Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Rel. 1.3 Installation and Upgrade Guide

February 16, 2012

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

Text Part Number: OL-25784-03

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

Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Rel. 1.3 Installation and Upgrade Guide

CONTENTS

Send document comments to vsg-docfeedback@cisco.com

CHAPTER 7

APPENDIX A

INDEX

Preface

The *Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Rel. 1.3 Installation and Upgrade Guide* provides procedures for installing Cisco Virtual Security Gateway (VSG) and Cisco Virtual Network Management Center (VNMC).

This preface includes the following sections:

Audience

This guide is for the following professionals who have an understanding of virtualization and experience using VMware tools such as vCenter to create virtual machines:

- Security Administrators—Define and administer security policies and rules.
- Network Administrators—Manage and associate the security policies to particular port profiles.
- ESX Server Administrators—Select the appropriate port-group (Cisco Nexus 1000V equivalent port-profile) for the particular virtual machines (VM).

Organization

This guide includes the following sections:

Part	Title	Description
Part 1	Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management Center	Provides procedures for installing the Cisco VNMC and the Cisco VSG. This part of the document should be followed for a first-time installation or for someone new to Cisco VNMC or Cisco VSG.
Part 2	Installation Guide for the Cisco Virtual Security Gateway	Provides more details on the procedures to install the Cisco VSG.

Part	Title	Description
Part 3	Installation Guide for the Cisco Virtual Network Management Center	Provides more details on the procedures to install the Cisco VNMC.
Part 4	Installing the Cisco VSG on a Cisco Nexus 1010 Appliance	Provides details on how to install the Cisco VSG on a Cisco Nexus 1010 appliance.
Part 5	Upgrading the Cisco VSG and the Cisco VNMC	Provides details on how to upgrade the Cisco VSG and Cisco VNMC.

This document (particularly the Quick Start Guide in Part 1) is intended to give you the most effective way to install and set up a basic working configuration of the Cisco VNMC and the Cisco VSG. If Part 1 is followed in the order as the steps are presented, you should have a base upon which you can build a more comprehensive virtual data center and tenant network.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` 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.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

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

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

This section contains information about the documentation available for Cisco Virtual Security Gateway and related products.

Cisco Virtual Security Gateway Documentation

The following Cisco Virtual Security Gateway for the Nexus 1000V Series Switch documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(3.1)*

Cisco Virtual Network Management Center Documentation

The following Cisco Virtual Network Management Center documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

Cisco Nexus 1000V Series Switch Documentation

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

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Overview

This chapter provides information about the Cisco Virtual Security Gateway (Cisco VSG) and the Cisco Virtual Network Management Center (Cisco VNMC). It also provides information about high availability (HA).

This chapter includes the following sections:

- Information About Installing the Cisco Virtual Network Management Center and the Cisco Virtual Security Gateway, page 1-1
- Information About Cisco Virtual Security Gateway, page 1-1
- Information About the Cisco Virtual Network Management Center, page 1-6
- Information About High Availability, page 1-9

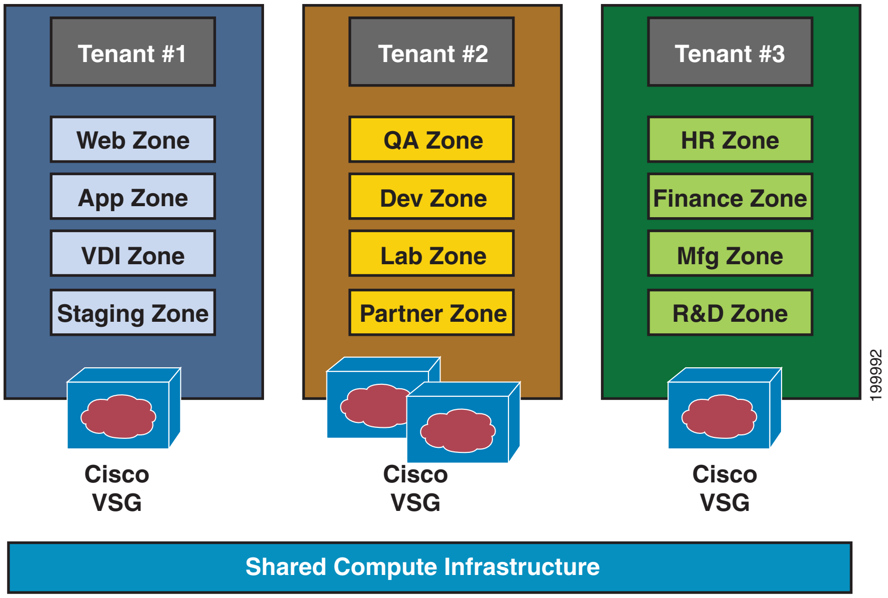
Information About Installing the Cisco Virtual Network Management Center and the Cisco Virtual Security Gateway

You must install the Cisco VNMC and the Cisco VSG in a particular sequence on the Cisco Nexus 1000V switch in order to have a functioning virtual system. Part 1, the *Quick Start Guide for Cisco Virtual Security Gateway and Cisco Virtual Network Management Center,* provides that critical sequence information that you need for a successful installation on the Cisco Nexus 1000V switch. Part 4, *Installing* Cisco *VSG on a Cisco Nexus 1010*, provides the information required for installing the Cisco VSG on the Cisco Nexus 1010 Virtual Services Appliance.

Information About Cisco Virtual Security Gateway

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. Figure 1-1 shows the trusted zone-based access control that is used in per-tenant enforcement with the Cisco VSG.

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



VNMC and VSG Architecture

The Cisco VSG operates with the Cisco Nexus 1000V Series switch in the VMware vSphere Hypervisor or the Cisco Nexus 1010 Virtual Services Appliance, and the Cisco VSG leverages the virtual network service data path (vPath) (see Figure 1-2). 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.

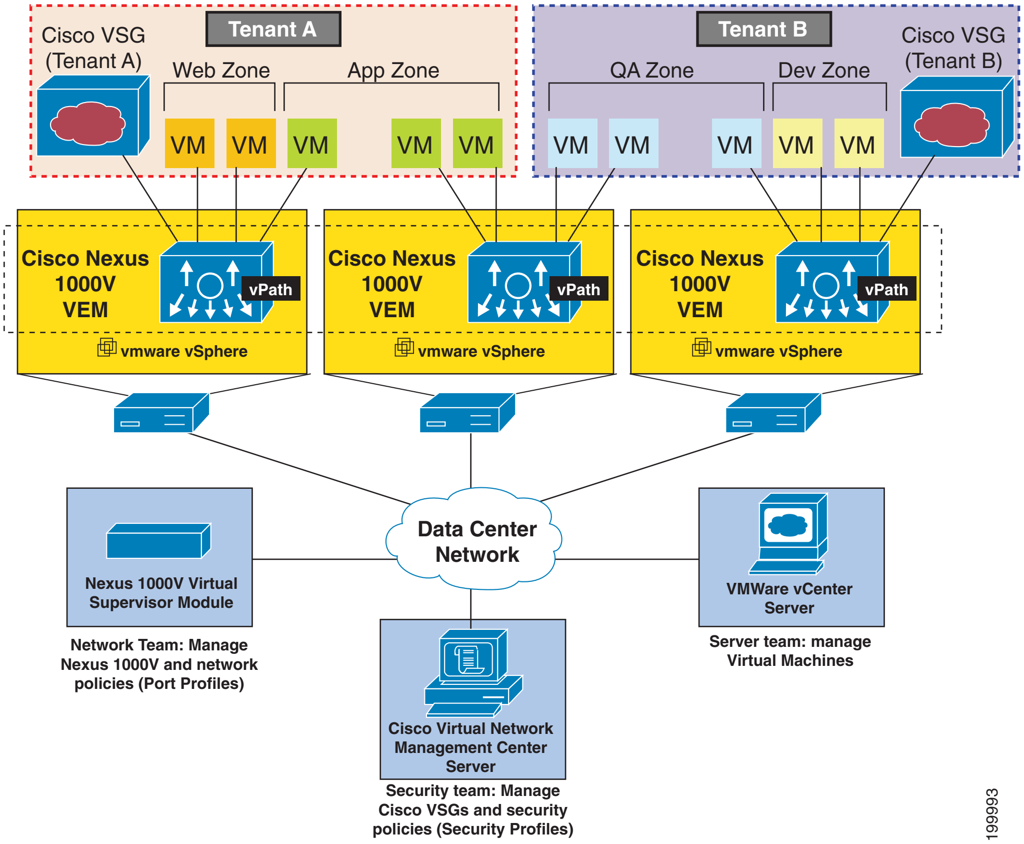
vPath supports the following features:

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

The Cisco VSG and the VEM provide the following benefits (see Figure 1-3):

- 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 (VEM) modules, the Cisco VSG enhances security performance through distributed vPath-based enforcement.
- You can use the Cisco VSG without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling, which is based on security profiles, simplifies physical server upgrades without compromising security or incurring application outages.
- For each tenant, you can deploy the Cisco VSG in an active-standby mode to ensure that vPath redirects packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.
- You can place the Cisco VSG on a dedicated server so that you can allocate the maximum compute capacity to application workloads. This feature enables capacity planning to occur independently and allows for operational segregation across security, network, and server groups.

Figure 1-2 Cisco Virtual Security Gateway Deployment Topology



Trusted Multitenant Access

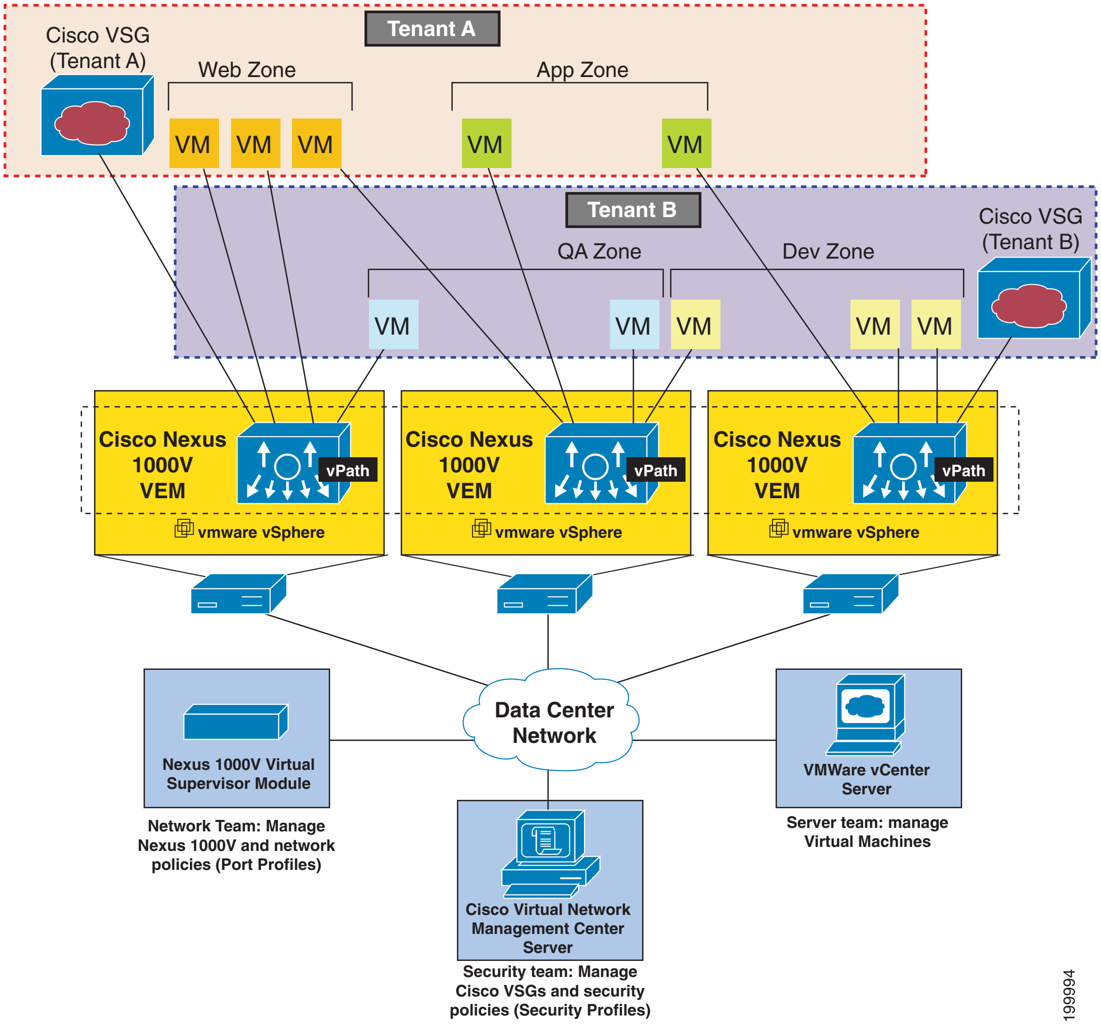
You can transparently insert a Cisco VSG into the VMware vSphere environment where the Cisco Nexus 1000V is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic 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 (see Figure 1-2). 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. Figure 1-3 shows how the structured environment shown in Figure 1-2 can change over time due to this dynamic VMs.

Figure 1-3 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 VNMC, 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 Virtual Center [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 VSGs and VLANs

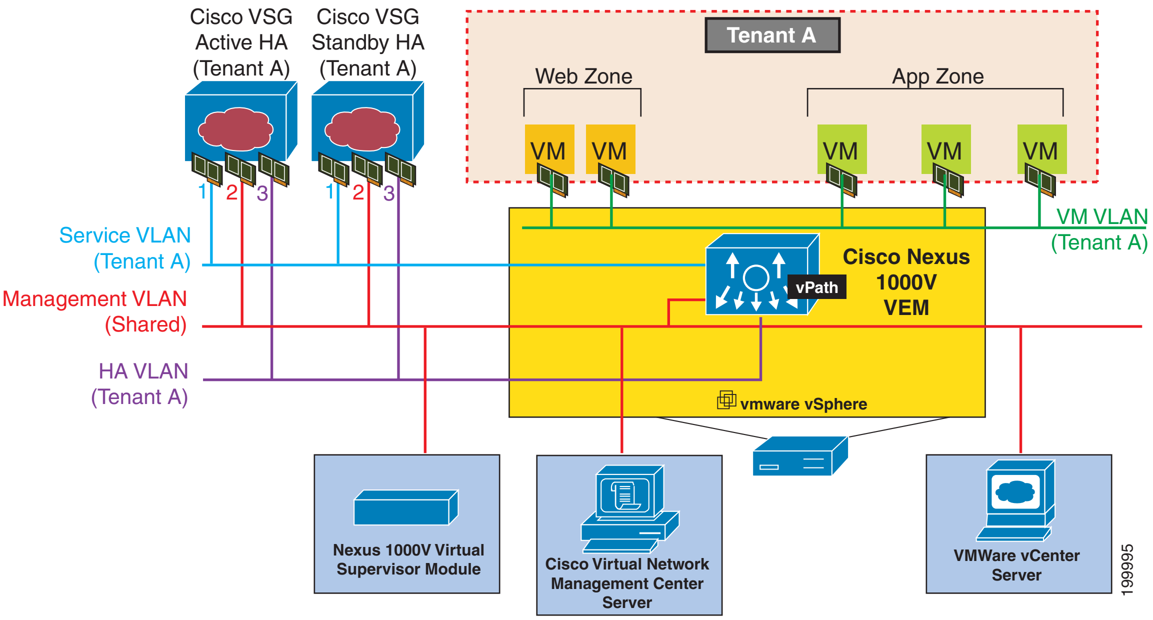
You can set up a Cisco VSG in an overlay fashion so that VMs can reach a Cisco VSG irrespective of its location. The vPath component in the Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

Figure 1-4 shows Cisco VSGs in a typical arrangement. In the 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. The VLAN functions are as follows:

- The service VLAN provides communications between the Cisco Nexus 1000V VEM and Cisco VSGs. All the Cisco VSG data interfaces are part of the service VLAN and the VEM uses this VLAN for its interaction with Cisco VSGs.
- The management VLAN connects the management platforms such as the VMware vCenter, the Cisco Virtual Network Management Center, 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 heart-beat mechanism and identifies the active and standby relationship between the 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 VLAN 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.

Figure 1-4 Cisco Virtual Security Gateway VLAN Usages



Information About the Cisco Virtual Network Management Center

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

This section includes the following topics:

- Cisco VNMC Components, page 1-6
- System Requirements, page 1-8

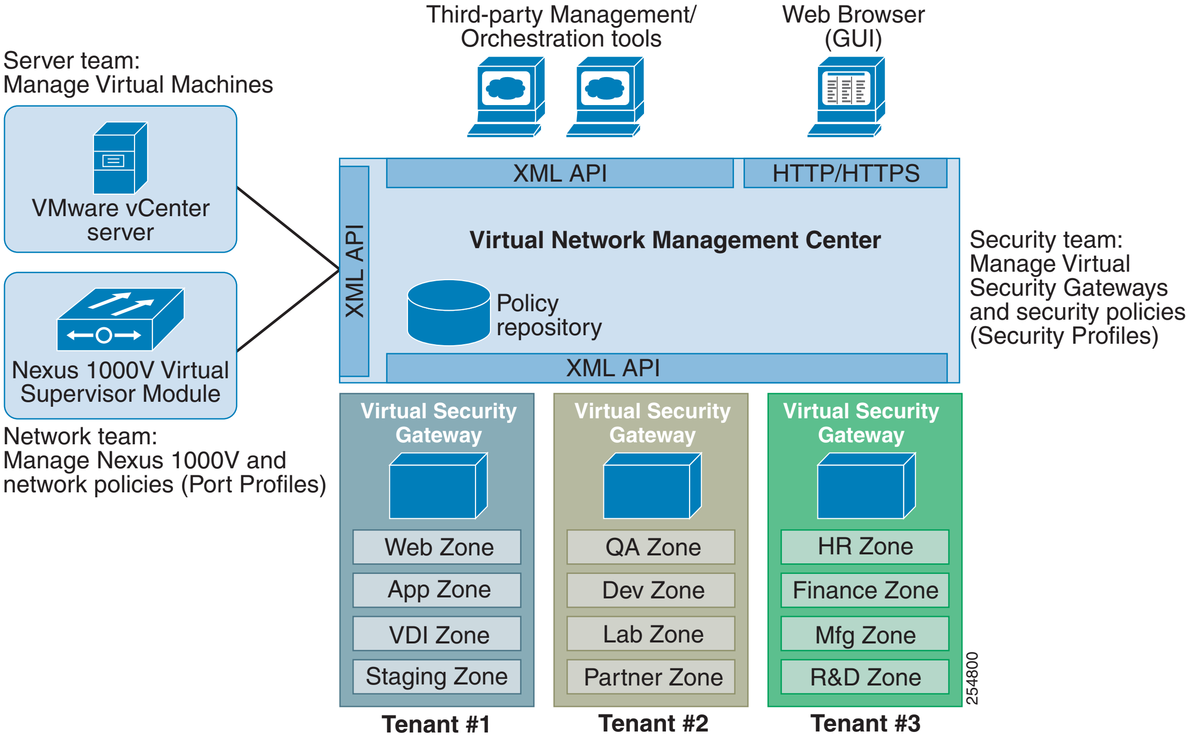
Cisco VNMC Components

This section includes the following topics:

- Cisco VNMC Key Benefits, page 1-7
- Cisco VNMC Architecture, page 1-7
- Cisco VNMC Security, page 1-8
- Cisco VNMC API, page 1-8
- Cisco VNMC and VSM, page 1-8

Figure 1-5 shows the Cisco VNMC components.

Figure 1-5 Cisco VNMC Components


Third-party Management/ Orchestration tools
Web Browser (GUI)
Server team: Manage Virtual Machines
VMware vCenter server
Nexus 1000V Virtual Supervisor Module
Network team: Manage Nexus 1000V and network policies (Port Profiles)
XML API
HTTP/HTTPS
XML API
Virtual Network Management Center
Policy repository
XML API
Security team: Manage Virtual Security Gateways and security policies (Security Profiles)
Virtual Security Gateway
Web Zone
App Zone
VDI Zone
Staging Zone
Tenant #1
Virtual Security Gateway
QA Zone
Dev Zone
Lab Zone
Partner Zone
Tenant #2
Virtual Security Gateway
HR Zone
Finance Zone
Mfg Zone
R&D Zone
Tenant #3
254800

Cisco VNMC Key Benefits

The Cisco VNMC 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 VNMC Architecture

The Cisco VNMC 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 VNMC Security

The Cisco VNMC 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 VNMC API

The Cisco VNMC 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 VNMC and VSM

The Cisco VNMC operates with the Cisco Nexus 1000V 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 port profiles through the Cisco VNMC interface.
- Network administrators who author and manage port profiles as well as manage Cisco Nexus 1000V switches. Port profiles are referenced in vCenter through the Cisco Nexus 1000V VSM interface.
- Server administrators who select the appropriate port profiles in the vCenter when instantiating a virtual machine.

System Requirements

System requirements for a Cisco VNMC are as follows:

- x86 Intel or AMD server with a 64-bit processor listed in the VMware compatibility matrix
- Intel VT that is enabled in the BIOS
- VMware ESX 4.0 (non-VM), 4.1 or 5.0
- VMware vSphere Hypervisor
- VMware vCenter 5.0 (4.1 VMware supports only 4.1 host)
- 3 GB is required for VNMC ISO installation.
- Datastore with at least 25-GB disk space available on shared Network File System/Storage Area Network (NFS/SAN) storage when the Cisco VNMC is deployed in an HA cluster
- Flash 10.0 or 10.1
- Internet Explorer 8.0, 9.0 or Mozilla Firefox 8.x on Windows

  Access to Cisco VNMC application using a web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports):

  - 443 (HTTP)
  - 80 (HTTP/TCP)
  - 843 (TCP)

Note If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 10.1, a message displays asking you to install Flash and provides a link to the Adobe website.

Note You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php

Information About High Availability

VMware high availability (HA) provides a base level of protection for a Cisco VNMC VM by restarting it on another host in the HA cluster. With VMware HA, data is protected through a shared storage. The Cisco VNMC 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 VNMC 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.

PART 1

Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management Center

CHAPTER 2

Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management Center

This chapter provides a Quick Start reference for installing and completing the basic configuration for the Cisco Virtual Network Management Center (VNMC) and the Cisco Virtual Security Gateway (VSG) software.

This chapter includes the following sections:

Information About Installing Cisco VNMC and Cisco VSG

This chapter presents an example of an effective way to install and set up a basic working configuration of the Cisco VNMC 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 is up and running and endpoint VMs are already installed.

Cisco VSG and Cisco VNMC Installation Planning Checklists

Planning the arrangement and architecture of your network and equipment is essential for successful operation of the Cisco VNMC and Cisco VSG. This section provides some planning and information checklists to assist you in installing the Cisco VNMC and Cisco VSG.

This section includes the following checklists:

- Table 2-1Basic Hardware and Software Requirements, page 2-2
- Table 2-2Preparation of the Cisco Nexus 1000V Series Switch for Further Installation Processes, page 2-3
- Table 2-3Your Cisco VNMC and Cisco VSG Information for Use Later During Installation, page 2-3
- Table 2-4Tasks, Descriptions, and Prerequisites Checklist, page 2-4

Table 2-1 Basic Hardware and Software Requirements

Item	Do You Have?	Your Information
1	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix	
2	Intel VT enabled in the BIOS	
3	VMware ESX 4.1 or 5.0	
4	ESX or ESXi platform that runs VMware software release 4.1. or 5.0 with a minimum of 4-GB physical RAM for the Cisco VSG and similar for the Cisco VNMC or 6 GB for both.	
5	VMware vSphere Hypervisor	
6	VMware vCenter 5.0 (4.1 VMware supports only 4.1 host)	
7	1 processor	
8	CPU speed of 1.5 Ghz	
9	Datastore with at least 25-GB disk space available on shared NFS/SAN storage when the Cisco VNMC is deployed in an HA cluster	
10	Internet Explorer 8.0 or Mozilla Firefox 3.6.x on Windows	
11	Flash 10.0 or 10.1	
12	Cisco VSG software available for download at the following URL: http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html	
13	Cisco VNMC software available for download at the following URL: http://www.cisco.com/en/US/products/ps11213/index.html	

Table 2-2 Preparation of the Cisco Nexus 1000V Series Switch for Further Installation Processes

Item	Requirement	Your Information
1	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)	
2	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)	

Table 2-3 Your Cisco VNMC and Cisco VSG Information for Use Later During Installation

Item	Type	Your Information
1	Cisco VSG name—Unique within the inventory folder and up to 80 characters long	
2	Hostname—Where the Cisco VSG will be installed in the inventory folder	
3	Datastore name—Where the VM files will be stored	
4	Cisco VSG management IP address	
5	VSM management IP address	
6	Cisco VNMC instance IP address	
7	Mode for installing the Cisco VSG	• Standalone • HA primary • HA secondary • Manual installation
8	Cisco VSG VLAN number	
	Service (1)	
	Management (2)	
	High availability (HA) (3)	
9	Cisco VSG port profile name	
	Data (1)	
	Management (2)	
	High availability (HA) (3)	
10	HA pair ID (HA domain ID)	
11	Cisco VSG admin password	
12	Cisco VNMC admin password	
13	Cisco VSM admin password	
14	Shared secret password (Cisco VNMC, Cisco VSG policy agent, Cisco VSM policy agent)	

Table 2-4 Tasks, Descriptions, and Prerequisites Checklist

Task	Description	Prerequisites	Completed
1	Installing the Cisco VNMC software from an OVA template	Before starting the procedure, know or do the following: • Verify that the Cisco VNMC OVA image is available in the vCenter • IP/subnet mask/gateway information for the Cisco VNMC • The admin password and hostname that you want to use • The shared secret password that you want to use (this password is what enables communication between the Cisco VNMC, VSM, and Cisco VSG) • The DNS server and domain name information • 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 VSM. The port profile is configured in the VSM and is used for the Cisco VNMC management interface. • Make sure that the host has 2-GB RAM and 25-GB available hard-disk space	
2	On the Cisco VNMC, setting up VM-Mgr for vCenter connectivity	Before starting the procedure, know or do the following: • Install Adobe Flash Player (Version 10.1.102.64 or later versions) • The IP address of the Cisco VNMC • The admin user password	
3	On the VSM, configuring the Cisco VNMC policy agent	Before starting the procedure, know or do the following: • The Cisco VNMC policy-agent image is available on the VSM (for example, `vnmc-vsmpa.1.0.1j.bin`) **Note** The string **`vsmpa`** must appear in the image name as highlighted. • The IP address of the Cisco VNMC • The shared secret password that you defined during the Cisco VNMC installation • IP connectivity between the VSM and the Cisco VNMC is okay.	
4	On the VSM, preparing the Cisco VSG port profiles	Before starting the procedure, know or do 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) None of these VLANs need to be system VLANs.	

Table 2-4 Tasks, Descriptions, and Prerequisites Checklist (continued)

Task	Description	Prerequisites	Completed
5	Installing the Cisco VSG from an OVA template	Before starting the procedure, know or do the following: • Make sure that the Cisco VSG OVA image is available in the vCenter • Cisco VSG-data and Cisco VSG-ha port profile are created on the VSM • 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 VNMC management interface. • HA pair ID • IP/subnet mask/gateway information for the Cisco VSG • Admin password • 2-GB RAM and 3-GB hard disk space are available • Cisco VNMC IP • Shared secret password • IP connectivity between the Cisco VSG and the Cisco VNMC is okay • Cisco VSG VNM-PA image name (`vnmc-vsgpa.1.0.1j.bin`)	
6	On the Cisco VSG, verifying the VNM policy-agent status	Shows Cisco VNM-PA status	
7	On the Cisco VNMC, configuring a tenant and security profile	Before starting the procedure, know or do the following: • Install Adobe Flash Player (Version 10.1) • IP address of the Cisco VNMC • Admin user password	
8	On the Cisco VNMC, assigning the Cisco VSG to the compute firewall	—	
9	On the Cisco VNMC, configuring a permit-all rule	—	
10	On the Cisco VSG, verifying the permit-all rule	—	
11	Enabling logging	—	

Table 2-4 Tasks, Descriptions, and Prerequisites Checklist (continued)

Task	Description	Prerequisites	Completed
12	Preparing Traffic VM's Port-Profile for Firewall Protection and Verifying the VSM/VEM	Make sure you have the following: • Cisco VSG data IP address (10.10.10.200) and VLAN ID (100) • Security profile name (for example, sp-web) • Organization (Org) name (for example, root/Tenant-A) • The port profile that you will edit to enable firewall protection	
13	Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs	• Make sure that you have the VM (Server-VM) that is using the port profile (pp-webserver) configured for firewall protection. • Log in to any of your client VMs (Client-VMs) and send traffic (for example, HTTP) to your ServerVM. • Check the policy-engine statistics and log on the Cisco VSG.	

Host Requirements

The Cisco VSG and Cisco VNMC installations have the following host requirements:

- ESX/ESXi platform that runs VMware software release 4.1 or 5.0 with a minimum of 4-GB physical RAM for the Cisco VSG and similar requirements for the Cisco VNMC, or 6 GB for both.
- 1 processor
- CPU speed of 1.5 GHz

Obtaining the Cisco VNMC 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/tsd_products_support_series_home.html

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

http://www.cisco.com/en/US/products/ps11213/index.html

Task 1—Installing the Cisco VNMC Software from an OVA Template

As with most software application installations, there is an order of installation for the Cisco VNMC and the Cisco VSG that must be followed to ensure that all components work and communicate properly. This first task involves using an OVA Template to install the Cisco VNMC software.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- Verify that the Cisco VNMC OVA image is available in the vCenter

- IP/subnet mask/gateway information for the Cisco VNMC
- The admin password, shared_secret, hostname that you want to use
- The DNS server and domain name information
- 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 VSM. The port profile is configured in the VSM and is used for the Cisco VNMC management interface.

- Make sure that the host has 2-GB RAM and 25-GB available hard-disk space
- Have a shared secret password available (this password is what enables communication between the Cisco VNMC, VSM, and Cisco VSG)

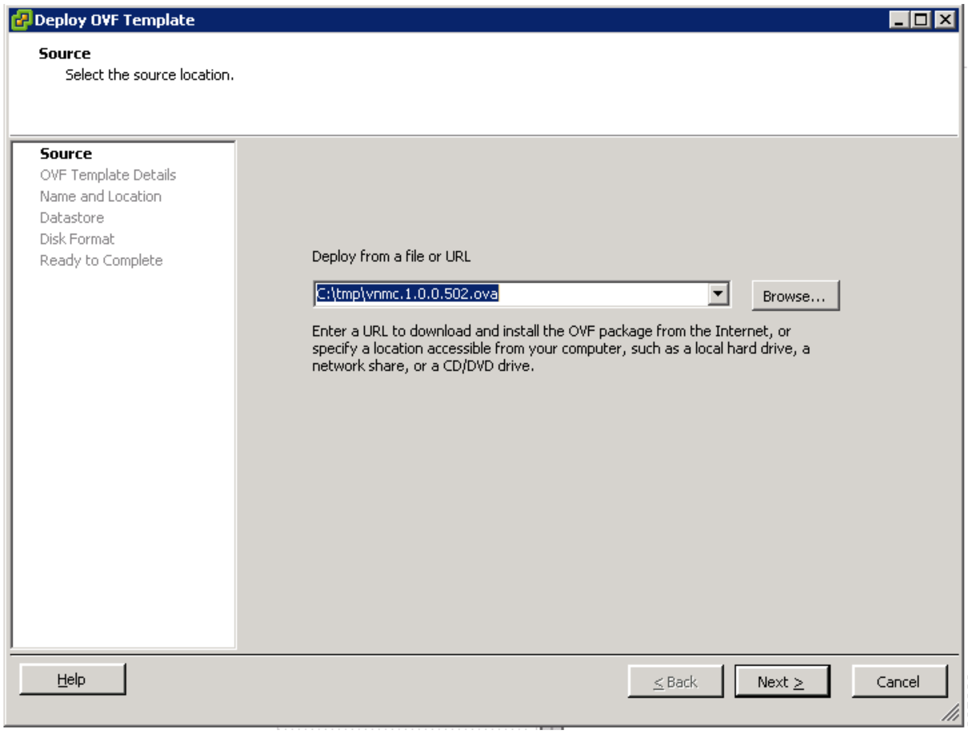
PROCEDURE

Step 1 Choose the host on which to deploy the Cisco VNMC VM.

Step 2 From the File menu, choose **Deploy OVF Template**.

The Deploy OVF Template window opens. See Figure 2-1.

Figure 2-1 Deploy OVF Template—Source Window



Deploy from a file or URL

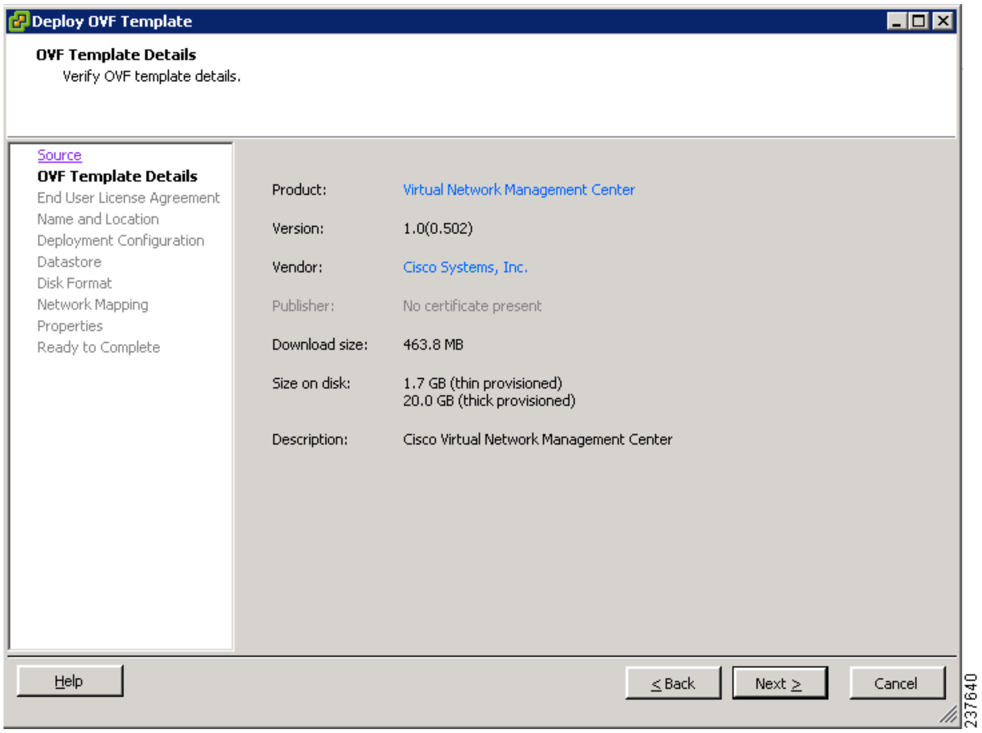
C:\tmp\vnmc.1.0.0.502.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Step 3 In the Deploy from a file or URL field, enter the path to the Cisco VNMC OVA file and click **Next**.

The OVF Template Details window opens. See Figure 2-2.

Figure 2-2 Deploy OVF Template—OVF Template Details Window



OVF Template Details

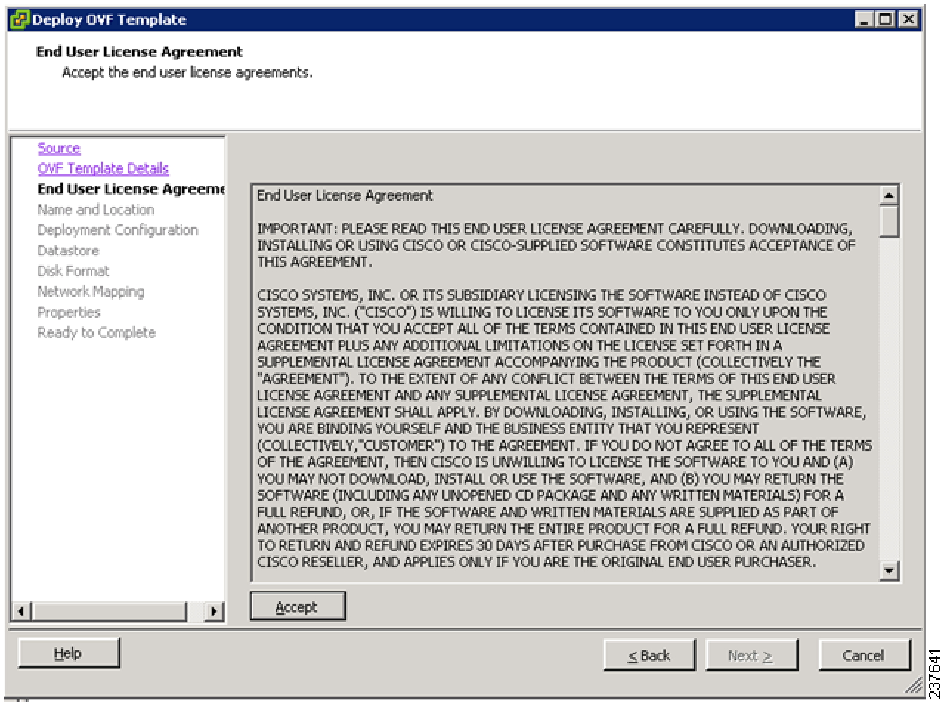
Verify OVF template details.

Product:	Virtual Network Management Center
Version:	1.0(0.502)
Vendor:	Cisco Systems, Inc.
Publisher:	No certificate present
Download size:	463.8 MB
Size on disk:	1.7 GB (thin provisioned) 20.0 GB (thick provisioned)
Description:	Cisco Virtual Network Management Center

Step 4 Review the details of the Cisco VNMC template and click **Next**.

The End User License Agreement window opens. See Figure 2-3.

Figure 2-3 Deploy OVF Template—End User License Agreement Window



End User License Agreement

Accept the end user license agreements.

End User License Agreement

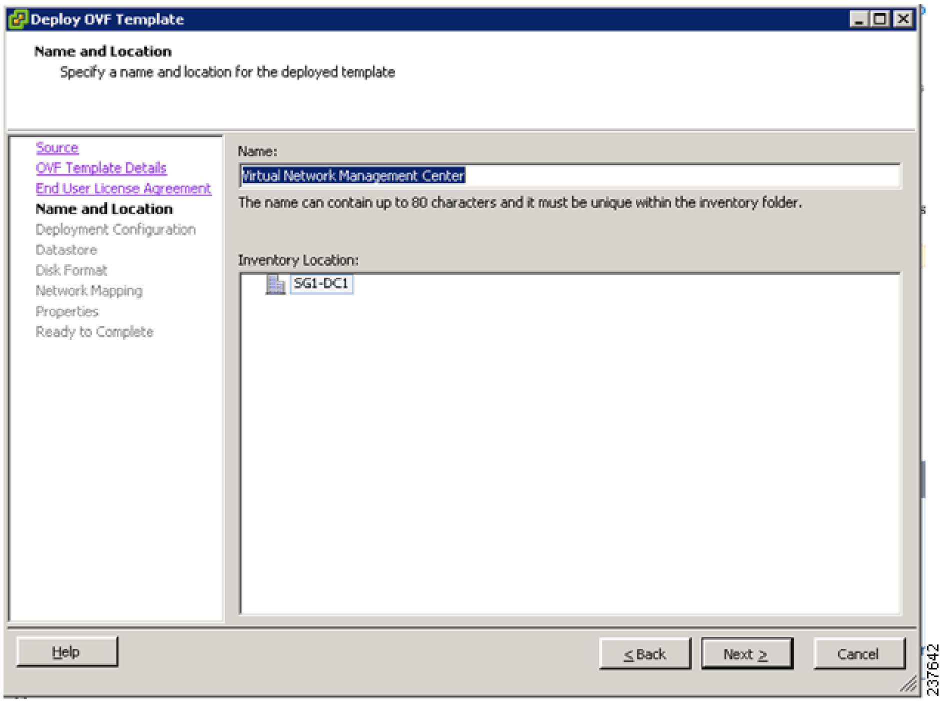
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY,"CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

Step 5 Click **Accept** to accept the End User License Agreement and click **Next.**

The Name and Location window opens. See Figure 2-4.

Figure 2-4 Deploy OVF Template—Name and Location



Name and Location

Specify a name and location for the deployed template

Name:

Virtual Network Management Center

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

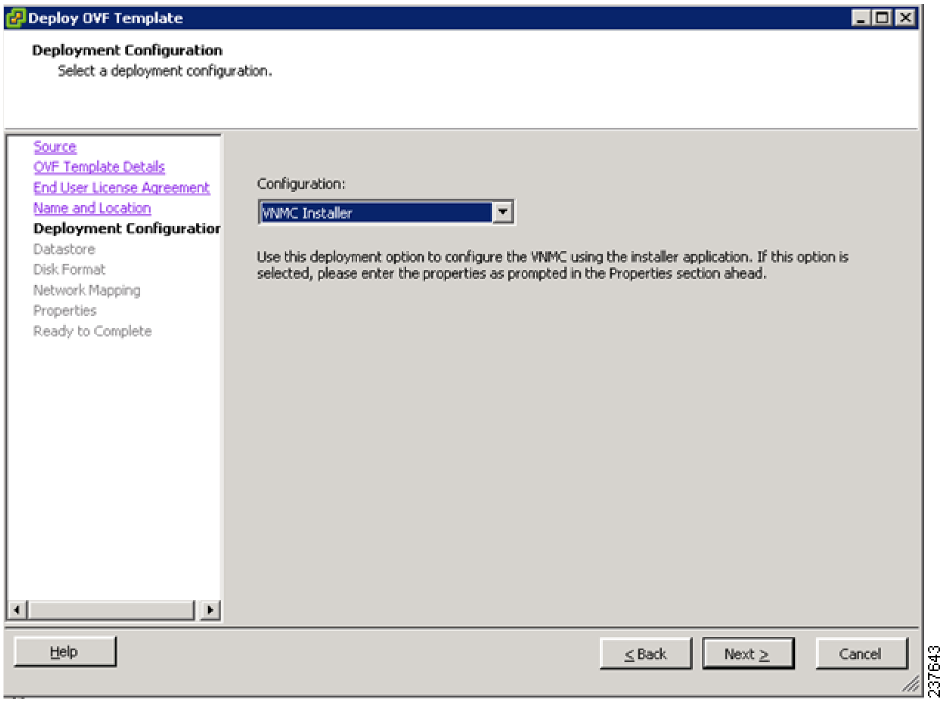
SG1-DC1

Step 6 In the Name field, enter the name of the Cisco Virtual Network Management Center. The name can contain up to 80 characters and must be unique within the inventory folder.

Step 7 In the Inventory Location pane, choose the location that you would like to use and click **Next**.

The Deployment Configuration window opens. See Figure 2-5.

Figure 2-5 Deploy OVF Template—Deployment Configuration Window



Deployment Configuration
Select a deployment configuration.

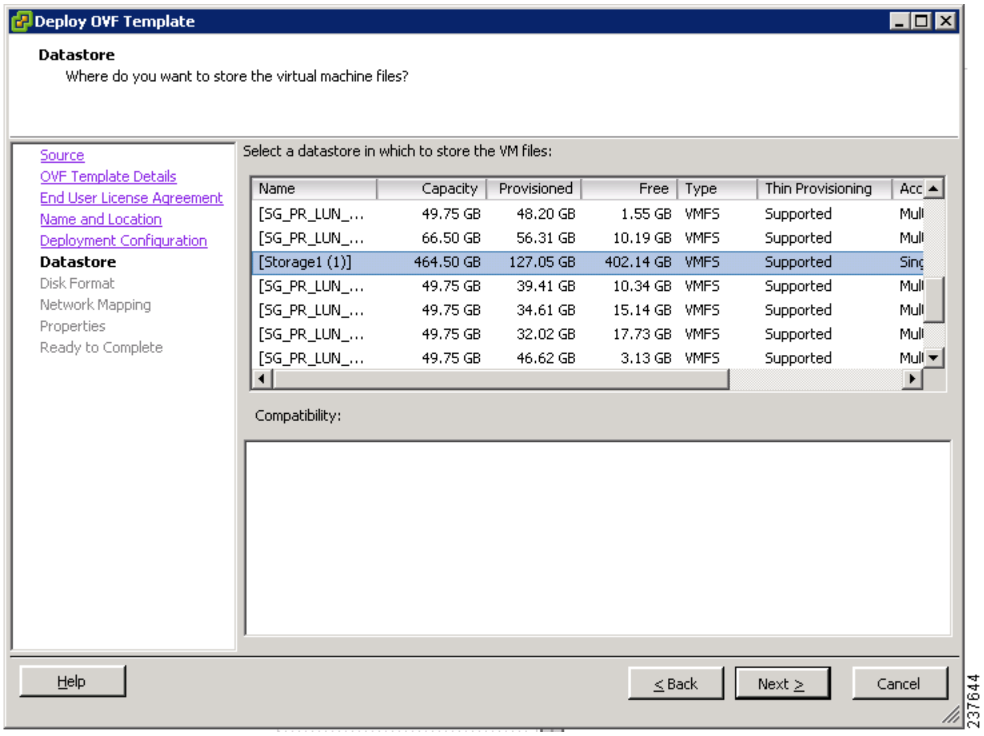
Configuration: VNMC Installer

Use this deployment option to configure the VNMC using the installer application. If this option is selected, please enter the properties as prompted in the Properties section ahead.

Step 8 From the Configuration drop-down list, choose **VNMC Installer** and click **Next**.

The Datastore window opens. See Figure 2-6.

Figure 2-6 Deploy OVF Template—Datastore Window



Datastore
Where do you want to store the virtual machine files?

Select a datastore in which to store the VM files:

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Acc
[SG_PR_LUN_...	49.75 GB	48.20 GB	1.55 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	66.50 GB	56.31 GB	10.19 GB	VMFS	Supported	Mul
[Storage1 (1)]	464.50 GB	127.05 GB	402.14 GB	VMFS	Supported	Sing
[SG_PR_LUN_...	49.75 GB	39.41 GB	10.34 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	49.75 GB	34.61 GB	15.14 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	49.75 GB	32.02 GB	17.73 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	49.75 GB	46.62 GB	3.13 GB	VMFS	Supported	Mul

Compatibility:

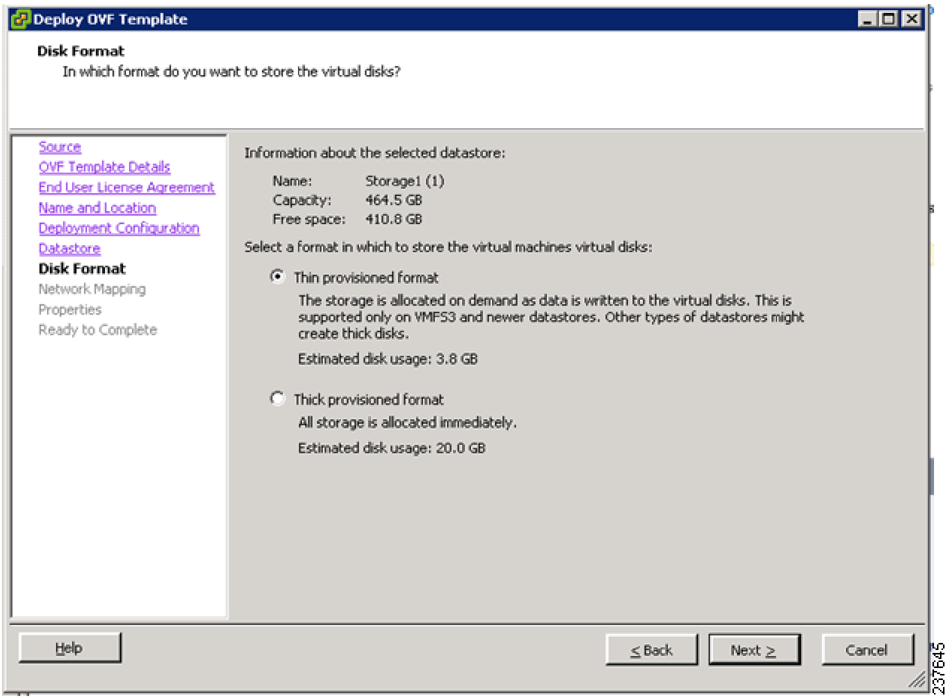
Step 9 In the Datastore pane, choose the datastore for the VM and click **Next**.

Note 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 ESX host, this window does not display and you are assigned to the one that is available.

The Disk Format window opens. See Figure 2-7.

Figure 2-7 Deploy OVF Template—Disk Format Window



Disk Format
In which format do you want to store the virtual disks?

Information about the selected datastore:

Name: Storage1 (1)
Capacity: 464.5 GB
Free space: 410.8 GB

Select a format in which to store the virtual machines virtual disks:

● Thin provisioned format
The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.
Estimated disk usage: 3.8 GB

○ Thick provisioned format
All storage is allocated immediately.
Estimated disk usage: 20.0 GB

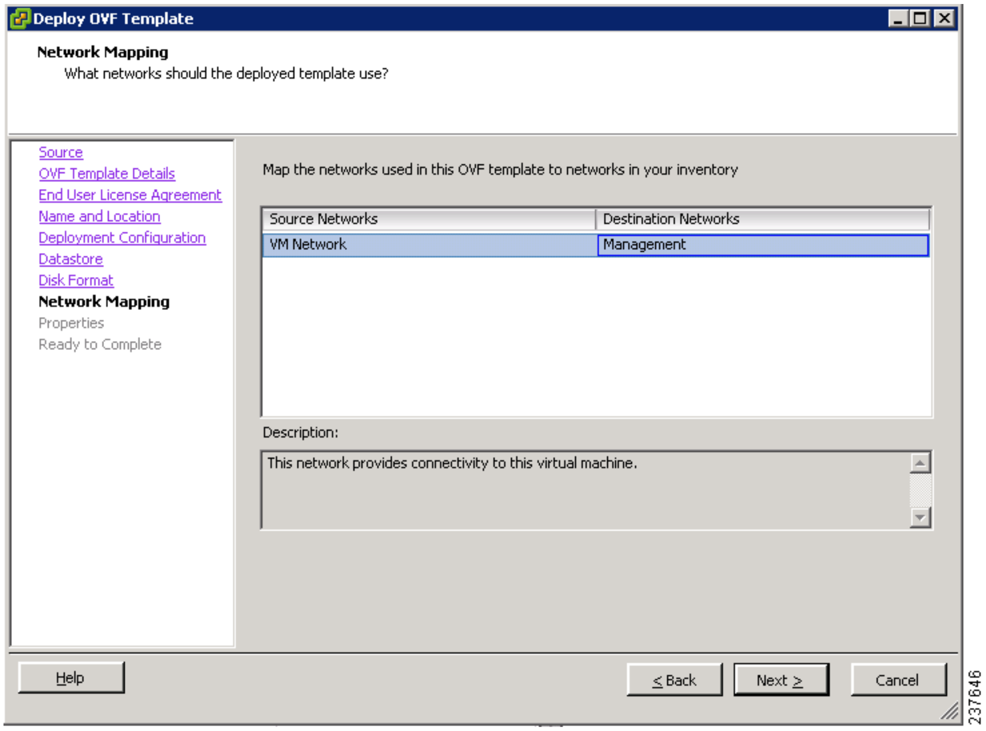
Step 10 Click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks and click **Next**.

Note The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.

Note Ignore the red text in the window.

The Network Mapping window opens. See Figure 2-8.

Figure 2-8 Deploy OVF Template—Network Mapping Window



Deploy OVF Template

Network Mapping
What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

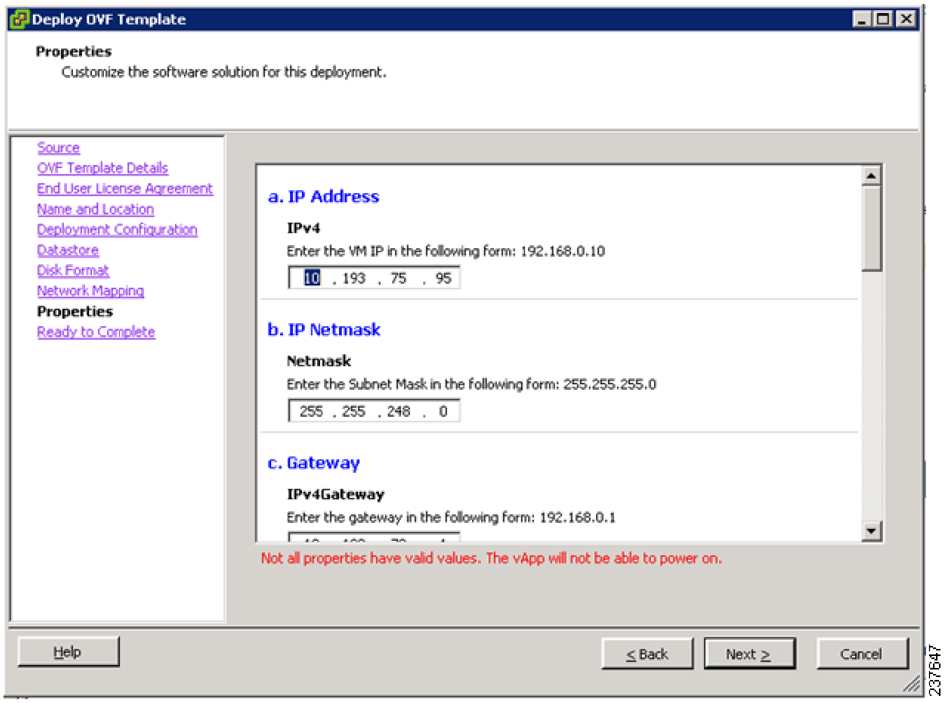
Source Networks	Destination Networks
VM Network	Management

Description:
This network provides connectivity to this virtual machine.

Step 11 In the network mapping pane, choose the management network port profile for the VM and click **Next**.

The Properties window opens. See Figure 2-9.

Figure 2-9 Deploy OVF Template—Properties Window



Properties
Customize the software solution for this deployment.

a. IP Address

IPv4
Enter the VM IP in the following form: 192.168.0.10
10 . 193 . 75 . 95

b. IP Netmask

Netmask
Enter the Subnet Mask in the following form: 255.255.255.0
255 . 255 . 248 . 0

c. Gateway

IPv4Gateway
Enter the gateway in the following form: 192.168.0.1

Not all properties have valid values. The vApp will not be able to power on.

Step 12 Do the following:

a. In the IPv4 field, enter the IP address.

b. In the Netmask field, enter the subnet mask.

c. In the IPv4Gateway field, enter the gateway.

d. In the Hostname section:

- In the DomainName field, enter the domain name.
- In the DNS field, enter the domain name server name.

e. In the Passwords section:

- In the Password field, enter the admin password.
- In the Secret field, enter the shared secret password Shared Secret:

Note Parameters for choosing the Shared Secret password:
- The password must be more than eight characters long.
- Characters not supported for shared secret password: & ' " ` ( )<>|\ characters and all other characters supported on the keyboard.
- The password should contain lowercase letters, uppercase letters, digits and special characters.
- The password should not contain characters, repeated three or more times consecutively.
- The new shared secret passwords should not repeat or reverse the username
- The password should not be "cisco", "ocsic", or any variant obtained by changing the capitalization of letters therein.
- The password should not be formed by easy permutations of characters present in the username or Cisco.

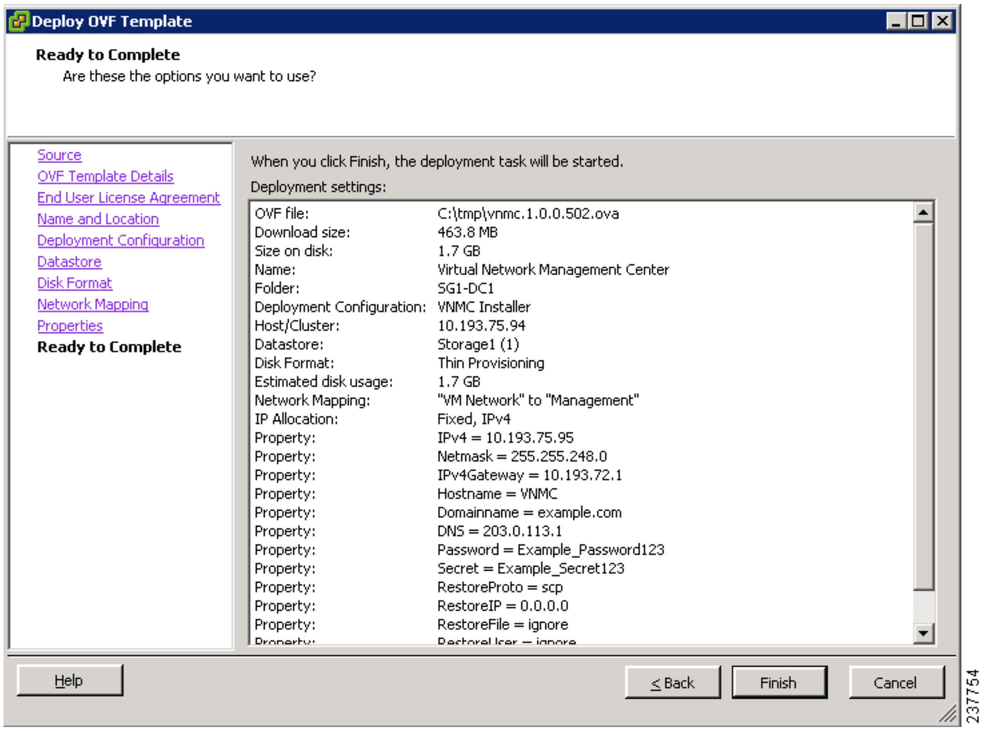
Step 13 Click **Next**.

Note 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.

Note Ignore the VNMC Restore fields.

The Ready to Complete window opens. See Figure 2-10.

Figure 2-10 Deploy OVF Template—Ready to Complete Window



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\tmp\vnmc.1.0.0.502.ova
Download size:	463.8 MB
Size on disk:	1.7 GB
Name:	Virtual Network Management Center
Folder:	SG1-DC1
Deployment Configuration:	VNMC Installer
Host/Cluster:	10.193.75.94
Datastore:	Storage1 (1)
Disk Format:	Thin Provisioning
Estimated disk usage:	1.7 GB
Network Mapping:	"VM Network" to "Management"
IP Allocation:	Fixed, IPv4
Property:	IPv4 = 10.193.75.95
Property:	Netmask = 255.255.248.0
Property:	IPv4Gateway = 10.193.72.1
Property:	Hostname = VNMC
Property:	Domainname = example.com
Property:	DNS = 203.0.113.1
Property:	Password = Example_Password123
Property:	Secret = Example_Secret123
Property:	RestoreProto = scp
Property:	RestoreIP = 0.0.0.0
Property:	RestoreFile = ignore
Property:	RestoreUser = ignore

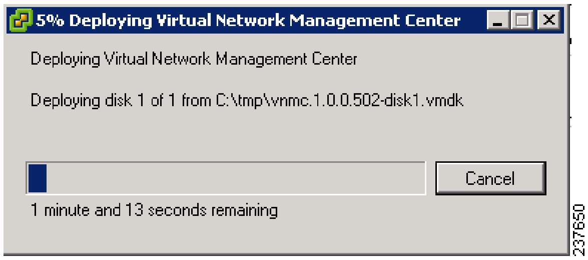
Step 14 Review the deployment settings information and click **Finish**.

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

The Deploying Virtual Network Management Center progress indicator opens. See Figure 2-11.

The progress bar in Figure 2-11 shows how much of the deployment task is completed before the Cisco VNMC is deployed.

Figure 2-11 Deploying Virtual Network Management Center—Deploying Disk Files Progress Indicator



5% Deploying Virtual Network Management Center

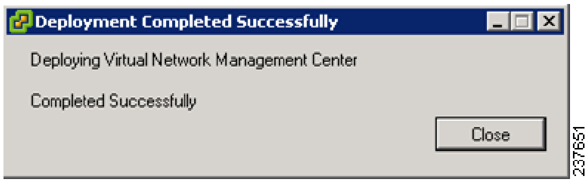
Deploying Virtual Network Management Center

Deploying disk 1 of 1 from C:\tmp\vnmc.1.0.0.502-disk1.vmdk

1 minute and 13 seconds remaining

The progress indicator in Figure 2-12 shows that the deployment has completed successfully.

Figure 2-12 Deployment Completed Successfully Progress Indicator



Deployment Completed Successfully

Deploying Virtual Network Management Center

Completed Successfully

Step 15 Click **Close**.

Step 16 Power on the Cisco VNMC VM.

Task 2—On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity

This section includes the following topics:

- Downloading the vCenter Extension File from the Cisco VNMC, page 2-15
- Registering the vCenter Extension Plugin in the vCenter, page 2-18
- Configuring the vCenter in VM-Manager in the Cisco VNMC, page 2-19

BEFORE YOU BEGIN

Before doing this procedure, know or do the following:

- Install Adobe Flash Player (Version 10.1.102.64)
- IP address of the Cisco VNMC
- Admin user password

Downloading the vCenter Extension File from the Cisco VNMC

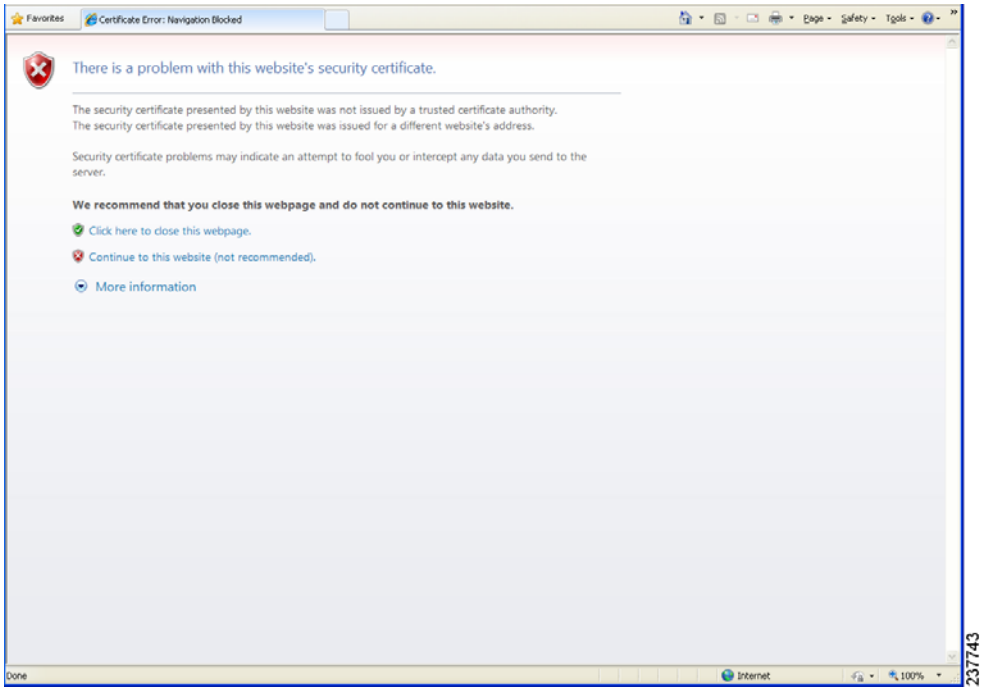
You can download the vCenter extension file from the Cisco VNMC.

PROCEDURE

Step 1 For Cisco VNMC access, from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://xxx.xxx.xxx.xxx).

A Website Security Certification window opens. See Figure 2-13.

Figure 2-13 Website Security Certification Window



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

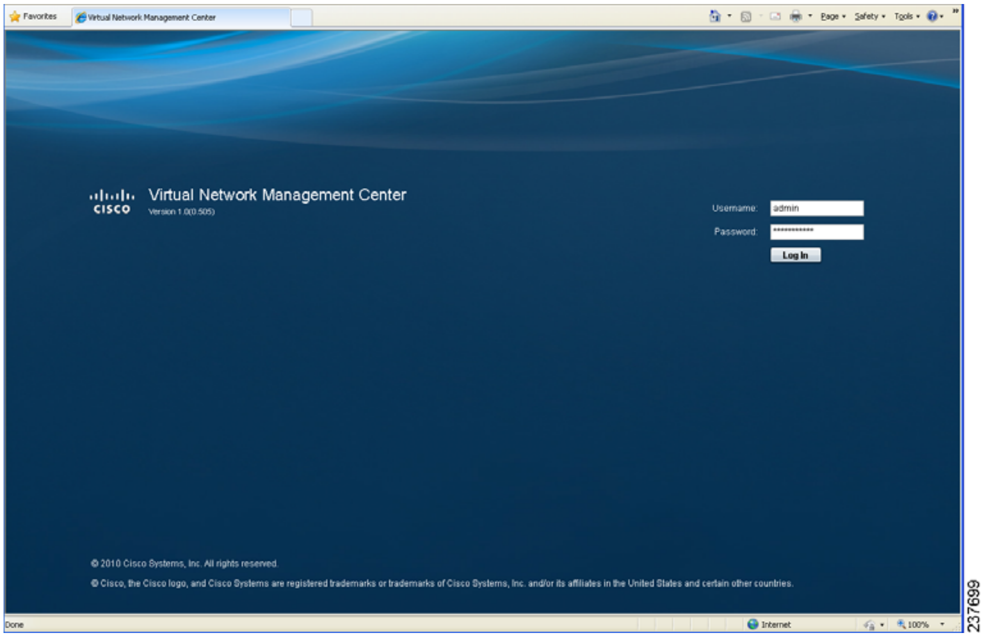
Continue to this website (not recommended).

More information

Step 2 On the certificate warning window, click **Continue to this website**.

The Cisco VNMC Access window opens. See Figure 2-14.

Figure 2-14 VNMC Access Window



Username: admin

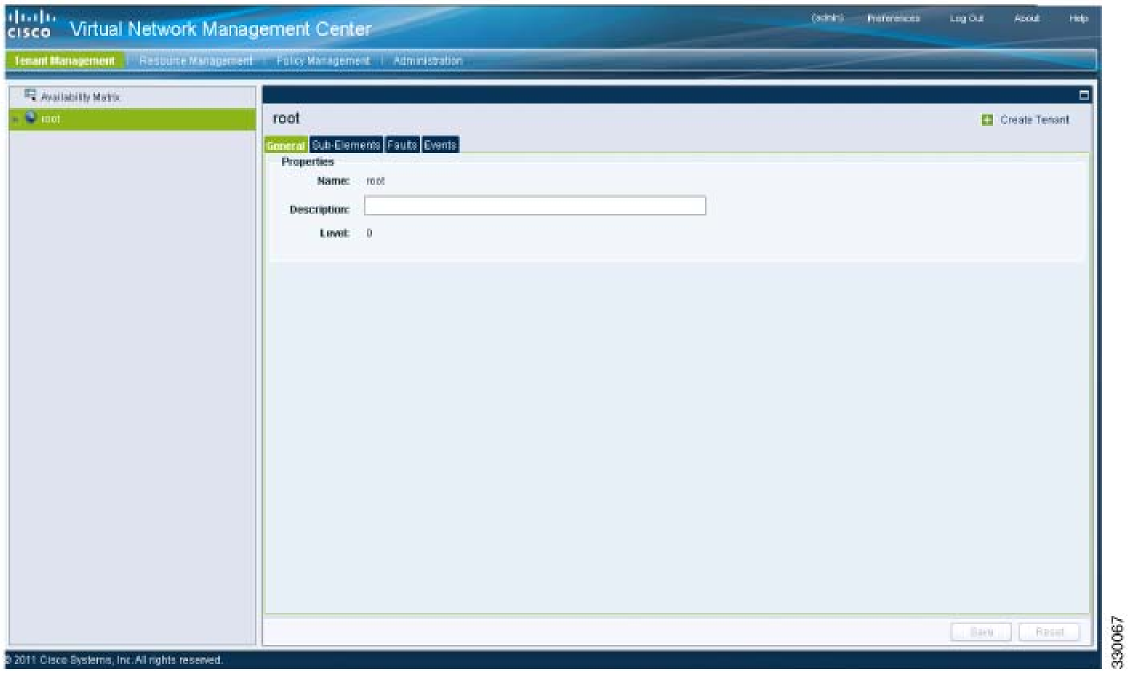
Password: ************

© 2010 Cisco Systems, Inc. All rights reserved.

© Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 3 Log in to the Cisco VNMC with the username “admin” and your password that you set when installing the application. The VNMC Main window opens. See Figure 2-15.

Figure 2-15 Cisco Virtual Network Management Center—Opening Window



Name: root

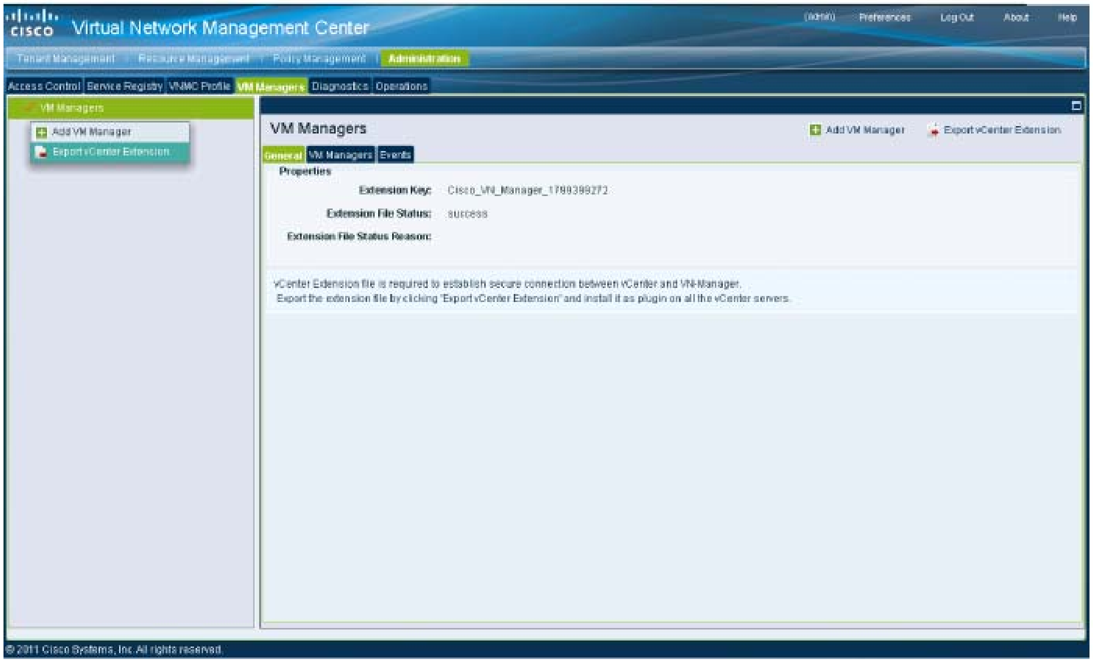
Description:

Level: 0

© 2011 Cisco Systems, Inc. All rights reserved.

Step 4 Choose **Administration > VM Managers**. The Cisco Virtual Network Management Center VM Managers window opens. See Figure 2-16.

Figure 2-16 Cisco VNMC Administration VM Managers Window



Extension Key: Cisco_VN_Manager_1789399272

Extension File Status: success

Extension File Status Reason:

vCenter Extension file is required to establish secure connection between vCenter and VN-Manager.
Export the extension file by clicking "Export vCenter Extension" and install it as plugin on all the vCenter servers.

Step 5 From VM Managers, right-click and choose **Export vCenter Extension**, and save the file on your vCenter Desktop.

Step 6 The vCenter Desktop displays as shown in Figure 2-17.

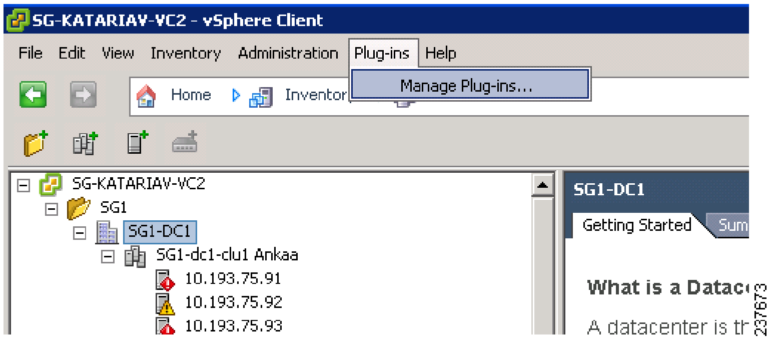
Registering the vCenter Extension Plugin in the vCenter

This task is completed from within your client desktop vSphere client directory.

PROCEDURE

Step 1 From vSphere client, log in to vCenter. See Figure 2-17.

Figure 2-17 vSphere Client Directory Window

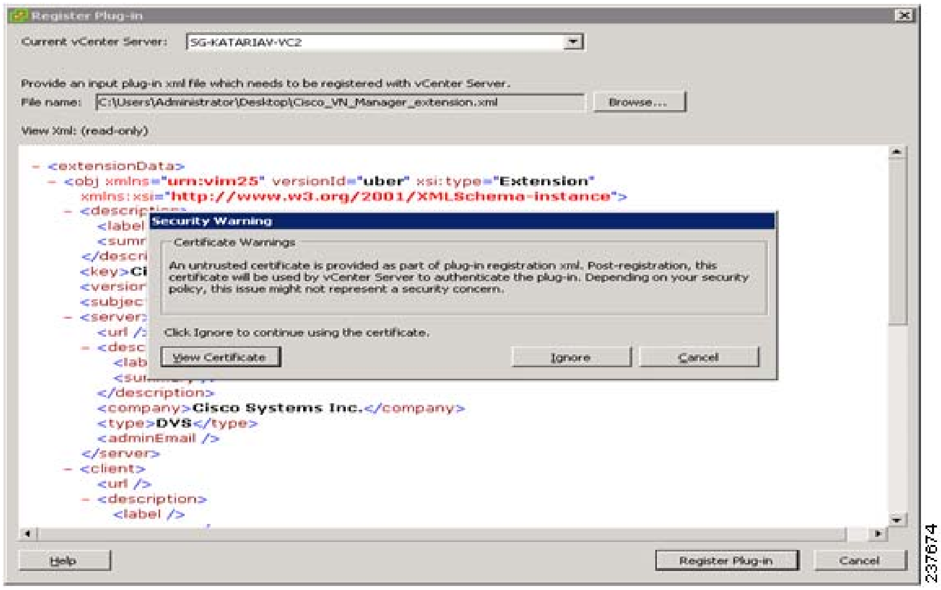


Step 2 Choose **Plug-ins** > **Manage Plug-ins**.

Step 3 Right-click in an empty space, and in the drop-down list, choose **New Plug-in**.

The Register Plug-in window that contains the vSphere client and vCenter directory for managing plug-ins opens. See Figure 2-18.

Figure 2-18 vSphere Client and vCenter Directory for Managing Plug-ins with Security Warning



Register Plug-in

Current vCenter Server: SG-KATARIAV-VC2

Provide an input plug-in xml file which needs to be registered with vCenter Server.

File name: C:\Users\Administrator\Desktop\Cisco_VN_Manager_extension.xml

View Xml: (read-only)

```
- <extensionData>
  - <obj xmlns="urn:vim25" versionId="uber" xsi:type="Extension"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    - <descrip
        <label
        <sumr
      </descri
      <key>Ci
      <versior
      <subjec
    - <server
        <url /
      - <desc
          <lab
          <su
        </description>
        <company>Cisco Systems Inc.</company>
        <type>DVS</type>
        <adminEmail />
      </server>
    - <client>
        <url />
      - <description>
          <label />
```

Security Warning

Certificate Warnings

An untrusted certificate is provided as part of plug-in registration xml. Post-registration, this certificate will be used by vCenter Server to authenticate the plug-in. Depending on your security policy, this issue might not represent a security concern.

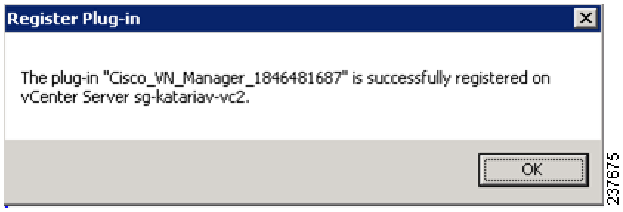
Click Ignore to continue using the certificate.

Step 4 Browse to the Cisco VNMC vCenter extension file and click **Register Plug-in**.

Step 5 On the security warning that displays, click **Ignore**.

The Register Plug-in progress indicator opens. When the registration has completed successfully, the successful registration message will display. See Figure 2-19.

Figure 2-19 Register Plug-in Progress Success Indicator



Register Plug-in

The plug-in "Cisco_VN_Manager_1846481687" is successfully registered on vCenter Server sg-katariav-vc2.

Step 6 Click **OK**.

Step 7 Click **Close**.

Configuring the vCenter in VM-Manager in the Cisco VNMC

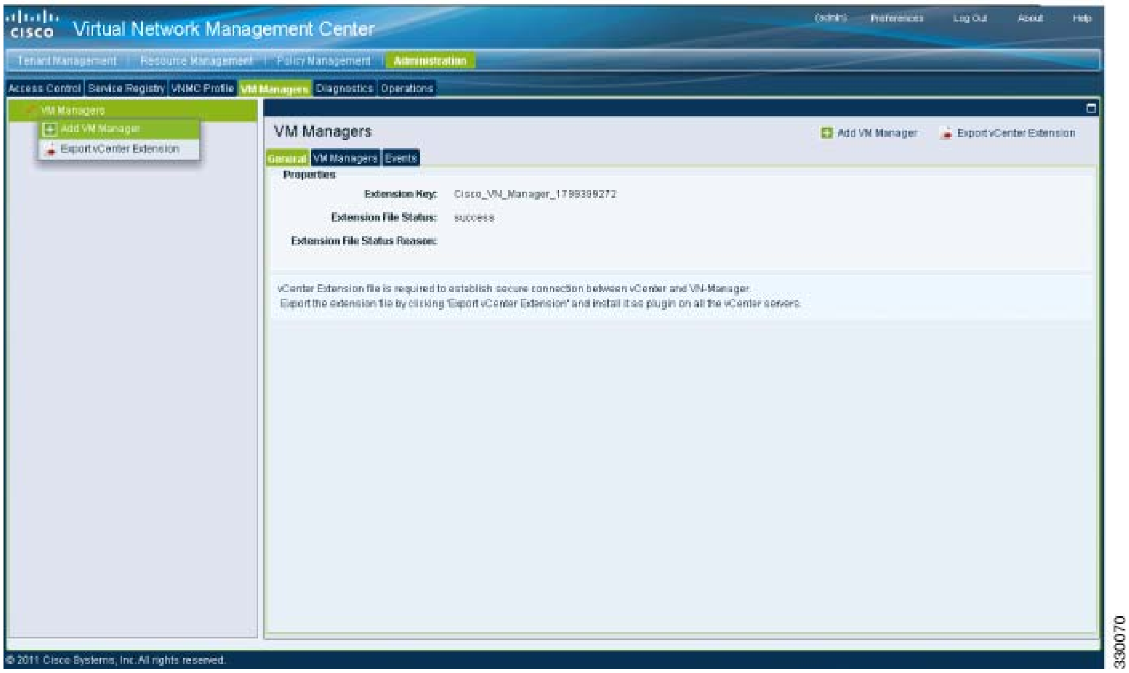
You can configure the vCenter in VM-Manager in the Cisco VNMC.

PROCEDURE

Step 1 Return to the Cisco VNMC and click **Administration** > **VM Managers**.

The Cisco VNMC Administration VM Managers window opens. See Figure 2-20.

Figure 2-20 Cisco VNMC Administration VM Managers Window



Properties

Extension Key: Cisco_VN_Manager_1799399272

Extension File Status: success

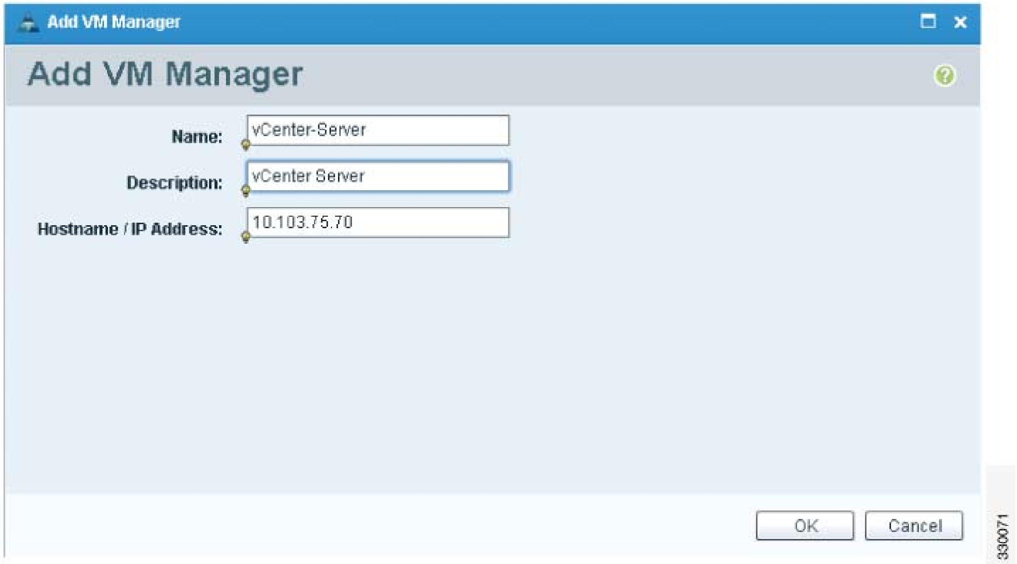
Extension File Status Reason:

vCenter Extension file is required to establish secure connection between vCenter and VN-Manager.
Export the extension file by clicking 'Export vCenter Extension' and install it as plugin on all the vCenter servers.

Step 2 Choose VM Managers > Add VM Manager.

The Add VM Manager dialog box opens. See Figure 2-21.

Figure 2-21 Add VM Manager Dialog Box



Add VM Manager

Name: vCenter-Server

Description: vCenter Server

Hostname / IP Address: 10.103.75.70

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 The successful addition should display the Admin State as enable and the Operational State as up with the version information.

Task 3—On the VSM, Configuring the Cisco VNMC Policy-Agent

Once you have the Cisco VNMC installed, you must register the VSM with the Cisco VNMC policy agent.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- Make sure that the Cisco VNMC policy-agent image is available on the VSM (for example, vnmc-**vsmpa**.1.0.1j.bin)

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

- The IP address of the Cisco VNMC
- The shared secret password you defined during Cisco VNMC installation

- Make sure that IP connectivity between the VSM and the Cisco VNMC is okay.

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

PROCEDURE

Step 1 On the VSM, enter the following commands:

```
vsm# configure terminal
vsm(config)# vnm-policy-agent
vsm(config-vnm-policy-agent)# registration-ip 10.193.75.95
vsm(config-vnm-policy-agent)# shared-secret Example_Secret123
vsm(config-vnm-policy-agent)# policy-agent-image vnmc-vsmpa.1.0.1j.bin
vsm(config-vnm-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

Step 2 Check the status of the VNM policy agent configuration to verify that you have installed the Cisco VNMC correctly and it is reachable by entering the **show vnm-pa status** command.

This example shows that the Cisco VNMC is reachable and the installation is correct:

```
vsm# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.0(1j)-vsm
vsm#
```

The VSM is now registered with the Cisco VNMC.

EXAMPLES

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

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

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

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

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

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

BEFORE YOU BEGIN

Before starting the procedure, know or do 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 To exit, press **Ctrl-Z**.

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 To end the session, press **Ctrl-Z**.

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)#
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)#
```

To end the session, press **Ctrl-Z**.

Task 5—Installing the Cisco VSG from an OVA Template

Once you have installed the Cisco Virtual Network Management Center (Cisco VNMC), configured the Cisco VNM policy agent on the VSM, and prepared the Cisco VSG port profiles by creating the VLANs that will be used, you now must install the Cisco VSG.

For this example, the OVF Template is used to install a Cisco VSG in standalone mode.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- Make sure that the Cisco VSG OVA image is available in the vCenter.
- Cisco VSG-Data and Cisco VSG-ha port profile are created on VSM.
- 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 VNMC management interface.

- VSG Data port-profile: VSG-Data
- VSG HA port-profile: VSG-ha
- HA ID
- IP/subnet mask/gateway information for the Cisco VSG
- Admin password
- 2-GB RAM and 3-GB hard disk space
- Cisco VNMC IP
- Shared secret
- IP connectivity between Cisco VSG and Cisco VNMC is okay
- Cisco VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)

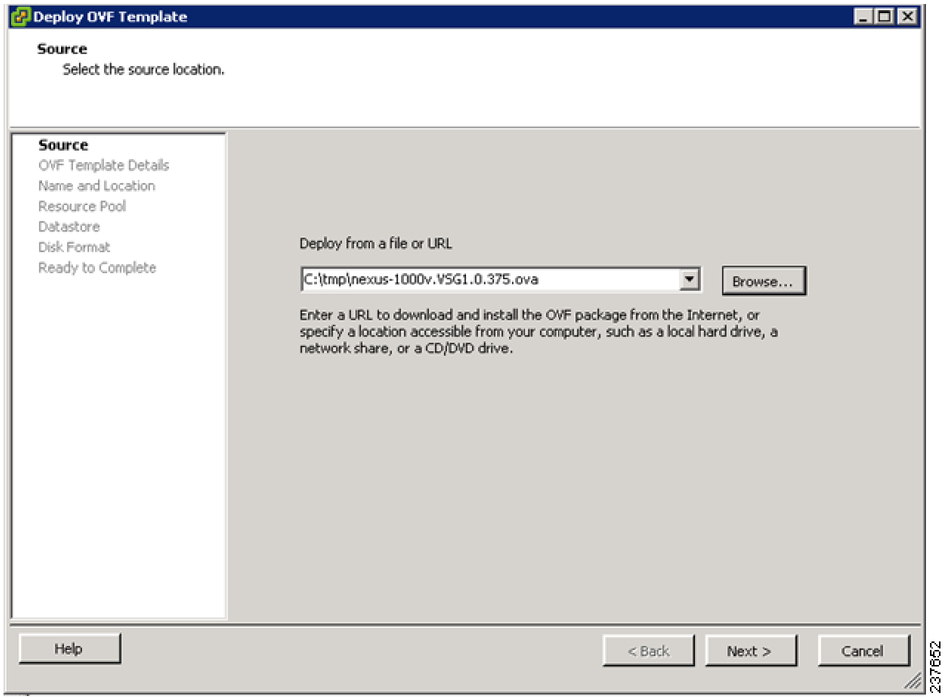
PROCEDURE

Step 1 Choose your host on which to deploy the Cisco VSG VM.

Step 2 From the File menu, choose **Deploy OVF Template**.

The Source window opens. See Figure 2-22.

Figure 2-22 Deploy OVF Template—Source Window



Source

Select the source location.

Deploy from a file or URL

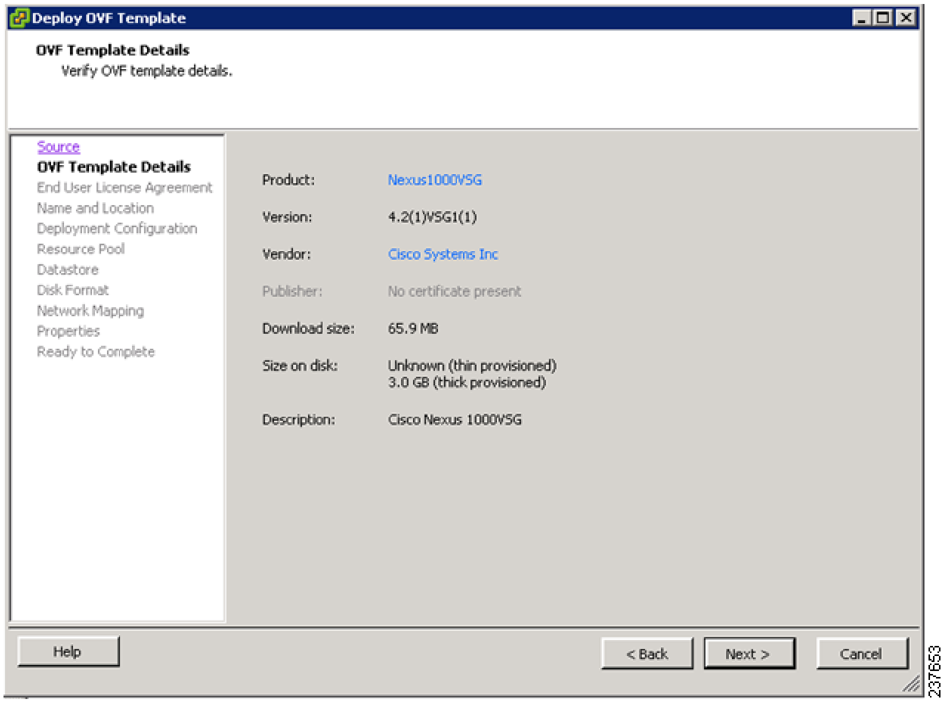
C:\tmp\nexus-1000v.VSG1.0.375.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Step 3 In the Deploy from a file or URL field, enter the path to the Cisco VSG OVA file and click **Next**.

The OVF Template Details window opens. See Figure 2-23.

Figure 2-23   Deploy OVF Template—OVF Template Details Window



OVF Template Details
Verify OVF template details.

Product: Nexus1000VSG

Version: 4.2(1)VSG1(1)

Vendor: Cisco Systems Inc

Publisher: No certificate present

Download size: 65.9 MB

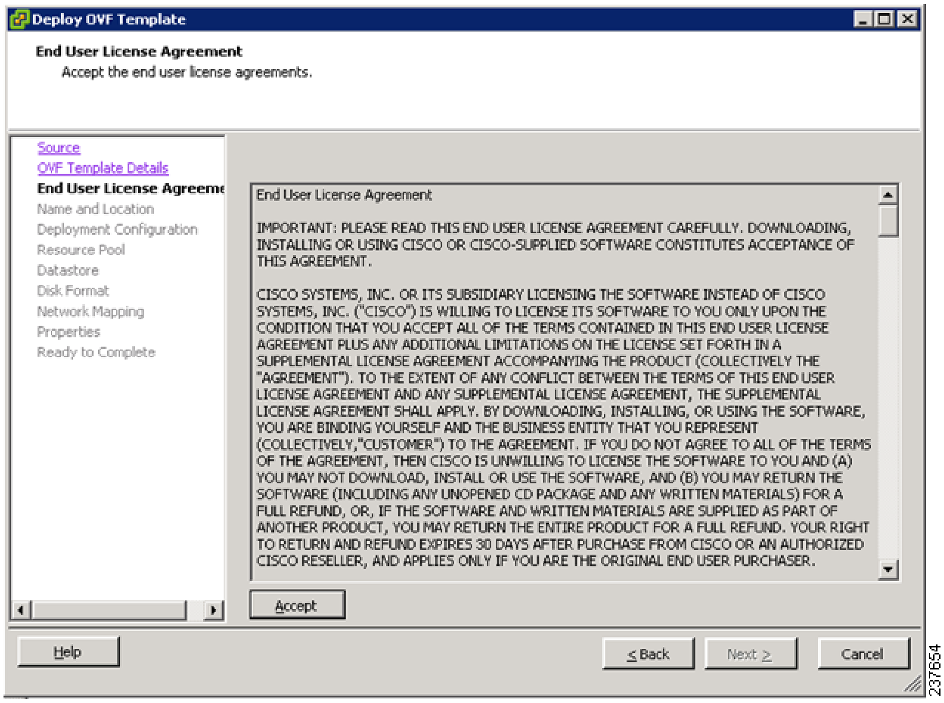
Size on disk: Unknown (thin provisioned)
3.0 GB (thick provisioned)

Description: Cisco Nexus 1000VSG

Step 4   Review the details of the Cisco VSG template and click **Next**.

The End User License Agreement window opens. See Figure 2-24.

Figure 2-24   Deploy OVF Template—End User License Agreement Window



End User License Agreement
Accept the end user license agreements.

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

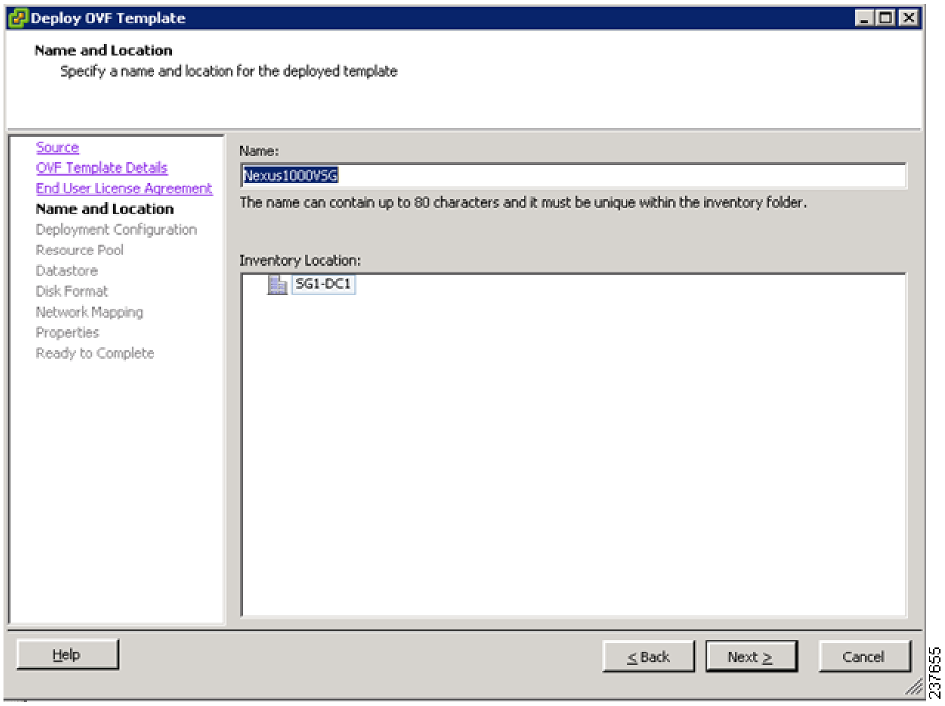
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY,"CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

Step 5 Click **Accept** to accept the End User License Agreement.

Step 6 Click **Next**.

The Name and Location window opens. See Figure 2-25.

Figure 2-25 Deploy OVF Template—Name and Location Window



Deploy OVF Template

Name and Location

Specify a name and location for the deployed template

Name: Nexus1000VSG

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location: SG1-DC1

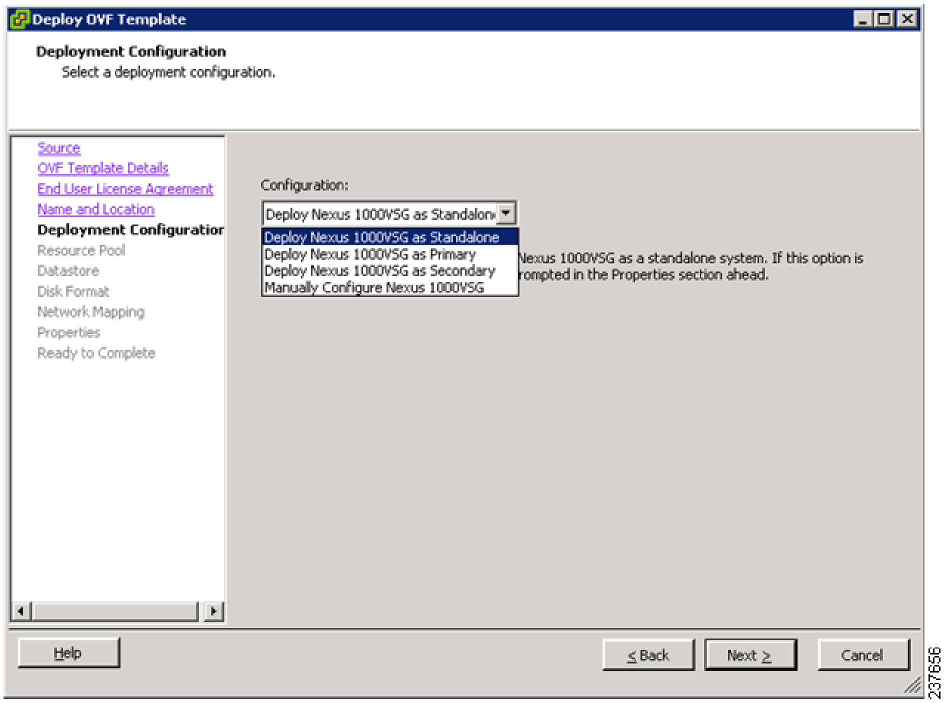
Step 7 In the Name field, enter the name that you want to use for the Cisco VSG.

Step 8 In the Inventory Location field, choose the location that you want to use for hosting the Cisco VSG.

Step 9 Click **Next**.

The Deployment Configuration window opens. See Figure 2-26.

Figure 2-26 Deploy OVF Template—Deployment Configuration Window


Deployment Configuration

Select a deployment configuration.

Configuration:

Deploy Nexus 1000VSG as Standalon

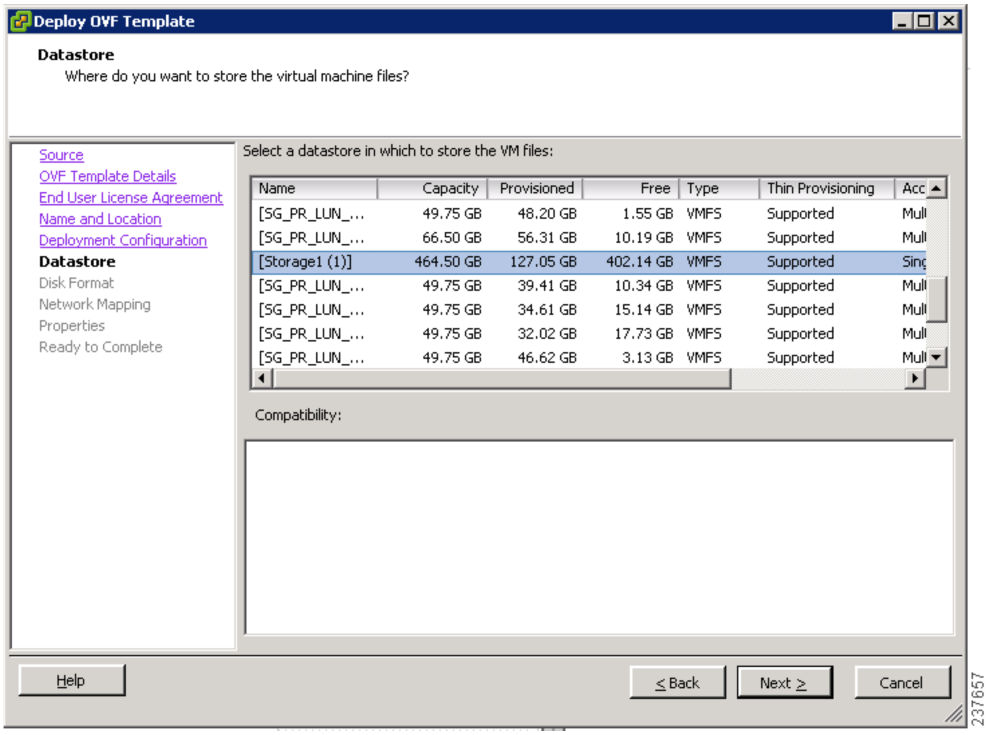
- Deploy Nexus 1000VSG as Standalone
- Deploy Nexus 1000VSG as Primary
- Deploy Nexus 1000VSG as Secondary
- Manually Configure Nexus 1000VSG

Nexus 1000VSG as a standalone system. If this option is
rompted in the Properties section ahead.

Step 10 From the Configuration drop-down list, choose **Deploy Nexus 1000V as Standalone** and click **Next**.

The Datastore window opens. See Figure 2-27.

Figure 2-27 Deploy OVF Template—Datastore Window



Deploy OVF Template

Datastore
Where do you want to store the virtual machine files?

- Source
- OVF Template Details
- End User License Agreement
- Name and Location
- Deployment Configuration
- **Datastore**
- Disk Format
- Network Mapping
- Properties
- Ready to Complete

Select a datastore in which to store the VM files:

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Acc
[SG_PR_LUN_...	49.75 GB	48.20 GB	1.55 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	66.50 GB	56.31 GB	10.19 GB	VMFS	Supported	Mul
[Storage1 (1)]	464.50 GB	127.05 GB	402.14 GB	VMFS	Supported	Sing
[SG_PR_LUN_...	49.75 GB	39.41 GB	10.34 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	49.75 GB	34.61 GB	15.14 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	49.75 GB	32.02 GB	17.73 GB	VMFS	Supported	Mul
[SG_PR_LUN_...	49.75 GB	46.62 GB	3.13 GB	VMFS	Supported	Mul

Compatibility:

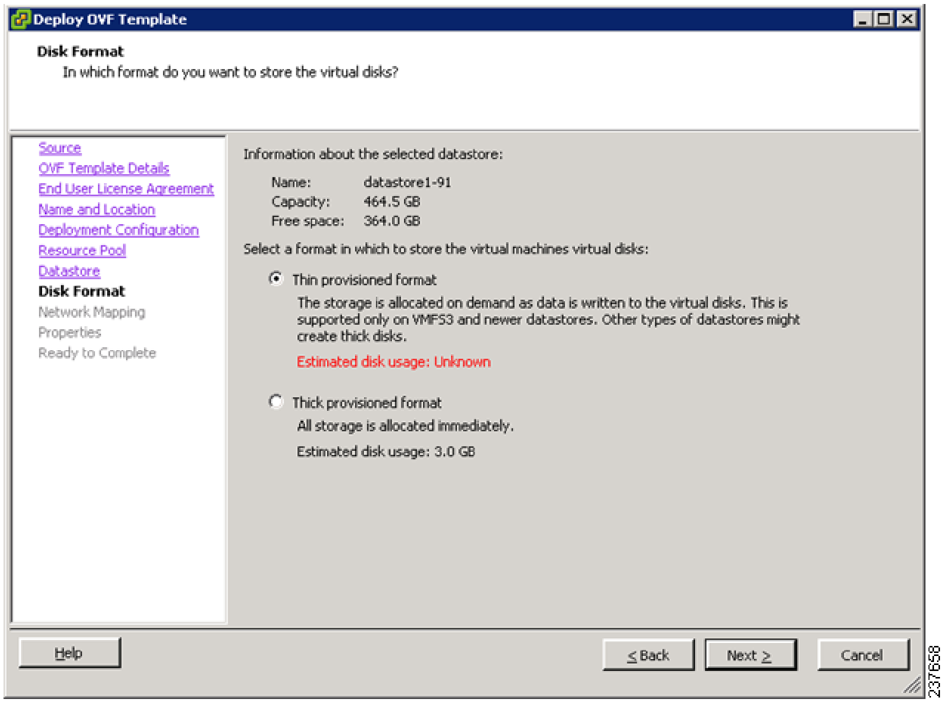
Step 11 In the Select a datastore in which to store the VM files pane, choose the datastore for the VM and click **Next**.

Note Storage can be local or shared-remote such as a network file storage (NFS) or a storage area network (SAN).

Note If only one storage location is available for an ESX host, this window does not display and you are assigned to the storage location that is available.

The Disk Format window opens. See Figure 2-28.

Figure 2-28 Deploy OVF Template—Disk Format Window



Disk Format

In which format do you want to store the virtual disks?

Information about the selected datastore:

Name:	datastore1-91
Capacity:	464.5 GB
Free space:	364.0 GB

Select a format in which to store the virtual machines virtual disks:

● Thin provisioned format

The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks.

Estimated disk usage: Unknown

○ Thick provisioned format

All storage is allocated immediately.

Estimated disk usage: 3.0 GB

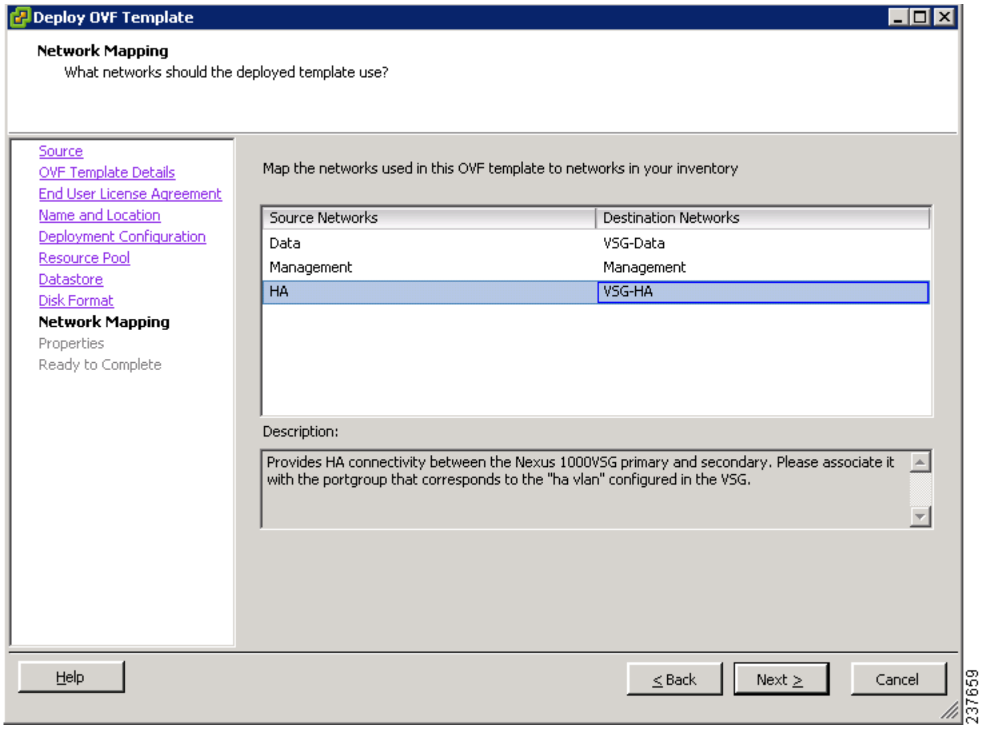
Step 12 Click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks and click **Next**.

Note The default is thick provisioned. If you do not want to allocate the storage immediately, use thin provisioned.

Note Ignore the red text in the window.

The Network Mapping window opens. See Figure 2-29.

Figure 2-29 Deploy OVF Template—Network Mapping Window



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Data	VSG-Data
Management	Management
HA	VSG-HA

Description:

Provides HA connectivity between the Nexus 1000VSG primary and secondary. Please associate it with the portgroup that corresponds to the "ha vlan" configured in the VSG.

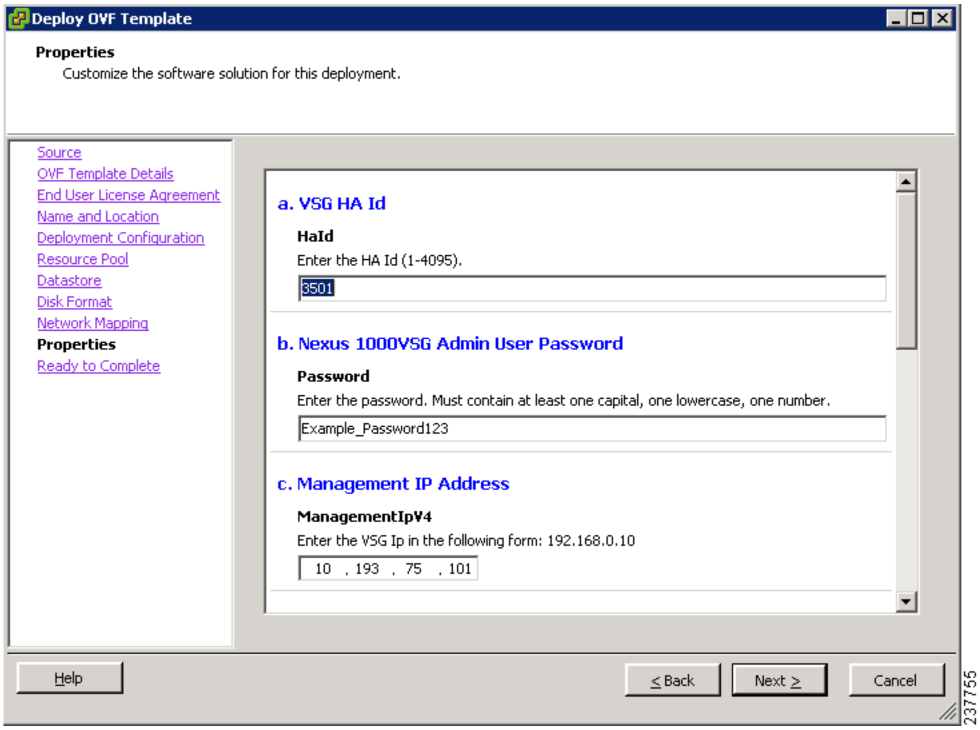
Step 13 Choose the data interface port profile as **VSG-Data**, choose the management interface port profile as **Management**, and choose the HA interface port profile as **VSG-ha**.

Step 14 Click **Next**.

Note In this example, for VSG-Data and VSG-ha port profiles created in Task 4—On the VSM, Preparing Cisco VSG Port Profiles, page 2-22, the management port profile is used for management connectivity and is the same as in the VSM and Cisco VNMC.

The Properties window opens. See Figure 2-30.

Figure 2-30 Deploy OVF Template—Properties Window



Properties
Customize the software solution for this deployment.

a. VSG HA Id

HaId
Enter the HA Id (1-4095).
3501

b. Nexus 1000VSG Admin User Password

Password
Enter the password. Must contain at least one capital, one lowercase, one number.
Example_Password123

c. Management IP Address

ManagementIpV4
Enter the VSG Ip in the following form: 192.168.0.10
10 . 193 . 75 . 101

Step 15 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 Management IP Address section, do the following:

  - In the ManagementIpV4 field, enter the IP address for the Cisco VSG.
  - In the ManagementIpV4 Subnet field, enter the subnet mask.

d. In the Gateway field, enter the gateway name.

e. In the VnmcIpV4 field, enter the IP address of the Cisco VNMC.

f. In the SharedSecret field, enter the shared secret password defined during the Cisco VNMC installation.

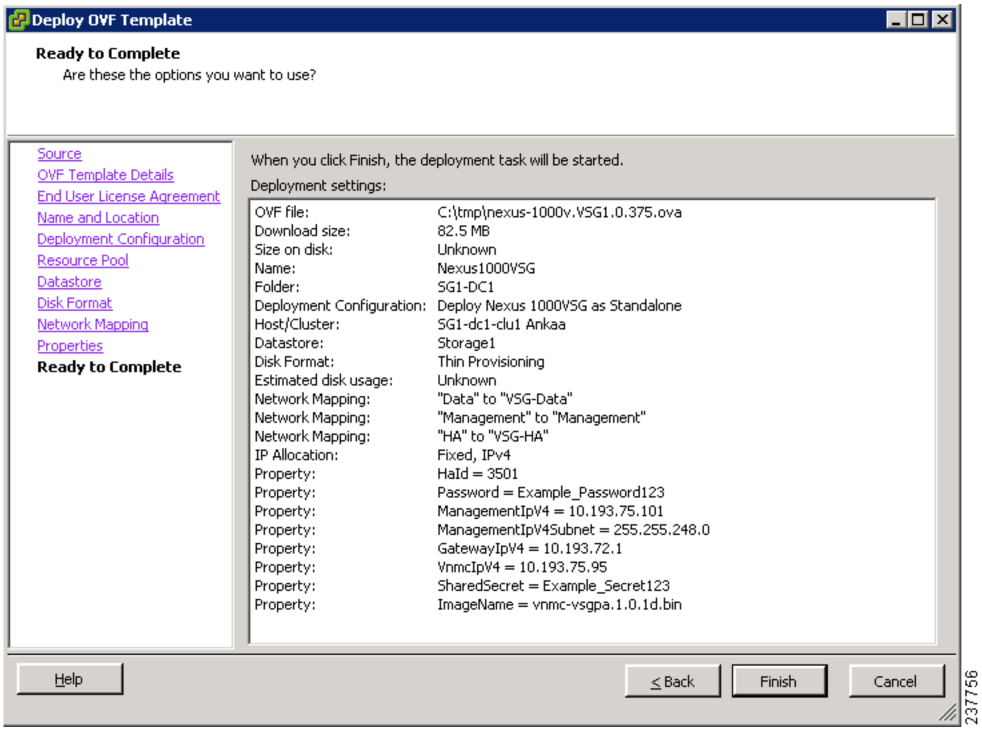
g. In the ImageName field, enter the VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)

Step 16 Click **Next**.

Note 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.

The Ready to Complete window opens. See Figure 2-31.

Figure 2-31 Deploy OVF Template—Ready to Complete Window



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\tmp\nexus-1000v.VSG1.0.375.ova
Download size:	82.5 MB
Size on disk:	Unknown
Name:	Nexus1000VSG
Folder:	SG1-DC1
Deployment Configuration:	Deploy Nexus 1000VSG as Standalone
Host/Cluster:	SG1-dc1-clu1 Ankaa
Datastore:	Storage1
Disk Format:	Thin Provisioning
Estimated disk usage:	Unknown
Network Mapping:	"Data" to "VSG-Data"
Network Mapping:	"Management" to "Management"
Network Mapping:	"HA" to "VSG-HA"
IP Allocation:	Fixed, IPv4
Property:	HaId = 3501
Property:	Password = Example_Password123
Property:	ManagementIpV4 = 10.193.75.101
Property:	ManagementIpV4Subnet = 255.255.248.0
Property:	GatewayIpV4 = 10.193.72.1
Property:	VnmcIpV4 = 10.193.75.95
Property:	SharedSecret = Example_Secret123
Property:	ImageName = vnmc-vsgpa.1.0.1d.bin

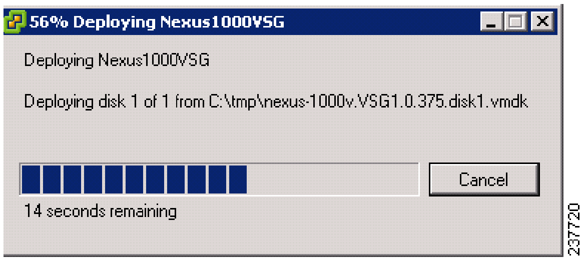
Step 17 Review the deployment settings information and click **Finish**.

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

The Deploying Nexus1000VSG Progress Indicator opens. See Figure 2-32.

The progress bar in Figure 2-32 shows how much of the deployment task is completed before the Cisco VSG is deployed.

Figure 2-32 Deploying Nexus1000VSG—Deploying Disk Files Progress Indicator



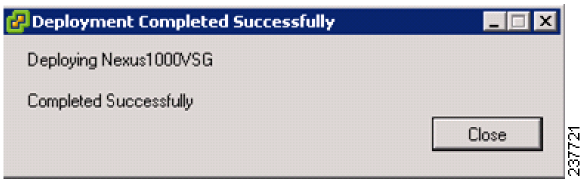
Deploying Nexus1000VSG

Deploying disk 1 of 1 from C:\tmp\nexus-1000v.VSG1.0.375.disk1.vmdk

14 seconds remaining

The progress indicator in Figure 2-33 shows that the deployment has completed successfully.

Figure 2-33 Deployment Completed Successfully Progress Indicator



Deploying Nexus1000VSG

Completed Successfully

Step 18 Click **Close**.

Step 19 Power on the Cisco VSG VM

Task 6—On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy Agent Status

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

PROCEDURE

Step 1 Log in to the Cisco VSG.

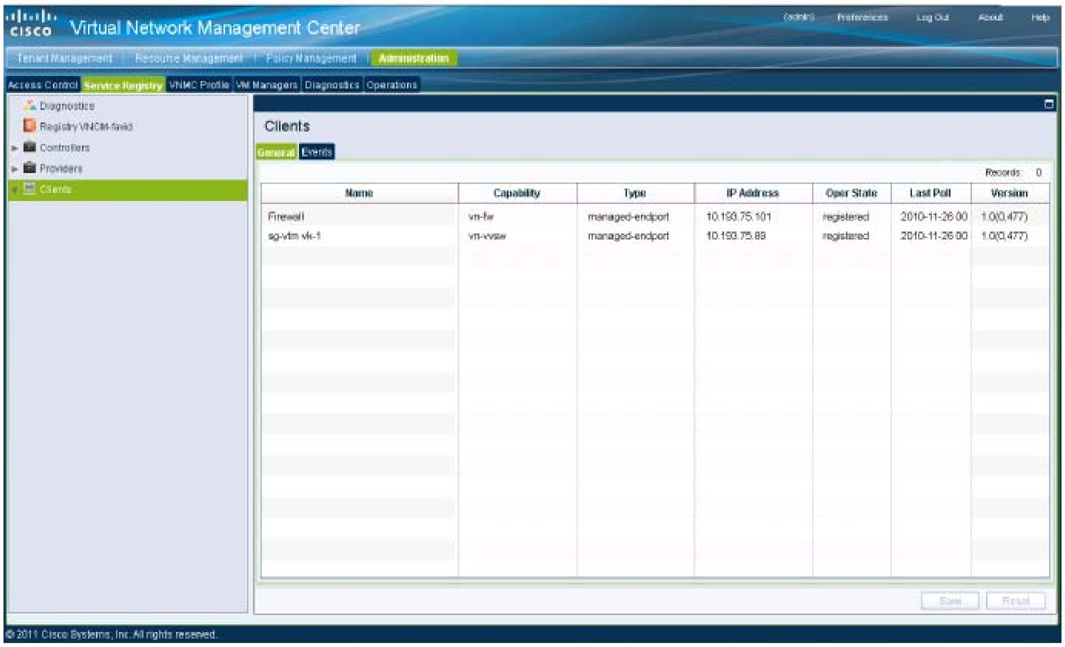
Step 2 Check the status of VNM-PA configuration by entering the following command:

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.0(1j)-vsg
vsg#
```

Step 3 Log in to the Cisco VNMC.

Step 4 Choose **Administration** > **Service Registry** > **Clients** > **General**. The VNMC Administration Service Registry Window opens. See Figure 2-34.

Figure 2-34 VNMC Administration Service Registry Window



Clients

Records: 0

Name	Capability	Type	IP Address	Oper State	Last Poll	Version
Firewall	vn-fw	managed-endport	10.193.75.101	registered	2010-11-26 00	1.0(0.477)
sg-vtm vk-1	vn-vvsw	managed-endport	10.193.75.89	registered	2010-11-26 00	1.0(0.477)

Step 5 In the Clients pane, verify that the Cisco VSG and VSM information is listed.

Task 7—On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall

Now that you have the Cisco VNMC and the Cisco VSG successfully installed with the basic configurations (completed through the OVA File Template wizard), you should configure some of the basic security profiles and policies.

BEFORE YOU BEGIN

Before doing this procedure, know or do the following:

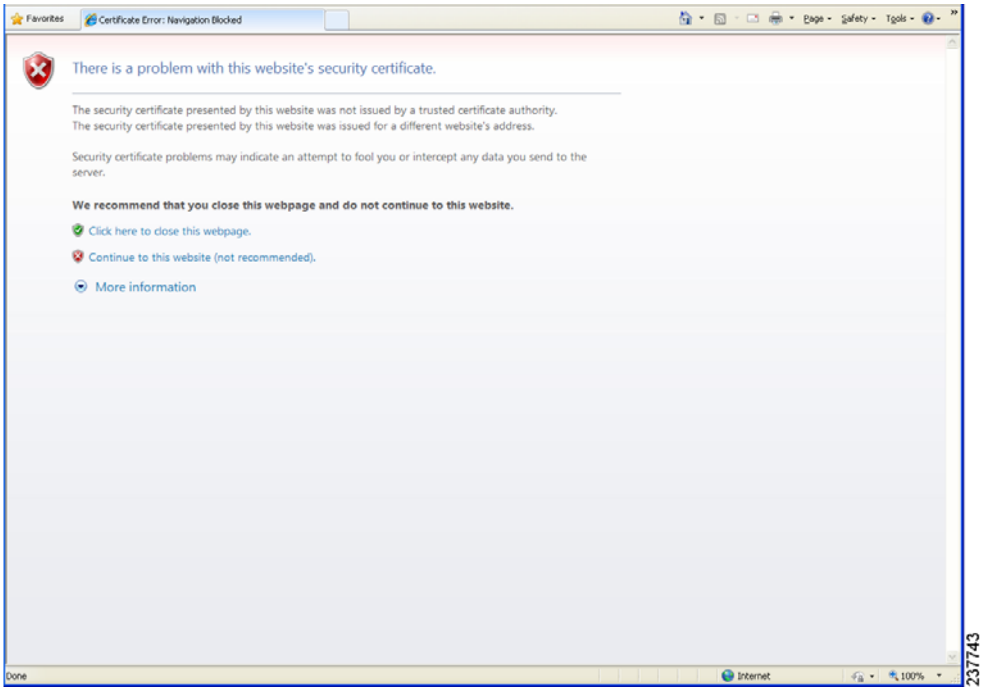
- Install Adobe Flash Player (Version 10.1 or later)
- IP address of the Cisco VNMC
- Admin user password

PROCEDURE

Step 1 For Cisco VNMC access, from your client machine, open Internet Explorer and access https://vnmc-ip/ (https://xxx.xxx.xxx.xxx).

A Website Security Certification window opens. See Figure 2-35.

Figure 2-35 Website Security Certification Window



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

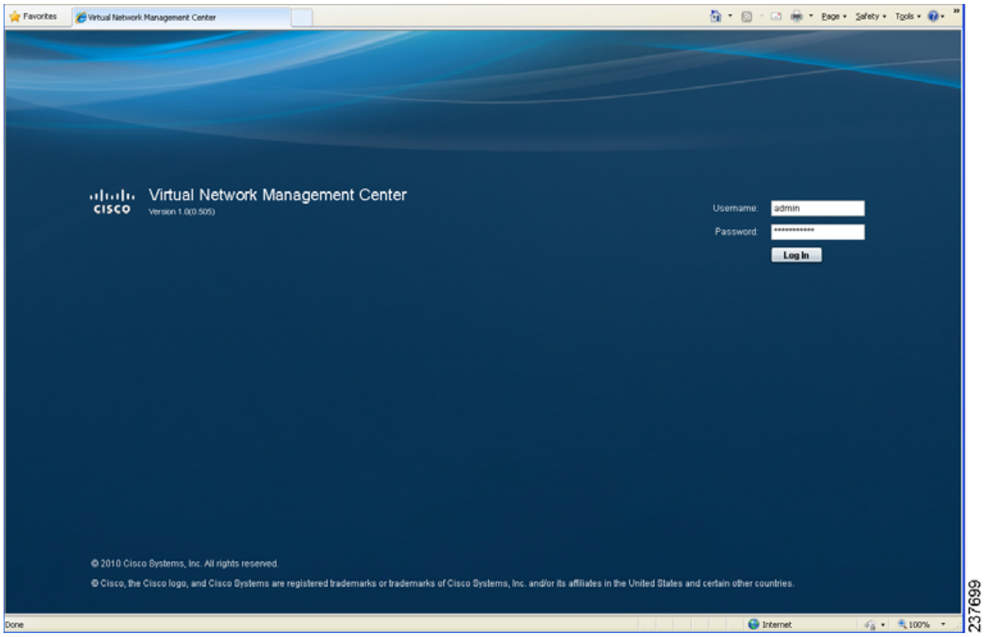
Continue to this website (not recommended).

More information

Step 2 On the certificate warning, click **Continue to this website**.

The Cisco VNMC Access window opens. See Figure 2-36.

Figure 2-36 VNMC Access Window



Virtual Network Management Center
Version 1.0(0.505)

Username: admin
Password: ************

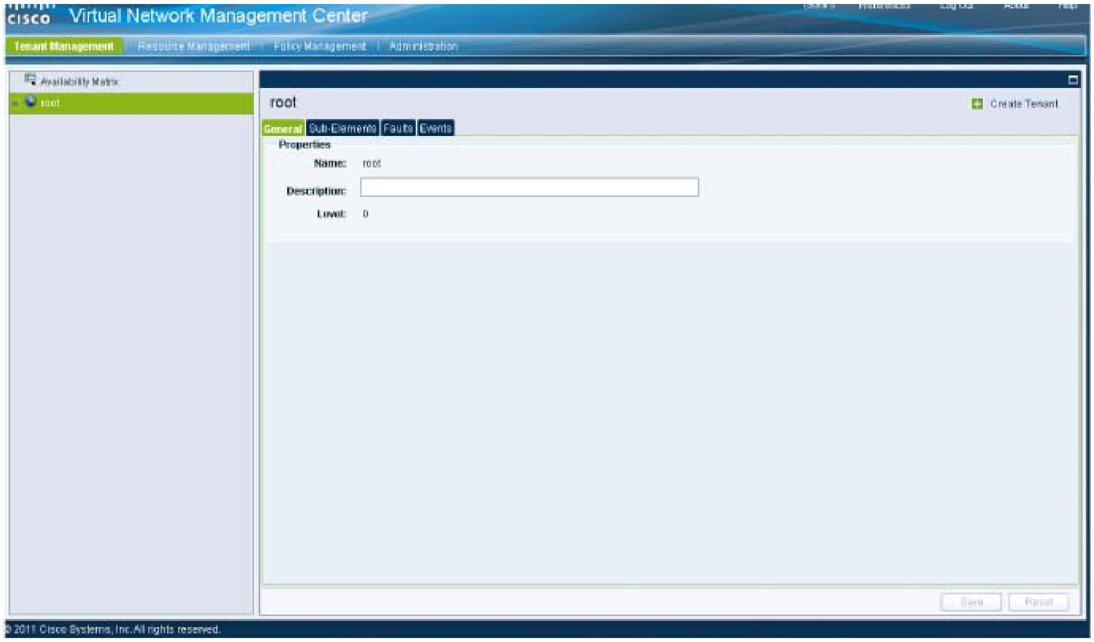
© 2010 Cisco Systems, Inc. All rights reserved.

© Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 3 Log in to the Cisco VNMC with the username “admin” and your password.

Step 4 The Cisco VNMC Main window opens. See Figure 2-37.

Figure 2-37 Cisco Virtual Network Management Center—Opening Page



root

Properties

Name: root

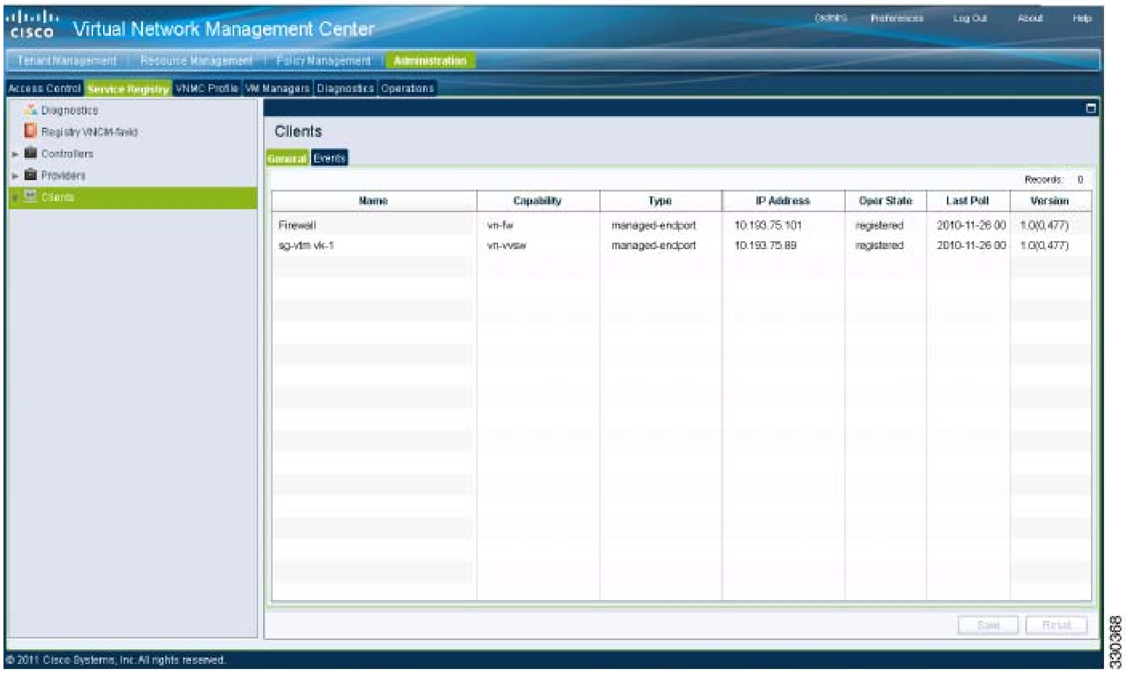
Description:

Level: 0

Step 5 Choose **Administration > Service Registry > Clients** to check the Cisco VSG and VSM registration in the Cisco VNMC.

The Clients pane of the Cisco VNMC opens. See Figure 2-38.

Figure 2-38 VNMC Administration Service Registry Window Clients Pane



Clients

Records: 0

Name	Capability	Type	IP Address	Oper State	Last Poll	Version
Firewall	vn-fw	managed-endpoint	10.193.75.101	registered	2010-11-26 00	1.0(0.477)
sg-vtm vk-1	vn-vvsw	managed-endpoint	10.193.75.89	registered	2010-11-26 00	1.0(0.477)

The Cisco VSG and VSM information should be listed in the Clients pane.

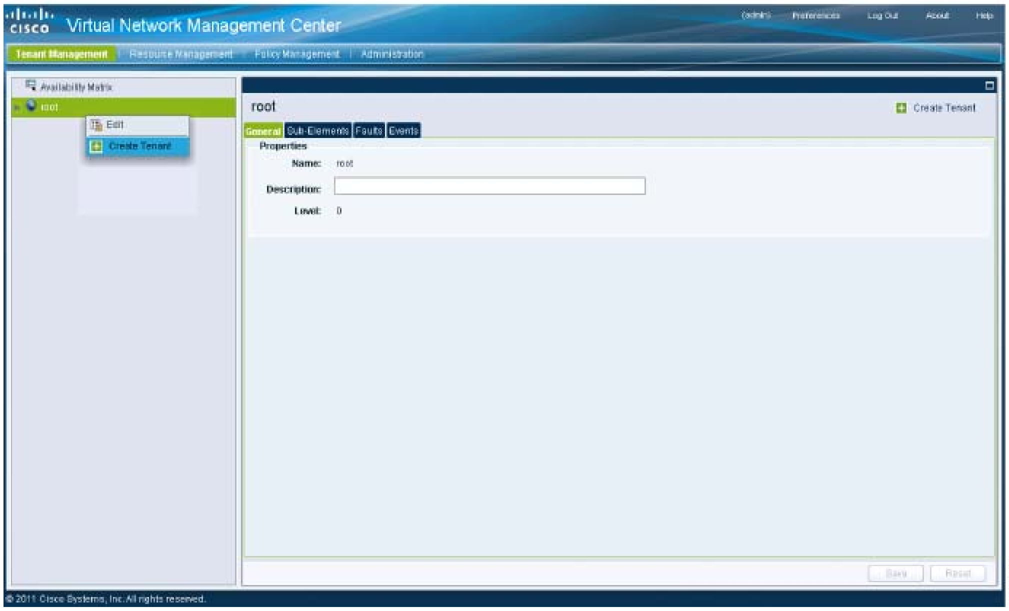
Configuring a Tenant on the Cisco VNMC

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

Step 1 From the Cisco VNMC top toolbar, click the **Tenant Management** tab.

The root pane opens. See Figure 2-39.

Figure 2-39 VNMC Window Tenant Management Tab root Pane



Properties

Name: root

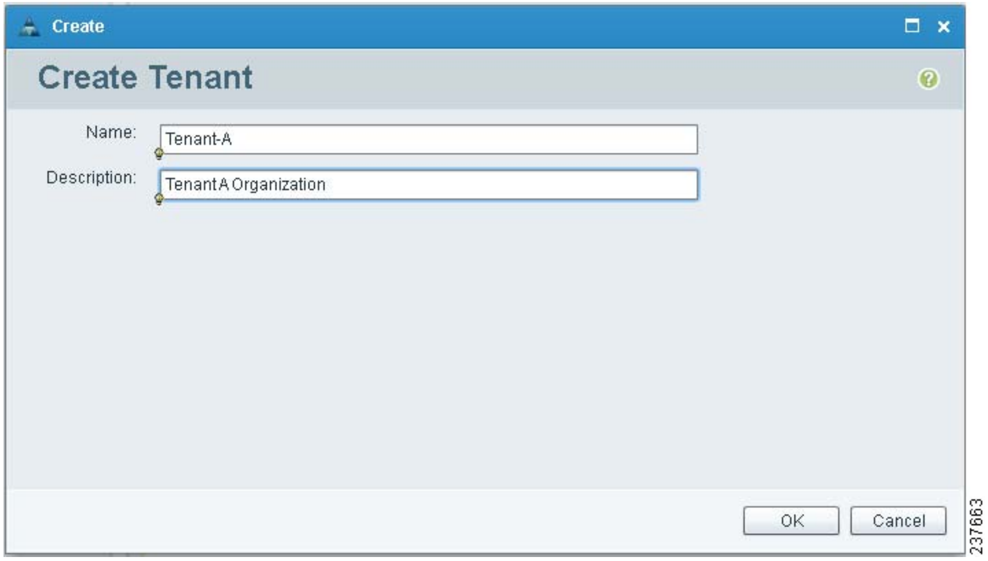
Description:

Level: 0

Step 2 In the left pane directory tree right-click on **Root**, and from the drop-down list, choose **Create Tenant**.

The Create Tenant dialog box opens. See Figure 2-40.

Figure 2-40 Create Tenant Dialog Box



Name: Tenant-A

Description: TenantA Organization

Step 3 Do the following:

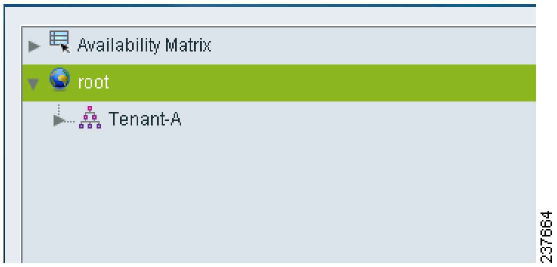
a. In the Name field, enter the tenant name; for example, *Tenant-A*.

b. In the Description field, enter a description for that tenant.

Step 4 Click **OK**.

Notice that the tenant you just created is now listed in the left-side pane under root. See Figure 2-41.

Figure 2-41 Cisco VNMC VSG Configuration Directory Tree Pane



Configuring a Security Profile on the Cisco VNMC

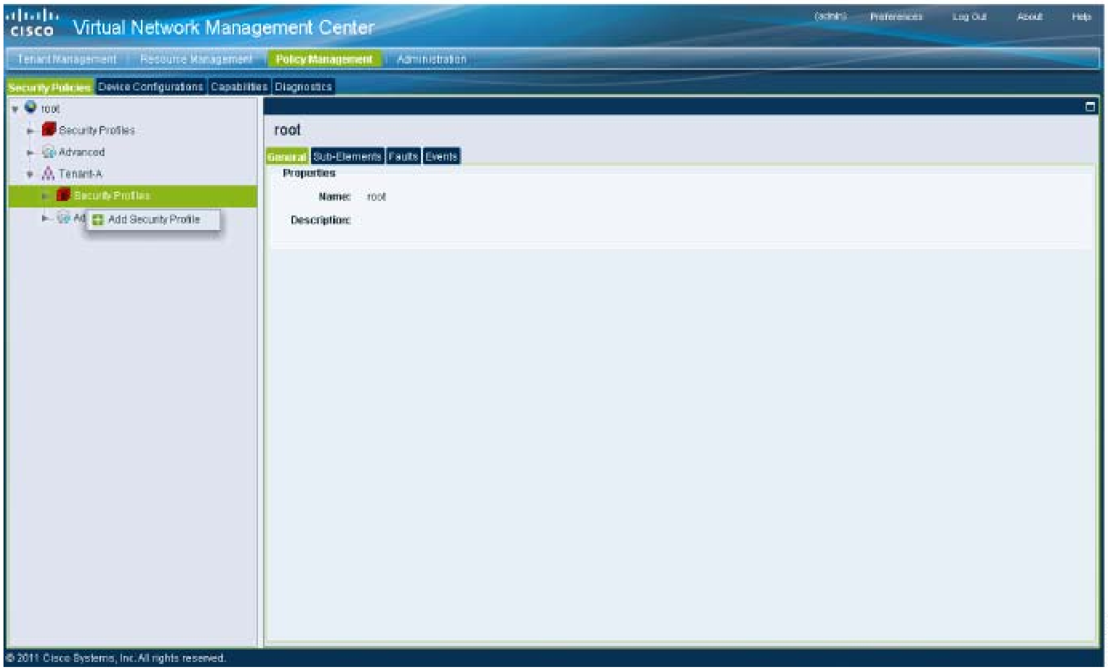
You can configure a security profile on the Cisco VNMC.

PROCEDURE

Step 1 In the Cisco VNMC top row toolbar, click the **Policy Management** tab.

The Policy Management Security Policies window opens. See Figure 2-42.

Figure 2-42 VNMC Policy Management Security Policies Window



root

Properties

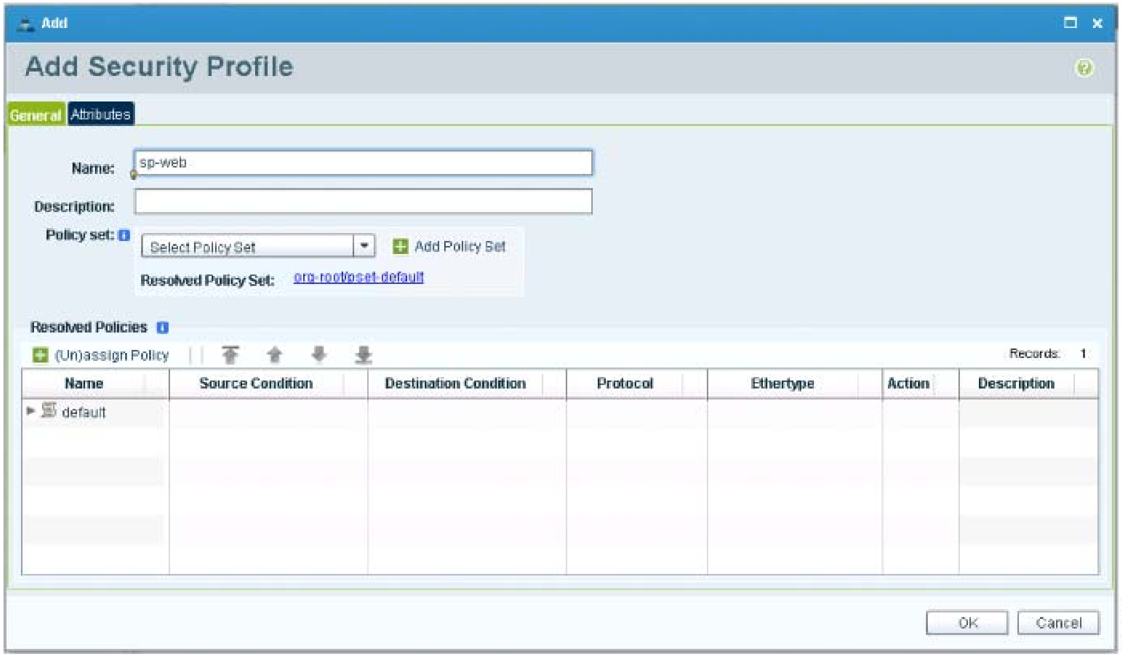
Name: root

Description:

Step 2 From the directory path, choose **Security Policies** > **root** > **Tenant-A** > **Security Profiles**. Right-click in an empty space and from the drop-down list, choose **Add Security Profile**.

The Add Security Profile dialog box opens. See Figure 2-43.

Figure 2-43 Add Security Profile Dialog Box



Name: sp-web

Description:

Policy set: Select Policy Set

Resolved Policy Set: org-root/pset-default

Resolved Policies

Records: 1

Name	Source Condition	Destination Condition	Protocol	Ethertype	Action	Description
default						

Step 3 Do the following:

a. In the Name field, enter a name for the security profile; for example, *sp-web*.

b. In the Description field, enter a brief description of this security profile.

Step 4 Click **OK**.

Configuring a Compute Firewall on the Cisco VNMC,

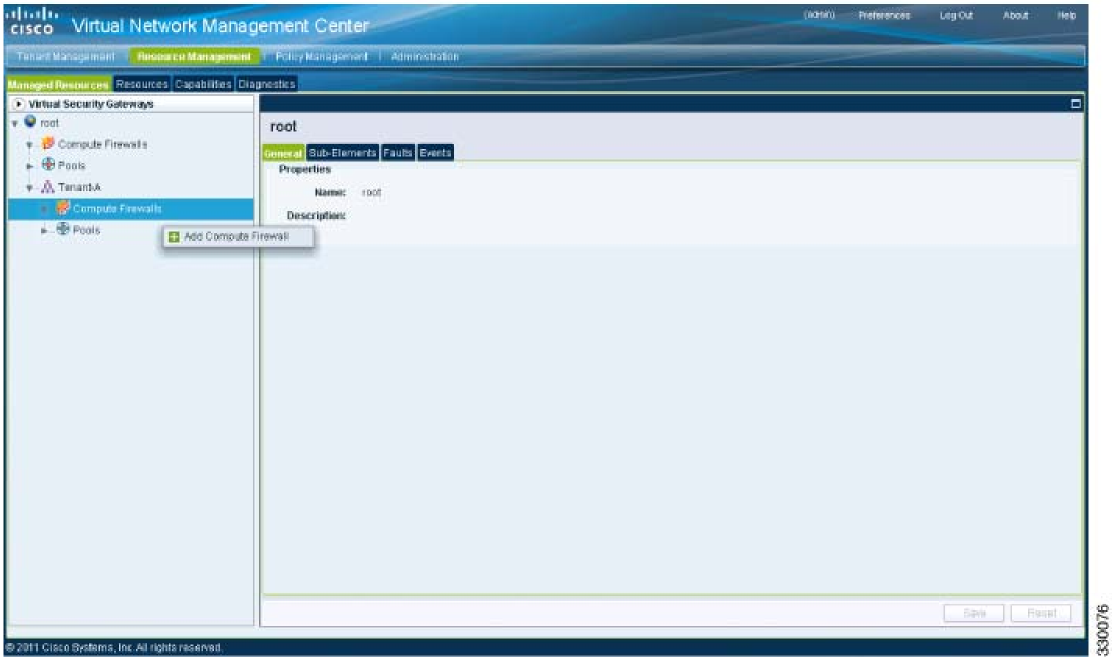
The compute firewall is a logical virtual entity that contains the device profile that you can bind (assign) to a Cisco VSG virtual machine. The device policy in the device profile is then pushed from the Cisco VNMC to the Cisco VSG. Once this is complete, the compute firewall is in the *applied* configuration state on the Cisco VNMC.

PROCEDURE

Step 1 From the Cisco VNMC, choose **Resource Management** > **Managed Resources**.

The VNMC Resource Management, Managed Resources, Firewall Profiles window opens. See Figure 2-44.

Figure 2-44 VNMC Resource Management, Managed Resources, Firewall Profiles Window



Name: root

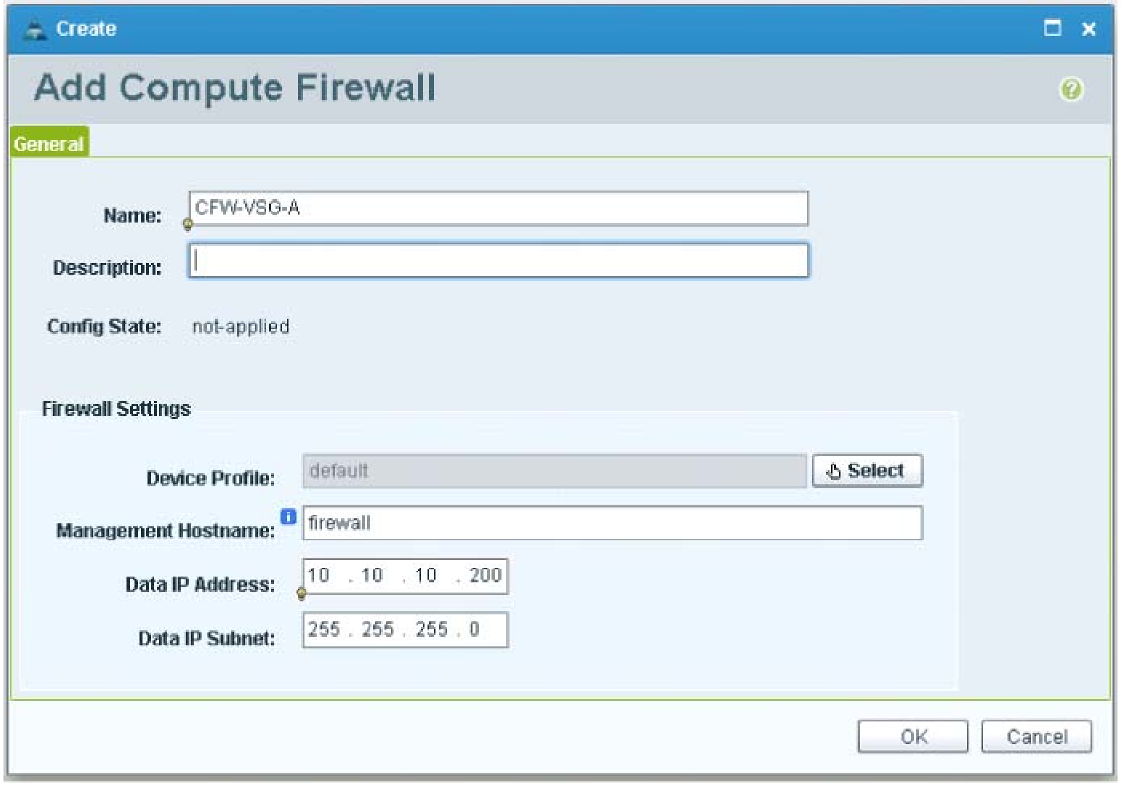
Description:

Step 2 On the left-pane directory tree, choose **root > Tenant-A > Compute Firewall**.

Step 3 From the drop-down list, choose **Add Compute Firewall**.

The Add Compute Firewall dialog box opens. See Figure 2-45.

Figure 2-45 Add Compute Firewall Dialog Box



Name: CFW-VSG-A

Description:

Config State: not-applied

Firewall Settings

Device Profile: default

Management Hostname: firewall

Data IP Address: 10 . 10 . 10 . 200

Data IP Subnet: 255 . 255 . 255 . 0

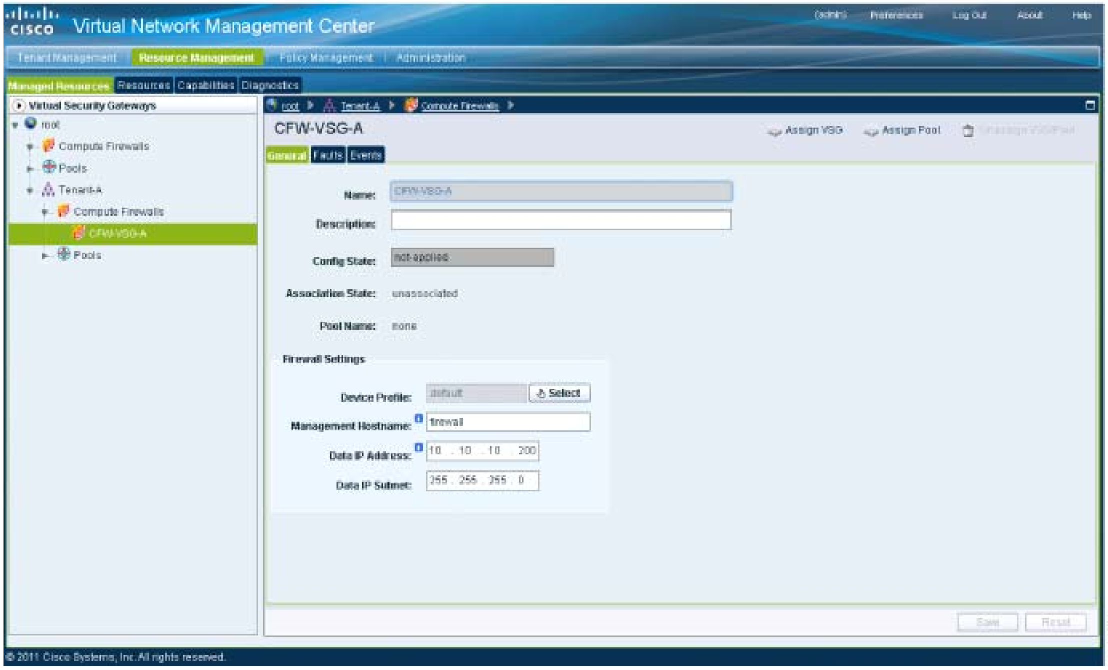
Step 4 In the Add Compute Firewall dialog box, do the following:

- In the Name field, enter a name for the compute firewall.
- In the Description field, enter a brief description of the compute firewall.
- In the Management Hostname field, enter the name for your Cisco VSG.
- In the Data IP Address field, enter the data IP address, if it is different from what is the default.

Step 5 Click **OK**.

The new Compute Firewall pane displays with the information that you provided. See Figure 2-46.

Figure 2-46 Compute Firewall Pane



CFW-VSG-A

Name: CFW-VSG-A

Description:

Config State: not-applied

Association State: unassociated

Pool Name: none

Firewall Settings

Device Profile: default

Management Hostname: firewall

Data IP Address: 10 . 10 . 10 . 200

Data IP Subnet: 255 . 255 . 255 . 0

Task 8—On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall

The compute firewall is a logical virtual entity that contains the device profile that can be later bound to the device for communication with the Cisco VNMC and VSM.

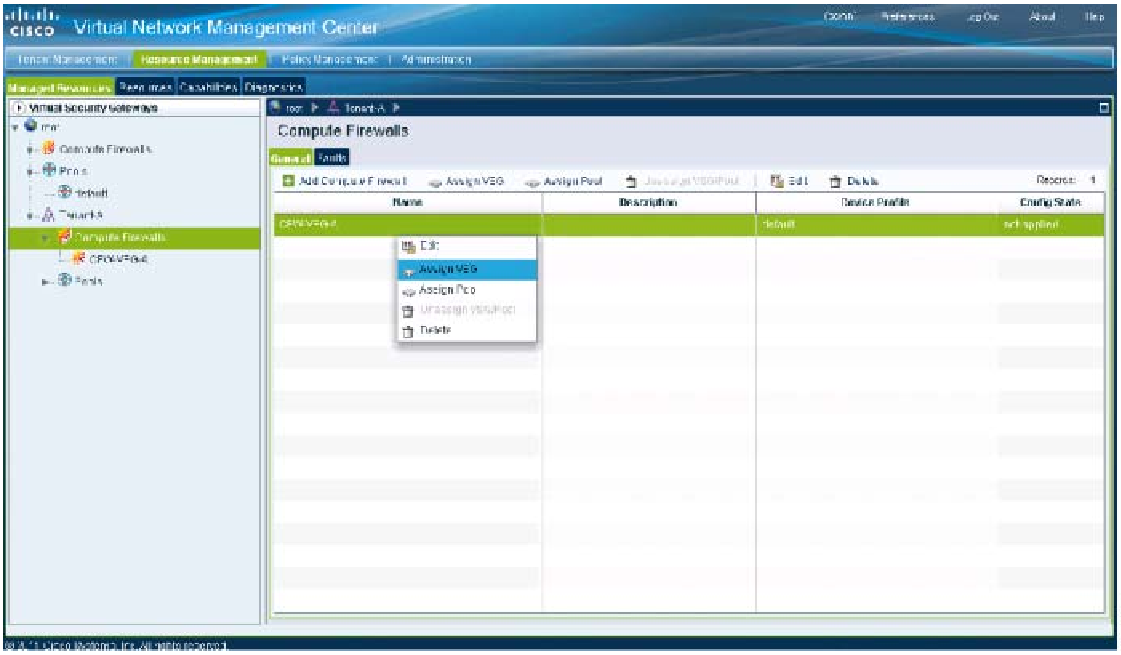
You can assign the Cisco VSG to the compute firewall on the Cisco VNMC.

PROCEDURE

Step 1 Choose **Resource Management** > **Managed Resources**.

The VNMC Resource Management Managed Resources Compute Firewalls window opens. See Figure 2-47.

Figure 2-47 VNMC Resource Management Managed Resources Compute Firewalls Window

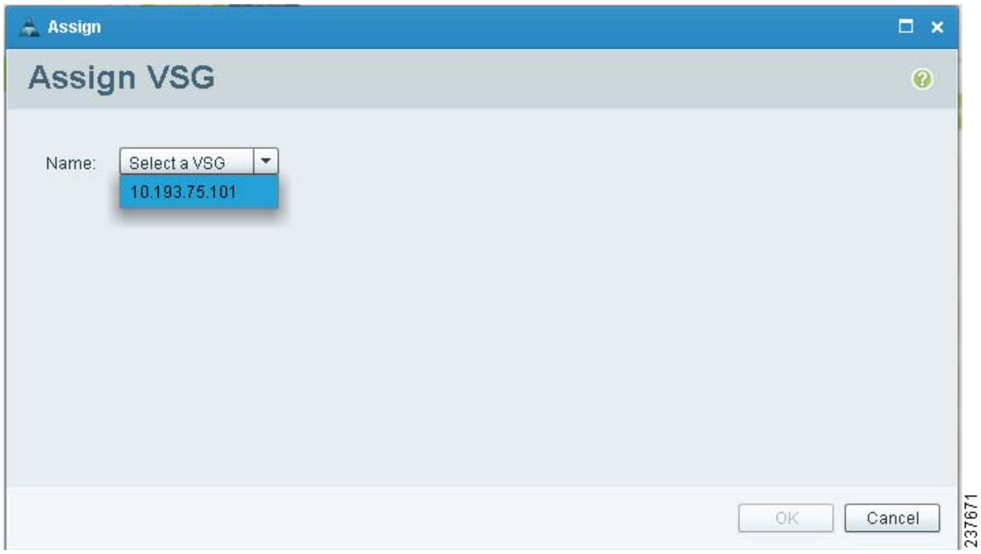


Step 2 Choose **root > Tenant-A > Compute Firewalls**.

Step 3 Right-click **Compute Firewalls**, and from the drop-down list, choose **Assign VSG**.

The Assign VSG dialog box opens. See Figure 2-48.

Figure 2-48 Assign VSG Dialog Box



Step 4 From the Name drop-down list, choose the Cisco VSG IP address.

Step 5 Click **OK**.

Note The Config State status changes from “not-applied” to “applying” and then to “applied.”

Task 9—On the Cisco VNMC, Configuring a Permit-All Rule

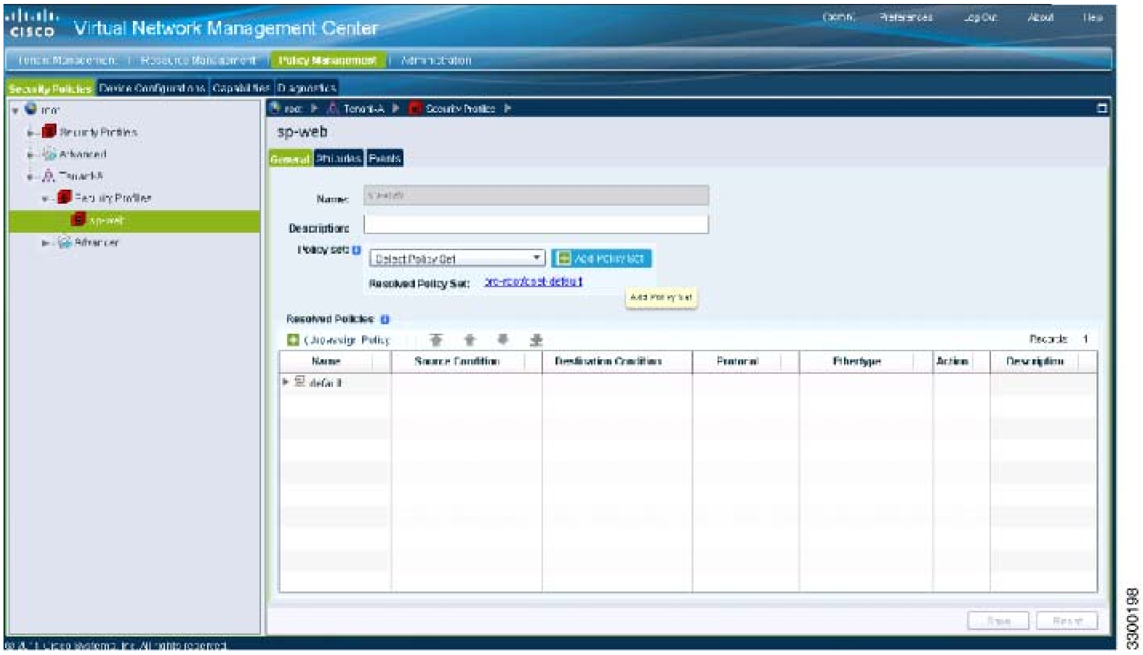
You can configure a permit-all rule in the Cisco VNMC.

PROCEDURE

Step 1 Log in to the Cisco VNMC and choose **Policy Management** > **Security Policies**.

The Cisco VNMC Policy Management Security Policies window opens. See Figure 2-49.

Figure 2-49 Cisco Virtual Network Management Center—Policy Management Security Policies Window

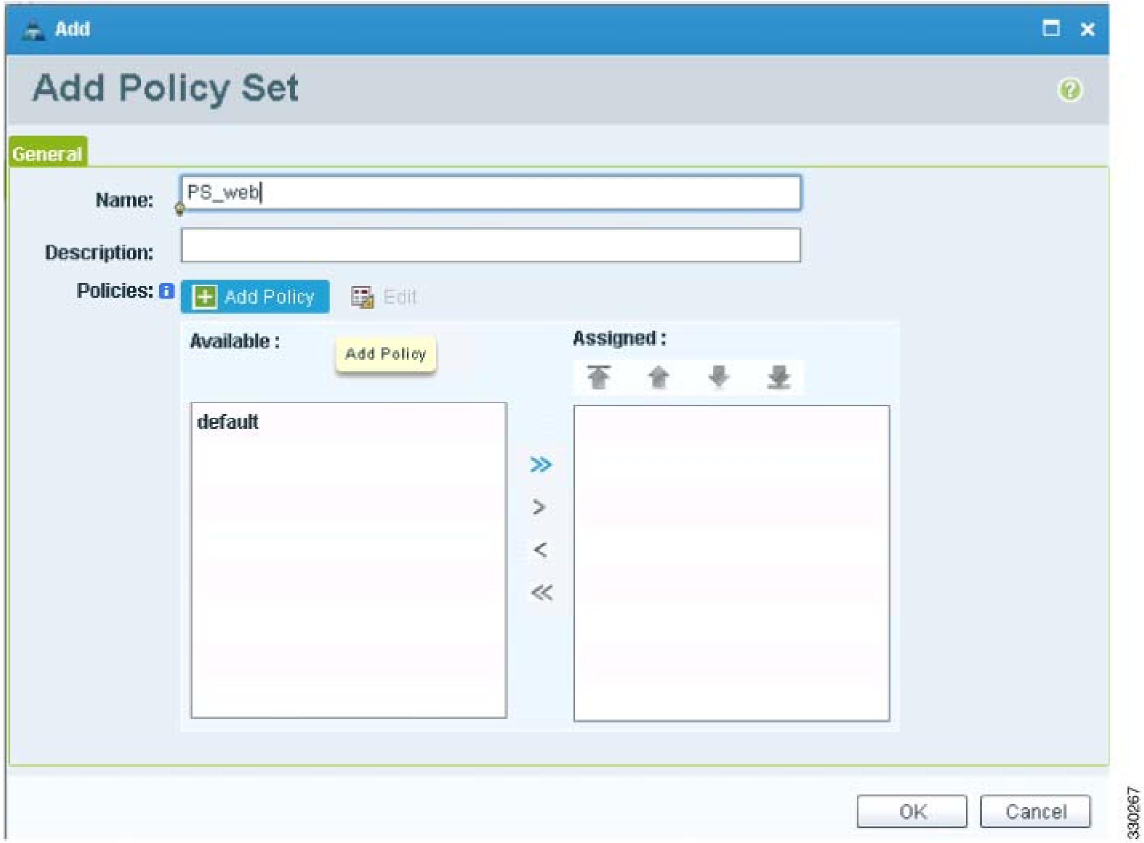


Step 2 Choose **root > Tenant-A > Security-Profile > sp-web**.

Step 3 From the button to the right of the sp-web pane Policy sets field, click **Add policy set**.

The Add Policy Set dialog box opens. See Figure 2-50.

Figure 2-50 Add Policy Set Dialog Box



Name: PS_web

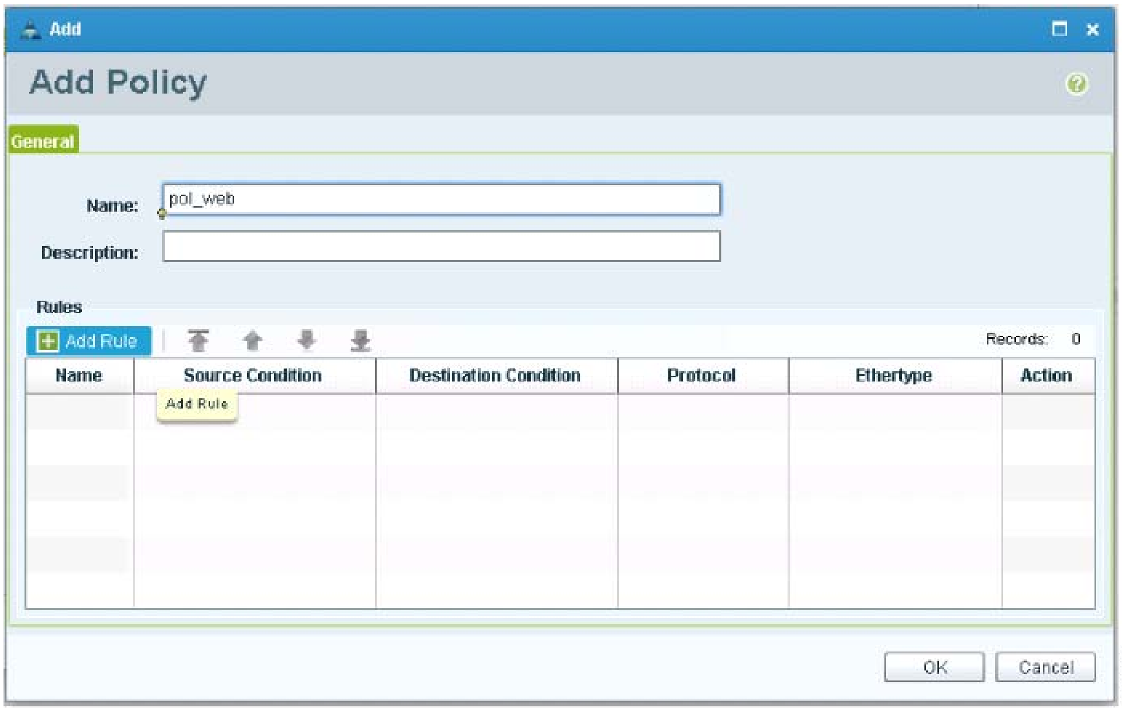
Description:

Policies:

default

Step 4 Click **Add Policy**. The Add Policy dialog box appears. See Figure 2-51.

Figure 2-51 Add Policy Dialog Box



Add Policy

Name: pol_web

Description:

Name	Source Condition	Destination Condition	Protocol	Ethertype	Action

Step 5 Do the following:

a. In the Name field, enter the security policy name.

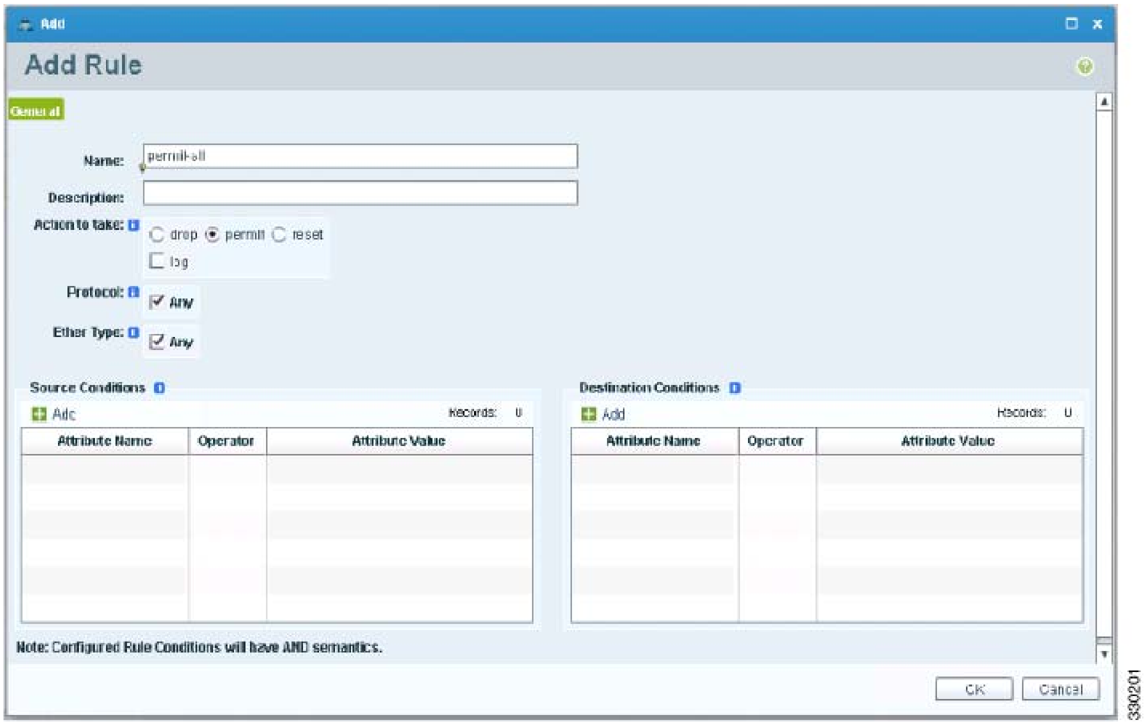
b. In the Description field, enter a brief description of the security policy.

c. Above the Name column, click **Add Rule**.

The Add Rule dialog box displays. See Figure 2-52.

Send document comments to vsg-docfeedback@cisco.com

Figure 2-52 VNMC Add Rule Dialog Box



Add

Add Rule

General

Name: permit-all

Description:

Action to take: ○ drop ● permit ○ reset

□ log

Protocol: ☑ Any

Ether Type: ☑ Any

Source Conditions

Add Records: 0

Attribute Name	Operator	Attribute Value

Destination Conditions

Add Records: 0

Attribute Name	Operator	Attribute Value

Note: Configured Rule Conditions will have AND semantics.

Step 6 In the Name field, enter the rule name.

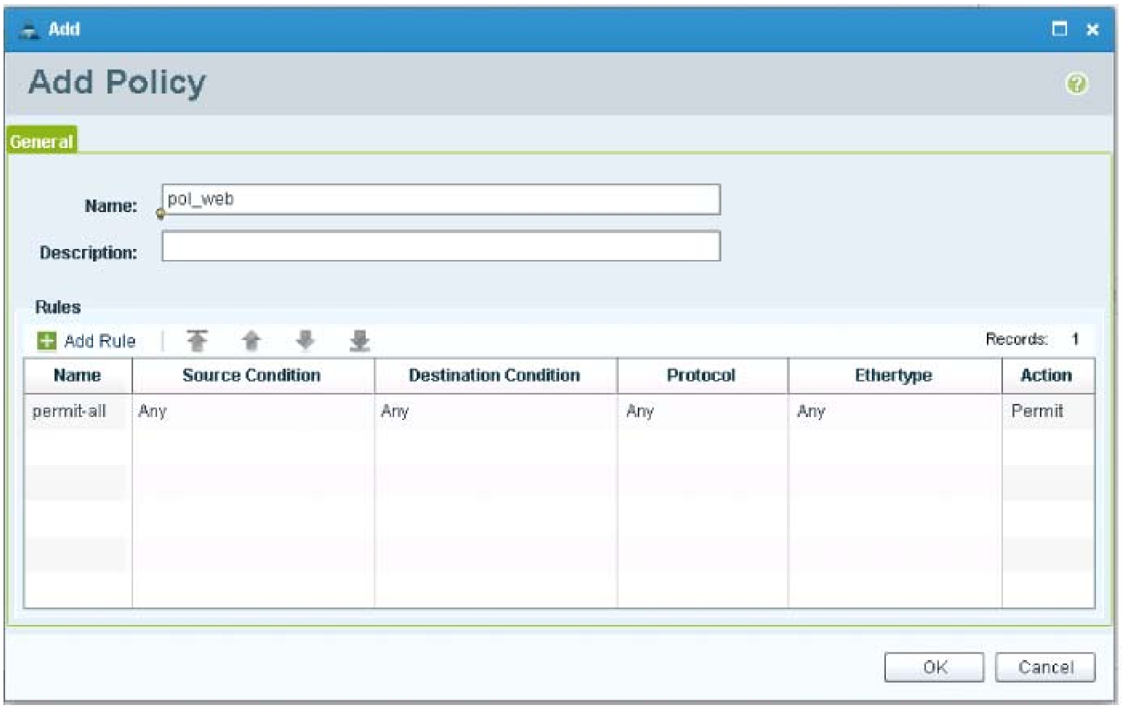
Step 7 In the Description field, enter a brief description of the rule.

Step 8 From the Action to Take buttons, choose the rule action that you want this rule to have; in this case, **permit**.

Step 9 Click **OK** in this Add Rule dialog box.

The Add Policy dialog box reappears showing a policy with the new rule. See Figure 2-53.

Figure 2-53 VNMC Add Policy Dialog Box



Add Policy

General

Name: pol_web

Description:

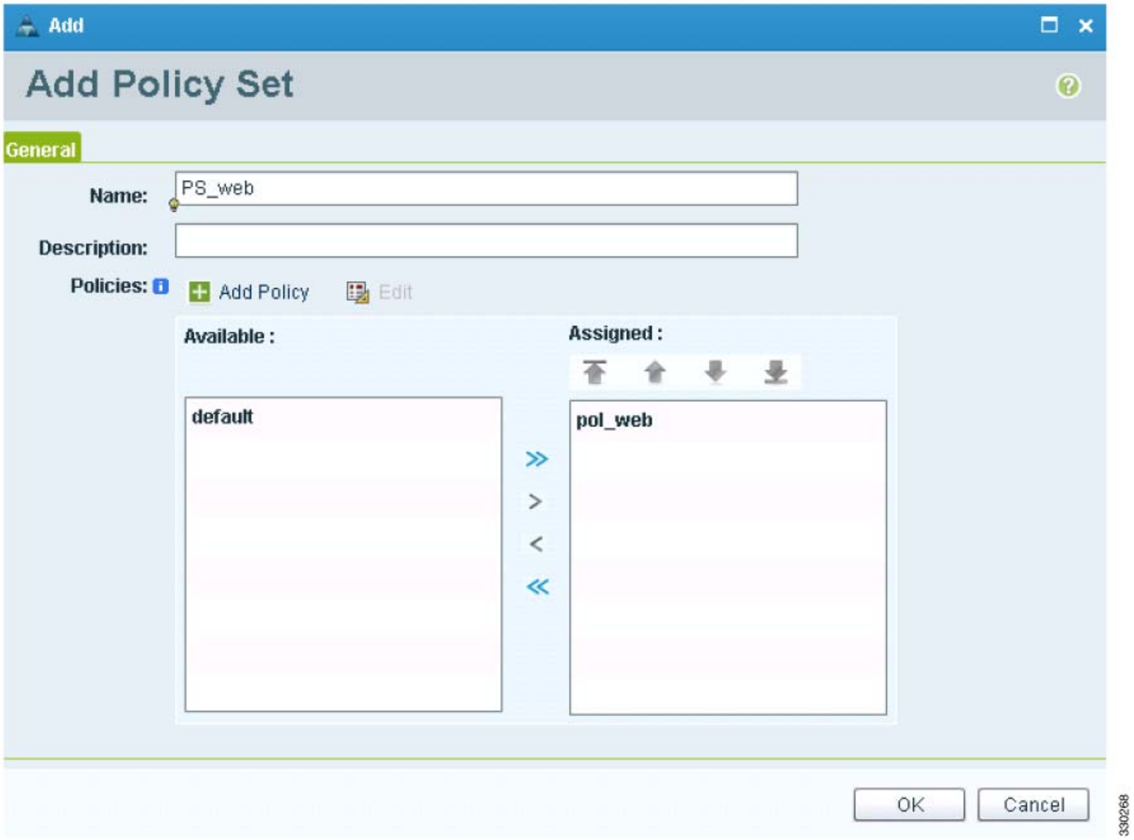
Rules

Name	Source Condition	Destination Condition	Protocol	Ethertype	Action
permit-all	Any	Any	Any	Any	Permit

Step 10 Click **OK** in the Add Policy dialog box.

Step 11 Click **OK** in the Add Policy Set dialog box. The newly created policy is displayed in the Assigned: field. See Figure 2-54.

Figure 2-54 Add Policy Set Dialog Box



Name: PS_web

Description:

Policies:

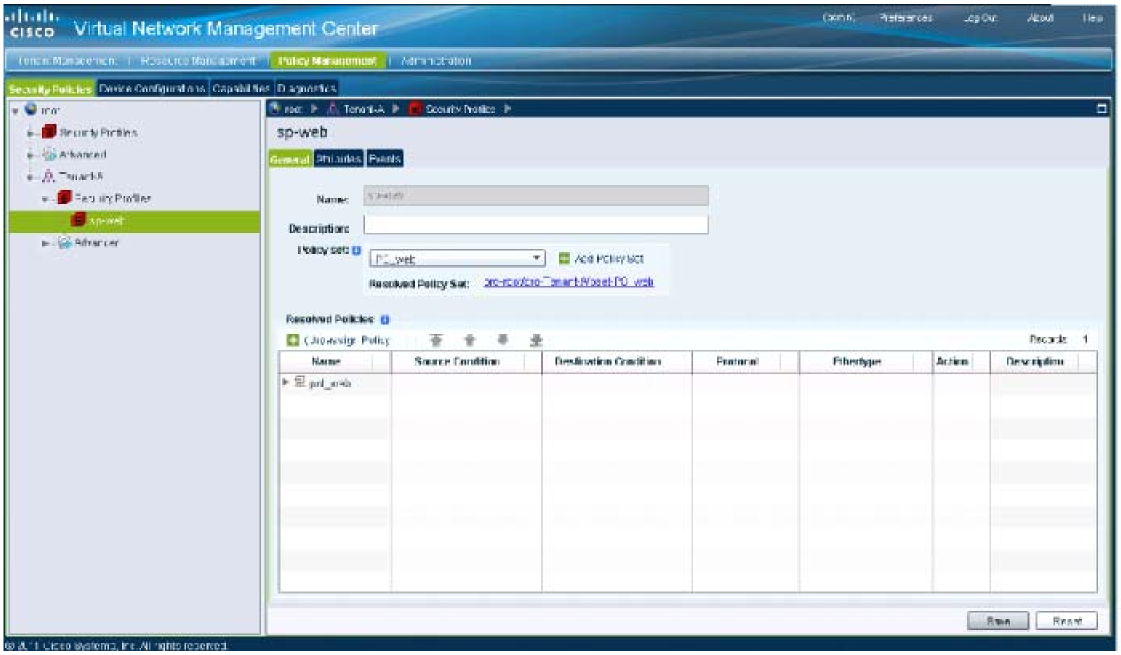
Available: default

Assigned: pol_web

Step 12 Click **OK** in the Add Policy Set dialog box.

Step 13 Click **Save** in the Security Profile window. See Figure 2-55.

Figure 2-55 Cisco Virtual Network Management Center—Policy Management Window



Task 10—On the Cisco VSG, Verifying the Permit-All Rule

To verify the rule presence in the Cisco VSG, use the Cisco VSG CLI and the **show** commands.

PROCEDURE

Step 1 Log in to the Cisco VSG and enter the following commands:

```
vsg# show running-config | begin security
security-profile default@root
  policy default@root
  custom-attribute vnsporg "root"

security-profile sp-web@root/Tenant-A
  policy PS_web@root/Tenant-A
  custom-attribute vnsporg "root/Tenant-A"
rule default/default-rule@root
  action 10 drop
rule pol_web/permit-all@root/Tenant-A
  action 10 log
  action 11 permit
policy default@root
  rule default/default-rule@root order 2
policy PS_web@root/Tenant-A
  rule pol_web/permit-all@root/Tenant-A order 101
```

Task 11—Enabling Logging

This section includes the following topics:

- Enabling Logging Level 6 for Policy-Engine Logging, page 2-52
- Enabling Global Policy-Engine Logging, page 2-55

Enabling Logging Level 6 for Policy-Engine Logging

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

You can enable Logging Level 6 for policy-engine logging in a monitor session.

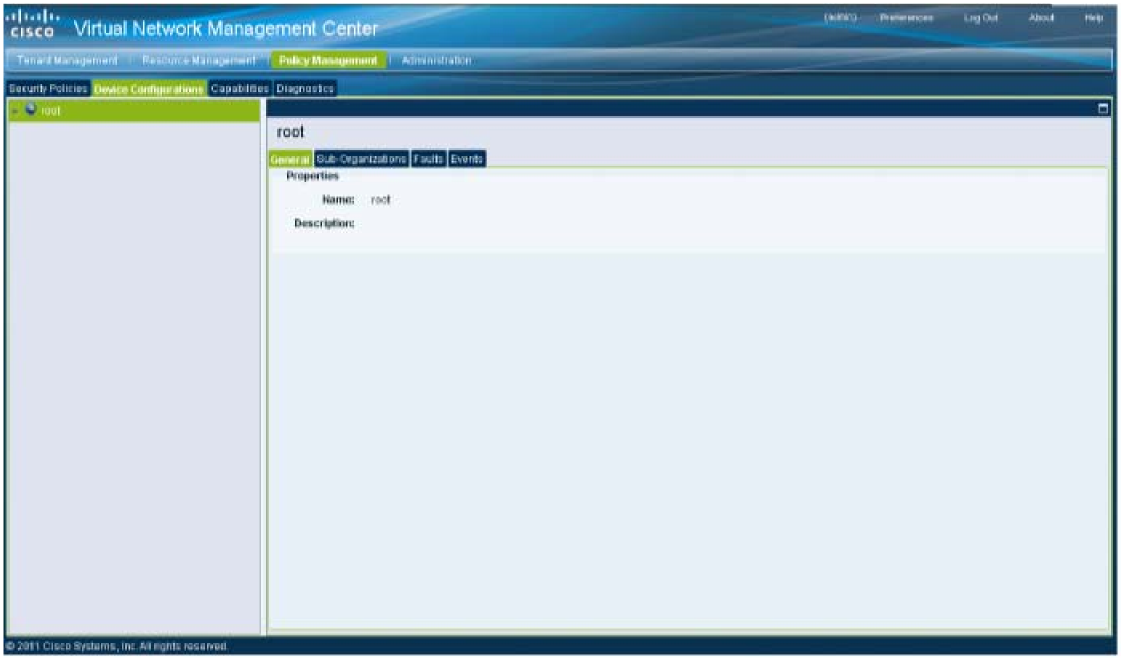
PROCEDURE

Step 1 Log in to the Cisco VNMC.

Step 2 Choose **Policy Management** > **Device Configurations**.

The Device Configuration window opens, See Figure 2-56.

Figure 2-56 Cisco Virtual Network Management Center—Device Configurations Window



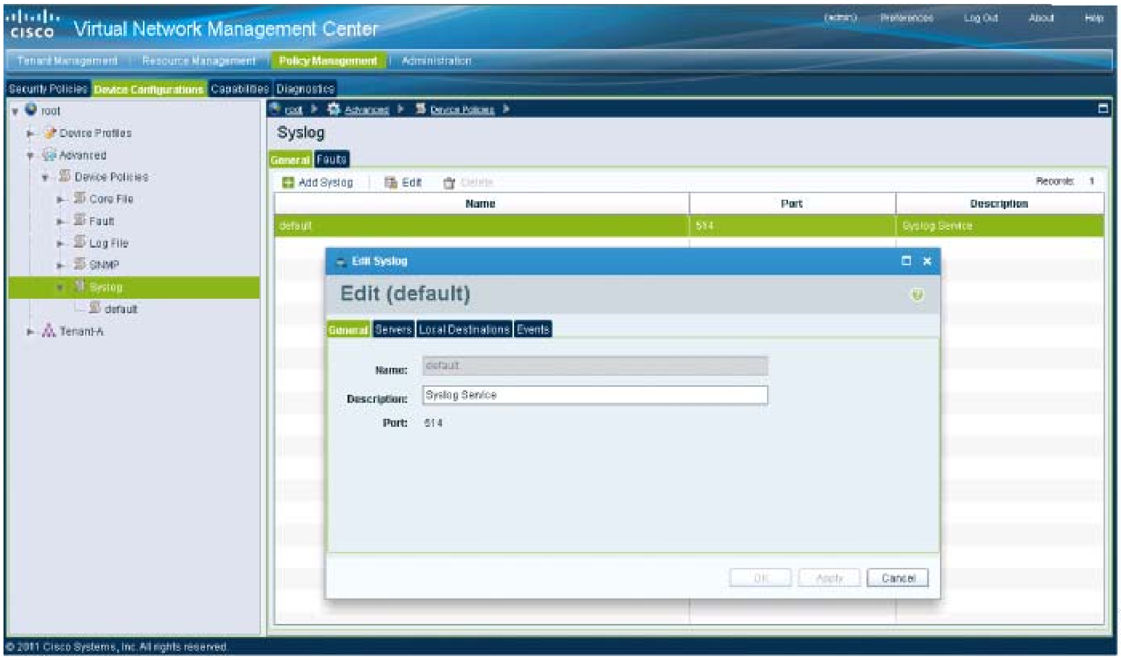
Name: root
Description:

Step 3 From the left pane navigation tree, choose **root** > **Advanced** > **Device Policies** > **Syslog**.

Step 4 From the Syslog pane on the right, choose **Default** and click **Edit**.

The Edit Syslog dialog box opens, see Figure 2-57.

Figure 2-57 Cisco Virtual Network Management Center Syslog Pane Edit Syslog Dialog Box


Virtual Network Management Center
(admin) Preferences Log Out About Help
Tenant Management Resource Management Policy Management Administration
Security Policies Device Configurations Capabilities Diagnostics
root
Device Profiles
Advanced
Device Policies
Core File
Fault
Log File
SNMP
Syslog
default
Tenant-A
root Advanced Device Policies
Syslog
General Faults
Add Syslog Edit Delete
Records: 1
Edit Syslog
Edit (default)
General Servers Local Destinations Events
OK Apply Cancel
© 2011 Cisco Systems, Inc. All rights reserved.
330321

Name	Port	Description
default	514	Syslog Service

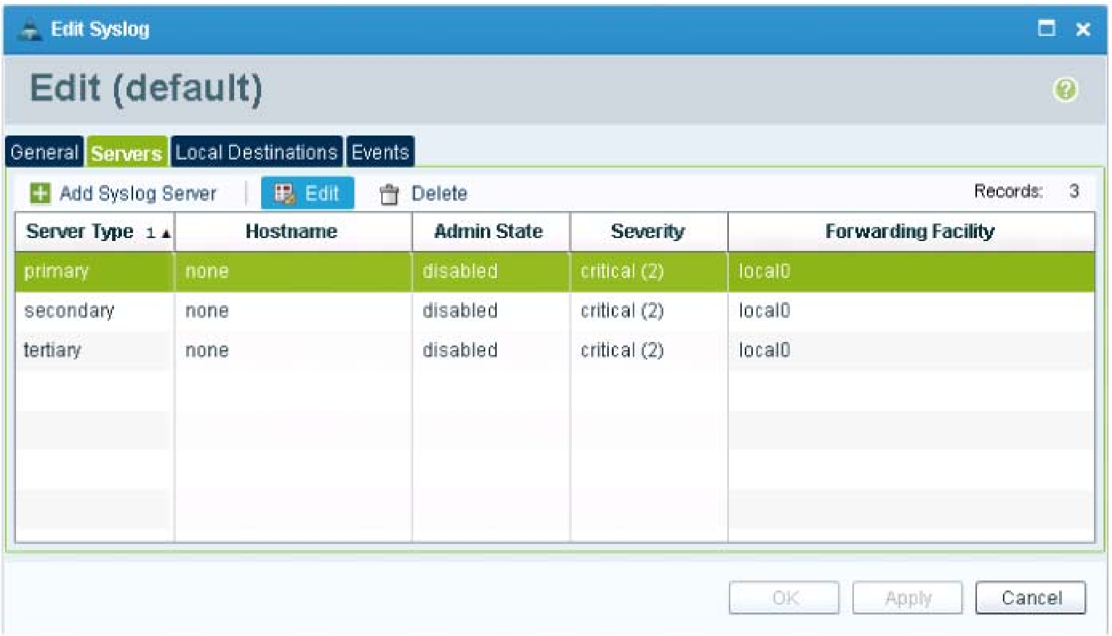
Name: default

Description: Syslog Service

Port: 514

Step 5 Click **Servers** tab. See Figure 2-58.

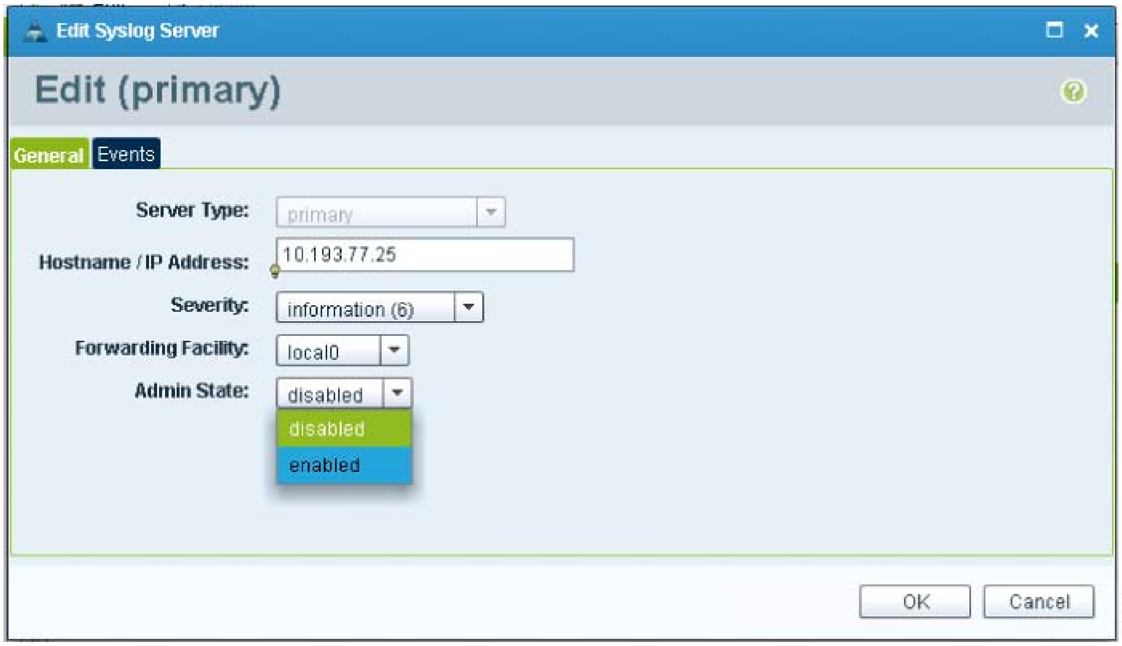
Figure 2-58 Cisco Virtual Network Management Center Edit Syslog Dialog Box


Edit Syslog
Edit (default)
General Servers Local Destinations Events
Add Syslog Server Edit Delete
Records: 3
OK Apply Cancel
330336

Server Type 1 ▲	Hostname	Admin State	Severity	Forwarding Facility
primary	none	disabled	critical (2)	local0
secondary	none	disabled	critical (2)	local0
tertiary	none	disabled	critical (2)	local0

Step 6 From the Server Type column, choose the primary server type from the displayed list and from the pane toolbar, click **Edit**. See Figure 2-59.

Figure 2-59 Edit Syslog Server Dialog Box



Server Type: primary

Hostname / IP Address: 10.193.77.25

Severity: information (6)

Forwarding Facility: local0

Admin State: disabled

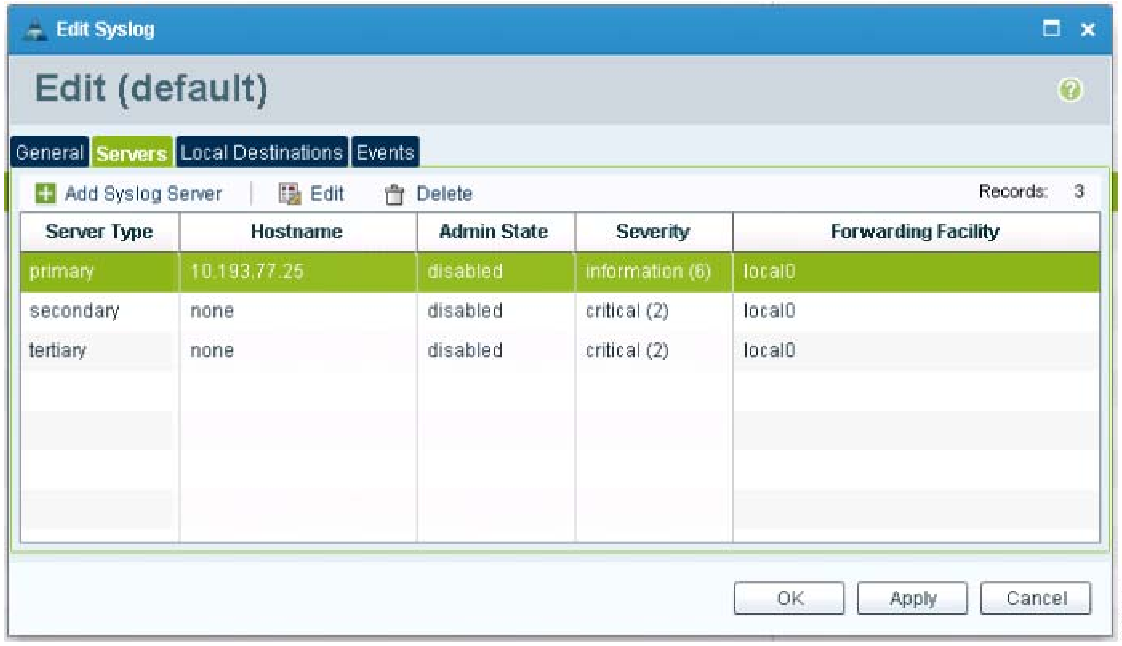
Step 7 In the Hostname/IP address field, enter the syslog server IP address.

Step 8 From the Severity drop-down list, choose **Information(6)**.

Step 9 From the Admin State drop-down list, choose **Enabled**.

Step 10 Click **OK**. See Figure 2-60.

Figure 2-60 Edit Syslog Dialog Box



Records: 3

Server Type	Hostname	Admin State	Severity	Forwarding Facility
primary	10.193.77.25	disabled	information (6)	local0
secondary	none	disabled	critical (2)	local0
tertiary	none	disabled	critical (2)	local0

Step 11 Click **OK**.

Enabling Global Policy-Engine Logging

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

You can enable global policy-engine logging.

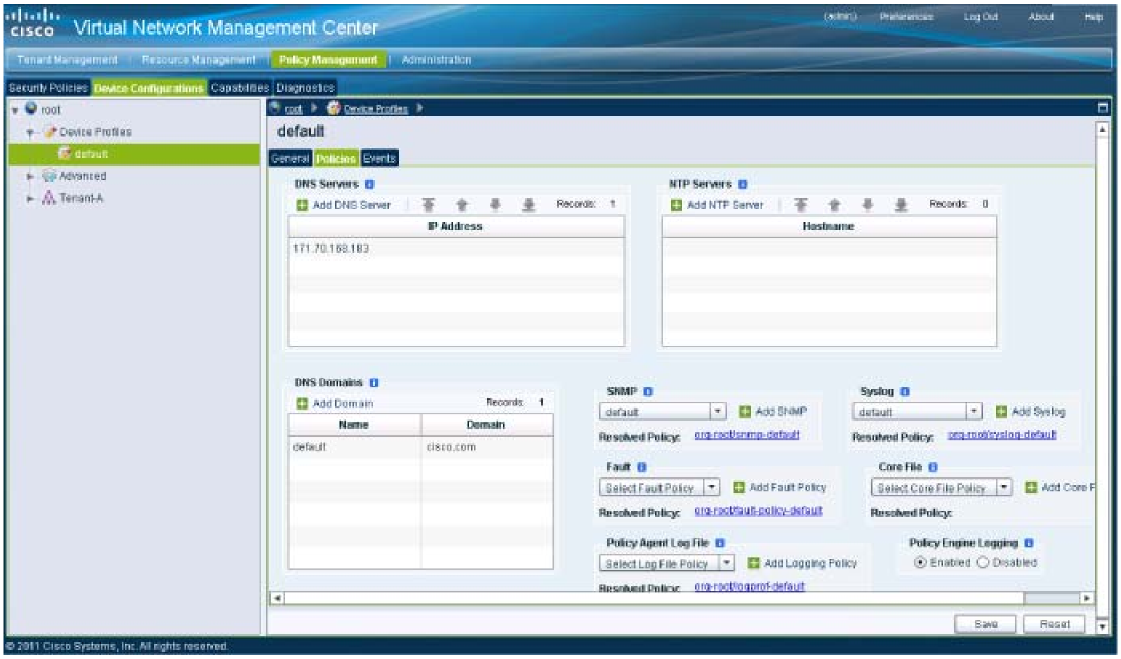
PROCEDURE

Step 1 Log in to the Cisco VNMC and choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles** > **default**.

The Cisco VNMC Policy Management window opens.

Step 2 In the Device Profiles pane, choose **Policies**. See Figure 2-61.

Figure 2-61 Cisco Virtual Network Management Center Policy Management Device Configurations Profiles Pane



default

DNS Servers Records: 1

IP Address
171.70.168.183

NTP Servers Records: 0

Hostname

DNS Domains Records: 1

Name	Domain
default	cisco.com

SNMP: default
Resolved Policy: org-root/snmp-default

Syslog: default
Resolved Policy: org-root/syslog-default

Fault: Select Fault Policy
Resolved Policy: org-root/fault-policy-default

Core File: Select Core File Policy
Resolved Policy:

Policy Agent Log File: Select Log File Policy
Resolved Policy: org-root/logprof-default

Policy Engine Logging: ● Enabled ○ Disabled

Step 3 In the Policy Engine Logging area at the bottom of the pane, click **Enabled**.

Step 4 Click **Save** to save the configuration.

Task 12—Enabling the Traffic VM's Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG

This section includes the following topics:

- Enabling Traffic VM's Port-Profile for Firewall Protection, page 2-56
- Verifying the VSM/VEM for Cisco VSG Reachability, page 2-57
- Checking the VM Veth Port for Firewall Protection, page 2-57

BEFORE YOU BEGIN

Make sure that you have the following:

- Server virtual machine running with an access port-profile (for example, webserver)
- Cisco VSG data IP (10.10.10.200) and VLAN ID (100)
- Security profile name (for example, sp-web)
- Organization (Org) name (for example, root/Tenant-A)
- The port-profile that you would like to edit to enable firewall protection
- One active port in the port-profile with vPATH configuration needs to be up to see the above status

Enabling Traffic VM's Port-Profile for Firewall Protection

This example shows the traffic VM port profile before firewall protection:

```
port-profile type vethernet pp-webserver
  vmware port-group
  switchport mode access
  switchport access vlan 3770
  no shutdown
  state enabled
```

This example shows how to enable firewall protection:

```
vsm(config)# port-profile pp-webserver
vsm(config-port-prof)# vn-service ip-address 10.10.10.200 vlan 100 security-profile sp-web
vsm(config-port-prof)# org root/Tenant-A
```

This example shows the traffic VM port profile after firewall protection:

```
port-profile type vethernet pp-webserver
  vmware port-group
  switchport mode access
  switchport access vlan 3770
  vn-service ip-address 10.10.10.200 vlan 100 security-profile sp-web
  org root/Tenant-A
  no shutdown
  state enabled
```

Verifying the VSM/VEM for Cisco VSG Reachability

This example show how to verify VEM/VSG communication:

```
vsm# show vsn brief
 VLAN           IP-ADDR           MAC-ADDR  FAIL-MODE  STATE  MODULE
100      10.10.10.200  00:50:56:83:00:46      Close    Up  3
vsm#
```

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 Veth Port for Firewall Protection

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

```
vsm# show vsn port vethernet16
Veth             : Veth16
VM Name          : sg-allrun-centos2
VM uuid          : 42 03 d1 ab 29 20 fd 01-57 89 80 1a 6f fe 04 8b
DV Port          : 2112
DVS uuid         : 40 f2 03 50 4b b3 50 eb-2e 13 bc 0c 82 ee 54 58
Flags            : 0x148
VSN Data IP      : 10.10.10.200
Security Profile : sp-web
Org              : root/Tenant-A
VNSP id          : 2
IP addresses:
    172.31.2.92
```

Note Make sure that your VNSP ID value is more than 1.

Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs

This section includes the following topics:

- Sending Traffic Flow, page 2-57
- Verifying Policy-Engine Statistics and Logs on the Cisco VSG,, page 2-59

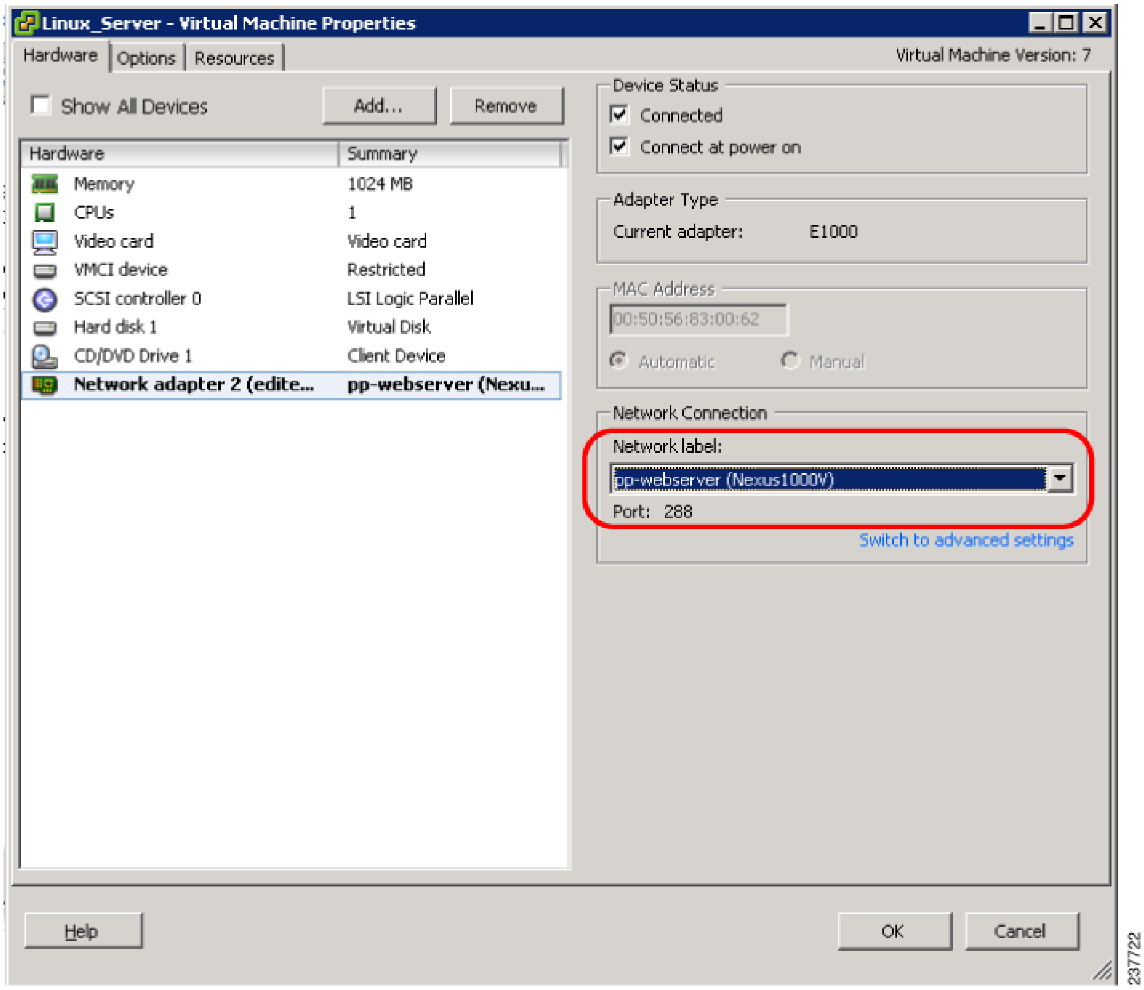
Sending Traffic Flow

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

PROCEDURE

Step 1 Ensure that you have the VM (Server-VM) that is using the port profile (pp-webserver) configured for firewall protection. See Figure 2-62.

Figure 2-62 Virtual Machine Properties Window



Linux_Server - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 7

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD Drive 1	Client Device
Network adapter 2 (edite...	**pp-webserver (Nexu...**

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: E1000

MAC Address
00:50:56:83:00:62
● Automatic ○ Manual

Network Connection
Network label:
pp-webserver (Nexus1000V)
Port: 288
Switch to advanced settings

Help — OK — Cancel

Step 2 Log in to any of your client VM (Client-VM) and send traffic (for example, HTTP) to your Server-VM.

```
[root@sg-centos-vk1 ~]# 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@sg-centos-vk1 ~]#
```

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

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
```

PART 2

Installation Guide for the Cisco Virtual Security Gateway

CHAPTER 3

Installing the Cisco Virtual Security Gateway

This chapter describes how to install and complete the basic configuration of the Cisco Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series switch software.

This chapter includes the following sections:

Information About the Cisco VSG

This section describes the Cisco VSG and includes the following topics:

Host and VM Requirements

The Cisco VSG has the following requirements:

- ESX or ESXi platform running VMware software release 4.1 or 5.0 and requiring a minimum of 4GB physical 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.
  - 1 processor
  - 2-GB RAM
  - 3 NICs (1 of type VMXNET3 and 2 of type E1000)
  - Minimum 3-GB SCSI hard disk with LSI Logic Parallel adapter (default)

- CPU speed of 1.5 GHz

Cisco Virtual Security Gateway and Supported Cisco Nexus 1000V Series Switch Terminology

Table 3-1lists the terminology is used in the Cisco Virtual Security Gateway implementation.

Table 3-1 Cisco Virtual Security Gateway Terminology

Term	Description
Distributed Virtual Switch (DVS)	Logical switch that spans one or more VMware ESX servers. It is controlled by one VSM instance.
ESX/ESXi	Virtualization platform used to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine.
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.
vCenter Server	Service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a VMware ESX host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual data center as defined by VMware vCenter Server.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines 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 VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual switch 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 ESX/ESXi from any windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

Prerequisites to Installing Cisco VSG Software

The Cisco VSG has the following prerequisites:

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/tsd_products_support_series_home.html

Installing the Cisco VSG Software

You can install the Cisco VSG software on a virtual machine (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, page 3-3
- Installing the Cisco VSG Software from an ISO File, page 3-6

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

Before starting the procedure, know or do the following:

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

- HA Secondary
- Manual Installation

PROCEDURE

Step 1 From the vSphere Client menu, choose the data center where you want to install the OVA file for the Cisco VSG.

Step 2 Choose **File** > **Deploy OVF Template**.

The Source dialog box opens.

Step 3 Click the **Deploy from file** radio button to browse and choose the location of the OVA file on the local disk.

Step 4 Click **Next**.

The OVF Template Details dialog box opens displaying product information, including the size of the file and the size of the VM disk.

Step 5 Click **Next**.

The End User License Agreement dialog box opens.

Step 6 Read the End User License Agreement.

Step 7 Click **Accept** and then click **Next**.

The Name and Location dialog box opens.

Step 8 In the Name field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.

Step 9 From the Select a datastore in which to store the VM files pane, choose your datastore and click **Next**.

The Deployment Configuration window opens.

Step 10 In the Configuration field, you will be presented with four options:

- Standalone
- HA Primary
- HA Secondary
- Manual Installation

  For this example, choose **Standalone** and click **Next**.

The Disk Format dialog box opens.

Note We are using the Standalone installation for this document as an example. If you chose Manual Installation mode, you would choose the default values for the following steps.

Note In Standalone mode, be sure to fill in all the fields indicated below (they will be indicated on the GUI with red type).

Step 11 From the Select a format in which to store the virtual machines virtual disks, click the radio button for the format you choose and click **Next**.

The Host or Cluster window opens.

Step 12 Choose the host where the Cisco VSG will be installed.

Step 13 Click **Next**.

The Datastore dialog box opens.

Step 14 From the Select a datastore in which to store the VM files pane, choose your datastore.

Step 15 Click **Next**.

The Network Mapping dialog box opens.

Step 16 Click the drop-down arrows for Data (Service), Management, and HA to associate port profiles.

Step 17 Click **Next**.

The Properties dialog boxes opens.

Step 18 Do the following:

a. In the Cisco VSG HA ID field, enter a unique number between 1 and 4095. This number helps you to identify your Cisco VSG HA pairs.

b. In the Nexus 1000VSG Administration User Password field, enter your password.

c. In the Management IP Address field, enter the management address value.

d. In the Management IP Subnet Mask field, enter the management subnet mask value.

e. In the Management IP Gateway field, enter the management gateway value.

The Ready to Complete dialog box opens displaying details about your settings.

Step 19 Click **Next**.

Step 20 If the settings are correct, click **Finish.**

The deployment task begins in a dialog box that notifies you when the installation completes successfully.

Step 21 Click **Close**.

You have completed installing the Cisco Virtual Security Gateway software and creating a VM for the Cisco VSG.

Step 22 Power on the Cisco VSG you just created.

Step 23 If you chose the Standalone mode for installation in Step 10, 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 Nexus 1000V Series Switch Fireway Policy Guide, Release 4.2(1)VSG1(3).*

Step 24 If you chose the manual installation in Step 10, see the "Configuring Initial Settings" section on page 3-7 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 Virtual Security Gateway from an ISO file.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- A name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- The name of the host where the Cisco VSG will be installed in the inventory folder.
- The name of the datastore in which the VM files will be stored.
- The names of the network port profiles used for the VM.
- 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 ESX host where you want to install the Cisco Virtual Security Gateway and choose **New Virtual Machine**.

The Create New Virtual Machine dialog box opens.

For VM requirements, see the "Host and VM Requirements" section on page 3-1. For detailed information about how to create a VM, see the VMware documentation.

Step 3 Click the **Custom** radio button to create a VM, and click **Next**.

The Create New Virtual Machine dialog box opens.

Step 4 In the Name field, add a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.

Step 5 In the Inventory Location field, choose your data center and click **Next**.

The Datastore dialog box opens.

Step 6 From the Select a datastore in which to store the VM files pane, choose your datastore and click **Next**.

The Virtual Machine Version dialog box opens.

Step 7 Click the **Virtual Machine Version:** Keep the selected virtual machine version.

The Guest Operating System dialog box opens.

Step 8 Click the **Linux** radio button.

Step 9 In the Version field, from the drop-down list, choose **Other 2.6x Linux (32-bit)** from the drop-down list. Click **Next**.

The CPUs dialog box opens.

Step 10 In the Number of virtual processors field, from the drop-down list, choose **1** and click **Next**.

The Memory dialog box opens.

Step 11 Choose **2 GB** memory size and click **Next**.

The Create Network Connectors dialog box opens.

Step 12 In the How many NICs do you want to connect? field, from the drop-down list, choose **3**.

Step 13 In the Network pane, from the drop-down lists, choose **service**, **management**, and **HA** port profiles in that sequence for the NIC 1, NIC 2, and NIC 3. Choose **VMXNET3** for the adapter type for NIC 1. Choose E1000 for the adapter type for NIC 2 and NIC 3 and click **Next**.

The SCSI Controller dialog box opens.

Step 14 The radio button for the default SCSI controller is chosen. Click **Next**.

The Select a Disk dialog box opens. The radio button for the default disk is chosen.

Step 15 Click **Next**.

The Create a Disk dialog box opens. The default virtual disk size and policy is chosen.

Step 16 Click **Next**.

The Advanced Options dialog box opens. The default options are chosen.

Step 17 Click **Next**.

The Ready to Complete dialog box opens.

Step 18 In the Settings for the new virtual machine pane, review your settings.

Step 19 Check the **Edit the virtual machine before completion** check box and click **Continue**.

A dialog box with device details opens.

Step 20 From the Hardware pane, choose your **New CD/DVD (adding)**.

Step 21 Click the **Datastore ISO File** radio button to browse and, from the drop-down list, select your ISO file.

Step 22 In the Device Status pane, check the **Connect at power on** check box and click **Finish**.

The Summary tab window opens.

Step 23 In the Recent Tasks pane, wait for the Create virtual machine status to complete.

Step 24 From the vSphere Client menu, choose your recently installed VM and in the VM pane, click **Power on the virtual machine**.

Step 25 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 on page 3-7 to configure the initial settings on the Cisco VSG.

Note To allocate additional RAM, first power off the VM by right-clicking on the VM icon and then choosing **Power** > **Power Off** from the popup window.
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 initial settings on the Cisco VSG and includes the following topic:

- Configuring Initial Settings on a Standby Cisco VSG, page 3-9

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 the "Installing the Cisco VSG Software" section on page 3-3.

BEFORE YOU BEGIN

See Table 3-2 to determine if you must configure initial settings as described in this section.

Table 3-2 Configure Initial Settings Based on Cisco Virtual Security Gateway Installation Method

Your Cisco Virtual Security Gateway Software Installation Method	Do You Proceed with "Configuring Initial Settings"?
Installing an OVA file and choosing Manually Configure Nexus 1000VSG 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 At the Console tab on your VM after the Cisco VSG software image boots, create the admin password.

```
Enter the password for "admin":<password>
```

Note This password is required for further access for Cisco VSG administrators.

Step 2 Confirm the admin password.

Step 3 Enter the HA role of the Cisco VSG.

```
Enter HA role[standalone/primary/secondary]:primary
```

Step 4 Enter an ID number for the HA pair.

```
Enter the ha id(1-4095): 25
```

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 enter is identical to the other Cisco VSG in the pair.

Step 5 Enter the basic system configuration setup dialog.

This example shows how to configure a basic system configuration setup dialog:

```
Would you like to enter the basic configuration dialog (yes/no):yes
```

```
Create another login account(yes/no)[n]:n

Configure read-only SNMP community string (yes/no)[n]:n

Enter the Virtual Security Gateway (VSG) name:VSG-demo

Continue with Out-of-band (mgmt0) management configuration? (yes/no)[y]:y

Mgmt IPv4 address:10.10.10.11

Mgmt IPv4 netmask:255.255.255.0

Configure the default gateway? (yes/no)[y]:y

IPv4 address of the default gateway:10.10.10.1

Configure the DNS IPv4 address? (yes/no)[no]:no

Enable the telnet service? (yes/no)[y]:n

Configure the ntp server? (yes/no) [n]:n

The following configuration will be applied:
    Interface mgmt0
    ip address 10.10.10.11 255.255.255.0
    no shutdown
    interface data0
    ip address 215.1.1.1 255.255.0
    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

Would you like to edit the configuration? (yes/no)[n]:n

Use this configuration and save it? (yes/no)[y]:y
[########################################################] 100%
```

Step 6 Enter the administrator login.

```
User Access Verification
VSG login: <admin>
```

Step 7 Enter the password.

```
Password: <password>
```

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 At the Console tab on your VM after the Cisco VSG software image boots, enter the admin password.

```
Enter the password for "admin":<password>
```

Step 2 Confirm the admin password.

Step 3 Enter an ID number for the HA pair.

```
Enter the ha-pair id(1-4095): 25
```

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 4 Enter the HA role of the Cisco VSG.

```
Enter HA role[standalone/primary/secondary]:secondary
```

Step 5 Enter the administrator login.

```
User Access Verification
VSG login: <admin>
```

Step 6 Enter the password.

```
Password: <password>
```

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

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
data0    --           up     172.168.1.1                               1000     1500


vsg# show vsg
```

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

vsg#
```

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 VNMC.

PART 3

Installation Guide for the Cisco Virtual Network Management Center

CHAPTER 4

Installing the Cisco Virtual Network Management Center

This chapter provides procedures for installing the Cisco Virtual Network Management Center (VNMC).

This chapter includes the following sections:

Information About Installing the Cisco VNMC

You can install the Cisco VNMC on a virtual machine by deploying the OVF template using a preexisting Open Virtual Appliance (OVA), or by creating a virtual machine and using the optical disk media (ISO) installer. Once installed, you register the Cisco VSG and the Cisco Nexus 1000V switch with the Cisco VNMC. When registration is complete, the Cisco VNMC can manage the Cisco VSG and the Cisco Nexus 1000V switch.

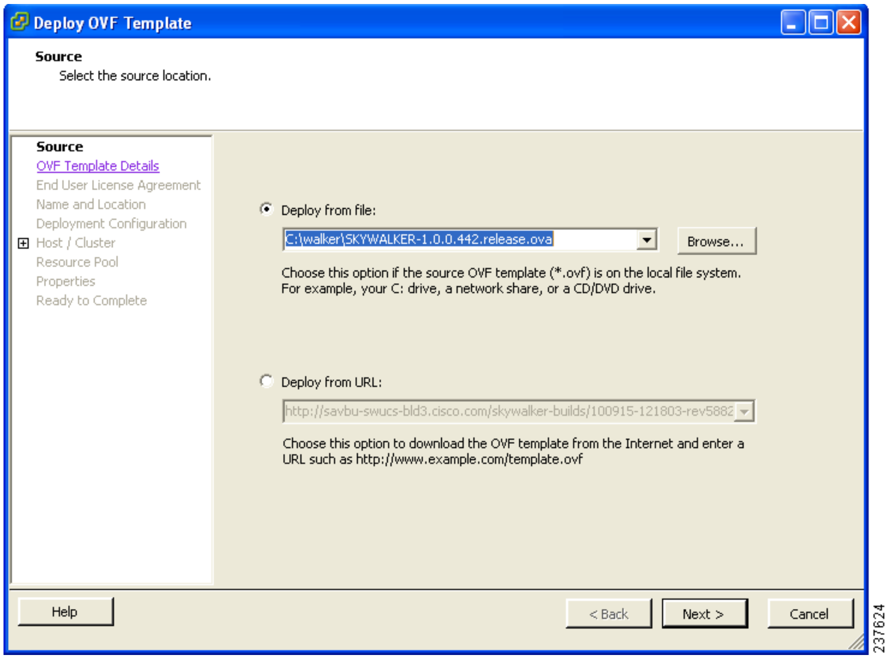
Information About Deploying the OVF Template

All the properties fields in the OVF template must have values. The selection you make on the Deployment Configuration page controls which fields are required and which fields are not. Optional and unused fields are automatically filled with null values. If you want to use an optional field, change the value. Password fields are not masked in the OVF Template wizard and can be viewed after deployment. Red error messages display under a field if an invalid value is entered. When a field changes validity, going from an invalid value to a valid value or valid value to an invalid value, the focus changes to the top of the window.

During initial power on, all input is validated. Once validated, the Cisco VNMC is installed, and the Virtual Machine (VM) is configured and then rebooted.

Figure 4-1 shows the first page of the OVF template.

Figure 4-1 Deploy OVF Template—Source



Source

Select the source location.

● Deploy from file:

C:\walker\SKYWALKER-1.0.0.442.release.ova

Choose this option if the source OVF template (*.ovf) is on the local file system. For example, your C: drive, a network share, or a CD/DVD drive.

○ Deploy from URL:

http://savbu-swucs-bld3.cisco.com/skywalker-builds/100915-121803-rev5882

Choose this option to download the OVF template from the Internet and enter a URL such as http://www.example.com/template.ovf

Installing the Cisco VNMC by Deploying the OVF Template

You can install the Cisco VNMC by deploying the OVF template.

Note During initial power on, extra validation is performed on user values. If any of the values are invalid, a console message appears warning that the values must be corrected. The installation does not start until all values are correct.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- Ensure that you have all the proper networking information available, including the IP address that you will use for the Cisco VNMC.
- If you are using the OVF template for deployment, see Appendix A, "Examples of Cisco VNMC OVA Template Deployment and Cisco VNMC ISO Installations."

PROCEDURE

Step 1 Open your VMware client.

Step 2 Download the .ova file using one of the following methods:

a. Use a conventional download method to download the Cisco VNMC .ova file from http://www.cisco.com/en/US/products/ps11213/index.html, and then start the OVF template.

b. Start the OVF template and download the Cisco VNMC .ova as follows:

- Use your OVF template to select a file on your local machine.
- Use your OVF template to download the file from cisco.com.

Step 3 Follow the steps presented by the OVF template to install the Cisco VNMC:

a. When you reach the Deployment Configuration page, from the Configuration drop-down list, choose **VNM Installer**.

b. When you reach the Properties page, enter values in the appropriate fields:

- In the IP Address area, enter the IP address, the gateway, and the netmask of the virtual machine.
- (Optional) In the VNM DNS area, enter an IP address that is the IP address of your DNS server.
- In the VNM DNS area, enter a hostname and a domain name.
- In the VNM Password area, enter the password for the admin account and the shared secret password.

Note Before the VMware software release 5.0, passwords were not masked when you entered them.

Note You do not need to enter any values in the Cisco VNMC Restore area.

Step 4 When you reach the page that summarizes your template settings, verify them and click **Finish**.

A progress dialog box appears. When the progress dialog box reaches 100%, another dialog box appears to let you know the status of your installation.

Step 5 Click **Close**.

The Cisco VNMC is installed.

Step 6 Power on the virtual machine.

Note Additional input validation is performed when you first boot up. You may have to reenter values during boot up.

When you open your console, the login prompt should appear.

Restoring the Cisco VNMC by Deploying the OVF Template

You can restore the Cisco VNMC by deploying the OVF template.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- You must have a full-state backup to restore. Ensure that you have the location of your full-state backup, including the transfer protocol, the remote IP address, the credentials, and the filename.

- During the restore, the virtual machine must have initial network connectivity. Ensure that you have all the proper networking information available to retrieve the full-state backup, including the IP address of your Cisco VNMC.
- During the initial boot after completing the OVF template, the full-state backup is downloaded. If any issues with the restore occur, boot will stop and display an error message. The VM will also be rebooted on restore.

PROCEDURE

Step 1 Open your VMware client.

Step 2 Download the .ova file using one of the following methods:

a. Use a conventional download method to download the Cisco VNMC .ova file from http://www.cisco.com/en/US/products/ps11213/index.html, and then start the OVF template.

b. Start the OVF template and download the Cisco VNMC .ova as follows:

- Use your OVF template to select a file on your local machine.
- Use your OVF template to download the file from cisco.com.

Step 3 Follow the steps presented by the OVF template to restore the Cisco VNMC:

a. When you reach the Deployment Configuration page, from the Configuration drop-down list, choose **VNMC Restore**.

b. When you reach the Properties page, enter values in the appropriate fields:

- In the IP Address area, enter the IP address, the gateway, and the netmask of the virtual machine.
- In the VNMC Restore area, enter all restore information.

Note Passwords are not masked when you enter them.

Step 4 When you reach the page that summarizes your template settings, verify them and click **Finish**.

A progress dialog box appears. When the progress dialog box reaches 100%, another dialog box appears to let you know the status of your installation.

Step 5 Click **Close**.

The Cisco VNMC is restored.

Step 6 Power on the virtual machine.

When you open your console, the login prompt should appear.

Installing the Cisco VNMC Using an ISO Image

You can install or restore an instance of Cisco VNMC using an ISO image.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- Ensure that your hard drive size is at least 25 GB.

- See Appendix A, "Examples of Cisco VNMC OVA Template Deployment and Cisco VNMC ISO Installations," for a detailed example of an ISO installation.

PROCEDURE

Step 1 Open your client.

Step 2 Download an ISO image from the Cisco.com.

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

a. Ensure that your virtual machine size is 20 GB.

b. Ensure that your virtual machine has 3-GB RAM.

c. Choose **Red Hat Enterprise Linux 5 64-bit** as your operating system.

Step 4 Boot your virtual machine from the ISO image.

The ISO installer appears.

Step 5 Enter the appropriate values in the ISO installer.

Step 6 Once the installation is completed, click **Reboot**.

The Cisco VNMC instance is created.

Connecting to the Cisco VNMC

You can use your browser to connect to the Cisco VNMC.

PROCEDURE

Step 1 Open a browser.

Step 2 In the browser Address field, enter the IP address that you designated for your Cisco VNMC instance and click **Go**.

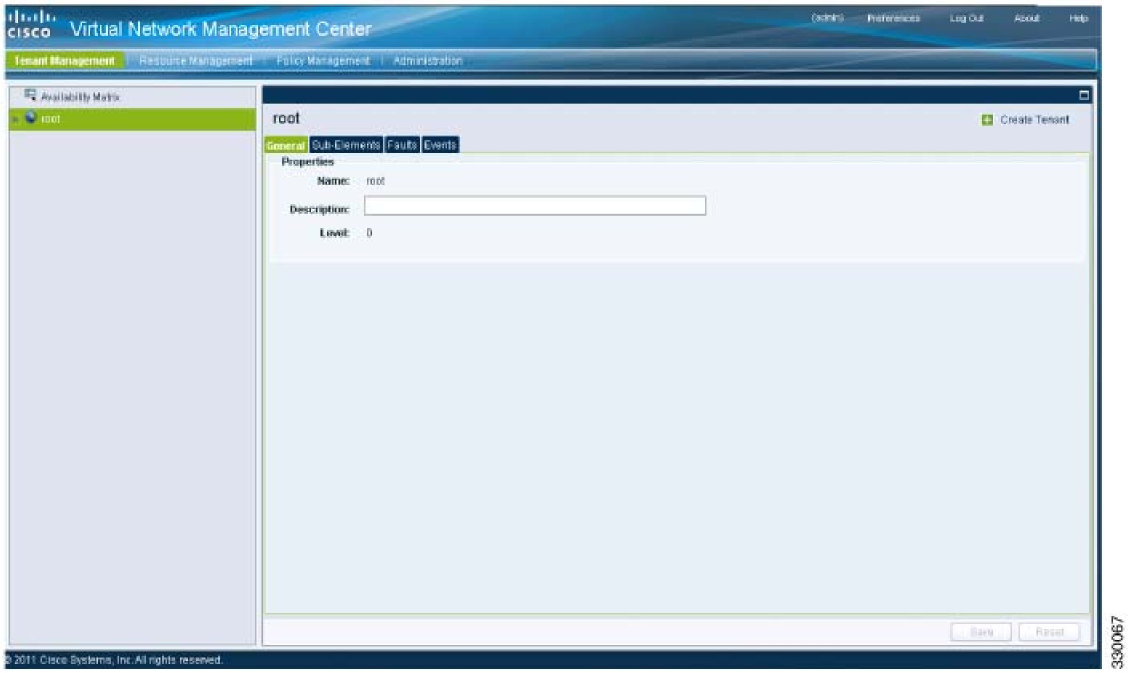
The login dialog box for Cisco VNMC appears.

Step 3 Using the appropriate username and password, log into the Cisco VNMC.

You are connected to the Cisco VNMC.

Figure 4-2 shows the main window of the Cisco VNMC.

Figure 4-2 Cisco Virtual Network Management Center, Main Window



root

Properties

Name: root

Description:

Level: 0

Verifying Cisco VNMC Providers

You can verify the Cisco VNMC service providers as a way to ensure that the Cisco VNMC is running properly.

PROCEDURE

Step 1 In the CLI, enter the **connect local-mgmt** command.

```
VNMC# connect local-mgmt
```

Step 2 Enter the **service status** command.

```
VNMC(local-mgmt)# service status
```

Step 3 Ensure that the following providers are listed as running:

- **policy-mgr-svc_pol_dme**
- **resource-mgr-svc_res_dme**
- **vm-mgr-svc_vmm_dme**

You are ready to register the Cisco VSG and the Cisco Nexus 1000V.

CHAPTER 5

Registering Devices With the Cisco VNMC

This chapter provides information about registering devices with the Cisco Virtual Network Management Center (VNMC).

This chapter includes the following sections:

Registering a Cisco VSG

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

PROCEDURE

Step 1 Copy the vnmc-vsgpa.1.2.1b.bin file into the Cisco VSG bootflash:.

```
vsg# copy ftp://guest@172.18.217.188/n1kv/vnmc-vsgpa.1.2.1b.bin bootflash:
```

Step 2 On the command line, enter configuration mode.

```
vsg# configure
```

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

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

Step 4 Set the Cisco VNMC registration IP address.

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

Step 5 Specify the shared-secret of Cisco VNMC.

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

Step 6 Install the policy agent.

```
vsg (config-vnm-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.1.2.1b.bin
```

Step 7 Exit all modes.

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

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

```
vsg# show vnm-pa status
```

If registration was successful, you should see the following message:

```
"VNM Policy-Agent status is - Installed Successfully. Version 1.2(1b)-vsg"
```

The Cisco VSG registration is complete.

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

```
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 VNMC. Registration enables communication between the Cisco Nexus 1000V VSM and VNMC.

PROCEDURE

Step 1 Copy the vnmc-vsmpa.1.2.1b.bin file into the VSM bootflash:

```
vsm # copy ftp://guest@172.18.217.188/n1kv/vnmc-vsmpa.1.2.1b.bin bootflash:
```

Step 2 Enter **configure** to enter configuration mode.

```
n1kv# configure
```

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

```
n1kv (config)# vnm-policy-agent
```

Step 4 Set the VNMC registration IP address.

```
n1kv (config-vnm-policy-agent)# registration-ip 209.165.200.226
```

Step 5 Specify the shared-secret of Cisco VNMC.

```
n1kv (config-vnm-policy-agent)# shared-secret ********
```

Step 6 Install the policy agent.

```
n1kv (config-vnm-policy-agent)# policy-agent-image bootflash:vnmc-vsmpa.1.2.1b.bin
```

Step 7 Exit all modes.

```
n1kv (config-vnm-policy-agent)# end
```

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

```
n1kv# show vnm-pa status
```

If registration was successful, you should see the following message:

"VNM Policy-Agent status is - Installed Successfully. Version 1.2(1b)-vsm"

The Cisco Nexus 1000V VSM registration is completed.

Step 9 On the command line, enter the following command.

```
n1kv# 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 Virtual Network Management Center CLI Configuration Guide* for detailed information about configuring the Cisco VNMC using the CLIs.

Registering vCenter

You can register vCenter with the Cisco VNMC.

PROCEDURE

Step 1 Log into the Cisco VNMC.

Step 2 In the Cisco VNMC, choose **Administration** > **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 VNMC 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 VNMC and choose **Administration** > **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**.

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

vCenter is registered.

Part 4

Installing the Cisco VSG on a Cisco Nexus 1010 Appliance

CHAPTER 6

Installing the Cisco Virtual Security Gateway on a Cisco Nexus 1010 Virtual Services Appliance

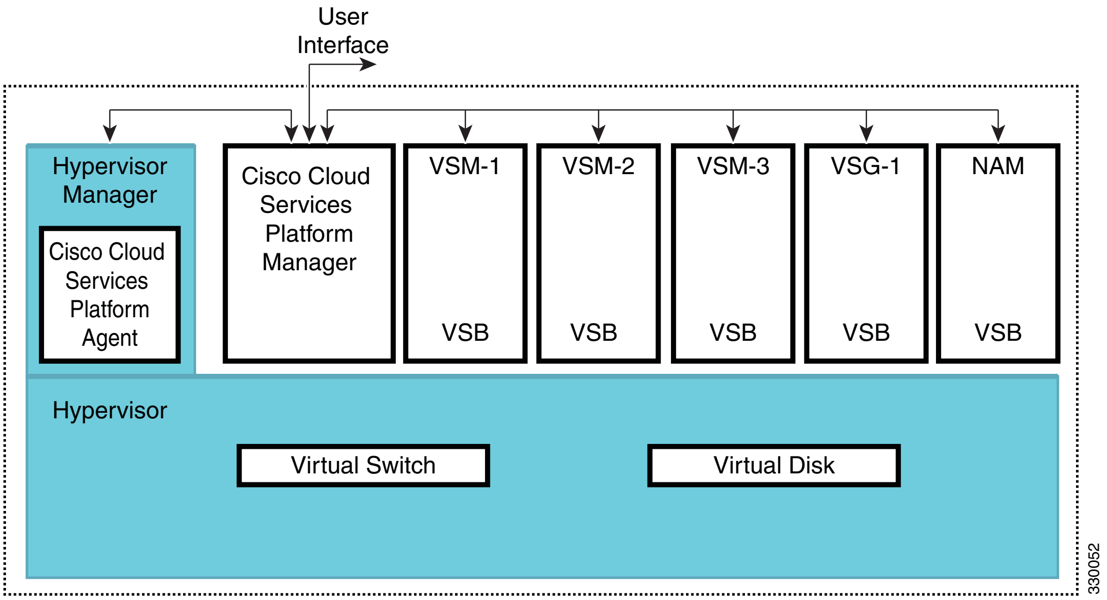
This chapter describes how to install the Cisco Virtual Security Gateway (VSG) on a Cisco Nexus 1010 Virtual Services Appliance.

This chapter includes the following sections:

Information About Installing the Cisco VSG on the Cisco Nexus1010

The Cisco VSG software is provided with the other virtual service blade (VSB) software in the Cisco Nexus 1010 bootflash: repository directory. As shown in Figure 6-1, the Cisco Nexus 1010 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 6-1 Cisco Nexus 1010 Architecture Showing Virtual Service Blades Usage



Prerequisites

Installing the Cisco VSG on a Cisco Nexus 1010 has the following prerequisites:

- You must first install the Cisco Nexus 1010 Virtual Services Appliance and connect it to the network. For procedures on installing the hardware, see the *Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide*.
- After you install the hardware appliance and connect it to the network, you can configure the Cisco Nexus 1010 management software, migrate existing VSMs residing on a VM to the Cisco Nexus 1010 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 Nexus 1010 Software Configuration Guide*.

Guidelines and Limitations

Installing the Cisco VSG on a Cisco Nexus 1010 as a VSB has the following guidelines and limitations:

- The Cisco Nexus 1010 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 Nexus 1010.

Caution Do not change the management VLAN on a VSB. Because the management VLAN is inherited from the Cisco Nexus 1010, any changes to the management VLAN are applied to both the Cisco Nexus 1010 and all of its hosted VSBs.

Installing a Cisco VSG on a Cisco Nexus 1010

You can install the Cisco VSG on a Cisco Nexus 1010 as a virtual service blade (VSB).

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You 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.VSG1.2.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.
- You know the following properties for the Cisco VSG VSB:
  - HA ID
  - Management IP address
  - Management subnet mask length
  - Default gateway IPV4 address
  - Cisco VSG name
  - 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 1010.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**configure** **Example:** N1010# configure N1010(config)#	Places you in the global configuration mode.
Step 2	**virtual-service-blade** *name* **Example:** N1010(config)# virtual-service-blade vsg-1 N1010(config-vsb-config)#	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	**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.

Example:

```
N1010(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
switch(config-vsb-config)#
```

Step 4	**virtual-service-blade-type** [**name** *name* | **new** *iso file name*] **Example:** N1010(config-vsb-config)# virtual-service-blade-type new nexus-1000v.VSG1.2.iso N1010(config-vsb-config)# **Example:** N1010(config-vsb-config)# virtual-service-blade-type name VSG-1 N1010(config-vsb-config)#	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	**description** *description* **Example:** N1010(config-vsb-config)# description vsg-1 for Tenant1 N1010(config-vsb-config)#	(Optional) Adds a description to the Cisco VSG VSB. The *description* is an alphanumeric string of up to 80 characters.

Command | **Purpose**

Step 6

Command:

```
show virtual-service-blade name name

Example:
N1010(config-vsb-config)# show
virtual-service-blade name vsg-1
virtual-service-blade vsm2
  Description:
  Slot id:        2
  Host Name:
  Management IP:
  VSB Type Name :  VSG-1.0
  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:
switch(config-vsb-config)#
```

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

Step 7

Command:

```
interface name vlan vlanid

Example:
N1010(config-vsb-config)# interface data
vlan 1044
N1010(config-vsb-config)#

Example:
N1010(config-vsb-config)# interface ha
vlan 1045
N1010(config-vsb-config)#
```

Purpose: Applies the interface and VLAN ID to this Cisco VSG. Use the interface names from 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 1010.

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.

	Command	Purpose

Step 9	**`enable [primary	secondary]`**
		Example:
		`N1010(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:  VSG-1`
		` Enter the password for 'admin':`
		`Hello_123`
		`N1010(config-vsb-config)#`
			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 1010 prompts you for the following:
			• HA ID
			• Management IP address
			• Management subnet mask length
			• Default gateway IPV4 address
			• Cisco VSG name
			• Administrator password

	Command	Purpose

Step 10	**show virtual-service-blade name** *name*
	
	Example:
	N1010(config-vsb-config)# show
	virtual-service-blade name vsg-1
	virtual-service-blade vsg-1
	  Description:
	  Slot id: 1
	  SW version: 4.0(4)SV1(3)
	  Host Name: vsg-1
	  Management IP: 10.78.108.40
	  VSB Type Name : VSG-1.1
	  Interface: ha vlan: 1044
	  Interface: management vlan: 1032
	  Interface: data vlan: 1045
	  Interface: internal vlan: NA
	  Ramsize: 2048
	  Disksize: 3
	  Heartbeat: 1156
	  HA Admin role: Primary
	    HA Oper role: STANDBY
	    Status: VB POWERED ON
	    Location: PRIMARY
	  HA Admin role: Secondary
	    HA Oper role: ACTIVE
	    Status: VB POWERED ON
	    Location: SECONDARY
	  VB Info:
	    Domain ID : 1054
	switch(config-vsb-config)#
		(Optional) Displays the new VSB for verification.
		
		While the Cisco Nexus 1010 management software is configuring the Cisco VSG, the output for this command progresses from *in progress* to *powered on*.

Step 11	**copy running-config startup-config** **Example:** N1010(config-vsb-config)# copy running-config startup-config	(Optional)Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

EXAMPLES

This example shows how to display the contents of the bootflash: repository directory:

```
N1010# dir bootflash:repository
  159250432     May 11 06:35:04 2011  nam-app-x86_64.4-2-1n.iso
  183412736     May 10 23:03:23 2011  nam-app-x86_64.5-1-1.iso
  255090688     May 03 17:45:25 2011  nexus-1010.4.2.1.SP1.2.15.iso
  109043712     May 12 21:51:15 2011  nexus-1000v.VSG1.2.iso

Usage for bootflash://sup-local
  386187264 bytes used
 3605192704 bytes free
 3991379968 bytes total
```

This example shows how to configure a Nexus 1010 appliance VSB as a Cisco VSG:

```
N1010# configure
Enter configuration commands, one per line.  End with CNTL/Z.
N1010(config)# virtual-service-blade vsg1
N1010(config-vsb-config)# virtual-service-blade-type new nexus-1000v.VSG1.2.iso
N1010(config-vsb-config)# interface data vlan 72
N1010(config-vsb-config)# interface ha vlan 72
N1010(config-vsb-config)# enable
Enter vsb image: [nexus-1000v.VSG1.2.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
N1010(config-vsb-config)#
N1010(config-vsb-config)# end
N1010#
```

This example shows how to display a virtual service blade summary on the Cisco Nexus 1010:

```
N1010# 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
N1010#
.
.
.
```

PART 5

Upgrading the Cisco VSG and the Cisco VNMC

CHAPTER 7

Upgrading the Cisco Virtual Security Gateway and Cisco Virtual Network Management Center

This chapter describes how to install and complete an upgrade for the Cisco Virtual Security Gateway (VSG) and the Cisco Virtual Network Management Center (VNMC).

This chapter includes the following sections:

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, everything is as is. Because the Cisco VSG is stateless, it gets all this information from the Cisco VNMC at bootup.

Information About Cisco VNMC Upgrades

When you upgrade the Cisco VNMC 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.

Complete Upgrade Procedure

When you need to upgrade the Cisco VNMC, Cisco VSG, and Cisco Nexus 1000V, follow these steps:

1. Stage 1: Upgrading Cisco VNMC, page 7-4
2. Stage 2: Upgrading a Cisco VSG Pair, page 7-7
3. Stage 3: Upgrading the VSM Pair and the VEM, page 7-9

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

For a full In-service Software Upgrade (ISSU) upgrade on both the Cisco VSG and VSM, follow these rules:

- Install the Cisco VNMC before installing the Cisco VSG and VSM. The ISSU upgrade installs a new PA.
- A new PA with an old Cisco VNMC 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.

Note You should take a snapshot or backup (clone) of the original VNMC and VSM prior to the upgrade process. We recommend that you perform an ISSU upgrade process on both the VSM and the Cisco VSG. We do not recommend that you perform a manual upgrade.

Table 7-1 provides 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.

All the tests are performed on the Cisco VMware vCenter 5.0.

Table 7-1 Cisco VSG and VNMC Staged Upgrade Procedure Support

Virtual Appliance	Original State	Stage 1: Cisco VNMC Upgrade Only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade (ISSU: PA Upgrade)	Stage 3: VSM/VEM Upgrade (ISSU: PA Upgrade)
VNMC	Old 1.2(1b)	New 1.3	New 1.3	New 1.3
VSM	Old 4.2(1)SV1(4a)	Old 4.2(1)SV1(4a)	Old 4.2(1)SV1(4a)	New 4.2(1)SV1(5.1)
VEM	Old 4.2(1)SV1(4a)	Old 4.2(1)SV1(4a)	Old 4.2(1)SV1(4a)	New 4.2(1)SV1(5.1)
VSM PA	Old1.2(1b)	Old 1.2(1b)	Old 1.2(1b)	New1.3(1c)
VSG	Old 4.2(1)VSG1(2)	Old 4.2(1)VSG1(2)	New 4.2(1) VSG1(3.1)	New 4.2(1) VSG1(3.1)
VSG PA	Old 1.2(1b)	Old1.2(1b)	New 1.3	New 1.3(1c)

Table 7-1 Cisco VSG and VNMC Staged Upgrade Procedure Support

Virtual Appliance	Original State	Stage 1: Cisco VNMC Upgrade Only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade (ISSU: PA Upgrade)	Stage 3: VSM/VEM Upgrade (ISSU: PA Upgrade)
Supported Operations	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 • Non-vn-service port profiles can be converted to vn-service port profiles on 5.0 hosts	• Full 5.0 host support, except that fault-tolerance operations will fail • Short disruption in new data session establishment during the Cisco VSG upgrade • Other operations are fully supported	• Once upgraded: All operations are supported if all VEMs are upgraded as well • Restricted operations (below) apply only if all VEMs are not upgraded • Disruption of data traffic during VEM upgrades
Restricted Operations	None	• No Cisco VNMC policy configuration changes • No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, and so on) • No new vn-service VMs brought up • No bootstrap of devices (Cisco VNMC, Cisco VSG, and VSM) • No vMotion of vn-service firewalled VMs on Cisco Nexus 1000V Switch • No vn-service port profile operations or modifications (toggles, removal, changing the port profiles on VSM) • Cisco VSG failover not supported, VSM failover (vns-agent) not supported • All VSM to Cisco VNMC to Cisco VSG control operations are restricted	• Fault-tolerance operations will fail with MN 5.0 host	• Restricted operations (below) apply only if all VEMs are not upgraded • No Cisco VNMC policy configuration changes • No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, and so on) • No new vn-service VMs brought up • No bootstrap of devices (Cisco VNMC, Cisco VSG, and VSM) • No vMotion of vn-service firewalled VMs on Cisco Nexus 1000V Switch • No vn-service port profile operations or modifications (toggles, removal, changing the port profiles on VSM)

Table 7-1 Cisco VSG and VNMC Staged Upgrade Procedure Support

Virtual Appliance	Original State	Stage 1: Cisco VNMC Upgrade Only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade (ISSU: PA Upgrade)	Stage 3: VSM/VEM Upgrade (ISSU: PA Upgrade)
				• No Cisco Nexus 1000 Switch (non vn-service) operations, including non-vn-service port profiles • All VSM to Cisco VNMC to Cisco VSG control operations are restricted

Mixed Version Upgrade Procedure

This section describes the different software version combinations supported and the upgrade process associated with these combinations.

The two software version combination supported are as follows:

1. Upgrade only the Cisco VNMC and the Cisco VSG to 4.2(1)VSG1(3.1) without upgrading the VSM and VEM. The VSM PA should remain on 1.2(1b). The Cisco VSG PA must be upgraded to 1.3(1c).

   To upgrade this combination, follow these steps:

   a. Stage 1: Upgrading Cisco VNMC, page 7-4

   b. Stage 2: Upgrading a Cisco VSG Pair, page 7-7

2. Upgrade only the Cisco VNMC, VSM Pair and VEM to 4.2(1)SV1(5.1) without upgrading the Cisco VSG. The VSM PA must be upgraded to 1.3(1c). The Cisco VSG PA must remain on 1.2(1b).

To upgrade this combination of software, follow these steps:

   a. Stage 1: Upgrading Cisco VNMC, page 7-4

   b. Stage 3: Upgrading the VSM Pair and the VEM, page 7-9

Restricted Operations

- The Cisco VSG in the Layer 3 mode is not supported.
- The Virtual Extensible Local Area Network (VXLAN) is not supported.

Stage 1: Upgrading Cisco VNMC

This section describes how to upgrade the Cisco VNMC.

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

- You are logged in as admin to the CLI in EXEC mode.

- You have already copied the new software files into the bootflash file system.
- You must have the Cisco VNMC Release 1.3 installed.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**connect local-mgmt**
	Example:
	`vnmc# connect local-mgmt`
	`vnmc(local-mgmt)#`
		Places you in local management mode.

Step 2	**show version** **Example:** `vnmc(local-mgmt)# show version`	(Optional) Displays the version information for the Cisco VNMC software.

Step 3	**copy scp://user@***example-server-ip* */example-dir/filename* bootflash:/
	Example:
	`vnmc(local-mgmt)# copy`
	`scp://<user@example-server-ip>/example1-dir`
	`/vnmc.1.3.1a.bin bootflash:/`
		Copies the Cisco VNMC software file to the VM.

Step 4	**dir bootflash:/** **Example:** `vnmc(local-mgmt)# dir bootflash:/`	Verifies that the desired file is copied in the directory.

Step 5	**update bootflash:** *filename*
	Example:
	`vnmc(local-mgmt)# update`
	`bootflash:/vnmc.1.3.1a.bin`
		Begins the update of the Cisco VNMC software.

Step 6	**show version** **Example:** `vnmc(local-mgmt)# show version`	(Optional) Allows you to verify that the Cisco VNMC software version is updated.

EXAMPLES

This example shows how to connect to the local-mgmt mode:

```
vnmc# connect local-mgmt
Cisco Virtual Network Management Center
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
```

```
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

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

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

Name                Package             Version       GUI
----                -------             -------       ----
core                Base System         1.2(1b)     1.2(1b)
service-reg         Service Registry    1.2(1b)     1.2(1b)
policy-mgr          Policy Manager      1.2(1b)     1.2(1b)
resource-mgr        Resource Manager    1.2(1b)     1.2(1b)
vm-mgr              VM manager          1.2(1b)     none
```

This example shows how to copy the Cisco VNMC software to the VM:

```
vnmc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/vnmc.1.2.0.635.bin
bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

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

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

            887 Jul 28 2011  vnmc-dplug.1.2.1b.bin
            20M Jul 28 2011  vnmc-vsgpa.1.2.1b.bin
            20M Jul 28 2011  vnmc-vsmpa.1.2.1b.bin
           403M Jan 31 01:58 vnmc.1.3.1a.bin


Usage for bootflash://

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

This example shows how to start the update for the Cisco VNMC:

```
vnmc(local-mgmt)# update bootflash:/vnmc.1.2.0.635.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.
```

This example shows how to display the updated version for the Cisco VNMC:

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

Name                Package             Version       GUI
----                -------             -------       ----
core                Base System         1.3(1a)     1.3(1a)
service-reg         Service Registry    1.3(1a)     1.3(1a)
policy-mgr          Policy Manager      1.3(1a)     1.3(1a)
resource-mgr        Resource Manager    1.3(1a)     1.3(1a)
vm-mgr              VM manager          1.3(1a)     none
```

Stage 2: Upgrading a Cisco VSG Pair

This section describes how to upgrade a Cisco VSG pair from Cisco VSG 1.2 to Cisco VSG 1.3 and from Cisco VSG 1.1 to Cisco VSG 1.3.

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

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

```
switch# copy
scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart-mz.VSG1.3.1.bin
bootflash:nexus-1000v-kickstart-mz.VSG1.3.1.bin

switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-mz.VSG1.3.1.bin
bootflash:nexus-1000v-mz.VSG1.3.1.bin

switch# copy scp://user@scpserver.cisco.com/downloads/vnmc-vsgpa.1.3.1c.bin
bootflash:vnmc-vsgpa.1.3.1c.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

This procedure shows how to upgrade the Cisco VSG Pair from Cisco VSG 1.2 to Cisco VSG 1.3.

Step 1 Enter the following command on all the Cisco VSG nodes on your network.

```
VSG# config
VSG(config)# feature http-server
VSG(config)#
```

Step 2 Install the kickstart image, system image, and policy agent (PA) image.

```
vsg# install all kickstart bootflash:nexus-1000v-kickstart-mz.VSG1.3.1.bin system
bootflash:nexus-1000v-mz.VSG1.3.1.bin vnmpa bootflash:vnmc-vsgpa.1.3.1c.bin
```

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. For example, see the1.3.1c image in the above command example.

You can check if there is an existing PA installed by executing the following command:

vsg# **show vnm-pa status**

VNM Policy-Agent status is - Installed Successfully. Version 1.3(1c)-vsg

If a PA image is installed and passed as a parameter to the **install all** command, it upgrades the PA image with the system and kickstart images.

Note You must have an existing PA installed before upgrading the PA by using the install command.

If the PA image is not passed as a parameter to the **install all** command, the other parts of the upgrade (kickstart 1.3.1 and system 1.3.1, in the example above) will be upgraded properly, but the PA will not be upgraded.

PROCEDURE

This procedure shows how to upgrade the Cisco VSG Pair from Cisco VSG 1.1 to Cisco VSG 1.3. There is no install or upgrade command in Cisco VSG 1.1.

Step 1 Enter the config menu:

```
VSG# config
```

Step 2 Unset the kickstart and system images on the active Cisco VSG.

a. `VSG(config)# no boot kickstart`

b. `VSG(config)# no boot system`

Step 3 Set the kickstart and system images to the new image.

```
VSG(config)# boot kickstart nexus-1000v-kickstart-mz.VSG1.3.1.bin
VSG(config)# boot system nexus-1000v-mz.VSG1.3.1.bin
```

Step 4 Uninstall the existing VNM-PA on the Cisco VSG.

a. Enter the PA sub-menu as follows:

```
VSG(config)# vnm-policy-agent
VSG(config-vnm-policy-agent)# no policy-agent-image
VSG(config-vnm-policy-agent)# end
```

Step 5 Enable the HTTP feature.

```
VSG# config t
VSG(config)# feature http-server
```

Step 6 Initiate an image and boot variable synchronization to the standby Cisco VSG.

```
VSG# copy running-config startup-config
```

Step 7 Verify if the boot images are set properly.

```
VSG(config)# show boot
```

Step 8 Once the image synchronization is done, reload the standby module.

```
VSG(config)# reload module standby_module_no
```

If the primary Cisco VSG is active, the **standby_module_no** will be 2. If secondary Cisco VSG is active, the **standby_module_no** will be 1.

Step 9 Check for an established HA pair with the new images. The configuration will be synchronized. Enter the **show system redundancy status** command and verify "Active with standby" is displayed in the output.

```
VSG# show system redundancy status
```

Step 10 Perform a system switchover on current active VSG.

```
VSG# system switchover
```

Step 11 Check for an established HA pair with the new images. The configuration will be synchronized.

Enter the **show system redundancy status** command and verify "Active with standby" is displayed

```
VSG# show system redundancy status
```

Step 12 Copy the VSG PA image on the Cisco VSG under bootflash to the new active VSG(1.3 PA).

```
VSG# copy scp://ipaddress/location_of_pa_image/vnmc-vsgpa.1.3.1c.bin bootflash
```

Step 13 Install the new VNM-PA image on the Cisco VSG.

```
VSG# config
VSG(config)# vnm-policy-agent
VSG(config-vnm-policy-agent)# policy-agent-image vnmc-vsgpa.1.3.1c.bin
VSG(config-vnm-policy-agent)# end
```

Step 14 Check if the PA installation is successful.

```
VSG# show vnm-pa status
```

Step 15 Copy 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.

Stage 3: Upgrading the VSM Pair and the VEM

This section provides information on upgrading to the Cisco Nexus 1000V to Release 4.2(1)SV1(5.1).

Note When installing the PA on the latest VSM, enable the **feature http-server** command on all VSM nodes on your network as follows:

```
VSM# config
VSM(config) # feature http-server
VSM(config)
```

This section includes the following topics:

- Information About the Software Upgrade, page 7-9
- Prerequisites for the Upgrade, page 7-10
- Guidelines and Limitations for Upgrading the Cisco Nexus 1000V, page 7-11
- Upgrading to Release 4.2(1)SV1(5.1), page 7-13

Information About the Software Upgrade

This section provides information about how to upgrade the Cisco Nexus 1000V to Release 4.2(1)SV1(5.1).

This section includes the following topic:

- Obtaining the Upgrade Software, page 7-10

Obtaining the Upgrade Software

You can obtain your upgrade-related software from the following sources listed in Table 7-2.

Table 7-2 Obtaining the Upgrade Software

Source	Description
Cisco	Download the Cisco Nexus 1000V Release 4.2(1)SV1(5.1) software from Cisco.com.
VMware	Download the VMware software from the VMware website.

For information about your software and platform compatibility, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1).*

Prerequisites for the Upgrade

This section describes how to upgrade the Cisco Nexus 1000V software on a Virtual Supervisor Module (VSM) virtual machine (VM) and how to upgrade the Virtual Ethernet Module (VEM).

This section includes the following topics:

- Prerequisites for Upgrading VSMs, page 7-10
- Prerequisites for Upgrading VEMs, page 7-10

Prerequisites for Upgrading VSMs

Upgrading the VSMs has the following prerequisites:

- Close any active configuration sessions before upgrading the Cisco Nexus 1000V software.
- Note that the network and server administrators must coordinate the upgrade procedure with each other.
- You have saved all changes in the running configuration to the startup configuration to be preserved through the upgrade.
- You have saved a backup copy of the running configuration in external storage.
- You have performed a VSM backup. See the “Configuring VSM Backup and Recovery” chapter in the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1).*

  For information about backing up a configuration file, see the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1).*

Prerequisites for Upgrading VEMs

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

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

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

- You are logged in to the VSM CLI in EXEC mode.
- Network and server administrators coordinate the VEM upgrade with each other.
- You have a copy of your VMware documentation available for installing software on a host.
- You have already obtained a copy of the VEM software file from one of the sources listed in Table 2-1, "Obtaining VEM Software" of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at

  http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_install.html
- For more information, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*.
- You have placed the VEM software file in /tmp on the vSphere host. Placing it in the root (/) directory might interfere with the upgrade. Make sure that the root RAM disk has at least 12 MB of free space as displayed by the **vdf** command.
- If you use a proxy server to connect VUM to the Internet, you might need to disable the proxy before starting a VUM upgrade. In VMware versions before VUM Update 1, the proxy prevents VUM from communicating locally with the VSM. For this reason, automatic VEM upgrades might fail if you do not disable the proxy first.
- On your upstream switches, you must have the following configuration.
  - On Catalyst 6500 Series Switches with Cisco IOS software:
    (config-if) **portfast trunk**
    or
    (config-if) **portfast edge trunk**
  - On Cisco Nexus 5000 Series Switches with Cisco NX-OS software:
    (config-if) **spanning-tree port type edge trunk**
- On your upstream switches, we highly recommend that you globally enable the following:
  - Global BPDU Filtering
  - Global BPDU Guard
- On your upstream switches where you cannot globally enable BPDU Filtering and BPDU Guard, we highly recommended that you enter the following commands:
  - (config-if) **spanning-tree bpdu filter**
  - (config-if) **spanning-tree bpdu guard**
- For more information about configuring spanning tree, BPDU, or PortFast, see the documentation for your upstream switch.

Guidelines and Limitations for Upgrading the Cisco Nexus 1000V

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

- You are upgrading the Cisco Nexus 1000V software to Release 4.2(1)SV1(5.1).

- Scheduling — Schedule the upgrade when your network is stable and steady. Ensure that everyone who has access to the switch or the network is not configuring the switch or the network during this time. You cannot configure a switch during an upgrade.
- Hardware — Avoid power interruptions to the hosts that run the VSM VMs during any installation procedure.
- Connectivity to remote servers — do the following:
  - Copy the kickstart and system images from the remote server to the Cisco Nexus 1000V.
  - Ensure that the switch has a route to the remote server. The switch and the remote server must be in the same subnetwork if you do not have a router to route traffic between subnets.
- Software images — do the following:
  - Make sure that the system and kickstart images are the same version.
  - Retrieve the images in one of two ways:

    Locally—Images are locally available on the upgrade CD-ROM/ISO image.

    Remotely—Images are in a remote location and you specify the destination using the remote server parameters and the filename to be used locally.
- Commands to use — do the following:
  - Verify connectivity to the remote server by using the **ping** command.
  - Use the one-step **install all** command to upgrade your software. This command upgrades the VSMs.
  - Do not enter another **install all** command while running the installation. You can run commands other than configuration commands.
  - During the VSM upgrade, if you try to add a new VEM or any of the VEMs are detached due to uplink flaps, the VEM attachment is queued until the upgrade completes.

Note If the VEMs are not compatible with the software image that you install on the VSM, a traffic disruption occurs in those modules, depending on your configuration. The **install all** command output identifies these scenarios. You can choose to proceed with the upgrade or end at this point.

- Local Authentication — We recommend that you use local authentication during the upgrade process. If a remote server is needed, you must make sure that the admin account is configured with network-admin privileges.

Before upgrading the VEMs, note these guidelines and limitations:

- The VEM software can be upgraded manually using the CLI or upgraded automatically using VUM.
- During the VEM upgrade process, VEMs reattach to the VSM.
- Connectivity to the VSM can be lost during a VEM upgrade when the interfaces of a VSM VM connect to its own Distributed Virtual Switch (DVS).
- Connectivity between an active and standby VSM can be lost during a VEM upgrade when the VEM being upgraded provides interface connectivity to one of the VSMs. In this case, both VSMs become active and lose connectivity. To prevent this problem, make sure that you are at the appropriate patch levels. See Table 7-2.
- If you are upgrading a VEM using a Cisco Nexus 1000V bundle, follow the instructions in your VMware documentation. For more details about VMware bundled software, see the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*.

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

Upgrade Paths

This section describes how to upgrade the Cisco Nexus 1000V software on a Virtual Supervisor Module (VSM) virtual machine (VM) and how to upgrade the Virtual Ethernet Module (VEM).

Table 7-3 shows the upgrade procedure you must take to upgrade to Release 4.2(1)SV1(5.1).

Table 7-3 Upgrade Paths from Cisco Nexus 1000V Releases

If you are upgrading from Release	Go to

4.2(1)SV1(4)
4.2(1)SV1(4a)
	Upgrading to Release 4.2(1)SV1(5.1), page 7-13

4.0(4)SV1(3)
4.0(4)SV1(3a)
4.0(4)SV1(3b)
4.0(4)SV1(3c)
4.0(4)SV1(3d)
	Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.1), page 7-37

Note Upgrades from Cisco Nexus 1000V Release 4.0(4)SV1(1) and Cisco Nexus 1000V Release 4.0(4)SV1(2) are no longer supported. VMware 4.0 is also no longer supported.

For upgrade procedures to ESX/ESXi 4.1.0 and ESXi 5.0.0, see Appendix A, “Installing and Upgrading VMware” of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_upgrade_vmware.html#wp705174

- The upgrade process is irrevocable. After the software is upgraded, you can downgrade by removing the current installation and reinstalling the software. For more information, see the “Recreating the Installation” section of *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1).*

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

Upgrading to Release 4.2(1)SV1(5.1)

This section describes how to upgrade to Release 4.2(1)SV1(5.1).

This section contains the following topics:

- Upgrading from Releases 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-14
- Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.1), page 7-37

Note For ESXi 5.0.0 releases and later releases, the minimum VC/VUM version required is 380461/380316. For ESX/ESXi Release 4.1.0 and later releases, the minimum VC/VUM version required is 258902/256596.

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

Caution If your hosts are running a release prior to VMWare 4.1, upgrade to VMWare 4.1 or VMware 5.0. See Appendix A, “Installing and Upgrading VMware” of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at *http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_upgrade_vmware.html#wp705174*

Upgrading from Releases 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)

The following section describes how to upgrade the Cisco Nexus 1000V software from Releases 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1).

This section includes the following topics:

- Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-17
- Upgrading the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-26

Table 7-4 lists the upgrade steps when upgrading to vSphere 4.1 and Release 4.2(1)SV1(5.1).

Table 7-4 Upgrade Procedures to vSphere 4.1 and Release 4.2(1)SV1(5.1)

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4) with a vSphere release 4.0 Update 1 or later	1. Upgrading from VMware Release 4.0 to VMware Release 4.1. See Appendix A, "Installing and Upgrading VMware" of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_upgrade_vmware.html#wp705174. 2. Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-17. 3. Upgrading the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-26
Release 4.2(1)SV1(4) with a vSphere release 4.1 GA, patches, or updates	1. Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-17. 2. Upgrading the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-26
Release 4.2(1)SV1(4a) with a vSphere release 4.0 Update 1 or later	1. Upgrading from VMware Release 4.0 to VMware Release 4.1. See Appendix A, "Installing and Upgrading VMware" of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_upgrade_vmware.html#wp705174. 2. Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-17. 3. Upgrading the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-26

Table 7-4 Upgrade Procedures to vSphere 4.1 and Release 4.2(1)SV1(5.1) (continued)

If you are running this configuration	Follow these steps
Release 4.2(1)SV1(4a) with a vSphere release 4.1 GA, patches, or updates	1. Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-17. 2. Upgrading the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-26
Release 4.2(1)SV1(4a) with a vSphere release 5.0 GA, patches, or updates	N/A

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

- You are running primary and secondary VSMs as an active-standby pair or a standalone VSM.
- The upgrade application cannot be used for the upgrade of the VSMs from Release 4.2(1)SV1(4) to Release 4.2(1)SV1(5.1).
- A pair of VSMs in a high availability (HA) pair is required to support a nondisruptive upgrade.
- A system with a single VSM can only be upgraded in a disruptive manner.

When upgrading the VSM from Release 4.2(1)SV1(4) or a later release to Release 4.2(1)SV1(5.1), if any of the VEM hosts are running a vSphere version prior to 4.1, the **install all** command displays that host as incompatible. The incompatibility warning applies only if you do not upgrade the ESX version with the VEM version. It is possible to manually upgrade the ESX and VEM in one maintenance mode as follows:

1. Place the host in maintenance mode.
2. Upgrade the ESX to 4.1 or 5.0, as needed.
3. Install the Release 4.2(1)SV1(5.1)VEM VIB, while the host is still in maintenance mode.
4. Remove the host from maintenance mode.

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

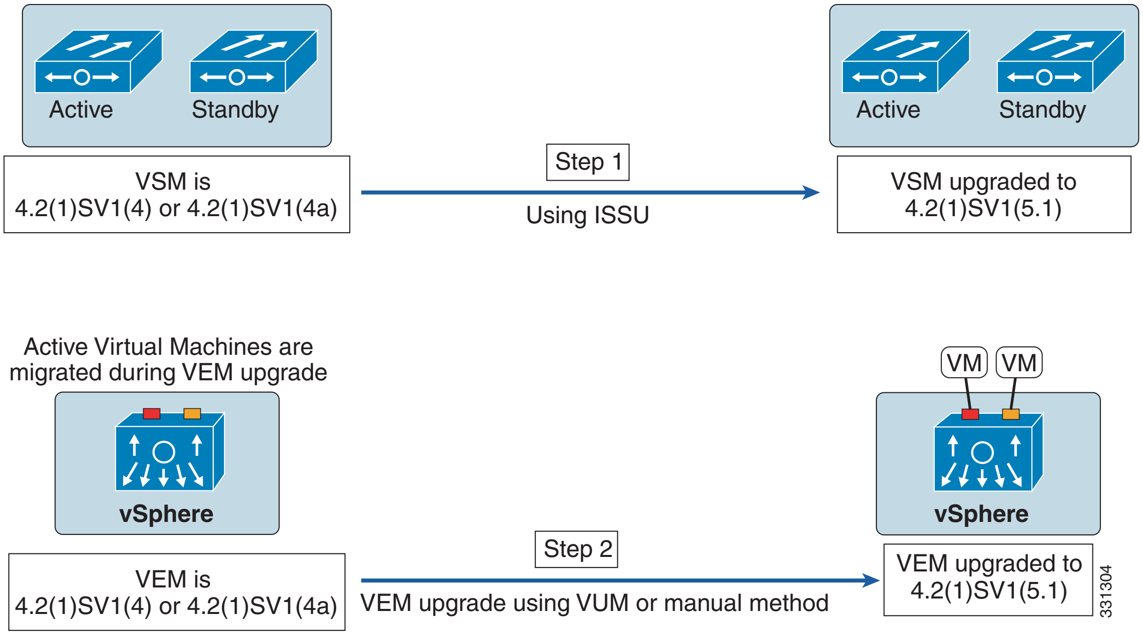
- You can abort the upgrade procedure by pressing **Ctrl-C**.

PROCEDURE

Step 1 Upgrade the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1). For this procedure, see the "Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)" section on page 7-17. See Figure 7-1.

Step 2 Upgrade the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1). For this procedure, see the "Upgrading the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)" section on page 7-26. See Figure 7-1.

Figure 7-1 Upgrading from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)


Active
Standby
VSM is
4.2(1)SV1(4) or 4.2(1)SV1(4a)
Step 1
Using ISSU
Active
Standby
VSM upgraded to
4.2(1)SV1(5.1)
Active Virtual Machines are
migrated during VEM upgrade
vSphere
VEM is
4.2(1)SV1(4) or 4.2(1)SV1(4a)
Step 2
VEM upgrade using VUM or manual method
VM
VM
vSphere
VEM upgraded to
4.2(1)SV1(5.1)
331304

Upgrading the VSMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)

This section includes the following topics:

- Software Images, page 7-17
- In-Service Software Upgrades on Systems with Dual VSMs, page 7-17
- Upgrading a System with Dual VSMs Using ISSU, page 7-19
- Upgrading a System with Dual VSMs, page 7-19

Software Images

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

- Software images—The kickstart, system, and VSM Policy-Agent 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.
- VSM—There are single or dual VSMs.

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
- VSM Policy-Agent image
- VEM images

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

Figure 7-2 shows the ISSU process.

Figure 7-2 ISSU Process

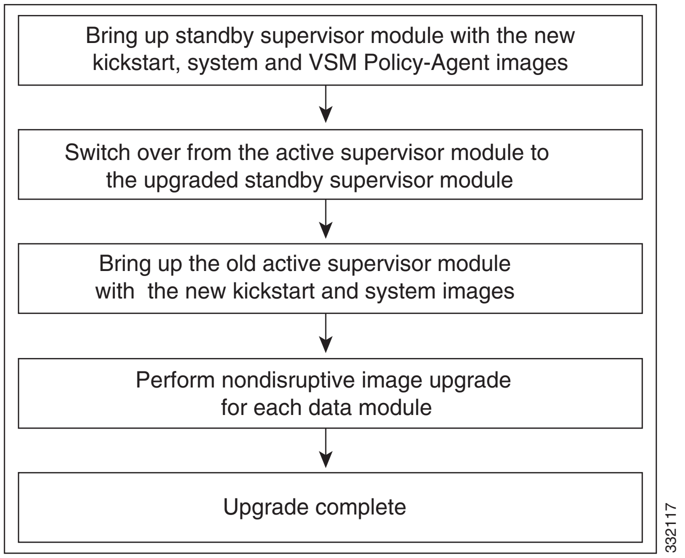
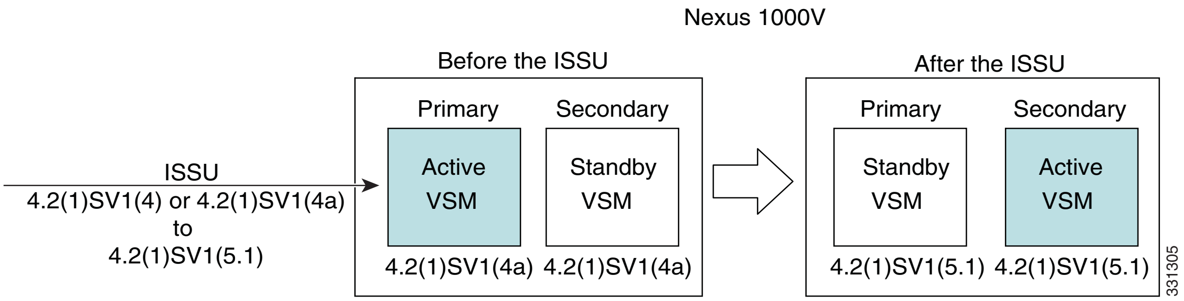

Bring up standby supervisor module with the new kickstart, system and VSM Policy-Agent images
Switch over from the active supervisor module to the upgraded standby supervisor module
Bring up the old active supervisor module with the new kickstart and system images
Perform nondisruptive image upgrade for each data module
Upgrade complete
332117

Figure 7-3 provides an example of the VSM status before and after an ISSU switchover.

Figure 7-3 Example of an ISSU VSM Switchover



Upgrading a System with Dual VSMs Using ISSU

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, system, and VSM Policy-Agent 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.

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

- You can upgrade the VSM by using just one 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 only see the progress 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 a System with Dual VSMs

This section describes how to upgrade to the latest Cisco Nexus 1000V software on systems with dual VSMs.

PROCEDURE

Step 1 Log in to the active VSM.

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

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

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

Step 4 Navigate to the download site for your system.

You see links to the download images for your switch.

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

Step 6 Download the vnmc-vsmpa image.

Step 7 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 8 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 9 Delete any unnecessary files to make space available if you need more space on the standby VSM.

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

Step 10 If you plan to install the images from the bootflash:, copy the Cisco Nexus 1000V kickstart, system, and VSM Policy-Agent 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, system, and VSM Policy-Agent images.

```
switch# copy
scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin
bootflash:nexus-1000v-kickstart-4.2.1.SV1.5.1.bin

switch# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-4.2.1.SV1.5.1.bin
bootflash:nexus-1000v-4.2.1.SV1.5.1.bin

switch# copy scp://user@scpserver.cisco.com/downloads/vnmc-vsmpa.1.3.1b.bin
bootflash:vnmc-vsmpa.1.3.1b.bin
```

Step 11 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-4.2.1.SV1.5.1.bin system
bootflash:nexus-1000v-4.2.1.SV1.5.1.bin

Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin.
[####################] 100% -- SUCCESS

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



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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           4.2(1)SV1(4a)            4.2(1)SV1(5.1)           yes
     1   kickstart           4.2(1)SV1(4a)            4.2(1)SV1(5.1)           yes
     2      system           4.2(1)SV1(4a)            4.2(1)SV1(5.1)           yes
     2   kickstart           4.2(1)SV1(4a)            4.2(1)SV1(5.1)           yes

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

Step 12 Read the release notes for the related image file. See the *Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.1)*.

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, Release 4.2(1)SV1(5.1)*.

Step 15 Perform the upgrade on the active VSM using the kickstart, system, and VSM Policy-Agent images.

- Upgrade using the kickstart, system, and VSM Policy-Agent images.

```
switch# install all kickstart bootflash:nexus-1000v-kickstart-mz.4.2.1.SV1.5.1.bin
system bootflash:nexus-1000v-mz.4.2.1.SV1.5.1.bin
vnmpa bootflash:vnmc-vnmpa.1.3.1b.bin
```

```
Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin for boot variable "system".
[####################] 100% -- SUCCESS

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

Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin.
[####################] 100% -- SUCCESS

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



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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           4.2(1)SV1(4a)           4.2(1)SV1(5.1)           yes
     1   kickstart           4.2(1)SV1(4a)           4.2(1)SV1(5.1)           yes
     2      system           4.2(1)SV1(4a)           4.2(1)SV1(5.1)           yes
     2   kickstart           4.2(1)SV1(4a)           4.2(1)SV1(5.1)           yes


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

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

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

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

```
Install is in progress, please wait.

Syncing image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin to standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin to standby.
[####################] 100% -- SUCCESS

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

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

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

```
Continuing with installation, please wait

Module 2: Waiting for module online
-- SUCCESS

Install has been successful
```

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

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

Software
  loader:    version unavailable [last: loader version not available]
  kickstart: version 4.2(1)SV1(5.1) [build 4.2(1)SV1(5.1)]
  system:    version 4.2(1)SV1(5.1) [build 4.2(1)SV1(5.1)]
  kickstart image file is: bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin
  kickstart compile time:  1/11/2012 3:00:00 [01/11/2012 12:49:49]
  system image file is:    bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin
  system compile time:     1/11/2012 3:00:00 [01/11/2012 13:42:57]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU         with 2075740 kB of memory.
  Processor Board ID T5056B1802D
  Device name: Nexus1000v
  bootflash:    1557496 kB

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


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
...
switch# show vnmc-vnmpa status
VSM Policy-Agent status is - Installed Successfully. Version 1.3(1b)-vsm
switch#
```

Step 18 Display the log of the last installation.

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

Verifying image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin for boot variable
"kickstart".

 -- SUCCESS

Verifying image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin for boot variable "system".

 -- SUCCESS

Verifying image type.

 -- SUCCESS

Extracting "system" version from image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin.

 -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin.

 -- SUCCESS

Notifying services about system upgrade.

 -- SUCCESS


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



Images will be upgraded according to following table:
Module       Image         Running-Version             New-Version  Upg-Required
------  ----------  ----------------------  ----------------------  ------------
     1      system           4.2(1)SV1(4a)          4.2(1)SV1(5.1)           yes
     1   kickstart           4.2(1)SV1(4a)          4.2(1)SV1(5.1)           yes
     2      system           4.2(1)SV1(4a)          4.2(1)SV1(5.1)           yes
     2   kickstart           4.2(1)SV1(4a)          4.2(1)SV1(5.1)           yes


Images will be upgraded according to following table:
```

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


Install is in progress, please wait.

Syncing image bootflash:/nexus-1000v-kickstart-4.2.1.SV1.5.1.bin to standby.
 -- SUCCESS

Syncing image bootflash:/nexus-1000v-4.2.1.SV1.5.1.bin to standby.
 -- SUCCESS

Setting boot variables.
 -- SUCCESS

Performing configuration copy.
 -- SUCCESS

Module 2: Waiting for module online.
 -- SUCCESS

Notifying services about the switchover.
 -- SUCCESS


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

switch# attach module 2
Attaching to module 2 ...
To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(standby)#
switch(standby)# show in
incompatibility   install           interface         inventory
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 the VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)

This section describes how to upgrade VEMs from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)and includes the following topics:

- Choosing a VEM Software Upgrade Procedure, page 7-26
- Upgrading the VEMs Using VMware Update Manager from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-28
- Upgrading the VEMs Manually from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1), page 7-31

Choosing a VEM Software Upgrade Procedure

This section describes how you can upgrade the ESX/ESXi host with the VEM software installed or install or upgrade the VEM software.

Figure 7-4 and Figure 7-5 show recommended workflows depending on the version of Cisco Nexus 1000V software that you have installed. These workflows are for stateful ESXi hosts. For information on stateless ESXi hosts, see Chapter 2, “Installing the VEM Software on a Stateless ESXi Host” section in the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_install.html#wp1177567.

Figure 7-4 describes the upgrade workflow with Cisco Nexus 1000V Release 4.2(1)SV1(4) or SV1(4a) installed.

Figure 7-4 Workflow with a Cisco Nexus 1000V Version 4.2(1)SV1(4) or SV1(4a) Installed

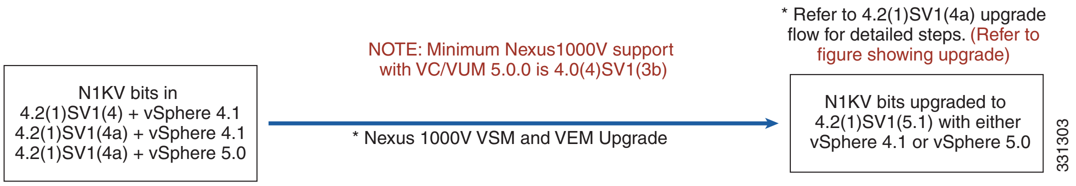
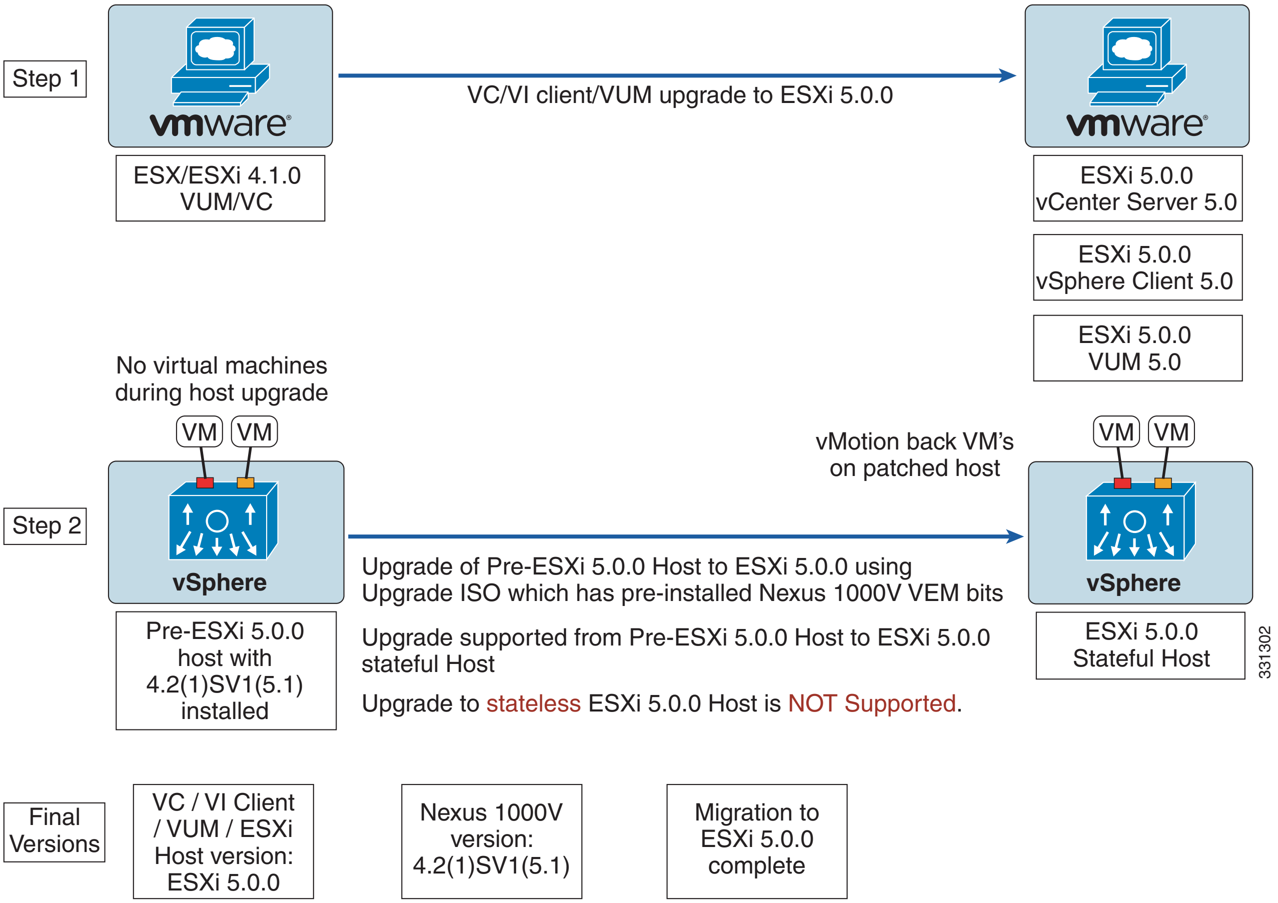

N1KV bits in
4.2(1)SV1(4) + vSphere 4.1
4.2(1)SV1(4a) + vSphere 4.1
4.2(1)SV1(4a) + vSphere 5.0
NOTE: Minimum Nexus1000V support with VC/VUM 5.0.0 is 4.0(4)SV1(3b)
* Nexus 1000V VSM and VEM Upgrade
* Refer to 4.2(1)SV1(4a) upgrade flow for detailed steps. (Refer to figure showing upgrade)
N1KV bits upgraded to 4.2(1)SV1(5.1) with either vSphere 4.1 or vSphere 5.0
331303

Figure 7-5 describes the upgrade workflow with Cisco Nexus 1000V Release 4.2(1)SV1(5.1) installed and you are upgrading from VMware 4.1 to 5.0.

Figure 7-5 Workflow with Cisco Nexus 1000V 4.2(1)SV1(5.1) Installed and Upgrading ESX from 4.1 to 5.0



You can upgrade the ESX/ESXi host as follows:

Note The upgrade ISO can be generated by using the procedure in the "Creating an Upgrade ISO with a VMware ESX Image and a Cisco Nexus 1000V VEM Image" section of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_upgrade_vmware.html#wp706205

- Upgrading the ESX/ESXi host with VEM software installed.
- If you are using VUM to upgrade the host:
  - Prior to VMware vSphere 5.0, you must create a host patch baseline and include the appropriate VMware patch or update bulletins and the corresponding Cisco Nexus 1000V VEM bulletin in the baseline. You can then upgrade the host by applying the baseline to the host and remediating.

  - If you are using the vCLI, enter the **vihostupdate** command or the **esxupdate** command. For more information, see the "Installing ESXi 5.0.0 Host Software Using the CLI" section. See Appendix A, "Installing and Upgrading VMware" of the *Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)* at http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_1/install_upgrade/vsm_vem/guide/n1000v_installupgrade_upgrade_vmware.html#wp635033.

- Upgrading the VEM software
  - When VEM upgrades are triggered from the VSM, the VEM software is automatically upgraded on the host.
  - If you are using the vCLI, enter the **vihostupdate** command or the **esxupdate** command. For more information, see the "Upgrading the VEM Software Using the CLI" section on page 7-35.

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

The following section describes how to update the Cisco Nexus 1000V from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1)by using the VUM.

PROCEDURE

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

Step 1 Display the current configuration.

```
switch (config)# 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: VEM400-201107031-RG
    DVS: VEM400-201101030-BG
```

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

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

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

Step 3 Verify that the upgrade notification was sent.

```
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade VEM Image
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Sun May 9 22:04:54 2010
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
```

```
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201101030-BG
```

Note Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1)*.

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

For more information about how the server administrator accepts the VEM upgrade, see the "Accepting the VEM Upgrade in vCenter Server" section on page 7-34.

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

```
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Sun May 9 22:04:54 2010
Upgrade Status Time(vCenter):  Tue May 11 07:42:32 2010
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201101030-BG
```

Note Verify that the Upgrade Status contains the highlighted text. If the text is not present, check the Upgrade Error line and see the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1)*.

Step 5 Initiate the VUM upgrade process.

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

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

```
switch# vmware vem upgrade proceed
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade VEM Image
Upgrade Status: Upgrade In Progress in vCenter
Upgrade Notification Sent Time: Wed Mar 17 15:19:05 2010
Upgrade Status Time(vCenter): Wed Mar 17 17:28:46 2010
Upgrade Start Time: Wed Mar 17 15:20:06 2010
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201107031-RG
```

Note The DVS bundle ID is updated and is highlighted.

Note If the ESX/ESXi host is using ESX/ESXi 4.1.0 or later releases and your DRS settings are enabled to allow it, VUM automatically vMotions the VMs from the host to another host in the cluster and places the ESX/ESXi in maintenance mode to upgrade the VEM. This process is continued for other hosts in the DRS cluster until all the hosts are upgraded in the cluster.

Step 6 Check for the upgrade complete status.

```
switch# show vmware vem upgrade status
Upgrade VIBs: System VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Wed Mar 17 15:19:05 2010
Upgrade Status Time(vCenter): Wed Mar 17 17:28:46 2010
Upgrade Start Time: Wed Mar 17 15:20:06 2010
Upgrade End Time(vCenter): Wed Mar 17 17:30:48 2010
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201107031-RG
```

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

```
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade 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: VEM400-201107031-RG
    DVS: VEM400-201107031-RG
```

Step 8 Verify that the upgrade process is complete.

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

Mod  Sw               Hw
---  ---------------  ------
1    4.2(1)SV1(5.1)     0.0
2    4.2(1)SV1(5.1)     0.0
3    4.2(1)SV1(5.1)     VMware ESXi 5.0.0 Releasebuild-260247 (2.0)
4    4.2(1)SV1(5.1)     VMware ESXi 5.0.0 Releasebuild-260247 (2.0)

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    10.78.109.100    NA                                    NA
2    10.78.109.100    NA                                    NA
```

```
3    10.78.109.104    1ee15784-f2e8-383e-8132-9026577ca1bb  10.78.109.104
4    10.78.109.102    44454c4c-4700-104e-804d-cac04f563153  10.78.109.102
* this terminal session
```

Note The line with the bold characters in the preceding example displays that all VEMs are upgraded to Release 4.2(1)SV1(5.1).

Step 9 The upgrade is complete.

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

The following section describes how to upgrade Cisco Nexus 1000V from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.1) manually.

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

Note If VUM is installed, it should be disabled.

To manually install or upgrade the Cisco Nexus 1000V VEM on an ESX/ESXi host by following the steps in the "Upgrading the VEM Software Using the CLI" section on page 7-35.

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

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

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

PROCEDURE

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

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

Step 2 Verify that the upgrade notification was sent.

```
switch (config)# show vmware vem upgrade status
Upgrade Status: Upgrade Availability Notified in vCenter
Upgrade Notification Sent Time: Sun May  9 22:04:54 2010
Upgrade Status Time(vCenter):
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201101030-RG
```

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

For details about the server administrator accepting the VEM upgrade, see the "Accepting the VEM Upgrade in vCenter Server" section on page 7-34.

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

```
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade VEM Image
Upgrade Status: Upgrade Accepted by vCenter Admin
Upgrade Notification Sent Time: Sun May  9 22:04:54 2010
Upgrade Status Time(vCenter): Tue May 11 07:42:32 2010
Upgrade Start Time:
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201101030-BG
```

Step 4 Perform on of the following:

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

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

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

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

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

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

```
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade VEM Image
Upgrade Status: Upgrade in Progress in vCenter
Upgrade Notification Sent Time: Wed Mar 17 15:19:05 2010
Upgrade Status Time(vCenter): Wed Mar 17 17:28:46 2010
Upgrade Start Time: Wed Mar 17 15:20:06 2010
Upgrade End Time(vCenter):
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201107031-RG
```

Step 6 Check for the Upgrade Complete status.

```
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade VEM Image
Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Wed Mar 17 15:19:05 2010
Upgrade Status Time(vCenter): Wed Mar 17 17:28:46 2010
Upgrade Start Time: Wed Mar 17 15:20:06 2010
Upgrade End Time(vCenter): Wed Mar 17 17:28:48 2010
Upgrade Error:
Upgrade Bundle ID:
    VSM: VEM400-201107031-RG
    DVS: VEM400-201107031-RG
```

Step 7 Coordinate with and wait until the server administrator upgrades all ESX host VEMs with the new VEM software release and informs you that the upgrade process is complete.

The server administrator performs the manual upgrade using the **vihostupdate** command or the **esxcli** command. For more information, see the "Upgrading the VEM Software Using the CLI" section on page 7-35.

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

```
switch# vmware vem upgrade complete
switch# show vmware vem upgrade status
Upgrade VIBs: Upgrade 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: VEM400-201107031-RG
    DVS: VEM400-201107031-RG
```

Step 9 Verify that the upgrade process is complete.

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

Mod  Sw               Hw
---  ---------------  ------
1    4.2(1)SV1(4a)     0.0
2    4.2(1)SV1(4a)     0.0
3    4.2(1)SV1(5.1)     VMware ESXi 4.1.0 Releasebuild-260247 (2.0)
4    4.2(1)SV1(5.1)     VMware ESXi 4.1.0 Releasebuild-260247 (2.0)

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    10.78.109.100    NA                                    NA
2    10.78.109.100    NA                                    NA
3    10.78.109.104    1ee15784-f2e8-383e-8132-9026577ca1bb  10.78.109.104
4    10.78.109.102    44454c4c-4700-104e-804d-cac04f563153  10.78.109.102
* this terminal session
```

Note The line with the bold characters in the preceding example display that all VEMs are upgraded to Release 4.2(1)SV1(5.1).

Step 10 Run the VSM backup procedure.

See the “Configuring VSM Backup and Recovery” chapter of the *Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*.

The upgrade is complete.

Accepting the VEM Upgrade in vCenter Server

This section describes the steps that a server administrator follows to accept a VEM upgrade in vCenter Server.

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

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

Accepting the VEM Upgrade

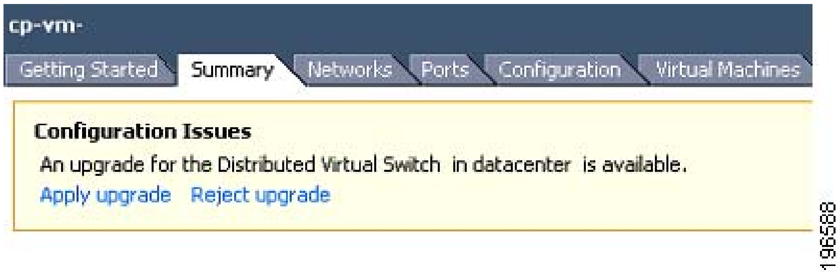
The server administrator accepts the VEM upgrade after the network administrator has upgraded the VSM and notified vCenter server of the availability of the new VEM software version.

Note This procedure is performed by the server administrator.

Step 1 In vCenter Server, choose Inventory > Networking.

Step 2 Click the **vSphere Client DVS Summary** tab to check for the availability of a software upgrade (see Figure 7-6).

Figure 7-6 vSphere Client DVS Summary Tab



Configuration Issues

An upgrade for the Distributed Virtual Switch in datacenter is available.

Step 3 Click **Apply upgrade**.

The following actions occur:

- The network administrator is notified that you are ready to apply the upgrade to the VEMs.
- The network administrator notifies vCenter to proceed with the VEM upgrades.

- If you are using VUM, vCenter locks the DVS and triggers VUM to upgrade the VEMs.

Upgrading the VEM Software Using the CLI

You can upgrade the Cisco Nexus 1000V VEM software on an ESX/ESXi host by using the CLI.

BEFORE YOU BEGIN

Before starting the procedure, you must know or do the following:

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

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

- If you are using the **esxupdate** command:
  - You are logged in to the ESX host.
- Check the *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*, for compatible versions.
- You have already copied the VEM software installation file to the /tmp directory.
- You know the name of the VEM software file to be installed.

PROCEDURE

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

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

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

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

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

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

```
[root@serialport tmp]# vihostupdate --install --bundle VEM400-201107401.zip --server
192.0.2.0
Enter username: root
Enter password:
```

```
Please wait installation in progress …
The update completed successfully, but the system needs to be rebooted for the changes
to be effective.
[root@serialport tmp]#
```

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

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

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

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

Step 3 Display values with which to compare to *Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(5.1)*.

```
[root@serialport tmp]# vmware -v
VMware ESXi 5.0.0 build-469512
```

The highlighted text shows the upgraded Cisco VEM.

```
root@serialport tmp]# esxupdate query
-----Bulletin ID----- -----Installed----- ----------Summary----------
ESXi400-Update01      2011-07-28T14:30:58 VMware ESXi 4.0 Update 1
VEM400-201107273451115-BG  2011-07-28T14:48:36 Cisco Nexus 1000V 4.2(1)SV1(4a)
[root@host212 ~]# vem status -v
Package vssnet-esx4.1.0-00000-release
Version 4.2.1.1.4.1.0-1.9.1
Build 1
Date Wed Jul 27 04:42:14 PDT 2011

Number of PassThru NICs are 0
VEM modules are loaded

Switch Name     Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0        32          2           32                1500    vmnic0
DVS Name        Num Ports   Used Ports  Configured Ports  Uplinks
byru-215        256         56          256               vmnic2,vmnic1

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

[root@host212 ~]# vem version -v
Number of PassThru NICs are 0
Running esx version -208167 x86_64
VEM Version: 4.2.1.1.4.1.0-1.9.1
VSM Version: 4.2(1)SV1(4a)
System Version: VMware ESX 4.0.0 Releasebuild-208167
```

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

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

```
1     4.0(4)SV1(5.1)     0.0
2     4.0(4)SV1(5.1)     0.0
3     4.2(1)SV1(5.1)    VMware ESXi 4.0.0 build-208167 (1.9)

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

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
1    10.104.62.220    NA                                    NA
4    10.104.62.217    3fa746d4-de2f-11de-bd5d-c47d4f7ca460  visor
```

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

Step 5

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

You have completed this procedure.

Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(5.1)

Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)VSG1(3.1) is a two-step process.

1. See the "Upgrading from Releases 4.0(4)SV1(3, 3a, 3b, 3c, 3d) to Release 4.2(1)SV1(4a)" section in the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4a)*.
2. See the "Upgrading to Release 4.2(1)SV1(5.1)" section on page 7-13.

APPENDIX A

Examples of Cisco VNMC OVA Template Deployment and Cisco VNMC ISO Installations

This appendix provides example procedures for OVF and ISO installations.

This appendix includes the following sections:

OVA Installation Using vSphere 4.0 Installer

You can perform an OVA installation using vSphere 4.0 Installer.

BEFORE YOU BEGIN

- Before starting the procedure, you must know or do the following:
- Ensure that you have the VSM IP address available.
- Ensure that you have all the proper networking information available, including the IP address you will use for your VNMC instance.

PROCEDURE

Step 1 Open your vSphere client.

Step 2 Click **Hosts and Clusters** and choose a host.

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

The Deploy OVF Template dialog box appears. In the dialog box, choose an .ova file on your local machine, or choose a file from another location (URL).

Step 4 Click **Deploy from File**.

Step 5 Click **Browse**.

The Open dialog box appears.

Step 6 From the Open dialog box, choose the appropriate .ova file and click **Open**.

Step 7 Click **Next**.

The OVF Template Details page appears inside the Deploy OVF Template dialog box. The OVF Template Details page is the first of six pages in the Deploy OVF Template dialog box that you use to set parameters for the Cisco VNMC instance.

Step 8 View your template details and click **Next**.

The End User License Agreement page appears.

Step 9 View the license and click **Accept**.

Step 10 Click **Next**.

The Name and Location page appears.

Step 11 In the Name field, enter a template name.

Step 12 In the Inventory Location area, choose the appropriate folder.

Step 13 Click **Next**.

The VNMC Installer page appears.

Step 14 From the Configuration drop-down list, choose **VNMC Installer**.

Step 15 Click **Next**.

Step 16 Choose the appropriate network and click **Next**.

The Properties page appears.

Step 17 In the IP Address area, enter an IP address in the IPv4 IP Address field and a gateway address in the IPv4 Gateway field.

Note The netmask is defaulted to 255.255.255.0.

Step 18 (Optional) In the VNMC DNS area, enter an IP address in the DNS field.

Step 19 In the VNMC DNS area, enter a hostname in the Host Name field and a domain name in the Domain Name field.

Step 20 In the VNMC Password area, enter a password in the Password field or the Secret field.

Note You enter the admin password in the Password field.

Step 21 Verify that any value is entered in the following fields of the VNMC Restore area:

a. RestoreFile

b. RestoreIP

c. RestorePassword

d. RestoreProto

e. RestoreUser

Step 22 Click **Next**.

The Ready to Complete page appears.

Step 23 View your installation settings and click **Finish**.

The progress dialog box appears. Once the virtual machine is installed, the Deployment Completed Successfully dialog box appears.

Step 24 Click **Close**.

The Cisco VNMC instance is created.

OVA Installation Using an ISO Image

You can perform an OVA installation using an ISO image.

PROCEDURE

Step 1 Download a Cisco VNMC 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 20 GB.

b. Ensure your virtual machine has 2 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 pressing **Ctrl+Alt+Del**.

The ISO installer appears.

Step 7 Enter the appropriate values in the ISO installer.

Step 8 Once installation is completed, click **Reboot**.

The Cisco VNMC instance is created.

INDEX