



Cisco VSG for VMware vSphere, Release 4.2(1)/VSG2(1.1) and Cisco Prime NSC, Release 3.2 Installation and Upgrade Guide

First Published: February 05, 2014

Last Modified: February 28, 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:

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 NON-INFRINGEMENT 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.

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

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)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface ix

Audience ix

Document Conventions ix

Related Documentation for Cisco Virtual Security Gateway for VMware vSphere x

Documentation Feedback xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

Overview 1

Information About Installing the Cisco Prime NSC and the Cisco VSG 1

Information About Cisco VSG 1

Cisco Prime NSC and Cisco VSG Architecture 2

Trusted Multitenant Access 4

Dynamic Virtualization-Aware Operation 5

Setting Up the Cisco VSG and VLAN 6

Information About the Cisco Prime NSC 7

Cisco Prime NSC Key Benefits 7

Cisco Prime NSC Components 7

Cisco Prime NSC Architecture 8

Cisco Prime NSC Security 8

Cisco Prime NSC API 9

Cisco Prime NSC and Cisco VSG 9

System Requirements 9

Information About High Availability 11

CHAPTER 2

Installing the Cisco VSG and the Cisco Prime NSC-Quick Start 13

Information About Installing the Cisco Prime NSC and the Cisco VSG 13

Cisco VSG and Cisco Prime NSC Installation Planning Checklists 14

Basic Hardware and Software Requirements	14
License Requirements	15
VLAN Configuration Requirements	16
Required Cisco Prime NSC and Cisco VSG Information	16
Tasks and Prerequisites Checklist	18
Host Requirements	21
Obtaining the Cisco Prime NSC and the Cisco VSG Software	21
Task 1: Installing the Cisco Prime NSC from an OVA Template	21
Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity	23
Downloading the vCenter Extension File from the Cisco Prime NSC	23
Registering the vCenter Extension Plugin in the vCenter	24
Configuring the vCenter in VM Manager in the Cisco Prime NSC	24
Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent	25
Task 4: On the VSM, Preparing Cisco VSG Port Profiles	26
Task 5: Installing the Cisco VSG from an OVA Template	27
Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status	30
Task 7: On the Cisco Prime NSC, Configuring a Tenant and Security Profile	30
Configuring a Tenant on the Cisco Prime NSC	31
Configuring a Security Profile on the Cisco Prime NSC	31
Task 8: On the Cisco Prime NSC, Importing Service Image	32
Task 9: On the Cisco Prime NSC, Adding a Compute Firewall	32
Properties Window	34
Service Device Window	34
Task 10: On the Cisco Prime NSC, Configuring a Permit-All Rule	35
Task 11: On the Cisco VSG, Verifying the Permit-All Rule	36
Task 12: Enabling Logging	36
Enabling Policy-Engine Logging in a Monitor Session	36
Enabling Global Policy-Engine Logging	37
Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG	37
Enabling Traffic VM Port-Profile for Firewall Protection	38
Verifying the VSM or VEM for Cisco VSG Reachability	38
Checking the VM Virtual Ethernet Port for Firewall Protection	39
Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs	39

Sending Traffic Flow	40
Verifying Policy-Engine Statistics and Logs on the Cisco VSG	41

CHAPTER 3**Installing Cisco Prime Network Services Controller 43**

Information About the Cisco Prime NSC	43
Installation Requirements	43
Cisco Prime NSC System Requirements	43
Web-Based GUI Client Requirements	45
Firewall Ports Requiring Access	45
Information Required for Installation and Configuration	46
Shared Secret Password Criteria	47
Configuring Chrome for Use with Cisco Prime NSC	47
ESXi Server Requirement	48
Installing Cisco Prime NSC	48

CHAPTER 4**Installing the Cisco VSG 51**

Information About the Cisco VSG	51
Host and VM Requirements	51
Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology	52
Prerequisites for Installing the Cisco VSG Software	53
Obtaining the Cisco VSG Software	53
Installing the Cisco VSG Software	53
Installing the Cisco VSG Software from an OVA File	54
Installing the Cisco VSG Software from an ISO File	55
Configuring Initial Settings	57
Configuring Initial Settings on a Standby Cisco VSG	59
Verifying the Cisco VSG Configuration	60
Where to Go Next	60

CHAPTER 5**Registering Devices With the Cisco Prime NSC 61**

Registering a Cisco VSG	61
Registering a Cisco Nexus 1000V VSM	62
Registering vCenter	63

CHAPTER 6**Installing the Cisco VSG on a Cisco Cloud Services Platform Virtual Services Appliance 65**

Information About Installing the Cisco VSG on the Cisco Cloud Services Platform	65
Prerequisites for Installing Cisco VSG on Cisco Cloud Services Platform	66
Guidelines and Limitations	66
Installing a Cisco VSG on a Cisco Cloud Services Platform	67

CHAPTER 7**Upgrading the Cisco VSG and the Cisco Prime NSC 73**

Complete Upgrade Procedure	73
Information About Cisco Prime NSC Upgrades	74
Information About Cisco VSG Upgrades	74
Upgrade Guidelines and Limitations	75
Upgrade Procedure for Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1), Cisco VNMC Release 2.1 to Cisco Prime NSC Release 3.2 and Cisco Nexus 1000V Release 4.2(1)SV1(5.2) to Release 4.2(1)SV2(2.2)	75
Cisco VSG Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1) and Cisco VNMC 2.1 to Cisco Prime NSC 3.2 Staged Upgrade	76
Upgrading VNMC Release 2.1 to Cisco Prime NSC 3.0.2	79
Upgrading Cisco Prime NSC 3.0.2 to Cisco Prime NSC 3.2	81
Upgrading Cisco VSG from Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1)	83
Upgrading VSMs	84
Upgrade Procedures	84
Software Images	85
In-Service Software Upgrades on Systems with Dual VSMs	86
ISSU Process for the Cisco Nexus 1000V	87
ISSU VSM Switchover	87
ISSU Command Attributes	87
Upgrading VSMs from Releases 4.2(1)SV2(1.1x), 4.2(1)SV2(2.1x) to 5.2(1)SV3(1.1)	88
Upgrading VEMs	96
VEM Upgrade Procedures	96
VEM Upgrade Methods from Release 4.2(1)SV1(5x), or Release 4.2(1)SV2(1.1x) to the Current Release	97
Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(5x) and Later Releases to the Current Release	97
Upgrading the VEMs Manually from Release 4.2(1)SV1(5x) and Later Releases to the Current Release	101

Accepting the VEM Upgrade	104
Upgrading the VEM Software Using the vCLI	105
Upgrade Procedure for Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1), Cisco VNMC Release 2.0 to Release 2.1 and Cisco Nexus 1000V Release 4.2(1)SV1(5.2) to Release 4.2(1)SV2(2.2)	108
Cisco VSG Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1) and Cisco VNMC 2.0 to 2.1 Staged Upgrade	108
Upgrading VNMC from Release 2.0 to Release 2.1	111
Upgrading Cisco VSG from Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1)	113
Upgrading VSMs	114
Upgrade Procedures	114
Software Images	115
In-Service Software Upgrades on Systems with Dual VSMs	116
ISSU Process for the Cisco Nexus 1000V	117
ISSU VSM Switchover	117
ISSU Command Attributes	117
Upgrading VSMs from Releases 4.2(1)SV2(1.1x), 4.2(1)SV2(2.1x) to 5.2(1)SV3(1.1)	118
Upgrading VEMs	126
VEM Upgrade Procedures	126
VEM Upgrade Methods from Release 4.2(1)SV1(5x), or Release 4.2(1)SV2(1.1x) to the Current Release	127
Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(5x) and Later Releases to the Current Release	127
Upgrading the VEMs Manually from Release 4.2(1)SV1(5x) and Later Releases to the Current Release	131
Accepting the VEM Upgrade	134
Upgrading the VEM Software Using the vCLI	135

CHAPTER 8
Examples of Cisco Prime NSC OVA Template Deployment and Cisco Prime NSC ISO

Installations	139
OVA Installation Using vSphere 5.0 Installer	139
OVA Installation Using an ISO Image	141



Preface

This preface contains the following sections:

- [Audience](#), page ix
- [Document Conventions](#), page ix
- [Related Documentation for Cisco Virtual Security Gateway for VMware vSphere](#), page x
- [Documentation Feedback](#), page xi
- [Obtaining Documentation and Submitting a Service Request](#), page xi

Audience

This publication is for network administrators and server administrators who understand virtualization.

Document Conventions

Command descriptions use the following conventions:

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

Convention	Description
[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.
<i>variable</i>	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
<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
boldface screen font	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 Cisco Virtual Security Gateway for VMware vSphere

This section lists the documents available for Cisco Virtual Security Gateway and related products.

Cisco Virtual Security Gateway Documentation

The *Cisco Virtual Security Gateway for Nexus 1000V Series Switch* documentation is available at http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html.

Cisco Virtual Security Gateway for VMware vSphere Release Notes

Cisco VSG for VMware vSphere and Cisco VNMC Installation and Upgrade Guide

Cisco Virtual Security Gateway for VMware vSphere License Configuration Guide

Cisco Virtual Security Gateway for VMware vSphere Configuration Guide

Cisco Virtual Security Gateway for VMware vSphere Troubleshooting Guide

Cisco Virtual Security Gateway for VMware vSphere Command Reference

Cisco vPath and vServices Reference Guide for VMware vSphere

Cisco Virtual Network Management Center Documentation

The *Virtual Network Management Center* documentation is available at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html.

Related Documentation for Nexus 1000V Series NX-OS Software

The *Cisco Nexus 1000V Series Switch* documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/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 vsg-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

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

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



Overview

This chapter contains the following sections:

- [Information About Installing the Cisco Prime NSC and the Cisco VSG, page 1](#)
- [Information About the Cisco Prime NSC, page 7](#)
- [Information About High Availability, page 11](#)

Information About Installing the Cisco Prime NSC and the Cisco VSG

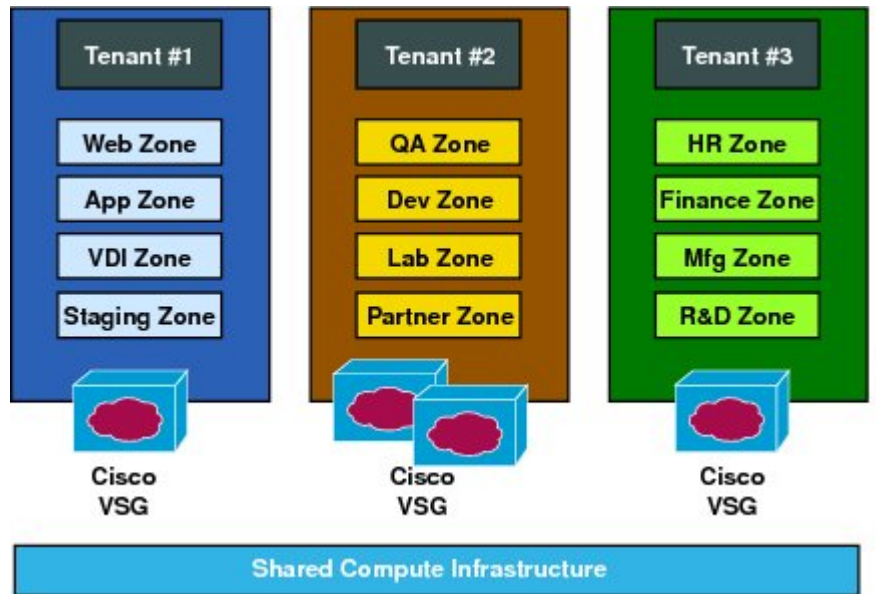
You must install the Cisco Prime Network Services Controller (Cisco Prime NSC) and the Cisco Virtual Security Gateway (Cisco VSG) in a particular sequence on the Cisco Nexus 1000V switch in order to have a functioning virtual system. For the critical sequence information that you need for a successful installation on the Cisco Nexus 1000V switch, see Chapter 2, *Installing the Cisco VSG and the Cisco Prime NSC-Quick Start*. For installing the Cisco VSG on the Cisco Cloud Services Platform Virtual Services Appliance, see Chapter 6, *Installing the Cisco VSG on a Cisco Cloud Services Platform Virtual Services Appliance*.

Information About Cisco VSG

The Cisco VSG is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments with dynamic policy-driven operation, mobility-transparent enforcement, and scale-out deployment for dense multitenancy. By associating one or more virtual machines (VMs) into distinct trust zones, the Cisco VSG ensures that access to trust zones is controlled and monitored through established

security policies. The following figure shows the trusted zone-based access control that is used in per-tenant enforcement with the Cisco VSG.

Figure 1: Trusted Zone-Based Access Control Using Per-Tenant Enforcement with the Cisco VSG

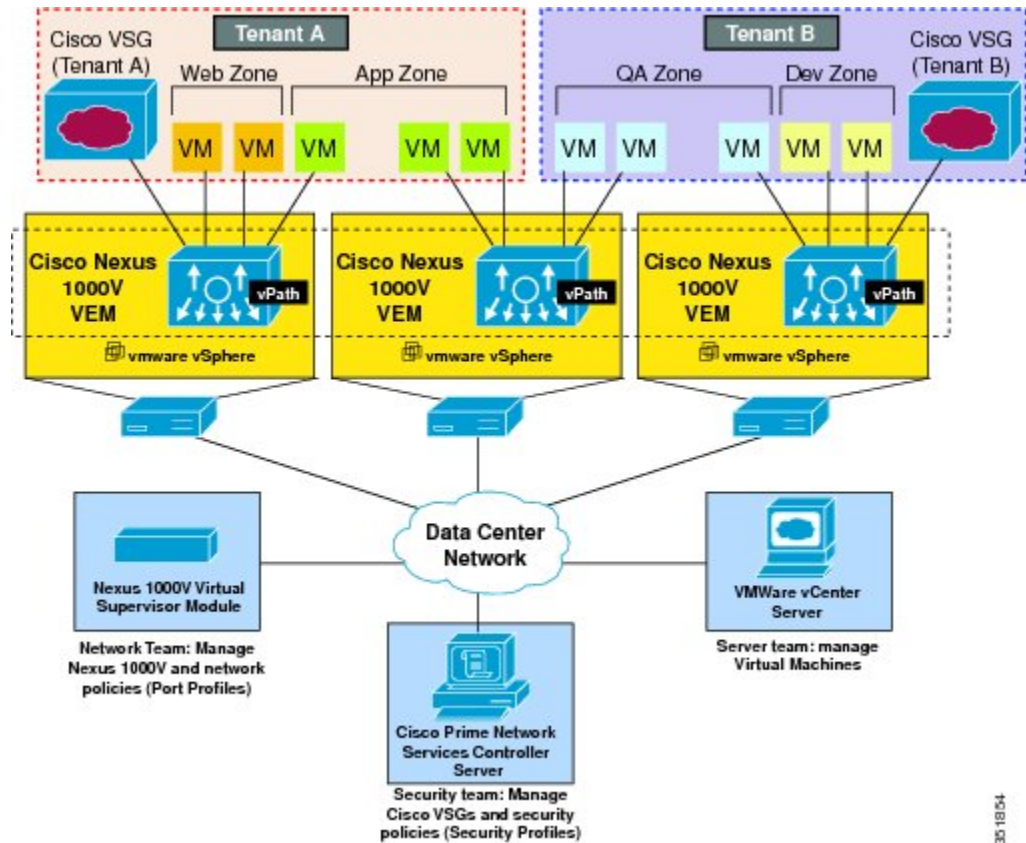


Cisco Prime NSC and Cisco VSG Architecture

The Cisco VSG operates with the Cisco Nexus 1000V Series switch in the VMWare vSphere Hypervisor or the Cisco Cloud Services Platform Virtual Services Appliance, and the Cisco VSG leverages the virtual network service data path (vPath). vPath steers traffic, whether external-to-VM or VM-to-VM, to the Cisco VSG of a tenant. Initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement.

After the policy decision is made, the Cisco VSG offloads policy enforcement of the remaining packets to vPath.

Figure 2: Cisco Virtual Security Gateway Deployment Topology



vPath supports the following features:

- Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant
- Per-tenant policy enforcement of flows offloaded by the Cisco VSG to vPath

The Cisco VSG and the VEM provide the following benefits:

- Each Cisco VSG can provide protection across multiple physical servers, which eliminates the need for you to deploy a virtual appliance per physical server.
- By offloading the fast-path to one or more vPath Virtual Ethernet Modules (VEMs), the Cisco VSG enhances security performance through distributed vPath-based enforcement.
- You can use the Cisco VSG without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling, which is based on security profiles, simplifies physical server upgrades without compromising security or incurring application outages.
- For each tenant, you can deploy the Cisco VSG in an active-standby mode to ensure that vPath redirects packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.

- You can place the Cisco VSG on a dedicated server so that you can allocate the maximum compute capacity to application workloads. This feature enables capacity planning to occur independently and allows for operational segregation across security, network, and server groups.

Trusted Multitenant Access

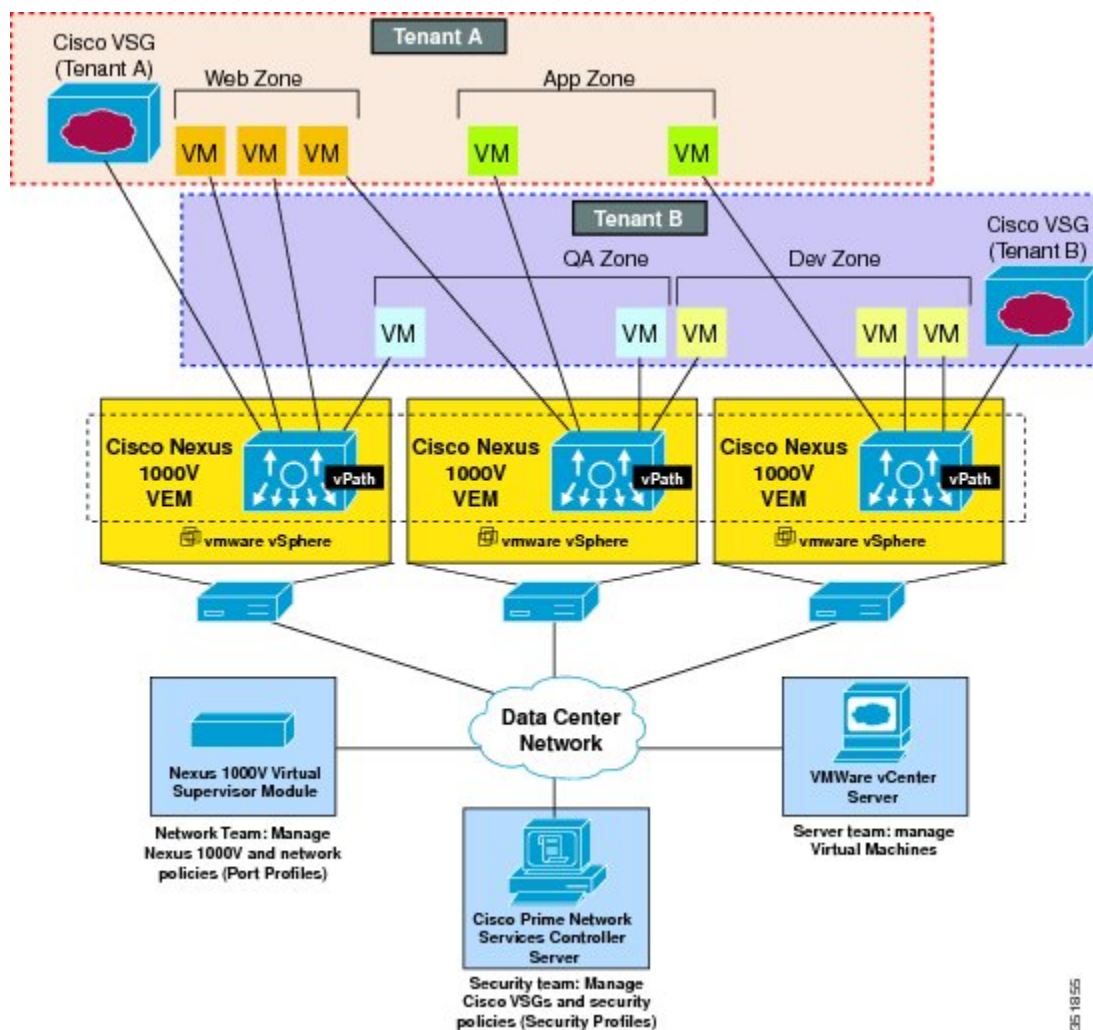
You can transparently insert a Cisco VSG into the VMware vSphere environment where the Cisco Nexus 1000V is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy a Cisco VSG at the tenant level, at the virtual data center (vDC) level, or at the vApp level.

As you instantiate VMs for a given tenant, their association to security profiles (or zone membership) occurs immediately through binding with the Cisco Nexus 1000V port profile. Each VM is placed upon instantiation into a logical trust zone. Security profiles contain context-aware rule sets that specify access policies for traffic that enters and exits each zone. In addition to VM and network contexts, security administrators can also leverage custom attributes that define zones directly through security profiles. You can apply controls to zone-to-zone traffic and to external-to-zone (and zone-to-external) traffic. Zone-based enforcement occurs within a VLAN because a VLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then offloads enforcement to the Cisco Nexus 1000V VEM vPath module. Upon enforcement, the Cisco VSG can permit or deny access and can generate optional access logs. The Cisco VSG also provides policy-based traffic monitoring capability with access logs.

Dynamic Virtualization-Aware Operation

A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. Live migration of VMs can occur due to manual or programmatic VMotion events. The following figure shows how the structured environment can change over time due to dynamic VMs.

Figure 3: Cisco VSG Security in a Dynamic VM Environment, Including VM Live Migration



The Cisco VSG operating with the Cisco Nexus 1000V (and vPath) supports a dynamic VM environment. When you create a tenant with the Cisco VSG (standalone or active-standby pair) on the Cisco Prime NSC, associated security profiles are defined that include trust zone definitions and access control rules. Each security profile is bound to a Cisco Nexus 1000V port profile (authored on the Cisco Nexus 1000V Virtual Supervisor Module (VSM) and published to the VMware vCenter.

When a new VM is instantiated, the server administrator assigns appropriate port profiles to the virtual Ethernet port of the VM. Because the port profile uniquely refers to a security profile and VM zone membership, the Cisco VSG immediately applies the security controls. You can repurpose a VM by assigning it to a different port profile or security profile.

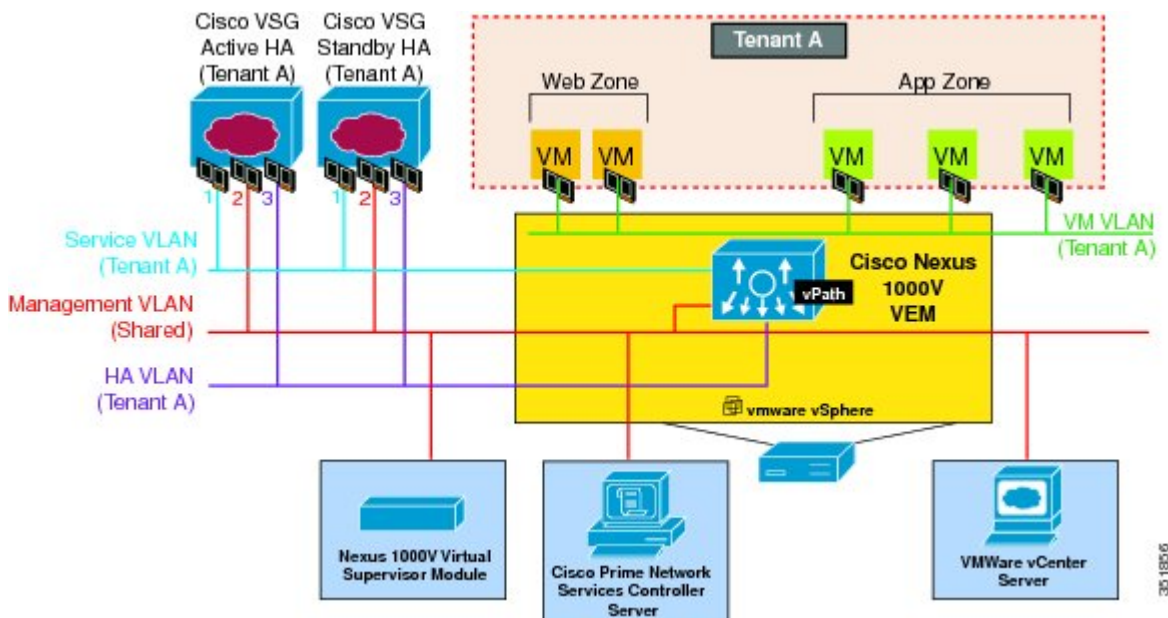
As VMotion events are triggered, VMs move across physical servers. Because the Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to VMotion events.

Setting Up the Cisco VSG and VLAN

You can set up a Cisco VSG in an overlay fashion so that VMs can reach a Cisco VSG irrespective of its location. The vPath component in the Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

In the following figure, the Cisco VSG connects to three different VLANs (service VLAN, management VLAN, and HA VLAN). A Cisco VSG is configured with three vNICs—data vNIC (1), management vNIC (2), and HA vNIC (3)—with each of the vNICs connected to one of the VLANs through a port profile.

Figure 4: Cisco Virtual Security Gateway VLAN Usages



The VLAN functions are as follows:

- The service VLAN provides communications between the Cisco Nexus 1000V VEM and Cisco VSG. All the Cisco VSG data interfaces are part of the service VLAN and the VEM uses this VLAN for its interaction with Cisco VSG.
- The management VLAN connects the management platforms such as the VMware vCenter, the Cisco Prime NSC, the Cisco Nexus 1000V VSM, and the managed Cisco VSGs. The Cisco VSG management vNIC is part of the management VLAN.
- The HA VLAN provides the heartbeat mechanism and identifies the active and standby relationship between the Cisco VSGs. The Cisco VSG vNICs are part of the HA VLAN.

You can allocate one or more VM data VLANs for VM-to-VM communications. In a typical multitenant environment, the management VLAN is shared among all the tenants and the service VLAN, HA VLAN, and

the VM data. VLANs are allocated on a per-tenant basis. However, when VLAN resources become scarce, you might decide to use a single VLAN for service and HA functions.

Information About the Cisco Prime NSC

The Cisco Prime NSC virtual appliance is based on Red Hat Enterprise Linux (RHEL), which provides centralized device and security policy management of the Cisco VSG for the Cisco Nexus 1000V Series switch. Designed for multitenant operation, the Cisco Prime NSC provides seamless, scalable, and automation-centric management for virtual data center and cloud environments. With a web-based GUI, CLI, and XML APIs, the Cisco Prime NSC enables you to manage Cisco VSGs that are deployed throughout the data center from a centralized location.



Note

Multitenancy is when a single instance of the software runs on a Software-as-a-Service (SaaS) server, serving multiple client organizations or tenants. In contrast, multi-instance architecture has separate software instances set up for different client organizations. With a multitenant architecture, a software application can virtually partition data and configurations so that each tenant works with a customized virtual application instance.

The Cisco Prime NSC is built on an information model-driven architecture, where each managed device is represented by its subcomponents.

Cisco Prime NSC Key Benefits

The Cisco Prime NSC provides the following key benefits:

- Rapid and scalable deployment with dynamic, template-driven policy management based on security profiles.
- Seamless operational management through XML APIs that enable integration with third-party management tools.
- Greater collaboration across security and server administrators, while maintaining administrative separation and reducing administrative errors.

Cisco Prime NSC Components

The Cisco Prime NSC architecture includes the following components:

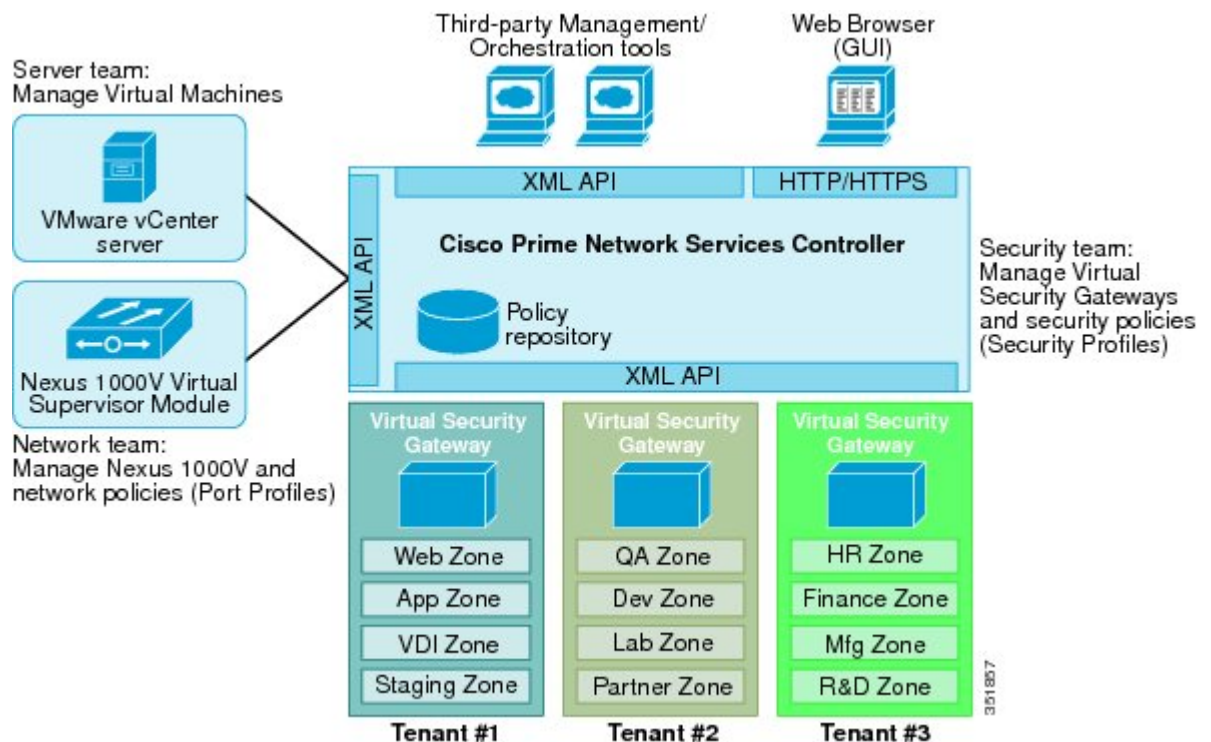
- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning. This function simplifies large scale deployments as follows:
 - Devices can be preinstantiated and then configured on demand

- Devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools
- A distributed management-plane function that uses an embedded management agent on each device that allows for a scalable management framework.

Cisco Prime NSC Architecture

The Cisco Prime NSC architecture includes the components in the following figure:

Figure 5: Cisco Prime NSC Components



Cisco Prime NSC Security

The Cisco Prime NSC uses security profiles for tenant-centric template-based configuration of security policies. A security profile is a collection of security policies that are predefined and applied on an on-demand basis at the time of Virtual Machine (VM) instantiation. These profiles simplify authoring, deployment, and management of security policies in a dense multitenant environment, reduce administrative errors, and simplify audits.

Cisco Prime NSC API

The Cisco Prime NSC API allows you to coordinate with third-party provisioning tools for programmatic provisioning and management of Cisco VSGs. This feature allows you to simplify data center operational processes and reduce the cost of infrastructure management.

Cisco Prime NSC and Cisco VSG

The Cisco Prime NSC operates with the Cisco Nexus 1000V Series VSM to achieve the following scenarios:

- Security administrators who author and manage security profiles as well as manage Cisco VSG instances. Security profiles are referenced in Cisco Nexus 1000V Series port profiles through the Cisco Prime NSC interface.
- Network administrators who author and manage port profiles as well as manage Cisco Nexus 1000V Series switches. Port profiles are referenced in the vCenter through the Cisco Nexus 1000V Series VSM interface.
- Server administrators who select the appropriate port profiles in the vCenter when instantiating a virtual machine.

System Requirements

System requirements for a Cisco Prime NSC are as follows:

Requirement	Description
Four Virtual CPUs	1.5 GHz for each Virtual CPU
Memory	4 GB RAM
Disk Space	<p>One of the following, depending on InterCloud functionality:</p> <ul style="list-style-type: none"> • With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows: <ul style="list-style-type: none"> ◦ Disk 1: 20 GB ◦ Disk 2: 200 GB • Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: <ul style="list-style-type: none"> ◦ Disk 1: 20 GB ◦ Disk 2: 20 GB

Requirement	Description
Processor	x86 Intel or AMD server with a 64-bit processor listed in the VMware compatibility matrix. Note You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php .
VMware vSphere	ESXi 5.0, 5.1, and 5.5
VMware vCenter	Release 5.5 (5.1 vCenter supports host version upto 5.1)
Intel Virtualization Technology (VT)	Enabled in the BIOS
Browser	Any of the following browsers: <ul style="list-style-type: none"> • Internet Explorer 9.0 or higher • Mozilla Firefox 23.0 or higher • Google Chrome 29.0 or higher Note If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website. Note Before using Google Chrome with Cisco Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco Prime NSC , on page 47.
Ports	Access to the Cisco Prime NSC application using a web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports): <ul style="list-style-type: none"> • 443 (HTTPS) • 80 (HTTP/TCP) • 843 (Adobe Flash)
Flash Player	Adobe Flash Player plugin 11.2 or higher

Information About High Availability

VMware high availability (HA) provides a base level of protection for a Cisco VSG VM by restarting it on another host in the HA cluster. With VMware HA, data is protected through a shared storage. The Cisco Prime NSC services can be restored in a few minutes. Transient data such as user sessions is not preserved in the service transfer. Existing users or service requests must be reauthenticated.

Requirements for supporting VMware HA in Cisco Prime NSC are as follows:

- At least two hosts per HA cluster
- VM and configuration files located on the shared storage and hosts are configured to access that shared storage

For additional details, see the VMware guides for HA and fault tolerance.



Installing the Cisco VSG and the Cisco Prime NSC-Quick Start

This chapter contains the following sections:

- [Information About Installing the Cisco Prime NSC and the Cisco VSG](#), page 13
- [Task 1: Installing the Cisco Prime NSC from an OVA Template](#), page 21
- [Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity](#), page 23
- [Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent](#), page 25
- [Task 4: On the VSM, Preparing Cisco VSG Port Profiles](#), page 26
- [Task 5: Installing the Cisco VSG from an OVA Template](#), page 27
- [Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status](#), page 30
- [Task 7: On the Cisco Prime NSC, Configuring a Tenant and Security Profile](#), page 30
- [Task 8: On the Cisco Prime NSC, Importing Service Image](#), page 32
- [Task 9: On the Cisco Prime NSC, Adding a Compute Firewall](#), page 32
- [Task 10: On the Cisco Prime NSC, Configuring a Permit-All Rule](#), page 35
- [Task 11: On the Cisco VSG, Verifying the Permit-All Rule](#), page 36
- [Task 12: Enabling Logging](#), page 36
- [Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG](#), page 37
- [Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs](#), page 39

Information About Installing the Cisco Prime NSC and the Cisco VSG

This chapter describes how to install and set up a basic working configuration of the Cisco Prime NSC and Cisco VSG. The example in this chapter uses the OVF template method to install the OVA files of the software.

The steps assume that the Cisco Nexus 1000V Series switch is operational, and endpoint VMs are already installed.

Cisco VSG and Cisco Prime NSC Installation Planning Checklists

Planning the arrangement and architecture of your network and equipment is essential for a successful operation of the Cisco Prime NSC and Cisco VSG.

Basic Hardware and Software Requirements

The following table lists the basic hardware and software requirements for Cisco VSG and Cisco Prime NSC installation.

The Cisco VSG software is available for download at <http://www.cisco.com/en/US/products/ps13095/index.html> and the Cisco Prime NSC software is available for download at <http://www.cisco.com/en/US/products/ps13213/index.html>.

Requirement	Description
Four Virtual CPUs	1.5 GHz for each Virtual CPU
Memory	4 GB RAM for the Cisco VSG and 4 GB RAM for the Cisco Prime NSC or 8 GB for both
Disk Space	<p>One of the following, depending on InterCloud functionality:</p> <ul style="list-style-type: none"> • With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows: <ul style="list-style-type: none"> ◦ Disk 1: 20 GB ◦ Disk 2: 200 GB • Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: <ul style="list-style-type: none"> ◦ Disk 1: 20 GB ◦ Disk 2: 20 GB
Processor	<p>x86 Intel or AMD server with a 64-bit processor listed in the VMware compatibility matrix.</p> <p>Note You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php.</p>
VMware vSphere	ESXi 5.0, 5.1, and 5.5

Requirement	Description
VMware vCenter	Release 5.5 (5.1 vCenter supports host version upto 5.1)
Intel Virtualization Technology (VT)	Enabled in the BIOS
Browser	<p>Any of the following browsers:</p> <ul style="list-style-type: none"> • Internet Explorer 9.0 or higher • Mozilla Firefox 23.0 or higher • Google Chrome 29.0 or higher <p>Note If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website.</p> <p>Note Before using Google Chrome with Cisco Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco Prime NSC, on page 47.</p>
Ports	<p>Access to the Cisco Prime NSC application using a web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports):</p> <ul style="list-style-type: none"> • 443 (HTTPS) • 80 (HTTP/TCP) • 843 (Adobe Flash)
Flash Player	Adobe Flash Player plugin 11.2 or higher

License Requirements

Cisco VSG license is integrated with the Nexus1000V Multi-Hypervisor License. You need to install the Nexus1000V Multi-Hypervisor License for Cisco VSG for VMware vSphere. The Cisco N1kv VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Nexus1000V Multi-Hypervisor License and change the VSM mode to advanced mode. When the Nexus1000V Multi-Hypervisor License is installed, the license for Cisco VSG is automatically included.

**Note**

If you try to access VSG services with VSM in essential mode, an error message is generated on VSM console indicating that the Nexus1000V Multi-Hypervisor License is required for VSG.

The Nexus1000V Multi-Hypervisor License is available in three different types:

- Default: The Nexus 1000v switch may be configured in Essential or Advanced mode.
 - Essential Mode: Not Supported.
 - Advanced Mode: After upgrading the software, Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

**Note**

You must install either the evaluation or the permanent (MSFT PKG) license prior to upgrading to the latest software.

- Evaluation: The Nexus 1000V switch should be in Advanced mode. After upgrading the software, Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.
- Permanent: The Nexus 1000V switch should be in Advanced mode. After upgrading the software, Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

**Note**

You have to request for an evaluation or permanent Nexus1000V Multi-Hypervisor License.

For more information about the Cisco Nexus 1000V for VMware vSphere licenses, see the *Cisco Nexus 1000V for VMware vSphere License Configuration Guide*.

VLAN Configuration Requirements

Follow these VLAN requirements to prepare the Cisco Nexus 1000V Series switch for further installation processes:

- You must have two VLANs that are configured on the Cisco Nexus 1000V Series switch uplink ports: the service VLAN and an HA VLAN (the VLAN does not need to be the system VLAN).
- You must have two port profiles that are configured on the Cisco Nexus 1000V Series switch: one port profile for the service VLAN and one port profile for the HA VLAN (you will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000V Series switch can communicate with it)

Required Cisco Prime NSC and Cisco VSG Information

The following information can be used later during the Cisco Prime NSC and Cisco VSG installation.

Type	Your Information
Cisco VSG name—Unique within the inventory folder and up to 80 characters	

Type	Your Information
Hostname—Where the Cisco VSG will be installed in the inventory folder	
Datastore name—Where the VM files will be stored	
Cisco VSG management IP address	
VSM management IP address	
Cisco Prime NSC instance IP address	
Mode for installing the Cisco VSG	<ul style="list-style-type: none"> • Standalone • HA primary • HA secondary • Manual installation
Cisco VSG VLAN number <ul style="list-style-type: none"> • Service (1) • Management (2) • High availability (HA) (3) 	
Cisco VSG port profile name <ul style="list-style-type: none"> • Data (1) • Management (2) • High availability (HA) (3) <p>Note The numbers indicate the VSG port profile that must be associated with the VSG VLAN number.</p>	
HA pair ID (HA domain ID)	
NSC DNS IP address	
NSC NTP IP address	
Cisco VSG admin password	
Cisco Prime NSC admin password	
Cisco VSM admin password	

Type	Your Information
Shared secret password (Cisco Prime NSC, Cisco VSG policy agent, Cisco VSM policy agent)	

Tasks and Prerequisites Checklist

Tasks	Prerequisites
Task 1: Installing the Cisco Prime NSC from an OVA Template, on page 21	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • The Cisco Prime NSC OVA image is available in the vCenter. • Know the IP/subnet mask/gateway information for the Cisco Prime NSC. • Know the admin password, shared_secret, hostname that you want to use. • Know the DNS server and domain name information. • Know the NTP server information. • Know the management port-profile name for the Virtual Machine (VM) (management). <p>Note The management port profile is the same port profile that is used for the Virtual Supervisor Module (VSM). The port profile is configured in the VSM and is used for the Cisco Prime NSC management interface.</p> <ul style="list-style-type: none"> • Make sure that all system requirements are met as specified in System Requirements. • A shared secret password is available (this password enables communication between the Cisco Prime NSC, VSM, and Cisco VSG).
Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity, on page 23	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • Supported Adobe Flash Player given in System Requirements, on page 9 • IP address of the Cisco Prime NSC • The password for Admin user

Tasks	Prerequisites
<p>Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent, on page 25</p>	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • The Cisco Prime NSC policy-agent image is available on the VSM (for example, vnmc-vsmpa.2.1.1e.bin) <p>Note The string vsmpa must appear in the image name as highlighted.</p> <ul style="list-style-type: none"> • The IP address of the Cisco Prime NSC • The shared secret password you defined during the Cisco Prime NSC installation • That IP connectivity between the VSM and the Cisco Prime NSC is working <p>Note If you upgrade your VSM, you must also copy the latest Cisco VSM policy agent image. This image is available in the Cisco Prime NSC image bundle to boot from a flash drive and to complete registration with the Cisco Prime NSC.</p>
<p>Task 4: On the VSM, Preparing Cisco VSG Port Profiles, on page 26</p>	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • The uplink port-profile name. • The VLAN ID for the Cisco VSG data interface (for example,100). • The VLAN ID for the Cisco VSG-ha interface (for example, 200). • The management VLAN (management). <p>Note None of these VLANs need to be system VLANs.</p>

Tasks	Prerequisites
<p>Task 5: Installing the Cisco VSG from an OVA Template, on page 27</p>	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • The Cisco VSG OVA image is available in the vCenter. • Cisco VSG-Data and Cisco VSG-ha port profiles are created on the VSM. • The management port profile (management) <ul style="list-style-type: none"> Note The management port profile is the same port profile that is used for the VSM. The port profile is configured in the VSM and is used for the Cisco Prime NSC management interface. • The Cisco VSG-Data port profile: VSG-Data • The Cisco VSG-ha port profile: VSG-ha • The HA ID • The IP/subnet mask/gateway information for the Cisco VSG • The admin password • 2 GB RAM and 3 GB hard disk space are available • The Cisco Prime NSC IP address • The shared secret password • The IP connectivity between Cisco VSG and Cisco Prime NSC is okay. • The Cisco VSG VNM-PA image name (vnmc-vsipa.2.1.1b.bin) is available.
<p>Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status, on page 30</p>	<p>—</p>
<p>Task 7: On the Cisco Prime NSC, Configuring a Tenant and Security Profile, on page 30</p>	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • Supported Adobe Flash Player given in System Requirements, on page 9 • The IP address of the Cisco Prime NSC • The password for Admin user
<p>Task 8: On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall</p>	<p>—</p>
<p>Task 10: On the Cisco Prime NSC, Configuring a Permit-All Rule, on page 35</p>	<p>—</p>

Tasks	Prerequisites
Task 11: On the Cisco VSG, Verifying the Permit-All Rule, on page 36	—
Task 12: Enabling Logging, on page 36	—
Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, on page 37	<p>Make sure that you know the following:</p> <ul style="list-style-type: none"> • The server virtual machine that runs with an access port profile (for example, web server) • The Cisco VSG data IP address (10.10.10.200) and VLAN ID (100) • The security profile name (for example, sp-web) • The organization (Org) name (for example, root/Tenant-A) • The port profile that you would like to edit to enable firewall protection • That one active port in the port-profile with vPath configuration has been set up
Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, on page 39	—

Host Requirements

- ESXi platform that runs VMware software release 5.0 , 5.1, and 5.5 with a minimum of 4 GB physical RAM for the Cisco VSG and 4 GB physical RAM for the Cisco Prime NSC.
- 1 processor
- Four Virtual CPUs with speed of 1.5 GHz for each virtual CPU

Obtaining the Cisco Prime NSC and the Cisco VSG Software

The Cisco VSG software is available for download at the following URL:

<http://www.cisco.com/en/US/products/ps13095/index.html>

The Cisco Prime NSC software is available for download at the following URL:

<http://www.cisco.com/en/US/products/ps13213/index.html>

Task 1: Installing the Cisco Prime NSC from an OVA Template

Before You Begin

Know the following:

- The Cisco Prime NSC OVA image is available in the vCenter.
- Know the IP/subnet mask/gateway information for the Cisco Prime NSC.
- Know the admin password, shared_secret, hostname that you want to use.
- Know the DNS server and domain name information.
- Know the NTP server information.
- Know the management port-profile name for the Virtual Machine (VM) (management).



Note The management port profile is the same port profile that is used for the Virtual Supervisor Module (VSM). The port profile is configured in the VSM and is used for the Cisco Prime NSC management interface.

- Make sure that all system requirements are met as specified in [System Requirements](#).
- A shared secret password is available (this password enables communication between the Cisco Prime NSC, VSM, and Cisco VSG).

-
- Step 1** Use the VMware vSphere Client to log into the vCenter server.
- Step 2** Choose the host on which to deploy the Cisco Prime NSC VM.
- Step 3** From the File menu, choose **Deploy OVF Template**.
- Step 4** In the **Source** window, choose the Cisco Prime NSC OVA, then click **Next**.
- Step 5** In the **OVF Template Details** window, review the details of the Cisco Prime NSC template, and then click **Next**.
- Step 6** In the **End User License Agreement** window, click **Accept** after reviewing the End User License Agreement, and then click **Next**.
- Step 7** In the **Name and Location** window, provide the required information, and then click **Next**.
The name can contain up to 80 characters and must be unique within the inventory folder.
- Step 8** In the **Deployment Configuration** window, choose **Installer** from the Configuration drop-down list, then click **Next**.
- Step 9** In the **Datastore** window, select the data store for the VM, and then click **Next**.
Note The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN). If only one storage location is available for an ESXi host, this window does not display and you are assigned to the one that is available.
- Step 10** In the **Disk Format** window, click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks, and then click **Next**.
The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.
- Step 11** In the **Network Mapping** window, select the management network port group for the VM, then click **Next**.
- Step 12** In the **Properties** window, provide the required information, address any errors described in the red text messages below the selection box, and then click **Next**. If needed, you can enter placeholder information as long as your entry meets the field requirements.
Note You can safely ignore the Cisco Prime NSC Restore fields.
Note For choosing the shared secret password, follow the guidelines given in [Shared Secret Password Criteria](#), on page 47.

- Step 13** In the **Ready to Complete** window, review the deployment settings information, and then click **Finish**.
- Caution** Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, gateway, and DNS and NTP IP address information.
A progress indicator shows the task progress until Cisco Prime NSC is deployed.
- Step 14** After Cisco Prime NSC is successfully deployed, click **Close**.
- Step 15** Power on the Cisco VSG VM.
-

Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity

Perform the following tasks in the same order as listed below to set up the VM-manager for vCenter connectivity:

- [Downloading the vCenter Extension File from the Cisco Prime NSC, on page 23](#)
- [Registering the vCenter Extension Plugin in the vCenter, on page 24](#)
- [Configuring the vCenter in VM Manager in the Cisco Prime NSC, on page 24](#)

Downloading the vCenter Extension File from the Cisco Prime NSC

Before You Begin

Make sure that you have the following:

- Supported Adobe Flash Player given in [System Requirements, on page 9](#)
- IP address of the Cisco Prime NSC
- The password for Admin user

-
- Step 1** In your browser, enter `https://server-ip-address` where *server-ip-address* is the Cisco Prime NSC IP address.
- Step 2** In the **Website Security Certificate** window, choose **Continue to this website**.
- Step 3** In the Cisco Prime NSC login window, enter the username **admin** and the admin user password. This is the password that you set when installing the Cisco Prime NSC.
- Step 4** In the Cisco Prime NSC window, choose **Resource Management > VM Managers > VM Managers**.
- Step 5** In the VM Managers pane, click **Export vCenter Extension**.
- Step 6** Save the vCenter extension file in a directory that the vSphere Client can access, because you will need to register the vCenter extension plug-in from within the vSphere Client (see [Registering the vCenter Extension Plugin in the vCenter, on page 24](#)).
-

What to Do Next

Go to [Registering the vCenter Extension Plugin in the vCenter](#), on page 24.

Registering the vCenter Extension Plugin in the vCenter

This task is completed within your client desktop vSphere client directory

Before You Begin

See [Downloading the vCenter Extension File from the Cisco Prime NSC](#), on page 23.

-
- Step 1** From the VMware vSphere Client, log into the vCenter server.
 - Step 2** In the **vSphere Client** window, choose **Plug-ins > Manage Plug-ins**.
 - Step 3** Right-click the window background and choose **New Plug-in**.
 - Step 4** Browse to the Cisco Prime NSC vCenter extension file that you previously downloaded and click **Register Plug-in**. The vCenter Register Plug-in Window appears, displaying a security warning.
 - Step 5** In the security warning message box, click **Ignore**.
A progress indicator shows the task status.
 - Step 6** When the success message is displayed, click **OK**, then click **Close**.
-

What to Do Next

Go to [Configuring the vCenter in VM Manager in the Cisco Prime NSC](#), on page 24.

Configuring the vCenter in VM Manager in the Cisco Prime NSC

Before You Begin

See [Task 2: On the Cisco Prime NSC, Setting Up VM-Mgr for vCenter Connectivity](#), on page 23.

-
- Step 1** In Cisco Prime NSC, choose **Resource Management > VM Managers > VM Managers**.
 - Step 2** In the VM Managers pane, click the **Add VM Manager** tab.
 - Step 3** In the Add VM Manager dialog box, do the following:
 - a) In the **Name** field, enter the vCenter name (no spaces allowed).
 - b) In the **Description** field, enter a brief description of the vCenter.
 - c) In the **Hostname/IP Address** field, enter the vCenter IP address.
 - Step 4** Click **OK**.

Note A successfully added VM Manager is displayed with the following information:

- Admin State of *enable*
- Operational State of *up*
- VMware vCenter version

Task 3: On the VSM, Configuring the Cisco Prime NSC Policy Agent

After installing the Cisco Prime NSC, you must register the VSM with the Cisco Prime NSC policy.

Before You Begin

Make sure that you know the following:

- The Cisco Prime NSC policy-agent image is available on the VSM (for example, `vnmc-vsmpa.2.1.1e.bin`)



Note The string `vsmpa` must appear in the image name as highlighted.

- The IP address of the Cisco Prime NSC
- The shared secret password you defined during the Cisco Prime NSC installation
- That IP connectivity between the VSM and the Cisco Prime NSC is working



Note If you upgrade your VSM, you must also copy the latest Cisco VSM policy agent image. This image is available in the Cisco Prime NSC image bundle to boot from a flash drive and to complete registration with the Cisco Prime NSC.

Step 1

On the VSM, enter the following commands:

```
vsm# configure terminal
vsm(config)# vnm-policy-agent
vsm(config-vnm-policy-agent)# registration-ip 10.193.75.95
vsm(config-vnm-policy-agent)# shared-secret Example_Secret123
vsm(config-vnm-policy-agent)# policy-agent-image vnmc-vsmpa.2.1.1e.bin
vsm(config-vnm-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 2 Check the status of the VNM policy agent configuration to verify that you have installed the Cisco Prime NSC correctly and it is reachable by entering the **show vnm-pa status** command. This example shows that the Cisco Prime NSC is reachable and the installation is correct:

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsm
vsm
The VSM is now registered with the Cisco Prime NSC.
```

This example shows that the Cisco Prime NSC is unreachable or an incorrect IP is configured:

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installation Failure
VNM not reachable.
vsm#
```

This example shows that the VNM policy-agent is not configured or installed:

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

Task 4: On the VSM, Preparing Cisco VSG Port Profiles

To prepare Cisco VSG port profiles, you must create the VLANs and use the VLANs in the Cisco VSG data port profile and the Cisco VSG-ha port profile.

Before You Begin

Make sure that you know the following:

- The uplink port-profile name.
- The VLAN ID for the Cisco VSG data interface (for example, 100).
- The VLAN ID for the Cisco VSG-ha interface (for example, 200).
- The management VLAN (management).



Note None of these VLANs need to be system VLANs.

Step 1 On the VSM, create the VLANs by first entering global configuration mode using the following command:

```
vsm# configure
```

Step 2 Enter the following configuration commands:

```
vsm(config)# vlan 100
vsm(config-vlan)# no shutdown
vsm(config-vlan)# exit
vsm(config)# vlan 200
vsm(config-vlan)# no shutdown
vsm(config-vlan)# exit
vsm(config)# exit
```

```
vsm# configure
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 3 Press Ctrl-Z to exit.

Step 4 Create a Cisco VSG data port profile and a Cisco VSG-ha port profile by first enabling the Cisco VSG data port-profile configuration mode. Use the **configure** command to enter global configuration mode.

```
vsm# configure
```

Step 5 Enter the following configuration commands:

```
vsm(config)# port-profile VSG-Data
vsm(config-port-prof)# vmware port-group
vsm(config-port-prof)# switchport mode access
vsm(config-port-prof)# switchport access vlan 100
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# exit
vsm(config)#
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 6 Press Ctrl-Z to end the session.

Step 7 Enable the Cisco VSG-ha port profile configuration mode.

```
vsm# configure
```

Step 8 Enter the following configuration commands:

```
vsm(config)# port-profile VSG-HA
vsm(config-port-prof)# vmware port-group
vsm(config-port-prof)# switchport mode access
vsm(config-port-prof)# switchport access vlan 200
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 9 Add the VLANs created for the Cisco VSG data and Cisco VSG-ha interfaces as part of the allowed VLANs into the uplink port profile. Use the **configure** command to enter global configuration mode.

```
vsm# configure
```

Step 10 Enter the following configuration commands:

```
vsm(config)# port-profile type ethernet uplink
vsm(config-port-prof)# switchport trunk allowed vlan add 100, 200
vsm(config-port-prof)# exit
vsm(config)#
```

Step 11 Press Ctrl-Z to end the session.

Task 5: Installing the Cisco VSG from an OVA Template

Before You Begin

Make sure that you know the following:

- The Cisco VSG OVA image is available in the vCenter.
- Cisco VSG-Data and Cisco VSG-ha port profiles are created on the VSM.
- The management port profile (management)



Note The management port profile is the same port profile that is used for the VSM. The port profile is configured in the VSM and is used for the Cisco Prime NSC management interface.

- The Cisco VSG-Data port profile: VSG-Data
- The Cisco VSG-ha port profile: VSG-ha
- The HA ID
- The IP/subnet mask/gateway information for the Cisco VSG
- The admin password
- 2 GB RAM and 3 GB hard disk space are available
- The Cisco Prime NSC IP address
- The shared secret password
- The IP connectivity between Cisco VSG and Cisco Prime NSC is okay.
- The Cisco VSG VNM-PA image name (vnmc-vsgpa.2.1.1b.bin) is available.

-
- Step 1** Choose the host on which to deploy the Cisco VSG VM.
- Step 2** Choose **File > Deploy OVF Template**.
- Step 3** In the **Deploy OVF Template—Source** window, browse to the path to the Cisco VSG OVA file, and then click **Next**.
- Step 4** In the **Deploy OVF Template—OVF Template Details** window, review the product information including the size of the file and the VM disk, and then click **Next**.
- Step 5** In the **Deploy OVF Template—End User License Agreement** window, click **Accept** after reviewing the end user license agreement and then click **Next**.
- Step 6** In the **Deploy OVF Template—Name and Location** window, do the following:
- a) In the **Name** field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
 - b) In the **Inventory Location** pane, choose the location that you would like to use for hosting the Cisco VSG.
 - c) Click **Next**.
- Step 7** In the **Deploy OVF Template—Deployment Configuration** window, from the **Configuration** drop-down list, choose **Deploy medium VSG**, and then click **Next**.
- Step 8** In the **Deploy OVF Template—Datastore** window, choose the data store for the VM and click **Next**. The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN).
- Note** If only one storage location is available for an ESXi host, this window does not display and you are assigned to the one that is available.

- Step 9** In the **Deploy OVF Template—Disk Format** window, do the following:
- Click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks.
The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned. Ignore the red text in the window.
 - Click **Next**.
- Step 10** In the **Deploy OVF Template—Network Mapping** window, do the following:
- Choose **VSG Data** for the data interface port profile.
 - Choose **Management** for the management interface port profile.
 - Choose **VSG-ha** for the HA interface port profile .
 - Click **Next**.
- Note** In this example, for Cisco VSG-Data and Cisco VSG-ha port profiles created in the previous task, the management port profile is used for management connectivity and is the same as in the VSM and Cisco Prime NSC.
- Step 11** In the **Deploy OVF Template—Properties** window, do the following:
- In the **OvfDeployment** field, select **ovf** to continue the configuration. Select **ignore** for manual configuration.
 - From the **HARole** drop-down list, choose HA role.
 - In the **HAid** field, enter the high-availability identification number for a Cisco VSG pair (value from 1 through 4095).
 - In the **Password** field, enter a password that contains at least one uppercase letter, one lowercase letter, and one number.
 - In the **ManagementIPv4** field, enter the IP address for the Cisco VSG.
 - In the **ManagementIPv4 Subnet** field, enter the subnet mask.
 - In the **Gateway** field, enter the gateway name.
 - In the **VnmclpV4** field, enter the IP address of the Cisco Prime NSC.
 - In the **SharedSecret** field, enter the shared secret password defined during the Cisco Prime NSC installation.
 - Click **Next**.
- Note** For the shared secret password guidelines, see [Shared Secret Password Criteria](#), on page 47.
- Note** In the following step, make sure that red text messages do not appear before you click **Next**. If you do not want to enter valid information in the red-indicated fields, use null values to fill those fields. If those fields are left empty or filled with invalid null values, the application does not power on. Ignore the Cisco Prime NSC Restore fields.
- Step 12** In the **Ready to Complete** window, review the deployment settings information .
- Note** Review the IP/mask/gateway information carefully because any discrepancies might cause the VM to have bootup issues.
- Step 13** Click **Finish**. The **Deploying Nexus 1000VSG** dialog box opens.
The progress bar in the **Deploying Nexus 1000VSG** dialog box shows how much of the deployment task is completed before the Cisco Prime NSC is deployed.
- Step 14** Wait and click **Close** after the progress indicator shows that the deployment is completed successfully.
- Step 15** From your virtual machines, do one of the following:
- Right click and choose **Edit Settings**.
 - Click the **Getting Started** tab from the menu bar and then click the link **Edit Virtual Machine Settings**.
- Step 16** In the **Virtual Machine Properties** window, do the following:
- From the **CPUs** drop-down list, choose the appropriate vCPU number.
For older version of ESXi hosts, you can directly select a number for the vCPUs.

- b) From the **Number of Virtual Sockets** drop down list, choose the appropriate socket with cores.
For the latest version of ESXi hosts, you can directly select a number for the vCPUs.

Choosing 2 CPUs results in a higher performance.

Step 17 Power on the Cisco VSG VM.

Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status

You can use the **show vnm-pa status** command to verify the VNM policy-agent status (which can indicate that you have installed the policy-agent successfully).

Step 1 Log in to the Cisco VSG.

Step 2 Check the status of VNM-PA configuration by entering the following command:

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg
vsg#
```

Step 3 Log in to the Cisco Prime NSC.

Step 4 Choose **Resource Management > Resources > VSG**.

Step 5 Confirm that the table in the Clients window contains the registered value in the **Oper State** column for the Cisco VSG and VSM entries.

Task 7: On the Cisco Prime NSC, Configuring a Tenant and Security Profile

This task includes the following subtasks:

- [Configuring a Tenant on the Cisco Prime NSC, on page 31](#)
- [Configuring a Security Profile on the Cisco Prime NSC, on page 31](#)

Before You Begin

Make sure that you know the following:

- Supported Adobe Flash Player given in [System Requirements, on page 9](#)
- The IP address of the Cisco Prime NSC

- The password for Admin user

-
- Step 1** In your browser, enter `https://server-ip-address` where *server-ip-address* is the Cisco Prime NSC IP address.
- Step 2** In the **Website Security Certificate** window, choose **Continue to this website**.
- Step 3** In the Cisco Prime NSC login window, enter the username **admin** and the admin user password.
- Step 4** In the Cisco Prime NSC main window, choose **Administration > Service Registry > Clients** to check the Cisco VSG and VSM registration in the Cisco Prime NSC.
The **Clients** pane lists the Cisco VSG and VSM information.
-

What to Do Next

Go to [Configuring a Tenant on the Cisco Prime NSC](#), on page 31

Configuring a Tenant on the Cisco Prime NSC

Tenants are entities (businesses, agencies, institutions, and so on) whose data and processes are hosted on VMs on the virtual data center. To provide firewall security for each tenant, the tenant must first be configured in the Cisco Prime NSC.

-
- Step 1** In the Cisco Prime NSC, choose **Tenant Management > root**.
- Step 2** In the upper-right corner of the Tenant Management Root pane, click **Create Tenant**.
The tenant name can contain 1 to 32 alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created. The newly created tenant is listed in the navigation pane under root.
-

What to Do Next

Go to [Configuring a Security Profile on the Cisco Prime NSC](#), on page 31

Configuring a Security Profile on the Cisco Prime NSC

You can configure a security profile on the Cisco Prime NSC.

-
- Step 1** Choose **Policy Management > Service Profiles > root > tenant > Compute Firewall > Compute Security Profiles** where *tenant* is the required tenant.
- Step 2** In the General tab, click **Add Compute Security Profile**.
- Step 3** In the **Add Compute Security Profile** dialog box, enter a name and description for the security profile, and then click **OK**.
-

What to Do Next

Next, you need to add a compute firewall as described in [Task 9: On the Cisco Prime NSC, Adding a Compute Firewall, on page 32](#). While adding a compute firewall, you either instantiate a VSG service device from an image or assign a VSG or VSG pool. To instantiate a VSG service device from an image, you first need to import the VSG service image as described in [Task 8: On the Cisco Prime NSC, Importing Service Image, on page 32](#).

Task 8: On the Cisco Prime NSC, Importing Service Image

This step is required to instantiate a VSG service device from an image in [Task 9: On the Cisco Prime NSC, Adding a Compute Firewall, on page 32](#). This step is not required for assigning a VSG or VSG pool option in [Task 9: On the Cisco Prime NSC, Adding a Compute Firewall, on page 32](#).

-
- Step 1** Log in to the Cisco Prime NSC.
- Step 2** Choose **Resource Management > Resources > Service Devices > Images**.
- Step 3** Click **Import Service Image**.
- Step 4** In the Import Service Image dialog box, do the following:
- Enter a name and description for the image you are importing.
 - In the **Type** field, select **VSG**.
 - In the **Version** field, enter a version to assign to the image.
 - In the **Protocol** field, choose a protocol.
 - In the **Hostname / IP Address** field, enter the hostname or IP address of the remote host to which you downloaded the images.
 - In the **User Name** field, enter the account username for the remote host.
 - In the **Password** field, enter the account password for the remote host.
 - In the **Remote File** field, enter the absolute path and filename of the service image, starting with a slash, such as `/mnt/nexus-1000v.VSG2.1.1.ova`.
-

Task 9: On the Cisco Prime NSC, Adding a Compute Firewall

You can add a compute firewall and assign it to a Cisco VSG, thereby placing the Cisco VSG in service. A wizard walks you through the configuration process, which includes assigning a Cisco VSG, assigning profiles, and configuring interfaces.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in Cisco Prime NSC as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

Before You Begin

To place a Cisco VSG in service, at least one of the following must exist:

- To assign a Cisco VSG, an available Cisco VSG must be registered in Cisco Prime NSC. For more information, see [Task 6: On the Cisco VSG and Cisco Prime NSC, Verifying the VNM Policy-Agent Status](#), on page 30.
- To assign a Cisco VSG pool, a Cisco VSG pool must have at least one available Cisco VSG.
- To instantiate a Cisco VSG service device, a VM service image must be imported and VM Manager must be configured in the Cisco Prime NSC. For more information on importing service images, see [Task 8: On the Cisco Prime NSC, Importing Service Image](#), on page 32.

-
- Step 1** Log in to the Cisco Prime NSC.
- Step 2** Choose **Resource Management > Managed Resources > root > tenant > Compute Firewalls**.
- Step 3** In the General tab, click **Add Compute Firewall**.
The Add Compute Firewall Wizard opens.
- Step 4** In the Properties window, supply the information as described in the [Properties Window](#), on page 34, and then click **Next**.
- Step 5** In the Service Device window, select the required VSG service device as described in the [Service Device Window](#), on page 34, and then click **Next**.
- Step 6** (Instantiate option only) If you instantiate a VSG service device from an image, do one or both of the following in the Placement screen, then click **Next**:
- Navigate to and choose the host or resource pool to use for the VSG instance.
 - If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary VSG instance.
- Step 7** In the Interfaces window, configure interfaces as follows, and then click **Next**:
- If you assigned a VSG, enter the data IP address and subnet mask.
 - If you assigned a VSG pool, enter the data IP address and subnet mask.
 - If you instantiated a VSG service device without high availability, add management and data interfaces.
 - If you instantiated a VSG service device with high availability, add management, data, and HA interfaces.
- For field-level help when configuring the interfaces, see the online help.
- Step 8** In the Summary window, confirm that the information is correct, and then click **Finish**.
-

Properties Window

Field	Description
Name	<p>Compute firewall name.</p> <p>This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.</p>
Description	Compute firewall description.
Host Name	Management hostname of the firewall.
Device Configuration Profile	<p>Do either of the following:</p> <ul style="list-style-type: none"> • Click the profile name to view or optionally modify the currently assigned device configuration profile. • Click Select to choose a different device configuration profile.

Service Device Window

Field	Description
Assign VSG	<p>Assign a VSG to the compute firewall.</p> <p>In the VSG Device drop-down list, choose the required service device.</p>
Assign VSG Pool	<p>Assign a VSG pool to the compute firewall.</p> <p>In the VSG Pool field, either choose the required pool from the drop-down list or click Add Pool to add a new pool.</p>

Field	Description
Instantiate	<p>Instantiate a VSG service device from an available image.</p> <ol style="list-style-type: none"> 1 In the list of available images, select the image to use to instantiate a new VSG service device. 2 In the High Availability field, check the Enable HA check box to enable high availability. 3 In the VM Access password fields, enter the password for the admin user account.

Task 10: On the Cisco Prime NSC, Configuring a Permit-All Rule

You can configure a permit-all rule in the Cisco Prime NSC.

-
- Step 1** Log in to the Cisco Prime NSC.
- Step 2** In the Cisco Prime NSC window, choose **Policy Management > Service Profiles**.
- Step 3** In the **Service Profile** window, choose **root > tenant > Compute Security-Profiles > SP1**.
- Step 4** In the right pane, click **Add ACL Policy Set**.
- Step 5** In the Add ACL Policy Set dialog box, enter a name and description for the policy set, and then click **Add ACL Policy**.
- Step 6** In the **Add ACL Policy** dialog box, enter a name and description for the policy, and then click **Add Rule** above the **Name** column.
- Step 7** In the **Add ACL Policy Rule** dialog box, do the following:
- a) In the **Name** field, enter the rule name.
 - b) In the **Description** field, enter a description for the rule.
 - c) In the **Action To Take** area, choose **permit**.
 - d) In the **Condition Match Criteria** field, select a matching condition.
 - e) In the **Source Conditions** field, enter the source condition of the rule.
 - f) In the **Destination Conditions** field, enter the destination condition of the rule.
 - g) In the **Service** field, enter the service expression.
 - h) In the **Protocol** tab, select a protocol for the rule.
 - i) In the **Ether Type** tab, specify the ether type for the rule.
 - j) Click **OK**.
- Step 8** In the **Add ACL Policy** dialog box, click **OK**.
The newly created policy is displayed in the **Assigned** field.
- Step 9** In the **Add ACL Policy Set** dialog box, click **OK**.
- Step 10** In the **Security Profile** window, click **Save**.
-

Task 11: On the Cisco VSG, Verifying the Permit-All Rule

You can verify the rule presence in the Cisco VSG, by using the Cisco VSG CLI and the **show** commands.

```
vsg# show running-config | begin security
security-profile SP_web@root/Tenant-A
  policy PS_web@root/Tenant-A
    custom-attribute vnsporg "root/tenant-a"
security-profile default@root
  policy default@root
    custom-attribute vnsporg "root"
rule Pol_web/permit-all@root/Tenant-A cond-match-criteria: match-all
  action permit
  action log
rule default/default-rule@root cond-match-criteria: match-all
  action drop
Policy PS_web@root/Tenant-A
  rule Pol_web/permit-all@root/Tenant-A order 101
Policy default@root
  rule default/default-rule@root order 2
```

Task 12: Enabling Logging

To enable logging follow these procedures:

- [Enabling Policy-Engine Logging in a Monitor Session, on page 36](#)
- [Enabling Global Policy-Engine Logging, on page 37](#)

Enabling Policy-Engine Logging in a Monitor Session

Configuring a syslog policy enables you to specify the level of syslog messages to log and where to log the messages.

-
- Step 1** Log in to the Cisco Prime NSC.
 - Step 2** In the Cisco Prime NSC window, choose **Policy Management > Device Configurations > root > Policies > Syslog**.
 - Step 3** In the Syslog table, select **default**, then click **Edit**.
 - Step 4** In the **Edit Syslog** dialog box, click the **Servers** tab.
 - Step 5** In the Syslog Policy table, select the primary server type, then click **Edit**.
 - Step 6** In the **Edit Syslog Client** dialog box, provide the following information, then click **OK** in the open dialog boxes:
 - Hostname/IP Address—Enter the syslog server IP address or hostname.
 - Severity—Choose **information (6)**.
 - Admin State—Choose **enabled**.
-

What to Do Next

Go to [Enabling Global Policy-Engine Logging](#), on page 37.

Enabling Global Policy-Engine Logging

Logging enables you to see what traffic is going through your monitored VM. This logging is helpful for verifying that you have a proper configuration and to help in troubleshooting.

-
- Step 1** Log in to the Cisco Prime NSC.
- Step 2** In the Cisco Prime NSC window, choose **Policy Management > Device Configurations > root > Device Profiles > default**. The **default** Device Profile window opens.
- Step 3** In the Device Profiles pane, click the **Policies** tab.
- Step 4** In the Policy Engine Logging area at the lower-right of the Policies tab, click **Enabled**, and then click **Save**.
-

Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG

This section includes the following topics:

[Enabling Traffic VM Port-Profile for Firewall Protection](#), on page 38

[Verifying the VSM or VEM for Cisco VSG Reachability](#), on page 38

[Checking the VM Virtual Ethernet Port for Firewall Protection](#), on page 39

Before You Begin

Make sure that you know the following:

- The server virtual machine that runs with an access port profile (for example, web server)
- The Cisco VSG data IP address (10.10.10.200) and VLAN ID (100)
- The security profile name (for example, sp-web)
- The organization (Org) name (for example, root/Tenant-A)
- The port profile that you would like to edit to enable firewall protection
- That one active port in the port-profile with vPath configuration has been set up

Enabling Traffic VM Port-Profile for Firewall Protection

You can enable a traffic VM port profile for traffic protection.

Verify the traffic VM port profile before firewall protection.

```
vsm(config)# port-profile type vethernet pp-webserver
vmware port-group
switchport mode access
switchport access vlan 756
no shutdown
state enabled
```

Enable firewall protection.

```
VSM(config)# port-profile pp-webserver
VSM(config-port-prof)# vservice node vsgr profile SP_web
VSM(config-port-prof)# org root/Tenant-A
Verify the traffic VM port profile after firewall protection.
```

```
VSM(config)# port-profile type vethernet pp-webserver
vmware port-group
switchport mode access
switchport access vlan 756
org root/Tenant-A
vservice node vsgr profile SP_web
no shutdown
state enabled
```

What to Do Next

Go to [Verifying the VSM or VEM for Cisco VSG Reachability](#), on page 38.

Verifying the VSM or VEM for Cisco VSG Reachability

This example shows how to verify the communication between the VEM and the VSG:

```
vsm(config)# show vservice brief
-----
License Information
-----
Type In-Use-Lic-Count UnLicensed-Mod
asa 0

-----
Node Information
-----
ID Name Type IP-Address Mode State Module
2 VSG-L2-V vsgr 10.1.1.251 v-920 Alive 3,6,

-----
Path Information
-----
Port Information
-----
PortProfile:Vsg215
```

```

Org:root/T1
Node:VSG-L2-V(10.1.1.251) Profile(Id):sp11(5)
Veth Mod VM-Name vNIC IP-Address
9 6 inside_vm 1 10.1.1.81
19 3 outside_vm 1 10.1.1.82

```

A display showing the MAC-ADDR Listing and Up state verifies that the VEM can communicate with the Cisco VSG.



Note In order to see the above status, one active port in the port profile with vPath configuration needs to be up.

Checking the VM Virtual Ethernet Port for Firewall Protection

This example shows how to verify the VM Virtual Ethernet port for firewall protection:

```
VSM(config)# show vservice port brief vethernet 23
```

```
-----
Port Information
-----
```

```

PortProfile:pp-webserver
Org:root/Tenant-A
Node:vsg1(40.40.40.40) Profile(Id):SP_web(29)
Veth Mod VM-Name vNIC IP-Address
23 4 vm1 2 14.14.14.21

```



Note Make sure that your VNISP ID value is greater than 1.

Task 14: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

This section includes the following topics:

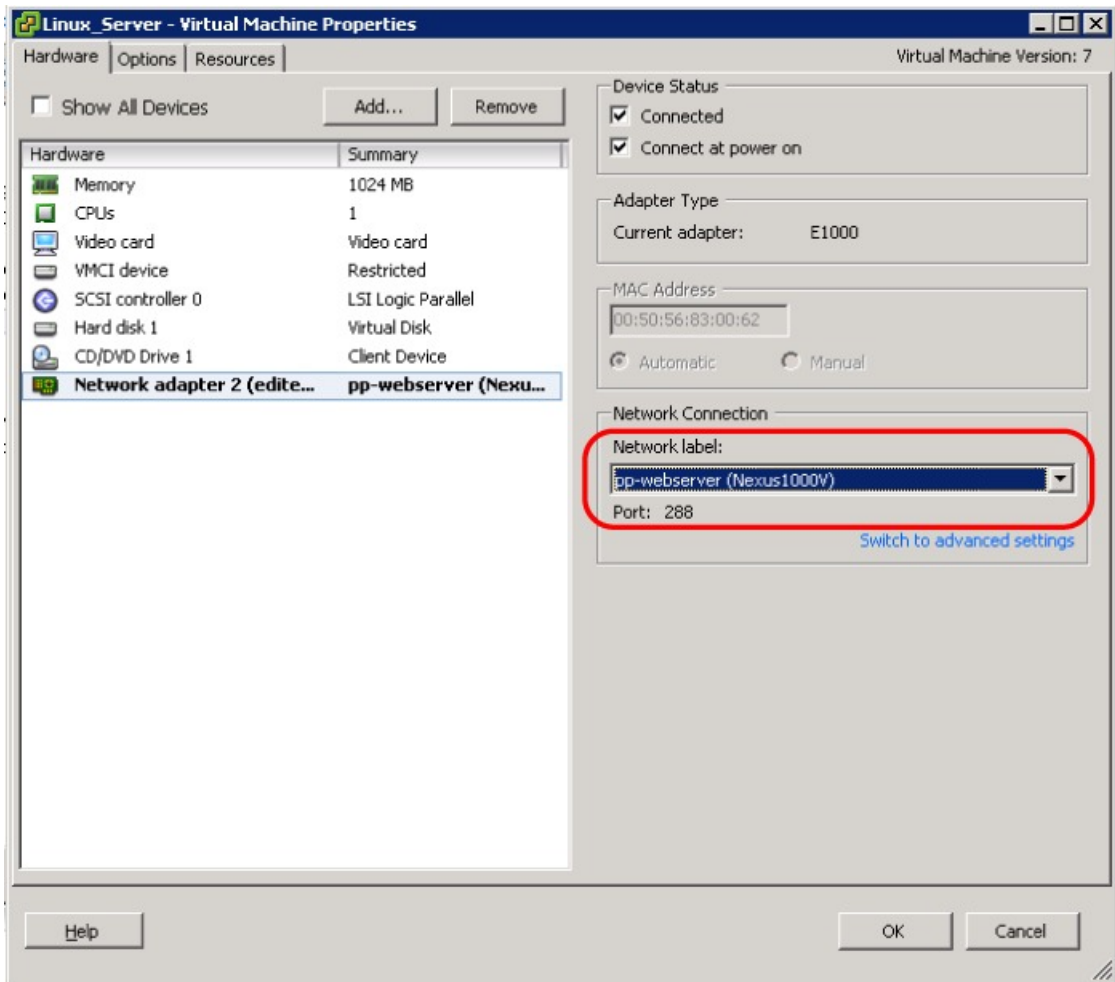
- [Sending Traffic Flow, on page 40](#)
- [Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 41](#)

Sending Traffic Flow

You can send traffic flow through the Cisco VSG to ensure that it is functioning properly.

Step 1 Ensure that the VM (Server-VM) is using the port profile (pp-webserver) configured for firewall protection.

Figure 6: Virtual Machine Properties Window



Step 2 In the **Virtual Machine Properties** window, do the following:

- Log in to any of your client virtual machine (Client-VM).
- Send traffic (for example, HTTP) to your Server-VM.

```
[root@]# wget http://172.31.2.92/
--2010-11-28 13:38:40-- http://172.31.2.92/
Connecting to 172.31.2.92:80... connected.
HTTP request sent, awaiting response... 200 OK
```

```

Length: 258 [text/html]
Saving to: `index.html'

100%[=====>] 258      --.-K/s
   in 0s

2010-11-28 13:38:40 (16.4 MB/s) - `index.html' saved [258/258]

[root]#

```

Step 3 Check the policy-engine statistics and log on the Cisco VSG.

What to Do Next

Go to [Verifying Policy-Engine Statistics and Logs on the Cisco VSG](#), on page 41.

Verifying Policy-Engine Statistics and Logs on the Cisco VSG

Log in to the Cisco VSG and check the policy-engine statistics and logs.

This example shows how to check the policy-engine statistics and logs:

```

vsg# show policy-engine stats
Policy Match Stats:
default@root          :          0
  default/default-rule@root :      0 (Drop)
  NOT_APPLICABLE       :          0 (Drop)

PS_web@root/Tenant-A :          1
  pol_web/permit-all@root/Tenant-A :      1 (Log, Permit)
  NOT_APPLICABLE       :          0 (Drop)

vsg# terminal monitor
vsg# 2010 Nov 28 05:41:27 firewall %POLICY_ENGINE-6-POLICY_LOOKUP_EVENT:
policy=PS_web@root/Tenant-A rule=pol_web/permit-all@root/Tenant-A action=Permit
direction=egress src.net.ip-address=172.31.2.91 src.net.port=48278
dst.net.ip-address=172.31.2.92 dst.net.port=80 net.protocol=6 net.ethertype=800

```




Installing Cisco Prime Network Services Controller

This chapter contains the following sections:

- [Information About the Cisco Prime NSC](#) , page 43
- [Installation Requirements](#), page 43
- [ESXi Server Requirement](#), page 48
- [Installing Cisco Prime NSC](#), page 48

Information About the Cisco Prime NSC

The Cisco Prime Network Services Controller (Cisco Prime NSC) is a virtual appliance that provides centralized device and security policy management for Cisco virtual services. Designed to support enterprise and multiple-tenant cloud deployments, the Cisco Prime NSC provides transparent, seamless, and scalable management for securing virtualized data center and cloud environments.

Installation Requirements

Cisco Prime NSC System Requirements

Requirement	Description
Virtual Appliance	
Four Virtual CPUs	1.5 GHz for each virtual CPU
Memory	4 GB RAM

Requirement	Description
Disk Space	<p>One of the following, depending on InterCloud functionality:</p> <ul style="list-style-type: none"> • With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows: <ul style="list-style-type: none"> ◦ Disk 1: 20 GB ◦ Disk 2: 200 GB • Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: <ul style="list-style-type: none"> ◦ Disk 1: 20 GB ◦ Disk 2: 20 GB
Management interface	One management network interface
Processor	<p>x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix</p> <p>Note You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php.</p>
VMware	
VMware vSphere	ESXi 5.0, 5.1, and 5.5
VMware vCenter	Release 5.5 (5.1 vCenter supports host version upto 5.1)
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Any of the following: <ul style="list-style-type: none"> • Microsoft Windows • Apple Mac OS
Browser	Any of the following browsers: <ul style="list-style-type: none"> • Internet Explorer 9.0 or higher • Mozilla Firefox 23.0 or higher • Google Chrome 29.0 or higher <p>Note If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website.</p> <p>Note Before using Google Chrome with Cisco Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco Prime NSC, on page 47.</p>
Flash Player	Adobe Flash Player plugin 11.2 or higher

Firewall Ports Requiring Access

Requirement	Description
80	HTTP/TCP
443	HTTPS
843	Adobe Flash

Information Required for Installation and Configuration

Information Type	Your Information
For Deploying the Cisco Prime NSC OVA	
Name	
Location of files	
Datastore location	
Storage location, if more than one location is available	
Management port profile name for VM management Note The management port profile is the same port profile that is used for VSM. The port profile is configured in VSM and is used for the Cisco Prime NSC management interface.	
IP address	
Subnet mask	
Gateway IP address	
Domain name	
DNS server	
NTP server	
Admin password	
Shared secret password for communications between the Cisco Prime NSC, Cisco VSG, and VSM.	
For Configuring VMware vCenter in Cisco Prime NSC	
vCenter name	
Description	
Hostname or IP address	

Shared Secret Password Criteria

A shared secret password is a password that is known only to those using a secure communication. Passwords are designated strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between the Cisco Prime NSC, Cisco VSG, and VSM, adhere to the following criteria for setting valid, strong passwords:

Do not include the following items in passwords:

- Characters: & ' " ` () < > | \ ; \$
- Spaces

Create strong passwords based on the following characteristics:

Table 1: Characteristics of Strong Passwords

Strong passwords have...	Strong passwords do not have...
<ul style="list-style-type: none"> • At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters. 	<ul style="list-style-type: none"> • Consecutive characters, such as <i>abcd</i>. • Characters repeated three or more times, such as <i>aaabbb</i>. • A variation of the word Cisco, such as <i>cisco</i>, <i>ocsic</i>, or one that changes the capitalization of letters in the word <i>Cisco</i>. • The username or the username in reverse. • A permutation of characters present in the username or <i>Cisco</i>.

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Configuring Chrome for Use with Cisco Prime NSC

To use Chrome with Cisco Prime NSC, you must disable the Adobe Flash Players that are installed by default with Chrome.

**Note**

You must perform this procedure each time your client machine reboots. Chrome automatically enables the Adobe Flash Players when the system on which it is running reboots.

-
- Step 1** In the Chrome URL field, enter `chrome://plugins`.
- Step 2** Click **Details**.
- Step 3** Locate the Adobe Flash Player plugins, and disable each one.
- Step 4** Download and install Adobe Flash Player version 11.6.602.180.
- Step 5** Close and reopen Chrome before logging into the Cisco Prime NSC
-

ESXi Server Requirement

You must set the clock to the correct time on all ESXi servers that will run Cisco Prime NSC, ASA 1000V instances, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco Prime NSC CA certificate that is created when the Cisco Prime NSC VM is deployed might have an invalid time stamp. An invalid time stamp can prevent you from successfully registering ASA 1000V instances to the Cisco Prime NSC.

After you set the clock to the correct time on all ESXi servers that run the Cisco Prime NSC, you can, as an option, set the clock on the Cisco Prime NSC as follows:

- If you set the clock manually, be sure to enter the correct time zone as a Coordinated Universal Time (UTC) offset.
- If you set the clock by synchronizing with the Network Time Protocol (NTP), you can select the UTC time zone.

Installing Cisco Prime NSC

You can deploy the Cisco Prime NSC OVA, resulting in a Cisco Prime NSC VM.

Before You Begin

- Set your keyboard to United States English before installing the Cisco Prime NSC and using the VM console.
- Verify that the Cisco Prime NSC OVA image is available in the vSphere client.
- Make sure that all system requirements are met as recommended in [Cisco Prime NSC System Requirements](#), on page 43.
- Make sure you have the information identified as in [Information Required for Installation and Configuration](#).

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

-
- Step 1** Use the VMware vSphere Client to log into the vCenter server.
- Step 2** Choose the host on which to deploy the Cisco Prime NSC VM.
- Step 3** From the File menu, choose **Deploy OVF Template**.
- Step 4** In the **Source** window, choose the Cisco Prime NSC OVA, then click **Next**.
- Step 5** In the **OVF Template Details** window, review the details of the Cisco Prime NSC template, and then click **Next**.
- Step 6** In the **End User License Agreement** window, click **Accept** after reviewing the End User License Agreement, and then click **Next**.
- Step 7** In the **Name and Location** window, provide the required information, and then click **Next**.
The name can contain up to 80 characters and must be unique within the inventory folder.
- Step 8** In the **Deployment Configuration** window, choose **Installer** from the Configuration drop-down list, then click **Next**.
- Step 9** In the **Datastore** window, select the data store for the VM, and then click **Next**.
Note The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN). If only one storage location is available for an ESXi host, this window does not display and you are assigned to the one that is available.
- Step 10** In the **Disk Format** window, click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks, and then click **Next**.
The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.
- Step 11** In the **Network Mapping** window, select the management network port group for the VM, then click **Next**.
- Step 12** In the **Properties** window, provide the required information, address any errors described in the red text messages below the selection box, and then click **Next**. If needed, you can enter placeholder information as long as your entry meets the field requirements.
Note You can safely ignore the Cisco Prime NSC Restore fields.
Note For choosing the shared secret password, follow the guidelines given in [Shared Secret Password Criteria](#), on page 47.
- Step 13** In the **Ready to Complete** window, review the deployment settings information, and then click **Finish**.
Caution Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information.
A progress indicator shows the task progress until Cisco Prime NSC is deployed.
- Step 14** After Cisco Prime NSC is successfully deployed, click **Close**.
-



Installing the Cisco VSG

This chapter contains the following sections:

- [Information About the Cisco VSG, page 51](#)
- [Prerequisites for Installing the Cisco VSG Software, page 53](#)
- [Obtaining the Cisco VSG Software, page 53](#)
- [Installing the Cisco VSG Software, page 53](#)
- [Configuring Initial Settings, page 57](#)
- [Verifying the Cisco VSG Configuration, page 60](#)
- [Where to Go Next, page 60](#)

Information About the Cisco VSG

This section describes how to install and complete the basic configuration of the Cisco VSG for VMware vSphere software.

- [Host and VM Requirements, on page 51](#)
- [Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology, on page 52](#)

Host and VM Requirements

The Cisco VSG has the following requirements:

- ESXi platform running VMware software release 5.x and requiring a minimum of 4 GB RAM to host a Cisco VSG VM
- Virtual Machine (VM)
 - 32-bit VM is required and “Other 2.6.x (32-bit) Linux” is a recommended VM type.
 - 2 processors (1 processor is optional.)
 - 2-GB RAM

- 3 NICs (1 of type VMXNET3 and 2 of type E1000)
 - Minimum of 3 GB of SCSI hard disk with LSI Logic Parallel adapter (default)
 - Minimum CPU speed of 1 GHz
- There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology

The following table lists the terminology is used in the Cisco VSG implementation.

Term	Description
Distributed Virtual Switch (DVS)	Logical switch that spans one or more VMware ESX servers. It is controlled by one VSM instance.
ESXi	Virtualization platform used to create the virtual machines as a set of configuration and disk files.
NIC	Network interface card.
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging: <ul style="list-style-type: none"> • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	Platform-independent method of packaging and distributing Virtual Machines (VMs).
vCenter Server	Service that acts as a central administrator for VMware ESXi hosts that are connected on a network. vCenter Server directs actions on the VMs and the VM hosts (the ESXi hosts).
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a VMware ESX 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 the VMware vCenter Server.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
VMotion	Practice of migrating virtual machines live from server to server. (The Cisco VSGs cannot be moved by VMotion.)

Term	Description
vPath	Component in the Cisco Nexus 1000V Series switch with a VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual device that runs on a virtual machine (VM) and is based on Cisco NX-OS.
vSphere Client	User interface that enables users to connect remotely to the vCenter Server or ESXi from any windows PC. The primary interface for creating, managing, and monitoring VMs, their resources, and their hosts. It also provides console access to VMs.

Prerequisites for Installing the Cisco VSG Software

The following components must be installed and configured:

- On the Cisco Nexus 1000V Series switch, configure two VLANs, a service VLAN, and an HA VLAN on the switch uplink ports. (The VLAN does not need to be the system VLAN.)
- On the Cisco Nexus 1000V Series switch, configure two port profiles for the Cisco VSG: one for the service VLAN and the other for the HA VLAN. (You will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000V Series switch can communicate with it.)

Details about configuring VLANs and port profiles on the Cisco Nexus 1000V Series switch are available in the Cisco Nexus 1000V Series switch documentation.

Obtaining the Cisco VSG Software

You can obtain the Cisco VSG software files at this URL:

<http://www.cisco.com/en/US/products/ps13095/index.html>

Installing the Cisco VSG Software

You can install the Cisco VSG software on a VM by using an open virtual appliance (OVA) file or an ISO image file from the CD. Depending upon the type of file that you are installing, use one of the installation methods described in the following topics

- [Installing the Cisco VSG Software from an OVA File](#), on page 54
- [Installing the Cisco VSG Software from an ISO File](#), on page 55

Installing the Cisco VSG Software from an OVA File

To install the Cisco VSG software from an OVA file, obtain the OVA file and either install it directly from the URL or copy the file to the local disk from where you connect to the vCenter Server.

Before You Begin

- Specify a name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Know the name of the host where the Cisco VSG will be installed in the inventory folder.
- Know the name of the datastore in which the VM files will be stored.
- Know the names of the network port profiles used for the VM.
- Know the Cisco VSG IP address.
- Know the mode in which you will be installing the Cisco VSG:
 - Standalone
 - HA Primary
 - HA Secondary
 - Manual Installation

-
- Step 1** Choose the host on which to deploy the Cisco VSG VM.
- Step 2** Choose **File > Deploy OVF Template**.
- Step 3** In the **Deploy OVF Template—Source** window, do the following:
- Browse to the path to the Cisco VSG OVA file in the **Deploy from a file or URL** field.
 - Click **Next**. The **Deploy OVF Template—OVF Template Details** window opens.
- Step 4** In the **Deploy OVF Template—OVF Template Details** window, review the product information including the size of the file and the VM disk and then click **Next**.
- Step 5** In the **Deploy OVF Template—End User License Agreement** window, click **Accept** after reviewing the end user license agreement, and then click **Next**.
- Step 6** In the **Deploy OVF Template—Name and Location** window, do the following:
- In the **Name** field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
 - In the **Inventory Location** pane, choose the location that you would like to use for hosting the Cisco VSG.
 - Click **Next**.
- Step 7** In the **Deploy OVF Template—Deployment Configuration** window, do the following:
- From the **Configuration** drop-down list, choose **Standalone**.

b) Click **Next**.

Note The Standalone Installation for this document is an example in this publication. If you chose Manual Installation mode, you would choose the default values for the following steps. In Standalone mode, be sure to fill in all the fields indicated (they will be indicated on the GUI with red type).

Step 8 In the **Disk Format** dialog box, choose the radio button for the selected format and click **Next**.

Step 9 In the **Host or Cluster** window, choose the host where the Cisco VSG will be installed, and then click **Next**.

Step 10 From the **Select a datastore** field in which to store the VM files pane, choose your datastore, and then click **Next**.

Step 11 Click the drop-down arrows for Data (Service), Management, and HA to associate port profiles, and then click **Next**.

Step 12 In the **Deploy OVF Template—Properties** window, do the following:

- a) In the **HaId** field, enter the high-availability identification number for a Cisco VSG pair (value from 1 through 4095).
- b) In the **Password** field, enter a password that contains at least one uppercase letter, one lowercase letter, and one number.
- c) In the **ManagementIPv4** field, enter the IP address for the Cisco VSG.
- d) In the **ManagementIPv4 Subnet** field, enter the subnet mask.
- e) In the **Gateway** field, enter the gateway name.
- f) In the **VnmcIPv4** field, enter the IP address of the Cisco Prime NSC.
- g) In the **SharedSecret** field, enter the shared secret password defined during the Cisco Prime NSC installation.
- h) In the **ImageName** field, enter the VSG VNM-PA image name (vnmc-vsgpa.2.1.1b.bin).
- i) Click **Next**.

Note In the following step, make sure that red text messages do not appear before you click **Next**. If you do not want to enter valid information in the red-indicated fields, use null values to fill those fields. If those fields are left empty or filled with invalid null values, the application does not power on. Ignore the Cisco Prime NSC Restore fields.

Step 13 In the **Ready to Complete** window, review the deployment settings information.

Note Review the IP/mask/gateway information carefully because any discrepancies might cause the VM to have bootup issues.

Step 14 Click **Finish**. The **Deploying Nexus 1000VSG** dialog box opens.

The progress bar in the **Deploying Nexus 1000VSG** dialog box shows how much of the deployment task is completed before the Cisco Prime NSC is deployed.

Step 15 Wait and click **Close** after the progress indicator shows that the deployment is completed successfully.

Step 16 Power on the Cisco VSG VM.

Step 17 If you chose the Standalone mode for installation earlier, you now see the Cisco VSG login prompt. Log in with your Cisco VSG administration password. You may now proceed with configuring the Cisco Virtual Security Gateway. For details, see the *Cisco Virtual Security Gateway for VMware vSphere Configuration Guide*.

Step 18 If you chose the manual installation in the Configuration field earlier, see [Configuring Initial Settings, on page 57](#) to configure the initial settings on the Cisco VSG.

Note If you are installing high availability (HA), you must configure the software on the primary Cisco VSG before installing the software on the secondary Cisco VSG.

Installing the Cisco VSG Software from an ISO File

You can install the Cisco VSG from an ISO file.

Before You Begin

- Specify a name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Know the name of the host where the Cisco VSG will be installed in the inventory folder.
- Know the name of the datastore in which the VM files will be stored.
- Know the names of the network port profiles used for the VM.
- Know the Cisco VSG IP address.

-
- Step 1** Upload the Cisco Virtual Security Gateway ISO image to the vCenter datastore.
- Step 2** From the data center in the vSphere Client menu, choose your ESXi host where you want to install the Cisco VSG and choose **New Virtual Machine**.
For VM requirements, see the [Host and VM Requirements, on page 51](#).
For detailed information about how to create a VM, see the VMware documentation.
- Step 3** In the **Create New Virtual Machine** dialog box, do the following:
- Click **Custom** to create a virtual machine.
 - Click **Next**.
- Step 4** In the **Create New Virtual Machine** dialog box, do the following:
- In the **Name** field, add a name for the Cisco VSG.
The Cisco VSG name must be a unique name within the inventory folder and should be up to 80 characters.
 - In the **Inventory Location** field, choose your data center and click **Next**.
- Step 5** In the **Datastore** dialog box, choose your datastore from the **Select a datastore** and then click **Next**.
- Step 6** In the **Virtual Machine Version** dialog box, click the **Virtual Machine Version**.
Note Keep the selected virtual machine version.
- Step 7** In the **Guest Operating System** dialog box, do the following:
- Click the **Linux** radio button.
 - In the **Version** field, choose **Other 2.6x Linux (32-bit)** from the drop-down list and click **Next**.
- Step 8** In the **CPUs** dialog box, choose 1 socket with 2 cores or 2 sockets each with one core, and then click **Next**.
By default, the Cisco VSG virtual machine deployed with OVA has only one vCPU. You can choose 2 vCPUs. For an older version of the ESX hosts, you can directly select the number of vCPUs.
- Step 9** In the **Memory** dialog box, choose **2 GB** memory size, and then click **Next**.
- Step 10** In the **Create Network Connectors** dialog box, do the following:
- In the **How many NICs do you want to connect?** field, choose **3** from the drop-down list.
 - In the Network area, choose **service, management, and HA** port profiles in that sequence for the NIC 1, NIC 2, and NIC 3 from the drop-down list. Choose **VMXNET3** for the adapter type for NIC 1. Choose **E1000** for the adapter type for NIC 2 and NIC 3.
- Step 11** Click **Next**. The **SCSI Controller** dialog box opens.
The radio button for the default SCSI controller is chosen.
- Step 12** Click **Next**. The **Select a Disk** dialog box opens.

The radio button for the default disk is chosen.

- Step 13** Click **Next**. The **Create a Disk** dialog box opens. The default virtual disk size and policy is chosen.
- Step 14** Click **Next**. The **Advanced Options** dialog box opens. The default options are chosen.
- Step 15** Click **Next**. The **Ready to Complete** dialog box opens.
- Step 16** Review your settings in the **Settings for the new virtual machine** area.
- Step 17** Check the **Edit the virtual machine before completion** check box and click **Continue** to open a dialog box with the device details.
- Step 18** In the Work pane, choose your **New CD/DVD (adding)** in the **Hardware** area.
- Step 19** Click **Datastore ISO File**, and select your ISO file from the drop-down list.
- Step 20** In the work pane, check the **Connect at power on** check box and click **Finish**. The **Summary tab** window opens. The **Create virtual machine status** completes.
- Step 21** From the **vSphere Client** menu, choose your recently installed VM.
- Step 22** In the work pane, click **Power on the virtual machine**.
- Step 23** Click the **Console** tab to view the VM console. Wait for the Install Virtual Firewall and bring up the new image to boot. See the Configuring Initial Settings section to configure the initial settings on the Cisco VSG.
- Note** To allocate additional RAM, right-click the **VM** icon to power off the VM and then choose **Power > Power Off** from the dialog box. After the VM is powered down, edit the configuration settings on the VM for controlling memory resources.

Configuring Initial Settings

This section describes how to configure the initial settings on the Cisco VSG and configure a standby Cisco VSG with its initial settings. For configuring a standby Cisco VSG, see [Configuring Initial Settings on a Standby Cisco VSG, on page 59](#) section.

When you power on the Cisco VSG for the first time, depending on which mode you used to install your Cisco VSG, you might be prompted to log in to the Cisco VSG to configure initial settings at the console on your vSphere Client. For details about installing Cisco VSG, see [Installing the Cisco VSG Software, on page 53](#) in this chapter.

Before You Begin

The following table determines if you must configure the initial settings as described in this section.

Your Cisco Virtual Security Gateway Software Installation Method	Do You Need to Proceed with “Configuring Initial Settings”?
Installing an OVA file and choosing Manually Configure Nexus 1000 VSG in the configuration field during installation.	Yes. Proceed with configuring initial settings described in this section.

Your Cisco Virtual Security Gateway Software Installation Method	Do You Need to Proceed with "Configuring Initial Settings"?
Installing an OVA file and choosing any of the options other than the manual method in the configuration field during installation.	No. You have already configured the initial settings during the OVA file installation.
Installing an ISO file.	Yes. Proceed with configuring initial settings described in this section.

-
- Step 1** Navigate to the **Console** tab in the VM. Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.
- Step 2** At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.
- Step 3** At the prompt, confirm the admin password and press **Enter**.
- Step 4** At the `Enter HA role[standalone/primary/secondary]` prompt, enter the HA role you want to use and press **Enter**.
This can be one of the following:
- standalone
 - primary
 - secondary
- Step 5** At the `Enter the ha id(1-4095)` prompt, enter the HA ID for the pair and press **Enter**.
Note If you entered secondary in the earlier step, the HA ID for this system must be the same as the HA ID for the primary system.
- Step 6** If you want to perform basic system configuration, at the `Would you like to enter the basic configuration dialog (yes/no)` prompt, enter **yes** and press **Enter**, then complete the following steps.
- a) At the `Create another login account (yes/no) [n]` prompt, do one of the following:
- To create a second login account, enter **yes** and press **Enter**.
 - Press **Enter**.
- b) (Optional) At the `Configure read-only SNMP community string (yes/no) [n]` prompt, do one of the following:
- To create an SNMP community string, enter **yes** and press **Enter**.
 - Press **Enter**.

c) At the Enter the Virtual Security Gateway (VSG) name prompt, enter **VSG-demo** and press **Enter**.

- Step 7** At the Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: prompt, enter **yes** and press **Enter**.
- Step 8** At the Mgmt IPv4 address: prompt, enter **10.10.10.11** and press **Enter**.
- Step 9** At the Mgmt IPv4 netmask prompt, enter **255.255.255.0** and press **Enter**.
- Step 10** At the Configure the default gateway? (yes/no) [y] prompt, enter **yes** and press **Enter**.
- Step 11** At the Enable the telnet service? (yes/no) [y]: prompt, enter **no** and press **Enter**.
- Step 12** At the Enable the telnet service? (yes/no) [y]: prompt, enter **no**.
- Step 13** At the Configure the ntp server? (yes/no) [n] prompt, enter **no** and press **Enter**.
The following configuration will be applied:
- ```
Interface mgmt0
ip address 10.10.10.11 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/10.10.11.1
no telnet server enable
ssh key rsa 768 force
ssh server enable
no feature http-server
ha-pair id 25
```
- Step 14** At the Would you like to edit the configuration? (yes/no) [n] prompt, enter **n** and press **Enter**.
- Step 15** At the Use this configuration and save it? (yes/no) [y]: prompt, enter **y** and press **Enter**.
- Step 16** At the VSG login prompt, enter the name of the admin account you want to use and press **Enter**.  
The default account name is admin.
- Step 17** At the Password prompt, enter the name of the password for the admin account and press **Enter**.  
You are now at the Cisco VSG node.

## Configuring Initial Settings on a Standby Cisco VSG

You can add a standby Cisco VSG by logging in to the Cisco VSG you have identified as secondary and using the following procedure to configure a standby Cisco VSG with its initial settings.

- Step 1** Navigate to the **Console** tab in the VM.  
Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.
- Step 2** At the Enter the password for "admin" prompt, enter the password for the admin account and press **Enter**.
- Step 3** At the prompt, confirm the admin password and press **Enter**.
- Step 4** At the Enter HA role[standalone/primary/secondary] prompt, enter the secondary HA role and press **Enter**.
- Step 5** At the Enter the ha id(1-4095) prompt, enter **25** for the HA pair id and press **Enter**.

**Note** The HA ID uniquely identifies the two Cisco VSGs in an HA pair. If you are configuring Cisco VSGs in an HA pair, make sure that the ID number you provide is identical to the other Cisco VSG in the pair.

**Step 6** At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**. The default account name is `admin`.

**Step 7** At the `Password` prompt, enter the name of the password for the admin account and press **Enter**. You are now at the Cisco VSG node.

## Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, perform one of the tasks:

| Command                           | Purpose                                                |
|-----------------------------------|--------------------------------------------------------|
| <code>show interface brief</code> | Displays brief status and interface information.       |
| <code>show vsg</code>             | Displays the Cisco VSG and system-related information. |

This example shows how to verify the Cisco VSG configurations:

```
vsg# show interface brief
```

```

Port VRF Status IP Address Speed MTU

mgmt0 -- up 10.193.77.217 1000 1500
```

```
vsg# show vsg
```

```
Model: VSG
HA ID: 3437
VSG Software Version: 4.2(1)VSG1(1) build [4.2(1)VSG1(0.399)]
VNMC IP: 10.193.75.73
```

## Where to Go Next

After installing and completing the initial configuration of the Cisco VSG, you can configure firewall policies on the Cisco VSG through the Cisco Prime NSC.





# Registering Devices With the Cisco Prime NSC

This chapter contains the following sections:

- [Registering a Cisco VSG, page 61](#)
- [Registering a Cisco Nexus 1000V VSM, page 62](#)
- [Registering vCenter, page 63](#)

## Registering a Cisco VSG

You can register a Cisco VSG with the Cisco Prime NSC. Registration enables communication between the Cisco VSG and the Cisco Prime NSC.

### SUMMARY STEPS

1. Copy the `vnmc-vsgpa.2.1.1b.bin` file into the Cisco VSG bootflash:
2. On the command line, enter configuration mode.
3. Enter the `config-vnm-policy-agent` mode.
4. Set the Cisco Prime NSC registration IP address.
5. Specify the shared-secret of Cisco Prime NSC.
6. Install the policy agent.
7. Exit all modes.
8. On the Cisco VSG command line, enter the `show vnm-pa status` command:
9. Save the change persistently through reboots and restarts by copying the running configuration to the startup configuration:

### DETAILED STEPS

- Step 1** Copy the `vnmc-vsgpa.2.1.1b.bin` file into the Cisco VSG bootflash:
- ```
vsg# copy ftp://guest@172.18.217.188/n1kv/vnmc-vsgpa.2.1.1b.bin bootflash
```
- Step 2** On the command line, enter configuration mode.
- ```
vsg# configure
```

- Step 3** Enter the config-vnm-policy-agent mode.  
vsg (config)# **vnm-policy-agent**
- Step 4** Set the Cisco Prime NSC registration IP address.  
vsg (config-vnm-policy-agent)# **registration-ip 209.165.200.225**
- Step 5** Specify the shared-secret of Cisco Prime NSC.  
vsg (config-vnm-policy-agent)#  
**shared-secret \*\*\*\*\***
- Step 6** Install the policy agent.  
vsg (config-vnm-policy-agent)#  
**policy-agent-image bootflash: vnmc-vsmpa.2.1.1b.bin**
- Step 7** Exit all modes.  
vsg (config-vnm-policy-agent)# **end**
- Step 8** On the Cisco VSG command line, enter the **show vnm-pa status** command:  
vsg# **show vnm-pa status**  
If registration was successful, you should see the following message:  
"VNM Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg"  
The Cisco VSG registration is complete.
- Step 9** Save the change persistently through reboots and restarts by copying the running configuration to the startup configuration:  
vsg# **copy running-config startup-config**  
Executing this command ensures that the registration becomes part of the basic configuration
- 

## Registering a Cisco Nexus 1000V VSM

You can register a Cisco Nexus 1000V with the Cisco Prime NSC. Registration enables communication between the Cisco Nexus 1000V VSM and Cisco Prime NSC.

- Step 1** Copy the vnmc-vsmpa.2.1.1e.bin file into the VSM bootflash:  
vsm# **copy ftp://guest@172.18.217.188/n1kv/vnmc-vsmpa.2.1.1e.bin bootflash:**
- Step 2** On the command line, enter configuration mode.  
vsm# **configure**
- Step 3** Enter config-vnm-policy-agent mode.  
vsm(config)# **vnm-policy-agent**
- Step 4** Set the Cisco Prime NSC registration IP address.  
vsm(config-vnm-policy-agent)# **registration-ip 209.165.200.226**
- Step 5** Specify the shared-secret of Cisco Prime NSC.  
vsm(config-vnm-policy-agent)# **shared-secret \*\*\*\*\***
- Step 6** Install the policy agent.  
vsm(config-vnm-policy-agent)# **policy-agent-image bootflash:vnmc-vsmpa.2.1.1e.bin**
- Step 7** Exit all modes.  
vsm(config-vnm-policy-agent)# **top**
- Step 8** On the command line, enter the following command:  
vsm# **show vnm-pa status**  
If registration was successful, you should see the following message:

```
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsg
The Cisco Nexus 1000V VSM registration is complete.
```

**Step 9** On the command line, enter the following command:

```
vsm# copy running-config startup-config
```

Executing this command ensures that the registration becomes part of the basic configuration.

---

### What to Do Next

See the *Cisco Prime Network Services Controller CLI Configuration Guide* for detailed information about configuring the Cisco Prime NSC using the CLI.

## Registering vCenter

---

**Step 1** Log into Cisco Prime NSC.

**Step 2** Choose **Resource Management > VM Managers**.

**Step 3** In the **Navigation** pane, right-click **VM Managers**.

**Step 4** Choose **Export vCenter Extension**.

**Step 5** In the dialog box that appears, choose the appropriate extension, and click **Save**.

**Step 6** Log into vSphere.

**Step 7** In your vSphere client, log into **vCenter**.

**Step 8** Choose **Plug-ins > Manage Plug-ins**.

**Step 9** Right-click the empty space and click **New Plug-in**.

**Step 10** Browse to the Cisco Prime NSC vCenter extension file, and then click **Register Plug-in**.

**Step 11** Click **Ignore** for any security warning.  
You should see a message that reports a successful registration.

**Step 12** Log into the Cisco Prime NSC and choose **Resource Management > VM Managers**.

**Step 13** In the **Navigation** pane, right-click **VM Managers**.

**Step 14** Click **Add VM Manager**.

**Step 15** Enter the vCenter name and IP address information and click **OK**.

**Note** The Successful Addition State field should display the word Enabled, and the Operational State field should display the version information.

vCenter is registered.

---





# Installing the Cisco VSG on a Cisco Cloud Services Platform Virtual Services Appliance

---

This chapter contains the following sections:

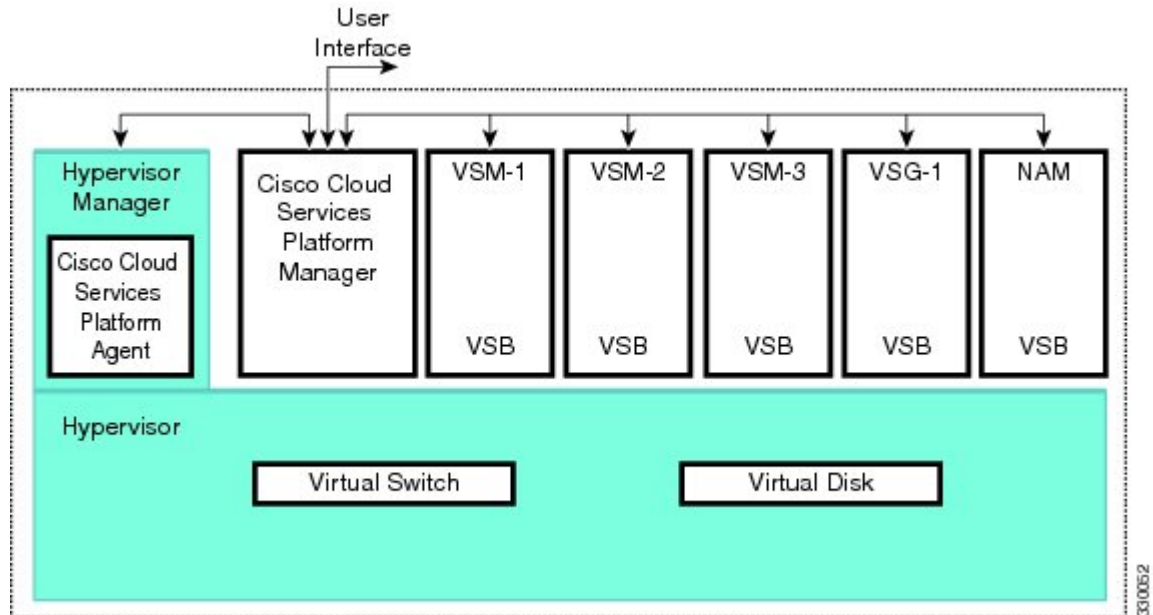
- [Information About Installing the Cisco VSG on the Cisco Cloud Services Platform, page 65](#)
- [Prerequisites for Installing Cisco VSG on Cisco Cloud Services Platform, page 66](#)
- [Guidelines and Limitations, page 66](#)
- [Installing a Cisco VSG on a Cisco Cloud Services Platform, page 67](#)

## Information About Installing the Cisco VSG on the Cisco Cloud Services Platform

The Cisco VSG software is provided with the other virtual service blade (VSB) software in the Cisco Cloud Services Platform bootflash: repository directory. The Cisco Cloud Services Platform has up to six virtual

service blades (VSBs) on which you can choose to place a Cisco VSG, VSM, or Network Analysis Module (NAM).

**Figure 7: Cisco Cloud Services Platform Architecture Showing Virtual service Blades Usage**



## Prerequisites for Installing Cisco VSG on Cisco Cloud Services Platform

- You must first install the Cisco Cloud Services Platform Virtual Services Appliance and connect it to the network. For procedures on installing the hardware, see the *Cisco Cloud Services Platform Virtual Services Appliance Hardware Installation Guide*.
- After you install the hardware appliance and connect it to the network, you can configure the Cisco Cloud Services Platform management software, migrate existing VSMs residing on a VM to the Cisco Cloud Services Platform as virtual service blades (VSBs), and create and configure new VSBs that might host the Cisco VSG. For procedures on configuring the software, see the *Cisco Cloud Services Platform Software Configuration Guide*.

## Guidelines and Limitations

- The Cisco Cloud Services Platform appliance and its hosted Cisco VSG VSBs must share the same management VLAN.
- Unlike the data and high availability (HA) VLANs that are set when a Cisco VSG VSB is created, a Cisco VSG VSB inherits its management VLAN from the Cisco Cloud Services Platform.

**Caution**

Do not change the management VLAN on a VSB. Because the management VLAN is inherited from the Cisco Cloud Services Platform, any changes to the management VLAN are applied to both the Cisco Cloud Services Platform and all of its hosted VSBs.

## Installing a Cisco VSG on a Cisco Cloud Services Platform

You can install the Cisco VSG on a Cisco Nexus 1000V as a virtual service blade (VSB).

### Before You Begin

- Log in to the CLI in EXEC mode.
- Know the name of the Cisco VSG VSB that you want to create.
- Whether you are using a new ISO file from the bootflash repository folder or from an existing VSB, do one of the following:
  - If you are using a new ISO file in the bootflash repository, you know the filename.  
Cisco VSG: nexus-1000v.VSG2.1.1.iso
  - If you are using an ISO file from an existing VSB, you must know the name of the VSB type. This procedure includes information about identifying this name.
- Know the following properties for the Cisco VSG VSB:
  - HA ID –Management IP address
  - Cisco VSG name
  - Management subnet mask length
  - Default gateway IPV4 address
  - Administrator password
  - Data and HA VLAN IDs
- This procedure shows you how to identify and assign data and HA VLANs for the Cisco VSG VSB. Do not assign a management VLAN because the management VLAN is inherited from the Cisco Nexus 1000V.

## SUMMARY STEPS

1. switch# **configure terminal**
2. (config)# **virtual-service-blade** *name*
3. (config-vsbs-config)# **show virtual-service-blade-type summary**
4. (config-vsbs-config)# **virtual-service-blade-type** [*name name* | **new iso file name**]
5. (config-vsbs-config)# **description** *description*
6. (config-vsbs-config)# **show virtual-service-blade** *name name*
7. (config-vsbs-config)# **interface** *name* **vlan** *vlanid*
8. Repeat Step 7 to apply additional interfaces
9. (config-vsbs-config)# **enable** [**primary** | **secondary**]
10. (config-vsbs-config)# **show virtual-service-blade** *name name*
11. (Optional) (config-vsbs-config)# **copy running-config startup-config**

## DETAILED STEPS

|               | Command or Action                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 2</b> | (config)# <b>virtual-service-blade</b> <i>name</i>                                                      | Creates the named VSB and places you into configuration mode for that service. The name can be an alphanumeric string of up to 80 characters.                                                                                                                                                                                                                                                                                           |
| <b>Step 3</b> | (config-vsbs-config)# <b>show virtual-service-blade-type summary</b>                                    | (Optional) Displays a summary of all VSB configurations by type name, such as Cisco VSG, VSM, or NAM. You use this type name (in this case, the name for the Cisco VSG) in the next step.                                                                                                                                                                                                                                               |
| <b>Step 4</b> | (config-vsbs-config)# <b>virtual-service-blade-type</b> [ <i>name name</i>   <b>new iso file name</b> ] | Specifies the type and name of the software image file to add to this Cisco VSG VSB: <ul style="list-style-type: none"> <li>• Use the <b>new</b> keyword to specify the name of the new Cisco VSG ISO software image file in the bootflash repository folder.</li> <li>• Use the <b>name</b> keyword to specify the name of the existing Cisco VSG VSB type. Enter the name of an existing type found in the command output.</li> </ul> |
| <b>Step 5</b> | (config-vsbs-config)# <b>description</b> <i>description</i>                                             | (Optional) Adds a description to the Cisco VSG VSB. The <i>description</i> is an alphanumeric string of up to 80 characters.                                                                                                                                                                                                                                                                                                            |
| <b>Step 6</b> | (config-vsbs-config)# <b>show virtual-service-blade</b> <i>name name</i>                                | Displays the Cisco VSG VSB that you have just created including the interface names that you configure in the next step.                                                                                                                                                                                                                                                                                                                |
| <b>Step 7</b> | (config-vsbs-config)# <b>interface</b> <i>name</i> <b>vlan</b> <i>vlanid</i>                            | Applies the interface and VLAN ID to this Cisco VSG. Use the interface names from the command output. <p><b>Note</b> If you try to apply an interface that is not present, the following error is displayed:</p> <p>ERROR: Interface name not found in the associated virtual-service-blade type.</p>                                                                                                                                   |



|                | Command or Action                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                   | <p><b>Caution</b> Do not assign a management VLAN. Unlike data and HA VLANs, the management VLAN is inherited from the Cisco Nexus 1000V.</p> <p><b>Caution</b> To prevent loss of connectivity, you must configure the same data and HA VLANs on the hosted Cisco VSGs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 8</b>  | Repeat Step 7 to apply additional interfaces                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 9</b>  | (config-vsbs-config)# <b>enable [primary   secondary]</b>         | <p>Initiates the configuration of the VSB and then enables it.</p> <p>If you enter the <b>enable</b> command without the optional <b>primary</b> or <b>secondary</b> keywords, it enables both.</p> <p>If you are deploying a redundant pair, you do not need to specify primary or secondary.</p> <p>If you are enabling a nonredundant VSB, you can specify its HA role as follows:</p> <ul style="list-style-type: none"> <li>• Use the <b>primary</b> keyword to designate the VSB in a primary role.</li> <li>• Use the <b>secondary</b> keyword to designate the VSB in a secondary role</li> </ul> <p>The Cisco Nexus 1000V prompts you for the following:</p> <ul style="list-style-type: none"> <li>• HA ID</li> <li>• Management IP address</li> <li>• Management subnet mask length</li> <li>• Default gateway IPV4 address</li> <li>• Cisco VSG name</li> <li>• Administrator password</li> </ul> |
| <b>Step 10</b> | (config-vsbs-config)# <b>show virtual-service-blade name name</b> | <p>(Optional) Displays the new VSB for verification.</p> <p>While the Cisco Nexus 1000V management software is configuring the Cisco VSG, the output for this command progresses from in progress to powered on.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 11</b> | (config-vsbs-config)# <b>copy running-config startup-config</b>   | <p>(Optional)</p> <p>Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

This example shows how to configure a Cisco Nexus 1000V appliance VSB as a Cisco VSG:

```
N1110# configure
Enter configuration commands, one per line. End with CNTL/Z.
N1110(config)# virtual-service-blade vsg1
N1110(config-vsbs-config)# virtual-service-blade-type new nexus-1000v.VSG2.1.1.iso
N1110(config-vsbs-config)# interface data vlan 72
N1110(config-vsbs-config)# interface ha vlan 72
N1110(config-vsbs-config)# enable
Enter vsb image: [nexus-1000v.VSG2.1.1.iso]
Enter HA id[1-4095]: 1233
Management IP version [V4/V6]: [V4]
```

```

Enter Management IP address: 10.193.73.42
Enter Management subnet mask: 255.255.248.0
IPv4 address of the default gateway: 10.193.72.1
Enter HostName: vsg-1
Enter the password for 'admin': Hello_123
N1110(config-vsbs-config)# end
N1110#

```

This example show how to install the Cisco VSG on a Cisco Nexus 1000V as a VSB.

```

N1110# configure
N1110(config)# virtual-service-blade vsg-1
N1110(config-vsbs-config)# show virtual-service-blade-type summary

Virtual-Service-Blade-Type Virtual-Service-Blade

VSM_SV1_3 vsm-1 vsm-2
NAM-MV nam-1
VSG-1 vsg-1

N1110(config-vsbs-config)# virtual-service-blade-type new nexus-1000v.VSG2.1.1.iso
or
N1110(config-vsbs-config)# show virtual-service-blade name vsg-1

N1110(config-vsbs-config)# description vsg-1 for Tenant1
N1110(config-vsbs-config)# show virtual-service-blade name vsg-1

virtual-service-blade vsg-1
Description:
Slot id: 2
Host Name:
Management IP:
VSB Type Name : VSG-2.1.1
Interface: ha vlan: 0
Interface: management vlan: 231
Interface: data vlan: 0
Interface: internal vlan: NA
Ramsize: 2048
Disksize: 3
Heartbeat: 0
HA Admin role: Primary
HA Oper role: NONE
Status: VSB NOT PRESENT
Location: PRIMARY
SW version:
HA Admin role: Secondary
HA Oper role: NONE
Status: VSB NOT PRESENT
Location: SECONDARY
SW version:
VSB Info:

N1110(config-vsbs-config)# interface data vlan 1044
or
N1110(config-vsbs-config)# interface ha vlan 1045

N1110(config-vsbs-config)# enable

Enter domain id[1-4095]: 1054
Enter Management IP address: 10.78.108.40
Enter Management subnet mask length 28
IPv4 address of the default gateway: 10.78.108.117
Enter Switchname:Hostname
Enter the password for 'admin': Hello_123

N1110(config-vsbs-config)# show virtual-service-blade name vsg-1

virtual-service-blade vsg-1
Description:
Slot id: 1
SW version: 4.0(4)SV2(1)
Host Name: vsg-1

```

```

Management IP: 10.78.108.40
VSB Type Name : VSG-2.1.1
Interface: ha vlan: 1044
Interface: management vlan: 1032
Interface: data vlan: 1045
Interface: internal vlan: NA
Ramsize: 2048
Disksize: 3
Heartbeat: 1156
HA Admin role: Primary
HA Oper role: STANDBY
Status: VB POWERED ON
Location: PRIMARY
HA Admin role: Secondary
HA Oper role: ACTIVE
Status: VB POWERED ON
Location: SECONDARY
VB Info:
Domain ID : 1054

```

```

N1110(config-vsbs-config)# copy running-config startup-config
```

This example shows how to display a virtual service blade summary on the Cisco Nexus 1000V:

```
N1110# show virtual-service-blade summary
```

```

Name Role State Nexus1010-Module

vsg-1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
vsg-1 SECONDARY VSB POWERED OFF Nexus1010-SECONDARY
vsg9 PRIMARY VSB NOT PRESENT Nexus1010-PRIMARY
vsg9 SECONDARY VSB DEPLOY IN PROGRESS Nexus1010-SECONDARY
nam_1 PRIMARY VSB POWERED OFF Nexus1010-PRIMARY
nam_1 SECONDARY VSB NOT PRESENT Nexus1010-SECONDARY
vsgc1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
vsgc1 SECONDARY VSB POWERED ON Nexus1010-SECONDARY
nam_2 PRIMARY VSB POWERED OFF Nexus1010-PRIMARY
nam_2 SECONDARY VSB NOT PRESENT Nexus1010-SECONDARY

```





# Upgrading the Cisco VSG and the Cisco Prime NSC

This chapter contains the following sections:

- [Complete Upgrade Procedure](#), page 73
- [Upgrade Guidelines and Limitations](#), page 75
- [Upgrade Procedure for Cisco VSG Release 4.2\(1\)VSG1\(4.1\) to Release 4.2\(1\)VSG2\(1.1\), Cisco VNMC Release 2.1 to Cisco Prime NSC Release 3.2 and Cisco Nexus 1000V Release 4.2\(1\)SV1\(5.2\) to Release 4.2\(1\)SV2\(2.2\)](#), page 75
- [Upgrade Procedure for Cisco VSG Release 4.2\(1\)VSG1\(4.1\) to Release 4.2\(1\)VSG2\(1.1\), Cisco VNMC Release 2.0 to Release 2.1 and Cisco Nexus 1000V Release 4.2\(1\)SV1\(5.2\) to Release 4.2\(1\)SV2\(2.2\)](#), page 108

## Complete Upgrade Procedure

**Table 2: Refer to the Section in Table Based on your Pre-upgrade Product Release**

| <b>You are Upgrading From</b>                                                                                          | <b>Follow The Sequential Steps in the Following Section:</b>                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1) and Cisco VNMC Release 2.1 to Cisco Prime NSC Release 3.2 | Upgrade Procedures for Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1) and Cisco VNMC 2.1 to Cisco Prime NSC Release 3.2.<br><br>This includes upgrade procedures for Cisco Nexus 1000V Release 4.2(1)SV1(5.2) to Release 4.2(1)SV2(2.2). |

| You are Upgrading From                                                                                 | Follow The Sequential Steps in the Following Section:                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1) and Cisco VNMC Release 2.0 to Release 2.1 | <p>Upgrade Procedures for Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1) and Cisco VNMC Release 2.0 to Release 2.1.</p> <p>This includes upgrade procedures for Cisco Nexus 1000V Release 4.2(1)SV1(5.2) to Release 4.2(1)SV2(2.2).</p> |

To upgrade the Cisco Prime NSC, Cisco VSG, and Cisco Nexus 1000V, follow the steps sequentially:

- 1 Stage 1: Upgrading Cisco Prime NSC
- 2 Stage 2: Upgrading a Cisco VSG Pair
- 3 Stage 3: Upgrading the VSM pair and the VEMs

**Note**

We highly recommend that you upgrade the Cisco VSG and the Cisco Prime NSC in the sequence listed. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco Prime NSC must be upgraded with the corresponding policy agent (PA).

**Note**

To upgrade from VNMC Release 2.1 Cisco Prime NSC 3.2, you need to first upgrade to Release Cisco Prime NSC 3.0.2.

## Information About Cisco Prime NSC Upgrades

When you upgrade the Cisco Prime NSC software, all current (command-line interface) CLI and (graphical user interface) GUI sessions are interrupted, which means that you must restart any CLI or GUI sessions.

## Information About Cisco VSG Upgrades

The upgrade procedure for a standalone Cisco VSG is hitful, which means that you must manually reload the Cisco VSG for the new image to become effective. In HA mode, the upgrade is hitless, which means that the standby Cisco VSG is upgraded first and then after a switchover, the previously active Cisco VSG is upgraded.

Because license information is not stored with the Cisco VSG but is maintained between the Virtual Supervisor Module (VSM) and Virtual Ethernet Module (VEM), if packets are received at the Cisco VSG, that means that the license is valid and the packets are processed.

An upgrade affects two bin files: the kickstart file and the system file.

An upgrade does not erase any of the existing information, when the Cisco VSG comes online. Because the Cisco VSG is stateless, it gets all this information from the Cisco Prime NSC at bootstrap.

# Upgrade Guidelines and Limitations

Before upgrading the Cisco Prime NSC, Cisco VSG, and Cisco Nexus 1000V, read the following:

- We highly recommend that you upgrade the Cisco VSG and the Cisco Prime NSC in the order provided. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco Prime NSC must be upgraded with the corresponding policy agent (PA).
- We recommend that you take a snapshot or backup (clone) of the original Cisco Prime NSC and VSM prior to the upgrade process and then perform an ISSU upgrade process on both the VSM and the Cisco VSG. We do not recommend that you perform a manual upgrade.
- For a full In-service Software Upgrade (ISSU) upgrade on both the Cisco VSG and VSM, follow these rules:
  - Install the Cisco Prime NSC before installing the Cisco VSG and VSM. The ISSU upgrade installs a new PA.
  - A new PA with an old Cisco Prime NSC is not supported and there should never be an interim stage in this state.
  - A copy run start is not required after the VSM upgrade.
- The **vn-service** command is changed to the **vservice** command on the VSM port-profile in VSM Release 4.2(1)SV1(5.2).
- Upgrade instructions include the following information:
  - Different stages of complete upgrade procedures and operations which are supported at different stages.
  - Different component versions after each stage.
  - Different operations supported after each stage.

## Upgrade Procedure for Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1), Cisco VNMC Release 2.1 to Cisco Prime

## NSC Release 3.2 and Cisco Nexus 1000V Release 4.2(1)SV1(5.2) to Release 4.2(1)SV2(2.2)

### Cisco VSG Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1) and Cisco VNMC 2.1 to Cisco Prime NSC 3.2 Staged Upgrade

| Virtual Appliance | Original State      | Stage 1: Cisco Prime NSC Upgrade only (no PAs upgraded) | Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade) | Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade) |
|-------------------|---------------------|---------------------------------------------------------|-----------------------------------------------|---------------------------------------------|
| Cisco Prime NSC   | Old Cisco VNMC 2.1  | New Cisco Prime NSC 3.0.2<br>New Cisco Prime NSC 3.2    | New Cisco Prime NSC 3.2                       | New Cisco Prime NSC 3.2                     |
| Cisco VSG         | Old 4.2(1)VSG1(4.1) | Old 4.2(1)VSG1(4.1)                                     | New 4.2(1)VSG2(2.1)                           | New 4.2(1)VSG2(2.1)                         |
| VSG PA            | Old 2.0             | Old 2.0                                                 | New 2.1                                       | New 2.1                                     |
| VSM               | 4.2(1)SV1(5.2b)     | 4.2(1)SV1(5.2b)                                         | 4.2(1)SV1(5.2b)                               | 4.2(1)SV2(2.2)                              |
| VEM               | Old 4.2(1)SV1(5.2b) | Old 4.2(1)SV1(5.2b)                                     | Old 4.2(1)SV1(5.2b)                           | New 4.2(1)SV2(2.2)                          |
| VSM PA            | Old 2.0             | Old 2.0                                                 | Old 2.0                                       | New 2.1                                     |



| Virtual Appliance                                  | Original State           | Stage 1: Cisco Prime NSC Upgrade only (no PAs upgraded)                                                                                                                                                                              | Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade)                                                                                                                                                                                           | Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade)                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported operations after upgrading to each stage | All operations supported | <ul style="list-style-type: none"> <li>• Existing data sessions (offloaded).</li> <li>• New data sessions.</li> <li>• Allows Cisco Nexus 1000V switch (non-vn-service) operations including non-vn-service port profiles.</li> </ul> | <ul style="list-style-type: none"> <li>• Short disruption in new data session establishment during the Cisco VSG upgrade.</li> <li>• Other operations are fully supported.</li> <li>• Full Layer 3 VSG and VM VXLAN support.</li> </ul> | <ul style="list-style-type: none"> <li>• All operations are supported if all the upgrades including VEMs are successful.</li> <li>• Restricted operations (below) apply only if all VEMs are not upgraded</li> <li>• Disruption of data traffic during VEM upgrades.</li> <li>• Full service chaining is supported.</li> <li>• Layer 3 VSG and VM VXLAN support.</li> <li>• VSG on VXLAN is supported.</li> </ul> |

| Virtual Appliance                                   | Original State | Stage 1: Cisco Prime NSC Upgrade only (no PAs upgraded)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restricted operations after upgrading to each stage | None           | <ul style="list-style-type: none"> <li>• No Cisco Prime NSC policy cfg change (assuming silent drops).</li> <li>• No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc).</li> <li>• No new vn-service VMs is supported.</li> <li>• No Vmotion of vn-service firewalled VMs on N1k</li> <li>• No vn-service PP operations or modifications (toggles, removal, changing the PP on VSM).</li> <li>• VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to Cisco Prime NSC to VSG control operations are restricted).</li> </ul> | <ul style="list-style-type: none"> <li>• No Cisco Prime NSC policy cfg change (assuming silent drops).</li> <li>• No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc).</li> <li>• No new vn-service VMs is supported.</li> <li>• No Vmotion of vn-service firewalled VMs on N1k.</li> <li>• No vn-service PP operations or modifications (toggles, removal, changing the PP on VSM).</li> <li>• VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to Cisco Prime NSC to VSG control operations are restricted).</li> </ul> | <p><b>The following restricted operations apply only if all VEMs are not upgraded:</b></p> <ul style="list-style-type: none"> <li>• No Cisco Prime NSC policy cfg change (assuming silent drops).</li> <li>• No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc).</li> <li>• No new vn-service VMs is supported.</li> <li>• No boot strap of devices (VNMC, VSM, VSG).</li> <li>• No Vmotion of vn-service VMs on N1k.</li> <li>• No vn-service PP operations or modifications (toggles, removal, changing the PP on VSM).</li> <li>• No N1k switch (non vn-service) operations, including non-vn-service PPs (VSM+VEM upgraded) (All VSM to Cisco Prime NSC to VSG control operations are restricted).</li> </ul> |



**Note** Because we support full ISSU upgrade on both VSG and VSM that involves installing a new PA, you should install the Cisco Prime NSC first. The new PA may not support the old VNMC.

## Upgrading VNMC Release 2.1 to Cisco Prime NSC 3.0.2

### Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco Prime NSC Release 3.0.2 downloaded.
- You have added two hard disks to the VNMC VM. For more information on Cisco Prime NSC requirements, see [System Requirements, on page 9](#).

### SUMMARY STEPS

1. nsc# **connect local-mgmt**
2. (Optional) nsc (local-mgmt)# **show version**
3. (Optional) nsc (local-mgmt)# **copy scp://user@example-server-ip/example-dir/filename bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/filename**
6. (Optional) nsc (local-mgmt)# **service status**
7. (Optional) nsc (local-mgmt)# **show version**

### DETAILED STEPS

|               | Command or Action                                                                           | Purpose                                                                          |
|---------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Step 1</b> | nsc# <b>connect local-mgmt</b>                                                              | Places you in local management mode.                                             |
| <b>Step 2</b> | nsc (local-mgmt)# <b>show version</b>                                                       | (Optional)<br>Displays the version information for the Cisco Prime NSC software. |
| <b>Step 3</b> | nsc (local-mgmt)# <b>copy scp://user@example-server-ip/example-dir/filename bootflash:/</b> | (Optional)<br>Copies the Cisco Prime NSC software file to the VM.                |
| <b>Step 4</b> | nsc (local-mgmt)# <b>dir bootflash:/</b>                                                    | Verifies that the desired file is copied in the directory.                       |
| <b>Step 5</b> | nsc (local-mgmt)# <b>update bootflash:/filename</b>                                         | Begins the update of the Cisco Prime NSC software.                               |

|               | Command or Action                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 6</b> | nsc (local-mgmt)# <b>service status</b> | (Optional)<br>Allows you to verify that the server is operating as desired.                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 7</b> | nsc (local-mgmt)# <b>show version</b>   | (Optional)<br>Allows you to verify that the Cisco Prime NSC software version is updated.<br><br><b>Note</b> After you upgrade to Cisco Prime NSC Release 3.0.2, you might see the previous version of Cisco VNMC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome. |

### Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, 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
```

The following example shows how to display version information for the Cisco VNMC:

```
nsc(local-mgmt)# show version

Name Package Version GUI
---- -
core Base System 2.1 2.1
service-reg Service Registry 2.1 2.1
policy-mgr Policy Manager 2.1 2.1
resource-mgr Resource Manager 2.1 2.1
vm-mgr VM manager 2.1 none
```

The following example shows how to copy the Cisco Prime NSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.0.2e.bin bootflash:/
Enter password:
100% 143MB 11.9MB/s 00:12
```

The following example shows how to see the directory information for Cisco Prime NSC:

```
nsc(local-mgmt)# dir bootflash:/

 1.1G Oct 14 00:57 nsc.3.0.2e.bin

Usage for bootflash://

 6359716 KB used
 10889320 KB free
 18187836 KB total
```

The following example shows how to start the update for the Cisco Prime NSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.0.2e.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco Prime NSC:

```
nsc(local-mgmt)# show version
```

| Name              | Package            | Version  | GUI      |
|-------------------|--------------------|----------|----------|
| core              | Base System        | 3.0 (2e) | 3.0 (2e) |
| service-reg       | Service Registry   | 3.0 (2e) | 3.0 (2e) |
| policy-mgr        | Policy Manager     | 3.0 (2e) | 3.0 (2e) |
| resource-mgr      | Resource Manager   | 3.0 (2e) | 3.0 (2e) |
| vm-mgr            | VM manager         | 3.0 (2e) | none     |
| cloudprovider-mgr | Cloud Provider Mgr | 3.0 (2e) | none     |

## Upgrading Cisco Prime NSC 3.0.2 to Cisco Prime NSC 3.2

### Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco Prime NSC Release 3.2 downloaded.

### SUMMARY STEPS

1. nsc# **connect local-mgmt**
2. (Optional) nsc (local-mgmt)# **show version**
3. (Optional) nsc (local-mgmt)# **copy scp://user@example-server-ip/example-dir/filename bootflash:/**
4. nsc (local-mgmt)# **dir bootflash:/**
5. nsc (local-mgmt)# **update bootflash:/filename**
6. (Optional) nsc (local-mgmt)# **service status**
7. (Optional) nsc (local-mgmt)# **show version**

### DETAILED STEPS

|               | Command or Action                                                                           | Purpose                                                                          |
|---------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Step 1</b> | nsc# <b>connect local-mgmt</b>                                                              | Places you in local management mode.                                             |
| <b>Step 2</b> | nsc (local-mgmt)# <b>show version</b>                                                       | (Optional)<br>Displays the version information for the Cisco Prime NSC software. |
| <b>Step 3</b> | nsc (local-mgmt)# <b>copy scp://user@example-server-ip/example-dir/filename bootflash:/</b> | (Optional)<br>Copies the Cisco Prime NSC software file to the VM.                |

|               | Command or Action                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | nsc (local-mgmt)# <b>dir bootflash:/</b>            | Verifies that the desired file is copied in the directory.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 5</b> | nsc (local-mgmt)# <b>update bootflash:/filename</b> | Begins the update of the Cisco Prime NSC software.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 6</b> | nsc (local-mgmt)# <b>service status</b>             | (Optional)<br>Allows you to verify that the server is operating as desired.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 7</b> | nsc (local-mgmt)# <b>show version</b>               | (Optional)<br>Allows you to verify that the Cisco Prime NSC software version is updated.<br><br><b>Note</b> After you upgrade to Cisco Prime NSC Release 3.2, you might see the previous version of Cisco Prime NSC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome. |

### Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, 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
```

The following example shows how to display version information for the Cisco Prime NSC:

```
nsc(local-mgmt)# show version

Name Package Version GUI

core Base System 3.0(2e) 3.0(2e)
service-reg Service Registry 3.0(2e) 3.0(2e)
policy-mgr Policy Manager 3.0(2e) 3.0(2e)
resource-mgr Resource Manager 3.0(2e) 3.0(2e)
vm-mgr VM manager 3.0(2e) none
cloudprovider-mgr Cloud Provider Mgr 3.0(2e) none
```

The following example shows how to copy the Cisco Prime NSC software to the VM:

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.2.bin bootflash:/
Enter password:
```

The following example shows how to see the directory information for Cisco Prime NSC:

```
nsc(local-mgmt)# dir bootflash:/

 1.1G Oct 14 00:57 nsc.3.2.bin

Usage for bootflash://
```

```
6359716 KB used
10889320 KB free
18187836 KB total
```

The following example shows how to start the update for the Cisco Prime NSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.2.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco Prime NSC:

```
nsc(local-mgmt)# show version
```

| Name              | Package            | Version | GUI  |
|-------------------|--------------------|---------|------|
| core              | Base System        | 3.2     | 3.2  |
| service-reg       | Service Registry   | 3.2     | 3.2  |
| policy-mgr        | Policy Manager     | 3.2     | 3.2  |
| resource-mgr      | Resource Manager   | 3.2     | 3.2  |
| vm-mgr            | VM manager         | 3.2     | none |
| cloudprovider-mgr | Cloud Provider Mgr | 3.2     | none |

## Upgrading Cisco VSG from Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1)

Enter the commands on all Cisco VSG nodes on your network.

### Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have copied the new system image, kickstart image and the Cisco VSG policy agent image into the bootflash file system using the following commands:
 

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart-mz.VSG2.1.bin
bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin

switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-mz.VSG2.1.bin
bootflash:nexus-1000v-mz.VSG2.1.bin

switch# copy scp://user@scpserver.cisco.com/downloads/vnmc-vsgpa.2.1(1b).bin
bootflash:vnmc-vsgpa.2.1(1b).bin
```
- You have confirmed that the system is in high availability (HA) mode for an HA upgrade using the **show system redundancy status** command.

### SUMMARY STEPS

1. **configure terminal**
2. **install all kickstart bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin system bootflash:nexus-1000v-mz.VSG2.1.bin vnmpa bootflash:vnmc-vsgpa.2.1(1b).bin**
3. **show vnm-pa status**
4. **copy running-config startup-config**

### DETAILED STEPS

|        | Command or Action  | Purpose                           |
|--------|--------------------|-----------------------------------|
| Step 1 | configure terminal | Enters global configuration mode. |

|               | Command or Action                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>install all kickstart</b><br><b>bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin</b><br><b>system bootflash:nexus-1000v-mz.VSG2.1.bin</b><br><b>vnmpa bootflash:vnmc-vsghpa.2.1(1b).bin</b> | Installs the kickstart image, system image, and policy agent (PA) image.<br><br><b>Note</b> If you do not have a policy agent installed on the Cisco VSG before the <b>install all</b> command is executed, the PA will not be upgraded (installed) with the image. Make sure that the current version of policy agent is installed before you begin the upgrade process. |
| <b>Step 3</b> | <b>show vnm-pa status</b>                                                                                                                                                                   | Verifies that the new PA is installed and the upgrade was successful.<br><br><b>Note</b> You must have an existing PA installed before upgrading the PA using the <b>install all</b> command.                                                                                                                                                                             |
| <b>Step 4</b> | <b>copy running-config startup-config</b>                                                                                                                                                   | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.                                                                                                                                                                                                                                             |

### Configuration Example

The following example shows how to upgrade Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1):

```
vsg # configure terminal
vsg (config)# install all kickstart bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin system
bootflash:nexus-1000v-mz.VSG2.1.bin vnmpa bootflash:vnmc-vsghpa.2.1(1b).bin
vsg (config)# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg
vsg(config)# copy running-config startup-config
```

## Upgrading VSMs

### Upgrade Procedures

The following table lists the upgrade steps.



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

**Table 3: 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. |



| If you are running this configuration                                           | Follow these steps                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Releases 4.0(4)SV1(3x) Series                                                   | <ol style="list-style-type: none"> <li>1 Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b)</li> <li>2 Upgrade from Releases 4.2(1)SV1(4x) and later releases to the current release</li> </ol>                                                                                |
| Release 4.2(1)SV1(4x) Series 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</li> <li>2 Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> <li>3 Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> </ol> |
| Release 4.2(1)SV1(4x) Series 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) and later releases to the current release</li> <li>2 Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> </ol>                                                                    |

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

**Table 4: Upgrade Paths from Releases 4.2(1)SV1(5x) and Later Releases**

| If you are running this configuration     | Follow these steps                                                                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| With vSphere 5.0 GA, patches, or updates. | <ol style="list-style-type: none"> <li>1 Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> <li>2 Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> </ol> |

## 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

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:

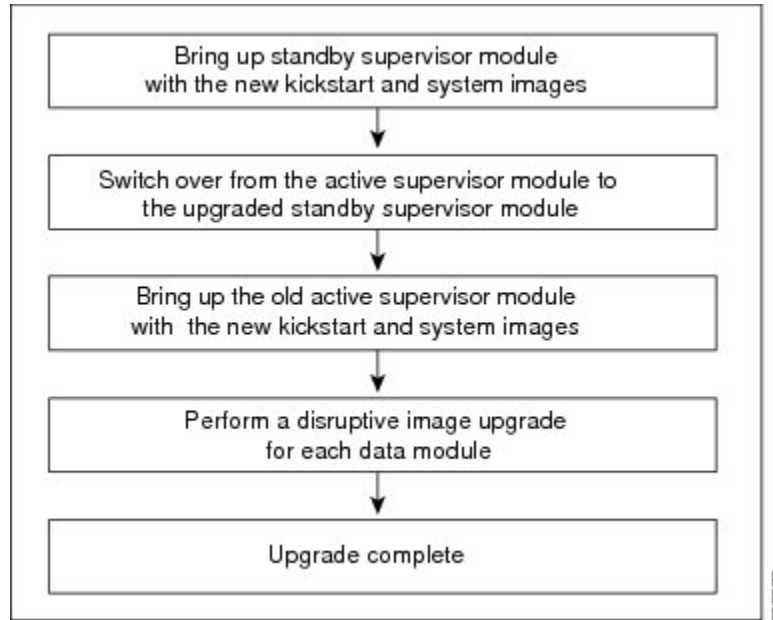
- Kickstart image
- System image
- VEM images

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.

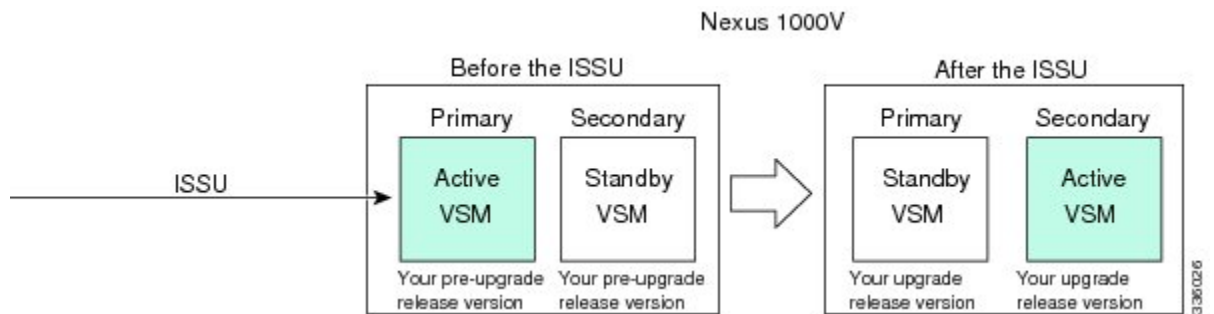
**Figure 8: ISSU Process**



### ISSU VSM Switchover

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

**Figure 9: 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)SV2(1.1x), 4.2(1)SV2(2.1x) to 5.2(1)SV3(1.1)

- 
- 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://software.cisco.com/download/navigator.html>

**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.SV2.2.2.iso
bootflash:nexus-1000v.4.2.1.SV2.2.2.iso
```

- Copy kickstart and system images.

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin
bootflash:nexus-1000v-kickstart-4.2.1.SV2.1.1a.bin
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.4.2.1.SV2.2.2.bin
bootflash:nexus-1000v-4.2.1.SV2.1.1a.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.SV2.2.2.iso
```

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

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

```

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

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

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

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

```

Compatibility check is done:

| Module | bootable | Impact         | Install-type | Reason |
|--------|----------|----------------|--------------|--------|
| 1      | yes      | 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 (2.2) | yes          |
| 1      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | system    | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |

| Module     | Running-Version   | ESX Version                                 | VSM |
|------------|-------------------|---------------------------------------------|-----|
| 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.SV2.2.2.bin system
bootflash:nexus-1000v.4.2.1.SV2.2.2.bin

```

```

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

```

```

Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1a.bin for boot variable "system".
[#####] 100% -- SUCCESS

```

```

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

```

```

Extracting "system" version from image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin.

```

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

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

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

```
Compatibility check is done:
Module bootable Impact Install-type Reason

1 yes 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(2.2) yes
1 kickstart 4.2(1)SV1(5.2) 4.2(1)SV2(2.2) yes
2 system 4.2(1)SV1(5.2) 4.2(1)SV2(2.2) yes
2 kickstart 4.2(1)SV1(5.2) 4.2(1)SV2(2.2) 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 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 and Cisco Virtual Network Management Center Installation and Upgrade Guide*.

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

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

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

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

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

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

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

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

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

- Upgrade using the ISO image.

```
switch# install all iso bootflash:nexus-1000v.4.2.1.SV2.2.2.iso
```

- Upgrade using the kickstart and system images.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart.4.2.1.SV2.2.2.bin system
bootflash:nexus-1000v.4.2.1.SV2.2.2.bin
```

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

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

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

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

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

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

Compatibility check is done:

| Module | bootable | Impact         | Install-type | Reason |
|--------|----------|----------------|--------------|--------|
| 1      | yes      | 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 (2.2) | yes          |
| 1      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | system    | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |

| Module        | Running-Version   | ESX Version | VSM |
|---------------|-------------------|-------------|-----|
| Compatibility | ESX Compatibility |             |     |



```

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

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

```

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

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

Install is in progress, please wait.

```

Syncing image bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin to standby.
[#####] 100% -- SUCCESS

```

```

Syncing image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin to standby.
[#####] 100% -- SUCCESS

```

```

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

```

```

Performing configuration copy.
[#####] 100%2013 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) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
 loader: version unavailable [last: loader version not available]
 kickstart: version 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
 system: version 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
 kickstart image file is: bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin
 kickstart compile time: 1/11/2012 3:00:00 [01/11/2012 12:49:49]

```

```

system image file is: bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin
system compile time: 1/11/2012 3:00:00 [01/11/2012 13:42:57]

```

## Hardware

```

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

```

```

Device name: Nexus1000v
bootflash: 1557496 kB

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```
-- SUCCESS
```

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

```
-- SUCCESS
```

```
Verifying image type.
```

```
-- SUCCESS
```

```
Extracting "system" version from image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin.
```

```
-- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin.
```

```
-- SUCCESS
```

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

```
-- SUCCESS
```

```
Compatibility check is done:
```

```
Module bootable Impact Install-type Reason
```

```

 1 yes non-disruptive reset
 2 yes non-disruptive reset

```

Images will be upgraded according to following table:

| Module | Image     | Running-Version | New-Version    | Upg-Required |
|--------|-----------|-----------------|----------------|--------------|
| 1      | system    | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | yes          |
| 1      | kickstart | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | yes          |
| 2      | system    | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | yes          |
| 2      | kickstart | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | 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.SV2.2.2.bin to standby.
-- SUCCESS

```

```

Syncing image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin to standby.
-- SUCCESS

```

```

Setting boot variables.
-- SUCCESS

```

```

Performing configuration copy.
-- SUCCESS

```

```

Module 2: Waiting for module online.
-- SUCCESS

```

```

Notifying services about the switchover.
-- SUCCESS

```

```

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

```

```

switch# attach module 2
Attaching to module 2 ...

```

```

To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, 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)#

```

---

## Upgrading VEMs

### VEM Upgrade Procedures

- VUM Upgrade Procedures
  - Set up VUM baselines. See [http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4\\_2\\_1\\_s\\_v\\_1\\_5\\_2/install\\_upgrade/vsm\\_vem/guide/b\\_Installation\\_and\\_Upgrade\\_Release\\_4\\_2\\_1SV1\\_5\\_2\\_appendix\\_0100.html#task\\_A93C11451B0B43F98468D15C83C1E5E5](http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_2/install_upgrade/vsm_vem/guide/b_Installation_and_Upgrade_Release_4_2_1SV1_5_2_appendix_0100.html#task_A93C11451B0B43F98468D15C83C1E5E5).
  - Initiate an upgrade from VUM. See [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97.
  - Upgrade VEM from VSM. See [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97.
- Manual upgrade procedures
  - Upgrading VIB Manually from the CLI. See [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 101
- Installing or upgrading stateless ESXi. See [Installing the VEM Software on a Stateless ESXi Host](#).

VEM upgrades fall into three types:

- An upgrade of 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](#).

An upgrade of 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 ESXi version intact. The first figure shows this flow.
- 2 Upgrade the ESX/ESXi without a change of the Cisco Nexus 1000V version. This process is addressed in the Workflow 2 figure.

If you are using VUM, set up a host patch baseline with the VEM's offline bundle. Then follow [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97.

If you are upgrading from the command line, see [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 101.

- 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 ESXi 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 ESXi 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 ESXi 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](#).
  - You can upgrade the ESXi 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.

### VEM Upgrade Methods from Release 4.2(1)SV1(5x), or Release 4.2(1)SV2(1.1x) to the Current Release

There are two methods for upgrading the VEMs.

- [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97
- [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 101

*Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(5x) and Later Releases to the Current Release*



#### Caution

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

## SUMMARY STEPS

1. switch# **show vmware vem upgrade status**
2. switch# **vmware vem upgrade notify**
3. switch# **show vmware vem upgrade status**
4. switch# **show vmware vem upgrade status**
5. Initiate the VUM upgrade process with the following commands.
6. switch# **show vmware vem upgrade status**
7. Clear the VEM upgrade status after the upgrade process is complete with the following commands.
8. switch# **show module**

## DETAILED STEPS

- 
- Step 1** switch# **show vmware vem upgrade status**  
Display the current configuration.
- Note** The minimum release of Cisco Nexus 1000V for VMware ESXi 5.0.0 hosts is Release 4.2(1)SV1(5).
- Step 2** switch# **vmware vem upgrade notify**  
Coordinate with and notify the server administrator of the VEM upgrade process.
- Step 3** switch# **show vmware vem upgrade status**  
Verify that the upgrade notification was sent.
- Note** Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.
- Step 4** switch# **show vmware vem upgrade status**  
Verify that the server administrator has accepted the upgrade in the vCenter. For more information about how the server administrator accepts the VEM upgrade, see [Accepting the VEM Upgrade, on page 104](#). Coordinate the notification acceptance with the server administrator. After the server administrator accepts the upgrade, proceed with the VEM upgrade.
- Note** Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.
- Step 5** Initiate the VUM upgrade process with the following commands.
- Note** Before entering the following commands, communicate with the server administrator to confirm that the VUM process is operational.
- The vCenter Server locks the DVS and triggers VUM to upgrade the VEMs.
- a) switch# **vmware vem upgrade proceed**
  - b) switch# **show vmware vem upgrade status**
- Note** The DVS bundle ID is updated and is highlighted.
- If the ESXi host is using 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 ESXi in maintenance mode to upgrade the VEM. This process is continued for other hosts in the DRS cluster until all the hosts are upgraded in the cluster. For details about DRS settings required and vMotion of VMs, visit the VMware documentation related to Creating a DRS Cluster.
- Step 6** switch# **show vmware vem upgrade status**

Check for the upgrade complete status.

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

- a) switch# **vmware vem upgrade complete**
- b) switch# **show vmware vem upgrade status**

**Step 8** switch# **show module**

Verify that the upgrade process is complete.

The upgrade is complete.

The following example shows how to upgrade VEMs using VUM.



**Note**

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

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM410-201301152101-BG
switch#
switch# vmware vem upgrade notify
Warning:
Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to
corresponding
"Cisco Nexus 1000V and VMware Compatibility Information" guide.
switch# show vmware vem upgrade status

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

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

```

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

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter) : Tue Jan 27 02:06:53 2014
Upgrade Start Time: : Tue Jan 27 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
switch#
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: : Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter): : Tue Jan 27 02:06:53 2014
Upgrade Start Time: : Tue Jan 27 10:09:08 2013
Upgrade End Time(vCenter): : Tue Jan 27 10:09:08 2014
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
switch#
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
switch#
switch# show module

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

Mod Sw Hw
--- ---
1 4.2(1)SV2(2.2) 0.0
2 4.2(1)SV2(2.2) 0.0
3 4.2(1)SV2(2.2) VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4 4.2(1)SV2(2.2) VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

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

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

```



```
* this terminal session
switch#
```



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

### Upgrading the VEMs Manually from Release 4.2(1)SV1(5x) and Later Releases to the Current Release

#### Before You Begin



**Note** If VUM is installed, it should be disabled.

To manually install or upgrade the Cisco Nexus 1000V VEM on an ESXi host, follow the steps in [Upgrading the VEM Software Using the vCLI, on page 105](#).

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.

## SUMMARY STEPS

1. switch# **vmware vem upgrade notify**
2. switch# **show vmware vem upgrade status**
3. switch# **show vmware vem upgrade status**
4. Perform one of the following tasks:
5. switch# **vmware vem upgrade proceed**
6. switch# **show vmware vem upgrade status**
7. Coordinate with and wait until the server administrator upgrades all ESXi host VEMs with the new VEM software release and informs you that the upgrade process is complete.
8. switch# **vmware vem upgrade complete**
9. switch# **show vmware vem upgrade status**
10. switch# **show module**

## DETAILED STEPS

- Step 1** switch# **vmware vem upgrade notify**  
Coordinate with and notify the server administrator of the VEM upgrade process.

- Step 2** switch# **show vmware vem upgrade status**  
Verify that the upgrade notification was sent.
- Step 3** switch# **show vmware vem upgrade status**  
Verify that the server administrator has accepted the upgrade in vCenter Server. For details about the server administrator accepting the VEM upgrade, see [Accepting the VEM Upgrade, on page 104](#). After the server administrator accepts the upgrade, proceed with the VEM upgrade.
- Step 4** Perform one of the following tasks:
- If the ESXi host is not hosting the VSM, proceed to Step 5.
  - If the ESXi host is hosting the VSM, coordinate with the server administrator to migrate the VSM to a host that is not being upgraded. Proceed to Step 5.
- Step 5** switch# **vmware vem upgrade proceed**  
Initiate the Cisco Nexus 1000V Bundle ID upgrade process.
- Note** If VUM is enabled in the vCenter environment, disable it before entering the **vmware vem upgrade proceed** command to prevent the new VIBs from being pushed to all the hosts.  
Enter the **vmware vem upgrade proceed** command so that the Cisco Nexus 1000V Bundle ID on the vCenter Server gets updated. If VUM is enabled and you do not update the Bundle ID, an incorrect VIB version is pushed to the VEM when you next add the ESXi to the VSM.
- Note** If VUM is not installed, the “The object or item referred to could not be found” error appears in the vCenter Server task bar. You can ignore this error message.
- Step 6** switch# **show vmware vem upgrade status**  
Check for the upgrade complete status.
- Step 7** Coordinate with and wait until the server administrator upgrades all ESXi 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 105](#).
- Step 8** switch# **vmware vem upgrade complete**  
Clear the VEM upgrade status after the upgrade process is complete.
- Step 9** switch# **show vmware vem upgrade status**  
Check the upgrade status once again.
- Step 10** switch# **show module**  
Verify that the upgrade process is complete.
- Note** The line with the bold characters in the preceding example display that all VEMs are upgraded to the current release.  
The upgrade is complete.

---

The following example shows how to upgrade VEMs manually.

**Note**

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM410-201401152101-BG
```

```
switch#
```

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

```
Warning:
```

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

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

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

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

```
switch#
```

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Tue Jan 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jan 28 02:06:53 2014
Upgrade Start Time: Tue Jan 28 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
```

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

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

```
switch#
```

```
switch# vmware vem upgrade complete
```

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

```
Upgrade VIBs: System VEM Image
```

```

Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG

```

```

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

```

```

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

```

```

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

```

```

* this terminal session
switch#

```

### 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.

## SUMMARY STEPS

1. In the vCenter Server, choose **Inventory > Networking**.
2. Click the **vSphere Client DVS Summary** tab to check for the availability of a software upgrade.
3. Click **Apply upgrade**.

## DETAILED STEPS

**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 10: 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.

### 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 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 ESXi system that the vCenter Server system manages. vCLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

- 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.

## SUMMARY STEPS

1. [root@serialport -]# **cd tmp**
2. Determine the upgrade method that you want to use and enter the appropriate command.
  - **vihostupdate**  
Installs the ESXi and VEM software simultaneously if you are using the vCLI.
3. For ESXi 5.0.0 or later hosts, enter the appropriate commands as they apply to you.
4. Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information* by typing the following commands.
5. switch# **show module**

## DETAILED STEPS

- 
- Step 1** [root@serialport -]# **cd tmp**  
Go to the directory where the new VEM software was copied.
- Step 2** Determine the upgrade method that you want to use and enter the appropriate command.
- **vihostupdate**  
Installs the ESXi and VEM software simultaneously if you are using the vCLI.
- Step 3** For ESXi 5.0.0 or later hosts, enter the appropriate commands as they apply to you.
- a) ~ # **esxcli software vib install -d /absolute-path/VEM\_bundle**
  - b) ~ # **esxcli software vib install -v /absolute-path/vib\_file**
- Note** You must specify the absolute path to the *VEM\_bundle* and *vib\_file* files. The absolute path is the path that starts at the root of the file system such as `/tmp/vib_file`.
- Step 4** Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information* by typing the following commands.
- a) [root@serialport tmp]# **vmware -v**
  - b) root@serialport tmp]# # **esxupdate query**
  - c) [root@host212 ~]# . ~ # **vem status -v**
  - d) [root@host212 ~]# **vemcmd show version**
- Step 5** switch# **show module**  
Display that the VEMs were upgraded by entering the command on the VSM.
- 

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

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



**Note**

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

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

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v164-4.2.1.2.2.2.0-3.0.1.vib
Installation Result
 Message: Operation finished successfully.
 Reboot Required: false
 VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1
 VIBs Removed:
 VIBs Skipped:
~ #

[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-843203
root@serialport tmp]# # esxupdate query
-----Bulletin ID----- Installed----- Summary-----
VEM500-201401164100 2014-01-27T08:18:22 Cisco Nexus 1000V 4.2(1)SV2(2.2)

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

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

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

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

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

6 4.2(1)SV2(2.2) VMware ESXi 5.1.0 Releasebuild-843203 (3.0)

```

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

```

switch#



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

## Upgrade Procedure for Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1), Cisco VNMC Release 2.0 to Release 2.1 and Cisco Nexus 1000V Release 4.2(1)SV1(5.2) to Release 4.2(1)SV2(2.2)

### Cisco VSG Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1) and Cisco VNMC 2.0 to 2.1 Staged Upgrade



**Note** The `vn-service` command is changed to the `vservice` command on the VSM port-profile in VSM Release 4.2(1)SV1(5.2).

| Virtual Appliance | Original State      | Stage 1: Cisco VNMC Upgrade only (no PAs upgraded) | Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade) | Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade) |
|-------------------|---------------------|----------------------------------------------------|-----------------------------------------------|---------------------------------------------|
| VNMC              | Old 2.0             | New 2.1                                            | New 2.1                                       | New 2.1                                     |
| Cisco VSG         | Old 4.2(1)VSG1(4.1) | Old 4.2(1)VSG1(4.1)                                | New 4.2(1)VSG2(2.1)                           | New 4.2(1)VSG2(2.1)                         |
| VSG PA            | Old 2.0             | Old 2.0                                            | New 2.1                                       | New 2.1                                     |
| VSM               | 4.2(1)SV1(5.2b)     | 4.2(1)SV1(5.2b)                                    | 4.2(1)SV1(5.2b)                               | New 4.2(1)SV2(2.2)                          |
| VEM               | Old 4.2(1)SV1(5.2b) | Old 4.2(1)SV1(5.2b)                                | Old 4.2(1)SV1(5.2b)                           | New 4.2(1)SV2(2.2)                          |
| VSM PA            | Old 2.0             | Old 2.0                                            | Old 2.0                                       | New 2.1                                     |



| Virtual Appliance                                  | Original State           | Stage 1: Cisco VNMC Upgrade only (no PAs upgraded)                                                                                                                                                                                   | Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade)                                                                                                                                                                                           | Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade)                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported operations after upgrading to each stage | All operations supported | <ul style="list-style-type: none"> <li>• Existing data sessions (offloaded).</li> <li>• New data sessions.</li> <li>• Allows Cisco Nexus 1000V switch (non-vn-service) operations including non-vn-service port profiles.</li> </ul> | <ul style="list-style-type: none"> <li>• Short disruption in new data session establishment during the Cisco VSG upgrade.</li> <li>• Other operations are fully supported.</li> <li>• Full Layer 3 VSG and VM VXLAN support.</li> </ul> | <ul style="list-style-type: none"> <li>• All operations are supported if all the upgrades including VEMs are successful.</li> <li>• Restricted operations (below) apply only if all VEMs are not upgraded</li> <li>• Disruption of data traffic during VEM upgrades.</li> <li>• Full service chaining is supported.</li> <li>• Layer 3 VSG and VM VXLAN support.</li> <li>• VSG on VXLAN is supported.</li> </ul> |

| Virtual Appliance                                   | Original State | Stage 1: Cisco VNMC Upgrade only (no PAs upgraded)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restricted operations after upgrading to each stage | None           | <ul style="list-style-type: none"> <li>• No VNMC policy cfg change (assuming silent drops).</li> <li>• No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc).</li> <li>• No new vn-service VMs is supported.</li> <li>• No Vmotion of vn-service firewalled VMs on N1k</li> <li>• No vn-service PP operations or modifications (toggles, removal, changing the PP on VSM).</li> <li>• VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to VNMC to VSG control operations are restricted).</li> </ul> | <ul style="list-style-type: none"> <li>• No VNMC policy cfg change (assuming silent drops).</li> <li>• No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc).</li> <li>• No new vn-service VMs is supported.</li> <li>• No Vmotion of vn-service firewalled VMs on N1k.</li> <li>• No vn-service PP operations or modifications (toggles, removal, changing the PP on VSM).</li> <li>• VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to VNMC to VSG control operations are restricted).</li> </ul> | <p><b>The following restricted operations apply only if all VEMs are not upgraded:</b></p> <ul style="list-style-type: none"> <li>• No VNMC policy cfg change (assuming silent drops).</li> <li>• No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc).</li> <li>• No new vn-service VMs is supported.</li> <li>• No boot strap of devices (VNMC, VSM, VSG).</li> <li>• No Vmotion of vn-service VMs on N1k.</li> <li>• No vn-service PP operations or modifications (toggles, removal, changing the PP on VSM).</li> <li>• No N1k switch (non vn-service) operations, including non-vn-service PPs (VSM+VEM upgraded) (All VSM to VNMC to VSG control operations are restricted).</li> </ul> |



**Note** Because we support full ISSU upgrade on both VSG and VSM that involves installing a new PA, you should install the VNMC first. The new PA may not support the old VNMC.

## Upgrading VNMC from Release 2.0 to Release 2.1

### Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco VNMC Release 2.1 downloaded.

### SUMMARY STEPS

1. `vnmc# connect local-mgmt`
2. (Optional) `vnmc (local-mgmt)# show version`
3. (Optional) `vnmc (local-mgmt)# copy scp://user@example-server-ip/example-dir/filename bootflash:/`
4. `vnmc (local-mgmt)# dir bootflash:/`
5. `vnmc (local-mgmt)# update bootflash:/filename`
6. `vnmc (local-mgmt)# service restart`
7. (Optional) `vnmc (local-mgmt)# service status`
8. (Optional) `vnmc (local-mgmt)# show version`

### DETAILED STEPS

|               | Command or Action                                                                                          | Purpose                                                                     |
|---------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>Step 1</b> | <code>vnmc# connect local-mgmt</code>                                                                      | Places you in local management mode.                                        |
| <b>Step 2</b> | <code>vnmc (local-mgmt)# show version</code>                                                               | (Optional)<br>Displays the version information for the Cisco VNMC software. |
| <b>Step 3</b> | <code>vnmc (local-mgmt)# copy<br/>scp://user@example-server-ip/example-dir/filename<br/>bootflash:/</code> | (Optional)<br>Copies the Cisco VNMC software file to the VM.                |
| <b>Step 4</b> | <code>vnmc (local-mgmt)# dir bootflash:/</code>                                                            | Verifies that the desired file is copied in the directory.                  |
| <b>Step 5</b> | <code>vnmc (local-mgmt)# update bootflash:/filename</code>                                                 | Begins the update of the Cisco VNMC software.                               |
| <b>Step 6</b> | <code>vnmc (local-mgmt)# service restart</code>                                                            | Restarts the server.                                                        |

|        | Command or Action                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <code>vnmc (local-mgmt)# service status</code> | (Optional)<br>Allows you to verify that the server is operating as desired.                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <code>vnmc (local-mgmt)# show version</code>   | (Optional)<br>Allows you to verify that the Cisco VNMC software version is updated.<br><br><b>Note</b> After you upgrade to Cisco VNMC Release 2.1, you might see the previous version of Cisco VNMC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome. |

### Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
vnmc# connect local-mgmt
Cisco Virtual Network Management Center
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, 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
```

The following example shows how to display version information for the Cisco VNMC:

```
vnmc (local-mgmt) # show version

Name Package Version GUI
---- -
core Base System 2.0(1) 2.0(1)
service-reg Service Registry 2.0(1) 2.0(1)
policy-mgr Policy Manager 2.0(1) 2.0(1)
resource-mgr Resource Manager 2.0(1) 2.0(1)
vm-mgr VM manager 2.0(1) none
```

The following example shows how to copy the Cisco VNMC software to the VM:

```
vnmc (local-mgmt) # copy scp://<user@example-server-ip>/example1-dir/vnmc.2.1.bin bootflash:/
Enter password:
100% 143MB 11.9MB/s 00:12
```

The following example shows how to see the directory information for Cisco VNMC:

```
vnmc (local-mgmt) # dir bootflash:/
14M Jul 28 2011 gui-automation.tgz

 887 May 28 2013 vnmc-dplug.2.0.1.bin
 20M May 28 2013 vnmc-vsgpa.2.0.1.bin
 20M May 28 2013 vnmc-vsmpa.2.0.1.bin
 403M Jan 31 01:58 vnmc.2.0.bin
```

```
Usage for bootflash://
```

```
18187836 bytes used
 3842128 bytes free
 22029964 bytes total
```

The following example shows how to start the update for the Cisco VNMCM:

```
vnmc(local-mgmt)# update bootflash:/vnmc.2.1.1a.bin
It is recommended that you perform a full-state backup before updating any VNMCM component.
Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco VNMCM:

```
vnmc(local-mgmt)# show version
```

| Name         | Package          | Version | GUI  |
|--------------|------------------|---------|------|
| core         | Base System      | 2.1     | 2.1  |
| service-reg  | Service Registry | 2.1     | 2.1  |
| policy-mgr   | Policy Manager   | 2.1     | 2.1  |
| resource-mgr | Resource Manager | 2.1     | 2.1  |
| vm-mgr       | VM manager       | 2.1     | none |

## Upgrading Cisco VSG from Release 4.2(1)VSG1(4.1) to 4.2(1)VSG2(1.1)

Enter the commands on all Cisco VSG nodes on your network.

### Before You Begin

- You are logged in to the CLI in EXEC mode.
- You have copied the new system image, kickstart image and the Cisco VSG policy agent image into the bootflash file system using the following commands:

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart-mz.VSG2.1.bin
bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin
```

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-mz.VSG2.1.bin
bootflash:nexus-1000v-mz.VSG2.1.bin
```

```
switch# copy scp://user@scpserver.cisco.com/downloads/vnmc-vsgpa.2.1(1b).bin
bootflash:vnmc-vsgpa.2.1(1b).bin
```

- You have confirmed that the system is in high availability (HA) mode for an HA upgrade using the **show system redundancy status** command.

### SUMMARY STEPS

1. **configure terminal**
2. **install all kickstart bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin system bootflash:nexus-1000v-mz.VSG2.1.bin vnmpa bootflash:vnmc-vsgpa.2.1(1b).bin**
3. **show vnmpa status**
4. **copy running-config startup-config**

### DETAILED STEPS

|        | Command or Action  | Purpose                           |
|--------|--------------------|-----------------------------------|
| Step 1 | configure terminal | Enters global configuration mode. |

|               | Command or Action                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>install all kickstart</b><br><b>bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin</b><br><b>system bootflash:nexus-1000v-mz.VSG2.1.bin</b><br><b>vnmpa bootflash:vnmc-vsghpa.2.1(1b).bin</b> | Installs the kickstart image, system image, and policy agent (PA) image.<br><br><b>Note</b> If you do not have a policy agent installed on the Cisco VSG before the <b>install all</b> command is executed, the PA will not be upgraded (installed) with the image. Make sure that the current version of policy agent is installed before you begin the upgrade process. |
| <b>Step 3</b> | <b>show vnm-pa status</b>                                                                                                                                                                   | Verifies that the new PA is installed and the upgrade was successful.<br><br><b>Note</b> You must have an existing PA installed before upgrading the PA using the <b>install all</b> command.                                                                                                                                                                             |
| <b>Step 4</b> | <b>copy running-config startup-config</b>                                                                                                                                                   | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.                                                                                                                                                                                                                                             |

### Configuration Example

The following example shows how to upgrade Cisco VSG Release 4.2(1)VSG1(4.1) to Release 4.2(1)VSG2(1.1):

```
vsg # configure terminal
vsg (config)# install all kickstart bootflash:nexus-1000v-kickstart-mz.VSG2.1.bin system
bootflash:nexus-1000v-mz.VSG2.1.bin vnmpa bootflash:vnmc-vsghpa.2.1(1b).bin
vsg (config)# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.1(1b)-vsg
vsg (config)# copy running-config startup-config
```

## Upgrading VSMs

### Upgrade Procedures

The following table lists the upgrade steps.



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

**Table 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. |

| If you are running this configuration                                           | Follow these steps                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Releases 4.0(4)SV1(3x) Series                                                   | <ol style="list-style-type: none"> <li>1 Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b)</li> <li>2 Upgrade from Releases 4.2(1)SV1(4x) and later releases to the current release</li> </ol>                                                                                |
| Release 4.2(1)SV1(4x) Series 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</li> <li>2 Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> <li>3 Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> </ol> |
| Release 4.2(1)SV1(4x) Series 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) and later releases to the current release</li> <li>2 Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> </ol>                                                                    |

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

**Table 6: Upgrade Paths from Releases 4.2(1)SV1(5x) and Later Releases**

| If you are running this configuration     | Follow these steps                                                                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| With vSphere 5.0 GA, patches, or updates. | <ol style="list-style-type: none"> <li>1 Upgrading VSMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> <li>2 Upgrading VEMs from Releases 4.2(1)SV1(4) and later releases to the current release</li> </ol> |

## 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

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

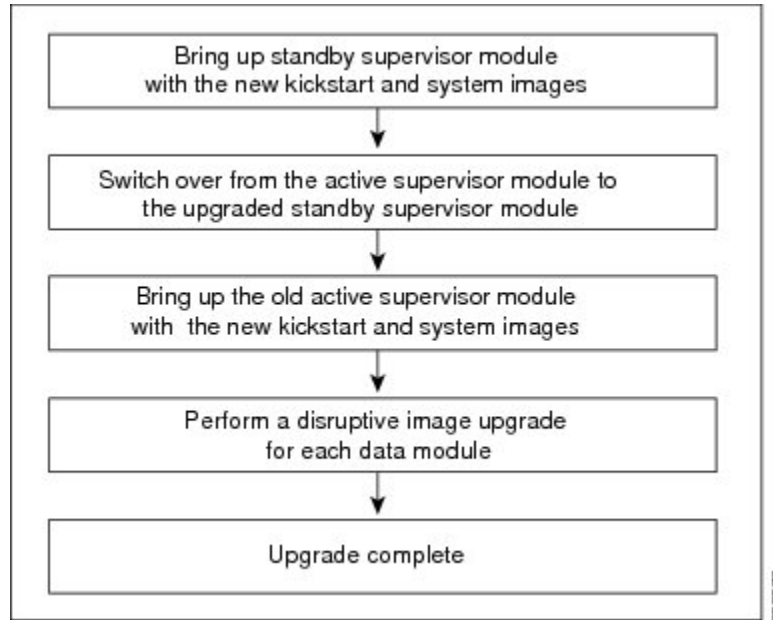
All of the following processes are initiated automatically by the upgrade process after the network administrator enters the **install all** command.



### ISSU Process for the Cisco Nexus 1000V

The following figure shows the ISSU process.

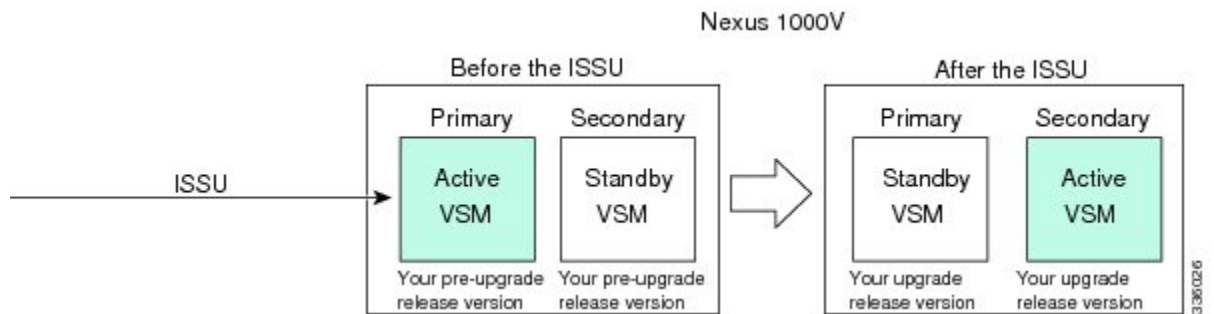
**Figure 11: ISSU Process**



### ISSU VSM Switchover

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

**Figure 12: 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)SV2(1.1x), 4.2(1)SV2(2.1x) to 5.2(1)SV3(1.1)

- 
- 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://software.cisco.com/download/navigator.html>

**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.SV2.2.2.iso
bootflash:nexus-1000v.4.2.1.SV2.2.2.iso
```

- Copy kickstart and system images.

```
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin
bootflash:nexus-1000v-kickstart-4.2.1.SV2.1.1a.bin
switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.4.2.1.SV2.2.2.bin
bootflash:nexus-1000v-4.2.1.SV2.1.1a.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.SV2.2.2.iso
```

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

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

```

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

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

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

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

```

Compatibility check is done:

| Module | bootable | Impact         | Install-type | Reason |
|--------|----------|----------------|--------------|--------|
| 1      | yes      | 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 (2.2) | yes          |
| 1      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | system    | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |

| Module     | Running-Version   | ESX Version                                 | VSM |
|------------|-------------------|---------------------------------------------|-----|
| 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.SV2.2.2.bin system
bootflash:nexus-1000v.4.2.1.SV2.2.2.bin

```

```

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

```

```

Verifying image bootflash:/nexus-1000v-4.2.1.SV2.1.1a.bin for boot variable "system".
[#####] 100% -- SUCCESS

```

```

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

```

```

Extracting "system" version from image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin.

```

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

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

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

```
Compatibility check is done:
Module bootable Impact Install-type Reason
----- -
 1 yes 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(2.2) yes
 1 kickstart 4.2(1)SV1(5.2) 4.2(1)SV2(2.2) yes
 2 system 4.2(1)SV1(5.2) 4.2(1)SV2(2.2) yes
 2 kickstart 4.2(1)SV1(5.2) 4.2(1)SV2(2.2) 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 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 and Cisco Virtual Network Management Center Installation and Upgrade Guide*.

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

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

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

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

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

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

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

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

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

- Upgrade using the ISO image.

```
switch# install all iso bootflash:nexus-1000v.4.2.1.SV2.2.2.iso
```

- Upgrade using the kickstart and system images.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart.4.2.1.SV2.2.2.bin system
bootflash:nexus-1000v.4.2.1.SV2.2.2.bin
```

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

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

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

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

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

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

Compatibility check is done:

| Module | bootable | Impact         | Install-type | Reason |
|--------|----------|----------------|--------------|--------|
| 1      | yes      | 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 (2.2) | yes          |
| 1      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | system    | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |
| 2      | kickstart | 4.2 (1) SV1 (5.2) | 4.2 (1) SV2 (2.2) | yes          |

| Module        | Running-Version   | ESX Version | VSM |
|---------------|-------------------|-------------|-----|
| Compatibility | ESX Compatibility |             |     |

```

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

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

```

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

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

Install is in progress, please wait.

```

Syncing image bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin to standby.
[#####] 100% -- SUCCESS

```

```

Syncing image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin to standby.
[#####] 100% -- SUCCESS

```

```

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

```

```

Performing configuration copy.
[#####] 100%2013 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) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
 loader: version unavailable [last: loader version not available]
 kickstart: version 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
 system: version 4.2(1)SV2(2.2) [build 4.2(1)SV2(2.2)]
 kickstart image file is: bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin
 kickstart compile time: 1/11/2012 3:00:00 [01/11/2012 12:49:49]

```

```

system image file is: bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin
system compile time: 1/11/2012 3:00:00 [01/11/2012 13:42:57]

```

## Hardware

```

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

```

```

Device name: Nexus1000v
bootflash: 1557496 kB

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```
-- SUCCESS
```

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

```
-- SUCCESS
```

```
Verifying image type.
```

```
-- SUCCESS
```

```
Extracting "system" version from image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin.
```

```
-- SUCCESS
```

```
Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart.4.2.1.SV2.2.2.bin.
```

```
-- SUCCESS
```

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

```
-- SUCCESS
```

```
Compatibility check is done:
```

```
Module bootable Impact Install-type Reason
```



```

 1 yes non-disruptive reset
 2 yes non-disruptive reset

```

Images will be upgraded according to following table:

| Module | Image     | Running-Version | New-Version    | Upg-Required |
|--------|-----------|-----------------|----------------|--------------|
| 1      | system    | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | yes          |
| 1      | kickstart | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | yes          |
| 2      | system    | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | yes          |
| 2      | kickstart | 4.2(1)SV1(5.2)  | 4.2(1)SV2(2.2) | 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.SV2.2.2.bin to standby.
-- SUCCESS

```

```

Syncing image bootflash:/nexus-1000v.4.2.1.SV2.2.2.bin to standby.
-- SUCCESS

```

```

Setting boot variables.
-- SUCCESS

```

```

Performing configuration copy.
-- SUCCESS

```

```

Module 2: Waiting for module online.
-- SUCCESS

```

```

Notifying services about the switchover.
-- SUCCESS

```

```

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

```

```

switch# attach module 2
Attaching to module 2 ...

```

```

To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, 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)#

```

---

## Upgrading VEMs

### VEM Upgrade Procedures

- VUM Upgrade Procedures
  - Set up VUM baselines. See [http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4\\_2\\_1\\_s\\_v\\_1\\_5\\_2/install\\_upgrade/vsm\\_vem/guide/b\\_Installation\\_and\\_Upgrade\\_Release\\_4\\_2\\_1SV1\\_5\\_2\\_appendix\\_0100.html#task\\_A93C11451B0B43F98468D15C83C1E5E5](http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_2/install_upgrade/vsm_vem/guide/b_Installation_and_Upgrade_Release_4_2_1SV1_5_2_appendix_0100.html#task_A93C11451B0B43F98468D15C83C1E5E5).
  - Initiate an upgrade from VUM. See [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97.
  - Upgrade VEM from VSM. See [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97.
- Manual upgrade procedures
  - Upgrading VIB Manually from the CLI. See [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 101
- Installing or upgrading stateless ESXi. See [Installing the VEM Software on a Stateless ESXi Host](#).

VEM upgrades fall into three types:

- An upgrade of 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](#).

An upgrade of 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 ESXi version intact. The first figure shows this flow.
- 2 Upgrade the ESX/ESXi without a change of the Cisco Nexus 1000V version. This process is addressed in the Workflow 2 figure.

If you are using VUM, set up a host patch baseline with the VEM's offline bundle. Then follow [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97.

If you are upgrading from the command line, see [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 101.

- 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 ESXi 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 ESXi 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 ESXi 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](#).
  - You can upgrade the ESXi 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.

### VEM Upgrade Methods from Release 4.2(1)SV1(5x), or Release 4.2(1)SV2(1.1x) to the Current Release

There are two methods for upgrading the VEMs.

- [Upgrading the VEMs Using VMware Update Manager from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 97
- [Upgrading the VEMs Manually from Release 4.2\(1\)SV1\(5x\) and Later Releases to the Current Release](#), on page 101

*Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(5x) and Later Releases to the Current Release*



#### Caution

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

## SUMMARY STEPS

1. switch# **show vmware vem upgrade status**
2. switch# **vmware vem upgrade notify**
3. switch# **show vmware vem upgrade status**
4. switch# **show vmware vem upgrade status**
5. Initiate the VUM upgrade process with the following commands.
6. switch# **show vmware vem upgrade status**
7. Clear the VEM upgrade status after the upgrade process is complete with the following commands.
8. switch# **show module**

## DETAILED STEPS

- 
- Step 1**      switch# **show vmware vem upgrade status**  
Display the current configuration.
- Note**      The minimum release of Cisco Nexus 1000V for VMware ESXi 5.0.0 hosts is Release 4.2(1)SV1(5).
- Step 2**      switch# **vmware vem upgrade notify**  
Coordinate with and notify the server administrator of the VEM upgrade process.
- Step 3**      switch# **show vmware vem upgrade status**  
Verify that the upgrade notification was sent.
- Note**      Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.
- Step 4**      switch# **show vmware vem upgrade status**  
Verify that the server administrator has accepted the upgrade in the vCenter. For more information about how the server administrator accepts the VEM upgrade, see [Accepting the VEM Upgrade, on page 104](#). Coordinate the notification acceptance with the server administrator. After the server administrator accepts the upgrade, proceed with the VEM upgrade.
- Note**      Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and consult the *Cisco Nexus 1000V Troubleshooting Guide*.
- Step 5**      Initiate the VUM upgrade process with the following commands.
- Note**      Before entering the following commands, communicate with the server administrator to confirm that the VUM process is operational.
- The vCenter Server locks the DVS and triggers VUM to upgrade the VEMs.
- a) switch# **vmware vem upgrade proceed**
  - b) switch# **show vmware vem upgrade status**
- Note**      The DVS bundle ID is updated and is highlighted.
- If the ESXi host is using 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 ESXi in maintenance mode to upgrade the VEM. This process is continued for other hosts in the DRS cluster until all the hosts are upgraded in the cluster. For details about DRS settings required and vMotion of VMs, visit the VMware documentation related to Creating a DRS Cluster.
- Step 6**      switch# **show vmware vem upgrade status**

Check for the upgrade complete status.

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

- a) switch# **vmware vem upgrade complete**
- b) switch# **show vmware vem upgrade status**

**Step 8** switch# **show module**

Verify that the upgrade process is complete.

The upgrade is complete.

The following example shows how to upgrade VEMs using VUM.



**Note**

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

```
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM410-201301152101-BG
switch#
switch# vmware vem upgrade notify
Warning:
Please ensure the hosts are running compatible ESX versions for the upgrade. Refer to
corresponding
"Cisco Nexus 1000V and VMware Compatibility Information" guide.
switch# show vmware vem upgrade status

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

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

```

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

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter) : Tue Jan 27 02:06:53 2014
Upgrade Start Time: : Tue Jan 27 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
switch#
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: : Tue Jan 27 10:03:24 2014
Upgrade Status Time(vCenter): : Tue Jan 27 02:06:53 2014
Upgrade Start Time: : Tue Jan 27 10:09:08 2013
Upgrade End Time(vCenter): : Tue Jan 27 10:09:08 2014
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
switch#
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status

Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
switch#
switch# show module

```

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

```

Mod Sw Hw

1 4.2(1)SV2(2.2) 0.0
2 4.2(1)SV2(2.2) 0.0
3 4.2(1)SV2(2.2) VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4 4.2(1)SV2(2.2) VMware ESXi 5.0.0 Releasebuild-623860 (3.0)

```

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

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

```
* this terminal session
switch#
```



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

### Upgrading the VEMs Manually from Release 4.2(1)SV1(5x) and Later Releases to the Current Release

#### Before You Begin



**Note** If VUM is installed, it should be disabled.

To manually install or upgrade the Cisco Nexus 1000V VEM on an ESXi host, follow the steps in [Upgrading the VEM Software Using the vCLI](#), on page 105.

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.

## SUMMARY STEPS

1. switch# **vmware vem upgrade notify**
2. switch# **show vmware vem upgrade status**
3. switch# **show vmware vem upgrade status**
4. Perform one of the following tasks:
5. switch# **vmware vem upgrade proceed**
6. switch# **show vmware vem upgrade status**
7. Coordinate with and wait until the server administrator upgrades all ESXi host VEMs with the new VEM software release and informs you that the upgrade process is complete.
8. switch# **vmware vem upgrade complete**
9. switch# **show vmware vem upgrade status**
10. switch# **show module**

## DETAILED STEPS

### Step 1

switch# **vmware vem upgrade notify**

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

- Step 2** switch# **show vmware vem upgrade status**  
Verify that the upgrade notification was sent.
- Step 3** switch# **show vmware vem upgrade status**  
Verify that the server administrator has accepted the upgrade in vCenter Server. For details about the server administrator accepting the VEM upgrade, see [Accepting the VEM Upgrade, on page 104](#). After the server administrator accepts the upgrade, proceed with the VEM upgrade.
- Step 4** Perform one of the following tasks:
- If the ESXi host is not hosting the VSM, proceed to Step 5.
  - If the ESXi host is hosting the VSM, coordinate with the server administrator to migrate the VSM to a host that is not being upgraded. Proceed to Step 5.
- Step 5** switch# **vmware vem upgrade proceed**  
Initiate the Cisco Nexus 1000V Bundle ID upgrade process.
- Note** If VUM is enabled in the vCenter environment, disable it before entering the **vmware vem upgrade proceed** command to prevent the new VIBs from being pushed to all the hosts.  
Enter the **vmware vem upgrade proceed** command so that the Cisco Nexus 1000V Bundle ID on the vCenter Server gets updated. If VUM is enabled and you do not update the Bundle ID, an incorrect VIB version is pushed to the VEM when you next add the ESXi to the VSM.
- Note** If VUM is not installed, the “The object or item referred to could not be found” error appears in the vCenter Server task bar. You can ignore this error message.
- Step 6** switch# **show vmware vem upgrade status**  
Check for the upgrade complete status.
- Step 7** Coordinate with and wait until the server administrator upgrades all ESXi 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 105](#).
- Step 8** switch# **vmware vem upgrade complete**  
Clear the VEM upgrade status after the upgrade process is complete.
- Step 9** switch# **show vmware vem upgrade status**  
Check the upgrade status once again.
- Step 10** switch# **show module**  
Verify that the upgrade process is complete.
- Note** The line with the bold characters in the preceding example display that all VEMs are upgraded to the current release.  
The upgrade is complete.

---

The following example shows how to upgrade VEMs manually.



**Note**

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM410-201401152101-BG
```

```
switch#
```

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

```
Warning:
```

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

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

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

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

```
switch#
```

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

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

```
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Tue Jan 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jan 28 02:06:53 2014
Upgrade Start Time: Tue Jan 28 10:09:08 2014
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG
```

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

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

```
switch#
```

```
switch# vmware vem upgrade complete
```

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

```
Upgrade VIBs: System VEM Image
```

```

Upgrade Status:
Upgrade Notification Sent Time:
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error
Upgrade Bundle ID:
 VSM: VEM500-201401164100-BG
 DVS: VEM500-201401164100-BG

```

```

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

```

```

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

```

```

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

```

```

* this terminal session
switch#

```

### 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.

## SUMMARY STEPS

1. In the vCenter Server, choose **Inventory > Networking**.
2. Click the **vSphere Client DVS Summary** tab to check for the availability of a software upgrade.
3. Click **Apply upgrade**.

## DETAILED STEPS

**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 13: 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.

### 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 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 ESXi system that the vCenter Server system manages. vCLI commands are especially useful for ESXi hosts because ESXi does not include a service console.

- 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.

## SUMMARY STEPS

1. [root@serialport -]# **cd tmp**
2. Determine the upgrade method that you want to use and enter the appropriate command.
  - **vihostupdate**  
Installs the ESXi and VEM software simultaneously if you are using the vCLI.
3. For ESXi 5.0.0 or later hosts, enter the appropriate commands as they apply to you.
4. Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information* by typing the following commands.
5. switch# **show module**

## DETAILED STEPS

- 
- Step 1** [root@serialport -]# **cd tmp**  
Go to the directory where the new VEM software was copied.
- Step 2** Determine the upgrade method that you want to use and enter the appropriate command.
- **vihostupdate**  
Installs the ESXi and VEM software simultaneously if you are using the vCLI.
- Step 3** For ESXi 5.0.0 or later hosts, enter the appropriate commands as they apply to you.
- a) ~ # **esxcli software vib install -d /absolute-path/VEM\_bundle**
  - b) ~ # **esxcli software vib install -v /absolute-path/vib\_file**
- Note** You must specify the absolute path to the *VEM\_bundle* and *vib\_file* files. The absolute path is the path that starts at the root of the file system such as `/tmp/vib_file`.
- Step 4** Display values with which to compare to *Cisco Nexus 1000V and VMware Compatibility Information* by typing the following commands.
- a) [root@serialport tmp]# **vmware -v**
  - b) root@serialport tmp]# # **esxupdate query**
  - c) [root@host212 ~]# . ~ # **vem status -v**
  - d) [root@host212 ~]# **vemcmd show version**
- Step 5** switch# **show module**  
Display that the VEMs were upgraded by entering the command on the VSM.
- 

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

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



**Note**

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

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

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v164-4.2.1.2.2.2.0-3.0.1.vib
Installation Result
 Message: Operation finished successfully.
 Reboot Required: false
 VIBs Installed: Cisco_bootbank_cisco-vem-v164-esx_4.2.1.2.2.2.0-3.0.1
 VIBs Removed:
 VIBs Skipped:
~ #

[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-843203
root@serialport tmp]# # esxupdate query
-----Bulletin ID----- Installed----- Summary-----
VEM500-201401164100 2014-01-27T08:18:22 Cisco Nexus 1000V 4.2(1)SV2(2.2)

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

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

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

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

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

```
6 4.2(1)SV2(2.2) VMware ESXi 5.1.0 Releasebuild-843203 (3.0)
```

```
Mod Server-IP Server-UUID Server-Name
--- -
1 10.105.232.25 NA NA
2 10.105.232.25 NA NA
3 10.105.232.72 e6c1a563-bc9e-11e0-bd1d-30e4dbc2baba 10.105.232.72
6 10.105.232.70 ecebfd42-bc0e-11e0-bd1d-30e4dbc2b892 10.105.232.70
```

```
switch#
```

**Note**

---

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

---



# Examples of Cisco Prime NSC OVA Template Deployment and Cisco Prime NSC ISO Installations

---

This chapter contains the following sections:

- [OVA Installation Using vSphere 5.0 Installer, page 139](#)
- [OVA Installation Using an ISO Image, page 141](#)

## OVA Installation Using vSphere 5.0 Installer

### Before You Begin

- Ensure that you have the Virtual Supervisor Module (VSM) IP address available
- Ensure that you have all the proper networking information available, including the IP address you will use for your Cisco Prime NSC instance
- Ensure that you have the Cisco Prime NSC ova image

- 
- Step 1** Open your vSphere client.
- Step 2** Click **Hosts and Clusters** and choose an ESXi host.
- Step 3** From the toolbar, choose **File > Deploy OVF Template**.
- Step 4** In the **Deploy OVF Template** dialog box, click **Browse** to choose an .ova file on your local machine, or choose a file from another location (URL).
- Step 5** From the **Open** dialog box, choose the appropriate .ova file and click **Open**.
- Step 6** Click **Next**.  
The **OVF Template Details** dialog box appears inside the **Deploy OVF Template** dialog box. The **OVF Template Details** dialog box is the first of ten pages in the **Deploy OVF Template** dialog box that you use to set parameters for the Cisco Prime NSC instance.

- Step 7** View your template details and click **Next**.
- Step 8** In the **User License Agreement** window, view the license and click **Accept**.
- Step 9** Click **Next**.
- Step 10** In the **Name and Location** window, do the following:
- In the **Name** field, enter a template name.
  - In the **Inventory Location** area, choose the appropriate folder and click **Next**.
- Step 11** In the **Deploy Configuration** window, from the Configuration drop-down list, choose **NSC Installer** and click **Next**.
- Step 12** In the **Resource Pool** window, choose the appropriate location to deploy the Cisco Prime NSC and click **Next**.
- Step 13** In the **Storage** window, choose an appropriate location to store the virtual machine files and click **Next**.
- Step 14** In the **Display Format** window, keep default settings and click **Next**.
- Step 15** In the **Network Mapping** window, choose an appropriate configured management network VLAN for Cisco Prime NSC and click **Next**.
- Step 16** In the **Properties** window, in the **IP Address** area, do the following:
- Enter an IP address in the **IPv4 IP Address** field.
  - Enter an IP netmask in the **IPv4 IP Netmask** field.
  - Enter a gate address in the **IPv4 Gateway** field.
- Note** The netmask is defaulted to 255.255.255.0.
- Step 17** In the **NSC DNS** area, do the following:
- Enter the host name in the **Host Name** field.
  - Enter an IP address in the **NSC IP** field.
- Step 18** In the **NSC NTP** area, enter the NTP server IP address in the **NTP server** field.
- Step 19** In the **NSC Password** area, enter a password in the **NSC Password** field or the **NSC Secret** field.
- Note** You enter the admin password in the **Password** field.
- Step 20** Click **Next**.
- Step 21** In the **Ready to Complete** window, verify the configuration details for Cisco Prime NSC and click **Finish** to deploy Cisco Prime NSC on the selected ESXi host.
- Note** Select **Power on after deployment** check box to start Cisco Prime NSC immediately after the deployment completes.
- The progress dialog box appears. Once the virtual machine is installed, the **Deployment Completed Successfully** dialog box opens.
- Step 22** Click **Close**.  
The Cisco Prime NSC instance is created.
-



# OVA Installation Using an ISO Image

---

- Step 1** Download a Cisco Prime NSC ISO to your client machine.
- Step 2** Open a vCenter client.
- Step 3** Create a virtual machine on the appropriate host as follows:
- Ensure your virtual machine size is 220 GB split into two disks (Disk1 having 20GB and Disk2 having 200GB).
  - Ensure your virtual machine has 4 GB of RAM.
  - Choose **Red Hat Enterprise Linux 5 64-bit** as your operating system.
- Step 4** Power on your virtual machine.
- Step 5** Mount the ISO to the virtual machine CD ROM drive as follows:
- Right-click the virtual machine and choose **Open the VM Console**.
  - From the virtual machine console, click Connect/Disconnect CD/DVD Devices.
  - Choose **CD/DVD Drive1**.
  - Choose **Connect to ISO Image on Local Disk**.
  - Choose the ISO image that you downloaded.
- Step 6** Reboot the VM using VM, Guest, and press **Ctrl-Alt-Del**.
- Step 7** In the ISO installer, enter the appropriate values in the **ISO installer** field.
- Step 8** Once installation is completed, click **Reboot** to create the Cisco Prime NSC instance.
-





## INDEX

### A

- accepting VEM upgrade [104, 134](#)
- access [45](#)
  - firewall ports [45](#)

### B

- bootflash [65](#)

### C

- Cisco Cloud Services Platform [65](#)
  - installation [65](#)
- Cisco port profile [26](#)
- Cisco Prime NSC [43](#)
  - overview [43](#)
  - system requirements [43](#)
- Cisco VSG [1](#)
- configuring [31, 57](#)
  - initial settings [57](#)
  - tenant on Prime NSC [31](#)
- configuring {security profile} [30](#)
  - tenant [30](#)

### D

- datastore [54](#)
- downloading [23](#)
  - vCenter extension file [23](#)
- dynamic operation [5](#)

### E

- enabling [37](#)
  - global policy engine logging [37](#)
- enabling logging [36](#)

- enabling traffic [37, 38](#)
- ESXi server [48](#)
  - requirement [48](#)

### F

- firewall ports [45](#)
  - access [45](#)
- firewall protection [37, 38](#)

### G

- global policy-engine [37](#)
- guidelines and limitation [66](#)
  - Cisco Cloud Services Platform [66](#)

### H

- hardware requirements [14](#)
- high availability [11, 54](#)
- host requirements [21, 51](#)

### I

- information [46, 74](#)
  - configuration [46](#)
  - installation [46](#)
    - Prime NSC upgrade [74](#)
- initial settings [59](#)
- installing [48](#)
  - Cisco Prime NSC [48](#)
- Installing [27](#)
  - VSG from OVA template [27](#)
- installing Cisco VSG [55](#)
- ISO file [55](#)
- ISO image [54, 141](#)

ISSU [86, 87, 116, 117](#)

command attributes [87, 117](#)

dual VSMs [86, 116](#)

VSM switchover [87, 117](#)

ISSU process [87, 117](#)

## L

log [39](#)

logging [36](#)

enabling [36](#)

level 6 [36](#)

policy engine [36](#)

## M

multitenancy [1](#)

multitenant [7](#)

multitenant access [4](#)

## N

Nexus 1000V device terminology [52](#)

## O

OVA file [13](#)

OVA installation [141](#)

OVF template [13, 54](#)

## P

password [47](#)

shared secret [47](#)

planning checklist [14](#)

PNSC [7](#)

prerequisites [18, 53](#)

installing the VSG [53](#)

Prime NSC [79, 81](#)

Prime NSC architecture [2, 8](#)

Prime NSC benefits [7](#)

Prime NSC components [7](#)

Prime NSC installation [21](#)

Prime NSC security [8](#)

## R

registering [24, 61, 62, 63](#)

vCenter extension plugin [24](#)

Cisco VSG [61](#)

Nexus 1000V [62](#)

vCenter [63](#)

requirements [16, 45](#)

Prime NSC installation [16](#)

VLAN configuration [16](#)

web-based GUI client [45](#)

rule [35](#)

permit-all [35](#)

## S

security policy [35](#)

security profile [31](#)

policy management [31](#)

shared secret [47](#)

password [47](#)

shared secret password [21](#)

software images [85, 115](#)

software requirements [14](#)

standby Cisco VSG [59](#)

statistics [39](#)

system requirements [43](#)

Cisco Prime NSC [43](#)

## T

traffic flow [39, 40](#)

trusted zones [1](#)

## U

upgrade [73, 75](#)

guidelines [75](#)

limitations [75](#)

procedure [73](#)

upgrade procedures [84, 96, 114, 126](#)

VEM [96, 126](#)

upgrading [79, 81, 88, 97, 101, 105, 111, 118, 127, 131, 135](#)

VEM software using the vCLI [105, 135](#)

VSMs from 4.2(1) SV1(4), (4a), (4b), (5.1), (5.1a), (5.2) to SV2(1.1a) [88, 118](#)

**V**

VEM [96, 97, 126, 127](#)  
    upgrade methods [97, 127](#)  
    upgrade procedures [96, 126](#)  
verifying [36](#)  
    permit-all rule [36](#)  
verifying communication [37](#)  
virtualization [5](#)  
VLAN [4](#)  
VLAN setting [6](#)  
VLAN usages [6](#)  
VM communication [6](#)  
VM port-profile [38](#)  
VM requirements [51](#)

vnmc [79](#)  
VNMC [111](#)  
VSG [74](#)  
    upgrade [74](#)  
VSG architecture [2](#)  
VSG device terminology [52](#)  
VSG information [16](#)  
VSG setting [6](#)

**W**

web-based GUI client [45](#)  
    requirements [45](#)

