Cisco VSG for Microsoft Hyper-V, Release 5.2(1)VSG1(4.1) and Cisco VNMC, Release 2.1 Installation Guide

First Published: June 03, 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-28943-01

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.

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

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

CONTENTS

Preface

CHAPTER 1

CHAPTER 2

Preface

This preface contains the following sections:

Audience

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

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

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

Examples use the following conventions:

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

This document uses the following conventions:

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

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

Documentation Feedback

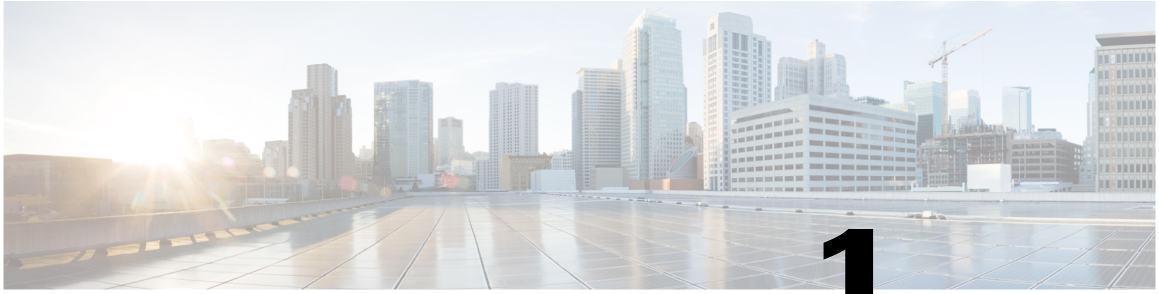
To provide technical feedback on this document, or to report an error or omission, please send your comments to vsg-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, 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 contains the following sections:

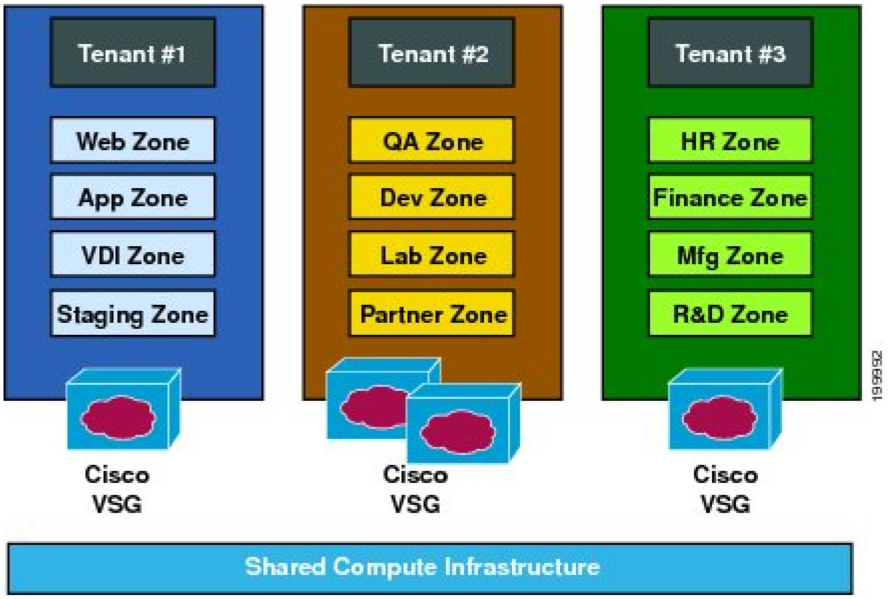
Information About Installing the Cisco VNMC and the Cisco VSG

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

Information About Cisco VSG

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

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

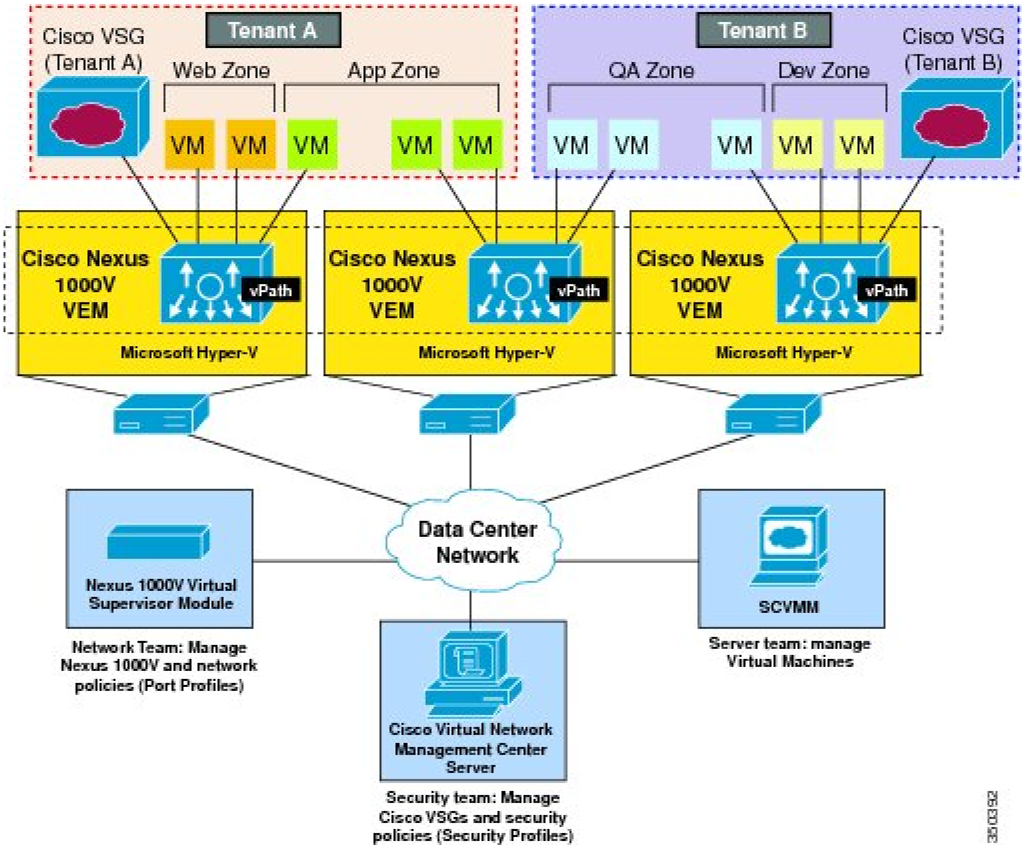


Cisco VNMC and VSG Architecture

The Cisco VSG operates with the Cisco Nexus 1000V Series switch in the Microsoft Hyper-V or the Cisco Cloud Service Platform Virtual Services Appliance, and the Cisco VSG leverages the virtual network service data path (vPath). vPath steers traffic, whether external-to-VM or VM-to-VM, to the Cisco VSG of a tenant.

Initial packet processing occurs in the Cisco VSG for policy evaluation and enforcement. After the policy decision is made, the Cisco VSG offloads policy enforcement of the remaining packets to vPath.

Figure 2: Cisco Virtual Security Gateway Deployment Topology


Cisco VSG (Tenant A)
Tenant A
Web Zone
App Zone
Tenant B
QA Zone
Dev Zone
Cisco VSG (Tenant B)
VM
Cisco Nexus 1000V VEM
vPath
Microsoft Hyper-V
Data Center Network
Nexus 1000V Virtual Supervisor Module
Network Team: Manage Nexus 1000V and network policies (Port Profiles)
SCVMM
Server team: manage Virtual Machines
Cisco Virtual Network Management Center Server
Security team: Manage Cisco VSGs and security policies (Security Profiles)
350392

vPath supports the following features:

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

The Cisco VSG and the VEM provide the following benefits:

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

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

Trusted Multitenant Access

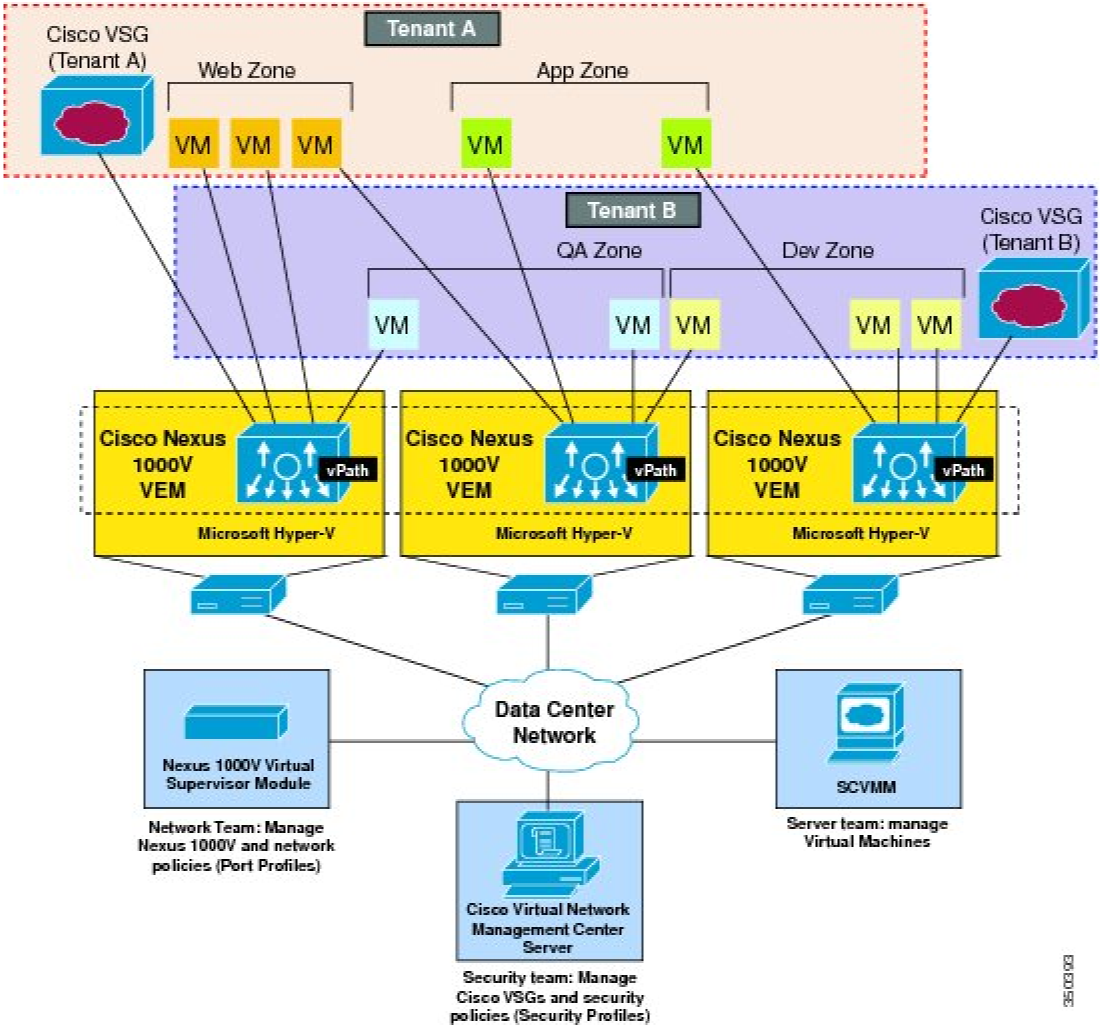
You can transparently insert a Cisco VSG into the Microsoft Hyper-V environment where the Cisco Nexus 1000V is deployed. One or more instances of the Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy a Cisco VSG at the tenant level in Hyper-V and manage each tenant instance using System Center Virtual Machine Manager (SCVMM).

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

Dynamic Virtualization-Aware Operation

A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. The following figure shows how the structured environment can change over time due to dynamic VMs.

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



The Cisco VSG operating with the Cisco Nexus 1000V (and vPath) supports a dynamic VM environment. When you create a tenant with the Cisco VSG (standalone or active-standby pair) on the Cisco 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 Microsoft SCVMM.

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 re-purpose a VM by assigning it to a different port profile or security profile.

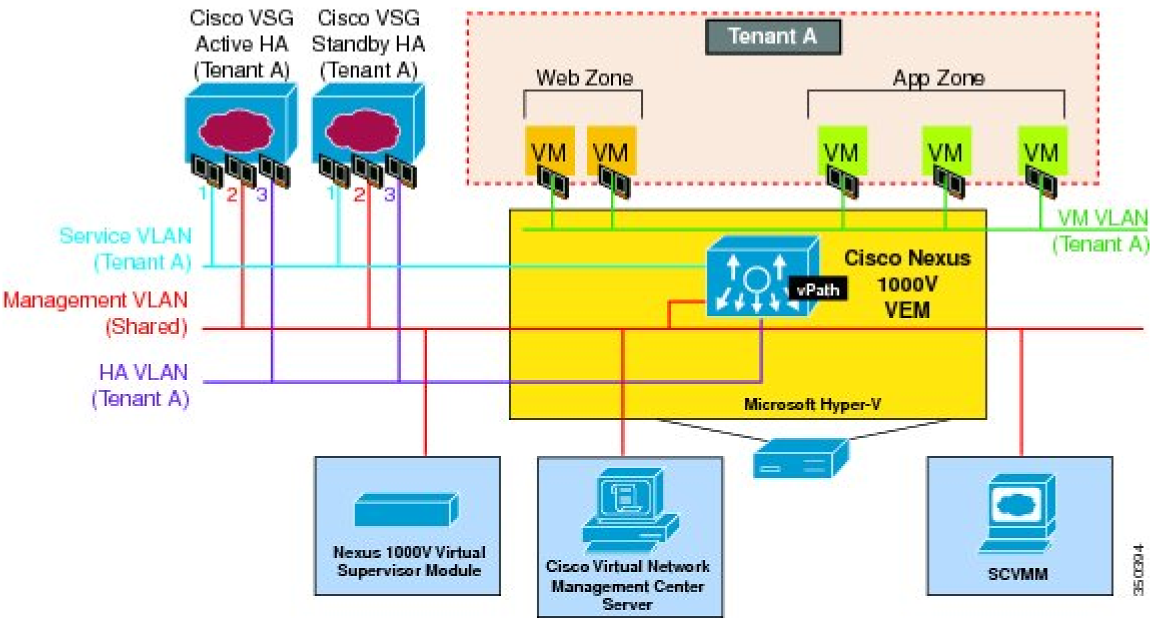
As VM migration events are triggered, VMs move across physical servers. Because the Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to the migration events.

Setting Up the Cisco VSG and VLAN

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

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

Figure 4: Cisco Virtual Security Gateway VLAN Usages



The VLAN functions are as follows:

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

You can allocate one or more VM data VLANs for VM-to-VM communications. In a typical multitenant environment, the management VLAN is shared among all the tenants and the service VLAN, HA VLAN, and the VM data. VLANs are allocated on a per-tenant basis. However, when VLAN resources become scarce, you might decide to use a single VLAN for service and HA functions.

Information About the Cisco VNMC

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

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

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

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 Components

The Cisco VNMC architecture includes the following components:

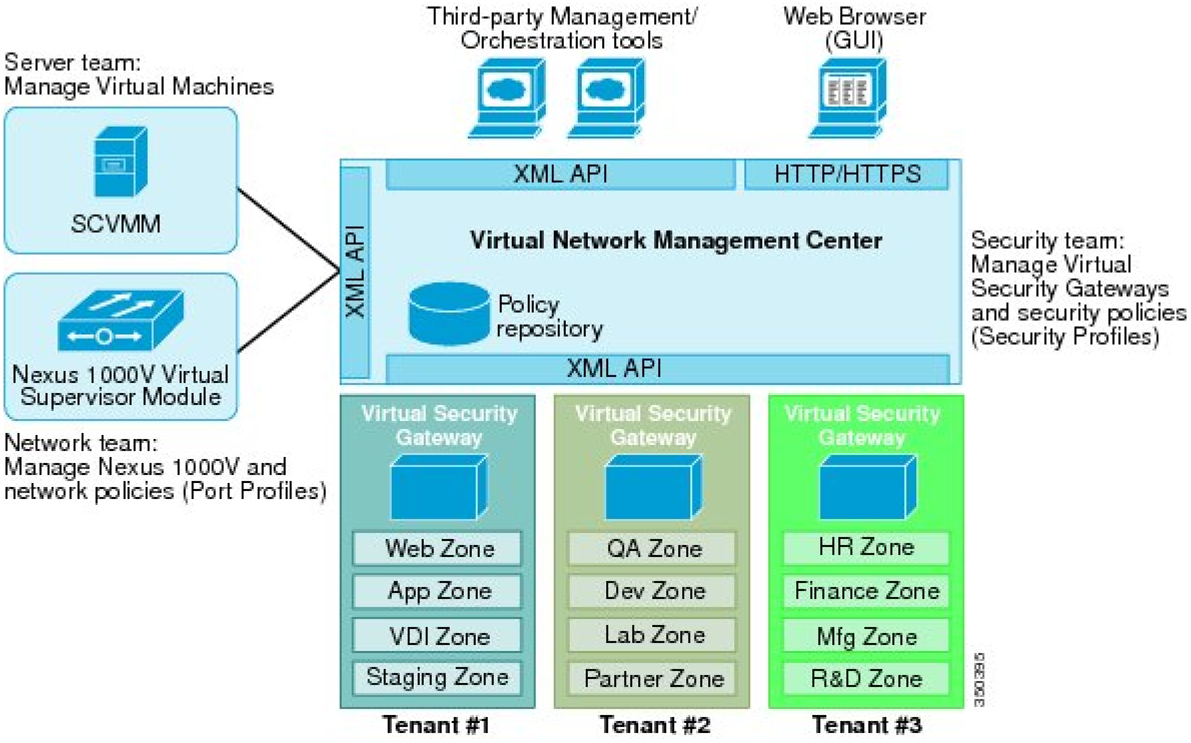
- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning.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

- A distributed management-plane function that uses an embedded management agent on each device that allows for a scalable management framework.

Cisco VNMC Architecture

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

Figure 5: Cisco VNMC Components


Third-party Management/ Orchestration tools
Web Browser (GUI)
Server team: Manage Virtual Machines
SCVMM
Nexus 1000V Virtual Supervisor Module
Network team: Manage Nexus 1000V and network policies (Port Profiles)
XML API
HTTP/HTTPS
XML API
Virtual Network Management Center
Policy repository
XML API
Security team: Manage Virtual Security Gateways and security policies (Security Profiles)
Virtual Security Gateway
Web Zone
App Zone
VDI Zone
Staging Zone
Tenant #1
Virtual Security Gateway
QA Zone
Dev Zone
Lab Zone
Partner Zone
Tenant #2
Virtual Security Gateway
HR Zone
Finance Zone
Mfg Zone
R&D Zone
Tenant #3
350395

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 VSG

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

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

System Requirements

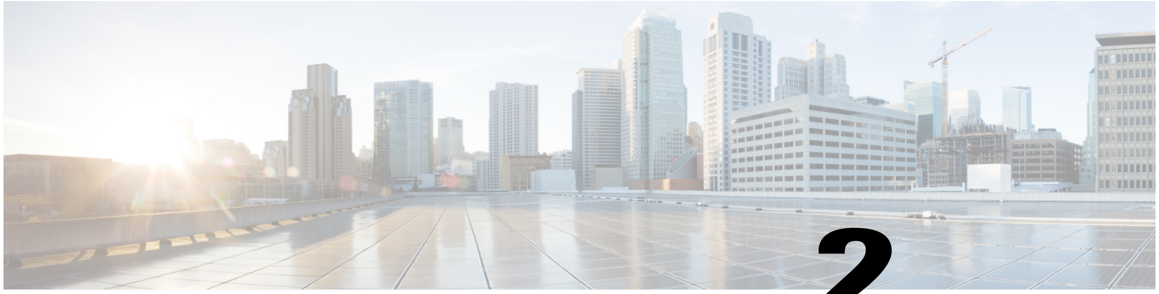
System requirements for a Cisco VNMC are as follows:

- Microsoft Windows Server with SCVMM SP1.
- Intel VT that is enabled in the BIOS.
- 4 GB is required for VNMC ISO installation.
- 25 GB disk space available on shared Network File System/Storage Area Network (NFS/SAN) storage when the Cisco VNMC is deployed in an HA cluster.
- Flash 10.1.
- Internet Explorer 9.0 or Mozilla Firefox11.0 on Windows or Chrome 26.0

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

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

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



CHAPTER 2

Installing the Cisco VNMC and Cisco VSG - Quick Start

This chapter contains the following sections:

Information About Installing the Cisco VNMC and the Cisco VSG

This chapter describes how to install and set up a basic working configuration of the Cisco VNMC and Cisco VSG. The example in this chapter uses the ISO files of the software for installation. The steps assume that the Cisco Nexus 1000V Series switch is operational, 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 a successful operation of the Cisco VNMC and Cisco VSG.

Basic Hardware and Software Requirements

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

Important Cisco VSG is supported as VSB on Nexus Cloud Services platform only.

- Microsoft SCVMM SP1
- 6 GB (2 GB for VSG and 4 GB for VNMC) of memory
- 27 GB (2 GB for VSG and 25 GB for VNMC) of disk space
- Three Network Interfaces (NICs) for VSG
- Cisco VSG software available for download at http://www.cisco.com/en/US/products/ps11208/index.html
- Cisco VNMC software available for download at http://www.cisco.com/en/US/products/ps11213/index.html

VLAN Configuration Requirements

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

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

Required Cisco VNMC and Cisco VSG Information

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

Type	Your Information
Cisco VSG name—Unique within the inventory folder and up to 80 characters	
Hostname—Where the Cisco VSG will be installed in the inventory folder	

Type	Your Information
ISOs—Managed within SCVMM library, if stored at C:\ProgramData\Virtual Machine Manager Library Files\ISO to manage. Refresh the SCVMM library after saving the ISO file to the specified location.	
Cisco VSG management IP address	
VSM management IP address	
Cisco VNMC instance IP address	
Mode for installing the Cisco VSG	• Standalone • HA primary • HA secondary • Manual installation
Cisco VSG VLAN number • Service (1) • Management (2) • High availability (HA) (3)	
Cisco VSG port profile name • Data (1) • Management (2) • High availability (HA) (3) **Note** The numbers indicate the VSG port profile that must be associated with the VSG VLAN number.	
HA pair ID (HA domain ID)	
Cisco VSG admin password	
Cisco VNMC admin password	
Cisco VSM admin password	
Shared secret password (Cisco VNMC, Cisco VSG policy agent, Cisco VSM policy agent)	

Tasks and Prerequisites Checklist

Tasks	Prerequisites
Task 1: Installing the Cisco VNMC from an ISO Image.	• Verify that the Hyper-V host on which to deploy the VNMC VM is available in SCVMM. • Copy the VNMC 2.1 ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose Library > Library Servers, right-click on the library location, and then refresh.
Task 2: On the VSM, Configuring the Cisco VNMC Policy Agent, on page 21	Make sure that you know the following: • The Cisco VNMC policy-agent image is available on the VSM (for example, vsmhv-pa.2.1.1a.bin) **Note** The string **vsmhv-pa** must appear in the image name as highlighted. • The IP address of the Cisco VNMC • The shared secret password you defined during the Cisco VNMC installation • That IP connectivity between the VSM and the Cisco VNMC is working **Note** If you upgrade your VSM, you must also copy the latest Cisco VSM policy agent image. This image is available in the Cisco VNMC image bundle to boot from a flash drive and to complete registration with the Cisco VNMC.
Task 3: On the VSM, Preparing Cisco VSG Port Profiles, on page 23	Make sure that you know the following: • The uplink port-profile name. • The VLAN ID for the Cisco VSG data interface (for example,100). • The VLAN ID for the Cisco VSG-ha interface (for example, 200). • The management VLAN (management). **Note** None of these VLANs need to be system VLANs.

Tasks	Prerequisites
Task 4: Installing the Cisco VSG from an ISO Image, on page 24	Make sure that you know the following: • Microsoft SCVMM SP1 is installed. • Download the Cisco VSG ISO image and upload it to the server (C:\ProgramData\Virtual Machine Manager Library Files\ISO). Refresh the library server under the Library tab. • The Cisco VSG-Data port profile: VSG-Data • The Cisco VSG-ha port profile: VSG-ha • The HA ID • The IP/subnet mask/gateway information for the Cisco VSG • The admin password • 2 GB RAM and 2 GB hard disk space are available • The Cisco VNMC IP address • The shared secret password • The IP connectivity between Cisco VSG and Cisco VNMC is okay. • The Cisco VSG VNM-PA image name (vsghv-pa.2.1.1a.bin) is available.
Task 5: On the VSG, Configuring the Cisco VNMC Policy Agent, on page 29	Make sure that you know the following: • The Cisco VNMC policy-agent image is available on the VSM (for example, vsmhv-pa.2.1.1a.bin) **Note** The string **vsmhv-pa** must appear in the image name as highlighted. • The IP address of the Cisco VNMC • The shared secret password you defined during the Cisco VNMC installation • That IP connectivity between the VSM and the Cisco VNMC is working **Note** If you upgrade your VSM, you must also copy the latest Cisco VSM policy agent image. This image is available in the Cisco VNMC image bundle to boot from a flash drive and to complete registration with the Cisco VNMC.

Tasks	Prerequisites
Task 6: On the Cisco VSG and Cisco VNMC, Verifying the VNM Policy-Agent Status, on page 30	—
Task 7: On the Cisco VNMC, Configuring a Tenant, Security Profile, and Compute Firewall, on page 32	Make sure that you know the following: • Adobe Flash Player (Version 10.1 or later) has been installed • The IP address of the Cisco VNMC • The admin user password
Task 8: On the Cisco VNMC, Assigning the Cisco VSG to the Compute Firewall, on page 38	—
Task 9: On the Cisco VNMC, Configuring a Permit-All Rule, on page 40	—
Task 10: On the Cisco VSG, Verifying the Permit-All Rule, on page 42	—
Task 11: Enabling Logging, on page 42	—
Task 12: Enabling the Traffic VM Port-Profile for Firewall Protection and Verifying the Communication Between the VSM, VEM, and VSG, on page 45	Make sure that you know the following: • The server virtual machine that runs with an access port profile (for example, web server) • The Cisco VSG data IP address (10.10.10.200) and VLAN ID (100) • The security profile name (for example, sp-web) • The organization (Org) name (for example, root/Tenant-A) • The port profile that you would like to edit to enable firewall protection • That one active port in the port-profile with vPath configuration has been set up
Task 13: Sending Traffic Flow and on the Cisco VSG Verifying Statistics and Logs, on page 48	—

Host Requirements

- Microsoft SCVMM SP1
- Microsoft Windows Server 2012

- 6 GB RAM

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/ps11208/index.html
The Cisco VNMC software is available for download at the following URL:

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

Task 1: Installing the Cisco VNMC from an ISO Image

Before You Begin

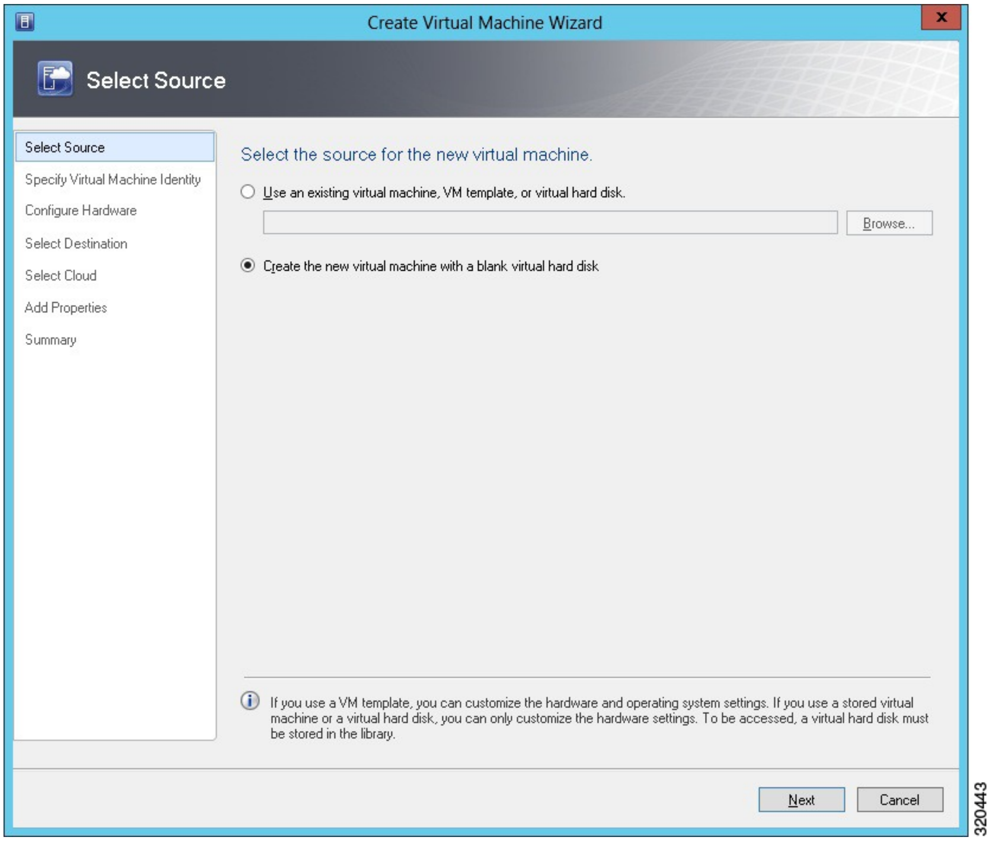
Know the following:

- Verify that the Hyper-V host on which to deploy the VNMC VM is available in SCVMM.

- Copy the VNMC 2.1 ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose **Library > Library Servers**, right-click on the library location, and then refresh.

Step 1 Launch the SCVMM.

Figure 6: Create Virtual Machine Wizard - Select Source



Select the source for the new virtual machine.

○ Use an existing virtual machine, VM template, or virtual hard disk.

● Create the new virtual machine with a blank virtual hard disk

If you use a VM template, you can customize the hardware and operating system settings. If you use a stored virtual machine or a virtual hard disk, you can only customize the hardware settings. To be accessed, a virtual hard disk must be stored in the library.

Step 2 Choose the Hyper-V host on which to deploy the VNMC VM.

Step 3 Right-click the Hyper-V host and choose **Create Virtual Machine**.

Step 4 In the Create Virtual Machine wizard, from the **Select Source** screen, select the **Create the new virtual machine with a blank virtual hard disk** radio button, then click **Next.**

Step 5 In the Specify Virtual Machine Identity screen, provide the required information, then click **Next.**

Step 6 In the **Configure Hardware** screen, do the following:

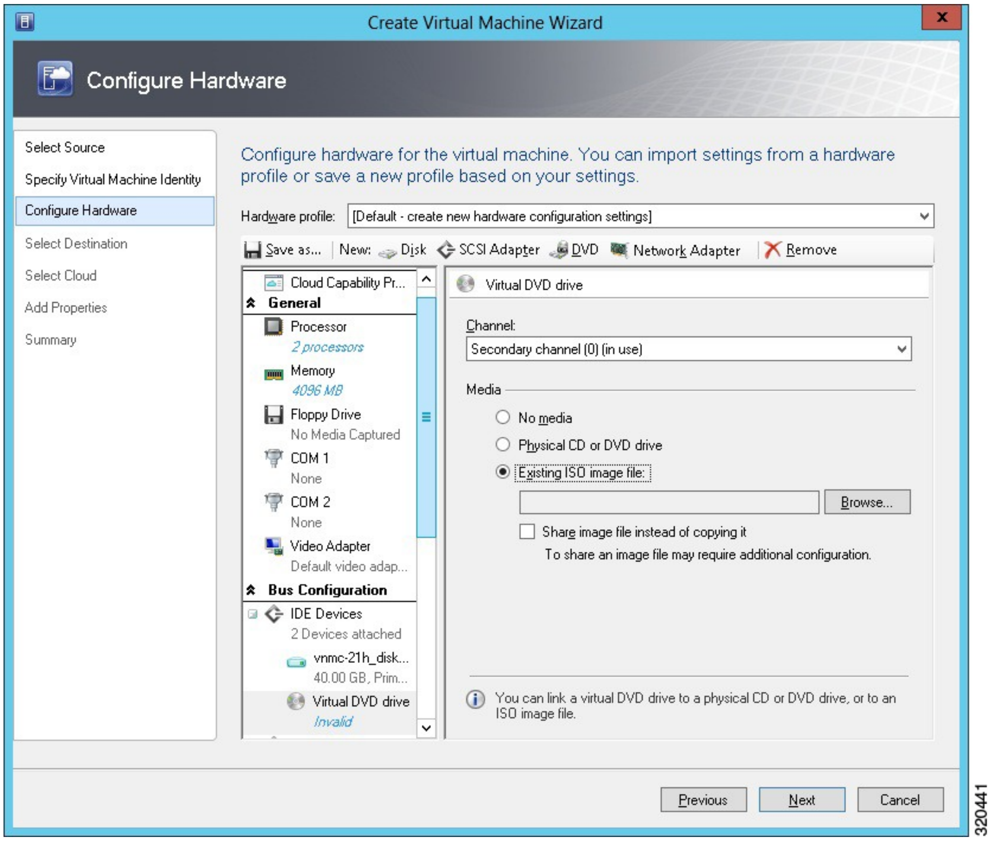
a) From General, do the following:

- Choose **Processor** and set the number of processors to two.
- Choose **Memory** and choose the required memory value. You will need minimum 4 GB memory.

b) From **Bus Configuration > IDE Devices**, do the following:

- Choose **Hard Disk**, enter the required size of the hard disk. You will need at least 20 GB.
- Choose **Virtual DVD Drive**, select the **Existing ISO image file** radio button, and browse to select the VNMC 2.1 ISO image file.

Figure 7: Create Virtual Machine Wizard - Configure Hardware



Create Virtual Machine Wizard

Configure Hardware

Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

Virtual DVD drive

Channel: Secondary channel (0) (in use)

Media

○ No media

○ Physical CD or DVD drive

● Existing ISO image file:

□ Share image file instead of copying it

To share an image file may require additional configuration.

You can link a virtual DVD drive to a physical CD or DVD drive, or to an ISO image file.

c) Choose **Network Adapters > Network Adapter 1**, select the **Connect to a VM Network** radio button, and browse to select a VM Network.

d) Click **Next.**

Step 7 In the **Select Destination** screen, do the following:

a) Select the **Place the virtual machine on a host** radio button.

b) Choose **All hosts** from the **Destination** drop-down list.

c) Click **Next.**

Step 8 In the **Select Host** screen, choose the destination, then click **Next.**

Step 9 In the **Configure Settings** screen, review the virtual machine settings, then click **Next.**

Step 10 In the **Add properties** screen, select the **Red Hat Enterprise Linux 5 (64 bit)** operating system, then click **Next.**

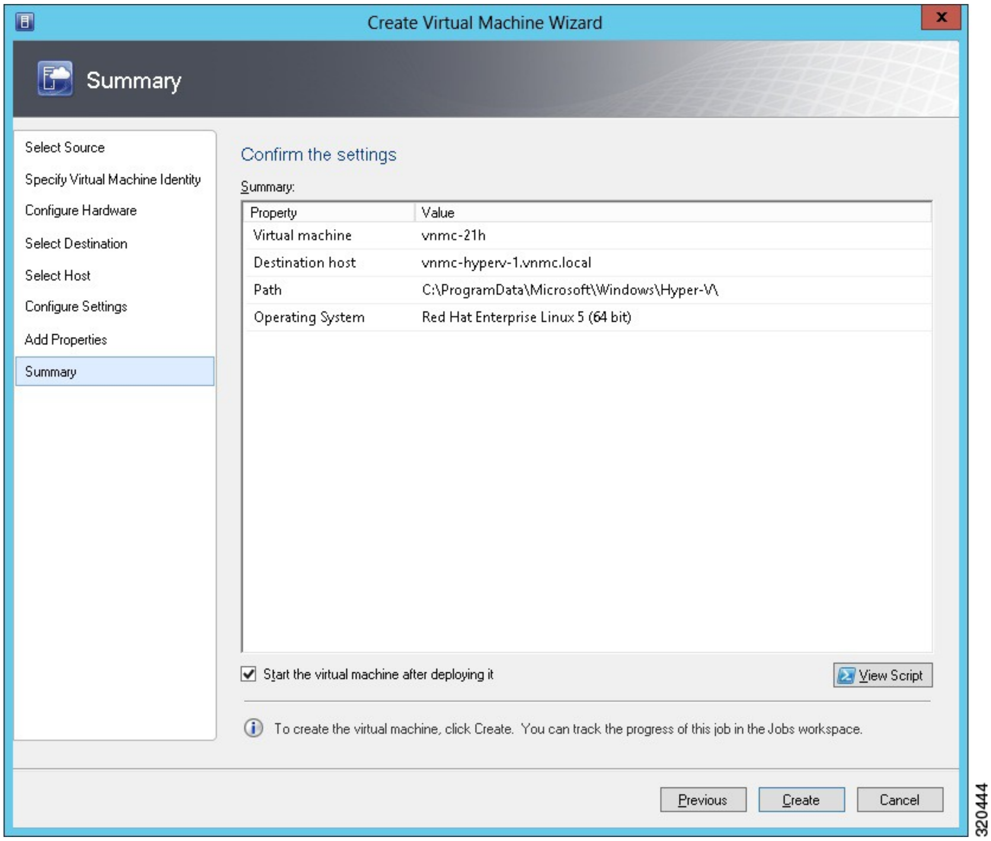
Step 11 In the **Summary** screen, do the following:

a) Verify the settings.

b) Check the **Start the virtual machine after deploying it** check box.

c) Click **Create.**

Figure 8: Create Virtual Machine Wizard - Summary



Confirm the settings

Summary:

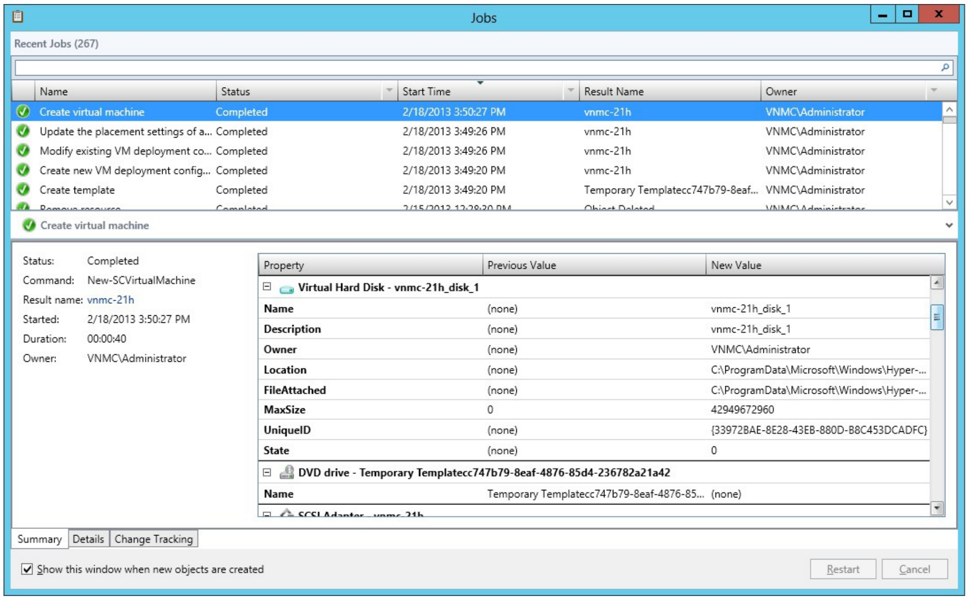
Property	Value
Virtual machine	vnmc-21h
Destination host	vnmc-hyperv-1.vnmc.local
Path	C:\ProgramData\Microsoft\Windows\Hyper-V\
Operating System	Red Hat Enterprise Linux 5 (64 bit)

☑ Start the virtual machine after deploying it

To create the virtual machine, click Create. You can track the progress of this job in the Jobs workspace.

The job Create virtual machine starts. You can see the status of this job in The Recent Jobs window. Ensure that the job completes without any errors.

Figure 9: Jobs Window



Name	Status	Start Time	Result Name	Owner
Create virtual machine	Completed	2/18/2013 3:50:27 PM	vnmc-21h	VNMC\Administrator
Update the placement settings of a...	Completed	2/18/2013 3:49:26 PM	vnmc-21h	VNMC\Administrator
Modify existing VM deployment co...	Completed	2/18/2013 3:49:26 PM	vnmc-21h	VNMC\Administrator
Create new VM deployment config...	Completed	2/18/2013 3:49:20 PM	vnmc-21h	VNMC\Administrator
Create template	Completed	2/18/2013 3:49:20 PM	Temporary Templatecc747b79-8eaf...	VNMC\Administrator
Remove resource	Completed	2/15/2013 12:28:30 PM	Object Deleted	VNMC\Administrator

Create virtual machine

Status: Completed
Command: New-SCVirtualMachine
Result name: vnmc-21h
Started: 2/18/2013 3:50:27 PM
Duration: 00:00:40
Owner: VNMC\Administrator

Property	Previous Value	New Value
Virtual Hard Disk - vnmc-21h_disk_1		
Name	(none)	vnmc-21h_disk_1
Description	(none)	vnmc-21h_disk_1
Owner	(none)	VNMC\Administrator
Location	(none)	C:\ProgramData\Microsoft\Windows\Hyper-...
FileAttached	(none)	C:\ProgramData\Microsoft\Windows\Hyper-...
MaxSize	0	42949672960
UniqueID	(none)	{33972BAE-8E28-43EB-880D-B8C453DCADFC}
State	(none)	0
DVD drive - Temporary Templatecc747b79-8eaf-4876-85d4-236782a21a42		
Name	Temporary Templatecc747b79-8eaf-4876-85...	(none)
SCSI Adapter - vnmc-21h		

Summary | Details | Change Tracking

☑ Show this window when new objects are created

Restart | Cancel

Step 12 After the virtual machine is successfully created, right-click the new Virtual Machine (vnmc21-perf in this case) and choose **Connect or View > Connect Via Console**.

Step 13 Launch the console and install VNMC

Note Before the final VNMC installation step, before you reboot, launch SCVMM again and right-click the Virtual machine (vnmc21-hyperv in this case) and choose **Properties > Hardware Configuration > Bus Configuration > Virtual DVD Drive > no media**, so that VNMC does not use the ISO image at boot time.

Step 14 After VNMC is successfully deployed, click **Close** and power on the VNMC VM.

Task 2: On the VSM, Configuring the Cisco VNMC Policy Agent

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

Before You Begin

Make sure that you know the following:

- The Cisco VNMC policy-agent image is available on the VSM (for example, vsmhv-pa.2.1.1a.bin)

Note The string **vsmhv-pa** must appear in the image name as highlighted.

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

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

Note VSM clock should be synchronized with the VNMC clock.

SUMMARY STEPS

1. On the VSM, enter the following commands:
2. Check the status of the VNM policy agent configuration to verify that you have installed the Cisco VNMC correctly and it is reachable by entering the **show vnm-pa status** command. This example shows that the Cisco VNMC is reachable and the installation is correct:

DETAILED STEPS

Step 1 On the VSM, enter the following commands:

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

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

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

The VSM is now registered with the Cisco VNMC.

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 3: On the VSM, Preparing Cisco VSG Port Profiles

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

Before You Begin

Make sure that you know the following:

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

Note None of these VLANs need to be system VLANs.

SUMMARY STEPS

1. 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.
2. Enter the configuration commands to set up an uplink port-profile.
3. Create the network segment and port-profile for the Data VLAN.
4. Create the network segment and port-profile for the HA VLAN.

DETAILED STEPS

Step 1 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 2 Enter the configuration commands to set up an uplink port-profile.

```
vsm(config)# nsm network logical vsm_LogicalNet
vsm(config-logical-net)# exit

vsm(config)# nsm network segment pool vsm_NetworkSite
vsm(config-net-seg-pool)# member-of network logical vsm_LogicalNet
vsm(config-net-seg-pool)# exit

vsm(config)# nsm ip pool template VM_IP_Pool
vsm(config-ip-pool-template)# ip-address 10.0.0.2 10.0.0.255
vsm(config-ip-pool-template)# netmask 255.255.255.0
vsm(config-ip-pool-template)# gateway 10.0.0.1
vsm(config-ip-pool-template)# exit

vsm(config)# nsm network uplink vsm_Uplink
vsm(config-uplink-net)# allow network segment pool vsm_NetworkSite
vsm(config-uplink-net)# publish uplink-network
vsm(config-uplink-net)# exit
```

Step 3 Create the network segment and port-profile for the Data VLAN.

```
vsm(config)# nsm network segment VMAccess_502
vsm(config-net-seg)# member-of network segment pool vsm_NetworkSite
vsm(config-net-seg)# switchport access vlan 502
vsm(config-net-seg)# import ip-pool-template VM_IP_Pool
vsm(config-net-seg)# publish network-segment
vsm(config-net-seg)# exit
vsm(config)# port-profile type vethernet VSG_Data
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# publish port-profile
vsm(config-port-prof)# exit
```

Step 4 Create the network segment and port-profile for the HA VLAN.

```
vsm(config)# nsm network segment VMAccess_503
vsm(config-net-seg)# member-of network segment pool vsm_NetworkSite
vsm(config-net-seg)# switchport access vlan 503
vsm(config-net-seg)# import ip-pool-template VM_IP_Pool
vsm(config-net-seg)# publish network-segment
vsm(config-net-seg)# exit
vsm(config)# port-profile type vethernet VSG_HA
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# publish port-profile
vsm(config-port-prof)# exit
```

Task 4: Installing the Cisco VSG from an ISO Image

Note Cisco VSG is supported as VSB on Nexus Cloud Services platform only.

Before You Begin

Make sure that you know the following:

- Microsoft SCVMM SP1 is installed.
- Download the Cisco VSG ISO image and upload it to the server (C:\ProgramData\Virtual Machine Manager Library Files\ISO). Refresh the library server under the Library tab.
- The Cisco VSG-Data port profile: VSG-Data
- The Cisco VSG-ha port profile: VSG-ha

- The HA ID
- The IP/subnet mask/gateway information for the Cisco VSG
- The admin password
- 2 GB RAM and 4 GB hard disk space are available
- The Cisco VNMC IP address
- The shared secret password
- The IP connectivity between Cisco VSG and Cisco VNMC is okay.
- The Cisco VSG VNM-PA image name (vsghv-pa.2.1.1a.bin) is available.

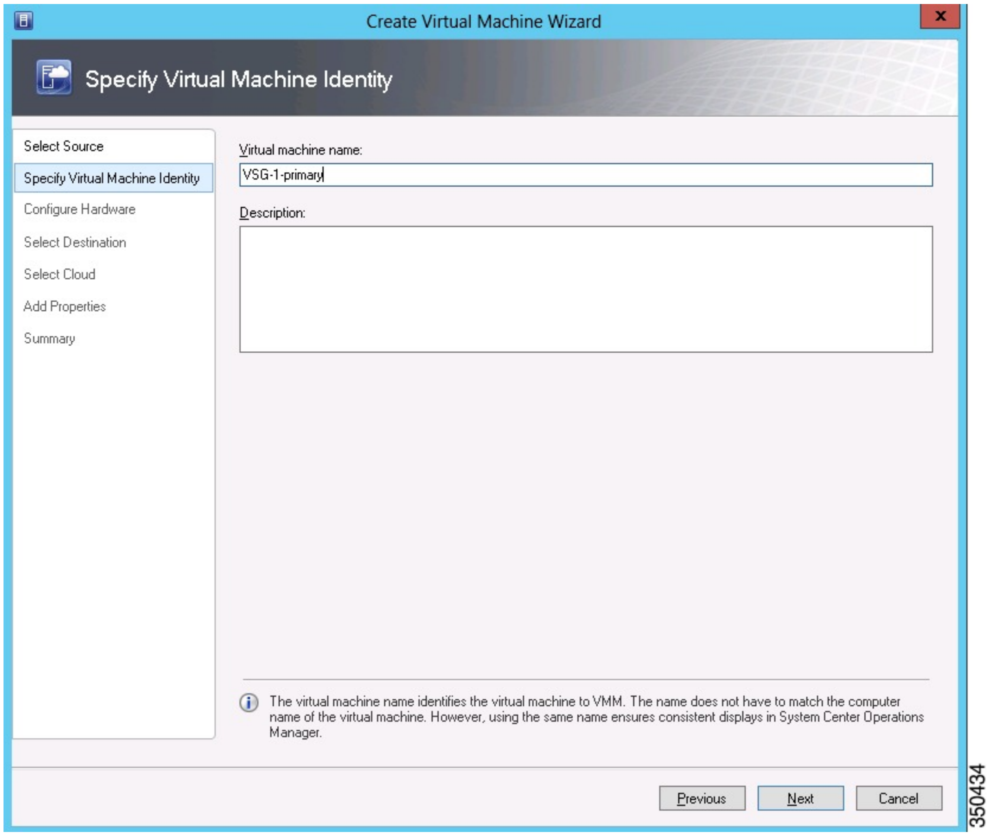
Step 1 Launch SCVMM.

Step 2 In the **VMs and Services** tab, click **Create Virtual Machine**.

Step 3 In the Create Virtual Machine Wizard, in the**Select Source** screen, check **Create the new virtual machine with a blank virtual hard disk** radio button and click **Next**.

Step 4 In the **Specify Virtual Machine Identity** screen, enter the name for the Cisco VSG in the **Virtual machine name** field and click **Next.**

Figure 10: Create Virtual Machine Wizard - Specify Virtual Machine Identity



Virtual machine name:
VSG-1-primary

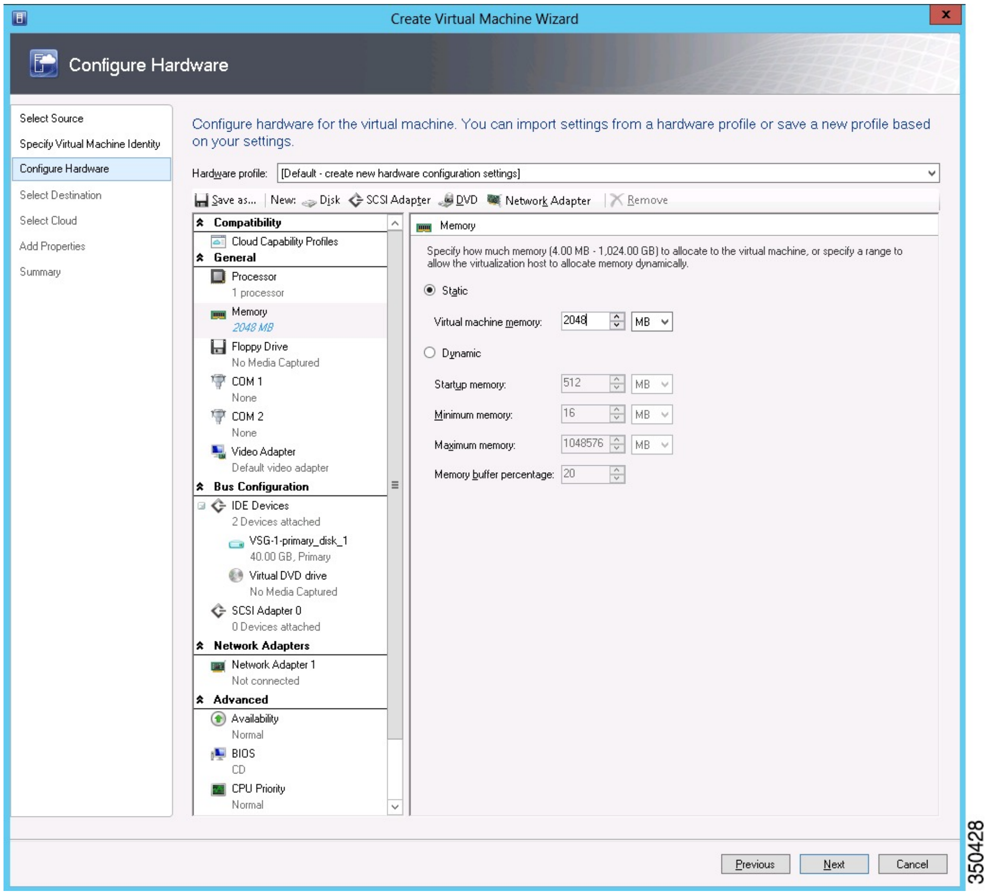
Description:

The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, using the same name ensures consistent displays in System Center Operations Manager.

Step 5 In the **Configure Hardware** section, do the following:

a) Under **General**, select **Memory**, select the **Static** option, and enter 2048 MB in the **Virtual machine memory** field.

Figure 11: Create Virtual Machine Wizard - Configure Hardware



Create Virtual Machine Wizard

Configure Hardware

Select Source
Specify Virtual Machine Identity
Configure Hardware
Select Destination
Select Cloud
Add Properties
Summary

Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

Save as... | New: Disk | SCSI Adapter | DVD | Network Adapter | Remove

Compatibility
- Cloud Capability Profiles

General
- Processor: 1 processor
- Memory: 2048 MB
- Floppy Drive: No Media Captured
- COM 1: None
- COM 2: None
- Video Adapter: Default video adapter

Bus Configuration
- IDE Devices: 2 Devices attached
  - VSG-1-primary_disk_1: 40.00 GB, Primary
  - Virtual DVD drive: No Media Captured
- SCSI Adapter 0: 0 Devices attached

Network Adapters
- Network Adapter 1: Not connected

Advanced
- Availability: Normal
- BIOS: CD
- CPU Priority: Normal

Memory

Specify how much memory (4.00 MB - 1,024.00 GB) to allocate to the virtual machine, or specify a range to allow the virtualization host to allocate memory dynamically.

● Static

Virtual machine memory: 2048 MB

○ Dynamic

Startup memory: 512 MB
Minimum memory: 16 MB
Maximum memory: 1048576 MB
Memory buffer percentage: 20

b) Under **Bus Configuration**, select the primary disk and enter 2 in the Size (GB) field.

c) Select the virtual DVD Drive, select **Existing ISO image file** radio button and browse for the VSG ISO within the SCVMM Library.

d) Select the **Network Adapter** drop-down near the top of the Create Virtual Machine Wizard and create two new Network Adapters (not Legacy).

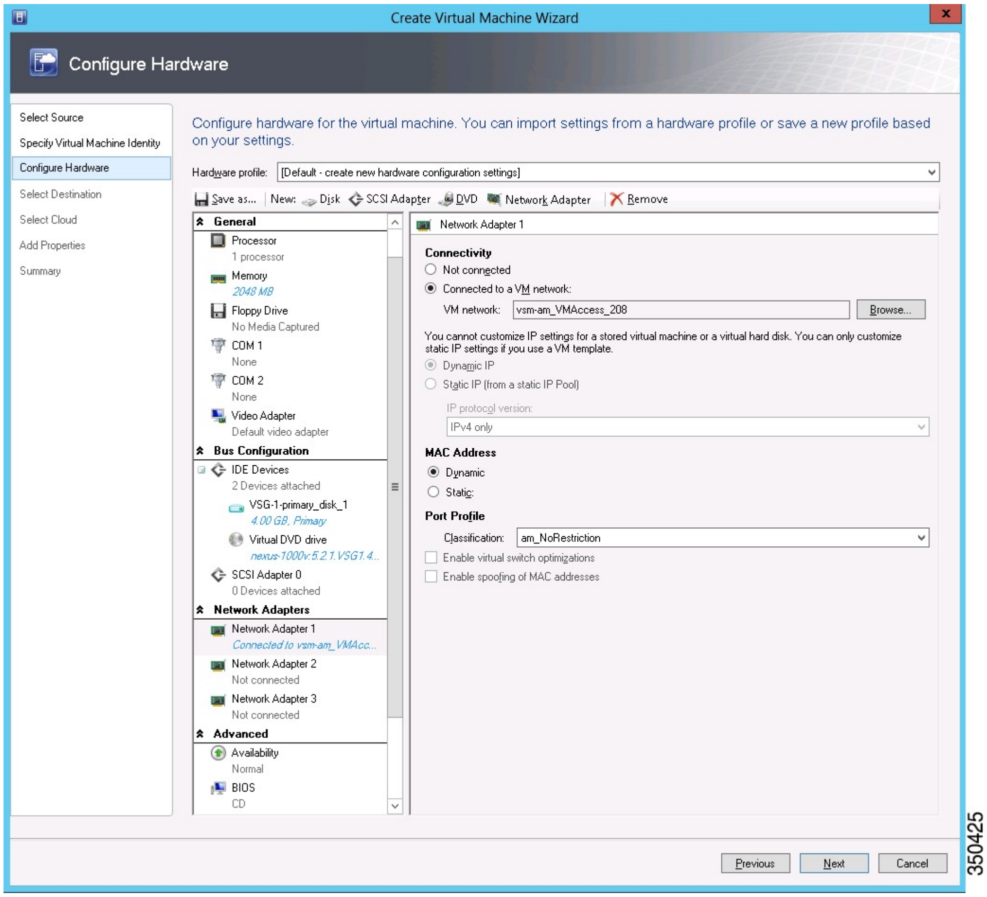
- Under the **Network Adapters** section, select **Network Adapter 1**, then select **Connected to a VM network** and browse for the appropriate network corresponding to the network segment for the VSG's data interface.

  Note Network Adapter 1 is Service/Data network, use it to connect to the Data network.

  Note Network Adapter 2 is the management network, connect it to the management network for the VSG.

Note Network Adapter 3 is the HA network, connect it to the HA network.

Figure 12: Create Virtual Machine Wizard - Configure Hardware



Create Virtual Machine Wizard

Configure Hardware

- Select Source
- Specify Virtual Machine Identity
- Configure Hardware
- Select Destination
- Select Cloud
- Add Properties
- Summary

Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

Save as... | New: Disk SCSI Adapter DVD Network Adapter | Remove

General
- Processor: 1 processor
- Memory: 2048 MB
- Floppy Drive: No Media Captured
- COM 1: None
- COM 2: None
- Video Adapter: Default video adapter

Bus Configuration
- IDE Devices: 2 Devices attached
  - VSG-1-primary_disk_1: 4.00 GB, Primary
  - Virtual DVD drive: nexus-1000v.5.2.1.VSG1.4...
- SCSI Adapter 0: 0 Devices attached

Network Adapters
- Network Adapter 1: Connected to vsm-am_VMAcc...
- Network Adapter 2: Not connected
- Network Adapter 3: Not connected

Advanced
- Availability: Normal
- BIOS: CD

Network Adapter 1

Connectivity
- ○ Not connected
- ● Connected to a VM network:

VM network: vsm-am_VMAccess_208 Browse...

You cannot customize IP settings for a stored virtual machine or a virtual hard disk. You can only customize static IP settings if you use a VM template.
- ● Dynamic IP
- ○ Static IP (from a static IP Pool)

IP protocol version: IPv4 only

MAC Address
- ● Dynamic
- ○ Static:

Port Profile

Classification: am_NoRestriction
- □ Enable virtual switch optimizations
- □ Enable spoofing of MAC addresses

Previous | Next | Cancel

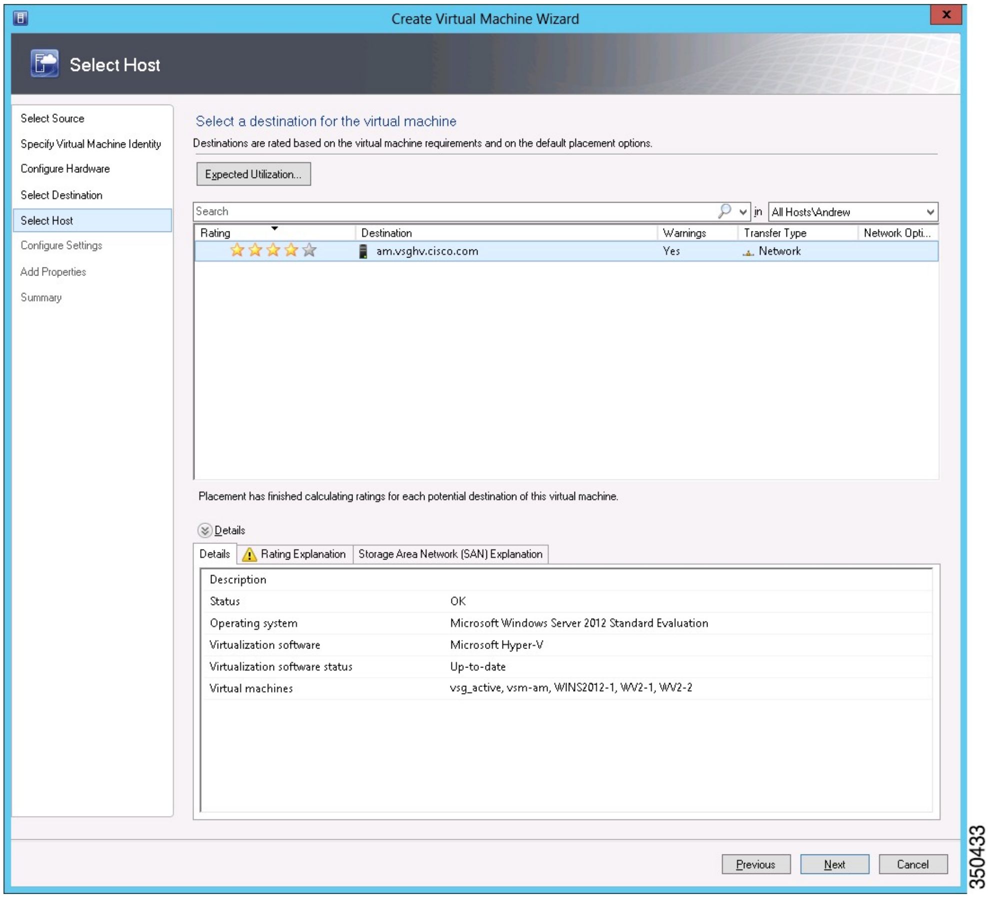
- From the **Classification** Drop-down, select the port-profile corresponding to the VSG's data interface.

Note Repeat the step d to create network adapters for service and HA.

Step 6 In the **Select Destination** section, choose **Place the virtual machine in a host** and select the host group on which you want to store the VSG from the drop-down and click **Next**.

Step 7 In the **Select Host** section, select the host you wish to place the VSG on and click **Next.**

Figure 13: Create Virtual Machine Wizard - Select Host



Select a destination for the virtual machine

Destinations are rated based on the virtual machine requirements and on the default placement options.

Rating	Destination	Warnings	Transfer Type	Network Opti...
★★★★☆	am.vsghv.cisco.com	Yes	Network	

Placement has finished calculating ratings for each potential destination of this virtual machine.

Description	
Status	OK
Operating system	Microsoft Windows Server 2012 Standard Evaluation
Virtualization software	Microsoft Hyper-V
Virtualization software status	Up-to-date
Virtual machines	vsg_active, vsm-am, WINS2012-1, WV2-1, WV2-2

Step 8 In the **Configure Settings** section, review the virtual machine settings to ensure they are correct and click **Next**.

Step 9 (Optional) In the **Add Properties** section, select **Other Linux (64-bit) from the Operating System** drop-down, then click **Next.**

Step 10 In the **Summary** section, click **Create.**

Step 11 Launch the Microsoft Hyper-V Manager on the server hosting the VSG.

Step 12 In the left pane, select the server that hosts the VSG instance you created.

Step 13 Under **Virtual Machines**, select the VSG you created.

Step 14 Under **Actions**, click **Settings** to open the **Settings** dialog-box.

Step 15 Select the first interface for the VSG instance and select **Advanced Features**.

Step 16 Under **MAC address**, select **Enable MAC address spoofing**.

Step 17 Click **OK**.

Step 18 Close the Microsoft Hyper-V Manager to return to the SCVMM interface.

Step 19 After MAC spoofing is configured and the VSG is successfully installed, select the VSG in the **VMs and Services** tab and click **Power On**.

Step 20 Connect to the VSG using **Connect or View -> Connect via Console**.

Task 5: On the VSG, Configuring the Cisco VNMC Policy Agent

Once the Cisco VNMC is installed, you must register the VSG with the Cisco VNMC.

Before You Begin

Make sure that you know the following:

- The Cisco VNMC policy-agent image is available on the VSG (for example, vsghv-pa.2.1.1a.bin)

Note The string **vsghv-pa** must appear in the image name as highlighted.

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

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

Note VSG clock should be synchronized with the VNMC clock.

SUMMARY STEPS

1. On the VSG, enter the following commands:
2. Check the status of the VNM policy agent configuration to verify that you have installed the Cisco VNMC correctly and it is reachable by entering the **show vnm-pa status** command. This example shows that the Cisco VNMC is reachable and the installation is correct:

DETAILED STEPS

Step 1 On the VSG, enter the following commands:

```
vsg# configure terminal
vsg(config)# vnm-policy-agent
vsg(config-vnm-policy-agent)# registration-ip 10.193.75.95
vsg(config-vnm-policy-agent)# shared-secret Example_Secret123
vsg(config-vnm-policy-agent)# policy-agent-image vsghv-pa.2.1.1a.bin
vsg(config-vnm-policy-agent)# exit
vsg(config)# copy running-config startup-config
vsg(config)# exit
```

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

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

The VSG is now registered with the Cisco VNMC.

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

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

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

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

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 policy-agent successfully).

SUMMARY STEPS

1. Log in to the Cisco VSG.
2. Check the status of VNM-PA configuration by entering the following command:
3. Log in to the Cisco VNMC. The **VNMC Administration on Service Registry** window opens.
4. Choose **Administration** > **Service Registry** > **Clients** > **General**.
5. In the **Client** pane of the **VNMC Administration Service Registry** window, verify that the Cisco VSG and VSM information is listed.

DETAILED STEPS

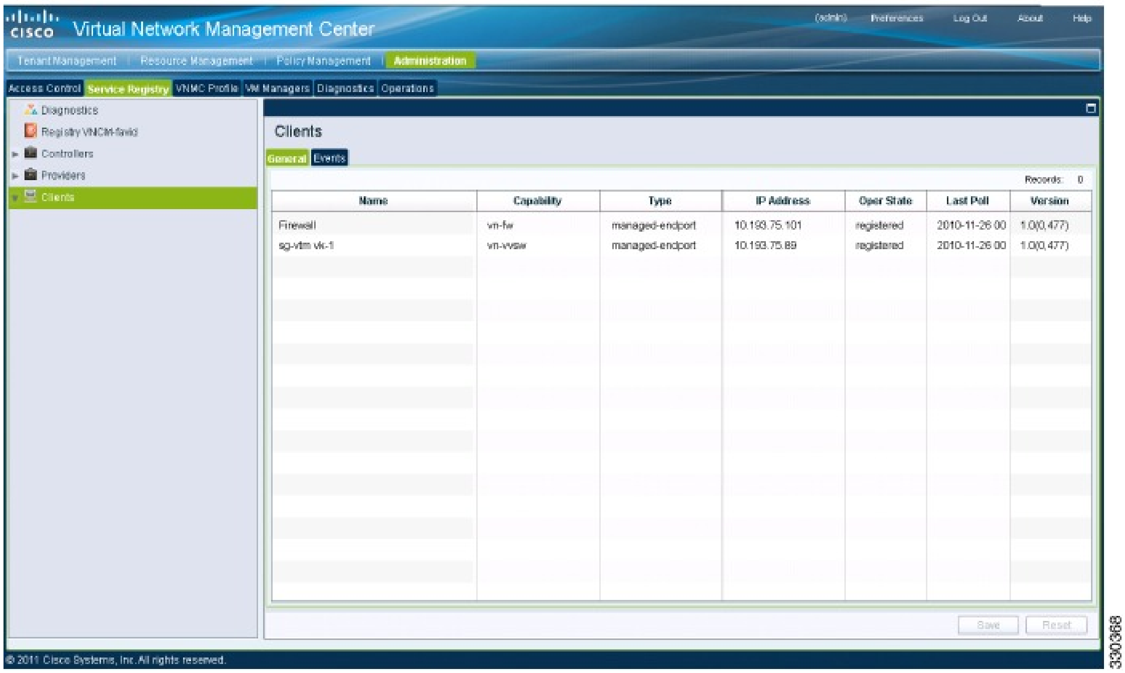
Step 1 Log in to the Cisco VSG.

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

```
vsg# show vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 2.0(1a)-vsg
vsg#
```

Step 3 Log in to the Cisco VNMC. The **VNMC Administration on Service Registry** window opens.

Figure 14: VNMC Administration Service Registry Window



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

Step 4 Choose **Administration** > **Service Registry** > **Clients** > **General**.

Step 5 In the **Client** pane of the **VNMC Administration Service Registry** window, 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, you should configure some of the basic security profiles and policies.

This task includes the following subtasks:

- Verifying Cisco VSG and VSM Registration in VNMC
- Configuring a Tenant on the Cisco VNMC, on page 32
- Configuring a Security Profile on the Cisco VNMC, on page 34
- Configuring a Compute Firewall on the Cisco VNMC, on page 35

What to Do Next

Go to Configuring a Tenant on the Cisco VNMC, on page 32

Configuring a Tenant on the Cisco VNMC

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

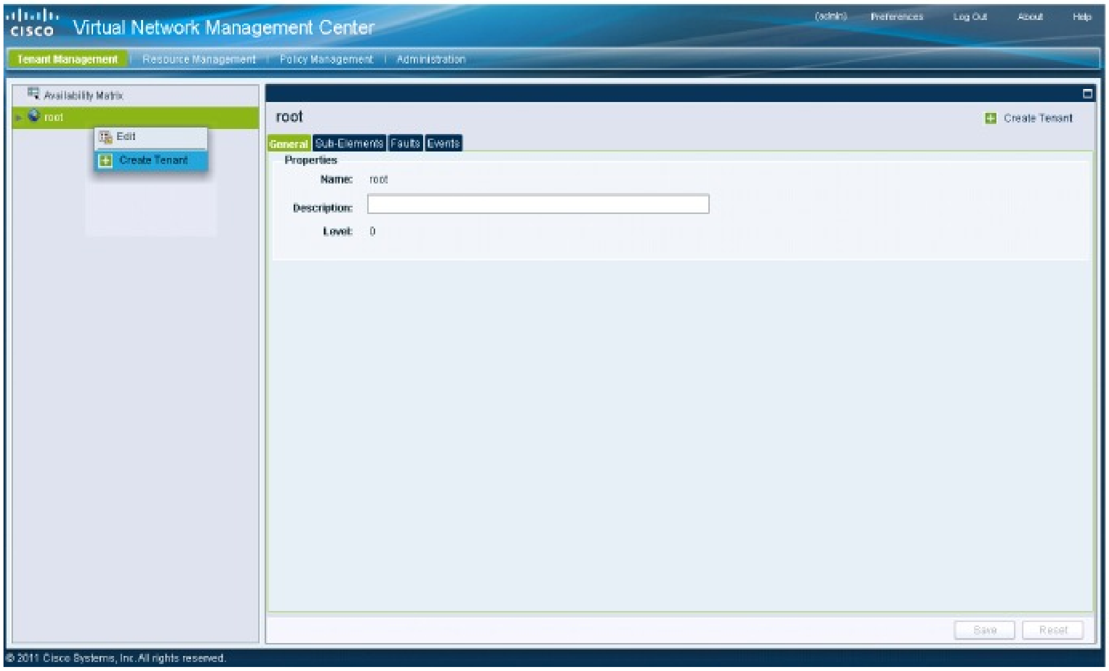
SUMMARY STEPS

1. From the Cisco VNMC toolbar, click the **Tenant Management** tab.
2. In the Navigation pane directory tree, right-click on **root**, and from the drop-down list, choose **Create Tenant**.
3. In the **root** pane, click the **General** tab and do the following:
4. Click **OK**.

DETAILED STEPS

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

Figure 15: VNMC Window Tenant Management Tab root Pane



Properties

Name: root

Description:

Level: 0

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

Step 3 In the **root** pane, click the **General** tab and 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 listed in the left-side pane under root.

What to Do Next

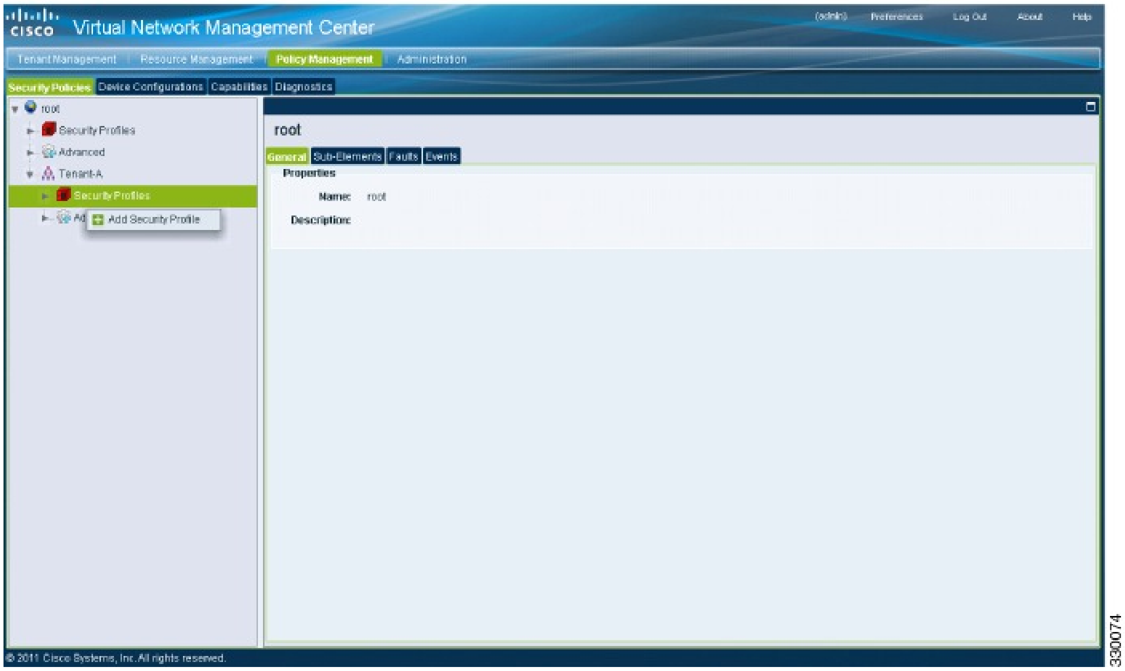
Go to Configuring a Security Profile on the Cisco VNMC, on page 34

Configuring a Security Profile on the Cisco VNMC

You can configure a security profile on the Cisco VNMC.

Step 1 Click the **Policy Management** tab in the Cisco VNMC toolbar. The **Policy Management** window opens.

Figure 16: Security Policies root Window



Name: root

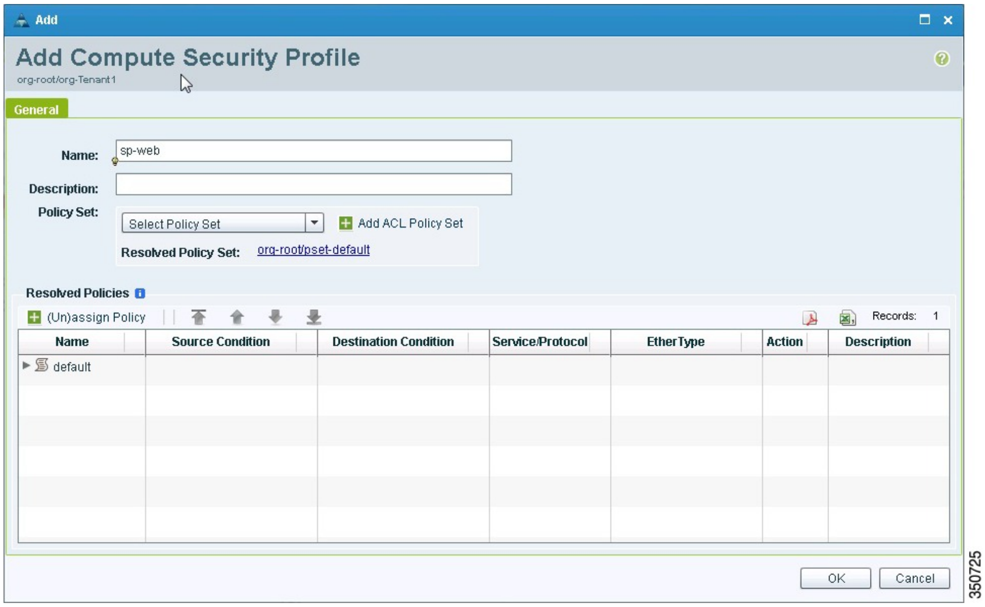
Description:

Step 2 In the **Policy Management Security Policies** window, from the directory path, choose **Security Policies** > **root** > **Tenant-A** > **Security Profiles**.

Step 3 Right click in an empty space and choose **Add Security Profile** from the drop-down list.

The **Add Security Profile** dialog box opens.

Figure 17: Add Compute Security Profile Dialog Box



Add Compute Security Profile
org-root/org-Tenant1

Name: sp-web
Description:
Policy Set: Select Policy Set
Resolved Policy Set: org-root/pset-default

Resolved Policies

Records: 1

Name	Source Condition	Destination Condition	Service/Protocol	EtherType	Action	Description
▶ default						

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

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

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

Step 5 Click **OK**

What to Do Next

Go to Configuring a Compute Firewall on the Cisco VNMC, on page 35

Configuring a Compute Firewall on the Cisco VNMC

The compute firewall is a logical virtual entity that contains the device profile that you can bind (assign) to a Cisco VSG VM. 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.

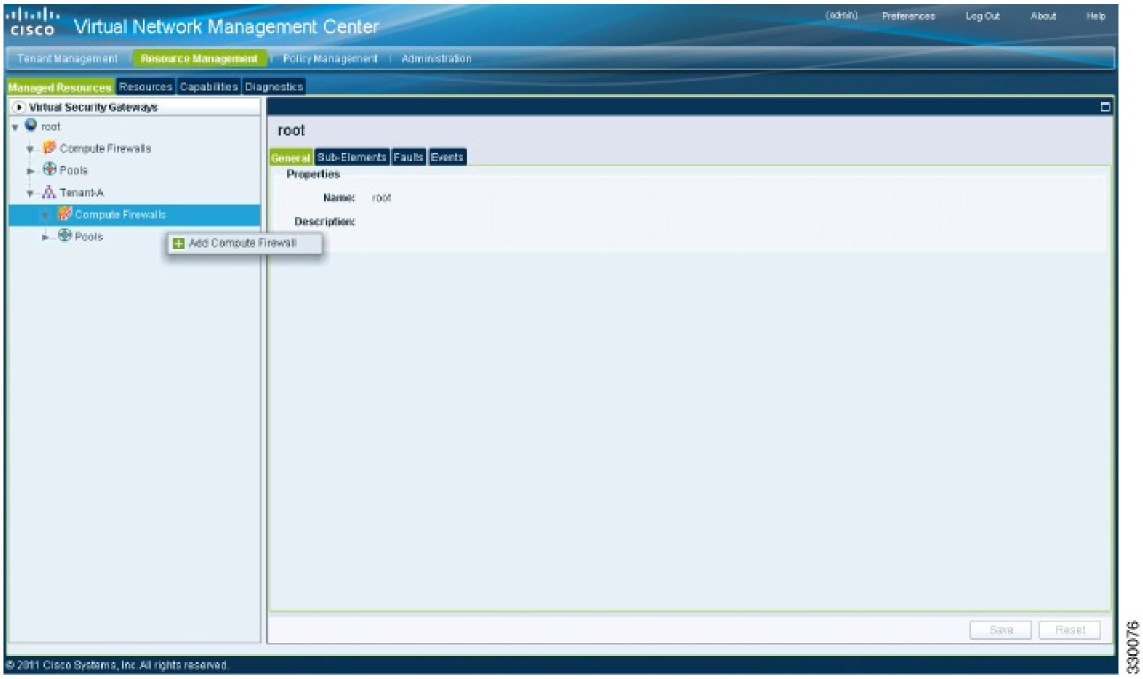
SUMMARY STEPS

1. From the Cisco VNMC, choose **Resource Management** > **Managed Resources**.
2. On the left-pane directory tree, choose **root** > **Tenant-A** > **Compute Firewall**.
3. From the drop-down list, choose **Add Compute Firewall**. The **Add Compute Firewall** dialog box opens.
4. In the **Add Compute Firewall** dialog box, do the following:
5. Click **OK**.

DETAILED STEPS

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

Figure 18: VNMC Resource Management, Managed Resources, Firewall Profiles Window



Properties

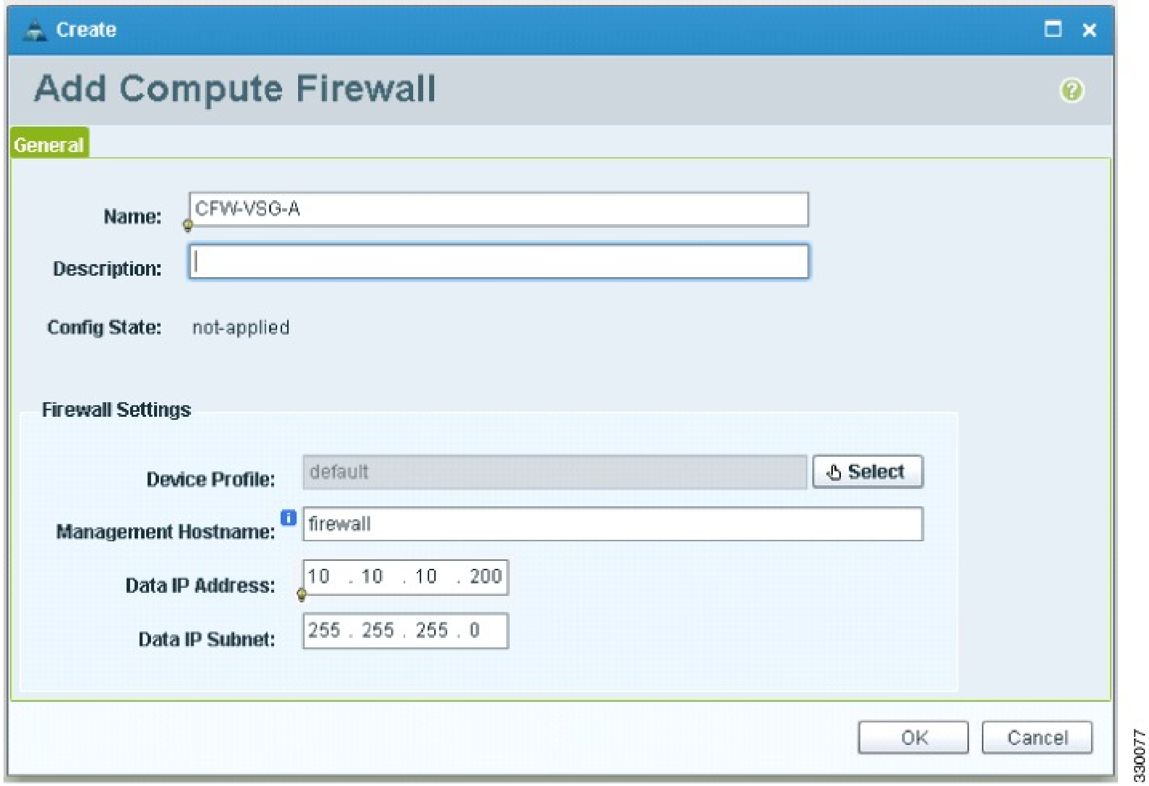
Name: root

Description:

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

Step 3 From the drop-down list, choose **Add Compute Firewall**. The **Add Compute Firewall** dialog box opens.

Figure 19: Add Compute Firewall Dialog Box



Add Compute Firewall

Name: CFW-VSG-A

Description:

Config State: not-applied

Firewall Settings

Device Profile: default [Select]

Management Hostname: firewall

Data IP Address: 10 . 10 . 10 . 200

Data IP Subnet: 255 . 255 . 255 . 0

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

a) In the **Name** field, enter a name for the compute firewall.
b) In the **Description** field, enter a brief description of the compute firewall.
c) In the **Management Hostname** field, enter the name for your Cisco VSG.
d) In the **Data IP Address** field, enter the data IP address.

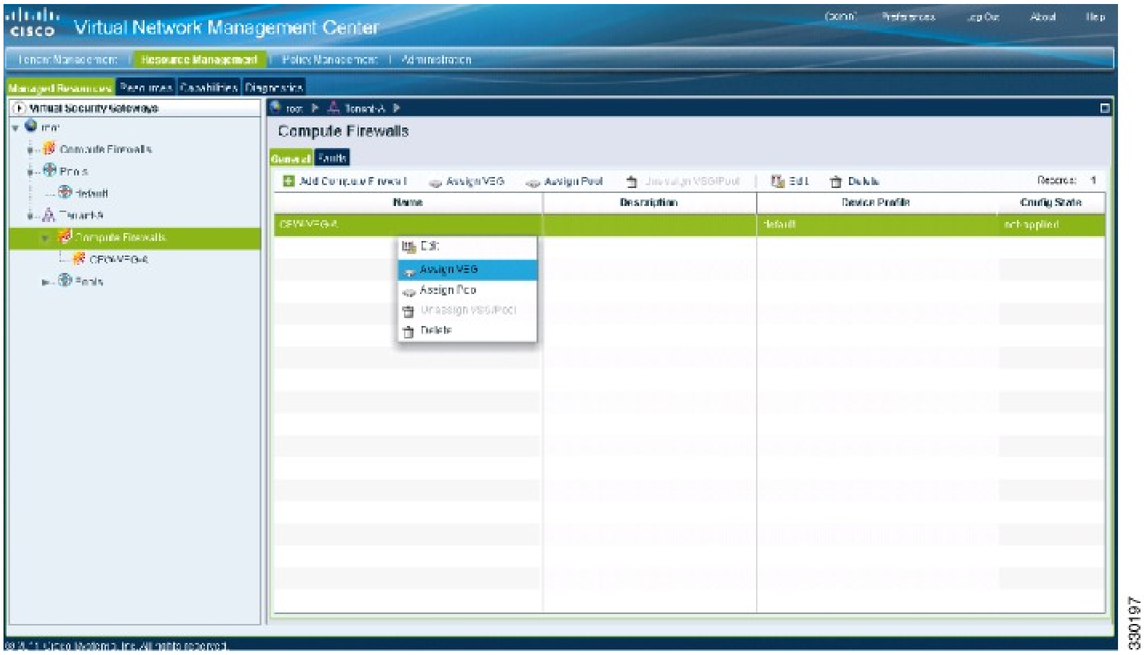
Step 5 Click **OK**.
The new Compute Firewall pane displays with the information that you provided.

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

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

Step 1 Choose **Resource Management** > **Managed Resources** > **Tenant-A** > **Compute Firewalls**.

Figure 20: VNMC Resource Management Resources Compute Firewalls Window

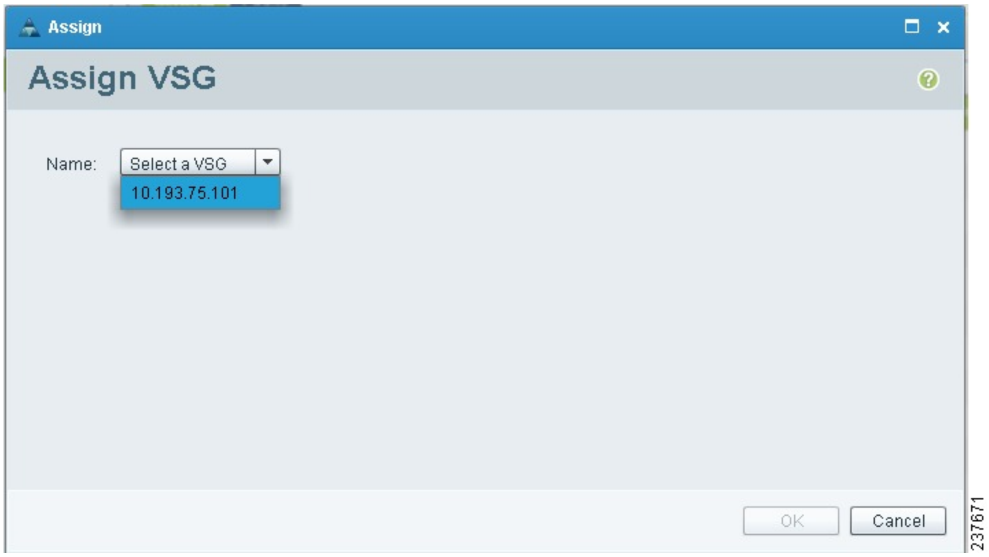


Name	Description	Device Profile	Config State
CFW-VSG-A		default	not applied

Step 2 Right-click in the **Compute Firewalls** pane and choose **Assign VSG** from the drop-down list.

The **Assign VSG** dialog box opens.

Figure 21: Assign VSG Dialog Box



Step 3 From the **Name** drop-down list, choose the Cisco VSG IP address.

Step 4 Click **OK**.

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

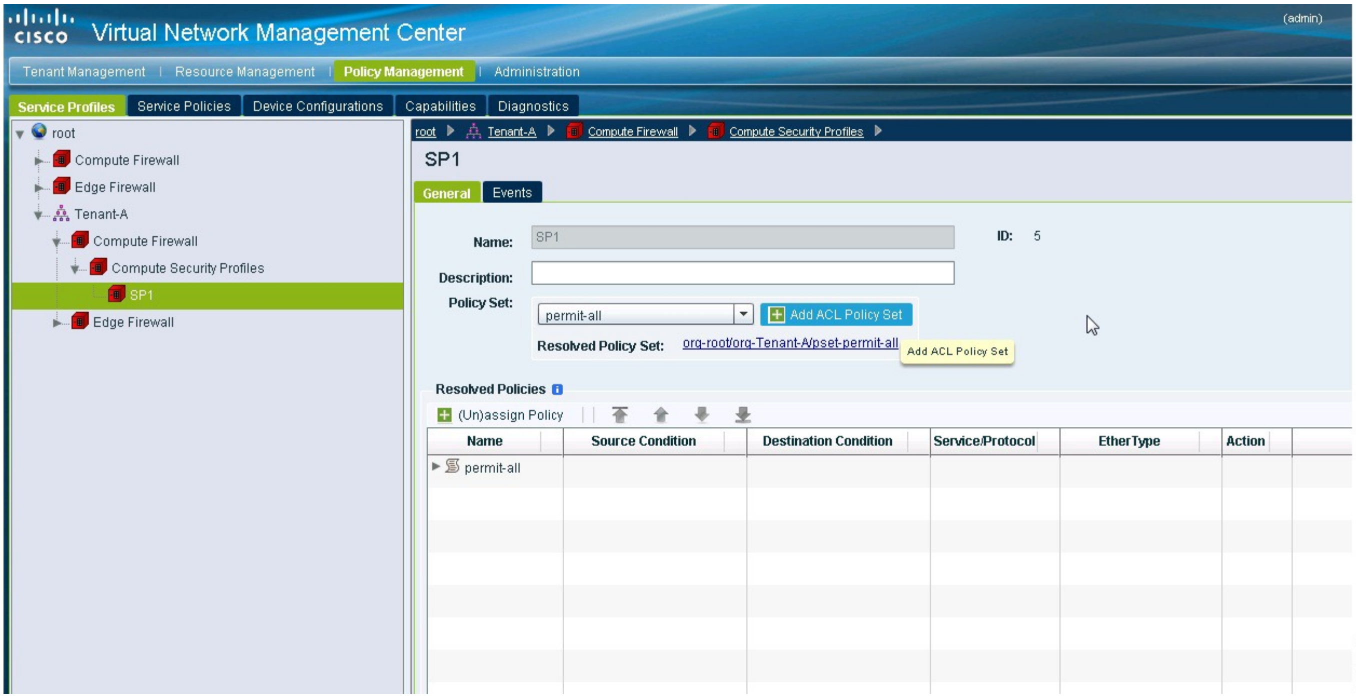
Task 9: On the Cisco VNMC, Configuring a Permit-All Rule

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

Step 1 Log in to the Cisco VNMC.

Step 2 Choose **Policy Management** > **Service Profiles**. The **Cisco VNMC Policy Management Security Policies** window opens.

Figure 22: Cisco VNMC Policy Management Security Policies Window


Virtual Network Management Center
(admin)
Tenant Management | Resource Management | Policy Management | Administration
Service Profiles | Service Policies | Device Configurations | Capabilities | Diagnostics
root
Compute Firewall
Edge Firewall
Tenant-A
Compute Firewall
Compute Security Profiles
SP1
Edge Firewall
root ▶ Tenant-A ▶ Compute Firewall ▶ Compute Security Profiles ▶
SP1
General | Events
Name: SP1
ID: 5
Description:
Policy Set: permit-all
Add ACL Policy Set
Resolved Policy Set: org-root/org-Tenant-A/pset-permit-all
Add ACL Policy Set
Resolved Policies
(Un)assign Policy
Name | Source Condition | Destination Condition | Service/Protocol | EtherType | Action
permit-all
350727

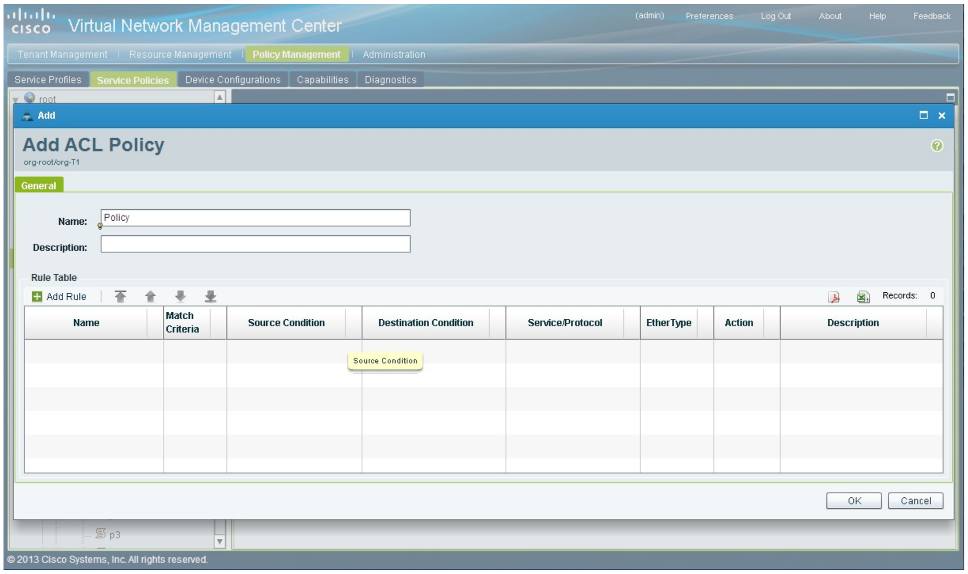
Step 3 In the **Cisco VNMC Policy Management Security Policies**, window do the following:

a) Choose **root** > **Tenant-A** > **Compute Firewall** > **Compute Security Profiles** > **sp-web**.

b) In the right pane, click **Add ACL Policy Set**.

Step 4 Click **Add Policy**. The **Add Policy** dialog box opens.

Figure 23: Add Policy Dialog Box



Add ACL Policy
org-root/org-T1

Name: Policy
Description:

Rule Table

Records: 0

Name	Match Criteria	Source Condition	Destination Condition	Service/Protocol	EtherType	Action	Description

Step 5 In the **Add Policy** dialog box, do the following:

a) In the **Name** field, enter the ACL Policy Set name.
b) In the **Description** field, enter a brief description of the ACL Policy Set.
c) Above the **Name** column, click **Add Rule**.
d) Click **Add ACL Policy**.

Step 6 In the **Add Rule dialog** box, do the following:

a) In the **Name** field, enter the rule name.
b) In the **Action** radio button, select the matching condition (for example, Permit-All to permit all the traffic).
c) In the **Condition Match Criteria** field, select the required condition.
d) In the **Source - Destination - Service** tab, click **Add** to add source/destination conditions or service.
e) In the **Protocol** tab, uncheck **Any** to select specific protocols. Do not uncheck **Any** if you wish to match all the protocols.
f) In the **Ether-Type** tab, click **Add** to specify an ethertype for the rule.
g) In the **Time Range** tab, keep the default option to leave the rule enabled.
h) In the **Advanced** tab, click **Add** to add checks for source ports.
i) Click **Ok**.

Step 7 In the **Add Policy** dialog box, click **OK**.
The newly created policy is displayed in the **Assigned** field.

Step 8 In the **Add Policy Set** dialog box, click **OK**.

Step 9 In the **Service Profile** window, click **Save**.

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

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

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

Task 11: Enabling Logging

To enable logging follow these procedures:

- Enabling Logging level 6 for Policy-Engine Logging, on page 42
- Enabling Global Policy-Engine Logging, on page 44

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.

Step 1 Log in to the Cisco VNMC.

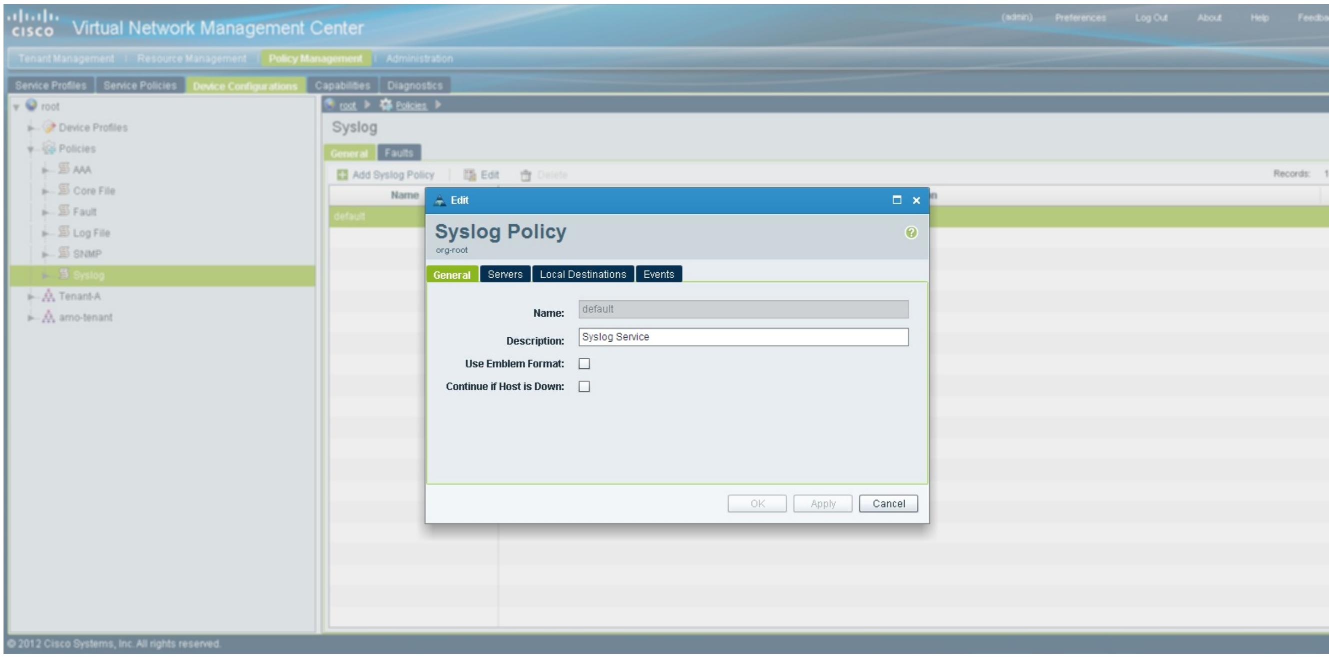
Step 2 Choose **Policy Management** > **Device Configurations**.

Step 3 In the **Device Configuration** window, do the following:

a) In the **Navigation** pane, choose **root** > **Policies** > **Syslog**.

b) In the **Work** pane, choose **Default** and click **Edit**.
The **Edit (default)** dialog box opens.

Figure 24: Cisco Virtual Network Center - Edit Syslog Policy



Syslog Policy
org-root

Name: default

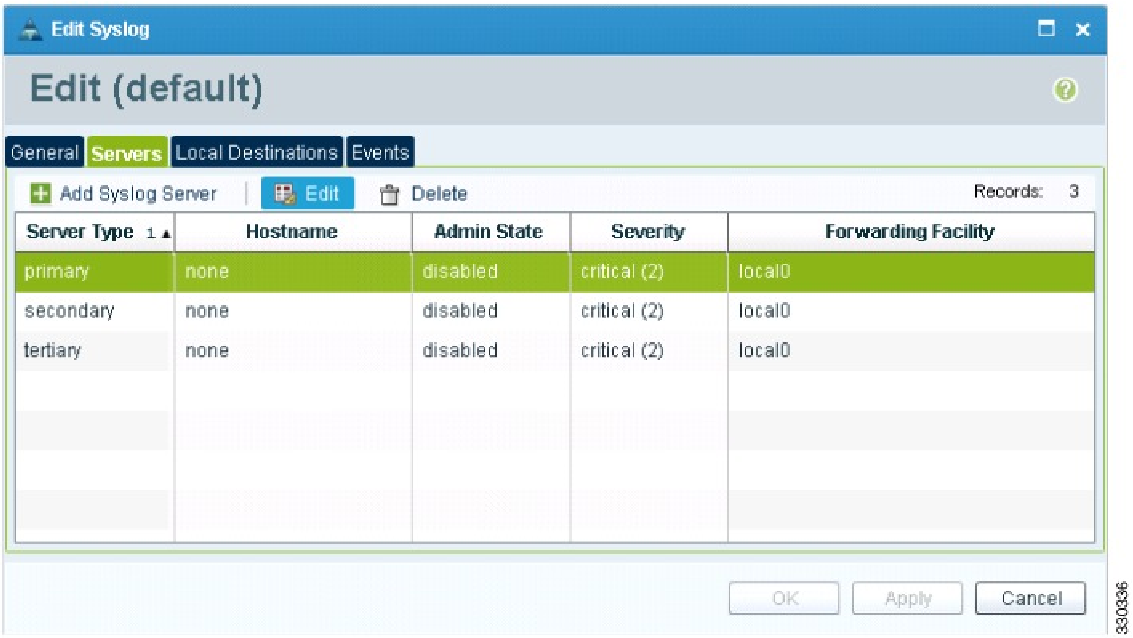
Description: Syslog Service

Use Emblem Format: □

Continue if Host is Down: □

Step 4 In the **Edit Syslog** dialog box, do the following:

Figure 25: Edit Syslog Dialog Box



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

a) Click the **Servers** tab.

b) From the **Server Type** column, choose the **primary** server type from the displayed list.

c) From the pane toolbar, click **Edit.**

Step 5 In the **Edit (Primary) Syslog Server** dialog box, do the following:

a) In the **Hostname/IP address** field, enter the syslog server IP address.

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

c) From the **Admin State** drop-down list, check **Enabled** radio button.

d) Click **OK**.

Step 6 Click **OK**.

What to Do Next

Go to Enabling Global Policy-Engine Logging, on page 44.

Enabling Global Policy-Engine Logging

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

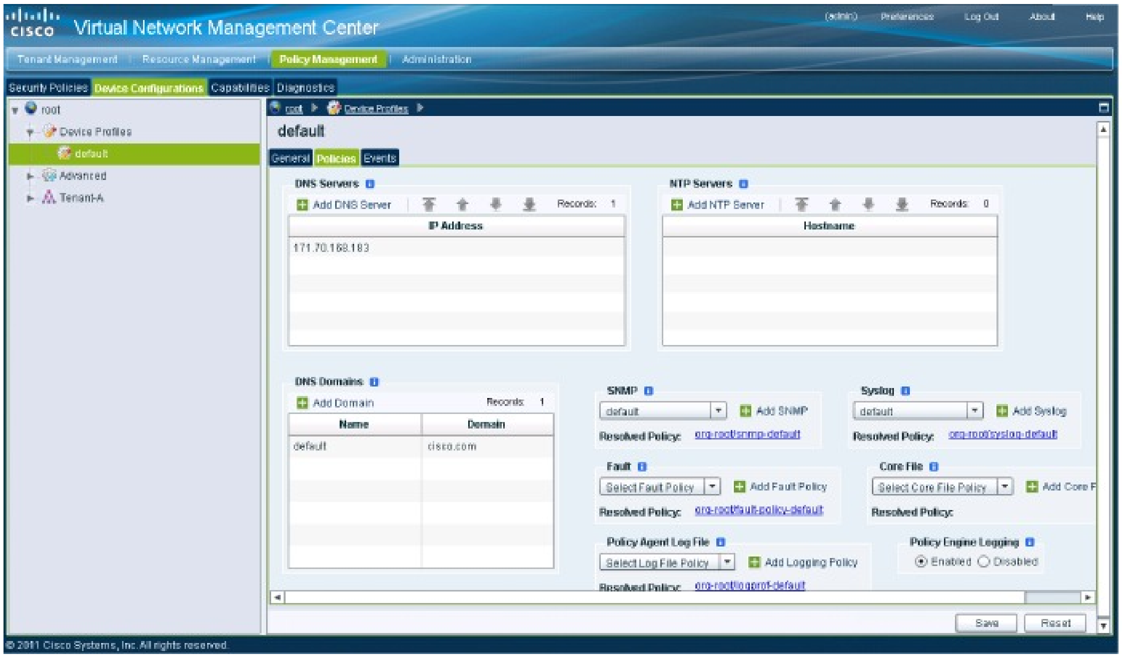
SUMMARY STEPS

1. Log in to the Cisco VNMC.
2. In the **Virtual Network Management Control** window, choose **Policy Management** > **Device Configurations** > **Device Configurations** > **root** > **Device Profiles** > **default**. The **default** Device Profile window opens.
3. In the **default** window, do the following:
4. Click **Save**.

DETAILED STEPS

Step 1 Log in to the Cisco VNMC.

Figure 26: Cisco Virtual Management Center Policy management Device Configuration Profiles Pane



IP Address
171.70.168.183

Name	Domain
default	cisco.com

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

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

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

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

Policy Engine Logging: ● Enabled ○ Disabled

Step 2 In the **Virtual Network Management Control** window, choose **Policy Management** > **Device Configurations** > **Device Configurations** > **root** > **Device Profiles** > **default**. The **default** Device Profile window opens.

Step 3 In the **default** window, do the following:

a) In the **Work** pane, click the **Policies** tab.

b) At the bottom of the **Work** pane, under the **Policy Engine Logging** field, click **Enabled**.

Step 4 Click **Save**.

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

This section includes the following topics:

- Enabling Traffic VM Port-Profile for Firewall Protection , on page 46
- Verifying the VSM or VEM for Cisco VSG Reachability, on page 47

- Checking the VM Virtual Ethernet Port for Firewall Protection, on page 47

Before You Begin

Make sure that you know the following:

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

Enabling Traffic VM Port-Profile for Firewall Protection

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

SUMMARY STEPS

1. Enabling Traffic VM Port-Profile for Firewall Protection.

DETAILED STEPS

Enabling Traffic VM Port-Profile for Firewall Protection.

```
vsm(config)# nsm network segment VMAccess_400
vsm(config-net-seg)# member-of network segment pool vsm_NetworkSite
vsm(config-net-seg)# switchport access vlan 400
vsm(config-net-seg)# import ip-pool-template VM_IP_Pool
vsm(config-net-seg)# publish network-segment
vsm(config-net-seg)# exit

vsm(config)# port-profile type vethernet pp-webserver
vsm(config-port-prof)# org root/Tenant-A
vsm(config-port-prof)# vservice node VSG profile sp-web
vsm(config-port-prof)# no shutdown
vsm(config-port-prof)# state enabled
vsm(config-port-prof)# publish port-profile
vsm(config-port-prof)# exit
vsm(config)# show port-profile pp-webserver
```

What to Do Next

Go to Verifying the VSM or VEM for Cisco VSG Reachability, on page 47.

Verifying the VSM or VEM for Cisco VSG Reachability

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

```
vsm# show vservice brief
--------------------------------------------------------------------------------
                                   License Information
--------------------------------------------------------------------------------
Type      In-Use-Lic-Count  UnLicensed-Mod
vsg                      4
asa                      0

--------------------------------------------------------------------------------
                                   Node Information
--------------------------------------------------------------------------------
 ID Name                         Type   IP-Address      Mode   State   Module
  1 VSG_Root                     vsg    10.1.0.150      l3     Alive   4,5,

--------------------------------------------------------------------------------
                                   Path Information
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
                                   Port Information
--------------------------------------------------------------------------------

PortProfile:veth-10
Org:root/Tenant-1/VDC-1/App-1/Tier-1
Node:VSG-Root(10.1.0.150)         Profile(Id):SP100(22)
Veth Mod VM-Name
6     5  vm-ub-20
7     4  vm-ub-10
```

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

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

Checking the VM Virtual Ethernet Port for Firewall Protection

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

```
VSM(config)# show vservice port brief vethernet 10
--------------------------------------------------------------------------------
                                   Port Information
--------------------------------------------------------------------------------
PortProfile:veth-10
Org:root/Tenant-1/VDC-1/App-1/Tier-1
Node:VSG-Root(10.1.0.150)                        Profile(Id):SP100(22)
Veth   Mod   VM-Name
 6     5     vm-ub-20
 7     4     vm-ub-10
```

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

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

This section includes the following topics:

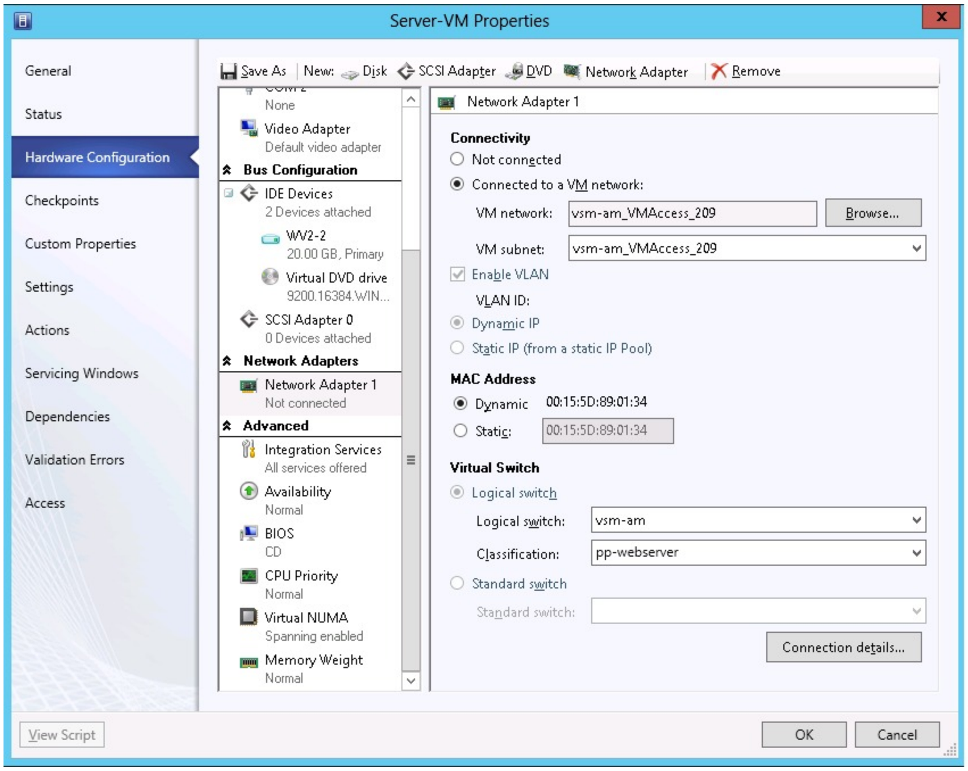
- Sending Traffic Flow, on page 48
- Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 49

Sending Traffic Flow

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

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

Figure 27: Virtual Machine Properties Window



Server-VM Properties

Network Adapter 1

Connectivity
○ Not connected
● Connected to a VM network:
VM network: vsm-am_VMAccess_209
VM subnet: vsm-am_VMAccess_209
☑ Enable VLAN
VLAN ID:
○ Dynamic IP
○ Static IP (from a static IP Pool)

MAC Address
● Dynamic 00:15:5D:89:01:34
○ Static: 00:15:5D:89:01:34

Virtual Switch
● Logical switch
Logical switch: vsm-am
Classification: pp-webserver
○ Standard switch
Standard switch:

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

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

b) Send traffic (for example, HTTP) to your Server-VM.

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

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

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

[root]#
```

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

What to Do Next

Go to Verifying Policy-Engine Statistics and Logs on the Cisco VSG, on page 49.

Verifying Policy-Engine Statistics and Logs on the Cisco VSG

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

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

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

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

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

CHAPTER 3

Installing the Cisco VNMC

This chapter contains the following sections:

Information About the Cisco VNMC

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

Installation Requirements

Cisco VNMC System Requirements

Requirement	Description
Virtual Appliance	
One virtual CPU	1.5 GHz
Memory	4 GB RAM
Disk space	25 GB on a shared network file storage (NFS) or a storage area network (SAN) if Cisco VNMC is deployed in a high availability (HA) cluster

Requirement	Description
Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor
Microsoft Hyper-V	
Microsoft SCVMM SP1	
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Web-Based GUI Client Requirements

Requirement	Description
Operating system	Any of the following: • Windows • Apple Mac OS
Browser	Any of the following: • Internet Explorer 9.0 • Mozilla Firefox 11.0[1] • Chrome 26.0
Flash Player	Adobe Flash Player plugin (version 10.1 or later)

[1] We recommend Mozilla Firefox 11.0 with Adobe Flash Player 11.2.

Note Before you can use Chrome with VNMC 2.1, you must first disable the Adobe Flash Players that are installed by default with Chrome.

Firewall Ports Requiring Access

Requirement	Description
80	HTTP/TCP
443	HTTP
843	TCP

Cisco Nexus 1000V Series Switch Requirements

Requirement	Notes
General	
The procedures in this guide assume that the Cisco Nexus 1000V Series switch is up and running, and that endpoint Virtual Machines (VMs) are installed.	—
VLANs	
One HA VLAN configured on the Cisco Nexus 1000V Series switch uplink port.	VLAN need not be the system VLAN.
Port Profiles	
One port profile configured on the Cisco Nexus 1000V Series Switch for the service VLAN.	—

Information Required for Installation and Configuration

Information Type	Your Information
For Deploying the VNMC ISO	
Name	

Information Type	Your Information
ISO file location	
Storage location, if more than one location is available	
Management port profile name for VM management **Note** The management port profile is the same port profile that is used for VSM. The port profile is configured in VSM and is used for the Cisco VNMC management interface.	
IP address	
Subnet mask	
Gateway IP address	
Domain name	
DNS server	
Admin password	
Shared secret password for communications between the Cisco VNMC, Cisco VSG, and VSM.	

Shared Secret Password Criteria

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

Do not include the following items in passwords:

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

Create strong passwords based on the following characteristics:

Table 1: Characteristics of Strong Passwords

Strong passwords have...	Strong passwords do not have...
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive characters, such as *abcd*. • Characters repeated three or more times, such as *aaabbb*. • A variation of the word Cisco, such as *cisco*, *ocsic*, or one that changes the capitalization of letters in the word *Cisco*. • The username or the username in reverse. • A permutation of characters present in the username or *Cisco*.

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Microsoft Hyper-V Server Requirement

You must set the clock to the correct time on all the Microsoft Hyper-V servers that will run Cisco VNMC, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco VNMC CA certificate that is created when the Cisco VNMC VM is deployed might have an invalid time stamp.

After you set the clock to the correct time on all the Hyper-V servers that run the Cisco VNMC, you can, as an option, set the clock on the Cisco VNMC as follows:

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

Installing Cisco VNMC

Before You Begin

- Verify that the Hyper-V host on which to deploy the VNMC VM is available in SCVMM.
- Copy the VNMC 2.1 ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose **Library > Library Servers**, right-click on the library location, and then refresh.

SUMMARY STEPS

1. Launch the SCVMM.
2. Choose the Hyper-V host on which to deploy the VNMC VM.
3. Right-click the Hyper-V host and choose **Create Virtual Machine**.
4. In the Create Virtual Machine wizard, from the **Select Source** screen, select the **Create the new virtual machine with a blank virtual hard disk** radio button, then click **Next.**
5. In the Specify Virtual Machine Identity screen, provide the required information, then click **Next.**
6. In the **Configure Hardware** screen, do the following:
7. In the **Select Destination** screen, do the following:
8. In the **Select Host** screen, choose the destination, then click **Next.**
9. In the **Configure Settings** screen, review the virtual machine settings, then click **Next.**
10. In the **Add properties** screen, select the **Red Hat Enterprise Linux 5 (64 bit)** operating system, then click **Next.**
11. In the **Summary** screen, do the following:
12. After the virtual machine is successfully created, right-click the new Virtual Machine (vnmc21-perf in this case) and choose **Connect or View > Connect Via Console**.
13. Launch the console and install VNMC
14. After VNMC is successfully deployed, click **Close** and power on the VNMC VM.

DETAILED STEPS

Step 1 Launch the SCVMM.

Step 2 Choose the Hyper-V host on which to deploy the VNMC VM.

Step 3 Right-click the Hyper-V host and choose **Create Virtual Machine**.

Step 4 In the Create Virtual Machine wizard, from the **Select Source** screen, select the **Create the new virtual machine with a blank virtual hard disk** radio button, then click **Next.**

Step 5 In the Specify Virtual Machine Identity screen, provide the required information, then click **Next.**

Step 6 In the **Configure Hardware** screen, do the following:

a) From General, do the following:

- Choose **Processor** and set the number of processors to two.
- Choose **Memory** and choose the required memory value. You will need minimum 3 GB memory.

b) From **Bus Configuration > IDE Devices**, do the following:

- Choose **Hard Disk**, enter the required size of the hard disk. You will need at least 20 GB.
- Choose **Virtual DVD Drive**, select the **Existing ISO image file** radio button, and browse to select the VNMC 2.1 ISO image file.

c) Choose **Network Adapters > Network Adapter 1**, select the **Connect to a VM Network** radio button, and browse to select a VM Network.

d) Click **Next.**

Step 7 In the **Select Destination** screen, do the following:

a) Select the **Place the virtual machine on a host** radio button.
b) Choose **All hosts** from the **Destination** drop-down list.
c) Click **Next.**

Step 8 In the **Select Host** screen, choose the destination, then click **Next.**

Step 9 In the **Configure Settings** screen, review the virtual machine settings, then click **Next.**

Step 10 In the **Add properties** screen, select the **Red Hat Enterprise Linux 5 (64 bit)** operating system, then click **Next.**

Step 11 In the **Summary** screen, do the following:

a) Verify the settings.
b) Check the **Start the virtual machine after deploying it** check box.
c) Click **Create.**
The job Create virtual machine starts. You can see the status of this job in The Recent Jobs window. Ensure that the job completes without any errors.

Step 12 After the virtual machine is successfully created, right-click the new Virtual Machine (vnmc21-perf in this case) and choose **Connect or View > Connect Via Console**.

Step 13 Launch the console and install VNMC

Note Before the final VNMC installation step, before you reboot, launch SCVMM again and right-click the Virtual machine (vnmc21-hyperv in this case) and choose **Properties > Hardware Configuration > Bus Configuration > Virtual DVD Drive > no media**, so that VNMC does not use the ISO image at boot time.

Step 14 After VNMC is successfully deployed, click **Close** and power on the VNMC VM.

CHAPTER 4

Installing the Cisco VSG

This chapter contains the following sections:

Information About the Cisco VSG

This section describes how to install and complete the basic configuration of the Cisco VSG for Cisco Nexus 1000v Series switch software.

Host and VM Requirements

The Cisco VSG has the following requirements:

- Microsoft SCVMM SP1
- Virtual Machine (VM)
    - 64-bit VM is required.
    - 1 processor
    - 2 GB RAM

- ◦ 3 NICs
- ◦ Minimum 2 GB hard disk with LSI Logic Parallel adapter (default)
- ◦ Minimum CPU speed of 1 GHz

Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology

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

Term	Description
Logical Switch	Logical switch that spans one or more servers. It is controlled by one VSM instance.
NIC	Network interface card.
Server hosting SCVMM	Service that acts as a central administrator for Microsoft Hyper-V hosts that are connected on a network. The server directs actions on the VMs and the VM hosts .
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a Microsoft Hyper-V host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual data center as defined by the Hyper-V Server.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
vPath	Component in the Cisco Nexus 1000V Series switch with a VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual device that runs on a virtual machine (VM) and is based on Cisco NX-OS.
SCVMM	System Center Virtual Machine Manager Connect remotely to Hyper-V server. It is the primary interface for creating, managing, and monitoring VMs, their resources, and their hosts. It also provides console access to VMs.

Prerequisites for Installing the Cisco VSG Software

The following components must be installed and configured:

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

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

Obtaining the Cisco VSG Software

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

http://www.cisco.com/en/US/products/ps11208/index.html

Installing the Cisco VSG Software

You can install the Cisco VSG software on a VM by using an ISO image file from the CD.

Installing the Cisco VSG Software from an ISO File

Before You Begin

Make sure that you know the following:

- Microsoft SCVMM SP1 is installed.
- Download the Cisco VSG ISO image and upload it to the server (C:\ProgramData\Virtual Machine Manager Library Files\ISO). Refresh the library server under the Library tab.
- The Cisco VSG-Data port profile: VSG-Data
- The Cisco VSG-ha port profile: VSG-ha
- The HA ID
- The IP/subnet mask/gateway information for the Cisco VSG
- The admin password
- 2 GB RAM and 2 GB hard disk space are available
- The Cisco VNMC IP address
- The shared secret password

- The IP connectivity between Cisco VSG and Cisco VNMC is okay.
- The Cisco VSG VNM-PA image name (vsghv-pa.2.1.1a.bin) is available.

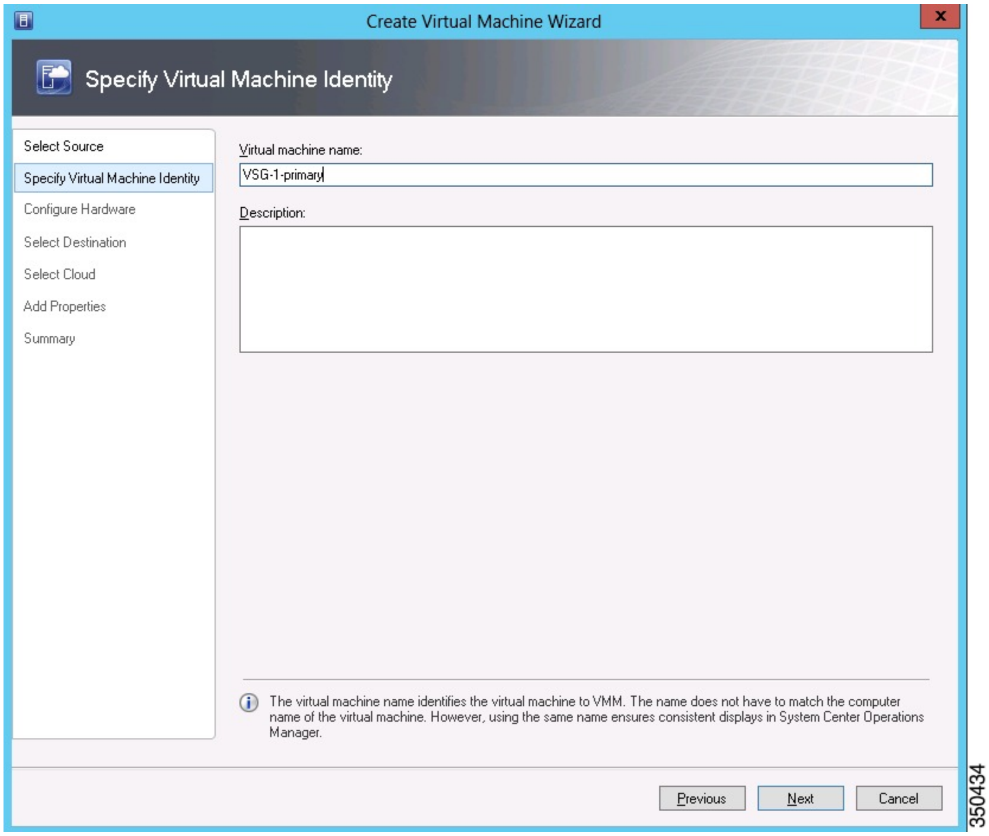
Step 1 Launch SCVMM.

Step 2 In the **VMs and Services** tab, click **Create Virtual Machine**.

Step 3 In the Create Virtual Machine Wizard, in the**Select Source** screen, check **Create the new virtual machine with a blank virtual hard disk** radio button and click **Next**.

Step 4 In the **Specify Virtual Machine Identity** screen, enter the name for the Cisco VSG in the **Virtual machine name** field and click **Next.**

Figure 28: Create Virtual Machine Wizard - Specify Virtual Machine Identity



Create Virtual Machine Wizard

Specify Virtual Machine Identity

Virtual machine name: VSG-1-primary

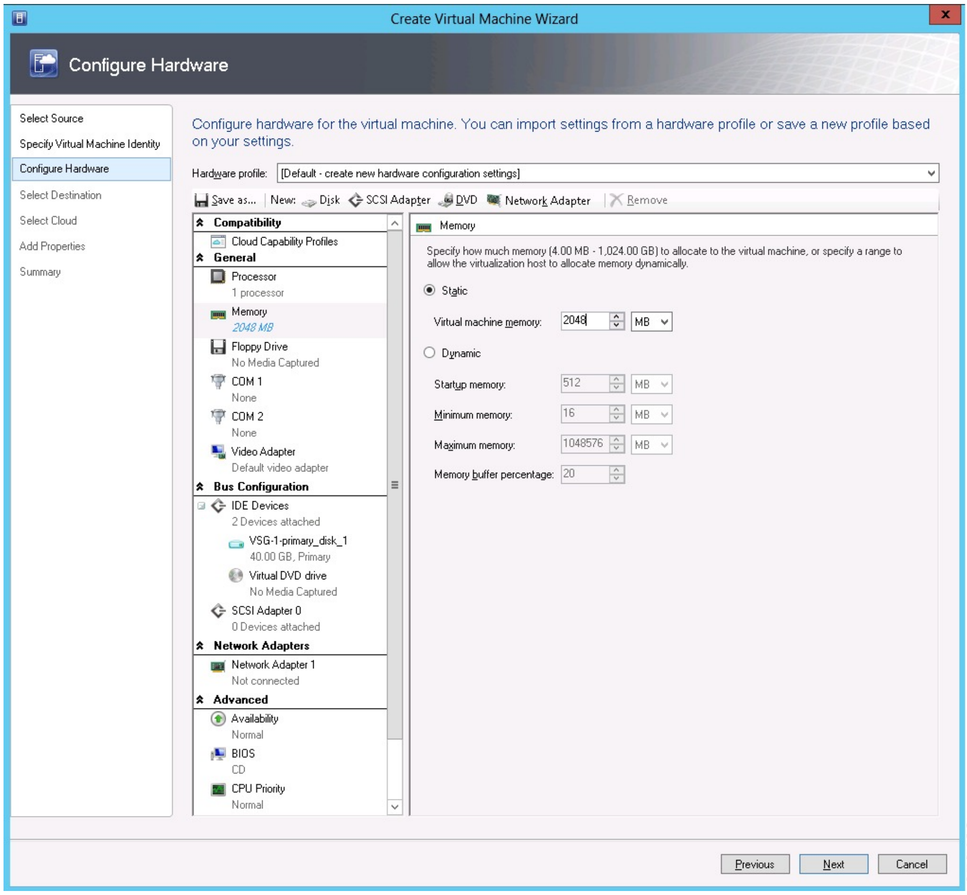
Description:

The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, using the same name ensures consistent displays in System Center Operations Manager.

Step 5 In the **Configure Hardware** section, do the following:

a) Under **General**, select **Memory**, select the **Static** option, and enter 2048 MB in the **Virtual machine memory** field.

Figure 29: Create Virtual Machine Wizard - Configure Hardware



Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

Memory

Specify how much memory (4.00 MB - 1,024.00 GB) to allocate to the virtual machine, or specify a range to allow the virtualization host to allocate memory dynamically.

● Static

Virtual machine memory: 2048 MB

○ Dynamic

Startup memory: 512 MB

Minimum memory: 16 MB

Maximum memory: 1048576 MB

Memory buffer percentage: 20

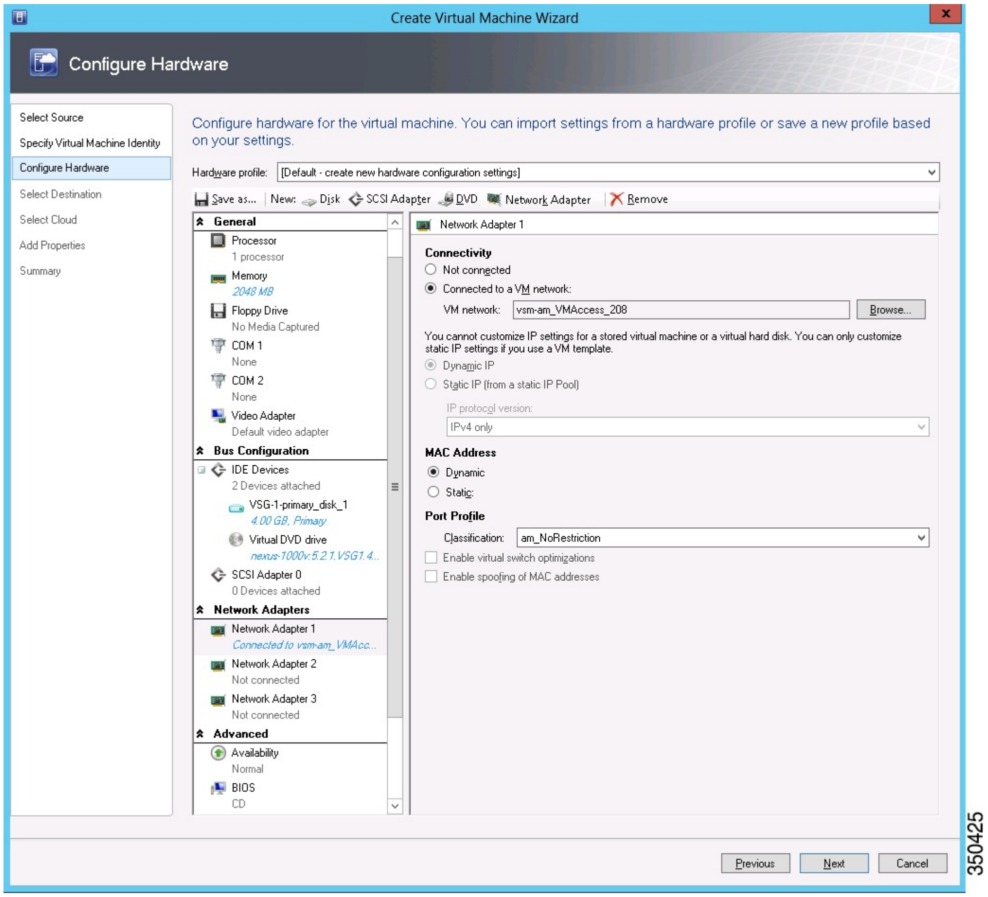
b) Under **Bus Configuration**, select the primary disk and enter 2 in the Size (GB) field.

c) Select the virtual DVD Drive, select **Existing ISO image file** radio button and browse for the VSG ISO within the SCVMM Library.

d) Select the **Network Adapter** drop-down near the top of the Create Virtual Machine Wizard and create two new Network Adapters (not Legacy).

- Under the **Network Adapters** section, select **Network Adapter 1**, then select **Connected to a VM network** and browse for the appropriate network corresponding to the network segment for the VSG's data interface.

Figure 30: Create Virtual Machine Wizard - Configure Hardware



Create Virtual Machine Wizard

Configure Hardware

Select Source
Specify Virtual Machine Identity
Configure Hardware
Select Destination
Select Cloud
Add Properties
Summary

Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings.

Hardware profile: [Default - create new hardware configuration settings]

General
Processor: 1 processor
Memory: 2048 MB
Floppy Drive: No Media Captured
COM 1: None
COM 2: None
Video Adapter: Default video adapter

Bus Configuration
IDE Devices: 2 Devices attached
VSG-1-primary_disk_1: 4.00 GB, Primary
Virtual DVD drive: nexus-1000v.5.2.1.VSG1.4...
SCSI Adapter 0: 0 Devices attached

Network Adapters
Network Adapter 1: Connected to vsm-am_VMAcc...
Network Adapter 2: Not connected
Network Adapter 3: Not connected

Advanced
Availability: Normal
BIOS: CD

Network Adapter 1

Connectivity
○ Not connected
● Connected to a VM network:
VM network: vsm-am_VMAccess_208

You cannot customize IP settings for a stored virtual machine or a virtual hard disk. You can only customize static IP settings if you use a VM template.
● Dynamic IP
○ Static IP (from a static IP Pool)
IP protocol version: IPv4 only

MAC Address
● Dynamic
○ Static:

Port Profile
Classification: am_NoRestriction
□ Enable virtual switch optimizations
□ Enable spoofing of MAC addresses

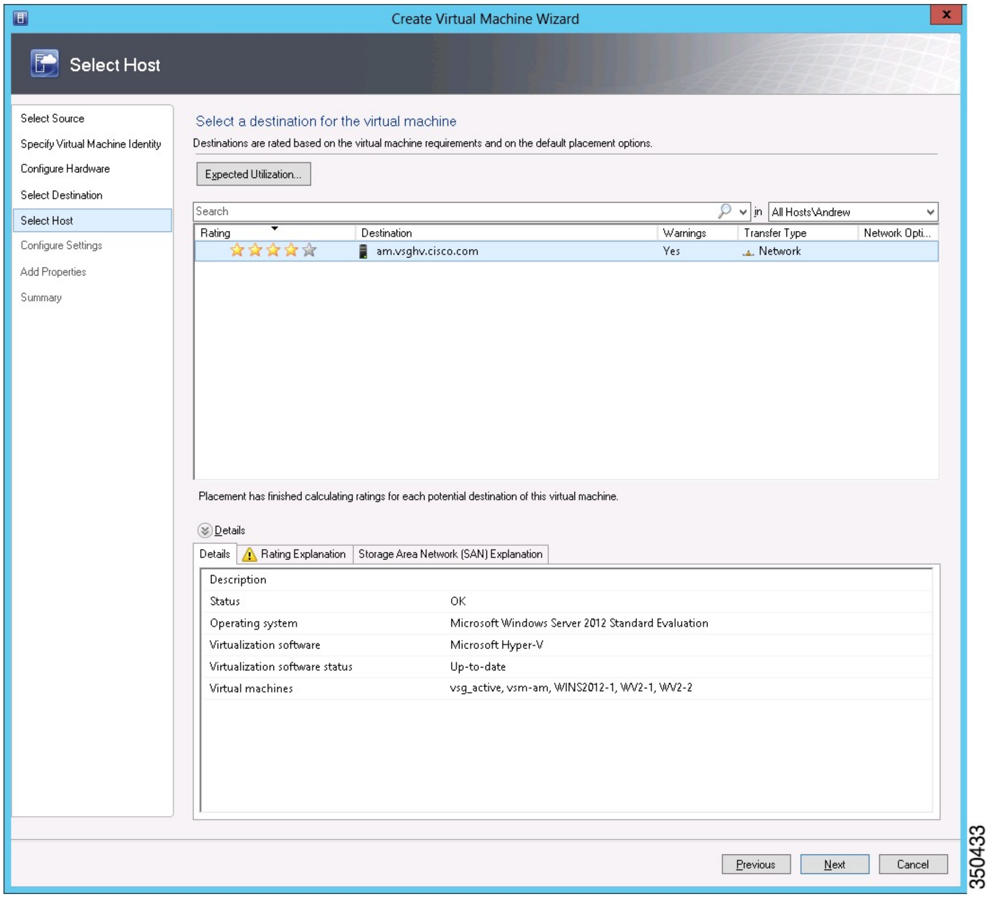
- From the **Classification** Drop-down, select the port-profile corresponding to the VSG's data interface.

Note Repeat the step d to create network adapters for service and HA.

Step 6 In the **Select Destination** section, choose **Place the virtual machine in a host** and select the host group on which you want to store the VSG from the drop-down and click **Next**.

Step 7 In the **Select Host** section, select the host you wish to place the VSG on and click **Next.**

Figure 31: Create Virtual Machine Wizard - Select Host



Select a destination for the virtual machine

Destinations are rated based on the virtual machine requirements and on the default placement options.

Rating	Destination	Warnings	Transfer Type	Network Opti...
★★★★☆	am.vsghv.cisco.com	Yes	Network	

Placement has finished calculating ratings for each potential destination of this virtual machine.

Description	
Status	OK
Operating system	Microsoft Windows Server 2012 Standard Evaluation
Virtualization software	Microsoft Hyper-V
Virtualization software status	Up-to-date
Virtual machines	vsg_active, vsm-am, WINS2012-1, WV2-1, WV2-2

Step 8 In the **Configure Settings** section, review the virtual machine settings to ensure they are correct and click **Next**.

Step 9 (Optional) In the **Add Properties** section, select **Other Linux (64-bit) from the Operating System** drop-down, then click **Next.**

Step 10 In the **Summary** section, click **Create.**

Step 11 Launch the Microsoft Hyper-V Manager on the server hosting the VSG.

Step 12 In the left pane, select the server that hosts the VSG instance you created.

Step 13 Under **Virtual Machines**, select the VSG you created.

Step 14 Under **Actions**, click **Settings** to open the **Settings** dialog-box.

Step 15 Select the first interface for the VSG instance and select **Advanced Features**.

Step 16 Under **MAC address**, select **Enable MAC address spoofing**.

Step 17 Click **OK**.

Step 18 Close the Microsoft Hyper-V Manager to return to the SCVMM interface.

Step 19 After MAC spoofing is configured and the VSG is successfully installed, select the VSG in the **VMs and Services** tab and click **Power On**.

Step 20 Connect to the VSG using **Connect or View -> Connect via Console**.

Configuring Initial Settings

This section describes how to configure the initial settings on the Cisco VSG and configure a standby Cisco VSG with its initial settings. For configuring a standby Cisco VSG, see Configuring Initial Settings on a Secondary Cisco VSG, on page 69 section.

You can connect to a VSG VM console through the SCVMM user interface by right-clicking a VM instance and connecting to it.

Step 1 Navigate to the **Console** tab in the VM.
Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.

Step 2 At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.

Step 3 At the prompt, confirm the admin password and press **Enter**.

Step 4 At the `Enter HA role[standalone/primary/secondary]` prompt, enter the HA role you want to use and press **Enter**.
This can be one of the following:

- standalone
- primary
- secondary

Step 5 At the `Enter the ha id(1-1024)` prompt, enter the HA ID for the pair and press **Enter**.

Note If you entered secondary in the earlier step, the HA ID for this system must be the same as the HA ID for the primary system.

Step 6 If you want to perform basic system configuration, at the `Would you like to enter the basic configuration dialog (yes/no)` prompt, enter **yes** and press **Enter**, then complete the following steps.

a) At the `Create another login account (yes/no)[n]` prompt, do one of the following:

- To create a second login account, enter **yes** and press **Enter**.
- Press **Enter**.

b) (Optional) At the `Configure read-only SNMP community string (yes/no)[n]` prompt, do one of the following:

- To create an SNMP community string, enter **yes** and press **Enter**.
- Press **Enter**.

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

Step 7 At the `Continue with Out-of-band (mgmt0) management configuration? (yes/no)[y]:` prompt, enter **yes** and press **Enter**.

Step 8 At the `Mgmt IPv4 address:` prompt, enter **10.10.10.11** and press **Enter**.

Step 9 At the `Mgmt IPv4 netmask` prompt, enter **255.255.255.0** and press **Enter**.

Step 10 At the `Configure the default gateway? (yes/no)[y]` prompt, enter **yes** and press **Enter**.

Step 11 At the `Enable the telnet service? (yes/no)[y]:` prompt, enter **no** and press **Enter**.

Step 12 At the `Configure the ntp server? (yes/no)[n]` prompt, enter **NTP server** information and press **Enter**. The following configuration will be applied:

```
Interface mgmt0
ip address 10.10.10.11 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/10.10.11.1
no telnet server enable
ssh key rsa 768 force
ssh server enable
feature http-server
ha-pair id 25
```

Step 13 At the `Would you like to edit the configuration? (yes/no)[n]` prompt, enter **n** and press **Enter**.

Step 14 At the `Use this configuration and save it? (yes/no)[y]:` prompt, enter **y** and press **Enter**.

Step 15 At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**.
The default account name is `admin`.

Step 16 At the `Password` prompt, enter the name of the password for the admin account and press **Enter**.
You are now at the Cisco VSG node.

On the VSG, Configuring the Cisco VNMC Policy Agent

Once the Cisco VNMC is installed, you must register the VSG with the Cisco VNMC.

Note Cisco VSG is supported as VSB on Nexus Cloud Services platform only.

Before You Begin

Make sure that you know the following:

- The Cisco VNMC policy-agent image is available on the VSG (for example, vsghv-pa.2.1.1a.bin)

  Note The string **vsghv-pa** must appear in the image name as highlighted.

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

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

Note VSG clock should be synchronized with the VNMC clock.

Step 1 On the VSG, enter the following commands:

```
vsg# configure terminal
vsg(config)# vnm-policy-agent
vsg(config-vnm-policy-agent)# registration-ip 10.193.75.95
vsg(config-vnm-policy-agent)# shared-secret Example_Secret123
vsg(config-vnm-policy-agent)# policy-agent-image vsghv-pa.2.1.1a.bin
vsg(config-vnm-policy-agent)# exit
vsg(config)# copy running-config startup-config
vsg(config)# exit
```

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

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

The VSG is now registered with the Cisco VNMC.

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

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

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

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

Configuring Initial Settings on a Secondary Cisco VSG

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

Step 1 Navigate to the **Console** tab in the VM.
Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.

Step 2 At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.

Step 3 At the prompt, confirm the admin password and press **Enter**.

Step 4 At the `Enter HA role[standalone/primary/secondary]` prompt, enter the secondary HA role and press **Enter**.

Step 5 At the `Enter the ha id(1-1024)` prompt, enter **25** for the HA pair id and press **Enter**.

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

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

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

Verifying the Cisco VSG Configuration

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

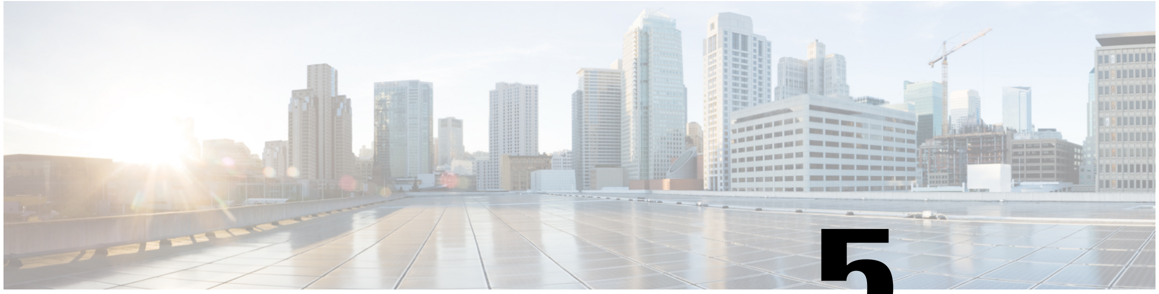
Command	Purpose
show interface brief	Displays brief status and interface information.

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
```

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.



CHAPTER 5

Registering Devices with the Cisco VNMC

This chapter contains the following sections:

Registering a Cisco VSG

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

SUMMARY STEPS

1. Copy the vsghv-pa.2.1.1a.bin file into the Cisco VSG bootflash:
2. On the command line, enter configuration mode.
3. Enter config-vnm-policy-agent mode.
4. Set the Cisco VNMC registration IP address.
5. Specify the shared-secret of Cisco VNMC.
6. Install the policy agent.
7. Exit all modes.
8. On the Cisco VSG command line, enter the following command:
9. On the command line, enter the following command:

DETAILED STEPS

Step 1 Copy the vsghv-pa.2.1.1a.bin file into the Cisco VSG bootflash:

```
vsg# copy ftp://guest@172.18.217.188/n1kv/vsghv-pa.2.1.1a.bin bootflash
```

Step 2 On the command line, enter configuration mode.

```
vsg# configure
```

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

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

Step 4 Set the Cisco VNMC registration IP address.

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

Step 5 Specify the shared-secret of Cisco VNMC.

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

Step 6 Install the policy agent.

```
vsg (config-vnm-policy-agent)#
policy-agent-image bootflash: vsghv-pa.2.1.1a.bin
```

Step 7 Exit all modes.

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

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

```
vsg# show vnm-pa status
If registration was successful, you should see the following message:
"VNM Policy-Agent status is - Installed Successfully. Version 2.1(1a)-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 Cisco VNMC.

SUMMARY STEPS

1. Copy the vsmhv-pa.2.1.1a.bin file into the VSM bootflash:
2. On the command line, enter configuration mode.
3. Enter config-vnm-policy-agent mode.
4. Set the Cisco VNMC registration IP address.
5. Specify the shared-secret of Cisco VNMC.
6. Install the policy agent.
7. Exit all modes.
8. On the command line, enter the following command:
9. On the command line, enter the following command:

DETAILED STEPS

Step 1 Copy the vsmhv-pa.2.1.1a.bin file into the VSM bootflash:

```
vsm# copy ftp://guest@172.18.217.188/n1kv/vsmhv-pa.2.1.1a.bin bootflash:
```

Step 2 On the command line, enter configuration mode.

```
vsg# configure
```

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

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

Step 4 Set the Cisco VNMC registration IP address.

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

Step 5 Specify the shared-secret of Cisco VNMC.

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

Step 6 Install the policy agent.

```
vsg(config-vnm-policy-agent)# policy-agent-image bootflash:vsmhv-pa.2.1.1a.bin
```

Step 7 Exit all modes.

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

Step 8 On the 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 2.1(1a)-vsg
The Cisco Nexus 1000V VSM 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.
```

What to Do Next

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

CHAPTER 6

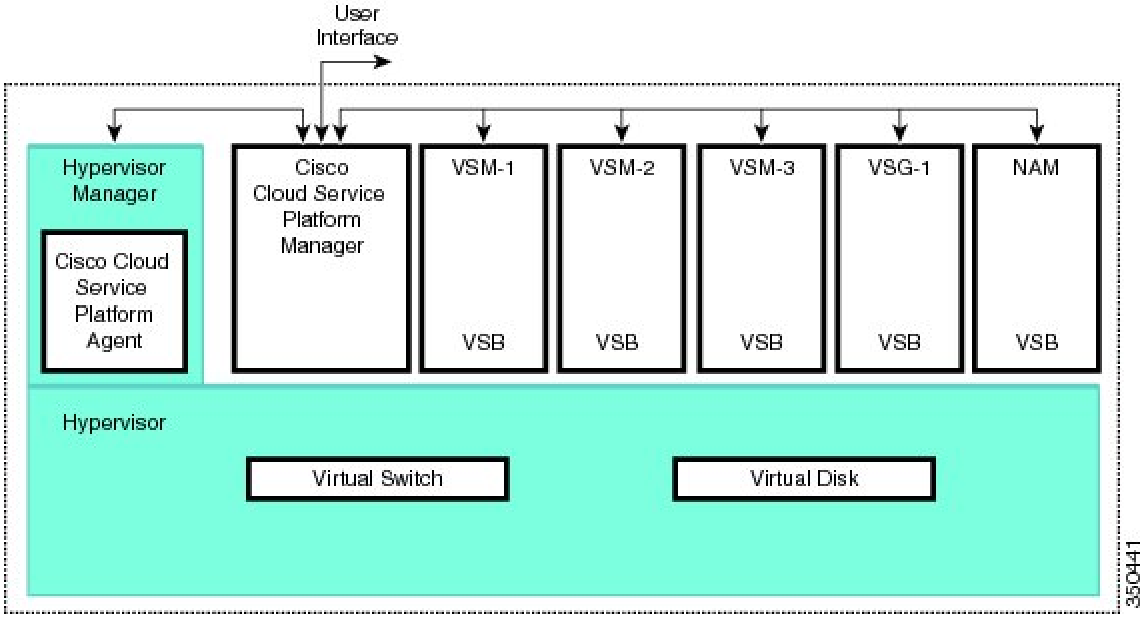
Installing the Cisco VSG on a Cisco Cloud Service Platform Virtual Services Appliance

This chapter contains the following sections:

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

The Cisco VSG software is provided with the other virtual service blade (VSB) software in the Cisco Cloud Service Platform bootflash: repository directory. The Cisco Cloud Service Platform has up to six virtual service blades (VSBs) on which you can choose to place a Cisco VSG, VSM, or Network Analysis Module (NAM).

Figure 32: Cisco Cloud Service Platform Architecture Showing Virtual service Blades Usage



Prerequisites for Installing Cisco VSG on Cisco Cloud Service Platform

- You must first install the Cisco Cloud Service Platform Virtual Services Appliance and connect it to the network. For procedures on installing the hardware, see the *Cisco Cloud Service Platform Virtual Services Appliance Hardware Installation Guide*.
- After you install the hardware appliance and connect it to the network, you can configure the Cisco Cloud Service Platform management software and create and configure new VSBs that might host the Cisco VSG. For procedures on configuring the software, see the *Cisco Cloud Service Platform Software Configuration Guide*.

Guidelines and Limitations

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

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

Installing a Cisco VSG on a Cisco Cloud Service Platform

You can install the Cisco VSG on a Cisco Cloud Service Platform as a virtual service blade (VSB).

Before You Begin

- Log in to the CLI in EXEC mode.
- Know the name of the Cisco VSG VSB that you want to create.
- Whether you are using a new ISO file from the bootflash repository folder or from an existing VSB, do one of the following:

  – If you are using a new ISO file in the bootflash repository, you know the filename, for example, nexus-1000v.5.2.1.VSG1.4.1.iso

  – If you are using an ISO file from an existing VSB, you must know the name of the VSB type. This procedure includes information about identifying this name.
- Know the following properties for the Cisco VSG VSB:

  – HA ID –Management IP address

  – Cisco VSG name

  – Management subnet mask length

  – Default gateway IPV4 address

  – Administrator password

  – Data and HA VLAN IDs
- This procedure shows you how to identify and assign data and HA VLANs for the Cisco VSG VSB. Do not assign a management VLAN because the management VLAN is inherited from the Cisco Cloud Service Platform.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	(config)# **virtual-service-blade** *name*	Creates the named VSB and places you into configuration mode for that service. The name can be an alphanumeric string of up to 80 characters.
Step 3	(config-vsb-config)# **description** *description*	(Optional) Adds a description to the Cisco VSG VSB. The *description* is an alphanumeric string of up to 80 characters.
Step 4	(config-vsb-config)# **virtual-service-blade-type** [**name** *name* | **new** *iso file name*]	Specifies the type and name of the software image file to add to this Cisco VSG VSB: • Use the new keyword to specify the name of the new Cisco VSG ISO software image file in the bootflash repository folder. • Use the **name** keyword to specify the name of the existing Cisco VSG VSB type. Enter the name of an existing type found in the command output.
Step 5	(config-vsb-config)# **interface** *name* **vlan** *vlanid*	Applies the interface and VLAN ID to this Cisco VSG. Use the interface names from the command output. **Note** If you try to apply an interface that is not present, the following error is displayed: ERROR: Interface name not found in the associated virtual-service-blade type. **Caution** Do not assign a management VLAN. Unlike data and HA VLANs, the management VLAN is inherited from the Cisco Cloud Service Platform. **Caution** To prevent loss of connectivity, you must configure the same data and HA VLANs on the hosted Cisco VSGs.
Step 6	Repeat Step 7 to apply additional interfaces	

	Command or Action	Purpose
Step 7	(config-vsb-config)# **enable [primary | secondary]**	Initiates the configuration of the VSB and then enables it. If you enter the **enable** command without the optional **primary** or **secondary** keywords, it enables both. If you are deploying a redundant pair, you do not need to specify primary or secondary. If you are enabling a nonredundant VSB, you can specify its HA role as follows: • Use the **primary** keyword to designate the VSB in a primary role. • Use the **secondary** keyword to designate the VSB in a secondary role The Cisco Cloud Service platform prompts you for the following: • HA ID • Management IP address • Management subnet mask length • Default gateway IPV4 address • Cisco VSG name • Administrator password
Step 8	(config-vsb-config)# **show virtual-service-blade name** *name*	(Optional) Displays the new VSB for verification. While the Cisco Cloud Service Platform management software is configuring the Cisco VSG, the output for this command progresses from in progress to powered on.
Step 9	(config-vsb-config)# **copy running-config startup-config**	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure a Cisco Cloud Service Platform appliance VSB as a Cisco VSG:

```
csp# configure
Enter configuration commands, one per line. End with CNTL/Z.
N1010-63(config)# virtual-service-blade vsg-1
N1010-63(config)# description vsg-1 for Tenant1
N1010-63(config-vsb-config)# virtual-service-blade-type new nexus-1000v.5.2.1.VSG1.4.1.iso
N1010-63(config-vsb-config)# interface data vlan 923
N1010-63(config-vsb-config)# interface ha vlan 930
N1010-63(config-vsb-config)# no shutdown
N1010-63(config-vsb-config)# enable
Enter vsb image: [nexus-1000v.5.2.1.VSG1.4.1.iso]
Enter HA id[1-4095]: 1002
Management IP version [V4/V6]: [V4]
Enter Management IP address: 10.2.71.117
Enter Management subnet mask: 255.255.255.0
IPv4 address of the default gateway: 10.2.0.1
Enter HostName: VSG-1
Enter the password for 'admin': Hello123
```

```
N1010-63(config-vsb-config)#exit
N1010-63)#
```

This example show how to install the Cisco VSG on a Cisco Cloud Service Platform as a VSB.

```
N1010-63# configure
N1010-63(config)# virtual-service-blade vsg-1
N1010-63(config-vsb-config)# show virtual-service-blade-type summary

-------------------------------------------------------------------------------
Virtual-Service-Blade-Type    Virtual-Service-Blade
-------------------------------------------------------------------------------
VSG-1.2                       VSG-NH-hpv
                              hyperv-soak
                              VSG-354
                              VSG-357
                              vsg-1


N1010-63(config-vsb-config)# virtual-service-blade-type new nexus-1000v.5.2.1.VSG1.4.1.iso
or
N1010-63(config-vsb-config)# show virtual-service-blade name vsg-1

N1010-63(config-vsb-config)# description vsg-1 for Tenant1
N1010-63(config-vsb-config)# show virtual-service-blade name vsg-1
-------------------------------------------------------------------------------
   virtual-service-blade vsm2
   Description:
   Slot id: 2
   Host Name:
   Management IP:
   VSB Type Name : VSG-1.0
   Interface: ha vlan: 0
   Interface: management vlan: 231
   Interface: data vlan: 0
   Interface: internal vlan: NA
   Ramsize: 2048
   Disksize: 3
   Heartbeat: 0
   HA Admin role: Primary
   HA Oper role: NONE
   Status: VSB NOT PRESENT
   Location: PRIMARY
   SW version:
   HA Admin role: Secondary
   HA Oper role: NONE
   Status: VSB NOT PRESENT
   Location: SECONDARY
   SW version:
   VSB Info:
-------------------------------------------------------------------------------
N1010-63(config-vsb-config)# interface data vlan 1044
or
N1010-63(config-vsb-config)# interface ha vlan 1045

N1010-63(config-vsb-config)# enable
-------------------------------------------------------------------------------
    Enter domain id[1-1024]: 1014
    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
-------------------------------------------------------------------------------
N1010-63(config-vsb-config)# show virtual-service-blade name vsg-1
  Description:
  Slot id:        4
  Host Name:      VSG-Fire-hpv
  Management IP:  10.78.108.40
  VSB Type Name :  VSG-1.2
  Configured vCPU:           1
  Operational vCPU:           1
  Configured Ramsize:        2048
  Operational Ramsize:        2048
  Disksize:       3
  Heartbeat:      521511

  Legends:   P -  Passthrough
  ---------------------------------------------------------------------------
   Interface           Type         MAC     VLAN    State   Uplink-Int
                                                  Pri  Sec Oper  Adm
  ---------------------------------------------------------------------------
  VsbEthernet4/1        data 0002.3d70.3f0c  1044   up   up Po3    Po3
  VsbEthernet4/2  management 0002.3d70.3f0b   231   up   up Po1    Po1
  VsbEthernet4/3          ha 0002.3d70.3f0d  1045   up   up Po2    Po2
        internal          NA        NA       NA     up   up
  HA Role: Primary
    HA Status: ACTIVE
    Status:       VSB POWERED ON
    Location:     PRIMARY
    SW version:   5.2(1)VSG1(4.1)
  HA Role: Secondary
    HA Status: STANDBY
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:   5.2(1)VSG1(4.1)
  VSB Info:
    Domain ID : 1054
-------------------------------------------------------------------------------
N1010-63(config-vsb-config)# copy running-config startup-config
```

This example shows how to display a virtual service blade summary on the Cisco Cloud Service Platform:

```
N1010-63(config-vsb-config)# show virtual-service-blade summary

-------------------------------------------------------------------------------
Name                HA-Role     HA-Status   Status                   Location
-------------------------------------------------------------------------------
VSG-NH-hpv          PRIMARY     ACTIVE      VSB POWERED ON           PRIMARY
VSG-NH-hpv          SECONDARY   STANDBY     VSB POWERED ON           SECONDARY
hyperv-soak         PRIMARY     NONE        VSB NOT PRESENT          PRIMARY
hyperv-soak         SECONDARY   NONE        VSB NOT PRESENT          SECONDARY
VSG-354             PRIMARY     ACTIVE      VSB POWERED ON           PRIMARY
VSG-354             SECONDARY   STANDBY     VSB POWERED ON           SECONDARY
VSG-1               PRIMARY     ACTIVE      VSB POWERED ON           PRIMARY
VSG-1               SECONDARY   STANDBY     VSB POWERED ON           SECONDARY
```

INDEX