CHAPTER 9

Configuring Network Servers

This chapter describes how to configure the Network Servers feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Network Servers

During device discovery, Cisco DCNM can discover the host bus adapters (HBAs) and Ethernet network adapters of the network servers that are connected to Cisco NX-OS devices in your network. Cisco DCNM uses the Link Layer Discovery Protocol (LLDP) to retrieve information about the Ethernet network adapters from network servers; however, the information retrieved by LLDP is not adequate for Cisco DCNM to determine if the discovered network adapters are part of the same network server.

Beginning with Cisco DCNM Release 5.1, you can use Cisco DCNM to discover the servers that are either directly connected to Cisco Nexus 5000 Series switches or use Converged Network Adapters (CNAs). You can see the discovered CNA adapters in the Static Server-Adapter Mapping feature pane. Cisco DCNM does not allow you to automatically correlate adapters that are connected to Cisco Nexus 5000 Series switches via CNA. However, you can manually correlate the CNA adapters that belong to a network server. For more information about the discovery process, see Chapter 5, “Administering Device Discovery.”

The Network Servers feature allows you to associate HBAs and Ethernet network adapters that Cisco DCNM discovered with LLDP to servers. The topology map can show the network servers that you define.

Note Cisco DCNM supports discovery and management of VMware ESX servers, Linux servers, and Windows 2008 servers only.

The Network Servers feature also allows you to view server connectivity information.

Automatic Correlation of Adapters to Servers

If you provide Cisco DCNM with a valid username and password that it can use to log into a network server, Cisco DCNM can automatically associate the network adapters of a network server, which allows Cisco DCNM to retrieve enough information from the network server to determine which of the discovered adapters are a part of the same network server. The DCNM topology view displays a graphical representation of the associations between adapters and servers.

A network server is considered managed if Cisco DCNM can successfully log into the server and retrieve the connectivity information.

To more easily manage your network servers, you can use the DCNM server correlation feature to set up the login credentials for multiple servers. You can configure multiple servers to use the same credentials or unique credentials for each server.

Manual Correlation of Adapters to Servers

If you cannot provide Cisco DCNM with credentials to log into a network server, you can manually correlate, or bind, adapters to a network server.

Licensing Requirements for Network Servers

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Network Servers requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Network Servers

The Network Servers feature has the following prerequisites:

- LLDP must be enabled on network servers.
- Cisco DCNM must have discovered the network adapters of a server before you can use the Network Servers feature to correlate adapters automatically or bind them manually to a server.

Guidelines and Limitations for Network Servers

The Network Servers feature has the following configuration guidelines and limitations:

- Cisco DCNM can discover the network servers that run a Linux operating system.
- Cisco DCNM can automatically correlate the network servers for HBA ports that are manufactured by Emulex or Qlogic only.
- Cisco DCNM can automatically correlate the adapters on the Linux operating system and ESX servers only.
- Cisco DCNM supports CNAs that are manufactured by Emulex or Qlogic only.
- Because the CNA does not advertise the IP address of the server, you must manually correlate one CNA before you can trigger the automatic correlation of subsequent entries.

Configuring Network Servers

This section includes the following topics:

Configuring Default Server Credentials

You can configure the default server credentials, which Cisco DCNM uses to authenticate itself when it connects to a newly discovered server. Cisco DCNM uses the default server credentials to communicate with each discovered server that you have not configured with unique server credentials.

Note Server credentials are unique for each Cisco DCNM user.

BEFORE YOU BEGIN

Determine what the default server credentials should be. All servers that Cisco DCNM uses the default server credentials to communicate with must have a user account configured with a username and password that are identical to the default server credentials that you configure in Cisco DCNM.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The Server Credentials area appears in the Contents pane, above the Servers area, which lists the discovered servers.

Step 2 In the User Name field, enter the username for the default server credentials. A valid username can be 1 to 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Step 3 To the right of the Password field, click the down-arrow button.

Step 4 In the Password field and the Confirm Password field, enter the password for the default credentials. Valid passwords are numbers, symbols, and case-sensitive letters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to save the default credentials.

Clearing Default Server Credentials

You can clear the default server credentials.

Note If you clear the default server credentials, Cisco DCNM can connect to discovered servers only if you have configured unique credentials for each managed server.

BEFORE YOU BEGIN

If you intend to use Cisco DCNM without default server credentials, you should ensure that Cisco DCNM is configured with unique server credentials for each discovered server before you perform this procedure.

For more information, see the "Configuring Unique Credentials for a Server" section on page 9-5.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The Server Credentials area appears in the Contents pane, above the Servers area, which lists the discovered servers.

Step 2 In the Default Credentials area, click **Clear**.

The User Name field and the Password field clear.

Step 3 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Configuring Unique Credentials for a Server

You can configure credentials that are unique to a discovered server. When unique credentials exist for a discovered server, Cisco DCNM uses them when it connects to the server rather than using the default server credentials.

Note Server credentials are unique for each Cisco DCNM user.

BEFORE YOU BEGIN

Determine the username and password for a user account on the discovered server.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The discovered servers appear in the Servers area of the Contents pane.

Step 2 In the User Credentials column for the server, double-click the entry and then click the down-arrow button.

Step 3 In the User Name field, enter the username. Valid usernames are between 1 and 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Step 4 In the Password field and the Confirm Password field, enter the password. Valid passwords are numbers, symbols, and case-sensitive letters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to save the server credentials to the Cisco DCNM server.

Clearing Unique Credentials for a Server

You can clear unique credentials for a discovered server.

Note If you clear the unique credentials for a discovered server, Cisco DCNM uses the default credentials to connect to the server.

BEFORE YOU BEGIN

If you intend to operate Cisco DCNM without unique credentials for the server, ensure that Cisco DCNM is configured with default server credentials before you perform this procedure.

For more information, see the "Configuring Default Server Credentials" section on page 9-3.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

Discovered servers appear in the Servers area of the Contents pane.

Step 2 In the Servers area, click the server that has credentials that you want to clear.

Step 3 From the menu bar, choose **Actions > Clear Credentials**.

A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Correlating Servers

Correlating servers helps you manage a range of servers. An operation performed on a range of servers applies the operation to all the servers in that range

BEFORE YOU BEGIN

Ensure that the following have been confirmed and set for your appropriate platform.

- For Windows Server 2003:
  - Only Windows Server 2003 R2 (5.2.3970 or higher version) is supported.
  - WinRM system utility is installed.
    (Available from Windows Server installation CD or Microsoft Support site.)
  - Telnet service is enabled and running.
  - User level privileges are enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **iponfig /all** CLI command.
  - HBAs have been identified.
    To verify that the HBAs have been identified, you can use the **winrm e wmi/root/wmi/MSFC_FibrePortHBAAttributes** CLI command.

  Note Command output may display an error if an HBA is not installed on the server. This is expected. Ignore the error.

- For Windows Server 2008:
  - Windows Server 2008 Standard, Enterprise, and R2 (6.0.6001 or higher version) is supported.
  - WinRM system utility is installed.
  - Telnet service is enabled and running.
  - User level privileges are enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **iponfig /all** CLI command.

  - HBAs have been identified.
    To verify that the HBAs have been identified, you can use the **winrm e wmi/root/wmi/MSFC_FibrePortHBAAttributes** CLI command.

Note Command output may display an error if an HBA is not installed on the server. This is expected. Ignore the error.

- For RHEL:
  - RHEL 4.5 is supported.
  - SSH is enabled.
  - User level privileges are enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **ifconfig -a** CLI command.
  - HBAs have been identified.

    To verify that Qlogic HBAs have been identified, you can use the **grep adapter-port /proc/scsi/qla2xxx/*** CLI command.

    To verify that Emulex HBAs have been identified, you can use the
    find /sys/class/scsi_host/ -name port_name
    and the **find /sys/class/fc_host/ -name port_name** CLI commands.

    View the consolidated information by using 'cat' on the resulting files.
- For VMware ESX:
  - ESX 3.5 or higher version is supported.
  - SSH is enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **esxcfg-nics -l** CLI command.
  - HBAs have been identified.
    To verify that the HBAs have been identified, you can use the **esxcfg-scsidevs -a** CLI command.
  - HBAs and CNAs of Qlogic and Emulex have been tested and supported.

Note For a virtual machine, the HBA information is not displayed in the virtual machine. In the virtual machine display, the SAN details are disabled for the virtual machine. The HBA information is displayed in the ESX.

- Device version support:
  - For Nexus 7000, LLDP is supported from 5.0.
  - For Nexus 5000, LLDP is supported from4.2(1)N1(1).
  - For Nexus 5000, FC is supported for all versions.
  - For MDS, is supported from 3.3(2).

Table 9-1 Summary

	Windows Server 2003	Windows Server 2008	RHEL	ESX
Supported NIC	All	All	All	All
Supported HBA	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex
Supported CNA	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex
Operating System	R2 (All editions) 32 bit and 64 bit	All editions 32 bit and 64 bit	RHEL 4.5	ESX 3.5
Required service	Telnet/ssh WinRM	Telnet/ssh WinRM	SSH/Telnet	SSH/Telnet
Authority	User level privileges	User level privileges	User level privileges	User level privileges

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The discovered servers appear in the Servers area of the Contents pane.

Step 2 In the Servers pane, right-click to access the context menu.

Step 3 Select **New Server** in the context menu.
A new row for the server is displayed.

Step 4 In the IP Address field, enter the IP addresses of the range of servers.
IP address are delimited with commas or hyphens.
After the IP addresses are entered, the system validates the addresses. A red colored border indicates an error condition. A yellow colored border indicates a valid entry.

Step 5 Double-click the User Credentials field to access the Set User Credentials dialog box.

Step 6 In the User Name field, enter the username. Valid usernames are between 1 and 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Step 7 In the Password field and the Confirm Password field, enter the password. Valid passwords are numbers, symbols, and case-sensitive letters.

Step 8 Click **OK**.

Step 9 From the menu bar, choose **File > Deploy** to save the settings to the Cisco DCNM server.

Step 10 To start server correlation, right-click the row or a single server in the range to access the context menu.

Step 11 Select **Correlate** in the context menu.

The operation changes the status of each server to Discovering. When the operation completes, the adapters are bound to the servers. If the operation fails, the status of the server becomes Unreachable and accompanied with a message.

Correlating a Server to Adapters Automatically

Cisco DCNM can log into servers that run a Linux operating system and use the network connectivity information that it retrieves to correlate HBA network adapters that it has detected to the Linux server.

BEFORE YOU BEGIN

You must configure valid server credentials for the server that you want Cisco DCNM to correlate with HBA adapters automatically. You can configure credentials unique to the server, or if the credentials are valid with other servers, too, you can configure default server credentials.

Note If the server credentials are unavailable, you can bind the adapter to a server manually. For more information, see the "Binding Adapters to a Server Manually" section on page 9-9.

Cisco DCNM must have discovered one or more HBA network adapters and one network server.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Servers**.

Discovered servers appear in the Servers area of the Summary pane.

Step 2 Under the Server column, click the server that you want to correlate with adapters automatically.

Tip If you want to correlate more than one server at a time, press and hold **Ctrl** and then click each server that you want to correlate with adapters.

Step 3 Right-click on the selected server(s) and choose **Correlate Server(s)**.

Cisco DCNM begins discovering network connectivity information from the selected server(s).

After discovery completes, the Connected Switches column shows any additional connections correlated to the server. The local topology shown to the right of the selected server is also updated to show any connections correlated with the server.

Binding Adapters to a Server Manually

Cisco DCNM allows you to associate HBA network adapters that it has detected to a discovered server. This process does not depend upon Cisco DCNM being able to log into the server and retrieve information from it.

The connection between a managed device and the server can be displayed on the topology map after you have successfully bound the adapter to a server.

BEFORE YOU BEGIN

Cisco DCNM must have discovered one or more HBA network adapters.

Cisco DCNM must be able to reach the server to which you want to bind the adapter, either by IP address or DNS name.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Static Server-Adapter Mapping**.

The Contents pane lists discovered HBA network adapters.

Step 2 Press and hold the **Ctrl** key and then click each adapter that you want to bind to a server.

Step 3 Right-click on any selected adapter and choose **Bind to Server**.

The Enter Server Name dialog box appears

Step 4 In the Server Name field, enter the IP address or DNS name of the server, and then click **OK**.

Step 5 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

In the topology map, the connection between the adapter and the managed device is available for viewing when you choose to view the connections to end devices for the managed device.

Unbinding an Adapter from a Server

You can remove a server-adapter binding that you have created. This process does not depend upon Cisco DCNM being able to log into the server and retrieve information from it.

BEFORE YOU BEGIN

The server-adapter binding that you want to remove must exist in Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Static Server-Adapter Mapping**.

The Contents pane lists discovered HBA network adapters.

Step 2 Under the Server Port column, click the adapter that you want to unbind.

Step 3 Right-click the adapter and choose **Unbind from Server**.

The Server Name field for the selected adapter clears.

Step 4 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

In the topology map, the connection between the adapter and the managed device is no longer available for viewing.

Viewing Server Connectivity Information

You can view connectivity information for the Cisco DCNM server.

Step 1 From the Feature Selector pane, choose **Network Servers > Servers**.

The Summary pane lists discovered servers.

Step 2 In the Summary pane, click the server whose network connectivity information you want to view.

The local topology for the server appears to the right of the Summary pane.

Step 3 (Optional) If you want to view Ethernet network or storage area network connectivity for the server, on the Server Details tab, expand the **LAN Connectivity** or **SAN Connectivity** section, as needed.

Field Descriptions for Network Servers

This section includes the following field descriptions for the Network Servers feature:

- Field Descriptions for Servers, page 9-11
- Servers Summary Pane, page 9-11
- Field Descriptions for Server Credentials, page 9-13

Field Descriptions for Servers

This section includes the following field descriptions:

- Servers Summary Pane, page 9-11
- Server: Server Details: LAN Connectivity Section, page 9-12
- Server: Server Details: LAN Connectivity Section, page 9-12

Servers Summary Pane

Table 9-2 Servers Summary Pane

Field	Description
Server	*Display only.* DNS name or IP address of the server. If Cisco DCNM could not determine the DNS name of the server, the IP address is shown instead.
Connected Switches	*Display only.* Name and IP address of each discovered device that is connected to the server.
Status	*Display only.* Whether the Cisco DCNM server can connect to and log into the server. Valid values are as follows: • Managed—Cisco DCNM has successfully logged into the server during automatic correlation of the server adapters. • Unmanaged—Cisco DCNM has not attempted to log into the server yet. By default, a discovered server is unmanaged until you attempt to correlate its adapters automatically. • Unreachable—During automatic correlation of the server adapters, Cisco DCNM could not reach the server or authentication failed. A message indicates the reason for the status.

Server: Server Details: LAN Connectivity Section

Table 9-3 Server: Server Details: LAN Connectivity Section

Field	Description
Switch	
Name	*Display only.* Name and IP address of devices that the server is connected to with an Ethernet connection.
Port Name	*Display only.* Name of the Ethernet interface on the device, such as Ethernet1/2.
Server	
MAC Address	*Display only.* MAC address of the Ethernet adapter on the server that is connected to the device.
Port Name	*Display only.* Name of the interface on the server.

Server: Server Details: SAN Connectivity Section

Table 9-4 Server: Server Details: SAN Connectivity Section

Field	Description
Switch	
Name	*Display only.* Name and IP address of devices that the server is connected to with a Fibre Channel connection.
FC Port WWN	*Display only.* World Wide Name (WWN) of the Fibre Channel interface on the device.
Port Name	*Display only.* Name of the Fibre Channel interface on the device, such as Fc1/4.
Server	
FC Port WWN	*Display only.* World Wide Name of the HBA interface on the server.

Field Descriptions for Static Server-Adapter Mapping

Table 9-5 Static Server-Adapter Mapping Contents Pane

Field	Description
Server Port	*Display only.* Identifies the server adapter, depending upon the adapter type, as follows: • For an HBA adapter, this field displays the WWN assigned to the adapter. • For an Ethernet adapter, this field displays the MAC address of the adapter. Ethernet adapters appear on the Static Server-Adapter Mapping contents pane when the server does not advertise the IP address of the adapter in LLDP.
Server Name	DNS name or IP address of the network server that the adapter is bound to.

Table 9-5 Static Server-Adapter Mapping Contents Pane (continued)

Field	Description
Vendor	*Display only.* Name of the manufacturer of the adapter.
Switch Port	*Display only.* Name and WWN of the Fibre Channel interface on the connected device.
Switch Name	*Display only.* Name and IP address of the connected device.

Field Descriptions for Server Credentials

Table 9-6 Server Credentials Content Pane

Field	Description
Default Credentials	
User Name	Name of the server user account that the Cisco DCNM server uses to access servers that it is discovering or that it is managing. On the server, the user account must have adequate permissions to retrieve information about the server network adapters. **Note** The information in the User Credentials field in the Servers area overrides the information in the Default Credentials section.
Password	Password for the server user account specified in the User Name field. By default, this field is blank.
Servers	
IP Address	*Display only.* IPv4 address of the server.
Name	*Display only.* Name of the server. If Cisco DCNM cannot determine the name of the server, the IP address of the server is shown.
User Credentials	The server user account that Cisco DCNM uses to connect to the server. **Note** If you configure this field, Cisco DCNM uses the user account that you configure when it connects to the server. If this field is blank, Cisco DCNM uses the user account specified in the Default Credentials area. By default, this field is blank.
Status	*Display only.* Whether the Cisco DCNM server can connect to and log into the server. Valid values are as follows: • Managed—Cisco DCNM has successfully logged into the server during automatic correlation of the server adapters. • Unmanaged—Cisco DCNM has not attempted to log into the server yet. By default, a discovered server is unmanaged until you attempt to correlate its adapters automatically. • Unreachable—During automatic correlation of the server adapters, Cisco DCNM could not reach the server or authentication failed. A message indicates the reason for the status.

Additional References

For additional information related to administering Network Servers, see the following sections:

- Related Documents, page 9-14
- Standards, page 9-14

Related Documents

Related Topic	Document Title
Device discovery	*Chapter 5, "Administering Device Discovery"*
Topology map	*Chapter 8, "Working with Topology"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Network Servers

Table 9-7 lists the release history for this feature.

Table 9-7 Feature History for Network Servers

Feature Name	Releases	Feature Information
Network Servers	5.0(2)	Support was added.