Cisco Prime Network Services Controller 3.2.2 Release Notes

December 17, 2014

These release notes contain the following sections for the Cisco Prime Network Services Controller 3.2.2 (Prime Network Services Controller 3.2.2) release:

Introduction

The dynamic nature of virtualized 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 Prime Network Services Controller simplifies operations with centralized, automated multi-device and policy management for Cisco and third-party network virtual services.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prime Network Services Controller is the primary management element for Cisco Nexus 1000V (Nexus 1000V) Series Virtual Switches and Services. Working together, they enable a transparent, scalable, and automation-centric network management solution for virtualized data center environments. Nexus 1000V switches and services deliver a highly secure multi-tenant environment by adding virtualization intelligence to the data center network. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Prime Network Services Controller enables the centralized management of Cisco virtual services to be performed by an administrator through its GUI or programmatically through its XML API. Prime Network Services Controller is built on an information-model architecture in which each managed device is represented by its subcomponents (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 (VSG) and Cisco ASA 1000V (ASA 1000V) firewall virtual security services.

In addition, Prime Network Services Controller supports Cisco Cloud Service Router 1000V (CSR 1000V) edge routers, and Citrix NetScaler VPX and Citrix NetScaler 1000V 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.

New Features and Enhancements

Note Prime Network Services Controller 3.2.2 does not support InterCloud functionality. If you are using a version of Prime Network Services Controller that includes InterCloud functionality, you will not be able to upgrade to version 3.2.2 until you remove all InterCloud objects from your current installation. For more information, see the *Cisco Prime Network Services Controller 3.2.2 Quick Start Guide*.

Prime Network Services Controller 3.2.2 includes the following new features and enhancements:

- OpenStack support for Prime Network Services Controller for CSR 1000V edge routers and Citrix NetScaler VPX load balancers
- Edge router enhancements
  - Cisco Smart Licensing support
  - Subinterface configuration
  - Tunnel interface configuration
  - Additional policy configuration (Site-to-site IPsec VPN, EIGRP, and DHCP)
- Load balancer enhancements
  - License automation support
  - Dynamic addition of virtual servers
  - Assigning Citrix NetScaler VPX load balancers in OpenStack
- Automatic instantiation of edge router and load balancer network services in Prime Network Services Controller from Cisco Data Center Network Manager (DCNM)

For more information about these features and how to use them, see Using Prime Network Services Controller 3.2.2 Features, page 9.

Functionality Changes

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

System Requirements

Table 1 identifies Prime Network Services Controller 3.2.2 system requirements.

Table 1 Prime Network Services Controller System Requirements

Requirement	Description
Prime Network Services Controller Virtual Appliance	
Four virtual CPUs	1.8 GHz
Memory	4 GB RAM
Disk Space	220 GB on shared NFS or SAN, configured on two disks as follows: • Disk 1—20 GB • Disk 2—200 GB
Management Interface	One management network interface.
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
Prime Network Services Controller Device Adapter[1]	
Two virtual CPUs	1.8 GHz
Memory	2 GB RAM
Disk Space	20 GB
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

[1] The Prime Network Services Controller Device Adapter must be installed prior to deploying and registering third-party service nodes.

The following sections described additional Prime Network Services Controller requirements:

- Hypervisor Requirements, page 4
- Web-Based GUI Client Requirements, page 5
- Prime Network Services Controller Firewall Ports Requiring Access, page 5

Hypervisor Requirements

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

- See the VMware Compatibility Guide to verify that VMware supports your hardware platform.
- See the Windows Server Catalog to verify that Microsoft Hyper-V supports your hardware platform.
- See the following links to verify that OpenStack supports your hardware platform:
  - OpenStack Compute and Image System Requirements
  - OpenStack for Cisco DFA Install Guide for Using the Cisco OpenStack Installer

Table 2 Hypervisor Requirements

Requirement	Description
VMware	
VMware vSphere	Release 5.0, 5.1, or 5.5 with VMware ESXi (English only)
VMware vCenter	Release 5.0, 5.1 or 5.5 (English Only)
KVM with OpenStack	
KVM Hypervisor	Ubuntu 12.04 LTS server, 64-bit
KVM Kernel	Version 3.2.0-52-generic
Cisco OpenStack Installer	Version depends on Installation mode: • Standalone Mode—Grizzly • Orchestrator Mode—Dynamic Fabric Automation (DFA) OpenStack
Microsoft	
Microsoft Server	Microsoft Hyper-V Server 2012 R2 (Standard or Data Center)
Microsoft SCVMM	Microsoft SCVMM 2012 R2

Web-Based GUI Client Requirements

Table 3 Web-Based GUI Client Requirements

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

[1] Before you can use Chrome with Prime Network Services Controller, you must first 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, page 5.

Configuring Chrome for Use with Prime Network Services Controller

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

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

Step 2 Click **Details**.

Step 3 Locate the Adobe Flash Player plug-ins, and disable each one.

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

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

Prime Network Services Controller Firewall Ports Requiring Access

Table 4 Prime Network Services Controller Firewall Ports Requiring Access

Port	Description
80	HTTP
443	HTTPS
843	Adobe Flash

Performance and Scalability

The following tables list the performance and scalability data for Prime Network Services Controller when using VMware.

Table 5 Performance and Scalability with VMware

Item	Scalability Numbers
Endpoints (ASA 1000Vs, CSR 1000Vs, Citrix NetScaler load balancers, and VSGs)	511
Hypervisors	600
Locales	256
Object Groups	65536
Orgs	2048
Policies	4096
Policy Sets	2048
Rules	16384
Security Profiles	2048
Tenants	256
Managed VMs	5000
Users	260
Zones	8192

Hypervisor Support

The following table identifies the hypervisor support in Prime Network Services Controller 3.2.2.

Table 6 Hypervisor Support in Prime Network Services Controller 3.2.2

Feature and Device Support	VMware vSphere	KVM with OpenStack	Microsoft Hyper-V Hypervisor
Feature Support			
Integration with DCNM	Supported	Supported	Not supported
InterCloud Functionality	Not supported	Not supported	Not supported
Licensing for CSR 1000V and Citrix NetScaler	Supported	Not supported	Not supported
Network Attributes	All	All	All
Network Refresh button	N/A	Supported	Supported

Table 6 Hypervisor Support in Prime Network Services Controller 3.2.2 (continued)

Feature and Device Support	VMware vSphere	KVM with OpenStack	Microsoft Hyper-V Hypervisor
VM Attribute Support	Supported: • Cluster Name • Guest OS Full • Name • Hypervisor Name • Parent Application Name • Port Profile Name • Resource Pool • VM DNS Name • VM Name	N/A	Supported: • Guest OS Full • Name • Port Profile Name • VM DNS Name • VM Name
Device Support			
ASA 1000V	Supported	Not supported	Not supported
Citrix NetScaler 1000V	Supported	Not supported	Not supported
Citrix NetScaler VPX	Supported	Supported	Not supported
CSR 1000V	Supported	Supported	Not supported
VSG	Supported	Not supported	Supported

Important Notes

The following topics provide important information for using Prime Network Services Controller:

- Cisco ASA Instances Do Not Register with Prime Network Services Controller, page 7
- VM DNS Attributes Are Not Populated in Hyper-V Hypervisor, page 8
- Cloned Linux Virtual Machines, page 8
- Editing Firewall Interfaces, page 8
- Online Help Includes InterCloud Management Topics, page 8
- Searching with Special Characters, page 8
- User Account Password Expiration, page 8

Cisco ASA Instances Do Not Register with Prime Network Services Controller

If you instantiate an ASA 1000V service using the asa871-8.ova image, the service instance will not register with Prime Network Services Controller. Contact Cisco Technical Assistance Center (TAC) for help in addressing this issue.

You can contact the TAC over the phone or via the Web:

- Regional phone numbers are available at http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html#numbers.
- To use the Web, go to http://www.cisco.com/cisco/web/support/index.html.

VM DNS Attributes Are Not Populated in Hyper-V Hypervisor

When using Hyper-V Hypervisor, some DNS attributes are not displayed in Prime Network Services Controller. This situation occurs due to recent changes in requirements for Linux VMs running in Hyper-V Hypervisor. For more information and the Microsoft services that must be installed for Prime Network Services Controller to fetch the VM DNS attributes from SCVMM, see http://technet.microsoft.com/en-us/library/jj860438.aspx.

Cloned Linux Virtual Machines

When virtual machines are cloned, new MAC addresses are assigned. This causes a MAC address mismatch between the virtual machine settings and the Linux Guest OS. If you encounter this situation, the following message is displayed:

```
The Guest OS either does not contain interface configuration for the VM NICs or the
interfaces are explicitly disabled.
```

For information on how to resolve the MAC address mismatch, see the VMware Knowledge Base.

Editing Firewall Interfaces

We recommend that you do not edit the data interfaces of compute or edge firewalls. Changing the data interface via the Prime Network Services Controller GUI will stop communications between the Cisco Nexus 1000V VEM link and the firewall, and thereby stop vPath traffic.

If you change the data interfaces of compute or edge firewalls via the Prime Network Services Controller GUI, make the appropriate configuration changes on the Nexus 1000V.

Online Help Includes InterCloud Management Topics

The Prime Network Services Controller 3.2.2 online help includes InterCloud Management topics even though this release does not support InterCloud functionality.

Searching with Special Characters

Searching for organization names will not work if the organization names include special characters such as $.

User Account Password Expiration

When adding a user account, the administrator can choose to expire the account password and select the date on which it expires. When the expiration date is reached, the account is disabled and the user cannot log in to Prime Network Services Controller until a user with administrator privileges extends the expiration date.

Using Prime Network Services Controller 3.2.2 Features

The following topics describe the new features in Cisco Prime Network Services Controller 3.2.2 and how to use them:

Support for OpenStack with KVM

Prime Network Services Controller supports the Kernel Virtual Machine (KVM) hypervisor in an OpenStack environment. You can deploy Prime Network Services Controller in an OpenStack environment in Standalone or Orchestrator mode, register the hypervisor Virtual Machine Manager (VMM) with Prime Network Services Controller, and integrate with Cisco Data Center Network Manager (DCNM). In addition, you can do the following on KVM/OpenStack:

- Instantiate Cisco CSR 1000V edge routers—See Instantiating Edge Routers in an OpenStack Environment, page 14.
- Assign Citrix NetScaler VPX load balancers— See Assigning a Citrix NetScaler VPX Load Balancer in an OpenStack Environment, page 18.

Additional KVM/OpenStack support in Prime Network Services Controller includes the following:

- Integration with OpenStack via HTTPS/HTTP.
- Concurrent interoperation with multiple KVM/OpenStack instances.

Standalone Mode

When Prime Network Services Controller is installed in Standalone mode and you add a tenant, Prime Network Services Controller discovers the networks from OpenStack and automatically associates an OpenStack network with a Prime Network Services Controller network role depending on the following network attributes:

- Shared or not shared
- External or internal

The following table shows how Prime Network Services Controller maps an OpenStack network to a network role, and the scope of that role:

Table 7 OpenStack Network to Prime Network Services Controller Network Role Mapping

Shared Network	External Network	Prime Network Services Controller Network Role	Automatic Creation	Prime Network Services Controller Network Scope
Yes	Yes	External	Yes	root
Yes	No	None	Yes	root
No	Yes	External	Yes	tenant
No	No	Host	Yes	tenant

The following information and conditions apply to Prime Network Services Controller deployed on OpenStack in standalone mode:

- If a discovered network is mapped to None in Prime Network Services Controller, you must change the role to Management or HA.
- For infrastructure networks, if changes are made to the network after the information is initially discovered from OpenStack, you must request a rediscovery of the OpenStack networks. To do this, choose **Resource Management > Managed Resources > root >** *tenant* **> Networks tab**, and then click **Refresh Network**.
- Tenants are created and managed via Prime Network Services Controller as follows:
  - A tenant's name in Prime Network Services Controller must be the same as the project name in OpenStack.
  - The member list in the OpenStack project must contain a superuser admin with the admin role. For information on how to add an admin user to the member list and assign the admin role, see the OpenStack documentation at docs.openstack.org.
  - When a tenant is added to Prime Network Services Controller, Prime Network Services Controller queries OpenStack, learns the various tenant data networks, and maps them to roles as described in Table 7.
  - If either of the following occurs after the information is initially discovered from OpenStack, you must request a rediscovery of the OpenStack network:

    - A data network for a tenant is added, modified, or deleted in OpenStack.

    - Prime Network Services Controller receives a network service creation request.

    To request a rediscovery of the OpenStack networks, choose **Resource Management > Managed Resources > root >** *tenant* **> Networks tab**, and then click **Refresh Network**.
- You must remove a tenant from Prime Network Services Controller before deleting the tenant from OpenStack.

Orchestrator Mode

Prime Network Services Controller supports deployment in Orchestrator mode on Dynamic Fabric Automation (DFA) OpenStack.

After you deploy Prime Network Services Controller in a DFA OpenStack environment in Orchestrator mode, configuration proceeds as follows:

1. You create a tenant and any required networks on DFA OpenStack.
2. DCNM automatically creates the corresponding organization and partitions.
3. DCNM sends the organization and partition configuration information to Prime Network Services Controller.
4. Prime Network Services Controller displays the tenant, any virtual data centers, and all related networks along with their configuration specifics.

To integrate Prime Network Services Controller in a DFA OpenStack environment with DCNM:

Step 1 Deploy Prime Network Services Controller in Orchestrator mode in KVM/OpenStack.

Step 2 Follow the instructions provided in Configuring Connectivity with DCNM in the *Cisco Prime Network Services Controller 3.2 User Guide*.

Edge Router Enhancements

The following topics describe edge router enhancements and how to use them:

- Cisco Smart Licensing Support, page 11
- Subinterface Configuration, page 12
- Tunnel Interface Configuration, page 13
- Additional Edge Router Policy Support, page 14
- Instantiating Edge Routers in an OpenStack Environment, page 14

Cisco Smart Licensing Support

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

Configuring Smart Licensing

Prerequisites

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

Note

- Only one smart license can be configured per tenant.
- Smart Licensing in Prime Network Services Controller must be configured before an edge router is instantiated. If you want to configure licensing after the edge router has been added in Prime Network Services Controller, then you must execute Smart License commands on the edge router.
- If you are registering an edge router that has been manually deployed, you must execute the Smart License commands on the edge router.
- Do not use Smart Licensing for a CSR 1000V that is deployed in an OpenStack environment. Instead, perform any license-related configuration directly on the CSR 1000V.

To configure a smart license for CSR 1000V:

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

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

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

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

a. Enter a license name.

b. (Optional) Enter a description.

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

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

Note

- By default, call home options are configured on the CSR 1000V. You can check the default call home check box in most cases.
- The following call home settings are configurable:
  - User Name—The user must be AAA authorized.
  - Rate Limit—Time is in minutes.
  - Data Private Hostname—This security option can be checked or unchecked.
  - Data Privacy Level—High or Normal.
  - Proxy Server—If checked, you can enter your own proxy server and port to communicate to the Smart License server.

Step 5 Click **OK**. The smart license is created for this tenant.

Step 6 Configure static routing so that the edge router can communicate with the Smart License server (**Policy Management** > **Service Policies** > **root** > **Policies** > **Routing** and click **Add Routing Policy**). For information on configuring routing policies, see "Configuring Routing Policies" in the Cisco Prime Network Services Controller 3.2 User Guide.

Step 7 Configure the DNS policy so that the edge router can resolve the Smart License server URL provided in the Call Home configuration (**Policy Management** > **Device Configurations** > **root** and click **Add Device Profile**). For more information on configuring the DNS policy, see "Configuring Device Polices and Profiles" in the Cisco Prime Network Services Controller 3.2 User Guide.

Step 8 Add an edge router as you normally would under the same tenant and apply the policies you created. Also, in the Select Service Device screen, check the **Enable License** check box and select the license category from the drop-down list. For more information on adding an edge router, see "Edge Router Configuration Workflow" in the online help.

Subinterface Configuration

Note Subinterface configuration is only available on CSR 1000V version 3.12. Confirm that any CSR 1000V image used for registration or instantiation is version 3.12.

In addition to physical (data, management, and gigabit ethernet) interface configuration, Prime Network Services Controller supports subinterface (logical interfaces on a physical interface) configuration. Because there is only one trunk between the devices, you need subinterfaces for multiple VLANs. You can configure subinterfaces with a default gateway to route traffic.

You configure subinterfaces by selecting a Trunk group and designating VLAN IDs when you add an edge router (**Resource Management** > **Managed Resources** > *tenant* and click **Add Edge Router**) or edit its properties in the Network Interface tab (**Resource Management > Managed Resources >** *tenant* **>** *edge-router* and choose **Edit**).

Prerequisite

Create a trunk port profile group on a distributed virtual switch.

From the Add Interface window:

Step 1 Enter the name and description (optional), and choose the physical interface (Gigabit or Management) on which you want to create the subinterfaces.

Step 2 If available, edit the index number if you do not want the default index assigned.

Step 3 Click **Trunk** as the Mode.

Step 4 Choose a trunk port profile group from the Port Group drop-down list.

Step 5 If available, click **Sub-Interface** as the category.

Step 6 Enter a VLAN ID. The VLAN ID must be included in the port profile group you selected in the previous step.

Step 7 Enter sub-management IP, port, and edge router IP address information, as you normally would for a physical interface, and then click **OK**.

Tunnel Interface Configuration

Prime Network Services Controller supports the configuration for site-to-site VPN using IPSEC tunneling. This allows secure transfer between two sites using various encryption algorithms. The following configuration modes and options are supported:

- Internet Security Association and key Management Protocol (ISAKMP) using only Internet Key Exchange version 1 (IKEv1)
- ESP tunnel mode
- NAT Traversal
- Split Tunnel
- Crypto map entries and its application to interfaces

You configure a tunnel interface when you add an edge router (**Resource Management** > **Managed Resources >** *tenant* and click **Add Edge Router**) or edit its properties in the Network Interfaces tab (**Resource Management** > **Managed Resources** > *tenant* > *edge router* and click **Edit**).

From the Add Interface window:

Step 1 Enter the name and description (optional), and check **Tunnel**.

Step 2 Select a previously created subinterface.

Step 3 Enter the appropriate information for the rest of the fields and click **OK**.

Additional Edge Router Policy Support

Prime Network Services Controller supports the following policies on CSR 1000V edge routers that are version 3.12 or higher:

Supported Policy	For More Information, See...[1]
Site-to-site IPsec VPN[2]	Configuring Site-to-Site IPsec VPN Policies For edge router VPN policy configuration to work: • Gigabit interfaces must have crypto rules configured. Also, the IPsec policy can have only one IPsec proposal set listed in the IPsec IKE Proposal Table (**Policy Management > Service Policies > root > Policies > VPN > IPsec Policies**, then click **Add** or **Edit**). The default IPsec policy has a number of proposal sets. • Tunnel interfaces should not have any crypto rules. • After policy configuration, select and apply the policies to the edge router (**Policy Management** > **Service Profiles** > **tenant** > **Edge Router**, then click **Device Service Profiles** and **Interface Service Profiles**).
DHCP	Configuring DHCP Policies
EIGRP	Configuring Routing Policies

[1] To access these policies, see the corresponding sections in the Cisco Prime Optical user guide.

[2] VPN policy configuration is a premium feature and is available only with a premium license.

Instantiating Edge Routers in an OpenStack Environment

Prime Network Services Controller enables you to instantiate and manage CSR 1000V edge routers in an OpenStack environment.

Before You Begin

Confirm the following:

- Prime Network Services Controller is successfully deployed in an OpenStack environment.
- OpenStack Controller has been added as a VMM in Prime Network Services Controller.
- The project in which you want to instantiate the edge router has been created in OpenStack.
- The project contains a flavor with the following attributes:
  - vCPU—1
  - RAM—2560 MB
  - Root Disk—8 MB
  - Ephemeral Disk—0 MB
  - Swap Disk—0 MB
- The member list for the OpenStack project includes a superuser admin with the admin role.

Note Do not use Smart Licensing for a CSR 1000V that is deployed in an OpenStack environment. Instead, perform any license-related configuration directly on the CSR 1000V.

To instantiate an edge router in an OpenStack environment:

1. Complete the steps as described in Table 8.
2. Remove the anti-spoofing rules as described in Removing Anti-Spoofing Rules in OpenStack, page 16. You must remove the anti-spoofing rules for the service VMs to work in OpenStack.

Table 8 Instantiating Edge Routers in KVM/OpenStack

Step	Comments
1. In Prime Network Services Controller, create a tenant with the same name as the project created in OpenStack.	After the tenant is created, the networks for the tenant will automatically be populated in Prime Network Services Controller.
2. In Prime Network Services Controller, locate the management network that was configured in OpenStack by choosing **Resource Management > Managed Resources > root** (or **root >** *tenant*) and then clicking the **Networks** tab.	—
3. From the list of Layer 2 networks that is displayed in the Networks tab, choose the management network and confirm that the role is either Management or HA. If the role is None, click **Edit** to set the role to Management.	The network will not work properly if the role is set to None.
4. Choose **Resource Management > Resources > Images**, and import a CSR 1000V image. The image must be a .qcow2 file.	For more information about importing images, see "Importing Service Images" in the *Cisco Prime Network Services Controller 3.2 User Guide* or online help.
5. (Optional) Create a device profile by choosing **Policy Management > Device Configurations > root > Device Profiles**.	You can use the default device profile or create a new one. For more information, see the *Cisco Prime Network Services Controller 3.2 User Guide* or online help.
6. Add an edge router under the tenant created in Step 1.	The edge router will be available in OpenStack in approximately five to ten minutes. For more information, see the *Cisco Prime Network Services Controller 3.2 User Guide* or the online help.

Table 8 Instantiating Edge Routers in KVM/OpenStack (continued)

Step	Comments
7. Remove anti-spoofing rules from the iptable of the compute node.	See Removing Anti-Spoofing Rules in OpenStack, page 16.
8. If NAT is configured, enter the following command on the compute node on which the edge router VM is running to add an iptables rule for the NAT IP address. **iptables -i** *chain-name* **1 -p all -s** *nat-ip* **-j**	If you do not add a NAT IP address entry to iptables, all traffic for the NAT IP address will be dropped. Enter this command if the VM is moved to a different compute node.

The *Cisco Prime Network Services Controller 3.2 User Guide* is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-services-controller/products-user-guide-list.html.

Removing Anti-Spoofing Rules in OpenStack

For hosts running OVS-based OpenStack, a situation exists that affects all devices with routing functionality, such as CSR 1000V and Citrix NetScaler VPX service VMs.

In this situation, the OVS Quantum plugin enters anti-spoofing entries for each vNIC of the VM. For each vNIC interface, two iptables entries must be removed to enable ANY-ANY routing for VM services.

Note This procedure includes OpenStack commands. For additional information about any of these commands, see the OpenStack documentation at docs.openstack.org.

Perform the following procedure:

- On the compute node on which the service VM is running.
- Each time the service VM is migrated to another compute node.

Step 1 Display iptables entries by entering the following OpenStack command:

```
iptables -L --line-numbers
```

The output should resemble the following example output:

```
Chain quantum-openvswi-oc4ea12ff-e (2 references)
num  target   prot  opt source        destination
1    DROP      all  --  anywhere      anywhere     MAC ! FA:16:3E:16:6E:EE
2    RETURN    udp  --  anywhere      anywhere     udp spt:bootpc dpt:bootps
3    DROP      all  -- !193.1.1.6     anywhere
4    DROP      udp  --  anywhere      anywhere     udp spt:bootps dpt:bootpc
5    DROP      all  --  anywhere      anywhere     state INVALID
6    RETURN    all  --  anywhere      anywhere     state RELATED,ESTABLISHED
7    RETURN    all  --  anywhere      anywhere
8    quantum-openvswi-sg-fallback  all  --  anywhere    anywhere
```

Step 2 In the output, locate the iptable rule chains that contain the VM data interface IP address and MAC address.

In the example, DROP rules 1 and 3 are for a CSR 1000V data interface with the MAC address FA:16:3E:16:6E:EE and the IP address 193.1.1.6.

These are the rules that you will need to remove as described in the following steps.

Step 3 Remove rule 1 by entering the command **ip-tables -D** command. This command uses the format **ip-tables -D** *chain-name rule-number*. Using the example, the command to remove rule 1 would be:

```
iptables -D quantum-openvswi-oc4ea12ff-e 1
```

Step 4 Enter the following command to refresh the list of rules:

```
iptables -L --line-numbers
```

Note Entering this command after removing an entry helps ensure that you delete the correct entry with the next command.

Step 5 In the output, identify the next rule to delete, and repeat Step 3 and Step 4.

Load Balancer Enhancements

The following topics describe the load balancer enhancements and how to use them:

- License Automation Support, page 17
- Dynamic Addition of Virtual Servers, page 18
- Assigning a Citrix NetScaler VPX Load Balancer in an OpenStack Environment, page 18

License Automation Support

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

Prerequisite

1. The license files have been obtained. For information on how to generate and obtain the license files for Citrix NetScaler VPX and 1000V load balancers, see http://support.citrix.com/article/CTX122426.
2. The license category (feature and throughput level package) that has been purchased for the load balancer. For more information on the license categories available, see http://support.citrix.com/article/CTX122426.

Note

- The license files must be imported before the load balancer is instantiated.
- Multiple license bundles can be imported. However, the bundles cannot have files with the same host ID or the same filename as previous bundles.

- You cannot delete any licenses if it is assigned to a load balancer service node.

To configure licensing for Citrix NetScaler VPX and 1000V load balancers:

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

> **Note** If licenses are imported at root, all tenants below root have the ability to use the license. For more granular control, import licenses at the tenant level or below.

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

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

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

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

Step 6 Add a load balancer as you normally would by instantiation. However, in the Select Service Device screen check the **Enable License** check box and select the license category from the drop-down list. For more information on adding a load balancer, see the “Load Balancer Configuration Workflow” topic in the Cisco Prime Network Services Controller 3.2 User Guide.

Dynamic Addition of Virtual Servers

In this release, you can add (or delete) virtual IP addresses (VIPs) to an existing load balancer that has been registered or instantiated. You can assign a single virtual server profile to multiple VIPs.

To add VIPs:

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

Step 2 In the Network Services tab, choose an existing load balancer and click **Edit**.

Step 3 In the Virtual Servers tab, click **Add Virtual IP**.

Step 4 Enter the VIP details and click **OK**. You can repeat the process to add multiple VIPs.

Assigning a Citrix NetScaler VPX Load Balancer in an OpenStack Environment

Assigning a Citrix NetScaler VPX load balancer on OpenStack involves the following tasks:

1. Configuring OpenStack for Citrix NetScaler VPX Load Balancers, page 19
2. Instantiating a Citrix NetScaler VPX Load Balancer, page 20
3. Registering the Citrix NetScaler VPX Instance with Prime Network Services Controller, page 21

Configuring OpenStack for Citrix NetScaler VPX Load Balancers

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

- Creating an initialization shell script.
- Creating a flavor.
- Uploading a Citrix NetScaler VPX image.
- Creating the required subnet.

Note This procedure includes OpenStack commands. For additional information about any of these commands, see the OpenStack documentation at docs.openstack.org.

Before You Begin

Confirm the following:

- Prime Network Services Controller has been installed and is accessible from OpenStack.
- The Prime Network Services Controller Device Adapter has been installed on OpenStack and is registered with Prime Network Services Controller. For more information, see the *Cisco Prime Network Services Controller 3.2.2 Quick Start Guide*.
- The project in which you want to instantiate the load balancer has been created in OpenStack.
- The member list for the OpenStack project includes a superuser admin with the admin role.
- The following network requirements are met:
  - Two vNICs are available: one for management and one for data.
  - The management interface is in the same subnet as Prime Network Services Controller.

Note The project name in OpenStack must be the same as the tenant name in Prime Network Services Controller when you register the Citrix NetScaler VPX load balancer.

To configure OpenStack:

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

a. Open an SSH session on the OpenStack controller.

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

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

c. Run the shell script.

Step 2 In the OpenStack dashboard, create a flavor with the following attributes for the Citrix NetScaler VPX image:

- vCPU—2
- RAM—4096 MB

- Root Disk—0 MB
- Ephemeral Disk—0 MB
- Swap Disk—0 MB

Step 3 Upload the Citrix NetScaler VPX image by entering the following command:

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

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

Your command might resemble the following:

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

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

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

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

Step 5 Create a private subnet by entering the following command:

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

Note The Citrix NetScaler VPX data interfaces must be in a different subnet than the management interface.

Instantiating a Citrix NetScaler VPX Load Balancer

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

Note This procedure includes OpenStack commands. For additional information about any of these commands, see the OpenStack documentation at docs.openstack.org.

Before You Begin

- Make sure you have completed the tasks in Configuring OpenStack for Citrix NetScaler VPX Load Balancers, page 19.
- Disable anti-spoofing in OpenStack. For information on how to disable anti-spoofing, see Removing Anti-Spoofing Rules in OpenStack, page 16.

To instantiate a Citrix NetScaler VPX load balancer:

Step 1 Obtain the UUIDs of the following networks:

- The network you created in Configuring OpenStack for Citrix NetScaler VPX Load Balancers, page 19.
- The network corresponding to “external.”

Step 2 Enter the OpenStack **nova boot** command to create the Citrix NetScaler VPX instance.

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

For example, your command might resemble the following:

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

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

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

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

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

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

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

Step 8 In the shell, edit the /nsconfig/ns.conf file as follows:

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

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

c. Save and exit the file.

Step 9 Reboot at the shell command line.

The Citrix NetScaler VPX VM will restart. After it restarts, you can use SSH to connect to the management IP address.

Registering the Citrix NetScaler VPX Instance with Prime Network Services Controller

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

Before You Begin

Confirm that a virtual server profile has been configured.

To register the Citrix NetScaler VPX:

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

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

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

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

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

    – IP address
    – Subnet mask
    – Gateway IP address
    – Type—Choose **VPX**.
    – Version—Choose the version.
    – Access credentials

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

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

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

Automatic Instantiation of Network Services

Prime Network Services Controller 3.2.2 enables you to automatically instantiate the following network services in Prime Network Services Controller from DCNM:

- Compute firewall
- Edge router
- Load balancer

This functionality includes the following new network segment roles and areas of responsibility:

- Management—Management interface connectivity for service nodes.
- HA—High availability interface connectivity for service nodes.
- External—Outside interface connection on an edge router service.
- Service-ES—Inside interface connection on an edge router service.
- Service-LB—One-armed load-balancer service for a virtual data center.
- Service-vPath—Connectivity for a Layer 3 adjacent compute firewall.

See the following topics for more information about instantiating network services:

- Service Instantiation Workflow, page 23
- Prerequisites for Instantiating Network Services, page 23

Service Instantiation Workflow

Table 9 describes the high-level tasks required to configure and instantiate network services in Prime Network Services Controller.

Table 9 Service Instantiation Workflow

Task	Related Topic
1. Confirm that the prerequisites are met.	See Prerequisites for Instantiating Network Services, page 23.
2. In Prime Network Services Controller, create a service automation definition.	See Creating a Service Automation Definition, page 23.
3. In Prime Network Services Controller, create a management network and subnet.	See Creating a Management Network, page 25.
4. In DCNM, create a vPath network.	See Creating a vPath Network in DCNM, page 26.
5. In DCNM, instantiate the required network service.	See either of the following: • Instantiating an Edge Router Service, page 26 • Instantiating a Load Balancer Service, page 27

Prerequisites for Instantiating Network Services

Confirm that the following prerequisites are met before configuring and instantiating network services:

- Prime Network Services Controller is deployed in Orchestrator mode.
- The hypervisor Virtual Machine Manager (VMM) is registered with Prime Network Services Controller.
- The following VM images have been imported into Prime Network Services Controller:
  - VSG
  - CSR 1000V
  - Citrix NetScaler VPX

  Depending on the service that you want to instantiate, you can import any or all of these images.
- Prime Network Services Controller is registered with DCNM.

  For more information, see the Cisco Prime Network Services Controller documentation.

Creating a Service Automation Definition

This procedure is part of the workflow for instantiating network services. For more information, see Service Instantiation Workflow, page 23.

A service automation definition enables you to specify the profiles, image, and credentials to be used when instantiating a service. Depending on the type of service, additional options are available. You must create a definition for each service type: compute firewall, edge router, and load balancer.

To configure a service automation definition:

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

Step 2 Click the **Service Automation** tab.

Step 3 Under Service Automation Definitions, click the **Add** button for the service that you plan to instantiate: compute firewall, edge router, or load balancer.

Step 4 In the Add Network Service dialog box, provide the information as described in Table 10, and then click **OK**. Depending on the type of service, you will see different fields.

Note You must set the Admin state to *enable* to instantiate the service.

Table 10 Add Network Service Dialog Box

Field	Description
Properties	
Admin State	Choose the administrative state of the network service: enable or disable. You must set the Admin state to *enable* to instantiate a network service.
HA Mode	(Compute firewall only) Choose whether the service should operate in standalone or active standby mode.
Deployment Size	(Compute firewall only) Choose the size of the deployment: small, medium, or large. For more information, see Compute Firewall Deployment Options in the online help.
Enable License	(Edge router and load balancer) Check the check box to enable licensing for the network service.
Feature License	Appears if you check the Enable License check box. Choose an existing license category or create a new one.
Compute	
CPU Cores	(Edge router only) Choose the number of virtual CPUs for this deployment. For more information, see Edge Router Deployment Options in the online help.
Memory Size (MB)	(Edge router only) Choose the amount of memory for this deployment. For more information, see Edge Router Deployment Options in the online help.

Table 10 Add Network Service Dialog Box (continued)

Field	Description
Placement / Availability Zone	Host or cluster on which the service VM is to be deployed. If no location is entered, Prime Network Services Controller will select the location using a round-robin selection process.
Profiles	
Device Config Profile	Choose the device configuration profile to use for the network service.
Device Service Profile	(Edge router only) Choose the device service profile to use for the network service.
Inside Interface Service Profile	(Edge router only) Choose the inside interface service profile to use for the network service.
Outside Interface Service Profile	(Edge router only) Choose the outside interface service profile to use for the network service.
Access	
Login User	User account for administrative access.
Login Password	User password for administrative access.
Confirm Password	Confirming password entry.
VM Image Table	
image	Choose the VM image to use to instantiate the network service.

Creating a Management Network

This procedure is part of the workflow for instantiating network services. For more information, see Service Instantiation Workflow, page 23.

You must create one management network at root in Prime Network Services Controller to instantiate network services.

To create a management network at root:

Step 1 Choose **Resource Management** > **Managed Resources** > **root** > **Networks** > **L2 Networks**.

Step 2 Click **Add** to add a management network under L2 Networks, and then provide the following information:

a. In the Add L2 Network dialog box, add a name for the network.

b. In the Role drop-down list, choose **Management**.

c. Choose the VM Manager and port group.

Note It is important to choose the correct port group. The port group that you choose will be used for all instantiated services.

d. Click **Add**.

Step 3 In the Networks tab, choose the network that you created in Step 2 and click **Add** above the Subnetworks table.

Step 4 In the Add Subnetwork dialog box, provide the following information and then click **OK**:

- Subnet mask
- Gateway IP address
- Subnet name
- IP address range

Creating a vPath Network in DCNM

This procedure is part of the workflow for instantiating network services. For more information, see Service Instantiation Workflow, page 23.

A vPath network is required to provide connectivity to the Layer 3 adjacent compute firewall.

To create a vPath network in DCNM:

Step 1 Navigate to the vPath organization and partition that were created automatically when DCNM booted.

Step 2 In the partition, add a vPath network, being sure to choose **Service-vPath Network** from the Network Role drop-down list.

For more information about configuring networks in DCNM, see the DCNM documentation at www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/tsd-products-support-series-home.html.

After the vPath network is created, it is displayed in Prime Network Services Controller in the Networks tab for root (**Resource Management** > **Managed Resources** > **root**).

Instantiating an Edge Router Service

This procedure is part of the workflow for instantiating network services. For more information, see Service Instantiation Workflow, page 23.

The following configuration must exist in DCNM to instantiate an edge router service:

- Two partitions must exist under the required organization:
  - A partition for the edge router service network
  - A partition for an external network
- The external partition must have the same name as the service network partition with -ext appended to the name. For example, if the service network partition is named partition123, the external network partition must be named partition123-ext.

To set up the required networks and instantiate an edge router service:

Step 1 In DCNM, create an organization and partition for the edge router service.

Step 2 In the partition that you created in Step 1, create a network for the edge router service, making sure that you choose **Service-ES Network** from the Network Role drop-down list.

After the network is created, the following information is displayed in Prime Network Services Controller:

- The organization and partition are displayed as a tenant and virtual data center (VDC).
- The VDC Networks tab contains an edge router entry for the service network.

Step 3 In DCNM, create an external partition under the organization created in Step 1. The external partition must have the same name as the first partition with the extension -ext. For example, if the first partition is named partition123, and the external network partition must be named partition123-ext.

Step 4 Add a network to the external partition by choosing **External Network** from the Network Role drop-down list.

After the network is created, the following information is displayed in Prime Network Services Controller for the VDC:

- The Networks tab displays the external network created in DCNM.
- The Network Services tab displays the instantiated edge router service with the name Auto-EdgeRouter.

Instantiating a Load Balancer Service

This procedure is part of the workflow for instantiating network services. For more information, see Service Instantiation Workflow, page 23.

To instantiate a load balancer service:

Step 1 In DCNM, create an organization and partition for the load balancer service.

Step 2 In the partition that you created in Step 1, create a network for the service, making sure that you choose **Service-LB Network** from the Network Role drop-down list.

After the network is created, the following information is available in Prime Network Services Controller:

- The organization and partition are displayed in Prime Network Services Controller as a tenant and VDC.
- For the VDC:
  - The Networks tab contains an entry for the load balancer service network.
  - The Network Services tab displays the instantiated load balancer service (Auto-LoadBalancer).

Open Bugs

Table 11 lists open bugs in Prime Network Services Controller 3.2.2.

Table 11 Open Bugs in Prime Network Services Controller 3.2.2

Bug ID	Description
CSCul78911	If you attempt to add an interface to a CSR 1000V edge router when the admin state is set to disabled, you receive the error "Cannot assign IP, admin state for Router Interface *name* is disabled."
CSCun83926	When configuring CSR 1000V Smart Licensing, if you check the Use Default Call Home check box, an error message is displayed.
CSCuo16775	When creating VPN Crypto Map policy rules for CSR 1000V edge routers, no information is available regarding supported or unsupported operators (such as equals, not equals, and so on).
CSCuo80418	If you enter incorrect credentials when adding OpenStack as a Virtual Machine Manager (VMM), correct the credentials, and refresh the network, the networks are not displayed in the GUI under root or the tenant (Resource Management > Managed Resources > root > Networks tab).
CSCuo96606	When using CSR 1000V with Smart Licensing enabled, the following can occur: • A CSR 1000V does not complete the instantiation process. • When instantiating a CSR 1000V in an OpenStack environment, you must manually register the CSR 1000V with the Smart Licensing server.

Using the Bug Search Tool

This section explains how to use the Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Enter**.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter Cisco Prime Network Services Controller 3.2.2 and press **Enter**. (Leave the other fields empty.)

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

Tip To export the results to a spreadsheet, click the **Export Results to Excel** link.

Related Documentation

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

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

- *Cisco Prime Network Services Controller 3.2.2 Documentation Roadmap*
- *Cisco Prime Network Services Controller 3.2.2 Release Notes*
- *Cisco Prime Network Services Controller 3.2.2 Quick Start Guide*
- *Cisco Prime Network Services Controller 3.2 User Guide*
- *Cisco Prime Network Services Controller 3.2.2 Supported Devices Table*
- *Cisco Prime Network Services Controller 3.0 CLI Configuration Guide*
- *Cisco Prime Network Services Controller 3.2 XML API Reference Guide*
- *Open Source Used in Cisco Prime Network Services Controller 3.2.2*

Accessibility Features in Prime Network Services Controller 3.2.2

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.