Release Notes for Cisco Virtual Network Management Center, Release 1.3

Revised: May 14, 2012
OL-26568-03

This document describes the features, caveats, and limitations for Cisco Virtual Network Management Center. Use this document in combination with the documents listed in Related Documentation, page 7.

Note Release notes are sometimes updated with new information about restrictions and caveats. For the most recent version of the *Release Notes for Cisco Virtual Network Management Center, Release 1.3*, see http://www.cisco.com/go/techdocs.

Table 1 shows the online change history for this document.

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-25868-03	2	May 14, 2012	Added Bug ID CSCtz01525 to Table 3 on page 6.
OL-25868-02	1	May 1, 2012	Added Bug ID CSCtx67252 to Table 3 on page 6.
OL-26568-01	--	January 31, 2012	Created release notes for Cisco Virtual Network Management Center, Release 1.3.

Contents

This document includes the following sections:

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

Introduction

The Cisco Virtual Network Management Center (Cisco VNMC) is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco Virtual Security Gateways (Cisco VSGs) for the Cisco Nexus 1000V Series switch. Designed for multi-tenant operation, the Cisco VNMC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. With built-in GUI, CLI, and XML APIs, the Cisco VNMC allows you to manage Cisco VSGs that are deployed throughout the data center from a centralized location. The Cisco VNMC is built on the information model-driven architecture where each managed device is represented by its sub-components (or objects) that are parametrically defined. This model-centric approach enables a flexible and simple mechanism to securing virtualized infrastructure with Cisco VSG.

System Requirements

Cisco VNMC has the following system requirements:

- Cisco VNMC Virtual Appliance:
  - 1 virtual CPU at 1.5-GHz
  - 3-GB RAM (required for Cisco VNMC ISO installation)
  - 25-Gb hard disk (vDisk)
  - 1 management network interface
- Hypervisor and Hypervisor Manager:
  - VMware vSphere 4.1.0 or 5.0 releases with VMware ESX or ESXi
  - VMware vCenter 5.0 releases. (4.1 VMware supports only 4.1 host)
- Interfaces and Protocols—HTTP/HTTPS, Lightweight Directory Access Protocol (LDAP)
- Web-based GUI client:
  - Adobe Flash Player 10.1 or later version
  - Access to Cisco VNMC using a Web browser and the following ports. If the deployment uses a firewall, make sure to permit the following ports:

    - 443 (HTTP)

    - 80 (HTTP/TCP)

    - 843 (TCP)

– Operating System—See Table 2 for support.

Table 2 Operating System Support Matrix for Client Device Cisco VNMC GUI

Operating System	Internet Explorer 7.x and 8.x	Firefox 8.x
Windows	Supported	Supported
Apple MAC OS	X	X
Linux	X	X

Software Features

This section briefly describes the important features of the Cisco VNMC Release 1.2 and Release 1.3 for the Cisco Nexus 1000V switch and the Cisco Virtual Security Gateway.

This section includes the following topics:

Multi-Device Management

All Cisco VSG devices are centrally managed, which simplifies provisioning and troubleshooting in a scaled-out data center. In addition, the device profile object specifies device configuration policies that you can apply to one or more firewall profile managed resources.

Security Profile

A security profile enables you to represent the Cisco VSG security policy configuration in a profile, which simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and enables a highly scaled-out data center environment.

Stateless Device Provisioning

The stateless configuration model is enabled with a management agent that is embedded with Cisco VSGs, that allows the Cisco VNMC to be a highly scalable device provisioning model.

Security Policy Management

Security policies are authored, edited and provisioned for all Cisco VSGs in a data center, which simplifies the operation and management of security policies as well as ensures that the security requirements are accurately represented in the associated security policies.

Context-Aware Security Policies

The Cisco VNMC interacts with VMware vCenter to obtain VM contexts that you can leverage to institute granular policy controls across their virtual infrastructure.

Dynamic Security Policy and Zone Provisioning

The Cisco VNMC interacts with the Cisco Nexus 1000V Series switch 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

The Cisco VNMC can manage Cisco VSGs and 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 are able to reduce administrative errors and simultaneously simplify auditing requirements. The Cisco VNMC supports local and remote authentication with RBAC.

XML-Based API

The Cisco VNMC full-featured XML API allows external system management and orchestration tools to programmatically provision Cisco VSGs and provide seamless and scalable operational management.

New and Changed Information

Cisco VNMC 1.3 includes vSphere 5.0 support for the Cisco VSG.

Limitations

The following topics describe the limitations in Cisco VNMC Release 1.3 for the Cisco Nexus 1000v switch and the Cisco Virtual Security Gateway:

Cisco VNMC VM Manager and VMware vCenter Server Connections

Cisco 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 Cisco VNMC and linked on the VM Managers tab. You install it as a plugin on all the vCenter servers to which you want to connect.

Characters in Names Fetched from the vCenter

In the Resource Management > Resources > Virtual Machines area, the following set of characters are not allowed in names that are fetched from the vCenter:

", ', ^, &, `, <, >, ?, =, \, "

If any name attribute that is fetched from the vCenter, such as the following name attributes, contains the preceding characters, Cisco VNMC will not recognize the characters:

- VM name
- VM DNS name
- Parent Application name property of VM
- Resource Pool name property of VM
- Cluster name property of Hypervisor

As a result, the VNMC attribute names will not display correctly on the GUI and may also be evaluated differently when these attributes are used in policy conditions.

Value Displayed in Parent Application or Resource Pool Fields

In the Resource Management > Resources > Virtual Machines area, the VM Properties pane displays Parent Application names and Resource Pool names. If the name of the Parent Application displays, the name of the Resource Pool does not display. The VM can only be part of a Parent Application or part of a Resource Pool, so only one of these fields will display a value at a time.

Change in SSL Certificate with the Change in VNMC Hostname

Change in VNMC hostname results in changing SSL certificates on the clients. If any other service uses this certificate on the client node, that service will be affected. For example, if NSM service is installed on the VSM with an vsmPA, changes to VNMC hostname will affect the communication between NSM and vShield Manager. To work around the issue, refer to the corresponding service configuration guide.

Bugs

The following sections describe the open and resolved bugs in Cisco VNMC Release 1.3 for the Cisco Nexus 1000v switch and the Cisco Virtual Security Gateway:

- Open Bugs, page 6
- Resolved Bugs, page 7

Open Bugs

Table 3 describes the open bugs in Cisco VNMC 1.3.

Table 3 Open Bugs in Cisco VNMC 1.3

Bug ID	Headline
CSCtk47220	A syslog message is not generated on a Cisco VSG when the timezone is changed from the Cisco VNMC.
CSCtk60381	The **show running** command on the CLI always displays the log level of the policy agent as info.
CSCtk82548	Restoring a saved configuration with a shared secret does not work.
CSCtl02840	A shared secret with special characters causes the policy agent installation to fail.
CSCto06046	During a Cisco VNMC ISO installation, the Next button is not activated in the Device/Network Settings pane.
CSCto61627	The Cisco VSG compute firewall remains associated to a deleted VSG IP from the pool that is associated to the compute firewall.
CSCto92238	The Cisco VNMC Policy Manager consumes over 90% of the CPU, and the page displays “Data Error.”
CSCtr54339	Swapping out the vCenter (new one) with the same IP address does not result in all the vCenter attributes getting updated in the Cisco VNMC.
CSCtr78442	When adding a DNS provider, an error appears on the screen.
CSCtw50864	If a pool has a Cisco VSG that gets stuck when trying to associate a state, disassociate the state, it should free the IP address or stop the association.
CSCtw52837	TFTP does not work with import or export and backup or restore.
CSCtx44366	Duplicate network adapters on VNMC resources.
CSCtx67252	Blank hostname displayed in VNMC in case of MN stateless IP changes.
CSCtz01525	If you create a device policy and associate it with a compute firewall, the device profile parameters (such as DNS, NTP, and SNMP) are not applied to the Cisco VSG.

Resolved Bugs

Table 4 describes the caveats that were open in Cisco VNMC 1.2 and are resolved in Cisco VNMC 1.3.

Table 4 Bugs Open in Cisco VNMC 1.2 and Resolved in Cisco VNMC 1.3

Bug ID	Headline
CSCtr00650	The service status may not display the status for all the services in the Cisco VNMC.
CSCtr04974	VM attribute values do not auto populate with VM NICs in separate tenants.
CSCtr29484	LDAP authentication does not work with SSL.

Related Documentation

This section contains information about the documentation available for Cisco Virtual Network Management Center and related products.

This section includes the following topics:

Cisco Virtual Network Management Center Documentation

The following Cisco Virtual Network Management Center documents are available on Cisco.com at the following URL:

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

- *Release Notes for Cisco Virtual Network Management Center, Release 1.3*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.3*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.3*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.3*

Cisco Virtual Security Gateway Documentation

The following Cisco Virtual Security Gateway for the Nexus 1000V Series Switch documents are available on Cisco.com at the following URL:

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

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(3.1)*

- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(3.1)*

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available 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 a Really Simple Syndication (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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.