CHAPTER 1

Overview

This chapter provides a brief overview of Cisco Data Center Network Manager (DCNM). It also includes general DCNM deployment steps and details about preparing Cisco NX-OS devices for management and monitoring by DCNM.

This chapter includes the following sections:

Information About DCNM

DCNM is a management solution that maximizes overall data center infrastructure uptime and reliability, which improves business continuity. Focused on the management requirements of the data center network, DCNM provides a robust framework and rich feature set that fulfills the switching needs of present and future data centers. In particular, DCNM automates the provisioning process.

DCNM is a solution designed for Cisco NX-OS-enabled hardware platforms. Cisco NX-OS provides the foundation for the Cisco Nexus product family, including the Cisco Nexus 7000 Series.

This section includes the following topics:

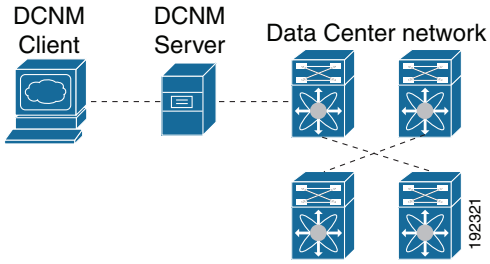
DCNM Client and Server

DCNM is Java-based client-server application. For Java requirements, server system requirements, and client system requirements, see the *Cisco DCNM Release Notes, Release 4.1*.

Figure 1-1 shows the DCNM client-server environment. The DCNM client communicates with the DCNM server only, never directly with managed Cisco NX-OS devices. The DCNM server uses the XML management interface of Cisco NX-OS devices to manage and monitor them. The XML

management interface is a programmatic method based on the NETCONF protocol that complements the command-line interface (CLI) functionality. For more information, see the *Cisco NX-OS XML Management Interface User Guide, Release 4.1*.

Figure 1-1 DCNM Client-Server Environment



Features in DCNM, Release 4.1

DCNM Release 4.1 supports the configuration and monitoring of the following Cisco NX-OS features:

- Ethernet switching
  - Physical ports
  - Port channels and virtual port channels (vPCs)
  - Loopback and management interfaces
  - VLAN network interfaces (sometimes referred to as switched virtual interfaces or SVIs)
  - VLAN and private VLAN (PVLAN)
  - Spanning Tree Protocol, including Rapid Spanning Tree (RST) and Multi-Instance Spanning Tree Protocol (MST)

  Ethernet routing
  - Gateway Load Balancing Protocol (GLBP) and object tracking
  - Hot Standby Router Protocol (HSRP)

  Network security
  - Access control lists
  - IEEE 802.1X
  - Authentication, authorization, and accounting (AAA)
  - Role-based access control
  - Dynamic Host Configuration Protocol (DHCP) snooping
  - Dynamic Address Resolution Protocol (ARP) inspection
  - IP Source Guard
  - Traffic storm control
  - Port security
  - Keychain management

General

- Virtual Device Context
- Gateway Load Balancing Protocol (GLBP), object tracking, and keychain management
- Hardware resource utilization with Ternary Content Addressable Memory (TCAM) statistics
- Switched Port Analyzer (SPAN)

DCNM includes the following features for assistance with management of your network:

Topology viewer

Event browser

Configuration Change Management

Device OS Management

Hardware inventory

DCNM includes the following administrative features:

DCNM server user accounts

Device discovery, including support for Cisco Discovery Protocol

Automatic synchronization with discovered devices

Statistical data collection management

DCNM server and client logging

DCNM Licensing

Many of the features of DCNM 4.1 do not require a license; however, the following features are enabled in DCNM only after you have installed a LAN Enterprise license:

- vPCs
- 802.1X
- Gateway load-balancing protocol (GLBP)
- Object tracking
- Keychain management
- DHCP snooping
- Dynamic ARP Inspection
- ARP access control lists (ACLs)
- IP Source Guard
- Traffic storm control
- Port security
- IP tunnels
- Virtual Device Contexts (VDCs)
- Logical vPC view of the Topology feature
- Display of historical statistical data

For information about obtaining and installing a DCNM LAN Enterprise license, see the "Installing Licenses" section on page 2-7.

Documentation About DCNM

The documentation for DCNM includes several configuration guides and other documents. For more information about the DCNM documentation, see the "Related Documentation" section on page xxi.

Deploying DCNM

You can deploy DCNM to manage and monitor supported network devices. This procedure provides the general steps that you must take to deploy DCNM and links to more detailed procedures to help you with each general step.

BEFORE YOU BEGIN

Determine which computer will run the DCNM server software. This computer should meet the system requirements for the DCNM server. For details about system requirements, see the *Cisco DCNM Release Notes, Release 4.1*.

DETAILED STEPS

To deploy DCNM, follow these steps:

Step 1 Prepare the computer that you want to install the DCNM server on. For more information, see the "Prerequisites for Installing the DCNM Server" section on page 2-1.

Step 2 Download Cisco DCNM. For more information, see the "Downloading the DCNM Server Software" section on page 2-2.

Step 3 Install the DCNM server software. For more information, see the "Installing the DCNM Server" section on page 2-3.

Step 4 Start the DCNM server. For more information, see the "Starting the DCNM Server" section on page 2-6.

Step 5 (Optional) Install the license on the DCNM server. For more information, see the "Installing Licenses" section on page 2-7

Step 6 Install the DCNM client. For more information, see Chapter 3, "Downloading and Launching the DCNM Client."

Step 7 Prepare each Cisco NX-OS device that you want to manage and monitor by using DCNM. For more information, see the "Preparing a Cisco NX-OS Device for Management by DCNM" section on page 1-5.

Note Remember that each virtual device context (VDC) on a physical device that runs Cisco NX-OS is considered a Cisco NX-OS device. You must perform the steps in "Preparing a Cisco NX-OS Device for Management by DCNM" section on page 1-5 for each VDC that you want to manage and monitor with DCNM.

Step 8 Perform device discovery for one or more devices. For more information, see the "Administering Device Discovery" section on page 6-1.

Step 9 (Optional) If you installed a license, enable DCNM to use licensed features on specific devices by adding managed devices to the license. For more information, see the "Administering DCNM Licensed Devices" section on page 8-1.

Step 10 Begin using DCNM to configure and monitor the managed devices. For more information about using DCNM, see the Cisco DCNM configuration guides.

Cisco NX-OS Device Configuration Requirements

This section provides information about device configuration requirements and configuration tasks you must perform on Cisco NX-OS devices that you want to manage and monitor by using DCNM. You must perform the configuration tasks by using a method other than DCNM, such as the CLI.

Note For up-to-date information about Cisco network device operating systems and hardware supported by DCNM, see the *Cisco DCNM Release Notes, Release 4.1*.

This section includes the following topics:

Preparing a Cisco NX-OS Device for Management by DCNM

Before you perform device discovery with DCNM, you should perform the following procedure on each Cisco NX-OS device that you want to manage and monitor with DCNM. This procedure helps ensure that device discovery succeeds and that DCNM can effectively manage and monitor the device.

Note Remember that each VDC on a physical device that runs Cisco NX-OS is considered a Cisco NX-OS device. You must perform the steps in "Preparing a Cisco NX-OS Device for Management by DCNM" section on page 1-5 for each VDC that you want to manage and monitor with DCNM.

DETAILED STEPS

To successfully discover a Cisco NX-OS device, DCNM requires that you configuring the following items in each VDC that you want to manage and monitor with DCNM:

Step 1 Log into the CLI of the Cisco NX-OS device.

Step 2 Use the **configure terminal** command to access global configuration mode.

Step 3 Ensure that an RSA or DSA key exists so that secure shell (SSH) connections can succeed. To do so, use the **show ssh key rsa** or **show ssh key dsa** command.

If you need to generate a key, use the **ssh key** command.

Note You must disable the SSH server before you can generate a key. To do so, use the **no feature ssh** command.

Step 4 Ensure that the SSH server is enabled. To do so, use the **show ssh server** command.

If the SSH server is not enabled, use the **feature ssh** command to enable it.

Step 5 Ensure that CDP is enabled globally and on the interface that DCNM uses to connect to the device. Use the **show run cdp all** command to see whether CDP is enabled. For assistance with configuring CDP, see the *Cisco NX-OS System Management Configuration Guide, Release 4.1*.

Step 6 Ensure that the Cisco NX-OS device meets the system-message logging requirements of DCNM. For more information, see the "Cisco NX-OS System-Message Logging Requirements" section on page 1-6.

Cisco NX-OS System-Message Logging Requirements

To monitor and manage devices, DCNM depends partly on system messages for some Cisco NX-OS features. To ensure that DCNM receives the messages that it needs, you must ensure that all Cisco NX-OS devices managed and monitored by DCNM meet the logging requirements described in this section.

For information about configuring system-message logging on a Cisco NX-OS device, see the *Cisco NX-OS System Management Configuration Guide, Release 4.1*.

This section includes the following topics:

Interface Link-Status Events Logging Requirement

You must configure the device to log system messages about interface link-status change events. This requirement ensures that DCNM receives information about interface link-status changes. The following two commands must be present in the running configuration on the device:

logging event link-status enable

logging event link status default

To ensure that these commands are configured on the device, perform the steps in the "Configuring a Device to Meet DCNM Logging Requirements" section on page 1-9.

Logfile Requirements

You must configure the device to store system messages that are severity level 6 or lower in the log file.

Although you can specify any name for the log file, we recommend that you do not change the name of the log file. When you change the name of the log file, the device clears previous system messages. The default name of the log file is "messages".

If you use the default name for the log file, the following command must be present in the running configuration on the device:

logging logfile messages 6

To ensure that this command is configured on the device, perform the steps in the "Configuring a Device to Meet DCNM Logging Requirements" section on page 1-9.

Logging Severity-Level Requirements

All enabled features on a Cisco NX-OS have a default logging level. For features supported by DCNM, DCNM requires the logging severity levels set to a specific level depending on the feature. The logging level required varies from feature to feature. DCNM cannot configure logging levels on the managed Cisco NX-OS devices. We plan to enhance DCNM to configure logging levels in a future release; however, with Cisco DCNM Release 4.1, you must ensure that any Cisco NX-OS device that you want to manage and monitor with DCNM is configured with logging levels that meet the logging-level requirements listed in Table 1-1.

When evaluating the logging-level configuration of a device, consider the following:

- DCNM has logging-level requirements for only the features listed in Table 1-1. If a Cisco NX-OS logging facility does not appear in Table 1-1, you do not need to configure a logging level in order for DCNM to successfully manage and monitor the device.
- The default Cisco NX-OS logging level for some facilities is not high enough to support management of the feature by DCNM. Be sure that you raise the logging level for a facility when its default level is not high enough to satisfy the DCNM logging-level requirement. In Table 1-1, DCNM logging levels that exceed the default logging level appear in **bold** text.
- You can set a logging level higher than the DCNM requirement. The maximum logging severity level is 7. If a logging level exceeds the DCNM requirement, you do not need to lower the logging level.
- Cisco NX-OS does not support logging-level configuration for disabled features. If you disable a feature, any nondefault logging level configuration is lost and is not restored if you reenable the feature later. When you enable a feature, perform the steps in the "Configuring a Device to Meet DCNM Logging Requirements" section on page 1-9 to ensure that the logging level configuration for the feature meets DCNM requirements.
- When you create a new VDC, its running configuration includes only the default logging levels. For each VDC that you create, perform the steps in the "Configuring a Device to Meet DCNM Logging Requirements" section on page 1-9 to ensure that the logging level configuration in each VDC meets DCNM requirements.

To ensure that logging severity levels are correctly configured on the device, perform the steps in the "Configuring a Device to Meet DCNM Logging Requirements" section on page 1-9.

Table 1-1 Logging Levels per DCNM Feature

DCNM Feature	Cisco NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum DCNM-Required Logging Level[1]	Your Current Logging Level
AAA	AAA	Yes	aaa	3	**5**	
	RADIUS	Yes	radius	3	**5**	
	TACACS+	No	tacacs+	3	**5**	
Device Discovery	CDP	Yes	cdp	2	**6**	
Topology						
DHCP snooping	DHCP snooping	No	dhcp	2	**6**	
Dynamic ARP Inspection						
IP Source Guard						
Dot1X	802.1X	No	dot1x	2	**5**	
Traffic Storm Control	Ethernet port manager	Yes	ethpm	5	5	
Ethernet Interfaces						
	Unidirectional Link Detection (UDLD)	No	udld	5	5	
Gateway Load Balancing Protocol (GLBP)	GLBP	No	glbp	3	**6**	
Hot Standby Router Protocol (HSRP)	HSRP engine	No	hsrp_engine	3	**6**	
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**	
Inventory	Module	Yes	module	5	5	
	Platform	Yes	platform	5	5	
	System manager	Yes	sysmgr	3	3	
SPAN	SPAN	Yes	monitor	7	6	
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**	
Port security	Port security	No	port-security	2	**5**	
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**	
Object Tracking	Object tracking	Yes	track	3	**6**	
Virtual Device Contexts (VDCs)	VDC manager	Yes	vdc_mgr	6	6	
Virtual Port Channel (vPC)	VPC	No	vpc	2	**6**	

1. Minimum DCNM logging levels appear in **bold** text for Cisco NX-OS logging facilities that have a default logging level that is too low.

Configuring a Device to Meet DCNM Logging Requirements

When you are preparing a device for management and monitoring by DCNM, you can perform an initial logging configuration. If you later enable a feature that was previously disabled, we recommend that you perform this procedure again to ensure that logging configuration on the device meets DCNM requirements.

You should also perform this procedure in a newly created VDC. Regardless of whether you used DCNM to create the VDC or whether you used the CLI, the logging configuration of a new VDC is only the default configuration and must be configured to support management and monitoring by DCNM.

BEFORE YOU BEGIN

Consider printing Table 1-1. You can use the Your Current Logging Level column to make notes about logging level configuration on the device.

For more information about configuring logging levels, see the *Cisco NX-OS System Management Configuration Guide, Release 4.1*.

DETAILED STEPS

To perform the initial Cisco NX-OS logging configuration, follow these steps:

Step 1 Log into the Cisco NX-OS device.

Step 2 Access the global configuration mode.

```
switch# configure terminal
switch(config)#
```

Verify that the **logging event link-status default** and **logging event link-status enable** commands are configured.

```
switch(config)# show running-config all | include "logging event link-status"
logging event link-status default
logging event link-status enable
```

If either command is missing, enter it to add it to the running configuration.

The **logging event link-status enable** is included in the default Cisco NX-OS configuration. The **show running-config** command displays the default configuration only if you use the **all** keyword.

Verify that the device is configured to log system messages that are severity 6 or lower.

The default name of the log file is “messages”; however, we recommend that you use the log-file name currently configured on the device. If you change the name of the log file, the device clears previous system messages.

```
switch(config)# show running-config all | include logfile
logging logfile logfile-name 6
```

If the **logging logfile** command does not appear or if the severity level is less than 6, configure the **logging logfile** command.

```
switch(config)# logging logfile logfile-name 6
```

Step 5 Determine which nondefault features are enabled on the device.

```
switch(config)#
feature feature1
feature feature2
feature feature3
.
.
.
```

Step 6 View the logging levels currently configured on the device. The **show logging level** command displays logging levels only for features that are enabled. The Current Session Severity column lists the current logging level.

```
switch(config)#
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       5
aclmgr                  3                       3
.
.
.
```

Tip You can use the **show logging level** command with the facility name when you want to see the logging level of a single logging facility, such as **show logging level aaa**.

Step 7 Determine which logging levels on the device are below the minimum DCNM-required logging levels. To do so, compare the logging levels displayed in Step 6 to the minimum DCNM-required logging levels that are listed in Table 1-1.

Step 8 For each logging facility with a logging level that is below the minimum DCNM-required logging level, configure the device with a logging level that meets or exceeds the DCNM requirement.

```
switch(config)#               facility severity-level
```

The *facility* argument is the applicable logging-facility keyword from Table 1-1 and *severity-level* is the applicable minimum DCNM-required logging level or higher (up to 7).

Step 9 Use the **show logging level** command to verify your changes to the configuration.

Step 10 Copy the running configuration to the startup configuration to save your changes.

```
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```