# Cisco Nexus 1000V Release Notes, Release 4.2(1)SV2(2.1)

**Last Updated: 2014-02-27**
**Release: NX-OS Release 4.2(1)SV2(2.1)**

This document describes the features, limitations, and bugs for the Cisco Nexus 1000V Release 4.2(1)SV2(2.1) software. The following is the change history for this document.

| Date | Description |
|---|---|
| 2014-02-27 | Added CSCum99528 to Platform, Infrastructure, Ports, Port Channel, and Port Profiles, page 12. |
| 2013-09-19 | Added support for vSphere 5.5 in Software Compatibility with VMware, page 2 and added VXLAN Offload, page 4. |
| 2013-09-12 | Updated the value of Active VLANs and VXLANs across all VEMs in Table 1. |
| 2013-09-03 | Updated the supported limit for vEthernet interfaces per port profile in Table 1 and added CSCug48013 in Resolved Bugs, page 16. |
| 2013-08-12 | Added Extending VEMs for Centralized Management of Data Centers and Branch Offices, page 4. |
| 2013-08-01 | Updated LACP, page 9 and added Upstream Switch Ports, page 9. |
| 2013-07-19 | Added CSCug23327 in Resolved Bugs, page 16. |
| 2013-06-22 | Created release notes for Release 4.2(1)SV2(2.1). |

**Cisco Systems, Inc.**
www.cisco.com

# 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 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 two 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.

# 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, 5.1, and 5.0 release trains. For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information*.

**Note** All virtual machine network adapter types that VMware vSphere supports are supported with the Cisco Nexus 1000V. 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)SV1(4) and later releases. For additional information, see the *Cisco Nexus 1000V Software Upgrade Guide*.

# New Information

The following software features were added in Cisco Nexus 1000V Release 4.2(1)SV2(2.1):



## VXLAN 1.5

A VXLAN supports two different modes for flood traffic:

- Multicast mode—A VXLAN uses an IP multicast network to send broadcast, multicast, and unknown unicast flood frames. Each multicast mode VXLAN has an assigned multicast group ID address. When a new VM joins a host in multicast mode VXLAN, VEM joins the assigned multicast group ID address by sending IGMP join messages. Flood traffic, that is broadcast, multicast and unknown unicast, from the VM is encapsulated and is sent using the assigned multicast group IP as destination IP address. Packets sent to known unicast MAC address are encapsulated and sent directly to the destination server VTEP IP addresses.
- Unicast-only mode—A VXLAN uses each VEM's single unicast IP address as the destination IP address to send broadcast, multicast, and unknown unicast flood frames of designated VTEP on each VEM that has at least one VM in the corresponding VXLAN. When a new VM joins the host in unicast-mode VXLAN, a designated VTEP is selected for receiving flood traffic on that host. This designated VTEP is communicated to all other hosts through the VSM. Flood traffic, that is broadcast, multicast and unknown unicast, is replicated on each VEMs designated VTEP in that VXLAN by encapsulating it with a VXLAN header. Packets are sent only to VEMs with a VM in that VXLAN. Packets that have an unicast MAC address are encapsulated and sent directly to the destination servers VTEP IP address.
  - MAC distribution mode (supported only in unicast mode)—In this mode, the unknown unicast flooding in the network is eliminated. Virtual Supervisor Module (VSM) learns all the mac-addresses from VEMs in all VXLANs and distributes those MAC addresses with VTEP IP mappings to other VEMs. Hence, there is no unknown unicast mac-address in the network when VMs on VEMs are communicating and controlled by same VSM.

## VXLAN Gateway

VXLAN termination (encapsulation and decapsulation) is supported only on virtual switches. As a result, the only endpoints that can connect into VXLANs are VMs that are connected to a virtual switch. Physical servers cannot be in VXLANs and routers or services that have traditional VLAN interfaces cannot be used by VXLAN networks. The only way that VXLANs can currently interconnect with traditional VLANs is through VM-based software routers.

The VXLAN gateways supported are as follows:

- VMware vShield Edge
- Cisco VXLAN gateway

- Cisco ASA1000V

The configuration for such VXLAN-VLAN translation/mappings for the VXLAN gateway must be configured through the VSM and must always be a 1:1 mapping for each Layer 2 domain. Each VXLAN gateway can support multiple VXLAN-VLAN mappings.

## VXLAN Trunks

A VXLAN trunk allows you to trunk multiple VXLANs on a single virtual Ethernet interface. In order to achieve this configuration, you must encapsulate a VXLAN-VLAN mapping on the virtual Ethernet interface.

VXLAN-VLAN mappings are configured through the VSM and must always be a 1:1 mapping for each Layer 2 domain. VXLAN-VLAN mappings are applied on a virtual Ethernet interface using a port-profile. A single port profile can support multiple VLAN-VXLAN mappings.

## VXLAN Offload

The Cisco Nexus 1000V supports offloading VXLAN checksum and TSO computations of inner packets for VXLAN encapsulated packets. The VXLAN offload feature is supported only if an adapter supports the offload feature and the VMware supports the offload feature on that adapter. For more information, see the *Cisco Nexus 1000V VXLAN Configuration Guide*.

## Multi-MAC Capability

You can use multi-MAC addresses to mark a virtual Ethernet interface as capable of sourcing packets from multiple MAC addresses. For example, you can use this feature if you have a virtual Ethernet port and you have enabled VXLAN trunking on it and the VM that is connected to the port bridges packets that are sourced from multiple MAC addresses.

By using this feature, you can easily identify such multi-MAC capable ports and handle live migration scenarios correctly for those ports.

## Extending VEMs for Centralized Management of Data Centers and Branch Offices

To facilitate a centralized management environment, it is possible to have the VSM at a central location in the main Data Center, while the VEMs are spread across different branch locations. The maximum latency recommended between VSMs and VEMs in such cases should be 100 ms.

# Limitations and Restrictions

This section describes the Cisco Nexus 1000V limitations and restrictions.

# Configuration Limits

Table 1 lists the Cisco Nexus 1000V configuration limits.

***Table 1 Configuration Limits for Cisco Nexus 1000V***

| Component | Supported Limits for a Single Cisco Nexus 1000V Deployment Spanning up to 2 Physical Data Centers |
|---|---|
| Maximum Modules | 130 |
| Virtual Ethernet Module (VEM) | 128 |
| Virtual Supervisor Module (VSM) | The VSMs can be placed in different physical data centers.<br>Note that the previous restrictions requiring the active-standby VSMs in a single physical data center do not apply anymore. |
| Hosts | 128 |
| Active VLANs and VXLANs across all VEMs | 2048 VLANs and 2048 VXLANs (with a combined maximum of 4096) |
| MACs per VEM | 32000 |
| MACs per VLAN per VEM | 4096 |
| vEthernet interfaces per port profile | 1024 (without **static auto expand** port binding)<br>Same as DVS maximum (with **static auto expand** port binding) |
| PVLAN | 512 |
| Distributed Virtual Switches (DVS) per vCenter with VMware vCloud Director (vCD) | 32 |
| DVS per vCenter without vCD | 32 |
| vCenter Server connections | 1 per VSM HA pair<br>Only one connection to vCenter server is permitted at a time. |
| Maximum latency between VSMs and VEMs | 100 ms |

*Table 1 Configuration Limits for Cisco Nexus 1000V (continued)*

| Component | Supported Limits for a Single Cisco Nexus 1000V Deployment Spanning up to 2 Physical Data Centers (continued) | |
|---|---|---|
| | Per DVS | Per Host |
| vEthernet interfaces | 4096 | 300[1] |
| Port profiles | 2048 | — |
| System port profiles | 32 | 32 |
| Port channel | 512 | 8 |
| Physical trunks | 512 | — |
| Physical NICs | — | 32 |
| vEthernet trunks | 256 | 8 |
| ACL | 128 | 16<br>This number can be exceeded if the VEM has available memory. |
| ACEs per ACL | 128 | 128 |
| ACL instances | 4096 | 300 |
| NetFlow policies | 32 | 8 |
| NetFlow instances | 256 | 32 |
| SPAN/ERSPAN sessions | 64 | 64 |
| QoS policy map | 128 | 16 |
| QoS class map | 1024 | 128 |
| QoS instances | 4096 | 300 |
| Port security | 2048 | 216 |
| Multicast groups | 512 | 512 |

1. Upgrade from an earlier version of Cisco Nexus 1000V software to the current version of Cisco Nexus 1000V software displays the maximum vEth ports as 216. To get the current supported vEth limit, remove the host from DVS and add the host again.

# Single VMware Data Center Support

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

# VMotion of VSM

VMotion of the VSM has the following limitations and restrictions:

- VMotion of a 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 virtual machines 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 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.

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

# Access Lists

ACLs have the following limitations and restrictions.

### Limitations:

- IPV6 ACL rules are not supported.
- VLAN-based ACLs (VACLs) are not supported.
- ACLs are not supported on port channels.

### Restrictions:

- IP ACL rules do not support the following:
  - fragments option
  - addressgroup option
  - portgroup option
  - interface ranges
- Control VLAN traffic between the VSM and VEM does not go through ACL processing.

# NetFlow

The NetFlow configuration has the following support, limitations, and restrictions:

- Layer 2 match fields are not supported.
- NetFlow Sampler is not supported.
- NetFlow Exporter format V9 is supported
- NetFlow Exporter format V5 is not supported.
- The multicast traffic type is not supported. Cache entries are created for multicast packets, but the packet/byte count does not reflect replicated packets.
- NetFlow is not supported on port channels.

The NetFlow cache table has the following limitation:

- Immediate and permanent cache types are not supported.

**Note** The cache size that is configured using the CLI defines the number of entries, not the size in bytes. The configured entries are allocated for each processor in the ESX host and the total memory allocated depends on the number of processors.

# Port Security

Port security has the following support, 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.
- The port security violation actions that are supported on a secure port are **Shutdown** and **Protect**. The **Restrict** violation action is not supported.
- Port security is not supported on the PVLAN promiscuous ports.

# Port Profiles

Port profiles have the following restrictions or limitations:

- There is a limit of 255 characters in a **port-profile** command attribute.
- We recommend that you save the configuration across reboots, which shortens the VSM bringup time.
- We recommend that if you are altering or removing a port channel, you migrate the interfaces that inherit the port channel port profile to a port profile with the desired configuration. Do not edit the original port channel port profile directly.
- If you attempt to remove a port profile that is in use (hat is, one that has already been auto-assigned to an interface), the Cisco Nexus 1000V generates an error message and does not allow the removal.
- 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.

# SSH Support

Only SSH version 2 (SSHv2) is supported.

For information, see the *Cisco Nexus 1000V Security Configuration Guide*.

# 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.

For information, see the *Cisco Nexus 1000V Command Reference*.

## Layer 2 Switching: No Spanning Tree Protocol

The Cisco Nexus 1000V forwarding logic is designed to prevent network loops so it does not need to 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.

For information about Layer 2 switching, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide*.

## 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.

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.

## LACP

The Link Aggregation Control Protocol (LACP) is an IEEE standard protocol that aggregates Ethernet links into an EtherChannel.

The Cisco Nexus 1000V has the following restrictions for enabling LACP on ports carrying the control and packet VLANs:

**Note** These restrictions do not apply to other data ports using LACP.

- If LACP offload is disabled, at least two ports must be configured as part of LACP channel.

**Note** This restriction does not apply if LACP offload is enabled. You can check the LACP offload status by using the **show lacp offload status** command.

- The upstream switch ports must be configured in **spanning-tree port type edge trunk** mode.

## Upstream Switch Ports

All upstream switch ports must be configured in **spanning-tree port type edge trunk** mode.

Without spanning-tree PortFast on upstream switch ports, it takes approximately 30 seconds to recover these ports on the upstream switch. Because these ports are carrying control and packet VLANs, the VSM loses connectivity to the VEM.

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**

## DNS Resolution

The Cisco Nexus 1010 (1000V) cannot resolve a domain name or hostname to an IP address.

## Interfaces

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

## Layer 3 VSG

When a VEM communicates with 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 running the **copy running-config startup-config** command, do not press the PrtScn key. If you do, the command will abort.

## Dynamic Entries Are Not Deleted for a Linux VM

On a Linux VM that has multiple adapters, a DHCP release packet is sent from an incorrect interface (because of OS functionality) and the DHCP release packet is dropped. As a result, the binding entry is not deleted. This issue is a Linux issue where the packets from all interfaces go out of one interface (which is the default interface). To avoid this issue, put the interfaces in different subnets and make sure that the default gateways for each interface is set.

## Source Filter TX VLANs Are Missing After the VSM Restarts

When a SPAN (erspan-source) session is created and the source interface is configured as a port channel and PVLAN Promiscuous access is programmed, the filter RX is not configured and the configured programmed filter TX is not persistent on VSM reload.

To work around this issue, configure all the primary and secondary VLANs as filter VLANs while using the port channel with PVLAN Promiscuous access as the source interface.

## Default SSH Inactive Session Timeout

The default SSH inactive session timeout is 30 minutes, but the timeout setting is disabled by default, so the connection remains active. The **exec-timeout** command can be used to explicitly configure the inactive session timeout limit.

## Queueing Policy Cannot Be Changed in Flexible Upgrade Setup

Queuing is valid starting from Cisco NX-OS Release 4.2(1)SV1(5.1). Any queueing configuration that exists on the VSM in an earlier release will stop working. All port profiles that have a queueing configuration cannot be used. If a port is down, it should be moved to a profile without QoS queueing.

## Clear QoS Statistics Fails on the VSM

When a policy map of type “queuing” has a class map of type “match-any” without any match criteria, and is applied on an interface, a resource pool is not created for that specific class ID. As a result, the collection of statistics fails and no data is sent back to the VSM. To work around this issue, add a match criteria on the empty class map.

# Bugs

This section includes the following topics:



## Open Bugs

The following are descriptions of the bugs in Cisco Nexus 1000V Release 4.2(1)SV2(2.1). The IDs are linked to the Cisco Bug Search tool.

### VXLAN Gateway

| ID | Headline |
|---|---|
| CSCui27814 | Port channel is down after **shut** or **no shut** command on uplink port-profile of VXLAN gateway. |
| CSCug95878 | The **Show process CPU** command does not show the same result for vssnet. |
| CSCuh17360 | Start_cnt for vssnet does not change after restarting. |

| ID | Headline |
|---|---|
| CSCug73194 | Configuration fails on port-profile inherited by VTEPs on VEM and VXLAN gateway. |
| CSCug92356 | The **show module** command does not display updated VXLAN gateway management IP address. |
| CSCuh20704 | There are no OVA files for gateway to do the deployment as a VSB on a VSA. |
| CSCug93645 | The **attach module gateway** command hangs if VSM is on Layer 3 through control interface. |
| CSCug33235 | VXLAN gateway goes offline on the VSM before it returns to attach when running multicast traffic. |
| CSCug67857 | The **show cdp neighbors** command on VSM or VLXLAN gateway does not show details of upstream for VXGW module. |
| CSCuh17978 | The **show process** command does not display the reason for crash. |
| CSCuh24446 | In high traffic scenarios there is a possibility that IGMP-Query packets may be queued behind data packets. This can cause IGMP-Join(s) not to be sent for the corresponding VXLAN segments hence causing traffic to fail for unknown-unicast/multicast/broadcast. |
| CSCuh41892 | You will see the VSM and gateway out-of-sync after you reload the VSM after changing the port-profile. |
| CSCuh48661 | Gateway module fluctuates when traffic flows with varied 1000 SMAC ICMP traffic. |
| CSCuh52879 | System log messages not going to external system log server from gateway. |
| CSCuh53773 | Existing traffic drops when converting mappings to VXLAN 1.0. |
| CSCuh38606 | VXLAN gateway port-channel goes down when attaching to the VSM. |
| CSCuh40181 | Unable to deploy VXLAN gateway VSB using the **enable properties** command on Cisco N1010. |
| CSCud87990 | Output for certain fields are missing for **vemcmd show card** command output in the VXLAN gateway. |
| CSCuh53503 | When you deploy VXLAN gateway, the MAC address entered will not get validated for proper syntax. |

## Platform, Infrastructure, Ports, Port Channel, and Port Profiles

| ID | Headline |
|---|---|
| CSCti98977 | Not able to migrate VC/VSM and normal VM when adding host to DVS. |
| CSCtj70071 | SNMP V3 traps are not getting generated. |
| CSCtn62514 | LACP offload configuration is not persisting in stateless mode. |
| CSCtq92519 | CDP does not work for certain NIC cards without VLAN 1 allowed. |
| CSCtr34519 | Continuous SNMP polling causes high CPU usage. |

| ID | Headline |
|---|---|
| CSCts24105 | The **load-interval counter** command configuration is not working. |
| CSCtt17073 | A port profile through VCD fails when done immediately after a switchover. |
| CSCtt24735 | Editing a port profile fails with the error message “ERROR: unknown error.” |
| CSCtz04587 | Reloading the VSM takes 12 minutes for modules to come online and vEthernet interfaces to come up |
| CSCtw96064 | The **show tech-support dvs** command does not have output related to DHCP snooping. |
| CSCtx06864 | A native VLAN configured on the interface port channel is not programmed on the VEM. |
| CSCtx30435 | After upgrading the VEM to Cisco NX-OS Release 4.2(1)SV1(5.1), two Cisco VIBs are installed. |
| CSCua00940 | PPM does not perform configuration checks when you configure a PVLAN in an offline port-profile mode. |
| CSCua02145 | “SYSMGR_EXITCODE_FAILURE_NOCALLHOME” error message received while upgrading with ISO images from Release 4.2(1)SV1(4) or 4.2(1)SV1(4a) to Release 4.2(1)SV1(5.2). |
| CSCua16092 | If you add a PVLAN promiscuous trunk port channel or Ethernet interface as the SPAN/ERSPAN source, some of the VLANs allowed on the port might not be spanned. |
| CSCua30287 | An error occurs while trying to override the PVLAN mapping in the child port profile. |
| CSCua73549 | Modules are not reattached after a VMKnic MAC address change in Layer 3 mode. |
| CSCub23161 | VCD does not display relevant error descriptions for error codes. |
| CSCub25986 | NSM should fix the Cisco Nexus 1000V feature limitation issue. |
| CSCub33444 | Powering up a single VM configures all vApp networks. |
| CSCub69289 | Veths mapped to the port profiles are not counted in the **show resource-availability monitor** command. |
| CSCub79332 | The server IP address becomes 0.0.0.0 for a MN stateless host. |
| CSCuc63801 | Traffic loss occurs after the VSM reloads if PSEC is restricted and the DSM bit is set. |
| CSCug25018 | You cannot process large number of IGMP queries from the upstream switch on Cisco Nexus 1000V. |
| CSCuf89892 | VEM doesn't increase the number of maximum ports after an upgrade to the current version of Cisco Nexus 1000V. |
| CSCue17860 | snmpwalk does not return values of SyslogServer objects. |
| CSCue77534 | Internal VLANs (3968-4047) are being trunked to configure on ports. |
| CSCug23565 | Downloading the files from VSM configuration with IPV6 throws an error. |

| ID | Headline |
|---|---|
| CSCug36502 | When the VSM is setup with an IPv6 address and accessed, the server drops or resets the connection randomly causing multiple issues. |
| CSCug66317 | When trying to install a license file, installation fails with a error message “file already exists” and license file is not installed. |
| CSCuc75590 | When plan mappings are configured on the port-channel interface directly, the mappings are incorrect on the VEM. |
| CSCug51163 | VEM upgrade from previous releases of Cisco Nexus 1000V software to the current release of Cisco Nexus 1000V software fails. |
| CSCue50621 | ifHCInOctets and ifInOctets wrap while taking snapshot of virtual machines. |
| CSCug36191 | SNMP times out when browsing the entire tree or the CISCO-PROCESS-MIB. |
| CSCug10319 | When you select the Install VIB option, the installer checks for the SVS Connection and list the hosts in host selection page to proceed to VEM Install. |
| CSCuh20779 | When you deploy a gateway as VSB, you are asked to enter the VSMs domain ID. For gateway, we do not need the domain ID. |
| CSCue06575 | Unable to create DVportgroup during bulk VMotion. |
| CSCuh52327 | ISSU upgrade compatibility table is not modified to accommodate VXLAN gateway. |
| CSCuh52373 | The **show install service-module** command does not display the service module ISSU status. |
| CSCum99528 | IP address configuration on interface control0 is not persistent upon VSM reload. |

## Quality of Service

| ID | Headline |
|---|---|
| CSCtu36119 | QoS marking limitation in VCD environment. |

## Features

| ID | Headline |
|---|---|
| CSCtk65252 | PSEC with multiple MAC addresses and PVLAN not supported. |
| CSCtl04632 | Port migration with switchover causing ports to go to “No port-profile.” |
| CSCtr06833 | Split brain causes pending ACL/QoS transactions into err-disabled. |

| ID | Headline |
|---|---|
| CSCtr09746 | Interface configuration fails when veths are nonparticipating due to unreachable module. |
| CSCub44964 | A RADIUS AAA error occurs when feature CTS is enabled and there is a switchover. |
| CSCue36581 | Copy run start takes 8 to 10 minutes to complete the copy. |
| CSCug85914 | The **show bridge-domain vteps** command shows the IP even after removing the veth. |
| CSCug72814 | When ACL deny is applied on mgmt0 to block http and https, ACL counters are not incremented but HTTP and HTTS is blocked as expected. |
| CSCug72823 | When ACL applied to mgmt interface is changed, IP tables adds entries to existing tables without clearing and rebuilding as per the new ACL causing incorrect filtering. |
| CSCug74311 | VTEP IP stuck in VTEP list after a headless VEM reconnects to the VSM. |
| CSCuh08385 | ACL does not work on IGMP version 2 and v3. |
| CSCuh11701 | The **no acllog match-log-level <level>** command does not reset the ACL logging level to the default value. |
| CSCug07730 | The vethPerHostUsed field is displaying the same value as the vethUsed field in the XML response for http://vsm_ip/api/vc/limits API. It should display the number of Veths on the host with the maximum used Veths. |
| CSCuh11779 | Incorrect default value is shown for max-deny flows and max-permit flows. |

## VMware

| ID | Headline |
|---|---|
| CSCui80024 | ESXi 5.5 Bandwidth allocated for a queue is not as expected on congestion. |
| CSCuj19963 | When ESX is upgraded to vSphere 5.5, Mellanox NICs get policy mismatch. |
| CSCuj26459 | When ESX is upgraded to vSphere 5.5, the Host management connectivity is lost. |
| CSCuj19983 | CDN NIC gets previous port policy after reboot. |
| CSCti34737 | Removing host with Intel Oplin from DVS causes all ports to reset. |
| CSCtk02322 | After an ESX host exception, the port group configuration on PNIC is changed. |
| CSCtk07337 | Fully qualified domain name/user with port-profile visibility fails. |
| CSCtk10837 | Port-profile visibility feature is not able to update permissions. |
| CSCtk53802 | Improper sync with vCenter when port-profile names have special characters. |

| ID | Headline |
|---|---|
| CSCts80394 | A VEM upgrade fails when the scratch space is a network file system. |
| CSCtt00444 | After unregistering Cisco Nexus 1000V on Vshield, the alert timer runs. |
| CSCua30356 | An existing vAPP cannot be powered down, and a new vAPP cannot be deployed. |
| CSCub56123 | Wrong message for VC user id and Password. |
| CSCuc71793 | Ports go to error disabled state during ACL or QoS Commit Errors. |
| CSCuc75398 | App fail power on with insufficient resource error. |
| CSCuc80063 | IGMP process failing to read PVLAN association. |

# Resolved Bugs

The following are descriptions of bugs that are resolved in Cisco Nexus 1000V Release 4.2(1)SV2(2.1). The IDs are linked to the Cisco Bug Search tool.

| ID | Headline |
|---|---|
| CSCug48013 | Increase TCP Idle Timeout in vPath to 2 minutes. |
| CSCug23327 | SNMP Fails with Community String ACL. |
| CSCti39155 | Need to send traffic from the destination VM to learn the vns-binding. |
| CSCtq04886 | Eth_port_sec crash occurs during migration in VC with interface override in VSM. |
| CSCtr36181 | Integrate Apache with netstack. |
| CSCtr55311 | Legacy LACP takes 30 minutes to come up after a link flap. |
| CSCts50066 | Post module flap violated port is secured and the secured port is violated. |
| CSCtt07479 | A port profile configured with the **port-binding static auto** command reserves more than the default ports. |
| CSCtu10144 | A virtual Ethernet interface as trunk has pinning issue in MN ESX hosts. |
| CSCtu17512 | The Cisco Nexus 1000V to vShield Manager connection is down after release of VCD, DB, VSM.<br>**Note** Only applicable with VMware vCloud Director 1.5.1 and vShield Manager 5.0.1. |
| CSCtw93579 | Active VSMs CPU utilization is more than 50% when there are 512 groups. |
| CSCty59712 | If you add a primary PVLAN as the SPAN/ERSPAN source, its promiscuous trunk members are not added to the SPAN session. |

| ID | Headline |
|---|---|
| CSCua06287 | Incorrect mapping for ethernet port profile with PVLAN configuration is displayed in the running configuration. |
| CSCua11227 | Cannot copy the running configuration from the TFTP server to the current running configuration. |
| CSCua12342 | A Link Aggregation Control Protocol (LACP) port channel member port goes to the suspended state when the port is newly added to the LACP port channel, or the port is removed and re-added to the LACP port channel. |
| CSCua12592 | Password validity is not checked when installing a VSM using an OVA installation. |
| CSCua59482 | Traffic is being redirected to the incorrect VSG. |
| CSCub90212 | SPAN sources are deleted on the VEM output while adding the source interfaces. Duplicated by CSCtz82836. |
| CSCuc58678 | The installer displays an error when a host with multiple VMKnics in the same VLAN is migrated. |
| CSCuc49513 | The **show processes cpu history** command output has the graphing backwards. |
| CSCtl00949 | Configuring child with **no service policy** command is causing inherit to fail. |
| CSCtq34938 | Applying policy fails sharing ACL between two class-maps of same policy. |
| CSCty78076 | VEM upgrade error occurs when using VMware Update Manager. |
| CSCua40492 | When the VEM is disconnected from the VSM (headless mode), the maximum number of vEthernet interfaces limit cannot be connected. |
| CSCua78262 | The incorrect release description name and release note URL is displayed with the ESX/ESXi 4.1.0 offline bundle. |
| CSCub90212 | Span sources gets deleted on VEM output while adding source intfs. |

# 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, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/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.