Cisco Prime Network Services Controller 3.0 Release Notes

October 6, 2014

These release notes contain the following sections for the Cisco Prime Network Services Controller 3.0 (Prime Network Services Controller 3.0) release:

- New and Changed Information, page 1
- Introduction, page 2
- Requirements, page 3
- New Features, page 6
- Important Notes, page 7
- Open Bugs, page 9
- Related Documentation, page 9
- Obtaining Documentation and Submitting a Service Request, page 10

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
March 25, 2014	Added CSCum89284 to the list of open bugs.	Open Bugs, page 9
July 2013	Initial release.	—

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

Introduction

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 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.

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) Cloud Firewall virtual security services.

Table 1 details the primary features and benefits of Prime Network Services Controller.

Table 1 Features and Benefits

Feature	Description	Benefits
Multiple-Device Management	Central management of VSG and ASA 1000V for Nexus 1000V series switches.	Simplifies provisioning and troubleshooting in a scaled-out data center.
Security Profiles	Representation of VSG and ASA 1000V security policy configuration in a profile.	• Simplifies provisioning. • Reduces administrative errors during security policy changes. • Reduces audit complexities. • Helps enable a highly scaled-out data center environment.
Stateless Device Provisioning	The management agents in VSG and ASA 1000V are stateless, receiving information from Prime Network Services Controller.	• Enhances scalability. • Provides robust endpoint failure recovery without loss of configuration state.
Security Policy Management	Security policies are authored, edited, and provisioned centrally.	• Simplifies the operation and management of security policies. • Helps ensure that security intent is accurately represented in the associated security policies.
Context-Aware Security Policies	Prime Network Services Controller obtains virtual machine contexts from VMware vCenter.	Allows a security administrator to institute highly specific policy controls across the entire virtual infrastructure.

Table 1 Features and Benefits (continued)

Feature	Description	Benefits
Dynamic Security Policy and Zone Provisioning	Prime Network Services Controller interacts with the Nexus 1000V Virtual Supervisor Module (VSM) to bind the security profile to the corresponding Nexus 1000V port profile. When virtual machines are dynamically instantiated by server administrators and the appropriate port profiles applied, their association with trust zones is also established.	Helps enable security profiles to stay aligned with rapid changes in the virtual data center.
Multi-Tenant Management	Prime Network Services Controller is designed to manage VSG and ASA 1000V security policies in a dense, multi-tenant environment so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies.	• Reduces administrative errors. • Helps ensure segregation of duties in administrative terms. • Simplifies audit procedures.
Role-Based Access Control (RBAC)	RBAC simplifies operation tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures.	• Reduces administrative errors. • Enables detailed control of user privileges. • Simplifies auditing requirements.
XML-Based API	The Prime Network Services Controller XML API allows external system management and orchestration tools to programmatically provision VSG and ASA 1000V devices.	• Allows use of best-in-class management software. • Offers transparent and scalable operation management.

Requirements

The following tables identify Prime Network Services Controller 3.0 requirements:

- Table 2—Prime Network Services Controller System Requirements
- Table 3—Web-Based GUI Client Requirements
- Table 4—Prime Network Services Controller Firewall Ports Requiring Access
- Table 5—Ports to Access Amazon AWS

Table 2 Prime Network Services Controller System Requirements

Requirement	Description
Virtual Appliance	
Two Virtual CPUs	1.5 GHz
Memory	4 GB RAM
Disk Space	220 GB on shared network file storage (NFS) or storage area network (SAN) in the following configuration: • Disk 1—20 GB • Disk 2—200 GB

Table 2 Prime Network Services Controller System Requirements (continued)

Requirement	Description
Management Interface	One management network interface.
Processor	x86 Intel or AMD server with 64-bit processor listed in the VMware compatibility matrix
VMware	
VMware vSphere	Release 5.0 or 5.1 with VMware ESX or ESXi (American English only)
VMware vCenter	Release 5.0 or 5.1 (American English only)
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

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 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 you can use Chrome with Prime Network Services Controller 3.0, 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.

Table 4 Prime Network Services Controller Firewall Ports Requiring Access

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

Table 5 Ports to Access Amazon AWS

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

Configuring Chrome for Use with Prime Network Services Controller

To use Chrome with Prime Network Services Controller 3.0, 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 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.

New Features

Table 6 describes the new features available in Prime Network Services Controller 3.0.

Table 6 New Features in Prime Network Services Controller 3.0

Feature	Description
InterCloud Management	Manage InterCloud Management resources: • Import InterCloud images so that you can create InterCloud links. • Create Virtual Private Clouds (VPCs) on a public cloud. • Via InterCloud links, extend your enterprise data center into the cloud. • Create InterCloud links in either standalone or active standby mode. • Establish secure tunnels for communications between the local data center and the public cloud, and within the public cloud. • Import VM images for use on the public cloud. • Place VM images (referred to as *templates*) on the public cloud, from either an imported image or a VM in the enterprise data center. • Instantiate VMs on the cloud from templates. • Monitor the status of jobs you have initiated. • Monitor the status of InterCloud links. • Update InterCloud link images. • Remove InterCloud links.
Policies and Profiles	Support a new Tunnel profile: • Key policy • Connection Parameter policy The Device profile supports InterCloud Extenders and Switches.
Support for AMI, ISO, and OVA images	Import VM images in AMI, ISO, or OVA format so that you can create templates on the cloud. In addition, depending on the image format, you can configure image-specific attributes when creating a template.

Table 6 New Features in Prime Network Services Controller 3.0 (continued)

Feature	Description
User roles and privileges	Two new roles and their associated privileges: • intercloud-infra—Read and write access for InterCloud operations, including creating InterCloud links, creating provider accounts, and managing InterCloud extender and switch images. • intercloud-server—Read and write access for cloud VMs. Users can create or move VMs from the enterprise to the cloud. Users can monitor cloud VMs for multiple tenants.
Wizards	New wizards guide you through the following cloud-related activities: • Adding an InterCloud link. • Creating a template on a cloud. • Enabling high availability on an InterCloud link. • Adding a new template. • Migrating an enterprise data center VM to the cloud. • Instantiating a cloud VM. • Updating an InterCloud link.

Important Notes

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

- Creating Multiple Templates, page 7
- Prerequisites for Migrating Windows VMs, page 7
- Searching with Special Characters, page 8
- Changing DNS Name Repeatedly Stops Cloud Provider Manager, page 8
- User Account Password Expiration, page 8

Creating Multiple Templates

We recommend that you create no more than three templates simultaneously. This limitation applies to creating templates using either of the following methods, or a combination of these methods:

- Creating a template from an AMI.
- Creating a template by migrating a VM from the enterprise data center.

Prerequisites for Migrating Windows VMs

This topic details the prerequisites that must be met before you perform either of the following procedures:

- Migrate an existing Windows VM from VMware vCenter to the cloud.
- Create an AMI image from a Windows VM and import it into Prime Network Services Controller.

Before migrating a Windows VM, do the following:

- Disable automatic logon.
- Ensure the following:
  - Network interfaces are enabled.
  - The DHCP client service is enabled and running.
  - The Windows Firewall allows the following InterCloud ports: 22 (TCP), 3389 (TCP), and 6644 (TCP and UDP).
  - There is no security software or firewall that can prevent network connectivity.
- Disable any service or application on the VM that uses port 22.
- If the Windows VM is joined to a domain, confirm the following:
  - No domain policies exist that prohibit device driver installation for network interface devices.
  - Trusted publisher policies do not prohibit installation of Cisco's certificate into the system.

  Although it is rare for such policies to be set, check with the Windows Enterprise Domain Administrator if you are uncertain.
- Shut down the Windows VM properly:
  - Before using the Windows VM to create an AMI image, confirm that the Windows VM was shut down properly.
  - If you are migrating a Windows VM to the cloud, Prime Network Services Controller will shut down the VM if VMware Tools is installed on the VM. If VMware Tools is not installed on the VM, power down the Windows VM before initiating the migration.
- Enable Remote Desktop Protocol (RDP) on the source machine.
- We recommend that you install the Windows hotfix available at http://support.microsoft.com/kb/2528507 for crash dump support in case the driver crashes.

Searching with Special Characters

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

Changing DNS Name Repeatedly Stops Cloud Provider Manager

If you change the DNS name four or more times, Cloud Provider Manager stops working. If this occurs, log into the Prime Network Services Controller server via the CLI and enter the following commands:

```
nsc# connect local-mgmt
nsc (local-mgmt)# service restart
```

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.

Open Bugs

Table 7 lists open bugs in Prime Network Services Controller 3.0.

Table 7 Open Bugs in Prime Network Services Controller 3.0

Bug ID	Description
CSCuh53130	Moving a Windows VMDK from the enterprise to the cloud includes only actual interfaces configured in the VM.
CSCuh64656	InterCloud Switch and InterCloud Extender enter lost-visibility state if their hostnames are changed in Prime Network Services Controller.
CSCuh73079	If you edit the InterCloud Extender so that it points to a new ESXi host on a new vCenter, deployment of the InterCloud Extender fails.
CSCuh74272	One port ID is lost whenever the creation of a VM fails.
CSCuh76446	Editing the management IP address of an InterCloud Extender after the Extender is deployed stops the deployment.
CSCuh82610	Migrating a Linux VM fails with a vmware-mount error.
CSCuh82727	If you create a VSM port profile that is configured with an organization and then create a cloud VM using that port profile, incomplete information for that port profile is displayed when you view the properties for the VSM or cloud VM in **Resource Management > Resources**.
CSCuh84843	If a DNS server is not configured, VM Manager process fails.
CSCuh85315	Windows registry entries for NICs are displayed in random order.
CSCuh88154	The MAC address pool is not replenished when a cloud VM is terminated.
CSCuh88175	The access tunnel is up in the InterCloud Switch, but it is displayed as down in the GUI.
CSCuh97084	The InterCloud Agent Image URL www.cisco.com/go/network-controller that is noted in the GUI, results in a 404 error on cisco.com. The URL should be http://software.cisco.com/download/release.html?i=!y&mdfid=284653427&softwareid=282088129&release=5.2(1)IC1(1.1)&os=.
CSCuh99777	Prime Network Services Controller fails to open known_hosts file during InterCloud link creation.
CSCum89284	VSG is missing some or all protected virtual machines (VMs) and thus dropping all traffic for those VMs.

Related Documentation

The following Prime Network Services Controller documentation is available for this release:

- *Cisco Prime Network Services Controller 3.0 Quick Start Guide*
- *Cisco Prime Network Services Controller 3.0 User Guide*
- *Cisco Prime Network Services Controller 3.0 Release Notes*
- *Cisco Prime Network Services Controller 3.0 CLI Configuration Guide*
- *Cisco Prime Network Services Controller 3.0 XML API Guide*

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/en/US/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.