



## **Cisco DCNM Installation Guide, Release 10.4(1)**

October 2017

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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

© 2017 Cisco Systems, Inc. All rights reserved.



## **Preface 1**

- Audience 1
- Document Conventions 1
- Related Documentation 2
- Documentation Feedback 4
- Obtain Documentation and Submit a Service Request 4

---

## **CHAPTER 1**

### **Overview 1-1**

- Introduction of Cisco DCNM 1-1
  - Cisco DCNM Server 1-2
  - Cisco DCNM Web Client 1-2
  - Cisco DCNM-SAN Client 1-2
  - Device Manager 1-2
  - Performance Manager 1-2
- Programmable Fabric and non-Programmable Fabric 1-2
  - Information about Programmable Fabric 1-3
  - Information about non-Programmable Fabric 1-3
- Installation Options 1-4
  - DCNM Open Virtual Appliance for VMware 1-4
  - DCNM ISO Virtual Appliance for VMware/KVM/UCS-C Series 1-4
  - DCNM Installer for Windows (64-bit) 1-4
  - DCNM Installer for Linux (64-bit) 1-4
- Deployment Options 1-4
  - Standalone Server 1-5
  - Standalone with external Oracle 1-5
  - High Availability for Virtual Appliances 1-5

---

## **CHAPTER 2**

### **Prerequisites 2-1**

- Prerequisites for Programmable Fabric Installation 2-1
  - Prerequisites for DCNM Open Virtual Appliance 2-1
  - Prerequisites for DCNM ISO Virtual Appliance 2-2
- Prerequisites for non-Programmable Fabric Installation 2-3

General Prerequisites for Installing the Cisco DCNM on Windows and Linux	2-3
Prerequisites for Windows Installer	2-16
Prerequisites for Linux RHEL Server	2-17
Prerequisites for non-Programmable Fabric Open Virtual Appliance	2-17
Prerequisites for non-Programmable Fabric ISO Virtual Appliance	2-17
Supported Software	2-17
Oracle Database for DCNM Servers	2-19
Oracle SQL*Plus Command-Line Tool	2-19
init.ora File	2-20
Backing up the Oracle Database	2-20
Preparing the Oracle Database	2-21
Database for HA environment	2-24
Database for Federation Setup	2-24
Antivirus exclusion	2-25
Configuring Certificates for Cisco DCNM	2-25
Using a self signed SSL Certificate	2-25
Using a SSL Certificate when certificate request is generated using OpenSSL	2-25
Using a SSL Certificate when certificate request is generated using Keytool	2-26
Configuring Secure Client Communications for Cisco DCNM Servers	2-28
Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance	2-28
Enabling SSL/HTTPS on Cisco DCNM in HA Environment on RHEL or Windows	2-29
Adding a CA signed SSL Certificate in Cisco DCNM	2-29
Server Ports	2-30

## CHAPTER 3

<b>Installation of DCNM</b>	<b>3-1</b>
Installation options	3-1
Fresh Installation	3-1
Upgrade	3-1
DCNM Programmable Fabric Installation	3-2
DCNM Open Virtual Appliance Installation in Programmable Fabric mode	3-2
DCNM ISO Virtual Appliance Installation	3-9
Setting the Timezone for Cisco DCNM Virtual Appliances	3-20
DCNM installation without Enhanced Fabric Management capabilities	3-20
Windows Installation	3-21
Linux RHEL Server Installation	3-21
Installing DCNM (Windows or Linux) in a Server Federation Environment	3-26
DCNM Open Virtual Appliance (OVA) Installation	3-27
ISO Virtual Appliance Installation on KVM	3-27
DCNM OVA in High Availability/Federation	3-28

DCNM Native HA Installation	3-30
Example for DCM Native HA Installation	3-32
Running Cisco DCM Behind a Firewall	3-34

---

**CHAPTER 4**
**Installation of DCM POAP Templates** 4-1

POAP Templates for Cisco DCM	4-1
Installing DCM POAP Templates	4-2
Installing Individual POAP Template from the Cisco DCM Web Client	4-2
Installing POAP Template from the Cisco DCM Web Client	4-3
Installing Templates Using Unzip and Restart	4-3

---

**CHAPTER 5**
**Upgrading Cisco DCM** 5-1

Retaining the CA Signed Certificate	5-2
Upgrading Cisco DCM Windows and Linux through GUI Installation	5-2
Upgrading Cisco DCM Windows and Linux through Silent Installation	5-3
Upgrading Cisco DCM Windows and Linux Federation through GUI Installation	5-3
Upgrading Cisco DCM Windows and Linux Federation through Silent Installation	5-4
Upgrading Cisco DCM Virtual Appliance with Local PostgreSQL Database	5-5
Upgrading Cisco DCM Virtual Appliance with External Oracle Database	5-6
Upgrading Cisco DCM appliances with Enhanced Fabric Management in HA Environment	5-7
Upgrading Cisco DCM appliances without Enhanced Fabric Management in HA Environment	5-9
Upgrading Cisco DCM Native HA appliances	5-11
Database Utility Scripts	5-13
Local PostgreSQL Database Utility Scripts for Backup and Restore	5-13
Remote Oracle Database Utility Scripts for Backup and Restore	5-13

---

**CHAPTER 6**
**Managing Applications After DCM Deployment** 6-1

Cisco DCM Applications	6-1
Application Details	6-2
Network Management	6-2
Network Services	6-3
Orchestration	6-6
Device Power On Auto Provisioning	6-7
Group Provisioning of Switches	6-8
Managing Applications	6-8
Verifying the Application Status after Deployment	6-9
Stopping, Starting, and Resetting Applications	6-9

XMPP User and Group Management	6-10
Change from Local Database to an External Database	6-11
Change password for Linux root user	6-12
Backing Up Cisco DCNM and Application Data	6-12
Backing Up Cisco DCNM	6-12
Backing Up Application Data	6-13
Using Scripted Backups for Backing Up Application Data	6-13
Collecting Log Files	6-13
Restoring Applications	6-14
Updating the SFTP Server Address for IPv6	6-15

**CHAPTER 7****Managing Applications in a High-Availability Environment 7-1**

Information About Application Level HA in the Cisco DCNM Open Virtual Appliance	7-1
Automatic Failover	7-2
Manually Triggered Failovers	7-2
Prerequisites for Cisco DCNM Open Virtual Appliance HA	7-2
Deploying Cisco DCNM OVAs	7-3
Creating an NFS/SCP Repository	7-3
Availability of Virtual IP Addresses	7-4
Installing an NTP Server	7-4
Application High Availability Details	7-4
Data Center Network Management	7-5
RabbitMQ	7-7
OpenLightweight Directory Access Protocol	7-8
DCHP HA	7-9
Repositories	7-10
Extensible Messaging and Presence Protocol (XMPP)	7-10
Configuring DCNM HA	7-11
Configuring the Active Peer	7-11
Configuring the Standby peer	7-13
Starting Applications in the Active Peer	7-15
Starting Applications in the Standby Peer	7-15
Starting DHCP in an HA Setup	7-15



## Preface

---

This preface describes the audience, organization, and conventions of the *Cisco DCNM Installation Guide, Release 10.4(1)*. It also provides information on how to obtain related documentation.

This preface includes the following topics:

- [Audience, page 1](#)
- [Document Conventions, page 1](#)
- [Related Documentation, page 2](#)
- [Documentation Feedback, page 4](#)
- [Obtain Documentation and Submit a Service Request, page 4](#)

## Audience

This publication is for experienced network administrators who plan to install Cisco Data Center Network Manager (DCNM) Open Virtual Appliance, DCNM ISO Virtual Appliance, DCNM Windows Installer, and DCNM Linux Installer to configure, monitor, and maintain applications. Cisco Fabric works with only certain Cisco Nexus products. Consult your Cisco Fabric documentation for specific information about products that work with Cisco Fabric.

## Document Conventions

This document uses the following conventions:



### Note

Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.



### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

In this document, the following shortened names are used:

- Cisco Data Center Network Manager is also referred to as Cisco DCNM.

- Cisco Data Center Network Manager Open Virtual Appliance is also referred to as Cisco DCNM Open Virtual Appliance.
- Cisco Dynamic Fabric Automation is also referred to as Cisco Fabric.

## Related Documentation

This section contains information about the documentation available for Cisco DCNM Open Virtual Appliance, and for the platforms that Cisco DCNM Open Virtual Appliance.

This section includes the following topics:

- [Cisco DCNM Documentation, page 2](#)
- [Cisco Nexus 1000V Series Switch Documentation, page 2](#)
- [Cisco Nexus 2000 Series Fabric Extender Documentation, page 3](#)
- [Cisco Nexus 3000 Series Switch Documentation, page 3](#)
- [Cisco Nexus 4000 Series Switch Documentation, page 3](#)
- [Cisco Nexus 5000 Series Switch Documentation, page 3](#)
- [Cisco Nexus 6000 Series Switch Documentation, page 3](#)
- [Cisco Nexus 7000 Series Switch Documentation, page 3](#)
- [Cisco Nexus 9000 Series Switch Documentation, page 3](#)
- [Cisco UCS Manager Documentation, page 4](#)
- [Cisco Dynamic Fabric Automation Documentation, page 3](#)

## Cisco DCNM Documentation

The Cisco DCNM documentation is available at the following URL:

[http://www.cisco.com/en/US/products/ps9369/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html)

The documentation set for Cisco DCNM includes the following documents:

### Release Notes

*Cisco Prime DCNM Release Notes, Release 10.4(1)*

### Cisco DCNM 10.4(1) Fundamentals Guide

*Cisco Prime DCNM Fundamentals Guide, Release 10.4(1)*

## Cisco Nexus 1000V Series Switch Documentation

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

[http://www.cisco.com/en/US/products/ps9902/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html)



## Cisco Nexus 2000 Series Fabric Extender Documentation

The Cisco Nexus 2000 Series Fabric Extender documentation is available at the following URL:  
[http://www.cisco.com/en/US/products/ps10110/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html)

## Cisco Nexus 3000 Series Switch Documentation

The Cisco Nexus 3000 Series switch documentation is available at the following URL:  
[http://www.cisco.com/en/US/products/ps11541/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html)

## Cisco Nexus 4000 Series Switch Documentation

The Cisco Nexus 4000 Series Switch documentation is available at the following URL:  
[http://www.cisco.com/en/US/products/ps10596/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html)

## Cisco Nexus 5000 Series Switch Documentation

The Cisco Nexus 5000 Series Switch documentation is available at the following URL:  
[http://www.cisco.com/en/US/products/ps9670/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html)

## Cisco Nexus 6000 Series Switch Documentation

Cisco Nexus 6000 Series Switch Documentation is available at the following URL:  
[http://www.cisco.com/en/US/products/ps12806/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html)

## Cisco Nexus 7000 Series Switch Documentation

The Cisco Nexus 7000 Series Switch documentation is available at the following URL:  
[http://www.cisco.com/en/US/products/ps9902/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html)

## Cisco Nexus 9000 Series Switch Documentation

The Cisco Nexus 9000 Series Switch documentation is available at the following URL:  
<http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html>

## Cisco Dynamic Fabric Automation Documentation

This Cisco Dynamic Fabric Automation documentation is available at the following URL:

[http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns945/dynamic\\_fabric\\_automation.html#~Products](http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns945/dynamic_fabric_automation.html#~Products)

## Cisco UCS Manager Documentation

The Cisco UCS Manager documentation is available at the following URL:

<http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/tsd-products-support-series-home.html>

## Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to: [dcnm-docfeedback@cisco.com](mailto:dcnm-docfeedback@cisco.com).

We appreciate your feedback.

## Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation (<https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed ([https://www.cisco.com/assets/cdc\\_content\\_elements/rss/whats\\_new/whatsnew\\_rss\\_feed.xml](https://www.cisco.com/assets/cdc_content_elements/rss/whats_new/whatsnew_rss_feed.xml)). The RSS feeds are a free service.



# Overview

---

Cisco Data Center Network Manager (DCNM) is a management system for Cisco NXOS-based Programmable Fabrics and 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. During the DCNM installation, you can choose install applications related to Programmable Fabric only for Programmable Fabric-mode installations. Cisco DCNM also includes Cisco DCNM-SAN client functionality.

From Cisco DCNM Release 10.0.x, DCNM-LAN thick client is not supported. However, most of salient features are migrated and the operations can be performed from the Cisco DCNM Web Client.

This chapters contains the following:

- [Introduction of Cisco DCNM, page 1-1](#)
- [Programmable Fabric and non-Programmable Fabric, page 1-2](#)
- [Installation Options, page 1-4](#)
- [Deployment Options, page 1-4](#)

## Introduction of Cisco DCNM

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. These in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fiber Channel Ping and Traceroute.

Cisco DCNM-SAN includes these management applications:

- [Cisco DCNM Server, page 1-2](#)
- [Cisco DCNM Web Client, page 1-2](#)
- [Cisco DCNM-SAN Client, page 1-2](#)
- [Device Manager, page 1-2](#)
- [Performance Manager, page 1-2](#)

## Cisco DCNM Server

The Cisco DCNM-SAN Server component must be started before running Cisco DCNM-SAN. On a Windows PC, 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 Client

The Cisco DCNM Web Client 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 client.

From Cisco DCNM Release 10.0(1), 10.1(1), or 10.1(2), the salient features of the DCNM LAN Client are migrated to be accessed and monitored via the Web Client. The Web Client now provides provisioning, monitoring of Ethernet interfaces for the Ethernet switches. It allows you to configure complex features such as vPC, VDC, and FabricPath and provides the topology representation of vPC, port channel, VLAN mappings, and FabricPath.

## 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

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 detailed 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 with any web browser.

# Programmable Fabric and non-Programmable Fabric

This section details basic overview on Programmable Fabric and non-Programmable Fabric.

- [Information about Programmable Fabric, page 1-3](#)
- [Information about non-Programmable Fabric, page 1-3](#)

## Information about Programmable Fabric

Cisco Programmable Fabric boosts network flexibility and efficiency. Programmable Fabric innovations simplify fabric management, optimize fabric infrastructure, and automate provisioning across physical and virtual environments.

Programmable Fabric offers the following functionalities:

### Optimized Fabric Infrastructure for Enhanced Efficiency and Scale

The optimized spine-leaf topology provides enhanced forwarding, distributed control plane, and integrated physical and virtual environments. The topologies enable any network anywhere, supporting transparent mobility for physical servers and virtual machines, including network extensibility. This increases the resiliency with smaller failure domains and multitenant scale.

### Simplified Fabric Management with Open APIs for Ease of Operations

Cisco Programmable Fabric allows centralized fabric management across both physical servers and virtual machines. It provides automated network provisioning, common point of fabric access, and host, network, and tenant visibility. Open APIs allow better integration with orchestration and automation tools, in addition to cloud platforms.

### Automated Provisioning for Greater Agility

With complete mobility across the fabric, the Programmable Fabric uses network automation and provisioning to simplify physical server and virtual machine deployments. The network administrator can define profile templates for both physical and virtual machine. When a server administrator provisions virtual machine and physical servers, instances of network policies are automatically created and applied to the network leaf switch. As virtual machines move across the fabric, the network policy is automatically applied to the leaf switch.

## Information about non-Programmable Fabric

Cisco DCNM in non-Programmable Fabric mode provisions and optimizes the overall uptime and reliability of the data center fabric. The following are the significance of Programmable Fabric mode:

- centralize fabric management to facilitate resource movement including adding and editing resources
- monitors SAN client, and detects performance degradation
- aids easy diagnosis and troubleshooting of data center outages
- simplifies operational management of virtualized data centers

# Installation Options

Cisco DCNM Release 10.4(1) offers four types of installers. The images are packaged with the Cisco DCNM installer, signature certificate, and signature verification script.

You must 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.

This section includes 4 options

- [DCNM Open Virtual Appliance for VMware, page 1-4](#)
- [DCNM ISO Virtual Appliance for VMware/KVM/UCS-C Series, page 1-4](#)
- [DCNM Installer for Windows \(64-bit\), page 1-4](#)
- [DCNM Installer for Linux \(64-bit\), page 1-4](#)

## DCNM Open Virtual Appliance for VMware

This installer is available as an Open Virtual Appliance file (.ova). The installer contains a pre-installed OS, DCNM and other applications needed for Programmable Fabric. This requires a vCenter Server and ESXi environment. This can be deployed either in Programmable Fabric or in non-Programmable Fabric modes. By default, it is deployed in Programmable Fabric mode.

## DCNM ISO Virtual Appliance for VMware/KVM/UCS-C Series

This installer is available as an ISO image (.iso). The installer is a bundle of OS, DCNM and other applications needed for Dynamic Fabric Automation. This can be deployed either on VMware ESXi 5.x or 6.5. environment or as a Kernel-based Virtual Machine on RHEL 6.x. This can be deployed either in Programmable Fabric or in non-Programmable Fabric modes. By default, it gets deployed in Programmable Fabric mode.

## DCNM Installer for Windows (64-bit)

This installer is available as an executable (.exe) and does not support Programmable Fabric features.

## DCNM Installer for Linux (64-bit)

This installer is available as a binary (.bin) and does not support Programmable Fabric features.

# Deployment Options

The installer available for Cisco DCNM Release 10.4(1) can be deployed in one of the below modes.

- [Standalone Server, page 1-5](#)
- [Standalone with external Oracle, page 1-5](#)
- [High Availability for Virtual Appliances, page 1-5](#)

## Standalone Server

All types of installers (.ova, .iso, .bin, .exe) 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 than 50 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 as described under section [Oracle Database for DCNM Servers](#), page 2-19.

## High Availability for Virtual Appliances

The DCNM Virtual appliances, both OVA and ISO, can be deployed in High Availability mode to have resilience in case of application or OS failures. For more information, see [Managing Applications in a High-Availability Environment](#).







## CHAPTER 2

# Prerequisites

---

This chapter details the general prerequisites for installing the Cisco DCNM.

- [Prerequisites for Programmable Fabric Installation, page 2-1](#)
- [Prerequisites for non-Programmable Fabric Installation, page 2-3](#)
- [Supported Software, page 2-18](#)
- [Oracle Database for DCNM Servers, page 2-19](#)
- [Configuring Certificates for Cisco DCNM, page 2-25](#)
- [Configuring Secure Client Communications for Cisco DCNM Servers, page 2-28](#)
- [Server Ports, page 2-30](#)

## Prerequisites for Programmable Fabric Installation

This sections details the various prerequisites, hardware and software requirements that you must equip with, before installing Programmable Fabric DCNM. This section contains prerequisites for the following:

- [Prerequisites for DCNM Open Virtual Appliance, page 2-1](#)
- [Prerequisites for DCNM ISO Virtual Appliance, page 2-2](#)

## Prerequisites for DCNM Open Virtual Appliance

Before you install the Cisco DCNM Open Virtual Appliance, you will need to meet following software and database requirements:

- Cisco DCNM Release 10.4(1) supports the running of the Cisco DCNM server on the following hypervisors:
  - VMware ESXi 6.0
  - VMware ESXi 6.5
  - VMware ESXi 6.7
  - VMware ESXi 6.7 U1
  - VMware vCenter 6.0
  - VMware vCenter 6.5

- VMware vCenter 6.7
- VMware vCenter 6.7 U1
- Two port groups on the ESXi host:
  - DCNM Management Network
  - Enhanced Fabric Management Network



**Note** The DCNM Open Virtual Appliance cannot be deployed by connecting the vSphere client directly to the ESXi server.

- Determine the number of switches in your Cisco Programmable Fabric that will be managed by the Cisco DCNM Open Virtual Appliance.
- Ensure that no anti-virus software (such as McAfee) is running on the host where the VMware vCenter web client is launched for the DCNM OVA installation. If the anti-virus software is running, the DCNM installation might fail.



**Note** Once you start using the PostgreSQL database that is built in to the Cisco DCNM Open Virtual Appliance, you cannot migrate the data to an Oracle database.



**Note** On vCenter Server 6.5 web client, when an OVA VM is deployed, enable the administrator role and privileges before clicking the Power-On button.



**Note** To accommodate for HA application functions, additional prerequisites are required.



**Note** The DCNM Open Virtual Appliance is compatible to be deployed in ESXi 5.5 host as well. For deploying in the ESXi 5.5 host, VMware vSphere Client application is mandatory.

## Prerequisites for DCNM ISO Virtual Appliance

You have to setup the host or the hypervisor before you install the Cisco DCNM ISO Virtual Appliance. Based on the requirement, setup the host.

You can setup one of the following hosts to install the DCNM ISO Virtual Appliance.

- [VMware ESXi, page 2-2](#)
- [Kernel-based Virtual Machine \(KVM\), page 2-3](#)
- Cisco UCS C-Series bare metal host

## VMware ESXi

The host machine is installed with ESXi and two port groups are created—one for EFM network and the other for DCNM Management network.

## Kernel-based Virtual Machine (KVM)

The host machine is installed with Red Hat Enterprise Linux 6.x with KVM libraries and Graphical User Interface (GUI) access. The GUI allows to access the Virtual Machine Manager, to deploy and manage the Cisco DCNM Virtual Appliances. Two networks are created—EFM network and DCNM Management network. Typically, the DCNM management network is bridged to gain access from other subnets. Refer the KVM documentation on how to create different types of networks.

**Note**

KVM on other platforms like CentOS/Ubuntu will not be supported as it increases the compatibility matrix.

## Prerequisites for non-Programmable Fabric Installation

This sections details the various prerequisites, hardware and software requirements that you must equip with, before installing Cisco non-Programmable Fabric DCNM. This section contains prerequisites for the following:

- [General Prerequisites for Installing the Cisco DCNM on Windows and Linux, page 2-3](#)
- [Prerequisites for Windows Installer, page 2-16](#)
- [Prerequisites for Linux RHEL Server, page 2-17](#)
- [Prerequisites for non-Programmable Fabric Open Virtual Appliance, page 2-17](#)
- [Prerequisites for non-Programmable Fabric ISO Virtual Appliance, page 2-17](#)

## General Prerequisites for Installing the Cisco DCNM on Windows and Linux

This section includes the following topics:

- [Before you begin, page 2-3](#)
- [Initial Setup Routine, page 2-5](#)
- [Preparing to Configure the Switch, page 2-5](#)
- [Default Login, page 2-6](#)
- [Setup Options, page 2-6](#)
- [Assigning Setup Information, page 2-7](#)
- [Configuring Out-of-Band Management, page 2-7](#)
- [Configuring In-Band Management, page 2-11](#)
- [Using the setup Command, page 2-14](#)
- [Starting a Switch in the Cisco MDS 9000 Family, page 2-15](#)
- [Accessing the Switch, page 2-15](#)

### 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 DB.
- Users installing Cisco DCNM must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. These ports are used by Cisco DCNM Server and the PostgreSQL database: 1098, 1099, 4444, 4445, 8009, 8083, 8090, 8092, 8093, 514, 5432.
- 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 1.7(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**

The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (\_), and hyphen (-).

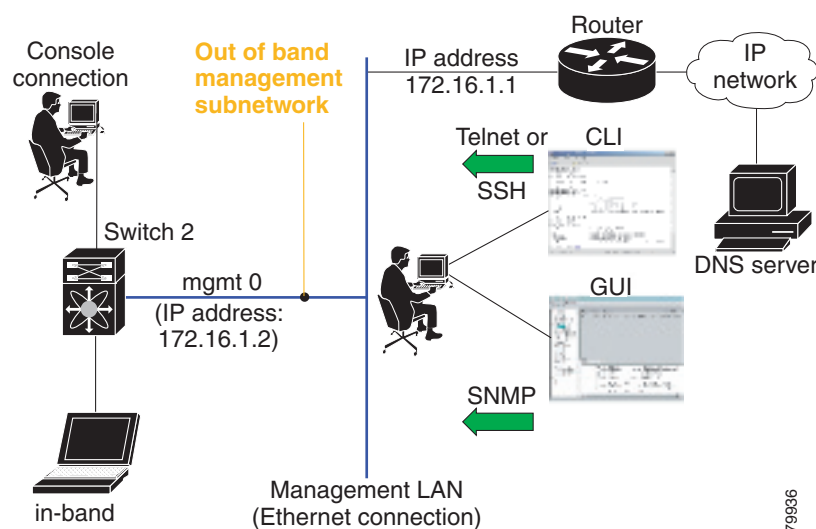
## Setup Options

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 2-1](#)).

**Note**

Some concepts such as out-of-band management and in-band management are briefly explained here. These concepts are explained in more detail in subsequent chapters.

**Figure 2-1 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 [Step 11c](#) and [Step 11d](#) in the following procedure.

### DETAILED STEPS

**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\*1kjh17**

**Note**

The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (\_), and hyphen (-).

b. Confirm the administrator password.

Confirm the password for admin: **2008asdf\*1kjh17**

**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*

The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (\_), and hyphen (-).

**b.** Enter the user password.

Enter the password for user\_name: *user-password*

**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 [Step 11c](#).

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 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 **Yes** in both [Step 9c](#) and [Step 9d](#) in the following procedure.

## DETAILED STEPS

**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\*1kj18**

**Tip**

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive. The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (\_), and hyphen (-).

**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 additional 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 would like to generate.

Type the SSH key you would like to generate (dsa/rsa/rsal)? **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 just 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.

### DETAILED STEPS

- 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.
- See the *Cisco MDS 9000 Family Hardware Installation Guide* (for the required product) for more information.
-  **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:

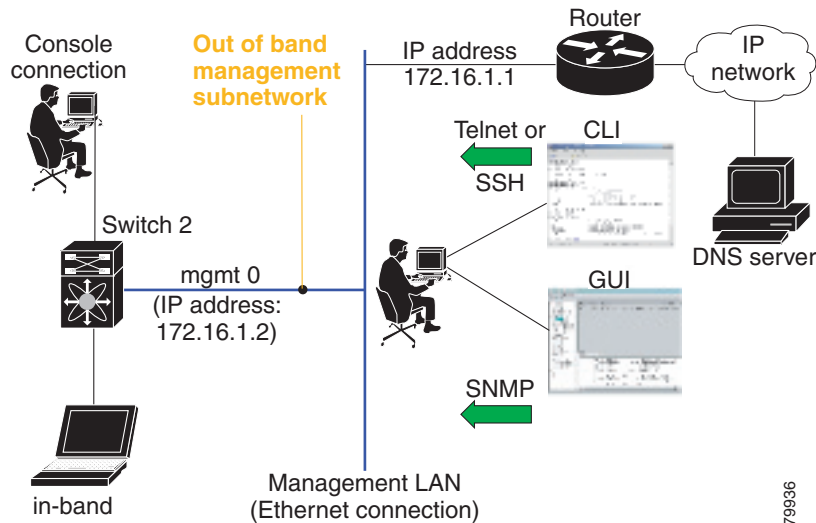
- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet 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 2-2](#)):

- 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 2-2** *Switch Access Options*



## Prerequisites for Windows Installer

- During the initial installation, disable all security and anti virus 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 host name 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 should 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 very important if the default PostgreSQL database is used with Cisco DCNM, because this database requires the local console for all installations and upgrades.
- Before installing Cisco DCNM on a Windows Vista or Windows 2008 server system, turn the User Account Control (UAC) off. To turn off UAC, choose **Start > Control Panel > User Accounts > Turn User Account Control on or off**, clear the **Use User Account Control (UAC) to help protect your computer** check box, and then click **OK**. Click **Restart Now** to apply the change.
- 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, you need to give it the permission to continue). Check the **Telnet Client** check box and then click **OK**.



- You can run CiscoWorks on the same PC as Cisco DCNM even though 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 required for CiscoWorks. Both versions of Java can coexist on your PC.

## Prerequisites for Linux RHEL Server

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/8.4/interactive/kernel-resources.html>

The server system must be registered with the DNS servers. No other programs are running on the server. Ensure that you select English as the preferred language during RHEL installation.

## 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/wiki/Running\\_%26\\_Installing\\_PostgreSQL\\_On\\_Native\\_Windows#Antivirus\\_software](https://wiki.postgresql.org/wiki/Running_%26_Installing_PostgreSQL_On_Native_Windows#Antivirus_software).



### 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.

This recommendation is also applicable to DCNM installations in an ISO/OVA format.

## Prerequisites for non-Programmable Fabric Open Virtual Appliance

For information on prerequisites to install DCNM Open Virtual Appliance, refer to [Prerequisites for DCNM Open Virtual Appliance, page 2-1](#).

## Prerequisites for non-Programmable Fabric ISO Virtual Appliance

For information on prerequisites to install ISO Virtual Appliance, refer to [Prerequisites for DCNM ISO Virtual Appliance, page 2-2](#).

# Supported Software

**Note**

For the latest information on supported software, see the *Cisco DCNM Release Notes, Release 10.4(1)*.

The following are the supported software for Cisco DCNM 10.4(1):

## Supported Software for DCNM Windows/Linux Installers

- Java Requirements
  - Cisco DCNM Server is distributed with Java JRE 1.8.0\_101. The DCNM installer installs JRE 1.8.0\_101 to the following directory: **DCNM\_root\_directory/java/jre1.8**
  - Cisco DCNM Client has been validated with Java versions JRE 1.8.0\_101.
- Operating System
  - Microsoft Windows 2008 R2 SP2 (64-bit only)
  - Microsoft Windows 2012 R2
  - Red Hat Enterprise Linux Release 6.6 and 7.0
  - Red Hat Enterprise Linux Release 7 (64-bit)

## Supported Software for DCNM Virtual Appliances (OVA/ISO)

- Databases:
  - Oracle 11g Express (XE), Standard, and Enterprise Editions, and Oracle 11g Real Application Clusters (RAC)
  - PostgreSQL 9.4.5
  - Oracle 12c Enterprise Edition (Conventional)–Non-pluggable Installation

**Note**

Cisco DCNM Release 10.4(1) does not support Oracle 12c pluggable database version installation.

- Oracle 12c RAC–Non-pluggable 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**

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

## Supported Security for all DCNM Virtual Appliances (Windows/Linux/OVA/ISO)

- Security
  - Cisco ACS 3.1 and 4.0
  - PIX Firewall
  - IP Tables
  - SSH v2
  - Global Enforce SNMP Privacy Encryption
  - HTTPS

## 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. For instructions, see [Change from Local Database to an External Database, page 6-11](#).

**Note**

Cisco DCNM is configured with AL32UTF8 character set.

This section contains the following:

- [Oracle SQL\\*Plus Command-Line Tool, page 2-20](#)
- [init.ora File, page 2-20](#)
- [Backing up the Oracle Database, page 2-20](#)
- [Preparing the Oracle Database, page 2-21](#)
- [Database for HA environment, page 2-24](#)
- [Database for Federation Setup, page 2-25](#)
- [Antivirus exclusion, page 2-25](#)

**Note**

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.

## Oracle SQL\*Plus 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 [Table 2-1](#).

**Table 2-1** Name and Default Location of init.ora File

Oracle Version	Operating System	Content of init.ora File
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dfs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dfs/initORCL.ora

The init.ora file should contain only one line, which is the full path of the server parameter file, as shown in [Table 2-2](#).

**Table 2-2** Content of init.ora File

Oracle Version	Operating System	Content of init.ora File
11g	Microsoft Windows	SPFILE='C:\oracle\app\oracle\product\11.1.0\server\dfs\spfileXE.ora
	Linux	SPFILE='/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dfs/spfileXE.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



**Note** Replace /usr/lib/oracle with the Oracle installation path.

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



**Note** Replace C:\oraclexe with the Oracle installation path.

## Preparing the Oracle Database

You can prepare an Oracle database.

### DETAILED STEPS

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Increase the number of sessions and processes to 150 each. For more information, see the <a href="#">“Increasing the Number of Sessions and Processes to 150 Each”</a> section on page 2-22. |
| <b>Step 2</b> | Increase the number of open cursors to 1000. For more information, see the <a href="#">“Increasing the Number of Open Cursors to 1000”</a> section on page 2-23.                             |
- 

This section includes the following:

- [Logging Into Oracle, page 2-21](#)
- [Increasing the SYSTEM Tablespace, page 2-22](#)
- [Increasing the Number of Sessions and Processes to 150 Each, page 2-22](#)
- [Increasing the Number of Open Cursors to 1000, page 2-23](#)
- [Creating an Oracle DB User using the Command Prompt, page 2-24](#)
- [Connecting to an Oracle RAC with SCAN Feature Type DB, page 2-24](#)
- [Adding a CA signed SSL Certificate in Cisco DCNM, page 2-29](#)

## 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.

### DETAILED STEPS

- 
- |               |                              |
|---------------|------------------------------|
| <b>Step 1</b> | 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:

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

---

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.

### DETAILED STEPS

---

**Step 1** Use the SQL\*Plus command-line tool to log in to the Oracle database. For more information, see the [“Oracle SQL\\*Plus Command-Line Tool” section on page 2-20](#).

**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 [Step 2](#).

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.

## DETAILED STEPS

- 
- 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” section on page 2-20](#).
- Step 2** Use the SQL\*Plus command-line tool to log in to the Oracle database. For more information, see the [“Oracle SQL\\*Plus Command-Line Tool” section on page 2-20](#).
- 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” section on page 2-20](#).
- Step 5** Set the number of sessions to 150 by entering the following command:
- ```
alter system set sessions = 150 scope=spfile;
```
- Step 6** Set the number of processes to 150 by entering the following command:
- ```
alter system set processes = 150 scope=spfile;
```
- Step 7** Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.
- Step 8** Start up the system by entering the **startup** command.
- Step 9** Verify that the number of sessions and processes is changed to 150 by entering the following command:
- ```
show parameter sessions
```
- Step 10** Exit by entering the **exit** command.
- 

## Increasing the Number of Open Cursors to 1000

You can increase the number of open cursors to 1000.

## DETAILED STEPS

- 
- 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” section on page 2-20](#).
- Step 2** Use the SQL\*Plus command-line tool to log in to the Oracle database. For more information, see the [“Oracle SQL\\*Plus Command-Line Tool” section on page 2-20](#).
- 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](#)” section on page 2-20.

**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 HA environment

If you need High Availability (HA) for DCNM database, utilize the Oracle HA solutions.

**Note**

Ensure that the NTP server is synchronized between the DCNM active and standby peers. This is essential for the functioning of DCNM applications in HA environment.

---



## 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.

## 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 Oracle database, exclude the directory that you have selected during Oracle installation.

## Configuring Certificates for Cisco DCNM

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

This section contains the following topics:



- [Using a self signed SSL Certificate, page 2-25](#)
- [Using a SSL Certificate when certificate request is generated using OpenSSL, page 2-26](#)
- [Using a SSL Certificate when certificate request is generated using Keytool, page 2-27](#)

## Using a self signed SSL Certificate

- 
- |               |                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From command prompt, navigate to <b>&lt;DCNM install root&gt;/dcm/java/jre1.8/bin/</b> .                                                                                                                                                                                                                     |
| <b>Step 2</b> | Rename the keystore located at<br><b>&lt;DCNM_install_root&gt;\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks</b><br>to<br><b>&lt;DCNM_install_root&gt;\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old</b>                                                               |
| <b>Step 3</b> | Generate a self signed certificate using following command<br><pre>keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore &lt;DCNM_install_root&gt;\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048</pre> |
| <b>Step 4</b> | Stop the DCNM services, or DCNM application by using the <b>appmgr stop dcnm</b> command.                                                                                                                                                                                                                    |
| <b>Step 5</b> | Start the DCNM services, or the DCNM applications in the server by using the <b>appmgr start dcnm</b> command.                                                                                                                                                                                               |
-

## Using a SSL Certificate when certificate request is generated using OpenSSL

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

- 
- Step 1** From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.8/bin/**.
- Step 2** Rename the keystore located at:  
**<DCNM\_install\_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks**  
 to  
**<DCNM\_install\_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks.old**
- Step 3** Generate the RSA private key using OpenSSL.  
**openssl genrsa -out dcnm.key 2048**
- Step 4** Generate a certificate-signing request (CSR) by using following command:  
**openssl req -new -key dcnm.key -sha256 -out dcnm.csr**
- Step 5** 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 provides the PKCS 7 format, go to [Step 6](#) to convert it to PEM format. If CA provides the PEM format, go to [Step 7](#).
- Step 6** Convert the PKCS 7 certificate chain to X509 certificate chain.  
**openssl pkcs7 -print\_certs -in cert-chain.p7b -out cert-chain.pem**
- Step 7** 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 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 8** 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/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks -deststoretype JKS -name 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 9** Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.
- Step 10** Start the DCNM services, or the DCNM applications in the server by using the **appmgr start dcnm** command.
-

## Using a SSL Certificate when certificate request is generated using Keytool

- Step 1** From command prompt, navigate to the appropriate folder:
- For Linux/CentOS DCNM installation, use the following path:  
`<DCNM install root>/dcm/java/jre1.8/bin/`
  - For Windows DCNM sever installation, use the following path:  
`<DCNM install root>\dcm\java\jre1.8\bin\`
- Step 2** Rename the keystore.
- For Linux/CentOS DCNM installation, rename the keystore located at:  
`<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks`  
to  
`<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks.old`
  - For Windows DCNM sever installation, rename the keystore located at:  
`<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks`  
to  
`<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old`
- Step 3** Generate the public-private key pair in DCNM keystore by using the following command:
- For Linux/Centos environment use the following command:  
`./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore  
<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks  
-storepass fmserver_1_2_3 -validity 360 -keysize 2048`
  - For Windows DCNM sever installation, use the following command:  
`keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore  
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks  
-storepass fmserver_1_2_3 -validity 360 -keysize 2048`
- Step 4** Generate the certificate-signing request (CSR) from the public key generated in [Step 6](#).
- For Linux/Centos environment use the following command:  
`./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install  
root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks" -storepass  
fmserver_1_2_3`
  - For Windows DCNM sever installation, use the following command:  
`keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install  
root>\dcm\jboss-as-7.2.0.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 5** 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 6](#) to convert it to PEM format. If CA provided PEM format, then go to [Step 7](#).

**Step 6** 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 7** Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

- For Linux/Centos environment use the following command:

```
./keytool -importcert -trustcacerts -file cert-chain.pem -keystore  
<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks  
-storepass fmserver_1_2_3 -alias sme
```

- For Windows DCNM sever installation, use the following command:

```
keytool -importcert -trustcacerts -file cert-chain.pem -keystore  
<DCNM_install_root>\dcm\jboss-as-7.2.0.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 8** Stop the DCNM application by using the **appmgr stop dcnm** command.

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

## Configuring 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 HA Environment on Virtual Appliance, page 2-29](#)
- [Enabling SSL/HTTPS on Cisco DCNM in HA Environment on RHEL or Windows, page 2-29](#)
- [Adding a CA signed SSL Certificate in Cisco DCNM, page 2-29](#)

## Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance

To enable SSL/HTTPS on a Virtual Appliance for Cisco DCNM in HA mode, perform the following:

**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 by using the procedure [Configuring Certificates for Cisco DCNM, page 2-25](#). Ensure that the certificate is signed by the signing certificate chain which is common for both the servers.

**Step 2** On the secondary server, locate the keystore.

**Step 3** Rename the keystore located at

```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration
\fmserver.jks
```

to

```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration
\fmserver.jks.old
```

**Step 4** Copy the file “fmserver.jks” generated in primary server to secondary server into folders

```
<dcnm-home> /dcm/jboss-as-7.2.0.Final/standalone/configuration/
<dcnm-home>/dcm/fm/conf/cert/
```

## Enabling SSL/HTTPS on Cisco DCNM in HA Environment on RHEL or Windows

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

**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 by using the procedure [Configuring Certificates for Cisco DCNM, page 2-25](#). 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.

## Adding a CA signed SSL Certificate in Cisco DCNM



**Note** This section applies to both all the Cisco DCNM installers.

To add CA signed SSL certificate for DCNM Windows or RHEL Setup, perform the following:

- 
- Step 1** From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.8/bin/**.
- Step 2** Rename the keystore located at
- ```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks
```
- to
- ```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old
```
- Step 3** Generate the certificate-signing request (CSR) from the public key generated in [Step 2](#).
- ```
keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3
```
- Step 4** Submit the CSR to certificate signing authority to digitally sign it.
- CA provides the certificate and signing certificate in as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file.
- If CA provided PKCS 7 format go to [Step 5](#) to convert it to PEM format. If CA provided PEM format then go to [Step 6](#).
- Step 5** Convert the PKCS 7 certificate chain to X509 certificate chain using openssl
- ```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```
- Step 6** 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\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -alias sme
```
- Step 7** Stop the DCNM application by using the **appmgr stop dcnm** command.
- Step 8** Start the applications in the server by using the **appmgr start dcnm** command.



**Note**

You must configure the Cisco DCNM Web Port again, after adding a ca signed SSL certificate. For more information, see [Reconfigure DCNM to use an external Oracle database, page 6-11](#).

---

## Server Ports

Cisco DCNM is installed with default port set. If you need to change the default port values due to security considerations, update the port details in **installer.properties** file and install DCNM in the silent installation mode. Ensure that you set the **RESOLVE\_PORT\_CONFLICTS** to **FALSE**. This ensures that the DCNM installer does not auto-resolve ports when the specified ports are unavailable.

For Windows PCs running Cisco DCNM-SAN, Device Manager, behind a firewall, certain ports need to be available. For more information, see [Running Cisco DCNM Behind a Firewall, page 3-34](#).

**Note**

This is of significance to the users deploying DCNM on a Windows or Linux system, and not applicable to the Open Virtual Appliance. This is not applicable to the Open Virtual Appliance (OVA), as the operating system controls the ports set.

Table 2-3 lists the default ports that services on a Cisco DCNM-SAN server listen to for client communications. One port is not configurable. You can configure the other ports. The server installer can resolve port conflicts automatically.

**Table 2-3** *Default TCP Ports for Client Communications*

Service Name	Default Port for SAN	Configurable?
RMI	1198	During installation
Naming Service	9099	During installation
SSL	3943	During installation
EJB	3973	During installation
Server Bind 1	5644	During installation
Server Bind 2	5446	During installation
JMS	5457	During installation
Syslog (system message) Receiver	5545	During installation
AJP Connector	9009	During installation
Web Server	80	During installation
Web Services	9093	During installation
RMI Object	244444	During installation
UIL2	—	During installation

Table 2-4 displays the default server ports with DCNM installed in HTTPS mode.

**Table 2-4** *Default Server Ports*

Service Name	Default Port
SAN Server Bind	5644
Web Services Port	8083
SAN invoker bind port	5446
DCNM Server	1099
EJB SSL	3843
SAN Management Native	9999
SAN JMS	5457
RMI Object	14444

**Table 2-4**      **Default Server Ports (continued)**

<b>Service Name</b>	<b>Default Port</b>
EJB	3873
DCNM Server Bind	4445
DCNM Web Port	8443
Invoker Bind	4446
SAN Management HTTP Port	9990
SAN AJP Connector	9009
RMI	1098
SAN Syslog	5545
AJP Connector	8009
SAN Management HTTP Port	9443
SAN Server	4447
SAN Web Services	9093
SAN RMI Object	24444
SAN EJB	3973
SAN Web	443
JMS Port	4457
SAN RMI	1198
SAN EJB SSL	3943
Syslog	5445
External Oracle Database	1521





## CHAPTER 3

# Installation of DCNM

---

Before upgrading or uninstalling Cisco DCNM or Device Manager, make sure that any instances of these applications have been shut down.

This chapter contains the following sections:

- [Installation options](#)
- [DCNM Programmable Fabric Installation](#)
- [DCNM installation without Enhanced Fabric Management capabilities](#)
- [DCNM Native HA Installation](#)
- [Running Cisco DCNM Behind a Firewall](#)

## Installation options

### Fresh Installation

- For Windows and Linux installers, the installer installs Cisco DCNM-SAN and Cisco SMI-S agent on your system.
- For Virtual Appliances (OVA/ISO), the installer installs the Operating system and Cisco DCNM components.



#### Note

When the ISO/OVA appliance is deployed in DFA mode, the Cisco SMI-S component will not start by default. However, the component can be managed using the following commands:

**appmgr start** or **stop dcnm-smis**

The **appmgr start** or the **stop dcnm** command will start or stop the Web component.

While for non-DFA deployments (ISO/OVA/.exe/.bin), all services will be started by default.

For more information about the application management, see [Managing Applications, page 6-8](#).

---

### Upgrade

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

- For Virtual Appliances (OVA/ISO), you must execute the **appmgr** command to upgrade. For more information, see [“Upgrading Cisco DCNM”](#).

**Note**

The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for Linux/Windows/OVA/ISO platforms are: SPACE, double quotes, single quotes, &, \$, %, ^, =, <, >, :, . Do not use the following characters in your password: "&\$%'" and <SPACE>.

This chapter describes how to install Cisco Data Center Network Manager (DCNM) and includes the following sections:

- [DCNM Programmable Fabric Installation, page 3-2](#)
- [DCNM installation without Enhanced Fabric Management capabilities, page 3-20](#)
- [Running Cisco DCNM Behind a Firewall, page 3-34](#)

## DCNM Programmable Fabric Installation

This section contains the following:

- [DCNM Open Virtual Appliance Installation in Programmable Fabric mode, page 3-2](#)
- [DCNM ISO Virtual Appliance Installation, page 3-9](#)
- [Configuring Media Controller for IP Fabric, page 3-28](#)
- [DCNM OVA in High Availability/Federation, page 3-28](#)

**Note**

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-20](#).

## DCNM Open Virtual Appliance Installation in Programmable Fabric mode

For information about the Prerequisites before you begin the installation, see [Prerequisites for DCNM Open Virtual Appliance](#) section.

Three steps are required to install the DCNM Open Virtual Appliance:

1. Verify Prerequisites. You must install various VMware components before you install the Open Virtual Appliance. See [Verifying Prerequisites, page 3-3](#).
2. Download the Open Virtual Appliance file. You can access the required dcnm.ova file from [www.cisco.com](http://www.cisco.com). See [Downloading the Open Virtual Appliance File, page 3-3](#).
3. Deploy the Open Virtual Appliance as an OVF template. A step-by-step template in the vSphere Client guides you through this process. After you have completed the step-by-step template, you can review all of the information that you provided, make any corrections, and then deploy the Open Virtual Appliance. See [Deploying the Open Virtual Appliance as an OVF Template, page 3-3](#).

**Note**

If you are using a high-availability (HA) environment for applications that are bundled within the DCNM ISO Virtual Appliance, you must download the ISO and deploy twice, once for Active and once for Host-Standby. For more information, see [Chapter 7, “Managing Applications in a High-Availability Environment”](#).

**Verifying Prerequisites**

For more information, see [Prerequisites for DCNM Open Virtual Appliance](#) section.

**Downloading the Open Virtual Appliance File**

The first step to installing the Open Virtual Appliance is to download the dcnm.ova file. You will point to that dcnm.ova file on your computer when deploying the OVF template.

**Note**

If you plan to use HA application functions, you must deploy the dcnm.ova file twice.

**DETAILED STEPS**

- 
- Step 1** Go to the following site: <http://software.cisco.com/download/>.
- Step 2** In the **Product/Technology Support** section, choose **Download Software**.
- Step 3** In the **Select a Product** section, navigate to the DCNM software by choosing **Products > Switches > Data Center Switches > Data Center Network Management > Cisco Data Center Network Manager**.
- A list of the latest release software for Cisco DCNM is available for download.
- Step 4** In the **Latest Releases** list, choose **10.4(1)**.
- Step 5** Locate the DCNM Open Virtual Appliance Installer and click the **Download** button.
- Step 6** Save the dcnm.ova file to your computer in a place that will be easy to find when you start to deploy the OVF template.
- 

**Deploying the Open Virtual Appliance as an OVF Template**

After you download the Open Virtual Appliance file, you will deploy the OVF template from the vSphere Client application or the vCenter Server 6.5.

**DETAILED STEPS for Host ESXi 6.5**

- 
- Step 1** Log in to vCenter Server 6.5:
- Open the vCenter Server 6.5 application.
  - Connect to the vCenter Server with your vCenter user credentials.

**Note**

ESXi 6.5 host should have been added to the vCenter Server 6.5 application.

- Step 2** Use the vSphere Server application to access the OVF template:
- Choose **Home > Inventory > Hosts and Clusters**
  - Choose the host on which the OVF template will be deployed.
  - Right click on **Host > Deploy OVF Template** to open the Deploy OVF Template window.
- Step 3** Choose the Source location:
- Click the **Browse** button.
  - Locate the dcnm.ova file that you downloaded to your computer and click **Next**.
- Step 4** Specify the name and location of the Cisco DCNM Open Virtual Appliance.
- In the **Name** box, enter a name for the virtual appliance. This name is not the hostname, but the name of the virtual appliance hardware and is specific to the vSphere infrastructure. The name can contain up to 80 alphanumeric characters and must be unique within the Inventory folder.
  - In the Data center Selection tree, choose the Data Center under the ESXi 6.5 host.
  - Click **Next**.
- Step 5** Choose the resource where you want to run the deployed template.
- Choose the Host server or Resource pool.
  - Click **Next**.
- Step 6** Review the OVF Template Details and click **Next**.

Some of the details about the Cisco DCNM virtual appliance include:

- Version number
- Download size
- Size on disk:
  - Thin provision for the amount of disk space consumed by the virtual appliance immediately after deployment. It is the minimum amount of disk space needed to deploy the virtual appliance.
  - Thick provision for the maximum amount of disk space the virtual appliance can consume.

**Step 7** Read and accept the End User License Agreement and click **Next**.

**Step 8** Choose the deployment configuration:

- Choose Small** to configure the virtual machine with two vCPUs and 8G RAM.
- Choose Large** to configure the virtual machine with four vCPUs and 12G RAM.
- Click **Next**.



**Note**

We recommend that you use a Large deployment configuration when you are managing more than 50 devices (and up to the upper limit of the Cisco Programmable Fabric) to leverage better RAM, heap memory, and CPUs.

For setups that could grow, choose **Large**.

Choose **Small** for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time.

**Step 9** Choose the disk format and the destination storage for the virtual machine file, and click **Next**.

- Disk formats - Choose one of the thick provision types if you have enough storage capacity as required by the virtual appliance and want to set a specific allocation of space for the virtual disks:
  - **Thick Provision Lazy Zeroed:** The space that is required for the virtual disk is allocated when the virtual disk is created. The data that remains on the physical device is not erased when the virtual disk is created but is zeroed out on demand at a later time on first write from the virtual disk.
  - **Thick Provision Eager Zeroed:** The space that is required for the virtual disk is allocated when the virtual disk is created. Unlike the Lazy Zeroed option, the data that remains on the physical device is erased when the virtual disk is created.
- Choose **Thin Provision** if you have less than 100 GB of disk space available. The initial disk consumption will be 3GB and will increase as the size of the database increases with the number of devices being managed.

**Step 10** Choose your network mapping.

- The dcnm-mgmt network provides connectivity (ssh, scp, http, https) to the Cisco DCNM Open Virtual Appliance. In the **Destination Network** column, associate the network mapping with the port group that corresponds to the subnet that is associated with the Cisco DCNM management network.
- Map the enhanced-fabric-mgmt network to the port group that connects to the management network of switches.



**Note**

If you are deploying more than one DCNM Open Virtual Appliance for HA functionality, you must meet the following criteria:

- Both OVAs should have their management access (eth0) and enhanced fabric management (eth1) interfaces in the same subnet.
- Both OVAs should be deployed with the same administrative password. This is to ensure that both OVAs are duplicates of each other for application access.  
Do not use the following characters in your password: "&\$%" and <SPACE>.

**Step 11** Click **Next**.

**Step 12** Choose the Cisco DCNM Open Virtual Appliance Properties.

- The **Application Management** check box is selected by default to install the SAN management functionalities.
- In the **Management Properties** section, enter a password in the **Enter Password** and **Confirm Password** boxes to establish the password that will be used to connect all applications in the DCNM Open Virtual Appliance.



**Note**

The password can contain a combination of alphabets, numeric, and special characters. The only characters that are not allowed in the DCNM password for Linux/Windows/OVA/ISO platforms are: <SPACE>&\$% single and double quotes. And the rest are all allowed: ! @ # ^ \* - + = ; : , . / ~ ` \ | < > (). Do not use the following characters in your password: "&\$%" and <SPACE>.

If you do not comply with these password requirements, you can continue with the DCNM Open Virtual Appliance deployment, but subsequently may not be able to log in to other applications like DCNM.

- In the **DCNM Network** section, complete each of the required fields:

- **Hostname** (should be a fully qualified domain name, otherwise you may encounter issues when using the XMPP application after deployment)
  - **IP Address** (for the outside management address for DCNM)
  - **Subnet Mask**
  - **Default Gateway**
  - **DNS IP**
- d. In the **Enhanced Fabric Management** section, complete each of the required fields:
- **IP Address** (for the inside fabric management address or OOB Management Network)
  - **Subnet mask**
  - **DNS IP**
  - **IPv6 Address (Optional)**

**Note**

If the parameters in this section are not provided, features such as POAP and auto-configuration will not be functional.

**Step 13** Click **Next**

**Step 14** Review each of the deployment settings that you have established. Press the **Back** button to go to any settings if you want to change them.

After you have reviewed each of the deployment settings in the OVF template, Click **Finish**.

**Step 15** Power On button in the deployed VM is not enabled automatically. You need to set the Admin permissions on the VM to be able to power on the VM.

- a. Right click on **VM > Add Permission**.
- b. Specify the user with Admin Privileges to add.
- c. Right Click on **VM > Power > Power On**.

**Note**

Unlike in ESXi 5.5, the option to Auto power on after the deployment is complete, is not available. The VM should be powered on manually, and this needs Admin privileges to be set for each VM.

## Deploying Virtual Machines

**Step 1** Check the **Power on after deployment** check box.

**Step 2** Click the **Finish** button.

A Deploying DCNM\_OVA window appears and the Open Virtual Appliance deployment starts and requires some time to complete.

**Note**

The time for the DCNM Open Virtual Appliance deployment could take 5 to 6 minutes (or more) depending on the network latency.

After the Open Virtual Appliance is deployed, a Deployment Completed Successfully message appears.

**Step 3** On the **Summary** tab in the vSphere Client, review the information about the VM and make note of the IP address.

- Step 4** Check the console of the VM in the vSphere Client for the login prompt. Once the login prompt appears, log in with root credentials and use the **appmgr status all** command to check the status of the applications. After all applications are up and running, go to the next step.



**Note** For more information about verifying application status see the [Verifying the Application Status after Deployment, page 6-9](#).

- Step 5** Log in to the Cisco DCNM web UI:
- Put the IP address in your browser.  
The Cisco Data Center Network Manager window is displayed.
  - In the **User Name** field, enter **admin**.
  - In the **Password** field, enter the administrative password given to you during the DCNM Open Virtual Appliance deployment.



**Note** If you are deploying multiple OVAs for HA functions, you should deploy both the OVAs with the same administrative password. This action ensures that both OVAs are duplicates of each other for application access.

You are ready to begin POAP configuration and Device Discovery.



**Note** See the *Cisco DCNM Fundamentals Guide* for configuration information.

## Configuring the Oracle Database for DCNM Virtual Appliances

Cisco DCNM, Release 10.4(1) contains a built-in PostgreSQL database that supports full-scale deployments with High-Availability. However, you can optionally use the Oracle Database for backend storage.

### DETAILED STEPS

- Step 1** Prepare the Oracle database.  
For more information, see [Preparing the Oracle Database, page 2-21](#).



**Note** If you are configuring the Oracle database for an HA environment, only [Step 1](#) is required. If you are configuring the Oracle database for a standalone DCNM, continue with the following steps in the procedure.

- Step 2** Get the JDBC database URL, database username, and database password.
- Step 3** Stop the Cisco DCNM application in the Open Virtual Appliance by entering the following command:  
**appmgr stop dcnm**
- Step 4** Open the SSH terminal and enter the following CLI command:

```
appmgr update dcnm -u <DB_URL> -n <DB_USER> -p <DB_PASSWORD>
```

**Step 5** Enter the root password of the Cisco DCNM Open Virtual Appliance.

This password is used to access AMQP/LDAP by default. You can change this password later in Cisco DCNM Web Client by using the following path: **Configure > LAN Fabric Settings > General**.

```
[root@DCNM ~]# appmgr update dcnm -u jdbc:oracle:thin:@10.77.247.11:1521:XE -n extuser -p extuserpwd
```

The external DCNM database will be configured to access all the Programmable Fabric applications using the root password of this server. You can change the password from the Cisco DCNM Web Client on **Configure > LAN Fabric Settings > General** page.

```
Root password :
Enter it again for verification:
Please wait...this could take a few minutes
```

```
Done.
```



**Note**

The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for Linux/Windows/OVA/ISO platforms are: <SPACE>&\$% single and double quotes. And the rest are all allowed: ! @ # ^ \* - + = : ; ? , / ~ ` \ | < > (). Do not use the following characters in your password: "&\$%' and <SPACE>.

**Step 6** Start the Cisco DCNM application in the Open Virtual Appliance by entering the following command:

```
appmgr start dcnm
```

**Step 7** Update the Fabric setting in Cisco DCNM, if necessary.

## Configuring the Oracle Database for XMPP

Perform the following steps to configure Oracle Database for XMPP:



**Note**

If you configure a remote Oracle database for both DCNM and XMPP in an appliance (OVA/ISO), create two separate database users—one for the DCNM and the other for XMPP.

**Step 1** Prepare the Oracle database.

For more information, see [Preparing the Oracle Database, page 2-21](#).

**Step 2** Get the JDBC database URL, database username and database password.

**Step 3** Stop the Cisco XMPP application in the DCNM Open Virtual Appliance.

**Step 4** Open the SSH terminal and enter the following command:

```
appmgr update xmpp -u <oracle_jdbc_url> -n <oracle_db_user> -p <oracle_db_password>
```

where:

```
-u <oracle_jdbc_url> : Oracle JDBC URL
-n <oracle_db_user> : Database Username
-p <oracle_db_password>: Database User Password
```



For example,  
 appmgr update xmpp -u jdbc:oracle:thin:@1.2.3.4:1521:XE -n admin -p secret

**Step 5** Start the Cisco XMPP application in the DCNM Open Virtual Appliance.



**Note**

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-20](#).

## DCNM ISO Virtual Appliance Installation

The DCNM ISO Virtual Appliance can be deployed in ESXi and KVM Hypervisors.

You can change from the local database to an external Oracle database, if required. For instructions, see [Change from Local Database to an External Database, page 6-11](#).

During the installation of the Cisco DCNM ISO Virtual Appliance, an error message appears on the graphical console, based on based on the hardware of the setup.

If an unsupported Hardware Detected, perform one of the following:

- Ignore the error message and click OK to continue with the installation
- Try installing the DCNM ISO Virtual Appliance on a different hardware platform. Refer to the the CentOS hardware compatibility matrix located at [www.centos.org/hardware](http://www.centos.org/hardware)



**Note**

It is strongly recommended to install the Cisco DCNM ISO Virtual Appliance on a supported hardware platform.

### Downloading DCNM ISO Virtual Appliance Installer



**Note**

This procedure is common to both DCNM ISO Virtual Appliance Installation on VMWare ESXi and KVM deployments.

- 
- Step 1** Navigate to <http://software.cisco.com/download/navigator.html>.
- Step 2** In the **Product/Technology Support** section, select **Download Software**.
- Step 3** In the **Select a Product** section, navigate to the DCNM software. Select **Products > Switches > Data Center Switches > Data Center Network Management > Data Center Network Manager**.  
 A list of the latest release software for Cisco DCNM is available for download.
- Step 4** In the Latest Releases list, choose 10.4(1)
- Step 5** Locate the DCNM ISO **dcnm-va.iso** at **DCNM Virtual Appliance for VMWare, KVM** and click **Download**.
- Step 6** Locate the **DCNM VM templates** at **DCNM Virtual Appliance definition files for VMWare (.ovf) and KVM (domain XMLs) environment** and click **Download**.
-

Proceed to one of the following:

**Note**

You can change from the local database to an external Oracle database, if required. For instructions, see [Change from Local Database to an External Database](#), page 6-11.

- [Installing the DCNM ISO Virtual Appliance on VMWare ESXi](#), page 3-10
- [Installing the DCNM ISO Virtual Appliance on KVM](#), page 3-14
- [Installing the DCNM ISO Virtual Appliance on N1110](#), page 3-16
- [Installing the DCNM ISO Virtual Appliance on UCS](#), page 3-18

## Installing the DCNM ISO Virtual Appliance on VMWare ESXi

Perform the following tasks to install the ISO virtual appliance on VMWare ESXi.

- 
- Step 1** Unzip and extract the **dcnm-va-ovf-kvm-files.10.4.1.zip** and locate **dcnm-esxi-vm.ovf** file.
- Step 2** Connect to the vCenter Server (Flash client or web client) using vCenter Server user credentials.
- Step 3** Use the vCenter Server application to deploy OVF template.
- Step 4** Navigate to **Home > Inventory > Hosts and Clusters**.  
Select the host on which the OVF template must be deployed.
- Step 5** Navigate to **File > Deploy OVF Template** to open the Deploy OVF template window.  
Choose the Source location, and click **Browse**.
- Step 6** Locate the **dcnm-esxi-vm.ovf** file and click **Next**.
- Step 7** Review the OVF template details and click **Next**.
- Step 8** Read and accept the End User License Agreement and click **Next**.
- Step 9** Specify the name and location of the Cisco DCNM appliance.  
In the Name box, enter a name for the ISO Virtual Appliance. This is the name of the virtual appliance hardware and is specific to the vSphere infrastructure. The name can contain up to 80 alphanumeric characters and must be unique within the Inventory folder.
- Step 10** In the **Inventory Location** tree, choose the folder location for the virtual appliance and click **Next**.
- Step 11** Choose the deployment configuration:
- Small—to configure the virtual machine with two vCPUs and 8G RAM.
  - Large—to configure the virtual machine with four vCPUs and 12G RAM.

**Note**

Cisco recommends that you use a Large deployment configuration when you are managing more than 50 devices (and up to the upper limit of the Cisco Fabric) to leverage better RAM, heap memory, and CPUs. For setups that could grow, you should choose Large. Choose Small for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time. You can change from the local database to an external Oracle database, if required. For instructions, see [Change from Local Database to an External Database](#), page 6-11.

Click **Next**.

**Step 12** Specify the **Host** and click **Next**.

**Note**

A host will not be available if you already selected a host in the vSphere Client before you deploy the Cisco DCNM Appliance.

**Step 13** Choose a destination storage for the virtual machine files.

**Step 14** Choose the disk format.

- Select any the thick provision types if you have enough storage capacity as required by the virtual appliance and want to set a specific allocation of space for the virtual disks:
  - Thick Provision Lazy Zeroed  
The space required for the virtual disk is allocated when the virtual disk is created. The data on the physical device will not be erased when the virtual disk is created. However, it is erased when the new data is saved from the virtual disk.
  - Thick Provision Eager Zeroed  
The space required for the virtual disk is allocated when the virtual disk is created. The data on the physical device is erased when the virtual disk is created.
- Choose Thin Provision if you have less than 100 GB of disk space available. The initial disk consumption will be around 3 GB and will increase as the size of the database increases with the number of devices being managed.

**Step 15** Choose your network mapping for the networks created in the prerequisites.

The **dcnm-mgmt** network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. In the **Destination Network** column, associate the network mapping with the port group that corresponds to the subnet associated with the Cisco DCNM management network.

- a. Map the enhanced-fabric-mgmt network to the port group that connects to the management network of switches.
- b. If you are deploying more than one OVA for HA functionality, the following criteria must be met:
  - Both Appliances should have their management access (eth0) and enhanced fabric management (eth1) interfaces in the same subnet.
  - Both Appliances should be deployed with the same administrative password. This is to ensure that both Open Virtual Appliances are duplicates of each other for application access.

**Step 16** Click **Next**.

**Note**

Do not select **Power on after deployment**.

**Step 17** Click **Finish**.

The **Deploying DCNM Virtual Machine Template** appears and the virtual hardware is created. After the VM is deployed, a **Deployment Completed Successfully** message appears.

**Step 18** Right click on the VM and select **Edit Settings**.

**Step 19** Navigate Hardware and click **Add**.

**Step 20** Select a **Hard Disk** and click **Next**.

**Step 21** With the default option set to **Create a new virtual disk**, click **Next**.

**Step 22** In the Disk Size field, enter **100GB**.

**Step 23** Select thick or thin provisioning based on the requirement.

**Step 24** Click **Next**.

**Step 25** Select the location as **Store** with the virtual machine.

**Step 26** Retain the default values for Virtual Device Node. Click **Next**.




---

**Note** Ensure that you do not select **Mode**.

---

**Step 27** Click **Finish**.

**Step 28** You can link the DCNM ISO to the VM by one of the following methods:

- connecting to the ISO Virtual Appliance image on local disk, if the ISO is on the same system as the vSphere client. This must be performed only after the VM is powered on.
- connecting to the host device, if the ISO Virtual Appliance is located on the ESXi host.
- connecting to ISO Virtual Appliance image on datastore, if the ISO is located on the datastore.

Navigate to **Hardware**.

**Step 29** Click the **CD/DVD** drive. Select the Datastore ISO File and locate the ISO file.

**Step 30** Click **OK**.

**Step 31** Power on the Virtual Machine. The operating system is installed.

**Step 32** Log on to the VM console in vSphere client using the default credentials

**username: root**

**password: cisco123**

**Step 33** Run the appmgr CLI to setup the network properties.

The status of all the applications is displayed after the installation is complete.

---

### Example: appmgr CLI to setup network properties

```
[root@dcnm ~]# appmgr setup standalone
Hostname (Fully Qualified Domain Name): dcnm.cisco.com

*** Configuring DCNM Management network ***
IP address   : 10.197.67.57
Subnet Mask  : 255.255.255.192
Gateway      : 10.197.67.1
DNS server   : 72.163.128.140

Do you want to install SA
*** Configuring EFM Management network ***
Do you want to install SAN management features along with LAN? Yes/No [Yes] :
IP address   : 192.168.57.57
Subnet Mask  : 255.255.255.0
DNS server   : 72.163.128.140
Do you want to configure IPv6 on EFM management network? Yes/No [No]:
Yes
IPv6 Address with prefix (eg: 2001:db8:abcd:0012::0/96) :

*** Administrative settings ***

Management password :
```

Enter it again for verification:

You have entered these values..

```

HOSTNAME=dcnm.cisco.com
ETH0_IP=10.197.67.57
ETH0_NM=255.255.255.192
ETH0_GW=10.197.67.1
ETH0_DNS=72.163.128.140
ETH1_IP=192.168.57.57
ETH1_NM=255.255.255.0
ETH1_DNS=0.0.0.0
ETH1_IPv6=2001:db8:abcd:0012::0/96

```

INSTALL\_OPTION=BOTH(LAN+SAN)

Press 'y' to continue installation, 'n' to re-enter values, 'q' to quit [y] y

Installing applications..  
done.

appmgr status all

DCNM v10 will only use HTTPS. Insecure access via HTTP is now disabled.  
Please use the url <https://DCNM-IP-ADDRESS> or <https://HOSTNAME> to launch the DCNM UI.

DCNM Status

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1562	root	20	0	3940m	763m	27m	S	0.0	9.7	18:28.59	java

LDAP Status

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1208	ldap	20	0	210m	5312	2100	S	0.0	0.1	0:00.02	slapd

TFTP Status

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1236	root	20	0	22188	1020	764	S	0.0	0.0	0:00.00	xinetd

DHCP Status

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1249	dhcpcd	20	0	46336	1212	196	S	0.0	0.0	0:00.00	dhcpcd

XMPP Status


PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1791	root	20	0	1389m	16m	6640	S	0.0	0.2	0:14.15	jabberd

AMQP Status

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1326	rabbitmq	20	0	1103m	71m	2704	S	0.0	0.9	8:14.46	beam.smp

## Installing the DCNM ISO Virtual Appliance on KVM

Perform the following tasks to install the ISO virtual appliance on KVM.

- 
- Step 1** Unzip and extract **dcnm-va-ovf-kvm-files.10.4.1.zip** and locate the **dcnm-kvm-vm.xml** file.
- Step 2** Upload this file on the RHEL server that is running KVM to the same location as the ISO.
- Step 3** Connect to the RHEL server running KVM via SCP File transfer terminal.
- Step 4** Upload the **dcnm-va.iso** and **dcnm-kvm-vm.xml** to the RHEL server.
- Step 5** Close the file transfer session.
- Step 6** Connect to the RHEL server running KVM via SSH terminal.
- Step 7** Navigate to the location where both the ISO and domain XMLs is downloaded.
- Step 8** Create the VM (or Domains, as they are known in the KVM terminology) using the **virsh** command.
- ```
sudo virsh define dcnm-kvm-vm.xml
```
- Step 9** Enable a VNC server and open the required firewall ports.
- Step 10** Close the SSH session.
- Step 11** Connect to the RHEL server running KVM via a VNC terminal.
- Step 12** Navigate to **Applications -> System Tools -> Virtual Machine Manager (VMM)**  
A VM is created in the Virtual Machine Manager.
- Step 13** From Virtual Machine Manager, edit the VM by selecting the VM in the listing. Click **Edit > Virtual Machine Details > Show virtual hardware details**.
- Step 14** In the Virtual Hardware Details, navigate to **Add Hardware > Storage**.
- Step 15** Create a hard disk with Device type with the following specifications
- device type: IDE disk
  - cache-mode: default
  - storage format: raw
- 

**Note** Cisco recommends that you use storage size of 100GB for Programmable Fabric deployments.
- 
- Step 16** Select **IDE CDROM** on the edit window of the Virtual Machine and click **Connect**.
- Step 17** Navigate to **dcnm-va.iso** and click **OK**.
- Step 18** Select both the NICs and assign appropriate networks created. Refer to [Prerequisites for DCNM ISO Virtual Appliance, page 2-2](#).
- Step 19** Power on the Virtual Machine.  
The operating system is installed.  
The VM is powered off automatically after the OS installation.
- Step 20** Navigate to **Edit > Virtual Machine Details > Show virtual hardware details** and edit the Virtual Machine.
- Step 21** Click **IDE CDROM** in the Hardware section and disconnect the ISO from the VM.

This is to ensure that the next time the VM boots, it boots from the hard disk instead of CD/DVD.

**Step 22** Click **OK**.

**Step 23** Power on the Virtual Machine.

**Step 24** Logon to the VM console in Virtual Machine Manager using the default credentials

**username : root**

**password : cisco123**

**Step 25** Run the **appmgr** command to setup the network properties. For more information, see the example below.

The status of all the applications is displayed after the installation is complete.

### Example: appmgr CLI to setup network properties

```
[root@dcnm ~]# appmgr setup standalone
Hostname (Fully Qualified Domain Name): dcnm.cisco.com
*** Configuring DCNM Management network ***
IP address : 10.197.67.57
Subnet Mask : 255.255.255.192
Gateway : 10.197.67.1
DNS server : 72.163.128.140
*** Configuring EFM Management network ***
Do you want to install SAN management features along with LAN? Yes/No [Yes] :
IP address : 192.168.57.57
Subnet Mask : 255.255.255.0
DNS server : 72.163.128.140
Do you want to configure IPv6 on EFM management network? Yes/No [No]:
Yes
IPv6 Address with prefix (eg: 2001:db8:abcd:0012::0/96) :
*** Administrative settings ***
Management password :
Enter it again for verification:
You have entered these values..
HOSTNAME=dcnm.cisco.com
ETH0_IP=10.197.67.57
ETH0_NM=255.255.255.192
ETH0_GW=10.197.67.1
ETH0_DNS=72.163.128.140
ETH1_IP=192.168.57.57
ETH1_NM=255.255.255.0
ETH1_DNS=0.0.0.0
ETH1_IPv6=2001:db8:abcd:0012::0/96
Press 'y' to continue installation, 'n' to re-enter values, 'q' to quit [y] y
Installing applications..
done.

appmgr status all

DCNM v10 will only use HTTPS. Insecure access via HTTP is now disabled.
Please use the url https://DCNM-IP-ADDRESS or https://HOSTNAME to launch the DCNM UI.

DCNM Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1562 root 20 0 3940m 763m 27m S 0.0 9.7 18:28.59 java

LDAP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
```

```

=== =====
1208 ldap 20 0 210m 5312 2100 S 0.0 0.1 0:00.02 slapd

TFTP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1236 root 20 0 22188 1020 764 S 0.0 0.0 0:00.00 xinetd

DHCP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1249 dhcpd 20 0 46336 1212 196 S 0.0 0.0 0:00.00 dhcpd

XMPP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1791 root 20 0 1389m 16m 6640 S 0.0 0.2 0:14.15 jabberd

AMQP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1326 rabbitmq 20 0 1103m 71m 2704 S 0.0 0.9 8:14.46 beam.smp

```

## Installing the DCNM ISO Virtual Appliance on N1110

Perform the following tasks to install the ISO virtual appliance on KVM.

- 
- Step 1** Launch the CSP 2100 UI and navigate to **Configuration > Repository > Select > Upload**.
- Step 2** Select **dcnm-csp2100.iso**. Click **Upload**.
- Step 3** On the Configuration tab, click **Services > Create**.  
The Service Creation page appears.
- Step 4** In the service creation panel, enter the following parameters.
- Enter the **Service Name**.
  - Select the **Target Host Name**.
  - Select the **HA Host Name**.  
The default value is none.
  - Select the image that you have uploaded in [Step 1](#).  
After you select the image, 2 vNIC's and Resource Config tab is populated with resource (4core, 80GB, 8192MB RAM) information.
  - In the vNIC tab, navigate to **vNIC1 > Network Name > Internal/External Network**.  
On the Select Network Interface panel, select the physical network interface.
  - Navigate to **vNIC2 > Network Name > Internal/External Network**.  
On the Select Network Interface panel, select the physical network interface.
  - The Resource Config tab displays the minimum resources to deploy the Cisco DCNM Application.  
You can modify the resources to have higher resource values, based on your requirement.
  - (Optional) On the **Storage Config** tab, add the storage details.



- i. (Optional) On the VNC Password tab, enter **VNC password** to access the virtual machine VNC Console.
- j. (Optional) Enter the **Crypto Bandwidth** and **Serial Port** details.
- k. Click **Save**.

**Step 5** Select the image which is uploaded to enter additional information.

Upon selection of the image in [Step 4d.](#), **Additional Image Info Required** window appears.

- a. In the HA Role for the appliance, enter **Primary** or **Secondary**.
- b. Enter fully qualified **hostname**.  
For example: **dcnm.cisco.com**.
- c. Enter **Management IP address**, **Subnet Mask**, **Gateway** and **DNS** for DCNM Management.
- d. Enter **Default Gateway IP address**, **Subnet Mask** and **DNS** for Spine Management.
- e. From the **Enable DFA for DCNM** drop-down, choose “Y” or “N”
- f. Enter **Administrative Password**.
- g. Click **Save**.

**Step 6** Click **Deploy** to deploy the virtual machine with the above configured values.

**Step 7** Navigate to **Configuration > Services** to check the status of deployment.

The values of Power/State will show **on/deployed**.

**Step 8** Click on the **Console** icon to launch the VM console.

Virtual machine VNC console appears.

Please input the VNC password entered earlier in step 3 and click connect. If no password is entered, just click on connect to access the Console.

**Step 9** Enter the **VNC password**, provided in [Step i](#), and click **Connect**.

If no password was entered earlier, click **Connect** to access the Console.

**Step 10** After the OS boots, launch the CLI using the credentials:

```
username: root
password: cisco123
```

**Step 11** Install Cisco DCNM by using one of the following commands:

- **appmgr setup standalone**

Enter the following parameters:

```
Hostname (Fully Qualified Domain Name): dcnm.cisco.com
*** Configuring DCNM Management network ***
IP address: 10.197.67.57
Subnet Mask: 255.255.255.192
Gateway: 10.197.67.1
DNS server: 72.163.128.140
*** Configuring EFM Management network ***
IP address: 192.168.57.57
Subnet Mask: 255.255.255.0
DNS server: 72.163.128.140
Do you want to configure IPv6 on EFM management network? Yes/No [No]: Yes
IPv6 Address with prefix (eg: 2001:db8:abcd:0012::0/96) :
*** Administrative settings ***
Do you want to install DFA applications True/False [True]: True
Management password:
```

Enter it again for verification:

- **appmgr setup standalone -i silent -f <filename>**

This command reads the parameters from the file located at  
/root/packaged-files/properties/fabric-installer.properties

The installation will proceed with the parameters provided in the file.

- **appmgr setup standalone -i silent -f <filename>**

This command allows you to specify the filename which contains the user-defined parameters. The installation will proceed with the parameters provided in the file.

**Step 12** Enter **Y** to proceed with the installation.

Enter **N** to modify the parameters.

**Step 13** After the successful installation verify if Cisco DCNM is operational, by using the **appmgr status all** command.



**Note**

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances](#), page 3-20.

## Installing the DCNM ISO Virtual Appliance on UCS



**Note**

DCNM 10.4(1) is supported on UCS 220M3, 220M4, and 240M4.

Perform the following tasks to install the DCNM ISO virtual appliance on UCS.

**Step 1** Launch Cisco Integrated Management Controller (CIMC).

**Step 2** Click the **Launch KVM Console** button.

**Step 3** Click the **Virtual Media** menu, and then click **Activate Virtual Devices**.

**Step 4** After you activate virtual devices, you can browse and upload DCNM ISO images from the following locations:

- Map CD/DVD
- Map Removable Disk
- Map Floppy Disk

**Step 5** Restart the UCS box using **Macros > Static Macros > Ctrl+Alt+Del**.

**Step 6** Press **F6** when the server starts to select a boot device. The boot selection menu appears.

For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:

[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/sw/ucsscu/user/guide/31/UCS\\_SCU/booting.html#wp1078073](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/31/UCS_SCU/booting.html#wp1078073)

**Step 7** Use the arrow keys to select Cisco Virtual CD/DVD and then press Enter. The server boots with the DCNM ISO image and starts the installation of the CentOS.

If an unsupported hardware is detected, perform one of the following:

- Ignore the error message and click OK to continue with the installation.
- Try installing the DCNM ISO Virtual Appliance on a different hardware platform.

**Step 8** After the installation of CentOS, log in to CentOS as a root user using the default credentials:

User name: root

Password: cisco123

**Step 9** Run the **appmgr setup standalone** command to setup the network properties. For more information, see the example below. This step completes the installation and the status of all the applications is displayed as below.

```
Example: appmgr CLI to setup network properties
[root@dcnm ~]# appmgr setup standalone
Hostname (Fully Qualified Domain Name): dcnm.cisco.com
*** Configuring DCNM Management network ***
IP address : 10.197.67.57
Subnet Mask : 255.255.255.192
Gateway : 10.197.67.1
DNS server : 72.163.128.140
*** Configuring EFM Management network ***
Do you want to install SAN management features along with LAN? Yes/No [Yes] :
IP address : 192.168.57.57
Subnet Mask : 255.255.255.0
DNS server : 72.163.128.140
Do you want to configure IPv6 on EFM management network? Yes/No [No]:
Yes
IPv6 Address with prefix (eg: 2001:db8:abcd:0012::0/96) :
*** Administrative settings ***
Management password :
Enter it again for verification:
You have entered these values..
HOSTNAME=dcnm.cisco.com
ETH0_IP=10.197.67.57
ETH0_NM=255.255.255.192
ETH0_GW=10.197.67.1
ETH0_DNS=72.163.128.140
ETH1_IP=192.168.57.57
ETH1_NM=255.255.255.0
ETH1_DNS=0.0.0.0
Press 'y' to continue installation, 'n' to re-enter values, 'q' to quit [y] y
Installing applications..
done.
appmgr status all
DCNM v10 will only use HTTPS. Insecure access via HTTP is now disabled.
Please use the url https://DCNM-IP-ADDRESS or https://HOSTNAME to launch the DCNM UI.
DCNM Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1562 root 20 0 3940m 763m 27m S 0.0 9.7 18:28.59 java
LDAP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1208 ldap 20 0 210m 5312 2100 S 0.0 0.1 0:00.02 slapd
TFTP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1236 root 20 0 22188 1020 764 S 0.0 0.0 0:00.00 xinetd
DHCP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
```

```

1249 dhcpd 20 0 46336 1212 196 S 0.0 0.0 0:00.00 dhcpd
XMPP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1791 root 20 0 1389m 16m 6640 S 0.0 0.2 0:14.15 jabberd
AMQP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== =====
1326 rabbitmq 20 0 1103m 71m 2704 S 0.0 0.9 8:14.46 beam.smp

```

---

## Setting the Timezone for Cisco DCNM Virtual Appliances

After installing Cisco DCNM Virtual Appliances, before performing any operations, ensure that you set the timezone on the DCNM Appliance. This will ensure that the system-generated reports and other statistics show the correct date as per your timezone.

Perform the following procedure to set the timezone.

- 
- Step 1** On the Cisco DCNM Virtual appliance, save the current timezone by using the following command:
- ```
mv /etc/localtime /etc/localtime.bak
```
- Step 2** Update the current timezone to your desired timezone, using the following command:
- ```
ln -s /usr/share/zoneinfo/<<country_name>>/<<state_name>> /etc/localtime
```
- Step 3** Check and confirm if the timezone is updated using the following command: --- date is the command they need to run.
- ```
date
```
- Step 4** Restart the Cisco DCNM, using the **appmgr restart dcnm** command.



### Note

If you have installed Cisco DCNM Native HA appliance, restart using the **appmgr restart ha-apps** command.

---

## DCNM installation without Enhanced Fabric Management capabilities

This section details the tasks for DCNM installation without Enhanced Fabric Management capabilities based on the installers. This section contains the following:

- [Windows Installation, page 3-21](#)
- [Linux RHEL Server Installation, page 3-21](#)
- [DCNM Open Virtual Appliance \(OVA\) Installation, page 3-27](#)
- [ISO Virtual Appliance Installation on KVM, page 3-27](#)
- [DCNM OVA in High Availability/Federation, page 3-28](#)

## Windows Installation

You can install DCNM on the either Windows XP, Windows 2008, Windows 7 and Windows 2012.

- For instructions on how to install DCNM for Windows 2012, see [Installing Cisco DCNM on Windows 2012](#).
- For other versions of Windows, see [Installing Cisco DCNM on Windows and Linux using the GUI](#).

### Prerequisites

For information about the prerequisites before you begin the installation, see the following sections:

- [General Prerequisites for Installing the Cisco DCNM on Windows and Linux, page 2-3](#)
- [Prerequisites for Windows Installer, page 2-16](#).

## Installing Cisco DCNM on Windows 2012

Perform the following steps to install DCNM:

### DETAILED STEPS

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Right click on the installer and select <b>Troubleshoot compatibility</b> . to troubleshoot issues if your system is not compatible with the installer. |
| <b>Step 2</b> | Select <b>Try recommended settings</b> . Click <b>Next</b> to test run the program using recommended compatibility settings.                            |
| <b>Step 3</b> | After settings are applied, click <b>Next</b> .<br>Cancel the installation process at that point  |
| <b>Step 4</b> | Select <b>Save the settings for this program</b> and close the troubleshooter.  |
| <b>Step 5</b> | Invoke the installer.exe and install the DCNM.  |
- 

## Linux RHEL Server Installation

Perform the following steps to install DCNM:

### Prerequisites

For information about the prerequisites before you begin the installation, see the following sections:

- [General Prerequisites for Installing the Cisco DCNM on Windows and Linux, page 2-3](#)
- [Prerequisites for Linux RHEL Server, page 2-17](#).

## Installing Cisco DCNM on Windows and Linux using the GUI



### Note

Before upgrading or uninstalling the Cisco DCNM or Device Manager, ensure that all the instances are shut down.

If the PostgreSQL database is not present on your computer, the installer installs PostgreSQL9.4. You can change the default credentials after the installation is complete.



### Note

When installing or upgrading Cisco DCNM SAN federation with same or different subnets, Cisco DCNM-SAN services do not start at the end of the DCNM installation. You must start the Cisco DCNM services manually using the shortcuts available under `../dcnm/fm/bin` or when asked by installer in the end of the installation.

Cisco DCNM has only 64-bit executable. 32-bit executable is not supported for Cisco DCNM.



### Note

Before you execute the installer, ensure that you create a database user with a user role and assigned schema. If you are using the Oracle database, a mapped schema is already created. If you are using a PostgreSQL database, ensure that you create a new schema with the exact string as the new username and that the new user is the schema owner.

## DETAILED STEPS

- Step 1** Go to the directory where you downloaded the Cisco DCNM software and run the `dcnm-release.exe` file. After the installer prepares the installation, the Introduction step appears in the Cisco DCNM installer window.
- Step 2** Click **Next** when the Introduction step appears in the Cisco DCNM installer window after the installer prepares the installation.
- Step 3** Click **Next** when the Please Read Before Continuing information appears in the Cisco DCNM installer window.
- Step 4** Enter the following when the Choose Install Folder step appears in the Cisco DCNM installer window:
  - a. (Optional) If you want to add the server to the existing federation, check the **Add Server to an existing server federation** checkbox.
  - b. (Optional) If you want to change the default installation folder, enter or choose the desired installation folder.
  - c. Click **Next**.

As part of the Cisco DCNM installation, one of the following options are displayed according to your system requirements.

- New installation—The installer installs Cisco DCNM-SAN, and SMI-S for the first time.



### Note

Cisco DCNM-SAN federation can be deployed across nodes and databases in the different subnets.

- Upgrade Cisco DCNM—The installer discovered previous version of Cisco DCNM and upgrades to latest version.

- Upgrade Cisco DCNM-SAN—The installer discovered a previous version of Cisco DCNM-SAN. The installer upgrades to the latest version of Cisco DCNM-SAN and SMI-S agent.

The Database Options step appears in the Cisco DCNM installer window. You can use an existing PostgreSQL installation or an existing Oracle installation. If PostgreSQL is not installed on the server system, you can use the Cisco DCNM installer to add a PostgreSQL installation.

**Step 5** If you want to install PostgreSQL, do the following:



**Note**

When you install PostgreSQL with Cisco DCNM, the database admin username and password is the same as the database username and password appended with 123. For example, if your database username is dcnmuser, the admin username is dcnmuser123. Similarly, if the database password is dcnmtest, the admin password is dcnmtest123.



**Note**

- On Linux—If you want install PostgreSQL, ensure you have a non-root privileged user called postgres in the server. If you have not created a non-root privileged user, the installer will prompt you to create one and if you skip entering the details, the installer will automatically create a user called postgres with non-root privileges.
  - On Linux—To allow remote access to the database, modify the pg\_hba.conf file and restart the postgres service using the command `<dbroot>/bin/pg_ctl`.
- a. Next to RDBMS, click **Install PostgreSQL**.  
If your server system runs RHEL, the System User dialog box appears.
  - b. (RHEL only) In the System User dialog box, enter the username for the user account that should be used to run the PostgreSQL software. This user account should not have administrator or root privileges.
  - c. In the DCNM DB User field, enter the username that Cisco DCNM-SAN should use to access the database. The default username is dcnmuser. The installer creates the user account that you specify.
  - d. In the DCNM DB Password field, enter the password for the database user account that you specified.
  - e. In the Confirm DCNM DB Password field, reenter the password for the database user account that you specified.
  - f. (Optional) If you want to change the default PostgreSQL database installation folder, in the Install Location field, enter or choose the desired installation folder.

**Step 6** If you want to use an existing relational database management system (RDBMS) installation, do the following:

- a. Next to RDBMS, click one of the following:
  - Use existing PostgreSQL 8.1/8.2/8.3/9.4
  - Use existing Oracle 10g/11g
  - Use Oracle RAC

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

**Note**

Cisco DCNM installation with existing PostgreSQL requires an existing schema with the same name as the DCNM username, owned by the same username. When there are 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”.

**Note**

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

- b. If the DB URL field does not have the correct URL to the database, enter the correct URL.

**Note**

The database is not automatically created. You must manually create the database. A valid database URL is required to create a database schema and connect to it.

- c. In the DCNM DB User field, enter the username that Cisco DCNM should use to access the database.
- d. In the DCNM DB Password field, enter the password for the database user account that you specified.
- e. If user selects “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.

**Step 7** If you want to use an existing Oracle 10g/11g RAC, do the following:

- a. Next to RDBMS, click the following:
  - Use the existing Oracle 10g/11g RAC

The Oracle RAC configuration dialog box appears.

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

**Step 8** Click **Next**.

The Configuration Options step appears in the Cisco DCNM installer window.

**Step 9** In the Configuration Options dialog box, do the following:

**Note**

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

- a. 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.
- b. 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.

**Step 10** If you want to change the data path for federation, use a shared path. By default, the data path will be *install\_dir/dcnm/data*.

**Step 11** Click **Next**.



The Local User Credentials step appears in the Cisco DCNM installer window.

- Step 12** In the Local 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.
- Step 13** In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.



**Note** The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for Windows/Linux platforms are: SPACE, double quotes, single quotes, &, \$, %, ^, =, <, >, :, ;, . Do not use the following characters in your password: "&\$%' and <SPACE>.

- Step 14** Click **Next**.

The Authentication Settings step appears in the Cisco DCNM installer window.

Choose the authentication method that the Cisco DCNM server should use to authenticate users who log into 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 15** 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**.

- Step 16** Click **Next**.

If you are using Microsoft Windows, the installer asks you to specify a shortcut to the application. If you are using RHEL, the installer asks you to specify a link folder.

- Step 17** Choose the shortcut or link options that you want.

- Step 18** (Optional) 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.

- Step 19** Click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

- Step 20** Carefully review the summary of your choices. If you need to change anything, click **Previous** until the Cisco DCNM installer window displays the step that you need to change, and then return to the applicable preceding step.

- Step 21** Click **Next** when you are ready to install the Cisco DCNM server software.

The installer installs the Cisco DCNM server software.

The Installing Cisco DCNM installer window appears. By default, the server will be started after installation is complete. The Install Complete step appears in the Cisco DCNM installer window. The Cisco DCNM instance ID number is displayed.

- Step 22** (Optional) If you plan to order licenses for Cisco DCNM, record the Cisco DCNM instance ID number. The licensing process requires that you enter that number.



**Note** You can begin using Cisco DCNM without a license but some features are not available unless you purchase and install a license and apply the license to managed devices that you want to use licensed features with.

- Step 23** Click **Done**.

## Installing DCNM (Windows or Linux) in a Server Federation Environment

To install DCNM (Windows or Linux) in a server federation environment:

- Step 1** Follow the steps explained in the [Windows Installation, page 3-21](#) or [Linux RHEL Server Installation, page 3-21](#) sections.
- Step 2** You can add a server to the existing federation, by selecting the **Add Server to an existing server federation** check box.
- Step 3** If you select the **Add Server to an existing federation** check box, modify the database URL by selecting the corresponding RDBMS option. 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.

## Copying Certificates

When you add a new Cisco DCNM instance to an existing federation or cluster, ensure you copy fmtrust.jks and fmserver.jks certificate files manually from any one of the nodes present in the Cisco DCNM federation or cluster.

You should get the certificate files under the following folders:

- **On Microsoft Windows**—<DCNM install folder>\dcm\jboss-4.2.2.GA\server\fm\conf
- **On Linux**—<DCNM install folder>/dcm/jboss-4.2.2.GA/server/fm/conf

In the new node, you should copy the certificate files under the following folders:

- **On Microsoft Windows**—<DCNM install folder>\dcm\jboss-4.2.2.GA\server\fm\conf
- **On Linux**—<DCNM install folder>/dcm/jboss-4.2.2.GA/server/fm/conf

**Note**

Ensure you restart the Cisco DCNM servers after copying the certificate files.

## Collecting PM Data

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

- 
- Step 1** Locate the server.properties file under C:\Program Files\Cisco Systems\dcnm\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.
- 

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.

## DCNM Open Virtual Appliance (OVA) Installation

For instruction on how to install DCNM Open Virtual Appliance in non-Programmable Fabric mode, see [DCNM Open Virtual Appliance Installation in Programmable Fabric mode, page 3-2](#).

**Note**

During installation, when you enter the OVF properties in vSphere client, do not enter any values for the parameters under the section "**Enhanced Fabric Management Network**".

## ISO Virtual Appliance Installation on KVM

For instruction on how to install DCNM ISO Virtual Appliance in non-Programmable Fabric mode, see [DCNM ISO Virtual Appliance Installation, page 3-9](#).

**Note**

During the installation, when you configure the appliance using the appmgr setup standalone command, ensure that you provide the default values for EFM Management network as like below

```
*** Configuring EFM Management network ***  
IP address : 0.0.0.0  
Subnet Mask : 0.0.0.0  
DNS server : 1.1.1.1
```

## Configuring Media Controller for IP Fabric

Beginning from Release 10.1(2), Cisco DCNM OVA or ISO installation allows you to monitor and control IP Fabric for Cisco Nexus 9000 Series Switched through Cisco DCNM Web Client. This feature is available if you have enabled the Media Controller feature explicitly, after the Cisco DCNM OVA/ISO installation is complete.



### Note

This feature can be enabled only on the DCNM Open Virtual Appliance or DCNM ISO Virtual Appliance Installation.

To enable the Media Controller feature on the Cisco DCNM Web Client, perform the following.

- 
- Step 1** Log in to the SSH terminal of the Cisco DCNM OVA/ISO.
- Step 2** Stop all the applications by using the following command:
- ```
appmgr stop dcnm
```
- Step 3** Enable the Media Controller on the Cisco DCNM Web Client, by using the following command:
- ```
appmgr set-mode media-controller
```
- 

Logon to Cisco DCNM **Web Client** > **Media Controller** to perform various operations on the IP Fabric, for Cisco Nexus 9000 Series Switches.



### Note

To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco DCNM **Web Client** > **Configure** > **Deploy** > **POAP**.

## DCNM OVA in High Availability/Federation

To achieve non-Programmable Fabric Federation (HA for Non-Enhanced Fabric mode) that are run on the Cisco DCNM Open Virtual Appliance. Deploying a federation includes one primary server and one and more secondary servers. This procedure provides the general steps that you must take to deploy a federated Cisco DCNM environment.



### Note

XMPP takes the first server from the Oracle RAC URL. If the first server is down, then swap the server IP address.

This section includes:

- [Configuring First Node, page 3-29](#)
- [Configuring Federated Nodes, page 3-30](#)
- [Application or Server Failover, page 3-30](#)

### Prerequisites

This section contains the following topics that describe the prerequisites for obtaining a Non DFA Federation environment. OVA/ISO should be deployed in a Non-Enhanced Fabric mode.

For more information, see [Prerequisites for Cisco DCNM Open Virtual Appliance HA, page 7-2](#).

## Configuring First Node

Perform the following procedure to configure the Cisco DCNM non-Unified appliance as first node.

**Step 1** Stop all the applications by using the following command:

**appmgr stop all**

**Step 2** Log in to the SSH terminal of the Open Virtual Appliance that you want designate as the first node, by using the following command:

**appmgr setup ha-type first-node**

The following prompt appears.

\*\*\*\*\*

You are about to be federated for DCNM alone in this DCNM appliance.

Please make sure that you have the following

1. An Oracle Database with a user defined for DCNM.
2. A repository with NFS capabilities.
3. An NTP server for time synchronization.

\*\*\*\*\*

**Step 3** Choose **Y** to continue.

A prompt for the Database for DCNM appears.

**Step 4** Configure the database.

- a. Enter the database URL to configure the database.

The script uses a JDBC thin driver. Therefore, enter the URL in the same format.

- b. Enter the database password.

- c. Enter the database password again for verification.

The script runs a sample query from the database to validate the details entered. The Cisco DCNM schema and related data are loaded after the data is validated.

- d. Enter the database username for DCNM tables.

- e. Enter the database password for DCNM tables.

- f. Enter the database password again for verification.

**Step 5** Configure the Repository and NFS.



**Note** A repository server in the non-Unified network must have NFS capability.

- a. Enter the SCP/NFS repository IP address.

- b. Enter the location for the NFS Exported file.

The system performs a test mount to ensure that the server is reachable. The system also performs a test-write to ensure the exported directory is writable

**Step 6** Enter an NTP server for time synchronization.

A summary of the details entered will be displayed.

**Step 7** Choose **Y** to continue.

Choose **N** to edit or update the details.

**Step 8** After the high availability configuration is complete, check the role by using the following command.

**appmgr show ha-role**

This node is part of HA Federation.

---

## Configuring Federated Nodes



### Note

In the standby node, before starting High Availability setup, you need to stop all application using the **appmgr stop all** command.

---

Perform the following procedure to configure the Cisco DCNM non-Unified appliance as a federated node.

---

**Step 1** Log in to the SSH terminal of OVA-B.

**Step 2** Configure the federated node by using the following command:

**appmgr setup ha-type federated-node**

**Step 3** Choose **Y** to continue.

**Step 4** Enter the existing Federated server IP (eth0 IP) address.

**Step 5** Enter the root password of the peer.

After confirmation, the OVA-B is configured as a federated node, and the following message is displayed.

**appmgr start dcnm in first-node and then federated-node**

---

## Application or Server Failover

Automatic failover option enabled in the Cisco DCNM UI. This process ensures that if the DCNM that is running on OVA-A fails, all the fabrics and shallow-discovered LANs managed by DCNM-A are managed by DCNM-B automatically after a given time interval (usually about 5 minutes after the failure of DCNM on OVA-A).

## DCNM Native HA Installation

The native HA is only supported on DCNM appliances with ISO or OVA installation. Unlike HA mechanisms, it doesn't require any external dependencies like an Oracle database or a shared NFS filesystem.

By default, Cisco DCNM is bundled with an embedded PostgreSQL database engine. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM will take over with the same database data and resume the operation.

Perform the following task to setup Native HA for DCNM.

**Step 1** Deploy two DCNM virtual appliances (OVA/ISO).



**Note** For example, let us indicate them as dcnm1 and dcnm2.

If both eth0 and eth1 interfaces are in the same subnet, edit the `/etc/sysctl.conf` file for DCNM ISO Virtual appliance Native HA installation on both active and standby nodes for both the appliances, as follows:

- Change the value of `net.ipv4.conf.default.rp_filter` from **1** to **2**.
- Add `net.ipv4.conf.all.rp_filter = 2` to the `sysctl.conf` file.

Save and close the file. On the SSH terminal, execute the `sysctl --system` command.

**Step 2** Wait for all the applications to be operational.

Use the `appmgr status all` command to check the status of the applications.

```
dcnm1# appmgr status all
dcnm2# appmgr status all
```

**Step 3** Use the `appmgr stop all` command to shut down all applications on both the Cisco DCNM applications.

Use the `appmgr status all` command to check the status of the applications.

```
dcnm1# appmgr stop all
dcnm2# appmgr status all
```

**Step 4** On the active node, edit the `ha-setup.properties` file, by using the following command:

```
dcnm1# vi /root/packaged-files/properties/ha-setup.properties
```



**Note** Do not turn on `auto_failback` in heartbeat configuration file.

**Step 5** Edit the active node parameters and enter appropriate values.



**Note** Please refer to [Example for DCNM Native HA Installation, page 3-32](#) section for more information.

**Step 6** Install NativeHA on the active node with the following command:

```
dcnm1# appmgr setup native-ha active
```

**Step 7** On the standby node, check if the below property values are updated in the `ha-setup.properties` file, by using the following command:

```
dcnm2# vi /root/packaged-files/properties/ha-setup.properties
```

**Step 8** Verify if the secondary node parameters are updated.



**Note** To setup Cisco DCNM Native HA successfully, it is important to use valid FQDN as hostname for both hosts while installing DCNM OVA/ISO. After installation, you must be able to ping the FQDN for both hosts. If the ping is not successful, the Native HA setup may fail.

**Step 9** If it is auto-populated and validated, install Native HA on the stand-by node, using the following command:

```
dcnm2# appmgr setup native-ha standby
```

On the active node, all the applications, excluding DHCP will be started. On the standby node only LDAP and AMQP will be enabled.

Launch the DCNM on the active node and enter the **POAP IP Range** on the Cisco DCNM **Web Client** > **Configure** > **POAP** > **DHCP Scope**. DHCP will be started automatically on both the active and standby nodes.

DCNM, XMPP and TFTP are automatically started on the standby node immediately after the active node stops working.

## Example for DCNM Native HA Installation

The example in this section considers the following parameters and shows how to install DCNM Native HA.

Parameter	Active	Standby	Virtual IP (VIP)
Eth0 IP	1.1.1.1/24	1.1.1.2/24	1.1.1.3/24
Eth1 IP	2.2.0.1/16	2.2.0.2/16	2.2.0.3/16
Hostname (FQDN)	dcnm1.cisco.com	dcnm2.cisco.com	dcnm3.cisco.com

On the active node, edit the property file by using the following command:

```
dcnm1# vi /root/packaged-files/properties/ha-setup.properties
```



---

```

#Copyright (c) 2017 by Cisco Systems, Inc.
#All rights reserved.
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=2
# Example:  NODE_ID=2
NODE_ID=2

# IPv4 address of the peer
# Example : PEER_ETH0_IP=10.197.67.20
PEER_ETH0_IP=10.197.67.20

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=10.197.67.24
VIP_ADDRESS=10.197.67.24

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=26
VIP_PREFIX=26

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth1
network)
# Example : VIP1_ADDRESS=10.197.67.25
VIP1_ADDRESS=10.197.67.25

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=26
VIP1_PREFIX=26

# Optional eth1 VIP address for IPv6 if configured. If not configured, leave them empty
# IPv6 address has to be in long format, no ':::' in it.
VIP1_ADDRESS_IPV6=
VIP1_PREFIX_IPV6=

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=dcnm24.cisco.com
VIP_FQDN=dcnm24.cisco.com

# NTP server IP address (1.2.3.4) or the hostname (clock.cisco.com)
NTP_SERVER=clock.cisco.com

```

---

On the standby node, check if the property values are updated in  
 /root/packaged-files/properties/ha-setup.properties

**dcnm2# vi /root/packaged-files/properties/ha-setup.properties**

---

```

#Copyright (c) 2017 by Cisco Systems, Inc.
#All rights reserved.
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=2
# Example:  NODE_ID=2
NODE_ID=2

# IPv4 address of the peer
# Example : PEER_ETH0_IP=10.197.67.20
PEER_ETH0_IP=10.197.67.20

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=10.197.67.24
VIP_ADDRESS=10.197.67.24

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=26
VIP_PREFIX=26

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth1
network)
# Example : VIP1_ADDRESS=10.197.67.25
VIP1_ADDRESS=10.197.67.25

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=26
VIP1_PREFIX=26

# Optional eth1 VIP address for IPv6 if configured. If not configured, leave them empty
# IPv6 address has to be in long format, no ':::' in it.
VIP1_ADDRESS_IPV6=
VIP1_PREFIX_IPV6=

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=dcnm24.cisco.com
VIP_FQDN=dcnm24.cisco.com

# NTP server IP address (1.2.3.4) or the hostname (clock.cisco.com)
NTP_SERVER=clock.cisco.com

```

---

**Note**

The Virtual IP (VIP) is seen on the active node. You can verify VIP by using the **ip address show** command.

---

## Running Cisco DCNM Behind a Firewall

For Windows PCs running Cisco DCNM-SAN, Device Manager, behind a firewall, certain ports need to be available.

By default, Cisco DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses. The UDP SNMP trap local ports are 1162 for Cisco DCNM-SAN, and 1163 or 1164 for Device Manager. Cisco DCNM-SAN Server also opens TCP RMI port 4447.

In DCNM Release 5.0(1) or later releases, you can select the UDP port that Fabric Manager Client or Device Manager uses for SNMP responses by uncommenting the following statement:

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

```
rem JVMARGS=%JVMARGS% -Dsnmp.localport=9001
```

- On a UNIX desktop, uncomment the following in the FabricManager.sh or DeviceManager.sh file in the \$HOME/.cisco\_mds9000/bin directory:

```
# JVMARGS=$JVMARGS -Dsnmp.localport=9001
```

From Cisco DCNM Release 6.3(1), DCNM San Client initiates communication with DCNM San Server on the following ports:

- 4447 for Java Remoting,
- 5457 and 5455 for Java Messaging Service.

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

The DCNM San Server component requires two predictable TCP ports to be opened on the firewall for an incoming connection:

- 4447 for Server
- 9100 for Server Data



#### Note

The Fabric Manager Client can connect to the server only if these two ports are open. Other TCP ports connected to DCNM San Client are initiated by the server, which is behind the firewall.

The following table lists all ports used by Cisco DCNM applications:

Communication Type	Port(s) Used
<b>Used by All Applications</b>	
SSH	Port 22 (TCP)
Telnet	Port 23 (TCP)
HTTP	Port 80 (TCP)
SLAPd	Port 636 (TCP)
LDAP	Port 389 (TCP)
XMPP/Jabber	Port 7400
TFTP	Port 69 (UDP)
RabbitMQ	Port 4369 (TCP)
Open AMQP	Port 5672 (TCP)
SNMP	Port 161 (UDP/TCP)
	<b>Note</b> DCNM configured via server.properties to use TCP will use TCP port 161 instead of UDP port 161.
Syslog	Port 514 (UDP)
<b>Used by Cisco DCNM-SAN Server and Performance Manager</b>	

Communication Type	Port(s) Used
SNMP_TRAP	Port 2162 (UDP)
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in <code>server.properties</code> .
Java Remoting	4447
Java Messaging	5457, 5455
<b>Used by Cisco DCNM-SAN Client</b>	
SNMP	Picks a random free local port (UDP) if SNMP proxy is enabled. Can be changed with the client <code>-Dsnmp.localport</code> option.
<b>Used by Device Manager</b>	
SNMP_TRAP	Picks a free local port between 1163 and 1170 (UDP).
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in <code>server.properties</code> .

The following table lists all the ports and descriptions:

Port(s) Used/Type	Service Descriptor	Service Name	Attribute Name	Description
80 or 443	Standalone/configuration/standalone-san.xml	JBoss http (or https) port	http (or https ) service for webclient, SOAP and REST API	http (or https ) service for webclient, SOAP and REST API
4447	Standalone/configuration/standalone-san.xml	jboss:service=Remoting	Remoting Service Port	This port is for JNDI-based naming services. The client look up this port for JNDI-binding objects and resources.
5455 5457	Standalone/configuration/standalone-san.xml	Messaging Service	Unified Invocation Layer for JMS	This port is used for JMS services.



# CHAPTER 4

## Installation of DCNM POAP Templates

---

Cisco DCNM allows you to add, edit or delete user-defined templates configured across different Cisco Nexus and Cisco MDS platforms. From Cisco DCNM Release 10.0(x), Cisco-defined DFA and VXLAN EVPN Programmable Fabric POAP templates are provided as a separate download on the official Cisco website. These templates are compatible for use with the DCNM Virtual Appliance (OVA or ISO) for use with Nexus 5000, Nexus 6000, Nexus 7000, and Nexus 9000 Series switches.

You can download the Cisco-defined templates from <https://software.cisco.com/download/release.html>.

This chapter contains the following:

- “POAP Templates for Cisco DCNM” section on page 4-1
- “Installing DCNM POAP Templates” section on page 4-2

## POAP Templates for Cisco DCNM

You can download the POAP templates for the Cisco DCNM Releases mentioned in this section. The Cisco DCNM 10.2.1 templates should be used for the new provisioning mode for LAN fabrics (also known as top down).



### Note

The templates in the *dcnm\_deprecated\_templates.10.1.1.ST.1.zip*, *dcnm\_deprecated\_templates.10.1.2.ST.1.zip*, and *dcnm\_deprecated\_templates.10.2.1.ST.1.zip*, files are being deprecated, and they will be dropped from future template zip releases.

### Cisco DCNM POAP Template Package Release 10.2(1)ST(1)

The following lists the POAP templates available for download:

- *dcnm\_ip\_vxlan\_fabric\_templates.10.2.1.ST.1.zip*
- *dcnm\_fabricpath\_fabric\_templates.10.2.1.ST.1.zip*
- *dcnm\_deprecated\_templates.10.2.1.ST.1.zip*

### Cisco DCNM POAP Template Package Release 10.1(2)ST(1)

The following lists the POAP templates available for download:

- *dcnm\_ip\_vxlan\_fabric\_templates.10.1.2.ST.1.zip*

- *dcnm\_fabricpath\_fabric\_templates.10.1.2.ST.1.zip*
- *dcnm\_deprecated\_templates.10.1.2.ST.1.zip*

## Cisco DCNM POAP Template Package Release 10.1(1)ST(1)

The following lists the POAP templates available for download:

- *dcnm\_ip\_vxlan\_fabric\_templates.10.1.1.ST.1.zip*
- *dcnm\_fabricpath\_fabric\_templates.10.1.1.ST.1.zip*
- *dcnm\_deprecated\_templates.10.1.1.ST.1.zip*

# Installing DCNM POAP Templates

This section provides you the procedure to install the Cisco DCNM POAP templates.

- [Installing Individual POAP Template from the Cisco DCNM Web Client, page 4-2](#)
- [Installing POAP Template from the Cisco DCNM Web Client, page 4-3](#)
- [Installing Templates Using Unzip and Restart, page 4-3](#)

## Installing Individual POAP Template from the Cisco DCNM Web Client

### Prerequisites

- Ensure that the Cisco DCNM is installed in the high availability mode or as Standalone DCNM ISO/OVA, Release 10.4(1)

### Detailed Steps

Perform the following tasks to install an individual POAP template from the Cisco DCNM Web Client.

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Navigate to <a href="https://cisco.com/go/dcnm">cisco.com/go/dcnm</a> and download the required template file.<br>For the list of available templates, see <a href="#">POAP Templates for Cisco DCNM, page 4-1</a> . |
| <b>Step 2</b> | Unzip the .zip files from your local drive.  |
| <b>Step 3</b> | Launch the Cisco DCNM Web Client and navigate to <b>Configure &gt; Templates &gt; Deploy</b> .   |
| <b>Step 4</b> | Roll over your mouse, find and click <b>Import Template</b> button (counter-clockwise arrow).  |
| <b>Step 5</b> | Select one of the templates from your local drive, and then click Open.  |
| <b>Step 6</b> | Repeat the above steps for additional individual template files.   |
-

## Installing POAP Template from the Cisco DCNM Web Client

### Prerequisites

- Ensure that the Cisco DCNM is installed in the high availability mode or as Standalone DCNM ISO/OVA, Release 10.4(1).

### Detailed Steps

Perform the following tasks to install the POAP templates from the Cisco DCNM Web Client.

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Navigate to <a href="https://cisco.com/go/dcnm">cisco.com/go/dcnm</a> and download the required template file.<br>For the list of available templates, see <a href="#">POAP Templates for Cisco DCNM, page 4-1</a> . |
| <b>Step 2</b> | Launch the Cisco DCNM Web Client and navigate to <b>Configure &gt; Templates &gt; Deploy</b> .   |
| <b>Step 3</b> | Click the <b>Import</b> button.  |
| <b>Step 4</b> | Select one of the template .zip files from your local drive, and then click Open.  |
| <b>Step 5</b> | Repeat the above steps for additional template zip files.  |
- 

## Installing Templates Using Unzip and Restart

This section contains the following:

- [Installing POAP Templates on a Standalone DCNM, page 4-3](#)
- [Installing POAP Templates in a Native HA setup, page 4-4](#)
- [Installing POAP Templates in an Oracle-based LVS High Availability Setup, page 4-5](#)

## Installing POAP Templates on a Standalone DCNM

### Prerequisites

- If it is a fresh installation of 10.4(1), ensure that the DCNM virtual appliance (ISO/OVA) is installed.
- If it is an upgraded setup (or a to be upgraded setup), ensure that the upgrade process is complete.

### Detailed Steps

Perform the following tasks to install the POAP Templates for Standalone DCNM.

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Navigate to <a href="https://www.cisco.com/go/dcnm">www.cisco.com/go/dcnm</a> and download the required template file.<br>For the list of available templates, see <a href="#">POAP Templates for Cisco DCNM, page 4-1</a> . |
| <b>Step 2</b> | SCP the .zip file to the DCNM home directory located at /root.   |
| <b>Step 3</b> | Unzip this .zip file into your templates location at <code>/usr/local/cisco/dcm/dcnm/data/templates</code> .<br>Example:   |

```
unzip -o -d /usr/local/cisco/dcm/dcnm/data/templates
dcnm_ip_vxlan_fabric_templates.10.2.1.ST.1.zip -x readme.txt
```

- Step 4** Restart DCNM appliance using the **appmgr restart dcnm** command.
- 

## Installing POAP Templates in a Native HA setup

### Prerequisites

- The following steps assume that the Native HA is already setup on the Cisco DCNM Release 10.4(1) and the applications are up and running.

### Detailed Steps

Perform the following tasks to install the POAP Templates for Cisco DCNM in a Native HA Setup.

---

- Step 1** Navigate to [www.cisco.com/go/dcnm](http://www.cisco.com/go/dcnm) and download the required template file.  
For the list of available templates, see [POAP Templates for Cisco DCNM, page 4-1](#).
- Step 2** SCP the .zip file to the DCNM home directory of both Active and Standby appliance, located at */root*.
- Step 3** On the Active peer, unzip the file to the templates location at */usr/local/cisco/dcm/dcnm/data/templates/*  
Example:  

```
unzip -o -d /usr/local/cisco/dcm/dcnm/data/templates
dcnm_ip_vxlan_fabric_templates.10.2.1.ST.1.zip -x readme.txt
```
- Step 4** Verify that the templates synchronize on the Standby at */usr/local/cisco/dcm/dcnm/data/templates*.



**Note** It may take a minute or more for the templates to get synchronized to the Standby.

---

- Step 5** Restart DCNM in the following sequence.
- Stop the Native HA applications on the Standby peer, using the **appmgr stop ha-apps** command.
  - Stop the Native HA applications on the Active peer, using the **appmgr stop ha-apps** command.
  - Start the Native HA applications on the Active peer, using the **appmgr start ha-apps** command.
  - Wait until all the applications are operational.
  - Start the Native HA applications on the Standby peer, using the **appmgr start ha-apps** command.
-



## Installing POAP Templates in an Oracle-based LVS High Availability Setup

### Prerequisites

- Ensure that the Oracle-based LVS HA is already setup.

### Detailed Steps

Perform the following tasks to install POAP templates for Cisco DCNM in an Oracle-based LVS High Availability setup.

- 
- Step 1** Navigate to [www.cisco.com/go/dcnm](http://www.cisco.com/go/dcnm) and download the required template file.  
For the list of available templates, see [POAP Templates for Cisco DCNM, page 4-1](#).
- Step 2** SCP the zip file to the DCNM home directory, located at */root*.
- Step 3** On the Active peer, unzip the .zip file to the templates location at */var/lib/dcnm/data/templates*  
Example:  

```
unzip -o -d /var/lib/dcnm/data/templates dcnm_ip_vxlan_fabric_templates.10.2.1.ST.1.zip -x  
readme.txt
```
- Step 4** Restart DCNM on both the peers in the following sequence.
- a. Stop DCNM on the Standby peer, using the **appmgr stop dcnm** command.
  - b. Stop DCNM on the Active peer, using the **appmgr stop dcnm** command.
  - c. Start DCNM on the Active peer, using the **appmgr start dcnm** command.
  - d. Wait until all the applications are operational.
  - e. Start DCNM on the Standby peer, using the **appmgr start DCNM** command.
-





# CHAPTER 5

## Upgrading Cisco DCNM

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

Cisco DCNM Installer version	Release from which you can upgrade
DCNM 10.4(1) ISO/OVA	<ul style="list-style-type: none"><li>• Cisco DCNM, Release 10.3(1)</li><li>• Cisco DCNM, Release 10.2(1)</li></ul>
DCNM 10.3(1) ISO/OVA	<ul style="list-style-type: none"><li>• Cisco DCNM, Release 10.2(1)</li><li>• Cisco DCNM, Release 10.0(1)</li></ul>
DCNM 10.2(1) ISO/OVA	<ul style="list-style-type: none"><li>• Cisco DCNM, Release 10.0(1)</li></ul>

You can migrate Cisco DCNM with a local PostgreSQL database and an external Oracle database and Cisco DCNM in a High Availability (HA) environment.



### Note

Cisco DCNM Release 10.1(x) allows the HA setup for XMPP uses external oracle database. You must provide username and password for external oracle database. Create a new username and password for the XMPP application to use in the same remote Database instance, used by the Cisco DCNM.



### Note

Before upgrading Cisco DCNM, ensure that automatic failover is disabled. Otherwise, if one server within the federation is down, the devices discovered by the server will be moved to the other DCNM server which comes up first after upgrade. To prevent the automatic failover for DCNM upgrade, you need to disable the automatic failover on all DCNMs within the federation, and then upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the automatic failover again. To enable / disable automatic failover, go to **Administration > DCNM Server > Federation** from DCNM web page, click the check box at top left for **Enable Automatic Failover**.



### Note

When upgrading to a newer DCNM version, you should use the same administrative password (as used in the existing setup) for the new DCNM setup. If you want to use a different password in the new setup, change the password in the existing DCNM setup before taking a backup and initiating the upgrade process.


This chapter contains the following:

- [Retaining the CA Signed Certificate, page 5-2](#)
- [Upgrading Cisco DCNM Windows and Linux through GUI Installation, page 5-2](#)
- [Upgrading Cisco DCNM Windows and Linux through Silent Installation, page 5-3](#)
- [Upgrading Cisco DCNM Windows and Linux Federation through GUI Installation, page 5-3](#)
- [Upgrading Cisco DCNM Windows and Linux Federation through Silent Installation, page 5-4](#)
- [Upgrading Cisco DCNM Virtual Appliance with External Oracle Database, page 5-6](#)
- [Upgrading Cisco DCNM appliances with Enhanced Fabric Management in HA Environment, page 5-7](#)
- [Upgrading Cisco DCNM Virtual Appliance with Local PostgreSQL Database, page 5-5](#)
- [Upgrading Cisco DCNM appliances without Enhanced Fabric Management in HA Environment, page 5-9](#)
- [Upgrading Cisco DCNM Native HA appliances, page 5-11](#)
- [Database Utility Scripts, page 5-13](#)

## Retaining the CA Signed Certificate

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

### DETAILED STEPS

- 
- Step 1** Backup the signed certificate from the location  
`<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks`
- Step 2** Upgrade to Cisco DCNM Release 10.4(1) based on the requirement.
- 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](#).
- 
- Step 4** Open the following files:
- `<Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/standalone-san.xml`
  - `<Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/ standalone-lan.xml`
- Step 5** Search for **key-alias="sme"** and replace with `key-alias=<key-alias used to create CA signed SSL Certificate>`
- Step 6** Restart the DCNM Services.
- 

## Upgrading Cisco DCNM Windows and Linux through GUI Installation

Before you begin, make sure that Cisco DCNM 10.0(1) or 10.2(1) is up and running.

- 
- Step 1** Stop the DCNM services.
- Step 2** Run the Cisco DCNM software for Release 10.4(1) 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 10.4(1) services will start automatically.
- 

## Upgrading Cisco DCNM Windows and Linux through Silent Installation

Before you begin, make sure that Cisco DCNM 10.0(1) or 10.2(1) is up and running.



### Note

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

### DETAILED STEPS

- 
- 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:
- For Windows installer—*dcnm-release.exe -i silent -f <path\_of\_installer.properties>*
  - For Linux installer—*dcnm-release.bin -i silent -f <path\_of\_installer.properties>*
- The Cisco DCNM Release 10.4(1) services will start after the upgrade is complete.



### Note

For Windows upgrade, you can check the status of the upgrade in the Task Manager process.

For Linux upgrade, 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 Windows and Linux Federation through GUI Installation

Before you begin, make sure that Cisco DCNM 10.0(1) or 10.2(1) is up and running.

**Note**

Ensure that both primary and secondary database properties are same.

- 
- Step 1** Stop both the primary and secondary DCNM services.
- Step 2** On the primary server, run the Cisco DCNM Release 10.4(1) executable file.  
Upgrade notification window appears.
- Step 3** Click **OK** to begin the upgrade.
- Step 4** On the secondary server, perform run the Cisco DCNM Release 10.4(1) executable file.  
Upgrade notification window appears.
- Step 5** Click **OK** to begin the upgrade.
- Step 6** On the primary server, click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.4(1) services will start automatically on the primary server.
- Step 7** On the secondary server, click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.4(1) services will start automatically on the secondary server.
- 

## Upgrading Cisco DCNM Windows and Linux Federation through Silent Installation

Before you begin, make sure that Cisco DCNM 10.0(1) or 10.2(1) is up and running.

**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.

- 
- 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:
- For Windows installer—`dcnm-release.exe -i silent -f <path_of_installer.properties>`
  - For Linux installer—`dcnm-release.bin -i silent -f <path_of_installer.properties>`

**Note**

For Windows upgrade, you can check the status of the upgrade in the Task Manager process.

For Linux upgrade, 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.

- 
- Step 4** On the secondary server, open the *installer.properties* file and update the following properties:
- ```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
SAN_FEDERATION=TRUE
```
- Step 5** Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:
- For Windows installer—*dcnm-release.exe -i silent -f <path\_of\_installer.properties>*
  - For Linux installer—*dcnm-release.bin -i silent -f <path\_of\_installer.properties>*
- Step 6** On the primary server, click **Done** after the upgrade is complete.  
 The Cisco DCNM Release 10.2(x) services will start automatically on the primary server.
- Step 7** On the secondary server, click **Done** after the upgrade is complete.  
 The Cisco DCNM Release 10.2(x) services will start automatically on the secondary server.
- 

## Upgrading Cisco DCNM Virtual Appliance with Local PostgreSQL Database

Before you begin, make sure that Cisco DCNM 10.0(1) or 10.2(1) is up and running.

- 
- Step 1** Use the **appmgr backup all** command to backup all applications associated with the installation of Cisco DCNM 10.0(x).  
 A prompt appears to provide the DCNM DB password and XMPP DB password. By default, this password is the administrative password provided during the Open Virtual Appliance installation.
- Step 2** On Cisco DCNM 10.4(1), ensure that the MAC addresses along with all network settings such as the IP address, default gateway, hostname, etc., are identical to the Cisco DCNM 10.0(x) installation.
- Step 3** Transfer the backup file to an external file system.
- Step 4** Power off Cisco DCNM 10.0(x).
- Step 5** Deploy the Cisco DCNM Open Virtual Appliance file for version 10.4(1).
- Use the same network parameters (IP address/subnet/gateway/DNS).
  - Use the same administrative password.
  - Use the same vCenter port groups for both network interfaces.
  - Disable auto-power-on. (The Power on Open Virtual Appliance after deployment check-box should not be selected).
- Step 6** After Cisco DCNM 10.4(1) is deployed, right-click on **VM > Edit Settings > Hardware**.  
 For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.0(x). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.

- Step 7** Power on DCNM 10.4(1) VM.
- Step 8** Copy the Cisco DCNM 10.0(x) backup file from the external repository to Cisco DCNM 10.4(1).
- Step 9** Use the **appmgr status all** status all command to make sure that all applications are up and running.
- Step 10** Use the **appmgr stop all** to shut down all applications on Cisco DCNM 10.4(1).
- Step 11** Use the **appmgr upgrade <backup filename>** command to run the upgrade script on Cisco DCNM 10.4(1).

The application displays the following message:

```
Please Shut Down All Applications Before Continuing.
Press 'y' to continue [y/n] [n]
```

- Step 12** Press **Y** to continue.

```
Press [1] or [2] or [3] when prompted, based on your Cisco DCNM 7.2.x setup:
Choose [1] Standalone DCNM with Local PostgreSQL database
[2] Standalone DCNM with External Oracle database
[3] High Availability
[4] Native High Availability
```

If you choose option [1] Standalone DCNM with Local PostgreSQL database, It will get upgraded successfully.

If you choose option [2] Standalone DCNM with External Oracle database, ensure that the external database is up and running. For more information, see [Upgrading Cisco DCNM Virtual Appliance with External Oracle Database, page 5-6](#).

## Upgrading Cisco DCNM Virtual Appliance with External Oracle Database

Perform the following procedure to upgrade Cisco DCNM Virtual Appliance with external Oracle database.



### Note

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-20](#).

When you select Option [2] in [Step 12](#) of the procedure [Upgrading Cisco DCNM Virtual Appliance with Local PostgreSQL Database, page 5-5](#), the following query appears:

Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?

```
Press 'y' to continue [y/n] [n]
```

- Step 1** Press **Y** to continue.
- Step 2** Enter the DB URL.

```
Example: jdbc:oracle:thin:@10.2.3.4:1521:XE
```



- Step 3** Enter the DB username
- Step 4** Enter the DB password.  
Enter it again for verification:
- Step 5** Enter the administrative password provided during Virtual Appliance installation, when prompted for the root password.
- The external DCNM database will be configured to access all the Fabric applications using the root password of this server.

**Note**

You can change the password using the Cisco DCNM Web Client. To change the password, choose **Administration > Management Users > Local**.

**Note**

Upgrading from Non-DFA to Cisco DCNM 10.4(1) with a Local PostgreSQL or External Oracle Database. Deploy the Cisco DCNM 10.4(1) with the Enhanced Fabric Management Network fields with default values (i.e., IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0 and DNS IP: 1.1.1.1). Perform the procedure detailed in [Upgrading Cisco DCNM Virtual Appliance with External Oracle Database, page 5-6](#).

**Note**

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-20](#).

## Upgrading Cisco DCNM appliances with Enhanced Fabric Management in HA Environment

Before you begin, ensure that:

- Both the Cisco DCNM 10.2(1) Active and Standby peers are up and running.
- Automatic failover is stopped manually. To disable automatic failover, go to **Administration > DCNM Server > Federation** in the DCNM web page, and clear the Enable Automatic Failover check box at the top left part of the screen.

**Note**

For more information on Active and Standby peers in a High Availability environment, see [“Managing Applications in a High-Availability Environment”](#).

- Step 1** Verify if the **appmgr backup all** command was executed on both the Active and Standby peers. Check if separate tar archives are stored in an external file system.

Example: `active.tar.gz` and `standby.tar.gz`

**Note**

If it is the non-DFA environment, please verify if the **appmgr backup dcnm** command was executed on both the Active and Standby peers.

- Step 2** Power off the Cisco DCNM 10.2(1) Active peer.
- Step 3** Power-on the Cisco DCNM 10.4(1) Active peer.
- Step 4** Use the **appmgr status all** command to ensure that all the applications are up and running on the Cisco DCNM 10.4(1) Active peer.
- Step 5** Stop all DCNM applications on the Cisco DCNM 10.4(1) Active peer, by using **appmgr stop all** command.
- Step 6** Use the **appmgr upgrade <active.tar.gz>** command to run the upgrade script.
- a. PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING.  
Press 'y' to continue [y/n] [n]  
y
  - b. Choose option [3] High Availability when prompted.  
Choose option [1] Standalone DCNM with Local PostgreSQL database  
[2] Standalone DCNM with External Oracle database  
[3] High Availability  
[4] Native High Availability
  - c. Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?  
Press 'y' to continue [y/n] [n]  
y
  - d. Select option [1] Active when prompted.  
Choose [1] Active [2] Standby
  - f. Enter the standby eth0 IP address.  
After the upgrade is completed successfully, you will see the following message:  
\*\*\*\* Check /root/upgrade.log for details...\*\*\*\*  
Ensure that all applications are running on the Cisco DCNM 10.4(1) Active peer.
- Step 7** Power off the Cisco DCNM 10.2(1) Standby peer.
- Step 8** Power on the Cisco DCNM 10.4(1) Standby peer. Use the **appmgr status all** command to make sure that all applications are up and running.
- Step 9** Stop all applications on the Cisco DCNM 10.4(1) Standby peer.
- Step 10** Run the below NTP command on the standby to synchronize the time.  
**ntpdate -b -u NTP\_SERVER\_IPADDRESS**
- Step 11** Use the **appmgr upgrade <standby.tar.gz>** command to run the upgrade script on the Cisco DCNM 10.4(1) Standby peer.
- a. Choose option [3] **High Availability** when prompted.  
Choose option [1] Standalone DCNM with Local PostgreSQL database  
[2] Standalone DCNM with External Oracle database  
[3] High Availability  
[4] Native High Availability
  - b. Select option [2] **Standby** when prompted.  
Choose [1] Active [2] Standby

To migrate the standby peer, perform the following:

- a. Enter the active **eth0 IP** address.

**Step 12** Invoke the following on the Active peer to establish SSH trust to the Standby peer:

```
sh /root/sshAutoLogin.sh <STANDBY_PEER_IP>
```

**Step 13** Restart the active Cisco DCNM, using the **appmgr restart dcnm** command.



**Note**

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-20](#).

## Upgrading Cisco DCNM appliances without Enhanced Fabric Management in HA Environment

Before you begin, ensure that:

- The virtual appliance is installed in Non Programmable Fabric mode.
- Automatic failover is stopped manually. To disable automatic failover, go to **Administration > DCNM Server > Federation** in the DCNM web page, and clear the Enable Automatic Failover check box at the top left part of the screen.



**Note**

For instruction about installing these applications with the Cisco DCNM Open Virtual Appliance, see [DCNM installation without Enhanced Fabric Management capabilities, page 3-20](#). For more information on NON DFA High Availability environment, see [Managing Applications in a High-Availability Environment, page 7-1](#).

**Step 1** Make sure that both Cisco DCNM DCNM 10.3(x) servers are deployed, powered on and made it as a First and Federated node by using the below commands.

```
appmgr setup ha -type first-node
```

```
appmgr setup ha -type federated-node
```

**Step 2** Verify if the **appmgr backup dcnm** command was executed on both the First Node and Federated Node using the below command. Check if separate tar archives are stored in an external file system.

```
Example: first_node.tar.gz
         federated_node.tar.gz
```

**Step 3** Bring up the DCNM 10.4(x) First and Federated node. Do not power on the DCNM yet.

**Step 4** Power off the Cisco DCNM 10.3(x) First and Federated Node virtual appliance.

**Step 5** Power-on the Cisco DCNM 10.4(x) First and Federated Node virtual appliance which should be deployed in the same eth0 IP of 10.3(x).

**Note**

While deploying Cisco DCNM 10.4(x) First and Federated Node virtual appliance, the Enhanced Fabric Management Network fields must contain default values (i.e., IP Address:0.0.0.0, Subnet Mask:0.0.0.0 and DNS IP:1.1.1.1)

**Step 6** Use the **appmgr status all** command to ensure that DCNM applications are up and running on the Cisco DCNM 10.4(x) First and Federated Nodes.

**Step 7** Stop the applications on the Cisco DCNM 10.4(x) First node, by using **appmgr stop dcnm** command.

**Step 8** Use the command **appmgr upgrade <first\_node.tar.gz>** on the Cisco DCNM 10.4(x) First node to run the upgrade script. After issuing **appmgr upgrade <first\_node.tar.gz>** on First Node, user will be prompted for various inputs. Provide the inputs as per the sample given below.

```
PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING. .
```

```
Press 'y' to continue [y/n]
```

```
y
```

```
Select an option for upgrading this appliance [ ] :
```

```
[1] Standalone DCNM with Local PostgreSQL database
```

```
[2] Standalone DCNM with External Oracle database
```

```
[3] High Availability
```

```
[4] Native High Availability
```

```
Choice [1|2|3|4]
```

```
3
```

```
Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?
```

```
Press 'y' to continue [y/n]
```

```
y
```

```
Please enter the type of server:
```

```
[1] First Node | [2] Federated Node
```

```
1
```

```
*****
```

```
You are about to be federated for DCNM alone in this DCNM appliance.
```

```
Please make sure that you have the following
```

```
1. An Oracle Database with a user defined for DCNM.
```

```
2. A repository with NFS capabilities.
```

```
3. An NTP server for time synchronization.
```

```
*****
```

```
a) Do you want to continue? [y/n] [y]
```

```
b) Enter the DB URL {ex. jdbc:oracle:thin:@ipaddr:1521:<SID or Servicename>} :
```

```
c) Enter the DB username for DCNM tables: <dcnm-dbuser>
```

```
d) Enter the DB password for DCNM tables:
```

```
e) Enter it again for verification:
```

```
f) Enter the SCP/NFS repository IP : <repository IP>
```

```
g) NFS Exported location {ex. /var/shared/dcnm/} :
```

```
h) Enter an NTP server for time synchronization "NTP_SERVER":
```

```
*****Successfully Completed. Run 'appmgr start dcnm'*****
```

```
i) Verify whether HA Federation enabled after upgrade by using command appmgr show ha-role.
```

```
j) Start DCNM using appmgr start dcnm.
```

**Step 9** Stop DCNM applications on the Cisco DCNM 10.4(x) Federated Node by using **appmgr stop dcnm** command.

**Step 10** Run the below NTP command on standby to sync the time.

**ntpdate -b -u clock.cisco.com**

- Step 11** Use the **appmgr upgrade <federated\_node.tar.gz>** command to run the upgrade script on the Cisco DCNM 10.4(x) Federated Node. After issuing **appmgr upgrade <first\_node.tar.gz>** on First Node, user will be prompted for various inputs. Provide the inputs as per the sample given below.

```
PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING..
```

```
Press 'y' to continue [y/n]
```

```
y
```

```
Select an option for upgrading this appliance [] :
```

```
[1] Standalone DCNM with Local PostgreSQL database
```

```
[2] Standalone DCNM with External Oracle database
```

```
[3] High Availability
```

```
[4] Native High Availability
```

```
Choice [1|2|3|4]
```

```
3
```

```
Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?
```

```
Press 'y' to continue [y/n]
```

```
y
```

```
Please enter the type of server :
```

```
[1] First Node | [2] Federated Node
```

```
2
```

```
*****
```

```
You are about to enable High Availability for DCNM alone in this DCNM appliance. Please make sure that you have the following:
```

```
1. An Existing Federated server.
```

```
*****
```

```
a) Do you want to continue? [y/n] [y]
```

```
b) Enter the existing Federated server IP (eth0 IP) : <PEER_ETH0_IP>
```

```
c) Enter the root password of the peer
```

```
d) Root password : <root_password_of_this_node>
```

```
***** Successfully Completed.*****
```

## Upgrading Cisco DCNM Native HA appliances

Perform the following to upgrade the Cisco DCNM Native HA appliances to Release 10.4(1).

Before you begin, ensure that both the Cisco DCNM 10.2(1) Active and Standby peers are up and running.

- 
- Step 1** Verify if the **appmgr backup all** command was executed on both the Active and Standby peers. Check if separate **.tar** archives are stored in an external file system.
- Step 2** Power off the Cisco DCNM 10.2(1) Standby host first and then power off the Active host.
- Step 3** Power on the Cisco DCNM 10.4(1) Active host, and then power on the Standby host with the same IP and MAC address.

If both eth0 and eth1 interfaces are in the same subnet, edit the `/etc/sysctl.conf` file for DCNM ISO Virtual appliance Native HA installation on both active and standby nodes for both the appliances, as follows:

- Change the value of `net.ipv4.conf.default.rp_filter` from **1** to **2**.
- Add **`net.ipv4.conf.all.rp_filter = 2`** to the `sysctl.conf` file.

Save and close the file. On the SSH terminal, execute the **`sysctl --system`** command.

**Step 4** Ensure that all the applications are up and running on the Cisco DCNM 10.4(1) Active host. Use the **`appmgr status all`** command to ensure that

**Step 5** Stop all the DCNM applications on the Cisco DCNM 10.4(1) Active host, by using **`appmgr stop all`** command.

**Step 6** Transfer the backup file from the external file system to the corresponding setup.

**Step 7** Run the upgrade script on the Active host, by using the **`appmgr upgrade <active.tar.gz>`** command.

**Step 8** Provide the inputs as per the sample given below.

```
PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING.
Press 'y' to continue [y/n]
y
```

```
Select an option for upgrading this appliance [] :
[1] Standalone DCNM with Local PostgreSQL database
[2] Standalone DCNM with External Oracle database
[3] High Availability
[4] Native High Availability
Choice [1|2|3|4]
4
```

```
Choose [1] Active
[2] Standby
1
```

```
You are about to enable Native High Availability on this DCNM virtual appliance.
Please make sure that you have the following
1. A couple of free IP addresses to be used as Virtual IPs (one on each port group)
2. A peer DCNM deployed with the same user profile (same username/password)
3. Shut down all applications in this server using 'appmgr stop all'
*****
Do you want to continue? [y/n]
y
```

**Step 9** Stop all the DCNM applications on the Cisco DCNM 10.4(1) Standby host, by using **`appmgr stop all`** command.

**Step 10** Run the upgrade script on the Standby host, by using the **`appmgr upgrade <standby.tar.gz>`** command.

**Step 11** Provide the inputs as per the sample given below.

```
PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING.
Press 'y' to continue [y/n]
y
```

```
Select an option for upgrading this appliance []:
[1] Standalone DCNM with Local PostgreSQL database
[2] Standalone DCNM with External Oracle database
[3] High Availability
[4] Native High Availability
Choice [1|2|3|4]
4
```

```
Choose [1] Active
[2] Standby
2
```

```

You are about to enable Native High Availability on this DCNM virtual appliance.
Please make sure that you have the following
1. A couple of free IP addresses to be used as Virtual IPs (one on each port group)
2. A peer DCNM deployed with the same user profile (same username/password)
3. Shut down all applications in this server using 'appmgr stop all'
*****
Do you want to continue? [y/n]
Y

```

---

## Database Utility Scripts

### 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

### 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 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.

---





## CHAPTER 6

# Managing Applications After DCNM Deployment

This chapter describes how to verify and manage all of the applications that provide DC3 (Programmable Fabric) central point of management functions after the DCNM is deployed. This chapter includes the following sections:

- [Cisco DCNM Applications, page 6-1](#)
- [Application Details, page 6-2](#)
- [Managing Applications, page 6-8](#)
- [Backing Up Cisco DCNM and Application Data, page 6-12](#)
- [Restoring Applications, page 6-14](#)
- [Updating the SFTP Server Address for IPv6, page 6-15](#)



### Note

For information about managing these applications in a high-availability (HA) environment, see [“Managing Applications in a High-Availability Environment” section on page 7-1](#).

## Cisco DCNM Applications

A complete list of applications included in Cisco DCNM that provide Cisco Programmable Fabric is in [Table 6-1](#). Information about these applications and the corresponding login credentials are included.

**Table 6-1** *Cisco DCNM Applications*

| Category           | Application                                     | Username                                                         | Password                                                         | Protocol Implemented                           |
|--------------------|-------------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------------|
| Network Management | Data Center Network Manager                     | admin                                                            | User choice <sup>1</sup>                                         | Network Management                             |
| Network Services   | Cisco Prime Network Services Controller Adapter | created by Cisco Prime Network Services Controller administrator | Created by Cisco Prime Network Services Controller administrator | Network services (firewall and load balancing) |

| Category                          | Application                                           | Username                                              | Password                 | Protocol Implemented                       |
|-----------------------------------|-------------------------------------------------------|-------------------------------------------------------|--------------------------|--------------------------------------------|
| Orchestration                     | RabbitMQ                                              | admin                                                 | User choice <sup>1</sup> | Advanced Messaging Queuing Protocol        |
| Orchestration                     | OpenLDAP                                              | cn=admin<br>dc=cisco<br>dc=com                        | User choice <sup>1</sup> | Lightweight Directory Access Protocol      |
| Group Provisioning of Switches    | Cisco Jabber Extensible Communications Platform (XCP) | admin@fully qualified domain name (FQDN) <sup>2</sup> | User choice <sup>1</sup> | Extensible Messaging and Presence Protocol |
| Device Power On Auto-Provisioning | DHCP                                                  | —                                                     | —                        | Dynamic Host Configuration Protocol        |
| Device Power on Auto-Provisioning | TFTP servers <sup>2</sup><br>SSH/SFTP server          | —                                                     | —                        | Trivial File Transfer Protocol             |

<sup>1</sup>User choice refers to the administration password entered by the user during the deployment.

<sup>2</sup>FQDN is the one that was entered during deployment

<sup>2</sup>Place the files that you want to be accessed from outside through TFTP at /var/lib/dcnm/.

## Application Details

This section describes the details of all the applications within the functions they provide in Cisco DCNM. The functions are as follows:

- Network Management
- Network Services
- Orchestration
- Power On Auto Provisioning (POAP)
- Group provisioning of switches

## Network Management

The data center network management function is provided by the Cisco Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser: [http://\[host/ip\]](http://[host/ip]).



### Note

For more information about Cisco DCNM, see <http://cisco.com/go/dcnm>

## Network Services

In the Cisco Programmable Fabric solution, traditional services, such as firewalls and load balancers, are deployed at regular leaf nodes within the spine-leaf topology, and at border leaf nodes, unlike more traditional data centers where these services are deployed at the aggregation layer.

Cisco Prime Network Services Controller (NSC) provides the orchestration and automation of network services in Cisco Programmable Fabric. The Prime NSC supports integration with virtual computer and storage managers such as vCenter and System Center Virtual Machine Manager (SCVMM) and provides end-to-end orchestration and automation for services in Cisco Programmable Fabric.

**Note**

For more information about the Prime NSC, see the Cisco Prime Network Services Controller documentation at the following URL:

[http://www.cisco.com/en/US/partner/products/ps13213/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/partner/products/ps13213/tsd_products_support_series_home.html).

A Prime NSC Adapter is bundled within the Cisco DCNM. It performs the following functions:

- Enables DCNM to interoperate with one or more instances of the Prime NSC.
- Provides translation of DCNM language and objects into the Prime NSC language and objects.
- Ensures that the Prime NSC and DCNM are always synchronized.
- Maps the tenants and virtual data centers to the Prime NSC instances responsible for network services

**Note**

The Prime NSC Adapter supports DCNM-to-Prime NSC integration for multiple Prime NSC instances. A single Prime NSC instance is not able to fulfill Programmable Fabric scalability requirements for tenants and VMs. Consequently, multiple instances are required to achieve the scale that Programmable Fabric requires.

## Config Profiles

When you are using autoconfiguration for Programmable Fabric, the network is associated with a configuration profile (config profile). A config profile template instance is created on leaf nodes wherever a network appears. When using services in the Cisco Prime Network Services Controller (NSC), you must select the correct config profile to orchestrate and automate the services in the Programmable Fabric network.

[Table 6-2](#) includes the sample guidelines for edge firewall with regards to selecting config profiles when you are using services.

**Table 6-2 Service configuration profiles**

| Service Node                           | Network                           | Routing | Service Profile                                                                                                                                                                           |
|----------------------------------------|-----------------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edge Firewall                          | Host Networks                     | N/A     | defaultNetworkIpv4EfESProfile                                                                                                                                                             |
|                                        |                                   |         | defaultNetworkIpv4TfESProfile                                                                                                                                                             |
|                                        | Tenant Service Network            | Static  | serviceNetworkIpv4TfStaticRoutingESProfile                                                                                                                                                |
|                                        |                                   | Dynamic | serviceNetworkIpv4DynamicRoutingESProfile                                                                                                                                                 |
|                                        | Tenant-Ext Service Network        | Static  | externalNetworkIpv4TfStaticRoutingESProfile                                                                                                                                               |
|                                        |                                   | Dynamic | externalNetworkIpv4DynamicRoutingESProfile                                                                                                                                                |
| Compute Firewall (L3 vPath)            | Host Networks                     | N/A     | defaultNetworkIpv4EfProfile<br>defaultNetworkIpv4TfProfile                                                                                                                                |
|                                        | Tenant Service Network            | N/A     | serviceNetworkIpv4TfL3VpathServiceNodeProfile                                                                                                                                             |
|                                        | Tenant Service Classifier Network | N/A     | serviceNetworkIpv4EfL3VpathServiceClassifierProfile                                                                                                                                       |
| Compute Firewall (L2 vPath)            | Host Networks                     | N/A     | defaultNetworkIpv4EfProfile<br>defaultNetworkIpv4TfProfile                                                                                                                                |
|                                        | Tenant Service Network            | N/A     | serviceNetworkL2VpathProfile                                                                                                                                                              |
| Service Node as Router/Default Gateway | Host Networks                     | N/A     | defaultNetworkL2Profile                                                                                                                                                                   |
| Load Balancer                          | Host Networks                     | N/A     | defaultNetworkIpv4TfStaticRoutingLBProfile/<br>defaultNetworkIpv4TfDynamicRoutingLBProfile/<br>defaultNetworkIpv4EfDynamicRoutingLBProfile/<br>defaultNetworkIpv4EfStaticRoutingLBProfile |
|                                        |                                   |         |                                                                                                                                                                                           |
|                                        | Tenant Service Network            | Static  | serviceNetworkIpv4TfStaticRoutingLBProfile                                                                                                                                                |
|                                        |                                   | Dynamic | serviceNetworkIpv4DynamicRoutingLBProfile                                                                                                                                                 |
| Load Balancer + Edge Firewall          | Host Networks                     | N/A     | defaultNetworkIpv4EfChainLBESProfile/<br>defaultNetworkIpv4TfChainLBESProfile                                                                                                             |
|                                        | Load Balancer Service Network     | Dynamic | serviceNetworkIpv4ESChainLBESProfile                                                                                                                                                      |
|                                        | Edge Firewall Service Network     | Dynamic | serviceNetworkIpv4LBChainLBESProfile                                                                                                                                                      |

## Universal config profile selection for Load Balancer and Edge Services

From Cisco DCNM Release 7.1.1, the universal configuration profiles are to decouple network profiles from VRF profiles, and therefore, allowing you to choose the network/VRF profile combination which best suits your requirement.

The table below shows how to use those universal profiles for a few cases with load balancers and (tenant) edge routers, depending on how such services are deployed.

**Table 6-3**

| Load balancer        | Edge Router          | Internal vrf profile               | External vrf profile                     | Internal Host network profile                                        | Internal LB service network profile             | Internal ES service network profile            | External service network profile   |
|----------------------|----------------------|------------------------------------|------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------|------------------------------------------------|------------------------------------|
| No                   | No                   | vrf-common-universal               | N/A                                      | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | N/A                                             | N/A                                            | N/A                                |
| Yes, static routing  | No                   | vrf-common-universal-static        | N/A                                      | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | serviceNetworkUniversalTfStaticRoutingProfile   | N/A                                            | N/A                                |
| Yes, dynamic routing | No                   | vrf-common-universal-dynamic-LB-ES | N/A                                      | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | serviceNetworkUniversalDynamicRoutingLBPProfile | N/A                                            | N/A                                |
| No                   | Yes, static routing  | vrf-common-universal               | vrf-common-universal-external-static     | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | N/A                                             | serviceNetworkUniversalTfStaticRoutingProfile  | externalUniversalTfStaticRoutingES |
| No                   | Yes, dynamic routing | vrf-common-universal-dynamic-LB-ES | vrf-common-universal-external-dynamic-ES | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | N/A                                             | serviceNetworkUniversalDynamicRoutingESProfile | externalUniversalDynamicRoutingES  |

Table 6-3

| Load balancer        | Edge Router          | Internal vrf profile               | External vrf profile                     | Internal Host network profile                                        | Internal LB service network profile            | Internal ES service network profile               | External service network profile        |
|----------------------|----------------------|------------------------------------|------------------------------------------|----------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------|-----------------------------------------|
| Yes, static routing  | Yes, static routing  | vrf-common-universal-static        | vrf-common-universal-external-static     | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | serviceNetworkUniversalTfStaticRoutingProfile  | serviceNetworkUniversalTfStaticRoutingProfile     | externalUniversalTfStaticRoutingProfile |
| Yes, static routing  | Yes, dynamic routing | vrf-common-universal-static        | vrf-common-universal-external-dynamic-ES | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | serviceNetworkUniversalTfStaticRoutingProfile  | serviceNetworkUniversalESChainedStaticLBESProfile | externalUniversalTfStaticRoutingProfile |
| Yes, dynamic routing | Yes, static routing  | vrf-common-universal-dynamic-LB-ES | vrf-common-universal-external-static     | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | serviceNetworkUniversalDynamicRoutingLBProfile | serviceNetworkUniversalTfStaticRoutingProfile     | externalUniversalTfStaticRoutingProfile |
| Yes, dynamic routing | Yes, dynamic routing | vrf-common-universal-dynamic-LB-ES | vrf-common-universal-external-dynamic-ES | defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles | serviceNetworkUniversalDynamicRoutingLBProfile | serviceNetworkUniversalESChainedLBESProfile       | externalUniversalTfStaticRoutingProfile |

## Orchestration

Three components provide orchestration functions.

- RabbitMQ

Rabbit MQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP). The RabbitMQ message broker sends events from the vCloud Director/vShield Manager to the Python script for parsing. You can configure this protocol by using certain CLI commands from the Secure Shell (SSH) console of the firmware.

**Note**

You need to stop and restart AMQP on both DCNM's server in HA within 30 seconds, otherwise AMQP may not start.

For more information about RabbitMQ, go to <http://www.rabbitmq.com/documentation.html>

- Python Integration Script

The orchestration Python script receives and parses events from VMware's vCloud Director/vShield Manager through the RabbitMQ message broker. It communicates with vCloud Director/vShield Manager through web service APIs for detailed information and then calls Cisco DCNM REST APIs to populate data that is to be used by the fabric.

The Python integration scripts and the configuration files in the DCNM Open Virtual Appliance are as follows:

`/root/utils/vCDclient.py`

`/root/utils/vCDclient-ini.conf`

You should edit the `vCDclient-ini.conf` file with your specific information and start the integration using Python2.7 as `python2.7 vCDclient.py`

**Tip**

By invoking the script with the Python command, you will invoke the default Python 2.6 version, which might fail; the integration script requires certain modules that are available only in Python 2.7.

- OpenLightweight Directory Access Protocol (LDAP)

The DCNM Open Virtual Appliance installs LDAP that serves as an asset database to the switches.

**Note**

From Cisco DCNM Release 7.1.x, during installation of Virtual Appliances, Secure LDAP is enabled by default on Port 636.

## Device Power On Auto Provisioning

Power On Auto Provisioning (POAP) occurs when a switch boots without any startup configuration. It is accomplished by two components that were installed:

- DHCP Server

The DHCP server parcels out IP addresses to switches in the fabric and points to the location of the POAP database, which provides the Python script and associates the devices with images and configurations.

During the Cisco DCNM installation, you define the IP Address for the inside fabric management address or OOB management network and the subnets associated with the Cisco Programmable Fabric management.

**Note**

You should always configure DHCP through Cisco DCNM web UI by choosing: **UI > Configure > POAP > DHCP Scopes**. Editing the `/etc/dhcp/dhcp.conf` file from an SSH terminal might lead to unexpected behavior.

- Repositories

The TFTP server hosts boot scripts that are used for POAP.

The SCP server downloads the database files, configuration files, and the software images.

## Group Provisioning of Switches

You can accomplish group provisioning of switches by using the Extensible Messaging and Presence Protocol (XMPP) server. Through the XMPP server and Cisco Jabber, you have access to all devices in the fabric and can create chat groups of spines and leaves for group provisioning of switches.

The initial XMPP configuration can be done through the Cisco DCNM web UI by choosing: **Configure > LAN Fabric Settings > General**.



### Note

Before a switch can participate in XMPP, it must be added to the XMPP database by using the **appmgr** CLI command shown in [Table 6-4](#). See the “[XMPP User and Group Management](#)” section on [page 6-10](#) for information.

## Managing Applications

You can manage the applications for Cisco Programmable Fabric in the Cisco DCNM through commands in an SSH terminal.

Enter the **appmgr** command from the SSH terminal by using the following credentials:

- Username: root
- Password: Administrative password provided during deployment.



### Note

For your reference, context sensitive help is available for the **appmgr** command. Use the **appmgr** command to display help.

Use the **appmgr tech\_support** command to produce a dump of the log files. You can then provide this information to the TAC team for troubleshooting and analysis of your setup.



### Note

This section does not describe commands for Network Services using Cisco Prime Network Services Controller.

This section includes the following:

- [Verifying the Application Status after Deployment, page 6-9](#)
- [Stopping, Starting, and Resetting Applications, page 6-9](#)
- [XMPP User and Group Management, page 6-10](#)
- [Change from Local Database to an External Database, page 6-11](#)
- [Change password for Linux root user, page 6-12](#)



## Verifying the Application Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of the applications that were deployed in the file. You can use the **appmgr status** command in an SSH session to perform this procedure.



### Note

Context-sensitive help is available for the **appmgr status** command. Use the **appmgr status ?** command to display help.

### DETAILED STEPS

- Step 1** Open up an SSH session:
- Enter the **ssh root *DCNM network IP address*** command.
  - Enter the *administrative password* to login.
- Step 2** Check the status of the applications by entering this command:

```
appmgr status all
```

#### DCNM Status

| PID  | USER | PR | NI | VIRT  | RES  | SHR | S | %CPU | %MEM | TIME+   | COMMAND |
|------|------|----|----|-------|------|-----|---|------|------|---------|---------|
| 1891 | root | 20 | 0  | 2635m | 815m | 15m | S | 0.0  | 21.3 | 1:32.09 | java    |

#### LDAP Status

| PID  | USER | PR | NI | VIRT | RES | SHR  | S | %CPU | %MEM | TIME+   | COMMAND |
|------|------|----|----|------|-----|------|---|------|------|---------|---------|
| 1470 | ldap | 20 | 0  | 692m | 12m | 4508 | S | 0.0  | 0.3  | 0:00.02 | slapd   |

#### AMQP Status

| PID  | USER | PR | NI | VIRT  | RES | SHR | S | %CPU | %MEM | TIME+   | COMMAND  |
|------|------|----|----|-------|-----|-----|---|------|------|---------|----------|
| 1504 | root | 20 | 0  | 52068 | 772 | 268 | S | 0.0  | 0.0  | 0:00.00 | rabbitmq |

#### TFTP Status

| PID  | USER | PR | NI | VIRT  | RES  | SHR | S | %CPU | %MEM | TIME+   | COMMAND |
|------|------|----|----|-------|------|-----|---|------|------|---------|---------|
| 1493 | root | 20 | 0  | 22088 | 1012 | 780 | S | 0.0  | 0.0  | 0:00.00 | xinetd  |

#### DHCP Status

| PID  | USER   | PR | NI | VIRT  | RES  | SHR | S | %CPU | %MEM | TIME+   | COMMAND |
|------|--------|----|----|-------|------|-----|---|------|------|---------|---------|
| 1668 | dhcpcd | 20 | 0  | 46356 | 3724 | 408 | S | 0.0  | 0.0  | 0:05.23 | dhcpcd  |

## Stopping, Starting, and Resetting Applications

Use the following CLI commands for stopping, starting, and resetting applications:

- To stop an application, use the **appmgr stop *application*** command.

```
# appmgr stop dhcp
Shutting down dhcpd: [ OK ]
```

- To start an application, use the **appmgr start *application*** command.

```
# appmgr start amqp
Starting vsftpd for amqp: [ OK ]
```

- To restart an application use the **appmgr restart *application*** command.

```
# appmgr restart tftp
Restarting TFTP...
Stopping xinetd: [ OK ]
Starting xinetd: [ OK ]
```

**Note**

From Cisco DCNM Release 7.1.x, when you stop an application by using the **appmgr stop <<app\_name>>** command, the application will not start during successive reboots.

For example, if DHCP is stopped by using the **appmgr stop dhcp** command, and the OS is rebooted, the DHCP application will still be down after the OS is up and running.

To start again, use the command **appmgr start dhcp**. The DHCP application will be started after reboots also. This is to ensure that when an environment uses an application that is not packaged as part of the virtual appliance (like CPNR instead of DHCP), the application locally packaged with the virtual appliance will not interfere with its function after any OS reboots.

**Note**

When a DCNM appliance (ISO/OVA) is deployed, the Cisco SMIS component will not get started by default. However, this component can be managed using the appmgr CLI:  
**appmgr start/stop dcnm-smis**  
**appmgr start/stop dcnm** will start/stop only the DCNM web component.

## XMPP User and Group Management

XMPP in-band registration is disabled in the Cisco DCNM from a security perspective.

Before a switch can participate in XMPP, it must be added to the XMPP database by using the **appmgr** CLI command shown in [Table 6-4](#).

**Note**

A switch that has gone through POAP does *not* need to be added to the XMPP database using the **appmgr** CLI commands.

When POAP definitions are created in DCNM Web UI for a given switch, an XMPP user for that switch is automatically created in the XMPP database with the switch hostname “XMPP user” and with an XMPP password specified in the POAP definitions.

When the Cisco DCNM is deployed, an XMPP user named “admin” and a group named “dcnm-dfa” are created. This can be changed later in the DCNM Web UI by choosing **Configure > LAN Fabric Settings > General**.

Table 6-4 CLI Commands for XMPP user and group management

| CLI Commands                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>appmgr add_user xmpp -u username -p password</b>                | <p>-u is XMPP user ID without the domain name</p> <p>-p is XMPP user password (if user already exists, the password will be updated)</p> <p>For example, <b>appmgr add_user xmpp -u admin -p secret</b> creates a Jabber ID '<a href="mailto:admin@xyz.com">admin@xyz.com</a>' with password 'secret', where xyz.com is the FQDN</p>                                                                                      |
| <b>appmgr add_group xmpp -u username -p password -g group-name</b> | <p>-u is XMPP user ID without the domain name</p> <p>-p is XMPP password</p> <p>-g XMPP group to be created, if it does not exist already</p> <p>For example, <b>appmgr add_group xmpp -u admin -g dcnm-dfa</b> creates an XMPP group 'dcnm-dfa' created by Jabber ID 'admin@xyz.com'</p>                                                                                                                                 |
| <b>appmgr list_users xmpp</b>                                      | Lists the XMPP users                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>appmgr list_groups xmpp</b>                                     | Lists the XMPP groups                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>appmgr delete_user xmpp -u user</b>                             | <p>Deletes the XMPP user.</p> <p>You cannot delete a user if any group created by that user still exists in the XMPP database.</p>                                                                                                                                                                                                                                                                                        |
| <b>appmgr delete_group xmpp -u username -p password -g group</b>   | <p>Deletes the XMPP group</p> <p>-u is the XMPP user ID without the domain name</p> <p>-p is the XMPP user password</p> <p>-g is the XMPP group to be deleted</p> <p>For example, <b>appmgr delete_group xmpp -u admin -p cisco123 -g dcnm-dfa</b> deletes the XMPP group 'dcnm-dfa' created by Jabber ID 'admin@xyz.com.'</p> <p>You cannot delete a group created by one user with the credentials of another user.</p> |

## Change from Local Database to an External Database

Cisco recommends that you use an external Oracle database if you have large number of devices to be managed by your Cisco DCNM. Perform the following procedures to change from local database to an external database, when required.

### Reconfigure DCNM to use an external Oracle database



#### Note

Reconfiguring Cisco DCNM to use an external Oracle database is supported only for OVA/ISO deployments.

Perform the following steps to reconfigure the DCNM to use an external Oracle database.

- 
- Step 1** Stop DCNM server.
- Step 2** To configure the DCNM to use an external Oracle database, use **appmgr update dcnm -u <oracle\_jdbc\_url> -n <oracle\_db\_user> -p <oracle\_db\_password>** command.
- where,
- u <oracle\_jdbc\_url> : Oracle JDBC URL, example, jdbc:oracle:thin:@1.2.3.4:1521:XE
- n <oracle\_db\_user> : Database Username
- p <oracle\_db\_password>: Database User Password
- Step 3** Start DCNM server.
- 

## Change password for Linux root user

Use the following CLI command to change the password of the Linux root user.

```
appmgr change_pwd ssh root
```

At the prompt, enter the new password:

```
Enter the new ssh password for root user : <new password>
```

```
Enter it again for verification: <new password>
```



### Note

Do not use the following characters in your password:  
"&\$%' and <SPACE>.

## Backing Up Cisco DCNM and Application Data

You can use the **appmgr backup** command to back up Cisco DCNM and application data. See the following sections for details about backing up data.



### Note

For your reference, context sensitive help is available for the **appmgr backup** command. Use the **appmgr backup ?** command to display help.

## Backing Up Cisco DCNM

You can back up Cisco DCNM with a single command.

- To back up Cisco DCNM, use the **appmgr backup dcnm** command.



### Note

Configuration archive directories are not part of this backup. The command backs up only the local PostgreSQL database used by Cisco DCNM.

## Backing Up Application Data

Backing up all application data can be performed for a specific application or for all applications at once. Refer to the following table for CLI backup commands.

**Table 6-5** CLI Commands for backing up application data

| Command                   | Description                                                                                                                                                                                                                                                       |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>appmgr backup all</b>  | Backs up data for all applications.                                                                                                                                                                                                                               |
| <b>appmgr backup dcnm</b> | Backs up data for DCNM.                                                                                                                                                                                                                                           |
| <b>appmgr backup ldap</b> | Backs up data for LDAP.                                                                                                                                                                                                                                           |
| <b>appmgr backup xmpp</b> | Backs up data for both the XMPP/XCP configuration files and the local XMPP/XCP database.                                                                                                                                                                          |
| <b>appmgr backup amqp</b> | Backs up data for AMQP.                                                                                                                                                                                                                                           |
| <b>appmgr backup repo</b> | Backs up data for the repository contents (under /var/lib/dcnm).<br><br>The <b>appmgr backup repo</b> command excludes the backup of image files (all files ending in the .bin extension under /var/lib/dcnm) to prevent the backup file from becoming too large. |
| <b>appmgr back dhcp</b>   | Backs up data for the DHCP server.                                                                                                                                                                                                                                |

## Using Scripted Backups for Backing Up Application Data

If you use cron jobs for backup procedures, the database passwords can be assigned arguments so that there are no prompts. For example, you can use the **-p1** command for the Cisco DCNM database password. You can use the **-p2** command for the XMPP database password. Both passwords apply only to local databases.

```
appmgr backup dcnm -p1 dcnmdbpass
appmgr backup xmpp -p2 xmppdbpass
appmgr backup all -p1 dcnmdbpass -p2 xmppdbpass
```

## Collecting Log Files

Log files are needed to troubleshoot the Cisco DCNM installation.

Cisco DCNM-SAN is installed under <DCNM\_HOME>. The following are the default installation directories:

- Microsoft Windows—*C:\Program Files\Cisco Systems*



**Note** In Microsoft Windows, when a Cisco DCNM 32-bit installer is used for installation in a 64-bit environment, the default installation directory is *C:\Program Files <x86>\Cisco Systems*.

- Linux—*/usr/local/cisco*
- OVA/ISO—**appmgr tech\_support** command

Once the Cisco DCNM installation is complete, you can find the installer logs under:

- Microsoft Windows—*USER\_HOME\dcnm\_installer.log*
- Linux—*/root/dcnm\_installer.log*
- OVA/ISO— **appmgr tech\_support** command

**Note**

When you have several Cisco DCNM installations on the same machine, the installer preserves the logs with a timestamp. When the installation is done in the debug mode, the *dcnm\_installer.log* file is not available.

The PostgreSQL install logs are available under:

- Microsoft Windows—*USER\_TEMP\_DIR\install-postgresql.log*
- Linux: */tmp/install-postgresql.log*
- OVA/ISO— **appmgr tech\_support** command

The Cisco DCNM-SAN server logs are available under:

- Microsoft Windows—*DCNM\_HOME>\dcm\jboss\server\fm\logs*
- Linux—*DCNM\_HOME/dcm/jboss/server/fm/logs*
- OVA/ISO— **appmgr tech\_support** command

**Note**

For Cisco DCNM Virtual Appliance, use the **appmgr tech\_support** command to produce a dump of the log files. You can then provide this information to the TAC team for troubleshooting and analysis of your setup.

## Restoring Applications

Restoring an application clears all the existing data from that application. Before you restore an application, you should shut down the application.

Because all data will be cleared, you should perform a backup of the application that you are going to restore.

Use the following procedure to back up application data and restore the application on a new DCNM Open Virtual Appliance.

**Note**

A backup and restore procedure is supported only on either the same Open Virtual Appliance or a new Open Virtual Appliance deployed with an identical network configuration as the backed-up Open Virtual Appliance.

### DETAILED STEPS

- Step 1** Use the **appmgr backup** command on the existing Open Virtual Appliance.

- Step 2** Transfer the backup file to any repository.
- Step 3** Power off the first Open Virtual Appliance.
- Step 4** Deploy another Open Virtual Appliance with the same network configuration as the existing one, using the same IP/Netmask/Gateway/Hostname/DNS.
- Step 5** Transfer the backup file to the second Open Virtual Appliance.
- Step 6** Run the **appmgr restore** with the new backup on the new Open Virtual Appliance.



**Note** See [Table 6-6](#) for a list of CLI commands to restore applications.

**Table 6-6** CLI commands for restoring applications

| Command                         | Description                      |
|---------------------------------|----------------------------------|
| <b>appmgr restore all file</b>  | Restores all applications.       |
| <b>appmgr restore dcnm file</b> | Restores DCNM.                   |
| <b>appmgr restore ldap file</b> | Restore LDAP.                    |
| <b>appmgr restore amqp file</b> | Restores AMQP.                   |
| <b>appmgr restore repo file</b> | Restores the repository contents |
| <b>appmgr restore dhcp file</b> | Restores the DHCP server.        |
| <b>appmgr restore xmpp file</b> | Restores the XMPP server.        |

## Updating the SFTP Server Address for IPv6

After deploying the DCNM OVA/ISO successfully with EFM IPv4 and IPv6, by default the SFTP address is pointed to IPv4 only. You need to change the IPv6 address manually in the following two places:

- In the DCNM Web Client, choose **Administration > Server Properties** and then update the below fields to IPv6 and click the **Apply Changes** button.

```
#
# GENERAL>xFTP CREDENTIAL
#

# xFTP server's ip address for copying switch files:
server.FileServerAddress
```

- Log in to the DCNM through ssh and update the SFTP address with IPv6 manually in the server.properties file (/usr/local/cisco/dcm/fm/conf/server.properties).

```
# xFTP server's ip address for copying switch files:
server.FileServerAddress=2001:420:5446:2006::224:19
```







## CHAPTER 7

# Managing Applications in a High-Availability Environment

---

This chapter describes how to configure a high-availability (HA) environment in your Cisco DCNM Open Virtual Appliance deployment for your Cisco Programmable Fabric solution. It also includes details about the HA functionality for each of the applications bundled within the Cisco DCNM Open Virtual Appliance.



### Note

Ensure that the NTP server is synchronized between active and standby peers is essential for proper HA functioning in DCNM

---

This chapter includes the following sections:

- [Information About Application Level HA in the Cisco DCNM Open Virtual Appliance, page 7-1](#)
- [Prerequisites for Cisco DCNM Open Virtual Appliance HA, page 7-2](#)
- [Application High Availability Details, page 7-4](#)
- [Configuring DCNM HA, page 7-11](#)



### Note

For instruction about installing these applications with the Cisco DCNM Open Virtual Appliance, see the [“DCNM Open Virtual Appliance Installation in Programmable Fabric mode”](#) section on page 3-2.

---

## Information About Application Level HA in the Cisco DCNM Open Virtual Appliance

To achieve HA for applications that are run on the Cisco DCNM Open Virtual Appliance, you can run two virtual appliances. You can run one in Active mode and the other in Standby mode.



### Note

This document refers to these appliances as OVA-A and OVA-B, respectively.

---

In this scenario:

1. All applications run on both appliances.

The application data is either constantly synchronized or applications share a common database as applicable.

2. Only one of the applications running on the two appliances serves the client requests. Initially this would be the applications running on OVA-A. The application continues to do so until one of the following happens:
  - The application on OVA-A crashes.
  - The operating system on OVA-A crashes.
  - OVA-A is powered off for some reason.
3. At this point, the application running on the other appliance (OVA-B) takes over.
 

For DCNM REST API and AMQP, this transition is done by a load-balancing software that hides the interface address of the appliances using a Virtual IP (VIP) address.

For LDAP, both nodes are configured as duplicates of each other. The LDAP clients (switches) are configured with primary and secondary LDAP IPs, so if the active LDAP fails they try contacting the LDAP running on the standby.

For DHCP, when the first node fails, the second node starts serving the IP addresses.
4. The existing connections to OVA-A are dropped and the new connections are routed to OVA-B. This scenario demonstrates why one of the nodes (OVA-A) is initially referred to as the Active node and OVA-B is referred as the Standby node.

## Automatic Failover

The application-level and virtual machine (VM)-level and switchover process is as follows.

- If any of the applications managed by the load-balancing software (DCNM/AMQP) goes down on OVA-A, the Active node that handles the client requests detects the failure and redirects subsequent requests to the Standby node (OVA-B). This process provides an application-level switchover.
- If the Active node (OVA-A) fails or is powered-off for some reason, the Standby node (OVA-B) detects the failure and enables the VIP address for Cisco DCNM/AMQP on OVA-B. It also sends a gratuitous ARP to the local switch to indicate the new MAC address that is associated with the IP address. For applications not using VIP, the DHCPD running on OVA-B detects the failure of DHCPD on OVA-A and activates itself; whereas LDAP running on OVA-B continues running as LDAP is deployed Active-Active. Consequently, a VM-level failover is accomplished for all four applications (DCNM/AMQP/DHCP/LDAP).

## Manually Triggered Failovers

An application-level failover can also be triggered manually. For instance, you might want to run AMQP on OVA-B and the rest of the applications on OVA-A. In that case, you can log in to the SSH terminal of OVA-A and stop AMQP by using the **appmgr stop amqp** command.

This failover triggers the same process that is described in the [“Automatic Failover” section on page 7-2](#); subsequent requests to the AMQP Virtual IP address are redirected to OVA-B.

## Prerequisites for Cisco DCNM Open Virtual Appliance HA

This section contains the following topics that describe the prerequisites for obtaining a high-availability (HA) environment.

- [Oracle Database for DCNM Servers](#)
- [Deploying Cisco DCNM OVAs](#)
- [Creating an NFS/SCP Repository](#)
- [Availability of Virtual IP Addresses](#)
- [Installing an NTP Server](#)

## Deploying Cisco DCNM OVAs

You must deploy two standalone Open Virtual Appliance (OVAs). When you deploy both OVAs, you must meet the following criteria:

- Both OVAs must have the respective management access (eth0) and enhanced fabric management (eth1) interfaces in the same subnet. The eth0 of the active OVA must be in the same subnet as eth0 of the standby OVA. The eth1 of the active OVA must be in the same subnet as eth1 of the standby OVA.
- Both OVAs must be deployed with the same administrative password. This process ensures that both OVAs are duplicates of each other.

After the DCNM Open Virtual Appliance is powered up, verify that all the applications are up and running by using the **appmgr status all** command.

After all of the applications are up and running, stop the applications by using the **appmgr stop all** command.



**Note**

When the Open Virtual Appliance is started up for the first time, please wait for all the applications to run before you shut down any of the applications or power off the virtual appliance.

## Creating an NFS/SCP Repository

The DCNM HA cluster needs a server that has both NFS/SCP capabilities. This server is typically a Linux server.



**Note**

The server has to be in the enhanced fabric management network because the switches will use this server to download images and configurations.

Make sure that the exported directory is writable from both peers. The procedure to export a directory /var/lib/sharedarchive on a CentOS server is listed in the following paragraph. The steps will vary based on your environment.



**Note**

You might need root privileges to execute these commands. If you are a nonroot user, please use them with 'sudo'.

```
[root@repository ~]# mkdir -p /var/lib/sharedarchive
[root@repository ~]# chmod 777 -R /var/lib/sharedarchive
[root@repository ~]# vi /etc/exports
/var/lib/sharedarchive *(rw, sync)

[root@repository ~]# cd /etc/init.d
```

```
[root@repository ~]# service nfs restart
```

The same folder `/var/lib/sharedarchive` can also be accessed through SCP with SCP credentials.

The `/var/lib/sharedarchive * (rw, sync)` command provides read-write permissions to all servers on `/var/lib/sharedarchive`. Refer to CentOS documentation for information on restricting write permissions to specific peers.

## Availability of Virtual IP Addresses

Two free IPv4 addresses are needed to set up VIP addresses. The first IP address will be used in the management access network; it should be in the same subnet as the management access (eth0) interface of the OVAs. The second IP address should be in the same subnet as enhanced fabric management (eth1) interfaces (switch/POAP management network).

## Installing an NTP Server

For most of the HA functionality to work, you must synchronize the time on both OVAs by using an NTP server. The installation would typically be in the management access network (eth0) interfaces.

## Application High Availability Details

This section describes all of the Cisco Programmable Fabric HA applications.

Cisco DCNM Open Virtual Appliance has two interfaces: one that connects to the Open Virtual Appliance management network and one that connects to the enhanced Programmable Fabric network. Virtual IP addresses are defined for both interfaces.

- From the Open Virtual Appliance management network, the DCNM-REST API, DCNM interface, and AMQP are accessed through the VIP address
- From the enhanced fabric management network, LDAP and DHCP are accessed directly.

Only three Virtual IPs are defined:

- DCNM REST API (on dcnm management network)
- DCNM REST API (on enhanced fabric management network)
- AMQP (on dcnm management network)



### Note

Although DCNM Open Virtual Appliance in HA sets up a VIP, the VIP is intended to be used for the access of DCNM, REST API. For GUI access, we still recommend that you use the individual IP addresses of the DCNM HA peers and use the same to launch DCNM SAN Java clients, etc.

See the following table for a complete list of Programmable Fabric applications and their corresponding HA mechanisms.

| Programmable Fabric Application | HA Mechanism                     | Use of Virtual IPs | Comments                                      |
|---------------------------------|----------------------------------|--------------------|-----------------------------------------------|
| Data Center Network Manager     | DCNM Clustering/<br>Federation   | Yes                | Two VIPs defined, one on each network         |
| RabbitMQ                        | RabbitMQ Mirrored Queues         | Yes                | One VIP defined on the OVA management network |
| LDAP                            | OpenLDAP Mirror-mode replication | No                 | —                                             |
| XMPP                            | Not available in HA              | Yes                | Two VIPs defined, one on each network         |
| DHCP                            | ISC DHCPD Failover               | No                 | —                                             |
| Repositories                    | —                                | —                  | External repositories have to be used         |

## Data Center Network Management

The data center network management function is provided by the Cisco Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser at [http://\[host/ip\]](http://[host/ip]).



### Note

For more information about Cisco DCNM, see <http://cisco.com/go/dcnm>.

### HA Implementation

Cisco DCNMs that run on both OVAs are configured in clustering and federated modes for HA. 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.

You can enable automatic failover in the Cisco DCNM UI by choosing: **Admin > Federation**. If you enable an automatic failover and the Cisco DCNM that is running on OVA-A fails, the automatic failover moves only the fabrics and shallow-discovered LANs that are managed by OVA-A to OVA-B automatically.

### DCNM Virtual IP Usage

An Open Virtual Appliance HA setup has two VIP addresses (one for each network) for the Cisco DCNM at the default HTTP port. These VIPs can be used for accessing the DCNM RESTful services on the Open Virtual Appliance management network and the enhanced fabric management network. For example, external systems such as Cisco UCS Director can point to the VIP in the Open Virtual Appliance management network and the request gets directed to the active Cisco DCNM. Similarly, the switches in an enhanced fabric management network access the VIP address on the enhanced fabric management network during the POAP process.

You can still directly connect to Cisco DCNM real IP addresses and use them as you would in a DCNM in a cluster/federated set up.

**Note**

Cisco recommends that you must use VIP addresses only for accessing DCNM REST API. To access the Cisco DCNM Web or SAN client, you must connect using the IP address of the server.

**Licenses**

For Cisco DCNM, we recommend that you have licenses on the first instance and a spare matching license on the second instance.

**Application Failovers**

Enable an automatic failover option in the Cisco DCNM UI when an Open Virtual Appliance HA pair is set up by choosing: **Admin > Federation**. This process ensures that if the DCNM that is running on OVA-A fails, all the fabrics and shallow-discovered LANs managed by DCNM-A are managed by DCNM-B automatically after a given time interval (usually about 5 minutes after the failure of DCNM on OVA-A).

The Cisco DCNM VIP address still resides on OVA-A. The Representational State Transfer Web Services (REST) calls initially hit the VIP addresses on OVA-A and get redirected to the Cisco DCNM that is running on OVA-B.

**Application Failbacks**

When the Cisco DCNM on OVA-A comes up, the VIP address automatically redirects the REST requests to DCNM-A.

**Virtual-IP Failovers**

The VIP address that is configured for Cisco DCNM REST API on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.

The VIP address of Cisco DCNM automatically migrates to OVA-B. The only difference is which DCNM will be used after the failover.

- If a load-balancing software failure occurs, the VIP address on OVA-B directs the requests to DCNM-A.
- If an OVA-A failure occurs, the VIP address on OVA-B directs the requests to DCNM-B.

The automatic failover ensures that the ownership of all of the fabrics and shallow-discovered LANs managed by DCNM-A automatically change to DCNM-B.

**Virtual-IP Failbacks**

When OVA-A is brought up and Cisco DCNM is running, the VIP addresses keep running on the Standby node. The failback of Virtual IP addresses from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up.
2. Cisco DCNM runs on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B.

# RabbitMQ

RabbitMQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP).

**Note**

You need to stop and restart AMQP on both DCNM's server in HA within 30 seconds, otherwise AMQP may not start.  
For more information about RabbitMQ, go to <http://www.rabbitmq.com/documentation.html>

## HA Implementation

Enabling the HA on the Open Virtual Appliance creates a VIP address in the Open Virtual Appliance management network. Orchestration systems such as vCloud Director, set their AMQP broker to the VIP address.

Enabling the HA on the Open Virtual Appliance also configures the RabbitMQ broker that runs on each node to be a duplicate of the broker that is running on the other node. Both OVAs act as “disk nodes” of a RabbitMQ cluster, which means that all the persistent messages stored in durable queues are replicated. The RabbitMQ policy ensures that all the queues are automatically replicated to all the nodes.

## Application Failovers

If RabbitMQ-A fails, the VIP address on OVA-A redirects the subsequent AMQP requests to RabbitMQ-B.

## Application Failbacks

When RabbitMQ-A comes up, the VIP address automatically starts directing the AMQP requests to RabbitMQ-A.

## Virtual-IP Failovers

The VIP address configured for the AMQP broker on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.

In both cases, the VIP address of the AMQP automatically migrates to OVA-B. The only difference is which AMQP broker will be used after the failover.

- In a load-balancing software failure, the VIP address on OVA-B directs the requests to RabbitMQ-A.
- In an OVA-A failure, the VIP address on OVA-B directs the requests to RabbitMQ-B.

## “Virtual-IP” Failbacks

When OVA-A is brought up and AMQP-A is running, the VIP addresses keep running on the OVA-B (directing the requests to AMQP-A). The failback of the RabbitMQ VIP from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up.
2. RabbitMQ runs on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B.

## OpenLightweight Directory Access Protocol

The DCNM Open Virtual Appliance installs an LDAP server and an asset database to the switches.

This section contains the following topics:

- “Using the DCNM Open Virtual Appliance-Packaged (Local) LDAP Server” section on page 7-8
- “Using the Remote LDAP Server” section on page 7-9

### Using the DCNM Open Virtual Appliance-Packaged (Local) LDAP Server

LDAP HA is achieved through OpenLDAP mirror mode replication. Each LDAP server that is running on one DCNM Open Virtual Appliance becomes a duplicate of the LDAP server that is running on the other Open Virtual Appliance.

#### DCNM and LDAP Interaction

Both LDAP IP addresses show up in the Cisco DCNM Web Client (**Admin->Fabric Settings**) in the following order: LDAP-A, LDAP-B.

Cisco DCNM attempts to write on LDAP-A as follows.

- If the write operation succeeds, the data gets replicated to LDAP-B.
- If the write operation fails, then Cisco DCNM writes to LDAP-B.

The data on LDAP-B eventually gets replicated to LDAP-A when it becomes available.

#### Switch and LDAP Interaction

When you configure the asset databases, every switch is configured with multiple LDAP servers, as shown in the following example.

The first active LDAP server that is configured in the switch becomes the Active LDAP server. The Active LDAP server is queried first for autoconfigurations.

For every read operation that the switch needs to perform, the Active LDAP server is contacted first, followed by the rest of the LDAP servers.

```
Leaf-0 # fabric database type network
Leaf-0 (config-fabric-db)# server protocol ldap host <LDAP-1-IP> vrf management
Leaf-0 (config-fabric-db)# db-table ou=networks,dc=cisco,dc=com key-type 1
Leaf-0 (config-fabric-db)# server protocol ldap host <LDAP-2-IP> vrf management
Leaf-0 (config-fabric-db)# db-table ou=networks,dc=cisco,dc=com key-type 1
```

Use the **show fabric database statistics** command to find the Active LDAP server, which is marked by an asterisk (\*) in the output.

```
Leaf-0 # show fabric database statistics
DB-Type           Requests    Dispatched  Not dispatched  Re-dispatched
-----
network           1           1           0               0
cabling           0           0           0               0
profile           1           1           0               0
-----
TOTAL             2           2           0               0

Per Database stats:
T Prot Server/DB           Reqs    OK    NoRes    Err    TmOut    Pend
-----
n ldap 10.77.247.147       5       2     1       2       0       0
```



```

*n ldap 10.77.247.148          3      3      0      0      0      0
*p ldap 172.23.244.122        1      1      0      0      0      0
Legend:
  T-Type (N-Network, C-Cabling, P-Profile)
  *-Active Server

```

In the previous example, during autoconfiguration, a leaf switch first queries 10.77.247.148, which is the active network database (indicated by “\*n”). If that is not available, it automatically contacts the second LDAP server configured as an network database (10.77.247.147 in this example).

## Using the Remote LDAP Server

This section describes the behavior when you use a remote LDAP server in an HA environment.

### Cisco DCNM and LDAP Interaction

Cisco DCNM allows only two external LDAP servers that are assumed to be synchronized with each other.

### Switch and LDAP interaction

The switch and LDAP interaction that use the remote LDAP server is the same interaction as when you are using the Open Virtual Appliance-packaged LDAP. The Active LDAP server is contacted first; if it is not reachable, the switch then attempts to read from the next available LDAP server.

## DCHP HA

DHCP on both OVAs listen on the interface of the enhanced fabric management network. The native Internet Systems Consortium (ISC) DHCPD failover mechanism is be used for HA. The lease information is automatically synchronized using native code.

## DHCP POAP

The switches do a DHCP broadcast and get response from the Active DHCP server.

## DHCP Autoconfiguration

When a tenant host or virtual machine (VM) comes up, it sends a broadcast that is relayed by the leaf node. In such a scenario, the VM profiles should be configured with both relay addresses of OVA-A and OVA-B.

```

interface vlan $vlanid
. . .
ip dhcp relay 1.2.3.4 vrf ..# eth1 IP of OVA-A
ip dhcp relay 1.2.3.5 vrf ..# eth1 IP of OVA-B

```

## Changing DHCP Scope Configurations

Scope changes through the Cisco DCNM UI ensure proper synchronization of scopes among the peers. We do not recommend that you do a manual configuration of the DHCP scope configuration file.

**Note**

You must update the IP range for the default scope before creating the new scope, otherwise DHCP will be unable to start. See the [“Starting DHCP in an HA Setup” section on page 7-15](#) for information on updating the IP range for the DHCP scope through the Cisco DCNM UI.

## Repositories

All repositories must be remote.

## Extensible Messaging and Presence Protocol (XMPP)

### HA Implementation

XMPP HA is achieved by having two instances of XMPP applications run with a common database and having a Virtual (floating) IP direct the traffic to the active/standby XMPP.

### XMPP Virtual IP Usage

An OVA HA setup has two VIP addresses (one for each network) for the Cisco XCP at the default XMPP port. These VIPs can be used for accessing XMPP services on the OVA management network and the enhanced fabric management network. For example, jabber clients can point to the VIP in the OVA management network and the request gets directed to the active Cisco DCNM. Similarly, the switches in an enhanced fabric management network access the VIP address on the enhanced fabric management network during the group chat interactions.

### Application Failovers

If the XMPP on OVA-A fails, VIP address still resides on OVA-A but the traffic gets redirected to the XMPP that is running on OVA-B.

### Application Failbacks

When the XMPP on OVA-A comes up, the VIP address automatically redirects the successive requests to the XMPP running on OVA-A.

### Virtual-IP Failovers

The VIP address that is configured by default on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.
  - If a load-balancing software failure occurs, the VIP address floats over to OVA-B, and from there it directs the requests to the XMPP on OVA-A.
  - If an OVA-A failure occurs, the VIP address floats over to OVA-B, and directs the requests to XMPP-B. In both cases, the VIP address of Cisco DCNM automatically migrates to OVA-B. The only difference is which XMPP will be used after the failover.

## Virtual-IP Failbacks

When OVA-A is brought up and Cisco DCNM is running, the VIP addresses keep running on the Standby node. The failback of Virtual IP addresses from OVA-B to OVA-A occurs only in the following sequence.

When OVA-A is brought up and XMPP is starts running, the VIP addresses keep running on the Standby node. The failback of Virtual IP addresses from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up
2. XMPP starts on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B

## Configuring DCNM HA

Because both of the OVAs in an HA environment are deployed identically, either one of them can be the Active peer. The other Open Virtual Appliance would be the Standby peer. All of the configuration CLI commands in the following sections are executed from the secure shell (SSH) terminal.

## Configuring the Active Peer



### Note

Before starting the High Availability setup in active and standby, you need to stop all applications using the **appmgr stop all** command

- Step 1** Log in to the SSH terminal of the Open Virtual Appliance that you want to become the Active peer and enter the **appmgr setup ha active** command.

```
Active-peer# appmgr setup ha active
*****
You are about to enable High Availability in this DCNM virtual appliance.
Please make sure that you the following
1.      An Oracle Database with one user defined for DCNM and one for XMPP
2.      A repository with NFS/SCP capabilities
3.      An NTP server for time synchronization
4.      A couple of free IP addresses to be used as Virtual IPs (one on each port group)
5.      A peer DCNM deployed with the same user profile (same username/password)
6.      Shut down all applications in this server using 'appmgr stop all'

*****
Do you want to continue? [y/n] [y]
```

- Step 2** Make sure that each prerequisite is in place and press **y**; if not all of the prerequisites are in place, press **n** to exit.

A prompt for the root password appears.

```
. . .
Enter the root password of this DCNM : <root-password-of-active-peer>
Enter it again for verification: <root-password-of-active-peer>
. . .
```

- Step 3** Enter the administrative password created during Open Virtual Appliance installation.

You will now be prompted for the management access interface (eth0 IP address) of the Standby peer.

- Step 4** Enter the management IP address of the peer DCNM.

The active Open Virtual Appliance generates a pair of authentication keys and transfers it to the peer's authorized keys.

- a. Enter the root password of the Standby peer when prompted.

All of the other network information needed from the Standby peer is automatically picked up by the Active peer and displayed for confirmation.

- b. Ensure that it is the correct peer and press **y** to continue.

```
. . .
Enter the mgmt IP of the peer DCNM (eth0 IP) : <peer eth0 IP>
Generating ssh keys..
Enter the root password of the peer
root@10.77.247.148's password: <standby-peer root password>
Retrieving information...
Peer Details :
=====
Hostname: abc.xyz.com
Eth0 IP : 1.2.3.4
Eth1 IP : 192.168.57.148
Do you want to continue? [y/n] [y]
```

- Step 5** Enter the VIP addresses for both the management access (eth0) and enhanced fabric management networks (eth1).

Make sure that the VIP addresses are currently not used by any other interfaces in their respective networks.

```
Setting the Virtual IP addresses
=====
The Virtual IP in the eth0 network.
It serves as a single point of access for the following applications: DCNM REST API, AMQP
Enter the VIP : <a free IP from eth0 subnet>

The Virtual IP in the eth1 network.
It serves as a single point of access for the following applications: DCNM REST API from
the switch network
Enter the VIP : <a free IP from eth1 subnet>
```

- Step 6** Enter the database URL to set the database. The script uses a JDBC thin driver, so you should enter the URL in the same format.

- a. Enter the database password.
- b. Enter the database password again for verification.

The script tries to do a sample query from the database to check the details entered. The Cisco DCNM schema and related data are loaded after you confirm that all the data are valid.

```
Setting the Database for DCNM and XMPP
=====
Enter the DB URL {ex. jdbc:oracle:thin:@ipaddr:1521:<SID or Servicename>}
Enter the DB username for DCNM tables: <dcnm-dbuser>
Enter the DB password for DCNM tables :
Enter it again for verification:
Enter the DB username for XMPP tables: <xmpp-dbuser>
Enter the DB password for XMPP tables :
Enter it again for verification:
```

- Step 7** Enter an FQDN that will be used as a common XMPP domain name.

```
Common FQDN for Virtual IPs on both DCNM mgmt and EFM networks
=====
Enter the common FQDN for VIP on both DCNM mgmt and EFM networks:
```

**Step 8** Enter repository settings:

- a. Enter an SCP/NFS repository IP address for the enhanced fabric management network.
- b. Enter the IP/exported-directory location.

The script does a test mount and unmounts it shortly after. It is permanently mounted after user confirmation. Similar checks are done for SCP repository users.

- c. You will have to enter the SCP password three times (twice for the script and the third time when the script does a test write on the repository).
- d. Enter an NTP server IP address. This step is very important for all the applications that run on a cluster.

Repository/NTP Details

```
note: A repository server in the DFA network that has both NFS and SSH/SCP capability.
=====
Enter the SCP/NFS repository IP : <repository IP>
NFS Exported location {ex. /var/shared/dcnm/} : /var/lib/dcnmuser
Performing a test mount to ensure that the server is reachable..
Performing a test-write to ensure the exported directory is writable
test-write successful. Proceeding..
Enter the SCP username for <repository IP> : <repository user>
Enter the SCP password :
Enter it again for verification:
Performing a test-write to ensure the directory is writable through SCP..
root@<repository-ip>'s password:
test-write successful. Proceeding..
Enter an NTP server for time synchronization : 10.56.14.161
```

**Step 9** A summary of the details entered will be displayed. If you want to reenter the details, press **n**.

Once the HA setup is complete, you can check the role of the ha as follows:

```
OVA-A # appmgr show ha-role
Active
```

## Configuring the Standby peer

**Step 1** Log in to the SSH terminal of OVA-B and enter the **appmgr setup ha standby** command.

```
OVA-B # appmgr setup ha standby
*****
You are about to enable High Availability in this DCNM virtual appliance.
Please make sure that you the following
1.      A peer DCNM virtual appliance deployed with the same user and configured as Active
peer
2.      Shut down all applications in this server using 'appmgr stop all'
*****
Do you want to continue? [y/n] [y]
```

**Step 2** Press **y** to continue.

The standby Open Virtual Appliance generates a pair of authentication keys and transfers it to the peer's authorized keys.

- a. Enter the root password of the Active peer when prompted.

All the other network information entered during active the Open Virtual Appliance setup is automatically picked up by the Standby peer and displayed for confirmation.

- b. Carefully check if it is the correct peer and press **y** to continue.

```
Retrieving information from details entered on Active...
Generating ssh keys..
```

```
Enter the root password of the peer
```

```
Warning: Permanently added '10.77.247.147' (RSA) to the list of known hosts.
```

```
Peer Details :
```

```
=====
```

```
Hostname      : somehost.cisco.com
```

```
Eth0 IP : 10.77.247.147
```

```
Eth1 IP : 192.168.57.147
```

```
*****
```

```
Summary of details entered
```

```
*****
```

```
Virtual IP
```

```
=====
```

```
Virtual IP in eth0 n/w : 10.77.247.143
```

```
Virtual IP in eth1 n/w : 192.168.57.143
```

```
Database for DCNM and XMPP
```

```
=====
```

```
DB URL : jdbc:oracle:thin:@10.77.247.11:1521:XE
```

```
DB username for DCNM : dcnmuser
```

```
DB Username for XMPP : xmppuser
```

```
Archives/Repositories
```

```
=====
```

```
SCP/NFS repository IP : 10.77.247.11
```

```
NFS Exported location : /var/lib/dcnmuser
```

```
SCP username : root
```

```
NTP server : 10.56.14.161
```

```
*****
```

```
Do you want to continue? [y/n] [y]
```

Once confirmed, OVA-B is configured to be a Standby peer, and the following message is displayed.

```
...
```

```
*****
```

```
This node has been configured as standby
```

```
Please run 'appmgr start all' first on the active peer (10.77.247.147), and then on the
standby peer(10.77.247.148) to start using applications.
```

```
** note ** : dhcpd will not be up until the default poap scopes are updated with free IP
addresses from DCNM GUI
```

```
*****
```



#### Note

For information about updating default POAP scopes and starting DHCP using HA, please see, [Starting DHCP in an HA Setup, page 7-15](#).

- Step 3** Check the HA role of the node by entering the **appmgr show ha-role** command.

```
OVA-A # appmgr show ha-role
```

---

Standby

---

## Starting Applications in the Active Peer

- Step 1** Log in to the SSH terminal of the Active peer (OVA-A) and start all applications by entering the **appmgr start all** command.
- Step 2** Wait for all the applications to start. Once all applications (except dhcpd) are up and running, go to the next procedure.



**Note** To start DHCP using HA, see the [“Starting DHCP in an HA Setup” section on page 7-15](#).

---

## Starting Applications in the Standby Peer

- Step 1** Login to the SSH terminal of the Standby peer and start all applications using the **appmgr start all** command. Wait for all the applications to start.
- Step 2** Once all applications (except dhcpd) are up/running, proceed to the next step.



**Note** For starting DHCP using HA, please see, [Starting DHCP in an HA Setup, page 7-15](#)

---

## Starting DHCP in an HA Setup

In an HA setup, DHCPD will be initially down. In this procedure, you will update the IP range address for the POAP DHCP scope. Use the following procedure to bring up DHCP.



**Note** You must update the IP range for the default scope before creating the new scope, otherwise DHCP will be unable to start.

---

- Step 1** Log in to Cisco DCNM web UI.
- Step 2** On the menu bar, choose **Config> POAP > DHCP Scope** and enter the free IP range address for the default DHCP scope named enhanced\_fabric\_mgmt\_scope.
- Step 3** Click **Apply**.
- DHCP is automatically started on both the OVAs.
- Step 4** Verify all applications are running by opening an SSH terminal session and using the **appmgr status all** command.
-

