



Cisco DCNM Release Notes, Release 6.1

Release Date: November 30, 2012
Part Number: OL-26852-04 D0
Current Release: 6.1(2)

This document provides the release notes for Cisco Data Center Network Manager (DCNM), Release 6.1. Use this document in combination with the documents listed in the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 33.



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.

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-26852-01	A0	June 28, 2012	Created release notes for Release 6.1(1).
OL-26852-02	A0	July 5, 2012	Created release notes for Release 6.1(1a).
	B0	July 12, 2012	Updated the “Java Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN” section.
	C0	July 24, 2012	Updated the “Server System Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN” section.
	D0	August 13, 2012	<ul style="list-style-type: none">Removed the Cisco Nexus 1010-X Virtual Services Appliance as a supported device.Added a best practice about user authentication to the “Deployment Best Practices” section.
	E0	August 23, 2012	Added a Note about Cisco DCNM Essentials Edition to the “Licensing” section.



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

Table 1 Online History Change (continued)

Part Number	Revision	Date	Description
OL-26852-03	A0	September 13, 2012	Created release notes for 6.1(1b).
	B0	October 16, 2012	Added CSCth49735 to the “Resolved Caveats—Cisco DCNM SAN Release 6.1(1a)” section.
	C0	October 18, 2012	Added a limitation about the license installer to the “General Limitations for Cisco DCNM Release 6.1” section.
OL-26852-04	A0	November 30, 2012	Created release notes for Release 6.1(2).
	B0	December 12, 2012	Added CSCud47550 to the “Resolved Caveats—Cisco DCNM SAN Release 6.1(2)” section.
	C0	January 31, 2013	Updated system server requirements. Added resolved caveat CSCuc55057 to the “Resolved Caveats—Cisco DCNM LAN Release 6.1(2)” section.
	D0	February 14, 2013	Updated the system server requirements for Microsoft Windows 2008.

Contents

This document includes the following sections:

- [Introduction, page 3](#)
- [System Requirements, page 3](#)
- [Supported Cisco Platforms and Software Versions, page 7](#)
- [Hardware Supported, page 7](#)
- [Software Download Site, page 10](#)
- [Deployment Best Practices, page 10](#)
- [Installation Notes, page 11](#)
- [New Features and Enhancements in Cisco DCNM Release 6.1, page 12](#)
- [Licensing, page 16](#)
- [Limitations in Cisco DCNM Release 6.1\(x\), page 17](#)
- [Caveats, page 18](#)
- [Related Documentation, page 30](#)
- [Obtaining Documentation and Submitting a Service Request, page 33](#)

Introduction

Cisco Data Center Network Manager combines the management of Ethernet and storage networks into a single dashboard to help network and storage administrators manage and troubleshoot health and performance across the following product families that run Cisco NX-OS software:

- Cisco MDS 9500 Series Multilayer Directors and Cisco MDS 9200 and 9100 Series Multilayer Switches
- Cisco Nexus 1000V Series Switches and Cisco Nexus 1010 Virtual Services Appliance
- Cisco Nexus 2000 Series Fabric Extenders
- Cisco Nexus 3000, 4000, 5000, and 7000 Series Switches
- Cisco Catalyst 6500 Series Switches
- Cisco UCS 6100 and 6200 Series Fabric Interconnects
- Cisco FireWall Service Module (FWSM)

System Requirements

This section lists the software that Cisco has tested and supports for Cisco DCNM-LAN and Cisco DCNM-SAN. Both Cisco DCNM-LAN and Cisco DCNM-SAN have been tested in English locales only.

This section includes the following topics:

- [Supported Databases for Cisco DCNM-LAN and Cisco DCNM-SAN, page 3](#)
- [Java Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN, page 4](#)
- [Server System Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN, page 4](#)
- [Client System Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN, page 6](#)
- [Browsers, page 6](#)
- [Other Supported Software, page 6](#)
- [Supported Cisco Platforms and Software Versions, page 7](#)
- [Hardware Supported, page 7](#)

Supported Databases for Cisco DCNM-LAN and Cisco DCNM-SAN

Cisco DCNM Release 6.1(x) supports the following databases:

- Oracle 10g and Oracle11g Express (XE), Standard, and Enterprise Editions, and Oracle 11g Real Application Clusters (RAC).
 - We recommend deploying Oracle 10g or Oracle11g for mission-critical production environments.
 - We recommend Oracle RAC for high availability of your Cisco DCNM database.
- PostgreSQL 8.3
 - We recommend PostgreSQL for nonproduction or lab environments.

**Note**

Customers are responsible for all support associated with Oracle and PostgreSQL databases, including maintenance, troubleshooting, and recovery. Cisco recommends that customers perform regular database backups, either daily or weekly, to ensure that all data is preserved.

Java Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN

Cisco DCNM is a Java-based client-server application. Cisco DCNM Server is distributed with Java JRE 1.6.0_31. We recommend that Cisco DCNM clients use Java JRE 1.6.0_31. The DCNM installer installs JRE 1.6.0_31 to the following directory: DCNM_root_directory/java/jre1.6.

Server System Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN

Cisco DCNM Release 6.1(x) supports running the Cisco DCNM-LAN and Cisco DCNM-SAN servers on these operating systems:

- Microsoft Windows 2003, 32-bit or 64-bit with Service Pack 2
- Microsoft Windows 2008 R2 SP1 and Windows 2008 Standard SP2 (32-bit and 64-bit)
- Red Hat Enterprise Linux Release 5.6 and 5.7 (32-bit and 64-bit) or a lower version

**Note**

If a service pack for the Windows operating system is not listed, the service pack is not supported.

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

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

Component	Minimum Requirements	Recommended Requirements
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

SAN-Only Cisco DCNM Server Requirements

Table 4 lists the server resource requirements for deploying Cisco DCNM in a SAN-only environment.

Table 4 Cisco DCNM Server Resources for a SAN-Only Environment

Small SAN: Up to 50 Switches and Up to 2000 Ports	Medium SAN: Up to 200 Switches and Up to 5000 Ports	Large SAN: More than 200 Switches and More than 5000 Ports
Dual Core CPUs, 2 GHz	Quad Core CPUs, 2 Ghz	Quad Core CPUs, 2 Ghz
4-GB memory, 60-GB free hard disk	8-GB memory, 80-GB free hard disk	12-GB memory, 100-GB hard disk
PostgreSQL, Oracle 10g, and Oracle11g Express (XE)	Oracle 10g and Oracle11g Express (XE) or Standard	Oracle11g Standard or Enterprise

LAN-Only Cisco DCNM Server Requirements

Table 5 lists the server resource requirements for deploying Cisco DCNM in a LAN-only environment.

Table 5 Cisco DCNM Server Resources for a LAN-Only Environment

Small LAN: Up to 25 Switches and Up to 1000 Ports	Medium LAN: Up to 100 Switches and Up to 3000 Ports	Large LAN: More than 100 Switches and More than 3000 Ports
Dual Core CPUs, 2 GHz	Quad Core CPUs, 2 Ghz	Quad Core CPUs, 2 Ghz
4-GB memory, 60-GB free hard disk	8-GB memory, 80-GB free hard disk	12-GB memory, 100-GB hard disk LAN clustering to scale
PostgreSQL, Oracle 10g, and Oracle11g Express (XE)	Oracle 10g and Oracle11g Express (XE) or Standard	Oracle11g Standard or Enterprise

LAN and SAN Cisco DCNM Server Requirements

Table 6 lists the server resource requirements for deploying Cisco DCNM in a LAN and SAN environment.

Table 6 Cisco DCNM Server Resources for a LAN and SAN Environment

LAN: 25 Switches and up to 1000 Ports SAN: 50 Switches and up to 2000 Ports	LAN: 100 Switches and up to 3000 Ports SAN: 200 Switches and up to 5000 Ports
Dual Core CPUs, 2 GHz	Quad Core CPUs, 2 Ghz
8-GB memory, 80-GB free hard disk	12-GB memory, 100-GB free hard disk 2 servers, LAN or SAN cluster or federation
Oracle 10g, Oracle11g Standard or Enterprise	Oracle11g Standard or Enterprise

**Note**

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

Client System Requirements for Cisco DCNM-LAN and Cisco DCNM-SAN

Table 7 lists the minimum hardware requirements for these client systems.

Table 7 *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)	2 GB

If Cisco DCNM-LAN and DCNM-SAN clients are launched together, the need for more CPU and memory goes up to 2.0 GHz, 2 GB of free RAM, and 200 MB of free disk space.

**Note**

If you install Cisco DCNM-SAN in a virtual machine, we recommend that you reserve resources equal to the server resource requirements to ensure a baseline with physical machines.

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 6.x](#).

Be sure to set the correct time zone value on the system clock (for example, UTC). Otherwise, Cisco DCNM-LAN cannot manage the switch properly.

Browsers

Web browsers that support Adobe Flash 10 are qualified for use with Cisco DCNM. These include Internet Explorer, Firefox, and Safari.

Other Supported Software

Table 8 lists other software supported by Cisco DCNM Release 6.1(x).

Table 8 *Other Software Supported by Cisco DCNM*

Other Supported Software
Security:
ACS Versions, 4.0, and 5.1
Firewall/Cisco DCNM-SAN Server Proxy: PIX Firewall, IP Tables
Telnet Disabled: SSH version 1, SSH version 2, Global Enforce SNMP Privacy Encryption

Table 8 Other Software Supported by Cisco DCNM (continued)**Other Supported Software**

Web Client and Cisco DCNM-SANServer Encryption: HTTPS

Performance Manager:

SNMP over UDP

SNMP over TCP

VMs:

VMs that run any qualified or supported operating system version can run Cisco DCNM.

In addition, Cisco DCNM supports the following types of events: EMC Call Home events, fabric change events, and events that are forwarded by traps and e-mail.

Supported Cisco Platforms and Software Versions

For information about the software platforms and versions that Cisco DCNM supports, see the [Cisco DCNM Release Compatibility Matrix](#).

**Note**

For compatibility reasons, we recommend that you run the same version (or a later version) of Cisco DCNM as Cisco NX-OS software.

Cisco DCNM-SAN Release 6.1(1b) and later releases do not support Cisco Nexus 5000 Series switches and UCS devices running Cisco NX-OS Release 4.1(3) or an earlier release.

Hardware Supported

[Table 9](#) lists the products and components that Cisco DCNM Release 6.1 supports.

Table 9 Hardware Features Supported by Cisco DCNM Release 6.1

Product/Component	Part Number
Cisco MDS 9000 Family	
Cisco MDS 9513 Multilayer Director	DS-C9513
Cisco MDS 9509 Multilayer Director	DS-C9509
Cisco MDS 9506 Multilayer Director	DS-C9506
Cisco MDS 9222i Multilayer Fabric Switch	DS-C9222i-K9
Cisco MDS 9216i Multilayer Fabric Switch	DS-C9216i-K9
Cisco MDS 9148 48-Port Multilayer Fabric Switch	DS-C9148-K9
Cisco MDS 9134 34-Port Multilayer Fabric Switch	DS-C9134-K9

Table 9 Hardware Features Supported by Cisco DCNM Release 6.1 (continued)

Product/Component	Part Number
Cisco MDS 9124 24-Port Multilayer Fabric Switch	DS-C9124-K9
Cisco MDS 9500 Series Supervisor-2 Module	DS-X9530-SF2-K9
Cisco MDS 9500 Series Supervisor-2A Module	DS-X9530-SF2A-K9
Cisco MDS 9500 Series Supervisor-1 Module	DS-X9530-SF1-K9
Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module	DS-X9112
Cisco MDS 9000 24-port 4-Gbps Fibre Channel Switching Module	DS-X9124
Cisco MDS 9000 48-port 4-Gbps Fibre Channel Switching Module	DS-X9148
Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module	DS-X9704
Cisco MDS 9000 Family 14-Port Fibre Channel and 2-port Gigabit Ethernet Module	DS-X9302-14K9
Cisco MDS 9000 16-Port 2-Gbps Fibre Channel Switching Module	DS-X9016
Cisco MDS 9000 32-Port 2-Gbps Fibre Channel Switching Module	DS-X9032
Cisco MDS 9000 32-Port Storage Services Module	DS-X9032-SSM
Cisco MDS 9000 8-port 1-Gbps IP Storage Module	DS-X9308-SMIP
Cisco MDS 9000 4-port 1-Gbps IP Storage Module	DS-X9304-SMIP
Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module	DS-X9224-96K9
Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module	DS-X9248-96K9
Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module	DS-X9248-48K9
Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) Module	DS-X9708-K9
Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module	DS-X9232-256K9
Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module	DS-X9248-256K9
Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16)	DS-X9316-SSNK9
Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)	DS-X9304-18K9
Cisco Nexus 7000 Series Switches	
Cisco Nexus 7004 chassis	N7K-C7004
Cisco Nexus 7009 chassis	N7K-C7009
Cisco Nexus 7010 chassis	N7K-C7010
Cisco Nexus 7018 chassis	N7K-C7018
Supervisor 1 module	N7K-SUP1
Supervisor 2 module	N7K-SUP2
Supervisor 2 Enhanced module	N7K-SUP2E
Fabric module, Cisco Nexus 7018 chassis	N7K-C7018-FAB-2
Fabric module, Cisco Nexus 7018 chassis	N7K-C7018-FAB-1

Table 9 Hardware Features Supported by Cisco DCNM Release 6.1 (continued)

Product/Component	Part Number
Fabric module, Cisco Nexus 7010 chassis	N7K-C7010-FAB-2
Fabric module, Cisco Nexus 7010 chassis	N7K-C7018-FAB-1
Fabric module, Cisco Nexus 7009 chassis	N7K-C7009-FAB-2
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
32-port 10-Gigabit Ethernet SFP+ I/O module with XL Option	N7K-M132XP-12L
8-Port 10-Gigabit Ethernet Module with XL Option (requires X2)	N7K-M108X2-12L
2-port 100-Gigabit Ethernet I/O module with XL option	N7K-M202CF-22L
6-port 40-Gigabit Ethernet I/O module with XL option	N7K-M206FQ-23L
24-port 10-Gigabit Ethernet I/O module with XL option	N7K-M224XP-23L
32-port 1- and 10-Gigabit Ethernet SFP+ I/O module	N7K-F132XP-15
48-port 1/10 Gigabit Ethernet SFP+ I/O module (F2 Series)	N7K-F248XP-25
48-port 1/10 Gigabit Ethernet SFP+ I/O module (Enhanced F2 Series)	N7K-F248XP-25E
48 Port 1/10 GBase-T RJ45 Module (Enhanced F2-Series)	N7K-F248XT-25E
Cisco Nexus 5000 Series Switches	
Cisco Nexus 5596UP Switch	N5K-C5596UP-FA
Cisco Nexus 5548UP Switch	N5K-C5548UP-FA
Cisco Nexus 5548P Switch	N5K-C5548P-FA
Cisco Nexus 5010 chassis	N5K-C5010P-BF
Cisco Nexus 5020 chassis	N5K-C5020P-BF
	N5K-C5020P-BF-XL
Cisco Nexus 0296-UPT chassis and GEM N55-M12T support	N5K-C5596T-FA-SUP
16-port Universal GEM, Cisco Nexus 5500	N5K-M16UP
Layer 3 GEM, Cisco Nexus 5596	N5K-M160L3
Layer 3 GEM	N55-M160L3-V2
Layer 3 module, Cisco Nexus 5548	N55-D160L3
Version 2, Layer 3 daughter card	N55-D160L3-V2
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=
Cisco Nexus 4000 Series Switches	
Cisco Nexus 4001I Switch Module	N4K-4001I-XPX

Table 9 Hardware Features Supported by Cisco DCNM Release 6.1 (continued)

Product/Component	Part Number
Cisco Nexus 4005I Switch Module	N4K-4005I-XPX
Cisco Nexus 3000 Series Switches	
Cisco Nexus 3016 Switch	N3K-C3016Q-40GE
Cisco Nexus 3048 Switch	N3K-C3048TP-1GE
Cisco Nexus 3064 Switch	N3K-C3064PQ
Cisco Nexus 3064-E Switch	N3K-C3064PQ-10GE
Cisco Nexus 3064-X Switch	N3K-C3064PQ-10GX
Cisco Nexus 3548 Switch	N3K-C3548P-10G
Cisco Nexus 2000 Series Fabric Extenders	
Cisco Nexus 2148 1 GE Fabric Extender	N2K-C2148T-1GE
Cisco Nexus 2224TP Fabric Extender	N2K-C2224TP-1GE
Cisco Nexus 2232TM 10GE Fabric Extender	N2K-C2232TM-10GE
Cisco Nexus 2232TM 10GE Fabric Extender	N2K-C2232TM-E-10GE
Cisco Nexus 2232PP 10 GE Fabric Extender	N2K-C2232PP-10GE
Cisco Nexus 2248TP 1 GE Fabric Extender	N2K-C2248TP-1GE
Cisco Nexus 2248TP E GE Fabric Extender	N2K-C2248TP-E GE
Cisco Nexus 222 Fabric Extender for HP	N2K-B22HP-P
Cisco Nexus 222 Fabric Extender for Fujitsu	N2K-B22FJ-P
Cisco Nexus 1000V Series Switch	
Cisco Nexus 1010 Virtual Services Appliance	N1K-C1010
Cisco Nexus 1010-X Virtual Services Appliance	N1K-C1010-X
Catalyst 6500 Switches	

Software Download Site

To download the latest Cisco DCNM software, go to <http://www.cisco.com/go/dcnm> and click Download Software.



Note

If you would like to request a copy of the source code under the terms of either GPL or LGPL, send an e-mail to mds-software-disclosure@cisco.com.

Deployment Best Practices

Observe the following guidelines when deploying Cisco DCNM:

- During the initial installation, disable all security and antivirus tools that are running on your server.

- Do not run any other management applications on the Cisco DCNM server or the Cisco DCNM database server.
- When Cisco DCNM is deployed as a virtual machine (VM), do not share CPU and memory resources with other VMs on the virtual host.
- When Cisco DCMM is deployed as a VM, do not share the data store with other VMs.
- Do not deploy Cisco DCNM when network latency is more than 50 ms from the switch management subnet to the Cisco DCNM server and Cisco DCNM database.
- Deploy an Oracle database when managing production or mission critical environments.
- Deploy an Oracle database on a separate server from the Cisco DCNM application server.
- Deploy Cisco DCNM on high-performance tier storage (2 ms to 4 ms response time).
- Deploy Cisco DCNM SAN in a federated configuration when the switch count exceeds 150 switches or the port count exceeds 15,000 connected ports per management server (whichever comes first).
- 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 500 from the default of 300.
- Create users with the same password digest (for example, MD5) and encryption algorithm (for example, DES) for the same user on all switches in the Fibre Channel fabric. (MD5 and DES are the defaults.) Otherwise, Cisco DCNM-SAN will not be able to authenticate a user on the fabric if that user has different digest and encryption algorithms.

Installation Notes

The following installation notes apply to Cisco DCNM Release 6.1:

- The Cisco DCNM Installer installs Cisco DCNM LAN, SAN, and SMI-S together.
- The installer is bundled with PostgreSQL 8.3 and Strawberry Perl version 5.10.0.
- Cisco DCNM installers are available in 32-bit and 64-bit versions.
- Upgrade support is available from Cisco DCNM Release 5.2(x), Cisco DCNM-LAN Release 5.2(x), and Cisco DCNM-SAN Release 5.2(x) to Cisco DCNM Release 6.1.



Note Cisco DCNM SAN Release 6.1(1a) and later releases do not support running the Cisco DCNM SAN client in standalone mode. If you were running the SAN client in standalone mode in Release 5.2(x), you should uninstall it and install Cisco DCNM SAN server Release 6.1(1a) or a later release. You cannot upgrade the standalone SAN client from DCNM Release 5.2(x) to Release 6.1(1a) or a later release.

For information about installing and uninstalling Cisco DCNM Release 6.(x), see the *Cisco DCNM Installation and Licensing Guide, Release 6.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

Oracle 11g Express Password Expiration

By default, the password for the Oracle 11g Express (XE) database expires after 180 days. You can change this setting by following these steps:

1. Log in to the Oracle database.
2. Enter the commands as shown in this example:

```
SQL> GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO username IDENTIFIED BY password;
Grant succeeded.
SQL> select username,password from dba_users where username='username';
SQL> ALTER PROFILE DEFAULT LIMIT
      2 FAILED_LOG_ATTEMPTS UNLIMITED
      3 PASSWORD_LIFE_TIME UNLIMITED;
Profile altered.
SQL> EXIT
```

PostgreSQL Installation Bundle

Cisco DCNM Release 6.1(1b) includes an option for a bundled PostgreSQL installation. During this type of installation, the authentication for the user “postgres” is autogenerated, and the install wizard skips the DB Admin Username and DB Admin Password fields. As a result, the password is not known so it is not possible to access the database with administrator privileges.

In addition, if a user has an existing database instance that was installed as part of Cisco DCNM and wants to create another login role to be used with another Cisco DCNM install elsewhere, the user will not be able to log in to the PostgreSQL server because the password is unknown.

If access to database is required for backup purposes, you can use a database front-end tool, such as PGAdmin3, to connect to the database. When doing so, set the database field to the database name used during the installation (dcmdb is the default name). Enter the username and password provided during the installation as the database login credentials.

New Features and Enhancements in Cisco DCNM Release 6.1

Cisco DCNM Release 6.1 is a major release that includes new features, enhancements, and hardware.

Common Features

The following features are available in the web client for both Cisco DCNM LAN and Cisco DCNM SAN:

- Summary, host, and switch dashboards
- Last 24-hour view of the most active host, ISLs or trunks, and storage ports (as measured by packets sent)
- Peak utilization switch topology view with mouseovers
- Customizable switch and fabric groups
- Switch health percent indicator and chart
- Web template-based engine that provides Cisco certified templates that are customizable

- Template-based engine that can be leveraged for storing existing LAN and SAN scripts or turning them into templates
- VM Path analytics through vCenter northbound API integration that provides the visibility into performance of virtual hosts and their virtual machines
- Search engine with in-context based cross-launch dashboards
- Application and switch-based user accounting logs
- Events browser with acknowledge and delete functions
- Policy-based event forwarding through e-mail and traps
- Historic performance trending and forecasting
- Capacity manager that provides port tier utilization and forecast analysis
- Lightweight Directory Access Protocol (LDAP) remote authentication that adds to existing TACACS+ and RADIUS protocols
- Inventory based on physical and logical path attributes
- Template-based and custom reports that include switch health, performance, and discrepancies
- Backup of switch configuration files with compare and copy functions

New Features in Cisco DCNM Release 6.1(1a)

The following new features are available in Cisco DCNM Release 6.1(1a):

- VM-aware path for LAN leveraging vCenter APIs (VM-aware path for LAN is already available in Cisco DCNM Release 5.2 through integration with Cisco Nexus 1000v that covers VMware hypervisors)
- The host dashboard now provides a unified fabric view of a host regardless of LAN or SAN protocols
- Switch and storage dashboards
- Capacity Manager that provides port tier utilization and forecast analysis
- Web template-based provisioning for SAN and LAN
- Templates for OTV, FCoE, port channel, zoning, and so on
- OTV Wizard
- Script import
- Switch health bar
- Support for Cisco firewall service module (FWSM)
- Event acknowledge and delete
- Custom groupings for dashboard selection
- Device Manager for Cisco Nexus 7000 Series virtual device connect (VDC)
- LAN web reports
- LDAP support (remote authentication protocol)
- Port mapper report showing spanning tree protocol (STP), Per VLAN Spanning Tree (PVST), Cisco's Rapid per VLAN Spanning Tree (RPVST), Multiple Spanning Tree protocol (MST) status
- Virtual port channel (vPC) inconsistency report and auto resolve

- Cross launch to CiscoView
- Virtual eXtensible Local Area Network (VXLAN) support for Cisco Nexus 1000v
- Host tracking
- Support for FabricPath on the Cisco Nexus 5500 Series switch

Enhancements in Cisco DCNM Release 6.1(1a)

The following enhancements are available in Cisco DCNM Release 6.1(1a):

- License installation and assignment are now part of the web client
- License that is triggered by automated performance discovery
- LAN-based event forwarding (e-mail or trap) on facility and severity
- Event entity consolidation: alert count or first and last seen
- The search engine is extended to MAC and IP address
- The search engine provides an in-search context-launch dashboard
- Consolidation of traps and syslogs
- Both LAN and SAN data sources are part of the web client
- Two levels of LAN discovery (quick and detailed)
- Column search filters
- Consolidated LAN and SAN configuration archive, compare, and copy
- Accounting logs track application changes for Cisco DCNM
- Enhanced host autoresolution for Cisco DCNM SAN
- Maintaining peak utilization trending for a year
- Host and storage dashboard topology include all versus first shortest-path selection
- Host and storage dashboard topology with switch and link health status and cross-launch capability into switch dashboard
- Data sources provide a list of switches collected
- Support for Oracle RAC
- SME Disk snapshot and master key recovery
- Smart Zoning Wizard

Platform-Specific Features

Cisco DCNM Release 6.1 supports certain platform-specific features:

- Cisco Nexus 1000V Series: Virtual eXtensible Local Area Network (VXLAN) features that address the requirements of Layer 2 and Layer 3 data center network infrastructures in the presence of VMs in a multitenant environment.
- Cisco Nexus 5000 Series: Single-click Fabric Extender (FEX) setup, two-layer virtual port channel (vPC), and FabricPath licensing.
- Cisco Nexus 5000 Series: two-layer vPC feature.

- Cisco Nexus 5000 Series: FabricPath support.
- Cisco Nexus 5000 Series: support for Cisco NX-OS Release 5.2(1)N1(1).
- Cisco Nexus 7000 Series: Admin virtual device connect (VDC) support, storage VDC creation and management without licensing, and overlay transport virtualization (OTV) wizard.
- Firewall Service Module (FWSM) support

New Features in Cisco DCNM Release 6.1(1b)

Cisco DCNM Release 6.1(1b) is a maintenance release with bug fixes. It does not include new features.

New Features in Cisco DCNM Release 6.1(2)

The following new features are available in Cisco DCNM Release 6.1(2):

- Cisco DCNM Server federation offers high availability (automatic failover).
- The Performance Manager Printer Report shows Rx and Tx peaks.
- The Performance Manager shows Rx, Tx, PeakRx, and PeakTx utilization percentage.
- The Performance Manager provides data export in a unit-less number for CSV/Excel format.
- The host and storage dashboard Performance Manager traffic chart shows events.
- An alert notification for new events has been added to the Health Events table.
- NPV discovery property is enabled in the discovery dialog box.
- The switch dashboard shows a 24-hour Rx and Tx chart.
- A map toggle allows you to hide or show NPV switches.
- Host enclosure names can now be edited in the host dashboard.
- Host tracking is enhanced to include these features:
 - An option to delete servers that are timed out, such as when a server's MAC address has timed out on a Cisco Nexus switch.
 - Servers that are removed from the network are automatically removed from the Network Servers screen.
- Device groups are enhanced to be in sync for both Cisco DCNM LAN and the web client.
- NPV devices now show attached ports as non-loop ports.
- End-to-end path does not show loops in a topology.
- A Move Fabric task and a Move LAN task have been added to the web client.
- A search capability to edit all local zone sets panels has been added.
- SAN scope device alias creation and modification has been enhanced.
- A 24-hour Performance Manager chart in the topology view for the summary dashboard is now available.
- The capability to show when the Performance Manager threshold exceeds a percentage in the data center summary ISL and host or storage pods is now available.
- Cisco DCNM LAN now supports TCP clustering.
- OTV overlay support is now available.

- IPv6 features, including HSRP and interfaces, are now supported on Cisco Nexus 5000 Series and Cisco Nexus 5500 Series devices.
- VM FEX extends the fabric from the Cisco Nexus 5500 Series platform switch chassis such as the Cisco Nexus 5548UP, Cisco Nexus 5596UP to the Virtual Machine (VM).
- The Adapter-FEX provides the benefits of the Cisco Fabric Extender Link (FEXLink) architecture with that of a server I/O virtualization to create multiple virtual interfaces over a single Ethernet interface that allows the deployment of a dual-port NIC on the server.
- This release supports the Cisco Nexus 3000 Series, including the Cisco Nexus 3064-TQ switch and feature support for Cisco NX-OS Release 5.0(3)U4(1) and later releases.
- Support for the following features on the Cisco Nexus 3000 Series is provided:
 - IPv6 addressing for routed interfaces, subinterfaces, switch virtual interfaces (SVI), and port-channel interfaces
 - IPv6 support for router ACLs
 - HSRP support (both IPv4 and IPv6)
- This release supports the Cisco Nexus 7004 switch and the Cisco Nexus 7000 Enhanced F2-Series 48-port 1/10 Gigabit Ethernet SFP+ I/O module and the Cisco Nexus 7000 Enhanced F2-Series 48 Port 1/10 GBase-T RJ45 Module.
- Support for the Catalyst 6000 Supervisor 2T is available in this release.

Licensing

The essential product features that come with Cisco DCNM are referred to as Cisco DCNM Essentials Edition, even though they do not require a license. They are included at no cost and are a part of the image that can be downloaded from <http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>.



Note

Cisco DCNM Essentials Edition supports the Cisco DCNM client-server application, which cannot be run in standalone mode. Earlier releases of Cisco DCNM SAN supported running the Cisco DCNM SAN client in standalone mode, but Cisco DCNM SAN Release 6.1(1a) and later releases do not support that.

The Cisco DCNM Advanced Edition license adds capabilities such as vCenter integration, performance trending, advanced provisioning, backup, dashboards, and scale-out architecture. Cisco DCNM Advanced Edition can be licensed for both LAN and SAN switches using the product IDs listed in [Table 10](#).

Table 10 Cisco DCNM Advanced Edition License Product IDs

Product	PID, Paper Delivery (envelope)	PIDS, Electronic Delivery (e-mail)	Service Contract PIDs
Cisco MDS 9500	DCNM-SAN-M95-K9=	L-DCNM-SAN-M95-K9=	CON-SAU-SM95K9
Cisco MDS 9200	DCNM-SAN-M92-K9=	L-DCNM-SAN-M92-K9=	CON-SAU-SM92K9
Cisco MDS 9100	DCNM-SAN-M91-K9=	L-DCNM-SAN-M91-K9=	CON-SAU-SM91K9
Cisco Nexus 7000 SAN	DCNM-SAN-N7K-K9=	L-DCNM-SAN-N7K-K9=	CON-SAU-N7SDCNM
Cisco Nexus 7000 LAN	DCNM-N7K-K9=	L-DCNM-N7K-K9=	CON-SAU-N7DCNM
Cisco Nexus 5000 SAN	DCNM-SAN-N5K-K9=	L-DCNM-SAN-N5K-K9=	CON-SAU-N5SDCNM

Table 10 Cisco DCNM Advanced Edition License Product IDs (continued)

Product	PID, Paper Delivery (envelope)	PIDS, Electronic Delivery (e-mail)	Service Contract PIDs
Cisco Nexus 5000 LAN	DCNM-LAN-N5K-K9=	L-DCNM-LAN-N5K-K9=	CON-SAU-N5DCNM
Cisco Nexus 5000 SAN and LAN	DCNM-LS-N5K-K9=	L-DCNM-LS-N5K-K9=	CON-SAU-N5LSDCNM
Cisco Nexus 3000	DCNM-LAN-N3K-K9=	L-DCNM-LAN-N3K-K9=	CON-SAU-N3DCNM

**Note**

Cisco Nexus Access licenses (DCNM-NXACC-100-K9 and DCNM-NXACC-250-K9) are no longer available in Cisco DCNM Release 6.1(1a) and later releases.

Product IDs for Cisco Fabric Manager licenses are listed in [Table 11](#).

Table 11 Cisco Fabric Manager License Product IDs

Platform	PID, Paper Delivery (envelope)	PID, Electronic Delivery (e-mail)
Cisco MDS 9500	M9500FMS1K9=	L-M9500FMS1K9=
Cisco MDS 9200	M9200FMS1K9=	L-M9200FMS1K9=
Cisco MDS 9100	M9100FMS1K9=	L-M9100FMS1K9=
Cisco Nexus 5000 SAN	N5000FMS1K9=	L-N5000FMS1K9=

In addition, Cisco DCNM supports the existing switch based SAN license, FMS_SERVER_PKG. For additional information about Cisco Fabric Manager licenses, see the [Cisco Fabric Manager Release Notes](#) on Cisco.com.

Service contract PIDs are required for opening a case with TAC for breakage or repair and for upgrade from older versions of Cisco DCNM and Fabric Manager. You can also select Cisco DCNM as part of the purchase of a switch chassis, under software options. For more information on licensing, see the FAQs at this URL: http://www.cisco.com/en/US/products/ps9369/prod_literature.html.

Registering a Product Authorization Key

To receive a Cisco DCNM license, you must register the Product Authorization Key (PAK) that you receive when you purchase Cisco DCNM. To register the PAK, follow these steps:

1. Go to <http://www.cisco.com/go/license>.
2. Enter the PAK, contact information, and MAC address or host ID of the Cisco DCNM server.

The license is sent as an e-mail attachment or downloaded directly to your Cisco DCNM Server, depending on which option you select.

Limitations in Cisco DCNM Release 6.1(x)

This section includes the following topics:

- [General Limitations for Cisco DCNM Release 6.1, page 18](#)

- [Limitations for the Cisco Nexus 7000 Series with Cisco DCNM Release 6.1, page 18](#)

General Limitations for Cisco DCNM Release 6.1

The license installer in Cisco DCNM Release 6.1 supports only US English. Attempting to install a license for any locale other than US English results in an error.

A Storage Management Initiative Specification (SMI-S) API is not supported in a federated Cisco DCNM configuration.

Limitations for the Cisco Nexus 7000 Series with Cisco DCNM Release 6.1

This section describes the limitations in Cisco DCNM Release 6.1(x) for the Cisco Nexus 7000 Series.

Cisco DCNM Cannot Display Multidestination Paths

Cisco DCNM cannot display all available multidestination paths in DCNM Layer 2 View Topology. If a Cisco Nexus 7000 Series switch is running Cisco NX-OS software earlier than Release 5.2(4) or Release 6.0(x), the multidestination path information is incorrect in the DCNM Layer 2 View Topology. The workaround is to upgrade the Cisco Nexus 7000 Series switch to Cisco NX-OS Release 5.2(4) or a later release, or upgrade to Cisco NX-OS Release 6.1(x). This limitation is associated with caveat CSCtw73523 and applies only to Cisco Nexus 7000 Series switches.

Caveats

This section includes the following topics:

- [Open Caveats—Cisco DCNM Release 6.1, page 18](#)
- [Open Caveats—Cisco DCNM SAN Release 6.1, page 19](#)
- [Open Caveats—Cisco DCNM-LAN, Release 6.1, page 20](#)
- [Resolved Caveats—Cisco DCNM SAN Release 6.1\(2\), page 24](#)
- [Resolved Caveats—Cisco DCNM LAN Release 6.1\(2\), page 24](#)
- [Resolved Caveats—Cisco DCNM SAN Release 6.1\(1b\), page 25](#)
- [Resolved Caveats—Cisco DCNM LAN Release 6.1\(1b\), page 26](#)
- [Resolved Caveats—Cisco DCNM SAN Release 6.1\(1b\), page 27](#)
- [Resolved Caveats—Cisco DCNM LAN Release 6.1\(1a\), page 28](#)
- [Resolved Caveats—Cisco DCNM SAN Release 6.1\(1a\), page 30](#)

Open Caveats—Cisco DCNM Release 6.1

This section lists caveats that apply to both Cisco DCNM-LAN and Cisco DCNM-SAN.

- CSCto59733
Symptom: The Cisco DCNM installer is unable to launch.

Conditions: The Cisco DCNM installer displays the following exception when you install Cisco DCNM on a Linux machine where the shared library libXtst.so got installed:

```

Launching installer...
Invocation of this Java Application has caused an InvocationTargetException. This
application will now exit. (LAX)
Stack Trace:
java.lang.UnsatisfiedLinkError:
/tmp/install.dir.13806/Linux/resource/jre/lib/i386/xawt/libmawt.so: libXtst.so.6:
cannot open shared object file: No such file or directory
    at java.lang.ClassLoader$NativeLibrary.load(Native Method)
    at java.lang.ClassLoader.loadLibrary0(Unknown Source)
    at java.lang.ClassLoader.loadLibrary(Unknown Source)

```

Workaround: This is a known issue with InstallAnywhere:

<http://community.flexerasoftware.com/showthread.php?p=461440>

The solution is available at this URL:

http://docsfree.com/uimodules/docs/docs_frame.jsp?meme_id=130971&category_id=null&topic_id=null&searchstring=null

Install the missing “xorg-x11-deprecated-libs” package by following these steps:

1. Enter the following command to confirm that libXp is missing:

```
$ rpm --query --whatprovides 'libXp.so.6'
```

2. Install the package by entering the following command:

```
# rpm -ivh xorg-x11-deprecated-libs.rpm
```

Examples of rpm packages that contain libXp.so.6 are as follows:

- xorg-x11-deprecated-libs-6.8.1-12.i386.rpm,
- xorg-x11-deprecated-libs-6.8.2-31.i386.rpm

Alternatively, you can install the package by entering the following command:

```
yum install xorg-x11-deprecated-libs
```

Open Caveats—Cisco DCNM SAN Release 6.1

- CSCud31480

Symptom: In an https federation setup, the web client Admin -> Logs menu displays an Http Request error when trying to retrieve logs from a remote server.

Conditions: This symptom occurs only with https, regardless of the browser type.

Workaround: Open another browser page that points directly to the remote server. Click Admin -> Logs to see all logs listed.

- CSCud43249

Symptom: When a server that is down comes up, the Admin/Status shows Performance Collector “Status=Running” and still collecting entries, even though the server’s managed LAN tasks were taken over by another live server through auto failover .

Conditions: The symptom might be seen in a federation setup when one of the server networks is down.

Workaround: Restart the Cisco DCNM server whose network was down earlier.

- CSCud43274

Symptom: When a server that was down comes up, the Performance Manager log shows “Exception: No Valid user found in database for this IP,” even though the server’s managed LAN tasks have been taken over by another live server through auto failover.

Conditions: The symptom might be seen in a federation setup when one of the server networks is down.

Workaround: Restart the Cisco DCNM server whose network was down earlier. The exception in the log can be ignored as there is no impact to the Performance Manager functionality.

Open Caveats—Cisco DCNM-LAN, Release 6.1

- CSCty88102

Symptom: Discovery cannot be canceled.

Conditions: This symptom might be seen immediately after triggering the discovery if you want to change the hop count.

Workaround: None. Wait until the discovery completes.

- CSCtz41585

Symptom: If any statistics are started for the FWSM platform and devices that have undergone rediscovery because of failover, those statistics are not start automatically once the rediscovery finishes.

Conditions: This symptom might be seen in the case of failover, and when the switching of the FWSM management IP address occurs.

Workaround: Navigate to the respective statistics screen and manually start the statistics. You can navigate from the statistical data collection screen. All statistics will start with the previously populated data.

- CSCua30325

Symptom: The Layer 2 view in the Cisco DCNM LAN topology does not show a link between two Firewall service Modules (FWSM).

Conditions: This symptom might occur when two firewall modules that are in routed mode are present in the same Catalyst 6500 Series chassis and failover is triggered by bringing down one of the firewall modules.

Workaround: From the **Admin --> Data source --> LAN** screen in the web client, rediscover the discovery task that contains the firewall modules.

- CSCua30596

Symptom: FWSM discovery is not triggered when a failover occurs. The LAN discovery screen shows no owner or IP addresses.

Conditions: This symptom might be seen when there are active and standby FWSMs discovered in two different tasks in the web interface.

Workaround: Delete both tasks and discover the FWSMs in a single task in the web interface.

- CSCua48938

Symptom: The Cisco DCNM topology does not show the correct connections for the two-layer vPC.

Conditions: This symptom might be seen when the port channel is flapped from the shut to no shut state.

Workaround: Rediscover the vPC peer devices. After rediscovery the connections show correctly for the two-layer vPC.

- CSCua49026

Symptom: The Cisco DCNM topology does not show the correct connections for the two-layer vPC. It shows two entries for the same two-layer vPC.

Conditions: This symptom might be seen when the discovery of a Cisco Nexus 1000V is done with hop count 1, which is not consistent.

Workaround: Rediscover the vPC peer devices. After rediscovery, the connections will show correctly for the two-layer vPC.

- CSCua52269

Symptom: The topology and vPC configuration screens show partial or incorrect information that is not consistent with the CLI for a two-layer vPC (enhanced vPC) that is configured between two Cisco Nexus 5000 Series switches and two Cisco Nexus 2000 FEXs and a host that is running a Cisco Nexus 1000v after a two-layer vPC was successfully discovered in Cisco DCNM

Conditions: This symptom might be seen when a two-layer vPC goes down under the following conditions:

- Physical interfaces that participate in the two-layer vPC go down.
- A port-channel interface between ports in the two-layer vPC goes down.

Workaround: Rediscover the discovery task that has devices (Cisco Nexus 5000 Series, Cisco Nexus 2000 Series, and Cisco Nexus 1000V) using the Admin, LAN data source in the Cisco DCNM web client.

- CSCua60206

Symptom: Automatic discovery is triggered after a device is deleted.

Conditions: This symptom might be seen when Cisco DCNM runs with more than one node.

Workaround: To work around this issue, follow these steps:

1. Trigger a discovery from the web user interface on the same IP address.
2. Navigate to Cisco DCNM Server **Administration -> Auto Synchronization with Devices**.
3. Select the device that triggered discovery.
4. Stop the poller by right clicking on the stop button from the toolbar.
5. Delete the device.

- CSCua63676

Symptom: Port channels are not listed under Cisco Nexus 7000 Series after rediscovery because a fabric extender (FEX) came online.

Conditions: This symptom might be seen when discovery completes successfully, and the newly discovered device appears on the other features screen, but it does not appear in the port-channel screen.

Workaround: Press F5 to refresh the port-channel screen. The port-channels appear under the device.

- CSCua67553

Symptom: Occasionally the menu option to resolve the vPC inconsistency on the vPC peer link does not appear in the Port Channel and vPC view of the Cisco DCNM Topology screen.

Conditions: This issue might be seen when the vPC graceful configuration is enabled on the device.

Workaround: Go to the vPC feature screen and resolve the inconsistency for the vPC and the global inconsistency.

- CSCua68164

Symptom: The FEX Power Status is not updated on the Cisco DCNM LAN client Inventory screen after a FEX power supply Online Insertion and Removal (OIR).

Conditions: This symptom might be seen when you do an OIR of the FEX power supply.

Workaround: Trigger a discovery from the web user interface on the same IP address after the FEX power supply OIR.

- CSCua69495

Symptom: FEX inventory information is not correct after the automatic discovery.

Conditions: This symptom might be seen after the FEX was enabled through Cisco DCNM.

Workaround: Rediscover the device manually.

- CSCuc31485

Symptom: A Unicast OTV overlay cloud is not removed, even if the OTV adjacency is down.

Conditions: This symptom might be seen if you configure two OTV edge devices to set up a unicast adjacency. Device A is the primary adjacency server and device B is the client. Enter the **otv use-adjacency-server 2.2.2.1 unicast-only** command on client B to bring the unicast adjacency up. When the primary adjacency server is removed from client B, the adjacency goes down. The syslog on the device is not correct, which is why the overlay OTV cloud node cannot be removed from the Cisco DCNM LAN topology.

Workaround: Rediscover the OTV edge devices.

- CSCuc37293

Symptom: An internal error might occur when launching the Topology view. Because of this error, the topology in the Cisco DCNM LAN client does not load and is in an indefinite mode.

Conditions: This symptom might be seen in the Cisco DCNM LAN client with JRE 1.6_u31. It occurs intermittently and usually during the first-time launch of the Cisco DCNM LAN client in some machines.

Workaround: Downgrade the JRE version to 1.6.u_21 or upgrade the JRE version to 1.6.u_32.

- CSCuc78211

Symptom: Following an upgrade from Cisco DCNM Release 5.2(2e) to Release 6.1(2), auto rediscovery on the Cisco Nexus 5000 Series device is not triggered in Cisco DCNM LAN. In addition, the device is shown in the unmanage state because the release running on the device is not supported in Cisco DCNM Release 5.2(2e).

Conditions: This symptom might be seen when the Cisco DCNM LAN server ignores the auto rediscovery request because the Cisco Nexus 5000 Series device is running Cisco NX-OS Release 5.2(1)N1(x) and the device was in an unmanage state in Cisco DCNM Release 5.2(2e).

Workaround: Rediscover the Cisco Nexus 5000 Series device that is running Cisco NX-OS Release 5.2(1)N1(x) after the upgrade from the web client, and the Cisco DCNM LAN cluster is stabilized.

- CSCud05054

Symptom: Following an upgrade from Cisco DCNM Release 5.2(2e) to Release 6.1(2), FEX device groups disappear.

Conditions: This symptom might be seen when the Cisco DCNM LAN server ignores the FEX device groups after an upgrade from Cisco DCNM Release 5.2(2e) to Release 6.1(2).

Workaround: Create the device groups manually from the web client and associate the FEX with the device groups.

- CSCud21648

Symptom: Following an upgrade from Cisco DCNM Release 6.1(1a) to Release 6.1(2), automatic rediscovery of a device in Cisco DCNM LAN is not triggered.

Conditions: This symptom might be seen when the Cisco DCNM LAN server ignores the rediscovery request because of the following conditions:

- The Cisco DCNM LAN cluster is stabilizing.
- The device is already managed and was in a managed state.

DCNM LAN server ignores the rediscovery request due to following cases:

Workaround: When the Cisco DCNM LAN cluster stabilizes after the upgrade, rediscover the tasks from the web client.

- CSCud41199

Symptom: The Cisco DCNM LAN client cannot connect to the Cisco DCNM server when connectivity is lost between the Cisco DCNM server and the database.

Conditions: This symptom might be seen when the Cisco DCNM server and database are on different machines and the Cisco DCNM server loses connectivity to the database. Cisco DCNM LAN stops working, but the Cisco DCNM SAN client and web client still work.

Workaround: Stop all the nodes in the Cisco DCNM LAN cluster and restart it.

Resolved Caveats—Cisco DCNM SAN Release 6.1(2)

- CSCud42820
Symptom: The fabric name information is empty in the Move Fabric popup.
Conditions: This symptom occurs only after a Move LAN Task is selected and the Move LAN Task popup appears.
Workaround: This issue is resolved.
- CSCud47550
Symptom: The global scope filter is missing from the **Config -> Archive -> Job** page. Backup job creation fails with the error message:
“Please select a single fabric or a single LAN group from the scope selector above.”
Workaround: Select the global scope filter from any other page where it is visible, such as **Dashboard -> Summary**, and then select **Config -> Archive -> Job**. The backup job will be created.
This issue is resolved.

Resolved Caveats—Cisco DCNM LAN Release 6.1(2)

- CSCua30884
Symptom: The Network Server screen in the Cisco DCNM LAN client does not show information about virtual machines that are imported from vCenter using the web client.
Conditions: This symptom might be seen after you import server information using the vCenter data source in the web client. You can see only the MAC address information, but the virtual machine name and IP address information are not shown.
Workaround: This issue is resolved.
- CSCua52396
Symptom: The Network Server screen in the Cisco DCNM LAN swing client does not display the end host that was recently reloaded.
Conditions: This symptom might be seen once Cisco DCNM discovers Cisco Nexus switches and the corresponding end host. If the end host is reloaded by the user, Cisco DCNM should remove that end host from the Network Server screen and display it again once the end host is back online, but Cisco DCNM does not remove the end host entry and it goes to a stale state.
Workaround: This issue is resolved.
- CSCua54752
Symptom: Some of the end hosts that are connected in the network are not visible in the Cisco DCNM LAN Swing Client Network Server screen.
Conditions: This symptom might be seen when Cisco DCNM discovery is complete. If you add any new end hosts to the network, those end hosts are not automatically detected by Cisco DCNM.
Workaround: This issue is resolved.

- CSCua73490
Symptom: Switch information is not displayed.
Conditions: This symptom might be seen after MAC address entries time out in the switch.
Workaround: This issue is resolved.
- CSCuc55057
Symptom: After discovery, the Cisco DCNM LAN client topology does not show the FEX device connected to Cisco Nexus devices.
Conditions: This symptom might be seen following device discovery.
Workaround: This issue is resolved.

Resolved Caveats—Cisco DCNM SAN Release 6.1(1b)

- CSCtz45718
Symptom: The status column in the inventory screen shows an incorrect status for the FWSM service card for a Catalyst 6500 Series switch.
Conditions: This symptom might occur if you enter the **hw-module module slot shutdown** command on the Catalyst 6500 Series switch after discovering it in Cisco DCNM. Because a syslog is not generated when the FWSM service card is shut down with this command, Cisco DCNM is not able to update the status.
Workaround: This issue is resolved.
- CSCua63790
Symptom: The Cisco DCNM installation fails with a “password authentication failure” error if the database password contains two \$\$ (dollar sign) characters.
Conditions: This symptom might be seen when there are two \$\$ (dollar sign) characters in the password.
Workaround: This issue is resolved.
- CSCua68765
Symptom: When a PostgreSQL installation fails, the install log folders are placed by default in the Application Data/Temp folder. Users do not have permission to open the Application Data folder.
Conditions: This symptom is seen only on Windows 2008 R2 Enterprise servers where there is no default READ permission for that folder for any users.
Workaround: This enhancement request is resolved. Right click the Application Data folder and give everyone/administrator full control.
- CSCua75480

Symptom: Discovery of Cisco Nexus 1000 from Cisco DCNM Release 6.1(1a) fails with the error message:

Unmanaged(Error when executing database query)

Workaround: This issue is resolved.

- CSCub02066

Symptom: After device discovery, the discovery status reports:

Successful:1, Failed:1 (x.x.x.x is unreachable during Topology discovery)

The x.x.x.x is an IP address that does not belong to any of the switches. It is a VMware ESX neighbor.

Conditions: This symptom might be seen in Cisco DCNM Release 5.2(2c) when devices are discovered.

Workaround: This issue is resolved.

- CSCub61898

Symptom: The Cisco DCNM Server fails to start after four minutes.

Workaround: This issue is resolved.

- CSCub85382

Symptom: Occasionally, the slot numbering shows a negative integer.

Conditions: This symptom might be seen in the Storage VDC section.

Workaround: This issue is resolved.

Resolved Caveats—Cisco DCNM LAN Release 6.1(1b)

- CSCua63613

Symptom: If you associate a routed port to a port channel of fex-fabric mode with the force option, and you attempt to administratively bring the port up and down, the following error message appears: “port already in a port-channel, config not allowed.”

Conditions: This symptom might be seen with ports that are capable of rate mode dedicated. It is not seen with ports that are capable of rate mode shared.

Workaround: This issue is resolved.

- CSCua70875

Symptom: The Cisco DCNM server displays an error when you delete a non-default VDC from Cisco DCNM user interface.

Conditions: The conditions when this symptom is seen are inconsistent.

Workaround: This issue is resolved.

Resolved Caveats—Cisco DCNM SAN Release 6.1(1b)

- CSCua91667

Symptom: Cisco DCNM failed to discover Cisco IT VCenter.

The fmserver.log has the following errors:

```
Got database constraint error when persisting datastore. The discovery is aborted.
java.sql.BatchUpdateException: ORA-00001: unique constraint
(DON.SYS_PK_VM_DATASTORE_INFO) violated
at
oracle.jdbc.driver.DatabaseError.throwBatchUpdateException(DatabaseError.java:343)
at
oracle.jdbc.driver.OraclePreparedStatement.executeBatch(OraclePreparedStatement.java:1
0657)
at
org.apache.commons.dbcp.DelegatingStatement.executeBatch(DelegatingStatement.java:294)
at
com.cisco.dcbu.sm.server.db.InventoryPersistentManager.persistVmDataStores(InventoryPe
rsistentManager.java:944)
at
com.cisco.dcbu.sm.server.db.InventoryPersistentManager.persistVIDataStores(InventoryPe
rsistentManager.java:2515)
at
com.cisco.dcbu.sm.server.db.InventoryPersistentManager.persistVmWare(InventoryPersiste
ntManager.java:2861)
at com.cisco.dcbu.vi.discover.VCenterWorker.discover(VCenterWorker.java:381)
at com.cisco.dcbu.vi.discover.VCenterWorker.run(VCenterWorker.java:140)
at
com.cisco.dcbu.lib.concurrent.PooledThreadExecutor$ThreadPoolWorker.run(PooledThreadEx
ecutor.java:259)
```

Workaround: This issue is resolved.

- CSCub00060

Symptom: The Cisco DCNM Release 6.1 web client does not display any information if the customer uses more than 256 VLANs.

Workaround: This issue is resolved.

- CSCub00415

Symptom: There is a locking issue in persistent code where the fabric is not flushed correctly into the database.

Workaround: This issue is resolved.

- CSCub11737

Symptom: A period character (.) within a username causes an empty report when you try to generate a report.

Conditions: This symptom might be seen when you try to generate a report and a period character (.) is in the username. The following message displays in fm_web:

```
2012.07.18 16:33:55 ERROR FM.web com.cisco.dcbu.web.client.aggr.CustomReportAction
perform() String index out of range: -1
```

Workaround: This issue is resolved.

- CSCub21607
Symptom: Health Events in the Cisco DCNM web client report VSAN unreachable and Fibre Channel port down events.
Conditions: This symptom might be seen when the management port on a Cisco MDS 9000 switch goes down and the switch becomes unreachable through an SNMP timeout event. The VSAN does not actually go down on the Cisco MDS 9000 switch.
Workaround: This issue is resolved.

- CSCub24948
Symptom: When the Performance Manager polling interval is set to 30 seconds through the PM->ISLs table, data displays for Rx or Tx traffic, but clicking the chart does not display any graphs.
Conditions: This symptom might be seen in Cisco DCNM Release 5.2(2).
Workaround: This issue is resolved.

- CSCub24979
Symptom: The server.properties file shows a duplicate client.maxAuthenticationPoolSize attribute.
Workaround: This issue is resolved.

- CSCub25195
Symptom: The Admin->PM->DB ISL 30-second polling interval reverts to 5 minutes after you log in again.
Conditions: This symptom might be seen in the Cisco DCNM Web client.
Workaround: This issue is resolved.

- CSCub71480
Symptom: Occasionally, the status column shows Error:Null.
Conditions: The symptom seems to occur for some CLI commands that take a long time to execute and when the TCP timeout value is small.
Workaround: This issue is resolved.

Resolved Caveats—Cisco DCNM LAN Release 6.1(1a)

- CSCtr35544
Symptom: Cisco DCNM-LAN shows an unexpected difference when you compare a checkpoint archived version with the startup configuration in the version browser screen.
 In addition, there are unexpected differences when you compare the Cisco DCNM Release 4.2(1) checkpoint archived version with the Cisco DCNM Release 5.2(x) checkpoint version.
Conditions: This symptom might be seen if the Cisco Nexus device has an image version greater than Release 4.2(1).

Workaround: This issue is resolved.

- CSCtx16177

Symptom: The install.conf file was not found during an upgrade of Cisco DCNM-SAN.

Conditions: This symptom might be seen if a different administrator attempts to perform the upgrade.

Workaround: This issue is resolved.

- CSCtx39981

Symptom: Cisco DCNM-LAN is unable to discover Cisco Nexus 5000 Series or Cisco Nexus 7000 Series devices. The following error message appears in the debug or trace mode related to the SSH protocol being unavailable: “device didn't allow new connection because of either exceeded connection limit or transport protocol is down.” The devices status is “Unmanaged” in the topology pane.

Conditions: This symptom might be seen if Cisco DCNM-LAN hangs SSH communication when the Cisco NX-OS software on a Cisco Nexus 5000 Series or Cisco Nexus 7000 device takes more than eight seconds to answer with the sshd version when running the following test:

```
C:\>plink -v user@a.b.c.d
...
Server version: SSH-2.0-OpenSSH_5.5 FIPS
....
Using SSH protocol version 2
....
```

If sshd is the first process with the highest usage, high CPU occurs in the Cisco Nexus switch.

Workaround: This issue is resolved.

- CSCtx75958

Symptom: Interfaces that are present in the device (VDC) are not synchronized with DCNM-LAN.

Conditions: This symptom might be seen when you attempt to allocate an interface in the unallocated pool from the interfaces association panel. Only some of the interfaces are added to the VDC, but all the interfaces that belong to the port group are added to the device.

Workaround: This issue is resolved.

- CSCtx79298

Symptom: A VDC link is missing in the Topology screen.

Conditions: The **show hostname** command displays the fully qualified domain name such as myhost-VDC.dc.example.gov.au. Cisco DCNM-LAN expects to see myhost-VDC.

Workaround: This issue is resolved.

- CSCtz40661

Symptom: Discovery fails due to an error when saving data to the database during discovery.

Conditions: This symptom might be seen if discovery runs concurrently on two switches that are connected to the same FEX.

Workaround: This issue is resolved.

- CSCua52343

Symptom: The LLDP transmit and receive details are not correct in port details in the Ethernet screen.

Conditions: This symptom might be seen after discovery or CLI changes on a device with an LLDP transmit or receive command.

Workaround: None.

Resolved Caveats—Cisco DCNM SAN Release 6.1(1a)

- CSCth49735

Symptom: The version of PostgreSQL in Cisco Fabric Manager is 8.2.3.

Conditions: This caveat addresses the need to upgrade the version of PostgreSQL that is bundled with Cisco Fabric Manager.

Workaround: This issue is resolved.

- CSCua70866

Symptom: If you upgrade Cisco DCNM Release 5.2x to Release 6.1(1a), the older backup jobs might not run because the Release 6.1(1a) backup uses Fabric DBID instead of Fabric ID to accommodate the group concept.

Conditions: This symptom might be seen when you upgrade from Cisco DCNM Release 5.2(x) to Release 6.1(1a).

Workaround: This issue is resolved.

Related Documentation

This section contains information about the documentation available for Cisco DCNM and for the platforms that Cisco DCNM manages.

This section includes the following topics:

- [Cisco DCNM Documentation](#)
- [Cisco Nexus 1000V Series Switch Documentation](#)
- [Cisco Nexus 2000 Series Fabric Extender Documentation](#)
- [Cisco Nexus 3000 Series Switch Documentation](#)
- [Cisco Nexus 4000 Series Switch Documentation](#)
- [Cisco Nexus 5000 Series Switch Documentation](#)
- [Cisco Nexus 7000 Series Switch Documentation](#)
- [Catalyst 6500 Series Switch Documentation](#)

Cisco DCNM Documentation

The Cisco DCNM documentation is available at the following URL:

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

The documentation set for Cisco DCNM includes the following documents:

Release Notes

Cisco DCNM Release Notes, Release 6.x

Installation and Licensing

Cisco DCNM Installation and Licensing Guide, Release 6.x

Cisco DCNM Fundamentals Guide

Cisco DCNM Fundamentals Guide, Release 6.x

Cisco DCNM Troubleshooting Guide

Cisco DCNM Troubleshooting Guide

Cisco DCNM for LAN Configuration Guides

FabricPath Configuration Guide, Cisco DCNM for LAN, Release 6.x

Cisco DCNM Interfaces Configuration Guide, Release 6.x

Cisco DCNM Layer 2 Switching Configuration Guide, Release 6.x

Cisco DCNM Security Configuration Guide, Release 6.x

Cisco DCNM System Management Configuration Guide, Release 6.x

Cisco DCNM Unicast Routing Configuration Guide, Release 6.x

Cisco DCNM Virtual Device Context Configuration Guide, Release 6.x

Cisco DCNM Getting Started with Virtual Device Contexts, Release 6.x

Cisco DCNM Web Services API Guide, Release 6.x

Cisco DCNM for SAN Configuration Guides

System Management Configuration Guide, Cisco DCNM for SAN, Release 6.x

Interfaces Configuration Guide, Cisco DCNM for SAN, Release 6.x

Fabric Configuration Guide, Cisco DCNM for SAN, Release 6.x

Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 6.x

Security Configuration Guide, Cisco DCNM for SAN, Release 6.x

IP Services Configuration Guide, Cisco DCNM for SAN, Release 6.x

Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 6.x

High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 6.x

Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 6.x

SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 6.x

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available at the following URL:

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

Cisco Nexus 2000 Series Fabric Extender Documentation

The Cisco Nexus 2000 Series Fabric Extender documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 3000 Series Switch Documentation

The Cisco Nexus 3000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Cisco Nexus 4000 Series Switch Documentation

The Cisco Nexus 4000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 5000 Series Switch Documentation

The Cisco Nexus 5000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 7000 Series Switch Documentation

The Cisco Nexus 7000 Series switch documentation is available at the following URL:

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

Catalyst 6500 Series Switch Documentation

The Catalyst 6500 Series documentation is available at the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/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 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 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)

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.

© 2008-2012 Cisco Systems, Inc. All rights reserved.

