Release Notes for Cisco Virtual Network Management Center, Release 1.0.1

First Published: January 31, 2011
OL-24090-01

This document describes the features, caveats, and limitations for Cisco Virtual Network Management Center. Use this document in combination with the documents listed in the "Related Documentation" section on page 5.

Note Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the *Release Notes for Cisco Virtual Network Management Center, Release 1.0.1*:
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-24090-01	-	January 31, 2011	Created release notes for Cisco Virtual Network Management Center, Release 1.0.1

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, 2-Gb RAM, 25-Gb hard disk (vDisk), 1 management network interface
- Hypervisor and Hypervisor Manager—
  - VMware vSphere 4.0.1, 4.0.2, 4.1.0 releases with VMware ESX or ESXi
  - VMware vCenter 4.0.1, 4.0.2, and 4.1.0 releases
- Interfaces and Protocols—HTTP/HTTPS, Lightweight Directory Access Protocol (LDAP)
- Web-based GUI client—
  - Adobe Flash Player 10.1
  - Operating System—Support is as follows (see Table 2):

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

Operating System	Internet Explorer 7.x and 8.x	Firefox 3.x
Windows	Supported	Supported
Apple MAC OS	X	X
Linux	X	X

Software Features

The Cisco VNMC includes the following features:

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 APIs allow external system management and orchestration tools to programmatically provision Cisco VSGs and provide seamless and scalable operational management.

Caveats

This section describes the open caveats in Cisco VNMC and includes the following open caveats:

Bug ID	Caveat 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.
CSCtk82321	After a Cisco VNMC GUI administration import and export operation, the password field may not automatically clear.
CSCtk82548	Restoring a saved configuration with a shared secret does not work.
CSCtl00323	For locally defined non-admin users the change password configuration is not available.
CSCtl02840	A shared secret with special characters causes the policy agent installation to fail.
CSCtl04751	The VM Manager cannot be set to enable state if the Admin State is disable and the Operational State is bad-credentials.
CSCtl46168	The Cluster Name property does not change for newly added hosts in a cluster.
CSCtl80434	When installing Cisco VNMC using an ISO image, if the Prefix (Netmask) field is completed using dotted decimal notation AFTER both the Gateway and IP Address fields, the installer generates an error.
CSCtl89501	The client browser encounters an Error #2032 when connected to the Cisco VNMC GUI.
CSCtl91828	Restore fails when restoring from the OVA or ISO installations with the error message as follows: There was an error, please try again - Permission denied. The remote host credentials have been verified.

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 1.0.1*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.0.1*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.0.1*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.0.1*

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)VSG(1)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(1) and Cisco Virtual Network Management Center, Release 1.0.1 Installation Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(1)*

Send document comments to vnmc-docfeedback@cisco.com.

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.