Cisco Nexus 1000V for Microsoft Hyper-V
Release Notes, Release 5.2(1)SM3(2.1)

First Published: 2018-12-21

This document describes the features, limitations, and bugs for Cisco Nexus 1000V for Microsoft Hyper-V Release 5.2(1)SM3(2.1).

Contents

This document includes the following sections:

- Introduction, page 2
- Software Compatibility with Microsoft Servers, page 3
- Software Compatibility with Cisco Nexus 1000V, page 3
- Limitations and Restrictions, page 3
- Upgrading Cisco Network Service Provider (Cisco VSEM) to the Current Release, page 4
- Configuration Limits, page 5
- Open Bugs, page 6
- Resolved Bugs, page 6
- Using the Bug Search Tool, page 6
- MIB Support, page 6
- Documentation Feedback, page 7
- Related Documentation, page 7
- Obtaining Documentation and Submitting a Service Request, page 7
Introduction

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

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. 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, Cisco Nexus 1000V supports the Cisco Virtual Network-Link (VN-Link) server virtualization technology to provide the 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 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 nonvirtualized deployments.

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

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 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 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

Cisco Nexus 1000V for Microsoft Hyper-V consists of two distinct administrative entities that manage the environment on the same set of hardware. Each entity 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 the network administrator through the VSM or its management tools.

Network and server administrators cannot make administrative changes to the system at the same time. Operations such as deployment, upgrade, configuration, and troubleshooting can be carried out in an asynchronous fashion by 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 Servers**

Ensure that the servers that run the Cisco Nexus 1000V VSM and VEM are in the Hardware Compatibility list.

This release of Cisco Nexus 1000V supports the following server:

- Microsoft Windows Server 2016

For additional compatibility information, see the *Cisco Nexus 1000V and Microsoft Hyper-V Compatibility Information, Release 5.2(1)SM3(2.1)*.

**Software Compatibility with Cisco Nexus 1000V**

This release supports an upgrade only from Release 5.2(1)SM1(1.1c). For an upgrade from Release 5.2(1)SM3(1.1) and later, you must first upgrade to Release 5.2(1)SM1(1.1c) before you upgrade to Release 5.2(1)SM3(2.1). This section describes how to upgrade Cisco Network Service Provider to the current release. The upgrade procedure for all other components is described in the *Cisco Nexus 1000V for Microsoft Hyper-V Installation and Upgrade Guide*.

Cisco Virtual Security Gateway (VSG) is installed on the Cisco Nexus 1000V switch and is managed using Cisco PNSC.

With Cisco Nexus 1000V Release 5.2(1)SM3(2.1) you can install Cisco VSG Release 5.2(1)VSG2(2.1).

**Limitations and Restrictions**

This section describes the limitations and restrictions of the Cisco Nexus 1000V for Microsoft Hyper-V, Release 5.2(1)SM3(2.1).

- TACACS+ type-6 password encryption is applicable in the following order:
  1. feature configuration
  2. creating the master key
  3. configuration of the TACACS+ server key

**Note** You will not be able to achieve a proper TACACS+ type-6 password encryption if the above order is not followed.
Upgrading Cisco Network Service Provider (Cisco VSEM) to the Current Release

Note Starting with Release 5.2(1)SM3(1.1), Cisco VSEM is referred to as Cisco Network Service Provider.

Upgrading Cisco Network Service Provider from Release 5.2(1)SM3(1.1c) to the Current Release

To upgrade Cisco Network Service Provider, perform the following steps:

Step 1 Install the Nexus1000V-NetworkServiceProvider-5.2.1.SM3.2.1.0.msi from the Cisco Nexus 1000V zip location on the SCVMM server.

The installation restarts the SCVMM service, uninstalls the existing Cisco Network Service Provider MSI, and installs the new Cisco Network Service Provider MSI.

After a successful installation, the PowerShell scripts needed to upgrade VEM are placed in the %ProgramFiles%\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade directory on the SCVMM server (for example, C:\Program Files\Cisco\Nexus1000V\V2\Scripts\VEMUpgrade).

Step 2 Verify that Cisco Network Service Provider is installed correctly by completing the following steps:
   a. Click the Start button and choose Control Panel > Programs > Programs and Features.
   b. Verify that the current version of the Cisco Nexus 1000V Network Service Provider program is 2.01.000.

Step 3 Refresh the Cisco Nexus 1000V Extension Manager by completing the following steps:
   a. Open the SCVMM console.
   b. Navigate to the Fabric workspace.
   c. On the Fabric pane, expand Networking, and click Network Service.
   d. In the Results pane, right-click Cisco Systems Nexus 1000V extension, and choose Refresh.
## Configuration Limits

The following table shows the Cisco Nexus 1000V configuration limits.

<table>
<thead>
<tr>
<th>Component</th>
<th>Per VSM</th>
<th>Per VEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control lists (ACLs)</td>
<td>128</td>
<td>—</td>
</tr>
<tr>
<td>ACL instances</td>
<td>2048</td>
<td>216</td>
</tr>
<tr>
<td>Active VLANs</td>
<td>2048</td>
<td>—</td>
</tr>
<tr>
<td>Application Control Engines (ACEs) per ACL</td>
<td>128</td>
<td>—</td>
</tr>
<tr>
<td>Hosts</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>MAC addresses per VLAN</td>
<td>4096</td>
<td>32,000</td>
</tr>
<tr>
<td>MAC addresses per DVS</td>
<td>32,000</td>
<td>—</td>
</tr>
<tr>
<td>Multicast groups</td>
<td>512</td>
<td>64</td>
</tr>
<tr>
<td>NetFlow interfaces</td>
<td>2048</td>
<td>216</td>
</tr>
<tr>
<td>NetFlow policies</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Physical trunks</td>
<td>512</td>
<td>—</td>
</tr>
<tr>
<td>PNICs/hosts</td>
<td>32</td>
<td>—</td>
</tr>
<tr>
<td>Port channels</td>
<td>256</td>
<td>8</td>
</tr>
<tr>
<td>Port profiles</td>
<td>1000 dynamic port profiles (vEthernet)</td>
<td>—</td>
</tr>
<tr>
<td>Port security</td>
<td>2048</td>
<td>216</td>
</tr>
<tr>
<td>Private VLANs (PVLANS)</td>
<td>512</td>
<td>—</td>
</tr>
<tr>
<td>Quality of service (QoS) class maps</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>QoS instances</td>
<td>2048</td>
<td>216</td>
</tr>
<tr>
<td>QoS policy maps</td>
<td>128</td>
<td>16</td>
</tr>
<tr>
<td>Network segment</td>
<td>2048</td>
<td>—</td>
</tr>
<tr>
<td>Switched Port Analyzer (SPAN)/Encapsulated</td>
<td>64</td>
<td>4</td>
</tr>
<tr>
<td>Remote SPAN (ERSPAN) sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System network segments</td>
<td>32</td>
<td>—</td>
</tr>
<tr>
<td>System profiles</td>
<td>32</td>
<td>—</td>
</tr>
<tr>
<td>Virtual Ethernet (vEthernet) trunks</td>
<td>Not supported</td>
<td>—</td>
</tr>
<tr>
<td>vEthernet interfaces per port profile</td>
<td>1024</td>
<td>—</td>
</tr>
<tr>
<td>vEthernet interfaces</td>
<td>2048</td>
<td>216</td>
</tr>
<tr>
<td>Reserved-ip per ip pool template</td>
<td>128</td>
<td>—</td>
</tr>
<tr>
<td>Netbios-name-server per ip pool template</td>
<td>16</td>
<td>—</td>
</tr>
<tr>
<td>DNS-server per ip pool template</td>
<td>16</td>
<td>—</td>
</tr>
<tr>
<td>DNS-suffix per ip pool template</td>
<td>16</td>
<td>—</td>
</tr>
</tbody>
</table>
Open Bugs

There are no open bugs in Cisco Nexus 1000V Release 5.2(1)SM3(2.1).

Resolved Bugs

There are no resolved bugs in The following table lists the resolved bugs in Cisco Nexus 1000V Release 5.2(1)SM3(2.1).

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Step 1  Go to http://tools.cisco.com/bugsearch.
Step 2  At the Log In screen, enter your registered Cisco.com username and password; then, click Log In. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3  To search for a specific bug, enter the bug ID in the Search For field and press Return.
Step 4  To search for bugs in the current release:
a. In the Search For field, enter Cisco Nexus 1000V and press Return. (Leave the other fields empty.)
b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.
To export the results to a spreadsheet, click the Export Results to Excel link.

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:
Documentation Feedback

To provide technical feedback on this document or report an error or omission, send your comments to nexus1k-docfeedback@cisco.com.
We appreciate your feedback.

Related Documentation

Cisco Nexus 1000V for Microsoft Hyper-V

Cisco Nexus 1000V for Microsoft Hyper-V documentation

Cisco Nexus 1000V for VMware

Cisco Nexus 1000V for VMware vSphere documentation

Cisco Virtual Security Gateway

Cisco Virtual Security Gateway documentation

Cisco Prime Network Services Controller

Cisco Prime Network Services Controller documentation

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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 and Cisco currently supports RSS Version 2.0.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Internet Protocol (IP) addresses that are used in the examples, command display output, and figures within this document are for illustration only. If an actual IP address appears in this document, it is coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.