



## **Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV2(1.1)**

**First Published:** October 21, 2012

**Last Modified:** February 05, 2014

### **Americas Headquarters**

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

Text Part Number: OL-27734-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009-2014 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface ix

Audience ix

Document Conventions ix

Related Documentation for Nexus 1000V Series NX-OS Software xi

Documentation Feedback xii

Obtaining Documentation and Submitting a Service Request xii

---

### CHAPTER 1

#### Overview 1

Information About Virtualization 1

Information About the Cisco Nexus 1000V 2

Cisco Nexus 1000V and Its Components 3

Information About the Virtual Supervisor Module 4

Information About the Virtual Ethernet Module 6

Information About Port Profiles 6

Information About Administrator Roles 7

Differences Between the Cisco Nexus 1000V and a Physical Switch 7

Layer 3 and Layer 2 Control Modes 8

VSM to VEM Communication 8

Layer 3 Control Mode 8

Layer 2 Control Mode 8

Management, Control, and Packet VLANs 9

Information About the Control VLAN 9

Management VLANs 9

Information About the Packet VLAN 9

System Port Profiles and System VLANs 10

Information About System Port Profiles 10

Information About System VLANs 10

## Recommended Topologies 11

### Layer 3 Topology 11

### Control and Management on the Same VLAN Topology 13

### Control and Management on Separate VLANs Topology 14

## VMware Interaction 14

## CHAPTER 2

## Installing the Cisco Nexus 1000V 15

### Information About Installing the Cisco Nexus 1000V 16

#### VSM Software 16

#### VEM Software 16

#### Information About the Cisco Nexus 1000V Installer App 16

### Prerequisites for Installing the Cisco Nexus 1000V 17

#### Cisco Nexus 1000V Installer App Prerequisites 17

#### Host Prerequisites 17

#### Upstream Switch Prerequisites 19

#### VSM Prerequisites 19

#### VEM Prerequisites 20

### Guidelines and Limitations 21

#### Guidelines and Limitations of the Cisco Nexus 1000V Installer App 21

#### Guidelines and Limitations for Installing the Cisco Nexus 1000V 21

### Installing a VSM HA Pair with L3 Mode Behind a VEM Using the Cisco Nexus 1000V Installer App 23

### Installing VSM Software Using the Cisco Nexus 1000V Installer App 23

### Installing Cisco Nexus 1000V in Standard Mode 23

### Installing the Cisco Nexus 1000V in Custom Mode 39

### Information About Layer 2 Connectivity 62

#### Layer 2 on the Same Host 64

#### Configuring Layer 2 Connectivity 64

### Installing the VEM Software Using the Cisco Nexus 1000V Installer App 65

### Adding VEM Hosts to the Distributed Virtual Switch 74

### Setting Virtual Machine Startup and Shutdown Parameters 78

### Installing the VEM Software Using VUM 81

### Installing the VEM Software Using the CLI 82

### Installing VEM Software Locally on a VMware 4.1 Host by Using the CLI 82

### Installing the VEM Software Remotely on a VMware 4.1 Host by Using the CLI 83



Installing the VEM Software Locally on a VMware 5.0 Host by Using the CLI	85
Installing VEM Software Remotely on a VMware 5.0 Host by Using the CLI	86
Installing the VEM Software on a Stateless ESXi Host	87
Stateless ESXi Host	87
Adding the Cisco Nexus 1000V to an ESXi Image Profile	87
Installing the VEM Software on a Stateless ESXi Host Using esxcli	90
Installing the VEM Software on a Stateless ESXi Host Using VUM	92
Installing a VSM on the Cisco Nexus 1010	92
Feature History for Installing the Cisco Nexus 1000V	95

## CHAPTER 3

### Upgrading the Cisco Nexus 1000V 97

Information About the Software Upgrade	97
Upgrade Software Sources	97
Prerequisites for the Upgrade	98
Before You Begin	98
Prerequisites for Upgrading VSMs	99
Prerequisites for Upgrading VEMs	99
Guidelines and Limitations for Upgrading the Cisco Nexus 1000V	100
Upgrade Procedures	102
Upgrade Types	104
Upgrading the Cisco Nexus 1000V Only	104
Combined Upgrade of vSphere and Cisco Nexus 1000V	105
VSM Upgrade Procedures	107
Software Images	107
In-Service Software Upgrades on Systems with Dual VSMs	107
ISSU Process for the Cisco Nexus 1000V	108
ISSU VSM Switchover	109
ISSU Command Attributes	109
Upgrading VSMs from Releases 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1)	110
VEM Upgrade Procedures	118
VUM Upgrade Procedures	120
Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image	120
Upgrading the vCenter Server to Release 5.1	123

Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)	125
Accepting the VEM Upgrade	128
Manual Upgrade Procedures	128
Upgrading the VEM Software Using the vCLI	128
Upgrading the VEMs Manually from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)	132
Installing the VEM Software on a Stateless ESXi Host	135
Installing the VEM Software on a Stateless ESXi Host Using esxcli	136
Installing the VEM Software on a Stateless ESXi Host Using VUM	137
Simplified Upgrade Process	138
Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV2(1.1)	140
Migrating from Layer 2 to Layer 3	140
Layer 3 Advantages	140
Layer 2 to 3 Conversion Tool	141
About VSM-VEM Layer 2 to 3 Conversion Tool	141
Prerequisites for Using VSM-VEM Layer 2 to 3 Conversion Tool	141
Using VSM-VEM Layer 2 to 3 Conversion Tool	142
142	
Using Extract Mode	143
Using Convert Mode	143
Interface Comparisons Between mgmt0 and control0	145
Configuring the Layer 3 Interface	146
Creating a Port Profile with Layer 3 Control Capability	147
Creating a VMKernel on the Host	148
Configuring the SVS Domain in the VSM	148
Feature History for Upgrading the Cisco Nexus 1000V	149

## APPENDIX A

### Installing and Upgrading VMware 151

VMware Release 4.0 to VMware Release 4.1 Upgrade	151
Upgrading from VMware Release 4.0 to VMware Release 4.1	151
Upgrading the vCenter Server to VMware Release 4.1	152
Upgrading the vCenter Update Manager to VMware Release 4.1	153
Upgrading the ESX/ESXi Hosts to VMware Release 4.1	154
Verifying the Upgrade to Release 4.1	157

VMware Release 4.0/4.1/5.0 to VMware Release 5.1 Upgrade	158
Upgrading from VMware Releases 4.0/4.1/5.0 to VMware Release 5.1	158
Upgrading the vCenter Server to Release 5.1	158
Upgrading the vCenter Update Manager to Release 5.1	160
Augmenting the Customized ISO for VMware Release 5.1	161
Upgrading the ESXi Hosts to Release 5.1	161
Verifying the Build Number and Upgrade	163
Upgrading to VMware ESXi 5.0 Patch 01	164
Upgrading a VMware ESXi 5.0 Stateful Host to VMware ESXi 5.0 Patch 01	164
Installing ESXi 5.1 Host Software Using the CLI	165
Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image	168

---

## APPENDIX B

<b>Installing the Cisco Nexus 1000V Software Using ISO or OVA Files</b>	<b>171</b>
Installing the VSM Software	171
Installing the Software from the ISO Image	171
Installing the Software from an OVA Image	176
Establishing the SVS Connection	187

---

## APPENDIX C

<b>Upgrading a Standalone VSM</b>	<b>193</b>
Upgrading a System with a Standalone VSM	193
Upgrading a Standalone VSM	193

---

## APPENDIX D

<b>Glossary</b>	<b>197</b>
Glossary for Cisco Nexus 1000V	197





## Preface

---

This preface contains the following sections:

- [Audience, page ix](#)
- [Document Conventions, page ix](#)
- [Related Documentation for Nexus 1000V Series NX-OS Software , page xi](#)
- [Documentation Feedback , page xii](#)
- [Obtaining Documentation and Submitting a Service Request, page xii](#)

## Audience

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

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

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



### Note

---

Knowledge of VMware vNetwork Distributed Switch is not required.

---

## Document Conventions

Command descriptions use the following conventions:

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

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

Examples use the following conventions:

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

This document uses the following conventions:



#### Note

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

**Caution**

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

## Related Documentation for Nexus 1000V Series NX-OS Software

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

[http://www.cisco.com/en/US/products/ps9902/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html)

### General Information

*Cisco Nexus 1000V Documentation Roadmap*

*Cisco Nexus 1000V Release Notes*

*Cisco Nexus 1000V and VMware Compatibility Information*

### Install and Upgrade

*Cisco Nexus 1000V Installation and Upgrade Guide*

### Configuration Guides

*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide*

*Cisco Nexus 1000V Interface Configuration Guide*

*Cisco Nexus 1000V Layer 2 Switching Configuration Guide*

*Cisco Nexus 1000V License Configuration Guide*

*Cisco Nexus 1000V Network Segmentation Manager Configuration Guide*

*Cisco Nexus 1000V Port Profile Configuration Guide*

*Cisco Nexus 1000V Quality of Service Configuration Guide*

*Cisco Nexus 1000V Security Configuration Guide*

*Cisco Nexus 1000V System Management Configuration Guide*

*Cisco Nexus 1000V vCenter Plugin Configuration Guide*

*Cisco Nexus 1000V VXLAN Configuration Guide*

### Programming Guide

*Cisco Nexus 1000V XML API Configuration Guide*

### Reference Guides

*Cisco Nexus 1000V Command Reference*

*Cisco Nexus 1000V MIB Quick Reference*

*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*

**Virtual Services Appliance Documentation**

The *Cisco Nexus Virtual Services Appliance* documentation is available at [http://www.cisco.com/en/US/products/ps9902/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html).

**Virtual Security Gateway Documentation**

The *Cisco Virtual Security Gateway for Nexus 1000V Series Switch* documentation is available at [http://www.cisco.com/en/US/products/ps11208/tsd\\_products\\_support\\_model\\_home.html](http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html).

**Virtual Wide Area Application Services (vWAAS) Documentation**

The *Virtual Wide Area Application Services* documentation is available at [http://www.cisco.com/en/US/products/ps6870/tsd\\_products\\_support\\_series\\_home.html](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](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 [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com). We appreciate your feedback.

## Obtaining Documentation and Submitting a Service Request

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

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

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





# Overview

---

This chapter contains the following sections:

- [Information About Virtualization, page 1](#)
- [Information About the Cisco Nexus 1000V, page 2](#)
- [Cisco Nexus 1000V and Its Components, page 3](#)
- [Information About the Virtual Supervisor Module, page 4](#)
- [Information About the Virtual Ethernet Module, page 6](#)
- [Information About Port Profiles, page 6](#)
- [Information About Administrator Roles, page 7](#)
- [Differences Between the Cisco Nexus 1000V and a Physical Switch, page 7](#)
- [Layer 3 and Layer 2 Control Modes, page 8](#)
- [System Port Profiles and System VLANs, page 10](#)
- [Recommended Topologies, page 11](#)
- [VMware Interaction, page 14](#)

## Information About Virtualization

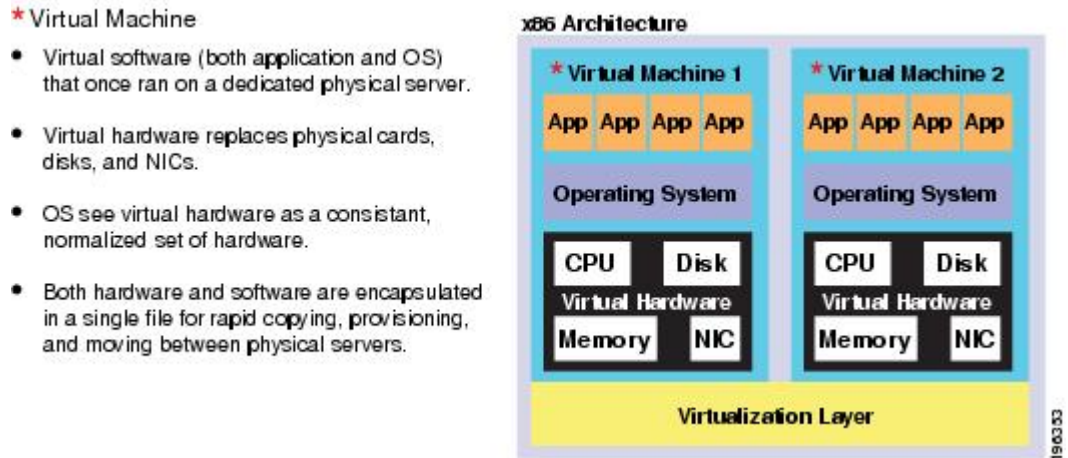
Virtualization allows multiple virtual machines to run in isolation, side by side on the same physical machine.

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

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

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

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



The following table lists the documents and videos that you need to use when performing a new installation or upgrade to this release.

Procedure	Document	Video
New Installation	<a href="#">Installing the Cisco Nexus 1000V, on page 15</a>	Choose one of the following: <ul style="list-style-type: none"> <li>• <a href="#">Cisco Nexus 1000V Release 4.2(1)SV2(1.1) Standard Installation</a></li> <li>• <a href="#">Cisco Nexus 1000V Release 4.2(1)SV2(1.1) Custom Installation</a></li> </ul>
Upgrading from Release 4.0(1)SV1(3) through Release 4.0(1)SV1(3d) to Release 4.2(1)SV1(5.2).	<a href="#">Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV2(1.1), on page 140</a>	<a href="#">Upgrading from Release 4.0(4)SV1(3, 3a, 3b) to Release 4.2(1)SV1(4)</a>
Upgrading from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a) or (5.2) to the current release.	<a href="#">Upgrading from Releases 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</a>	<a href="#">Upgrading the Cisco Nexus 1000V VSMs from Release 4.2(1)SV1(4) to Release 4.2(1)SV1(4a)</a>

## Information About the Cisco Nexus 1000V

The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is Ethernet standard compliant, including the Catalyst 6500 series switch, Cisco Nexus switches, and switches from other network

vendors. The Cisco Nexus 1000V is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL).

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

## Cisco Nexus 1000V and Its Components

**Note**

---

A list of terms used with the Cisco Nexus 1000V can be found in [Glossary, on page 197](#).

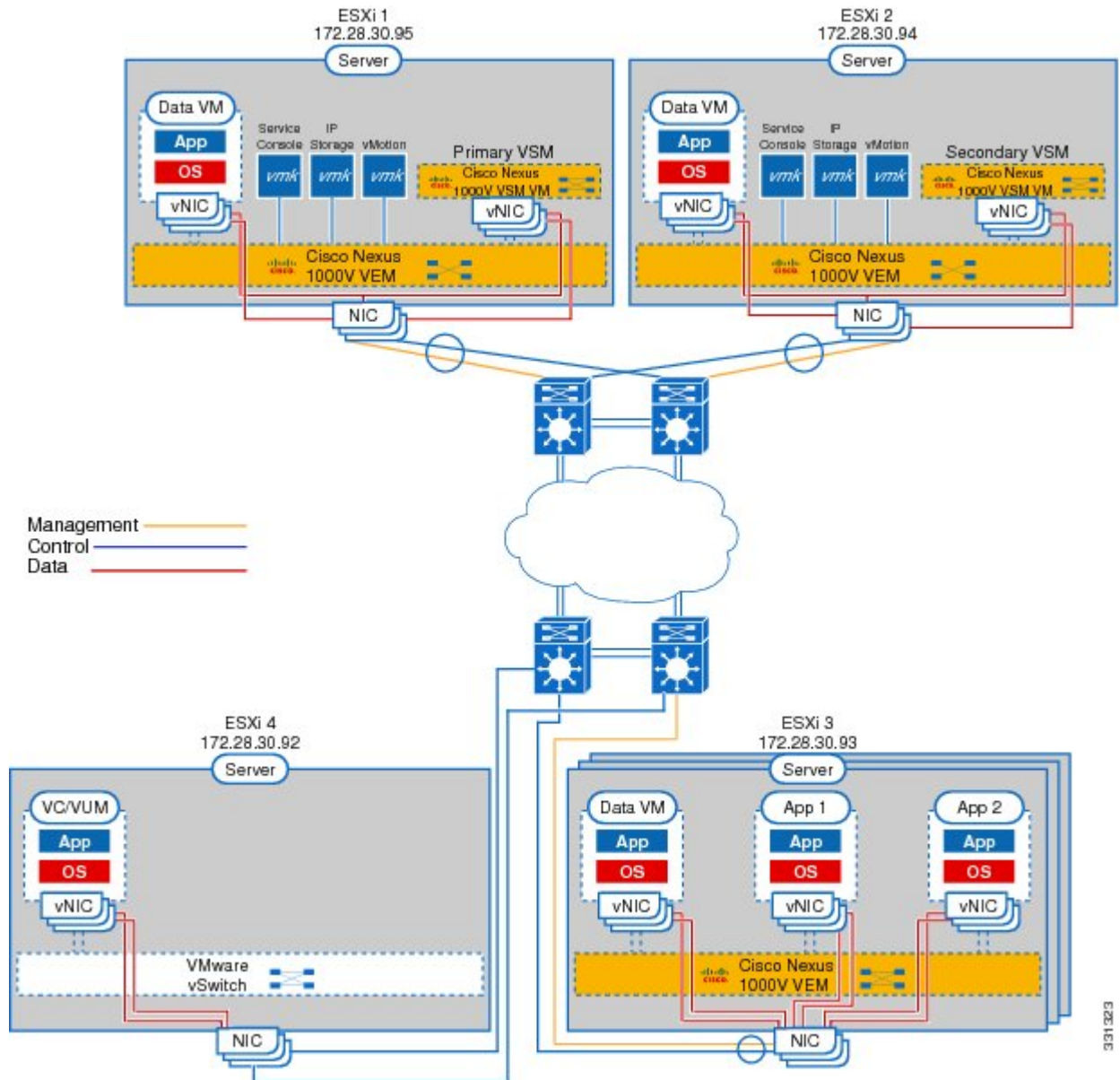
---

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

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

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

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



## Information About the Virtual Supervisor Module

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

- Configuration
- Management

- Monitoring
- Diagnostics
- Integration with VMware vCenter Server

A single VSM can manage up to 64 VEMs.



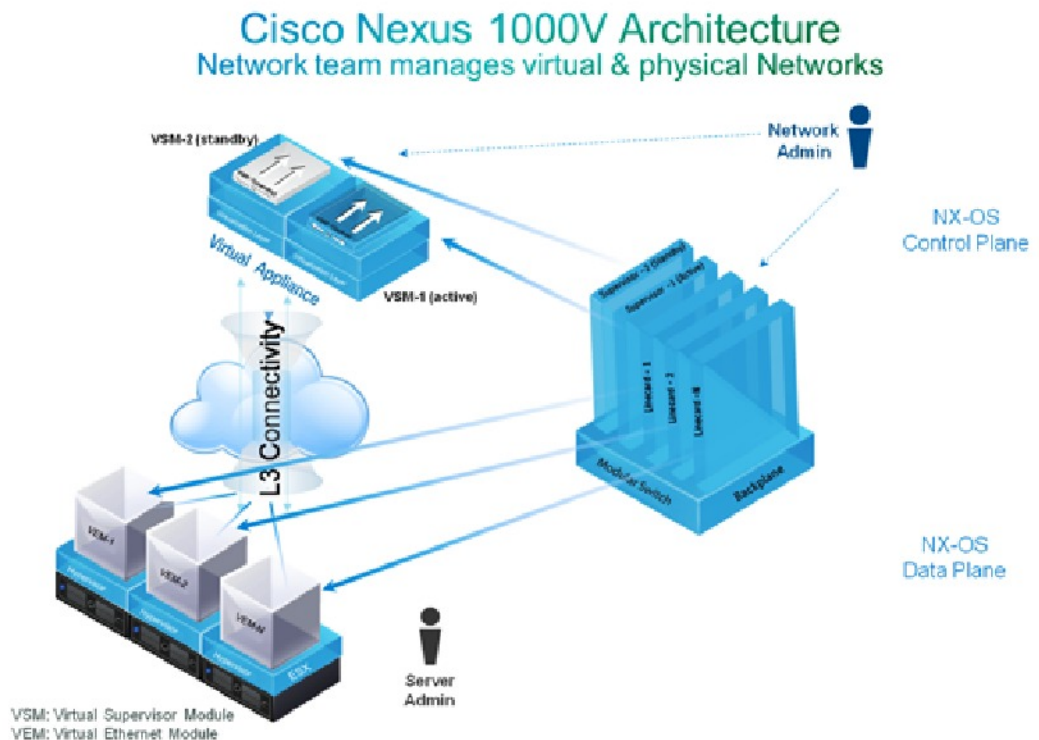
#### Note

We recommend an active/standby HA pair configuration.

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

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

**Figure 3: Cisco Nexus 1000V Architecture**



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

## Information About the Virtual Ethernet Module

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

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

**Note**

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

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

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

## Information About Port Profiles

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

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

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

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

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

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

## Information About Administrator Roles

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

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

Network Administrator	Server Administrator
<ul style="list-style-type: none"> <li>• Creates, configures, and manages virtual switches (VMware vSwitches).</li> <li>• Creates, configures, and manages port profiles, including the following:               <ul style="list-style-type: none"> <li>◦ Security</li> <li>◦ Port channels</li> <li>◦ QoS policies</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Assigns the following to port groups:               <ul style="list-style-type: none"> <li>◦ vNICs</li> <li>◦ VMkernel interfaces</li> <li>◦ Service console interfaces</li> </ul> </li> <li>• Assigns physical NICs (also called PNICs).</li> </ul>

## Differences Between the Cisco Nexus 1000V and a Physical Switch

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

- Joint management by network and server administrators

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

## Layer 3 and Layer 2 Control Modes

### VSM to VEM Communication

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

#### Layer 3 Control Mode

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

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

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

#### Layer 2 Control Mode

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

For more information on Layer 2 control mode, see [Configuring Layer 2 Connectivity, on page 64](#) and [Migrating from Layer 2 to Layer 3](#).



# Management, Control, and Packet VLANs

## Information About the Control VLAN

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

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

## Management VLANs

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

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

## Information About the Packet VLAN

**Note**

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

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

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

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

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

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

# System Port Profiles and System VLANs

## Information About System Port Profiles

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

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

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

**Caution**

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

## Information About System VLANs

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

The following ports must use system VLANs:

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

**Caution**

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

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

**Note**

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

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

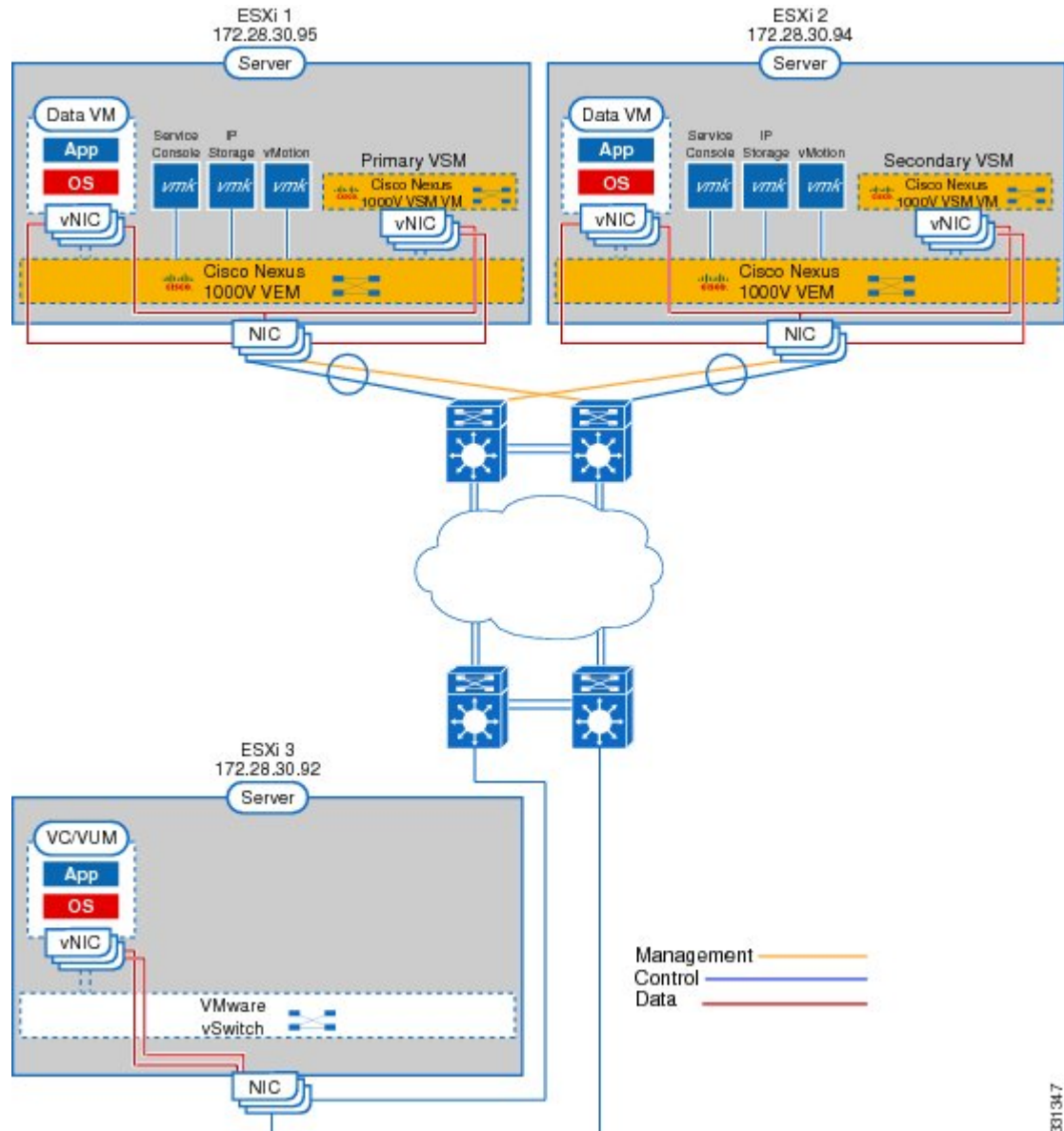
## Recommended Topologies

### Layer 3 Topology

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

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

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

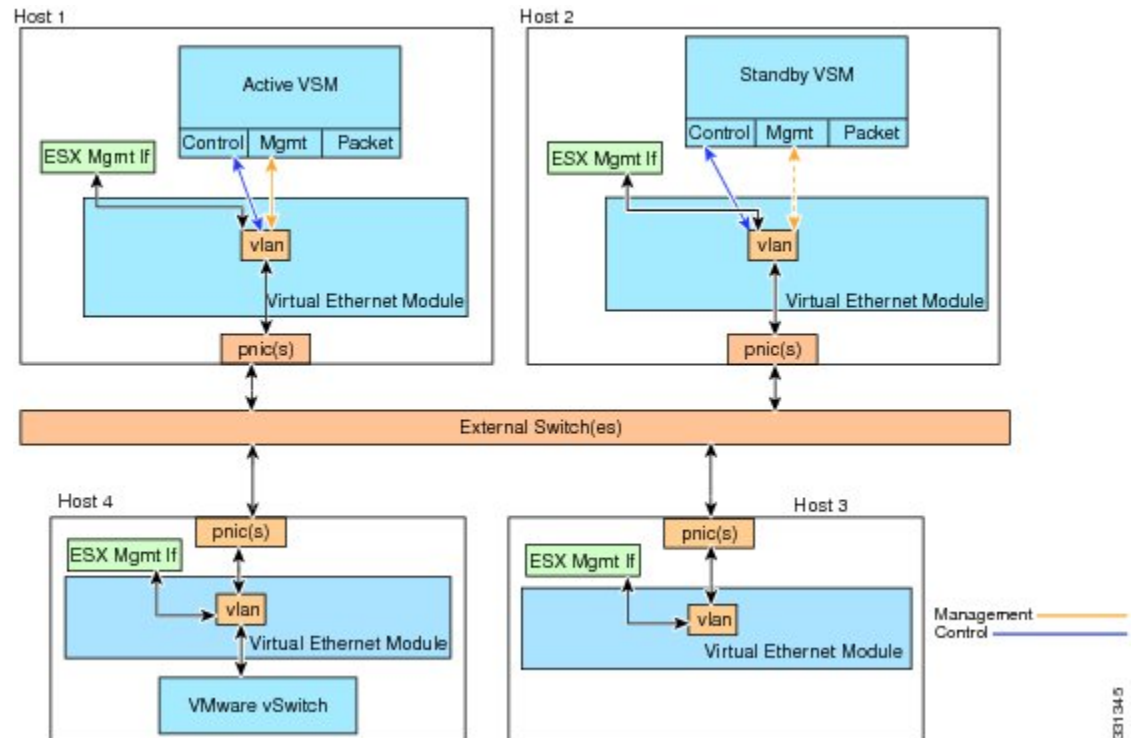


33134.7

## Control and Management on the Same VLAN Topology

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

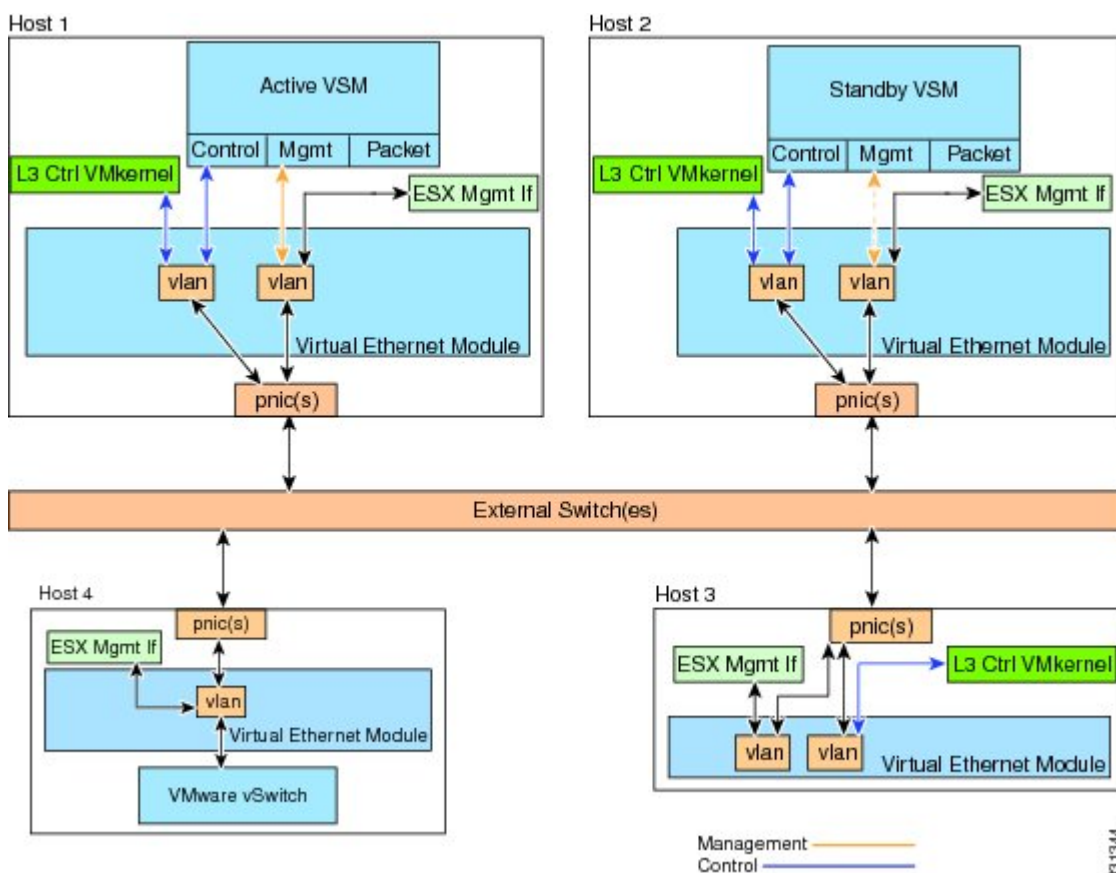
**Figure 5: Control and Management on Same VLAN**



## Control and Management on Separate VLANs Topology

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

**Figure 6: Control and Management on Separate VLAN**



## VMware Interaction

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

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



# Installing the Cisco Nexus 1000V

---

This chapter contains the following sections:

- [Information About Installing the Cisco Nexus 1000V, page 16](#)
- [Prerequisites for Installing the Cisco Nexus 1000V, page 17](#)
- [Guidelines and Limitations, page 21](#)
- [Installing a VSM HA Pair with L3 Mode Behind a VEM Using the Cisco Nexus 1000V Installer App, page 23](#)
- [Installing VSM Software Using the Cisco Nexus 1000V Installer App, page 23](#)
- [Installing Cisco Nexus 1000V in Standard Mode, page 23](#)
- [Installing the Cisco Nexus 1000V in Custom Mode, page 39](#)
- [Information About Layer 2 Connectivity, page 62](#)
- [Installing the VEM Software Using the Cisco Nexus 1000V Installer App, page 65](#)
- [Adding VEM Hosts to the Distributed Virtual Switch, page 74](#)
- [Setting Virtual Machine Startup and Shutdown Parameters, page 78](#)
- [Installing the VEM Software Using VUM, page 81](#)
- [Installing the VEM Software Using the CLI, page 82](#)
- [Installing VEM Software Locally on a VMware 4.1 Host by Using the CLI, page 82](#)
- [Installing the VEM Software Remotely on a VMware 4.1 Host by Using the CLI, page 83](#)
- [Installing the VEM Software Locally on a VMware 5.0 Host by Using the CLI, page 85](#)
- [Installing VEM Software Remotely on a VMware 5.0 Host by Using the CLI, page 86](#)
- [Installing the VEM Software on a Stateless ESXi Host, page 87](#)
- [Installing a VSM on the Cisco Nexus 1010 , page 92](#)
- [Feature History for Installing the Cisco Nexus 1000V, page 95](#)

# Information About Installing the Cisco Nexus 1000V

## VSM Software

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

[Cisco Nexus 1000V Download Software page](#)

The file name is `Nexus1000v.4.2.1.SV2.1.1.zip`.

## VEM Software

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

**Table 1: VEM Software Sources**

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

## Information About the Cisco Nexus 1000V Installer App

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

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

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

The migration process supports Layer 2 and Layer 3 topologies.

The installer does the following:

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



**Note**

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

- Enables Telnet and Secure Shell (SSH) and configures an SSH connection.
- Creates a Cisco Nexus 1000V plug-in and registers it on the vCenter Server.
- Migrates each VMware port group or kernel NIC to the correct port profile.
- Migrates each physical network interface card (PNIC) from the VMware vSwitch to the correct uplink on the DVS.
- Adds the host to the DVS.
- The Cisco Nexus 1000V Installer App provides a quick method for a user to 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 best practice recommendations in the deployment of Cisco Nexus 1000V: [http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide\\_c07-556626.html](http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html).

## Prerequisites for Installing the Cisco Nexus 1000V

### Cisco Nexus 1000V Installer App Prerequisites

**Note**

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

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

- The host must have one or more physical NICs on each VMware vSwitch in use.
- The VMware vSwitch must not have any active VMs.  
To prevent a disruption in connectivity during migration, any VMs that share a VMware vSwitch with port groups used by the VSM must be powered off.
- You must also configure the VSM connection to the vCenter server datacenter where the host resides.
- Host should have only one VMware vSwitch.
- Make sure no VEMs were previously installed on the host where the VSM resides.
- You must have administrative credentials for the vCenter Server.
- The java.exe file must be located within the search path defined in your system.

### Host Prerequisites

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

- You have already installed and prepared the vCenter Server for host management using the instructions from VMware.
- You should have the VMware vSphere Client installed.
- You have already installed the VMware Enterprise Plus license on the hosts.
- All VEM hosts must be running ESX/ESXi 4.1 or later releases.
- You have two physical NICs on each host for redundancy. Deployment is also possible with one physical NIC.
- If you are using a set of switches, make sure that the inter-switch trunk links carry all relevant VLANs, including control and packet VLANs. The uplink should be a trunk port that carries all VLANs configured on the host.
- The control and management VLANs must already be configured on the host to be used for the VSM VM.
- Make sure that the VM to be used for the VSM meets the minimum requirements listed in the following table.
- All the vmnics should have the same configuration upstream.

**Caution**

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

The following table lists the minimum requirements for hosting a VSM.

**Table 2: Minimum Requirements for a VM Hosting a VSM**

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

<sup>1</sup> 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 171](#) to reserve RAM and set the memory size.

<sup>2</sup> 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 171](#) to reserve RAM and set the memory size.

## Upstream Switch Prerequisites

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

- If you are using a set of switches, make sure that the inter-switch trunk links carry all relevant VLANs, including the control and packet VLANs. The uplink must be a trunk port that carries all the VLANs that are configured on the host.
- The following spanning tree prerequisites apply to the switch upstream from the Cisco Nexus 1000V on the ports connected to the VEM.
  - On upstream switches, the following configuration is mandatory:  
 On your Catalyst series switches with Cisco IOS software, enter the following command:  
 (config-if) **spanning-tree portfast trunk**  
 or  
 (config-if) **spanning-tree portfast edge trunk**  
 On your Cisco Nexus 5000 series switches with Cisco NX-OS software, enter the following command:  
 (config-if) **spanning-tree port type edge trunk**
  - On upstream switches we highly recommend that you enable the following globally:  
 Global BPDU Filtering  
 Global BPDU Guard
  - On upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:  
 (config-if) **spanning-tree bpdu filter**  
 (config-if) **spanning-tree bpdu guard**

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

- Run the following commands on the upstream switch:

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

end
```

## VSM Prerequisites

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

- You have the VSM IP address.

- You have installed the appropriate vCenter Server and VMware Update Manager (VUM) versions.
- If you are installing redundant VSMs, make sure that you first install and set up the software on the primary VSM before installing and setting up the software on the secondary VSM.
- You have already identified the HA role for this VSM from the list in the following table.

**Table 3: HA Roles**

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

**Note**

A standalone VSM is not supported in a production environment.

- You are familiar with the Cisco Nexus 1000V topology diagram that is shown in [Layer 3 Topology, on page 11](#).

## VEM Prerequisites

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

**Note**

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

- When you perform any VUM operation on hosts that are a part of a cluster, ensure that VMware HA, VMware fault tolerance (FT), and VMware distributed power management (DPM) features are disabled for the entire cluster. Otherwise, VUM cannot install the hosts in the cluster.
- 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.
- You have already obtained a copy of the VEM software file from one of the sources listed in [VEM Software, on page 16](#).
- You have already downloaded the correct VEM software based on the current ESX/ESXi host patch level. For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.
- For a VUM-based installation, you must deploy VUM and make sure that the VSM is connected to the vCenter Server.

# Guidelines and Limitations

## Guidelines and Limitations of the Cisco Nexus 1000V Installer App

Configuring the software using the Cisco Nexus 1000V Installer App has the following guidelines and limitations:

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

**Caution**

Host management connectivity might be interrupted if the management vmknics or vswifs 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*.
- For a user using the VC Connection installer, once the SVS connection is completed, the user must check the VSM using the **show svcs connection** command to view an accurate status.
- Layer 3 mode of deployment is supported by the Cisco Nexus 1000V Installer App with ESXi host only.
- VEM installation and migration are supported for a maximum of four vmknics in a single subnet per host to deploy 64 VEMs. No more than four vmknics can be present on a single host during VEM installations.
- The Cisco Nexus 1000V Installer App can support 14 different subnets during module additions when reusing port profiles.
- The Cisco Nexus 1000V Installer App will always deploy with VSM HA pairs.
- If the Installer App fails, check the vCenter Server event status. If an event shows failure due to a timeout, then it could be because of a vCenter Server overload. Please consult the VMware website to address a vCenter Server overload event.

## Guidelines and Limitations for Installing the Cisco Nexus 1000V

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.

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 a VSM HA Pair with L3 Mode Behind a VEM Using the Cisco Nexus 1000V Installer App

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

### Procedure

- 
- Step 1** [Installing VSM Software Using the Cisco Nexus 1000V Installer App, on page 23](#)
  - Step 2** [Installing the VEM Software Using the Cisco Nexus 1000V Installer App, on page 65](#)
  - Step 3** [Adding VEM Hosts to the Distributed Virtual Switch, on page 74](#)
  - Step 4** [Setting Virtual Machine Startup and Shutdown Parameters, on page 78](#)
- 

## 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 Cisco Nexus 1000V in Standard Mode, on page 23](#)
- [Installing the Cisco Nexus 1000V in Custom Mode, on page 39](#)

## Installing Cisco Nexus 1000V in Standard Mode

### Before You Begin

- You have the following information:



---

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

---

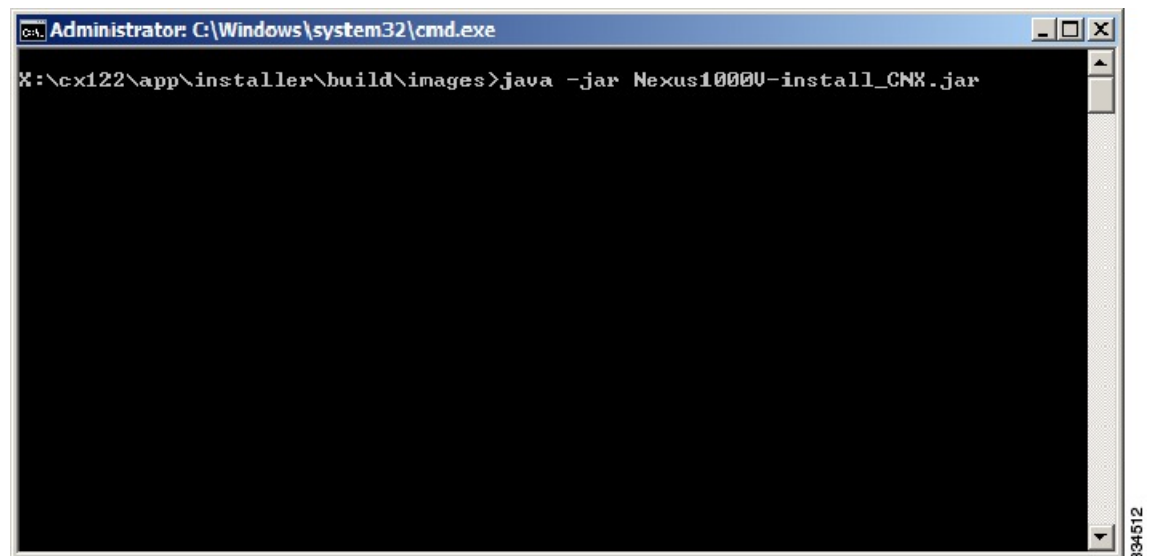
- Management VLAN ID
- Domain ID
- Management IP address

- 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 the user selects the migration to DVS option as yes, then the migration of hosts that have VSMs will migrate all the interfaces under the vSwitch that have the ESXi management interface (say vmk0 ).

## Procedure

- Step 1** Double-click on 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
```

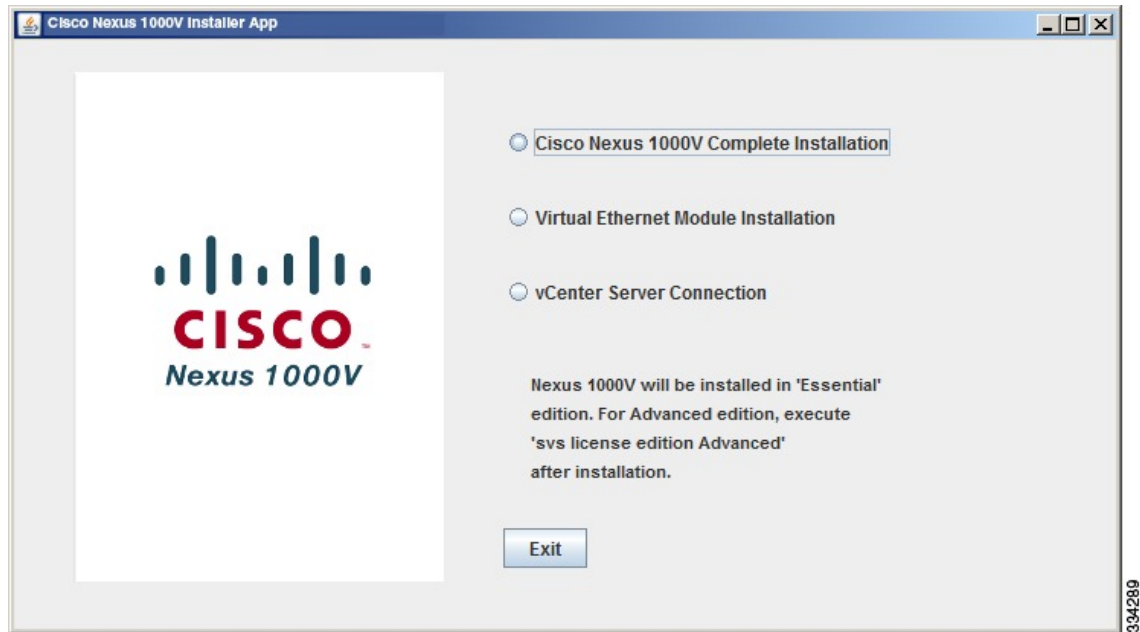
*Figure 7: Command Line Interface*





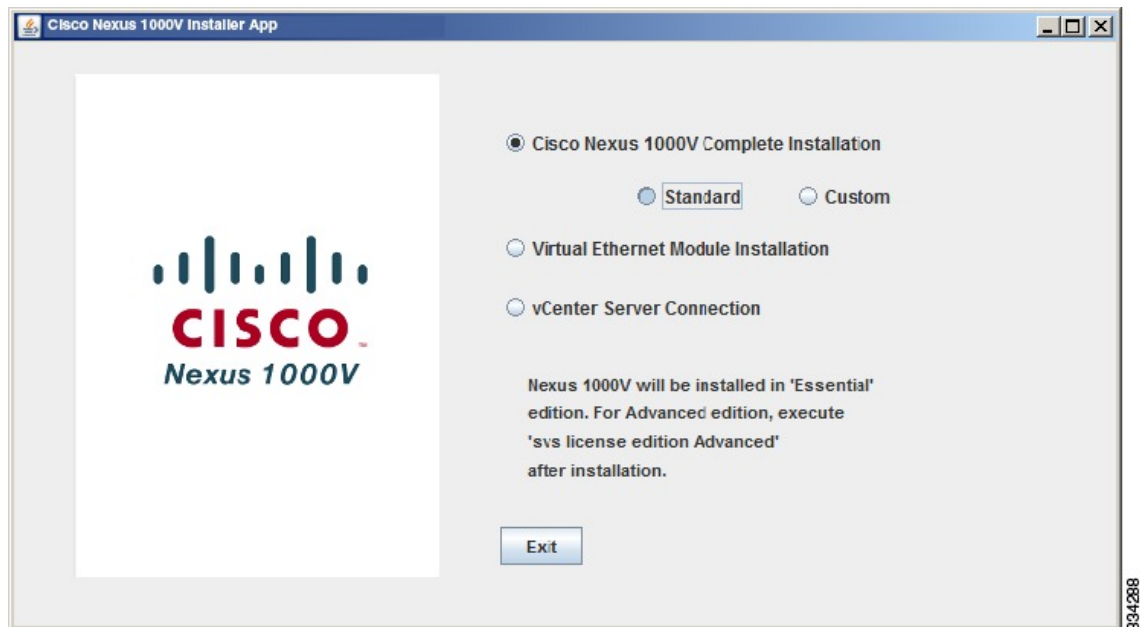
**Step 2** Click the **Cisco Nexus 1000V Complete Installation** radio button.

**Figure 8: Standard Cisco Nexus 1000V Complete Installation Screen**



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

**Figure 9: Standard Option Screen**



**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**.

**Figure 10: vCenter Server Credentials Screen**

The screenshot shows the 'vCenter Server Credentials' screen of the Cisco Nexus 1000V Installer App. On the left, a 'Steps' pane lists the installation process: 1. Prerequisites, 2. vCenter Server Credentials (highlighted), 3. Basic Configuration Data, 4. Basic Configuration Review, 5. Confirmation, 6. Hosts Selection, and 7. Host Review. Below the steps is the Cisco logo and 'Nexus 1000V' text. The main area contains four input fields: 'IP Address' with the value '172.23.181.10', 'Port (https only)' with '443', 'User ID' with 'Administrator', and 'Password' with masked characters '\*\*\*\*\*'. At the bottom right are four buttons: '< Prev', 'Next >' (highlighted), 'Finish', and 'Cancel'. A vertical text '334281' is on the far right edge.

| vCenter Server Credentials |               |
|----------------------------|---------------|
| IP Address                 | 172.23.181.10 |
| Port (https only)          | 443           |
| User ID                    | Administrator |
| Password                   | *****         |

< Prev   Next >   Finish   Cancel

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

**Figure 11: Standard Configuration Data Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. On the left, a 'Steps' pane lists the installation process: 1. Prerequisites, 2. vCenter Server Credentials, 3. **Standard Configuration Data** (highlighted), 4. Standard Configuration Review, 5. Confirmation, 6. Hosts Selection, and 7. Host Review. Below the list is the Cisco Nexus 1000V logo. The main area is titled 'Standard Configuration Data' and contains an 'Import Configuration' button at the top. Below it are fields for 'Host 1' and 'Host 2', each with 'IP Address / Name' and 'Data Store' fields, each followed by a 'Browse' button. There are also fields for 'Virtual Machine Name' and 'OVA Image Location' with a 'Browse' button. The 'Layer 2 / Layer 3 Connectivity' section has radio buttons for 'Layer L2' and 'Layer L3' (selected). Below this are fields for 'VSM IP Address', 'Subnet Mask', 'Gateway IP Address', 'Domain ID', and 'Management VLAN'. The 'Migrate Host(s) to DVS' section has radio buttons for 'Yes' and 'No' (selected). A 'Save Configuration' button is at the bottom left of the main area. A status bar at the bottom says 'Enter a valid primary host IP address.' and navigation buttons '< Prev', 'Next >', 'Finish', and 'Cancel' are on the right. A vertical text '334443' is on the far right edge.

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

- Choose the host for the primary VSM.
- 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.

**Figure 12: Standard Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Standard Configuration Data**
4. Standard Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Standard Configuration Data**

Import Configuration

Host 1

IP Address / Name: esx-host-146.cisco.com **Browse**

Data Store: datastore1 (2) **Browse**

Host 2

IP Address / Name: **Browse**

Data Store: **Browse**

Virtual Machine Name:

OVA Image Location: **Browse**

Layer 2 / Layer 3 Connectivity: ☒ Layer L2 ☐ Layer L3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Management VLAN: 232

Migrate Host(s) to DVS: ☐ Yes ☒ No

**Save Configuration**

Enter a valid secondary host IP address

< Prev Next > Finish Cancel

**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.

**Figure 13: Standard Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Standard Configuration Data**
4. Standard Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Standard Configuration Data**

Import Configuration

Host 1

IP Address / Name: esx-host-146.cisco.com Browse

Data Store: datastore1 (2) Browse

Host 2

IP Address / Name: esx-host-133.cisco.com Browse

Data Store: datastore1 (1) Browse

Virtual Machine Name:

OVA Image Location:  Browse

Layer 2 / Layer 3 Connectivity: ☐ Layer L2 ☒ Layer L3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Management VLAN: 232

Migrate Host(s) to DVS: ☐ Yes ☒ No

Save Configuration

Enter a valid Virtual Machine Name (No special characters allowed, Maximum 80 characters).

< Prev Next > Finish Cancel

**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**.

**Figure 14: Standard Configuration Data Screen**

The screenshot shows the 'Standard Configuration Data' screen in the Cisco Nexus 1000V Installer App. The left sidebar lists the installation steps: 1. Prerequisites, 2. vCenter Server Credentials, 3. Standard Configuration Data (selected), 4. Standard Configuration Review, 5. Confirmation, 6. Hosts Selection, and 7. Host Review. The main configuration area includes an 'Import Configuration' button, fields for Host 1 and Host 2 (IP Address / Name, Data Store), Virtual Machine Name, OVA Image Location, Layer 2 / Layer 3 Connectivity (Layer L2 and Layer L3), VSM IP Address, Subnet Mask, Gateway IP Address, Domain ID, Management VLAN (set to 232), and a checkbox for 'Migrate Host(s) to DVS' (set to No). A 'Save Configuration' button is located at the bottom left. A status bar at the bottom indicates 'Enter a valid OVA image location'. Navigation buttons '< Prev', 'Next >', 'Finish', and 'Cancel' are at the bottom right.

**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 allows you to import and pre-populate common values in the template for later use.

d) Click **Next**.

**Figure 15: Standard Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Standard Configuration Data**
4. Standard Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Standard Configuration Data**

Import Configuration

Host 1

IP Address / Name: esx-host-146.cisco.com Browse

Data Store: datastore1 (2) Browse

Host 2

IP Address / Name: esx-host-133.cisco.com Browse

Data Store: datastore1 (1) Browse

Virtual Machine Name: demo

OVA Image Location: ages/final/nexus-1000v-4.2.1.SV2.1.0.122.ova Browse

Layer 2 / Layer 3 Connectivity: ☐ Layer L2 ☒ Layer L3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Management VLAN: 232

Migrate Host(s) to DVS: ☐ Yes ☒ No

Save Configuration

Please enter a valid management IP address. (i.e. 192.168.0.10)

< Prev Next > Finish Cancel

**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.

Figure 16: Standard Configuration Review Screen

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
3. Standard Configuration Data
- 4. Standard Configuration Review**
5. Confirmation
6. Hosts Selection
7. Host Review

**Standard Configuration Review**

Host 1

IP Address / Name: esx-host-146.cisco.com

Data Store: datastore1 (2)

Host 2

IP Address / Name: esx-host-133.cisco.com

Data Store: datastore1 (1)

Virtual Machine Name: demo

OVA Image Location: X:\cx122\build\images\final\nexus-1000v.4.2.1.SV2.1.0.122.ova

Layer 2 / Layer 3 Connectivity: ☒ Layer 2 ☐ Layer 3

VSM IP Address: 172.23.232.102

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.23.232.1

Domain ID: 1029

Management VLAN: 232

Migrate Host(s) to DVS: ☒ Yes ☐ No

Notes: The Nexus 1000V VSM will be named "demo" and its password will be set to "admin". The portgroups n1kv-mgmt and n1kv-ctrl will be created with the above Management

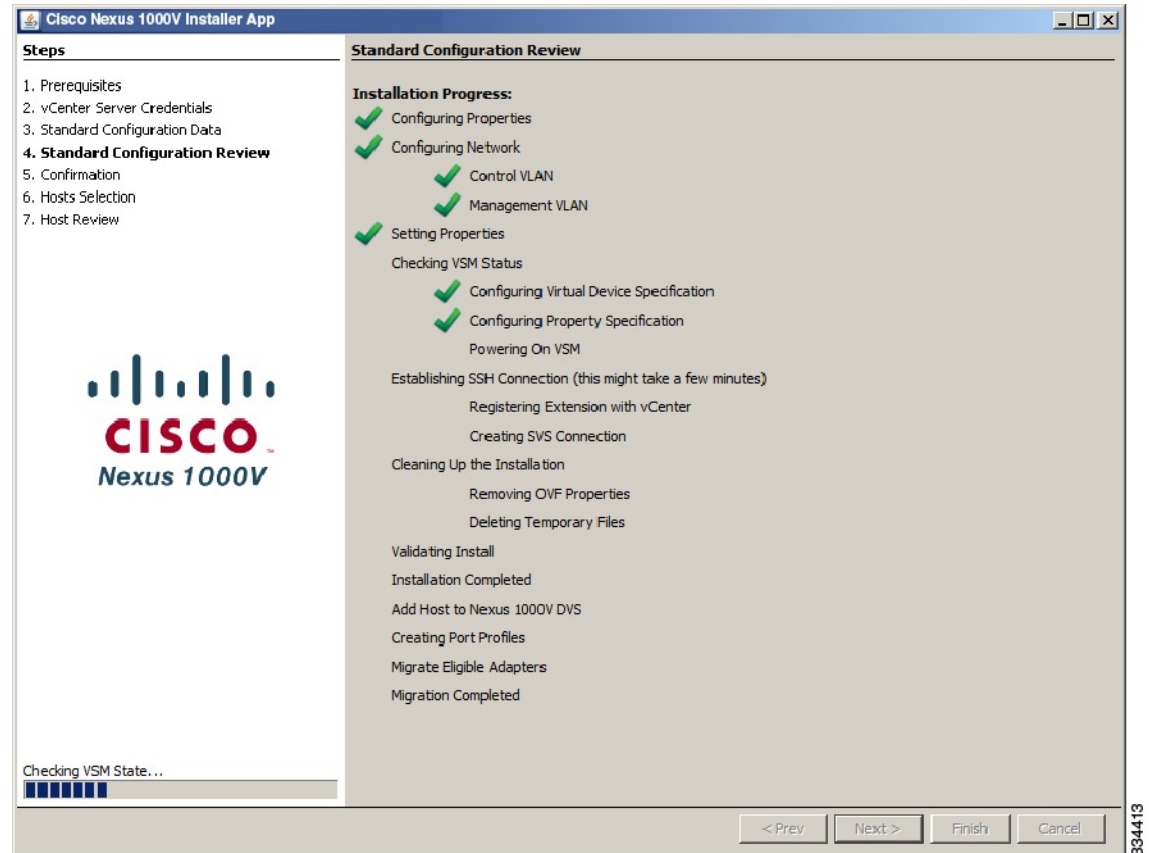
< Prev Next > Finish Cancel

334423



The **Standard Installation Progress** screen opens.

**Figure 17: Standard Installation Progress Screen**

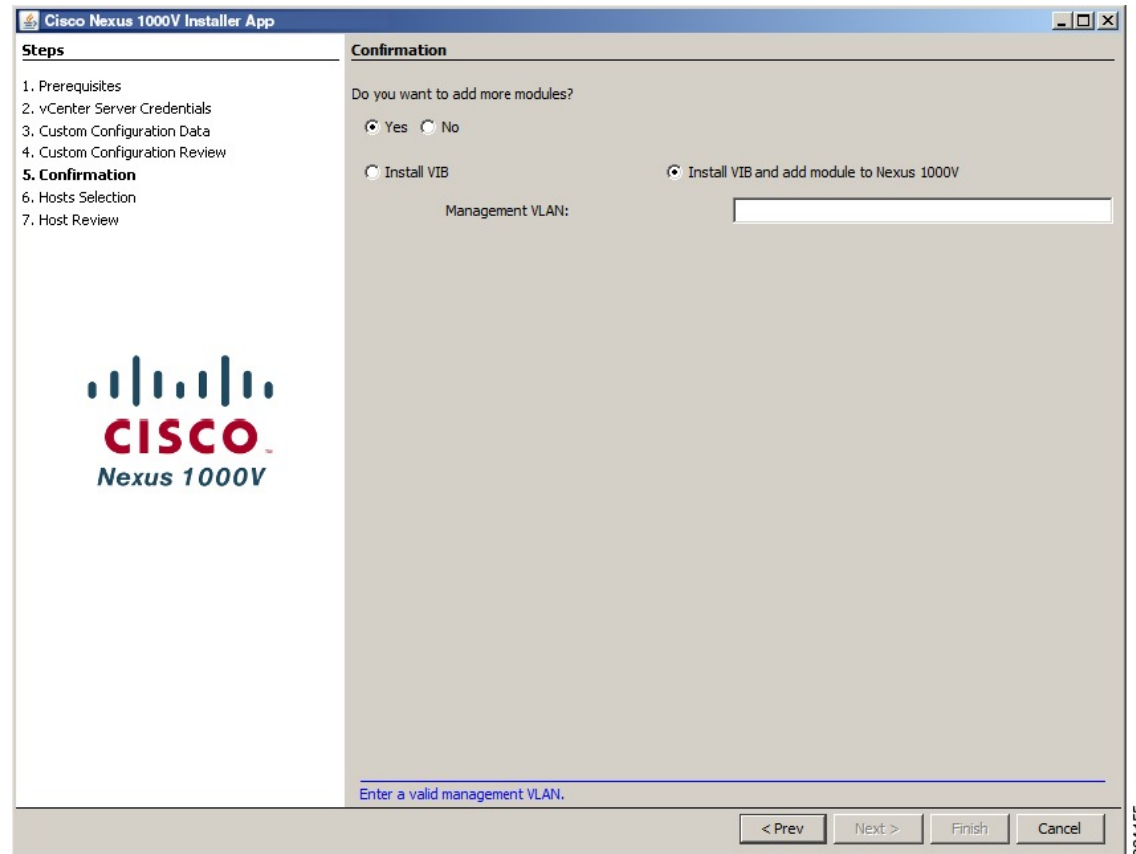


When the installation process completes, the **Confirmation** screen is displayed. A typical installation of the VSM takes about 6-8 minutes.

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

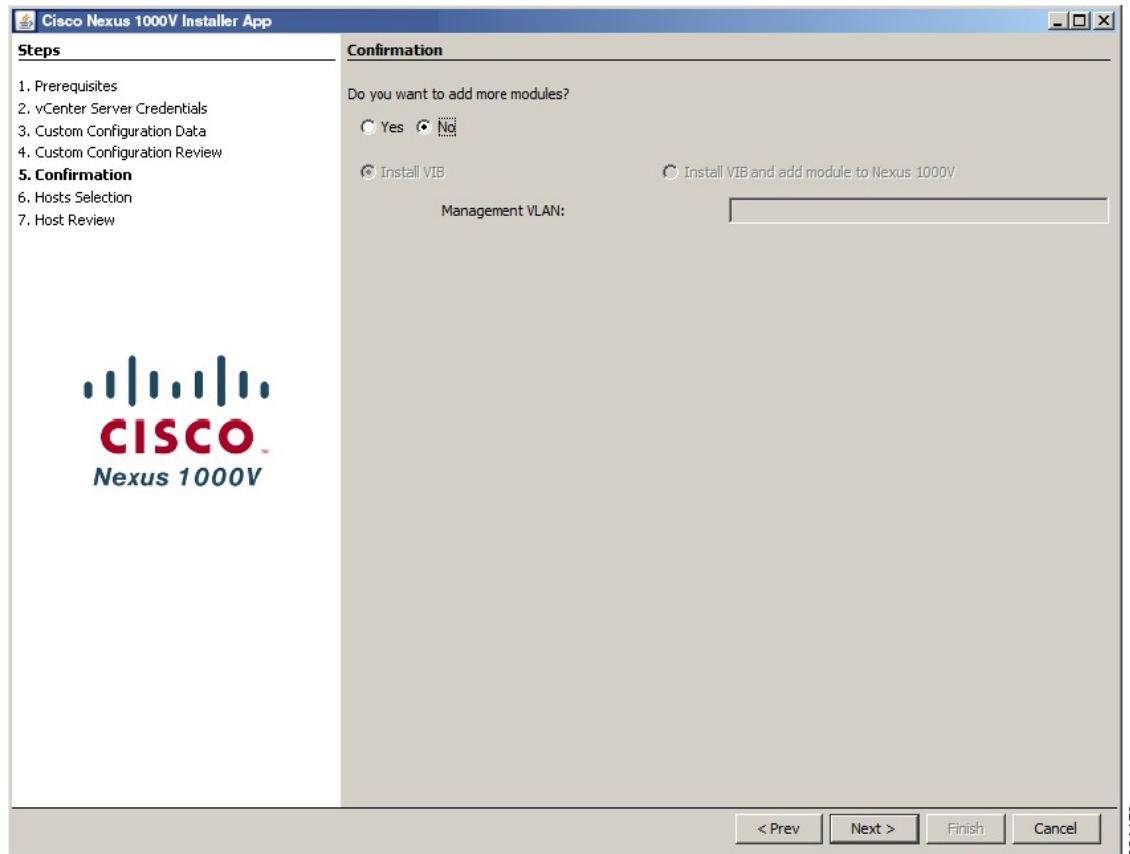
- Click **Yes** if you want to add more modules and continue to the next step.

**Figure 18: Confirmation Screen**



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

**Figure 19: Not Adding Modules Screen**



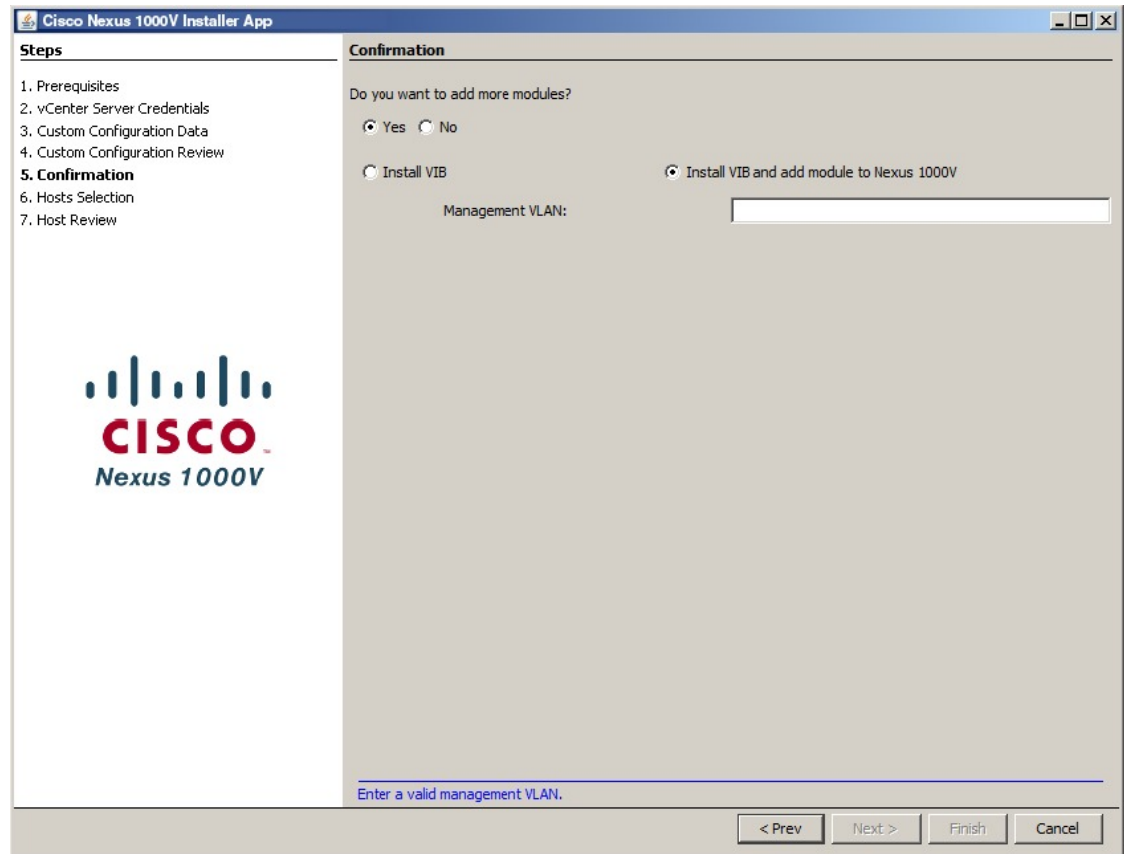
**Step 15** In the **Adding Modules** screen, do the following:

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 Nexus 1000V.

- b) Enter a VLAN ID in the **Management VLAN** field.

**Figure 20: Adding Modules Screen**

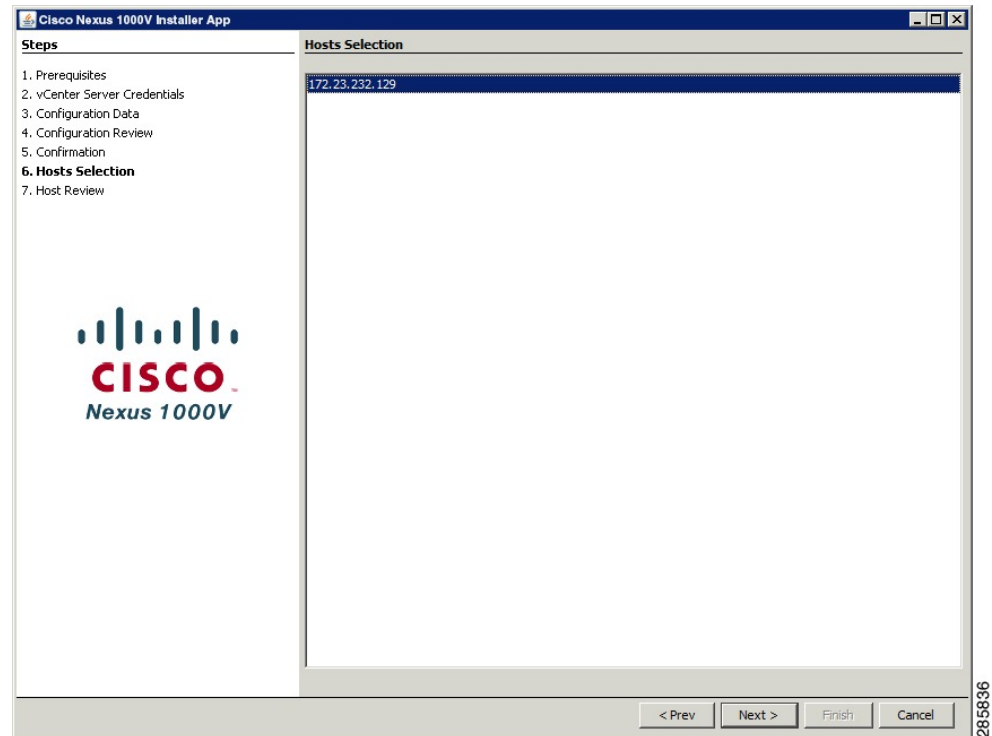


**Step 16** In the **Hosts Selection** screen, do the following:

- a) Choose the hosts you want to add.

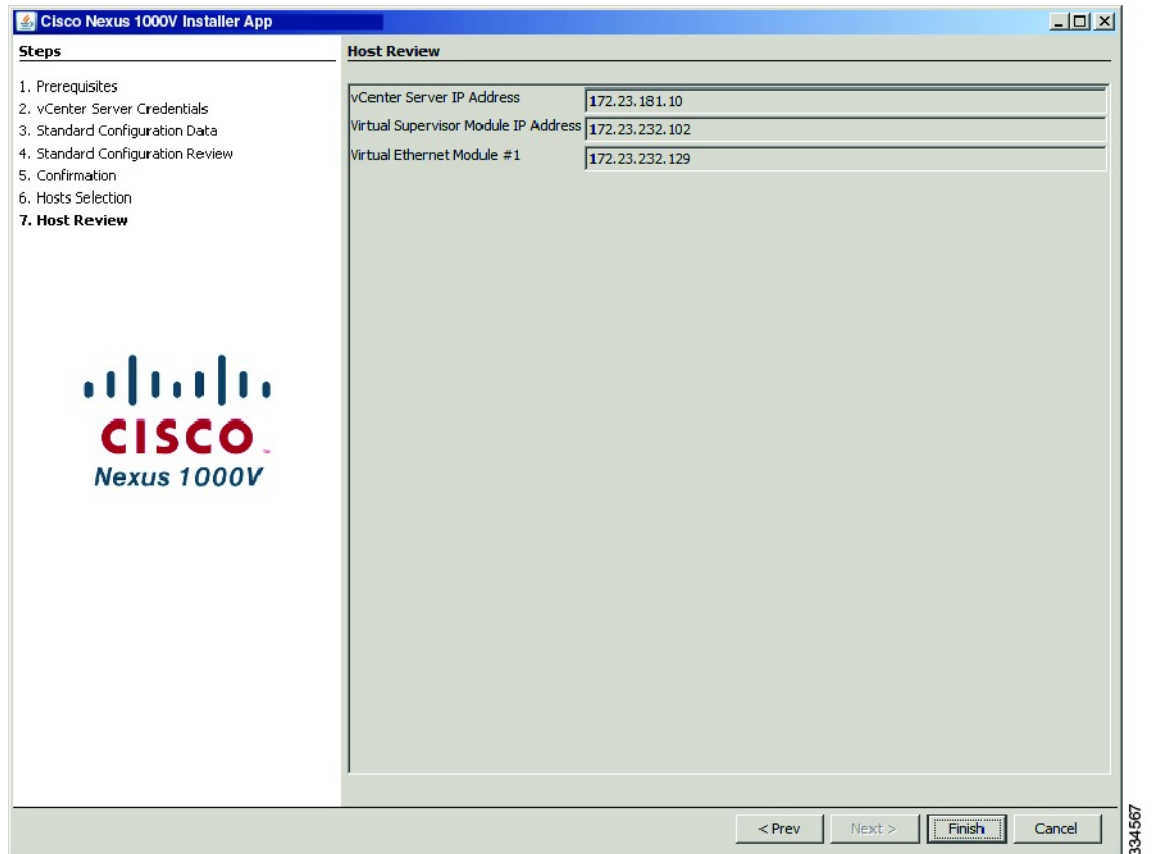
b) Click **Next**.

**Figure 21: Hosts Selection Screen**



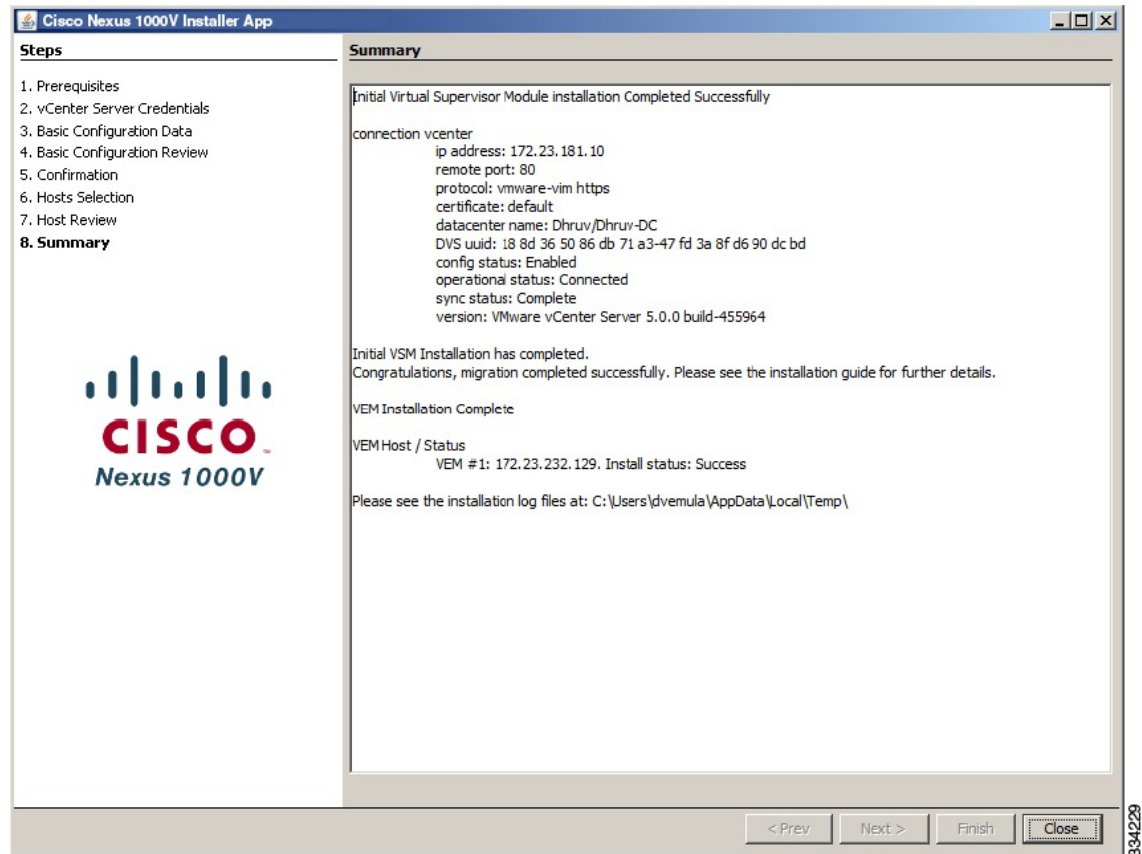
**Step 17** In the **Host Review** screen, do the following:

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

**Figure 22: Host Review Screen**

**Step 18** Click Close.

**Figure 23: Summary Screen**



## Installing the Cisco Nexus 1000V in Custom Mode

### Before You Begin

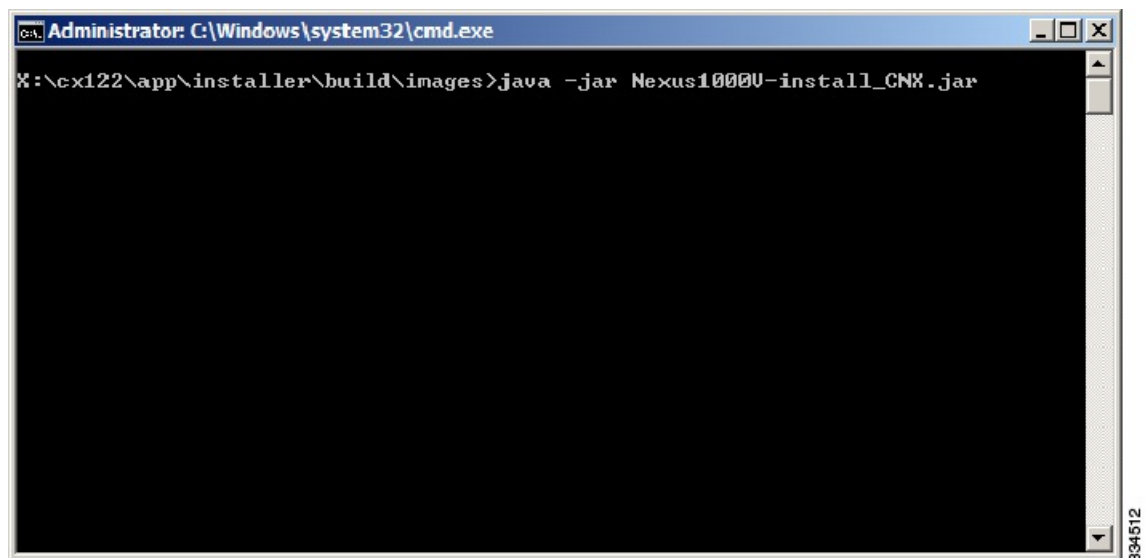
- You have the following information:
  - Control VLAN ID
  - Packet VLAN ID
  - Management VLAN ID
  - Domain ID
  - Management IP address
  - Subnet mask

- 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 on 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
```

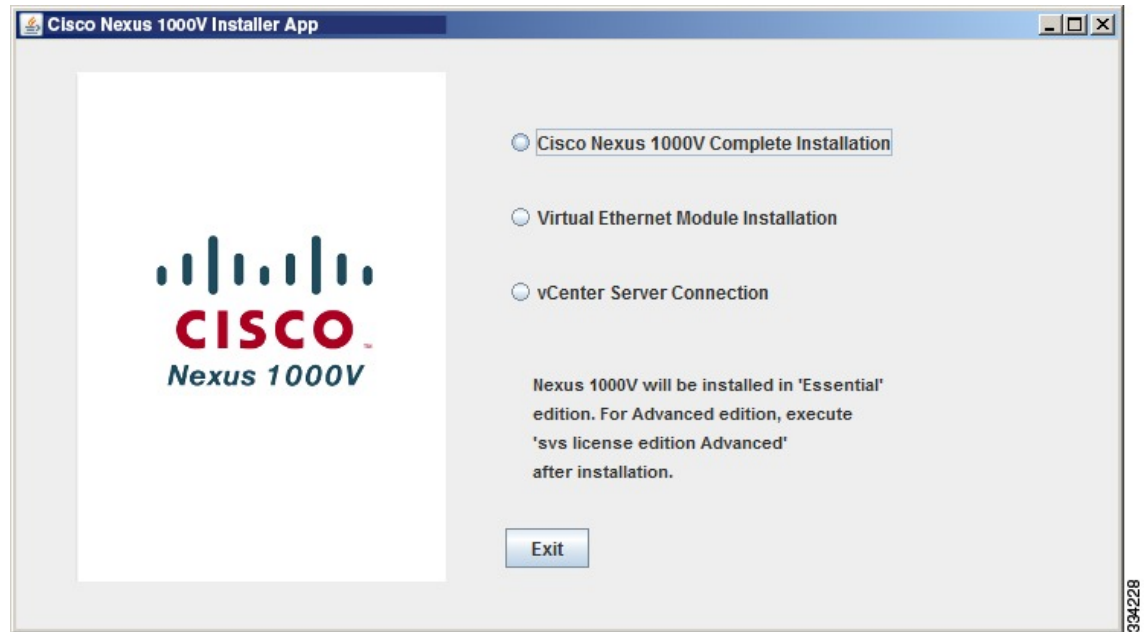
*Figure 24: Command Line Interface*





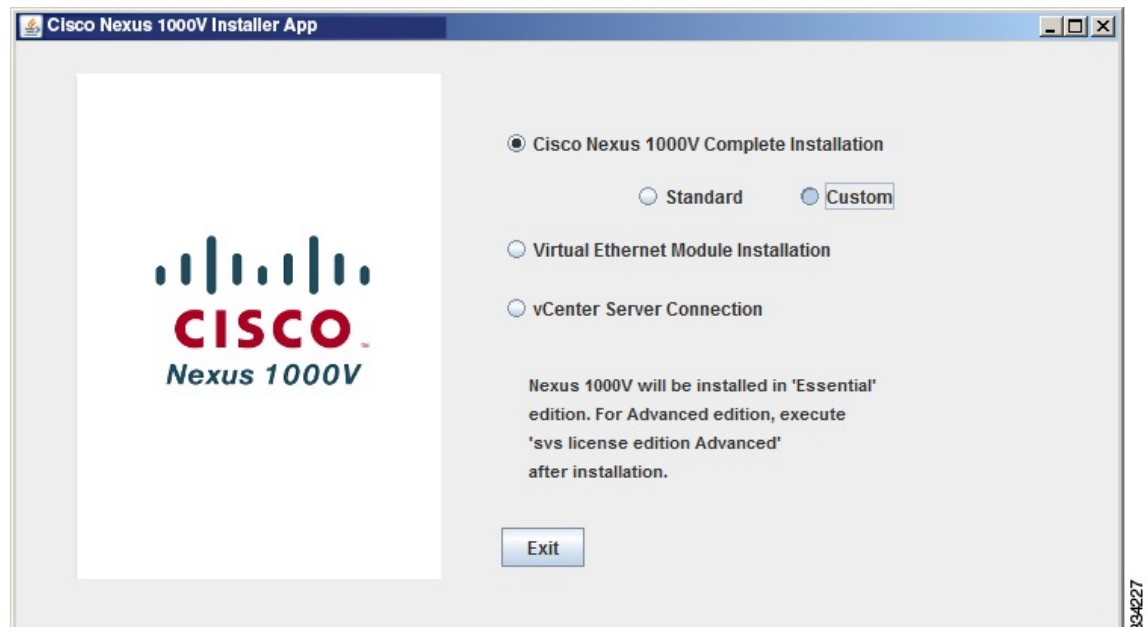
**Step 2** Click the **Cisco Nexus 1000V Complete Installation** radio button.

**Figure 25: Cisco Nexus 1000V Complete Installation Screen**



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

**Figure 26: Custom Installation**



**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**.

**Figure 27: vCenter Server Credentials Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. On the left, a 'Steps' list shows the progress: 1. Prerequisites, 2. vCenter Server Credentials (current), 3. Custom Configuration Data, 4. Custom Configuration Review, 5. Confirmation, 6. Hosts Selection, and 7. Host Review. Below the list is the Cisco logo and 'Nexus 1000V'. The main area is titled 'vCenter Server Credentials' and contains four input fields: 'IP Address' (172.23.181.10), 'Port (https only)' (443), 'User ID' (Administrator), and 'Password' (masked with asterisks). At the bottom right are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'. A vertical text '334219' is on the far right edge.

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

**Figure 28: Custom Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

Import Configuration

Host 1

IP Address / Name

Data Store

vSwitch

Host 2

IP Address / Name

Data Store

vSwitch

Switch Name

Admin User Name

Admin Password

Confirm Admin Password

Virtual Machine Name

OVA Image Location

Layer 2 / Layer 3 Connectivity ☐ Layer 2 ☒ Layer 3

VSM IP Address

Subnet Mask

Gateway IP Address

Domain ID

Data Center Name

Enable Telnet ☐

Control Port Group ☐ Create New ☒ Choose Existing

Enter a valid primary host IP address.

< Prev Next > Finish Cancel

**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.

**Figure 29: Host 1 vSwitch Custom Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

**Import Configuration**

**Host 1**

IP Address / Name: esx-host-146.cisco.com **Browse**

Data Store: datastore1 (2) **Browse**

vSwitch: **Browse**

**Host 2**

IP Address / Name: **Browse**

Data Store: **Browse**

vSwitch: **Browse**

Switch Name:

Admin User Name:

Admin Password:

Confirm Admin Password:

Virtual Machine Name:

OVA Image Location: **Browse**

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Data Center Name: **Browse**

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Enter a valid primary vSwitch.

< Prev Next > Finish Cancel

- 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.

**Figure 30: Host 2 IP Address Custom Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

**Import Configuration**

**Host 1**

IP Address / Name: esx-host-146.cisco.com **Browse**

Data Store: datastore1 (2) **Browse**

vSwitch: vSwitch2 **Browse**

**Host 2**

IP Address / Name: **Browse**

Data Store: **Browse**

vSwitch: **Browse**

Switch Name:

Admin User Name:

Admin Password:

Confirm Admin Password:

Virtual Machine Name:

OVA Image Location: **Browse**

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Data Center Name: **Browse**

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Enter a valid secondary host IP address

< Prev Next > Finish Cancel

- 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.

**Figure 31: Host 2 vSwitch Custom Configuration Data Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

**Import Configuration**

**Host 1**

IP Address / Name: esx-host-146.cisco.com **Browse**

Data Store: datastore1 (2) **Browse**

vSwitch: vSwitch2 **Browse**

**Host 2**

IP Address / Name: esx-host-133.cisco.com **Browse**

Data Store: datastore1 (1) **Browse**

vSwitch: **Browse**

Switch Name:

Admin User Name:

Admin Password:

Confirm Admin Password:

Virtual Machine Name:

OVA Image Location:  **Browse**

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Data Center Name:  **Browse**

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Enter a valid secondary vSwitch.

**< Prev** **Next >** **Finish** **Cancel**

**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**.

**Figure 32: Switch Name Custom Configuration Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

Import Configuration

Host 1

IP Address / Name:

Data Store:

vSwitch:

Host 2

IP Address / Name:

Data Store:

vSwitch:

Switch Name:

Admin User Name:

Admin Password:

Confirm Admin Password:

Virtual Machine Name:

OVA Image Location:

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address:

Subnet Mask:

Gateway IP Address:

Domain ID:

Data Center Name:

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Please enter a valid switch name.

< Prev Next > Finish Cancel

334/203

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

**Figure 33: OVA Image Custom Configuration Data Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. On the left is a 'Steps' sidebar with a list: 1. Prerequisites, 2. vCenter Server Credentials, 3. Custom Configuration Data (highlighted), 4. Custom Configuration Review, 5. Confirmation, 6. Hosts Selection, and 7. Host Review. Below the list is the Cisco Nexus 1000V logo. The main area is titled 'Custom Configuration Data' and contains an 'Import Configuration' tab. Below this are configuration fields for two hosts. Host 1 fields include IP Address / Name (esx-host-146.cisco.com), Data Store (datastore1 (2)), and vSwitch (vSwitch2), each with a 'Browse' button. Host 2 fields include IP Address / Name (esx-host-133.cisco.com), Data Store (datastore1 (1)), and vSwitch (vSwitch0), each with a 'Browse' button. Other fields include Switch Name (demo-dvs), Admin User Name (admin), Admin Password (masked with asterisks), Confirm Admin Password (masked with asterisks), Virtual Machine Name (demo), OVA Image Location (empty field with a 'Browse' button), Layer 2 / Layer 3 Connectivity (radio buttons for Layer 2 and Layer 3, with Layer 3 selected), VSM IP Address, Subnet Mask, Gateway IP Address, Domain ID, Data Center Name (with a 'Browse' button), Enable Telnet (checkbox), and Control Port Group (radio buttons for Create New and Choose Existing, with Choose Existing selected). At the bottom, there is a message 'Enter a valid OVA image location' and navigation buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'. A vertical text '334198' is on the right edge of the window.

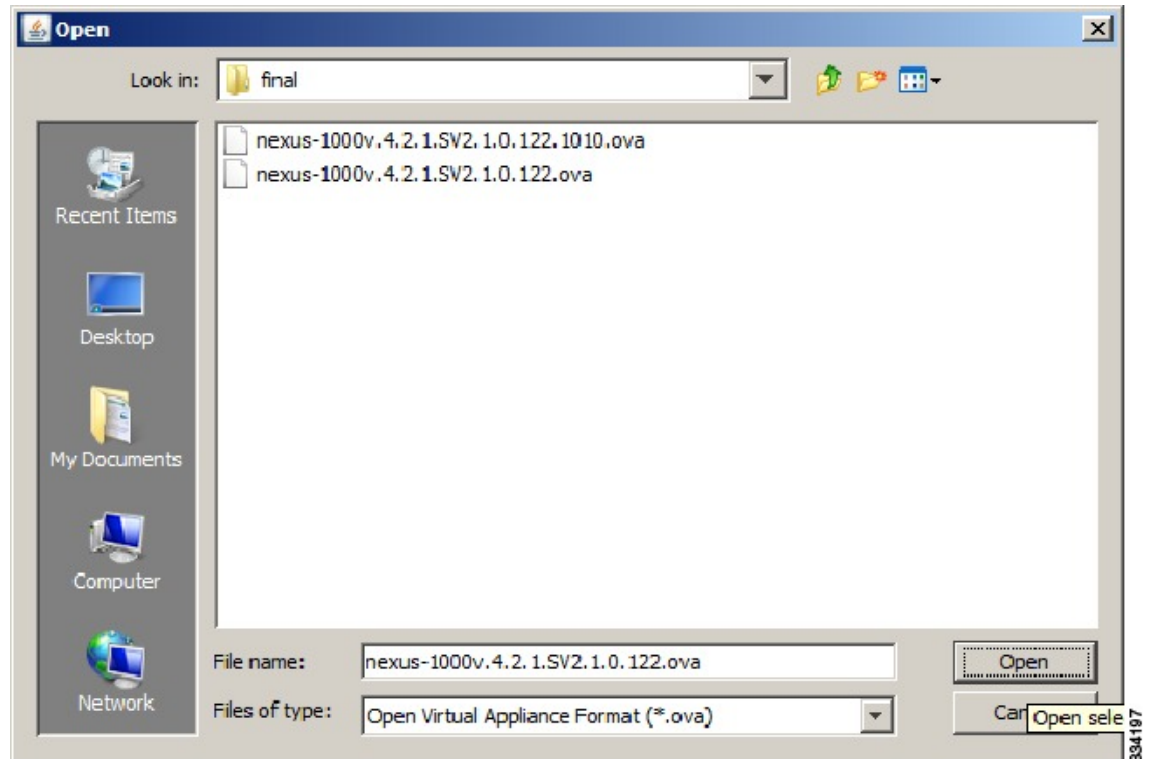
**Step 16** In the **OVA File Location** screen, do the following:

- Browse to the OVA file.
- Choose the OVA file.



- c) Click **Open**.

**Figure 34: OVA File Location Screen**



**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.

Figure 35: VSM IP Address Custom Configuration Data Screen

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

Virtual Machine Name: demo

OVA Image Location: jges\final\nexus-1000v-4.2.1.SV2.1.0.122.ova Browse

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address: 172.23.232.102

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.23.232.1

Domain ID: 1029

Data Center Name: Browse

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: Browse

VLAN ID: Browse

Management Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: Browse

VLAN ID: Browse

Packet Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: Browse

VLAN ID: Browse

Management VLAN: Browse

Migrate Host(s) to DVS: ☐ Yes ☒ No

Save Configuration

Enter a valid System Data Center.

< Prev Next > Finish Cancel

334190

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

**Figure 36: Data Center Name Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. On the left is a 'Steps' sidebar with 7 steps, where '3. Custom Configuration Data' is highlighted. The main area is titled 'Custom Configuration Data'. It contains several configuration fields: 'Virtual Machine Name' (demo), 'OVA Image Location' (ges\final\nexus-1000v.4.2.1.SV2.1.0.122.ova) with a 'Browse' button, 'Layer 2 / Layer 3 Connectivity' (radio buttons for Layer 2 and Layer 3, with Layer 3 selected), 'VSM IP Address' (172.23.232.102), 'Subnet Mask' (255.255.255.0), 'Gateway IP Address' (172.23.232.1), 'Domain ID' (1029), 'Data Center Name' (empty) with a 'Browse' button, 'Enable Telnet' (checkbox), 'Control Port Group' (radio buttons for Create New and Choose Existing, with Choose Existing selected), 'Port Group Name' (empty) with a 'Browse' button, 'VLAN ID' (empty), 'Management Port Group' (radio buttons for Create New and Choose Existing, with Choose Existing selected), 'Port Group Name' (empty) with a 'Browse' button, 'VLAN ID' (empty), 'Packet Port Group' (radio buttons for Create New and Choose Existing, with Choose Existing selected), 'Port Group Name' (empty) with a 'Browse' button, 'VLAN ID' (empty), 'Management VLAN' (empty), and 'Migrate Host(s) to DVS' (radio buttons for Yes and No, with No selected). At the bottom, there is a 'Save Configuration' button and a status bar that says 'Enter a valid System Data Center.' with navigation buttons '< Prev', 'Next >', 'Finish', and 'Cancel'.

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

- Choose a data center.
- Click **Select**.

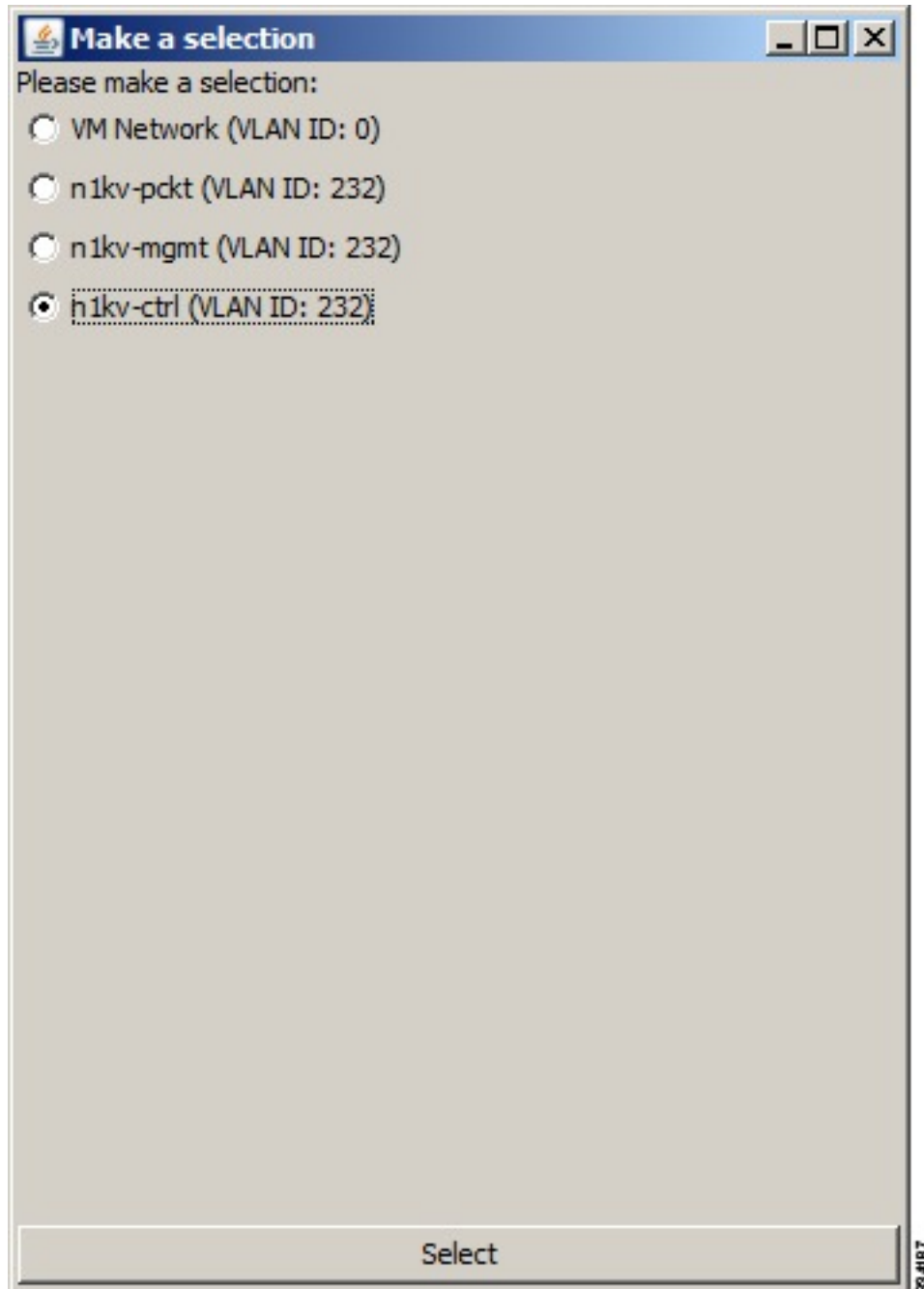
**Step 20** Click the **Browse** button for the Control Port Group **Port Group Name** field.

**Step 21** In the **Choose Control Port Group - Port Group VLAN ID** screen, do the following:

- Choose a VLAN ID.

- Click **Select**.

*Figure 37: Choose Control Port Group - Port Group VLAN ID Screen*



- Step 22** In the **Management Port Group - Port Group Name** screen, do the following to create a new Management Port Group:
- a) Choose the **Create New** radio button

- b) Enter the **Port Group Name**.
- c) Enter the **VLAN ID**.

**Figure 38: Management Port Group - Port Group Name Screen**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

Virtual Machine Name: demo

OVA Image Location: iges\final\nexus-1000v.4.2.1.SV2.1.0.122.ova Browse

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address: 172.23.232.102

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.23.232.1

Domain ID: 1029

Data Center Name: Dhruv-DC Browse

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: n1kv-ctrl Browse

VLAN ID: 232

Management Port Group: ☒ Create New ☐ Choose Existing

Port Group Name: Browse

VLAN ID: Browse

Packet Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: Browse

VLAN ID: Browse

Management VLAN: Browse

Migrate Host(s) to DVS: ☒ Yes ☐ No

Save Configuration

Enter a valid management port group.

< Prev Next > Finish Cancel

**Step 23** In the **Management VLAN** screen, do the following:

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

- a) Enter a VLAN ID in the **Management VLAN ID** field.
- b) Click **Yes** or **No** to migrate the hosts to the DVS.
- c) Click the **Save Configuration** button if you want to save the settings to a configuration file.

d) Click Next.

**Figure 39: Management VLAN Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Custom Configuration Data**
4. Custom Configuration Review
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Data**

Virtual Machine Name: demo

OVA Image Location: jges\final\nexus-1000v-4.2.1.SV2.1.0.122.ova Browse

Layer 2 / Layer 3 Connectivity: ☐ Layer 2 ☒ Layer 3

VSM IP Address: 172.23.232.102

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.23.232.1

Domain ID: 1029

Data Center Name: Dhruv-DC Browse

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: n1kv-ctrl Browse

VLAN ID: 232

Management Port Group: ☒ Create New ☐ Choose Existing

Port Group Name: n1kv-mgmt Browse

VLAN ID: 232

Packet Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: Browse

VLAN ID: Browse

Management VLAN: Browse

Migrate Host(s) to DVS: ☐ Yes ☒ No

Save Configuration

Please enter a valid Management VLAN ID <1-3967,4048-4093> or 0.

< Prev Next > Finish Cancel

**Step 24** In the **Custom Configuration Review** screen, do the following:

- Validate the input.

- Click **Next**.

**Figure 40: Custom Configuration Review Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
3. Custom Configuration Data
- 4. Custom Configuration Review**
5. Confirmation
6. Hosts Selection
7. Host Review

**Custom Configuration Review**

Virtual Machine Name: demo

OVA Image Location: X:\cx122\build\images\final\nexus-1000v.4.2.1.SV2.1.0.122.ova

Layer 2 / Layer 3 Connectivity: ☐ L2 ☒ L3

VSM IP Address: 172.23.232.102

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.23.232.1

Domain ID: 1029

SVS Datacenter Name: Dhruv-DC

Enable Telnet: ☐

Control Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: n1kv-ctrl

VLAN ID: 232

Management Port Group: ☐ Create New ☒ Choose Existing

Port Group Name: n1kv-mgmt

VLAN ID: 232

Packet Port Group: ☐ Create New ☒ Choose Existing

Port Group Name:

VLAN ID:

Management VLAN: 232

Migrate Host(s) to DVS: ☒ Yes ☐ No

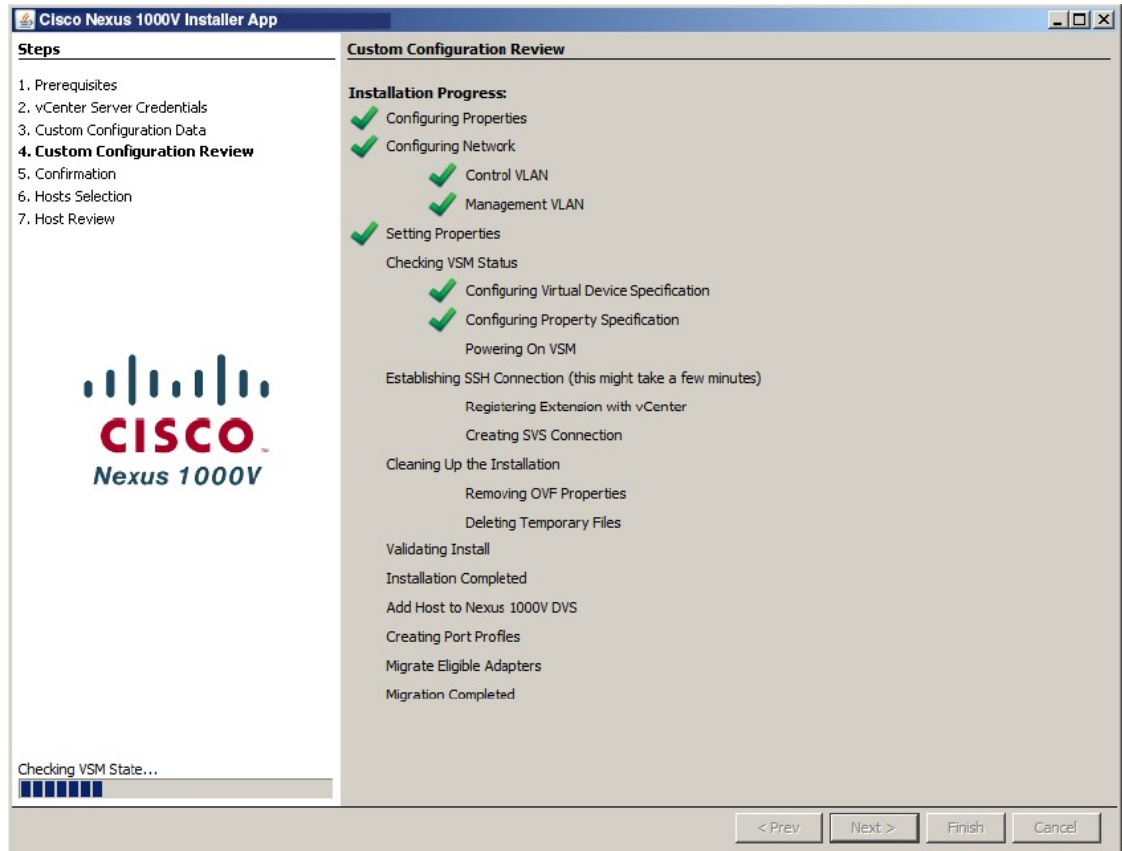
Notes: The interfaces on the selected vSwitch will be migrated to the Nexus 1000V vDS. If the management interface is on a different vSwitch, it will be migrated as well.

< Prev Next > Finish Cancel

394171

The **Custom Configuration Review Installation Progress** screen is displayed.

**Figure 41: Custom Configuration Review Installation Progress Screen**



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

**Step 25** 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.

**Figure 42: Custom Confirmation Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. On the left, a 'Steps' pane lists the installation process: 1. Prerequisites, 2. vCenter Server Credentials, 3. Custom Configuration Data, 4. Custom Configuration Review, 5. Confirmation (highlighted), 6. Hosts Selection, and 7. Host Review. Below the list is the Cisco logo and 'Nexus 1000V'. The main area is titled 'Confirmation' and asks 'Do you want to add more modules?'. It has two radio buttons: 'Yes' (selected) and 'No'. Below this, there are two options: 'Install VIB' (selected) and 'Install VIB and add module to Nexus 1000V'. A 'Management VLAN:' label is followed by an empty text box. At the bottom, a blue error message reads 'Enter a valid management VLAN.' and there are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
3. Custom Configuration Data
4. Custom Configuration Review
- 5. Confirmation**
6. Hosts Selection
7. Host Review

**Confirmation**

Do you want to add more modules?

☒ Yes ☐ No

☐ Install VIB ☒ Install VIB and add module to Nexus 1000V

Management VLAN:

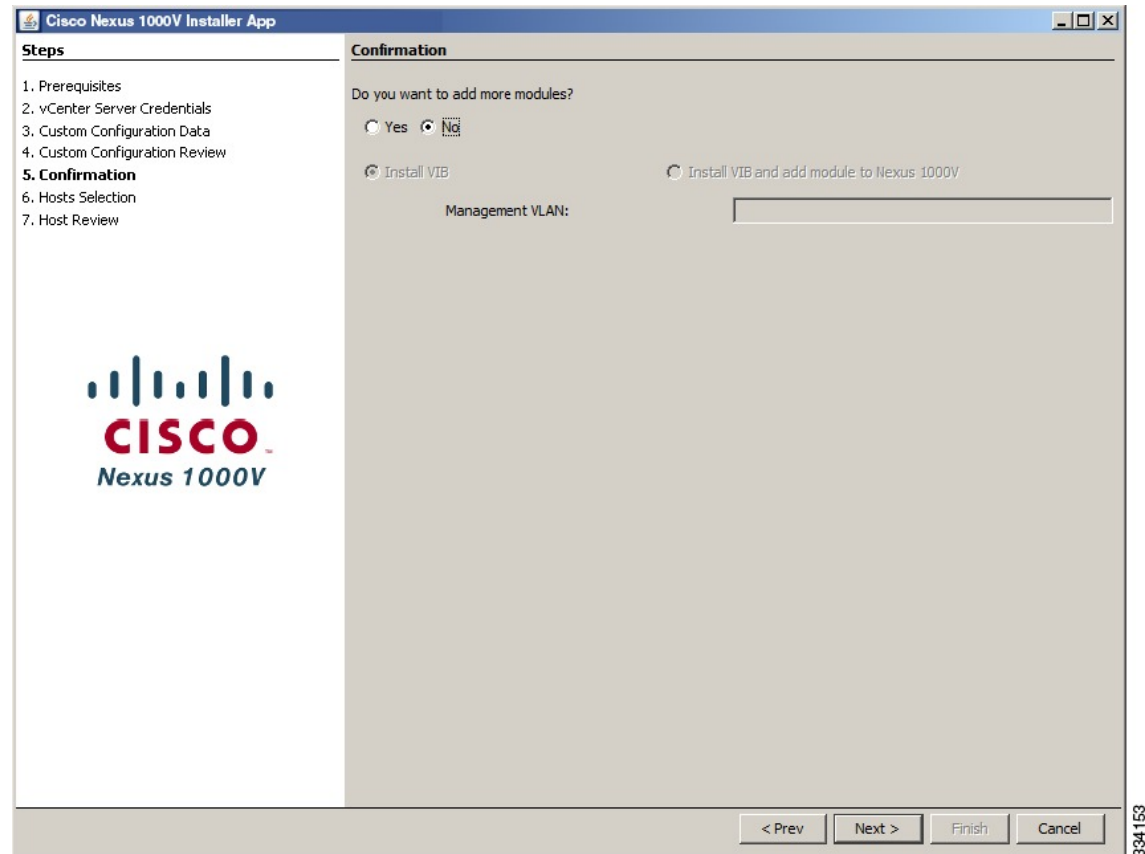
Enter a valid management VLAN.

< Prev Next > Finish Cancel

334 155

- Click **No** if you do not want to add more modules and continue with Step 29 .

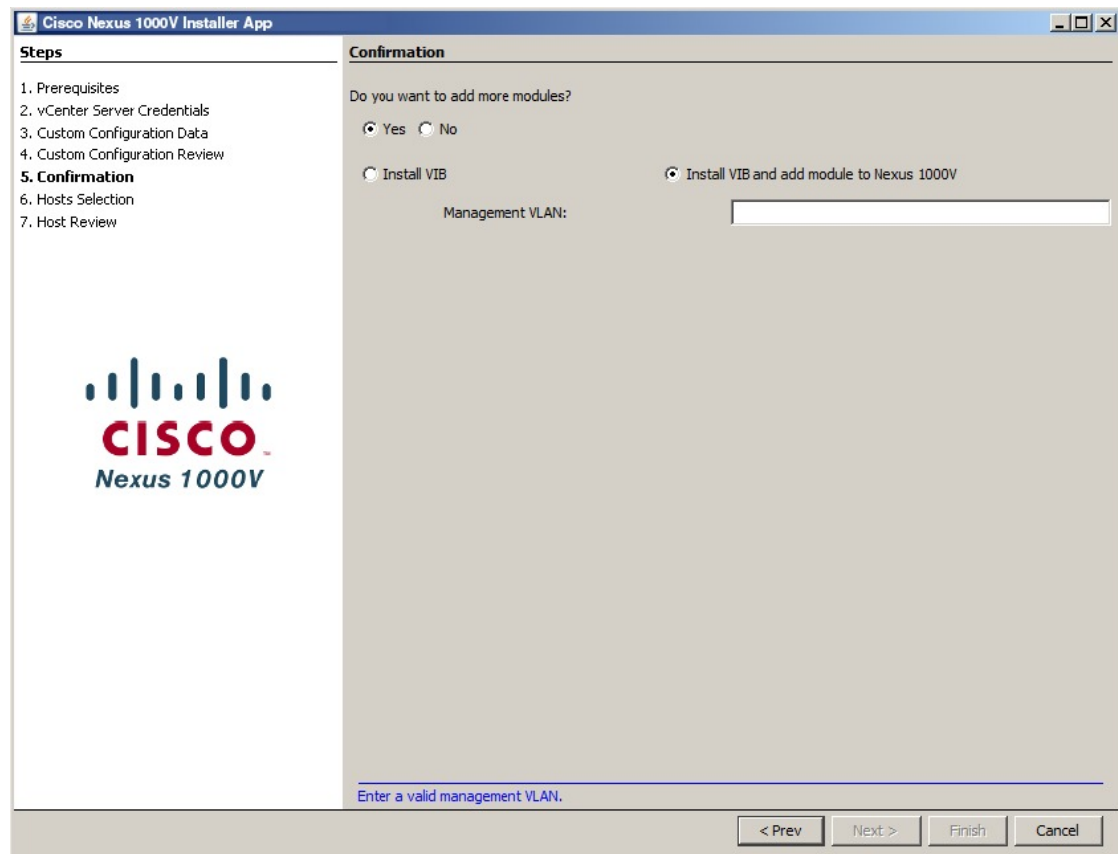
**Figure 43: Not Adding Modules Screen**



**Step 26** In the **Confirmation** screen, do the following:

- 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.
- Enter a VLAN ID in the **Management VLAN** field.
 

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

**Figure 44: Confirmation Screen**

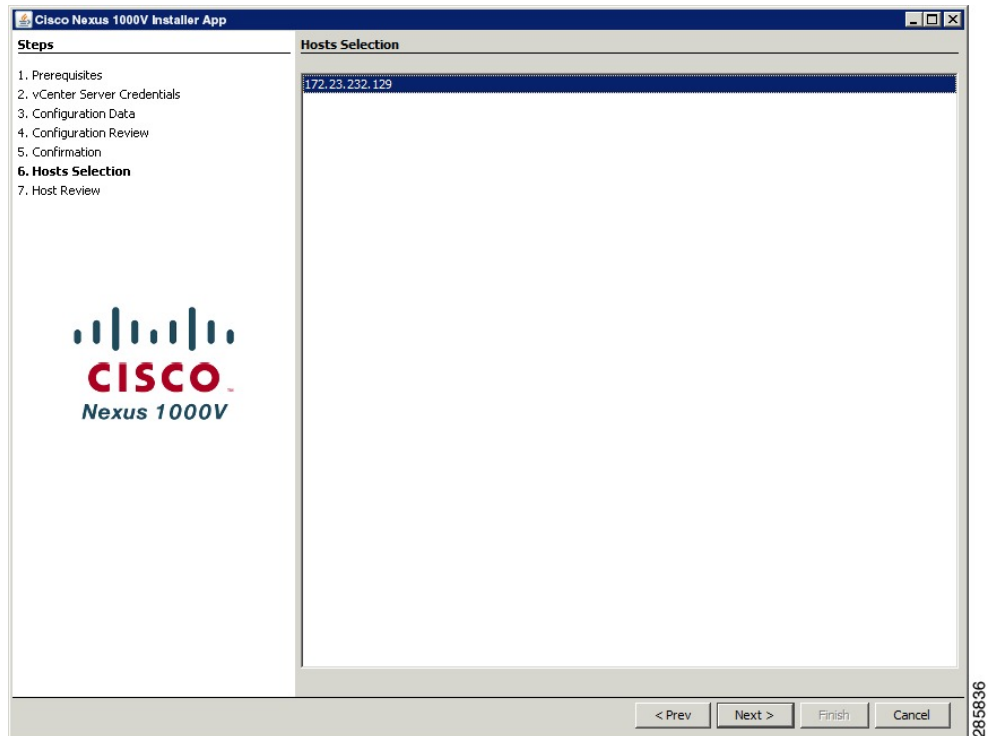
334155

**Step 27** In the **Hosts Selection** screen, do the following:

- a) Choose the hosts you want to add.

b) Click **Next**.

**Figure 45: Hosts Selection Screen**



**Step 28** In the **Host Review** screen, do the following:

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

**Figure 46: Host Review Screen**

**Cisco Nexus 1000V Installer App**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
3. Basic Configuration Data
4. Basic Configuration Review
5. Confirmation
6. Hosts Selection
- 7. Host Review**

**CISCO**  
Nexus 1000V

**Host Review**

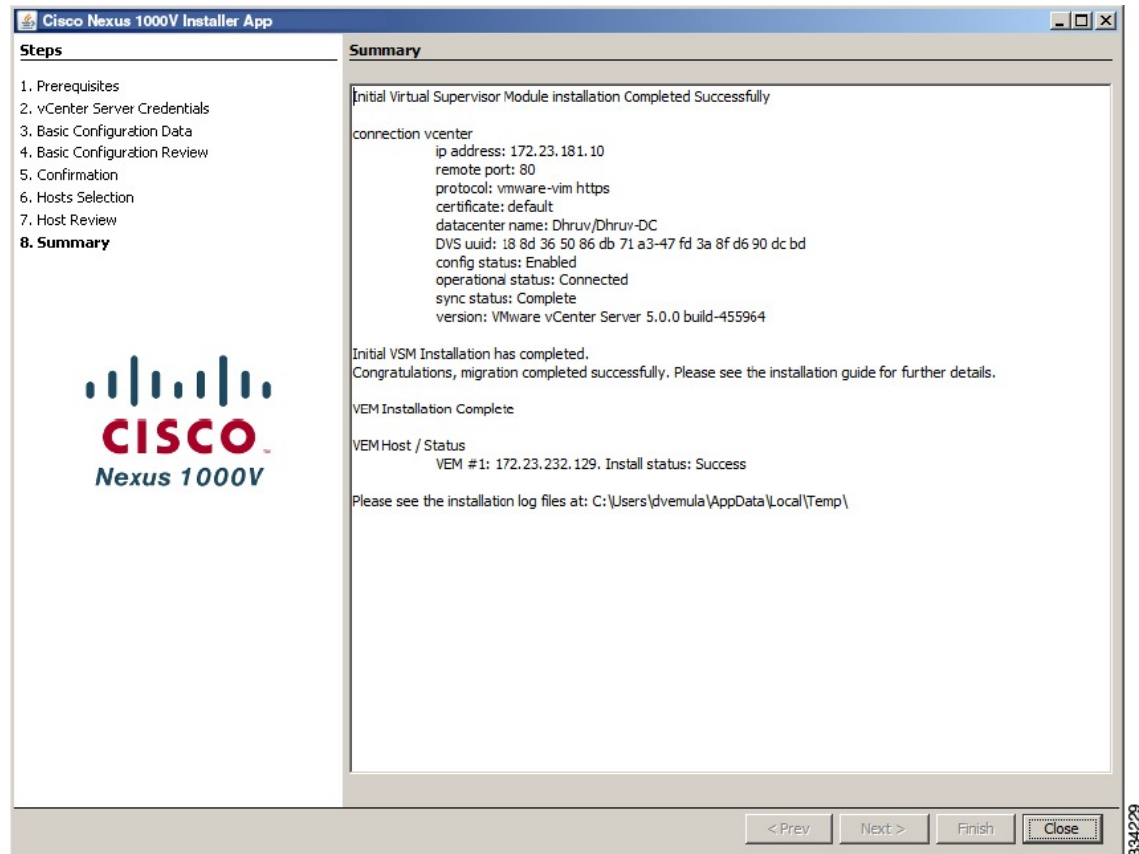
vCenter Server IP Address	172.23.181.10
Virtual Supervisor Module IP Address	172.23.232.102
Virtual Ethernet Module #1	172.23.232.129

< Prev   Next >   Finish   Cancel

334233

**Step 29** In the Custom Summary screen, click **Close**.

**Figure 47: Custom Summary Screen**



## Information About Layer 2 Connectivity

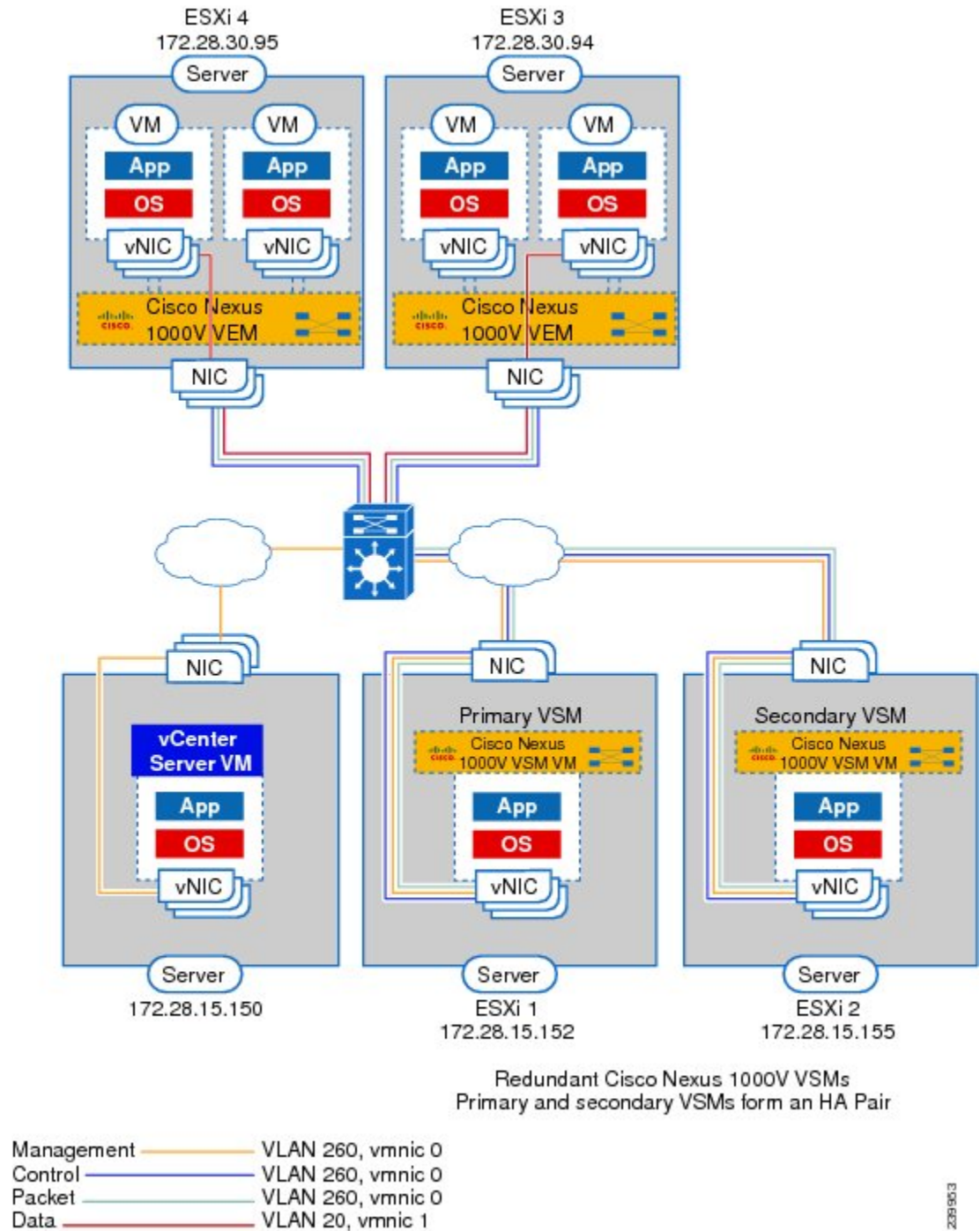


### Note

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

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

**Figure 48: Cisco Nexus 1000V Installation Diagram for Layer 2**







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

- Click **Next**.

**Figure 50: Configure Networking Screen**

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

## 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 Nexus 1000V VEMs
- If a particular VEM is capable of hosting VSMs, the network administrator must manually allow 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 VIB files. Uninstall any Cisco Nexus 1000V VIBs before starting the Cisco Nexus 1000V Installer App.

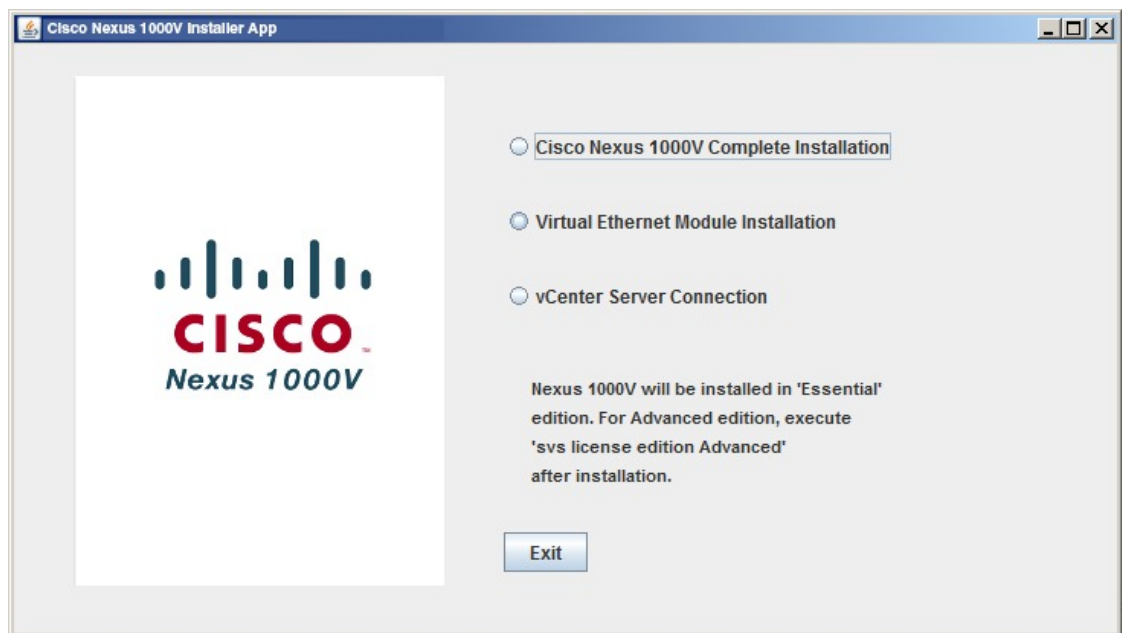
## Procedure

**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 Installer App.

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

**Step 2** Click the **Virtual Ethernet Module Installation** radio button.

*Figure 51: Cisco Nexus 1000V Installer App Screen*



**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**.

**Figure 52: VEM Enter vCenter Credentials Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. On the left, a 'Steps' list shows: 1. Prerequisites, 2. vCenter Server Credentials (highlighted), 3. Enter VSM IP & Credentials, 4. Confirmation, 5. Hosts Selection, and 6. Host Review. Below the list is the Cisco Nexus 1000V logo. The main area is titled 'vCenter Server Credentials' and contains four input fields: 'IP Address' with the value '172.23.181.10', 'Port (https only)' with the value '443', 'User ID' with the value 'Administrator', and 'Password' with masked characters '\*\*\*\*\*'. At the bottom right are four buttons: '< Prev', 'Next >' (highlighted with a dashed border), 'Finish', and 'Cancel'. A vertical text '334143' is on the far right edge.

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

a) Enter the following credentials:

- **VSM IP address**

- **VSM Password**

b) Click **Next**.

**Figure 53: VEM Enter VSM IP & Credentials Screen**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
- 3. Enter VSM IP & Credentials**
4. Confirmation
5. Hosts Selection
6. Host Review

**Enter VSM IP & Credentials**

VSM IP Address: 172.23.232.102

VSM User Name: admin

VSM Password: \*\*\*\*\*

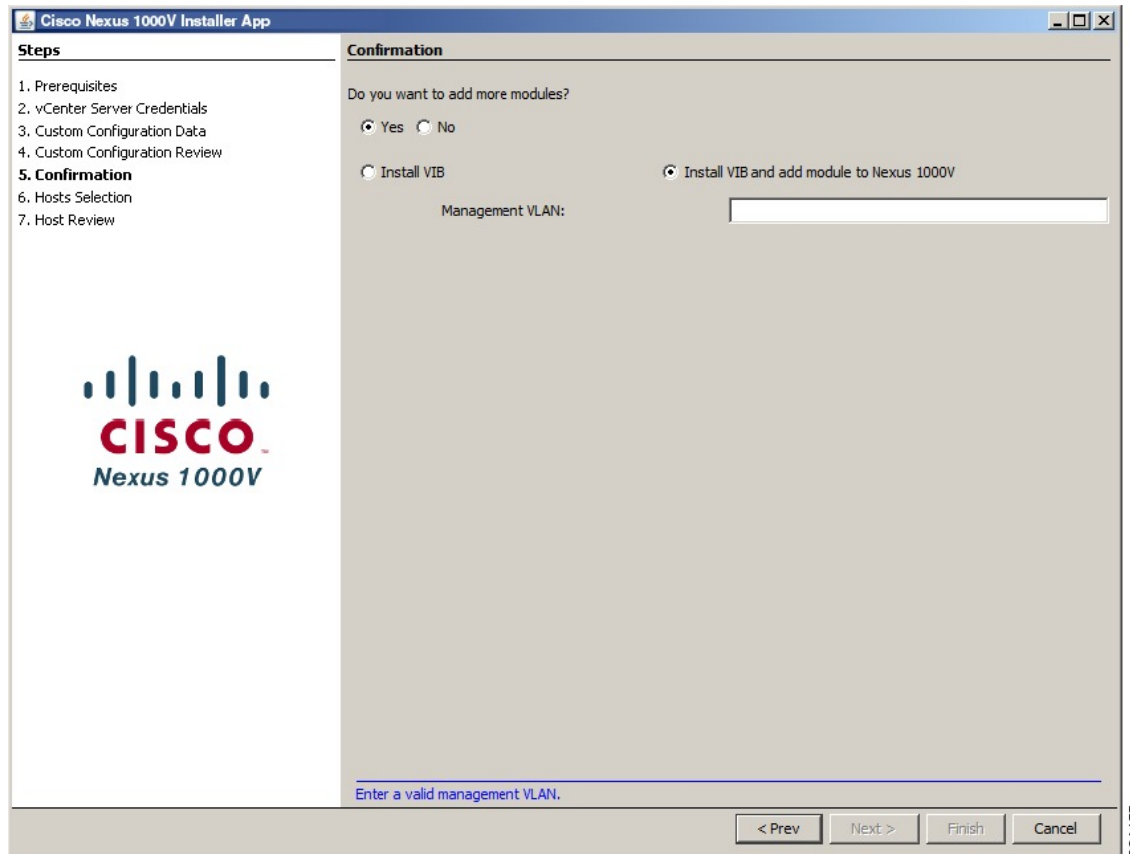
**CISCO**  
Nexus 1000V

< Prev   Next >   Finish   Cancel

**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.

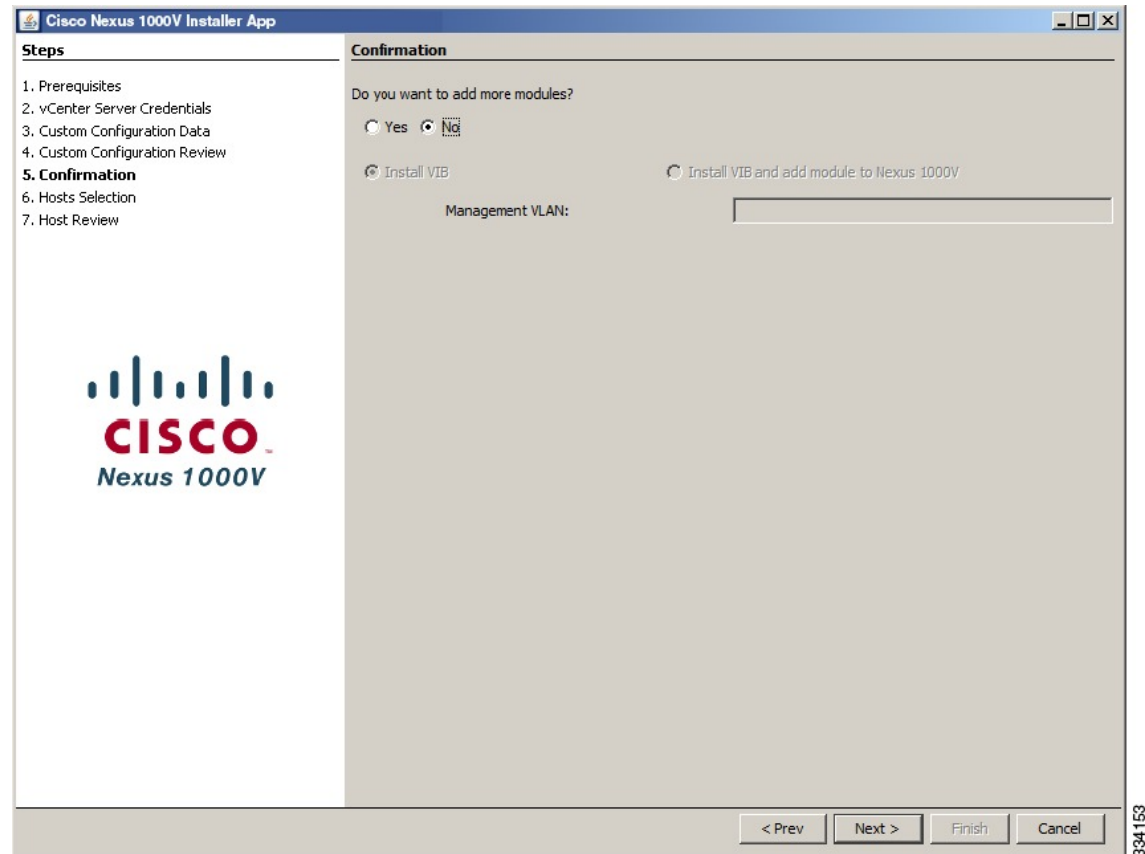
**Figure 54: Confirmation Screen**



334 155

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

**Figure 55: Not Adding Modules Screen**

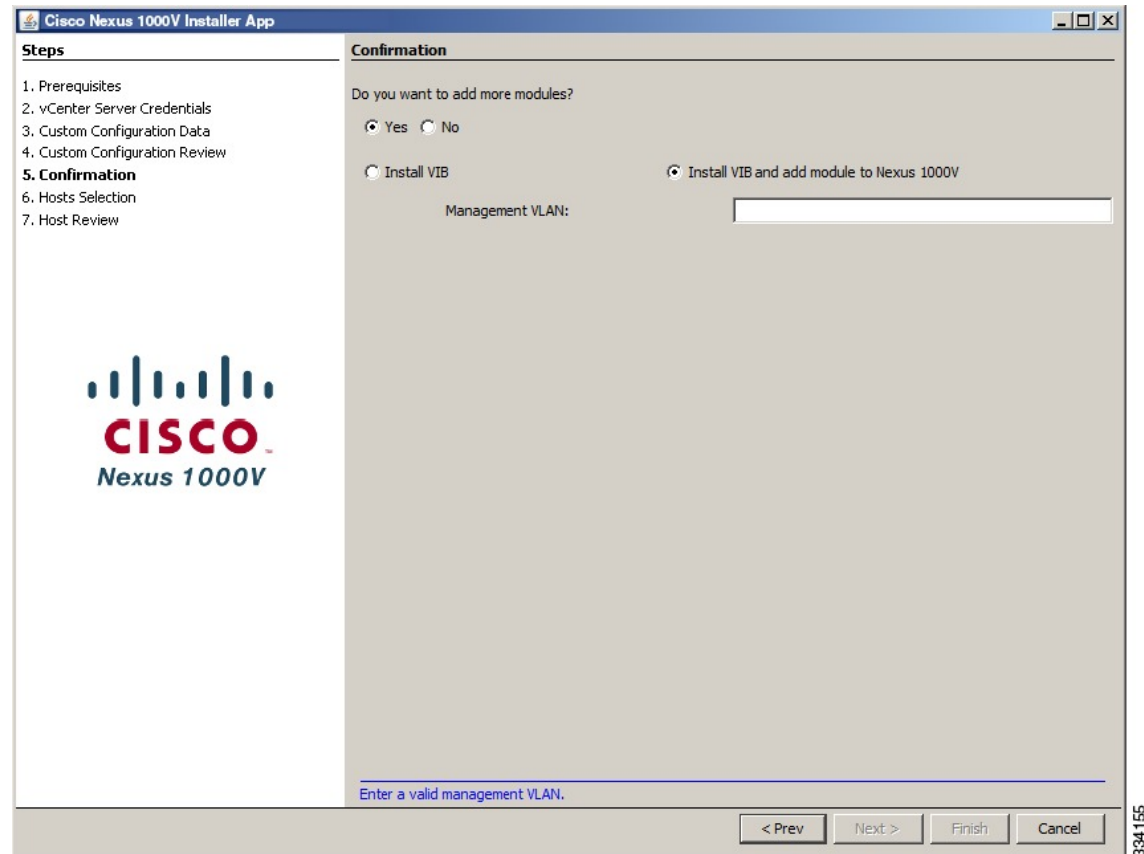


**Step 7** In the **Adding Modules** screen, do the following:

- 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 Nexus 1000V.

- b) Enter a VLAN ID in the **Management VLAN** field.

**Figure 56: Adding Modules Screen**

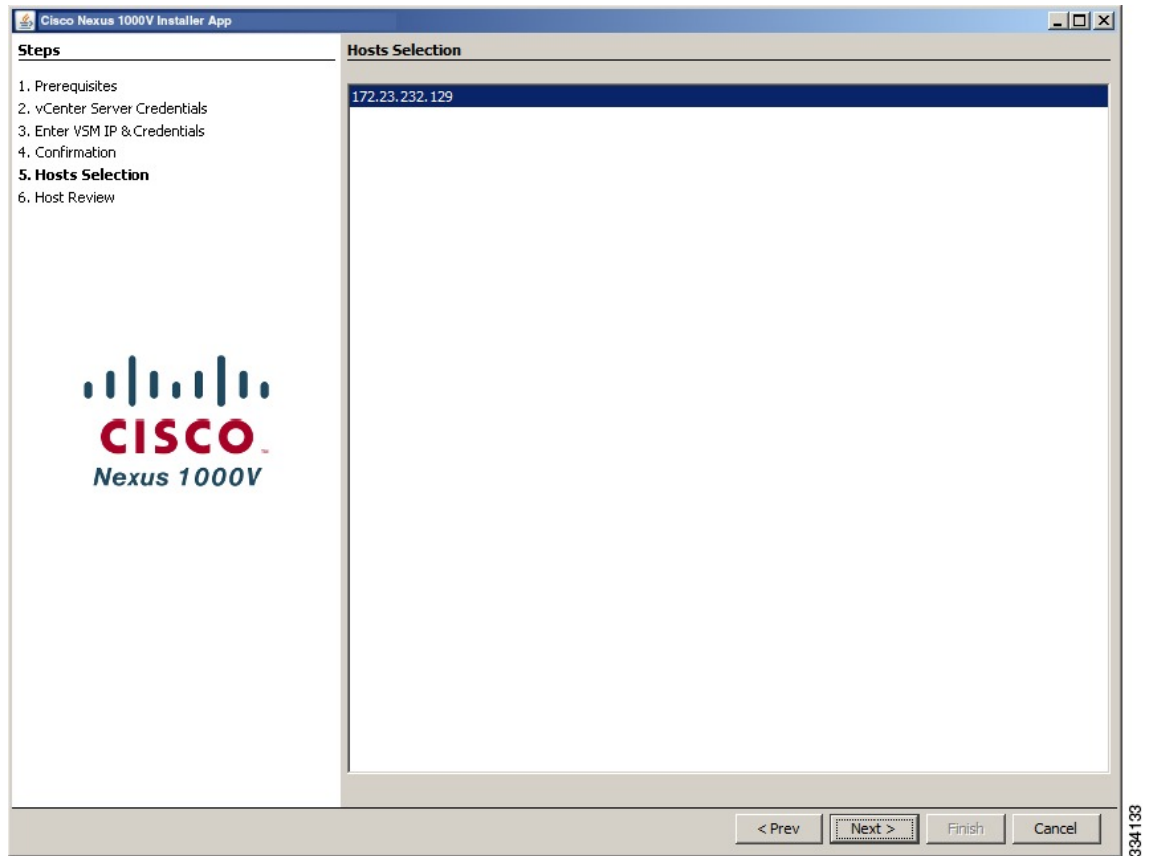


**Step 8** In the **VEM Hosts Selection** screen, do the following:

- a) Choose the hosts you want to add.

b) Click **Next**.

**Figure 57: VEM Hosts Selection Screen**



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

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



**Figure 58: VEM Host Review Screen**

**Steps**

1. Prerequisites
2. vCenter Server Credentials
3. Enter VSM IP & Credentials
4. Confirmation
5. Hosts Selection
- 6. Host Review**

**Host Review**

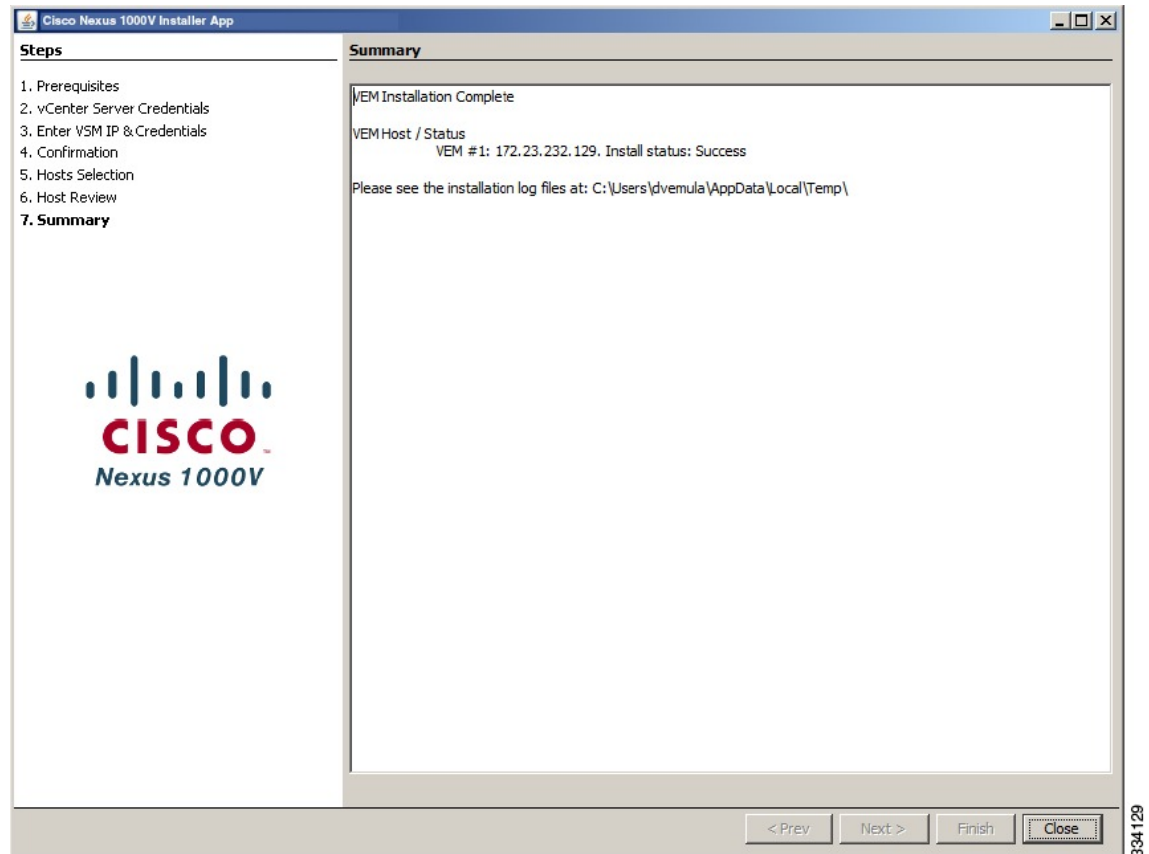
vCenter Server IP Address	172.23.181.10
Virtual Supervisor Module IP Address	172.23.232.102
Virtual Ethernet Module #1	172.23.232.129

< Prev   Next >   Finish   Cancel

334132

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

**Figure 59: VEM Summary Screen**



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

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

## Adding VEM Hosts to the Distributed Virtual Switch

### Before You Begin

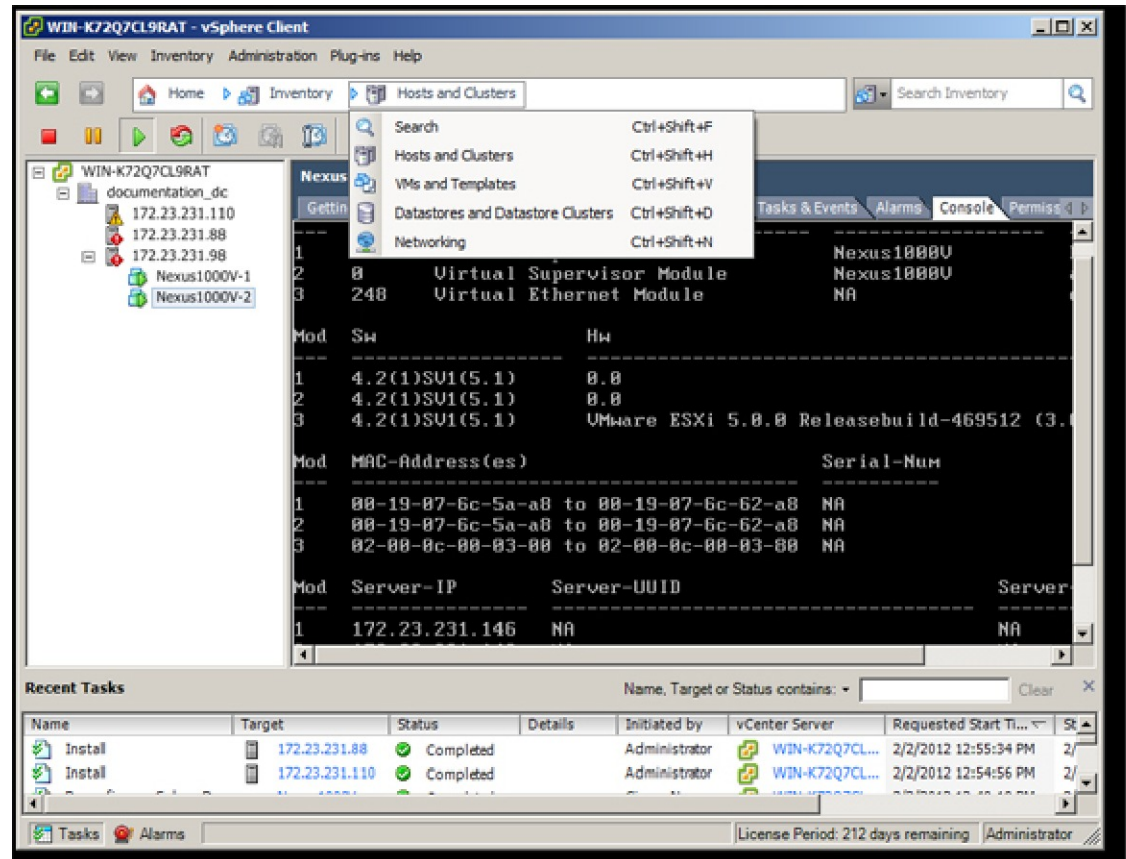
- You have the following information:
  - Physical adapters

- Uplink port groups

## Procedure

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

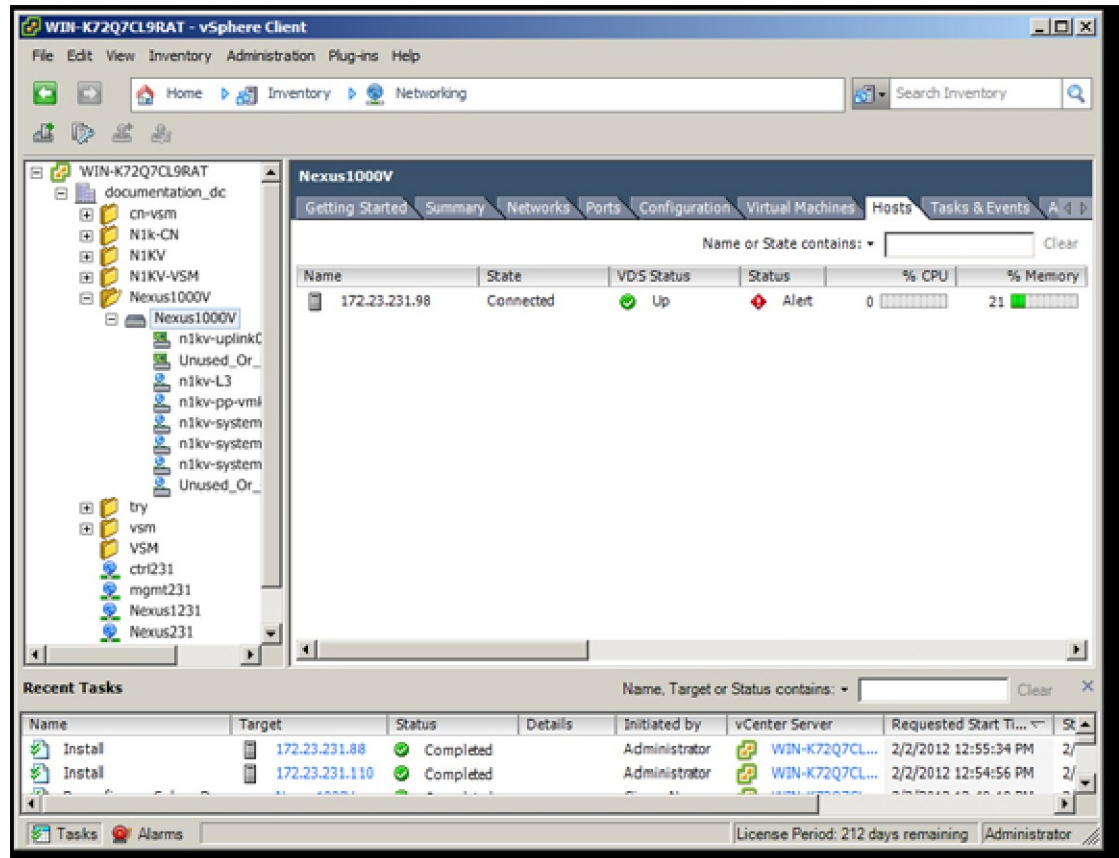
**Figure 60: vSphere Client Window**



331974

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

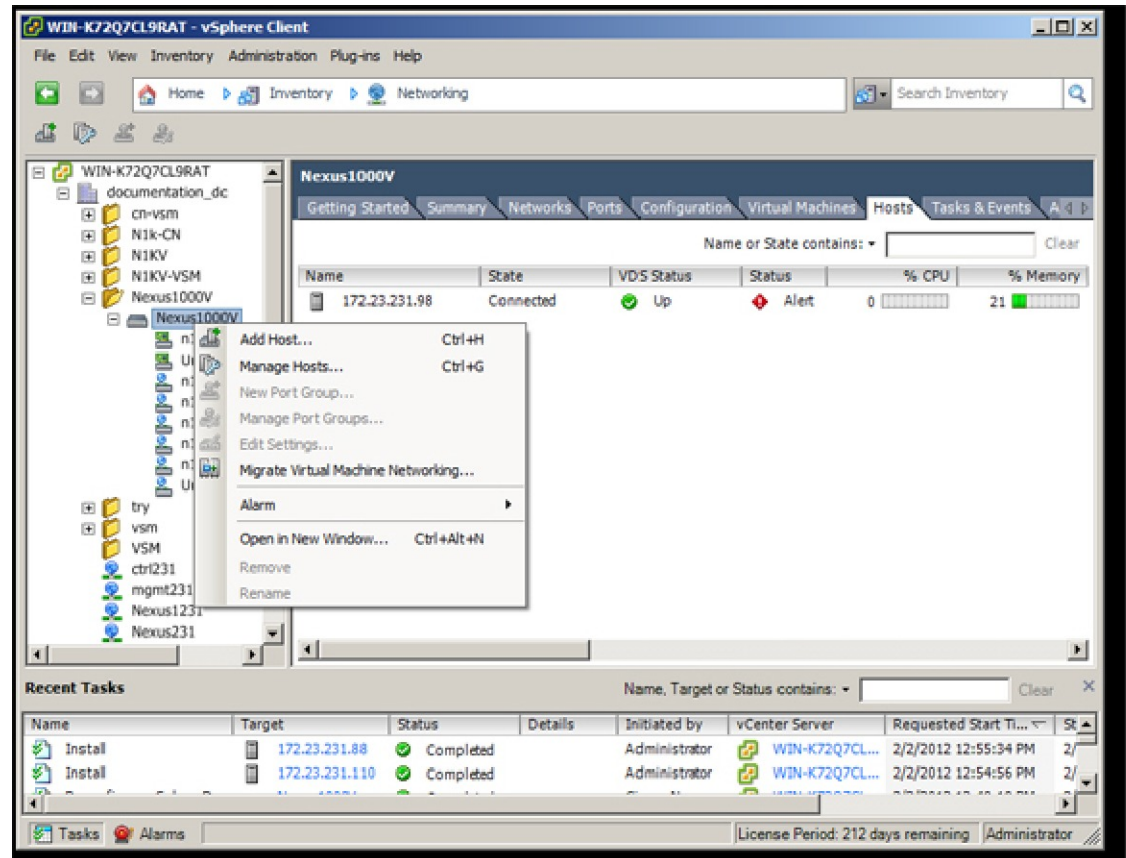
**Figure 61: vSphere Client Hosts Window**



331975

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

**Figure 62: 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, click **Next**.

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

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

**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.

# Setting Virtual Machine Startup and Shutdown Parameters

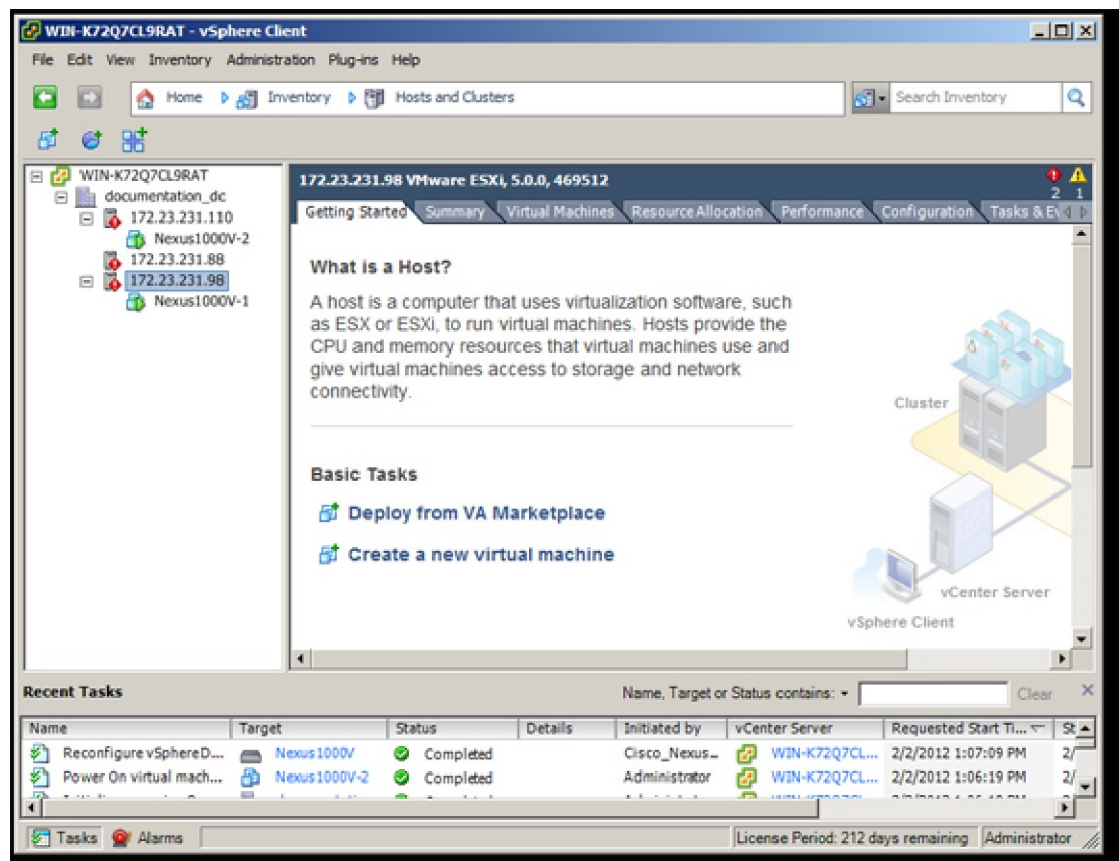
## Before You Begin

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

## Procedure

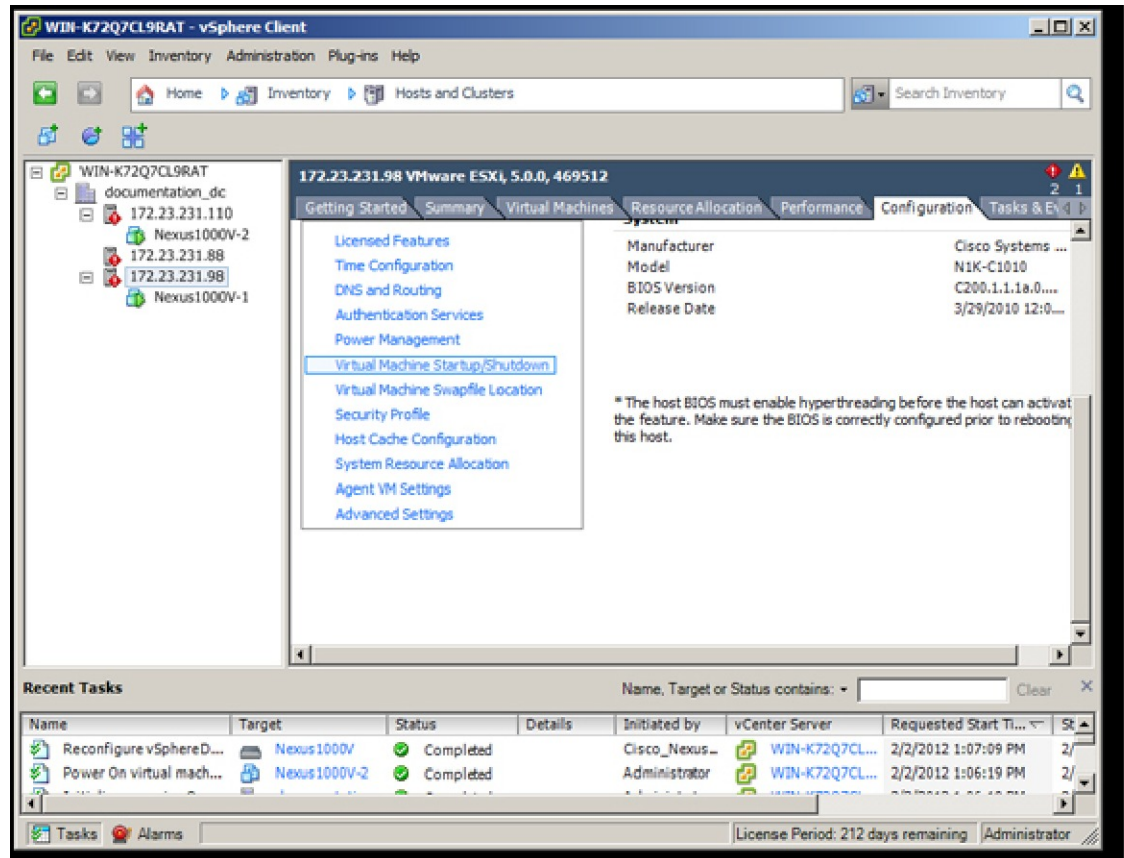
- Step 1** In the vSphere Client window, choose a host and click the **Configuration** tab.

*Figure 63: vSphere Client Window*



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

**Figure 64: Configuration Pane**

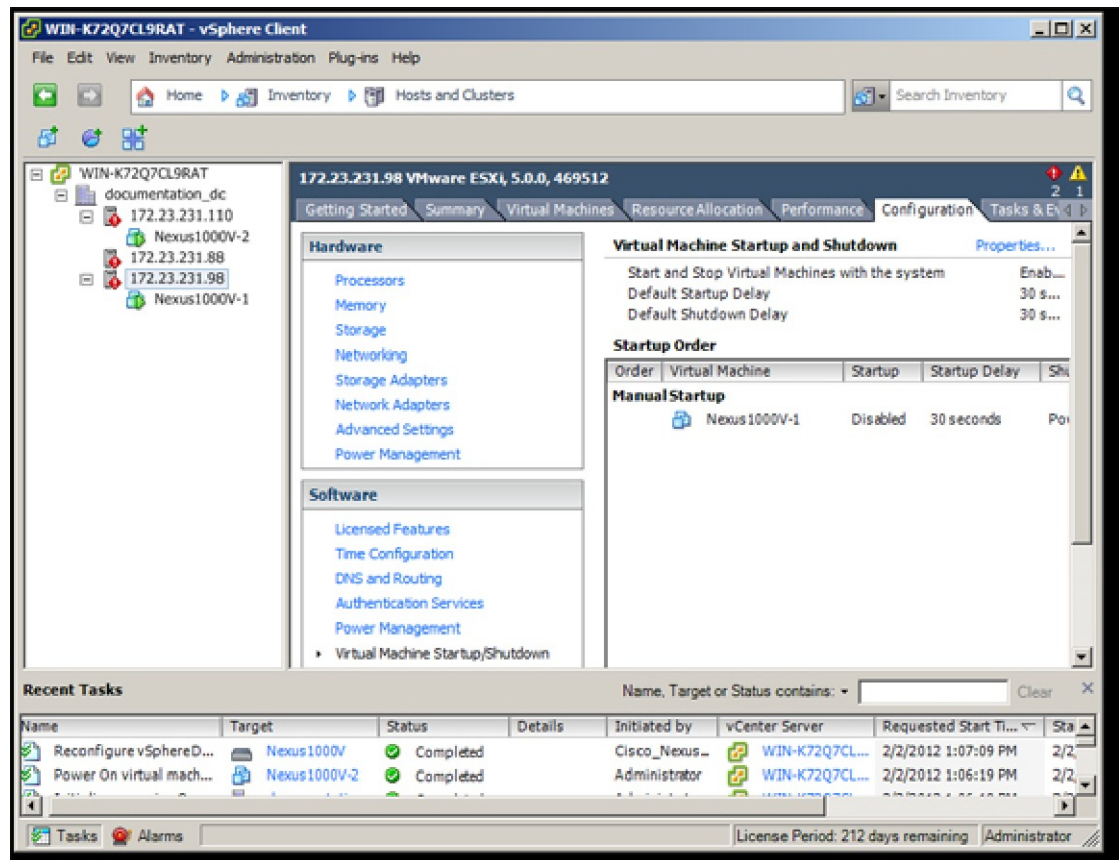


331992



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

*Figure 65: Virtual Machine Startup and Shutdown Pane*



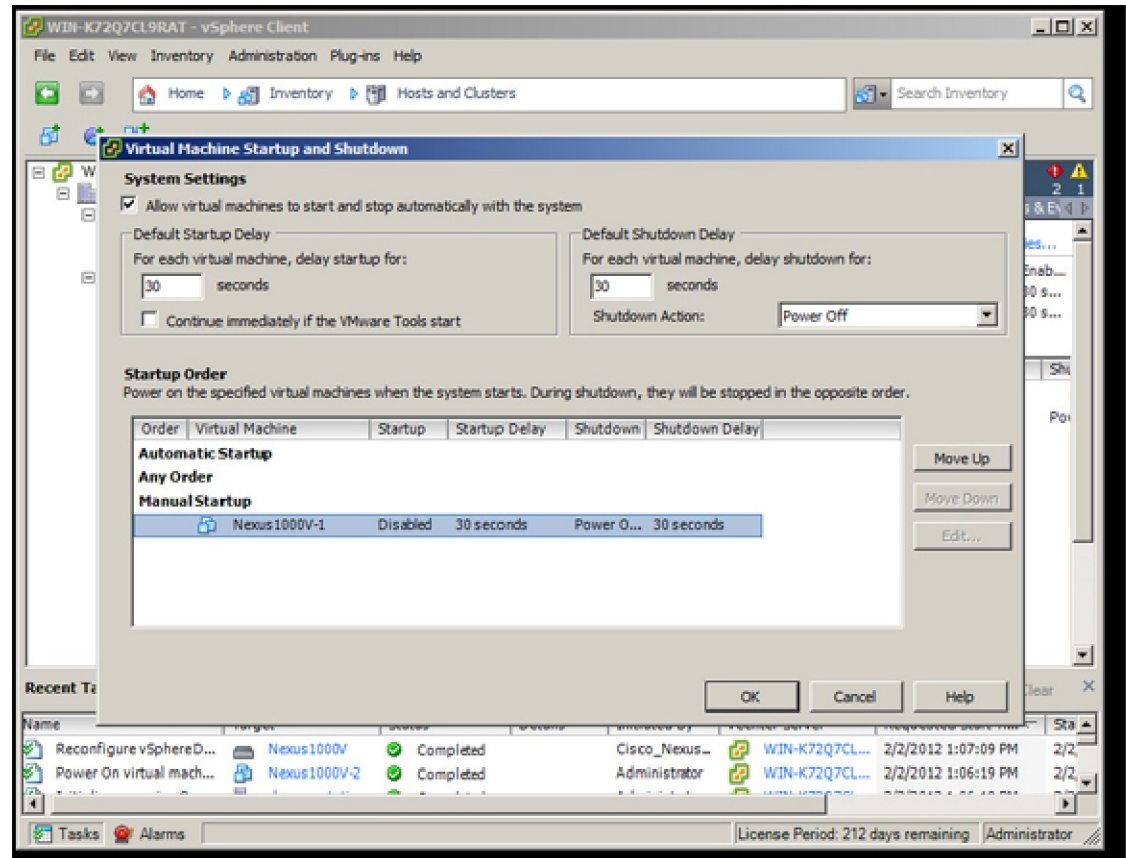
**Step 4** In the **System Settings** dialog box, do the following:

- Check the **Allow virtual machines to start and stop automatically with the system** check box.
- In the System Settings pane, do the following:
  - Enter a number of seconds in the **Default Startup Delay seconds** field.
  - Enter a number of seconds in the **Default Shutdown Delay seconds** field.
- In the **Startup Order** pane, do the following:
  - Choose the virtual machine.
  - Click the **Move Up** button until the virtual machine is under Automatic Startup.
- Click **OK**.



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

**Figure 66: System Settings Dialog Box**



Startup and shutdown settings are complete.

## Installing the VEM Software Using VUM

### Before You Begin

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



#### Note

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

# Installing the VEM Software Using the CLI

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

- [Installing VEM Software Locally on a VMware 4.1 Host by Using the CLI, on page 82](#)
- [Installing the VEM Software Remotely on a VMware 4.1 Host by Using the CLI, on page 83](#)
- [Installing the VEM Software Locally on a VMware 5.0 Host by Using the CLI, on page 85](#)
- [Installing VEM Software Remotely on a VMware 5.0 Host by Using the CLI, on page 86](#)

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

### Before You Begin

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

### Procedure

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

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

```
esxupdate --bundle VMware_offline_update_bundle update
```

#### Example:

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

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

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

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

```
esxupdate -b VIB_file update
```

#### Example:

```
/tmp # esxupdate -b cross_cisco-vem-v140-4.2.1.2.1.1.0-2.0.1.vib update
```

```
Unpacking cross_cisco-vem-vl40-esx.. #####
[100%]
```

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

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

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

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

```
/tmp # esxupdate --vib-view query | grep cisco
cross_cisco-vem-vl40-4.2.1.2.1.1.0-2.0.1.vib                installed
2012-02-02T12:29:18.728890+00:00
```

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

```
/tmp # vem status -v
Package vssnet-esx5.5.0-00000-release
Version 4.2.1.2.1.1.0-2.0.2
Build 2
Date Tue Jan 31 05:01:37 PST 2012
```

```
Number of PassThru NICs are 0
VEM modules are loaded
```

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

```
Number of PassThru NICs are 0
```

**VEM Agent (vemdpa) is running**

**Step 4** Do one of the following:

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

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

### Before You Begin

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

**Note**

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

**Procedure**

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

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

**Step 2** Install the VEM software.

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

**Example:**

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

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

```
vihostupdate.pl -q --server host_ip_address
```

**Example:**

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

-----Bulletin ID----- Installed-----Summary-----
VEM410-201201401-BG          2012-02-02T00:54:14 Cisco Nexus 1000V 4.2(1)SV2(1.1)
```

**Step 4** Do one of the following:

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

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

## Procedure

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

**Step 2** Begin the VEM installation procedure.

```
esxcli software vib install -v /tmp/VIB_FILE
```

### Example:

```
~ # esxcli software vib install -v /tmp/cross_cisco-vem-vl40-4.2.1.2.1.1.0-3.0.1.vib
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: Cisco_bootbank_cisco-vem-vl40-esx_4.2.1.2.1.1.0-3.0.1
  VIBs Removed:
  VIBs Skipped:
```

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

```
~ # esxcli software vib list | grep cisco
cisco-vem-vl40-esx 4.2.1.2.1.1.0-3.0.1 Cisco PartnerSupported
2012-02-02
```

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

### Example:

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.2.1.1.0-3.0.1
Build 1
Date Mon Jan 30 18:38:49 PST 2012

Number of PassThru NICs are 0
VEM modules are loaded

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

**Step 5** Do one of the following:

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

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

## Procedure

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

**Step 2** Enter the following command from the remote machine where the vCLI is installed.

```
esxcli --server=[server ip] software vib install --depot=Path_to_the_NFS_storage_mounted__on_ESXi_5.0
host
```

### Example:

```
vi-admin@localhost:~> esxcli --server=192.0.2.2 software vib install
--depot=/vmfs/volumes/newnfs/MN-patch01/CN-FCS/VEM500-201201140102-BG-release.zip
Enter username: root
Enter password:
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: Cisco_bootbank_cisco-vem-v140-esx_4.2.1.2.1.1.0-3.0.1
  VIBs Removed:
  VIBs Skipped:
```

where 192.0.2.2 is the target ESXi 5.0 host IP address and newnfs is the NFS storage mounted on the ESXi 5.0 host.

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

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

```
esxcli --server=host_ip_address software vib list
```

### Example:

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

Look for the following:

Name	Version	Vendor	Acceptance Lev
el Install Date			
-----	-----	-----	-----
--			
cisco-vem-v140-esx	4.2.1.2.1.1.0-3.0.1	Cisco	PartnerSupport
ed 2012-04-06			

**Step 4** Do one of the following:

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

# Installing the VEM Software on a Stateless ESXi Host

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

## Procedure

- 
- Step 1** See the procedure for [Adding the Cisco Nexus 1000V to an ESXi Image Profile](#), on page 87.
- 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 90
  - [Installing the VEM Software on a Stateless ESXi Host Using VUM](#), on page 92
- Step 3** See the procedure for [Configuring Layer 2 Connectivity](#), on page 64.
- 

## Stateless ESXi Host



### Note

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

VMware vSphere 5.0.0 introduces the VMware Auto Deploy, which provides the infrastructure for loading the ESXi image directly into the host's memory. The software image of a stateless ESXi is loaded from the Auto Deploy Server after every boot. In this context, the image with which the host boots is identified as the image profile.

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

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

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

For more information about the VMware Auto Deploy Infrastructure and stateless boot process, see the "Installing ESXi using VMware Auto Deploy" chapter of the *vSphere Installation and Setup, vSphere 5.0.0* document.

## Adding the Cisco Nexus 1000V to an ESXi Image Profile

### Before You Begin

- Install and set up the VMware Auto Deploy Server. See the *vSphere Installation and Setup* document.

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



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

## Procedure

**Step 1** Start the vSphere PowerCLI application.

**Step 2** Connect to the vCenter Server.

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

**Step 3** Load the image profile offline bundle.

**Note** Each image profile bundle can include multiple image profiles.

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

**Step 4** List the image profiles.

```
[vSphere PowerCLI] > Get-ESXImageProfile
```

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

```
[vSphere PowerCLI] > Get-DeployRuleSet
```

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

**Step 13** Reboot the host.

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

## Installing the VEM Software on a Stateless ESXi Host Using esxcli

### Before You Begin

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

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

### Procedure

**Step 1** Display the VMware version and build number.

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

**Step 2** Log in to the ESXi stateless host.

**Step 3** Copy the offline bundle to the host.

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

```
Installation Result
```

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

```
Reboot Required: false
```

```
VIBs Installed: Cisco_bootbank_cisco-vem-vl50-esx_4.2.1.2.1.0-3.0.1
```

```
VIBs Removed:
```

```
VIBs Skipped:
```

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

**Step 4** Verify that the VIB has installed.

```
~ # esxcli software vib list | grep cisco
cisco-vem-v150-esx      4.2.1.2.1.0-3.0.1      Cisco    PartnerSupported    2012-10-09
```

**Step 5** Check that the VEM agent is running.

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.2.1.0-3.0.1
Build 5
Date Thu Jul 28 01:37:10 PDT 2011
Number of PassThru NICs are 0
VEM modules are loaded
Switch Name      Num Ports  Used Ports  Configured Ports  MTU      Uplinks
vSwitch0         128        4           128              1500     vmnic4
Number of PassThru NICs are 0
VEM Agent (vemdpd) is running
```

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

```
~ # vemcmd show version
VEM Version: 4.2.1.2.1.0-3.0.1
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

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

```
~ # vem version -v
Number of PassThru NICs are 0
Running esx version -441354 x86_64
VEM Version: 4.2.1.2.1.0-3.0.1
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

**Step 8** Add the host to the DVS by using the vCenter Server.**Step 9** On the VSM, verify that the VEM software has been installed.

```
switch# show module
```

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

```
Mod Sw Hw
```

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

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

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

```
Mod Server-IP Server-UUID Server-Name
```

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

## Installing the VEM Software on a Stateless ESXi Host Using VUM

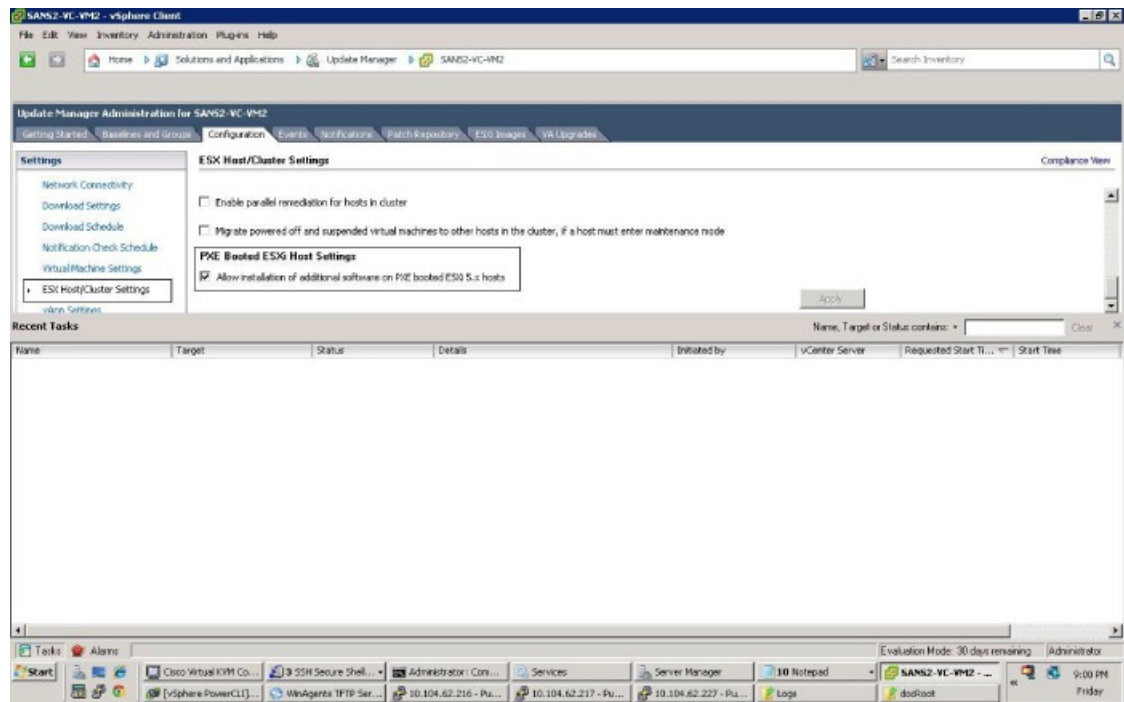
### Before You Begin

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

### Procedure

- Step 1** In the vCenter Server, choose **Home > Update Manager > Configuration > ESX host/Cluster** settings.
- Step 2** Check the **PXE Booted ESXi Host Settings** check box.

*Figure 67: ESX Host/Cluster Settings Window*



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

## Installing a VSM on the Cisco Nexus 1010

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

**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.

**Before You Begin**

Copy the ISO file to the bootflash:repository/ of the virtual service blade.

**Procedure**

- Step 1** Create a virtual service blade by entering the following commands.

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

```
-----
Name           HA-Role      HA-Status    Status          Location
-----
```

```
switch(config)# virtual-service-blade vsm-1
```

```
switch(config-vsb-config)# virtual-service-blade-type new nexus-1000v.4.2.1.SV2.1.1.iso
```

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

```
-----
Name           HA-Role      HA-Status    Status          Location
-----
vsm-1          PRIMARY      NONE         VSB NOT PRESENT PRIMARY
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.SV2.1.1.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 svcs mode from Layer 2 to Layer 3 in Cisco Nexus 1000V.

**Note** The configuration in the highlighted code is optional to change svcs mode from Layer 2 to Layer 3.

```
switch(config)# svcs-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)# svcs mode L3 interface mgmt0
Warning: Config saved but not pushed to vCenter Server due to inactive connection!
switch(config-svs-domain)# show svcs domain
switch(config-svs-domain)# show svcs 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)#
```

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

## 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
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.







# Upgrading the Cisco Nexus 1000V

This chapter contains the following sections:

- [Information About the Software Upgrade, page 97](#)
- [Prerequisites for the Upgrade, page 98](#)
- [Guidelines and Limitations for Upgrading the Cisco Nexus 1000V, page 100](#)
- [Upgrade Procedures, page 102](#)
- [Upgrade Types, page 104](#)
- [Simplified Upgrade Process, page 138](#)
- [Upgrading from Releases 4.0\(4\)SV1\(3, 3a, 3b, 3c, 3d\) to Release 4.2\(1\)SV2\(1.1\), page 140](#)
- [Migrating from Layer 2 to Layer 3, page 140](#)
- [Feature History for Upgrading the Cisco Nexus 1000V, page 149](#)

## Information About the Software Upgrade

### Upgrade Software Sources



**Note**

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

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

**Table 4: Obtaining the Upgrade Software**

Source	Description
Cisco	Download the current release of the Cisco Nexus 1000V software from <a href="#">Cisco.com</a> .

Source	Description
VMware	<p>Download the VMware software from the <a href="#">VMware website</a>.</p> <p>The current Cisco Nexus 1000V software release image for VMware Release 5.1 is at the VMware web site:</p> <p><b>Note</b>    <b>The following paths are not available for the Beta release.</b></p> <ul style="list-style-type: none"> <li>• Online portal for VMware Update Manager (VUM): <a href="http://hostupdate.vmware.com/software/VUM/PRODUCTION/cisco-main/esx/cisco/cisco-index.xml">http://hostupdate.vmware.com/software/VUM/PRODUCTION/cisco-main/esx/cisco/cisco-index.xml</a></li> <li>• Offline patch portal: <a href="http://www.vmware.com/patchmgr/download.portal">http://www.vmware.com/patchmgr/download.portal</a></li> </ul>

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

## Prerequisites for the Upgrade

### Before You Begin

- The Upgrade Application cannot be used for the upgrade of the Virtual Supervisor Modules (VSMs) from Release 4.2(1)SV1(4) to 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 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 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 VUM-based upgrades. You can abort the upgrade procedure by pressing Ctrl-C.

## Prerequisites for Upgrading VSMs

Upgrading VSMs has the following prerequisites:

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



### Important

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

## Prerequisites for Upgrading VEMs



### Caution

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



### Note

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

- You are logged in to the VSM command-line interface (CLI) in EXEC mode.
- You have a copy of your VMware documentation available for installing software on a host.
- You have already obtained a copy of the VEM software file from one of the sources listed in [VEM Software, on page 16](#). For more information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.
- If you need to migrate a vSphere host from ESX to ESXi, do it before the Cisco Nexus 1000V upgrade.

- You have placed the VEM software file in `/tmp` on the vSphere host. Placing it in the root (`/`) directory might interfere with the upgrade. Make sure that the root RAM disk has at least 12 MB of free space by entering the **vdf** command.
- On your upstream switches, you must have the following configuration.
  - On Catalyst 6500 Series switches with the Cisco IOS software, enter one of the following commands:  
   (config-if) **portfast trunk**  
   or  
   (config-if) **portfast edge trunk**
  - On Cisco Nexus 5000 Series switches with Cisco NX-OS software, enter the **spanning-tree port type edge trunk** command.
- On your upstream switches, we highly recommend that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On your upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommend that you enter the following commands:
  - (config-if) **spanning-tree bpdn filter**
  - (config-if) **spanning-tree bpdn guard**
- For more information about configuring spanning tree, BPDU, or PortFast, see the documentation for your upstream switch.

## Guidelines and Limitations for Upgrading the Cisco Nexus 1000V

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



### Caution

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



### Note

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

- You are upgrading the Cisco Nexus 1000V software to 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 one-step **install all** command to upgrade your software. This command upgrades the VSMs.
  - Do not enter another **install all** command while running the installation. You can run commands other than configuration commands.
  - During the VSM upgrade, if you try to add a new VEM or any of the VEMs are detached due to uplink flaps, the VEM attachment is queued until the upgrade completes.

**Note**

If the 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:

- 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*.
- 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.

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

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

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

**Note**

If your hosts are running a release prior to VMware 4.1, upgrade to VMware 4.1, VMware 5.0, or VMware 5.1. See [Installing and Upgrading VMware, on page 151](#).

- 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 when upgrading to the current release.

**Table 5: Upgrade Paths from Cisco Nexus 1000V Releases**

If you are running this configuration	Follow these steps
Release 4.0(4)SV1(1) or 4.0(4)SV1(2)	Upgrades from these releases are not supported.
Releases 4.0(4)SV1(3), 4.0(4)SV1(3a), 4.0(4)SV1(3b), 4.0(4)SV1(3c), or 4.0(4)SV1(3d)	<ol style="list-style-type: none"> <li>1 <a href="#">Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b)</a></li> <li>2 <a href="#">Upgrading from Releases 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</a></li> </ol>

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4, 4a, or 4b) with a vSphere release 4.0 Update 1 or later	<ol style="list-style-type: none"> <li>1 Upgrading from VMware Release 4.0 to VMware Release 4.1, on page 151</li> <li>2 Upgrading VSMs from Releases 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1), on page 110</li> <li>3 VEM Upgrade Methods from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</li> </ol>
Release 4.2(1)SV1(4, 4a, or 4b) with a vSphere release 4.1 GA, patches, or updates	<ol style="list-style-type: none"> <li>1 Upgrading VSMs from Releases 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1), on page 110</li> <li>2 VEM Upgrade Methods from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</li> </ol>
Release 4.2(1)SV1(4a) or 4.2(1)SV1(4b) with a vSphere release 5.0 GA, patches, or updates	<ol style="list-style-type: none"> <li>1 Upgrading VSMs from Releases 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1), on page 110</li> <li>2 VEM Upgrade Methods from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</li> </ol>

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

**Table 6: Upgrade Paths from Releases 4.2(1)SV1(5.1), 4.2(1)SV1(5.1a), 4.2(1)SV1(5.2)**

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(5.1) or 4.2(1)SV1(5.1a) with vSphere 4.1 GA, patches, or updates.	<ol style="list-style-type: none"> <li>1 Upgrading VSMs from Releases 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1), on page 110</li> <li>2 VEM Upgrade Methods from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</li> </ol>

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(5.1), 4.2(1)SV1(5.1a), or 4.2(1)SV1(5.2) with vSphere 5.0 GA, patches, or updates.	<ol style="list-style-type: none"> <li>1 <a href="#">Upgrading VSMs from Releases 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1), on page 110</a></li> <li>2 <a href="#">VEM Upgrade Methods from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)</a></li> </ol>
Release 4.2(1)SV2(1.1) with ESX version upgrade.	<a href="#">Installing and Upgrading VMware, on page 151</a>

## Upgrade Types

Upgrades can be one of three types:

- Upgrade of Cisco Nexus 1000V version only, with vSphere version intact. See [Upgrading the Cisco Nexus 1000V Only, on page 104](#).
- Upgrade of both vSphere and Cisco Nexus 1000V versions together. See [Combined Upgrade of vSphere and Cisco Nexus 1000V, on page 105](#).
- Upgrade of vSphere version only, with Cisco Nexus 1000V version intact. See the [Installing and Upgrading VMware, on page 151](#) appendix.

## Upgrading the Cisco Nexus 1000V Only

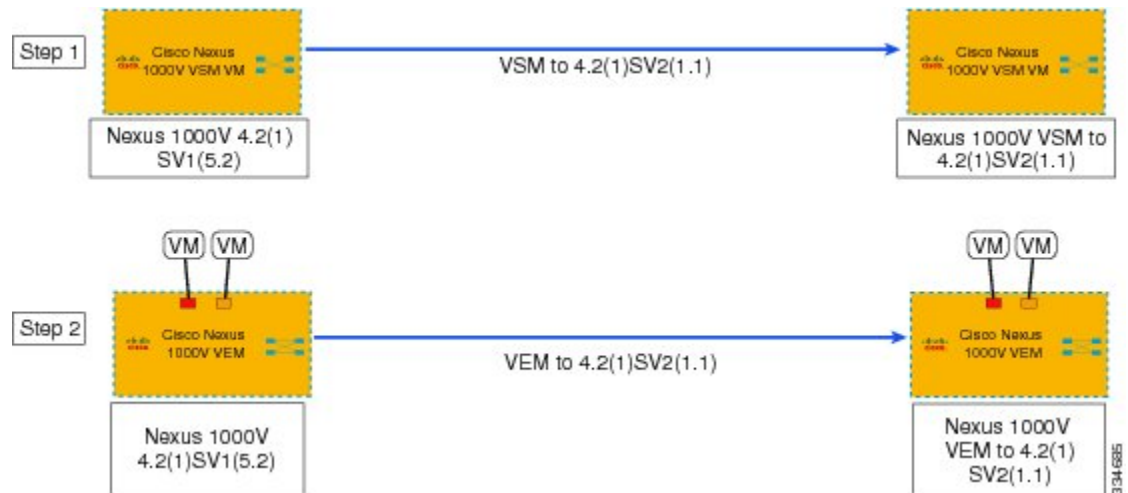
You must complete the following procedures to upgrade the Cisco Nexus 1000V only.

- 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 87](#).
  - For a VUM-based upgrade of a Stateful ESX or ESXi, use a host upgrade baseline with the VEM depot. See [Upgrading the ESXi Hosts to Release 5.1, on page 161](#).
  - For a stateful manual upgrade using the **esxupdate** or **esxcli** commands, see [Installing ESXi 5.1 Host Software Using the CLI, on page 165](#).



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

**Figure 68: Cisco Nexus 1000V Only Upgrade**



## Combined Upgrade of vSphere and Cisco Nexus 1000V

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

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

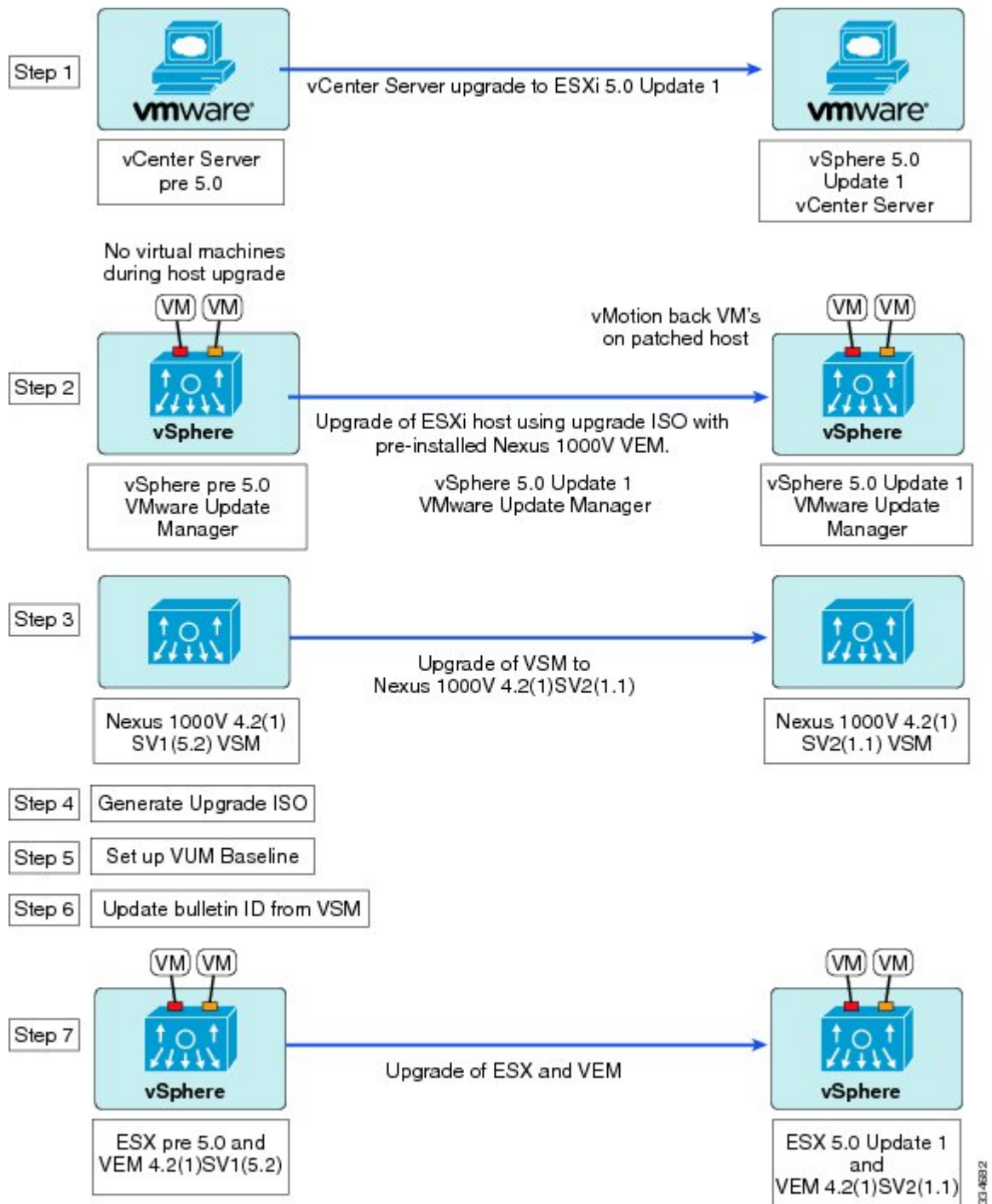


### Note

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

The following figure shows the workflow for a combined upgrade.

**Figure 69: Combined Upgrade Workflow**



The following procedures are necessary to perform a combined upgrade.

- 1 [Upgrading the vCenter Server to Release 5.1, on page 123](#)
- 2 [Upgrading the vCenter Update Manager to Release 5.1, on page 160](#)
- 3 [Upgrading VSMs from Releases 4.2\(1\)SV1\(4\), SV1\(4a\), SV1\(4b\), SV1\(5.1\), SV1\(5.1a\), or SV1\(5.2\) to Release 4.2\(1\)SV2\(1.1\), on page 110](#)
- 4 [Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, on page 120](#)
- 5 [Upgrading the ESXi Hosts to Release 5.1, on page 161](#)
- 6 [Verifying the Build Number and Upgrade, on page 163](#)

## 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:

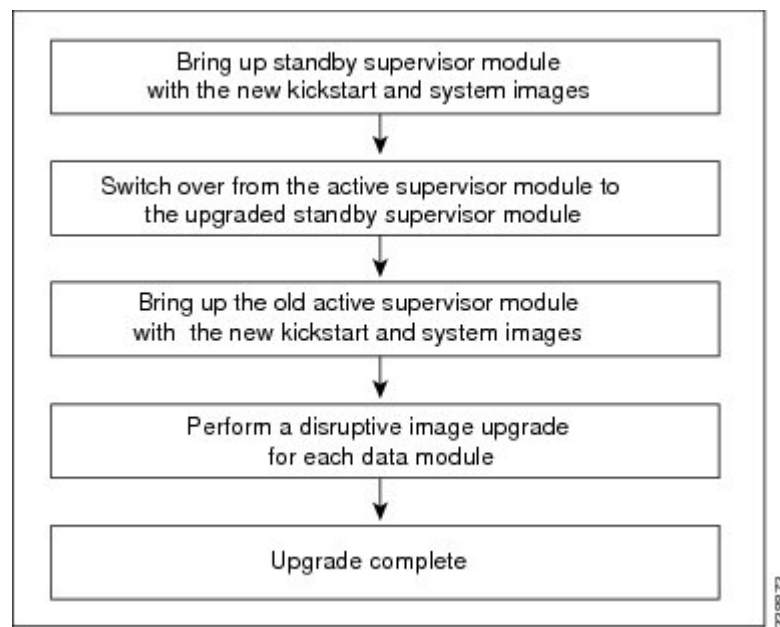
- Kickstart image
- System image
- VEM images

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.

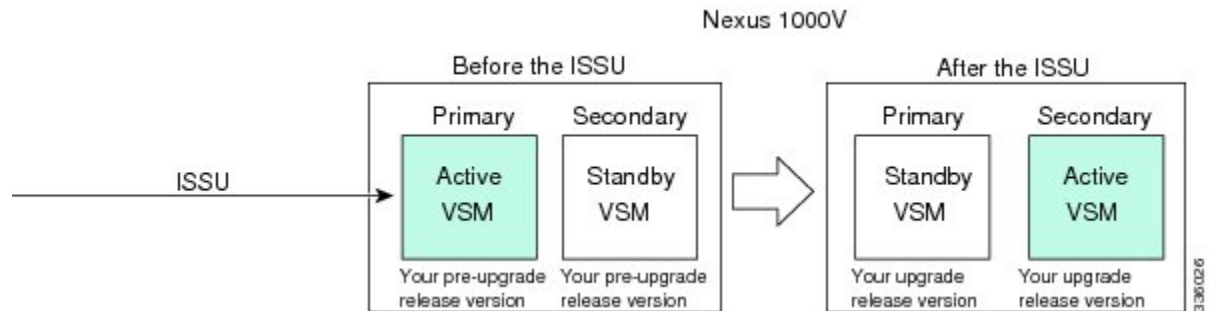
**Figure 70: ISSU Process**



## ISSU VSM Switchover

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

**Figure 71: 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), SV1(4a), SV1(4b), SV1(5.1), SV1(5.1a), or SV1(5.2) to Release 4.2(1)SV2(1.1)

### Procedure

**Step 1** Log in to the active VSM.

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

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

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

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

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

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

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

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

**Step 7** Verify that there is space available on the standby VSM.

```
switch# dir bootflash://sup-standby/
.
.
.
Usage for bootflash://
  485830656 bytes used
```

```
1109045248 bytes free
1594875904 bytes total
```

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

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

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

- Copy the ISO image.

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.4.2.1.SV2.1.1.iso
bootflash:nexus-1000v.4.2.1.SV2.1.1.iso
```

- Copy kickstart and system images.

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin
bootflash:nexus-1000v-kickstart-4.2.1.SV2.1.1.bin
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-4.2.1.SV2.1.1.bin
bootflash:nexus-1000v-4.2.1.SV2.1.1.bin
```

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

- ISO

```
switch# show install all impact iso bootflash:nexus-1000v.4.2.1.SV2.1.1.iso
```

```
Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin for boot variable
"kickstart".
```

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

```
Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin for boot variable "system".
```

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

```
Verifying image type.
```

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

```
Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin.
```

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

```
Extracting "kickstart" version from image
```

```
bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin.
```

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

```
Notifying services about system upgrade.
```

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

```
Compatibility check is done:
```

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	reset	
2	yes	non-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
1	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
1	kickstart	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
2	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
2	kickstart	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes

Module	Running-Version	ESX Version
VSM Compatibility	ESX Compatibility	
3	4.2(1)SV1(5.2)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
	COMPATIBLE	COMPATIBLE
4	4.2(1)SV1(5.2)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
	COMPATIBLE	COMPATIBLE

- kickstart and system

```
switch# show install all impact kickstart bootflash:nexus-1000v-kickstart.4.2.1.SV2.1.1.bin system
bootflash:nexus-1000v.4.2.1.SV2.1.1.bin
```

```
Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin for boot variable
"kickstart".
```

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

```
Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin for boot variable "system".
```

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

```
Verifying image type.
```

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

```
Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin.
```

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

```
Extracting "kickstart" version from image
```

```
bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin.
```

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

```
Notifying services about system upgrade.
```

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

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	reset	
2	yes	non-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
1	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes



1	kickstart	4.2 (1) SV1 (5.2)	4.2 (1) SV2 (1.1)	yes
2	system	4.2 (1) SV1 (5.2)	4.2 (1) SV2 (1.1)	yes
2	kickstart	4.2 (1) SV1 (5.2)	4.2 (1) SV2 (1.1)	yes

Module	Running-Version	ESX Version
VSM Compatibility	ESX Compatibility	
3	4.2(1) SV1 (5.2)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
	COMPATIBLE	COMPATIBLE
4	4.2(1) SV1 (5.2)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
	COMPATIBLE	COMPATIBLE

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

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

- If the following output is displayed, the Cisco VSG is configured in the deployment. You must follow the upgrade procedure in the “Complete Upgrade Procedure” section in Chapter 7, “Upgrading the Cisco Virtual Security Gateway and Cisco Virtual Network Management Center” of the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1)* and *Cisco Virtual Network Management Center Release 1.3 Installation and Upgrade Guide*.

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

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

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

**Step 13** Save the running configuration to the startup configuration.

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

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

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

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

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

- Upgrade using the ISO image.

```
switch# install all iso bootflash:nexus-1000v-4.2.1.SV2.1.1.iso
```

- Upgrade using the kickstart and system images.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart-4.2.1.SV2.1.1.bin system
bootflash:nexus-1000v-4.2.1.SV2.1.1.bin
```

```
Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin for boot variable
"kickstart".
```

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

```
Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin for boot variable "system".
```

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

```

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

Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin.
[#####] 100% -- SUCCESS

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

```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	reset	
2	yes	non-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
1	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
1	kickstart	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
2	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
2	kickstart	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes

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

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

### Step 16 Continue with the installation by pressing Y.

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

Install is in progress, please wait.

```

Syncing image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin to standby.
[#####] 100% -- SUCCESS

```

```

Syncing image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin to standby.
[#####] 100% -- SUCCESS

```

```

Setting boot variables.
[#####] 100% -- SUCCESS

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

```

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

Continuing with installation, please wait

```

Module 2: Waiting for module online
-- SUCCESS

```

Install has been successful

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

```

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

Software
  loader:    version unavailable [last: loader version not available]
  kickstart: version 4.2(1)SV2(1.1) [build 4.2(1)SV2(1.1)]
  system:    version 4.2(1)SV2(1.1) [build 4.2(1)SV2(1.1)]
  kickstart image file is: bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin
  kickstart compile time: 1/11/2012 3:00:00 [01/11/2012 12:49:49]
  system image file is:   bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin
  system compile time:    1/11/2012 3:00:00 [01/11/2012 13:42:57]

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

  Device name: Nexus1000v
  bootflash:   1557496 kB

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

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

```

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

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

**Step 19** Display the log of the last installation.

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

```
Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin for boot variable
"kickstart".
```

```
-- SUCCESS
```

```
Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin for boot variable "system".
```

```
-- SUCCESS
```

```
Verifying image type.
```

```
-- SUCCESS
```

```
Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin.
```

```
-- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin.
```

```
-- SUCCESS
```

```
Notifying services about system upgrade.
```

```
-- SUCCESS
```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	reset	
2	yes	non-disruptive	reset	

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
1	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
1	kickstart	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
2	system	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes
2	kickstart	4.2(1)SV1(5.2)	4.2(1)SV2(1.1)	yes

Images will be upgraded according to following table:

Module	Running-Version	ESX Version
--------	-----------------	-------------

VSM Compatibility	ESX Compatibility	
-----	-----	-----
3	4.2(1)SV1(5.2)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
COMPATIBLE	COMPATIBLE	
4	4.2(1)SV1(5.2)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
COMPATIBLE	COMPATIBLE	

Install is in progress, please wait.

Syncing image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin to standby.  
-- SUCCESS

Syncing image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin to standby.  
-- SUCCESS

Setting boot variables.  
-- SUCCESS

Performing configuration copy.  
-- SUCCESS

Module 2: Waiting for module online.  
-- SUCCESS

Notifying services about the switchover.  
-- SUCCESS

"Switching over onto standby".

switch#  
switch#  
switch#

```
switch# attach module 2
Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(standby)#
switch(standby)# show install all status
This is the log of last installation.
```

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

```

Module 2: Waiting for module online.
-- SUCCESS

Install has been successful.
switch(standby) #

```

---

## VEM Upgrade Procedures

- VUM Upgrade Procedures
  - Generate an upgrade ISO. See [Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image](#), on page 120.
  - Set up VUM baselines. See [Upgrading the ESXi Hosts to Release 5.1](#), on page 161.
  - Initiate an upgrade from VUM. See [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(4\), \(4a\), \(4b\), \(5.1\), \(5.1a\), or \(5.2\) to Release 4.2\(1\)SV2\(1.1\)](#), on page 125.
  - Upgrade VEM from VSM. See [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(4\), \(4a\), \(4b\), \(5.1\), \(5.1a\), or \(5.2\) to Release 4.2\(1\)SV2\(1.1\)](#), on page 125.
- Manual upgrade procedures
  - Upgrading VIB Manually from the CLI. See [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(4\), \(4a\), \(4b\), \(5.1\), \(5.1a\), or \(5.2\) to Release 4.2\(1\)SV2\(1.1\)](#), on page 132
- Installing or upgrading stateless ESXi. See [Installing the VEM Software on a Stateless ESXi Host](#), on page 87.

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 87.
- An upgrade that involve a migration from ESX to ESXi (of the same or different vSphere version).

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

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

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

**Figure 72: Workflow 1 with a Cisco Nexus 1000V Version 4.2(1)SV1(4), SV1(4a), SV1(4b), SV1(5.1), or SV1(5.2) Installed**

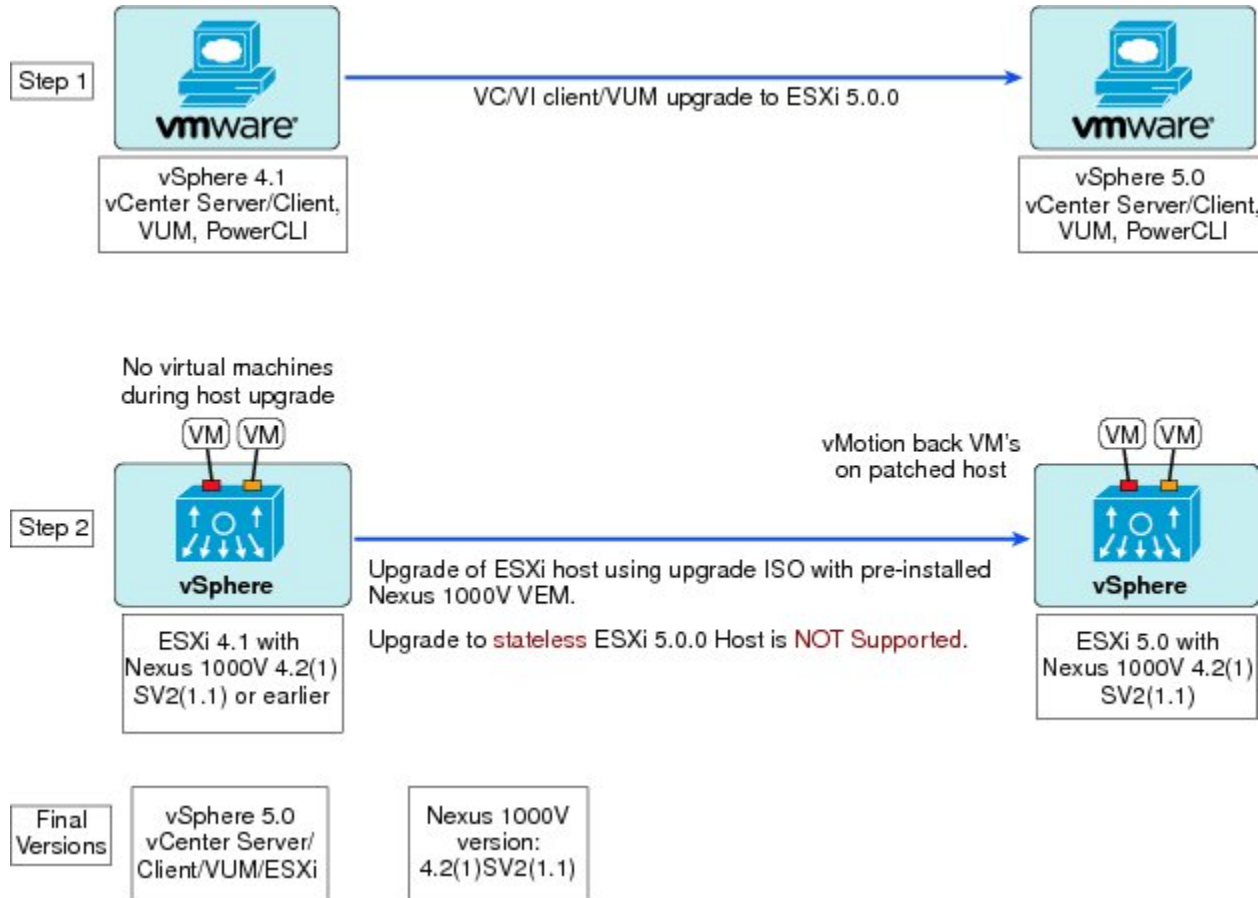


If you are using VUM, set up a host patch baseline with the VEM's offline bundle. Then follow [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(4\), \(4a\), \(4b\), \(5.1\), \(5.1a\), or \(5.2\) to Release 4.2\(1\)SV2\(1.1\)](#), on page 125.

If you are upgrading from the command line, see [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(4\), \(4a\), \(4b\), \(5.1\), \(5.1a\), or \(5.2\) to Release 4.2\(1\)SV2\(1.1\)](#), on page 132.

The following figure shows Workflow 2 where Cisco Nexus 1000V Release 4.2(1)SV2(1.1) is installed and VMware 4.1 is upgraded to 5.0.

**Figure 73: Workflow 2 with Cisco Nexus 1000V 4.2(1)SV2(1.2) Installed and Upgrading ESX from 4.1 to 5.0**



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

- If you are using VUM versions prior to 5.0, do one of the following:
  - If you are upgrading the ESX host to a new patch level, use a host patch baseline (independent of whether the VEM version is being changed as well).
  - If you are upgrading the ESX host to a new update within a release or major release, use a host upgrade baseline (again independent of whether the VEM version is being changed as well).
  - You cannot upgrade the ESX version and VEM version simultaneously. You need to schedule them as two separate upgrades.
- If you are using VUM version 5.0 or later, use the following method (independent of whether the VEM version is being changed as well):
  - If you are upgrading the ESX host to a new patch level within a release, use a host patch baseline. For example, vSphere 4.1 GA to 4.1 Patch 03.
  - If you are upgrading the ESX host to a new update within a release, use a host upgrade baseline. For example, vSphere 5.0 GA to 5.0 U1.
  - If you are upgrading the ESX host to a major release (for example, vSphere 4.1 U2 to 5.0 U1), generate an upgrade ISO and set up a host upgrade baseline. The upgrade ISO must have the desired final images for both ESX and VEM. The procedure to generate an upgrade ISO is in [Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image](#), on page 120.
  - You can upgrade the ESX version and VEM version simultaneously if you are using VUM 5.0 Update 1 or later. VUM 5.0 GA does not support a combined upgrade.


**Note**

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

## VUM Upgrade Procedures

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

#### Before You Begin

- Install the VMware PowerCLI on a Windows platform. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform, where the VMware PowerCLI is installed, do one of the following:
  - Download the ESX depot, which is a .zip file, to a local file path.
  - Download the VEM offline bundle, which is a .zip file, to a local file path.



**Note**

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

**Procedure**

**Step 1** Start the VMWare PowerCLI application.

**Step 2** Connect to the vCenter Server.

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

**Step 3** Load the ESX depot.

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot c:\vmware-ESXi-5.1.0-depot.zip
```

**Step 4** Display the image profiles.

```
[vSphere PowerCLI] > Get-ESXImageProfile
```

Name	Vendor	Last Modified	Acceptance Level
ESXi-5.1.0-799733-no-tools	VMware, Inc.	8/19/2011 1:...	PartnerSupported
ESXi-5.1.0-799733-standard	VMware, Inc.	8/19/2011 1:...	PartnerSupported

**Step 5** Clone the ESX standard image profile.

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

```
[vSphere PowerCLI] > New-ESXImageProfile -CloneProfile ESXi-5.0.0-469512-standard -Name nlkv-Image
```

Name	Vendor	Last Modified	Acceptance Level
nlkv-Image	VMware, Inc.	8/19/2011 1:...	PartnerSupported

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

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot C:\ VEM510-201210150105-BG-release.zip
```

```
Depot Url
```

```
-----
zip:C:\Users\Administrator\Documents\ VEM510-201210150105-BG-release.zip?in...
```

**Step 7** Confirm that the nlkv-vib package is loaded.

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

Name	Version	Vendor	Release Date
cisco-vem-v150-esx	4.2.1.2.1.0-3.0.1	Cisco	1/21/2012...

**Step 8** Bundle the nlkv-package into the cloned image profile.

```
[vSphere PowerCLI] > Add-ESXSoftwarePackage -ImageProfile nlkv-Image -SoftwarePackage cisco-vem-v140-esx
```

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

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

```
[vSphere PowerCLI]> $img = Get-ESXImageProfile nlkv-Image
```

```
[vSphere PowerCLI]> $img.vibList
```

Name	Version	Vendor	Release Date
----	-----	-----	-----
net-ixgbe	2.0.84.8.2-10vmw.500.0.0.46...	VMware	8/19/2011...
ata-pata-hpt3x2n	0.3.4-3vmw.500.0.0.469512	VMware	8/19/2011...
ehci-ehci-hcd	1.0-3vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-atiixp	0.4.6-3vmw.500.0.0.469512	VMware	8/19/2011...
scsi-megaraid2	2.00.4-9vmw.500.0.0.469512	VMware	8/19/2011...
uhci-usb-uhci	1.0-3vmw.500.0.0.469512	VMware	8/19/2011...
net-r8168	8.013.00-3vmw.500.0.0.469512	VMware	8/19/2011...
ohci-usb-ohci	1.0-3vmw.500.0.0.469512	VMware	8/19/2011...
scsi-qla4xxx	5.01.03.2-3vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-sil680	0.4.8-3vmw.500.0.0.469512	VMware	8/19/2011...
scsi-megaraid-sas	4.32-1vmw.500.0.0.469512	VMware	8/19/2011...
scsi-aic79xx	3.1-5vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-amd	0.3.10-3vmw.500.0.0.469512	VMware	8/19/2011...
net-bnx2	2.0.15g.v50.11-5vmw.500.0.0...	VMware	8/19/2011...
misc-drivers	5.0.0-0.0.469512	VMware	8/19/2011...
sata-ahci	3.0-6vmw.500.0.0.469512	VMware	8/19/2011...
scsi-fnic	1.5.0.3-1vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-pdc2027x	1.0-3vmw.500.0.0.469512	VMware	8/19/2011...
scsi-hpsa	5.0.0-17vmw.500.0.0.469512	VMware	8/19/2011...
sata-sata-sil	2.3-3vmw.500.0.0.469512	VMware	8/19/2011...
net-igb	2.1.11.1-3vmw.500.0.0.469512	VMware	8/19/2011...
net-e1000e	1.1.2-3vmw.500.0.0.469512	VMware	8/19/2011...
net-forcedeth	0.61-2vmw.500.0.0.469512	VMware	8/19/2011...
sata-ata-piix	2.12-4vmw.500.0.0.469512	VMware	8/19/2011...
scsi-qla2xxx	901.k1.1-14vmw.500.0.0.469512	VMware	8/19/2011...
scsi-adp94xx	1.0.8.12-6vmw.500.0.0.469512	VMware	8/19/2011...
net-sky2	1.20-2vmw.500.0.0.469512	VMware	8/19/2011...
cisco-vem-v150-esx	4.2.1.2.1.0-3.0.1	Cisco	1/21/2012...
ipmi-ipmi-msghandler	39.1-4vmw.500.0.0.469512	VMware	8/19/2011...
net-be2net	4.0.88.0-1vmw.500.0.0.469512	VMware	8/19/2011...
esx-base	5.0.0-0.0.469512	VMware	8/19/2011...
ipmi-ipmi-si-drv	39.1-4vmw.500.0.0.469512	VMware	8/19/2011...
scsi-megaraid-mbox	2.20.5.1-6vmw.500.0.0.469512	VMware	8/19/2011...
net-nx-nic	4.0.557-3vmw.500.0.0.469512	VMware	8/19/2011...
sata-sata-promise	2.12-3vmw.500.0.0.469512	VMware	8/19/2011...
scsi-ips	7.12.05-4vmw.500.0.0.469512	VMware	8/19/2011...
scsi-lpfc820	8.2.2.1-18vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-cmd64x	0.2.5-3vmw.500.0.0.469512	VMware	8/19/2011...
sata-sata-svw	2.3-3vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-via	0.3.3-2vmw.500.0.0.469512	VMware	8/19/2011...
esx-tboot	5.0.0-0.0.469512	VMware	8/19/2011...
misc-cnic-register	1.1-1vmw.500.0.0.469512	VMware	8/19/2011...
net-s2io	2.1.4.13427-3vmw.500.0.0.46...	VMware	8/19/2011...
net-e1000	8.0.3.1-2vmw.500.0.0.469512	VMware	8/19/2011...
block-cciss	3.6.14-10vmw.500.0.0.469512	VMware	8/19/2011...
net-enic	1.4.2.15a-1vmw.500.0.0.469512	VMware	8/19/2011...
net-bnx2x	1.61.15.v50.1-1vmw.500.0.0...	VMware	8/19/2011...
scsi-mpt2sas	06.00.00.00-5vmw.500.0.0.46...	VMware	8/19/2011...
sata-sata-nv	3.5-3vmw.500.0.0.469512	VMware	8/19/2011...
ata-pata-serverworks	0.4.3-3vmw.500.0.0.469512	VMware	8/19/2011...
net-cnic	1.10.2j.v50.7-2vmw.500.0.0...	VMware	8/19/2011...
scsi-mptsas	4.23.01.00-5vmw.500.0.0.469512	VMware	8/19/2011...

```

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

```

**Step 10** Export the image profile to an ISO file.

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

**Upgrading the vCenter Server to Release 5.1****Note**

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

**Before You Begin**

- Download the upgrade ISO file that contains the ESXi 5.1 image and the Cisco Nexus 1000V Release 4.2(1)SV1(5.2) 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 5.1 installation file.

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

- Step 2** Double-click **autorun**.
- Step 3** In the **VMware vCenter Installer** window, click **vCenter Server**.
- Step 4** Click **Install**.
- Step 5** Choose a language and click **OK**.
- Step 6** Click **Next**.
- Step 7** In the Patent Agreement window, click **Next**.
- Step 8** In the **License Agreement** window, click the **I agree to the terms in the license agreement** radio button.
- Step 9** Click **Next**.
- Step 10** In the **Database Options** screen, click **Next**.
- Step 11** Click the **Upgrade existing vCenter Server database** radio button and check the **I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\** check box.
- Step 12** From the **Windows Start** Menu, click **Run**.
- Step 13** Enter the name of the folder that contains the vCenter Server database and click **OK**.
- Step 14** Drag a copy of the parent folder (SSL) to the desktop as a backup.
- Step 15** Return to the installer program.
- Step 16** Click **Next**.
- Step 17** In the vCenter Agent Upgrade window, click the **Automatic** radio button.
- Step 18** Click **Next**.
- Step 19** In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box.
- Step 20** Click **Next**.
- Step 21** Review the port settings and click **Next**.
- Step 22** In the **vCenter Server JVM Memory** screen based on the number of hosts, click the appropriate memory radio button.
- Step 23** Click **Next**.
- Step 24** Click **Install**.
- Step 25** Click **Finish**.  
This step completes the upgrade of the vCenter Server.
- Step 26** Upgrade the VMware vSphere Client to ESXi 5.1.
- Step 27** Open the VMware vSphere Client.
- Step 28** From the **Help** menu, choose **About VMware vSphere**.
- Step 29** Confirm that the vSphere Client and the VMware vCenter Server are both version VMware 5.1.
- Step 30** Click **OK**, and exit the VMware vSphere Client.
- 

### What to Do Next

Complete the steps in [Upgrading the vCenter Update Manager to Release 5.1](#), on page 160.

## Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)



### Caution

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

### Procedure

#### Step 1 Display the current configuration.

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

```
Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201209150101-BG
    DVS: VEM410-201208144101-BG
switch#
```

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

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

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

#### Step 3 Verify that the upgrade notification was sent.

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM410-201209150101-BG
    DVS: VEM410-201208144101-BG
switch#
```

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

#### Step 4 Verify that the server administrator has accepted the upgrade in the vCenter.

For more information about how the server administrator accepts the VEM upgrade, see [Accepting the VEM Upgrade](#), on page 128.

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
  VSM: VEM410-201209150101-BG
  DVS: VEM410-201208144101-BG
switch#
```

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

**Step 5** Initiate the VUM upgrade process.

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

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
  VSM: VEM410-201209150101-BG
  DVS: VEM410-201209150101-BG
switch#
```

**Note** The DVS bundle ID is updated and is highlighted.

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

**Step 6** Check for the upgrade complete status.

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

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

```

VSM: VEM410-201209150101-BG
DVS: VEM410-201209150101-BG
switch#

```

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

```

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

```

```

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
VSM: VEM410-201209150101-BG
DVS: VEM410-201209150101-BG
switch#

```

**Step 8** Verify that the upgrade process is complete.

```
switch# show module
```

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

Mod	Sw	Hw
1	4.2(1)SV2(1.1)	0.0
2	4.2(1)SV2(1.1)	0.0
<b>3</b>	<b>4.2(1)SV2(1.1)</b>	<b>VMware ESXi 5.0.0 Releasebuild-469512 (3.0)</b>
<b>4</b>	<b>4.2(1)SV2(1.1)</b>	<b>VMware ESXi 5.0.0 Releasebuild-623860 (3.0)</b>

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.

The upgrade is complete.

---

## Accepting the VEM Upgrade

### Before You Begin

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

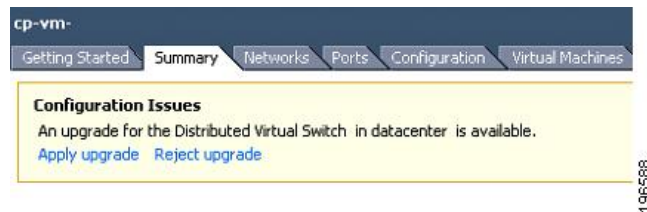
### Procedure

---

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

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

*Figure 74: vSphere Client DVS Summary Tab*



**Step 3** Click **Apply upgrade**.

The network administrator is notified that you are ready to apply the upgrade to the VEMs.

---

## Manual Upgrade Procedures

### Upgrading the VEM Software Using the vCLI

You can upgrade the VEM software by using the vCLI.

### Before You Begin

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



**Note**

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

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

**Procedure**

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

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

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

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

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

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

```
[root@serialport tmp]# vihostupdate -install -bundle VEM410-201209150101.zip
```

```
Enter username: root
```

```
Enter password:
```

```
Please wait installation in progress ...
```

```
The update completed successfully, but the system needs to be rebooted for the changes to be effective.
```

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

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

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

```
esxupdate -b [VMware offline update bundle] update
```

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

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

```
/tmp # esxupdate --bundle=VEM410 201209150101.zip
Unpacking cross_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1
#####
[100%]

Installing packages :cross_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1
#####
[100%]

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

/tmp # esxupdate -b cross_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1 update
Unpacking cross_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1
#####
[100%]

Installing packages :installing cross_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1
#####
[100%]

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

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

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

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

```
~ # esxcli software vib install -d /tmp/VEM500-20120803150112-BG-release.zip
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: Cisco_bootbank_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1.vib
  VIBs Removed:
  VIBs Skipped:
~ #

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v144-4.2.1.2.1.1.0-3.0.2.vib
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: Cisco_bootbank_cisco-vem-v144-esx_4.2.1.2.1.1.0-3.0.2
  VIBs Removed:
  VIBs Skipped:
~ #
```

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

```
[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-469512
root@serialport tmp]# # esxupdate query
-----Bulletin ID----- Installed-----Summary-----
VEM410-201209150101-BG 2012-08-21T08:18:22 Cisco Nexus 1000V 4.2(1)SV2(1.1)

[root@host212 ~]# . ~ # vem status -v
Package vssnet-esx5.5.0-00000-release
Version 4.2.1.2.1.0-3.0.1
Build 1
Date Fri Aug 3 00:02:21 PDT 2012

Number of PassThru NICs are 0
VEM modules are loaded

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

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

~ #

[root@host212 ~]# vemcmd show version
VEM Version: 4.2.1.2.1.0-3.0.1
VSM Version: 4.2(1)SV2(1.1)
System Version: VMware ESXi 4.1.0 Releasebuild-502767
~ #
```

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

```
switch# show module
```

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

Mod	Sw	Hw
1	4.2(1)SV2(1.1)	0.0
2	4.2(1)SV2(1.1)	0.0
3	4.2(1)SV2(1.1)	VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4	4.2(1)SV2(1.1)	VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

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

```
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA
```

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

\* this terminal session

switch#

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

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

## Upgrading the VEMs Manually from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to Release 4.2(1)SV2(1.1)



### Note

The important fields are highlighted in the steps. Bundle ID names may change depending on the build date.

### 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 128](#).

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



### Note

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



### Caution

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

### Procedure

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

```
switch# vmware vem upgrade notify
```

Warning:

Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to corresponding

"Cisco Nexus 1000V and VMware Compatibility Information" guide.

**Step 2** Verify that the upgrade notification was sent.

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

```
Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
```

```
VSM: VEM410-201209150101-BG
```

```
DVS: VEM410-201208144101-BG
```

```
switch#
```

**Step 3** Verify that the server administrator has accepted the upgrade in vCenter Server.

For details about the server administrator accepting the VEM upgrade, see [Accepting the VEM Upgrade](#), on page 128.

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
```

```
VSM: VEM410-201209150101-BG
```

```
DVS: VEM410-201208144101-BG
```

```
switch#
```

**Step 4** Perform one of the following tasks:

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

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

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

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

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

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

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

```

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
  VSM: VEM410-201209150101-BG
  DVS: VEM410-201209150101-BG BG
switch#

```

**Step 6** Check for the Upgrade Complete status.

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

```

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Mon Aug 20 23:40:51 2012
Upgrade Status Time(vCenter): Tue Aug 21 19:13:07 2012
Upgrade Start Time: Mon Aug 20 23:44:50 2012
Upgrade End Time(vCenter): Tue Aug 21 19:14:38 2012
Upgrade Error:
Upgrade Bundle ID:
  VSM: VEM410-201209150101-BG
  DVS: VEM410-201209150101-BG BG
switch#

```

**Step 7** Coordinate with and wait until the server administrator upgrades all ESX host VEMs with the new VEM software release and informs you that the upgrade process is complete.  
The server administrator performs the manual upgrade by using the **vihostupdate** command or the **esxcli** command. For more information, see [Upgrading the VEM Software Using the vCLI](#), on page 128.

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

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

```

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
  VSM: VEM410-201209150101-BG
  DVS: VEM410-201209150101-BG BG
switch#

```

**Step 9** Verify that the upgrade process is complete.

```
switch# show module
```

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

```

Mod  Sw                      Hw
---  ---                      ---
1    4.2(1)SV2(1.1)          0.0
2    4.2(1)SV2(1.1)          0.0
3    4.2(1)SV2(1.1)          VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    4.2(1)SV2(1.1)          VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

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

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

```

\* this terminal session

switch#

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

The upgrade is complete.

## Installing the VEM Software on a Stateless ESXi Host

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

### Procedure

- Step 1** See the procedure for [Adding the Cisco Nexus 1000V to an ESXi Image Profile](#), on page 87.
- 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 90
  - [Installing the VEM Software on a Stateless ESXi Host Using VUM](#), on page 92
- Step 3** See the procedure for [Configuring Layer 2 Connectivity](#), on page 64.

## Installing the VEM Software on a Stateless ESXi Host Using esxcli

### Before You Begin

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

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

### Procedure

**Step 1** Display the VMware version and build number.

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

**Step 2** Log in to the ESXi stateless host.

**Step 3** Copy the offline bundle to the host.

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

Installation Result

```
Message: WARNING: Only live system was updated, the change is not persistent.
Reboot Required: false
VIBs Installed: Cisco_bootbank_cisco-vem-v150-esx_4.2.1.2.1.0-3.0.1
VIBs Removed:
VIBs Skipped:
```

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

**Step 4** Verify that the VIB has installed.

```
~ # esxcli software vib list | grep cisco
cisco-vem-v150-esx 4.2.1.2.1.0-3.0.1 Cisco PartnerSupported 2012-10-09
```

**Step 5** Check that the VEM agent is running.

```
~ # vem status -v
Package vssnet-esxmn-ga-release
Version 4.2.1.2.1.0-3.0.1
Build 5
Date Thu Jul 28 01:37:10 PDT 2011
Number of PassThru NICs are 0
VEM modules are loaded
Switch Name      Num Ports  Used Ports  Configured Ports  MTU      Uplinks
vSwitch0         128        4           128              1500     vmnic4
Number of PassThru NICs are 0
VEM Agent (vemdpa) is running
```

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

```
~ # vemcmd show version
VEM Version: 4.2.1.2.1.0-3.0.1
VSM Version:
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```



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

```
~ # vem version -v
```

```
Number of PassThru NICs are 0
```

```
Running esx version -441354 x86_64
```

```
VEM Version: 4.2.1.2.1.0-3.0.1
```

```
VSM Version:
```

```
System Version: VMware ESXi 5.0.0 Releasebuild-441354
```

**Step 8** Add the host to the DVS by using the vCenter Server.**Step 9** On the VSM, verify that the VEM software has been installed.

```
switch# show module
```

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

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

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

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

## Installing the VEM Software on a Stateless ESXi Host Using VUM

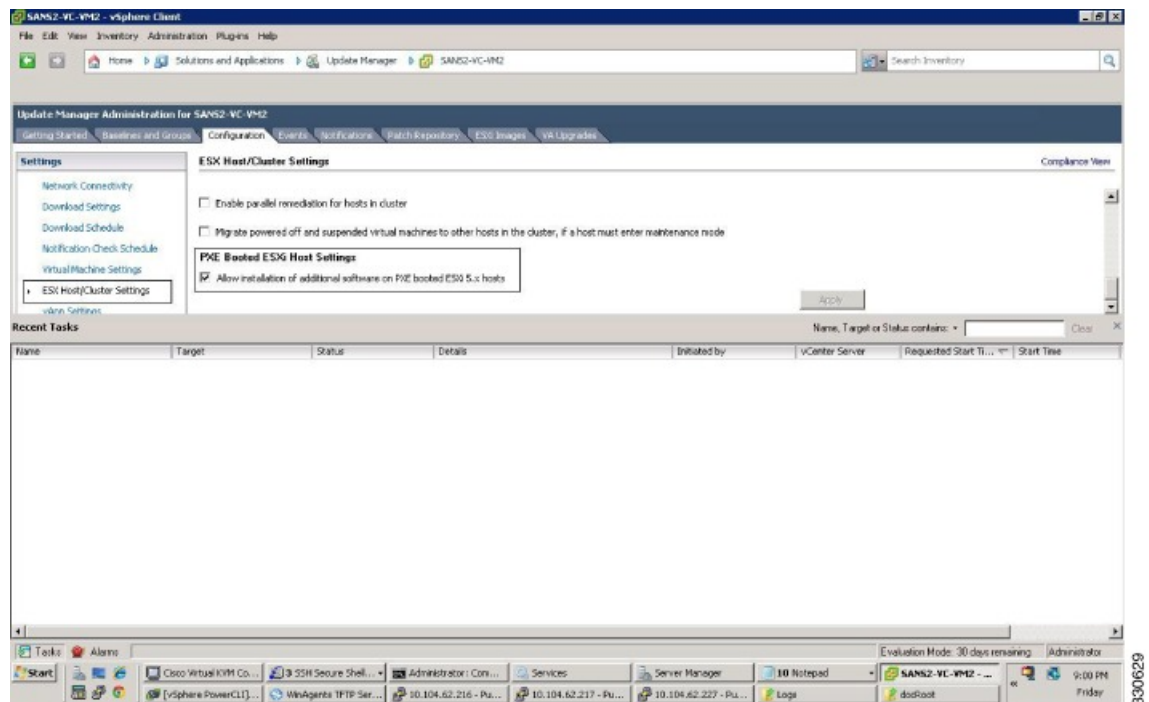
### Before You Begin

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

## Procedure

- Step 1** In the vCenter Server, choose **Home > Update Manager > Configuration > ESX host/Cluster** settings.
- Step 2** Check the **PXE Booted ESXi Host Settings** check box.

**Figure 75: ESX Host/Cluster Settings Window**



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

# 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 maintenance 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(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV2(1.1)

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 the [Upgrade Paths](#).

## Migrating from Layer 2 to Layer 3

### Layer 3 Advantages

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

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

- If the management VMKernel (vmk0) is used as the Layer 3 control interface in the VEM, there is no need for another IP address because the host's management IP address is used for VSM-VEM Layer 3 connectivity.

**Note**

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

## 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 vmknix 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
<b>Step 1</b>	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
<b>Step 1</b>	Rename the Extract.csv file to Convert.csv	The migration tool will retrieve the data from the Convert.csv file.
<b>Step 2</b>	Populate your Convert.csv file (in C:\Windows\Temp) with the vmknics IP address and netmask.	
<b>Step 3</b>	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.

- 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
```
- 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.

- 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 interfaces 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 147](#).
  - 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 svcs mode from Layer 2 to Layer 3 with the mgmt0 interface as the Layer 3 control interface.
- ```
switch(config-svs-domain) # svcs 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 **svcs mode l3 interface control0** command:
- Step 4** Restore the VSM to vCenter Server connection.
- ```
switch(config) # svcs connection toVC
switch(config-svs-conn) # connect
switch(config-svs-conn) # end
```
- Note** After entering the **svcs 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 svcs 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 4.0 to VMware Release 4.1 Upgrade, page 151](#)
- [VMware Release 4.0/4.1/5.0 to VMware Release 5.1 Upgrade, page 158](#)
- [Upgrading to VMware ESXi 5.0 Patch 01, page 164](#)
- [Installing ESXi 5.1 Host Software Using the CLI, page 165](#)
- [Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image, page 168](#)

## VMware Release 4.0 to VMware Release 4.1 Upgrade

### Upgrading from VMware Release 4.0 to VMware Release 4.1

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

#### Before You Begin

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

## Procedure

---

- Step 1** [Upgrading the vCenter Server to VMware Release 4.1, on page 152](#)
  - Step 2** [Upgrading the vCenter Update Manager to VMware Release 4.1, on page 153](#)
  - Step 3** [Upgrading the ESX/ESXi Hosts to VMware Release 4.1, on page 154](#)
  - Step 4** [Verifying the Upgrade to Release 4.1, on page 157](#)
- 

## Upgrading the vCenter Server to VMware Release 4.1

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

## Procedure

---

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



The **VMware vCenter Installer** wizard opens.

- Step 3** In the **VMware Product Installers** area, click **vCenter Server**.
  - Step 4** Choose a language and click **OK**.
  - Step 5** Click **Next**.
  - Step 6** In the **Patent Agreement** window, click **Next**.
  - Step 7** In the **License Agreement** screen, click the **I agree to the terms in the license agreement** radio button and click **Next**.
  - Step 8** In the **Database Options** window, click **Next**.
  - Step 9** Click the **Upgrade existing vCenter Server database** radio button and check the **I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\**, check box.
  - Step 10** From the **Windows Start Menu**, click **Run**.
  - Step 11** Enter the name of the folder that contains the vCenter Server database and click **OK**.
  - Step 12** Drag a copy of the parent folder (SSL) to your Desktop as a backup.
  - Step 13** Return to the installer program and click **Next**.
  - Step 14** In the **vCenter Agent Upgrade** screen, click the **Automatic** radio button and click **Next**.
  - Step 15** In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box and click **Next**.
  - Step 16** In the **Configure Ports** screen, review the port settings and click **Next**.
  - Step 17** Based on the number of hosts, in the **vCenter Server JVM Memory** screen click the appropriate **memory** radio button and click **Next**.
  - Step 18** In the **Ready to Install the Program** screen, click **Install**.
  - Step 19** In the **Installation Completed** screen, click **Finish**.
  - Step 20** Upgrade the VMware vSphere Client to ESXi 4.1.0.
  - Step 21** Open the VMware vSphere Client.
  - Step 22** From the **Help** menu, choose **About VMware vSphere**.
  - Step 23** Confirm that the vSphere Client and the VMware vCenter Server are both version 4.1.0, Build 258902, click **OK**, and exit the VMware vSphere Client.
- 

### What to Do Next

Complete the steps in [Upgrading the vCenter Update Manager to VMware Release 4.1](#), on page 153.

## Upgrading the vCenter Update Manager to VMware Release 4.1

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

## Procedure

---

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

## What to Do Next

Complete the steps in [Upgrading the ESX/ESXi Hosts to VMware Release 4.1](#), on page 154.

## Upgrading the ESX/ESXi Hosts to VMware Release 4.1

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

## Procedure

---

- Step 1** In the vSphere Client, click **Home**.
- Step 2** Click the **Update Manager** tab.
- Step 3** Click the **Host Upgrade Release** tab.
- Step 4** In the **Imported Upgrade Releases** area, click **Import Upgrade Release**.
- Step 5** In the **Select Upgrade Files** screen, click **Browse** and navigate to the location of the upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip Zip bundle.
- Step 6** Choose the zip file and click **Open**.
- Step 7** In the **Select Upgrade Files** screen, click **Next**.  
If you receive a Security Warning about the certificate, you can install the certificate or ignore the warning. Go to Step 8 if you must install a certificate. If you do not need to install a certificate, go to Step 9.
- Step 8** Click **Finish** when the upload is successful.
- Step 9** In the **Host Upgrade Releases** tab, click **Create Baseline** to create a baseline.  
When you create a baseline and attach it to a host or cluster, the Update Manager can remediate the device by applying all updates needed to bring it into compliance with the baseline.
- Step 10** In the **Baseline Name and Description** area, enter a Name.
- Step 11** In the **Baseline Type** area, click the **Host Upgrade** radio button and click **Next**.
- Step 12** Click the **Host Upgrade Release** and click **Next**.
- Step 13** Click **Next**.
- Step 14** Check the **Try to reboot the host and roll back the upgrade in case of failure** check box.
- Step 15** In the **COS VMDK Location** screen, click **Next**.
- Step 16** Review the upgrade information and click **Finish**.

The baseline has been created.

- Step 17** Click **Home**.
- Step 18** Click the **Host and Cluster Inventory** tab.
- Step 19** Click the **Cluster** icon to upgrade all hosts in the cluster.
- Step 20** Click the **Update Manager** tab.
- Step 21** In the **Cluster** area, click **Attach**.
- Step 22** In the **Individual Baselines by Type** pane, check the **4.0 to 4.1** check box.
- Step 23** Click **Attach**.
- Step 24** In the **Cluster** area, click **Scan** to test the cluster's compliance to the baseline.
- Step 25** In the **Confirm Scan** window, check the **Upgrades** check box.
- Step 26** Uncheck the **Patches and Extensions** check box.
- Step 27** Click **Scan**.
- Step 28** In the **Host Compliance** pane, verify that all hosts are Non-Compliant and click **Remediate**.
- Step 29** In the **Remediation Selection** screen, click **Next**.
- Step 30** Click the **I agree to the term in the license agreement** radio button and click **Next**.
- Step 31** In the **ESX 4.1.0 Upgrade** window, click **Next**.
- Step 32** In the **Maintenance Mode Options** area, check the **Disable any removable media devices connected to the virtual machines on the host** check box and click **Next**.
- Step 33** In the **Cluster Remediation Options** screen, check all check boxes and click **Next**.
- Step 34** Click **Finish** to begin the remediation.
  - Note** You can monitor the remediation progress in the **Recent Tasks** section of the **vSphere Server** window.
- Step 35** In the **Confirming Host ESX/ESXi Release** window, click each host in the left-hand pane to check the host versions and confirm that 4.1.0, 260247 appears in the top-left corner of the right-hand pane.
- Step 36** Determine upgrade completion as follows:
  - a) If all hosts have been upgraded, the upgrade is complete.
  - b) If any one of the hosts was not upgraded, perform Step 42 through Step 61 for each host that requires an upgrade.
- Step 37** Right-click the host's IP address and choose **Enter Maintenance Mode**.
- Step 38** In the **Confirm Maintenance Mode** dialog box, click **Yes**.

The host's VMs are migrated.

- Step 39** Click the **Update Manager** tab.
  - Step 40** In the **Attached Baselines** section, right-click the **4.0 to 4.1** baseline.
  - Step 41** In the drop-down list, choose **Detach Baseline**.
  - Step 42** In the **Detach Baseline from Cluster** window, check the **Cluster** check box and click **Detach**.
  - Step 43** In the **Update Manager - Attach Baseline** window, click **Attach** to attach the baseline to the host that did not upgrade.
  - Step 44** In the **Individual Baselines by Type** pane, check the **4.0 to 4.1** check box and click **Attach**.
  - Step 45** In the **Host Compliance** pane, verify that all hosts are Non-Compliant and click **Remediate**.
  - Step 46** In the **Remediation Selection** pane, click **Next**.
  - Step 47** Click the **I agree to the term in the license agreement** radio button.
  - Step 48** Click **Next**.
  - Step 49** In the **ESX 4.1.0 Upgrade** window, click **Next**.
  - Step 50** In the **Maintenance Mode Options** area, check the **Disable any removable media devices connected to the virtual machines on the host** check box.
  - Step 51** Click **Next**.
  - Step 52** In the **Cluster Remediation Options** screen, check all check boxes.
  - Step 53** Click **Next**.
  - Step 54** In the **Ready to Complete** screen, click **Finish** to begin the remediation.
  - Step 55** When the remediation is complete, confirm that the host is compliant in the Host Compliance section.
  - Step 56** In the left-hand pane of the **Exit Maintenance Mode** window, right-click on the host and choose **Exit Maintenance Mode**.
  - Step 57** In the left-hand pane of the **Select Cluster** window, choose **Cluster** to scan the entire cluster for compliance.
  - Step 58** Detach the baseline from the host and attach it to the cluster.
- Note** You can also confirm the upgrade by entering the show module command on the VSM and check that the VEMs are on the correct build.

---

The upgrade is complete.

### What to Do Next

Complete the steps in [Verifying the Upgrade to Release 4.1](#), on page 157.

## Verifying the Upgrade to Release 4.1

### Procedure

---

- Step 1** Verify the build number on the ESX host by entering the following command:  

```
[root@hostname~] # rpm -qa | grep vmkernel | awk -F. '{print $5}'
260247
```
- Step 2** Verify the build number on the ESXi host by entering the following command:  

```
~ # vmware -v
VMware ESXi 4.1.0 build-260247
```

**Step 3** Verify the upgrade on the Cisco Nexus 1000V by entering the following commands.

```
switch# show module
```

a) Enter the following command on the VSM:

```
switch# show module
```

b) Enter the following commands on the VEM:

```
~ # vem status
```

```
~ # vemcmd show card
```

# VMware Release 4.0/4.1/5.0 to VMware Release 5.1 Upgrade

## Upgrading from VMware Releases 4.0/4.1/5.0 to VMware Release 5.1

The steps to upgrade from VMware Releases 4.0/4.1/5.0 to VMware Release 5.1 are as follows:

### Procedure

- Step 1** [Upgrading the vCenter Server to Release 5.1, on page 123](#)
- Step 2** [Upgrading the vCenter Update Manager to Release 5.1, on page 160](#)
- Step 3** [Augmenting the Customized ISO for VMware Release 5.1, on page 161](#)
- Step 4** [Upgrading the ESXi Hosts to Release 5.1, on page 161](#)
- Step 5** [Verifying the Build Number and Upgrade, on page 163](#)

## Upgrading the vCenter Server to Release 5.1



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

### Before You Begin

- Download the upgrade ISO file that contains the ESXi 5.1 image and the Cisco Nexus 1000V Release 4.2(1)SV1(5.2) 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 5.1 installation file.

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

- Step 2** Double-click **autorun**.
  - Step 3** In the **VMware vCenter Installer** window, click **vCenter Server**.
  - Step 4** Click **Install**.
  - Step 5** Choose a language and click **OK**.
  - Step 6** Click **Next**.
  - Step 7** In the Patent Agreement window, click **Next**.
  - Step 8** In the **License Agreement** window, click the **I agree to the terms in the license agreement** radio button.
  - Step 9** Click **Next**.
  - Step 10** In the **Database Options** screen, click **Next**.
  - Step 11** Click the **Upgrade existing vCenter Server database** radio button and check the **I have taken a backup of the existing vCenter Server database and SSL certificates in the folder: C:\ProgramData\VMware\VMware VirtualCenter\SSL\** check box.
  - Step 12** From the **Windows Start Menu**, click **Run**.
  - Step 13** Enter the name of the folder that contains the vCenter Server database and click **OK**.
  - Step 14** Drag a copy of the parent folder (SSL) to the desktop as a backup.
  - Step 15** Return to the installer program.
  - Step 16** Click **Next**.
  - Step 17** In the vCenter Agent Upgrade window, click the **Automatic** radio button.
  - Step 18** Click **Next**.
  - Step 19** In the **vCenter Server Service** screen, check the **Use SYSTEM Account** check box.
  - Step 20** Click **Next**.
  - Step 21** Review the port settings and click **Next**.
  - Step 22** In the **vCenter Server JVM Memory** screen based on the number of hosts, click the appropriate memory radio button.
  - Step 23** Click **Next**.
  - Step 24** Click **Install**.
  - Step 25** Click **Finish**.  
This step completes the upgrade of the vCenter Server.
  - Step 26** Upgrade the VMware vSphere Client to ESXi 5.1.
  - Step 27** Open the VMware vSphere Client.
  - Step 28** From the **Help** menu, choose **About VMware vSphere**.
  - Step 29** Confirm that the vSphere Client and the VMware vCenter Server are both version VMware 5.1.
  - Step 30** Click **OK**, and exit the VMware vSphere Client.
- 

### What to Do Next

Complete the steps in [Upgrading the vCenter Update Manager to Release 5.1](#), on page 160.

## Upgrading the vCenter Update Manager to Release 5.1

**Note**

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

**Before You Begin**

You have upgraded the vCenter Server to VMware ESXi 5.1.

**Procedure**

- Step 1** On the local drive, double-click **VMware-UpdateManager**.
- Step 2** Choose a language and click **OK**.  
The Update Manager Installer opens.
- Step 3** Click **OK** to upgrade to 5.1.
- Step 4** Click **Next** to begin.
- Step 5** Click **Next** at the Patent Agreement.
- Step 6** Click the **I agree to the terms in the license agreement** radio button.
- Step 7** Click **Next**.
- Step 8** In the **VMware vCenter Server Information** area, verify the IP address and username.
- Step 9** In the **Password** field, enter your password.
- Step 10** Click **Next**.
- Step 11** Click **Next**.
- Step 12** Click the **Yes, I want to upgrade my Update Manager database** radio button.
- Step 13** Click **Next**.
- Step 14** Verify the Update Manager port settings.
- Step 15** Click **Next**.
- Step 16** Verify the proxy settings.
- Step 17** Click **Next**.
- Step 18** Click **Install** to begin the upgrade.
- Step 19** Click **OK** to acknowledge that a reboot will be required to complete the setup.



During the upgrade, the vSphere Client is disconnected.

- Step 20** Click **Cancel** for the attempt to reconnect.
  - Step 21** Click **OK** in the **Server Connection Invalid** dialog box.
  - Step 22** Click **Finish**.
  - Step 23** Reboot the VUM/vCenter Server.
  - Step 24** In the **Shut Down Windows** dialog box from the **Option** drop-down list, choose **Other (Planned)**, enter a value in the **comment** field, and click **OK**.
  - Step 25** After the system has rebooted, browse to the C:\ProgramData\VMware\VMware Update Manager\Logs\ folder.
  - Step 26** Open the vmware-vum-server-log4cpp file.
  - Step 27** From the **VMware vCenter Server's Plug-in** menu, choose **Manage Plug-ins**.
  - Step 28** Under **Available Plug-ins**, click **Download and Install** for VMware vSphere Update Manager Extension.
- 

### What to Do Next

Complete the steps in [Augmenting the Customized ISO for VMware Release 5.1](#), on page 161.

## Augmenting the Customized ISO for VMware Release 5.1

### Before You Begin

If you are using a QLogic NIC, download the driver to include in the customized ISO for that specific NIC.

### Procedure

If the ESXi host that is being upgraded to VMware 5.1 needs any Async drivers that are not already in VMware 5.1, see the respective vendor's documentation for the drivers and the procedure to update the customized ISO.

### What to Do Next

Complete the steps in [Upgrading the ESXi Hosts to Release 5.1](#), on page 161.

## Upgrading the ESXi Hosts to Release 5.1



### Note

- This upgrade procedure also applies to ESXi hosts 5.0 and 5.0 Update 1 and later.
  - If you have multiple vmkernel interfaces on the same subnet when upgrading to ESXi 5.1, you must place your management vmkernel interface into the Layer 3 capable port profile.
-

## Procedure

---

- Step 1** In the vSphere Client, click **Home**.
- Step 2** Click the **Update Manager** tab.
- Step 3** Click the **ESXi Image** tab.
- Step 4** Click the **Import ESXi Image** link in the **ESXi Image** window.
- Step 5** Click the **Browse** button and navigate to the customized upgrade ISO image.
- Step 6** Choose the upgrade file and click **Open**.
- Step 7** To import the ISO file, click **Next**.
- Step 8** When the upgrade ISO file is uploaded, click **Next**.
- Step 9** In the **Baseline Name and Description** area, enter a name for the baseline and an optional description.
- Step 10** Click **Finish**.
- Step 11** In the vSphere Client, choose **Home > Hosts and Clusters**.
- Step 12** In the **left-hand** pane, select the host or cluster to upgrade and click the **Update Manager** tab.
- Step 13** Click **Attach**.
- Step 14** In the **Individual Baselines by Type** area, check your upgrade baseline's check box.
- Step 15** Click **Attach**.
- Step 16** Click **Scan**.  
After the scan, the baseline will display non-compliant.
- Step 17** In the **Confirm Scan** dialog box, check the **Upgrades** check box and click **Scan**.
- Step 18** In the **Upgrade Details** window, if the Compliance State has a value of Incompatible, reboot the host with the baseline attached.

After the reboot, the Compliance State will have a value of Non-Compliant.

- Step 19** When you are finished viewing the upgrade details, click **Close**.
- Step 20** Verify that all hosts are Non-Compliant.
- Step 21** Click **Remediate**.
- Step 22** Click **Next**.
- Step 23** In the **End User License Agreement** screen, check the **I accept the terms and license agreement** check box.
- Step 24** Click **Next**.
- Step 25** In the **ESXi 5.x Upgrade** window, click **Next**.
- Step 26** Click **Next**.
- Step 27** In the **Maintenance Mode Options** area, check the **Disable any removable media devices connected to the virtual machines on the host** check box.
- Step 28** Click **Next**.
- Step 29** In the **Cluster Remediation Options** window, check all check boxes.
- Step 30** Click **Next**.
- Step 31** Click **Finish** to begin the remediation.
- Step 32** To check the host versions, click each host in the left-hand pane and confirm that 5.1 appears in the top-left corner of the right-hand pane and that the version information matches the contents of the *Cisco Nexus 1000V and VMware Compatibility Information*.
- Step 33** The upgrade can also be confirmed by running the **show module** command on the VSM and observing that the VEMs are on the correct build.

---

The upgrade is complete.

### What to Do Next

Complete the steps in [Verifying the Build Number and Upgrade](#), on page 163.

## Verifying the Build Number and Upgrade

### Before You Begin

- You have upgraded the VSMs and VEMs to the current Cisco Nexus 1000V release.
- You have upgraded the vCenter Server to VMware Release 5.0.0.
- You have upgraded the VMware Update Manager to VMware Release 5.0.0.
- You have upgraded your ESX/ESXi hosts to VMware Release 5.0.0.

### Procedure

---

- Step 1** Verify the build number on the ESXi host.

```
~ # vmware -v
VMware ESXi 5.0.0 build-469512
```

**Step 2** Verify the upgrade on the Cisco Nexus 1000V.

```
switch# show module
```

```
N1KV-VSM# show mod
```

| Mod | Ports | Module-Type               | Model      | Status     |
|-----|-------|---------------------------|------------|------------|
| 1   | 0     | Virtual Supervisor Module | Nexus1000V | active *   |
| 2   | 0     | Virtual Supervisor Module | Nexus1000V | ha-standby |
| 3   | 248   | Virtual Ethernet Module   | NA         | ok         |

| Mod | Sw             | Hw  |
|-----|----------------|-----|
| 1   | 4.2(1)SV2(2.1) | 0.0 |
| 2   | 4.2(1)SV2(2.1) | 0.0 |
| 3   | 4.2(1)SV2(2.1) | 3.0 |

| Mod | MAC-Address(es)                        | Serial-Num |
|-----|----------------------------------------|------------|
| 1   | 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 | NA         |
| 2   | 00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8 | NA         |
| 3   | 02-00-0c-00-09-00 to 02-00-0c-00-09-80 | NA         |

| Mod | Server-IP      | Server-UUID                          | Server-Name           |
|-----|----------------|--------------------------------------|-----------------------|
| 1   | 10.104.245.152 | NA                                   | NA                    |
| 2   | 10.104.245.152 | NA                                   | NA                    |
| 3   | 10.104.245.140 | 42064d20-4e52-62d1-e0ee-0b14be4388d6 | mn-esxi-5.0-statefull |

\* this terminal session

The upgrade to VMware Release 5.0 is complete.

## Upgrading to VMware ESXi 5.0 Patch 01

### Upgrading a VMware ESXi 5.0 Stateful Host to VMware ESXi 5.0 Patch 01

#### Procedure

**Step 1** Copy the ESXi 5.0 Patch 01 bundle (ESXi500-201109001.zip) to the host.

**Step 2** Upgrade the host to ESXi 5.0 Patch 01.

```
~ # esxcli software vib update -d /vmfs/volumes/newnfs/MN-patch01/ESXi500-201109001.zip
```

Installation Result

Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.

Reboot Required: true

VIBs Installed: VMware\_bootbank\_esx-base\_5.0.0-0.3.474610,  
VMware\_locker\_tools-light\_5.0.0-0.3.474610

VIBs Removed: VMware\_bootbank\_esx-base\_5.0.0-0.0.469512,  
VMware\_locker\_tools-light\_5.0.0-0.0.469512

VIBs Skipped: VMware\_bootbank\_ata-pata-amd\_0.3.10-3vmw.500.0.0.469512,  
VMware\_bootbank\_ata-pata-atiixp\_0.4.6-3vmw.500.0.0.469512,

---

```
VMware_bootbank_scsi-qla4xxx_5.01.03.2-3vmw.500.0.0.469512,
VMware_bootbank_uhci-usb-uhci_1.0-3vmw.500.0.0.469512
```

---

## Installing ESXi 5.1 Host Software Using the CLI

You can upgrade an ESXi host by installing a VMware patch or update with the compatible Cisco Nexus 1000V VEM software.

### Before You Begin

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



#### Note

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

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

### Procedure

**Step 1** Download the VEM bits and copy them to the local host.

**Step 2** Determine the upgrade method that you want to use.

- If you are using the vCLI, enter the **esxcli** command and install the ESXi and VEM software simultaneously.

**Note** When using the **esxcli software vib install** command, you must log in to each host and enter the command. ESXi 5.1 expects the VIB to be in the `/var/log/vmware` directory if the absolute path is not specified.

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

This example shows how to install ESXi 5.1 on a host.

```
~ # esxcli software vib install -d /var/log/vmware/VEM510-201210150105-BG-release.zip
```

Installation Result

Message: Operation finished successfully.

Reboot Required: false

VIBs Installed: Cisco\_bootbank\_cisco-vem-v150-esx\_4.2.1.2.1.0-3.1.1

VIBs Removed:

VIBs Skipped:

```
~ # esxcli software vib install -v /var/log/vmware/
```

```
Cisco_bootbank_cisco-vem-v150-esx_4.2.1.2.1.0-3.1.1.vib
```

Installation Result

Message: Operation finished successfully.

Reboot Required: false

VIBs Installed: Cisco\_bootbank\_cisco-vem-v150-esx\_4.2.1.2.1.0-3.1.1

VIBs Removed:

VIBs Skipped:

```
~ #
```

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

### Step 3 Verify that the installation was successful.

```
~ # vmware -v -l
```

VMware ESXi 5.1.0 build-799733

VMware ESXi 5.1.0 GA

```
~ #
```

```
~ # vemcmd show version
```

VEM Version: 4.2.1.2.1.0-3.1.1

VSM Version: 4.2(1)SV2(1.1)

System Version: VMware ESXi 5.1.0 Releasebuild-799733

```
~ # vem status -v
```

Package vssnet-esxmn-next-release

Version 4.2.1.2.1.0-3.1.1

Build 2

Date Fri Aug 3 05:11:27 PDT 2012

Number of PassThru NICs are 0

VEM modules are loaded

| Switch Name | Num Ports | Used Ports | Configured Ports | MTU  | Uplinks              |
|-------------|-----------|------------|------------------|------|----------------------|
| vSwitch0    | 128       | 24         | 128              | 1500 | vmnic2               |
| DVS Name    | Num Ports | Used Ports | Configured Ports | MTU  | Uplinks              |
| switch      | 256       | 14         | 256              | 1500 | vmnic5,vmnic4,vmnic3 |

Number of PassThru NICs are 0

**VEM Agent (vemdpa) is running**

```
~ # esxcli software vib list | grep cisco
```

cisco-vem-v150-esx 4.2.1.2.1.0-3.1.1

Cisco PartnerSupported

2012-10-09

```
~ #
```

```

~ # vem version -v
Number of PassThru NICs are 0
Running esx version -799733 x86_64
VEM Version: 4.2.1.2.1.0.194-3.1.1
VSM Version: 4.2(1)SV2(1.1) [build 4.2(1)SV2(1.0.194)]
System Version: VMware ESXi 5.1.0 Releasebuild-799733
~ #

```

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

**Step 4** Verify that the VEM has been upgraded by entering the following command from the VSM.

```

switch# show module

```

| Mod | Ports | Module-Type               | Model      | Status     |
|-----|-------|---------------------------|------------|------------|
| 1   | 0     | Virtual Supervisor Module | Nexus1000V | ha-standby |
| 2   | 0     | Virtual Supervisor Module | Nexus1000V | active *   |
| 3   | 248   | Virtual Ethernet Module   | NA         | ok         |
| 4   | 248   | Virtual Ethernet Module   | NA         | ok         |

| Mod | Sw             | Hw                                                         |
|-----|----------------|------------------------------------------------------------|
| 1   | 4.2(1)SV2(1.1) | 0.0                                                        |
| 2   | 4.2(1)SV2(1.1) | 0.0                                                        |
| 3   | 4.2(1)SV2(1.1) | 4.2(1)SV2(1.1) VMware ESXi 5.1.0 Releasebuild-799733 (3.1) |
| 4   | 4.2(1)SV2(1.1) | 4.2(1)SV2(1.1) VMware ESXi 5.1.0 Releasebuild-799733 (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-00-03-00 to 02-00-0c-00-03-80 | NA         |
| 4   | 02-00-0c-00-04-00 to 02-00-0c-00-04-80 | NA         |

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

\* this terminal session

```
switch#
```

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

**Step 5** Do one of the following:

- If the installation was successful, you do nothing because the installation procedure is complete.
- If not, see the *Recreating the Cisco Nexus 1000V Installation* section in the *Cisco Nexus 1000V Troubleshooting Guide*.

You have completed this procedure.

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

## Before You Begin

- Install the VMware PowerCLI on a Windows platform. For more information, see the *vSphere PowerCLI Installation Guide*.
- On the same Windows platform, where the VMware PowerCLI is installed, do one of the following:
  - Download the ESX depot, which is a .zip file, to a local file path.
  - Download the VEM offline bundle, which is a .zip file, to a local file path.



### Note

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

## Procedure

**Step 1** Start the VMWare PowerCLI application.

**Step 2** Connect to the vCenter Server.

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

**Step 3** Load the ESX depot.

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot c:\vmware-ESXi-5.1.0-depot.zip
```

**Step 4** Display the image profiles.

```
[vSphere PowerCLI] > Get-ESXImageProfile
```

| Name                       | Vendor       | Last Modified   | Acceptance Level |
|----------------------------|--------------|-----------------|------------------|
| ESXi-5.1.0-799733-no-tools | VMware, Inc. | 8/19/2011 1:... | PartnerSupported |
| ESXi-5.1.0-799733-standard | VMware, Inc. | 8/19/2011 1:... | PartnerSupported |

**Step 5** Clone the ESX standard image profile.

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

```
[vSphere PowerCLI] > New-ESXImageProfile -CloneProfile ESXi-5.0.0-469512-standard -Name n1kv-Image
```

| Name       | Vendor       | Last Modified   | Acceptance Level |
|------------|--------------|-----------------|------------------|
| n1kv-Image | VMware, Inc. | 8/19/2011 1:... | PartnerSupported |

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

```
[vSphere PowerCLI] > Add-ESXSoftwareDepot C:\VEM510-201210150105-BG-release.zip
```

Depot Url



```
-----
zip:C:\Users\Administrator\Documents\ VEM510-201210150105-BG-release.zip?in...
```

**Step 7** Confirm that the nlkv-vib package is loaded.

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

| Name               | Version           | Vendor | Release Date |
|--------------------|-------------------|--------|--------------|
| cisco-vem-v150-esx | 4.2.1.2.1.0-3.0.1 | Cisco  | 1/21/2012... |

**Step 8** Bundle the nlkv-package into the cloned image profile.

```
[vSphere PowerCLI] > Add-ExsSoftwarePackage -ImageProfile nlkv-Image -SoftwarePackage
cisco-vem-v140-esx
```

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

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

```
[vSphere PowerCLI]> $img = Get-ExsImageProfile nlkv-Image
```

```
[vSphere PowerCLI]> $img.vibList
```

| Name                 | Version                        | Vendor | Release Date |
|----------------------|--------------------------------|--------|--------------|
| net-ixgbe            | 2.0.84.8.2-10vmw.500.0.0.46... | VMware | 8/19/2011... |
| ata-pata-hpt3x2n     | 0.3.4-3vmw.500.0.0.469512      | VMware | 8/19/2011... |
| ehci-ehci-hcd        | 1.0-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| ata-pata-atiixp      | 0.4.6-3vmw.500.0.0.469512      | VMware | 8/19/2011... |
| scsi-megaraid2       | 2.00.4-9vmw.500.0.0.469512     | VMware | 8/19/2011... |
| uhci-usb-uhci        | 1.0-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| net-r8168            | 8.013.00-3vmw.500.0.0.469512   | VMware | 8/19/2011... |
| ohci-usb-ohci        | 1.0-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| scsi-qla4xxx         | 5.01.03.2-3vmw.500.0.0.469512  | VMware | 8/19/2011... |
| ata-pata-sil680      | 0.4.8-3vmw.500.0.0.469512      | VMware | 8/19/2011... |
| scsi-megaraid-sas    | 4.32-1vmw.500.0.0.469512       | VMware | 8/19/2011... |
| scsi-aic79xx         | 3.1-5vmw.500.0.0.469512        | VMware | 8/19/2011... |
| ata-pata-amd         | 0.3.10-3vmw.500.0.0.469512     | VMware | 8/19/2011... |
| net-bnx2             | 2.0.15g.v50.11-5vmw.500.0.0... | VMware | 8/19/2011... |
| misc-drivers         | 5.0.0-0.0.469512               | VMware | 8/19/2011... |
| sata-ahci            | 3.0-6vmw.500.0.0.469512        | VMware | 8/19/2011... |
| scsi-fnic            | 1.5.0.3-1vmw.500.0.0.469512    | VMware | 8/19/2011... |
| ata-pata-pdc2027x    | 1.0-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| scsi-hpsa            | 5.0.0-17vmw.500.0.0.469512     | VMware | 8/19/2011... |
| sata-sata-sil        | 2.3-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| net-igb              | 2.1.11.1-3vmw.500.0.0.469512   | VMware | 8/19/2011... |
| net-e1000e           | 1.1.2-3vmw.500.0.0.469512      | VMware | 8/19/2011... |
| net-forcedeth        | 0.61-2vmw.500.0.0.469512       | VMware | 8/19/2011... |
| sata-ata-piix        | 2.12-4vmw.500.0.0.469512       | VMware | 8/19/2011... |
| scsi-qla2xxx         | 901.k1.1-14vmw.500.0.0.469512  | VMware | 8/19/2011... |
| scsi-adp94xx         | 1.0.8.12-6vmw.500.0.0.469512   | VMware | 8/19/2011... |
| net-sky2             | 1.20-2vmw.500.0.0.469512       | VMware | 8/19/2011... |
| cisco-vem-v150-esx   | 4.2.1.2.1.0-3.0.1              | Cisco  | 1/21/2012... |
| ipmi-ipmi-msghandler | 39.1-4vmw.500.0.0.469512       | VMware | 8/19/2011... |
| net-be2net           | 4.0.88.0-1vmw.500.0.0.469512   | VMware | 8/19/2011... |
| esx-base             | 5.0.0-0.0.469512               | VMware | 8/19/2011... |
| ipmi-ipmi-si-drv     | 39.1-4vmw.500.0.0.469512       | VMware | 8/19/2011... |
| scsi-megaraid-mbox   | 2.20.5.1-6vmw.500.0.0.469512   | VMware | 8/19/2011... |
| net-nx-nic           | 4.0.557-3vmw.500.0.0.469512    | VMware | 8/19/2011... |

|                      |                                |        |              |
|----------------------|--------------------------------|--------|--------------|
| sata-sata-promise    | 2.12-3vmw.500.0.0.469512       | VMware | 8/19/2011... |
| scsi-ips             | 7.12.05-4vmw.500.0.0.469512    | VMware | 8/19/2011... |
| scsi-lpfc820         | 8.2.2.1-18vmw.500.0.0.469512   | VMware | 8/19/2011... |
| ata-pata-cmd64x      | 0.2.5-3vmw.500.0.0.469512      | VMware | 8/19/2011... |
| sata-sata-svw        | 2.3-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| ata-pata-via         | 0.3.3-2vmw.500.0.0.469512      | VMware | 8/19/2011... |
| esx-tboot            | 5.0.0-0.0.469512               | VMware | 8/19/2011... |
| misc-cnric-register  | 1.1-1vmw.500.0.0.469512        | VMware | 8/19/2011... |
| net-s2io             | 2.1.4.13427-3vmw.500.0.0.46... | VMware | 8/19/2011... |
| net-el000            | 8.0.3.1-2vmw.500.0.0.469512    | VMware | 8/19/2011... |
| block-cciss          | 3.6.14-10vmw.500.0.0.469512    | VMware | 8/19/2011... |
| net-enic             | 1.4.2.15a-1vmw.500.0.0.469512  | VMware | 8/19/2011... |
| net-bnx2x            | 1.61.15.v50.1-1vmw.500.0.0.... | VMware | 8/19/2011... |
| scsi-mpt2sas         | 06.00.00.00-5vmw.500.0.0.46... | VMware | 8/19/2011... |
| sata-sata-nv         | 3.5-3vmw.500.0.0.469512        | VMware | 8/19/2011... |
| ata-pata-serverworks | 0.4.3-3vmw.500.0.0.469512      | VMware | 8/19/2011... |
| net-cnric            | 1.10.2j.v50.7-2vmw.500.0.0.... | VMware | 8/19/2011... |
| scsi-mptsas          | 4.23.01.00-5vmw.500.0.0.469512 | VMware | 8/19/2011... |
| scsi-aacraid         | 1.1.5.1-9vmw.500.0.0.469512    | VMware | 8/19/2011... |
| tools-light          | 5.0.0-0.0.469512               | VMware | 8/19/2011... |
| ima-qla4xxx          | 2.01.07-1vmw.500.0.0.469512    | VMware | 8/19/2011... |
| ipmi-ipmi-devintf    | 39.1-4vmw.500.0.0.469512       | VMware | 8/19/2011... |
| net-tg3              | 3.110h.v50.4-4vmw.500.0.0.4... | VMware | 8/19/2011... |
| scsi-bnx2i           | 1.9.1d.v50.1-3vmw.500.0.0.4... | VMware | 8/19/2011... |
| net-r8169            | 6.011.00-2vmw.500.0.0.469512   | VMware | 8/19/2011... |
| scsi-mptspi          | 4.23.01.00-5vmw.500.0.0.469512 | VMware | 8/19/2011... |

**Step 10** Export the image profile to an ISO file.

```
[vSphere PowerCLI]> Export-ESXImageProfile -ImageProfile nlkv-Image -FilePath
C:\nlkv15-esx50.iso -ExportToIso
```



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

---

This chapter contains the following sections:

- [Installing the VSM Software, page 171](#)

## Installing the VSM Software

### Installing the Software from the ISO Image

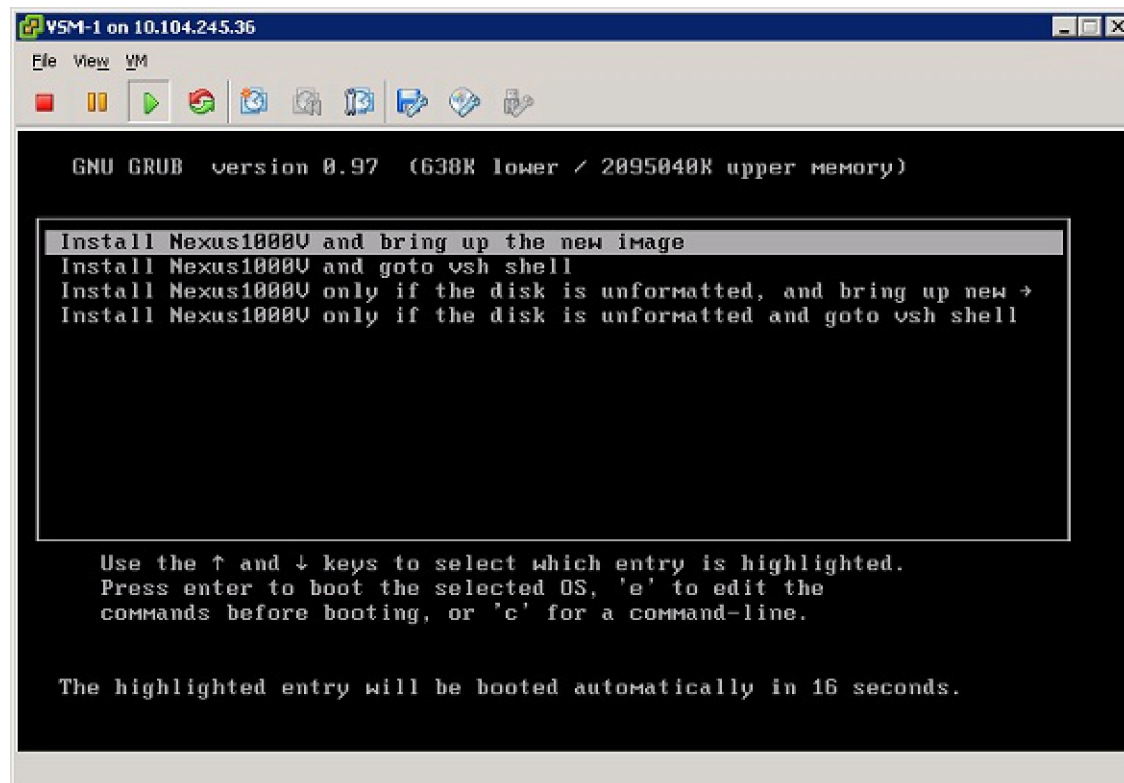
#### Before You Begin

- The ISO image is located at `zip_file_location/Nexus1000v.4.2.1.SV2.1.1/VSM/Install/nexus-1000v.4.2.1.SV2.1.1.iso`
- You have already read the [Prerequisites for Installing the Cisco Nexus 1000V, on page 17](#).
- You have already manually provisioned the VM to be used for the VSM. For more information, see the *vSphere Virtual Machine Administration Guide*.
- The VSM VM requires the following and this procedure includes steps for updating these properties:
  - Minimum of 2 GB of RAM reserved and allocated.
  - Minimum CPU speed of 1500 MHz.
- Do not create more than one virtual CPU. The Cisco Nexus 1000V supports only one virtual CPU.

## Procedure

- Step 1** Using your VMware documentation, attach the VSM ISO image to the virtual CD-ROM and copy the software to a virtual machine (VM).
- Step 2** Make sure that the VSM VM is powered off.
- Step 3** In the **vSphere client Virtual Machine Properties** window **Hardware** tab, choose **Memory**.
- Step 4** In the **Memory Size** field, choose 2 GB.
- Step 5** In the **Resources** tab, choose **Memory**.  
The Resource Allocation settings display in the right-hand pane.
- Step 6** In the **Reservation** field, choose 2048 MB.
- Step 7** In the **Resources** tab, choose CPU.  
The Resource Allocation settings display in the right-hand pane.
- Step 8** In the **Reservation** field, choose 1500 MHz.
- Step 9** Click **OK**.  
The VSM VM memory and CPU speed settings are saved in VMware vSphere Client.
- Step 10** Right-click the VSM and choose **Open Console**.
- Step 11** Choose **Install Nexus1000V and bring up the new image** entry and press **Enter**.

*Figure 76: Install Nexus1000V and Bring Up the New Image Window*

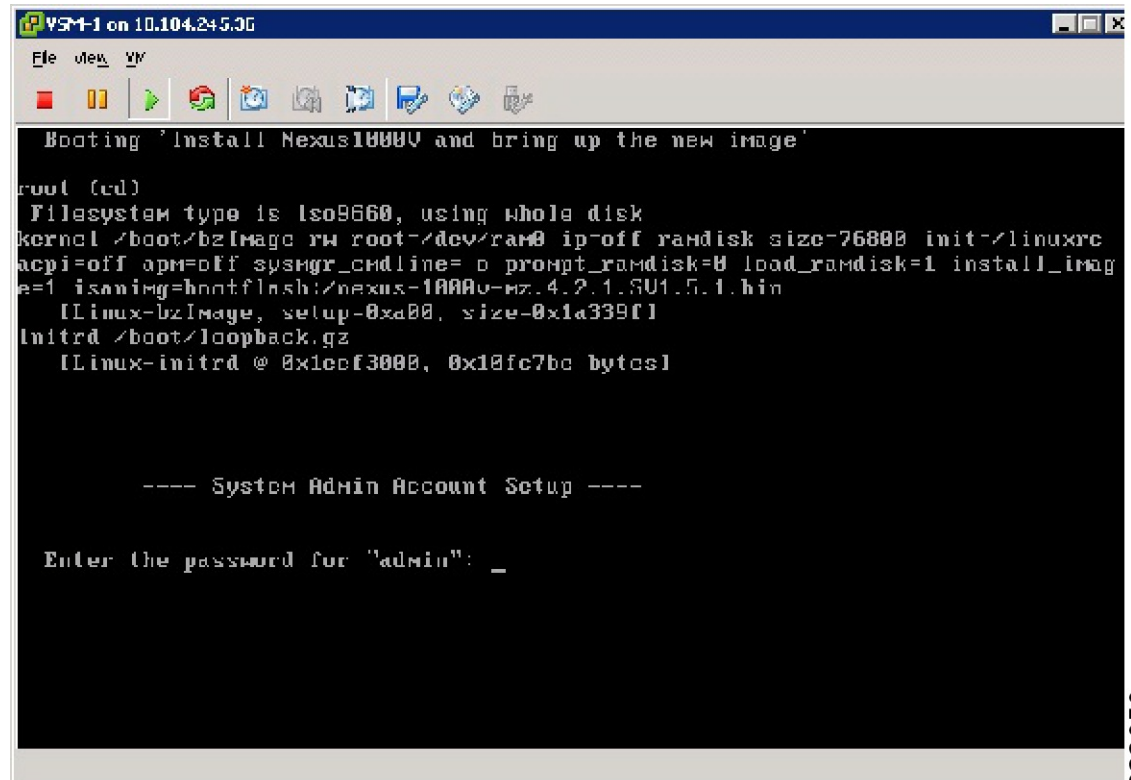


332052

**Step 12** Enter and confirm the Administrator password.

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

**Figure 77: System Admin Account Setup Window**



332050

**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 svcs 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(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

**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
svcs-domain
no control vlan
no packet vlan
svcs 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 187](#).

## Installing the Software from an OVA Image

### Before You Begin

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

- The OVA image is located at `zip_file_location/Nexus1000v.4.2.1.SV2.1.1/VSM/Install/nexus-1000v.4.2.1.SV2.1.1.ova`
- You have already read the [Prerequisites for Installing the Cisco Nexus 1000V, on page 17](#).
- You have a copy of the following Cisco Nexus 1000V software image files on your local drive, depending on the installation type you are using:

| Installation Type | Filename                      | Used with ESX or ESXi Host Software Version |
|-------------------|-------------------------------|---------------------------------------------|
| OVA               | nexus-1000v.4.2.1.SV2.1.1.ova | 4.1 or later                                |

- For detailed information about using the Deploy OVF Template wizard, see the *vSphere Virtual Machine Administration Guide*.
- You have the following information available for creating a VM for the VSM and mapping the required port groups:
  - A name for the new VSM that is unique within the inventory folder and up to 80 characters.
  - The name of the host where the VSM will be installed in the inventory folder.
  - The name of the datastore in which the VM files will be stored.
  - The names of the network port groups used for the VM.
  - The Cisco Nexus 1000V VSM IP address.
- If you are using the OVA file for installation, make sure that you have the following information available for creating and saving an initial configuration file on the VSM:

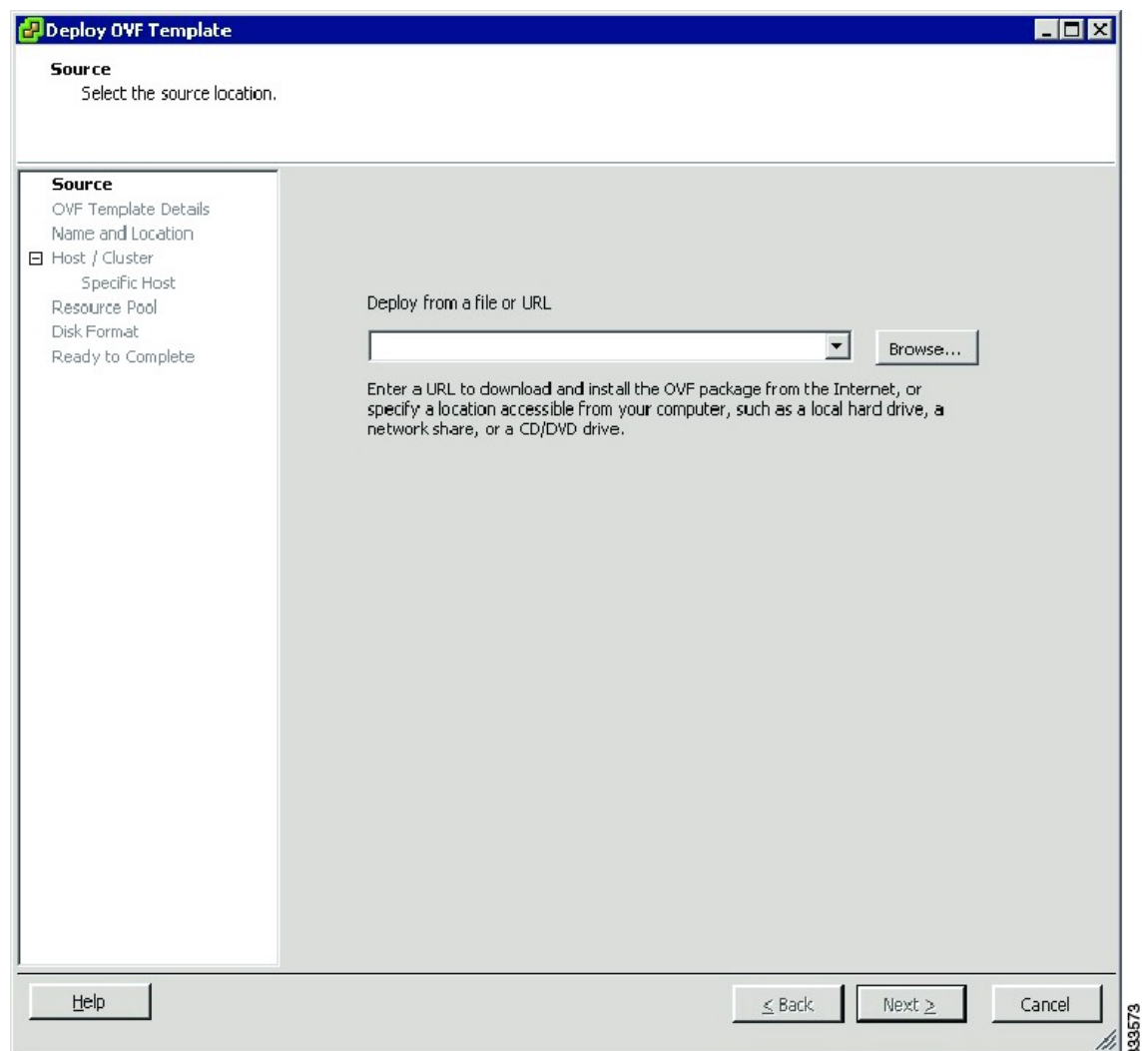


- VSM domain ID
- Admin password
- Management IP address, subnet mask, and gateway

## Procedure

- Step 1** From the vSphere Client, choose **File > Deploy OVF Template**.
- Step 2** In the **Source** screen, specify the location of the OVA file and click **Next**.

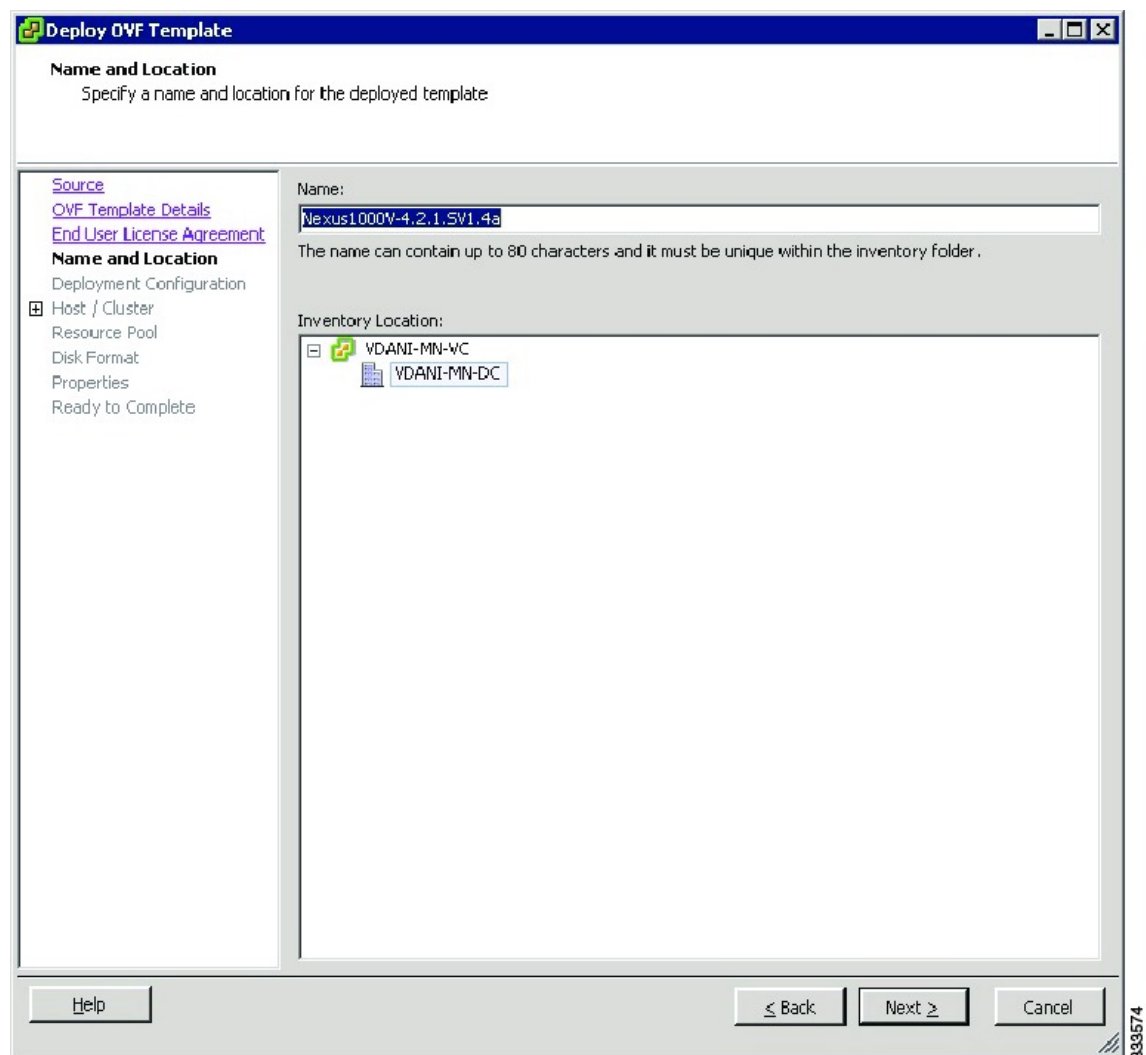
**Figure 78: Source Screen**



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

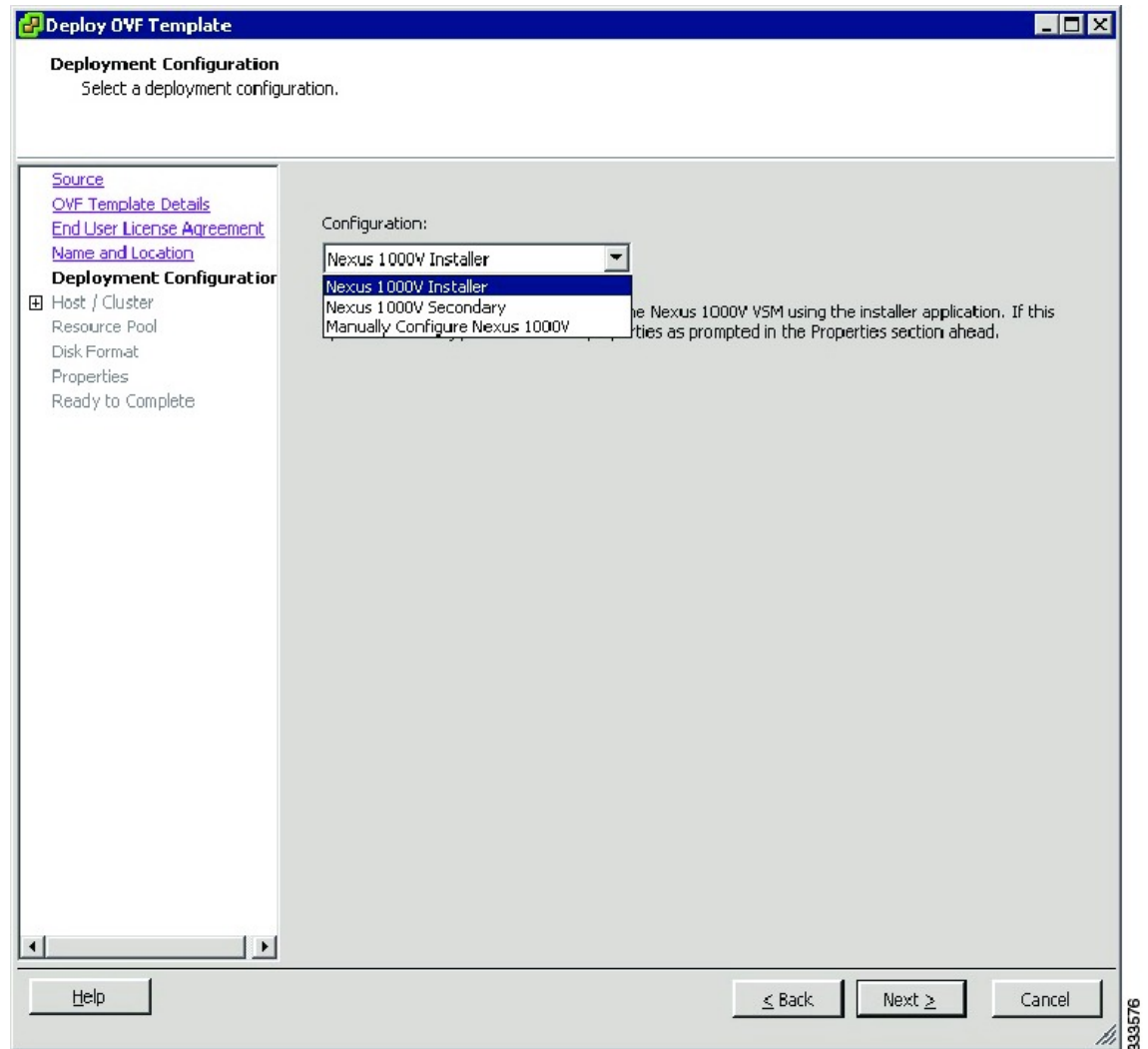
- Step 3** Click **Next**.
- Step 4** Read the Cisco Nexus 1000V License Agreement.
- Step 5** Click **Accept** and then click **Next**.
- Step 6** Add the VSM name, choose the folder location within the inventory where it will reside, and click **Next**. The name for the VSM must be unique within the inventory folder and less than 80 characters.

**Figure 79: Deploy OVF Template Screen**



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

**Figure 80: Deployment Configuration Screen**



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

**Step 8** Click **Next**.

**Step 9** Choose the data center or cluster on which to install the VSM.

**Step 10** Click **Next**

**Step 11** Choose the datastore in which to store the file if one is available.

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

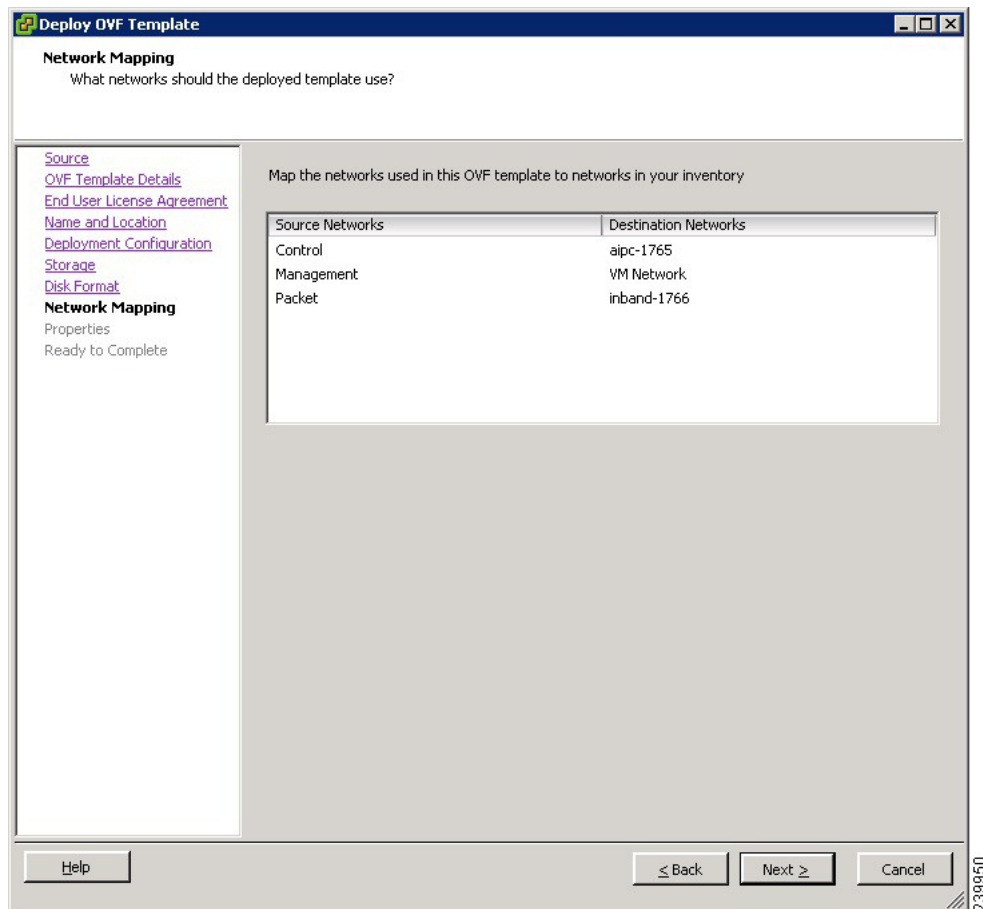
**Step 12** Click **Next**

**Step 13** Choose the Thick provisioned disk format for storing virtual machine virtual disks, and click **Next**.

| Format            | Description                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Thin Provisioned  | The storage is allocated on demand as data is written to the virtual disks.<br><b>Note</b> This disk format is not supported for Cisco Nexus 1000V. |
| Thick Provisioned | All storage is immediately allocated.                                                                                                               |
| Flat Provisioned  | <b>Note</b> This format is only available with VMWare ESXi 5.0.                                                                                     |
| Flat Disk         | All storage for the virtual disk is allocated in advance.                                                                                           |

**Step 14** In the **Network Mapping** screen, choose the networks (the control, management, and packet port groups) that are present in your inventory.

**Figure 81: Network Mapping Screen**



**Step 15** Click **Next****Step 16** Do one of the following:

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

- Admin password (use the same password entered for the primary).

**Figure 82: Properties Screen**

**Deploy OVF Template**

**Properties**  
Customize the software solution for this deployment.

[Source](#)  
[OVF Template Details](#)  
[End User License Agreement](#)  
[Name and Location](#)  
[Deployment Configuration](#)  
[Datastore](#)  
[Network Mapping](#)  
**Properties**  
Ready to Complete

**a. VSM Domain Id**  
**DomainId**  
Enter the Domain Id (1-4095)  
  
Enter an integer value between 1 and 4095.

**b. Nexus 1000V Admin User Password**  
**Password**  
Enter the password.  
Must contain at least one capital, one lowercase, one number.  
  
Enter a string value with 8 to 64 characters.

**c. Management IP Address**  
**ManagementIpV4**  
Enter the VSM Ip in the following form: 192.168.0.10

**d. Management IP Subnet Mask**  
**ManagementIpV4Subnet**  
Enter the Subnet Mask in the following form: 255.255.255.0

**e. Management IP Gateway**  
**GatewayIpV4**  
Enter the gateway in the following form: 192.168.0.1

Not all properties have valid values.  
The vApp will not be able to power on.

≤ Back    Next ≥    Cancel

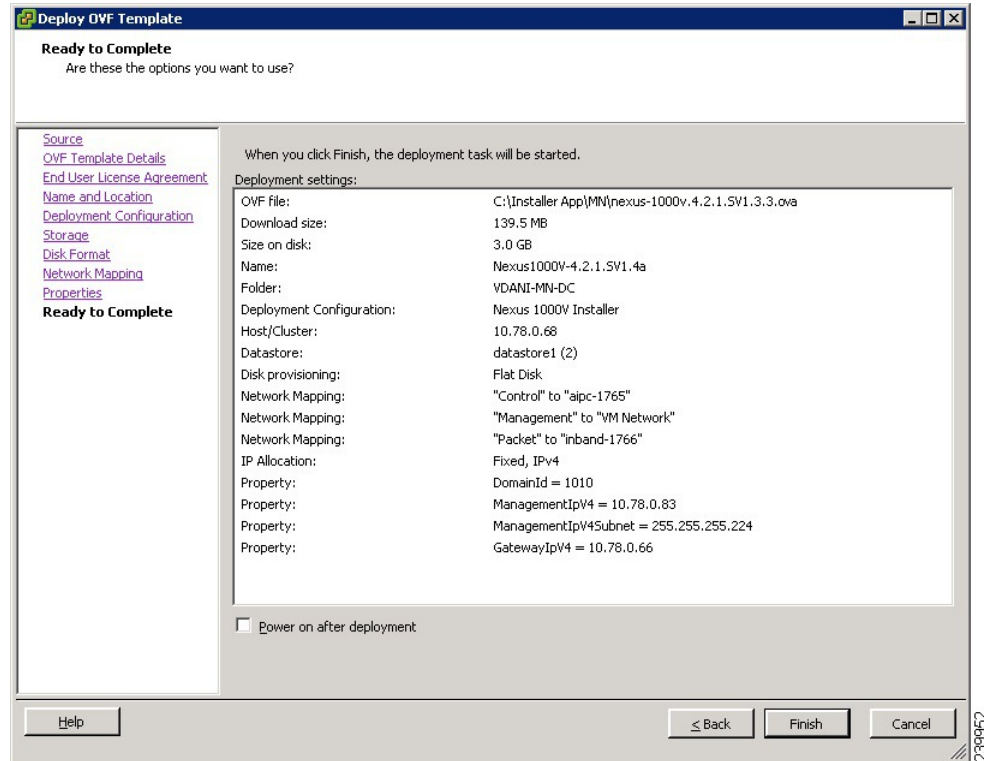
333575

**Step 17** Click **Next**.

**Step 18** If the configuration is correct, click **Finish**.

A status bar displays as the VM installation progresses.

**Figure 83: Ready to Complete Screen**



**Step 19** Click **Close**.

You have completed installing the Cisco Nexus 1000V software.

**Step 20** Right-click the VSM and choose **Open Console**.

**Step 21** Click the **green arrow** to power on the VSM.

**Step 22** Enter the following commands at the VSM prompt.

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

**Step 23** Enter the HA role.

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

This example shows the HA role as primary.

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

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

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

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

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

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

Would you like to enter the basic configuration dialog (yes/no):  
This example shows the HA role as secondary.

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

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

**Step 24** Do one of the following:

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

**Step 25** If you have set up the VSM virtual machine (VM) to boot from the CD-ROM, and are installing the secondary VSM from the ISO image attached to your CD-ROM, remove the virtual CD-ROM now so that the VSM does not boot from the CD.

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

**Step 26** If you are setting up the secondary/standby VSM, when prompted to reboot the VSM, answer yes. The secondary VSM VM is rebooted and brought up in standby mode.

The password on the secondary VSM is synchronized with the password on the active/primary VSM.

Any configuration made on the active/primary VSM is now automatically synchronized with the standby.

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

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

[#####] 100%

HA mode set to secondary. Rebooting now...

You have completed this procedure for the secondary VSM.

**Step 27** Enter yes to enter the basic configuration dialog.

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

**Step 28** Enter no to create another Login account.

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

**Step 29** Enter no to configure a read-only SNMP community string.

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

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

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

**Step 31** Enter a name for the switch.

Enter the switch name: **n1000v**

**Step 32** Enter yes to configure out-of-band management and then enter the mgmt0 IPv4 address and subnet mask.

Continue with Out-of-band (mgmt0) management configuration? [yes/no] [y]: **yes**

Mgmt0 IPv4 address: **172.28.15.152**

Mgmt0 IPv4 netmask: **255.255.255.0**



**Step 33** Enter yes to configure the default gateway.

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

IPv4 address of the default gateway : **172.23.233.1**

**Step 34** Enter no to configure advanced IP options.

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

**Step 35** Enter yes to enable the Telnet service.

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

**Step 36** Enter yes to enable the SSH service and then enter the key type and number of key bits.

Enable the ssh service? (yes/no) [y]: **yes**

Type of ssh key you would like to generate (dsa/rsa) : **rsa**

Number of key bits <768-2048> : **1024**

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

**Step 37** Enter yes to enable the HTTP server.

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

**Step 38** Enter no to configure the NTP server.

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

**Step 39** Enter yes to configure the SVS domain parameters and then enter the mode (L2 or L3), and the control and packet VLAN IDs.

Configure svcs 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 187.

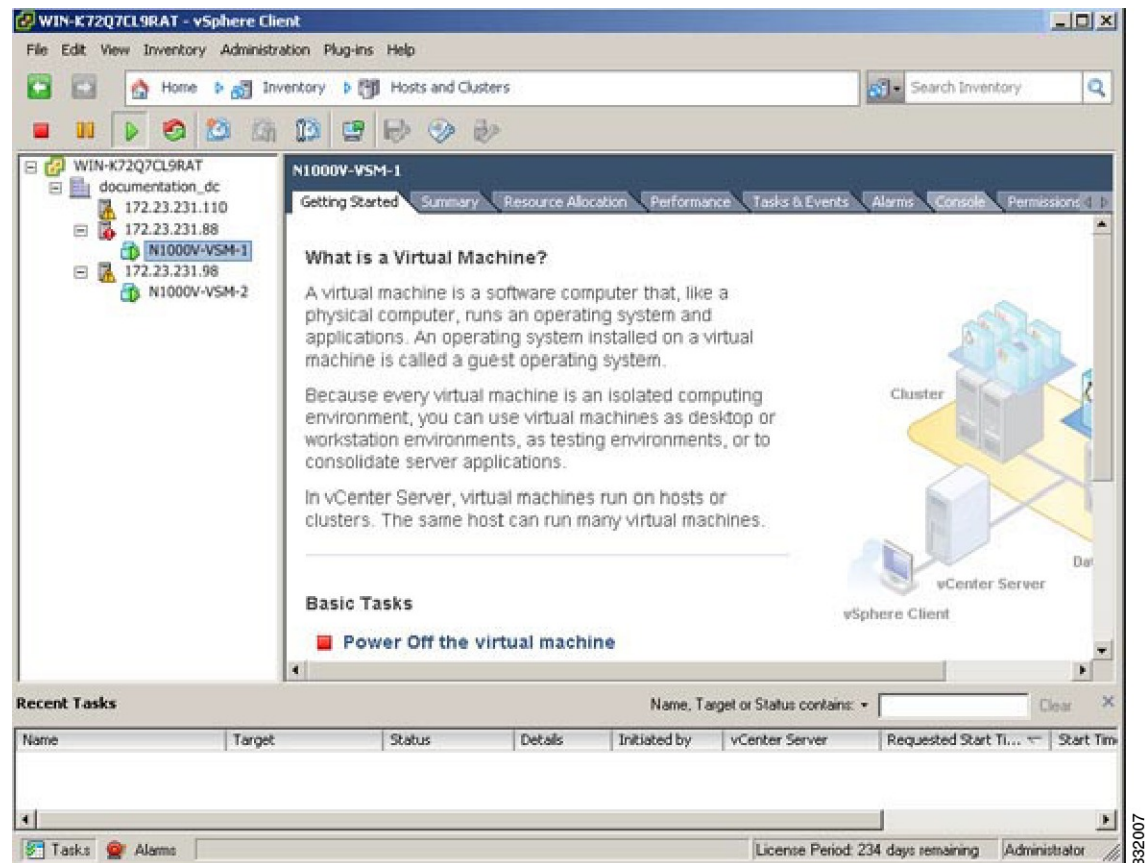
---

## Establishing the SVS Connection

### Procedure

- Step 1** Open the vSphere Client.
- Step 2** Choose the primary VSM.

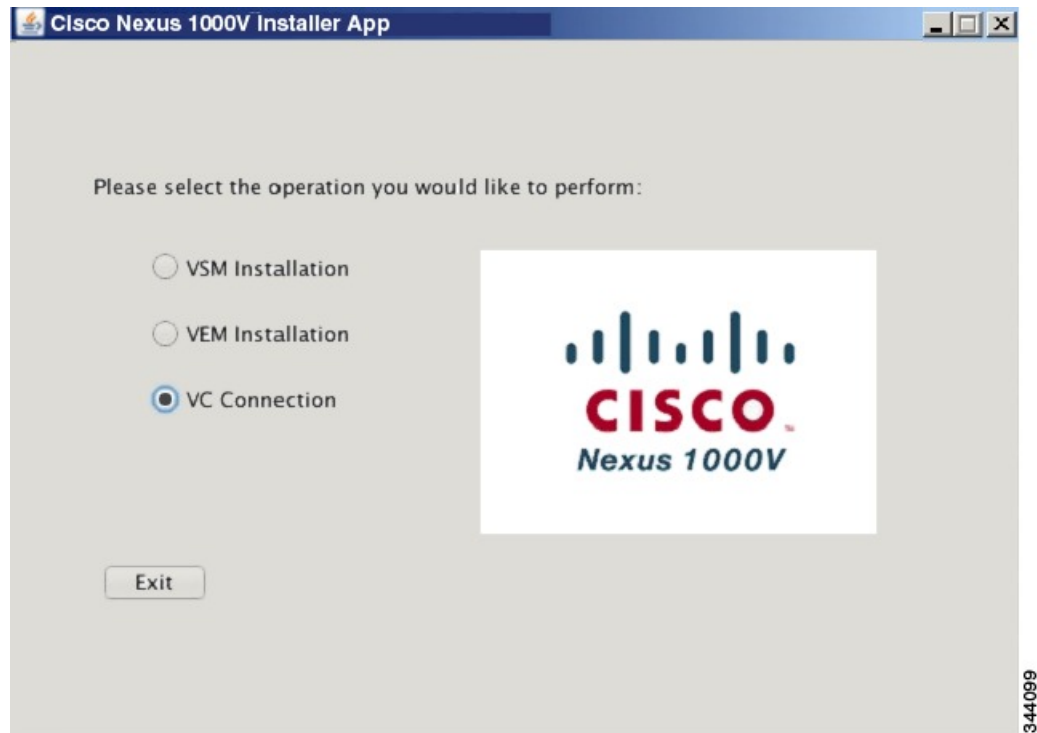
**Figure 84: vSphere Client Window**



332007

- Step 3** Choose the **Console** tab.
- Step 4** Enter the **show svcs connections** command to confirm that there is not an SVS connection.
- Step 5** Open a command window.
- Step 6** Enter the **java -jar Nexus1000V-launchPad.jar** command.
- Step 7** In the **Cisco Nexus 1000V Installer App** window, click the **VC Connection** radio button.

*Figure 85: Cisco Nexus 1000V Installer App Window*



- Step 8** Enter the following vCenter credentials:
- vCenter IP address
  - Secure HTTP port  
Port 443 is configured by default, but you can change the port if needed.
  - vCenter User ID (for a vCenter user with administrator-level privileges)

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

**Figure 86: Enter vCenter Credentials Screen**

The screenshot shows the 'Cisco Nexus 1000V Installer App' window. The title bar reads 'Cisco Nexus 1000V Installer App'. The window is divided into two main sections. On the left, a 'Steps' pane lists two steps: '1. Enter vCenter Credentials' (which is the current step) and '2. Enter VSM IP & Credentials'. Below the steps is the Cisco logo and the text 'Nexus 1000V'. The right section is titled 'Enter vCenter Credentials' and contains four input fields: 'vCenter IP' with the value '172.23.231.145', 'Port (https only)' with the value '443', 'vCenter User ID' with the value 'Administrator', and 'vCenter Password' which is masked with asterisks. At the bottom right of the window are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'. A vertical text '332005' is visible on the far right edge of the window.

**Step 9** Click **Next**.

**Step 10** Enter the following VSM credentials:

- VSM IP Address
- VSM Password
- From the **SVS Datacenter Name** drop-down list, choose the data center.

**Step 11** Click **Finish**.

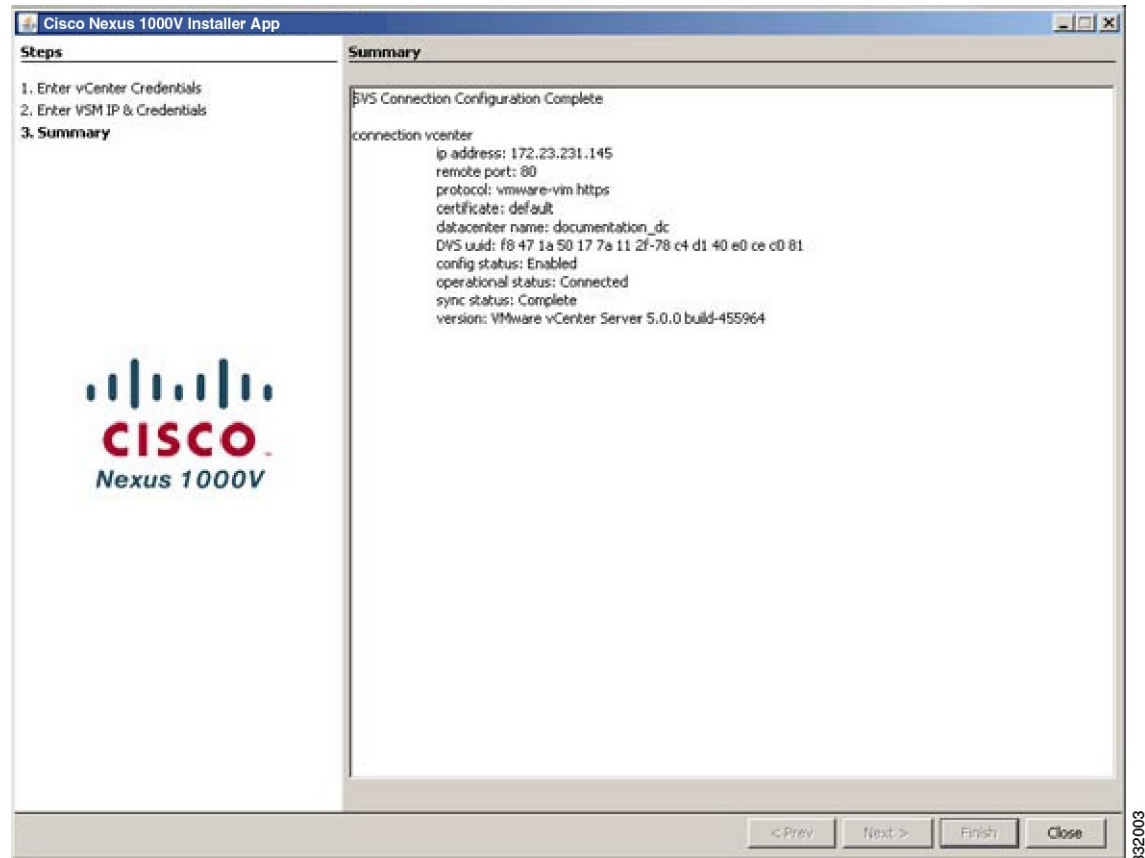
**Figure 87: Enter VSM IP & Credentials Screen**

The screenshot displays the 'Cisco Nexus 1000V Installer App' window. On the left, a 'Steps' pane lists two steps: '1. Enter vCenter Credentials' and '2. Enter VSM IP & Credentials', with the second step being the active one. The main area is titled 'Enter VSM IP & Credentials' and contains four input fields: 'VSM IP Address' (172.23.231.146), 'VSM User Name' (admin), 'VSM Password' (masked with asterisks), and 'SVS Datacenter Name' (documentation\_dc). The Cisco logo and 'Nexus 1000V' text are visible on the left side of the main area. At the bottom, there are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

332004

**Step 12** Click Close.

**Figure 88: Summary Screen**



**Step 13** In the **vSphere Console** window, enter the **show svs connections** command. The operational status is Connected.

You have completed establishing the SVS connection.







## APPENDIX

# C

## Upgrading a Standalone VSM

---

This chapter contains the following sections:

- [Upgrading a System with a Standalone VSM, page 193](#)
- [Upgrading a Standalone VSM, page 193](#)

## Upgrading a System with a Standalone VSM

## Upgrading a Standalone VSM

### Procedure

---

**Step 1** Log in to the VSM on the console.

**Step 2** Log in to cisco.com to access the links provided in this document.

To log in to cisco.com, go to the URL <http://www.cisco.com/> and click **Log In** at the top of the page. Enter your Cisco username and password.

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

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

**Step 4** Navigate to the download site for your switch.

You see links to the download images for your switch.

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

**Step 6** Ensure that the required space is available for the image files to be copied.

```
switch# dir bootflash:
```

```
.  
. .  
.
```

```
Usage for bootflash://
```

```
485830656 bytes used
```

```
1109045248 bytes free
1594875904 bytes total
```

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

**Step 7** Delete unnecessary files to make space available if you need more space on the VSM bootflash,

**Step 8** If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V kickstart and system images to the active VSM bootflash using a transfer protocol. You can use ftp:, tftp:, scp:, or sftp:. The examples in this procedure use scp:.

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

```
switch# copy
scp://user@scpserver.cisco.com//downloads/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin
bootflash:nexus-1000v-kickstart-4.2.1.SV2.1.1.bin
switch# copy scp://user@scpserver.cisco.com//downloads/nexus-1000v-4.2.1.SV2.1.1.bin
bootflash:nexus-1000v-4.2.1.SV2.1.1.bin
```

**Step 9** Read the release notes for the related image file. See the *Cisco Nexus 1000V Release Notes*.

**Step 10** Determine the VSM status.

```
switch# show system redundancy status
Redundancy role
-----
      administrative:  standalone
      operational:    standalone

Redundancy mode
-----
      administrative:  HA
      operational:    None

This supervisor (sup-1)
-----
      Redundancy state:  Active
      Supervisor state:  Active
      Internal state:    Active with no standby

Other supervisor (sup-2)
-----
      Redundancy state:  Not present
```

**Step 11** Save the running configuration to the start configuration.

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

**Step 12** Update the boot variables and module images on the VSM.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart-4.2.1.SV2.1.1.bin system
bootflash:nexus-1000v-4.2.1.SV2.1.1.bin
```

```
Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin for boot variable
"kickstart".
```

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

```
Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin for boot variable "system".
```

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

```
Verifying image type.
```

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

```
Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin.
[#####] 100% -- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.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(1.1) | yes          |
| 1      | kickstart | 4.2(1)SV1(4)    | 4.2(1)SV2(1.1) | yes          |

| Module            | Running-Version   | ESX Version                                 |
|-------------------|-------------------|---------------------------------------------|
| VSM Compatibility | ESX Compatibility |                                             |
| 3                 | 4.2(1)SV1(4)      | VMware ESXi 4.0.0 Releasebuild-208167 (1.9) |
| COMPATIBLE        | COMPATIBLE        |                                             |

```
Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)? [n]
```

### Step 13 Continue with the installation by pressing Y.

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

Install is in progress, please wait.

```
Setting boot variables.
[#####] 100% -- SUCCESS
```

```
Performing configuration copy.
[#####] 100% -- SUCCESS
```

Finishing the upgrade, switch will reboot in 10 seconds.

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

#### Example:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
```

```

TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:      version unavailable [last: loader version not available]
  kickstart: version 4.2(1)SV2(1.1)
  system:      version 4.2(1)SV2(1.1)
  kickstart image file is: bootflash:/nexus-1000v-kickstart-4.2.1.SV2.1.1.bin
  kickstart compile time: 3/27/2011 14:00:00 [03/27/2011 22:26:45]
  system image file is:   bootflash:/nexus-1000v-4.2.1.SV2.1.1.bin
  system compile time:    3/27/2011 14:00:00 [03/28/2011 00:56:08]

Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU          with 2075740 kB of memory.
  Processor Board ID T5056B050BB

  Device name: BL1-VSM
  bootflash:   3122988 kB

Kernel uptime is 0 day(s), 0 hour(s), 6 minute(s), 23 second(s)

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

```

---

## What to Do Next

Continue to [Upgrading VSMs from Releases 4.2\(1\)SV1\(4\), SV1\(4a\), SV1\(4b\), SV1\(5.1\), SV1\(5.1a\), or SV1\(5.2\) to Release 4.2\(1\)SV2\(1.1\)](#), on page 110.



## APPENDIX

# D

## Glossary

This chapter contains the following sections:

- [Glossary for Cisco Nexus 1000V, page 197](#)

## Glossary for Cisco Nexus 1000V

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

**Table 7: Cisco Nexus 1000V Terminology**

| Term                                 | Description                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Control VLAN                         | One of two VLANs used for the communication between the VSM and VEM. The control VLAN is used to exchange control messages. The network administrator configures the control VLAN.                                                                                                                                                                                                        |
| Distributed Resource Scheduler (DRS) | Balances the workload across your defined resources (hosts, shared storage, network presence, and resource pools) in a cluster.                                                                                                                                                                                                                                                           |
| Distributed Virtual Switch (DVS)     | A logical switch that spans one or more VMware ESX/ESXi 4.1 or ESXi 5.0 servers. It is controlled by one VSM instance.                                                                                                                                                                                                                                                                    |
| ESX/ESXi                             | <p>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.</p> <p>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.</p> |
| 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 | <p>The package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging:</p> <ul style="list-style-type: none"> <li>• Descriptor file (.OVF)</li> <li>• Manifest (.MF) and certificate files (optional)</li> </ul>                                                                                                                                                                                                                                                                                                           |
| 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)                    | <p>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.</p> <p>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.</p>                                                                                     |
| 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) | <p>The software application that manages Cisco Nexus 1000V software installation and VEM upgrades.</p> <p><b>Note</b> VUM is not a requirement. Software can be installed manually without using VUM.</p>                                                                                                                                                          |
| vSphere Client                   | The user interface that connects users remotely to the vCenter Server or ESX/ESXi from any Windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.                                                                                       |







## INDEX

### A

- accepting VEM upgrade [128](#)
- adding [74, 87](#)
  - Cisco Nexus 1000V to an ESXi image profile [87](#)
  - VEM hosts to DVS [74](#)
- augmenting [161](#)
  - customized ISO for VMware Release 5.0 [161](#)

### C

- Cisco Nexus 1000V Installer App [16, 17, 21](#)
  - guidelines and limitations [21](#)
  - information about [16](#)
  - prerequisites [17](#)
- combined upgrade [105](#)
- components of the Cisco Nexus 1000V [3](#)
- configuring [64, 146, 148](#)
  - layer 2 connectivity [64](#)
  - layer 3 interface [146](#)
  - svs domain in the VSM [148](#)
- control VLAN [9](#)
  - information about [9](#)
- creating [120, 147, 148, 168](#)
  - port profile with Layer 3 capability [147](#)
  - upgrade ISO [120, 168](#)
  - vmkernel on host [148](#)

### D

- differences between the Cisco Nexus 1000V and a physical switch [7](#)

### E

- establishing [187](#)
  - svs connection [187](#)

### F

- feature history [95, 149](#)
  - installing the Cisco Nexus 1000V [95](#)
  - upgrading Cisco Nexus 1000V [149](#)

### G

- glossary [197](#)
- guidelines and limitations [21, 100](#)
  - Cisco Nexus 1000V Installer App [21](#)
  - installing the Cisco Nexus 1000V [21](#)
  - upgrading Cisco Nexus 1000V [100](#)

### H

- host [17](#)
  - prerequisites [17](#)

### I

- information about [1, 2, 4, 6, 7, 9, 10, 16, 62](#)
  - administrator roles [7](#)
  - Cisco Nexus 1000V [2](#)
  - Cisco Nexus 1000V Installer App [16](#)
  - control VLAN [9](#)
  - layer 2 connectivity [62](#)
  - management VLAN [9](#)
  - packet VLAN [9](#)
  - port profiles [6](#)
  - system port profiles [10](#)
  - system VLANs [10](#)
  - virtual ethernet module [6](#)
  - virtual supervisor module [4](#)
  - virtualization [1](#)
- installing [23, 39, 82, 87, 135, 165, 171, 176](#)
  - custom mode [39](#)
  - ESXi 5.1 using the CLI [165](#)

- installing (*continued*)
  - from OVA image [176](#)
  - ISO image [171](#)
  - standard mode [23](#)
  - VEM software on a stateless ESXi host [87, 135](#)
  - VEM software using the CLI [82](#)
- installing a VSM [92](#)
  - on the Cisco Nexus 1010 [92](#)
- installing a VSM HA pair [23](#)
  - with L3 mode using the Cisco Nexus 1000V Installer App [23](#)
- installing the Cisco Nexus 1000V [21](#)
  - guidelines and limitations [21](#)
- installing the VEM software [81, 90, 92, 136, 137](#)
  - on a stateless ESX host using VUM [92, 137](#)
  - on a stateless ESXi host using esxcli [90, 136](#)
  - using VUM [81](#)
- installing VEM software [65, 82](#)
  - locally on a VMware 4.1 host using the CLI [82](#)
  - using the Cisco Nexus 1000V Installer App [65](#)
- installing VEM software locally [85](#)
  - on a VMware 5.0 host by using the CLI [85](#)
- installing VEM software remotely [83, 86](#)
  - on a VMware 5.0 host using the CLI [86](#)
  - VMware 4.1 host using the CLI [83](#)
- interface comparisons [145](#)
- ISO image [171](#)
  - installing [171](#)
- ISSU [107, 109](#)
  - command attributes [109](#)
  - dual VSMs [107](#)
  - VSM switchover [109](#)
- ISSU process [108](#)

## L

- layer 2 [64](#)
  - on the same host [64](#)
- layer 2 connectivity [62, 64](#)
  - configuring [64](#)
  - information about [62](#)
- layer 2 control mode [8](#)
- layer 3 [11](#)
  - topology [11](#)
- layer 3 advantages [140](#)
- layer 3 control mode [8](#)

## M

- management VLAN [9](#)
  - information about [9](#)

## P

- packet VLAN [9](#)
  - information about [9](#)
- port profile [147](#)
  - creating with Layer 3 capability [147](#)
- port profiles [6](#)
  - information about [6](#)
- prerequisites [17, 19, 20, 98, 99](#)
  - Cisco Nexus 1000V Installer App [17](#)
  - host [17](#)
  - upgrade [98](#)
  - upgrading VSMs [99](#)
  - upstream switch [19](#)
  - VEM [20](#)
  - VSM [19](#)
- procedures [23](#)
  - standard or custom [23](#)

## S

- setting [78](#)
  - virtual machine startup and shutdown parameters [78](#)
- simplified [138](#)
  - upgrade [138](#)
- software [16](#)
  - VEM [16](#)
  - VSM [16](#)
- software images [107](#)
- standalone VSM [193](#)
  - upgrading [193](#)
- stateless ESXi host [87](#)
- svs connection [187](#)
  - establishing [187](#)
- system port profiles [10](#)
  - information about [10](#)
- system VLANs [10](#)
  - information about [10](#)

## T

- topologies [11, 13, 14](#)
  - control and management on separate VLANs [14](#)
  - control and management on the same VLAN [13](#)
  - layer 3 [11](#)

## U

- upgrade [104](#)
  - Cisco Nexus 1000V only [104](#)

upgrade procedures [102, 118](#)

VEM [118](#)

upgrade software [97](#)

upgrade types [104](#)

upgrading [110, 123, 125, 128, 132, 140, 151, 152, 153, 154, 158, 160, 161, 164, 193](#)

VEMs manually from Release 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a) or (5.2) [132](#)

from 4.0 or 4.1 or 5.0 to 5.1 [158](#)

from releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV2(1.1) [140](#)

hosts [154, 161](#)

5.0, 5.0 Update 1, 5.1 [161](#)

to 4.1 [154](#)

standalone VSM [193](#)

stateful host [164](#)

5.0 patch 01 [164](#)

vCenter Server [123, 152, 158](#)

4.1 [152](#)

to 5.0, 5.0 Update 1, 5.1 [123, 158](#)

VEM software using the vCLI [128](#)

VEMs using VUM from Releases 4.2(1)SV1(4), (4a), (4b), (5.1), (5.1a) or (5.2) to 4.2(1)SV2(1.1) [125](#)

VMware release 4.0 to release 4.1 [151](#)

VSMs from 4.2(1) SV1(4), (4a), (4b), (5.1), (5.1a), or (5.2) to SV2(1.1) [110](#)

VUM [153, 160](#)

5.0, 5.0 Update 1, 5.1 [160](#)

VMware 4.1 [153](#)

upstream switch [19](#)

prerequisites [19](#)

## V

VEM [16, 20, 118](#)

prerequisites [20](#)

software [16](#)

upgrade procedures [118](#)

VEM software using the CLI [82](#)

installing [82](#)

verifying [157, 163](#)

build number [163](#)

upgrade [157, 163](#)

to VMware 4.1 [157](#)

virtual ethernet module [6](#)

information about [6](#)

virtual supervisor module [4](#)

information about [4](#)

virtualization [1](#)

information about [1](#)

VMware interaction [14](#)

VSM [16, 19](#)

prerequisites [19](#)

software [16](#)

VSM to VEM communication [8](#)

