Installing the Cisco Prime Network Services Controller

This chapter contains the following sections:

- Information About the Cisco PNSC , page 1
- Installation Requirements, page 2
- OpenStack Installation Overview, page 7

Information About the Cisco PNSC

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

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. Cisco PNSC simplifies operations with centralized, automated multi-device and policy management for Cisco network virtual services.

Cisco PNSC is the primary management element for Cisco Nexus 1000V (Nexus 1000V) switches and services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000V switches and services deliver a highly secure multi-tenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Cisco PNSC enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. Cisco PNSC is built on an information-model architecture in which each managed device is represented by its sub-components (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall virtual security services.

In addition, Prime Network Services Controller supports Cisco Cloud Services Router 1000V (CSR 1000V) edge routers, and Citrix NetScaler 1000V and Citrix NetScaler VPX load balancers. This combination of

virtual services brings numerous possibilities to customers, enabling them to build virtual data centers with all of the required components to provide best-in-class cloud services.

For detailed information on how to install Cisco Prime Network Services Controller, see Cisco Prime Network Services Controller 3.4 Installation Guide.

Installation Requirements

Cisco PNSC System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four Virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk Space	220 GB on shared NFS or SAN, configured on two disks as follows: • Disk 1—20 GB • Disk 2—200 GB
Management Interface	One management network interface
Processor	x86 Intel or AMD server with 64-bit processor
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

Cisco PNSC is a multi-hypervisor virtual appliance that can be deployed on OpenStack KVM Hypervisor. See the following links to confirm that OpenStack KVM supports your hardware platform:

- OpenStack Compute and Image System Requirements
- OpenStack for Cisco DFA Install Guide for Using the Cisco OpenStack Installer

Requirement	Description
OpenStack KVM	
KVM Hypervisor	Ubuntu 12.04 LTS server, 64-bit
KVM Kernel	Version 3.2.0-52-generic
Cisco OpenStack Installer	Havana (Standalone mode only) Cisco PNSC Release 3.4 does not support Orchestrator mode. The version depends on the installation mode: • Standalone Mode—Grizzly • Orchestrator Mode—Dynamic Fabric Automation (DFA) OpenStack

Web-Based GUI Client Requirements

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

Firewall Ports Requiring Access

If Cisco PNSC is protected by a firewall, the following ports on the firewall must be open so that clients can contact Cisco PNSC.

Requirement	Description
22	TCP
80	HTTP
443	HTTPS
843	Adobe Flash
6644, 6646	TCP, UDP

Cisco Nexus 1000V Series Switch Requirements

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

Information Required for Installation and Configuration

Required Information	Your Information/Notes
For Preinstallation Configuration	
ISO or OVA image location	
ISO or OVA image name	
Network / Port Profile for VM management [1]	
VM instance name	
KVM flavor name	
KVM Instance Security Group	
VMware datastore location	
For Prime Network Services Controller Installation	
IP address For OpenStack environments, use the IP address that is assigned to the Prime Network Services Controller instance in OpenStack.	
Subnet mask	
Hostname	
Domain name	
Gateway IP address	
DNS server IP address	
NTP server IP address	
Admin password	
Shared secret password for communication between Prime Network Services Controller and managed VMs. (See Shared Secret Password Criteria.)	

1 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 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. Passwords are designated strong if they cannot be easily guessed for unauthorized access. When you set a shared secret password for communications between the Cisco PNSC, Cisco VSG, and VSM, adhere to the following criteria for setting valid, strong passwords:

Do not include the following items in passwords:

- Characters: & ' " ` ( ) < > | \ ; $
- Spaces

Create strong passwords based on the following characteristics:

Table 1: Characteristics of Strong Passwords

Strong passwords have...	Strong passwords do not have...
• At least eight characters. • Lowercase letters, uppercase letters, digits, and special characters.	• Consecutive characters, such as *abcd*. • Characters repeated three or more times, such as *aaabbb*. • A variation of the word Cisco, such as *cisco*, *ocsic*, or one that changes the capitalization of letters in the word *Cisco.* • The username or the username in reverse. • A permutation of characters present in the username or *Cisco.*

Examples of strong passwords are:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Configuring Chrome for Use with Cisco PNSC

To use Chrome with Cisco PNSC, you must disable the Adobe Flash Player plugins that are installed by default with Chrome.

Note Because Chrome automatically enables Adobe Flash Player plugins each time the system reboots, you must perform this procedure each time your client machine 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 plugin version 11.9 or higher.
Step 5 Close and reopen Chrome before logging in to Cisco PNSC.

OpenStack Installation Overview

You install Cisco PNSC on OpenStack by using the ISO image. The installation time varies from 10 to 20 minutes depending on the host and the storage area network load.

To install Cisco PNSC on OpenStack, complete the tasks described in the following topics:

1 Configuring OpenStack for Prime Network Services Controller
2 Installing Prime Network Services Controller on OpenStack KVM
3 Rebooting Cisco PNSC from OpenStack, on page 10

Configuring OpenStack for Cisco PNSC

To prepare OpenStack for installing Cisco PNSC using the Cisco OpenStack Installer (COI), you must create a flavor, import an image, and launch an instance. This procedure describes how to complete these tasks.

Before You Begin

In OpenStack:

- Confirm that you have met the requirements in Requirements Overview. OpenStack Havana is required for Cisco PNSC, Release 3.4 functionality.

Note Although you can install Cisco PNSC, Release 3.4 on OpenStack Grizzly, you will not have access to release 3.4 functionality unless you use OpenStack Havana.

- Gather the information required for configuration as identified in Information Required for Configuration and Installation.
- Confirm that you have admin privileges.
- Confirm that the Cinder service is up and running.
- Create a project on which to install Cisco PNSC.
- Create a Cinder volume with the size of 20 GB.
- Configure a security group that allows TCP, UDP, and ICMP traffic with Cisco PNSC.

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**, and then click **Create Flavor**.

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

- Name—Flavor name.
- vCPUs—Enter **4**.
- RAM MB—Enter **4096**.
- Root Disk—Enter **20 GB**.
- Ephemeral Disk—Enter **20 GB**.
- Swap Disk—Enter **400 MB**.

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

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

- Name—Enter an image name.
- Image Source—Specify the image source.
- 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 users with access to the current project.
- Protected—Check the check box to ensure that only users with permission can delete the image.

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* **> Manage Compute > Volumes**, and click **Create Volume**.

Step 6 In the Create Volume dialog box, add a volume with the size of 20 GB, and click **Create Volume**.

Step 7 At the command line, enter the following command to launch the Cisco PNSC instance:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=volume-id:::0 pnsc-image-name
```

Step 8 In the OpenStack GUI, choose **Project >** *project* **> Manage Compute > Instances**.

Step 9 In the Instances pane, note the IP address of the launched instance.

Step 10 Click the instance and choose **More > Console** to start the Cisco PNSC installation procedure.

What to Do Next

Install Cisco PNSC as described in Installing Prime Network Services Controller on OpenStack KVM.

Installing Cisco PNSC on OpenStack KVM

Before You Begin

- All system requirements are met as specified in System Requirements.
- Confirm that you have admin privileges.
- You have configured the hypervisor for the Cisco PNSC installation procedure.
- A VM has been created for Cisco PNSC and has network access.
- You can access the VM console.
- You have the IP address for the instance launched in OpenStack.

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

Note For more information on how to install Cisco PNSC, see Cisco Prime Network Services Controller 3.4 Installation Guide.

Procedure

Step 1 Open the VM console if it is not already open. If you have just finished configuring the hypervisor, the Cisco PNSC installer displays within a few minutes.

Step 2 In the Network Configuration screen, click **Edit** in the Network Devices area, enter the IP address and netmask for the Cisco PNSC VM, and click **OK**.

Step 3 In the Network Configuration area, enter the hostname, domain name, and IP addresses for the gateway, DNS server, and NTP server.

Step 4 In the Modes screen, choose the required modes, and click **Next**:

- Prime Network Services Controller Operation Mode: Choose **Standalone**. This release of Cisco PNSC is available in Standalone mode only.
- 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 5 In the Administrative Access screen, enter the administrator and shared secret passwords with confirming entries.
For information on creating a strong password, see Shared Secret Password Criteria.

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

Step 6 In the Summary screen, confirm that the information is accurate, and then click **Finish**. Prime Network Services Controller installs on the VM. This takes a few minutes.

Step 7 When prompted, disconnect from the media source and then click **Reboot**. Prime Network Services Controller is then installed on the VM.

Step 8 To confirm that Cisco PNSC is accessible, connect to Cisco PNSC through the console for the CLI or a browser for the GUI.

What to Do Next

Reboot the Cisco PNSC from OpenStack, see *Cisco Prime Network Services Controller 3.4 Installation Guide*.

Rebooting Cisco PNSC from OpenStack

If you reboot a Cisco PNSC instance from the OpenStack Horizon UI, the reboot operation fails and the console contains a message stating that no bootable image can be found. This situation occurs for instances that were created using an ISO image, such as Cisco PNSC.

In OpenStack, the first time an instance is created by using an ISO image and rebooted, the root device name is set to /dev/hda. After the instance is created, the bootable image is located on hda. However, with the implementation of hard and soft reboot options in OpenStack, the disk definitions change. As a result, a bootable image cannot be found for the Cisco PNSC instance.

To reboot Cisco PNSC in OpenStack, use either of the following procedures:

- Rebooting Cisco PNSC Without an Image, on page 10
- Rebooting Cisco PNSC by Changing the Disk Files, on page 11

Rebooting Cisco PNSC Without an Image

Use this procedure to reboot a Cisco PNSC instance in OpenStack. For more information about OpenStack, see http://docs.openstack.org/.

Procedure

Step 1 Create a flavor with the following attributes:

- Root Disk GB—20 GB
- Ephemeral Disk GB—0 GB (no ephemeral disk)

Step 2 Using either the Horizon GUI or the CLI, create one volume (vda) for Cisco PNSC and one volume (vdb) for storing imported images.
To use the CLI, enter the following commands:

```
cinder create --display-name vda-name 20
cinder create --display-name vdb-name 200
```

Step 3 Using the CLI, boot the instance and install Cisco PNSC as follows:

a) Enter the following command:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=vda-id:::0 --block-device-mapping
vdc=vdb-id:::0 pnsc-image-name
```

b) When prompted to reboot after the installation, click **Stop**.

Step 4 Terminate the instance created in Step 3 to remove the instance while retaining the required two volumes.

Step 5 To boot the Cisco PNSC instance, enter the **boot** command without the `--image` parameter and using the correct volume IDs:

```
nova boot --flavor=flavor-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vda=vda-id:::0 --block-device-mapping
vdb=vdb-id:::0 pnsc-image-name
```

Rebooting Cisco PNSC by Changing the Disk Files

Use this procedure to reboot a Cisco PNSC instance in OpenStack. For more information about OpenStack, see http://docs.openstack.org.

Procedure

Step 1 Create a flavor with the following attributes:

- Root Disk GB—20 GB
- Ephemeral Disk GB—20 GB

The ephemeral disk will act as the Cisco PNSC system disk.

Step 2 Using either the Horizon UI or the CLI, create one volume (vdb) for storing imported images.
To use the CLI, enter the following command:

```
cinder create --display-name vdb-name 200
```

Step 3 Using the CLI, boot the instance and install Cisco PNSC by entering the following command:

```
nova boot --flavor=flavor-id --image=image-id
--nic net-id=network-id,v4-fixed-ip=pnsc-ip
--block-device-mapping vdb=volume-id:::0 pnsc-image-name
```

Step 4 When prompted, disconnect from the media source and click **Reboot**.
Cisco PNSC is then installed on the VM.

Step 5 Change the disk files by entering the following commands:

```
mv /var/lib/nova/instance-uuid/disk /var/lib/nova/instance-uuid/disk.tmp
ln -s /var/lib/nova/instance-uuid/disk.local
/var/lib/nova/instance-uuid/disk
```