Cisco Nexus 1000V Release Notes, Release 5.2(1)SV3(3.15)

First Published: 2017-11-07

Last Modified: 2018-11-30

Cisco Nexus 1000V Release Notes

This document describes the features, limitations, and bugs for Cisco Nexus 1000V Release 5.2(1)SV3(3.15).

Cisco Nexus 1000V for VMware

The Cisco Nexus 1000V for VMware provides a distributed, Layer 2 virtual switch that extends across multiple virtualized hosts. The Cisco Nexus 1000V manages a data center defined by the vCenter Server. 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.

The Cisco Nexus 1000V consists of the following components:

- Virtual Supervisor Module (VSM), which contains the Cisco CLI, configuration, and high-level features.
- Virtual Ethernet Module (VEM), which acts as a line card and runs in each virtualized server to handle packet forwarding and other localized functions.

Note Nexus 1000v syslog messages do not include hostname field.

Software Compatibility with VMware

The servers that run the Cisco Nexus 1000V VSM and VEM must be in the VMware Hardware Compatibility list. This release of the Cisco Nexus 1000V supports vSphere 5.5, 6.0, and 6.5a release trains. For additional compatibility information, see the *Cisco Nexus 1000V and VMware Compatibility Information*.

Note

- VSM hardware versions 7, 8, 9, and 10 are supported. VSM hardware version 11 is not supported.
- The Cisco Nexus 1000V supports all virtual machine network adapter types that VMware vSphere supports. Refer to the VMware documentation when choosing a network adapter. For more information, see the *VMware Knowledge Base article #1001805*.

Software Compatibility with Cisco Nexus 1000V

This release supports hitless upgrades from Release 4.2(1)SV2(1.1) and later. For more information, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

New Features and Enhancements

Cisco Nexus 1000V Release 5.2(1)SV3(3.15) includes the following features, enhancements, and support:

Feature	Description
Fixes for various customer issues	See Resolved Bugs, on page 14 for various bugs resolved for this release.
802.1X Security Support	Added Support for 802.1X security feature.

Configuration Scale Limits

The following topics provide configuration scale limit information:

- Cisco Nexus 1000V Configuration Scale Limits
- Cisco VSG Configuration Scale Limits, on page 4
- Cisco AVS Configuration Scale Limits, on page 4
- VDP Configuration Scale Limits, on page 5

Cisco Nexus 1000V Configuration Scale Limits

The following table lists the configuration scale limit information for the Cisco Nexus 1000V Advanced edition.

Note The scale limits for the Cisco Nexus 1000V Essential edition are half of what is stated in the following table.

Feature	VEM	DVS	Other
Hosts/DVS	—	250 (includes gateways)	—
Total vEth ports	1000	10,240	—
Ports per port profile	1024	2048	—
Port profiles	6144	6144	—
Physical NICs	32	2000	—
Physical trunks	32	2000	—
vEthernet trunks	32	1024	—
Port channels	8	1024	—

Feature	VEM	DVS	Other
Active VLANs	4094	4094	—
VXLANs (bridge domains)	6144	6144	—
VXLAN trunks	32	1024	—
VXLAN mappings per trunk	512	—	—
VXLAN VNI	1044	6144	—
VTEPs	4	1024	512 per bridge domain
BGP peers	8 VSM	—	—
Route reflectors	—	—	2 per VXLAN control plane
MAC addresses	32,000	—	—
MAC address per VLAN	4094	4094	—
DHCP IP bindings	1024	10,240	—
ACLs	128	128	—
ACEs per ACL	—	128	—
ACL instances	6000	42,000	6 instances per port
NetFlow policies	32,000 flows	• 64 monitor sessions • 64 records • 64 exporters	—
QoS policy maps	—	128	—
QoS class	—	1024	—
QoS class maps/policy maps	—	—	64
QoS instances (ingress and egress)	—	9000	—
Multicast groups	1024	1024	—
PVLANs	512	512	—
Port security MACs	2048	24,000	5 MACs per port
SPAN/ERSPAN sessions	64	64	—

Feature	VEM	DVS	Other
Source interfaces per session	—	128 vEths or 32 physical Eths or port channels	—
Source VLANs per session	—	32	—
Destination interfaces per session	—	32	—
SPAN sessions per source interface	—	4	—
Source profiles per session	—	16	—
Destination profiles per session	—	8	—
Cisco TrustSec	—	• 6000 IP-SGT mappings • 4000 IP-Subnet-SGT mappings • 128 SGACLs • 128 ACEs per SGACL • 8 SXP peers	—
Number of VSMs per VC	—	—	64
Domain ID range	—	—	1-1023
802.1x vEthernet Ports	130	1000 (Maximum number of vEthernet ports that can be authenticated at a time).	N/A

Cisco VSG Configuration Scale Limits

In this release, when Cisco Virtual Security Gateway (VSG) solutions using version 5.2(1)VSG3(3.1) are deployed, the following scale limitations apply and supersede the scale numbers shown in *Cisco Nexus 1000V Configuration Scale Limits* section.

Feature	VEM	DVS	Number of VEM Modules
VSG	512 vEth ports per VEM	10,000 vEth ports with up to 6000 vEth ports protected by VSG	250 per DVS

Cisco AVS Configuration Scale Limits

In this release, when Cisco Application Virtual Switch (AVS) solutions are deployed, the following scale limitations apply and supersede the scale numbers shown in *Cisco Nexus 1000V Configuration Scale Limits* section.

Feature	VEM	Top of Rack
AVS	300 vEth ports per VEM	40 VEM modules

VDP Configuration Scale Limits

In this release, when VSI Discovery Protocol (VDP) solutions are deployed, the following scale limitations apply and supersede the scale numbers shown in *Cisco Nexus 1000V Configuration Scale Limits* section.

Feature	VEM	DVS	Number of VEM Modules
VDP	300 vEth ports per VEM	4000 vEth ports	128 per DVS

Important Notes and Limitations

The following topics provide important notes and limitations.

Using VSM Control0 Interface as the SVS Control Interface

If the Cisco Nexus 1000V SVS domain is configured to use layer-3 control mode in an environment where the VSM control0 interface is not in the same IP subnet as the packet/control VMKernel interface on the ESXi hosts, it is necessary to configure a static route on the VSM in the default VRF. A static route is required so that the VSM has a known route to the subnet(s) used by the ESXi host VMK interfaces used for Nexus 1000V packet/control. A default static route is ignored and you need to configure a specific static route that includes all the destination networks used by ESXi host VMK packet/control interfaces. A static route that is more specific than a default "/0" route is required to route packets/traffic between the VSM and VEM. For example, the following two static routes can be used as a direct replacement of a default static route:

```
ip route 0.0.0.0/1 <vsm-control0-def-gw-ip>
ip route 128.0.0.0/1 <vsm-control0-def-gw-ip>
```

Where <vsm-control0-def-gw-ip> is the IP address of the default gateway for the VSM control0 interface subnet.

Attention When upgrading, check the configuration of the existing Cisco Nexus 1000V, if a default static route is used in the default VRF, make sure that you add a specific static route in the default VRF for the traffic to VMK network to use control0 interface gateway. Failing to make this configuration change will cause all VEMs that are not in the same subnet as the VSM control0 interface to go offline.

Configuration Container Names Must Be Unique

All Cisco Nexus 1000V VSM configuration containers—port profiles, bridge domains, ACLs, class maps, policy maps, and so on—must have unique names.

In releases earlier than 5.2(1)SV3(1.1), you could create two configuration containers (for example, two port profiles) with the same name but different case sensitivity; for example, vmotion and VMOTION.

In later releases, you cannot create two configuration containers (for example, two port profiles) with the same name but different case sensitivity. During an upgrade, one of the port profiles with a duplicate name is deleted, which moves the corresponding ports in vCenter into quarantined state.

For example, do not create bridge domains with the same name (one uppercase, one lowercase) that point to different segments. See the following examples:

This is an example of an uppercase name:

```
switch# show bridge-domain VXLAN14095
Bridge-domain VXLAN14095 (0 ports in all)
Segment ID: 12333 (Manual/Active)
Mode: Unicast-only
MAC Distribution: Disable
BGP control mode: Enable
Group IP: NULL
Encap Mode: VXLAN*
State: UP Mac learning: Enabled
```

This is an example of a lowercase name:

```
switch# show bridge-domain vxlan14095
Bridge-domain vxlan14095 (0 ports in all)
Segment ID: 14095 (Manual/Active)
Mode: Unicast-only
MAC Distribution: Disable
BGP control mode: Enable
Group IP: 237.1.1.196
Encap Mode: VXLAN*
State: UP Mac learning: Enabled
```

Single VMware Data Center Support

The Cisco Nexus 1000V for VMware can be connected to a single VMware vCenter Server data center object. Note that this virtual data center can span multiple physical data centers.

Each VMware vCenter can support multiple Cisco Nexus 1000V VSMs per vCenter data center.

VDP

Implementing VDP on the Cisco Nexus 1000V has the following limitations and restrictions:

- The Cisco Nexus 1000V supports the Cisco DFA-capable VDP based on the IEEE Standard 802.1 Qbg, Draft 2.2, and does not support the Link Layer Discovery Protocol (LLDP). Therefore, the EVB type, length, and value are not originated or processed by the Cisco Nexus 1000V.
- The VDP implementation in the current release supports a matching LLDP-less implementation on the bridge side, which is delivered as part of the Cisco DFA solution. For more information on the Cisco DFA, see the *Cisco DFA Solutions Guide*.
- Timer-related parameters are individually configurable in the station and in the leaf.
- Connectivity to multiple unclustered bridges is not supported in this release.
- IPv6 addresses in filter format are not supported in this release.
- VDP is supported for only segmentation-based port profiles. VDP for VLAN-based port profiles is not supported in this release.
- The dynamic VLANs allocated by VDP are local to the VEM; they should not be configured on the Cisco Nexus 1000V VSM.
- VDP is supported on VMware ESX releases 5.0, 5.1, 5.5, and 6.0 in this release.

Custom TCP/IP Stack

Cisco Nexus 1000V VEM does not support ESXi custom TCP/IP stack and control traffic through the custom TCP/IP stack.

DFA

Fabric forwarding mode is not supported under the VLAN configuration.

ERSPAN

If the ERSPAN source and destination are in different subnets, and if the ERSPAN source is an L3 control VM kernel NIC attached to a Cisco Nexus 1000V VEM, you must enable proxy-ARP on the upstream switch.

If you do not enable proxy-ARP on the upstream switch (or router, if there is no default gateway), ERSPAN packets are not sent to the destination.

VMotion of VSM

VMotion of VSM has the following limitations and restrictions:

- VMotion of VSM is supported for both the active and standby VSM VMs. For high availability, we recommend that the active VSM and standby VSM reside on separate hosts.
- If you enable Distributed Resource Scheduler (DRS), you must use the VMware anti-affinity rules to ensure that the two VMs are never on the same host, and that a host failure cannot result in the loss of both the active and standby VSM.
- VMware VMotion does not complete when using an open virtual appliance (OVA) VSM deployment if the CD image is still mounted. To complete the VMotion, either click **Edit Settings** on the VM to disconnect the mounted CD image, or power off the VM. No functional impact results from this limitation.
- If you are adding one host in a DRS cluster that is using a vSwitch to a VSM, you must move the remaining hosts in the DRS cluster to the VSM. Otherwise, the DRS logic does not work, the VMs that are deployed on the VEM could be moved to a host in the cluster that does not have a VEM, and the VMs lose network connectivity.

Note For more information about VMotion of VSM, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

Access Lists

ACLs have the following limitations and restrictions:

- VLAN-based ACLs (VACLs) are not supported.
- ACLs are not supported on port channels.
- The **access-class** command is not supported on the vty interface. Use management interface ACL for any access-list requirements.

NetFlow

The NetFlow configuration has the following limitations and restrictions:

- NetFlow Sampler is not supported.
- NetFlow Exporter format V9 is supported.
- NetFlow Exporter format V5 is not supported.
- NetFlow is not supported on port channels.
- The NetFlow cache table does not support immediate or permanent cache types.

Port Security

Port security has the following limitations and restrictions:

- Port security is enabled globally by default.
- The **feature/no feature port-security** command is not supported.
- In response to a security violation, you can shut down the port.

Port Profiles

Port profiles have the following limitations and restrictions:

- There is a limit of 255 characters in a **port-profile** command attribute.
- We recommend that if you are altering or removing a port channel, you should migrate the interfaces that inherit the port channel port profile to a port profile with the desired configuration, rather than editing the original port channel port profile directly.
- When you remove a port profile that is mapped to a VMware port group, the associated port group and settings within the vCenter Server are also removed.
- Policy names are not checked against the policy database when ACL/NetFlow policies are applied through the port profile. It is possible to apply a nonexistent policy.
- The port profile name can be up to 80 alphanumeric characters, is not case-sensitive, and must be unique for each port profile on the Cisco Nexus 1000V. The port profile name cannot contain any spaces. The port profile name can include all the ASCII special characters except the forward slash (/), backslash (\), percent (%), and question mark (?).

Note If there are any existing port profiles (created in earlier Cisco Nexus 1000V releases) with names that contain a forward slash (/), backslash (\), percent (%), or question mark (?), you can continue to use them in this release.

SSH Support

Only SSH version 2(SSHv2) is supported.

Mixed-Mode Upgrade Support

Starting with Release 5.2(1)SV3(1.15), Cisco Nexus 1000V deployment supports a configuration where the VSM version can be the same or later than the VEM version. With the mixed-mode upgrade functionality, you can upgrade the VSM without upgrading the VEM and reduce the overhead involved in the Cisco Nexus

1000V upgrade. For more information on mixed-mode upgrade support, see the *Cisco Nexus 1000V Installation and Upgrade Guide*.

LACP

Only LACP offload to VEM is supported. Upgrades from earlier releases to this release change LACP to offload mode by default.

Cisco NX-OS Commands Might Differ from Cisco IOS

Be aware that the Cisco NX-OS CLI commands and modes might differ from those commands and modes used in the Cisco IOS software.

No Spanning Tree Protocol

The Cisco Nexus 1000V for VMware forwarding logic is designed to prevent network loops; therefore, it does not use the Spanning Tree Protocol. Packets that are received from the network on any link connecting the host to the network are not forwarded back to the network by the Cisco Nexus 1000V.

No Support for VXLAN Gateway

Starting with Cisco Nexus 1000V Release 5.2(1)SV3(1.15), the VXLAN Gateway feature is not supported.

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is enabled globally by default.

CDP runs on all Cisco-manufactured equipment over the data link layer and does the following:

- Advertises information to all attached Cisco devices.
- Discovers and views information about those Cisco devices.
    - CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.

Note If you disable CDP globally, CDP is also disabled for all interfaces.

For more information about CDP, see the *Cisco Nexus 1000V System Management Configuration Guide*.

DHCP Not Supported for the Management IP

DHCP is not supported for the management IP. The management IP must be configured statically.

Upstream Switch Ports

We recommend that you configure spanning-tree port type edge on upstream switches for faster convergence.

The following commands are available to use on Cisco upstream switch ports in interface configuration mode:

- spanning-tree portfast
- spanning-tree portfast trunk
- spanning-tree portfast edge trunk

Interfaces

When the maximum transmission unit (MTU) is configured on an operationally up interface, the interface goes down and comes back up.

Supported MTU values vary according to underlying physical NIC capability.

Layer 3 VSG

When a VEM communicates with the Cisco VSG in Layer 3 mode, an additional header with 94 bytes is added to the original packet. You must set the MTU to a minimum of 1594 bytes to accommodate this extra header for any network interface through which the traffic passes between the Cisco Nexus 1000V and the Cisco VSG. These interfaces can include the uplink port profile, the proxy ARP router, or a virtual switch.

Copy Running-Config Startup-Config Command

When you are using the **copy running-config startup-config** command, do not press the PrtScn key. If you do, the command aborts.

SNMP User Accounts Must Be Reconfigured After an Upgrade

If you are upgrading from a release earlier than 5.2(1)SV3(1.5), the SNMP engine ID changes internally to a unique engine ID. You must reconfigure all the SNMP user accounts to work with the new engine ID. Until the SNMP user accounts are reconfigured, all SNMPv3 queries fail. This restriction is associated with the defect CSCuo12696 and CSCvb16199.

After an upgrade, use the **show snmp user** command to view the engine ID:

```
switch# show snmp user
_____________________________________________________________________
SNMP USERS
_____________________________________________________________________

User Auth Priv(enforce) Groups
____ ____ _____________ ______
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________

User Auth Priv
____ ____ ____
admin md5 des
(EngineID 128:0:0:9:3:2:0:12:0:0:0)
```

Complete the following steps to reconfigure SNMP user accounts. Reconfiguring an SNMP user account involves deleting and recreating a new SNMP username and password. Note that *paswd123* is an example that represents the SNMP user password.

Procedure

Step 1 Delete the username. For example:

```
switch(config)#no snmp user admin auth md5 paswd123 engineID 128:0:0:9:3:2:0:12:0:0:0
```

Step 2 Use one of the following options to recreate the SNMP username and password. For example:

- Option 1

  ```
  switch(config)# snmp user admin auth md5 paswd123
  ```

- Option 2

```
switch(config)# snmp-server user admin auth md5 paswd123 priv aes-128 paswd123
```

Step 3 Confirm that the engine ID has been updated. For example:

- Option 1

```
switch# show snmp user
_____________________________________________________________________
SNMP USERS
_____________________________________________________________________
User Auth Priv(enforce) Groups
____ ____ _____________ ______
admin md5 no network-operator
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
```

- Option 2

```
switch(config)# show snmp user
_____________________________________________________________________
SNMP USERS
_____________________________________________________________________
User Auth Priv(enforce) Groups
____ ____ _____________ ______
admin md5 aes-128(no) network-operator
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
```

Step 4 Verify that the engine ID is unique. For example:

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903005056A0544E
[Dec] 128:000:000:009:003:000:080:086:160:084:078
```

Viewing the Distributed Virtual Switch Version in the VMware vSphere Web Client GUI

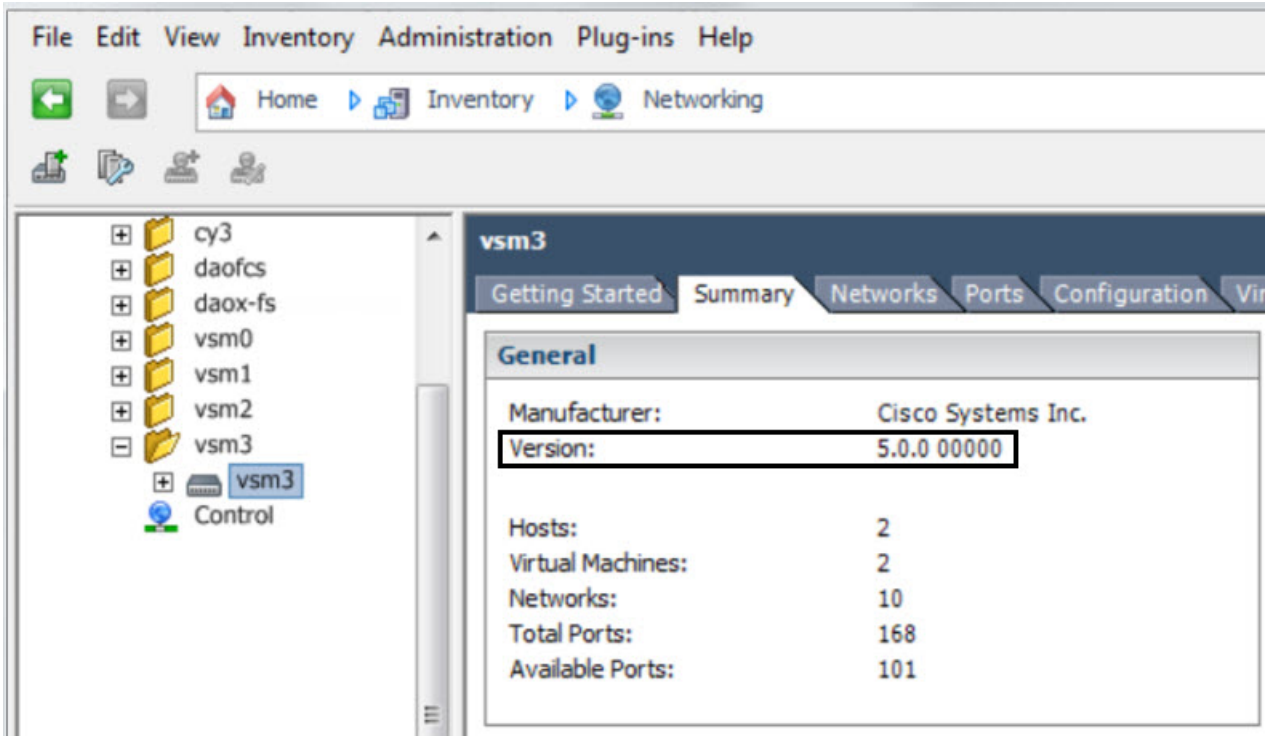
You can use the VMware vSphere Web Client GUI to view which distributed virtual switch (DVS) version you are using.

Procedure

Step 1 Log in to the VMware vSphere Web Client.

Step 2 Under **Home** > **Inventory** > **Networking**, expand the data center folder and select the DVS.

Step 3 Click the **Summary** tab; the DVS version is displayed in the **General** area. For example:



Viewing the Distributed Virtual Switch Version in the Virtual Supervisor Module CLI

You can use the Virtual Supervisor Module (VSM) CLI to view which DVS version you are using.

Procedure

Step 1 Log in to the VSM CLI in EXEC mode.

Step 2 Enter the **show svs connections** command.

Step 3 The command output shows the DVS version; for example:

```
switch# show svs connections

connection vc:
    hostname: -
    ip address: 10.197.135.64
    ipv6 address: -
    remote port: 80
    transport type: ipv4
    protocol: vmware-vim https
    certificate: default
    datacenter name: dc1
    admin:
    max-ports: 12000
    DVS uuid: 50 1a bb c1 3a 92 00 ce-72 8f 4e 91 40 48 b1 f0
    dvs version: 5.0.0
    config status: Enabled
    operational status: Connected
    sync status: Complete
```

```
    version: VMware vCenter Server 6.5.0 build-4944578
    vc-uuid: 9bc4215b-e927-4701-8173-9fede105fcda
    ssl-cert: self-signed or not authenticated
sv331_812_ip_155#

switch#
```

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.

Procedure

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 In the Log In screen, enter your registered Cisco.com username and password, and 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 **Enter**.

Step 4 To search for bugs in the current release:

a) In the Search For field, enter **Cisco Nexus 1000V for VMware** and press **Enter**. (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 status, severity, modified date, and so forth.

Tip To export the results to a spreadsheet, click the **Export Results to Excel** link.

Open Bugs

The following table lists the bug ID and description of open bugs that apply to the Cisco Nexus 1000V for VMware Release 5.2(1)SV3(3.15).

Bug ID	Description
CSCvd48465	ISE SXP connection resets while adding a new SXP peer on VSM in the *BOTH* mode.
CSCva18884	The first SXP IPSGT entry is not getting pushed to VEMs post upgrade.
CSCvd62497	DCPN case 44221(vSphere6.5a) - Module not coming online post reboot of a stateless host.

Resolved Bugs

The following table lists the bug ID and description of a select number of resolved high-priority bugs in the Cisco Nexus 1000V for VMware Release 5.2(1)SV3(3.15).

Bug ID	Description
CSCuu85149	PSOD occurs during hot swap operation.
CSCuv61358	Cisco Nexus 1000v ARP Denial of Service (DoS) Vulnerability.
CSCux56196	NTP does not restrict passive associations on Cisco Nexus 1000v.
CSCux56266	The **`ntp authenticate`** option should be enabled by default on Cisco Nexus 1000v.
CSCuw02034	Cisco NX-OS Malformed ARP Header Vulnerability.
CSCux06540	Error message when configure DNS related command under management VRF.
CSCux95103	Evaluation of Cisco Nexus 1000V for NTP January 2016.
CSCuz44149	Evaluation of Cisco Nexus 1000V for NTP April 2016.
CSCuz92663	Evaluation of Cisco Nexus 1000V for NTP June 2016.
CSCva13732	The **debug snmp req-latency-time** command on Nexus 1000V gives misleading output.
CSCvb16199	Command to reset SNMP v3 engineID required.
CSCuz38798	Adding any VLAN to uplink causes `vlan misconfig syslogs` error.
CSCvb48570	Evaluation of Cisco Nexus 1000V for NTP September 2016.
CSCvb68247	Using control0 Interface as L3 Control does not work.
CSCvd72174	Evaluation of nexus-1000v for NTP March 2017.
CSCve62810	Cisco Nexus 1000v CLI command injection vulnerability.
CSCvf52749	VSM internal file system gets filled up due to high volume of PNSC, and VSM web accesses.
CSCve11609	Nexus 1000v Unsupported OpenSSL version < 1.0.1

Accessibility Features in Cisco Nexus 1000V

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

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 Series switch.

The MIB Support List is available at the following FTP site:
ftp://ftp.cisco.com/pub/mibs/supportlists/nexus1000v/Nexus1000VMIBSupportList.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.

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. RSS feeds are a free service.