Cisco Network Services Manager 5.0.2 Release Notes

December 6, 2012

These release notes contain the following sections:

- Overview, page 1
- System Requirements, page 3
- New Features and Enhancements, page 4
- Important Notes and Limitations, page 8
- Open Bugs, page 12
- Related Documentation, page 13
- Obtaining Documentation and Submitting a Service Request, page 13

Overview

Cisco Network Services Manager (Network Services Manager) is network management software that helps build the network services you need to securely create and deploy a cloud computing infrastructure. By using Network Services Manager, you can organize your network resources into a flexible cloud infrastructure that integrates the network with your existing IT tools and processes.

Table 1 describes Network Services Manager features.

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

Table 1 Network Services Manager Features

Feature	Description
Abstraction and virtualization	Network Services Manager virtualizes network services by abstracting a logical representation of the physical network that it manages. Logical topologies, ordered via the Network Services Manager API, are provisioned as data paths on the physical network devices. Network Services Manager offers an abstract API for configuring an entire virtual multi-tenant data center architecture. This abstraction reduces network operations costs and accelerates service delivery.
Policy implementation and adherence	Policies enforce topology models, network features, and network behaviors, thereby ensuring adherence to organizational or architectural requirements, such as security or access to resources.
Dynamic topology support	Network Services Manager can derive a data path to deploy the same logical topology on a variety of physical topologies. Network Services Manager evaluates the defined policies against the different physical topologies to determine how to configure the data path for the required services.
Automates end-to-end infrastructure as a service	Network Services Manager enables just-in-time service delivery models to automatically translate a topology request or *Network Container*, into an end-to-end network service topology, including the configuration of all associated routers, switches, firewalls, and other devices on the network.
Administration user interface (UI)	Network Services Manager provides a browser-based Administration UI that enables you to examine and modify properties of metamodel-instantiated resources.
Northbound (NB) Application Programming Interface (API)	The Network Services Manager NB API provides an integration interface for automated network provisioning as part of a larger cloud environment. The NB API enables you to instantiate cloud service models and topologies, create new cloud service offerings, modify existing offerings, and support containers and workloads. Additions, changes, or deletions made using the NB API are reflected in the Administration UI. Similarly, any changes made in the Administration UI are available via the NB API.

System Requirements

Table 2 identifies the physical hardware requirements for Network Services Manager 5.0.2.

Table 2 Physical Hardware Requirements

Item	Requirement
Hardware	Dual core CPU with 4 GB memory minimum (8 GB[1] recommended).
Software	VMware ESXi software with the vSphere client.
Availability	Expected to be part of a highly available management cluster within a data center.
Access	Provide console access to the OVA.

1. We recommend 8 GB memory if vCenter and other management VMs are running on the ESXi host.

Table 3 identifies the system requirements for the Network Services Manager engine and controller OVAs.

Table 3 System Requirements for Network Services Manager Software

Item	Requirement
Network Services Manager Engine Software	
Hardware	Dual core CPU
Disk space	40 GB
Memory	2 GB
Network Services Manager Controller Software	
Hardware	Dual core CPU
Disk space	40 GB
Memory	1 GB

Table 4 identifies the browser requirements for access to Network Services Manager via the Administration UI.

Table 4 Browser Requirements for Network Services Manager

Item	Requirement
Operating system	Microsoft Windows or Apple OSX
Browser	• Firefox 3.6 to 15 • Internet Explorer 7, 8, or 9

New Features and Enhancements

The following topics describe the new features, enhancements, and changes in Network Services Manager 5.0.2:

- New Features, page 4
- New and Enhanced Object Support, page 5
- Device Support, page 6
- User Interface, page 7
- New Script for Changing User Passwords, page 7
- Network Container Terminology Change, page 8

New Features

Table 5 describes the new features available in Network Services Manager 5.0.2.

Table 5 New Features in Network Services Manager 5.0.2

Feature	Description
Global address pools that are defined at the provider level and available to all tenants	• This support includes pools that are defined globally by the provider as publicly routable, and tenant-provided private address pools for use with their environment or routable across their MPLS cloud. • IP address reservation and ongoing pool management for any address pool via both the API and the browser-based UI.
Support for up to four pods in a Network Services Manager deployment	The pods can be uniquely defined for a Network Services Manager installation. Network Services Manager 5.0.2 includes the following pod types by default: • VMDC 2.1 Collapsed Compact Pod with Edge Routers and no Layer 2 Access Switches • VMDC 2.1 Collapsed Compact Pod with no Edge Routers and no Layer 2 Access Switches • VMDC 2.1 Compact Pod with Edge Routers • VMDC 2.1 Compact Pod with no Edge Routers
Service policies	Service policies define how traffic is allowed to flow from one part of the network (within a tenant network container) to another. Network Services Manager 5.0.2 provides the following types of service policies: • Firewall policies with one common firewall context per tenant • Load balancer policies with one context in each zone • Dynamic PAT policies • Static NAT policies with one-to-one translation • Static NAT policies with port redirection Service policies can be created and managed via both the API and the UI.
Support for multiple zones	Tenant network containers can support up to four zones.

Table 5 New Features in Network Services Manager 5.0.2 (continued)

Feature	Description
Task information	The Network Services Manager 5.0.2 NB API generates the following response types as part of the Task object: • Success—The requested operation was successfully provisioned and device configurations were updated. • Pending—The requested operation was successfully provisioned, but not all device configuration updates have completed. • Failure—The requested operation was successfully provisioned, but one or more device configurations failed to update. For failure responses, Network Services Manager returns a textual description of the encountered problem, which might or might not require manual intervention to correct. For example, an attempt to write the configuration to a device might fail due to a device temporarily not responding as opposed to the device being down. Network Services Manager responds to a temporary failure by retaining knowledge of the provisioned resources and continuing to retry the operation until the device configurations have been updated. It is the responsibility of the Northbound System to react to reported failures if manual intervention is required.
API Specification and Reference guide	*Cisco Network Services Manager 5.0.2 API Specification and Reference Guide* is available on cisco.com at http://www.cisco.com/en/US/products/ps11636/products_programming_reference_guides_list.html.

New and Enhanced Object Support

Table 6 identifies new and enhanced object support in Network Services Manager 5.0.2.

Table 6 New Object Support in Network Services Manager 5.0.2

Object	New Support
Pod	Ability to: • Allow or prevent Network Services Manager from configuring the device in the provider edge role. • Create and update the following based on four static pod topology definitions: – Device credentials – Uplink or downlink ports
Provider	New layer in the hierarchy that: • Maintains common address pools across all tenants. • Is a container for all other resources.

Table 6 New Object Support in Network Services Manager 5.0.2 (continued)

Object	New Support
Service Policy	New services for instantiation: • Load balancer • Firewall • Dynamic PAT • Static NAT one-to-one • Static NAT with port redirection
Tenant Network Container	Support for four zones.
External Network	• New object that allows a tenant to define remote networks that are reachable from the pod, including the Internet (0.0.0.0/0). • A collection of subnets that represent a Network Services Manager-unmanaged site that is accessible by a tenant.
External Network Connection	Support for MPLS and direct connections.
Zone	• Support for the following zone types: – Internet Edge – Secured Internet Edge – Private Edge – Secured Private Edge • Support for each of the above zone types with a load balancer. • Container for network segment objects.
Network Segment	• New object type that represents a VLAN to which virtual machines (VMs) can be attached. • Support for the following types of VLANs: – Nonroutable Layer 2 VLAN – Routable Layer 3 VLAN
IP Address Reservation	• IP address reservation via the Administration UI or API, thereby allowing: – Reservations for VM interfaces – VIPs for load balancing – Mapped addresses for NAT • IP address reservation in any pool, whether a global pool, a tenant private pool, or pools created per VLAN.

Device Support

Network Services Manager 5.0.2 includes the following new device support:

- Cisco ACE30 Application Control Engine Load Balancer Services Modules
- Cisco ACE20 Application Control Engine Load Balancer Services Modules

- Cisco Adaptive Security Appliance (ASA) Services Modules
- Cisco Catalyst 6500 Series Switches, in the Layer 3 Aggregation role
- Cisco Nexus 5500 Series Switches
- Cisco UCS 6200 Series Fabric Interconnects

For more information on Network Services Manager device and software version support, see *Cisco Network Services Manager 5.0.2 Supported Devices*.

User Interface

The Network Services Manager Administration UI includes the following new features:

- Enhanced metamodel support, including:
  - The ability to instantiate metamodels.
  - The ability to review, update and delete resources created via metamodel instantiation.
  - The ability to modify the metaproperties of metamodel-instantiated objects.
- An Active Network Topology Viewer that assists in troubleshooting activities by enabling you to quickly identify resource pairs, site contexts, and VLAN details.
- New icons in the toolbar for creating metamodels and reserving IP addresses.
- Updated icons representing resources in the Explorer View.
- Field-level enhancements for improved ease of use, such as tooltips or drop-down lists that replace fields requiring user entry.
- A Help button in the menu bar that opens the Network Services Manager online help.

New Script for Changing User Passwords

Network Services Manager 5.0.2 provides a new script for changing user passwords. The following procedure describes how to change user passwords using the new script.

We recommend that you change user passwords for security purposes.

The following conventions apply when changing user passwords:

- The password must contain at least eight characters.
- The password must contain characters from three of the following groups:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Special characters: ! “ ‘ # $ ` % & ( ) * + - . / : ; < = > ? @ \ ^ _ [ ] { } | ~) space

If your organization requires different password policy settings, review and edit the passwordpolicy.properties file on the engine in the following directory:

/usr/local/overdrive/engine/bin/UtilUpdateUserPassword

To change the password for the Network Services Manager Administration UI or API client account:

Step 1 Using the vSphere console, log into the Network Services Manager engine.

Step 2 Enter **shell** and, when prompted, the shell password.

Step 3 Enter the following command:

/usr/local/overdrive/engine/bin/updatepassword.sh *username old-password new-password*

where:

- *username* is **admin** for the Administration UI account, or **apiclient** for the API client account.
- *old-password* is the current account password.
- *new-password* is the new account password.

Note Some special characters must be preceded by a backslash (\). For example, a dollar sign must be preceded by a backslash as in the following example:
/usr/local/overdrive/engine/bin/updatepassword.sh admin *old-password* **NsMPas\$word3**

Step 4 Enter **exit**.

Step 5 Update the clients for the account with the new password, as follows:

- Administration UI account—Close any browser sessions that are logged into Network Services Manager using the old password, then log in again using the new password.
- API client account—Update any application that uses the apiclient account with the new password.

Network Container Terminology Change

Previous versions of Network Services Manager used the term *network container* to refer to certain objects. Beginning with 5.0.2, this term network container has been replaced by either *zone* or *network segment*, as follows:

- Zone—Logical collection of network components that share the same security profile.
- Network segment—Object representing a VLAN to which VMs can be attached.

This change applies to both the Administration UI and API.

Important Notes and Limitations

The following topics describe important notes and limitations associated with Network Services Manager 5.0.2:

- Service Policies, page 9
- Firewall Services Modules, page 10
- Cisco ASA Devices and ICMP, page 11
- Deleting Containers with VM Associated with Port Groups for Nexus 1000V Devices, page 11

- Established Connections Remain After Firewall Configuration Changes, page 11
- Redundant Device Configuration, page 12
- Naming Requirements for Containers, page 12

Service Policies

The following topics describe limitations associated with service policies:

- Source VLANs and Dynamic PAT Policies, page 9
- Load-Balancing Policies and Port Ranges, page 9
- Naming Convention for Service Policies, page 9

Source VLANs and Dynamic PAT Policies

If you use a source VLAN with a Dynamic Port Address Translation (PAT) policy set to ANY, and then attempt to initiate traffic to individual host addresses on the VLAN, the reverse traffic is subject to NAT, and Cisco Adaptive Security Appliance (ASA) Services Modules (SMs) issue messages similar to the following regarding NAT reverse path failures:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-111005: 127.0.1.50 end configuration: OK
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for icmp src
ba1ac877:65.0.0.10 dst 759ed2f9:192.168.240.36 (type 8, code 0) denied due to NAT reverse path failure
```

To enable access to hosts on the VLAN from outside the firewall, use static one-to-one NAT.

Load-Balancing Policies and Port Ranges

If you configure a load-balancing policy and specify a port range, Network Services Manager 5.0.2 uses only the first port in the range.

Naming Convention for Service Policies

We recommend that you use a naming convention for service policies so that they can be readily identified by type by subsequent API calls. The recommended naming format for service policy names is *type-servicename*. Examples of names for service policies using this format are lb-webservers and fw-public-vlan-to-protected-vlan.

Firewall Services Modules

The following topics describe limitations associated with firewall services modules:

- Firewall Services Modules and Connectionless Protocols, page 10
- Firewall Services Modules and Static NAT with Port Redirection, page 10
- Firewall Services Module Config Mode when Network Services Manager Applies a Configuration, page 10

Firewall Services Modules and Connectionless Protocols

To allow return traffic from firewall services modules when using connectionless protocols, such as ICMP, apply service policies in both directions for ICMP.

Return traffic for TCP and UDP connections are handled automatically by the firewall modules and do not require additional configuration with regard to service policies.

Firewall Services Modules and Static NAT with Port Redirection

Firewall services modules support only one IP address mapping for static Network Address Translation (NAT), whereas Network Services Manager 5.0.2 supports the mapping of multiple IP addresses to a single IP address for static NAT. As a result, if you configure multiple IP address mappings in Network Services Manager for a firewall services module, only the first mapping that is submitted will be functional on the device.

Firewall Services Module Config Mode when Network Services Manager Applies a Configuration

If Network Services Manager attempts to apply a configuration while you are logged into the firewall services module in config mode, an error similar to the following is displayed in the controller log:

```
nsm1-c2-controller 2012-12-27 192:168:11,321 [pool thread 5]-ERROR FirewallService -
/ROOT/Service Provider - 1/Tenant - 1/default(71ad6ed041bb465494fa8a730a9322a3) apply failed: Multiple logins
on Firewall in config mode. Exit from config mode from other sessions before applying policy from NSM.
/ROOT/Service Provider - 1/Tenant - 1/default net.linesider.overdrive.device.firewall.FirewallException:
Multiple logins on Firewall in config mode. Exit from config mode from other sessions before applying policy
from NSM. \
/ROOT/Service Provider - 1/Tenant - 1/default at
net.linesider.overdrive.cisco.device.CiscoFWSMContext.handleDeviceException(CiscoFWSMContext.java:277) at
net.linesider.overdrive.cisco.device.CiscoFWSMContext.getAllAclIds(CiscoFWSMContext.java:595) at
net.linesider.overdrive.cisco.device.CiscoFWSMContext.getContextAclRules(CiscoFWSMContext.java:551) at
net.linesider.overdrive.cisco.device.FWSMAccessControl.getRules(FWSMAccessControl.java:53) at
net.linesider.overdrive.agent.firewall.PeerPolicyManager.<init>(PeerPolicyManager.java:44) at
net.linesider.overdrive.agent.firewall.PeerPolicyManager.create(PeerPolicyManager.java:31) at
net.linesider.overdrive.agent.firewall.FirewallService$DeviceConfig.applyPolicyChange
(FirewithOutcome.java:223)
```

In subsequent controller retries, the device context is configured correctly without user intervention.

Cisco ASA Devices and ICMP

If your device stack includes Cisco ASA devices, ICMP, as a stateless protocol, fails between zones. To avoid this situation, include the following lines in the Cisco ASA device configuration, or use a configuration boilerplate that includes these lines:

```
policy-map global_policy
 class inspection_default
inspect icmp
```

Deleting Containers with VM Associated with Port Groups for Nexus 1000V Devices

In Network Services Manager, if you delete a container with deployed VMs that are associated with port groups in VMware, the port profile is not completely removed by the Cisco Nexus 1000V (Nexus 1000V) device.

To ensure that the port profile is fully removed after you delete it in Network Services Manager:

Step 1 In the VMware vSphere client, detach the VM network interface cards (NICs) from the port groups created by the Nexus 1000V.

Step 2 Using the Nexus 1000V CLI, confirm that the port profile has been removed.

Established Connections Remain After Firewall Configuration Changes

If you remove or change a configured firewall TCP port, a connection established on the original port remains operational even though the original port is no longer allowed on the firewall.

This situation occurs as follows:

1. In Network Services Manager, configure a provider with a device stack, tenant, tenant network container, zones, VLANs, external network, and external network connections.
2. Create a firewall between two zones with TCP ports 22 and 80.
3. Via SSH, connect the two VMs on port 22.
4. Edit the firewall by removing port 22 or changing it to a different number.
5. Save the configuration.

The connection remains up even though the firewall no longer allows port 22.

You can remove these connections by doing either of the following:

- Reboot the VM hosts that participate in the firewall policy.
- Terminate the connections on the VM hosts that participate in the policy.

Redundant Device Configuration

Network Services Manager expects redundant pairs by design, with the following effects:

- If a device stack contains only one firewall or load balancer, Network Services Manager does not provision the available device.
- If one device in a redundant pair becomes unavailable, and a provisioning request arrives while the primary device is reloading, the request fails and no further provisioning occurs until both devices are restored.

Naming Requirements for Containers

Names for subordinate containers must be unique within the parent container in Network Services Manager. For example, you cannot use duplicate zone names within a tenant network container.

Open Bugs

The open bugs for Network Services Manager 5.0.2 are available in the Cisco Bug Toolkit. The Cisco Bug Toolkit enables you to search for a bug by identifier or product and version, and can provide additional details about the bug, such as more information or that the bug has been fixed.

Table 7 identifies the bugs that are open in the Network Services Manager 5.0.2 release.

Table 7 Open Bugs in Network Services Manager 5.0.2

Bug ID	Symptom
CSCtq81843	Accessing Cisco Network Services Manager NB API using the arbitrary HTTP URL returns: 200 OK
CSCub51123	Metamodel Instantiation Fails: Failed to instantiate Metamodel
CSCuc16437	Service policies are not provisioned if an external network connection (ENC) is created after the policies are created
CSCuc46596	Configurations are orphaned on devices if a PoD is deleted before provisioned Service Policies
CSCuc71435	When adding a policy, the IP address is not validated against the zone or IP address pool
CSCuc90536	Cannot update the names of Explicit and Layer 2 VLANs, and they fail with the following message: `Save failed. Invalid value for "mask". Cause: must specify valid mask when using an address pool`
CSCuc96218	While adding a VLAN, this message is received: `Failed to instantiate Metamodel Com.pfn.wirepower.common.exception.ProvisioninException: error.invalidsettingcom.pfn.wirepower.common.exception.ProvisioningException: error.invalidsetting`

Table 7 Open Bugs in Network Services Manager 5.0.2 (continued)

Bug ID	Symptom

CSCud03439	Alerts tab displays an alert like this:
	`Problem with Device : [/ROOT/Provider-1/OD-C2-PoD/OD-C2-PoD/UCSM]`
	`Problem is :[[SwitchProblem message='Failed to create vlans from device (Command 'create vlan test-(paren-2016 2016' failed:`
	`create vlan test-(paren-2016 2016`
	`^`
	`% Invalid Value at '^' marker, accepted value is: WORD (Disallowed character ()`
	`od-c2-ucs-A /eth-uplink #) UCSM' ,type=null, device=UCSM(874dc79ec2a54f93be01a4e4438de4db)]]`
	`Date is : Mon Nov 19 2012 07:41:14 GMT-0500 (Eastern Standard Time)]`

CSCud05311	Model has two Service Providers defined.
CSCud32265	TaskInfo for a request to create a network segment remains in failure status even after correcting the root cause of the failure such that a success status is expected.

Related Documentation

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

The following documents are available for Cisco Network Services Manager 5.0.2:

- *Cisco Network Services Manager 5.0 Quick Start Guide*
- *Cisco Network Services Manager 5.0.2 Release Notes*
- *Cisco Network Services Manager 5.0 User Guide*
- *Cisco Network Services Manager 5.0.2 API Specification and Reference Guide*
- *Open Source Used in Cisco Network Services Manager 5.0.2*
- *Supported Devices for Cisco Network Services Manager 5.0.2*
- *Cisco Network Services Manager 5.0.2 Technical Reference*

Obtaining Documentation and Submitting a Service Request

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

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

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