Inventory

This chapter contains the following topics:

Viewing Inventory Information

Beginning with Cisco Prime DCNM release 6.x, you can view the inventory and the performance for both SAN and LAN switches by using the global Scope pane. You can select LAN, SAN, or both to view the inventory information. You can also export and print the inventory information.

You can either Print this information or export to Microsoft Excel.

Note You can use the **Print** icon to print the information that is displayed or you can also use the **Export** icon to export the information that is displayed to a Microsoft Excel spreadsheet. You can also choose the column that you want to display.

The Inventory menu includes the following submenus:

Viewing Inventory Information for Switches

To view the inventory information for switches from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The **Switches** window with a list of all the switches for a selected Scope is displayed.

Step 2 You can also view the following information.

- **Group** column displays the switch group to which the switch belongs.
- In the **Device Name** column, select a switch to display the Switch Dashboard.

- **IP Address** column displays the IP address of the switch.
- **WWN/Chassis ID** displays the Worldwide Name (WWN) if available or chassis ID.
- **Health** displays the health situation of the switch.

  Note To refresh and recalculate the latest health data for all the switches on Cisco DCNM, click the **Recalculate Health** button above the switches table.

- **Status** column displays the status of the switch.
- **# Ports** column displays the number of ports.
- **Model** column displays the model name of the switch.
- **Serial No.** column displays the serial number of the switch.
- **Release** column displays the switch version.
- **License** column displays the DCNM license that is installed on the switch.
- **Up Time** column displays the time period for which the switch is active.

Step 3 In the **Health** column, the switch health is calculated by the capacity manager based on the following formula in the server.properties file.

The function to implement is:

calculate(x, x1, y, y1, z).

@param x: Total number of modules.

@param x1: Total number of modules in warning.

@param y: Total number of switch ports.

@param y1: Total number of switch ports in warning.

@param z: Total number of events with severity of warning or above.

Step 4 The value in the **Health** column is calculated based on the following default equation.

((x-x1)*1.0/x) *0.4 + ((y-y1)*1.0/y)*0.3 + ((z*1.0/1000>=1) ? 0: ((1000-z)*1.0/1000)*0.3).

In the above formula, the switch health value is calculated based on the following:

- Percentage of Warning Modules (Contributes 40% of the total health).
- Percentage of Warning Ports (Contributes 30% of the total health).
- Percentage of events with severity of Warning or above (Contributes 30% of the total health. If there are more than 1000 warning events, the event health value is 0).

You may also have your own health calculation formula by implementing the common interface class: com.cisco.dcbu.sm.common.rif.HealthCalculatorRif. Add the `.jar` file to the DCNM server and modify the health.calculator property to point to the class name you have created.

The default Java class is defined as: health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculator.

- Capacity Manager calculates health only for the license switches. If the health column does not display a value, the switch either does not have a license or it has missed the capacity manager daily cycle.

- If the switch is unlicensed, click **Unlicensed** in the DCNM License column. The **Administration** > **License** window appears which allows you to assign a license to the user.
- The capacity manager runs two hours after the DCNM server starts. So, if you discover a device after two hours of the DCNM start time, the health will be calculated 24 hours after this DCNM start time

Viewing System Information

The switch dashboard displays the details of the selected switch.

Procedure

Step 1 From the Cisco DCNM home page, choose **Inventory** > **View** > **Switches**.

An inventory of all the switches that are discovered by Cisco DCNM Web UI is displayed.

Step 2 Click a switch in the **Device Name** column.

The **Switch** dashboard that corresponds to that switch is displayed along with the following information:

Step 3 Click the **System Information** tab. This tab displays detailed system information such as group name, health, module, time when system is up, serial number, the version number, contact, location, DCNM license, status, system log sending status, CPU and memory utilization, and VTEP IP address are displayed. Click **Health** to access the Health score screen, which includes health score calculation and health trend. The popup contains Overview, Modules, Switch Ports, and Events tabs.

- (Optional) Click **SSH** to access the switch through Secure Shell (SSH).
- (Optional) Click **Device Manager** to view a graphical representation of a Cisco MDS 9000 Family switch chassis, a Cisco Nexus 5000 Series switch chassis, a Cisco Nexus 7000 Series switch chassis, or a Cisco Nexus 9000 Series switch chassis including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.
- (Optional) Click **HTTP** to access the switch through Hypertext Transfer Protocol (HTTP) for that switch.
- (Optional) Click **Accounting** to go to the Viewing Accounting Information window pertaining to this switch.
- (Optional) Click **Backup** to go to the Viewing a Configuration window.
- (Optional) Click **Events** to go to the Viewing Events Registration window.
- (Optional) Click **Show Commands** to display the device show commands. The Device Show Commands page helps you to view commands and execute them.
- (Optional) Click **Copy Running Config to Startup Config** to copy the running configuration to the startup configuration.

Interfaces

Adding Interfaces

To add the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Add** to add a logical interface. The **Add Interface** window appears.
If you want to add a sub-interface, you select an interface and click **Add**.

Step 5 In the **Type** field, choose the type of the interface. For example, VLAN, loopback, NVE.

Step 6 In the **Number** field, specify the interface number.

Step 7 Select the **Admin State ON** check box to specify whether the interface is shut down or not.

Editing Interfaces

To edit the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Edit** to edit an interface. The variables that are shown in the **Edit Configuration** window are based on the template and its policy.

- The **Admin State ON** check box in the **Edit Configuration** window indicates whether the interface is shut down or not.
- The **Clear Config** before the deployment check box helps you to set a port to its default configuration. When there is a set of configurations already available on the port and these configurations conflict with the configurations that want to place on the port, you may need to clear the configurations before the deployment.
- In the **Preview** window, the left pane shows the configurations that the template generated based on your input, whereas the right pane shows the configurations that are currently available on the switch.

Deleting Interfaces

To delete the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Delete** to add a logical interface.

Shutting Down and Bring Up Interfaces

To shut down and bring up the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.
The **Switches** window is displayed with a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Shutdown** to disable an interface. For example, you may want to isolate a host from the network or a host that is not active in the network.

To enable an interface, Click **No Shutdown** button.

Displaying Interface Show Commands

To display interface show commands from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.
You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Show** to display the interface show commands.

The **Interface Show Commands** window helps you to view commands and execute them.

Rediscovering Interfaces

To rediscover interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The **Switches** window is displayed showing a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Rediscover** to rediscover the selected interfaces. For example, after you edit or enable an interface, you can rediscover the interface.

Viewing Interface History

To view the interface history from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

You see the Switches window displaying a list of all the switches for a selected Scope.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Interface History** to display the interface history details such as **Policy Name**, **Time of Execution**, and so on.

VLAN

You create a VLAN by assigning a number to it; you can delete VLANs and move them from the active operational state to the suspended operational state.

To configure VLANs, choose **Inventory** > **View** > **Switches**, and then click a switch in the **Device Name** column.

The following table describes the buttons that appear on this page.

Table 1: VLAN Tab

Field	Description
Clear Selections	Allows you to unselect all the VLANs that you selected.
Add	Allows you to create Classical Ethernet or Fabric Path VLANs.

Field	Description
Edit	Allows you to edit a VLAN.
Delete	Allows you to delete a VLAN.
No Shutdown	Allows you to enable a VLAN.
Shutdown	Allows you to disable a VLAN.
Show	Allows you to display the VLAN show commands.

This section contains the following:

Adding a VLAN

To add a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display the **Switch Dashboard**.

Step 3 Click the **VLAN** tab.

Step 4 Click **Add** to create Classical Ethernet or Fabric Path VLANs. In the **Add VLAN** window, specify the following fields:

a) In the **Vlan Id** field, enter the VLAN ID.
b) In the **Mode** field, specify whether you are adding Classical Ethernet or Fabric Path VLAN.
c) Select the **Admin State ON** check box to specify whether the VLAN is shut down or not.

Editing a VLAN

To edit a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The **Switches** window is displayed with a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display the **Switch Dashboard**.

Step 3 Select one or more VLANs, and then click the **Edit**.

Deleting a VLAN

To delete a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display the **Switch Dashboard**.

Step 3 Click **VLAN** tab.

Step 4 Select the VLAN that you want to delete, and then click **Delete**.

Shutting Down a VLAN

To shut down a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **VLAN** tab.

Step 4 Click **Shutdown** to disable a VLAN.

To enable a VLAN, click **No Shutdown** button. For example, if you want to start traffic flow on a VLAN you can enable it.

Displaying VLAN Show Commands

To display VLAN show commands from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The **Switches** window is displayed, showing a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **VLAN** tab.

Step 4 Click **Show** to display the VLAN show commands. Based on the VLAN selection, you can show the VLAN commands. **Interface Show Commands** window displays the commands and allows you to execute them.

FEX

The Fabric Extender feature allows you to manage a Cisco Nexus 2000 Series Fabric Extender and its association with the Cisco NX-OS switch that it is attached to. A Fabric Extender is connected to the switch through physical Ethernet interfaces or a Port Channel. By default, the switch does not allow the attached Fabric Extender to connect until it has been assigned a chassis ID and is associated with the connected interface. You can configure a Fabric Extender host interface port as a routed or Layer 3 port. However, no routing protocols can be tied to this routed interface.

Note FEX feature is available on LAN devices only. Therefore, you will see FEX on Cisco DCNM **Inventory Switches**. FEX is also not supported on Cisco Nexus 1000V devices.

Note 4x10G breakout for FEX connectivity is not supported on Cisco Nexus 9500 Switches.

Note The Fabric Extender may connect to the switch through several separate physical Ethernet interfaces or at most one port channel interface.

This section describes how to manage Fabric Extender (FEX) on Cisco Nexus Switches through Cisco DCNM.

You can create and manage FEX from Cisco DCNM **Inventory** > **Switches**.

Note FEX tab is visible only if you choose a LAN device.

The following table describes the fields that appear on this page.

Table 2: FEX Operations

Field	Description
Add	Click to add a new FEX to a Cisco Nexus Switch.
Edit	Select any active FEX radio button and click Edit to edit the FEX configuration. You can create an edit template and use it for editing FEX. Select template type as POLICY and sub type as FEX.
Delete	Select the FEX radio button, and click Delete icon to delete the FEX associated with the switch.

Field	Description
Show	Allows you to view various configuration details for the selected FEX ID. You can select the following from the drop-down list. • show_diagnostic • show_fex • show_fex_detail • show_fex_fabric • show_fex_inventory • show_fex_module The variables for respective show commands are displayed in the Variables area. Review the Variables and click **Execute**. The output appears in the **Output** area. You can create a show template for FEX. Select template type as SHOW and sub type as FEX.
FEX History	Allows you to view the history of the FEX configuration tasks for a particular FEX. You can review the Event Type, Policy Name, Status, Time of Execution, User Name for the selected FEX.

Table 3: FEX Field and Description

Field	Description
Fex Id	Uniquely identifies a Fabric Extender that is connected to a Cisco NX-OS device.
Fex Description	Description that is configured for the Fabric Extender.
Fex Version	Specifies the version of the FEX that is associated with the switch.
Pinning	An integer value that denotes the maximum pinning uplinks of the Fabric Extender that is active at a time.
State	Specifies the status of the FEX as associated with the Cisco Nexus Switch.
Model	Specifies the model of the FEX.
Serial No.	Specifies the configured serial number. **Note** If this configured serial number and the serial number of the Fabric Extender are not the same, the Fabric Extender will not be active.
Port Channel	Specifies the port channel number to which the FEX is physically connected to the Switch.
Ethernet	Refers to the physical interfaces to which the FEX is connected.

Field	Description
vPC ID	Specifies the vPC ID configured for FEX.

This chapter includes the following sections:

Add FEX

To add single-home FEX from the Cisco DCNM Web UI, perform the following steps:

Before you begin

You can add a Fabric Extender (FEX) to the Cisco Nexus Switches through the Cisco DCNM Web Client. If the FEX is physically connected to the switch, FEX will become online after it is added. If the FEX is not physically connected to the switch, the configuration is deployed to the switch, which in turn enables FEX when connected.

Note You can create only single homed FEX through **Inventory** > **Switches** > **FEX** > **Add FEX**. To create a dual-homed FEX, use the vPC wizard through **Configure** > **Deploy** > **vPC**.

Ensure that you have successfully discovered LAN devices and configured LAN credentials before you configure FEX.

Procedure

Step 1 Choose **Inventory** > **Switches** > **FEX**.

The **FEX** window is displayed.

Step 2 Click the **Add** FEX icon.

Step 3 In the General tab, in the **PORTCHANNEL** field, enter the interface port channel number which is connected to the FEX.

Step 4 In the **INT_RANGE** field, enter the interface range within which the FEX is connected to the switch.

Note Do not enter the interface range, if the interfaces are already a part of port channel.

Step 5 In the **FEX_ID** field, enter the ID for FEX that is connected to a Cisco NX-OS device.

The identifier must be an integer value between 100 to 199.

Step 6 Click **Add**.

The configured Single-home FEX appears in the list of FEXs associated to the device.

Edit FEX

To edit and deploy FEX from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Switches** > **FEX**.

The **FEX** window is displayed.

Step 2 Select the FEX radio button that you must edit. Click **Edit** FEX icon.

Step 3 In the Edit Configuration window, from the Policy drop-down list, select **Edit_FEX** to edit the FEX configuration.

Step 4 Edit the **pinning** and **FEX_DESC** fields, as required.

Note If you initially configured port 33 on the parent switch as your only fabric interface, all 48 host interfaces are pinned to this port. If you provision another port, for example 35, then you must perform this procedure to redistribute the host interfaces. All host interfaces are brought down and host interfaces 1 to 24 are pinned to fabric interface 33 and host interfaces 25 to 48 are pinned to fabric interface 35.

Step 5 Click **Preview**.

You can view the generated configuration for the selected FEX ID. The following is a configuration example for FEX ID 101.

```
fex 101
pinning max-links 1
description test
```

Step 6 After you review the configuration summary on the Preview window, on the Edit Configuration screen, click **Deploy** to deploy the FEX for the switch.

VDCs

This section describes how to manage Virtual Device Contexts (VDCs) on Cisco Nexus 7000 Switches through Cisco DCNM.

Users with the network administrator (network-admin) role can create Virtual Device Contexts (VDCs). VDC resource templates limit the amount of physical device resources available to the VDC. The Cisco NX-OS software provides a default resource template, or you can create resource templates.

You can create and manage VDCs from Cisco DCNM **Inventory** > **Switches** > **VDCs**. As Cisco DCNM supports DCNM on Cisco Nexus 7000 Series only, click an active Cisco Nexus 7000 Switch. After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies.

The following table describes the fields that appear on this page.

Table 4: Vdc Operations

Field	Description
Add	Click to add a new VDC.
Edit	Select any active VDC radio button and click Edit to edit the VDC configuration.

Field	Description
Delete	Allows you to edit the VDC configuration. Select any active VDC radio button and click Edit to edit the VDC configuration.
Resume	Allows you to delete the VDC. Select any active VDC radio button and click Delete to remove the VDC associated with the device.
Suspend	Allows you to suspend an active non-default VDC. Save the VDC running configuration to the startup configuration before suspending the VDC. Otherwise, you will lose the changes to the running configuration. **Note** You cannot suspend the default VDC. **Caution** Suspending a VDC disrupts all traffic on the VDC.
Rediscover	Allows you to resume a non-default VDC from the suspended state. The VDC resumes with the configuration that is saved in the startup configuration.
Show	Allows you to view the Interfaces and Resources that are allocated to the selected VDC. In the Interface tab, you can view the mode, admin-status, and operational status for each interface associated with the VDC. In the Resource tab, you can view the allocation of resources and current usage of these resources.

Table 5: Vdc Table Field and Description

Field	Description
Name	Displays the unique name for the VDC
Type	Species the type of VDC. The two types of VDCs are: • Ethernet • Storage
Status	Specifies the status of the VDC.
Resource Limit-Module Type	Displays the allocated resource limit and module type.

Field	Description
HA-Policy • Single Supervisor • Dual Supervisor	Specifies the action that the Cisco NX-OS software takes when an unrecoverable VDC fault occurs. You can specify the HA policies for single supervisor module and dual supervisor module configurations when you create the VDC. The HA policy options are as follows: **Single supervisor module configuration:** • Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device. • Reload—Reloads the supervisor module. • Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration. **Dual supervisor module configuration:** • Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device. • Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration. • Switchover—Initiates a supervisor module switchover. The default HA policies for a non-default VDC that you create is restart for a single supervisor module configuration and switchover for a dual supervisor module configuration. The default HA policy for the default VDC is reload for a single supervisor module configuration and switchover for a dual supervisor module configuration.
Mac Address	Specifies the default VDC management MAC address.
Management Interface • IP Address Prefix • Status	Species the IP Address of the VDC Management interface. The status shows if the interface if up or down.
SSH	Specifies the SSH status

Note If you change the VDC hostname of a neighbor device after initial configuration, the link to the old VDC hostname is not replaced with the new hostname automatically. As a workaround, we recommend manually deleting the link to the old VDC hostname.

This chapter includes the following sections:

Add VDCs

To add VDC from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Ensure that you have discovered the physical device using a username that has the network-admin role.

Obtain an IPv4 or IPv6 address for the management interface (mgmt 0) if you want to use out-of-band management for the VDC.

Create a storage VDC to run FCoE. The storage VDC cannot be the default VDC and you can have one storage VDC on the device.

Procedure

Step 1 Choose **Inventory** > **Switches** > **VDC**.

The **VDC** window is displayed.

Step 2 Click the **Add** VDC icon.

Step 3 From the drop-down list, select the VDC type.

You can configure the VDC in two modes.

- Configuring Ethernet VDCs
- Configuring Storage VDCs

The default VDC type is Ethernet.

Step 4 Click **OK**.

Configuring Ethernet VDCs

To configure VDC in Ethernet mode from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 In the General Parameter tab, specify the VDC **Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

Step 2 In the Allocate Interface tab, select the network interfaces (dedicated interfaces membership) to be allocated to the VDC.

Click **Next**.

Step 3 In the Allocate Resource tab, specify the resource limits for the VDC.

Select the radio button and choose **Select a Template from existing Templates** or **Create a New Resource Template**. VDC resource templates describe the minimum and maximum resources that the VDC can use. If you do not specify a VDC resource template when you create a VDC, the Cisco NX-OS software uses the default template, vdc-default.

- If you choose Select a Template from existing Templates, from the **Template Name** drop-down list, you can select **None**, **global-default**, or **vdc-default**.

  The template resource limits are detailed in the following below:

Table 6: Template Resource Limits

Resource	Minimum	Maximum
Global Default VDC Template Resource Limits		
Anycast Bundled		
IPv6 multicast route memory	8	8 Route memory is in megabytes.
IPv4 multicast route memory	48	48
IPv6 unicast route memory	32	32
IPv4 unicast route memory		
VDC Default Template Resource Limits		
Monitor session extended		
Monitor session mx exception		
Monitor SRC INBAND		
Port Channels		
Monitor DST ERSPAN		
SPAN Sessions		
VLAN		
Anycast Bundled		
IPv6 multicast route memory		
IPv4 multicast route memory		
IPv6 unicast route memory		
IPv4 unicast route memory		

Resource	Minimum	Maximum
VRF		

- If you choose Create New Resource Template, enter a unique **Template Name**. In the Resource Limits area, enter the minimum and maximum limits, as required for the resources.

You can edit individual resource limits for a single VDC through the Cisco DCNM **Web Client** > **Inventory** > **Switches** > **VDC**.

Click **Next**.

Step 4 In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if necessary.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.
- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button not to expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, which are separated by commas.
- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

Step 5 In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

Step 6 In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

Step 7 In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands that are executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

Configuring Storage VDCs

To configure VDCs in storage mode from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Create a separate storage VDC when you run FCoE on the device. Only one of the VDCs can be a storage VDC, and the default VDC cannot be configured as a storage VDC.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. The shared interface is allocated to both an Ethernet and a storage VDC.

Procedure

Step 1 In the General Parameter tab, specify the VDC **Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

Step 2 In the Allocate FCoE Vlan tab, select the available **Ethernet Vdc** from the drop-down list.

The existing Ethernet VLANs range is displayed. Select **None** not to choose any available Ethernet VDCs.

You can allocate specified FCoE VLANs to the storage VDC and specified interfaces.

Click **Next**.

Step 3 In the Allocate Interface tab, add the dedicated and shared interfaces to the FCoE VDC.

Note The dedicated interface carries only FCoE traffic and the shared interface carries both the Ethernet and the FCoE traffic.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. FCoE VLAN and shared interface can be allocated from same Ethernet VDC.

Click **Next**.

Step 4 In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if necessary.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.
- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button not to expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, which are separated by commas.

- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

Step 5 In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

Step 6 In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

Step 7 In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands that are executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

Edit VDC

To edit VDC from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Switches** > **VDC**.

The **VDC** window is displayed.

Step 2 Select the VDC radio button that you must edit. Click the **Edit** VDC icon.

Step 3 Modify the parameters as required.

Step 4 After you review the configuration summary on the Summary tab, click **Deploy** the VDC with the new configuration.

Switch On-Board Analytics

For the selected switch, the **Switch On-Board Analytics** dashboard displays the following charts:

Note The graph data cannot be retrieved if correct certificates are not added to the Switch. Ensure that the certificates are valid for nxapi feature and SAN analytics to function properly.

- Top 10 Slowest Ports
- Top 10 Slowest Target Ports
- Top 10 Slowest Flows

- Top 10 Slowest ITLs
- Top 10 Port Traffic
- Top 10 Target Ports Traffic
- Top 10 Flow Traffic
- Top 10 ITL Traffic

The following metrics are supported by the Switch On-Board Analytics charts:

- Read and Write Completion Time—Time that is taken for an IO to complete successfully, that is, the time gap between IO status from a Target and IO command from an Initiator. The following metrics are supported:
  - Read Completion Time Min
  - Read Completion Time Max
  - Write Completion Time Min
  - Write Completion Time Max

  The IO engine tracks the maximum and minimum IO completion time for read and write commands in the context of a switch’s port, target port, flows, initiators, and LUNs.
- Read and Write Initiation Time—Time that is taken for an IO to initiate, that is, the time gap between the first response packet from a Target and IO Command from Initiator. The following metrics are supported:
  - Read Initiation Time Min
  - Read Initiation Time Max
  - Write Initiation Time Min
  - Write Initiation Time Max

  The IO engine tracks the maximum and minimum IO initiation time for read and write commands in the context of a switch’s port, target port, flows, initiators, and LUNs.
- Read and Write IO Bandwidth—Read and write command bandwidth observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The IO bandwidth is computed at every four second time interval based on the number of bytes read or written.
- Read and Write IO Rate—Read and write command IO rate observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The IO rate is computed at every four second time interval that is based on the number of IO performed.
- Read and Write IO Size—Read and write command IO size observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The following metrics are supported:
  - Read IO Size Min
  - Read IO Size Max
  - Write IO Size Min
  - Write IO Size Max

The IO engine tracks the maximum and minimum IO size for read and write commands.

Viewing Switch On-Board Analytics

You can view the switch on-board analytics information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The discovered switches are displayed.

Step 2 Click a switch name in the **Device Name** column.

The **Switch** dashboard that corresponds to that switch is displayed.

Step 3 Click the **Switch On-Board Analytics** tab.

This tab displays the Switch On-Board Analytics charts.

Configuring Settings for the Switch On-Board Analytics Charts

Perform the following actions to configure the settings for the switch on-board analytics charts:

- From the **Show Time as** drop-down list, choose time to be shown in the charts. You can choose one of the following options:
  - **Microseconds**
  - **Milliseconds**
  - **Seconds**

  By default, **Microseconds** is chosen.

  Note The **Show Time** drop-down list is applicable only for the top ten slowest ports, target ports, flows, and ITLs.

- From the **Show Flow From** drop-down list, choose whether to show flows from a **Target** or from an **Initiator**. By default, flows from a **Target** are chosen.

  Note The **Show Flow From** drop-down list is applicable only for the charts displaying flows and ITLs.

- From the **Show bandwidth and Size as** drop-down list, choose the traffic information to be shown in the charts. You can choose one of the following options:
  - **Bytes**

- **KB**
- **MB**

By default, **Bytes** is chosen.

- Check the **Filter results** check box, and click either the **by fc port** or **by VSAN** radio button and specify the appropriate values to filter the chart results. The FC port value must be in the **fc** *slot*/*port* format and the VSAN value must be a digit within the allowed VSAN range.

  Click the Filter icon next to the **by fc port** to apply changes.

  Note Filtering results by VSAN is not applicable for the **Top 10 Slowest Ports** or **Top 10 Port Traffic** charts.

- Check the **Single Column** check box to display the charts in a single column instead of double columns.
- Click the **Refresh** icon in the upper-right corner to refresh the charts.

Viewing Switch On-Board Analytics Charts

Perform the following actions to view the charts under the **Switch On-Board Analytics** tab:

- View the charts for the top ten slowest ports, target ports, flows, and ITLs by choosing one of the following variables from the drop-down list:
  - **Read Completion Time**—The read command completion time observed in the context of a switch's port.
  - **Write Completion Time**—The write command completion time observed in the context of a switch's port.
  - **Read Initiation Time**—The read command initiation time observed in the context of a switch's port.
  - **Write Initiation Time**—The write command initiation time observed in the context of a switch's port.

  Note
  - By default, **Read Completion Time** is selected and all the units for time are in **Microseconds**.
  - Each chart contains a legend that provides information about the variable displayed. Each variable has a check box. Unselecting the check box removes the variable data from the chart or table.

- View the charts for the top ten port traffic, target port traffic, flow traffic, and ITL traffic by choosing one of the following variables from the drop-down list:
  - **Read IO Rate**—The read command data observed in the context of a switch's port.
  - **Write IO Rate**—The write command observed in the context of a switch's port.

- **Read IO Size**—The read command size observed in the context of a switch's port.
- **Write IO Size**—The write command size observed in the context of a switch's port.
- **Read IO Bandwidth**—The read command bandwidth observed in the context of a switch's port.
- **Write IO Bandwidth**—The write command bandwidth observed in the context of a switch's port.

Note

- By default, **Read IO Rate** is selected. The **Read IO Rate** is IO per second. Both **Rate** and **Bandwidth** units are per second over an 8-second range. The **Size** value is for the life of the switch or since the last clear command was run from the CLI.
- The **Read IO Size** and **Read IO Bandwidth** units are in bytes per second. You can change this unit by using the **Show Bandwidth and Size** drop-down list. You can choose from the three options: **Bytes**, **KB**, and **MB**.
- Each chart contains a legend that provides information about the variable displayed. Each variable has a check box. Unselecting the check box removes the variable data from the chart or table.

- Choose the format to display information from the **Show** drop-down list. You can choose one of the following formats:
  - **Chart**
  - **Table**
  - **Chart and Table**

Note

- To display information in the **Chart and Table** format, enlarge your browser window or check the **Single Column** check box on the upper right corner.
- The default for Top ten Slowest Ports and Top 10 Port Traffic is **Chart and Table**.

- Use the **Chart Type** drop-down list to display information in the **Bar Chart** or **Stacked Bar Chart**.
- Use the **Actions** drop-down list to export information in a CSV or PDF, or print the required information.
- To view a chart or a table in a new window, click the **Detach** icon on the upper-right corner of a chart or a table. After detaching a chart or table, you can view the top 25 slowest ports, target ports, flows, ITLs, or their traffic.

Viewing Inventory Information for Modules

To view the inventory information for modules from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Modules**.

The **Modules** window is displayed with a list of all the switches and its details for a selected Scope.

Step 2 You can view the following information.

- **Group** column displays the group name of the module.
- **Switch** column displays the switch name on which the module is discovered.
- **Name** displays the module name.
- **ModelName** displays the model name.
- **SerialNum** column displays the serial number.
- **2nd SerialNum** column displays the second serial number.
- **Type** column displays the type of the module.
- **Slot** column displays the slot number.
- **Hardware Revision** column displays the hardware version of the module.
- **Software Revision** column displays the software version of the module.
- **Asset ID** column displays the asset id of the module.
- **OperStatus** column displays the operation status of the module.

Viewing Inventory Information for Licenses

To view the inventory information for licenses from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Licenses**.

The **Licenses** window is displayed based on the selected Scope.

Step 2 You can view the following information.

- **Group** column displays the group name of switches.
- **Switch** column displays the switch name on which the feature is enabled.
- **Feature** displays the installed feature.
- **Status** displays the usage status of the license.
- **Type** column displays the type of the license.

- **Warnings** column displays the warning message.

Discovery

Starting from Cisco DCNM release 10.x, Cisco DCNM Web Client allows the **admin** to associate **user** to one or more device scope or group. That means you can only access and configure the associated group or scope devices based on Role Based Access Control (RBAC). Though you might not have the access to other users' associated devices, you can still see all the discovered devices under the **Inventory > Discovery** tab.

From the left menu bar, go to **Administration > Management Users**. You can create users and associate groups, manage remote authentication, and see all the connected clients. For more information about RBAC, navigate to **Management Users**.

Adding, Editing, Re-Discovering, Purging and Removing LAN, LAN Tasks and Switch

Cisco DCNM Web Client reports information that is obtained by the Cisco DCNM-LAN devices.

Tip If the discovered Device is not in the scope of the current user the check box for the LAN Device in the LAN table grays out.

This section contains the following:

Adding LAN Switches

To add LAN switches from the Cisco DCNM Web UI, perform the following steps.

Procedure

Step 1 Choose **Inventory > Discovery > LAN** Switches.

You see the list of LAN devices in the **Switch** column.

Step 2 Click the **Add** icon to add LAN.

You see the **Add LAN Devices**dialog box.

Step 3 Select **Hops from seed Switch** or **Switch List**. The fields vary depending on your selection.

Step 4 Enter the **Seed Switch** IP address for the fabric.

For LAN Switches Discovery, DCNM allow both IPv4 and IPv6 address for the Seed Switch.

Step 5 The options vary depending on the discovery type selected. For example, if you check **Use SNMPv3/SSH**, varied fields are displayed.

Step 6 Click the drop-down list and choose **Auth-Privacy** security level.

Step 7 Enter the **Community**, or user credentials.

Step 8 Select the LAN group from the LAN groups candidates which is in the scope of the current user.

Note Select DCNM server and click **Add** to add LAN switches.

Step 9 Click **Next** to begin the shallow discovery.

Step 10 In the **LAN Discovery** window, you can select all switches by using the checkbox next to the switch name column or select individual switches. Click Previous to go back and edit the parameters.

Note .

- In the Status column, if the switch status is **timeout** or **Cannot be contacted**, these switches cannot be added. Only the switches that are reachable and not managed yet are available to select. The checkbox is disabled for the switches that are not available
- When you add or discover LAN devices in DCNM, ICMP echo packets are sent as part of the discovery process. If you have a firewall that blocks ICMP messages, the discovery process fails. You can skip sending the ICMP echo packets by setting the **cdp.discoverPingDisable** server property to **true**. For more information about how to set a server property, see Server Properties.

Step 11 Select a switch and click **Add** to add a switch to the switch group.

If one of more seed switches is not reachable, it is shown as “unknown” on the shallow Discovery window.

Editing LAN Devices

To edit LAN devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Discovery** > **LAN Switches**.

Step 2 Select the check box next to the LAN that you want to edit and click **Edit** icon.

You see the **Edit LAN** dialog box.

Step 3 Enter the **Username** and **Password**.

Note Select **Credential** or **Management State** to change the Credential or Management state. If **Credential** is selected, you can change the SNMP version and Auth-Privacy if v3, username or password. If **Management State** is selected, you can change the status to managed or unmanaged.

Step 4 Select the LAN status as **Managed** or **Unmanaged**.

Step 5 Click **Apply** to save the changes.

Removing LAN Devices from Cisco DCNM

You can remove a LAN switch from Cisco DCNM.

Procedure

Step 1 Choose **Inventory** > **Discovery** > **LAN Switches**.

Step 2 Select the check box next to the LAN that you want to remove and click **Delete** to remove the switches and all their data.

Step 3 Click **Yes** to review the LAN device.

Rediscover LAN Task

Procedure

Step 1 Choose **Inventory** > **Discovery** > **LAN Switches**.

Step 2 Click **Rediscover LAN**.

Step 3 Click **Yes** in the pop-up window to rediscover the LAN.