Cisco Prime Network Services Controller 3.2.2b Quick Start Guide

Getting Started with Cisco Prime Network Services Controller 2

Installation Requirements 2

VMware Installation Overview 7

Configuring Prime Network Services Controller 21

Troubleshooting 39

Upgrading Prime Network Services Controller 42

Backing Up and Restoring Prime Network Services Controller 46

Additional Information 49

Revised: July 20, 2016,

Getting Started with Cisco Prime Network Services Controller

The high-level workflow for installing and using Prime Network Services Controller includes the tasks in the following table. The related topics provide the information needed for completing these tasks.

Task	Related Topic
1. Confirm that the requirements for installation are met.	Requirements Overview, on page 2
2. Install Prime Network Services Controller and perform post-installation tasks.	VMware Installation Overview, on page 7
3. Configure Prime Network Services Controller for initial use.	Configuring Overview, on page 21

The following information applies to Prime Network Services Controller 3.2.2b:

- Prime Network Services Controller 3.2.2b can be installed in VMware environments in Standalone mode only. It is not available for OpenStack or Hyper-V Hypervisor environments, or in Orchestrator mode.
- You can upgrade a standalone deployment of Prime Network Services Controller 3.2 or 3.2.2a on VMware to Prime Network Services Controller 3.2.2b. If you are using an earlier version, upgrade to 3.2 or 3.2.2a before upgrading to 3.2.2b. For more information about upgrading to 3.2 or 3.2.2a, see the following guides:
    - Cisco Prime Network Services Controller 3.2 Quick Start Guide
    - Cisco Prime Network Services Controller 3.2.2 Quick Start Guide

Installation Requirements

Requirements Overview

This release of Prime Network Services Controller contains new support and bug fixes. For more information, see the Cisco Prime Network Services Controller 3.2.2b Release Notes.

Note

- Prime Network Services Controller 3.2.2b does not support Intercloud functionality. If you upgrade from a previous version of Prime Network Services Controller with Intercloud objects, the upgrade procedure will detect those objects and stop the upgrade process. You must delete all Intercloud objects before you can upgrade to 3.2.2b.
- Prime Network Services Controller 3.2.2b supports only VMware Hypervisor.

The following topics identify the primary requirements for installing and using Prime Network Services Controller:

- System Requirements, on page 3
- Hypervisor Requirements, on page 4
- Web-Based GUI Client Requirements, on page 4
- Configuring Chrome for Use with Prime Network Services Controller, on page 4
- Firewall Ports Requiring Access, on page 5
- Cisco Nexus 1000V Series Switch Requirements, on page 5
- Information Required for Configuration and Installation, on page 6
- Shared Secret Password Criteria, on page 6

System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four Virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk Space	220 GB on shared NFS or SAN, configured on two disks as follows: • Disk 1—20 GB • Disk 2—200 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	

Requirement	Description
Intel Virtualization Technology (VT)	Enabled in the BIOS

Hypervisor Requirements

Prime Network Services Controller is a virtual appliance that can be deployed on VMware vSphere. See the VMware Compatibility Guide to verify that VMware supports your hardware platform.

Requirement	Description
VMware	
VMware vSphere	5.1 and 5.5 with VMware ESXi (English only)
VMware vCenter	5.1 and 5.5 (English only)

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 4.

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

Cisco Nexus 1000V Series Switch Requirements

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

Information Required for Configuration and Installation

Required Information	Your Information
For Preinstallation Configuration	
ISO or OVA image location	
ISO or OVA image name	
Network / Port Profile for VM management [2]	
VM name	
VMware datastore location	
For Prime Network Services Controller Installation	
IP address	
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
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 6.)	

[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 to only 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	Weak Passwords
• At least eight characters. • Lowercase letters, uppercase letters, numbers, 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

VMware Installation Overview

You can install Prime Network Services Controller on VMware by using either an ISO or an OVA image. The installation time varies from 10 to 20 minutes, depending on the host and the storage area network load.

To install Prime Network Services Controller on VMware, complete the following tasks:

Task	Comments
1. Configuring VMware for Prime Network Services Controller, on page 8	Required for ISO installations only.
2. Installing Prime Network Services Controller	Use the procedure appropriate for your environment: • Installing Prime Network Services Controller Using the ISO Image, on page 9 • Installing Prime Network Services Controller Using the OVA Image, on page 10
3. Performing VMware Post-Installation Tasks, on page 12	Required for all installations.

Configuring VMware for Prime Network Services Controller

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

Before You Begin

- Confirm that the system requirements have been met (see Requirements Overview, on page 2).
- Gather the information required for configuration as identified in Information Required for Configuration and Installation, on page 6.

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 **4**.
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 **4**.

c) Click **New Hard Disk** and then click **Add** to create a new hard disk. The disk requires a minimum of 20 GB.

d) After you supply 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** check box, 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.

What to Do Next

Install Prime Network Services Controller as described in Installing Prime Network Services Controller Using the ISO Image, on page 9.

Installing Prime Network Services Controller Using the ISO Image

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

Note Prime Network Services Controller 3.2.2b can be installed on VMware in Standalone mode. Prime Network Services Controller 3.2.2b is not available for OpenStack or Hyper-V Hypervisor environments, or in Orchestrator mode.

Before You Begin

Confirm the following items:

- All system requirements are met as specified in System Requirements, on page 3.
- You have the information identified in Information Required for Configuration and Installation, on page 6.
- The hypervisor is configured and prepared for the Prime Network Services Controller installation procedure.
- 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 Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 5 In the Modes screen, choose the required modes:

- Prime Network Services Controller Operation Mode—Choose **Standalone**. Prime Network Services Controller 3.2.2b does not support Orchestrator mode.
- Prime Network Services Controller Configuration
  - Prime Network Services Controller Installation—Installs Prime Network Services Controller for the first time on a VM.
  - Restore Prime Network Services Controller—Restores a previous Prime Network Services Controller installation.

Step 6 In the Administrative Access screen, enter the admin and shared secret passwords with confirming entries.
For information on creating a strong password, see Shared Secret Password Criteria, on page 6.

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.

Step 9 To confirm that Prime Network Services Controller is accessible, connect to Prime Network Services Controller via the console for the CLI or a browser for the GUI.

Installing Prime Network Services Controller Using the OVA Image

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

Note Prime Network Services Controller 3.2.2b supports Standalone mode only.

Before You Begin

- Set your keyboard to United States English.
- 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.
- Gather the information identified in Information Required for Configuration and Installation, on page 6.

Procedure

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

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

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

Step 4 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.
Network Mapping	Choose the management network port group for the VM.
Properties Address any errors that are indicated in red text below a selection box. You can enter placeholder information as long as your entry meets the field requirements.	
A. IP Address	VM management IP address.
B. IP Netmask	VM subnet mask.
C. Gateway	Gateway IP address.

Screen	Action
D. DNS	• VM hostname. • VM domain. • DNS server IP address.
E. NTP	NTP server IP address.
F. Operation Mode	• Standalone—Operates as a standalone VM. • Orchestrator—Integrates through an orchestrator with a northbound application. **Note** Prime Network Services Controller 3.2.2b supports Standalone mode only.
G. Passwords	• Administrator password • Shared secret password
H. Restore	You can safely ignore the 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 for accuracy.

Step 5 Click **Finish**.
A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 6 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 7 Power on the Prime Network Services Controller VM.

Performing VMware Post-Installation Tasks

After you install Prime Network Services Controller, complete the following tasks to ensure that Prime Network Services Controller can communicate with VMware and the VMs that Prime Network Services Controller will manage:

Task	Related Topic
1. Configure NTP on VMs and Prime Network Services Controller.	Configuring NTP, on page 13
2. Configure connectivity with Prime Network Services Controller.	Configuring Connectivity with VMware vCenter, on page 14

Task	Related Topic
3. Register service VMs with Prime Network Services Controller.	Registering Service VMs on VMware, on page 16
4. (Recommended) Delete the default service path.	Deleting the Default Service Path, on page 20

Configuring NTP

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

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

If you do not configure these items with NTP, the components will not be able to register with Prime Network Services Controller.

For information on configuring NTP, see the following topics:

- Configuring NTP on VMs, on page 13
- Configuring NTP in Prime Network Services Controller, on page 14

Configuring NTP on VMs

Configure NTP on VMs by 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 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 the Citrix NetScaler documentation.
Citrix NetScaler VPX	For information on setting NTP on Citrix NetScaler 1000V, see the Citrix NetScaler documentation.
CSR 1000V	For information on setting NTP on CSR 1000V, see the CSR 1000V documentation.
VSG	Configure the NTP server in the Prime Network Services Controller GUI as described in the Prime Network Services Controller User Guide, section "Configuring NTP."

For this VM:	Do this:

VSM	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.

Configuring Connectivity with VMware vCenter

After installing Prime Network Services Controller, 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 will manage. Prime Network Services Controller communicates with the VMM to perform the following actions on the VMs that it manages:

- Obtain the VM attributes that Prime Network Services Controller uses for VM management.
- Instantiate, start, stop, restart, or delete VMs.
- Map VM network interfaces.
- Instantiate and configure services on service VMs.

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

1. Exporting the vCenter Extension File, on page 15
2. Registering the vCenter Extension Plug-in in vCenter, on page 15
3. Configuring Connectivity with vCenter, on page 16

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 15).

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

Registering the vCenter Extension Plug-in in vCenter

Register the vCenter extension plug-in so that you can create a VMM. The VMM enables Prime Network Services Controller communicate with vCenter 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 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 registering the vCenter extension plug-in with vCenter, configure Prime Network Services Controller so that it can communicate with the VMM for the hypervisor and the VMs that Prime Network Services Controller will manage.

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.

Registering Service VMs on VMware

Registering service VMs with Prime Network Services Controller ensures that Prime Network Services Controller recognizes and can communicate with the VMs.

See the following topics for information on how to register Cisco and third-party VMs that are deployed on VMware with Prime Network Services Controller:

- For Cisco service VMs, see Registering Cisco VMs, on page 16.
- For third-party service VMs, see Registering Third-Party VMs in VMware, on page 17.

Registering Cisco VMs

This procedure describes how to register the following Cisco VMs with Prime Network Services Controller. This procedure applies only to those Cisco VMs that have been installed directly on the hypervisor. Cisco VMs that are instantiated on a hypervisor through Prime Network Services Controller are automatically registered with Prime Network Services Controller upon instantiation.

- ASA 1000V
- VSM

You do not need to manually register a VSG that is installed directly on the hypervisor. The deployment procedure automatically registers with Prime Network Services Controller.

Before You Begin

- Configure NTP on the required hypervisor.
- Install the required Cisco VMs on the hypervisor.
- Confirm that each Cisco VM is deployed and powered on.
- 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 hypervisor, navigate to the VM to be registered with Prime Network Services Controller.

Step 2 Open a console window for the VM.

Step 3 In the CLI, register the VM as follows:

- ASA 1000V

```
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
vm-name(config-vnmc-policy-agent)# copy running-config startup-config
```

- VSM (Version 5.2(1)SV3(1.1) and higher)

```
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:vsmcpa.n.n.n.bin
vm-name(config-nsc-policy-agent)# copy running-config startup-config
```

- VSM (Versions prior to 5.2(1)SV3(1.1))

```
vm-name# configure
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: vnmc-vsgpa.n.n.n.bin
vm-name(config-vnm-policy-agent)# copy running-config startup-config
```

Registering Third-Party VMs in VMware

To register third-party VMs in Prime Network Services Controller, you must install the Prime Network Services Controller Device Adapter and then deploy and register the third-party VMs.

The following table identifies the tasks and related topics for deploying a Citrix NetScaler load balancer on VMware and registering the load balancer with Prime Network Services Controller:

Task	Comments
1. Install Prime Network Services Controller Device Adapter.	See Deploying the Prime Network Services Controller Device Adapter on VMware, on page 18.
2. (Optional) Configure licensing for the Citrix NetScaler load balancer.	See Importing and Configuring Load Balancer Licenses, on page 32.
3. Deploy a Citrix NetScaler load balancer.	Deploy the Citrix NetScaler load balancer VM in VMware. For more information, see the following URLs: • Citrix product documentation at http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html. • Citrix licensing information at http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-10-1/ns-initial-config-using-ftu-wizard-tsk.html.
4. Register the Citrix NetScaler load balancer with Prime Network Services Controller.	See Registering a Citrix NetScaler Load Balancer with Prime Network Services Controller, on page 20.

Deploying the Prime Network Services Controller Device Adapter on VMware

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

This procedure installs the Prime Network Services Controller Device Adapter on a VMware host using an OVA image. For information on how to deploy a VM using an ISO image, see the VMware documentation.

The following guidelines apply when deploying the Prime Network Services Controller Device Adapter:

- Prime Network Services Controller Device Adapter is required and must be installed before you can deploy and register third-party service nodes, such as Citrix NetScaler load balancers.
- 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.
- If you reinitialize Prime Network Services Controller, you must also reinitialize Prime Network Services Controller Device Adapter.

Before You Begin

Confirm 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.3.2.2b.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.
Storage	Choose the data store for the VM.
Disk Format	Choose the required format.
Network Mapping	Choose the management network port group for the VM.
Properties	Provide the following information: • VM IP address, subnet mask, and gateway IP address. • DNS server and NTP server IP addresses. • IP address for the Prime Network Services Controller server. • Password and shared secret password for access to the VM.
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.

Registering a Citrix NetScaler Load Balancer with Prime Network Services Controller

After a Citrix NetScaler load balancer VM starts, you can register it with Prime Network Services Controller.

Before You Begin

- Deploy a Citrix NetScaler load balancer on VMware. For more information, see Citrix product documentation at http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html.
- Configure a virtual server profile in Prime Network Services Controller.

Procedure

Step 1 In Prime Network Services Controller, choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, from the **Active** drop-down list, choose **Add Load Balancer**.

Step 3 In the Add Load Balancer wizard, provide the following information:

a) In the Properties screen, enter a name and hostname for the load balancer.

b) In the Service Device screen, choose **Register** and provide the following information:

- IP address
- Subnet mask
- Gateway IP address
- Device type
- Version
- Access credentials

c) In the Interfaces screen, add a data interface.

d) In the Virtual Server screen, add a virtual IP address and select the virtual server profile to use.

e) In the Summary screen, review the information for accuracy, and then click **Finish**.

Deleting the Default Service Path

By default, Prime Network Services Controller 3.2.2b includes a service path for use with the automatic instantiation of network services. This service path is not needed if it cannot be configured for the instantiation of network services in Orchestrator mode and can cause issues if it is used by a port profile. As a result, we recommend that you remove the default service path from Prime Network Services Controller 3.2.2b.

Procedure

Step 1 Choose **Policy Management > Service Policies > root > Policies > Service Path**.

Step 2 In the General tab, choose the default service path and then click **Delete**.

Configuring Prime Network Services Controller

Configuring Overview

The topics in the following table describe how to initially configure Prime Network Services Controller for use. The procedures reflect a high-level workflow and are intended to introduce you to the Prime Network Services Controller GUI and features. For more detailed information, see the Cisco Prime Network Services Controller User Guide or the online help.

Topic	Description
Task 1—Verifying Service VM Registration, on page 21	Confirms that the required service VMs are registered with Prime Network Services Controller.
Task 2—Configuring a Tenant, on page 22	Establishes a tenant to which you can allocate resources, such as compute or edge firewalls, edge routers, and load balancers.
Task 3—Configuring Access Policies, on page 22	Allows or prevents access to resources based on the criteria that you specify.
Task 4—Configuring a Service Profile, on page 27	Enables you to apply a set of security-related policies (such as access and threat mitigation policies) to one or more objects.
Task 5—Configuring a Device Profile, on page 28	Enables you to apply a set of custom security attributes and device policies to a port profile or other resources.
Task 6—Importing Images, on page 28	Enables you to import images for instantiation of service devices.
Task 7—Configuring Service Licenses, on page 29	Enables you to manage licensing for CSR 1000V edge routers and Citrix NetScaler load balancers.
Task 8—Adding Service Devices, on page 32	Enables you to place resources in service under a tenant or another level in the organizational hierarchy.
Task 9—Configuring an Edge Security Profile, on page 34	Creates an edge profile with policies and policy sets that you can apply to edge firewalls.
Task 10—Enabling Logging, on page 38	Ensures that you receive syslog messages for the severities that you specify.

Task 1—Verifying Service VM Registration

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

Procedure

Step 1 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.

Step 2 To confirm that service VMs are registered 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 3 Confirm that the table contains *registered* or *not-associated* in the Status column for each VM that you registered.

Task 2—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 The tenant is the lowest organizational level used in this guide. You can configure subordinate levels as needed.

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 3—Configuring Access Policies

Access policies prevent unauthorized access to resources. For example, ACL policies specify the criteria that enable or deny access to a tenant and its resources.

For more information, see the following topics:

- Access Policy Best Practices, on page 22
- Configuring an ACL Policy, on page 23

Access Policy Best Practices

Keep the following best practices in mind when configuring access policies:

- Identify, on paper, the services that you want to allow and the source of the service.
- Use objects groups whenever possible. That is, create logical groups of IP addresses, protocols, services, or ICMP types and refer to these groups in your access lists.
- Apply the ACL on the interface closest to the source of the traffic.
- Put the ACLs that are matched more frequently before those matched less frequently. The sooner a matching rule is found, the sooner the next packet can be handled.
- Organize your access list so that more specific references in a network or subnet appear before those that are more general.
- Include a **deny ip any any** rule implicitly at the end of any access list.
- Use ACLs and inspections for access control instead of relying on the lack of a NAT rule to prevent traffic.

Note Prime Network Services Controller supports up to eight instances of a single attribute in an ACL rule or vZone. If more than eight instances are specified, the configuration will fail when it is applied to a VSG.

For information on NAT best practices, see http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html#nat-bp.

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 2—Configuring a Tenant, on page 22.

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 23, 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.	
Source Conditions	1 Click **Add**. 2 Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value 3 Click **OK**.

Field	Description
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**.
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.

Field	Description
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.
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.

Field	Description
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.
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 4—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 5—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:

a) Enter a name and description for the profile.
b) Configure additional options as required.
c) Click **OK**.

Task 6—Importing Images

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

All imported 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 and password for the remote host.
- Absolute image path and filename, starting with a slash, such as /mnt/nexus-1000v.VSG2.1.1.ova.

Task 7—Configuring Service Licenses

Prime Network Services Controller enables you to configure licenses for edge routers and load balancers as described in the following topics:

- Configuring Smart Licensing for CSR 1000V Edge Routers, on page 29
- Configuring Load Balancer Licenses, on page 30

Configuring Smart Licensing for CSR 1000V Edge Routers

Smart Software Licensing is a tool that provides a central portal where all licenses (if supported by the device or application) per customer are shown. The portal provides you the ability to manage license distribution and measure software usage, by dividing accounts or departments into logical license pools. For more information about Cisco Smart Licensing, see http://www.cisco.com/c/en/us/products/abt_sw.html. Prime Network Services Controller supports Smart Licensing for Cisco Cloud Services Router 1000V version 3.12 and higher.

Note

- Only one smart license can be configured per tenant.
- Smart licensing in Prime Network Services Controller must be configured before an edge router is instantiated. To configure licensing after the edge router has been added in Prime Network Services Controller, you must execute the Smart License commands on the edge router.
- If you are registering an edge router that has been manually deployed, you must execute the Smart License commands on the edge router.

Before You Begin

Confirm the following:

- The license category (throughput level and technology package) has been purchased for the edge router. For more information on the license throughput level and technology packages available, see the Cisco Cloud Services Router 1000V Data Sheet.
- You have generated a license token from the Smart License portal (http://tools.cisco.com/rhodui/index).
- A tenant has been created.

Procedure

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

Step 2 In the License tab, click **Create Remote License Category**.

Step 3 Enter a category name and select the category applicable to the edge router you will add later, and then click **OK**.

Step 4 In the License tab, click **Create Smart License** and do the following:

a) Enter a license name.

b) (Optional) Enter a description.

c) Enter the token that you obtained from the Smart License portal.

d) Check the default call home check box or enter custom call home settings. Smart Licensing uses call home settings to communicate between the device and the Smart License server.

Note
- By default, call home options are configured on the Cisco Cloud Services Router 1000V. You can check the default call home check box in most cases.
- The following call home settings can be configured:
  - User Name—The user must be aaa-authorized.
  - Data Private Hostname—You can select or deselect this setting.
  - Proxy Server—If you check this option, you can enter your own proxy server and port to communicate with the Smart License server.

Step 5 Click **OK**. The Smart License is created for the selected tenant.

Step 6 Configure static routing so that the edge router can communicate with the Smart License server (**Policy Management** > **Service Policies** > **root** > **Policies** > **Routing** and click **Add Routing Policy**).

Step 7 Configure the DNS policy so that the edge router can resolve the Smart License server URL provided in the Call Home configuration (**Policy Management** > **Device Configurations** > **root** and click **Add Device Profile**).

Step 8 Add the required edge router. For more information on adding an edge router, see the online help.

What to Do Next

Confirm that the edge router is up and running in the Prime Network Services Controller GUI and that the edge router was instantiated with a license. (Choose **Resource Management** > **Managed Resources** > **root** > *tenant* > **Network Services** > *edge-router* > **Edit**. The Instantiated with License field should display Yes.)

If the Instantiated with License field displays No, see Registering CSR 1000V Licenses, on page 40 for information on registering the license with the edge router.

Configuring Load Balancer Licenses

Prime Network Services Controller enables you to import bundled Citrix NetScaler load balancer licenses and prepare those licenses for assigning to load balancers. For more information, see the following topics:

- Citrix Load Balancer Bundled Licenses, on page 30
- Importing and Configuring Load Balancer Licenses, on page 32

Citrix Load Balancer Bundled Licenses

A Citrix NetScaler load balancer license bundle is a .zip file that contains:

- One or more license files with the extension .lic.
- A license.xml file.

To view an example license.xml file, see Example license.xml File, on page 31.

The following conditions apply to license bundles:

- All license files in the bundle must be from the same vendor and for a single platform. For the current release, the only supported vendor/platform combinations are *Citrix* and *VPX* or *NS1000V*.
- All license files in the bundle must be of the same license category. For example, they must have same feature level (such as Standard or Premium) and throughput level (such as 10 or 1000).
- You must import the license bundle before instantiating the load balancer.
- You can import multiple license bundles, but the bundles cannot contain files with the same host ID or the same filename as an existing file.
- You cannot delete a license if it is assigned to a load balancer service device.

Example license.xml File

```
xml version="1.0" encoding="UTF-8"
<LicenseBundle>
  <Vendor>vendor-name</Vendor>
  <Platform>platform-type</Platform>
  <LicenseCategory>
     <FeatureLevel>feature-level</FeatureLevel>
     <ThroughputLevel>throughput-level</ThroughputLevel>
     <Licenses>
         <License file="license1.lic">
            <HostId>host1-id</HostId>
         <License file="license2.lic">
            <HostId>host2-id</HostId>
     </Licenses>
  </LicenseCategory>
</LicenseBundle>
```

License XML Tag	Description	Example
Vendor	Vendor from whom the licenses were obtained.	Citrix
Platform	Platform for which the licences can be used.	VPX
LicenseCategory	License category based on feature and throughput level.	
FeatureLevel	Feature level of the licenses in the bundle.	Standard
ThroughputLevel	Throughput level of the licenses in the bundle.	10
Licenses	Licenses in the bundle.	
License file	License filename.	"GID_6087fdd1_1435dda300b__6e02.lic"
HostId	Host ID of the device for which the license was issued.	005056a91f72

Importing and Configuring Load Balancer Licenses

This topic describes how to import bundled Citrix NetScaler load balancer licenses and prepare those licenses for assigning to load balancers.

Before You Begin

- Generate and download a license bundle for the required type of Citrix NetScaler load balancer. For more information, see:
    - Citrix Load Balancer Bundled Licenses, on page 30
    - http://support.citrix.com/article/CTX122426
- Confirm the license category that has been purchased. For more information about the available license categories for Citrix NetScaler load balancers, see http://support.citrix.com/article/CTX122426.

Procedure

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

Note If licenses are imported at root, all tenants below root can use the license. For more granular control, import licenses at the tenant level or lower.

Step 2 In the License tab, click **Import License Bundle**.

Step 3 Enter the import details, and then click **OK**. To check the import status, view the Recent Jobs window. After the import completes, the bundle is displayed in the table with a success status.

Step 4 Under the Feature License per platform area, choose the device and the license category.

Step 5 Click **Edit** to view the different licenses available for that category. You can also look at this table at a later time to see which licenses are assigned to instantiated load balancers.

You can now instantiate load balancers using the imported licenses as described in Task 8—Adding Service Devices, on page 32.

Task 8—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 images, you can instantiate service devices for a tenant from an image.

For some resources, such as VSGs, you can create a resource pool and then associate that 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 one of the following:

- A service device has been deployed on your hypervisor and is registered with Prime Network Services Controller (**Resource Management** > **Resources** > *resource*).
- The required image has been imported (**Resource Management** > **Resources** > **Images**).

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 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 33
  - Edge Router Deployment Options, on page 34

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 an image. Tooltips provide specific interface 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 the desired throughput.

Throughput	Technology Package		
Speed	**Standard**	**Advanced**	**Premium**
10 Mbps	1 vCPU, 2560 MB RAM	1 vCPU, 2560 MB RAM	1 vCPU, 2560 MB RAM
50 Mbps	1 vCPU, 2560 MB RAM	1 vCPU, 2560 MB RAM	1 vCPU, 2560 MB RAM
100 Mbps	1 vCPU, 2560 MB RAM	1 vCPU, 2560 MB RAM	1 vCPU, 2560 MB RAM
250 Mbps	4 vCPU, 4096 MB RAM	4 vCPU, 4096 MB RAM	4 vCPU, 4096 MB RAM
500 Mbps	4 vCPU, 4096 MB RAM	—	—
1 Gbps	4 vCPU, 4096 MB RAM	—	—

Task 9—Configuring an Edge Security Profile

If you created an edge firewall in Task 8—Adding Service Devices, on page 32, 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. For information on best practices when creating access policies, see Access Policy Best Practices, on page 22.

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 3—Configuring Access Policies, on page 22.

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 35.

c) To add a NAT policy, click **Add NAT Policy** and enter the information as described in Add NAT Policy Dialog Box, on page 35.

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 36.

e) To add a rule condition, click **Add Rule Condition** and enter the information as described in Add Condition Dialog Box, on page 38.

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	Change 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.

Field	Description
Admin State	Administrative status of the policy: enabled or disabled.
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 10—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, on page 39
- Enabling Global Policy-Engine Logging, on page 39

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:

- Registering CSR 1000V Licenses, on page 40
- Updating Device Adapter Properties, on page 40
- Device Adapter Not Reachable, on page 40
- Troubleshooting Devices and Services, on page 42

Registering CSR 1000V Licenses

If you configure Smart Licensing for a CSR 1000V edge router but the license does not automatically register with the edge router, you must manually register the license by using the CLI as described in this procedure.

Before You Begin

- In the Prime Network Services Controller GUI, confirm that the CSR 1000V edge router is up and running.
- Obtain the token from the Smart License portal.

Procedure

Step 1 Using the CSR 1000V management IP address, open the console for the edge router and log in to the CLI.

Step 2 Confirm that the license is not registered with the edge router by entering the **show license all** command. The Smart Licensing State field displays `unidentified` to indicate that no license is registered.

Step 3 Register the license with the edge router by entering the command **license smart register idtoken** *token* where *token* is the token obtained from the Smart License portal.

Step 4 Wait one minute and enter the **show license all** command again to confirm that the license has been registered with the edge router.

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.

Device Adapter Not Reachable

Certain circumstances, such as loss of network connectivity, can cause Prime Network Services Controller and the Prime Network Services Controller Device Adapter (Device Adapter) to lose communication with each other. If this occurs, use the instructions in this topic to recover communications.

First, verify that Prime Network Services Controller and the Device Adapter cannot communicate with each other. To do this, log in to the Prime Network Services Controller GUI and choose **Administration > Service Registry**. The Device Adapter should be displayed with two entries: managed-endpoint and mgmt-controller. If both entries are in *lost-visibility* state, it indicates that Prime

Network Services Controller and the Device Adapter have not been able to communicate with each other for an extended period of time. If Prime Network Services Controller and the Device Adapter can resume communication with each other, they will recover from the lost-visibility state.

If communication with the endpoint cannot be reestablished, you can remove the managed endpoints that are in lost-visibility state. **However, do not remove the managed endpoint for the Device Adapter.** Instead, replace the Device Adapter VM by using the same host information (hostname, access credentials, and management IP address) as the Device Adapter VM that is in lost-visibility state.

By removing the existing VM and recreating the Device Adapter VM with the same host information, Prime Network Services Controller will recognize the new Device Adapter VM as a replacement for the previous Device Adapter VM. In addition, the new Device Adapter VM will assume management of any third-party devices that the previous Device Adapter VM managed.

Scenario 1

In this scenario, Prime Network Services Controller is deployed with the Device Adapter.

1. Prime Network Services Controller deploys three load balancers (lb1, lb2, and lb3) that are managed by Adapter1.
2. Adapter 1 becomes unavailable.
3. The administrator does not remove the managed-endpoint for Adapter1.
4. The administrator removes the Adapter1 VM and recreates it by using the same host information as that for the original Device Adapter.
5. Prime Network Services Controller recovers connectivity and recognizes the new Device Adapter VM as a replacement for the previous Adapter1.
6. The new Adapter1 assumes management of the existing service nodes. In addition, Prime Network Services Controller will deploy new service nodes (such as lb4) that are assigned to the new Adapter1.

Note The new Adapter1 might attempt to reapply the configuration to the existing service nodes (lb1, lb2, and lb3). If this occurs, Prime Network Services Controller might update the configuration state for these service nodes to *failed-to-apply*. If this occurs, reboot the service nodes to display the correct configuration state.

Scenario 2

In this scenario, the new Device Adapter has different host information than the original Device Adapter.

If the new Device Adapter VM has different host information, such as a different management IP address or hostname, Prime Network Services Controller might not recognize it as a replacement for the existing VM. All existing service nodes that were managed by the original Device Adapter VM will continue to run, but in headless mode. Any additional configuration changes that are made to those service nodes by using Prime Network Services Controller will not be applied. In addition, because Prime Network Services Controller does not recognize the new Device Adapter VM as the replacement for the previous Device Adapter VM, subsequent deployments will fail because they cannot be assigned to the original Device Adapter.

As in the previous scenario, Prime Network Services Controller is deployed with Device Adapter (Adapater1).

1. Prime Network Services Controller deploys three load balancers (lb1, lb2, and lb3).
2. Adapter1 enters lost-visibility state.
3. The administrator does not remove the managed-endpoint for Adapter1.

4. The administrator deploys a new Device Adapter VM (Adapter2) with a management IP address that is different from the management IP address for Adapter1.
5. Prime Network Services Controller does not recognize Adapter2 as a replacement for Adapter1 and instead considers it a new instance of the Device Adapter.
6. All services (lb1, lb2, and lb3) that were managed by Adapter1 continue to run, but in headless mode; that is, any attempt by Prime Network Services Controller to change the configuration for those services fails.
7. Additional deployments, such as lb4, might be assigned to Adapter1 for management and will therefore fail to complete deployment.

Note If you delete the managed-endpoint for the Device Adapter before replacing the Device Adapter VM, Prime Network Services Controller will not recognize the new Device Adapter VM as a replacement for the original Device Adapter VM. Instead, you will encounter the behavior described in this scenario.

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

The following information applies to Prime Network Services Controller 3.2.2b:

- Prime Network Services Controller 3.2.2b does not support InterCloud functionality. If you upgrade from a previous version of Prime Network Services Controller with InterCloud objects, the upgrade procedure will detect those objects and stop the upgrade process. You must delete all InterCloud object before you can upgrade to 3.2.2b.
- You can upgrade a standalone deployment of Prime Network Services Controller 3.2 or 3.2.2a on VMware to Prime Network Services Controller 3.2.2b. If you are using an earlier version, upgrade to 3.2 or 3.2.2a before upgrading to 3.2.2b.
- Upgrading to Prime Network Services Controller 3.2.2b is not available for OpenStack or Hyper-V Hypervisor environments, or in Orchestrator mode.

The following table shows the supported upgrade paths for Prime Network Services Controller 3.2.2b.

Table 1: Supported Upgrade Paths for Prime Network Services Controller 3.2.2b

Hypervisor	Supported Upgrade Versions	
	Standalone Mode	Orchestrator Mode
VMware	3.2, 3.2.2a	Not applicable

To upgrade from VNMC 2.x to Prime Network Services Controller 3.2.2b, you must first upgrade to on e of the supported upgrade versions.

The following scenarios are not supported:

- Backing up from VNMC 1.x or 2.x and restoring to Prime Network Services Controller 3.2.2b.
- Exporting from VNMC 1.x or 2.x and importing to Prime Network Services Controller 3.2.2b.

To upgrade to Prime Network Services Controller 3.2.2b, confirm that you meet the following requirements:

1. If you are upgrading from VNMC 2.1, ensure that 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 3.2 or 3.2.2a. See the *Cisco Prime Network Services Controller 3.2 Quick Start Guide* or the *Cisco Prime Network Services Controller 3.2.2 Quick Start Guide* at http://www.cisco.com/en/US/products/ps13213/prod_installation_guides_list.html.

Task	Notes
1. Perform a full-state backup of Prime Network Services Controller using the Secure Copy (SCP) protocol.	See Backing Up Data, on page 44.
2. Stop the Prime Network Services Controller Device Adapter VM.	Do not delete this VM yet. You can delete it after you verify that the upgrade is successful and that you do not need to restore the previous version.
3. Upgrade Prime Network Services Controller by using the CLI **update bootflash** command.	See Upgrading to Prime Network Services Controller , on page 45.
4. Using the new Prime Network Services Controller Device Adapter version, deploy a new Prime Network Services Controller Device Adapter VM and power it up.	When configuring the new Prime Network Services Controller Device Adapter VM, use the same host information (hostname, access credentials, and management IP address) as the previous version.
5. Verify that Prime Network Services Controller has been successfully upgraded.	**1** In the console, enter the **show version** command to confirm that the new version is installed. **2** Log in to the Prime Network Services Controller GUI and confirm that the service nodes are registered.
6. Delete the previous Prime Network Services Controller Device Adapter VM.	After verifying that the service nodes are registered, you can delete this VM.

After upgrading Prime Network Services Controller:

- Allow the system to synchronize and stabilize for at least 15 minutes. Do not add or modify policies or service devices during this time.
- Allow about 5 minutes per node for each service node to register with Prime Network Services Controller.
- If you see the previous version of Prime Network Services Controller in your browser, clear the browser cache and history, and restart the browser. This applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Google Chrome.

Backing Up Data

You can back up data before upgrading Prime Network Services Controller by using either the CLI or the GUI. To use the CLI, continue with this topic. To use the GUI, see Backing Up Prime Network Services Controller, on page 47.

Note

- Temporarily disable the Cisco Security Agent (CSA) on the remote file server.
- Do not use TFTP to back up data.
- Do not perform a backup while the system is importing images.
- 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.

Procedure

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

Step 2 Enter system mode:

```
scope system
```

Step 3 Create a full-state backup file:

```
create backup scp://user@host/file full-state 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

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

Note

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

Before You Begin

Confirm the following:

- You have backed up your current system for recovery purposes, if needed. For more information, see Backing Up Data, on page 44.
- Prime Network Services Controller has 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 .

Procedure

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

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 image from a remote file server:

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

Step 5 Upgrade to Prime Network Services Controller :

```
update bootflash:/nsc.3.2.2b.bin
```

where *nsc.3.2.2b.bin* is the image name.

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 VMM.

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

For more information, see Configuring Connectivity with VMware vCenter, on page 14.

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 use export and import operations.
- If you import a configuration from another Prime Network Services Controller instance, your current session will end. Log in again to continue.

For more information, see "Configuring Administrative Operations" in the Cisco Prime Network Services Controller 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 and restoring to Prime Network Services Controller .

Backing up one version and restoring to another version (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller) 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:

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

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) is not supported.

We recommend the following:

- Do not perform a backup while the system is importing images.
- Use backup and restore as a disaster recovery mechanism. To save a state for recovery purposes, perform a backup using one of the following methods:
    - Using the CLI—See Backing Up Data, on page 44.
    - Using the GUI—See the "Configuring Administrative Operations" section in the Cisco Prime Network Services Controller User Guide.

Restoring the Previous Version

Note

- Do not use TFTP to update data.
- 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.

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.

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:/ 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 48.

Post-Restoration Tasks

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

1. Updating VM Managers, on page 49
2. Reimporting Images, on page 49

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 To retain a VM Manager, add the VM Manager again. For more information, see Configuring Connectivity with VMware vCenter, on page 14.

Step 3 Delete any stale VM Manager entries.

Reimporting Images

Prime Network Services Controller does not restore 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 disrupt traffic for standalone service nodes.

Before You Begin

Restore Prime Network Services Controller as described in Restoring the Previous Version, on page 47.

Procedure

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

Step 2 Choose **Resource Management** > **Resources** > **Images**.

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

Tip To find the original location of the image, 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.

Additional Information

Related Documentation

Prime Network Services Controller

The Prime Network Services Controller documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-services-controller/tsd-products-support-series-home.html

Cisco Intercloud Fabric Documentation

The Cisco Intercloud Fabric documentation is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/intercloud-fabric/tsd-products-support-series-home.html

Cisco ASA 1000V Documentation

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

http://www.cisco.com/c/en/us/support/security/asa-1000v-cloud-firewall/tsd-products-support-series-home.html

Cisco Cloud Services Router 1000V Documentation

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

http://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v-series/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/c/en/us/support/switches/nexus-1000v-switch-vmware-vsphere/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/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/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/c/en/us/support/switches/virtual-security-gateway/tsd-products-support-series-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.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. 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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.