Cisco Virtual Network Management Center 2.1 Release Notes

June 3, 2013

This document describes the features, bugs, and limitations for the Cisco Virtual Network Management Center (VNMC) 2.1 release.

Use this document in combination with the documents listed in the "Related Documentation" section on page 10.

Contents

This document includes the following sections:

New and Changed Information

Table 1 describes information that has been added or changed since the initial release of this document.

Cisco Systems, Inc.
www.cisco.com

Table 1 New and Changed Information

Date	Revision	Location
February 12, 2014	Updated disk and space requirements. Only one disk with 20GB or more disk space can be used.	System Requirements, page 3

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 2 describes the primary features of VNMC.

Table 2 VNMC 2.1 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.

Table 2 VNMC 2.1 Features (continued)

Feature	Description
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.
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 3 identifies VNMC system requirements.

Table 3 VNMC System Requirements

Requirement	Description
Virtual Appliance	
Two virtual CPUs	1.5 GHz
Memory	3 GB RAM
Disk space	20 GB on a single disk **Note** If VNMC is deployed in a high availability (HA) cluster, the disk may be configured on a shared disk (provisioned using SAN or NFS).
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 (LDAP)	—
Ports	
If the VNMC server is protected by a firewall, the following ports must be enabled.	
80	HTTP

Table 3 VNMC System Requirements (continued)

Requirement	Description
443	HTTPS
843	Adobe Flash
Intel VT	
Intel Virtualization Technology (VT)	Enabled in the BIOS
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 20.0[1] • Chrome 26.0[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 20.0 with Adobe Flash Player 11.2.
2. Before you can use Chrome with VNMC 2.1, you must first disable the Adobe Flash Players that are installed by default with Chrome. For more information, see Configuring Chrome for Use with VNMC, page 4.

Hypervisor Requirements

VNMC is a multi-hypervisor virtual appliance that could be deployed on either VMware vSphere or Microsoft Hyper-V Server 2012 (Hyper-V Hypervisor). See the VMware Compatibility Guide to verify thatVMware supports your hardware platform. See the Windows Server Catalog to verify that Microsoft Hyper-V supports your hardware platform.

Requirement	Description
VMware	
VMware vSphere	Release 4.1, 5.0, or 5.1 with VMware ESXi (English Only)
VMware vCenter	Release 4.1 or 5.0 (English Only)
Microsoft	
Server	Microsoft Windows Server 2012 with Hyper-V (Standard or Data Center)
SCVMM	Microsoft SCVMM 2012 SP1 or later

Configuring Chrome for Use with VNMC

To use Chrome with VNMC 2.1, 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 2.1.

Performance and Scalability

Table 4 lists the performance and scalability data for VNMC 2.1.

Table 4 VNMC 2.1 Performance and Scalability

Item	Scalability Numbers
ASA 1000Vs and VSGs	256
Hypervisors	600
Locales	128
Object Group	65536
Orgs	2048
Policies	4096
Policy Sets	2048
Rules	16384
Security Profiles	2048
Tenants	128
Users	128
Managed 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 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 6.

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 7

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 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 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 2.1

The following sections describe the new features introduced in the VNMC 2.1 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.

Microsoft Hyper-V Support

VNMC can be installed on the VMWare Provisory and the Microsoft Hyper-V Hypervisor. The following are some of the VNMC features that are not supported when VNMC is installed on Hyper-V Hypervisor.

When you are adding a rule to create the ACL policy:

- The option to match any one rule is disabled. The only available option is to match all the rules.
- The service condition is disabled.
- When you are setting source or destination conditions, the VM attribute type is not supported.

When you are adding an object group:

- When the attribute type is Network, the attribute name Service is not supported.
- The VM attribute type is not supported.

When you are working with vZones, the option to match any one rule is disabled. The vZone must match all the conditions.

Clone

You can create a clone for an organization, policy, or policy set at a VNMC destination of your choice. The hierarchy of an organization's clone and the names of the elements in it cannot be changed. Once created, a clone cannot be renamed or moved to another location.

Search

You can search for instances of organizations in VNMC using the search tab in the policy management, tenant management, and resource management tabs.

When you enter an organization name as a pattern or a regular expression in the search text box, the search result is displayed. From the search result, you can expand the organization's hierarchy and launch devices and polices in that organization.

Condition Match Criterion in vZone

You can now choose a condition match criterion when you add a vZone. This option enables you to choose all conditions or any one condition to be applied on the vZone.

Service Attribute in Object Group

You can group different types of objects within the same field; for example, you can group port and protocols. The service attribute in the ACL rule enables you to configure protocol and destination port in a single condition.

Limitations

The following topics describe the limitations in VNMC 2.1:

SSH Vulnerability

VNMC 2.1 SSH service has multiple vulnerabilities. For more information, see OpenSSH Security at http://www.openssh.com/security.html.

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 2.1 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 ESXi host IP address in dotted-decimal format (*x.x.x.x*)

- *vm* is a specific VM.

Searching for Organization Names

If an organization name contains special characters, it will not be searchable.

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 5 identifies the bugs that are open in the VNMC 2.1 release.

Table 5 Open Bugs in VNMC 2.1

Bug ID	Summary
CSCug92883	After VNMC 2.1 is installed on Hyper-V Hypervisor for the first time, it takes a long time to start up initially.
CSCud36833	VNMC 2.1 displays obsolete information in the Compute Security Profile window.
CSCuf38328	In VNMC 2.1, when multiple vCenters are added or deleted in VM Manager, you will need to log out and log in again to see the refreshed data.
CSCue66204	When more than 512 Policy Object groups are added for a tenant in VNMC 2.1, the API does not respond with an error. However, the GUI displays an error message stating that the maximum capacity is exceeded. This results in the creation of incorrect policy objects.
CSCtt12629	User access control in VNMC 2.1 is not entirely multi-tenant capable.
CSCuf61693	When a secure VM is deployed, the VNMC 2.1 GUI takes an hour to display the VM.

Related Documentation

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

- Cisco Virtual Network Management Center Documentation, page 10
- Cisco ASA 1000V Documentation, page 11
- Cisco Virtual Security Gateway Documentation, page 11
- Cisco Nexus 1000V Series Switch Documentation, page 11

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 2.1 Documentation Overview*
- *Cisco Virtual Network Management Center 2.1 Release Notes*
- *Cisco Virtual Network Management Center 2.1 Quick Start Guide*
- *Cisco Virtual Network Management Center 2.1 CLI Configuration Guide*
- *Cisco Virtual Network Management Center 2.1 GUI Configuration Guide*
- *Cisco Virtual Network Management Center 2.1 XML API Reference Guide*
- *Open Source Used in Cisco Virtual Network Management Center 2.1*

Cisco ASA 1000V Documentation

The Cisco Adaptive Security Appliance (ASA) 1000V 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 *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.