Cisco Nexus 1000V for Microsoft Hyper-V Release Notes, Release 5.2(1)SM1(5.1)

First Published: September 13, 2013
Last Updated: October 16, 2014

This document describes the features, limitations, and caveats for the Cisco Nexus 1000V for Microsoft Hyper-V Release 5.2(1)SM1(5.1) software.

Contents

This document includes the following sections:

Introduction

The Cisco Nexus 1000V provides a distributed, Layer 2 virtual switch that extends across many virtualized hosts. The Cisco Nexus 1000V manages a data center. Each server in the data center is represented as a line card in the Cisco Nexus 1000V and can be managed as if it were a line card in a physical Cisco switch.

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

When server virtualization is implemented, the edge of the network is pushed from the traditional network access layer, which is implemented in physical switches, to the virtual network access layer that is implemented through the software in the Server Hypervisor. The Cisco Nexus 1000V is an intelligent virtual network access layer switch that runs Cisco NX-OS, which is Cisco's data center operating system common to all of Cisco's data center products.

Operating inside the Microsoft Hyper-V Hypervisor, the Cisco Nexus 1000V supports the Cisco Virtual Network-Link (VN-Link) server virtualization technology to provide to following:

- Policy-based Virtual Machine (VM) connectivity
- Mobile VM security and network policy
- Nondisruptive operational model for your server virtualization and networking teams.

Data center virtualization servers and VMs are not managed the same way as physical servers. Server virtualization is treated as a special deployment, leading to longer deployment time, with a greater degree of coordination among server, network, storage, and security administrators. With the Cisco Nexus 1000V, you have a consistent networking feature set and a configuration and provisioning model for both the physical and the virtual networks.

VM networks can use the same network configuration, security policy, diagnostic tools, and operational models as physical server deployments that are connected to physical switches. This unified approach to quicker deployment and troubleshooting makes virtualization environments no different from non virtualized deployments.

Developed with Microsoft, the Cisco Nexus 1000V is Microsoft certified and integrates with the Windows Server and Systems Center Virtual Machine Manager (SCVMM).

The Cisco Nexus 1000V consists of two basic components:

- Virtual Supervisor Module (VSM), also known as the Control Plane (CP). The VSM acts as the supervisor and contains the Cisco command-line interface (CLI), configuration, and high-level features.
- Virtual Ethernet Module (VEM), also known as the Data Plane (DP). The VEM acts as a line card and runs in each Hyper-V virtual switch to handle packet forwarding and other localized functions.

Hyper-V Webinar

Cisco offers a Cisco Nexus 1000V for Microsoft Hyper-V webinar as either a video demonstration or a PDF download. In the webinar, you can learn how the Cisco Nexus 1000V virtual access/distributed switch can simplify your Hyper-V virtual environment through a nondisruptive operational model, policy based provisioning, and a strong services ecosystem. You can also learn about the Cisco Nexus 1000V architecture, how it integrates with Microsoft SCVMM, and the networking capabilities it brings to Hyper-V environments.

Administrative Model

There are now two distinct administrative entities that manage the environment on the same set of hardware. Each has its own separate goals, abilities, and responsibilities. Server and VM policies can be set only by the server administrator through SCVMM or its management tools. Network policies can be set only by network administrator through the VSM or its management tools.

Some things we must support:

- Network and server administrators cannot make administrative changes to the system at the same time. Operations like deployment, upgrade, configuration, and troubleshooting can be carried out in an asynchronous fashion by respective administrators.
- If the network administrator has set up appropriate policies, the server administrator can add, remove, and move both physical hosts and VMs, as well as install physical interfaces in hosts and add virtual interfaces to VMs.

Software Compatibility with Microsoft

Ensure that the servers that run the Cisco Nexus 1000 VSM and VEM are in the Hardware Compatibility list. This release of the Cisco Nexus 1000V supports the Microsoft SCVMM server. For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information, Release 5.2(1)SM1(5.1)*.

Software Compatibility with Cisco Nexus 1000

This release supports Cisco Nexus 1000V for Microsoft Hyper-V Release 5.2(1)SM1(5.1). For additional information, see the *Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide, Release 5.2(1)SM1(5.1)*.

New and Changed Information

This section provides the following information about Cisco Nexus 1000V Release 5.2(1)SM1(5.1):

- Configuration Limits, page 3
- New Software Features, page 4

Configuration Limits

Component	Per VSM	Per VEM
Access control lists (ACLs)	128	—
ACL interfaces	500	216
Active VLANs	512	—
Application Control Engines (ACEs) per ACL	128	—
Failover cluster size	64	2012 (Windows server)
Hosts	64	
MAC addresses	4096	32000
Multicast groups	256/32	32
NetFlow interfaces	500	216
NetFlow policies	16	8

Component	Per VSM	Per VEM
Physical trunks	256	—
PNICs/hosts	31	—
Policy profiles	256	—
Port channels	256	8
Port profiles	1000 dynamic port profiles (vEthernet) 64 uplink dynamic port profiles	—
Port security	500	216
Private VLANs (PVLANs)	64	—
Quality of service (QoS) class maps	512	128
QoS interfaces	500	216
QoS policy maps	128	16
Segments	512	—
Switched Port Analyzer (SPAN)/Encapsulated Remote SPAN (ERSPAN) sessions	4	4
System network segments	16	—
System profiles	32	—
Virtual Ethernet (vEthernet) trunks	Not supported	—
vEthernet interfaces per port profile	1024	—
vEthernet interfaces	1000	216
VSM per aggregation	—	—

New Software Features

The following software features were added in the Cisco Nexus 1000V Release 5.2(1)SM1(5.1):

Installer

The Cisco Nexus 1000V Installer App is now a standalone C# application that can you can use to install the Cisco Nexus 1000V Logical Switch (VSM).

Release Support

This release supports Cisco Nexus 1000V for Microsoft Hyper-V Release 5.2(1)SM1(5.1).

VEM as a Forwarding Extension

The Cisco Nexus 1000V VEM is a forwarding extension in the Microsoft Hyper-V extensible switch framework, and it is deployed on each Microsoft Hyper-V host managed by the Cisco Nexus 1000V.

The VSM communicates with VEMs and with SCVMM. All configuration policies defined on the VSM are automatically propagated to SCVMM, so the SCVMM administrator can use these policies when creating Virtual Machines (VMs).

The VSM and VEM communicate using the following interfaces:

- SCVMM provider DLL—Interface provided by Microsoft that the VSM uses to talk to SCVMM and set or retrieve configuration information.
- Layer 3 asynchronous inter-process communication (AIPC)—Cisco proprietary packet-based protocol used by one Cisco NX-OS component to talk other NX-OS component. The Cisco Nexus 1000V extends this AIPC packet format to operate over a Layer 3 network. It is used by the VSM to control and manage the VEMs. All VEM configuration is handled through Layer 3-AIPC messages by the data path agent (DPA). Notifications from the VEM to the VSM also make use of AIPC.
- Input/Output Control (IOCTL)—Mechanism that is used between the Cisco Nexus 1000V forwarding extension and DPA in the Hyper-V host.
- Packet interface—Interface used to send protocol packets, such as the Cisco Discovery Protocol, between the VSM and the VEMs. It is also known as an inband channel. Both AIPC and the inband channel go over the same Layer 3 channel between the VSM and VEM.

Multiple User Constructs with SCVMM Networking Model

The Microsoft SCVMM networking model introduces multiple user-defined constructs including logical networks, network sites, and VM networks to abstract the underlying physical network. New commands have been added to the Cisco Nexus 1000V to define these constructs in the VSM.

Open Caveats

The following are descriptions of the caveats in Cisco Nexus 1000V Release 5.2(1)SM1(5.1). The ID links you to the Cisco Bug Search tool.

Table 1 Open Caveats in Cisco Nexus 1000V Release 5.2(1)SM1(5.1)

Category / ID		Open Caveat Headline
ACLs		
1.	CSCug56195	The **access-group** command leaks into vEthernet when an access group is deleted from a port profile.
Microsoft		
2.	CSCua16092	ERSPAN TX is not working when src is PC-PVLAN and the vEthernet interface is in PVLAN mode.

	Category / ID	Open Caveat Headline
3.	CSCuc98084	Module flaps are due to an HB loss during a performance test.
4.	CSCud36575	Multiple flows on the same CPU core reduces throughput.
5.	CSCud43237	The “attach ack failed by vem” message appeared when adding more NICs to an existing uplink network.
6.	CSCuf65918	Change in host IP, does not change module IP on VSM.
7.	CSCug53822	The ERSPAN packets generated by the receiving (RX) SPAN on the vEthernet interface are missing IP headers.
8.	CSCug93872	Outbound ACL does not work on the mgmt0 interface.
Management		
9.	CSCuc04803	Nonswitchport Ethernet port profiles should not be published.
10.	CSCud60409	A Server Virtualization Switch (SVS) connection is needed in Hyper-V with HTTPS.
11.	CSCue05498	VMs get stuck in a stopping state when some VMs are powered off.
12.	CSCue09970	A normal VMND and vEthernet port-profile policy update fails due to stale VMND information on the VEM.
13.	CSCue62007	Error occurs when adding Neighbor Discovery (ND) in the uplinknetwork where the system VLAN is set.
14.	CSCuf24560	Published names are ignored for network segments.
15.	CSCug33359	VM connectivity fails with the Intel NIC when the native profile is used.
16.	CSCug60850	Network Segmentation Manager (NSM) should check the current mode before flapping ports.
17.	CSCug65812	Remove the stale configuration from uplink network and port profile.
18.	CSCug85666	Creation of a Cisco Nexus 1000V instance fails on the Management NIC of a Windows 2012 server core host.
19.	CSCug91821	Switch deletion fails on the SCVMM and a host reboot is needed.
20.	CSCuh01806	There is an issue with Save Configuration if the host and VSM are in a different VLAN.
21.	CSCuh23791	The NSM causes a cascading failure when an uplink update fails.
22.	CSCuh24163	A PVLAN mapping command is missing on changing the mode to PVLAN trunk from trunk.
Platform		
23.	CSCue12918	No relevant information is captured by the **show tech-support svs detail** command.

Category / ID		Open Caveat Headline
24.	CSCue23291	The object cvnDVSPort returns Distributed Virtual Switch (DVS) port value zero.
25.	CSCug71001	The speed shown in the **show int capability** command output is incorrect.
Port Profile		
26.	CSCue07615	When you create a logical switch on the host, from an upgrade to a new build, an extra port channel interface is created.
27.	CSCuf43572	If the NetFlow monitor (NFM) configuration is applied as an interface override, the override configuration fails to show up in the running configuration.
Quality of Service (QoS)		
28.	CSCuf96620	A response timeout error is seen with an snmpwalk command on IF-MIB.
29.	CSCug16404	QoS statistics on the VEM get enabled after the Cisco Nexus1000V agent is restarted.
Representational State Transfer (REST)		
30.	CSCue29655	A user is authenticated when invoking REST to RADIUS/TACACS is configured.
Security		
31.	CSCue56757	TACACS authentication is not working on IPv6.
32.	CSCue88531	Failed to configure DHCP on the interface while powering on VMs with the DHCP configuration.
33.	CSCuf09114	A “seq timeout” error occurred with MTS_SAP_DHCP_SNOOP.
34.	CSCuf50018	The DHCP table is missing the vEthernet interface number for host vNICs.
35.	CSCuf50672	TACACS is not able to change the default authorization.
36.	CSCug64630	The IP table is not updating when changing an ACL.
SNMP		
37.	CSCue46090	An snmpwalk command for v3 after a system switchover fails with an unknown user name.
38.	CSCuh03748	SNMP gives the wrong statistics for several OIDs.
39.	CSCuh12495	An snmpquery fails for a community with a user-created SNMP group.
Virtual Machine Manager (VMM)		
40.	CSCuc16682	An SCVMM error occurred at port classification-> dependent resources.
41.	CSCuc44853	Switch extension manager (SEM) addition is taking too long (150 minutes).

Category / ID		Open Caveat Headline
42.	CSCud46791	Maximum ports are not being enforced.
43.	CSCue19084	Stale extension manager seen on the VMM UI.
44.	CSCue26596	Extension manager removal fails on the VMM.
45.	CSCug88520	Jobs fail as they lock while changing uplinks.
46.	CSCug88526	VM deployment with untagged VLAN fails.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 1000V.

The MIB Support List is available at the following FTP site:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus1000v/Nexus1000VMIBSupportList.html

Related Documentation

This section lists the documents used with the Cisco Nexus 1000V for Microsoft Hyper-V.

General Information

Cisco Nexus 1000V for Microsoft Hyper-V Release Notes

Install and Upgrade

Cisco Nexus 1000V for Microsoft Hyper-V Installation Guide

Configuration Guides

Cisco Nexus 1000V for Microsoft Hyper-V High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V Interface Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V Layer 2 Switching Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V Network Segmentation Manager Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V Port Profile Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V Quality of Service Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V Security Configuration Guide

Cisco Nexus 1000V for Microsoft Hyper-V System Management Configuration Guide

Programming Guide

Cisco Nexus 1000V for Microsoft Hyper-V REST API Guide

Reference and Troubleshooting Guides

Cisco Nexus 1000V for Microsoft Hyper-V Command Reference

Cisco Nexus 1000V for Microsoft Hyper-V Troubleshooting Guide

Virtual Services Appliance Documentation

The Cisco Nexus Virtual Services Appliance (VSA) documentation is available at http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway documentation is available at http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Virtual Network Management Center

The Cisco Virtual Network Management Center documentation is available at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

Virtual Wide Area Application Services (vWAAS)

The Virtual Wide Area Application Services documentation is available at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html

ASA 1000V Cloud Firewall

The ASA 1000V Cloud Firewall documentation is available at

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/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.