Cisco Prime Network Services Controller 3.2 Quick Start Guide

Revised: April 3, 2014, OL-30752-01

Getting Started with Cisco Prime Network Services Controller

New and Changed Information

The following table describes information that has been added or changed since the initial release of this document.

Date	Revision	Location
February 14, 2014	Updated information for upgrading from VNMC 2.1.	Upgrading Overview, on page 43

Installation Requirements

Requirements Overview

The following topics identify the requirements for installing and using Cisco Prime Network Services Controller (Prime Network Services Controller) 3.2:

Note This release of Prime Network Services Controller contains many new features. For information on these features and additional changes in this release, see the Cisco Prime Network Services Controller 3.2 Release Notes.

System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four Virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk Space	One of the following, depending on InterCloud functionality: • With InterCloud functionality, 220 GB on shared NFS or 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
Management Interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
Prime Network Services Controller Device Adapter	
Two virtual CPUs	1.8 GHz
Memory	2 GB RAM
Disk Space	20 GB
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Hypervisor Requirements

Prime Network Services Controller is a multi-hypervisor virtual appliance that can be deployed on either VMware vSphere or Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor).

- See the VMware Compatibility Guide to verify that VMware supports your hardware platform.
- See the Windows Server Catalog to verify that Microsoft Hyper-V supports your hardware platform.

Requirement	Description
VMware	
VMware vSphere	Release 5.0, 5.1, or 5.5 with VMware ESXi (English Only)
VMware vCenter	Release 5.0, 5.1, or 5.5 (English Only)
Microsoft	
Microsoft Server	Microsoft Hyper-V Server 2012 R2 (Standard or Data Center)
Microsoft System Center Virtual Machine Manager (SCVMM)	Microsoft SCVMM 2012 R2

Web-Based GUI Client Requirements

Requirement	Description
Operating System	Either of the following: • Microsoft Windows • Apple Mac OS
Browser	Any of the following: • Internet Explorer 10.0 or higher • Mozilla Firefox 26.0 or higher • Google Chrome 32.0 or higher[1]
Flash Player	Adobe Flash Player plugin 11.9 or higher

1 Before using Chrome with Prime Network Services Controller, you must disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with Prime Network Services Controller, on page 5.

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller, you must disable the Adobe Flash Player plugins that are installed by default with Chrome.

Note You must perform this procedure each time your client machine reboots. Chrome automatically enables the Adobe Flash Players when the system on which it is running reboots.

Procedure

Step 1 In the Chrome URL field, enter **chrome://plugins**.

Step 2 Click **Details** to expand all the files associated with each plugin.

Step 3 Locate the Adobe Flash Player plugins, and disable each one.

Step 4 Download and install Adobe Flash Player version 11.9 or higher.

Step 5 Close and reopen Chrome before logging in to Prime Network Services Controller.

Firewall Ports Requiring Access

If Prime Network Services Controller is protected by a firewall, the following ports on the firewall must be open so that clients can contact Prime Network Services Controller.

Port	Description
80	HTTP
443	HTTPS
843	Adobe Flash

Ports to Access Amazon AWS

This table lists the port numbers you must enable to access the Amazon Web Services (AWS) public IP address ranges listed at https://forums.aws.amazon.com/ann.jspa?annID=1701.

Protocol	Ports
TCP	22, 443, 3389, 6644, and 6646
UDP	6644 and 6646

Cisco Nexus 1000V Series Switch Requirements

Requirement	Description
General	
The procedures in this guide assume that the Cisco Nexus 1000V Series Switch (Nexus 1000V) is operational and that virtual machines (VMs) are installed.	—
VLANs	
Two VLANs configured on the Nexus 1000V uplink ports: • Service VLAN • HA VLAN	Neither VLAN needs to be the system VLAN.
Port Profiles	
One port profile configured on the Nexus 1000V for the service VLAN.	—

Information Required for Configuration and Installation

Required Information	Your Information
For Preinstallation Configuration	
ISO image location	
ISO image name	
Network / Port Profile for VM management [2]	
VM name	
VMware: Data store location	
For Prime Network Services Controller Installation	
IP address	
Subnet mask	
Hostname	
Domain name	

Required Information	Your Information
Gateway IP address	
DNS server IP address **Note** Access to a DNS server is required for Prime Network Services Controller to communicate with the Amazon Cloud Provider.	
NTP server IP address	
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria, on page 7.)	

[2] The management port profile is the same port profile that is used for Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and is used for the Prime Network Services Controller management interface.

Shared Secret Password Criteria

A shared secret password is a password that is known only to those using a secure communication channel. Passwords are designated as strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between Prime Network Services Controller, VSG, ASA 1000V, and VSM, adhere to the following criteria for setting valid, strong passwords:

- Do not include the following items in passwords:
  - These characters: & ' " ` ( ) < > | \ ; $
  - Spaces
- Make sure your password contains the characteristics of strong passwords as described in the following table:

Strong Passwords have:	Strong Passwords do not have:
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive alphanumeric characters, such as abcd or 123 • 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
- Es@1955#Ap

Installing Prime Network Services Controller

Installing Overview

You install Prime Network Services Controller by using an ISO or OVA image. The image that you use depends on your hypervisor:

- Microsoft Hyper-V Hypervisor—Install using the ISO image. You cannot install Prime Network Services Controller on Microsoft Hyper-V Hypervisor using the OVA image.
- VMware vSphere Hypervisor—Install using either the ISO or OVA image.

Installing an ISO image requires two procedures:

1. Configuring the hypervisor
2. Installing Prime Network Services Controller

See the following topics for more information:

- Configuring Hyper-V Hypervisor for Prime Network Services Controller, on page 8
- Configuring VMware for Prime Network Services Controller, on page 10
- Installing Prime Network Services Controller, on page 11
- Deploying the Prime Network Services Controller OVA on VMware vSphere, on page 13

Note The installation time varies from 10 to 20 minutes depending on the host and storage area network load.

Configuring Hyper-V Hypervisor for Prime Network Services Controller

Before you can install Prime Network Services Controller on Hyper-V Hypervisor, you must create a VM. This procedure describes how to create a VM for Prime Network Services Controller.

Before You Begin

- Verify that the Hyper-V Hypervisor host on which you are going to deploy the Prime Network Services Controller VM is available in the System Center Virtual Machine Manager (SCVMM).
- Copy the Prime Network Services Controller 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 click **Refresh**.

Procedure

Step 1 Launch the SCVMM.

Step 2 Right-click the Hyper-V Hypervisor host on which to deploy the Prime Network Services Controller VM, and choose **Create Virtual Machine**.

Step 3 In the Create Virtual Machine wizard, provide the information as described in the following table:

Screen	Action
Select Source	Click **Create the new virtual machine with a blank virtual hard disk**.
Specify Virtual Machine Identity	Enter the VM name.
Configure Hardware	**1** In the Hardware Profile field, choose **Default**. **2** From General: **a** Choose **Processor** and set the number of processors to **2**. **b** Choose **Memory** and set the VM memory to **4 GB**. **3** From **Bus Configuration > IDE Devices**: **a** Choose **Hard Disk** and enter **20 GB**. **b** Choose **Virtual DVD Drive**, click **Existing ISO image file**, and choose the Prime Network Services Controller ISO image. **4** Choose **Network Adapters > Network Adapter 1**, click **Connect to a VM Network**, and choose a VM network.
Select Destination	**1** Click **Place the virtual machine on a host**. **2** From the Destination drop-down list, choose **All hosts**.
Select Host	Choose the destination.
Configure Settings	Review the VM settings.
Select Networks	Confirm that the correct virtual switch is specified.
Add Properties	Choose **64-bit edition of Windows Server 2012**.
Summary	**1** Confirm that the settings are correct. **2** Check the **Start the virtual machine after deploying** check box. **3** Click **Create**.

The Jobs window displays the status of the VM being created. Verify that the job completes successfully.

Step 4 After the VM is successfully created, right-click it and choose **Connect or View > Connect Via Console**.

Step 5 Launch the console and install Prime Network Services Controller. For more information, see Installing Prime Network Services Controller, on page 11.

Step 6 After Prime Network Services Controller is successfully deployed, click **Close** and power on the Prime Network Services Controller VM.

Configuring VMware for Prime Network Services Controller

Before you can install Prime Network Services Controller on VMware using an ISO image, you must configure a VM. This procedure describes how to configure the VM so that you can install Prime Network Services Controller.

Procedure

Step 1 Download a Prime Network Services Controller ISO image to your client machine.

Step 2 Open the VMware vSphere Client.

Step 3 Right-click the host on which to install the ISO image, and then choose **New Virtual Machine**.

Step 4 Create a new VM by providing the information as described in the following table:

Screen	Action
Configuration	Choose **Custom**.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the data store.
Virtual Machine Version	Choose **Version 8**.
Guest Operating System	Choose **Linux** and **Red Hat Enterprise Linux 5 (64-bit)**.
CPUs	Set the number of virtual sockets to **2**.
Memory	Set the memory to **4 GB**.
Network	**1** Set the number of NICs to **1**. A single NIC is required for Prime Network Services Controller. **2** Choose a NIC. **3** From the Adapter drop-down list, choose **E1000**. Prime Network Services Controller supports only E1000 adapters.
SCSI Controller	Choose **LSI Logic Parallel**.
Select a Disk	Choose **Create a new virtual disk**.

Screen	Action
Create a Disk	1 Disk Size—Enter a minimum of 20 GB. 2 Disk Provisioning—Choose **Thin Provision** or **Thick Provision**. 3 Location—Specify the location of the data store.
Advanced Options	Specify options as needed.

Step 5 In the Ready to Complete screen, review the information for accuracy, check the **Edit the Virtual Machine Settings Before Completion** check box, and then click **Continue**.

Step 6 In the Virtual Machine Properties dialog box in the Hardware tab, do the following:

a) Click **Memory** and in the Memory Size field, choose **4 GB**.

b) Click **CPUs** and in the Number of Virtual Sockets field, choose the number of CPUs that you want to use.

c) Click **New Hard Disk** and then click **Add** to create a new hard disk. The size of the this disk depends on whether or not you plan to use Prime Network Services Controller InterCloud functionality:

- To use with InterCloud functionality—Add the disk with a minimum size of 200 GB.
- To use without InterCloud functionality—Add the disk with a minimum size of 20 GB.

d) After you have supplied the information in the Add Hardware Wizard, click **Finish** to create the new disk and to return to the Virtual Machine Properties dialog box.

Step 7 In the **Options** tab, choose **Boot Options**, check the **Force BIOS Setup** checkbox, and then click **Finish**.

Step 8 After the new VM is created, power it on.

Step 9 Mount the ISO to the VM CD ROM drive as follows:

a) Right-click the VM and choose **Open Console**.

b) From the VM console, click **Connect/Disconnect the CD/DVD Devices of the virtual machine**.

c) Choose **CD/DVD Drive 1**.

d) Choose **Connect to ISO Image on Local Disk**.

e) Choose the ISO image that you downloaded in Step 1.

You are now ready to install Prime Network Services Controller. For more information, see Installing Prime Network Services Controller, on page 11.

Installing Prime Network Services Controller

This procedure describes how to install an ISO image on a hypervisor that has been configured for Prime Network Services Controller.

Before You Begin

Confirm the following items:

- Make sure that all system requirements are met as specified in System Requirements, on page 3.

- The hypervisor is configured and prepared for the Prime Network Services Controller installation procedure. For more information, see the following topics:
  - Configuring Hyper-V Hypervisor for Prime Network Services Controller, on page 8
  - Configuring VMware for Prime Network Services Controller, on page 10
- The VM has network access.
- You can access the VM console.

Procedure

Step 1 Open the VM console if it is not already open.
If you have just finished configuring the hypervisor, the Prime Network Services Controller installer will be displayed within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area.

Step 3 In the Edit Interface dialog box, enter the IP address and netmask for the Prime Network Services Controller VM, and then click **OK**.

Step 4 In the Network Settings area, enter the following information for Prime Network Services Controller, and then click **Next**:

- Hostname
- Domain name
- Gateway IP address
- DNS server IP address
- NTP server IP address

Step 5 In the Modes screen, choose the required modes, and then click **Next**:

- NSC Operation Mode:
  - Standalone—Choose if Prime Network Services Controller will operate as a standalone VM.
  - Orchestrator—Choose if Prime Network Services Controller will be integrated via an orchestrator with a northbound application. For more information about using orchestrator mode, see the Integrating with DCNM section in the *Cisco Prime Network Services Controller 3.2 User Guide*.
- NSC Configuration:
  - NSC Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore NSC—Choose if you are restoring a previous Prime Network Services Controller installation.

Step 6 In the Administrative Access screen, enter the following information, and then click **Next**:

- Admin password, and a confirming entry.
- Shared secret password, and a confirming entry, using the criteria described in Shared Secret Password Criteria, on page 7.

Note If you configure a weak shared secret password, no error message will be generated when you enter it here, but the shared secret password will not be usable when the VM is started during the installation process.

Step 7 In the Summary screen, confirm that the information is accurate, and then click **Finish**.
Prime Network Services Controller will then be installed on the VM. This can take a few minutes.

Step 8 When prompted, click **Reboot**.
Prime Network Services Controller is successfully installed on the VM.

Deploying the Prime Network Services Controller OVA on VMware vSphere

This procedure describes how to deploy a Prime Network Services Controller OVA on VMware.

Before You Begin

- Set your keyboard to United States English before installing Prime Network Services Controller and using the VM console.
- Confirm that the Prime Network Services Controller OVA image is available from the VMware vSphere Client.
- Make sure that all system requirements are met as specified in System Requirements, on page 3.
- Determine whether you will install Prime Network Services Controller in Standalone or Orchestrator mode:
  - Standalone mode is used when Prime Network Services Controller will operate as a standalone VM.
  - Orchestrator mode is used when Prime Network Services Controller will be integrated via an orchestrator with a northbound application. For more information, see the Integrating with DCNM section in the *Cisco Prime Network Services Controller 3.2 User Guide*.

  You cannot change the Operation mode after you deploy Prime Network Services Controller.
- Make sure that you have the information identified in Information Required for Configuration and Installation, on page 6.
- Configure NTP on all ESX and ESXi servers that run any of the following images:
  - ASA 1000V
  - Citrix NetScaler 1000V
  - Citrix NetScaler VPX
  - CSR 1000V
  - InterCloud images
  - Prime Network Services Controller
  - Prime Network Services Controller Device Adapter
  - VSG
  - VSM

  For more information, see "Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and 5.0 hosts using the VMware vSphere Client" at http://kb.vmware.com/kb/2012069.

Procedure

Step 1 If you are installing Prime Network Services Controller on an ESXi 5.0 host, enable hardware-assisted virtualization by adding the property vhv.allow = TRUE to /etc/vmware/config.

Step 2 Use the VMware vSphere Client to log in to the vCenter server.

Step 3 Choose the host on which to deploy the Prime Network Services Controller VM.

Step 4 Choose **File > Deploy OVF Template**.

Step 5 In the wizard, provide the information as described in the following table:

Screen	Action
Source	Choose the Prime Network Services Controller OVA.
OVF Template Details	Review the details.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Enter a name and choose a location for the template.
Deployment Configuration	Choose **Installer**.
Datastore	Select the data store for the VM. The storage can be local or shared remote, such as NFS or SAN.
Disk Format	Choose either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks. If you will not use the InterCloud functionality in Prime Network Services Controller, you can choose thin provisioning.
Network Mapping	Choose the management network port group for the VM.

Screen	Action
Properties	Provide the following information: • VM IP address • IP subnet mask • Gateway IP address • DNS hostname • DNS domain • DNS server IP address • NTP server IP address • Operation mode: standalone or orchestrator • Admin password • Shared secret password **Note** • You cannot change the Operation mode after you deploy Prime Network Services Controller. • Address any errors presented in red text below the selection box. You can enter placeholder information as long as your entry meets the field requirements. • You can safely ignore the Prime Network Services Controller Restore fields.
Ready to Complete	Review the deployment settings. **Caution** Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information.

Step 6 Click **Finish**.
A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 7 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 8 For ESXi 5.1 hosts, enable hardware-assisted virtualization by doing the following:

1. In the vSphere Client, right-click the Prime Network Services Controller VM, and choose **Upgrade Virtual Hardware**.
2. In the vSphere Web Client, right-click the Prime Network Services Controller VM, and choose **Configuration > Upgrade Virtual Hardware**.

VMware upgrades the virtual hardware to the latest supported version.

Step 9 Power on the Prime Network Services Controller VM.

Configuring Prime Network Services Controller

Configuring Overview

The following topics describe how to initially configure Prime Network Services Controller for use:

Topic	Description
Task 1—Configuring NTP, on page 17	Ensures that service VMs can successfully register with Prime Network Services Controller and that communications with AWS can occur.
Task 2—Configuring Connectivity with VM Managers, on page 19	Establishes a connection between Prime Network Services Controller and VM management software.
Task 3—Registering Service VMs, on page 22	Enables Prime Network Services Controller to recognize and communicate with service VMs.
Task 4—Verifying Service VM Registration, on page 28	Confirms that the required service VMs are registered with Prime Network Services Controller.
Task 5—Configuring a Tenant, on page 28	Establishes a tenant to which you can allocate resources, such as compute or edge firewalls, edge routers, and load balancers.
Task 6—Configuring Access Policies, on page 28	Allows or prevents access to resources based on the criteria that you specify.
Task 7—Configuring a Service Profile, on page 34	Enables you to apply a set of security-related policies (such as access and threat mitigation policies) to one or more objects.
Task 8—Configuring a Device Profile, on page 34	Enables you to apply a set of custom security attributes and device policies to a port profile or other resources.
Task 9—Importing Service Images, on page 35	Enables you to instantiate a service device from an image.
Task 10—Adding Service Devices, on page 35	Enables you to place resources in service under a tenant or another level in the organizational hierarchy.
Task 11—Creating an Edge Security Profile, on page 37	Creates an edge profile with policies and policy sets that you can apply to edge firewalls.
Task 12—Enabling Logging, on page 41	Ensures that you receive syslog messages for the severities that you specify.

Task 1—Configuring NTP

Before you perform any operations on the Prime Network Services Controller system, configure Network Time Protocol (NTP) on Prime Network Services Controller and any of the following deployed VMs:

- ASA 1000V
- Citrix NetScaler 1000V
- Citrix NetScaler VPX
- CSR 1000V
- VSG
- Cloud VSM
- Enterprise VSM

If you do not configure these items with NTP, the following will occur:

- The components will not be able to register with Prime Network Services Controller.
- InterCloud functionality will not work because the AWS API requires the request time to be within a few seconds of the current time.

For information on configuring NTP, see the following topics:

- Configuring NTP in VMs, on page 17
- Configuring NTP in Prime Network Services Controller, on page 19

Configuring NTP in VMs

Configure NTP on all VMs using the information in the following table.

For this VM:	Do this:
ASA 1000V	(VMware only) Before you install ASA 1000V in Prime Network Services Controller, configure NTP on all ESX and ESXi servers that run ASA 1000V. For information, see "Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client" at kb.vmware.com/kb/2012069. After installation, the ASA 1000V receives the Real Time Clock (RTC) value from the VMware ESX or ESXi host.
Citrix NetScaler 1000V	For information on setting NTP on Citrix NetScaler 1000V, see Citrix NetScaler documentation, available at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.

For this VM:	Do this:
Citrix NetScaler VPX	For information on setting NTP on Citrix NetScaler 1000V, see Citrix NetScaler documentation, available at http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html.
CSR 1000V	For information on setting NTP on CSR 1000V, see http://www.cisco.com/en/US/products/ps12559/tsd_products_support_series_home.html.
InterCloud Extender VM	Configure the NTP server in the Prime Network Services Controller GUI by choosing **InterCloud Management > InterCloud Policies > Device Profiles**. You can add the NTP server to the existing default device profile or create a new device profile with the required NTP server.
InterCloud Switch VM	When instantiating the InterCloud extender and InterCloud switch in Prime Network Services Controller using the InterCloud Link Wizard, choose a device profile with an NTP server configured to use for that instantiation.

VSG	Enter the following CLI commands from the VSG console, where *x.x.x.x* is the NTP server IP address. If you use a host name, a DNS server must be configured.
	
	`clock timezone zone-name offset-hours offset-minutes`
	`clock summer-time zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes`
	`ntp server x.x.x.x.`
	
	For example, your entries might resemble the following:
	
	`clock timezone EST -5.0`
	`ntp server 10.10.1.1`
	
	Note The **ntp server** command is not available in the VSG console if the Prime Network Services Controller policy agent is enabled. To disable the Prime Network Services Controller policy agent, enter the following commands:
	
	`configure terminal`
	`nsc-policy-agent`
	`no-policy-agent-image`

For this VM:	Do this:
VSM (cloud or enterprise)	Enter the following CLI command from the VSM console, where *x.x.x.x* is the NTP server IP address. **clock timezone** *zone-name offset-hours offset-minutes* **clock summer-time** *zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes* **ntp server** *x.x.x.x*

Configuring NTP in Prime Network Services Controller

Use this procedure to configure NTP in Prime Network Services Controller.

Procedure

Step 1 In your browser, enter **https://***server-ip-address* where *server-ip-address* is the Prime Network Services Controller IP address.

Step 2 In the Prime Network Services Controller login window, enter the username **admin** and the admin user password. This is the password that you set when installing Prime Network Services Controller.

Step 3 Set the time zone by doing the following:

a) Choose **Administration > System Profile > root > Profile > default** and click **Edit**.
b) In the General tab, choose the time zone in which the Prime Network Services Controller server resides.
c) Click **Save**.

Step 4 Add an external NTP server as the time source as follows:

a) Choose **Administration > System Profile > root > Profile > default** and click **Edit**.
b) In the Policy tab, click **Add NTP Server**.
c) Enter the NTP server hostname or IP address and click **OK**.
d) Click **Save**.

Caution We recommend that you do not set the time zone after you add the NTP server.

Task 2—Configuring Connectivity with VM Managers

After installing Prime Network Services Controller on a hypervisor, you must configure Prime Network Services Controller so that it can communicate with the Virtual Machine Manager (VMM) for that hypervisor and the VMs that Prime Network Services Controller manages.

Prime Network Services Controller communicates with the VMM to perform the following actions on the VMs that Prime Network Services Controller manages:

- Obtain the VM attributes that Prime Network Services Controller uses to define security or service policies for Nexus 1000V switches, VSG compute firewalls, and CSR 1000V edge routers.
- Instantiate, start, stop, restart, or delete VMs.
- Map VM network interfaces.
- Instantiate and configure services on service VMs.

For information on configuring VMM connectivity, see the following topics:

- Configuring Connectivity with VMware vCenter, on page 20
- Configuring Connectivity with Microsoft SCVMM, on page 22

Note You must reestablish connectivity with the VMM if you change the Prime Network Services Controller server hostname or fully qualified domain name (FQDN).

Configuring Connectivity with VMware vCenter

Establish connectivity between Prime Network Services Controller and VMware vCenter by performing the following tasks:

1. Exporting the vCenter Extension File, on page 20
2. Registering the vCenter Extension Plug-in in vCenter, on page 21
3. Configuring Connectivity with vCenter, on page 21

Exporting the vCenter Extension File

The first step in configuring connectivity with VMware vCenter is to export the vCenter extension file.

Before You Begin

If you use Internet Explorer, do one of the following to ensure that you can download the extension file:

- Open Internet Explorer in Administrator mode.
- After starting Internet Explorer, choose **Tools > Internet Options > Security**, and uncheck the **Enable Protected Mode** check box.

Procedure

Step 1 In Prime Network Services Controller, choose **Resource Management > VM Managers > VM Managers**.

Step 2 In the VM Managers pane, click **Export vCenter Extension**.

Step 3 Save the vCenter extension file in a directory that the vSphere Client can access because you will need to register the vCenter extension plug-in from within the vSphere Client (see Registering the vCenter Extension Plug-in in vCenter, on page 21).

Step 4 Open the XML extension file to confirm that the content is available.

Registering the vCenter Extension Plug-in in vCenter

Registering the vCenter extension plug-in enables you to create a VM Manager in Prime Network Services Controller and communicate with the vCenter VMM and the VMs that Prime Network Services Controller manages.

Procedure

Step 1 From the VMware vSphere Client, log in to the vCenter server that you want to manage by using Prime Network Services Controller.

Step 2 In the vSphere Client, choose **Plug-ins > Manage Plug-ins**.

Step 3 Right-click the window background and choose **New Plug-in**.

Tip Scroll down and right-click near the bottom of the window to view the New Plug-in option.

Step 4 Browse to the Prime Network Services Controller vCenter extension file that you previously exported and click **Register Plug-in**.

The vCenter Register Plug-in window appears, displaying a security warning.

Step 5 In the security warning message box, click **Ignore**.

Note If desired, you can install this certificate for further integration with Public Key Infrastructure (PKI) and Kerberos facilities.

A progress indicator shows the task status.

Step 6 When the success message is displayed, click **OK**, and then click **Close**.

Configuring Connectivity with vCenter

After you register the vCenter extension plug-in in vCenter, you can configure connectivity with vCenter in Prime Network Services Controller.

Procedure

Step 1 Choose **Resource Management > VM Managers > VM Managers**, and then click **Add VM Manager**.

Step 2 In the Add VM Manager dialog box, enter the following information and then click **OK**:

- Name—VMM name.
- Description—VMM description.
- Hostname / IP Address—Hostname or IP address of the VMM.
- Port Number—Port number to use for communications.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- VMware vCenter version.

Configuring Connectivity with Microsoft SCVMM

Use this procedure to configure Prime Network Services Controller connectivity with Microsoft SCVMM (SCVMM).

Before You Begin

- Confirm that you have the username and password for SCVMM access.
- Install Microsoft Service Provider Framework (SPF) so that Prime Network Services Controller can communicate with SCVMM. For more information, see http://technet.microsoft.com/en-us/library/jj642895.aspx.
- Confirm that SPF is installed correctly and functional in SCVMM by connecting to https://spf_host_ip:8090/SC2012R2/VMM/Microsoft.Management.Odata.Svc.

Procedure

Step 1 Choose **Resource Management > VM Managers**, and then click **Add VM Manager**.

Step 2 In the Add VM Manager dialog box, provide the information described in the following table, and then click **OK**:

Field	Description
Name	VMM name.
Description	VMM description.
Hostname / IP Address	Hostname or IP address of the VMM.
Domain Name / Username	Domain or username for SCVMM access.
Password	Password for SCVMM access.
Port Number	Port to use for communications.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- SCVMM version.

Task 3—Registering Service VMs

Registering service VMs with Prime Network Services Controller ensures that Prime Network Services Controller recognizes and can communicate with the service VMs. The method that you use to register service VMs depends on the type of VM:

- For Cisco service VMs, see Registering Cisco Service VMs, on page 23.

- For third-party service VMs, such as Citrix NetScaler 1000V and Citrix NetScaler VPX, see Registering Third-Party VMs, on page 25.

Registering Cisco Service VMs

This procedure describes how to register the following Cisco service VMs with Prime Network Services Controller:

- ASA 1000V
- VSG
- Cloud VSM
- Enterprise VSM

Before You Begin

- Configure NTP on the required hypervisor.
- Install the required service VMs on the hypervisor.
- Make sure that a network path exists between each VM management IP address and the Prime Network Services Controller management IP address.

Procedure

Step 1 In the VMware vSphere Client, choose **Home > Inventory > Hosts and Clusters**.

Step 2 Navigate to the newly deployed (and powered on) VM.

Step 3 Click the **Console** tab to access the CLI.

Step 4 In the CLI, register each VM as follows, depending on the type of VM and hypervisor:

VMware	Hyper-V Hypervisor
ASA 1000V VM	
vm-name> **enable** Password: vm-name# **configure terminal** vm-name(config)# **vnmc policy-agent** vm-name(config-vnmc-policy-agent)# **registration host** *n.n.n.n* vm-name(config-vnmc-policy-agent)# **shared-secret** *MySharedSecret*	—
VSG VM	

VMware	Hyper-V Hypervisor
vm-name# **configure terminal** vm-name(config)# **vnm-policy-agent** vm-name(config-vnm-policy-agent)# **registration-ip** *n.n.n.n* vm-name(config-vnm-policy-agent)# **shared-secret** *MySharedSecret*	vm-name# **configure** vm-name(config)# **nsc-policy-agent** vm-name(config-nsc-policy-agent)# **registration-ip** *n.n.n.n* vm-name(config-nsc-policy-agent)# **shared-secret** *MySharedSecret* vm-name(config-nsc-policy-agent)# **policy-agent-image bootflash:***vnmc-vsgpa.n.n.n.bin* vm-name(config-nsc-policy-agent)# **exit** vm-name(config)# **copy running-config startup-config** vm-name(config)# **exit** vm-name# **show nsc-pa status**
Enterprise VSM VM	
vm-name# **configure terminal** vm-name(config)# **vnm-policy-agent** vm-name(config-vnm-policy-agent)# **registration-ip** *n.n.n.n* vm-name(config-vnm-policy-agent)# **shared-secret** *MySharedSecret* vm-name(config-vnm-policy-agent)# **policy-agent-image bootflash:***vsmpa.n.n.n.bin* vm-name(config-vnm-policy-agent)# **copy r s**	vm-name# **configure terminal** vm-name(config)# **nsc-policy-agent** vm-name(config-nsc-policy-agent)# **registration-ip** *n.n.n.n* vm-name(config-nsc-policy-agent)# **shared-secret** *MySharedSecret* vm-name(config-nsc-policy-agent)# **policy-agent-image bootflash:***vsmpa.n.n.n.bin* vm-name(config-nsc-policy-agent)# **copy r s**
Cloud VSM VM	
vm-name# **configure terminal** vm-name(config)# **nsc-policy-agent** vm-name(config-nsc-policy-agent)# **registration-ip** *n.n.n.n* vm-name(config-nsc-policy-agent)# **shared-secret** *MySharedSecret* vm-name(config-nsc-policy-agent)# **policy-agent-image bootflash:***vsmpa.n.n.n.bin* vm-name(config-nsc-policy-agent)# **copy r s**	vm-name# **configure terminal** vm-name(config)# **nsc-policy-agent** vm-name(config-nsc-policy-agent)# **registration-ip** *n.n.n.n* vm-name(config-nsc-policy-agent)# **shared-secret** *MySharedSecret* vm-name(config-nsc-policy-agent)# **policy-agent-image bootflash:***vsmpa.n.n.n.bin* vm-name(config-nsc-policy-agent)# **copy r s**

Registering Third-Party VMs

Registering third-party VMs in Prime Network Services Controller is a two-step process, as described in the following topics:

1 Installing the Prime Network Services Controller Device Adapter, on page 25
2 Deploying and Registering Third-Party VMs, on page 26

Installing the Prime Network Services Controller Device Adapter

The Prime Network Services Controller Device Adapter enables third-party VMs (such as Citrix NetScaler load balancers) to register with Prime Network Services Controller.

Note

- Prime Network Services Controller Device Adapter is required and must be installed before you deploy and register third-party service nodes, such as Citrix NetScaler 1000V and Citrix NetScaler VPX service nodes.
- Adding or editing policies from the Prime Network Services Controller Device Adapter is not supported. All configuration must be performed using the Prime Network Services Controller GUI.
- You need to install the Prime Network Services Controller Device Adapter only once for each Prime Network Services Controller instance.

Before You Begin

Make sure that a network path exists between the Prime Network Services Controller Device Adapter IP address and the Prime Network Services Controller management IP address.

Procedure

Step 1 Use the VMware vSphere Client to log in to the vCenter server.

Step 2 Choose the host on which to deploy the Prime Network Services Controller Device Adapter.

Step 3 Choose **File > Deploy OVF Template**.

Step 4 In the wizard, provide the required information as described in the following table:

Screen	Action
Source	Navigate to and choose the nsc-device-adapter.3.2.*nx*.ova file.
OVF Template Details	Review the details of the Prime Network Services Controller Device Adapter template.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Specify a name and location for the VM. The name must begin with a letter.
Deployment Configuration	Choose **Installer**.
Storage	Choose the data store for the VM.

Screen	Action
Disk Format	Choose the required format.
Network Mapping	Choose the management network port group for the VM.
Properties	Provide the required information with particular attention to the following fields: • NTP—Enter the IP address for an NTP server. • Prime Network Services Controller Device Adapter IP Address RegIP—Enter the IP address for the Prime Network Services Controller server.
Ready to Complete	Review the deployment settings for accuracy.

Step 5 Click **Finish**.

Step 6 After the deployment is complete, power up the VM.
You can monitor the progress of the deployment by opening the VM console.

Step 7 Confirm that the Prime Network Services Controller Device Adapter VM is successfully registered with Prime Network Services Controller by logging in to the Prime Network Services Controller server and choosing **Administration > Service Registry > Providers**.
The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM that you deployed.

Deploying and Registering Third-Party VMs

This procedure describes how to deploy third-party VMs (such as Citrix NetScaler 1000V and Citrix NetScaler VPX) and register them with Prime Network Services Controller.

Before You Begin

Confirm the following:

- Prime Network Services Controller Device Adapter is successfully registered with Prime Network Services Controller by choosing **Administration > Service Registry > Providers**. The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM.
- The third-party OVA is available from the VMware vSphere Client.

Note If you are prompted with a third-party login screen requesting information (for example, management IP information or upload feature licenses), you can do either of the following:

- Use the existing configuration and ignore this screen.
- Refer to the following URL for additional Citrix licensing features: http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-10-1/ns-initial-config-using-ftu-wizard-tsk.html

Procedure

Step 1 In VMware, choose the host on which to deploy the third-party VM.

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

Step 3 In the wizard, provide the information as described in the following table.

Note The same information is required for both Citrix NetScaler 1000V and Citrix NetScaler VPX VMs.

Screen	Action
Source	Choose the OVA that you want to deploy.
OVF Template Details	Review the details.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the location for the VM files.
Disk Format	Choose the format in which to store the virtual disks.
Network Mapping	Choose the destination networks for the VM.

Step 4 In the Ready to Complete screen, review the deployment settings for accuracy, and then click **Finish**.

Step 5 Open the VM console so that you can monitor the deployment status.

Step 6 When prompted in the console, enter the following information for the VM:

- IP address
- Subnet mask
- Gateway IP address

Step 7 When the information is correct, enter **4** and press **Return**.
You can continue to monitor the progress in the console.

Step 8 Confirm that the VM is registered in Prime Network Services Controller by choosing **Resource Management > Resources > *resource***. For example, for Citrix NetScaler load balancer VMs, you would choose **Resource Management > Resources > VPX**.

Task 4—Verifying Service VM Registration

This procedure enables you to verify that the service VMs are registered with Prime Network Services Controller.

Procedure

Step 1 In Prime Network Services Controller, choose **Resource Management > Resources >** *resource* where *resource* is the type of resource, such as ASA 1000V, VSM, or VPX.

Step 2 Confirm that the table contains *registered* or *not-applied* in the Status column for each VM that you registered.

Step 3 To confirm that the Prime Network Services Controller Device Adapter is registered with Prime Network Services Controller, choose **Administration > Service Registry > Providers**.
The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter that you deployed and the Oper Status column should contain *registered* for the entries.

Task 5—Configuring a Tenant

Tenants are entities (such as businesses, agencies, or institutions) whose data and processes are hosted on VMs in a virtual data center. To provide firewall security for each tenant, you must first configure the tenant in Prime Network Services Controller.

Note

- For the purposes of this guide, a tenant is the lowest level of configuration required. You can configure subordinate levels as needed.
- For differences in the interface when Prime Network Services Controller is installed in Orchestrator mode, see the Integrating with DCNM section in the *Cisco Prime Network Services Controller 3.2 User Guide*.

Procedure

Step 1 Choose **Tenant Management > root**.

Step 2 In the upper-right corner of the Tenant Management Root pane, click **Create Tenant**.

Step 3 In the Create Tenant dialog box, enter a name and brief description for the tenant, and then click **OK**.
The tenant name can contain 1 to 32 alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.

The newly created tenant is listed in the navigation pane under root.

Task 6—Configuring Access Policies

The following access policies prevent unauthorized access to resources:

- IP groups identify the IP addresses that can access cloud or enterprise resources.

Caution Failure to configure at least one IP group could permit unauthorized access to your InterCloud switch, cloud VMs, or enterprise data center.

- ACL policies specify the criteria that enables or denies access to a tenant and its resources.

For information on configuring IP groups and ACL policies, see the following topics:

- Configuring an IP Group, on page 29
- Configuring an ACL Policy, on page 29

Configuring an IP Group

An IP group protects cloud resources by ensuring that SSH access to the public interface of cloud VMs in a Virtual Private Cloud (VPC) is allowed ONLY from IP addresses in the IP group.

In InterCloud Management in Prime Network Services Controller, IP groups are applied on a per-VPC basis. This is, only those IP addresses in an IP group that is associated with a VPC have SSH access to the cloud VMs for that VPC.

Caution Failure to configure at least one IP group could permit unauthorized access to your cloud VMs, InterCloud Switch, and enterprise data center.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > IP Groups**.

Step 2 Click **Add IP Group**.

Step 3 In the Add IP Group dialog box, do the following:

a) Enter a name for the IP group.

b) Click **Add IP Address Range**.

c) In the Add IP Address Range dialog box, enter the NATed IP address and prefix for the range of IP addresses to add to the IP group.

Step 4 Click **OK** in the open dialog boxes.

Configuring an ACL Policy

You can define criteria for ACL policies for the following attributes:

- Source conditions
- Destination conditions
- Service
- Protocol

- EtherType
- Time ranges or frequency

Procedure

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policies > ACL> ACL Policies** where *tenant* is the tenant that you created in Task 5—Configuring a Tenant, on page 28.

Step 2 In the General tab, click **Add ACL Policy**.

Step 3 In the Add ACL Policy dialog box, enter a name and description for the policy, and then click **Add Rule**.

Step 4 In the Add Rule Policy dialog box, define a rule using the information described in Add ACL Policy Rule Dialog Box, on page 30, and then click **OK** in the open dialog boxes.

Add ACL Policy Rule Dialog Box

Field	Description
Name	Rule name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	Brief rule description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Action to Take	1 Click the action to take if the rule conditions are met: • **Drop—**Drops traffic or denies access. • **Permit—**Forwards traffic or allows access. • **Reset—**Resets the connection. 2 Check the **Log** check box to enable logging.
Condition Match Criteria	Do one of the following: • Click **match-all** for the ACL Policy Rule to match all the conditions (AND). • Click **match-any** for the ACL Policy Rule to match any one condition (OR).
Src-Dest-Service Tab A rule can have a service condition or a protocol condition, but not both.	

Field	Description
Source Conditions	**1** Click **Add**. **2** Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value **3** Click **OK**.
Destination Conditions	**1** Click **Add**. **2** Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value **3** Click **OK**.
Service	**1** Click **Add**. **2** Enter the required values for following: • Operator • Protocol • Port **3** Click **OK**.

Field	Description
Protocol Tab	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the **Operator** drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
Ether Type Tab	Specify the encapsulated protocols to be examined for this rule: **1** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Greater than, Less than, Member, Not Member, In range, or Not in range. **2** In the Value fields, specify the hexadecimal value, object group, or hexadecimal range.
Time Range Tab	
To apply the rule all the time	Check the **Always** check box.
To apply the rule for a specific time range	**1** Uncheck the **Always** check box. **2** Check the **Range** check box. **3** In the Absolute Start Time fields, provide the start date and time. **4** In the Absolute End Time fields, provide the end date and time.

Field	Description
To apply the rule based on membership in an object group	1 Uncheck the **Always** check box. 2 Check the **Pattern** check box. 3 From the Operator drop-down list, choose **member (Member of)**. 4 Do any of the following : • From the **Select Object Group** drop-down list, choose an existing object group. • Click **Add Object Group** to create a new object group. • Click the Resolved Object Group link to review or modify the specified object group.
To apply the rule on a periodic basis, with the frequency you specify	1 Uncheck the **Always** check box. 2 Check the **Pattern** check box. 3 From the Operator drop-down list, choose **range (In range)**. 4 In the Begin fields: 1 From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range. 2 Choose the beginning hour and minute, and AM or PM. 5 In the End fields: 1 From the End drop-down list, choose the ending day of the week or frequency. 2 Choose the ending hour and minute, and AM or PM. **Note** If you choose a frequency from the Begin drop-down list, choose the same frequency from the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.

Field	Description
Advanced Tab	Specify any source port attributes that must be matched for the current policy to apply: **1** Click **Add**. **2** Provide the required information in the following fields, and then click **OK**: • Attribute Name • Operator • Attribute Value

Task 7—Configuring a Service Profile

A profile is a collection of policies. By creating a profile and then applying that profile to one or more objects (such as a data interface for an ASA 1000V or a VSM port profile), you can ensure that those objects have consistent policies.

Procedure

Step 1 Choose **Policy Management > Service Profiles > root >** *tenant* **> Compute Firewall > Compute Security Profiles** where *tenant* is the required tenant.

Step 2 In the General tab, click **Add Compute Security Profile**.

Step 3 In the Add Compute Security Profile dialog box, enter a name and description for the security profile, and then click **OK**.

Task 8—Configuring a Device Profile

Device profiles enable you to apply multiple policies to one or more devices and ensure policy consistency across devices that use the same profile.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root >** *tenant* **> Device Profiles** where *tenant* is the required tenant.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, enter a name and description for the device profile, and then click **OK**.

Task 9—Importing Service Images

Importing service images enables you to instantiate service devices from images, associate them with tenants, and deploy them on the hypervisor.

All imported service images are listed in the Images table (**Resource Management > Resources > Images**).

Procedure

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

Step 2 Click **Import Service Image**.

Step 3 In the Import Service Image dialog box:

a) Enter a name and description for the image you are importing.
b) Choose the service image type.
c) Enter a version to assign to the image.
d) In the Import area, provide the following information, and then click **OK**:

- Protocol to use for the import operations: FTP, SCP, or SFTP.
- Hostname or IP address of the remote host to which you downloaded the images.
- Account username for the remote host.
- Account password for the remote host.
- Absolute image path and filename, starting with a slash, such as /mnt/nexus-1000v.VSG2.1.1.ova.

Task 10—Adding Service Devices

After tenants, policies, and profiles are configured, you can add resources, or *service devices*, to the tenants. Service devices include compute firewalls, edge firewalls, edge routers, and load balancers. You can add service devices to tenants in either of the following ways:

- If a service device has been deployed in your hypervisor and is registered with Prime Network Services Controller, you can associate that service device with a tenant.
- If you have imported service images, you can instantiate service devices for a tenant from a service image.

For some resources, if you have created a resource pool, such as a VSG pool, you can associate the pool with a tenant.

Wizards guide you through the process of adding service devices to tenants, ensuring that the required information is provided for configuration.

Note We recommend that you add service devices at the tenant level or below, and not at the root level.

The following procedure provides the high-level steps required for adding a service device; the specific information required depends on the service device that you are adding. For additional information on any of the screens, see the online help.

Before You Begin

Confirm at least one of the following:

- A service device has been deployed in your hypervisor and is registered with Prime Network Services Controller.
- A service image has been imported.

Procedure

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

Step 2 In the Network Services tab, from the **Actions** drop-down list, choose the type of service device that you want to add, such as a compute firewall or load balancer.
The wizard opens and displays the Properties screen.

Step 3 In the Properties screen, enter the required information, and confirm that the policy or policies are correct for the service device.

Step 4 In the Service Device screen, do one of the following:

- To assign a deployed service device, click **Assign** and then choose the required device or device pool.
- To instantiate a service device from an imported service image, click **Instantiate** and provide the required information for the service device.

  Note Compute firewalls and edge routers offer deployment options when they are instantiated from an image. For more information, see the following topics:

  - Compute Firewall Deployment Options, on page 36
  - Edge Router Deployment Options, on page 37

Step 5 (Instantiate option only) In the Placement screen, navigate to and choose the VM host or resource pool to use for the service device.

Step 6 In the Interfaces screen, configure the required interfaces. The number and types of interfaces to be configured depend on the type of service device and whether or not it was instantiated from a service image. Tooltips provide specific requirements for each service device.

Step 7 In the Summary screen, review the information for accuracy, and then click **Finish**.

Compute Firewall Deployment Options

VSG compute firewalls are available in the following deployment models based on the memory, CPU speed, and number of virtual CPUs. Choose the deployment size that is appropriate for your environment.

Deployment Size	Memory	CPU Speed	Number of Virtual CPUs
Small	2 GB	1.0 GHz	1
Medium	2 GB	1.5 GHz	1

Deployment Size	Memory	CPU Speed	Number of Virtual CPUs
Large	2 GB	1.5 GHz	2

Edge Router Deployment Options

Edge routers can support different amounts of throughput based on the number of virtual CPUs and amount of memory. Choose the number of virtual CPUs and amount of memory that are appropriate for your environment and for the desired throughput.

Throughput	Technology Package		
Speed	**Standard**	**Advanced**	**Premium**
10 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
50 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
100 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
250 Mbps	4 vCPU, 4 GB RAM	4 vCPU, 4 GB RAM	4 vCPU, 4 GB RAM
500 Mbps	4 vCPU, 4 GB RAM	—	—
1 Gbps	4 vCPU, 4 GB RAM	—	—

Task 11—Creating an Edge Security Profile

If you created an edge firewall in Task 10—Adding Service Devices, on page 35, you can create an edge security profile. Edge security profiles include the policies and policy sets that you choose to ensure security for your edge firewalls.

Procedure

Step 1 Choose **Policy Management > Service Profiles > root >** *tenant* **> Edge Firewall > Edge Security Profiles**.

Step 2 In the General Tab, click **Add Edge Security Profile**.

Step 3 In the Add Edge Security Profile dialog box, do the following:

a) In the General tab, enter a name and description for the Edge Security Profile.

b) In the Ingress tab, choose a policy set from the Ingress Policy Set drop-down list.

c) In the Egress tab, choose a policy set from the Egress Policy Set drop-down list.

Note To add an ACL Policy set, click **Add ACL Policy Set** and follow the instructions in Task 6—Configuring Access Policies, on page 28.

Step 4 In the NAT tab, either choose an existing NAT policy set or add a new policy set, as follows:

a) Click **Add NAT Policy Set**.

b) In the Add NAT Policy Set dialog box, enter the information as described in Add NAT Policy Set Dialog Box, on page 38.

c) To add a NAT policy, click **Add NAT Policy** and enter the information as described in Add NAT Policy Dialog Box, on page 38.
d) To add a rule to the NAT policy, click **Add Rule** and enter the information as described in Add NAT Policy Rule Dialog Box, on page 39.
e) To add a rule condition, click **Add Rule Condition** and enter the information as described in Add Condition Dialog Box, on page 41.

For field-level information on the VPN and Advanced tabs, see the online help.

Step 5 Click **OK** in the open dialog boxes.

Add NAT Policy Set Dialog Box

Field	Description
Name	Policy set name.
Description	Brief description of the policy set.
Admin State	Whether the administrative state of the policy set is enabled or disabled.
Policies Area	
Add NAT Policy	Adds a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Add NAT Policy Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.

Field	Description
Rule Table	
Add Rule	Adds a rule to the current policy.
Name	Rule name.
Source Condition	Source attributes that must be matched for the current policy to apply.
Destination Condition	Destination attributes that must be matched for the current policy to apply.
Protocol	Protocols to which the policy applies.
Action	Whether the NAT translation is static or dynamic.
Source IP Pool	Translated address pool for a source IP address match condition.
Source Port Pool	Translated address pool for a source port match condition.
Source IP PAT Pool	Translated address pool for a source port address translation (PAT) match condition.
Destination IP Pool	Translated address pool for a destination IP address match condition.
Destination Port Pool	Translated address pool for a destination port match condition.

Add NAT Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Original Packet Match Conditions	
Source Match Conditions	Source attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.

Field	Description
Destination Match Conditions	Destination attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.
Protocol	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
NAT Action Table	
NAT Action	From the drop-down list, choose the required translation option: Static or Dynamic.
Translated Address	Identify a translated address pool for each original packet match condition from the following options: • Source IP Pool • Source Port Pool • Source IP PAT Pool • Destination IP Pool • Destination Port Pool For example, if you specify a source IP address match condition, you must identify a Source IP Pool object group. Similarly, a destination network port match requires a Destination Port Pool object group. The Source IP PAT Pool option is available only if you choose dynamic translation. Click **Add Object Group** to add object groups for the translation actions.

Field	Description
NAT Options	Check and uncheck the check boxes as required: • Enable Bidirectional—Check the check box for connections to be initiated bidirectionally; that is, both to and from the host. Available only for static address translation. • Enable DNS—Check the check box to enable DNS for NAT. • Enable Round Robin IP—Check the check box to allocate IP addresses on a round-robin basis. Available only for dynamic address translation. • Disable Proxy ARP—Check the check box to disable proxy ARP. Available only for static address translation.

Add Condition Dialog Box

Field	Description
Attribute Type	Attribute type for this condition. The available types depend on the type of policy that is being configured. For example, the attribute types available for an ACL policy differ from those available for a NAT policy.
Expression	
Attribute Name	Attribute names. The attributes that are available depend on the hypervisor that you are using.
Operator	Available operators to apply to the attribute. Depending upon the operator you choose, different information is required in the **Attribute Value** field.
Attribute Value	Attribute value. The information required depends upon the attribute name and operator.

Task 12—Enabling Logging

Configuring and enabling a syslog policy for a service device ensures that you receive syslog messages for the severities that you specify. For example, depending on the syslog policy, you could receive syslog messages notifying you that a firewall rule has been invoked and that a permit or deny action has been taken.

Logging enables you to monitor traffic, troubleshoot issues, and verify that devices are configured and operating properly.

You can configure and enable syslog policies for service devices by doing either or both of the following:

Enabling Policy-Engine Logging in a Monitor Session

Configuring a syslog policy enables you to specify the level of syslog messages to log and where to log the messages.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the Syslog table, choose **default**, and then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.

Step 4 In the Syslog Policy table, choose the primary server type, and then click **Edit**.

Step 5 In the Edit Syslog Client dialog box, provide the following information, and then click **OK** in the open dialog boxes:

- Hostname/IP Address—Enter the syslog server IP address or hostname.
- Severity—Choose **information (6)**.
- Admin State—Choose **enabled**.

Enabling Global Policy-Engine Logging

Prime Network Services Controller enables you to set system-wide logging for the policy engine.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles > default**.

Step 2 In the Device Profiles pane, click the **Policies** tab.

Step 3 In the Policy Engine Logging area at the lower-right of the Policies tab, click **Enabled**, and then click **Save**.

Troubleshooting

The following topics can help you troubleshoot issues you might encounter when installing or configuring Prime Network Services Controller:

Updating Device Adapter Properties

If you enter incorrect information when deploying the Prime Network Services Controller Device Adapter, it will not be able to register with Prime Network Services Controller. For example, if you enter the wrong IP address or shared secret password when deploying the OVF, the Device Adapter cannot register with Prime Network Services Controller. If this occurs, use the following procedure to correct the situation.

Procedure

Step 1 In the hypervisor, stop the Device Adapter VM.

Step 2 Navigate to the OVF settings in the hypervisor and update the properties as required.

Step 3 Restart the Device Adapter.
The Device Adapter should register with Prime Network Services Controller.

Troubleshooting Devices and Services

You can use Prime Network Services Controller to troubleshoot faults associated with managed devices and services.

Procedure

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

Step 2 In the Network Services tab, choose the required service or device, and then click **Edit**.

Step 3 In the General tab, review the Status area for any issues or states affecting reachability, configuration, or association.

Step 4 In the Faults tab, review the displayed faults. To view additional information about a fault, double-click the entry, or choose the entry and then click **Properties**.

Upgrading Prime Network Services Controller

Upgrading Overview

Use the following procedure to upgrade to a newer Prime Network Services Controller version. For Prime Network Services Controller 3.2, the only supported upgrade paths are from Prime Network Services Controller 3.0 or 3.0.2. If you want to upgrade from VNMC 2.x to Prime Network Services Controller 3.2, you must first upgrade to Prime Network Services Controller 3.0 or 3.0.2.

Note If upgrading from VNMC 2.1, the VNMC 2.1 deployment must span only one disk. If it spans more than a single disk, you cannot upgrade to Prime Network Services Controller 3.x.

The following scenarios are not supported:

- Backing up from VNMC 1.x or 2.x and restoring to Prime Network Services Controller 3.2.

- Exporting from VNMC 1.x or 2.x and importing to Prime Network Services Controller 3.2.

To upgrade to Prime Network Services Controller 3.2, perform the following tasks:

1. If you are upgrading from VNMC 2.1, ensure that the VNMC 2.1 is deployed in a single disk. The upgrade will fail if the VNMC 2.1 deployment spans more than one disk.
2. If you are upgrading from VNMC 2.0 or 2.1, first upgrade to Prime Network Services Controller 3.0 or 3.0.2—See the *Cisco Prime Network Services Controller 3.0 Quick Start Guide* or the *Cisco Prime Network Services Controller 3.0.2 Quick Start Guide* at http://www.cisco.com/en/US/products/ps13213/prod_installation_guides_list.html.
3. Perform a full-state backup of Prime Network Services Controller 3.0 or 3.0.2 by using Secure Copy (SCP) protocol—See Backing Up Data, on page 44.
4. Upgrade to Prime Network Services Controller 3.2 by using the CLI **update bootflash** command—See Upgrading to Prime Network Services Controller 3.2, on page 45.

Note

- After you upgrade to Prime Network Services Controller 3.2, we recommend that you allow the system to synchronize and stabilize for at least 15 minutes. We recommend that you do not add or modify policies or service devices during this time.
- After you upgrade to Prime Network Services Controller 3.2, you might see the previous version in your browser. To view the upgraded version, clear the browser cache and history, and restart the browser. This applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Chrome.
- After you upgrade or reboot, it will take some time (about five minutes per node) for each service node to register with Prime Network Services Controller.

Backing Up Data

You can use either of the following methods to back up data before upgrading Prime Network Services Controller:

- To use the CLI, continue with this topic.
- To use the GUI, see Backing Up Prime Network Services Controller, on page 47 .

We recommend that you *do not* perform a backup when any of the following tasks are running on the system:

- Image import
- Migration of a VM to the cloud
- Deployment of an InterCloud Switch
- Creation of an InterCloud link

Note

- Temporarily disable the Cisco Security Agent (CSA) on the remote file server.
- Do not use TFTP to back up data.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

Note We recommend that you access the CLI via the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

Step 2 Enter system mode:

```
scope system
```

Step 3 Create a full-state backup file:

```
create backup scp://user@host/file fullstate enabled
```

where:

- *user* is the username.
- *host* is the system name.
- */file* is the full path and name of the backup file.

Step 4 When prompted, enter the required password.

Step 5 At the `/system/backup*` prompt, enter:

```
commit-buffer
```

Step 6 Log in to the SCP server, and make sure that */file* exists and that the file size is not zero (0).

Upgrading to Prime Network Services Controller 3.2

After you back up the data for your existing Prime Network Services Controller 3.0 or 3.0.2 installation, you can upgrade to Prime Network Services Controller 3.2.

Caution To save a state for recovery purposes, perform a backup before beginning the upgrade. For more information, see Backing Up Data, on page 44.

Note

- Do not use TFTP to update data.
- Do not access the GUI during the upgrade process.

Before You Begin

- Ensure that Prime Network Services Controller can access a DNS server and an NTP server. If a DNS server and an NTP server are not accessible, Prime Network Services Controller will not be able to access the Amazon Cloud Provider.

- Prime Network Services Controller 3.2 requires two virtual disks with the following configuration:
  - Disk 1—20 GB
  - Disk 2—200 GB

If you do not have two disks configured, you will not be able to upgrade to 3.2.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

Note We recommend that you access the CLI via the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 (Optional) Check the current version of the Prime Network Services Controller software:

```
show version
```

Step 4 Download the Prime Network Services Controller 3.2 image from a remote file server:

```
copy scp://imageURLtoBinFile bootflash:/
```

Step 5 Upgrade to Prime Network Services Controller 3.2:

```
update bootflash:/nsc.3.2.nx.bin
```

where *nsc.3.2.nx.bin* is the image name, such as nsc.3.2.1b.bin.

Step 6 Restart the server:

```
service restart
```

Step 7 (Optional) Confirm that the Prime Network Services Controller server is operating as desired:

```
service status
```

Step 8 (Optional) Verify that the Prime Network Services Controller software version has been updated:

```
show version
```

Step 9 To confirm that Prime Network Services Controller is fully accessible after the upgrade, log in via the GUI.
If your browser displays the previous version instead of the upgraded version, clear the browser cache and browsing history, and restart the browser.

Step 10 If you have changed the server hostname or fully qualified domain name (FQDN), reconfigure Prime Network Services Controller connectivity with the hypervisor. For more information, see Task 2—Configuring Connectivity with VM Managers, on page 19.

Note You must perform this step before attempting any enterprise VM-related operations.

Backing Up and Restoring Prime Network Services Controller

Backing Up and Restoring Overview

Note We recommend that you use backup and restore as a disaster recovery mechanism. To migrate configuration data from one Prime Network Services Controller server to another, see the Cisco Prime Network Services Controller 3.2 User Guide.

Prime Network Services Controller enables you to back up and restore data for the same Prime Network Services Controller version. That is, the following backup and restore operations are supported:

- Backing up VNMC 2.1 and restoring to VNMC 2.1.
- Backing up Prime Network Services Controller 3.2 and restoring to Prime Network Services Controller 3.2.

Backing up one version and restoring to another version (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.2) is not supported.

After you restore Prime Network Services Controller, we recommend that you allow the system to synchronize and stabilize for at least 15 minutes. Do not add or modify policies or service devices during this time.

Note Do not use TFTP for backup and restore operations.

The following topics describe how to back up and restore data for Prime Network Services Controller 3.2:

- Backing Up Prime Network Services Controller, on page 47
- Restoring the Previous Version, on page 48

Backing Up Prime Network Services Controller

Prime Network Services Controller enables you to perform a backup using either the GUI or the CLI. You can back up and restore data for the same Prime Network Services Controller version. Backing up one version and restoring to another (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.2) is not supported.

We recommend the following:

- Do not perform a backup when any of the following tasks are running on the system:
  - Image import
  - Migration of a VM to the cloud
  - Deployment of an InterCloud Switch
  - Creation of an InterCloud link

- Use backup and restore as a disaster recovery mechanism. To save a state for recovery purposes, perform a backup via the GUI or CLI, using one of the following methods:
  - CLI—See Backing Up Data, on page 44.
  - GUI—See the Cisco Prime Network Services Controller 3.2 User Guide.

Restoring the Previous Version

Note Do not use TFTP to update data.

Before You Begin

Temporarily disable the CSA on the remote file server.

Procedure

Step 1 Using the console, log in to Prime Network Services Controller as admin.

Note We recommend that you access the CLI via the console instead of using SSH. If the SSH session should disconnect, you will not be able to access the VM.

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 (Optional) Check the current version of Prime Network Services Controller:

```
show version
```

Step 4 Download the required image from a remote file server:

```
copy scp://imageURLtoBinFile bootflash:/
```

Step 5 Enter the **update** command:

```
update bootflash:/nsc.3.2.nx.bin force
```

Step 6 Restore the previous version:

```
restore scp://user@host-ip-address/tmp/backup-file.tgz
```

where:

- *user* is the username for accessing the remote host.
- *host-ip-address* is the IP address of the remote host with the backup file.
- */tmp/backup-file.tgz* is the path and filename for the backup file.

Step 7 Restart the server:

```
service restart
```

Step 8 (Optional) Confirm that the Prime Network Services Controller server is operating as desired:

```
service status
```

Step 9 (Optional) Verify that the Prime Network Services Controller software version has been restored:

```
show version
```

Step 10 Allow the system to synchronize and stabilize for at least 15 minutes. Do not add or modify policies or service devices during this time.

Step 11 To confirm that Prime Network Services Controller is fully accessible, log in via the GUI.

What to Do Next

Perform the post-restoration tasks described in Post-Restoration Tasks, on page 49.

Post-Restoration Tasks

After you successfully restore Prime Network Services Controller, complete the following tasks to reestablish the previous environment:

1. Update VM Managers—See Updating VM Managers, on page 49.
2. Reimport InterCloud and VM images—See Reimporting InterCloud and VM Images, on page 49.
3. Verify InterCloud status—See Verifying InterCloud Status, on page 50.

Updating VM Managers

You must update any configured VM Managers after you upgrade or restore Prime Network Services Controller.

Procedure

Step 1 Choose **Resource Management > VM Managers**.

Step 2 For VMware, for existing vCenters that you wish to retain, export and add the vCenter Extension plugin in VMware again. For more information, see Configuring Connectivity with VMware vCenter, on page 20.

Step 3 Check and delete any stale VM Manager entries.

Reimporting InterCloud and VM Images

Prime Network Services Controller does not restore service, VM, or InterCloud images that were previously imported. After you restore Prime Network Services Controller, complete the following procedure to reimport any required images.

Note Although you can upgrade a device out-of-band, doing so can result in traffic disruption for standalone service nodes.

Before You Begin

Restore Prime Network Services Controller as described in Restoring the Previous Version, on page 48.

Procedure

Step 1 Log in to the Prime Network Services Controller GUI.

Step 2 Review the imported images in the following screens:

- Service images—Choose **Resource Management > Resources > Images**.
- VM images—Choose **InterCloud Management > Enterprise > VM Images**.
- InterCloud images—Choose **InterCloud Management > InterCloud Link > Images**.

Step 3 For each image or image bundle that you want to reimport, note the image properties, such as the image name, operating system, and version. You can delete images that you no longer use or need.

Note To find the original location of the image or bundle, right-click the item and choose **Edit** or **Properties**. The dialog box includes the location and name of the source file.

Step 4 After noting the details, delete each image from Prime Network Services Controller.

Step 5 Reimport the images using the information that you collected in Step 3.

Verifying InterCloud Status

When a backup is performed, InterCloud-related tasks might be running but not completed. When the system is restored, Prime Network Services Controller starts the tasks from the point at which it was backed up. The following steps enable you to verify the status of InterCloud-related objects after you restore the system.

If a task fails for any reason, we recommend that you abort, terminate, or undeploy the task as appropriate, and then restart the task.

Note InterCloud functionality is supported only on VMware ESXi hypervisors.

Before You Begin

Successfully restore Prime Network Services Controller as described in Restoring the Previous Version, on page 48.

Procedure

Step 1 Choose **InterCloud Management > InterCloud Link > Provider Accounts** and confirm that the provider accounts are valid.

Step 2 Choose **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* and review the link status:

- If an InterCloud link was deployed in the backed-up system, but is no longer deployed:

  1. Choose **Resource Management > Resources > InterCloud**.
  2. If the Oper State column contains *lost-visibility*, wait approximately 10 minutes to see if visibility is regained. If visibility is not regained after 10 minutes, continue with the next steps.
  3. In VMware vCenter, verify that the InterCloud Extender exists in the VM placement detail. The path in VMware is *vm-manager* **>** *datacenter* **>** *cluster/host* **>** *extender-vm* **> Edit > Placement**.
  4. Log in to Amazon Web Services (AWS) Elastic Compute Cloud (EC2), and verify that the InterCloud Switch VM exists and has the same name and instance ID as that shown in the Prime Network Services Controller GUI.
  5. If the InterCloud Extender or InterCloud Switch does not exist, undeploy the link and then delete it.

- If an InterCloud link was being deployed when the system was backed up and completed deployment after the backup, Prime Network Services Controller will attempt to deploy the link from the point at which the system was backed up. In this situation, do either of the following, as appropriate:
  - Because the InterCloud Extender and InterCloud Switch exist in the network, you can wait to see if the link will be deployed within a few minutes.
  - If the InterCloud link deployment task displays an error, undeploy the link and redeploy it.

Step 3 Choose **InterCloud Management > Public Cloud VPCs >** *vpc* **> VMs** and review cloud VM status:

- If a cloud VM was deployed and existed in the backed-up system but was deleted due to VM termination after the system backup:

  1. In the list of cloud VMs, obtain the cloud instance ID.
  2. Check the public cloud for the selected cloud instance.
  3. If the VM instance does not exist on the cloud, you can delete the VM.

- If a user created a cloud VM instance after the backup, the restored system will not have a record of it. There is no way to recover the cloud VM instance. You will need to create a new cloud VM.
- If a cloud VM was being instantiated when the system was backed up and completed deployment after the backup, Prime Network Services Controller will start the VM instantiation task from the point at which the system was backed up. In this situation, do either of the following, as appropriate:
  - Wait for a while to see if the cloud VM will be instantiated.
  - If the instantiation fails for any reason, terminate the VM instantiation process, and initiate a new cloud VM instantiation.

Step 4 Reconcile the InterCloud Switch and cloud VM public IP addresses.
If the InterCloud Switch and cloud VM public IP addresses are changed after the backup, you need to restore the IP addresses manually. This situation can occur if the InterCloud Switch or cloud VM is rebooted after the backup. To reconcile the IP addresses:

1. If the InterCloud Switch is in lost-visibility state (**Resource Management > Resources > InterCloud**), reboot the InterCloud Switch by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* **> InterCloud Switch Tab >** *intercloud-switch* **> Reboot**.

2 If the cloud VM tunnel is not *up* (**InterCloud Management > Public Cloud > VPCs >** *vpc* **> VMs**), reboot the cloud VM.

Step 5 Reconcile the InterCloud link and cloud VM that were created after the backup on Prime Network Services Controller, as follows:

a) For InterCloud links that were created after the backup, do the following:

1 Remove the InterCloud Extender in vCenter.

2 Remove the InterCloud Switch in Amazon Web Services (AWS).

3 Remove the cloud VMs from AWS.

b) For Intercloud links that were deleted after the backup, perform the following steps in the Prime Network Services Controller GUI:

1 Terminate the cloud VMs by choosing **InterCloud Management > InterCloud Link > VPCs > VMs tab >** *cloud-vm* **> Terminate**.

2 Undeploy the InterCloud link by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* **> Undeploy**.

3 Delete the InterCloud link by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* **> Delete**.

Additional Information

Related Documentation

Cisco Prime Network Services Controller

The following Cisco Prime Network Services Controller documents are available on Cisco.com at the following URL:

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

- *Cisco Prime Network Services Controller 3.2 Documentation Overview*
- *Cisco Prime Network Services Controller 3.2 Release Notes*
- *Cisco Prime Network Services Controller 3.2 Quick Start Guide*
- *Cisco Prime Network Services Controller 3.2 User Guide*
- *Cisco Prime Network Services Controller 3.0 CLI Configuration Guide*
- *Cisco Prime Network Services Controller 3.0 XML API Reference Guide*
- *Open Source Used in Cisco Prime Network Services Controller 3.2*

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

Cisco CSR 1000V Documentation

The Cisco Cloud Services Router 1000V (CSR 1000V) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps12559/tsd_products_support_series_home.html

Cisco Nexus 1000V InterCloud Documentation

The Cisco Nexus 1000V InterCloud documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps12904/tsd_products_support_series_home.html

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available on Cisco.com at the following URL:

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

Cisco Prime Data Center Network Manager Documentation

The Cisco Prime Data Center Network Manager (DCNM) documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Cisco Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway (VSG) documentation is available on Cisco.com at the following URL:

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands