Cisco Prime Network Services Controller 3.0.2 Quick Start Guide

Revised: April 3, 2014, OL-30215-01

Getting Started with Cisco Prime Network Services Controller

New and Changed Information

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

Date	Revision	Location
February 18, 2014	Updated information for upgrading from Prime Network Services Controller	Upgrading Overview, on page 39

Installation Requirements

Requirements Overview

The following topics identify the requirements for installing and using Cisco Prime Network Services Controller (Prime Network Services Controller) 3.0.2:

Note This release of Cisco Prime Network Services Controller contains many new features. For information on these features and additional changes in this release, see the Cisco Prime Network Services Controller 3.0.2 Release Notes.

- System Requirements, on page 3
- Hypervisor Requirements, on page 3
- Web-Based GUI Client Requirements, on page 4
- Firewall Ports Requiring Access, on page 4
- Ports to Access Amazon AWS, on page 5
- Cisco Nexus 1000V Series Switch Requirements, on page 5
- Information Required for Installation and Configuration, on page 5
- Shared Secret Password Criteria, on page 6
- Configuring Chrome for Use with Prime Network Services Controller, on page 7

System Requirements

Requirement	Description
Virtual Appliance	
Four Virtual CPUs	1.5 GHz
Memory	4 GB RAM
Disk Space	One of the following, depending on InterCloud functionality: • With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows: ◦ Disk 1—20 GB ◦ Disk 2—200 GB • Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows: ◦ Disk 1—20 GB ◦ Disk 2—20 GB
Management Interface	One management network interface.
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Hypervisor Requirements

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

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

Table 1: Hypervisor Requirements

Requirement	Description
VMware	
VMware vSphere	Release 5.0 or 5.1 with VMware ESXi (English Only)
VMware vCenter	Release 5.0 or 5.1 (English Only)
Microsoft	
Microsoft Server	Microsoft Windows Server 2012 with Hyper-V (Standard or Data Center)
Microsoft SCVMM	Microsoft SCVMM 2012 SP1 or higher

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 9.0 or higher • Mozilla Firefox 11.0 or higher • Google Chrome 18.0 or higher[1]
Flash Player	Adobe Flash Player plugin 11.2 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 7.

Firewall Ports Requiring Access

The following Prime Network Services Controller ports require access.

Port	Description
80	HTTP
443	HTTPS

Port	Description
843	Adobe Flash

Ports to Access Amazon AWS

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

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

Cisco Nexus 1000V Series Switch Requirements

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

Information Required for Installation and Configuration

Required Information	Your Information
For Deploying the Prime Network Services Controller OVA	
Name	

Required Information	**Your Information**
Location of files	
Data store location	
Storage location, if more than one location is available	
Management port profile name for virtual machine (VM) management **Note** The management port profile is the same port profile that is used for the Cisco Virtual Supervisor Module (VSM). The port profile is configured in VSM and is used for the Prime Network Services Controller management interface.	
IP Address	
Subnet mask	
Gateway IP Address	
Domain Name	
DNS Server **Note** Access to a DNS server is required for Prime Network Services Controller to communicate with the Amazon Cloud Provider.	
Admin Password	
Shared secret password for communications between Prime Network Services Controller, Cisco Virtual Security Gateway (VSG), Cisco Adaptive Security Appliance 1000V (ASA 1000V), and VSM. (See Shared Secret Password Criteria, on page 6.)	
For Configuring VMware vCenter in Prime Network Services Controller	
vCenter name	
Description	
Hostname or IP address	

Shared Secret Password Criteria

A shared secret password is a password that is known only to those using a secure communication 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

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller, you must disable the Adobe Flash Players 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**.

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

Step 4 Download and install Adobe Flash Player version 11.6.602.180.

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

Installing Prime Network Services Controller

Installing Overview

The following sections describe how to install Prime Network Services Controller:

- Deploying the Prime Network Services Controller OVA, on page 11
- Installing from an ISO Image, on page 10
- Installing on Microsoft Hyper-V Hypervisor, on page 8

Note Installation time varies (10-20 minutes) depending on the host or storage area network load.

Installing on Microsoft Hyper-V Hypervisor

For information on feature differences when Prime Network Services Controller is installed on Hyper-V Hypervisor, see the Cisco Prime Network Services Controller 3.0.2 User Guide.

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, then choose **Refresh**.

Procedure

Step 1 Launch the SCVMM.

Step 2 Choose the Hyper-V Hypervisor host on which to deploy the Prime Network Services Controller VM.

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

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

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

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

a) From **General**, do the following:

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

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

1. Choose **Hard Disk**, and enter the required size of the hard disk. You will need at least 20 GB.
2. Choose **Virtual DVD Drive**, select the **Existing ISO image file** radio button, and browse to select the ISO image file for Prime Network Services Controller.

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

d) Click **Next**.

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

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

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

c) Click **Next**.

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

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

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

Step 11 In the Summary screen, do the following:

a) Verify the settings.

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

c) Click **Create**.

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

Step 12 After the virtual machine is successfully created, right-click it and choose **Connect or View > Connect Via Console**.

Step 13 Launch the console and install Prime Network Services Controller. For more information, see Deploying the Prime Network Services Controller OVA, on page 11.

Step 14 After Prime Network Services Controller is successfully deployed, click **Close** and power on the Prime Network Services Controller VM.

Task Title

Prime Network Services Controller

Before You Begin

Procedure

Step 1 Choose **InterCloud Management** > **InterCloud Link** > **Infrastructure** >.

Step 2

Step 3

Step 4

Step 5

Installing from an ISO Image

You can perform an installation using an ISO image.

Procedure

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

Step 2 Open the VMware vSphere Client.

Step 3 Create a new virtual machine (VM) on the appropriate host as follows:

a) Enter the required information in the Configuration, Name and Location, and Storage screens.

b) In the Operating System screen, choose **Linux** and **Red Hat Enterprise Linux 5 64-bit**.

c) In the Network screen, do the following:

1. Choose a NIC. A single NIC is required for Prime Network Services Controller.
2. Confirm that E1000 is selected in the **Adapter** drop-down list. Prime Network Services Controller supports only E1000 adapters.

d) In the Create a Disk screen, provide the following information:

- Virtual Disk Size—Enter a minimum of 20 GB.
- Disk Provisioning—Choose **Thin Provision** or **Thick Provision**.

e) In the Ready to Complete screen, review the information for accuracy and check the **Edit the Virtual Machine Settings Before Completion** check box.

f) In the Virtual Machine Properties dialog box, do the following:

1. In the Memory field, select **4 GB**.
2. In the Number of Virtual Sockets field, choose **4**.
3. Click **Add** to create a new hard disk with a minimum 200 GB disk size.

4 Click **OK** to create the new disk and to return to the Virtual Machine Properties dialog box.

g) In the Options tab, in the Boot Options field, choose **Force BIOS Setup**.
h) Click **Finish**.

Step 4 When the new VM is created, power it on.

Step 5 Mount the ISO to the VM CD ROM drive as follows:

1. Right-click the VM and choose **Open the VM Console**.
2. From the VM console, click **Connect/Disconnect CD/DVD Devices**.
3. Choose **CD/DVD Drive 1**.
4. Choose **Connect to ISO Image on Local Disk**.
5. Choose the ISO image that you downloaded.

Step 6 When prompted, enter the following information, then click **Next**:

- IP address
- Subnet mask
- Hostname
- Domain name
- Gateway IP address
- DNS server IP address

Step 7 In the Set Up NSC screen, enter the following information, 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 6.

Note If you configure a weak shared secret password, no error message will be generated at this point, but the shared secret password will not be usable later.

Step 8 Confirm that the information is correct as displayed, then click **Next**.
Prime Network Services Controller is installed.

Step 9 When the installation is complete, reboot the VM.

Deploying the Prime Network Services Controller OVA

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 in the VMware vSphere Client.

- Make sure that all system requirements are met as specified in System Requirements, on page 3.
- Make sure that you have the information identified in Information Required for Installation and Configuration, on page 5.
- Configure NTP on all ESX and ESXi servers that run Prime Network Services Controller, ASA 1000V, VSG, VSM, and InterCloud images. 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/0212069.

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 into the vCenter server.

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

Step 4 From the File menu, choose **Deploy OVF Template**.

Step 5 In the Source screen, choose the Prime Network Services Controller OVA, then click **Next**.

Step 6 In the OVF Template Details screen, review the details of the Prime Network Services Controller template, then click **Next**.

Step 7 In the End User License Agreement screen, click **Accept**, then click **Next**.

Step 8 In the Name and Location screen, provide the required information, then click **Next**.

Step 9 In the Deployment Configuration screen, choose **Installer** from the Configuration drop-down list, then click **Next**.

Step 10 In the Datastore screen, select the data store for the VM, then click **Next**. The storage can be local or shared remote, such as NFS or SAN.

Step 11 In the Disk Format screen, click either **Thin provisioned format** or **Thick provisioned format** to store the VM virtual disks, then click **Next**. If you will not use the InterCloud functionality in Prime Network Services Controller, you can choose thin provisioning.

Step 12 In the Network Mapping screen, select the management network port group for the VM, then click **Next**.

Step 13 In the Properties screen, provide the required information, address any errors described in the red text messages below the selection box, and then click **Next**. If needed, you can enter placeholder information as long as your entry meets the field requirements.

Note You can safely ignore the Prime Network Services Controller Restore fields.

Step 14 In the Ready to Complete screen, review the deployment settings, then click **Finish**.

Caution Any discrepancies can cause VM booting issues. Carefully review the IP address, subnet mask, and gateway information.

A progress indicator shows the task progress until Prime Network Services Controller is deployed.

Step 15 After Prime Network Services Controller is successfully deployed, click **Close**.

Step 16 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 17 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 14	Ensures that service VMs can successfully register with Prime Network Services Controller and that communications with AWS can occur.
Task 2—Configuring Prime Network Services Controller Connectivity with vCenter, on page 16	Establishes a connection between Prime Network Services Controller and VM management software.
Task 3—Registering Service VMs, on page 18	Enables Prime Network Services Controller to recognize and communicate with service VMs.
Task 4—Verifying Service VM Registration, on page 19	Confirms that the required service VMs are registered with Prime Network Services Controller.
Task 5—Configuring a Tenant, on page 21	Establishes a tenant to which you can allocate resources, such as compute or edge firewalls.
Task 6—Configuring Access Policies, on page 21	Allows or prevents access to resources based on the criteria that you specify.
Task 7—Configuring a Service Profile, on page 27	Enables you to apply a set of security-related policies (such as access and threat mitigation policies) to one or more objects.
Task 8—Configuring a Device Profile, on page 27	Enables you to apply a set of custom security attributes and device policies to a port profile or compute or edge firewall.
Task 9—Importing Service Images, on page 28	Enables you to instantiate a service device from an image.
Task 10—Adding a Compute Firewall, on page 28	Enables you to place a compute firewall in service under a tenant or another level in the organizational hierarchy.
Task 11—Adding an Edge Firewall, on page 30	Enables you to place an edge firewall in service under a tenant or another level in the organizational hierarchy.
Task 12—Creating an Edge Security Profile, on page 32	Creates an edge profile with policies and policy sets that you can apply to edge firewalls.
Task 13—Enabling Logging, on page 37	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, ASA 1000V, VSG, and VSM. NTP must be configured with a working NTP server. If you do not configure these items with a working NTP server, the following will occur:

- You will need to manually configure the ASA 1000V, VSG, and VSM components for the date and time or they will not be able to register with Prime Network Services Controller.
- InterCloud functionality will not work because the AWS API requires the request time to be within a few seconds of the current time.

For information on configuring NTP, see the following topics:

- Configuring NTP in VMs, on page 14
- Configuring NTP in Prime Network Services Controller, on page 15

Configuring NTP in VMs

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

For this VM:	Do this:
ASA 1000V	**Hyper-V Hypervisor** If Prime Network Services Controller is installed on Hyper-V Hypervisor, ensure that all Hyper-V hosts and SCVMM are in time synch with a common NTP server. **VMware** Before you install ASA 1000V in Prime Network Services Controller, configure NTP on all ESX and ESXi servers that run ASA 1000V. For information, see "Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client" at kb.vmware.com/kb/2012069. After installation, the ASA 1000V receives the Real Time Clock (RTC) value from the VMware ESX or ESXi host.
InterCloud Extender VM	Configure the NTP server in the Prime Network Services Controller GUI by choosing **InterCloud Management > InterCloud Policies > Device Profiles**. You can add the NTP server to the existing default device profile or create a new device profile with the required NTP server.
InterCloud Switch VM	When instantiating the InterCloud extender and InterCloud switch in Prime Network Services Controller using the InterCloud Link Wizard, select the correct device profile (with an NTP server configured) in the wizard to use for that instantiation.

For this VM:	Do this:

VSG	Enter the following CLI commands from the VSG console, where *x.x.x.x* is the NTP server IP address. If you use a host name, a DNS server must be configured.
	`clock timezone zone-name offset-hours offset-minutes`
	`clock summer-time zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes`
	`ntp server x.x.x.x.`
	For example, your entries might resemble the following:
	`clock timezone EST -5.0`
	`ntp server 10.10.1.1`
	Note The NTP server command is not available in the VSG console if you have installed the Prime Network Services Controller policy agent. To configure NTP in VSG, you must uninstall the Prime Network Services Controller policy agent.

VSM	Enter the following CLI command from the VSM console, where *x.x.x.x* is the NTP server IP address.
	`clock timezone zone-name offset-hours offset-minutes`
	`clock summer-time zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes`
	`ntp server x.x.x.x`

Configuring NTP in Prime Network Services Controller

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

Procedure

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

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

Step 3 Set the time zone by doing the following:

a) Choose **Administration** > **System Profile** > **root** > **Profile** > **default**.

b) In the General tab, select the time zone in which the Prime Network Services Controller server resides.

c) Click **Save**.

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

a) Choose **Administration** > **System Profile** > **root** > **Profile** > **default**.

b) In the Policy tab, select **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 Prime Network Services Controller Connectivity with vCenter

Note This feature is not supported on Hyper-V Hypervisor.

After you deploy the Prime Network Services Controller OVA, you need to establish connectivity with VMware vCenter by:

1. Downloading the vCenter Extension File, on page 16
2. Registering the vCenter Extension Plug-in in vCenter, on page 17
3. Configuring vCenter in VM Manager, on page 17

Note You must reestablish connectivity with VMware vCenter by repeating these steps if you change the Prime Network Services Controller server hostname or fully qualified domain name (FQDN).

Downloading the vCenter Extension File

The first step in setting up vCenter connectivity is to download the vCenter extension file.

Before You Begin

- Make sure you have the information identified in Information Required for Installation and Configuration, on page 5.
- 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 17).

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

Registering the vCenter Extension Plug-in in vCenter

Registering the vCenter Extension plug-in enables you to create a VM Manager in Prime Network Services Controller and connect to VMs.

Before You Begin

Make sure you have the information identified in Information Required for Installation and Configuration, on page 5.

Procedure

Step 1 From the VMware vSphere Client, log into 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 You might need to 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 downloaded 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**, then click **Close**.

Configuring vCenter in VM Manager

Configuring a VM Manager in Prime Network Services Controller enables you to connect directly to VMs.

Procedure

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

Step 2 In the VM Managers pane, click **Add VM Manager**.

Step 3 In the Add VM Manager dialog box, enter the required information for vCenter, then click **OK**.
A successfully added VM Manager is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- VMware vCenter 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 service VMs that must be registered are:

- ASA 1000V
- VSG
- VSM

Before You Begin

- Configure NTP on all ESXi servers that run VMs. For more information, see "Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client" at http://kb.vmware.com/kb/2012069.
- Deploy the VMs using the VMware vSphere Client.
- Make sure that a network path exists between each VM management IP address and the Prime Network Services Controller management IP address.
- Make sure that each VM has access to or has installed the Prime Network Services Controller policy agent image.

Procedure

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

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

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

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

- For ASA 1000V VMs, configure the Prime Network Services Controller IP address and the shared secret by entering the following commands:

```
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
```

- For VSG VMs, configure the Prime Network Services Controller IP address and the shared secret by entering the following commands:

```
vm-name# configure terminal
vm-name(config)# vnm-policy-agent
vm-name(config-vnmc-policy-agent)# registration-ip n.n.n.n
vm-name(config-vnmc-policy-agent)# shared-secret MySharedSecret
```

- For enterprise VSM VMs:

1. Configure the Prime Network Services Controller IP address and the shared secret by entering the following commands:

```
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:nsc-vsmpa.n.n.n.bin
```

2. Before reloading, save the configuration by entering the **copy r s** command.

Task 4—Verifying Service VM Registration

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

Before You Begin

- Make sure you have the information identified in Information Required for Installation and Configuration, on page 5.
- Confirm the following:

For this device:	Confirm that:
ASA 1000V	• The ASA 1000V is installed. • NTP is set up on the ASA 1000V. • The Prime Network Services Controller policy agent status is correct on the ASA 1000V. For more information, see http://www.cisco.com/en/US/products/ps12233/prod_installation_guides_list.html. • The ASA 1000V is registered to Prime Network Services Controller. For more information, see Task 3—Registering Service VMs, on page 18.
VSG	• The VSG is installed. • NTP is set up on the VSG. • The Prime Network Services Controller policy agent status is correct on the VSG. For more information, see http://www.cisco.com/en/US/products/ps13095/prod_installation_guides_list.html. • The VSG is registered to Prime Network Services Controller. For more information, see Task 3—Registering Service VMs, on page 18.
VSM	• The VSM is registered to Prime Network Services Controller. • NTP is set up on the VSM. • The VSG and ASA 1000V port profiles are configured on the VSM. For more information, see http://www.cisco.com/en/US/products/ps13095/prod_installation_guides_list.html. • The Prime Network Services Controller policy agent status is correct on the VSM.

For more information about configuring NTP, see Task 1—Configuring NTP, on page 14.

Procedure

Step 1 In Prime Network Services Controller, choose **Administration** > **Service Registry** > **Clients**.

Step 2 Confirm that the table in the Clients window contains *registered* in the Oper State column for the ASA 1000V, VSG, and VSM entries.

Task 5—Configuring a Tenant

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

Note For the purposes of this guide, a tenant is the lowest level of configuration required. You can configure subordinate levels as appropriate for your environment.

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, then click **OK**.
The tenant name can contain 1 to 32 alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.

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

Task 6—Configuring Access Policies

The following access policies prevent unauthorized access to resources:

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

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

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

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

- Configuring an IP Group, on page 22
- Configuring an ACL Policy, on page 22

Configuring an IP Group

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

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

⚠

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

Procedure

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

Step 2 Click **Add IP Group**.

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

a) Enter a name for the IP group.

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

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

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

Configuring an ACL Policy

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

- Source conditions
- Destination conditions
- Service
- Protocol
- EtherType
- Time ranges or frequency

Procedure

Step 1 Choose **Policy Management** > **Service Policies** > **root** > *tenant* > **Policies** > **ACL> ACL Policies** where *tenant* is the tenant that you created in Task 5—Configuring a Tenant, on page 21.

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, then click **Add Rule**.

Step 4 In the Add Rule Policy dialog box, define a rule using the information described in Add ACL Policy Rule Dialog Box, on page 23, 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 Select 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	Condition Match Options. • Choose match-all for the ACL Policy Rule to match all the conditions (AND). • Choose 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	Source Rule Condition 1 Click **Add**. 2 Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value 3 Click **OK**.
Destination Conditions	Destination Rule Condition 1 Click **Add**. 2 Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value 3 Click **OK**.
Service	Service Expression 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. To examine specific encapsulated protocols: **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 in the Begin drop-down list, choose the same frequency in the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.

Field	Description
Advanced Tab	Source port attributes that must be matched for the current policy to apply. To add a new source port: **1** Click **Add**. **2** Provide the required information in the following fields, 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, then click **OK**.

Note The Attributes tab in the Add Compute Security Profile is not available if Prime Network Services Controller is installed on Hyper-V Hypervisor.

Task 8—Configuring a Device Profile

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

Procedure

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

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

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

Task 9—Importing Service Images

To instantiate a service device from an image, you must first import the service image.

After the image is imported, Prime Network Services Controller automatically places the zipped files in the correct locations and populates the Service Images table.

Procedure

Step 1 Choose **Resource Management** > **Resources** > **Service Devices** > **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) Select the service image type: ASA 1000V or VSG.
c) Enter a version to assign to the image.
d) In the Import area, provide the following information, then click **OK**:

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

Task 10—Adding a Compute Firewall

You can add a compute firewall and assign it to a VSG, thereby placing the VSG in service. A wizard walks you through the configuration process, which includes assigning a VSG, assigning profiles, and configuring interfaces.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in Prime Network Services Controller as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

Users with infrastructure-admin and tenant-admin roles can work with service VMs as follows:

- Users with the infrastructure-admin role can instantiate and delete service VMs.
- Users with the tenant-admin role can view service VM details, but cannot instantiate or delete service VMs.

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

Before You Begin

To place a VSG in service, at least one of the following must exist:

- To assign a VSG, an available VSG must be registered in Prime Network Services Controller. For more information, see Task 4—Verifying Service VM Registration, on page 19.
- To assign a VSG pool, a VSG pool must have at least one available VSG.
- To instantiate a VSG service device, a VM service image must be imported and VM Manager must be configured in Prime Network Services Controller. For more information on importing service images, see Task 9—Importing Service Images, on page 28.

Procedure

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

Step 2 In the General tab, click **Add Compute Firewall**.
The Add Compute Firewall Wizard opens.

Step 3 In the Properties screen, supply the information as described in Properties Screen, on page 29, then click **Next**.

Step 4 In the Service Device screen, select the required VSG service device as described in Service Device Screen, on page 30, then click **Next**.

Step 5 (Instantiate option only) If you instantiate a VSG service device from an image, do one or both of the following in the Placement screen, then click **Next**:

- Navigate to and choose the host or resource pool to use for the VSG instance.
- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary VSG instance.

Step 6 In the Interfaces screen, configure interfaces as follows, then click **Next**:

- If you assigned a VSG, enter the data IP address and subnet mask.
- If you assigned a VSG pool, enter the data IP address and subnet mask.
- If you instantiated a VSG service device without high availability, add management and data interfaces.
- If you instantiated a VSG service device with high availability, add management, data, and HA interfaces.

For field-level help when configuring the interfaces, see the online help.

Step 7 In the Summary screen, confirm that the information is correct, then click **Finish**.

Properties Screen

Field	Description
Name	Compute firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Compute firewall description.

Field	Description
Host Name	Management hostname of the firewall.
Device Configuration Profile	Do either of the following: • Click the profile name to view or optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.

Service Device Screen

Field	Description
Assign VSG	Assign a VSG to the compute firewall. In the **VSG Device** drop-down list, choose the required service device.
Assign VSG Pool	Assign a VSG pool to the compute firewall. In the **VSG Pool** field, either choose the required pool from the drop-down list or click **Add Pool** to add a new pool.
Instantiate	Instantiate a VSG service device from an available image. **1** In the list of available images, select the image to use to instantiate a new VSG service device. **2** In the High Availability field, check the **Enable HA** check box to enable high availability. **3** In the VM Access password fields, enter the password for the admin user account.

Task 11—Adding an Edge Firewall

You can add an edge firewall and assign it to an ASA 1000V, thereby placing the ASA 1000V in service. A wizard walks you through the configuration process, which includes assigning configuration and service profiles, assigning an ASA 1000V, and configuring interfaces.

Users with infrastructure-admin and tenant-admin roles can work with service VMs as follows:

- Users with the infrastructure-admin role can instantiate and delete service VMs.
- Users with the tenant-admin role can view service VM details, but cannot instantiate or delete service VMs.

Before You Begin

At least one of the following must exist:

- To assign an ASA 1000V to the edge firewall, an ASA 1000V must be registered in Prime Network Services Controller and must be available for assignment. For more information about VM registration, see Task 4—Verifying Service VM Registration, on page 19.
- To instantiate an ASA 1000V service device from an image, an ASA 1000V service must be imported and VM Manager must be configured in Prime Network Services Controller. For more information on importing service images, seeTask 9—Importing Service Images, on page 28.

Procedure

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

Step 2 In the General tab, click **Add Edge Firewall**.
The Add Edge Firewall Wizard opens.

Step 3 In the Properties screen, provide the information described in Properties Screen, on page 32, then click **Next**.

Step 4 In the Service Device screen, do one of the following, then click **Next**:

- To assign an existing ASA 1000V service device:
  1. Click **Assign ASA 1000V**.
  2. In the **ASA 1000V Device** drop-down list, choose the required ASA 1000V.
- To instantiate a new ASA 1000V:
  1. Click **Instantiate**.
  2. In the list of available VMs, select the VM to use to instantiate a new ASA 1000V service device.
  3. In the VM Access password fields, enter the password for the admin user account.

Step 5 (Instantiate option only) If you instantiate anASA 1000V service device from an image, do one or both of the following in the Placement screen, then click **Next**:

- Navigate to and choose the host or resource pool to use for the ASA 1000V instance.
- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary ASA 1000V instance

Step 6 In the Interfaces screen, add the required interfaces as follows, then click **Next**:

- If you assigned an ASA 1000V without high availability, configure one inside and one outside interface.
- If you assigned an ASA 1000V with high availability, configure one inside and one outside interface, each with a secondary IP address.
- If you instantiated an ASA 1000V without high availability, configure management, inside, and outside interfaces.

- If you instantiated an ASA 1000V with high availability, configure management, inside, outside, and HA interfaces.

Step 7 In the Summary screen, confirm that the information is accurate, then click **Finish**.

Step 8 If you instantiated the ASA 1000V from a service image, you must do the following to ensure registration with Prime Network Services Controller:

a) **Within 15 minutes of instantiation**, manually register the ASA 1000V to Prime Network Services Controller by using the ASA 1000V vCenter console.

b) If you do not register the ASA 1000V within 15 minutes of instantiation, the instantiated ASA 1000V will enter a failed state, and you must delete it manually from Prime Network Services Controller and vCenter.

Properties Screen

Field	Description
Name	Edge firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Edge firewall description.
Host Name	Management hostname of the firewall.
High Availability	Check the **Enable HA** check box to enable high availability.
Device Configuration Profile	Do either of the following: • Click the profile name to view and optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.
Device Service Profile	Do either of the following: • Click the profile name to view and optionally modify the currently assigned device service profile. • Click **Select** to choose a different device service profile.

Task 12—Creating an Edge Security Profile

Edge security profiles include the policies and policy sets that you choose to ensure security for your edge firewalls.

Procedure

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

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

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

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

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

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

Note To add an ACL Policy set, click **Add ACL Policy Set** and follow the instructions in Task 13—Configuring Access Rules.

Step 4 In the NAT tab, either select 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 33.

c) To add a NAT policy, click **Add NAT Policy** and enter the information as described in Add NAT Policy Dialog Box, on page 34.

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 35.

e) To add a rule condition, click Add Rule Condition and enter the information as described in Add Condition Dialog Box, on page 37.

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

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

Add NAT Policy Set Dialog Box

Field	Description
Name	Policy set name.
Description	Brief description of the policy set.
Admin State	Whether the administrative state of the policy set is enabled or disabled.
Policies Area	
Add NAT Policy	Adds a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.

Field	Description
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Add NAT Policy Dialog Box

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

Add NAT Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Original Packet Match Conditions	
Source Match Conditions	Source attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.
Destination Match Conditions	Destination attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.
Protocol	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
NAT Action Table	
NAT Action	From the drop-down list, choose the required translation option: Static or Dynamic.

Field	Description
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	One of the following attribute types: • Network—Network attributes. **Note** Network attributes can be source and destination IP addresses, port and protocol, Ether Type and application. • VM—Virtual machine attributes. • User-Defined—User-defined attributes defined in an attribute dictionary. **Note** User-defined attribute are specified in security profiles. • vZone—Virtual zone attributes.
Expression	
Attribute Name	Drop-down list that allows you to select an attribute name.
Operator	Drop-down list that allows you to select an operator. Depending upon the value you select from this drop-down list, different values are available in the **Attribute Value** field.
Attribute Value	Attribute value. The attribute value that you enter depends upon the attribute name selected.

Task 13—Enabling Logging

Configuring and enabling a syslog policy for a VSG or ASA 1000V element 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 VSG or ASA 1000V elements by doing either or both of the following:

- Enabling Policy-Engine Logging in a Monitor Session, on page 37
- Enabling Global Policy-Engine Logging, on page 38

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, select **default**, then click **Edit**.

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

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

Step 5 In the Edit Syslog Client dialog box, provide the following information, 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 Installation and Configuration

Troubleshooting Overview

Prime Network Services Controller enables you to review the faults associated with compute and edge firewalls.

To examine faults for firewalls:

- Examining Faults and Errors for Edge Firewalls
- Examining Faults for Compute Firewalls, on page 38

Examining Faults for Compute Firewalls

Prime Network Services Controller enables you to examine faults and configuration errors for compute firewalls.

Before You Begin

Assign the compute firewall to a VSG instance.

Procedure

Step 1 Choose **Resource Management** > **Managed Resources** > **root** > *tenant* > **Compute Firewalls**.
The Edit Compute Firewall dialog box is displayed.

Step 2 In the Compute Firewalls table, select the required firewall, then click **Edit**.

Step 3 In the General tab, in the Status area, check the configuration, association, and reachability status.

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

Examining Faults for Edge Firewalls

Prime Network Services Controller enables you to view faults for edge firewalls.

Before You Begin

Assign the edge firewall to an ASA 1000V instance or instantiate an ASA 1000V service VM.

Procedure

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

Step 2 In the Edge Firewalls table, choose the required edge firewall, then click **Edit**.

Step 3 In the General tab, in the Status area, check the configuration, association, and reachability status.

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

Upgrading and Patching Prime Network Services Controller

Upgrading Overview

Use the following procedure when you upgrade to a newer Prime Network Services Controller version. For Prime Network Services Controller 3.0.2, the supported upgrade paths are from Cisco Virtual Network Management Center (VNMC) 2.1 or Prime Network Services Controller 3.0. If you want to upgrade from VNMC 1.3 or 2.0 to Prime Network Services Controller 3.0.2, you must first upgrade to VNMC 2.1 or Prime Network Services Controller 3.0.

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

The following scenarios are not supported:

- Backing up from VNMC 2.1 and restoring to Cisco Virtual Network Management Center 3.0.2.

- Exporting from VNMC 2.1 and importing to Cisco Virtual Network Management Center 3.0.2.

To upgrade from VNMC 2.1 or Prime Network Services Controller 3.0 to Prime Network Services Controller 3.0.2, complete the following tasks:

1. If you are upgrading from VNMC 1.3 or 2.0, first upgrade to VNMC 2.1 or Cisco Virtual Network Management Center 3.0—See the *Cisco Virtual Network Management Center 2.1 Quick Start Guide* at http://www.cisco.com/en/US/products/ps11213/prod_installation_guides_list.html or the *Cisco Prime Network Services Controller 3.0 Quick Start Guide* at http://www.cisco.com/en/US/products/ps13213/prod_installation_guides_list.html.
2. Perform a full-state backup of VNMC 2.1 or Cisco Virtual Network Management Center 3.0 by using Secure Copy (SCP) protocol—See the section on backing up and restoring Prime Network Services Controller.
3. Upgrade to Cisco Virtual Network Management Center 3.0.2 by using the CLI **update bootflash** command—See Upgrading to Prime Network Services Controller 3.0.2, on page 41.

Note

- After you upgrade to Cisco Virtual Network Management Center 3.0.2, you might see the previous version in your browser. To view the upgraded version, clear the browser cache and browsing history in the browser, and restart the browser. This note applies to all supported browsers: Internet Explorer, Mozilla Firefox, and Google 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 Backing Up Prime Network Services Controller, on page 44 .

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

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

Note

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

Procedure

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

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

Step 2 Enter system mode:

```
scope system
```

Step 3 Create a full-state backup file:

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

where:

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

Step 4 When prompted, enter the required password.

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

```
commit-buffer
```

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

Upgrading to Prime Network Services Controller 3.0.2

After you back up the date for your existing VNMC 2.1 or Prime Network Services Controller 3.0 installation, you can upgrade to Prime Network Services Controller 3.0.2.

Caution To save a state for recovery purposes, perform a backup before beginning the upgrade. For more information, see Backing Up Data, on page 40.

Note

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

Before You Begin

- Ensure that Prime Network Services Controller can access a DNS server and an NTP server. If a DNS server and an NTP server are not accessible, Prime Network Services Controller will not be able to access the Amazon Cloud Provider.
- Prime Network Services Controller 3.0.2 requires two virtual disks with the following configuration:
    - Disk 1—20 GB
    - Disk 2—200 GB

If you do not have two disks configured, you will not be able to upgrade to 3.0.2.

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 3.0.2 image from a remote file server:

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

Step 5 Upgrade to Prime Network Services Controller 3.0.2:

```
update bootflash:/nsc.3.0.2.XXXX.bin
```

where *nsc.3.0.2.XXXX.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 vCenter. For more information, see Task 2—Configuring Prime Network Services Controller Connectivity with vCenter, on page 16.

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

Patching Prime Network Services Controller

Use the CLI to apply the patch.

Procedure

Step 1 As user admin, log into the Prime Network Services Controller system to be patched:

```
ssh admin@server-ip-address
```

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

Step 3 Update the bootflash:

```
update bootflash:/nsc.3.0.2.XXXX.bin
```

where *nsc.3.0.2.XXXX.bin* is the name of the patch file.

Step 4 Restart the Prime Network Services Controller services:

```
service restart
```

Step 5 Verify that all services are running:

```
service status
```

Step 6 To verify that the patch was applied, check the update history:

```
show update-history
```

Backing Up and Restoring Prime Network Services Controller

Backing Up and Restoring Overview

Note We recommend that you use backup and restore as a disaster recovery mechanism. To migrate configuration data from one Prime Network Services Controller server to another, see the Cisco Prime Network Services Controller 3.0.2 User Guide.

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

- Backing up VNMC 2.1 and restoring to VNMC 2.1.

- Backing up Prime Network Services Controller 3.0.2 and restoring to Prime Network Services Controller 3.0.2.

Backing up one version and restoring to another version (such as backing up VNMC 2.1 and restoring to Prime Network Services Controller 3.0.2) is not supported.

Note Do not use TFTP for backup and restore operations.

The following topics describe how to back up data and restore data for Prime Network Services Controller 3.0.2:

- Backing Up Prime Network Services Controller, on page 44
- Restoring the Previous Version, on page 44

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 3.0.2) is not supported.

We recommend the following:

- Do not perform a backup when any of the following tasks are running on the system:
    - Image import
    - Migration of a VM to the cloud
    - Deployment of an InterCloud Switch
    - Creation of an InterCloud link
- Use backup and restore as a disaster recovery mechanism. To save a state for recovery purposes, perform a backup via the GUI or CLI, using one of the following methods:
    - CLI—See Backing Up Data, on page 40.
    - GUI—See the Cisco Prime Network Services Controller 3.0.2 User Guide.

Restoring the Previous Version

Note Do not use TFTP to update data.

Before You Begin

Temporarily disable the CSA on the remote file server.

Procedure

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

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

Step 2 Connect to local-mgmt:

```
connect local-mgmt
```

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

```
show version
```

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

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

Step 5 Enter the **update** command:

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

Step 6 Restore the previous version:

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

where:

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

Step 7 Restart the server:

```
service restart
```

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

```
service status
```

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

```
show version
```

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

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

What to Do Next

Perform the post-restoration tasks described in Post-Restoration Tasks, on page 46.

Post-Restoration Tasks

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

- Update VM Managers—See Updating VM Managers, on page 46.
- Reimport InterCloud and VM images—See Reimporting InterCloud and VM Images, on page 46.
- Verify InterCloud status—See Verifying InterCloud Status, on page 47.

Updating VM Managers

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

Procedure

Step 1 Choose **InterCloud Management** > **Enterprise** > **VM Managers**.

Step 2 For existing vCenters that you wish to retain, reimport the vCenter Extension plugin. For more information, see the Cisco Prime Network Services Controller 3.0.2 User Guide.

Step 3 Check and delete any stale VM Manager entries.

Reimporting InterCloud and VM Images

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

Before You Begin

Successfully restore Prime Network Services Controller as described in Restoring the Previous Version, on page 44.

Procedure

Step 1 Log into the Prime Network Services Controller GUI.

Step 2 Review the imported images in the following screens:

- VM Images—Choose **InterCloud Management** > **Enterprise** > **VM Images**.
- Bundled Images—Choose **InterCloud Management** > **InterCloud Link** > **Images**.

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

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

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

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

Verifying InterCloud Status

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

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

Before You Begin

Successfully restore Prime Network Services Controller as described in Restoring the Previous Version, on page 44.

Procedure

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

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

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

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

- If an InterCloud link was being deployed when the system was backed up and completed deployment after the backup, Prime Network Services Controller will attempt to deploy the link from the point at which the system was backed up. In this situation, do either of the following, as appropriate:

  - Because the InterCloud Extender and InterCloud Switch exist in the network, you can wait to see if the link will be deployed within a few minutes.
  - If the InterCloud link deployment task displays an error, undeploy the link and redeploy it.

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

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

  1. In the list of cloud VMs, obtain the cloud instance ID.

2. Check the public cloud for the selected cloud instance.
3. If the VM instance does not exist on the cloud, you can delete the VM.

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

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

1. If the InterCloud Switch is in lost-visibility state (**Administration > Service Registry > Clients**), reboot the InterCloud Switch by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* **> InterCloud Switch Tab >** *intercloud-switch* **> Reboot**.
2. If the cloud VM tunnel is not *up* (**InterCloud Management > Public Cloud > VPCs >** *vpc* **> VMs**), reboot the cloud VM.

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

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

   1. Remove the InterCloud Extender in vCenter.
   2. Remove the InterCloud Switch in Amazon Web Services (AWS).
   3. Remove the cloud VMs from AWS.

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

   1. Terminate the cloud VMs by choosing **InterCloud Management > InterCloud Link > VPCs > VMs tab >** *cloud-vm* **> Terminate**.
   2. Undeploy the InterCloud link by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* **> Undelploy**.
   3. Delete the InterCloud link by choosing **InterCloud Management > InterCloud Link > VPCs >** *vpc* **>** *intercloud-link* **> Delete**.

Additional Information

Related Documentation

Cisco Prime Network Services Controller

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

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

- *Cisco Prime Network Services Controller 3.0.2 Documentation Overview*
- *Cisco Prime Network Services Controller 3.0.2 Release Notes*
- *Cisco Prime Network Services Controller 3.0.2 Quick Start Guide*
- *Cisco Prime Network Services Controller 3.0.2 User Guide*
- *Cisco Prime Network Services Controller 3.0 CLI Configuration Guide*
- *Cisco Prime Network Services Controller 3.0 XML API Reference Guide*
- *Open Source Used in Cisco Prime Network Services Controller 3.0.2*

Cisco ASA 1000V Documentation

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

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

Cisco Nexus 1000V InterCloud Documentation

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

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

Cisco Nexus 1000V Series Switch Documentation

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

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

Cisco Virtual Security Gateway Documentation

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

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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