Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV2(2.2)

First Published: January 31, 2014

Last Modified: September 04, 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-31463-01

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 and server administrators with the following experience and knowledge:

Note Knowledge of VMware vNetwork Distributed Switch is not required.

- An understanding of virtualization
- An understanding of the corresponding hypervisor management software for your switch, such as VMware vSwitch, Microsoft System Center Virtual Machine Manager (SCVMM), or OpenStack

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.

Convention	Description
[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 for VMware vSphere

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 REST API Plug-In Configuration Guide

Cisco Nexus 1000V Security Configuration Guide

Cisco Nexus 1000V System Management Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Cisco Nexus 1000V VXLAN Configuration Guide

Cisco Nexus 1000V VDP Configuration Guide

Cisco Nexus 1000V DFA Configuration Guide

Programming Guide

Cisco Nexus 1000V XML API Configuration Guide

Reference Guides

Cisco Nexus 1000V Command Reference

Cisco Nexus 1000V Resource Availability Reference

Troubleshooting and Alerts

Cisco Nexus 1000V Troubleshooting Guide

Cisco Nexus 1000V Password Recovery Procedure

Cisco NX-OS System Messages Reference

Cloud Services Platform Documentation

The *Cisco Cloud Services Platform* documentation is available at http://www.cisco.com/en/US/products/ps12752/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/ps13095/tsd_products_support_series_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 one of the following:

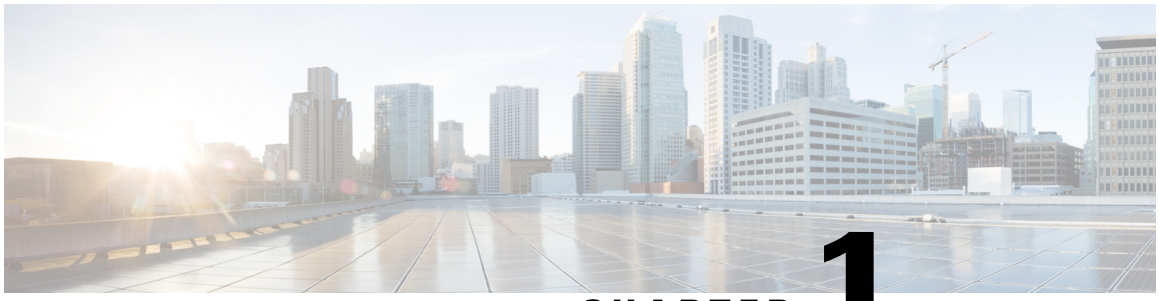
- nexus1k-docfeedback@cisco.com

We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

Overview

This chapter contains the following sections:

Information About Virtualization

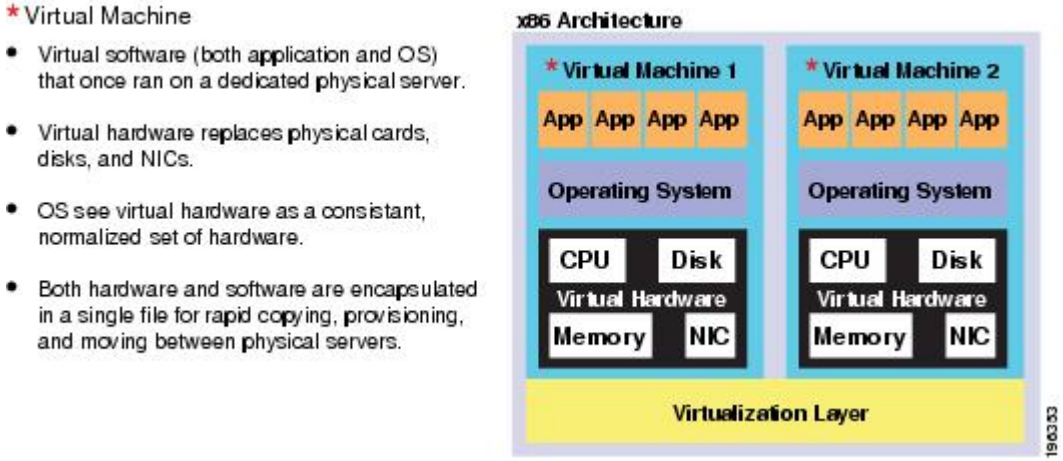
Virtualization allows multiple Virtual Machines (VMs) to run in isolation, side by side on the same physical machine.

Each VM 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.

VMs 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.

This figure shows two VMs side by side on a single host.

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



Information About 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.

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 that is listed in the VMware Hardware Compatibility List (HCL).

The Cisco Nexus 1000Vhas the following components:

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

See Glossary, on page 129 for a comprehensive list of terms that are used with the Cisco Nexus 1000V.

Information About Installing the Cisco Nexus 1000V 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 file name for **Release 4.2(1)SV2(2.2)** is `Nexus1000v.4.2.1.SV2.2.2.zip`.

  Extract the zip file and you will see the following components:

Component	Destination Folder
VSM	The ISO and OVA files for VSM Installation are located in the Nexus1000v.4.2.1.SV2.2.2/VSM/Install directory. The filenames are: • ISO—nexus-1000v.4.2.1.SV2.2.2.iso • OVA—nexus-1000v.4.2.1.SV2.2.2.ova **Note** You should use the ESXi host software version 5.0 or later.
Installer Application	The Cisco Nexus 1000V Installer Application is located in the Nexus1000v.4.2.1.SV2.2.2/VSM/Installer_App directory. The filename is Nexus1000V-install_CNX.jar. **Note** You should use this file with VMware vCenter Version 5.0 or later.
VEM	The VEM Software is located in the Nexus1000v.4.2.1.SV2.2.2/VEM directory.

After you install the VSM as a Virtual Machine (VM), copy the file that contains the VEM software from the Virtual Supervisor Module (VSM) web page: http://VSM_IP_Address/

Cisco Nexus 1000V and Its Components

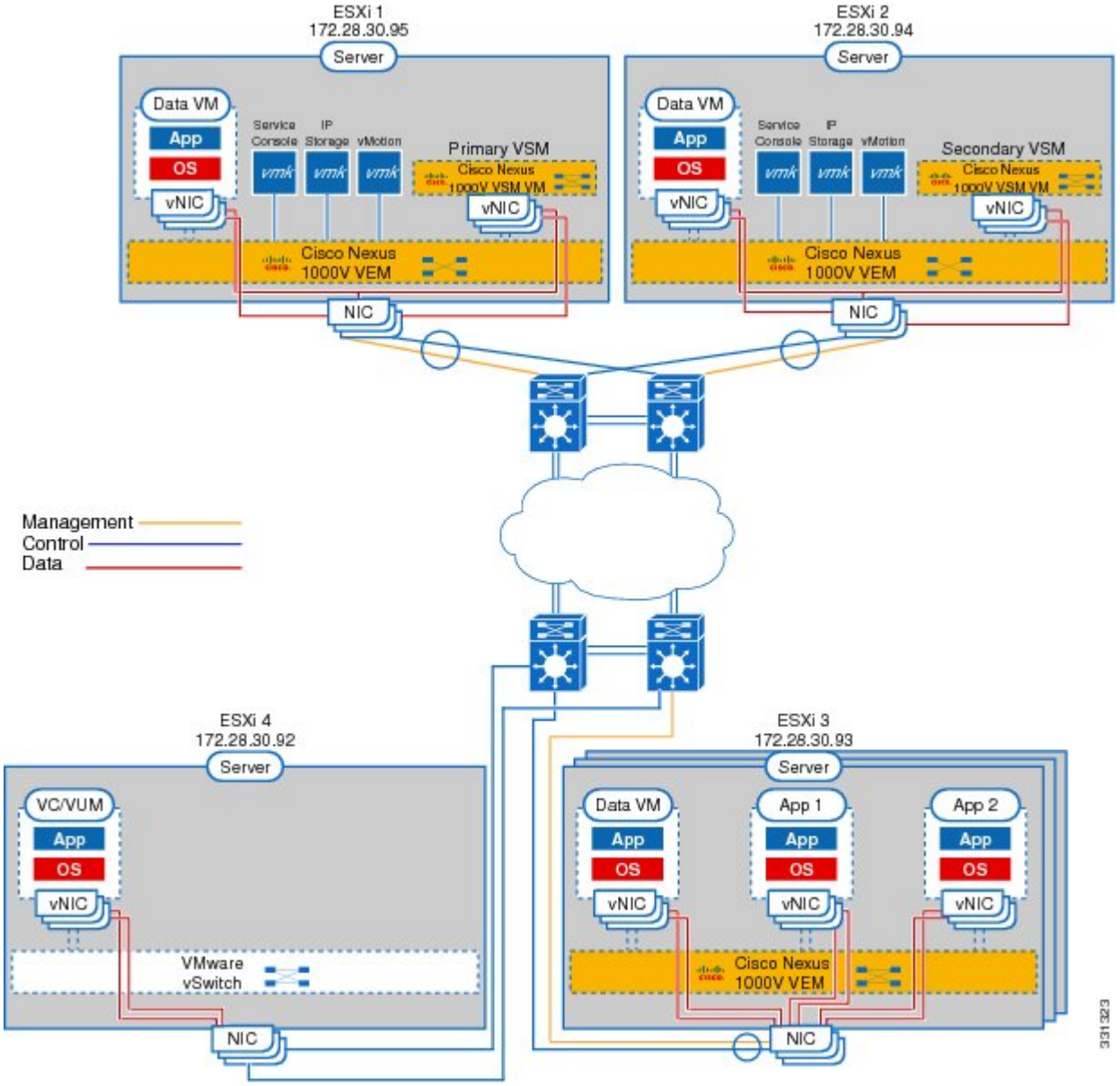
Note A list of terms used with the Cisco Nexus 1000V can be found in Glossary, on page 129.

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 VM that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)—A virtual line card that is 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.

This 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

You can install the VSM in either a standalone or active/standby high-availability (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

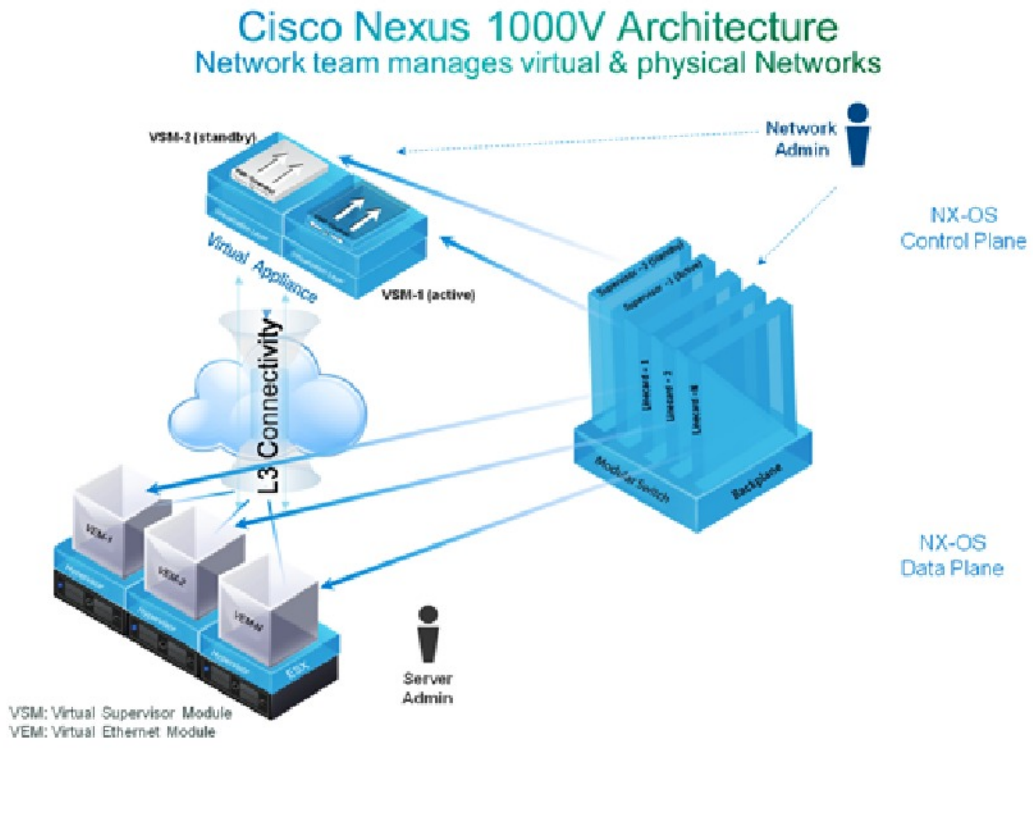
A single VSM can manage up to 64 VEMs.

Note We recommend that you use 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 that are connected to VM vNICs but do not switch the 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. The Cisco Nexus 1000V architecture is shown in this 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 VMs
- 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, the traffic is switched between VMs locally at each VEM instance. Each VEM also interconnects the local VM 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 with 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 that are 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 Encapsulated Remote Switched Port Analyzer (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 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.

This 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 differences between the Cisco Nexus 1000V and a physical switch are as follows:

- 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 packets by 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 the 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 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 Layer 3 Control vmknic, must have a system port profile applied to it (see the System Port Profiles, on page 10 and System VLANs, on page 10), so the VEM can enable it before contacting the VSM.

For more information about 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 about Layer 2 control mode, see Configuring Layer 2 Connectivity.

Management, Control, and Packet VLANs

Control VLANs

A 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 VM network properties.

- A 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.

Packet VLANs

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

A 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 VM network properties.

A 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

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 a 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 the system port profiles and system VLANs, to 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 that use the system port profile, which are members of one of the defined system VLANs, are automatically enabled and forward 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.

System VLANs

You must define a system VLAN 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 is not 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.
- The 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, Secure Shell (SSH), or Telnet connections.
- The VLAN that is used for remote storage access (iSCSI or NFS).

Caution You must use system VLANs sparingly and only as described in this 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 you remove the port profile from service. This action prevents you from 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*.

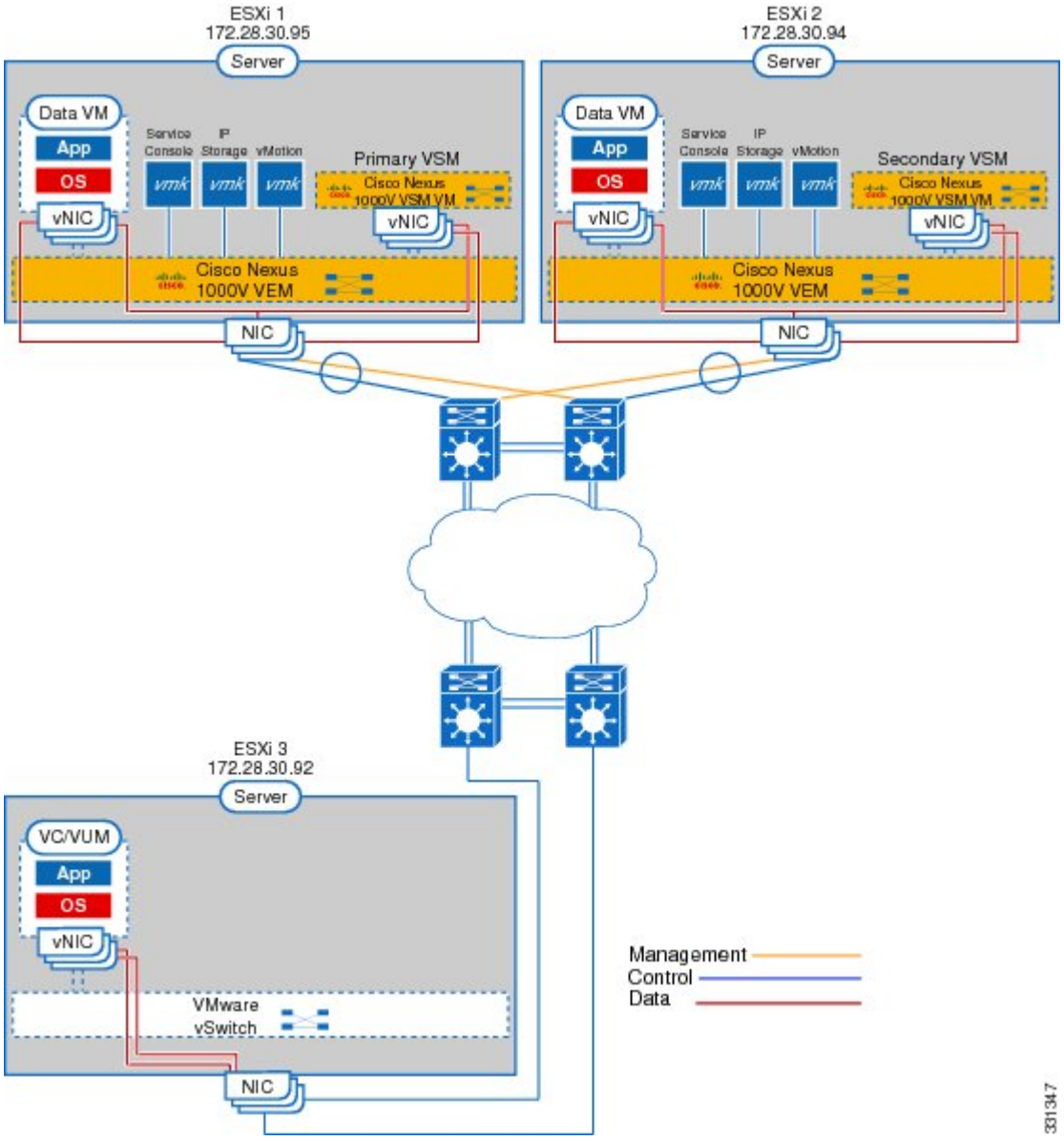
Recommended Topologies

Layer 3

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

This 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

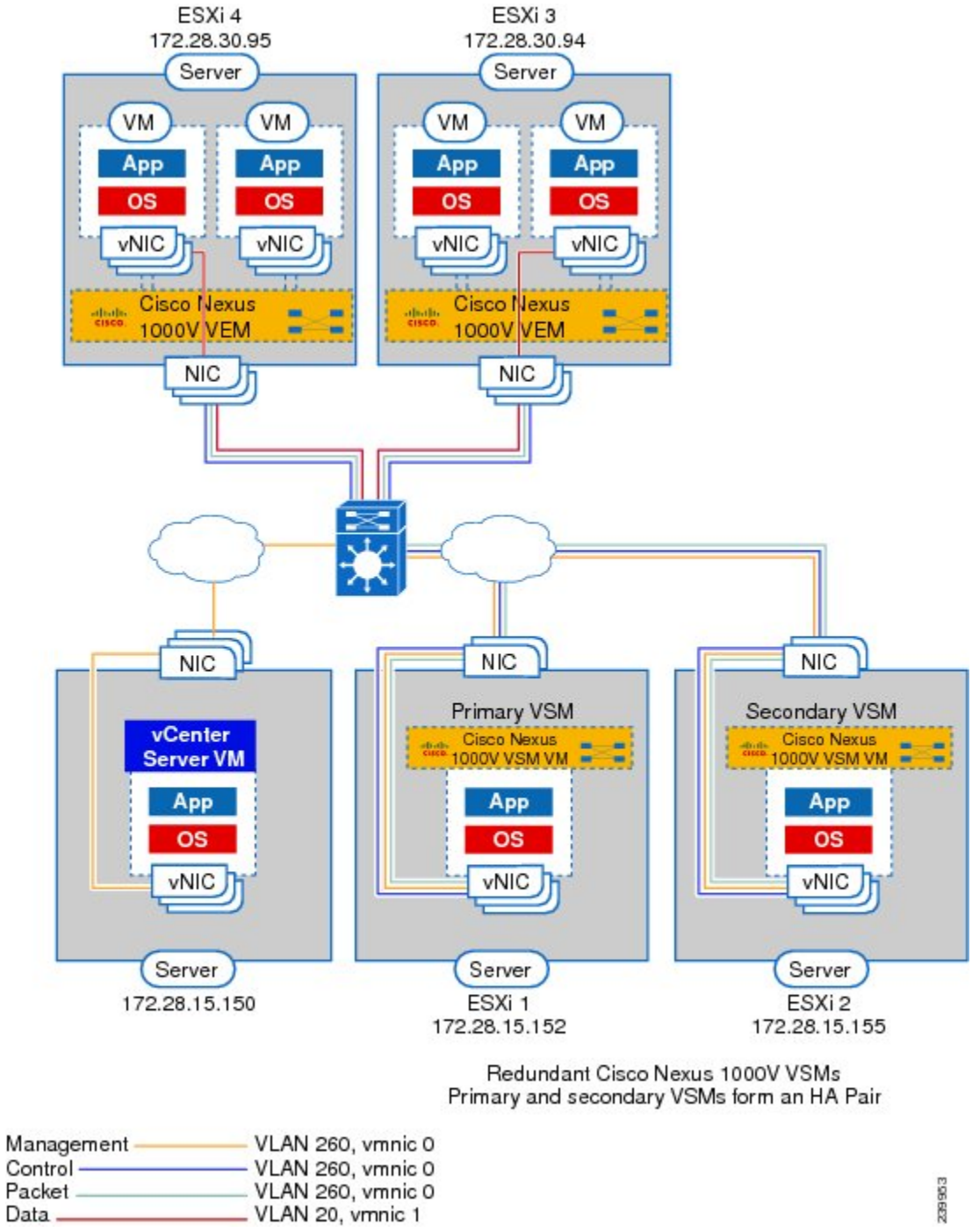


Information About Layer 2 Connectivity

Note Layer 3 connectivity is the preferred method for communications between the VSM and the VEMs.

This 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.

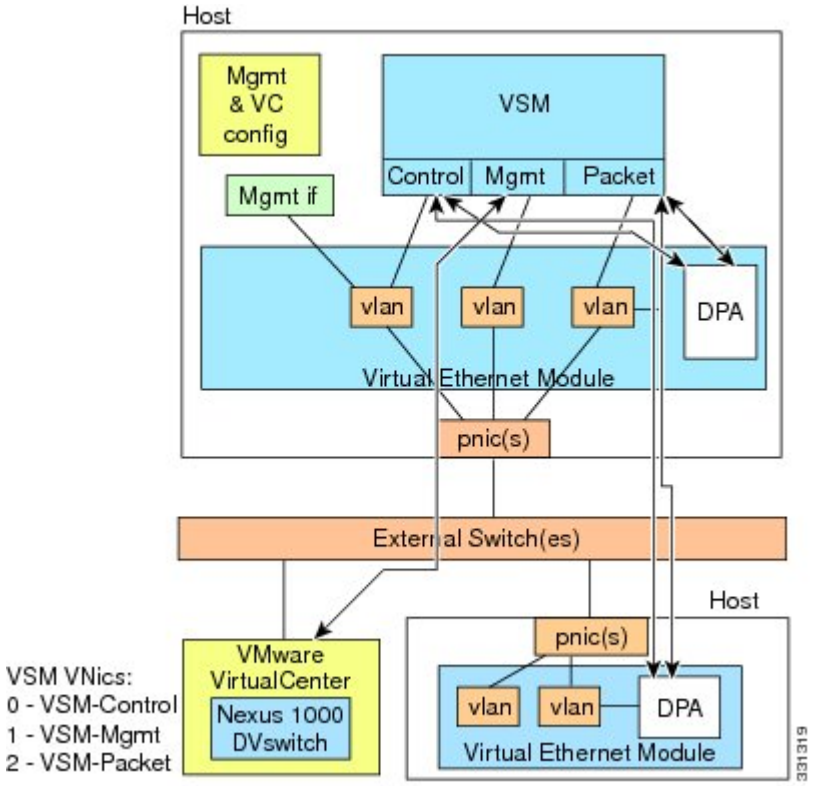
Figure 5: Cisco Nexus 1000V Installation Diagram for Layer 2



Layer 2 on the Same Host

This figure shows a VSM and VEM that is running on the same host in Layer 2 mode.

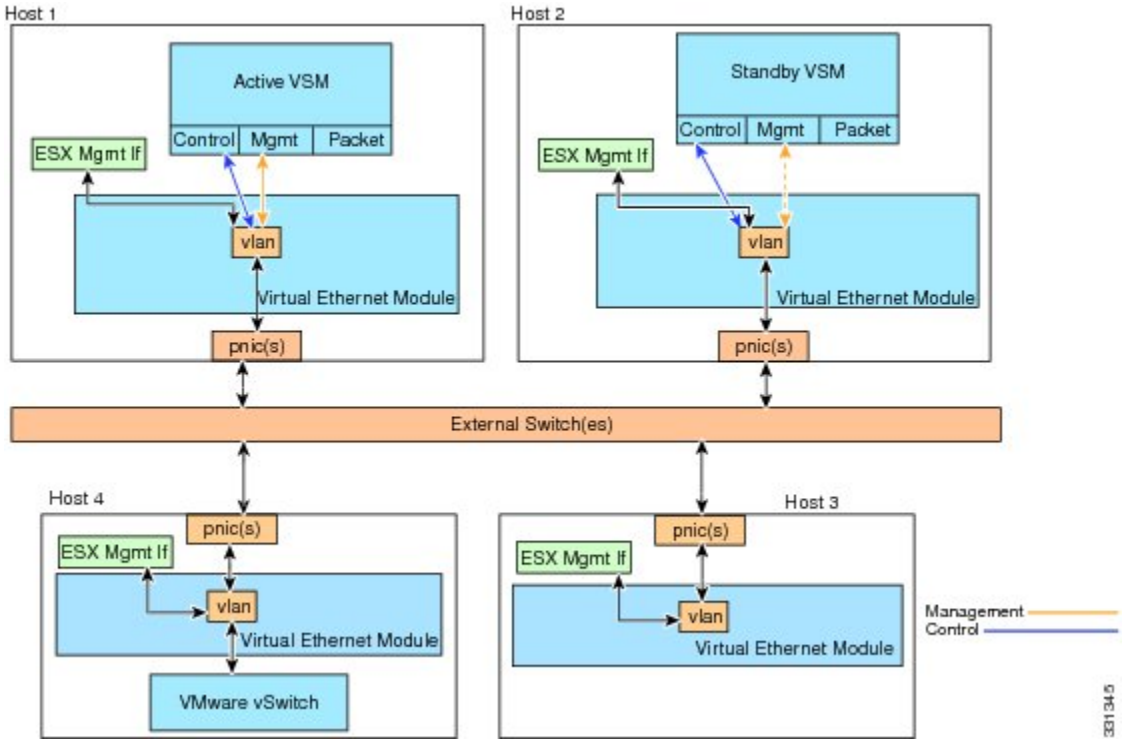
Figure 6: VSM and VEM on the Same Host in Layer 2 Mode



Control and Management on the Same VLAN

This 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.

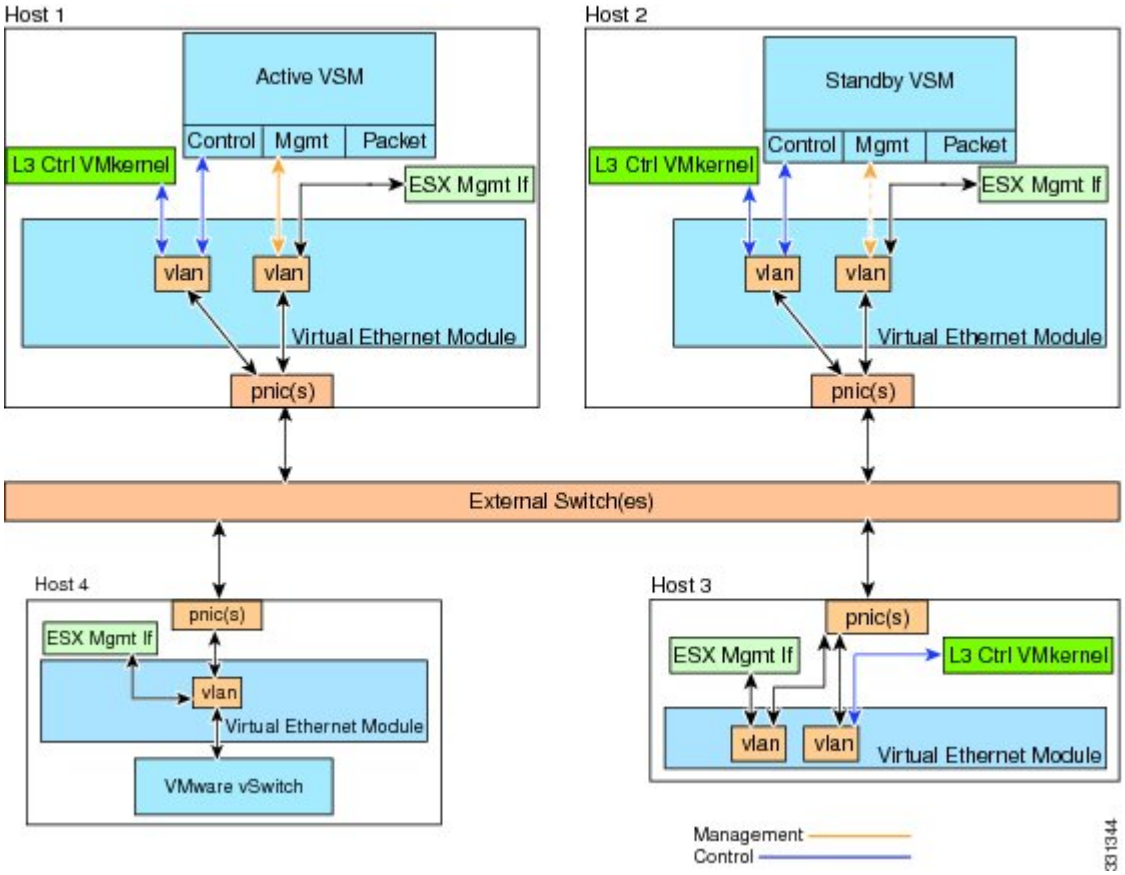
Figure 7: Control and Management on the Same VLAN



Control and Management on Separate VLANs

This 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.

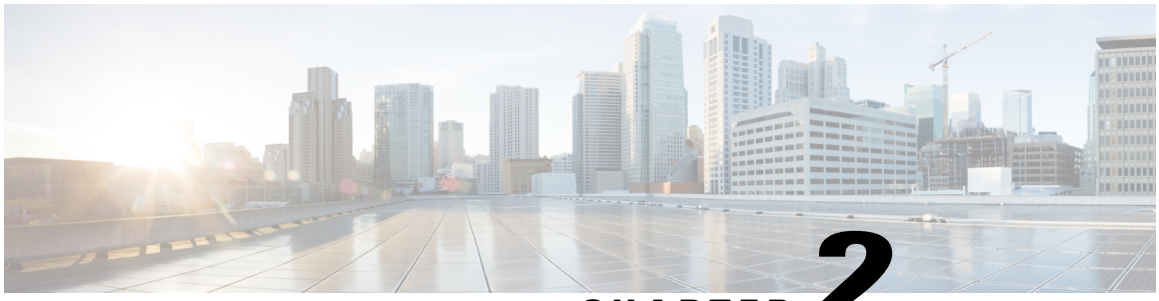
Figure 8: Control and Management on Separate VLAN



VMware Interaction

You can use a Cisco Nexus 1000V VSM as a VM 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 contains the following sections:

Installing the Cisco Nexus 1000V Software using the Installer Application

Cisco Nexus 1000V Installer App

The Cisco Nexus 1000V Installer App is the graphical user interface (GUI) that you use to install 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 app 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 vCenter Server.
- Migrates each VMware port group or kernel NIC to the correct port profile.
- Migrates each PNIC from the VMware vSwitch to the correct uplink on the DVS.
- Adds the host to the DVS.
- Enables you to quickly deploy VSMs and VEMs with minimal or custom inputs on a single screen and expect a fully functional Cisco Nexus 1000V setup. See the following link for more information: Cisco Nexus 1000V: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html.

Cisco Nexus 1000V Installer App Prerequisites

Note The Installation Application 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.
- Make sure no VEMs were previously installed on the host where the VSM resides.
- You must have administrative credentials for the vCenter Server.
- The java.exe file must be located within the search path defined in your system.

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.
- You have already installed the VMware Enterprise Plus license on the hosts.
- The host must have one or more physical NICs on each VMware vSwitch that is being used.
- All VEM hosts must be running ESX/ESXi 5.0 or later releases.
- You have installed the appropriate vCenter Server and VMware Update Manager (VUM) versions.
- You are familiar with the Cisco Nexus 1000V topology diagram that is shown in Layer 3, on page 11.

- 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.
- If the hosts are in ESXi stateless mode, then enable the Pxe Booted ESXi host settings available under **Home** > **Update Manager** > **Configuration** > **ESXi host/cluster**.
- You have a copy of your VMware documentation available for installing software on a host.

Upstream Switch Prerequisites

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

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

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

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

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

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

end
```

Guidelines and Limitations of the Cisco Nexus 1000V Installer App

The Cisco Nexus 1000V Installer app has the following configuration 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 you are using the VC Connection installer, after the SVS connection is completed, you must check the VSM by using the **show svs connection** command to view an accurate status.
- To install VEM using the Installer App, ensure the SVS Connection is connected and active.
- Layer 3 mode of deployment is supported by the Cisco Nexus 1000V Installer App with ESXi host only.
- The Cisco Nexus 1000V Installer App can support 14 different subnets during module additions when reusing port profiles.
- The Cisco Nexus 1000V Installer App always deploys with VSM HA pairs.
- If you are executing the Installer App on a Ubuntu operating system, ensure you have installed Oracle JRE.
- When you move 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.

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

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

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

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

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

3. Last configuration change

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

- If both VSMs have the same number of modules and no VC connectivity, the VSM with the latest configuration remains active and the other VSM is rebooted.

4 Last active VSM

- If the previous three conditions are not met, the VSM that became active most recently is rebooted.

To improve redundancy, install primary and secondary VSM VMs on separate hosts that are connected to different upstream switches.

Installing the Cisco Nexus 1000V Software using the Installer Application

Installing VSM Software Using the Cisco Nexus 1000V Installer App

There are two procedures for installing the Cisco Nexus 1000V VSMs. The standard procedure is for the novice administrator. The custom procedure is for the more experienced administrator. The custom procedure has more configuration inputs to be used by administrators already familiar with the installation process and requiring more installation options.

- Installing the Cisco Nexus 1000V in Standard Mode (Layer 3 Mode), on page 21
- Installing the Cisco Nexus 1000V in Custom Mode (Layer 3 and Layer 2 Mode), on page 24

Installing the Cisco Nexus 1000V in Standard Mode (Layer 3 Mode)

Before You Begin

- You have the following information:

Note The VSM IP address must be in the same management VLAN as the host.

  - Management VLAN ID
  - Domain ID
  - Management IP address
  - Subnet mask
  - Gateway IP address

- You have the JDK version 1.6 or later installed on the host running the Cisco Nexus 1000V Installer App.
- The VSM will be deployed with the following credentials:

- username: admin
- password: admin

- If you select the migration to DVS option as yes, the migration of hosts that have VSMs migrate all the interfaces under the vSwitch that have the ESXi management interface (for example, vmk0).

Procedure

Step 1 Double-click the installation file icon or at the command-line interface, enter the following command to start the Cisco Nexus 1000V Installer App:

```
java -jar Nexus1000V-install_CNX.jar
```

Step 2 Click the **Cisco Nexus 1000V Complete Installation** radio button.

Step 3 Click the **Standard** radio button.

Step 4 After reading the prerequisites, click **Next**.

Step 5 In the **vCenter Server Credentials** screen, do the following:

a) Enter the following vCenter credentials:

- **IP Address**
- **Port (https only)**

  Note This field is prepopulated but can be modified.

- **User ID**
- **Password**

b) Click **Next.**

Step 6 In the **Standard Configuration Data** screen, click the **Browse** button for the Host 1 IP address.

Step 7 In the **vCenter Inventory** screen, do the following:

a) Choose the host for the primary VSM.
b) Click **Select Host**.

The **IP Address / Name** and **Data Store** for Host 1 populate.

Step 8 In the **Standard Configuration Data** screen, click the **Browse** button for the Host 2 IP address.

Step 9 In the **vCenter Inventory** screen, do the following:

a) Choose the host for the secondary VSM.
b) Click **Select Host**.

Step 10 In the **Standard Configuration Data** screen, enter the Virtual Machine Name.

Step 11 In the **Standard Configuration Data** screen, do the following:

a) Click the **Browse** button for the OVA Image Location field.
b) Browse to the OVA file.
c) Choose the OVA file.
d) Click **Open.**

Step 12 In the **Standard Configuration Data** screen, do the following:

a) Enter the remaining configuration data:

- **VSM IP Address**
- **Subnet Mask**
- **Gateway IP Address**
- **Domain ID**
- **Management VLAN**

b) Click **Yes** or **No** to migrate the hosts to the DVS.

c) (Optional) Click **Save Configuration**.

Note The save configuration option allows you to create an XML configuration file for later use. This steps allows you to import and prepopulate common values in the template for later use.

d) Click **Next.**

Step 13 After reviewing the values in the **Standard Configuration Review** screen, choose one of the following:

- Click **Next** to continue.
- Click **Prev** to return to the previous screens and modify the entries.

The **Standard Installation Progress** screen opens.

When the installation process completes, the **Confirmation** screen is displayed. A typical installation of the VSM takes about 6 to 8 minutes.

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

- Click **Yes** if you want to add more modules and continue to the next step.
- Click **No** if you do not want to add more modules and continue with Step 18.

Step 15 In the **Adding Modules** screen, do the following:

a) Do one of the following:

- Click **Install VIB** to install VIBs on this host.
- Click **Install VIB and add module to Nexus 1000V** to install VIBs on this host and move them to the Cisco Nexus 1000V.

b) In the **Management VLAN** field, enter a VLAN ID.

Step 16 In the **Hosts Selection** screen, do the following:

a) Choose the hosts that you want to add.

b) Click **Next**.

Step 17 In the **Host Review** screen, do the following:

- Review the entries.
- Click **Finish**.

Step 18 In the **Summary** screen, click **Close.**

Installing the Cisco Nexus 1000V in Custom Mode (Layer 3 and Layer 2 Mode)

Before You Begin

- You have the following information:
  - Control VLAN ID
  - Packet VLAN ID
  - Management VLAN ID
  - Domain ID
  - Management IP address
  - Subnet mask
  - Gateway IP address
  - SVS datacenter name
  - Control, packet, and management port groups
  - Management VLAN ID of ESXi hosts
- You have the JDK version 1.6 or later installed on the host running the Cisco Nexus 1000V Installer App.

Procedure

Step 1 Double-click the application icon or at the command-line interface, enter the following command to start the Cisco Nexus 1000V Installer App:

```
java -jar Nexus1000V-install_CNX.jar
```

Step 2 Click the **Cisco Nexus 1000V Complete Installation** radio button.

Step 3 Click the **Custom** radio button.

Step 4 After reading the prerequisites, click **Next**.

Step 5 In the **vCenter Server Credentials** screen, do the following:

a) Enter the following vCenter credentials:

- **IP Address**
- **Port (https only)**

  Note This field is prepopulated but can be modified.
- **User ID**
- **Password**

b) Click **Next.**

Step 6 In the **Custom Configuration Data** screen, click the **Browse** button for the **Host 1 IP Address / Name** field.

Step 7 In the **Host 1 Selection vCenter Inventory** screen, do the following:

a) Choose the host for the primary VSM.
b) Click **Select Host**.

The **Host 1 IP Address / Name** and **Data Store** fields are populated.

Step 8 In the **Host 1 vSwitch Custom Configuration Data** screen, click the **Browse** button for the **Host 1 vSwitch** field.

Step 9 In the **Host 1 vSwitch Selection** screen, do the following:

- Choose a vSwitch.
- Click **Select**.

The **Host 1 vSwitch** field is populated.

Step 10 In the **Host 2 IP Address Custom Configuration Data** screen, click the **Browse** button for the **Host 2 IP Address / Name** field.

Step 11 In the **Host 2 Selection vCenter Inventory Screen** screen, do the following:

- Choose the host for the secondary VSM.
- Click **Select Host**.

Step 12 In the **Host 2 vSwitch Custom Configuration Data** screen, click the **Browse** button for the **Host 2 vSwitch** field.

Step 13 In the **Host 2 vSwitch Make a Selection** screen, do the following:

- Choose a **vSwitch**.
- Click **Select**.

Step 14 In the **Switch Name Custom Configuration** screen, do the following:

a) Enter the **Switch Name**.
b) Enter the **Admin User Name**.
c) Enter the **Admin Password**.
d) Enter the **Confirm the Admin Password**.
e) Enter the **Virtual Machine Name**.

Step 15 In the **OVA Image Custom Configuration Data** screen, click the **Browse** button for the **OVA Image Location** field.

Step 16 In the **OVA File Location** screen, do the following:

a) Browse to the OVA file.
b) Choose the OVA file.
c) Click **Open**.

Step 17 In the **VSM IP Address Custom Configuration Data** screen, do the following:

a) Click the **Layer L2** or **Layer L3** radio button.
The Layer 3 mode is selected by default.

b) Enter the remaining configuration data:

- **VSM IP Address**
- **Subnet Mask**
- **Gateway IP Address**
- **Domain ID**

c) Check the **Enable Telnet** check box if you want to enable Telnet.
By default, only SSH is enabled.

Step 18 Click the **Browse** button for the **Data Center Name**.

Step 19 In the **Choose a Data Center** screen, do the following:

a) Choose a data center.
b) Click **Select.**

Step 20 Click the **Browse** button for the Control Port Group **Port Group Name** field.

Step 21 In the **Make a selection** screen, do the following:

- Choose a VLAN ID.
- Click **Select**.

Step 22 In the **Custom Configuration Data** screen, do the following to create a new Management Port Group:

Note The Installer App assumes the use of dot1q trunking and requires you to specify the management VLAN.

a) Choose the **Create New** radio button.
b) Enter the **Port Group Name**.
c) Enter the **VLAN ID**.
d) Enter a VLAN ID in the **Management VLAN ID** field.
e) Click **Yes** or **No** to migrate the hosts to the DVS.
f) Click the **Save Configuration** button if you want to save the settings to a configuration file.
g) Click **Next**.

Step 23 In the **Custom Configuration Review** screen, do the following:

- Validate the input.
- Click **Next**.

The **Custom Configuration Review Installation Progress** screen opens.

When the installation completes, the **Confirmation** screen opens.

Step 24 In the **Custom Confirmation** screen, do one of the following:

- Click **Yes** if you want to add more modules and continue to the next step.
- Click **No** if you do not want to add more modules, and proceed with the steps as prompted to complete the process.

Step 25 In the **Confirmation** screen, complete the tasks as follows:

a) Do one of the following:

- Click **Install VIB** to install VIBs on this host.
- Click **Install VIB and add module to Nexus 1000V** to install VIBS on this host and move them to the Cisco Nexus 1000V.

b) In the **Management VLAN** field, enter a VLAN ID.

Note In the Management VLAN field, add the same VLAN that is assigned to your vmkernel interface.

Step 26 In the **Hosts Selection** screen, do the following:

a) Choose the hosts you want to add.
b) Click **Next**.

Step 27 In the **Host Review** screen, do the following:

- Review the entries.
- Click **Finish**.

Step 28 In the **Custom Summary** screen, click **Close**.

Installing the VEM Software Using the Cisco Nexus 1000V Installer App

- When the Cisco Nexus 1000V Installer App installs VEMs, it migrates all VEM kernels and their corresponding vmnics across vSwitches to the Cisco Nexus 1000V VEMs

  .

- If a particular VEM is capable of hosting VSMs, the network administrator must manually allow a control VLAN in the uplink port profile of VEMs in Layer 3 deployment mode for VSM HA communication.

Before You Begin

- You have the following information:
  - vCenter IP address
  - vCenter user ID
  - vCenter password
  - VSM IP address
  - VSM password

Note The hosts that will be installed as VEMs should not have any Cisco Nexus 1000V vSphere Installation Bundle (VIB) files. Uninstall any Cisco Nexus 1000V VIBs before starting the Cisco Nexus 1000V Installer App.

Procedure

Step 1 Double-click the installation application icon or at the command-line interface, enter the following command to start the Cisco Nexus 1000V Installer App.

```
java -jar Nexus1000V-install_CNX.jar
```

Step 2 In the **Cisco Nexus 1000V Installer App** screen, click the **Virtual Ethernet Module Installation** radio button.

Step 3 After reading the prerequisites, click **Next**.

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

a) Enter the following vCenter Credentials:

- **IP address**
- **Port (https only)**

  Note This field is prepopulated but can be modified.

- **User ID** (for a vCenter user with administrator-level privileges)
- **Password** (for a vCenter user with administrator-level privileges)

b) Click **Next**.

Step 5 In the **Enter VSM IP & Credentials** screen, do the following:

a) Enter the following credentials:

- **VSM IP address**
- **VSM Password**

b) Click **Next**.

Step 6 In the **Confirmation** screen, do one of the following:

- Click **Yes** if you want to add more modules and continue to the next step.
- Click **No** if you do not want to add more modules and continue with Step 10.

Step 7 In the **Adding Modules** screen, do the following:

a) Do one of the following:

- Click **Install VIB** to install VIBs on this host.
- Click **Install VIB and add module to Nexus 1000V** to install VIBs on this host and move them to the Cisco Nexus 1000V.

b) In the **Management VLAN** field, enter a VLAN ID.

Step 8 In the **VEM Hosts Selection** screen, do the following:

a) Choose the hosts that you want to add.

b) Click **Next**.

Step 9 In the **VEM Host Review** screen, do the following:

- Review the entries.
- Click **Finish**.

Step 10 In the **VEM Summary** screen, click **Close**.

Note
- If the VEM software fails to install on a host, "Install status: Failure" message appears.
- Once the Cisco Nexus 1000V Installer App completes the VEM installation, verify the current status of modules from the VSM by using the **show module** command.

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

Connecting to the vCenter Server

To establish connection between the VSM and the vCenter Server, perform the following steps:

Before You Begin

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

Procedure

Step 1 Double-click on the installation application icon. Or, at the command-line interface, enter the following command to start the Cisco Nexus 1000V.

```
java -jar Nexus1000V-install_CNX.jar
```

Step 2 In the **Cisco Nexus 1000V Installer App** screen, click the **VC Connection** radio button.

Step 3 After reading the Prerequisites, click **Next**.

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

a) Enter the following vCenter Credentials:

- **IP address**

- **Port (https only)**

  Note This field is prepopulated but can be modified.

- **User ID** (for a vCenter user with administrator-level privileges)
- **Password** (for a vCenter user with administrator-level privileges)

b) Click **Next**.

Step 5 In the **Enter VSM IP & Credentials** screen, do the following:

a) Enter the following credentials:

- **VSM IP address**
- **VSM Password**
- **SVS Datacenter Name**

b) Click **Finish**.

Installing the Cisco Nexus 1000V Software Manually

Prerequisites for Installing the Cisco Nexus 1000V

ESX or ESXi Host Prerequisites

ESX or ESXi hosts have the following prerequisites:

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

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

This table lists the minimum requirements for hosting a VSM.

Table 1: 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)	3 GB[1]
NIC	3
SCSI Hard Disk	3 GB with LSI Logic Parallel adapter
CPU speed	2048 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 35 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 35 to reserve RAM and set the memory size.

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 2: 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, on page 11.

Upstream Switch Prerequisites

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

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

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

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

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

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

end
```

VEM Prerequisites

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

Note If 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.
- If the hosts are in ESXi stateless mode, enable the PXE booted ESXi host settings under **Home** > **Update Manager** > **Configuration** > **ESXi host/cluster**.
- You have a copy of your VMware documentation available for installing software on a host.
- You have already obtained a copy of the VEM software file from one of the sources listed in Cisco Nexus 1000V Download Software page.
- 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 vCenter Server.

Guidelines and Limitations for Installing the Cisco Nexus 1000V

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

- Do not enable VMware fault tolerance (FT) for the VSM VM because it is not supported. Instead, Cisco NX-OS HA provides high availability for the VSM.
- The VSM VM supports VMware HA. However, we strongly recommend that you deploy redundant VSMs and configure Cisco NX-OS HA between them. Use the VMware recommendations for the VMware HA.
- Do not enable VM monitoring for the VSM VM because it is not supported, even if you enable the VMware HA on the underlying host. Cisco NX-OS redundancy is the preferred method.
- When you move a VSM from the VMware vSwitch to the Cisco Nexus 1000V DVS, the connectivity between the active and standby VSM might get temporarily lost. In that situation, both active and standby VSMs assume the active role.

Note We recommend you to monitor and install all the relevant patch applications from VMware ESX host server.

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

1. The number of modules attached to the VSM
   - If more modules are attached on one of the VSMs and there is no virtual channel (VC) connectivity on both VSMs, the VSM that has the smaller number of modules is rebooted.

- If modules are attached to both VSMs and one of the VSMs has VC connectivity, the VSM without connectivity is rebooted.

2 VC connectivity

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

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

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

3 Last configuration change

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

- If both VSMs have the same number of modules and no VC connectivity, the VSM with the latest configuration remains active and the other VSM is rebooted.

4 Last active VSM

- If the previous three conditions are not met, the VSM that became active most recently is rebooted.

- If the VSM is moved from the VMware vSwitch to the Cisco Nexus 1000V DVS, we recommend that you configure port security on the VSM vEthernet interfaces to secure control/packet MAC addresses.
- To improve redundancy, install primary and secondary VSM VMs on separate hosts that are connected to different upstream switches.
- The Cisco Nexus 1000V VSM always uses the following three network interfaces in the same order as specified below:

  1 Control Interface
  2 Management Interface
  3 Packet Interface

- There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

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

Installing the VSM Software

Installing the Software from the ISO Image

Before You Begin

- Know the location and image name of the ISO image you require for the installation.
- You have already read the Prerequisites for Installing the Cisco Nexus 1000V, on page 30.
- 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 3 GB of RAM reserved and allocated.
  - Minimum CPU speed of 2048 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 3 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 2048 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**.

Step 12 Enter and confirm the Administrator password.
Note All alphanumeric characters and symbols on a standard US keyboard are allowed except for these three: $ \ ?

Step 13 Enter the domain ID.

```
Enter the domain id<1-4095>: 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)SV2(2.2),
Do you want to reconfigure? (yes/no) [n] yes
          Current vem feature level is set to 4.2(1)SV2(2.2)
          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 44.

Installing the Software from an OVA Image

Before You Begin

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

- Know the location and image name of the OVA image you require for the installation.
- You have already read the Prerequisites for Installing the Cisco Nexus 1000V, on page 30.
- You have a copy of the following Cisco Nexus 1000V software image files on your local drive, depending on the installation type you are using:
- For detailed information about using the Deploy OVF Template wizard, see the *vSphere Virtual Machine Administration Guide*.
- You have the following information available for creating a VM for the VSM and mapping the required port groups:
  - A name for the new VSM that is unique within the inventory folder and up to 80 characters.
  - The name of the host where the VSM will be installed in the inventory folder.

- The name of the datastore in which the VM files will be stored.
- The names of the network port groups used for the VM.
- The Cisco Nexus 1000V VSM IP address.

- If you are using the OVA file for installation, make sure that you have the following information available for creating and saving an initial configuration file on the VSM:
  - VSM domain ID
  - Admin password
  - Management IP address, subnet mask, and gateway

Procedure

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

Step 2 In the **Source** screen, specify the location of the OVA file and click **Next.**
The OVF Template Details screen opens displaying product information, including the size of the file and the size of the VM disk.

Step 3 Click **Next.**

Step 4 Read the Cisco Nexus 1000V License Agreement.

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

Step 6 In the **Name:** field, add the VSM name, choose the folder location within the inventory where it will reside, and click **Next.**
The name for the VSM must be unique within the inventory folder and less than 80 characters.

Step 7 From the **Configuration** drop-down list, choose **Nexus 1000V Installer**.
This choice configures the primary VSM using the GUI setup dialog.

Step 8 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.

Format	Description
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.

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).

Step 17 Click **Next.**

Step 18 In the **Ready to Complete** screen, if the configuration is correct, click **Finish**.
A status bar displays as the VM installation progresses.

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)SV2(1.1),
Do you want to reconfigure? (yes/no) [n] yes
          Current vem feature level is set to 4.2(1)SV2(1.1)
          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 44.

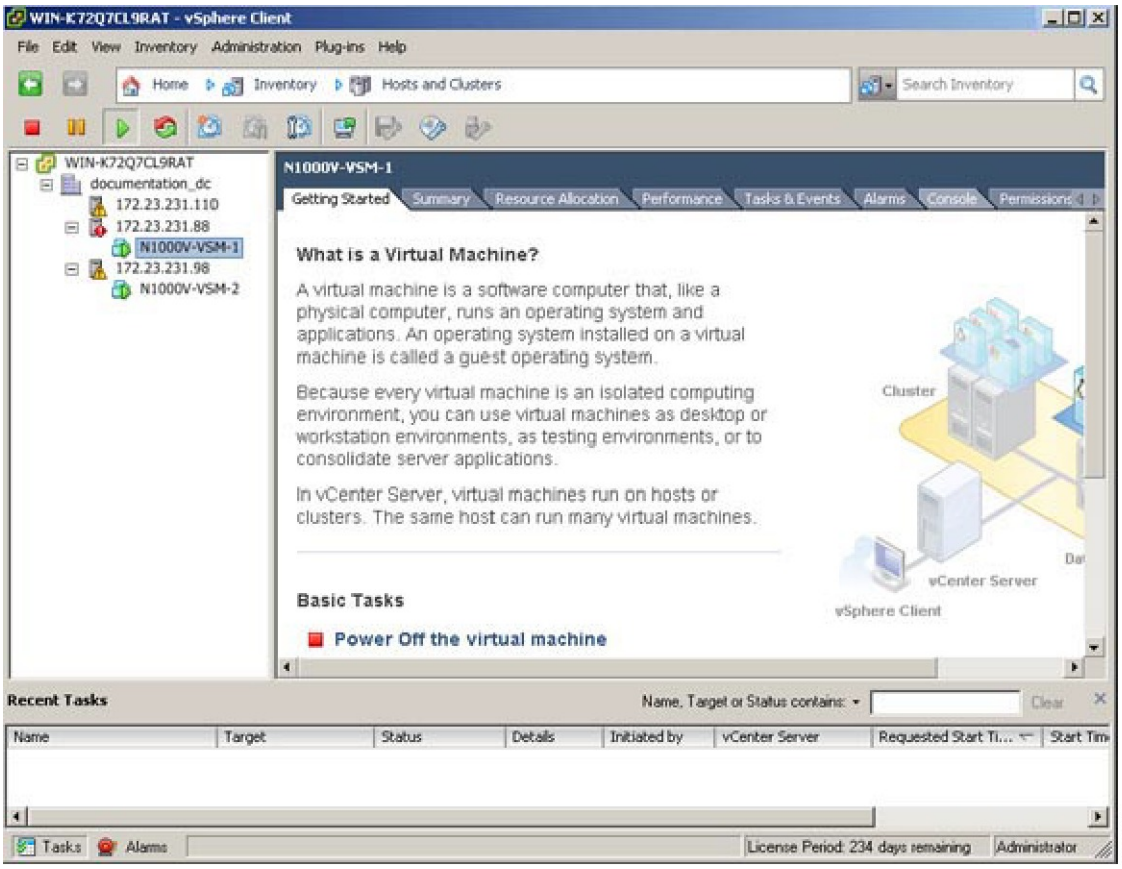
Establishing the SVS Connection

Procedure

Step 1 Open the vSphere Client.

Step 2 Choose the primary VSM.

Figure 9: vSphere Client Window



Step 3 Choose the **Console** tab.

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

Step 5 Open a command window.

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

```
svs connection < Name of the Connection >
      protocol vmware-vim
      remote ip address  <VC Ip address >  port  80
      vmware dvs datacenter-name  <name>
      max-ports 8192
      Connect
```

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

The operational status is Connected.

You have completed establishing the SVS connection.

Setting Virtual Machine Startup and Shutdown Parameters

Before You Begin

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

Procedure

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

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

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

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

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

b) In the System Settings pane, do the following:

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

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

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

d) Click **OK**.

e) Repeat Step 2 through Step 4 for the other VM.

Startup and shutdown settings are complete.

Adding VEM Hosts to the Distributed Virtual Switch

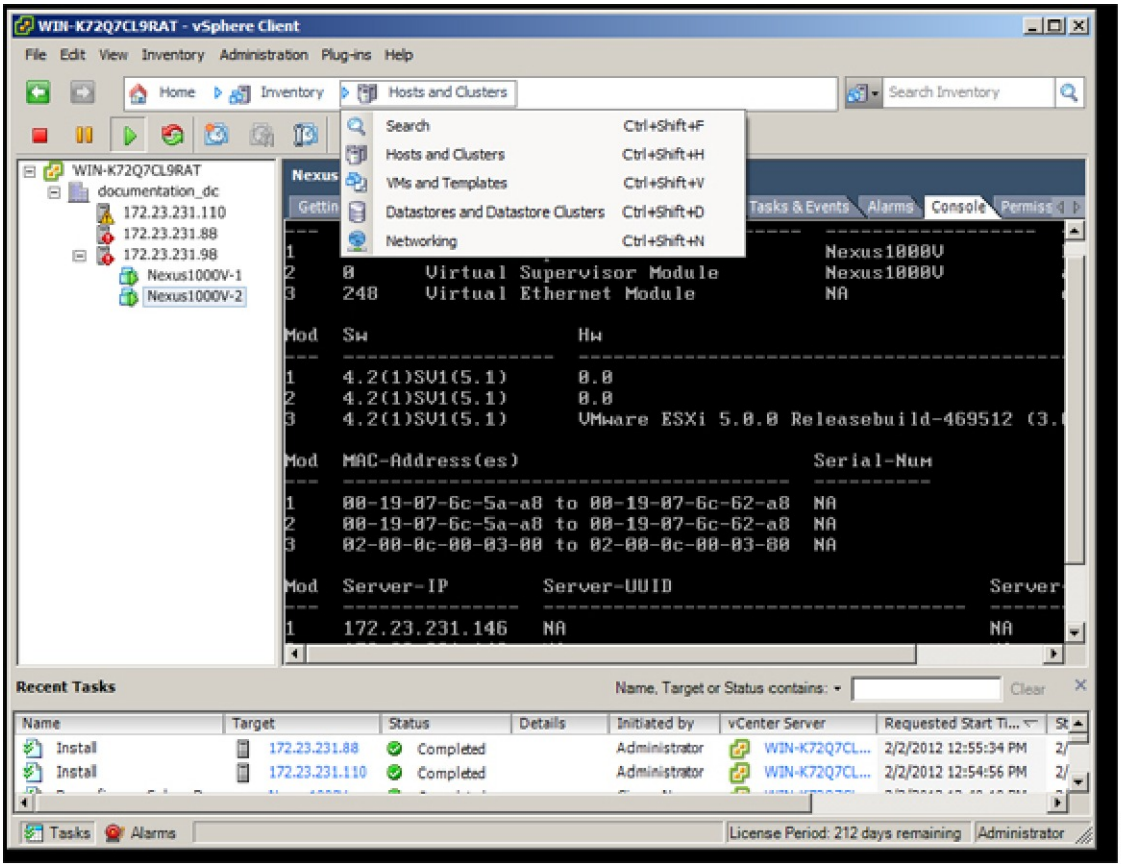
Before You Begin

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

Procedure

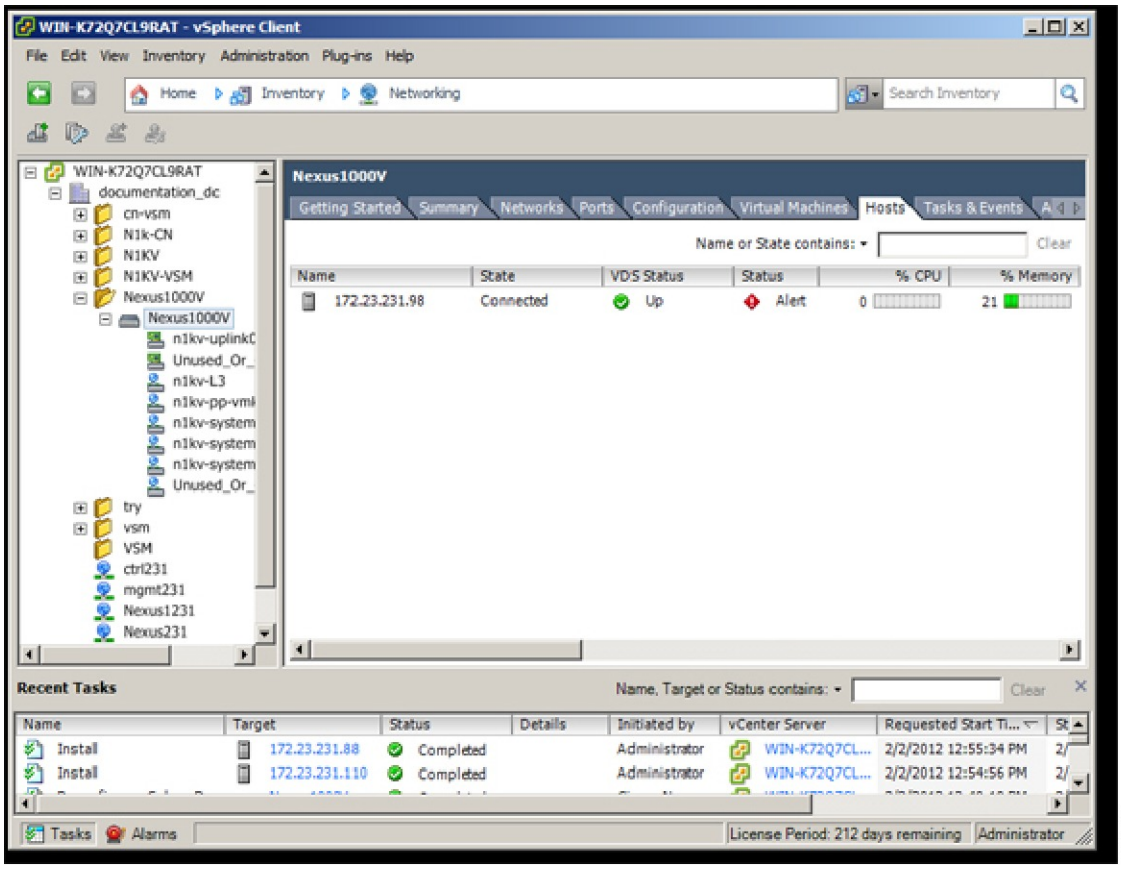
Step 1 In the **vSphere Client** window, choose **Hosts and Clusters > Networking**.

Figure 10: vSphere Client WIndow



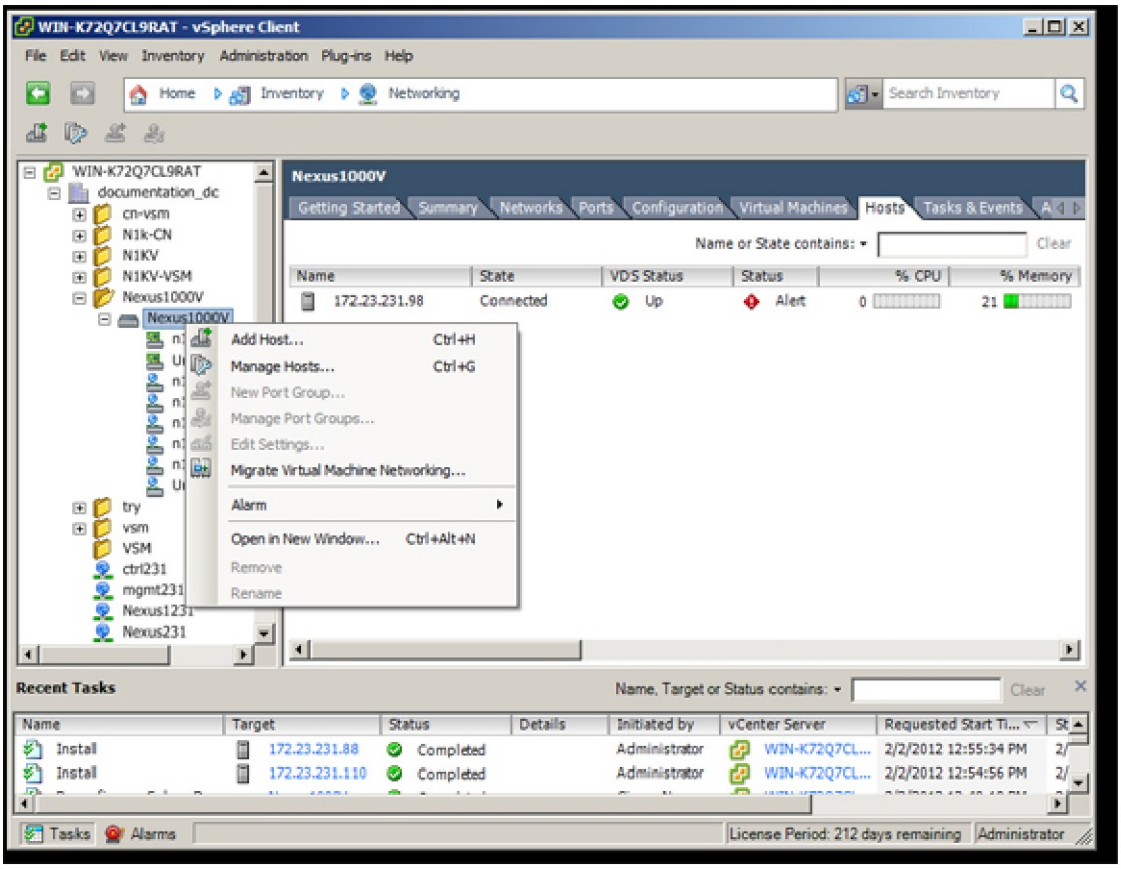
Step 2 In the **vSphere Client Hosts** window, choose the DVS and click the **Hosts** tab.

Figure 11: 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 12: Add Hosts to DVS



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

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

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

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

b) Click **Next**.

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

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

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

The host connection process is complete.

Installing the VEM Software Using VUM

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 32 to ensure that the VUM operation proceeds without failure.

Installing the VEM Software Using the CLI

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

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

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

Procedure

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

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

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

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

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*.

The following example shows how to install VEM software locally on a VMware 5.0 host using the CLI.

```
~ # esxcli software vib install -v /Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1.vib

Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
```

```
   VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1.vib
   VIBs Removed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.1.5.2.0-3.0.1
   VIBs Skipped

~ # vem status -v
Package vssnet-esxmn-release
Version 4.2.1.2.2.2.0-3.0.1
Build 1
Date Sat Jan 25 04:56:14 PDT 2014

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         4           128               1500    vmnic4
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
p-1              256         19          256               1500
vmnic7,vmnic6,vmnic3,vmnic2,vmnic1,vmnic0

VEM Agent (vemdpa) is running

~ # esxcli software vib list | grep cisco
cisco-vem-v164-esx             4.2.1.2.2.2.0-3.0.1               Cisco   PartnerSupported
  2014-01-25
~ #

~ # vemcmd show version
VEM Version: 4.2.1.2.2.2.0-3.0.1
VSM Version: 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
System Version: VMware ESXi 5.0.0 Releasebuild-843203
```

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

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

Procedure

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

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

Note See the official VMware documentation for further information on the **esxcli** command.

Step 3 **esxcli --server=***host_ip_address* **software vib list**
Verify that the VEM software is installed on the host. Look for the installation summary and bulletin ID.

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*.

This example shows how to install VEM software remotely on a VMware 5.0 host using the CLI.

```
vi-admin@localhost:~> esxcli --server=192.0.2.2 software vib
install--depot=/vmfs/volumes/newnfs/MN-patch01/
CY-FCS/VEM500-201401164100-BG-release.zip
Enter username: root
Enter password:
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1
VIBs Removed:
VIBs Skipped:
vi-admin@localhost:~> esxcli --server=192.0.2.1 software vib list
Enter username:
```

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 52.

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 56
- Installing the VEM Software on a Stateless ESXi Host Using VUM, on page 57

Step 3 See the procedure for Configuring Layer 2 Connectivity.

Stateless ESXi Host

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

VMware vSphere 5.0.0 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. The image profile includes base VIBs from VMware and additional VIBs from partners.

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

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

For more information about the VMware Auto Deploy Infrastructure and stateless boot process, see the "Installing ESXi using VMware Auto Deploy" chapter of the *vSphere Installation and Setup, vSphere 5.0.0* 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 into the image profile. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform where VMware PowerCLI is installed, do the following:
  - Download the image profile offline bundle, which is a ZIP file, to a local file path.
  - Download the VEM offline bundle, which is a ZIP file, to a local file path.

Procedure

Step 1 Start the vSphere PowerCLI application.

Step 2 Connect to vCenter Server by entering the following command:
Connect-VIServer *IP_address* **–User Administrator –Password** *XXXXX*.

Step 3 Load the image profile offline bundle by entering the following command:
Add-ESXSoftwareDepot *image_profile_bundle*

Note Each image profile bundle can include multiple image profiles.

Step 4 List the image profiles by entering the following command:
[vSphere PowerCLI] > **Get-EsxImageProfile**

Step 5 Choose the image profile into which the VEM is to be bundled by entering the following command:
New-EsxImageProfile -CloneProfile *image_profile_name* **-Name n1kv-Image**

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

Step 6 change to Load the Cisco Nexus 1000V offline bundle by entering the following command:
Add-EsxSoftwareDepot *VEM_bundle*

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

Step 7 Confirm that the n1kv-vib package is loaded by entering the following command:
Get-EsxSoftwarePackage -Name *cisco**

Step 8 Bundle the n1kv-package into the cloned image profile by entering the following command:
Add-EsxSoftwarePackage -ImageProfile n1kv-Image -SoftwarePackage *n1kv_package_name*

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

a) **$img = Get-EsxImageProfile n1kv-Image**

b) **$img.vibList**

Step 10 Export the image profile to a depot file for future use by entering the following command:
Export-EsxImageProfile –ImageProfile n1kv-Image –FilePath C:\n1kv-Image.zip –ExportToBundle

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

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

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

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

Step 13 Reboot the host.
The host contacts the Auto-Deploy Server and presents the host boot parameters. The Auto Deploy server checks the rules to find the image profile associated with this host and loads the image to the host's memory. The host boots from the image.

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

```
vSphere PowerCLI> Set-ExecutionPolicy unrestricted

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

Working with multiple default servers?

    Select [Y] if you want to work with more than one default servers. In this
case, every time when you connect to a different server using Connect-VIServer,
 the new server connection is stored in an array variable together with the
previously connected servers. When you run a cmdlet and the target servers
cannot be determined from the specified parameters, the cmdlet runs against all
 servers stored in the array variable.
    Select [N] if you want to work with a single default server. In this case,
when you run a cmdlet and the target servers cannot be determined from the
specified parameters, the cmdlet runs against the last connected server.

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

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

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


vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\VMware-ESXi-
5.1.0-799733-depot.zip'

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

```
vSphere PowerCLI>  Get-EsxImageProfile

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.1.0-20121201001s-no-... VMware, Inc.    12/7/2012 7:... PartnerSupported
CN1-CY                         CISCO           4/22/2013 11... PartnerSupported
ESXi-5.1.0-20121204001-stan... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-20121201001s-sta... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-no-tools     VMware, Inc.    8/2/2012 3:0... PartnerSupported
ESXi-5.1.0-20121204001-no-t... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-standard     VMware, Inc.    8/2/2012 3:0... PartnerSupported


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

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

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           8/2/2012 3:0... PartnerSupported


vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\cisco-vem-v1
64-4.2.1.2.2.2.0-3.1.1.zip'

Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\cisco-vem-v1...


vSphere PowerCLI> Get-EsxSoftwarePackage cisco*

Name                     Version                        Vendor     Creation Dat
                                                                   e
----                     -------                        ------     ------------
cisco-vem-v164-esx       4.2.1.2.2.2.0-3.1.1         Cisco      1/24/2014...


vSphere PowerCLI> Add-EsxSoftwarePackage -SoftwarePackage cisco-vem-v164-esx -ImageProfile
 FINAL

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           1/24/2014 3:... PartnerSupported


vSphere PowerCLI> $img = Get-EsxImageProfile FINAL


Name                     Version                        Vendor     Creation Dat
                                                                   e
----                     -------                        ------     ------------
scsi-bnx2i               1.9.1d.v50.1-5vmw.510.0.0.7... VMware     8/2/2012 ...
sata-sata-promise        2.12-3vmw.510.0.0.799733       VMware     8/2/2012 ...
net-forcedeth            0.61-2vmw.510.0.0.799733       VMware     8/2/2012 ...
esx-xserver              5.1.0-0.0.799733               VMware     8/2/2012 ...
misc-cnic-register       1.1-1vmw.510.0.0.799733        VMware     8/2/2012 ...
net-tg3                  3.110h.v50.4-4vmw.510.0.0.7... VMware     8/2/2012 ...
scsi-megaraid-sas        5.34-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-megaraid-mbox       2.20.5.1-6vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-ips                 7.12.05-4vmw.510.0.0.799733    VMware     8/2/2012 ...
net-e1000e               1.1.2-3vmw.510.0.0.799733      VMware     8/2/2012 ...
sata-ahci                3.0-13vmw.510.0.0.799733       VMware     8/2/2012 ...
sata-sata-svw            2.3-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-cnic                 1.10.2j.v50.7-3vmw.510.0.0.... VMware     8/2/2012 ...
net-e1000                8.0.3.1-2vmw.510.0.0.799733    VMware     8/2/2012 ...
```

```
ata-pata-serverworks     0.4.3-3vmw.510.0.0.799733      VMware     8/2/2012 ...
scsi-mptspi              4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...
ata-pata-hpt3x2n         0.3.4-3vmw.510.0.0.799733      VMware     8/2/2012 ...
net-s2io                 2.1.4.13427-3vmw.510.0.0.79... VMware     8/2/2012 ...
esx-base                 5.1.0-0.0.799733               VMware     8/2/2012 ...
net-vmxnet3              1.1.3.0-3vmw.510.0.0.799733    VMware     8/2/2012 ...
net-bnx2                 2.0.15g.v50.11-7vmw.510.0.0... VMware     8/2/2012 ...
cisco-vem-v164-esx       4.2.1.2.2.2.0-3.1.1            Cisco      1/24/2014...
scsi-megaraid2           2.00.4-9vmw.510.0.0.799733     VMware     8/2/2012 ...
ata-pata-amd             0.3.10-3vmw.510.0.0.799733     VMware     8/2/2012 ...
ipmi-ipmi-si-drv         39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-lpfc820             8.2.3.1-127vmw.510.0.0.799733  VMware     8/2/2012 ...
ata-pata-atiixp          0.4.6-4vmw.510.0.0.799733      VMware     8/2/2012 ...
esx-dvfilter-generic-... 5.1.0-0.0.799733               VMware     8/2/2012 ...
net-sky2                 1.20-2vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-qla2xxx             902.k1.1-9vmw.510.0.0.799733   VMware     8/2/2012 ...
net-r8169                6.011.00-2vmw.510.0.0.799733   VMware     8/2/2012 ...
sata-sata-sil            2.3-4vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-mpt2sas             10.00.00.00-5vmw.510.0.0.79... VMware     8/2/2012 ...
sata-ata-piix            2.12-6vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-hpsa                5.0.0-21vmw.510.0.0.799733     VMware     8/2/2012 ...
ata-pata-via             0.3.3-2vmw.510.0.0.799733      VMware     8/2/2012 ...
scsi-aacraid             1.1.5.1-9vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-rste                2.0.2.0088-1vmw.510.0.0.799733 VMware     8/2/2012 ...
ata-pata-cmd64x          0.2.5-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ima-qla4xxx              2.01.31-1vmw.510.0.0.799733    VMware     8/2/2012 ...
net-igb                  2.1.11.1-3vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-qla4xxx             5.01.03.2-4vmw.510.0.0.799733  VMware     8/2/2012 ...
block-cciss              3.6.14-10vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-aic79xx             3.1-5vmw.510.0.0.799733        VMware     8/2/2012 ...
tools-light              5.1.0-0.0.799733               VMware     8/2/2012 ...
uhci-usb-uhci            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
sata-sata-nv             3.5-4vmw.510.0.0.799733        VMware     8/2/2012 ...
sata-sata-sil24          1.1-1vmw.510.0.0.799733        VMware     8/2/2012 ...
net-ixgbe                3.7.13.6iov-10vmw.510.0.0.7... VMware     8/2/2012 ...
ipmi-ipmi-msghandler     39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-adp94xx             1.0.8.12-6vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-fnic                1.5.0.3-1vmw.510.0.0.799733    VMware     8/2/2012 ...
ata-pata-pdc2027x        1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
misc-drivers             5.1.0-0.0.799733               VMware     8/2/2012 ...
net-enic                 1.4.2.15a-1vmw.510.0.0.799733  VMware     8/2/2012 ...
net-be2net               4.1.255.11-1vmw.510.0.0.799733 VMware     8/2/2012 ...
net-nx-nic               4.0.558-3vmw.510.0.0.799733    VMware     8/2/2012 ...
esx-xlibs                5.1.0-0.0.799733               VMware     8/2/2012 ...
net-bnx2x                1.61.15.v50.3-1vmw.510.0.0.... VMware     8/2/2012 ...
ehci-ehci-hcd            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
ohci-usb-ohci            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-r8168                8.013.00-3vmw.510.0.0.799733   VMware     8/2/2012 ...
esx-tboot                5.1.0-0.0.799733               VMware     8/2/2012 ...
ata-pata-sil680          0.4.8-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ipmi-ipmi-devintf        39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-mptsas              4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...
```

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

Installing the VEM Software on a Stateless ESXi Host Using esxcli

Before You Begin

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

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

Procedure

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

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

Step 2 Log in to the ESXi stateless host.

Step 3 Copy the offline bundle to the host by entering the the following command:
esxcli software vib install -d *file_path/offline_bundle*

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

Step 4 Verify that the VIB has installed by entering the following command:
esxcli software vib list | grep cisco

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

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

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

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

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

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

```
~ # vmware -v
VMware ESXi 5.0.0 build-843203
~ #
~ # vmware -l
VMware ESXi 5.0.0 U2

~ # esxcli software vib install –d
/vmfs/volumes/newnfs/MN-VEM/VEM500-201401164100-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-v164-esx_4.2.1.2.2.2.0-3.0.1
VIBs Removed:
VIBs Skipped:
```

```
~ # esxcli software vib list | grep cisco
cisco-vem-v164-esx     4.2.1.2.2.2.0-3.0.1                Cisco   PartnerSupported
2014-01-24

~ # vem status -v
Package vssnet-esxmn-release
Version 4.2.1.2.2.2.0-3.0.1
Build 1
Date Sat Jan 24 04:56:14 PDT 2014
VEM modules are loaded
Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         4           128               1500    vmnic4
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
p-1              256         19          256               1500
vmnic7,vmnic6,vmnic3,vmnic2,vmnic1,vmnic0
 VEM Agent (vemdpa) is running

~ # vemcmd show version
vemcmd show version
VEM Version: 4.2.1.2.2.2.0-3.0.1
VSM Version: 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
System Version: VMware ESXi 5.0.0 Releasebuild-843203

p-1# show module
Mod  Ports  Module-Type                       Model               Status
---  -----  --------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module         Nexus1000V          active *
2    0      Virtual Supervisor Module         Nexus1000V          ha-standby
3    332    Virtual Ethernet Module           NA                  ok
6    248    Virtual Ethernet Module           NA                  ok

Mod    Sw                Hw
---  ----------------  ------------------------------------------------
4.2(1) SV2(2.2)        0.0
4.2(1) SV2(2.2)        0.0
3      4.2(1)SV2(2.2)      VMware ESXi 5.0.0 Releasebuild-843203 (3.0)
6      4.2(1)SV2(2.2)      VMware ESXi 5.1.0 Releasebuild-843203 (3.0)

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.105.232.25    NA                                    NA
2    10.105.232.25    NA                                    NA
3    10.105.232.72    e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba  10.105.232.72
6    10.105.232.70    ecebdf42-bc0e-11e0-bd1d-30e4dbc2b892  10.105.232.70
```

Installing the VEM Software on a Stateless ESXi Host Using VUM

Before You Begin

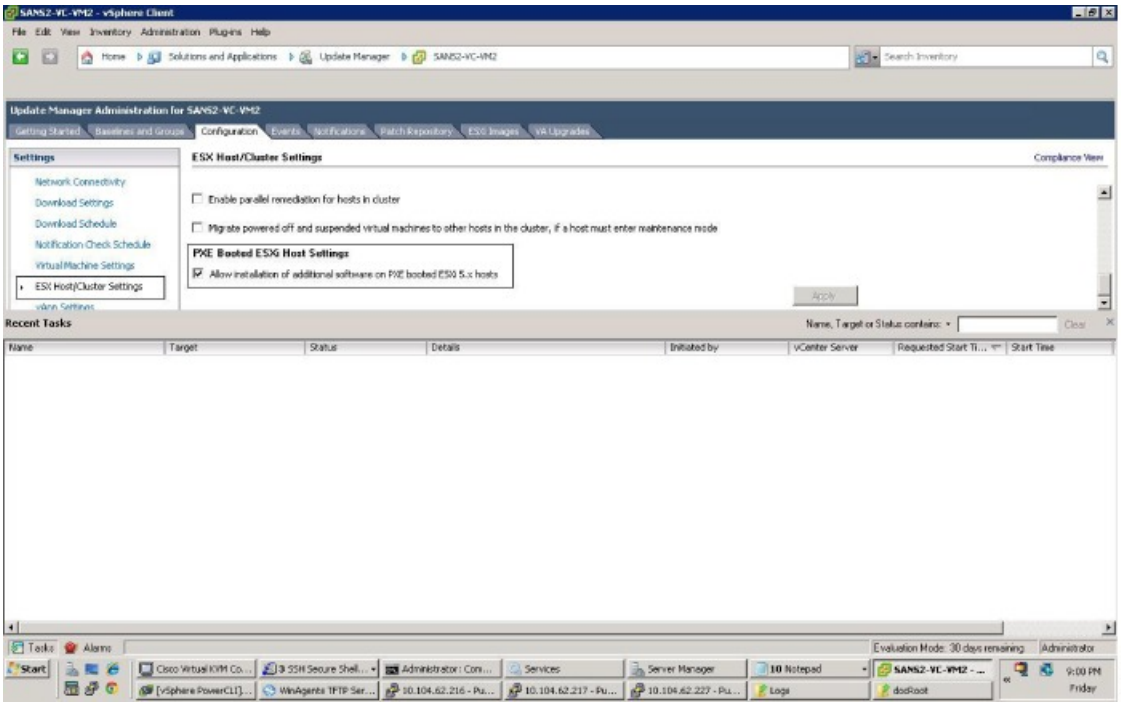
- Make sure that the VUM patch repository has the VEM software downloaded.

Procedure

Step 1 In vCenter Server, choose **Home > Update Manager > Configuration > ESX host/Cluster** settings. The ESX Host/Cluster Settings window opens.

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

Figure 13: ESX Host/Cluster Settings Window



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

Installing a VSM on the Cisco Nexus Cloud Services Platform

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

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

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

Before You Begin

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

Procedure

Step 1 Create a virtual service blade.

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

------------------------------------------------------------------------------
Name        HA-Role       HA-Status     Status               Location
------------------------------------------------------------------------------
switch(config)# virtual-service-blade vsm-1
switch(config-vsb-config)# virtual-service-blade-type new nexus-1000v.4.2.1.SV2.2.2.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.SV2.2.2.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 the Cisco Nexus 1000V.

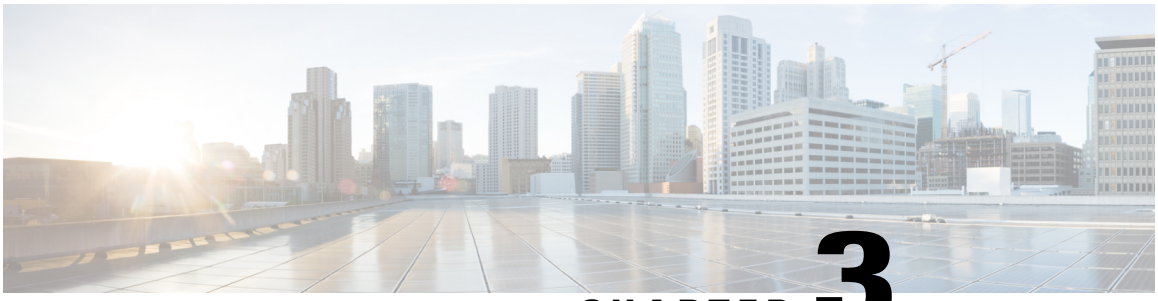
Note The configuration in the highlighted code is optional.

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

Feature History for Installing the Cisco Nexus 1000V

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

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



CHAPTER 3

Upgrading the Cisco Nexus 1000V

This chapter contains 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 this table:

Table 3: Obtaining the Upgrade Software

Source	Description
Cisco	Download the current release of the Cisco Nexus 1000V software from http://www.cisco.com/en/US/products/ps9902/index.html.
VMware	Download the VMware software from the VMware website. The current Cisco Nexus 1000V software release 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 the *Cisco Nexus 1000V and VMware Compatibility Information* document.

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 the current release.
- 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 Virtual Ethernet Module (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 VEM vSphere Installation Bundle (VIB) while the host is still in maintenance mode.

4 Remove the host from maintenance mode.

The steps for the manual combined upgrade procedure do not apply for VMware Update Manager (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.
- 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 Cisco Integrated Management Control (CIMC), do not initiate commands that are CPU intensive, such as copying image from the TFTP server to bootflash or generating 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 VMware vCenter Server is hosted on the same ESX/ESXi host as a Cisco Nexus 1000V VEM, a VUM-assisted upgrade on the host fails. 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 Cisco Nexus 1000V Download Software page. For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information* document.
- 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 the **portfast trunk** command or the **portfast edge trunk** command.
  - On Cisco Nexus 5000 Series switches with the 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:
  - **spanning-tree bpdu filter**
  - **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 We recommended that you use vSphere 5.0 Update 1 or later instead of vSphere 5.0.

- You are upgrading the Cisco Nexus 1000V software to the current release.
- 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 **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 ESX hosts 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.

Before upgrading the VEMs, note these guidelines and limitations.

Note It is your responsibility to monitor and install all the relevant patches on VMware ESX hosts.

- 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).
- 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* document.

- 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 5.1 release (799733), the minimum versions are as follows:

- VMware vCenter Server 5.1, 799731
- VMware Update Manager 5.1, 782803

For the ESXi 5.0.0 release, 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.

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.

- You can upgrade the hosts in the DVS a few at a time across multiple maintenance windows. The only exception is if you are upgrading the VEM alone using VUM with the ESX version unchanged.

Upgrade Procedures

The following table lists the upgrade steps.

Note Ensure that you have changed the VSM mode to advanced, before upgrading VSM. VSG services are not available in the essential mode.

Table 4: 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(3x) Series	**1** Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b) **2** Upgrade from Releases 4.2(1)SV1(4x) and later releases to the current release

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4x) Series with a vSphere release 4.0 Update 1 or later	**1** Upgrading from VMware Release 4.0 to VMware Release 4.1 **2** Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release **3** Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release
Release 4.2(1)SV1(4x) Series with a vSphere release 4.1 GA, patches, or updates	**1** Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release **2** Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release
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) and later releases to the current release **2** Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release

The following table lists the upgrade steps when upgrading from Release 4.2(1)SV1(5x) and later releases to the current release.

Table 5: Upgrade Paths from Releases 4.2(1)SV1(5x) and Later Releases

If you are running this configuration	Follow these steps
With vSphere 4.1 GA, patches, or updates.	**1** Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release **2** Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release
With vSphere 5.0 GA, patches, or updates.	**1** Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release **2** Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release
With ESX version upgrade.	Installing and Upgrading VMware

Upgrade Types

Upgrades can be one of three types:

- Upgrade of the Cisco Nexus 1000V version only, with vSphere version intact. See Upgrading the Cisco Nexus 1000V Only, on page 70.
- Upgrade of both vSphere and Cisco Nexus 1000V versions together. See Combined Upgrade of vSphere and Cisco Nexus 1000V, on page 70.
- Upgrade of vSphere version only, with the Cisco Nexus 1000V version intact. See the Installing and Upgrading VMware, on page 107 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 51.
   - 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.x, on page 113.
   - For a stateful manual upgrade using the **esxupdate** or **esxcli** commands, see Installing ESXi 5.1 Host Software Using the CLI, on page 119.

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 Starting with the current release, during an VSM upgrade, if you have incompatible hosts attached to the VSM you will be allowed to upgrade from the current release of Cisco Nexus 1000V software to the later releases. You will see a warning message on incompatible host when you upgrade. Ignore the warning message and continue with the upgrade and the VSM will be upgraded to the latest version. You can perform a combined upgrade on the incompatible hosts.

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

The following procedures are necessary to perform a combined upgrade.

1 Upgrading the vCenter Server, on page 83
2 Upgrading the vCenter Update Manager to Release 5.5, on page 111
3 Upgrading VSMs from Releases 4.2(1)SV1(4x), 4.2(1)SV1(5x), 4.2(1)SV2(1.1x) to Release 4.2(1)SV2(2.2)
4 Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, on page 80
5 Upgrading the ESXi Hosts to Release 5.x, on page 113
6 Verifying the Build Number and Upgrade

Reserving the Memory and CPU on the Virtual Supervisor Module Virtual Machine

From the current release of Cisco Nexus 1000V software, VSM requires 4 GB RAM and 2048 MHz of CPU reservation to accommodate the new scalability limits.

Note When you install the Cisco Nexus 1000V software VSM through the OVA files for the first time, the RAM and CPU reservations are automatically reflected.

To upgrade to the current release of Cisco Nexus 1000V software and update the CPU and RAM reservations, use the following procedure:

Procedure

Step 1 Upgrade from the previous release of Cisco Nexus 1000V software to the current release of Cisco Nexus 1000V software. For information on how to upgrade, see Upgrading VSMs from Releases 4.2(1)SV1(4) and Later Releases to Release 4.2(1)SV2(2.x) Series

Step 2 Once the upgrade is complete, power off the secondary VSM.

Step 3 Change the RAM size from 2GB/3GB to 4 GB and change the RAM reservation from 2GB/3GB to 4 GB.

Step 4 Change the CPU reservation from 1.5 to 2048 MHz.

Step 5 Power on the secondary VSM.

Step 6 Perform a system switch over to get the secondary VSM as Active.

Step 7 Power off the primary VSM and repeat steps 3 to 6.

Step 8 Once the primary and secondary VSM have the correct CPU and RAM reservations, the VSM should now accommodate 256 VEM modules and 12000 interfaces.

Note You do not have to change the CPU and RAM reservations to continue support for 64 VEM Modules and 2000 veth interfaces .

Reserving the Memory and CPU for the Virtual Supervisor Module in VSB on the Cloud Services Platform

To change the memory reservations in the VSM VSB, use the following procedure:

Note You do not need to reserve the CPU or vCPU on this VSM.

Before You Begin

From the current release of Cisco Nexus 1000V software, VSM requires 3 GB RAM reservation to accommodate the new scalability limits.

Procedure

Step 1 Login to the Cloud Services Platform command prompt.

Step 2 Enter the VSM configuration mode.

Step 3 Change the RAM size from 2 to 3 GB.

Note With Cisco Nexus Cloud Services Platform Release 4.2(1)SP1(6.1) and later, the virtual service blades can remain powered on when you change the RAM size. In Cisco Nexus Cloud Services Platform releases earlier than 4.2(1)SP1(6.1), the primary/secondary virtual service blades must be powered off before you can change the RAM size.

Step 4 Copy the running configuration to the startup configuration.

Step 5 Reboot the secondary VSM VSB by using the **shut** and **no shut** commands.

Step 6 Check if the secondary VSM has 3 GB of RAM reservation.

Step 7 Perform a system switch over from primary VSM to make the secondary VSM as active with 3 GB RAM. The primary VSM reboots and is in the standby state with 3 GB RAM.

Reserving the Memory and CPU for the Virtual Supervisor Module in VSB on the Cloud Services Platform Using the CLI

To change the memory reservations in the VSM VSB using the CLI, use the following procedure:

Before You Begin

From the current release of Cisco Nexus 1000V software, VSM requires 3 GB RAM reservation to accommodate the new scalability limits.

Procedure

	Command or Action	Purpose
Step 1	CSP **configure terminal**	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	CSP(config)# **virtual-service-blade** *VSM for the current release*	Enters the VSM configuration mode.
Step 3	CSP(config-vsb-config)# **ramsize** *3072*	Change the RAM size from 2 to 3 GB. **Note** The virtual service blade is powered ON. Restart the VSB to reflect the change in RAM size. Perform a shutdown using the **shutdown** and **no shutdown** commands.
Step 4	CSP(config-vsb-config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.
Step 5	CSP(config-vsb-config)# **shutdown secondary**	Shuts down the secondary VSB.
Step 6	CSP(config-vsb-config)# **no shutdown secondary**	Applies the RAM changes.
Step 7	VSM# **system switchover**	Performs a system switch over from primary VSM to make the secondary VSM as active with 3 GB RAM.
Step 8	**VSM(standby)# show system resources**	Displays if the secondary VSM has 3 GB of RAM reservation.

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 the current release of Cisco Nexus 1000V using ISO files is not supported. You must use kickstart and system files to perform an ISSU upgrade to the current release of Cisco Nexus 1000V.

The Cisco Nexus 1000V software supports in-service software upgrades (ISSUs) for systems with dual VSMs. An ISSU can update the software images on your switch without disrupting data traffic. Only control traffic is disrupted. If an ISSU causes a disruption of data traffic, the Cisco Nexus 1000V software warns you before proceeding so that you can stop the upgrade and reschedule it to a time that minimizes the impact on your network.

Note On systems with dual VSMs, you should have access to the console of both VSMs to maintain connectivity when the switchover occurs during upgrades. If you are performing the upgrade over Secure Shell (SSH) or Telnet, the connection will drop when the system switchover occurs, and you must reestablish the connection.

An ISSU updates the following images:

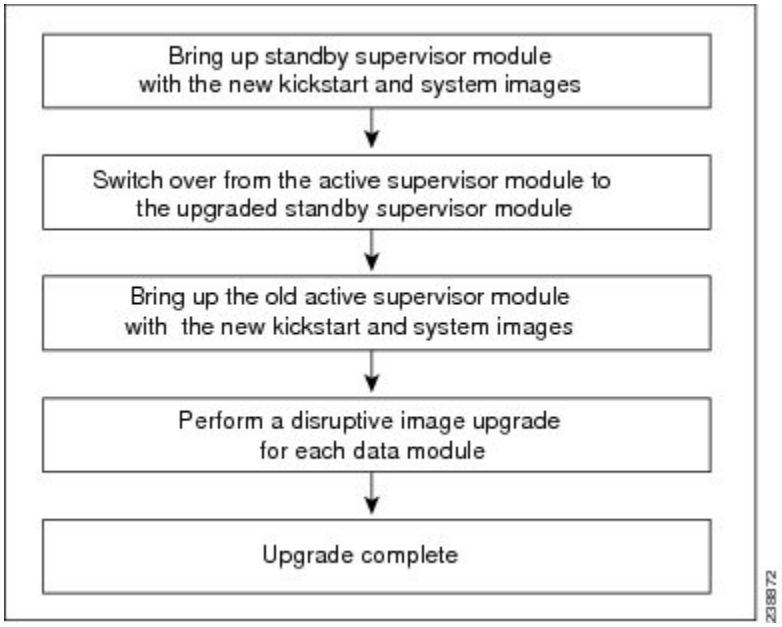
- Kickstart image
- System image
- VEM images

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.

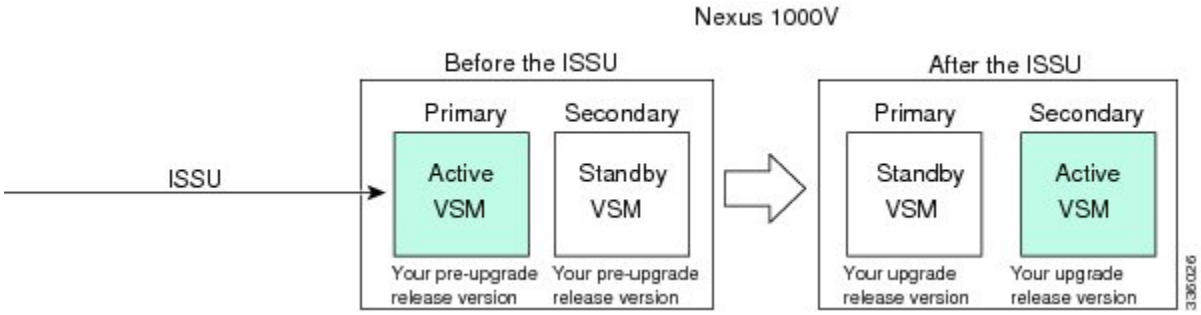
Figure 14: ISSU Process



ISSU VSM Switchover

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

Figure 15: 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) and Later Releases to Release 4.2(1)SV2(2.x) Series

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 by entering the **dir bootflash:** command.

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 by entering the **dir bootflash://sup-standby/** command .

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 copies a kickstart and system image using 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.

a) switch# **copy scp://***filepath/kickstart_filename* **bootflash:***kickstart_filename*
Copy the ISO image.

b) switch# **copy scp://***filepath/system_filename* **bootflash:***system_filename*
Copy kickstart and system images.

Step 10 switch# **show install all impact kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename*
Verify the ISSU upgrade for the kickstart and system images or the ISO image. The example in this procedure shows the kickstart and system images.

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

Step 12 Determine if the Cisco Virtual Security Gateway (Cisco VSG) is configured in the deployment by using the **show vnm-pa status** command .

Note If an output displaying a successful installation is displayed as in the example, 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*. If an output displaying that the policy agent has not installed is displayed, continue to Step 13.

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

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

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*.

a) Save the running configuration on the bootflash by using the **copy running-config bootflash:run-cfg-backup** command.

b) Save the running configuration externally by using the **copy running-config scp://***external_backup_location* command.

Step 15 Perform the upgrade on the active VSM using the ISO or kickstart and system images by using the **install all kickstart bootflash:***kickstart_filename* **system bootflash:***system_filename* command. The example in this procedure shows the kickstart and system images.

Step 16 Continue with the installation by pressing Y.
If you press N, the installation exits gracefully.

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.

Step 17 After the installation operation completes, log in and verify that the switch is running the required software version by using the switch# **show version** command

Step 18 Copy the running configuration to the startup configuration to adjust the startup-config size by using the switch# **copy running-config startup-config** command

Step 19 Display the log for the last installation by entering the following commands.

a) switch# **show install all status**

b) switch# **attach** *module_name*

c) switch# **show install all status**

Step 20 Review information about reserving memory and CPU on the VSM VM at the following URL: Reserving the Memory and CPU on the Virtual Supervisor Module Virtual Machine, on page 71.

Note You must review this information, to accommodate the new scalability limits.

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 80.
  - Set up VUM baselines. See http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_2/install_upgrade/vsm_vem/guide/b_Installation_and_Upgrade_Release_4_2_1SV1_5_2_appendix_0100.html#task_A93C11451B0B43F98468D15C83C1E5E5.
  - Initiate an upgrade from VUM. See Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4x), and Later Releases to the Current Release, on page 85.

- Upgrade VEM from VSM. See Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4x), and Later Releases to the Current Release, on page 85.

- Manual upgrade procedures
  - Upgrading VIB Manually from the CLI. See Upgrading the VEMs Manually from Release 4.2(1)SV1(4x), Release and Later Releases to the Current Release, on page 91

- Installing or upgrading stateless ESXi. See Installing the VEM Software on a Stateless ESXi Host, on page 51.

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 51.
- 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.

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(4x), and Later Releases to the Current Release, on page 85.

If you are upgrading from the command line, see Upgrading the VEMs Manually from Release 4.2(1)SV1(4x), Release and Later Releases to the Current Release, on page 91.

- 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 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 80.
  - 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.

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.

Procedure

Step 1 Start the VMWare PowerCLI application.

Step 2 Connect to the vCenter Server by using the **Connect-VIServer** *IP_address* **-User Administrator -Password** *password_name* command.

Step 3 Load the ESX depot by using the **Add-ESXSoftwareDepot** *path_name\file_name* command.

Step 4 Display the image profiles by using the **Get-EsxImageProfile** command.

Step 5 Clone the ESX standard image profile by using the **New-ESxImageProfile -CloneProfile** *ESXImageProfile_name* **-Name** *clone_profile* command.

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

Step 6 Load the Cisco Nexus 1000V VEM offline bundle by using the **Add-EsxSoftwareDepot** *VEM_offline_bundle* command.

Step 7 Confirm that the n1kv-vib package is loaded by using the **Get-EsxSoftwarePackage -Name** *package_name* command.

Step 8 Bundle the n1kv-package into the cloned image profile by using the **Add-EsxSoftwarePackage -ImageProfile** *n1kv-Image* **-SoftwarePackage** *cloned_image_profile* command.

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

a) **$img = Get-EsxImageProfile** *n1kv-Image*

b) **$img.vibList**

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

Step 10 Export the image profile to an ISO file by using the **Export-EsxImageProfile -ImageProfile** *n1kv-Image* **-FilePath** *iso_filepath* command.

This example shows how to create an upgrade ISO with a VMware ESX image and a Cisco VEM image.

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

```
vSphere PowerCLI> Connect-VIServer 10.105.231.40 -User administrator -Password 'XXXXXXXX'

Working with multiple default servers?

    Select [Y] if you want to work with more than one default servers. In this
case, every time when you connect to a different server using Connect-VIServer,
 the new server connection is stored in an array variable together with the
previously connected servers. When you run a cmdlet and the target servers
cannot be determined from the specified parameters, the cmdlet runs against all
 servers stored in the array variable.
    Select [N] if you want to work with a single default server. In this case,
when you run a cmdlet and the target servers cannot be determined from the
specified parameters, the cmdlet runs against the last connected server.

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

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

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

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\VMware-ESXi-5.1.0-799733-depot.zip'

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

vSphere PowerCLI> Get-EsxImageProfile

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.1.0-20121201001s-no-... VMware, Inc.    12/7/2012 7:... PartnerSupported
CN1-CY                         CISCO           4/22/2013 11... PartnerSupported
ESXi-5.1.0-20121204001-stan... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-20121201001s-sta... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-no-tools     VMware, Inc.    8/2/2012 3:0... PartnerSupported
ESXi-5.1.0-20121204001-no-t... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-standard     VMware, Inc.    8/2/2012 3:0... PartnerSupported

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

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

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           8/2/2012 3:0... PartnerSupported

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229
\cisco-vem-v164-4.2.1.2.2.2.0-3.1.1.zip'

Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\cisco-vem-v1...

vSphere PowerCLI> Get-EsxSoftwarePackage cisco*
```

```
Name                      Version                         Vendor     Creation Dat
                                                                     e
----                      -------                         ------     ------------
cisco-vem-v164-esx        4.2.1.2.2.2.0-3.1.1          Cisco      1/24/2014...

vSphere PowerCLI> Add-EsxSoftwarePackage -SoftwarePackage cisco-vem-v164-esx -ImageProfile
 FINAL

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           1/24/2014 3:... PartnerSupported

vSphere PowerCLI> $img = Get-EsxImageProfile FINAL

vSphere PowerCLI> $img.vibList

Name                      Version                         Vendor     Creation Dat
                                                                     e
----                      -------                         ------     ------------
scsi-bnx2i                1.9.1d.v50.1-5vmw.510.0.0.7... VMware     8/2/2012 ...
sata-sata-promise         2.12-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-forcedeth             0.61-2vmw.510.0.0.799733        VMware     8/2/2012 ...
esx-xserver               5.1.0-0.0.799733                VMware     8/2/2012 ...
misc-cnic-register        1.1-1vmw.510.0.0.799733         VMware     8/2/2012 ...
net-tg3                   3.110h.v50.4-4vmw.510.0.0.7... VMware     8/2/2012 ...
scsi-megaraid-sas         5.34-4vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-megaraid-mbox        2.20.5.1-6vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-ips                  7.12.05-4vmw.510.0.0.799733     VMware     8/2/2012 ...
net-e1000e                1.1.2-3vmw.510.0.0.799733       VMware     8/2/2012 ...
sata-ahci                 3.0-13vmw.510.0.0.799733        VMware     8/2/2012 ...
sata-sata-svw             2.3-3vmw.510.0.0.799733         VMware     8/2/2012 ...
net-cnic                  1.10.2j.v50.7-3vmw.510.0.0.... VMware     8/2/2012 ...
net-e1000                 8.0.3.1-2vmw.510.0.0.799733     VMware     8/2/2012 ...
ata-pata-serverworks      0.4.3-3vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-mptspi               4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...
ata-pata-hpt3x2n          0.3.4-3vmw.510.0.0.799733       VMware     8/2/2012 ...
net-s2io                  2.1.4.13427-3vmw.510.0.0.79... VMware     8/2/2012 ...
esx-base                  5.1.0-0.0.799733                VMware     8/2/2012 ...
net-vmxnet3               1.1.3.0-3vmw.510.0.0.799733     VMware     8/2/2012 ...
net-bnx2                  2.0.15g.v50.11-7vmw.510.0.0... VMware     8/2/2012 ...
cisco-vem-v164-esx        4.2.1.2.2.2.0-3.1.1             Cisco      1/24/2014...
scsi-megaraid2            2.00.4-9vmw.510.0.0.799733      VMware     8/2/2012 ...
ata-pata-amd              0.3.10-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ipmi-ipmi-si-drv          39.1-4vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-lpfc820              8.2.3.1-127vmw.510.0.0.799733  VMware     8/2/2012 ...
ata-pata-atiixp           0.4.6-4vmw.510.0.0.799733       VMware     8/2/2012 ...
esx-dvfilter-generic-... 5.1.0-0.0.799733                VMware     8/2/2012 ...
net-sky2                  1.20-2vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-qla2xxx              902.k1.1-9vmw.510.0.0.799733    VMware     8/2/2012 ...
net-r8169                 6.011.00-2vmw.510.0.0.799733    VMware     8/2/2012 ...
sata-sata-sil             2.3-4vmw.510.0.0.799733         VMware     8/2/2012 ...
scsi-mpt2sas              10.00.00.00-5vmw.510.0.0.79... VMware     8/2/2012 ...
sata-ata-piix             2.12-6vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-hpsa                 5.0.0-21vmw.510.0.0.799733      VMware     8/2/2012 ...
ata-pata-via              0.3.3-2vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-aacraid              1.1.5.1-9vmw.510.0.0.799733     VMware     8/2/2012 ...
scsi-rste                 2.0.2.0088-1vmw.510.0.0.799733 VMware     8/2/2012 ...
ata-pata-cmd64x           0.2.5-3vmw.510.0.0.799733       VMware     8/2/2012 ...
ima-qla4xxx               2.01.31-1vmw.510.0.0.799733     VMware     8/2/2012 ...
net-igb                   2.1.11.1-3vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-qla4xxx              5.01.03.2-4vmw.510.0.0.799733  VMware     8/2/2012 ...
block-cciss               3.6.14-10vmw.510.0.0.799733     VMware     8/2/2012 ...
scsi-aic79xx              3.1-5vmw.510.0.0.799733         VMware     8/2/2012 ...
tools-light               5.1.0-0.0.799733                VMware     8/2/2012 ...
uhci-usb-uhci             1.0-3vmw.510.0.0.799733         VMware     8/2/2012 ...
sata-sata-nv              3.5-4vmw.510.0.0.799733         VMware     8/2/2012 ...
sata-sata-sil24           1.1-1vmw.510.0.0.799733         VMware     8/2/2012 ...
net-ixgbe                 3.7.13.6iov-10vmw.510.0.0.7... VMware     8/2/2012 ...
ipmi-ipmi-msghandler      39.1-4vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-adp94xx              1.0.8.12-6vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-fnic                 1.5.0.3-1vmw.510.0.0.799733     VMware     8/2/2012 ...
ata-pata-pdc2027x         1.0-3vmw.510.0.0.799733         VMware     8/2/2012 ...
misc-drivers              5.1.0-0.0.799733                VMware     8/2/2012 ...
```

```
net-enic                1.4.2.15a-1vmw.510.0.0.799733  VMware     8/2/2012 ...
net-be2net              4.1.255.11-1vmw.510.0.0.799733 VMware     8/2/2012 ...
net-nx-nic              4.0.558-3vmw.510.0.0.799733    VMware     8/2/2012 ...
esx-xlibs               5.1.0-0.0.799733               VMware     8/2/2012 ...
net-bnx2x               1.61.15.v50.3-1vmw.510.0.0.... VMware     8/2/2012 ...
ehci-ehci-hcd           1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
ohci-usb-ohci           1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-r8168               8.013.00-3vmw.510.0.0.799733   VMware     8/2/2012 ...
esx-tboot               5.1.0-0.0.799733               VMware     8/2/2012 ...
ata-pata-sil680         0.4.8-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ipmi-ipmi-devintf       39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-mptsas             4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...

vSphere PowerCLI> Export-EsxImageProfile -ImageProfile FINAL -FilePath 'C:\Documents and
Settings\Administrator\Desktop\FINAL.iso' -ExportToIso
```

Upgrading the vCenter Server

Note This upgrade procedure applies to vCenter Server 5.0, 5.0 Update 1 and later, 5.1, and 5.5 versions.

Before You Begin

- Download the upgrade ISO file that contains your desired ESXi image and the desired Cisco Nexus 1000V image.
- 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 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** screen, 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** screen, click **Next.**

Step 8 In the **License Agreement** screen, 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** screen, 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 your desired ESXi version.

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 the same VMware versions.

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 5.5, on page 111.

Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4x), and Later Releases to the Current Release

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 switch# **show vmware vem upgrade status**
Display the current configuration.

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

Step 2 switch# **vmware vem upgrade notify**
Coordinate with and notify the server administrator of the VEM upgrade process.

Step 3 switch# **show vmware vem upgrade status**
Verify that the upgrade notification was sent.

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 switch# **show vmware vem upgrade status**
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 88. Coordinate the notification acceptance with the server administrator. After the server administrator accepts the upgrade, proceed with the VEM upgrade.

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 with the following commands.

Note Before entering the following commands, 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.

a) switch# **vmware vem upgrade proceed**
b) switch# **show vmware vem upgrade status**

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 switch# **show vmware vem upgrade status**
Check for the upgrade complete status.

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

a) switch# **vmware vem upgrade complete**

b) switch# **show vmware vem upgrade status**

Step 8 switch# **show module**
Verify that the upgrade process is complete.

The upgrade is complete.

The following example shows how to upgrade VEMs using VUM.

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

```
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: VEM500-201401164100-BG
    DVS: VEM410-201301152101-BG
switch#
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.
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM:  VEM500-201401164100-BG
    DVS:  VEM410-201301152101-BG
switch#
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jan 27 02:06:53 2014
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201401164100-BG
    DVS: VEM410-201301152101-BG
switch#
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: Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter) : Tue Jan 27 02:06:53 2014
```

```
Upgrade Start Time: : Tue Jan 27 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201401164100-BG
    DVS: VEM500-201401164100-BG
switch#
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: : Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter): : Tue Jan 27 02:06:53 2014
Upgrade Start Time: : Tue Jan 27 10:09:08 2013
Upgrade End Time(vCenter): : Tue Jan 27 10:09:08 2014
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201401164100-BG
    DVS: VEM500-201401164100-BG
switch#
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: VEM500-201401164100-BG
    DVS: VEM500-201401164100-BG
switch#
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)SV2(2.2)    0.0
2    4.2(1)SV2(2.2)    0.0
3    4.2(1)SV2(2.2)    VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV2(2.2)    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 the current release.

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 16: 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 [root@serialport -]# **cd tmp**
Go to the directory where the new VEM software was copied.

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

- **vihostupdate**
  Installs the ESX/ESXi and VEM software simultaneously if you are using the vCLI.
- **esxupdate**
  Installs the VEM software from the ESX host /tmp directory.
  Note You must log in to each host and enter this command. This command loads the software manually on the host, loads the kernel modules, and starts the VEM agent on the running system.

Step 3 For ESXi 5.0.0 or later hosts, enter the appropriate commands as they apply to you.

a) ~ # **esxcli software vib install -d** */absolute-path/VEM_bundle*
b) ~ # **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`.

Step 4 Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information* by typing the following commands.

a) [root@serialport tmp]# **vmware -v**
b) root@serialport tmp]# # **esxupdate query**
c) [root@host212 ~]# . ~ # **vem status -v**
d) [root@host212 ~]# **vemcmd show version**

Step 5 switch# **show module**
Display that the VEMs were upgraded by entering the command on the VSM.

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

The following example shows how to upgrade the VEM software using the vCLI.

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

```
[root@serialport -]# cd tmp
[root@serialport tmp]#
esxupdate -b [VMware offline update bundle] update
~ # esxcli software vib install -d /tmp/VEM500-201401164100-BG-zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1
   VIBs Removed:
   VIBs Skipped:
~ #

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v164-4.2.1.2.2.2.0-3.0.1.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1
   VIBs Removed:
   VIBs Skipped:
~ #
[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-843203
root@serialport tmp]# # esxupdate query
------Bulletin ID------- -----Installed----- --------------Summary---------------
VEM500-201401164100 2014-01-27T08:18:22 Cisco Nexus 1000V 4.2(1)SV2(2.2)


[root@host212 ~]# . ~ # vem status -v
Package vssnet-esxmn-release
Version 4.2.1.2.2.2.0-3.0.1
Build 1
Date Mon Jan 27 04:56:14 PDT 2014

VEM modules are loaded
Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0         128         4           128               1500    vmnic4
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
p-1              256         19          256               1500
vmnic7,vmnic6,vmnic3,vmnic2,vmnic1,vmnic0
VEM Agent (vemdpa) is running
~ #


[root@host212 ~]# vemcmd show version
vemcmd show version
VEM Version: 4.2.1.2.2.2.0-3.0.1
VSM Version: 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
System Version: VMware ESXi 5.0.0 Releasebuild-843203

~ #
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    332    Virtual Ethernet Module           NA                  ok
6    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                Hw
```

```
---  ------------------  --------------------------------------------------
1    4.2(1)SV2(2.2)  0.0
2    4.2(1)SV2(2.2)  0.0
3    4.2(1)SV2(2.2)      VMware ESXi 5.0.0 Releasebuild-843203 (3.0)
6    4.2(1)SV2(2.2)      VMware ESXi 5.1.0 Releasebuild-843203 (3.0)

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.105.232.25    NA                                   NA
2    10.105.232.25    NA                                   NA
3    10.105.232.72    e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba  10.105.232.72
6    10.105.232.70    ecebdf42-bc0e-11e0-bd1d-30e4dbc2b892  10.105.232.70

switch#
```

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

Upgrading the VEMs Manually from Release 4.2(1)SV1(4x), Release and Later Releases to the Current Release

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 88.

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 switch# **vmware vem upgrade notify**
Coordinate with and notify the server administrator of the VEM upgrade process.

Step 2 switch# **show vmware vem upgrade status**
Verify that the upgrade notification was sent.

Step 3 switch# **show vmware vem upgrade status**

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

Step 4 Perform one of the following tasks:

- If the ESXESXi host is not hosting the VSM, proceed to Step 5.
- If the ESXESXi 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 switch# **vmware vem upgrade proceed**
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 ESXESXi to the VSM.

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

Step 6 switch# **show vmware vem upgrade status**
Check for the upgrade complete status.

Step 7 Coordinate with and wait until the server administrator upgrades all ESXESXi 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 88.

Step 8 switch# **vmware vem upgrade complete**
Clear the VEM upgrade status after the upgrade process is complete.

Step 9 switch# **show vmware vem upgrade status**
Check the upgrade status once again.

Step 10 switch# **show module**
Verify that the upgrade process is complete.

Note The line with the bold characters in the preceding example display that all VEMs are upgraded to the current release.

The upgrade is complete.

The following example shows how to upgrade VEMs manually.

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

```
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: VEM500-201401164100-BG
    DVS: VEM410-201401152101-BG
switch#
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.

switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Tue Jan 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jan 28 02:06:53 2014
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201401164100-BG
    DVS: VEM410-201401152101-BG

switch#
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: Tue Jan 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jan 28 02:06:53 2014
Upgrade Start Time: Tue Jan 28 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM500-201401164100-BG
    DVS: VEM500-201401164100-BG

switch# show vmware vem upgrade status
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Tue Jan 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jan 28 02:06:53 2014
Upgrade Start Time: Tue Jan 28 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error
Upgrade Bundle ID:
    VSM: VEM500-201401164100-BG
    DVS: VEM500-201401164100-BG

switch#
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: VEM500-201401164100-BG
    DVS: VEM500-201401164100-BG

switch#
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    332    Virtual Ethernet Module           NA                  ok
6    248    Virtual Ethernet Module           NA                  ok

Mod  Sw                 Hw
---  -----------------  ------------------------------------------------
1    4.2(1)SV2(2.2)  0.0
2    4.2(1)SV2(2.2)  0.0
3    4.2(1)SV2(2.2)     VMware ESXi 5.0.0 Releasebuild-843203 (3.0)
6    4.2(1)SV2(2.2)     VMware ESXi 5.1.0 Releasebuild-843203 (3.0)

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.105.232.25    NA                                   NA
2    10.105.232.25    NA                                   NA
3    10.105.232.72    e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba  10.105.232.72
6    10.105.232.70    ecebdf42-bc0e-11e0-bd1d-30e4dbc2b892  10.105.232.70

* this terminal session
switch#
```

Simplified Upgrade Process

Combined Upgrade

You can upgrade the VEM and ESX version simultaneously. It requires vSphere version 5.0 Update1 and later versions. It is supported in Cisco Nexus 1000V Release 4.2(1)SV1(5.2) and later. This upgrade can be implemented manually or by using VUM.

Selective Upgrade

You can upgrade a selective set of VEMs and a few hosts or clusters at a time in a single maintenance window. This enables incremental upgrades during short maintenance windows. It is supported with combined upgrades of VEM and ESX, and also with manual upgrades of VEMs only. It is supported for VUM-based combined upgrades with select hosts or clusters using the GUI. It is not supported with VUM-based upgrades of VEMs alone. To upgrade manually using this procedure follow these general steps:

- Identify the cluster or set of hosts in a cluster
- Place the selected hosts in maintenance mode (to vacate the VMs)
- Upgrade the VEM image on the hosts using the manual command or scripts
- Take the hosts out of maintenance mode, allowing Distributed Resource Scheduler (DRS) to rebalance VMs

Background Upgrade

You can upgrade VEMs without a maintenance window for VEMs. You use the manual procedure to upgrade VEMs during production. Place the host in maintenance mode, upgrade the VEM, and remove the host from the maintenance mode. You do not have to shut off HA Admission Control and such (as you would during VUM upgrades). You must ensure the spare capacity in the cluster and perform a health check before the upgrade. To upgrade using this procedure follow these general steps:

- Upgrade the VSM first as usual. This may be done in a maintenance window
- Place one host at a time in maintenance mode (to vacate the VMs)
- Upgrade the VEM image on that host using manual commands or scripts
- Take the host out of maintenance mode, allowing the DRS to rebalance the VMs.
- Repeat the same procedure for every host in the DVS.

Note Make sure there is enough spare capacity for HA and that all required ports have system profiles (such as mgmt vmk). Check the host health before upgrading.

Extended Upgrade

You can modify configurations between the upgrade maintenance windows. VSM configuration changes are allowed where you can add or remove modules, port configurations, VLANs, and other similar changes. If a set of hosts are upgraded to the latest VEM version using the Selective Upgrade or the Background Upgrade, the remaining set of hosts will remain in older VEM versions. During that time, various Cisco Nexus 1000V configuration changes are allowed between maintenanance windows.

Note Do not make configuration changes during a maintenance window when the VEMs are being upgraded.

The list of allowed configuration changes are as follows:

- Add or remove modules
- Add or remove ports (ETH and VETH)
- Shut or no-shut a port
- Migrate ports to or from a vswitch
- Change port modes (trunk or access) on ports
- Add or remove port profiles
- Modify port profiles to add or remove specific features such as VLANS, ACLs, QoS, or PortSec.
- Change port channel modes in uplink port profiles
- Add or delete VLANs and VLAN ranges
- Add or delete static MACs in VEMs

Note Queuing configuration changes are not supported on QoS.

Upgrading from Releases 4.0(4)SV1(3x) to the Current Release

Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to the current release 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 Upgrade Procedures, on page 68.

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.

Layer 2 to 3 Conversion Tool

About VSM-VEM Layer 2 to 3 Conversion Tool

Use the VSM-VEM Layer 2 to 3 Conversion Tool as an optional, simplified method to migrate from Layer 2 to Layer 3 mode. The tool enables you to do the following:

- Check whether the prerequisites are met for the migration from L2 to L3 mode.
- Migrate the VSM from Layer 2 to Layer 3 Mode, with user interaction.

In the process of migration, the tool creates a port profile. You can use port profiles to configure interfaces, which you can assign to other interfaces to give them the same configuration. The VSM-VEM Layer 2 to 3 Conversion Tool also gives you the option of retrieving the IP addresses from a local file (static).

Prerequisites for Using VSM-VEM Layer 2 to 3 Conversion Tool

The L2-L3_CT.zip file contains the applications required to run VSM-VEM Layer 2 to 3 Conversion Tool

Before you begin:

- Log in as administrator to use this conversion tool script.
- Download the L2-L3_CT.zip file from the CCO Download Center.
- Install Tool Conversion Language (TCL) version 8.4 or later on the workstation.
- Install VMware PowerShell API version 5.0 or later on both the vCenter and the workstation.
- Install OpenSSH on the workstation.
- In the workstation environment variables, add `installation_directory_for_OpenSSH\bin` directory to the end of the Windows path variable.
- Ensure that VLANs are allowed on the uplinks.

Note You must install vCenter, VSM, and OpenSSH with admin privileges.

Using VSM-VEM Layer 2 to 3 Conversion Tool

Procedure

Step 1 On your workstation, unzip the L2-L3_CT.zip file to any folder.
When you unzip the file, a Pre-Migrate-Check-Logs folder is created that holds all the running logs. Debugging log files will be created in this folder.

Step 2 Inside the L2-L3_CT folder, run migration.bat as an administrator.
This starts the VSM-VEM Layer 2 to 3 Conversion Tool.

Step 3 Enter the VSM IP address.

Step 4 Enter the VSM username.

Step 5 Enter the vCenter IP.

Step 6 Enter the vCenter username.

Step 7 Enter the VSM password.

Step 8 Enter the vCenter password.
The migration tool begins creating the .csv file for the user, and then checks for a port profile with layer 3 capability.

Step 9 If there is no layer 3-capable port profile, the tool will prompt for the creation of one. If you don't want to create a layer-3 capable port profile, skip to the next step.

a) Enter yes to confirm when asked to create 1 layer 3-capable port profile.
b) Enter a layer 3 port profile name.
c) Enter access VLAN ID

This creates a port profile with the required configuration. You can select this port profile when prompted by the tool. The migration tool checks for connectivity between VSM, vCenter, and VEM modules. Wait for the message to display that all connectivity is fine.

Step 10 Enter yes to continue when asked if you want to continue.
The migration tool proceeds to create an extract .csv file.

Step 11 Open the extract.csv file (in `C:\Windows\Temp`).

Step 12 Enter the vmknic IP details at the end of the text, delimited by semicolons, and save the file as convert.csv.

Step 13 Press any key to continue.

Step 14 Enter yes to confirm when asked if you are sure you completed the required steps.

Step 15 Enter the VSM password.

Step 16 Enter the vCenter password.
The migration tool connects to the vCenter and VSM of the user.

Step 17 Enter yes to confirm when asked if you want to continue.
The migration process continues.

Step 18 Enter the port profile name from the list of port profiles that appears at the prompt.
Once the port profile is selected, the max port value is automatically changed to 128.

Step 19 Enter yes to confirm when asked if you have updated convert.csv file as per the instructions.

Step 20 Enter yes to confirm, when asked if you want to continue.
The tool checks the connectivity between VSM, vCenter, and VEM modules. A message is displayed that the addition to vmknics are successful and all connectivity is fine. The **VmkNicAddingToHost** window will remain open until the configuration is complete.

Step 21 Enter yes to confirm that you would like to proceed with mode change from L2 to L3.

Step 22 Enter yes to confirm when asked if you wish to continue.
Wait for the SUCCESSFULLY COMPLETED MIGRATION message to display. The migration from layer 2 to layer 3 is now complete. The operating mode should now be listed as L3.

Using Extract Mode

You can use Extract Mode to extract the attached VEM states and save them to the Extract.csv file, which is located in `C:\Windows\Temp`.

Procedure

	Command or Action	Purpose
Step 1	Choose extract mode when prompted by VSM-VEM Layer 2 to 3 Conversion Tool. You can now view the data in the Extract.csv file in the Windows temp folder of your workstation.	This mode will not migrate the VSM.

Using Convert Mode

You can use Convert Mode to migrate the VSM from Layer 2 to Layer 3.

Procedure

	Command or Action	Purpose
Step 1	Rename the Extract.csv file to Convert.csv	The migration tool will retrieve the data from the Convert.csv file.
Step 2	Populate your Convert.csv file (in `C:\Windows\Temp`) with the vmknic IP address and netmask.	
Step 3	Run migration.bat.	This will migrate the VSM mode from Layer 2 to Layer 3 .

Example

The following example shows how to use the VSM-VEM Layer 2 to 3 Conversion Tool.

```
Enter VSM IP:
enter VSM Username:
Enter VC IP:
enter VC Username:
Enter VSM password:
Enter VC password:
create the Csv File for User I/P: C:\windows\temp\extract.csv
#### VSM DETAILS STARTS ##########
.........
..............
#### VC DETAILS END ##########
..............
..................
Operating Mode : L2
Operatoinal Mode is L2 Currently ......
################################################################################
List of port profiles on VSM:
-----------------------------
################################################################################
==========
 CHECK 1: Checking for a port profile with capability l3control set and Enabled.
..................
==========
There is not even One L3 Capable Port Profile

Do you want to Create One L3 Capable Port Profile
```

```
Please Give Option (Yes/No):Yes
Please Enter L3 PortProfile Name: L3-Control
Please Give Access Vlan Id :5
Creating L3 Port Profile : L3-Control with Access Vlan : 5
.................................
.................................................
L3 capable port profiles: L3-Control
Modules Registered:[10.105.228.116]
=========
 CHECK 3:  Checking for connectivity between VSM and VC, VSM and VEM Modules
=========
.................
.....................................

## All connectivity is fine
################################################################################
Please wait for a few minutes.
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
Creating csv file: C:\windows\temp\extract.csv
Modules : 10.105.228.116
##########################################################
Modules Registered:[3 10.105.228.116]
##########################################################

##########################################################
################################################################################
Extraction of VEM connection status has been dumped in: C:\windows\temp\extract.
csv
Please rename this file before using Convert Mode
Update the VMKNic IP and NetMask for all disconnected entries
################################################################################
!##############################################################################
########!
!Open c:\windows\temp\Extract.csv and save as Convert.csv (in the same directory
)
!Enter the VMKNic IP and netmask in the Convert.csv file as shown below
!VEM_Host_IP;PPConnectionStatus;Vem_Vmk_IP;NetMask!
!PPConnectionStatus Should not be changed!
!10.10.10.12;DisConnected;10.10.10.100;255.255.255.0!
!After Updating the IP and Netmask, save the file in the same directory
!##############################################################################
########!
Press any key to continue . . .
Are you sure you completed the above steps? (yes/no):yes

################################################################################

##Tool expects this File have an IP/Netmask given for disconnected VEM in the co
rrect format : C:\windows\temp\Convert.csv

##10.10.10.12;DisConnected;10.10.10.100;255.255.255.0

################################################################################
VSM password required 10.105.228.115:

VC password required 10.105.228.113:

create the Csv File for User I/P: C:\windows\temp\extract.csv
.....................
.............................
## All connectivity is fine

################################################################################
Please wait for a few minutes.
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
.............................
.....................................................
######################################################
Name the port profile you want to proceed with : [l3-pp]
Please type any port profile mentioned above       ||:l3-pp
```

```
You Selected : l3-pp
.....................
.....................................
######################################################################
## Have you created a Convert.csv file with a proper VMKNic IP and NetMask?
## In the C:\windows\temp\Convert.csv file for disconnected VEMs.
######################################################################
Have you Updated C:\windows\temp\Convert.csv as per the above instructions?(Yes)
:yes
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
.............................
.................................................

Addition to VmKNics are successful
## All connectivity is Fine
.................................
.....................................
################################################################################

Would You Like to Proceed with Mode Change from L2 to L3....(yes/no):yes
Do you want to Continue,Please Type ....(yes/no):yes
Migration Tool Proceeding ....
.....................
.........................
switch#
Operating Mode : L3
Operatoinal Mode is L3 Currently
Svs Connection Mode : L3
Vem IP : 10.10.10.108 Connected Back
..................
.......................
All VEMs are back: pass
 ==============SUCCESSFULLY COMPLETED MIGRATION============================
```

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

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.

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.

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 102.

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 (Optional) 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.

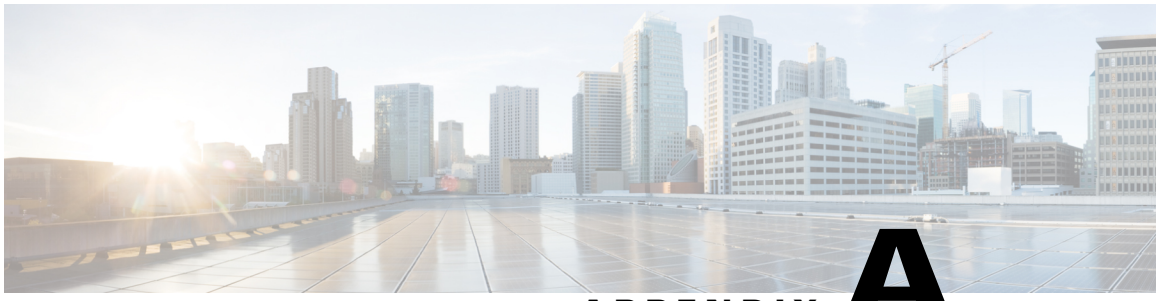
Step 5 Display the SVS domain configuration.

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

Note: Control VLAN and Packet VLAN are not used in L3 mode.
```

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 contains the following sections:

VMware Release Upgrades

Upgrading from VMware Releases 4.0, 4.1, 5.0, 5.1 to VMware Release 5.5

The steps to upgrade are as follows:

Note From vCenter Server Release 5.1, you cannot directly upgrade an existing vCenter Server from an older version to Release 5.1. vSphere 5.1 introduces the vCenter Single Sign On service as part of the vCenter Server management infrastructure. This change affects vCenter Server installation, upgrading, and operation. When you upgrade to vCenter Server 5.1, the upgrade process installs vCenter Single Sign On first and then upgrades the vCenter Server.

Procedure

Step 1 Installing the vCenter Single Sign On
Step 2 Installing the vCenter Inventory Service
Step 3 Upgrading the vCenter Server, on page 83
Step 4 Upgrading the vCenter Update Manager to Release 5.5, on page 111
Step 5 Augmenting the Customized ISO for VMware Release 5.1 and Later, on page 112
Step 6 Upgrading the ESXi Hosts to Release 5.x, on page 113

Installing the vCenter Single Sign On

Before You Begin

- Download the upgrade ISO file that contains the ESXi image and the Cisco Nexus 1000V software image files.
- 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 desired VMware vSphere 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 Single Sign On**.
Step 4 Click **OK** on the warning message and click **Next**.
Step 5 In the Patent Agreement window, click **Next**.
Step 6 In the License Agreement window, click the **I agree to the terms in the license agreement radio button** and Click **Next**.
Step 7 In the vCenter Single Sign On Deployment Type window, keep the default setting of installing vCenter Single SignOn with basic node and click **Next**.
Step 8 In the vCenter Single Sign On Type window, keep the default setting of Install basic vCenter Single Sign On and click **Next**.
Step 9 In the vCenter Single Sign On Information window, provide the single sign on server password and click **Next**.
Note Ensure your single sign on server password is different from the windows VM password.

Step 10 In the Database Options screen, click **Next**.
Step 11 In the Database User Information screen, provide the SSO password for RSA_DBA and RSA_USER.
Step 12 In the Local system information screen, provide the IP address of your local machine.
Step 13 Ignore the warning message and Click **Ok**.
Step 14 Click **Next**.
Step 15 Retain the default HTTPs port settings and Click **Next**.
Step 16 Click **Install**.
Step 17 Click **Finish**.

Installing the vCenter Inventory Service

Procedure

Step 1 In the VMware vCenter Installer window, click **vCenter Inventory Service**.
Step 2 Click **Install**.
Step 3 Choose the desired language and click **OK**.
Step 4 Click **Next**.
Step 5 In the Patent Agreement window, click **Next**.
Step 6 In the License Agreement window, click **I agree to the terms in the license agreement radio button** and click **Next**.
Step 7 In the Database Options screen, click **Next** .
Step 8 In the Local system information window, provide the IP address of your local machine.
Step 9 Ignore the warning message and Click **Ok**.
Step 10 Click **Next**.
Step 11 Retain the default configured port settings and Click **Next**.
Step 12 Retain the default Inventory size for vCenter Server deployment and Click **Next** .
Step 13 Enter the vCenter Single Sign On server credentials and Click **Next** .
Step 14 In the Certificate Installation for Secure Connection window, select **Overwrite Certificates**.
Step 15 Click **Install**.
Step 16 Click **Finish**.

Upgrading the vCenter Server

Note This upgrade procedure applies to vCenter Server 5.0, 5.0 Update 1 and later, 5.1, and 5.5 versions.

Before You Begin

- Download the upgrade ISO file that contains your desired ESXi image and the desired Cisco Nexus 1000V image.
- 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 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** screen, 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** screen, click **Next.**

Step 8 In the **License Agreement** screen, 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** screen, 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 your desired ESXi version.

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 the same VMware versions.

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 5.5, on page 111.

Upgrading the vCenter Update Manager to Release 5.5

Note This upgrade procedure also applies to vCenter Update Manager 5.0, 5.0 Update 1 and later, 5.1, and 5.5 versions.

Before You Begin

You have upgraded the vCenter Server to the desired VMware ESXi version.

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.
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 and Later, on page 112.

Augmenting the Customized ISO for VMware Release 5.1 and Later

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 needs any Async drivers that are not already in the VMware release, see the respective vendor 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.x, on page 113.

Upgrading the ESXi Hosts to Release 5.x

Note

- This upgrade procedure also applies to ESXi hosts 5.0, 5.0 Update 1, 5.1 and 5.5 versions.
- If you have multiple vmkernel interfaces on the same subnet when upgrading you ESXi host, 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.

VMware Release 5.1 to VMware Release 5.1 Update 1

Creating the Host Patch Baseline for 5.1 Update 1

Before You Begin

Ensure you configure the VMware Update Manager Download settings with proxy enabled and VMware production portal links for VMware ESX/ESXi in connected state and download those images into the VUM patch repository.

Procedure

Step 1 Under **Home** > **Solutions and Applications** > **Update Manager**, select **Baselines and Groups** tab.

Step 2 Under **Baseline**, click **Create** to create a baseline.

Step 3 In the **Baseline Name and Type** window, enter a name for the baseline, select the **Host Patch** radio button and click **Next**.

Step 4 In the **Patch Options** window, select the **Fixed** radio button and click **Next**.

Step 5 In the **Patches** window, select the required patch to upgrade to version 5.1 Update 1 and move the selected patch to **Fixed patches to Add** column and click **Next**.

Note To know the 5.1 update 1 patches, refer to http://www.vmware.com/patchmgr/findPatch.portal .

Note In the combined upgrade scenario, add the required Cisco Nexus 1000V VEM patch that corresponds to 5.1 Update 1 release to the **Fixed patches to Add** column along with ESXi 5.1 Update 1 patches. You can get the required Cisco Nexus 1000V VEM patches into the VUM patch repository either from www.cisco.com, VMWare production portal links or through the VSM home page.

Upgrading the ESXi Hosts to Release 5.1 Update 1 using VMware Update Manager

Note Follow the same procedure to upgrade ESXi hosts 5.0 to 5.0 Update 1 and later.

Procedure

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

Step 2 From the left navigation pane, select the host or cluster that needs to be upgraded and click **Update Manager**.

Step 3 Click **Attach**.

Step 4 In the Individual Baselines by Type area, select your Patch baseline's radio button check box.

Step 5 Click **Attach**.

Step 6 Click **Scan**.

Step 7 In the Confirm Scan dialog box, check the **Patches and extensions box** and click **Scan**.
Verify if all the hosts are non-compliant.

Step 8 Click **Stage**.

Step 9 In Baseline Selection window, keep the default selected baseline and click **Next**.

Step 10 In Patch and Extension exclusion window, keep the default selected baseline and click **Next**.

Step 11 Click **Finish**.

Step 12 Click **Remediate** and click **Next**.

Step 13 In Patch and Extension exclusion window, keep the default selected baseline and click **Next**.

Step 14 Click **Next**.

Step 15 In the Host Remediate Options window, under Maintenance Mode Options, select the **Disable any removable media devices connected to the virtual machines on the host** check box.

Note If you have stateless host in your setup, select **Enable Patch Remediation on Powered on PXE booted ESXi hosts** radio button.

Step 16 Click **Next**.

Step 17 In the Cluster Remediation Options window, select all the check boxes and click **Next**.

Step 18 Click **Finish** to begin the remediation.

To check the host versions, on the left-hand pane, click on each host to confirm if version 5.1 appears in the top-left corner of the right-hand pane and the version information matches the information provided under the *Cisco Nexus 1000V and VMware Compatibility Information* guide.

You can also confirm if the upgrade was successful by executing the **show module** command on the VSM and check if the VEMs are running the correct build.

Note Follow the same procedure for combined upgrade of 5.0 or 5.1 and the initial version of Cisco Nexus 1000V to 5.0 Update1 or 5.1 Update1 and the upgraded version of Cisco Nexus 1000V.

Upgrading the ESXi Hosts to Release 5.1 Update 1 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

- 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 software 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.

esxcli software vib install -v *full-path-to-vib*

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 update -d /var/tmp/update-from-esxi5.1-5.1_update01.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_5.1.0-0.12.1065491,
VMware_locker_tools-light_5.1.0-0.12.1065491
   VIBs Removed: VMware_bootbank_esx-base_5.1.0-0.3.799733,
VMware_locker_tools-light_5.0.0-0.0.799733
   VIBs Skipped: VMware_bootbank_ata-pata-amd_0.3.10-3vmw.510.0. 3.799733,
VMware_bootbank_ata-pata-atiixp_0.4.6-3vmw.510.0. 3.799733,

<=============================================================================>

   VMware_bootbank_scsi-qla4xxx_5.01.03.2-3vmw.510.0.3.799733.,
VMware_bootbank_uhci-usb-uhci_1.0-3vmw.510.0.3.799733
```

What to Do Next

Complete the steps under Verifying the Build Number and Upgrade

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 5.1 Update 1.
- You have upgraded the VMware Update Manager to VMware Release 5. 1 Update 1.
- You have upgraded your ESX/ESXi hosts to VMware Release 5. 1 Update 1.

Procedure

Step 1 Verify the build number on the ESXi host.

```
~ # vmware -v
VMware ESXi 5.1.0 build-1065491
VMware ESXi 5.1.0 Update 1
```

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(1.1a)   0.0
2    4.2(1)SV2(1.1a)   0.0
3    4.2(1)SV2(1.1a)   3.1
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    10.105.235.74   NA                                    NA
2    10.105.235.74   NA                                    NA
3    10.105.235.72   42064d20-4e52-62d1-e0ee-0b14be4388d6  mnn-update1-esxi-statefull

* this terminal session
```

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- 201301152108.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/ESXi500-201301152108.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 and use the following steps.

a) ~ # **esxcli software vib install -d** *full_path_to_VEM_bundle*

b) ~ # **esxcli software vib install –v***full_path_to_VIB*

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.

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 by typing the following commands.

Note If the VEM Agent is not running, see the *Cisco Nexus 1000V Troubleshooting Guide*.

a) ~ # **vmware -v -l**
b) ~ # **vemcmd show version**
c) ~ # **vem status -v**
d) ~ # **esxcli software vib list | grep** *name*
e) ~ # **vem version -v**

Step 4 switch# **show module**

Verify that the VEM has been upgraded by entering the following command from the VSM.

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

Step 5 Do one of the following:

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

The following example shows how to install ESXi 5.1 software using the CLI.

```
~ # esxcli software vib install -d /var/log/vmware/VEM510-201306160101-BG-release.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.1.1.vib
   VIBs Removed:
   VIBs Skipped:

~ # esxcli software vib install –v
/var/log/vmware/Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.1.1.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.1.1
   VIBs Removed:
   VIBs Skipped:
~ #
~ # vmware -v -l
VMware ESXi 5.1.0 build-1029768
VMware ESXi 5.1.0 Update 1
~ #

~ # vemcmd show version
VEM Version: 4.2.1.2.2.2.0-3.1.1
VSM Version: 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
System Version: VMware ESXi 5.1.0 Releasebuild-1029768


~ # vem status -v
Package vssnet-esxmn-next-release
Version 4.2.1.2.2.2.0-3.1.1
Build 1
Date Tue Jan 28 04:56:14 PDT 2014

VEM modules are loaded

Switch Name      Num Ports   Used Ports  Configured Ports  MTU     Uplinks
```

```
vSwitch0         128         4           128               1500    vmnic4

DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
p-1              256         19          256               1500
vmnic7,vmnic6,vmnic3,vmnic2,vmnic1,vmnic0

VEM Agent (vemdpa) is running

~ # esxcli software vib list | grep cisco
cisco-vem-v164-esx             4.2.1.2.2.2.0-3.1.1               Cisco   PartnerSupported
  2013-04-22
~ #

~ # vem version -v
Running esx version -1029768 x86_64
VEM Version: 4.2.1.2.2.2.0-3.1.1
VSM Version: 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
System Version: VMware ESXi 5.1.0 Releasebuild-1029768

~ #
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    332    Virtual Ethernet Module          NA                  ok
6    248    Virtual Ethernet Module          NA                  ok


Mod  Sw                  Hw
---  ------------------  ------------------------------------------------
1    4.2(1)SV2(2.2)  0.0
2    4.2(1)SV2(2.2)  0.0
3    4.2(1)SV2(2.2)      VMware ESXi 5.1.0 Releasebuild-911593 (3.1)
6    4.2(1)SV2(2.2)      VMware ESXi 5.1.0 Releasebuild-1029768 (3.1)

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.105.232.25    NA                                   NA
2    10.105.232.25    NA                                   NA
3    10.105.232.72    e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba 10.105.232.72
6    10.105.232.70    ecebdf42-bc0e-11e0-bd1d-30e4dbc2b892 10.105.232.70

* this terminal session
switch#
```

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.

Procedure

Step 1 Start the VMWare PowerCLI application.

Step 2 Connect to the vCenter Server by using the **Connect-VIServer** *IP_address* **-User Administrator -Password** *password_name* command.

Step 3 Load the ESX depot by using the **Add-ESXSoftwareDepot** *path_name\file_name* command.

Step 4 Display the image profiles by using the **Get-EsxImageProfile** command.

Step 5 Clone the ESX standard image profile by using the **New-ESxImageProfile -CloneProfile** *ESXImageProfile_name* **-Name** *clone_profile* command.

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

Step 6 Load the Cisco Nexus 1000V VEM offline bundle by using the **Add-EsxSoftwareDepot** *VEM_offline_bundle* command.

Step 7 Confirm that the n1kv-vib package is loaded by using the **Get-EsxSoftwarePackage -Name** *package_name* command.

Step 8 Bundle the n1kv-package into the cloned image profile by using the **Add-EsxSoftwarePackage -ImageProfile** *n1kv-Image* **-SoftwarePackage** *cloned_image_profile* command.

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

a) **$img = Get-EsxImageProfile** *n1kv-Image*

b) **$img.vibList**

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

Step 10 Export the image profile to an ISO file by using the **Export-EsxImageProfile -ImageProfile** *n1kv-Image* **-FilePath** *iso_filepath* command.

This example shows how to create an upgrade ISO with a VMware ESX image and a Cisco VEM image.

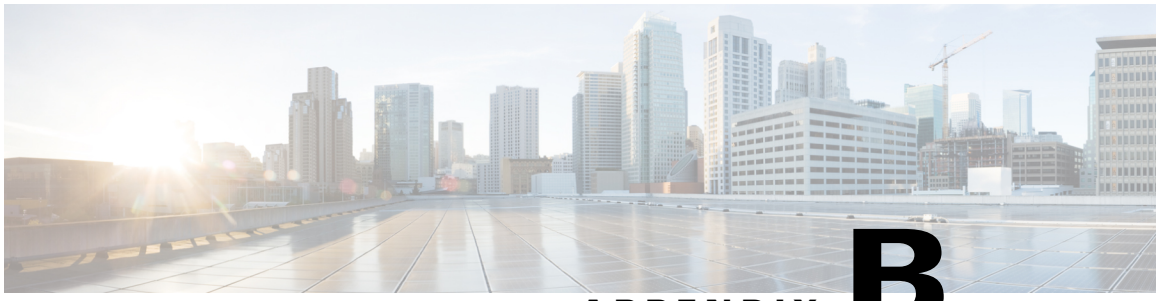
Note The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
vSphere PowerCLI> Connect-VIServer 10.105.231.40 -User administrator -Password 'XXXXXXXX'

Working with multiple default servers?

    Select [Y] if you want to work with more than one default servers. In this
case, every time when you connect to a different server using Connect-VIServer,
 the new server connection is stored in an array variable together with the
previously connected servers. When you run a cmdlet and the target servers
cannot be determined from the specified parameters, the cmdlet runs against all
 servers stored in the array variable.
    Select [N] if you want to work with a single default server. In this case,
when you run a cmdlet and the target servers cannot be determined from the
specified parameters, the cmdlet runs against the last connected server.

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

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

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

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229\VMware-ESXi-5.1.0-799733-depot.zip'

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

vSphere PowerCLI> Get-EsxImageProfile

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
ESXi-5.1.0-20121201001s-no-... VMware, Inc.    12/7/2012 7:... PartnerSupported
CN1-CY                         CISCO           4/22/2013 11... PartnerSupported
ESXi-5.1.0-20121204001-stan... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-20121201001s-sta... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-no-tools     VMware, Inc.    8/2/2012 3:0... PartnerSupported
ESXi-5.1.0-20121204001-no-t... VMware, Inc.    12/7/2012 7:... PartnerSupported
ESXi-5.1.0-799733-standard     VMware, Inc.    8/2/2012 3:0... PartnerSupported

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

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

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           8/2/2012 3:0... PartnerSupported

vSphere PowerCLI> Add-EsxSoftwareDepot 'C:\Documents and
Settings\Administrator\Desktop\upgrade\229
\cisco-vem-v164-4.2.1.2.2.2.0-3.1.1.zip'

Depot Url
---------
zip:C:\Documents and Settings\Administrator\Desktop\upgrade\229\cisco-vem-v1...

vSphere PowerCLI> Get-EsxSoftwarePackage cisco*

Name                     Version                        Vendor     Creation Dat
                                                                   e
----                     -------                        ------     ------------
cisco-vem-v164-esx       4.2.1.2.2.2.0-3.1.1          Cisco      1/24/2014...

vSphere PowerCLI> Add-EsxSoftwarePackage -SoftwarePackage cisco-vem-v164-esx -ImageProfile
 FINAL

Name                           Vendor          Last Modified   Acceptance Level
----                           ------          -------------   ----------------
FINAL                          CISCO           1/24/2014 3:... PartnerSupported

vSphere PowerCLI> $img = Get-EsxImageProfile FINAL

vSphere PowerCLI> $img.vibList

Name                     Version                        Vendor     Creation Dat
                                                                   e
----                     -------                        ------     ------------
scsi-bnx2i               1.9.1d.v50.1-5vmw.510.0.0.7... VMware     8/2/2012 ...
sata-sata-promise        2.12-3vmw.510.0.0.799733       VMware     8/2/2012 ...
net-forcedeth            0.61-2vmw.510.0.0.799733       VMware     8/2/2012 ...
esx-xserver              5.1.0-0.0.799733               VMware     8/2/2012 ...
misc-cnic-register       1.1-1vmw.510.0.0.799733        VMware     8/2/2012 ...
net-tg3                  3.110h.v50.4-4vmw.510.0.0.7... VMware     8/2/2012 ...
```

```
scsi-megaraid-sas        5.34-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-megaraid-mbox       2.20.5.1-6vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-ips                 7.12.05-4vmw.510.0.0.799733    VMware     8/2/2012 ...
net-e1000e               1.1.2-3vmw.510.0.0.799733      VMware     8/2/2012 ...
sata-ahci                3.0-13vmw.510.0.0.799733       VMware     8/2/2012 ...
sata-sata-svw            2.3-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-cnic                 1.10.2j.v50.7-3vmw.510.0.0.... VMware     8/2/2012 ...
net-e1000                8.0.3.1-2vmw.510.0.0.799733    VMware     8/2/2012 ...
ata-pata-serverworks     0.4.3-3vmw.510.0.0.799733      VMware     8/2/2012 ...
scsi-mptspi              4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...
ata-pata-hpt3x2n         0.3.4-3vmw.510.0.0.799733      VMware     8/2/2012 ...
net-s2io                 2.1.4.13427-3vmw.510.0.0.79... VMware     8/2/2012 ...
esx-base                 5.1.0-0.0.799733               VMware     8/2/2012 ...
net-vmxnet3              1.1.3.0-3vmw.510.0.0.799733    VMware     8/2/2012 ...
net-bnx2                 2.0.15g.v50.11-7vmw.510.0.0... VMware     8/2/2012 ...
cisco-vem-v164-esx       4.2.1.2.2.2.0-3.1.1            Cisco      1/24/2014...
scsi-megaraid2           2.00.4-9vmw.510.0.0.799733     VMware     8/2/2012 ...
ata-pata-amd             0.3.10-3vmw.510.0.0.799733     VMware     8/2/2012 ...
ipmi-ipmi-si-drv         39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-lpfc820             8.2.3.1-127vmw.510.0.0.799733  VMware     8/2/2012 ...
ata-pata-atiixp          0.4.6-4vmw.510.0.0.799733      VMware     8/2/2012 ...
esx-dvfilter-generic-... 5.1.0-0.0.799733               VMware     8/2/2012 ...
net-sky2                 1.20-2vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-qla2xxx             902.k1.1-9vmw.510.0.0.799733   VMware     8/2/2012 ...
net-r8169                6.011.00-2vmw.510.0.0.799733   VMware     8/2/2012 ...
sata-sata-sil            2.3-4vmw.510.0.0.799733        VMware     8/2/2012 ...
scsi-mpt2sas             10.00.00.00-5vmw.510.0.0.79... VMware     8/2/2012 ...
sata-ata-piix            2.12-6vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-hpsa                5.0.0-21vmw.510.0.0.799733     VMware     8/2/2012 ...
ata-pata-via             0.3.3-2vmw.510.0.0.799733      VMware     8/2/2012 ...
scsi-aacraid             1.1.5.1-9vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-rste                2.0.2.0088-1vmw.510.0.0.799733 VMware     8/2/2012 ...
ata-pata-cmd64x          0.2.5-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ima-qla4xxx              2.01.31-1vmw.510.0.0.799733    VMware     8/2/2012 ...
net-igb                  2.1.11.1-3vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-qla4xxx             5.01.03.2-4vmw.510.0.0.799733  VMware     8/2/2012 ...
block-cciss              3.6.14-10vmw.510.0.0.799733    VMware     8/2/2012 ...
scsi-aic79xx             3.1-5vmw.510.0.0.799733        VMware     8/2/2012 ...
tools-light              5.1.0-0.0.799733               VMware     8/2/2012 ...
uhci-usb-uhci            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
sata-sata-nv             3.5-4vmw.510.0.0.799733        VMware     8/2/2012 ...
sata-sata-sil24          1.1-1vmw.510.0.0.799733        VMware     8/2/2012 ...
net-ixgbe                3.7.13.6iov-10vmw.510.0.0.7... VMware     8/2/2012 ...
ipmi-ipmi-msghandler     39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-adp94xx             1.0.8.12-6vmw.510.0.0.799733   VMware     8/2/2012 ...
scsi-fnic                1.5.0.3-1vmw.510.0.0.799733    VMware     8/2/2012 ...
ata-pata-pdc2027x        1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
misc-drivers             5.1.0-0.0.799733               VMware     8/2/2012 ...
net-enic                 1.4.2.15a-1vmw.510.0.0.799733  VMware     8/2/2012 ...
net-be2net               4.1.255.11-1vmw.510.0.0.799733 VMware     8/2/2012 ...
net-nx-nic               4.0.558-3vmw.510.0.0.799733    VMware     8/2/2012 ...
esx-xlibs                5.1.0-0.0.799733               VMware     8/2/2012 ...
net-bnx2x                1.61.15.v50.3-1vmw.510.0.0.... VMware     8/2/2012 ...
ehci-ehci-hcd            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
ohci-usb-ohci            1.0-3vmw.510.0.0.799733        VMware     8/2/2012 ...
net-r8168                8.013.00-3vmw.510.0.0.799733   VMware     8/2/2012 ...
esx-tboot                5.1.0-0.0.799733               VMware     8/2/2012 ...
ata-pata-sil680          0.4.8-3vmw.510.0.0.799733      VMware     8/2/2012 ...
ipmi-ipmi-devintf        39.1-4vmw.510.0.0.799733       VMware     8/2/2012 ...
scsi-mptsas              4.23.01.00-6vmw.510.0.0.799733 VMware     8/2/2012 ...
```

```
vSphere PowerCLI> Export-EsxImageProfile -ImageProfile FINAL -FilePath 'C:\Documents and
Settings\Administrator\Desktop\FINAL.iso' -ExportToIso
```



APPENDIX B

Upgrading a Standalone VSM

This chapter contains the following sections:

Upgrading a System with a Standalone VSM

Upgrading a Standalone VSM

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

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.SV2.2.2.bin
bootflash:nexus-1000v-kickstart.4.2.1.SV2.2.2.bin
switch# copy
scp://user@scpserver.cisco.com//downloads/nexus-1000v.4.2.1.SV2.2.2.175.bin
bootflash:nexus-1000v.4.2.1.SV2.2.2.175.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 system bootflash:nexus-1000v.4.2.1.SV2.2.2.bin kickstart
bootflash:nexus-1000v-kickstart.4.2.1.SV2.2.2.bin

Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.2.2.bin for boot variable
```

```
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-4.2.1.SV2.2.2.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

Extracting "system" version from image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.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)SV2(2.2)           yes
     1   kickstart            4.2(1)SV1(4)           4.2(1)SV2(2.2)           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.
```

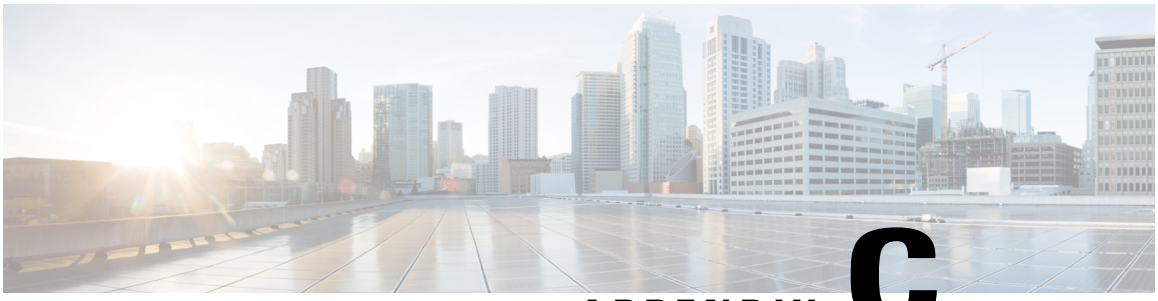
Step 14 After the switch completes the reload operation, log in and verify that the switch is running the required software version.

Example:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, 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)SV2(2.2)
  system:    version 4.2(1)SV2(2.2)
  kickstart image file is: bootflash:/nexus-1000v-kickstart-4.2.1.SV2.2.2.bin
  kickstart compile time:  1/27/2014 14:00:00 [01/27/2011 22:26:45]
  system image file is:    bootflash:/nexus-1000v-4.2.1.SV2.2.2.bin
  system compile time:     1/27/2014 14:00:00 [01/28/2011 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(4x), 4.2(1)SV1(5x), 4.2(1)SV2(1.1x) to Release 4.2(1)SV2(2.2).



APPENDIX C

Glossary

This chapter contains the following sections:

Glossary for Cisco Nexus 1000V

The following table lists the terminology in the Cisco Nexus 1000V implementation.

Table 6: 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.