Cisco VSG for Microsoft Hyper-V, Release 5.2(1)VSG2(1.2b) and Cisco Prime NSC, Release 3.4 Installation and Upgrade Guide

First Published: 2014-12-19

Last Modified: 2018-12-20

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

CONTENTS

Preface

The preface contains the following sections:

Audience

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

Document Conventions

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

Command descriptions use the following conventions:

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

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

Examples use the following conventions:

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

This document uses the following conventions:

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

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

Related Documentation for Cisco Virtual Security Gateway for Microsoft Hyper-V

This section lists the documents available for Cisco Virtual Security Gateway for Microsoft Hyper-V and related products.

Cisco Virtual Security Gateway Documentation

The *Cisco Virtual Security Gateway for Microsoft Hyper-V* documentation is available at http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html.

Cisco Virtual Security Gateway for Microsoft Hyper-V Release Notes

Cisco Virtual Security Gateway for Microsoft Hyper-V Installation Guide

Cisco Virtual Security Gateway for Microsoft Hyper-V Configuration Guide

Cisco Virtual Security Gateway for Microsoft Hyper-V Troubleshooting Guide

Cisco Virtual Security Gateway for Microsoft Hyper-V Command Reference

Cisco vPath and vServices Reference Guide for Microsoft Hyper-V

Related Documentation for Nexus 1000V Series NX-OS for Microsoft Hyper-V Software

The *Cisco Nexus 1000V Series Switch for Microsoft Hyper-V* documents are available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps13056/tsd_products_support_series_home.html

Documentation Feedback

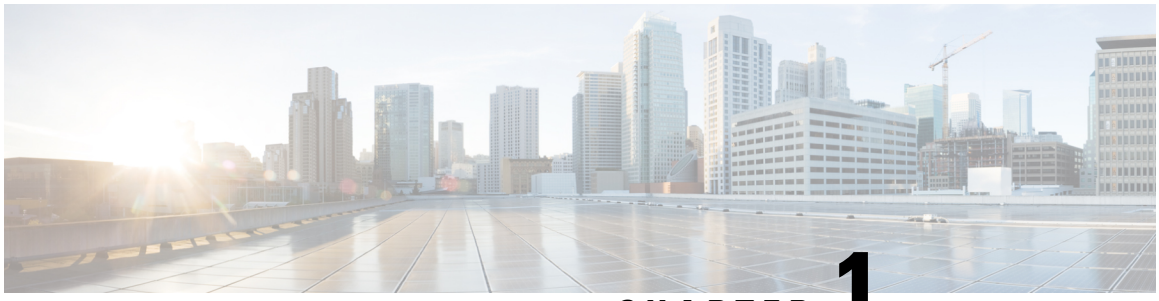
To provide technical feedback on this document, or to report an error or omission, please send your comments to vsg-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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



CHAPTER 1

Overview

This chapter contains the following sections:

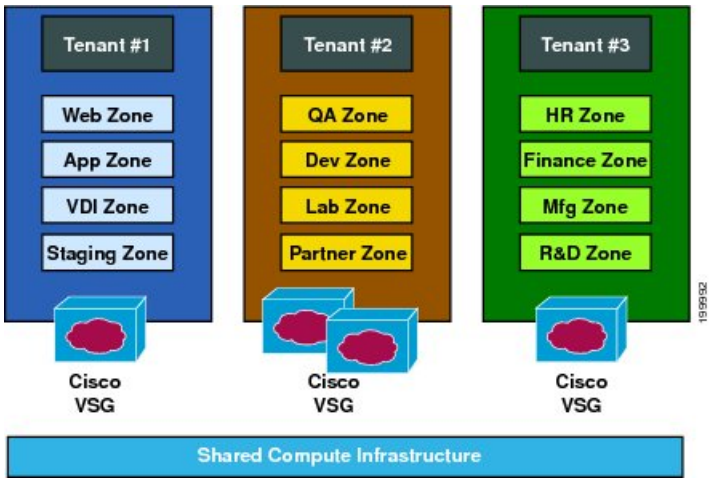
Information About Installing Cisco PNSC and Cisco VSG

You must install Cisco Prime Network Services Controller (PNSC) and Cisco VSG in a particular sequence on the Cisco Nexus 1000V switch to have a functioning virtual system.

Information About Cisco VSG

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 multi-tenancy. By associating one or more Virtual Machines (VMs) into distinct trust zones, 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 Cisco VSG.

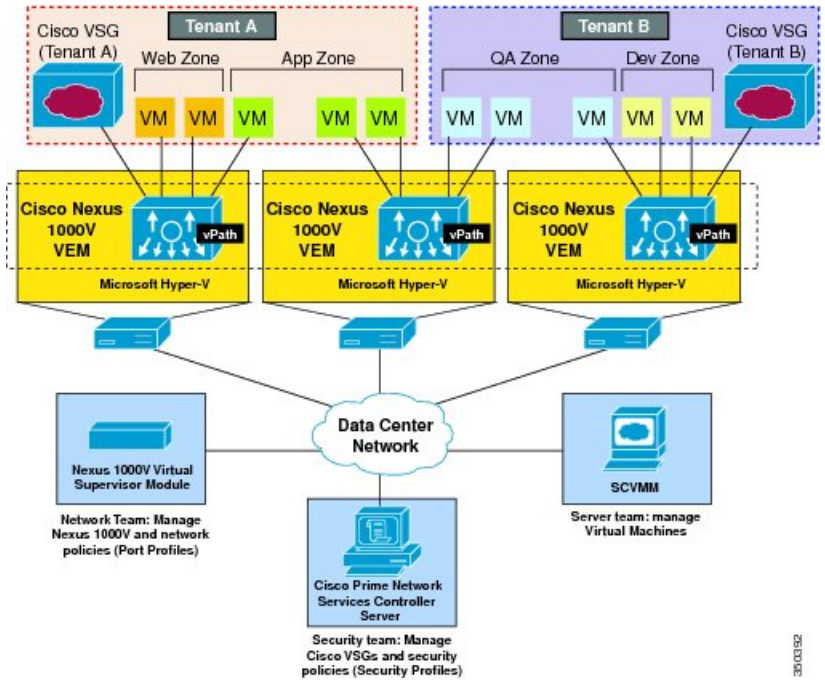
Figure 1: Trusted Zone-Based Access Control Using Per-Tenant Enforcement with Cisco VSG



Cisco Prime NSC and VSG Architecture

Cisco VSG operates with Cisco Nexus 1000V Series switch on KVM on Red Hat Enterprise Linux OpenStack Platform and leverages the virtual network service data path (Cisco vPath). Cisco vPath steers traffic, whether external-to-VM or VM-to-VM, to Cisco VSG of a tenant. Initial packet processing occurs in Cisco VSG for policy evaluation and enforcement. After the policy decision is made, Cisco VSG offloads policy enforcement of the remaining packets to Cisco vPath.

Figure 2: Cisco Virtual Security Gateway Deployment Topology



Cisco vPath supports the following features:

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

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 Cisco vPath Virtual Ethernet Modules (VEMs), Cisco VSG enhances security performance through distributed Cisco vPath-based enforcement.
- You can use 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 Cisco VSG in an active-standby mode to ensure that Cisco vPath redirects packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.
- You can place 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

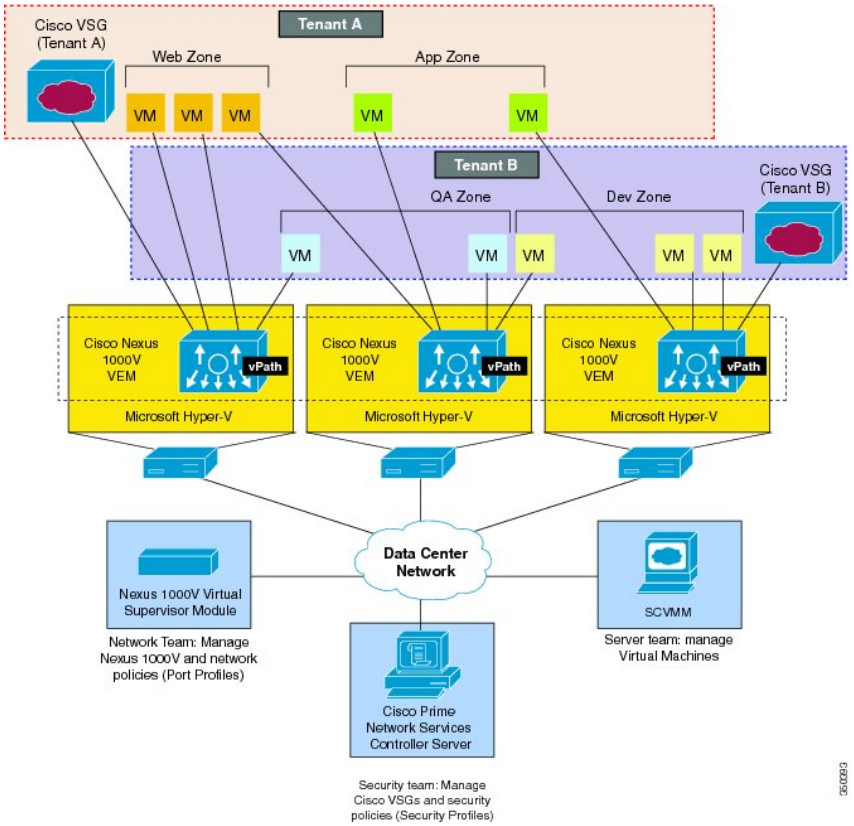
You can transparently insert a Cisco VSG into the Microsoft Hyper-V environment where Cisco Nexus 1000V is deployed. One or more instances of Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy Cisco VSG at the tenant level in Hyper-V and manage each tenant instance using Microsoft 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, Cisco VSG can permit or deny access and can generate optional access logs. Cisco VSG also provides policy-based traffic monitoring capability with access logs.

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



Cisco VSG operating with Cisco Nexus 1000V (and Cisco vPath) supports a dynamic VM environment. When you create a tenant with Cisco VSG (standalone or active-standby pair) on Cisco Prime NSC, 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 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, Cisco VSG immediately applies the security controls. You can repurpose a VM by assigning it to a different port profile or security profile.

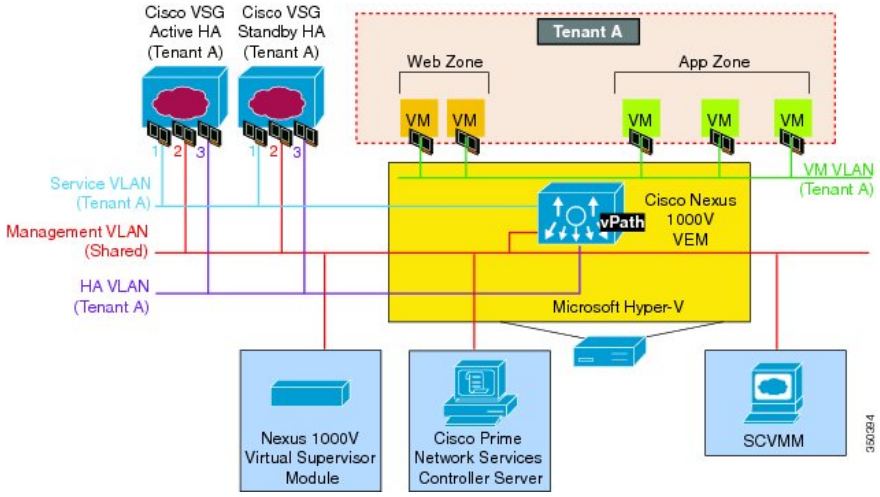
As VM migration events are triggered, VMs move across physical servers. Because Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to the migration events.

Setting Up Cisco VSG and VLAN

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

Figure 4: Cisco Virtual Security Gateway VLAN Usages

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



The VLAN functions are as follows:

- The service VLAN provides communications between Cisco Nexus 1000V VEM and Cisco VSG through a physical router. Cisco VSG data interface and VEM interface are configured on different subnets. All the Cisco VSG data interfaces are part of the service VLAN and the VEM interacts with Cisco VSG using the router.
- The management VLAN connects the management platforms such as ????Microsoft SCVMM????, Cisco PNSC, Cisco Nexus 1000V VSM, and 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 multi-tenant 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 Cisco Prime NSC

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

Note Multi-tenancy 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 multi-tenant architecture, a software application can virtually partition data and configurations so that each tenant works with a customized virtual application instance.

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

Cisco Prime NSC Key Benefits

Cisco PNSC provides the following key benefits:

- Rapid and scalable deployment with dynamic, template-driven policy management based on security profiles.
- Seamless operational management through XML APIs that enable integration with third-party management tools.
- Greater collaboration across security and server administrators, while maintaining administrative separation and reducing administrative errors.

Cisco Prime NSC Components

Cisco PNSC architecture includes the following components:

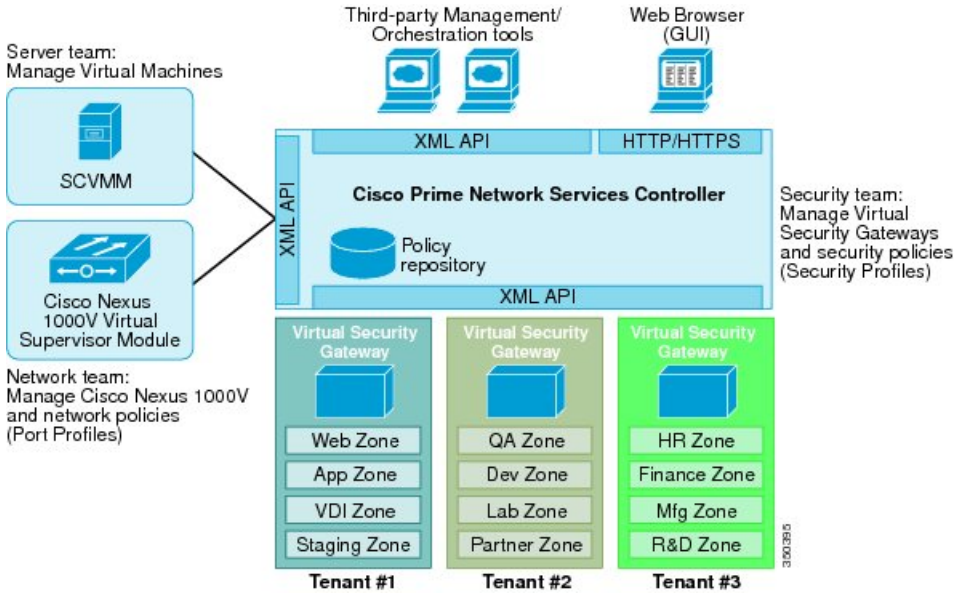
- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning. This function simplifies large scale deployments as follows:
  - Devices can be pre-instantiated 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 Prime NSC Architecture

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

Figure 5: Cisco Prime NSC Components



Cisco Prime NSC Security

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

Cisco Prime NSC API

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

Cisco Prime NSC and VSG

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

- Security administrators who author and manage security profiles as well as manage Cisco VSG instances. Security profiles are referenced in Cisco Nexus 1000V Series port profiles through Cisco PNSC interface.
- Network administrators who author and manage port profiles as well as manage Cisco Nexus 1000V Series switches. Port profiles are referenced in ?????Microsoft SCVMM???? through the Cisco Nexus 1000V Series VSM interface.

- Server administrators who select the appropriate port profiles in ?????Microsoft SCVMM???? when instantiating a virtual machine.

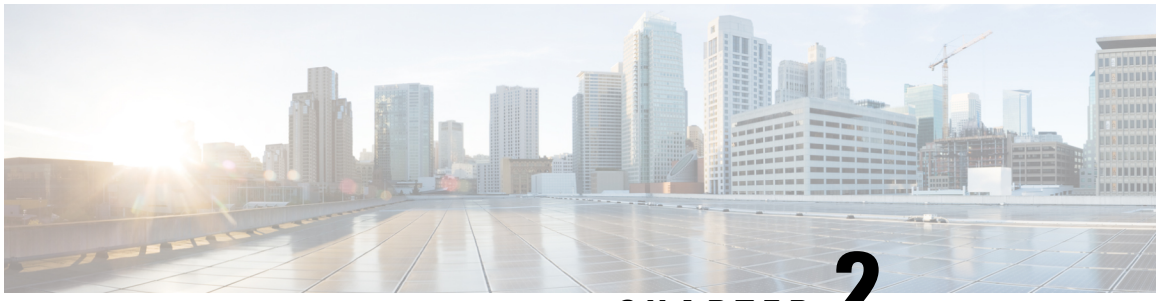
System Requirements

System requirements for Cisco Prime NSC are as follows:

- Microsoft Windows Server with SCVMM 2012 SP1, SCVMM 2012 R2, or SCVMM 2016.
- Intel VT that is enabled in the BIOS.
- 4 GB RAM for Prime NSC ISO installation.
- One of the following, depending on InterCloud functionality:
  - With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows:
    - Disk 1: 20 GB
    - Disk 2: 200 GB
  - Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows:
    - Disk 1: 20 GB
    - Disk 2: 20 GB
- Adobe Flash Player plugin 11.2 or higher.
- Any of the following browsers:
  - Internet Explorer 9.0 or higher
  - Mozilla Firefox 23.0 or higher
  - Google Chrome 29.0 or higher

  Access to Cisco Prime NSC application using a Web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports):
  - 443 (HTTPs)
  - 80 (HTTP/TCP)
  - 843 (Adobe Flash)

Note If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website.



CHAPTER 2

Installing the Cisco Prime NSC and Cisco VSG-Quick Start

This chapter contains the following sections:

Information About Installing Cisco Prime NSC and Cisco VSG

This chapter describes how to install and set up a basic working configuration of Cisco Prime Network Services Controller (Cisco PNSC) and Cisco Virtual Security Gateway (Cisco VSG). The example in this chapter uses the ISO files of the software for installation. The steps assume that Cisco Nexus 1000V Series switch is operational, and endpoint VMs are already installed.

Cisco VSG and Cisco Prime NSC Installation Planning Checklists

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

Basic Hardware and Software Requirements

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

Requirement	Description
Virtual CPUs	• Cisco VSG: 1 (1.5 GHz) • Cisco PNSC: 4 (1.8 GHz each)
Memory	• Cisco VSG: 2GB RAM • Cisco PNSC: 4GB RAM
Disk Space	Cisco VSG: 3 GB Cisco Prime NSC: Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: • Disk 1: 20 GB • Disk 2: 20 GB
Processor	x86 Intel or AMD server with a 64-bit processor.
Network Interfaces	• Cisco VSG: 3 • Cisco PNSC: 1
Microsoft SCVMM	SCVMM 2012 SP1, SCVMM 2012 R2, or SCVMM 2016
Browser	Any of the following browsers: • Internet Explorer 9.0 or higher • Mozilla Firefox 23.0 or higher • Google Chrome 29.0 or higher **Note** If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website. **Note** Before using Google Chrome with Cisco PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome.

Requirement	Description
Ports	Access to the Cisco PNSC application using a web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports): • 443 (HTTPS) • 80 (HTTP/TCP) • 843 (Adobe Flash)
Flash Player	Adobe Flash Player plugin 11.2 or higher

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

License Requirements

Cisco VSG license is integrated with the Nexus1000V Multi-Hypervisor License. You need to install the Nexus1000V Multi-Hypervisor License for Cisco VSG for Microsoft Hyper-V. The Cisco N1kv VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Nexus1000V Multi-Hypervisor License and change the VSM mode to advanced mode. When the Nexus1000V Multi-Hypervisor License is installed, the license for Cisco VSG is automatically included.

Note If you try to access VSG services with VSM in essential mode, an error message is generated on VSM console indicating that the Nexus1000V Multi-Hypervisor License is required for VSG.

Starting with Release 5.2(1)SM1(5.2), Cisco Nexus1000V Multi-Hypervisor License is available in three different types:

- Default: The Nexus 1000v switch may be configured in Essential or Advanced mode.
  - Essential Mode: Not Supported.
  - Advanced Mode: After upgrade to Software Release 5.2(1)SM(5.2) or later- Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

    Note You must install either the evaluation or the permanent (MSFT PKG) license prior to upgrading to the Software Release 5.2(1)SM1(5.2) or later.

- Evaluation: The Nexus 1000V switch should be in Advanced mode. After upgrading to Software Release 5.2(1)SM1(5.2) or later - Nexus1000V Multi-Hypervisor License is available with1024 Socket Count and expires in 60 days.

- Permanent: The Nexus 1000V switch should be in Advanced mode. After upgrading to Software Release 5.2(1)SM1(5.2) or later - Nexus1000V Multi-Hypervisor License is available with 1024 Socket Count and expires in 60 days.

Note You have to request for an evaluation or permanent Nexus1000V Multi-Hypervisor License.

For more information about the Cisco Nexus 1000V for Microsoft Hyper-V licenses, see the *Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide*.

VLAN Configuration Requirements for VSG

You must have two port-profiles configured on two different VLANs in the VSM:

- Service interface VLAN
- HA interface VLAN

Required Cisco Prime NSC and Cisco VSG Information

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

Type	Your Information
Cisco VSG name—Unique within the inventory folder and up to 80 characters	
Hostname—Where the Cisco VSG will be installed in the inventory folder	
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 PNSC instance IP address	
Mode for installing the Cisco VSG	• Standalone • HA primary • HA secondary
Cisco VSG VLAN number • Service (1) • Management (2) • High availability (HA) (3)	

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

Host Requirements

- Microsoft SCVMM 2012 R2 or Microsoft SCVMM 2016
- Windows Server 2012 R2 or Windows Server 2016
- 6 GB RAM

Obtaining Cisco Prime NSC and Cisco VSG Software

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

http://software.cisco.com/download/navigator.html

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

http://software.cisco.com/download/navigator.html

Task 1: Installing the Cisco Prime NSC from an ISO Image

Before you begin

Ensure that you have:

- Verified that the Hyper-V host on which to deploy Cisco PNSC VM is available in SCVMM.

- Copied the Cisco PNSC 3.4 ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose **Library** > **Library Servers**, right-click the library location, and then refresh.
- NTP server information.

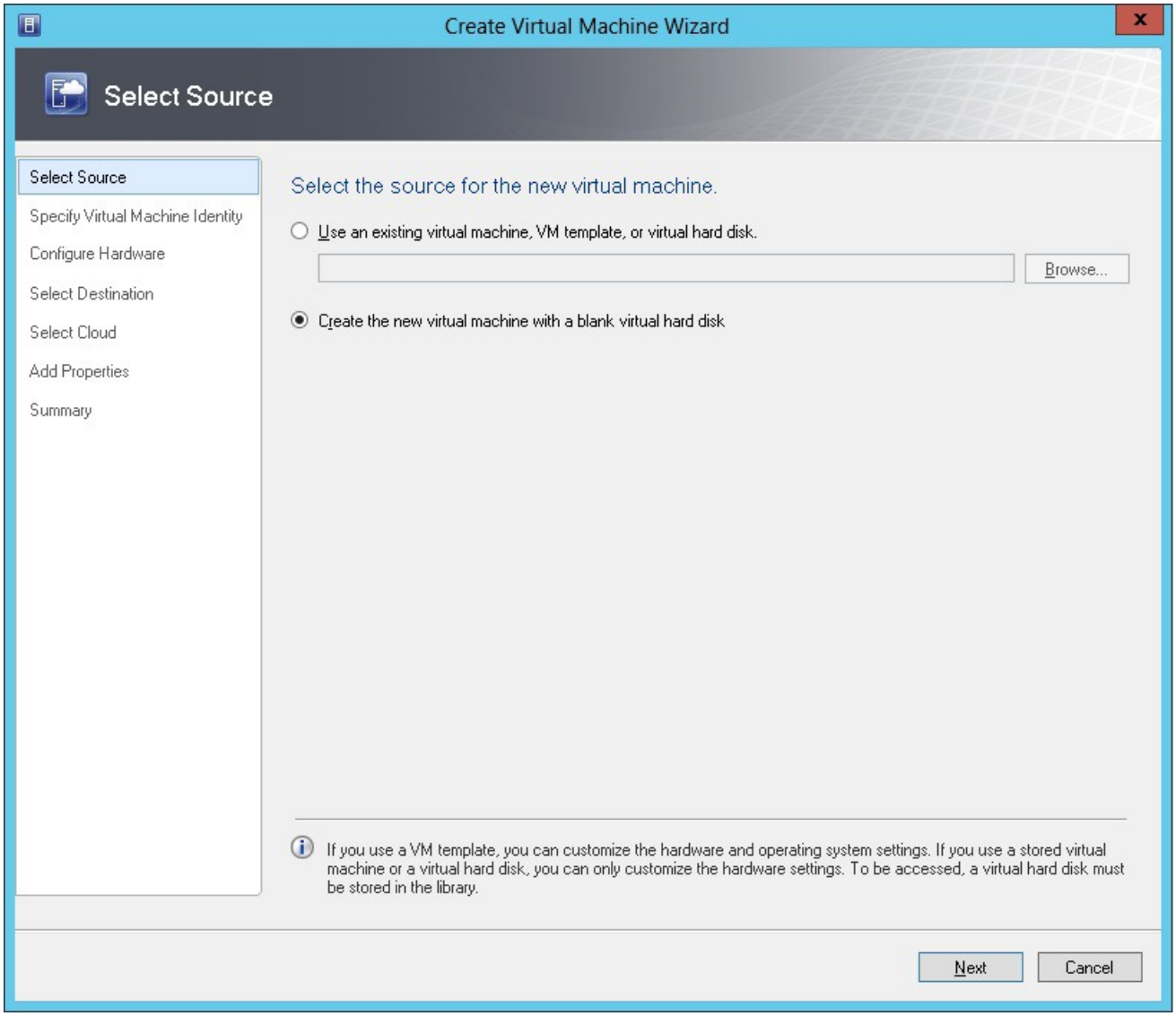
SUMMARY STEPS

1. Launch the SCVMM.
2. In the **VMs and Services** pane, choose the Hyper-V host on which to deploy the Cisco PNSC 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, choose the **Create the new virtual machine with a blank virtual hard disk** radio button, and then click **Next.**
5. In the **Specify Virtual Machine Identity** screen, Specify the name and description for the virtual machine, and 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, and then click **Next.**
9. In the **Configure Settings** screen, click **Browse** and navigate to the storage location of virtual machine file, and then click **Next.**
10. In the **Add properties** screen, choose the **Red Hat Enterprise Linux 5 (64 bit)** operating system, and then click **Next.**
11. In the **Summary** screen, do the following:
12. After the VM is successfully created, right-click the new Virtual Machine and choose **Connect or View > Connect Via Console**.
13. Launch the console and install Cisco PNSC.
14. After Cisco PNSC is successfully deployed, click **Close** and power on the Cisco PNSC VM.

DETAILED STEPS

Step 1 Launch the SCVMM.

Figure 6: Create Virtual Machine Wizard - Select Source



Step 2 In the **VMs and Services** pane, choose the Hyper-V host on which to deploy the Cisco PNSC 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, choose the **Create the new virtual machine with a blank virtual hard disk** radio button, and then click **Next.**

Step 5 In the **Specify Virtual Machine Identity** screen, Specify the name and description for the virtual machine, and 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.
- Choose **Memory** and choose the required memory value. You will need a minimum 4 GB of memory.

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

- Choose the hard disk with the virtual machine name you specified and enter the required size of the hard disk. You will need at least 20 GB.
- Click **New** > **Disk** to add a new hard disk, enter hard disk name in the **File Name** field, set the hard disk size to 20 GB and click **Ok**.
- Choose **Virtual DVD Drive**, choose the **Existing ISO image file** radio button, and browse to select the Cisco PNSC 3.4 ISO image file from the library in the **Select ISO** dialog box.

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

b) From the **Destination** drop-down list, choose **All hosts**.

c) Click **Next.**

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

Step 9 In the **Configure Settings** screen, click **Browse** and navigate to the storage location of virtual machine file, and then click **Next.**

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

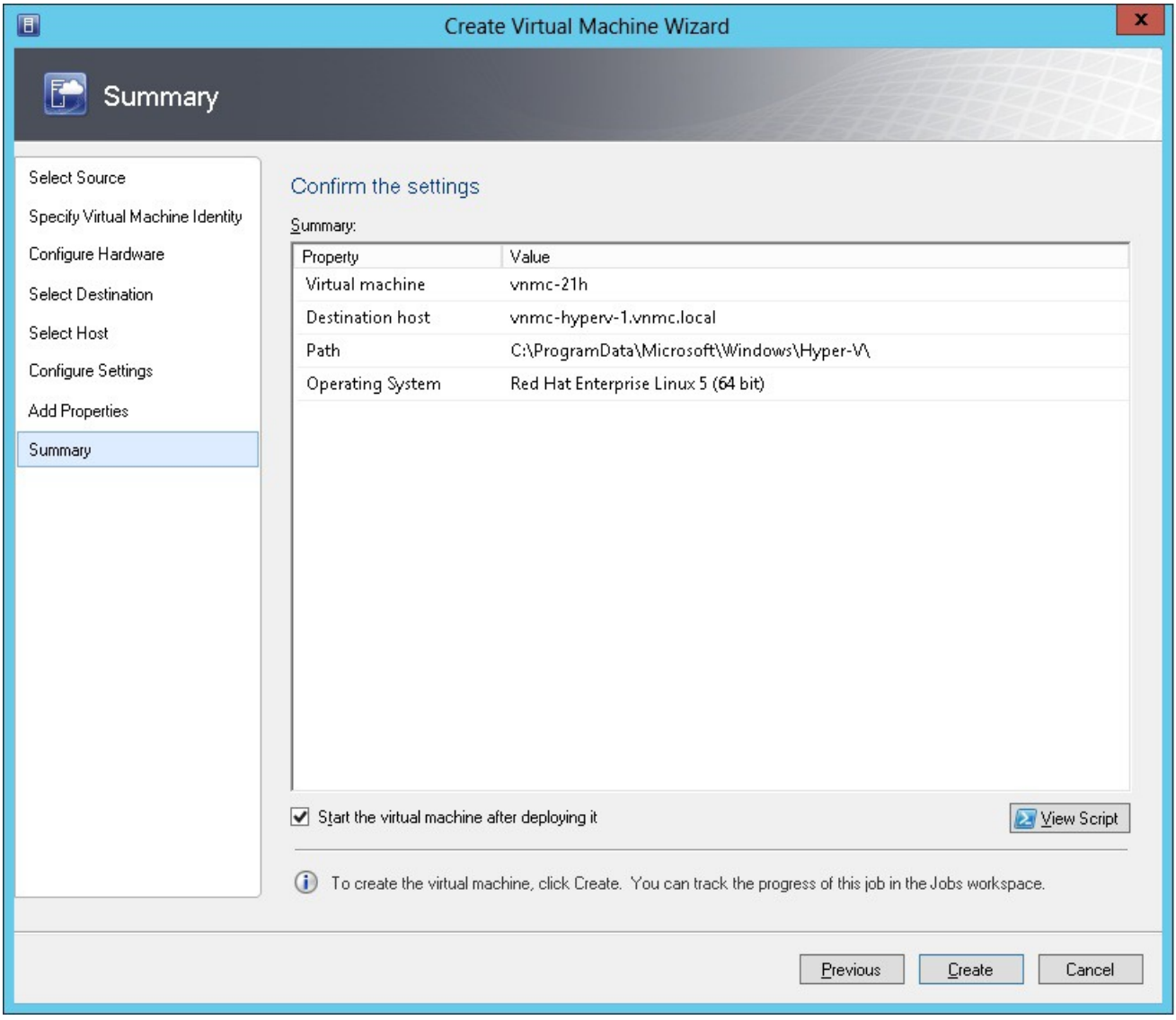
Step 11 In the **Summary** screen, do the following:

a) Verify the settings.

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

c) Click **Create.**

Figure 7: Create Virtual Machine Wizard - Summary



The job Create VM 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 VM is successfully created, right-click the new Virtual Machine and choose **Connect or View > Connect Via Console**.

Step 13 Launch the console and install Cisco PNSC.

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

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

Task 2: On the VSM, Configuring Cisco Prime NSC Policy Agent

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

Before you begin

Ensure that you have:

- Cisco PNSC policy-agent image on the VSM (for example, vsmhv-pa.3.2.1e.bin)

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

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

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

Note VSM clock should be synchronized with Cisco PNSC clock.

SUMMARY STEPS

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

DETAILED STEPS

Step 1 On the VSM, enter the following commands:

```
vsm# configure terminal
vsm(config)# nsc-policy-agent
vsm(config-nsc-policy-agent)# registration-ip 10.193.75.95
vsm(config-nsc-policy-agent)# shared-secret Example_Secret123
vsm(config-nsc-policy-agent)# policy-agent-image vsmhv-pa.3.2.1e.bin
vsm(config-nsc-policy-agent)# exit
vsm(config)# copy running-config startup-config
vsm(config)# exit
```

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

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1e)-vsm
vsm
```

The VSM is now registered with Cisco PNSC.

Example

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

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

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

```
vsm# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

Task 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 Cisco VSG data port profile and the Cisco VSG-ha port profile.

Before you begin

Ensure that you have:

- Logical Switch name (Network Uplink port-profile name).
- VLAN ID for the Cisco VSG data interface (for example,100).
- VLAN ID for the Cisco VSG-ha interface (for example, 200).
- 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. Cisco VSG data interface should be in the system VLAN. To configure VSG data interface in the system VLAN, you need a system network segment, a system port-profile, and an uplink configured as a system uplink. Use the **configure** command to enter global configuration mode.

2. Create Network Uplink port-profile and use it in the Logical Switch.
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. Cisco VSG data interface should be in the system VLAN. To configure VSG data interface in the system VLAN, you need a system network segment, a system port-profile, and an uplink configured as a system uplink. Use the **configure** command to enter global configuration mode.

Important Ensure that all the critical VMs are configured in the system VLANs.

```
vsm# configure
```

Step 2 Create Network Uplink port-profile and use it in the Logical Switch.

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

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

vsm(config)# nsm ip pool template pool-vmk-n
vsm(config-ip-pool-template)# address family ipv4
vsm(config-ip-pool-template)# network 90.90.90.0/24
vsm(config-ip-pool-template)# ip address 90.90.90.2 90.90.90.100
vsm(config-ip-pool-template)# default-router 90.90.90.1
vsm(config-ip-pool-template)# exit

vsm(config)#port-profile type ethernet sys-uplink
vsm(config-port-prof)#channel-group auto
vsm(config-port-prof)#no shutdown
vsm(config-port-prof)#system port-profile
vsm(config-port-prof)#state enabled
vsm(config-port-prof)#exit

vsm(config)# nsm network uplink vsm_Uplink
vsm(config-uplink-net)# allow network segment pool vsm_NetworkSite
vsm(config-uplink-net)# import port-profile sys_Uplink
vsm(config-uplink-net)# system network uplink
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)# system network segment
vsm(config-net-seg)# switchport access vlan 502
vsm(config-net-seg)# ip pool import 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)# system port-profile
```

```
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)# ip pool import 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: On the VSM, Configuring Virtual Network Adapters on the Hosts

Now that you have prepared Cisco VSG port profiles on VSM, you should configure virtual network adapters on the hosts.

This task includes the following subtasks:

- Create Port-profile for the Virtual Network Adapter, on page 21
- Creating Virtual Network Adapter, on page 22

Before you begin

Ensure that you have:

- Cisco VSG port-profile configured on VSM.

Create Port-profile for the Virtual Network Adapter

You need to log in to VSM to create port-profile for the virtual network adapter.

SUMMARY STEPS

1. Create port-profile for the virtual network adapter in VSM.

DETAILED STEPS

Create port-profile for the virtual network adapter in VSM.

Example:

```
vsm#configure terminal
vsm(config)#port-profile type vethernet Virtual-Net-PP
```

```
vsm(config-port-prof)#capability l3-vservice
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#copy running-config startup-config
```

Creating Virtual Network Adapter

Before you begin

Make sure that you know the following:

- Port-profile for virtual network adapter is created.

Step 1 Launch SCVMM.

Step 2 In the **VMs and Services** tab, click **All Hosts**.

Step 3 Choose the host on which you want to add the virtual network adapter.

Step 4 Right-click the host and choose **Properties** from the pop-up menu.

Step 5 In the **Properties** window, click **Virtual Switches**.

Step 6 On the **Virtual Switches** tab, click **New Virtual Network Adapter**.

Step 7 In the **Name** field, enter name of virtual network adapter.

Step 8 Under the **Connectivity**, in the **VM Network** field, choose an appropriate VM network.

Step 9 Under **Port profile**, select L3 service enabled port-profile that you created from the **Classification** drop-down list.

Step 10 Under **IP address configuration**, check **Static** radio-button and do the following:

a) Choose IP-pool for virtual network adapter from the **IPv4 pool** drop-down list.
b) In the **IPv4 address** field, enter IP address for virtual network adapter.

Step 11 Click **Ok**.

Step 12 The VM manager warning message appears, click **Ok**.

What to do next

Add a physical router between VSG and virtual network adapter.

Task 5: Installing Cisco VSG from an ISO Image

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

Before you begin

Ensure that you have:

- Installed Microsoft SCVMM 2012 R2 or Microsoft SCVMM 2016.
- Downloaded the Cisco VSG ISO image and uploaded it to the server (C:\ProgramData\Virtual Machine Manager Library Files\ISO). Refresh the library server under the Library tab.
- Cisco VSG-Data port profile: VSG-Data.
- Cisco VSG-ha port profile: VSG-ha.
- HA ID.
- IP/subnet mask/gateway information for Cisco VSG
- Administrator password
- Minimum of 2 GB RAM and 3 GB hard disk space, recommended space is 4 GB RAM and 4 GB hard disk.
- Cisco PNSC IP address.
- The shared secret password.
- IP connectivity between Cisco VSG and Cisco PNSC is okay.
- Cisco VSG NSC-PA image name (vnmc-vsgpa.2.1.2a.bin) is available.

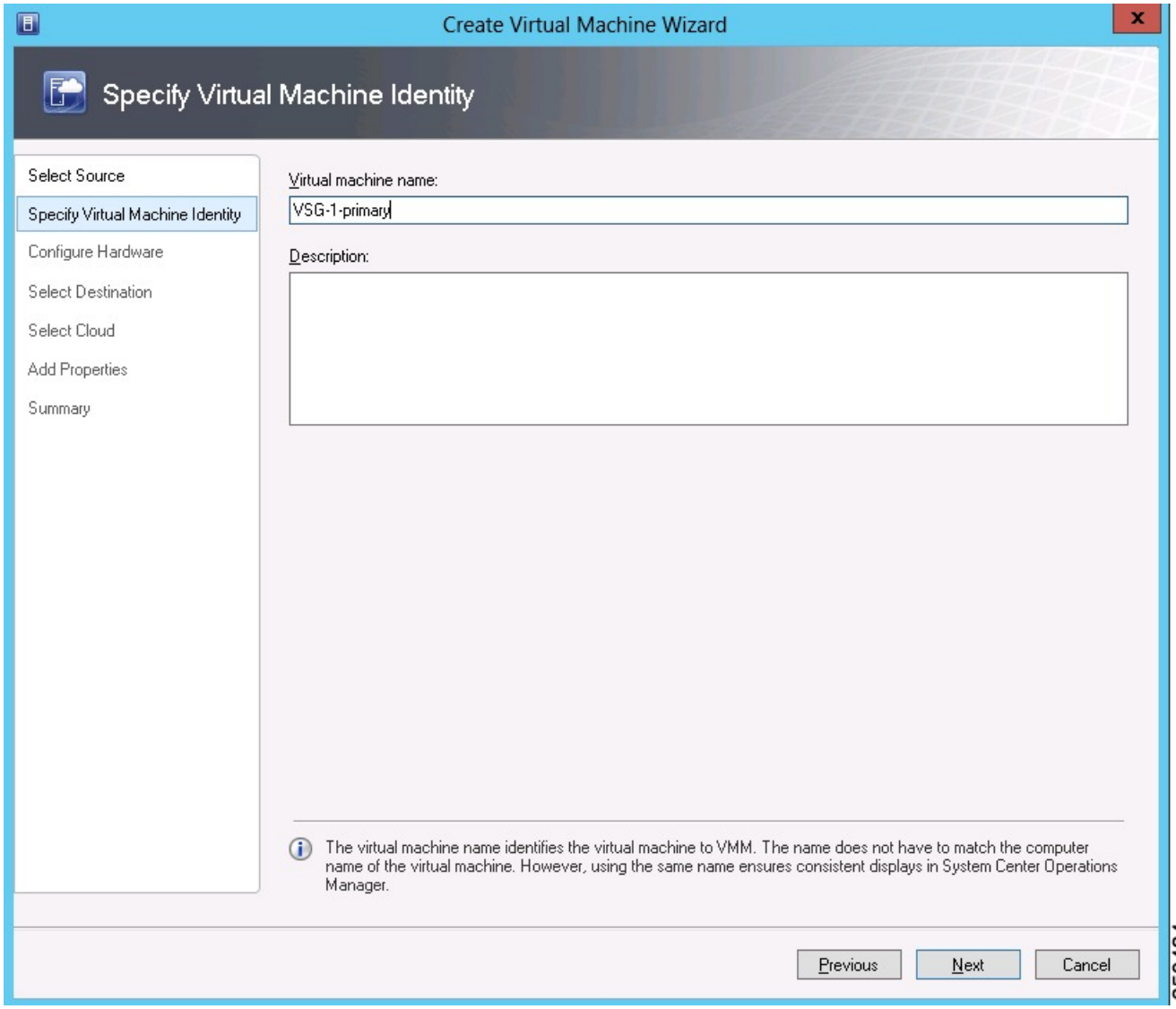
Step 1 Launch SCVMM.

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

Step 3 In the Create Virtual Machine Wizard, in the **Select Source** screen, check the **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 8: Create Virtual Machine Wizard - Specify Virtual Machine Identity



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

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

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

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

d) Click **New** > **Network Adapter** to create a total of three new Network Adapters.

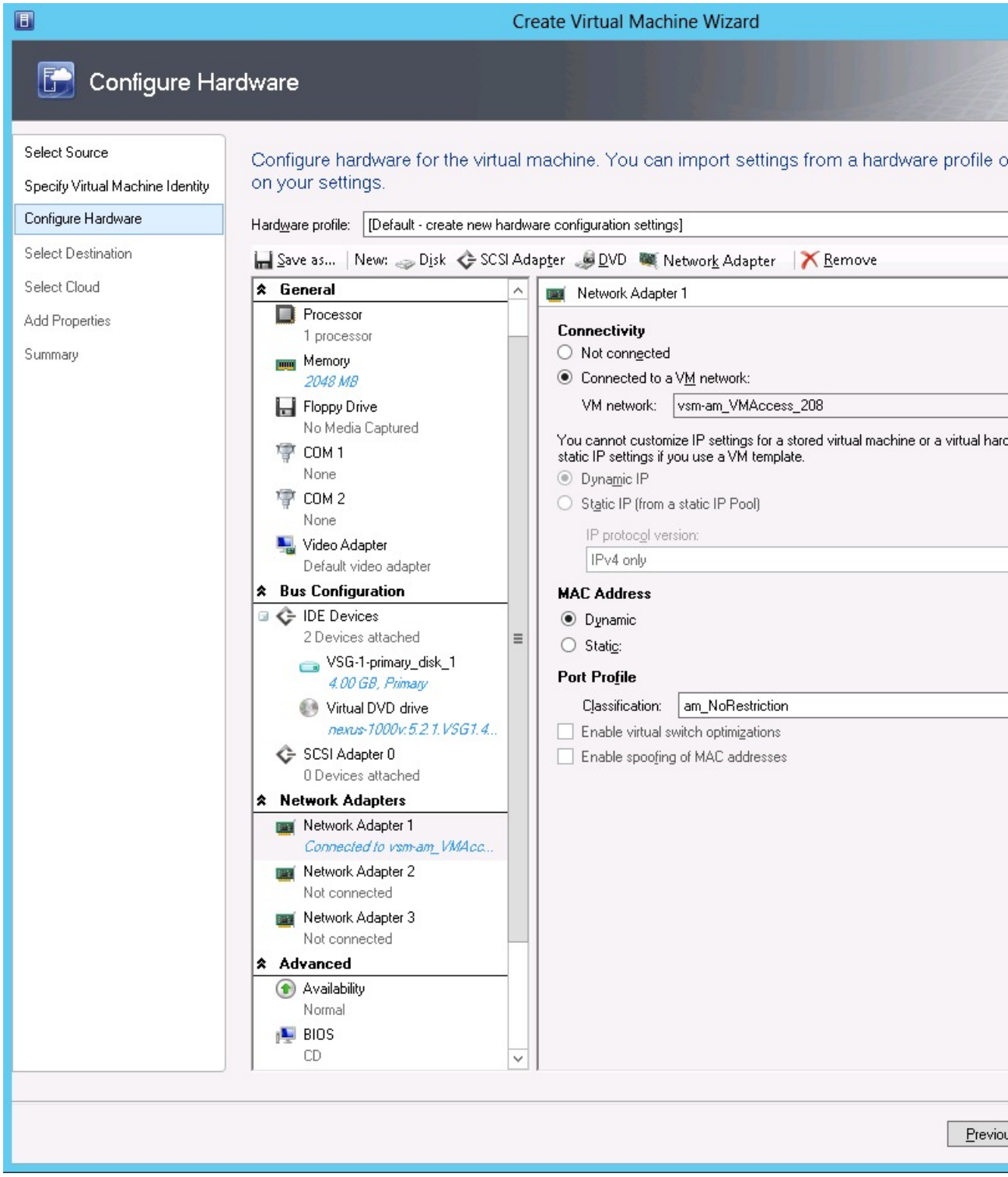
- Under the **Network Adapters** section, choose **Network Adapter 1**, and then choose **Connected to a VM network** and browse for the appropriate network that corresponds to the network segment for the VSG's data interface.

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 9: Create Virtual Machine Wizard - Configure Hardware



- From the **Classification** drop-down list, choose the port-profile corresponding to the VSG's data interface.

Note Repeat Step d to create network adapters for management and HA.

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

Step 7 In the **Select Host** section, choose the host that you want to place the VSG on and click **Next.**

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, choose the **Other Linux (64-bit) from the Operating System** from the drop-down list, and then click **Next.**

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

Step 11 Once the VSG is successfully installed, choose the VSG on the **VMs and Services** tab, and click **Power On**.

Step 12 Connect to the VSG using **Connect or View** > **Connect via Console**.

Task 6: On the VSG, Configuring the Cisco Prime NSC Policy Agent

Once Cisco PNSC is installed, you must register Cisco VSG with Cisco PNSC.

Before you begin

Ensure that you have:

- The Cisco PNSC policy-agent image on Cisco VSG (for example, vnmc-vsgpa.2.1.2a.bin).

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

- IP address of the Cisco PNSC.
- Shared secret password you defined during the Cisco PNSC installation.
- IP connectivity between the VSG and the Cisco PNSC.

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

Note VSG clock should be synchronized with Cisco PNSC clock.

SUMMARY STEPS

1. On Cisco VSG, configure the NSC policy agent:

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

DETAILED STEPS

Step 1 On Cisco VSG, configure the NSC policy agent:

```
VSG-Firewall# configure
Enter configuration commands, one per line.  End with CNTL/Z.
VSG-Firewall(config)# nsc-policy-agent
VSG-Firewall(config-nsc-policy-agent)# registration-ip 10.193.72.242
VSG-Firewall(config-nsc-policy-agent)# shared-secret Sgate123
VSG-Firewall(config-nsc-policy-agent)# policy-agent-image vnmc-vsgpa.2.1.2a.bin
VSG-Firewall(config-nsc-policy-agent)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
VSG-Firewall(config-nsc-policy-agent)# exit
```

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

```
VSG-Firewall(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(2a)-vsg
```

Cisco VSG is now registered with Cisco PNSC.

Example

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

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

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

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Not Installed
```

Task 7: On Cisco VSG, Cisco VSM, and Cisco PNSC, Verifying the NSC Policy-Agent Status

You can use the **show nsc-pa status** command to verify the nsc policy-agent status on Cisco VSG, Cisco VSM, and Cisco Prime NSC (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 NSC-PA configuration by entering the following command:

3. Log in to the Cisco VSM.
4. Check the status of NSC-PA configuration by entering the following command:
5. Log in to Cisco PNSC.
6. Click **Resource Management** and then click **Resources**.
7. In the **navigation** pane, click **VSMs** and verify the VSM information in the **VSMs** pane.
8. In the **navigation** pane, click **VSGs** and verify the VSG information in the **VSGs** pane.

DETAILED STEPS

Step 1 Log in to the Cisco VSG.

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

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(2a)-vsg
vsg#
```

Step 3 Log in to the Cisco VSM.

Step 4 Check the status of NSC-PA configuration by entering the following command:

```
VSM# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1e)-vsm
VSM#
```

Step 5 Log in to Cisco PNSC.

Step 6 Click **Resource Management** and then click **Resources**.

Step 7 In the **navigation** pane, click **VSMs** and verify the VSM information in the **VSMs** pane.

Step 8 In the **navigation** pane, click **VSGs** and verify the VSG information in the **VSGs** pane.

Task 8: On Cisco PNSC, Configuring a Tenant, Security Profile, Compute Firewall, and Assigning Cisco VSG to the Compute Firewall

Now that you have Cisco PNSC and Cisco VSG successfully installed with the basic configurations, you should configure the basic security profiles and policies.

This task includes the following subtasks:

- Configuring a Tenant on Cisco Prime NSC, on page 30
- Configuring a Security Profile on the Cisco Prime NSC, on page 30
- Configuring a Compute Firewall and Assigning Cisco VSG to Cisco Prime NSC, on page 31

What to do next

Go to Configuring a Tenant on Cisco Prime NSC, on page 30

Configuring a Tenant on Cisco Prime NSC

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 Cisco PNSC.

SUMMARY STEPS

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

DETAILED STEPS

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

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

Step 3 In the **Create Tenant** dialog box, 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 that you have just created is listed in the left-side pane under root.

What to do next

See Configuring a Security Profile on the Cisco Prime NSC, on page 30

Configuring a Security Profile on the Cisco Prime NSC

You can configure a security profile on Cisco PNSC.

Step 1 In the Cisco PNSC toolbar, click the **Policy Management**>**Service Profiles**.

Step 2 In the **Root** navigation window, from the directory path, choose **Tenant** > **Compute Firewall** > **Compute Security Profile**.

Step 3 Right-click **Compute Security Profile** and choose **Add Compute Security Profile**.

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

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

See Configuring a Compute Firewall and Assigning Cisco VSG to Cisco Prime NSC, on page 31

Configuring a Compute Firewall and Assigning Cisco VSG to Cisco Prime NSC

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

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

Step 2 On the left-pane directory tree, navigate to choose a tenant.

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

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 **Host Name** field, enter the name for your Cisco VSG.

Step 5 Click **Next**.

The new Compute Firewall pane displays with the information that you provided.

Step 6 In the **Select Service Devices** pane, choose **Assign VSG** radio button, from the **VSG Devices** drop-down, choose a VSG. then and click **Next**.

Step 7 In the **Interface** tab, **Configure Data Interface** pane, enter data interface (data0) IP address and subnet mask, and click **Next**.

Step 8 Verify the configuration in **Summary** tab and click **Finish**.

Step 9 Click **Root** > **Tenant** > **Network Services** and verify the status of the firewall.

Task 9: On the Prime NSC, Configuring a Permit-All Rule

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

Step 1 Log in to the Cisco PNSC.

Step 2 Choose **Policy Management** > **Service Profiles**.

Step 3 Choose **Root** > **Tenant** > **Compute Firewall** > **Compute Security Profile**, and then select a security profile.

Step 4 In the right pane, click **Add ACL Policy Set**.

Step 5 In the **Add ACL 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) Click **Add ACL Policy**.

Step 6 In the **Add ACL Policy** dialog-box, enter the policy name, enter policy description, and then click **Add Rule**.

Step 7 In the **Add Rule dialog** box, do the following:

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

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

The newly created policy is displayed in the **Assigned** field.

Step 9 In the **Add Policy Set** dialog box, click **OK**.

Step 10 In the **Service Profile** window, click **Save**.

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

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

```
vsg# show running-config rule
rule POL-DEMO/R-DEMO@root/Tenant/VDC
cond-match-criteria: match-allaction permit
rule POL1/R1@root/Tenant/VDC
cond-match-criteria: match-allaction permit
rule default/default-rule@root
cond-match-criteria: match-allaction drop
vsg#
```

Task 11: Enabling Logging

To enable logging follow these procedures:

- Enabling Logging level 6 for Policy-Engine Logging, on page 32
- Enabling Global Policy-Engine Logging, on page 33

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 Cisco PNSC.

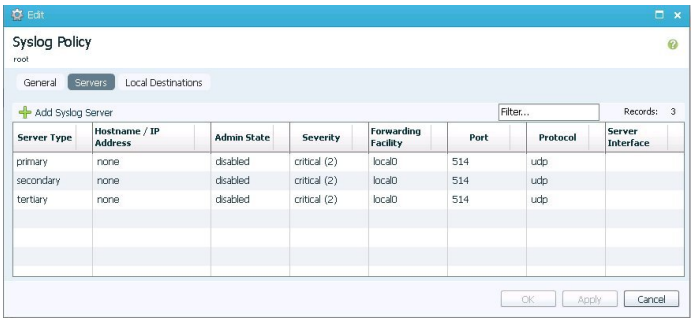
Step 2 Choose **Policy Management** > **Device Configurations**.

Step 3 In the **Navigation** pane, choose **root** > **Policies** > **Syslog** > **Default**, and then click **Edit**.

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

a) Click the **Servers** tab.
b) In the **Server Type** column, choose the **primary** server type from the displayed list.
c) From the pane toolbar, click **Edit.**

Figure 10: Edit Syslog Dialog Box



Step 5 In the **Edit Syslog Client** 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

See Enabling Global Policy-Engine Logging, on page 33.

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.

Step 1 Log in to Cisco PNSC.

Step 2 In the **Cisco Prime NSC** window, choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles** > **default**. The **default** Device Profile window opens.

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

a) In the **Work** pane, click the **General** tab.
b) In the **Policy Engine Logging** field, check the **Enabled** radio button.

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:

Before you begin

Ensure that you have:

- Server VM that runs with an access port profile (for example, web server)
- Cisco VSG data IP address (for example, 10.10.10.200) and VLAN ID (for example, 100)
- Set up the Virtual Network Adapter
- Security profile name (for example, sp-web)
- Organization (Org) name (for example, root/Tenant-A)
- Port profile that you would like to edit to enable firewall protection

Enabling Traffic VM Port-Profile for Firewall Protection

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

SUMMARY STEPS

1. Create VSG node.
2. Create the network segment and Traffic VM Port-Profile for Firewall Protection.

DETAILED STEPS

Step 1 Create VSG node.

```
vsm#configure terminal
vsm (config)# vservice node VSG type vsg
vsm (config-vservice-node)# ip address 10.10.10.200
vsm (config-vservice-node)# adjacency l3
vsm (config-vservice-node)# exit
vsm (config)# copy running-config startup-config
```

Step 2 Create the network segment and 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)# ip pool import 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 name pp-webserver
```

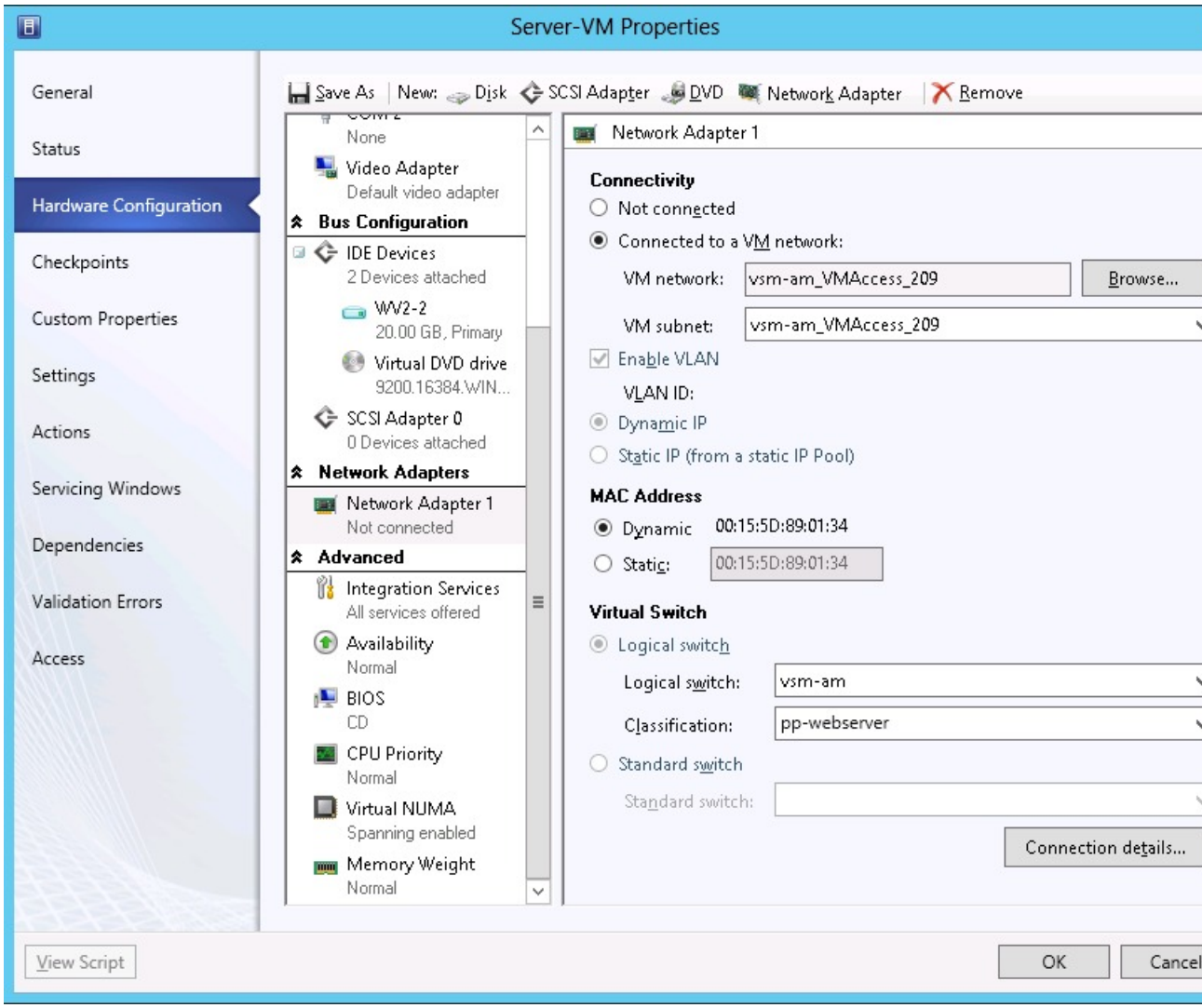
What to do next

See Verifying the VSM or VEM for Cisco VSG Reachability, on page 35.

Verifying the VSM or VEM for Cisco VSG Reachability

Ensure that you have assigned the traffic VM port profile with firewall protection to the traffic VM.

Figure 11: Virtual Machine Properties Window



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

```
VSM# show vservice brief
------------------------------------------------------------------------------
                                Node Information
------------------------------------------------------------------------------
 ID Name                    Type    IP-Address      Mode    State   Module
  1 VSG-1                   vsg     192.161.0.85    l3      Alive   3,4,

------------------------------------------------------------------------------
                                Path Information
------------------------------------------------------------------------------
------------------------------------------------------------------------------
                                Port Information
------------------------------------------------------------------------------
PortProfile:PP-VSERVICE
Org:root/Tenant1
Node:VSG-1(192.161.0.85)                    Profile(Id):SP1(6)
Veth Mod VM-Name                            vNIC IP-Address
```

```
   4    4 traffic-vm-win-22                       192.163.0.53,
   8    3 traffic-vm-win-12                       192.163.0.76
  10    3 traffic-vm-ubuntu-61                    192.163.0.80,
  11    3 traffic-vm-ubuntu-52                    192.163.0.52,
```

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

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 port-profile VSGDemo-WEB-FW
--------------------------------------------------------------------------------
                                  Port Information
--------------------------------------------------------------------------------
PortProfile:VSGDemo-WEB-FW
Org:root/Demo
Node:VSG(153.1.1.13)                          Profile(Id):Demo-Default-Security-Profile(6)
Veth Mod VM-Name                              vNIC IP-Address
   1    3 web-server1                              152.1.1.11,
```

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

Task 13: Installing Microsoft Service Provider Foundation

After installing Cisco Prime NSC, you need to enable communication between the Prime NSC and Microsoft SCVMM. This is required for virtual machine attribute based policies to work on VSG. Microsoft Service Provider Foundation (SPF) is a plugin that enables communication between Microsoft SCVMM and Cisco Prime NSC. The following table lists the SPF versions compatible with Cisco Prime NSC 3.4:

Table 1: SPF versions compatible with Cisco Prime NSC 3.4

SCVMM Version	SPF Version
System Center 2012 Service Pack 1	7.1.3117.0
System Center 2016	7.2.379.0

This task includes the following subtasks:

- Installing Service Provider Foundation, on page 38
- Configuring Service Provider Foundation, on page 38
- Verifying Service Provider Foundation Installation, on page 39
- Creating VM Manager on Cisco Prime NSC, on page 39

What to do next

See Installing Service Provider Foundation, on page 38

Installing Service Provider Foundation

For detailed information about installing Service Provider Foundation, see *How to Install Service Provider Foundation for System Center 2012 R2* or *How to Install Service Provider Foundation for System Center 2016* available at: http://technet.microsoft.com/en-us/library/dn266007.aspx.

Before you begin

Ensure that you have:

- Downloaded install system center 2012 R2 or 2016 orchestrator based on your requirement.
- Verified the system requirements for Service Provider Foundation (SPF). For information on system requirements, refer to *System Requirements for Service Provider Foundation for System Center 2012 SP1* or *System Requirements for Service Provider Foundation for System Center 2016* , available at: http://technet.microsoft.com/en-us/library/jj642899.aspx.
- NTP server information.

Configuring Service Provider Foundation

After the Service Provider Foundation (SPF) is successfully installed, you need to a create stamp ID (stampId) and associate it with the Microsoft SCVMM server. For more information about configuring SPF, see http://technet.microsoft.com/en-us/library/jj613915.aspx.

Before you begin

See Verifying Service Provider Foundation Installation, on page 39

Step 1 Open a **Windows** powers shell.

Step 2 Run **import-module spfadmin**.

Step 3 Enter **$server = New-SCSPFServer -Name** *"scvmm server"* **-ServerType VMM**

This is the server name that is displayed in the login window.

Step 4 **$tenant = New-SCSPFTenant -Name** *"tenant-name"*

Step 5 $tenant = New-SCSPFTenant -Name "<tenant-name>"

Enter the VM name as the tenant name.

Step 6 **$stamp = New-SCSPFStamp -Name "Stamp" -Servers $server**

Step 7 **Set-SCSPFStamp -Stamp $stam -Tenants $tenant**

Verifying Service Provider Foundation Installation

To check if the SPF installation is successful and functional, launch the following VMM REST interface web link:

`https://<spf_host>:8090/SC2016R2/VMM/Microsoft.Management.Odata.Svc`

where <spf_host> is the IP address for the Microsoft SCVMM VM.

Use the following link to launch the Virtual Machines REST URL:

`https://<spf_host>:8090/SC2016R2/VMM/Microsoft.Management.Odata.Svc/VirtualMachines`

where <spf_host> is the IP address for the SCVMM VM.

Creating VM Manager on Cisco Prime NSC

You need to create a VM manager to enable Prime NSC to retrieve VM information from Microsoft SCVMM.

Step 1 Launch Cisco Prime NSC.

Step 2 Choose **Resource Management** > **VM Manager** > **Add VM Manager**.

Step 3 In the **Add VM Manager** dialog box, enter the following:

a) Name for VM manager.
b) Description for the VM manager
c) Hostname/IP address of SCVMM.
d) Domain-Name/User-name.
e) Password SCVMM host.
f) Keep the default Port Number.
g) Click **OK**.

Task 14: Sending Traffic Flow and on Cisco VSG Verifying Statistics and Logs

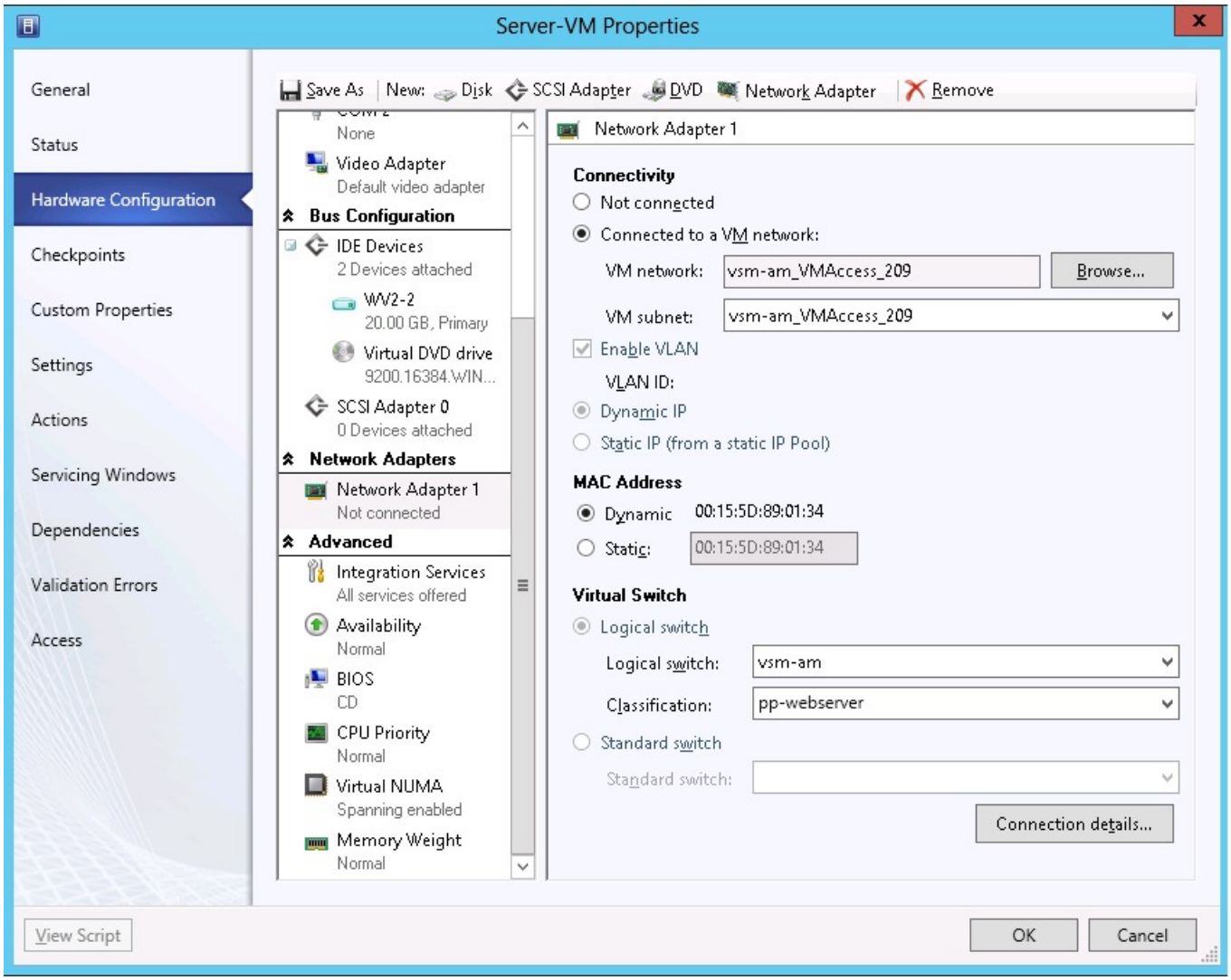
This section includes the following topics:

Sending Traffic Flow

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

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

Figure 12: Virtual Machine Properties Window



Step 2 Log in to any of your client virtual machine (Client-VM).

Step 3 Send traffic (for example, HTTP) to your Server-VM.

```
[root@]# wget http://172.31.2.92/
--2014-11-28 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

2014-11-28 13:38:40 (16.4 MB/s) - `index.html' saved [258/258]

[root]#
```

Step 4 Check the policy-engine statistics and log in to Cisco VSG.

In the Cisco VSG Layer 3 mode, IP fragmentation is not supported on the VEM virtual machine network interface card (vmnic) for traffic leaving the host. Hence, after vPath encapsulation, if an IP packet is received by a VEM from a virtual machine with a packet size greater than the outgoing interface MTU value, it will be dropped, and an ICMP error message (error code = 4) will be sent back to the source virtual machine. To avoid packet drops in this scenario, increase the outgoing server port MTU value by 94 bytes. For example, if the MTU values of client and server virtual machines and uplinks are all 1500 bytes, set the uplink MTU value to 1594 bytes

What to do next

See Verifying Policy-Engine Statistics and Logs on Cisco VSG, on page 41.

Verifying Policy-Engine Statistics and Logs on Cisco VSG

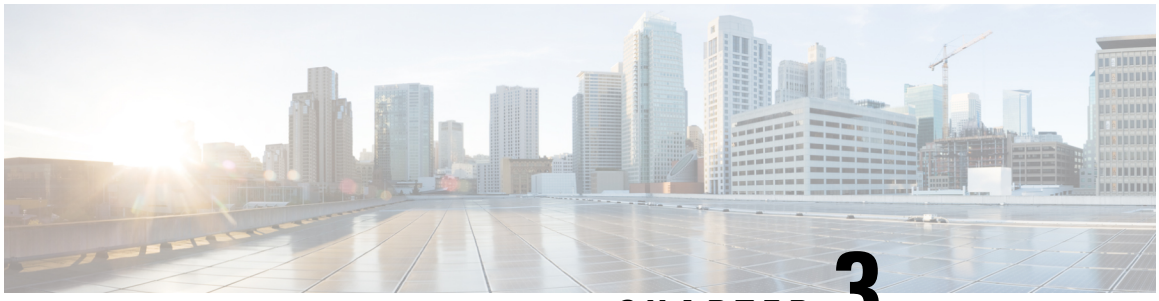
Log in to Cisco VSG and check the policy-engine statistics and logs.

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# 2014 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 Prime Network Services Controller

This chapter contains the following sections:

Information About the Cisco Prime NSC

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

Installation Requirements

Cisco Prime NSC System Requirements

Requirement	Description
Virtual Appliance	
Four virtual CPUs	1.8 GHz each
Memory	Minimum 4 GB RAM, recommended 4 GB RAM
Disk space	Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: • Disk 1: 20 GB • Disk 2: 20 GB

Requirement	Description
Management interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor
Microsoft Hyper-V	
Microsoft SCVMM 2016 R2	
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 23.0 • Chrome 29.0 **Note** If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website. **Note** Before using Google Chrome with Cisco PNSC, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Cisco PNSC.
Flash Player	Adobe Flash Player plugin (Version 11.2 or higher)

Note Before you can use Chrome with Prime NSC 3.2, 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.	—
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 Cisco PNSC ISO	
Name	
ISO file location	
Storage location	
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 PNSC management interface.	

Information Type	Your Information
IP address	
Subnet mask	
Gateway IP address	
Domain name	
DNS server	
Admin password	
Shared secret password for communications between the Cisco PNSC, Cisco VSG, and VSM.	
For Configuring Microsoft Hyper-V in Cisco PNSC	
HyperV name	
Description	
Hostname or IP address	

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 PNSC, 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 characteristics in this table:

Table 2: 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 PNSC, Cisco VSG, or VSM. If you do not set the correct time on the server, the Cisco PNSC CA certificate that is created when the Cisco PNSC VM is deployed might have an invalid time stamp.

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

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

Installing Cisco Prime NSC

Before you begin

- Verify that the Hyper-V host on which to deploy the Cisco PNSC VM is available in SCVMM.
- Copy the Cisco PNSC ISO image to the SCVMM library location on the file system. To make this image available in SCVMM, choose **Library > Library Servers**, right-click the library location, and then refresh.
- Set your keyboard to United State English before installing the Cisco PNSC and using the VM console.

- There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

Step 1 Launch the SCVMM.

Step 2 Choose the Hyper-V host on which to deploy the Cisco PNSC 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, choose 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 choose the number of processors.
- Choose **Memory** and choose the required memory value. You will need a minimum 4 GB of memory for Prime NSC.

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

- Choose **Hard Disk**, enter the required size of the hard disk. You will need a minimum of 20 GB of hard disk.
- Choose **Virtual DVD Drive**, check the **Existing ISO image file** radio button, and browse to choose theCisco PNSC 3.4 ISO image file.

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

d) Click **Next.**

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

a) Check 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, choose 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.**

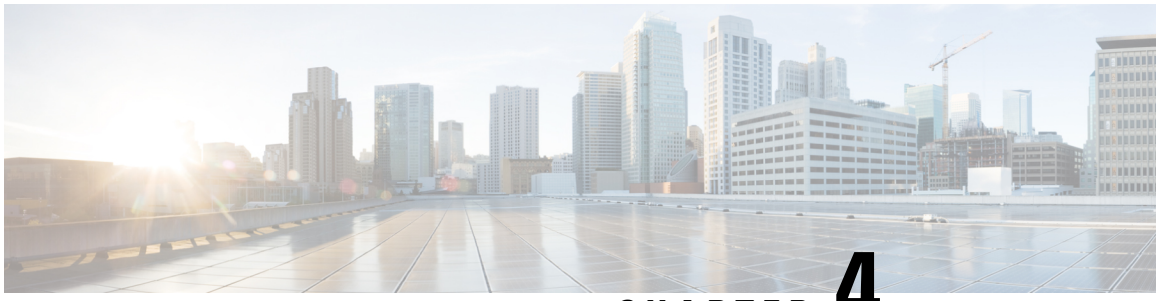
The job Create virtual machine starts. You can see the status of this job in The Recent Jobs window. Ensure that the job completes without any errors.

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 Cisco PNSC.

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

Step 14 After Cisco PNSC is successfully deployed, click **Close** and power on the Cisco PNSC 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 R2
- Virtual Machine (VM)
  - 64-bit VM is required.
  - x86 Intel or AMD server with a 64-bit processor.
  - 2 GB RAM, recommended space is 4 GB RAM.
  - 3 NICs.
  - Minimum 3 GB hard disk space with LSI Logic Parallel adapter (default), recommended space is 4 GB hard disk.
  - Minimum CPU speed of 1.5 GHz.

Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology

This table lists the terminology 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 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://software.cisco.com/download/navigator.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

Ensure that you have:

- Installed Microsoft SCVMM 2012 R2 or Microsoft SCVMM 2016.
- Downloaded the Cisco VSG ISO image and uploaded it to the server (C:\ProgramData\Virtual Machine Manager Library Files\ISO). Refresh the library server under the Library tab.
- Cisco VSG-Data port profile: VSG-Data.
- Cisco VSG-ha port profile: VSG-ha.
- HA ID.
- IP/subnet mask/gateway information for the Cisco VSG.
- Admin password.
- 2 GB RAM and 3 GB hard disk space.
- Cisco PNSC IP address.
- The shared secret password.
- IP connectivity between Cisco VSG and Cisco PNSC.
- Cisco VSG NSC-PA image name (vnmc-vsgpa.2.1.2a.bin).

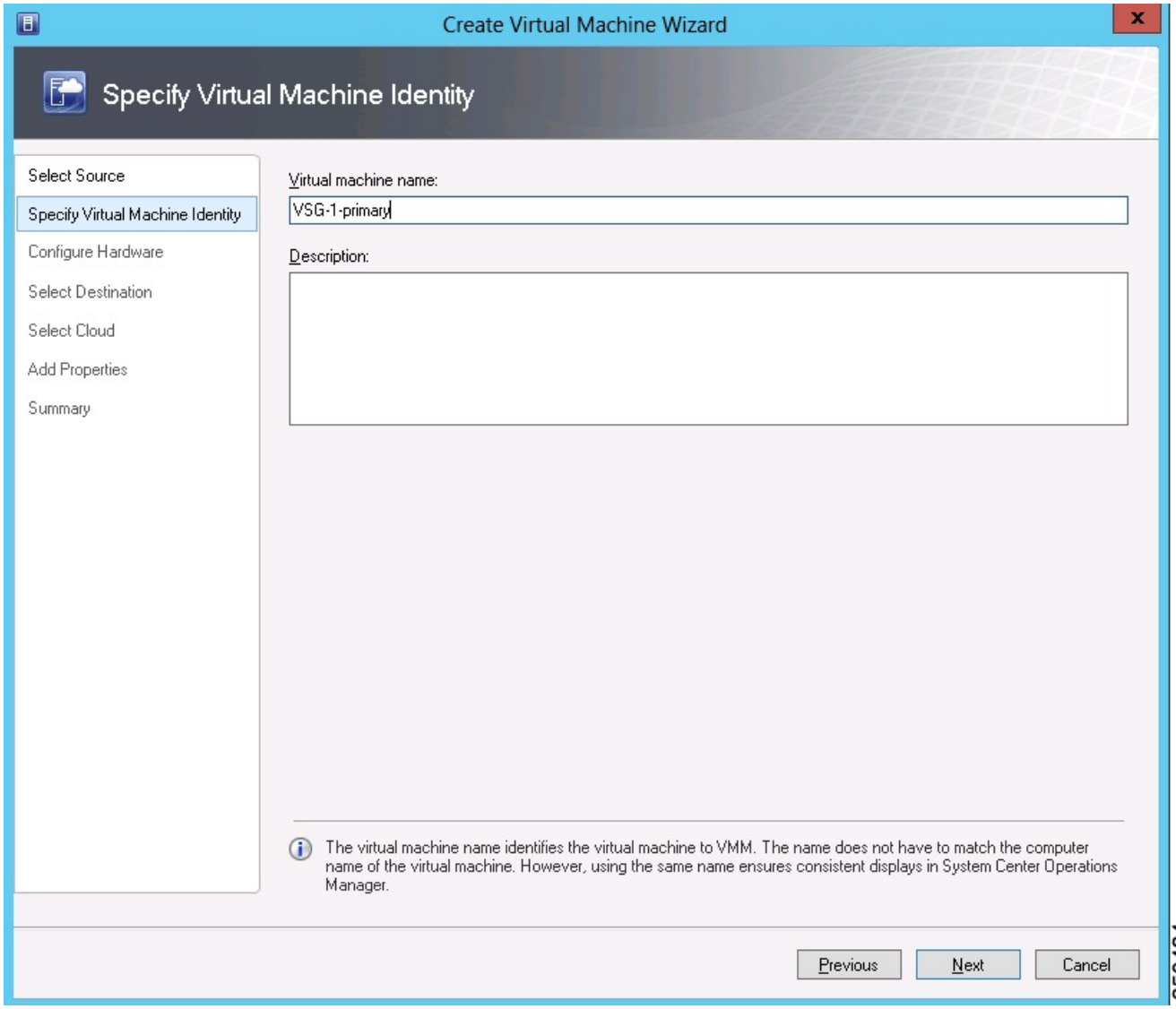
Step 1 Launch SCVMM.

Step 2 On 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 13: Create Virtual Machine Wizard - Specify Virtual Machine Identity



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

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

b) Under **Bus Configuration**, choose the primary disk and enter 3 in the Size (GB) field.

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

d) Choose the **Network Adapter** drop-down near the top of the Create Virtual Machine Wizard and create two new Network Adapters.

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

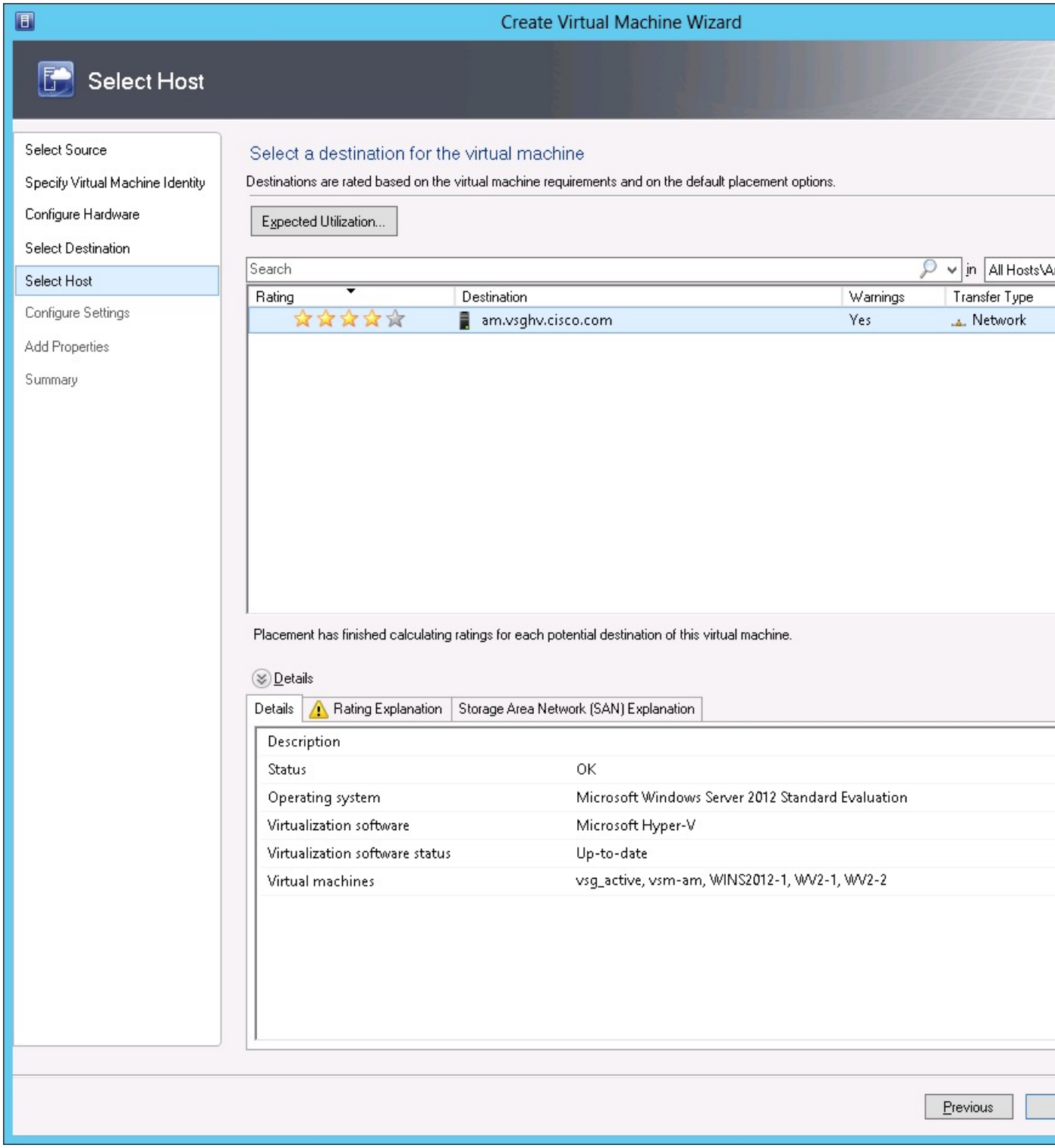
- From the **Classification** drop-down list, choose the port-profile corresponding to the VSG's data interface.

Note Repeat Step d to create network adapters for service interface.

Step 6 In the **Select Destination** section, choose **Place the virtual machine in a host** and choose 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 that you want to place the VSG on and click **Next.**

Figure 14: Create Virtual Machine Wizard - Select Host



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, choose **Other Linux (64-bit) from the Operating System** drop-down list, and then click **Next.**

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

Step 11 Choose the VSG in the **VMs and Services** tab and click **Power On**.

Step 12 Connect to the VSG using **Connect or View -> Connect via Console**.

Configuring Initial Settings

This section describes how to configure the initial settings on 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 60 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.

The 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 that 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 Prime NSC Policy Agent

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

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 PNSC policy-agent image is available on the VSG (for example, vnmc-vsgpa.2.1.2a.bin)

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

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

Note VSG clock should be synchronized with the Cisco PNSC clock.

Step 1 On the VSG, enter the following commands:

```
VSG-Firewall# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSG-Firewall(config)# nsc-policy-agent
VSG-Firewall(config-nsc-policy-agent)# registration-ip 10.193.72.242
VSG-Firewall(config-nsc-policy-agent)# shared-secret Sgate123
VSG-Firewall(config-nsc-policy-agent)# policy-agent-image vnmc-vsgpa.2.1.2a.bin
VSG-Firewall(config-nsc-policy-agent)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
VSG-Firewall(config-nsc-policy-agent)# exit
```

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

```
VSG-Firewall(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(2a)-vsg
```

The VSG is now registered with the Cisco PNSC.

Example

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

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

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

```
vsg# show nsc-pa status
NSC 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 this task:

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

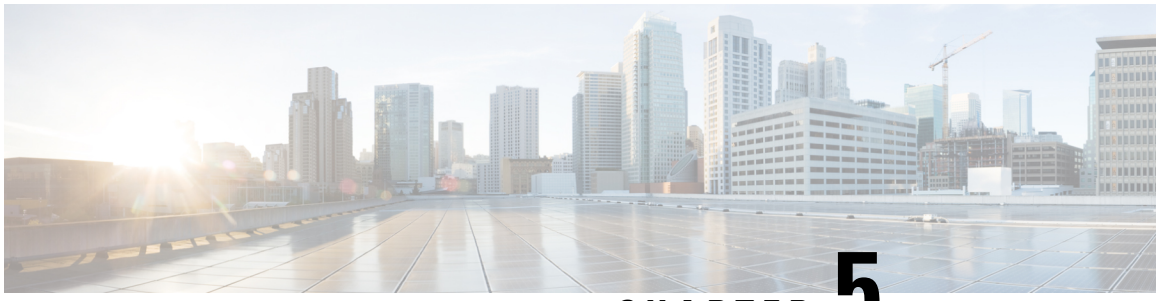
This example shows how to verify the Cisco VSG configurations:

```
firewall# show interface brief
--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    --           up     10.2.71.43                              --       1500

--------------------------------------------------------------------------------
Port     VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
data0    --           up                                         --       9000
```

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 Prime NSC.



CHAPTER 5

Registering Devices with the Cisco Prime NSC

This chapter contains the following sections:

Registering a Cisco VSG

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

Step 1 Copy the vnmc-vsgpa.2.1.2a.bin file into the Cisco VSG bootflash:

```
vsg# copy ftp://guest@172.18.217.188/n1kv/vnmc-vsgpa.2.1.2a.bin bootflash
```

Step 2 Enter global configuration mode.

```
vsg# configure
```

Step 3 Enter nsc-policy-agent mode.

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

Step 4 Set the Cisco PNSC registration IP address.

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

Step 5 Specify the shared-secret of Cisco PNSC.

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

Step 6 Install the policy agent.

```
vsg (config-nsc-policy-agent)#
policy-agent-image bootflash: vnmc-vsgpa.2.1.2a.bin
```

Step 7 Exit all modes.

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

Step 8 On the Cisco VSG command line, display the NSC PA status:

```
vsg# show nsc-pa status
If registration was successful, you should see the following message:
"NSC Policy-Agent status is - Installed Successfully. Version 2.1(2a)-vsg"
The Cisco VSG registration is complete.
```

Step 9 Copy the running configuration to the startup configuration:

```
vsg# copy running-config startup-config
Executing this command ensures that the registration becomes part of the basic configuration
```

Registering Cisco Nexus 1000V VSM

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

SUMMARY STEPS

1. Copy the vsmhv-pa.3.2.1e.bin file into the VSM bootflash:
2. Enter global configuration mode.
3. Enter config nsc-policy-agent mode.
4. Set the Cisco PNSC registration IP address.
5. Specify the shared-secret of Cisco PNSC.
6. Install the policy agent.
7. Exit all modes.
8. Display the NSC PA status:
9. Copy the running configuration to the startup configuration:

DETAILED STEPS

Step 1 Copy the vsmhv-pa.3.2.1e.bin file into the VSM bootflash:

```
vsm# copy ftp://guest@172.18.217.188/n1kv/vsmhv-pa.3.2.1e.bin bootflash:
```

Step 2 Enter global configuration mode.

```
vsm# configure
```

Step 3 Enter config nsc-policy-agent mode.

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

Step 4 Set the Cisco PNSC registration IP address.

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

Step 5 Specify the shared-secret of Cisco PNSC.

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

Step 6 Install the policy agent.

```
vsm(config-nsc-policy-agent)# policy-agent-image bootflash:vsmhv-pa.3.2.1e.bin
```

Step 7 Exit all modes.

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

Step 8 Display the NSC PA status:

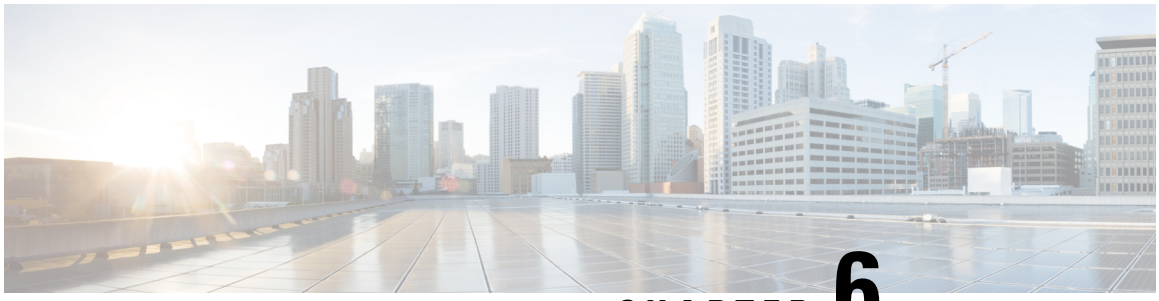
```
vsm# show nsc-pa status
If registration was successful, you should see the following message:
NSC Policy-Agent status is - Installed Successfully. Version 3.2(1e)-vsg
The Cisco Nexus 1000V VSM registration is complete.
```

Step 9 Copy the running configuration to the startup configuration:

```
vsm# copy running-config startup-config
Executing this command ensures that the registration becomes part of the basic configuration.
```

What to do next

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



CHAPTER 6

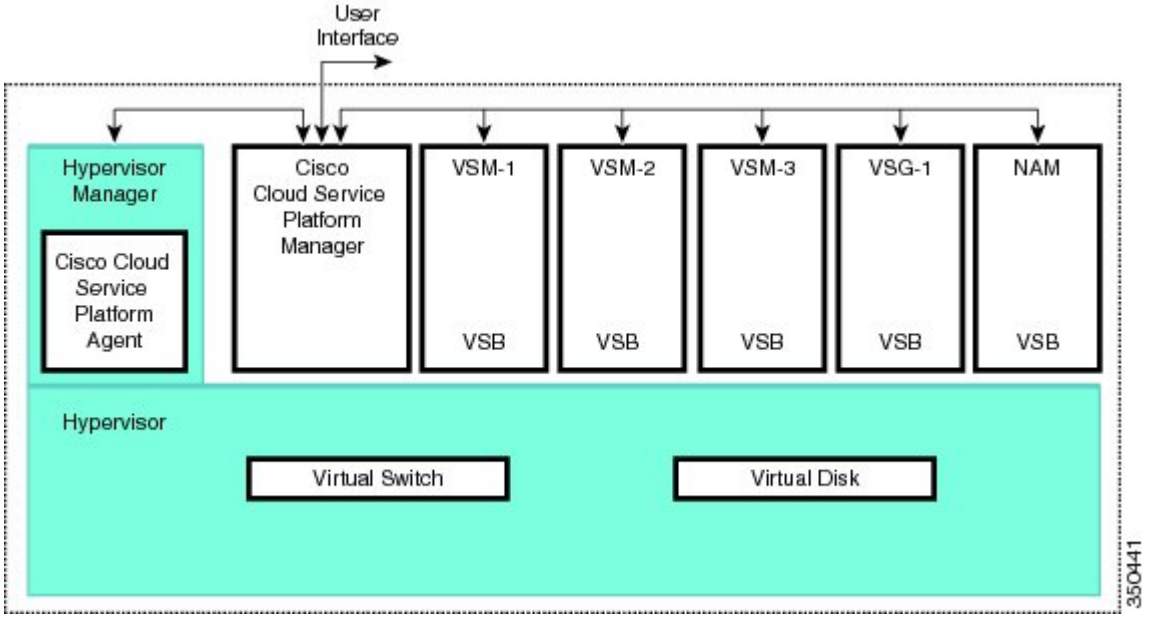
Installing the Cisco VSG on a Cisco Cloud Service Platform Virtual Services Appliance

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 15: Cisco Cloud Service Platform Architecture Showing Virtual service Blades Usage



Prerequisites for Installing Cisco VSG on the 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 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.VSG2.1.2a.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. (config-vsb-config)# **no shutdown**
7. (config-vsb-config)# **interface** *name* **vlan** *vlanid*
8. (config-vsb-config)# **enable [primary | secondary]**
9. (config-vsb-config)# **show virtual-service-blade name** *name*
10. (Optional) (config-vsb-config)# **copy running-config startup-config**

DETAILED STEPS

Step 1 switch# **configure terminal**

Enters global configuration mode.

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

Creates the named VSB and places you in to 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 (config-vsb-config)# **no shutdown**

Enables the interface.

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

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

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

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

Caution Do not assign a management VLAN. Unlike data and HA VLANs, the management VLAN is inherited from the Cisco Cloud Service Platform.

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

Step 8 (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 9 (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 10 (Optional) (config-vsb-config)# **copy running-config startup-config**

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

Example

This example shows how to configure a Cisco 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.VSG2.1.2a.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.VSG2.1.2a.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-2.1                       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.VSG2.1.2a.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-2.1
   Interface: ha vlan: 0
   Interface: management vlan: 231
   Interface: data vlan: 0
   Interface: internal vlan: NA
   Ramsize: 2048
   Disksize: 3
   Heartbeat: 0
   HA Admin role: Primary
   HA Oper role: NONE
   Status: VSB NOT PRESENT
   Location: PRIMARY
   SW version:
   HA Admin role: Secondary
   HA Oper role: NONE
   Status: VSB NOT PRESENT
   Location: SECONDARY
   SW version:
   VSB Info:
--------------------------------------------------------------------------------
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
```

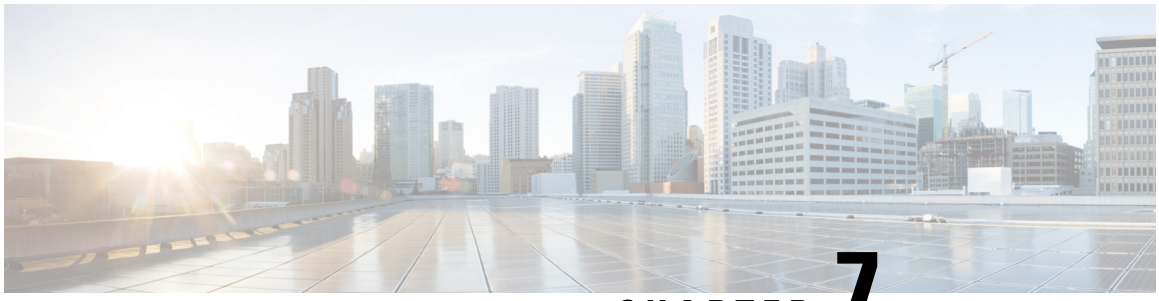
```
  Management IP:  10.78.108.40
  VSB Type Name :  VSG-1.2
  Configured vCPU:           1
  Operational vCPU:           1
  Configured Ramsize:        2048
  Operational Ramsize:        2048
  Disksize:       3
  Heartbeat:      521511

  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)VSG2(1.2a)
  HA Role: Secondary
    HA Status: STANDBY
    Status:       VSB POWERED ON
    Location:     SECONDARY
    SW version:   5.2(1)VSG2(1.2a)
  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
```



CHAPTER 7

Upgrading the Cisco VSG and the Cisco Prime NSC

This chapter contains the following sections:

Complete Upgrade Procedure

Table 3: Refer to the Section in Table Based on your Pre-upgrade Product Release

You are Upgrading From	Follow The Sequential Steps in the Following Section:
Cisco VSG Release 5.2(1)VSG2(1.1b) to Release 5.2(1)VSG2(1.2b) and Cisco PNSC Release 3.2 to Cisco PNSC Release 3.4.	Upgrade Procedures for Cisco VSG Release 5.2(1)VSG2(1.1b) to Release 5.2(1)VSG2(1.2b) and Cisco PNSC Release 3.2 to Cisco PNSC Release 3.4. This includes upgrade procedures for Cisco Nexus 1000V Release 5.2(1)SM1(5.2b) to Release 5.2(1)SM3(1.1).

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

1. Stage 1: Upgrading Cisco PNSC
2. Stage 2: Upgrading a Cisco VSG Pair
3. Stage 3: Upgrading the VSM pair and the VEMs

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

Information About Cisco Prime NSC Upgrades

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

Information About Cisco VSG Upgrades

The upgrade procedure for Cisco VSG in standalone or HA mode is hitful, which means that you must manually reload the Cisco VSG for the new image to become effective.

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

An upgrade affects two bin files: the kickstart file and the system file.

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

Upgrade Guidelines and Limitations

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

- We highly recommend that you upgrade the Cisco VSG and the Cisco PNSC in the order provided. Any deviation from the ordered steps could cause disruption of your connectivity and data communication. The Cisco PNSC must be upgraded with the corresponding policy agent (PA).
- Before upgrading to a new VSG version with VSG Universal License (UL), make sure that you change VSM mode to advanced and save the configuration. Installing VSG with UL without changing the VSM mode to advanced may cause VSG service failure.
- We recommend that you take a snapshot or backup (clone) of the original Cisco PNSC and VSM prior to the upgrade process and then perform an ISSU upgrade process on the VSM. We do not recommend that you perform a manual upgrade.
- For a full In-service Software Upgrade (ISSU) upgrade on VSM, follow these rules:
  - Install the Cisco PNSC before installing the VSM. The ISSU upgrade installs a new PA.
  - A new PA with an old Cisco PNSC is not supported and there should never be an interim stage in this state.
  - A copy run start is not required after the VSM upgrade.
- Upgrade instructions include the following information:
  - Different stages of complete upgrade procedures and operations which are supported at different stages.
  - Different component versions after each stage.
  - Different operations supported after each stage.

Upgrade Procedure for Cisco VSG Release 5.2(1)VSG2(1.1b) to Release 5.2(1)VSG2(1.2b), Cisco Prime NSC Release 3.2 to Cisco Prime NSC Release 3.4 and Cisco Nexus 1000V Release 5.2(1)SM1(5.2b) to Release 5.2(1)SM3(1.1)

Cisco VSG Release 5.2(1)VSG2(1.1b) to 5.2(1)VSG2(1.2b) and Cisco Prime NSC 3.2 to Cisco Prime NSC 3.4 Staged Upgrade

Virtual Appliance	Original State	Stage 1: Cisco PNSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade	Stage 3: VSM/VEM Upgrade
Cisco PNSC	Old Cisco Prime NSC 3.2	New Cisco Prime NSC 3.4	New Cisco Prime NSC 3.4	New Cisco Prime NSC 3.4
Cisco VSG	Old 5.2(1)VSG2(1.1b)	Old 5.2(1)VSG2(1.1b)	New 5.2(1)VSG2(1.2b)	New 5.2(1)VSG2(1.2b)
VSG PA	Old 2.1.1e	Old 2.1.1e	New 2.1.2a	New 2.1.2a
VSM	Old 5.2(1)SM1(5.2b)	Old 5.2(1)SM1(5.2b)	Old 5.2(1)SM1(5.2b)	New 5.2(1)SM3(1.1)
VEM	Old 5.2(1)SM1(5.2b)	Old 5.2(1)SM1(5.2b)	Old 5.2(1)SM1(5.2b)	New 5.2(1)SM3(1.1)
VSM PA	Old 3.2.1c	Old 3.2.1c	Old 3.2.1c	New 3.2.1e
Supported operations after upgrading to each stage	All operations supported	• Existing data sessions (offloaded). • New data sessions. • Allows Cisco Nexus 1000V switch (non-vservice) operations including non-vservice port profiles.	• Short disruption in new data session establishment during the Cisco VSG upgrade. • Other operations are fully supported. • Full Layer 3 VSG and VM VLAN support.	• All operations are supported if all the upgrades including VEMs are successful. • Restricted operations (below) apply only if all VEMs are not upgraded • Disruption of data traffic during VEM upgrades. • Layer 3 VSG and VM VLAN support.

Virtual Appliance	Original State	Stage 1: Cisco PNSC Upgrade only (no PAs upgraded)	Stage 2: Cisco VSG Upgrade	Stage 3: VSM/VEM Upgrade
Restricted operations after upgrading to each stage	None	• No Cisco PNSC policy cfg change (assuming silent drops). • No VSM/VEM vservice VM operations (shutdown/bring up existing vservice VMs, bring down net adapters, etc). • No new vservice VMs is supported. • No Vmotion of vservice firewalled VMs on N1k • No vservice PP operations or modifications (toggles, removal, changing the PP on VSM). • VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to Cisco PNSC to VSG control operations are restricted).	• No Cisco PNSC policy cfg change (assuming silent drops). • No VSM/VEM vservice VM operations (shutdown/bring up existing vservice VMs, bring down net adapters, etc). • No new vservice VMs is supported. • No Vmotion of vservice firewalled VMs on N1k. • No vservice PP operations or modifications (toggles, removal, changing the PP on VSM). • VSG failover not supported, VSM failover (vns-agent) not supported (All VSM to Cisco PNSC to VSG control operations are restricted).	**The following restricted operations apply only if all VEMs are not upgraded:** • No Cisco PNSC policy cfg change (assuming silent drops). • No VSM/VEM vservice VM operations (shutdown/bring up existing vservice VMs, bring down net adapters, etc). • No new vservice VMs is supported. • No boot strap of devices (VNMC, VSM,VSG). • No Vmotion of vservice VMs on N1k. • No vservice PP operations or modifications (toggles, removal, changing the PP on VSM). • No N1k switch (non vservice) operations, including non-vservice PPs (VSM+VEM ugraded) (All VSM to Cisco PNSC to VSG control operations are restricted).

Upgrading Cisco Prime NSC 3.2 to Cisco Prime NSC 3.4

Before you begin

- You are logged in to the CLI in EXEC mode.
- You have backed up the new software files to a remote server and have verified that the backup file was created on the remote server.
- You must have the Cisco PNSC Release 3.4 downloaded.
- You have added two hard disks to the Cisco PNSC VM. For more information on Cisco PNSC requirements, see System Requirements, on page 7.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	nsc# **connect local-mgmt**	Places you in local management mode.
Step 2	(Optional) nsc (local-mgmt)# **show version**	Displays the version information for the Cisco PNSC software.
Step 3	(Optional) nsc (local-mgmt)# **copy scp://user@***example-server-ip/example-dir/filename* **bootflash:/**	Copies the Cisco PNSC software file to the VM.
Step 4	nsc (local-mgmt)# **dir bootflash:/**	Verifies that the desired file is copied in the directory.
Step 5	nsc (local-mgmt)# **update bootflash:/***filename*	Begins the update of the Cisco PNSC software.
Step 6	(Optional) nsc (local-mgmt)# **service status**	Allows you to verify that the server is operating as desired.
Step 7	(Optional) nsc (local-mgmt)# **show version**	Allows you to verify that the Cisco PNSC software version is updated. **Note** After you upgrade to Cisco PNSC Release 3.4, you might see the previous version of Cisco PNSC in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.

Configuration Example

The following example shows how to connect to the local-mgmt mode:

```
nsc# connect local-mgmt
Cisco Prime Network Services Controller
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

The following example shows how to display version information for the Cisco PNSC:

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

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.2)           3.2
service-reg         Service Registry    3.2            3.2
policy-mgr          Policy Manager      3.2            3.2
resource-mgr        Resource Manager    3.2            3.2
vm-mgr              VM manager          3.2            none
cloudprovider-mgr   Cloud Provider Mgr  3.2            none
```

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

```
nsc(local-mgmt)# copy scp://<user@example-server-ip>/example1-dir/nsc.3.4.bin bootflash:/
Enter password:
100%  143MB  11.9MB/s   00:12
```

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

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

    1.1G Oct 14 00:57 nsc.3.4.bin

Usage for bootflash://

             6359716 KB used
            10889320 KB free
            18187836 KB total
```

The following example shows how to start the update for the Cisco PNSC:

```
nsc(local-mgmt)# update bootflash:/nsc.3.4.bin
It is recommended that you perform a full-state backup before updating any VNMC component.
  Press enter to continue or Ctrl-c to exit.
```

The following example shows how to display the updated version for the Cisco PNSC:

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

Name                Package             Version        GUI
---- ------- ------- ----
core                Base System         3.4        3.4
service-reg         Service Registry    3.4        3.4
policy-mgr          Policy Manager      3.4        3.4
resource-mgr        Resource Manager    3.4        3.4
```

```
vm-mgr              VM manager          3.4        none
cloudprovider-mgr   Cloud Provider Mgr  3.4        none
```

Upgrading Cisco VSG from Release 5.2(1)VSG2(1.1b) to 5.2(1)VSG2(1.2b)

This section includes the following topics:

Before you begin

- You are logged in to the CLI in EXEC mode.
- You have closed all the active VSG configuration sessions before upgrading the Cisco VSG software.
- You have copied the kickstart and system images from the remote server to the Cisco Nexus 1000V.

Cisco VSG Software Upgrade Guidelines

Follow these VSG upgrade guidelines while upgrading the VSG:

- Schedule the upgrade when the network is stable. Ensure that nobody is configuring the switch during the upgrade.
- Ensure that sufficient space is available for copying the upgrade images. A minimum of 200 MB of free bootflash space is required on both the active and standby VSGs.
- Avoid power interruptions to the hosts running the VSG VMs during any installation procedure.
- Ensure that the management (mgmt0) interface of the VSG is working and accessible.
- Ensure that the specified system and kickstart images are compatible with each other.
- Verify connectivity to the remote server by using the **ping** command.

Upgrade a VSG Pair in HA Mode

You can upgrade VSG pair in the High Availability (HA) mode.

SUMMARY STEPS

1. Log in to the active VSG.
2. Display the current boot variables.
3. Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.
4. Verify that required space is available on the standby VSG. Delete unnecessary files if required to create more space available for copying the new VSG image.
5. Copy the Cisco Nexus 1000V kickstart and system software files to a server.

6. Remove current boot variables.
7. Display the current boot variables.
8. Load the new boot variables and copy the running configuration to the startup configuration.
9. Manually reboot the system.
10. After the installation operation completes, log in and verify that the switch is running the upgraded software version.

DETAILED STEPS

Step 1 Log in to the active VSG.

Step 2 Display the current boot variables.

```
vsg# show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
No module boot variable set
```

Step 3 Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.

```
vsg(config)# dir
.
.
.
Usage for bootflash://
  692117504 bytes used
 5711851520 bytes free
 6403969024 bytes total
```

Step 4 Verify that required space is available on the standby VSG. Delete unnecessary files if required to create more space available for copying the new VSG image.

```
vsg(config)# dir bootflash://sup-standby/
.
.
.
Usage for bootflash://sup-standby
  577372160 bytes used
 5826600960 bytes free
 6403973120 bytes total
```

Step 5 Copy the Cisco Nexus 1000V kickstart and system software files to a server.

```
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.1.2b.bin
 ./
vsg(config)#copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.5.2.1.VSG2.1.2b.bin ./
```

Step 6 Remove current boot variables.

```
vsg(config)# no boot system
vsg(config)# no boot kickstart
```

Step 7 Display the current boot variables.

```
vsg(config)#  show boot
Current Boot Variables:
sup-1
kickstart variable not set
system variable not set
sup-2
kickstart variable not set
system variable not set
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
No module boot variable set
```

Step 8 Load the new boot variables and copy the running configuration to the startup configuration.

```
vsg# configure terminal
vsg(config)# boot system bootflash:///nexus-1000v.5.2.1.VSG2.1.2b.bin
vsg(config)# boot kickstart bootflash:///nexus-1000v-kickstart.5.2.1.VSG2.1.2b.bin
vsg(config)# copy running-config startup-config
```

Step 9 Manually reboot the system.

```
vsg(config)# reload
This command will reboot the system. (y/n)?  [n]

If you want to continue with the reboot, press Y.
```

Note The system reboot takes approximately 10 seconds.

Step 10 After the installation operation completes, log in and verify that the switch is running the upgraded software version.

Note The new software version will reflect after you reload the system.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
```

```
  kickstart: version 5.2(1)VSG2(1.2b)
  system:    version 5.2(1)VSG2(1.2b)
  system image file is:    bootflash:///nexus-1000v.5.2.1.VSG2.1.2b.bin
  system compile time:     12/6/2013 16:00:00 [12/10/2014 21:10:51]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2609 with 1933768 kB of memory.
  Processor Board ID T155D4BC001

  Device name: VSG_Fire
  bootflash:    1451180 kB

Kernel uptime is 1 day(s), 16 hour(s), 30 minute(s), 38 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
vsg #
```

Upgrading a Device for Standalone VSG

SUMMARY STEPS

1. Log in to the active VSG.
2. Use the **show boot** command to display the current boot variables.
3. Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.
4. Copy the Cisco VSG kickstart and system software files to a server.
5. Remove current boot variables.
6. Display the current boot variables.
7. Load the new boot variables and copy the running configuration to the startup configuration.
8. Manually reboot the system.
9. After the installation operation completes, log in and verify that the switch is running the upgraded software version.

DETAILED STEPS

Step 1 Log in to the active VSG.

Step 2 Use the **show boot** command to display the current boot variables.

```
vsg# show boot
Current Boot Variables:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
No module boot variable set
```

```
Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
No module boot variable set
```

Step 3 Verify that required space is available to copy the image files. Delete unnecessary files if required to create more space available for copying the new VSG image.

```
vsg(config)# dir
.
.
.
Usage for bootflash://
  692117504 bytes used
 5711851520 bytes free
 6403969024 bytes total
```

Step 4 Copy the Cisco VSG kickstart and system software files to a server.

```
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v-kickstart.5.2.1.VSG2.1.2b.bin
 ./
vsg(config)# copy scp://user@scpserver.cisco.com/downloads/nexus-1000v.5.2.1.VSG2.1.2b.bin ./
```

Step 5 Remove current boot variables.

```
vsg(config)# no boot system
vsg(config)# no boot kickstart
```

Step 6 Display the current boot variables.

```
vsg(config)# show boot
Current Boot Variables:
sup-1
kickstart variable not set
system variable not set
sup-2
kickstart variable not set
system variable not set
No module boot variable set

Boot Variables on next reload:

sup-1
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
sup-2
kickstart variable = bootflash:/nexus-1000v-kickstart.5.2.1.VSG2.1.1b.bin
system variable = bootflash:/nexus-1000v.5.2.1.VSG2.1.1b.bin
No module boot variable set
```

Step 7 Load the new boot variables and copy the running configuration to the startup configuration.

```
vsg# configure terminal
vsg(config)# boot system bootflash:///nexus-1000v.5.2.1.VSG2.1.2b.bin
vsg(config)# boot kickstart bootflash:///nexus-1000v-kickstart.5.2.1.VSG2.1.2b.bin
vsg(config)# copy running-config startup-config
```

Step 8 Manually reboot the system.

```
vsg(config)# reload
This command will reboot the system. (y/n)?  [n]

If you want to continue with the reboot, press Y.
```

Note The system reboot takes approximately 10 seconds.

Step 9 After the installation operation completes, log in and verify that the switch is running the upgraded software version.

Note The new software version will reflect after you reload the system.

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  loader:    version unavailable [last: image booted through mgmt0]
  kickstart: version 5.2(1)VSG2(1.2b)
  system:    version 5.2(1)VSG2(1.2b)
  system image file is:    bootflash:///nexus-1000v.5.2.1.VSG2.1.2b.bin
  system compile time:     11/10/2014 16:00:00 [11/10/2014 21:10:51]


Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2609 with 1933768 kB of memory.
  Processor Board ID T155D4BC001

  Device name: VSG_Fire
  bootflash:    1451180 kB

Kernel uptime is 1 day(s), 16 hour(s), 30 minute(s), 38 second(s)


plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
vsg #
```

Re-registering the Policy Agent with the Upgraded VSG

You need to re-register the policy agent after upgrading the Cisco VSG.

SUMMARY STEPS

1. Log in to the active VSG.
2. Check the current policy agent version.
3. Enter the configuration mode.
4. Unregister the old policy agent from VSG.
5. Register the new policy agent with the VSG.
6. Copy the current running configuration to the startup configuration.

7. Verify the updated policy agent version.

DETAILED STEPS

Step 1 Log in to the active VSG.

Step 2 Check the current policy agent version.

```
vsg# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(1e)-vsg
VSG#
```

Step 3 Enter the configuration mode.

```
vsg# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSG(config)#
```

Step 4 Unregister the old policy agent from VSG.

```
VSG(config)# nsc-policy-agent
VSG(config-nsc-policy-agent)# no policy-agent-image
```

Step 5 Register the new policy agent with the VSG.

```
VSG(config-nsc-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.2.1.2a.bin
VSG(config-nsc-policy-agent)# exit
VSG(config)#
```

Step 6 Copy the current running configuration to the startup configuration.

```
VSG(config)# copy running startup
[########################################] 100%
```

Step 7 Verify the updated policy agent version.

```
VSG(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.1(2a)-vsg
VSG(config)#
```

Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V

Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V

Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V platform involves:

- Upgrading the VSM
- Upgrading the Cisco VSEM
- Upgrading the VEM Software

For detailed information about upgrading the Cisco Nexus 1000V for Microsoft Hyper-V, see the Upgrading the Cisco Nexus 1000V for Microsoft Hyper-V chapter in Cisco Nexus 1000V for Microsoft Hyper-V

Installation and Upgrade Guide, available at: http://www.cisco.com/en/US/partner/products/ps13056/prod_installation_guides_list.html

INDEX

P

R

S

T

U

V

W