Send document comments to vsg-docfeedback@cisco.com

Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide

July 3, 2013

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-24126-04

Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide

Send document comments to vsg-docfeedback@cisco.com

CONTENTS

Send document comments to vsg-docfeedback@cisco.com

Send document comments to vsg-docfeedback@cisco.com

Preface

The *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide* provides procedures for installing Cisco Virtual Security Gateway (VSG) and Cisco Virtual Network Management Center (VNMC).

This preface includes the following topics:

Audience

This guide is for the following professionals with an understanding of virtualization and experience using VMware tools such as vCenter and vSphere 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 (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 Cisco Virtual Security Gateway and Cisco Virtual Network Management Center	Provides procedures for installing VNMC and VSG. This part of the document should be followed for a first-time installation or for someone new to Cisco VNMC or VSG.

Send document comments to vsg-docfeedback@cisco.com

Part	Title	Description
Part 2	Installation Guide for Cisco Virtual Security Gateway	Provides more details on the procedures to install the Cisco VSG.
Part 3	Installation Guide for Cisco Virtual Network Management Center	Provides more details on the procedures to install the 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 Cisco VNMC and 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.

Send document comments to vsg-docfeedback@cisco.com

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(1)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(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

- *Release Notes for Cisco Virtual Network Management Center, Release 1.0.1*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.0.1*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.0.1*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.0.1*

Send document comments to vsg-docfeedback@cisco.com

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 HA (High Availability).

This chapter includes the following sections:

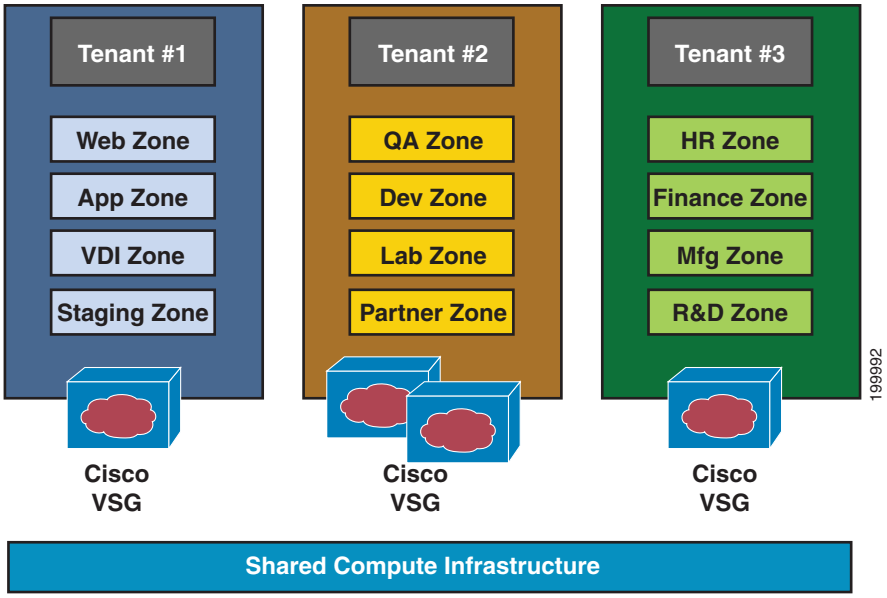
Information About Installing the Cisco Virtual Network Management Center and the Cisco Virtual Security Gateway

The Cisco Virtual Network Management Center (Cisco VNMC) and the Cisco Virtual Security Gateway (Cisco VSG) must be installed in a particular sequence 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.

Information About Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway (VSG) for the Cisco Nexus 1000V Series switch 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 multi-tenancy. 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 distributed virtual switch in the VMware vSphere Hypervisor, and the Cisco VSG leverages the virtual network service data path (vPath) that is embedded in the Nexus 1000V virtual ethernet module (VEM) (see Figure 1-2). vPath steers traffic, whether external-to-VM or VM-to-VM, to the Cisco VSG of a tenant. A split-processing model is applied where initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement. After the policy decision is made, the Cisco VSG off-loads policy enforcement of the remaining packets to vPath.

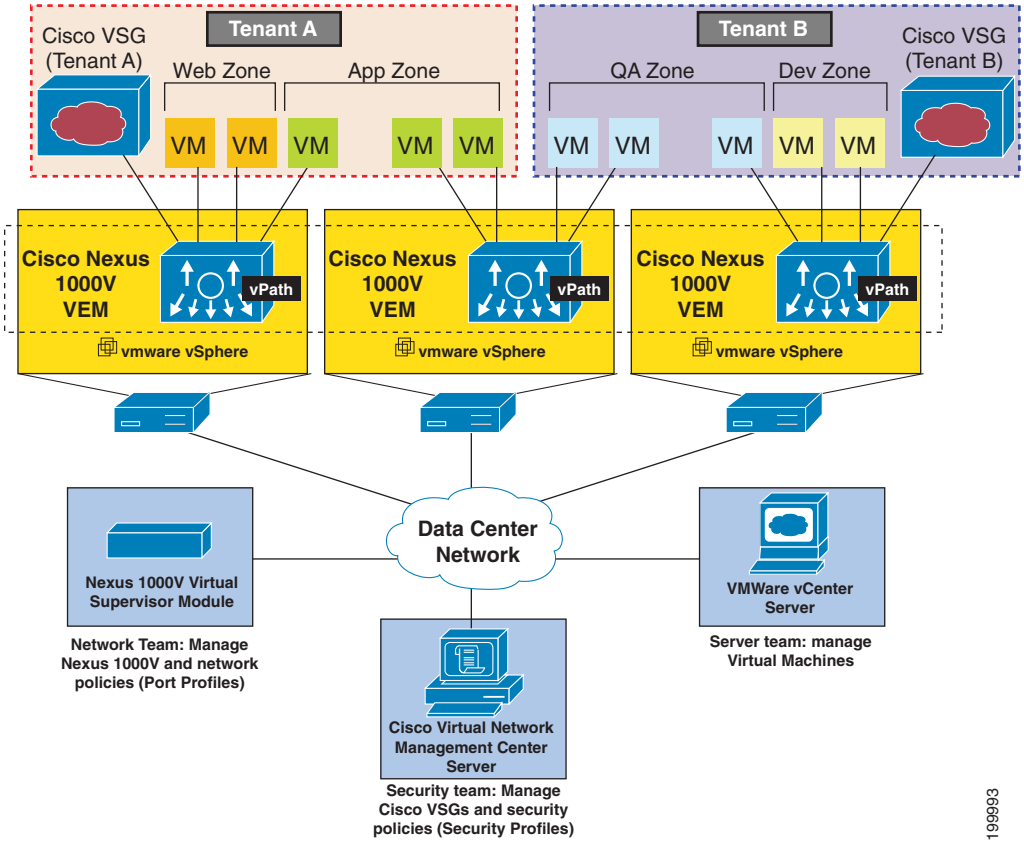
vPath supports the following features:

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

The Cisco VSG and Cisco Nexus 1000V VEM provide the following benefits (see Figure 1-3):

- Each Cisco VSG can protect across multiple physical servers, which eliminates the need for you to deploy one virtual appliance per physical server.
- By offloading the fast-path to one or more Cisco Nexus 1000V VEM vPath modules, the Cisco VSG enhances performance through distributed vPath-based enforcement.
- You can insert the Cisco VSG in one-arm mode without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling is based on security profiles not on vNICs that are limited for virtual appliances, which 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 the security operations team can allocate the maximum compute capacity to application workloads. This feature enables capacity planning to occur independently across server and security teams, and operational segregation across security, network, and server teams.

Figure 1-2 Cisco Virtual Security Gateway Deployment Topology



Trusted Multitenant Access

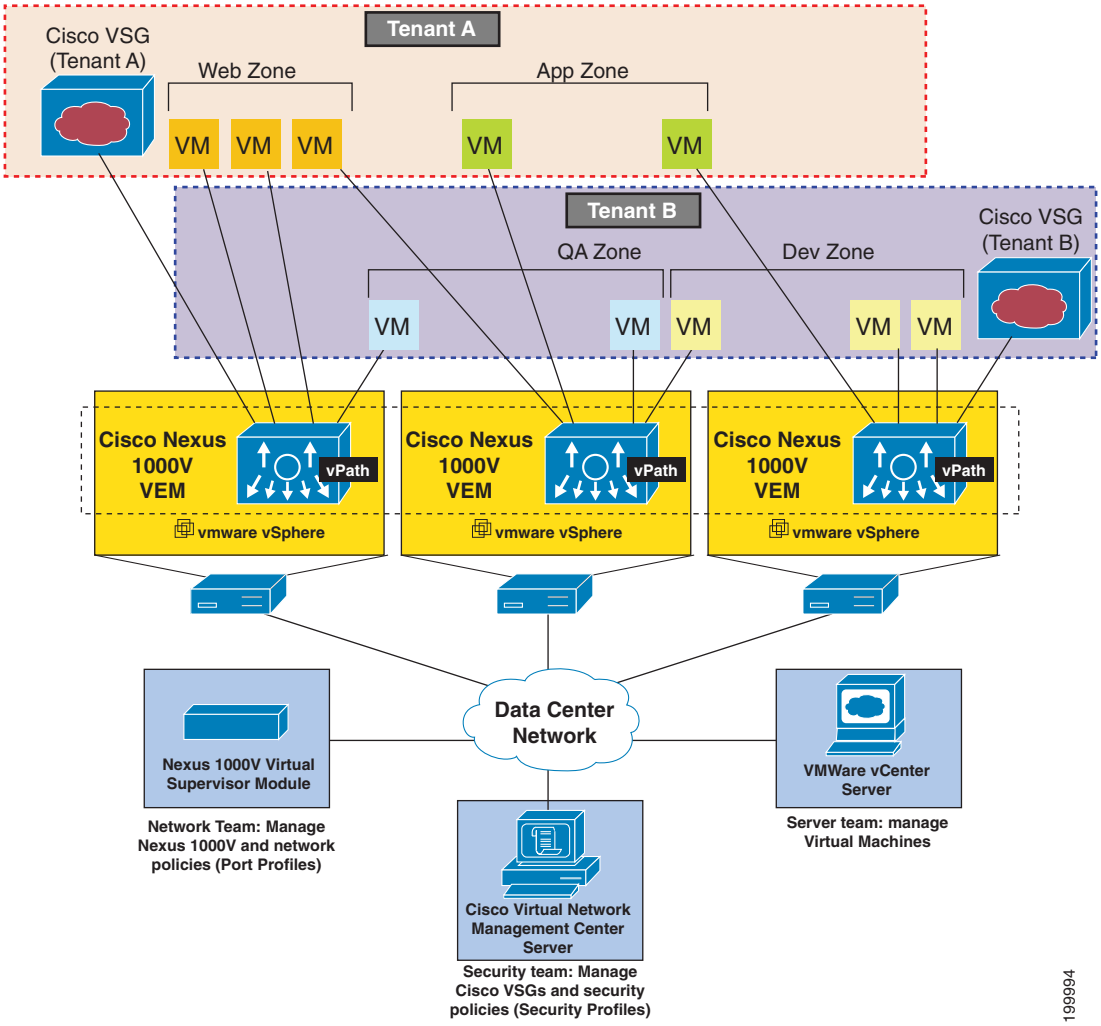
You can transparently insert a Cisco VSG into the VMware vSphere environment where the Cisco Nexus 1000V is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic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

As VMs are instantiated for a given tenant, their association to security profiles and hence zone membership occurs immediately through binding with the Nexus 1000V port profile. Each VM is hence 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. Controls are applied to zone-to-zone traffic as well as to external-to-zone (and zone-to-external) traffic. Zone-based enforcement can occur within a VLAN because a VLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then off-loads enforcement to the Nexus 1000V VEM vPath module for performance optimization. Upon enforcement, action can be taken to permit or deny access and optional access logs can be generated. 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 especially across VMs. Live migration of VMs can occur due to manual or programmatic vMotion events. Figure 1-3 shows how a structured environment of Figure 1-2 can change over time due to this dynamic VM environment.

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. Typically, when you create a tenant with the Cisco VSG (standalone or active-standby pair) on the Cisco Virtual Network Management Center (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, security controls are immediately applied. A VM can be repurposed by assigning a different port profile or security profile.

As vMotion events are triggered, VMs move across physical servers. Since 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 Cisco VSG and VLAN Usages

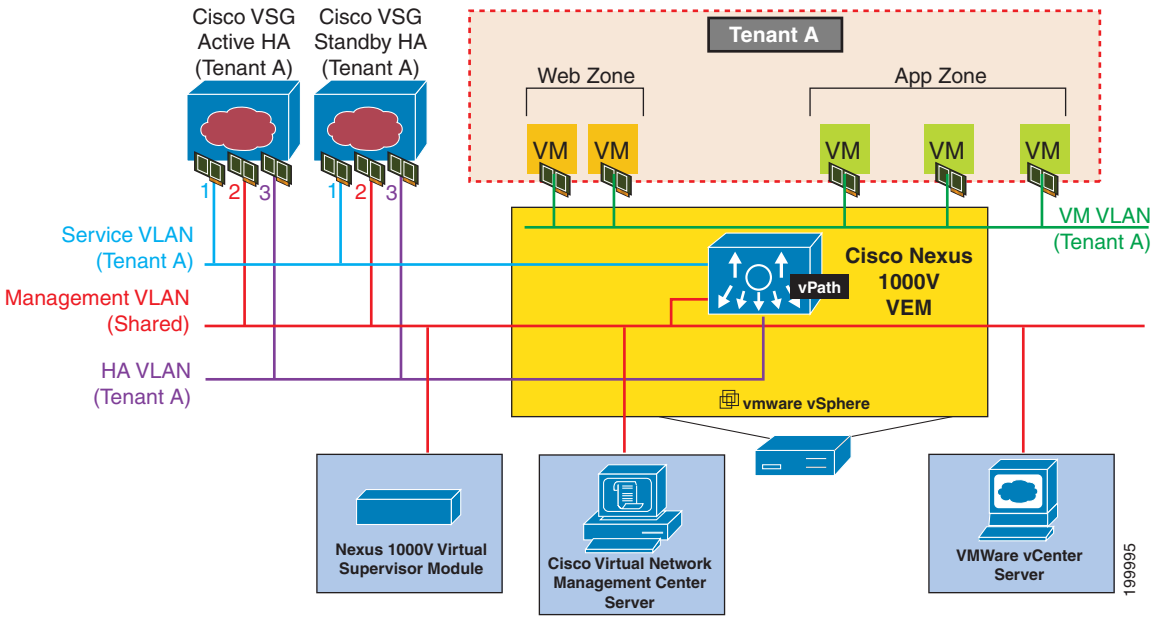
The Cisco VSG is set up in an overlay fashion so that VMs can reach a Cisco VSG irrespective of its location. The vPath component in the Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to the Cisco VSG for further processing.

Figure 1-4 shows Cisco VSGs in a typical arrangement. In the figure, the Cisco VSG has connectivity 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, and 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 betweenthe VSGs. The Cisco VSG vNICs are part of the HA VLAN.

You can allocate one or more VM data VLAN(s) 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

Cisco VNMC is a virtual appliance, based on Red Hat Enterprise Linux (RHEL), that provides centralized device and security policy management of the Cisco Virtual Security Gateway (VSG) for the Cisco Nexus 1000V Series switch. Designed for multitenant operation, 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, Cisco VNMC enables you to manage Cisco VSGs that are deployed throughout the data center from a centralized location.

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.

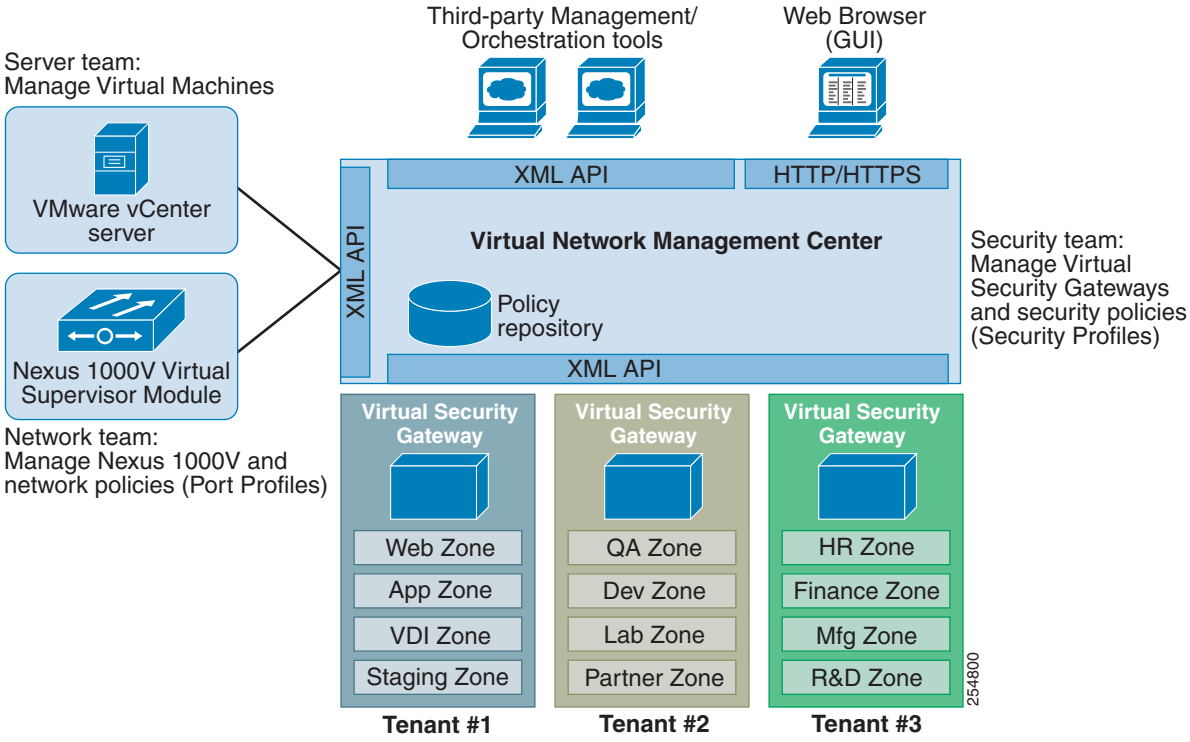
This section includes the following topics:

Cisco VNMC Components

This section includes the following topics:

Figure 1-5 shows the Cisco VNMC components.

Figure 1-5 Cisco VNMC Components



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.
- Nondisruptive administration model that enables greater collaboration across security and server administrators, while maintaining administrative separation and reducing administrative errors.

Cisco VNMC Architecture

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 because:
  - 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

An important component of the Cisco VNMC is the XML API, which 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 Virtual Supervisor Module (VSM) to achieve the following scenarios:

- Security administrators author and manage security profiles as well as manage Cisco VSG instances. Security profiles are referenced in Cisco Nexus 1000V port profiles via the Cisco VNMC interface.
- Network administrators author and manage port profiles as well as manage Cisco Nexus 1000V switches. Port profiles are referenced in vCenter via the Cisco Nexus 1000V VSM interface.
- Server administrators 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 64-bit processor listed in the VMware compatibility matrix
- Intel VT is enabled in the BIOS
- VMware ESX 4.0, 4.0 U1, 4.0 U2 or 4.1
- VMware vSphere Hypervisor
- VMware vCenter 4.0, 4.0 U1, 4.0 U2 or 4.1
- 2-GB memory reserved for each Cisco VNMC installation
- Datastore with at least 25-GB disk space available on shared NFS/SAN storage when Cisco VNMC is deployed in an HA cluster
- Internet Explorer 7.0 or Mozilla Firefox 3.6.x on Windows
- Flash 10.0 or 10.1

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. The express install wizard appears.

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. 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 refer to the VMware HA and Fault Tolerance guide.

PART 1

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

CHAPTER 2

Quick Start Guide for Cisco Virtual Security Gateway and 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:

- Basic Hardware and Software Requirements
- Preparation of the Cisco Nexus 1000V Series Switch for Further Installation Processes
- Your Cisco VNMC and Cisco VSG Information for Use Later During Installation

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 is enabled in the BIOS	
3	VMware ESX 4.0, 4.0 U1, 4.0 U2 or 4.1	
4	ESX/ESXi platform that runs VMware software release 4.0.0 or 4.1.0 with a minimum of 4-GB physical RAM for VSG and similar for VNMC or 6-GB for both.	
5	VMware vSphere Hypervisor	
6	VMware vCenter 4.0, 4.0 U1, 4.0 U2 or 4.1	
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 Cisco VNMC is deployed in an HA cluster	
10	Internet Explorer 7.0 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 are configured on the Cisco Nexus 1000V Series switch uplink ports: the service VLAN and an HA VLAN (the VLAN do not need to be the system VLAN)	
2	Two port profiles are configured on the Cisco Nexus 1000V Series switch: one for the service VLAN and one 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 Particulars Checklist

Task	Task Description	Task Particulars	Completed
1	Installing 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 Cisco VNMC • The admin password and hostname that you want to use • The shared secret password 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 one 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) • 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 (it will look like `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 • 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.	

Task	Task Description	Task Particulars	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 created on VSM • Management port-profile (management) **Note** The management port profile is the same one 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/SubnetMask/Gateway information for Cisco VSG • Admin password • 2-GB RAM and 3-GB hard disk space • Cisco VNMC IP • Shared secret password • IP connectivity between Cisco VSG and 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	—	
7	On the Cisco VNMC, Configuring a Tenant and Security Profile	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	
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		

Task	Task Description	Task Particulars	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 (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 port-profile (pp-webserver) configured for firewall protection. • Log in to any of your client VM (Client-VM) and send traffic (for example, HTTP) to your Server-VM. • Check the policy-engine statistics and log on the Cisco VSG.	

Host Requirements

The Cisco VSG and Cisco VNMC installation has the following host requirements:

- ESX/ESXi platform that runs VMware software release 4.0.0 or 4.1.0 with a minimum of 4-GB physical RAM for the Cisco VSG and similar 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 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, host name 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 one 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)

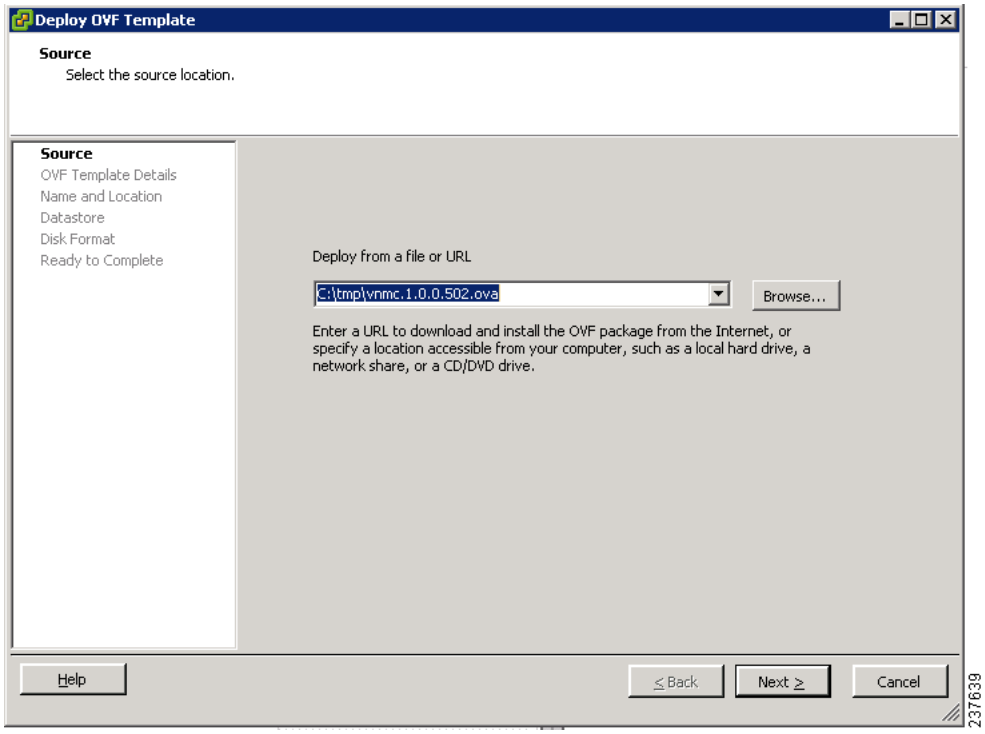
PROCEDURE

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

Step 2 Select from the File Menu **Deploy OVF Template**.

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

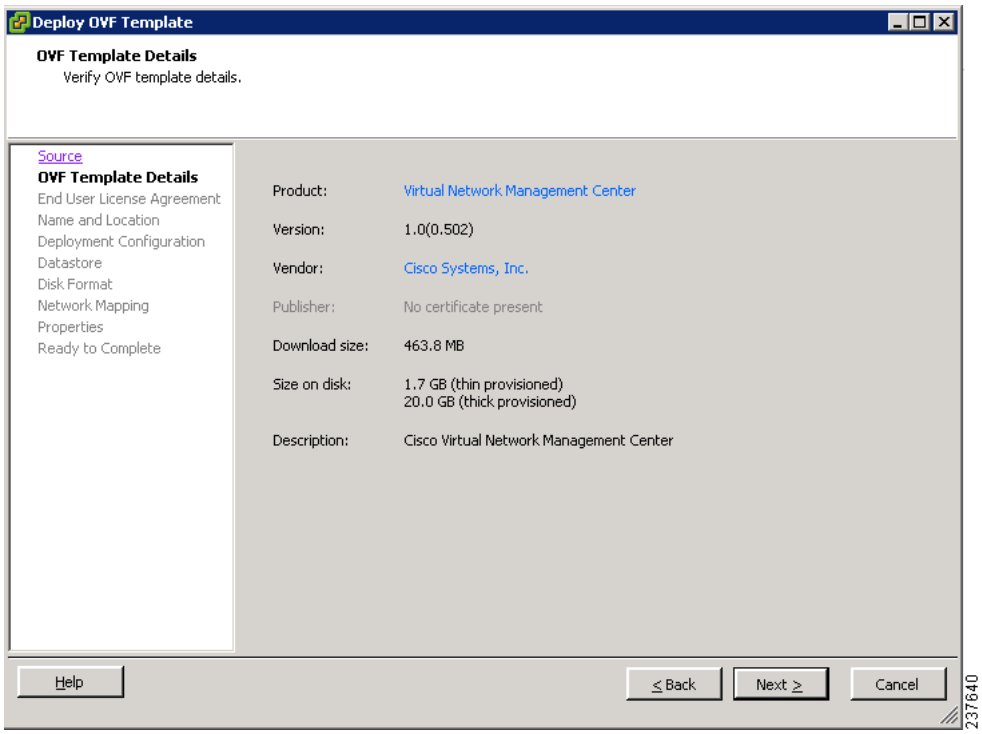
Figure 2-1 Deploy OVF Template—Source Window



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

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

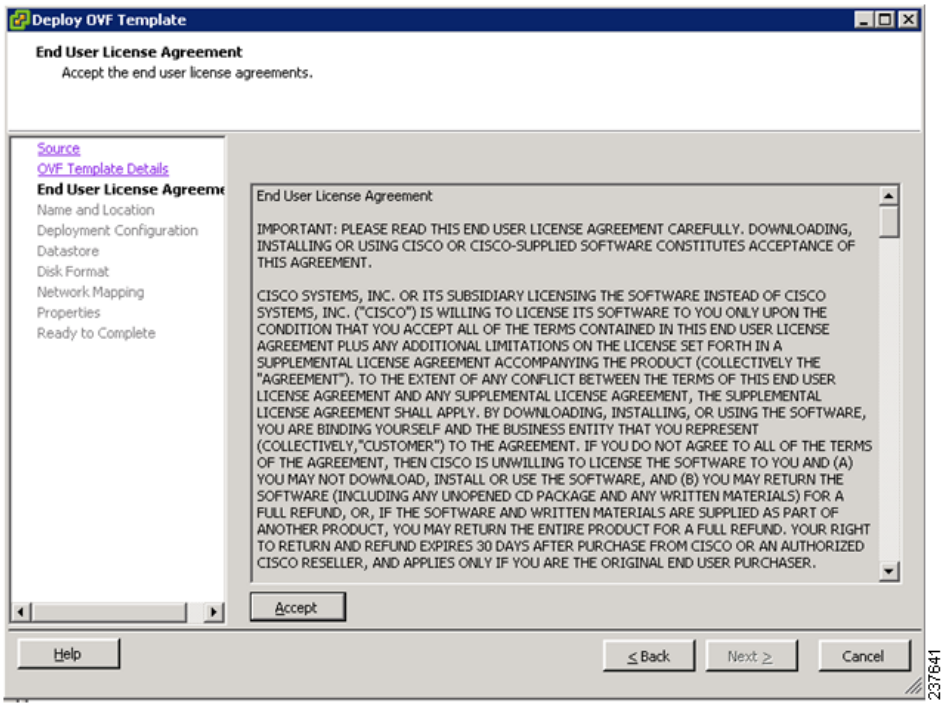
Figure 2-2 Deploy OVF Template—OVF Template Details Window



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

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

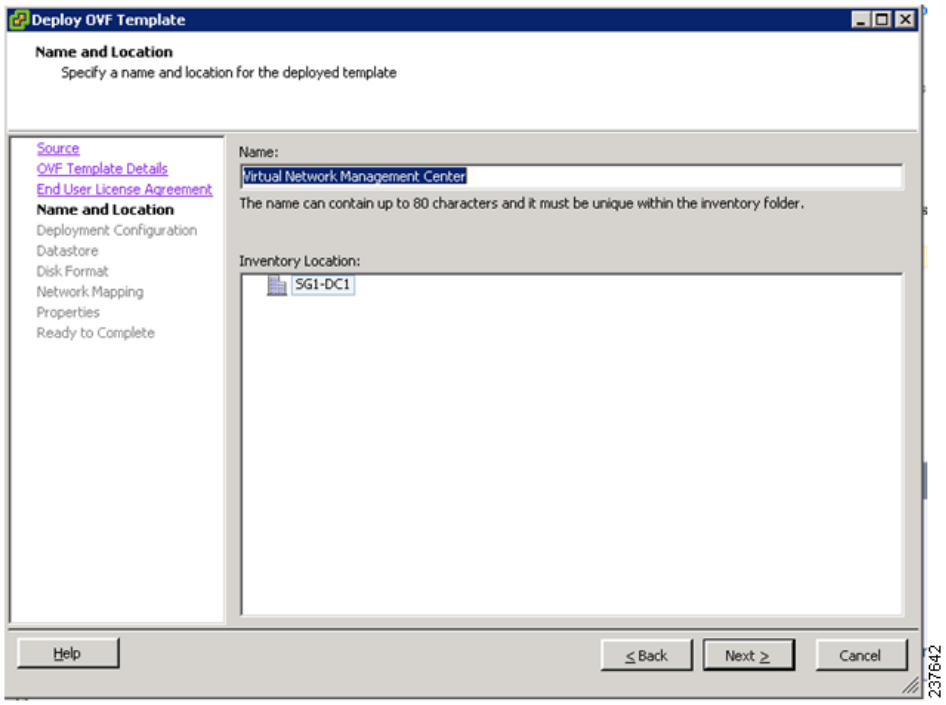
Figure 2-3 Deploy OVF Template—End User License Agreement Window



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

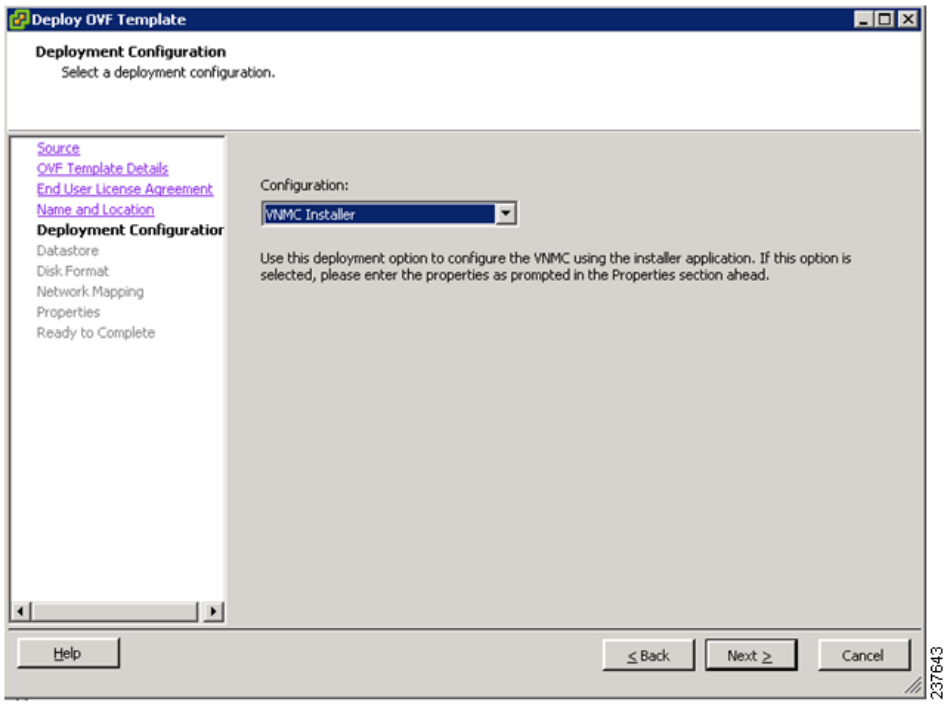


Step 6 In the Name field, enter the Name.

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

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

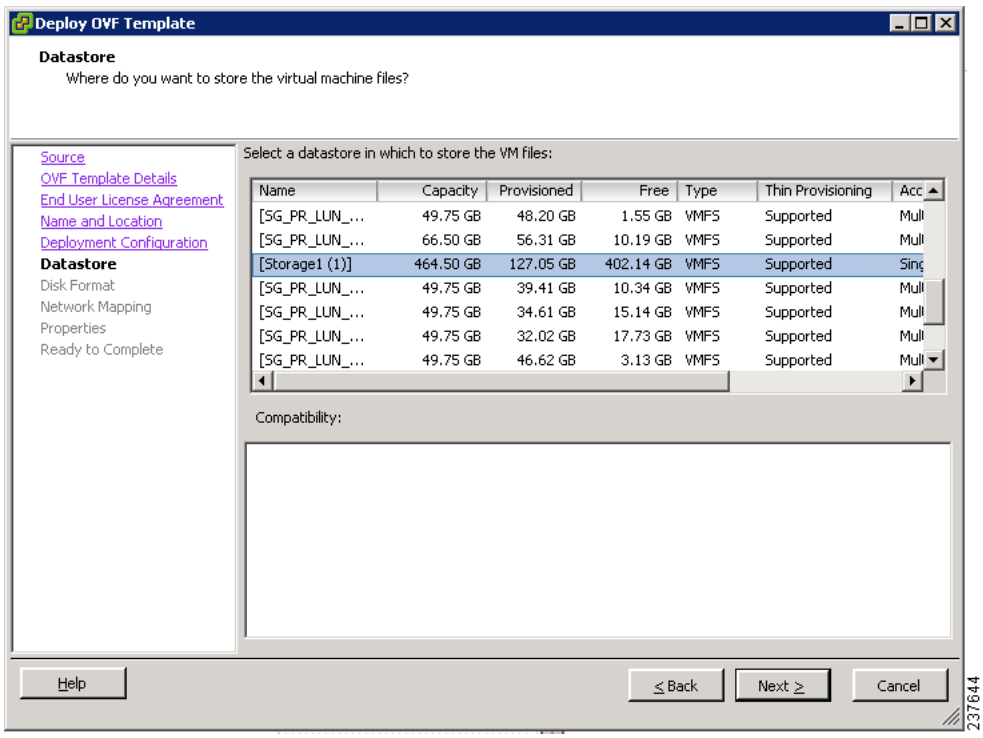
Figure 2-5 Deploy OVF Template—Deployment Configuration Window



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



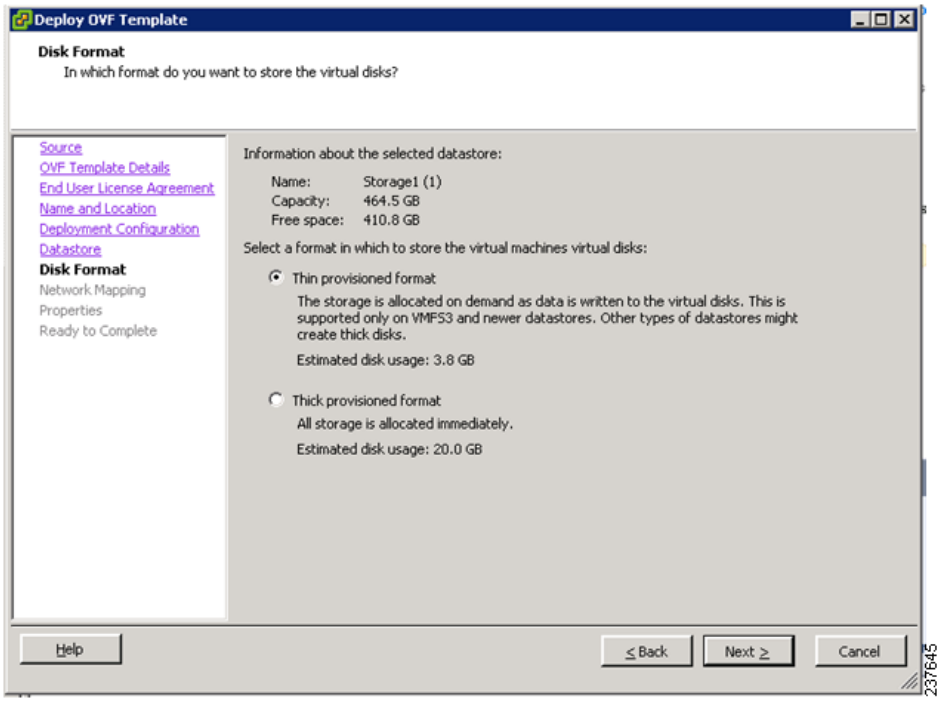
Step 9 In the **Datastore** pane, choose the datastore for the VM and click **Next**.

Note The storage can be local or shared remote such as network file storage (NFS) or 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's available.

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

Figure 2-7 Deploy OVF Template—Disk Format Window

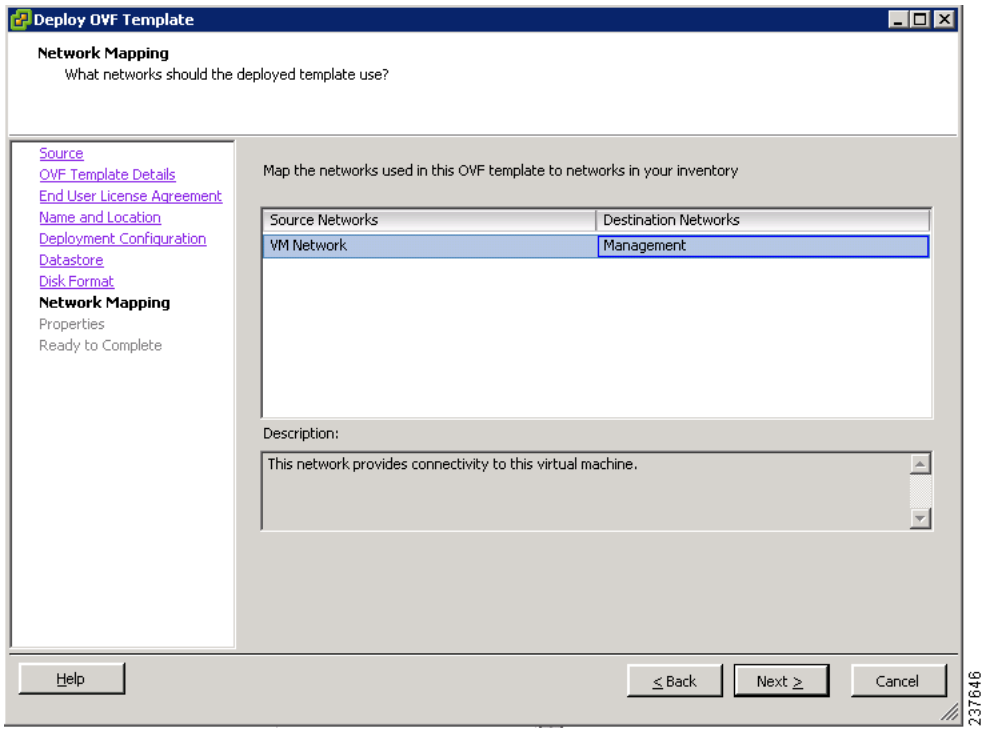


Step 10 Click either **Thin provisioned format** or **Thick provisioned format** to store the VM vdisks and click **Next**.

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

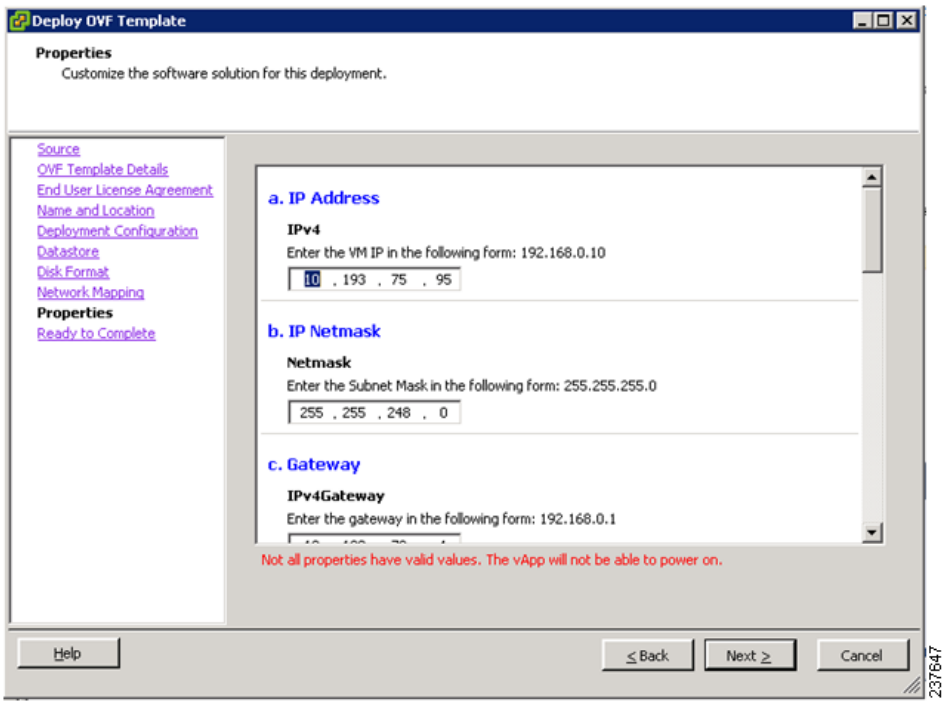
The Network Mapping window opens. See Figure 2-8.

Figure 2-8 Deploy OVF Template—Network Mapping Window



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



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.

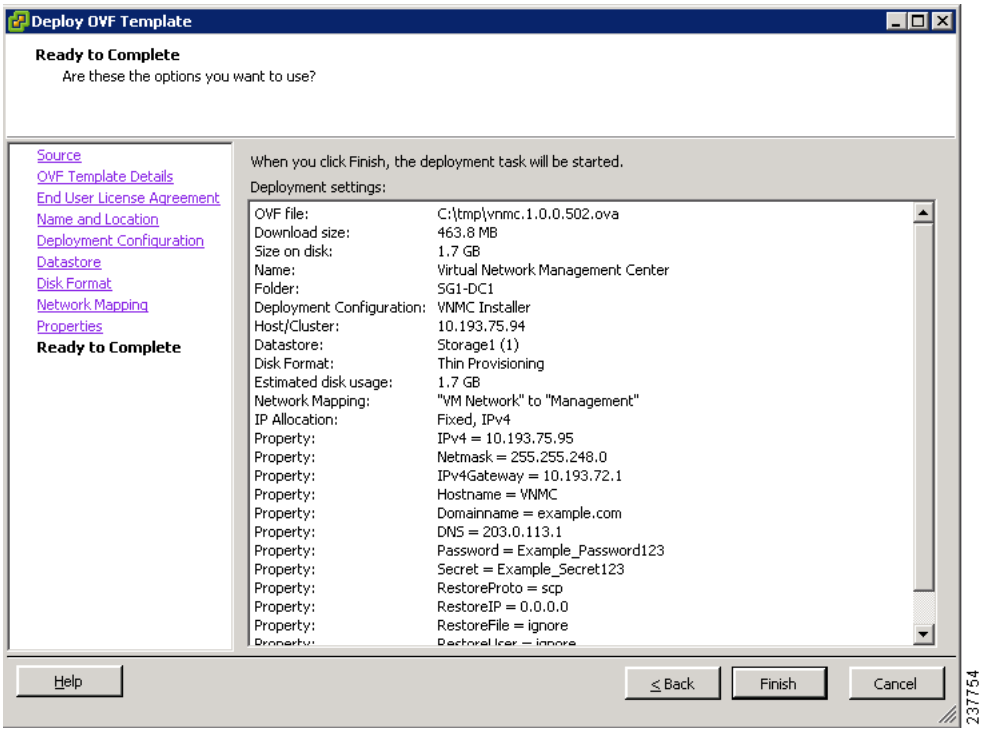
Step 13 Click **Next**.

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 **f. VNMC Restore** fields.

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

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



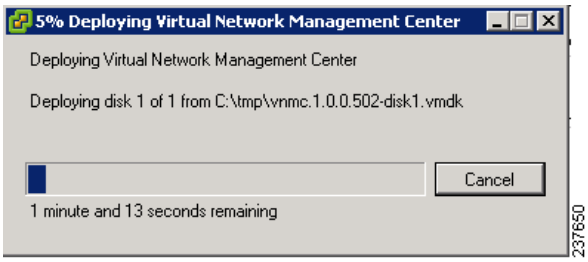
Step 14 Review the deployment settings information and click **Finish**.

Note Review the IP/Mask/gateway information carefully because any failure of these parameters may cause the VM to have bootup issues.

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

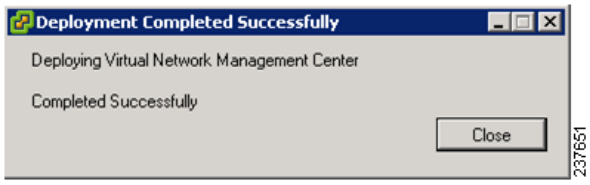
The progress bar in Figure 2-11 shows how much of the deployment task is completed before the Cisco VNMC is deployed.

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



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

Figure 2-12 Deployment Completed Successfully Progress Indicator



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

Download vCenter extension file from the Cisco VNMC

Register vCenter extension plugin in the vCenter

Configure vCenter in VM-Manager in the Cisco VNMC

BEFORE YOU BEGIN

Before doing this procedure, know or do the following:

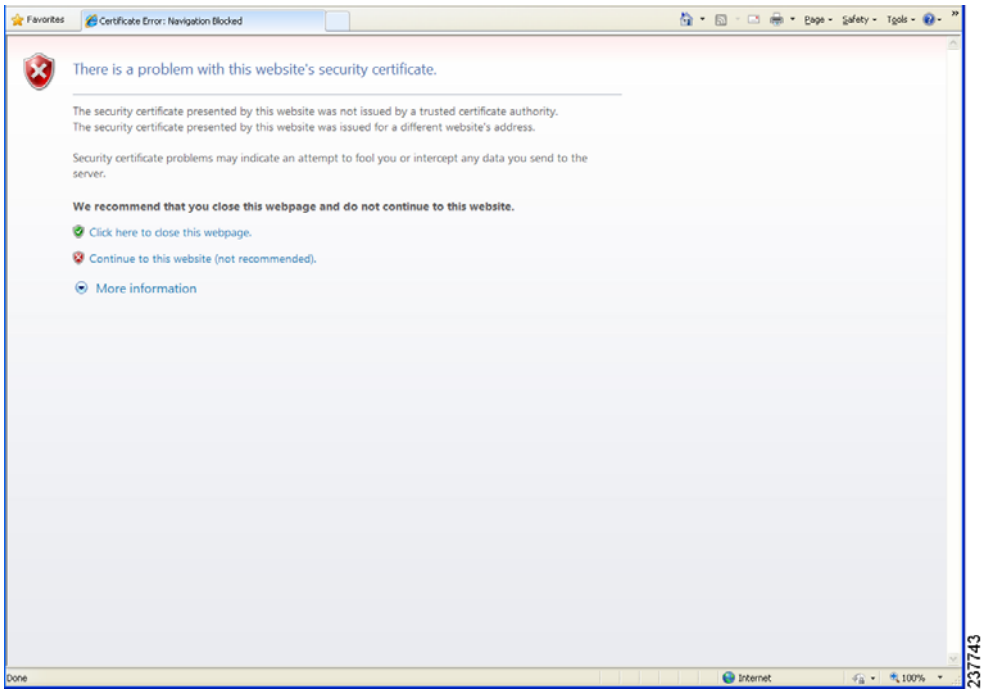
- Install Adobe Flash Player (Version 10.1.102.64)
- IP address of the Cisco VNMC
- Admin user password

Downloading the vCenter Extension File from the Cisco VNMC

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.

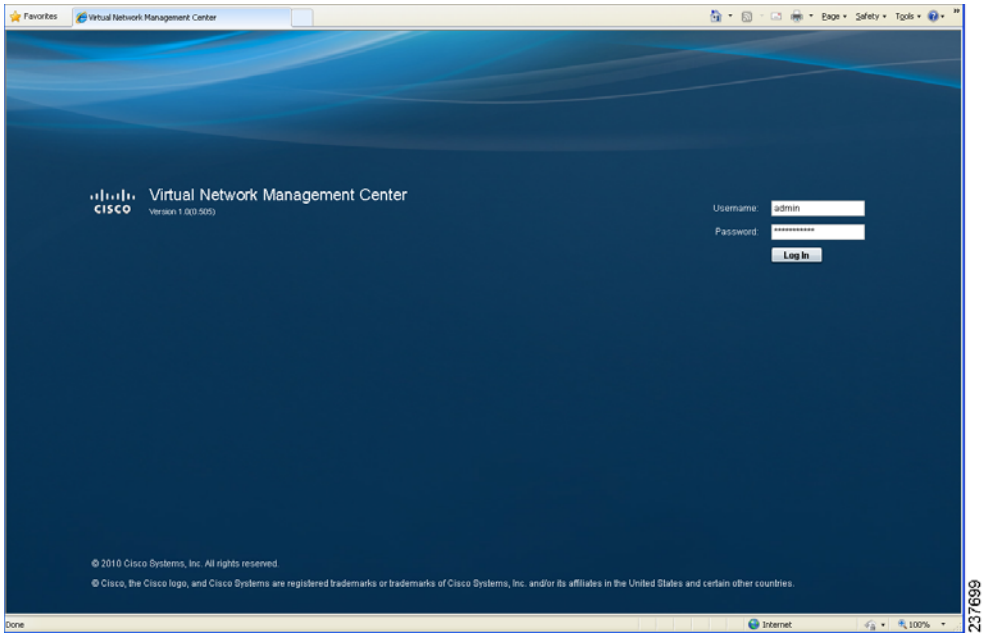
Figure 2-13 Website Security Certification Warning



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

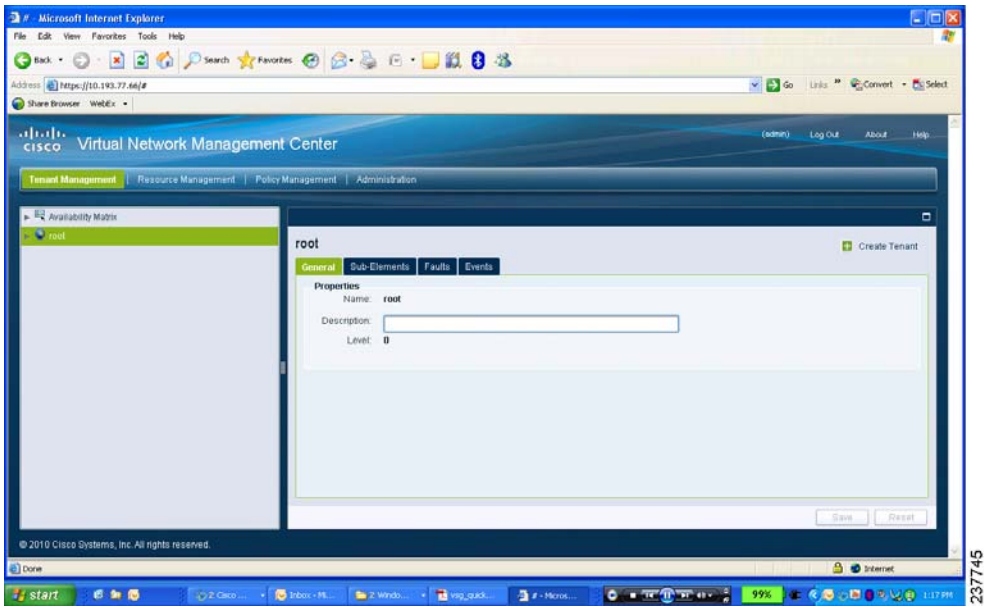
The Cisco VNMC access window opens. See Figure 2-14

Figure 2-14 VNMC Access Window



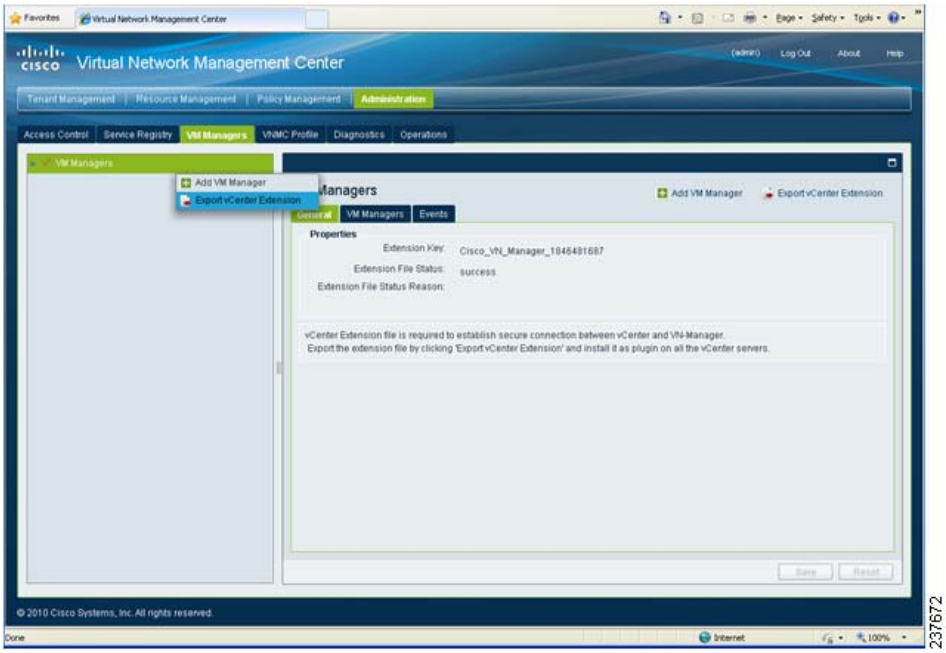
Step 3 Log in to the Cisco VNMC with the username **admin** and *password*. The VNMC Main window opens. See Figure 2-15.

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



Step 4 Click 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



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

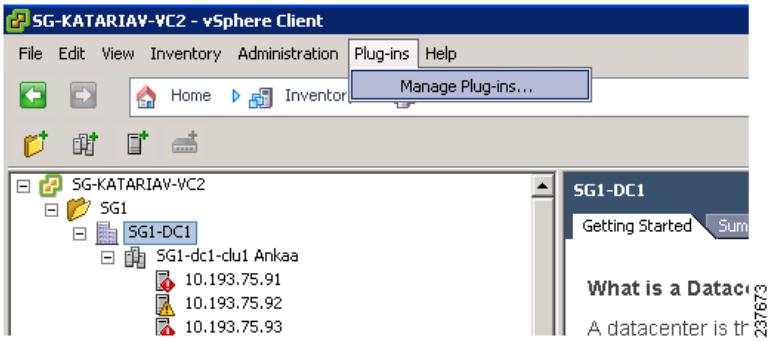
Step 6 The vCenter Desktop displays as shown in Figure 2-17.

Registering the vCenter Extension Plugin in the vCenter

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

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

Figure 2-17 vSphere Client Directory Window

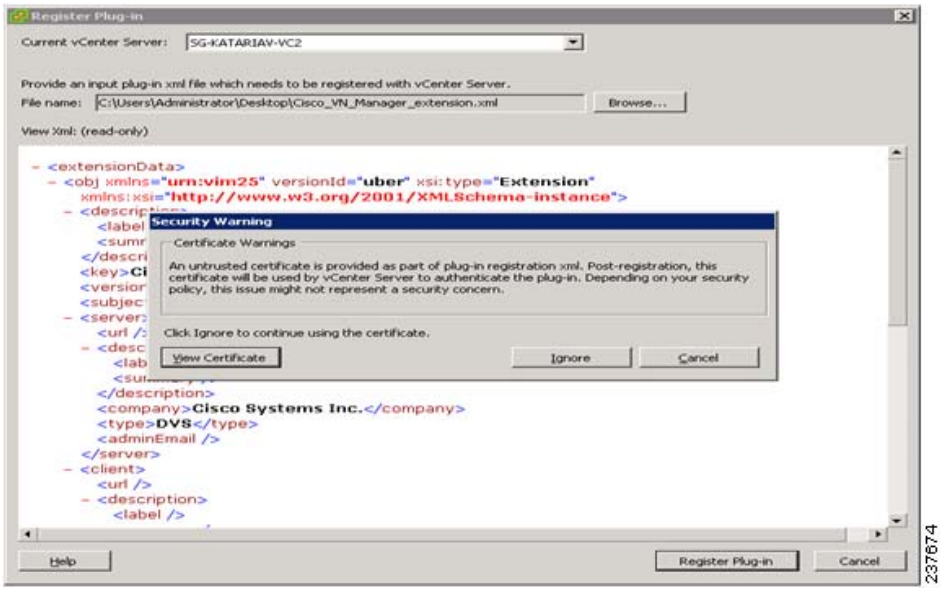


Step 2 Choose **Plug-ins** > **Manage Plug-ins**.

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

The Register Plug-in window opens. See Figure 2-18.

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

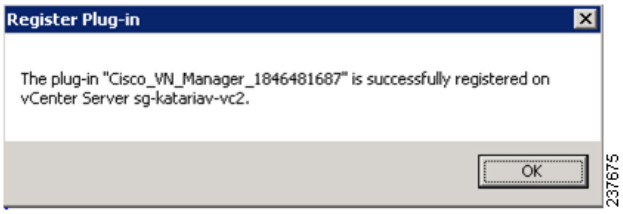


Step 4 Browse to the Cisco VNMC vCenter extension file and click **Register Plug-in**.

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

The successful registration message should display. See Figure 2-19.

Figure 2-19 Register Plug-in Progress Success Indicator



Step 6 Click **OK**.

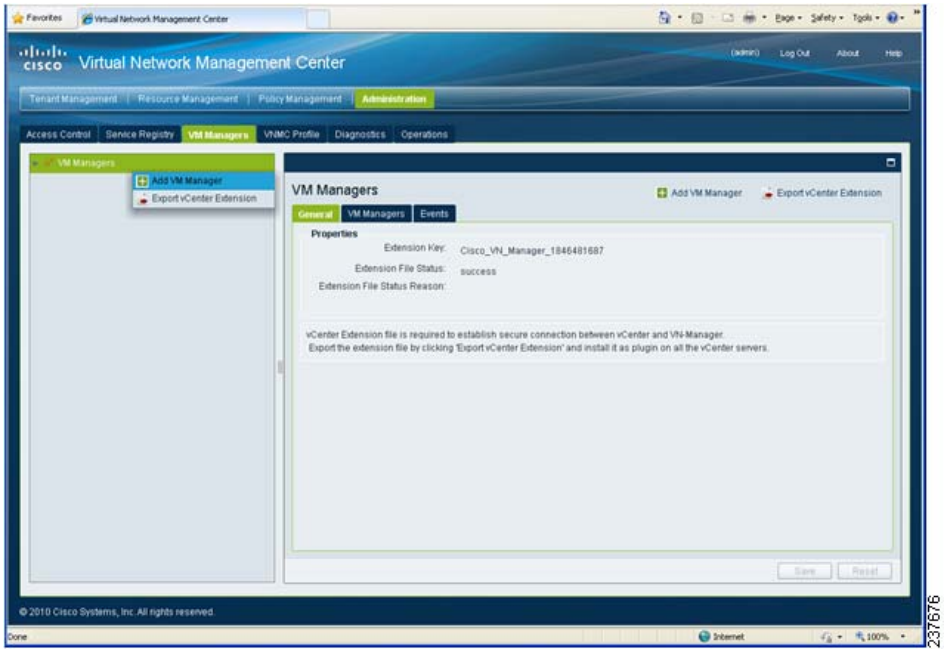
Step 7 Click **Close**.

Configuring the vCenter in VM-Manager in the Cisco VNMC

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



Step 2 Choose **VM Managers** > **Add VM Manager.**

On the right panel, the vCenter Server pane opens. See Figure 2-21.

Figure 2-21 Virtual Network Management Center—Administration Window vCenter-Server Pane

Step 3 In the right-side vCenter-Server panel, do the following:

a. In the Name field, enter the vCenter name.

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 Virtual Supervisor Module (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 (it will look like `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 have upgraded your VSM to 1.4, you need to copy the VSM policy agent image, available in VNMC image bundle, to bootflash to complete registration with 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.

The following example shows that the Cisco VNMC is reachable and the install 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.

Other Status Messages

The following 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#
```

The following 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, one per line.

```
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 **Cntl-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 **confgure** command to enter global configuration mode:

```
vsm# configure
```

Step 5 Enter the following configuration commands, one per line.

```
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 **Cntl-Z**.

Step 7 Enable the Cisco VSG HA port profile configuration mode.

```
vsm# configure
```

Step 8 Enter the following configuration commands, one per line.

```
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 VSG data and VSG HA interfaces as part of the allowed VLANs into the uplink port-profile. Use the **confgure** command to enter global configuration mode:

```
vsm# configure
```

Step 10 Enter the following configuration commands, one per line:

```
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 **Cntl-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 created on VSM
- Management port-profile (management)

Note The management port profile is the same one used for the VSM. The port profile is configured in the VSM and is used for the Cisco VNMC management interface.

- HA ID
- IP/SubnetMask/Gateway information for 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)

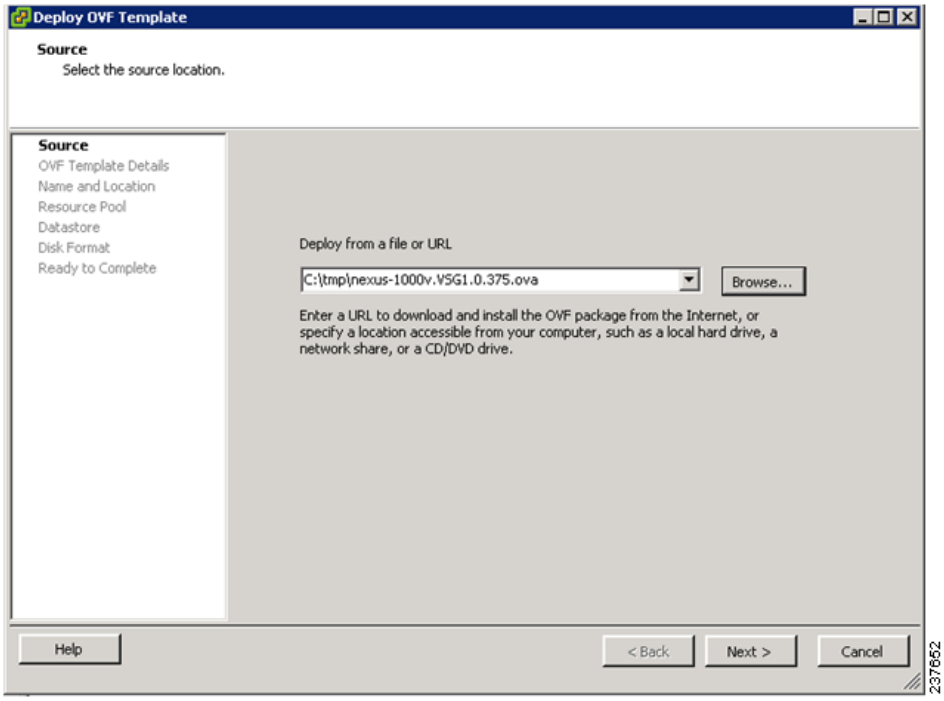
PROCEDURES

Step 1 Select Your Host to deploy the VSG VM

Step 2 Select **Deploy OVF Template** from the File Menu

The Source window opens. See Figure 2-22.

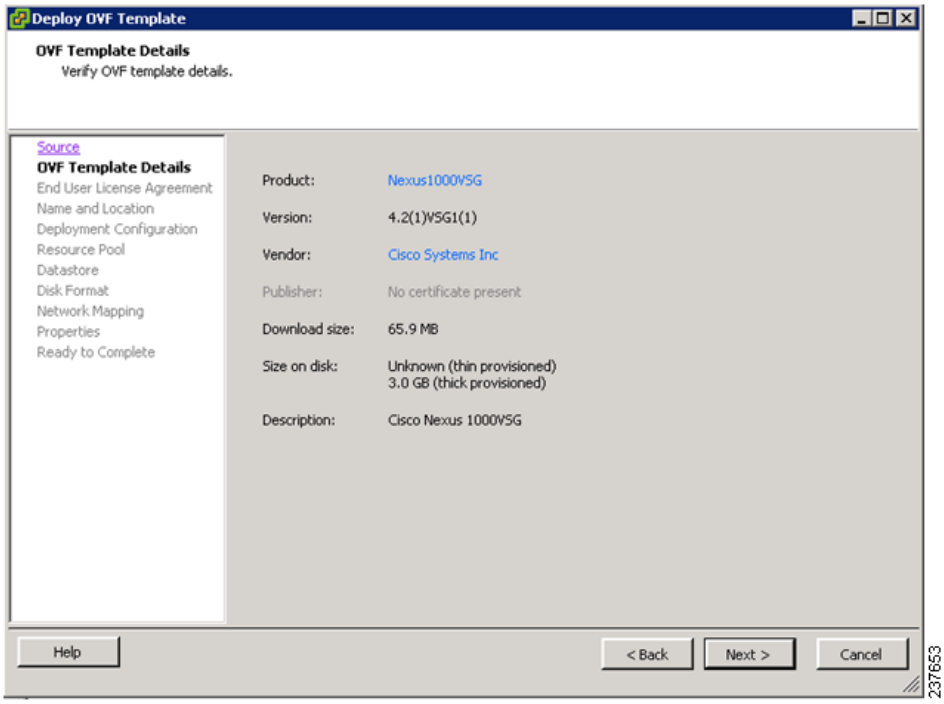
Figure 2-22 Deploy OVF Template—Source Window



Step 3 Provide the path to the Cisco VSG OVA file and click **Next**.

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

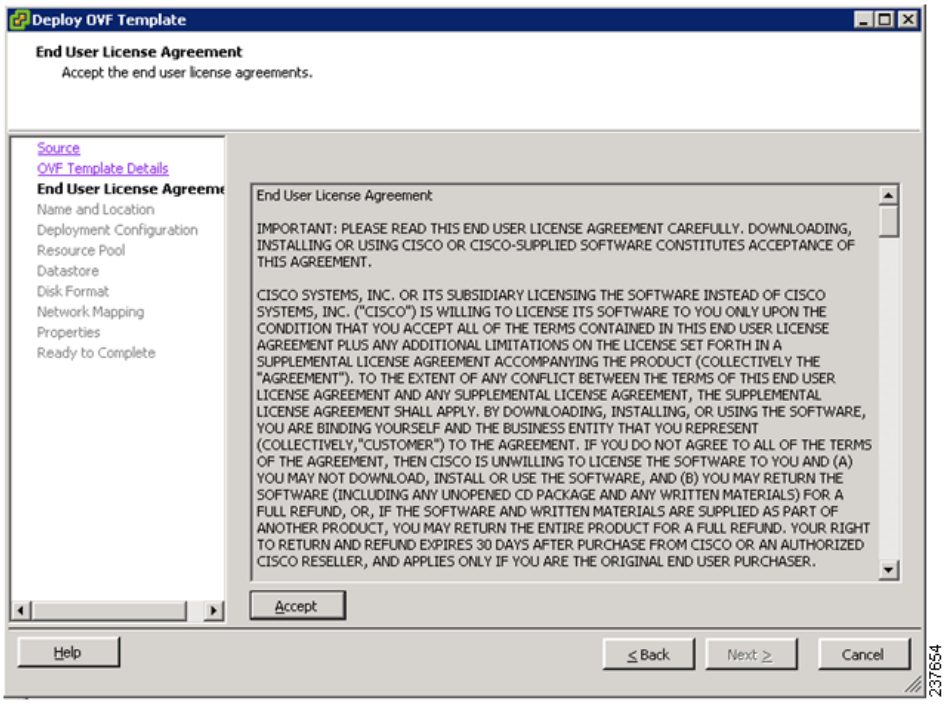
Figure 2-23 Deploy OVF Template—OVF Template Details Window



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

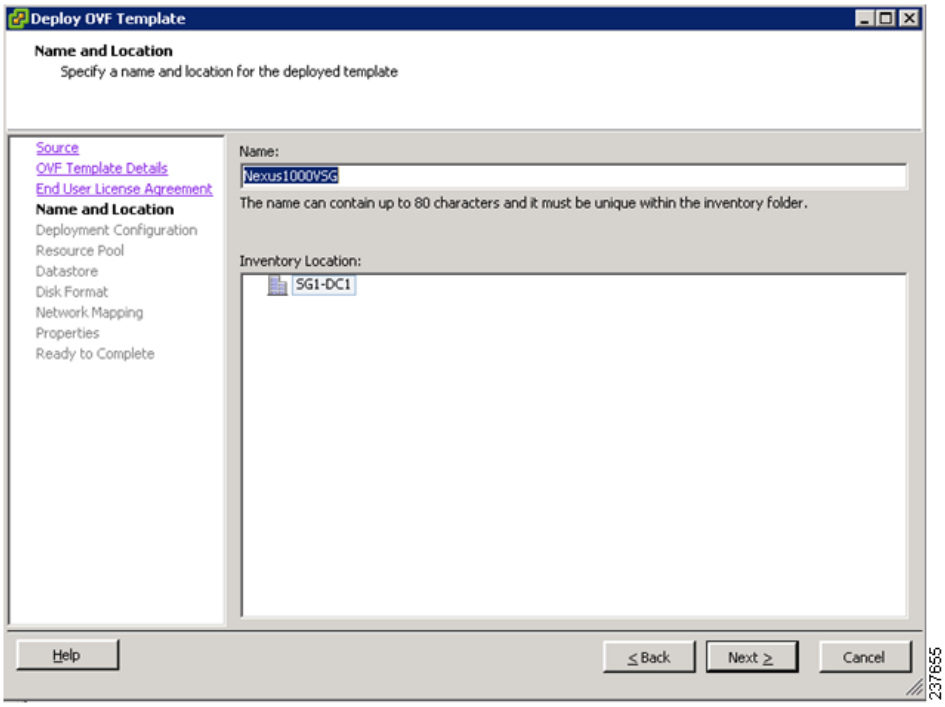


Step 5 Click **Accept** to accept the End User License Agreement.

Step 6 Click **Next**.

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

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



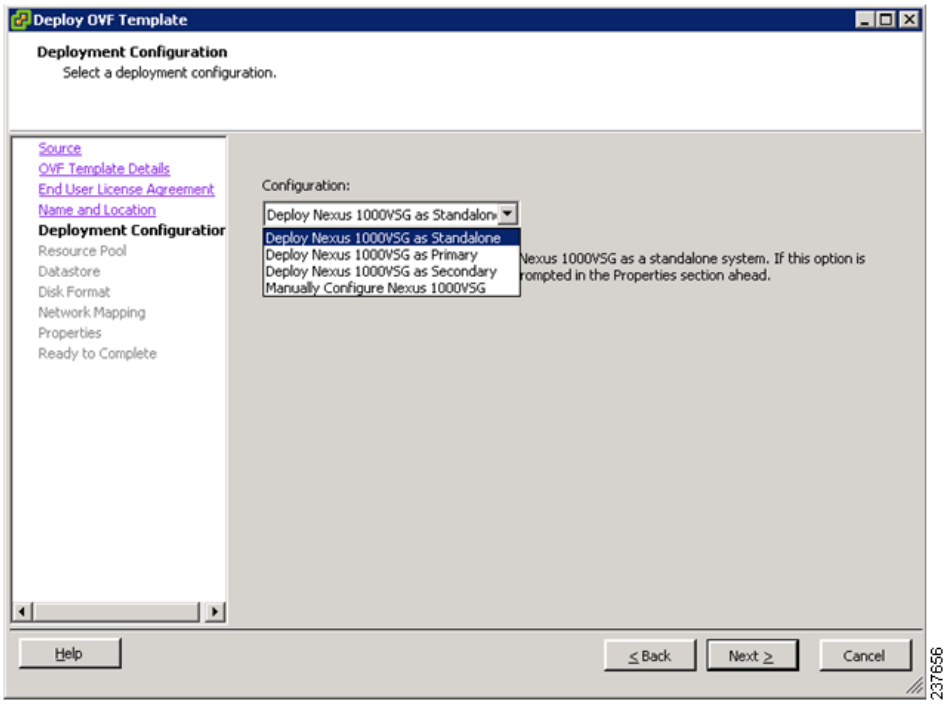
Step 7 In the **Name** field, enter the name you want to use for the Cisco VSG.

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

Step 9 Click **Next**.

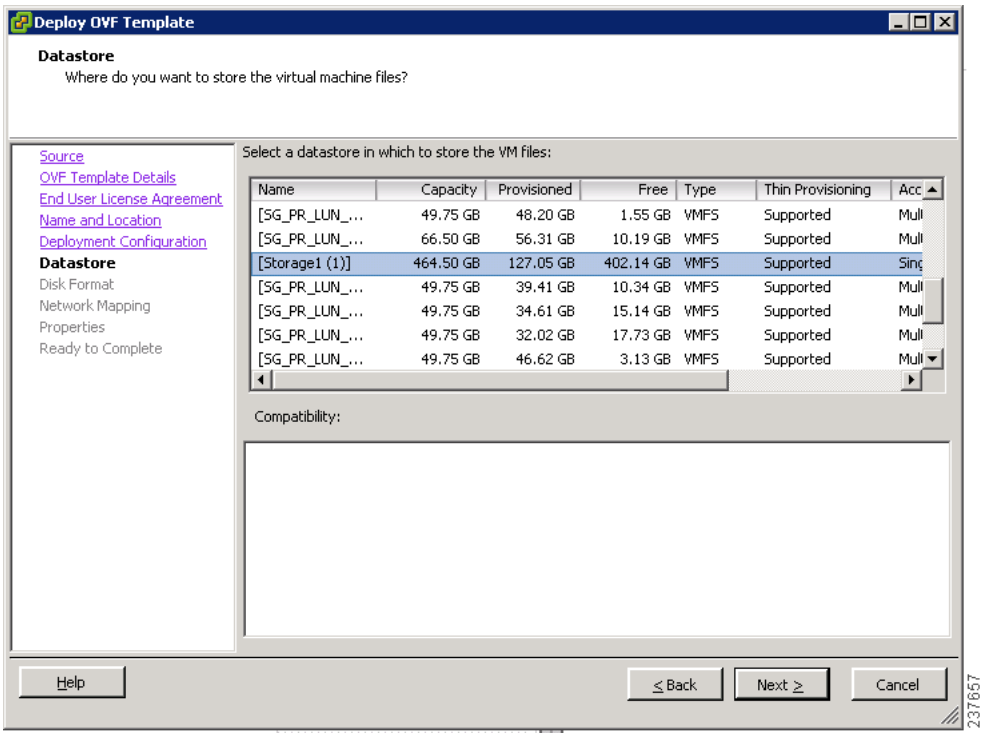
The Deployment Configuration window opens. See Figure 2-26.

Figure 2-26 Deploy OVF Template—Select a Deployment Configuration Window



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



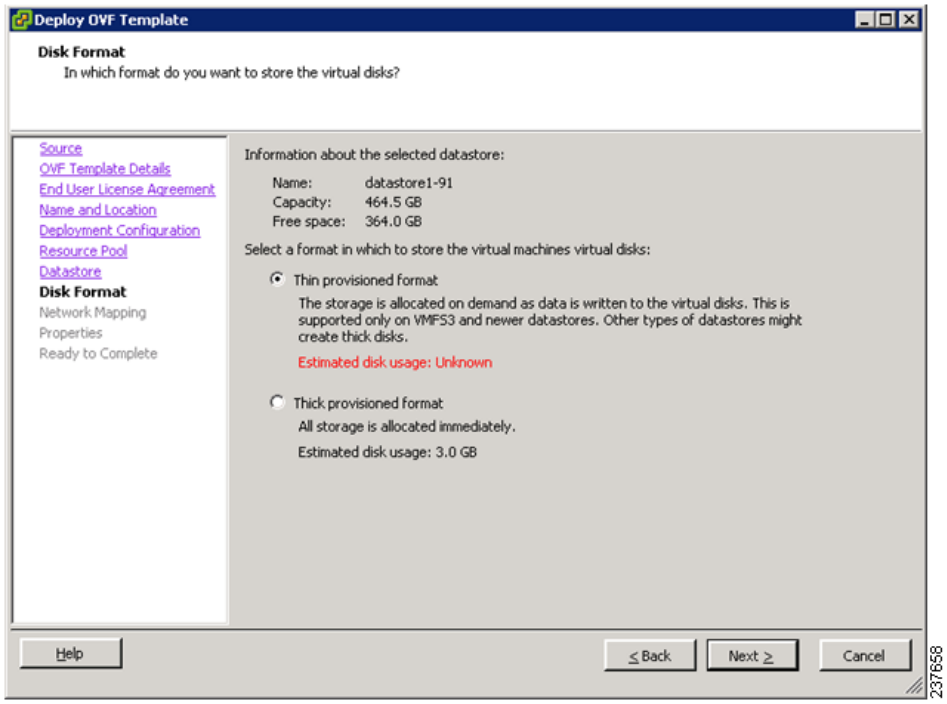
Step 11 In the **Datastore** pane, choose the datastore for the VM and click **Next**.

Note Storage can be local or shared-remote such network file storage (NFS) or 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's available.

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

Figure 2-28 Deploy OVF Template—Disk Format Window



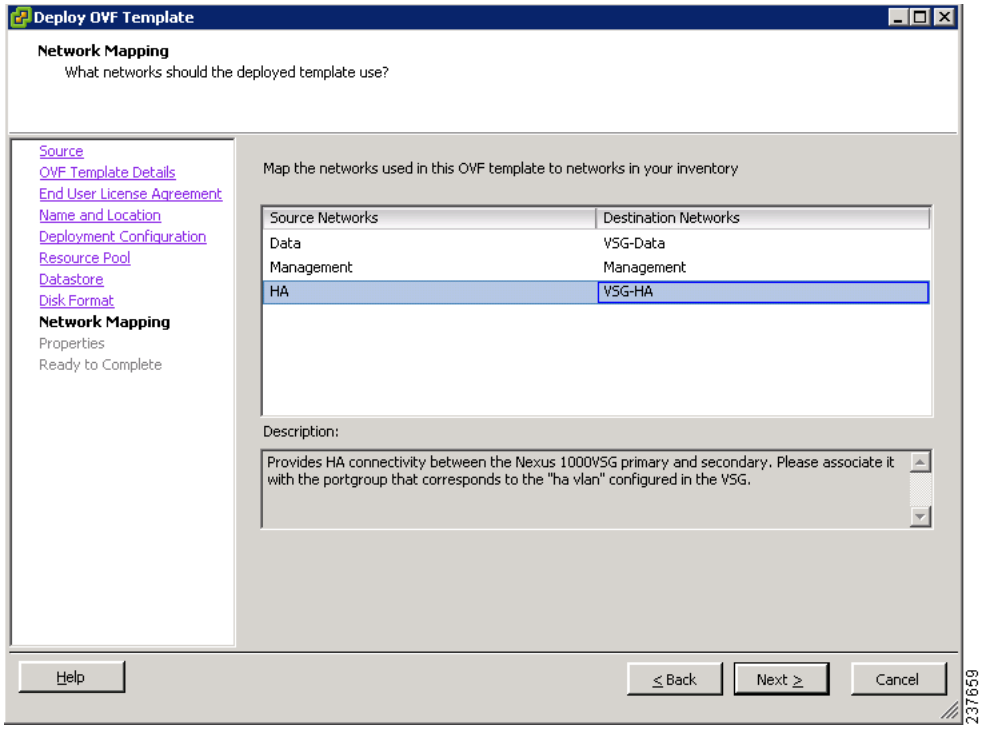
Step 12 Select the Disk Format in which to store the VM vdisks and click **Next**.

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



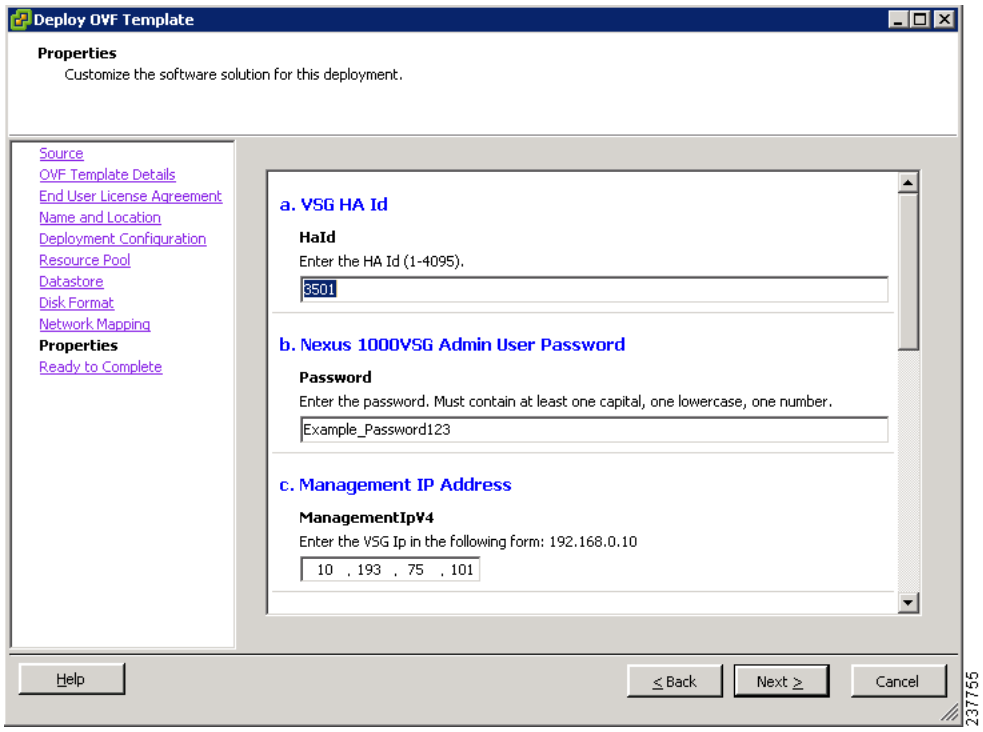
Step 13 Choose the data interface port profile as **VSG-Data**, choose the management interface port profile as **Management**, and choose the HA interface port profile as **VSG-HA**.

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 2-21, 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



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 capital, one lower case, 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.

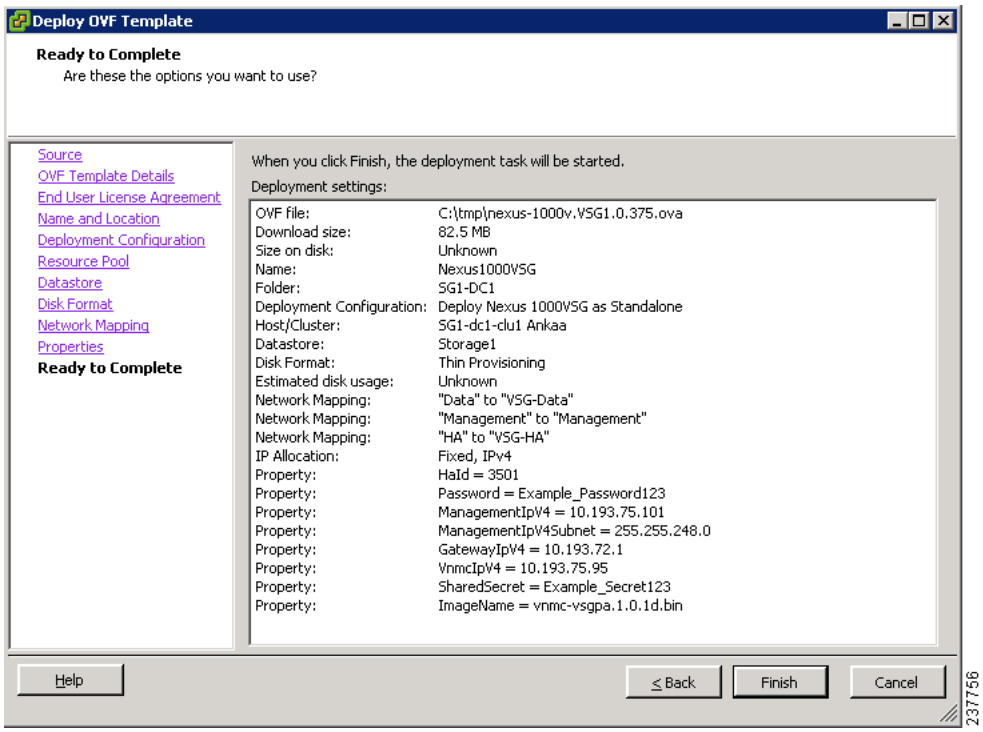
g. In the **ImageName** field, enter the VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)

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



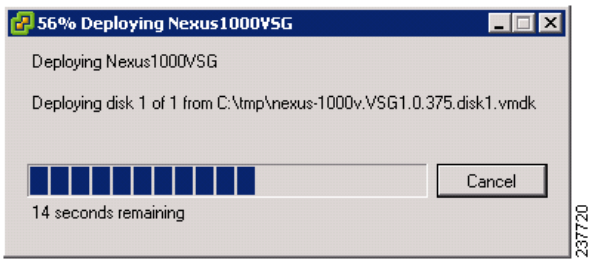
Step 17 Review the deployment settings information and click **Finish**.

Note Review the IP/mask/gateway information carefully. Any discrepancies here may cause the VM to have bootup issues.

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

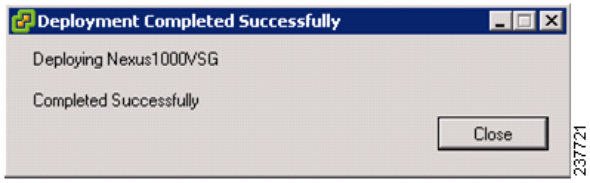
The progress bar in Figure 2-32 shows how much of the deployment task is completed before the Cisco VSG is deployed.

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



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

Figure 2-33 Deployment Completed Successfully Progress Indicator



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).

PROCEDURES

Step 1 Log in to the Cisco VSG.

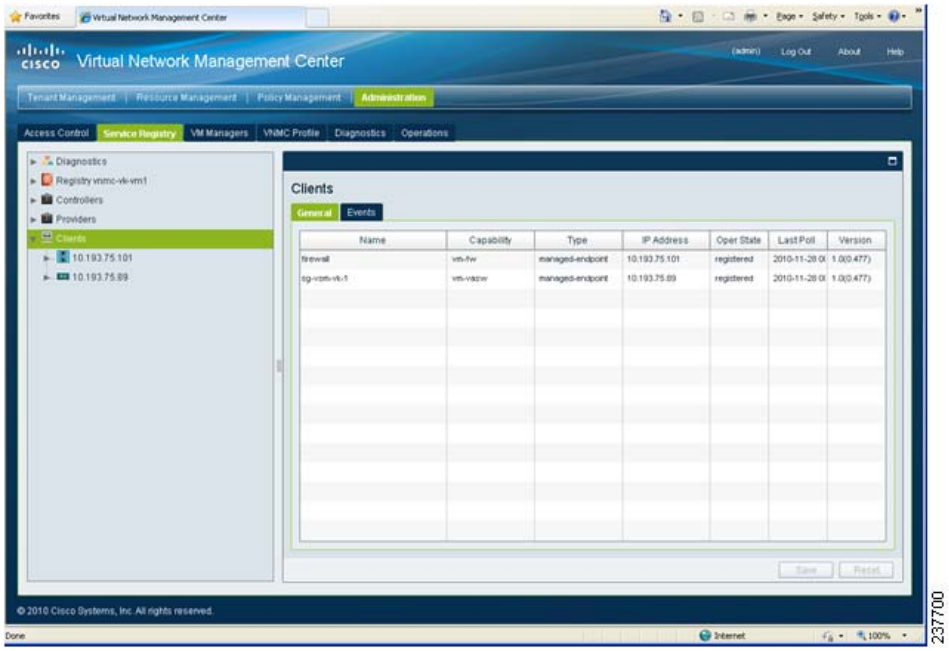
Step 2 Check the status of VNM-PA configuration by entering the following command:

```
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 Navigate to the **Administration** > **Service Registry** > **Clients** > **General** pane. See Figure 2-34.

Figure 2-34 VNMC Administration Service Registry Window Clients Pane



Step 5 Verify that the VSM and VSG information is listed in the Clients pane.

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), it's time to start configuring some of the basic security profiles and policies. Use the following steps to complete this process.

BEFORE YOU BEGIN

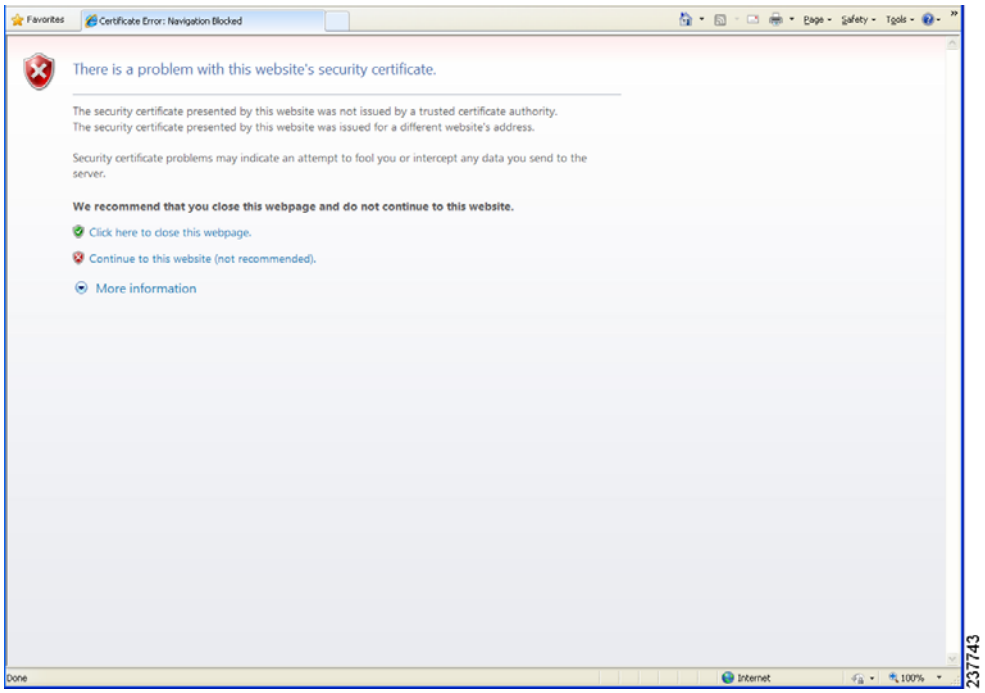
Before doing this procedure, know or do the following:

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

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.

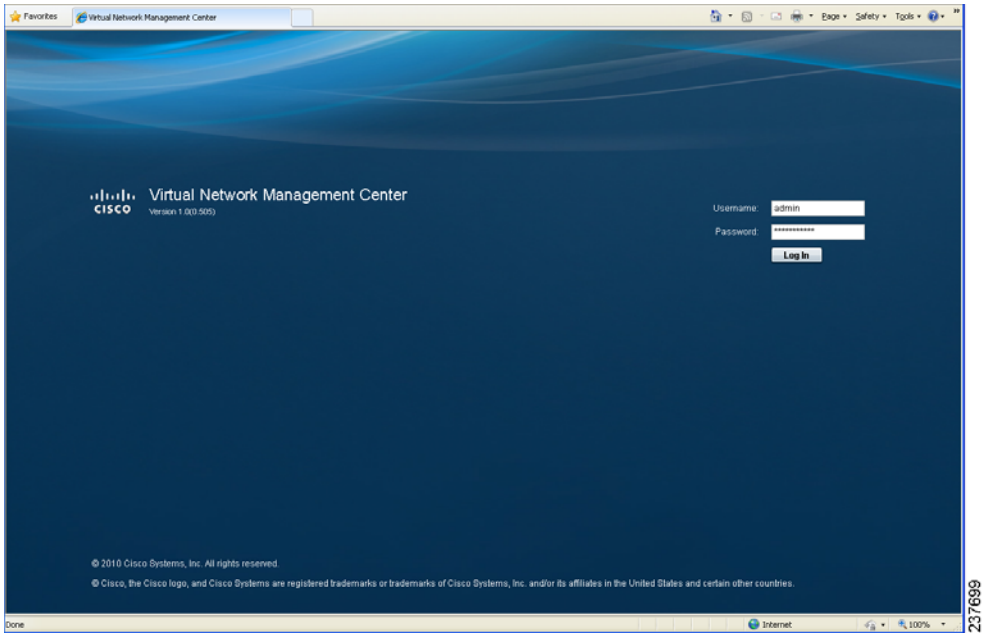
Figure 2-35 Website Security Certification Warning



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

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

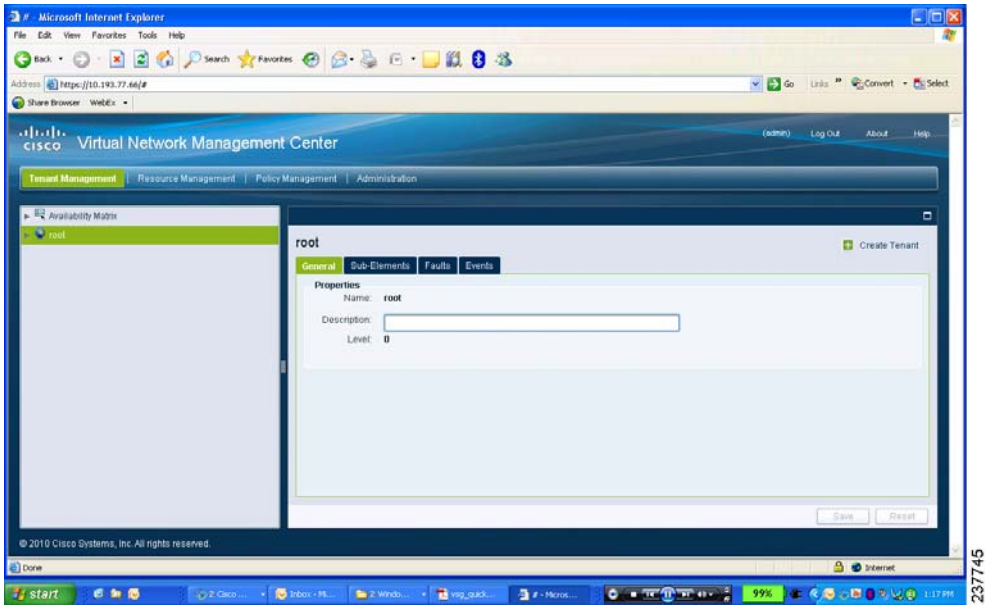
Figure 2-36 VNMC Access Window



Step 3 Log in to the Cisco VNMC with the username **admin** and *password*.

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

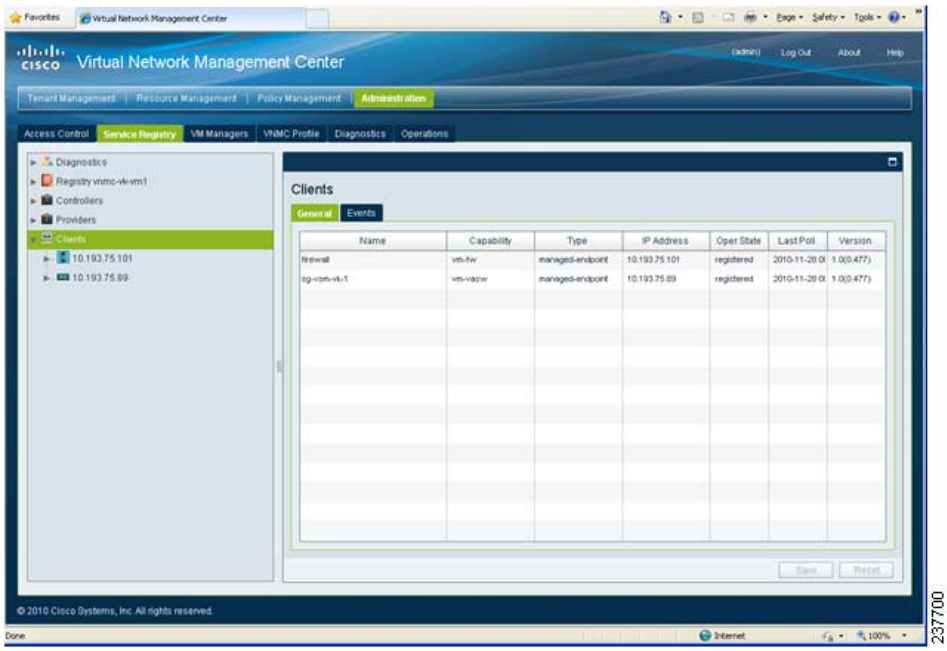
Figure 2-37 Cisco Virtual Network Management Center—Opening Page



Step 5 To quickly check the VSM and VSG registration in the Cisco VNMC, click **Administration > Service Registry > Clients**.

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

Figure 2-38 VNMC Administration Service Registry Window Clients Pane



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

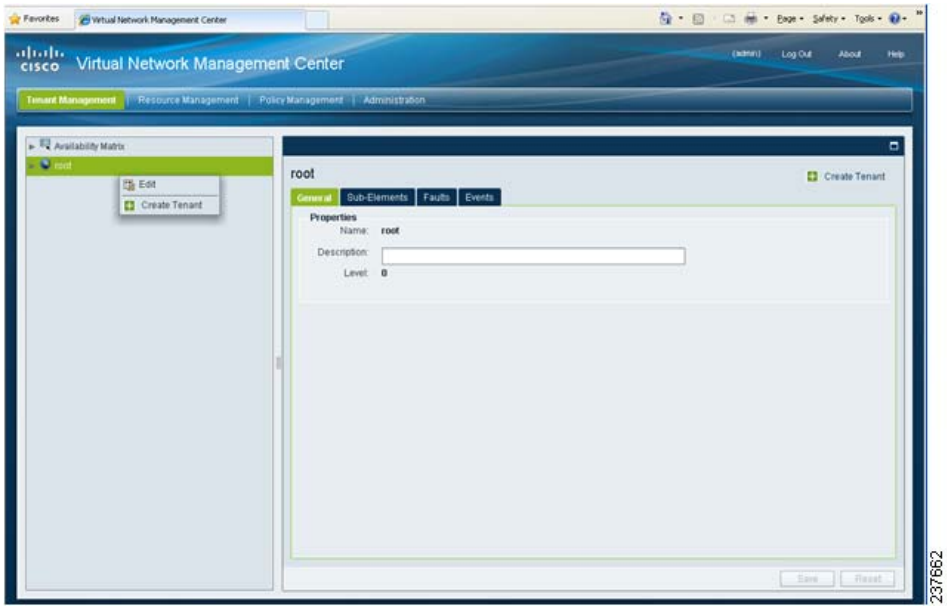
Configuring a Tenant in the Cisco VNMC

Tenants are entities (businesses, agencies, institutions, and so on) whose data and processes are hosted on virtual machines (VM) 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 tool bar, click the **Tenant Management** tab.

The root pane opens. See Figure 2-39.

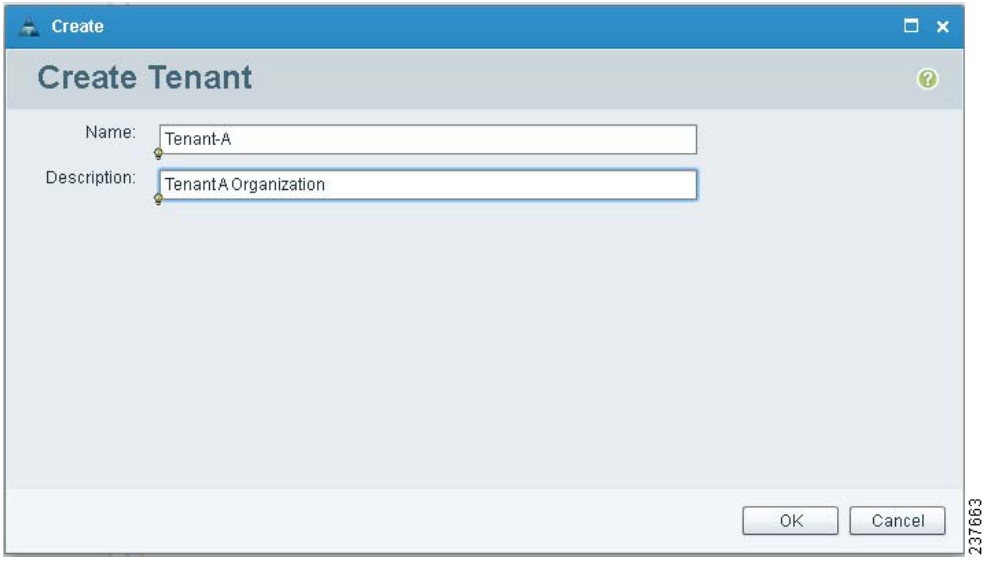
Figure 2-39 VNMC Window Tenant Management Tab root Pane



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

Step 3 The Create Tenant dialog box opens. See Figure 2-40

Figure 2-40 Create Tenant Dialog Box



Step 4 Do the following:

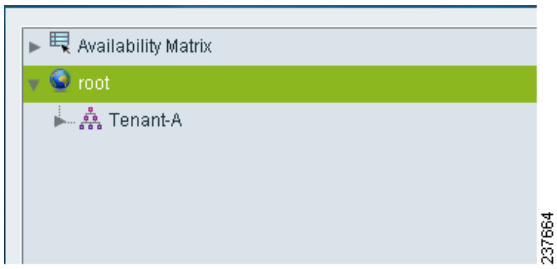
a. In the **Name** field, enter the tenant name; for example, *Tenant-A*.

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

Step 5 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

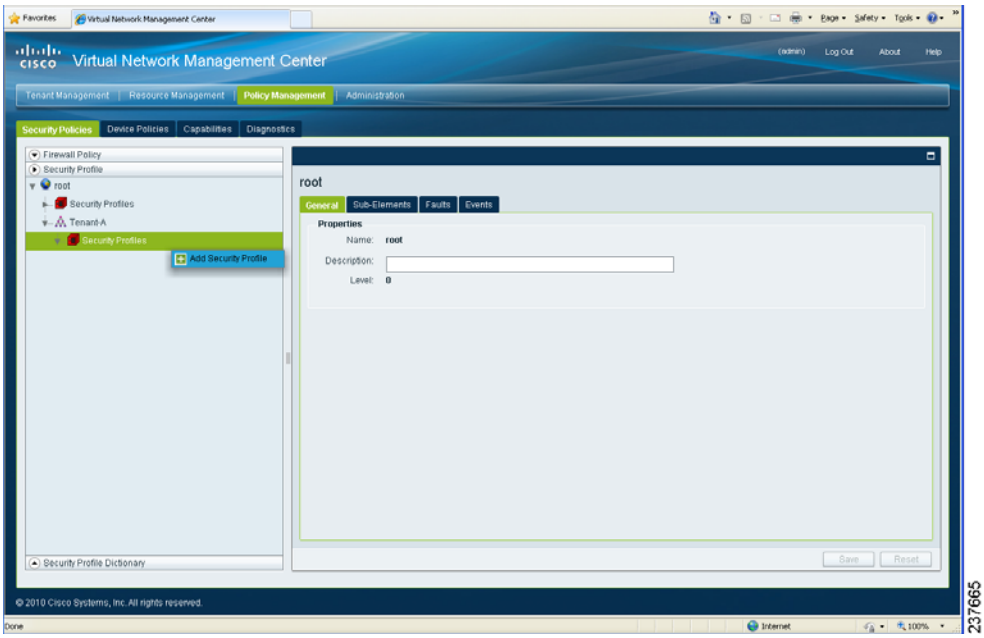


Configuring a Security Profile in the Cisco VNMC

Step 1 Click on the **Policy Management** tab in the Cisco VNMC top row tool bar.

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

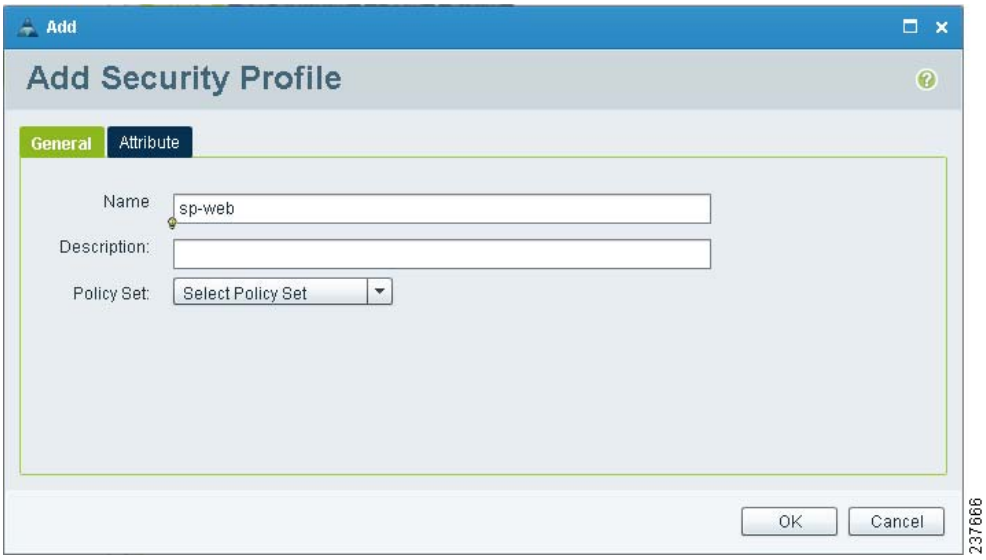
Figure 2-42 VNMC Policy Management Security Policies Window



Step 2 From the directory path **Security Policies > Security Profile > root > Tenant-A > Security Profiles**, right-click and choose from the drop-down **Add Security Profile**.

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

Figure 2-43 Add Security Profile Dialog Box



Step 3 Do the following:

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

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

Step 4 Click **OK**.

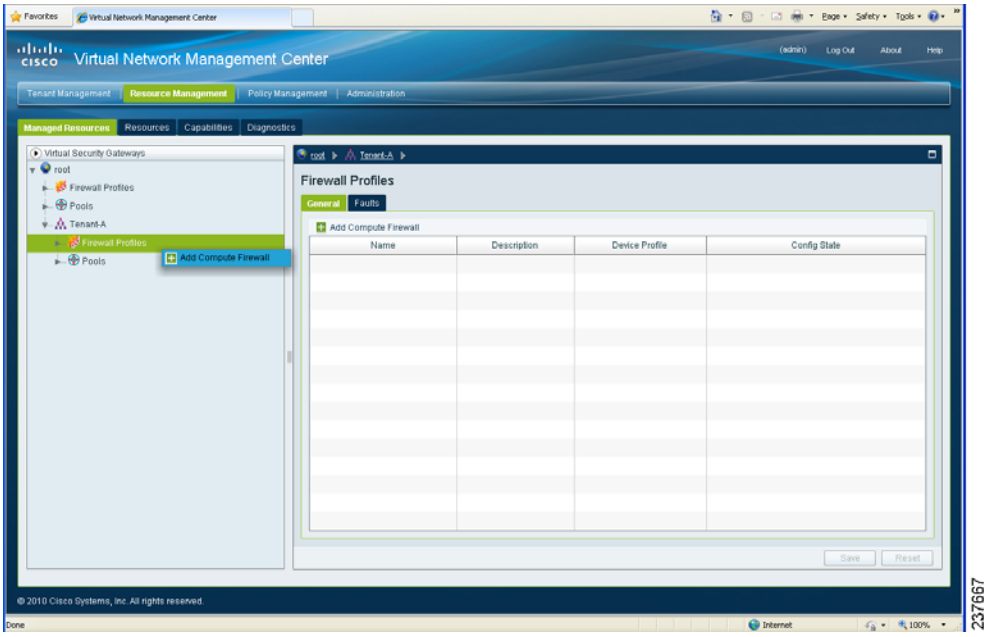
On the Cisco VNMC, Configuring a Compute Firewall

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.

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

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

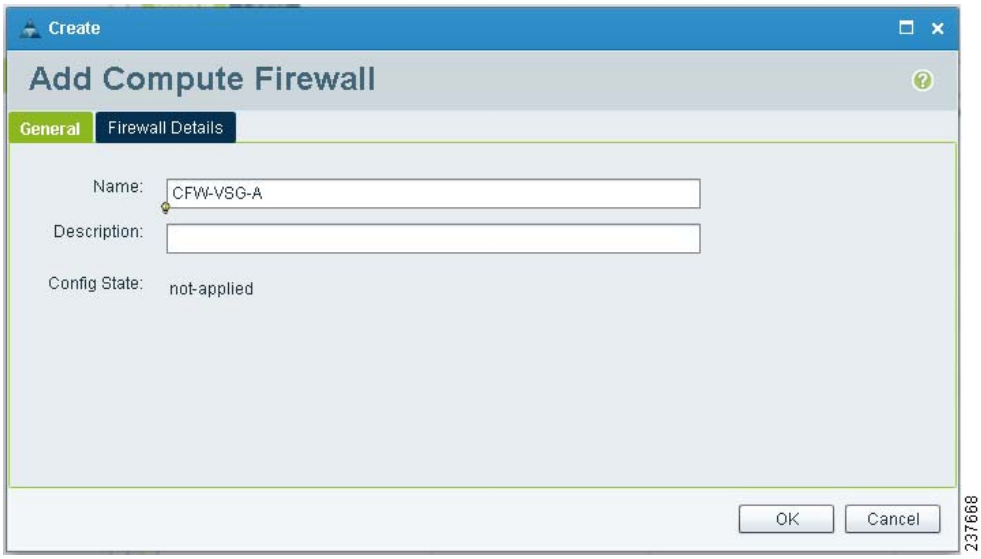
Figure 2-44 VNMC Resource Management, Managed Resources, Firewall Profiles Window



Step 2 On the left-pane directory tree, right-click on **Firewall Profiles** and choose from the drop-down list **Add Compute Firewall**.

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

Figure 2-45 Add Compute Firewall Dialog Box—General



Step 3 In the General tab display, do the following:

- In the **Name** field, enter a name for the compute firewall.
- In the **Decription** field, enter a brief description of the compute firewall.

Step 4 Click on the Firewall Details tab. See Figure 2-46.

Figure 2-46 Add Compute Firewall Dialog Box—Firewall Details

Step 5 In the Firewall Details tab view, do the following:

- In the **Management Hostname** field, enter the name for your Cisco VSG.

Step 6 Click **OK**.

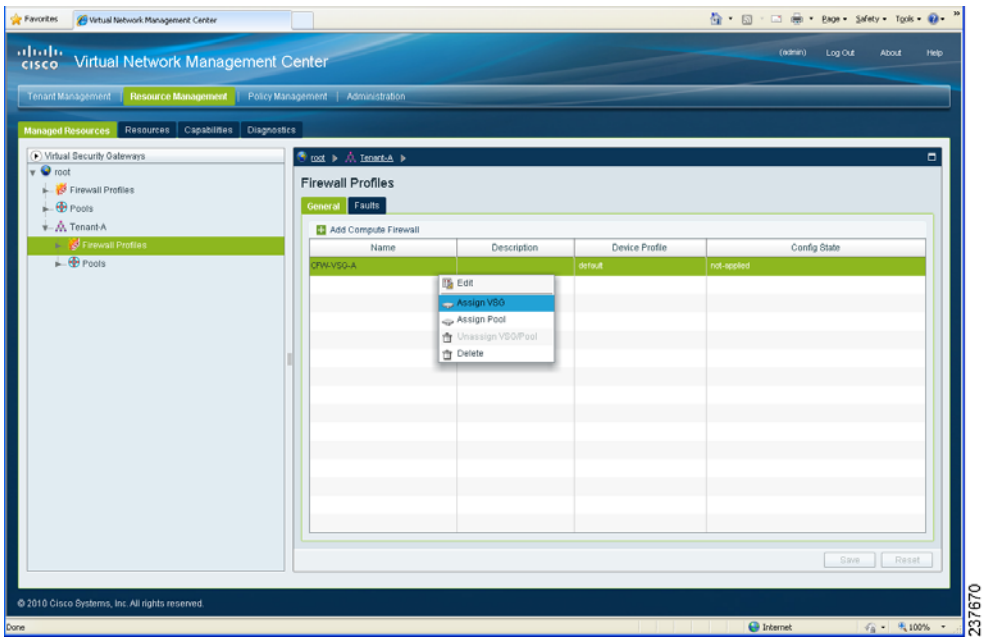
Task 8—On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall

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. This procedure shows how to assign the Cisco VSG to the compute firewall on the Cisco VNMC.

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

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

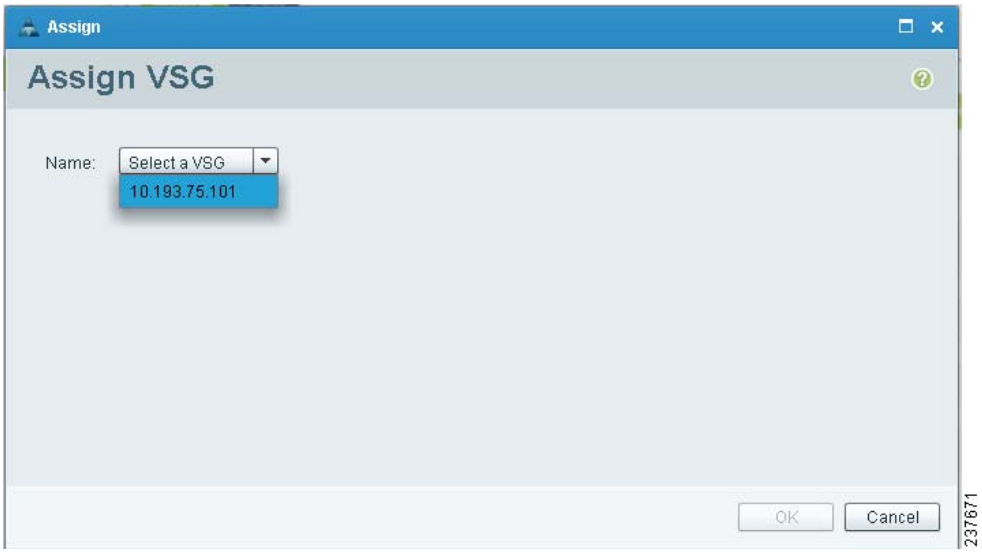
Figure 2-47 VNMC Resource Management Managed Resources Firewall Profiles Window



Step 2 Click **root** > **Tenant-A** > **Firewall Profiles**, right-click **Add Compute Firewall** 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 3 From the Name drop-down list, choose the Cisco VSG IP address.

Step 4 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

Configure a permit-all rule in the Cisco VNMC.

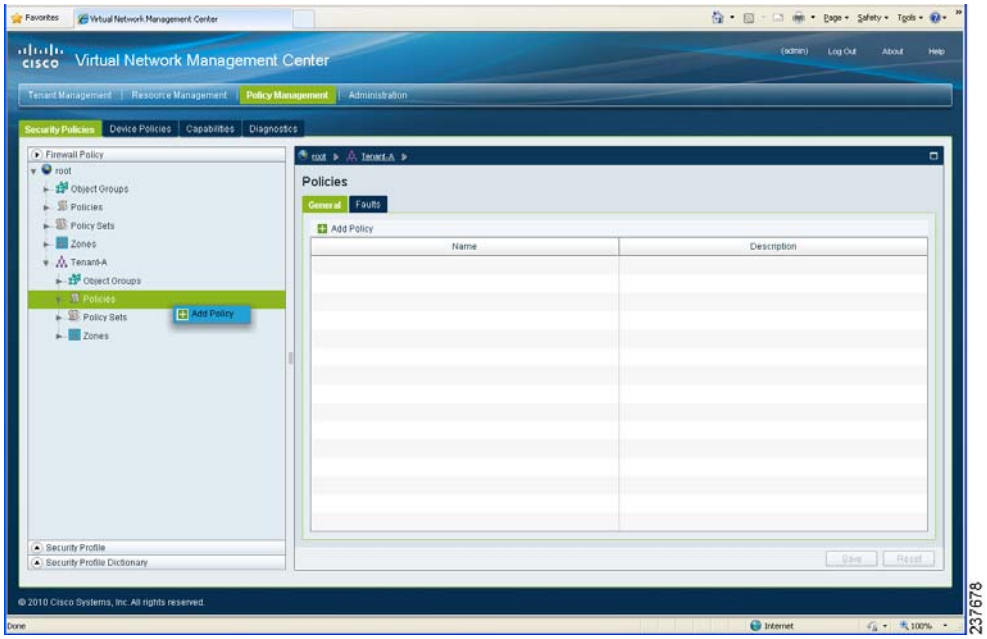
Configuring a Permit-All Rule in the Cisco VNMC

You can use the following procedure to configure a permit-all rule in the Cisco VNMC.

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.

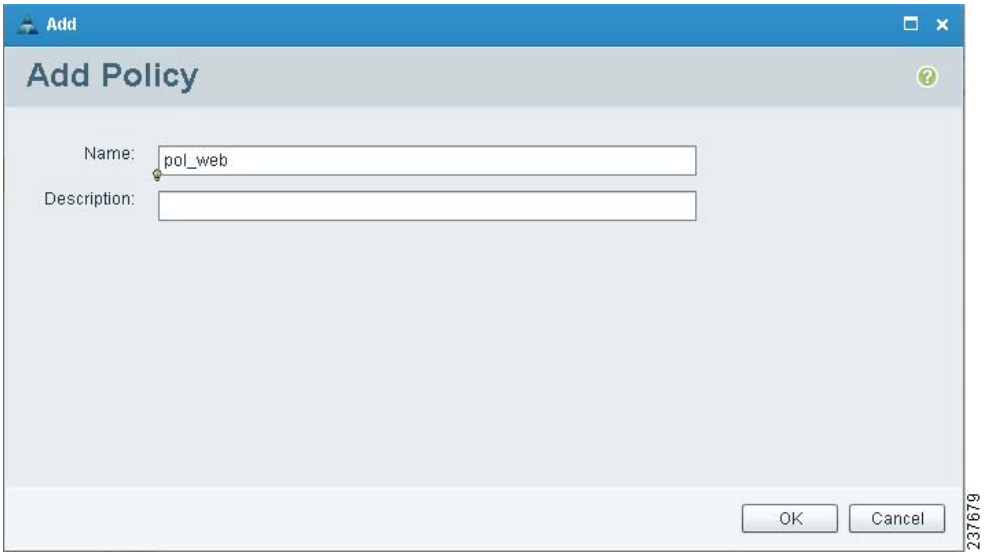
Figure 2-49 Virtual Network Management Center—Policy Management Policies Window



Step 2 Choose **Firewall Policy** > **root** > **Tenant-A** > **Policies**, right-click **Policies** and from the drop-down list, choose **Add Policy**.

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

Figure 2-50 Add Policy Dialog Box



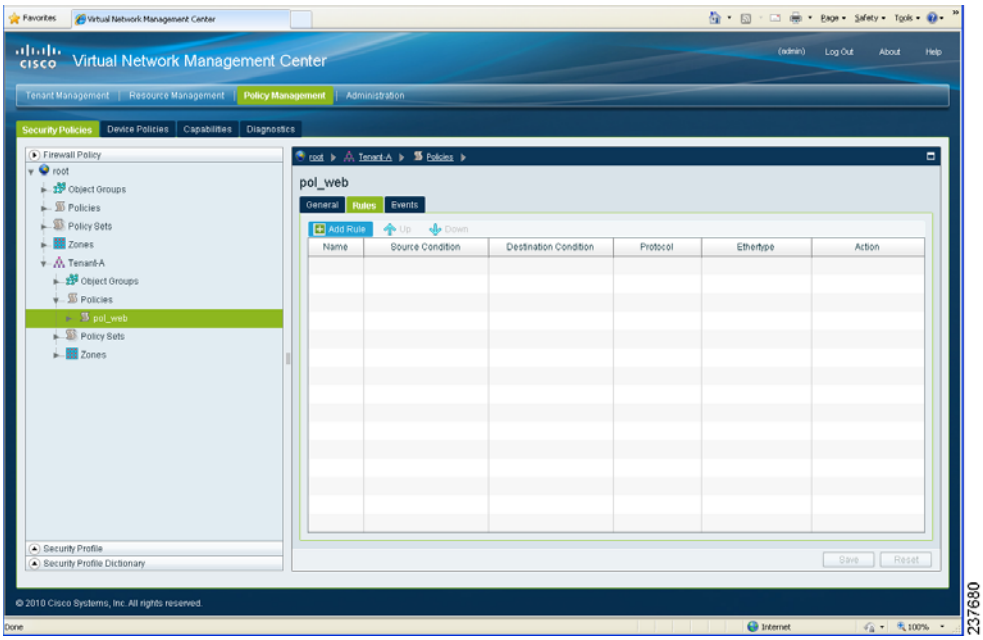
Step 3 Do the following:

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

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

Step 4 Click **OK**.

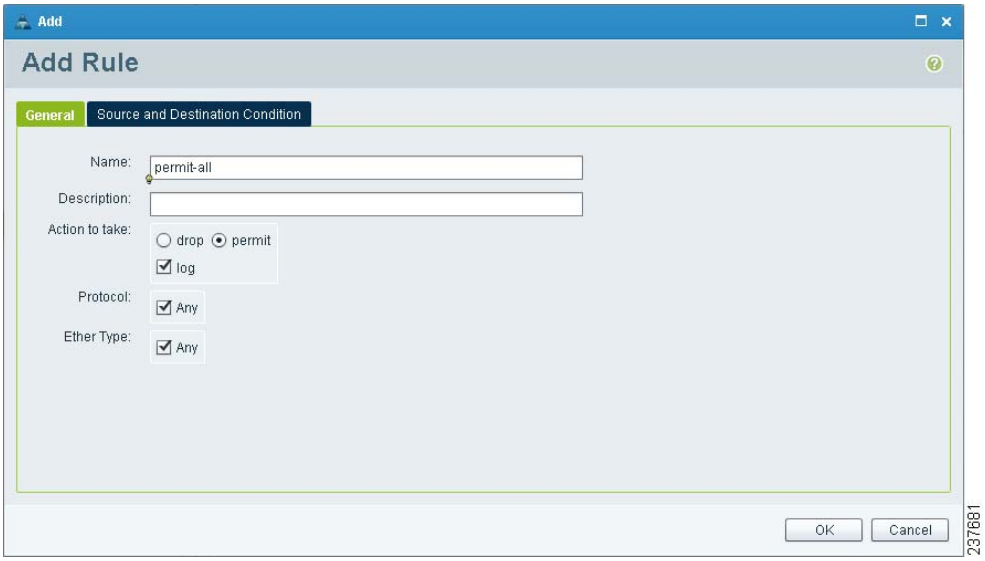
Figure 2-51 Virtual Network Management Center—Policy Management Window pol-web Pane



Step 5 Log in to VNMC, click **Policy Management** tab > **Security Policies** sub-tab.

Step 6 Click **Firewall Policy** > **root** > **Tenant-A** > **Policies** > **pol_web**. Click the **Rules** tab on the right side, click **Add Rule**. The Add Rule dialog box appears. See Figure 2-52.

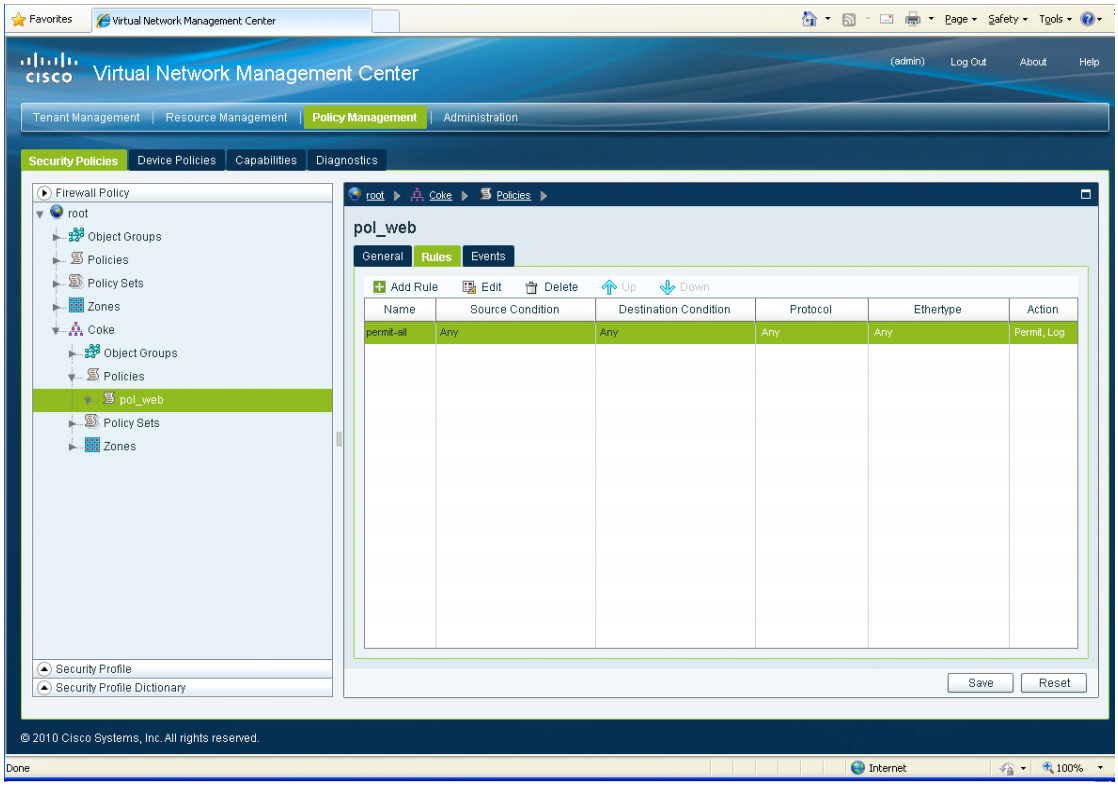
Figure 2-52 Add Rule Dialog Box



Step 7 Provide the name, select **Permit** and **Log** from the Actions and click **OK**.

The newly created rule is now listed in the pol-web pane. See Figure 2-53.

Figure 2-53 Virtual Network Management Center—Policy Management Window pol_web Rules Pane



Step 8 Click **Save** to save the configuration.

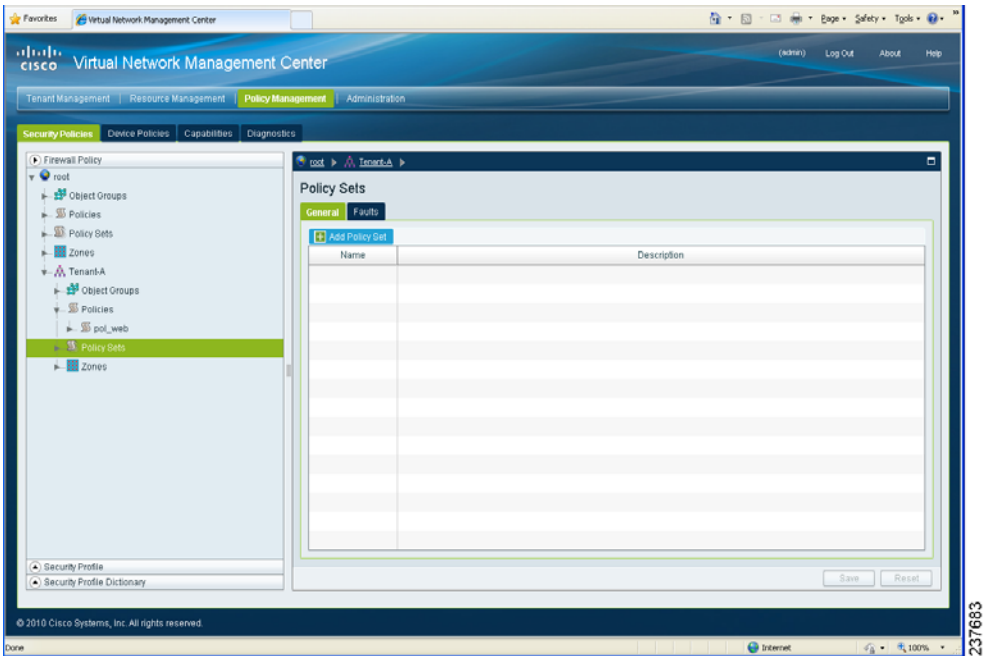
On the Cisco VNMC, Configuring a Policy Set

You can configure a policy set on the Cisco VNMC.

Step 1 From the Cisco VNMC main window, choose **Policy Management** > **Security Policies** > **root** > **Tenant-A** > **Policy Sets**.

The Cisco VNMC Policy Management window opens to show the Policy Sets pane. See Figure 2-54.

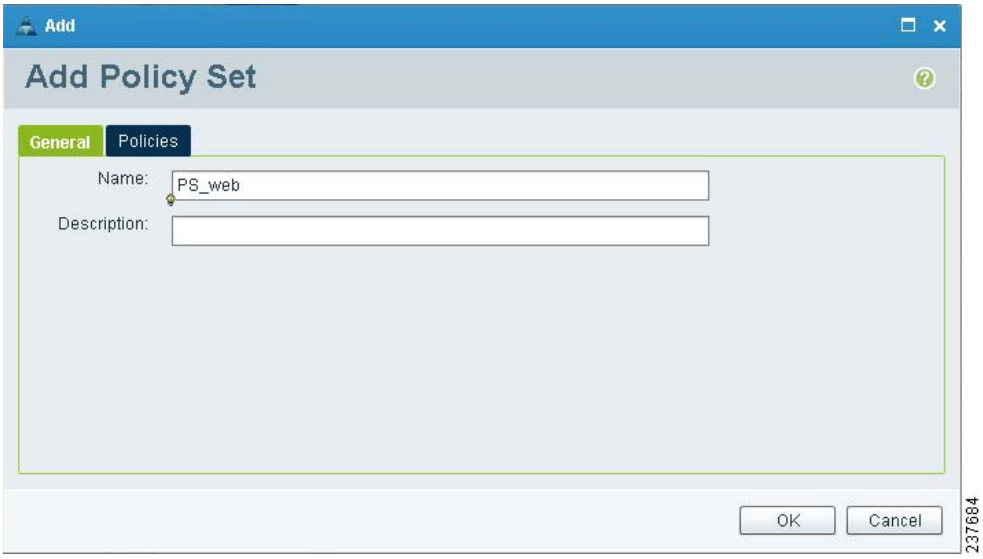
Figure 2-54 Virtual Network Management Center—Policy Management Window Policy Sets Pane



Step 2 Choose **Add Policy Set**.

The Add Policy Set dialog box opens. See Figure 2-55.

Figure 2-55 Add Policy Set Dialog Box



Step 3 From the General view of the Add Policy Set dialog box, do the following:

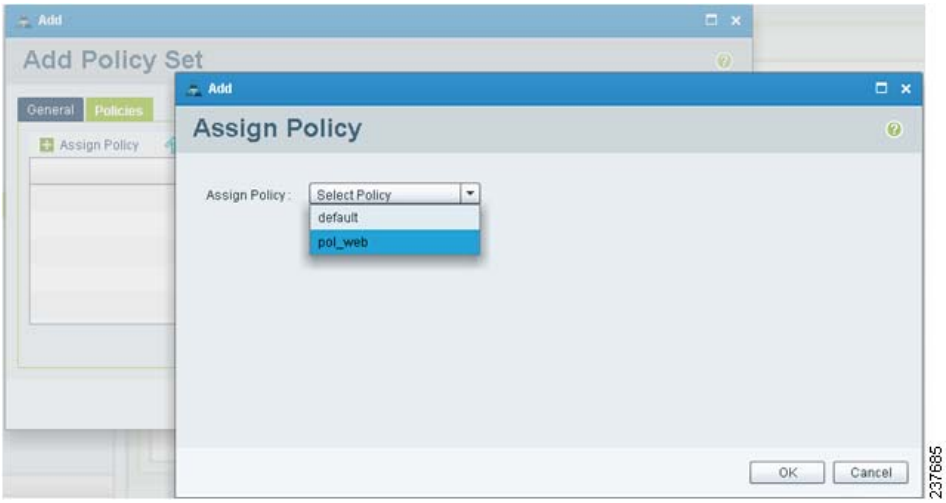
a. In the **Name** field, enter the policy set name.

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

Step 4 From the Policies view of the Add Policy Set dialog box, click **Assign Policy**.

The Assign Policy dialog opens. See Figure 2-56.

Figure 2-56 Add Policy Set Dialog Box and Assign Policy Dialog Box



Step 5 From the **Assign Policy** drop-down list, choose **pol_web**.

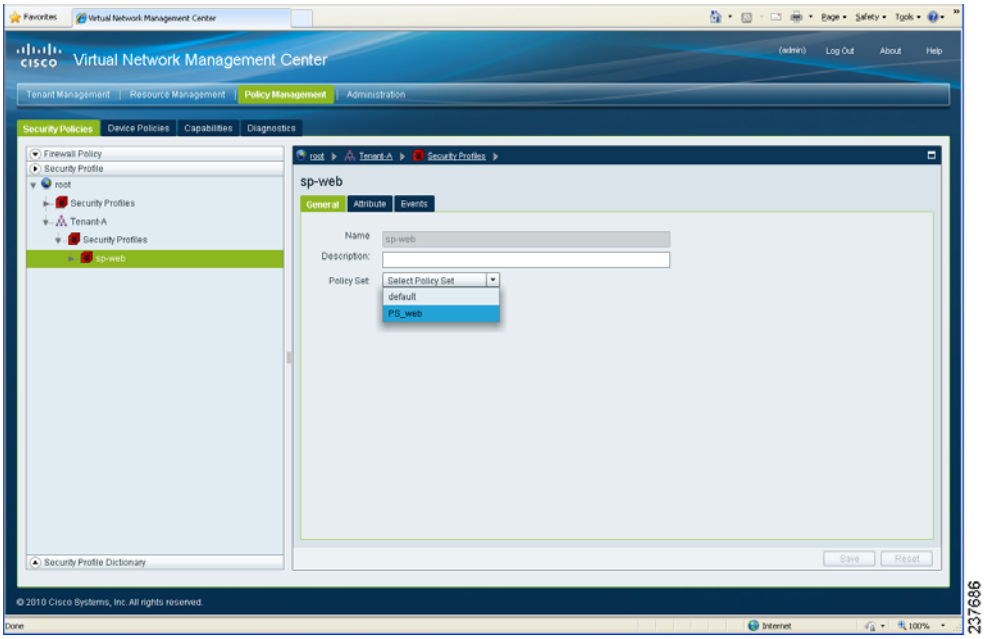
Step 6 Click **OK**.

Assign a Policy-Set to a Security Profile

Step 1 From the Cisco VNMC Policy Management window left panel directory tree, choose **Security Profile > root > Tenant-A > Security Profiles > sp-web**.

The Cisco VNMC Policy Management Window Security Profiles sp-web Pane opens. See Figure 2-57

Figure 2-57 Virtual Network Management Center—Policy Management Window



Step 2 Choose the **Policy Set** option on the right side sp-web panel and from the drop-down menu, select **PS_web**

Step 3 Click **Save** to save the configuration.

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.

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

```
vsg# show running-configure | 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

Enabling Logging Level 6 for Policy-Engine Logging

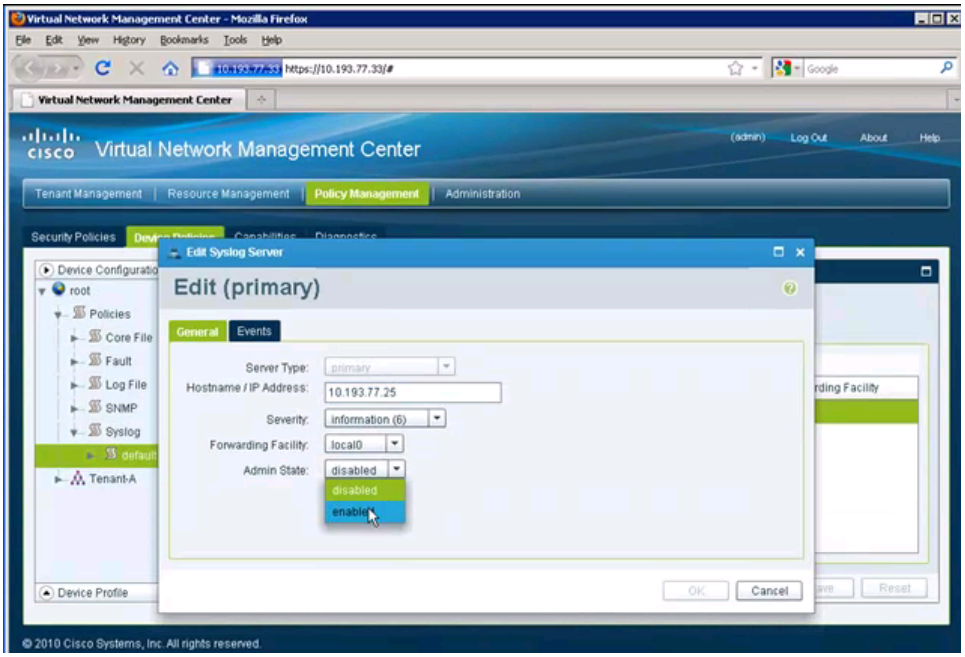
Logging enables you to see what traffic is going through your monitored virtual machine. This logging is helpful for verifying that you have a proper configuration and to help in troubleshooting.

Use the following steps to enable Logging Level 6 for policy-engine logging in a monitor sesson.

Step 1 Log in to the Cisco VNMC.

Step 2 Choose **Policy Management** > **Device Policies**. See Figure 2-58.

Figure 2-58 Virtual Network Management Center—Policy Management Window Edit Syslog Dialogue Box



Step 3 Click **Device Configuration** > **root** > **Policies** > **Syslog**. Click **Default** on the right side. Click **Edit**.

Step 4 Click **Servers**. Choose the primary server type from the displayed list.

Step 5 Click **Edit**. In the Hostname/IP address field, type in the syslog server IP address.

Step 6 Select **Information(6)** from the Severity drop-down list.

Step 7 Select **Enabled** from the Admin State drop-down list.

Step 8 Click **OK**.

Enabling Global Policy-Engine Logging

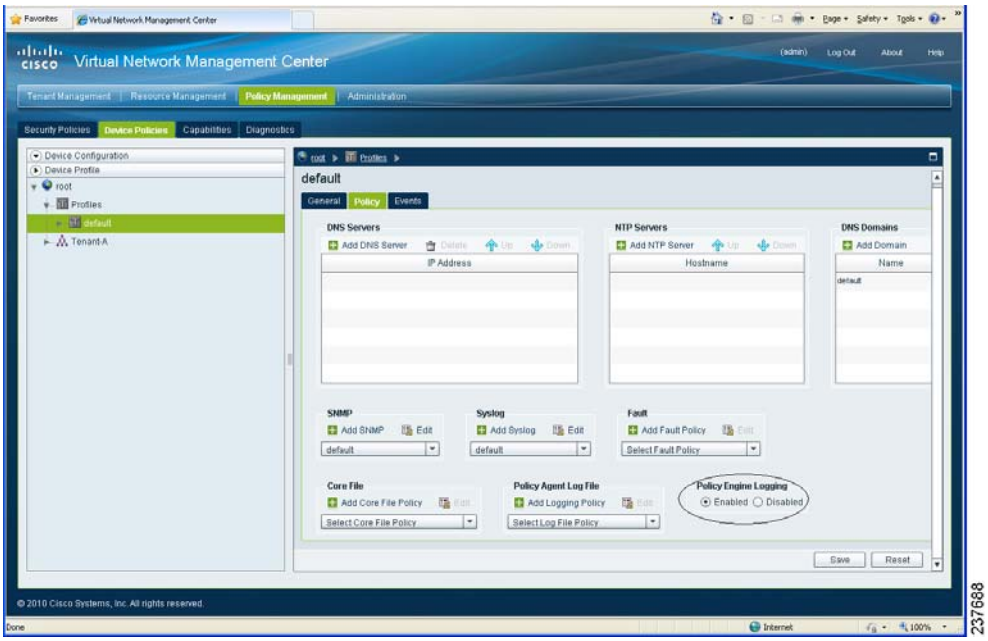
Logging enables you to see what traffic is going through your monitored virtual machine. This logging is helpful for verifying that you have a proper configuration and to help in troubleshooting.

Use the following steps to enable global policy-engine logging.

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

The Cisco VNMC Policy Management window opens with the default pane showing. See Figure 2-59.

Figure 2-59 Cisco VNMC—Policy Management Window Device Profile Default Policy Pane



Step 2 Choose the **Policy** tab on the right side default pane.

Step 3 Click **Enable** in the Policy Engine Logging area at the bottom of the pane.

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.

BEFORE YOU BEGIN

Make sure you have the following:

- 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

Enabling Traffic VM's Port-Profile for Firewall Protection

The following 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
```

The following example shows the commands required 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
```

The following 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

Verify **show vsn brief** to check 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.

Checking the VMs Veth Port for Firewall Protection

The following example shows how to verify **show vsn port vethernet** output:

```
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
```

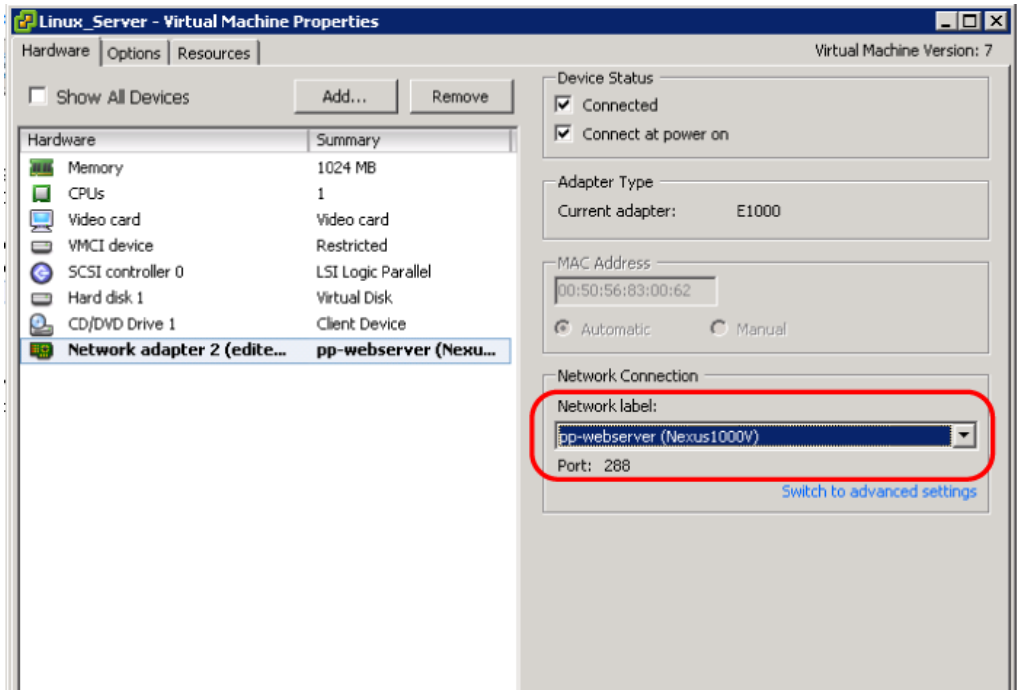
Note Make sure that your VNSP ID value is more than 1.

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

- Make sure that you have the VM (Server-VM) that is using port-profile (pp-webserver) configured for firewall protection.
- Log in to any of your client VM (Client-VM) and send traffic (for example, HTTP) to your Server-VM.
- Check the policy-engine statistics and log on the Cisco VSG.

Sending Traffic Flow

Figure 2-60 Virtual Machine Properties Window



Make sure that you have VM (Server-VM) configured with pp-webserver port-profile configured for firewall protection.

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 ~]#
```

On the Cisco VSG, Verifying Policy-Engine Statistics and Logs

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

The following example shows how to check these parameters:

Example:

```
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 Cisco Virtual Security Gateway

CHAPTER 3

Installing the Cisco Virtual Security Gateway

This document 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/ESXi platform running VMware software release 4.0.0 or 4.1.0 and requiring a minimum of 4-GB physical RAM to host a Cisco VSG VM.
- Virtual Machine (VM)
  - 32-bit VM is required and “Other 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

The following terminology is used in the Cisco Virtual Security Gateway implementation.

Table 3-1 Cisco Virtual Security Gateway Terminology

Term	Description
Distributed Virtual Switch (DVS)	This is a logical switch that spans one or more VMware ESX 4.0 servers. It is controlled by one VSM instance.
ESX/ESXi	A virtualization platform used to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine.
NIC	Network Interface Card.
Open Virtual Appliance or Application (OVA) file	The package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging. • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	A platform independent method of packaging and distributing virtual machines.
vCenter Server	A service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).
Virtual Ethernet Module (VEM)	This is the part of Nexus 1000 V Series switch that switches data traffic. It runs on a VMware ESX 4.0 host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual Data Center as defined by VMware vCenter Server.
Virtual Machine (VM)	A 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	The practice of migrating virtual machines live from server to server. (The VSGs cannot be moved by vMotion.)
vPath	A component in the Cisco Nexus 1000V Series switch VEM, it directs the appropriate traffic to the VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the VSG.
Virtual Security Gateway (VSG)	VSG 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)	This is the control software of the Cisco Nexus 1000V Series distributed virtual switch. It runs on a virtual machine (VM) and is based on Cisco NX-OS.
vSphere Client	The user interface that lets users 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 VSG Software

Before installing the VSG, the following prerequisites must be satisfied.

For a VSG to function, 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 need not be the system VLAN).
- On the Cisco Nexus 1000V Series switch configure two port profiles for the VSG: one for the service VLAN and the other for the HA VLAN. (You will be configuring the VSG IP address on the 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 VSG Software

How and where to obtain the Cisco VSG software files:

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

Note For the VSG to function in your network, you also must meet specific prerequisites. See the "Prerequisites to Installing VSG Software" section on page 3-3.

Installing the VSG Software

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

This section includes the following topics:

Installing the VSG Software from an OVA File

To install the 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

Have the following information available:

- A name for the new VSG that is unique within the inventory folder and up to 80 characters long.
- The name of the host where the 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 VSG IP address.
- Decide on what mode in which you will be installing the VSG:
  - Standalone
  - HA Primary
  - HA Secondary
  - Manual Installation

The following steps specifically present those for installing a standalone instance of a VSG.

DETAILED STEPS

Step 1 From the vSphere Client menu, choose the data center where you want to install the OVA file for the 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, add a name for the VSG that is unique within the inventory folder and less than 80 characters long.

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

The Host or Cluster window opens.

Step 12 Choose the host where the 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.

a. In the Cisco VSG HA ID field, enter a unique number between 1 and 4095. This number helps you 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. Click **Next**.

Step 18 If the settings are correct, click **Finish.**

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

Step 19 Click **Close**.

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

a. Power on the VSG you just created.

b. If you chose the Standalone mode for installation in Step 10, you will now see the VSG login prompt. Login with your 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(1).*

c. If you chose the Manual installation in Step 10, proceed to "Configuring Initial Settings" section on page 3-8 to configure the initial settings on the VSG.

Note If you are installing HA VSGs, you must configure the software on the primary VSG before installing the software on the secondary VSG.

Installing the VSG Software from an ISO File

To install the Virtual Security Gateway from an ISO file, use the following procedure.

BEFORE YOU BEGIN

Have the following information available:

- A name for the new VSG that is unique within the inventory folder and up to 80 characters long.
- The name of the host where the 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 VSG IP address.

DETAILED STEPS

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 less than 80 characters long.

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

The Virtual Machine Version dialog box opens.

Step 7 Click the **Virtual Machine Version: 7** radio button to run on VMware ESX server version 4.0 or later and VMware Server 2.0.

The Guest Operating System dialog box opens.

Step 8 Click the Linux radio button.

Step 9 In the Version field, 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, choose **1** from the drop-down list. Click **Next**.

The Memory dialog box opens.

Step 11 Choose **2GB** memory size. Click **Next**.

The Create Network Connectors dialog box opens.

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

Step 13 In the Network pane, choose service, management, and HA port profiles in that sequence from the NIC 1, NIC 2, and NIC 3 drop-down lists as required. Choose VMXNET3 for the adapter type for NIC 1. Choose E1000 for the adapter type for NIC 2 and NIC 3. 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 box. 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 locate your ISO file from the drop-down menu.

Step 22 In the Device Status pane, check the **Connect at power on** box. 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 click **Power on the virtual machine** in the VM pane.

Step 25 Click the **Console** tab to view the VM console and wait for the Install Virtual Firewall and bring up the new image to boot.

Proceed to "Configuring Initial Settings" section on page 3-8 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 menu.
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 3-10

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 into the Cisco VSG to configure initial settings at the console on your vSphere Client.

For details about installing Cisco VSG, see the "Installing the 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.

Use the following procedure to configure the Cisco VSG with its initial settings:

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 passsword 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 provide is identical to the other Cisco VSG in the pair.

Step 5 Enter the basic system configuration setup dialog.

The following 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 VSG node.

Configuring Initial Settings on a Standby Cisco VSG

To add a standby Cisco VSG, login to the Cisco VSG you have identified as secondary and use the following procedure to configure a standby Cisco VSG with its initial settings:

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 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 these tasks:

Table 3-3 Verifying VSG Configuration

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

These examples show 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 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.

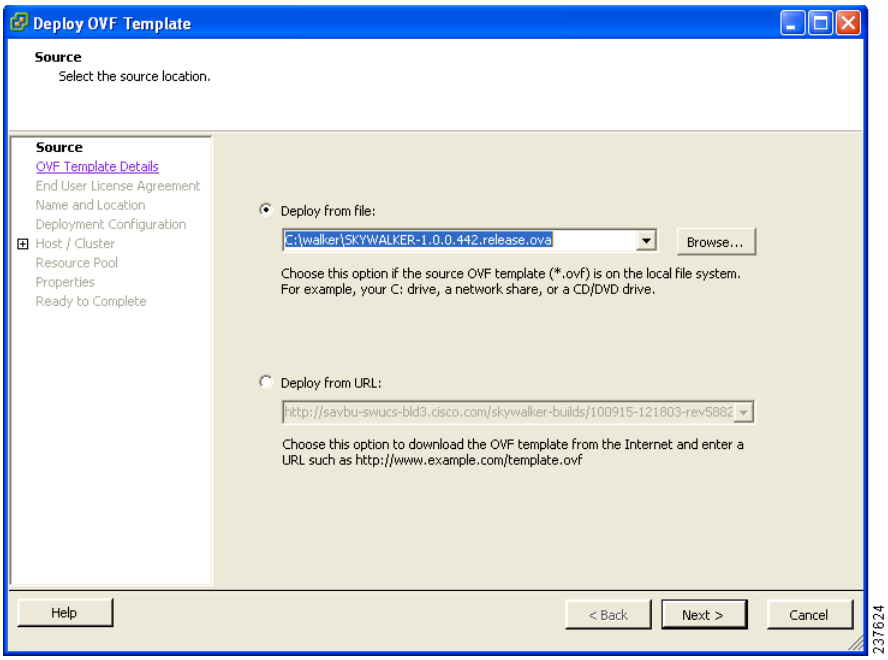
Information About Deploying the OVF Template

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 post-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



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

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 vSphere 4.0 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 Passwords are not masked when you enter 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

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 there are any issues with the restore, 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 **VNM 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 VNM 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

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 your virtual machine has the proper HDD size.

b. Ensure your virtual machine has 2-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**.

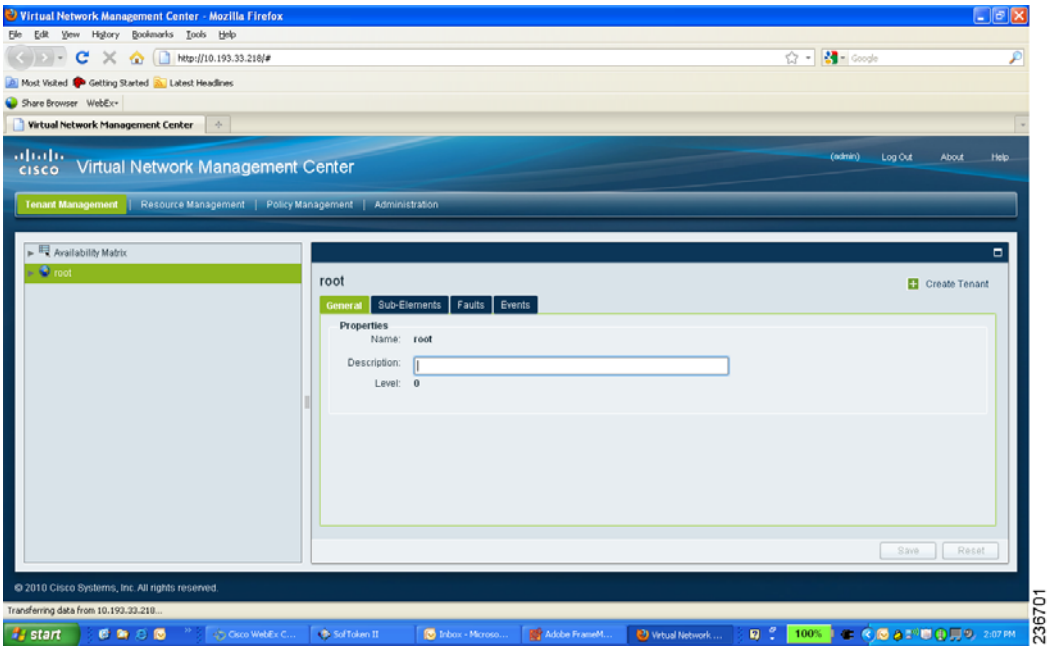
The login dialog box for Cisco VNMC appears.

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 first page of the Cisco VNMC.

Figure 4-2 Cisco VNMC



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)# show providers
```

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 Nexus-1000v-pa-mzg.VSG1.0.414.bin file into the Cisco VSG bootflash:.

```
vsg# copy ftp://guest@172.18.217.188/n1kv/nexus-1000v-pa-mzg.VSG1.0.414.bin bootflash:
```

Step 2 On the command line, enter the **configure** command to enter configuration mode:

```
vsg# configure
```

Step 3 Enter the **vnm-policy-agent** command to enter config-vnm-policy-agent mode:.

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

Step 4 Enter the **registration-ip** *vnmc ip address* command to set the Cisco VSG registration IP address:

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

Step 5 Enter the **shared-secret** *your password* command to assign a strong password for the Cisco VSG:

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

Step 6 Enter the **policy-agent-image** *the policy agent you copied* command to install the policy agent:

```
vsg (config-vnm-policy-agent)# policy-agent-image
bootflash:nexus-1000v-pa-mzg.VSG1.0.414.bin
```

Step 7 Exit all modes.

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

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

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

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

```
"VNM Policy-Agent status is - Installed Successfully. Version 1.0(0.414)-vsg"
```

The Cisco VSG registration is complete.

Step 9 On the command line, enter the **copy running-config startup-config** 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 nexus-1000v-vsmpa-mzg.4.2.1.SV1.3.414.bin file into the VSM bootflash:

```
vsm # copy ftp://guest@172.18.217.188/n1kv/nexus-1000v-vsmpa-mzg.4.2.1.SV1.3.414.bin
bootflash:
```

Step 2 On the command line, enter **configure** to enter configuration mode:

```
n1kv# configure
```

Step 3 Enter the **vnm-policy-agent** command to enter config-vnm-policy-agent mode:

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

Step 4 Enter the **registration-ip** *vnmc ip address* command to set the 1000V registration IP address:

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

Step 5 Enter the **shared-secret** *your password* command to assign a strong password for the VSG:

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

Step 6 Enter the **policy-agent-image** *the policy agent you copied* command to install the policy agent:

```
n1kv (config-vnm-policy-agent)# policy-agent-image
bootflash:nexus-1000v-vsmpa-mzg.4.2.1.SV1.3.414.bin
```

Step 7 Exit all modes.

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

Step 8 On the command line, enter **show vnm-pa status**.

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

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

"VNM Policy-Agent status is - Installed Successfully. Version 1.0(0.414)-vsm"

The Cisco Nexus 1000V VSM registration is completed.

Step 9 On the command line, enter **copy running-config startup-config**.

```
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 then 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 then 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 on **Add VM Manager**.

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

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

vCenter is registered.

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

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.

DETAILED STEPS

Step 1 Open your vSphere client.

Step 2 Click **Hosts and Clusters**, and then 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 then 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 then click **Next**.

The End User License Agreement page appears.

Step 9 View the license, and then 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 VNM Installer page appears.

Step 14 From the Configuration drop-down list, choose **VNM Installer**.

Step 15 Click **Next**.

Step 16 Choose the appropriate network, and then 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 VNM DNS area, enter an IP address in the DNS field.

Step 19 In the VNM DNS area, enter a hostname in the Host Name field and a domain name in the Domain Name field.

Step 20 In the VNM 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 the VNM 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 then 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 has the proper HDD size.
- **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, Send 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.

Send document comments to vsg-docfeedback@cisco.com

INDEX

I

L

M

N

O

P

R

S

T

V

X

Z