Inventory

This section contains context-sensitive Online Help content for the **Web Client > Inventory** tab.

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

The Inventory menu includes the following submenus:

Viewing Inventory Information for Switches

Procedure

Step 1 From the menu bar, choose **Inventory > View > Switches**.
You see the **Switches** window displaying a list of all the switches for a selected Scope.

Step 2 You can also view the following information.

- In the **Device Name** column, select a switch to display the Switch Dashboard. For more information about switch dashboard, see the Switch Dashboard section.
- **IP Address** column displays the IP address of the switch.

- **WWN/Chassis ID** displays the World Wide Name (WWN) if available or chassis ID.
- **Health** displays the health situation of the switch.
- **Satus** 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 installed on the switch.

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's daily cycle.
- If the switch is unlicensed, in the DCNM License column click **Unlicensed**. 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

Interfaces

The Interfaces tab displays all the interfaces that are discovered for the switch. You can view interface information such as the interface name, admin status, operation status, reason, policy, speed, MTU, Mode, VLANs, IP/Prefix, VRF, PC, Neighbor, and Description.

The Interface tab is based on the port selected on the device view and only works with the device view.

The VMIS range is from 1 to 255. This range is same at interface and VSAN.

You can configure interfaces on **Inventory > View > Switches**.

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

Field	Description
Clear Selections	Allows you to unselect all the interfaces that you selected.
Add	Allows you to add a logical interface
Edit	Allows you to edit an interface.
Delete	Allows you to delete a logical interface.
No Shutdown	Allows you to enable an interface.
Shutdown	Allows you to disable an interface.
Show	Allows you to display the interface show commands.
Rediscover	Allows you to rediscover the selected interfaces.
Interface History	Allows you to display the interface history details.

This section contains the following:

Adding Interfaces

Procedure

Step 1 From the menu bar, 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 **Interfaces** tab.

Step 4 Click **Add** to add a logical interface. The Add Interface window appears.
If you want to add a subinterface, you need to select an interface and then 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 shutdown or not.

Editing Interfaces

Procedure

Step 1 From the menu bar, 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 **Interfaces** tab.

Step 4 Click **Edit** to edit an interface. The variables 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 shutdown or not.
- The Clear Config prior to deployment check box helps you to set a port to its default configuration. That is, 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 prior to 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

Procedure

Step 1 From the menu bar, 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 **Interfaces** tab.

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

Shutting Down Interfaces

Procedure

Step 1 From the menu bar, 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 **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

Procedure

Step 1 From the menu bar, 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 **Interfaces** tab.

Step 4 Click **Show** to display the interface show commands. The Interface Show Commands page helps you to view commands and execute them.

Rediscovering Interfaces

Procedure

Step 1 From the menu bar, 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 **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

Procedure

Step 1 From the menu bar, 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 **Interfaces** tab.

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

HBA Link Diagnostics

The HBA Link Diagnostics feature helps in validating the health of links between Host Bus Adapters (HBAs) and Cisco MDS switches in a network. The servers connect to Storage Area Networks (SANs) through hardware devices are called HBAs. This connectivity comprises of many optical and electrical components that may develop faults during their lifetime. The HBA Link Diagnostics feature allows identification of faulty cables, transceivers, ASICs, drivers, firmware issues or software issues, thereby eliminating dropped frames and ensuring reliable I/O operations of the server.

For more information about the Configuring HBA Link Diagnostics for Cisco MDS switches in a network, see the Cisco MDS 9000 Series NX-OS System Management Configuration Guide.

From the menu bar of Cisco DCNM Web Client, choose **Inventory** > **Switches**, and then click the **Interfaces** tab. The HBA diagnostic button appears in the interfaces tab for SAN discovered switches. Click the HBA diagnostic button to launch Host Diagnostic. The Link Diagnostic screen appears.

Supported Platforms

Cisco DCNM 10.4(1) enables you to run HBA Link Diagnostics on the following platforms:

- Cisco MDS 48-Port 16-Gbps Fibre Channel Switching Module: DS-X9448-768K9
- Cisco MDS 48-Port 32-Gbps Fibre Channel Switching Module: DS-X9648-1536K9
- Cisco MDS 24/10 SAN Extension Module (FC ports only): DS-X9334-K9
- Cisco MDS 9396S Multilayer Fabric Switch

Getting Loopback Capabilities

The **Get Loopback Capabilities** button is disabled when you click the Start button. The Loopback Capabilities button is to be used before clicking the Start button to see the capabilities of port or HBA.

Aborting Link Diagnostic Tests on a Port

If you want to stop the link diagnostic test, click the **Stop** button in the Link Diagnostic screen.

Disabling a Port From the Diagnostic Mode

You can click the **Disable Diagnostic** button for taking the port out of diagnostic mode when you have finished the testing.

Monitoring the Running Diagnostic Test

You can click the **Monitor existing Diag** button to begin monitoring a test that is already running. If no test is running, then you will be informed of this and Cisco DCNM will attempt to retrieve the results from the last test that ran and display them. If the port has already been taken out of diagnostic mode then retrieving of the results will fail and a message will be printed.

Displaying Diagnostic Test Results

If the **Show Results during polling** check box is selected, it will output the CLI progress details to the output window for each poll for the test progress. Otherwise results are only printed at test completion.

Performing HBA Link Diagnostic Tests

To run the HBA Host Diagnostic test, perform the following steps:

Procedure

Step 1 From the menu bar, choose **Inventory** > **Switches**, and then click the **Interfaces** tab. The HBA diagnostic button appears in the interfaces tab for SAN discovered switches. By default, the button is disabled until an interface is selected. However, only one interface can be selected for performing the diagnostic operation. If multiple interfaces are selected, the button will be disabled.

Step 2 Click the HBA diagnostic button to launch Host Diagnostic. The Link Diagnostic screen appears.

Step 3 Specify the following fields.

- Frames: Count—Generates frames required to conduct the traffic tests. The range is from 1-2147483646. The default is 1000000.
- Frames: Duration—Specifies the duration of the link diagnostics tests per level. The range is from 1-86400.
- Frame size: Fixed—Sets the fixed size for the traffic generated. The minimum frame size is set to 64. The maximum frame size is set to 2048. The step value is set to 100.
- Frame size: Random—Configures the maximum frame size for the traffic generated. The value of frame-size max must be a multiple of four. The range is from 64-2048. The default is 2048.
- Payload—Configures the payload for the traffic generated.
- Data Rate—Configures the rate of the traffic generation of the generator port. The default is 100%. You can select any one of the following line rates at one time:
  - 100%—100% of the line rate
  - 12.5%—12.5% of the line rate
  - 25%—25% of the line rate
  - 50%—50% of the line rate
  - 6.25%—6.25% of the line rate

- Loopback Level—Runs the selected level of the diagnostics test on the diagnostic port. You can select any one of the following levels at a time:
  - Remote XCVR-Optical
  - Remote MAC
  - Remote Electrical
  - Remote All

Step 4 Click the **Start** button.

- When you click the Start button, the port will go offline because of the Diagnostic operation. The test may run for a long time depending upon the settings and therefore you can exit the dialog to perform other operations or to start a test on another port. When you exit the dialog box, the test will continue to run but you cannot continue to monitor the progress. When you return to this dialog for a port that, where you already started a test, you can click on the monitor existing button to begin monitoring the test progress again.

VXLAN

You can view VXLANs and their details under the **VXLAN** tab.

To view VXLANs, choose **Inventory > View > Switches**, and then click a switch name in the **Device Name** column.

The following table describes the fields that are displayed:

Table 1: The VXLAN Tab

Field	Description
VNI	Displays the Layer 2 (network) or Layer 3 (VRF) VXLAN VNI that is configured on a switch.
Multicast address	Displays the multicast address associated with the Layer 2 VNI, if applicable.
VNI Status	Displays the status of the VNI.
Mode	Displays the VNI modes: Control Plane or Data Plane.
Type	Displays whether the VXLAN VNI is associated with a network (Layer 2) or a VRF (Layer 3).
VRF	Displays the VRF name associated with the VXLAN VNI if it is a Layer 3 VNI.

Field	Description
Mapped VLAN	Displays the VLAN or Bridge domain mapped to VNI.

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 2: 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.
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

Procedure

Step 1 From the menu bar, 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 shutdown or not.

Editing a VLAN

Procedure

Step 1 From the menu bar, 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 Select one or more VLANs, and then click the **Edit** button.

Deleting a VLAN

Procedure

Step 1 From the menu bar, 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

Procedure

Step 1 From the menu bar, 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 **Shutdown** to disable a VLAN. For example, if you want to stop traffic on a you can shut the 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

Procedure

Step 1 From the menu bar, 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 **Show** to display the VLAN show commands. Based on the VLAN selection, you can show the VLAN commands. Interface Show Commands page helps users to view commands and 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 **Web Client > Inventory Switches**. If a Cisco Nexus Switch is discovered as part of SAN fabric, FEX feature is not available. 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 a number of 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 **Web Client > 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 3: 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.
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 4: FEX Table Field and Description

Field	Description
Fex Id	Uniquely identifies a Fabric Extender that is connected to a Cisco NX-OS device.

Field	Description
Fex Description	Description configured for the Fabric Extender.
Fex Version	Specifies the version of the FEX associated with the switch..
Pinning	An integer value that denotes the maximum pinning uplinks of the Fabric Extender that will be 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.
vPC ID	Specifies the vPC ID configured for FEX.

This chapter includes the following sections:

Add FEX

To add single-home FEX, perform the steps below.

Before You Begin

Cisco DCNM allows you to 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 will be deployed to the switch, which in turn will enable FEX when connected.

Note You can create only single homed FEX through Cisco DCNM **Web Client > Inventory > Switches > FEX > Add FEX**. To create a dual-homed FEX, use the vPC wizard through Cisco DCNM **Web Client > Configure > Deploy > vPC**. For more information, see Add vPC.

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

Procedure

Step 1 From the menu bar, select **Inventory > Switches > FEX**.

Step 2 Click **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 will be connected to the switch.

Note You must 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, perform the steps below.

Procedure

Step 1 From the menu bar, select **Inventory > Switches > FEX**.

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 **Web Client > Inventory > Switches > VDCs**. As Cisco DCNM supports DCNM on Cisco Nexus 7000 Series only, click on 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 5: 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.
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. You must 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 saved in the startup configuration.

Field	Description
Show	Allows you to view the Interfaces and Resources 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 6: 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

This chapter includes the following sections:

Add VDCs

To add VDC, perform the steps below.

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.

You must 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 From the menu bar, select **Inventory > Switches > VDC**.

Step 2 Click **Add** VDC icon.

Step 3 From the drop-down list, select the VDC type.
You can configure the VDC in two modes.

- Ethernet VDC
- Storage VDC

The default VDC type is Ethernet.

Step 4 Click **OK**.

Configuring Ethernet VDCs

To configure VDC in Ethernet mode, perform the steps below.

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-defualt**, or **vdc-default**.

  The template resource limits are detailed in the table below.

Table 7: Template Resource Limits

Resource	Minimum	Maximum
Global Default VDC Template Resource Limits		
Anycast Bundleid		
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 Bundleid		
IPv6 multicast route memory		
IPv4 multicast route memory		
IPv6 unicast route memory		
IPv4 unicast route memory		
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 required.
- 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 to never 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, 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 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, perform the steps below.

Before You Begin

You must 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** to not choose any available Ethernet VDCs.

You can allocate specified FCoE VLANs to the storage VDC as well as 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 required.
- 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 to never 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, 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 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, perform the steps below.

Procedure

Step 1 From the menu bar, select **Inventory > Switches > VDC**.

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

The **Switch On-Board Analytics** dashboard displays the following charts:

- 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 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 taken for an IO to initiate, that is, the time gap between 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 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 by performing these steps:

Procedure

Step 1 From the left menu bar, choose **Inventory > View > Switches**.
An inventory of all the switches that are discovered by Cisco DCNM Web Client is 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** 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 10 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 **bandwidth and size** 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.

  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 10 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 10 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 hand corner.

- 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.

Viewing Inventory Information for Modules

Procedure

Step 1 From the menu bar, choose **Inventory > View > Modules**.
You see the **Modules** window displaying 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.

Viewing Inventory Information for Licenses

Procedure

Step 1 From the menu bar, choose **Inventory > View > Licenses**.
You see the **Licenses** window displaying the license type and the warnings. 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). Even 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, mange remote authentication and see all the connected clients. For more information about RBAC, please go to Management Users.

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

Cisco DCNM Web Client reports information 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 greys out.

This section contains the following:

Adding LAN Switches

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > LAN Switches**.
You see the list of LAN devices in the **Switch** column.

Step 2 Click on 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 menu and choose the **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 greyed out for the switches that are not available.

Step 11 Select a switch and click **Add** to add a switch to the switch group.
If the seed switch(es) are not reachable, it will be shown as “unknown” on the shallow Discovery window.

Editing LAN Devices

You can modify a LAN from Cisco DCNM Web Client.

Procedure

Step 1 From the menu bar, 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 **User Name** 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 Web Client.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > LAN Switches**.

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

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

Moving LAN Devices Under a Task

You can move LAN devices under a task to a different server using Cisco DCNM Web Client. This feature is available only in the federation setup and the Move LAN is displayed in the federation setup screen.

You can move the LAN from a sever that is down to an active server. The management state remains the same.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > LAN Switches**.

Step 2 Choose the LAN Devices(s) from the LAN table. Click **Move**.

Step 3 In the **Move LAN Tasks to another DCNM Server** dialog box, enter the LAN Device that need to be moved and specify the DCNM server.
All the LAN devices under the selected tasks will be moved.

Re-discover LAN Task

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > LAN Switches**.

Step 2 Click the rediscover LAN icon.

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

Purging LAN

You can clean and update the LAN discovery table through **Purge**.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > LAN Switches**.

Step 2 Click the Purge unreachable devices or dead links in selected LAN icon.

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

Note In case of a federation set-up, you will have to select the LAN to purge.

Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics

Cisco DCNM Web Client reports information obtained by the Cisco DCNM-SAN on any fabric known to Cisco DCNM-SAN.

This section contains the following:

Adding a Fabric

You can discover new fabric and start managing a fabric from Cisco DCNM Web Client. Before you discover a new fabric, ensure you create a SNMP user on the switch.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > SAN Switches**.
You see a list of fabrics (if any) managed by Cisco DCNM-SAN in the Opened column.

Step 2 Click on the**Add** icon to add a new fabric.
You see the **Add Fabric** dialog box.

Step 3 Enter the **Fabric Seed Switch** IP address for this fabric.

Step 4 (Optional) Check the SNMPV3 check box. If you check SNMPV3, the field **Community** change to **Username** and **Password**.

Step 5 Enter the **User Name** and **Password** for this fabric.

Step 6 Select the privacy settings from the **Auth-Privacy** drop-down list.

Step 7 (Optional) Check the **Limit Discovery by VSAN** checkbox to specify the included VSAN list or excluded VSAN list from the VSANs provided to discover a new fabric.

Step 8 (Optional) Check the **Enable NPV Discovery in all Fabrics** check box. If you check enable NPV discovery in all fabrics, the changes are applied to all the fabrics that are previously discovered.

Step 9 Click **Options** button and specify the **UCS User Name** and **UCS Password**.

Step 10 Click **Add** to begin managing this fabric.
You can remove single or multiple fabrics from the Cisco DCNM Web Client.

Deleting a Fabric

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > SAN Switches**.

Step 2 Select the check box next to the fabric that you want to remove and click **Delete** fabric icon to remove the fabric from the datasource and to discontinue data collection for that fabric.

Editing a Fabric

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > SAN Switches**.

Step 2 Select the check box next to the fabric that you want to edit and click on the **Edit** icon.
You see the **Edit Fabric** dialog box. You can edit only one fabric at a time.

Step 3 Enter a new fabric **Name**.

Step 4 (Optional) Check the SNMPV3 check box. If you check SNMPV3, the **Community** field change to **Username** and **Password**.

Step 5 Enter the **User Name** and **Password**, privacy and specify how you want DCNM Web Client to manage the fabric by selecting one of the status options.

Step 6 Change the fabric management state to **Managed, Unmanaged**, or **Managed Continuously**.

Step 7 Click **Apply** to save the changes.

Note In the **Inventory > Discovery > SAN Switches**, select the fabric for which the fabric switch password is changed. Click **Edit** , unmanage the fabric, specify the new password and then manage the fabric. You will not be able to open the fabric as the new password will not sync with the database. To open the fabric, you can go to **Configure > SAN > Credentials** to sync the password.

Moving Fabrics to Another Server Federation

This feature is only available on the federation setup and the Move Fabric is only displayed in the federation setup screen.

You can move the fabrics from a sever that is down to an active server. The management state will remain the same.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > SAN Switches**.

Step 2 Select the switch that need to be moved from the switches table and click **Move**.

Step 3 In the **Move Fabrics to another Federation server** dialog box, select the DCNM server where the fabrics will be moved. The server drop-down list will list only the active servers.

Rediscovering a Fabric

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > SAN Switches**.

Step 2 Select the check box next to the fabric and click the **Rediscover** icon.

Step 3 Click **Yes** in the pop-up window.
The **Fabric** will now be re-discovered.

Purging a Fabric

You can clean and update the fabric discovery table through the **Purge** option.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > SAN Switches**.

Step 2 Select the check box next to the fabric and click the **Purge** fabric icon.

Step 3 Click **Yes** in the pop-up window.
The **Fabric** will now be purged.

Adding, editing, removing, rediscovering and refreshing SMI-S Storage

The SMI-S providers are managed using the Cisco DCNM Web Client.

This section contains the following:

Adding SMI-S Provider

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Storage Devices**.

Step 2 Click the **Add** SMI-S provider icon.

Step 3 In the **Add SMI-S Provider** window, use the drop-down to select the **Vendor**.
All the supported vendor can be found in the drop-down list. Additional SMI-S storage vendors are discovered through a 'best effort' handler using the **Other** vendor option in the drop-down.

Note At least one valid DCNM license must be provisioned before adding SMI-S storage discovery data sources.

Step 4 Specify the **SMI-S Server IP**, **User Name** and **Password**.

Step 5 Specify the **Name Space** and **Interop Name Space**.

Step 6 By default, the **Port** number is pre-populated.
If you select the **Secure** checkbox, then the default secure port number is populated.

When using the **Secure** mode with EMC, the default setting is mutual authentication. For more information, see EMC's documentation about adding an SSL certificate to their trust store, or set SSLClientAuthentication value to *None* in the *Security_Settings.xml* configuration file and then restart the ECOM service.

Step 7 Click **Add**.
The credentials are validated and if it's valid the storage discovery starts. If the credential check fails, you will be prompted to enter valid credentials.

Deleting SMI-S Provider

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Storage Devices**.

Step 2 Use the check-box to select the SMI-S provider and click the **Delete** icon.
The provider is removed and all data associated with the provider is purged from the system.

Editing SMI-S Provider

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Storage Devices**.

Step 2 Use the check-box to select the SMI-S provider and click the **Edit** SMI-S provider icon.

Step 3 In the **Edit SMI-S Provider** window, use the drop-down to select the **Vendor**.

Step 4 Specify the **SMI-S Sever IP**, **User Name** and **Password**.

Step 5 Specify the **Name Space** and **Interop Name Space**.

Step 6 By default, the **Port** number is pre-populated.
If you select the **Secure** checkbox, then the default secure port number is populated.

Step 7 Click **Apply**.
The storage discovery is stopped and a new task is created using the new information and the storage discovery is re-started.

Re-Discover SMI-S Provider

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Storage Devices**.

Step 2 Use the check-box to select the SMI-S provider and click the **Rediscover** SMI-S provider icon.

Purge SMI-S Provider

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Storage Devices**.

Step 2 Use the check-box to select the SMI-S provider and click the **Purge** icon.
The providers are purged.

Adding, Editing, Re-discovering and Removing VMware Servers

Cisco DCNM Web Client reports information gathered by Cisco DCNM-SAN on any VMware servers supported by Cisco DCNM-SAN.

Note Ensure that the LAN and SAN are discovered before you add the vCenter on the datasource.

This section contains the following:

Adding a Virtual Center Server

You can add a virtual center server from Cisco DCNM Web Client.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.
You see the list of VMware servers (if any) that are managed by Cisco DCNM-SAN in the table.

Step 2 Click the **Add** icon.
You see the **Add VCenter** dialog box.

Step 3 Enter the **Virtual Center Server** IP address for this VMware server.

Step 4 Enter the **User Name** and **Password** for this VMware server.

Step 5 Click **Add** to begin managing this VMware server.

Deleting a VMware Server

You can remove a VMware server from the Cisco DCNM Web Client.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.

Step 2 Select the check box next to the VMware server that you want to remove and click **Delete** to discontinue data collection for that VMware server.

Editing a VMware Server

You can edit a VMware server from Cisco DCNM Web Client.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.

Step 2 Check the check box next to the VMware server that you want to edit and click **Edit** virtual center icon.
You see the **Edit VCenter** dialog box.

Step 3 Enter a the **User Name** and **Password**.

Step 4 Select managed or unmanaged status.

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

Rediscovering a VMware Server

You can rediscover a VMware server from Cisco DCNM Web Client.

Procedure

Step 1 From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.

Step 2 Select the check box next to the VMware that you want to rediscover.

Step 3 Click **Rediscover** virtual center icon.

Step 4 Click **Yes** in the dialog box.