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

Release Date: March 4, 2014
Part Number: OL-30273-01
Current Release: NX-OS Release 4.2(1)SV2(2.1a)

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

Part Number	Revision	Date	Description
OL-30273-01	A1	February 27, 2014	Added caveat CSCum99528 to section Platform, Infrastructure, Ports, Port Channel, and Port Profiles.
OL-30273-01	A0	October 16, 2013	Created release notes for Release 4.2(1)SV2(2.1a).

Contents

This document includes the following sections:

- Introduction, page 2
- Software Compatibility, page 2
- New and Changed Information, page 2
- Limitations and Restrictions, page 3
- Caveats, page 10
- Related Documentation, page 16
- Obtaining Documentation and Submitting a Service Request, page 18

Cisco Systems, Inc.
www.cisco.com

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

This section includes the following topics:

- Software Compatibility with VMware, page 2
- Software Compatibility with Cisco Nexus 1000V, page 2

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 and Changed Information

This section provides the following information about Cisco Nexus 1000V Release 4.2(1)SV2(2.1a):

- New Software Features, page 3

New Software Features

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

- vCenter Server Certificate Validation, page 3
- VXLAN Gateway Upgrade, page 3

vCenter Server Certificate Validation

The Cisco Nexus 1000V VSM can validate the certificate presented by vCenter Server to authenticate it. The certificate may be self-signed or signed by a Certificate Authority (CA). The validation is done each time the VSM connects to the vCenter Server. If the certificate authentication fails, a warning is generated but the connection is not impaired. This is an optional feature.

VXLAN Gateway Upgrade

The Cisco Nexus 1000V VXLAN supports upgrading the VXLAN gateway through VSM. The following commands are added for VXLAN upgrade feature.

Command	Description
vsm# **install service-module kickstart bootflash:** *kickstart image* **system bootflash:** *system image* **module-num** *3–130*	Upgrades a VXLAN gateway service module (standalone) by using the kickstart and system image. The module number range is from 3 to 130.
vsm# **install service-module iso bootflash:***iso image* **module-num** 3–130	Upgrades a VXLAN gateway service module (standalone) by using the iso image. The module number range is from 3 to 130.
vsm# **install service-module kickstart bootflash:** *kickstart image* **system bootflash:** *system image* **cluster-id** *1–8*	Upgrades a VXLAN gateway high availability (HA) cluster by using the kickstart and system image. The cluster ID range is from 1 to 8.
vsm# **install service-module iso bootflash:***iso image* **cluster-id** *1–8*	Upgrades a VXLAN gateway HA cluster by using the iso image. The cluster ID range is from 1 to 8.

For detailed information about upgrading the VXLAN gateway, see *Cisco Nexus 1000V VXLAN Configuration Guide, Release 4.2(1)SV2(2.1a)*.

Limitations and Restrictions

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

Configuration Limits

Table 1 shows 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. 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) Same as DVM maximum (with **static auto expand** port binding)
PVLAN	512
Distributed Virtual Switches (DVS) per vCenter with VMware vCloud Director (vCD)	32
Distributed Virtual Switches (DVS) per vCenter without VMware vCloud Director (vCD)	32
vCenter Server connections	1 per VSM HA Pair[1]
Maximum latency between VSMs and VEMs	100ms

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[2]
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[3]
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. Only one connection to vCenter server is permitted at a time.
2. 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.
3. This number can be exceeded if VEM has available memory.

Single VMware Data Center Support

The Cisco Nexus 1000V can be connected to a single VMware vCenter Server datacenter object. Note that this virtual datacenter can span across 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 will shorten the VSM bringup time.
- 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.
- If you attempt to remove a port profile that is in use, that 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 more 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 about CLI commands, see the *Cisco Nexus 1000V Command Reference*.

Layer 2 Switching

This section lists the Layer 2 switching limitations and restrictions and includes the following topics:

- No Spanning Tree Protocol, page 8

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

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.

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 is not applicable 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. For more information about this restriction, see Upstream Switch Ports, page 9.

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, having a class-map of type "match-any" without any match criteria, 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.

Caveats

This section includes the following topics:

- Open Caveats, page 10
- Resolved Caveats, page 16

Open Caveats

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

The caveats are listed in the following categories:

- VXLAN Gateway, page 11
- Platform, Infrastructure, Ports, Port Channel, and Port Profiles, page 12
- Quality of Service, page 14
- Features, page 14

- VMware, page 15

VXLAN Gateway

	ID	Open Caveat Headline
1.	CSCuj31300	VXLAN gateway restarts or freezes when bridging traffic with unique source MAC addresses.
2.	CSCug33235	Multicast data traffic through VXLAN gateway not supported in VXLAN unicast-only mode.
3.	CSCuj33904	Related flows retained after removing VLAN:VXLAN mapping.
4.	CSCuj50237	VXLAN gateway module flaps when the VTEP IP address is changed in VSM.
5.	CSCuh24446	LACP packets not received on the VXLAN gateway VSB for higher than 260 Kbps traffic.
6.	CSCuh26605	Throughput decreases with unique source MAC address for each incoming flow.
7.	CSCuh52879	Syslog messages from the VXLAN gateway do not go to the external Syslog server.
8.	CSCug89113	Retain relevant debug components in the VXLAN gateway.
9.	CSCuh61074	VXLAN gateway does not inherit modified port profile on reattach.
10.	CSCui40317	Incorrect values in the InOctets/OutOctets columns with **show interface counters module** command.
11.	CSCui40646	InOctets counter for the VXLAN gateway veth(vxlannic0) interface not working.
12.	CSCui42010	Traffic does not fail over when the port is shutdown from VSM.
13.	CSCui84555	Throughput decrease and large packet getting dropped with UDP traffic.
14.	CSCui27814	Port channel is down after **shut** or **no shut** command on uplink port-profile of VXLAN gateway.
15.	CSCug95878	The **Show process CPU** command does not show the same result for vssnet.
16.	CSCug73194	Configuration fails on port-profile inherited by VTEPs on VEM and VXLAN gateway.
17.	CSCuh20704	There are no OVA files for gateway to do the deployment as a VSB on a VSA.
18.	CSCug93645	The **attach module gateway** command hangs if VSM is on Layer 3 through control interface.
19.	CSCug33235	VXLAN gateway goes offline on the VSM before it returns to attach when running multicast traffic.
20.	CSCug67857	The **show cdp neighbors** command on VSM or VLXLAN gateway does not show details of upstream for VXGW module.
21.	CSCuh17978	The **show process** command does not display the reason for crash.

	ID	Open Caveat Headline
22.	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.
23.	CSCuh41892	You will see the VSM and gateway out-of-sync after you reload the VSM after changing the port-profile.
24.	CSCuh52879	System log messages not going to external system log server from gateway.
25.	CSCuh40181	Unable to deploy VXLAN gateway VSB using the **enable properties** command on Cisco N1010.
26.	CSCud87990	Output for certain fields are missing for **vemcmd show card** command output in the VXLAN gateway.
27.	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	Open Caveat Headline
1.	CSCui71195	Installing an earlier REST-API plug-in version results in HTML errors.
2.	CSCui93564	Port channels do not come up in non-LACP offload setup.
3.	CSCti98977	Not able to migrate VC/VSM and normal VM when adding host to DVS.
4.	CSCtj70071	SNMP V3 traps are not getting generated.
5.	CSCtn62514	LACP offload configuration is not persisting in stateless mode.
6.	CSCtq92519	CDP does not work for certain NIC cards without VLAN 1 allowed.
7.	CSCtr34519	Continuous SNMP polling causes high CPU usage.
8.	CSCts24105	The **load-interval counter** command configuration is not working.
9.	CSCtt17073	A port profile through VCD fails when done immediately after a switchover.
10.	CSCtt24735	Editing a port profile fails with the error message “ERROR: unknown error.”
11.	CSCtz04587	Reloading the VSM takes 12 minutes for modules to come online and vEthernet interfaces to come up
12.	CSCtw96064	The **show tech-support dvs** command does not have output related to DHCP snooping.
13.	CSCtx06864	A native VLAN configured on the interface port channel is not programmed on the VEM.
14.	CSCtx30435	After upgrading the VEM to Cisco NX-OS Release 4.2(1)SV1(5.1), two Cisco VIBs are installed.

	ID	Open Caveat Headline
15.	CSCua00940	PPM does not perform configuration checks when you configure a PVLAN in an offline port-profile mode.
16.	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).
17.	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.
18.	CSCua30287	An error occurs while trying to override the PVLAN mapping in the child port profile.
19.	CSCua73549	Modules are not reattached after a VMKnic MAC address change in Layer 3 mode.
20.	CSCub23161	VCD does not display relevant error descriptions for error codes.
21.	CSCub25986	NSM should fix the Cisco Nexus 1000V feature limitation issue.
22.	CSCub33444	Powering up a single VM configures all vApp networks.
23.	CSCub69289	Veths mapped to the port profiles are not counted in the **show resource-availability monitor** command.
24.	CSCub79332	The server IP address becomes 0.0.0.0 for a MN stateless host.
25.	CSCuc63801	Traffic loss occurs after the VSM reloads if PSEC is restricted and the DSM bit is set.
26.	CSCug25018	You cannot process large number of IGMP queries from the upstream switch on Cisco Nexus 1000V.
27.	CSCuf89892	VEM doesn't increase the number of maximum ports after an upgrade to the current version of Cisco Nexus 1000V.
28.	CSCue17860	snmpwalk does not return values of SyslogServer objects.
29.	CSCue77534	Internal VLANs (3968-4047) are being trunked to configure on ports.
30.	CSCug23565	Downloading the files from VSM configuration with IPV6 throws an error.
31.	CSCug36502	When the VSM is setup with an IPv6 address and accessed, the server drops or resets the connection randomly causing multiple issues.
32.	CSCug66317	When trying to install a license file, installation fails with a error message "file already exists" and license file is not installed.
33.	CSCuc75590	When plan mappings are configured on the port-channel interface directly, the mappings are incorrect on the VEM.
34.	CSCug51163	VEM upgrade from previous releases of Cisco Nexus 1000V software to the current release of Cisco Nexus 1000V software fails.
35.	CSCue50621	ifHCInOctets and ifInOctets wrap while taking snapshot of virtual machines.

	ID	Open Caveat Headline
36.	CSCug36191	SNMP times out when browsing the entire tree or the CISCO-PROCESS-MIB.
37.	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.
38.	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.
39.	CSCue06575	Unable to create DVportgroup during bulk VMotion.
40.	CSCuh52327	ISSU upgrade compatibility table is not modified to accommodate VXLAN gateway.
41.	CSCuh52373	The **show install service-module** command does not display the service module ISSU status.
42.	CSCum99528	IP address configuration on interface control0 is not persistent upon VSM reload.

Quality of Service

	ID	Open Caveat Headline
1.	CSCtu36119	QoS marking limitation in VCD environment.

Features

	ID	Open Caveat Headline
1.	CSCtk65252	PSEC with multiple MAC addresses and PVLAN not supported.
2.	CSCtl04632	Port migration with switchover causing ports to go to “No port-profile.”
3.	CSCtr06833	Split brain causes pending ACL/QoS transactions into err-disabled.
4.	CSCtr09746	Interface configuration fails when veths are nonparticipating due to unreachable module.
5.	CSCub44964	A RADIUS AAA error occurs when feature CTS is enabled and there is a switchover.
6.	CSCue36581	Copy run start takes 8 to 10 minutes to complete the copy.
7.	CSCug85914	The **show bridge-domain vteps** command shows the IP even after removing the veth.
8.	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.
9.	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.

	ID	Open Caveat Headline
10.	CSCug74311	VTEP IP stuck in VTEP list after a headless VEM reconnects to the VSM.
11.	CSCuh08385	ACL does not work on IGMP version 2 and v3.
12.	CSCuh11701	The **no acllog match-log-level <level>** command does not reset the ACL logging level to the default value.
13.	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.
14.	CSCuh11779	Incorrect default value is shown for max-deny flows and max-permit flows.

VMware

	ID	Open Caveat Headline
1.	CSCui80024	ESXi 5.5 Bandwidth allocated for a queue is not as expected on congestion.
2.	CSCuj19963	When ESX is upgraded to vSphere 5.5, Mellanox NICs get policy mismatch.
3.	CSCuj26459	When ESX is upgraded to vSphere 5.5, the Host management connectivity is lost.
4.	CSCuj19983	CDN NIC gets previous port policy after reboot.
5.	CSCti34737	Removing host with Intel Oplin from DVS causes all ports to reset.
6.	CSCtk02322	After an ESX host exception, the port group configuration on PNIC is changed.
7.	CSCtk07337	Fully qualified domain name/user with port-profile visibility fails.
8.	CSCtk10837	Port-profile visibility feature is not able to update permissions.
9.	CSCtk53802	Improper sync with vCenter when port-profile names have special characters.
10.	CSCts80394	A VEM upgrade fails when the scratch space is a network file system.
11.	CSCtt00444	After unregistering Cisco Nexus 1000V on Vshield, the alert timer runs.
12.	CSCua30356	An existing vAPP cannot be powered down, and a new vAPP cannot be deployed.
13.	CSCub56123	Wrong message for VC user id and Password.
14.	CSCuc71793	Ports go to error disabled state during ACL or QoS Commit Errors.
15.	CSCuc75398	App fail power on with insufficient resource error.
16.	CSCuc80063	IGMP process failing to read PVLAN association.

Resolved Caveats

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

	ID	Resolved Caveat Headline
17.	CSCuh17360	Start_cnt for vssnet does not change after restarting.
18.	CSCug92356	The **show module** command does not display updated VXLAN gateway management IP address.
19.	CSCuh48661	Gateway module fluctuates when traffic flows with varied 1000 SMAC ICMP traffic.

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

Related Documentation

This section lists the documents used with the Cisco Nexus 1000V and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V Documentation Roadmap

Cisco Nexus 1000V Release Notes

Cisco Nexus 1000V Compatibility Information

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V Interface Configuration Guide

Cisco Nexus 1000V Layer 2 Switching Configuration Guide

Cisco Nexus 1000V License Configuration Guide

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide

Cisco Nexus 1000V Port Profile Configuration Guide

Cisco Nexus 1000V Quality of Service Configuration Guide

Cisco Nexus 1000V REST API Plug-in Configuration Guide

Cisco Nexus 1000V Security Configuration Guide

Cisco Nexus 1000V System Management Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Cisco Nexus 1000V VXLAN Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Programming Guide

Cisco Nexus 1000V XML API User Guide

Reference Guides

Cisco Nexus 1000V Command Reference

Cisco Nexus 1000V Resource Availability Reference

Troubleshooting, Password Recovery, System Messages Guides

Cisco Nexus 1000V Troubleshooting Guide

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

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/ps13095/tsd_products_support_series_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, 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.

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. (1110R)

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

© 2014 Cisco Systems, Inc. All rights reserved.