Cisco Prime Network Services Controller 3.2.2 Quick Start Guide

Getting Started with Cisco Prime Network Services Controller

Installation Requirements

Requirements Overview

This release of Cisco Prime Network Services Controller (Prime Network Services Controller) contains new features and bug fixes. For information about these features, see the Cisco Prime Network Services Controller 3.2.2 Release Notes.

✎

Note   Prime Network Services Controller 3.2.2 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 3.2.2.

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

- System Requirements, on page 2
- Hypervisor Requirements, on page 3
- Web-Based GUI Client Requirements, on page 4
- Configuring Chrome for Use with Prime Network Services Controller, on page 5
- 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 7

System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four Virtual CPUs	1.8 GHz
Memory	4 GB RAM

Requirement	Description
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	
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 VMware vSphere, KVM Hypervisor with OpenStack, 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.

- See the following links to verify that KVM on OpenStack supports your hardware platform:

    - OpenStack Compute and Image System Requirements

    - OpenStack for Cisco DFA Install Guide for Using the Cisco OpenStack Installer

Requirement	Description
VMware	

Requirement	Description
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)
KVM	
KVM Hypervisor	Ubuntu 12.04 LTS server, 64-bit
KVM Kernel	Version 3.2.0-52-generic
Cisco OpenStack Installer	Version depends on Installation mode: • Standalone Mode—Grizzly • Orchestrator Mode—Dynamic Fabric Automation (DFA) OpenStack
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

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	

Requirement	Description

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 / Instance name	
KVM: Flavor name	
KVM: Instance Security Group	
VMware: Data store 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	

Required Information	Your Information
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. The following table identifies the supported image formats and procedures for each environment.

Environment	Supported Image Format	Procedures
VMware vSphere Hypervisor	• ISO • OVA	To install using an ISO image, see: 1 Configuring VMware for Prime Network Services Controller, on page 8 2 Installing Prime Network Services Controller, on page 10 To install using an OVA image, see Deploying the Prime Network Services Controller OVA on VMware vSphere, on page 12.
KVM Hypervisor using Cisco OpenStack Installer (COI)	ISO	1 Configuring KVM on OpenStack for Prime Network Services Controller, on page 15 2 Installing Prime Network Services Controller, on page 10
Microsoft Hyper-V Hypervisor	ISO	1 Configuring Hyper-V Hypervisor for Prime Network Services Controller, on page 17 2 Installing Prime Network Services Controller, on page 10

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

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 **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**.
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.
This 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** 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 10.

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:

- All system requirements are met as specified in System Requirements, on page 2.

- 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. For more information, see the following topics:

  - Configuring VMware for Prime Network Services Controller, on page 8
  - Configuring KVM on OpenStack for Prime Network Services Controller, on page 15
  - Configuring Hyper-V Hypervisor for Prime Network Services Controller, on page 17

- 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**.

> **Note** For KVM/OpenStack installations, the IP address that you enter must be the IP address that you assigned to the Prime Network Services Controller instance.

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**:

- Prime Network Services Controller 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 following documentation:
    - "Integrating with DCNM" in the *Cisco Prime Network Services Controller 3.2 User Guide*
    - *Cisco Prime Network Services Controller 3.2.2 Release Notes*

- Prime Network Services Controller Configuration:
  - Prime Network Services Controller Installation—Choose if this is the initial Prime Network Services Controller installation on the VM.
  - Restore Prime Network Services Controller—Choose to restore 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.

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

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 2.

- Determine whether you will install Prime Network Services Controller in Standalone or Orchestrator mode:

  ◦ Standalone—Use if Prime Network Services Controller will operate as a standalone VM.

  ◦ Orchestrator—Use if Prime Network Services Controller will be integrated via an orchestrator with a northbound application. For more information, see "Integrating with DCNM" in the *Cisco Prime Network Services Controller 3.2 User Guide* and the *Cisco Prime Network Services Controller 3.2.2 Release Notes*.

  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

  - 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.
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 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 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 KVM on OpenStack for Prime Network Services Controller

Before you can install Prime Network Services Controller on KVM using the Cisco OpenStack Installer, you must create a flavor, import an image, and launch an instance. The following procedure describes how to complete these tasks.

✎

Note   After you install Prime Network Services Controller on OpenStack, you must disable anti-spoofing for service VMs to work. For information on disabling anti-spoofing in OpenStack, see the Cisco Prime Network Services Controller 3.2.2 Release Notes.

Before You Begin

In OpenStack:

- Confirm that you have admin privileges.

- Create a project on which to install Prime Network Services Controller.

- Configure the following items:

  - Two disks:

    - Cinder volume 1—20 GB

    - Cinder volume 2—200 GB

  - A security group that allows TCP, UDP, and ICMP traffic with Prime Network Services Controller.

For information on how to configure these items, see the OpenStack documentation at docs.openstack.org.

Procedure

Step 1   In the OpenStack Dashboard, choose **Admin > Flavors**, then click **Create Flavor**.

Step 2   In the Create Flavor dialog box, enter the following information, then click **Create Flavor**:

- Name—Enter the flavor name.

- vCPUs—Enter **4**.

- RAM MB—Enter **4096**.

Step 3   Choose **Admin > Images**, then click **Create Image**.

Step 4   In the Create an Image dialog box, provide the following information, then click **Create Image**:

- Name—Enter an image name.

- Image Location—Use this field if the image is available via HTTP from a remote host.

- Image File—Use this field if the image is available on your local system.

- Format—Choose **ISO - Optical Disk Image**.

- Public—Check the check box to make the image available to all tenants. Uncheck the check box to limit the image to a specific tenant.

After the image has been created, it appears in the Images table at **Admin > Images** or **Project >** *project* **> Manage Compute > Images & Snapshots**.

Step 5   Choose **Project >** *project* **> Instances > Launch Instance**.

Step 6   In the Launch Instance dialog box, enter the information in each tab as described in the following table:

Tab	Action
Details	1 Instance Source—Choose **Image**. 2 Image—Choose the image that you created in Step 4. 3 Instance Name—Enter a name for this instance. 4 Flavor—Choose the flavor that you created in Step 2. 5 Instance Count—Enter **1**.
Access & Security	Select the security group that was created as part of the prerequisites to permit traffic with Prime Network Services Controller.
Networking	Add the required networks from the list of available networks to the Selected Networks field. Prime Network Services Controller requires one vNIC.
Volume Options	1 Volume Options—Choose **Boot from volume**. 2 Volume—Choose the larger Cinder volume that you created as part of the prerequisites. 3 Device Name—Enter a unique name for the volume. 4 Delete on Terminate—Check the check box to delete the volume after the instance is launched. Uncheck the check box to retain the volume after the instance is launched.
Post-Creation	No action required.

Step 7   Click **Launch**.
When the VM is launched, the status in the Instances pane changes to Active.

Step 8   In the Instances pane, note the IP address of the launched instance.

Step 9   In the OpenStack Dashboard, locate the newly created VM and choose **More > Console** to start the Prime Network Services Controller installation procedure.
For information on installing Prime Network Services Controller, see Installing Prime Network Services Controller, on page 10.

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 **4**.
	     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.

Screen	Action
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 10.

Step 6 After Prime Network Services Controller is successfully deployed, click **Close** and 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 19	Ensures that service VMs can successfully register with Prime Network Services Controller.
Task 2—Configuring Connectivity with VM Managers, on page 21	Establishes a connection between Prime Network Services Controller and VM management software.
Task 3—Registering Service VMs, on page 25	Enables Prime Network Services Controller to recognize and communicate with service VMs.
Task 4—Verifying Service VM Registration, on page 36	Confirms that the required service VMs are registered with Prime Network Services Controller.
Task 5—Configuring a Tenant, on page 36	Establishes a tenant to which you can allocate resources, such as compute or edge firewalls, edge routers, and load balancers.

Topic	Description
Task 6—Configuring Access Policies, on page 37	Allows or prevents access to resources based on the criteria that you specify.
Task 7—Configuring a Service Profile, on page 42	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 42	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 43	Enables you to import images for instantiation of service devices.
Task 10—Configuring Service Licenses, on page 43	Enables you to manage licensing for CSR 1000V edge routers and Citrix NetScaler load balancers.
Task 11—Adding Service Devices, on page 46	Enables you to place resources in service under a tenant or another level in the organizational hierarchy.
Task 12—Creating an Edge Security Profile, on page 48	Creates an edge profile with policies and policy sets that you can apply to edge firewalls.
Task 13—Enabling Logging, on page 52	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
- Enterprise 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 20
- Configuring NTP in Prime Network Services Controller, on page 20

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."

VSM (enterprise)	Enter the following CLI command from the VSM console, where *x.x.x.x* is the NTP server IP address:
	
	<pre>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*</pre>

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 and VSG compute firewalls.

- 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 21

- Configuring Connectivity with KVM on OpenStack, on page 23

- Configuring Connectivity with Microsoft SCVMM, on page 24

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 21

2 Registering the vCenter Extension Plug-in in vCenter, on page 22

3 Configuring Connectivity with vCenter, on page 22

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 22).
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 VMM 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 KVM on OpenStack

Configuring a VM Manager (VMM) enables you to use to manage the VMs configured on the hypervisor.

Before You Begin

You must have the OpenStack admin or superuser username and password for OpenStack access.

Procedure

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

Step 2   In the Add VM Manager dialog box, add the required information as 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 OpenStack controller.
Secure	Check the check box to use HTTPS for connections between Prime Network Services Controller and OpenStack. Prime Network Services Controller uses HTTPS for communications with OpenStack by default. Uncheck the check box to use HTTP for connections between Prime Network Services Controller and OpenStack.

Field	Description
Domain Name / Username	OpenStack admin or superuser username.
Password	OpenStack admin or superuser password.
Port Number	Port number of the Keystone service running on the OpenStack controller.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.

- Operational State of *up*.

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 and your environment:

- For Cisco service VMs, see Registering Cisco VMs, on page 25.
- For third-party service VMs in a VMware environment, see Registering a Third-Party VM in VMware, on page 27.
- For third-party service VMs in an OpenStack environment, see Registering Third-Party VMs in OpenStack, on page 31.

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
- VSG
- Enterprise VSM

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 shown in the following table, depending on the type of VM and hypervisor.

Note   The VMs listed in this table are not supported in OpenStack in Prime Network Services Controller. As a result, the table does not include information for OpenStack.

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* **copy running-config startup-config**	—
VSG VM	
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)# **end** vm-name# **show vnm-pa status** vm-name# **copy running-config startup-config**	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**

Registering a Third-Party VM 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 involved in deploying a Citrix NetScaler VPX load balancer on VMware and registering the load balancer with Prime Network Services Controller:

Task	Notes
1. Confirm that the prerequisites are met.	See Prerequisites for Citrix NetScaler VPX Load Balancers in VMware, on page 27.
2. Install Prime Network Services Controller Device Adapter.	See Deploying the Prime Network Services Controller Device Adapter in VMware, on page 27.
3. (Optional) Configure licensing for the Citrix NetScaler VPX load balancer.	See Configuring Licensing for Citrix NetScaler Load Balancers, on page 45.
4. Deploy a Citrix NetScaler VPX load balancer.	See Deploying a Citrix NetScaler VPX Load Balancer in VMware, on page 29.
5. Register the Citrix NetScaler VPX load balancer with Prime Network Services Controller.	See Registering a Citrix NetScaler VPX Instance with Prime Network Services Controller, on page 30.

Prerequisites for Citrix NetScaler VPX Load Balancers in VMware

A network path must exist between the Prime Network Services Controller Device Adapter IP address and the Prime Network Services Controller management IP address.

The following guidelines apply when deploying Citrix NetScaler VPX load balancers in a VMware environment:

- 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.

Deploying the Prime Network Services Controller Device Adapter in 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.

✎

Note   If you reinitialize Prime Network Services Controller, you must also reinitialize Prime Network Services Controller Device Adapter.

Before You Begin

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.3.2.2*x*.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.

Deploying a Citrix NetScaler VPX Load Balancer in VMware

This procedure describes how to deploy third-party VMs (such as Citrix NetScaler 1000V and Citrix NetScaler VPX load balancers) in VMware so that you can 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.

Screen	Action
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.
After the VM is deployed, you can register it in Prime Network Services Controller.

Registering a Citrix NetScaler VPX Instance with Prime Network Services Controller

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

Before You Begin

Confirm the following:

- You have instantiated a Citrix NetScaler VPX load balancer as described in one of the following topics:

    - Deploying a Citrix NetScaler VPX Load Balancer in VMware, on page 29

    - Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack, on page 35

- A virtual server profile has been configured.

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

- Type—Choose **VPX**.

- Version—Choose the 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**.

Registering Third-Party VMs in OpenStack

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

The following table identifies the tasks involved in instantiating a Citrix NetScaler VPX load balancer on OpenStack and registering the load balancer with Prime Network Services Controller:

Task	Notes
1. Confirm that the prerequisites are met.	See Prerequisites for Citrix NetScaler VPX Load Balancers on OpenStack, on page 31.
2. Install Prime Network Services Controller Device Adapter.	See Installing the Prime Network Services Controller Device Adapter in OpenStack, on page 32.
3. Configure OpenStack.	Includes the following activities: **1** Creating an initialization shell script. **2** Uploading a Citrix NetScaler VPX image. **3** Creating the required subnets. See Configuring OpenStack for Citrix NetScaler VPX Load Balancers, on page 33 for details.
4. Instantiate a Citrix NetScaler VPX load balancer.	See Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack, on page 35.
5. Register the Citrix NetScaler VPX instance with Prime Network Services Controller.	See Registering a Citrix NetScaler VPX Instance with Prime Network Services Controller, on page 30.

Prerequisites for Citrix NetScaler VPX Load Balancers on OpenStack
The following table lists the prerequisites for instantiating Citrix NetScaler VPX load balancers on OpenStack and registering the load balancers with Prime Network Services Controller.

Item	Notes
Prime Network Services Controller has been installed and is accessible from OpenStack.	See the following topics: • Configuring KVM on OpenStack for Prime Network Services Controller, on page 15 • Installing Prime Network Services Controller, on page 10
A project has been created in OpenStack.	• The project name in OpenStack must be the same as the tenant name in Prime Network Services Controller when you register the Citrix NetScaler VPX load balancer. • The member list for the project includes a superuser admin with the admin role. For information on how to add an admin user to the member list and assign the admin role, see the OpenStack documentation at docs.openstack.org.
The following network requirements are met: • Two vNICs are available: One for management and one for data. • The management interface is in the same subnet as Prime Network Services Controller.	—

Installing the Prime Network Services Controller Device Adapter in OpenStack

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 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.

 • If you reinitialize Prime Network Services Controller, you must also reinitialize Prime Network Services Controller Device Adapter.

Use this procedure to install the Prime Network Services Controller Device Adapter in an OpenStack environment.

Before You Begin

Confirm the following in OpenStack:

- Prime Network Services Controller is running and accessible from OpenStack.

- A security group exists that allows TCP, UDP, and ICMP traffic from Prime Network Services Controller.

- A flavor exists for the Prime Network Services Controller Device Adapter.

- The Prime Network Services Controller Device Adapter image (nsc-device-adapter.3.2.2*x*.iso) has been uploaded to OpenStack.

For more information about OpenStack, see docs.openstack.org.

Procedure

Step 1	In the OpenStack Dashboard, in the Images table, choose the Prime Network Services Controller Device Adapter image, and click **Launch**.
Step 2	In the Launch Instance dialog box, provide the required information in the following tabs:

- Details—Specify the uploaded Prime Network Services Controller Device Adapter image, an instance name, the flavor for this instance, and the number of instances.

- Access & Security—Choose the security group that was created as part of the prerequisites.

- Networking—Choose the network to use for the Prime Network Services Controller Device Adapter vNIC. Prime Network Services Controller Device Adapter requires one vNIC.

Step 3	Click **Launch**.
Step 4	In the Instances pane, note the IP address of the launched instance.
Step 5	Click the Prime Network Services Controller Device Adapter instance and open the console. The Network Configuration screen is displayed.
Step 6	In the Network Devices area, click **Edit**.
Step 7	In the Edit Interface dialog box, enter the IP address and the netmask for the Prime Network Services Controller Device Adapter instance. The IP address is the one noted in Step 4.
Step 8	In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.
Step 9	In the Administrative Access screen, enter the Prime Network Services Controller IP address, admin password, and shared secret password.
Step 10	In the Summary screen, confirm that the information is accurate, and then click **Next**.
Step 11	When prompted, click **Reboot**. The Prime Network Services Controller Device Adapter is successfully installed.

Configuring OpenStack for Citrix NetScaler VPX Load Balancers

This procedure describes how to configure OpenStack so that you can instantiate a Citrix NetScaler VPX load balancer. The procedure involves:

- Creating an initialization shell script.

- Creating a flavor.

- Uploading a Citrix NetScaler VPX image.

- Creating the required subnet.

For more information about OpenStack and the commands included in this procedure, see the OpenStack documentation at docs.openstack.org.

Before You Begin

Confirm the following:

- The prerequisites have been met as described in Prerequisites for Citrix NetScaler VPX Load Balancers on OpenStack, on page 31.

- The Prime Network Services Controller Device Adapter has been installed on OpenStack and is registered with Prime Network Services Controller.

Procedure

Step 1 In OpenStack, create an initialization shell script as follows:

    a) Open an SSH session on the OpenStack controller.

    b) Create an initialization shell script that contains env variables for the default admin user and the project name.

        Note If needed, you can download a shell script from OpenStack using the OpenStack Horizon UI. The path is *tenant* > **Access & Security > API Access > Download OpenStack RC File**.

    c) Run the shell script.

Step 2 In the OpenStack dashboard, create a flavor with the following attributes:

- vCPU—2

- RAM—4096 MB

- Root Disk—0 MB

- Ephemeral Disk—0 MB

- Swap Disk—0 MB

Step 3 Upload a Citrix NetScaler VPX image using the following command:

    Note We recommend that you do not use the OpenStack dashboard to import the image.

```
# glance image-create --name image-name
--disk-format raw --container-format=bare --is-public=true
--file=/home/localadmin/images/image-name.raw
```

Your entry might resemble the following:

```
# glance image-create --name NSVPX-KVM-10.1-120.13 --disk-format raw
--container-format=bare --is-public=true --file=/home/localadmin/images/NSVPX-KVM-10.1-120.13_nc.raw
```

Step 4 After the image is uploaded, note the UUID of the image. Use the UUID instead of the image name to ensure that a unique value is specified.

    Tip If you need to obtain the UUID later, enter the following command:

```
# glance image-list | grep NSVPX*
```

Step 5 Create a private subnet by entering the following command. The Citrix NetScaler VPX data interface must be in a different subnet than the management interface.

```
# quantum net-create SubnetName
```

Instantiating a Citrix NetScaler VPX Load Balancer in OpenStack

This procedure describes how to instantiate a Citrix NetScaler VPX load balancer in OpenStack.

For more information about OpenStack and the commands included in this procedure, see the OpenStack documentation at docs.openstack.org.

Before You Begin

- Make sure that you have configured OpenStack as described in Configuring OpenStack for Citrix NetScaler VPX Load Balancers, on page 33.

- Confirm that anti-spoofing has been disabled on OpenStack. For information on disabling anti-spoofing in OpenStack, see the Cisco Prime Network Services Controller 3.2.2 Release Notes. If you do not disable anti-spoofing in OpenStack, service VMs will not work.

Procedure

Step 1 Obtain the following UUIDs:

- The subnet created in Configuring OpenStack for Citrix NetScaler VPX Load Balancers, on page 33.

- The network labeled "external."

Step 2 Enter the following command to create the Citrix NetScaler VPX instance:

```
# nova boot --flavor=flavorID --image=imageID --security-groups=securityGroup --nic net-id=netID1,
v4-fixed-ip=ipAddress1--nic net-id=netID2,v4-fixed-ip=ipAddress2 vmName
```

For example, your command might resemble the following:

```
# nova boot --flavor=99 --image=4c5716cd-eef9-4947-8bce-d2d1432d5ccd --security-groups=open_network
--nic net-id=645683e7-0b66-4c96-8f71-0edee35f1408,v4-fixed-ip=172.25.117.220
--nic net-id=39f7b506-b7f5-4bcd-b475-0e49b21da759,v4-fixed-ip=10.11.25.10 m-vpx-220
```

Note The two net-id values are different; be sure to enter the correct UUIDs.

Step 3 Note the IP address assignments. You must use the same IP address later in this procedure when you configure the Citrix NetScaler VPX load balancer.

Step 4 After the Citrix NetScaler VPX instance starts, access the instance console by clicking **Instances** in the dashboard and then choosing the **Console** tab.

Step 5 After the instance boots and the console displays a State UP message, press **Enter** twice to obtain the login prompt.

Step 6 Log in to the Citrix NetScaler VPX load balancer.

Step 7 At the command prompt, enter **shell**.

Step 8 In the shell, enter the following command:

```
root@ns# vi /nsconfig/na.conf
```

Step 9 Modify the na.conf file as follows:

a) Update the IPAddress line so that the IP address is the same as the management IP address that you used to boot the load balancer instance in Step 2.

b) Update the route information that is a few lines below the IPAddress line.

Step 10 Save the file and exit the editor.

Step 11 Reboot the Citrix NetScaler VPX load balancer instance.

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   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-applied* in the Status column for each VM that you registered.

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
- The tenant is the lowest organizational level used in this guide. 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

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 37
- Configuring an ACL Policy, on page 37

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   In Prime Network Services Controller you can have up to eight instances of a single attribute in an ACL rule or vZone. If there are more than eight instances 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 5—Configuring a Tenant, on page 36.
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 38, 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: a) Enter a name and description for the profile. b) Configure additional options as required. c) 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.

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—Configuring Service Licenses

Prime Network Services Controller enables you to configure licenses for the following service devices as described in the referenced topics:

- CSR 1000V edge routers—Configuring Smart Licensing for CSR 1000V Edge Routers, on page 43

- Citrix NetScaler load balancers—Configuring Licensing for Citrix NetScaler Load Balancers, on page 45

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 currently supports Smart Licensing for Cisco Cloud Services Router 1000V version 3.12.

✎

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 to 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.

Configuring Licensing for Citrix NetScaler Load Balancers

Prime Network Services Controller can manage feature licenses that require installation on load balancer service nodes for instantiated load balancers. The workflow begins with importing a license bundle and then installing the license during load balancer instantiation.

> **Note**
> - The license files must be imported before the load balancer is instantiated.
> - Multiple license bundles can be imported. However, the bundles cannot have files with the same host ID or the same filename as previous bundles.
> - You cannot delete a licenses if it is assigned to a load balancer service node.

Before You Begin

Confirm the following:

- The license files have been obtained. For information on how to generate and obtain the license files for a Citrix NetScaler load balancer, see http://support.citrix.com/article/CTX122426.
- The license category (feature and throughput level package) that has been purchased for the load balancer. For more information on the available license categories for the Citrix NetScaler load balancer, 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 an instantiated load balancer.
Step 6	Configure and add a load balancer. For information about adding a load balancer, see the online help.

Task 11—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 that at least one of the following exists:

- A service device has been deployed on 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.

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 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
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	—	—

Throughput	Technology Package		
1 Gbps	4 vCPU, 4096 MB RAM	—	—

Task 12—Creating an Edge Security Profile

If you created an edge firewall in Task 11—Adding Service Devices, on page 46, 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 37.

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 37.

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 48.

    c) To add a NAT policy, click **Add NAT Policy** and enter the information as described in Add NAT Policy Dialog Box, on page 49.

    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 50.

    e) To add a rule condition, click **Add Rule Condition** and enter the information as described in Add Condition Dialog Box, on page 51.

    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.

Field	Description
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.
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.

Field	Description
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.
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	

Field	Description
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.
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.

Field	Description
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 13—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 52
- Enabling Global Policy-Engine Logging, on page 53

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.

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

> ✎
>
> **Note**　Prime Network Services Controller 3.2.2 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 3.2.2.

Use the following procedure to upgrade to a newer Prime Network Services Controller version. For Prime Network Services Controller 3.2.2, the only supported upgrade paths are from Prime Network Services Controller 3.0.2 or 3.2 as shown in the following table.

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

Hypervisor	Supported Upgrade Versions	
	Standalone Mode	Orchestrator Mode
VMware	3.0.2, 3.2	3.2
Hyper-V Hypervisor	3.0.2, 3.2	—

To upgrade from VNMC 2.x to Prime Network Services Controller 3.2.2, you must first upgrade to Prime Network Services Controller 3.0.2 or 3.2.

Upgrade the individual components in the following sequence:

1 Upgrade Prime Network Services Controller.

2 Upgrade the Prime Network Services Controller Device Adapter.

3 (Orchestrator mode only) Upgrade the Prime Network Services Controller adapter in DCNM.

The following scenarios are not supported:

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

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

To upgrade to Prime Network Services Controller 3.2.2, 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 3.0.2 or 3.2—See the *Cisco Prime Network Services Controller 3.0.2 Quick Start Guide* or the *Cisco Prime Network Services Controller 3.2 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 3.0.2 or 3.2 by using Secure Copy (SCP) protocol—See Backing Up Data, on page 57.

4 Upgrade to Prime Network Services Controller 3.2.2 by using the CLI **update bootflash** command—See Upgrading to Prime Network Services Controller 3.2.2, on page 58.

Note
- After upgrading to Prime Network Services Controller 3.2.2, 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.

- After upgrading to Prime Network Services Controller 3.2.2, 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 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

✎

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.

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 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 3.2.2

✎

Note   Prime Network Services Controller 3.2.2 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 3.2.2.

After you back up the data for your existing Prime Network Services Controller installation, you can upgrade to Prime Network Services Controller 3.2.2.

✎

Note   • Do not use TFTP to update data.

          • Do not access the GUI during the upgrade process.

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 57.

- Prime Network Services Controller 3.2.2 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 3.2.2.

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 3.2.2 image from a remote file server:

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

Step 5   Upgrade to Prime Network Services Controller 3.2.2:

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

where *nsc.3.2.2x.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. For more information, see Task 2—Configuring Connectivity with VM Managers, on page 21.
    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 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 3.2.2 and restoring to Prime Network Services Controller 3.2.2.

Backing up one version and restoring to another version (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.2.2) 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:

-
-

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 3.2.2) 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 via the GUI or CLI, using one of the following methods:

  - CLI—See Backing Up Data, on page 57.

  - GUI—See the Cisco Prime Network Services Controller 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.3.2.2x.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 61.

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 61.

2   Reimport VM Images—See Reimporting VM Images, on page 62.

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. For more information, see Configuring Connectivity with VMware vCenter, on page 21.

Step 3   Check and delete any stale VM Manager entries.

Reimporting VM Images

Prime Network Services Controller does not restore service 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 60.

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 Prime Network Services Controller 3.2.2 Documentation Roadmap*

• *Cisco Prime Network Services Controller 3.2.2 Release Notes*

• *Cisco Prime Network Services Controller 3.2.2 Quick Start Guide*

• *Cisco Prime Network Services Controller 3.2 User Guide*

• *Cisco Prime Network Services Controller 3.2.2 Supported Devices Table*

• *Cisco Prime Network Services Controller 3.0 CLI Configuration Guide*

• *Cisco Prime Network Services Controller 3.2 XML API Reference Guide*

• *Open Source Used in Cisco Prime Network Services Controller 3.2.2*

Cisco ASA 1000V Documentation

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

http://www.cisco.com/c/en/us/support/security/asa-1000v-cloud-firewall/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/interfaces-modules/virtual-security-gateway-nexus-1000v-series-switch/
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/c/en/us/td/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.