Cisco VSG for VMware vSphere, Release 5.2(1)VSG2(1.2c) and Cisco Prime NSC, Release 3.4.1b Installation and Upgrade Guide

First Published: 2015-02-18

Last Modified: 2019-05-29

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

CONTENTS

Preface

The preface contains the following sections:

Audience

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

Document Conventions

Note As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.

Command descriptions use the following conventions:

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

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

Examples use the following conventions:

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

This document uses the following conventions:

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

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

Related Documentation for 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 PNSC 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 Prime Network Services Controller Documentation

The *Cisco Prime Network Services Controller* 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

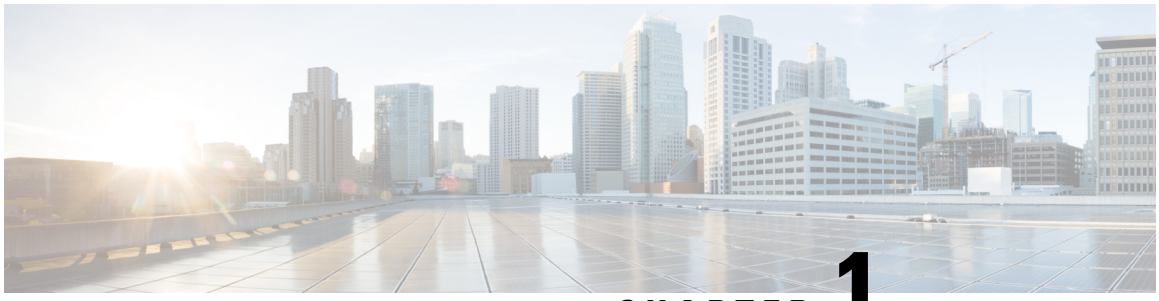
To provide technical feedback on this document, or to report an error or omission, please send your comments to vsg-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

Overview

This chapter contains the following sections:

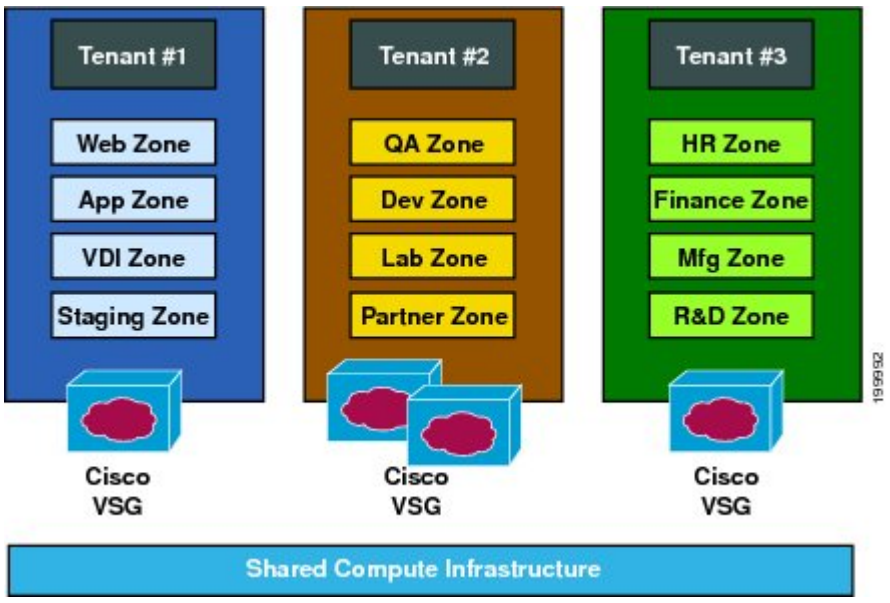
Information About Installing the Cisco PNSC and the Cisco VSG

You must install the Cisco Prime Network Services Controller (Cisco PNSC) 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 PNSC-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.

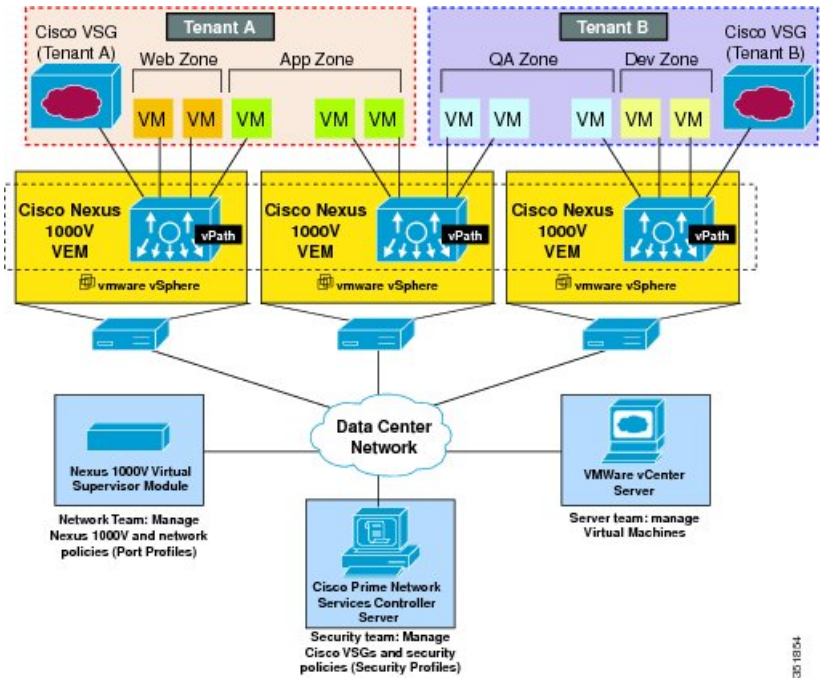
Figure 1: Trusted Zone-Based Access Control Using Per-Tenant Enforcement with the Cisco VSG



Cisco PNSC 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 (Cisco vPath). Cisco 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



Cisco 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 Cisco 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 Cisco 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

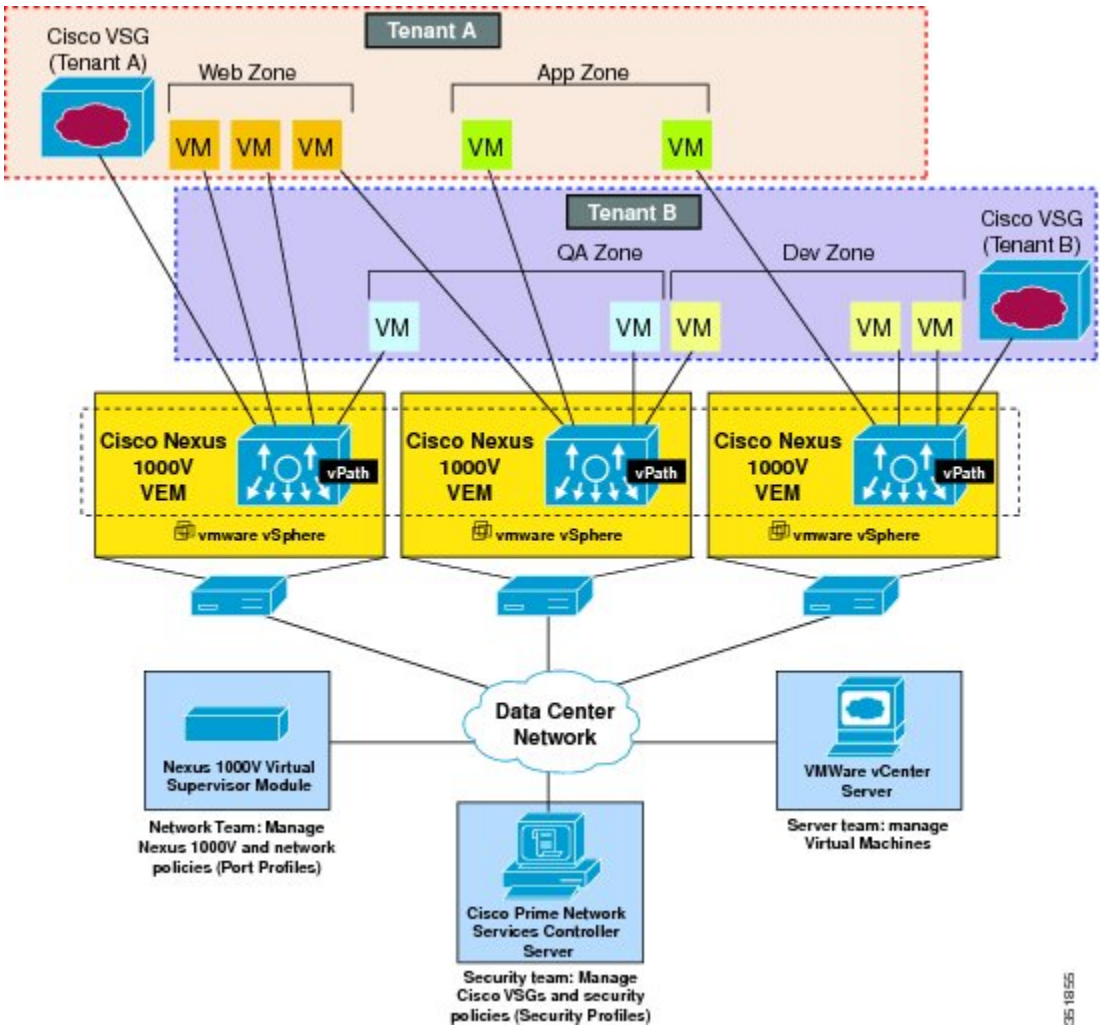
cross tenant boundaries. You can deploy a Cisco VSG at the tenant level, at the virtual data center (vDC) level, or at the vApp level.

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 PNSC, 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.

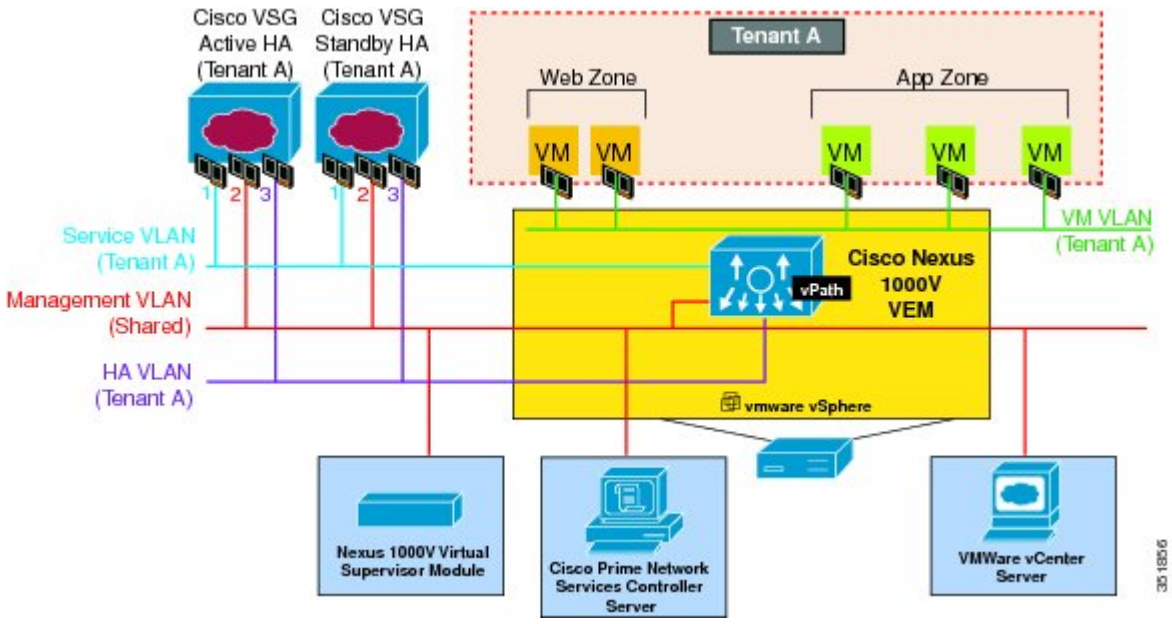
As VMotion events are triggered, VMs move across physical servers. Because the Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to VMotion events.

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 withCisco VSG.
- The management VLAN connects the management platforms such as the VMware vCenter, the Cisco PNSC, 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 PNSC

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

Cisco PNSC Key Benefits

The Cisco PNSC 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 PNSC Components

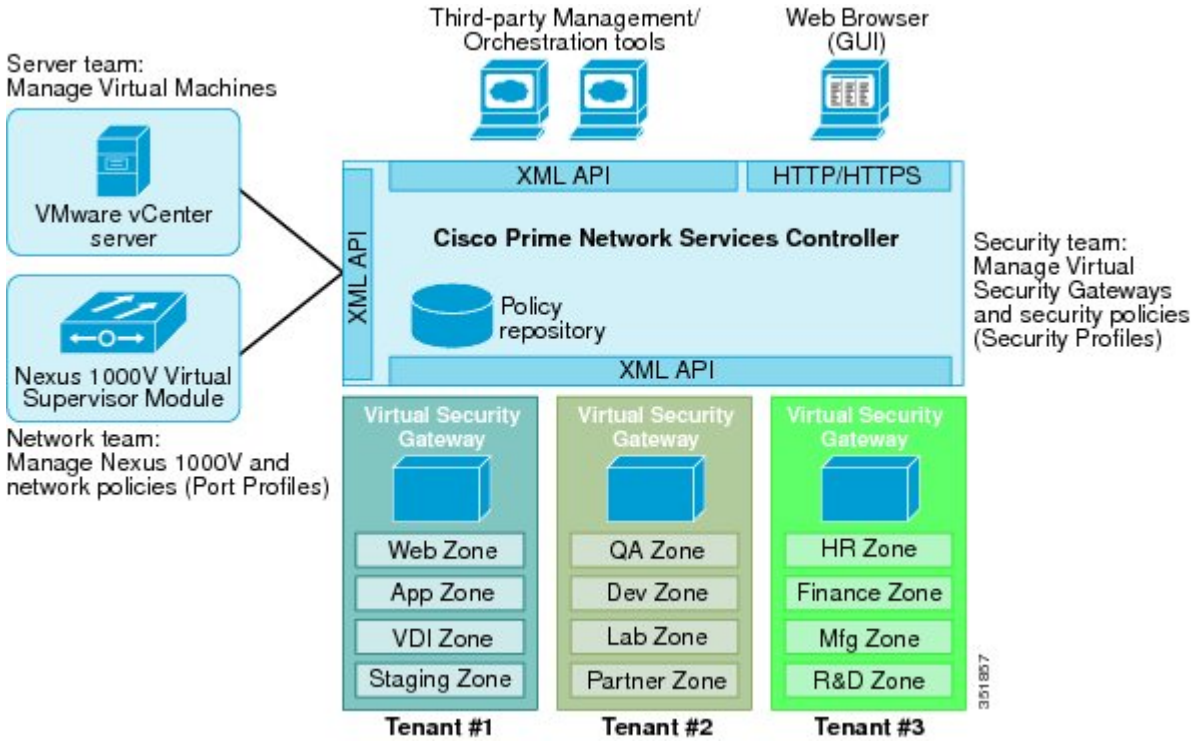
The Cisco PNSC architecture includes the following components:

- 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 PNSC Architecture

The Cisco PNSC architecture includes the components in the following figure:

Figure 5: Cisco PNSC Components



Cisco PNSC Security

The Cisco PNSC 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 PNSC API

The Cisco PNSC 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 PNSC and Cisco VSG

The Cisco PNSC 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 PNSC 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

For Cisco PNSC installation system requirement, see Installing Cisco Prime Network Services Controller, on page 41.

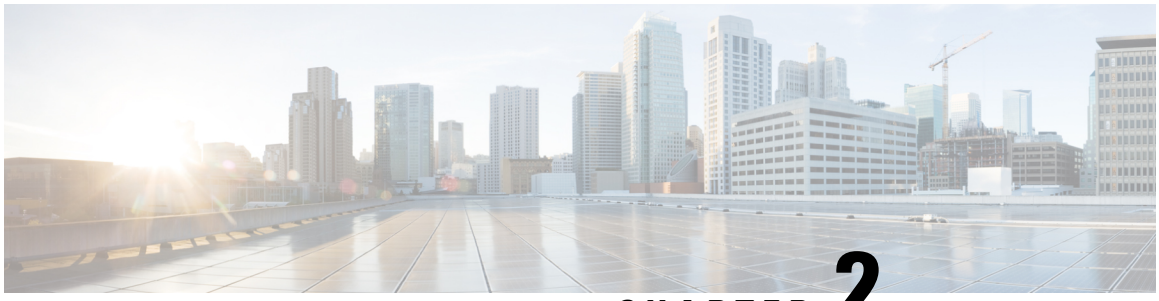
Information About High Availability

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 PNSC 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 PNSC 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.



CHAPTER 2

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

This chapter contains the following sections:

Information About Installing the Cisco PNSC and the Cisco VSG

This chapter describes how to install and set up a basic working configuration of the Cisco PNSC 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 PNSC Installation Planning Checklists

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

Basic Hardware and Software Requirements

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

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

Requirement	Description
Two Virtual CPUs	1.5 GHz for each Virtual CPU
Memory	4 GB RAM for the Cisco VSG and 4 GB RAM for the Cisco PNSC or 8 GB for both

Disk Space	One of the following, depending on InterCloud functionality:
	• With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows:
	  • 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:
	  • Disk 1: 20 GB
	  • Disk 2: 20 GB

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 or 5.1
VMware vCenter	Release 5.1 (5.0 vCenter supports host version upto 5.0)
Intel Virtualization Technology (VT)	Enabled in the BIOS

Requirement	Description
Browser	Any of the following browsers: • 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 PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome.
Ports	Access to the Cisco PNSC application using a web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports): • 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.

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 (NEXUS1000V_LAN_SERVICES_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 with1024 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 PNSC and Cisco VSG Information

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

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

Type	Your Information
Mode for installing the Cisco VSG	• Standalone • HA primary • HA secondary
Cisco VSG VLAN number • Service (1) • Management (2) • High availability (HA) (3)	
Cisco VSG port profile name • Data (1) • Management (2) • High availability (HA) (3) **Note** The numbers indicate the VSG port profile that must be associated with the VSG VLAN number.	
HA pair ID (HA domain ID)	
NSC DNS IP address	
NSC NTP IP address	
Cisco VSG admin password	
Cisco PNSC admin password	
Cisco VSM admin password	
Shared secret password (Cisco PNSC, Cisco VSG policy agent, Cisco VSM policy agent)	

Tasks and Prerequisites Checklist

Tasks	Prerequisites
Task 1: Installing the Cisco PNSC from an OVA Template, on page 19	Make sure that you know the following: • The Cisco PNSC OVA image is available in the vCenter. • Know the IP/subnet mask/gateway information for the Cisco PNSC. • 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 PNSC 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 PNSC, VSM, and Cisco VSG).
Task 2: On the Cisco PNSC, Setting Up VM-Mgr for vCenter Connectivity, on page 21	Make sure that you know the following: • Supported Adobe Flash Player given in System Requirements, on page 9 • IP address of the Cisco PNSC • The password for Admin user

Tasks	Prerequisites
Task 3: On the VSM, Configuring the Cisco PNSC Policy Agent, on page 23	Make sure that you know the following: • The Cisco PNSC policy-agent image is available on the VSM (for example, vsmcpa.3.2.3a.bin) **Note** The string **vsmcpa** must appear in the image name as highlighted. • The IP address of the Cisco PNSC • The shared secret password you defined during the Cisco PNSC installation • That IP connectivity between the VSM and the Cisco PNSC 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 PNSC image bundle to boot from a flash drive and to complete registration with the Cisco PNSC.
Task 4: On the VSM, Preparing Cisco VSG Port Profiles, on page 24	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.

Tasks	Prerequisites
Task 5: Installing the Cisco VSG from an OVA Template, on page 26	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 PNSC 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 PNSC IP address • The shared secret password • The IP connectivity between Cisco VSG and Cisco PNSC is okay. • The Cisco VSG NSC-PA image name (nsc-vsgpa.2.1.3i.bin) is available.
Task 6: On the Cisco VSG and Cisco PNSC, Verifying the NSC Policy-Agent Status, on page 29	—
Task 7: On the Cisco PNSC, Configuring a Tenant and Security Profile, on page 29	Make sure that you know the following: • Supported Adobe Flash Player given in System Requirements, on page 9 • The IP address of the Cisco PNSC • The password for Admin user
Task 8: On the Cisco PNSC, Importing Service Image, on page 31	—
Task 10: On the Cisco PNSC, Configuring a Permit-All Rule, on page 33	—

Tasks	Prerequisites
Task 11: On the Cisco VSG, Verifying the Permit-All Rule, on page 34	—
Task 12: Enabling Logging, on page 34	—
Task 13: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, on page 36	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 (for example, 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 38	—

Host Requirements

- ESXi platform that runs VMware software release 5.5, 6.0, and 6.5a with a minimum of 4 GB physical RAM for the Cisco VSG and 4 GB physical RAM for the Cisco PNSC.
- 1 processor
- Four Virtual CPUs with speed of 1.5 GHz for each virtual CPU

Obtaining the Cisco PNSC 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 PNSC software is available for download at the following URL:

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

Task 1: Installing the Cisco PNSC from an OVA Template

Before you begin

Know the following:

- The Cisco PNSC OVA image is available in the vCenter.

- Know the IP/subnet mask/gateway information for the Cisco PNSC.
- 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 PNSC 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 PNSC, VSM, and Cisco VSG).

Procedure

Step 1 Use the VMware vSphere Client to log into the vCenter server.

Step 2 Choose the host on which to deploy the Cisco PNSC VM.

Step 3 From the File menu, choose **Deploy OVF Template**.

Step 4 In the **Source** window, choose the Cisco PNSC OVA, then click **Next**.

Step 5 In the **OVF Template Details** window, review the details of the Cisco PNSC 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 PNSC Restore fields.

Note For choosing the shared secret password, see the *Shared Secret Password Criteria*.

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 PNSC is deployed.

Step 14 After Cisco PNSC is successfully deployed, click **Close**.

Step 15 Power on the Cisco VSG VM.

Task 2: On the Cisco PNSC, 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 PNSC, on page 21
- Registering the vCenter Extension Plugin in the vCenter, on page 22
- Configuring the vCenter in VM Manager in the Cisco PNSC, on page 22

Downloading the vCenter Extension File from the Cisco PNSC

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 PNSC
- The password for Admin user

Procedure

Step 1 In your browser, enter https://*server-ip-address* where *server-ip-address* is the Cisco PNSC IP address.

Step 2 In the **Website Security Certificate** window, choose **Continue to this website**.

Step 3 In the Cisco PNSC login window, enter the username **admin** and the admin user password. This is the password that you set when installing the Cisco PNSC.

Step 4 In the Cisco PNSC 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 22).

What to do next

Go to Registering the vCenter Extension Plugin in the vCenter, on page 22.

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 PNSC, on page 21.

Procedure

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 PNSC 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 PNSC, on page 22.

Configuring the vCenter in VM Manager in the Cisco PNSC

Before you begin

See Task 2: On the Cisco PNSC, Setting Up VM-Mgr for vCenter Connectivity, on page 21.

Procedure

Step 1 In Cisco PNSC, 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 PNSC Policy Agent

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

Before you begin

Make sure that you know the following:

- The Cisco PNSC policy-agent image is available on the VSM (for example, vsmcpa.3.2.3a.bin)

Note The string **vsmcpa** must appear in the image name as highlighted.

- The IP address of the Cisco PNSC
- The shared secret password you defined during the Cisco PNSC installation
- That IP connectivity between the VSM and the Cisco PNSC 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 PNSC image bundle to boot from a flash drive and to complete registration with the Cisco PNSC.

Procedure

Step 1 On the VSM, enter the following commands:

```
vsm# configure terminal
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# registration-ip 10.193.75.95
vsm(config-nsc-policy-agent)# shared-secret Example_Secret123
vsm(config-nsc-policy-agent)# policy-agent-image vsmcpa.3.2.3a.bin
vsm(config-nsc-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

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

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.4(2)-vsm
vsm
```

The VSM is now registered with the Cisco PNSC.

Example

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

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installation Failure
PNSC not reachable.
vsm#
```

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

```
vsm# show nsc-pa status
NSC 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.

Procedure

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 PNSC 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 PNSC IP address
- The shared secret password
- The IP connectivity between Cisco VSG and Cisco PNSC is okay.
- The Cisco VSG NSC-PA image name (nsc-vsgpa.2.1.3i.bin) is available.

Procedure

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:

a) 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.

b) Click **Next**.

Step 10 In the **Deploy OVF Template—Network Mapping** window, do the following:

a) Choose **VSG Data** for the data interface port profile.

b) Choose **Management** for the management interface port profile.

c) Choose **VSG-ha** for the HA interface port profile .

d) 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 PNSC.

Step 11 In the **Deploy OVF Template—Properties** window, do the following:

a) In the **OvfDeployment** field, select **ovf** to continue the configuration. Select **ignore** for manual configuration.

b) From the **HARole** drop-down list, choose HA role.

c) In the **HAid** field, enter the high-availability identification number for a Cisco VSG pair (value from 1 through 4095).
d) In the **Password** field, enter a password that contains at least one uppercase letter, one lowercase letter, and one number.
e) In the **ManagementIpV4** field, enter the IP address for the Cisco VSG.
f) In the **ManagementIpV4 Subnet** field, enter the subnet mask.
g) In the **Gateway** field, enter the gateway name.
h) In the **VnmcIpV4** field, enter the IP address of the Cisco PNSC.
i) In the **SharedSecret** field, enter the shared secret password defined during the Cisco PNSC installation.
j) Click **Next.**

Note For the shared secret password guidelines, see *Shared Secret Pasword* section.

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 PNSC 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 PNSC 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:

a) Right click and choose **Edit Settings**.
b) 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:

a) 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 PNSC, Verifying the NSC Policy-Agent Status

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

Procedure

Step 1 Log in to the Cisco VSG.

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

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
vsg#
```

Step 3 Log in to the Cisco PNSC.

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 PNSC, Configuring a Tenant and Security Profile

This task includes the following subtasks:

- Configuring a Tenant on the Cisco PNSC, on page 30
- Configuring a Security Profile on the Cisco PNSC, on page 30

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 PNSC
- The password for Admin user

Procedure

Step 1 In your browser, enter https://*server-ip-address* where *server-ip-address* is the Cisco PNSC IP address.

Step 2 In the **Website Security Certificate** window, choose **Continue to this website**.

Step 3 In the Cisco PNSC login window, enter the username **admin** and the admin user password.

Step 4 In the Cisco PNSC main window, choose **Resource Management** > **Resources** to check the Cisco VSG and VSM registration in the Cisco PNSC.

What to do next

Go to Configuring a Tenant on the Cisco PNSC, on page 30

Configuring a Tenant on the Cisco PNSC

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 PNSC.

Procedure

Step 1 In the Cisco PNSC, 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 PNSC, on page 30

Configuring a Security Profile on the Cisco PNSC

You can configure a security profile on the Cisco PNSC.

Procedure

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 PNSC, Adding a Compute Firewall, on page 31. 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 PNSC, Importing Service Image, on page 31.

Task 8: On the Cisco PNSC, Importing Service Image

This step is required to instantiate a VSG service device from an image in Task 9: On the Cisco PNSC, Adding a Compute Firewall, on page 31. This step is not required for assigning a VSG or VSG pool option in Task 9: On the Cisco PNSC, Adding a Compute Firewall, on page 31.

Procedure

Step 1 Log in to the Cisco PNSC.

Step 2 Choose **Resource Management** > **Resources** > **Images**.

Step 3 Click **Import Service Image**.

Step 4 In the Import Service Image dialog box, do the following:

a) Enter a name and description for the image you are importing.
b) In the **Type** field, select **VSG**.
c) In the **Version** field, enter a version to assign to the image.
d) In the **Protocol** field, choose a protocol.
e) In the **Hostname / IP Address** field, enter the hostname or IP address of the remote host to which you downloaded the images.
f) In the **User Name** field, enter the account username for the remote host.
g) In the **Password** field, enter the account password for the remote host.
h) In the **Remote File** field, enter the absolute path and filename of the service image, starting with a slash, such as /mnt/nexus-1000v.5.2.1.VSG2.2.1.ova.

Task 9: On the Cisco PNSC, 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 PNSC 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 PNSC. For more information, see Task 6: On the Cisco VSG and Cisco PNSC, Verifying the NSC Policy-Agent Status, on page 29.
- 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 PNSC. For more information on importing service images, see Task 8: On the Cisco PNSC, Importing Service Image, on page 31.

Procedure

Step 1 Log in to the Cisco PNSC.

Step 2 Choose **Resource Management** > **Managed Resources** > **root** > *tenant* > **Network Services**.

Step 3 From the **Actions** drop-down list, select **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 32, 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 33, 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	Compute firewall name. 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.
Description	Compute firewall description.
Host Name	Management hostname of the firewall.

Field	Description
Device Configuration Profile	Do either of the following: • 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	Assign a VSG to the compute firewall. In the **VSG Device** drop-down list, choose the required service device.
Assign VSG Pool	Assign a VSG pool to the compute firewall. In the **VSG Pool** field, either choose the required pool from the drop-down list or click **Add Pool** to add a new pool.
Instantiate	Instantiate a VSG service device from an available image. 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 PNSC, Configuring a Permit-All Rule

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

Procedure

Step 1 Log in to the Cisco PNSC.

Step 2 In the Cisco PNSC 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 35
- Enabling Global Policy-Engine Logging, on page 35

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.

Procedure

Step 1 Log in to the Cisco PNSC.

Step 2 In the Cisco PNSC 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 35.

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.

Procedure

Step 1 Log in to the Cisco PNSC.

Step 2 In the Cisco PNSC 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:

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 (for example, 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.

Procedure

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 vsg1 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 vsg1 profile SP_web
  no shutdown
  state enabled
```

What to do next

Go toVerifying the VSM or VEM for Cisco VSG Reachability, on page 37.

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 vsg 10.1.1.251 v-920 Alive 3,6,

------------------------------------------------------------------------------
Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Port Information
------------------------------------------------------------------------------
PortProfile:Vsg220
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 VNSP 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:

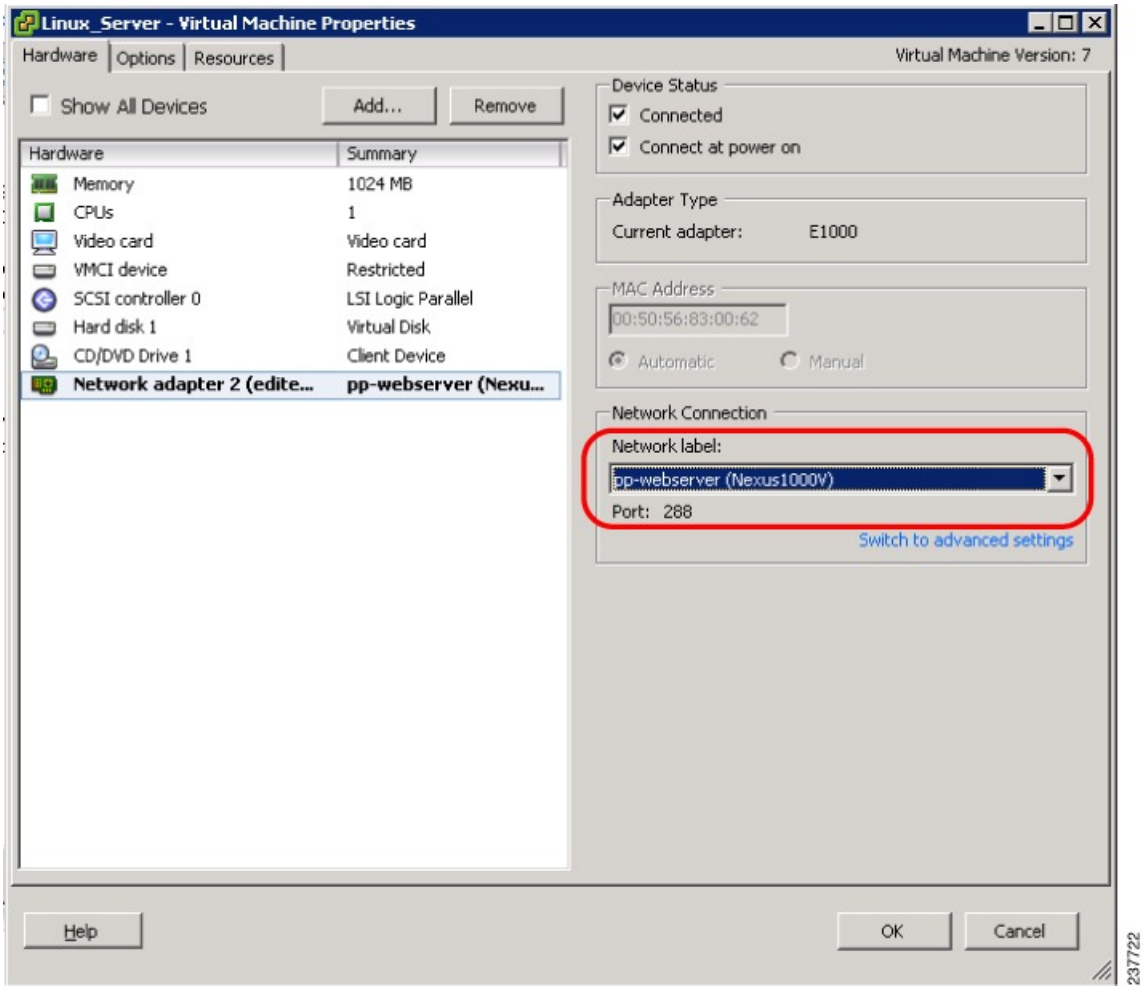
Sending Traffic Flow

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

Procedure

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:

a) Log in to any of your client virtual machine (Client-VM).

b) 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

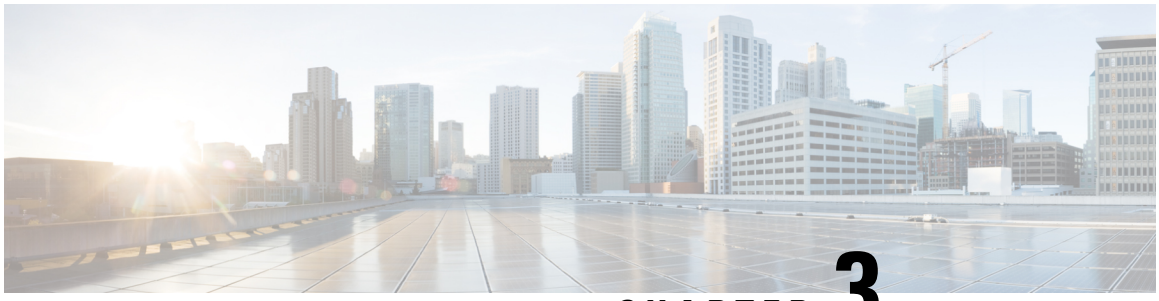
Go to Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 40.

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
```



CHAPTER 3

Installing Cisco Prime Network Services Controller

This chapter contains the following sections:

Information About the Cisco PNSC

The Cisco Prime Network Services Controller (Cisco PNSC) 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 PNSC provides transparent, seamless, and scalable management for securing virtualized data center and cloud environments.

Installation Requirements

Cisco PNSC System Requirements

Requirement	Description
Virtual Appliance	
Four Virtual CPUs	1.8 GHz for each virtual CPU
Memory	4 GB RAM

Requirement	Description

Disk Space	One of the following, depending on InterCloud functionality:
	• With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows:
	  • 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:
	  • Disk 1: 20 GB
	  • Disk 2: 20 GB

Management interface	One management network interface
Processor	x86 Intel or AMD server with 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	
VMware vSphere	5.5, 6.0, and 6.5a with VMware ESXi (English only)
VMware vCenter	5.5, 6.0, and 6.5a with VMware ESXi (English only)
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Hypervisor Requirements

Cisco PNSC is a multi-hypervisor virtual appliance that can be deployed on VMware vSphere.

For more information on VMware compatibility with your hardware platform, see the VMware Compatibility Guide.

Table 1: Hypervisor Requirements

Requirement	Description
VMware	
VMware vSphere	5.5, 6.0, and 6.5a with VMware ESXi (English only)
VMware vCenter	5.5, 6.0, and 6.5a with VMware ESXi (English only)

Note Cisco PNSC running as a virtual machine with version 3.4.1b and later can be hosted on VMware vSphere ESXi 6.0 hosts that are managed by VMware vCenter Server 6.0.

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Any of the following: • Microsoft Windows • Apple Mac OS
Browser	Any of the following browsers: • Internet Explorer 10.0 or higher • Mozilla Firefox 26.0 or higher • Google Chrome 32.0 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 11.9, a message displays asking you to install Flash and provides a link to the Adobe website. **Note** Before using Google Chrome with Cisco PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Prime Network Services Controller.
Flash Player	Adobe Flash Player plugin 11.9 or higher

Firewall Ports Requiring Access

Requirement	Description
22	TCP
80	HTTP/TCP
443	HTTPS
843	Adobe Flash

Information Required for Configuration and Installation

Before installation, collect the following information:

Required Information	Your Information/Notes
For Preinstallation Configuration	
ISO or OVA image location	
ISO or OVA image name	
Network / Port Profile for VM management [1]	
VM name	
VMware datastore Location	
For Prime Network Services Controller Installation	
IP address	
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
NTP server IP address	
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria, on page 45.)	

[1] The management port profile is the same port profile that is used for Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and used for the Prime Network Services Controller management interface.

Shared Secret Password Criteria

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

- Do not include special characters or spaces.
- Make sure your password contains the characteristics of strong passwords and avoids the characteristics of weak passwords as described in the following table:

Strong Passwords	Weak Passwords
• At least eight characters. • Contain characters from at least three of the following classes: lowercase letters, uppercase letters, and numbers.	• Consecutive alphanumeric characters, such as *abcd* or *123*. • Characters repeated three or more times, such as *aaabbb*. • A variation of the word *Cisco*, such as cisco, ocsic, or one that changes the capitalization of letters in the word Cisco. • The username or the username in reverse. • A permutation of characters present in the username or Cisco.

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21
- Es1955Ap

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller, you must disable the Adobe Flash Player plugins that are installed by default with Chrome.

Note Because Chrome automatically enables Adobe Flash Player plugins each time the system reboots, you must perform this procedure each time your client machine reboots.

Procedure

Step 1 In the Chrome URL field, enter **chrome://plugins**.

Step 2 Click **Details** to expand all the files associated with each plugin.

Step 3 Locate the Adobe Flash Player plugins, and disable each one.

Step 4 Download and install Adobe Flash Player plugin version 11.9 or higher.

Step 5 Close and reopen Chrome before logging in to Prime Network Services Controller.

ESXi Server Requirement

You must set the clock to the correct time on all ESXi servers that will run Cisco PNSC, ASA 1000V instances, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco PNSC CA certificate that is created when the Cisco PNSC 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 PNSC.

After you set the clock to the correct time on all ESXi servers that run the Cisco PNSC, you can, as an option, set the clock on the Cisco PNSC 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.

VMware Installation Overview

You can install Prime Network Services Controller on VMware by using either an ISO or an OVA image. The installation time varies from 10 to 20 minutes, depending on the host and the storage area network load.

To install Prime Network Services Controller on VMware, complete the following tasks:

Task	Comments
1. Configuring VMware for Prime Network Services Controller, on page 49	Required for ISO installations only.
2. Installing Prime Network Services Controller	Use the procedure appropriate for your environment: • Installing Prime Network Services Controller Using the ISO Image, on page 50 • Installing Prime Network Services Controller Using the OVA Image
3. Performing VMware Post-Installation Tasks	Required for all installations.

Installing Prime Network Services Controller Using the OVA Image

This procedure describes how to deploy the Prime Network Services Controller OVA image on VMware.

Before you begin

- Set your keyboard to United States English.
- Confirm that the Prime Network Services Controller OVA image is available from the VMware vSphere Client.
- Make sure that all system requirements are met.
- Gather the information identified in Information Required for Configuration and Installation, on page 44.

Procedure

Step 1 Using the VMware vSphere Client, log in to the vCenter server.

Step 2 Choose the host on which to deploy the Prime Network Services Controller VM.

Step 3 Right-click **Host** and select **Deploy OVF Template** from the Pop-up menu.

Step 4 In the wizard, provide the information as described in the following table:

Screen	Action
Source	Choose the Prime Network Services Controller OVA.
OVF Template Details	Review the details.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Enter a name and choose a location for the template.
Deployment Configuration	Choose **Installer**.
Datastore	Select the data store for the VM. The storage can be local or shared remote, such as NFS or SAN.
Disk Format	Choose either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks.
Network Mapping	Choose the management network port group for the VM.
Properties Address any errors that are indicated in red colored text below a selection box. You can enter placeholder information as long as your entry meets the field requirements.	

Screen	Action
A. IP Address	VM management IP address.
B. IP Netmask	VM subnet mask.
C. Gateway	Gateway IP address.
D. DNS	• VM hostname • VM domain • DNS server IP address
E. NTP	NTP server IP address.
F. Operation Mode	• Standalone—Operates as a standalone VM. • Orchestrator—Integrates through an orchestrator with a northbound application. **Note** Prime Network Services Controller does not support Orchestrator mode.
G. Passwords	• Administrator password • Shared secret password
H. Restore	You can safely ignore the Restore fields.
Ready to Complete	Review the deployment settings. **Caution** Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information for accuracy.

Step 5 Click **Finish**.
A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 6 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 7 Power on the Prime Network Services Controller VM.

Installing Prime Network Services Controller Using an ISO Image

To install Prime Network Services Controller in a VMware environment using an ISO image, complete the tasks described in the following topics:

1. Configuring VMware for Prime Network Services Controller, on page 49
2. Installing Prime Network Services Controller Using the ISO Image, on page 50

Configuring VMware for Prime Network Services Controller

Before you install Prime Network Services Controller (PNSC) on VMware using an ISO image, you must configure a VM for Prime Network Services Controller. This procedure describes how to configure the VM so that you can install Prime Network Services Controller on it.

Before you begin

- Confirm that the system requirements have been met.
- Gather the information required for configuration as identified in Information Required for Configuration and Installation, on page 44.

Procedure

Step 1 Download a Prime Network Services Controller ISO image to your client machine. In case of vSphere 6.5 and greater, upload the PNSC ISO image to datastore.

Step 2 Open the VMware vSphere Client (for version 5.5 or 6.0) or Web client (version 6.5a).

Step 3 Right-click the host on which to install the ISO image, and then choose **New Virtual Machine**.

Step 4 Create a new VM by providing the information as described in the following table:

Screen	Action
Configuration	Choose **Custom**.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the data store.
Virtual Machine Version	Choose **Version 8**.
Guest Operating System	Choose **Linux** and **Red Hat Enterprise Linux 5 (64-bit)**.
CPUs	Set the number of virtual sockets to **4**.
Memory	Set the memory to **4 GB**.
Network	**1.** Set the number of NICs to **1**. A single NIC is required for Prime Network Services Controller. **2.** Choose a NIC. **3.** From the Adapter drop-down list, choose **E1000**. Prime Network Services Controller supports only E1000 adapters.
SCSI Controller	Choose **LSI Logic Parallel**.
Select a Disk	Choose **Create a new virtual disk**.

Screen	Action
Create a Disk	1. Disk Size—Enter a minimum of 20 GB. 2. Disk Provisioning—Choose **Thin Provision** or **Thick Provision**. 3. Location—Specify the location of the data store.
Advanced Options	Specify options as needed.

Step 5 For VMware vSphere version 5.5 and 6.0, in the Ready to Complete screen, review the information for accuracy, check the **Edit the Virtual Machine Settings Before Completion** check box, and then click **Continue**.

Step 6 In the Virtual Machine Properties dialog box in the Hardware tab, do the following:

a) Click **Memory** and in the Memory Size field, choose **4 GB**.
b) Click **CPUs** and in the Number of Virtual Sockets field, choose **4**.
c) Click **New Hard Disk** and then click **Add** to create a new hard disk. The disk requires a minimum of 20 GB.
d) Create an additional hard disk with 200 GB memory with thin provisioning. For VMware vSphere 6.5 webclient, choose the **Network** and **ISO disk** from the datastore and select the **Connect** check box.
e) After you supply the information in the Add Hardware Wizard, click **Finish** to create the new disk and to return to the Virtual Machine Properties dialog box.
f) For VMware vSphere 6.5 webclient, choose the Network for the VM. For the Image choose your uploaded ISO disk from datastore.

Step 7 In the **Options** tab, choose **Boot Options**, check the **Force BIOS Setup** check box, and then click **Finish**.

Step 8 After the new VM is created, power it on.

Step 9 For VMware vSphere 5.5 and 6.0, mount the ISO to the VM CD ROM drive as follows:

a) Right-click the VM and choose **Open Console**.
b) From the VM console, click **Connect/Disconnect the CD/DVD Devices of the virtual machine**.
c) Choose **CD/DVD Drive 1**.
d) Choose **Connect to ISO Image on Local Disk**.
e) Choose the ISO image that you downloaded in Step 1.

What to do next

Install Prime Network Services Controller as described in Installing Prime Network Services Controller Using the ISO Image, on page 50.

Installing Prime Network Services Controller Using the ISO Image

This procedure describes how to install the ISO image on a VM that has been configured for Prime Network Services Controller.

Before you begin

Confirm the following items:

- All system requirements are met.
- You have the information identified in Information Required for Configuration and Installation, on page 44.
- You have configured the hypervisor for the Prime Network Services Controller installation procedure.
- A VM has been created for Prime Network Services Controller and has network access.
- You can access the VM console.

Procedure

Step 1 Open the VM console if it is not already open.

If you have just finished configuring the hypervisor, the Prime Network Services Controller installer displays within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Prime Network Services Controller VM, and click **OK**.

Step 3 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 4 In the Modes screen, choose the required modes, and click **Next**:

- Prime Network Services Controller Operation Mode: Choose **Standalone**. This release of Prime Network Services Controller is available in Standalone mode only.
- Prime Network Services Controller Configuration:
  - Prime Network Services Controller Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore Prime Network Services Controller—Choose to restore a previous Prime Network Services Controller installation.

Step 5 In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.

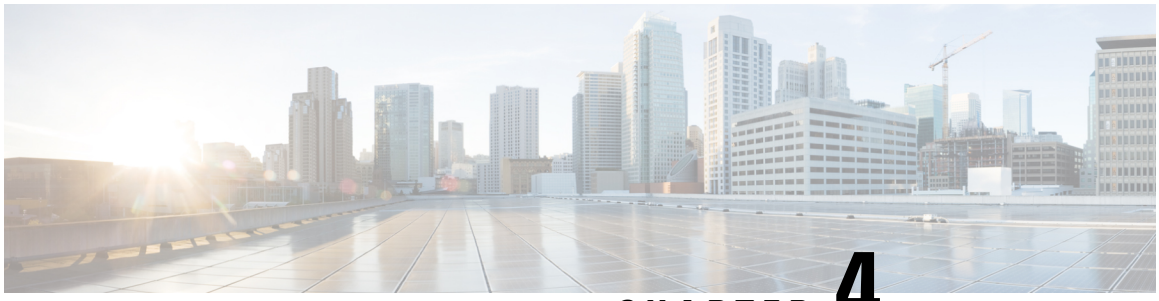
For information on creating a strong password, see Shared Secret Password Criteria, on page 45.

Note If you configure a weak shared secret password, no error message is generated during entry here, but the shared secret password is not usable when the VM is started during the installation process.

Step 6 In the Summary screen, confirm that the information is accurate, and then click **Finish**.
Prime Network Services Controller installs on the VM. This takes a few minutes.

Step 7 When prompted, disconnect from the media source and then click **Reboot**. For vSphere 6.5a Webclient, you need to power off the VM and edit the configuration to uncheck the **Connect** check box for ISO disk and then power on the VM again to complete the reboot.
Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller through the console for the CLI or a browser for the GUI.



CHAPTER 4

Installing the Cisco VSG

This chapter contains the following sections:

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

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: • 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.
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a ESX/ESXi 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.)
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.

Term	Description
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 55
- Installing the Cisco VSG Software from an ISO File, on page 57

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

Procedure

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:

a) Browse to the path to the Cisco VSG OVA file in the **Deploy from a file or URL** field.
b) 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:

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, do the following:

a) 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 PNSC.
g) In the **SharedSecret** field, enter the shared secret password defined during the Cisco PNSC installation.
h) In the **ImageName** field, enter the VSG VNM-PA image name (nsc-vsgpa.2.1.3i.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 PNSC 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 PNSC 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 59 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.

Procedure

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 53.

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:

a) Click **Custom** to create a virtual machine.
b) Click **Next**.

Step 4 In the **Create New Virtual Machine** dialog box, do the following:

a) 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.
b) 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:

a) Click the **Linux** radio button.
b) 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 one1 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:

a) In the **How many NICs do you want to connect?** field, choose **3** from the drop-down list.
b) 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 61 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 55 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.
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.

Procedure

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.

Procedure

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:

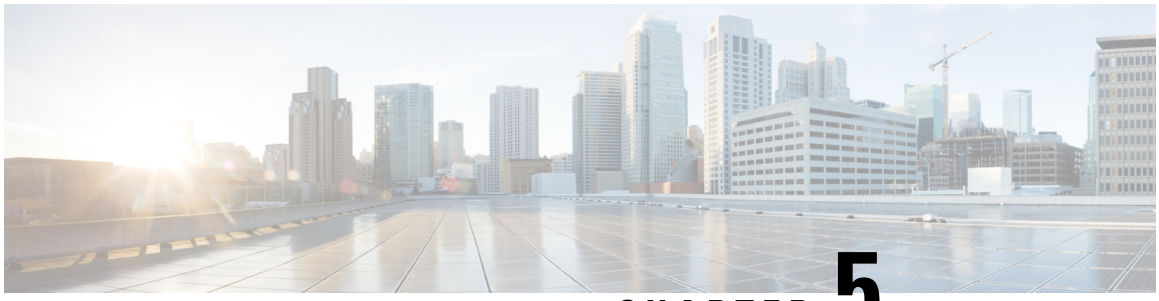
Command	Purpose
show interface brief	Displays brief status and interface information.
show vsg	Displays the Cisco VSG and system-related information.

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: 5.2(1)VSG2(2.2) build [5.2(1)VSG2(2.2)]
PNSC 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 PNSC.



CHAPTER 5

Registering Devices With the Cisco Prime NSC

This chapter contains the following sections:

Registering a Cisco VSG

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

Procedure

Step 1 Copy the nsc-vsgpa.2.1.3i.bin file into the Cisco VSG bootflash:

```
vsg# copy ftp://guest@172.18.217.188/n1kv/nsc-vsgpa.2.1.3i.bin bootflash
```

Step 2 On the command line, enter configuration mode.

```
vsg# configure
```

Step 3 Enter the config-nsc-policy-agent mode.

```
vsg (config)# nsc-policy-agent
```

Step 4 Set the Cisco PNSC registration IP address.

```
vsg (config-nsc-policy-agent)# registration-ip 209.165.200.225
```

Step 5 Specify the shared-secret of Cisco PNSC.

```
vsg (config-nsc-policy-agent)#
shared-secret ********
```

Step 6 Install the policy agent.

```
vsg (config-nsc-policy-agent)#
policy-agent-image bootflash: nsc-vsgpa.2.1.3i.bin
```

Step 7 Exit all modes.

```
vsg (config-nsc-policy-agent)# end
```

Step 8 On the Cisco VSG command line, enter the **show nsc-pa status** command:

```
vsg# show nsc-pa status
If registration was successful, you should see the following message:
"NSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-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 PNSC. Registration enables communication between the Cisco Nexus 1000V VSM and Cisco PNSC.

Procedure

Step 1 Copy the vsmcpa.3.2.3a.bin file into the VSM bootflash:

```
vsm# copy ftp://guest@172.18.217.188/n1kv/vsmcpa.3.2.3a.bin bootflash:
```

Step 2 On the command line, enter configuration mode.

```
vsm# configure
```

Step 3 Enter config-nsc-policy-agent mode.

```
vsm(config)# nsc-policy-agent
```

Step 4 Set the Cisco PNSC registration IP address.

```
vsm(config-nsc-policy-agent)# registration-ip 209.165.200.226
```

Step 5 Specify the shared-secret of Cisco PNSC.

```
vsm(config-nsc-policy-agent)# shared-secret ********
```

Step 6 Install the policy agent.

```
vsm(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.2.3a.bin
```

Step 7 Exit all modes.

```
vsm(config-nsc-policy-agent)# top
```

Step 8 On the command line, enter the following command:

```
vsm# show nsc-pa status
If registration was successful, you should see the following message:
nsc Policy-Agent status is - Installed Successfully. Version 3.2(3a)-vsm
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 PNSC using the CLI.

Registering vCenter

Procedure

Step 1 Log into Cisco PNSC.

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 PNSC 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 PNSC and choose **Resource Management** > **VM Managers**.

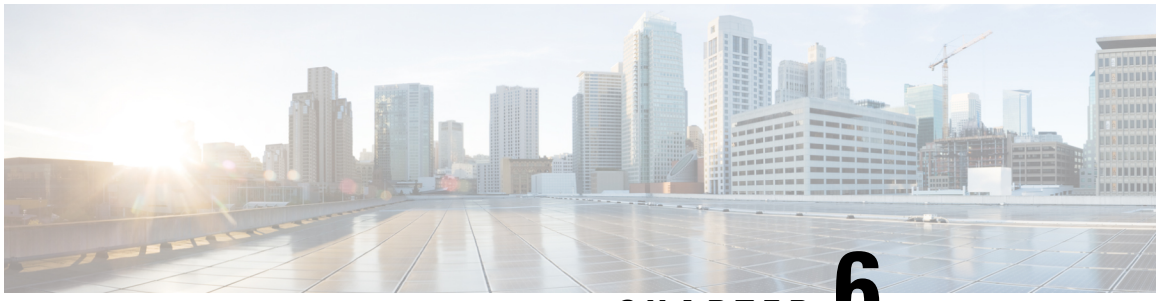
Step 13 In the **Navigation** pane, right-click **VM Managers**.

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.



CHAPTER 6

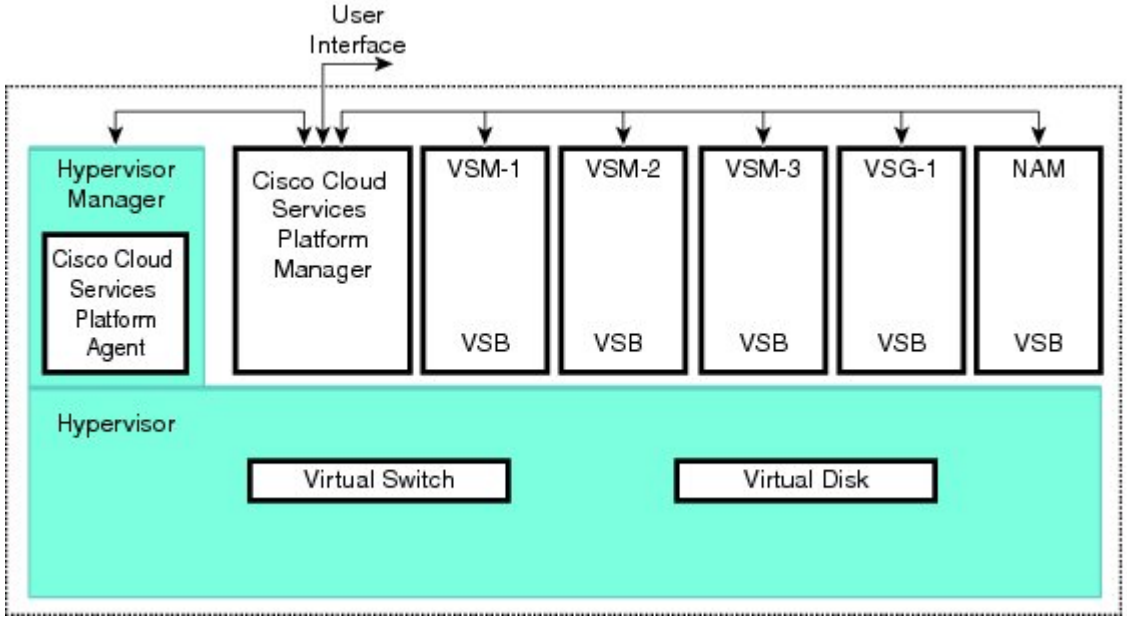
Installing the Cisco VSG on a Cisco Cloud Services Platform Virtual Services Appliance

This chapter contains the following sections:

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

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.5.2.1.VSG2.2.1.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.

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 (config)# **virtual-service-blade** *name*

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.

Step 3 (config-vsb-config)# **show virtual-service-blade-type summary**

(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.

Step 4 (config-vsb-config)# **virtual-service-blade-type** [**name** *name* | **new** *iso file name*]

Specifies the type and name of the software image file to add to this Cisco VSG VSB:

- Use the new keyword to specify the name of the new Cisco VSG ISO software image file in the bootflash repository folder.
- Use the **name** keyword to specify the name of the existing Cisco VSG VSB type. Enter the name of an existing type found in the command output.

Step 5 (config-vsb-config)# **description** *description*

(Optional) Adds a description to the Cisco VSG VSB.

The *description* is an alphanumeric string of up to 80 characters.

Step 6 (config-vsb-config)# **show virtual-service-blade name** *name*

Displays the Cisco VSG VSB that you have just created including the interface names that you configure in the next step.

Step 7 (config-vsb-config)# **interface** *name* **vlan** *vlanid*

Applies the interface and VLAN ID to this Cisco VSG. Use the interface names from the command output.

Note If you try to apply an interface that is not present, the following error is displayed:

ERROR: Interface name not found in the associated virtual-service-blade type.

Caution Do not assign a management VLAN. Unlike data and HA VLANs, the management VLAN is inherited from the Cisco Nexus 1000V.

Caution To prevent loss of connectivity, you must configure the same data and HA VLANs on the hosted Cisco VSGs.

Step 8 Repeat Step 7 to apply additional interfaces

Step 9 (config-vsb-config)# **enable [primary | secondary]**

Initiates the configuration of the VSB and then enables it.

If you enter the **enable** command without the optional **primary** or **secondary** keywords, it enables both.

If you are deploying a redundant pair, you do not need to specify primary or secondary.

If you are enabling a nonredundant VSB, you can specify its HA role as follows:

- Use the **primary** keyword to designate the VSB in a primary role.
- Use the **secondary** keyword to designate the VSB in a secondary role

The Cisco Nexus 1000V prompts you for the following:

- HA ID
- Management IP address

- Management subnet mask length
- Default gateway IPV4 address
- Cisco VSG name
- Administrator password

Step 10 (config-vsb-config)# **show virtual-service-blade name** *name*

(Optional) Displays the new VSB for verification.

While the Cisco Nexus 1000V management software is configuring the Cisco VSG, the output for this command progresses from in progress to powered on.

Step 11 (Optional) (config-vsb-config)# **copy running-config startup-config**

Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

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-vsb-config)# virtual-service-blade-type new nexus-1000v.5.2.1.VSG2.2.1.iso
N1110(config-vsb-config)# interface data vlan 72
N1110(config-vsb-config)# interface ha vlan 72
N1110(config-vsb-config)# enable
Enter vsb image: [nexus-1000v.5.2.1.VSG2.2.1.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-vsb-config)# end
N1110#
```

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

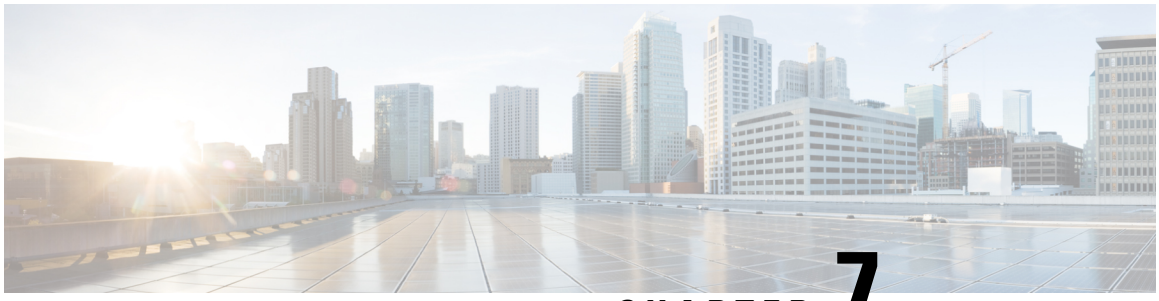
```
N1110# configure
N1110(config)# virtual-service-blade vsg-1
N1110(config-vsb-config)# show virtual-service-blade-type summary
    ---------------------------------------------------------------------------
    Virtual-Service-Blade-Type          Virtual-Service-Blade
    ---------------------------------------------------------------------------
    VSM_SV1_3                           vsm-1 vsm-2
    NAM-MV                              nam-1
    VSG-1                               vsg-1
    ---------------------------------------------------------------------------

N1110(config-vsb-config)# virtual-service-blade-type new nexus-1000v.5.2.1.VSG2.2.1.iso
or
N1110(config-vsb-config)# show virtual-service-blade name vsg-1
```

```
N1110(config-vsb-config)# description vsg-1 for Tenant1
N1110(config-vsb-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-2.2.1
   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-vsb-config)# interface data vlan 1044
or
N1110(config-vsb-config)# interface ha vlan 1045

N1110(config-vsb-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-vsb-config)# show virtual-service-blade name vsg-1
------------------------------------------------------------------------------
    virtual-service-blade vsg-1
    Description:
    Slot id: 1
    SW version: 5.2(1)SV3(3.1)
    Host Name: vsg-1
    Management IP: 10.78.108.40
    VSB Type Name : VSG-2.2.0
    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-vsb-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
```



CHAPTER 7

Upgrading the Cisco VSG and the Cisco Prime NSC

This chapter contains the following sections:

Complete Upgrade Procedure

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

You are Upgrading From	Follow The Sequential Steps in the Following Section:
Cisco VSG Release 5.2(1)VSG2(2.1) to Release 5.2(1)VSG2(2.2) and Cisco Prime NSC Release 3.4.2a to Release 3.4.2b	Upgrade Procedures for Cisco VSG Release 5.2(1)VSG2(2.1) to Release 5.2(1)VSG2(2.2) and Cisco Prime NSC Release 3.4.2a to Release 3.4.2b. This includes upgrade procedures for Cisco Nexus 1000V Release 5.2(1)SV3(2.8) to Release 5.2(1)SV3(3.1).
Cisco VSG Release 5.2(1)VSG2(2.0) to Release 5.2(1)VSG2(2.1) and Cisco Prime NSC Release 3.4.2a to Release 3.4.2b	Upgrade Procedures for Cisco VSG Release 5.2(1)VSG2(2.0) to Release 5.2(1)VSG2(2.1) and Cisco Prime NSC Release 3.4.2a to Release 3.4.2b. This includes upgrade procedures for Cisco Nexus 1000V Release 5.2(1)SV3(2.8) to Release 5.2(1)SV3(3.1).

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

1. Stage 1: Upgrading Cisco PNSC
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 PNSC in the sequence listed. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco PNSC must be upgraded with the corresponding policy agent (PA).

Information About Cisco Prime NSC Upgrades

When you upgrade the Cisco PNSC 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 PNSC at bootup.

Upgrade Guidelines and Limitations

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

- We highly recommend that you upgrade the Cisco VSG and the Cisco PNSC in the order provided. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco PNSC must be upgraded with the corresponding policy agent (PA).
- We recommend that you take a snapshot or backup (clone) of the original Cisco PNSC 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 PNSC before installing the Cisco VSG and VSM. The ISSU upgrade installs a new PA.
  - A new PA with an old Cisco PNSC 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.

VSG Environment Upgrade Matrix and Path

Cisco VSG upgrade involves upgrading the VSG, VNMC or PNSC, and Nexus 1000V environment. To upgrade VSG, you need to make sure that compatible versions of VSG, VNMC or PNSC, and Nexus 1000V are installed. This section lists the compatibility information and upgrade path for Cisco VSG, Cisco VNMC/PNSC, and Cisco Nexus 1000V versions.

Table 3: Cisco VSG, Cisco VNMC/PNSC, and Cisco Nexus 1000V Compatibility Matrix

VSG Version	Supported VNMC/PNSC Release	Supported Nexus 1000V Release
VSG 1.4	VNMC 2.0	4.2(1)SV2(1.1a)
VSG 2.1.1	VNMC 2.1	4.2(1)SV2(2.1)
VSG 2.1.1	PNSC 3.0.2e	4.2(1)SV2(2.1a)
VSG 2.1.1	PNSC 3.2.1d	4.2(1)SV2(2.2)
VSG 2.1.1	PNSC 3.2.1d	4.2(1)SV2(2.3)
VSG 2.1.2	PNSC 3.2.2b	5.2(1)SV3(1.1)
VSG 2.1.2a	PNSC 3.2.2b	5.2(1)SV3(1.2)
VSG 2.1.2c	PNSC 3.4.1b	5.2(1)SV3(1.3)
VSG 2.1.2c	PNSC 3.4.1b	5.2(1)SV3(1.4)
VSG 2.1.3	PNSC 3.4.1b	5.2(1)SV3(1.4)
VSG 2.1.3	PNSC 3.4.1c	5.2(1)SV3(1.5x)
VSG 2.1.4	PNSC 3.4.1d	5.2(1)SV3(1.6)
VSG 2.1.4	PNSC 3.4.1d	5.2(1)SV3(1.15)
VSG 2.1.4	PNSC 3.4.1d	5.2(1)SV3(2.1)
VSG 2.2.0	PNSC 3.4.2a	5.2(1)SV3(2.1)
VSG 2.2.0	PNSC 3.4.2a	5.2(1)SV3(2.8)

VSG 2.2.1	PNSC 3.4.2b	5.2(1)SV3(3.1)
VSG 2.2.1	PNSC 3.4.2c	5.2(1)SV3(3.1)
VSG 2.2.2	PNSC 3.4.2b	5.2(1)SV3(3.1)
VSG 2.2.2	PNSC 3.4.2c	5.2(1)SV3(3.1)

Table 4: Cisco VSG Upgrade Path

Initial VSG Version	Intermediate State	Final VSG Version
VSG 1(4.1)	NA	VSG 2(2.2)
VSG 2(1.1)	NA	VSG 2(2.2)
VSG 2(1.2)	NA	VSG 2(2.2)
VSG 2(1.2a)	NA	VSG 2(2.2)
VSG 2(1.1)	NA	VSG 2(2.2)
VSG 2(1.2a)	NA	VSG 2(2.2)
VSG 2(1.2c)	NA	VSG 2(2.2)
VSG 2(1.3)	NA	VSG 2(2.2)
VSG 2(1.4)	NA	VSG 2(2.2)
VSG 2(2.0)	NA	VSG 2(2.2)
VSG 2(2.1)	NA	VSG 2(2.2)

Table 5: Cisco VNMC/PNSC Upgrade Path

Initial Version	Intermediate State(s)	Final Version
2.0.3	2.1->3.0.2g->3.2.2a->3.4.1d	3.4.2c
2.1	3.0.2->3.2.2a->3.4.1d	3.4.2c
3.0.2	3.2.2a->3.4.1d	3.4.2c
3.2.1d	3.4.1d	3.4.2c
3.2.2b	3.4.1d	3.4.2c
3.4.1b	3.4.1d	3.4.2c
3.4.1c	3.4.1d	3.4.2c
3.4.1d	NA	3.4.2c
3.4.2a	NA	3.4.2c

3.4.2b	NA	3.4.2c

Note Follow PNSC upgrade path information for PNSC **import** feature.

Note For detailed information about Upgrading PNSC, see Upgrading Prime Network Services Controller.

Table 6: Cisco Nexus 1000V Upgrade Path

Initial Version	Intermediate State(s)	Final Version
4.2.1.SV1.5.1a	4.2.1.SV2.2.2	5.2(1)SV3(3.1)
4.2.1.SV1.5.2b	4.2.1.SV2.2.2	5.2(1)SV3(3.1)
4.2.1.SV2.1.1a	NA	5.2(1)SV3(3.1)
4.2.1.SV2.2.1a	NA	5.2(1)SV3(3.1)
4.2.1.SV2.2.2	NA	5.2(1)SV3(3.1)
4.2.1.SV2.2.3	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.1)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.2)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.3)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.4)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.5x)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.6)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(1.15)	NA	5.2(1)SV3(3.1)
5.2(1)SV3(2.8)	NA	5.2(1)SV3(3.1)

Note For detailed information about upgrading VSG/PNSC, see Cisco VSG Install and Upgrade Guides.

Note For information about Cisco Nexus 1000V and VMware ESX/ESXi upgade compatibility, see Cisco Nexus 1000V and VMware ESX/ESXi Upgrade Utility

Upgrade Procedure for Cisco VSG Release 5.2(1)VSG2(2.1) to Release 5.2(1)VSG2(2.2), Cisco PNSC Release 3.4.2b to Release 3.4.2c and Cisco Nexus 1000V Release 5.2(1)SV3(2.8) to Release 5.2(1)SV3(3.1)

Cisco VSG Release 5.2(1)VSG2(2.1) to 5.2(1)VSG2(2.2)

Virtual Appliance	Original State	Stage 1: Cisco PNSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade)	Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade)
Cisco PNSC	Old Cisco Prime NSC 3.4.2b	New Cisco Prime NSC 3.4.2c	New Cisco Prime NSC 3.4.2c	New Cisco Prime NSC 3.4.2c
Cisco VSG	Old 5.2(1)VSG2(2.1)	Old 5.2(1)VSG2(2.1)	New 5.2(1)VSG2(2.2)	New 5.2(1)VSG2(2.2)
VSG PA	Old 2.1(3b)	Old 2.1(3b)	New 2.1(3i)	New 2.1(3i)
VSM	Old 5.2(1)SV3(2.8)	Old 5.2(1)SV3(2.8)	Old 5.2(1)SV3(2.8)	New 5.2(1)SV3(3.1)
VEM	Old 5.2(1)SV3(2.8)	Old 5.2(1)SV3(2.8)	Old 5.2(1)SV3(2.8)	New 5.2(1)SV3(3.1)
VSM PA	3.2(2d)	3.2(2d)	3.2(2d)	3.2(3a)

Virtual Appliance	Original State	Stage 1: Cisco PNSC 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	• Existing data sessions (offloaded). • New data sessions. • Allows Cisco Nexus 1000V switch (non-vn-service) operations including non-vn-service port profiles.	• Short disruption in new data session establishment during the Cisco VSG upgrade. • Other operations are fully supported. • Full Layer 3 VSG and VM VXLAN support.	• All operations are supported if all the upgrades including VEMs are successful. • Restricted operations (below) apply only if all VEMs are not upgraded • Disruption of data traffic during VEM upgrades. • Full service chaining is supported. • Layer 3 VSG and VM VXLAN support. • VSG on VXLAN is supported.

Virtual Appliance	Original State	Stage 1: Cisco PNSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade (ISSU: PA upgrade)	Stage 3: VSM/VEM Upgrade (ISSU: PA upgrade)
		• Support for Cisco PNSC policy cfg change (assuming silent drops). • Support for VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc). • Support for new vn-service VMs. • Support for Vmotion of vn-service firewalled VMs on N1k. • Support for vn-service PP operations or modifications (toggles, removal, changing the PP on VSM). • Support for VSG failover, VSM failover (vns-agent) (All VSM to Cisco PNSC to VSG control operations are supported).	• Support for Cisco PNSC policy cfg change (assuming silent drops). • Support for VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc). • Support for new vn-service VMs. • Support for Vmotion of vn-service firewalled VMs on N1k. • Support for vn-service PP operations or modifications (toggles, removal, changing the PP on VSM). • Support for VSG failover, VSM failover (vns-agent). (All VSM to Cisco PNSC to VSG control operations are supported).	• Support for Cisco PNSC policy cfg change. • Support for VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, etc). • Support for new vn-service VMs. • Support for boot strap of devices (Cisco PNSC, VSM,VSG). • Support for Vmotion of vn-service VMs on N1k. • Support for vn-service PP operations or modifications (toggles, removal, changing the PP on VSM). • Support for N1k switch (non vn-service) operations, including non-vn-service PPs (VSM+VEM ugraded) (All VSM to Cisco PNSC to VSG control operations are supported).

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

Upgrading Cisco Prime NSC 3.4.2b to Cisco Prime NSC 3.4.2c

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 PNSC Release 3.4.2c downloaded.

Procedure

	Command or Action	Purpose
Step 1	nsc# **connect local-mgmt**	Places you in local management mode.
Step 2	(Optional) nsc (local-mgmt)# **show version**	Displays the version information for the Cisco PNSC software.
Step 3	(Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	Copies the Cisco PNSC software file to the VM.
Step 4	nsc (local-mgmt)# **dir bootflash:/**	Verifies that the desired file is copied in the directory.
Step 5	nsc (local-mgmt)# **update bootflash:***/filename*	Begins the update of the Cisco PNSC software.
Step 6	(Optional) nsc (local-mgmt)# **service status**	Allows you to verify that the server is operating as desired.
Step 7	(Optional) nsc (local-mgmt)# **show version**	Allows you to verify that the Cisco PNSC software version is updated. **Note** After you upgrade to Cisco PNSC Release 3.4.2c, you might see the previous version of Cisco PNSC 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.

	Command or Action	Purpose
		Note For detailed information about Upgrading PNSC, see Upgrading Prime Network Services Controller.

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) 2002-2017, 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 PNSC:

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

Name Package Version GUI
---- ------- ------- ----
core Base System 3.4(2b) 3.4(2b) service-reg
Service Registry 3.4(2b) 3.4(2b) policy-mgr
Policy Manager 3.4(2b) 3.4(2b) resource-mgr
Resource Manager 3.4(2b) 3.4(2b) vm-mgr
VM manager 3.4(2b) none vsm-service
VSM Service 3.4(2b) none cloudprovider-mgr
Cloud Provider Mgr 3.4(2b) none
localhost(local-mgmt)#
```

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

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.4.2c.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

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

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

    1.1G Dec 05 00:57 nsc.3.4.2c.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 PNSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.4.2c.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 PNSC:

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

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.4.2c         3.4.2c
service-reg         Service Registry    3.4.2c         3.4.2c
policy-mgr          Policy Manager      3.4.2c         3.4.2c
resource-mgr        Resource Manager    3.4.2c         3.4.2c
vm-mgr              VM manager          3.4.2c         none
cloudprovider-mgr   Cloud Provider Mgr  3.4.2c         none
```

Upgrading Cisco VSG from Release 5.2(1)VSG2(2.1) to 5.2(1)VSG2(2.2)

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:

```
vsg# copy
scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.2.2.bin
bootflash:nexus-1000v-kickstart.5.2.1.VSG2.2.2.bin

vsg# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.5.2.1.VSG2.2.2.bin
bootflash:nexus-1000v.5.2.1.VSG2.2.2.bin

vsg# copy scp://user@scpserver.cisco.com/downloads/nsc-vsgpa.2.1.3i.bin
bootflash:nsc-vsgpa.2.1.3i.bin
```

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**install all kickstart bootflash:***nexus-1000v-kickstart.5.2.1.VSG2.2.2.bin* **system bootflash:***nexus-1000v.5.2.1.VSG2.2.2.bin* **nscpa bootflash:***nsc-vsgpa.2.1.3i.bin*	Installs the kickstart image, system image, and policy agent (PA) image. **Note** If you do not have a policy agent installed on the Cisco VSG before the **install all** 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.

	Command or Action	Purpose
Step 3	**show nsc-pa status**	Verifies that the new PA is installed and the upgrade was successful. **Note** You must have an existing PA installed before upgrading the PA using the **install all** command.
Step 4	**copy running-config startup-config**	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 5.2(1)VSG2(2.1) to Release 5.2(1)VSG2(2.2):

```
vsg # configure terminal
vsg (config)# install all kickstart bootflash:nexus-1000v-kickstart.5.2.1.VSG2.2.2.bin
system bootflash:nexus-1000v.5.2.1.VSG2.2.2.bin nscpa bootflash:nsc-vsgpa.2.1.3i.bin
vsg (config)# show nsc-pa status
NNSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-vsg
vsg(config)# copy running-config startup-config
```

Upgrading Cisco VSG from Release 5.2(1)VSG2(2.1) to 5.2(1)VSG2(2.2) Using an ISO File

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 ISO image into the bootflash file system using the following commands:

  ```
  vsg# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.5.2.1.VSG2.2.2.iso
  bootflash:nexus-1000v.5.2.1.VSG2.2.2.iso
  ```

- You have confirmed that the system is in high availability (HA) mode.
- Cisco VSG upgrade using ISO file supported on Cisco Nexus 1000V Release 5.2(1)SV3(1.1) and later.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**install all iso bootflash:***nexus-1000v.5.2.1.VSG2.2.2.iso*	Installs the system image.

	Command or Action	Purpose
Step 3	**show nsc-pa status**	Verifies that the new PA is installed and the upgrade was successful.
Step 4	**copy running-config startup-config**	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 5.2(1)VSG2(2.1) to Release 5.2(1)VSG2(2.2) using an ISO file:

```
vsg # configure terminal
vsg (config)# install all iso bootflash:nexus-1000v.5.2.1.VSG2.2.2.iso
vsg (config)# show nsc-pa status
NNSC Policy-Agent status is - Installed Successfully. Version 2.1(3i)-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 7: Upgrade Paths from Cisco Nexus 1000V Releases

If you are running this configuration	Follow these steps
Release 4.0(4)SV1(1), 4.0(4)SV1(2), 4.2(1)SV1(4), 4.2(1)SV1(5.1), and 4.2(1)SV1(5.2)	Direct upgrades from these releases are not supported.
Releases 4.0(4)SV1(3x) Series	1. Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4b) 2. Upgrade from Releases 4.2(1)SV2(1.1) and later releases to the current release

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4x) Series with a vSphere release 4.0 Update 1 or later	**1.** Upgrading from VMware Release 4.0 to VMwrae Release 5.0 or later. **2.** Upgrading VSMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **3.** Upgarding VEMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **4.** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **5.** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.
Release 4.2(1)SV1(4x) Series with a vSphere release 4.1 GA, patches, or updates	**1.** Upgrading from VMware Release 4.1 to VMwrae Release 5.0 or later. **2.** Upgrading VSMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **3.** Upgarding VEMs from releases 4.2(1)SV1(4x) to 4.2(1)SV2(1.1) or later. **4.** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **5.** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.

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

Table 8: 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.	**1.** Upgrading VSMs from releases 4.2(1)SV1(5.1x) to 4.2(1)SV2(1.1) or later. **2.** Upgarding VEMs from releases 4.2(1)SV1(5.1x) to 4.2(1)SV2(1.1) or later. **3.** Upgrading VSMs from releases 4.2(1)SV2(1.1) or later to current release. **4.** Upgrading VEMs from releases 4.2(1)SV2(1.1) or later to current release.

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.

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:

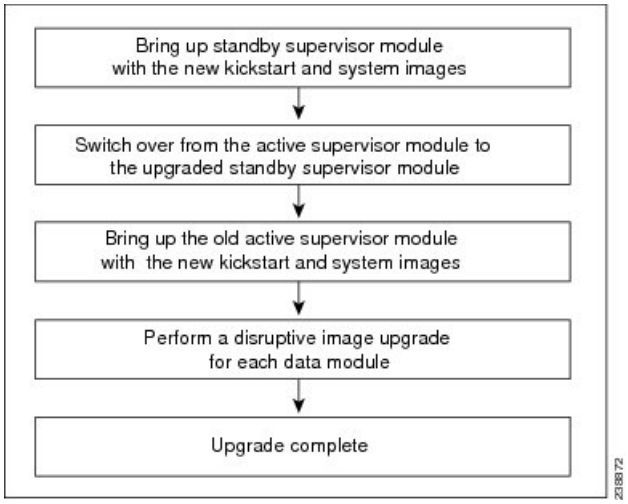
- Kickstart image
- System image
- VEM images
- Policy Agent image

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.

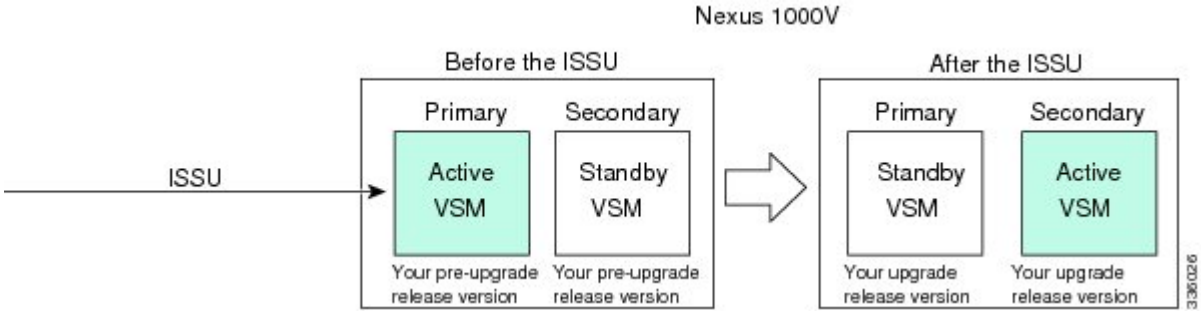
Figure 8: ISSU Process



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.
- 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), 5.2(1)SV3(1.x), 5.2(1)SV3(x) to 5.2(1)SV3(3.x)

Procedure

Step 1 Log in to the active VSM.

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

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

Step 3 Access the Software Download Center by using this URL:

http://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 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 kickstart and system images.

```
switch# copy
scp://user@scpserver.cisco.com/downloads/n1000v-dk9-kickstart.5.2.1.SV3.3.1.bin
bootflash:n1000v-dk9-kickstart.5.2.1.SV3.3.1.bin
switch# copy
scp://user@scpserver.cisco.com/downloads/n1000v-dk9.5.3.1.SV3.v.bin
bootflash:n1000v-dk9.5.2.1.SV3.3.1.bin vnmpa bootflash:vsmcpa.3.2.3a.bin
```

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

- kickstart and system

```
switch# show install all impact kickstart
bootflash:nexus-1000v-kickstart.5.2.1.SV3.3.1.bin system
bootflash:nexus-1000v.5.2.1.SV3.3.1.bin

Verifying image bootflash:/nexus-1000v-kickstart.5.2.1.SV3.3.1.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-5.2.1.SV3.3.1.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

```
Extracting "system" version from image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart.5.2.1.SV3.3.1.bin.
[####################] 100% -- SUCCESS

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



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


Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes
     1   kickstart           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes
     2      system           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes
     2   kickstart           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes


Module         Running-Version                                          ESX Version
   VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
----------------------  ----------------------
     3          5.2(1)SV3(3.1)         VMware ESXi 5.0.0 Releasebuild-469512 (3.1)
          COMPATIBLE              COMPATIBLE
     4          5.2(1)SV3(3.1)         VMware ESXi 5.0.0 Releasebuild-469512 (3.1)
          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 nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(3a)-vsm
switch#
```

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

```
switch# show nsc-pa status
NSC 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 kickstart and system images.

- Upgrade using the kickstart and system images.

```
switch# install all impact kickstart
bootflash:///n1000v-dk9-kickstart.5.2.1.SV3.3.1.bin system
bootflash:n1000v-dk9.5.2.1.SV3.3.1.bin vnmpa bootflash:vsmcpa.3.2.3a.bin
Verifying image bootflash:/nexus-1000v-kickstart.5.2.1.SV3.3.1.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

Extracting "system" version from image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart.5.2.1.SV3.3.1.bin.
[####################] 100% -- SUCCESS

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



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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes
     1   kickstart           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes
     2      system           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes
     2   kickstart           5.2(1)SV3(2.8)           5.2(1)SV3(3.1)           yes


Module         Running-Version                                          ESX Version
   VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
----------------------  ----------------------
     3           5.2(1)SV3(3.1)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
         COMPATIBLE              COMPATIBLE
     4           5.2(1)SV3(3.1)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
         COMPATIBLE              COMPATIBLE
```

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

Note Ensure that you provide the vnmpa parameter for the **install all** command while upgrading VSM.

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.5.2.1.SV3.3.1.bin to standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin to standby.
[####################] 100% -- SUCCESS

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

Performing configuration copy.
[####################] 100%2017 Feb 03 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) 2002-2016, 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 5.2(1)SV3(3.1) [build 5.2(1)SV3(3.1)]
  system:    version 5.2(1)SV3(3.1) [build 5.2(1)SV3(3.1)]
  kickstart image file is: bootflash:/nexus-1000v-kickstart.5.2(1)SV3(3.1).bin
  kickstart compile time:  03/30/2017 3:00:00 [03/30/2017 12:49:49]
  system image file is:    bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin
  system compile time:     03/30/2017 3:00:00 [03/30/2017 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.5.2.1.SV3.3.1.bin for boot variable
"kickstart".

 -- SUCCESS

Verifying image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin for boot variable "system".

 -- SUCCESS

Verifying image type.

 -- SUCCESS

Extracting "system" version from image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin.

 -- SUCCESS

Extracting "kickstart" version from image bootflash:/nexus-1000v-kickstart.5.2.1.SV3.3.1.bin.


 -- SUCCESS

Notifying services about system upgrade.

 -- SUCCESS


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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           5.2(1)SV3(2.8)          5.2(1)SV3(3.1)           yes
     1   kickstart           5.2(1)SV3(2.8)          5.2(1)SV3(3.1)           yes
```

```
     2      system           5.2(1)SV3(2.8)         5.2(1)SV3(3.1)           yes
     2   kickstart           5.2(1)SV3(2.8)         5.2(1)SV3(3.1)           yes


Images will be upgraded according to following table:
Module         Running-Version                                        ESX Version
VSM Compatibility       ESX Compatibility
------  ----------------------  ------------------------------------------------------
----------------------  ----------------------
     3           5.2(1)SV3(3.1)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
       COMPATIBLE              COMPATIBLE
     4           5.2(1)SV3(3.1)         VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
       COMPATIBLE              COMPATIBLE


Install is in progress, please wait.

Syncing image bootflash:/nexus-1000v-kickstart.5.2.1.SV3.3.1.bin to standby.
 -- SUCCESS

Syncing image bootflash:/nexus-1000v.5.2.1.SV3.3.1.bin to standby.
 -- SUCCESS

Setting boot variables.
 -- SUCCESS

Performing configuration copy.
 -- SUCCESS

Module 2: Waiting for module online.
 -- SUCCESS

Notifying services about the switchover.
 -- SUCCESS


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

switch# attach module 2
Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, 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 Procedure

- 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.
  - 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 101.
  - 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 101.
- 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 104
- Installing or upgrading stateless ESXi. See *Cisco Nexus 1000V Installation and Upgrade Guide*.

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. For detailed information about stateless ESXi host upgrade, see *Cisco Nexus 1000V Installation and Upgrade Guide*.

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.

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 101.

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 104.

- 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.
- 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 101
- Upgrading the VEMs Manually from Release 4.2(1)SV1(5x) and Later Releases to the Current Release, on page 104

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

Procedure

Step 1 switch# **show vmware vem upgrade status**

Display the current configuration.

Note The minimum release of Cisco Nexus 1000V for VMware ESXi 5.0.0 hosts is Release 4.2(1)SV1(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 108. 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.

Example

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 Jul 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 Jul 27 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jul 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 Jul 27 10:03:24 2014
Upgrade Status Time(vCenter) : Tue Jul 27 02:06:53 2014
Upgrade Start Time: : Tue Jul 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 Jul 27 10:03:24 2014
Upgrade Status Time(vCenter): : Tue Jul 27 02:06:53 2014
Upgrade Start Time: : Tue Jul 27 10:09:08 2013
Upgrade End Time(vCenter): : Tue Jul 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    5.2(1)SV3(1.2)      0.0
2    5.2(1)SV3(1.2)      0.0
3    5.2(1)SV3(1.2)      VMware ESXi 5.0.0 Releasebuild-469512 (3.0)
4    5.2(1)SV3(1.2)      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 108.

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.

Procedure

Step 1 switch# **vmware vem upgrade notify**

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

Step 2 switch# **show vmware vem upgrade status**

Verify that the upgrade notification was sent.

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

Verify that the server administrator has accepted the upgrade in vCenter Server. For details about the server administrator accepting the VEM upgrade, see Accepting the VEM Upgrade, on page 108. 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 108.

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.

Example

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 Jul 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jul 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 Jul 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jul 28 02:06:53 2014
Upgrade Start Time: Tue Jul 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 Jul 28 10:03:24 2014
Upgrade Status Time(vCenter): Tue Jul 28 02:06:53 2014
Upgrade Start Time: Tue Jul 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    5.2(1)SV3(1.2)  0.0
2    5.2(1)SV3(1.2)  0.0
3    5.2(1)SV3(1.2)      VMware ESXi 5.0.0 Releasebuild-843203 (3.0)
6    5.2(1)SV3(1.2)      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.

Procedure

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

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

Figure 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.

Procedure

Step 1 [root@serialport -]# **cd tmp**

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

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

- **vihostupdate**

  Installs the ESXi and VEM software simultaneously if you are using the vCLI.

Step 3 For ESXi 5.5 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.

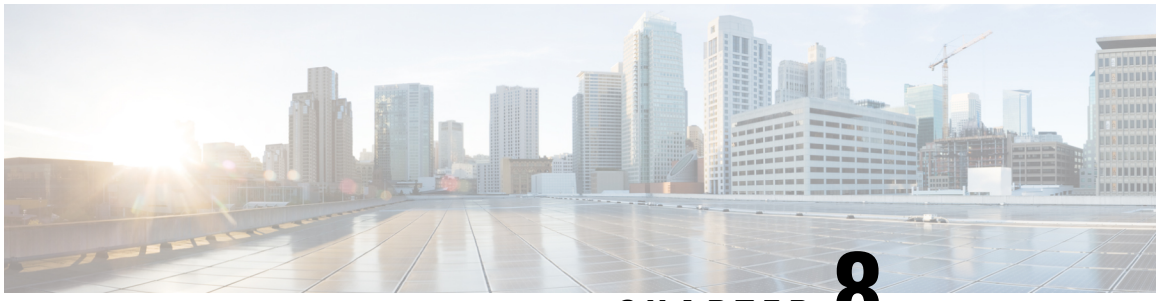
Note The example may contain Cisco Nexus 1000V versions and filenames that are not relevant to your release. Refer to the *Cisco Nexus 1000V and VMware Compatibility Information* for your specific versions and filenames.

```
[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: cross_cisco-vem-v170-5.2.1.3.1.2.0-3.0.1
   VIBs Removed:
   VIBs Skipped:
~ #

~ # esxcli software vib install -v /tmp/cross_cisco-vem-v170-5.2.1.3.1.2.0-3.0.1.vib
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v170-esx_5.2.1.3.1.2.0-3.0.1
   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 5.2(1)SV3(1.2)


[root@host212 ~]# . ~ # vem status -v
Package vssnet-esxmn-release
Version 5.2.1.3.1.2.0-3.0.1
Build 1
Date Mon Jul 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
Running esx version -1024429 x86_64
VEM Version: 5.2.1.3.1.2.0-3.0.1
VSM Version: 5.2(1)SV3(1.2)
System Version: VMware ESXi 5.0.0 Releasebuild-1024429
ESX Version Update Level: 2

~ #
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    5.2(1)SV3(1.2)  0.0
2    5.2(1)SV3(1.2)  0.0
3    5.2(1)SV3(1.2)      VMware ESXi 5.0.0 Releasebuild-843203 (3.0)
6    5.2(1)SV3(1.2)      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.



CHAPTER 8

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

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 PNSC instance
- Ensure that you have the Cisco Prime NSC ova image

Procedure

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 PNSC 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:

a) In the **Name** field, enter a template name.
b) 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 PNSC 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 PNSC and click **Next**.

Step 16 In the **Properties** window, in the **IP Address** area, do the following:

a) Enter an IP address in the **IPv4 IP Address** field.
b) Enter an IP netmask in the **IPv4 IP Netmask** field.
c) 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:

a) Enter the host name in the **Host Name** field.
b) 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 PNSC and click **Finish** to deploy Cisco PNSC on the selected ESXi host.

Note Select **Power on after deployment** check box to start Cisco PNSC 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 PNSC instance is created.

OVA Installation Using an ISO Image

Procedure

Step 1 Download a Cisco PNSC ISO to your client machine.

Step 2 Open a vCenter client.

Step 3 Create a virtual machine on the appropriate host as follows:

a) Ensure your virtual machine size is 220 GB split into two disks (Disk1 having 20GB and Disk2 having 200GB).
b) Ensure your virtual machine has 4 GB of RAM.
c) 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:

a) Right-click the virtual machine and choose **Open the VM Console**.
b) From the virtual machine console, click Connect/Disconnect CD/DVD Devices.
c) Choose **CD/DVD Drive1**.
d) Choose **Connect to ISO Image on Local Disk**.
e) 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 PNSC instance.

INDEX

L

M

N

O

P

R

S

T

U

V

W