



Send document comments to vsg-docfeedback@cisco.com



Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide

July 4, 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-25314-02

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

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

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

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

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

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

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

Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide
© 2011 Cisco Systems, Inc. All rights reserved.

Send document comments to vsg-docfeedback@cisco.com



CONTENTS

Preface v

Audience v

Organization v

Conventions vi

Related Documentation vii

 Cisco Virtual Security Gateway Documentation vii

 Cisco Virtual Network Management Center Documentation vii

 Cisco Nexus 1000V Series Switch Documentation viii

Obtaining Documentation and Submitting a Service Request viii

CHAPTER 1

Overview 1-1

Information About Installing the Cisco Virtual Network Management Center and the Cisco Virtual Security Gateway 1-1

Information About Cisco Virtual Security Gateway 1-1

 VNMC and VSG Architecture 1-2

 Trusted Multitenant Access 1-3

 Dynamic (Virtualization-Aware) Operation 1-4

 Setting Up the Cisco VSGs and VLANs 1-5

Information About the Cisco Virtual Network Management Center 1-6

 Cisco VNMC Components 1-6

 Cisco VNMC Key Benefits 1-7

 Cisco VNMC Architecture 1-7

 Cisco VNMC Security 1-8

 Cisco VNMC API 1-8

 Cisco VNMC and VSM 1-8

 System Requirements 1-8

Information About High Availability 1-9

PART 1

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

CHAPTER 2

Quick Start Guide for the Cisco Virtual Security Gateway and the Cisco Virtual Network Management Center 2-1

Information About Installing Cisco VNMC and Cisco VSG 2-2

Send document comments to vsg-docfeedback@cisco.com

- Cisco VSG and Cisco VNMC Installation Planning Checklists 2-2
- Host Requirements 2-6
- Obtaining the Cisco VNMC and the Cisco VSG Software 2-6
- Task 1—Installing Cisco VNMC Software from an OVA Template 2-6
- Task 2—On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity 2-15
 - Downloading the vCenter Extension File from the Cisco VNMC 2-15
 - Registering the vCenter Extension Plugin in the vCenter 2-18
 - Configuring the vCenter in VM-Manager in the Cisco VNMC 2-19
- Task 3—On the VSM, Configuring the Cisco VNMC Policy-Agent 2-21
- Task 4—On the VSM, Preparing Cisco VSG Port Profiles 2-22
- Task 5—Installing the Cisco VSG from an OVA Template 2-23
- Task 6—On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy Agent Status 2-34
- Task 7—On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall 2-35
 - Configuring a Tenant in the Cisco VNMC 2-38
 - Configuring a Security Profile in the Cisco VNMC 2-39
 - On the Cisco VNMC, Configuring a Compute Firewall 2-41
- Task 8—On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall 2-43
- Task 9—On the Cisco VNMC, Configuring a Permit-All Rule 2-45
- Task 10—On the Cisco VSG, Verifying the Permit-All Rule 2-51
- Task 11—Enabling Logging 2-52
 - Enabling Logging Level 6 for Policy-Engine Logging 2-52
 - Enabling Global Policy-Engine Logging 2-55
- Task 12—Enabling the Traffic VM’s Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG 2-56
 - Enabling Traffic VM’s Port-Profile for Firewall Protection 2-56
 - Verifying the VSM/VEM for Cisco VSG Reachability 2-56
 - Checking the VM Veth Port for Firewall Protection 2-57
- Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs 2-57
 - Sending Traffic Flow 2-57
 - On the Cisco VSG, Verifying Policy-Engine Statistics and Logs 2-59

PART 2

Installation Guide for the Cisco Virtual Security Gateway

CHAPTER 3

Installing the Cisco Virtual Security Gateway 3-1

- Information About the Cisco VSG 3-1
 - Host and VM Requirements 3-1
 - Cisco Virtual Security Gateway and Supported Cisco Nexus 1000V Series Switch Terminology 3-2
- Prerequisites to Installing Cisco VSG Software 3-3

Send document comments to vsg-docfeedback@cisco.com

Obtaining the Cisco VSG Software	3-3
Installing the Cisco VSG Software	3-3
Installing the Cisco VSG Software from an OVA File	3-3
Installing the VSG Software from an ISO File	3-6
Configuring Initial Settings	3-7
Configuring Initial Settings on a Standby Cisco VSG	3-9
Verifying the Cisco VSG Configuration	3-10
Where to Go Next	3-11

PART 3

Installation Guide for the Cisco Virtual Network Management Center

CHAPTER 4
Installing the Cisco Virtual Network Management Center 4-1

Information About Installing the Cisco VNMC	4-1
Information About Deploying the OVF Template	4-1
Installing the Cisco VNMC by Deploying the OVF Template	4-2
Restoring the Cisco VNMC by Deploying the OVF Template	4-3
Installing the Cisco VNMC Using an ISO Image	4-4
Connecting to the Cisco VNMC	4-5
Verifying Cisco VNMC Providers	4-6

CHAPTER 5
Registering Devices With the Cisco VNMC 5-1

Registering a Cisco VSG	5-1
Registering a Cisco Nexus 1000V VSM	5-2
Registering vCenter	5-3

PART 4

Installing the Cisco VSG on a Cisco Nexus 1010 Appliance

CHAPTER 6
Installing the Cisco Virtual Security Gateway on a Cisco Nexus 1010 Virtual Services Appliance 6-1

Information About Installing the Cisco VSG on the Cisco N1010	6-1
Prerequisites	6-2
Guidelines and Limitations	6-2
Installing a Cisco VSG on a Cisco Nexus 1010	6-3

PART 5

Upgrading the Cisco VSG and the Cisco VNMC

Send document comments to vsg-docfeedback@cisco.com

CHAPTER 7

Upgrading the Cisco Virtual Security Gateway and Cisco Virtual Network Management Center 7-1

- Information About Cisco VSG Upgrades 7-1
- Information About Cisco VNMC Upgrades 7-1
- Upgrade Procedure in Sequence 7-2
 - Upgrading a Cisco VSG Pair 7-2
 - Upgrading the VSM Pair 7-4
 - Using the copy running-config startup-config Command on the Active VSM 7-4
 - Upgrading the VEM 7-4
 - Upgrading Cisco VNMC 7-4
 - Upgrading the VSM-PA 7-6
 - Upgrading the Cisco VSG-PA 7-7
- Upgrade Compatibility Matrix 7-8

APPENDIX A

Examples of Cisco VNMC OVA Template Deployment and Cisco VNMC ISO Installations A-1

- OVA Installation Using vSphere 4.0 Installer A-1
- OVA Installation Using an ISO Image A-3

INDEX

Send document comments to vsg-docfeedback@cisco.com



Preface

The *Cisco Virtual Security Gateway, Rel. 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Rel. 1.2 Installation and Upgrade Guide* provides procedures for installing Cisco Virtual Security Gateway (VSG) and Cisco Virtual Network Management Center (VNMC).

This preface includes the following sections:

- [Audience, page v](#)
- [Organization, page v](#)
- [Conventions, page vi](#)
- [Obtaining Documentation and Submitting a Service Request, page viii](#)

Audience

This guide is for the following professionals who have 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 (Cisco Nexus 1000V equivalent port-profile) for the particular virtual machines (VM).

Organization

This guide includes the following sections:

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

Send document comments to vsg-docfeedback@cisco.com

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

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

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	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*.

Send document comments to vsg-docfeedback@cisco.com



Caution

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



Timesaver

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



Warning

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

Related Documentation

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

Cisco Virtual Security Gateway Documentation

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

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

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(2)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Release 1.2 Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(2)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(2)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(2)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(2)*

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 1.2*

Send document comments to vsg-docfeedback@cisco.com

- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(2) and Cisco Virtual Network Management Center, Release 1.2 Installation and Upgrade Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.2*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.2*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.2*

Cisco Nexus 1000V Series Switch Documentation

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

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Overview

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

This chapter includes the following sections:

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

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

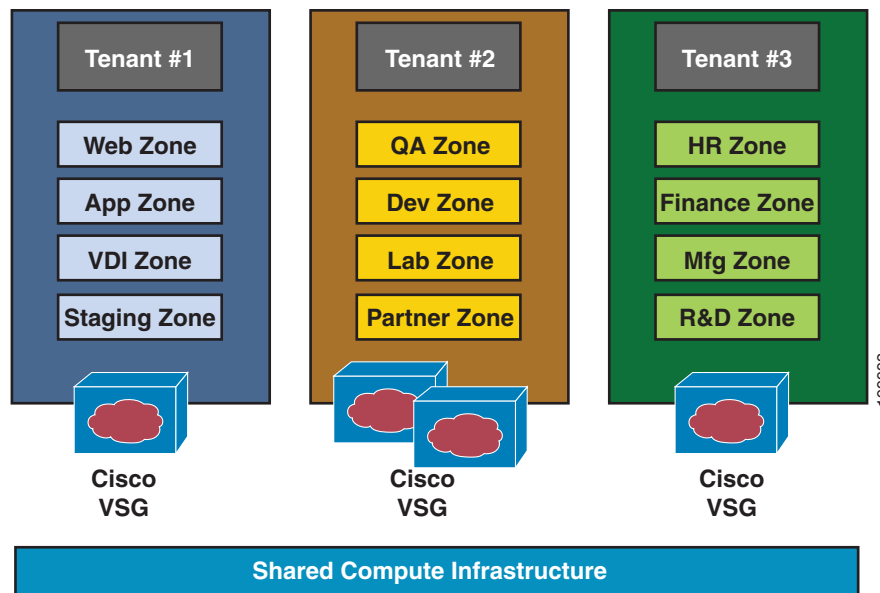
You must install the Cisco Virtual Network Management Center (Cisco VNMC) and the Cisco Virtual Security Gateway (Cisco VSG) in a particular sequence on the Cisco Nexus 1000V switch in order to have a functioning virtual system. Part 1, the *Quick Start Guide for Cisco Virtual Security Gateway and Cisco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

Information About Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments with dynamic policy-driven operation, mobility-transparent enforcement, and scale-out deployment for dense multitenancy. By associating one or more virtual machines (VMs) into distinct trust zones, the Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies. [Figure 1-1](#) shows the trusted zone-based access control that is used in per-tenant enforcement with the Cisco VSG.

Send document comments to vsg-docfeedback@cisco.com

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



VNMC and VSG Architecture

The Cisco VSG operates with the Cisco Nexus 1000V Series switch in the VMware vSphere Hypervisor or the Cisco Nexus 1010 Virtual Services Appliance, and the Cisco VSG leverages the virtual network service data path (vPath) (see [Figure 1-2](#)). vPath steers traffic, whether external to VM or VM to VM, to the Cisco VSG of a tenant. Initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement. After the policy decision is made, the Cisco VSG offloads policy enforcement of the remaining packets to vPath.

vPath supports the following features:

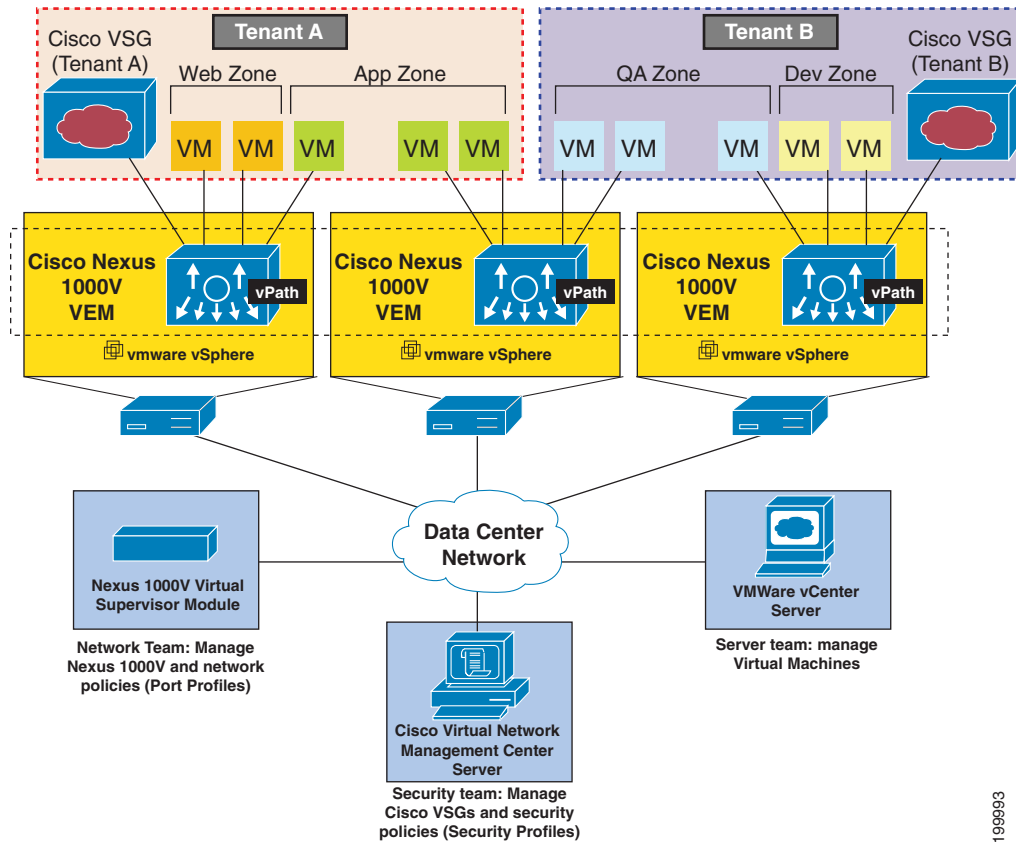
- Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant
- Per-tenant policy enforcement of flows offloaded by Cisco VSG to vPath

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

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

Send document comments to vsg-docfeedback@cisco.com

Figure 1-2 Cisco Virtual Security Gateway Deployment Topology



Trusted Multitenant Access

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

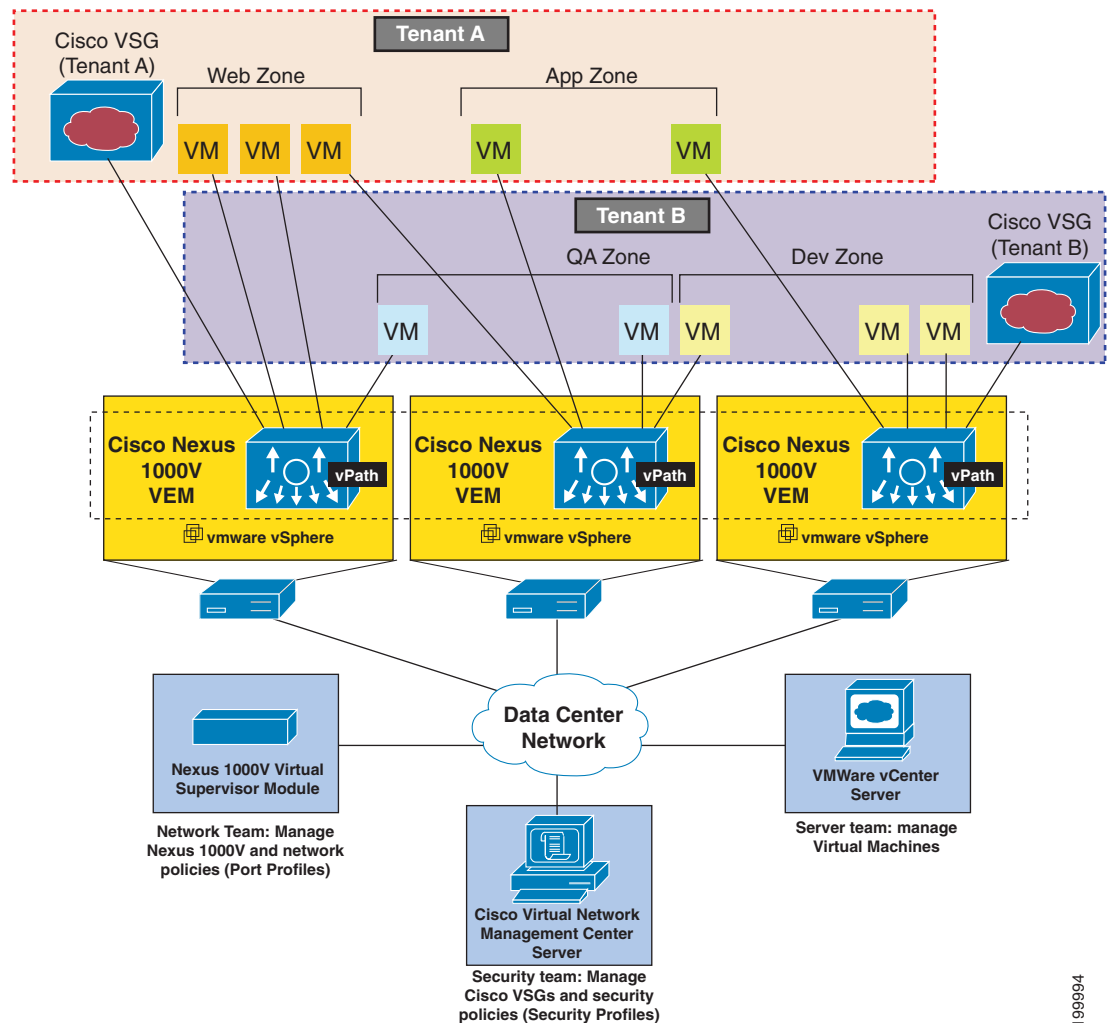
As you instantiate VMs for a given tenant, their association to security profiles (or zone membership) occurs immediately through binding with the Cisco Nexus 1000V port profile. Each VM is placed upon instantiation into a logical trust zone (see Figure 1-2). Security profiles contain context-aware rule sets that specify access policies for traffic that enters and exits each zone. In addition to VM and network contexts, security administrators can also leverage custom attributes that define zones directly through security profiles. You can apply controls to zone-to-zone traffic and to external-to-zone (and zone-to-external) traffic. Zone-based enforcement occurs within a VLAN because a VLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then offloads enforcement to the Cisco Nexus 1000V VEM vPath module. Upon enforcement, the Cisco VSG can permit or deny access and can generate optional access logs. Cisco VSG also provides policy-based traffic monitoring capability with access logs.

[Send document comments to vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)

Dynamic (Virtualization-Aware) Operation

A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. Live migration of VMs can occur due to manual or programmatic vMotion events. Figure 1-3 shows how 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. 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, the Cisco VSG immediately applies the security controls. You can repurpose a VM by assigning it to a different port profile or security profile.

199994

Send document comments to vsg-docfeedback@cisco.com

Information About the Cisco Virtual Network Management Center

The Cisco VNMC virtual appliance is 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, the Cisco VNMC enables you to manage Cisco VSGs that are deployed throughout the data center from a centralized location.

**Note**

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

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

This section includes the following topics:

- [Cisco VNMC Components, page 1-6](#)
- [System Requirements, page 1-8](#)

Cisco VNMC Components

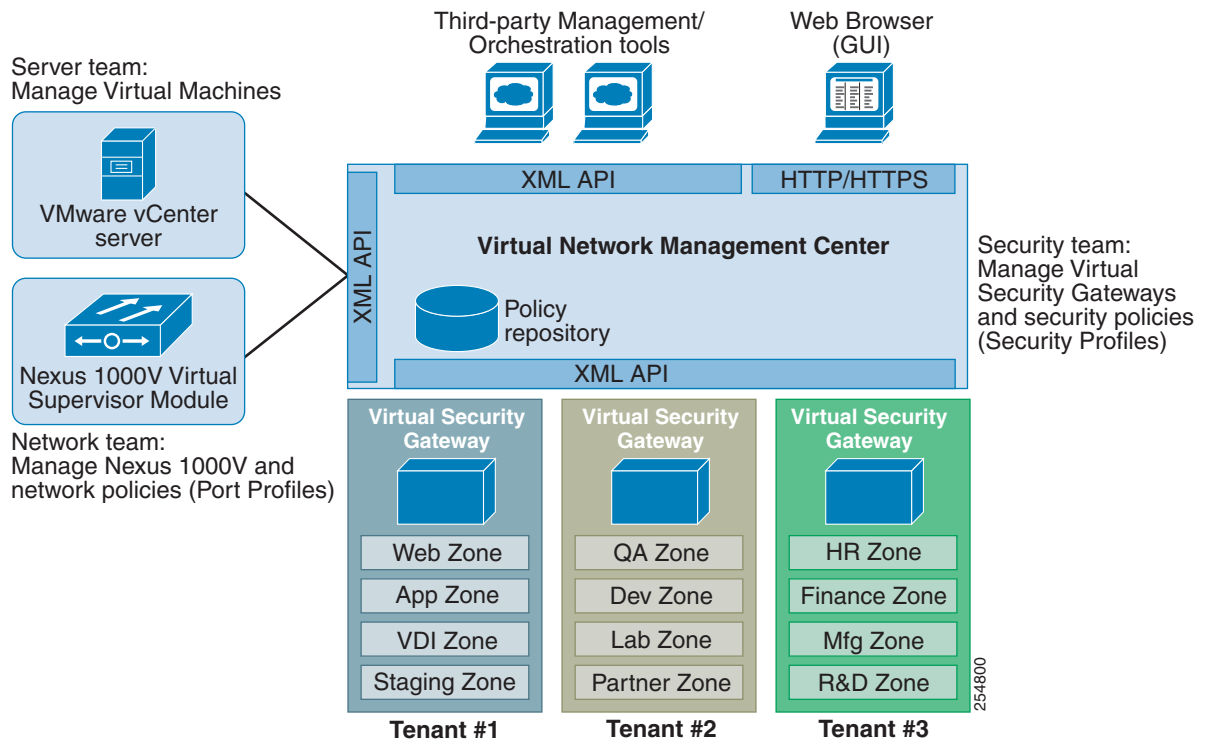
This section includes the following topics:

- [Cisco VNMC Key Benefits, page 1-7](#)
- [Cisco VNMC Architecture, page 1-7](#)
- [Cisco VNMC Security, page 1-8](#)
- [Cisco VNMC API, page 1-8](#)
- [Cisco VNMC and VSM, page 1-8](#)

[Figure 1-5](#) shows the Cisco VNMC components.

Send document comments to vsg-docfeedback@cisco.com

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.
- Greater collaboration across security and server administrators, while maintaining administrative separation and reducing administrative errors.

Cisco VNMC Architecture

The Cisco VNMC architecture includes the following components:

- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning. This function simplifies large scale deployments as follows:
 - Devices can be preinstantiated and then configured on demand
 - Devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools
- A distributed management-plane function that uses an embedded management agent on each device that allows for a scalable management framework.

Send document comments to vsg-docfeedback@cisco.com

Cisco VNMC Security

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

Cisco VNMC API

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

Cisco VNMC and VSM

The Cisco VNMC operates with the Cisco Nexus 1000V Virtual Supervisor Module (VSM) to achieve the following scenarios:

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

System Requirements

System requirements for a Cisco VNMC are as follows:

- x86 Intel or AMD server with a 64-bit processor listed in the VMware compatibility matrix
- Intel VT that is enabled in the BIOS
- VMware ESX 4.0, 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 Network File System/Storage Area Network (NFS/SAN) storage when the 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.

Send document comments to vsg-docfeedback@cisco.com

**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, see the VMware guides for HA and Fault Tolerance.

Send document comments to vsg-docfeedback@cisco.com



P A R T 1

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



CHAPTER 2

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

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

This chapter includes the following sections:

- [Information About Installing Cisco VNMC and Cisco VSG, page 2-2](#)
- [Host Requirements, page 2-6](#)
- [Obtaining the Cisco VNMC and the Cisco VSG Software, page 2-6](#)
- [Task 1—Installing Cisco VNMC Software from an OVA Template, page 2-6](#)
- [Task 2—On the Cisco VNMC, Setting Up VM-Mgr for vCenter Connectivity, page 2-15](#)
- [Task 3—On the VSM, Configuring the Cisco VNMC Policy-Agent, page 2-21](#)
- [Task 4—On the VSM, Preparing Cisco VSG Port Profiles, page 2-22](#)
- [Task 5—Installing the Cisco VSG from an OVA Template, page 2-23](#)
- [Task 6—On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy Agent Status, page 2-34](#)
- [Task 7—On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall, page 2-35](#)
- [Task 8—On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall, page 2-43](#)
- [Task 9—On the Cisco VNMC, Configuring a Permit-All Rule, page 2-45](#)
- [Task 10—On the Cisco VSG, Verifying the Permit-All Rule, page 2-51](#)
- [Task 11—Enabling Logging, page 2-52](#)
- [Task 12—Enabling the Traffic VM's Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, page 2-56](#)
- [Task 13—Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, page 2-57](#)

Send document comments to vsg-docfeedback@cisco.com

Information About Installing Cisco VNMC and Cisco VSG

This chapter presents an example of an effective way to install and set up a basic working configuration of the Cisco VNMC and Cisco VSG. The example in this chapter uses the OVF template method to install the OVA files of the software. The steps assume that the Cisco Nexus 1000V is up and running and endpoint VMs are already installed.

Cisco VSG and Cisco VNMC Installation Planning Checklists

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

This section includes the following checklists:

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

Table 2-1 Basic Hardware and Software Requirements

Item	Do You Have?	Your Information
1	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix	
2	Intel VT enabled in the BIOS	
3	VMware ESX 4.0, 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 the Cisco VSG and similar for the Cisco 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 the 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	

Send document comments to vsg-docfeedback@cisco.com**Table 2-2** Preparation of the Cisco Nexus 1000V Series Switch for Further Installation Processes



Item	Requirement	Your Information
1	Two VLANs that are configured on the Cisco Nexus 1000V Series switch uplink ports: the service VLAN and an HA VLAN (the VLAN do not need to be the system VLAN)	
2	Two port profiles that are configured on the Cisco Nexus 1000V Series switch: one port profile for the service VLAN and one port profile for the HA VLAN (you will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000V Series switch can communicate with it)	

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


Item	Type	Your Information
1	Cisco VSG name—unique within the inventory folder and up to 80 characters long	
2	Hostname—where the Cisco VSG will be installed in the inventory folder	
3	Datastore name—where the VM files will be stored	
4	Cisco VSG management IP address	
5	VSM management IP address	
6	Cisco VNMC instance IP address	
7	Mode for installing the Cisco VSG	<ul style="list-style-type: none"> • 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)	

Send document comments to vsg-docfeedback@cisco.com

Table 2-4 **Tasks, Descriptions, and Prerequisites Checklist**

Task	Description	Prerequisites	Completed
1	Installing the Cisco VNMC software from an OVA template	<p>Before starting the procedure, know or do the following:</p> <ul style="list-style-type: none"> • 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 that you want to use (this password is what enables communication between the Cisco VNMC, VSM, and Cisco VSG) • The DNS server and domain name information • The management port-profile name for the virtual machine (VM) (management) <p> Note The management port profile is the same port profile that is used for the VSM. The port profile is configured in the VSM and is used for the Cisco VNMC management interface.</p> <ul style="list-style-type: none"> • 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	<p>Before starting the procedure, know or do the following:</p> <ul style="list-style-type: none"> • Install Adobe Flash Player (Version 10.1.102.64 or later versions) • The IP address of the Cisco VNMC • The admin user password 	
3	On the VSM, configuring the Cisco VNMC policy agent	<p>Before starting the procedure, know or do the following:</p> <ul style="list-style-type: none"> • The Cisco VNMC policy-agent image is available on the VSM (for example, <code>vnmc-vsmpa.1.0.1j.bin</code>) <p> Note The string vsmpa must appear in the image name as highlighted.</p> <ul style="list-style-type: none"> • The IP address of the Cisco VNMC • The shared secret password that you defined during the Cisco VNMC installation • IP connectivity between the VSM and the Cisco VNMC is okay. 	
4	On the VSM, preparing the Cisco VSG port profiles	<p>Before starting the procedure, know or do the following:</p> <ul style="list-style-type: none"> • The uplink port-profile name • The VLAN ID for the Cisco VSG data interface (for example, 100) • The VLAN ID for the Cisco VSG HA interface (for example, 200) • The management VLAN (management) <p>None of these VLANs need to be system VLANs.</p>	

Send document comments to vsg-docfeedback@cisco.com

Task	Description	Prerequisites	Completed
5	Installing the Cisco VSG from an OVA template	<p>Before starting the procedure, know or do the following:</p> <ul style="list-style-type: none"> • Make sure that the Cisco VSG OVA image is available in the vCenter • Cisco VSG-data and Cisco VSG-HA port profile are created on the VSM • Management port profile (management) <p> Note The management port profile is the same port profile that is used for the VSM. The port profile is configured in the VSM and is used for the Cisco VNMC management interface.</p> <ul style="list-style-type: none"> • HA pair ID • IP/subnet mask/gateway information for the Cisco VSG • Admin password • 2-GB RAM and 3-GB hard disk space are available • Cisco VNMC IP • Shared secret password • IP connectivity between the Cisco VSG and the Cisco VNMC is okay • Cisco VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin) 	
6	On the Cisco VSG, verifying the VNM policy-agent Status	—	
7	On the Cisco VNMC, configuring a tenant and security profile	<p>Before starting the procedure, know or do the following:</p> <ul style="list-style-type: none"> • 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	—	

Send document comments to vsg-docfeedback@cisco.com

Task	Description	Prerequisites	Completed
12	Preparing Traffic VM's Port-Profile for Firewall Protection and Verifying the VSM/VEM	Make sure you have the following: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Make sure that you have the VM (Server-VM) that is using the port profile (pp-webserver) configured for firewall protection. • Log in to any of your client 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 installations have 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 requirements for the Cisco VNMC, or 6-GB for both.
- 1 processor
- CPU speed of 1.5 GHz

Obtaining the Cisco VNMC and the Cisco VSG Software

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

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

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

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

Task 1—Installing 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

Send document comments to vsg-docfeedback@cisco.com

- The admin password, shared_secret, hostname that you want to use
- The DNS server and domain name information
- The management port-profile name for the virtual machine (VM) (management)



Note

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

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

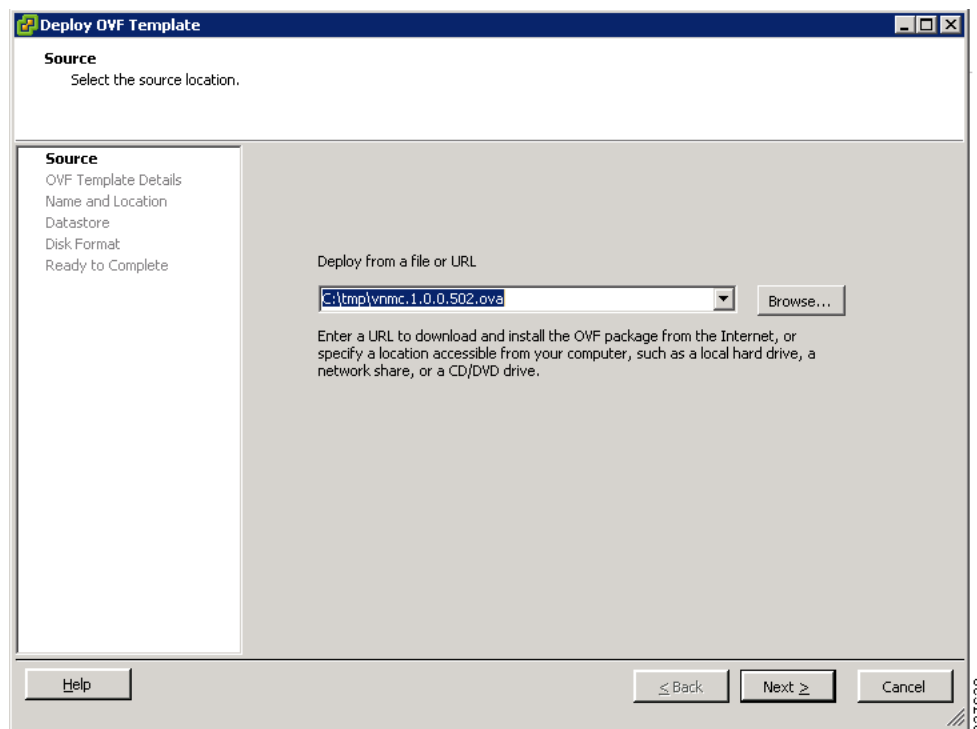
PROCEDURE

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

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

The Deploy OVF Template window opens. See [Figure 2-1](#).

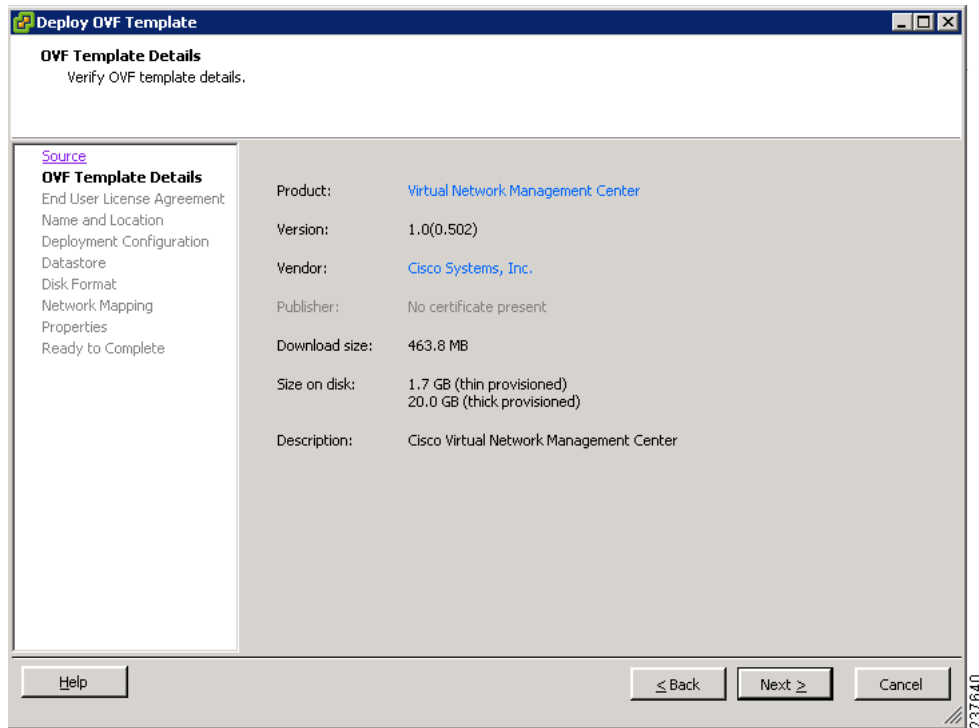
Figure 2-1 Deploy OVF Template—Source Window



Step 3 In the Deploy from a file or URL field, enter the path to the Cisco VNMC OVA file and click **Next**. The OVF Template Details window opens. See [Figure 2-2](#).

Send document comments to vsg-docfeedback@cisco.com

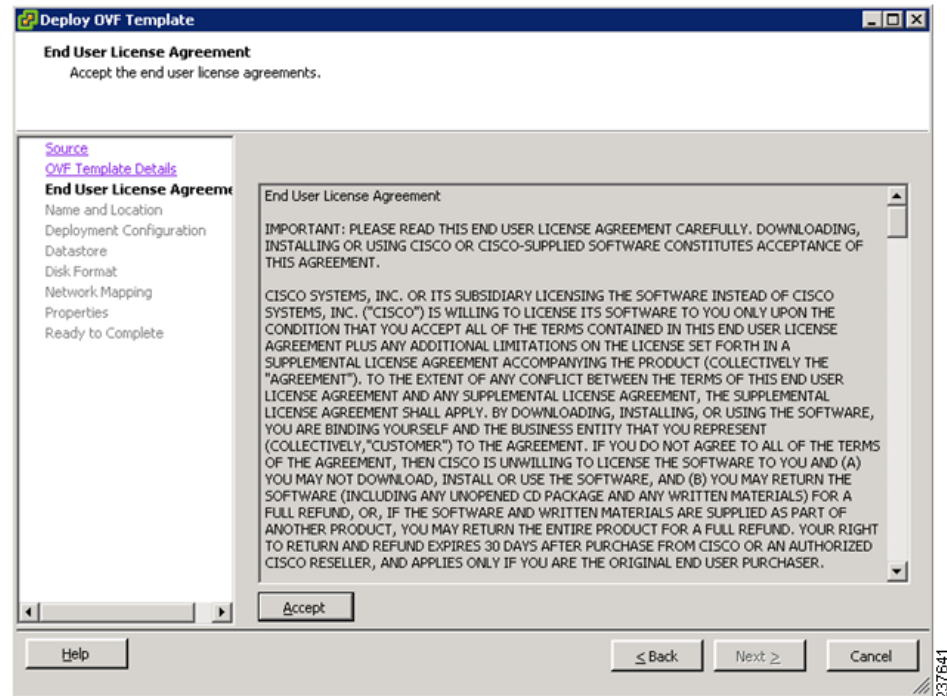
Figure 2-2 Deploy OVF Template—OVF Template Details Window



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

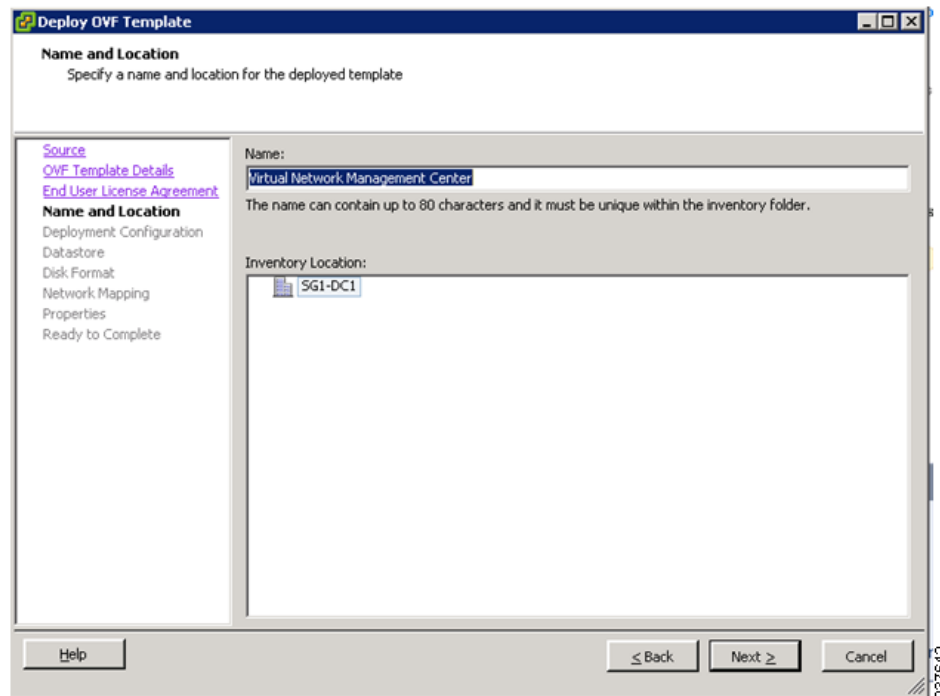


Step 5 Click **Accept** to accept the End User License Agreement and click **Next**.

Send document comments to vsg-docfeedback@cisco.com

The Name and Location window opens. See [Figure 2-4](#).

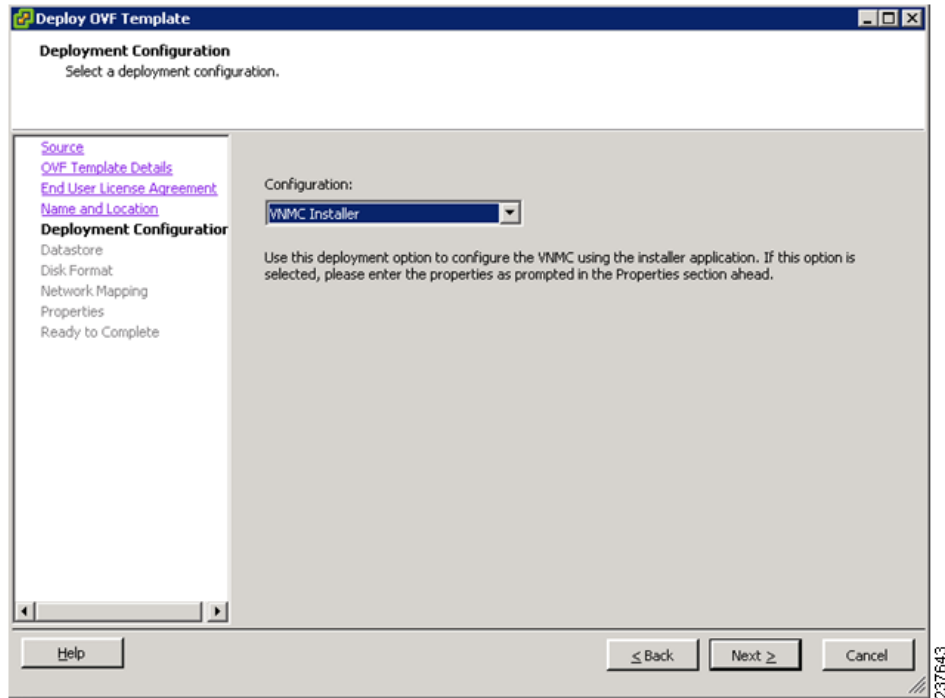
Figure 2-4 Deploy OVF Template—Name and Location



- Step 6** In the Name field, enter the name of the Cisco Virtual Network Management Center. The name can contain up to 80 characters and it must be unique within the inventory folder.
- Step 7** In the Inventory Location pane, choose the location that you would like to use and click **Next**. The Deployment Configuration window opens. See [Figure 2-5](#).

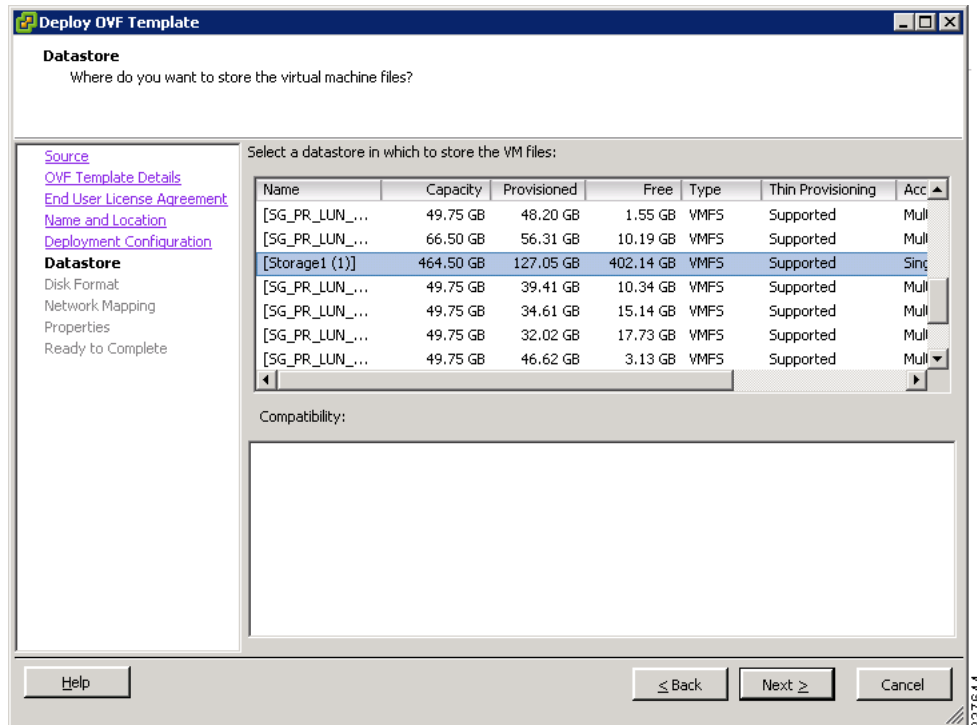
Send document comments to vsg-docfeedback@cisco.com

Figure 2-5 Deploy OVF Template—Deployment Configuration Window



- Step 8** From the Configuration drop-down list, choose **VNM 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**.

Send document comments to vsg-docfeedback@cisco.com



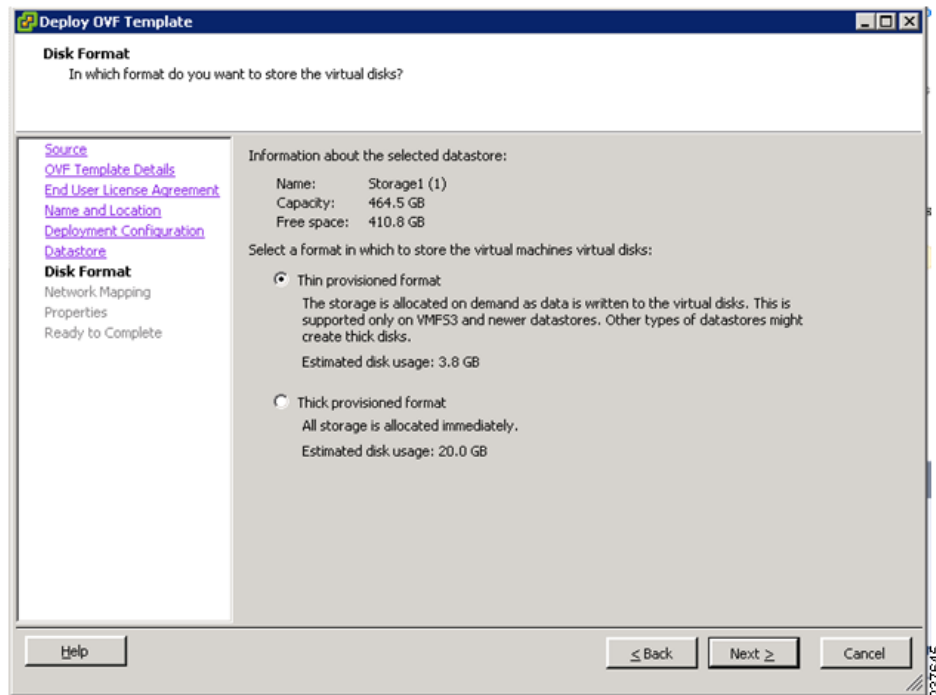
Note The storage can be local or shared remote such as the network file storage (NFS) or the storage area network (SAN).



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

The Disk Format window opens. See [Figure 2-7](#).

Figure 2-7 Deploy OVF Template—Disk Format Window



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



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

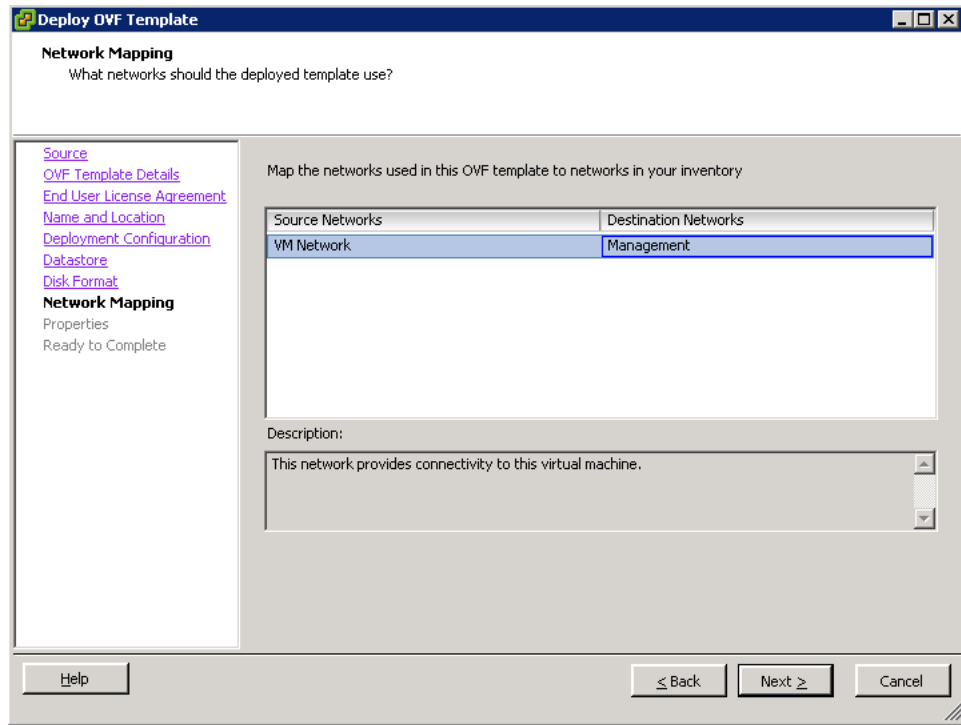


Note Ignore the red text in the window.

The Network Mapping window opens. See [Figure 2-8](#).

Send document comments to vsg-docfeedback@cisco.com

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](#).

Send document comments to vsg-docfeedback@cisco.com

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.

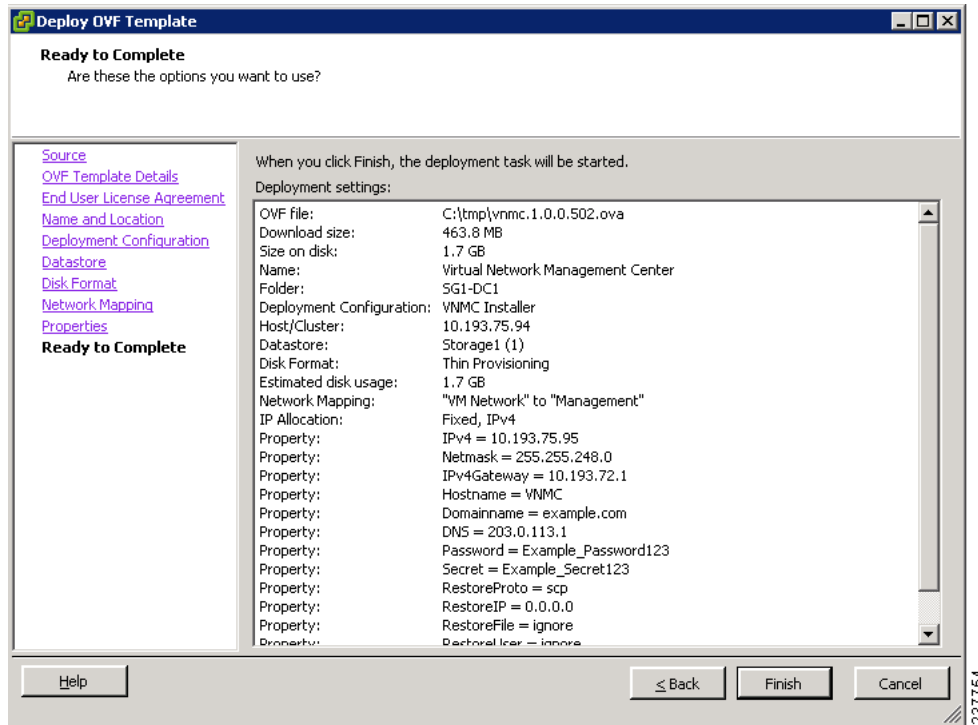


Note Ignore the VNM Restore fields.

The Ready to Complete window opens. See [Figure 2-10](#).

Send document comments to vsg-docfeedback@cisco.com

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



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

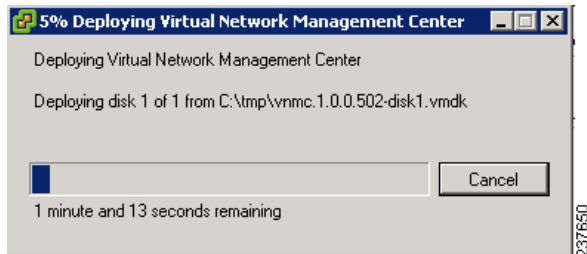


Note Review the IP/mask/gateway information carefully because any discrepancies might cause the VM to have bootup issues.

The Deploying Virtual Network Management Center progress indicator opens. See [Figure 2-11](#).

The progress bar in [Figure 2-11](#) shows how much of the deployment task is completed before the Cisco VNM is deployed.

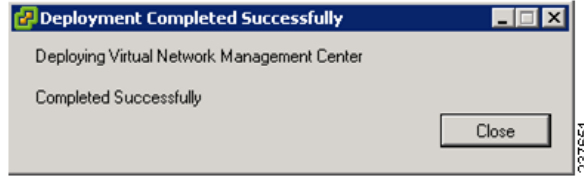
Figure 2-11 Deploying Virtual Network Management Center—Deploying Disk Files Progress Indicator



The progress indicator in [Figure 2-12](#) shows that the deployment has completed successfully.

Send document comments to vsg-docfeedback@cisco.com

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

This section includes the following topics:

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

BEFORE YOU BEGIN

Before doing this procedure, know or do the following:

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

Downloading the vCenter Extension File from the Cisco VNMC

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

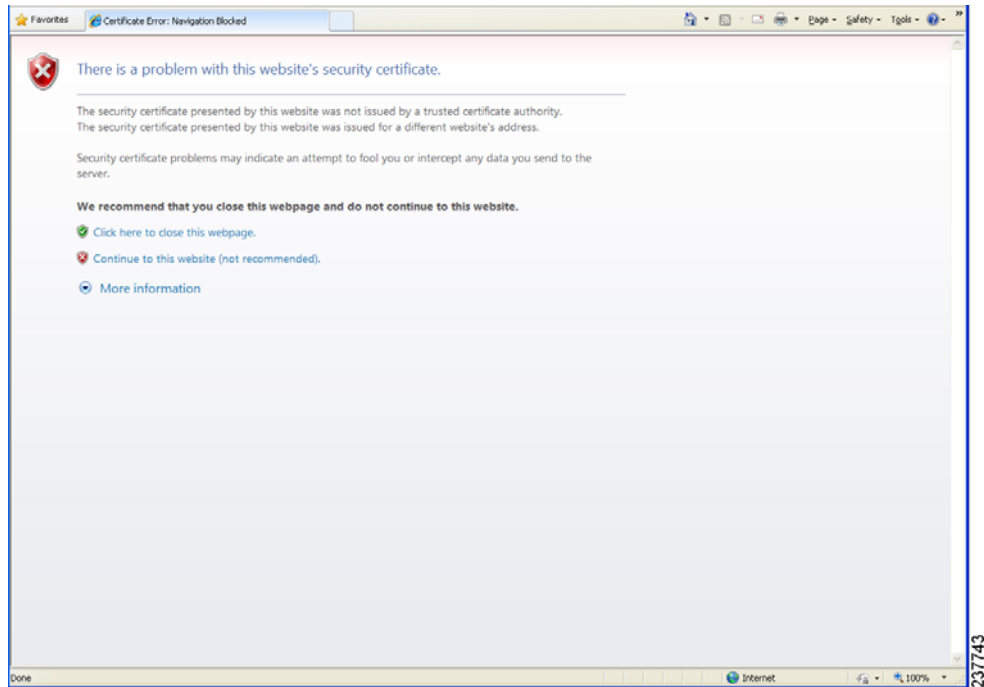
PROCEDURE

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

A Website Security Certification window opens. See [Figure 2-13](#).

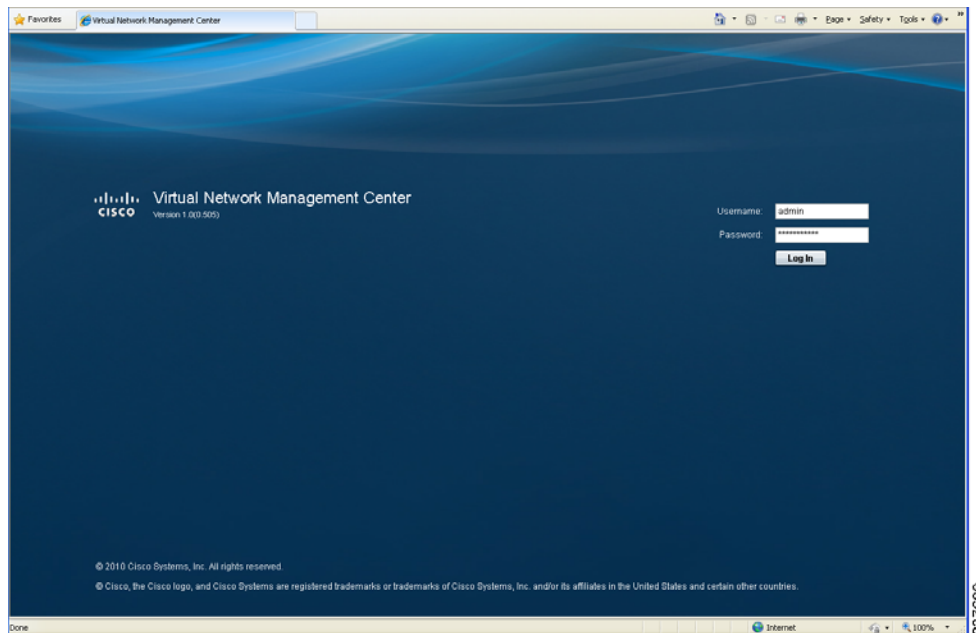
Send document comments to vsg-docfeedback@cisco.com

Figure 2-13 Website Security Certification Window



- Step 2** On the certificate warning window, click **Continue to this website**.
The Cisco VNMC Access window opens. See [Figure 2-14](#).

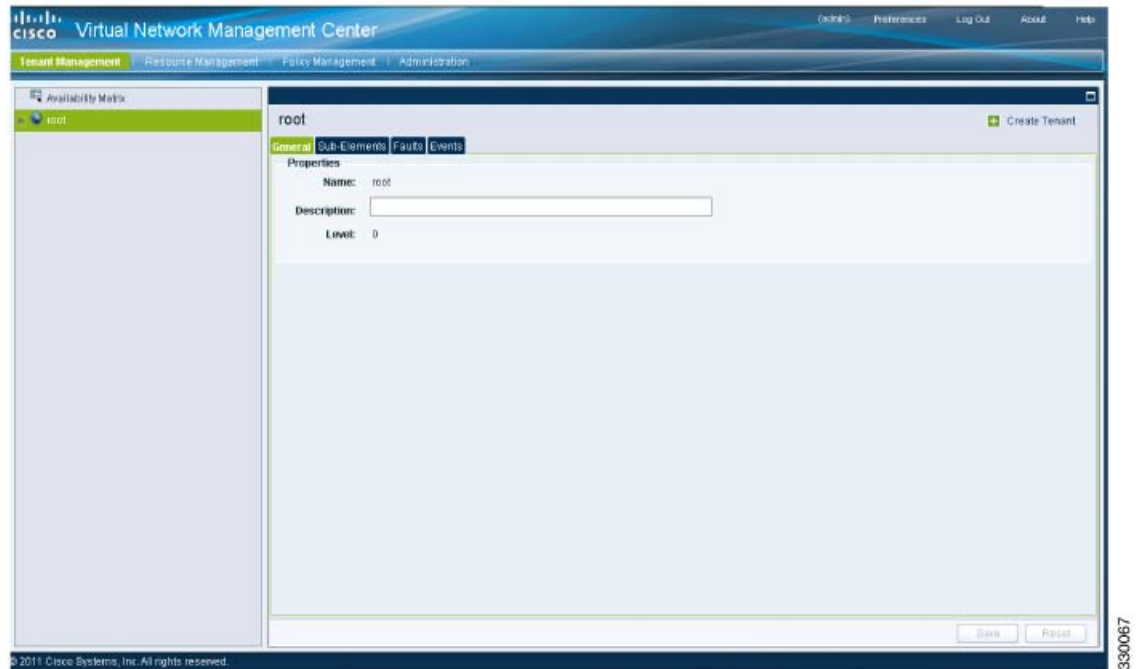
Figure 2-14 VNMC Access Window



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

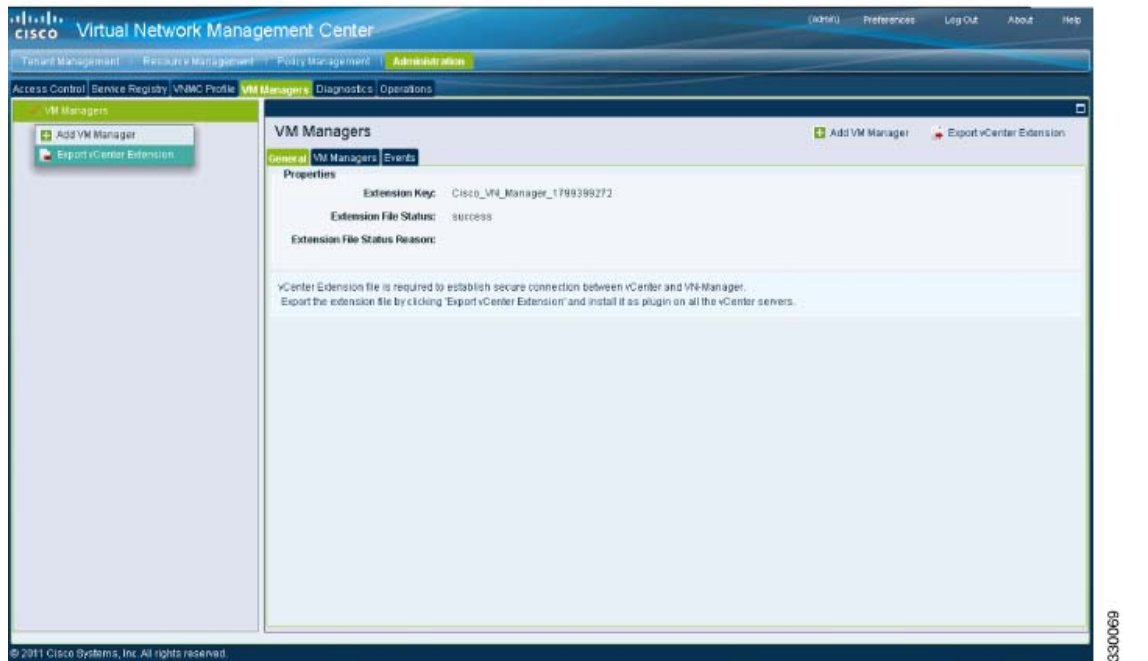
Send document comments to vsg-docfeedback@cisco.com

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



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

Figure 2-16 Cisco VNMCC Administration VM Managers Window



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

Send document comments to vsg-docfeedback@cisco.com

Step 6 The vCenter Desktop displays as shown in [Figure 2-17](#).

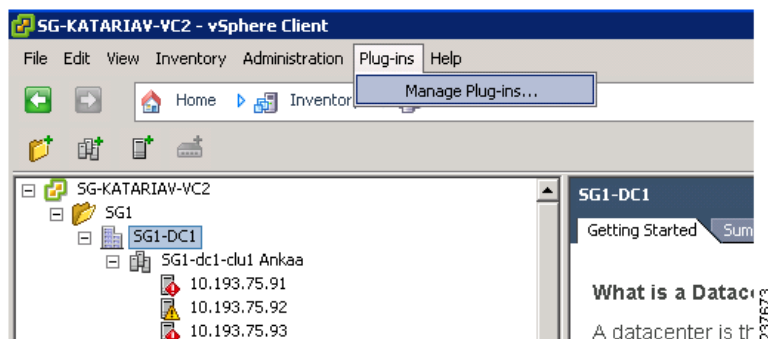
Registering the vCenter Extension Plugin in the vCenter

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

PROCEDURE

Step 1 From vSphere client, log in to vCenter. See [Figure 2-17](#).

Figure 2-17 vSphere Client Directory Window

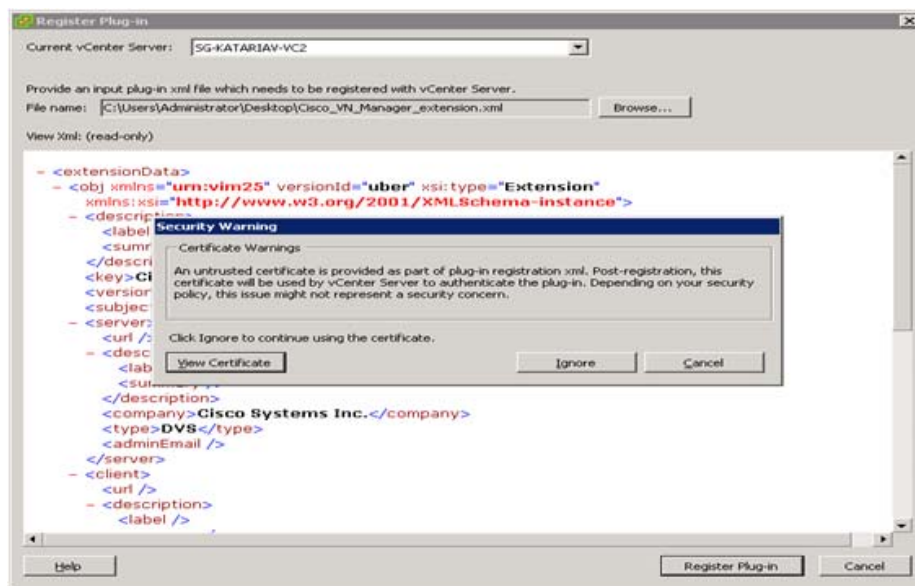


Step 2 Choose **Plug-ins > Manage Plug-ins**.

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

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

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



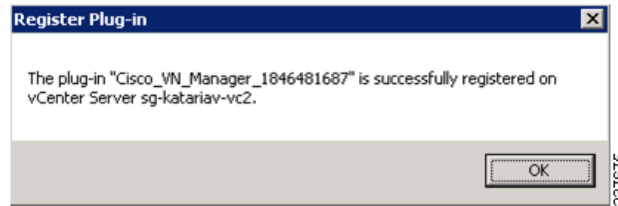
Send document comments to vsg-docfeedback@cisco.com

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

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

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

Figure 2-19 Register Plug-in Progress Success Indicator



Step 6 Click **OK**.

Step 7 Click **Close**.

Configuring the vCenter in VM-Manager in the Cisco VNMC

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

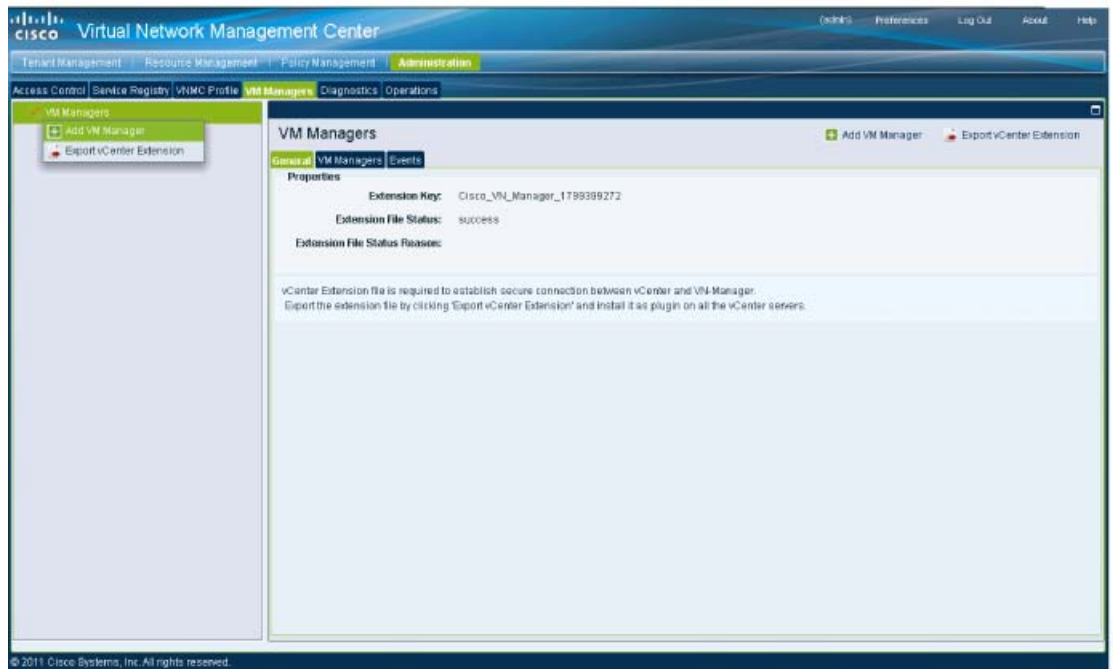
PROCEDURE

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

The Cisco VNMC Administration VM Managers window opens. See [Figure 2-20](#).

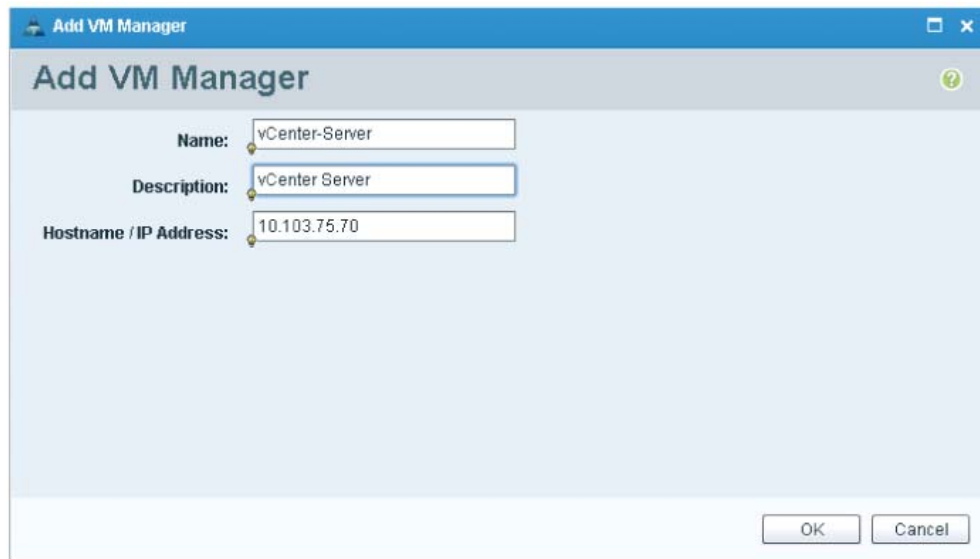
Send document comments to vsg-docfeedback@cisco.com

Figure 2-20 Cisco VNMC Administration VM Managers Window



- Step 2** Choose VM Managers > Add VM Manager.
The Add VM Manager dialog box opens. See [Figure 2-21](#).

Figure 2-21 Add VM Manager Dialog Box



- Step 3** In the Add VM Manager dialog box, do the following:
- In the Name field, enter the vCenter name (no spaces allowed).
 - In the Description field, enter a brief description of the vCenter.
 - In the Hostname/IP Address field, enter the vCenter IP address.

Send document comments to vsg-docfeedback@cisco.com

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 (for example, `vnmc-vsmpa.1.0.1j.bin`)



Note

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

- The IP address of the Cisco VNMC
- The shared secret password you defined during Cisco VNMC installation
- Make sure that IP connectivity between the VSM and the Cisco VNMC is okay.



Note

If you 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)# vnmc-policy-agent
vsm(config-vnmc-policy-agent)# registration-ip 10.193.75.95
vsm(config-vnmc-policy-agent)# shared-secret Example_Secret123
vsm(config-vnmc-policy-agent)# policy-agent-image vnmc-vsmpa.1.0.1j.bin
vsm(config-vnmc-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 vnmc-pa status** command.

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

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

Send document comments to vsg-docfeedback@cisco.com

The VSM is now registered with the Cisco VNMC.

EXAMPLES

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

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

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

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

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

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

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

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



Note

None of these VLANs need to be system VLANs.

PROCEDURE

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

```
vsm# configure
```

- Step 2** Enter the following configuration commands.

```
vsm(config)# vlan 100
vsm(config-vlan)# no shutdown
vsm(config-vlan)# exit
vsm(config)# vlan 200
vsm(config-vlan)# no shutdown
vsm(config-vlan)# exit
vsm(config)# exit
vsm# configure
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

- Step 3** To exit, press **Ctrl-Z**.

Send document comments to vsg-docfeedback@cisco.com

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

```
vsm# configure
```

- Step 5** Enter the following configuration commands.

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

- Step 6** To end the session, press **Ctrl-Z**.

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

```
vsm# configure
```

- Step 8** Enter the following configuration commands.

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

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

```
vsm# configure
```

- Step 10** Enter the following configuration commands:

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

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

Task 5—Installing the Cisco VSG from an OVA Template

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

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

Send document comments to vsg-docfeedback@cisco.com

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

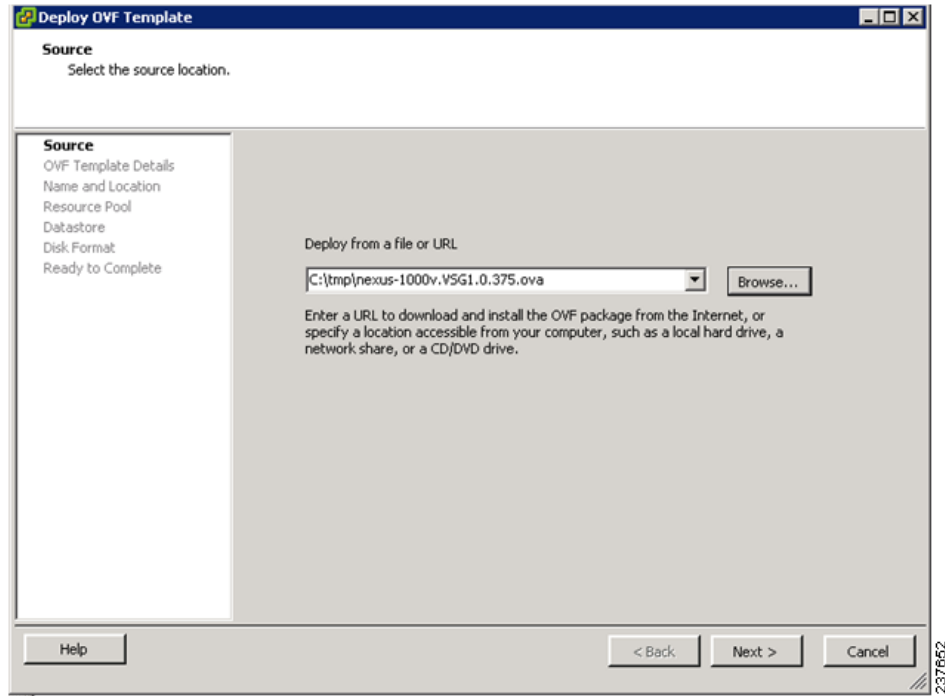
- HA ID
- IP/subnet mask/gateway information for the Cisco VSG
- Admin password
- 2-GB RAM and 3-GB hard disk space
- Cisco VNMC IP
- Shared secret
- IP connectivity between Cisco VSG and Cisco VNMC is okay
- Cisco VSG VNM-PA image name (vnmc-vsgpa.1.0.1j.bin)

PROCEDURE

-
- Step 1** Choose your host on which to deploy the Cisco VSG VM.
- Step 2** From the File menu, choose **Deploy OVF Template**.
The Source window opens. See [Figure 2-22](#).

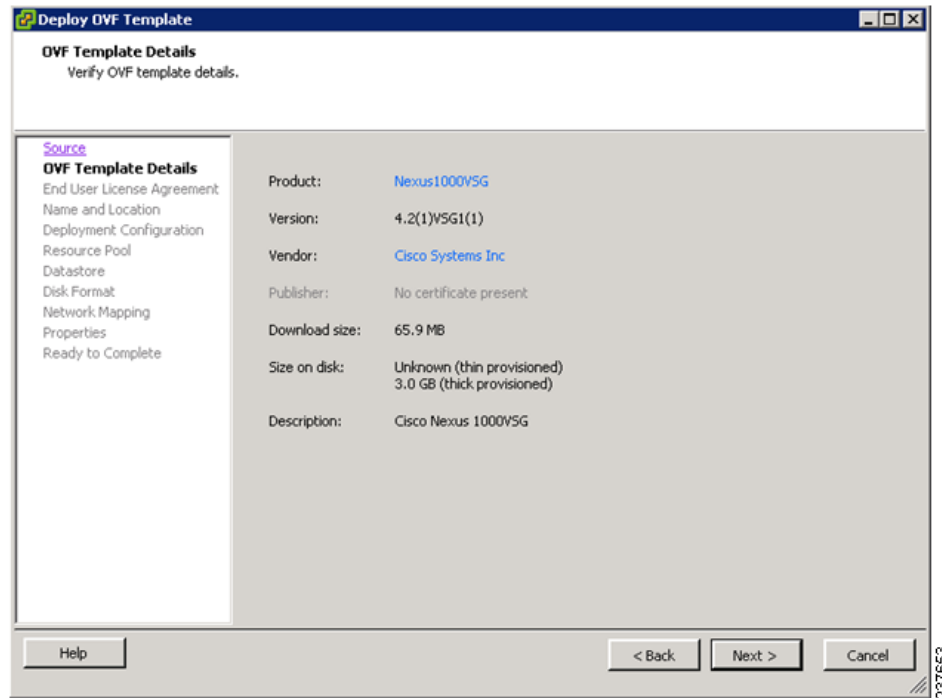
Send document comments to vsg-docfeedback@cisco.com

Figure 2-22 Deploy OVF Template—Source Window



- Step 3** In the Deploy from a file or URL field, enter the path to the Cisco VSG OVA file and click **Next**. The OVF Template Details window opens. See [Figure 2-23](#).

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

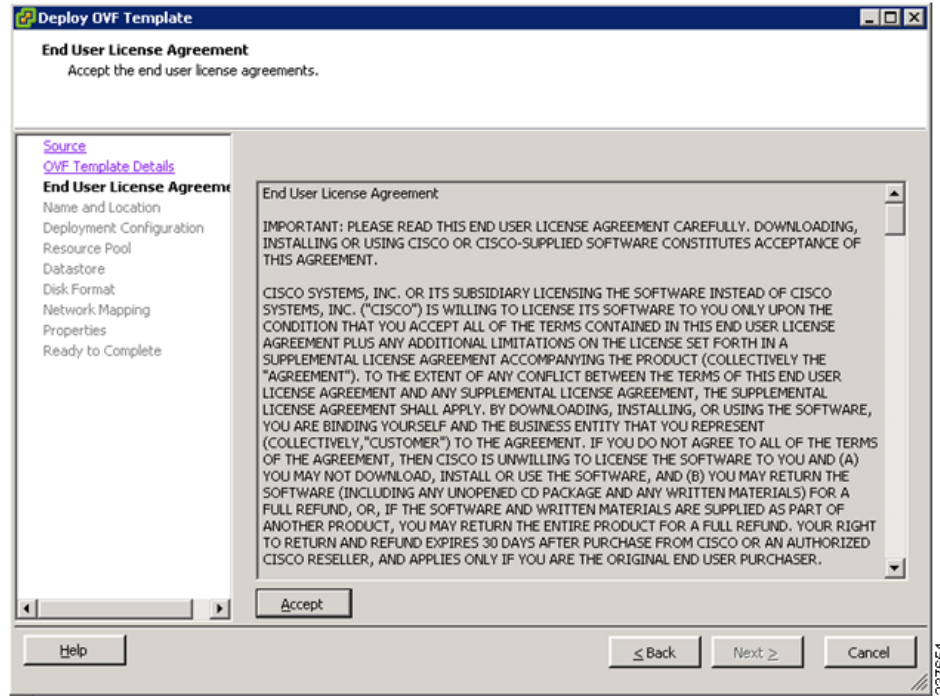


Send document comments to vsg-docfeedback@cisco.com

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



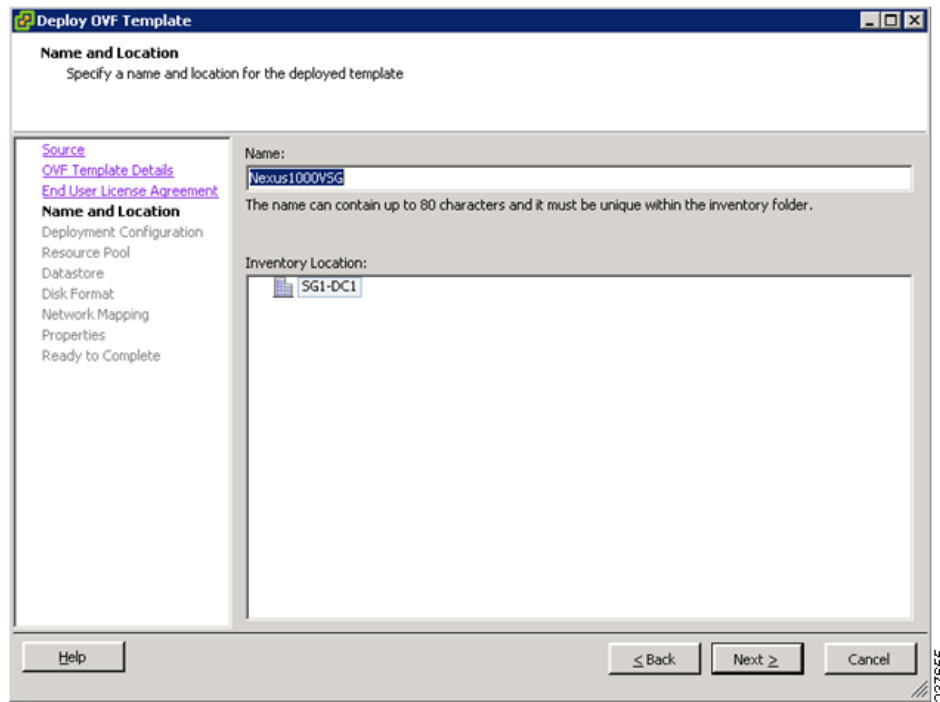
Step 5 Click **Accept** to accept the End User License Agreement.

Step 6 Click **Next**.

The Name and Location window opens. See [Figure 2-25](#).

Send document comments to vsg-docfeedback@cisco.com

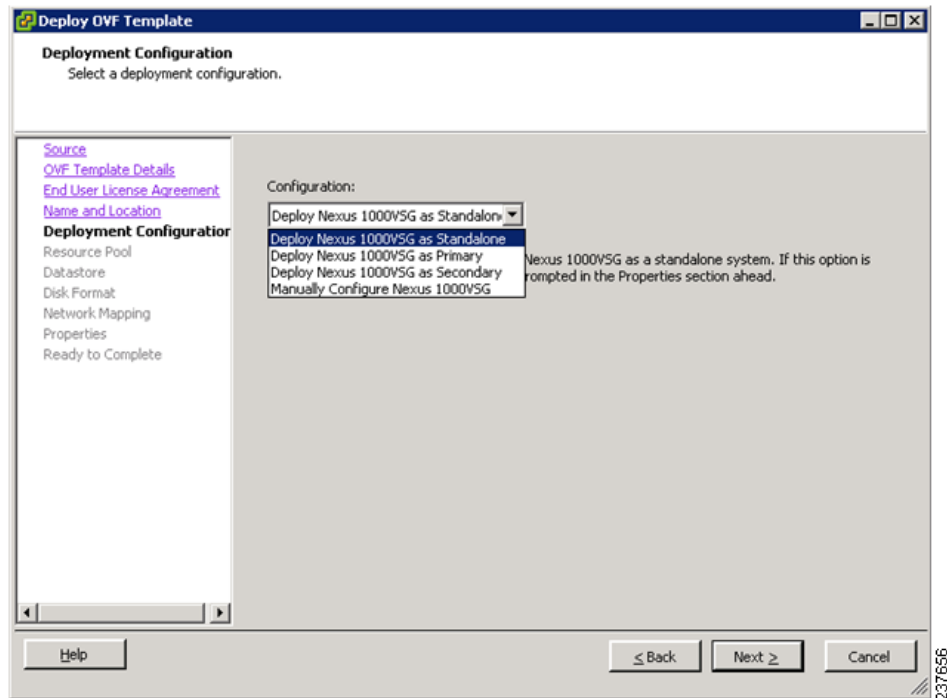
Figure 2-25 Deploy OVF Template—Name and Location Window



- Step 7** In the Name field, enter the name that you want to use for the Cisco VSG.
- Step 8** In the Inventory Location field, choose the location that you want to use for hosting the Cisco VSG.
- Step 9** Click **Next**.
- The Deployment Configuration window opens. See [Figure 2-26](#).

Send document comments to vsg-docfeedback@cisco.com

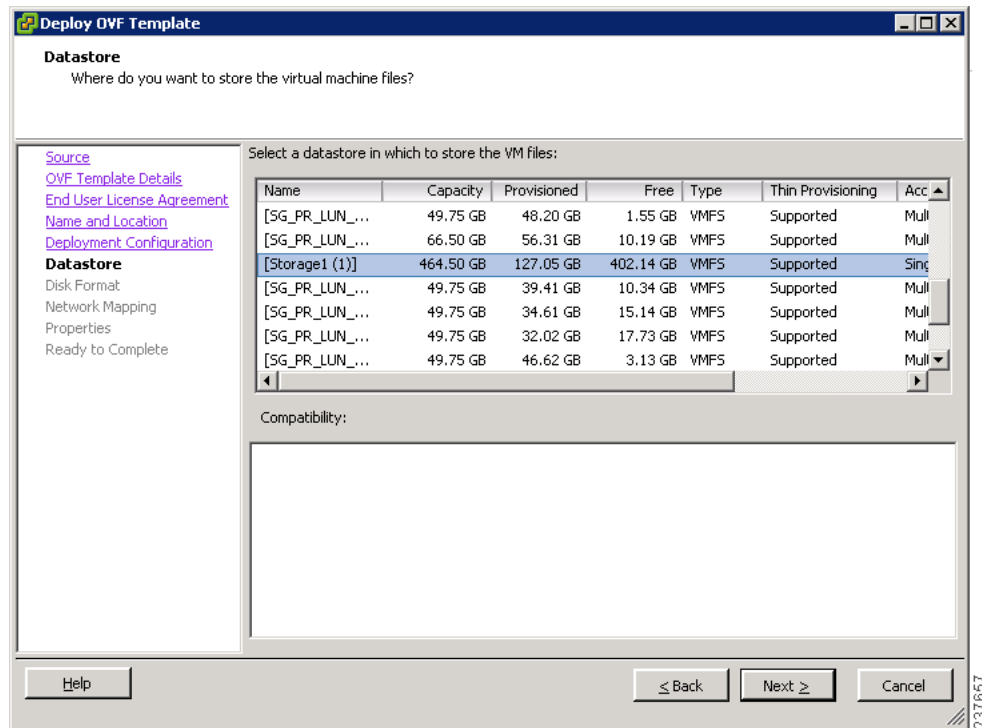
Figure 2-26 Deploy OVF Template—Deployment Configuration Window



- 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](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-27 Deploy OVF Template—Datastore Window



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



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

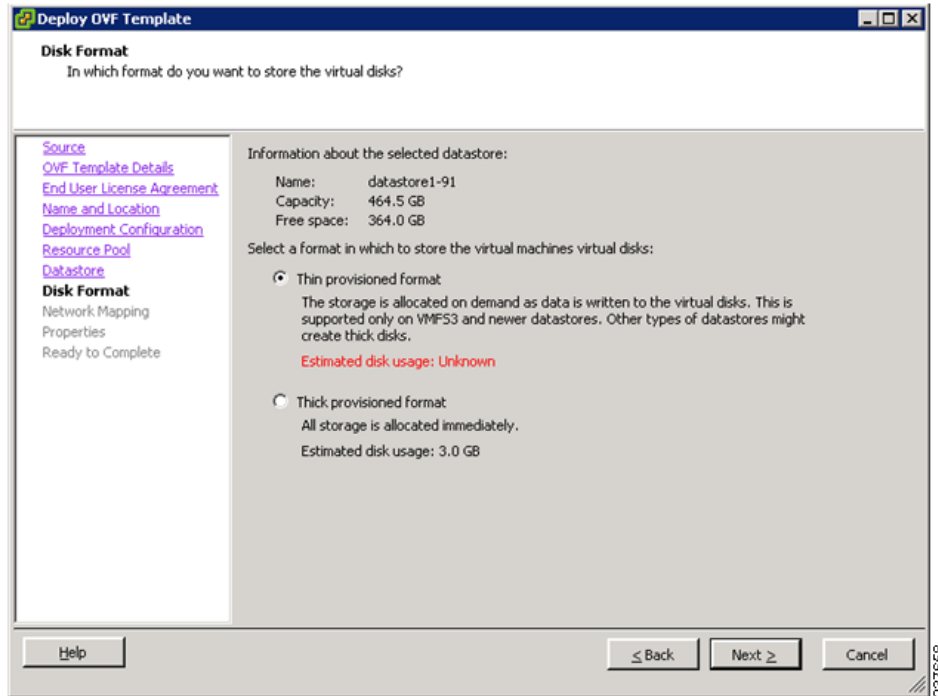


Note If only one storage location is available for an ESX host, this window does not display and you are assigned to the storage location that is available.

The Disk Format window opens. See [Figure 2-28](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-28 Deploy OVF Template—Disk Format Window



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



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

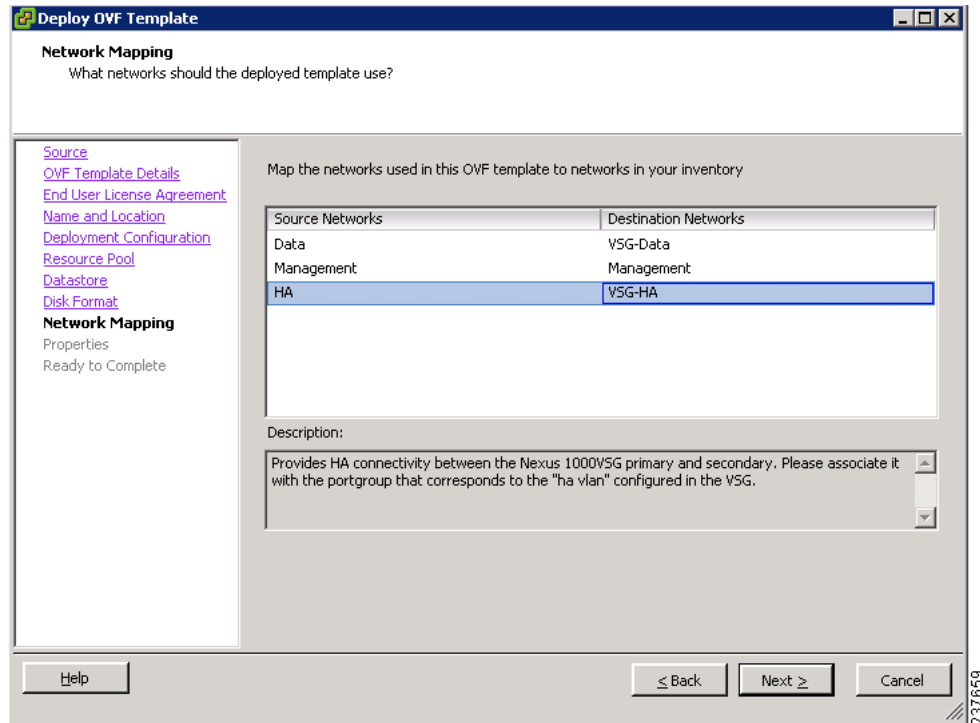


Note Ignore the red text in the window.

The Network Mapping window opens. See [Figure 2-29](#).

Send document comments to vsg-docfeedback@cisco.com

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 2-22](#), the management port profile is used for management connectivity and is the same as in the VSM and Cisco VNMC.

The Properties window opens. See [Figure 2-30](#).

Send document comments to vsg-docfeedback@cisco.com

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 uppercase letter, one lowercase letter, and one number.
- c. In the Management IP Address section, do the following:
 - In the ManagementIPv4 field, enter the IP address for the Cisco VSG.
 - In the ManagementIPv4 Subnet field, enter the subnet mask.
- d. In the Gateway field, enter the gateway name.
- e. In the VnmIpV4 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.

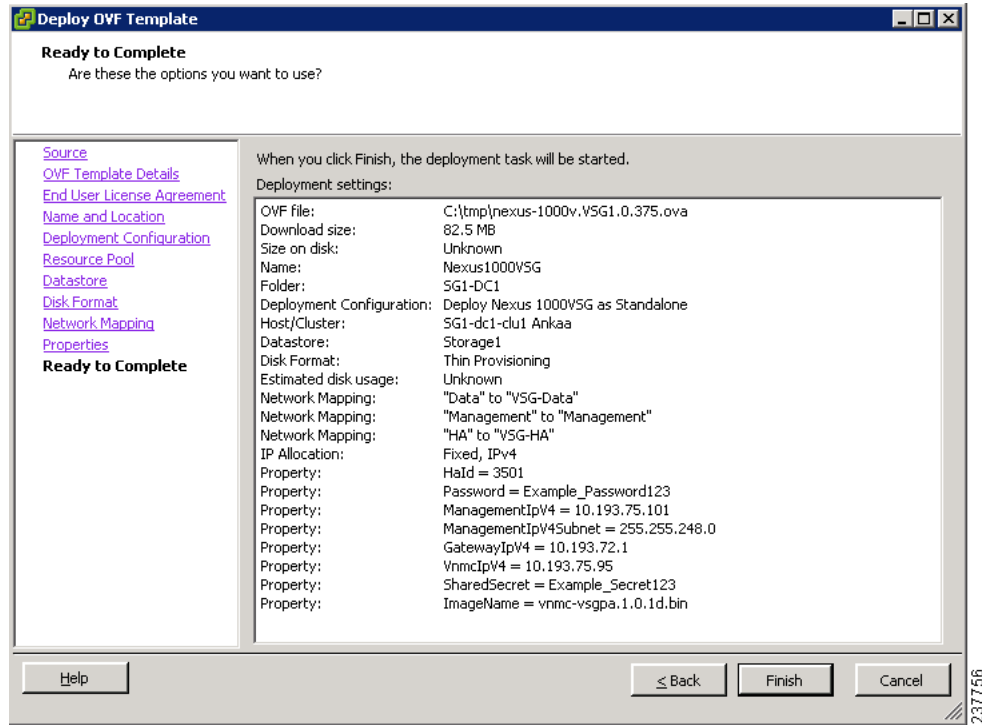


Note Make sure that red text messages do not appear before you click **Next**. If you do not want to enter valid information in the red-indicated fields, use null values to fill those fields. If those fields are left empty or filled with invalid null values, the application does not power on.

The Ready to Complete window opens. See [Figure 2-31](#).

Send document comments to vsg-docfeedback@cisco.com

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



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



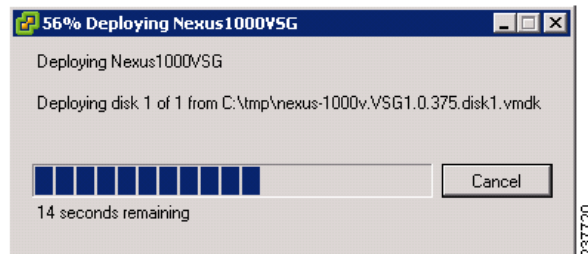
Note

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

The Deploying Nexus1000VSG Progress Indicator opens. See [Figure 2-32](#).

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

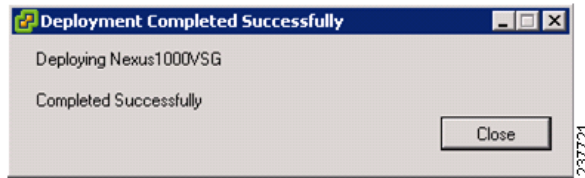
Figure 2-32 Deploying Nexus1000VSG—Deploying Disk Files Progress Indicator



The progress indicator in [Figure 2-33](#) shows that the deployment has completed successfully.

Send document comments to vsg-docfeedback@cisco.com

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).

PROCEDURE

Step 1 Log in to the Cisco VSG.

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

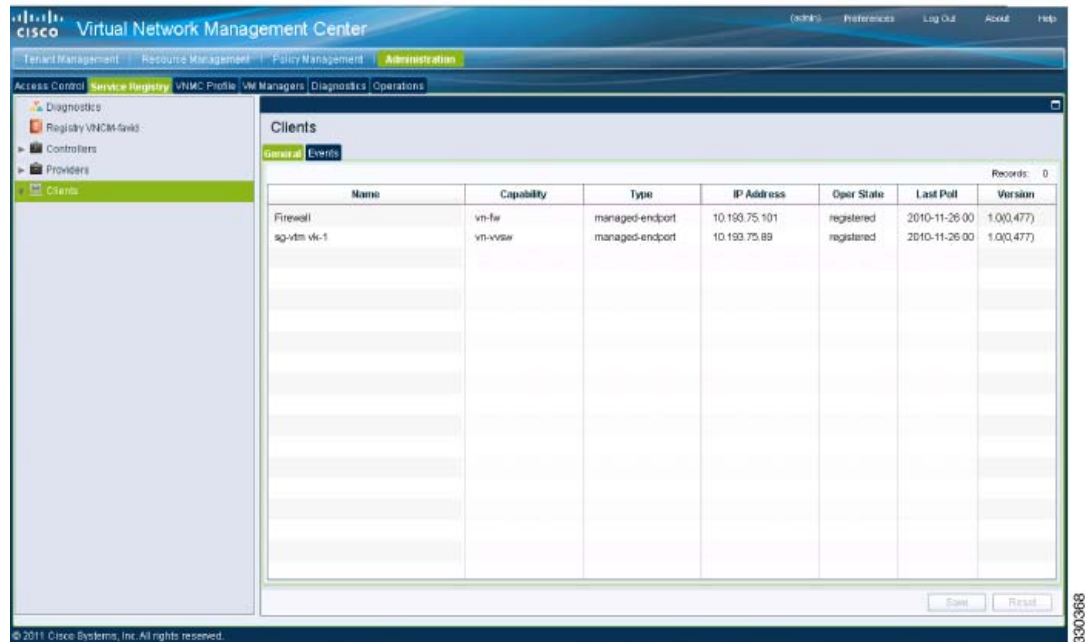
```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.0(1j)-vsg
vsg#
```

Step 3 Log in to the Cisco VNMC.

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

Send document comments to vsg-docfeedback@cisco.com

Figure 2-34 VNMC Administration Service Registry Window



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

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

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

BEFORE YOU BEGIN

Before doing this procedure, know or do the following:

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

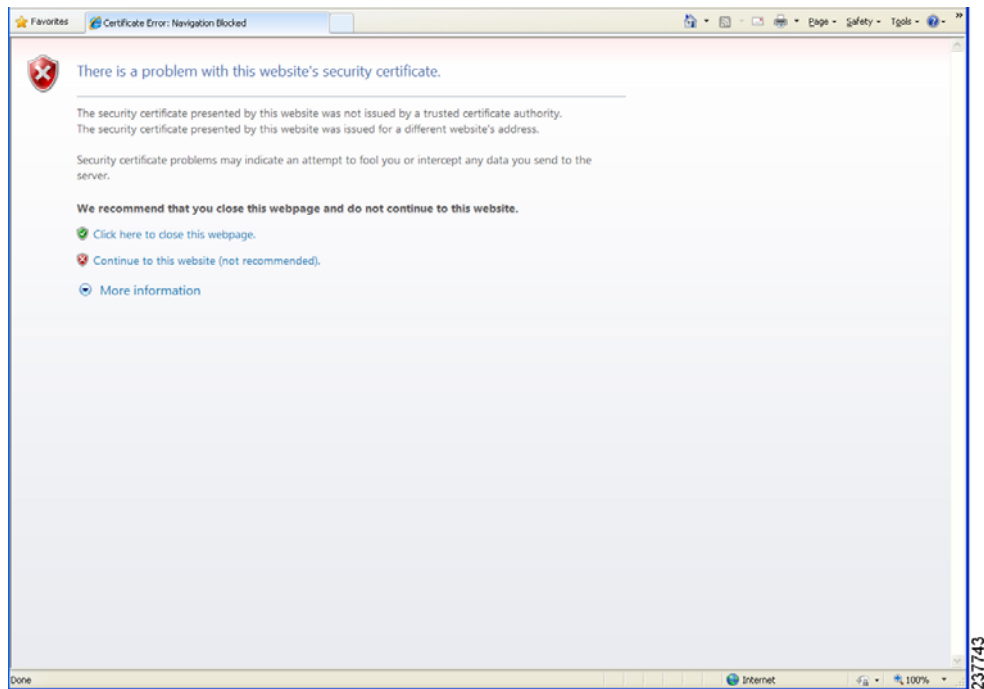
PROCEDURE

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

A Website Security Certification window opens. See [Figure 2-35](#).

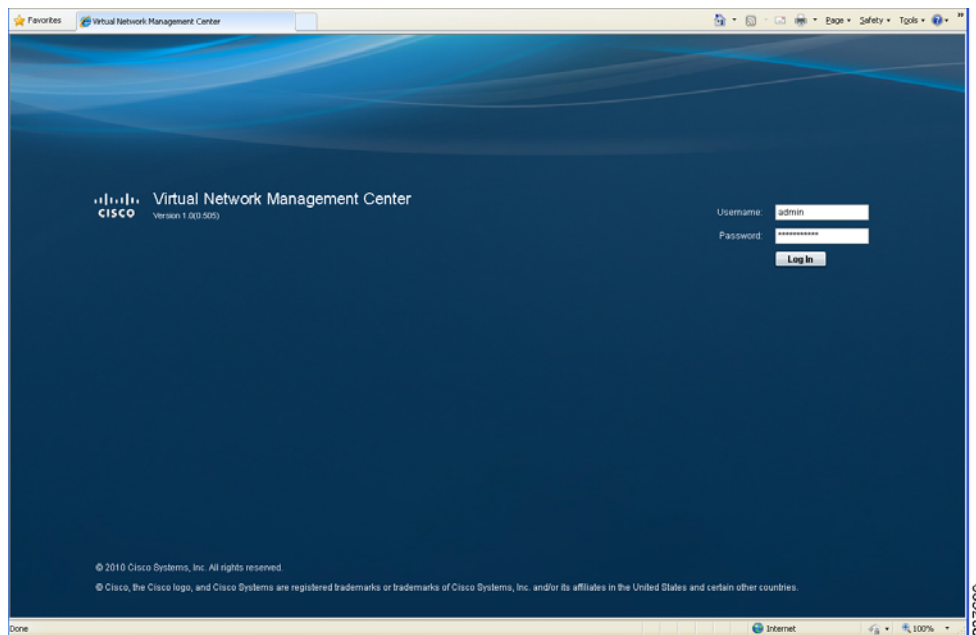
Send document comments to vsg-docfeedback@cisco.com

Figure 2-35 Website Security Certification Window



- 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

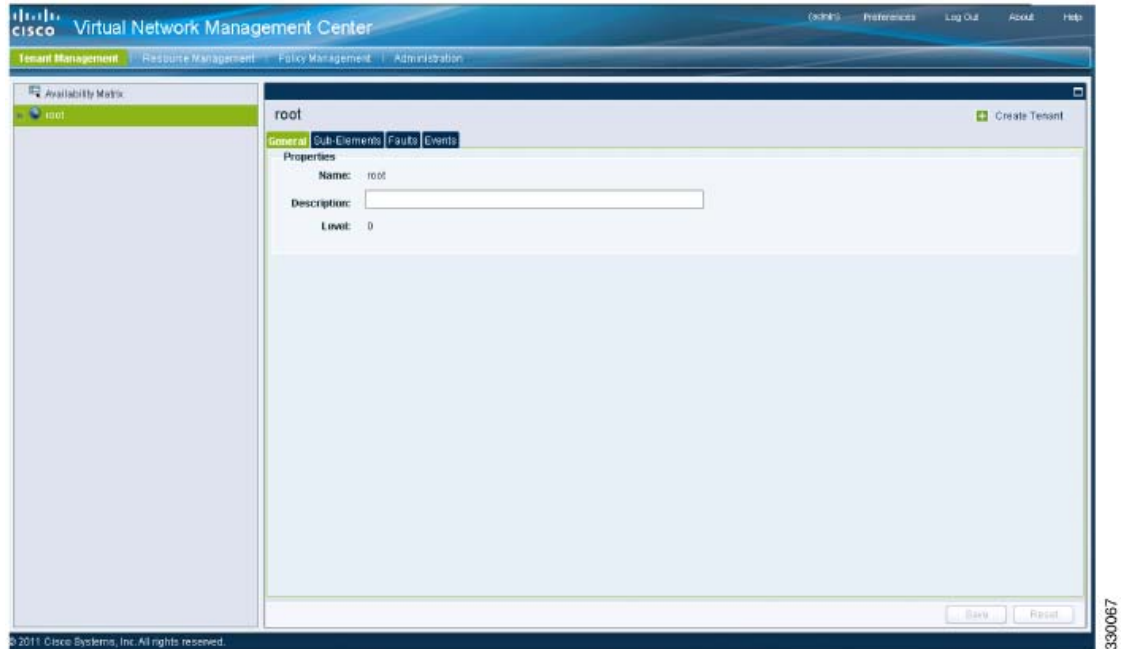


- Step 3** Log in to the Cisco VNMC with the username “admin” and your password.

Send document comments to vsg-docfeedback@cisco.com

Step 4 The Cisco VNMC Main window opens. See [Figure 2-37](#).

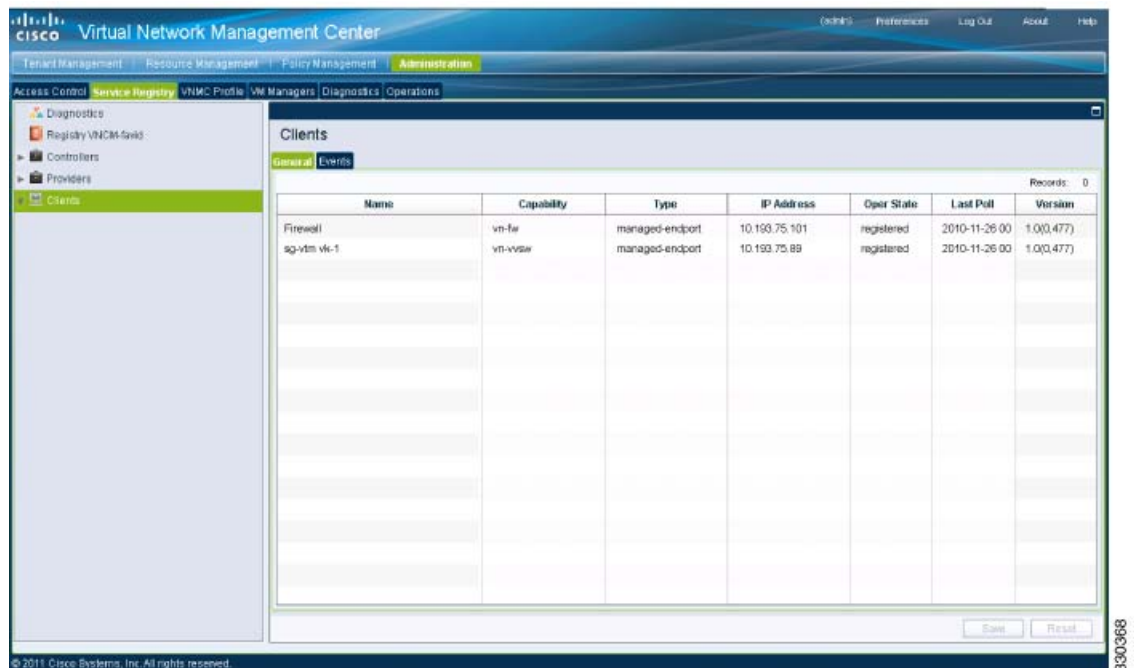
Figure 2-37 Cisco Virtual Network Management Center—Opening Page



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

The Clients pane of the Cisco VNMC opens. See [Figure 2-38](#).

Figure 2-38 VNMC Administration Service Registry Window Clients Pane



Send document comments to vsg-docfeedback@cisco.com

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

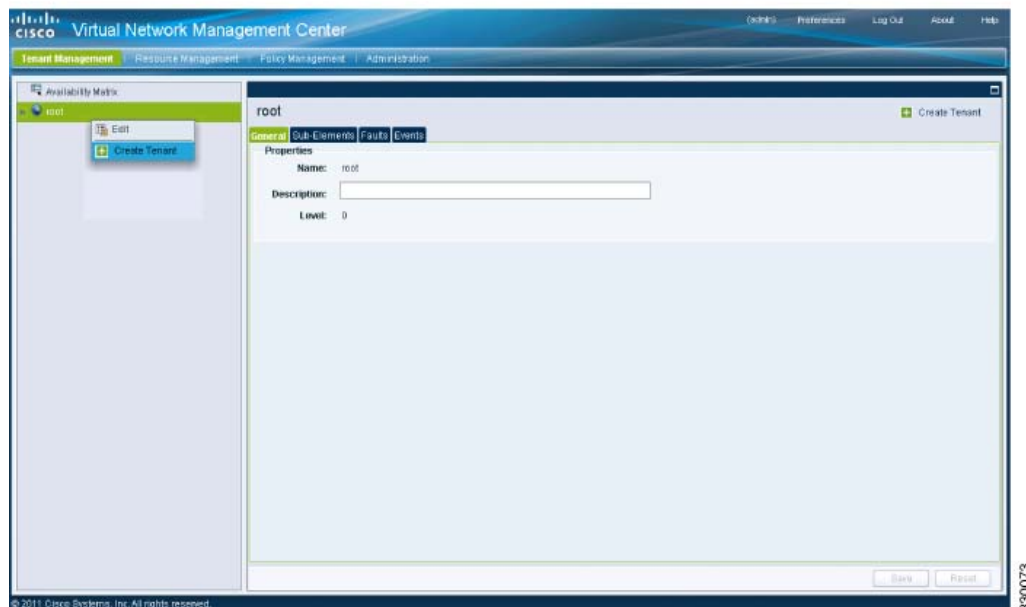
Configuring a Tenant in the Cisco VNMC

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

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

The root pane opens. See [Figure 2-39](#).

Figure 2-39 VNMC Window Tenant Management Tab root Pane

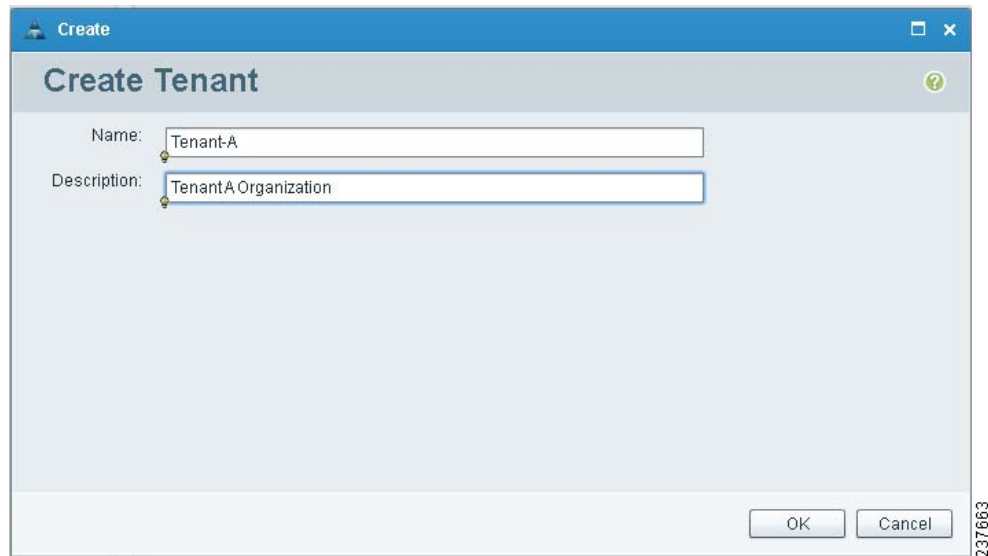


Step 2 In the left pane directory tree right-click on Root, and from the drop-down list, choose Create Tenant.

The Create Tenant dialog box opens. See [Figure 2-40](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-40 Create Tenant Dialog Box



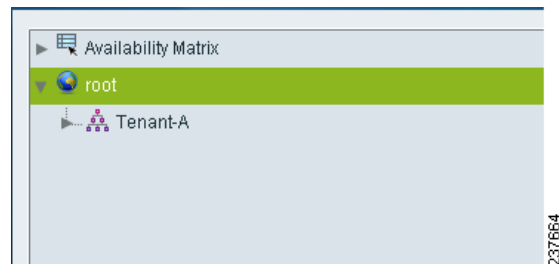
Step 3 Do the following:

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

Step 4 Click **OK**.

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

Figure 2-41 Cisco VNMC VSG Configuration Directory Tree Pane



Configuring a Security Profile in the Cisco VNMC

You can configure a security profile on the Cisco VNMC.

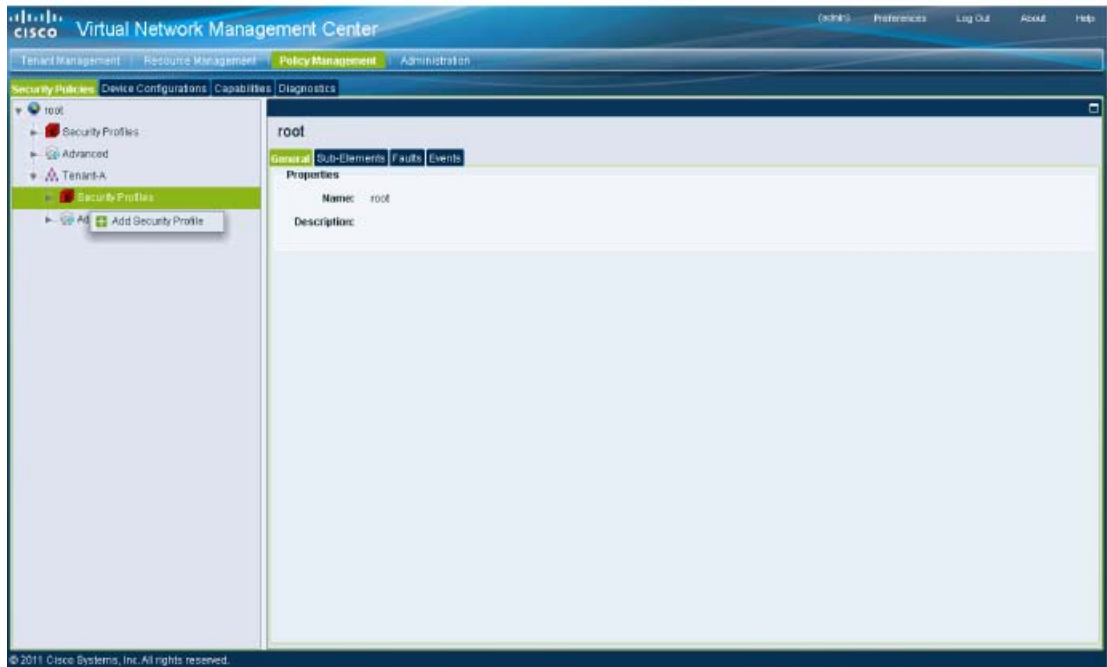
PROCEDURE

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

The Policy Management Security Policies window opens. See [Figure 2-42](#).

Send document comments to vsg-docfeedback@cisco.com

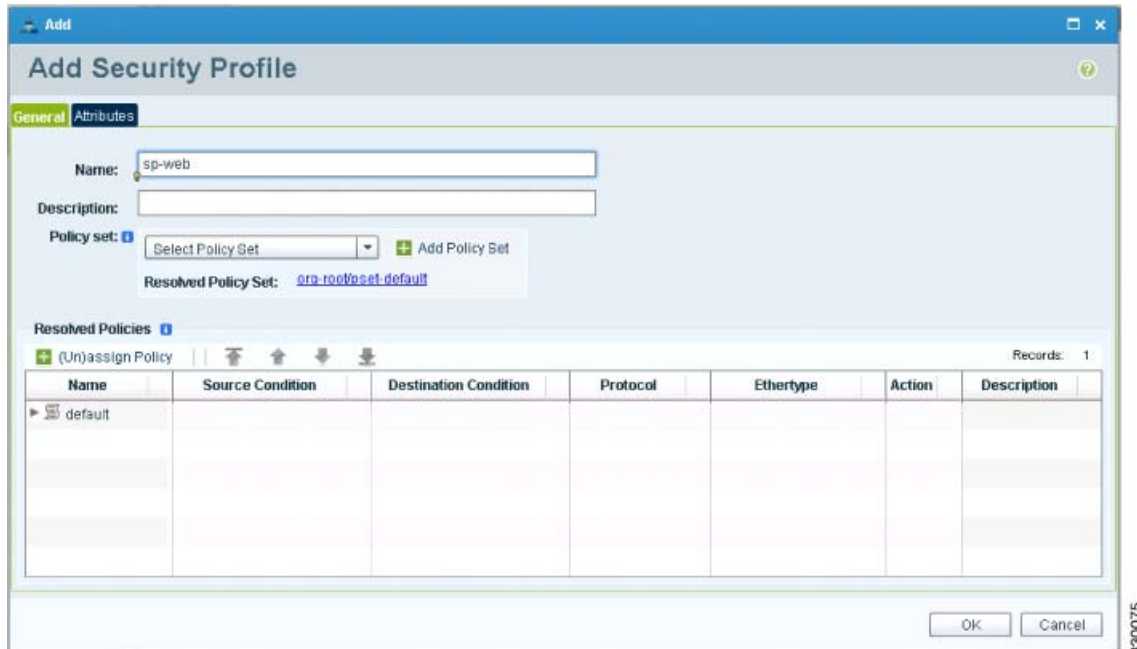
Figure 2-42 VNM Policy Management Security Policies Window



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

The Add Security Profile dialog box opens. See [Figure 2-43](#).

Figure 2-43 Add Security Profile Dialog Box



Step 3 Do the following:

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

Send document comments to vsg-docfeedback@cisco.com

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

Step 4 Click **OK**.

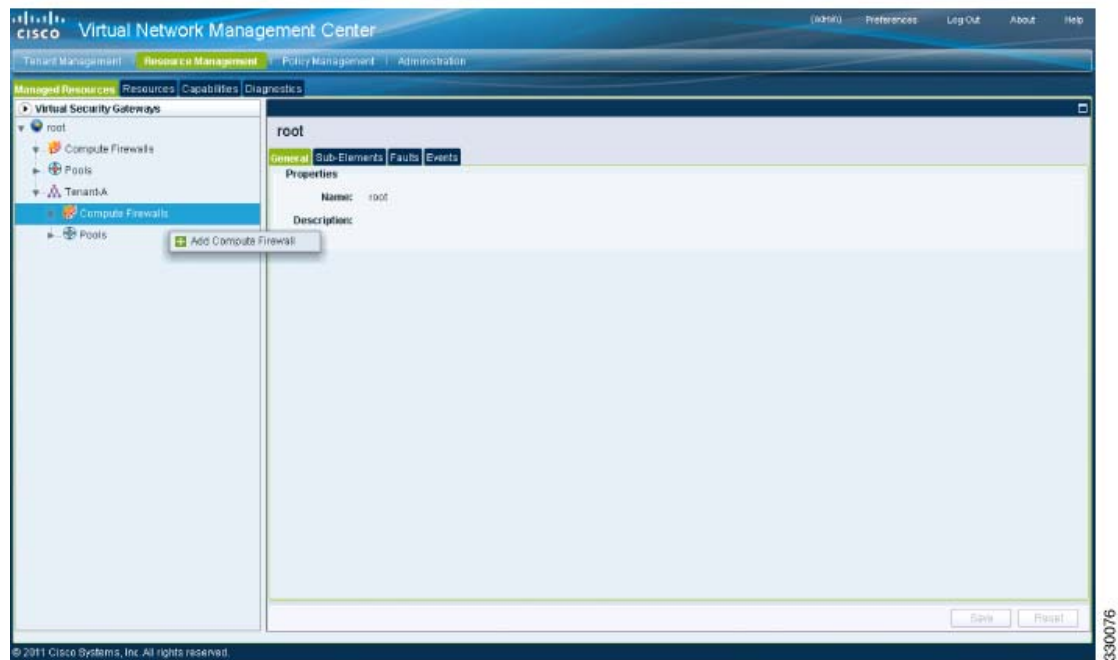
On the Cisco VNMC, Configuring a Compute Firewall

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.

PROCEDURE

Step 1 From the Cisco VNMC, choose **Resource Management > Managed Resources**.
The VNMC Resource Management, Managed Resources, Firewall Profiles window opens. See [Figure 2-44](#).

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



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

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

The Add Compute Firewall dialog box opens. See [Figure 2-45](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-45 Add Compute Firewall Dialog Box

The screenshot shows a dialog box titled "Add Compute Firewall" with a "Create" button in the top left corner. The dialog is divided into two main sections: "General" and "Firewall Settings".

General Section:

- Name:** CFW-VSG-A
- Description:** (empty field)
- Config State:** not-applied

Firewall Settings Section:

- Device Profile:** default (with a "Select" button)
- Management Hostname:** firewall
- Data IP Address:** 10 . 10 . 10 . 200
- Data IP Subnet:** 255 . 255 . 255 . 0

At the bottom right of the dialog, there are "OK" and "Cancel" buttons. A vertical ID number "330077" is visible on the right edge of the dialog box.

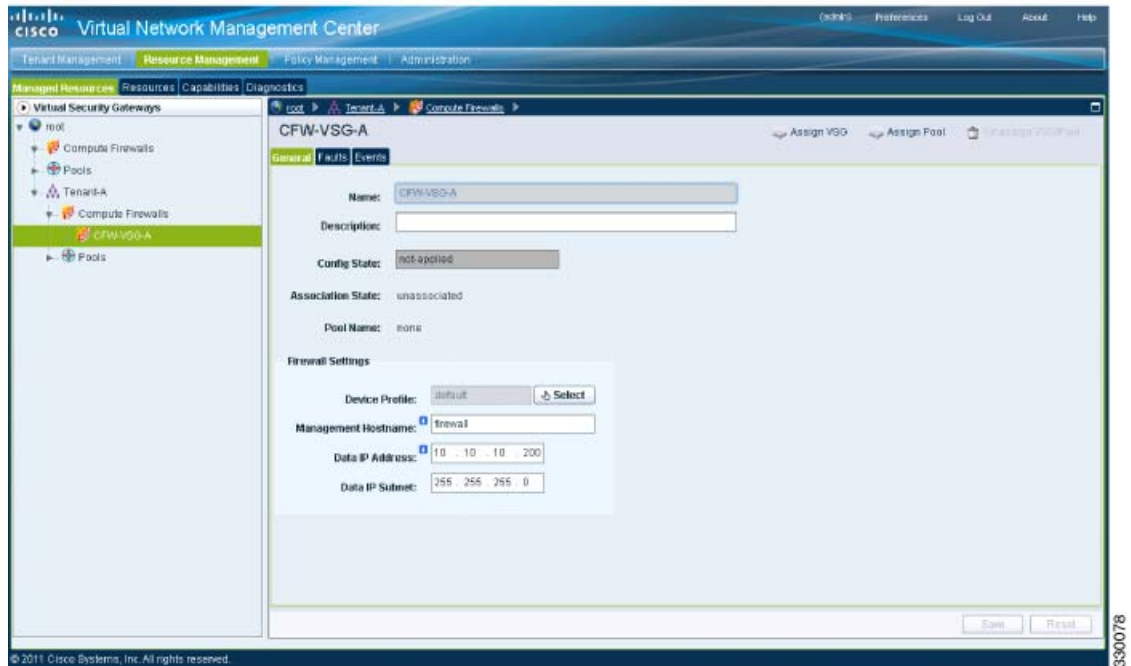
- Step 4** In the Add Compute Firewall dialog box, do the following:
- In the Name field, enter a name for the compute firewall.
 - In the Description field, enter a brief description of the compute firewall.
 - In the Management Hostname field, enter the name for your Cisco VSG.
 - In the Data IP Address field, enter the Data IP address, if it is different from what is the default.

- Step 5** Click **OK**.

The new Compute Firewall pane displays with the information that you provided. See [Figure 2-46](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-46 Compute Firewall Pane



Task 8—On the Cisco VNM, 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 VNM and VSM.

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

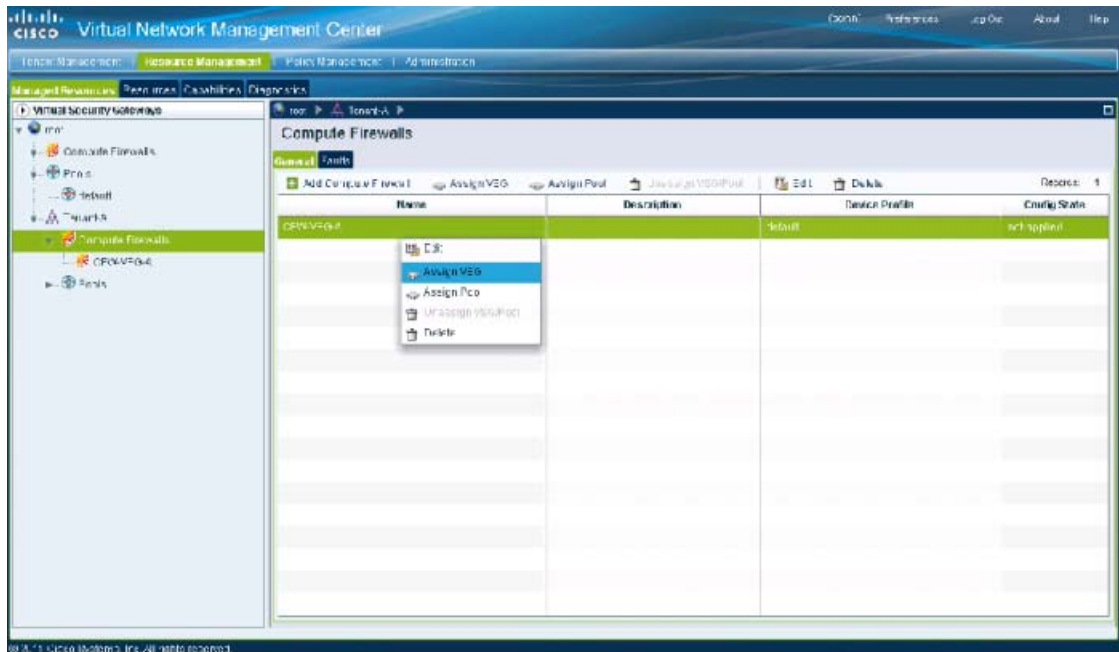
PROCEDURE

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

The VNM Resource Management Managed Resources Compute Firewalls window opens. See [Figure 2-47](#).

Send document comments to vsg-docfeedback@cisco.com

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

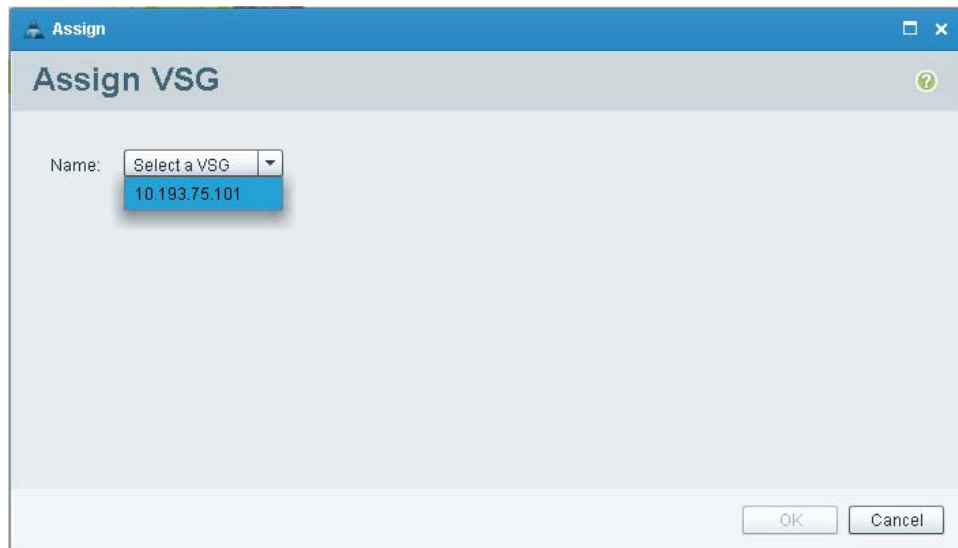


Step 2 Choose **root > Tenant-A > Compute Firewalls**.

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

The Assign VSG dialog box opens. See [Figure 2-48](#).

Figure 2-48 Assign VSG Dialog Box



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

Step 5 Click **OK**.

Send document comments to vsg-docfeedback@cisco.com



Note

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

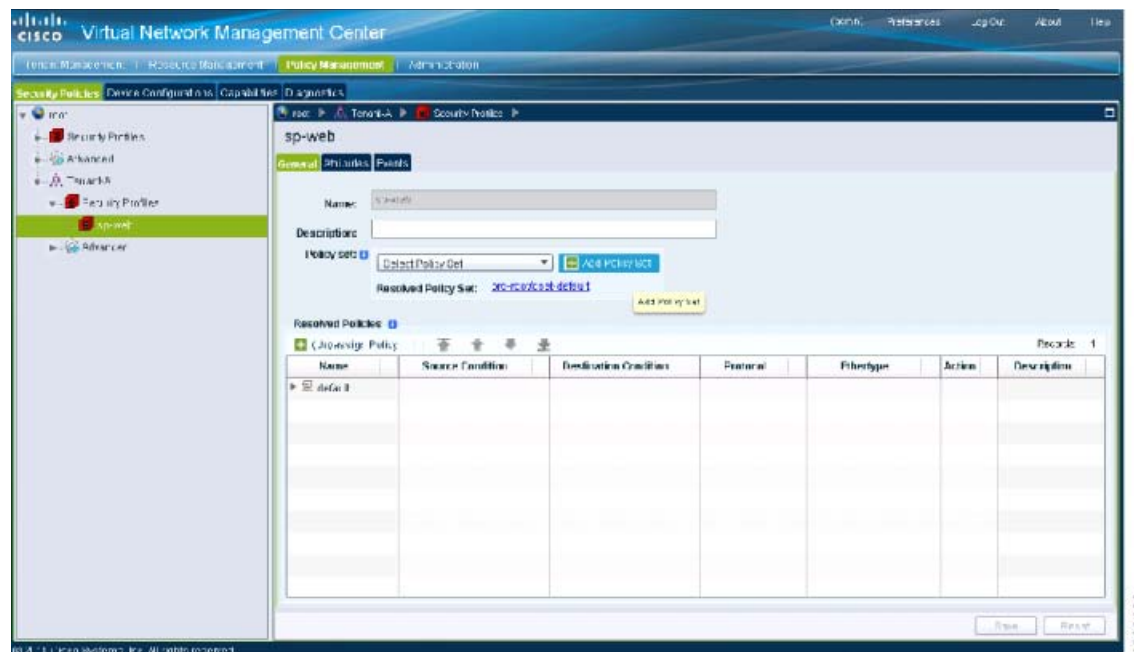
Task 9—On the Cisco VNMC, Configuring a Permit-All Rule

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

PROCEDURE

- Step 1** Log in to the Cisco VNMC and choose **Policy Management > Security Policies**.
The Cisco VNMC Policy Management Security Policies window opens. See [Figure 2-49](#).

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



- Step 2** Choose **root > Tenant-A > Security-Profile > sp-web**.
Step 3 From the button to the right of the sp-web pane Policy sets field, click **Add policy set**.
The Add Policy Set dialog box opens. See [Figure 2-50](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-50 Add Policy Set Dialog Box

The screenshot shows the 'Add Policy Set' dialog box. The title bar is blue with the text 'Add' and window control icons. The main title is 'Add Policy Set' in a grey header. Below the header is a 'General' tab. The 'Name' field is a text box containing 'PS_web'. The 'Description' field is an empty text box. Below these is a 'Policies' section with a blue '+ Add Policy' button and a grey 'Edit' button. Underneath, there are two list boxes: 'Available :' and 'Assigned :'. The 'Available :' list contains the text 'default'. Between the two lists are four arrow buttons: a double right arrow, a single right arrow, a single left arrow, and a double left arrow. At the bottom right of the dialog are 'OK' and 'Cancel' buttons. A vertical ID number '330267' is on the right edge.

Step 4 Click **Add Policy**. The Add Policy dialog box appears. See [Figure 2-51](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-51 Add Policy Dialog Box

The screenshot shows the 'Add Policy' dialog box with the following details:

- Title Bar:** Add
- Header:** Add Policy
- General Tab:**
 - Name:** pol_web
 - Description:** (empty field)
- Rules Section:**
 - Buttons:** + Add Rule, [Refresh], [Up], [Down], [Down]
 - Records:** 0
 - Table:**

Name	Source Condition	Destination Condition	Protocol	Ethertype	Action
	Add Rule				
- Bottom:** OK, Cancel

- Step 5** Do the following:
- In the Name field, enter the security policy name.
 - In the Description field, enter a brief description of the security policy.
 - Above the Name column, click **Add Rule**.
The Add Rule dialog box displays. See [Figure 2-52](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-52 VNM Add Rule Dialog Box

The screenshot shows the 'Add Rule' dialog box with the following configuration:

- Name:** permit-all
- Description:** (empty)
- Action to take:** drop, permit, reset, log
- Protocol:** Any
- Ether Type:** Any
- Source Conditions:** Table with 0 records.
- Destination Conditions:** Table with 0 records.
- Note:** Configured Rule Conditions will have AND semantics.
- Buttons:** OK, Cancel

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

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

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

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

The Add Policy dialog box reappears showing a policy with the new rule. See [Figure 2-53](#).

Send document comments to vsg-docfeedback@cisco.com

Figure 2-53 VNMC Add Policy Dialog Box

Add Policy

General

Name:

Description:

Rules

+ Add Rule | [Icons] Records: 1

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

OK Cancel

330202

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

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

Send document comments to vsg-docfeedback@cisco.com

Figure 2-54 Add Policy Set Dialog Box

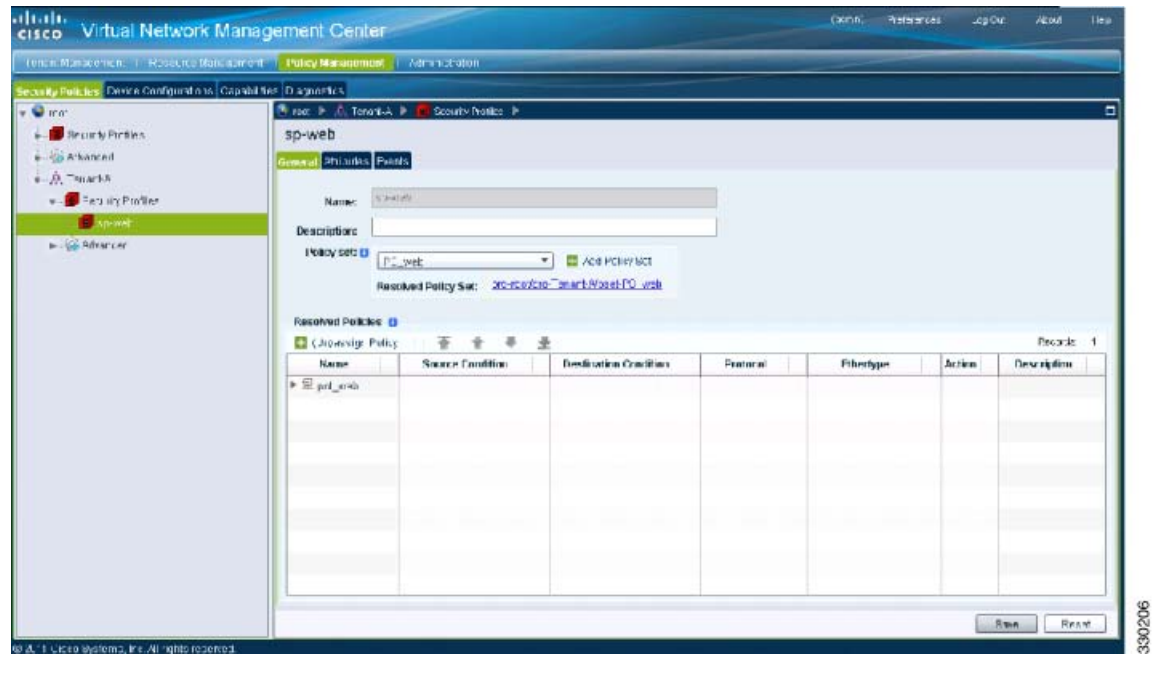
The screenshot shows the 'Add Policy Set' dialog box. The title bar is blue with the text 'Add' and window control icons. The main title is 'Add Policy Set' with a help icon. The 'General' tab is selected. The 'Name' field contains 'PS_web'. The 'Description' field is empty. Below the fields are 'Policies' with a count of 0, an '+ Add Policy' button, and an 'Edit' button. The central area is divided into two columns: 'Available' and 'Assigned'. The 'Available' column contains 'default'. The 'Assigned' column contains 'pol_web'. Between the columns are navigation arrows: a double right arrow (>>), a single right arrow (>), a single left arrow (<), and a double left arrow (<<). At the bottom right are 'OK' and 'Cancel' buttons. A small vertical number '330268' is on the right edge.

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

Step 13 Click **Save** in the Security Profile window. See [Figure 2-55](#).

Send document comments to vsg-docfeedback@cisco.com

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



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

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

PROCEDURE

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

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

security-profile sp-web@root/Tenant-A
  policy PS_web@root/Tenant-A
  custom-attribute vnsorg "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
```

Send document comments to vsg-docfeedback@cisco.com

Task 11—Enabling Logging

This section includes the following topics:

- [Enabling Logging Level 6 for Policy-Engine Logging, page 2-52](#)
- [Enabling Global Policy-Engine Logging, page 2-55](#)

Enabling Logging Level 6 for Policy-Engine Logging

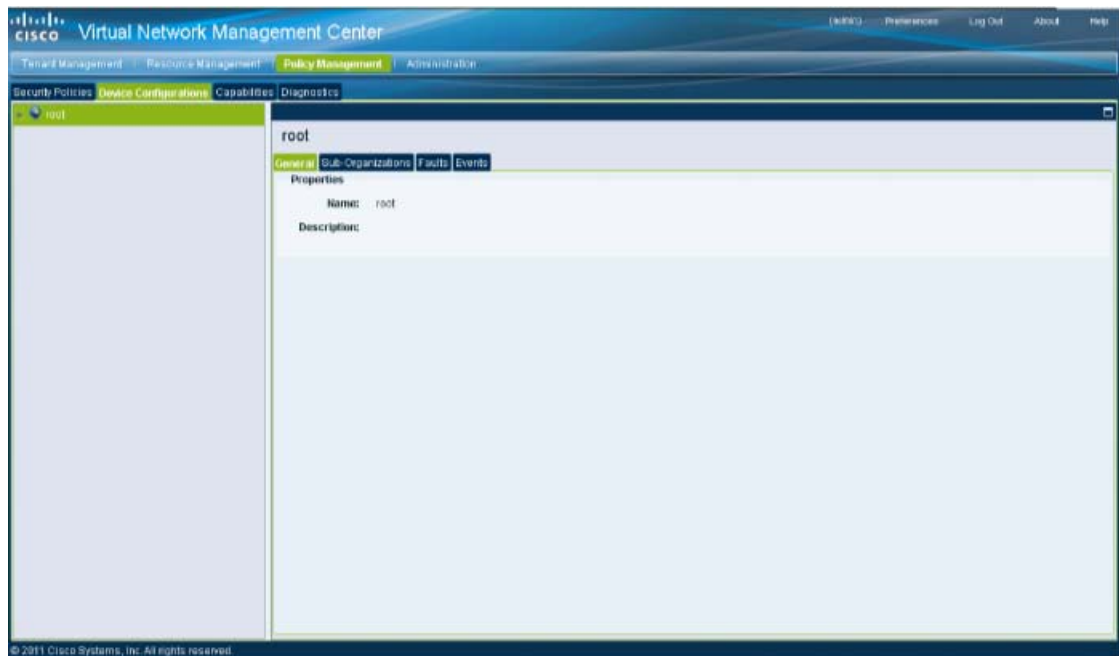
Logging enables you to see what traffic is going through your monitored virtual machine. This logging is helpful for verifying that you have a proper configuration and to help in troubleshooting.

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

PROCEDURE

-
- Step 1** Log in to the Cisco VNMCM.
- Step 2** Choose **Policy Management > Device Configurations**. See [Figure 2-56](#).

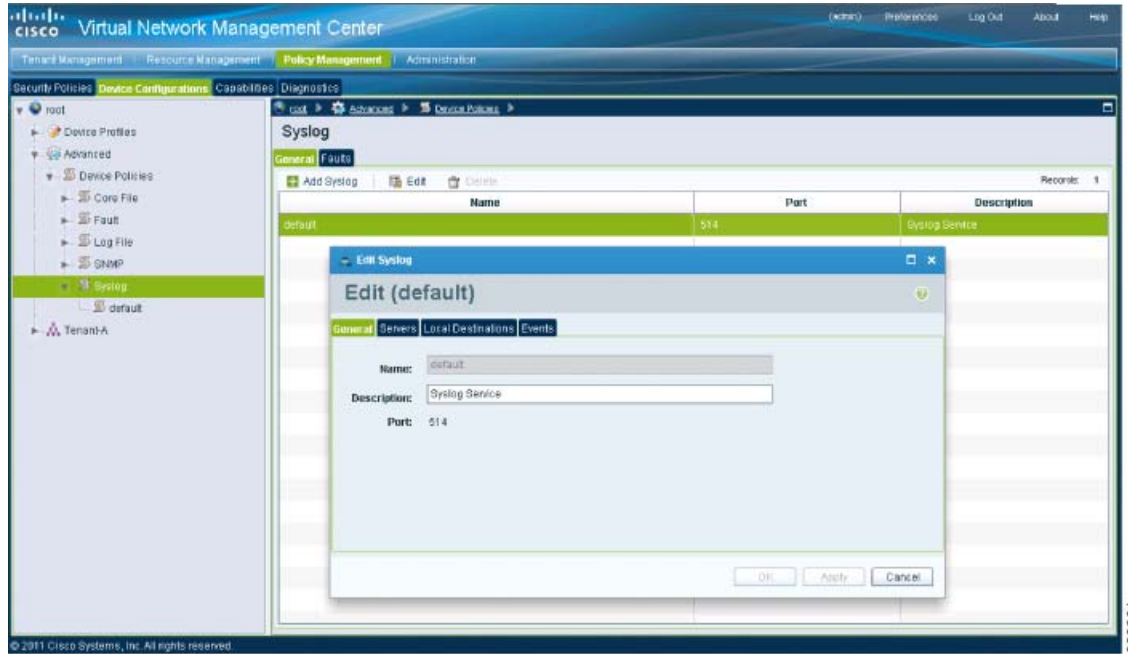
Figure 2-56 Cisco Virtual Network Management Center—Device Configurations Window



- Step 3** From the left pane navigation tree, choose **root > Advanced > Device Policies > Syslog**.
- Step 4** From the Syslog panel on the right, choose **Default** and click **Edit**.

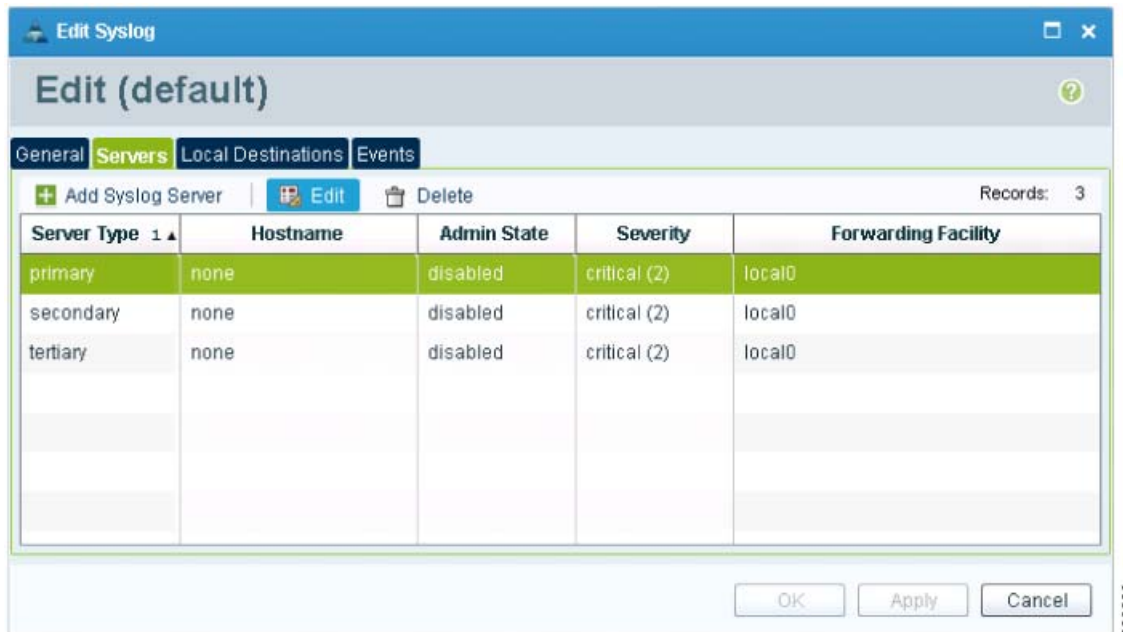
Send document comments to vsg-docfeedback@cisco.com

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



Step 5 Click on Servers tab. See [Figure 2-58](#).

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



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

Send document comments to vsg-docfeedback@cisco.com

Figure 2-59 Edit Syslog Server Dialog Box

- Step 7** In the Hostname/IP address field, enter the syslog server IP address.
- Step 8** From the Severity drop-down list, choose **Information(6)**.
- Step 9** From the Admin State drop-down list, choose **Enabled**.
- Step 10** Click **OK**.

Figure 2-60 Edit Syslog Dialog Box

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

Send document comments to vsg-docfeedback@cisco.com

Step 11 Click **OK**.

Enabling Global Policy-Engine Logging

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

You can enable global policy-engine logging.

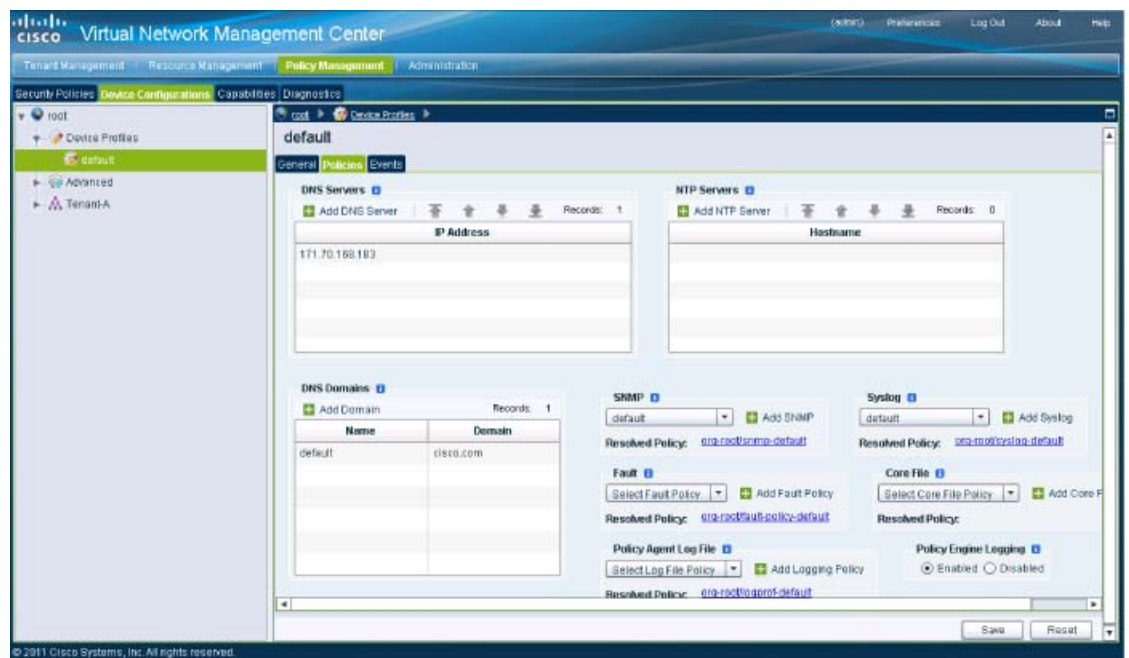
PROCEDURE

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

The Cisco VNMC Policy Management window opens.

Step 2 In the Device Profiles pane, choose **Policies**. See [Figure 2-61](#).

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



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

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

Send document comments to vsg-docfeedback@cisco.com

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

This section includes the following topics:

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

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

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

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

This example shows how to enable firewall protection:

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

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

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

Verifying the VSM/VEM for Cisco VSG Reachability

This example show how to verify VEM/VSG communication:

```
vsm# show vsn brief
```

Send document comments to vsg-docfeedback@cisco.com

```

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 VM Veth Port for Firewall Protection

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

```

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

```

**Note**

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

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

This section includes the following topics:

- [Sending Traffic Flow, page 2-57](#)
- [On the Cisco VSG, Verifying Policy-Engine Statistics and Logs, page 2-59](#)

Sending Traffic Flow

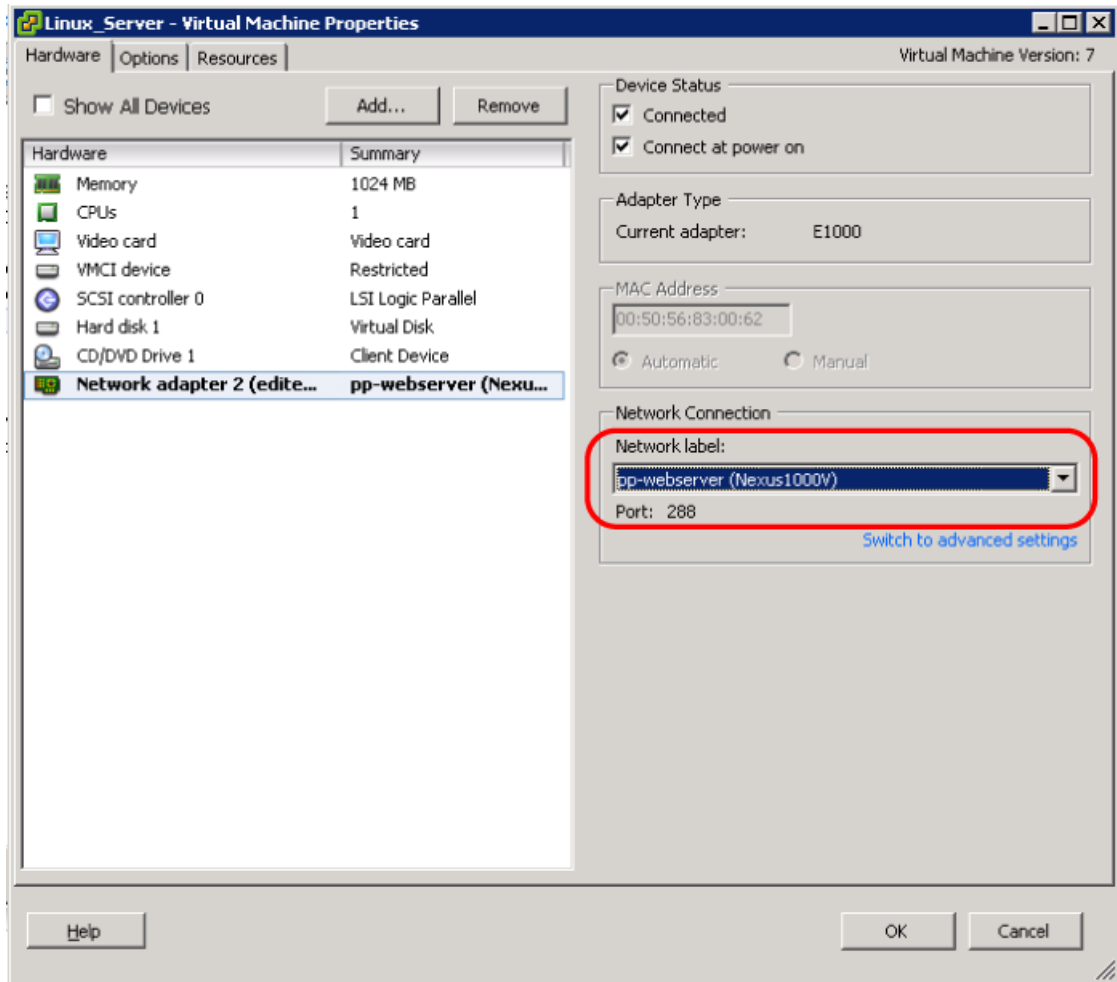
You can send traffic flow through the Cisco VSG to ensure that it is functioning properly.

PROCEDURE

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

Send document comments to vsg-docfeedback@cisco.com

Figure 2-62 Virtual Machine Properties Window



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

```
[root@sg-centos-vk1 ~]# wget http://172.31.2.92/
--2010-11-28 13:38:40-- http://172.31.2.92/
Connecting to 172.31.2.92:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 258 [text/html]
Saving to: `index.html'

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

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

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

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

Send document comments to vsg-docfeedback@cisco.com

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

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

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

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

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

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

Send document comments to vsg-docfeedback@cisco.com



PART 2

Installation Guide for the 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, page 3-1](#)
- [Prerequisites to Installing Cisco VSG Software, page 3-3](#)
- [Obtaining the Cisco VSG Software, page 3-3](#)
- [Installing the Cisco VSG Software, page 3-3](#)
- [Configuring Initial Settings, page 3-7](#)
- [Verifying the Cisco VSG Configuration, page 3-10](#)
- [Where to Go Next, page 3-11](#)

Information About the Cisco VSG

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

- [Host and VM Requirements, page 3-1](#)
- [Cisco Virtual Security Gateway and Supported Cisco Nexus 1000V Series Switch Terminology, page 3-2](#)

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)

[Send document comments to vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)

- 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)	Logical switch that spans one or more VMware ESX 4.0 servers. It is controlled by one VSM instance.
ESX/ESXi	Virtualization platform used to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine.
NIC	Network interface card.
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging: <ul style="list-style-type: none"> • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	Platform-independent method of packaging and distributing virtual machines.
vCenter Server	Service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 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 virtual supervisor module (VSM). All the VEMs that form a switch domain should be in the same virtual data center as defined by VMware vCenter Server.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host system concurrently.
vMotion	Practice of migrating virtual machines live from server to server. (The Cisco VSGs cannot be moved by vMotion.)
vPath	Component in the Cisco Nexus 1000V Series switch VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual switch that runs on a virtual machine (VM) and is based on Cisco NX-OS.
vSphere Client	User interface that enables users to connect remotely to the vCenter Server or ESX/ESXi from any windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

Send document comments to vsg-docfeedback@cisco.com

Prerequisites to Installing Cisco VSG Software

The Cisco VSG has the following prerequisites:

The following components must be installed and configured:

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

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

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

Installing the Cisco VSG Software

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

- [Installing the Cisco VSG Software from an OVA File, page 3-3](#)
- [Installing the VSG Software from an ISO File, page 3-6](#)

Installing the Cisco VSG Software from an OVA File

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

BEFORE YOU BEGIN



Before starting the procedure, know or do the following:

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

Send document comments to vsg-docfeedback@cisco.com

- HA Secondary
- Manual Installation

PROCEDURE

-
- Step 1** From the vSphere Client menu, choose the data center where you want to install the OVA file for the VSG.
- Step 2** Choose **File > Deploy OVF Template**.
The Source dialog box opens.
- Step 3** Click the **Deploy from file** radio button to browse and choose the location of the OVA file on the local disk.
- Step 4** Click **Next**.
The OVF Template Details dialog box opens displaying product information, including the size of the file and the size of the VM disk.
- Step 5** Click **Next**.
The End User License Agreement dialog box opens.
- Step 6** Read the End User License Agreement.
- Step 7** Click **Accept** and then click **Next**.
The Name and Location dialog box opens.
- Step 8** In the Name field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Step 9** From the Select a datastore in which to store the VM files pane, choose your datastore and click **Next**.
The Deployment Configuration window opens.
- Step 10** In the Configuration field, you will be presented with four options:
- Standalone
 - HA Primary
 - HA Secondary
 - Manual Installation
- For this example, choose **Standalone** and click **Next**.
The Disk Format dialog box opens.
-
-  **Note** We are using the Standalone installation for this document as an example. If you chose Manual Installation mode, you would choose the default values for the following steps.
-
-  **Note** In Standalone mode, be sure to fill in all the fields indicated below (they will be indicated on the GUI with red type).
-
- Step 11** From the Select a format in which to store the virtual machines virtual disks, click the radio button for the format you choose and click **Next**.

Send document comments to vsg-docfeedback@cisco.com

The Host or Cluster window opens.

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

Step 13 Click **Next**.

The Datastore dialog box opens.

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

Step 15 Click **Next**.

The Network Mapping dialog box opens.

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

Step 17 Click **Next**.

The Properties dialog boxes opens.

Step 18 Do the following:

- a. In the Cisco VSG HA ID field, enter a unique number between 1 and 4095. This number helps you to identify your Cisco VSG HA pairs.
- b. In the Nexus 1000VSG Administration User Password field, enter your password.
- c. In the Management IP Address field, enter the management address value.
- d. In the Management IP Subnet Mask field, enter the management subnet mask value.
- e. In the Management IP Gateway field, enter the management gateway value.

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

Step 19 Click **Next**.

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

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

Step 21 Click **Close**.

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

Step 22 Power on the Cisco VSG you just created.

Step 23 If you chose the Standalone mode for installation in [Step 10](#), you now see the Cisco VSG login prompt. Login with your Cisco VSG Administration password.

You may now proceed with configuring the Cisco Virtual Security Gateway. For details, see the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Fireway Policy Guide, Release 4.2(1)VSG1(2)*.

Step 24 If you chose the Manual installation in [Step 10](#), see the “[Configuring Initial Settings](#)” section on [page 3-7](#) to configure the initial settings on the Cisco VSG.

**Note**

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

Send document comments to vsg-docfeedback@cisco.com

Installing the VSG Software from an ISO File

You can install the Virtual Security Gateway from an ISO file.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

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

PROCEDURE

-
- Step 1** Upload the Cisco Virtual Security Gateway ISO image to the vCenter datastore.
- Step 2** From the data center in the vSphere Client menu, choose your ESX host where you want to install the Cisco Virtual Security Gateway and choose **New Virtual Machine**.
- The Create New Virtual Machine dialog box opens.
- For VM requirements, see the [“Host and VM Requirements” section on page 3-1](#). For detailed information about how to create a VM, see the VMware documentation.
- Step 3** Click the **Custom** radio button to create a VM, and click **Next**.
- The Create New Virtual Machine dialog box opens.
- Step 4** In the Name field, add a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Step 5** In the Inventory Location field, choose your data center and click **Next**.
- The Datastore dialog box opens.
- Step 6** From the Select a datastore in which to store the VM files pane, choose your datastore and click **Next**.
- The Virtual Machine Version dialog box opens.
- Step 7** Click the **Virtual Machine Version: 7** radio button to run on VMware ESX server version 4.0 or later versions 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, from the drop-down list, choose **Other 2.6x Linux (32-bit)** from the drop-down list. Click **Next**.
- The CPUs dialog box opens.
- Step 10** In the Number of virtual processors field, from the drop-down list, choose **1** and click **Next**.
- The Memory dialog box opens.
- Step 11** Choose **2GB** memory size and click **Next**.
- The Create Network Connectors dialog box opens.
- Step 12** In the How many NICs do you want to connect? field, from the drop-down list, choose **3**.

Send document comments to vsg-docfeedback@cisco.com

- Step 13** In the Network pane, from the drop-down lists, choose **service**, **management**, and **HA** port profiles in that sequence for the NIC 1, NIC 2, and NIC 3. Choose **VMXNET3** for the adapter type for NIC 1. Choose **E1000** for the adapter type for NIC 2 and NIC 3 and click **Next**.
The SCSI Controller dialog box opens.
- Step 14** The radio button for the default SCSI controller is chosen. Click **Next**.
The Select a Disk dialog box opens. The radio button for the default disk is chosen.
- Step 15** Click **Next**.
The Create a Disk dialog box opens. The default virtual disk size and policy is chosen.
- Step 16** Click **Next**.
The Advanced Options dialog box opens. The default options are chosen.
- Step 17** Click **Next**.
The Ready to Complete dialog box opens.
- Step 18** In the Settings for the new virtual machine pane, review your settings.
- Step 19** Check the **Edit the virtual machine before completion** check box and click **Continue**.
A dialog box with device details opens.
- Step 20** From the Hardware pane, choose your **New CD/DVD (adding)**.
- Step 21** Click the **Datastore ISO File** radio button to browse and, from the drop-down list, select your ISO file.
- Step 22** In the Device Status pane, check the **Connect at power on** check box and click **Finish**.
The Summary tab window opens.
- Step 23** In the Recent Tasks pane, wait for the Create virtual machine status to complete.
- Step 24** From the vSphere Client menu, choose your recently installed VM and in the VM pane, click **Power on the virtual machine**.
- Step 25** Click the **Console** tab to view the VM console. Wait for the Install Virtual Firewall and bring up the new image to boot.
See the [“Configuring Initial Settings” section on page 3-7](#) to configure the initial settings on the Cisco VSG.



Note To allocate additional RAM, first power off the VM by right-clicking on the VM icon and then choosing **Power > Power Off** from the popup window. After the VM is powered down, edit the configuration settings on the VM for controlling memory resources.

Configuring Initial Settings

This section describes how to configure initial settings on the Cisco VSG and includes the following topic:

- [Configuring Initial Settings on a Standby Cisco VSG, page 3-9](#)

Send document comments to vsg-docfeedback@cisco.com

When you power on the Cisco VSG for the first time, depending on which mode you used to install your Cisco VSG, you might be prompted to log in to the Cisco VSG to configure initial settings at the console on your vSphere Client.

For details about installing Cisco VSG, see the “Installing the Cisco VSG Software” section on page 3-3.

BEFORE YOU BEGIN

See [Table 3-2](#) to determine if you must configure initial settings as described in this section.

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

Your Cisco Virtual Security Gateway Software Installation Method	Do You Proceed with “Configuring Initial Settings”?
Installing an OVA file and choosing Manually Configure Nexus 1000VSG in the configuration field during installation.	Yes. Proceed with configuring initial settings described in this section.
Installing an OVA file and choosing any of the options other than the manual method in the configuration field during installation.	No. You have already configured the initial settings during the OVA file installation.
Installing an ISO file.	Yes. Proceed with configuring initial settings described in this section.

PROCEDURE

Step 1 At the Console tab on your VM after the Cisco VSG software image boots, create the admin password.

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



Note

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

Step 2 Confirm the admin password.

Step 3 Enter the HA role of the Cisco VSG.

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

Step 4 Enter an ID number for the HA pair.

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



Note

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

Step 5 Enter the basic system configuration setup dialog.

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

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

Send document comments to vsg-docfeedback@cisco.com

```

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

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

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

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

Mgmt IPv4 address:10.10.10.11

Mgmt IPv4 netmask:255.255.255.0

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

IPv4 address of the default gateway:10.10.10.1

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

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

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

The following configuration will be applied:
  Interface mgmt0
  ip address 10.10.10.11 255.255.255.0
  no shutdown
  interface data0
  ip address 215.1.1.1 255.255.0
  vrf context management
  ip route 0.0.0.0/10.10.11.1
  no telnet server enable
  ssh key rsa 768 force
  ssh server enable
  no feature http-server
  ha-pair id 25

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

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

```

Step 6 Enter the administrator login.

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

Step 7 Enter the password.

```
Password: <password>
```

You are now at the Cisco VSG node.

Configuring Initial Settings on a Standby Cisco VSG

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

Send document comments to vsg-docfeedback@cisco.com

PROCEDURE

Step 1 At the Console tab on your VM after the Cisco VSG software image boots, enter the admin password.

Enter the password for "admin":<password>

Step 2 Confirm the admin password.

Step 3 Enter an ID number for the HA pair.

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



Note

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

Step 4 Enter the HA role of the Cisco VSG.

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

Step 5 Enter the administrator login.

User Access Verification
VSG login: <admin>

Step 6 Enter the password.

Password: <password>

You are now at the Cisco VSG node.

Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, perform one of the tasks listed in [Table 3-3](#):

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

This example shows how to verify the Cisco VSG configurations.

vsg# **show interface brief**

```
-----
Port      VRF      Status IP Address      Speed  MTU
-----
mgmt0    --      up      10.193.77.217   1000   1500
-----
Port      VRF      Status IP Address      Speed  MTU
-----
data0    --      up      172.168.1.1     1000   1500
-----
```

Send document comments to vsg-docfeedback@cisco.com

```
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.

Send document comments to vsg-docfeedback@cisco.com



PART 3

Installation Guide for the Cisco Virtual Network Management Center



CHAPTER 4

Installing the Cisco Virtual Network Management Center

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

This chapter includes the following sections:

- [Information About Installing the Cisco VNMC, page 4-1](#)
- [Information About Deploying the OVF Template, page 4-1](#)
- [Installing the Cisco VNMC by Deploying the OVF Template, page 4-2](#)
- [Restoring the Cisco VNMC by Deploying the OVF Template, page 4-3](#)
- [Installing the Cisco VNMC Using an ISO Image, page 4-4](#)
- [Connecting to the Cisco VNMC, page 4-5](#)
- [Verifying Cisco VNMC Providers, page 4-6](#)

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

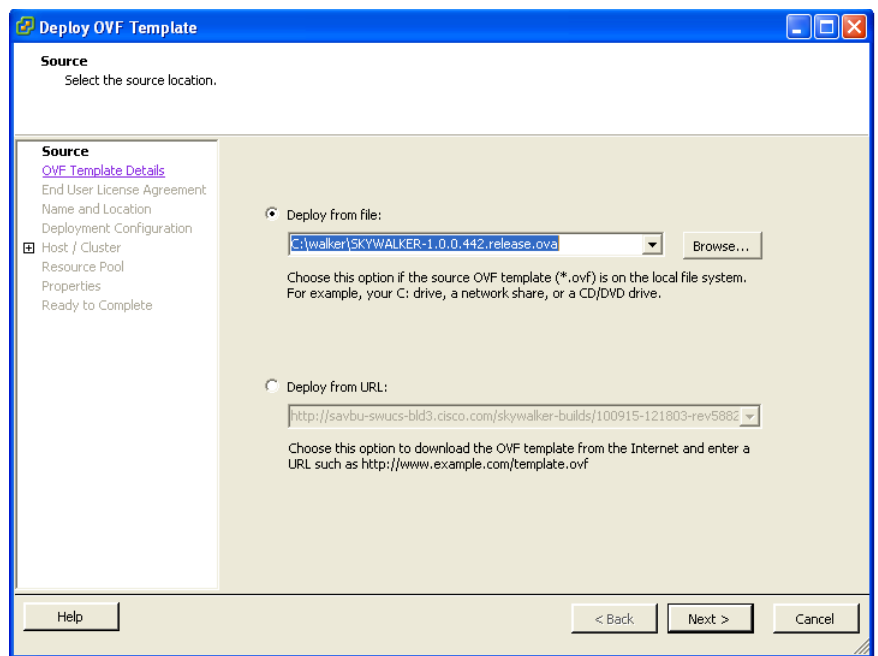
All the properties fields in the OVF template must have values. The selection you make on the Deployment Configuration page controls which fields are required and which fields are not. Optional and unused fields are automatically filled with null values. If you want to use an optional field, change the 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.

Send document comments to vsg-docfeedback@cisco.com

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.

Send document comments to vsg-docfeedback@cisco.com

- 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.

Send document comments to vsg-docfeedback@cisco.com

During the initial boot after completing the OVF template, the full-state backup is downloaded. If any issues with the restore occur, boot will stop and display an error message. The VM will also be rebooted on restore.

PROCEDURE

-
- Step 1** Open your VMware client.
- Step 2** Download the .ova file using one of the following methods:
- a. Use a conventional download method to download the Cisco VNMC .ova file from <http://www.cisco.com/en/US/products/ps11213/index.html>, and then start the OVF template.
 - b. Start the OVF template and download the Cisco VNMC .ova as follows:
 - Use your OVF template to select a file on your local machine.
 - Use your OVF template to download the file from cisco.com.
- Step 3** Follow the steps presented by the OVF template to restore the Cisco VNMC:
- a. When you reach the Deployment Configuration page, from the Configuration drop-down list, choose **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.

Send document comments to vsg-docfeedback@cisco.com

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:
- Ensure your virtual machine has the proper HDD size.
 - Ensure your virtual machine has 2-Gb RAM.
 - Choose **Red Hat Enterprise Linux 5 64-bit** as your operating system.
- Step 4** Boot your virtual machine from the ISO image.
The ISO installer appears.
- Step 5** Enter the appropriate values in the ISO installer.
- Step 6** Once the installation is completed, click **Reboot**.
The Cisco VNMC instance is created.
-

Connecting to the Cisco VNMC

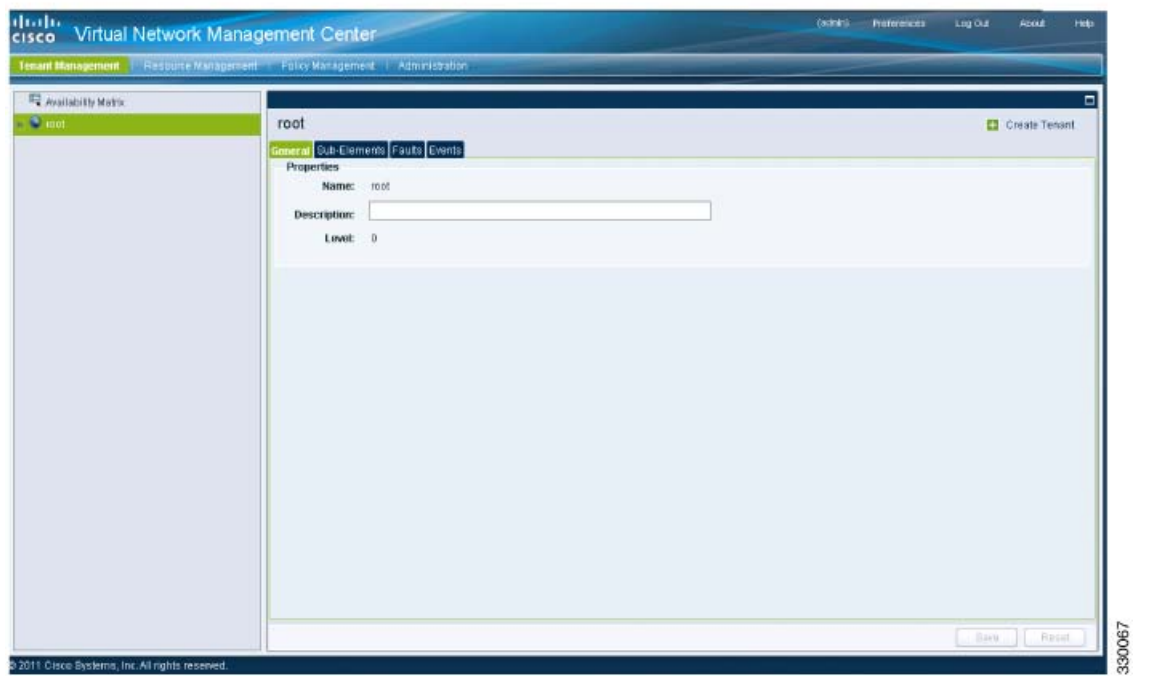
You can use your browser to connect to the Cisco VNMC.

PROCEDURE

-
- Step 1** Open a browser.
- Step 2** In the browser Address field, enter the IP address that you designated for your Cisco VNMC instance and click **Go**.
The login dialog box for Cisco VNMC appears.
- Step 3** Using the appropriate username and password, log into the Cisco VNMC.
You are connected to the Cisco VNMC.
[Figure 4-2](#) shows the main window of the Cisco VNMC.

Send document comments to vsg-docfeedback@cisco.com

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



Verifying Cisco VNMCM Providers

You can verify the Cisco VNMCM service providers as a way to ensure that the Cisco VNMCM 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, page 5-1](#)
- [Registering a Cisco Nexus 1000V VSM, page 5-2](#)
- [Registering vCenter, page 5-3](#)

Registering a Cisco VSG

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

PROCEDURE

- Step 1** Copy the `vnmc-vsgpa.1.2.1b.bin` file into the Cisco VSG bootflash:.
- ```
vsg# copy ftp://guest@172.18.217.188/n1kv/vnmc-vsgpa.1.2.1b.bin bootflash:
```
- Step 2** On the command line, enter configuration mode.
- ```
vsg# configure
```
- Step 3** Enter `config-vnm-policy-agent` mode.
- ```
vsg (config)# vnm-policy-agent
```
- Step 4** Set the Cisco VSG registration IP address.
- ```
vsg (config-vnm-policy-agent)# registration-ip 209.165.200.225
```
- Step 5** Assign a strong password for the Cisco VSG.
- ```
vsg (config-vnm-policy-agent)# shared-secret *****
```
- Step 6** Install the policy agent.
- ```
vsg (config-vnm-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.1.2.1b.bin
```
- Step 7** Exit all modes.
- ```
vsg (config-vnm-policy-agent)# top
```

**Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)**

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

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

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

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

The Cisco VSG registration is complete.

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

```
vsg# copy running-config startup-config
```

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

## Registering a Cisco Nexus 1000V VSM

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

### PROCEDURE

**Step 1** Copy the vnm-vmpa.1.2.1b.bin file into the VSM bootflash:

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

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

```
n1kv# configure
```

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

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

**Step 4** Set the 1000V registration IP address.

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

**Step 5** Assign a strong password for the VSG.

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

**Step 6** Install the policy agent.

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

**Step 7** Exit all modes.

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

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

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

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

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

The Cisco Nexus 1000V VSM registration is completed.

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

```
n1kv# copy running-config startup-config
```

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

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

---

### What To Do Next

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

## Registering vCenter

You can register vCenter with the Cisco VNMC.

### PROCEDURE

---

- Step 1** Log into the Cisco VNMC.
- Step 2** In the Cisco VNMC, choose **Administration > VM Managers**.
- Step 3** In the Navigation pane, right-click **VM Managers**.
- Step 4** Choose **Export vCenter Extension**.
- Step 5** In the dialog box that appears, choose the appropriate extension, and click **Save**.
- Step 6** Log into vSphere.
- Step 7** In your vSphere client, log into vCenter.
- Step 8** Choose **Plug-ins > Manage Plug-ins**.
- Step 9** Right-click the empty space and click **New Plug-in**.
- Step 10** Browse to the VNMC vCenter extension file, and then click **Register Plug-in**.
- Step 11** Click **Ignore** for any security warning.  
You should see a message that reports a successful registration.
- Step 12** Log into the Cisco VNMC and choose **Administration > VM Managers**.
- Step 13** In the Navigation pane, right-click **VM Managers**.
- Step 14** Click **Add VM Manager**.
- Step 15** Enter the vCenter name and IP address information and click **OK**.

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

vCenter is registered.

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***



## **PART 4**

### **Installing the Cisco VSG on a Cisco Nexus 1010 Appliance**





## CHAPTER 6

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

---

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

This chapter includes the following sections:

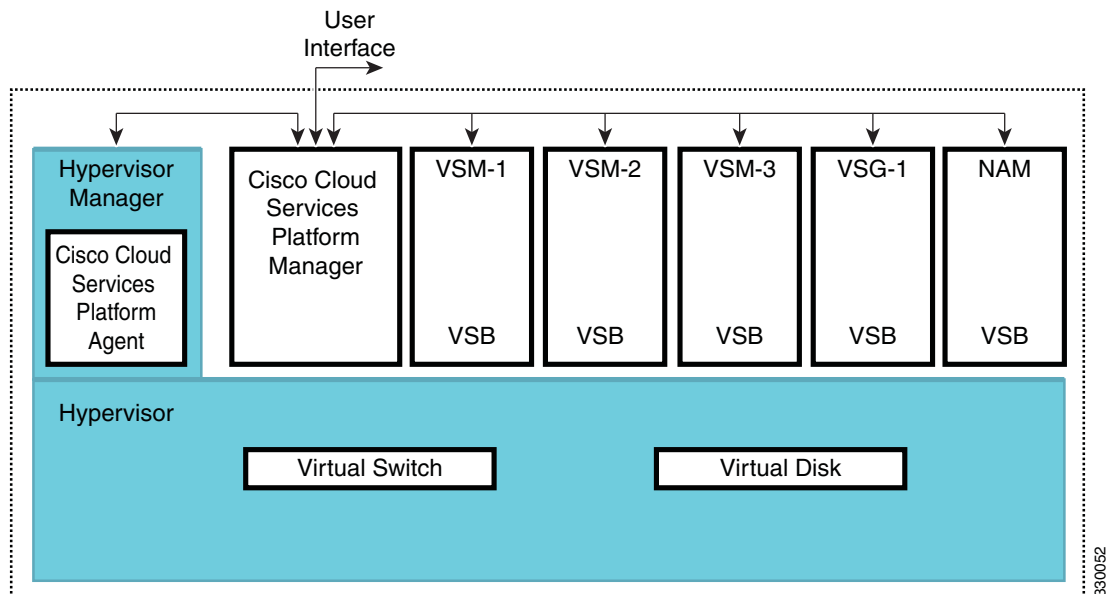
- [Information About Installing the Cisco VSG on the Cisco N1010, page 6-1](#)
- [Prerequisites, page 6-2](#)
- [Guidelines and Limitations, page 6-2](#)
- [Installing a Cisco VSG on a Cisco Nexus 1010, page 6-3](#)

## Information About Installing the Cisco VSG on the Cisco N1010

The Cisco VSG software is provided along with the other virtual service blade (VSB) software in the Cisco Nexus 1010 bootflash: repository directory. As shown in [Figure 6-1](#), the Cisco Nexus 1010 has up to six virtual service blades (VSBs) on which you can choose to place a Cisco VSG, VSM, or Network Analysis Module (NAM).

**Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)**

**Figure 6-1 Cisco Nexus 1010 Architecture Showing Virtual Service Blades Usage**



## Prerequisites

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

- You must first install the Cisco Nexus 1010 Virtual Services Appliance and connect it to the network. For procedures on installing the hardware, see the *Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide*.
- After you install the hardware appliance and connect it to the network, you can configure the Cisco Nexus 1010 management software, migrate existing VSMs residing on a VM to the Cisco Nexus 1010 as virtual service blades (VSBs), and create and configure new VSBs that may host the Cisco VSG. For procedures on configuring the software see the Cisco Nexus 1010 Software Configuration Guide, Release 4.2(1)SP1(3).

## Guidelines and Limitations

Installing the Cisco VSG on a Cisco Nexus 1010 as a virtual service blade (VSB) has the following guidelines and limitations:

- The Cisco Nexus 1010 appliance and its hosted Cisco VSG VSBs must share the same management VLAN.
- Unlike the data and high availability (HA) VLANs that are set when a Cisco VSG VSB is created, a Cisco VSG VSB inherits its management VLAN from the Cisco Nexus 1010.



### Caution

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



*Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)*

# Installing a Cisco VSG on a Cisco Nexus 1010

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

## BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You know the name of the Cisco VSG VSB that you want to create.
- Whether you are using a new ISO file from the bootflash repository folder or from an existing VSB, do one of the following.
  - If you are using a new ISO file in the bootflash repository, you know the filename.  
Cisco VSG: nexus-1000v.VSG1.2.iso
  - If you are using an ISO file from an existing VSB, you must know the name of the VSB type. This procedure includes information about identifying this name.
- You know the following properties for the Cisco VSG VSB:
  - HA ID
  - Management IP address
  - Management subnet mask length
  - Default gateway IPV4 address
  - Cisco VSG name
  - Administrator password
  - Data and HA VLAN IDs
- This procedure shows you how to identify and assign data and HA VLANs for the Cisco VSG VSB. Do not assign a management VLAN because the management VLAN is inherited from the Cisco Nexus 1010.

## SUMMARY STEPS



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

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>configure</b></p> <p><b>Example:</b><br/>N1010# configure<br/>N1010(config)#</p>                                                                                                                                                                                                                                                                                                                                                     | Places you in the global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 2 | <p><b>virtual-service-blade</b> <i>name</i></p> <p><b>Example:</b><br/>N1010(config)# virtual-service-blade vsg-1<br/>N1010(config-vsb-config)#</p>                                                                                                                                                                                                                                                                                        | <p>Creates the named VSB and places you into configuration mode for that service.</p> <p>The <i>name</i> can be an alphanumeric string of up to 80 characters.</p>                                                                                                                                                                                                                                                                         |
| Step 3 | <p><b>show virtual-service-blade-type summary</b></p> <p><b>Example:</b></p> <pre>N1010(config-vsb-config)# show virtual-service-blade-type summary</pre> <pre>----- Virtual-Service-Blade-Type   Virtual-Service-Blade -----</pre> <pre>VSM_SV1_3                   vsm-1                               vsm-2</pre> <pre>NAM-MV                       nam-1</pre> <pre>VSG-1                       vsg-1 switch(config-vsb-config)#</pre> | (Optional) Displays a summary of all VSB configurations by type name, such as Cisco VSG, VSM, or NAM. You use this type name (in this case, the name for the Cisco VSG) in the next step.                                                                                                                                                                                                                                                  |
| Step 4 | <p><b>virtual-service-blade-type</b> [<b>name</b> <i>name</i>   <b>new</b> <i>iso file name</i>]</p> <p><b>Example:</b><br/>N1010(config-vsb-config)# virtual-service-blade-type new nexus-1000v.VSG1.2.iso<br/>N1010(config-vsb-config)#</p> <p><b>Example:</b><br/>N1010(config-vsb-config)# virtual-service-blade-type name VSG-1<br/>N1010(config-vsb-config)#</p>                                                                     | <p>Specifies the type and name of the software image file to add to this Cisco VSG VSB.</p> <ul style="list-style-type: none"> <li>Use the <b>new</b> keyword to specify the name of the new Cisco VSG ISO software image file in the bootflash repository folder.</li> <li>Use the <b>name</b> keyword to specify the name of the existing Cisco VSG VSB type. Enter the name of an existing type found in the command output.</li> </ul> |
| Step 5 | <p><b>description</b> <i>description</i></p> <p><b>Example:</b><br/>N1010(config-vsb-config)# description vsg-1 for Tenant1<br/>N1010(config-vsb-config)#</p>                                                                                                                                                                                                                                                                              | <p>(Optional) Adds a description to the Cisco VSG VSB.</p> <p>The <i>description</i> is an alphanumeric string of up to 80 characters.</p>                                                                                                                                                                                                                                                                                                 |

**Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)**

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 6</b></p> <p><b>show virtual-service-blade name name</b></p> <p><b>Example:</b><br/> N1010(config-vs-b-config)# <b>show virtual-service-blade name vsg-1</b><br/> virtual-service-blade vsm2<br/> Description:<br/> Slot id: 2<br/> Host Name:<br/> Management IP:<br/> VSB Type Name : VSG-1.0<br/> Interface: ha vlan: 0<br/> Interface: management vlan: 231<br/> Interface: data vlan: 0<br/> Interface: internal vlan: NA<br/> Ramsize: 2048<br/> Disksize: 3<br/> Heartbeat: 0<br/> HA Admin role: Primary<br/> HA Oper role: NONE<br/> Status: VSB NOT PRESENT<br/> Location: PRIMARY<br/> SW version:<br/> HA Admin role: Secondary<br/> HA Oper role: NONE<br/> Status: VSB NOT PRESENT<br/> Location: SECONDARY<br/> SW version:<br/> VSB Info:<br/> switch(config-vs-b-config)#</p> | <p>Displays the Cisco VSG VSB that you have just created including the interface names that you configure in the next step.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p><b>Step 7</b></p> <p><b>interface name vlan vlanid</b></p> <p><b>Example:</b><br/> N1010(config-vs-b-config)# interface data<br/> vlan 1044<br/> N1010(config-vs-b-config)#</p> <p><b>Example:</b><br/> N1010(config-vs-b-config)# interface ha<br/> vlan 1045<br/> N1010(config-vs-b-config)#</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>Applies the interface and VLAN ID to this Cisco VSG. Use the interface names from command output.</p> <p><b>Note</b> If you try to apply an interface that is not present, the following error is displayed:</p> <p>ERROR: Interface name not found in the associated virtual-service-blade type.</p> <p><br/> <b>Caution</b> Do not assign a management VLAN. Unlike data and HA VLANs, the management VLAN is inherited from the Cisco Nexus 1010.</p> <p><br/> <b>Caution</b> To prevent loss of connectivity, you must configure the same data and HA VLANs on the hosted Cisco VSGs.</p> |
| <p><b>Step 8</b></p> <p>Repeat <a href="#">Step 7</a> to apply additional interfaces.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

|               | Command                                                                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 9</b> | <pre>enable [primary   secondary] <b>Example:</b> N1010(config-vsbs-config)# enable Enter domain id[1-4095]: 1054 Enter Management IP address: 10.78.108.40   Enter Management subnet mask length 28   IPv4 address of the default gateway: 10.78.108.117   Enter Switchname: VSG-1   Enter the password for 'admin': Hello_123 N1010(config-vsbs-config)#</pre> | <p>Initiates the configuration of the VSB and then enables it.</p> <p>If you enter the <b>enable</b> command without the optional <b>primary</b> or <b>secondary</b> keywords, it enables both.</p> <p>If you are deploying a redundant pair, you don't need to specify primary or secondary.</p> <p>If you are enabling a nonredundant VSB, you can specify its HA role as follows:</p> <ul style="list-style-type: none"> <li>• Use the <b>primary</b> keyword to designate the VSB in a primary role.</li> <li>• Use the <b>secondary</b> keyword to designate the VSB in a secondary role.</li> </ul> <p>The Cisco Nexus 1010 prompts you for the following:</p> <ul style="list-style-type: none"> <li>• HA ID</li> <li>• Management IP address</li> <li>• Management subnet mask length</li> <li>• Default gateway IPV4 address</li> <li>• Cisco VSG name</li> <li>• Administrator password</li> </ul> |

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

|                | <b>Command</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>Purpose</b>                                                                                                                                                                                                              |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 10</b> | <pre><b>show virtual-service-blade name name</b></pre> <p><b>Example:</b><br/> N1010(config-vs-b-config)# show<br/> virtual-service-blade name vsg-1<br/> virtual-service-blade vsg-1<br/> Description:<br/> Slot id: 1<br/> SW version: 4.0(4)SV1(3)<br/> Host Name: vsg-1<br/> Management IP: 10.78.108.40<br/> VSB Type Name : VSG-1.1<br/> Interface: ha vlan: 1044<br/> Interface: management vlan: 1032<br/> Interface: data vlan: 1045<br/> Interface: internal vlan: NA<br/> Ramsize: 2048<br/> Disksize: 3<br/> Heartbeat: 1156<br/> HA Admin role: Primary<br/> HA Oper role: STANDBY<br/> Status: VB POWERED ON<br/> Location: PRIMARY<br/> HA Admin role: Secondary<br/> HA Oper role: ACTIVE<br/> Status: VB POWERED ON<br/> Location: SECONDARY<br/> VB Info:<br/> Domain ID : 1054<br/> switch(config-vs-b-config)# </p> | <p>(Optional) Displays the new VSB for verification.</p> <p>While the Nexus 1010 management software is configuring the Cisco VSG, the output for this command progresses from <i>in progress</i> to <i>powered on</i>.</p> |
| <b>Step 11</b> | <pre><b>copy running-config startup-config</b></pre> <p><b>Example:</b><br/> N1010(config-vs-b-config)# copy<br/> running-config startup-config </p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <p>Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</p>                                                                                                |

## EXAMPLES

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

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

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

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

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

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

```

Enter HA id[1-4095]: 1233
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.193.73.42
Enter Management subnet mask: 255.255.248.0
IPv4 address of the default gateway: 10.193.72.1
Enter HostName: vsg-1
Enter the password for 'admin': Hello_123
N1010(config-vs-b-config)#
N1010(config-vs-b-config)# end
N1010#

```

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

```
N1010# show virtual-service-blade summary
```

```

Name Role State Nexus1010-Module

vsg-1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
vsg-1 SECONDARY VSB POWERED OFF Nexus1010-SECONDARY
vsg9 PRIMARY VSB NOT PRESENT Nexus1010-PRIMARY
vsg9 SECONDARY VSB DEPLOY IN PROGRESS Nexus1010-SECONDARY
nam_1 PRIMARY VSB POWERED OFF Nexus1010-PRIMARY
nam_1 SECONDARY VSB NOT PRESENT Nexus1010-SECONDARY
vsgc1 PRIMARY VSB POWERED ON Nexus1010-PRIMARY
vsgc1 SECONDARY VSB POWERED ON Nexus1010-SECONDARY
nam_2 PRIMARY VSB POWERED OFF Nexus1010-PRIMARY
nam_2 SECONDARY VSB NOT PRESENT Nexus1010-SECONDARY
N1010#

```

```

.
.
.

```



## **PART 5**

### **Upgrading the Cisco VSG and the Cisco VNMC**







## CHAPTER 7

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

---

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

This chapter includes the following sections:

- [Information About Cisco VSG Upgrades, page 7-1](#)
- [Information About Cisco VNMC Upgrades, page 7-1](#)
- [Upgrade Procedure in Sequence, page 7-2](#)
- [Upgrade Compatibility Matrix, page 7-8](#)

## Information About Cisco VSG Upgrades

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

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

An upgrade, there affects two bin files: one is the kickstart file and the other is the system file.

An upgrade does not erase any of the existing information. When the Cisco VSG comes online, everything is as is. Because the Cisco VSG is stateless, it gets all this information from the Cisco VNMC at bootup.

## Information About Cisco VNMC Upgrades

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

[Send document comments to vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)

## Upgrade Procedure in Sequence

This section describes the upgrade procedure.



### Note

We highly recommend that you use the following order for upgrading your Cisco VSG and Cisco VNMC.

- [Upgrading a Cisco VSG Pair, page 7-2](#)
- [Upgrading the VSM Pair, page 7-4](#)
- [Using the copy running-config startup-config Command on the Active VSM, page 7-4](#)
- [Upgrading the VEM, page 7-4](#)
- [Upgrading Cisco VNMC, page 7-4](#)
- [Upgrading the VSM-PA, page 7-6](#)
- [Upgrading the Cisco VSG-PA, page 7-7](#)



### Note

An upgraded Policy Agent (PA) without an upgraded Cisco VNMC will not be supported.

## Upgrading a Cisco VSG Pair

You can upgrade a Cisco VSG pair using the following procedure.



### Note

Although you might see the **install** command on the Cisco VSG CLI, the command is not operational for the current release. Please follow the steps provided in this section to upgrade your Cisco VSG software.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already copied the new software files into the bootflash file system.
- You have confirmed that the system is in high availability (HA) mode for an HA upgrade using the **show system redundancy status** command.

### SUMMARY STEPS

1. **configure**
2. **no boot system**
3. **no boot kickstart**
4. **boot system bootflash:** *system-filename*
5. **boot kickstart bootflash:** *kickstart-filename*
6. (Optional) **show boot**

## **Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)**

7. **copy running-config startup-config**
8. **reload module *standby\_module\_no***
9. **system switchover**

### DETAILED STEPS

|               | <b>Command</b>                                                                                                                                           | <b>Purpose</b>                                                                                                                                                                                                                               |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure</b><br><br><b>Example:</b><br>vsg# configure<br>vsg(config)#                                                                                | Places you in global configuration mode.                                                                                                                                                                                                     |
| <b>Step 2</b> | <b>no boot system</b><br><br><b>Example:</b><br>vsg(config)# no boot system                                                                              | Removes the existing system boot variable.                                                                                                                                                                                                   |
| <b>Step 3</b> | <b>no boot kickstart</b><br><br><b>Example:</b><br>vsg(config)# no boot kickstart                                                                        | Removes the existing kickstart boot variable.                                                                                                                                                                                                |
| <b>Step 4</b> | <b>boot system bootflash: <i>system-filename</i></b><br><br><b>Example:</b><br>vsg(config)# boot system bootflash:<br><i>system-filename</i>             | Adds the new system boot variable.                                                                                                                                                                                                           |
| <b>Step 5</b> | <b>boot kickstart bootflash: <i>kickstart-filename</i></b><br><br><b>Example:</b><br>vsg(config)# boot kickstart bootflash:<br><i>kickstart-filename</i> | Adds the new kickstart boot variable.                                                                                                                                                                                                        |
| <b>Step 6</b> | <b>show boot</b><br><br><b>Example:</b><br>vsg(config)# show boot                                                                                        | (Optional) Displays the system and kickstart variables for verification.                                                                                                                                                                     |
| <b>Step 7</b> | <b>copy running-config startup-config</b><br><br><b>Example:</b><br>vsg(config)# copy running-config<br>startup-config                                   | Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration. This step also initiates an image synchronization to the standby and the boot variable is synchronized to the standby. |
| <b>Step 8</b> | <b>reload module <i>standby_module_no</i></b><br><br><b>Example:</b><br>vsg(config)# reload module 2                                                     | If the primary Cisco VSG is active, the standby module number is 2. If the secondary Cisco VSG is active, the standby module number is 1. Make sure that the standby module has reloaded successfully and the HA pair is established.        |
| <b>Step 9</b> | <b>system switchover</b><br><br><b>Example:</b><br>vsg(config)# system switchover                                                                        | Reloads the active Cisco VSG to come up with the new image. Wait for HA synchronization to complete.                                                                                                                                         |

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

## Upgrading the VSM Pair

Upgrade the VSM pair according to the procedures in the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4a)*.

## Using the copy running-config startup-config Command on the Active VSM

Before continuing with the rest of the upgrade, you must use the **copy running-config startup-config** command on the active VSM.



### Note

It is critical that you enter the **copy running-config startup-config** command at this stage to keep your data flowing correctly.

## Upgrading the VEM

Upgrade the VEM according to the procedures in the *Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4a)*.

## Upgrading Cisco VNMC

You can upgrade the Cisco VNMC by using the following procedure.

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in as admin to the CLI in EXEC mode.
- You have already copied the new software files into the bootflash file system.
- You must have the Cisco VNMC Release 1.0.1 installed.

### SUMMARY STEPS

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

**Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)****DETAILED STEPS**

|               | <b>Command</b>                                                                                                                                                                                   | <b>Purpose</b>                                                                   |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>connect local-mgmt</b><br><br><b>Example:</b><br>vnm# connect local-mgmt<br>vnm(local-mgmt)#                                                                                                  | Places you in local management mode.                                             |
| <b>Step 2</b> | <b>show version</b><br><br><b>Example:</b><br>vnm(local-mgmt)# show version                                                                                                                      | (Optional) Displays the version information for the Cisco VNMC software.         |
| <b>Step 3</b> | <b>copy scp://example-server-ip/example-dir/ filename bootflash:/</b><br><br><b>Example:</b><br>vnm(local-mgmt)# copy<br>scp://<example-server-ip>/example-dir/vnm<br>.1.2.0.635.bin bootflash:/ | Copies the Cisco VNMC software file to the VM.                                   |
| <b>Step 4</b> | <b>dir bootflash:/</b><br><br><b>Example:</b><br>vnm(local-mgmt)# dir bootflash:/                                                                                                                | Verifies that the desired file is copied in the directory.                       |
| <b>Step 5</b> | <b>update bootflash: filename</b><br><br><b>Example:</b><br>vnm(local-mgmt)# update<br>bootflash:/vnm.1.2.0.635.bin                                                                              | Begins the update of the Cisco VNMC software.                                    |
| <b>Step 6</b> | <b>show version</b><br><br><b>Example:</b><br>vnm(local-mgmt)# show version                                                                                                                      | (Optional) Allows you to verify that the Cisco VNMC software version is updated. |

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

```
vnm# connect local-mgmt
Cisco Virtual Network Management Center
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

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

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

| Name         | Package          | Version | GUI     |
|--------------|------------------|---------|---------|
| ----         | -----            | -----   | ----    |
| core         | Base System      | 1.0(1m) | 1.0(1m) |
| service-reg  | Service Registry | 1.0(1m) | 1.0(1m) |
| policy-mgr   | Policy Manager   | 1.0(1m) | 1.0(1m) |
| resource-mgr | Resource Manager | 1.0(1m) | 1.0(1m) |
| vm-mgr       | VM manager       | 1.0(1m) | none    |

**Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)**

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

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

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

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

 891 Jun 10 05:52 vnmc-dplug.1.0.1m.bin
 21M Jun 8 21:01 vnmc-vsgpa.1.0.1m.bin
 20M Jun 8 21:01 vnmc-vsmpa.1.0.1m.bin
 144M Jun 16 21:32 vnmc.1.2.0.635.bin
```

Usage for bootflash://

```
18187836 bytes used
1534196 bytes free
19722032 bytes total
```

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

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

It is recommended that you perform a full-state backup before updating any VNMC component. Press enter to continue or Ctrl-c to exit.

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

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

| Name         | Package          | Version    | GUI        |
|--------------|------------------|------------|------------|
| core         | Base System      | 1.2(0.635) | 1.2(0.635) |
| service-reg  | Service Registry | 1.2(0.635) | 1.2(0.635) |
| policy-mgr   | Policy Manager   | 1.2(0.635) | 1.2(0.635) |
| resource-mgr | Resource Manager | 1.2(0.635) | 1.2(0.635) |
| vm-mgr       | VM manager       | 1.2(0.635) | none       |

## Upgrading the VSM-PA

Obtain the new VSM-PA from the Cisco VNMC download page. You can upgrade the VSM-PA by using the following procedure.

### PROCEDURE

**Step 1** Copy the image on the VSM in the bootflash directory.

```
vsg# copy scp://<example-server-ip>/example1-dir/vnmc-vsmpa.1.2.1b.bin bootflash:
```

**Step 2** Uninstall the existing VNM-PA on the Cisco VSM.

```
vsm# config
vsm(config)# vnm-policy-agent
vsm(config-policy-agent)# no policy-agent-image
```

**Step 3** Install the new VNM-PA image on the Cisco VSM.

## Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)

```
vsm(config-policy-agent)# policy-agent-image vnmc-vsmpa-image-name
vsm(config-policy-agent)# exit
vsm(config)# exit
vsm#
```

**Step 4** Verify if the installation was successful.

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.2(1b)
```

**Step 5** Copy the running configuration to the startup configuration.

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

---

## Upgrading the Cisco VSG-PA

You can upgrade the Cisco VSG-PA by using the following procedure.

### PROCEDURE

---

**Step 1** Copy the image on the Cisco VSG in the bootflash directory.

```
vsg# copy scp://<example-server-ip>/example1-dir/vnmc-vsgpa.1.2.1b.bin bootflash:
```

**Step 2** Uninstall the existing VNM-PA on the Cisco VSG.

```
vsg# config
vsg(config)# vnm-policy-agent
vsg(config-policy-agent)# no policy-agent-image
```

**Step 3** Install the new VNM-PA image on the Cisco VSG.

```
vsg(config-policy-agent)# policy-agent-image vnmc-vsgpa-image-name
vsg(config-policy-agent)# exit
vsg(config)# exit
vsg#
```

**Step 4** Verify if the installation was successful.

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.2(1b)
```

**Step 5** Copy the running configuration to the startup configuration.

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

---

[Send document comments to vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)

# Upgrade Compatibility Matrix

Table 7-1 shows how the components of a Cisco VSG and a Cisco VNMC upgrade work during the complete upgrade process.


**Note**

We highly recommend that you upgrade the Cisco VSG and the Cisco VNMC in the order provided. Any deviation from the ordered steps could cause disruption of your connectivity and data communication.

**Table 7-1** Cisco VSG and Cisco VNMC Upgrade Compatibility Matrix

| Virtual Appliance    | Original State        | Phase 1: VSG Upgrade (with old PA)                                                                                                                                                                                                                                                                                                           | Phase 2: VSM/VEM Upgrade (with old PA)                                                                                                        | Phase 3: VNMC Upgrade                                                                                                                                                                                      |
|----------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VSG                  | Release 4.2(1)VSG1(1) | Release 4.2(1)VSG1(2) (bin upgrade for HA or reassociated for standalone)                                                                                                                                                                                                                                                                    | Release 4.2(1)VSG1(2)                                                                                                                         | Release 4.2(1)VSG1(2)                                                                                                                                                                                      |
| VSM/VEM              | Old                   | Old                                                                                                                                                                                                                                                                                                                                          | New                                                                                                                                           | New                                                                                                                                                                                                        |
| VNMC                 | Release 1.0.1         | Release 1.0.1                                                                                                                                                                                                                                                                                                                                | Release 1.0.1                                                                                                                                 | Release 1.2                                                                                                                                                                                                |
| VSM Policy-Agent     | Old                   | Old                                                                                                                                                                                                                                                                                                                                          | Old                                                                                                                                           | New                                                                                                                                                                                                        |
| VSG Policy-Agent     | Old                   | Old                                                                                                                                                                                                                                                                                                                                          | Old                                                                                                                                           | New                                                                                                                                                                                                        |
| Supported Operations | All                   | <ul style="list-style-type: none"> <li>Existing data sessions (offloaded)</li> <li>New data sessions</li> <li>Short disruption in new data session establishment during Cisco VSG upgrade</li> <li>Allows Cisco Nexus 1000V switch (non-vn-service) operations including non-vn-service port profiles</li> <li>Cisco VSG failover</li> </ul> | <ul style="list-style-type: none"> <li>Reestablishment of existing sessions</li> <li>New data sessions</li> <li>Cisco VSG failover</li> </ul> | <ul style="list-style-type: none"> <li>Existing data sessions (offloaded)</li> <li>Allows Cisco Nexus 1000V switch (non-vn-service) operations</li> <li>Once upgraded, all operations supported</li> </ul> |



***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

| Virtual Appliance     | Original State | Phase 1: VSG Upgrade (with old PA)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Phase 2: VSM/VEM Upgrade (with old PA)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Phase 3: VNMC Upgrade |
|-----------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Restricted Operations | None           | <ul style="list-style-type: none"> <li>No Cisco VNMC policy configuration change (silent drops)</li> <li>No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, and so on)</li> <li>No new vn-service VMs brought up</li> <li>No bootstrap of devices (Cisco VNMC, Cisco VSG, VSM)</li> <li>No vMotion of vn-service firewalled VMs on Cisco Nexus 1000V Switch</li> <li>No vn-service port profile operations or modifications (toggles, removal, changing the port profiles on VSM)</li> <li>All VSM to Cisco VNMC to Cisco VSG control operations are restricted</li> </ul> | <ul style="list-style-type: none"> <li>No Cisco VNMC policy configuration change (silent drops)</li> <li>Allows Cisco Nexus 1000V switch (non-vn-service) operations, including non-vn service port profiles</li> <li>No VSM/VEM vn-service VM operations (shutdown/bring up existing vn-service VMs, bring down net adapters, and so on)</li> <li>No new vn-service VMs brought up</li> <li>No bootstrap of devices (Cisco VNMC, Cisco VSG, VSM)</li> <li>No vMotion of vn-service firewalled VMs on Cisco Nexus 1000V Switch</li> <li>No vn-service port profile operations or modifications (toggles, removal, changing the port profiles on VSM)</li> <li>All VSM to Cisco VNMC to Cisco VSG control operations are restricted</li> </ul> | None                  |

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***



## 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, page A-1](#)
- [OVA Installation Using an ISO Image, page A-3](#)

## 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.

### PROCEDURE

- 
- Step 1** Open your vSphere client.
  - Step 2** Click **Hosts and Clusters** and choose a host.
  - Step 3** From the toolbar, choose **File > Deploy OVF Template**.  
The Deploy OVF Template dialog box appears. In the dialog box, choose an .ova file on your local machine, or choose a file from another location (URL).
  - Step 4** Click **Deploy from File**.
  - Step 5** Click **Browse**.  
The Open dialog box appears.
  - Step 6** From the Open dialog box, choose the appropriate .ova file and click **Open**.
  - Step 7** Click **Next**.

**Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)**

The OVF Template Details page appears inside the Deploy OVF Template dialog box. The OVF Template Details page is the first of six pages in the Deploy OVF Template dialog box that you use to set parameters for the Cisco VNMC instance.

**Step 8** View your template details and click **Next**.

The End User License Agreement page appears.

**Step 9** View the license and click **Accept**.

**Step 10** Click **Next**.

The Name and Location page appears.

**Step 11** In the Name field, enter a template name.

**Step 12** In the Inventory Location area, choose the appropriate folder.

**Step 13** Click **Next**.

The 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 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 click **Finish**.

The progress dialog box appears. Once the virtual machine is installed, the Deployment Completed Successfully dialog box appears.

**Step 24** Click **Close**.

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

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:
- Ensure your virtual machine has the proper HDD size.
  - Ensure your virtual machine has 2 GB of RAM.
  - Choose **Red Hat Enterprise Linux 5 64-bit** as your operating system.
- Step 4** Power on your virtual machine.
- Step 5** Mount the ISO to the virtual machine CD ROM drive as follows:
- Right-click the virtual machine and choose **Open the VM Console**.
  - From the virtual machine console, click **Connect/Disconnect CD/DVD Devices**.
  - Choose **CD/DVD Drive1**.
  - Choose **Connect to ISO Image on Local Disk**.
  - Choose the ISO image that you downloaded.
- Step 6** Reboot the VM using VM, Guest, and pressing **Ctrl+Alt+Del**.  
The ISO installer appears.
- Step 7** Enter the appropriate values in the ISO installer.
- Step 8** Once installation is completed, click **Reboot**.  
The Cisco VNMC instance is created.
-

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***



## INDEX

---

### A

access control rule [1-3](#)  
access logs [1-3](#)  
admin password [2-7, 2-13](#)  
Adobe Flash Player [2-5, 2-15, 2-35](#)  
API [1-8](#)  
attribute  
    custom [1-3](#)

---

### C

Cisco Nexus 1000V  
    registration [5-2](#)  
Cisco Nexus 1000V Series switch [3-3](#)  
Cisco NX-OS [3-2](#)  
Cisco Virtual Network Management Center. See VNMC [1-4](#)  
Cisco Virtual Security Gateway (see VSG) [1-4](#)  
Cisco VNMC [1-6, 3-11](#)  
    API [1-8](#)  
    architecture [1-6, 1-7](#)  
    clients [2-38](#)  
    Firewall Profile [2-41](#)  
    policy management [2-39](#)  
    registration [5-1](#)  
    security profile [2-40](#)  
    tenant management [2-38](#)  
Cisco VNMC main window [2-16, 2-36](#)  
Cisco VSG  
    bootflash [5-1](#)  
    CLI [2-51, 5-2](#)  
    HA primary [3-3](#)

HA secondary [3-4](#)  
registration [5-1](#)  
secondary [3-9](#)  
standalone [3-3](#)  
standby [3-9](#)  
client [2-38](#)  
compute firewall [2-41](#)  
context-aware rule set [1-3](#)  
CPU speed [3-2](#)  
custom attributes [1-3](#)

---

### D

datastore [2-29, 3-3, 3-4, 3-5](#)  
Datastore window [2-10](#)  
Deployment Configuration window [3-4](#)  
Deploy OVF Template [2-7](#)  
disk format  
    thick provisioned format [2-11, 2-30](#)  
    thin provisioned format [2-11, 2-30](#)  
distributed virtual switch [1-2](#)  
distributed virtual switch. See DVS [3-2](#)  
DNS [4-3, A-2](#)  
domain name [2-13, 4-3, A-2](#)  
domain name server [2-13](#)

---

### E

E1000 [3-1](#)  
End User License Agreement [2-8, 2-26, 3-4](#)  
error message [4-1](#)  
ESX [2-2, 2-6, 2-29, 3-1, 3-2, 3-6](#)  
ESX host [2-11](#)

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

ESXi [2-2, 2-6, 3-1, 3-2](#)

Export vCenter Extension [2-17](#)

---

## F

firewall policies [3-11](#)

firewall security [2-38](#)

Flash Player [2-5, 2-15, 2-35](#)

---

## G

gateway [2-13, 4-3](#)

global policy-engine logging [2-55](#)

---

## H

HA [1-9, 2-23, 3-8](#)

HA ID [2-32, 3-5, 3-8](#)

HA primary [3-3](#)

HA secondary [3-4](#)

high availability. See HA [1-9](#)

host name [2-7](#)

hostname [2-13, 3-3, 4-3, A-2](#)

Hypervisor [1-2](#)

---

## I

inventory folder [3-3](#)

Inventory Location [2-27](#)

IP address [3-3, 4-3, A-2](#)

IPv4 [2-13](#)

ISO [3-3, 3-8, 4-1, 4-4, A-3](#)

ISO file [3-6](#)

---

## L

Linux [3-1, 3-6](#)

logging level 6 [2-52](#)

logical trust zone [1-3](#)

---

## M

management address [3-5](#)

management gateway [3-5](#)

Management IP Address [2-32](#)

management port-profile name [2-7](#)

manual installation [3-4](#)

---

## N

netmask [2-13, 4-3](#)

network file storage (see NFS) [2-11](#)

network mapping [2-12, 2-30](#)

NFS [2-11, 2-29](#)

NIC [3-1, 3-2, 3-6](#)

E1000 [3-1](#)

VMXNET3 [3-1](#)

null value [2-13, 4-1](#)

---

## O

object configuration [1-7](#)

Open Virtual Appliance or Application. See OVA [3-2](#)

Open Virtual Machine Format. See OVF [3-2](#)

optical disk media. See ISO [4-1](#)

OVA [3-2, 3-3, 3-8, 4-1, A-1](#)

OVA file [2-2, 2-25](#)

OVF [3-2](#)

OVF Template [2-23, 2-24](#)

OVF template [2-2, 3-4, 4-1, 4-4, A-2](#)

OVF Template Details [2-7](#)

---

## P

packet processing [1-2](#)

packets [1-5](#)



***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

password [2-7, 2-13, 3-5, 3-8, 4-3, 5-1, A-2](#)  
 permit-all rule [2-45](#)  
 policy agent [2-21, 2-34, 5-1](#)  
 policy agent image [2-4, 2-21](#)  
 policy-based traffic monitoring [1-3](#)  
 policy enforcement [1-2](#)  
 policy-engine logging [2-52](#)  
 policy-engine statistics [2-6, 2-58](#)  
 policy evaluation [1-2](#)  
 port profile [1-4, 1-8, 2-6, 2-22, 2-56, 3-3](#)  
     data interface [2-31](#)  
     HA interface [2-31](#)  
     management interface [2-31](#)  
 port profile name [3-3](#)  
 port-profile name [2-7](#)  
 port profile policies [1-5](#)

---

## R

red error message [4-1](#)  
 Red Hat Enterprise Linux. See RHEL [1-6, 4-5](#)  
 related documents [i-vii, 2-6](#)  
 RHEL [1-6](#)  
 rule  
     permit all [2-45](#)

---

## S

SAN [2-11, 2-29](#)  
 SCSI [3-1, 3-7](#)  
 security policy [1-8, 2-47](#)  
 security profile [1-3, 1-4, 1-8](#)  
 security profiles [1-5](#)  
 security template [1-7](#)  
 shared secret password [2-7, 2-13, 2-32, 4-3](#)  
 standby Cisco VSG [3-9](#)  
 storage [2-11](#)  
 storage area network (see SAN) [2-11](#)

switch uplink port [3-3](#)  
 system requirements [1-8](#)

---

## T

template-based configuration [1-8](#)  
 tenant [1-3, 2-38](#)  
 tenant management [2-38](#)  
 thick provisioned format [2-11, 2-30](#)  
 thin provisioned format [2-11, 2-30](#)  
 traffic [2-6, 2-58](#)  
 trust zone [1-1](#)

---

## V

vApp [1-3](#)  
 vCenter [1-4, 2-5, 2-24, 3-2](#)  
     registration [5-2, 5-3](#)  
 vDC [1-3, 2-38](#)  
 VEM [3-2](#)  
 virtual appliance [1-6](#)  
 Virtual Center. See vCenter [1-4](#)  
 virtual data center. See vDC [1-3, 1-6](#)  
 virtualization [1-4](#)  
 virtual machine. See VM [1-1](#)  
 virtual processor [3-6](#)  
 Virtual Supervisor Module. See VSM [1-4](#)  
 VLAN [1-3, 3-3](#)  
     HA [1-5](#)  
     management [1-5](#)  
     service [1-5](#)  
 VLAN creation [2-22](#)  
 VM [1-1, 2-38, 3-1, 3-2, 4-1](#)  
 vMotion [1-4, 3-2](#)  
 VMware [1-2, 1-3, 2-2, 2-6, 3-1, 3-6](#)  
 VMXNET3 [3-1](#)  
 vNIC  
     data [1-5](#)

***Send document comments to [vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)***

HA [1-5](#)

management [1-5](#)

VNMC. See Cisco VNMC [1-6](#)

VNMC Installer [2-10](#)

VNMC OVA file [2-7](#)

VNM policy agent [2-21](#)

vPath [1-2, 1-3, 1-5, 3-2](#)

VSG [3-2](#)

VSM [1-4, 1-8, 2-21, 3-2](#)

vSphere [1-2, 1-3, 2-18, 3-2, 3-4, 3-6](#)

Installer [A-1](#)

---

## W

Website Security Certification window [2-15, 2-35](#)

---

## X

XML [1-7](#)

XML API [1-7](#)

---

## Z

zone-based access control [1-1](#)

zone-based enforcement [1-3](#)

zone membership [1-3, 1-4](#)

zone scaling [1-2](#)