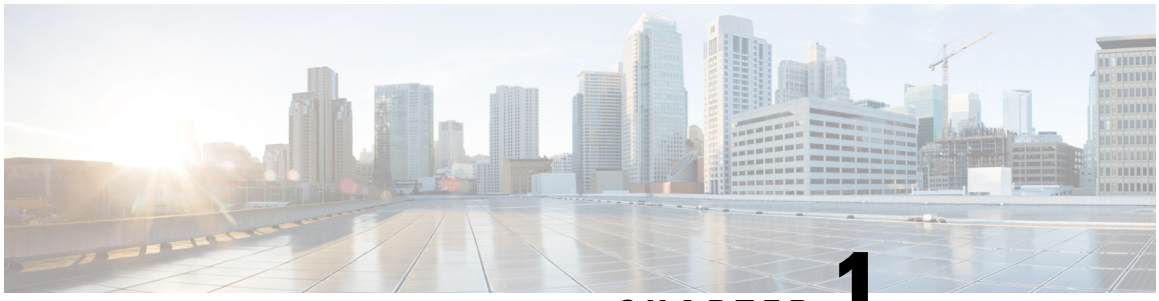
Cisco DCNM Installation and Upgrade Guide for SAN Deployment, Release 11.1(1)

First Published: 2018-12-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview

Cisco Data Center Network Manager (DCNM) is a management system for Cisco NXOS-based Storage Fabrics. In addition to provisioning, monitoring, and troubleshooting the datacenter network infrastructure, the Cisco DCNM provides a comprehensive feature-set that meets the routing, switching, and storage administration needs of datacenters. It streamlines the provisioning for the Programmable Fabric and monitors the SAN components.

Cisco DCNM provides a high level of visibility and control through a single web-based management console for Cisco Nexus Series Switches, Cisco MDS, and Cisco Unified Computing System (UCS) products. Cisco DCNM also includes Cisco DCNM-SAN client and Device Manager functionality.

This section contains the following sections:

Introduction

Cisco DCNM provides an alternative to the command-line interface (CLI) for switch configuration commands.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, Cisco DCNM-SAN provides powerful Fiber Channel troubleshooting tools. The in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fiber Channel Ping and Traceroute.

Beginning with Release 11.1(1), Cisco DCNM allows you to monitor Cisco UCS Blade servers also.

Cisco DCNM includes these management applications:

Cisco DCNM Server

The Cisco DCNM-SAN Server component must be started before running Cisco DCNM-SAN. Cisco DCNM-SAN Server is installed as a service. This service can then be administered using the Windows Services in the control panel. Cisco DCNM-SAN Server is responsible for discovery of the physical and logical fabric and for listening for SNMP traps, syslog messages, and Performance Manager threshold events.

Cisco DCNM Web UI

Cisco DCNM Web UI allows operators to monitor and obtain reports for Cisco MDS and Nexus events, performance, and inventory from a remote location using a web browser. Licensing and discovery are part of the Cisco DCNM Web UI. You can configure the MDS9000 Fabric, also.

Cisco DCNM-SAN Client

The Cisco DCNM-SAN Client displays a map of your network fabrics, including Cisco MDS 9000 Family switches, third-party switches, hosts, and storage devices. The Cisco DCNM-SAN Client provides multiple menus for accessing the features of the Cisco DCNM SAN functionality.

Device Manager

The Device Manager is embedded with the Cisco DCNM Web UI. After the switches are discovered, navigate to **Inventory > Switches > Device Manager** to launch the Device Manager.

Cisco DCNM-SAN automatically installs the Device Manager. Device Manager provides two views of a single switch:

- **Device View**—displays a graphic representation of the switch configuration and provides access to statistics and configuration information.
- **Summary View**—displays a summary of xE ports (Inter-Switch Links), Fx ports (fabric ports), and Nx ports (attached hosts and storage) on the switch, as well as Fibre Channel and IP neighbor devices. Summary or real-time statistics can be charted, printed, or saved to a file in tab-delimited format.

Performance Manager

Performance Manager presents detailed traffic analysis by capturing data with SNMP. This data is compiled into various graphs and charts that can be viewed on the Cisco DCNM Web UI. Performance Manager stores data into Elastic search time series database. API access to Elastic search is not supported.

Installation Options

Cisco DCNM Software images are packaged with the Cisco DCNM installer, signature certificate, and signature verification script. Unzip the desired Cisco DCNM Installer image zip file to a directory. Image signature can be verified by following the steps in README file. The installer from this package installs the Cisco DCNM software.

DCNM Windows Installer

This installer is available as a executable (.exe) file.

DCNM Linux Installer

This installer is available as a binary (.bin) file.

Deployment Options

The installer available for Cisco DCNM can be deployed in one of the below modes.

Standalone Server

All types of installers are packaged along with PostgreSQL database. The default installation steps for the respective installers result in this mode of deployment.

Standalone with external Oracle

If you have more switches in your setup or if you expect your setup to grow over time, an external Oracle server is recommended. This mode of deployment requires the default installation setup, followed by steps to configure DCNM to use the external Oracle. For more information about Scalability, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_0_1/scalability_guide/b_scale_guide_dcnm_11.html.

DCNM Federation

Cisco DCNM federation is the HA mechanism for SAN devices. Groups of SAN devices can be managed by each node in the DCNM federated setup. All the devices can be managed using a single client interface. Federation mode is used for resilience and scalability. It allows you to monitor 20,000 FC ports. DCNM Windows and Linux Installers can be deployed in Federation mode to have resilience in case of application or OS failures. For Cisco DCNM-SAN federation, the database URL (properties) must remain the same for all Cisco DCNM-SAN nodes in the federation.

System Requirements for Cisco DCNM, Release

Java Requirements

The Cisco DCNM Server is distributed with JRE 1.8.0_152 into the following directory:

```
DCNM_root_directory/java/jre1.8
```

Server Requirements

Cisco DCNM, Release , supports the Cisco DCNM Server on these 64-bit operating systems:

- **SAN Deployments:**
  - Microsoft Windows 2016
  - Microsoft Windows 2012 R2
  - Red Hat Enterprise Linux Release 7.3 and 7.4

Cisco DCNM Release supports the following databases:

- Oracle11g Express (XE), Standard, and Enterprise Editions, and Oracle 11g Real Application Clusters (RAC)
- Oracle 12c Enterprise Edition (Conventional)—(Nonpluggable installation)

Note Cisco DCNM Release does not support the Oracle 12c pluggable database version installation.

- Oracle 12c RAC (nonpluggable installation)

Note The Cisco DCNM database size is not limited, and increases according to the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. If you choose Oracle database, we recommend that you use Oracle SE or Enterprise edition, instead of Oracle XE due to table space limitations.

Note You are responsible for all the support that is associated with the Oracle databases, including maintenance, troubleshooting, and recovery. We recommend that you take regular database backups, either daily or weekly, to ensure that all the data is preserved.

Note Cisco DCNM can work on an alternative computing hardware as well, despite Cisco is only testing on Cisco UCS.

Server Resource Requirements

Table 1: Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Compute
SAN	Windows, Linux (standalone or VM)	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs **Note** Standalone functioning of SAN Insights require 28 vCPUs. RAM: 128 GB RAM(with SAN Insights) or 32 GB (without SAN Insights) DISK: 10 TB Disk (with SAN Insights) or 500 GB (without SAN Insights)	Not Applicable

Note

- The SAN Insights feature is not supported on small deployment.
- You can use the SAN Insights feature on a medium-sized deployment with 2 TB disk space as well.
- Every Federation node must consists of 3 Large configuration nodes.

Client Requirements

Cisco DCNM SAN desktop client and Cisco Device Manager support Microsoft Windows 10, Microsoft Windows 2012, and Red Hat Linux. The following table lists the minimum hardware requirements for these client systems.

Table 2: Client Hardware Requirements

Hardware	Minimum Requirements
RAM (free)	6 GB or more
CPU speed	3 GHz or faster
Disk space (free)	20 GB

If you install Cisco DCNM on a virtual machine, you must reserve resources equal to the server resource requirements to ensure a baseline with the physical machines.

Some Cisco DCNM features require a license. Before using the licensed features, you must install a Cisco DCNM license for each Nexus-managed or MDS-managed platform. For information about Licensing in DCNM, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_x/licensing/cisco_dcnm_licensing_guide_11_x.html.

Supported Web Browsers

Cisco DCNM supports the following web browsers:

-
-
-

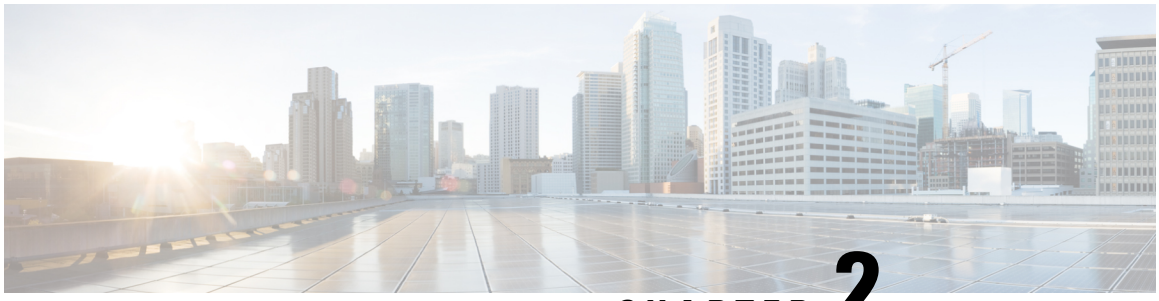
Other Supported Software

The following table lists the other software that is supported by Cisco DCNM, Release .

Table 3: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, and 5.5 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client and Cisco DCNM-SAN Server Encryption: HTTPS with TLS 1, 1.1 and 1.2

Also, Cisco DCNM supports call-home events, fabric change events, and events that are forwarded by traps and email.



CHAPTER 2

Guidelines and Limitations

Guidelines and Limitations

The guidelines and limitations for installing and upgrading Cisco DCNM are as follows:

General Guidelines and Limitations

- Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:
  - It must be at least 8 characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password: <SPACE> & $ % ‘ “ ^ = < > ; :
  - From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 11.0(1) is not valid. However, different passwords are allowed during Upgrade.

    The new Administrative password that is entered is used in the following scenarios.

    —accessing the DCNM appliance via its console.

    —accessing the appliance via SSH

    —for applications running on the appliance, e.g. Postgres DBMS

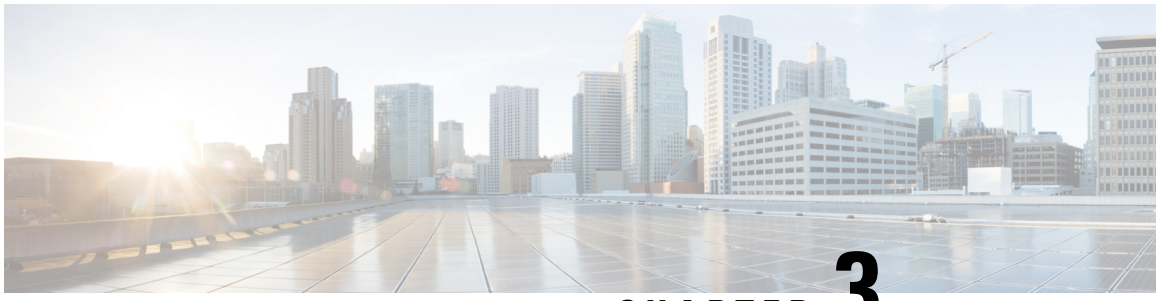
    However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.
- Do not interrupt the boot process (such as pressing the Ctrl+ALT + DELETE keys) when installing DCNM. If you interrupt, you must restart the installation process.
- Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. Use the NTP server for configuring timezones.

Fresh Installation

- For Windows and Linux installers, the installer installs Cisco DCNM-SAN and Cisco SMI-S agent on your system.

Upgrade

- For Windows and Linux installers, the default is to upgrade to the latest version of Cisco DCNM.



CHAPTER 3

Prerequisites

This chapter provides release-specific prerequisites information for your deployment of *Cisco Data Center Network Manager*.

General Prerequisites

This section includes the following topics:

Before you begin

Before you can install Cisco DCNM, ensure that the Cisco DCNM system meets the following prerequisites:

- Before installing Cisco DCNM, ensure that the host name is mapped with the IP address in the hosts file under the following location:
  - Microsoft Windows–`C:\WINDOWS\system32\drivers\etc\hosts`
  - Linux–`/etc/hosts`

  Note If Oracle RAC is chosen as the database for Cisco DCNM, ensure that the database host IP addresses and virtual IP addresses are added to the hosts file with their host-names.

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command:

  sysctl -w kernel.shmmax=268435456

This setting, kernel.shmmax=268435456, should be saved in the `/etc/sysctl.conf` file. If this setting is not present or if it is less than 268435456, the Cisco DCNM server will fail after the server system is rebooted. For more information, visit the following URL:

http://www.postgresql.org/docs/8.3/interactive/kernel-resources.html

The server system must be registered with the DNS servers. The server hosting DCNM application must be dedicated to run DCNM alone and must not be shared with any other applications which utilizes memory and system resources.

- While using Remote PostgreSQL Database server, ensure that the Cisco DCNM Host IP addresses are added to the `pg_hba.conf` file present in the PostgreSQL installation directory. After the entries are added, restart the database.
- Users installing Cisco DCNM must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. For more information, see Running Cisco DCNM Behind a Firewall, on page 53.
- When you connect to the server for the first time, Cisco DCNM checks to see if you have the correct Sun Java Virtual Machine version installed on your local workstation. Cisco DCNM desktop clients look for version 1.8(x) during installation. If required, install the Sun Java Virtual Machine software.

Note When launching the Cisco DCNM installer, the *console* command option is not supported.

Note Using the Cisco DCNM installer in GUI mode requires that you must log in to the remote server using VNC or XWindows. Using Telnet or SSH to install Cisco DCNM in GUI mode is not possible.

Before you can use Cisco DCNM to manage network switches, you must complete the following tasks:

- Install a supervisor module on each switch that you want to manage.
- Configure the supervisor module with the following values using the setup routine or the CLI:
  - IP address assigned to the mgmt0 interface
  - SNMP credentials (v3 user name and password or v1/v2 communities), maintaining the same user name and password for all the switches in the fabric.

Initial Setup Routine

The first time that you access a Cisco NXOS-based switch for MDS or Nexus, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch. All Cisco Nexus or Cisco MDS switches have the network administrator as a default user (Admin). You cannot change the default user at any time. You must explicitly configure a strong password for any switch in the Cisco Nexus or Cisco MDS. The setup scenario differs based on the subnet to which you are adding the new switch:

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port.
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS).

Note IP address for a Cisco Nexus switch or a Cisco MDS switch can be set via CLI or USB key or POAP.

Preparing to Configure the Switch

Before you configure a switch in the Cisco Nexus or Cisco MDS 9000 Family for the first time, you need the following information:

- Administrator password, including:
  - Creating a password for the administrator (required).
  - Creating an additional login account and password (optional).
- IP address for the switch management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface (recommended).
- Subnet mask for the switch's management interface (optional).
- IP addresses, including:
  - Destination prefix, destination prefix subnet mask, and next-hop IP address if you want to enable IP routing. Also, provide the IP address of the default network (optional).
  - Otherwise, provide an IP address of the default gateway (optional).
- SSH service on the switch—To enable this optional service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- DNS IP address (optional).
- Default domain name (optional).
- NTP server IP address (optional).
- SNMP community string (optional).
- Switch name—This is your switch prompt (optional).

Note Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

Note You should verify that the Cisco DCNM-SAN Server host name entry exists on the DNS server, unless the Cisco DCNM-SAN Server is configured to bind to a specific interface during installation.

Default Login

All Cisco Nexus and Cisco MDS 9000 Family switches have the network administrator as a default user (Admin). You cannot change the default user at any time (see the Security Configuration Guide, Cisco DCNM for SAN).

You have an option to enforce a secure password for any switch in the Cisco MDS 9000 Family. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a secure password (see the Security Configuration Guide, Cisco DCNM for SAN). If you configure and subsequently forget this new password, you have the option to recover this password (see the Security Configuration Guide, Cisco DCNM for SAN).

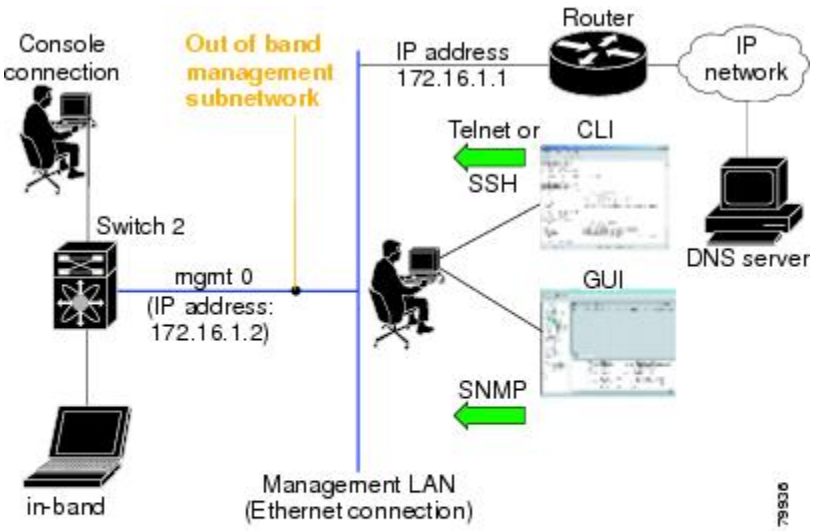
Note Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a Cisco MDS 9000 Family switch or a Cisco Nexus switch with an IP address to enable management connections from outside of the switch (see Figure 1: Management Access to Switches, on page 13).

Figure 1: Management Access to Switches



Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.

Note Press **Ctrl + C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point. Entering a new password for the administrator is a requirement and cannot be skipped.

Tip If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

Configuring Out-of-Band Management

You can configure both in-band and out-of-band configuration together by entering **Yes** in both in the following procedure.

Procedure

Step 1 Power on the switch. Switches in the Cisco Nexus and Cisco MDS 9000 Family boot automatically.

```
Do you want to enforce secure password standard (Yes/No)?
```

Step 2 Enter Yes to enforce a secure password.

a) Enter the administrator password.

```
Enter the password for admin: 2008asdf*lkjh17
```

Note The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

b) Confirm the administrator password.

```
Confirm the password for admin: 2008asdf*lkjh17
```

Tip If a password is trivial (short, easy to decipher), your password configuration is rejected. Be sure to configure a secure password as shown in the sample configuration. Passwords are case sensitive.

Step 3 Enter **yes** to enter the setup mode.

Note This setup utility guides you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

```
Please register Cisco MDS 9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. MDS devices must
be registered to receive entitled support services.
Press Enter anytime you want to skip any dialog. Use ctrl-c at anytime to skip away remaining
 dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process. Press **Ctrl + C** at any prompt to end the configuration process.

Step 4 Enter the new password for the administrator (Admin is the default).

```
Enter the password for admin: admin
```

Step 5 Enter **yes** (no is the default) to create additional accounts.

```
Create another login account (yes/no) [n]: yes
```

While configuring your initial setup, you can create an additional user account (in the network administrator role) in addition to the administrator’s account. See the Security Configuration Guide, Cisco DCNM for SAN for information on default roles and permissions.

Note User login IDs must contain non-numeric characters.

a) Enter the user login ID [administrator].

```
Enter the user login ID: user_name
```

b) Enter the user password.

```
Enter the password for user_name: user-password
```

The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

c) Confirm the user password.

```
Confirm the password for user_name: user-password
```

Step 6 Enter yes (no is the default) to create an SNMPv3 account.

```
Configure read-only SNMP community string (yes/no) [n]: yes
```

a) Enter the username (Admin is the default).

```
SNMPv3 user name [admin]: admin
```

b) Enter the SNMPv3 password (minimum of eight characters). The default is admin123.

```
SNMPv3 user authentication password: admin_pass
```

Step 7 Enter **yes** (no is the default) to configure the read-only or read-write SNMP community string.

```
Configure read-write SNMP community string (yes/no) [n]: yes
```

a) Enter the SNMP community string.

```
SNMP community string: snmp_community
```

Step 8 Enter a name for the switch.

```
Enter the switch name: switch_name
```

Step 9 Enter **yes** (yes is the default) to configure out-of-band management.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
```

a) Enter the mgmt0 IP address.

```
Mgmt0 IPv4 address: ip_address
```

b) Enter the mgmt0 subnet mask.

```
Mgmt0 IPv4 netmask: subnet_mask
```

Step 10 Enter **yes** (yes is the default) to configure the default gateway (recommended).

```
Configure the default-gateway: (yes/no) [y]: yes
```

a) Enter the default gateway IP address.

```
IPv4 address of the default gateway: default_gateway
```

Step 11 Enter **yes** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a) Enter **no** (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: no
```

b) Enter **yes** (no is the default) to enable IP routing capabilities.

```
Enable the ip routing? (yes/no) [n]: yes
```

c) Enter **yes** (no is the default) to configure a static route (recommended).

```
Configure static route: (yes/no) [n]: yes
```

Enter the destination prefix.

```
Destination prefix: dest_prefix
```

Enter the destination prefix mask.

```
Destination prefix mask: dest_mask
```

Enter the next-hop IP address.

```
Next hop ip address: next_hop_address
```

Note Be sure to configure the IP route, the default network IP address, and the default gateway IP address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

d) Enter **yes** (no is the default) to configure the default network (recommended).

```
Configure the default network: (yes/no) [n]: yes
```

Enter the default network IP address.

Note The default network IP address is the destination prefix provided in .

```
Default network IP address [dest_prefix]: dest_prefix
```

e) Enter **yes** (no is the default) to configure the DNS IP address.

```
Configure the DNS IPv4 address? (yes/no) [n]: yes
```

Enter the DNS IP address.

```
DNS IPv4 address: name_server
```

f) Enter **yes** (default is no) to configure the default domain name.

```
Configure the default domain name? (yes/no) [n]: yes
```

Enter the default domain name.

```
Default domain name: domain_name
```

Step 12 Enter yes (no is the default) to enable Telnet service.

```
Enable the telnet server? (yes/no) [n]: yes
```

Step 13 Enter **yes** (no is the default) to enable the SSH service.

```
Enabled SSH server? (yes/no) [n]: yes
```

Step 14 Enter the SSH key type.

```
Type the SSH key you would like to generate (dsa/rsa)? dsa
```

Step 15 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768 to 2048): 768
```

Step 16 Enter **yes** (no is the default) to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: yes
Configure clock? (yes/no) [n] :yes
Configure clock? (yes/no) [n] :yes
Configure timezone? (yes/no) [n] :yes
Configure summertime? (yes/no) [n] :yes
Configure the ntp server?  (yes/no) [n] : yes
```

a) Enter the NTP server IP address.

```
NTP server IP address: ntp_server_IP_address
```

Step 17 Enter **noshut** (shut is the default) to configure the default switch port interface to the shut state.

```
Configure default switchport interface state (shut/noshut) [shut]: noshut
```

Step 18 Enter **on** (on is the default) to configure the switch port trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [on]: on
```

Step 19 Enter no (no is the default) to configure switchport port mode F.

```
Configure default switchport port mode F (yes/no) [n] : no
```

Step 20 Enter **permit** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: permit
```

This step permits traffic flow to all members of the default zone.

Step 21 Enter **yes** (no is the default) to disable a full zone set distribution (see the Fabric Configuration Guide, Cisco DCNM for SAN). Disables the switch-wide default for the full zone set distribution feature.

```
Enable full zoneset distribution (yes/no) [n]: yes
```

You see the new configuration. Review and edit the configuration that you have just entered.

Step 22 Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
  username admin password admin_pass role network-admin
  username user_name password user_pass role network-admin
  snmp-server community snmp_community ro
  switchname switch
  interface mgmt0
    ip address ip_address subnet_mask
    no shutdown
  ip routing
  ip route dest_prefix dest_mask dest_address
  ip default-network dest_prefix
  ip default-gateway default_gateway
  ip name-server name_server
  ip domain-name domain_name
  telnet server enable
ssh key dsa 768 force
  ssh server enable
  ntp server ipaddr ntp_server
  system default switchport shutdown
  system default switchport trunk mode on
  system default port-channel auto-create
  zone default-zone permit vsan 1-4093
  zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 23 Enter yes (yes is default) to use and save this configuration:

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Enter **yes** to save the new configuration to ensure that the kickstart and system images are also automatically configured.

Configuring In-Band Management

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each

switch should have its VSAN 1 interface that is configured with an IP address in the same subnetwork. A default route that points to the switch that provides access to the IP network should be configured on every switch in the Fibre Channel fabric (see Fabric Configuration Guide, Cisco DCNM for SAN).

Note You can configure both in-band and out-of-band configuration together by entering in the following procedure.

Procedure

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

```
Enter the password for admin: 2004asdf*lkjh18
```

The password can contain a combination of alphabets, numeric, and special characters. The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Step 3 Enter **yes** to enter the setup mode.

```
This setup utility will guide you through the basic configuration of the system. Setup
configures only enough connectivity for management of the system.
Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to
register may affect response times for initial service calls.
MDS devices must be registered to receive entitled support services.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away remaining
 dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter **no** (no is the default) if you do not wish to create more accounts.

```
Create another login account (yes/no) [no]: no
```

Step 5 Configure the read-only or read-write SNMP community string.

a) Enter **no** (no is the default) to avoid configuring the read-only SNMP community string.

```
Configure read-only SNMP community string (yes/no) [n]: no
```

Step 6 Enter a name for the switch.

Note The switch name is limited to 32 alphanumeric characters. The default is switch.

```
Enter the switch name: switch_name
```

Step 7 Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: no
```

Step 8 Enter **yes** (yes is the default) to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes
```

a) Enter the default gateway IP address.

```
IP address of the default gateway: default_gateway
```

Step 9 Enter **yes** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a) Enter **yes** (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: yes
```

Enter the VSAN 1 IP address.

```
VSAN1 IP address: ip_address
```

Enter the subnet mask.

```
VSAN1 IP net mask: subnet_mask
```

b) Enter **no** (yes is the default) to enable IP routing capabilities.

```
Enable ip routing capabilities? (yes/no) [y]: no
```

c) Enter **no** (yes is the default) to configure a static route.

```
Configure static route: (yes/no) [y]: no
```

d) Enter **no** (yes is the default) to configure the default network.

```
Configure the default-network: (yes/no) [y]: no
```

e) Enter **no** (yes is the default) to configure the DNS IP address.

```
Configure the DNS IP address? (yes/no) [y]: no
```

f) Enter **no** (no is the default) to skip the default domain name configuration.

```
Configure the default domain name? (yes/no) [n]: no
```

Step 10 Enter **no** (yes is the default) to disable Telnet service.

```
Enable the telnet service? (yes/no) [y]: no
```

Step 11 Enter **yes** (no is the default) to enable the SSH service.

```
Enabled SSH service? (yes/no) [n]: yes
```

Step 12 Enter the SSH key type (see the Security Configuration Guide, Cisco DCNM for SAN) that you want to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? rsa
```

Step 13 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768 to 1024): 1024
```

Step 14 Enter **no** (no is the default) to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: no
```

Step 15 Enter **shut** (shut is the default) to configure the default switch port interface to the shut state.

```
Configure default switchport interface state (shut/noshut) [shut]: shut
```

Note The management Ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

Step 16 Enter **auto** (off is the default) to configure the switch port trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [off]: auto
```

Step 17 Enter **deny** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: deny
```

This step denies traffic flow to all members of the default zone.

Step 18 Enter **no** (no is the default) to disable a full zone set distribution.

```
Enable full zoneset distribution (yes/no) [n]: no
```

This step disables the switch-wide default for the full zone set distribution feature.

You see the new configuration. Review and edit the configuration that you have entered.

Step 19 Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
  username admin password admin_pass role network-admin
  snmp-server community snmp_community rw
  switchname switch
  interface vsan1
    ip address ip_address subnet_mask
    no shutdown
  ip default-gateway default_gateway
  no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  no system default switchport shutdown
  system default switchport trunk mode auto
  no zone default-zone permit vsan 1-4093
  no zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 20 Enter yes (yes is default) to use and save this configuration.

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Enter **yes** to save the new configuration. To ensure that the kickstart and system images are also automatically configured.

Using the setup Command

To make changes to the initial configuration at a later time, you can enter the **setup** command in EXEC mode.

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process.

Starting a Switch in the Cisco MDS 9000 Family

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.

Note You must use the CLI for initial switch start up.

Procedure

Step 1 Verify the following physical connections for the new Cisco MDS 9000 Family switch:

- The console port is physically connected to a computer terminal (or terminal server).
- The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.

Tip Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.

Step 2 Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

Step 3 Power on the switch.

The switch boots automatically and the switch# prompt appears in your terminal window.

Accessing the Switch

After initial configuration, you can access the switch in one of the three ways:

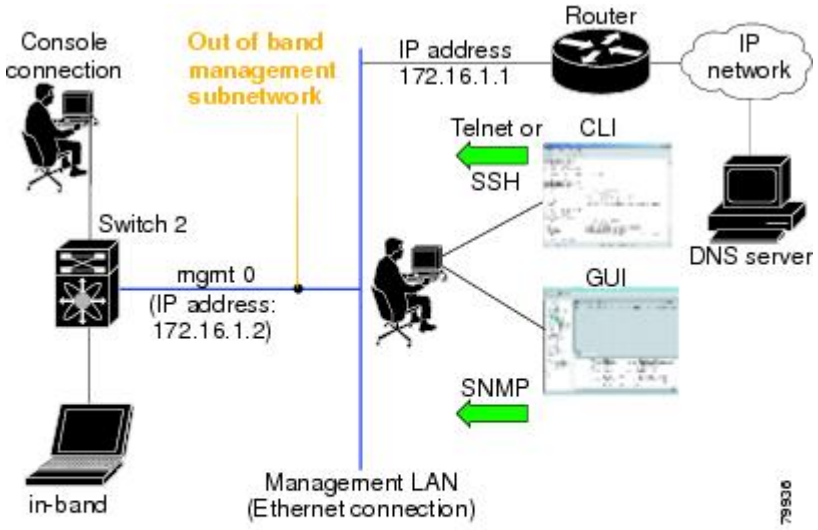
- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.

After initial configuration, you can access the switch in one of three ways (see Figure 2: Switch Access Options, on page 22):

- Serial console access—You can use a serial port connection to access the CLI.

- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco DCNM-SAN to access the switch.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco DCNM-SAN to access the switch.

Figure 2: Switch Access Options



Prerequisites for Installing DCNM on Windows

- During the initial installation, disable all security and antivirus tools that are running on your Windows server.
- Do not run any other management applications on the Cisco DCNM server or the Cisco DCNM database server.
- Before installing Cisco DCNM, ensure that the hostname is mapped with the IP address in the hosts file under the location **C:\WINDOWS\system32\drivers\etc\hosts**.
- On Windows, remote Cisco DCNM installations or upgrades must be done through the console using VNC or through the Remote Desktop Client (RDC) in console mode (ensuring RDC is used with the **/Console** option). This process is important if the default PostgreSQL database is used with Cisco DCNM, because this database requires the local console for all installations and upgrades.
- Telnet Client application is not installed by default on Microsoft Windows Vista. To install Telnet Client, choose **Start > Programs > Control Panel > Click Turn Windows features on or off** (if you have UAC turned on, provide permissions to continue). Check **Telnet Client** check box and click **Ok**.

- You can run CiscoWorks on the same PC as Cisco DCNM although the Java requirements are different. When installing the later Java version for Cisco DCNM, make sure that it does not overwrite the earlier Java version that is required for CiscoWorks. Both versions of Java can coexist on your PC.
- Ensure that you use the same Operating System for all the nodes in the Federation setup.
- In the Federation setup, ensure that the server time is synchronized across all the nodes of the Federation setup. The servers will not be able to communicate if the time is not synchronized. We recommend that you use NTP server to synchronize time across all the nodes.
- If you are installing DCNM on Windows 2016 server, ensure that you disable “Windows Defender” that is running by default.

Prerequisites for Installing DCNM on Linux

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command: **sysctl -w kernel.shmmax=268435456**. Save the **kernel.shmmax=268435456** value in the **/etc/sysctl.conf** file. If this value is not correct, the Cisco DCNM server fails after the server system reboots. For more information, visit the following URL:

  http://www.postgresql.org/docs/8.4/interactive/kernel-resources.html
- The server system must be registered with the DNS servers.
- No other programs must be running on the server.
- Ensure that you select English as the preferred language during RHEL installation.
- Ensure that you use the same Operating System for all the nodes in the Federation setup.
- In the Federation setup, ensure that the server time is synchronized across all the nodes of the Federation setup. The servers will not be able to communicate if the time is not synchronized. We recommend that you use NTP server to synchronize time across all the nodes.
- After you upgrade from Cisco DCNM Release 11.2(1) on Linux Standalone server, ensure that you clear the browser cache and Java console cache before you launch the Web UI and download the SAN Client. The Java console remembers the previous version of the SAN client data. If you do not clear Java console cache, you will not be able to use the latest downloaded SAN Client.

Antivirus exclusion

Scanning the Cisco DCNM includes the scanning of the database files. This process will hamper the performance on the DCNM while operation. While scanning the Cisco DCNM on Linux RHEL server, exclude the directory `/usr/local/cisco/dcm/db and /var/lib/dcnm`.

For more information, refer to https://wiki.postgresql.org.

Note We recommend you to stop Anti-Virus scanning while installing DCNM because the port being used or blocked might cause failures. After the installation, you can enable or install Anti-Virus application with specific guidelines to avoid DCNM directories as part of the scan.

Oracle Database for DCNM Servers

This section details about the database required for the installation of DCNM server.

Note This section is not applicable for Cisco DCNM Native HA installation.

Cisco DCNM supports the following databases:

- Oracle Database 11g
- Oracle Database 12c
- Oracle RAC 11g, and 12c

You can change from the local database to an external Oracle database, if required.

Note Cisco DCNM is configured with AL32UTF8 character set.

The Cisco DCNM Database size is not limited and increases based on the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. Cisco recommends that you use Oracle SE or Enterprise edition, instead of Oracle XE, due to table space limitations.

This section contains the following:

Oracle SQLPlus Command-Line Tool

The Oracle database procedures in this section require the use of the SQL*Plus command-line tool. The SQL*Plus executable is typically installed in the bin directory under the Oracle home directory.

Linux Environment Variables

If you are using Linux, before you use the SQL*Plus command-line tool, ensure that the ORACLE_HOME and ORACLE_SID environment variables are set to correct values.

For example, if you are using Oracle 11g on Linux, the following commands set the environment variables to the default Oracle home directory and SID if you are using a bash shell:

```
export ORACLE_HOME=<usr_home_directory>/app/oracle/product/11.2.0/
(or identify the Oracle home on the Oracle installed server)
export ORACLE_SID=XE
```

init.ora File

The init.ora file specifies startup parameters. The default name and location of the file is platform specific, as shown in the following table.

Table 4: Name and Default Location of init.ora File

Oracle Version	Operating System	Location of init.ora File
12c	Microsoft Windows	C:\app\Administrator\virtual\product\12.2.0\dbhome_1\srvm\admin\init.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/12.2.0/db_1/srvm/initORCL.ora
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dbs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dbs/initORCL.ora

Backing up the Oracle Database

Copy the oracle backup/restore script from the Cisco DCNM server directory `DCNM_SERVER_Install/dcm/dcnm/bin`.

For Linux, the script name is backup-remote-oracledb.sh/restore-remote-oracledb.sh and edit the DB_HOME variable to point to the Oracle installation.

For Windows, the script name is **backup-remote-oracledb.bat/restore-remote-oracledb.bat** and edit *DB_HOME* variable to point to the Oracle installation.

Use the following path for Oracle DBHOME:

- On Linux– `/usr/lib/oracle/xe/app/oracle/product/10.2.0/server`

  Replace `/usr/lib/oracle` with the Oracle installation path.

- On windows– `C:\oraclexe\app\oracle\product\10.2.0\server`

  Replace `C:\oraclexe` with the Oracle installation path.

Preparing the Oracle Database

You can prepare an Oracle database.

Procedure

Step 1 Increase the number of sessions and processes to 150 each. For more information, see the Increasing the Number of Sessions and Processes to 150 Each, on page 27.

Step 2 Increase the number of open cursors to 1000. For more information, see the Increasing the Number of Open Cursors to 1000, on page 27.

Logging Into Oracle

You can log into the Oracle database by using the SQL*Plus command-line tool.

Before you begin

Ensure that you know the database administrator username and password.

Procedure

Step 1 Run the SQL*Plus executable.

A command prompt appears.

Step 2 Enter the **connect** command.

The Username prompt appears.

Step 3 Enter the database administrator username.

The Password prompt appears.

Step 4 Enter the password for the username that you specified.

For example, if the Oracle administrator username is system and the password is oracle, you would log in as follows:

Example:

```
Username: sys as sysdba
Password: oracle
```

What to do next

For more information about using SQL*Plus, see the documentation for the Oracle database version that you are using.

Increasing the SYSTEM Tablespace

You can increase the SYSTEM tablespace.

Procedure

Step 1 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 24.

Step 2 Enter the following command:

```
select file_name, bytes, autoextensible, maxbytes
from dba_data_files where tablespace_name='SYSTEM';
```

Step 3 Enter the following command:

```
alter database datafile filename autoextend on next 100m maxsize 2000m;
```

where *file_name* is the filename from the output of the **select** command in the previous step.

The SYSTEM tablespace is increased.

Step 4 Enter the **exit** command.

Increasing the Number of Sessions and Processes to 150 Each

For each DCNM instance configured in the same Oracle database, the number of cursors and processes must be increased to more than the 150 and 1000.

For example, if two DCNM standalone (non HA) instances are configured to use the same Oracle database, the cursors and process must be increased to 300 and 2000 approximately, depending on any performance degradation or SQL Exception errors occurred during normal operations of either of the DCNM instances.

Procedure

Step 1 Ensure that the `init.ora` file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines, remove them.

For more information, see the init.ora File, on page 24.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 24.

Step 3 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 4 Enter the following command:

```
startup pfile='init_file_name';
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the init.ora File, on page 24.

Step 5 Set the number of sessions to 150 by entering the following command:

```
alter system set sessions = 150 scope=spfile;
```

Step 6 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 7 Start up the system by entering the **startup** command.

Step 8 Verify that the number of sessions and processes is changed to 150 by entering the following command:

```
show parameter sessions
```

Step 9 Exit by entering the **exit** command.

Increasing the Number of Open Cursors to 1000

You can increase the number of open cursors to 1000.

Procedure

Step 1 Ensure that the init.ora file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines in the file, remove them.

For more information, see the init.ora File, on page 24.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 24.

Step 3 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 4 Enter the following command:

```
startup pfile='init_file_name'
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the init.ora File, on page 24.

Step 5 Set the number of open cursors to 1000 by entering the following command:

```
alter system set open_cursors = 1000 scope=spfile;
```

Step 6 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 7 Start up the system by entering the **startup** command.

Step 8 Verify that the number of open cursors is changed to 1000 by entering the following command:

```
show parameter open_cursors
```

Step 9 Exit by entering the **exit** command.

Creating an Oracle DB User using the Command Prompt

To create an Oracle DB user using the command prompt, follow these steps:

```
export ORACLE_SID=XE
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
cd $ORACLE_HOME/bin
sqlplus
sys as sysdba
create user dcnmdbusername identified by dcnmdbuserpassword default tablespace users temporary
 tablespace temp;
grant connect, resource to dcnmdbusername;
grant create session to dcnmdbusername;
grant dba to dcnmdbusername;
```

Note Ensure you set the Oracle_SID and Oracle_Home and enter the values for the DB Username and password fields.

Note When a DBA account cannot be created, an account with DML/DDL/schema privilege is sufficient.

Connecting to an Oracle RAC with SCAN Feature Type DB

To connect to an Oracle RAC with SCAN Feature type DB, enter the following command:

```
# appmgr update -u jdbc:oracle:thin:@//[ip_addr]:1521/[service name] -n [username] -p
[password]
```

Database for Federation Setup

Cisco DCNM can be deployed as Cisco DCNM-SAN federation. For Cisco DCNM-SAN federation, the database URL (properties) must remain the same for all Cisco DCNM-SAN nodes in the federation.

Note Ensure that you do not provide multicast addresses to form the federation.

Remote Oracle Database Utility Scripts for Backup and Restore

Irrespective of the platform, Cisco DCNM is installed (Windows or Linux), the following scripts to backup and restore the remote Oracle database.

Utility scripts for Oracle database that is installed on Linux platform are;

1. backup-remote-oracledb.sh
2. restore-remote-oracledb.sh

Utility scripts for Oracle database that is installed on Windows platform are:

1. backup-remote-oracledb.bat
2. restore-remote-oracledb.bat

Cisco DCNM host is configured to run with a remote Oracle database. As part of housekeeping, you can copy DCNM utility scripts to a remote Oracle database and restore the DCNM database schema.

To run the utility scripts, you need the database administrator credentials. These scripts will prompt you for:

1. DCNM database password (the user name is already present)
2. Username/password of the admin user.

While entering the DBA user credentials, ensure that you do not to enter “sys” as sysdba" because in some versions of Oracle, the presence of space might cause the backup/restore to fail. Instead, user should provide valid user credentials that does not have a space in the user name, for example, system or sysdba. The admin credentials are not saved/cached and hence they do not leak sensitive credential information.

Note User scripts under **dcnm/bin** can be run only by administrator user.

Local PostgreSQL Database Utility Scripts for Backup and Restore

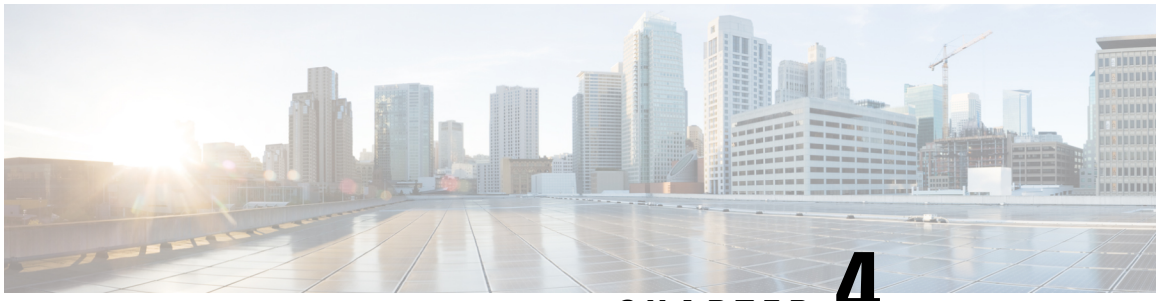
Utility scripts for Local PostgreSQL database that is installed in RHEL machine are:

1. backup-pgsql-dcnm-db.sh

2. restore-pgsql-dcnm-db.sh

Utility scripts for Local PG database that is installed in Windows machine are:

1. backup-pgsql-dcnm-db.bat
2. restore-pgsql-dcnm-db.bat



CHAPTER 4

Installing Cisco DCNM

This chapter contains the following sections:

Installing Cisco DCNM on Windows

Downloading the Cisco DCNM Windows Installer and Properties File

The first step to installing the DCNM on Windows is to download the dcnm.exe file.

Note If you plan to use Federation application functions, you must deploy the dcnm.exe file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose .

Step 5 Locate the DCNM Windows Installer and click the **Download** icon.

The installer file is of the format .

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM using GUI

Installing Cisco DCNM on Windows Using the GUI

Perform the following steps to install DCNM Windows using the GUI:

Procedure

Step 1 Locate the `dcnm.exe` file that you have downloaded.

Double click on the `dcnm.exe` file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from the OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager.
- IBM—to install the IBM Data Center Network Manager.

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the dcnm.exe.
- Existing PostgreSQL 9.4
- Existing Oracle 10g/11g/12c
- Existing Oracle 10g/11g/12c RAC

  In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click OK. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there are no schemas existing with the DCNM

username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, which is known as “public”.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the DCNM DB User field, enter the username that the Cisco DCNM uses to access the database. In the DCNM DB Password field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are not commonly used. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM LAN archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

  Note Ensure that this folder is accessible by all nodes in the Federation setup.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access both DCNM SAN and DCNM LAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

  Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly:

  - It must be at least 8 characters long and contain at least one alphabet and one numeral.

- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server should use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

You can configure LDAP authentication after installing DCNM.

Note After TACACS/RADIUS/LDAP is enabled, Local user "admin" cannot be accessible. This is default behavior.

Only if the TACACS/RADIUS/LDAP server is not reachable or down, the Local user will be validated and will be able to login.

If LDAP/RADIUS/TACACS server is reachable and authentication fails on TACACS/LDAP/RADIUS then no fall back to local.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

Step 12 In the Choose Shortcut Folder screen, specify path where you want to create the DCNM icons.

If you want the installer to create the shortcuts for all users who can log into the server system, check the **Create icons for All Users** check box.

Click **Next**.

Step 13 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 14 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 15 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

The prompt will return after the silent install is complete.

Step 16 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Windows for LAN and SAN Management.

Installing Cisco DCNM Windows in a Server Federation Environment using GUI

To install DCNM in a server federation environment:

Before you begin

Ensure that you have installed DCNM on the Primary server. Follow the instructions provided in Installing Cisco DCNM on Windows Using the GUI, on page 32 section.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers was enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If user you wants to use only strong ciphers for network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM user name and password of the primary server. Also, you must provide the database user name and password of the primary server.

The user name and password of the database are same for all the server installation forming the federation. Similarly, the user name and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM through Silent Installation

Installing Cisco DCNM Windows through Silent Installation

Cisco DCNM supports Silent installation only on Local Authorization mode and not on Remote Authorization mode.

Perform the following steps to install DCNM Windows through silent installation.

Procedure

Step 1 Unzip, extract and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties--------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=C:\\Program Files\\Cisco Systems
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#-----------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

PG_DB_PATH=C:\\Program Files\\Cisco Systems\\dcm\\db

#----------New Postgres---------------------------------
DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
```

If you are using the Oracle database, edit this block:

```
#-----------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 4 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-------------------------------------------------------------------------
```

Step 5 Configure IBM Raven to install IBM Data Center Network Manager.

```
#-----------------------------IBM Raven Support----------------------
#Set true if Vendor is IBM, by default false
#-------------------------------------------------------------------------

IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#-------------------------------------------------------------------------
```

Step 6 Navigate to the directory where you downloaded the Cisco DCNM Windows software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *path_of_installer.properties_file*

You can check the status of installation in the Task Manager process.

Step 7 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM on Linux

Downloading the Cisco DCNM Linux Installer and Properties File

The first step to installing the DCNM on Linux is to download the dcnm.bin file.

Note If you plan to use Federation application functions, you must deploy the dcnm.bin file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose Release 11.1(1).

Step 5 Locate the DCNM Linux Installer and click the **Download** icon.

The installer file is of the format `dcnm-installer-x64.11.1.1.bin`.

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM using GUI

Installing Cisco DCNM on Linux Using the GUI

Perform the following steps to install DCNM Linux using the GUI:

Procedure

Step 1 Locate the `dcnm-installer-x64.<release-name>.bin` file that you have downloaded.

Run the `dcnm.bin` installer file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager
- IBM—to install IBM Data Center Network Manager

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the `dcnm.bin`.
- Existing PostgreSQL 9.4—Existing PostgreSQL database that is already set up, with a clean schema.

- Existing Oracle 10g/11g/12c—Existing Oracle database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c RAC—Existing Oracle database that is already set up, with a clean schema.

In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click **OK**. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Note Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there is no schema existing with the DCNM username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, known as “public”.

If the tables are created in the default schema, you may encounter authentication issues after upgrading Cisco DCNM. You will have to create a schema with the sane name as the DCNM username owned by the same username. For instructions, see User and Schemas, on page 61.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the **DCNM DB User** field, enter the username that Cisco DCNM user uses to access the database. In the **DCNM DB Password** field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in Federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are free. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access DCNM SAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

  Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly:

  - It must be at least eight characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server must use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

The Choose Link Folder is skipped and by default the location is `/root` directory.

Step 12 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 13 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 14 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

Step 15 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM Linux in a Server Federation Environment Using GUI

To install DCNM in a server federation environment:

Before you begin

Ensure that you have installed DCNM on the Primary server. Follow the instructions in Installing Cisco DCNM on Linux Using the GUI, on page 38 section.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers were enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If you use only strong ciphers for the network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM username and password of the primary server. Also, you must provide the database username and password of the primary server.

The username and password of the database are same for all the server installation forming the federation. Similarly, the username and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM through Silent Installation

Installing Cisco DCNM Linux Through Silent Installation

Cisco DCNM supports Silent installation only on Local Authorization mode and not on Remote Authorization mode.

Perform the following steps to install DCNM Linux through silent installation.

Procedure

Step 1 Unzip, extract, and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties--------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=/usr/local/cisco/dcm
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#--------------New Postgress---------------------------
PG_DB_PATH=/usr/local/cisco/dcm/db

#PG_DB_PATH=/opt/dctest/cisco/dcm/db /*non-default installation directory*/
#BACKUP_FILE=/opt/dctest/cisco/dcm/dcnm/bin/<backup-filename> /*non-default backup file
directory*/

DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
#CLEAN_DATABASE=TRUE
```

If you are using the Oracle database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE
ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the Data Path for DCNM.

```
#---------------------DATA PATH----------------
#Data path is the folder location where DCNM LAN related
#information like Config archives, templates etc. are stored.
# In DCNM LAN Cluster mode this folder has to be a shared folder.
#For linux and windows it will be different as the folder structure vaires
#-----------------------------------------------------

DATA_PATH=/usr/local/cisco/dcm/dcnm
#---------------------DATA PATH----------------
```

Step 4 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-----------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 5 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-------------------------------------------------------------------------
```

Step 6 Configure IBM Raven to install IBM Data Center Network Manager.

```
#------------------------------IBM Raven Support----------------------
#Set true if Vendor is IBM, by default false
#-------------------------------------------------------------------------

IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#-------------------------------------------------------------------------
```

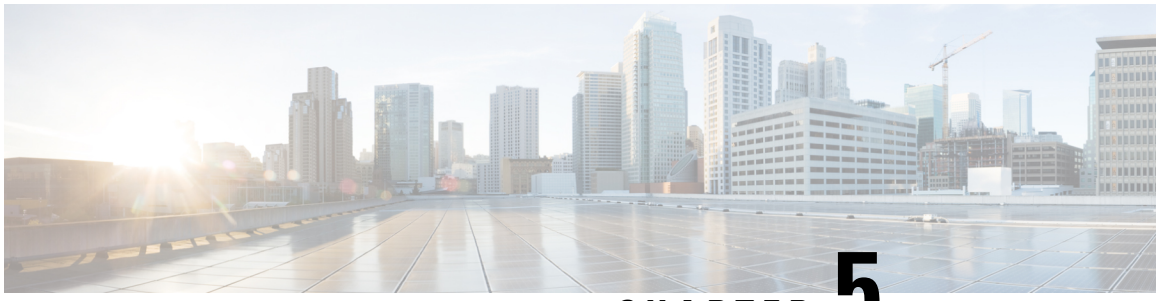
Step 7 Navigate to the directory where you downloaded the Cisco DCNM Linux software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *path_of_installer.properties_file*

You can check the status of installation by using the following command **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

Step 8 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Linux for SAN Management.



CHAPTER 5

Upgrading Cisco DCNM

This section includes instructions for upgrading your Cisco DCNM Appliance installation in the following scenarios:

The following table summarizes the upgrade options for Cisco DCNM Release .

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for all platforms:

  <SPACE> & $ % ‘ “ ^ = < > ; :

However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

This chapter contains the following:

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

```
<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\standalone-san.xml
```

Update the password in the **keystore** tag and alias:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks">
```

Procedure

Step 1 Backup the signed certificate from the location:

- For Windows: **<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks**
- For Linux: **<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks**

Step 2 Upgrade to Cisco DCNM Release 11.1(1).

Step 3 After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.

Note You must load the certificates to the same location as mentioned in Step 1, on page 46.

Step 4 Restart the DCNM Services.

Upgrading Cisco DCNM on Windows

Upgrading Cisco DCNM Windows using GUI

Procedure

Step 1 Stop the DCNM services.

Step 2 Run the Cisco DCNM software for Release executable file.

Upgrade Notification window appears

Step 3 Click **OK** to begin the upgrade.

Step 4 Click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically.

Upgrading Cisco DCNM Windows Federation using GUI

Note Ensure that both primary and secondary database properties are same.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, run the Cisco DCNM Release executable file.

Upgrade notification window appears.

Step 3 Click **OK** to begin the upgrade.

Step 4 On the primary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically on the primary server.

Step 5 On the secondary server, perform run the Cisco DCNM Release executable file.

Upgrade notification window appears.

Step 6 Click **OK** to begin the upgrade.

Step 7 On the secondary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically on the secondary server.

Upgrading Cisco DCNM Windows through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Procedure

Step 1 Stop the DCNM services.

Step 2 Open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
#---------------Use Existing Oracle-------------
DCNM_DB_URL=jdbc\:oracle\:thin\:@<ip_address_of_oracle_machine>\:1521\:XE
DCNM_DB_NAME=XE
SELECTED_DATABASE=oracle
DCNM_DB_USERNAME=oracledbadmin1
DCNM_DB_USER_PASSWORD=oracledbadmin1
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *<path_of_installer.properties>*

The Cisco DCNM Release services will start after the upgrade is complete.

You can check the status of the upgrade in the Task Manager process.

Upgrading Cisco DCNM Windows Federation through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Note Ensure that both primary and secondary database properties are same.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *<path_of_installer.properties>*

You can check the status of the upgrade in the Task Manager process.

The Cisco DCNM Release services will start automatically on the primary server.

Step 4 On the secondary server, open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
#---------------Use Existing Oracle--------------
DCNM_DB_URL=jdbc\:oracle\:thin\:@<ip_address_of_oracle_machine>\:1521\:XE
DCNM_DB_NAME=XE
SELECTED_DATABASE=oracle
DCNM_DB_USERNAME=oracledbadmin1
DCNM_DB_USER_PASSWORD=oracledbadmin1
```

Step 5 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *<path_of_installer.properties>*

You can check the status of the upgrade in the Task Manager process.

The Cisco DCNM Release services will start automatically on the secondary server.

Upgrading Cisco DCNM on Linux

Upgrading Cisco DCNM Linux using GUI

Procedure

Step 1 Stop the DCNM services.

Step 2 Run the Cisco DCNM software for Release executable file.

Upgrade Notification window appears

Step 3 Click **OK** to begin the upgrade.

Step 4 Click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically.

What to do next

After you upgrade from Cisco DCNM Release 11.2(1) on Linux Standalone server, ensure that you clear the browser cache and Java console cache before you launch the Web UI and download the SAN Client. The Java console remembers the previous version of the SAN client data. If you do not clear Java console cache, you will not be able to use the latest downloaded SAN Client.

Upgrading Cisco DCNM Linux Federation using GUI

Note Ensure that both primary and secondary database properties are same.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, run the Cisco DCNM Release executable file.

Upgrade notification window appears.

Step 3 Click **OK** to begin the upgrade.

Step 4 On the primary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically on the primary server.

Step 5 On the secondary server, perform run the Cisco DCNM Release executable file.

Upgrade notification window appears.

Step 6 Click **OK** to begin the upgrade.

Step 7 On the secondary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically on the secondary server.

Upgrading Cisco DCNM Linux through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Note You must use the same database for Release as in the existing DCNM set up.

Procedure

Step 1 Stop the DCNM services.

Step 2 Open the `installer.properties` file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *<path_of_installer.properties>*

The Cisco DCNM Release services will start after the upgrade is complete.

You can check the status of the upgrade process by using the following command: **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

Upgrading Cisco DCNM Linux Federation through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Note Ensure that both primary and secondary database properties are same as in the previous Release set up.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, open the `installer.properties` file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *<path_of_installer.properties>*

You can check the status of the upgrade process by using the following command: **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

The Cisco DCNM Release services will start automatically on the primary server.

Step 4 On the primary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release services will start automatically on the primary server.

Step 5 On the secondary server, open the installer.properties file and update the following properties:

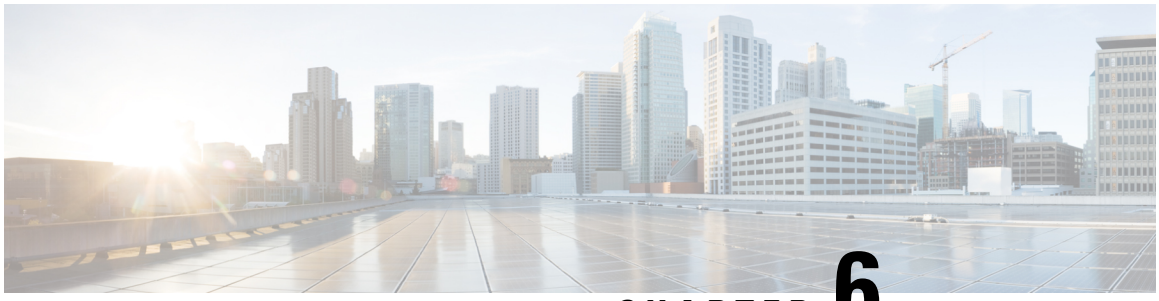
```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 6 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *<path_of_installer.properties>*

You can check the status of the upgrade process by using the following command: **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

The Cisco DCNM Release services will start automatically on the secondary server.



CHAPTER 6

Running Cisco DCNM Behind a Firewall

This chapter provides information about running Cisco DCNM behind a firewall.

Running Cisco DCNM Behind a Firewall

Generally, an Enterprise (external world) and Datacenter is separated by a firewall, i.e., DCNM is configured behind a firewall. The Cisco DCNM Web Client, Cisco DCNM SAN Client, and Cisco Device Manager connectivity will pass-through that firewall. A firewall can be placed between the DCNM Server and DCNM-managed devices also.

Beginning with Cisco DCNM Release 11.0(1), DCNM SAN Client initiates communication with DCNM SAN Server on HTTPS port 443. However, both DCNM SAN Client and Device Manager communicate with the devices directly also. Device Manager can be invoked through DCNM SAN Server UI and it runs within the context of the DCNM SAN Server. The Device Manager communication with devices remains same, as if it was running independently.

DCNM SNMP proxy services on DCNM SAN Server use a configurable TCP port (9198 by default) for SNMP communications between the DCNM SAN Client or Device Manager, and DCNM Server.

The UDP SNMP_TRAP local ports are between 1163-1170, for both Cisco DCNM-SAN and Device Manager. DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses.

You can select the UDP port that the Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the `DeviceManager.bat` file in the `C:\Program Files\Cisco Systems\MDS9000\bin` directory:

  ```
  rem JVMARGS=%JVMARGS% -Dsnmp.localport=[localport]
  ```

  Where [localport] is the value of free local port.
- On a LINUX desktop, uncomment the following in the `DeviceManager.sh` file in the `$HOME/.cisco_mds9000/bin` directory:

  ```
  # JVMARGS=$JVMARGS -Dsnmp.localport=[localport]
  ```

  Where [localport] is the value of free local port.

Any standard port where the Ingress traffic enters from clients cannot be modified unless you disable the local firewall.

Running Cisco DCNM Behind a Firewall

The following table lists all ports that are used for communication between DCNM Web Client, DCNM SAN Client, Device Manager, SSH Client, and DCNM Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	SSH to DCNM SAN Server	SSH access to external world is optional.
443	TCP	HTTPS	Client to DCNM SAN Server	Cisco DCNM Web Client, Cisco DCNM SAN Client to the Cisco DCNM Server
1099	TCP	Java RMI	Client to DCNM SAN Server	Cisco DCNM SAN Client to Server
1163 to 1170	UDP	SNMP_TRAP	Device to SAN Client and Device Manager	Cisco DCNM SAN Client and Cisco Device Manager use same range of ports.
3528	TCP	JBOSS	Client to DCNM SAN Server	Wildfly JBOSS IIOP
3529	TCP	JBOSS	Client to DCNM SAN Server	Wildfly JBOSS IIOP SSL
9198	UDP/TCP	SNMP	SAN Client, Device Manager to DCNM SAN Server[1]	Cisco DCNM SNMP proxy services use the TCP port (9198 by default) for SNMP communications between the Cisco DCNM SAN Client or Cisco Device Manager and the Cisco DCNM Server.
61616	TCP	Messaging	DCNM SAN Client to DCNM SAN Server	

[1] Cisco DCNM SAN Client picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. The port can be changed with the `client -Dsnmp.localport` option.

Cisco Device Manager picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. The port can be changed in `server.properties` file.

DCNM SNMP proxy is used when SAN Client or Device Manager cannot reach managed devices directly and SNMP responses coming to DCNM SAN Server from managed devices can be relayed to SAN Client and Device Manager. DCNM SAN Client and Device Manager must reach to DCNM SAN Server port 9198 (or whatever port is configured) to get the SNMP response.

The following table lists all the ports that are used for communication between the Cisco DCNM Server and other services which can be hosted on either side of the firewall.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
49	TCP/UDP	TACACS+	Cisco DCNM SAN Server to ACS Server	ACS Server can be on either side of the firewall.
53	TCP/UDP	DNS	Cisco DCNM SAN Server to DNS Server	DNS Server can be on either side of the firewall.
123	UDP	NTP	Cisco DCNM SAN Server to NTP Server	NTP Server can be on either side of the firewall.
1521	TCP	Oracle	DCNM SAN Server to the Oracle database Server	This is necessary if the Oracle server is installed external to the DCNM host machine. Oracle server may be configured to listen on a different port and in that case that port in question must be taken into account. **Note** You can choose the Oracle server port during DCNM SAN installation and must not be modified later, after installation.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
5432	TCP	Postgres	Cisco DCNM SAN Server to Postgres Server	The default installation of DCNM does not need this port. This is necessary if Postgres is installed externally to the DCNM host machine.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
9198	UDP\TCP	SNMP	DCNM SAN Client, Device Manager to DCNM SAN Server	

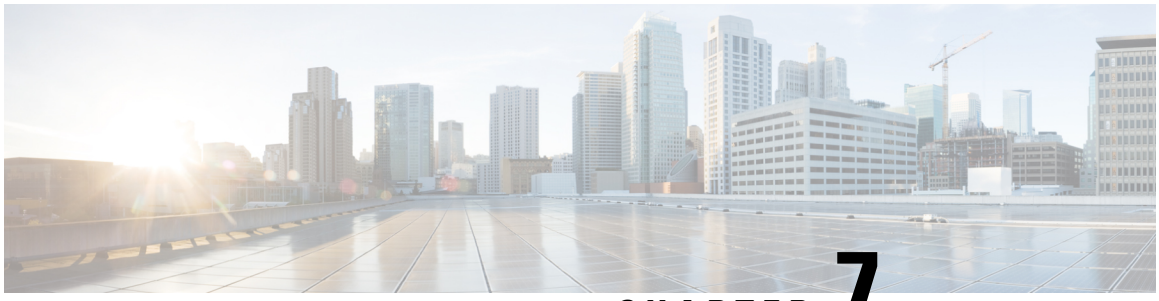
Port Number	Protocol	Service Name	Direction of Communication	Remarks
				Cisco DCNM SNMP proxy services use the TCP port (9198 by default) on DCNM SAN Server for SNMP communications between the Cisco DCNM SAN Client or Cisco Device Manager and the Cisco DCNM Server. Cisco DCNM SAN Client picks a random free local port (UDP) or 9198 (TCP) to reach SNMP proxy. The port can be changed with the client -Dsnmp.localportoption. Cisco Device Manager picks a random free local port (UDP) or 9198 (TCP) to reach SNMP proxy. The port can be changed in the server.properties file. DCNM SNMP proxy is used when SAN Client or Device Manager cannot reach the managed devices directly and SNMP responses coming to DCNM SAN Server from managed devices can be relayed to SAN Client and Device Manager. DCNM

Port Number	Protocol	Service Name	Direction of Communication	Remarks
				SAN Client and Device Manager must reach to DCNM SAN Server port 9198 (or whatever port is configured) to get the SNMP response.

The following table lists all the ports that are used for communication between Cisco DCNM Server and Managed devices.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	Both Direction	Server to Device – To manage devices. Device to Server – SCP (POAP)
67	UDP	DHCP	Device to DCNM SAN Server	
69	TCP	TFTP	Device to DCNM SAN Server	Required for POAP
161	TCP/UDP	SNMP	DCNM SAN Server to Device	Cisco DCNM configured via `server.properties` to use TCP on port 161 instead of UDP port 161.
514	UDP	Syslog	Device to DCNM SAN Server	
2162	UDP	SNMP_TRAP	Device to DCNM SAN Server	

Port Number	Protocol	Service Name	Direction of Communication	Remarks
5989	TCP	SMI-S Agent	Both direction	Server to Device. This is where the Storage device listens. An application to DCNM Server – When DCNM Server is acting as storage proxy. Server to the Storage device port number is depended upon where the storage device is listening on. It could be 5989, 5888, or other ports.
57500	TCP	gRPC	Device to DCNM SAN Server	SAN Telemetry Streaming



CHAPTER 7

User and Schemas

This chapter provides information about creating Users and user-specific schema for *Cisco Data Center Network Manager*.

Creating New Users

Perform this task, to create a new user.

Procedure

Step 1 Logon to the SSH terminal of the DCNM Appliance.

Step 2 Create a new user using the **create user** *username* command.

Step 3 Enter a valid password at the password prompt.

Step 4 Create a new schema with same name as the user, using the **create schema***username***authorization***username*.

Step 5 Enable all permissions on the schema, using the **grant all on schema***username***to***username*.

Example

The following example shows the sample output for creating new users

```
dcnm# create user user1
password: password
dcnm# create schema user1 authorization user1;
dcnm# grant all on schema user1 to user1;
```

Creating New Schema for Existing Users

Perform this task to retain the same create new schema to an existing user.

Procedure

Step 1 Logon to the SSH terminal of the DCNM Appliance.

Step 2 Drop the existing user by using the **drop user***username***cascade** command.

Step 3 Drop the existing schema with same name as username, by using the **drop schema***username***cascade** command.

Step 4 Create a new user using the **create user** *username* command.

Step 5 Enter a valid password at the password prompt.

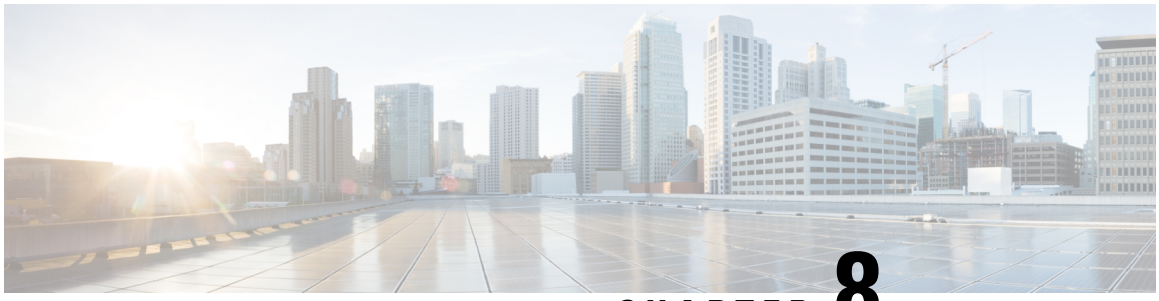
Step 6 Create a new schema with same name as the user, using the **create schema***username***authorization***username* command.

Step 7 Enable all permissions on the schema, using the **grant all on schema***username***to***username*.

Example

The following example shows the sample output for creating new users

```
dcnm# drop user user_old cascade
dcnm# drop schema user_old cascade
dcnm# create user user_new
password: password
dcnm# create schema user_new authorization user_new;
dcnm# grant all on schema user_new to user_new;
```



CHAPTER 8

Certificates

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

```
<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\standalone-san.xml
```

Update the password in the **keystore** tag and alias:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks">
```

Procedure

Step 1 Backup the signed certificate from the location:

- For Windows: **<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks**
- For Linux: **<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks**

Step 2 Upgrade to Cisco DCNM Release 11.1(1).

Step 3 After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.

Note You must load the certificates to the same location as mentioned in Step 1, on page 63.

Step 4 Restart the DCNM Services.

Configuring Certificates for Cisco DCNM

This section describes three ways on how to configure the certificates in Cisco DCNM.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias in the **key-alias** tag:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks">
```

This section contains the following topics:

Using a self signed SSL Certificate

Procedure

Step 1 Stop the DCNM services.

Step 2 Rename the keystore located at

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks`

to

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks.old`

Step 3 From command prompt, navigate to `<DCNM install root>\dcm\java\jre1.8\bin\`.

Step 4 Generate a self signed certificate using following command:

keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Start the DCNM services.

Using a SSL Certificate when certificate request is generated using Keytool on Windows

Procedure

Step 1 Stop the DCNM services.

Step 2 Rename the keystore located at:

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks`

to

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks.old`

Step 3 From command prompt, navigate to the appropriate folder:

`<DCNM install root>\dcm\java\jre1.8\bin\`

Step 4 Generate the public-private key pair in DCNM keystore by using the following command:

keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore "<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Generate the certificate-signing request (CSR) from the public key generated in Step 4, on page 65.

keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3

Note The `dcnm.csr` file is created in the keytool directory, located at `/usr/local/cisco/dcm/java/jre1.8/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the .p7b file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to Step 7, on page 65 to convert it to PEM format. If CA provided PEM format, then go to Step 8, on page 65.

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain using openssl.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of `cert-chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

keytool -importcert -trustcacerts -file cert-chain.pem -keystore "<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -alias sme

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Start the DCNM service.

Using an SSL Certificate When Certificate Request Is Generated Using Keytool on Linux

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.

Step 2 Rename the keystore that is located at:

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks`

To

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old`

Step 3 From command prompt, navigate to the appropriate folder:

`<DCNM install root>/dcm/java/jre1.8/bin/`

Step 4 Generate the public-private key pair in DCNM keystore by using the following command:

./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Generate the certificate-signing request (CSR) from the public key that is generated in Step 7, on page 66.

./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks" -storepass fmserver_1_2_3

Note The dcnm.csr file is created in the keytool directory, which is located at `/usr/local/cisco/dcm/java/jre1.8/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the `.p7b` file.

CA may provide the certificate and signing certificate as a certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided the certificate chain in PKCS 7 format, go to Step 7, on page 66 to convert it to PEM format. If CA provided the certificate chain in PEM format, then go to Step 8, on page 66.

Step 7 Convert the PKCS 7 certificate chain to the X509 certificate chain using OpenSSL.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of cert-`chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

./keytool -importcert -trustcacerts -file cert-chain.pem -keystore <DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks -storepass fmserver_1_2_3 -alias sme

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Start the applications in the server by using the **appmgr start dcnm** command.

Using a SSL Certificate when certificate request is generated using OpenSSL on Linux

To configure SSL certificates in Cisco DCNM, using certificate request generated using open SSL, perform the following steps.

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.

Step 2 Rename the keystore located at:

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks`

to

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old`

Step 3 From command prompt, navigate to `<DCNM install root>/dcm/java/jre1.8/bin/`.

Step 4 Generate the RSA private key using OpenSSL.

openssl genrsa -out dcnm.key 2048

Step 5 Generate a certificate-signing request (CSR) by using following command:

openssl req -new -key dcnm.key –sha256 -out dcnm.csr

Step 6 Submit the CSR to Certificate signing authority, and download the signed certificate chain in Base-64 format which creates the **.p7b** file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provids the PKCS 7 format, go to Step 7, on page 67 to convert it to PEM format. If CA provides the PEM format, go to Step 8, on page 67.

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Step 8 Convert the X509 certificate chain and private key to PKCS 12 format

openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password pass fmserver_1_2_3 -name sme

Note Ensure that the user provides either absolute path or relative path to the correct location of dcnm.key & `dcnm.p12` files in the above command.

Step 9 Import the intermediate certificate, the root certificate, and the signed certificate in the same order.

./keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore <DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks -deststoretype JKS -alias sme

Note Ensure that the user provides either absolute path or relative path to the correct location of `cert-chain.pem`, `dcnm.key`, and `dcnm.p12` files in the above command.

Step 10 Start the DCNM services, or the DCNM applications in the server by using the **appmgr start dcnm** command.

Collecting PM Data

To setup a shared rrd path to collect PM data, perform these steps:

Procedure

Step 1 Locate the **server.properties** file under **C:\Program Files\Cisco Systems\dcm\fm\conf**.

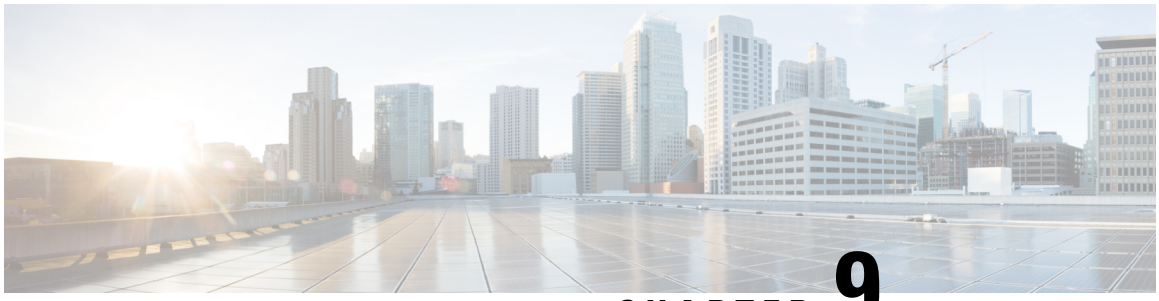
Step 2 Add the **pm.rrdpath** property file information to the server.properties file. For example, add the server location that needs to be accessible from the DCNM server.

Step 3 Save the server.properties file.

Step 4 Restart the Cisco DCNM-SAN server.

What to do next

Once PM server is ready, the new shared location will be used by the PM server to save .rrd files. PM will create a new directory called db under pm. Ensure you do not open or change these .rrd files as PM server is actively writing into the .rrd files.



CHAPTER 9

Secure Client Communications for Cisco DCNM Servers

This section describes how to configure HTTPS on Cisco Data Center Network Manager Servers.

Note You must enable SSL/HTTPS on the Cisco DCNM before you add a CA signed SSL certificate. Therefore, perform the procedure in the below mentioned order.

This section includes the following topics:

Enabling SSL/HTTPS on Cisco DCNM in Federation on RHEL or Windows

To enable SSL/HTTPS on RHEL or Windows for Cisco DCNM in Federation, perform the following:

Procedure

Step 1 Configure the primary server with a self signed SSL certificate.

Note In a CA signed certificate, each server has their own certificate generated. Ensure that the certificate is signed by the signing certificate chain which is common for both the servers.

Step 2 On the secondary server, perform one of the following:

- While executing the installer, choose HTTPS upfront and select to run in the HTTPs mode.
- While silent installation, choose HTTPs while you execute the installer.