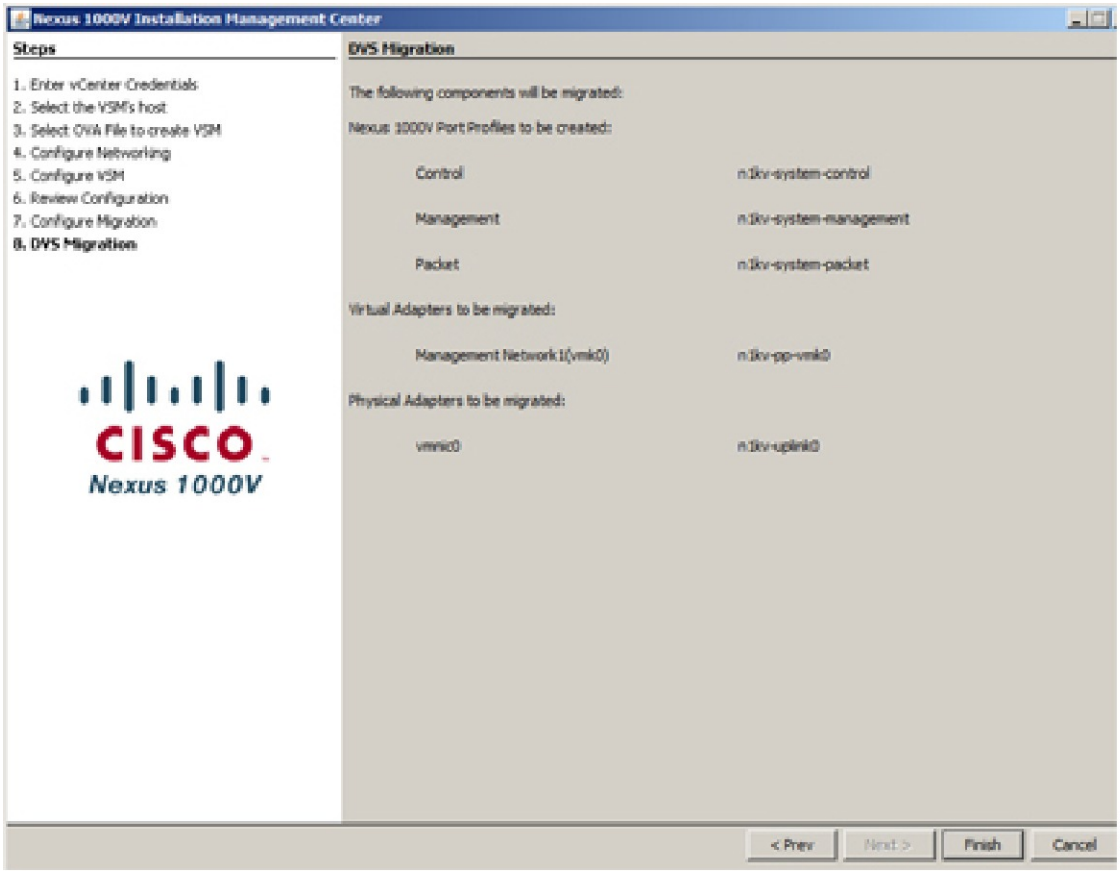
Step 17 In the **Configure Migration** screen, click **Next**.

Figure 14: Configure Migration Screen



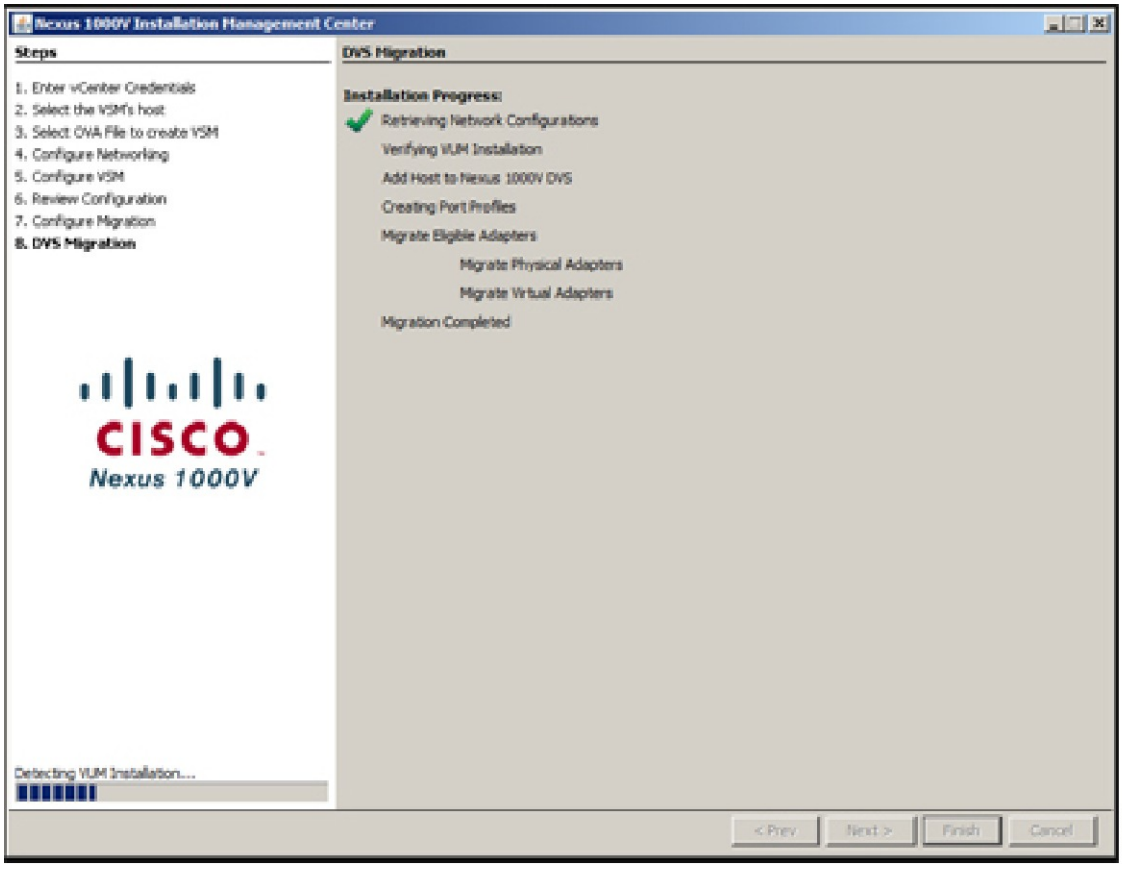
Step 18 In the **DVS Migration Components** screen, click **Finish**.

Figure 15: DVS Migration Components Screen



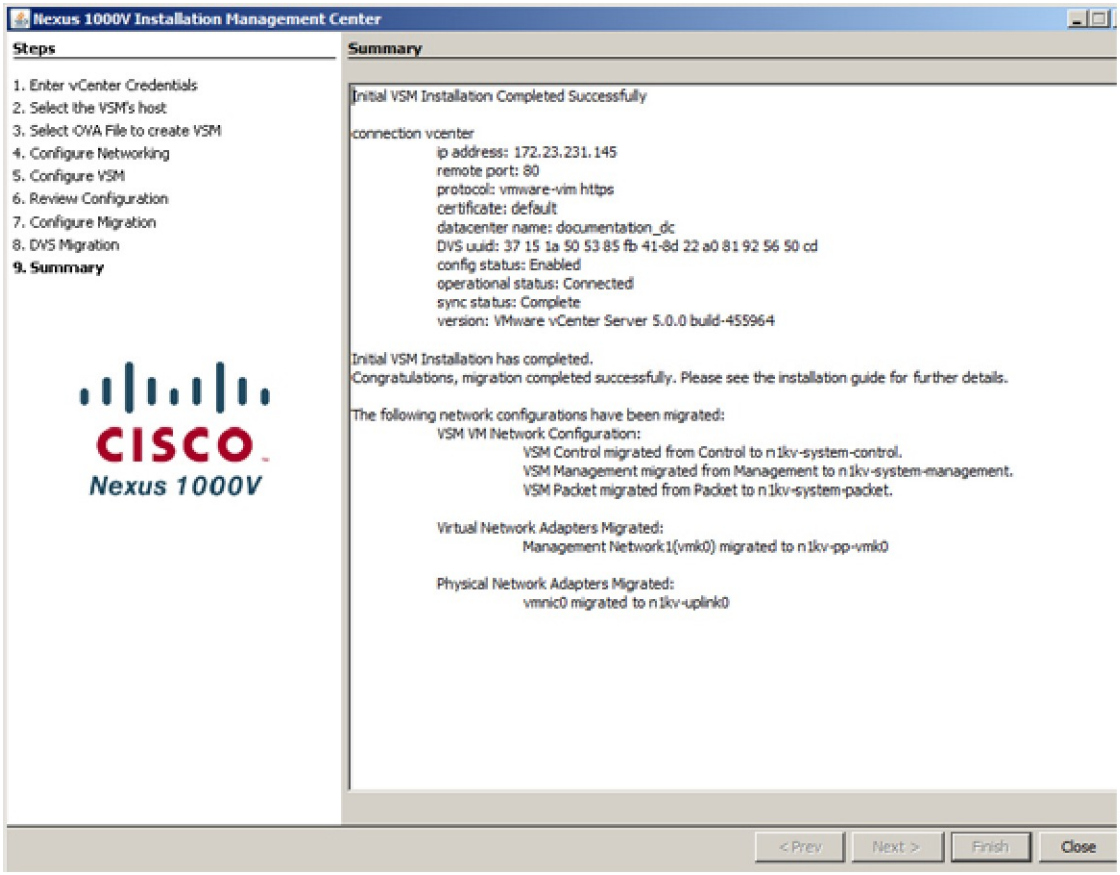
The migration starts and the **DVS Migration Installation Progress** screen opens.

Figure 16: DVS Migration Installation Progress Screen



Step 19 In the **Initial VSM Installation Completed Successfully** screen, click **Close**.

Figure 17: Initial VSM Installation Completed Successfully Screen



VSM installation is complete.

Installing VEM Software Using the Nexus 1000V Installation Management Center

Before You Begin

- You have the following information:
  - vCenter IP address
  - vCenter User ID
  - vCenter Password
  - VSM IP Address
  - VSM Password

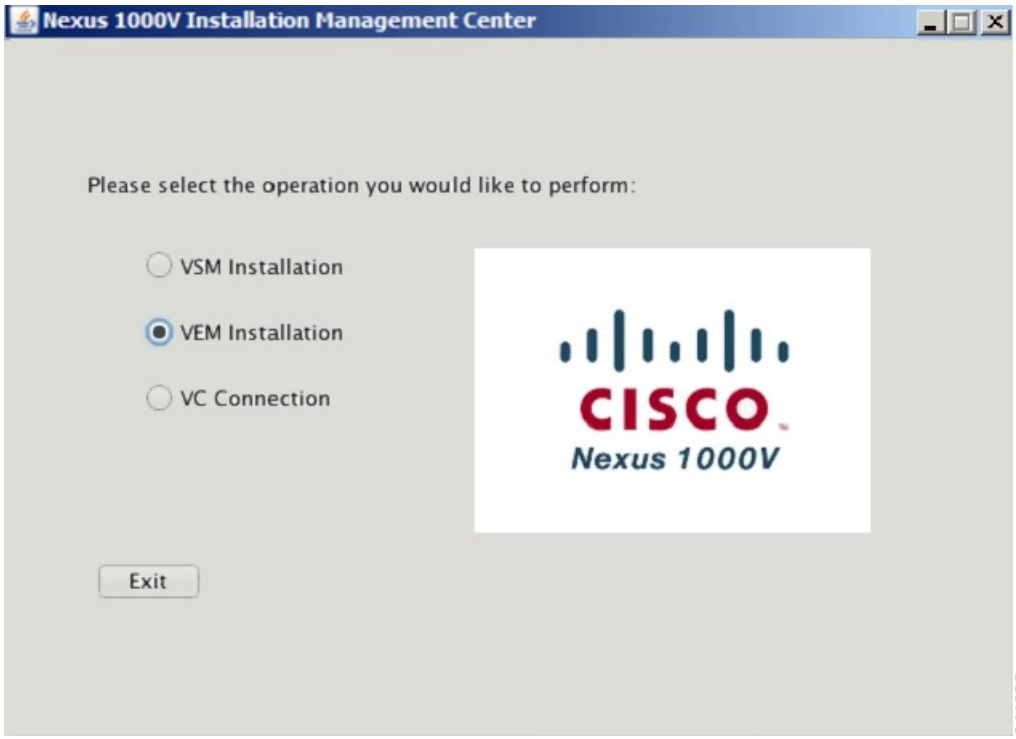
Note The installer application does not expect the VIBs to be available.

Procedure

Step 1 Enter the following command from a Windows, Linux, or Mac command prompt.
java -jar *zip_file_location*/**Nexus1000v.4.2.1.SV1.5.2/VSM/Installer_App/Nexus1000V-launchPad.jar**

Step 2 In the **Nexus 1000V Installation Management Center** window, click the **VEM Installation** radio button.

Figure 18: Nexus 1000V Installation Management Center Window



Step 3 In the **VEM Enter vCenter Credentials** screen, do the following:

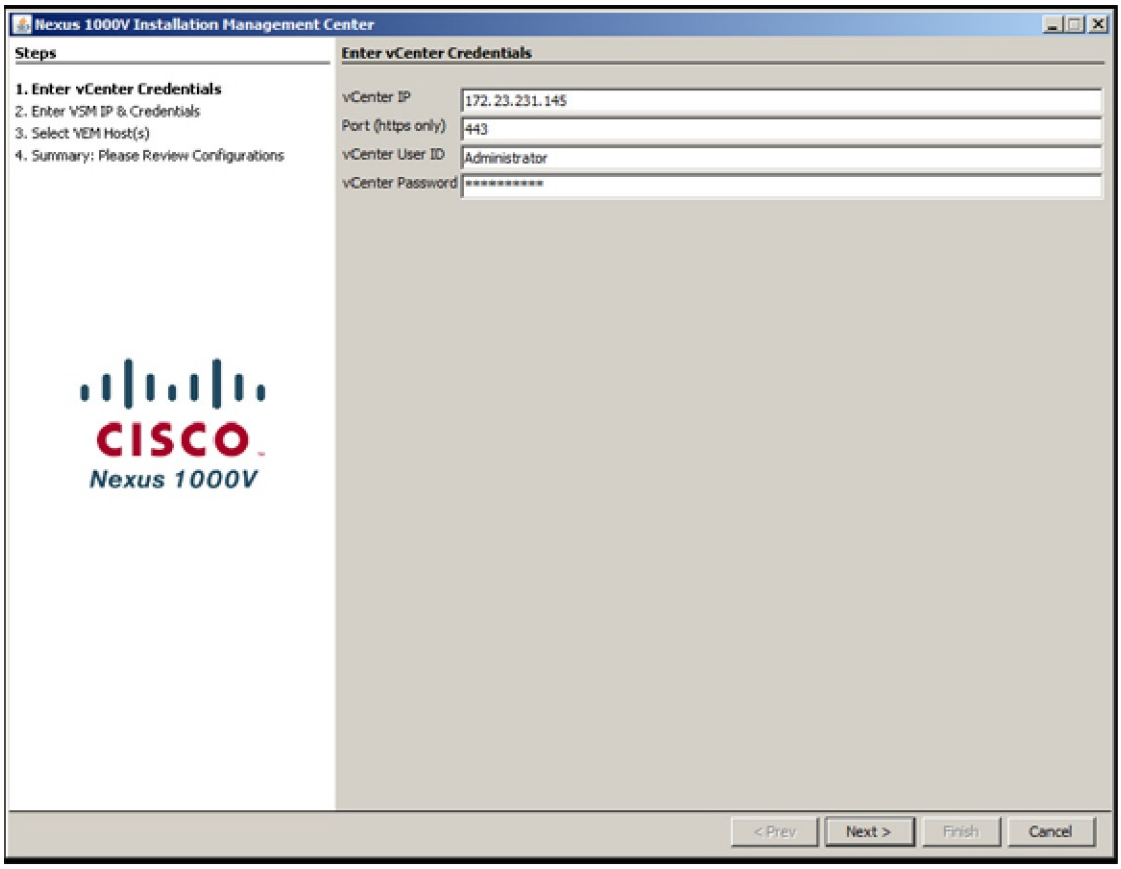
a) Enter the following vCenter Credentials:

- vCenter IP address
- Secure HTTP port

  Port 443 is configured by default, but you can change the port if needed.
- vCenter User ID (for a vCenter user with administrator-level privileges)
- vCenter Password (for a vCenter user with administrator-level privileges)

b) Click **Next**.

Figure 19: VEM Enter vCenter Credentials Screen



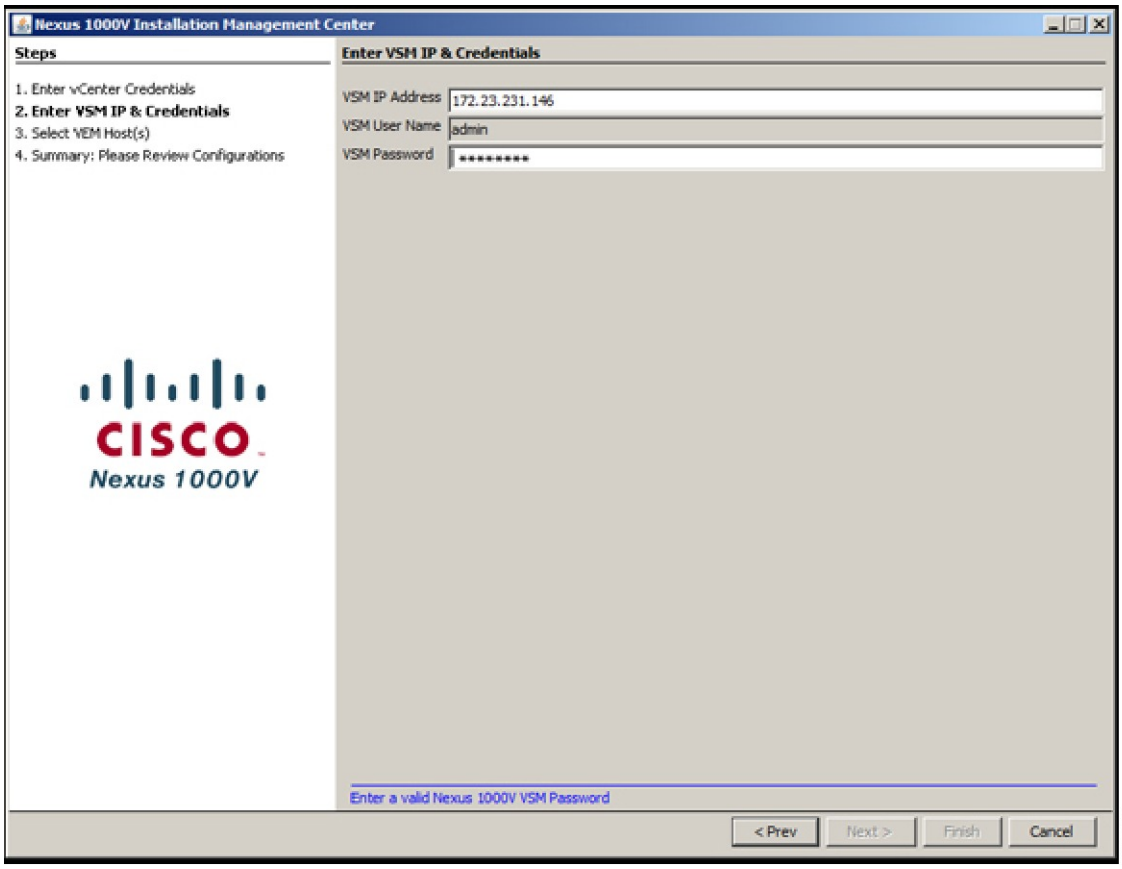
Step 4 In the **Enter VSM IP & Credentials** screen, do the following:

a) Enter the following credentials:

- VSM IP address
- VSM Password

b) Click **Next**.

Figure 20: VEM Enter VSM IP & Credentials Screen



Step 5 In the **Select VEM Host(s)** screen, do the following:

a) Choose the hosts on which to install the VEM software.

Note The hosts that are displayed in the **Select VEM Host(s)** pane are all the hosts in the datacenter.

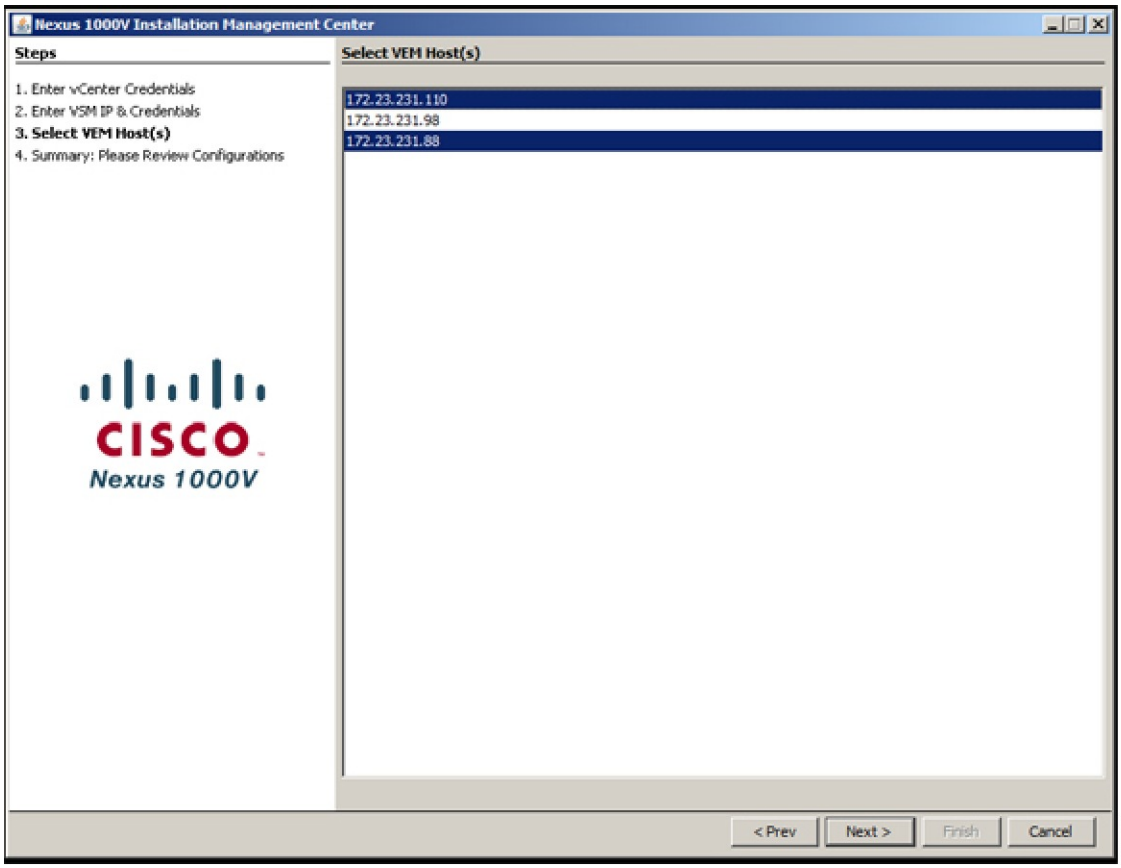
You do not need to install the VEM software on the host which contains the VSM. The VEM software was installed on the VSM host during the VSM installation process.

VIBs should be present on the selected hosts. If there are VIBs present, the application fails to install the VEM on that host.

b) Click **Next**.

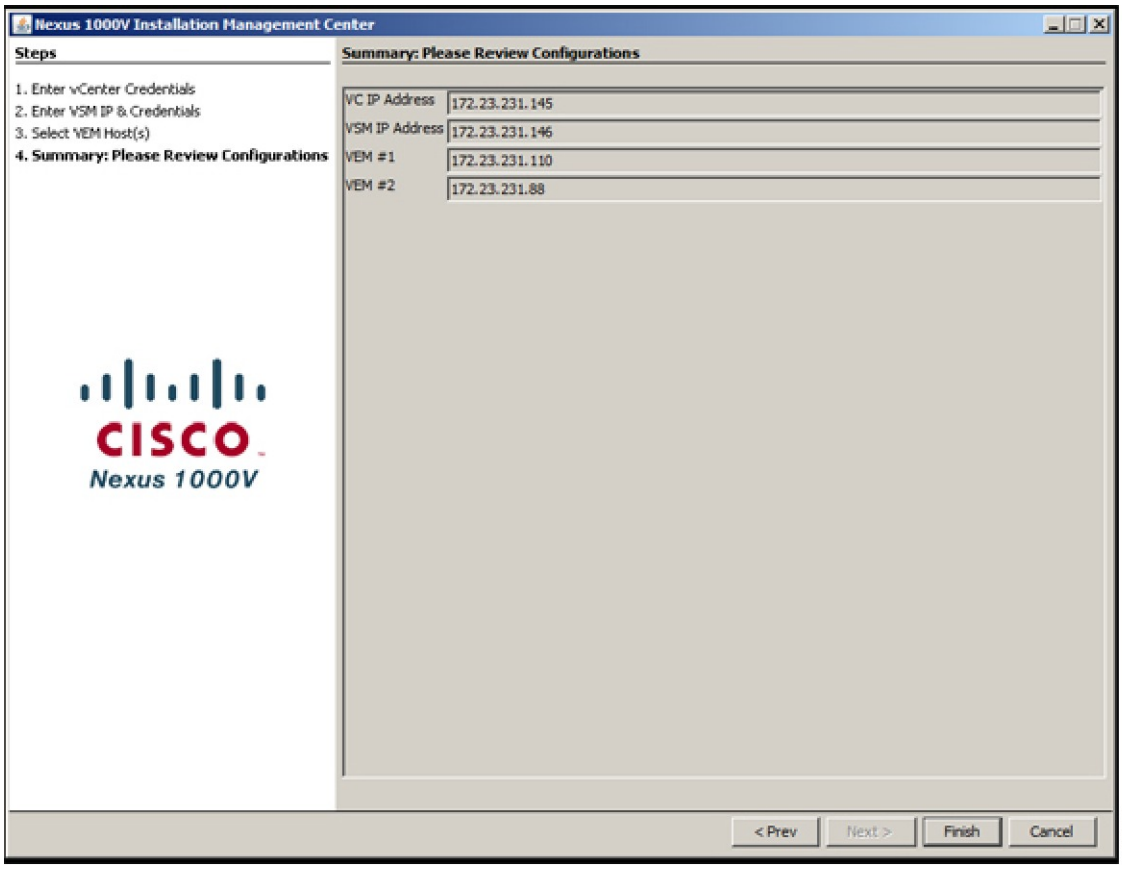
Note The VIBs should not present be present on the host. The VEM installer expects the host to be a clean host with no pre-installed Cisco VIBs.

Figure 21: Select VEM Host(s) Screen



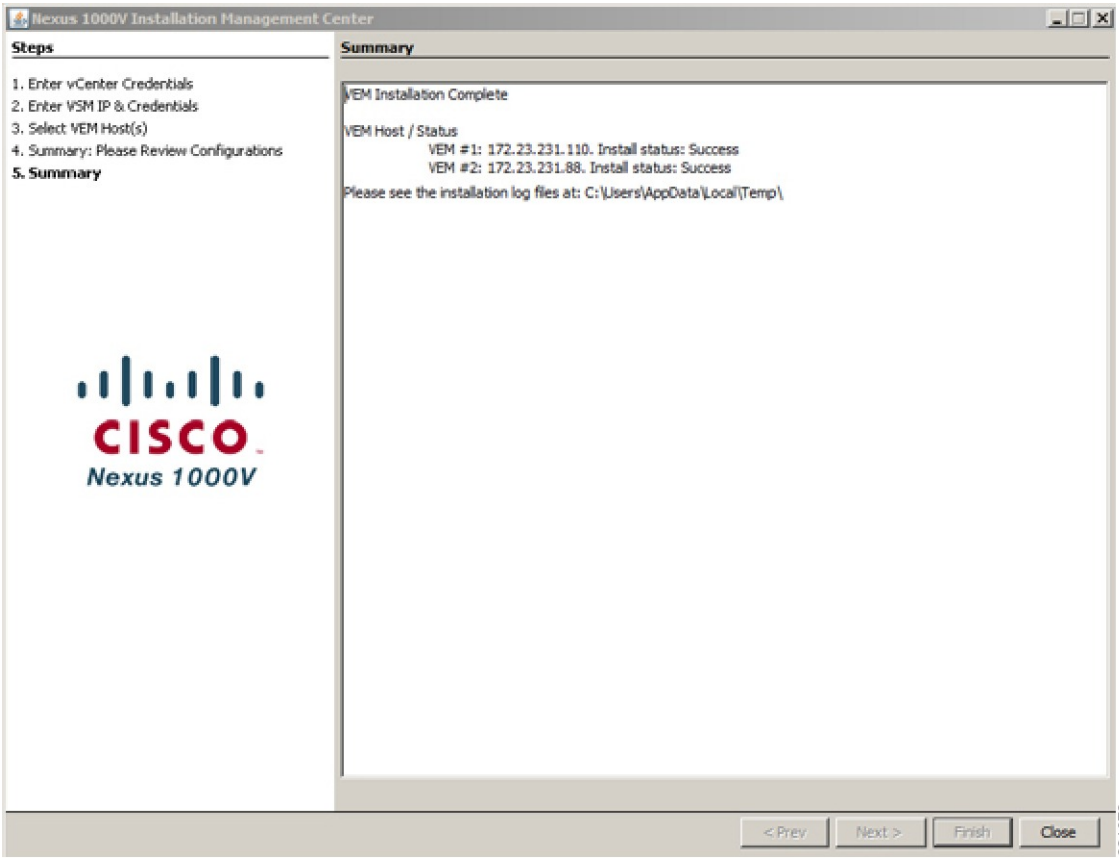
Step 6 In the **VEM Summary: Please Review Configuration** screen, validate the entries and click **Finish**.

Figure 22: VEM Summary: Please Review Configuration Screen



Step 7 In the **VEM Summary** screen, click **Close**.

Figure 23: VEM Summary Screen



Note If the VEM software fails to install on a host, the following message is displayed: Install status: Failure.

For more information about troubleshooting VSMs and VEMS, see the *Cisco Nexus 1000V Troubleshooting Guide*.

The installation of the VEM software is complete.

Adding VEM Hosts to the Distributed Virtual Switch

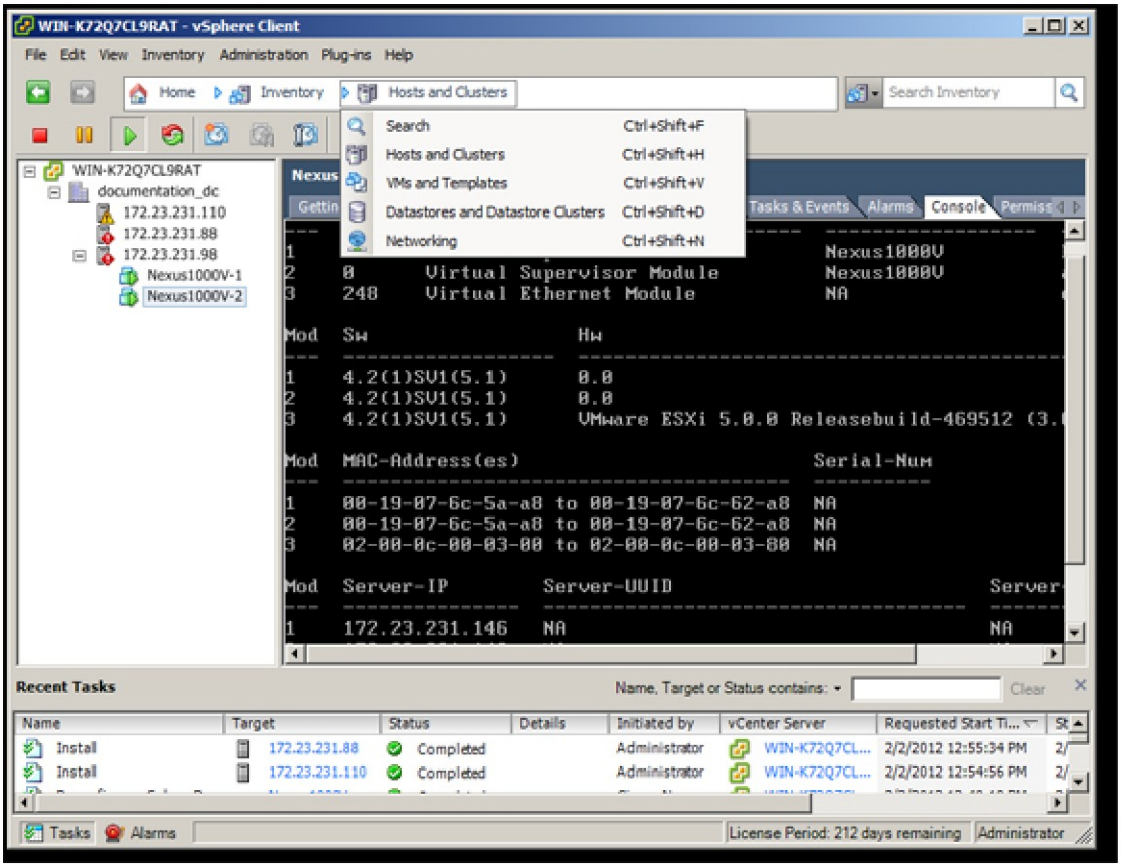
Before You Begin

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

Procedure

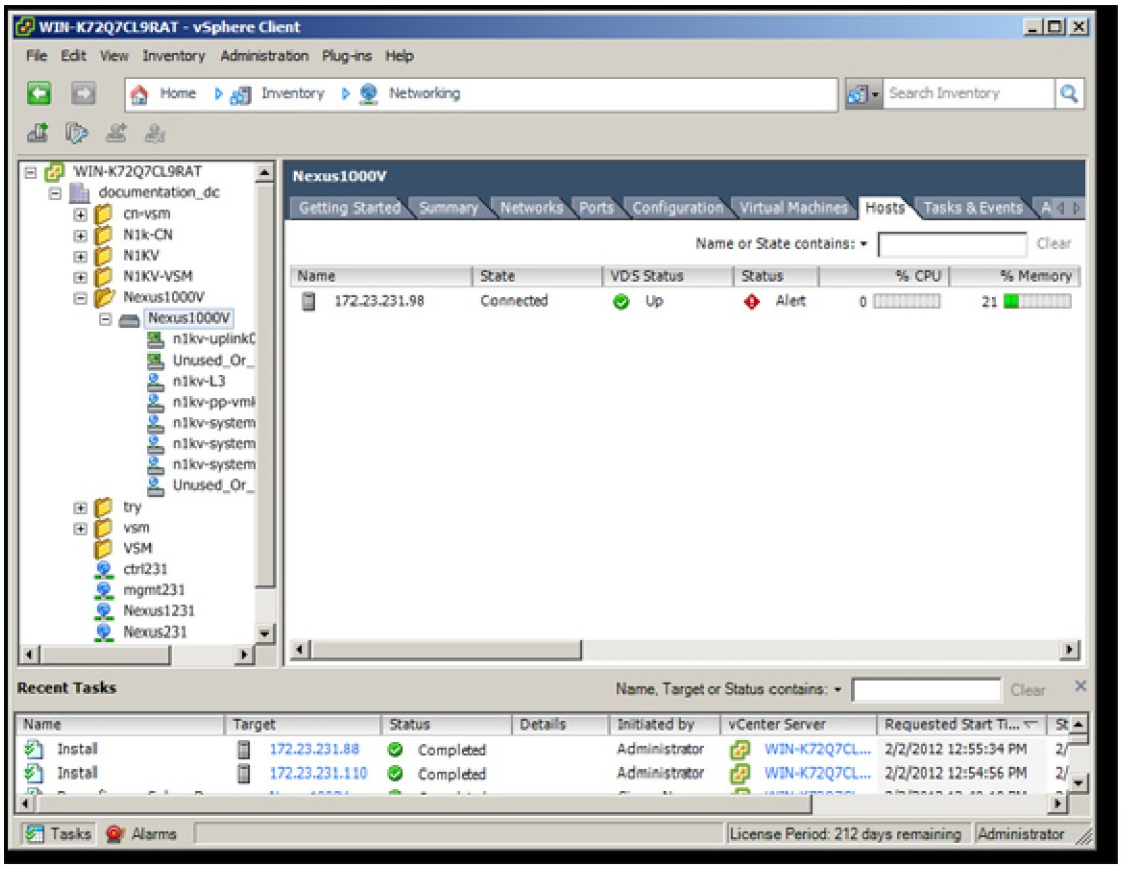
Step 1 In the **vSphere Client** window, choose **Hosts and Clusters > Networking**.

Figure 24: vSphere Client WIndow



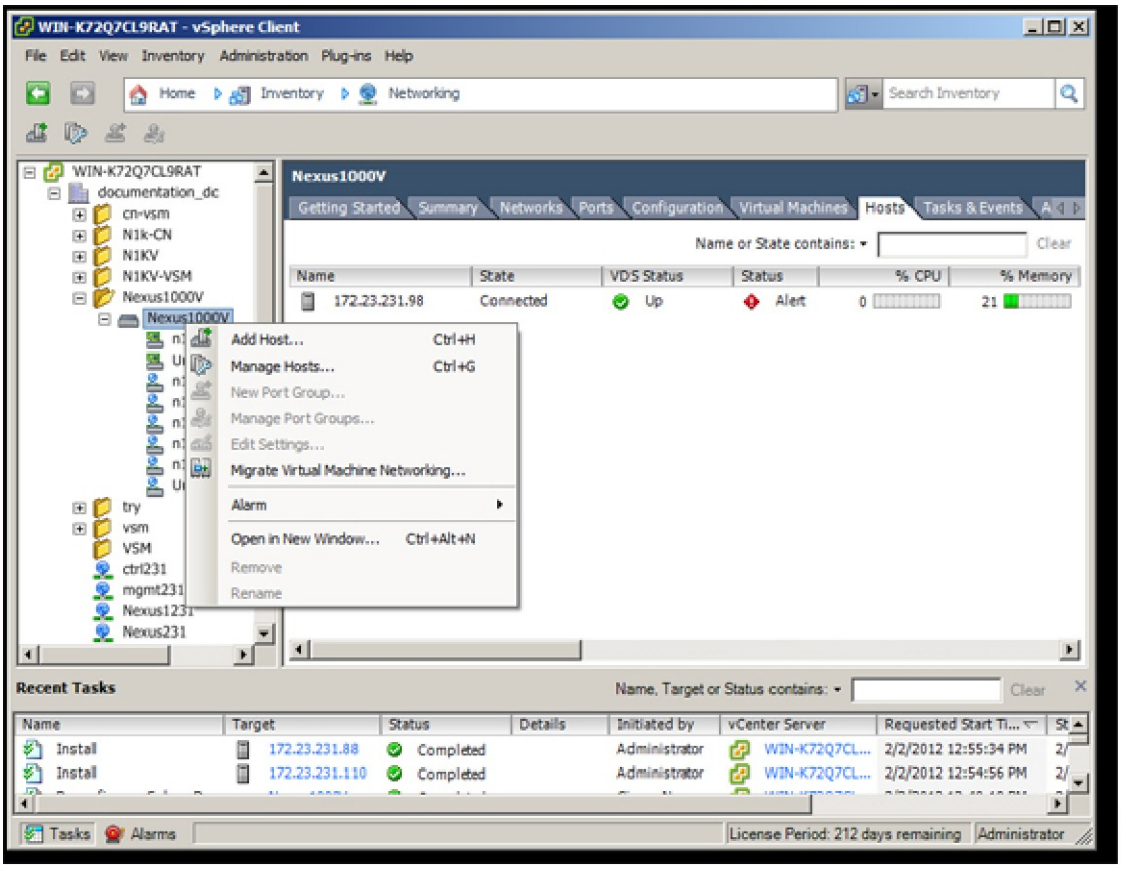
Step 2 In the **vSphere Client Hosts** window, choose the DVS and click the **Hosts** tab.

Figure 25: vSphere Client Hosts Window



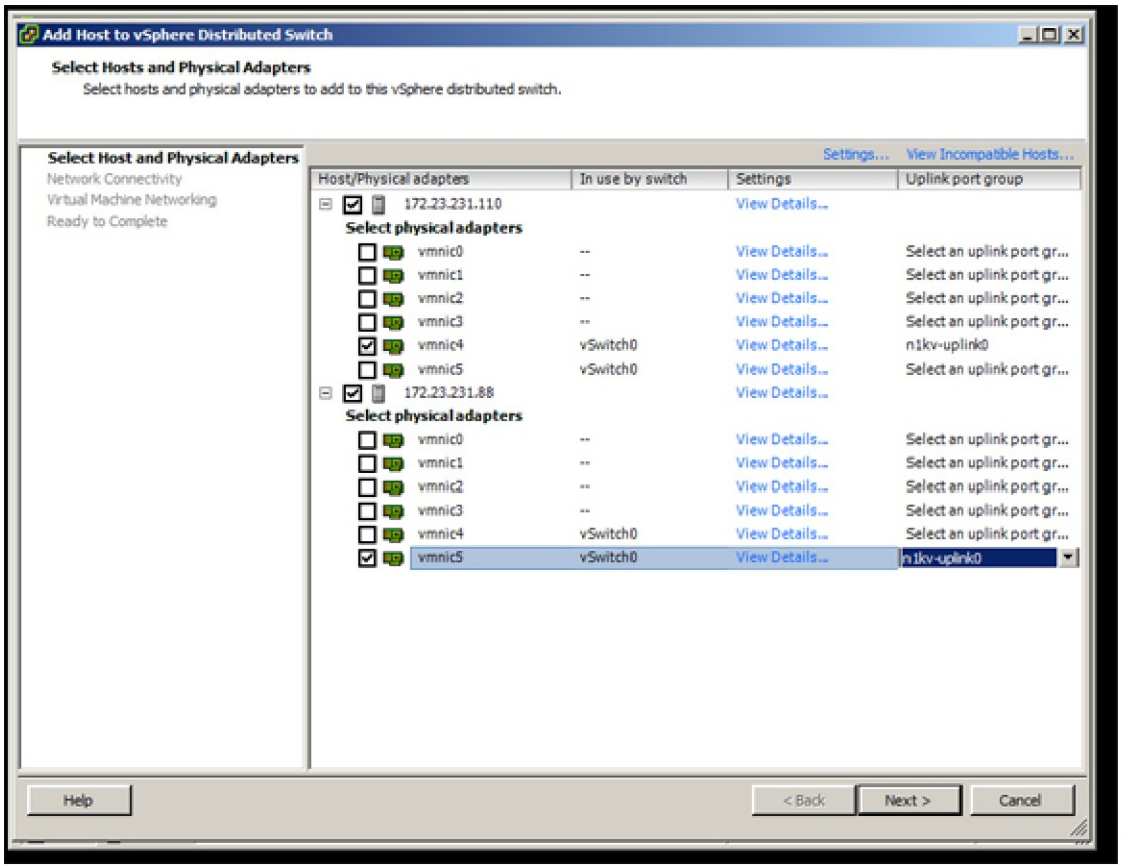
Step 3 In the **Add Hosts to DVS** window, right-click the DVS and from the drop-down list, choose **Add Host**.

Figure 26: Add Hosts to DVS



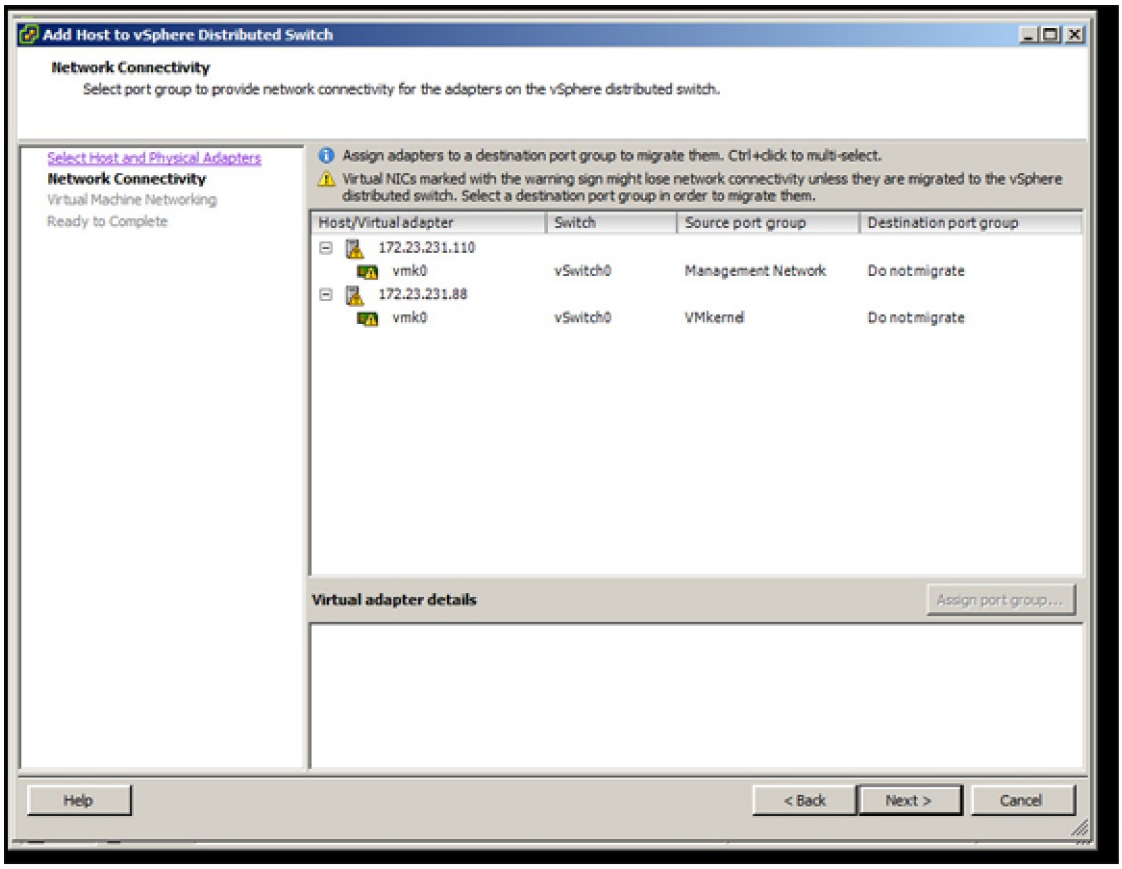
Step 4 In the **Select Hosts and Physical Adapters** screen, choose the hosts and the uplink port groups and click **Next.**

Figure 27: Select Hosts and Physical Adapters Screen



Step 5 In the **Network Connectivity** screen, click **Next**.

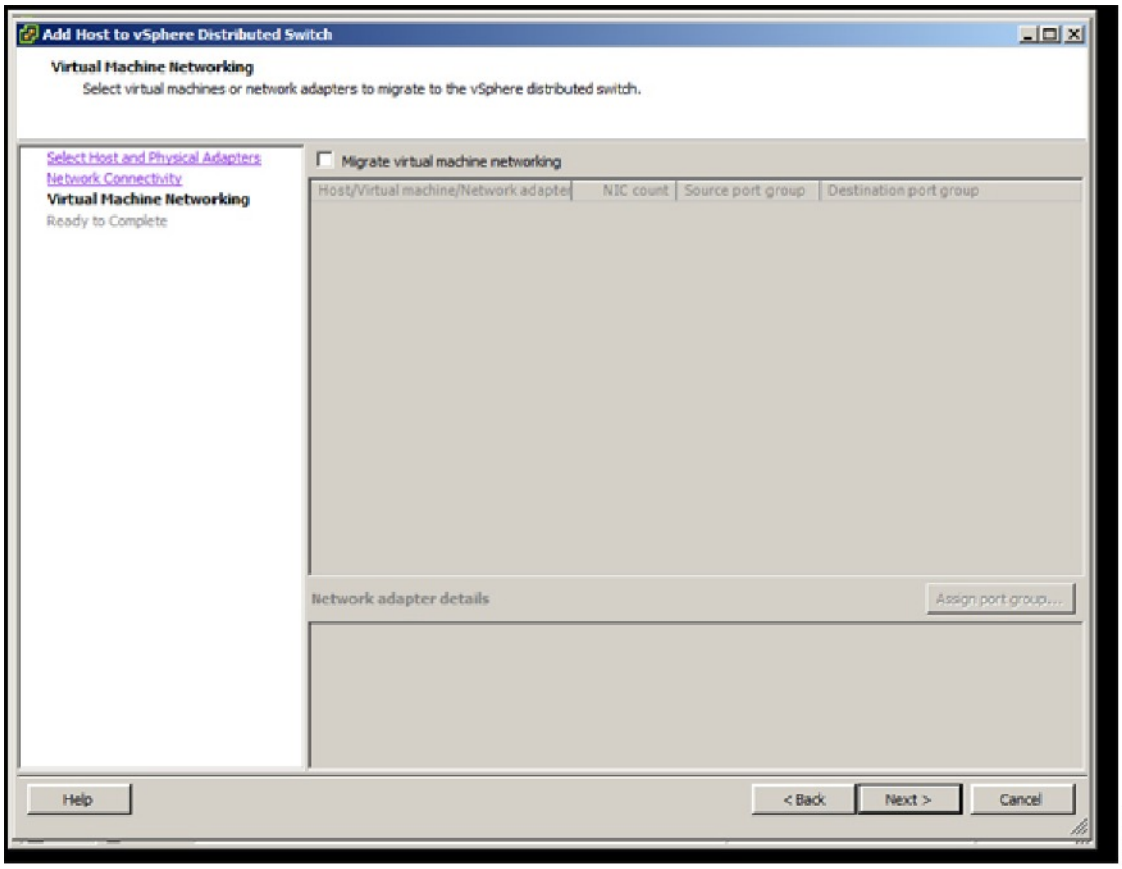
Figure 28: Network Connectivity Screen



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.

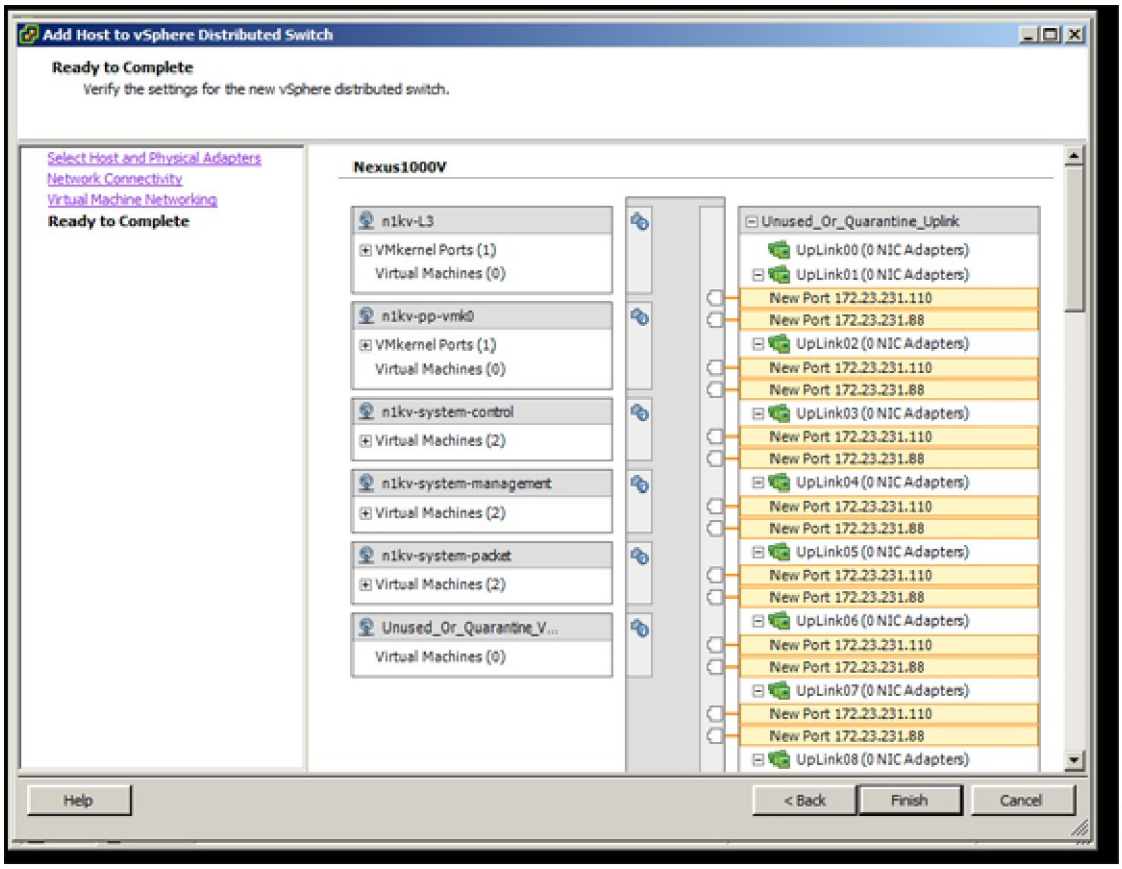
Step 6 In the **Virtual Machine Networking** screen, click **Next**.

Figure 29: Virtual Machine Networking Screen



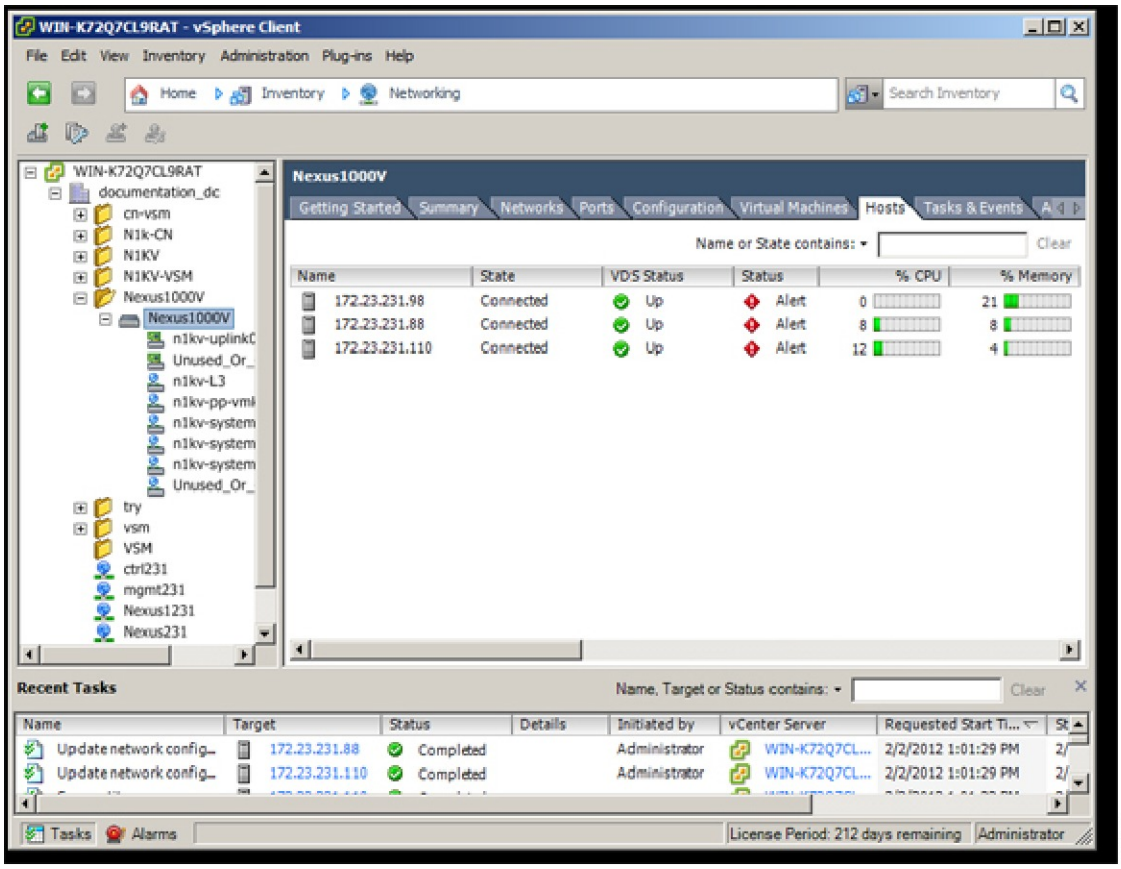
Step 7 In the **Ready to Complete** screen, click **Finish**.

Figure 30: Ready to Complete Screen



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

Figure 31: vSphere Client Hosts Window



The host connection process is complete.

Moving the Secondary VSM to a Different Host

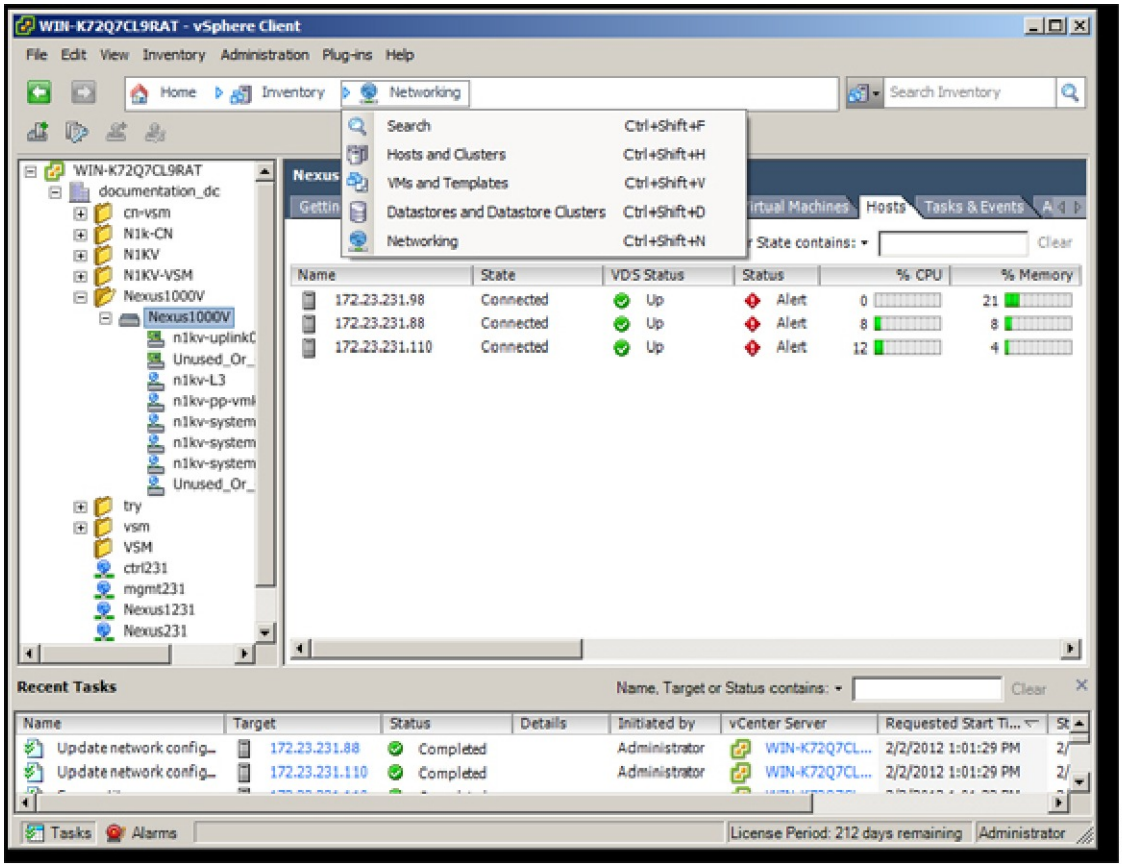
Before You Begin

- You have the following information:
  - Host to which you are moving the secondary VSM
  - The host to which you are moving the secondary VSM must be a part of the DVS

Procedure

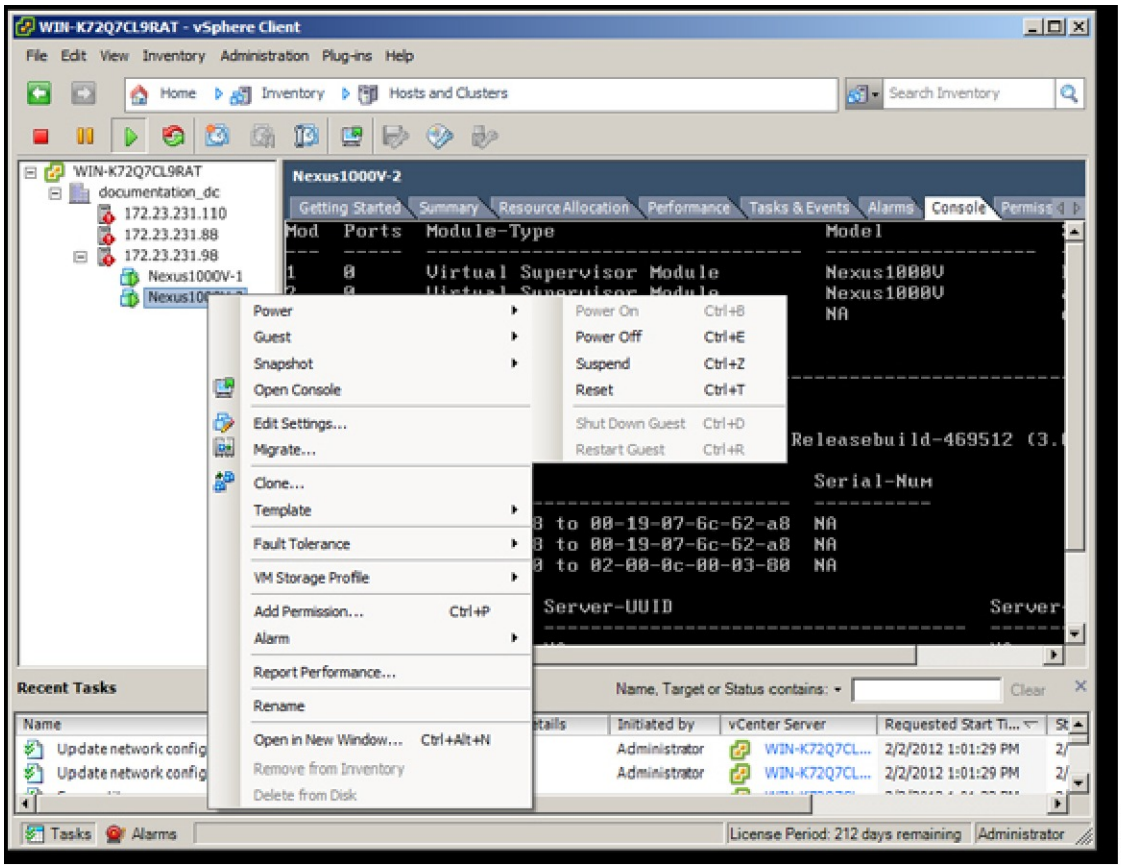
Step 1 In the **vSphere Client** window, choose **Networking > Host and Clusters**.

Figure 32: vSphere Client Window



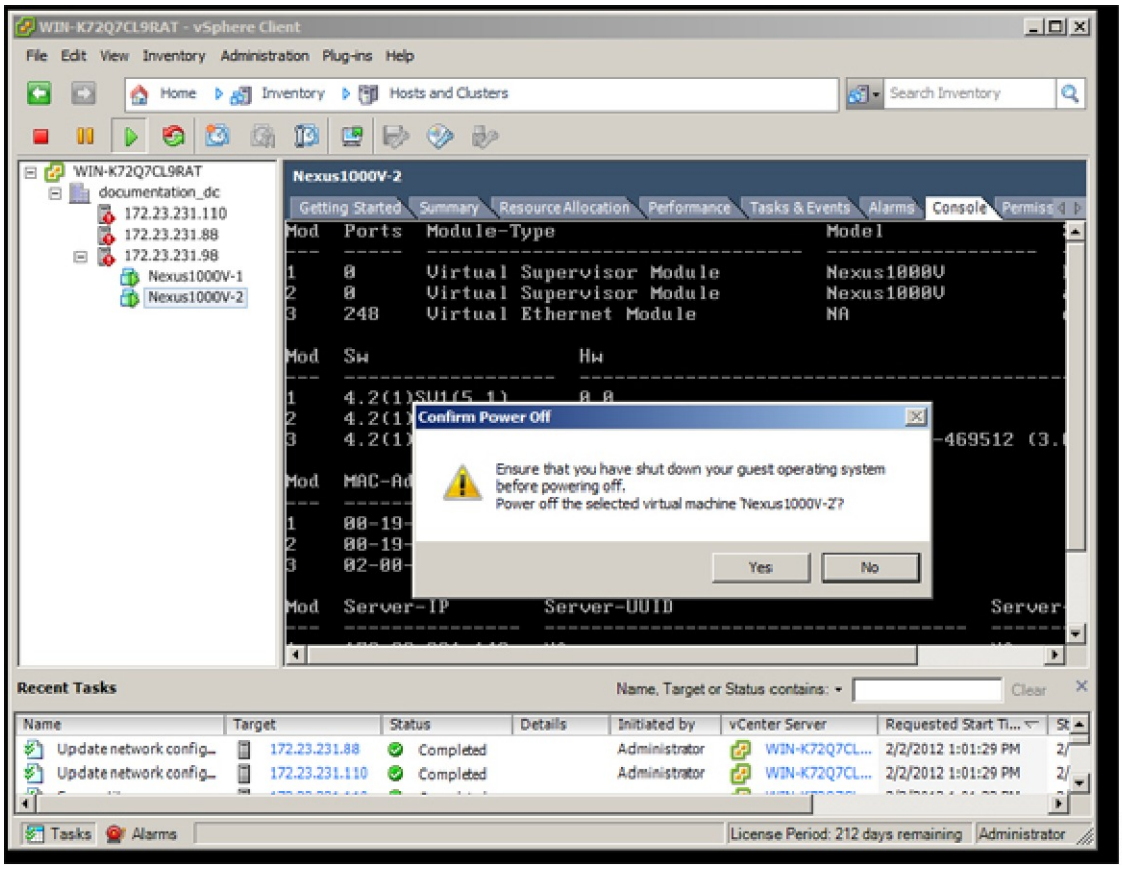
Step 2 In the **Powering Off Secondary VSM** window, right-click the secondary VSM and from the drop-down list, choose **Power > Power Off**.

Figure 33: Powering Off Secondary VSM Window



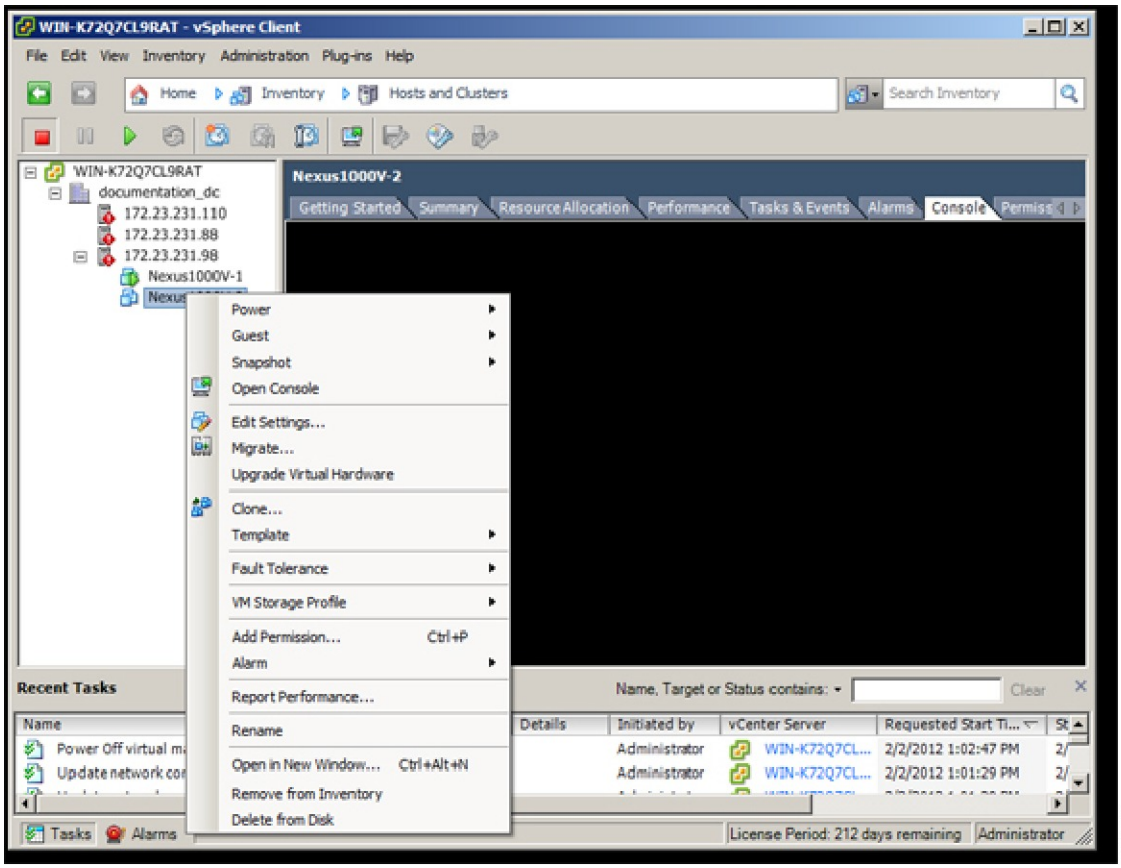
Step 3 In the **Confirm Power Off** dialog box, click **Yes**.

Figure 34: Confirm Power Off Dialog Box



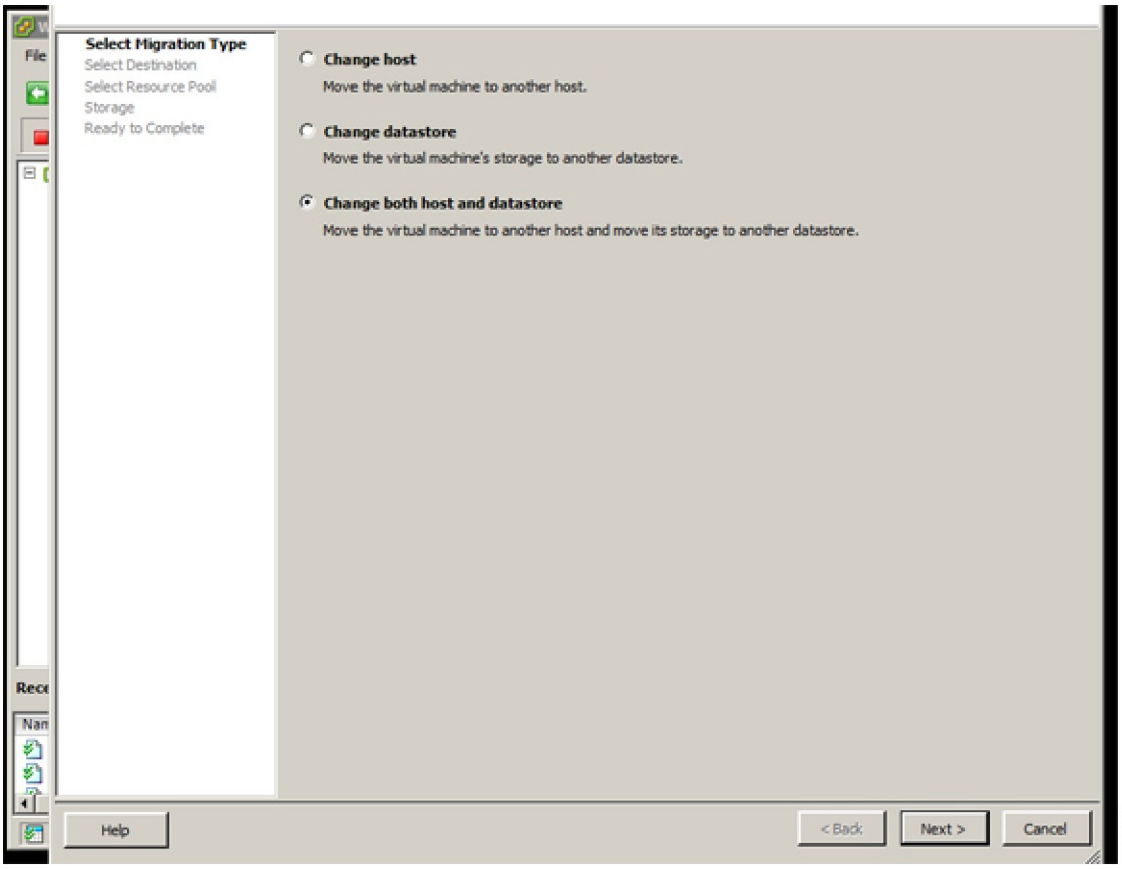
Step 4 In the **Migrate Secondary VSM** window, right-click the secondary VSM and from the drop-down list, choose **Migrate.**

Figure 35: Migrate Secondary VSM Window



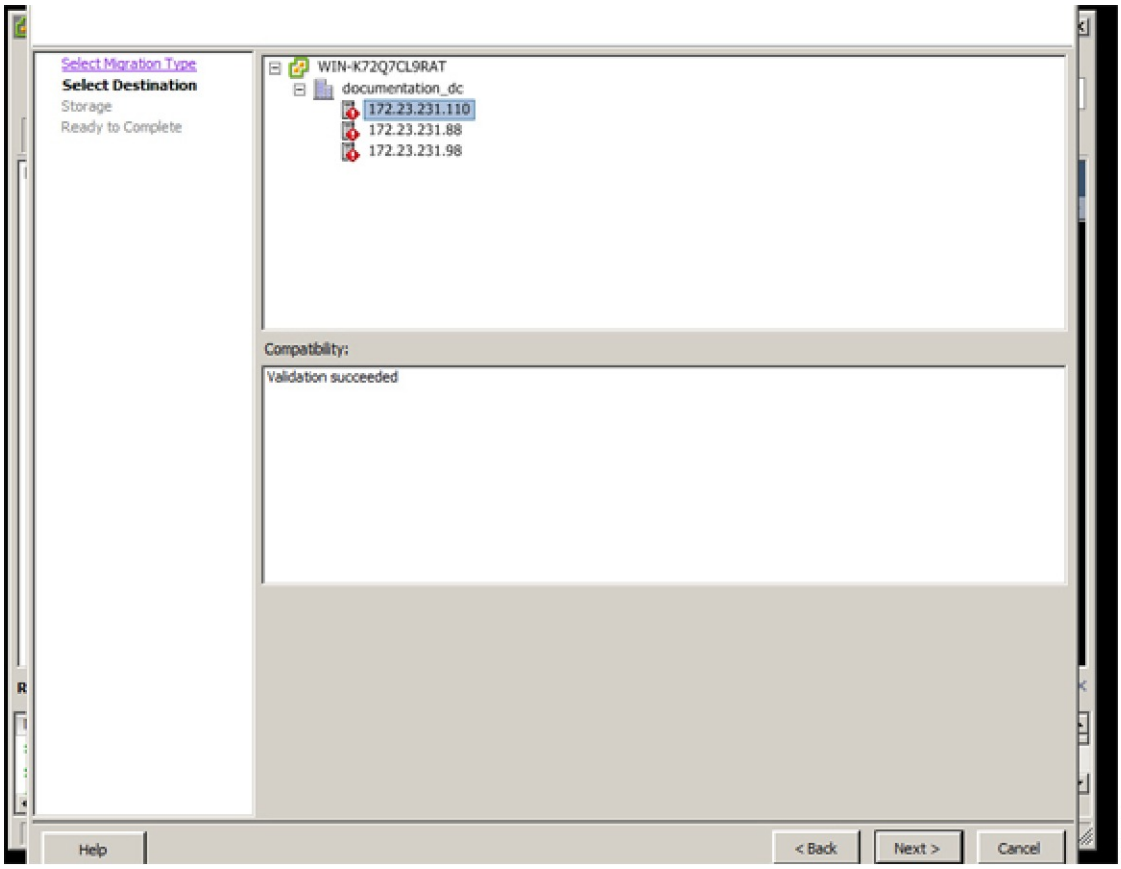
Step 5 In the **Select Migration Type** screen, click the **Change both host and datastore** radio button and click **Next.**

Figure 36: Select Migration Type Screen



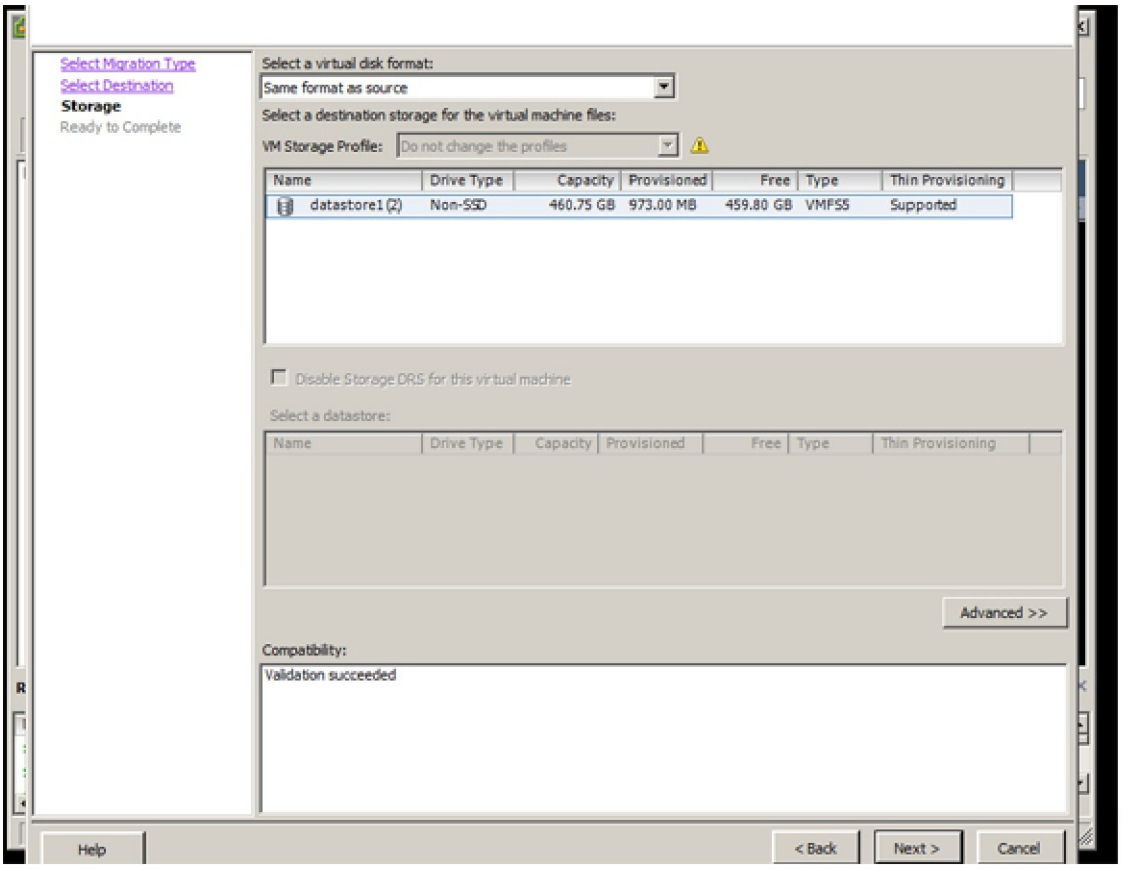
Step 6 In the **Select Destination** screen, choose the host for migration and click **Next.**

Figure 37: Select Destination Screen



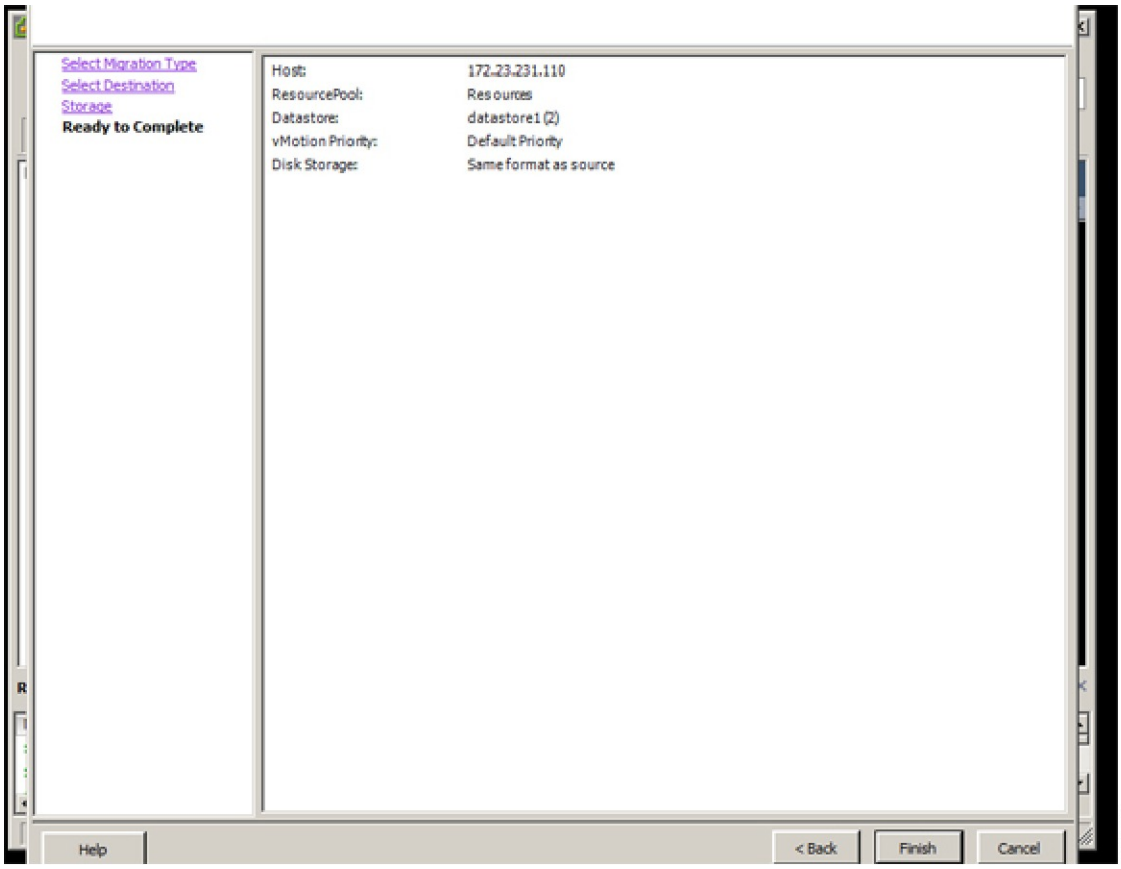
Step 7 In the **Storage** screen, click **Next**.

Figure 38: Storage Screen



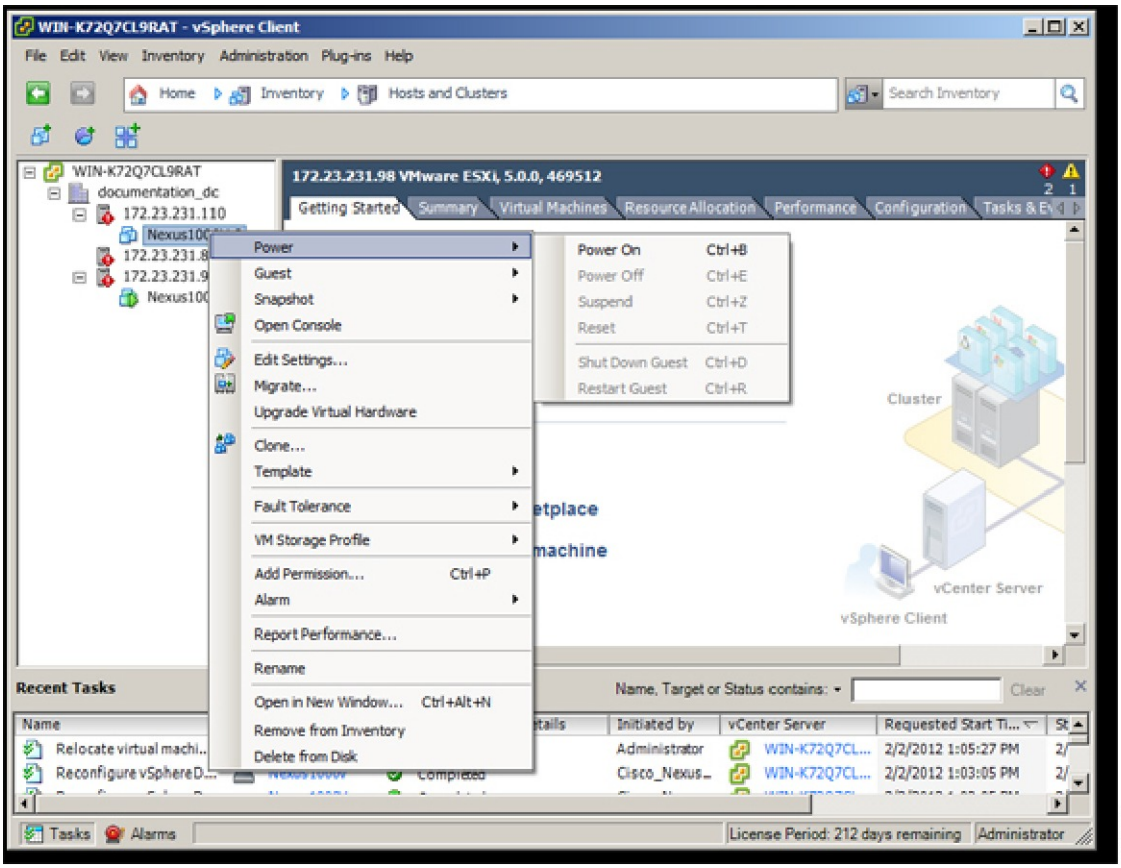
Step 8 In the **Ready to Complete** screen, click **Finish**.

Figure 39: Ready to Complete Screen



Step 9 In the **Power On** window, right-click the secondary VSM and from the drop-down list, choose **Power > Power On**.

Figure 40: Power On Window



The movement of the secondary VSM to a different host than the primary VSM is complete.

Setting Virtual Machine Startup and Shutdown Parameters

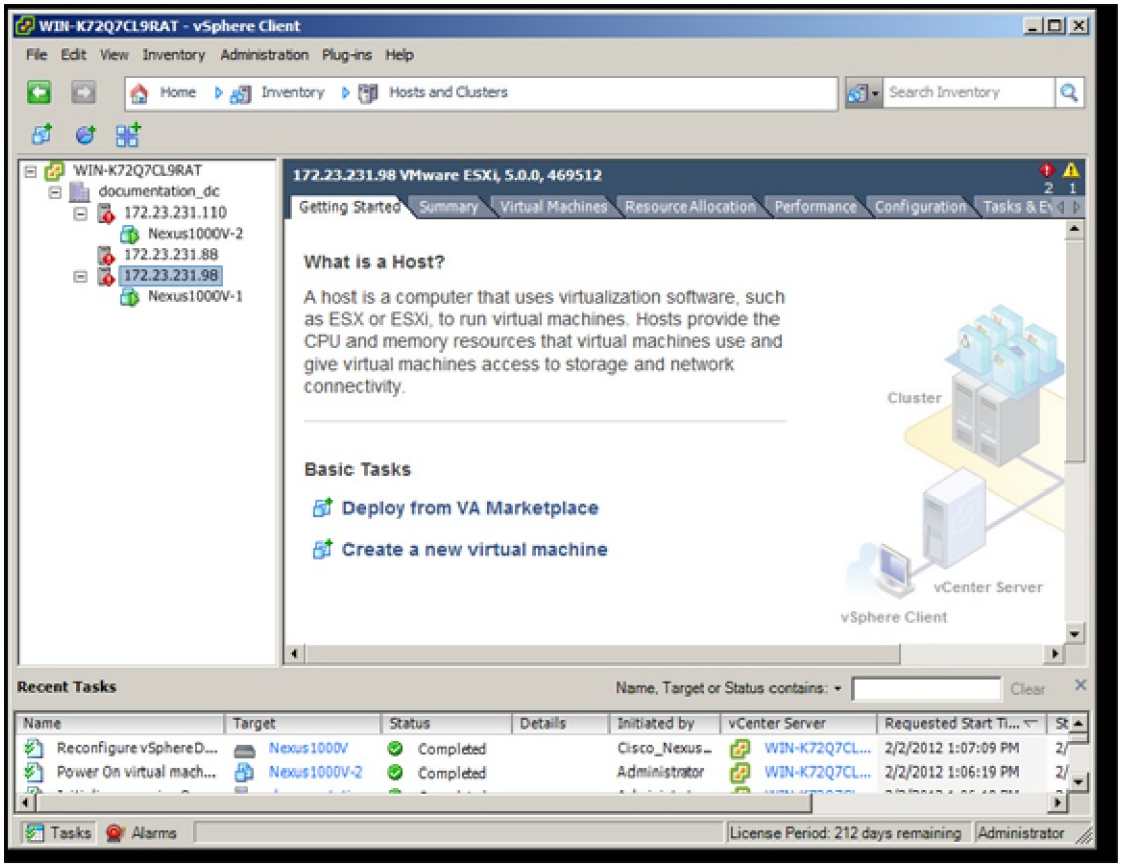
Before You Begin

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

Procedure

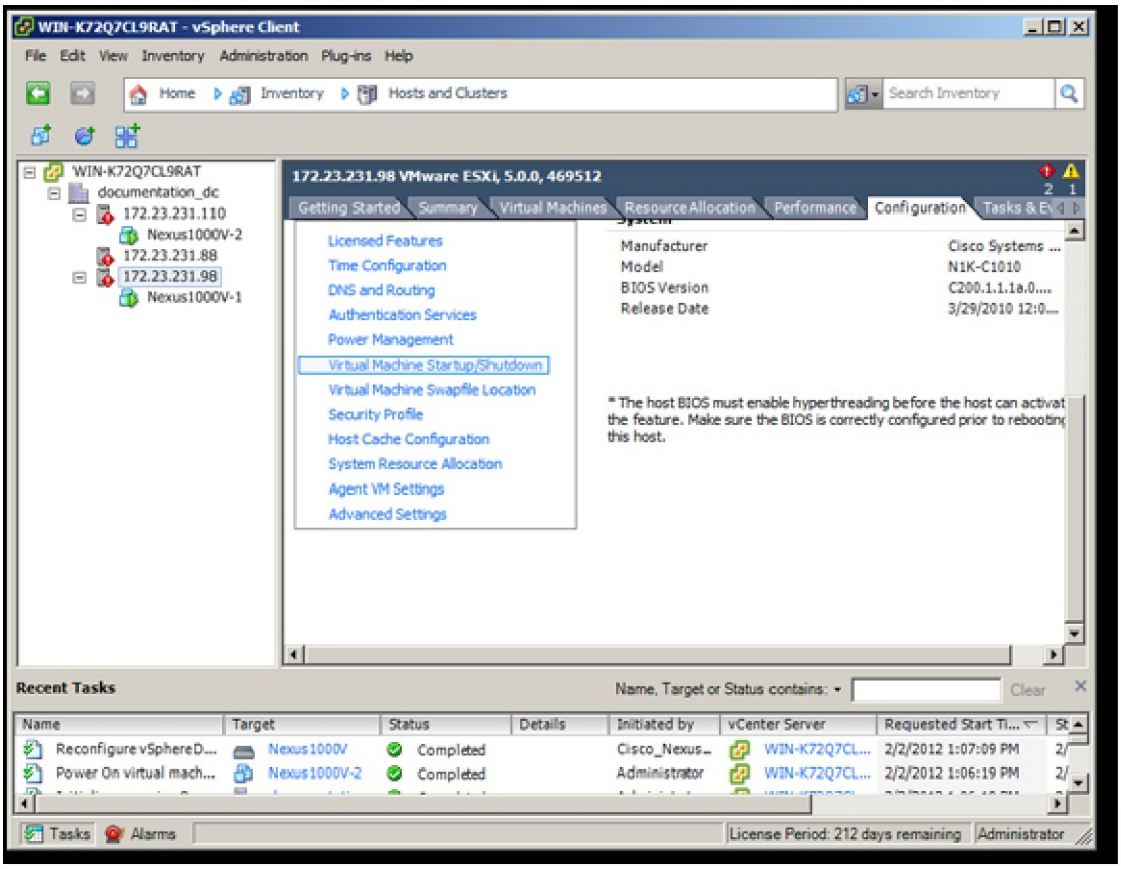
Step 1 In the **vSphere Client** window, choose a host and click the **Configuration** tab.

Figure 41: vSphere Client Window



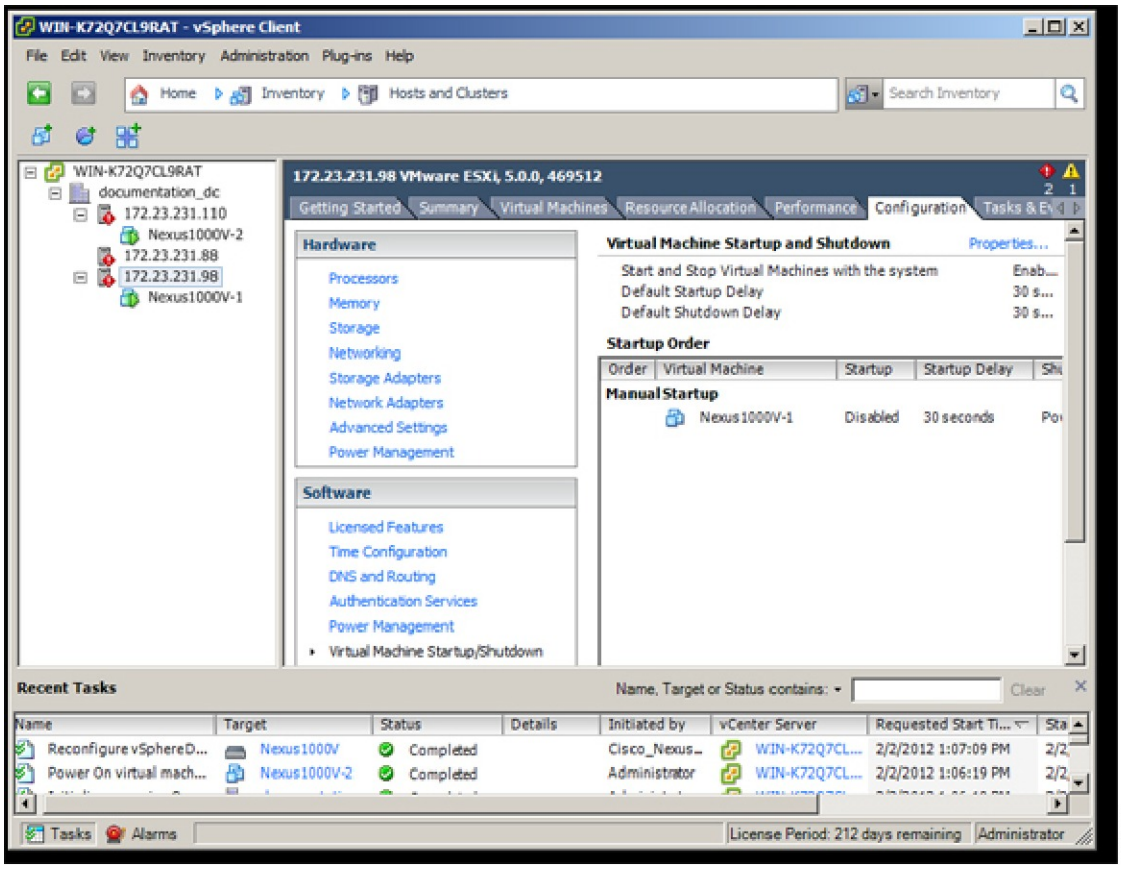
Step 2 In the **Configuration** pane, choose **Virtual Machine Startup/Shutdown**.

Figure 42: Configuration Pane



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

Figure 43: Virtual Machine Startup and Shutdown Pane



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 a number of seconds in the **Default Startup Delay seconds** field.
- Enter a number of seconds in the **Default Shutdown Delay seconds** field.

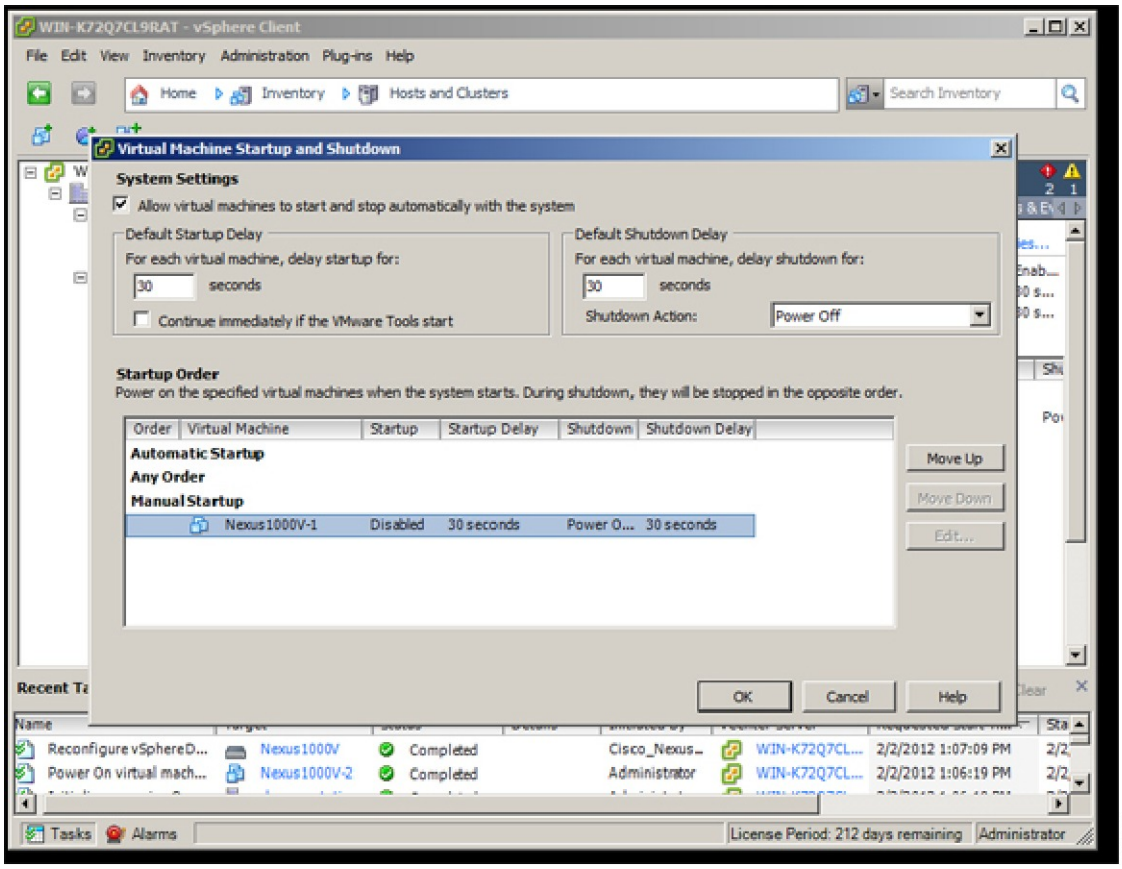
c) In the **Startup Order** pane, do the following:

- Choose the virtual machine.
- Click the **Move Up** button until the virtual machine is under Automatic Startup.

d) Click **OK**.

e) Repeat Step 2 through Step 4 for the other virtual machine.

Figure 44: System Settings Dialog Box



Startup and shutdown settings are complete.

Installing the VEM Software Using VUM

Before You Begin

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 Make sure that you read the VEM Prerequisites, on page 20 to ensure that the VUM operation proceeds without failure.

Installing the VEM Software Using the CLI

There are four different installation paths based on the version of VMware ESX/ESXi software that is running on the server:

- Installing VEM Software Locally on a VMware 4.1 Host by Using the CLI, on page 61
- Installing the VEM Software Remotely on a VMware 4.1 Host by Using the CLI, on page 62
- Installing the VEM Software Locally on a VMware 5.0 Host by Using the CLI, on page 64
- Installing VEM Software Remotely on a VMware 5.0 Host by Using the CLI, on page 65

Installing VEM Software Locally on a VMware 4.1 Host by Using the CLI

Before You Begin

- If you are using the **esxupdate** command, you are logged into the ESX host.
- Check the *Cisco Nexus 1000V and VMware Compatibility Information* for compatible versions.
- You have already copied the VEM software installation file to the `/tmp` directory.
- You know the name of the VEM software file to be installed.

Procedure

Step 1 From the ESX host `/tmp` directory, begin the VEM update procedure.

- If the offline bundle is used, enter the following command:

  esxupdate --bundle *VMware_offline_update_bundle* **update**

Example:

```
/tmp # esxupdate --bundle VEM410-201201401.zip update
Unpacking cross_cisco-vem-v14.. ######################################## [100%]

Installing packages :cross_ci.. ######################################## [100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
```

- If the VIB file is used, enter the following command:

  esxupdate -b *VIB_file* **update**

Example:

```
/tmp # esxupdate -b cross_cisco-vem-v140-4.2.1.1.5.2.0-2.0.1.vib update
```

```
Unpacking cross_cisco-vem-v140-esx.. ##################################################
[100%]

Installing packages :cross_cisco-v.. ##################################################
[100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
```

This command loads the software manually onto the host, loads the kernel modules, and starts the VEM Agent on the running system.

Step 2 Verify that the VEM software is installed on the host.

```
/tmp # esxupdate --vib-view query | grep cisco
cross_cisco-vem-v140-4.2.1.1.5.2.0-2.0.1.vib                              installed
2012-02-02T12:29:18.728890+00:00
```

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** command.

```
/tmp # vem status -v
Package vssnet-esx5.5.0-00000-release
Version 4.2.1.1.5.2.0-2.0.2
Build 2
Date Tue Jan 31 05:01:37 PST 2012

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         3           128               1500    vmnic0

Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Step 4 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*.

Installing the VEM Software Remotely on a VMware 4.1 Host by Using the CLI

Before You Begin

- If you are using the vSphere command-line interface (vCLI), do the following:
  - You have downloaded and installed the VMware vCLI. For information about installing the vCLI, see the VMware vCLI documentation.
  - You are logged in to the remote machine where the vCLI is installed.

Note The vCLI command set allows you to enter common system administration commands against ESX/ESXi systems from any machine with network access to those systems. You can also enter most CLI commands against a vCenter Server system and target any ESX/ESXi system that the vCenter Server system manages. vCLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

Procedure

Step 1 Go to the directory where the new VEM software was copied.

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
```

Step 2 Install the VEM software.

```
[root@serialport tmp]# vihostupdate -i -b ./Cisco_updated_VEM_offline_bundle --server
vsphere_host
```

Example:

```
[root@serialport tmp]# vihostupdate -i -b ./VEM410-201201401.zip --server 192.0.2.0
Enter username: root
Enter password:
Please wait patch installation is in progress ...
Host updated successfully.
```

Step 3 Verify that the VEM software is installed on the host.

vihostupdate.pl -q --server *host_ip_address*

Example:

```
[root@serialport tmp]# vihostupdate.pl -q --server 192.0.2.1
Enter username: root
Enter password:
```

Look for the following:

```
---------Bulletin ID--------- -----Installed----- ----------------Summary-------
----------
VEM410-201201401-BG           2012-02-02T00:54:14 Cisco Nexus 1000V 4.2(1)SV1(5.2)
```

Step 4 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*.

Installing the VEM Software Locally on a VMware 5.0 Host by Using the CLI

Procedure

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

Step 2 Begin the VEM installation procedure.
esxcli software vib install -v /tmp/*VIB_FILE*

Example:
```
~ # esxcli software vib install -v /tmp/cross_cisco-vem-v140-4.2.1.1.5.2.0-3.0.1.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v140-esx_4.2.1.1.5.2.0-3.0.1
   VIBs Removed:
   VIBs Skipped:
```

Step 3 Verify that the VEM software is installed on the host.
```
~ # esxcli software vib list | grep cisco
cisco-vem-v140-esx 4.2.1.1.5.2.0-3.0.1 Cisco PartnerSupported
2012-02-02
```

Step 4 Verify that the installation was successful by checking for the “VEM Agent (vemdpa) is running” statement in the output of the **vem status** command.

Example:
```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.5.2.0-3.0.1
Build 1
Date Mon Jan 30 18:38:49 PST 2012

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name    Num Ports   Used Ports  Configured Ports MTU   Uplinks
vSwitch0       128         3           128              1500  vmnic0
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Step 5 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*.

Installing VEM Software Remotely on a VMware 5.0 Host by Using the CLI

Procedure

Step 1 Copy the VEM software to the NFS storage which is mounted on the ESXi 5.0 host.

Step 2 Enter the following command from the remote machine where the vCLI is installed.
esxcli --server=[server ip] software vib install --depot=*Path_to_the_NFS_storage_mounted_ _on_ESXi_5.0 host*

Example:
```
vi-admin@localhost:~> esxcli --server=192.0.2.2 software vib install
--depot=/vmfs/volumes/newnfs/MN-patch01/CN-FCS/VEM500-201201140102-BG-release.zip
Enter username: root
Enter password:
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v140-esx_4.2.1.1.5.2.0-3.0.1
   VIBs Removed:
   VIBs Skipped:
```
where 192.0.2.2 is the target ESXi 5.0 host IP address and newnfs is the NFS storage mounted on the ESXi 5.0 host.

Note You should refer to the official VMware documentation for further information on the **esxcli** command.

Step 3 Verify that the VEM software is installed on the host.
esxcli --server=*host_ip_address* **software vib list**

Example:
```
vi-admin@localhost:~> esxcli --server=192.0.2.1 software vib list
Enter username: root
Enter password:
```

Look for the following:

```
Name                 Version                             Vendor  Acceptance Lev
el  Install Date
-------------------  ----------------------------------  ------  --------------
--  ------------
cisco-vem-v140-esx    4.2.1.1.5.2.0-3.0.1                Cisco   PartnerSupport
ed  2012-04-06
```

Step 4 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*.

Installing the VEM Software on a Stateless ESXi Host

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

Procedure

Step 1 See the procedure for Adding the Cisco Nexus 1000V to an ESXi Image Profile, on page 66.

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 69
- Installing the VEM Software on a Stateless ESXi Host Using VUM, on page 71

Step 3 See the procedure for Configuring Layer 2 Connectivity, on page 74.

Stateless ESXi Host

Note For Stateless ESXi, the VLAN used for 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 5.0.0 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 and the image profile includes base VIBs from VMware and additional VIBs from partners.

On a stateless host, VEM software can be installed or upgraded using either the VUM or CLI.

In addition, you should bundle the new or modified VEM module in the image profile from which the stateless host boots. If it is not bundled in the image profile, the VEM module 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 5.0.0* 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 module 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.

Note In the following procedure, the image profile bundle is available as `C:\ESXi-5.0.0-depot.zip` and the VEM bundle is available as `C:\VEM500-20110822140-BG.zip`.

Procedure

Step 1 Start the vSphere PowerCLI application.

Step 2 Connect to the vCenter Server.

```
[vSphere PowerCLI] > Connect-VIServer 192.0.2.1 –User Administrator –Password XXXXX
```

Step 3 Load the image profile offline bundle.

Note Each image profile bundle can include multiple image profiles.

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot c:\vmware-ESXi-5.0.0-depot.zip
```

Step 4 List the image profiles.

```
[vSphere PowerCLI] > Get-EsxImageProfile

Name                           Vendor          Last Modified
----                           ------          -------------
ESXi-5.0.0-standard            VMware, Inc.    2/25/2011 9:42:21 PM
ESXi-5.0.0-no-tools            VMware, Inc.    2/25/2011 9:42:21 PM
```

Step 5 Choose the image profile into which the VEM is to be bundled from the output of the **Get-EsxImageProfile** command.

Note The image profiles will be in read-only format. You need to clone the image profile before adding the VEM into it.

```
[vSphere PowerCLI] > New-EsxImageProfile -CloneProfile ESXi-5.0.0-standard -Name n1kv-Image
```

Note The n1kv-Image is the cloned image profile of the ESXi-5.0.0-standard.

Step 6 Load the Cisco Nexus 1000V VEM offline bundle.

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

```
[vSphere PowerCLI] > Add-EsxSoftwareDepot C:\VEM500-20110822140-BG.zip
```

Step 7 Confirm that the n1kv-vib package is loaded.

```
[vSphere PowerCLI] > Get-EsxSoftwarePackage -Name cisco*

Name                      Version              Vendor          Release
----                      -------              ------          -----------
cisco-vem-v131-esx        4.2.1.1.3.24.0-3.0.8 Cisco           8/22/2011.
```

Step 8 Bundle the n1kv-package into the cloned image profile.

```
[vSphere PowerCLI] > Add-EsxSoftwarePackage -ImageProfile n1kv-Image -SoftwarePackage
cisco-vem-v131-esx
```

Step 9 List all the VIBs in the cloned image profile.

```
[vSphere PowerCLI]> $img = Get-EsxImageProfile n1kv-Image
[vSphere PowerCLI]> $img.vibList
```

```
Name                      Version                        Vendor     Release Date
----                      -------                        ------     ------------
scsi-bnx2i                1.9.1d.v50.1-3vmw.500.0.0.4... VMware     6/22/2011...
net-s2io                  2.1.4.13427-3vmw.500.0.0.43... VMware     6/22/2011...
net-nx-nic                4.0.557-3vmw.500.0.0.434219    VMware     6/22/2011...
scsi-aic79xx              3.1-5vmw.500.0.0.434219        VMware     6/22/2011...
sata-ata-piix             2.12-4vmw.500.0.0.434219       VMware     6/22/2011...
net-e1000e                1.1.2-3vmw.500.0.0.434219      VMware     6/22/2011...
net-forcedeth             0.61-2vmw.500.0.0.434219       VMware     6/22/2011...
tools-light               5.0.0-0.0.434219               VMware     6/22/2011...
ipmi-ipmi-msghandler      39.1-4vmw.500.0.0.434219       VMware     6/22/2011...
scsi-aacraid              1.1.5.1-9vmw.500.0.0.434219    VMware     6/22/2011...
net-be2net                4.0.88.0-1vmw.500.0.0.434219   VMware     6/22/2011...
sata-ahci                 3.0-6vmw.500.0.0.434219        VMware     6/22/2011...
ima-qla4xxx               2.01.07-1vmw.500.0.0.434219    VMware     6/22/2011...
ata-pata-sil680           0.4.8-3vmw.500.0.0.434219      VMware     6/22/2011...
scsi-ips                  7.12.05-4vmw.500.0.0.434219    VMware     6/22/2011...
scsi-megaraid-sas         4.32-1vmw.500.0.0.434219       VMware     6/22/2011...
scsi-mpt2sas              06.00.00.00-5vmw.500.0.0.43... VMware     6/22/2011...
net-cnic                  1.10.2j.v50.7-2vmw.500.0.0.... VMware     6/22/2011...
ipmi-ipmi-si-drv          39.1-4vmw.500.0.0.434219       VMware     6/22/2011...
esx-base                  5.0.0-0.0.434219               VMware     6/22/2011...
ata-pata-serverworks      0.4.3-3vmw.500.0.0.434219      VMware     6/22/2011...
scsi-mptspi               4.23.01.00-5vmw.500.0.0.434219 VMware     6/22/2011...
net-bnx2x                 1.61.15.v50.1-1vmw.500.0.0.... VMware     6/22/2011...
ata-pata-hpt3x2n          0.3.4-3vmw.500.0.0.434219      VMware     6/22/2011...
sata-sata-sil             2.3-3vmw.500.0.0.434219        VMware     6/22/2011...
scsi-hpsa                 5.0.0-17vmw.500.0.0.434219     VMware     6/22/2011...
block-cciss               3.6.14-10vmw.500.0.0.434219    VMware     6/22/2011...
net-tg3                   3.110h.v50.4-4vmw.500.0.0.4... VMware     6/22/2011...
net-igb                   2.1.11.1-3vmw.500.0.0.434219   VMware     6/22/2011...
ata-pata-amd              0.3.10-3vmw.500.0.0.434219     VMware     6/22/2011...
ata-pata-via              0.3.3-2vmw.500.0.0.434219      VMware     6/22/2011...
net-e1000                 8.0.3.1-2vmw.500.0.0.434219    VMware     6/22/2011...
scsi-adp94xx              1.0.8.12-6vmw.500.0.0.434219   VMware     6/22/2011...
scsi-lpfc820              8.2.2.1-18vmw.500.0.0.434219   VMware     6/22/2011...
scsi-mptsas               4.23.01.00-5vmw.500.0.0.434219 VMware     6/22/2011...
ata-pata-cmd64x           0.2.5-3vmw.500.0.0.434219      VMware     6/22/2011...
sata-sata-svw             2.3-3vmw.500.0.0.434219        VMware     6/22/2011...
misc-cnic-register        1.1-1vmw.500.0.0.434219        VMware     6/22/2011...
ipmi-ipmi-devintf         39.1-4vmw.500.0.0.434219       VMware     6/22/2011...
sata-sata-promise         2.12-3vmw.500.0.0.434219       VMware     6/22/2011...
sata-sata-nv              3.5-3vmw.500.0.0.434219        VMware     6/22/2011...
cisco-vem-v131-esx        4.2.1.1.3.24.0-3.0.8           Cisco      6/30/2011...
```

Step 10 Export the image profile to a depot file for future use.

```
[vSphere PowerCLI] > Export-EsxImageProfile –ImageProfile n1kv-Image –FilePath
C:\n1kv-Image.zip –ExportToBundle.
```

Step 11 Set up the rule for the host to boot with this image profile.

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.

```
[vSphere PowerCLI] > New-deployrule -item $img -name rule-test –Pattern "mac=00:50:56:b6:03:c1"

[vSphere PowerCLI] > Add-DeployRule -DeployRule rule-test
```

Step 12 Display the configured rule to make sure that the correct image profile is associated with the host.

```
[vSphere PowerCLI] > Get-DeployRuleSet

Name        : rule-test
PatternList : {mac=00:50:56:b6:03:c1}
ItemList    : {n1kv-Image}
```

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.

Installing the VEM Software on a Stateless ESXi Host Using esxcli

Before You Begin

- When entering 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.

```
~ # vmware -v
VMware ESXi 5.0.0 build-441354
~ #
~ # vmware -l
VMware ESXi 5.0.0 GA
```

Step 2 Log in to the ESXi stateless host.

Step 3 Copy the offline bundle to the host.

```
~ # esxcli software vib install -d /vmfs/volumes/newnfs/MN-VEM/VEM500-20110728153-BG-release.zip

Installation Result
   Message: WARNING: Only live system was updated, the change is not persistent.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v131-esx_4.2.1.1.4.1.0-3.0.5
   VIBs Removed:
   VIBs Skipped:
```

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.

```
~ # esxcli software vib list | grep cisco
cisco-vem-v131-esx    4.2.1.1.4.1.0-3.0.5              Cisco   PartnerSupported  2011-08-18
```

Step 5 Check that the VEM agent is running.

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.4.1.0-3.0.5
Build 5
Date Thu Jul 28 01:37:10 PDT 2011
Number of PassThru NICs are 0
VEM modules are loaded
Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         4           128               1500    vmnic4
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Step 6 Display the VEM version, VSM version, and ESXi version.

```
~ # vemcmd show version
VEM Version: 4.2.1.1.4.1.0-3.0.5
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

Step 7 Display the ESXi version and details about pass-through NICs.

```
~ # vem version -v
Number of PassThru NICs are 0
Running esx version -441354 x86_64
VEM Version: 4.2.1.1.4.1.0-3.0.5
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

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.

```
switch# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
2    0      Virtual Supervisor Module         Nexus1000V          ha-standby
3    248    Virtual Ethernet Module          NA                            ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    4.2(1)SV1(4a)     0.0
2    4.2(1)SV1(4a)     0.0
3    4.2(1)SV1(4a)     VMware ESXi 5.0.0 Releasebuild-441354 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.62.227    NA                                    NA
2    10.104.62.227    NA                                    NA
3    10.104.62.216    3fa746d4-de2f-11de-bd5d-c47d4f7ca460  sans2-216.cisco.com
```

Installing the VEM Software on a Stateless ESXi Host Using VUM

Before You Begin

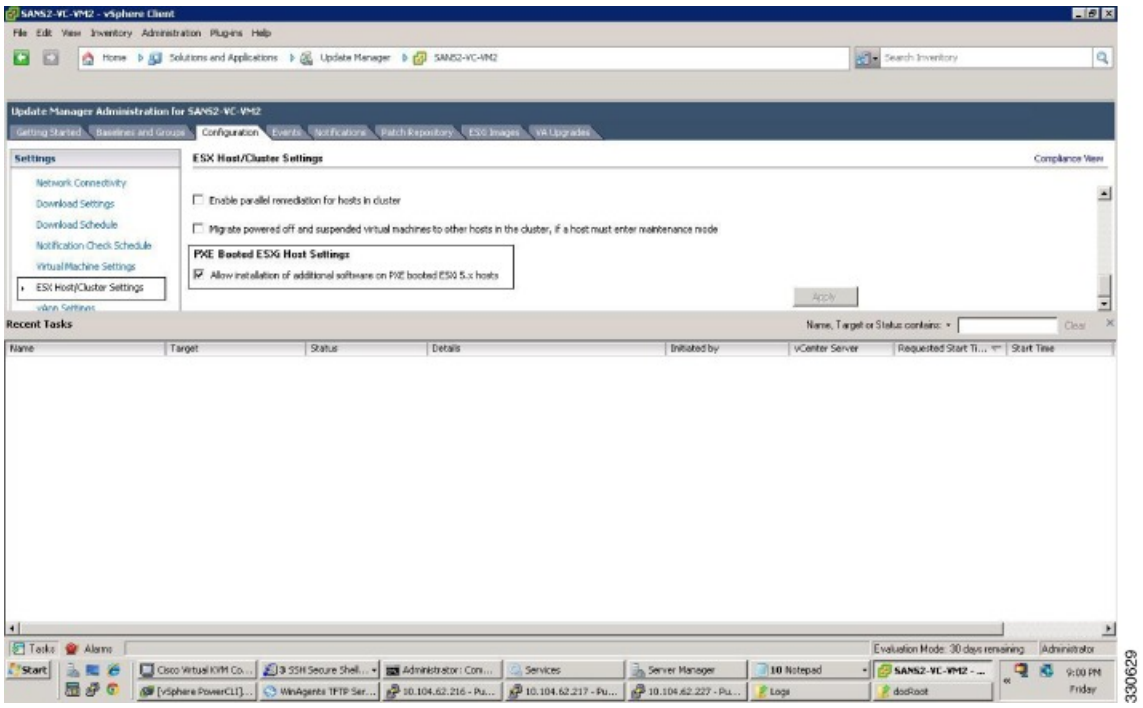
- Make sure that the VUM patch repository has the VEM software downloaded.

Procedure

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

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

Figure 45: ESX Host/Cluster Settings Window



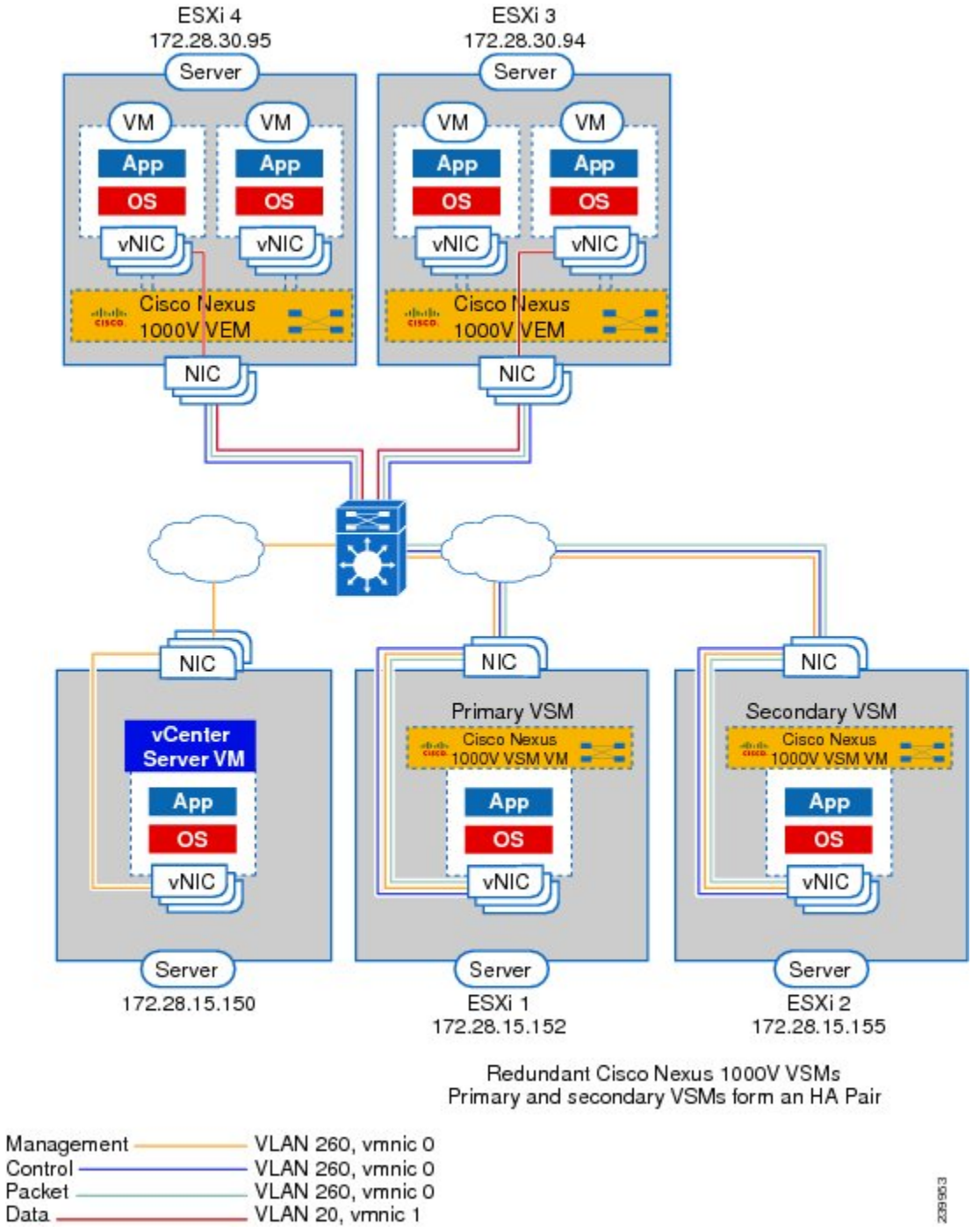
Step 3 Add the host to the DVS by using the vCenter Server.

Information About Layer 2 Connectivity

Note Layer 3 connectivity is the preferred method.

The following figure shows an example of redundant VSM VMs, where the software for the primary VSM is installed on ESXi 1, and the software for the secondary VSM is installed on ESXi 2 for Layer 2 connectivity.

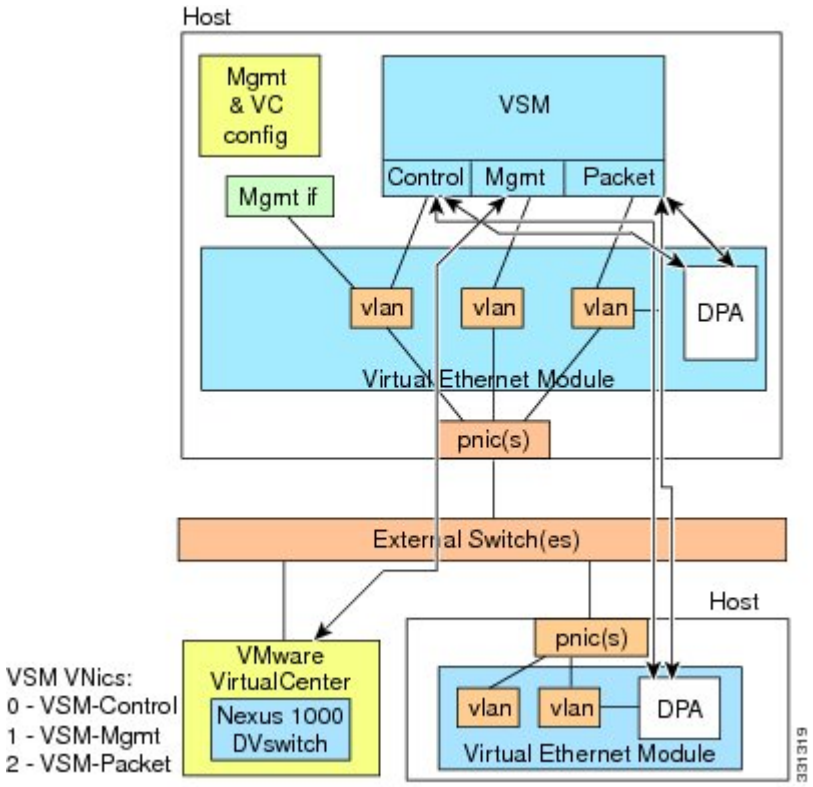
Figure 46: Cisco Nexus 1000V Installation Diagram for Layer 2



Layer 2 on the Same Host

The following figure shows a VSM and VEM running on the same host in Layer 2 mode.

Figure 47: VSM and VEM on the Same Host in Layer 2 Mode



Configuring Layer 2 Connectivity

Note Layer 3 connectivity is the preferred method.

Procedure

Step 1 To configure a different VMware vSwitch port group for each VSM network adapter, in the **Configure Networking** screen click **L2: Configure port groups for L2**.

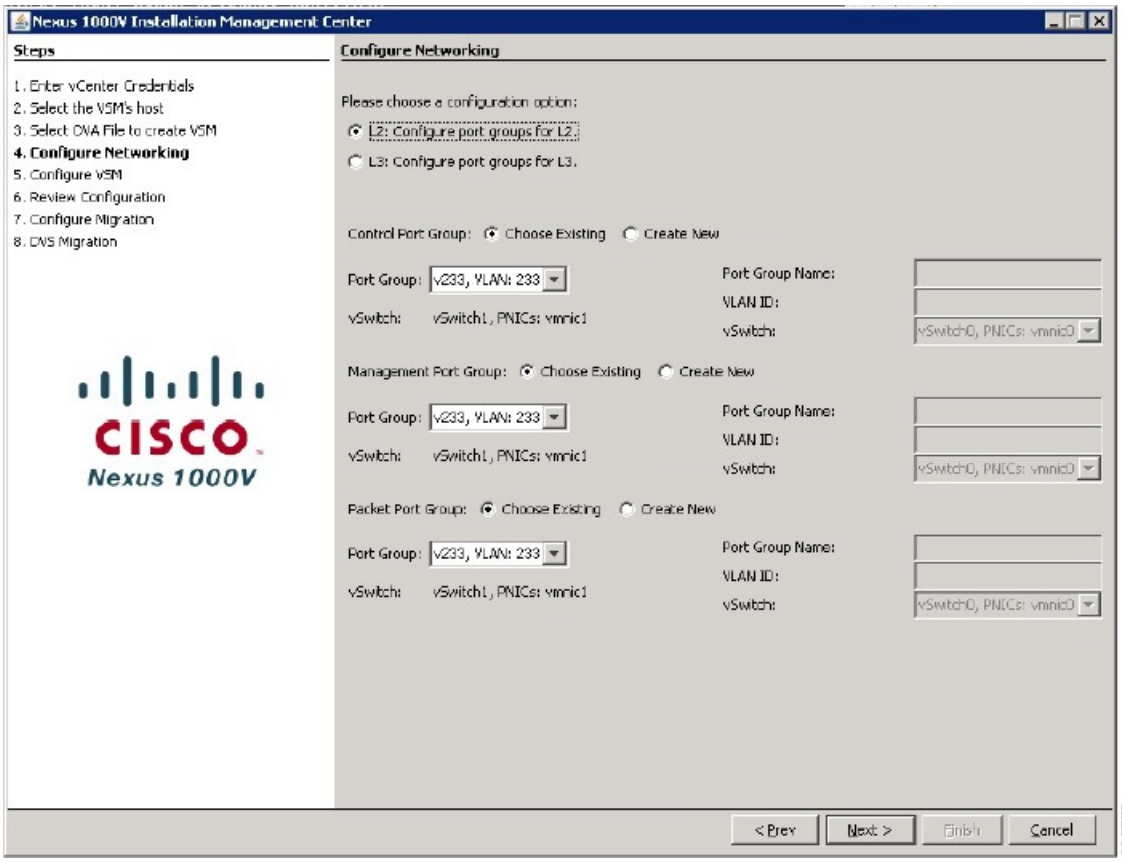
Step 2 In the **Configure Networking** screen, do the following:

- From the **Port Group** drop-down lists, choose your port groups.
- (Optional) In the **VLAN ID** field, enter the VLAN ID.

Note Only needed if you choose to create a new port group.

- Click **Next**.

Figure 48: Configure Networking Screen



Step 3 Return to Step 17 in the Layer 2 configuration procedure.

Installing a VSM on the Cisco Nexus 1010

You can install the VSM on the Cisco Nexus 1010 and move from Layer 2 to Layer 3 connectivity.

Procedure

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.4.2.1.SV1.5.2.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: [nexus-1000v.4.2.1.SV1.5.2.iso]
Enter domain id[1-4095]: 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) 2002-2012, 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#
```

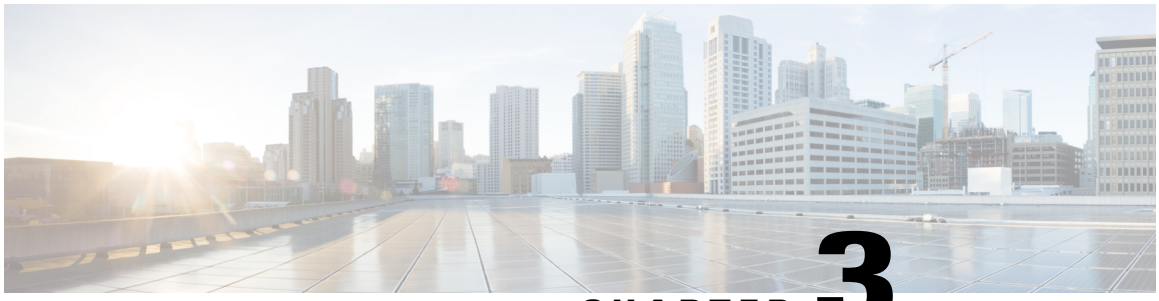
Step 6 Change svs mode from Layer 2 to Layer 3 in Cisco Nexus 1000V.

```
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
SVS domain config
  Domain id:    101
  Control vlan: 1
  Packet vlan:  1
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC failed: (communication failure to VC).
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
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.



CHAPTER 3

Upgrading the Cisco Nexus 1000V

This chapter includes the following sections:

Information About the Software Upgrade

Upgrade Software Sources

Note An interactive upgrade tool has been provided to assist you in determining the correct upgrade steps based on your current environment and the one to which you want to upgrade.

You can obtain your upgrade-related software from the following sources listed in the following table:

Table 4: Obtaining the Upgrade Software

Source	Description
Cisco	Download the Cisco Nexus 1000V Release 4.2(1)SV1(5.2) software from Cisco.com.

Source	Description
VMware	Download the VMware software from the VMware website. The Cisco Nexus 1000V Release 4.2(1)SV1(5.2) image for VMware Release 5.1 is at the VMware web site: • Online portal for VMware Update Manager (VUM): http://hostupdate.vmware.com/software/VUM/PRODUCTION/csco-main/esx/csco/csco-index.xml • Offline patch portal: http://www.vmware.com/patchmgr/download.portal

For information about your software and platform compatibility, see *Cisco Nexus 1000V and VMware Compatibility Information*.

Prerequisites for the Upgrade

Before You Begin

- The Upgrade Application cannot be used for the upgrade of the Virtual Supervisor Modules (VSMs) from Release 4.2(1)SV1(4) to Release 4.2(1)SV1(5.2).
- A pair of VSMs in a high availability (HA) pair is required in order to support a nondisruptive upgrade.
- A system with a single VSM can only be upgraded in a disruptive manner.

The network and server administrators must coordinate the upgrade procedure with each other.

The upgrade process is irrevocable. After the software is upgraded, you can downgrade by removing the current installation and reinstalling the software. For more information, see the “Recreating the Installation” section of the *Cisco Nexus 1000V Troubleshooting Guide*.

A combined upgrade of ESX and the VEM in a single maintenance mode is supported in this release. A combined upgrade requires at least vCenter 5.0 Update 1 whether you upgrade manually or are using the VMware Update Manager.

You can manually upgrade the ESX and VEM in one maintenance mode as follows:

1. Place the host in maintenance mode.
2. Upgrade ESX to 4.1 or 5.0 as needed.
3. Install the Release 4.2(1)SV1(5.2) VEM VIB while the host is still in maintenance mode.
4. Remove the host from maintenance mode.

This paired upgrade procedure is not applicable for VUM-based upgrades.

You can abort the upgrade procedure by pressing Ctrl-C.

Prerequisites for Upgrading VSMs

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, to be preserved through the upgrade.
- Save a backup copy of the running configuration in external storage.
- Perform a VSM backup. For more information, see the “Configuring VSM Backup and Recovery” chapter in the *Cisco Nexus 1000V System Management Configuration Guide*.
- Use the VSM management IP address to log into VSM and perform management tasks.

Important If you connect to a VSM using the VSA serial port or the "connect host" from the CIMC, do not initiate commands that are CPU intensive, such as copying image from tftp server to bootflash or generate a lot of screen output or updates. Use the VSA serial connections, including CIMC, only for operations such as debugging or basic configuration of the VSA.

Prerequisites for Upgrading VEMs

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

Note When you perform any VUM operation on hosts that are a part of a cluster, ensure that VMware HA, VMware fault tolerance (FT), and VMware Distributed Power Management (DPM) features are disabled for the entire cluster. Otherwise, VUM will fail to install the hosts in the cluster.

- You are logged in to the VSM command-line interface (CLI) in EXEC mode.
- 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 from one of the sources listed in VEM Software, on page 16. For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.
- If you need to migrate a vSphere host from ESX to ESXi, do it before the Cisco Nexus 1000V upgrade.

- You have placed the VEM software file in `/tmp` on the vSphere host. Placing it in the root (/) directory might interfere with the upgrade. Make sure that the root RAM disk has at least 12 MB of free space by entering the **vdf** command.
- On your upstream switches, you must have the following configuration.
  - On Catalyst 6500 Series switches with the Cisco IOS software, enter one of the following commands:

    (config-if) **portfast trunk**

    or

    (config-if) **portfast edge trunk**
  - On Cisco Nexus 5000 Series switches with Cisco NX-OS software, enter the **spanning-tree port type edge trunk** command.
- On your upstream switches, we highly recommend that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On your upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:
  - (config-if) **spanning-tree bpdu filter**
  - (config-if) **spanning-tree bpdu guard**
- For more information about configuring spanning tree, BPDU, or PortFast, see the documentation for your upstream switch.

Guidelines and Limitations for Upgrading the Cisco Nexus 1000V

Before attempting to migrate to any software image version, follow these guidelines:

Caution During the upgrade process, the Cisco Nexus 1000V does not support any new additions such as modules, Virtual NICs (vNICs), or VM NICs and does not support any configuration changes. VM NIC and vNIC port-profile changes might render VM NICs and vNICs in an unusable state.

Note vSphere 5.0 Update 1 or later is recommended over vSphere 5.0.

- You are upgrading the Cisco Nexus 1000V software to Release 4.2(1)SV1(5.2).
- Scheduling — Schedule the upgrade when your network is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure a switch during an upgrade.
- Hardware — Avoid power interruptions to the hosts that run the VSM VMs during any installation procedure.

- Connectivity to remote servers — do the following:
  - Copy the kickstart and system images from the remote server to the Cisco Nexus 1000V.
  - Ensure that the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets.
- Software images — do the following:
  - Make sure that the system and kickstart images are the same version.
  - Retrieve the images in one of two ways:
    - Locally—Images are locally available on the upgrade CD-ROM/ISO image.
    - Remotely—Images are in a remote location and you specify the destination using the remote server parameters and the filename to be used locally.
- Commands to use — do the following:
  - Verify connectivity to the remote server by using the **ping** command.
  - Use the one-step **install all** command to upgrade your software. This command upgrades the VSMs.
  - Do not enter another **install all** command while running the installation. You can run commands other than configuration commands.
  - During the VSM upgrade, if you try to add a new VEM or any of the VEMs are detached due to uplink flaps, the VEM attachment is queued until the upgrade completes.

Note If the VEMs are not compatible with the software image that you install on the VSM, a traffic disruption occurs in those modules, depending on your configuration. The **install all** command output identifies these scenarios. The hosts must be at the right version before the upgrade. If you are planning to do a combined upgrade of ESX and VEM to versions that are compatible with the VSM, you can proceed.

Before upgrading the VEMs, note these guidelines and limitations:

- The VEM software can be upgraded manually using the CLI or upgraded automatically using VUM.
- During the VEM upgrade process, VEMs reattach to the VSM.
- Connectivity to the VSM can be lost during a VEM upgrade when the interfaces of a VSM VM connect to its own Distributed Virtual Switch (DVS).
- Connectivity between an active and standby VSM can be lost during a VEM upgrade when the VEM being upgraded provides interface connectivity to one of the VSMs. In this case, both VSMs become active and lose connectivity. To prevent this problem, make sure that you are at the appropriate patch levels. See Upgrade Software Sources, on page 79.
- If you are upgrading a VEM using a Cisco Nexus 1000V bundle, follow the instructions in your VMware documentation. For more details about VMware bundled software, see the *Cisco Nexus 1000V and VMware Compatibility Information*.
- With ESX and ESXi 4.1, after the upgrade, the **esxupdate --vib-view query** command might show two Cisco VIBs as installed. If the upgrade has otherwise been successful, you can ignore this condition.

Caution Do not enter the **vemlog**, **vemcmd**, or **vempkt** commands during the VEM upgrade process because these commands impact the upgrade.

Note For the ESXi 5.0.0 release and later releases, the minimum versions are as follows:

- VMware vCenter Server 5.0.0, 455964
- VMware Update Manager 5.0.0 432001

If you plan to do a combined upgrade of ESX and VEM, the minimum vCenter Server/VUM version required is 623373/639867.

For the ESX/ESXi 4.1.0 release and later, the minimum versions are as follows:

- VMware vCenter Server 4.1.0, 258902
- VMware Update Manager 4.1.0 256596

This procedure is different from the upgrade to Release 4.2(1)SV1(4). In this procedure, you upgrade the VSMs first by using the **install all** command and then you upgrade the VEMs.

Note If your hosts are running a release prior to VMware 4.1, upgrade to VMware 4.1, VMware 5.0, or VMware 5.1. See Installing and Upgrading VMware, on page 129.

Upgrade Procedures

The following table lists the upgrade steps when upgrading to Release 4.2(1)SV1(5.2).

Table 5: Upgrade Paths from Cisco Nexus 1000V Releases

If you are running this configuration	Follow these steps
Release 4.0(4)SV1(1) or 4.0(4)SV1(2)	Upgrades from these releases are not supported.
Releases 4.0(4)SV1(3), 4.0(4)SV1(3a), 4.0(4)SV1(3b), 4.0(4)SV1(3c), or 4.0(4)SV1(3d)	1 Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b) 2 Upgrading from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2)

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4, 4a, or 4b) with a vSphere release 4.0 Update 1 or later	1 Upgrading from VMware Release 4.0 to VMware Release 4.1, on page 129 2 Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92 3 VEM Upgrade Methods from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)
Release 4.2(1)SV1(4, 4a, or 4b) with a vSphere release 4.1 GA, patches, or updates	1 Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92 2 VEM Upgrade Methods from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)
Release 4.2(1)SV1(4a) or 4.2(1)SV1(4b) with a vSphere release 5.0 GA, patches, or updates	1 Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92 2 VEM Upgrade Methods from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)

The following table lists the upgrade steps when upgrading from Release 4.2(1)SV1(5.1) and 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2).

Table 6: Upgrade Paths from Releases 4.2(1)SV1(5.1) and 4.2(1)SV1(5.1a)

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(5.1) or 4.2(1)SV1(5.1a) with vSphere 4.1 GA, patches, or updates.	1 Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92 2 VEM Upgrade Methods from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)
Release 4.2(1)SV1(5.1) or 4.2(1)SV1(5.1a) with vSphere 5.0 GA, patches, or updates.	1 Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92 2 VEM Upgrade Methods from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)
Release 4.2(1)SV1(5.2) with ESX version upgrade.	Installing and Upgrading VMware, on page 129

Upgrade Types

Upgrades can be one of three types:

- Upgrade of Cisco Nexus 1000V version only, with vSphere version intact. See Upgrading the Cisco Nexus 1000V Only, on page 86.
- Upgrade of both vSphere and Cisco Nexus 1000V versions together. See Combined Upgrade of vSphere and Cisco Nexus 1000V, on page 87.
- Upgrade of vSphere version only, with Cisco Nexus 1000V version intact. See the Installing and Upgrading VMware, on page 129 appendix.

Upgrading the Cisco Nexus 1000V Only

You must complete the following procedures to upgrade the Cisco Nexus 1000V only.

1 Upgrade the VSM. See VSM Upgrade Procedures.

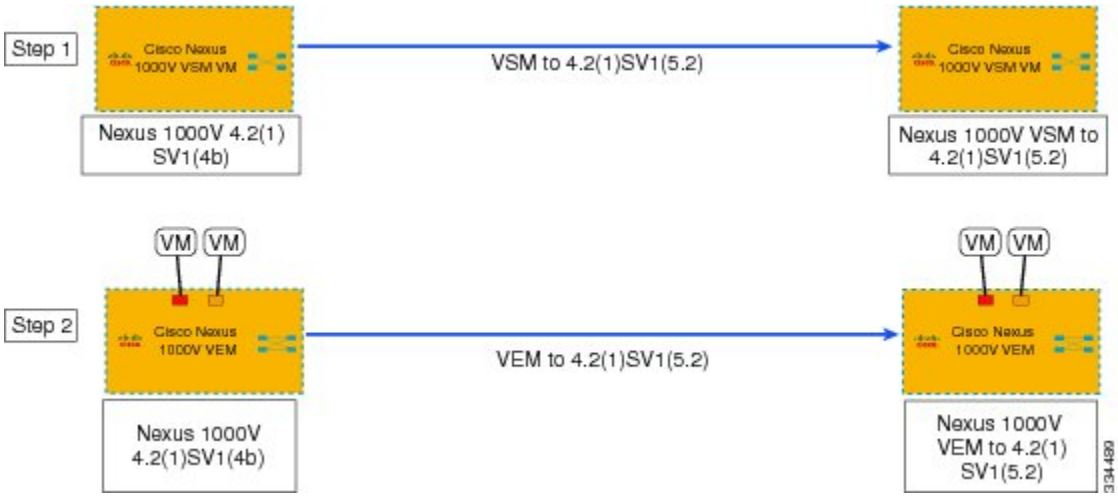
2 Upgrade the VEM.

   - For Stateless ESXi, see Installing the VEM Software on a Stateless ESXi Host, on page 66.

- For a VUM-based upgrade of a Stateful ESX or ESXi, use a host upgrade baseline with the VEM depot. See Upgrading the ESXi Hosts to Release 5.1, on page 139.
- For a stateful manual upgrade using the **esxupdate** or **esxcli** commands, see Installing ESXi 5.1 Host Software Using the CLI, on page 143.

The following figure shows the workflow for a Cisco Nexus 1000V only upgrade.

Figure 49: Cisco Nexus 1000V Only Upgrade



Combined Upgrade of vSphere and Cisco Nexus 1000V

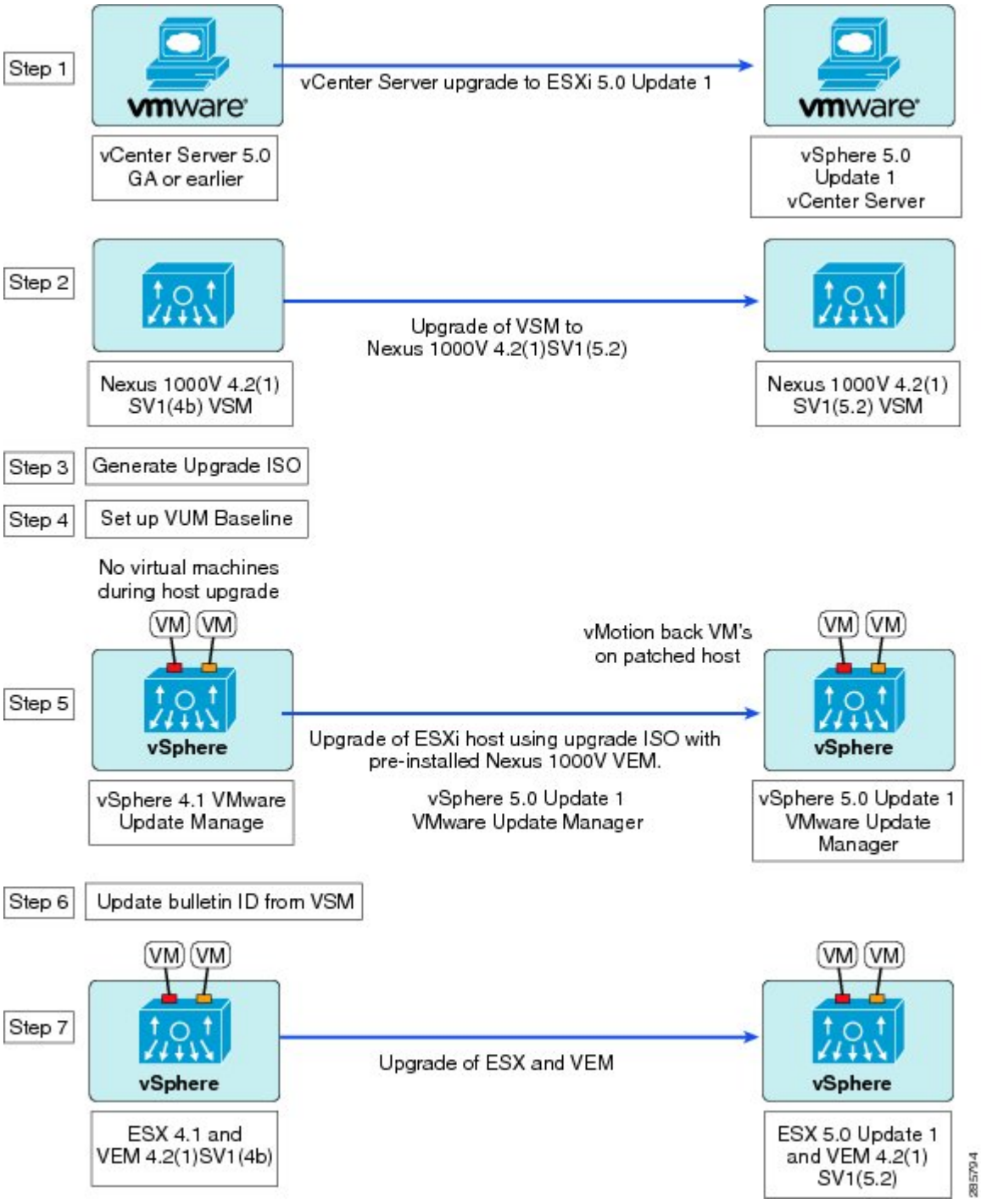
You can perform a combined upgrade of vSphere and Cisco Nexus 1000V.

If any of the hosts are running ESX 4.0 when the VSM is upgraded, the **installer** command displays that some VEMs are incompatible. You can proceed if you are planning a combined upgrade of the Cisco Nexus 1000V and ESX after the VSM upgrade completes.

Note A combined upgrade is supported only for vCenter Server 5.0 Update 1 or later.

The following figure shows the workflow for a combined upgrade.

Figure 50: Combined Upgrade Workflow



The following procedures are necessary to perform a combined upgrade.

1 Upgrading the vCenter Server to Release 5.1, on page 105
2 Upgrading the vCenter Update Manager to Release 5.1, on page 138
3 Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92
4 Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, on page 102
5 Upgrading the ESXi Hosts to Release 5.1, on page 139
6 Verifying the Build Number and Upgrade, on page 141

VSM Upgrade Procedures

Software Images

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

- Software images—The kickstart and system image files reside in directories or folders that you can access from the Cisco Nexus 1000V software prompt.
- Image version—Each image file has a version.
- Disk—The bootflash: resides on the VSM.
- ISO file—If a local ISO file is passed to the **install all** command, the kickstart and system images are extracted from the ISO file.

In-Service Software Upgrades on Systems with Dual VSMs

Note Performing an In-Service Software Upgrade (ISSU) from Cisco Nexus 1000V Release 4.2(1)SV1(4) or Release 4.2(1)SV1(4a) to Cisco Nexus 1000V Release 4.2(1)SV1(5.2) using ISO files is not supported. You must use kickstart and system files to perform an ISSU upgrade to Cisco Nexus 1000V Release 4.2(1)SV1(5.2).

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:

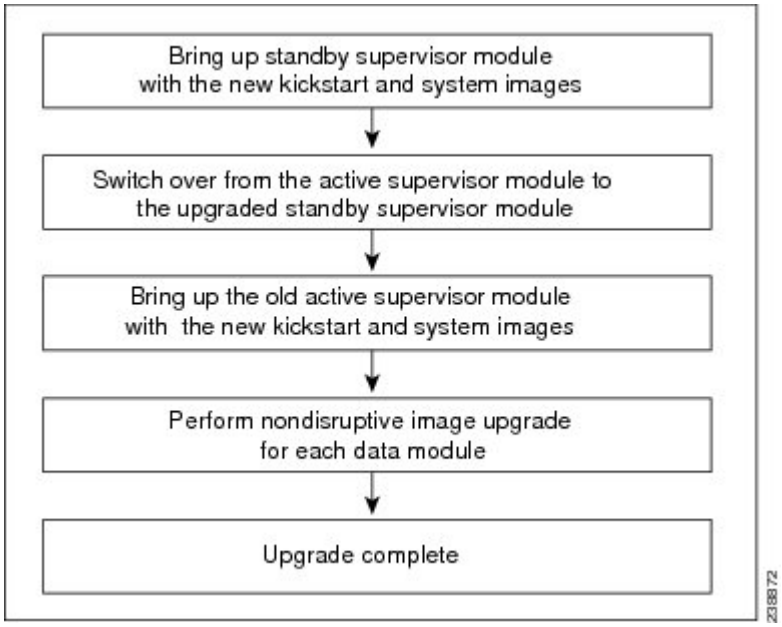
- Kickstart image
- System image
- VEM images

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

ISSU Process for the Cisco Nexus 1000V

The following figure shows the ISSU process.

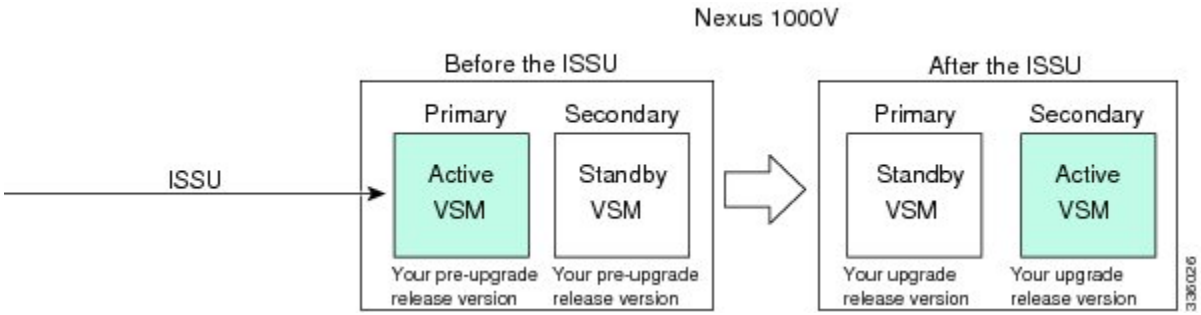
Figure 51: ISSU Process



ISSU VSM Switchover

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

Figure 52: Example of an ISSU VSM Switchover



ISSU Command Attributes

Support

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

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

Benefits

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

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

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

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

- Before a switchover process, you can see the progress only from the active VSM.

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

Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)

Procedure

Step 1 Log in to the active VSM.

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

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

Step 3 Access the Software Download Center by using this URL:
http://www.cisco.com/public/sw-center/index.shtml

Step 4 Navigate to the download site for your system.
You see links to the download images for your switch.

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

Step 6 Ensure that the required space is available for the image file(s) to be copied.

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

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

Step 7 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 8 Delete any unnecessary files to make space available if you need more space on the standby VSM.

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

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

- Copy the ISO image.

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.4.2.1.SV1.5.2.iso
bootflash:nexus-1000v.4.2.1.SV1.5.2.iso
```

- Copy kickstart and system images.

```
switch# copy
scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin
bootflash:nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-mz.4.2.1.SV1.5.2.bin
bootflash:nexus-1000v-mz.4.2.1.SV1.5.2.bin
```

Step 10 Check on the impact of the ISSU upgrade for the kickstart and system images or the ISO image.

- ISO

```
switch# show install all impact iso bootflash:nexus-1000v.4.2.1.SV1.5.2.iso

Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.2.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-4.2.1.SV1.5.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

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



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

```
Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     1   kickstart            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     2      system            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     2   kickstart            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes


Module         Running-Version                                          ESX Version
    VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
 ----------------------  ----------------------
     3           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
           COMPATIBLE              COMPATIBLE
     4           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
           COMPATIBLE              COMPATIBLE
```

- kickstart and system

```
switch# show install all impact kickstart bootflash:nexus-1000v-kickstart.mz.4.2.1.SV1.5.2.bin
system bootflash:nexus-1000v.mz.4.2.1.SV1.5.2.bin

Verifying image bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin for boot variable
 "kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

Extracting "system" version from image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

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



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


Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
```

```
     1      system            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     1   kickstart            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     2      system            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     2   kickstart            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes


Module         Running-Version                                          ESX Version
    VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
 ----------------------  ----------------------
     3           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
           COMPATIBLE              COMPATIBLE
     4           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
           COMPATIBLE              COMPATIBLE
```

Step 11 Read the release notes for the related image file. See the *Cisco Nexus 1000V Release Notes*.

Step 12 Determine if the Virtual Security Gateway (VSG) is configured in the deployment:

- If the following output is displayed, the Cisco VSG is configured in the deployment. You must follow the upgrade procedure in the *Cisco Virtual Security Gateway and Cisco Virtual Network Management Center Installation and Upgrade Guide*.

```
switch# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.2(0.689)-vsm
switch#
```

- If the following output is displayed, continue to Step 13.

```
switch# show vnm-pa status
VNM Policy-Agent status is - Not Installed
switch#
```

Step 13 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

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

```
switch# copy running-config bootflash:run-cfg-backup
switch# copy running-config scp://user@tftpserver.cisco.com/n1kv-run-cfg-backup
```

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

Step 15 Perform the upgrade on the active VSM using the ISO or kickstart and system images.

- Upgrade using the ISO image.

```
switch# install all iso bootflash:nexus-1000v.4.2.1.SV1.5.2.iso
```

- Upgrade using the kickstart and system images.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin system
bootflash:nexus-1000v-mz.4.2.1.SV1.5.2.bin
Verifying image bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin for boot variable
 "kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

Verifying image type.
```

```
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

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



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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     1   kickstart            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     2      system            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes
     2   kickstart            4.2(1)SV1(4a)           4.2(1)SV1(5.2)           yes


Module         Running-Version                                          ESX Version
    VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
 ----------------------  ----------------------
     3           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
           COMPATIBLE              COMPATIBLE
     4           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
           COMPATIBLE              COMPATIBLE

Do you want to continue with the installation (y/n)?  [n]
```

Step 16 Continue with the installation by pressing Y.

Note If you press N, the installation exits gracefully.

```
Install is in progress, please wait.

Syncing image bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin to standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin to standby.
[####################] 100% -- SUCCESS

Setting boot variables.
```

```
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100%2011 Mar 31 03:49:42 BL1-VSM %SYSMGR-STANDBY-5-CFGWRITE_STARTED:
 Configuration copy started (PID 3660).
[####################] 100% -- SUCCESS
```

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

```
Continuing with installation, please wait

Module 2: Waiting for module online
-- SUCCESS

Install has been successful
```

Step 17 After the installation operation completes, log in and verify that the switch is running the required software version.

```
switch# show version
Nexus1000v# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: loader version not available]
  kickstart: version 4.2(1)SV1(5.2) [build 4.2(1)SV1(5.2)]
  system:    version 4.2(1)SV1(5.2) [build 4.2(1)SV1(5.2)]
  kickstart image file is: bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin
  kickstart compile time:  1/11/2012 3:00:00 [01/11/2012 12:49:49]
  system image file is:    bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin
  system compile time:     1/11/2012 3:00:00 [01/11/2012 13:42:57]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU         with 2075740 kB of memory.
  Processor Board ID T5056B1802D

  Device name: Nexus1000v
  bootflash:    1557496 kB

Kernel uptime is 4 day(s), 8 hour(s), 31 minute(s), 3 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
...
```

Step 18 Copy the running configuration to the startup configuration to adjust the startup-cgf size.

```
switch# copy running-config startup-config
[########################################] 100%
switch#
```

Step 19 Display the log of the last installation.

```
switch# show install all status
This is the log of last installation.

Verifying image bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin for boot variable
"kickstart".

 -- SUCCESS

Verifying image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin for boot variable "system".

 -- SUCCESS

Verifying image type.

 -- SUCCESS

Extracting "system" version from image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin.

 -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin.

 -- SUCCESS

Notifying services about system upgrade.

 -- SUCCESS


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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           4.2(1)SV1(4a)          4.2(1)SV1(5.2)           yes
     1   kickstart           4.2(1)SV1(4a)          4.2(1)SV1(5.2)           yes
     2      system           4.2(1)SV1(4a)          4.2(1)SV1(5.2)           yes
     2   kickstart           4.2(1)SV1(4a)          4.2(1)SV1(5.2)           yes


Images will be upgraded according to following table:
Module         Running-Version                                       ESX Version
```

```
VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
----------------------  ----------------------
     3           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
      COMPATIBLE              COMPATIBLE
     4           4.2(1)SV1(4a)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
      COMPATIBLE              COMPATIBLE


Install is in progress, please wait.

Syncing image bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.5.2.bin to standby.
 -- SUCCESS

Syncing image bootflash:/nexus-1000v-mz.4.2.1.SV1.5.2.bin to standby.
 -- SUCCESS

Setting boot variables.
 -- SUCCESS

Performing configuration copy.
 -- SUCCESS

Module 2: Waiting for module online.
 -- SUCCESS

Notifying services about the switchover.
 -- SUCCESS


"Switching over onto standby".
switch#
switch#
switch#

switch# attach module 2
Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, 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(standby)#
switch(standby)# show install all status
This is the log of last installation.

Continuing with installation, please wait
Trying to start the installer...
```

```
Module 2: Waiting for module online.
 -- SUCCESS

Install has been successful.
switch(standby)#
```

VEM Upgrade Procedures

- VUM Upgrade Procedures
  - Generate an upgrade ISO. See Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, on page 102.
  - Set up VUM baselines. See Upgrading the ESXi Hosts to Release 5.1, on page 139.
  - Initiate an upgrade from VUM. See Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2), on page 107.
  - Upgrade VEM from VSM. See Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2), on page 107.
- Manual upgrade procedures
  - Upgrading VIB Manually from the CLI. See Upgrading the VEMs Manually from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 114
- Installing or upgrading stateless ESXi. See Installing the VEM Software on a Stateless ESXi Host, on page 66.

VEM upgrades fall into three types:

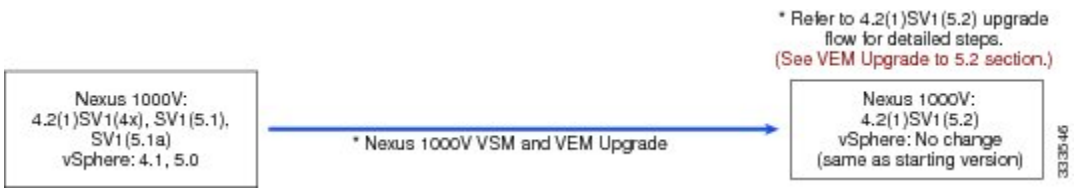
- An upgrade of an ESX or stateful ESXi host, without a migration from ESX (with a console OS) to ESXi. This upgrade type is described further in this section.
- An upgrade of a stateless ESXi host. This involves installing a new image on the host by updating the image profile and rebooting the host. The upgrade is described in Installing the VEM Software on a Stateless ESXi Host, on page 66.
- An upgrade that involve a migration from ESX to ESXi (of the same or different vSphere version).

An upgrade of an ESX or stateful ESXi host without a migration from ESX (which has a console OS) to ESXi falls into two separate workflows.

1. Upgrade the VEM alone, while keeping the ESX/ESXi version intact. The first figure shows this flow.
2. Upgrade the ESX/ESXi without a change of the Cisco Nexus 1000V version. This process is addressed in the Workflow 2 figure.

The following figure shows Workflow 1 where Cisco Nexus 1000V Release 4.2(1)SV1(4.x) or 4.2(1)SV1(5.1) is upgraded to Release 4.2(1)SV1(5.2), without a change of ESX versions.

Figure 53: Workflow 1 with a Cisco Nexus 1000V Version 4.2(1)SV1(4), SV1(4a), SV1(4b), or SV1(5.1) Installed

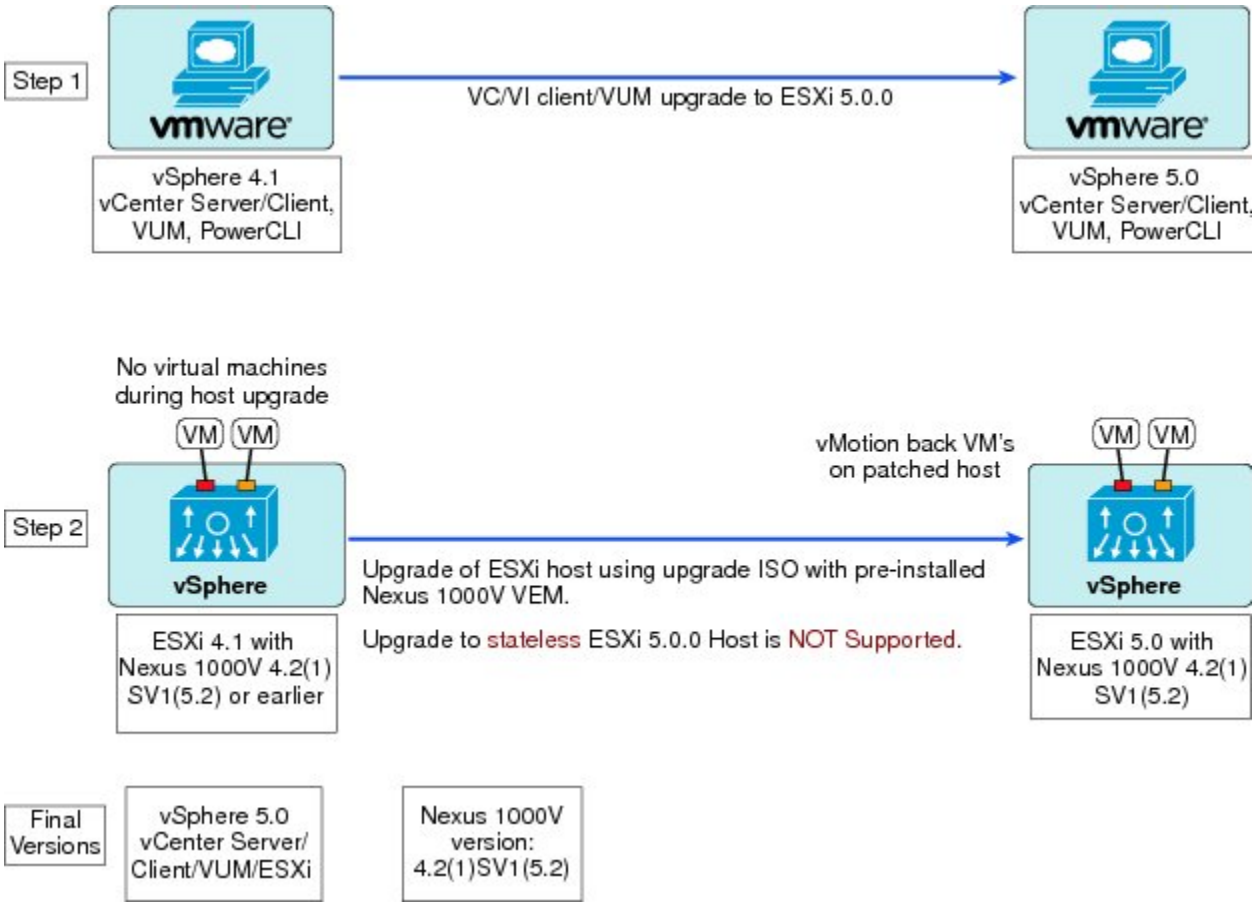


If you are using VUM, set up a host patch baseline with the VEM's offline bundle. Then follow Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2), on page 107.

If you are upgrading from the command line, see Upgrading the VEMs Manually from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 114.

The following figure shows Workflow 2 where Cisco Nexus 1000V Release 4.2(1)SV1(5.2) is installed and VMware 4.1 is upgraded to 5.0.

Figure 54: Workflow 2 with Cisco Nexus 1000V 4.2(1)SV1(5.2) Installed and Upgrading ESX from 4.1 to 5.0



If you are using VMware Update Manager, the following considerations apply:

- If you are using VUM versions prior to 5.0, do one of the following:
  - If you are upgrading the ESX host to a new patch level, use a host patch baseline (independent of whether the VEM version is being changed as well).
  - If you are upgrading the ESX host to a new update within a release or major release, use a host upgrade baseline (again independent of whether the VEM version is being changed as well).
  - You cannot upgrade the ESX version and VEM version simultaneously. You need to schedule them as two separate upgrades.
- If you are using VUM version 5.0 or later, use the following method (independent of whether the VEM version is being changed as well):
  - If you are upgrading the ESX host to a new patch level within a release, use a host patch baseline. For example, vSphere 4.1 GA to 4.1 Patch 03.
  - If you are upgrading the ESX host to a new update within a release, use a host upgrade baseline. For example, vSphere 5.0 GA to 5.0 U1.
  - If you are upgrading the ESX host to a major release (for example, vSphere 4.1 U2 to 5.0 U1), generate an upgrade ISO and set up a host upgrade baseline. The upgrade ISO must have the desired final images for both ESX and VEM. The procedure to generate an upgrade ISO is in Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, on page 102.
  - You can upgrade the ESX version and VEM version simultaneously if you are using VUM 5.0 Update 1 or later. VUM 5.0 GA does not support a combined upgrade.

Note If you plan to perform Workflow 2 and manually update to vSphere 5.0 or later, you must boot the host from an upgrade ISO with both ESX and VEM images.

VUM Upgrade Procedures

Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image

Before You Begin

- Install the VMware PowerCLI on a Windows platform. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform, where the VMware PowerCLI is installed, do one of the following:
  - Download the ESX depot, 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.

Note In the following procedure, the ESX depot is available as `C:\VMware-ESXi-5.0.0-469512-depot.zip` and the VEM bundle is available as `C:\VEM500-20110822140-BG.zip`.

Procedure

Step 1 Start the VMWare PowerCLI application.

Step 2 Connect to the vCenter Server.

```
[vSphere PowerCLI] > Connect-VIServer 192.0.2.1 -User Administrator -Password XXXXX
```

Step 3 Load the ESX depot.

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot c:\vmware-ESXi-5.0.0-depot.zip
```

Step 4 Display the image profiles.

```
[vSphere PowerCLI] > Get-EsxImageProfile
Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.0.0-469512-no-tools     VMware, Inc.    8/19/2011 1:... PartnerSupported
ESXi-5.0.0-469512-standard     VMware, Inc.    8/19/2011 1:... PartnerSupported
```

Step 5 Clone the ESX standard image profile.

Note The image profiles are usually in READ-ONLY format. You must clone the image profile before adding the VEM image to it.

```
[vSphere PowerCLI] > New-ESxImageProfile -CloneProfile ESXi-5.0.0-469512-standard -Name
n1kv-Image
Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
n1kv-Image                     VMware, Inc.    8/19/2011 1:... PartnerSupported
```

Step 6 Load the Cisco Nexus 1000V VEM offline bundle.

```
[vSphere PowerCLI] > Add-EsxSoftwareDepot C:\VEM500-20120121140109-BG-release.zip

Depot Url
---------
zip:C:\Users\Administrator\Documents\VEM500-20120121140109-BG-release.zip?in...
```

Step 7 Confirm that the n1kv-vib package is loaded.

```
[vSphere PowerCLI] > Get-EsxSoftwarePackage -Name cisco*
Name                    Version                       Vendor     Release Date
----                    -------                       ------     ------------
cisco-vem-v140-esx      4.2.1.1.5.1.0-3.0.2           Cisco      1/21/2012...
```

Step 8 Bundle the n1kv-package into the cloned image profile.

```
[vSphere PowerCLI] > Add-EsxSoftwarePackage -ImageProfile n1kv-Image -SoftwarePackage
cisco-vem-v140-esx

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
n1kv-Image                     VMware, Inc.    1/24/2012 5:... PartnerSupported
```

Step 9 Verify that the Cisco VIB is present by listing all the VIBs in the cloned image profile.

```
[vSphere PowerCLI]> $img = Get-EsxImageProfile n1kv-Image
[vSphere PowerCLI]> $img.vibList
```

```
Name                      Version                        Vendor     Release Date
----                      -------                        ------     ------------
net-ixgbe                 2.0.84.8.2-10vmw.500.0.0.46... VMware     8/19/2011...
ata-pata-hpt3x2n          0.3.4-3vmw.500.0.0.469512      VMware     8/19/2011...
ehci-ehci-hcd             1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-atiixp           0.4.6-3vmw.500.0.0.469512      VMware     8/19/2011...
scsi-megaraid2            2.00.4-9vmw.500.0.0.469512     VMware     8/19/2011...
uhci-usb-uhci             1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
net-r8168                 8.013.00-3vmw.500.0.0.469512   VMware     8/19/2011...
ohci-usb-ohci             1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
scsi-qla4xxx              5.01.03.2-3vmw.500.0.0.469512  VMware     8/19/2011...
ata-pata-sil680           0.4.8-3vmw.500.0.0.469512      VMware     8/19/2011...
scsi-megaraid-sas         4.32-1vmw.500.0.0.469512       VMware     8/19/2011...
scsi-aic79xx              3.1-5vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-amd              0.3.10-3vmw.500.0.0.469512     VMware     8/19/2011...
net-bnx2                  2.0.15g.v50.11-5vmw.500.0.0... VMware     8/19/2011...
misc-drivers              5.0.0-0.0.469512               VMware     8/19/2011...
sata-ahci                 3.0-6vmw.500.0.0.469512        VMware     8/19/2011...
scsi-fnic                 1.5.0.3-1vmw.500.0.0.469512    VMware     8/19/2011...
ata-pata-pdc2027x         1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
scsi-hpsa                 5.0.0-17vmw.500.0.0.469512     VMware     8/19/2011...
sata-sata-sil             2.3-3vmw.500.0.0.469512        VMware     8/19/2011...
net-igb                   2.1.11.1-3vmw.500.0.0.469512   VMware     8/19/2011...
net-e1000e                1.1.2-3vmw.500.0.0.469512      VMware     8/19/2011...
net-forcedeth             0.61-2vmw.500.0.0.469512       VMware     8/19/2011...
sata-ata-piix             2.12-4vmw.500.0.0.469512       VMware     8/19/2011...
scsi-qla2xxx              901.k1.1-14vmw.500.0.0.469512  VMware     8/19/2011...
scsi-adp94xx              1.0.8.12-6vmw.500.0.0.469512   VMware     8/19/2011...
net-sky2                  1.20-2vmw.500.0.0.469512       VMware     8/19/2011...
cisco-vem-v140-esx        4.2.1.1.5.1.0-3.0.2            Cisco      1/21/2012...
ipmi-ipmi-msghandler      39.1-4vmw.500.0.0.469512       VMware     8/19/2011...
net-be2net                4.0.88.0-1vmw.500.0.0.469512   VMware     8/19/2011...
esx-base                  5.0.0-0.0.469512               VMware     8/19/2011...
ipmi-ipmi-si-drv          39.1-4vmw.500.0.0.469512       VMware     8/19/2011...
scsi-megaraid-mbox        2.20.5.1-6vmw.500.0.0.469512   VMware     8/19/2011...
net-nx-nic                4.0.557-3vmw.500.0.0.469512    VMware     8/19/2011...
sata-sata-promise         2.12-3vmw.500.0.0.469512       VMware     8/19/2011...
scsi-ips                  7.12.05-4vmw.500.0.0.469512    VMware     8/19/2011...
scsi-lpfc820              8.2.2.1-18vmw.500.0.0.469512   VMware     8/19/2011...
ata-pata-cmd64x           0.2.5-3vmw.500.0.0.469512      VMware     8/19/2011...
sata-sata-svw             2.3-3vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-via              0.3.3-2vmw.500.0.0.469512      VMware     8/19/2011...
esx-tboot                 5.0.0-0.0.469512               VMware     8/19/2011...
misc-cnic-register        1.1-1vmw.500.0.0.469512        VMware     8/19/2011...
net-s2io                  2.1.4.13427-3vmw.500.0.0.46... VMware     8/19/2011...
net-e1000                 8.0.3.1-2vmw.500.0.0.469512    VMware     8/19/2011...
block-cciss               3.6.14-10vmw.500.0.0.469512    VMware     8/19/2011...
net-enic                  1.4.2.15a-1vmw.500.0.0.469512  VMware     8/19/2011...
net-bnx2x                 1.61.15.v50.1-1vmw.500.0.0.... VMware     8/19/2011...
scsi-mpt2sas              06.00.00.00-5vmw.500.0.0.46... VMware     8/19/2011...
sata-sata-nv              3.5-3vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-serverworks      0.4.3-3vmw.500.0.0.469512      VMware     8/19/2011...
net-cnic                  1.10.2j.v50.7-2vmw.500.0.0.... VMware     8/19/2011...
scsi-mptsas               4.23.01.00-5vmw.500.0.0.469512 VMware     8/19/2011...
```

```
scsi-aacraid             1.1.5.1-9vmw.500.0.0.469512    VMware     8/19/2011...
tools-light              5.0.0-0.0.469512               VMware     8/19/2011...
ima-qla4xxx              2.01.07-1vmw.500.0.0.469512    VMware     8/19/2011...
ipmi-ipmi-devintf        39.1-4vmw.500.0.0.469512       VMware     8/19/2011...
net-tg3                  3.110h.v50.4-4vmw.500.0.0.4... VMware     8/19/2011...
scsi-bnx2i               1.9.1d.v50.1-3vmw.500.0.0.4... VMware     8/19/2011...
net-r8169                6.011.00-2vmw.500.0.0.469512   VMware     8/19/2011...
scsi-mptspi              4.23.01.00-5vmw.500.0.0.469512 VMware     8/19/2011...
```

Step 10 Export the image profile to an ISO file.

```
[vSphere PowerCLI]> Export-EsxImageProfile -ImageProfile n1kv-Image -FilePath
C:\n1kv15-esx50.iso –ExportToIso
```

Upgrading the vCenter Server to Release 5.1

Note This upgrade procedure also applies to vCenter Server 5.0 and vCenter Server 5.0 Update 1 and later.

Before You Begin

- Download the upgrade ISO file that contains the ESXi 5.1 bits and the Cisco Nexus 1000V Release 4.2(1)SV1(5.2) bits.
- See the *Cisco Nexus 1000V and VMware Compatibility Information* document to determine the correct VIB Version, VEM Bundle, Host Build, vCenter Server, and Update Manager versions.

Procedure

Step 1 Navigate to the VMware vSphere 5.1 installation file.

Note If you have the ISO image, you should mount it on the host.

Step 2 Double-click **autorun.**

Step 3 In the **VMware vCenter Installer** window, click **vCenter Server**.

Step 4 Click **Install**.

Step 5 Choose a language and click **OK.**

Step 6 Click **Next.**

Step 7 In the Patent Agreement window, click **Next.**

Step 8 In the **License Agreement** window, click the **I agree to the terms in the license agreement** radio button.

Step 9 Click **Next.**

Step 10 In the **Database Options** screen, click **Next.**

Step 11 Click the **Upgrade existing vCenter Server database** radio button and check the **I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\.** check box.

Step 12 From the **Windows Start** Menu, click **Run.**

Step 13 Enter the name of the folder that contains the vCenter Server database and click **OK.**

Step 14 Drag a copy of the parent folder (SSL) to the desktop as a backup.

Step 15 Return to the installer program.

Step 16 Click **Next.**

Step 17 In the vCenter Agent Upgrade window, click the **Automatic** radio button.

Step 18 Click **Next.**

Step 19 In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box.

Step 20 Click **Next.**

Step 21 Review the port settings and click **Next.**

Step 22 In the **vCenter Server JVM Memory** screen based on the number of hosts, click the appropriate memory radio button.

Step 23 Click **Next.**

Step 24 Click **Install.**

Step 25 Click **Finish.**
This step completes the upgrade of the vCenter Server.

Step 26 Upgrade the VMware vSphere Client to ESXi 5.1.

Step 27 Open the VMware vSphere Client.

Step 28 From the **Help** menu, choose **About VMware vSphere**.

Step 29 Confirm that the vSphere Client and the VMware vCenter Server are both version VMware 5.1.

Step 30 Click **OK**, and exit the VMware vSphere Client.

What to Do Next

Complete the steps in Upgrading the vCenter Update Manager to Release 5.1, on page 138.

Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), or 4.2(1)SV1(5.1) to Release 4.2(1)SV1(5.2)

Caution If removable media is still connected (for example, if you have installed the VSM using ISO and forgot to remove the media), host movement to maintenance mode fails and the VUM upgrade fails.

Procedure

Step 1 Display the current configuration.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM400-201204033-RG
switch#
```

Note The minimum release of Cisco Nexus 1000V for VMware ESXi 5.0.0 hosts is Release 4.2(1)SV1(4a).

Step 2 Coordinate with and notify the server administrator of the VEM upgrade process.

```
switch# vmware vem upgrade notify
Warning:
Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to
corresponding
"Cisco Nexus 1000V and VMware Compatibility Information" guide.
```

Step 3 Verify that the upgrade notification was sent.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM400-201204033-RG
switch#
```

Note Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.

Step 4 Verify that the server administrator has accepted the upgrade in the vCenter.
For more information about how the server administrator accepts the VEM upgrade, see Accepting the VEM Upgrade, on page 110.

Coordinate the notification acceptance with the server administrator. After the server administrator accepts the upgrade, proceed with the VEM upgrade.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM400-201204033-RG
switch#
```

Note Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.

Step 5 Initiate the VUM upgrade process.

Note Before entering the following command, communicate with the server administrator to confirm that the VUM process is operational.

The vCenter Server locks the DVS and triggers VUM to upgrade the VEMs.

```
switch# vmware vem upgrade proceed
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM410-201208144101-BG
switch#
```

Note The DVS bundle ID is updated and is highlighted.

If the ESX/ESXi host is using ESX/ESXi 4.1.0 or a later release and your DRS settings are enabled to allow it, VUM automatically VMotions the VMs from the host to another host in the cluster and places the ESX/ESXi in maintenance mode to upgrade the VEM. This process is continued for other hosts in the DRS cluster until all the hosts are upgraded in the cluster. For details about DRS settings required and vMotion of VMs, visit the VMware documentation related to Creating a DRS Cluster.

Step 6 Check for the upgrade complete status.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter): Tue Aug 21 19:14:38 2012
Upgrade Error:
Upgrade Bundle ID:
```

```
    VSM: VEM410-201208144101-BG
    DVS: VEM410-201208144101-BG
switch#
```

Step 7 Clear the VEM upgrade status after the upgrade process is complete.

```
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM410-201208144101-BG
switch#
```

Step 8 Verify that the upgrade process is complete.

```
switch# show module
Mod  Ports  Module-Type                      Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    248    Virtual Ethernet Module           NA                  ok
4    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV1(5.2)      0.0
2    4.2(1)SV1(5.2)      0.0
3    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.249.171   NA                                    NA
2    10.104.249.171   NA                                    NA
3    10.104.249.172   7d41e666-b58a-11e0-bd1d-30e4dbc299c0  10.104.249.172
4    10.104.249.173   17d79824-b593-11e0-bd1d-30e4dbc29a0e  10.104.249.173

* this terminal session
switch#
```

Note The lines with the bold characters in the preceding example display that all VEMs are upgraded to Release 4.2(1)SV1(5.2).

The upgrade is complete.

Accepting the VEM Upgrade

Before You Begin

- The network and server administrators must coordinate the upgrade procedure with each other.
- You have received a notification in the vCenter Server that a VEM software upgrade is available.

Procedure

Step 1 In the vCenter Server, choose **Inventory > Networking**.

Step 2 Click the **vSphere Client DVS Summary** tab to check for the availability of a software upgrade.

Figure 55: vSphere Client DVS Summary Tab

Step 3 Click **Apply upgrade**.
The network administrator is notified that you are ready to apply the upgrade to the VEMs.

Manual Upgrade Procedures

Upgrading the VEM Software Using the vCLI

You can upgrade the VEM software by using the vCLI.

Before You Begin

- If you are using vCLI, do the following:
  - You have downloaded and installed the VMware vCLI. For information about installing the vCLI, see the VMware vCLI documentation.
  - You are logged in to the remote host where the vCLI is installed.

Note The vSphere command-line interface (vCLI) command set allows you to enter common system administration commands against ESX/ESXi systems from any machine with network access to those systems. You can also enter most vCLI commands against a vCenter Server system and target any ESX/ESXi system that the vCenter Server system manages. vCLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

- If you are using the **esxupdate** command, you are logged in to the ESX host.
- Check *Cisco Nexus 1000V and VMware Compatibility Information* for compatible versions.
- You have already copied the VEM software installation file to the `/tmp` directory. Do not copy the files to the root (/) folder.
- You know the name of the VEM software file to be installed.

Procedure

Step 1 Go to the directory where the new VEM software was copied.

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
```

Step 2 Determine the upgrade method that you want to use and enter the appropriate command:

- If you are using the vCLI, enter the **vihostupdate** command and install the ESX/ ESXi and VEM software simultaneously.
- If you are on an ESXi host running ESXi 4.1, enter one of the following commands:

vihostupdate --install --bundle [*path to Cisco updated VEM offline bundle*] **--server** [*vsphere host IP address*]

Note Put the host in maintenance mode before you enter the following command:

```
[root@serialport tmp]# vihostupdate --install --bundle VEM410-20120803144401.zip --server
192.0.2.0
Enter username: root
Enter password:
Please wait installation in progress ...
The update completed successfully, but the system needs to be rebooted for the changes to
be effective.
[root@serialport tmp]#
```

- If you are using the **esxupdate** command from the ESX host /tmp directory, install the VEM software as shown in the following example:

  Note When using the **esxupdate** command, you must log in to each host and enter the following command.

  esxupdate -b *[VMware offline update bundle]* **update**
  This command loads the software manually onto the host, loads the kernel modules, and starts the VEM Agent on the running system.

For ESX/ESXi 4.1.0 hosts, enter the following commands:

```
/tmp # esxupdate --bundle=VEM410-20120803144401.zip update
Unpacking cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.1
##################################################################################################################
 [100%]

Installing packages :cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.1
##################################################################################################################
 [100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
/tmp #

/tmp # esxupdate -b cross_cisco-vem-v144-4.2.1.1.5.2.0-2.0.2.vib update
Unpacking cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.2
##################################################################################################################
 [100%]

Installing packages :cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.2
##################################################################################################################
 [100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
/tmp #
```

For ESXi 5.0.0 or a later release host, enter the appropriate commands as they apply to you.

```
~ # esxcli software vib install -d /absolute-path/VEM_bundle
~ # esxcli software vib install -v /absolute-path/vib_file
```

Note You must specify the absolute path to the *VEM_bundle* and *vib_file* files. The absolute path is the path that starts at the root of the file system such as `/tmp/vib_file`.

```
~ # esxcli software vib install -d /tmp/VEM500-20120803144112-BG-release.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.2
   VIBs Removed:
   VIBs Skipped:
~ #

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v144-4.2.1.1.5.2.0-3.0.2.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.2
   VIBs Removed:
   VIBs Skipped:
~ #
```

Step 3 Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information*.

```
[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-469512
root@serialport tmp]# # esxupdate query
------Bulletin ID------- -----Installed----- --------------Summary---------------
```

```
VEM410-20120803144401-BG 2012-08-21T08:18:22 Cisco Nexus 1000V 4.2(1)SV1(5.2)

[root@host212 ~]# . ~ # vem status -v
Package vssnet-esx5.5.0-00000-release
Version 4.2.1.1.5.2.0-2.0.1
Build 1
Date Fri Aug 3 00:02:21 PDT 2012

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         3           128               1500    vmnic2
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
switch           256         40          256               1500
vmnic7,vmnic6,vmnic5,vmnic4,vmnic3

Number of PassThru NICs are 0
VEM Agent (vemdpa) is running

~ #


[root@host212 ~]# vemcmd show version
VEM Version: 4.2.1.1.5.2.0-2.0.1
VSM Version: 4.2(1)SV1(5.2)
System Version: VMware ESXi 4.1.0 Releasebuild-502767
~ #
```

Step 4 Display that the VEMs were upgraded by entering the following commands from the VSM.

```
switch# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    248    Virtual Ethernet Module           NA                  ok
4    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV1(5.2)      0.0
2    4.2(1)SV1(5.2)      0.0
3    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.249.171   NA                                    NA
```

```
2    10.104.249.171   NA                                    NA
3    10.104.249.172   7d41e666-b58a-11e0-bd1d-30e4dbc299c0  10.104.249.172
4    10.104.249.173   17d79824-b593-11e0-bd1d-30e4dbc29a0e  10.104.249.173

* this terminal session
switch#
```

Note The highlighted text in the previous command output confirms that the upgrade was successful.

If the upgrade was successful, the installation procedure is complete.

Upgrading the VEMs Manually from Release 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2)

Before You Begin

Note If VUM is installed, it should be disabled.

To manually install or upgrade the Cisco Nexus 1000V VEM on an ESX/ESXi host, follow the steps in Upgrading the VEM Software Using the vCLI, on page 110.

To upgrade the VEMs manually, perform the following steps as network administrator:

Note This procedure is performed by the network administrator. Before proceeding with the upgrade, make sure that the VMs are powered off if you are not running the required patch level.

Caution If removable media is still connected, (for example, if you have installed the VSM using ISO and forgot to remove the media), host movement to maintenance mode fails and the VEM upgrade fails.

Procedure

Step 1 Coordinate with and notify the server administrator of the VEM upgrade process.

```
switch# vmware vem upgrade notify
Warning:
Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to
corresponding
"Cisco Nexus 1000V and VMware Compatibility Information" guide.
```

Step 2 Verify that the upgrade notification was sent.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
```

```
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM400-201204033-RG
switch#
```

Step 3 Verify that the server administrator has accepted the upgrade in vCenter Server.
For details about the server administrator accepting the VEM upgrade, see Accepting the VEM Upgrade, on page 110.

After the server administrator accepts the upgrade, proceed with the VEM upgrade.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM400-201204033-RG
switch#
```

Step 4 Perform one of the following tasks:

- If the ESX host is not hosting the VSM, proceed to Step 5.
- If the ESX host is hosting the VSM, coordinate with the server administrator to migrate the VSM to a host that is not being upgraded. Proceed to Step 5.

Step 5 Initiate the Cisco Nexus 1000V Bundle ID upgrade process.

Note If VUM is enabled in the vCenter environment, disable it before entering the **vmware vem upgrade proceed** command to prevent the new VIBs from being pushed to all the hosts.

Enter the **vmware vem upgrade proceed** command so that the Cisco Nexus 1000V Bundle ID on the vCenter Server gets updated. If VUM is enabled and you do not update the Bundle ID, an incorrect VIB version is pushed to the VEM when you next add the ESX to the VSM.

```
switch# vmware vem upgrade proceed
```

Note If VUM is not installed, the "The object or item referred to could not be found" error appears in the vCenter Server's task bar. You can ignore this error message.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
```

```
    DVS: VEM410-201208144101-BG
switch#
```

Step 6 Check for the Upgrade Complete status.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter): Tue Aug 21 19:14:38 2012
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM410-201208144101-BG
switch#
```

Step 7 Coordinate with and wait until the server administrator upgrades all ESX host VEMs with the new VEM software release and informs you that the upgrade process is complete.
The server administrator performs the manual upgrade by using the **vihostupdate** command or the **esxcli** command. For more information, see Upgrading the VEM Software Using the vCLI, on page 110.

Step 8 Clear the VEM upgrade status after the upgrade process is complete.

```
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201208144101-BG
    DVS: VEM410-201208144101-BG
switch#
```

Step 9 Verify that the upgrade process is complete.

```
switch# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    248    Virtual Ethernet Module           NA                  ok
4    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV1(5.2)      0.0
2    4.2(1)SV1(5.2)      0.0
3    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
```

```
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.249.171   NA                                    NA
2    10.104.249.171   NA                                    NA
3    10.104.249.172   7d41e666-b58a-11e0-bd1d-30e4dbc299c0  10.104.249.172
4    10.104.249.173   17d79824-b593-11e0-bd1d-30e4dbc29a0e  10.104.249.173

* this terminal session
switch#
```

Note The line with the bold characters in the preceding example display that all VEMs are upgraded to Release 4.2(1)SV1(5.2).

The upgrade is complete.

Upgrading the VEM Software Using the vCLI

You can upgrade the VEM software by using the vCLI.

Before You Begin

- If you are using vCLI, do the following:
  - You have downloaded and installed the VMware vCLI. For information about installing the vCLI, see the VMware vCLI documentation.
  - You are logged in to the remote host where the vCLI is installed.

Note The vSphere command-line interface (vCLI) command set allows you to enter common system administration commands against ESX/ESXi systems from any machine with network access to those systems. You can also enter most vCLI commands against a vCenter Server system and target any ESX/ESXi system that the vCenter Server system manages. vCLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

- If you are using the **esxupdate** command, you are logged in to the ESX host.
- Check *Cisco Nexus 1000V and VMware Compatibility Information* for compatible versions.
- You have already copied the VEM software installation file to the `/tmp` directory. Do not copy the files to the root (/) folder.
- You know the name of the VEM software file to be installed.

Procedure

Step 1 Go to the directory where the new VEM software was copied.

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
```

Step 2 Determine the upgrade method that you want to use and enter the appropriate command:

- If you are using the vCLI, enter the **vihostupdate** command and install the ESX/ ESXi and VEM software simultaneously.
- If you are on an ESXi host running ESXi 4.1, enter one of the following commands:

vihostupdate --install --bundle [*path to Cisco updated VEM offline bundle*] **--server** [*vsphere host IP address*]

Note Put the host in maintenance mode before you enter the following command:

```
[root@serialport tmp]# vihostupdate --install --bundle VEM410-20120803144401.zip --server
192.0.2.0
Enter username: root
Enter password:
Please wait installation in progress ...
The update completed successfully, but the system needs to be rebooted for the changes to
be effective.
[root@serialport tmp]#
```

- If you are using the **esxupdate** command from the ESX host /tmp directory, install the VEM software as shown in the following example:

  Note When using the **esxupdate** command, you must log in to each host and enter the following command.

  esxupdate -b *[VMware offline update bundle]* **update**
  This command loads the software manually onto the host, loads the kernel modules, and starts the VEM Agent on the running system.

For ESX/ESXi 4.1.0 hosts, enter the following commands:

```
/tmp # esxupdate --bundle=VEM410-20120803144401.zip update
Unpacking cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.1
##################################################################################################################
 [100%]

Installing packages :cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.1
##################################################################################################################
 [100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
/tmp #

/tmp # esxupdate -b cross_cisco-vem-v144-4.2.1.1.5.2.0-2.0.2.vib update
Unpacking cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.2
##################################################################################################################
 [100%]
```

```
Installing packages :cross_cisco-vem-v144-esx_4.2.1.1.5.2.0-2.0.2
##################################################################################################################
 [100%]

Running [/usr/sbin/vmkmod-install.sh]...
ok.
/tmp #
```

For ESXi 5.0.0 or a later release host, enter the appropriate commands as they apply to you.

```
~ # esxcli software vib install -d /absolute-path/VEM_bundle
~ # esxcli software vib install -v /absolute-path/vib_file
```

Note You must specify the absolute path to the *VEM_bundle* and *vib_file* files. The absolute path is the path that starts at the root of the file system such as `/tmp/vib_file`.

```
~ # esxcli software vib install -d /tmp/VEM500-20120803144112-BG-release.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.2
   VIBs Removed:
   VIBs Skipped:
~ #

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v144-4.2.1.1.5.2.0-3.0.2.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.2
   VIBs Removed:
   VIBs Skipped:
~ #
```

Step 3 Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information*.

```
[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-469512
root@serialport tmp]# # esxupdate query
------Bulletin ID------- -----Installed----- --------------Summary---------------
VEM410-20120803144401-BG 2012-08-21T08:18:22 Cisco Nexus 1000V 4.2(1)SV1(5.2)

[root@host212 ~]# . ~ # vem status -v
Package vssnet-esx5.5.0-00000-release
Version 4.2.1.1.5.2.0-2.0.1
Build 1
Date Fri Aug 3 00:02:21 PDT 2012

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         3           128               1500    vmnic2
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
switch           256         40          256               1500
vmnic7,vmnic6,vmnic5,vmnic4,vmnic3

Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

```
~ #


[root@host212 ~]# vemcmd show version
VEM Version: 4.2.1.1.5.2.0-2.0.1
VSM Version: 4.2(1)SV1(5.2)
System Version: VMware ESXi 4.1.0 Releasebuild-502767
~ #
```

Step 4 Display that the VEMs were upgraded by entering the following commands from the VSM.

```
switch# show module
Mod  Ports  Module-Type                      Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    248    Virtual Ethernet Module           NA                  ok
4    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV1(5.2)      0.0
2    4.2(1)SV1(5.2)      0.0
3    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.249.171   NA                                    NA
2    10.104.249.171   NA                                    NA
3    10.104.249.172   7d41e666-b58a-11e0-bd1d-30e4dbc299c0  10.104.249.172
4    10.104.249.173   17d79824-b593-11e0-bd1d-30e4dbc29a0e  10.104.249.173

* this terminal session
switch#
```

Note The highlighted text in the previous command output confirms that the upgrade was successful.

If the upgrade was successful, the installation procedure is complete.

Installing the VEM Software on a Stateless ESXi Host

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

Procedure

Step 1 See the procedure for Adding the Cisco Nexus 1000V to an ESXi Image Profile, on page 66.

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 69
- Installing the VEM Software on a Stateless ESXi Host Using VUM, on page 71

Step 3 See the procedure for Configuring Layer 2 Connectivity, on page 74.

Installing the VEM Software on a Stateless ESXi Host Using esxcli

Before You Begin

- When entering 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.

```
~ # vmware -v
VMware ESXi 5.0.0 build-441354
~ #
~ # vmware -l
VMware ESXi 5.0.0 GA
```

Step 2 Log in to the ESXi stateless host.

Step 3 Copy the offline bundle to the host.

```
~ # esxcli software vib install -d /vmfs/volumes/newnfs/MN-VEM/VEM500-20110728153-BG-release.zip

Installation Result
   Message: WARNING: Only live system was updated, the change is not persistent.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v131-esx_4.2.1.1.4.1.0-3.0.5
   VIBs Removed:
   VIBs Skipped:
```

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.

```
~ # esxcli software vib list | grep cisco
cisco-vem-v131-esx    4.2.1.1.4.1.0-3.0.5              Cisco   PartnerSupported  2011-08-18
```

Step 5 Check that the VEM agent is running.

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.4.1.0-3.0.5
```

```
Build 5
Date Thu Jul 28 01:37:10 PDT 2011
Number of PassThru NICs are 0
VEM modules are loaded
Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         4           128               1500    vmnic4
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

Step 6 Display the VEM version, VSM version, and ESXi version.

```
~ # vemcmd show version
VEM Version: 4.2.1.1.4.1.0-3.0.5
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

Step 7 Display the ESXi version and details about pass-through NICs.

```
~ # vem version -v
Number of PassThru NICs are 0
Running esx version -441354 x86_64
VEM Version: 4.2.1.1.4.1.0-3.0.5
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

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.

```
switch# show module
Mod  Ports  Module-Type                      Model               Status
---  -----  -------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module        Nexus1000V          active *
2    0      Virtual Supervisor Module        Nexus1000V          ha-standby
3    248    Virtual Ethernet Module          NA                            ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    4.2(1)SV1(4a)     0.0
2    4.2(1)SV1(4a)     0.0
3    4.2(1)SV1(4a)     VMware ESXi 5.0.0 Releasebuild-441354 (3.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.62.227    NA                                    NA
2    10.104.62.227    NA                                    NA
3    10.104.62.216    3fa746d4-de2f-11de-bd5d-c47d4f7ca460  sans2-216.cisco.com
```

Installing the VEM Software on a Stateless ESXi Host Using VUM

Before You Begin

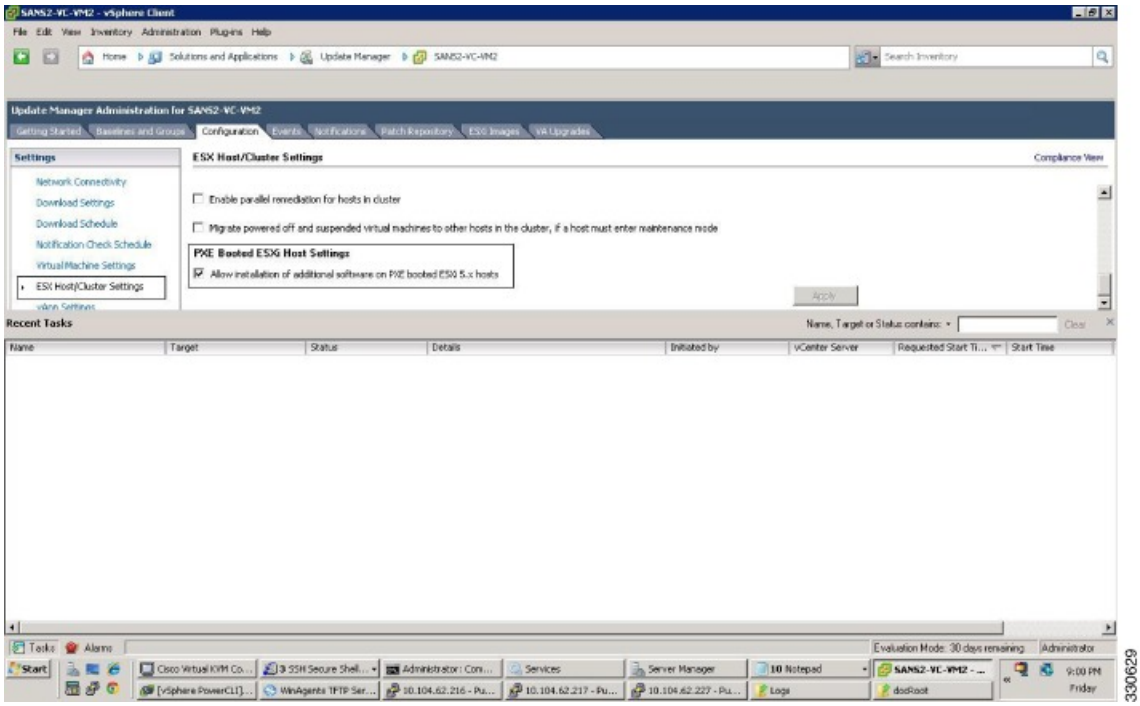
- Make sure that the VUM patch repository has the VEM software downloaded.

Procedure

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

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

Figure 56: ESX Host/Cluster Settings Window



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

Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.2)

Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.2) is a two-step process.

Procedure

Step 1 See the Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b) section in the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4b)*.

Step 2 See the Upgrade Paths.

Migrating from Layer 2 to Layer 3

Layer 3 Advantages

The following lists the advantages of using a Layer 3 configuration over a Layer 2 configuration:

- The VSM can control the VEMs that are in a different subnets.
- The VEMs can be in different subnets.
- Because the VEMs can be in different subnets, there is no constraint on the physical location of the hosts.
- Minimal VLAN configurations are required for establishing the VSM-VEM connection when compared to Layer 2 control mode. The IP address of the VEM (Layer 3 capable vmknic's IP address) and the VSM's control0/mgmt0 interface are the only required information.
- In the VSM, either the mgmt0 or the control0 interface can be used as the Layer 3 control interface. If mgmt0 is used, there is no need for another IP address as the VSM's management IP address is used for VSM-VEM Layer 3 connection.
- If the management VMKernel (vmk0) is used as the Layer 3 control interface in the VEM, there is no need for another IP address because the host's management IP address is used for VSM-VEM Layer 3 connectivity.

Note These advantages are applicable only for ESX-Visor hosts. On ESX-Cos hosts, a new VMKernel must be created.

Interface Comparisons Between mgmt0 and control0

The following describes the differences between using a mgmt0 interface or a control0 interface:

- On the VSM, there are two ways of connectivity via the mgmt0 or control0 interface.
- Setting mgmt0 as Layer 3 interface uses the mgmt0 interface on the VSM.
- The control0 interface is a special interface created for Layer 3 connectivity.

- The Layer 3 interface on the VEM is selected by designating the interface with the Layer 3 control capability.
- The egress control traffic route is decided by the VMware routing stack.
- On a VEM, the management vmknic (vmk0) can be used for Layer 3 control connectivity if it is managed by the Cisco Nexus 1000V and is designated with the Layer 3 control capability.

Configuring the Layer 3 Interface

Configure either the control0 (see Step 1) or mgmt0 interface (see Step 2).

Procedure

Step 1 Configuring the control0 interface.

Note When using control0 as the control interface on the VSM, the control0 interface must be assigned with an IP address.

a) Configure the IP address.

```
switch# configure terminal
switch(config)# interface control 0
switch(config-if)# ip address 5.5.5.2 255.255.255.0
```

b) Display the running configuration of the control0 interface.

```
switch# show running-config interface control 0
!Command: show running-config interface control0
!Time: Mon Dec 12 02:41:47 2011
version 4.2(1)SV1(5.1)
interface control0
  ip address 5.5.5.2/24
```

Step 2 Configure the mgmt0 interface.

Note When using mgmt0 as the control interface, no configuration on the VSM is required as the mgmt0 interface is assigned with the host's management IP address.

a) Display the running configuration of the mgmt0 interface.

```
switch# show running-config interface mgmt 0
!Command: show running-config interface mgmt0
!Time: Mon Dec 12 02:43:25 2011
version 4.2(1)SV1(5.1)
interface mgmt0
  ip address 10.104.249.37/27
```

Creating a Port Profile with Layer 3 Control Capability

Note VEM modules will 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. Migrate your management vmkernel interface into the Layer 3 capable port profile. Do not use multiple vmkernel interfaces on the same subnet.

Before You Begin

- You are creating a port profile with Layer 3 control capability.
- Allow the VLAN that you use for VSM to VEM connectivity in this port profile.
- Configure the VLAN as a system VLAN.

Procedure

Step 1 Create a Layer 3 port profile.

```
VSM_1# configure terminal
VSM_1(config)# port-profile type vethernet l3_control
VSM_1(config-port-prof)# switchport mode access
VSM_1(config-port-prof)# switchport access vlan 3160
VSM_1(config-port-prof)# capability l3control
VSM_1(config-port-prof)# vmware port-group
VSM_1(config-port-prof)# state enabled
VSM_1(config-port-prof)# no shutdown
```

Step 2 Display the port profile.

```
VSM_1# show port-profile name l3_control
port-profile l3_control
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 min-ports: 1
 inherit:
 config attributes:
  switchport mode access
  switchport access vlan 3160 (Allow the VLAN in access mode.)
  no shutdown
 evaluated config attributes:
  switchport mode access
  switchport access vlan 3160
  no shutdown
 assigned interfaces:
  Vethernet1
 port-group: l3_control
 system vlans: 3160 (Configure the VLAN as a system VLAN.)
 capability l3control: yes (Configure capability l3 control.)
 capability iscsi-multipath: no
```

```
capability vxlan: no
capability l3-vn-service: no
port-profile role: none port-binding: static
```

Creating a VMKernel on the Host

Procedure

Step 1 Log in to the vCenter Server.

Step 2 Choose **Home > Inventory > Hosts and Clusters**.

Step 3 Choose the host.

Step 4 Click the **Configuration** tab.

Step 5 In the Hardware pane, choose **Networking**.

Step 6 Click the **vSphere Distributed Switch** button.

Step 7 Go to **Manage Virtual Adapters**.

Step 8 Add and create a new VMKernel.

Note The management vmkernel can also be used as a Layer 3 control interface. For ESX-Visor hosts only. Migrate your management vmkernel interface into the Layer 3 capable port profile. Do not use multiple vmkernel interfaes on the same subnet.

Step 9 Assign the VMkernel to the port profile created in Creating a Port Profile with Layer 3 Control Capability, on page 126.

Step 10 Assign an IP address.

Configuring the SVS Domain in the VSM

Before You Begin

The control0 or mgmt0 interface can be assigned as the Layer 3 control interface.

Procedure

Step 1 Disconnect the VSM to vCenter Server connection.

```
switch# configure terminal
switch(config)# svs connection toVC
switch(config-svs-conn)# no connect
switch(config-svs-conn)# exit
```

Step 2 Remove the control and the packet VLAN configuration.

```
switch(config)# svs-domain
switch(config-svs-domain)# no control vlan
switch(config-svs-domain)# no packet vlan
```

Step 3 Change the svs mode from Layer 2 to Layer 3 with the mgmt0 interface as the Layer 3 control interface.

```
switch(config-svs-domain)# svs mode l3 interface mgmt0
switch(config-svs-domain)# exit
```

Note If the control0 interface is being used as the Layer 3 control interface, enter the **svs mode l3 interface control0** command:

Step 4 Restore the VSM to vCenter Server connection.

```
switch(config)# svs connection toVC
switch(config-svs-conn)# connect
switch(config-svs-conn)# end
```

Note After entering the **svs connection toVC** command, the module is detached and reattached in Layer 3 mode. If this delay is more than six seconds, a module flap occurs. This does not affect the data traffic.

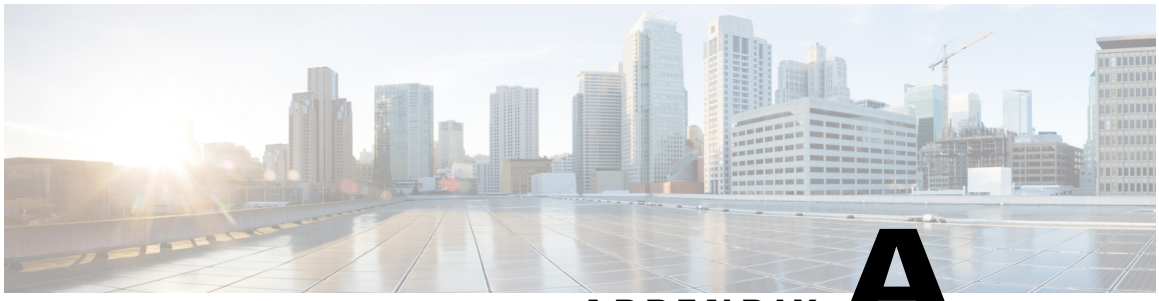
Step 5 Display the SVS domain configuration.

```
switch# show svs domain
SVS domain config:
  Domain id:    3185
  Control vlan: 1
  Packet vlan:  1
  L2/L3 Control mode: L3
  L3 control interface: mgmt0
  Status: Config push to VC successful.
```

Feature History for Upgrading the Cisco Nexus 1000V

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

Feature Name	Releases	Feature Information
Combined Upgrade	4.2(1)SV1(5.2)	The ability to perform a simultaneous upgrade of the VEM and ESXi host.
Upgrading the Cisco Nexus 1000V	4.0(4)SV1(2)	Introduced in this release.



APPENDIX A

Installing and Upgrading VMware

This chapter includes the following sections:

VMware Release 4.0 to VMware Release 4.1 Upgrade

Upgrading from VMware Release 4.0 to VMware Release 4.1

The steps to upgrade from VMware Release 4.0 to VMWare Release 4.1 are as follows:

Before You Begin

- Download the upgrade ZIP bundle to a local desktop or vCenter Server.
  - For ESX, download upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip
  - For ESXi, download upgrade-from-ESXi4.0-to-4.1.0-0.0.260247-release.zip
  - For Cisco Nexus 1000V, download the bundle from www.cisco.com (VEM-4.1.0-GA-v120.zip)
- See the *Cisco Nexus 1000V and VMware Compatibility Information* to determine the correct VIB version, VEM bundle, host build, vCenter Server, and Update Manager versions.

Procedure

Step 1 Upgrading the vCenter Server to VMware Release 4.1, on page 130
Step 2 Upgrading the vCenter Update Manager to VMware Release 4.1, on page 131
Step 3 Upgrading the ESX/ESXi Hosts to VMware Release 4.1, on page 132
Step 4 Verifying the Upgrade to Release 4.1, on page 135

Upgrading the vCenter Server to VMware Release 4.1

This upgrade procedure also applies to vCenter Server 4.1 Update 1 and later.

Procedure

Step 1 Navigate to the `VMware-vpx-all-4.1.0-258902` folder.
Step 2 Double-click **autorun**.

The **VMware vCenter Installer** wizard opens.

Step 3 In the **VMware Product Installers** area, click **vCenter Server**.

Step 4 Choose a language and click **OK.**.

Step 5 Click **Next.**

Step 6 In the **Patent Agreement** window, click **Next**.

Step 7 In the **License Agreement** screen, click the **I agree to the terms in the license agreement** radio button and click **Next.**

Step 8 In the Database Options window, click **Next.**

Step 9 Click the **Upgrade existing vCenter Server database radio button and check the I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\.** check box.

Step 10 From the **Windows Start Menu**, click **Run.**

Step 11 Enter the name of the folder that contains the vCenter Server database and click **OK**.

Step 12 Drag a copy of the parent folder (SSL) to your Desktop as a backup.

Step 13 Return to the installer program and click **Next**.

Step 14 In the **vCenter Agent Upgrade** screen, click the **Automatic** radio button and click **Next**.

Step 15 In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box and click **Next**.

Step 16 In the **Configure Ports** screen, review the port settings and click **Next**.

Step 17 Based on the number of hosts, in the **vCenter Server JVM Memory** screen click the appropriate **memory** radio button and click **Next**.

Step 18 In the **Ready to Install the Program** screen, click **Install.**

Step 19 In the **Installation Completed** screen, click **Finish.**

Step 20 Upgrade the VMware vSphere Client to ESXi 4.1.0.

Step 21 Open the VMware vSphere Client.

Step 22 From the **Help** menu, choose **About VMware vSphere**.

Step 23 Confirm that the vSphere Client and the VMware vCenter Server are both version 4.1.0, Build 258902, click **OK**, and exit the VMware vSphere Client.

What to Do Next

Complete the steps in Upgrading the vCenter Update Manager to VMware Release 4.1, on page 131.

Upgrading the vCenter Update Manager to VMware Release 4.1

This upgrade procedure also applies to vCenter Update Manager 4.1 Update 1 and later.

Procedure

Step 1 Copy the VUM bundle to your local drive.
Step 2 On the local drive, double-click **VMware-UpdateManager**.
Step 3 Choose a language and click **OK**.
Step 4 In the **VMWare vCenter Update Manager**, click **OK** to upgrade to 4.1.0.
Step 5 In the **Welcome** screen, click **Next.**
Step 6 In the **Patent Agreement** screen, click **Next**.
Step 7 Click the **I agree to the terms in the license agreement** radio button and click **Next**.
Step 8 In the **VMware vCenter Server Information** area, verify your IP address and username.
Step 9 In the **Password** field, enter your password and click **Next**.
Step 10 In the **Database Information** screen, click **Next.**
Step 11 In the **Database Upgrade** screen, click the **Yes, I want to upgrade my Update Manager database** radio button and click **Next**.
Step 12 Verify the Update Manager port settings and click **Next**.
Step 13 Verify the Proxy Settings and click **Next**.
Step 14 Click **Install** to begin the upgrade.
Step 15 Click **OK** to acknowledge that a reboot is required to complete the setup.
During the upgrade, the vSphere Client is disconnected.
Step 16 Click **Cancel** for the attempt to reconnect.
Step 17 Click **OK** in the **Server Connection Invalid** dialog box.
Step 18 Click **Finish.**
Step 19 Reboot the local PC.
Step 20 From the **Option** drop-down list, choose **Other (Planned)**.
Step 21 Enter an appropriate value in the comment field and click **OK**.
Step 22 After the system has rebooted, browse to the `C:\ProgramData\VMware\VMware Update Manager\Logs\` folder.
Step 23 Open the `vmware-vum-server-log4cpp` file.
Step 24 Verify the Update Manager version in the log files by searching for the Update Manager build number of 256596.
Step 25 From the VMware vCenter Server's **Plug-in** menu, choose Manage Plug-ins.
Step 26 Under Available Plug-ins, click Download and Install for VMware vSphere Update Manager Extension.

What to Do Next

Complete the steps in Upgrading the ESX/ESXi Hosts to VMware Release 4.1, on page 132.

Upgrading the ESX/ESXi Hosts to VMware Release 4.1

This upgrade procedure also applies to ESX/ESXi hosts 4.1 Update 1 and later.

Procedure

Step 1 In the vSphere Client, click **Home**.

Step 2 Click the **Update Manager** tab.

Step 3 Click the **Host Upgrade Release** tab.

Step 4 In the **Imported Upgrade Releases** area, click **Import Upgrade Release**.

Step 5 In the **Select Upgrade FIles** screen, click **Browse** and navigate to the location of the upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip Zip bundle.

Step 6 Choose the `Zip` file and click **Open.**

Step 7 In the **Select Upgrade Files** screen, click **Next**.
If you receive a Security Warning about the certificate, you can install the certificate or ignore the warning. Go to Step 8 if you must install a certificate. If you do not need to install a certificate, go to Step 9.

Step 8 Click **Finish** when the upload is successful.

Step 9 In the **Host Upgrade Releases** tab, click **Create Baseline** to create a baseline.
When you create a baseline and attach it to a host or cluster, the Update Manager can remediate the device by applying all updates needed to bring it into compliance with the baseline.

Step 10 In the **Baseline Name and Description** area, enter a Name.

Step 11 In the **Baseline Type** area, click the **Host Upgrade** radio button and click **Next.**

Step 12 Click the **Host Upgrade Release** and click **Next.**.

Step 13 Click **Next.**

Step 14 Check the **Try to reboot the host and roll back the upgrade in case of failure** check box

Step 15 In the **COS VMDK Location** screen, click **Next.**

Step 16 Review the upgrade information and click **Finish.**

The baseline has been created.

Step 17 Click **Home**.

Step 18 Click the **Host and Cluster Inventory** tab.

Step 19 Click the **Cluster** icon to upgrade all hosts in the cluster.

Step 20 Click the **Update Manager** tab.

Step 21 In the **Cluster** area, click **Attach.**

Step 22 In the **Individual Baselines by Type** pane, check the **4.0 to 4.1** check box.

Step 23 Click **Attach.**

Step 24 In the **Cluster** area, click **Scan** to test the cluster's compliance to the baseline.

Step 25 In the **Confirm Scan** window, check the **Upgrades** check box.

Step 26 Uncheck the **Patches and Extensions** check box.

Step 27 Click **Scan.**

Step 28 In the **Host Compliance** pane, verify that all hosts are Non-Compliant and click **Remediate**.

Step 29 In the **Remediation Selection** screen, click **Next.**

Step 30 Click the **I agree to the term in the license agreement** radio button and click **Next.**

Step 31 In the **ESX 4.1.0 Upgrade** window, click **Next.**

Step 32 In the **Maintenance Mode Options** area, check the **Disable any removable media devices connected to the virtual machines on the host** check box and click **Next.**

Step 33 In the **Cluster Remediation Options** screen, check all check boxes and click **Next**.

Step 34 Click **Finish** to begin the remediation.

Note You can monitor the remediation progress in the **Recent Tasks** section of the **vSphere Server** window.

Step 35 In the **Confirming Host ESX/ESXi Release** window, click each host in the left-hand pane to check the host versions and confirm that 4.1.0, 260247 appears in the top-left corner of the right-hand pane.

Step 36 Determine upgrade completion as follows:

a) If all hosts have been upgraded, the upgrade is complete.

b) If any one of the hosts was not upgraded, perform Step 42 through Step 61 for each host that requires an upgrade.

Step 37 Right-click the host's IP address and choose **Enter Maintenance Mode**.

Step 38 In the **Confirm Maintenance Mode** dialog box, click **Yes**.

The host's VMs are migrated.

Step 39 Click the **Update Manager** tab.

Step 40 In the **Attached Baselines** section, right-click the **4.0 to 4.1** baseline.

Step 41 In the drop-down list, choose **Detach Baseline**.

Step 42 In the **Detach Baseline from Cluster** window, check the **Cluster** check box and click **Detach.**

Step 43 In the **Update Manager - Attach Baseline** window, click **Attach** to attach the baseline to the host that did not upgrade.

Step 44 In the **Individual Baselines by Type** pane, check the **4.0 to 4.1** check box and click **Attach.**

Step 45 In the **Host Compliance** pane, verify that all hosts are Non-Compliant and click **Remediate**.

Step 46 In the **Remediation Selection** pane, click **Next.**

Step 47 Click the **I agree to the term in the license agreement** radio button.

Step 48 Click **Next.**

Step 49 In the **ESX 4.1.0 Upgrade** window, click **Next.**

Step 50 In the **Maintenance Mode Options** area, check the **Disable any removable media devices connected to the virtual machines on the host** check box.

Step 51 Click **Next.**

Step 52 In the **Cluster Remediation Options** screen, check all check boxes.

Step 53 Click **Next.**

Step 54 In the **Ready to Complete** screen, click **Finish** to begin the remediation.

Step 55 When the remediation is complete, confirm that the host is compliant in the Host Compliance section.

Step 56 In the left-hand pane of the **Exit Maintenance Mode** window, right-click on the host and choose **Exit Maintenance Mode**.

Step 57 In the left-hand pane of the **Select Cluster** window, choose **Cluster** to scan the entire cluster for compliance.

Step 58 Detach the baseline from the host and attach it to the cluster.

Note You can also be confirm the upgrade by entering the show module command on the VSM and check that the VEMs are on the correct build.

The upgrade is complete.

What to Do Next

Complete the steps in Verifying the Upgrade to Release 4.1, on page 135.

Verifying the Upgrade to Release 4.1

Procedure

Step 1 Verify the build number on the ESX host by entering the following command:

```
[root@hostname~] # rpm -qa | grep vmkernel | awk -F. '{print $5}'
260247
```

Step 2 Verify the build number on the ESXi host by entering the following command:

```
~ # vmware –v
VMware ESXi 4.1.0 build-260247
```

Step 3 Verify the upgrade on the Cisco Nexus 1000V by entering the following commands.
`switch#` **show module**

a) Enter the following command on the VSM:
`switch#` **show module**

b) Enter the following commands on the VEM:
`~ #` **vem status**

`~ #` **vemcmd show card**

VMware Release 4.0/4.1/5.0 to VMware Release 5.1 Upgrade

Upgrading from VMware Releases 4.0/4.1/5.0 to VMware Release 5.1

The steps to upgrade from VMware Releases 4.0/4.1/5.0 to VMWare Release 5.1 are as follows:

Procedure

Step 1 Upgrading the vCenter Server to Release 5.1, on page 105
Step 2 Upgrading the vCenter Update Manager to Release 5.1, on page 138
Step 3 Augmenting the Customized ISO for VMware Release 5.1, on page 139
Step 4 Upgrading the ESXi Hosts to Release 5.1, on page 139
Step 5 Verifying the Build Number and Upgrade, on page 141

Upgrading the vCenter Server to Release 5.1

Note This upgrade procedure also applies to vCenter Server 5.0 and vCenter Server 5.0 Update 1 and later.

Before You Begin

- Download the upgrade ISO file that contains the ESXi 5.1 bits and the Cisco Nexus 1000V Release 4.2(1)SV1(5.2) bits.
- See the *Cisco Nexus 1000V and VMware Compatibility Information* document to determine the correct VIB Version, VEM Bundle, Host Build, vCenter Server, and Update Manager versions.

Procedure

Step 1 Navigate to the VMware vSphere 5.1 installation file.

Note If you have the ISO image, you should mount it on the host.

Step 2 Double-click **autorun.**

Step 3 In the **VMware vCenter Installer** window, click **vCenter Server**.

Step 4 Click **Install**.

Step 5 Choose a language and click **OK.**

Step 6 Click **Next.**

Step 7 In the Patent Agreement window, click **Next.**

Step 8 In the **License Agreement** window, click the **I agree to the terms in the license agreement** radio button.

Step 9 Click **Next.**

Step 10 In the **Database Options** screen, click **Next.**

Step 11 Click the **Upgrade existing vCenter Server database** radio button and check the **I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\.** check box.

Step 12 From the **Windows Start** Menu, click **Run.**

Step 13 Enter the name of the folder that contains the vCenter Server database and click **OK.**

Step 14 Drag a copy of the parent folder (SSL) to the desktop as a backup.

Step 15 Return to the installer program.

Step 16 Click **Next.**

Step 17 In the vCenter Agent Upgrade window, click the **Automatic** radio button.

Step 18 Click **Next.**

Step 19 In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box.

Step 20 Click **Next.**

Step 21 Review the port settings and click **Next.**

Step 22 In the **vCenter Server JVM Memory** screen based on the number of hosts, click the appropriate memory radio button.

Step 23 Click **Next.**

Step 24 Click **Install.**

Step 25 Click **Finish.**
This step completes the upgrade of the vCenter Server.

Step 26 Upgrade the VMware vSphere Client to ESXi 5.1.

Step 27 Open the VMware vSphere Client.

Step 28 From the **Help** menu, choose **About VMware vSphere**.

Step 29 Confirm that the vSphere Client and the VMware vCenter Server are both version VMware 5.1.

Step 30 Click **OK**, and exit the VMware vSphere Client.

What to Do Next

Complete the steps in Upgrading the vCenter Update Manager to Release 5.1, on page 138.

Upgrading the vCenter Update Manager to Release 5.1

Note This upgrade procedure also applies to vCenter Update Manager 5.0 and vCenter Update Manager 5.0 Update 1 and later.

Before You Begin

You have upgraded the vCenter Server to VMware ESXi 5.1.

Procedure

Step 1 On the local drive, double-click **VMware-UpdateManager**.

Step 2 Choose a language and click **OK.**
The Update Manager Installer opens.

Step 3 Click **OK** to upgrade to 5.1.

Step 4 Click **Next** to begin.

Step 5 Click **Next** at the Patent Agreement.

Step 6 Click the **I agree to the terms in the license agreement** radio button.

Step 7 Click **Next.**

Step 8 In the **VMware vCenter Server Information** area, verify the IP address and username.

Step 9 In the **Password** field, enter your password.

Step 10 Click **Next.**

Step 11 Click **Next.**

Step 12 Click the **Yes, I want to upgrade my Update Manager database** radio button.

Step 13 Click **Next.**

Step 14 Verify the Update Manager port settings.

Step 15 Click **Next.**

Step 16 Verify the proxy settings.

Step 17 Click **Next.**

Step 18 Click **Install** to begin the upgrade.

Step 19 Click **OK** to acknowledge that a reboot will be required to complete the setup.

During the upgrade, the vSphere Client is disconnected.

Step 20 Click **Cancel** for the attempt to reconnect.

Step 21 Click **OK** in the **Server Connection Invalid** dialog box.

Step 22 Click **Finish.**

Step 23 Reboot the VUM/vCenter Server.

Step 24 In the **Shut Down Windows** dialog box from the **Option** drop-down list, choose **Other (Planned)**, enter a value in the **comment** field, and click **OK.**

Step 25 After the system has rebooted, browse to the `C:\ProgramData\VMware\VMware Update Manager\Logs\` folder.

Step 26 Open the `vmware-vum-server-log4cpp` file.

Step 27 From the **VMware vCenter Server's Plug-in** menu, choose **Manage Plug-ins**.

Step 28 Under **Available Plug-ins**, click **Download and Install** for VMware vSphere Update Manager Extension.

What to Do Next

Complete the steps in Augmenting the Customized ISO for VMware Release 5.1, on page 139.

Augmenting the Customized ISO for VMware Release 5.1

Before You Begin

If you are using a QLogic NIC, download the driver to include in the customized ISO for that specific NIC.

Procedure

If the ESXi host that is being upgraded to VMware 5.1 needs any Async drivers that are not already in VMware 5.1, see the respective vendor's documentation for the drivers and the procedure to update the customized ISO.

What to Do Next

Complete the steps in Upgrading the ESXi Hosts to Release 5.1, on page 139.

Upgrading the ESXi Hosts to Release 5.1

Note

- This upgrade procedure also applies to ESXi hosts 5.0 and 5.0 Update 1 and later.
- If you have multiple vmkernel interfaces on the same subnet when upgrading to ESXi 5.1, you must place your management vmkernel interface into the Layer 3 capable port profile.

Procedure

Step 1 In the vSphere Client, click **Home**.

Step 2 Click the **Update Manager** tab.

Step 3 Click the **ESXi Image** tab.

Step 4 Click the **Import ESXi Image** link in the **ESXi Image** window.

Step 5 Click the **Browse** button and navigate to the customized upgrade ISO image.

Step 6 Choose the upgrade file and click **Open.**

Step 7 To import the ISO file, click **Next**.

Step 8 When the upgrade ISO file is uploaded, click **Next**.

Step 9 In the **Baseline Name and Description** area, enter a name for the baseline and an optional description.

Step 10 Click **Finish.**

Step 11 In the vSphere Client, choose **Home** > **Hosts and Clusters**.

Step 12 In the **left-hand** pane, select the host or cluster to upgrade and click the **Update Manager** tab.

Step 13 Click **Attach.**

Step 14 In the **Individual Baselines by Type** area, check your upgrade baseline's check box.

Step 15 Click **Attach.**

Step 16 Click **Scan.**
After the scan, the baseline will display non-compliant.

Step 17 In the **Confirm Scan** dialog box, check the **Upgrades** check box and click **Scan.**

Step 18 In the **Upgrade Details** window, if the Compliance State has a value of Incompatible, reboot the host with the baseline attached.

After the reboot, the Compliance State will have a value of Non-Compliant.

Step 19 When you are finished viewing the upgrade details, click **Close**.

Step 20 Verify that all hosts are Non-Compliant.

Step 21 Click **Remediate**.

Step 22 Click **Next**

Step 23 In the **End User License Agreement** screen, check the **I accept the terms and license agreement** check box.

Step 24 Click **Next**

Step 25 In the **ESXi 5.x Upgrade** window, click **Next**.

Step 26 Click **Next**.

Step 27 In the **Maintenance Mode Options** area, check the **Disable any removable media devices connected to the virtual machines on the host** check box.

Step 28 Click **Next**.

Step 29 In the **Cluster Remediation Options** window, check all check boxes.

Step 30 Click **Next**.

Step 31 Click **Finish** to begin the remediation.

Step 32 To check the host versions, click each host in the left-hand pane and confirm that 5.1 appears in the top-left corner of the right-hand pane and that the version information matches the contents of the *Cisco Nexus 1000V and VMware Compatibility Information*.

Step 33 The upgrade can also be confirmed by running the **show module** command on the VSM and observing that the VEMs are on the correct build.

The upgrade is complete.

What to Do Next

Complete the steps in Verifying the Build Number and Upgrade, on page 141.

Verifying the Build Number and Upgrade

Before You Begin

- You have upgraded the VSMs and VEMs to the current Cisco Nexus 1000V release.
- You have upgraded the vCenter Server to VMware Release 5.0.0.
- You have upgraded the VMware Update Manager to VMware Release 5.0.0.
- You have upgraded your ESX/ESXi hosts to VMware Release 5.0.0.

Procedure

Step 1 Verify the build number on the ESXi host.

```
~ # vmware -v
VMware ESXi 5.0.0 build-469512
```

Step 2 Verify the upgrade on the Cisco Nexus 1000V.

```
switch# show module

N1KV-VSM# show mod
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    0      Virtual Supervisor Module        Nexus1000V         active *
2    0      Virtual Supervisor Module        Nexus1000V         ha-standby
3    248    Virtual Ethernet Module          NA                 ok
Mod  Sw               Hw
---  ---------------  ------
1    4.2(1)SV2(2.1)   0.0
2    4.2(1)SV2(2.1)   0.0
3    4.2(1)SV2(2.1)   3.0
Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-09-00 to 02-00-0c-00-09-80  NA
Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.245.152   NA                                    NA
2    10.104.245.152   NA                                    NA
3    10.104.245.140   42064d20-4e52-62d1-e0ee-0b14be4388d6  mn-esxi-5.0-statefull

* this terminal session
```

The upgrade to VMware Release 5.0 is complete.

Upgrading to VMware ESXi 5.0 Patch 01

Upgrading a VMware ESXi 5.0 Stateful Host to VMware ESXi 5.0 Patch 01

Procedure

Step 1 Copy the ESXi 5.0 Patch 01 bundle (`ESXi500-201109001.zip`) to the host.

Step 2 Upgrade the host to ESXi 5.0 Patch 01.

```
~ # esxcli software vib update -d /vmfs/volumes/newnfs/MN-patch01/ESXi500-201109001.zip
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the
 changes to be effective.
   Reboot Required: true
   VIBs Installed: VMware_bootbank_esx-base_5.0.0-0.3.474610,
VMware_locker_tools-light_5.0.0-0.3.474610
   VIBs Removed: VMware_bootbank_esx-base_5.0.0-0.0.469512,
VMware_locker_tools-light_5.0.0-0.0.469512
   VIBs Skipped: VMware_bootbank_ata-pata-amd_0.3.10-3vmw.500.0.0.469512,
VMware_bootbank_ata-pata-atiixp_0.4.6-3vmw.500.0.0.469512,
```

```
   VMware_bootbank_scsi-qla4xxx_5.01.03.2-3vmw.500.0.0.469512,
VMware_bootbank_uhci-usb-uhci_1.0-3vmw.500.0.0.469512
```

Installing ESXi 5.1 Host Software Using the CLI

You can upgrade an ESXi host by installing a VMware patch or update with the compatible Cisco Nexus 1000V VEM software.

Before You Begin

- If you are using the vCLI, do the following:
  - You have downloaded and installed the VMware vCLI. For information about installing the vCLI, see the VMware vCLI documentation.
  - You are logged in to the remote host when the vCLI is installed.

Note The vSphere Command-Line Interface (vSphere CLI) command set allows you to enter common system administration commands against ESXi systems from any machine with network access to those systems. You can also enter most vSphere CLI commands against a vCenter Server system and target any ESXi system that the vCenter Server system manages. vSphere CLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

- If you are using the **esxupdate** command, you are logged into the ESX host.
- Check the *Cisco Nexus 1000V and VMware Compatibility Information* for compatible versions.
- You have already copied the ESXi host software and VEM software installation file to the `/tmp` directory.
- You know the name of the ESXi and VEM software file to be installed.

Procedure

Step 1 Download the VEM bits and copy them to the local host.

Step 2 Determine the upgrade method that you want to use.

- If you are using the vCLI, enter the **esxcli** command and install the ESXi and VEM software simultaneously.

Note When using the **esxcli software vib install** command, you must log in to each host and enter the command. ESXi 5.1 expects the VIB to be in the `/var/log/vmware` directory if the absolute path is not specified.

esxcli software vib install -v *full-path-to-vib*

This example shows how to install ESXi 5.1 on a host.

```
~ # esxcli software vib install -d /var/log/vmware/VEM500-20120803144112-BG-release.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.2
   VIBs Removed:
   VIBs Skipped:

~ # esxcli software vib install -v
/var/log/vmware/cross_cisco-vem-v144-4.2.1.1.5.2.0-3.0.2.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.2
   VIBs Removed:
   VIBs Skipped:
~ #
```

This command loads the software manually onto the host, loads the kernel modules, and starts the VEM Agent on the running system.

Step 3 Verify that the installation was successful.

```
~ # vmware -v -l
VMware ESXi 5.0.0 build-469512
VMware ESXi 5.0.0 GA
~ #

~ # vemcmd show version
VEM Version: 4.2.1.1.5.2.0-3.0.2
VSM Version: 4.2(1)SV1(5.2)
System Version: VMware ESXi 5.0.0 Releasebuild-469512

~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.1.5.2.0-3.0.2
Build 2
Date Fri Aug 3 05:11:27 PDT 2012

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         24          128               1500    vmnic2
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
switch           256         14          256               1500    vmnic5,vmnic4,vmnic3

Number of PassThru NICs are 0
VEM Agent (vemdpa) is running

~ # esxcli software vib list | grep cisco
cisco-vem-v144-esx   4.2.1.1.5.2.0-3.0.2              Cisco   PartnerSupported  2012-08-21

~ #
```

```
~ # vem version -v
Number of PassThru NICs are 0
Running esx version -469512 x86_64
VEM Version: 4.2.1.1.5.2.0-3.0.2
VSM Version: 4.2(1)SV1(5.2)
System Version: VMware ESXi 5.0.0 Releasebuild-469512
~ #
```

Note If the VEM Agent is not running, see the *Cisco Nexus 1000V Troubleshooting Guide*.

Step 4 Verify that the VEM has been upgraded by entering the following command from the VSM.

```
switch# show module
Mod  Ports  Module-Type                      Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          ha-standby
2    0      Virtual Supervisor Module         Nexus1000V          active *
3    248    Virtual Ethernet Module           NA                  ok
4    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV1(5.2)      0.0
2    4.2(1)SV1(5.2)      0.0
3    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV1(5.2)      VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

Mod  MAC-Address(es)                          Serial-Num
---  --------------------------------------   ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8   NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8   NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80   NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80   NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.249.171   NA                                    NA
2    10.104.249.171   NA                                    NA
3    10.104.249.172   7d41e666-b58a-11e0-bd1d-30e4dbc299c0  10.104.249.172
4    10.104.249.173   17d79824-b593-11e0-bd1d-30e4dbc29a0e  10.104.249.173

* this terminal session
switch#
```

Note The highlighted text in the previous command output confirms that the upgrade was successful.

Step 5 Do one of the following:

- If the installation was successful, you do nothing because the installation procedure is complete.
- If not, see the *Recreating the Cisco Nexus 1000V Installation* section in the *Cisco Nexus 1000V Troubleshooting Guide*.

You have completed this procedure.

Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image

Before You Begin

- Install the VMware PowerCLI on a Windows platform. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform, where the VMware PowerCLI is installed, do one of the following:
  - Download the ESX depot, 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.

Note In the following procedure, the ESX depot is available as `C:\VMware-ESXi-5.0.0-469512-depot.zip` and the VEM bundle is available as `C:\VEM500-20110822140-BG.zip`.

Procedure

Step 1 Start the VMWare PowerCLI application.

Step 2 Connect to the vCenter Server.

```
[vSphere PowerCLI] > Connect-VIServer 192.0.2.1 -User Administrator -Password XXXXX
```

Step 3 Load the ESX depot.

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot c:\vmware-ESXi-5.0.0-depot.zip
```

Step 4 Display the image profiles.

```
[vSphere PowerCLI] > Get-EsxImageProfile
Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.0.0-469512-no-tools     VMware, Inc.    8/19/2011 1:... PartnerSupported
ESXi-5.0.0-469512-standard     VMware, Inc.    8/19/2011 1:... PartnerSupported
```

Step 5 Clone the ESX standard image profile.

Note The image profiles are usually in READ-ONLY format. You must clone the image profile before adding the VEM image to it.

```
[vSphere PowerCLI] > New-ESxImageProfile -CloneProfile ESXi-5.0.0-469512-standard -Name
n1kv-Image
Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
n1kv-Image                     VMware, Inc.    8/19/2011 1:... PartnerSupported
```

Step 6 Load the Cisco Nexus 1000V VEM offline bundle.

```
[vSphere PowerCLI] > Add-EsxSoftwareDepot C:\VEM500-20120121140109-BG-release.zip

Depot Url
---------
zip:C:\Users\Administrator\Documents\VEM500-20120121140109-BG-release.zip?in...
```

Step 7 Confirm that the n1kv-vib package is loaded.

```
[vSphere PowerCLI] > Get-EsxSoftwarePackage -Name cisco*
Name                     Version                        Vendor     Release Date
----                     -------                        ------     ------------
cisco-vem-v140-esx       4.2.1.1.5.1.0-3.0.2            Cisco      1/21/2012...
```

Step 8 Bundle the n1kv-package into the cloned image profile.

```
[vSphere PowerCLI] > Add-EsxSoftwarePackage -ImageProfile n1kv-Image -SoftwarePackage
cisco-vem-v140-esx

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
n1kv-Image                     VMware, Inc.    1/24/2012 5:... PartnerSupported
```

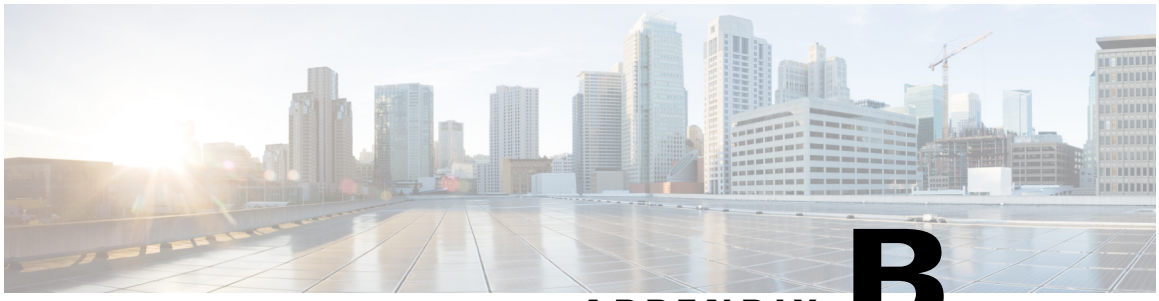
Step 9 Verify that the Cisco VIB is present by listing all the VIBs in the cloned image profile.

```
[vSphere PowerCLI]> $img = Get-EsxImageProfile n1kv-Image
[vSphere PowerCLI]> $img.vibList

Name                     Version                        Vendor     Release Date
----                     -------                        ------     ------------
net-ixgbe                2.0.84.8.2-10vmw.500.0.0.46... VMware     8/19/2011...
ata-pata-hpt3x2n         0.3.4-3vmw.500.0.0.469512      VMware     8/19/2011...
ehci-ehci-hcd            1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-atiixp          0.4.6-3vmw.500.0.0.469512      VMware     8/19/2011...
scsi-megaraid2           2.00.4-9vmw.500.0.0.469512     VMware     8/19/2011...
uhci-usb-uhci            1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
net-r8168                8.013.00-3vmw.500.0.0.469512   VMware     8/19/2011...
ohci-usb-ohci            1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
scsi-qla4xxx             5.01.03.2-3vmw.500.0.0.469512  VMware     8/19/2011...
ata-pata-sil680          0.4.8-3vmw.500.0.0.469512      VMware     8/19/2011...
scsi-megaraid-sas        4.32-1vmw.500.0.0.469512       VMware     8/19/2011...
scsi-aic79xx             3.1-5vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-amd             0.3.10-3vmw.500.0.0.469512     VMware     8/19/2011...
net-bnx2                 2.0.15g.v50.11-5vmw.500.0.0... VMware     8/19/2011...
misc-drivers             5.0.0-0.0.469512               VMware     8/19/2011...
sata-ahci                3.0-6vmw.500.0.0.469512        VMware     8/19/2011...
scsi-fnic                1.5.0.3-1vmw.500.0.0.469512    VMware     8/19/2011...
ata-pata-pdc2027x        1.0-3vmw.500.0.0.469512        VMware     8/19/2011...
scsi-hpsa                5.0.0-17vmw.500.0.0.469512     VMware     8/19/2011...
sata-sata-sil            2.3-3vmw.500.0.0.469512        VMware     8/19/2011...
net-igb                  2.1.11.1-3vmw.500.0.0.469512   VMware     8/19/2011...
net-e1000e               1.1.2-3vmw.500.0.0.469512      VMware     8/19/2011...
net-forcedeth            0.61-2vmw.500.0.0.469512       VMware     8/19/2011...
sata-ata-piix            2.12-4vmw.500.0.0.469512       VMware     8/19/2011...
scsi-qla2xxx             901.k1.1-14vmw.500.0.0.469512  VMware     8/19/2011...
scsi-adp94xx             1.0.8.12-6vmw.500.0.0.469512   VMware     8/19/2011...
net-sky2                 1.20-2vmw.500.0.0.469512       VMware     8/19/2011...
cisco-vem-v140-esx       4.2.1.1.5.1.0-3.0.2            Cisco      1/21/2012...
ipmi-ipmi-msghandler     39.1-4vmw.500.0.0.469512       VMware     8/19/2011...
net-be2net               4.0.88.0-1vmw.500.0.0.469512   VMware     8/19/2011...
esx-base                 5.0.0-0.0.469512               VMware     8/19/2011...
ipmi-ipmi-si-drv         39.1-4vmw.500.0.0.469512       VMware     8/19/2011...
scsi-megaraid-mbox       2.20.5.1-6vmw.500.0.0.469512   VMware     8/19/2011...
net-nx-nic               4.0.557-3vmw.500.0.0.469512    VMware     8/19/2011...
sata-sata-promise        2.12-3vmw.500.0.0.469512       VMware     8/19/2011...
scsi-ips                 7.12.05-4vmw.500.0.0.469512    VMware     8/19/2011...
```

```
scsi-lpfc820              8.2.2.1-18vmw.500.0.0.469512   VMware     8/19/2011...
ata-pata-cmd64x           0.2.5-3vmw.500.0.0.469512      VMware     8/19/2011...
sata-sata-svw             2.3-3vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-via              0.3.3-2vmw.500.0.0.469512      VMware     8/19/2011...
esx-tboot                 5.0.0-0.0.469512               VMware     8/19/2011...
misc-cnic-register        1.1-1vmw.500.0.0.469512        VMware     8/19/2011...
net-s2io                  2.1.4.13427-3vmw.500.0.0.46... VMware     8/19/2011...
net-e1000                 8.0.3.1-2vmw.500.0.0.469512    VMware     8/19/2011...
block-cciss               3.6.14-10vmw.500.0.0.469512    VMware     8/19/2011...
net-enic                  1.4.2.15a-1vmw.500.0.0.469512  VMware     8/19/2011...
net-bnx2x                 1.61.15.v50.1-1vmw.500.0.0.... VMware     8/19/2011...
scsi-mpt2sas              06.00.00.00-5vmw.500.0.0.46... VMware     8/19/2011...
sata-sata-nv              3.5-3vmw.500.0.0.469512        VMware     8/19/2011...
ata-pata-serverworks      0.4.3-3vmw.500.0.0.469512      VMware     8/19/2011...
net-cnic                  1.10.2j.v50.7-2vmw.500.0.0.... VMware     8/19/2011...
scsi-mptsas               4.23.01.00-5vmw.500.0.0.469512 VMware     8/19/2011...
scsi-aacraid              1.1.5.1-9vmw.500.0.0.469512    VMware     8/19/2011...
tools-light               5.0.0-0.0.469512               VMware     8/19/2011...
ima-qla4xxx               2.01.07-1vmw.500.0.0.469512    VMware     8/19/2011...
ipmi-ipmi-devintf         39.1-4vmw.500.0.0.469512       VMware     8/19/2011...
net-tg3                   3.110h.v50.4-4vmw.500.0.0.4... VMware     8/19/2011...
scsi-bnx2i                1.9.1d.v50.1-3vmw.500.0.0.4... VMware     8/19/2011...
net-r8169                 6.011.00-2vmw.500.0.0.469512   VMware     8/19/2011...
scsi-mptspi               4.23.01.00-5vmw.500.0.0.469512 VMware     8/19/2011...
```

Step 10 Export the image profile to an ISO file.

```
[vSphere PowerCLI]>  Export-EsxImageProfile -ImageProfile n1kv-Image -FilePath
C:\n1kv15-esx50.iso –ExportToIso
```



APPENDIX B

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

This chapter includes the following sections:

Installing the VSM Software

Installing the Software from the ISO Image

Before You Begin

- The ISO image is located at *zip_file_location*/`Nexus1000v.4.2.1.SV1.5.2/VSM/Install/nexus-1000v.4.2.1.SV1.5.2.iso`
- You have already read the Prerequisites for Installing the Cisco Nexus 1000V, on page 17.
- You have already manually provisioned the VM to be used for the VSM. For more information, see the *vSphere Virtual Machine Administration Guide*.
- The VSM VM requires the following and this procedure includes steps for updating these properties:
  - Minimum of 2 GB of RAM reserved and allocated.
  - Minimum CPU speed of 1500 MHz.
- Do not create more than one virtual CPU. The Cisco Nexus 1000V supports only one virtual CPU.

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 2 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 2048 MB.

Step 7 In the **Resources** tab, choose CPU.
The Resource Allocation settings display in the right-hand pane.

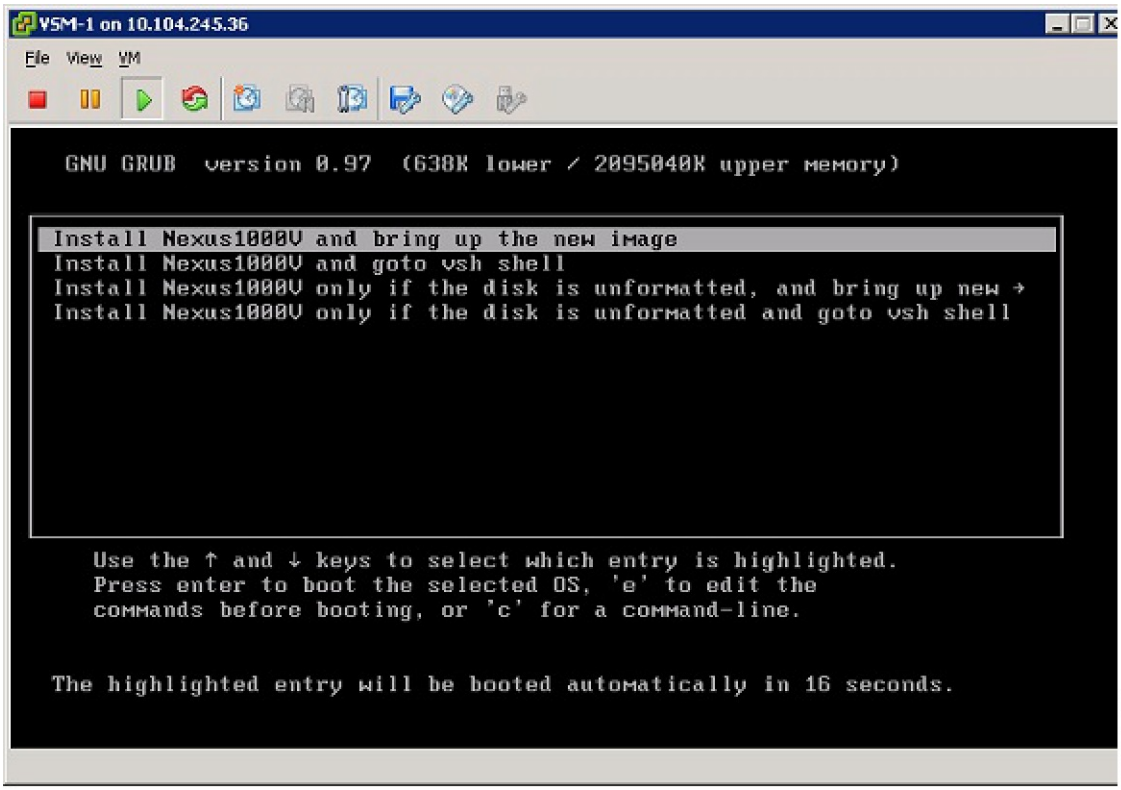
Step 8 In the **Reservation** field, choose 1500 MHz.

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**.

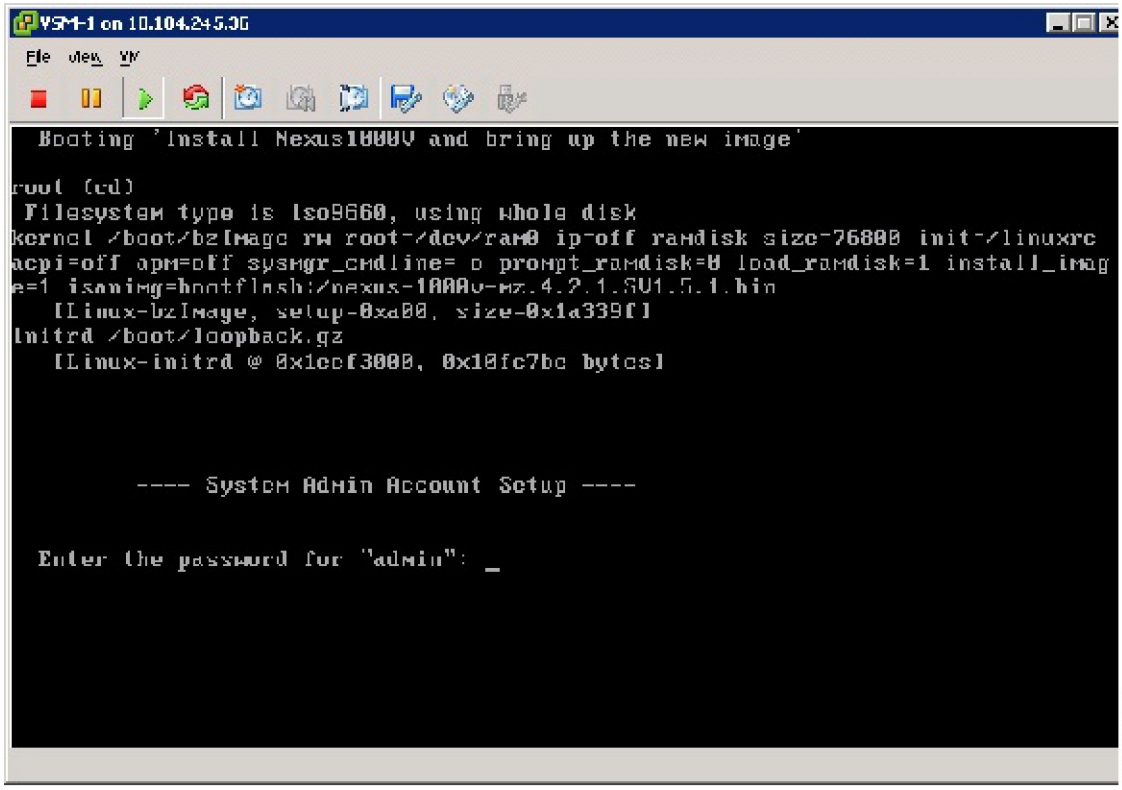
Figure 57: Install Nexus1000V and Bring Up the New Image Window



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: $ \ ?

Figure 58: System Admin Account Setup Window



Step 13 Enter the domain ID.

```
Enter the domain id<1-4095>: 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):


This example shows the HA role as secondary.
Enter HA role[standalone/primary/secondary]: secondary


  Setting HA role to secondary will cause a system reboot. Are you sure (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/standby VSM, when prompted to reboot the VSM, answer yes.
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 show the system rebooting when the HA role is set to secondary.

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

[######################################] 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 4.2(1)SV1(5.2),
Do you want to reconfigure? (yes/no) [n] yes
          Current vem feature level is set to 4.2(1)SV1(5.2)
          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 4.2(1)SV1(5.1) 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 165.

Installing the Software from an OVA Image

Before You Begin

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

- The OVA image is located at *zip_file_location*/`Nexus1000v.4.2.1.SV1.5.2/VSM/Install/nexus-1000v.4.2.1.SV1.5.2.ova`
- You have already read the Prerequisites for Installing the Cisco Nexus 1000V, on page 17.
- 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:

Installation Type	Filename	Used with ESX or ESXi Host Software Version
OVA	`nexus-1000v.4.2.1.SV1.5.2.ova`	4.1 or later

- 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:

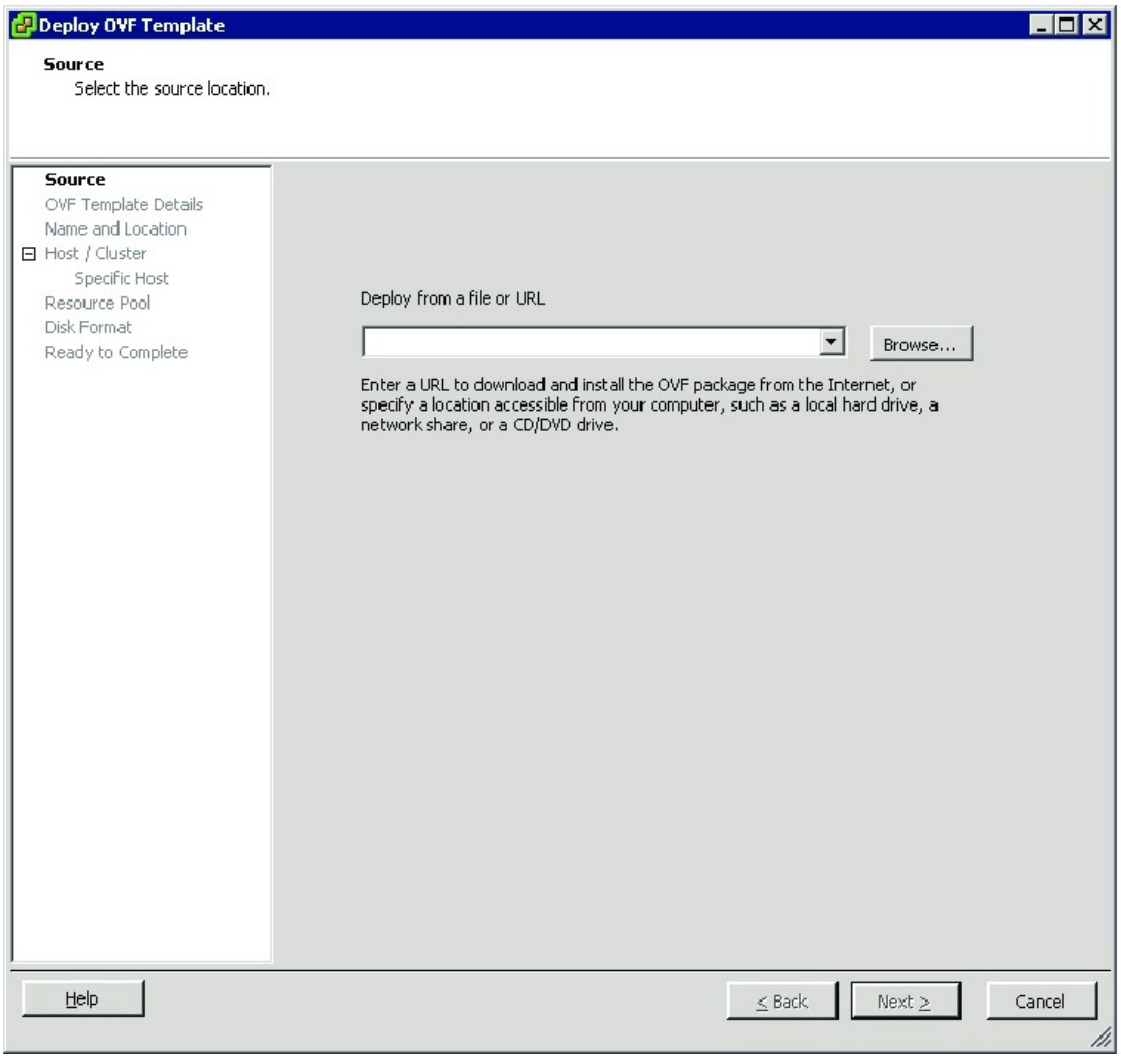
- VSM domain ID
- Admin password
- Management IP address, subnet mask, and gateway

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.**

Figure 59: Source Screen



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

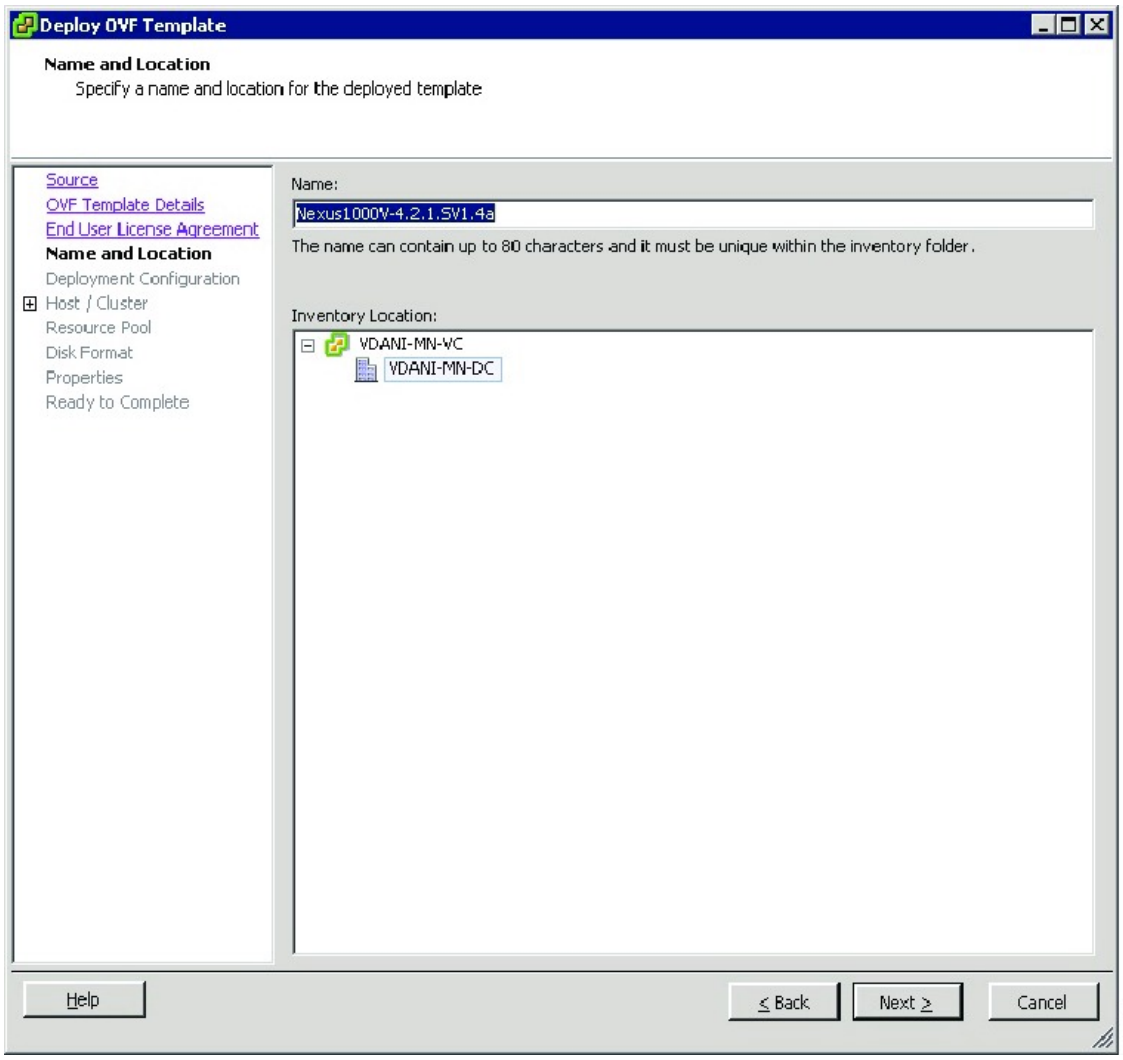
Step 3 Click **Next.**

Step 4 Read the Cisco Nexus 1000V License Agreement.

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

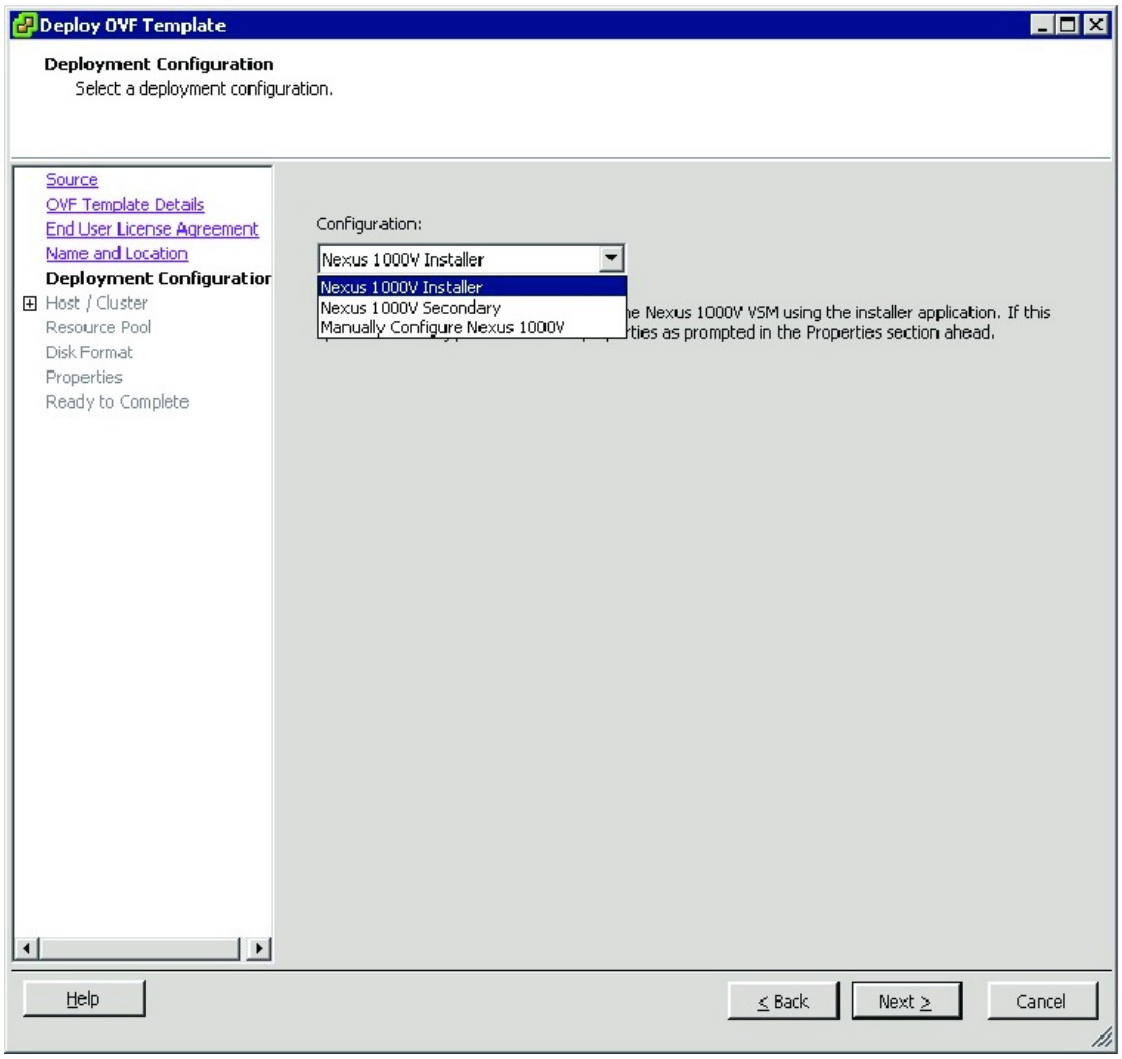
Step 6 Add the VSM name, choose the folder location within the inventory where it will reside, and click **Next.** The name for the VSM must be unique within the inventory folder and less than 80 characters.

Figure 60: Deploy OVF Template Screen



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

Figure 61: Deployment Configuration Screen



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

Step 8 Click **Next**.

Step 9 Choose the data center or cluster on which to install the VSM.

Step 10 Click **Next**

Step 11 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.

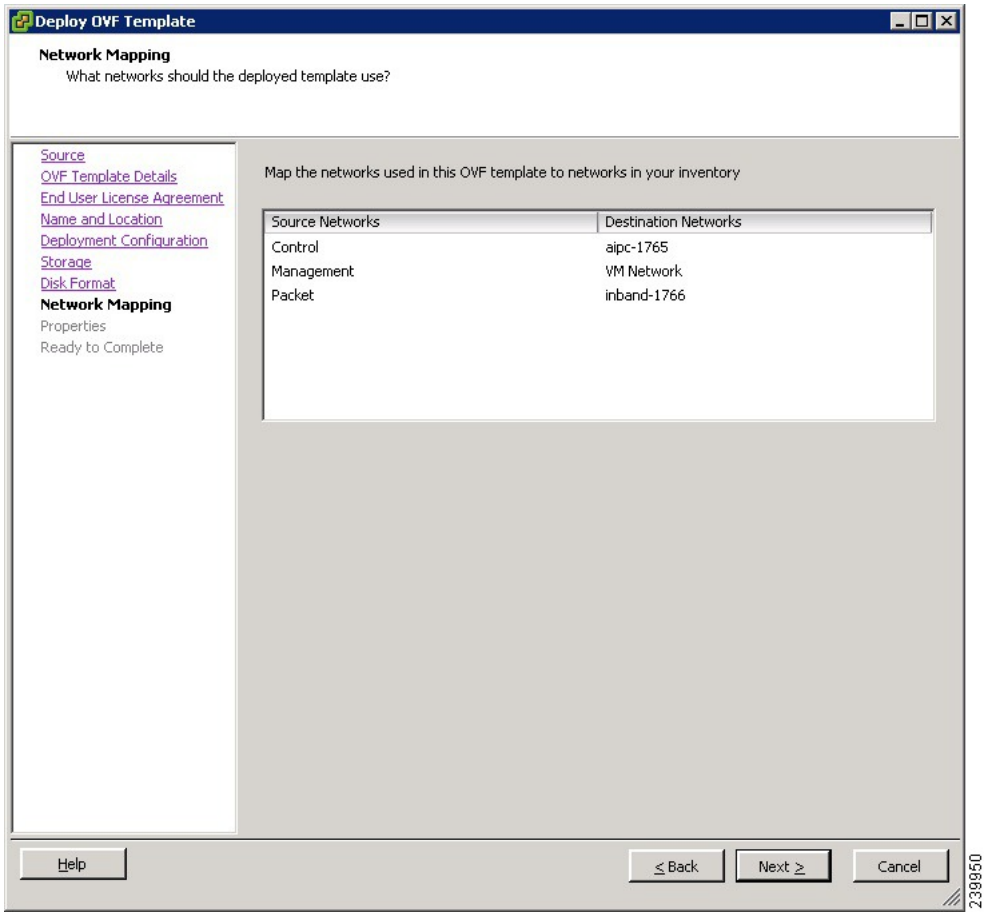
Step 12 Click **Next**

Step 13 Choose the Thick provisioned disk format for storing virtual machine virtual disks, and click **Next.**

Format	Description
Thin Provisioned	The storage is allocated on demand as data is written to the virtual disks. **Note** This disk format is not supported for Cisco Nexus 1000V.
Thick Provisioned	All storage is immediately allocated.
Flat Provisioned	**Note** This format is only available with VMWare ESXi 5.0.
Flat Disk	All storage for the virtual disk is allocated in advance.

Step 14 In the **Network Mapping** screen, choose the networks (the control, management, and packet port groups) that are present in your inventory.

Figure 62: Network Mapping Screen



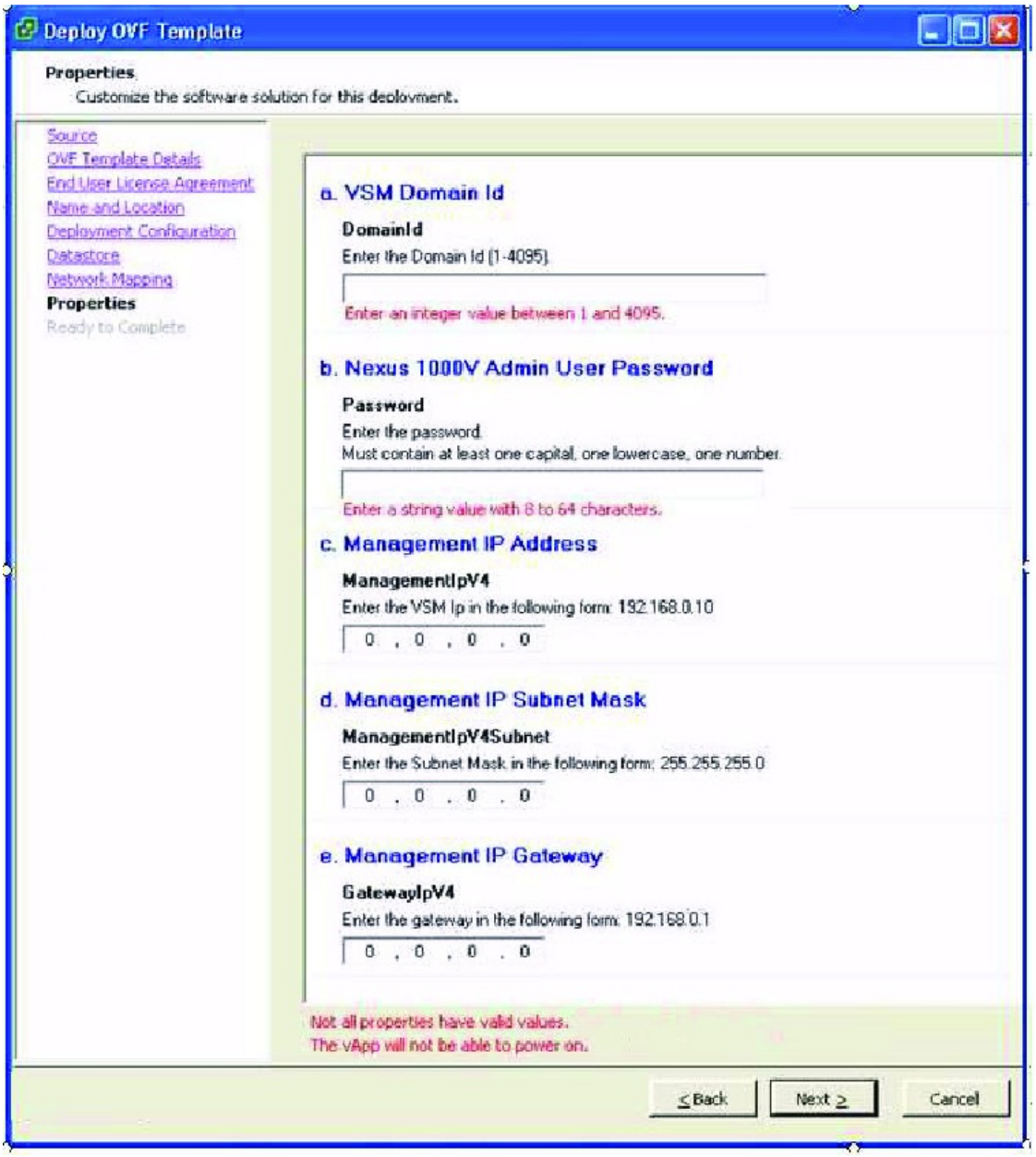
Step 15 Click **Next**

Step 16 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).

Figure 63: Properties Screen

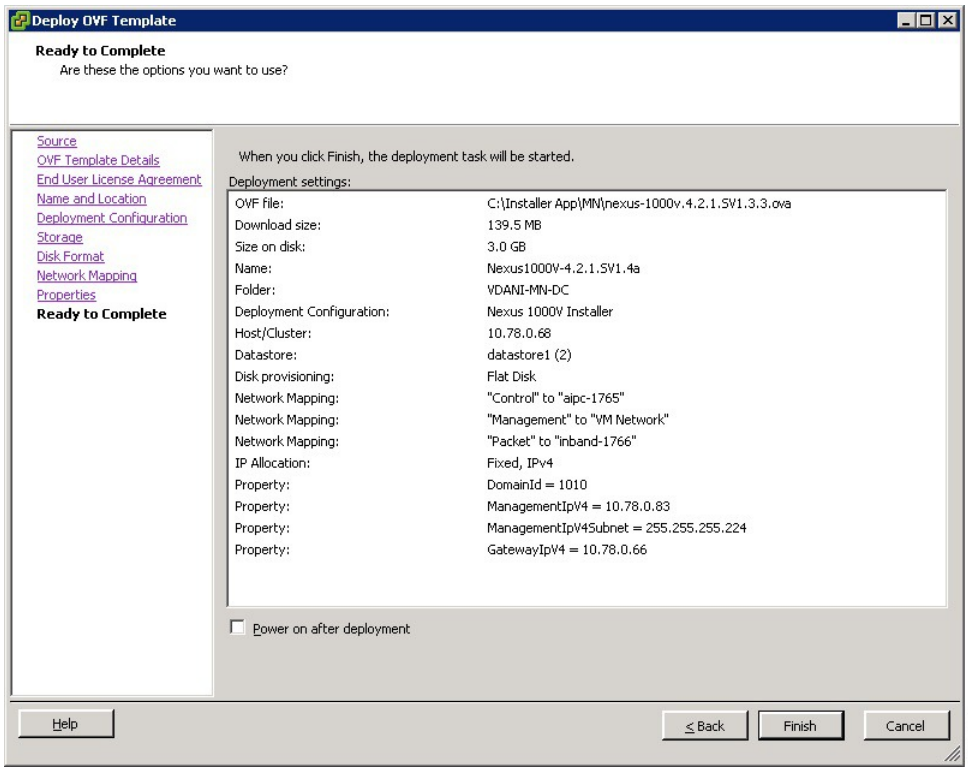


Step 17 Click **Next.**

Step 18 If the configuration is correct, click **Finish**.

A status bar displays as the VM installation progresses.

Figure 64: Ready to Complete Screen



Step 19 Click **Close.**
You have completed installing the Cisco Nexus 1000V software.

Step 20 Right-click the VSM and choose **Open Console**.

Step 21 Click the **green arrow** to power on the VSM.

Step 22 Enter the following commands at the VSM prompt.

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

Step 23 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):
```

This example shows the HA role as secondary.

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


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

Step 24 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 25 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 26 If you are setting up the secondary/standby VSM, when prompted to reboot the VSM, answer yes.
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.

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

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

  HA mode set to secondary. Rebooting now...
```

You have completed this procedure for the secondary VSM.

Step 27 Enter yes to enter the basic configuration dialog.

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

Step 28 Enter no to create another Login account.

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

Step 29 Enter no to configure a read-only SNMP community string.

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

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

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

Step 31 Enter a name for the switch.

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

Step 32 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 33 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 34 Enter no to configure advanced IP options.

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

Step 35 Enter yes to enable the Telnet service.

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

Step 36 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 37 Enter yes to enable the HTTP server.

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

Step 38 Enter no to configure the NTP server.

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

Step 39 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 40 Enter yes to configure the VEM feature level and then enter 0 or 1.

```
Vem feature level will be set to 4.2(1)SV1(5.2),
Do you want to reconfigure? (yes/no) [n] yes
          Current vem feature level is set to 4.2(1)SV1(5.2)
          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 41 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 42 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 43 Create the SVS connection manually or go to Establishing the SVS Connection, on page 165.

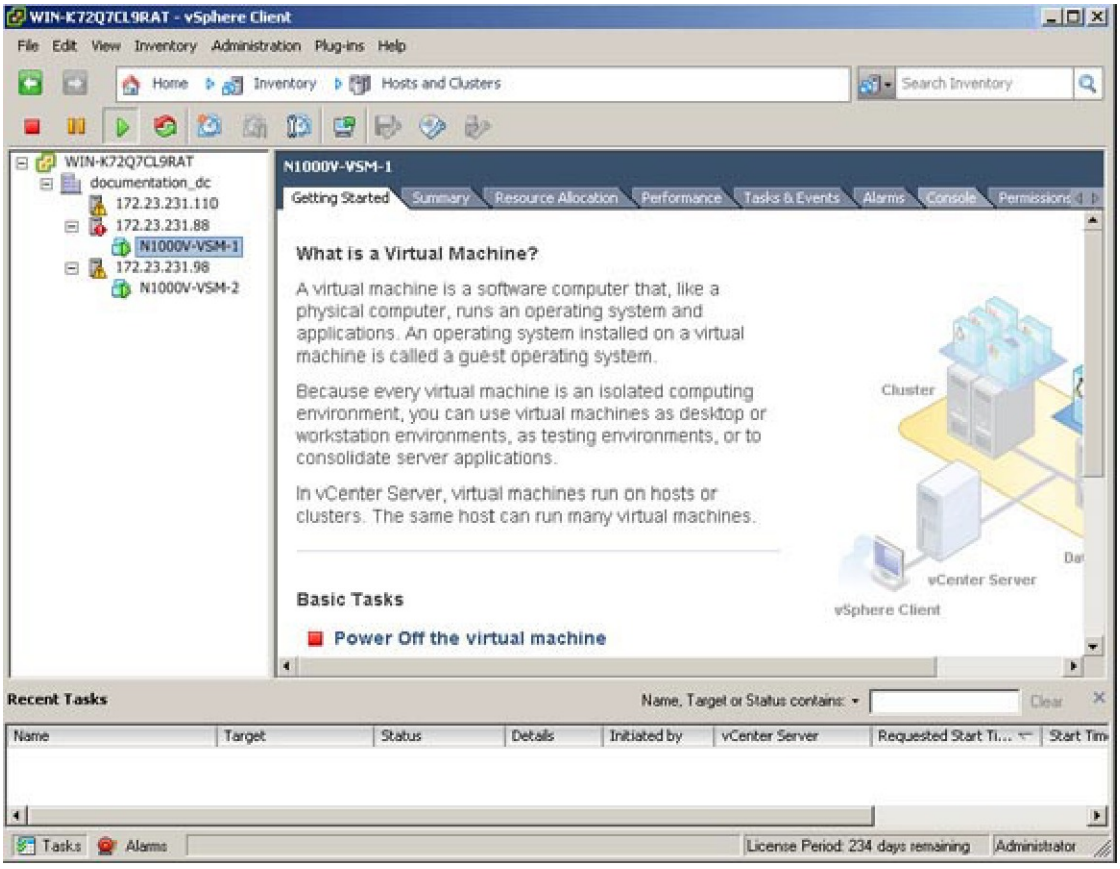
Establishing the SVS Connection

Procedure

Step 1 Open the vSphere Client.

Step 2 Choose the primary VSM.

Figure 65: vSphere Client Window



Step 3 Choose the **Console** tab.

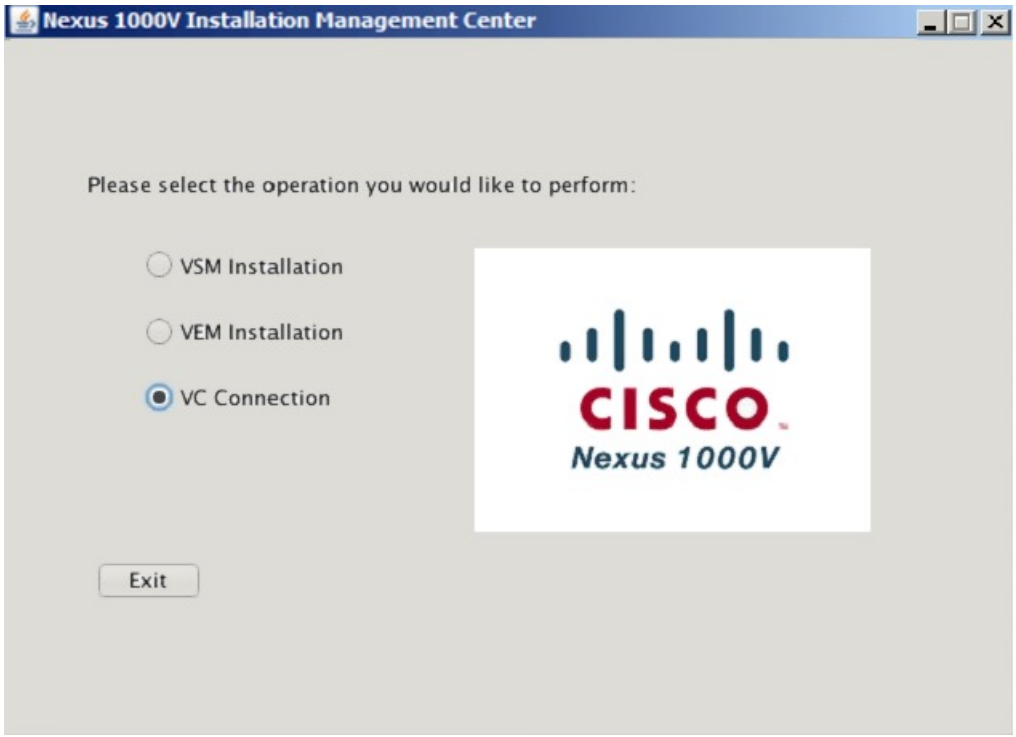
Step 4 Enter the **show svs connections** command to confirm that there is not an SVS connection.

Step 5 Open a command window.

Step 6 Enter the **java -jar Nexus1000V-launchPad.jar** command.

Step 7 In the **Nexus 1000V Installation Management Center** window, click the **VC Connection** radio button.

Figure 66: Nexus 1000V Installation Management Center Window



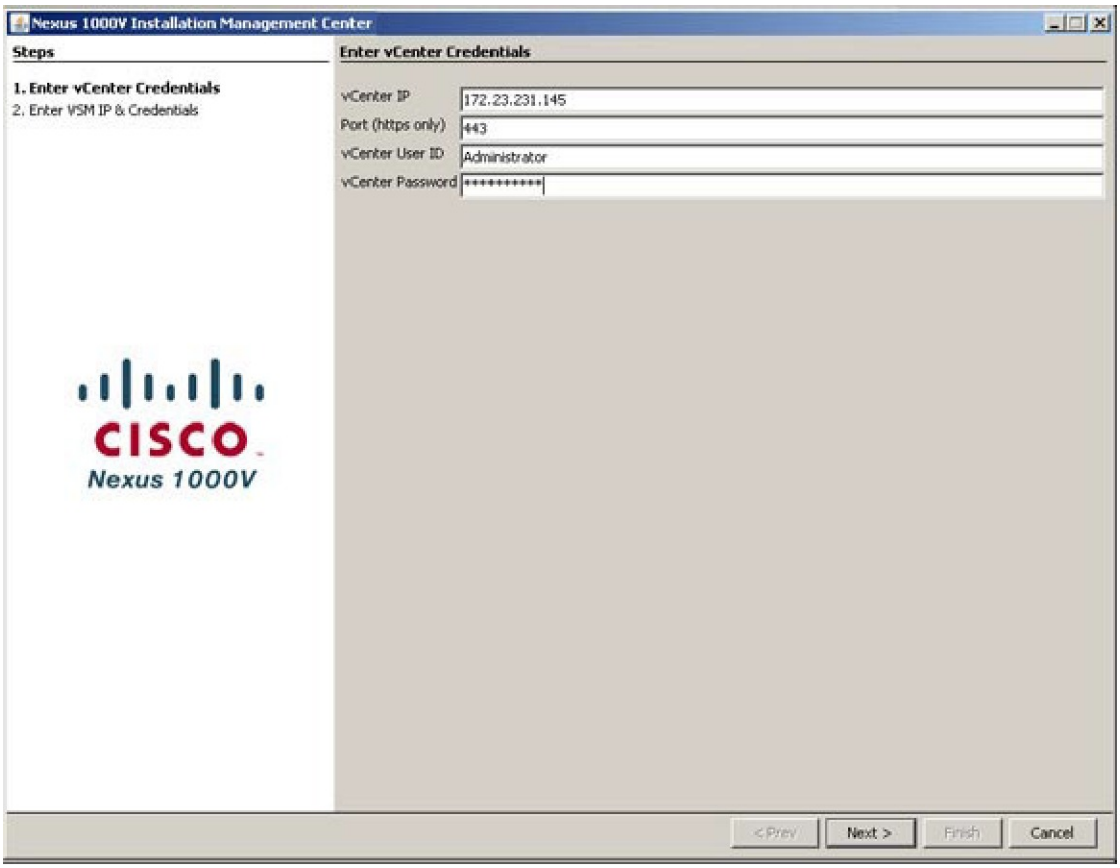
Step 8 Enter the following vCenter credentials:

- vCenter IP address
- Secure HTTP port

  Port 443 is configured by default, but you can change the port if needed.
- vCenter User ID (for a vCenter user with administrator-level privileges)

- vCenter Password (for a vCenter user with administrator-level privileges)

Figure 67: Enter vCenter Credentials Screen



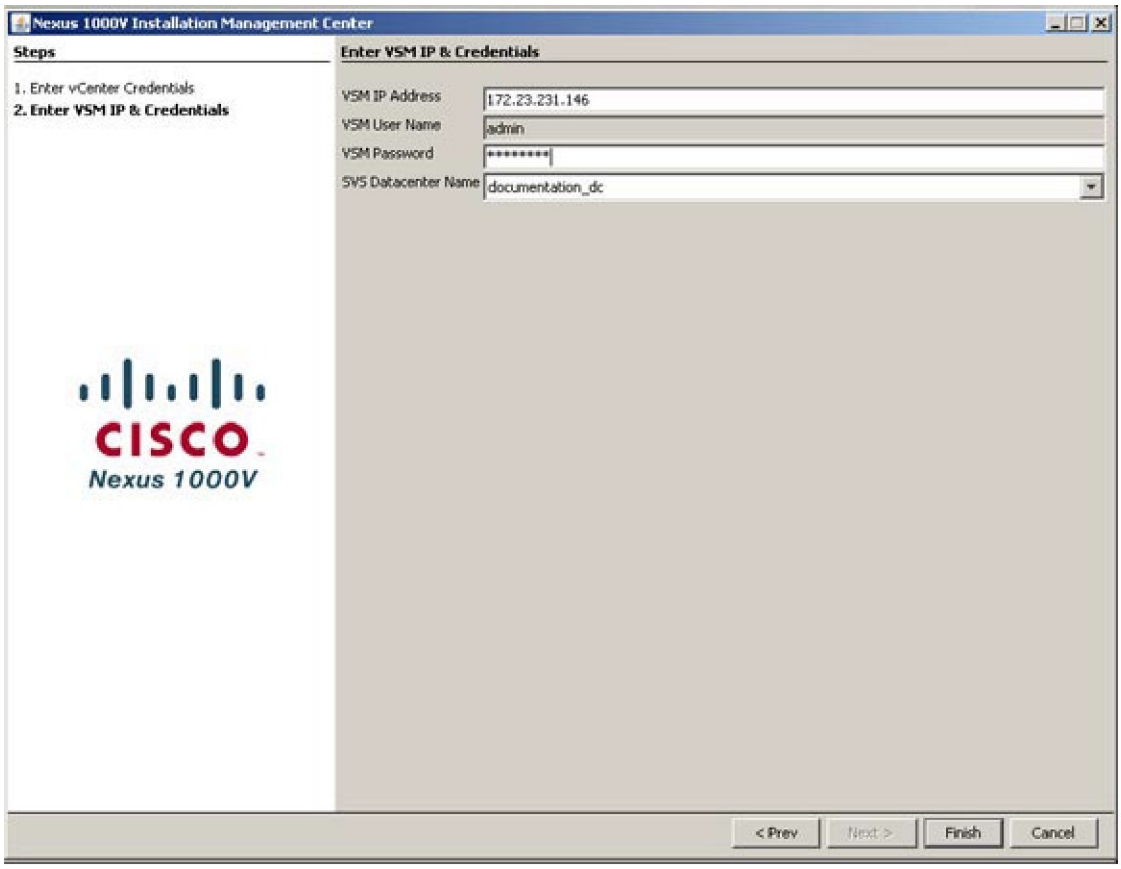
Step 9 Click **Next**.

Step 10 Enter the following VSM credentials:

- VSM IP Address
- VSM Password
- From the **SVS Datacenter Name** drop-down list, choose the data center.

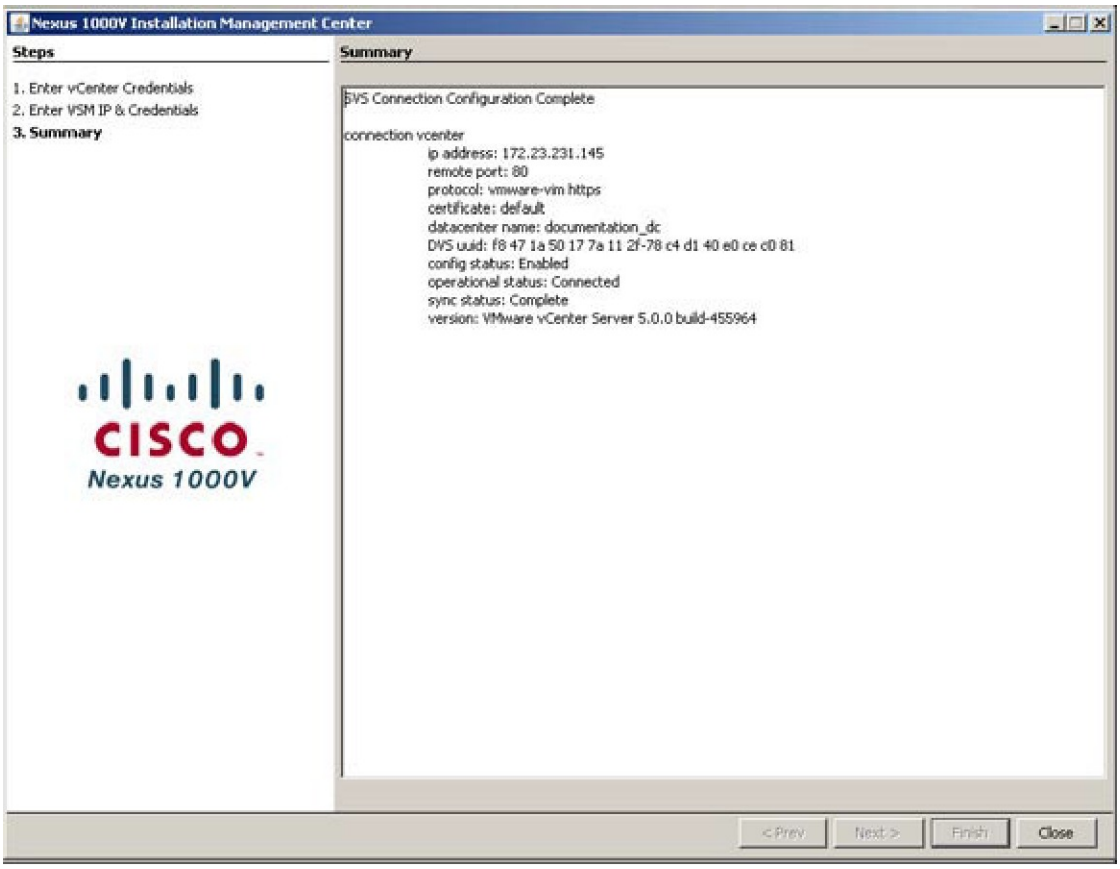
Step 11 Click **Finish**.

Figure 68: Enter VSM IP & Credentials Screen



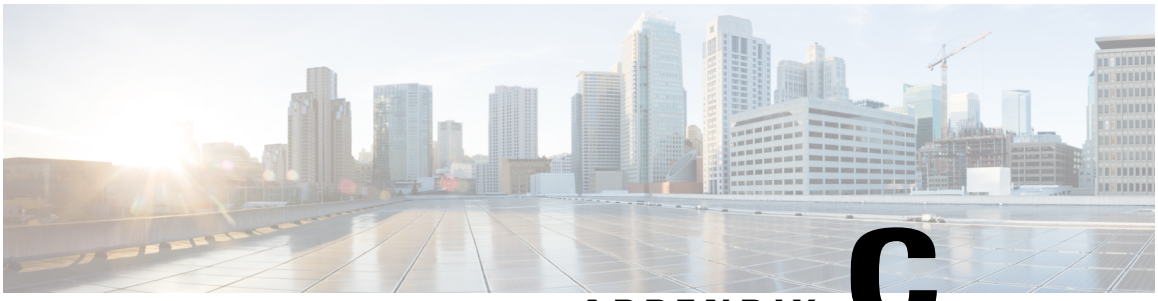
Step 12 Click **Close.**

Figure 69: Summary Screen



Step 13 In the **vSphere Console** window, enter the **show svs connections** command.
The operational status is Connected.

You have completed establishing the SVS connection.



APPENDIX C

Upgrading a Standalone VSM

This chapter includes the following sections:

Upgrading a System with a Standalone VSM

Upgrading a Standalone VSM

Procedure

Step 1 Log in to the VSM on the console.

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

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

Step 3 Access the Software Download Center by using this URL: http://www.cisco.com/public/sw-center/index.shtml

Step 4 Navigate to the download site for your switch.
You see links to the download images for your switch.

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

Step 6 Ensure that the required space is available for the image files to be copied.

```
switch# dir bootflash:
.
.
.
Usage for bootflash://
  485830656 bytes used
```

```
1109045248 bytes free
1594875904 bytes total
```

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

Step 7 Delete unnecessary files to make space available if you need more space on the VSM bootflash,

Step 8 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V kickstart and system images to the active VSM bootflash using a transfer protocol. You can use ftp:, tftp:, scp:, or sftp:. The examples in this procedure use scp:.

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

```
switch# copy
scp://user@scpserver.cisco.com//downloads/nexus-1000v-kickstart-4.2.1.SV1.5.2.bin
bootflash:nexus-1000v-kickstart-4.2.1.SV1.5.2.bin
switch# copy scp://user@scpserver.cisco.com//downloads/nexus-10000v-4.2.1.SV1.5.2.bin
bootflash:nexus-1000v-4.2.1.SV1.5.2.bin
```

Step 9 Read the release notes for the related image file. See the *Cisco Nexus 1000V Release Notes*.

Step 10 Determine the VSM status.

```
switch# show system redundancy status
Redundancy role
---------------
      administrative:   standalone
         operational:   standalone

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-2)
------------------------
    Redundancy state:   Not present
```

Step 11 Save the running configuration to the start configuration.

```
switch# copy running-config startup-config
```

Step 12 Update the boot variables and module images on the VSM.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart-4.2.1.SV1.5.2.bin system
bootflash:nexus-1000v-4.2.1.SV1.5.2.bin

Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.2.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-4.2.1.SV1.5.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

```
Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.2.bin.
[####################] 100% -- SUCCESS

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



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  Reset due to single supervisor



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system            4.2(1)SV1(4)           4.2(1)SV1(5.2)           yes
     1   kickstart            4.2(1)SV1(4)           4.2(1)SV1(5.2)           yes


Module         Running-Version                                        ESX Version
VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
----------------------  ----------------------
     3            4.2(1)SV1(4)         VMware ESXi 4.0.0 Releasebuild-208167 (1.9)
      COMPATIBLE              COMPATIBLE

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n]
```

Step 13 Continue with the installation by pressing Y.

Note If you press N, the installation exits gracefully.

```
Install is in progress, please wait.

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
```

Step 14 After the switch completes the reload operation, log in and verify that the switch is running the required software version.

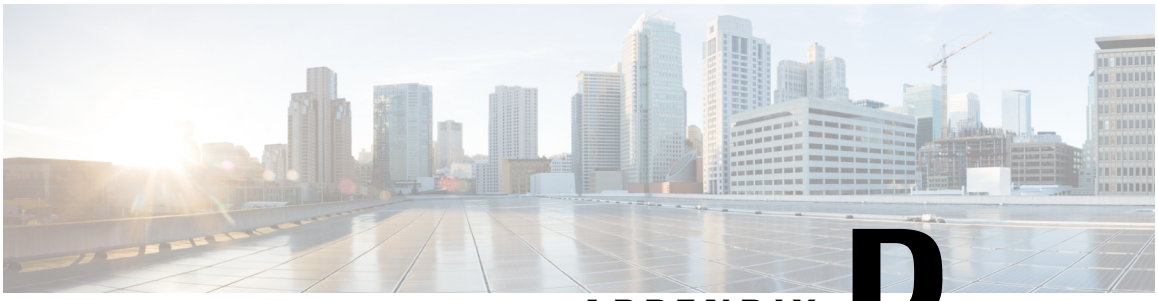
Example:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
```

```
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: loader version not available]
  kickstart: version 4.2(1)SV1(5.2)
  system:    version 4.2(1)SV1(5.2)
  kickstart image file is: bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.2.bin
  kickstart compile time:  3/27/2011 14:00:00 [03/27/2011 22:26:45]
  system image file is:    bootflash:/nexus-1000v-4.2.1.SV1.5.2.bin
  system compile time:     3/27/2011 14:00:00 [03/28/2011 00:56:08]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU         with 2075740 kB of memory.
  Processor Board ID T5056B050BB

  Device name: BL1-VSM
  bootflash:    3122988 kB

Kernel uptime is 0 day(s), 0 hour(s), 6 minute(s), 23 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
...
```

What to Do Next

Continue to Upgrading VSMs from Releases 4.2(1)SV1(4), 4.2(1)SV1(4a), 4.2(1)SV1(4b), 4.2(1)SV1(5.1), or 4.2(1)SV1(5.1a) to Release 4.2(1)SV1(5.2), on page 92.



APPENDIX D

Glossary

This chapter includes the following sections:

Glossary for Cisco Nexus 1000V

The following table lists the terminology in the Cisco Nexus 1000V implementation.

Table 7: Cisco Nexus 1000V Terminology

Term	Description
Control VLAN	One of two VLANs used for the communication between the VSM and VEM. The control VLAN is used to exchange control messages. The network administrator configures the control VLAN.
Distributed Resource Scheduler (DRS)	Balances the workload across your defined resources (hosts, shared storage, network presence, and resource pools) in a cluster.
Distributed Virtual Switch (DVS)	A logical switch that spans one or more VMware ESX/ESXi 4.1 or ESXi 5.0 servers. It is controlled by one VSM instance.
ESX/ESXi	A virtualization platform used to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine. Each ESX/ESXi host has a VI client available for management use. If your ESX/ESXi host is registered with the vCenter Server, a VI client that accommodates the vCenter Server features is available.
Managed Object Browser (MOB)	A tool that enables you to browse managed objects on vCenter Server and ESX Server systems.
Network Interface Card (NIC)	A device that connects to the network to send and receive traffic between the switch and data link layer.

Term	Description
Open Virtual Appliance or Application (OVA) file	The package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging: • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Packet VLAN	One of two VLANs used for the communication between the VSM and VEM. The packet VLAN forwards relevant data packets, such as CDP, from the VEM to the VSM. The network administrator configures the packet VLAN. See control VLAN.
Physical network interface card (PNIC)	A device that connects to the network to send and receive traffic between the physical switch and the data link layer.
Port profile	A collection of interface configuration commands that can be dynamically applied at either physical or virtual interfaces. A port profile can define a collection of attributes such as a VLAN ID, a private VLAN (PVLAN), an access control list (ACL), and port security. Port profiles are integrated with the management layer for the virtual machines and allow virtual machine administrators to choose from profiles as they create virtual machines. When a virtual machine is powered on or off, its corresponding profiles are used to dynamically configure the vEth interface.
vCenter Server	A service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).
Virtual Ethernet Interface (vEth)	Virtual equivalent of physical network access ports. vEths are dynamically provisioned based on network policies stored in the switch as the result of virtual machine provisioning operations at the hypervisor management layer.
Virtual Ethernet Module (VEM)	The component in the Cisco Nexus 1000V that actually switches data traffic. It runs on a VMware ESX/ESXi 4.1 or ESXi 5.0 host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual data center as defined by VMware vCenter Server. This software replaces the VMware vSwitch in each hypervisor. It performs switching between directly attached virtual machines and provides uplink capabilities to the rest of the network.
VMotion	The practice of migrating virtual machines live from server to server.

Term	Description
Virtual NIC (vNIC)	Logically connects a virtual machine to the VMware vSwitch and allows the virtual machine to send and receive traffic through that interface. If two vNICs attached to the same VMware vSwitch need to communicate with each other, the VMware vSwitch performs the Layer 2 switching function directly, without any need to send traffic to the physical network.
Virtual Supervisor Module (VSM)	The control software of the Cisco Nexus 1000V distributed virtual switch. It runs on a virtual machine (VM) and is based on Cisco NX-OS.
VMware Installation Bundle (VIB)	The software application that manages Cisco Nexus 1000V software installation and VEM upgrades. **Note** VUM is not a requirement. Software can be installed manually without using VUM.
vSphere Client	The user interface that connects users remotely to the vCenter Server or ESX/ESXi from any Windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

INDEX

L

M

N

P

S

T

U

V