Cisco Virtual Network Management Center 2.0 Release Notes

August 21, 2012

This document describes the features, bugs, and limitations for the Cisco Virtual Network Management Center (VNMC) 2.0 release.

Use this document in combination with the documents listed in the "Related Documentation" section on page 13.

Contents

This document includes the following sections:

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

Introduction

VNMC is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco virtual services. Designed for multiple-tenant operation, VNMC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. With both a built-in UI and an XML API, VNMC enables centralized management of Cisco virtual services by an administrator or through an API.

VNMC is built on an information model-driven architecture in which each managed device is represented by its subcomponents (or *objects*), which are parametrically defined. This model-centric approach enables VNMC to provide a secure, multiple-tenant virtualized infrastructure with Cisco Adaptive Security Appliance 1000V (ASA 1000V) and Cisco Virtual Security Gateway (VSG) virtual services.

Table 1 describes the primary features of VNMC.

Table 1 VNMC 2.0 Features

Feature	Description
Multiple-Device Management	All ASA 1000Vs and VSGs are centrally managed, thereby simplifying provisioning and troubleshooting in a scaled-out data center. By using device profiles with their specified device configuration policies, you can deploy consistent policies to one or more profile-managed resources.
Security Profile	Security profiles enable you to represent a security policy configuration in a profile that: • Simplifies provisioning • Reduces administrative errors during security policy changes • Reduces audit complexities • Enables a highly scaled-out data center environment
Stateless Device Provisioning	The management agents in VSG and ASA 1000V are stateless, receiving information from VNMC and thereby enhancing scalability.
Security Policy Management	Security policies are authored, edited, and provisioned for all VSGs and ASA 1000Vs in a data center, which simplifies the operation and management of security policies, and ensures that the required security is accurately represented in the associated security policies.
Context-Aware Security Policies	VNMC interacts with VMware vCenter to create virtual machine (VM) contexts that enable you to institute highly specific policy controls across the entire virtual infrastructure.
Dynamic Security Policy and Zone Provisioning	VNMC interacts with the Cisco Nexus 1000V VSM to bind the security profile with the corresponding Cisco Nexus 1000V Series switch port profile. When VMs are dynamically instantiated and applied to appropriate port profiles, their association to trust zones is also established.
Multi-Tenant Management	VNMC can manage compute and edge firewall security policies in a dense multi-tenant environment, so that you can rapidly add or delete tenants, and update tenant-specific configurations and security policies. This feature significantly reduces administrative errors, ensures segregation of duties within the administrative team, and simplifies audit procedures.

Table 1 VNMC 2.0 Features (continued)

Feature	Description
Role-Based Access Control	Role-Based Access Control (RBAC) simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures. With RBAC, organizations can reduce administrative errors and simultaneously simplify auditing requirements. VNMC supports local and remote authentication with RBAC.
XML-Based API	The VNMC XML application programming interface (API) allows external system management and orchestration tools to programmatically provision VSGs and ASA 1000Vs, and provides transparent and scalable operation management.

System Requirements

Table 2 identifies VNMC system requirements.

Table 2 VNMC System Requirements

Requirement	Description
Virtual Appliance	
One virtual CPU	1.5 GHz
Memory	3 GB RAM
Disk space	25 GB on a shared network file storage (NFS) or a storage area network (SAN) if VNMC is deployed in a high availability (HA) cluster
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 4.1 or 5.0 with VMware ESX or ESXi (American English)
VMware vCenter	Release 4.1 or 5.0 (American English)
Interfaces and Protocols	
HTTP/HTTPS	—
Lightweight Directory Access Protocol (LDAP)	—
Ports	
If the VNMC server is protected by a firewall, the following ports must be enabled.	
80	HTTP
443	HTTPS
843	Adobe Flash
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS

Table 2 VNMC System Requirements (continued)

Requirement	Description
Web-Based UI Client	
Operating System	Either of the following: • Windows • Apple Mac OS
Browser	Any of the following: • Internet Explorer 9.0 • Mozilla Firefox 11.0[1] • Chrome 18.0[2]
Flash Player	• For Internet Explorer and Mozilla Firefox, the supported Adobe Flash Player plugin version is 11.2. • For Chrome, the supported Adobe Flash Player plugin version is 11.3.300.265.

1. We recommend Mozilla Firefox 11.0 with Adobe Flash Player 11.2.
2. You must disable Pepper Flash in Chrome before using Chrome with VNMC 2.0. For more information, see Configuring Chrome for Use with VNMC, page 4.

Configuring Chrome for Use with VNMC

To use Chrome with VNMC 2.0, you must disable the default 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.

To disable default Adobe flash players in Chrome:

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

Step 2 Click **Details**.

Step 3 Locate the Flash player plugins, and disable each one.

Step 4 Download and install Adobe Flash player version 11.3.300.265.

Step 5 Close and reopen Chrome before logging into VNMC 2.0.

Performance and Scalability

Table 3 lists the performance and scalability data for VNMC 2.0.

Table 3 VNMC 2.0 Performance and Scalability

Item	Scalability Numbers
ASA 1000Vs and VSGs	128
Hypervisors	600
Locales	128
Orgs	2048
Policies	2048
Policy Sets	2048
Rules	8192
Security Profiles	2048
Tenants	128
Users	128
VMs	5000
Zones	8192

NTP Requirements for Deploying and Operating VNMC

You must do the following for proper VNMC operation with VMware, ASA 1000V, VSG, and VSM:

1. Before you deploy the VNMC OVA, configure Network Time Protocol (NTP) servers on all ESX and ESXi servers that run VNMC, ASA 1000V, VSG, and VSM to ensure proper operation. For information, see *Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client* at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2012069.
2. Before you perform any operation on VNMC after you deploy the OVA, configure NTP servers for VNMC, ASA 1000V, VSG, and VSM. If you do not do so, ASA 1000Vs, VSGs, and VSMs will not be able to register with VNMC. See Configuring NTP, page 5.

Configuring NTP

Before you perform any operation in VNMC, configure NTP on ASA 1000V, VSG, and VSM. If you do not do so, ASA 1000Vs, VSGs, and VSMs will not be able to register with VNMC.

To configure NTP in VNMC, ASA 1000V, VSG, and VSM:

1. Configuring NTP in VSM, page 6
2. Configuring NTP in VSG, page 6
3. Configuring NTP in ASA 1000V, page 6
4. Configuring NTP in VNMC, page 6

Configuring NTP in VSM

To configure NTP, enter the following CLI command from the VSM console:

ntp server *x.x.x.x*

where *x.x.x.x* is the NTP server IP address.

Configuring NTP in VSG

To configure NTP, enter the following CLI command from the VSG console:

ntp server *x.x.x.x*

where *x.x.x.x* is the NTP server IP address.

Note The **ntp server** command will not be available in the VSG console if you have installed the VNMC policy agent. To configure NTP in VSG, you must uninstall the VNMC policy agent.

Configuring NTP in ASA 1000V

Before you install ASA 1000V in VNMC, ensure that you have configured NTP on all ESX and ESXi servers that run ASA 1000V. For information, see *Configuring Network Time Protocol (NTP) on ESX/ESXi 4.1 and ESXi 5.0 hosts using the vSphere Client* at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2012069.

After installation, ASA 1000V receives the Real Time Clock (RTC) value from the VMware ESX or ESXi host.

Configuring NTP in VNMC

To synchronize VNMC with the NTP Server:

Step 1 In your browser, enter **https://***vnmc-ip* where *vnmc-ip* is the VNMC IP address.

Step 2 If you receive a certificate warning, choose to continue to the VNMC login window.

Step 3 In the VNMC login window, enter the username **admin** and the admin user password.

Step 4 From the VNMC GUI, to set the time zone:

a. Choose **Administration > VNMC Profile > root > VNMC Profile > default.**

b. In the General tab, select the time zone.

c. Click **Save**.

Step 5 From the VNMC GUI, to add an external NTP server as time source:

a. Choose **Administration > VNMC Profile > root > VNMC Profile > default.**

b. In the Policy tab, select **Add NTP Server**.

c. Enter the hostname or IP Address and click **OK**.

d. Click **Save**.

Caution We recommend that you do not set the time zone after you add the NTP server.

New Features in VNMC 2.0

The following sections describe the new features introduced in this VNMC 2.0 release:

For more information about these features, see the VNMC documentation, available on cisco.com at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html.

Cisco ASA 1000V Management

VNMC 2.0 adds support for ASA 1000V instances, enabling you to:

- Add and configure edge firewalls.
- Configure AAA and syslog device policies.
- Configure the following service policies:
  - ACL
  - Connection timeout
  - DHCP
  - IP audit
  - NAT and PAT
  - Packet inspection
  - Routing
  - TCP intercept
  - VPN

- Create and apply edge device profiles that contain the following policies:
  - DHCP
  - IP audit signature
  - Routing
  - VPN
- Create and apply edge security profiles that contain the following policies or policy sets:
  - ACL policy sets (ingress and egress)
  - Connection timeout
  - IP audit
  - NAT policy sets
  - Packet inspection
  - TCP intercept
  - VPN interface policy sets
- Apply profiles to edge firewalls, edge firewall interfaces, and port profiles (by using the VSM CLI).

Support for ASA 1000V in HA Configurations

VNMC 2.0 supports virtual ASA 1000V instances in high availability (HA) configurations by verifying that the HA role and mode match. The supported HA configurations are those that result from pool associations, in which a logical edge firewall is assigned to a pool of firewall instances.

VNMC supports virtual ASA 1000V instances in HA configurations by:

- Enabling you to specify the HA mode (either HA or Standalone) when you add an edge firewall to VNMC.
- Detecting HA mode and role changes in the HA configurations and acting on those changes as follows:
  - If an edge firewall HA mode changes, and the edge firewall is assigned to a pool but not yet associated, VNMC examines the resource pool for a matching resource. A matching resource must match the edge firewall HA mode and the virtual ASA 1000V instance HA role.
  - If the HA role of a virtual ASA 1000V instance changes, VNMC triggers reassociation for the logical edge firewall and looks for a match between the edge firewall HA mode and the virtual ASA 1000V instance HA role.

    This behavior occurs under the following conditions:

    —The ASA 1000V instance is in a pool.

    —The pool is assigned to a logical edge firewall.

    —No matching resources for the edge firewall were available before the HA role change.

Note VNMC does not verify that the HA role and mode match if a virtual ASA 1000V instance is directly associated with a logical edge firewall.

Site-to-Site VPNs

VNMC 2.0 adds support for site-to-site IPSec VPNs, enabling you to:

- Create and configure the following policies and policy sets:
  - Crypto map
  - IKE
  - IPSec
  - Peer authentication
  - VPN device
- Create interface policy sets that include the policies you specify.
- Include interface policy sets in edge profiles.
- Apply interface policy sets to edge firewall interfaces via the edge profiles.

NTP Support

VNMC enables you to configure NTP for compute firewalls, edge firewalls, and VNMC itself. You can configure three or more NTP servers for VNMC.

The default time zone value for the VNMC profile is UTC, and is selected in the UI when VNMC starts.

Security Policy View

VNMC enables you to verify and examine the resolved policies that have been applied to compute and edge firewalls. With this feature, you can:

- Verify the active policies for compute and edge firewalls.
- Examine the policies at a detailed level.
- Create, modify, and delete related policy objects.

Policy Administrative Status

VNMC allows you to enable or disable the administrative status for the following types of policies:

- AAA authentication
- Connection timeout
- Crypto map
- Interface policy set
- IP audit
- NAT
- NAT policy set
- Packet inspection

- Syslog (buffer)
- TCP intercept

Fault Detail View

The VNMC interface provides links to browser windows that enable you to:

- Examine the policy and configuration errors that prevent the successful application of a policy.
- Review the faults and events associated with successfully applied policies and configurations.
- Examine the faults associated with compute and edge firewalls.

ASDM Cross-Launch from VNMC

VNMC 2.0 enables you to launch the Cisco Adaptive Security Device Manager (ASDM) GUI from the UI.

After you deploy a virtual ASA 1000V instance and register the ASA 1000V instance to VNMC, you only need to navigate to the virtual ASA 1000V instance and click **Launch ASDM** for the ASDM GUI to open in a separate window.

System Enhancements

In addition to system upgrades, VNMC 2.0 provides system backup and restore operations.

User Interface Enhancements and Changes

The following topics describe new and changed features in the VNMC 2.0 UI:

- Policy Management Profiles and Policies, page 10
- Field Aids, page 11
- Event Log Option Removed, page 12

Policy Management Profiles and Policies

The following changes have been implemented in the VNMC interface to improve ease-of-use:

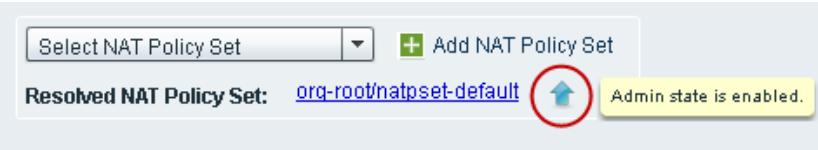
- Policy Management:
  - DHCP and Routing policies, previously under Device Configuration, are now under Service Policies.
  - A new Service Profiles tab holds all service profiles.
  - A new Service Policies tab holds all service policies.
- In Resource Management, Security Profile is now Compute Security Profile.

Field Aids

The VNMC interface includes the following new field aids:

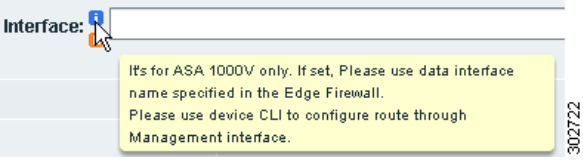
- An arrow indicates whether the administrative status of a policy is enabled or disabled, as shown in Figure 1.

Figure 1 Administrative Status Indicator



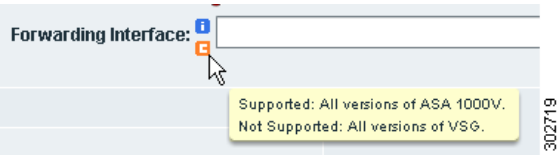
- An "i" icon provides additional information about a field, as shown in Figure 2.

Figure 2 Information Icon



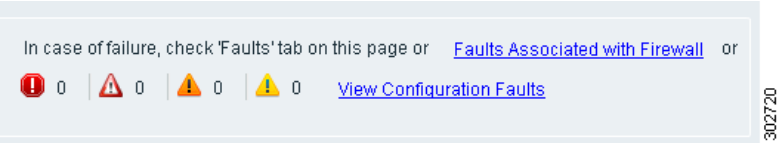
- A "c" icon identifies product compatibility for the field, as shown in Figure 3.

Figure 3 Compatibility Icon



- Fault icons provide current fault status, and links provide quick access to fault information, as shown in Figure 4.

Figure 4 Fault Information and Links



Event Log Option Removed

The Event Log option has been removed from the following locations in the UI:

- Resource Management > Diagnostics
- Policy Management > Diagnostics
- Administration > Diagnostics

Limitations

The following topics describe the limitations in VNMC 2.0:

VNMC VM Manager and VMware vCenter Server Connections

VNMC VM Manager automatically connects to the VMware vCenter server on HTTP port 80. A vCenter extension file is required to establish a connection between VM Manager and vCenter. The extension file is exported from VNMC and linked on the VM Managers tab. You install it as a plugin on all vCenter servers to which you want to connect.

For more information on installing and registering the vCenter extension file, see the *Cisco Virtual Network Management Center 2.0 GUI Configuration Guide*.

Upgrading vCenter to a New Version

If you upgrade vCenter to a new version and use the same IP address, vCenter attributes are not updated in VNMC. For example, the vCenter attributes for VMs and hosts on the upgraded vCenter are not updated.

To resolve this issue, add the vCenter to VNMC again by choosing **Resource Management > Resources > Virtual Machines > VM Managers** and clicking **Add VM Manager**.

Characters in Names Retrieved from vCenter

If you choose **Resource Management > Resources > Virtual Machines**, the following characters are not allowed in names that are retrieved from vCenter:

" ' ^ & ` < > ? = \ "

If a name that is retrieved from vCenter contains any of these characters, VNMC does not recognize the characters.

Names that can be affected include:

- VM name
- VM DNS name

- VM parent application name
- VM resource pool name
- Hypervisor cluster name

As a result of this behavior, VNMC attribute names do not display correctly in the UI and might be evaluated differently when these attributes are used in policy conditions.

Value Displayed in Parent App or Resource Pool Field

The VM Properties pane displays Parent App and Resource Pool fields, but only one field contains a value at any time. For example, if the parent application name is displayed, the resource pool name is not displayed. This situation occurs because a VM can be part of a parent application or part of a resource pool, but not both simultaneously.

You can view the VM Properties pane by choosing **Resource Management > Resources > Virtual Machines > VM Managers >** *vm-manager* **>** *host-ip-address* **>** *vm* where:

- *vm-manager* is a vCenter.
- *host-ip-address* is the ESX/ESXi host IP address in dotted-decimal format (*x.x.x.x*)
- *vm* is a specific VM.

Open Bugs

The open bugs for VNMC 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 4 identifies the bugs that are open in the VNMC 2.0 release.

Table 4 Open Bugs in VNMC 2.0

Bug ID	Summary
CSCub52030	ASA 1000V or VSG goes to config failed state due to policy errors after config push. Device fault links on right panel are missing. Or, if available, fault window presents empty screen.
CSCub59679	If you change the default syslog policy, it is not immediately propagated to the ASA 1000V.

Related Documentation

The following topics contain information about the documentation available for VNMC and related products:

- Cisco Virtual Network Management Center Documentation, page 14
- Cisco ASA 1000V Documentation, page 14
- Cisco Virtual Security Gateway Documentation, page 14
- Cisco Nexus 1000V Series Switch Documentation, page 14

Cisco Virtual Network Management Center Documentation

The following VNMC documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- *Cisco Virtual Network Management Center 2.0 Documentation Overview*
- *Cisco Virtual Network Management Center 2.0 Release Notes*
- *Cisco Virtual Network Management Center 2.0 Quick Start Guide*
- *Cisco Virtual Network Management Center 2.0 CLI Configuration Guide*
- *Cisco Virtual Network Management Center 2.0 GUI Configuration Guide*
- *Cisco Virtual Network Management Center 2.0 XML API Reference Guide*
- *Open Source Used in Cisco Virtual Network Management Center 2.0*

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

Cisco Virtual Security Gateway Documentation

The Cisco VSG documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

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, at:

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.

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