



Release Notes for Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.1)

First Published: November 21, 2014

Last Updated: May 12, 2016

This document describes the features and limitations for the Cisco Nexus 1000V for KVM software. It also provides information about how to find information about open and closed bugs. Use this document in combination with the documents listed in the [Related Documentation](#).

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Cisco Nexus 1000V for KVM Features, page 3](#)
- [Limitations and Restrictions, page 4](#)
- [Software Compatibility, page 7](#)
- [Server and NIC Requirements, page 7](#)
- [Installation of Cisco Nexus 1000V for KVM, page 8](#)
- [Using the Bug Search Tool, page 8](#)
- [MIB Support, page 9](#)
- [Documentation Feedback, page 9](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)



Introduction

Cisco Nexus 1000V for KVM is a virtual distributed switch that works with the Linux Kernel-based virtual machine (KVM) open source hypervisor.

Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.1) works with Red Hat Enterprise Linux OpenStack Platform (RHEL-OSP). RHEL-OSP provides interacting services that control its computing, storage, and networking resources and is the foundation on which to build a private or public Infrastructure-as-a-Service (IaaS) cloud.

The networking function of OpenStack is controlled and managed by the OpenStack Neutron Service. Neutron enables the Cisco Nexus 1000V switch to provide the networking capabilities to compute nodes and virtual machines (VMs). As Neutron creates and configures its networks for its environment, this configuration is passed to the Cisco Nexus 1000V switch.

Using OpenStack, you create VM networks and subnets on Cisco Nexus 1000V for KVM by defining components such as the following:

- Tenants
- Network segments, such as VLANs, VLAN trunks, and Virtual Extensible Local Area Networks (VXLANs)
- IP subnets

On the Virtual Supervisor Module (VSM), you create port profiles, which define feature policies for different types or classes of VMs and security policies for the VM's traffic.

When a VM is deployed, a port profile is dynamically created on Cisco Nexus 1000V for KVM for each unique combination of policy (or feature) port profile and network segment. All other VMs deployed with the same policy to this network reuse this dynamic port profile.

**Note**

You must consistently use OpenStack for all VM network, subnet, and port configurations. If you create VM networks, subnets, and ports directly on the VSM, the configuration is lost when the OpenStack synchronization occurs. For information about OpenStack, see the *Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*.

Cisco Nexus 1000V for KVM Features

Cisco Nexus 1000V for KVM, Release 5.2(1)SK3(2.1) supports the following features:

- [Red Hat Enterprise Linux OpenStack Platform Installer, page 3](#)
- [SPAN and ERSPAN, page 3](#)
- [vTracker, page 3](#)
- [PVLAN, page 4](#)
- [Unknown Unicast Floods, page 4](#)

Red Hat Enterprise Linux OpenStack Platform Installer

Cisco Nexus 1000V for KVM, Release 5.2(1)SK3(2.1) uses Red Hat deployment management tool called RHEL-OSP Installer to install the Cisco Nexus 1000V for KVM on RHEL in an OpenStack cloud environment.

RHEL OpenStack Platform provides the foundation to build a private or public Infrastructure-as-a-Service (IaaS) cloud on top of Red Hat Enterprise Linux.

SPAN and ERSPAN

Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.1) supports Switched Port Analyzer (SPAN), including local SPAN and encapsulated remote SPAN (ERSPAN).

The SPAN feature—sometimes called port mirroring or port monitoring—allows network traffic to be analyzed by a network analyzer such as a Cisco SwitchProbe or other Remote Monitoring (RMON) probes.

SPAN allows you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports where the network analyzer is attached.

See the *Cisco Nexus 1000V for KVM System Management Configuration Guide* for more information about SPAN and ERSPAN.

vTracker

Cisco Nexus 1000V for KVM, Release 5.2(1)SK3(2.1) supports vTracker, which provides information about the virtual network environment.

Once you enable vTracker, it becomes aware of all the modules and interfaces that are connected with the switch. vTracker provides various views that are based on the data sourced from the Redhat OpenStack dashboard, the Cisco Discovery Protocol (CDP), and other related systems connected with the virtual switch. You can use vTracker to troubleshoot, monitor, and maintain the systems.

See the *Cisco Nexus 1000V for KVM System Management Configuration Guide* for more information about vTracker.

PVLAN

Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.1) supports Private VLANs.

PVLANs achieve device isolation through the use of three separate port designations, each having its own unique set of rules that regulate each connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain.

Within a PVLAN domain, there are three separate port designations. Each port designation has its own unique set of rules that regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain.

The three port designations are as follows:

- promiscuous
- isolated
- community

See the *Cisco Nexus 1000V for KVM Layer 2 Configuration Guide* for more information about PVLAN.

Unknown Unicast Floods

Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.1) supports the unknown unicast packet flooding (UUFB) feature. UUFB limits unknown unicast flooding in the forwarding path to prevent the security risk of unwanted traffic reaching the Virtual Machines (VMs). UUFB prevents packets received on both vEthernet and Ethernet interfaces destined to unknown unicast addresses from flooding the VLAN.

When UUFB is applied, Virtual Ethernet Modules (VEMs) drop unknown unicast packets received on uplink ports, while unknown unicast packets received on vEthernet interfaces are sent out only on uplink ports.

See the *Cisco Nexus 1000V for KVM Security Configuration Guide* for more information about Unknown Unicast Floods.

Limitations and Restrictions

Scheduler for Neutron DHCP Port and Linux Router

- The Linux router scheduling is random. At any time, one network node might be provisioned with a greater number of Linux routers than other network nodes.
- The default DHCP agent scheduler algorithm is also random. At any time, one controller node might be provisioned with a greater number of DHCP ports than other controller nodes.
- Each controller node can support up to 990 ports (DHCP and router ports). When this limit is reached, any additional DHCP or router ports are not brought up on the VEM.

OpenStack Horizon Dashboard

- If you have more than 200 ports provisioned in the Cisco Nexus 1000V, the OpenStack Horizon dashboard navigation becomes very slow.
- If you are using the OpenStack Horizon dashboard, all vNIC interfaces on the same VM must have the same policy profile. If you need to have different policy profiles assigned to vNICs on the same VM, you can do so by using the OpenStack CLI.

DHCP Port

When you bring up a VSM, it should have the default port profile named **default-pp**. This port profile is not automatically created. You need to create this port profile.

The default-pp port profile is used to create DHCP ports. Do not apply any features on this port profile because it impacts the functioning of the DHCP ports. In addition, do not use this port profile to bring up a VM to which you want to apply the port profile features.

VSM

If you reboot the VSM before you enter the **copy running-config startup-config** command on the VSM, you must create the missing policy port-profiles in the VSM with the same UUID. For more information, see the *Cisco Nexus 1000V for KVM Troubleshooting Guide*.

vEthernet Trunks

Deploying vEthernet trunk ports is possible using a trunk policy profile configured on the VSM. With this profile configured on the port, all VLANs configured in the VSM are allowed. You can restrict the set of allowed VLANs by editing the trunk policy profile on the VSM. However, this change is applied to all ports configured with this profile.

Network Segmentation Manager

The VSM CLI does not prevent you from deleting or modifying objects on the VSM, such as a network segment pool, IP pool template, network segment, or dynamic port profile, that were created by the Network Segmentation Manager (NSM). If you do, your VSM configuration could become out-of-sync with the network configuration on OpenStack.

VXLAN Gateway

Starting with Release 5.2(1)SK3(1.1), Cisco Nexus 1000V for KVM does not support the VXLAN Gateway feature.

Virtual Ethernet Modules

- The slow path is referred to as the path the packet takes when it is punted to the process level for a switching decision before its kernel fast path flow cache is established. The VEM has a slow path maximum throughput. Traffic drops occur with throughput greater than 300 Mbps, and the amount of CPU being utilized spikes to 100 percent for switching processes.
- OpenStack does not support live migration to headless VEMs.
- If a VLAN reaches the 4000 MAC address limit, any additional traffic from new MAC addresses use the slow path.
- Any configuration change to a port profile results in flows getting reprogrammed, which temporarily slows traffic.

VXLAN Native and VXLAN Enhanced

- Having multiple VXLAN Tunnel Endpoints (VTEPs) in the same subnet requires an additional configuration file for the Address Resolution Protocol (ARP) to function.
- Multicast traffic on a VXLAN might impact performance.

Access Control Lists

If the applied ACL has rule with Layer 4 parameters, fragmented packets uses slow path, else fragmented packets gets switched in the fast path.

NetFlow

If the NetFlow record has Layer 4 match criteria, then the fragmented packets use the slow path. Otherwise, the fragmented packets gets switched in the fast path.

IGMP

The maximum multicast traffic throughput without packets being dropped is 3 Gbps on a single VEM.

VLANs

You cannot change the native VLAN from its default to a different type if you created the trunk network profile using OpenStack.

Troubleshooting Tools

The show logging information has been removed from the **show tech-support svcs** command output because the information it displayed was not related to the Cisco Nexus 1000V for KVM. If you need additional technical support information, you can use the **show tech-support svcs detail** command. Optionally, you can add the exclude interface pipe; for example, **show tech-support svcs detail | exclude interface**.

Software Compatibility

Table 1 lists the minimum supported software versions required for a Cisco Nexus 1000V for KVM Release 5.2(1)SK3(2.1) deployment.



Note

Depending on your specific Cisco Nexus 1000V for KVM release, it is your responsibility to monitor and install all relevant Linux patches on Linux hosts.

Table 1 Minimum Software Versions Supported by Release 5.2(1)SK3(2.1)

Name	Minimum Software Version
RHEL (for OpenStack Platform Installer hosts)	6.6
RHEL (for provisioning hosts)	7.0
OpenStack	Icehouse
Kernel	RedHat 3.10.0-x

Server and NIC Requirements

You can deploy Cisco Nexus 1000V for KVM on the following Cisco UCS servers:

- Standalone rack-mount servers that are managed by Cisco Integrated Management Controller (IMC)
- Integrated rack-mount servers that are managed by Cisco UCS Manager
- Blade servers that are managed by Cisco UCS Manager

The following NIC types have been tested and verified:

- Emulex OCE11102-FX 2 port 10 GbE CAN
- Intel X520 DA2 10Gbps 2 port NIC
- Intel I350 1 Gbps
- Intel 82599EB 10 Gbps
- Broadcom 5709 1 Gbps 4 port NIC

See the *Cisco Nexus 1000V for KVM Software Installation Guide* for additional information about the requirements for the Cisco UCS servers that you use for the nodes in your Cisco Nexus 1000V for KVM deployment.

Installation of Cisco Nexus 1000V for KVM

Release 5.2(1)SK3(2.1) release of Cisco Nexus 1000V for KVM uses the RHEL-OSP to facilitate the installation of OpenStack and Cisco Nexus 1000V for KVM. A description of each is as follows:

- RHEL-OSP—Linux operating system with the Red Hat's implementation of the latest OpenStack. RHEL-OSP provides interacting services that control its computing, storage, and networking resources and is the foundation on which to build a private or public Infrastructure-as-a-Service (IaaS) cloud.
- OpenStack—Scalable cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter.
- Cisco Nexus 1000V for KVM— Distributed virtual switch (DVS) that works with several different hypervisors. This DVS version is integrated with the Ubuntu Linux Kernel-based virtual machine (KVM) open source hypervisor.

You need to deploy RHEL-OSP before you can deploy OpenStack with the Cisco Nexus 1000V for KVM.

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:

- In the Search For field, enter **Cisco Nexus 1000V for KVM** and press **Return**. (Leave the other fields empty.)
- 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.



Tip 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.

For a list of MIBs that the Cisco Nexus 1000V for KVM supports, see the *Cisco Nexus 1000V for KVM System Management Configuration Guide*.

Documentation Feedback

To provide technical feedback on this document or report an error or omission, please send your comments to:

nexus1k-docfeedback@cisco.com

We appreciate your feedback.

Related Documentation

This section lists the documents used with the Cisco Nexus 1000V for KVM.

General Information

Cisco Nexus 1000V for KVM Release Notes

Install and Upgrade

Cisco Nexus 1000V for KVM Software Installation Guide

Cisco Nexus 1000V for KVM Software Installation Video

Cisco Nexus 1000V for KVM Software Installation Workflow

Configuration Guides

Cisco Nexus 1000V for KVM High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V for KVM Interface Configuration Guide

Cisco Nexus 1000V for KVM Layer2 Configuration Guide

Cisco Nexus 1000V for KVM License Configuration Guide

Cisco Nexus 1000V for KVM Port Profile Configuration Guide

Cisco Nexus 1000V for KVM REST API Configuration Guide

Cisco Nexus 1000V for KVM Security Configuration Guide

Cisco Nexus 1000V for KVM System Management Configuration Guide

Cisco Nexus 1000V for KVM Verified Scalability Guide

Cisco Nexus 1000V for KVM Virtual Network Configuration Guide

Cisco Nexus 1000V for KVM VXLAN Configuration Guide

Reference Guides

Cisco Nexus 1000V for KVM Command Reference

Cisco Nexus 1000V for KVM OpenStack API Reference Guide

Troubleshooting, Password Recovery, System Messages Guides

Cisco Nexus 1000V for KVM System Messages Guide

Cisco Nexus 1000V for KVM Troubleshooting Guide

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](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

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. (1110R)

Copyright © 2014-2016 Cisco Systems, Inc. All rights reserved.