

Send document comments to nexus7k-docfeedback@cisco.com



Cisco DCNM Release Notes, Release 5.0

Release Date: August 24, 2010

Part Number: OL-22900-02 C0

This document provides the release notes for Cisco Data Center Network Manager (DCNM), Release 5.x. Use this document in combination with the documents listed in the “[Obtaining Documentation and Submitting a Service Request](#)” section on page 28.



Note

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the Cisco DCNM Release Notes:

http://www.cisco.com/en/US/products/ps9369/prod_release_notes_list.html

[Table 1](#) shows the online change history for this document.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-22900-01	A0	May 24, 2010	Created release notes for Release 5.0(2).
	B0	June 02, 2010	<ul style="list-style-type: none"> Moved caveat CSCtg77948 from the “Resolved Caveats—Cisco DCNM Release 5.0(2)” section to the “Open Caveats—Cisco DCNM Release 5.0” section. Removed caveat CSCte82328 from the “Open Caveats—Cisco DCNM Release 5.0” section. Updated the version number of NX-OS Release 5.0(2) to 5.0(2a) in Table 4. Revised the description of the limitation “Incorrect DCNM Behavior After a Database Failure or a Connection Failure to the Database”.
OI-22900-02	A0	July 25, 2010	Created release notes for Release 5.0(3).
	B0	August 06, 2010	<ul style="list-style-type: none"> Corrected the description and bug ID of caveat CSCth75025.. Updated Table 5 to show all Cisco Nexus platforms that Cisco DCNM Release 5.0(3) supports.
	C0	August 24, 2010	<ul style="list-style-type: none"> Included Cisco Nexus 2232 and 2248 hardware.

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [New and Changed Information, page 8](#)
- [Limitations, page 13](#)
- [Installation Notes, page 14](#)
- [Caveats, page 14](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation and Submitting a Service Request, page 28](#)

Introduction

Cisco DCNM is a management solution for Cisco NX-OS-enabled hardware platforms. Focused on the management requirements of data center networks, Cisco DCNM automates the provisioning process, monitors the network for performance degradation, secures the network, and streamlines the diagnosis of dysfunctional network elements.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Cisco NX-OS supports the Cisco Nexus product family, including the Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, Cisco Nexus 4000 Series, Cisco Nexus 2000 Fabric Extension, and Cisco Nexus 1000V Series. For the most recent information on Cisco NX-OS, refer to the following website:

http://www.cisco.com/en/US/products/ps9372/prod_release_notes_list.html

System Requirements

This section includes the following topics:

- [Java Requirements, page 3](#)
- [Server System Requirements, page 3](#)
- [Client System Requirements, page 5](#)
- [Supported Cisco Platforms and Software Versions, page 5](#)
- [Hardware Supported, page 6](#)

Java Requirements

Cisco DCNM is a Java-based client-server application. The Cisco DCNM 5.0(3) server and client support Java JRE 1.5.0_11. The installation process uses Java version 1.5. If your system does not have that version of Java, the installation process will download it to the *DCNM_root_directory/java/jre1.5* directory.



Note

If you need an additional version of JRE, install the additional version at *DCNM_root_directory/java/jreversion_number*.

Server System Requirements

Cisco DCNM Release 5.0(2) supports running the Cisco DCNM server on these operating systems:

- Microsoft Windows Server 2003 Enterprise Edition, Service Pack 1 and Service Pack 2 (32-bit, 64-bit).
- Red Hat Enterprise Linux Release 5.4 (32-bit and 64-bit versions).



Note

For the 64-bit Linux version, the PostgreSQL database that comes with the Cisco DCNM installation might not work. If you encounter that problem, you can separately install a PostgreSQL version that supports a 64-bit Linux operating system.

- VMware ESX 4.0.



Note

You must use the static MAC address option for a virtual machine (VM). To find information about how to configure a static MAC address, search the VMware Knowledge Base at the following URL: <http://kb.vmware.com/selfservice/microsites/microsite.do>

Send document comments to nexus7k-docfeedback@cisco.com

The system requirements depend on whether you are running the Cisco DCNM server and the database server on the same machine or distinct machines (for example, in a cluster environment). [Table 2](#) and [Table 3](#) list the minimum and recommended Cisco DCNM requirements for each of these deployment scenarios.

Table 2 *Server System Requirements—Cisco DCNM and Database Servers Collocated*

Component	Minimum Requirements	Recommended Requirements
RAM (free)	4 GB	6 GB
CPU speed	2.5 GHz with dual-processor or dual-core CPU	3.45 GHz with dual-processor or dual-core CPU
Disk space (free)	60 GB	80 GB

Table 3 *Server System Requirements—Cisco DCNM and Database Servers on Separate Machines (Clustered)*

Component	Minimum Requirements	Recommended Requirements
Cisco DCNM Server		
RAM (free)	2 GB	3 GB
CPU speed	2.5 GHz with dual-processor or dual-core CPU	3.45 GHz with dual-processor or dual-core CPU
Disk space (free)	20 GB	30 GB
Database Server		
RAM (free)	2 GB	3 GB
CPU speed	2.5 GHz with dual-processor or dual-core CPU	3.45 GHz with dual-processor or dual-core CPU
Disk space (free)	40 GB	50 GB

If Cisco DCNM coexists with Fabric Manager on the same server, the server should have at least 6 GB of free RAM, 100 GB of free disk space, and two Ethernet ports running at 1 Gbps (each manager uses one Ethernet port). The server should include one of the following operating at 2.5 GHz:

- One quad-core processor
- Two dual-core processors
- Four single-core processors

Additionally, the following prerequisites must be in place for the server:

- The IP address of the server system should be statically assigned.
- A Perl environment must already be installed on the server system. We recommend Active Perl version 5.8.9.827. You can download ActivePerl for your server operating system from the following location:
<http://www.activestate.com/activeperl/downloads/>
- The path to the Perl executable must be defined in the server system PATH environment variable.
- No other programs are running on the server except for Cisco Fabric Manager Release 4.2(1) or later releases and the database software used by Fabric Manager.
- If you plan to use an Oracle 10g database, configure the Oracle database as follows:
 - Increase the SYSTEM tablespace to 2 GB from the default 1 GB of space.
 - Increase the number of sessions and processes to 150 each from the default of 50.

Send document comments to nexus7k-docfeedback@cisco.com

- Increase the number of open cursors to 1000 from the default of 50.
- If you plan to use an Oracle 11g database, configure the Oracle database as follows:
 - Increase the number of sessions and processes to 150 each from the default of 50.
 - Increase the number of open cursors to 1000 from the default of 300.



Note

Although it is not required, it is a good practice to register the server system with the DNS servers.

Client System Requirements

Cisco DCNM Release 5.0 supports running the Cisco DCNM client on Microsoft Windows XP Professional Service Pack 2 or Microsoft Windows XP Professional Service Pack 3 and Firefox browser version 3.0 on Red Hat Enterprise Linux AS Release 5.4 (32-bit and 64-bit versions). [Table 4](#) lists the minimum hardware requirements for these client systems.

Table 4 *Client Hardware Requirements*

Hardware	Minimum Requirements
RAM (free)	1 GB
CPU speed	2.16 GHz with one dual core processor or two single-core processors
Disk space (free)	100 MB
Network Interface Card	1 port at 1 Gbps

If Cisco DCNM coexists with Fabric Manager on your client system, the client system should include one dual-core processor or two single-core processors operating at 2.0 GHz, 2 GB of free RAM, and 200 MB of free disk space.

This installation process uses Java version 1.5.0_11. If your system does not have that version of Java, the installation process will download it to your system.

Some Cisco DCNM features require a license. Before you can use the licensed features, you must install the Cisco DCNM license. For more information, see the [Cisco DCNM Installation and Licensing Guide, Release 5.x](#).

Supported Cisco Platforms and Software Versions

Cisco DCNM is compatible with the platforms and software versions listed in [Table 5](#).

Table 5 *Cisco DCNM and Cisco Nexus Platform/NX-OS Compatibility*

DCNM Version	Platform	NX-OS Version
4.1(2)	Cisco Nexus 7000	4.1(2), 4.0(4), 4.0(3), 4.0(2)
4.1(3)	Cisco Nexus 7000	4.1(5), 4.1(4), 4.1(3), 4.1(2), 4.0(4), 4.0(3), 4.0(2)
4.2(1)	Cisco Nexus 7000	4.2(2a), 4.1(5), 4.1(4), 4.1(3), 4.1(2), 4.0(4), 4.0(3), 4.0(2)
	Cisco Nexus 5000 and Cisco Nexus 2000	4.1(3)N1(1)

Send document comments to nexus7k-docfeedback@cisco.com

Table 5 Cisco DCNM and Cisco Nexus Platform/NX-OS Compatibility (continued)

DCNM Version	Platform	NX-OS Version
4.2(3)	Cisco Nexus 7000	4.2(4), 4.2(2a), 4.2(3), 4.1(5), 4.1(4), 4.1(3), 4.1(2), 4.0(4), 4.0(3), 4.0(2)
	Cisco Nexus 5000 and Cisco Nexus 2000	4.1(3)N2(1), 4.1(3)N1(1a), 4.1(3)N1(1)
	Cisco Nexus 4000 (IBM)	4.1(2)E1(1)
5.0(2)	Cisco Nexus 7000	5.0(2a), 4.2(4), 4.2(2a), 4.2(3), 4.1(5), 4.1(4), 4.1(3), 4.1(2), 4.0(4), 4.0(3), 4.0(2)
	Cisco Nexus 5000 and Cisco Nexus 2000	4.1(3)N2(1a), 4.1(3)N1(1.1E), 4.1(3)N2(1), 4.1(3)N1(1a), 4.1(3)N1(1)
	Cisco Nexus 4000 (IBM)	4.1(2)E1(1)
	Cisco Nexus 1000V	4.0(4)SV1(3)
5.0(3)	Cisco Nexus 7000	5.0(3), 5.0(2a), 4.2(4), 4.2(2a), 4.2(3), 4.1(5), 4.1(4), 4.1(3), 4.1(2), 4.0(4), 4.0(3), 4.0(2)
	Cisco Nexus 5000 and Cisco Nexus 2000	4.1(3)N2(1a), 4.1(3)N1(1.1E), 4.1(3)N2(1), 4.1(3)N1(1a), 4.1(3)N1(1)
	Cisco Nexus 4000 (IBM)	4.1(2)E1(1)
	Cisco Nexus 1000V	4.0(4)SV1(3)

Hardware Supported

Table 6 lists the products and components that Cisco DCNM Release 5.x supports.

Table 6 Hardware Features Supported by Cisco DCNM Release 5.x

Product/Component	Part Number
Cisco Nexus 7000 Series Switch	—
Cisco Nexus 7010 chassis	N7K-C7010
Cisco Nexus 7018 chassis	N7K-C7018
Supervisor module	N7K-SUP1
Fabric module, Cisco Nexus 7010 chassis	N7K-C7010-FAB-1
Fabric module, Cisco Nexus 7018 chassis	N7K-C7018-FAB-1
48-port 10/100/1000 Ethernet I/O module	N7K-M148GT-11
48-port 1-Gigabit Ethernet SFP I/O module	N7K-M148GS-11
48-Port 1-Gigabit Ethernet Module with XL Option	N7K-M148GS-11L
32-port 10-Gigabit Ethernet SFP+ I/O module	N7K-M132XP-12

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Table 6 Hardware Features Supported by Cisco DCNM Release 5.x (continued)

Product/Component	Part Number
8-Port 10 Gigabit Ethernet Module with XL Option (requires X2)	N7K-M108X2-12L
System fan tray, Cisco Nexus 7010 chassis	N7K-C7010-FAN-S
Fabric fan tray, Cisco Nexus 7010 chassis	N7K-C7010-FAN-F
Fan tray, Cisco Nexus 7018 chassis	N7K-C7018-FAN
6-kW AC power supply unit	N7K-AC-6.0KW
7.5-kW AC power supply unit	
International version	N7K-AC-7.5KW-INT
US version	N7K-AC-7.5KW-US
6-kW DC power supply unit	N7K-DC-6.0KW
Cisco Nexus 5000 Series Switch	—
Cisco Nexus 5010 chassis	N5K-C5010P-BF
Cisco Nexus 5020 chassis	N5K-C5020P-BF
	N5K-C5020P-BF-XL
N5000 1000 Series Module 6port 10GE	N5K-M1600(=)
N5000 1000 Series Mod 4x10GE 4xFC 4/2/1G	N5K-M1404=
N5000 1000 Series Module 8port 4/2/1G	N5K-M1008=
N5000 1000 Series Module 6port 8/4/2G	N5K-M1060=
Fan module, Cisco Nexus 5010	N5K-C5010-FAN=
Fan module, Cisco Nexus 5020	N5K-C5020-FAN=
550 W AC Power Supply Module, Cisco Nexus 5010	N5K-PAC-550W(=)
1200 W AC Power Supply Module, Cisco Nexus 5020	N5K-PAC-1200W(=)
Cisco Nexus 4000 Series Switch	—
Cisco Nexus 4001I Switch Module	N4K-4001I-XPX
Cisco Nexus 4005I Switch Module	N4K-4005I-XPX
Cisco Nexus 2000 Series Fabric Extenders	
Cisco Nexus 2148 1 GE Fabric Extender	N2K-C2148T-1GE
Cisco Nexus 2148 FEX 1GE Fan Module	N2K-C2148T-FAN=
Cisco Nexus 2000 FEX 200 W AC Power Supply	N2K-PAC-200W(=)
Cisco Nexus 2232PP 10 GE Fabric Extender	N2K-C2232PP-10GE
Cisco Nexus 2232PP Fan Module	N2K-C2232-FAN=
Cisco Nexus 2000 FEX 400 W AC Power Supply	N2K-PAC-400W=
Cisco Nexus 2248TP 1 GE Fabric Extender	N2K-C2248TP-1GE
Cisco Nexus 2248TP Fan Module	N2K-C2248-FAN=
Cisco Nexus 2000 FEX 400 W AC Power Supply	N2K-PAC-400W=
Cisco Nexus 1000V Series Switch	—

Send document comments to nexus7k-docfeedback@cisco.com

New and Changed Information

This section includes the following topics:

- [New Hardware Features in Release 5.0\(3\)](#), page 8
- [New Database Features in Release 5.0\(3\)](#), page 8
- [New Software Features in Release 5.0\(3\)](#), page 8
- [New Hardware Features in Release 5.0\(2\)](#), page 8
- [New Database Features in Release 5.0\(2\)](#), page 8
- [New Software Features in Release 5.0\(2\)](#), page 9
- [Limitations](#), page 13

New Hardware Features in Release 5.0(3)

There is no new hardware in this release.

New Database Features in Release 5.0(3)

There are no new database features in this release.

New Software Features in Release 5.0(3)

There are no new software features in this release.

New Hardware Features in Release 5.0(2)

Cisco DCNM adds support for the following hardware:

- Cisco Nexus 7000 Series 8-port 10 Gigabit Ethernet Module with XL Option (requires X2)
- Cisco Nexus 7000 Series 48-port Gigabit Ethernet Module with XL Option (requires SFP)
- Cisco Nexus 2232PP 10 GE Fabric Extender
- Cisco Nexus 2248TP 1 GE/10 GE Fabric Extender

New Database Features in Release 5.0(2)

There are no new database features in this release.

Send document comments to nexus7k-docfeedback@cisco.com

New Software Features in Release 5.0(2)

This section describes the new Cisco DCNM software features introduced in Cisco DCNM Release 5.0(2). For detailed information about the features listed, see the documents listed in the “[Obtaining Documentation and Submitting a Service Request](#)” section on page 28. The “New and Changed Information” section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.

This section includes the following topics:

- [Cisco DCNM and Cisco Fabric Manager Integration, page 9](#)
- [LLDP, page 10](#)
- [Device Groups, page 10](#)
- [Clustering, page 10](#)
- [Automatic Logging-Level Configuration, page 10](#)
- [VMware Server, page 10](#)
- [Linux Client, page 10](#)
- [Event Enhancements, page 11](#)
- [Event Enhancements, page 11](#)
- [HSRP IPv6, page 11](#)
- [AAA Enhancements, page 11](#)
- [ACL Pagination, page 11](#)
- [ACL Object Groups, page 11](#)
- [IGMP Snooping, page 11](#)
- [Interface System Defaults, page 11](#)
- [vPC Enhancements, page 11](#)
- [Power Usage, page 12](#)
- [New Module Support, page 12](#)
- [Nexus 1000V Series Switch, page 12](#)
- [Nexus 4000 Series Switch, page 13](#)

Cisco DCNM and Cisco Fabric Manager Integration

Cisco DCNM discovers SAN devices and connections to network servers and displays them on the topology map.

In addition, you can launch the Cisco Fabric Manager client from the Cisco DCNM topology map.

**Note**

Both Cisco DCNM Release 5.0(2) and Cisco Fabric Manager Release 5.0(1a) cannot be installed on the same server. If they are, the DCNM server stops functioning. For additional information, see [CSCtf08888](#) in the “[Resolved Caveats—Cisco DCNM Release 5.0\(2\)](#)” section.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

LLDP

Cisco DCNM can discover the servers connected to Cisco Nexus 7000 Series devices using the Link Layer Discovery Protocol (LLDP). Servers connected to Cisco Nexus 7000 Series devices can be detected if they are running openLLDP software. Currently, openLLDP is supported only on Linux. Servers connected to Cisco Nexus 5000 Series devices are not discovered by Cisco DCNM in this release.

Device Groups

In Cisco DCNM, you can create device groups to simplify the visualization of interconnections between groups of devices in the topology map. You can categorize devices into device groups that you define. This allows you to focus on a limited number of devices when you view the topology.

Clustering

You can deploy Cisco DCNM in a server cluster, with up to five Cisco DCNM servers in a cluster. Cisco DCNM servers in a cluster communicate using multicast IP messages. The primary benefit of a clustered-server deployment is enhanced capacity for the device-management tasks that Cisco DCNM performs. A clustered-server deployment also helps to ensure availability of the Cisco DCNM server. Cisco DCNM distributes tasks among all servers in the cluster. Servers in the cluster are always active and never in a stand-by mode.

Automatic Logging-Level Configuration

The Cisco DCNM server needs specific log levels to be configured so that it can detect changes happening in the device. As of Cisco DCNM Release 5.0, the Cisco DCNM server automatically configures the log levels for feature such as ports, VLANs, and port channels so that the necessary syslogs are generated. If the necessary log levels are not configured, Cisco DCNM marks that device as unmanaged.

VMware Server

The Cisco DCNM server can run on the VMware ESX 4.0 operating system.

Linux Client

The Cisco DCNM client can run on Firefox browser version 3.0 on Red Hat Enterprise Linux AS Release 5.

SSL Protocol

For added security, the Cisco DSNM server and client communicate using the Secure Client Server Communications (Secure Socket Layer or SSL) protocol. SSL communication between the server and client is disabled by default. To enable SSL, see the detailed instructions in the “Enabling Encrypted Client-Server Communications” section of the *Cisco DCNM Installation and Licensing Guide*.

Send document comments to nexus7k-docfeedback@cisco.com

Event Enhancements

To improve performance, Cisco DCNM processes syslog messages concurrently across all managed devices. Cisco DCNM also processes syslog messages sequentially for events from the same device.

HSRP IPv6

You can configure IPv6 HSRP groups, including defining IPv6 addresses and enabling autoconfig on an IPv6 HSRP group.

AAA Enhancements

Cisco DCNM Release 5.0(2) adds the following enhancements to the AAA feature:

- Enable and disable the display of AAA authentication failure messages to the device console.
- Enable and disable default user roles for AAA authentication of remote users.
- Configure AAA authentication mode, including ASCII authentication for passwords on TACACS+ servers, MSCHAP authentication on RADIUS/TACACS+ servers, and MSCHAPv2 authentication on RADIUS servers.

ACL Pagination

Cisco DCNM employs a pagination scheme to display IPv4 and IPv6 ACL tables. Up to 100 ACEs are displayed at a time. With ACL pagination, you can quickly navigate to a particular ACE based on its sequence number.

ACL Object Groups

You can create address and port object groups to reduce the number of access rules required to implement a particular security policy.

IGMP Snooping

Cisco DCNM supports configuring the Internet Group Management Protocol (IGMP) snooping software. IGMP examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications.

Interface System Defaults

You can configure switch port admin status and port mode as the default for interfaces that do not have these attributes specifically configured.

vPC Enhancements

Cisco DCNM Release 5.0(2) adds the following enhancements to the vPC feature:

Send document comments to nexus7k-docfeedback@cisco.com

- The vPC summary pane displays interfaces in which peer-keepalive messages are sent and received.
- The Port Channel and vPC and the Logical vPC View topology maps display the interfaces used as the fault tolerant links in the port channel.

Power Usage

Cisco DCNM displays information about the power usage of managed Cisco Nexus 7000 Series switches including an aggregation of the power usage for all managed Cisco Nexus 7000 Series switches and summary information for a specific device, and graphical information for a selected device.

You can configure Cisco DCNM to collect power usage statistics for up to six managed devices.

New Module Support

Cisco DCNM provides support for discovering and managing the following new line card modules:

- Cisco Nexus 7000 Series 8-port 10 Gigabit Ethernet Module with XL Option (requires X2)
- Cisco Nexus 7000 Series 48-port Gigabit Ethernet Module with XL Option (requires SFP)

Nexus 1000V Series Switch

Cisco DCNM Release 5.0(2) introduces the following new features to support Cisco Nexus 1000V Series platforms:

- Virtual Ethernet Ports—DCNM allows you to discover the Virtual Ethernet (vEthernet) interfaces present in the Nexus1000V switch to create, modify, or delete vEthernet interfaces. You can also monitor the status, statistics and events pertaining to the vEthernet interfaces present in the switch.
- Port Profiles—DCNM allows you to discover the existing port profiles configured in the switch and to view the ports to which they are applied. It also allows you to do the following:
 - Create new port profiles and bind them to interfaces.
 - Modify existing profiles and their interface binding.
 - Delete port profiles.
- Domains and Network Connections—DCNM allows you to discover virtual switch domains and network connections of managed Cisco Nexus 1000V Series switches. You can also configure virtual switch domains and network connections and monitor virtual switch information.
- Static Pinning—You can configure static pinning on vEthernet interfaces.
- Layer 3 Control—You can configure the connection between the Virtual Supervisor Module (VSM) and Virtual Ethernet Modules (VEMs) to use the Layer 3 transport protocol for control and packet traffic.

Cisco DCNM Release 5.0(2) supports the following existing networking features on Cisco Nexus 1000V Series platforms:

- Physical Ethernet ports
- Management ports
- Port channels
- VLANs
- Private VLANs

Send document comments to nexus7k-docfeedback@cisco.com

- Local SPAN
- IPv4 and MAC ACLs
- AAA (RADIUS and TACACS+ server and server group management)
- RBAC (both roles and user management)
- Inventory
- CPU utilization
- Memory utilization

All of the Cisco DCNM Release 5.0(2) application features support the Cisco Nexus 1000V Series platform, except for Configuration Archive, Configuration Diff, and Software Image Management.

Nexus 4000 Series Switch

Cisco DCNM Release 5.0(2) introduces the following new feature to support Cisco Nexus 4000 Series platforms:

- FIP Snooping—You can configure the Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping feature.
- IGMP Snooping—You can configure Internet Group Management Protocol (IGMP) snooping feature.

All of the Cisco DCNM Release 5.0(2) application features support the Cisco Nexus 4000 Series platform.

Limitations

This section describes the limitations in Cisco DCNM Release 5.0(3) and Release 5.0(2). It includes the following topics:

- [Display of Default Bandwidth Depends on the Operational Status of the Interface, page 13](#)
- [Incorrect DCNM Behavior After a Database Failure or a Connection Failure to the Database, page 14](#)

Display of Default Bandwidth Depends on the Operational Status of the Interface

When you enter the **show running-config all** command, the output should show the default bandwidth for an interface. However, the output of this command depends on the operational status of the interface, so the output may not show the default value.

This limitation is associated with CSCte52885.

Send document comments to nexus7k-docfeedback@cisco.com

Incorrect DCNM Behavior After a Database Failure or a Connection Failure to the Database

If the database used by Cisco DCNM fails or if a connection to the database fails, the Cisco DCNM standalone server or the Cisco DCNM cluster environment will not work properly. As a result, you may see any of the following problems:

- A server connection error
- Inability to log in to the Cisco DCNM client
- The existing client does not correctly display network information
- Some statistics are stopped

If you experience this issue, take the following steps:

1. Stop the Cisco DCNM server or shut down the Cisco DCNM cluster.
2. Verify that the database or communication to the database is functioning properly.
3. Restart the Cisco DCNM server(s).

This limitation is associated with CSCte82328.

Installation Notes

For information about installing and uninstalling Cisco DCNM Release 5.0(3), see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*. You can find this publication on Cisco.com at this location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Caveats

This section includes the following topics:

- [Open Caveats—Cisco DCNM Release 5.0, page 15](#)
- [Resolved Caveats—Cisco DCNM Release 5.0\(3\), page 18](#)
- [Resolved Caveats—Cisco DCNM Release 5.0\(2\), page 19](#)
- [Open Caveats—Cisco DCNM Release 4.2, page 21](#)

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Open Caveats—Cisco DCNM Release 5.0

- CSCte37117

Symptom: The status of the RADIUS/TACACS+ server that is shown in DCNM is not in sync with the status shown on the switch.

Conditions: When a RADIUS or TACACS+ server is created in the switch without idle or dead time, the servers are in a non-monitored state. DCNM shows the status of the corresponding servers as non-monitored. If a user configures the idle time or dead time for that server on the switch, the switch will start monitoring the server. As soon as user configures idle time or dead time for that server, the server status will move from a non-monitored state to alive state. Because there is no syslog generated for this status change, DCNM is not aware of this status change, so it continues to show the status as non-monitored.

Workaround: None.
- CSCte54192

Symptom: DCNM takes a long time to discover the devices during a discovery task.

Conditions: You may see this symptom under the following condition:

 - DCNM takes a long time to discover the devices with a very large configuration.

Workaround: When this issue occurs in a huge configuration, discover devices individually with hop count zero to significantly reduce the discovery time. Even though discovery takes a long time, the device will get discovered eventually.
- CSCtf11112

Symptom: Statistics are not restored after the rediscovery of an unmanaged device.

Conditions: You may see this symptom if a device goes to an unmanaged state because of incorrect credentials or another reason and then the same device becomes managed again. The previously viewed statistics for the device are not restored.

Workaround: None. Start the statistics collection again.
- CSCtf27611

Symptom: Cisco DCNM takes a long time to discover the devices in a discovery task.

Conditions: You may see this symptom under the following conditions:

 - When the CDP hop count is greater than three and therefore more devices are added to the scope of discovery task.
 - Cisco DCNM takes additional time to discover devices in a large configuration.

Workaround: In a large configuration, you can discover devices individually with the hop count of zero to significantly reduce the discovery time.
- CSCtf33337

Symptom: Cisco DCNM is not able to show a port-profile association with a newly added physical interface for a VEM.

Conditions: You may see this symptom when you add a new physical interface to a particular VEM on a Cisco Nexus 1000V switch, and you have to associate that interface with a system port profile. The association between the interface and port profile is not shown in Cisco DCNM.

Workaround: Rediscover the switch.
- CSCtf48926

Symptom: Physical links take a long time to be reflected in the topology window.

Send document comments to nexus7k-docfeedback@cisco.com

Condition: This symptom may be seen when you view the topology window during a large network device discovery.

Workaround: Refresh the topology window to see the physical links once discovery is completed.

- CSCtg44540

Symptom: When you click a link in the Port Channel and vPC view in the topology, device names are truncated in the window. In addition, the ports are not sorted and there is no option to sort them.

Conditions: If the device names are long, then they are truncated in the window that shows details for the link.

Workaround: Use the mouse cursor to hover over the truncated device name. The full name is displayed in a tool tip. There is no workaround for the sorting for the ports.

- CSCtg77948

Symptom: Cisco Nexus series devices that do not support custom VDCs, such as the Cisco Nexus 5000 Series switch, become unmanageable in Cisco DCNM after their discovery.

Conditions: This symptom may be seen when the hostname that is set is longer than 20 characters.

Workaround: Set a short hostname of less than 20 characters and then discover the device. Cisco DCNM should be able to discover and manage the devices with hostnames shorter than 20 characters.

- CSCtg78225

Symptom: While adding the V6 address during a V6 HSRP Group creation, the address that you enter gets somewhat distorted.

Conditions: You may see this symptom when trying to enter the V6 Address while creating a V6 Group.

Workaround: Create the V6 Group and deploy it using Cisco DCNM, and then provide the required V6 address.

- CSCtg80791

Symptom: In the VDC setup wizard, Step 2 shows slot -1 under the selected interfaces table. Expanding slot -1 shows the port profiles that are configured on the device. When you allocate these port profiles, DCNM displays an error message and fails to create the VDC.

Conditions: You may see this symptom under the following conditions:

- You configure a port profile on the device through the CLI.
- You discover the device using DCNM.
- You create new VDC using DCNM.

Workaround: To work around this issue, do not select port profiles under Slot-1 to allocate the port profile in a VDC.

- CSCtg87233

Symptom: In an MDS device, when a module is powered up or a module is inserted, the device remains in the discovering state.

Conditions: You may see this symptom when a module is powered up or a module is inserted.

Workaround: Rediscover the device.

- CSCtg89207

Send document comments to nexus7k-docfeedback@cisco.com

Symptom: The licensing window incorrectly shows the message "License count not same across the cluster, click to view details," even though the license count is the same on all machines in the cluster.

Conditions: You may see this symptom if you create a cluster setup with three servers and install the same license file on all the three servers.

Workaround: To work around this issue, close the Cisco DCNM client and relaunch it. After relaunch, Cisco DCNM shows the correct license count.

- CSCtg90264

Symptom: Port information for a link between a Cisco Nexus 7000 Series device and a Linux server is shown incorrectly. The port information is reversed, so that the port on the Cisco Nexus 7000 Series device is shown as a port on a Linux server and vice-versa.

Conditions: You may see this symptom when you click the **Show End Devices** menu to show the server connected to a Cisco Nexus 7000 Series device.

Workaround: To work around this issue, rediscover the Cisco Nexus 7000 Series device.

- CSCth64121

Symptom: When you remove devices from the license pool, the license screen hangs.

Conditions: This symptom might be seen when multiple devices or devices with large configurations are selected for removal.

Workaround: Close the existing DCNM client and relaunch a new DCNM client.

- CSCth90196

Symptom: The Cisco DCNM GUI hangs when roles have any interface policy that is specific to VFC, FC, or SAN port-channel interfaces. A slow response might also be seen during various operations in the RBAC screen.

Conditions: The symptom might be seen under the following conditions:

1. Start the Cisco DCNM server.
2. Discover any Cisco Nexus 5000 device that has a role with an interface policy specific to VFC, FC, or SAN port channels. That is, the **show role name role-name** command on the device displays a configuration like the following:

```
.....
.....
permit interface fc2/1-8
    permit interface san-port-channel 1-256
    permit interface vfc1-8192
.....
```

3. Launch the Cisco DCNM client and visit **Security->RBAC->Roles** screen and select the role with the configuration shown in step 2.
4. Try to launch the permitted interfaces combination in the table for the role.

Workaround: Remove the configuration related to the FC, VFC, or SAN port channel and rediscover the Cisco Nexus 5000 device.

- CSCth90216

Symptom: The syslog poller stops polling in DCNM when roles on a Cisco Nexus 5000 device have a large number of VFC interface configurations as part of the interface policy.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Conditions: This symptom might be seen under the following conditions:

1. Start the DCNM server is started.
2. Discover any Cisco Nexus 5000 device.
3. Configure a role with an interface policy to permit or deny a large number of VFCs. The **show role name role-name** command on the device has a configuration like the following:

```
.....
.....
.....
    permit interface vfc1-8192
.....
```

The syslog poller does not work after Cisco DCNM parses the preceding CLI. Any changes on the device are not reflected in Cisco DCNM.

Workaround: Remove the configuration related to the role with the interface permit or deny policy for the large number of VFCs and re-discover the device.

Resolved Caveats—Cisco DCNM Release 5.0(3)

- CSCtf89686

Symptom: On the Linux platform, when you click the links in a topology, the port names are not completely visible. The names are truncated because the table column width is too small.

Conditions: If the port names are larger than the table column width, the names are truncated.

Workaround: This issue is resolved.
- CSCth13041

Symptom: Links are not shown properly in the logical vPC view.

Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

Workaround: This issue is resolved.
- CSCth50324

Symptom: Irrelevant devices are listed in some of the platform specific screens.

Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

Workaround: This issue is resolved.
- CSCth62075

Symptom: Link connectivity does not display correctly in the topology. The links do not end at the center of the node in the topology.

Send document comments to nexus7k-docfeedback@cisco.com

Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

Workaround: This issue is resolved.

- CSCth62200

Symptom: When you edit a vPC, the vPC wizard does not display any values.

Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

Workaround: This issue is resolved.

- CSCth66359

Symptom: When VDCs are moved across device groups, the hostnames are duplicated.

Conditions: This symptom might be seen under normal operating conditions of a Cisco Nexus 7000 Series switch.

Workaround: This issue is resolved.

- CSCth75025

Symptom: Cisco DCNM is unable to parse the **san-port-channel** keyword.

Conditions: This symptom might be seen for the following configuration:

```
switch# role name datacenter-admin
        interface policy deny
        permit interface san-port-channel 1-256
```

Workaround: This issue is resolved.

Resolved Caveats—Cisco DCNM Release 5.0(2)

- CSCsy33929

Symptom: When you use the Port Channel window to delete a port channel that has a neighbor, Cisco DCNM also deletes the neighboring port channel.

Conditions: The following steps cause this problem:

1. A device with a port channel, which has operationally up, links with another port channel.
2. Because there are operational links, Cisco DCNM establishes a neighbor.
3. You right click on the port channel and click Delete.

Workaround: This issue is resolved.

- CSCta89605

Symptom: While configuring a peer link port channel setting, vPC creation through the wizard fails with the error message “Error while applying configuration to the device Syntax error while parsing ‘switchport trunk allowed vlan add.’ ”

Send document comments to nexus7k-docfeedback@cisco.com

Conditions: You may see this symptom while creating a vPC through a wizard if you use the existing port channel and try to add a trunk-allowed VLAN to the already configured VLAN list. The Cisco DCNM server fails to deploy the VLAN list to the existing one.

Workaround: This issue is resolved.

- CSCtc76377

Symptom: In the GUI console, Cisco DCNM does not populate tear-off charts correctly.

Conditions: The conditions that lead to this problem are as follows:

- You launch the Cisco DCNM client and start monitoring for a particular entity.
- The chart is not populated with data and Cisco DCNM sends exceptions to the java console.

Workaround: This issue is resolved.

- CSCtc78573

Symptom: When upgrading from 4.2.1 to 4.2.3, if you try to go the previous page in the installation wizard, then the wizard freezes and you cannot move backward or forward because the forward and backward buttons are grayed out.

Conditions: This happens when the installation wizard is used on a Linux Platform.

Workaround: This issue is resolved.

- CSCtc91328

Symptom: The Cisco DCNM GUI shows an invalid status for the supervisor module in the inventory window after an ISSU.

Conditions: You may see this symptom through the DCNM Device OS Management window when an ISSU from Cisco DCNM Release 4.2(2) to Cisco DCNM Release 4.2(3) is performed.

Workaround: This issue is resolved.

- CSCtd02082

Symptom: An internal server error in the vPC wizard occurs after you delete and recreate a vPC.

Conditions: Have an operationally up vPC shown in the Cisco DCNM GUI. Delete a domain in one of the devices using the port-channel feature window. After you delete the vPC in the Cisco DCNM GUI, recreate the vPC with the same device and port-channel in which you deleted the vPC domain.

Workaround: This issue is resolved.

- CSCtd04188

Symptom: In the topology window, links between a managed device and an unmanaged device are not displayed.

Conditions: You may see this symptom during device discovery with the hop count greater than zero. CDP links may not be reflected in the topology if the discovery of neighbor devices fails due to invalid credentials or IP address.

Workaround: This issue is resolved.

- CSCtd08006

Symptom: Device discovery failed with an “Error saving data to DB for <ipaddress>” message.

Conditions:

- The device is reachable from two or more IP addresses (Valid Mgmt IP and any other port IP).

Send document comments to nexus7k-docfeedback@cisco.com

- The device, which has two reachable IP addresses, has been discovered with a non-management IP address in one of the following situations:
 - The same device is being discovered with another IP (Mgmt IP), when another device has been discovered with hop count that is greater than 0.
 - The same device is being discovered with another IP (Mgmt IP) from the device discovery window.

Workaround: This issue is resolved.

- CSCte000875

Symptom: The DCNM Client window does not indicate support for Nexus 4000 Series devices.

Conditions: This symptom may be seen under normal operating conditions for Cisco DCNM.

Workaround: This issue is resolved.

- CSCtf08888

Symptom: If DCNM Release 5.0(2) and Cisco Fabric Manager Release 5.0(1a) are both installed on the same server using Postgres as the database, the DCNM server stops functioning.

Conditions: This symptom may be seen when the DCNM Release 5.0(2) image and the Cisco Fabric Manager Release 5.0(1a) image are on the same machine.

Workaround: This issue is resolved in DCNM Release 5.0(2); however, the fix is not included in Fabric Manager Release 5.0(1a). Therefore, do not install these versions of DCNM and Fabric Manager on the same server. Alternatively, use the Oracle database. The fix will be included in the next 5.0(x) release of Fabric Manager.

Open Caveats—Cisco DCNM Release 4.2



Note

For caveats related to inconsistency between the information displayed in the Cisco DCNM client and the actual state or configuration of a managed device, a common workaround is to press F5 to refresh the Cisco DCNM client.

This section lists the open caveats for Release 4.2(1).

- CSCsu76583

Symptom: The DCNM Inventory window does not show the hardware and software versions of the Cisco Nexus 5000 Series fan and power supply modules.

Conditions: Cisco DCNM relies on the **show hardware** command to display the hardware and software versions of Cisco Nexus 5000 Series fan and power supply modules, but this command is not supported on the Cisco Nexus 5000 Series switch, so Cisco DCNM cannot show any hardware or software versions for those modules.

Workaround: None.

- CSCsu85966

Symptom: Cisco DCNM Release 4.2(1) does not support the vPC preempt option.

Conditions: You see this symptom in all conditions.

Workaround: No workaround.

Send document comments to nexus7k-docfeedback@cisco.com

- CSCsv54482

Symptom: Cisco DCNM is not showing the traffic storm control threshold events in the events tab of the traffic storm control window.

Conditions: When you configure a threshold for a specific traffic type (for example, unicast, multicast, or broadcast) on an interface, and when the traffic on that interface reaches the upper threshold, Cisco DCNM should capture such events and display them in the events tab. Cisco DCNM relies on the switch to send the syslog on the thresholds, but the switch cannot send such syslogs, so Cisco DCNM cannot display those events.

Workaround: None.

- CSCsw63130

Symptom: ImageMgmt: Version Compatibility check from the Cisco DCNM results to Error with the description “refer to client log” or [com.arjuna.ats.internal.jta.transaction.arjunacore.inactive] [com.arjuna.ats.internal.jta.transaction.arjunacore.inactive] The transaction is not active!

Conditions: This issue could occur if the Version Compatibility check operation takes more than 5 minutes.

Workaround: Increase the TransactionTimeout attribute value from 300 to 1000 in the jboss-service.xml file, which in a subdirectory of the jboss server directory.

For example, if Cisco DCNM is installed on a Windows 2003 server in the default location, the jboss server directory is C:\Program Files\Cisco Systems\DCNM\jboss-4.2.2.GA\server\dcnm\conf\jboss-service.xml. Edit the jboss-service.xmlm file and change the TransactionTime attribute value to 1000 as shown:

```
<mbean code="com.arjuna.ats.jbosstx.jta.TransactionManagerService"
  name="jboss:service=TransactionManager">
  <attribute name="TransactionTimeout">1000</attribute>
  <attribute name="ObjectStoreDir">${jboss.server.data.dir}/tx-object-store</attribute>
</mbean>
```

- CSCsw71645

Symptom: A Cisco DCNM discovery fails when the running-configuration file is not valid.

Conditions: You can use the CLI to configure a role that is allowed to make configuration changes on management interfaces, but the Cisco Nexus 5000 Series switch supports only the mgmt0 interface. If you identify the Mgmt interface as mgmt0, the device accepts the configuration, but it displays an incorrect command in the running-configuration file. When Cisco DCNM discovers these devices, device discovery fails.

Sample incorrect configuration:

```
role name Milan
  interface policy deny
    permit interface mgmt1
```

An incorrect configuration shown in the running-configuration file:

```
role name Milan
  interface policy deny
    permit interface mgmt0 on slot 3    <<<<<<<< slot 3 is incorrect.
```

Workaround: Remove the incorrect configuration and use Cisco DCNM to rediscover the device.

Send document comments to nexus7k-docfeedback@cisco.com

- CSCsy81802

Symptom: The Resolve Conflicts window does not show some of the Type 1 fields. A vPC has a consistency status of Failed, and either the Resolve Configuration Inconsistency dialog box indicates that no parameters are shown inconsistent or the STP enabled VLANs are shown inconsistent even if the disabled VLANs are consistent.

Conditions: Parameters (for example, STP MST Region name) that are not supported by the Resolve Configuration Inconsistency dialog box are inconsistent or the STP disabled VLANs are not consistent in peer devices, which Cisco DCNM does not handle.

Workaround: Check the conflicts listed by the **show vpc consistency-parameters global** and manually apply the same configuration as primary in the peer device. The consistency status changes to OK.
- CSCsz50131

Symptom: Cisco Nexus 5000 Series Release 4.1(3)N1(1) images support a maximum of 512 VLANs per switch. If you use the CLI to create more than 512 VLANs, an error occurs. When you use XML to perform the same configuration (Cisco DCNM uses XML to interact with the switch), an error does not occur but Cisco DCNM and the switch are not synchronized.

Conditions: When you use Cisco DCNM create more than 512 VLANs at a time (similar to the range option in CLI), Cisco DCNM will generate the appropriate XML request and send it to the device. Because the Cisco Nexus 5000 Series switch has a limit of 512 VLANs, the switch will create only 512 VLANs. It will not create the remaining VLANs and an error does not occur. Instead, it will send an OK XML response. On receiving the OK XML response, Cisco DCNM assumes that all the VLANs are created in the switch, and it updates its database and shows all those VLANs in the GUI, which causes Cisco DCNM and switch to not be synchronized.

Workaround: Use Cisco DCNM to rediscover the switch. Cisco DCNM will choose the latest status from the switch and display it properly.
- CSCsz67186

Symptom: Cisco DCNM shows an HIF port (FEX downlink port) as a SPAN destination port even though the device does not allow you to configure an HIF port as a SPAN destination. You see this message:

```
Configure an HIF port as a SPAN destination
```

Conditions: Use the CLI to configure a Cisco Nexus 2000 downlink port (also known as an FEX or Fabric Extender) as a SPAN destination interface. An error occurs and a message indicates that HIF ports cannot be configured as SPAN destinations, but a minute later, Cisco DCNM indicates that the HIF port is a SPAN destination in a SPAN window (as if the configuration change was a success).

Workaround: Use Cisco DCNM to rediscover the switch. Cisco DCNM will choose the latest status from the switch and display it properly.
- CSCsz82147

Symptom: When FEX uplinks are part of a port channel member, then the pinning max-link can only be 1 and cannot be modified. When you use Cisco DCNM to perform the configuration, the device accepts any value.

```
<CmdBold>
fex 100
  pinning max-link 1

interface port-channel 10
  switchport mode fex-fabric
  fex associate-id 100
  no shut
```

Send document comments to nexus7k-docfeedback@cisco.com

```
fex 100
  pinning max-link 2 >>>>>> This command will result in error in the CLI.

</CmdBold>
```

When you execute the same command using XML and Cisco DCNM, the command succeeds in the device without causing an error. Cisco DCNM assumes that the pinning has changed in the device and Cisco DCNM starts showing the new configured value.

Conditions: When you configure an FEX pinning max-links value to something other than 1 (even though the FEX uplinks are part of a port channel), Cisco DCNM allows that to occur.

Workaround: When FEX uplinks are part of a port channel, do not change the pinning value to something other than 1.

- CSCsz89132

Symptom: In some cases, Cisco DCNM does not show the correct duplex setting for the Cisco Nexus 2000 host interfaces.

Conditions: This happens for the host interfaces whose duplex setting are set to full. The output for the **show running-config** command does not show the **duplex full** command under these host interfaces, so Cisco DCNM is not able to show the correct duplex settings.

Workaround: None.

- CSCsz96326

Symptom: Cisco DCNM does not show the power supply status change that occurred in the switch.

Conditions: Even after a change in status of the switch power supply, Cisco DCNM continues to show the old power supply status because there is no status change syslog available for the power supply status change. Without that syslog, Cisco DCNM has no means to know that the change has occurred in the switch.

Workaround: Use Cisco DCNM to rediscover the switch. Cisco DCNM chooses the latest status for the switch and displays it properly.

- CSCta02977

Symptom: Cisco DCNM does not show power supply status changes that occur in the FEX.

Conditions: The Cisco DCNM Inventory window shows only the old power supply status even after the power supply status change occurred in FEX because there is no status change syslog available for the power supply unit.

Workaround: Use Cisco DCNM to rediscover the FEX. Cisco DCNM chooses the latest status and displays it properly.

- CSCta13742

Symptom: Even though FEX HIF ports (downlink port) cannot be configured with spanning-tree ports, Cisco DCNM allows you to configure them.

```
interface ethernet 100/1/1
  spanning-tree port type edge
```

You cannot perform the above configuration by using the CLI, but you can perform it using Cisco DCNM.

Conditions: When you use Cisco DCNM to perform the above configuration, the device gets a different validation than when you use the CLI. When you use Cisco DCNM, the switch sends the XML response of "ok," which indicates that the configuration was successful.

Send document comments to nexus7k-docfeedback@cisco.com

Workaround: The above configuration is not supported, so do not perform it. If you do perform it, then use Cisco DCNM to rediscover the device. Rediscovery solves the synchronization issue.

- CSCta13762

Symptom: Even though FEX HIF ports (downlink ports) cannot be configured with spanning-tree ports, Cisco DCNM displays them as configured.

```
Ex: interface ethernet 100/1/1
    spanning-tree port type edge
```

The above configuration is not supported by the CLI, but when you use the CLI to perform it, Cisco DCNM indicates that the above configuration was successful even though the configuration failed in the device.

Conditions: When you use the CLI to perform the above configuration, an error occurs (ERROR: Command not supported on fex port), but the device logs the command status as being successful. When Cisco DCNM reads the show accounting log command response in the next polling cycle, Cisco DCNM determines that the configuration was successful and it displays the configuration in the GUI.

Workaround: The above configuration is not supported, so do not use the CLI to perform it. If you do perform it, then use Cisco DCNM to rediscover the device. Rediscovery solves the synchronization issue.

- CSCta53275

Symptom: After a system switchover, Cisco DCNM displays an incorrect status for the standby supervisor.

Conditions: When you are using Cisco DCNM to manage a Cisco Nexus 7000 switch that has two supervisor modules (the supervisor in slot 5 is active and the supervisor in slot 6 is in standby mode) and there is more than one custom VDC in that device, if you use the **system switchover** command, Cisco DCNM continues to show the status as “initializing (vdc)” even though that supervisor goes back to the ha-standby state. This behavior occurs because the device sends an incorrect syslog.

Workaround: Rediscover the device in Cisco DCNM.

- CSCta73004

Symptom: Even though the device does not allow the FEX HIF ports (downlink ports) to be part of a port channel (when the FEX is connected to two Cisco Nexus 5000 Series switches [dual homed FEX]), Cisco DCNM displays the downlink port as a member of a port channel.

Conditions: Configure an FEX as a dual homed FEX (FEX connected to two Cisco Nexus 5000 Series switches in active-active state). Configure the FEX downlink ports as a part of a port channel as follows:

```
interface ethernet 100/1/1
    channel-group 10
```

The **channel-group 10** command will fail in the CLI because the configuration is not valid.

```
Fabric in Fex A-A mode, can't configure sat port as member
```

During the next polling interval, Cisco DCNM will show the above configuration as successful, even though it failed in the CLI. The command log shows the command status as successful. When Cisco DCNM reads the accounting log, it determines that the command was successful.

Workaround: Use Cisco DCNM to rediscover the switch. Cisco DCNM chooses the latest status for the switch and displays it properly.

- CSCta86487

Send document comments to nexus7k-docfeedback@cisco.com

Symptom: An unmanaged device is shown as a neighbor in the port channel feature window.

Conditions: When the port channels for a device have operating links with port channels of any other device and the neighboring device goes down or is rediscovered, the links still show up.

Workaround: Refresh the window using the Refresh button from the Toolbar or Menu bar or press F5.

- CSCta95512

Symptom: In the Interface port window, under the Detail pane, under the Port details tab, under the Advanced Setting pane, only one SPAN session can be seen for an interface, although more than one SPAN session can be configured for an interface.

Conditions: When you configure an interface as a destination port for more than one SPAN session, Cisco DCNM shows only one SPAN session.

Workaround: None.

- CSCta98661

Symptom: Using Cisco DCNM, you cannot configure both the speed and duplex settings for a port channel at the same time.

Conditions: When there is a port channel that has more than one member port and you try to change the speed and duplex value of the port channel and deploy the configuration using Cisco DCNM, the configuration fails.

Workaround: None.

- CSCtb17617

Symptom: The operational status of administratively up interfaces is not synchronized with the device.

Conditions: After a module reset occurs, the operational status of the interfaces that belong to the module are not synchronized with the device if the port is administratively up.

Workaround: Enter the **shutdown** command on the interface and then enter the **no shutdown** command.

- CSCtb85263

Symptom: Cisco DCNM does not show the MST port status properly.

Conditions: In the root switch, if you enable the root guard to the ports connected to the nonroot switch, the status of the port connected to the nonroot switch changes to Broken and moves to the Root inconsistent state, but Cisco DCNM shows the port status as Blocked instead of Broken. The switch sends the XML response as Blocked(BLK) instead of Broken(BKN).

Workaround: None.

- CSCtc05207

Symptom: The vPC creation wizard fails and reports a Network Element Exception.

Conditions: The port channels that are selected for a vPC/Peer-link are mapped to port profiles via the "inherit port profile" CLI or interfaces. The interfaces that are selected for a vPC/Peer-link port-channel members are mapped to port profiles via the "inherit port profile" CLI.

Workaround: Follow these steps:

1. Close the wizard.
2. Remove the port profile inheritance from the interfaces/port channels from the CLI.
3. If a vPC is partially created, rerun the wizard using the modify sequence.

Send document comments to nexus7k-docfeedback@cisco.com

4. If a vPC is not created, rerun the wizard.
- CSCtc37951

Symptom: Cisco DCNM server creates a new VlanAccessMapEntry instead of modifying the properties of the existing VlanAccessMapEntry for device CLI changes.

Conditions: Problem occurs when you create, modify, or delete VlanAccessMapEntry without using a sequence number.

Workaround: You should create, update, or delete vace with a sequence number from the device CLI.
 - CSCtc76410

Symptom: Cisco DCNM does not show the port channel speed changes when you are creating or editing FEX-VPCs.

Conditions: When using Cisco DCNM to configure the port-channel speed as 1000, the speed change is not reflected on the device because the speed change is not supported in the FEX fabric interface.

The accounting log shows a Success message instead of a Failure message when you apply a speed value 1000.

Workaround: None.

Related Documentation

This section includes the following topics:

- [Platform-Specific Release Notes, page 27](#)
- [Cisco DCNM Documentation, page 28](#)

Platform-Specific Release Notes

The software release notes for the platforms that Cisco DCNM supports are available on Cisco.com at the following locations:

- Cisco Nexus 7000 Series NX-OS Release Notes
http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html
- Cisco Nexus 5000 Series Release Notes
http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html
- Cisco Nexus 4000 Series Release Notes
http://www.cisco.com/en/US/products/ps10596/prod_release_notes_list.html
- Cisco Nexus 2000 Series Release Notes
http://www.cisco.com/en/US/products/ps10110/prod_release_notes_list.html
- Cisco Nexus 1000V Series Release Notes
http://www.cisco.com/en/US/products/ps9902/prod_release_notes_list.html

Send document comments to nexus7k-docfeedback@cisco.com

Cisco DCNM Documentation

Cisco DCNM documentation is available on Cisco.com at the following location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

The documentation for Cisco DCNM includes the following:

- *Cisco DCNM Installation and Licensing Guide, Release 5.x*
- *Cisco DCNM Fundamentals Configuration Guide, Release 5.x*
- *Cisco DCNM System Management Configuration Guide, Release 5.x*
- *Cisco DCNM Interfaces Configuration Guide, Release 5.x*
- *Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*
- *Cisco DCNM Security Configuration Guide, Release 5.x*
- *Cisco DCNM Unicast Routing Configuration Guide, Release 5.x*
- *Cisco DCNM Getting Started with Virtual Device Contexts, Release 5.x*
- *Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*
- *Cisco DCNM Web Services API Guide, Release 5.x*

Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008-2010 Cisco Systems, Inc. All rights reserved.