



Cisco Prime Network Services Controller 3.0.2 Release Notes

September 19, 2019

These release notes contain the following sections for the Cisco Prime Network Services Controller 3.0.2 (Prime Network Services Controller 3.0.2) release:

- [New and Changed Information, page 1](#)
- [Introduction, page 2](#)
- [Requirements, page 3](#)
- [Performance and Scalability, page 6](#)
- [New Features, page 7](#)
- [Important Notes, page 9](#)
- [Open Bugs, page 12](#)
- [Using the Bug Search Tool, page 12](#)
- [Related Documentation, page 13](#)
- [Accessibility Features in Prime Network Services Controller 3.0.2, page 13](#)
- [Obtaining Documentation and Submitting a Service Request, page 13](#)

New and Changed Information

[Table 1](#) describes information that has been added or changed since the initial release of this document.

Table 1 *New and Changed Information*

Date Released	Revision	Location
March 25, 2014	Added CSCum89284 to the list of open bugs.	Open Bugs, page 12



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

Table 1 New and Changed Information (continued)

Date Released	Revision	Location
November 6, 2013	Updated support information for Amazon Marketplace.	New Features, page 7
October 16, 2013	Initial release.	—

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 2](#) details the primary features and benefits of Prime Network Services Controller.

For information on new features included in this release, see [New Features, page 7](#).

Table 2 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Enhances scalability. Provides robust endpoint failure recovery without loss of configuration state.
Security Policy Management	Security policies are authored, edited, and provisioned centrally.	<ul style="list-style-type: none"> Simplifies the operation and management of security policies. Helps ensure that security intent is accurately represented in the associated security policies.

Table 2 *Features and Benefits (continued)*

Feature	Description	Benefits
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.
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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Allows use of best-in-class management software. • Offers transparent and scalable operation management.

Requirements

The following tables identify Prime Network Services Controller 3.0.2 requirements:

- [Table 3—Prime Network Services Controller System Requirements](#)
- [Table 4—Hypervisor Requirements](#)
- [Table 5—Web-Based GUI Client Requirements](#)
- [Table 6—Prime Network Services Controller Firewall Ports Requiring Access](#)
- [Table 7—Ports to Access Amazon AWS](#)

Table 3 *Prime Network Services Controller System Requirements*

Requirement	Description
Virtual Appliance	
Four Virtual CPUs	1.5 GHz
Memory	4 GB RAM

Table 3 Prime Network Services Controller System Requirements (continued)

Requirement	Description
Disk Space	One of the following, depending on InterCloud functionality: <ul style="list-style-type: none"> With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN) in the following configuration: <ul style="list-style-type: none"> Disk 1—20 GB Disk 2—200 GB Without InterCloud functionality, 40 GB on shared NFS or SAN in the following configuration: <ul style="list-style-type: none"> 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	—
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

**Note**

For information about PNSC upgrade path, see the latest [Cisco PNSC Upgrade Matrix](#).

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 4 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)

Table 4 Hypervisor Requirements (continued)

Requirement	Description
Microsoft	
Microsoft Server	Microsoft Windows Server 2012 with Hyper-V (Standard or Data Center)
Microsoft SCVMM	Microsoft SCVMM 2012 SP1 or higher

Table 5 Web-Based GUI Client Requirements

Requirement	Description
Operating System	Either of the following: <ul style="list-style-type: none"> Microsoft Windows Apple Mac OS
Browser	Any of the following: <ul style="list-style-type: none"> Internet Explorer 9.0 or higher Mozilla Firefox 11.0 or higher Google Chrome 18.0 or higher¹
Flash Player	Adobe Flash Player plugin 11.2 or higher

1. Before you can use Chrome with Prime Network Services Controller 3.0.2, 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 6.

Table 6 Prime Network Services Controller Firewall Ports Requiring Access

Port	Description
80	HTTP
443	HTTPS
843	Adobe Flash

[Table 7](#) lists the ports that must be enabled to access the Amazon Web Services (AWS) public IP address ranges listed at <https://forums.aws.amazon.com/ann.jspa?annID=1701>.

Table 7 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, 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 in to Prime Network Services Controller.
-

Performance and Scalability

[Table 8](#) lists the performance and scalability data for Prime Network Services Controller.

Table 8 *Prime Network Services Controller Performance and Scalability*

Item	Scalability Numbers
ASA 1000Vs and VSGs	255
Hypervisors	600
Locales	128
Object Group	65536
Orgs	2048
Policies	4096
Policy Sets	2048
Rules	16384
Security Profiles	2048
Tenants	256
Managed VMs	5000
Zones	8192

New Features

Table 9 describes the new features available in Prime Network Services Controller 3.0.2.

Table 9 *New Features in Prime Network Services Controller 3.0.2*

Feature	Description
Amazon Marketplace support	<p>Note The Amazon Marketplace feature is not supported in Prime Network Services Controller 3.0.2.</p> <p>Support for Amazon Marketplace provides the following benefits associated with creating an InterCloud link:</p> <ul style="list-style-type: none"> • Access to Amazon Marketplace is provided via the Add InterCloud Link wizard. • You can view and optionally purchase the number of cloud VM licenses that you need. • You can easily install an InterCloud Switch template from Amazon Marketplace. • The time required to create an InterCloud link is significantly reduced. • Amazon Marketplace manages the purchase and automatically charges the associated Amazon provider account. • Amazon tracks the available number of cloud VMs as cloud VMs are instantiated.
Bundle import of images	<p>To improve usability and simplify the process of creating an InterCloud link, Prime Network Services Controller enables you to import a single zipped file that contains the following images:</p> <ul style="list-style-type: none"> • InterCloud Extender image • InterCloud Switch image • Cloud VM driver images <p>After the zipped file is imported, Prime Network Services Controller automatically places the zipped files in the correct locations and populates the InterCloud Link Wizard with the images.</p> <p>This feature helps ensure that you always have the compatible images available for creating InterCloud links and instantiating cloud VMs.</p>

Table 9 *New Features in Prime Network Services Controller 3.0.2 (continued)*

Feature	Description
GUI changes	<ul style="list-style-type: none"> • The following GUI items have been removed: <ul style="list-style-type: none"> – Sub-Elements tabs – Events tabs – VM Managers tab from Administration • The following items have been changed: <ul style="list-style-type: none"> – The InterCloud Agent Images and Infrastructure Images options in InterCloud Management have been replaced by a single Images option. – The Administration Operations Backups table has been renamed to Administration Operations, and it includes all operation types (backups, import, and export). – The VM Managers tab has been moved under Resource Management. • The following new wizards have been added: <ul style="list-style-type: none"> – Add a Compute Firewall Wizard – Adding Edge Firewall • The following enhancements have been made: <ul style="list-style-type: none"> – Options have been consolidated in a single Actions drop-down list in table toolbars. – A Filter option has been added to tables. – A new Service Devices category has been added under Resource Management > Resources.
Hyper-V Hypervisor support	<p>Prime Network Services Controller can be installed on the VMware Hypervisor and the Microsoft Hyper-V Hypervisor. The following are some of the Prime Network Services Controller features that are not supported when Prime Network Services Controller is installed on Hyper-V Hypervisor:</p> <ul style="list-style-type: none"> • When adding a rule to create an ACL policy: <ul style="list-style-type: none"> – The option to match any one rule is disabled. The only available option is to match all the rules. – The service condition is disabled. – If you set source or destination conditions, the VM attribute type is not supported. • When adding an object group: <ul style="list-style-type: none"> – If the attribute type is Network, the attribute name Service is not supported. – The VM attribute type is not supported. • When working with vZones, the option to match any one rule is disabled. The vZone must match all the conditions.

Table 9 New Features in Prime Network Services Controller 3.0.2 (continued)

Feature	Description
Multi-tenancy	<p>Prime Network Services Controller adds a new role named tenant-admin. Users with tenant-admin role can see only those objects and resources related to the tenants with which they are associated. They cannot see the policies, resources, or logs of other tenants.</p> <p>Only users with the admin role can add users with the tenant-admin role, and they must associate the user with the tenant-admin role with a locale and organization.</p> <p>The tenant-admin role has the following privileges:</p> <ul style="list-style-type: none"> • Policy management • Resource configuration (except tenant addition or deletion) • Tenant management
Service VM instantiation and life cycle management	<ul style="list-style-type: none"> • Resources are available from a new Service Devices category and from the Virtual Supervisor Modules (Resources Management > Resources). • A new Images option enables you to import service images to use for instantiating compute and edge firewalls. • You now have the option to import new image versions.
InterCloud VPC-based security (IP groups)	Access to cloud VMs is limited to IP addresses identified in one or more IP groups for each Virtual Private Cloud (VPC).

Important Notes

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

- [Cloned Linux Virtual Machines, page 9](#)
- [Creating Multiple Templates, page 10](#)
- [Editing Firewall Interfaces, page 10](#)
- [Prerequisites for Migrating Windows VMs, page 10](#)
- [Searching with Special Characters, page 11](#)
- [Changing DNS Name Repeatedly Stops Cloud Provider Manager, page 11](#)
- [Warnings of Outdated OpenSSH and Potential Security Vulnerability, page 11](#)
- [User Account Password Expiration, page 11](#)

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](#).

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 Amazon Machine Image (AMI).
- Creating a template by migrating a VM from the enterprise data center.

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.

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 in to the Prime Network Services Controller server via the CLI and enter the following commands:

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

Warnings of Outdated OpenSSH and Potential Security Vulnerability

If you run a security scan against Prime Network Services Controller, the scan results in false OpenSSH security vulnerability warnings. Red Hat Enterprise Linux has verified that these issues do not pose security vulnerabilities. For more information, see the following URLs:

- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-2243>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-0726>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5794>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4925>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4109>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5229>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5052>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5051>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4925>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4924>

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 10 lists open bugs in Prime Network Services Controller 3.0.2.

Table 10 Open Bugs in Prime Network Services Controller 3.0.2

Bug ID	Description
CSCuh42121	Upon rare occasions, after rebooting Prime Network Services Controller, you might see a UCSSH log file that indicates that the UCSSH process has stopped while waiting for user input. Prime Network Services Controller components and processes are not affected by this situation.
CSCuh74272	A port ID is not returned when the creation of a VM fails.
CSCui79010	DNS entries disappear after a Windows VM is migrated to the cloud. This problem occurs when a Windows VM is configured with a static IP address and then migrated to a cloud.
CSCuj03315	Users cannot log into the Prime Network Services Controller GUI after upgrading from a previous release or after rebooting Prime Network Services Controller.
CSCuj43151	After an InterCloud Switch upgrade, no InterCloud Switch undeploy or deploy events are issued and the known_hosts file is not updated. This problem occurs if the attach module command is issued on a cloud VSM and the related keys in the known_hosts file are not removed when the module is detached or deleted.
CSCuj61197	No error is issued if the number of cloud VMs exceeds the number of available licenses from Amazon Marketplace. The cloud VMs that can be licensed are instantiated, but no message is issued to indicate that not all requested cloud VMs were instantiated or that the license limit has been exceeded.
CSCuj65409	After upgrading an InterCloud link in standalone mode, the InterCloud Switch is changed and a static route to the InterCloud Switch is not added as expected.
CSCuj79213	The Prime Network Services Controller GUI intermittently displays the error: Communication with the server has failed. Try again. If it continues to fail, check the server status and log in again.
CSCuj81064	When creating an InterCloud link, if you do not check the Enable HA check box in the Configure InterCloud Link screen and instead continue to the Configure Network Properties screen before returning to the Configure InterCloud Link screen and checking the Enable HA check box, you cannot configure high availability on the link because the Configure Network Interfaces screen does not contain the fields for the secondary InterCloud extender and the Next button is disabled.
CSCum89284	VSG is missing some or all protected virtual machines (VMs) and thus dropping all traffic for those VMs.

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 3.0.2 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

See the [Cisco Prime Network Services Controller 3.0.2 Documentation Overview](#) for a list of Prime Network Services Controller guides.

Accessibility Features in Prime Network Services Controller 3.0.2

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/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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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.

© 2013, 2014 Cisco Systems, Inc. All rights reserved.

