Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide, Release 11.5(x)

First Published: 2020-12-22

Last Modified: 2022-03-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 9

CHAPTER 1

Overview

Cisco Data Center Network Manager

Cisco Data Center Network Manager (Cisco DCNM) automates the infrastructure of Cisco Nexus 5000, 6000, 7000, and 9000 Series Switches and Cisco MDS 9000 Series switches. Cisco DCNM enables you to manage multiple devices, while providing ready-to-use capabilities, such as, control, automation, monitoring, visualization, and troubleshooting.

Note The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Configuring the Device Connector is mandatory if you've deployed Cisco DCNM in LAN Fabric mode. If you did not configure Device Connector during installation, a message appears asking you to configure Device Connector everytime you login. If you check the **Do not show again**, the message will not appear. However, an alarm notification will be added under the **Alarms** icon.

The Cisco DCNM home page contains a navigation pane to the left, and shortcuts to a few Cisco DCNM features in the middle pane.

This guide provides comprehensive information about the UI functionality for Cisco DCNM SAN deployment.

The top pane displays the following UI elements:

- **Help**: Launches the context-sensitive online help.
- **Search**: Helps locate records according to the following search criteria:
  - Name
  - IP Address
  - WWN

    - Alias
    - MAC Address
    - Serial Number

- *User Role*: Displays the role of the user who is currently logged in, for example, admin.
- **Gear** icon: Click on the gear icon to see a drop-down list with the following options:
    - **Logged in as**: displays the user role of the current logged in user.
    - **DCNM SAN & DM**: Click to download the SAN Client and Device Manager setup. You can install FM Client and Device Manager for management.

      Your system Java cache remembers the older version of DCNM. Therefore, when you download the latest version on the DCNM SAN and DM, ensure that you clear the Java cache before launching the applications.
    - **Change Password**: Allows you to change the password for current logged in user.

      If you are a **network administrator** user, you can modify the passwords of the other users.
    - **About**: Displays the Version, Installation Type, and time since when the Web UI is operational.
    - **REST API Tool**: Allows you to examine the APIs invoked for every operation. See the *REST API Tool* section for more information about the API inspection.
    - **Logout**: Allows you to terminate the Web UI and returns to the login screen.

For more information about Cisco DCNM, see:

https://www.cisco.com/c/en/us/support/cloud-systems-management/data-center-network-manager-11/model.html.

REST API Tool

Operations like discovery, fabric management, monitoring, and so on, which are performed in Cisco DCNM Web UI, invoke HTTP calls to fetch and commit the information accessed. The REST API tool enables you to examine the API call by viewing the structure of an API call. This tool also provides a corresponding CURL request to help with building quick prototypes and testing APIs.

The **REST API Tool** dialog box has the following fields.

Table 1: Fields and Description for the REST API Tool Dialog Box

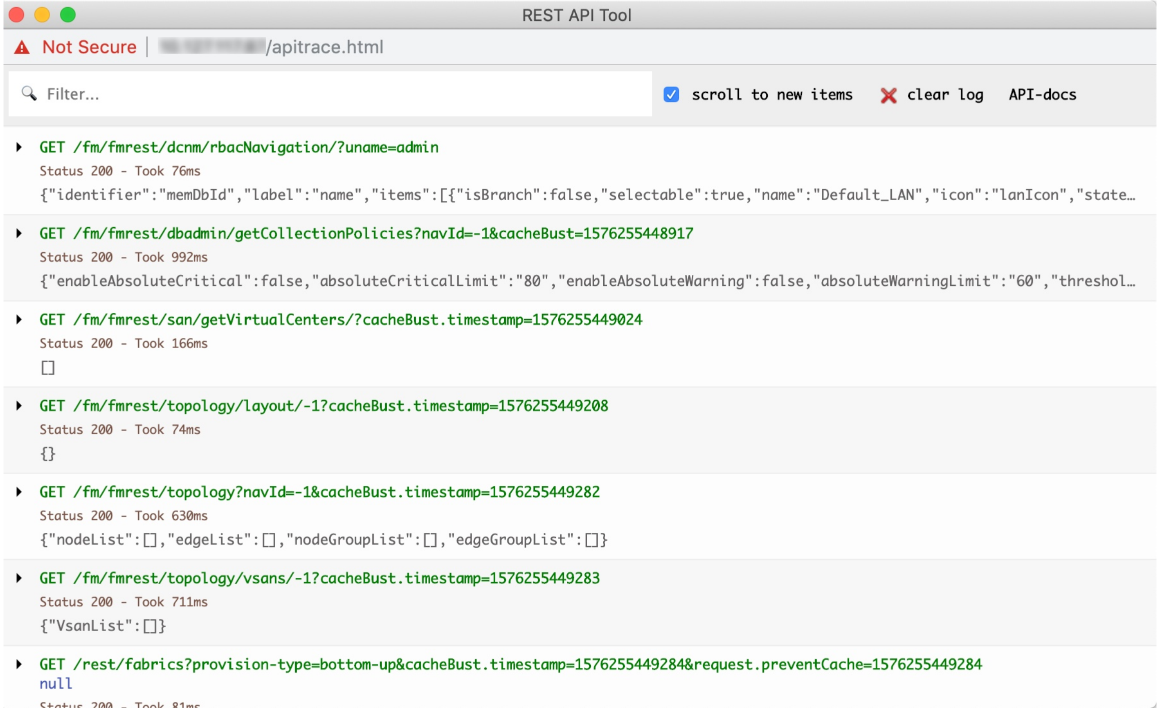
Field	Description
Filter	Enter any keyword to search the log.
scroll to new items	Check this check box to scroll to the new entries when you navigate back to the **REST API Tool** dialog box after you perform an operation in the Web UI. This check box is checked by default.

Field	Description
clear log	Click **clear log** to clear the log in the dialog box.
API-docs	Click API-docs to view the Cisco DCNM REST API documentation in the Web UI. Clicking this option takes you to the following URL: https://*DCNM-IP*/api-docs

All actions you perform in the Cisco DCNM Web UI appear in the API inspector tool. The following information appears in the APIs invoked for every operation:

- HTTP method
- URI
- Payload
- HTTP status code
- Time taken for the operation

The following image displays how the log appears in the **REST API Tool** dialog box.



[redacted]/apitrace.html

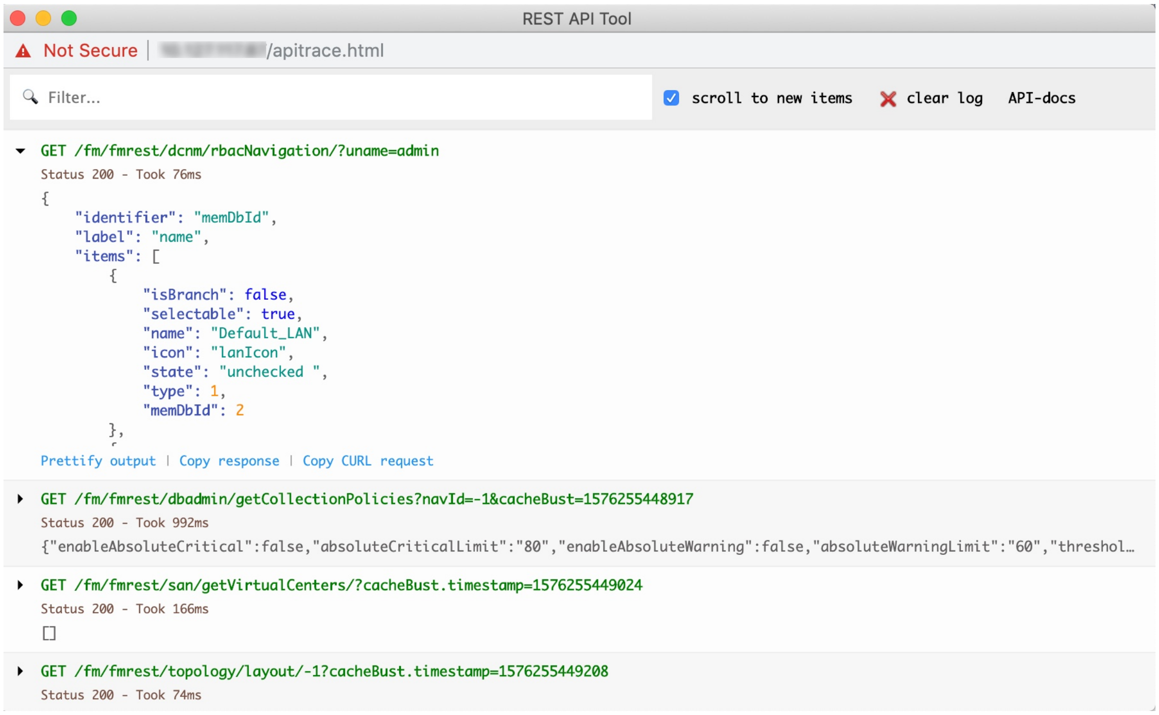
```
GET /fm/fmrest/dcnm/rbacNavigation/?uname=admin
Status 200 - Took 76ms
{"identifier":"memDbId","label":"name","items":[{"isBranch":false,"selectable":true,"name":"Default_LAN","icon":"lanIcon","state…

GET /fm/fmrest/dbadmin/getCollectionPolicies?navId=-1&cacheBust=1576255448917
Status 200 - Took 992ms
{"enableAbsoluteCritical":false,"absoluteCriticalLimit":"80","enableAbsoluteWarning":false,"absoluteWarningLimit":"60","threshol…

GET /fm/fmrest/san/getVirtualCenters/?cacheBust.timestamp=1576255449024
Status 200 - Took 166ms
[]

GET /fm/fmrest/topology/layout/-1?cacheBust.timestamp=1576255449208
Status 200 - Took 74ms
{}

GET /fm/fmrest/topology?navId=-1&cacheBust.timestamp=1576255449282
Status 200 - Took 630ms
{"nodeList":[],"edgeList":[],"nodeGroupList":[],"edgeGroupList":[]}

GET /fm/fmrest/topology/vsans/-1?cacheBust.timestamp=1576255449283
Status 200 - Took 711ms
{"VsanList":[]}

GET /rest/fabrics?provision-type=bottom-up&cacheBust.timestamp=1576255449284&request.preventCache=1576255449284
null
Status 200 - Took 81ms
```

Click the URI to expand or collapse each REST method. You can perform the following actions after expanding a REST method:

- **Prettify output**: Click this option to arrange the response code in a more presentable way, which otherwise appears in a single line. Scroll through the response to view it completely.
- **Copy response**: Click this option to copy the response code to your clipboard.

- **Copy CURL request**: Click this option to copy the CURL request to your clipboard.

```
curl -k -XGET --header 'Dcnm-Token: <DCNM_TOKEN>' --header 'Content-Type:
application/x-www-form-urlencoded'
https://<ip-address>/fm/fmrest/dcnm/rbacNavigation/?uname=admin
```


REST API Tool
Not Secure | [redacted]/apitrace.html
Filter...
☑ scroll to new items
✖ clear log
API-docs
Prettify output | Copy response | Copy CURL request

```
▾ GET /fm/fmrest/dcnm/rbacNavigation/?uname=admin
  Status 200 - Took 76ms
  {
      "identifier": "memDbId",
      "label": "name",
      "items": [
          {
              "isBranch": false,
              "selectable": true,
              "name": "Default_LAN",
              "icon": "lanIcon",
              "state": "unchecked ",
              "type": 1,
              "memDbId": 2
          },

▸ GET /fm/fmrest/dbadmin/getCollectionPolicies?navId=-1&cacheBust=1576255448917
  Status 200 - Took 992ms
  {"enableAbsoluteCritical":false,"absoluteCriticalLimit":"80","enableAbsoluteWarning":false,"absoluteWarningLimit":"60","threshol…

▸ GET /fm/fmrest/san/getVirtualCenters/?cacheBust.timestamp=1576255449024
  Status 200 - Took 166ms
  []

▸ GET /fm/fmrest/topology/layout/-1?cacheBust.timestamp=1576255449208
  Status 200 - Took 74ms
```

The **REST API Tool** dialog box updates every time the Cisco DCNM Web UI updates.

To use the API inspector from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Click the **Gear** icon in the top pane.

Step 2 Choose **REST API Tool** from the drop-down list.

The **REST API Tool** dialog box appears and the log is empty before you perform any operation in the Cisco DCNM Web UI.

Step 3 Minimize the **REST API Tool** dialog box.

Note You can also keep the dialog box open, but not close it.

Step 4 Perform an operation in the Cisco DCNM Web UI.

Note You can perform any operation in the Cisco DCNM Web UI like viewing any options, adding, deleting, and so on.

Step 5 Navigate back to the **REST API Tool** dialog box.

The log is populated with the REST APIs fetched depending on the operations you performed.

Note Closing the **REST API Tool** dialog box, instead of minimizing it before performing any operations, clears the log.

For a demo on some of the operations that can be performed using the REST API tool, see the Using REST API Tool in Cisco DCNM video.

CHAPTER 2

Dashboard

This chapter contains the following topics:

Summary Dashboard

The intent of the **Summary** dashboard is to enable network and storage administrators to focus on particular areas of concern around the health and performance of data center switching. This information is provided as 24-hour snapshots. The functional view of LAN and SAN switching consists of nine dynamic dashlets that display information in the context of the selected scope by default. The scope can be adjusted in the upper right corner of the window to display focused information that is particular to the managed domain. It offers details of a specific topology or set of topologies that is a part of the data center scope.

The various scopes that are available on the Cisco Data Center Network Manager (DCNM) web interface are:

- **Data Center**
- **Default_SAN**
- **Default_LAN**
- Each SAN Fabric
- Custom scopes that you create

From the left menu bar, choose **Dashboard** > **Summary**. The **Summary** window displays the default dashlets.

The following are the default dashlets that appear in the **Summary** window:

- Health
- Events
- Alarms
- Top ISLs/Port Channels

- Top SAN End Ports
- SAN Insights
- Errors
- Discards
- Inventory – Port Capacity

From the **Dashlets** drop-down list, you can choose more dashlets so that they are added to the Summary dashboard.

The panels can be added, removed, and dragged around to reorder.

Dashlets

By default, a subset of the available dashlets is automatically displayed in the dashboard. To add a dashlet that is not automatically displayed in a dashboard, from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard** > **Summary**.

Step 2 From the **Dashlets** drop-down list, choose the dashlet that you want to add in the dashboard.

In the **Dashlets** drop-down list, an icon appears before the selected dashlet.

The following table lists the dashlets that you can add on the **Summary Dashboard** window.

Dashlet	Description
Events	Displays events with **Critical**, **Error**, and **Warning** severity. In this dashlet, click the **Show Acknowledged Events** link to go to the **Monitor** > **Switch** > **Events**.
Alarms	Displays alarms with **Critical, Major, Minor**, and **Warning** severity. In this dashlet, click the **Show Acknowledged Alarms** link to go to the **Monitor** > **Alarms** > **View** window. Hover the mouse cursor over the blue **i** icon for more information about a specific alarm. Click **ACK** to acknowledge a specific alarm.
Link Traffic	Displays a diagram of Inter-Switch Link (ISL) and saturation link for transmitting and receiving in the data center.
Data Center	Displays the number of access, spine and leaf devices, and a generic health score for each switch group in the current scope. Devices are aggregated by type within a switch group.

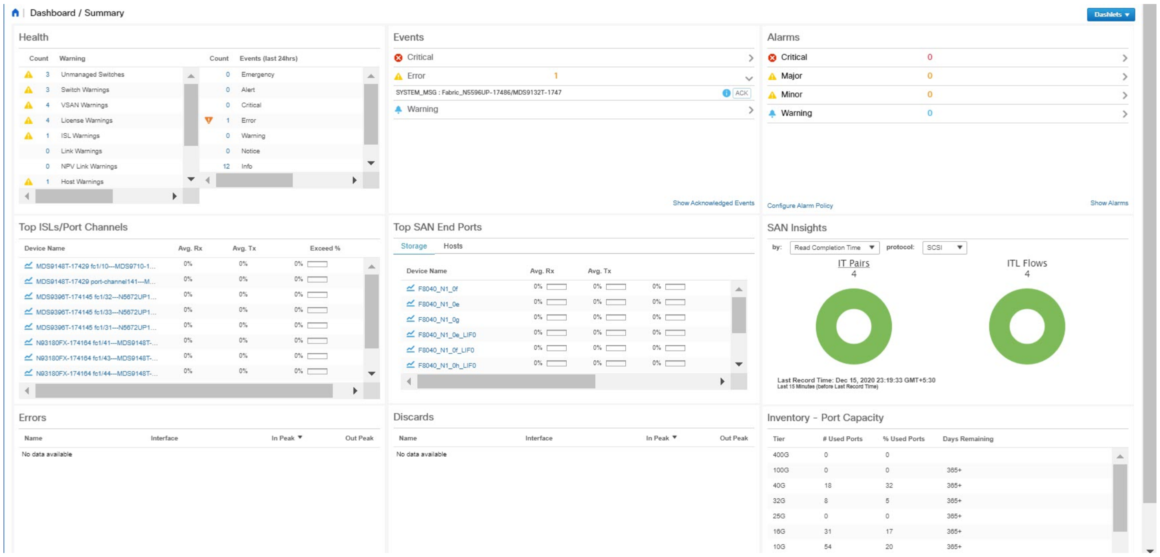
Dashlet	Description
Audit Log	Displays the accounting log table of Cisco DCNM.
Network Map	Displays the populated switch groups that are visible in your Role Based Access Control (RBAC) scope on a world map. If you use the scope selector, it limits the set of switch groups displayed. If you click detach option, the map opens in a new tab and can be configured. • The network map dialog box has properties that are different from the Summary dashboard view: • You can click and drag nodes to move them around the map. The map saves their new positions. • You can double click a node to trigger a slider that contains the summary inventory information pertaining to a specific switch group. • You can upload an image of your choice as the background to the network map. **Note** You will be prompted to upload an image file with recommended dimension, which is the current window size. Reset returns the network map to its default state, resetting the position of the nodes and clearing the custom image.
Server Status	Displays the status of DCNM and federation servers, and the health check status for the components. The following services, server, and status details are displayed under the **DCNM** tab. • Database Server • Search Indexer • Performance Collector • NTPD Server • DHCP Server • SNMP Traps • Syslog Server The following component status and details are displayed under the **Health Check** tab. • AMQP Server

Dashlet	Description
	- DHCP Server - TFTP Server - EPLS - EPLC
Top ISLs/Trunks	Displays the performance data for the top ten performing ISLs, trunk ports or both. Each entry shows the current average receive and transmit percentage, with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds.
Top SAN End Ports (SAN only)	Displays the performance data for the top ten performing SAN host and storage ports. Each entry shows the current receive and transmit percentage, with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds. **Note** This dashlet is only for SAN.
Top CPU	Displays CPU utilization for the discovered switches over the last 24 hours, with a red bar displaying the high watermark for that 24-hour period.
Top Temperature	Displays the module temperature sensor details of switches. **Note** This dashlet is only for LAN.
Health	Displays the health summary that contains two columns displaying the summary of problems and summary of events for the past 24 hours. Click the count adjacent to the warnings pertaining to switches, ISLs, hosts, or storage (other than 0) to view the corresponding inventory for that fabric. Click the count adjacent to the event severity levels (Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug) to view a summary of the corresponding events and descriptions. From Release 11.4(1), if you have deployed Cisco DCNM in HA mode, the Health Dashlet displays the status of the HA setup. Along with the HA State, it also displays the IP Addresses for the Active, Standby HA nodes and VIP.

Dashlet	Description
Errors	Displays the error packets for the selected interface. This information is retrieved from the **Errors > In-Peak** and **Errors > Out-Peak** columns of the **Monitor > LAN / Ethernet** page.
Discards	Displays the error packets that are discarded for the selected interface. **Note** The Discards dashlet is only for LAN.
Inventory (Ports)	Displays the ports inventory summary information.
Inventory (Modules)	Displays the switches on which the modules are discovered, the models name and the count.
Inventory (ISLs)	Displays the ISLs inventory summary information, such as the category and count of ISLs.
Inventory (Logical)	Displays the logical inventory summary information, such as the category and count of logical links.
Inventory (Switches)	Displays the switches inventory summary information such as the switch models and the corresponding count.
Inventory (Port Capacity)	Displays the port capacity inventory summary information such as the tiers, the number and percentage of the available ports, and the remaining days.
SAN Insights Flows (SAN only)	Displays donuts depicting the following: • Flow summary for **Initiator-Target (IT) Pairs** and **Initiator-Target- LUN(ITL Flows)** when the SCSI protocol is selected from the **protocol** dropdown list. • Flow summary for **Initiator-Target (IT) Pairs** and **Initiator-Target-Namespace (ITN Flows)** when the NVMe protocol is selected from the **protocol** dropdown list. You can display data for Read Completion Time or Write Completion Time by selecting the required option from the dropdown list. Hover over the sections on the donuts to display deviation percentage values. The percentage values can be configured as per your requirement by modifying the san.telemetry.deviation.low/med/high, san.telemetry.nvme.deviation.low/med/high and san.telemetry.default.protocol server properties.

Dashlet	Description
	The data-points are computed based on the last available 15 minutes of data in the Elasticsearch database. The **Last Record Time** is displayed in red if the data in the elasticsearch is older than 15 minutes for the selected **Scope**. For more information on SAN Insights, refer Introduction to SAN Insights. **Note** This dashlet is only for SAN.
Top FICON Host Ports	Displays data for top 10 performing FICON Channel (CH) Ports. Each entry shows port traffic of switch interface, specifies the device to which the FICON port is connected, specifies the average of Rx traffic and Tx traffic, and exceeded percentage value.
Top FICON Control Unit Ports	Displays data for top 10 performing FICON Control Unit (CU) Ports. Each entry shows port traffic of switch interface, specifies the device to which the FICON port is connected, specifies the average of Rx traffic and Tx traffic, and exceeded percentage value.
Top FCIP ISL	Displays data for top 10 performing FCIP ISLs. Each entry shows device name, specifies the average of Rx traffic and Tx traffic, and exceeded percentage value.

Note To restore the default dashlets in the dashboard page, click the **Default Set** link in the **Dashlet** drop-down list.



Dashboard / Summary

Health

Count	Warning	Count	Events (last 24hrs)
3	Unmanaged Switches	0	Emergency
3	Switch Warnings	0	Alert
4	VSAN Warnings	0	Critical
4	License Warnings	1	Error
1	ISL Warnings	0	Warning
0	Link Warnings	0	Notice
0	NPV Link Warnings	12	Info
1	Host Warnings		

Events

Critical	
Error	1
SYSTEM_MSG : Fabric_N5596UP-17486/MDS9132T-1747	ACK
Warning	

Alarms

Critical	0
Major	0
Minor	0
Warning	0

Top ISLs/Port Channels

Device Name	Avg. Rx	Avg. Tx	Exceed %
MDS9148T-17429 fc1/10---MDS9710-1...	0%	0%	0%
MDS9148T-17429 port-channel141---M...	0%	0%	0%
MDS9396T-174145 fc1/32---N5672UP1...	0%	0%	0%
MDS9396T-174145 fc1/33---N5672UP1...	0%	0%	0%
MDS9396T-174145 fc1/31---N5672UP1...	0%	0%	0%
N93180FX-174164 fc1/41---MDS9148T-...	0%	0%	0%
N93180FX-174164 fc1/43---MDS9148T-...	0%	0%	0%
N93180FX-174164 fc1/44---MDS9148T-...	0%	0%	0%

Top SAN End Ports

Device Name	Avg. Rx	Avg. Tx	
F8040_N1_0f	0%	0%	0%
F8040_N1_0e	0%	0%	0%
F8040_N1_0g	0%	0%	0%
F8040_N1_0e_LIF0	0%	0%	0%
F8040_N1_0f_LIF0	0%	0%	0%
F8040_N1_0h_LIF0	0%	0%	0%

SAN Insights

by: Read Completion Time ▾ protocol: SCSI ▾

Last Record Time: Dec 15, 2020 23:19:33 GMT+5:30
Last 15 Minutes (before Last Record Time)

Errors

Name	Interface	In Peak ▾	Out Peak
No data available			

Discards

Name	Interface	In Peak ▾	Out Peak
No data available			

Inventory - Port Capacity

Tier	# Used Ports	% Used Ports	Days Remaining
400G	0	0	
100G	0	0	365+
40G	18	32	365+
32G	8	5	365+
25G	0	0	365+
16G	31	17	365+
10G	54	20	365+

Storage Dashboard

The **Storage** dashboard provides information about the SAN and LAN storage.

To access the **Storage** dashboard, from the left menu bar, choose **Dashboard** > **Storage**.

Viewing Storage Enclosures Information

After a datasource is configured and the discovery is completed, the discovered storage systems are displayed under the **Name** column in the **Storage Enclosures** area. In this area, you can view details of SAN Storage Enclosures, Storage Systems, or both.

To view the storage enclosures information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard** > **Storage**.

Step 2 From the **Show** drop-down list, choose **SAN Storage Enclosures**.

Step 3 Choose the storage name to view more details.

The events, topology, and traffic information are displayed in the dashboard.

Step 4 To edit enclosure name, choose the storage name and click **Rename** icon. Enter a new name in the **Rename Enclosure** dialog box.

- You can rename each enclosure name to a different name. Choose the enclosure name, enter a new name, click **Save**. Repeat this procedure to change required all the required enclosure names, and click **Apply**.
- You can rename all enclosure names to the same new name. Check **Include All Members** checkbox, enter a new name, and click **Apply**.

Step 5 Click the **Filter** icon to filter the storage enclosures by **Name** or by **IP Address**.

Step 6 In the **Traffic** pane, the **Enclosure Traffic** is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.

Clicking on an individual port slice of the pie chart displays specific traffic utilization details for that port.

Viewing Storage Systems Information

To view information about storage systems from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard** > **Storage**.

Step 2 From the **Show** drop-down list, choose **Storage Systems**.

Note
- The datasource must be configured and discovered at least once to display the discovered storage system(s).
- Cisco DCNM now differentiate Block Storage and Filer Storage in terms of what it discovers and displays. Filer storage has additional elements: Shares, Quotas, and Q-trees.
  - **Shares**: Individual storage folders on the file server to which users have access.
  - **Quotas**: File and repository size limitations.
  - **Q-trees**: Tree based quotas. By using Q-trees, you can partition data and take advantage of different backup strategies, security styles, and settings.

Step 3 Click the **Click to see more details...** icon to view the storage systems summary.

The following are the elements of the **Storage Systems** area:

Components

Components are containers for a set or subset of the disks in a storage system. The Component elements view displays a table of disks in the collection, total number of disks managed. It also displays a summary of the collection's used vs. raw space.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 The right pane displays a summary of the storage components. Click each name to go to the item in the left menu.

Step 3 Hover the mouse cursor on the graph to display its details.

Step 4 In the left pane, select the storage component to view its details.

The number of disks that are managed along with its details are displayed.

Step 5 Click a Serial Number to display the disk and the mapped LUNs details.

Step 6 You can use the search box to search for a specific component.

Pools

Pools are user-defined collections of LUNs displaying the pool storage. The pools elements view displays a summary of the pools, lists the LUNs in the pool, and also displays the total managed and raw space.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

The bar graph next to each pool indicates the total managed space of that pool.

Step 2 In the left pane, select a pool to display:

- Status of the pool
- LUNs in the pool displaying the total raw space and the total managed space.
- Raid Type
- Disk Type
- Details of the LUNs in the pool

Step 3 You can use the search box to search for a specific pool.

LUNs

LUNs refer to a storage volume or a collection of volumes that are abstracted into a single volume. It is a unit of storage which can be pooled for access protection and management. Each LUN in the LUN Element View is displayed along with the mapping from Hosts to LUNs. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

You are able to create and delete LUNs, create and delete host and LUN maps, and create zoning for HLMs.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 You can create LUN from Cisco DCNM by choosing **Storage** > **LUNs**.

a) In the middle pane, click **Add LUN**.

b) Enter a valid **Name** for the LUN, and select its **Type** and **Size**. The pool which we carve the storage from is indicated.

Note The Create LUN pop-up window can also be accessed from a Pool's details page, when the LUN list view is selected.

c) Click **Add**.

A confirmation window displays each step. Once confirmed, the status is updated with the results of each step.

After LUN creation completes successfully, you can Assign Hosts, or click Close and assign Hosts later from the LUN Details view.

Step 3 Select a LUN in the left navigation pane to view the details.

- The LUN details along with its status and the number of Associated Hosts.
- The Host LUN Mapping details along with the Access (Granted) information.

If the associated fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.

Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Cisco DCNM. When the feature is disabled, all correlation fields display “Unlicensed Fabric.”

Step 4 You can delete LUNs in the SMI-S Storage Enclosure.

a) Navigate to **Storage** > **Storage System** > **LUNs**.

A list of LUNs in the SMI-S Storage Enclosure is displayed in the right.

b) Select one LUN from the list and then click **Remove**.

A confirmation window is displayed at each step. Once confirmed, the status will update with the results of each step.

c) Click **Apply**.

Step 5 You can add mapping from Host to LUN.

a) Select the **LUNs** from a pane on the left.

A list of LUNs in the SMI-S Storage Enclosure is displayed in the right.

b) Select a LUN from the list underneath.

The details for the selected LUN are displayed, including the current Host LUN Mappings for that LUN.

c) Click the **Add** button.

The **Add Hosts to Mask** window pops out.

d) Select one or more Hosts, and then click **Add**. The Hosts are then added to the LUN Mapping. In addition, each HLM pair is zoned if it is not already zoned.

Note Host LUN Mappings can also be added through the Host Dashboard. See Viewing Host Enclosures, on page 32, for more information.

Step 6 You can remove mapping from Host to LUN.

a) Select the **LUNs** from the pane on the left.

A list of LUNs in the SMI-S Storage Enclosure is displayed in the right.

b) Select a LUN from the list underneath.

The details for the selected LUN are displayed, including the current Host LUN Mappings for that LUN.

c) Select one or more existing Host LUN Mappings and click the remove icon.

A confirmation window appears and displays each step.

d) Click **Apply**.

The status will update with the results of each step.

Step 7 (Optional) You can add Zoning to the LUNs.

a) Select the **LUNs** from the left pane.

A list of LUNs in the SMI-S Storage Enclosure is displayed in the right.

b) Select a LUN from the list underneath.

The details for the selected LUN are displayed, including the current Host LUN Mappings for that LUN. One of the columns of the **Host LUN Mapping** table identifies the existing zones if any of the HLM currently has for zoning.

c) Select one or more HLMs which have Unknown or None for zoning, and click **Add Zoning**.

d) Click **Apply**.

The status will update with the results of each step.

Filer Volumes

Filer Volumes are applicable only for NetApp. The Filer Volume Element view displays the Status, Containing Aggregate along with the total capacity and used space.

To view filer volumes from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left pane, select the filer to display:

- The status of the filer along with the containing aggregate name.
- Hover the mouse cursor over the graph to view the total capacity and available storage of the filer.

Step 3 You can use the search box to search for a specific Filer.

Hosts

The Hosts describe the NWWNs associated with a host or host enclosure along with the associated Host-LUN Mapping and the Host Ports. If the associated Fabric has also been discovered, additional information concerning the connection between a host and LUN is also displayed.

To configure hosts from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Use the **Storage System** drop-down to select the storage system.

Step 2 In the left pane, select a Host to display:

- The NWWN (Node WWN) is the WWN of the device that is connected to the switch.
- The Host Ports along with the Host LUN Mapping.
- In the Host Ports section, click a Host Enclosure Name to view its Events, Topology, and SAN Traffic. For more information, see the Storage section.
- In the Host Ports sections, click a Host Interface to view the **Switch Dashboard**.
- In the Host-LUN Mapping section, click a Storage Interface to view the Switch Dashboard.
- In the Host-LUN Mapping section, click a Storage Name to view its Events, Topology, and SAN Traffic. For more information, see the Storage section.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the connection between the Host and LUN is also displayed.

Note All fabrics that are discovered must be licensed or the fabric correlation is disabled in the Web UI. When the feature is disabled, all correlation fields display “Unlicensed Fabric”.

Step 3 You can use the search box to search for a specific host.

Storage Processors

Storage processors are elements on a storage system, which enable some of its features. A storage processor includes the collection of storage ports it manages. In the Storage Processor Element View, the list of Storage Ports that are associated with a Storage Processor is displayed.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left pane, select a storage processor to display:

- The status, adapter details, and the number of ports of the storage processor.
- The storage ports details.

Step 3 You can use the search box to search for a specific storage processor.

Storage Ports

A storage port is a single port on the Storage System. It displays the summary information of each port selected.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left pane, select a storage port to display its details.

Step 3 You can use the search box to search for a specific storage port.

Viewing Storage Enclosure Events

To view the storage enclosure events information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard** > **Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

The list of storage enclosures is displayed in a table.

Step 2 Click the **Events** icon next to the storage enclosure to view the Events panel.

Step 3 You can use the slider control to resize the panel.

Viewing Storage Enclosure Topology

To view the storage enclosure topology information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard > Storage**. Use the drop-down to select **All**, **SAN Storage Enclosures**, or **Storage Systems**.

The list of storage enclosures in a table is displayed.

Step 2 Select the row to view the topology details.

Step 3 Use the mouse scroll wheel to zoom-in and zoom-out.

Step 4 Click the **Fabric/Network** icon to view the Fabric or Network path.

Step 5 Click the **All Paths** icon to view the complete setup.

Step 6 Click the **First Shortest Path** icon to view the shortest path.

Note Click **Map View** icon to enable the icons that are listed in the preceding Step 4, 5 and 6.

Step 7 Click the **Tabular View** icon to view the host topology in tabular format.

Viewing Storage Enclosure Traffic

To view the storage enclosure traffic from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

The list of storage enclosures is displayed in the table.

Step 2 Select the row to view the topology details.

Step 3 Use the drop-down to select the traffic according to the time duration.

Step 4 Select the icons to view the traffic as a **Grid, Line Chart** or **Stacked Chart**.

Step 5 Click the **Show Events** icon to view the events.

Step 6 Use the options at the bottom of the screen to view a pie chart or a line chart. Click on each name on the chart to view its details.

Introduction to SAN Insights

The SAN Insights feature enables you to configure, monitor, and view the flow analytics in fabrics. Cisco DCNM enables you to visualize the health-related indicators in the interface so that you can quickly identify issues in fabrics. Also, the health indicators enable you to understand the problems in fabrics. The SAN Insights feature also provides more comprehensive end-to-end flow-based data from the host to LUN.

From Release 11.2(1), Cisco DCNM supports SAN Telemetry Streaming (STS) using compact GPB transport, for better telemetry performance and to improve the overall scalability of SAN Insights.

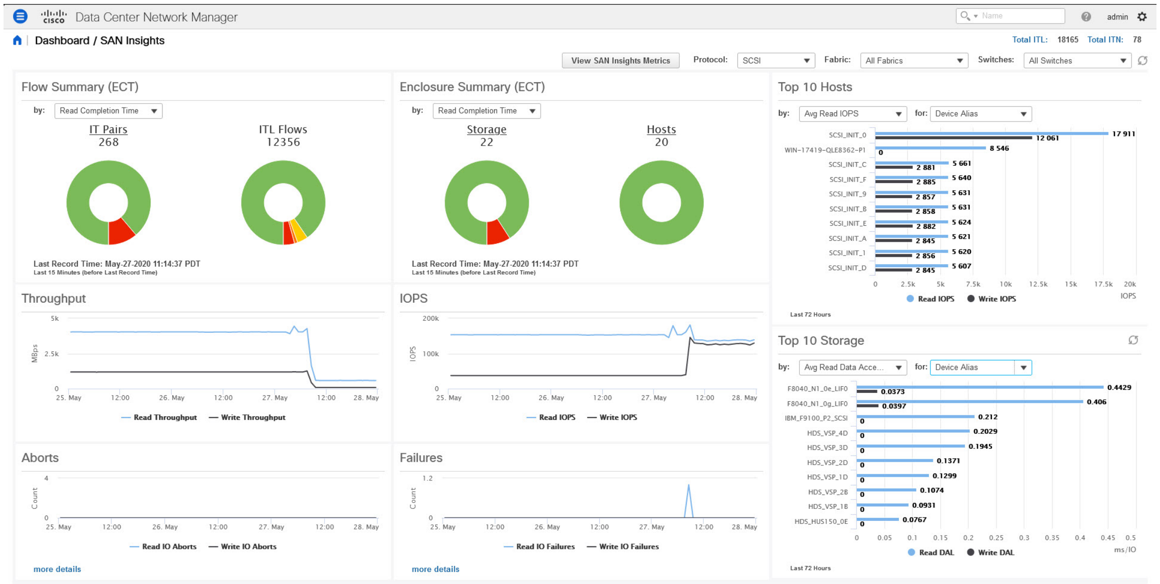
For SAN insights streaming stability and performance, refer to System Requirements section in the *Cisco DCNM Installation Guide for SAN Deployment Guide* and the section Increasing Elasticsearch Database Heap Size of the *Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide*. Ensure system RAM is of adequate size. Use of NTP is recommended to maintain time synchronization between the DCNM and the switches. Enable PM collection for viewing counter statistics.

SAN Insights Dashboard

Cisco DCNM visually displays fabric-level information in a holistic view from end-to-end. To view the SAN Insights Dashboard, choose **Dashboard** > **SAN Insights**. The SAN Insights Dashboard provides visibility for overall read/write IO operations/latency.

In the SAN Insights dashboard page, you can select protocol, fabric, and switches from protocol, fabric, and switches drop-down lists. The dashlets display insight data based on protocol, fabric, and switches that you select.

The dashboard displays the data over the last 72 hours. However, the Flow Summary and the Enclosure Summary donuts display the last 15 minutes from the latest updated time.



From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the

Administration > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

From the Fabric drop-down list, select the SAN Fabric for which you need to see the SAN Insights data and metrics. The switches that are capable and licensed for SAN Analytics are displayed in the drop-down list.

Note Click on the title on top of the donuts, to navigate to the relevant page on **Monitor** > **SAN** > **SAN Insights**. You can also click on different colored sections on the donuts to see more detailed counts in percentages.

The total distinct ITL count and the ITN count from the trained baseline is displayed in the top right-hand corner of the Dashboard. The donuts show the active ITL/ITN count only, for the last 15 minutes. The total ITL and ITN count, however, shows the count of all the ITLs and ITN for the scope selected.

The SAN Insights dashboard contains the following dashlets.

- Flow Summary (ECT)

  From the drop-down list, select Read Completion Time or Write Completion Time, based on which the donuts show IT Pairs and ITL Flows. These data-points are computed based on the last available 15mins data in the Elasticsearch.

- Enclosure Summary (ECT)

  From the drop-down list, select Read Completion Time or Write Completion Time, based on which the donuts display Storage and Hosts. These data-points are computed based on the last available 15mins data in the Elasticsearch.

- Throughput

  Displays the Read and Write throughput rate. Hover the mouse on the graph to view the value at that instance. The metrics in these line charts are computed based on the data during the last 72 hours.

- IOPS

  Displays the Read and Write IOPs trend. The metrics in these line charts are computed based on the data during the last 72 hours.

- Aborts

  Displays the Read and Write Aborts trend. The metrics in these line charts are computed based on the data during the last 72 hours. This metric is computed based on the **read_io_aborts** and **write_io_aborts** metric reported by the Cisco MDS SAN Analytics infrastructure.

  Click on **more details** to view the custom graphing for READ IO Aborts/Failures for the switch IP address that is selected on the Dashboard page.

- Failures

  Displays the Read and Write Failures trend. The metrics in these line charts are computed based on the data during the last 72 hours. This metric is computed based on the **read_io_failures** and **write_io_failures** metric reported by the Cisco MDS SAN Analytics infrastructure.

  Click on **more details** to view the custom graphing for READ IO Aborts/Failures for the switch IP address that is selected on the Dashboard page.

- Top 10 Hosts

Represents the top 10 Host Enclosures/WWPNs/Device Alias in the selected Protocol/Fabric/Switch scope based on the metric selected in the drop-down list. The data can be sorted by Read/Write IOPS, Throughput, Exchange Completion Time or Data Access Latency.

- Top 10 Storage

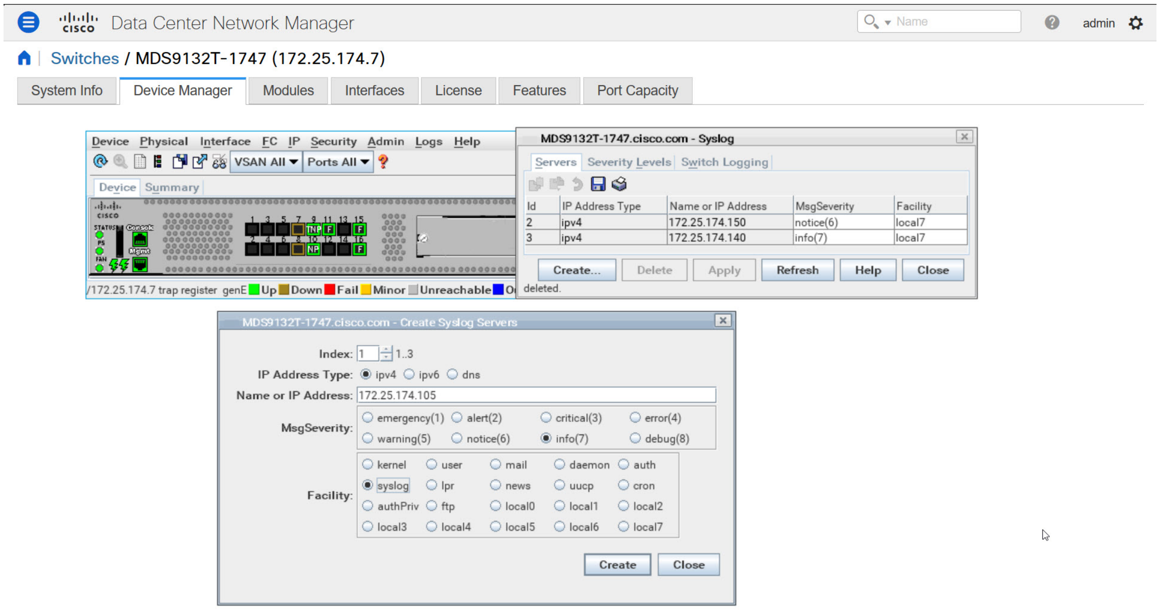
  Represents the top 10 Storage Enclosures/WWPNs/Device Alias in the selected Protocol/Fabric/Switch scope based on the metric selected in the drop-down list. The data can be sorted by Read/Write IOPS, Throughput, Exchange Completion Time or Data Access Latency.

Note The Top 10 Hosts and Top 10 Storage are computed over the last 72 hours, based on hourly data collected for the selected protocol, Fabric(s), and Switch(es). If you change the enclosure names for specific WWPNs, the names of the old enclosures names are visible until the data ages out after 72Hours.

A warning message appears as **HIGH NPU LOAD Detected** on top of the **Dashboard** > **SAN Insights** window. The warning implies that one or more switches has an unacknowledged Syslog event during the previous week. The event may affect the availability of the analytics data stored or displayed. You must acknowledge these events to remove the warning.

A warning appears as **HIGH ITL LOAD Detected** on top of the **Dashboard** > **SAN Insights** window. The warning is displayed when the number of ITLs seen in the last interval exceeds 20,000.

Ensure that you have configured Syslog on the DCNM Device Manager, to capture NPU and ITL Loads. Choose **Inventory** > **View** > **Switches**. Click on a switch to view System Info. On the Device Manager tab, click on **Logs** > **Syslog** > **Setup**. Click **Create**. Enter the required parameters. Ensure that you choose the **syslog** radio button in the Facility area. Click **Create** to enable Syslog on the DCNM server.



MDS9132T-1747.cisco.com - Syslog

Servers | Severity Levels | Switch Logging

Id	IP Address Type	Name or IP Address	MsgSeverity	Facility
2	ipv4	172.25.174.150	notice(6)	local7
3	ipv4	172.25.174.140	info(7)	local7

Create... | Delete | Apply | Refresh | Help | Close

deleted.

MDS9132T-1747.cisco.com - Create Syslog Servers

Index: 1 1..3

IP Address Type: ● ipv4 ○ ipv6 ○ dns

Name or IP Address: 172.25.174.105

MsgSeverity: ○ emergency(1) ○ alert(2) ○ critical(3) ○ error(4) ○ warning(5) ○ notice(6) ● info(7) ○ debug(8)

Facility: ○ kernel ○ user ○ mail ○ daemon ○ auth ● syslog ○ lpr ○ news ○ uucp ○ cron ○ authPriv ○ ftp ○ local0 ○ local1 ○ local2 ○ local3 ○ local4 ○ local5 ○ local6 ○ local7

Create | Close

To resolve the high NPU and high ITL loads, click on the **HIGH NPU LOAD Detected** or **HIGH ITL LOAD Detected** link. The **Monitor** > **Switch** > **Events** page appears. The list of events is filtered for **Type: HIGH_NPU_LOAD** and **Type: HIGH_ITL_LOAD**. Select all the switches and click **Acknowledge**. This removes the **HIGH NPU LOAD Detected** and **HIGH ITL LOAD Detected** warnings.

Viewing SAN Insights Metrics

To view the SAN Insights metrics, choose **Dashboard >SAN Insights**. The SAN Insights Dashboard page appears. Click the **View SAN Insights Metrics** button. From the **Use Case** drop-down list, choose **ECT Analysis** or **Custom Graphing**.

The dashboard displays the data over the last 72 hours. However, the Flow Summary and the Enclosure Summary donuts display the last 15 minutes from the latest updated time.

Note The refresh interval for ECT Analysis and Custom Graphing page is 5 minutes. Click on the Play icon ">" to refresh every 5 minutes automatically.

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

ECT Analysis

From the Cisco DCNM **Web UI** > **Dashboard** > **SAN Insights**, click on the View SAN Insights Metrics to view the ECT Analysis.

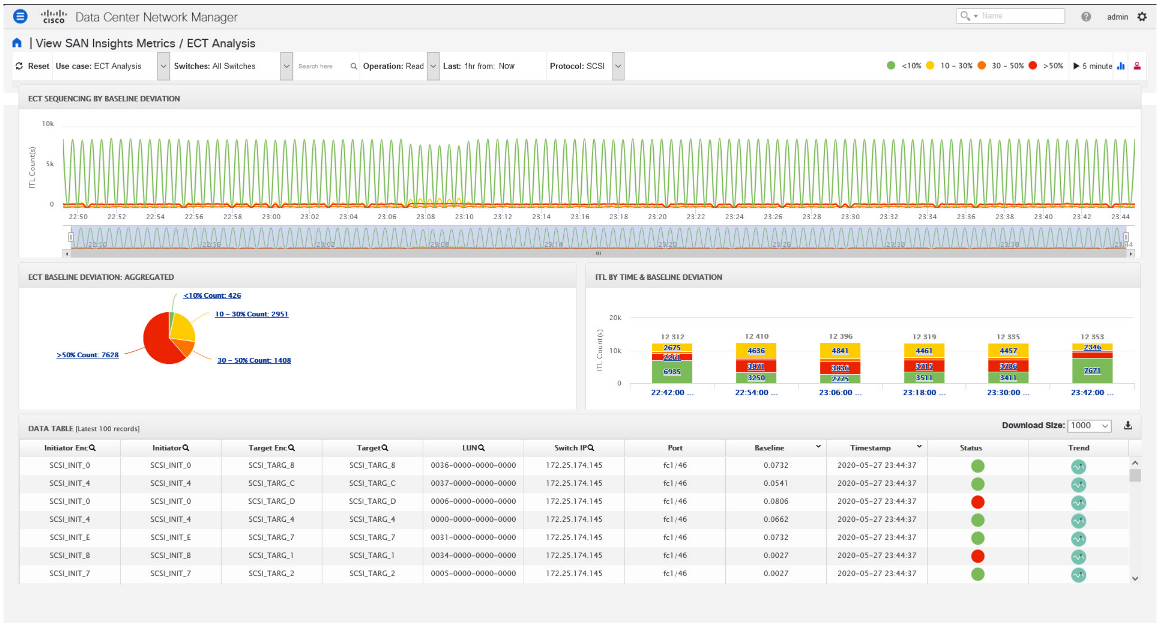
There are four components in ECT Analysis:

- Data table
- ECT Sequencing by Baseline Deviation
- ECT Baseline Deviation Aggregated
- ITL By Time & Baseline Deviation

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

From Release 11.4(1), Cisco DCNM allows you to view data for a time frame of any 14 days within the last 90 days. (up to a default maximum of 90 days). You can modify the **san.telemetry.expire.rollup property** on the **Web UI** > **Administration** > **DCNM Server** > **Server Properties** to modify the maximum default days. You can choose the date using the date picker and view the historical data starting from the selected date at hourly granularity.

Note The default duration of the ECT analysis 30 minutes60 minutes. You can click the **Reset** button to clear all the applied data filters.



Use case: ECT Analysis | Switches: All Switches | Operation: Read | Last: 1hr from: Now | Protocol: SCSI

Initiator Enc	Initiator	Target Enc	Target	LUN	Switch IP	Port	Baseline	Timestamp	Status	Trend
SCSI_INIT_0	SCSI_INIT_0	SCSI_TARG_8	SCSI_TARG_8	0036-0000-0000-0000	172.25.174.145	fc1/46	0.0732	2020-05-27 23:44:37	🟢	
SCSI_INIT_4	SCSI_INIT_4	SCSI_TARG_C	SCSI_TARG_C	0037-0000-0000-0000	172.25.174.145	fc1/46	0.0541	2020-05-27 23:44:37	🟢	
SCSI_INIT_0	SCSI_INIT_0	SCSI_TARG_D	SCSI_TARG_D	0006-0000-0000-0000	172.25.174.145	fc1/46	0.0806	2020-05-27 23:44:37	🔴	
SCSI_INIT_4	SCSI_INIT_4	SCSI_TARG_4	SCSI_TARG_4	0000-0000-0000-0000	172.25.174.145	fc1/46	0.0662	2020-05-27 23:44:37	🟢	
SCSI_INIT_E	SCSI_INIT_E	SCSI_TARG_7	SCSI_TARG_7	0031-0000-0000-0000	172.25.174.145	fc1/46	0.0732	2020-05-27 23:44:37	🟢	
SCSI_INIT_B	SCSI_INIT_B	SCSI_TARG_1	SCSI_TARG_1	0034-0000-0000-0000	172.25.174.145	fc1/46	0.0027	2020-05-27 23:44:37	🔴	
SCSI_INIT_7	SCSI_INIT_7	SCSI_TARG_2	SCSI_TARG_2	0005-0000-0000-0000	172.25.174.145	fc1/46	0.0027	2020-05-27 23:44:37	🟢	

Note The **Last** filter displays the period of historical data. The default period of the historical data is 30 minutes60 minutes.

When you upgrade from Release 11.1(1) to 11.2(1) or 11.3(1), the old data takes two weeks to age out. The performance of the SAN Insights metrics improves after two weeks, after the upgrade.

Note The data in the ECT Analysis view can be filtered by selecting the switch from the drop-down list or by specifying the WWPN\Enclosure Name\LUN-ID\Switch-IP in the **Search here** field. From Release 11.4(1), you can filter it by Device Alias, also.

You can enter the text in the **Search here** field to search for the value in the **ECT Sequencing by Baseline Deviation** table.

The **Search here** field in the filters indicates that you must search for their value.

The ECT Analysis page is representing the aggregated behavior of the ITL Flows by comparing the current normalized Exchange Completion Time (ECT) to its historical behavior (ECT Baseline) using the below logic. The normalized ECT value is the amount of time it takes to transfer a KB (kilobyte) of data.

ECT Baseline for each ITL Flow (Reads and Writes) is calculated using weighted average learned continuously over a training period:

- The ECT Baseline computation consists of two parts: the training period and the recalibration time.
- The training period for ECT Baseline is seven days by default (configurable).
- After the training is completed, the ECT Baseline remains the same until the recalibration is triggered after 7 days by default (configurable).
- By default every 14 days training runs for seven days (cyclic).

- The percentage (%) deviation shows the deviation of the current normalized ECT compared to the ECT Baseline.

Note Starting 11.4 release, the deviation of the ECT less than the baseline is considered as negative deviation. The Web UI screens are expected to display negative values for the computed deviation percentage.

Beginning from Release 11.4(1), the flows that have ECT lesser than the baseline is identified as having negative deviation. This impacts the average ECT deviation, reducing the severity of momentary spikes. However, it reflects a better true value of ECT performance.

When you upgrade to Release 11.4(1), some pages on the Web UI does not display correct color for older data. After two weeks, the new data will show proper color codes.

Note

- To configure the default training period, edit the `san.telemetry.train.timeframe` parameter (default 7) in the Cisco DCNM **Administration** > **Server Properties**. Restart the DCNM Server process. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)
- To configure the recalibration time, edit the `san.telemetry.train.reset` parameter (default 14 days) in the Cisco DCNM **Administration** > **Server Properties**. Restart the DCNM Server process. Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments.
- For example, to train the baseline for four days and recalibrate the baseline 10 days after the training period set the training period to four days and the recalibration time to 14 days.

Table 2: Baseline Color Legends

Relation	Value
If ECT is above 50% from Baseline	Red
If ECT is above and in range 30–50% from Baseline	Orange
If ECT is above and in range 10–30% from Baseline	Yellow
If ECT is below 10% from Baseline	Green (implies Normal)

The range of value for the Baseline Color Legends can be modified on the Server Properties file. See the **san.telemetry.deviation** definitions in the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments.

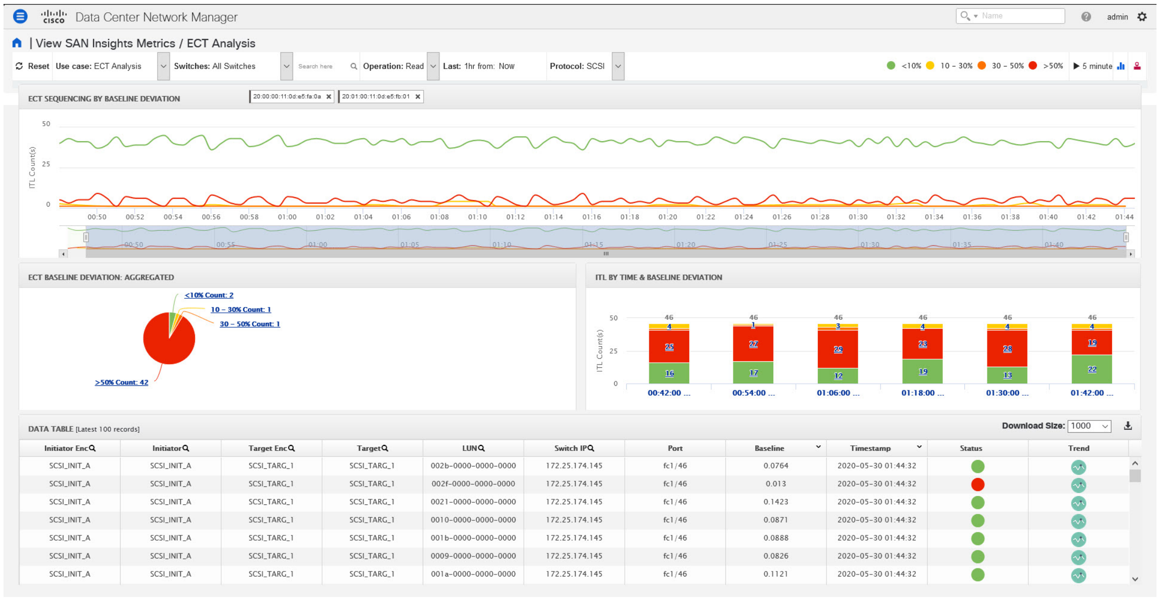
You can click on the Trend Identifier (📊) icon to navigate to Trend Identifier. For more information, see Trend Identifier, on page 29.

The data in the ECT Analysis UI can be filtered to view data of ITLs corresponding to the above legend, by clicking the circles to disable and enable. For example, on clicking and disabling the Yellow and Orange legend circles, the corresponding data will be displayed.

You can copy and paste the values in the data table into the **Search here** input field at the top of the UI to filter the data in all components. Values in all the columns marked with Magnifying Glass (🔍) icon in the data table are the only fields searchable for this functionality.

The data in the ECT BASELINE DEVIATION AGGREGATED component shows the number of ITLs that are in each deviation range. Similarly, the data in ITL BY TIME component shows the number of ITLs grouped by time that are in each deviation range. Clicking on a section of the pie chart or histogram shows drill down data with Initiator Enclosures, Initiator WWPNs, Target Enclosures, Target WWPNs, and LUN/Namespaces. Click on the corresponding section of the chart to download the results in a `.csv` format.

Note The maximum ECT Baseline Deviation aggregated data is set to 20000.



DATA TABLE [Latest 100 records]

Initiator Enc🔍	Initiator🔍	Target Enc🔍	Target🔍	LUN🔍	Switch IP🔍	Port	Baseline	Timestamp	Status	Trend
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002b-0000-0000-0000	172.25.174.145	fc1/46	0.0764	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002f-0000-0000-0000	172.25.174.145	fc1/46	0.013	2020-05-30 01:44:32	🔴	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0021-0000-0000-0000	172.25.174.145	fc1/46	0.1423	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0010-0000-0000-0000	172.25.174.145	fc1/46	0.0871	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	001b-0000-0000-0000	172.25.174.145	fc1/46	0.0888	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0009-0000-0000-0000	172.25.174.145	fc1/46	0.0826	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	001a-0000-0000-0000	172.25.174.145	fc1/46	0.1121	2020-05-30 01:44:32	🟢	

Script Timeout Error in Mozilla browser

In the Mozilla browser, if you see script timeout error with option **Stop** or **Wait**, don’t click **Stop**. Perform the following steps to troubleshoot the script timeout error.

1. Launch the Mozilla Firefox.
2. On the Firefox address bar type **about:config** and press Return key.
3. In the confirmation message, click **I accept the risk!**.
4. In the Search field, enter **dom.max_script_run_time**.

   The Preference names are displayed.

5. Right click on the **dom.max_script_run_time** Preference name.

Select **Modify**.

6. Enter an integer value of **0** or **20** for **dom.max_script_run_time**.
7. Click **OK** to confirm.
8. Restart the Mozilla Firefox browser.

Custom Graphing

This is a freestyle dashboard where multiple metrics can be selected and the real-time data for the selected metrics is shown in multi-line graph which is configured to refresh every 5 minutes and corresponding raw data will be shown in the data table.

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration > DCNM Server > Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

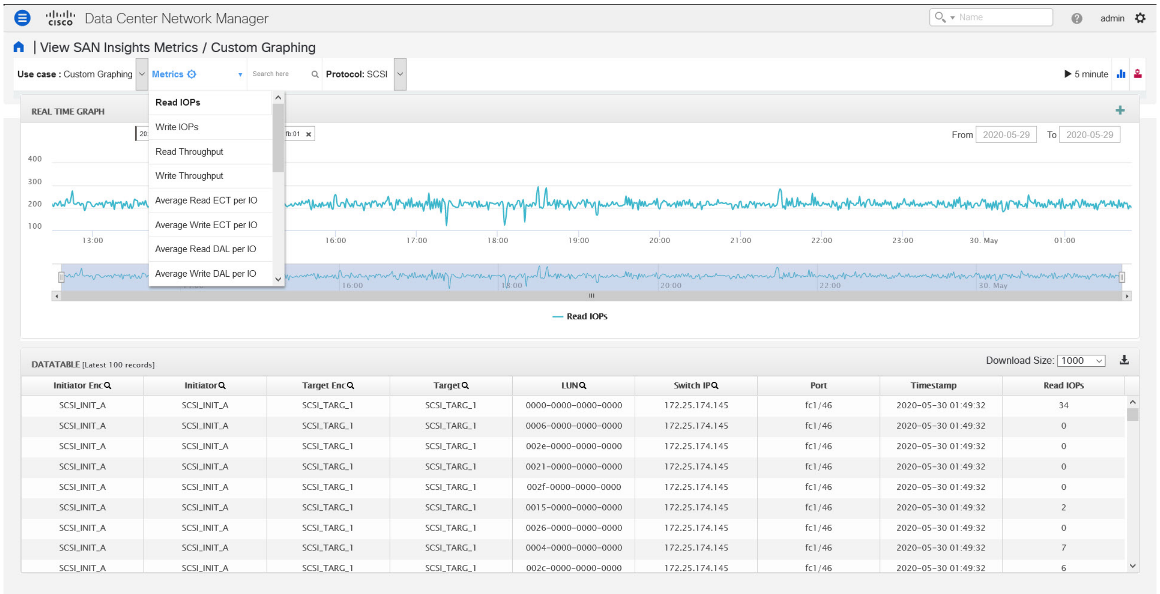
Note The Auto Refresh option is disabled by default. You must click on the pause icon to enable the Auto Refresh feature.

There are two components in the custom graphing use case.

- Real Time Graph
- Datatable

The Real Time Graph is plotted with corresponding metrics with from & to date selected. This component has the slider present below the graph as per your selection. It’s dynamic in nature as the data can be refreshed every 5 minutes, and can be converted into a static graph using the pause button.

Starting 11.4 release, Cisco DCNM allows the user to view data for more than two weeks’ time frame (up to a default maximum of 90 days. You can configure this time frame in the server properties. Select the date in the past using the To: date selector and view up to two weeks historical data from the date selected.



Use case : Custom Graphing

Protocol: SCSI

From 2020-05-29 To 2020-05-29

DATATABLE [Latest 100 records]

Download Size: 1000

Initiator Enc	Initiator	Target Enc	Target	LUN	Switch IP	Port	Timestamp	Read IOPs
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0000-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	34
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0006-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	0
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002e-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	0
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0021-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	0
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002f-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	0
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0015-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	2
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0026-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	0
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0004-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	7
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002c-0000-0000-0000	172.25.174.145	fc1/46	2020-05-30 01:49:32	6

In Release 11.4(1), the Custom Graphing metrics is enhanced to include the Write IO Failures, Read IO Failures, Write IO Aborts and Read IO Aborts to the drop-down metrics list.

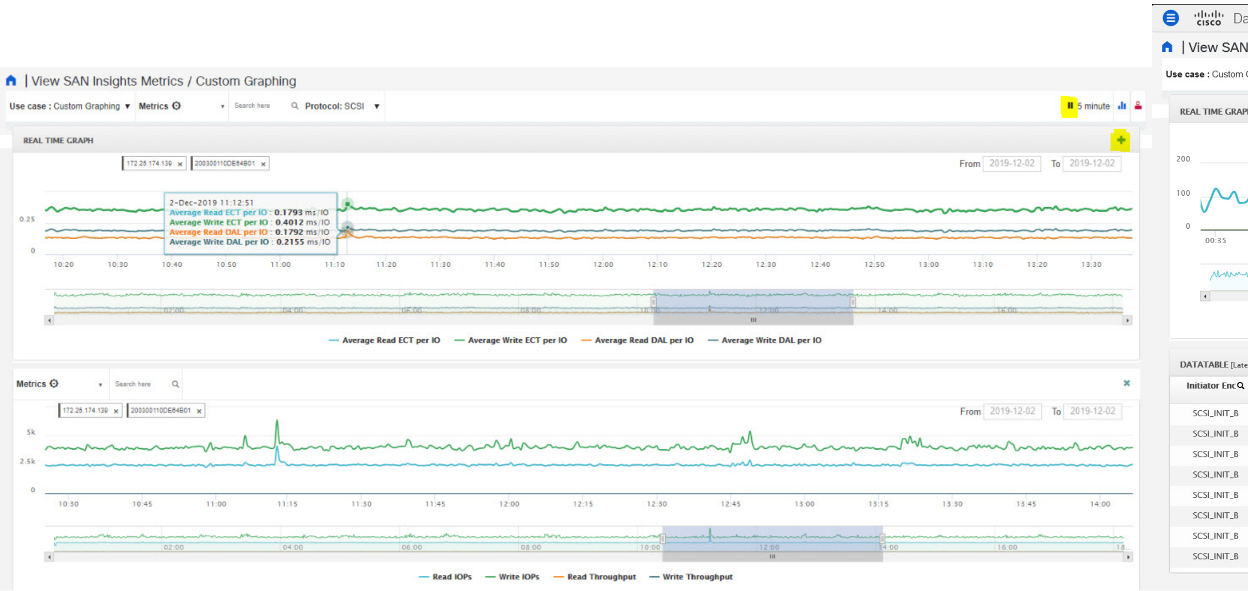
When you select a failure or abort metric from the drop-down list, the table list is filtered to show only the rows that have at least one of the selected failure or abort metrics as a nonzero entry. The table displays only 100 records. However, to help find their nonzero failures you can filter the table to show the last 100 records with an Abort or Failure that is nonzero. When you select failure or aborts, the table label changes to depict this behavior.

To view, input any of the seven dimensions (Initiator WWN, LUN/NSID, Target WWN, Source enclosure, Target enclosure, Switch IP, Device Alias) in the search tab, and select an associated metric.

Click on the download icon at the right corner to download the datatable information to your local database, for further analysis.

Note We recommend that you use Google Chrome browser to download the datatable information to your local database.

You can also add multiple graphs for comparison by clicking on the "+" icon at the top right. The data table is replaced by multiple Real Time graphs in this view and you can select the corresponding metric to be plotted by using the multiselect text search feature.

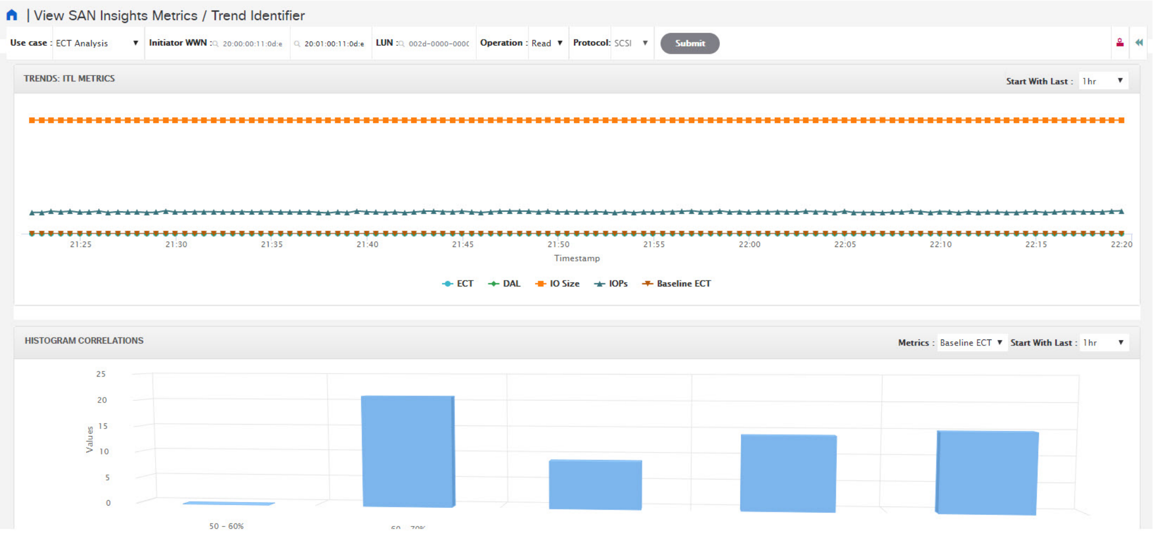


Trend Identifier

Click the Trend Identifier (📊) icon in the top-right corner to navigate to Trend Identifier.

You can also click on the Trend (〰) icon in each row of the data table to navigate to Trend Identifier, with prepopulated ITL/ITN input fields. There are two components showing data corresponding to selected ITL. Trends ITL Metrics shows area chart of ECT, DAL, IOPs, and Baseline ECT in the selected time interval (1 hour selected). Histogram Correlation tab shows the histogram of count of correlated ITLs with current ITL binned by correlation value. Clicking on any bar in this tab converts the histogram into datatable which shows the data corresponding to the selected bar.

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)



| View SAN Insights Metrics / Trend Identifier

Use case : ECT Analysis ▼ Initiator WWN : 20:00:00:11:0d:e 20:01:00:11:0d:e LUN : 002d-0000-000(Operation : Read ▼ Protocol: SCSI ▼ Submit

TRENDS: ITL METRICS — Start With Last : 1hr ▼

HISTOGRAM CORRELATIONS — Metrics : Baseline ECT ▼ Start With Last : 1hr ▼

Note

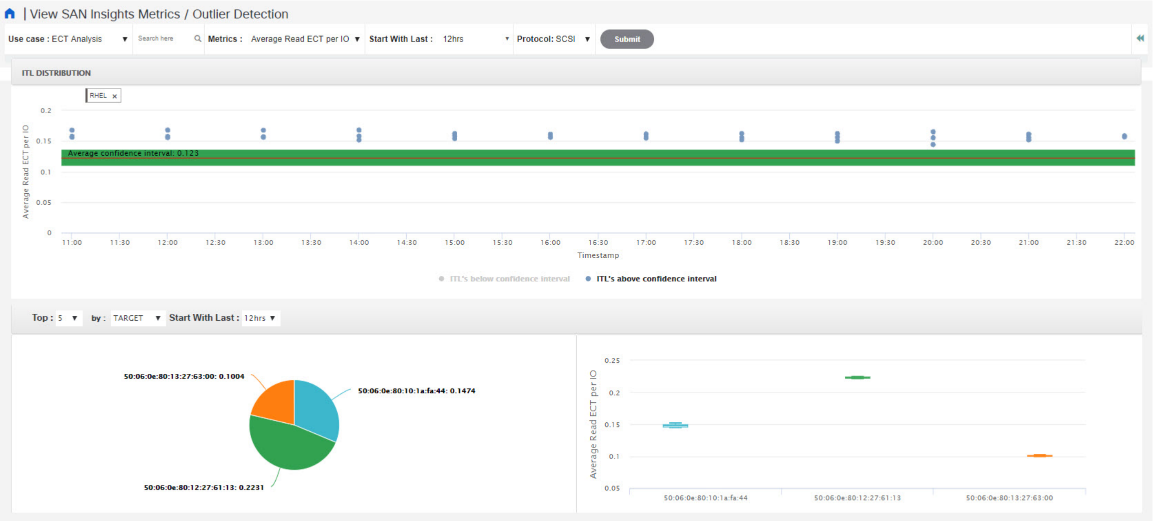
The default interval for the trend identifier is 30 minutes. You can specify the interval using the **Start With Last** drop-down list.

Outlier Detection

Click the Outlier Detection icon (🔒) that appears in the top-right corner of the page, to view the **Outlier Detection** metrics. To view data on this page, enter either Host-Enclosure or Initiator Enclosure name in the Search here input box, select a Metric, select a time range, and click **Submit**. This screen takes aggregated data for every 60 minutes.

ITL/ITN Distribution tab shows the scatter plot of metrics selected for all ITL/ITN's present in the selected time interval (1week in this case). To navigate to the Trend screen, click any of the dots (corresponds to specific ITL/ITN) in the scatter plot. Functionality added two tabs namely ITL/ITN's Below Confidence interval and ITL/ITN's above confidence interval. These two tabs are data calculated based on the Average Confidence Interval line.

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)



View SAN Insights Metrics / Outlier Detection

Use case : ECT Analysis | Search here | Metrics : Average Read ECT per IO | Start With Last : 12hrs | Protocol: SCSI | Submit

ITL DISTRIBUTION

Top : 5 | by : TARGET | Start With Last : 12hrs

You can zoom in to view the respective ITL/ITN dots at a more granular level by dragging the mouse and selecting a specific region to be viewed. Click on **Reset Zoom** in the zoomed screen to restore default zoom settings.

This use case consists of Multiselect text search feature, where you can search for specific text maximum up to two search criteria that can be present in any field (Initiator/Target Enclosure) and corresponding data is plotted in both the components.

Average Confidence Interval shows a band with an average line where most of the metric value lies in the selected time interval. Remaining two tabs shows Box Plot and Pie chart distribution of Top n (5 selected) Initiator/Target of the selected metric in the selected time interval.

Hosts

Note During Release 11.3(1) and earlier releases, this feature was called **Compute Dashboard**. Beginning from Release 11.4(1), it is renamed as **Hosts**.

The Hosts dashboard provides you with all the information that are related to the discovered SAN and LAN hosts. It provides detailed information that is related to the network, such as I/O traffic, disk latency, CPU, memory statistics, topology, and events about each individual host and virtual machines that are configured on top of the virtual host. The **Hosts** dashboard consists of four panels:

- **Host Enclosures** panel—Lists the hosts and their network attributes.
- **Traffic** panel—Provides the I/O statistics, CPU and memory information, and disk latency of individual hosts or virtual machines.
- **Topology** panel—Provides an end-to-end topology layout and path information between host enclosures and storage enclosures. The discovered virtual machines are displayed and when you select the virtual machine, the path to the SAN data source is displayed. You can toggle this view to list all data paths.
- **Event** panel—Provides information about events of all the switch ports that are configured within a specific host enclosure.

This section contains the following topics:

Viewing Host Enclosures

Beginning with Cisco NX-OS Release 6.x, you can view and search the network servers that are connected to the Cisco NX-OS devices. Cisco DCNM extends the fabric visibility up to the server and allows you to discover and search the end devices that are attached to the network.

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

Field	Description
Name	Displays the hostname.
IP Address	Displays the IP address of the switch.
#Macs	Displays the number of MAC addresses.
Mac Address(es)	Displays the MAC addresses.
#WWNs	Displays the number of World Wide Names (WWNs).
Port WWN(s)	Displays the port WWN.
FCID(s)	Specifies the associated FCID.
OS	Displays the OS details.
#VMs	Displays the number of VMs.
VHost Name	Displays the name of the virtual host.
VCluster	Displays the name of the virtual cluster.
Multipath	Displays the multipath details.
Protocol	Specifies if the Host is streaming SCSI protocol traffic or NVMe protocol traffic. This column displays data only for the Hosts for which data is streamed to the DCNM using SAN Insights.

Note

- Beginning with Cisco NX-OS Release 6.x, Server Credentials, Servers, and Static Server-Adapter Mapping are no longer available.
- Beginning from Cisco DCNM Release 10.1, you are able to assign storage to hosts.
- Collection level in the vCenter settings determines the amount of data that is gathered and displayed in charts. Level 1 is the default Collection Level for all collection intervals. Change the vCenter statistics settings to Level 2 or higher to collect disk I/O history data.
- From DCNM Release 11.4(1), you can set the default enclosure names from the Device Alias. Choose **Administration > DCNM Server > Server Properties**, and edit the **fabric.aliasRE** property.

To view the host enclosures from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard > Hosts**.

The list of hosts in the host enclosures table is displayed.

Step 2 Choose a host to view more details.

The events, topology, and traffic information on the dashboard are displayed. You can also click the corresponding icons on a host entry to view the events, topology, and traffic information.

From DCNM Release 11.5(1), traffic icons are added for VHost. It has multiple VM charts such as VHost CPU, and memory, latency, and network I/O. Click the radio button of a host to view respective traffic details in the traffic dashboard.

Step 3 To edit the hostname, select the row and click the **Rename** icon. Enter the new name in the pop-out dialog.

- If the host is not associated with port WWN or the end port is not discovered by DCNM, it is a VHost or LAN Host. The **Rename Enclosure** dialog box appears only for the existing name.
- If the host is associated with port WWN and the end port is discovered by DCNM. The **Rename Enclosure** dialog appears for the associated host names.
  - You can rename each enclosure name to a different name. Choose the enclosure name, enter a new name, click Save. Repeat this procedure to change all the required enclosure names and click **Apply**.
  - You can rename all enclosure names to the same new name. Check the **Include All Members** check box, enter a new name, and click **Apply**.

Note Specifying a blank name causes the server to default the name.

Cisco DCNM allows you to change the default assigned Host enclosure name or grouping multiple enclosures into the same enclosure by assigning the same name. Assigning custom enclosure names to respective WWPNs is supported on the Cisco DCNM SAN Client only.

Step 4 To assign storage to host, you can choose the host, and click the **Assign** icon next to the Rename icon.

The **Assign Storage to Host** window pops out. The selection of Host is by enclosure, and multiple selections of LUNs is allowed. Click **Assign**. A confirmation message is displayed. After confirmed, the status will update with the results of each step.

Step 5 Click **Quick Filter** drop down to filter **host** enclosures (not storage) by **LAN, SAN**, and **Virtual**.

Viewing Host Events

To view the host events from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard** > **Hosts**.

The list of hosts in the host enclosures table is displayed.

Step 2 Click the **Events** icon next to the host enclosure to view the Events panel.

You can use the slider control to resize the panel.

Viewing Host Topology

To view host topology from the Cisco DCNM Web UI, perform the following steps:

Procedure

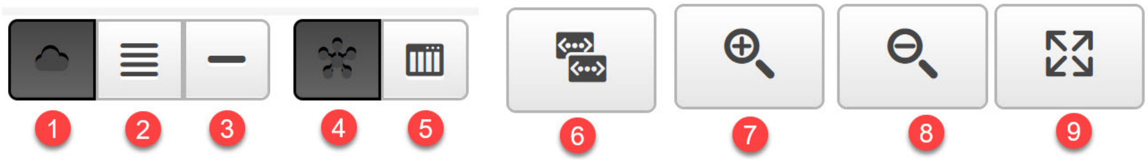
Step 1 Choose **Dashboard** > **Hosts**.

The list of hosts in the host enclosures table is displayed.

Step 2 Select the row to view the host topology details.

You can use the mouse scroll wheel to zoom-in and zoom-out.

Step 3 Click the **Fabric/Network** icon to view the fabric and network path.



1 - Fabric/Network

2 - All Paths

3 - First Shortest Path

6 - Custom Port Group

7 - Zoom In

8 - Zoom Out

4 - Map View	9 - Zoom Fit
5 - Tabular View	

Step 4 Click the **All Paths** icon to view the complete set-up.

Step 5 Click the **First Shortest Path** icon to view the first shortest path.

Note Click **Map View** icon to enable the icons that are listed in the preceding step 4, 5 and 6.

Step 6 Click the **Tabular View** icon to view the host topology in tabular format.

Step 7 Click the **Custom Port Group** icon to view the custom port group.

View Host Traffic

To view the host traffic from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 From the menu bar, choose **Dashboard** > **Hosts**.

The list of hosts in the host enclosures table is displayed.

Step 2 Select the row to view the host topology details.

Step 3 Use the drop-down to select the traffic according to the time duration.

Step 4 Select the icons to view the traffic as a **Grid, Line Chart**, or **Stacked Chart**.

Step 5 In the **Traffic** pane, the **Enclosure Traffic** is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.

CHAPTER 3

Topology

Topology

The Topology window displays color-encoded nodes and links that correspond to various network elements, including switches, links, fabric extenders, port-channel configurations, virtual port-channels, and more. For information about each of these elements, hover your cursor over the corresponding element. Also, click a node or the line for a link. A slide-in pane appears from the right side of the window. This pane displays detailed information about either the switch or the link.

Note You can open multiple tabs simultaneously and can function side by side to facilitate comparison and troubleshooting.

Status

The color coding of each node and link corresponds to its state. The colors and what they indicate are described in the following list:

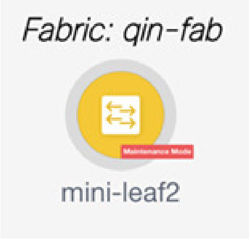
- Green: Indicates that the element is in good health and functioning as intended.
- Yellow: Indicates that the element is in warning state and requires attention to prevent any further problems.
- Red: Indicates that the element is in critical state and requires immediate attention.
- Gray: Indicates lack of information to identify the element or the element has been discovered.

Note

- In the **Topology** window, FEX appears in gray (**Unknown** or **n/a**) because health is not calculated for FEX.
- After moving a cable from one port to another port, the old fabric link is retained in the **Topology** window, and it is shown in the red color indicating that the link is down. The port movements are not updated in the **Topology** window. You need to rediscover the switch for the updated ports to be displayed in DCNM.

- Black: Indicates that the element is down.

Starting from Cisco DCNM Release 11.4(1), if a switch is in maintenance mode, a **Maintenance Mode** badge is displayed next to the switch. If a switch is in migration mode, a **Migration Mode** badge is displayed next to the switch.



Scope

You can search the topology based on the scope. The default scopes available from the **SCOPE** drop-down list is: **DEFAULT_LAN** and **DEFAULT_SAN**. The search options differ based on the chosen scope.

The following search options are available for **DEFAULT_LAN**:

- Quick Search
- VLAN

The following search options are available for **DEFAULT_SAN**:

- Quick Search
- VLAN
- VSAN ID/Name

Searching

When the number of nodes is large, it quickly becomes difficult to locate the intended switches and links. You can quickly find switches and links by performing a search. You are also able to search for VM tracker and generic setups. Searching feature enables you to see which leaf the host is connected to.

The following searches are available:

Note By default, Quick Search is selected.

Quick Search

Quick Search enables you to search for devices by name, IP address, model, serial number, and switch role. As you enter a search parameter in the **Search** field, the corresponding switches are highlighted in the topology. To perform a search for multiple nodes and links, separate multiple keywords using a comma, for example, ABCD12345, N7K, sw-dc4-12345, core, 172.23.45.67. Cisco DCNM supports wildcard searches too. If you know a serial number or switch name partially, you can build a search based on these partial terms that are preceded by an asterisk, for example, ABCD*, sw*12345, core, and so on.

To limit the scope of your search to a parameter, enter the parameter name followed by a space and the parameter in the Search field, for example, name=sw*12345, serialNumber=ABCD12345, and so on.

VLAN

Search by a given VLAN ID. VLAN search provides the search for the VLAN configured on the switch or the links. If STP is enabled, then it provides information that is related to the STP protocol and the STP information for links.

VSAN ID/Name

Search by a given VSAN ID. VSAN search provides the search for VSAN configured on the switch or the links. In order to view the STP details associated with the VSAN, click **STP Details** link.

This shows the STP details, if STP is enabled. If the link is blocked, it is marked as red, green in case of a forwarding link, and orange if the link is blocked for one VSAN range and forwarding for the other VSAN range.

This search is applicable to both the default LAN and SAN scopes.

Show Panel

You can choose to view your topology based on the following options:

- **Auto Refresh**: Check this check box to automatically refresh the topology.
- **Switch Health**: Check this check box to view the switch's health status.
- **FEX**: Check this check box to view the Fabric Extender.

Note The FEX feature is available only on LAN devices. Therefore, checking this check box displays only the Cisco Nexus switches that support FEX.

Note 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. Therefore, such devices will not be displayed in the topology when you check the **FEX** check box.

- **Links**: Check this check box to view links in the topology. The following options are available:
  - **Errors Only**: Click this radio button to view only links with errors.
  - **All**: Click this radio button to view all the links in the topology.
  - **VPC Only**: Check this check box to view only vPC peer-links and vPCs.
  - **Bandwidth**: Check this check box to view the color coding based on the bandwidth that is consumed by the links.
- **UI controls**: Check the check box to show or hide the various controls on the **Topology** window.
- **Refresh**: You can also perform a topology refresh by clicking the **Refresh** icon in the upper-right corner of this panel.

Layouts

The topology supports different layouts along with a **Save Layout** option that remembers how you positioned your topology.

- **Hierarchical** and **Hierarchical Left-Right**: Provide an architectural view of your topology. Various switch roles can be defined that will draw the nodes on how you configure your CLOS topology.

Note When running a large-scale setup, being able to easily view all your switches on a leaf-tier can become difficult. To mitigate this, DCNM splits your leaf-tier every 16 switches.

- **Random**: Nodes are placed randomly on the window. DCNM tries to make a guess and intelligently place nodes that belong together in close proximity.
- **Circular** and **Tiered-Circular**: Draw nodes in a circular or concentric circular pattern.
- **Custom saved layout**: Nodes can be dragged around according to your preference. After you position as required, click **Save** to retain the positions. The next time you come to the topology, DCNM will draw the nodes based on your last saved layout positions.

Before a layout is chosen, DCNM checks if a custom layout is applied. If a custom layout is applied, DCNM uses it. If a custom layout is not applied, DCNM checks if switches exist at different tiers, and chooses the Hierarchical layout or the Hierarchical Left-Right layout. Force-directed layout is chosen if all the other layouts fail.

Zooming, Panning, and Dragging

You can zoom in and zoom out using the controls that are provided at the bottom left of the windows or by using your mouse's wheel.

To pan, click and hold anywhere in the whitespace and drag the cursor up, down, left, or right.

To drag switches, click, hold, and move the cursor around the whitespace region of the topology.

Switch Slide-Out Panel

You can click on the switch to display the configured switch name, IP address, switch model, and other summary information such as status, serial number, health, last-polled CPU utilization, and last-polled memory utilization.

From DCNM release 11.5(1), switches have only two roles, Core Router and Edge Router.

Beacon

This button will be shown for switches that support the **beacon** command. After beaconing starts, the button will show a countdown. By default, the beaconing will stop after 60 seconds, but you can stop it immediately by clicking **Stop Beacon**.

Note The default time can be configured in `server.properties` file. Search for **beacon.turnOff.time**. The time value is in milliseconds. Note that this requires a server restart to take effect.

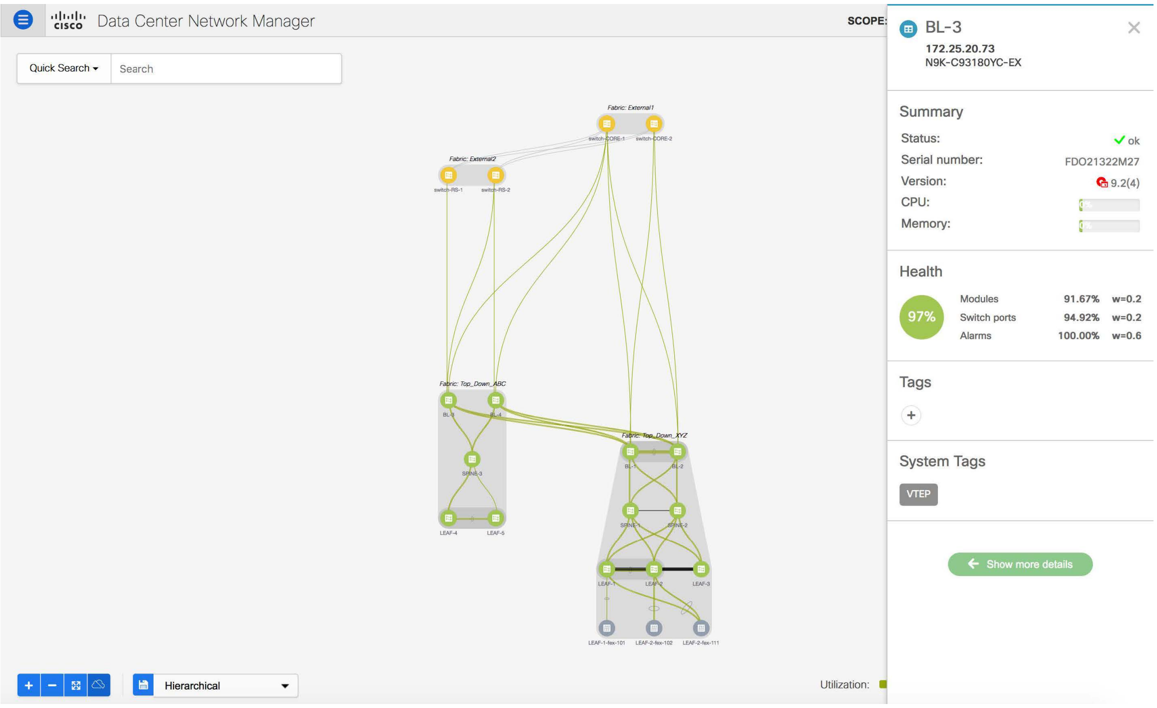
Tagging

Tagging is a powerful yet easy way to organize your switches. Tags can be virtually any string, for example, *building 6*, *floor 2*, *rack 7*, *problem switch*, and *Justin debugging*.

Use the search functionality to perform searches based on tags.

More Details

Click **Show more details** to display more information under the following tabs: **System Info, Modules, FEX, License, Features, VXLAN, VLAN, Capacity** and **Hosts**.



BL-3
172.25.20.73
N9K-C93180YC-EX

Summary

Status:	✓ ok
Serial number:	FDO21322M27
Version:	9.2(4)
CPU:	
Memory:	

Health

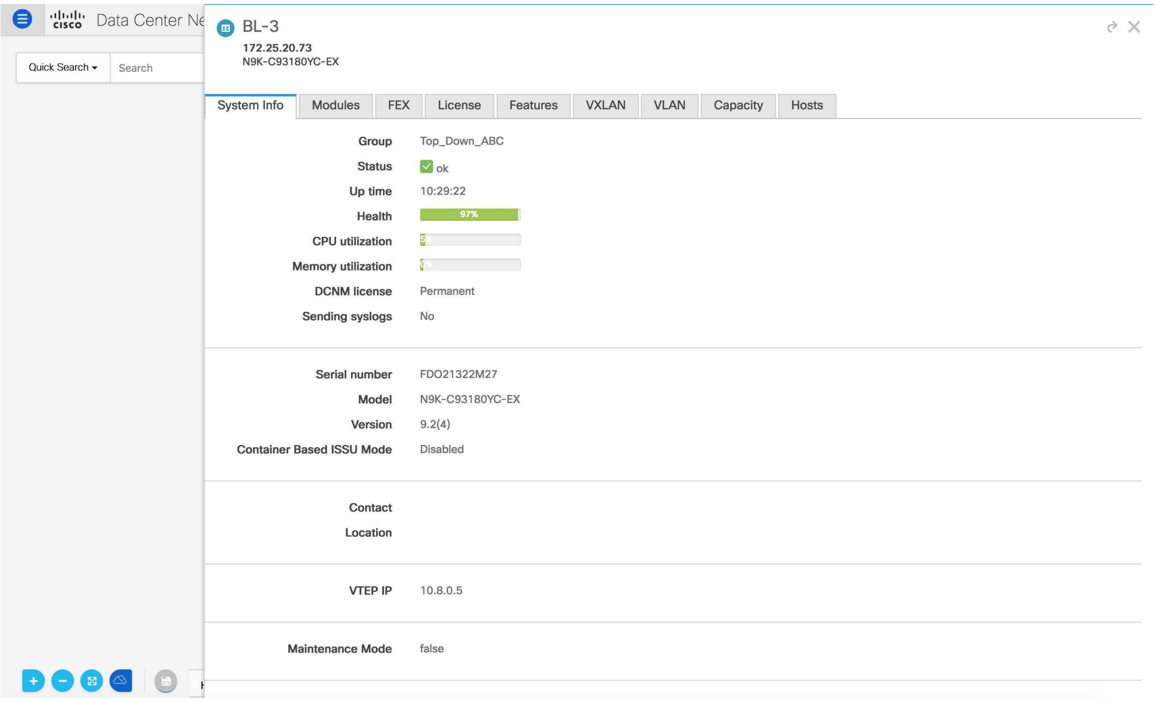
97%

Modules	91.67%	w=0.2
Switch ports	94.92%	w=0.2
Alarms	100.00%	w=0.6

Tags

System Tags

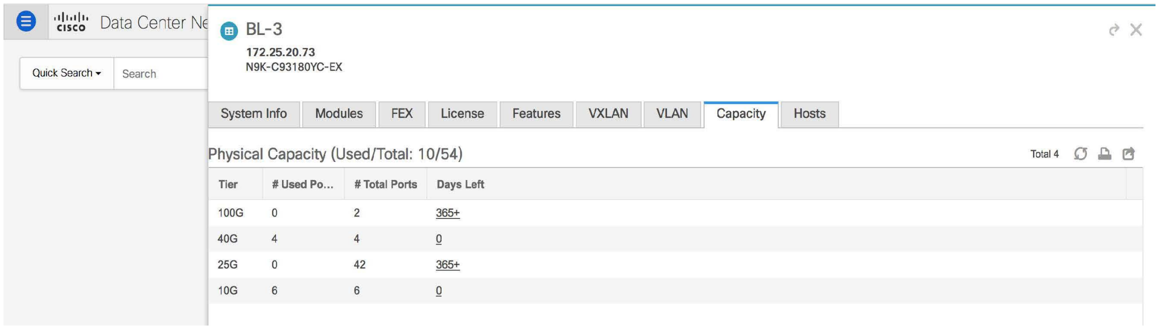
VTEP



BL-3
172.25.20.73
N9K-C93180YC-EX

Group	Top_Down_ABC
Status	☑ ok
Up time	10:29:22
Health	97%
CPU utilization	
Memory utilization	
DCNM license	Permanent
Sending syslogs	No
Serial number	FDO21322M27
Model	N9K-C93180YC-EX
Version	9.2(4)
Container Based ISSU Mode	Disabled
Contact	
Location	
VTEP IP	10.8.0.5
Maintenance Mode	false

Starting from Cisco DCNM Release 11.4(1), the 400G tier has also been added to the **Physical Capacity** table under the **Capacity** tab. However, the **Physical Capacity** table under the **Capacity** tab will only show information about the physical ports that are present on the switch. For example, if the switch does not have a 400G physical port, the 400G tier is not displayed in the **Physical Capacity** table.



Physical Capacity (Used/Total: 10/54)

Tier	# Used Po...	# Total Ports	Days Left
100G	0	2	365+
40G	4	4	0
25G	0	42	365+
10G	6	6	0

Link Slide-Out Panel

You can click a link to view the status and the port or switches that describe the link.

24-Hour Traffic

This feature requires **Performance Monitoring** to be turned **ON**. When **Performance Monitoring** is **ON**, traffic information is collected and the aggregate information is displayed along with a graph showing traffic utilization.

CHAPTER 4

Inventory

This chapter contains the following topics:

Viewing Inventory Information

Beginning with Cisco 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.

- **Mode** column displays the current mode of the switch. The switch can be in **Normal**, **Maintenance**, or **Migration** mode.
- **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.
- **Up Time** column displays the time period for which the switch is active.
- **Container Based ISSU Mode** column indicates whether the Container Based ISSU Mode is enabled or not. The container-based ISSU can be enabled for Cisco Nexus 3000 and Cisco Nexus 9000 series switches. This is a one-time configuration on the device.

  Enhanced in-service software upgrade (ISSU)—Enables you to upgrade the device software while the switch continues to forward traffic, which reduces the downtime typically caused by software upgrades (similar to the regular ISSU, also known as a non-disruptive upgrade). However, with container-based ISSU, the software runs inside a separate Linux container (LXC) for the supervisor and line cards, and a third container is created as part of the ISSU procedure and is brought up as a standby supervisor.

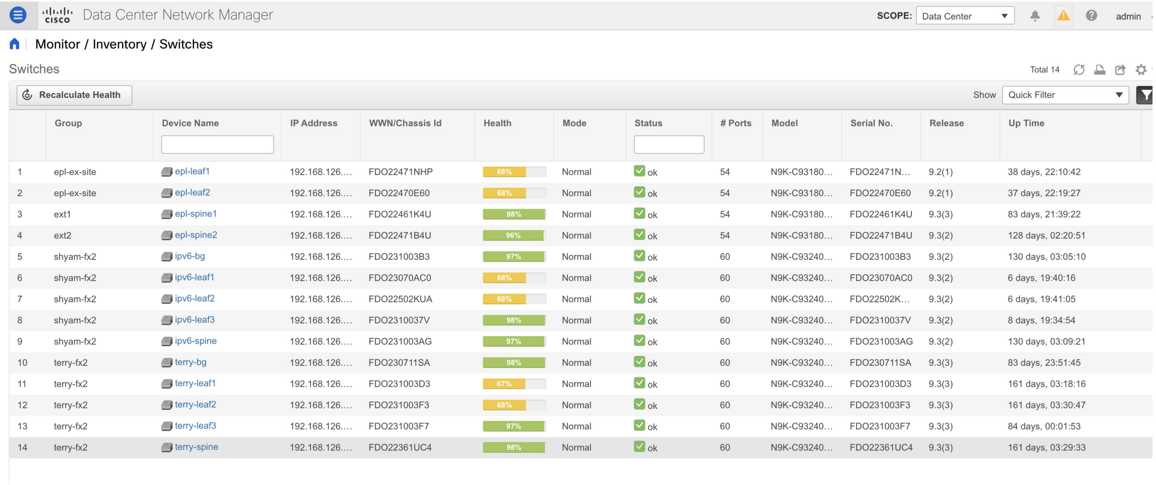
  Container-based ISSUs are supported on Cisco Nexus 3164Q, 9200 series switches, 9332PQ, 9372PX, 9372TX, 9396PX, 9396TX, 93120TX, and 93128TX switches.

  For more information about the Cisco Nexus 3000 and 9000 switches, where the Container-based ISSU feature is supported, see the following URLs:

  Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.x

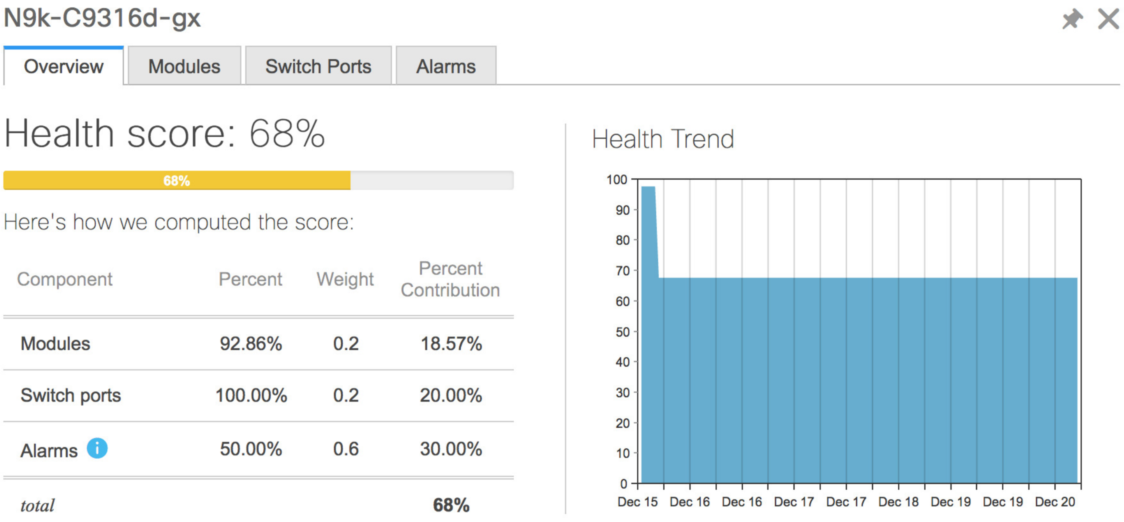
  Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 9.x

  Cisco NX-OS ISSU Support Matrix



	Group	Device Name	IP Address	WWN/Chassis Id	Health	Mode	Status	# Ports	Model	Serial No.	Release	Up Time
1	epl-ex-site	epl-leaf1	192.168.126....	FDO22471NHP	68%	Normal	✓ ok	54	N9K-C93180...	FDO22471N...	9.2(1)	38 days, 22:10:42
2	epl-ex-site	epl-leaf2	192.168.126....	FDO22470E60	68%	Normal	✓ ok	54	N9K-C93180...	FDO22470E60	9.2(1)	37 days, 22:19:27
3	ext1	epl-spine1	192.168.126....	FDO22461K4U	98%	Normal	✓ ok	54	N9K-C93180...	FDO22461K4U	9.3(3)	83 days, 21:39:22
4	ext2	epl-spine2	192.168.126....	FDO22471B4U	96%	Normal	✓ ok	54	N9K-C93180...	FDO22471B4U	9.3(2)	128 days, 02:20:51
5	shyam-fx2	ipv6-bg	192.168.126....	FDO231003B3	97%	Normal	✓ ok	60	N9K-C93240...	FDO231003B3	9.3(2)	130 days, 03:05:10
6	shyam-fx2	ipv6-leaf1	192.168.126....	FDO23070AC0	68%	Normal	✓ ok	60	N9K-C93240...	FDO23070AC0	9.3(2)	6 days, 19:40:16
7	shyam-fx2	ipv6-leaf2	192.168.126....	FDO22502KUA	68%	Normal	✓ ok	60	N9K-C93240...	FDO22502K...	9.3(2)	6 days, 19:41:05
8	shyam-fx2	ipv6-leaf3	192.168.126....	FDO2310037V	98%	Normal	✓ ok	60	N9K-C93240...	FDO2310037V	9.3(2)	8 days, 19:34:54
9	shyam-fx2	ipv6-spine	192.168.126....	FDO231003AG	97%	Normal	✓ ok	60	N9K-C93240...	FDO231003AG	9.3(2)	130 days, 03:09:21
10	terry-fx2	terry-bg	192.168.126....	FDO230711SA	98%	Normal	✓ ok	60	N9K-C93240...	FDO230711SA	9.3(3)	83 days, 23:51:45
11	terry-fx2	terry-leaf1	192.168.126....	FDO231003D3	67%	Normal	✓ ok	60	N9K-C93240...	FDO231003D3	9.3(3)	161 days, 03:18:16
12	terry-fx2	terry-leaf2	192.168.126....	FDO231003F3	68%	Normal	✓ ok	60	N9K-C93240...	FDO231003F3	9.3(3)	161 days, 03:30:47
13	terry-fx2	terry-leaf3	192.168.126....	FDO231003F7	97%	Normal	✓ ok	60	N9K-C93240...	FDO231003F7	9.3(3)	84 days, 00:01:53
14	terry-fx2	terry-spine	192.168.126....	FDO22361UC4	98%	Normal	✓ ok	60	N9K-C93240...	FDO22361UC4	9.3(3)	161 days, 03:29:33

Step 3 Click **Health** to access the Health score window for a device. The Health score window includes health score calculation and health trend. The Overview tab displays the overall health score. All the modules, switch ports and alarms are taken into consideration while calculating the health score. Hover over the graph under Health Trend for detailed information on specific dates. Hover over the info icon next to Alarms to display the number of Critical, Major, Minor, and Warning alarms that have been generated.

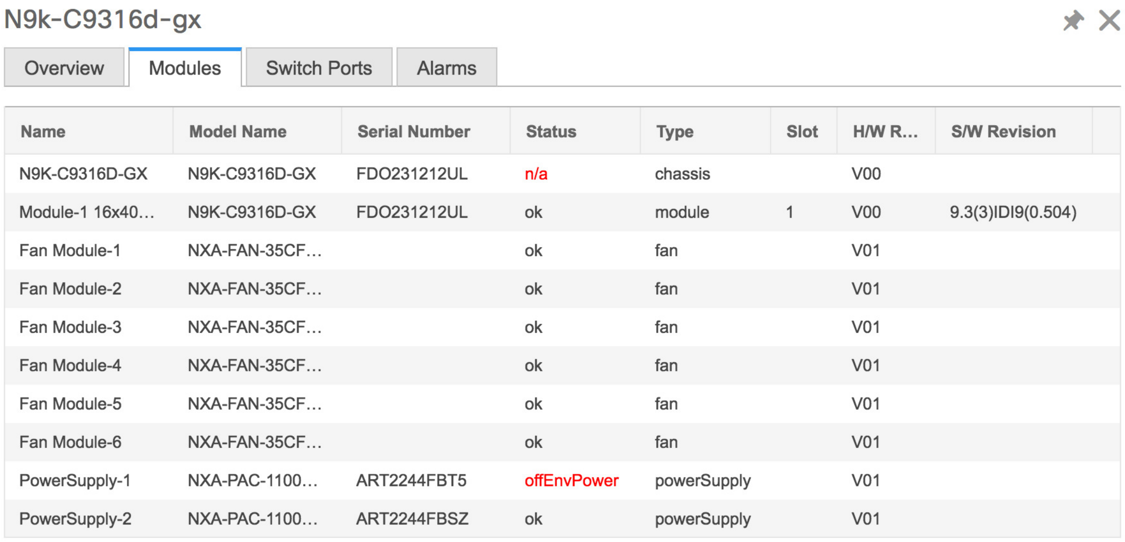


Health score: 68%

Here's how we computed the score:

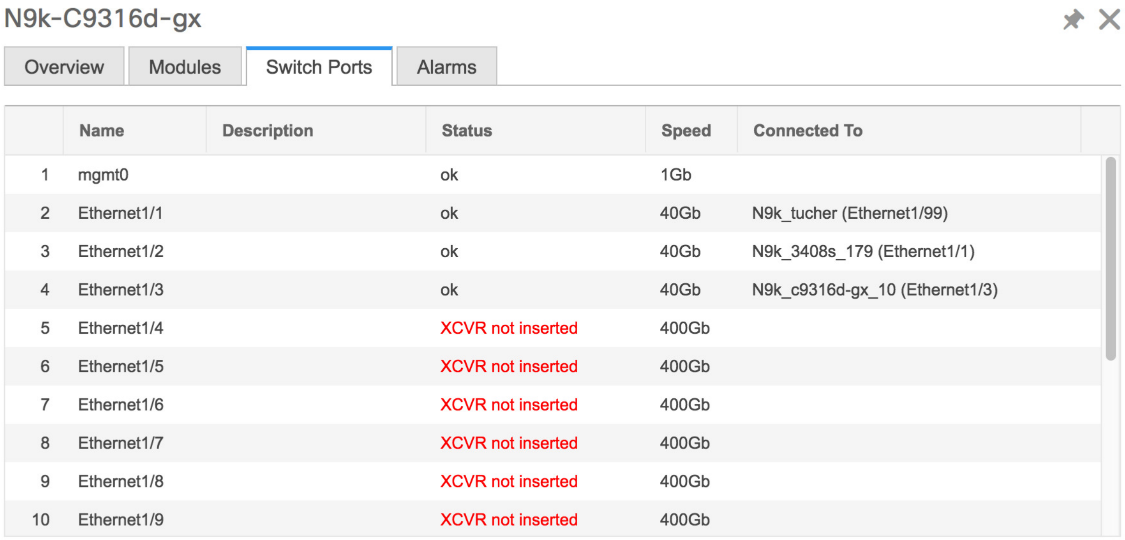
Component	Percent	Weight	Percent Contribution
Modules	92.86%	0.2	18.57%
Switch ports	100.00%	0.2	20.00%
Alarms ⓘ	50.00%	0.6	30.00%
total			68%

Click the **Modules** tab to display information about the various modules in the device. This tab displays information such as Name, Model name, Serial number, Status, Type, Slot, Hardware revision and Software revision.



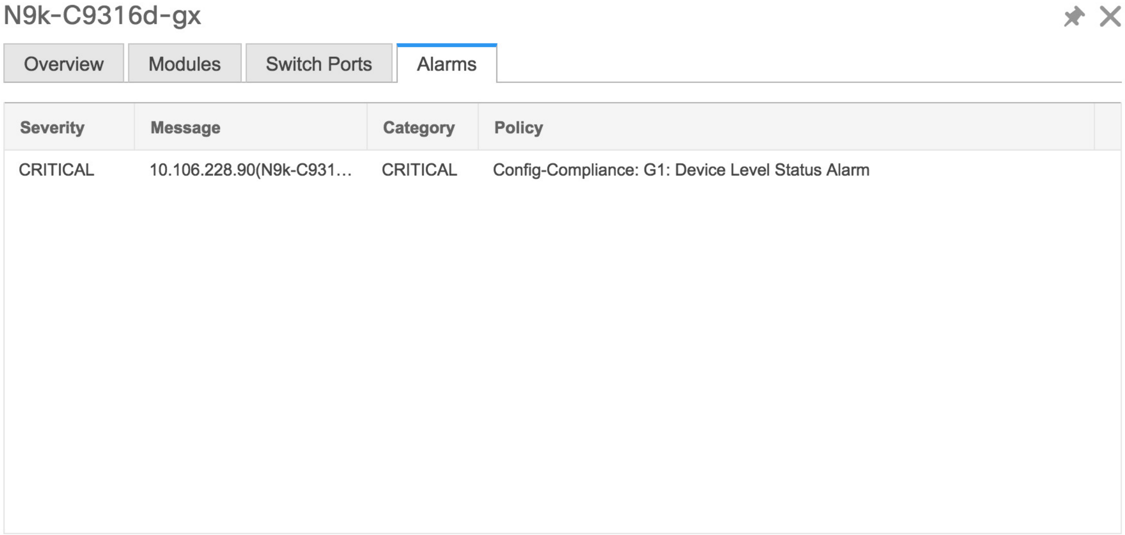
Name	Model Name	Serial Number	Status	Type	Slot	H/W R...	S/W Revision
N9K-C9316D-GX	N9K-C9316D-GX	FDO231212UL	n/a	chassis		V00	
Module-1 16x40...	N9K-C9316D-GX	FDO231212UL	ok	module	1	V00	9.3(3)IDI9(0.504)
Fan Module-1	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-2	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-3	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-4	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-5	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-6	NXA-FAN-35CF...		ok	fan		V01	
PowerSupply-1	NXA-PAC-1100...	ART2244FBT5	offEnvPower	powerSupply		V01	
PowerSupply-2	NXA-PAC-1100...	ART2244FBSZ	ok	powerSupply		V01	

Click the **Switch Ports** tab to display information about the device ports. This tab displays information such as Name, Description, Status, Speed, and the device to which a port is connected .



	Name	Description	Status	Speed	Connected To
1	mgmt0		ok	1Gb	
2	Ethernet1/1		ok	40Gb	N9k_tucher (Ethernet1/99)
3	Ethernet1/2		ok	40Gb	N9k_3408s_179 (Ethernet1/1)
4	Ethernet1/3		ok	40Gb	N9k_c9316d-gx_10 (Ethernet1/3)
5	Ethernet1/4		XCVR not inserted	400Gb	
6	Ethernet1/5		XCVR not inserted	400Gb	
7	Ethernet1/6		XCVR not inserted	400Gb	
8	Ethernet1/7		XCVR not inserted	400Gb	
9	Ethernet1/8		XCVR not inserted	400Gb	
10	Ethernet1/9		XCVR not inserted	400Gb	

Click the **Alarms** tab to display information about the alarms that have been generated. This tab displays information such as alarm Severity, Message, Category, and the Policy that has been activated due to which the alarm is generated.



Severity	Message	Category	Policy
CRITICAL	10.106.228.90(N9k-C931...	CRITICAL	Config-Compliance: G1: Device Level Status Alarm

In the **Health** column, the switch health is calculated by the capacity manager based on the following parameters:

- Total number of modules
- Total number of modules impacted by the warning
- Total number of switch ports
- Total number of switch ports impacted by the warning
- Total number of critical severity alarms
- Total number of warning severity alarms
- Total number of major severity alarms
- Total number of minor severity alarms

Step 4 The value in the **Health** column is calculated based on the following:

- Percentage of modules impacted by warnings (Contributes 20% of the total health).
- Percentage of ports impacted by warnings (Contributes 20% of the total health).
- Percentage of alarms (Contributes 60% of the total health). The critical alarms contribute the highest value to this percentage followed by major alarms, minor alarms and warning alarms.

You may also have your own health calculation formula by implementing the common interface class: com.cisco.dcbu.sm.common.rif.HealthCalculatorRif.

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

- 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

Starting from Cisco DCNM 11.3(1) Release, you can view information about switch health along with the switch summary by clicking on a switch in the **Topology** window or by choosing **Control>Fabrics>Fabric Builder**, selecting a fabric and clicking on a switch in the **Fabric Builder** window.

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, on page 315 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.
- Click **Generate tac-pac** to collect technical support from a device in Cisco DCNM. See the *Collecting Technical Support from Devices* section for more information.

Collecting Technical Support from Devices

You can choose the protocol while generating technical support from a device in Cisco DCNM Web Client. To collect technical support from a device in Cisco DCNM Web UI, perform the following steps:

Procedure

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

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

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

The switch dashboard that corresponds to that switch appears.

Step 3 In the **Actions** area, click **Generate tac-pac**.

The **Generate tac-pac** dialog box appears.

Step 4 Choose a management interface by clicking the appropriate radio button.

Valid values are **default**, **vrf management**, and **vrf default**. The default value selected is **default**.

Note This option is valid only for Nexus switches.

Step 5 Choose the transport protocol from switch to DCNM by clicking the appropriate radio button.

Valid values are **TFTP**, **SCP**, and **SFTP**.

Note If you choose the **SCP** or **SFTP** option, enter the DCNM server credentials.

Step 6 Click **Ok**.

After the tac-pac is generated and saved on server, a dialog box appears to open or save the file on your local machine.

Viewing Device Manager Information

Note After you install Cisco DCNM for Windows, you must edit and provide credentials in the Cisco DCNM SAN Services to Log on. Navigate to **Services > Cisco DCNM SAN Server > Cisco DCNM SAN Server Properties** > **Log On** tab. Select This account radio button, and provide username and password. Click **Ok**. Log on to SSH and stop DCNM services. After you start the DCNM services, you must be able to use Device Manager.

Note After you install Cisco DCNM for Linux, perform the procedure that is provided on the screen for Device Manager to be functional. Device Manager requires graphical environment that is configured properly in the Linux/OVA DCNM server.

The switch dashboard displays the details of the selected switch.

Procedure

Step 1 From the left menu bar, choose **Inventory > View > Switches**.

An inventory of switches discovered by Cisco DCNM Web Client 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 **Device Manager** tab. The Device Manager login dialog box appears. Log into the Device Manager application. The Device Manager provides a graphic representation of the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

For more information about the Device Manager, go to the following URL:

Cisco DCNM SAN Client Online Help

Installing a Switch License

To install a switch license from the Cisco DCNM Web UI, perform the following steps:

Procedure

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

Alternatively, you can choose **Inventory** > **View** > **Switches**.

Step 2 Click **License** in the switch dashboard.

Step 3 Click **Install** to install the switch license file on a switch.

A **Switch License Install** window appears.

Step 4 Click **Select License File**, and select the license file from your local system.

Step 5 Select the transport method. The available options are:

- SCP
- SFTP

Step 6 Enter the username and password to connect to the DCNM server.

Step 7 Click **Install**.

Rediscovering Switch Licenses

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

Procedure

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

Alternatively, you can choose **Inventory** > **View** > **Switches**.

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

Step 3 Click the **License** tab in the switch dashboard.

Step 4 Click **Rediscover** to rediscover switch licenses on a switch.

Rediscovering the switch licenses takes some time.

Step 5 Click the **Last Updated** icon to refresh the licenses.

Interfaces

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 3: 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

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**. 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 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 4: 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 5: 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.
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 6: 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 delete the VDC. Select any active VDC radio button and click Delete to remove the VDC associated with the device.
Resume	Allows you to resume a suspended VDC.
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 7: 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.
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.

Field	Description
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 8: 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		

Resource	Minimum	Maximum
VLAN		
Anycast Bundled		
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 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.

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.
- **IO FPGA** column displays the IO field programmable gate arrays (FPGA) version.
- **MI FPGA** column displays the MI field programmable gate arrays (FPGA) version.

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 Managing Local 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.

For any switch to be successfully imported into DCNM, the user defined on the switch via local or remote AAA, and used for import into DCNM should have the following permissions:

- SSH access to the switch
- Ability to perform SNMPv3 queries
- Ability to run **show** commands

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, java is used as a part of the discovery process. If firewall blocks the process then it uses TCP connection port 7 as a discovery process. Ensure that the **cdp.discoverPingDisable** server property is set to **true**. Choose **Web UI > Administration > DCNM Server > Server Properties** to set the server property.

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.

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 server, which is down, to an active server. The management state remains the same.

Procedure

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

Step 2 Choose the LAN devices from the LAN table. Click **Move**.

Step 3 In the **Move LAN Tasks to another DCNM Server** dialog box, enter the LAN Device to be moved and specify the DCNM server.

All the LAN devices under the selected tasks will be moved.

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.

Adding, Editing, Re-Discovering, Purging and Removing the Managed Fabrics

Cisco DCNM reports information that is obtained by the Cisco DCNM-SAN on any fabric known to Cisco DCNM-SAN. To view the SAN Switches, choose **Inventory** > **Discovery** > **SAN Switches**.

The Status column of the SAN Switches page displays the fabric status.

- managedContinuously—The fabric is automatically managed when the Cisco DCNM-SAN server starts and continues to be managed until this option is changed to Unmanage.
- managed—The fabric is managed by Cisco DCNM-SAN Server until there are no instances of DCNM-SAN viewing the fabric.
- unmanaged—Cisco DCNM-SAN Server stops managing this fabric.

This section contains the following:

Adding a Fabric

Before you begin

Before you discover a new fabric, ensure that you create an SNMP user on the switch.

Procedure

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

The **SAN Switches** window is displayed with a list of fabrics, if any, managed by Cisco DCNM-SAN.

Step 2 Click **Add** to add a new fabric.

The **Add Fabric** window appears.

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

Step 4 (Optional) Check the **SNMP** check box to use SNMPv3 or SSH. If you check the SNMP check box, the field **Community** changes to **Username** and **Password**.

Step 5 Enter the **Username** 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** check box 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** and specify the **UCS Username** and **UCS Password**.

Step 10 Select a DCNM server from the **DCNM Server** drop-down list.

Note This option is applicable only for Federation setups.

Step 11 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 Choose **Inventory** > **Discovery** > **SAN Switches**.

Step 2 Select the check box next to the fabric that you want to remove.

Step 3 Click **Delete** to remove the fabric from the datasource and to discontinue data collection for that fabric.

Editing a Fabric

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

Procedure

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

Step 2 Select the check box next to the fabric that you want to edit and click 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 **Username** 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.

Step 8 To modify the password, go to from the Cisco DCNM Web UI, perform the following steps:

a) Choose **Inventory** > **Discovery** > **SAN Switches**.

b) Select the fabric for which the fabric switch password is changed.

c) 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 is not be validated with the database.

You can go to **Administration** > **Credentials Management** > **SAN Credentials** to validate 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 server, which is down, to an active server. The management state remains the same.

Procedure

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

Step 2 Select the fabric(s) that you want to move to a different server, and then click **Move**.

Step 3 In the **Move Fabric** dialog box, select the DCNM server where the fabrics will be moved.

The **To DCNM Server** drop-down list lists only the active servers.

Note The status of the Fabric will display **Unmanaged** for a few minutes, and displays **managedContinuously**, later.

Rediscovering a Fabric

Procedure

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

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

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

The **Fabric** is rediscovered.

Purging a Fabric

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

Procedure

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

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

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

The **Fabric** is purged.

UCS Fabric Interconnect Integration

From Release 11.3(1), you can discover and manage UCS FI devices.

Enable Discovery

To allow Cisco DCNM to discover UCS FI server blade and service profile information, you must modify the **server.properties** file.

On the Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**. Locate the **fabric.enableUcsHttpDiscovery** property. Ensure that this value is set to **true**.

Discovering UCS FI devices

From Release 11.3(1), Cisco DCNM can discover UCS FI server blade and service profile from the Web UI.

To discover UCS FI devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

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

The SAN Switches window displays list of fabrics, if any, managed by Cisco DCNM-SAN.

Step 2 Click **Add (+)** icon to add a new fabric.

The Add Fabric window appears.

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

Step 4 (Optional) Check the **SNMP** check box to use SNMPv3 or SSH.

If you check the SNMP check box, the field Community changes to Username and Password.

Step 5 Enter the Username 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** check box 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.

Note By default, the Cisco UCS FI is in NPV mode. Therefore, we recommend that you check the **Enable NPV Discovery in All Fabrics** check box.

Step 9 Click **Options** and specify the UCS Username and UCS Password.

Note Username and password is the SNMP credential; while, UCS User Name and password is the UCS FI CLI admin credential.

Step 10 Select a DCNM server from the DCNM Server drop-down list.

This option is applicable only for Federation setups.

Step 11 Click **Add** to begin managing this fabric.

You can remove single or multiple fabrics from the Cisco DCNM Web Client.

Note UCS FI prohibits using SNMP user **admin**.

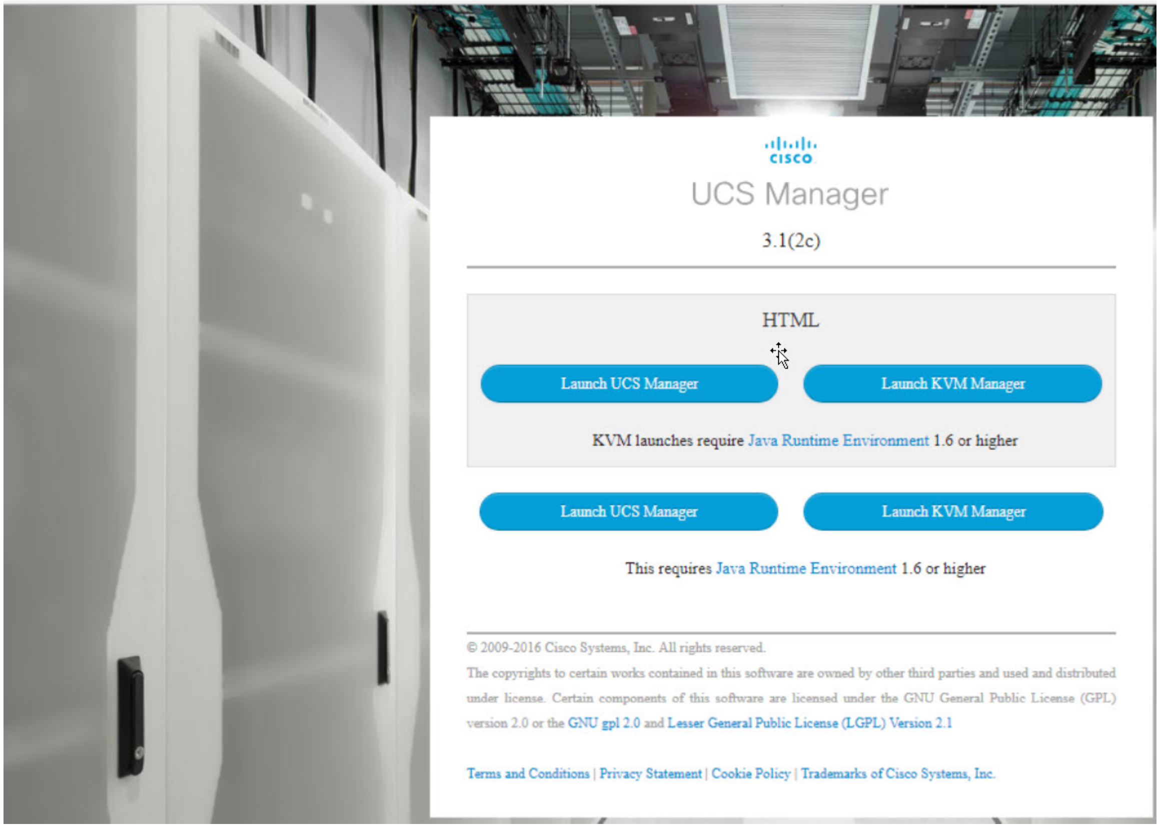
Creating SNMP User on UCS FI

To create a separate SNMP user on UCS FI, follow steps below.

Procedure

Step 1 Login to UCS Manager.

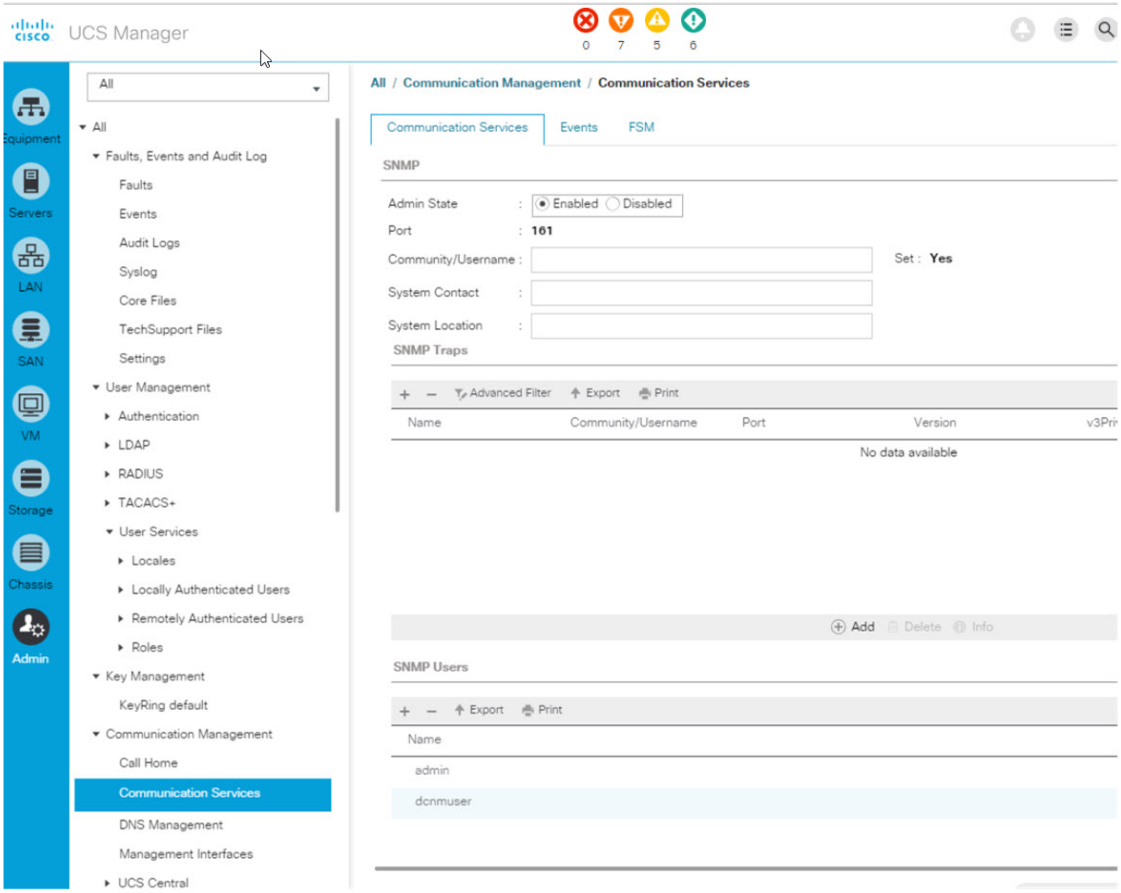
Enter appropriate UCS FI IP Address to the web browser and click **Launch UCS Manager**.



cisco
UCS Manager
3.1(2c)
HTML
Launch UCS Manager
Launch KVM Manager
KVM launches require Java Runtime Environment 1.6 or higher
Launch UCS Manager
Launch KVM Manager
This requires Java Runtime Environment 1.6 or higher
© 2009-2016 Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU gpl 2.0 and Lesser General Public License (LGPL) Version 2.1
Terms and Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Step 2 Click **Admin** tab and choose **Communication Management** > **Communication Services**.

Step 3 In the SNMP section **Admin State** field, select **Enabled**.



All / Communication Management / Communication Services

SNMP

Admin State : ● Enabled ○ Disabled

Port : 161

Community/Username : Set : Yes

System Contact :

System Location :

SNMP Traps

Name	Community/Username	Port	Version	v3Pri
No data available				

SNMP Users

Name
admin
dcnmuser

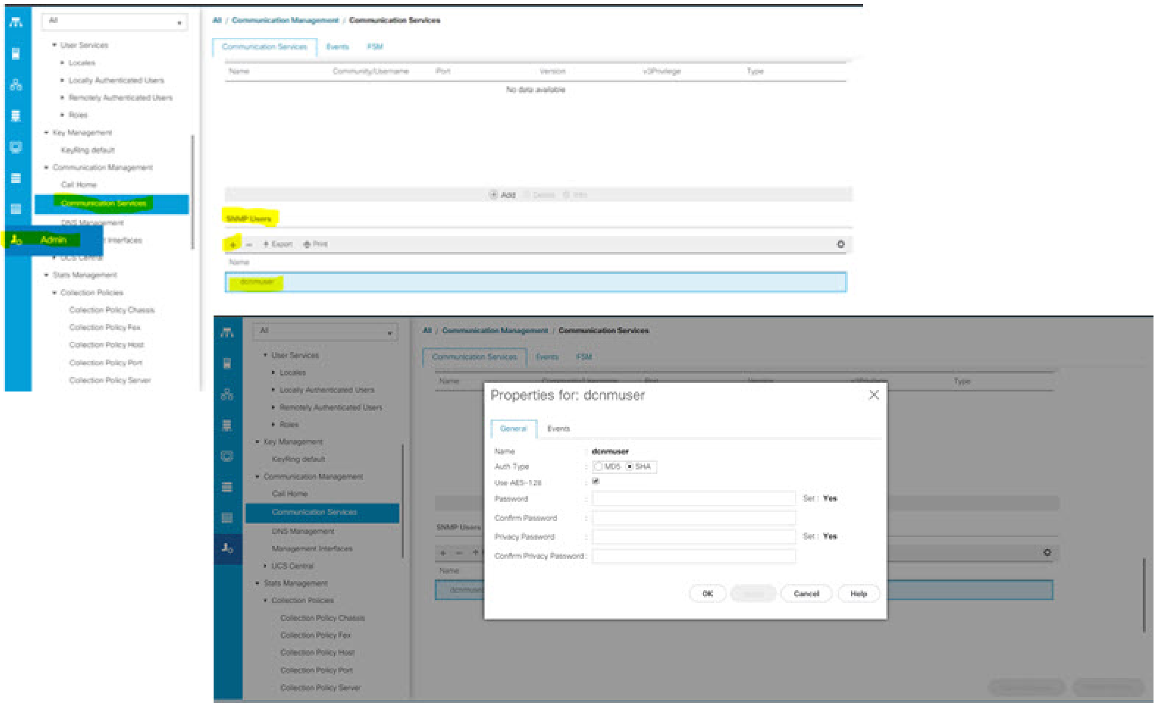
Step 4 Create a new SNMP user and provide the credentials.

UCS Manager 3.2(3) and later releases do not support MD5 authentication if SNMPv3 is in Federal Information Processing Standards (FIPS) mode.

Alternatively, use SHA with AES-128 encryption.

UCS FI supports SNMP communication over SHA_AES Authentication type only (not MD5). Therefore, you must configure SNMP user on both the UCS FI and all switches in the fabric, so that the DCNM can communicate with both the switches and the FI using that common user, such as **dcnmuser**.

Step 5 Configure **dcnmuser** on the UCS FI and set the SNMP password as **password1**. Note that this can be different from the **admin or read-only CLI user** password of the UCS FI, say **password2**.



Properties for: dcnmuser

General | Events

Name : dcnmuser
Auth Type : ○ MD5 ● SHA
Use AES-128 : ☑
Password : Set : Yes
Confirm Password :
Privacy Password : Set : Yes
Confirm Privacy Password :

OK | Apply | Cancel | Help

On all the switches in the fabric, you must configure the same SNMP user **dcnmuser** as **network-admin** or **network-operator** with authentication type as SHA_AES.

```
MDS9396T-174145# show run | i dcnmuser
username dcnmuser password **** role network-admin
snmp-server user dcnmuser network-admin auth sha **** priv aes-128
**** localizedkey
MDS9396T-174145#

MDS9396T-174145# show snmp user

________________________________________________________________
                  SNMP USERS

________________________________________________________________
User           Auth  Priv(enforce) Groups              acl_filter
____           ____  _____________ ______              __________
admin          md5   des(no)       network-admin
dcnmuser       sha   aes-128(no)   network-admin

_________________________________________________________________
NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_________________________________________________________________


User           Auth  Priv
____           ____  ____
```

This applies to the Cisco NPV switches, also.

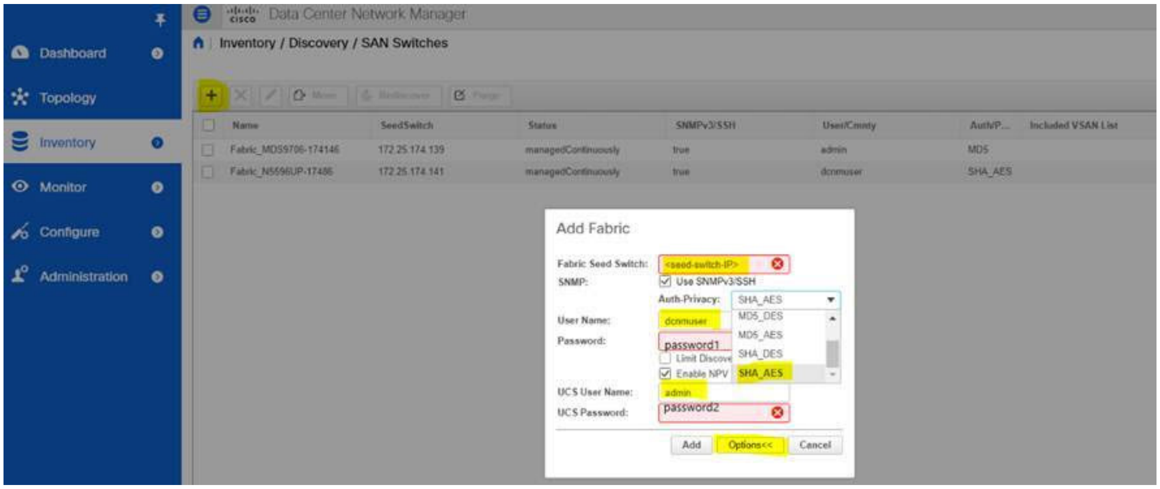
```
MDS9132T-1747# show feature | i npv
npv                   1         enabled

MDS9132T-1747# show snmp user
_________________________________________________________________
                  SNMP USERS
_________________________________________________________________
User           Auth  Priv(enforce) Groups              acl_filter
____           ____  _____________ ______              __________
```

```
admin           md5   des(no)       network-admin
dcnmuser        sha   aes-128(no)   network-admin       network-operator
_________________________________________________________________
NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_________________________________________________________________

User            Auth  Priv
____            ____  ____
```

Step 6 After the USC FI and the switches are accessible using te same credentials, username: **dcnmuser** and password: **password1**, you can discover the Fabric.

Choose **Inventory** > **Discovery** > **SAN Switches**, to discover the Fabric.

Note that you must use username: **admin or read-only CLI username** and password: **password2** for UCS FI.



Name	SeedSwitch	Status	SNMPv3/SSH	User/Cmnty	Auth/P...	Included VSAN List
Fabric_MDS9706-174146	172.25.174.139	managedContinuously	true	admin	MD5	
Fabric_N5596UP-17486	172.25.174.141	managedContinuously	true	dcnmuser	SHA_AES	

Add Fabric

Fabric Seed Switch: <seed-switch-IP>

SNMP: ☑ Use SNMPv3/SSH

Auth-Privacy: SHA_AES (MD5_DES, MD5_AES, SHA_DES, SHA_AES)

User Name: dcnmuser

Password: password1

☐ Limit Discove

☑ Enable NPV

UCS User Name: admin

UCS Password: password2

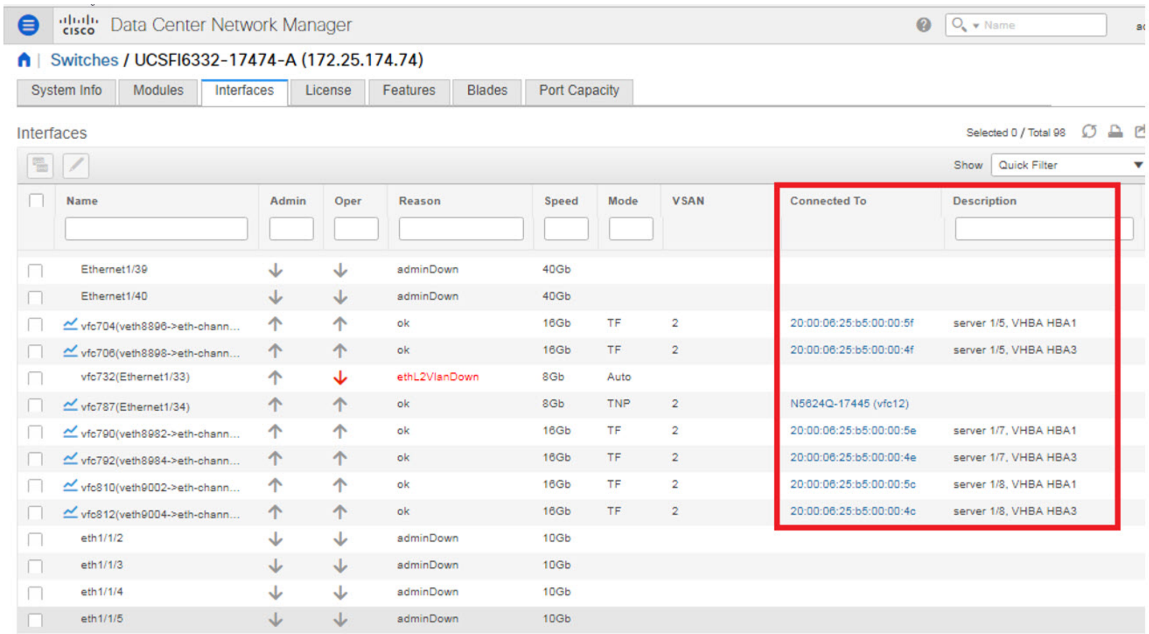
Step 7 Verify if the UCF FI switches are listed on Cisco DCNM **Web UI** > **Inventory** > **Switches**.

Ensure that the status of these switches are correct.

Viewing the UCS FI Switches in the Inventory

You can view the interfaces of the UCSFI switches through **Inventory** > **Switches** > **UCSFI** > **Interfaces**, on the Cisco DCNM Web Client.

The Interfaces tab shows the UCS FI interfaces and the Server Blades that they connect to.

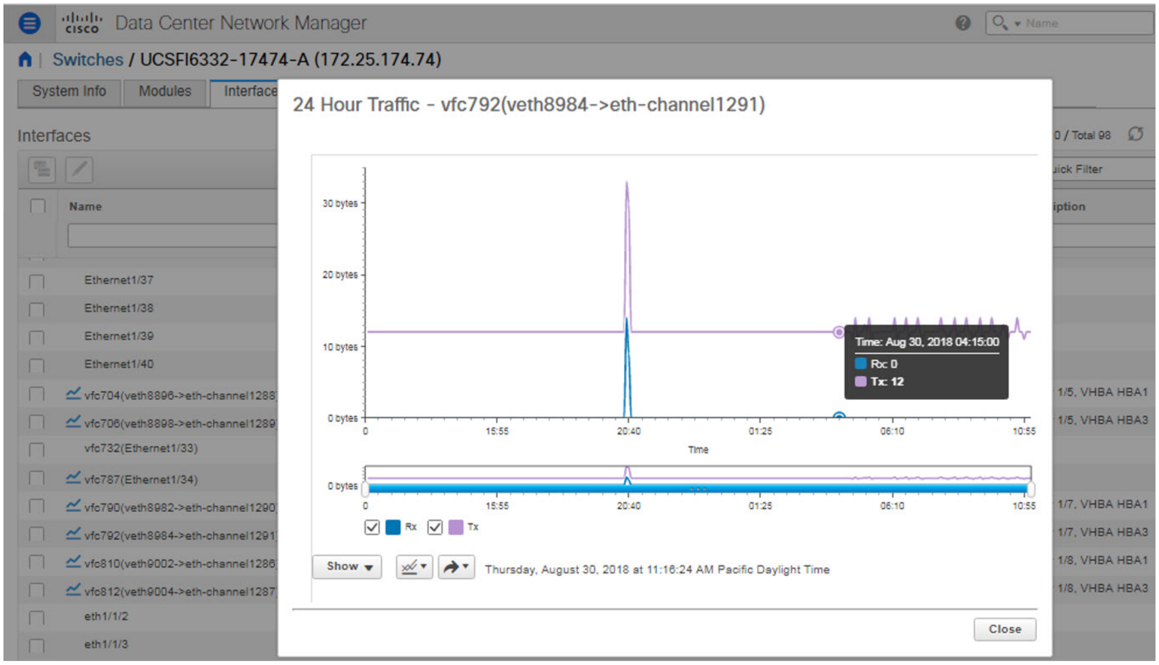


Interfaces

Selected 0 / Total 98

□	Name	Admin	Oper	Reason	Speed	Mode	VSAN	Connected To	Description
□	Ethernet1/39	↓	↓	adminDown	40Gb				
□	Ethernet1/40	↓	↓	adminDown	40Gb				
□	vfc704(veth8896->eth-chann...	↑	↑	ok	16Gb	TF	2	20:00:06:25:b5:00:00:5f	server 1/5, VHBA HBA1
□	vfc706(veth8898->eth-chann...	↑	↑	ok	16Gb	TF	2	20:00:06:25:b5:00:00:4f	server 1/5, VHBA HBA3
□	vfc732(Ethernet1/33)	↑	↓	ethL2VlanDown	8Gb	Auto			
□	vfc787(Ethernet1/34)	↑	↑	ok	8Gb	TNP	2	N5624Q-17445 (vfc12)	
□	vfc790(veth8982->eth-chann...	↑	↑	ok	16Gb	TF	2	20:00:06:25:b5:00:00:5e	server 1/7, VHBA HBA1
□	vfc792(veth8984->eth-chann...	↑	↑	ok	16Gb	TF	2	20:00:06:25:b5:00:00:4e	server 1/7, VHBA HBA3
□	vfc810(veth9002->eth-chann...	↑	↑	ok	16Gb	TF	2	20:00:06:25:b5:00:00:5c	server 1/8, VHBA HBA1
□	vfc812(veth9004->eth-chann...	↑	↑	ok	16Gb	TF	2	20:00:06:25:b5:00:00:4c	server 1/8, VHBA HBA3
□	eth1/1/2	↓	↓	adminDown	10Gb				
□	eth1/1/3	↓	↓	adminDown	10Gb				
□	eth1/1/4	↓	↓	adminDown	10Gb				
□	eth1/1/5	↓	↓	adminDown	10Gb				

Click on the chart icon under Name column to view the 24 hour traffic data for that port.

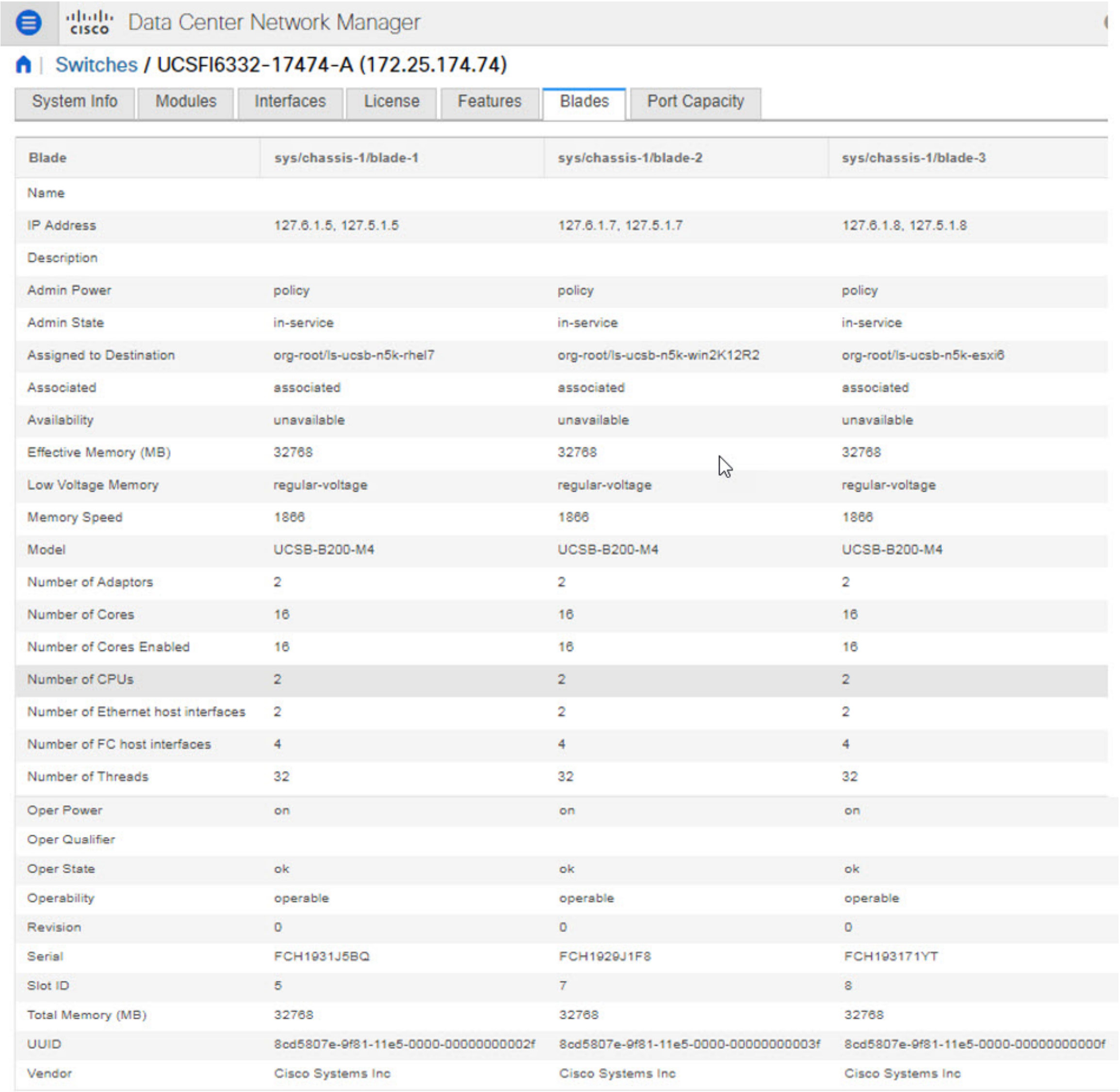


24 Hour Traffic - vfc792(veth8984->eth-channel1291)

Thursday, August 30, 2018 at 11:16:24 AM Pacific Daylight Time

System Info tab displays the corresponding Primary UCS FI IP for the Secondary UCS FI.

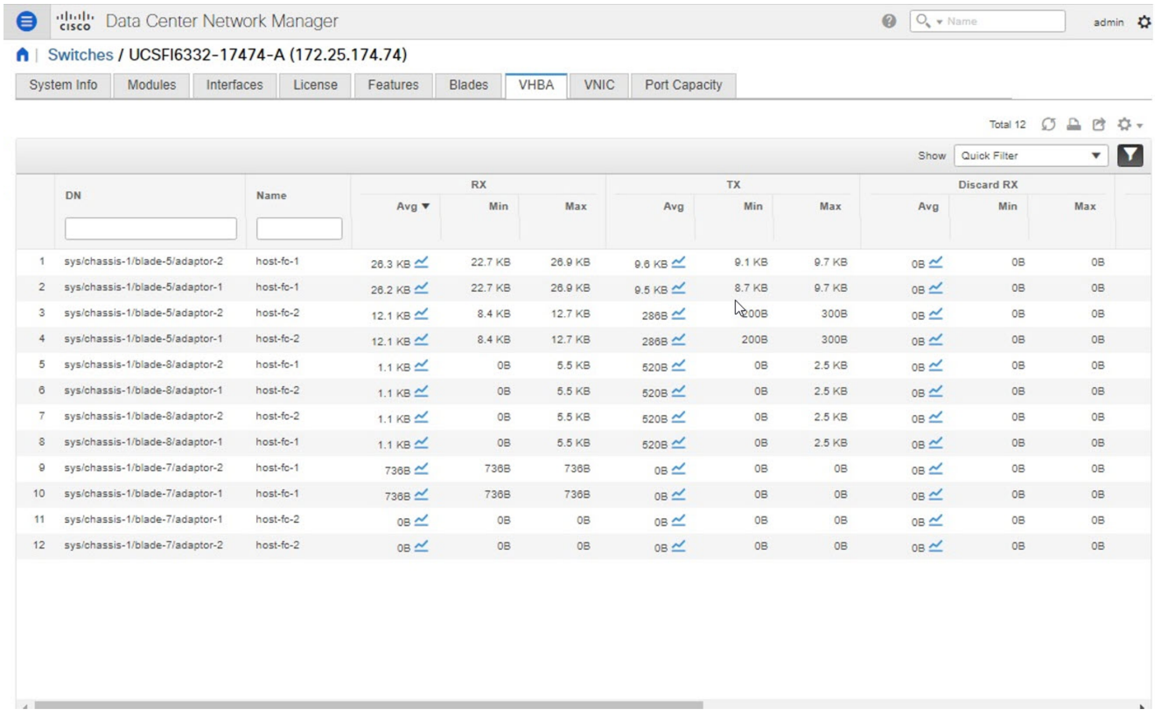
Blades tab displays information of all server blades attached to the UCS FI. Primary UCS FI only in redundancy setup or standalone UCS FI are displayed.



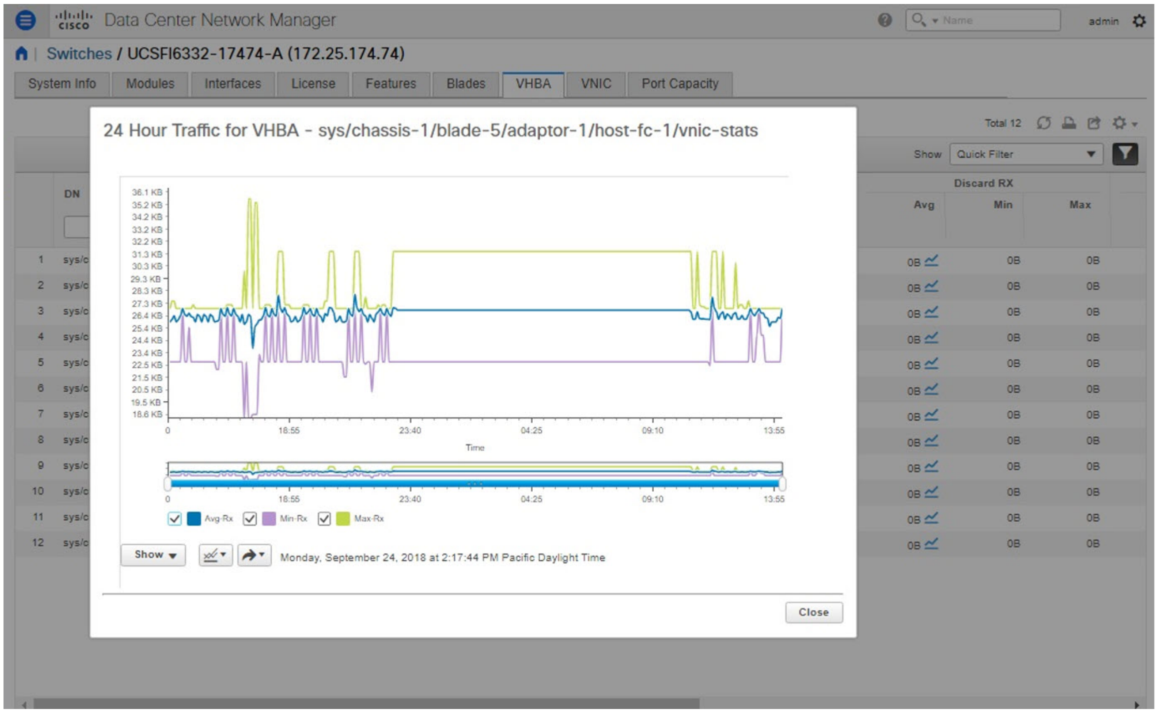
Data Center Network Manager
Switches / UCSFI6332-17474-A (172.25.174.74)
System Info
Modules
Interfaces
License
Features
Blades
Port Capacity

Blade	sys/chassis-1/blade-1	sys/chassis-1/blade-2	sys/chassis-1/blade-3
Name			
IP Address	127.6.1.5, 127.5.1.5	127.6.1.7, 127.5.1.7	127.6.1.8, 127.5.1.8
Description			
Admin Power	policy	policy	policy
Admin State	in-service	in-service	in-service
Assigned to Destination	org-root/ls-ucsb-n5k-rhel7	org-root/ls-ucsb-n5k-win2K12R2	org-root/ls-ucsb-n5k-esxi6
Associated	associated	associated	associated
Availability	unavailable	unavailable	unavailable
Effective Memory (MB)	32768	32768	32768
Low Voltage Memory	regular-voltage	regular-voltage	regular-voltage
Memory Speed	1866	1866	1866
Model	UCSB-B200-M4	UCSB-B200-M4	UCSB-B200-M4
Number of Adaptors	2	2	2
Number of Cores	16	16	16
Number of Cores Enabled	16	16	16
Number of CPUs	2	2	2
Number of Ethernet host interfaces	2	2	2
Number of FC host interfaces	4	4	4
Number of Threads	32	32	32
Oper Power	on	on	on
Oper Qualifier			
Oper State	ok	ok	ok
Operability	operable	operable	operable
Revision	0	0	0
Serial	FCH1931J5BQ	FCH1929J1F8	FCH193171YT
Slot ID	5	7	8
Total Memory (MB)	32768	32768	32768
UUID	8cd5807e-9f81-11e5-0000-00000000002f	8cd5807e-9f81-11e5-0000-00000000003f	8cd5807e-9f81-11e5-0000-00000000000f
Vendor	Cisco Systems Inc	Cisco Systems Inc	Cisco Systems Inc

vHBAs tab displays the list of vHBA for that particular UCS FI. Click the chart icon to view 24hour traffic for the vHBA.



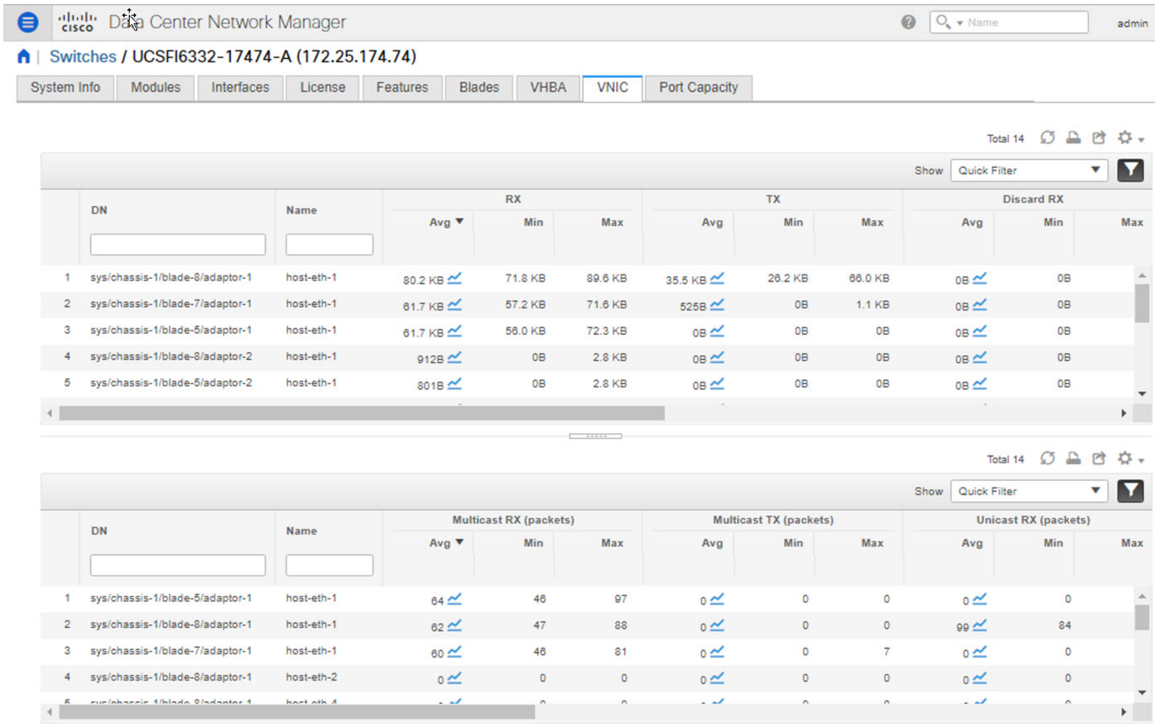
	DN	Name	RX			TX			Discard RX		
			Avg ▼	Min	Max	Avg	Min	Max	Avg	Min	Max
1	sys/chassis-1/blade-5/adaptor-2	host-fc-1	26.3 KB	22.7 KB	26.9 KB	9.6 KB	9.1 KB	9.7 KB	0B	0B	0B
2	sys/chassis-1/blade-5/adaptor-1	host-fc-1	26.2 KB	22.7 KB	26.9 KB	9.5 KB	8.7 KB	9.7 KB	0B	0B	0B
3	sys/chassis-1/blade-5/adaptor-2	host-fc-2	12.1 KB	8.4 KB	12.7 KB	286B	200B	300B	0B	0B	0B
4	sys/chassis-1/blade-5/adaptor-1	host-fc-2	12.1 KB	8.4 KB	12.7 KB	286B	200B	300B	0B	0B	0B
5	sys/chassis-1/blade-8/adaptor-2	host-fc-1	1.1 KB	0B	5.5 KB	520B	0B	2.5 KB	0B	0B	0B
6	sys/chassis-1/blade-8/adaptor-1	host-fc-2	1.1 KB	0B	5.5 KB	520B	0B	2.5 KB	0B	0B	0B
7	sys/chassis-1/blade-8/adaptor-2	host-fc-2	1.1 KB	0B	5.5 KB	520B	0B	2.5 KB	0B	0B	0B
8	sys/chassis-1/blade-8/adaptor-1	host-fc-1	1.1 KB	0B	5.5 KB	520B	0B	2.5 KB	0B	0B	0B
9	sys/chassis-1/blade-7/adaptor-2	host-fc-1	736B	736B	736B	0B	0B	0B	0B	0B	0B
10	sys/chassis-1/blade-7/adaptor-1	host-fc-1	736B	736B	736B	0B	0B	0B	0B	0B	0B
11	sys/chassis-1/blade-7/adaptor-1	host-fc-2	0B	0B	0B	0B	0B	0B	0B	0B	0B
12	sys/chassis-1/blade-7/adaptor-2	host-fc-2	0B	0B	0B	0B	0B	0B	0B	0B	0B



24 Hour Traffic for VHBA - sys/chassis-1/blade-5/adaptor-1/host-fc-1/vnic-stats

Monday, September 24, 2018 at 2:17:44 PM Pacific Daylight Time

vNICs tab displays the list of vNIC for that UCS FI. Click the chart icon will show the 24 hour traffic for the vNIC.



Switches / UCSFI6332-17474-A (172.25.174.74)

Total 14

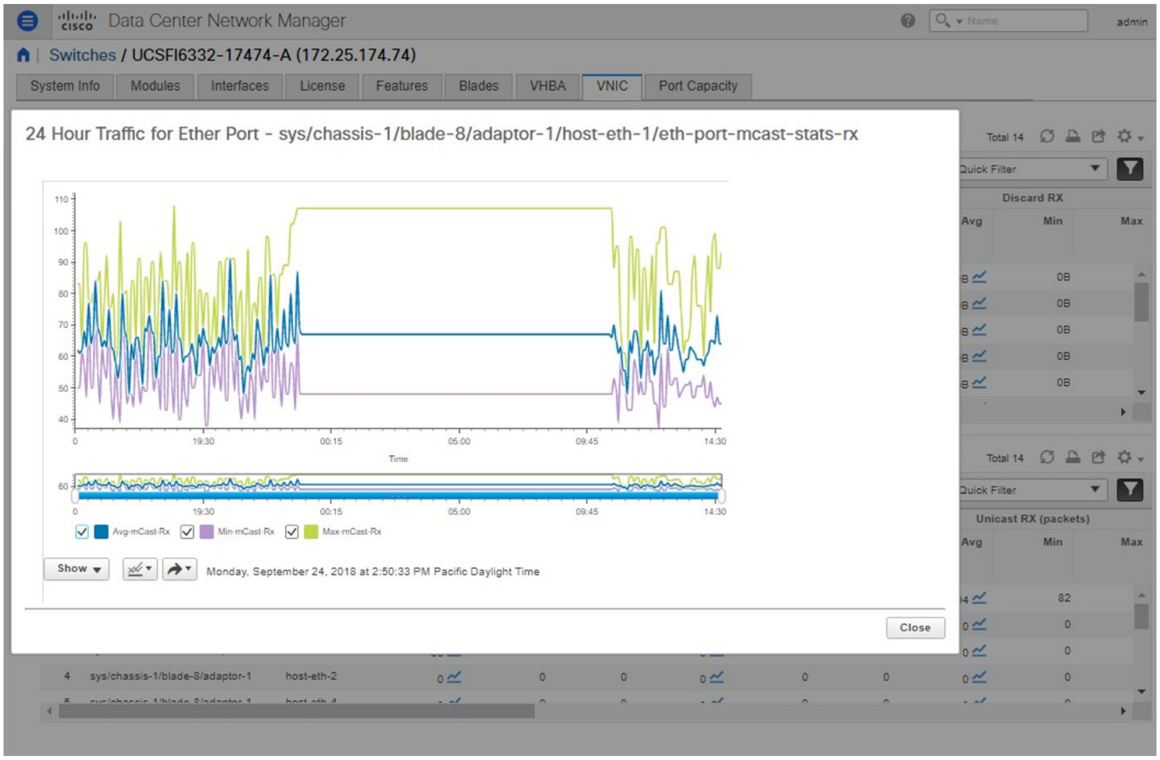
Show: Quick Filter

	DN	Name	RX			TX			Discard RX		
			Avg ▼	Min	Max	Avg	Min	Max	Avg	Min	Max
1	sys/chassis-1/blade-8/adaptor-1	host-eth-1	80.2 KB	71.8 KB	89.6 KB	35.5 KB	26.2 KB	66.0 KB	0B	0B	
2	sys/chassis-1/blade-7/adaptor-1	host-eth-1	61.7 KB	57.2 KB	71.6 KB	525B	0B	1.1 KB	0B	0B	
3	sys/chassis-1/blade-5/adaptor-1	host-eth-1	61.7 KB	56.0 KB	72.3 KB	0B	0B	0B	0B	0B	
4	sys/chassis-1/blade-8/adaptor-2	host-eth-1	912B	0B	2.8 KB	0B	0B	0B	0B	0B	
5	sys/chassis-1/blade-5/adaptor-2	host-eth-1	801B	0B	2.8 KB	0B	0B	0B	0B	0B	

Total 14

Show: Quick Filter

	DN	Name	Multicast RX (packets)			Multicast TX (packets)			Unicast RX (packets)		
			Avg ▼	Min	Max	Avg	Min	Max	Avg	Min	Max
1	sys/chassis-1/blade-5/adaptor-1	host-eth-1	64	46	97	0	0	0	0	0	
2	sys/chassis-1/blade-8/adaptor-1	host-eth-1	62	47	88	0	0	0	99	84	
3	sys/chassis-1/blade-7/adaptor-1	host-eth-1	60	46	81	0	0	7	0	0	
4	sys/chassis-1/blade-8/adaptor-1	host-eth-2	0	0	0	0	0	0	0	0	



Switches / UCSFI6332-17474-A (172.25.174.74)

24 Hour Traffic for Ether Port - sys/chassis-1/blade-8/adaptor-1/host-eth-1/eth-port-mcast-stats-rx

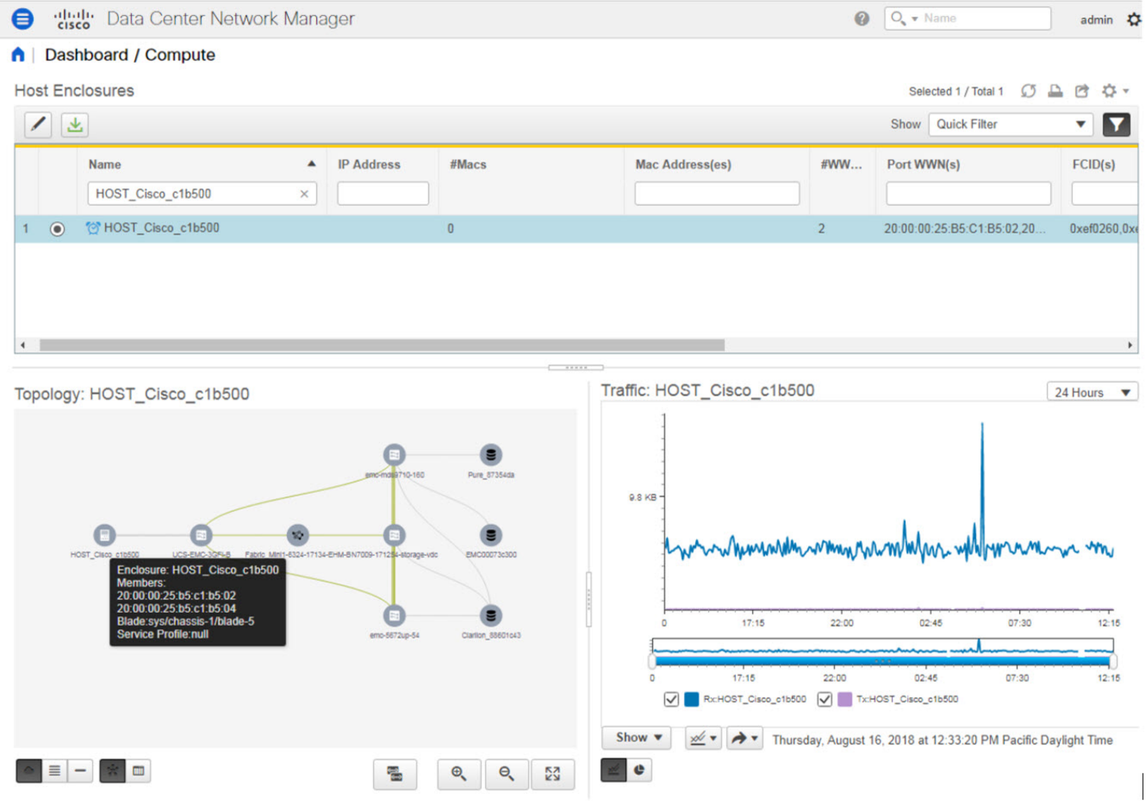
Monday, September 24, 2018 at 2:50:33 PM Pacific Daylight Time

Viewing UCS FI information on Compute Dashboard

From the Cisco DCNM Web UI, choose **Dashboard** > **Compute**.

Click on the details for Host Enclosure connecting to the UCS FIs to view the topology, the Server Blade information and its service profile.

To view the Blade and Service Profile information, hover over the host enclosure in the topology.



Host Enclosures

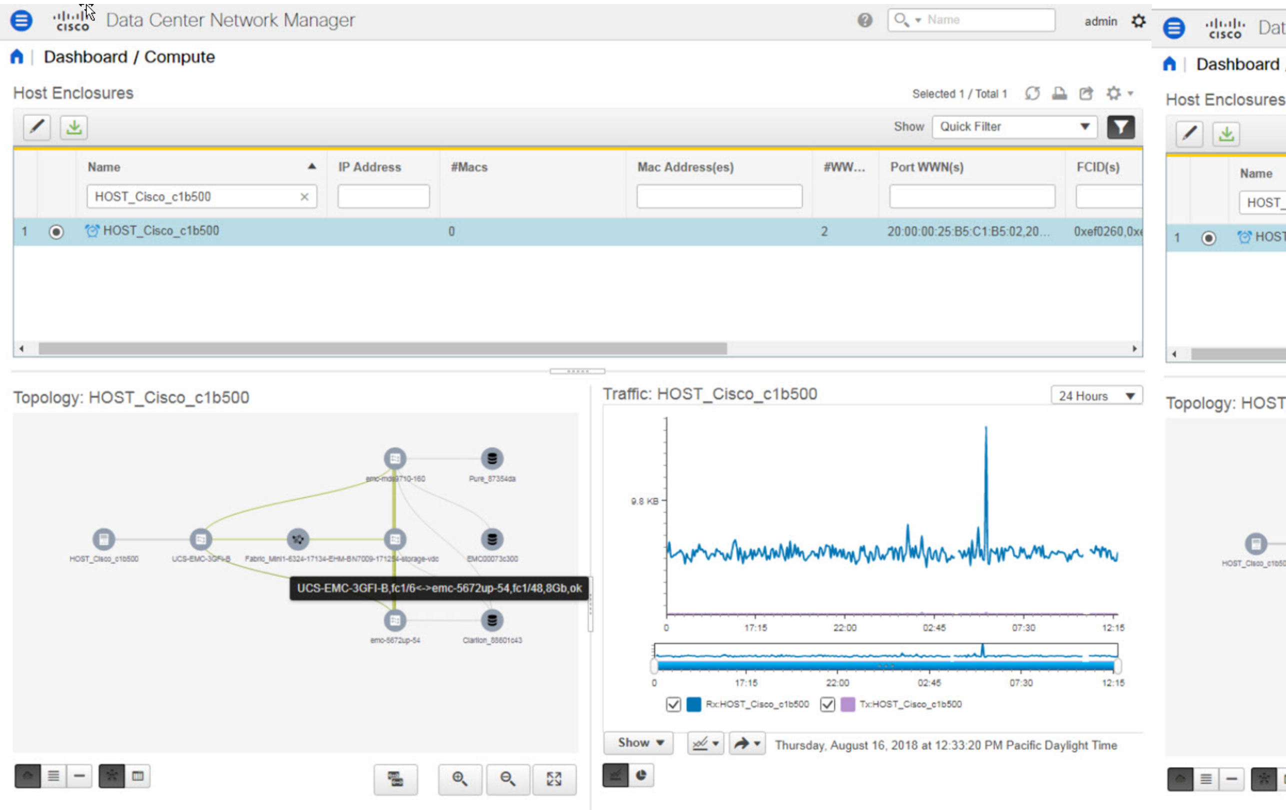
		Name	IP Address	#Macs	Mac Address(es)	#WW...	Port WWN(s)	FCID(s)
		HOST_Cisco_c1b500 ×						
1	●	HOST_Cisco_c1b500		0		2	20:00:00:25:B5:C1:B5:02,20...	0xef0260,0x

Topology: HOST_Cisco_c1b500

Enclosure: HOST_Cisco_c1b500
Members:
20:00:00:25:b5:c1:b5:02
20:00:00:25:b5:c1:b5:04
Blade:sys/chassis-1/blade-5
Service Profile:null

Traffic: HOST_Cisco_c1b500

Thursday, August 16, 2018 at 12:33:20 PM Pacific Daylight Time



		Name	IP Address	#Macs	Mac Address(es)	#WW...	Port WWN(s)	FCID(s)
		HOST_Cisco_c1b500						
1	●	HOST_Cisco_c1b500		0		2	20:00:00:25:B5:C1:B5:02,20...	0xef0260,0xe

Adding, Editing, Removing, Rediscovering and Refreshing SMI-S Storage

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

This section contains the following:

Adding SMI-S Provider

To add an SMI-S provider from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Discovery** > **Storage Devices**.

The **Storage Devices** window is displayed.

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

The **Add SMI-S Provider** window is displayed.

Step 3 Use the drop-down to select the **Vendor**.

All the supported vendors are available in the drop-down list. More 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 the data sources for SMI-S storage discovery.

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

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

Step 6 By default, the **Port** number is prepopulated.

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 the EMC documentation about adding an SSL certificate to their trust store. Also, you can set SSLClientAuthentication value to *None* in the *Security_Settings.xml* configuration file and 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

To delete the SMI-S provider from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Discovery** > **Storage Devices**.

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

The provider is removed and all data that is associated with the provider is purged from the system.

Editing SMI-S Provider

To edit the SMI-S provider from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 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 Choose **Inventory** > **Discovery** > **Storage Devices**.

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

Purge SMI-S Provider

Procedure

Step 1 Choose **Inventory** > **Discovery** > **Storage Devices**.

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

The providers are purged.

Adding, Editing, Re-Discovering and Removing VMware Servers

Cisco DCNM reports information that is gathered by Cisco DCNM-SAN on any VMware servers supported by Cisco DCNM-SAN.

Note Ensure that the SANdiscovered 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.

Procedure

Step 1 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 **Add**.

You see the **Add VCenter** window.

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.

Procedure

Step 1 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 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.

Procedure

Step 1 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**.

A dialog box with warning "Please wait for rediscovery operation to complete." appears.

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

CHAPTER 5

Monitor

This chapter contains the following topics:

Monitoring Switch

The Switch menu includes the following submenus:

Viewing Switch CPU Information

To view the switch CPU information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **CPU**.

The **CPU** window is displayed. This window displays the CPU information for the switches in that scope.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

Step 3 In the **Switch** column, click the switch name to view the Switch Dashboard.

Step 4 Click the chart icon in the **Switch** column to view the CPU utilization.

You can also change the chart timeline to Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year. You can choose the chart type and chart options to show as well.

Viewing Switch Memory Information

To view the switch memory information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **Memory**.

The memory panel is displayed. This panel displays the memory information for the switches in that scope.

Step 2 Use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

Step 3 Click the chart icon in the **Switch** column to see a graph of the memory usage of the switch.

Step 4 In the **Switch** column, click the switch name to view the Switch Dashboard.

Step 5 You can use the drop-down to view the chart in different time lines. Use the chart icons to view the memory utilization chart in varied views.

Viewing Switch Traffic and Errors Information

To view the switch traffic and errors information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **Traffic**.

The **Switch Traffic** panel is displayed. This panel displays the traffic on that device for the past 24 hours.

Step 2 Use the drop-down to filter the view by 24 hours, Week, Month, and Year.

Step 3 Click the **Export** icon in the upper-right corner to export the data into a spreadsheet.

Step 4 Click **Save**.

Step 5 Click the switch name to view the Switch Dashboard section.

Viewing Switch Temperature

Cisco DCNM includes the module temperature sensor monitoring feature, using which you can view the sensor temperature of a switch. You can choose an interval by which to filter the sensor list. The default interval is **Last Day**. Only sensors that have historical temperature data is shown in the list. You can choose between Last ten Minutes, Last Hour, Last Day, Last Week, and Last Month.

Note It is not necessary to configure the LAN or SAN credentials under the **Configure** > **Credentials Management** > **LAN Credentials** screen to fetch the temperature monitoring data from the switches.

To view the switch temperature information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Temperature**.

The **Switch Temperature** window is displayed with the following columns.

- **Scope**: The sensor belongs to a switch, which is part of a fabric. The fabric that it belongs to is shown as its scope. When the scope selector at the top of Cisco DCNM is used, the sensor list is filtered by that scope.
- **Switch**: Name of the switch the sensor belongs to.
- **IP Address**: IP Address of the switch.
- **Temperature Module**: The name of the sensor module.
- **Avg/Range**: The first number is the average temperature over the interval that is specified at the top of the table. The second set of numbers is the range of the temperature over that interval.
- **Peak**: The maximum temperature over the interval

Step 2 From this list, each row has a chart icon, which you can click.
A chart is displayed, which shows historical data for the sensor. The interval for this chart can be changed as well, between 24 hours, 1 week, and 1 month.

Enabling Temperature Monitoring

You can enable the temperature monitoring feature for LAN switches from the LAN Collections screen, and for the SAN switches by setting a few properties under Administration > DCNM Server > Server Properties screens.

Enabling Temperature Monitoring for SAN Switches

1. From the menu bar, select **Administration > DCNM Server > Server Properties**.
2. Navigate to the **# PERFORMANCE MANAGER > COLLECTIONS** area.
3. Set the environment fields **pm.collectSanTemperature** & **pm.sanSensorDiscovery** to **TRUE**.
4. Click **Apply Changes** to save the configuration.
5. Restart Cisco DCNM.

Viewing Other Statistics

To view the statistics in user-defined format from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > User Defined**.

The **Other** window is displayed.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month, and Year.

There are variations to this procedure. In addition to these basic steps, you can also do the following:

- Select the time range, and click **Filter** to filter the display.
- Click the chart icon in the **Switch** column to see a graph of the performance for this user-defined object. You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.
- Use the chart icons to view the traffic chart in varied views.

Viewing Switch Custom Port Groups Information

To view the custom port group information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **Custom Port Groups**.

The Custom Port Groups window shows statistics and performance details for custom port groups.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month, and Year.

Step 3 Click the **Export** icon in the upper-right corner to export the data into a spreadsheet.

Step 4 Click **Save**.

Step 5 Click the switch name to view the Switch Dashboard.

Viewing Accounting Information

To view the accounting information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **Accounting**.

The fabric name or the group name along with the accounting information is displayed.

Step 2 Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **Username**,**Time**, and **Description**. Or select **Quick Filter** to search under each column.

Step 3 You can also select a row and click the **Delete** icon to delete accounting information from the list.

Step 4 You can use the **Print** icon to print the accounting details and use the **Export** icon to export the data to a Microsoft Excel spreadsheet.

Viewing Events Information

To view the events and syslog from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **Events**.

The fabrics along with the switch name and the events details are displayed.

The **Count** column displays the number of times the same event has occurred during the time period as shown in the **Last Seen** and **First Seen** columns.

Click a switch name in the **Switch** column to view the switch dashboard.

Step 2 Select an event in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule.

Step 3 Select one or more events from the table and click the **Acknowledge** icon to acknowledge the event information for the fabric.

- After you acknowledge the event for a fabric, the acknowledge icon is displayed in the **Ack** column next to the fabric.

Step 4 Select the fabric and click the **Unacknowledge** icon to cancel an acknowledgment for a fabric.

Step 5 Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **Username**,**Time**, and **Description**. Or select **Quick Filter** to search under each column.

Step 6 Select a fabric and use the **Delete** icon to delete the fabric and event information from the list.

Step 7 Click the **Print** icon to print the event details.

Step 8 Click the **Export to Excel** icon to export the data.

Monitoring SAN

The SAN menu includes the following submenus:

Monitoring ISL Traffic and Errors

To monitor the ISL traffic and errors from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **ISLs**.

The **ISL Traffic and Errors** window is displayed. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month, and Year.

Note **NaN** (Not a Number) in the data grid means that the data is not available.

Note It is empty for non-FCIP ports under the **FCIP Compression Ratio** column.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict, and Interpolate Data. To view real-time information, choose **Refresh** icon from in the upper right corner. The real-time data is updated in every 10 seconds.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation formula.

  Note The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

  - Average Rx/Tx % = Average Rx/Tx divided by Speed * 100
  - Peak Rx/Tx % = Peak Rx/Tx divided by Speed * 100

If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

Viewing Performance Information for NPV Links

To view the performance of NPV links from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > SAN > NPV Links**.

The **NPV Links** window is displayed. This window displays the NPV links for the selected scope.

Step 2 You can use the drop-down to filter the view by **24 hours, Week, Month**, and **Year**.

Step 3 Click the chart icon in the **Name** column to see a list of the traffic for the past 24 hours.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for NPV links:

- You can change the time range for this information by selecting from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict**, and **Interpolate Data**.

- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save**.
- To view real-time information, choose **Real Time** from the drop-down list in the **Chart** menu.

Note If the performance tables do not contain any data, see the Performance Setup Thresholds, on page 313 section to turn on performance data collection.

Viewing Inventory Information for VSANs

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

Procedure

Choose **Monitor** > **SAN** > **VSANs**.

The **VSAN** window is displayed, showing the VSAN details along with the status and **Activated Zoneset** details.

Monitoring Performance Information for Ethernet Ports

To monitor the performance of Ethernet ports from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **Ports**.

The **Ethernet Ports** window is displayed.

Step 2 You can use the drop-down to filter the view by **24 hours, Week, Month**, and **Year**.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Choose an Ethernet port in the **Name** column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then **Save**.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict**, and **Interpolate Data**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation formula.

Note The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed * 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed * 100

Note If the performance tables do not contain any data, see the Performance Setup Thresholds, on page 313 section to turn on performance data collection.

Viewing Inventory Information for Host Ports on FC End Devices

To view the inventory information for host ports on FC end devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **FC Ports**.

The **Inventory** > **End Ports** window is displayed with details of the FC End Devices on the host ports.

Step 2 Use the drop-down to view All or Warning information for the FC End devices on host ports.

Step 3 Click the **Show Filter** icon to enable filtering by **Enclosure, Device Name**, or **VSAN**.

Viewing Performance Information on All Ports

To view the performance of devices that are connected to all the ports from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Performance** > **End Devices**.

The **End Devices Traffic and Errors** window is displayed.

Step 2 You can choose to display **All** ports, **Host** ports, or **Storage** ports from the drop-down list on the upper right corner.

Step 3 You can use the drop-down to filter the view by **24 hours, Week, Month**, and **Year**.

Step 4 To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save**.

Step 5 Click the chart icon in the **Name** column to see the following:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, click the refresh icon from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to **Append, Predict**, and **Interpolate Data**.

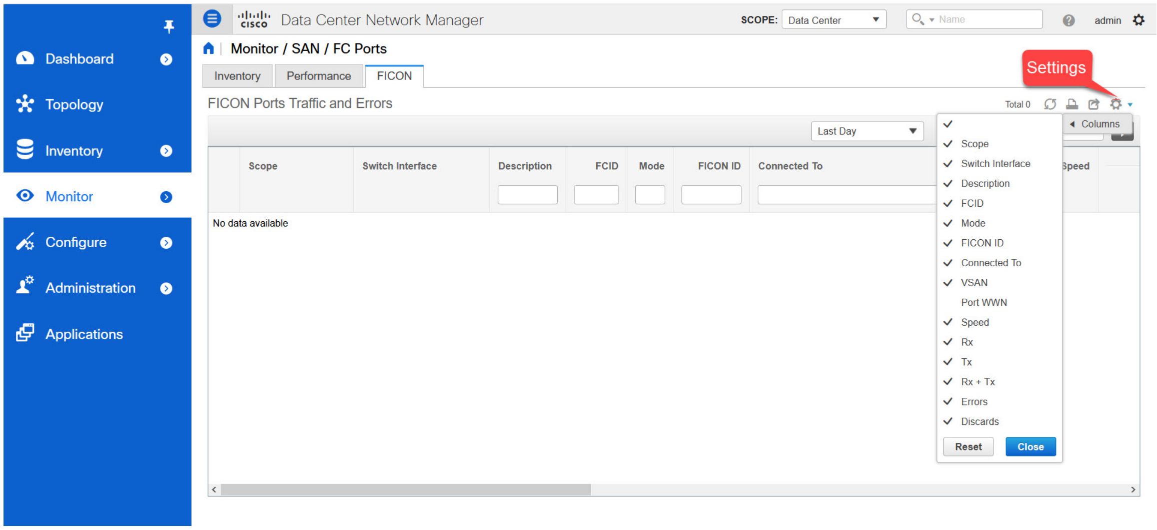
Note If the performance tables do not contain any data, see the Performance Setup Thresholds, on page 313 section to turn on performance data collection.

Viewing FICON Ports

The following table displays the traffic and error information for every FICON port.

Field	Description
Scope	Specifies the fabric scope, which has the FICON ports.
Switch Interface	Click the Show Chart icon to view the port traffic of the selected switch interface.
Description	Specifies the description of the FICON port.
FCID	Specifies the fibre channel ID.
Mode	Specifies the type of port. Valid values are **CH** and **CU**. The value is **CH** for FICON channels and **CU** for FICON control unit.
FICON ID	Specifies the FICON port ID.
Connected To	Specifies the device to which the FICON port is connected.
VSAN	Specifies the VSAN ID.
Speed	Specifies the speed of the FICON port.
Rx	Specifies the average and peak Rx traffic.
Tx	Specifies the average and peak Tx traffic.
Rx + Tx	Specifies the sum of Rx and Tx traffic.
Errors	Specifies the average and peak input and output errors.
Discards	Specifies the average and peak input and output discards.

You can view the Port WWN details by choosing **Settings** > **Columns** and choose the **Port WWN** option from the drop-down list.



You can print, export the data, or customize the columns you want to view. Refresh the table to see the latest data.

To view the traffic and errors of FICON ports from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **FC Ports**.

The **Inventory** window appears.

Step 2 Click the **FICON** tab.

Step 3 Click the **Show Chart** icon of the switch interface for which you want to view the traffic.

The real-time data is updated every 10 seconds. You can also use the icons to append, predict, or interpolate data.

Note Click the **Do Not interpolate Missing Data** icon to remove the missing data gap in the graph. By default, the missing data is interpolated in all graphs.

You can choose how you want to view the traffic. You can view the traffic details based on the time duration, format, and export this information.

You can view the port traffic for the following durations from the duration drop-down list:

- 24 Hours
- Week
- Month
- Year

Show: Click **Show**, and choose **Chart**, **Table**, or **Chart and Table** from the drop-down list to see how you want to view the traffic details.

If you choose **Chart**, hover over the traffic chart to view the Rx and Tx values, along the Y axis, for the corresponding time, along X axis. You can change the time duration values of the X axis by moving the sliders in the time range selector. You can choose the Y-axis values by checking or unchecking the Rx and Tx check boxes.

Note If you select **Week**, **Month**, or **Year** as the time duration, you can also view the Peak Rx and Peak Tx values along the Y axis.

Select **Table** to view the traffic information in tabular format.

Chart Type and **Chart Options**: Choose **Area Chart** or **Line Chart** from the **Chart Type** drop-down list.

You can choose the **Show Fill Patterns** chart option.

Actions: Export or print the traffic information by choosing the appropriate options from the **Actions** drop-down list.

Viewing Performance Information for FC Flows

To view the performance of the **FC Flow** traffic from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **FC Flows**.

The **FC Flows** window is displayed.

Step 2 You can use the drop-down to filter the view by **24 hours, Week, Month**, and **Year**.

Step 3 To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the **Name** column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, click the **Refresh** icon from the drop-down list in the upper right corner.
- You can also use the icons to **Append, Predict**, and **Interpolate Data**.

Note If the performance tables do not contain any data, see the Performance Setup Thresholds, on page 313 section to turn on performance data collection.

Viewing Performance Information on Enclosures

To view the performance of devices that are connected to the host enclosure from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **Enclosures**.

The **Enclosures Traffic and Errors** window is displayed.

Step 2 You can select to view **Host Enclosures** or **Storage Enclosures** from the drop-down list on the upper right corner.

Step 3 You can use the drop-down to filter the view by **24 hours, Week, Month**, and **Year**.

Step 4 To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

Step 5 Click the chart icon in the **Name** column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to **Append, Predict**, and **Interpolate Data**.

Note If the performance tables do not contain any data, see the Performance Setup Thresholds, on page 313 section to turn on performance data collection.

Viewing Performance Information on Port Groups

To view the performance of devices that connected to the port groups from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **SAN** > **Port Groups**.

The **Port Group Traffic and Errors** window is displayed.

Step 2 You can use the drop-down to filter the view by **24 hours, Week, Month**, and **Year**.

Step 3 Click the name port group to see the members of that port group.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for the port groups:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to **Append, Predict**, and **Interpolate Data**.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save**.

Note If the performance tables do not contain any data, see the Performance Setup Thresholds, on page 313 section to turn on performance data collection.

SAN Host Redundancy

The **SAN Host Path Redundancy** check enables you to view the non-redundant host storage paths. It helps you identify the host enclosure errors along with the resolution to fix the errors.

Note All fabrics that are discovered must be licensed or this feature will be disabled in the Cisco DCNM Web Client. When the feature is disabled, a notification is displayed stating unlicensed fabrics are discovered.

Host Path Redundancy determines that the ports are part of the same enclosure by using the enclosure name displayed in DCNM. If the enclosure names are not exactly the same, then they will be viewed as separate devices. When the names are not exactly the same, the user must manually change the names in the edit enclosure dialog in DCNM, in order for Host Path Redundancy and other features to consider them the same device.

From the menu bar, choose **Monitor** > **SAN** > **Host Path Redundancy**.

You can see two parts in this window:

Tests to Run

Procedure

Step 1 Choose **Monitor** > **SAN** > **Host Path Redundancy**.

Step 2 Under the upper **Tests to Run** area, use the check boxes to select the host redundancy optional checks.

Step 3 Check the **Automatically Run Check Every 24 hours** check box to enable periodic running of the checker. The checker will run every 24 hours starting 10 minutes after the server starts.

Step 4 Check **Limit by VSANs** check box, and select **Inclusion** or **Exclusion**. Enter VSAN or VSAN range in the text field to include or skip the host enclosures that belong to VSANs from the redundancy check.

Step 5 Check other optional checks to do the relevant check.

Step 6 Click **Clear Results** to clear all the errors displayed.

Step 7 Click **Run Tests Now** to run the check at anytime.

Step 8 The results are displayed in the below Results area.

Results

Procedure

Step 1 Choose **Monitor** > **SAN** > **Host Path Redundancy** tab.

Step 2 The bottom **Results** area has four tabs that are **Host Path Errors**, **Ignored Hosts**, **Ignored Storage**, and **Ignored Host Storage Pairs**.

Step 3 Click **Host Path Errors** tab to display the host path redundancy errors table. On the top of the table, the colored **Good, Skipped**, and **Errored** host enclosure counts, along with the last update time are displayed.

a) The **Host Enclosure** column displays the hosts that contain the errors. These are counts of each path in the host enclosures seeing an error. The **Storage Enclosure/Storage Port** column displays the connected storage that is involved the errors. In the **Fix?** column, hover the mouse cursor on the **?** icon to view a solution to fix the error.
b) Select a row and click **Ignore Hosts** to add the selected rows host enclosure to an exclusion list. The errors from that host will no longer be reported and the current errors will be purged from the database.
c) Select a row and click **Ignore Storage** to add the selected rows storage enclosure to an exclusion list.
d) Select a row and click **Ignore Host Storage Pair** to add the selected rows host-storage pair enclosure to an exclusion list.
e) In the drop-down list next to **Show** on the upper right corner of the table, select **Quick Filter**. Enter the keywords in the column headers of the table to filter the items. Select **All** to display all the items.
f) Click the circulation icon on the upper right corner of the table to refresh the table.
g) Click the **Print** icon on the upper right corner of the table to print the errors as tables.
h) Click the **Export** icon on the upper right corner of the table to export the table to a Microsoft excel spreadsheet.

Step 4 Click the **Ignored Hosts** tab to display the list of host enclosures that have been skipped or ignored by the redundancy check along with the reason the reason for skipping. The following reasons may be displayed:

- **Skipped: Enclosure has only one HBA.**
- **Host was ignored by the user.**
- **Host ports managed by more than one federated servers. Check can't be run.**
- Skipped: No path to storage found.

Select a host enclosure and click **Delete** to remove the host from the ignored list and begin receiving errors about a host you had chosen to ignore. However, you can delete entries with message **Host was ignored by user**.

Step 5 Click the **Ignored Storage** tab to display the list of storage enclosures that have been selected to be ignored during the redundancy check. Select a storage enclosure and click **Delete** to remove the storage from the ignored list and begin receiving errors about the storage you had chosen to ignore.

Step 6 Click the **Ignored Host Storage Pair** tab to display the list of host-storage pairs that have been selected to be ignored during the redundancy check. Select a row and click **Delete** to delete the storage pair from the ignored list.

Slow Drain Analysis

The **Slow Drain Analysis** enables you to view slow drain statistics at the switch level and the port level. You can monitor the slow drain issue within any duration. You can display the data in a chart format and export the data for analysis. You can also view the topology that provides a high-level view of txwait, drops, credit loss recovery, over utilization, and port monitor events.

The slow drain statistics are stored in the cache memory. Therefore, the statistics are lost when the server is restarted or a new diagnostic request is placed.

You can also watch the video and demonstrate how to use SAN Insights to identify if there are any slow drain metrics incrementing across a fabric using a Cisco DCNM. See Video: Slow Drain Analysis with SAN Insights.

Note The jobs run in the background, even after you log off.

Procedure

Step 1 Choose **Monitor** > **SAN** > **Slow Drain Analysis**.

Step 2 In the **Scope** field, select the fabric from the drop-down list.

Step 3 In the **Duration** drop-down list, select **Once** or **Daily** for the scheduled daily job. **Once** includes intervals, such as 10 min, 30 min, 1 hour, and other hours and run the job immediately. **Daily** allows you to select a start time, and run the job for the selected interval. Use the radio button to select the desired interval to collect data.

Only **Daily** slow drain job sends out report, which can be viewed from **Monitor** > **Report** > **View**.

Step 4 Click **Start Collection** to begin polling.

The server collects the slow drain statistics based on the scope defined by you. The **Time Remaining** is displayed in the right-side of the page.

Step 5 Click **Stop Collection** to stop polling.

The server maintains the counters in the cache, until a new diagnostic request is placed. You can stop the polling before the time is up.

Step 6 Click the arrow next to **Current jobs** to display the slow drain details for the jobs running on the fabric. The **Fabric Name**, the **Status** of polling, **Start**, **End**, and **Duration** icon for each fabric is displayed.

Step 7 Select the fabric and click **Result**, **Delete** or **Stop** to view, delete or stop a job.

A topology of the selected fabric will appear if you select a fabric and click **Result**, along with the slow drain details. See *Slow Drain Visualization* for more information.

Step 8 Click **Detail** to view the saved information.

Step 9 Click **Interface chart** to display the slow drain value for the switch port in the chart format.

Step 10 Click **Filter** to display the details based on the defined value for each column.

Step 11 Select the **Data Rows Only** check box to filter and display the nonzero entries in the statistics.

Step 12 Click **Print** to print the slow drain details.

Step 13 Click **Export** to export the slow drain statistics to a Microsoft Excel spreadsheet.

Slow Drain Visualization

A topology of the selected fabric appears if you select a fabric and click **Result**, along with the slow drain details. The topology window shows color-encoded nodes and links that correspond to various network elements. For each of the elements, you can hover over to fetch some more information. The links and switches are color-coded. Enable performance collections and SNMP traps to view the slow drain information on the topology. Choose **Administration** > **Performance Setup** > **SAN Collections** and enable the performance collections. See Performance Manager SAN Collections, on page 312 for more information on enabling the performance collections. Choose **Administration** > **Event Setup** > **Registration** and enable SNMP traps. See #unique_144 for more information on enabling SNMP traps.

The following table lists the color description that is associated with the links and switches.

Table 9: Color Description

Color	Name	Description
Blue (light)	Level 5	High utilization tx-datarate >= 80%
Green	Level 4	No slow drain found
Red	Level 3	Credit loss recovery
Orange	Level 2	Drops
Yellow (dark)	Level 1.5	txwait >= 30%
Yellow (light)	Level 1	txwait < 30%
Gray (light)	No Data	No Data

A switch color represents the highest level slow drain that is found on any link to switch. The maximum value is 3 and the minimum value is 1. A switch has two colors if overutilized. The right half of the switch is colored in light blue to represent the overutilization. A number on the switch represents the number of F ports with the slow drain. The color around the number represents the highest level slow drain that is found on F ports of the switch. Click the switch to see more slow drain details. Double click the switch to filter the slow drain table to view the slow drain data of that switch alone.

Two parallel lines are used to represent the slow drain on links. Links are bidirectional, hence each direction has a color to represent the highest level of slow drain. Hover over a link to view the switch and interface name of the source and destination. Double click a link to filter the slow drain table to view the slow drain data that is related to that link alone.

Note The highest slow drain level a link can have is **Level 4**. Valid colors for a link are Green, Red, Orange, Yellow (dark), Yellow (light), and Gray (light).

Viewing Inventory Information for Regular Zones

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

Procedure

Step 1 Choose **Monitor** > **SAN** > **Regular Zones**.

The **Regular Zones** window appears.

Step 2 Click the **Settings** icon to choose the displaying columns.

What to do next

From Cisco DCNM Release 11.4(1), you can migrate pWWN-based SAN zones from a Brocade switch to a Cisco MDS switch using the Zone Migration tool.

This feature supports migration of Brocade's fabric switches running Brocade Fabric OS v7.x.x or later in this release.

Zone Migration Tool

From Cisco DCNM Release 11.4(1), you can migrate pWWN-based SAN zones from a Brocade switch to a Cisco MDS switch. This involves the following steps:

1. Generating Brocade Configuration File
2. Converting Configuration Files Using the Zone Migration Tool
3. Applying the Zoning Output on Cisco MDS Switches

This feature supports migration of Brocade's fabric switches running Brocade Fabric OS v7.x.x or later in this release.

Generating Brocade Configuration File

Before you migrate a Brocade SAN zone to a Cisco MDS switch using Cisco DCNM, generate the Brocade configuration files.

You can generate the Brocade configuration files using one of the following options:

- Using CLI: Log in to the Brocade switch terminal using the admin or other equivalent role with admin access. Run the **cfgshow** command. Copy the command output to a text file, and save it.
- Using Brocade Fabric OS Web tools: Download the **Zoning Information** file from the **Switch Administration** window. See the *Viewing and Printing a Switch Report* section from the *Brocade Fabric OS Web Tools Administration Guide* for more information.

Converting Configuration Files Using the Zone Migration Tool

To convert the Brocade configuration files using Cisco DCNM, perform the following steps from Cisco DCNM Web UI:

Procedure

Step 1 Choose **Monitor** > **SAN** > **Regular Zones**.

Step 2 Click **Zone Migration Tool** button.

The **Zone Migration Tool** dialog box appears.

Step 3 Click **Select Input File** and choose a Brocade configuration file from your system.

Step 4 Enter the VSAN number to which the zone must be added.

The valid range is 1 to 4093.

Step 5 (Optional) Check **Enhanced Zone Mode** or **Enhanced Device-Alias Mode** check boxes.

Note Refer the *Configuring and Managing Zones* chapter and the *Distributing Device Alias Services* chapter from the *Cisco MDS 9000 Fabric Configuration guide* to see the advantages of enhanced zone mode and enhanced device-alias mode.

Step 6 Click **Convert** to start the conversion.

If there are no errors, the converted file will be downloaded to your local system.

Note

- If you try converting any hard zones or interface-based zones, you will get an error.
- If you try to migrate more than 2000 fcAlias zones from Brocade to Cisco MDS, they will be converted into device-alias zones.

What to do next

Run the downloaded file in a Cisco MDS switch.

Applying the Zoning Output on Cisco MDS Switches

After you convert Brocade configuration files to a format compatible with the Cisco MDS switches, apply them on your Cisco MDS switch.

To apply the output on a Cisco MDS switch, perform the following steps:

Procedure

Step 1 Log into your Cisco MDS switch console.

Step 2 Open the converted file using a text editor.

Step 3 Open the converted file using a text editor.

Step 4 Save the configurations using the **copy running-config startup-config** command.

The zones are migrated to the Cisco MDS switch.

Viewing Inventory Information for IVR Zones

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

Procedure

Step 1 Choose **Monitor > SAN > IVR Zones**.

The **IVR Zones** window is displayed with inventory details of the fabrics for the IVR zone.

Step 2 Click the **Settings** icon to choose the displaying columns.

Monitoring Insights Flows

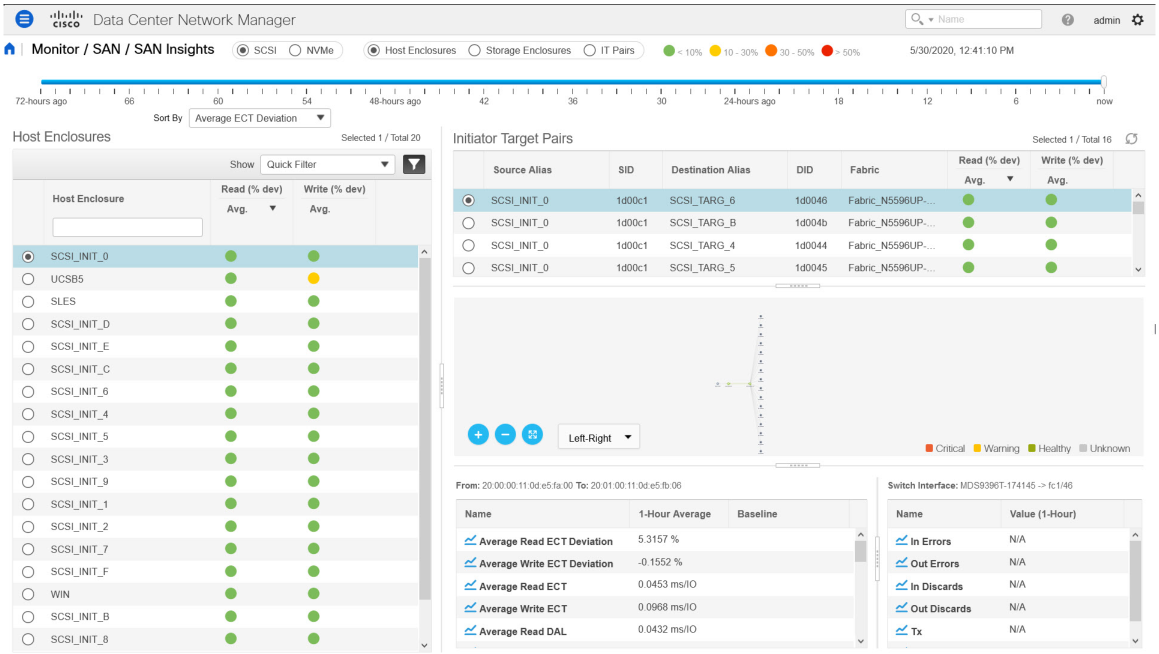
The SAN Insights page displays the health-related indicators in the interface so that you can quickly identify issues in your environment. You can use health indicators to understand where problems are in your fabrics.

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

Note If the interface is down, it's displayed in grey color.

Procedure

Step 1 To monitor the SAN Insights feature, choose **Monitor** > **SAN** > **SAN Insights**. The SAN Insights page appears.



◉ SCSI ○ NVMe

◉ Host Enclosures ○ Storage Enclosures ○ IT Pairs

5/30/2020, 12:41:10 PM

Sort By: Average ECT Deviation

Host Enclosures — Selected 1 / Total 20

Show: Quick Filter

	Host Enclosure	Read (% dev) Avg.	Write (% dev) Avg.
◉	SCSI_INIT_0	🟢	🟢
○	UCSB5	🟢	🟡
○	SLES	🟢	🟢
○	SCSI_INIT_D	🟢	🟢
○	SCSI_INIT_E	🟢	🟢
○	SCSI_INIT_C	🟢	🟢
○	SCSI_INIT_6	🟢	🟢
○	SCSI_INIT_4	🟢	🟢
○	SCSI_INIT_5	🟢	🟢
○	SCSI_INIT_3	🟢	🟢
○	SCSI_INIT_9	🟢	🟢
○	SCSI_INIT_1	🟢	🟢
○	SCSI_INIT_2	🟢	🟢
○	SCSI_INIT_7	🟢	🟢
○	SCSI_INIT_F	🟢	🟢
○	WIN	🟢	🟢
○	SCSI_INIT_B	🟢	🟢
○	SCSI_INIT_8	🟢	🟢

Initiator Target Pairs — Selected 1 / Total 16

	Source Alias	SID	Destination Alias	DID	Fabric	Read (% dev) Avg.	Write (% dev) Avg.
◉	SCSI_INIT_0	1d00c1	SCSI_TARG_6	1d0046	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_0	1d00c1	SCSI_TARG_B	1d004b	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_0	1d00c1	SCSI_TARG_4	1d0044	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_0	1d00c1	SCSI_TARG_5	1d0045	Fabric_N5596UP-...	🟢	🟢

From: 20:00:00:11:0d:e5:fa:00 **To:** 20:01:00:11:0d:e5:fb:06

Name	1-Hour Average	Baseline
Average Read ECT Deviation	5.3157 %	
Average Write ECT Deviation	-0.1552 %	
Average Read ECT	0.0453 ms/IO	
Average Write ECT	0.0968 ms/IO	
Average Read DAL	0.0432 ms/IO	

Switch Interface: MDS9396T-174145 -> fc1/46

Name	Value (1-Hour)
In Errors	N/A
Out Errors	N/A
In Discards	N/A
Out Discards	N/A
Tx	N/A

This page provides the basis for Insights data visualization showing counter data, visual topology map with indicators on the map. Also, you can view analytical information and historical insights. From Cisco DCNM Release 11.3(1), you can choose the data type to stream SAN Insights data. Select **SCSI** or **NVMe** to select the data type. The system time is displayed at the right corner of the window.

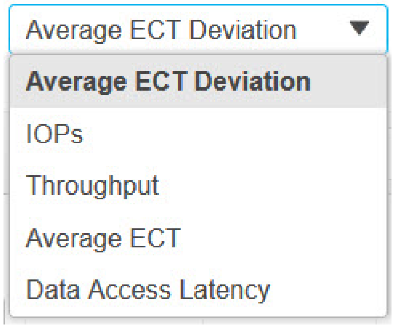
In **Monitor** > **SAN Insights** window, you can perform the tasks that are mentioned in the steps below.

The color of the status is arrived as an hourly average of Read and Write deviation for the respective Initiator Target Pairs.

Note Click the red status balls to **View SAN Insights Metrics** under the **Read (% dev)** or **Writer (% dev)** columns of the Initiator-target Pair table to navigate to the ECT Analysis page for more details on the respective Initiator-Target pair.

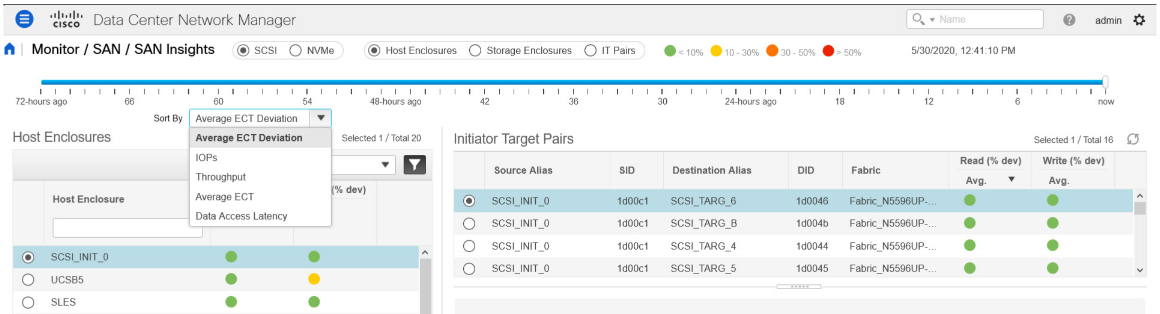
Step 2 View details about **Host Enclosure**, **Storage Enclosure**, or **IT Pairs**.

You can choose to view the enclosure details based on the average values as shown in the figure below. The Host Enclosures, Storage Enclosures, or IT-pairs can be filtered using the quick-filter functionality.



By default, the filter type **Average ECT Deviation** is selected. The Initiator target Pairs display the status of Read and Write deviation as colored status balls, upon which you can click to **View SAN Insights Metrics**. However, for all other filter types, the status of Read and Write percentage deviation is displayed in numerical format.

You can sort the Enclosures/IT-Pairs by Read/Write operation for the filtered metric. Click on the column headers to change the sorting. By default, it's sorted by Read operation.



Monitor / SAN / SAN Insights ◉ SCSI ○ NVMe ◉ Host Enclosures ○ Storage Enclosures ○ IT Pairs 🟢 < 10% 🟡 10 - 30% 🟠 30 - 50% 🔴 > 50% 5/30/2020, 12:41:10 PM

Sort By: Average ECT Deviation

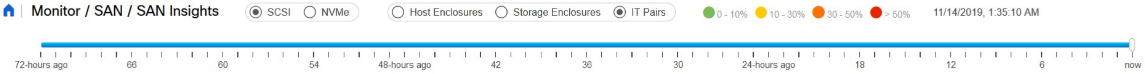
Host Enclosures Selected 1 / Total 20

	Host Enclosure		(% dev)
◉	SCSI_INIT_0	🟢	🟢
○	UCSB5	🟢	🟡
○	SLES	🟢	🟢

Initiator Target Pairs Selected 1 / Total 16

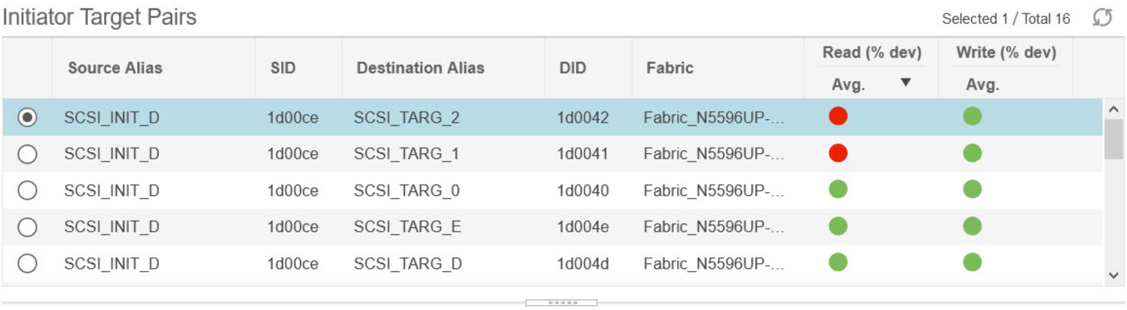
	Source Alias	SID	Destination Alias	DID	Fabric	Read (% dev) Avg.	Write (% dev) Avg.
◉	SCSI_INIT_0	1d00c1	SCSI_TARG_6	1d0046	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_0	1d00c1	SCSI_TARG_B	1d004b	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_0	1d00c1	SCSI_TARG_4	1d0044	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_0	1d00c1	SCSI_TARG_5	1d0045	Fabric_N5596UP-...	🟢	🟢

Step 3 Select time interval (such as now, 6-hours ago, 12-hours ago) to calculate status and fetch flow and port counters.



Monitor / SAN / SAN Insights ◉ SCSI ○ NVMe ○ Host Enclosures ○ Storage Enclosures ◉ IT Pairs 🟢 0 - 10% 🟡 10 - 30% 🟠 30 - 50% 🔴 > 50% 11/14/2019, 1:35:10 AM

Step 4 For each selected enclosure, view initiator target pair details such as Source Alias, SID, Destination Alias, DID, Fabric name, Read (% dev) and Writer (% dev).

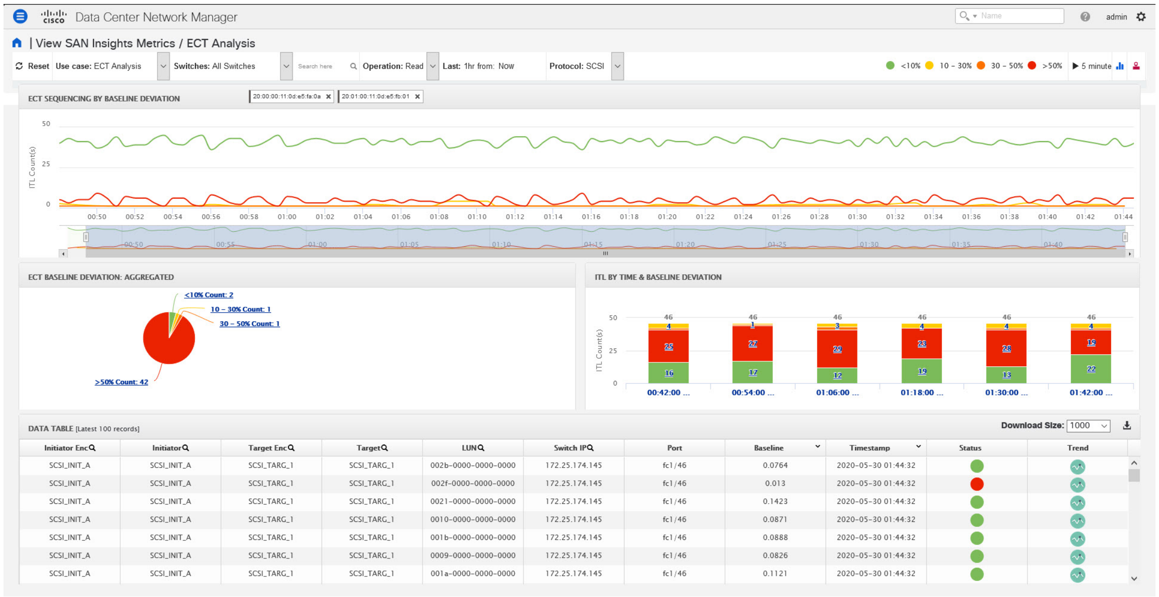


Initiator Target Pairs

Selected 1 / Total 16

	Source Alias	SID	Destination Alias	DID	Fabric	Read (% dev) Avg.	Write (% dev) Avg.
●	SCSI_INIT_D	1d00ce	SCSI_TARG_2	1d0042	Fabric_N5596UP-...	🔴	🟢
○	SCSI_INIT_D	1d00ce	SCSI_TARG_1	1d0041	Fabric_N5596UP-...	🔴	🟢
○	SCSI_INIT_D	1d00ce	SCSI_TARG_0	1d0040	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_D	1d00ce	SCSI_TARG_E	1d004e	Fabric_N5596UP-...	🟢	🟢
○	SCSI_INIT_D	1d00ce	SCSI_TARG_D	1d004d	Fabric_N5596UP-...	🟢	🟢

You can click the Status circle icon under **Read (% dev)** or **Writer (% dev)** columns in the **Initiator-target Pair** table to navigate to the ECT Analysis window, with corresponding Initiator and Target WWPNs prefiltered.



Data Center Network Manager

| View SAN Insights Metrics / ECT Analysis

Reset **Use case:** ECT Analysis **Switches:** All Switches **Operation:** Read **Last:** 1hr from: Now **Protocol:** SCSI

ECT SEQUENCING BY BASELINE DEVIATION

20:00:00:11:0d:e5:fa:0a
20:01:00:11:0d:e5:fb:01

ECT BASELINE DEVIATION: AGGREGATED

ITL BY TIME & BASELINE DEVIATION

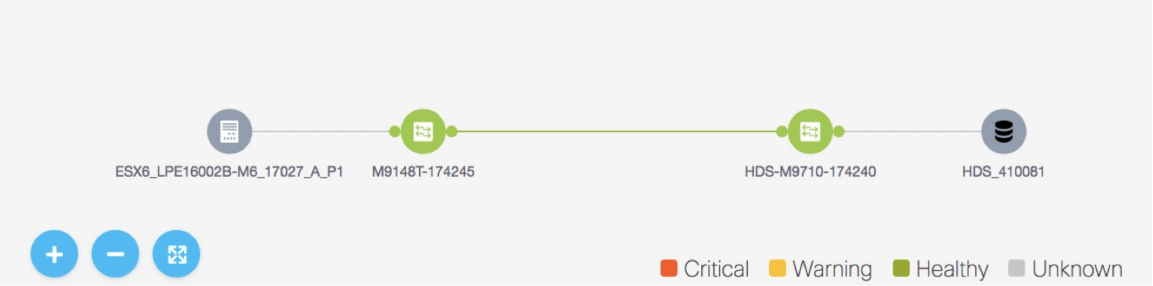
DATA TABLE [Latest 100 records]

Download Size: 1000

Initiator Enc	Initiator	Target Enc	Target	LUN	Switch IP	Port	Baseline	Timestamp	Status	Trend
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002b-0000-0000-0000	172.25.174.145	fc1/46	0.0764	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	002f-0000-0000-0000	172.25.174.145	fc1/46	0.013	2020-05-30 01:44:32	🔴	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0021-0000-0000-0000	172.25.174.145	fc1/46	0.1423	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0010-0000-0000-0000	172.25.174.145	fc1/46	0.0871	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	001b-0000-0000-0000	172.25.174.145	fc1/46	0.0888	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	0009-0000-0000-0000	172.25.174.145	fc1/46	0.0826	2020-05-30 01:44:32	🟢	
SCSI_INIT_A	SCSI_INIT_A	SCSI_TARG_1	SCSI_TARG_1	001a-0000-0000-0000	172.25.174.145	fc1/46	0.1121	2020-05-30 01:44:32	🟢	

Step 5 Use the map to view end-to-end connectivity from initiator to target. Host, storage, and switch have colored status indications. The color codes in the Topology area are only for the switch status. The switch color is governed by the Health score calculated for each switch. Double click on the colored switch icons to view the switch overlay for more details.

The switch interfaces also have status indications. The switch interface is rendered as a small circle at the end of the link that is attached to the switch. Selecting a switch interface populates one of the counter tables. Map displays latest connectivity (not affected by time slider setting).



Step 6 View counter data for the selected flow and switch interface.

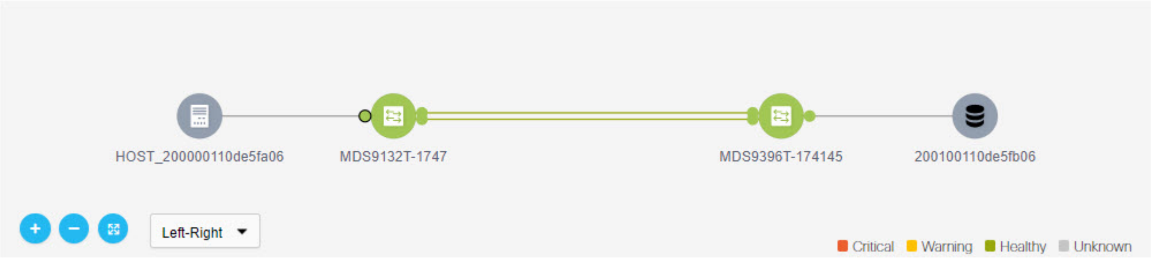
The data in the **Switch Interface** table is populated from Performance Monitoring and Slow Drain. You must enable Performance Monitoring for the fabric and schedule Slow Drain jobs. This table shows **NA**, otherwise.

To enable Performance Monitoring, choose **Administration** > **Performance Setup** > **SAN Collections**. Select the Fabric to monitor. Select all the parameter check boxes against the Fabric. Click **Apply** to begin Performance Monitoring.

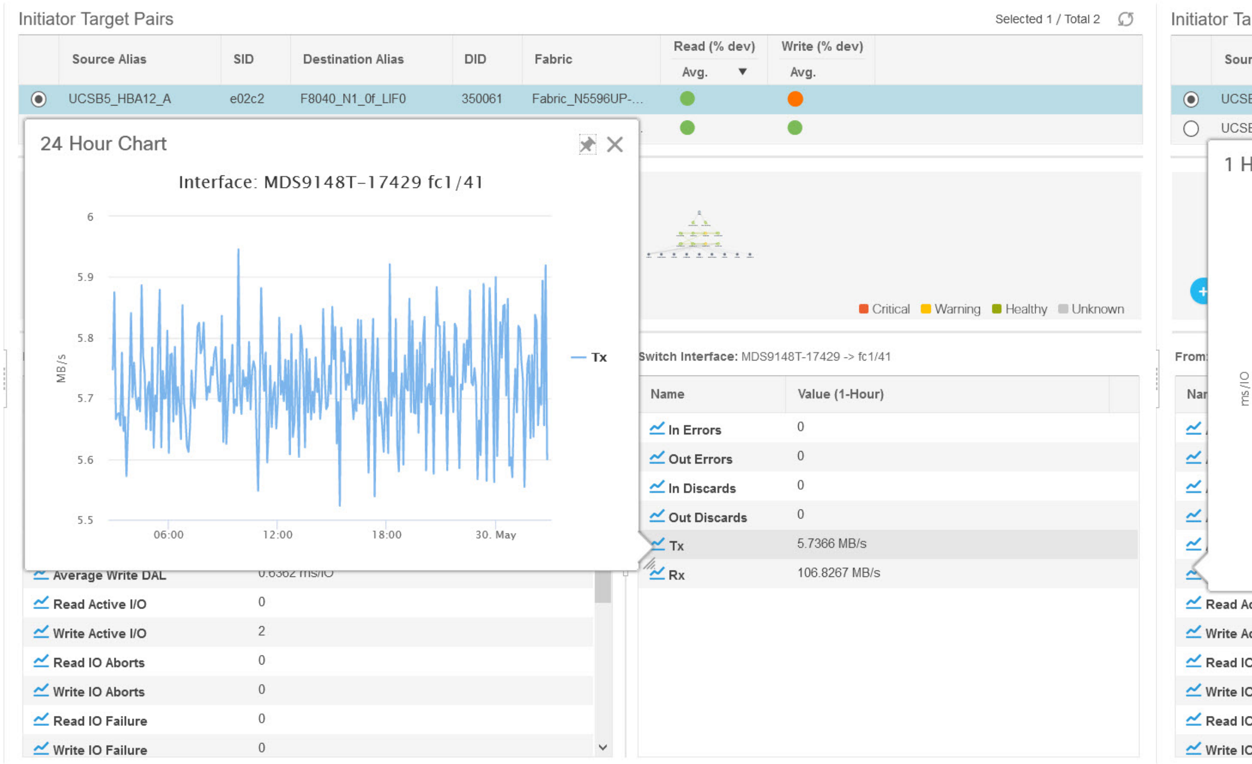
To enable Slow Drain metrics, choose **Monitor** > **SAN** > **Slow Drain Analysis**. Configure a current job on the Fabric. On the **Monitoring SAN Insights**, click the interface on the map. The **Slow Drain Metrics** is displayed in the Switch Interface table.

- Select the IT flow to display the topology and the flow metrics from the switch telemetry infrastructure in the bottom-left table.

  Select the specific interface in the topology view to display interface metrics from port-monitoring infrastructure. Beginning from Release 11.4(1), the interface corresponding the enclosure/IT pair selected is selected by default.



Step 7 On the Flow table and the Switch Interface tables, click on 📈 icon to view the 24-hour chart.



Initiator Target Pairs

Selected 1 / Total 2

	Source Alias	SID	Destination Alias	DID	Fabric	Read (% dev)	Write (% dev)
						Avg. ▼	Avg.
◉	UCSB5_HBA12_A	e02c2	F8040_N1_0f_LIF0	350061	Fabric_N5596UP-...	●	●
						●	●

24 Hour Chart

Interface: MDS9148T-17429 fc1/41

Name	Value
Average Write DAL	0.6362 ms/IO
Read Active I/O	0
Write Active I/O	2
Read IO Aborts	0
Write IO Aborts	0
Read IO Failure	0
Write IO Failure	0

Switch Interface: MDS9148T-17429 -> fc1/41

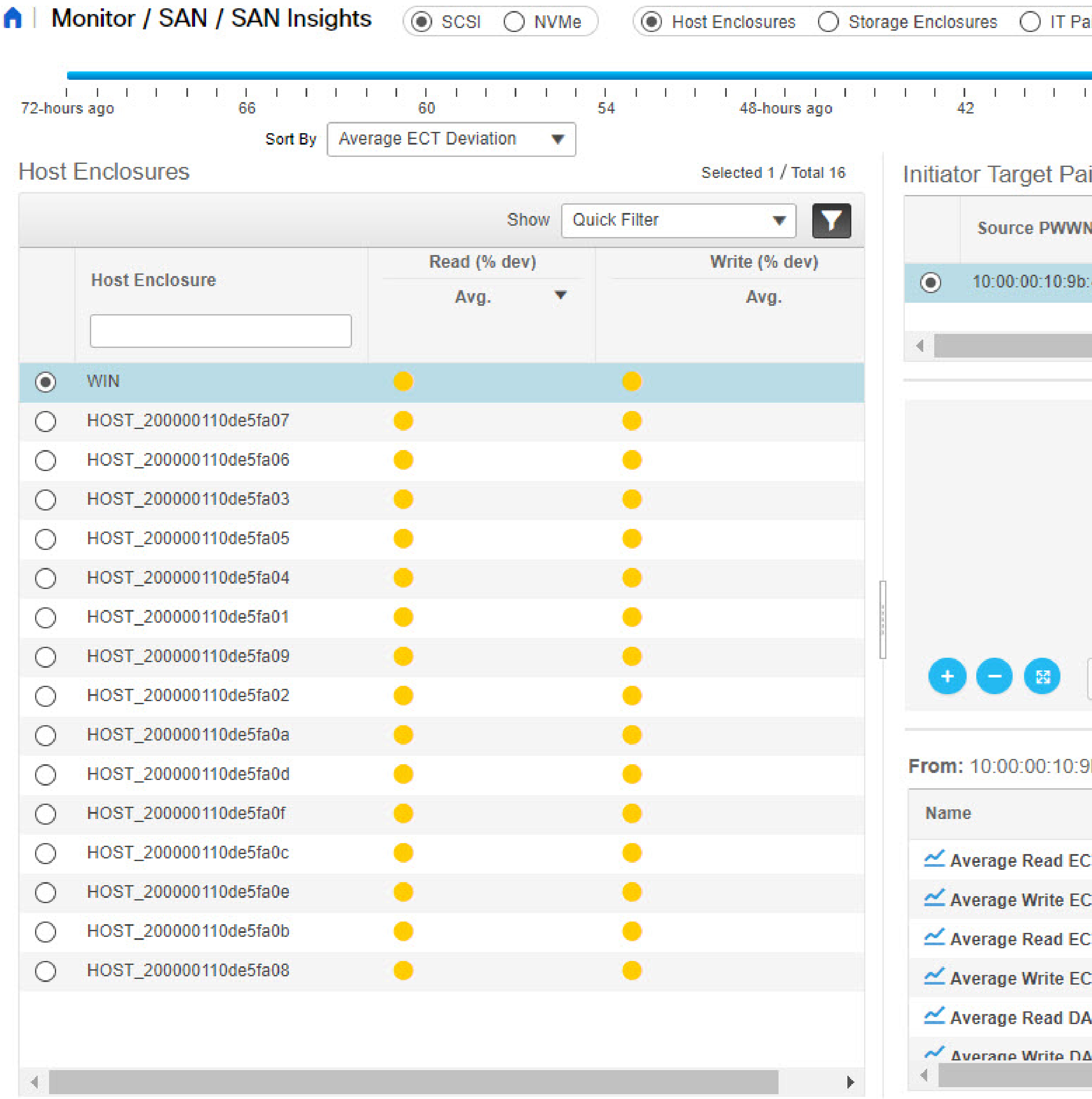
Name	Value (1-Hour)
In Errors	0
Out Errors	0
In Discards	0
Out Discards	0
Tx	5.7366 MB/s
Rx	106.8267 MB/s

Viewing Host Enclosures

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

To view the Host Enclosures from the Cisco DCNM Web UI, perform the following steps:

1. Choose **Monitor** > **SAN** > **SAN Insights**, and then choose **Host Enclosure**.



Monitor / SAN / SAN Insights ● SCSI ○ NVMe ● Host Enclosures ○ Storage Enclosures ○ IT Pa

Sort By: Average ECT Deviation

Host Enclosures — Selected 1 / Total 16

Show: Quick Filter

	Host Enclosure	Read (% dev) Avg.	Write (% dev) Avg.
●	WIN	●	●
○	HOST_200000110de5fa07	●	●
○	HOST_200000110de5fa06	●	●
○	HOST_200000110de5fa03	●	●
○	HOST_200000110de5fa05	●	●
○	HOST_200000110de5fa04	●	●
○	HOST_200000110de5fa01	●	●
○	HOST_200000110de5fa09	●	●
○	HOST_200000110de5fa02	●	●
○	HOST_200000110de5fa0a	●	●
○	HOST_200000110de5fa0d	●	●
○	HOST_200000110de5fa0f	●	●
○	HOST_200000110de5fa0c	●	●
○	HOST_200000110de5fa0e	●	●
○	HOST_200000110de5fa0b	●	●
○	HOST_200000110de5fa08	●	●

Initiator Target Pai

	Source PWWN
●	10:00:00:10:9b:

From: 10:00:00:10:9

Name
Average Read EC
Average Write EC
Average Read EC
Average Write EC
Average Read DA
Average Write DA

2. Specify a time interval using the time slider.

3. Select a host from the **Host Enclosures** table, which lists all the host enclosures.

4. Select one initiator-target pair from the **Initiator Target Pairs** table.

   This table lists all the initiator-target pairs for the selected host. The flow table shows the details of all metrics on ECT/DAL/read/write times, active I/Os, aborts, failures etc. along with their 1-hour average and the baseline information.

5. Select a switch interface from the topology map.

From Release 11.4(1), the switch interface is picked and selected by default. The **Switch Interface** table displays data for the last hour period selected for the selected interface. The switch name and the interface name are displayed on top of the switch interface table.

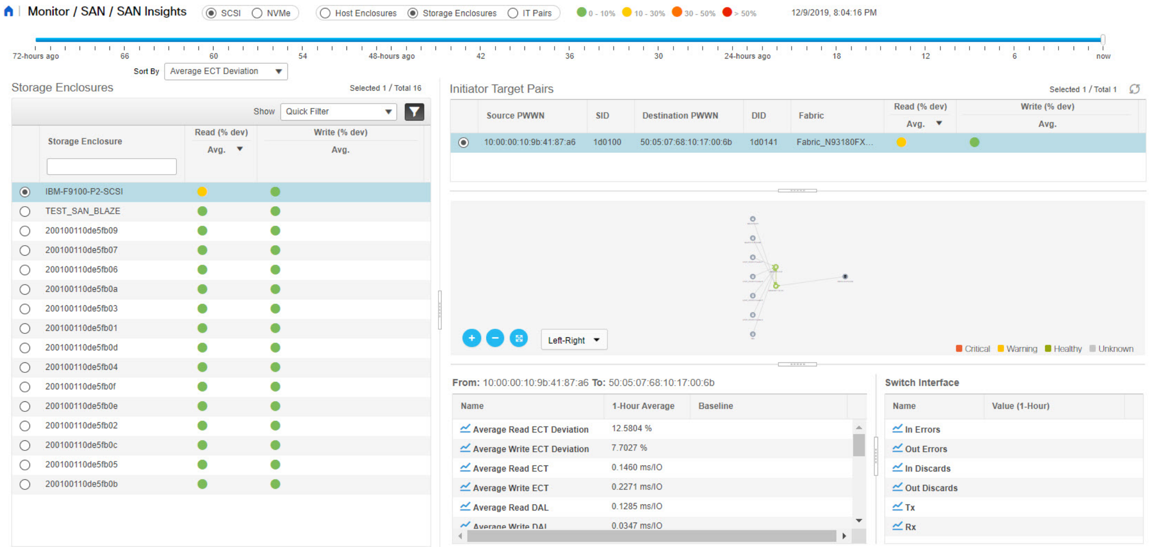
6. Click on the Status circle icon under **Read (% dev)** or **Write (% dev)** columns in the **Initiator-target Pair** table to navigate to the ECT Analysis window, with corresponding Initiator and Target WWPNs prefiltered.

Viewing Storage Enclosures

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

To view the Storage Enclosures from the Cisco DCNM Web UI, perform the following steps:

1. Choose **Monitor** > **SAN** > **SAN Insights**, and then choose **Storage Enclosure**.



● SCSI ○ NVMe

○ Host Enclosures ● Storage Enclosures ○ IT Pairs

12/9/2019, 8:04:16 PM

Sort By: Average ECT Deviation

Storage Enclosures — Selected 1 / Total 16

	Storage Enclosure	Read (% dev) Avg.	Write (% dev) Avg.
●	IBM-F9100-P2-SCSI	●	●
○	TEST_SAN_BLAZE	●	●
○	200100110de5fb09	●	●
○	200100110de5fb07	●	●
○	200100110de5fb06	●	●
○	200100110de5fb0a	●	●
○	200100110de5fb03	●	●
○	200100110de5fb01	●	●
○	200100110de5fb0d	●	●
○	200100110de5fb04	●	●
○	200100110de5fb0f	●	●
○	200100110de5fb0e	●	●
○	200100110de5fb02	●	●
○	200100110de5fb0c	●	●
○	200100110de5fb05	●	●
○	200100110de5fb0b	●	●

Initiator Target Pairs — Selected 1 / Total 1

	Source PWWN	SID	Destination PWWN	DID	Fabric	Read (% dev) Avg.	Write (% dev) Avg.
●	10:00:00:10:9b:41:87:a6	1d0100	50:05:07:68:10:17:00:6b	1d0141	Fabric_N93180FX...	●	●

From: 10:00:00:10:9b:41:87:a6 **To:** 50:05:07:68:10:17:00:6b

Name	1-Hour Average	Baseline
Average Read ECT Deviation	12.5804 %	
Average Write ECT Deviation	7.7027 %	
Average Read ECT	0.1460 ms/IO	
Average Write ECT	0.2271 ms/IO	
Average Read DAL	0.1285 ms/IO	
Average Write DAL	0.0347 ms/IO	

Switch Interface

Name	Value (1-Hour)
In Errors	
Out Errors	
In Discards	
Out Discards	
Tx	
Rx	

2. Specify a time interval using the time slider.

3. Select a storage enclosure from the **Storage Enclosures** table.

4. Select an initiator-target pair from the **Initiator Target Pairs** table.

5. Click on the Status circle icon under **Read (% dev)** or **Write (% dev)** columns in the **Initiator-target Pair** table to navigate to the ECT Analysis window, with corresponding Initiator and Target WWPNs prefiltered.

6. View the topology map represented for the selected initiator-target pair and the flow metrics.

   The flow metrics are displayed in the flow table.

7. Select a switch interface from the topology map.

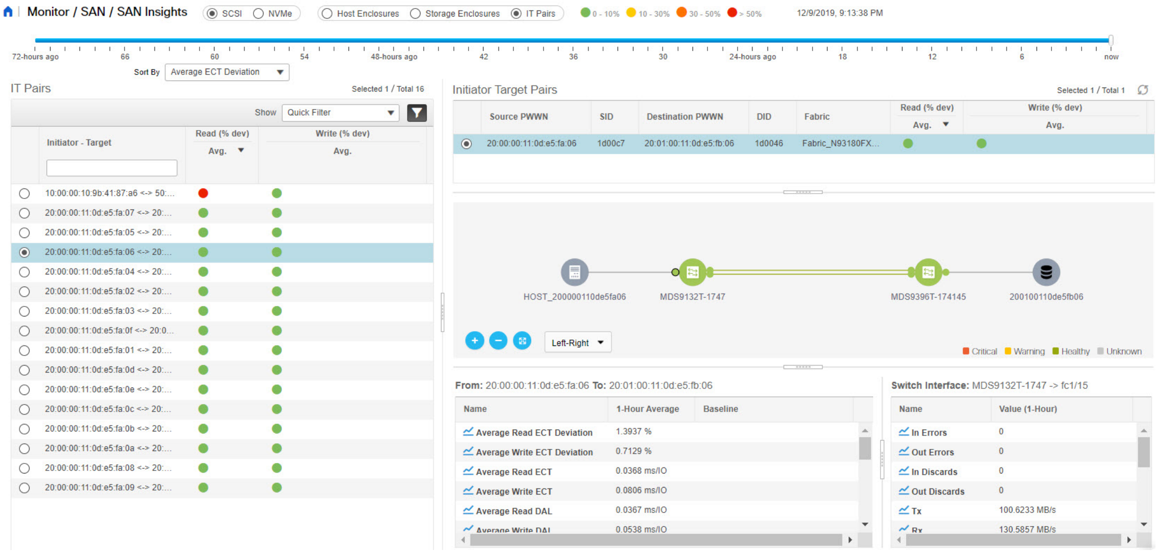
   The **Switch Interface** table displays data for the selected interface. From Release 11.4(1), the switch interface is picked and selected by default.

Viewing IT Pairs

From Release 11.3(1), Cisco DCNM allows you to view SAN Insights metrics based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Administration** > **DCNM Server** > **Server Properties**. Ensure that you restart the SAN Insights service to use the new properties. (Restart the SanInsight service on Linux or Pause/Resume Post Processor App on SAN-OVA/ISO/SE deployments)

To view the IT Pairs from the Cisco DCNM Web UI, perform the following steps:

1. Choose **Monitor** > **SAN** > **SAN Insights**, and then choose **IT Pairs**.



	Initiator - Target	Read (% dev) Avg.	Write (% dev) Avg.
○	10:00:00:10:9b:41:87:a6 <-> 50:...	●	●
○	20:00:00:11:0d:e5:fa:07 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:05 <-> 20:...	●	●
◉	20:00:00:11:0d:e5:fa:06 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:04 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:02 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:03 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:0f <-> 20:0...	●	●
○	20:00:00:11:0d:e5:fa:01 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:0d <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:0e <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:0c <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:0b <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:0a <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:08 <-> 20:...	●	●
○	20:00:00:11:0d:e5:fa:09 <-> 20:...	●	●

	Source PWWN	SID	Destination PWWN	DID	Fabric	Read (% dev) Avg.	Write (% dev) Avg.
◉	20:00:00:11:0d:e5:fa:06	1d00c7	20:01:00:11:0d:e5:fb:06	1d0046	Fabric_N93180FX...	●	●

From: 20:00:00:11:0d:e5:fa:06 **To:** 20:01:00:11:0d:e5:fb:06

Name	1-Hour Average	Baseline
Average Read ECT Deviation	1.3937 %	
Average Write ECT Deviation	0.7129 %	
Average Read ECT	0.0368 ms/IO	
Average Write ECT	0.0806 ms/IO	
Average Read DAL	0.0367 ms/IO	
Average Write DAL	0.0538 ms/IO	

Switch Interface: MDS9132T-1747 -> fc1/15

Name	Value (1-Hour)
In Errors	0
Out Errors	0
In Discards	0
Out Discards	0
Tx	100.6233 MB/s
Rx	130.5857 MB/s

2. Specify a time interval using the time slider.

3. Choose a flow from the **IT Pairs** table.

   The initiator-target pairs are listed in the **Initiator Target Pairs** table, the topology map is represented for the selected I-T pair. The flow metrics are displayed in the IT Pairs table.

4. The flow table in this window shows details about all metrics on ECT/DAL/read/write times, active I/Os, aborts, failures, and so on.

   Also, the flow table shows 1-hour average and the baseline information.

5. Click the status ball in the **Initiator Target Pairs** table.

   24-hour normalized R/W ECT deviation chart is displayed for the selected IT-pair.

6. Select a switch interface from the topology map.

   The **Switch Interface** table displays data for the selected interface.

Monitoring LAN

The LAN menu includes the following submenus:

Monitoring Performance Information for Ethernet

To monitor the performance information for ethernet from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **LAN** > **Ethernet**.

The **Ethernet** window is displayed.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the name of an Ethernet port from the **Name** column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save**.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict**, and **Do not interpolate data**.

  Note Set the **pmchart.doInterpolate** property in the **Server Properties** window to false to use the **Do not interpolate data** option.

- For the Rx/Tx calculation, see the following Rx/Tx calculation.

  Note The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

  - Average Rx/Tx % = Average Rx/Tx divided by Speed * 100
  - Peak Rx/Tx % = Peak Rx/Tx divided by Speed * 100

Note If the performance tables do not contain any data, see the Thresholds section to turn on performance data collection.

Note To change traffic display unit from bytes to bits, From Cisco DCNM Web UI, choose **Administration** > **DCNM Server** > **Server Properties**, enter value as true for **pm.showTrafficUnitAsbit** property, and click **Apply Changes**.

Monitoring ISL Traffic and Errors

To monitor the ISL traffic and errors from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **LAN** > **Link**.

The **ISL Traffic and Errors** window is displayed. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

Note **NaN** (Not a Number) in the data grid means that the data is not available.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict**, and **Do not interpolate data**.

  Note Set the **pmchart.doInterpolate** property in the **Server Properties** window to false to use the **Do not interpolate data** option.

- To export the data into a spreadsheet, choose **Export** from the drop-down list in the **Chart** menu and then click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation.

  Note The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

  - Average Rx/Tx % = Average Rx/Tx divided by Speed * 100
  - Peak Rx/Tx % = Peak Rx/Tx divided by Speed * 100

Note If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

Monitoring a vPC

The virtual port channel (vPC) feature enables you to view the links that are physically connected to different devices as a single port channel. A vPC is an extended form of a port channel which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. Traffic is distributed among two single device vPC endpoints. If there is an inconsistency in the vPC configurations, the vPC does not function correctly.

Note To view the vPC in **vPC Performance**, both primary and secondary device should be designated to the user. If either one kind of switch is not designated, vPC information is isplayed.

Cisco DCNM **Web Client** > **Monitor> vPC** displays only consistent vPCs displays both the consistent and inconsistent vPCs.

You can identify the inconsistent vPCs and resolve the inconsistencies in each vPC by using the Cisco DCNM **Web UI** > **Configure** > **Deploy** > **vPC Peer** and **Web Client** > **Configure** > **Deploy** > **vPC**.

Table 10: vPC Performance, on page 117 displays the following vPC configuration details in the data grid view.

Table 10: vPC Performance

Column	Description
Search box	Enter any string to filter the entries in their respective column.
vPC ID	Displays vPC ID's configured device.
Domain ID	Displays the domain ID of the vPC peer switches.
Multi Chassis vPC EndPoints	Displays the multi-chassis vPC endpoints for each vPC ID under a vPC domain.
Primary vPC Peer - Device Name	Displays the vPC Primary device name.
Primary vPC Peer - Primary vPC Interface	Displays the primary vPC interface.
Primary vPC Peer - Capacity	Displays the capacity for the primary vPC peer.
Primary vPC Peer - Avg. Rx/sec	Displays the average receiving speed of primary vPC peer.
Primary vPC Peer - Avg. Tx/sec	Displays the average sending speed of primary vPC peer.
Primary vPC Peer - Peak Util%	Displays the peak utilization percentage of primary vPC peer.
Secondary vPC Peer - Device Name	Displays the vPC secondary device name.
Secondary vPC Interface	Displays the secondary vPC interface.
Secondary vPC Peer - Capacity	Displays the capacity for the secondary vPC peer.
Secondary vPC Peer - Avg. Rx/sec	Displays the average receiving speed of secondary vPC peer.
Secondary vPC Peer - Avg. Tx/sec	Displays the average sending speed of secondary vPC peer.
Secondary vPC Peer - Peak Util%	Displays the peak utilization percentage of secondary vPC peer.

You can use this feature as following:

Monitoring vPC Performance

You can view the relationship among consistent virtual port channels (vPCs). You can view the statistics of all member interfaces and the aggregate of the statistics at the port-channel level.

Note This tab only displays consistent vPCs.

To view the VPC performance information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > vPC**.

The **vPC Performance** statistics is displayed. The aggregated statistics of all vPCs are displayed in a tabular manner.

Step 2 Click the **vPC ID**.

The vPC topology, **vPC Details**, **Peer-link Details**, and **Peer-link Status** are displayed.

The **vPC Consistency**, **Peer-link Consistency**, and **vPC Type2 Consistency** for the vPC are displayed.

- Click the **vPC Details** tab, you can view the parameter details of vPC **Basic Setting** and **Layer 2 Settings** for both Primary and Secondary vPC devices.
- Click the **Peer-link Details** tab, to view the parameter details of peer-link **vPC Global Setting** and **STP Global Settings** for both Primary and Secondary vPC devices.
- Click the **Peer-link Status** tab, the **vPC Consistency**, and **Peer-Link Consistency** status is displayed. The parameter details of **Role Status** and **vPC Peer keep-alive Status** for both Primary and Secondary vPC devices is also displayed.

Step 3 Click the peer-link icon in front of the **Device Name** in the **Primary vPC peer** or **Secondary vPC peer** column to view its member interface.

Step 4 Click the **Show Chart** icon of the corresponding interface to view its historical statistics.

The traffic distribution statistics appear at the bottom of the vPC window. By default, the Cisco DCNM Web Client displays the historical statistics for 24 hours.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for flows:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to **Append**, **Predict**, and **Do not interpolate data**.

Note Set the **pmchart.doInterpolate** property in the **Server Properties** window to false to use the **Do not interpolate data** option.

- To print the vPC Utilization data, click the **Print** icon in the upper-right corner. The vPC Utilization page appears.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save File**.

Note If the performance tables do not contain any data, see the Thresholds section to turn on performance data collection.

Monitoring Report

The Report menu includes the following submenus:

Viewing Reports

You can view the saved reports that are based on the following selection options:

- **By Template**
- **By User**
- From the menu bar, select **Monitor** > **Report** > **View**.

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

Procedure

Step 1 In the left pane, expand **By Template** or **By User** folder.

Step 2 Select the report that you wish to view.

You can view the report in the main screen or you can select the report in the **Report** column to view the HTML version of the report in a new browser.

Step 3 To delete a specific report, select the check box and click the **Delete** icon.

Step 4 To delete all reports, check the check box in the header, and click the **Delete** icon.

Note If you have multiple fabrics, you can select the DCNM-SAN group in the Scope to view Host to Storage connectivity of multiple fabrics in a single report.

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device hostname, number of faulty modules, and the module number with its PID.
- The information for the device of the module. The table contains details about the tests failed.

Generating a Report

You can generate reports that are based on a selected template or you can schedule the report to run at a specified time.

Procedure

Step 1 From the menu bar, select **Monitor** > **Report** > **Generate**.

You see the **Generate Report** window.

Step 2 In the configuration window, use the drop-down to define the scope for report generation.

In the **Scope** drop-down, you can select a scope group with dual fabrics, the traffic data that is generated by hosts and storage end devices are displayed side by side which enables you to view and compare traffic data that is generated on dual fabrics. To view this report, in the **Other Predefined** folder, select **Traffic by VSAN** (Dual Fabrics). Click Options to select the **Device Type** and **Fabrics**. Click **Save** to save the configuration.

Step 3 In the pane on the left, expand the folders and select the report.

Step 4 (Optional) In the pane on the right, you can edit the **Report Name**.

Step 5 (Optional) Check the **Export to Csv/Excel** check box to export the report to a Microsoft Excel spreadsheet.

Step 6 In the **Repeat** radio buttons, if you select:

- **Never** - The report is generated only during the current session.
- **Once** - The report is generated on a specified date and time apart from the current session.
- **Daily** - The report is generated everyday based on the Start and End date at a specified time.
- **Weekly** - The report is generated once a week based on the Start and End date at a specified time.
- **Monthly** - The report is generated once every month based on the Start and End date at a specified time.

When you generate a report for Network Configuration Audit, the daily job generates a report for the selected devices for last one day. Similarly, the weekly job generates a report for the last 7 days, and the monthly job generates a report for the last 30 days.

Step 7 Click the **Create** button to generate a report that is based on the specifications.

You see the report results in a new browser window.

Alternatively, you can view the report by choosing **Monitor** > **Report** > **View** and selecting the report name from the report template that you used in the navigation pane.

Note The **Start Date** must be at least five minutes earlier than the **End Date**.

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device hostname, number of faulty modules and the module number with its PID.
- A detailed information for the device of the module. The table contains details about the tests failed.

Creating SAN User Defined Reports

You can create custom reports from all or any subset of information that is obtained by Cisco DCNM-SAN. You create a report template by selecting events, performance, and inventory statistics you want in your report and set the desired SAN, fabrics, or VSAN to limit the scope of the template. You can generate and schedule a report of your fabric that is based on this template immediately or later. Cisco DCNM Web Client saves each report, which is generated based on the report template, and the time you generate the report.

Since the Cisco MDS NX-OS Release 5.0, the report template design has changed to resolve the limitations of the earlier versions. With the new design model, you can perform add, delete, and modify functionalities on a single page. You can choose multiple fabrics and VSANs using the new navigation system, which allows you to add new items and categories in the future.

The new design model has three panels:

- **Template** panel - The **Template** panel allows you to add new templates, modify existing templates and delete existing templates.
- **Configuration** panel - The **Configuration** panel allows you to configure a new template when it is added, and modify an existing template. The options in the configuration panel are disabled until you either add a new template or select an existing template. The upper portion of the configuration panel contains many categories that you can choose and configure.
- **User Selection** panel - The **User Selection** panel displays your configuration options in real time. While the configuration panel can display information pertaining to one category at a time, the **User Selection** panel displays all of your selections or configurations.

To create custom reports from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Report > User Defined**.

The **Create User-Defined** window is displayed.

Step 2 In the **Template** panel, under the **Name** column, select **CLICK TO ADD NEW CUSTOM** to edit the **Name** of the new report.

Step 3 In the **Configuration** panel, click **Scope** to define scope of the report. The default scope includes Data Center, SAN, LAN, and Fabric configurations.

Step 4 Click **Inventory** and use the checkbox to select the inventory information that is required in the report. You can also use the drop-down to filter by selecting the Top performance and the timeline that is required in the report.

Step 5 Click **Performance** and use the checkbox to select the performance information required in the report.

Step 6 Click **Health** and use the checkbox to select the health information required in the report.

Step 7 Click **Save** to save this report template.

A confirmation message is displayed confirming that the report is saved.

Deleting a Report Template

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

Procedure

Step 1 In the **Template** panel, select the report template that you want to delete.

Step 2 Click the **Delete** icon to delete the report.

Step 3 In the confirmation pop-up, click **Yes** to delete the template.

Modifying a Custom Report Template

Procedure

Step 1 Choose **Monitor > Report > User Defined**.

You see the **Template**, **Configuration**, and **User Selection** panels.

Step 2 Select a report from the **Template** panel.

You see the current information about this report in the **User Selection** panel.

Step 3 Modify the information in the **Configuration** panel.

Step 4 Click **Save** to save the report template.

A confirmation message is displayed confirming that the report is saved.

Note You cannot change the scope for an existing report. Generate a new report for a new scope.

Viewing Scheduled Jobs Based on a Report Template

To view the scheduled jobs that are based on a report template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Report > Jobs**.

The **Report Jobs** window is displayed with details of the reports that are scheduled for generation along with its status.

Step 2 Select the checkbox for a specific report and click the **Delete** Job icon to delete a report.

Alarms

The Alarms menu includes the following submenus:

Viewing Alarms and Events

You can view the alarms, cleared alarms, and events.

Procedure

Step 1 Choose **Monitor** > **Alarms** > **View**.

Step 2 Choose any of the following tabs.

- **Alarms**: This tab displays the alarms that are generated for various categories. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Last Updated (optional), Policy, and Message. You can specify the **Refresh Interval** in this tab. You can select one or more alarms and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete them.
- **Cleared Alarms**: This tab displays the cleared alarms. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Cleared At (optional), Cleared By, Policy, and Message. You can select one or more alarms and then click the **Delete** button to delete them.
- **Events**: This tab displays the events that are generated for the switches. This tab displays information such as **Ack**, **Acknowledged user**, **Group**, **Switch**, **Severity**, **Facility**, **Type**, **Count**, **Last Seen**, and **Description**. You can select one or more events and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete them. If you want to delete all events, click the **Delete All** button.

Monitoring and Adding Alarm Policies

Note

- Alarm policies are stored in compute nodes. Therefore, run the **appmgr backup** command on each compute node in addition to taking a backup of DCNM.
- In case the **Monitor>Alarms>Policies** window was open while migrating the Performance Manager data, the alarm index may get deleted. In such scenarios, restart the DCNM server for the alarm policies to work as expected.

In Cisco DCNM SAN Federation deployment on Windows and Linux, ensure that the **alarm.enable.external** value in the Server Properties is set to true on both the Primary and Secondary nodes. Navigate to **Administration** > **DCNM Server** > **Server Properties**. Locate the **alarm.enable.external** field, and ensure that it is set to **true**. You must restart DCNM Server to bring this into effect.

You can forward alarms to registered SNMP listeners in DCNM. From Cisco DCNM web UI, choose **Administration** > **DCNM Server** > **Server Properties**, enter an external port address in **alarm.trap.listener.address** field, click **Apply Changes,** and restart DCNM services.

Note Ensure that you select **Forwarding** check box in **Alarm Policy creation** dialog window to enable forwarding alarms to external SNMP listener.

You can add alarm policies for the following:

- **Device Health**: Device health policies enable you to create alarms when Device ICMP Unreachable, Device SNMP Unreachable, or Device SSH Unreachable. Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.
- **Interface Health**: Interface health policies enable you to monitor Up or Down, Packet Discard, Error, Bandwidth details of the interfaces. By default all interfaces are selected for monitoring.
- **Syslog Alarm**: Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one which clears the alarm.

Procedure

Step 1 Choose **Monitor** > **Alarms** > **Alarm Policies**.

Step 2 Select the **Enable Alarms** check box to enable alarm policies.

Step 3 From the **Add** drop-down list, choose any of the following:

- Device Health Policy: Select the devices for which you want to create policies. Specify the policy name, description, CPU Utilization parameters, Memory Utilization parameters, Environment Temperature parameters, device availability, and device features. Under **Device Features**, you can select the BFD, BGP, and HSRP protocols. When these check boxes are selected, alarms are triggered for the following traps: **BFD**- ciscoBfdSessDown, ciscoBfdSessUp, **BGP**- bgpEstablishedNotification, bgpBackwardTransNotification, cbgpPeer2BackwardTransition (), cbgpPeer2EstablishedNotification, and **HSRP**- cHsrpStateChange. Please refer https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en for detailed trap OID definition.
- Interface Health Policy: Select the devices for which you want to create policies. Specify the policy name, description, link-state, Bandwidth (In/Out), Inbound errors, Outbound errors, Inbound Discards, and Outbound Discards.
- Syslog Alarm Policy: Select the devices for which you want to create policies and then specify the following parameters.
  - Devices: Define the scope of this policy. Select individual devices or all devices to apply this policy.
  - Policy Name: Specify the name for this policy. It must be unique.
  - Description: Specify a brief description for this policy.
  - Severity: Define the severity level for this syslog alarm policy. Choices are: Critical, Major, Minor, and Warning.
  - Identifier: Specify the identifier portions of the raise & clear messages.
  - Raise Regex: Define the format of a syslog raise message. The syntax is as follows: **Facility-Severity-Type: Message**

- Clear Regex: Define the format of a syslog clear message. The syntax is as follows:
  Facility-Severity-Type: Message

The Regex definitions are simple expressions but not a complete regex. Variable regions of text are noted using $(LABEL) syntax. Each label represents a regex capture group (.+), which corresponds to one or more characters. The variable texts found in both raise and clear messages are used to associate the two messages. An Identifier is a sequence of one or more labels that appear in both messages. An Identifier is used to match a clear syslog message to the syslog message that raised the alarm. If the text appears only in one of the messages, it can be noted with a label and exclude it from the identifier.

Example: A policy with "Value": "ID1-ID2",

"syslogRaise": "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"

"syslogClear": "SVC-5-UP: $(ID1) module $(ID2) is up."

In the example, ID1 and ID2 labels can be marked as an identifier to find the alarm. This identifier will be found in corresponding syslog messages. Label “REASON” is in the raise but not in the clear message. This label can be excluded from the identifier, as it has no impact on the syslog message to clear the alarm.

Table 11: Example 1

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_ADMIN_UP: Interface Ethernet15/1 is admin up .
Clear Regex	ETHPORT-5-IF_DOWN_NONE: Interface Ethernet15/1 is down (Transceiver Absent)

In the above example, the regex expressions are part of the syslog messages that appear in the terminal monitor.

Table 12: Example 2

Identifier	ID1-ID2
Raise Regex	ETH_PORT_CHANNEL-5-PORT_DOWN: $(ID1): $(ID2) is down
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP: $(ID1): $(ID2) is up

Table 13: Example 3

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning cleared

Step 4 Click **OK** to add the policy.

Syslog Messages in Terminal Monitor and Console

The following examples show how the syslog messages appear in the terminal monitor and the console. The regex expression is matched with the part of the syslog messages after the % sign.

```
leaf-9516# terminal monitor
leaf-9516# conf t
leaf-9516(config)# int e15/1-32
leaf-9516(config-if-range)# no shut
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/1 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/1 is down (Transceiver Absent)
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/2 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/2 is down (Transceiver Absent)
2019 Aug 2 04:41:28 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/3 is admin up .
```

The syslog messages in the console have a similar format as they would appear in the terminal monitor, except for the additional port information enclosed in the %$ signs. However, the regex expression is matched with the part of the syslog messages after the last % sign.

```
SR-leaf1# 2019 Aug 26 23:55:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-
PFM_ALERT: FAN_BAD: fan6
2019 Aug 26 23:56:15 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:18 SR-leaf1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL:
System ready
2019 Aug 26 23:56:25 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:35 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully activated virtual service 'guestshell+'
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED:
The guest shell has been enabled. The command 'guestshell' may be used
to access it, 'guestshell destroy' to remove it.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FAN_REMOVED: Fan
module 5 (Serial number ) Fan5(sys_fan5) removed
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 2 minutes 0 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 1 minutes 40 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK:
Fan module 5 (Fan5(sys_fan5) fan) ok
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

Activating Policies

After you create new alarm policies, activate them.

Procedure

Step 1 Choose **Monitor** > **Alarms** > **Policies**.

Step 2 Select the policies that you want to activate and then click the **Activate** button.

Deactivating Policies

You can deactivate the active alarm policies.

Procedure

Step 1 Choose **Monitor** > **Alarms** > **Policies**.

Step 2 Select the policies that you want to deactivate and then click the **Deactivate** button.

Importing Policies

You can create alarm policies using the import functionality.

Procedure

Step 1 Choose **Monitor** > **Alarms** > **Policies** and then click the **Import** button.

Step 2 Browse and select the policy file saved on your computer.

You can only import policies in text format.

Exporting Policies

You can export the alarm policies into a text file.

Procedure

Step 1 From the menu bar, choose **Monitor** > **Alarms** > **Policies**.

Step 2 Click the **Export** button and then select a location on your computer to store the exported file.

Editing Policies

Procedure

Step 1 From the menu bar, choose **Monitor** > **Alarms** > **Policies**.

Step 2 Select the policy that you want to edit.

Step 3 Click the **Edit** button and then make necessary changes.

Step 4 Click the **OK** button.

Deleting Policies

Procedure

Step 1 From the menu bar, choose **Monitor** > **Alarms** > **Policies**.

Step 2 Select the policy that you want to delete.

Step 3 Click the **Delete** button. The policy is deleted.

Enabling External Alarms

You can enable external alarms using one of the following methods:

- Using Cisco DCNM Web UI
  1. From Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**.
  2. Locate the **alarm.enable.external** property.
  3. Enter the value in the field as **true**.
- Using REST APIs
  1. Go the API documentation URL from your DCNM setup: https://<*DCNM-ip*>/api-docs
  2. Navigate to the **Alarms** section.
  3. Click **POST** > **rest/alarms/enabledisableextalarm**.
  4. Choose the **body** parameter value as **true** from the **Value** drop-down list.
  5. Click **Try it out!**.
- Using CLI
  1. Log into the DCNM server using SSH.
  2. Set the **alarm.enable.external** property to **true** in the server.properties file.

     The filepath is `/usr/local/cisco/dcm/fm/config/server.properties`.

Health Monitor Alarms

Starting from Cisco DCNM Release 11.4(1), alarms are registered and created under the External alarm category by the Health Monitor.

Health Monitor: Alarm Policy

The Health Monitor external alarm category policy is automatically activated and enabled on all the devices in a fabric. The severity level of this alarm policy can be MINOR, MAJOR, or CRITICAL.

Alarms are raised and categorized as CRITICAL for the following events:

- Elasticsearch (ES) Cluster Status is Red: Critical (For Cluster/HA mode only)
- CPU/Memory/Disk Utilization/ES JVM Heap Used Percentage >= 90%

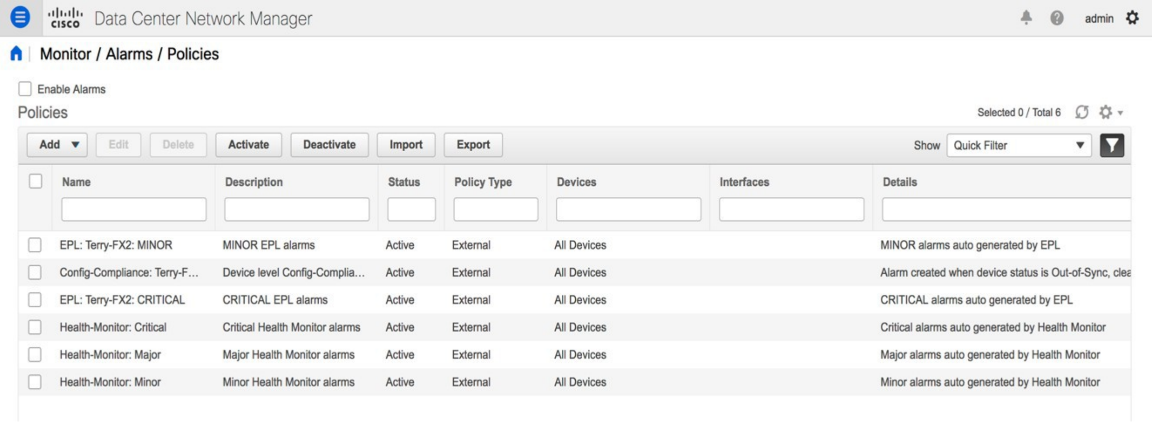
Alarms are raised and categorized as MAJOR for the following events:

- ES Cluster Status is Yellow (For Cluster/HA mode only)
- ES has unassigned shards (For Cluster/HA mode only)
- CPU/Memory/Disk Utilization/ES JVM Heap Used Percentage >= 80% and <90%

Alarms are raised and categorized as MINOR for the following events:

- CPU/Memory/Disk Utilization/ES JVM Heap Used Percentage >= 65% and <80%
- Kafka: Number of partitions without active leader > 0
- Kafka: Qualified partition leader not found. Unclear leaders > 0

Choose **Monitor>Alarms>Policies** to display the Health Monitor alarm policies. These alarm policies are not editable on the web UI. Click **Activate** or **Deactivate** to activate or deactivate the selected policy.



□ Enable Alarms

Policies

Selected 0 / Total 6

□	Name	Description	Status	Policy Type	Devices	Interfaces	Details
□	EPL: Terry-FX2: MINOR	MINOR EPL alarms	Active	External	All Devices		MINOR alarms auto generated by EPL
□	Config-Compliance: Terry-F...	Device level Config-Complia...	Active	External	All Devices		Alarm created when device status is Out-of-Sync, clea
□	EPL: Terry-FX2: CRITICAL	CRITICAL EPL alarms	Active	External	All Devices		CRITICAL alarms auto generated by EPL
□	Health-Monitor: Critical	Critical Health Monitor alarms	Active	External	All Devices		Critical alarms auto generated by Health Monitor
□	Health-Monitor: Major	Major Health Monitor alarms	Active	External	All Devices		Major alarms auto generated by Health Monitor
□	Health-Monitor: Minor	Minor Health Monitor alarms	Active	External	All Devices		Minor alarms auto generated by Health Monitor

In case an alarm policy is deactivated using the GUI, any alarms created or cleared for that policy will not be displayed in the **Monitor>Alarms>View** tab. To delete a policy, select the checkbox next to the policy and click **Delete**. However, we recommend not deleting a policy from the GUI. When a fabric is deleted, the alarm policy along with all the active alarms for the devices in that fabric are deleted.

Health Monitor: Active Alarms

Choose **Monitor>Alarms>View** to display the active alarms.

To clear active alarms, select the checkbox next to the alarm, click **Change Status** and select **Clear**.

To delete active alarms, select the checkbox next to the alarm and click **Delete**.

Health Monitor: Cleared Alarms

To view the cleared alarms, select **Monitor>Alarms>View>Cleared Alarms**.

Click the arrow icon ▶ to display detailed information about the required alarm.

To delete a cleared alarm from the list of cleared alarms, select the checkbox next to the alarm and click **Delete**.

For more information on Alarms and Policies, refer Alarms.

CHAPTER 6

Configure

This chapter contains the following topics:

Templates

The **Templates** menu includes the following option:

Template Library

Template Library includes the following tabs:

Template Library

You can add, edit, or delete templates that are configured across different Cisco Nexus and Cisco MDS platforms using Cisco DCNM Web client. From Cisco DCNM Web client home page, choose **Configure** > **Templates** > **Template Library** > **Templates**. The following parameters are displayed for each template that is configured on Cisco DCNM Web client. Templates support JavaScript. You can use the JavaScript function in a template to perform arithmetic operations and string manipulations in the template syntax.

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

Table 14: Templates Operations

Field	Description
Add Template	Allows you to add a new template.
Launch job creation wizard	Allows you to create jobs.
Modify/View Template	Allows you to view the template definition and modify as required.

Field	Description
Save Template As	Allows you to save the selected template in a different name. You can edit the template as required.
Delete Template	Allows you to delete a template
Import Template	Allows you to import a template from your local directory, one at a time.
Export template	Allows you to export the template configuration to a local directory location.
Import Template Zip File	Allows you to import `.zip` file, that contains more than one template that is bundled in a `.zip` format All the templates in the ZIP file are extracted and listed in the table as individual templates.

Note Notifications appear next to **Import Template Zip File** if there are issues while loading templates after restarting the server. Click the notifications to see the errors in the **Issues in loading Template** window. Templates with errors are not listed in the **Templates** window. To import these templates, correct the errors, and import them.

Table 15: Template Properties

Field	Description
Template Name	Displays the name of the configured template.
Template Description	Displays the description that is provided while configuring templates.
Tags	Displays the tag that is assigned for the template and aids to filter templates based on the tags.
Supported Platforms	Displays the supported Cisco Nexus platforms compatible with the template. Check the check box of platforms that are supported with the template. **Note** You can select multiple platforms.
Template Type	Displays the type of the template.
Template Sub Type	Specifies the sub type that is associated with the template.
Template Content Type	Specifies if it is Jython or Template CLI.

Table 16: Advanced Template Properties

Field	Description
Implements	Displays the abstract template to be implemented.
Dependencies	Specifies the specific feature of a switch.
Published	Specifies if the template is published or not.
Imports	Specifies the base template for importing.

In addition, from the menu bar, choose **Configure** > **Templates** > **Template Library** > **Templates** and you can also:

- Click **Show Filter** to filter the templates that is based on the headers.
- Click **Print** to print the list of templates.
- Click **Export to Excel** to export the list of template to a Microsoft Excel spreadsheet.

This section contains the following:

Template Structure

The configuration template content mainly consists of four parts. Click the **Help** icon next to the **Template Content** for information about editing the content of the template.

This section contains the following:

Template Format

This section describes the basic information of the template. The possible fields are as detailed in the table below.

Property Name	Description	Valid Values	Optional?
name	The name of the template	Text	No
description	Brief description about the template	Text	Yes
userDefined	Indicates whether the user created the template. Value is ‘true’ if user created.	“true” or “false”	Yes
supportedPlatforms	List of device platforms supports this configuration template. Specify ‘All’ to support all platforms.	N1K, N3K, N3500, N4K, N5K, N5500, N5600, N6K, N7K, N9K, MDS, VDC, N9K-9000v, IOS-XE, IOS-XR, Others, All Nexus Switches list separated by comma.	No

Property Name	Description	Valid Values	Optional?
templateType	Specifies the type of Template used.	• CLI • POAP • POLICY • SHOW • PROFILE • FABRIC • ABSTRACT	Yes

Property Name	Description	Valid Values	Optional?
templateSubType	Specifies the sub type associated with the template.		

Property Name	Description	Valid Values	Optional?
		• CLI • N/A • POAP • N/A • VXLAN • FABRICPATH • VLAN • PMN • POLICY • VLAN • INTERFACE_VLAN • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • INTERFACE_VLAN • INTERFACE_VPC	

Property Name	Description	Valid Values	Optional?
		• INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • PROFILE • VXLAN • FABRIC • NA	

Property Name	Description	Valid Values	Optional?
		• ABSTRACT • VLAN • INTERFACE_VLAN • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE	

Property Name	Description	Valid Values	Optional?
contentType		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI • POLICY • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • PROFILE • TEMPLATE_CLI • PYTHON • FABRIC • PYTHON • ABSTRACT • TEMPLATE_CLI • PYTHON	Yes
implements	Used to implement the abstract template.	Text	Yes
dependencies	Used to select the specific feature of a switch.	Text	Yes
published	Used to Mark the template as read only and avoids changes to it.	“true” or “false”	Yes

Template Variables

This section contains declared variables, the data type, default values, and valid values conditions for the parameters that are used in the template. These declared variables are used for value substitution in the template content section during the dynamic command generation process. Also these variables are used in decision making and in iteration blocks in the template content section. Variables have predefined data types. You can also add a description about the variable. The following table describes the syntax and usage for the available datatypes.

Variable Type	Valid Value	Iterative?
boolean	true|false	No
enum	Example: running-config, startup-config	No
float	Floating number format	No
floatRange	Example: 10.1,50.01	Yes
Integer	Any number	No
integerRange	Contiguous numbers separated by “-“ Discrete numbers separated by “,” Example: 1-10,15,18,20	Yes
interface	Format: <if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	No
interfaceRange	Example: eth10/1/20-25, eth11/1-5	Yes
ipAddress	IPv4 OR IPv6 address	No
ipAddressList	You can have a list of IPv4, IPv6, or a combination of both types of addresses. Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334 Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254	Yes

Variable Type	Valid Value	Iterative?

ipAddressWithoutPrefix	`Example: 192.168.1.1`
	or
	`Example: 1:2:3:4:5:6:7:8`
		No

ipV4Address	IPv4 address	No
ipV4AddressWithSubnet	`Example: 192.168.1.1/24`	No
ipV6Address	IPv6 address	No

ipV6AddressWithPrefix	`Example: 1:2:3:4:5:6:7:8`
	`22`
		No

ipV6AddressWithSubnet	IPv6 Address with Subnet	No
ISISNetAddress	`Example: 49.0001.00a0.c96b.c490.00`	No
long	`Example: 100`	No
macAddress	14 or 17 character length MAC address format	No

string	Free text, for example, used for the description of a variable
	`Example:`
	`string scheduledTime`
	`{`
	`regularExpr=^([01]\d|2[0-3]):([0-5]\d)$;`
	`}`
		No

string[]	`Example: {a,b,c,str1,str2}`	Yes

Variable Type	Valid Value	Iterative?

struct	Set of parameters that are bundled under a single variable.
	`struct <structure name declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [<structure_inst1>] [, <structure_inst2>] [, <structure_array_inst3 []>];`
	`struct interface_detail { string inf_name; string inf_description; ipAddress inf_host; enum duplex { validValues = auto, full, half; }; }myInterface, myInterfaceArray[];`
		No
		Note If the struct variable is declared as an array, the variable is iterative.

wwn (Available only in Cisco DCNM Web Client)	`Example: 20:01:00:08:02:11:05:03`	No

Example: Template Variables

```
##template variables
integer VSAN_ID;
string SLOT_NUMBER;
integerRange PORT_RANGE;
integer VFC_PREFIX;
##
```

Variable Meta Property

Each variable that is defined in the template variable section has a set of meta properties. The meta properties are mainly the validation rules that are defined for the variable.

The following table describes the various meta properties applicable for the available variable types.

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
boolean	A boolean value. Example: `true`	Yes											
enum			Yes										
float	signed real number. Example: `75.56, -8.5`	Yes	Yes	Yes	Yes	Yes							
floatRange	range of signed real numbers Example: `50.5 - 54.75`	Yes	Yes	Yes	Yes	Yes							
integer	signed number Example: `50, -75`	Yes	Yes		Yes	Yes							
integerRange	Range of signed numbers Example: `50-65`	Yes	Yes		Yes	Yes							
interface	specifies interface/port Example: `Ethernet 5/10`	Yes	Yes				Yes	Yes	Yes	Yes			
interfaceRange		Yes	Yes				Yes	Yes	Yes	Yes			

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
ipAddress	IP address in IPv4 or IPv6 format	Yes											

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
ipAddressList	You can have a list of IPv4, IPv6, or a combination of both types of addresses. `Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109` `Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334` `Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254` **Note** Separate the addresses in the list using commas and not hyphens.	Yes											

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
ipAddressWithoutPrefix	IPv4 or IPv6 Address (does not require prefix/subnet)												
ipV4Address	IPv4 address	Yes											
ipV4AddressWithSubnet	IPv4 Address with Subnet	Yes											
ipV6Address	IPv6 address	Yes											
ipV6AddressWithPrefix	IPv6 Address with prefix	Yes											
ipV6AddressWithSubnet	IPv6 Address with Subnet	Yes											
ISISNetAddress	`Example:` `49.0001.00a0.c96b.c490.00`												
long	`Example: 100`	Yes			Yes	Yes							
macAddress	MAC address												

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
string	literal string `Example for string` `Regular expression:` `string scheduleTime {` [illegible] `}`	Yes									Yes	Yes	Yes
string[]	string literals that are separated by a comma (,) `Example:` `{string1, string2}`	Yes											

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
struct	Set of parameters that are bundled under a single variable. `struct <structure name declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [<structure_inst1>] [, <structure_inst2>] [, <structure_array_inst3 []>];`												
wwn	WWN address												

Example: Meta Property Usage

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
 string inf_name;
 string inf_description;
 ipAddress inf_host;
 enum duplex {
  validValues = auto, full, half;
 };
}myInterface;

##
```

Variable Annotation

You can configure the variable properties marking the variables using annotations.

Note Variable Annotations are available for POAP only. However, the annotations do not impact on the template type 'CLI'.

The following annotations can be used in the template variable section.

Annotation Key	Valid Values	Description
AutoPopulate	Text	Copies values from one field to another
DataDepend	Text	
Description	Text	Description of the field appearing in the window
DisplayName	Text **Note** Enclose the text with quotes, if there is space.	Display name of the field appearing in the window
Enum	Text1, Text2, Text3, and so on	Lists the text or numeric values to select from
IsAlphaNumeric	"true" or "false"	Validates if the string is alphanumeric
IsAsn	"true" or "false"	
IsDestinationDevice	"true" or "false"	
IsDestinationFabric	"true" or "false"	
IsDestinationInterface	"true" or "false"	
IsDestinationSwitchName	"true" or "false"	
IsDeviceID	"true" or "false"	
IsDot1qId	"true" or "false"	

Annotation Key	Valid Values	Description
IsFEXID	“true” or “false”	
IsGateway	“true” or “false”	Validates if the IP address is a gateway
IsInternal	“true” or “false”	Makes the fields internal and does not display them on the window **Note** Use this annotation only for the ipAddress variable.
IsManagementIP	“true” or “false” **Note** This annotation must be marked only for variable “ipAddress”.	
IsMandatory	“true” or “false”	Validates if a value should be passed to the field mandatorily
IsMTU	“true” or “false”	
IsMultiCastGroupAddress	“true” or “false”	
IsMultiLineString	“true” or “false”	Converts a string field to multiline string text area
IsMultiplicity	“true” or “false”	
IsPassword	“true” or “false”	
IsPositive	“true” or “false”	Checks if the value is positive
IsReplicationMode	“true” or “false”	
IsShow	“true” or “false”	Displays or hides a field on the window
IsSiteId	“true” or “false”	
IsSourceDevice	“true” or “false”	
IsSourceFabric	“true” or “false”	
IsSourceInterface	“true” or “false”	

Annotation Key	Valid Values	Description
IsSourceSwitchName	"true" or "false"	
IsSwitchName	"true" or "false"	
IsRMID	"true" or "false"	
IsVPCDomainID	"true" or "false"	
IsVPCID	"true" or "false"	
IsVPCPeerLinkPort	"true" or "false"	
IsVPCPeerLinkPortChannel	"true" or "false"	
IsVPCPortChannel	"true" or "false"	
Password	Text	Validates the password field
UsePool	"true" or "false"	
UseDNSReverseLookup		
Username	Text	Displays the username field on the window
Warning	Text	Provides text to override the Description annotation

Example: AutoPopulate Annotation

```
##template variables
string BGP_AS;
 @(AutoPopulate="BGP_AS")
  string SITE_ID;
##
```

Example: DisplayName Annotation

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
ipAddress hostAddress;
##
```

Example: IsMandatory Annotation

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

Example: IsMultiLineString Annotation

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow Annotation

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual",  Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to true
or false
```

Example: Warning Annotation

```
##template variables
@(Warning="This is a warning msg")
  string SITE_ID;
##
```

Templates Content

This section includes the configuration commands and any parameters that you want to include in the template. These commands can include the variables declared in the template variables section. During the command generation process the variable values are substituted appropriately in the template content.

Note You must specify the commands that you include as if you were entering them in the global configuration command mode on any device. You must consider the command mode when you include commands.

Template content is governed by the usage of variables.

- Scalar variables: does not take a range or array of values which cannot be used for iteration (In the variable types table those marked iterate-able as 'No'). Scalar variables must be defined inside the template content.

  ```
  Syntax: $$<variable name>$$
  Example: $$USER_NAME$$
  ```

- Iterative variables: used for block iteration. These loop variable must be accessed as shown below inside the iteration block.

```
Syntax:@<loop variable>
Example:
foreach val in $$INTEGER_RANGE_VALUE$$ {
@val
}
```

- Scalar Structure Variable: Structure member variables can be accessed inside the template content.

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

- Array Structure Variable: Structure member variables can be accessed inside the template content.

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

In addition to the template variables, you can use the conditional and iterative command generation using the following statements:

- if-else if-else Statement: makes a logical decision in inclusion/exclusion of set of configuration command based on the value assigned for the variable in it.

```
Syntax: if(<operand 1>  <logical operator>  <operand 2>){
command1 ..
command2..
..
}
else  if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

- foreach Statement: used for iterating a block of commands. The iteration is performed based on the assigned loop variable value.

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
foreach ports in $$MY_INF_RANGE$${
interface @ports
no shut
}
```

- Optional parameters: By default all parameters are mandatory. To make a parameter optional, you must annotate the parameter.
- Interactive command handling: Include prompt and response as part of the template content for handling interactive commands.

```
Example:

##template variables
string srcFile;
string srcDir;
string password;
string vrf;
##

##template content
copy scp://root@10.127.117.65/$$srcFile$$ bootflash: vrf $$vrf$$ <prompt:'(yes/no)?',
response:'yes'> <prompt:'(y/n)?[n]',
response:'y'> <prompt:'password:',
response:'$$password$$'>
```

In the variable section, you can include the following command:

- **@(IsMandatory=false)**
- **Integer frequency;**

  In the template content section, a command can be excluded or included without using “if” condition check, by assigning a value to the parameter. The optional command can be framed as below:

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

Template Content Editor

The template content editor has the following features:

- Syntax highlighting: The editor highlights the syntax, like different types of statements, keywords, and so on, for Python scripting.
- Autocompletion: The editor suggests the template datatypes, annotations, or metaproperties when you start typing.
- Go to line: You can navigate to the exact line in the template content editor instead of scrolling. Press **Command-L** in Mac or **Ctrl-L** in Windows, and enter the line number to which you want to navigate to in the pop-up window.

  If you enter a value greater than the number of lines in the editor, you will be navigated to the last line in the editor window.

- Template search and replace: Press **Command-F** in Mac or **Ctrl-F** in Windows, enter the search term in the **Search for** field, and select the type of search in the search window. You can perform the following searches in the editor:
  - **RegExp Search**: You can perform the regular expression search in the editor.
  - **CaseSensitive Search**: You can perform a case-sensitive search in the editor.

  - **Whole Word Search**: You can perform a whole word search to find the exact words in the editor. For example, a regular search for the word "play" returns results where it is part of words like "display," but the whole word search returns results only when there is an exact match for the word "play".
  - **Search In Selection**: You can perform a search in the selected content. Select the content to which you want to limit the search and enter the search term.

  Choose the + icon in the search window to use the replace option. Enter the replacing word in the **Replace with** field. You can replace the selected word once by selecting **Replace**. To replace all the occurrences of the selected word, select **All**.

- Code folding: You can expand or group code blocks in the editor by clicking the arrow next to their line numbers.
- Other features: The editor automatically indents the code, the closing braces, and highlights the matching parenthesis.

Template Editor Settings

You can edit the following features of a template editor by clicking **Template Editor Settings**.

- **Theme**: Select the required theme for the editor from the drop-down list.
- **KeyBinding**: Select the editor mode from the **KeyBinding** drop-down list to customize the editor. **Vim** and **Ace** modes are supported. The default is **Ace**.
- **Font Size**: Select the required font size for the editor.

Advanced Features

The following are the advanced features available to configure templates.

- Assignment Operation

  Config template supports assignment of variable values inside the template content section. The values are validated for the declared data type of the variable. If there is a mismatch, the value is not assigned.

  Assignment operation can be used under the following guidelines:

  - The operator on the left must be any of the template parameters or a for loop parameter.
  - The operator on the right values can be any of the values from template parameters, for loop parameters, literal string values surrounded by quotes or simple string values.

  If a statement does not follow these guidelines, or if it does not suit this format, it will not be considered as assignment operation. It is substituted during command generation like other normal lines.

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
```

```
@(internal=true)
integer vlanName;
##
##template content
foreach vlanID in $$vlan_range$${
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

- Evaluate methods

  Config template uses the Java runtime provided Java script environment to perform arithmetic operations (such as ADD, SUBTRACT, and so on), string manipulations, and so on.

  Locate the JavaScript file in the template repository path. This file contains primary set of arithmetic, string functions. You can also add custom JavaScript methods.

  These methods can be called from config template content section in below format:

  ```
  Example1:
  $$somevar$$ = evalscript(add, "100", $$anothervar$$)
  ```

  Also the *evalscript* can be called inside if conditions as below:

  ```
  if($$range$$ > evalscript(sum, $$vlan_id$$,  -10)){
  do something...
  }
  ```

  You can call a method that is located at the backend of the Java script file.

- Dynamic decision

  Config template provides a special internal variable “LAST_CMD_RESPONSE”. This variable stores the last command response from the device during the execution of the command. This can be used in the config template content to make dynamic decisions to deliver the commands that are based on the device condition.

  Note The if block must be followed by an else block in a new line, which can be empty.

  An example use case to create a VLAN, if it is does not exist on the device.

  ```
  Example: Create VLAN
  ##template content
  show vlan id $$vlan_id$$
  if($$LAST_CMD_RESPONSE$$ contains "not found"){
  vlan $$vlan_id$$
  }
  else{
  }
  ##
  ```

  This special implicit variable can be used only in the “IF” blocks.

- Template referencing

  You can have a base template with all the variables defined. This base template can be imported to multiple templates. The base template content is substituted in the appropriate place of the extending template. The imported template parameters and the contents can be accessed inside the extending template.

```
Example: Template Referencing
Base template:
##template properties
 name =a vlan base;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = ;
##
##template variables
 integer vlan_id;
##
##template content
 vlan $$vlan_id$$
##

Derived Template:
##template properties
 name =a vlan extended;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = a vlan base,template2;
##
##template variables
 interface vlanInterface;
##
##template content
 <substitute a vlan base>
 interface $$vlanInterface$$
 <substitute a vlan base>
##
```

When you launch the extended template, the parameter inputs for the base template are also obtained. In addition, the substituted content is used for complete CLI command generation.

- Solution POAP Templates for VXLAN and FabricPath

  From Cisco DCNM Release 10.0(1), Cisco provides you a set of defined templates to aid in POAP operations. You can download Cisco-defined templates from https://software.cisco.com/download/release.html.

  For instructions on how to download and install POAP templates, see *Cisco DCNM Installation Guide, Release 10.0(x)*.

Adding a Template

To add user-defined templates and schedule jobs from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

The **Templates** window is displayed with the name of the template along with its description, supported platforms, and tags.

Step 2 Click **Add** to add a new template.

The Template Properties window appears.

Step 3 Specify a template name, description, tags, and supported platforms for the new template.

Step 4 Specify a **Template Type** for the template. Select **POAP** to make this template available when you power on the application.

Note The template is considered as a CLI template if **POAP** is not selected.

Step 5 Select a **Template Sub Type** and **Template Content Type** for the template.

Step 6 Click the **Advanced** tab to edit other properties like **Implements**, **Dependencies**, **Published**, and **Imports**. Select **Published** to make the template read-only. You cannot edit a published template.

Step 7 From the **Imports > Template Name** list, check the template check box.

The base template content is displayed in the **Template Content** window. The base template displays the template properties, template variables, and template content. This template can be imported in to another template and the base template content is substituted in the appropriate place of the extending template. When you launch the extended template, the parameter inputs for the base template are also obtained. Also, the substituted content is used for complete CLI command generation.

Note The base templates are CLI templates.

Step 8 Click **OK** to save the template properties, or click the cancel icon at the top-right corner of the window to revert the changes.

Note You can edit the template properties by clicking **Template Property**.

Step 9 Click **Template Content** to edit the template syntax. For information about the structure of the Configuration Template, see the *Template Structure* section.

Step 10 Click **Validate Template Syntax** to validate the template values.

If an error or a warning message appears, you can check the validation details in **Validation Table** by clicking the error and warnings field.

Note You can continue to save the template if there are warnings only. However, if there is an error, you must edit the templates to fix the errors before you proceed. Click the line number under the Start Line column to locate the error in the template content. You will get an error if you validate a template that does not have a template name.

Step 11 Click **Save** to save the template.

Step 12 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Configuring Template Job

To configure and schedule jobs for individual templates from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Templates > Template Library > Templates**.

Step 2 Select a template.

Note Config Job wizard is applicable only for CLI templates.

Step 3 Click **Launch job creation wizard** icon and click **Next**.

Step 4 Use the drop-down to select **Device Scope**.

The devices that are configured under the selected **Device Scope** are displayed.

Note If no devices are displayed, check if the device LAN credentials are configured by choosing **Administration > Credentials Management > LAN Credentials**.

Step 5 Use the arrows to move the devices to the right column for job creation and click **Next**.

Step 6 In the **Define Variable** section, specify the VSAN_ID, VLAN_ID, ETH_SLOT_NUMBER, VFC_SLOT_NUMBER, SWITCH_PORT_MODE, ETH_PORT_RANGE and ALLOWED_VLANS values.

Note Based on the selected template, variables vary.

Step 7 In the **Edit Variable Per Device** section, double click the fields to edit the variables for specific devices and click **Next**.

Step 8 If you have selected multiple devices, use the drop-down to select a specific device and preview its configuration. Click **Back** to edit the configuration or click **Next**.

Step 9 Specify a job name and description.

The Device Credentials are populated from **Administration > Credentials Management > LAN Credentials**.

Step 10 Use the radio button to select **Instant Job** or **Schedule Job**.

If you select **Schedule Job**, specify the date and time for the job delivery.

Step 11 Use the check box to select **Copy Run to Start**.

Step 12 If you want to configure more transaction and delivery options, use the check box to select **Show more options**.

Step 13 Under **Transaction Options(Optional)**, if you have a device with rollback feature support, select **Enable Rollback** check box and select the appropriate radio button.

You can choose one of the following options by selecting the appropriate radio button:

- **Rollback the configuration on a device if there is any failure on that device**
- **Rollback the configuration on all the devices if there is any failure on any device**
- **Rollback the configuration on a device if there is any failure on any device and stop further configuration delivery to remaining devices**

Step 14 Under **Delivery Options (Optional)**, specify the command response timeout in seconds and use the radio button to select a delivery order. The value of command response timeout ranges from 1 to 180.

You can choose one of the following options by selecting the appropriate radio button:

- **Deliver configuration one device at a time in sequential**

- **Delivery configuration in parallel to all devices at the same time**

Step 15 Click **Finish** to create the job.

A confirmation message is displayed that the job has been successfully created. The jobs are listed in the **Jobs** window.

Modifying a Template

You can edit the user-defined templates. However, the predefined templates and templates that are already published cannot be edited.

Procedure

Step 1 From **Configure** > **Templates** > **Template Library** > **Templates**, select a template.

Step 2 Click **Modify/View template**.

Step 3 Edit the template description and tags.

The edited template content is displayed in a pane on the right.

Step 4 From the **Imports** > **Template Name** list, check the template check box.

The base template content is displayed in the **Template Content** window. You can edit the template content based on your requirement in the **Template Content** window. Click the help icon next to the **Template Content** window for information about editing the content of the template.

Step 5 Edit the supported platforms for the template.

Step 6 Click **Validate Template Syntax** to validate the template values.

Step 7 Click **Save** to save the template.

Step 8 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Copying a Template

To copy a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates**, and select a template.

Step 2 Click **Save Template As**.

Step 3 Edit the template name, description, tags, and other parameters.

The edited template content is displayed in the right-hand pane.

Step 4 From the **Imports** > **Template Name** list, check the template check box.

The base template content is displayed in the **Template Content** window. You can edit the template content that is based on your requirement in the **Template Content** window. Click the help icon next to the **Template Content** window for information about editing the content of the template.

Step 5 Edit the supported platforms for the template.

Step 6 Click **Validate Template Syntax** to validate the template values.

Step 7 Click **Save** to save the template.

Step 8 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Deleting a Template

You can delete the user-defined templates. However, you cannot delete the predefined templates. From Cisco DCNM Release 11.0(1), you can delete multiple templates at once.

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

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

Step 2 Use the check box to select a template and click **Remove template** icon.

The template is deleted without any warning message.

What to do next

The template is deleted from the list of templates on the DCNM Web UI. When you restart the DCNM services, the deleted templates are displayed on the **Configure** > **Templates** > **Template Library** > **Templates** page.

To delete the template permanently, delete the template that is located in your local directory: `Cisco Systems\dcm\dcnm\data\templates\`.

Importing a Template

To import a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates** and click **Import Template**.

Step 2 Browse and select the template that is saved on your computer.

You can edit the template parameters, if necessary. For information, see Modifying a Template, on page 160.

Note The “\n” in the template is considered as a new line character when imported and edited, but it works fine when imported as a ZIP file.

Step 3 Click **Validate Template Syntax** to validate the template.

Step 4 Click **Save** to save the template or **Save and Exit** to save the template and exit.

Note You can import Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates to the Cisco DCNM Web Client. For more information, see *Installing POAP Templates*.

Exporting a Template

To export a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

Step 2 Use the check box to select a template and click **Export Template**.

The browser requests you to open or save the template to your directory.

Installing POAP Templates

Cisco DCNM allows you to add, edit, or delete user-defined templates that are configured across different Cisco Nexus platforms. From Cisco DCNM Release 10.0(x), Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates are provided as a separate download on the official Cisco website. These templates are compatible for use with the DCNM Virtual Appliance (OVA or ISO) for use with Nexus 2000, Nexus 5000, Nexus 6000, Nexus 7000, and Nexus 9000 Series switches.

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

Perform the following task to install the POAP templates from the Cisco DCNM.

Procedure

Step 1 Navigate to https://software.cisco.com/download/release.html, and download the file.

You can choose one of the following:

- `dcnm_ip_vxlan_fabric_templates.10.0.1a.zip`
- `dcnm_fabricpath_fabric_templates.10.0.1a.zip file`

Step 2 Unzip and extract the files to the local directory on your computer.

Step 3 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

Step 4 Click **Import Template**.

Step 5 Browse and select the template that is saved on your computer. You can edit the template parameters, if necessary.

Step 6 Check **POAP** and **Publish** check box to designate these templates as POAP templates.

Step 7 Click **Validate Template Syntax** to validate the template.

Step 8 Click **Save** to save the template or **Save and Exit** to save the template and exit.

Configuring Jobs

To configure jobs from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Templates Library** > **Jobs**.

The jobs are listed along with the Job ID, description and status. The latest task will be listed at the top.

Note If failover is triggered in Native HA, the Job ID sequence number is incremented by 32.

Step 2 Click **Show Filter** to filter the list.

In the **Status** column, use the drop-down to select the job status.

Step 3 Select a job and click the **Delete** icon to delete the job.

Step 4 To view the status of a job, click the **Job ID** radio button and click **Status**.

Step 5 To view the command execution status for a device, click the radio button of a device name from the **Devices** table in the **Job Execution Status** window.

Note You can delete multiple jobs at once, but you cannot view the status of multiple jobs at once.

Backup

The **Backup** menu includes the following submenus:

Switch Configuration

This feature allows you to backup device configurations from running configuration as a regular text file in the file system. However, you can also perform operations on startup configuration. The backup files can be stored in the DCNM server host or on a file server.

You can also configure the archive system to support scheduling of jobs for the selected list of devices. You can configure only one job for a switch.

The following tables describe the icons and fields that appear on **Configure** > **Backup** > **Switch Configuration**.

Table 17: Switch Configuration Operations

Icon	Description
Copy Configuration to bootflash	Allows you to copy a configuration file of a switch to the bootflash of the selected destination switches.
View Configuration	Allows you to view the configuration file.
Delete Configuration	Allows you to delete the configuration file.

Icon	Description
Compare Configuration	Allows you to compare two configuration files, from different devices or on the same device.
Export Configuration	Allows you to export a configuration file from the DCNM server.
Import User-Defined Configuration	Allows you to import a user-defined configuration file to the DCNM server.
Restore Configuration to devices	Allows you to restore configuration from the selected devices.
Archive Jobs	Allows you to add, delete, view, or modify the jobs.

Table 18: Switch Configuration Field and Description

Field	Description
Device Name	Displays the device name Click the arrow next to the device to view the configuration files.
IP Address	Displays the IP address of the device.
Group	Displays the group of the device.
Configuration	Displays the configuration files that are archived for that device.
Archive Time	Displays the time when the device configuration files were archived. The format is Day:Mon:DD:YYYY HH:MM:SS.
Size	Displays the size of the archived file.

This section contains the following:

Copy Configuration

You can copy the configuration files to the same device, to another device, or multiple devices concurrently.

Perform the following task to view the status of tasks.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure** > **Backup** > **Switch Configuration**. Select any startup/running/archive configuration of the device that you must copy.

Step 2 Click **Copy Configuration to bootflash**.

Copy Configuration to bootflash page appears, displaying the **Source Configuration Preview** and **Selected Devices** area.

Source Configuration Preview area shows the contents of running/startup/version configuration file which is copied to the devices.

Step 3 In the **Selected Devices** area, check the device name check box to copy the configuration to the device.

Note You can select multiple destination devices to copy the configuration.

The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration is copied.
- IP Address—Specifies the IP Address of the destination device.
- Group—Specifies the group to which the device belongs.
- Status—Specifies the status of the device.

Step 4 Click **Copy**.

A confirmation window appears.

Step 5 Click **Yes** to copy the configuration to the destination device configuration.

View Configuration

You can view or edit the configuration file on the device.

Perform the following task to view or edit the configuration file for the devices.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device. Select the configuration file radio button to view the configuration file.

Step 2 Click the View Configuration.

The View Configuration window appears showing the configuration file content.

Delete Configuration

Perform the following task to delete the configuration file from the device.

Note Ensure that you take a backup of the configuration file before you delete.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device.

Step 2 Click the configuration file radio button to be deleted.

Note You can delete multiple configuration files. However, you cannot delete startup, or running configuration files.

Step 3 Click **Yes** to delete the configuration file.

Compare Configuration Files

This feature allows you to compare the configuration file with another version of the same device or with the configuration file of another device.

Perform the following task to compare the configuration files.

Procedure

Step 1 Navigate to **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device.

Step 2 Check the check box and select two configuration files to compare.

The first file that you selected is designated as Source and the second configuration file is designated as the Target file.

Step 3 Click **Compare Configuration**.

View Config Diff page appears, displaying the difference between the two configuration files.

The Source and Target configuration files content is displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration. You can also choose **Changed** to view the configuration differences of the configuration files.

The differences in the configuration file are show in the table, with legends.

- **Red**: Deleted configuration details.
- **Green**: New added configuration.
- **Blue**: Modified configuration details.

Step 4 Click **Copy to Target** to copy the source configuration to the target configuration file. Click **Cancel** to revert to the configuration details page.

The Copy Configuration window displays the source configuration preview and the target device of the destination configuration. The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration is copied.
- IP Address—Specifies the IP Address of the destination device.

- Group—Specifies the group to which the device belongs.
- Status—Specifies the status of the device.

Step 5 Click **Yes** to copy the configuration to the destination device configuration.

Export Configuration

You can export a configuration file from the Cisco DCNM server. Perform the following task to export a configuration file.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure** > **Backup**, select a configuration to export.

Step 2 Click **Export Configuration**.

The files are downloaded in your local system. You can use the third-party file transfer tools to transfer these files to an external server.

Import Configuration File

You can import the configuration file from the file server to the Cisco DCNM.

Perform the following task to import a single or multiple configuration files.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure** > **Backup** > **Switch Configuration** and click **Import User-Defined Configuration**.

The file server directory opens.

Step 2 Browse the directory and select the configuration file that you want to import. Click **Open**.

A confirmation screen appears.

Note The file name should not contain forward slash (/) or backward slash (\).

The file name can be alphanumeric. It can also have a period (.), underscore (_), and a space. You can import only files with the .cfg extension.

Step 3 Click **Yes** to import the selected file.

The imported configuration file appears as a User Imported file.

Restore Configuration

You can restore the configuration file from the selected switches. From Cisco DCNM Release 11.0(1), you can restore configuration based on the selected date as well.

Note You cannot restore the configuration for SAN switches and FCoE-enabled switches.

Perform the following task to restore the configuration from the selected devices.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**, and click **Restore**.

Step 2 Select the type of restore from the drop-down list. You can choose **Version-based** or **Date-based**.

Note

- If you choose date-based restore, you have to select the date and time. The configuration available before the mentioned time is restored.
- If you choose version-based restore, you have to choose a configuration from the **Configuration** column. You can view the configuration details in the **View** column.

Step 3 Check the **Device Name** check box from which you want to restore the configuration. Click **Restore**.

The **Devices** area shows the following fields:

- Device Name—Specifies the device name from which the configuration file is restored.
- IP Address—Specifies the IP Address of the device.
- Group—Specifies the group to which the device belongs.
- Status—Specifies the status of the device.

Note You can restore the configuration only from the same device. If you select user-imported configuration files, you can restore configuration for any number of devices.

Archive Jobs

This section contains context-sensitive online help content under Cisco DCNM **Configure > Backup > Switch Configuration >Archive Jobs**.

DCNM switch archive jobs list SNMPv3 as a requirement. Error cause in job execution is "Switch is not managed using SNMPv3", status is "Not Eligible". This is not documented.

Note The configuration files from the archived jobs are located in the DCNM Server directory: `\dcm\dcnm\data\archive\<dcnm-ip-address>\`. You can use the third-party file transfer tools or file transfer commands to transfer these files to an external server.

The following table describes the fields that appear on the **Archive Jobs** window.

Field	Description
User	Specifies who created this job.
Group	Specifies the group to which this job belongs.
Group Job	Specifies whether it is a group job or a per-device job. The values are **true** or **false**.
Schedule	Specifies the schedule of the job. Also show the recurrence information.
Last Execution	Specifies the date and time at which this job was last executed.
Job Status	Specifies if the job was successful, scheduled, running, or failure. **Note** **Running** and **Scheduled** status is not applicable for existing jobs in an upgraded Cisco DCNM. Status shows **Not Eligible** and an error appears `Switch is not managed using SNMPv3`, when SNMPv3 is not enabled on DCNM.
User Comments	Specifies the comments or description provided by the user.

Archive Jobs

To add, delete or view the job from the Cisco DCNM Web UI, perform the following steps:

Note You must set the SFTP/TFTP/SCP credentials before you configure jobs. On the DCNM Web Client, navigate to **Administration** > **DCNM Server** > **Archive FTP Credentials** to set the credentials.

Procedure

Step 1 Choose **Configure** > **Backup** > **Switch Configuration** > **Archive Jobs** > **Archive Jobs** tab, and click **Add Job**.

The Create Job screen displays the Schedule, Device Selection and Selected Devices.

A backup is scheduled as defined.

a) In the **Schedule** area, configure the start time, repeat interval and repeat days.

- **Start At**: Configure the start time using the hour:minutes:second drop-down lists.
  - **Once**: Configure the job to be executed once, on the particular day. The time at which this job will be executed is determined by the **Start At** field.

    - Now—Configure the job to be executed immediately. Cisco DCNM will consider the default date and time as configured on the server.

      Note You can schedule a job to run **Now** even if a job is already scheduled.

    - **Daily**: Check the check box on the days you want this job to be executed. The time at which this job will be executed is determined by the **Start At** field.

    - **Real Time**: Configure the job to be executed if there is any configuration changes in the device. The device must be quiet for 5 minutes, after which the DCNM Sever will execute this job.

  - **Repeat Interval**: Check the Repeat Interval check box to repeat the job at scheduled intervals. Configure the intervals using either days or hours drop-down list.

  - **Comments**: Enter your comments, if any.

b) In the **Device Selection** area, use the radio button to choose one of the following:

  - **Device Group**: Click the Device Group radio button to select the entire group of devices for this job.

    Select the Device Group from the drop-down list.

    Note When the devices are not licensed, they will not be shown under the group on the Cisco DCNM **Configure > Backup > Switch Configuration > Archive Jobs**. When none of the devices under a group is licensed, the group alone will be shown with no devices, until a device under that group is licensed.

  - **Selected Devices**: Click the **Selected Devices** radio button to select one of multiple devices from various groups for this job.

    Select the devices from the drop-down list.

    From Cisco DCNM Release 11.2(1), you can apply VRF for all the selected devices simultaneously. You can either apply Management VRFs or Default VRFs.

  Note When the SAN and LAN credentials are not configured for a switch, it will not be listed in the Selected Devices drop-down list. To configure, navigate to **Administration > Credentials Management > SAN Credentials** and **Administration > Credentials Management > LAN Credentials**.

c) In the **Selected Devices** area, the following fields are shown:

  - **Name**: Specifies the name of the device on which the job is scheduled.

  - **IP Address**: Specifies the IP Address of the device.

  - **Group**: Specifies the group to which the device belongs.

  - **VRF**: Specifies the virtual routing and forwarding (VRF) instance.

    Select a VRF type to modify the existing VRF type to the specified device. You can either apply Management VRFs or Default VRFs.

  Note If a job for a device exists under device level, you can create a group level job which includes this switch as part of that group. However, this switch will be excluded during the execution of the job.

d) Click **Create** to add a new job.

Step 2 To delete a job, from the Cisco DCNM home page, choose **Configure** > **Backup** > **Switch Configuration** > **Archive Jobs** > **Archive Jobs**, and select a job.

a) Click **Delete Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

b) Click **Delete**.

Step 3 To view the details of the job, from the Cisco DCNM home page, choose **Configure** > **Backup** > **Switch Configuration** > **Archive Jobs** > **Archive Jobs**, and check the job check box.

a) Click **View/Modify Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

b) Modify the required details. Click **OK** to revert to view the list of jobs.

Note

- You cannot modify a job that is scheduled to be run **Now** to one that is scheduled to be run **Daily**.
- You cannot modify the repeat interval duration for an archive job. When you try to modify, the operation fails and the job is deleted. You must delete existing repeat interval archive job and create a new job.

What to do next

You can also configure the Cisco DCNM to retain the number of archived files per device. Choose **Administration** > **DCNM Server** > **Server Properties**, and update the **archived.versions.limit** field.

Job Execution Details

The Cisco DCNM **Web Client** > **Configure** > **Backup** > **Switch Configuration** > **Archive Jobs** > **Archive Jobs** > **Job Execution Details** tab shows the following tabs in the Job Execution History table.

Field	Description
Job Name	Displays the system-generated job name.
User	Specifies the persona of the person who created the job.
Device Group	Specifies fabric or the LAN group under which the job was created.
Device	Specifies the IP Address of the Device.
Server	Specifies the IP Address of the DCNM Server to which the device is associated with.
Protocol	Specifies if the SFTP, TFTP, or SCP protocol is applied.
Execution time	Specifies the time at which the job was last executed.

Field	Description
Status	Specifies the status of the job. • Skipped • Failed • Successful
Error Cause	Specifies the error if the job has failed. The categories are as follows: • No change in the configuration. • Switch is not managed by this server. **Note** If the error cause column is empty, it implies that the job was executed successfully. Hover over the error cause to view the complete description.

Archives

A user with network operator role can view configuration archives for a switch and their details in the **Archives** window.

The following tables describe the icons and fields that are displayed in this window.

Table 19: Archive Operations

Icon	Description
Compare	Allows you to compare two configuration files either from different devices or on the same device.
View	Allows you to view a configuration file.

Table 20: Archive Field and Description

Field Name	Description
Device Name	Displays the device name Click on the arrow next to the device to view the configuration files.
IP Address	Displays the IP address of the device.
Group	Displays the group of the device.
Configuration	Displays the configuration files that are archived for that device.

Field Name	Description
Archive Time	Displays the time at which the device configuration files were archived. The format is Day:Mon:DD:YYYY HH:MM:SS.
Size	Displays the size of the archived file.

This section contains the following:

Compare Configuration Files

You can compare one version of a configuration file with another version of the same configuration file in the same device, or the configuration files of two different devices.

To compare the configuration files from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Backup > Archives**.

Step 2 In the **Archives** area, click the arrow that is adjacent the name of the device whose configuration files you want to view. The list of configuration files is displayed.

Step 3 Check the check box next to configuration files and select two configuration files to compare.

The first file that you select is designated as the source and the second configuration file is designated as the target file.

Step 4 Click **Compare**.

The **View Config Diff** page displays the difference between the two configuration files.

The Source and Target configuration files content are displayed in two columns. Choose **All** from the drop-down list in the right-top corner to view the entire configuration. Choose **Changed** to view the configuration differences between the configuration files.

The differences in the configuration files are shown in a table, with legends.

- **Red**: Deleted configuration details.
- **Green**: New added configuration.
- **Blue**: Modified configuration details.

View Configuration

You can view an archived configuration file.

To view or edit the configuration file for the devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Backup** > **Archives**.

The **Archives** window is displayed.

Step 2 Click the arrow that is next to the name of the device whose configuration files you want to view.

The list of configuration files are displayed.

Step 3 Select the radio button that is next to the corresponding file you want to view.

Step 4 Click the **View** configuration icon.

The **View** configuration window appears showing the configuration file content in the right column.

Network Config Audit

Cisco DCNM provides auditing for the configuration changes across the network switches. The Network Audit Reporting feature enables you to a generate audit report so that you can track the added, deleted, or modified configurations. You will be able to generate the network audit reports only when you have existing archival jobs. Using the generated reports, you can view the config differences on a device for a specified period.

This section contains the following:

Generating Network Config Audit Reports

To generate the network config audit reports from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Backup** > **Network Config Audit**.

The **Network Audit Report** window is displayed.

Step 2 In the **Devices** drop-down list, choose the devices to generate a report.

Step 3 Specify the **Start Date** and the **End Date**.

Step 4 Click **Generate Report** to view the configuration differences. The configuration differences are color-coded.

- Red: Deleted Configuration
- Green: Newly Added Configuration
- Blue: Changed configuration
- Strikethrough: Old configuration

After you generate a report, you can export the configuration reports into an HTML file.

Creating a Network Config Audit Report

To create a network config audit job and view the configuration differences between the devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Report** > **Generate**.

The left pane shows various reports that you can create.

Step 2 Choose **Common** > **Network Config Audit**.

Step 3 In the **Report Name** field, enter the name of the report.

Step 4 In the **Repeat** field, choose the appropriate repeat interval, that is, Daily, Weekly, or Monthly.

Daily job generates a report of configuration differences for all the selected devices for last 1 day. Weekly job generates a report for the last 7 days, and the monthly job generates a report for the last 30 days.

Step 5 In the **Start** and **End** date fields, specify the start and end date for the report.

Step 6 In the **Email Report** field, specify the email delivery options.

- No: Select this option if you do not want to send the report through email.
- Link Only: Select this option if you want to send the link to the report.
- Contents: Select this option if you want to send the report content.

If you select Link Only or the Contents option, enter the email address and subject in the **To** and **Subject** fields.

Monitoring Network Config Audit Report

To monitor the network config audit report from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Report** > **View**.

Step 2 Choose **Common** > **Network Config Audit** in the left pane to the network config audit reports.

Deleting a Network Config Audit Report

To delete a network config audit report from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Report** > **View**.

Step 2 Choose **Common** > **Network Config Audit**.

The **View Reports** window is displayed with the reports that you have created.

Step 3 Select the reports that you want to delete, and click the **Delete** icon.

Image Management

Upgrading your devices to the latest software version manually might take a long time and prone to error, which requires a separate maintenance window. To ensure rapid and reliable software upgrades, image management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring. Image management is supported only for Cisco Nexus switches and Cisco MDS switches.

Note Before you upgrade, ensure that the POAP boot mode is disabled for Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches. To disable POAP, run the `no boot poap enable` command on the switch console. You can however, enable it after the upgrade.

The **Image Management** menu includes the following submenu:

Upgrade [ISSU]

The **Upgrade [ISSU]** menu includes the following submenus:

Upgrade History [ISSU]

This feature enables you to upgrade the Cisco Nexus Platform Switches using In-Service Software Upgrade (ISSU). This upgrade procedure may be disruptive or non-disruptive based on the device configuration. You can select the Kickstart, System, or SSI images required for the upgrade from a remote server using SFTP, SCP, TFTP, FTP or from image repository or the file system on the device. Image repository can use SCP, SFTP, FTP, or TFTP as file transfer protocol. To select the images from the repository, the same needs to be uploaded from **Configure > Image Management > Repositories** tab.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task will be listed in the top. **Note** If Failover is triggered in Native HA, the Task Id sequence number is incremented by 32.
Task Type	Specifies the type of task. • Compatibility • Upgrade
Owner	Based on the Role-Based Authentication Control (RBAC), specifies the owner who initiated this task.
Devices	Displays all the devices that were selected for this task.

Field	Description
Job Status	Specifies the status of the job. • Planned • In Progress • Completed • Completed with Exceptions **Note** If the job fails on a single or multiple devices, the status field shows COMPLETED WITH EXCEPTION indicating a failure.
Created Time	Specifies the time when the task was created.
Scheduled At	Specifies the time when the task is specified to be executed. You can also choose to schedule a task to be executed at a later time.
Completed Time	Specifies the time when the task was completed.
Comment	Shows any comments that the Owner has added while performing the task.

Note After a fresh Cisco DCNM installation, this page will have no entries.

You can perform the following:

New Installation

To upgrade the devices that are discovered from the Cisco DCNM, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

Step 2 Choose **New Installation** to install, or upgrade the kickstart and the system images on the devices.

The devices with default VDCs are displayed in the **Select Switches** window.

Step 3 Select the check box to the left of the switch name.

You can select more than one switch and move the switches to the right column.

Step 4 Click **Add** or **Remove** icons to include the appropriate switches for upgrade.

The selected switches appear in a column on the right.

Step 5 Click **Next**.

The **Pre-Post ISSU Reports** window appears.

Note Pre-Post ISSU Reports are not supported in SAN and Media Controller installations.

Step 6 Click **Next**.

The **Specify Software Images** window appears. This tab displays the switches that you selected in the previous screen. You can choose the images for upgrade as well.

- The **Auto File Selection** check box enables you to specify a file server, an image version, and a path where you can apply the upgraded image to the selected devices.
- In the **Select File Server** drop-down list, select the one of the file servers that is created in the Cisco DCNM repositories.
- In the **Image Version** field, specify the image version. For example, enter 7.3.9.D1.1 in the **Image Version** field if you have selected m9700-sf3ek9-kickstart-mz.7.3.0.D1.1.bin as the image version.
- In the **Path** field, specify the image path. Specify an absolute path if you choose SCP or SFTP. For example, `//root/images/`. Specify a relative path to the FTP or TFTP home directory if you choose FTP or TFTP. Specify the absolute path of the image if you're using TFTP server that is provided by Cisco DCNM, local DCNM TFTP. You can't use the same DCNM TFTP server for creating another job when the current job is in progress.

Step 7 Click **Select Image** in the **Kickstart image** column.

The **Software Image Browser** dialog box appears.

Note

- Cisco Nexus 3000 Series and 9000 Series Switches require only the system image to load the Cisco NX-OS operating system. Therefore, the option to select kickstart images for these devices is disabled.
- If there's an issue in viewing the **Software Image Browser** dialog box, reduce the font size of your browser and retry.

Step 8 Click **Select Image** in the **System Image** column.

The **Software Image Browser** dialog box appears.

Step 9 On the **Software Image Browser** dialog box, you can choose the image from **File Server** or **Switch File System**.

If you choose **File Server**:

a) From the **Select the File server** list, choose the appropriate file server on which the image is stored.

The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.

b) From the **Select Image** list, choose the appropriate image. Check the check box to use the same image for all other selected devices of the same platform.

Example: For platform types N7K-C7009 and N7K-C7010, logic matches platform (N7K) and three characters (C70) from subplatform. The same logic is used across all platform switches.

Note Only files with BIN extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

c) Choose a VRF from the **Select Vrf** drop-down list.

Note This field does not appear for Cisco MDS switches.

This VRF is selected for other selected devices by default. The default value is **management**.

d) Click **OK**.

If the file server selected is either `ftp` or `tftp`, in the text box, enter the relative path of the file from the home directory.

This image is selected for all other selected devices of same platform type.

If you choose **Switch File System**:

a) From the **Select Image** list, choose the appropriate image that is located on the flash memory of the device.

Note Only files with BIN extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK** to choose the kickstart image or **Cancel** to revert to the **Specify Software Images** dialog box.

Step 10 The **Vrf** column indicates the name of the virtual routing and forwarding (VRF).

VRF is not applicable for Cisco MDS devices.

Step 11 In the **Available Space** column, specify the available space for the **Primary Supervisor** and **Secondary Supervisor** modules of the switch.

Available Space column shows the available memory in MB on the switch (for less than 1 MB, it’s shown and marked as KB).

Bootflash browser shows the filename, size, and last modified date for all the files and directories on the switch bootflash. You can delete files by selecting them and clicking **Delete** to increase the available space on the switch.

Step 12 **Selected Files Size** column shows the size of images that are selected from the SCP or SFTP server.

If the total size of selected images is greater than available space on a switch, the file size is marked in red. We recommend that you create more space on the switch to copy images to it and install.

Step 13 Drag and drop the switches to reorder the upgrade task sequence.

Step 14 (Optional) Uncheck **Skip Version Compatibility** check box if you want to check the compatibility of Cisco NX-OS software version on your device with the upgraded images that you chose.

Step 15 Select **Select Parallel Line Card upgrade** to upgrade all the line cards at the same time.

Upgrading a parallel line card isn’t applicable for Cisco MDS devices.

Step 16 Click **Options** under the **Upgrade Options** column to choose the type of upgrade.

Upgrade Options window appears with two upgrade options. The drop-down list for **Upgrade Option 1** has the following options:

- **Disruptive**
- **Bios force**
- **Allow non-disruptive**
- **Force non-disruptive**

Disruptive is the default value for Cisco Nexus 9000 Series switches. The upgrade option is **Not Applicable** for other switches.

When you choose **Allow non-disruptive** under **Upgrade Option 1** and if the switch does not support non-disruptive upgrade, then it will go through a disruptive upgrade.

When you choose **Force non-disruptive** under **Upgrade Option 1**, the **Skip Version Compatibility** check box will be unchecked because compatibility check is mandatory for non-disruptive upgrade. If the switches you choose do not support non-disruptive upgrade, a warning message appears asking you to review the switch selection. Use the check boxes to choose or remove switches.

The drop-down list for **Upgrade Option 2** has the following options when you choose **Allow non-disruptive** or **Force non-disruptive** under **Upgrade Option 1**:

- **NA**
- **bios-force**

When you choose **Disruptive** or **Bios-force** under **Upgrade Option 1**, **Upgrade Option 2** is disabled.

Check the **Use this Option for all other selected devices** check box to use the selected option for all the selected devices and click **OK**.

Note
- The upgrade options are applicable only for Cisco Nexus 3000 Series and 9000 Series switches.
- Selecting the **Allow non-disruptive** option for upgrading does not ensure a non-disruptive upgrade. Perform a compatibility check to ensure that the device supports non-disruptive upgrade.

Step 17 Click **Next**.

If you didn’t select **Skip Version Compatibility**, the Cisco DCNM performs a compatibility check.

You can choose to wait until the check is complete or click **Finish Installation Later**.

The installation wizard is closed and a compatibility task is created in **Configure > Image Management > Upgrade [ISSU] > Upgrade History** tasks.

The time that is taken to check the image compatibility depends on the configuration and the load on the device.

The **Version Compatibility VerificationCompatibility Verification** status column displays the status of verification.

If you skip the version compatibility check by choosing **Skip Version Compatibility**, Cisco DCNM displays only the name of the device. The **Current Action** column displays **Completed**, and the **Compatibility Verification** column displays **Skipped**.

You can review the switch selection and check or uncheck the switches for upgrading accordingly.

Step 18 Click **Finish Installation Later** to perform the upgrade later.

Step 19 Click **Next**.

Step 20 Check the **Next** check box to put a device in maintenance mode before upgrade.

Step 21 Check the check box to save the running configuration to the startup configuration before upgrading the device.

Step 22 You can schedule the upgrade process to occur immediately or later.

a. Select **Deploy Now** to upgrade the device immediately.

b. Select **Choose time to Deploy** and specify the time in MMM/DD/YYYY HH:MM:SS format to perform the upgrade later.

   This value is relative to the server time. If the selected time to deploy is in the past, the job is executed immediately.

Step 23 You can choose the execution mode based on the devices and the line cards you have chosen to upgrade.

a. Select **Sequential** to upgrade the devices in the order you chose them.

   Note This option is disabled if you put the device in maintenance mode.

b. Select **Concurrent** to upgrade all the devices at the same time.

Step 24 Click **Finish** to begin the upgrade process.

The Installation wizard closes and a task to upgrade is created on the **Configure > Image Management > Upgrade [ISSU] > Upgrade History** page.

What to do next

After you complete the ISSU on the switch, ensure that you wait for 20 minutes to allow the switch to reboot, and stabilize the SNMP agent. DCNM discovers polling cycles in order to display the new version of the switch on the Cisco DCNM Web UI.

Finish Installation

You can choose to complete the installation for tasks which was completed on the **Compatibility Check** page. Perform the following task to complete the upgrade process on the devices.

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, select a task for which the compatibility check is complete.

Select only one task at a time.

Step 2 Click **Finish Installation**.

Software Installation Wizard appears.

Step 3 Review the switch selection and check or uncheck the switches for upgrading accordingly.

Step 4 Check the check box to save the running configuration to the startup configuration before upgrading the device.

Step 5 Check the check box to put a device in maintenance mode before upgrade. This option is valid only for the devices that support maintenance mode.

Step 6 You can schedule the upgrade process to occur immediately or later.

a. Select **Deploy Now** to upgrade the device immediately.

b. Select **Choose time to Deploy** and specify the time in DD/MM/YYYY HH:MM:SS format to perform the upgrade later.

Step 7 You can choose the execution mode that is based on the devices and the line cards that you have chosen to upgrade.

a. Select **Sequential** to upgrade the devices in the order in which they were chosen.

Note This option is disabled if you put the device in maintenance mode.

b. Select **Concurrent** to upgrade the devices at the same time.

Step 8 Click **Finish** to complete the upgrade process.

View

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

Procedure

Step 1 Choose **Configure** > **Image Management** > **Upgrade [ISSU]** > **Upgrade History**, check the task ID check box.

Select only one task at a time.

Step 2 Click **View**.

The **Installation Task Details** window appears.

Step 3 Click **Settings**. Expand the **Columns** menu and choose the details you want to view.

You can view the following information in this window:

- Location of the kickstart and system images
- Compatibility check status
- Installation status
- Descriptions
- Logs

Step 4 Select the device.

The detailed status of the task appears. For the completed tasks, the response from the device appears.

If the upgrade task is in progress, a live log of the installation process appears.

Note

- This table autorefreshes every 30 secs for jobs in progress, when you’re on this window.
- The switch-level status for an ongoing upgrade on a Cisco MDS switch doesn't appear for other users without SAN credentials. To apply SAN Credentials, choose **Administration > Credentials Management > SAN Credentials**.

Delete

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

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, and check the **Task ID** check box.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm deletion of the job.

Switch Level History

You can view the history of the upgrade process at a switch level. You can view the current version of the switch and other details.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History**.

Field	Description
Switch Name	Specifies the name of the switch
IP Address	Specifies the IP Address of the switch
Platform	Specifies the Cisco Nexus switch platform
Current Version	Specifies the current version on the switch software

Click the radio button next to a switch name to select the switch and view its upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History > View Device Upgrade Tasks**:

Field	Description
Owner	Specifies the owner who initiated the upgrade.

Field	Description
Job Status	Specifies the status of the job. • Planned • In Progress • Completed
KickStart Image	Specifies the kickStart image that is used to upgrade the Switch.
System Image	Specifies the system image that is used to upgrade the switch.
Completed Time	Specifies the date and time at which the upgrade was successfully completed.
Status Description	Specifies the installation log information of the job.

Patch [SMU]

The Patch [SMU] menu includes the following submenus:

Installation History

This feature allows you to activate or deactivate packages using Software Maintenance Update (SMU). Personnel with Admin privileges can perform this operation.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Installation History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task is listed at the top. The tasks are performed in the sequential order.
Switch Name	Specifies the name of the switch for which the patch file is installed.
IP Address	Specifies the IP Address of the device.
Task	Specifies if the patch is installed or uninstalled on this device.
Package	Specifies the name of the patch file.
Status	Specifies the status of installation or uninstallation of the patch files.

Field	Description
Status Description	Describes the status of installation or uninstallation of the patch files.

This section contains the following:

Install Patch

To install the patch on your devices from Cisco DCNM Web Client, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Install**.

The **Select Switches** window appears. All the Cisco Nexus switches that are discovered by Cisco DCNM are displayed.

Step 2 Select the check box to the left of a switch name.

You can select more than one device.

Step 3 Click **Add** or **Remove** icons to include the appropriate switches for installing the patch.

The selected switches appear in the right column.

Step 4 Click **Next**.

Step 5 Click **Select Packages** in the **Packages** column.

The **SMU Package Browser** dialog box appears.

Step 6 In the **SMU Package Browser** dialog box, you can choose the patch file from **File Server** or **Switch File System**.

If you choose **File Server**:

a) From the **Select the file server** list, choose the appropriate file server on which the patch is stored.

The servers, which are listed in the **Repositories** window, are displayed in the drop-down list. Choose **Configure > Image Management > Repositories** to view the **Repositories** window.

b) From the **Select Image** list, choose the appropriate patch that must be installed on the device.

You can select more than one patch file to be installed on the device.

Note If the patch installation results in the restart of the device, select only one patch file.

Check the check box to use the same patch for all other selected devices of the same platform.

Only files with BIN extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

c) From the **Select Vrf** list, choose the appropriate virtual routing and forwarding (VRF).

The two options in the drop-down list are **management** and **default**.

Check the check box to use the same VRF for all other selected devices.

d) Click **OK** to choose the patch image or **Cancel** to revert to the SMU installation wizard.

If you choose **Switch File System**:

a) From the **Select Image** list, choose the appropriate patch file image that is located on the flash memory of the device.

You can select more than one patch file to be installed on the device.

Only files with BIN extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK** to choose the image, **Clear Selections** to uncheck all the check boxes, or **Cancel** to revert to the **SMU Package Browser** dialog box.

Step 7 Click **Finish**.

You will get a confirmation window. Click **OK**.

Note SMU installation may reload the switch if the SMU is reloaded.

You can view the list of patches that are installed on the switch in the **Switches** window by choosing **DCNM > Inventory > Switches**.

Uninstall Patch

To uninstall the patch on your devices from Cisco DCNM Web Client, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Uninstall**.

The **Select Switches** page appears. The discovered Cisco Nexus switches are displayed.

Step 2 Check the check box on the left of the switch name.

You can select more than one image device.

Step 3 Click **Add** or **Remove** icons to include the appropriate switches for installing the patch.

The selected switches appear in a column on the right.

Step 4 Click **Next**.

The **Active Packages** page appears.

Step 5 Click **Select Packages** under the **Installed Packages** column.

The **Packages Installed** window appears, which lists the patches that are applied to the switch.

Step 6 Select the patches that you want to uninstall from this device.

You can select more than one patch that is applied on the device.

Note If the patch uninstallation results in the restart of the device, select only one patch.

Step 7 Click **Finish** to uninstall the patch from the device.

You will get a confirmation window. Click **OK**.

You can uninstall more than one patch at a time.

Note SMU uninstallation may reload the switch if the SMU is reloaded.

Delete Patch Installation Tasks

To delete the patch installation tasks from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, check the task ID check box.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm deletion of the patch installation task.

Switch Installed Patches

You can view the patches that are installed on all the switches in the network. You can refresh the view to see the latest installed patches.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Switch Installed Patches**.

Field	Description
Switch Name	Specifies the name of the switch.
IP Address	Specifies the IP address of the switch.
Platform	Specifies the Cisco Nexus switch platform.
Installed Patches	Specifies the currently installed patches on switches.

Click **Refresh** to refresh the table.

Package [RPM]

The Package [RPM] menu includes the following submenus:

Package Installation [RPM]

The package [RPM] feature allows you to install RPM packages. This feature is available for the Cisco Nexus 9000 Series and 3000 Series Switches.

The following table describes the fields that appear on **Configure > Image Management > Package [RPM] > Installation History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task is listed in the top. The tasks are performed in the sequential order.
Switch Name	Specifies the name of the switch for which the package file is installed.
IPAddress	Specifies the IP address of the device.
Task	Specifies if the package is installed or uninstalled on this device.
Package	Specifies the name of the package file.
Status	Specifies the status of installation or uninstallation of the package files.
Completed Time	Specifies the time at which the installation or uninstallation task completed.
Status Description	Describes the status of installation or uninstallation of the package files.

This section contains the following:

Install Package [RPM]

Perform the following task to install the package on your devices using Cisco DCNM Web client.

Procedure

Step 1 Choose **Configure** > **Image Management** > **Package [RPM]** > **Installation History**, click **Install**.

The **Select Switches** page appears.

Step 2 Check the check box on the left of the switch name.

You can select more than one device.

Step 3 Click **Add** or **Remove** to include appropriate switches for installing packaging.

The selected switches appear in a column on the right.

Step 4 Click **Next**.

Step 5 Click **Select Packages** in the **Packages** column.

The **RPM Package Browser** screen appears.

Step 6 Choose the package file from **File Server** or **Switch File System**.

If you choose **File Server**:

a) From the **Select the file server** list, choose the appropriate file server on which the package is stored.

The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.

b) From the **Select Image** list, choose the appropriate package that must be installed on the device.

You can select more than one package file to be installed on the device.

Only files with RPM extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

Check the check box to use the same package for all other selected devices of the same platform.

c) Click **OK** to choose the patch image or **Cancel** to revert to the RPM Installation Wizard.

If you choose **Switch File System**:

a) From the **Select Image** list, choose the appropriate package file image that is located on the flash memory of the device.

You can select more than one package file to be installed on the device.

Only files with RPM extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK**.

Step 7 In the **Installation Type** column, choose one of the installation types:

- **Normal**—Fresh installation
- **Upgrade**—Upgrading the existing RPM
- **Downgrade**—Downgrading the existing RPM

Step 8 Click **Finish**.

You can view the list of packages that are installed on the switch, on the **Web Client > Inventory > Switches** page.

Note If you are using Cisco DCNM Release 10.1(2), in case of installation of reload RPMs, perform a manual install commit on the switch after it switch reloads.

Uninstall Package [RPM]

To uninstall the RPM on your devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Package [RPM] > Installation History**, click **Uninstall**.

The **Select Switches** window appears.

Step 2 Check the check box on the left of the switch name.

You can select more than one switch.

Step 3 Click the **Add** or **Remove** icons to include the appropriate switches for uninstalling the package.

The selected switches appear in a column on the right.

Step 4 Click **Next**.

The **Active Packages** page appears.

Step 5 Click **Select Packages** under the **Installed Packages** column.

The **Packages Installed** window appears, which lists the packages that are installed in the switch.

Step 6 Click **Finish** to uninstall the package from the device.

You will get a confirmation window. Click **OK**.

You can uninstall more than one package at a time.

Note

- If you are using Cisco DCNM Release 10.1(2), in case of uninstallation of reload RPMs, a manual install commit needs to be performed on the switch once the switch is reloaded.
- RPM uninstallation may reload the switch if the RPM is reload RPM.

Delete Package Installation Tasks

To delete the package installation tasks from the history view from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Package [RPM] > Installation History**, select the task ID check box.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm deletion of the task.

Switch Installed Packages

You can view the RPM packages that are installed on all Switches in the network. You can refresh the view to see the latest installed packages.

The following table describes the fields that appear on **Configure > Image Management > Packages [RPM] > Switch Installed Packages**.

Field	Description
Switch Name	Specifies the name of the switch.
IP Address	Specifies the IP address of the switch.

Field	Description
Platform	Specifies the Cisco Nexus switch platform.
Installed Packages	Specifies the currently installed packages on the switches and the type of package. The installed packages can be base packages or non-base packages.

Click **Refresh** to refresh the table.

Maintenance Mode [GIR]

The Maintenance Mode [GIR] menu includes the following submenus:

Maintenance Mode

The maintenance mode allows you to isolate the Cisco Nexus Switch from the network to perform an upgrade or debug, using Graceful Insertion and Removal (GIR). When the switch maintenance is complete, you can return the switch to normal mode. When the switch is in the maintenance mode, all protocols are gracefully brought down and all physical ports are shut down. When the normal mode is restored, all the protocols and ports are initiated again.

Perform the following to change the system mode of the devices.

Procedure

Step 1 Choose **Configure > Image Management > Maintenance Mode [GIR] > Maintenance Mode**, check the switch name check box.

You can select multiple switches.

Step 2 Choose one of the following options under the **Mode Selection** column:

- Shutdown
- Isolate

Note Click the appropriate option before you change the mode.

Step 3 Click **Change System Mode**.

A confirmation message appears.

Step 4 Click **OK** to confirm to change the maintenance mode of the device.

The status of operation can be viewed in the **System Mode** and the **Maintenance Status**.

Switch Maintenance History

You can view the history of the maintenance mode changes executed from the Cisco DCNM.

The following table describes the fields that appear on **Configure > Image Management > Maintenance Mode [GIR] > Switch Maintenance History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest tasks that are listed in the top.
Switch Name	Specifies the name of the switch for which the maintenance mode was changed.
IP Address	Specifies the IP address of the switch.
User	Specifies the name of the user who initiated the maintenance.
System Mode	Specifies the mode of the system.
Maintenance Status	Specifies the mode of the maintenance process.
Status	Specifies the status of the mode change.
Completed Time	Specified the time at which the maintenance mode activity was completed.

Click the radio button next to the switch name to select the switch for which you need to view the upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure** > **Image Management** > **Upgrade [ISSU]** > **Switch Level History** > **View** > **Upgrade Tasks History**

Field	Description
Owner	Specifies the owner who initiated the upgrade.
Job Status	Specifies the status of the job. • Planned • In Progress • Completed
KickStart Image	Specifies the kickstart image that is used to upgrade the Switch.
System Image	Specifies the system image that is used to upgrade the switch.
Completed Time	Specifies the date and time at which the upgrade was successfully completed.

Image and Configuration Servers

To view the **Image and Configuration Servers** window from the Cisco DCNM Web UI homepage, choose **Configure > Image Management > Repositories**.

You can view the following details in the **Image and Configuration Servers** window.

Field	Descriptions
Name	Specifies the name of the repository you upload.
URL	Specifies the path where you uploaded the repository.
Username	Specifies the username of the remote server.
Last Modified	Specifies the date and timestamp of the last modification.

Add Image or Configuration Server URL

To add an image or a configuration server URL to the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the **Image and Configuration Servers** window, click the **Add** icon.

The **Add Image or Configuration Server URL** window is displayed.

Step 2 Specify a name for the image.

Step 3 Click the radio button to select the protocol.

The available protocols are **SCP**, **FTP**, **SFTP**, and **TFTP**. Use the SCP protocol for POAP and Image Management.

You can use IPv4 and IPv6 addresses with these protocols.

Step 4 Enter the hostname or IP address and the path to download or upload files.

Note If you choose **SCP** or **SFTP** protocol and the path is root or /directory, adding an image or configuration server will not be successful.

Step 5 Specify the username and password.

Step 6 Click **OK** to save.

Deleting an Image

To delete an image from the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Image Management** > **Repositories**.

The **Image and Configuration Servers** window appears.

Step 2 Choose an existing image from the list and click the **Delete Image** icon.

A confirmation window appears.

Step 3 Click **Yes** to delete the image.

Editing an Image or Configuration Server URL

To edit an image or a configuration server URL to the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the **Image and Configuration Servers** window, select an existing image and configuration server from the list, and click **Edit**.

Step 2 In the **Edit Image or Configuration Server URL** window, edit the required fields.

Step 3 Click **OK** to save or click **Cancel** to discard the changes.

File Browser

You can view the contents of the server on the **Image and Configuration Servers** page.

1. In the **Image and Configurations** page, check the **Server Name** check box to view the content.
2. Click **File Browser** to view the contents of this server.

Image Upload

To upload different types of images to the server from the Cisco DCNM Web UI, perform the following steps:

Note Devices use these images during POAP or image upgrade.

Your user role should be **network-admin** to upload an image. You can’t perform this operation with the **network-stager** user role.

Procedure

Step 1 Choose **Configure** > **Image Management** > **Repositories**.

The **Image and Configuration Servers** window appears.

Step 2 Click **Image Upload**.

The **Select File to Upload** dialog box appears.

Step 3 Click **Choose file** to choose a file from the local repository of your device.

Step 4 Choose the file and click **Upload**.

Step 5 Click **OK**.

The upload takes some time depending on the file size and network bandwidth.

LAN Telemetry Health

Starting from DCNM 11.2(1), Streaming LAN Telemetry preview feature in DCNM is obsolete and is replaced by Network Insights Resources (NIR) application. NIR can be deployed using Cisco DCNM Applications Framework on **Web UI > Applications**. After the NIR is enabled on a fabric, you can monitor the status on the window in the Cisco DCNM Web UI.

When the connection status is shown as **Disconnected** the port configuration may not be accepted by the switch correctly. On the switch image 7.0(3)I7(6), if a switch already had **nxapi** configuration, and later it was managed by DCNM and telemetry was enabled on that fabric, DCNM pushes **http port 80** configuration so that it could query some NXAPI commands such as **show telemetry transport** and **show telemetry data collector details**, to monitor telemetry connection statistics. In this case, the switch does not update **http port 80** in its configuration even though the command was executed correctly. In such a scenario, issue the following commands on the switch:

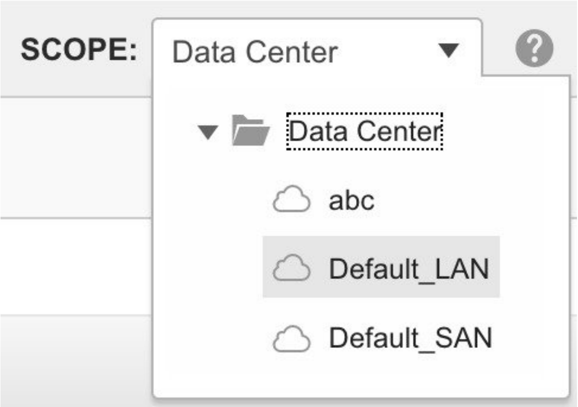
```
switch# configure
switch(config)# no feature nxapi
switch(config)# feature nxapi
switch(config)# http port 80
```

Note ICAM telemetry commands such as forwarding TCAM and ACL TCAM are not supported on Cisco Nexus C9504, C9508, and C9516 Series platforms for switch images 7.0(3)I7(5) and 7.0(3)I7(6)

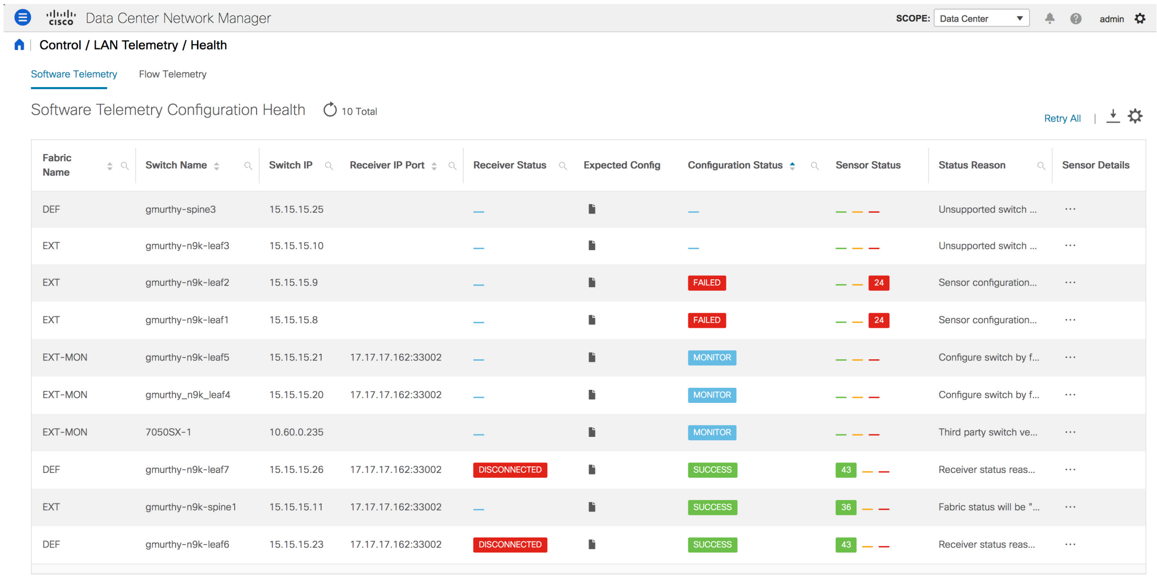
LAN Telemetry has the following topics:

Health

Cisco DCNM allows you to monitor the configuration health attributes of Software Telemetry and Flow Telemetry for each fabric. The attributes are displayed for a particular fabric or all fabrics based on the selected **SCOPE**. **Data Center scope** displays all fabrics by default.



Software Telemetry



Software Telemetry Configuration Health 10 Total

Fabric Name	Switch Name	Switch IP	Receiver IP Port	Receiver Status	Expected Config	Configuration Status	Sensor Status	Status Reason	Sensor Details
DEF	gmurthy-spine3	15.15.15.25		—	📄	—	— — —	Unsupported switch ...	···
EXT	gmurthy-n9k-leaf3	15.15.15.10		—	📄	—	— — —	Unsupported switch ...	···
EXT	gmurthy-n9k-leaf2	15.15.15.9		—	📄	FAILED	— — 24	Sensor configuration...	···
EXT	gmurthy-n9k-leaf1	15.15.15.8		—	📄	FAILED	— — 24	Sensor configuration...	···
EXT-MON	gmurthy-n9k-leaf5	15.15.15.21	17.17.17.162:33002	—	📄	MONITOR	— — —	Configure switch by f...	···
EXT-MON	gmurthy_n9k_leaf4	15.15.15.20	17.17.17.162:33002	—	📄	MONITOR	— — —	Configure switch by f...	···
EXT-MON	7050SX-1	10.60.0.235		—	📄	MONITOR	— — —	Third party switch ve...	···
DEF	gmurthy-n9k-leaf7	15.15.15.26	17.17.17.162:33002	DISCONNECTED	📄	SUCCESS	43 — —	Receiver status reas...	···
EXT	gmurthy-n9k-spine1	15.15.15.11	17.17.17.162:33002	—	📄	SUCCESS	36 — —	Fabric status will be "...	···
DEF	gmurthy-n9k-leaf6	15.15.15.23	17.17.17.162:33002	DISCONNECTED	📄	SUCCESS	43 — —	Receiver status reas...	···

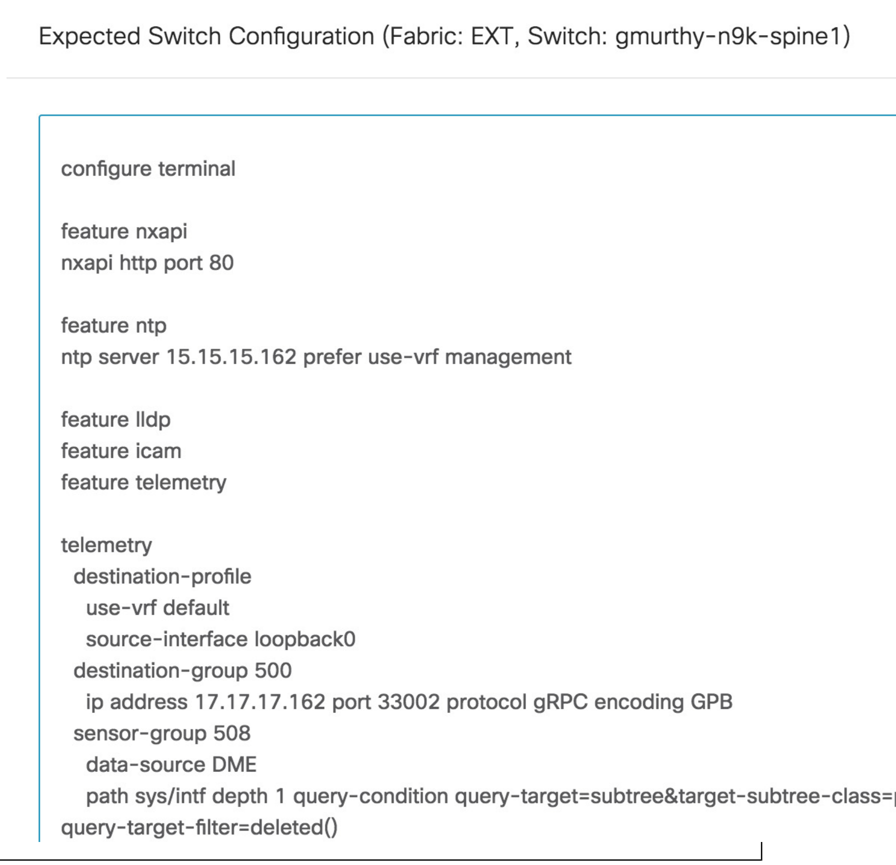
The following table describes the fields that appear in the **LAN Telemetry** > **Health** > **Software Telemetry** window.

Field	Description
Fabric Name	Displays the fabric name.
Switch Name	Displays the switch name.
Switch IP	Displays the switch management IP address.
Switch Serial	Displays the switch serial number. This column is hidden by default. Click the **Settings** icon, and check the **Switch Serial** check box to add it to the columns displayed.

Field	Description
Switch Model	Displays the switch model. This column is hidden by default. Click the **Settings** icon, and check the **Switch Model** check box to add it to the columns displayed.
Switch Version	Displays the switch image version. This column is hidden by default. Click the **Settings** icon, and check the **Switch Version** check box to add it to the columns displayed.
Receiver IP Port	Displays the receiver IP and port assigned to a switch to transport telemetry data. The assigned IP and port will be based on the configured telemetry network, out-of-band or in-band, and the corresponding receiver microservice that is running in NIR application.

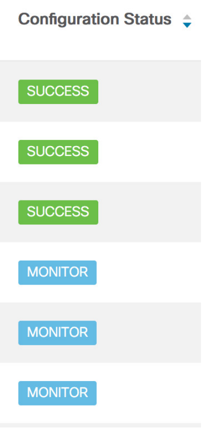
Receiver Status	Displays the status of the connection used to transport telemetry data between the switch and the receiver running in the NIR application.
	The telemetry manager polls the switch for the connection status every 5 mins.
	The valid values are:
	• **Connected**: The status is **Connected** when the telemetry manager is able to poll the receiver connection status from the switches.
	• **Disconnected**: If the status is **Disconnected**, the reason is mentioned in the **Status Reason** column.
	• **Null**: The status is **Null** when the telemetry manager in DCNM has not polled the receiver connection status from the switches or when it has not received any response from the switch for that request. When the receiver status is **Null** and if the configuration status is **MONITOR** or **SUCCESS**, log into the switch and check the nxapi configuration.
	When you enable telemetry on a fabric that is managed by DCNM, the telemetry manager pushes the **httpport 80** configuration. If the switch does not have **httpport 80** configuration, run the following commands on the switch:
	`switch# configure terminal`
	`switch(config)# no feature nxapi`
	`switch(config)# feature nxapi`
	`switch(config)# http port80`

Configuration Type	Displays the connection type ex: gRPC as reported by the switch. This value is obtained as part of the receiver connection status response from the switch. This column is hidden by default. It can be selected by clicking on the settings button.

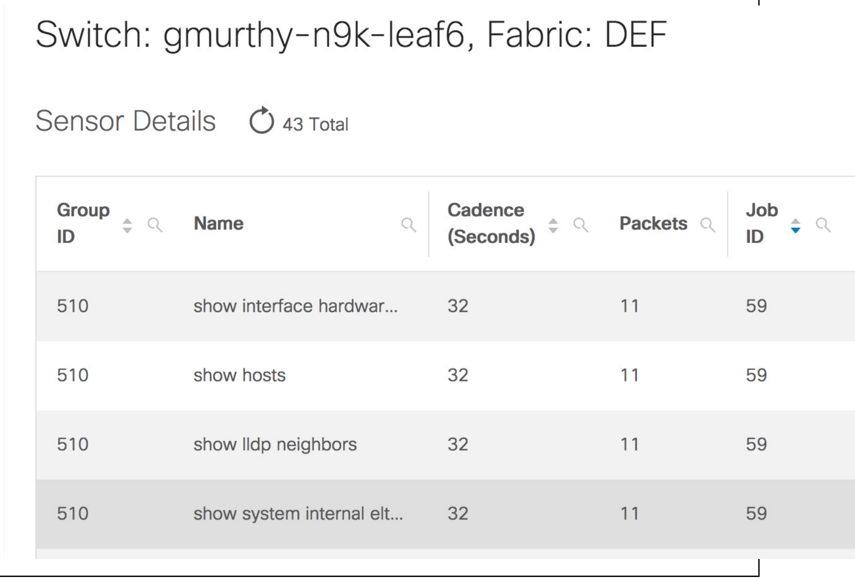
Field	Description
Expected Config	Click the **Expected Config** icon to view the expected configuration for the switch in a dialog box. In case of error, the error reason will be displayed in the output. 

Expected Switch Configuration (Fabric: EXT, Switch: gmurthy-n9k-spine1)

```
configure terminal

feature nxapi
nxapi http port 80

feature ntp
ntp server 15.15.15.162 prefer use-vrf management

feature lldp
feature icam
feature telemetry

telemetry
  destination-profile
    use-vrf default
    source-interface loopback0
  destination-group 500
    ip address 17.17.17.162 port 33002 protocol gRPC encoding GPB
  sensor-group 508
    data-source DME
    path sys/intf depth 1 query-condition query-target=subtree&target-subtree-class=
query-target-filter=deleted()
```

Field	Description
Configuration Status	Displays the telemetry configuration switch summary status. The valid values are: • **MONITOR**: Implies that the switch in the fabric was configured as **Monitored** in the NIR app. In this case, configure these switches manually with the telemetry configurations as displayed in the **Expected Config** column. • **PROCESSING**: Implies that the switch belonging to the fabric was configured as **Managed** in the NIR app. In this case, the telemetry manager will configure the switches and when configuration is in progress, it is displayed as **PROCESSING**. • **SUCCESS**: Implies that the switches were successfully configured. • **PARTIAL SUCCESS**: Implies that some of the telemetry configurations could not be pushed to the switches. The **Status Reason** column will indicate the failure reason. • **FAILED**: Implies that the DCNM job failed to configure the switches. It could happen that some configuration did get pushed to the switches while some did not, in that case also DCNM marks the whole job as **Failed**. The **Status Reason** column will indicate the failure reason. You can filter the switches based on a particular status using the search option or you can sort the switches based on the status.  Configuration Status SUCCESS SUCCESS SUCCESS MONITOR MONITOR MONITOR

Field	Description
Sensor Status	Displays the sensor configuration status in a distributed color format. The sensor count is divided into three categories: • Green color (Success): Number of sensor paths that got configured successfully • Yellow color (Pending): Number of sensor paths that are pending to be configured • Red color (Failed): Number of sensor paths that could not be configured
Status Reason	Displays the failure reasons for telemetry configuration status and receiver connection status or other information.

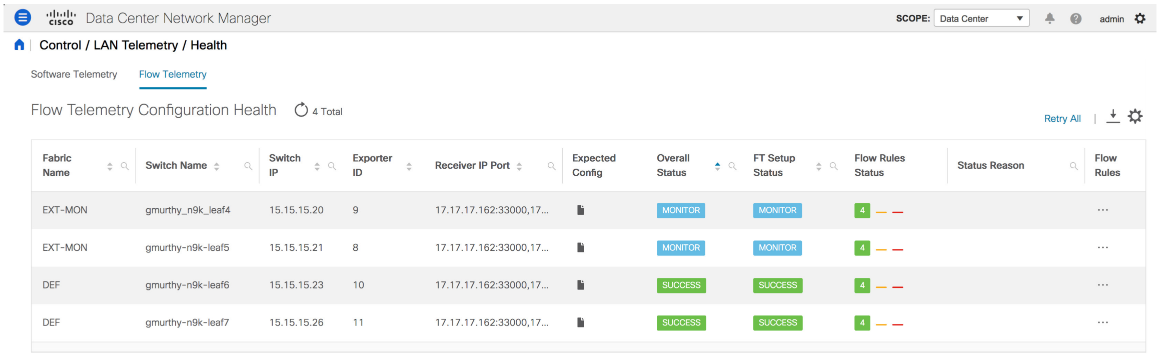
Field	Description
Sensor Details	Displays the following sensor details: • **Group ID**: The group ID to which the sensor path belongs • **Name**: The sensor path name as seen on the switch, for example: **show processes cpu** • **Cadence (Seconds)**: The sample interval, in seconds, at which the switch streams that sensor path. For example: If the value is 60, every 60 seconds the switch shall stream that sensor metric. • **Packets**: Specifies the number of metric samples that is collected till time. • **Job ID**: This is the DCNM telemetry job ID that was used to configure the sensor path on the switch. • **Status**: The status of the job. • **Status Reason**: The status reason of the job. In case the job failed, it specifies the failure reason of that job. 

Switch: gmurthy-n9k-leaf6, Fabric: DEF

Sensor Details 43 Total

Group ID	Name	Cadence (Seconds)	Packets	Job ID
510	show interface hardwar...	32	11	59
510	show hosts	32	11	59
510	show lldp neighbors	32	11	59
510	show system internal elt...	32	11	59

Flow Telemetry



Data Center Network Manager

SCOPE: Data Center

admin

Control / LAN Telemetry / Health

Software Telemetry | Flow Telemetry

Flow Telemetry Configuration Health 4 Total

Retry All

Fabric Name	Switch Name	Switch IP	Exporter ID	Receiver IP Port	Expected Config	Overall Status	FT Setup Status	Flow Rules Status	Status Reason	Flow Rules
EXT-MON	gmurthy_n9k_leaf4	15.15.15.20	9	17.17.17.162:33000,17...		MONITOR	MONITOR	4 — —		···
EXT-MON	gmurthy-n9k-leaf5	15.15.15.21	8	17.17.17.162:33000,17...		MONITOR	MONITOR	4 — —		···
DEF	gmurthy-n9k-leaf6	15.15.15.23	10	17.17.17.162:33000,17...		SUCCESS	SUCCESS	4 — —		···
DEF	gmurthy-n9k-leaf7	15.15.15.26	11	17.17.17.162:33000,17...		SUCCESS	SUCCESS	4 — —		···

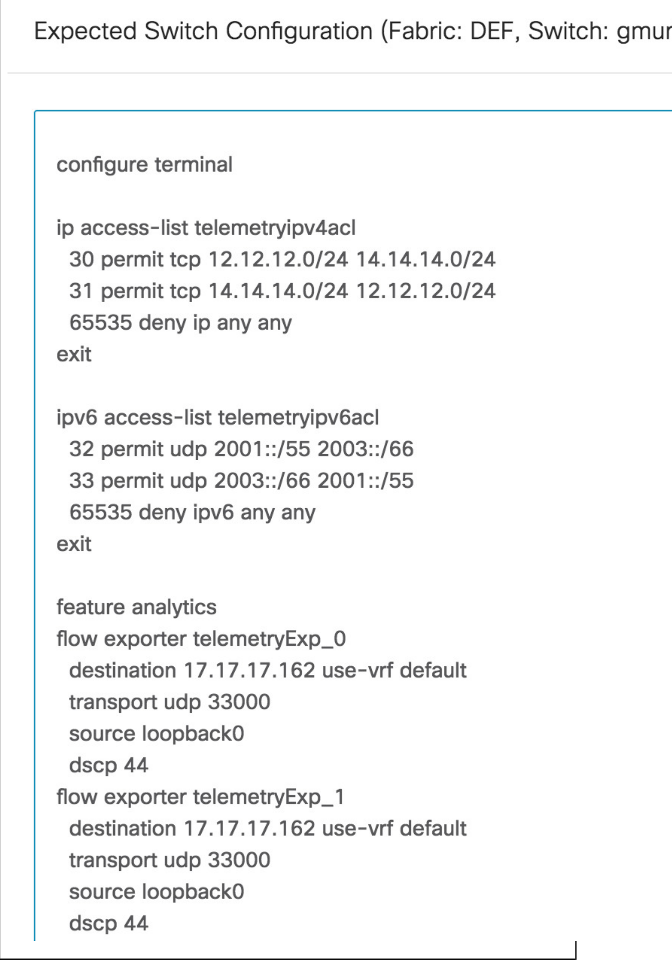
The following icons appear in the **LAN Telemetry** > **Health** > **Flow Telemetry** window.

- **Retry All**: Click the **Retry All** icon to retry the failed configurations on the switches. However, this option does not fix the issue for the unsupported configurations automatically.
- **Export**: Click the **Export** icon to download the data in a spreadsheet.
- **Settings**: Click the **Settings** icon to add or delete the columns you want to view.

The following table describes the columns in the **LAN Telemetry** > **Health** > **Flow Telemetry** tab.

Table 21: Fields and Description on Flow Telemetry Health tab

Field	Description
Fabric Name	Displays the name of the fabric.
Switch Name	Displays the name of the switch.
Switch IP	Displays the switch management IP address.
Switch Serial	Displays the serial number of the switch. By default, this column is hidden. It can be selected by clicking the Settings button.
Switch Model	Displays the switch model. By default, this column is hidden. It can be selected by clicking the Settings button.
Switch Version	Displays the switch image version. By default, this column is hidden. It can be selected by clicking the Settings button.
Exporter ID	Displays the exporter ID that is configured on the switch as part of the flow analytics configuration.

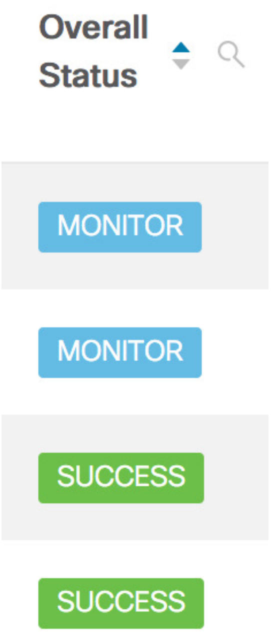
Field	Description
Receiver IP Port	Displays the comma-separated list of receiver IP addresses and ports assigned to a switch to transport flow telemetry data. The assigned IP addresses and ports will be that of the corresponding receiver microservices that are running in the NIR application and listening on the in-band network.
Expected Config	On clicking, it displays the expected configuration for the switch in a pop-up window. In case of an error, the reason for the error is displayed in the output. 

Expected Switch Configuration (Fabric: DEF, Switch: gmur

```
configure terminal

ip access-list telemetryipv4acl
  30 permit tcp 12.12.12.0/24 14.14.14.0/24
  31 permit tcp 14.14.14.0/24 12.12.12.0/24
  65535 deny ip any any
exit

ipv6 access-list telemetryipv6acl
  32 permit udp 2001::/55 2003::/66
  33 permit udp 2003::/66 2001::/55
  65535 deny ipv6 any any
exit

feature analytics
flow exporter telemetryExp_0
  destination 17.17.17.162 use-vrf default
  transport udp 33000
  source loopback0
  dscp 44
flow exporter telemetryExp_1
  destination 17.17.17.162 use-vrf default
  transport udp 33000
  source loopback0
  dscp 44
```

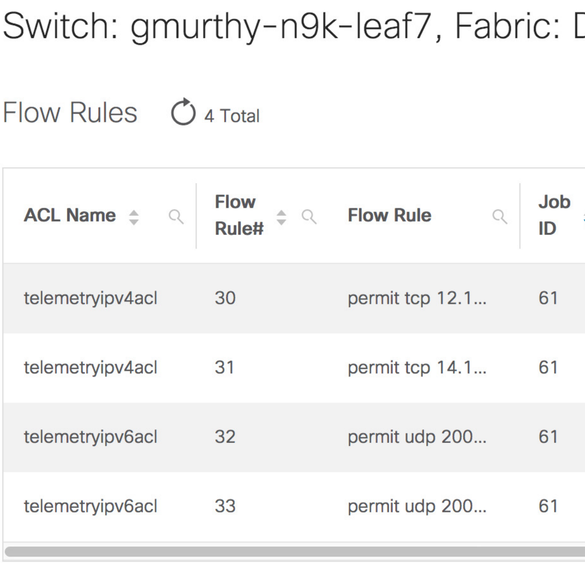
Field	Description
Overall Status	

Field	Description
	The flow telemetry configuration involves 2 components namely the Flow telemetry setup and Flow ACL configurations. The overall status column displays the summary of both these statuses. The following statuses are displayed: **MONITOR**: Implies that the switch in the fabric was configured as "Monitored" in the NIR app. In this case, it is your responsibility to configure these switches manually with the telemetry configurations as displayed in the Expected Config column. **PROCESSING**: This indicates that the switch belonging to the fabric was configured as "Managed" in the NIR app. In this case, the telemetry manager will configure the switches and when configuration is in progress, it is displayed as "PROCESSING". **SUCCESS**: This indicates that the switches were successfully configured. **PARTIAL SUCCESS**: This indicates that some of the telemetry configurations could not be pushed to the switches. The Status Reason column will indicate the failure reason. **FAILED**: This indicates that the DCNM job failed to configure the switches. It could happen that some configuration did get pushed to the switches while some did not, in that case also DCNM marks the whole job as Failed. The Status Reason column will indicate the failure reason. You can filter the switches based on a particular status using the search option (or) you can sort the switches based on the status.

Field	Description
	
FT Setup Status	Displays the Flow telemetry setup status. If this shows **Failed**, it indicated that the flow analytics could not be enabled on the switches correctly and hence, the flow data cannot be exported from the switches.
Flow Rules Status (or) Flow ACL Status	Displays the Flow ACL configuration status in a color-coded format. The flow rules status count is divided into 3 categories: • Green (Success): Number of flow rules (ACEs) that got configured successfully. • Yellow (Pending): Number of flow rules (ACEs) that are pending to be configured. • Red (Failed): Number of flow rules (ACEs) that could not be configured.
Status Reason	Displays the failure reasons for the flow telemetry configuration (or) other information.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Flow Rules</td><td>Displays the following flow rule details:

- **ACL Name**: The name of the access-list as configured on the switch. Only 2 ACLs get created namely telemetryipv4acl for IPv4 and telemetryipv6acl for IPv6.
- **Flow Rule#**: This is the ACE rule number as configured within a particular ACL.
- **Flow Rule**: This is the ACE rule that indicates the flow details like the protocol, source IP, source port, destination IP, destination port that should be exported.
- **Job ID**: This is the DCNM telemetry job id that was used to configure the flow rules on the switch.
- **Status**: The status of the job.
- **Reason**: The status reason of the job. In case the job failed, it displays the failure reason of that job. If successful, it may show compliance and deployment successful in the case of Lan Fabric deployments.



Switch: gmurthy-n9k-leaf7, Fabric: D

Flow Rules 4 Total

<table>
<tr><th>ACL Name</th><th>Flow Rule#</th><th>Flow Rule</th><th>Job ID</th></tr>
<tr><td>telemetryipv4acl</td><td>30</td><td>permit tcp 12.1...</td><td>61</td></tr>
<tr><td>telemetryipv4acl</td><td>31</td><td>permit tcp 14.1...</td><td>61</td></tr>
<tr><td>telemetryipv6acl</td><td>32</td><td>permit udp 200...</td><td>61</td></tr>
<tr><td>telemetryipv6acl</td><td>33</td><td>permit udp 200...</td><td>61</td></tr>
</table>
</td></tr>
</table>

Note In case of MONITOR mode, you can configure flow telemetry on the switches using the following API that is available at https://<dcnm-ip>/api-docs: /telemetry/switches/{serialNumber}/flow-analytics-config -> where serialNumber is the switch serial number as a string.

The Health table data gets refreshed every 70 seconds automatically. It can be manually refreshed by clicking the Refresh icon.

SAN

The SAN menu includes the following submenus:

VSANs

Beginning with Cisco DCNM Release 11, you can configure and manage Virtual SANs (VSANs) from the Cisco DCNM. From the menu bar, choose **Configure** > **SAN** > **VSAN** to view VSAN information. You can view or configure VSAN for the discovered fabrics, with either **Manageable** or **Manage Continuously** status. For the selected fabric, a VSAN Scope tree is displayed in the left panel.

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs) on Cisco Data Center Switches and Cisco MDS 9000 Family switches. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs, you can create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FC IDs) to be used simultaneously in different VSANs.

Note Cisco DCNM doesn’t discover, nor display any suspended VSAN.

Note When changing VSAN of the Switch port in DCNM, If the port was associated with Isolated VSAN, then the previous VSAN column will be blank.

The information that is associated with the selected VSAN scope appears in the right panel. If a VSAN is segmented, each individual segmented VSAN is a VSAN scope. For every selected VSAN scope, you can view information in tabs.

- Switches tab
- ISLs Tab
- Host Ports Tab
- Storage Tab
- Attributes Tab
- Domain ID Tab
- VSAN Membership Tab

For description on all fields that appear on the tabs, refer Field and Descriptions for VSANs, on page 218.

Information About VSANs

With the introduction of VSANs, the network administrator can build a single topology containing switches, links, and one or more VSANs. Each VSAN in this topology has the same behavior and property of a SAN. A VSAN has the following additional features:

- Multiple VSANs can share the same physical topology.
- The same Fibre Channel IDs (FC IDs) can be assigned to a host in another VSAN, thus increasing VSAN scalability.
- Every instance of a VSAN runs all required protocols such as FSPF, domain manager, and zoning.
- Fabric-related configurations in one VSAN don't affect the associated traffic in another VSAN.
- Events causing traffic disruptions in one VSAN are contained within that VSAN and aren't propagated to other VSANs.

A VSAN is in the operational state if the VSAN is active and at least one port is up. This state indicates that traffic can pass through this VSAN. This state can't be configured.

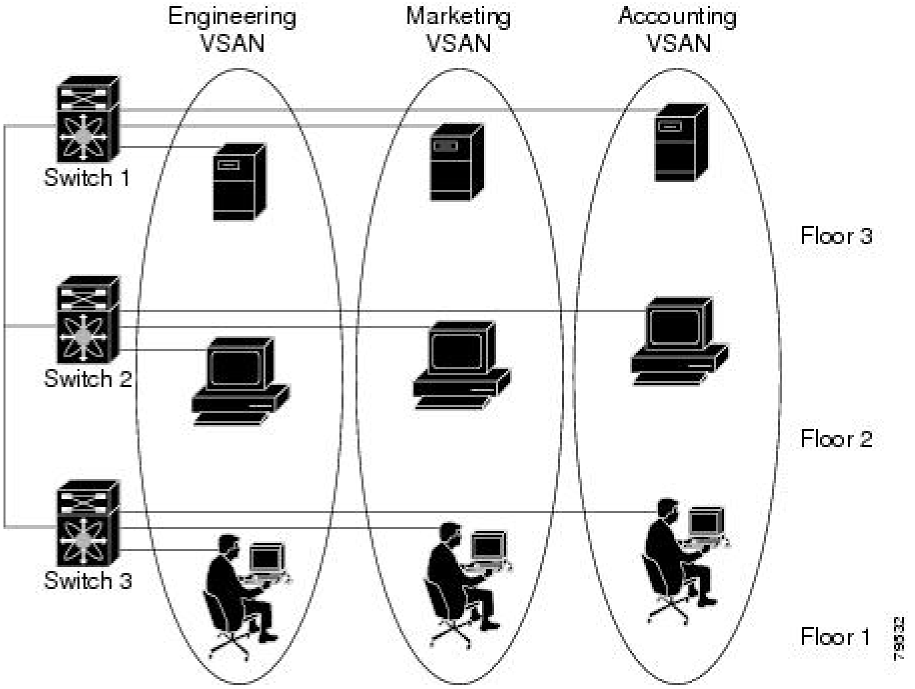
Interoperability enables the products of multiple vendors to come into contact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces. You can enable FICON in up to eight VSANs.

This section describes VSANs and includes the following topics:

VSAN Topologies

The following figure shows a fabric with three switches, one on each floor. The geographic location of the switches and the attached devices is independent of their segmentation into logical VSANs. No communication between VSANs is possible. Within each VSAN, all members can talk to one another.

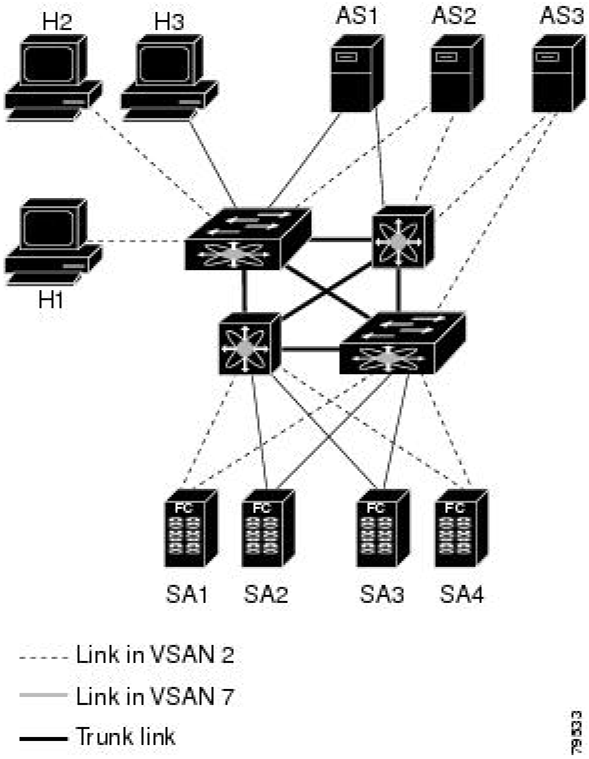
Figure 1: Logical VSAN Segmentation



The following shows a physical Fibre Channel switching infrastructure with two defined VSANs: VSAN 2 (dashed) and VSAN 7 (solid). VSAN 2 includes hosts H1 and H2, application servers AS2 and AS3, and storage arrays SA1 and SA4. VSAN 7 connects H3, AS1, SA2, and SA3.

The four switches in this network are interconnected by trunk links that carry both VSAN 2 and VSAN 7 traffic. The inter-switch topology of both VSAN 2 and VSAN 7 are identical. This isn’t a requirement and a network administrator can enable certain VSANs on certain links to create different VSAN topologies.

Figure 2: Example of Two VSANs



Without VSANs, a network administrator would need separate switches and links for separate SANs. By enabling VSANs, the same switches and links may be shared by multiple VSANs. VSANs allow SANs to be built on port granularity instead of switch granularity. The above figure illustrates that a VSAN is a group of hosts or storage devices that communicate with each other using a virtual topology defined on the physical SAN.

The criteria for creating such groups differ based on the VSAN topology:

- VSANs can separate traffic based on the following requirements:
  - Different customers in storage provider data centers
  - Production or test in an enterprise network
  - Low and high security requirements
  - Back up traffic on separate VSANs
  - Replicating data from user traffic
- VSANs can meet the needs of a particular department or application.

VSAN Advantages

VSANs offer the following advantages:

- Traffic isolation—Traffic is contained within VSAN boundaries and devices reside only in one VSAN ensuring absolute separation between user groups, if desired.

- Scalability—VSANs are overlaid on top of a single physical fabric. The ability to create several logical VSAN layers increases the scalability of the SAN.
- Per VSAN fabric services—Replication of fabric services on a per VSAN basis provides increased scalability and availability.
- Redundancy—Several VSANs created on the same physical SAN ensure redundancy. If one VSAN fails, redundant protection (to another VSAN in the same physical SAN) is configured using a backup path between the host and the device.
- Ease of configuration—Users can be added, moved, or changed between VSANs without changing the physical structure of a SAN. Moving a device from one VSAN to another only requires configuration at the port level, not at a physical level.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range 2–4093.

VSAN Configuration

VSANs have the following attributes:

- VSAN ID—The VSAN ID identifies the VSAN as the default VSAN (VSAN 1), user-defined VSANs (VSAN 2–4093), and the isolated VSAN (VSAN 4094).
- State—The administrative state of a VSAN can be configured to an active (default) or suspended state. Once VSANs are created, they may exist in various conditions or states.
    - The active state of a VSAN indicates that the VSAN is configured and enabled. By enabling a VSAN, you activate the services for that VSAN.
    - The suspended state of a VSAN indicates that the VSAN is configured but not enabled. If a port is configured in this VSAN, it’s disabled. Use this state to deactivate a VSAN without losing the VSAN’s configuration. All ports in a suspended VSAN are disabled. By suspending a VSAN, you can preconfigure all the VSAN parameters for the whole fabric and activate the VSAN immediately.
- VSAN name—This text string identifies the VSAN for management purposes. The name can be 1–32 characters long and it must be unique across all VSANs. By default, the VSAN name is a concatenation of VSAN and a four-digit string representing the VSAN ID. For example, the default name for VSAN 3 is VSAN0003.

Note A VSAN name must be unique.

- Load balancing attributes—These attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load-balancing path selection.

Note OX ID-based load balancing of IVR traffic from IVR-enabled switches isn’t supported on Generation 1 switching modules. OX ID-based load balancing of IVR traffic from a non-IVR MDS 9000 Family switch should work. Generation 2 switching modules support OX ID-based load balancing of IVR traffic from IVR-enabled switches.

- Load-balancing attributes indicate the use of the source-destination ID (src-dst-id) or the originator exchange OX ID (src-dst-ox-id, the default) for load-balancing path selection.

Port VSAN Membership

Port VSAN membership on the switch is assigned on a port-by-port basis. By default, each port belongs to the default VSAN. You can assign VSAN membership to ports using one of two methods:

- Statically—By assigning VSANs to ports
- Dynamically—By assigning VSANs based on the device WWN

  This method is referred to as dynamic port VSAN membership (DPVM).

Types of VSAN

The following are the different types of VSAN:

Default VSAN

The factory settings for switches in the Cisco MDS 9000 Family have only the default VSAN 1 enabled. We recommend that you don't use VSAN 1 as your production environment VSAN. If no VSANs are configured, all devices in the fabric are considered part of the default VSAN. By default, all ports are assigned to the default VSAN.

Note VSAN 1 can't be deleted, but it can be suspended.

Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range 2–4093.

Isolated VSAN

VSAN 4094 is an isolated VSAN. All nontrunking ports are transferred to this VSAN when the VSAN to which they belong is deleted. This avoids an implicit transfer of ports to the default VSAN or to another configured VSAN. All ports in the deleted VSAN are isolated (disabled).

Note When you configure a port in VSAN 4094 or move a port to VSAN 4094, that port is immediately isolated.

Caution Don't use an isolated VSAN to configure ports.

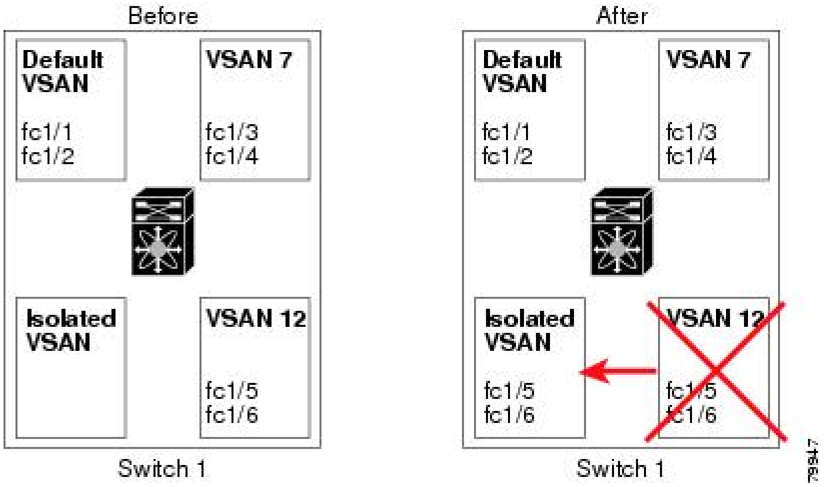
Up to 256 VSANs can be configured in a switch. Of these, one is a default VSAN (VSAN 1), and another is an isolated VSAN (VSAN 4094). User-specified VSAN IDs range 2–4093.

Static VSAN Deletion

When an active VSAN is deleted, all of its attributes are removed from the running configuration. VSAN-related information is maintained by the system software as follows:

- VSAN attributes and port membership details are maintained by the VSAN manager. This feature is affected when you delete a VSAN from the configuration. When a VSAN is deleted, all the ports in that VSAN are made inactive and the ports are moved to the isolated VSAN. If the same VSAN is recreated, the ports don't automatically get assigned to that VSAN. Reconfigure the port VSAN membership explicitly (see the following figure).

Figure 3: VSAN Port Membership Details – 79947.ps



- VSAN-based runtime (name server), zoning, and configuration (static routes) information is removed when the VSAN is deleted.
- Configured VSAN interface information is removed when the VSAN is deleted.

Note The allowed VSAN list isn't affected when a VSAN is deleted.

Any commands for a non-configured VSAN are rejected. For example, if VSAN 10 isn't configured in the system, then a command request to move a port to VSAN 10 is rejected.

Feature Information for Configuring and Managing VSANs

The following table shows the licensing requirements for this feature:

License Description

ENTERPRISE_PKG The enterprise license is required to enable VSAN. For a complete explanation of the licensing scheme, see the Cisco DCNM Licensing Guide.

License	License Description
ENTERPRISE_PKG	The enterprise license is required to enable VSAN. For a complete explanation of the licensing scheme, see the Cisco DCNM Licensing Guide.

Default VSAN Settings

The following table lists the default settings for all configured VSANs.

Parameters	Default
Default VSAN	VSAN 1.
State	Active State
Name	Concatenation of VSAN and a four-digit string representing the VSAN ID. For example, VSAN 3 is VSAN0003.
Load-balancing attribute	OX ID (src-dst-ox-id).

Create VSAN Wizard

VSAN Creation Wizard Work flow includes:

- Specify VSAN ID and name.
- Select Switches.
- Specify VSAN attributes.
- Specify VSAN Domain.
- Specify VSAN Members.

Beginning with Release 11, you can configure VSAN using a wizard that facilitates creating VSANs on multiple switches in a managed Fabric. Choose **Configure** > **SAN** > **VSAN**. After you select a Fabric from the drop-down list, click **Create VSAN Wizard** icon. The Welcome screen of the wizard is displayed.

Note Ensure that the VSAN isn't already created.

Note Ensure that you provide Switch credentials, if you are different from the Discover user. To provide SAN credentials, navigate to **Administration** > **Credentials Management** > **SAN Credentials**.

To create and configure VSANs from the Cisco DCNM Web UI, perform the following steps:

Before you begin

You cannot configure any application-specific parameters for a VSAN before creating the VSAN.

Ensure that the VSAN isn't already created. Do not create the VSAN in suspended state.

Note The suspended VSANs aren't managed.

Procedure

Step 1 On the Create VSAN Wizard Welcome screen, click **Next**.

The **Select VSAN ID and Name** window is displayed.

Step 2 In the Select VSAN ID and Name window, perform the following steps:

a) Ensure that the correct Fabric is against the Fabric field.
b) In the VSAN ID field, select VSAN ID from the drop-down list.

   The range is 2–4094. Create the list of VSAN ID in at least one Switch in the Fabric. VSAN ID 4079 is for reserved VSAN.

c) In the Name field, enter a name for VSAN.

   Note If the field is left blank, the Switch assigns a default name to the VSAN.

d) Click FICON checkbox to enable FICON on the switch.
e) Click Next.

Step 3 In the Select Switches screen, click the checkbox next to the Switch Name, to create the VSAN.

If the switch name is grayed out, it implies that the switch is already a part of VSAN. It may also imply that the switch doesn’t have FICON feature enabled, if FICON is checked in the previous step.

Click **Next**.

Step 4 In the Config VSAN Attributes screen, configure the VSAN attributes.

Note If you create a VSAN in a suspended state, it doesn’t appear on the Cisco DCNM as DCNM doesn’t manage suspended VSANs.

a) In the LoadBalancing, select the load balancing type to be used on the VSAN.

   The following types are available:

   - srcIdDestId: based on only source ID (S_ID) and destination ID (D_ID)
   - srcIdDestIdOxId: Originator exchange ID (OX_ID) is also used for load balancing, in addition to S_ID and D_ID. OX_ID is an exchange ID assigned by the originator Interconnect Port for an exchange with the target Interconnect Port.

   Note srcId/DestId/OxId is the default for non-FICON VSAN and it isn’t available for FICON VSAN, srcId/DestId is the default for FICON VSAN.

b) In the InterOp field, select the interoperability value the drop-down list.

   The InterOp value is used to interoperate with different vendor devices. You can choose from one of the following:

   - 0: implies that the interoperability is disabled.
   - 1: implies that the VSAN can interoperate with all the Fibre Channel vendor devices.
   - 2: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
   - 3: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.

- 4: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.

Note InterOp isn't supported on FICON VSAN.

c) In the Admin State field, select the configurable state for this VSAN.

- active: implies that the VSAN is configured and services for this VSAN is activated.
- suspended: implies that the VSAN is configured, but the service for this VSAN is deactivated.

  Choose this state to preconfigure all the VSAN parameters for the whole Fabric.

  Note DCNM doesn't manage a suspended VSAN, and therefore it does not appear in the VSAN scope.

d) Check the Inorder Delivery checkbox to allow in-order delivery.

When the value of fcInorderDelivery is changed, the value of this object is set to the new value of that object.

e) In the Add Fabric Binding DB field, check the checkbox if you want to enable the fabric binding for the FICON VSAN.

If the checkbox is selected, the all the peers in the selected switches are added to each switch in the selected list.

f) In the All Port Prohibited field, check the checkbox if you want to prohibit all the ports for FICON VSAN.

If the checkbox is selected, the FICON VSAN is created as all Ports prohibited, by default.

g) Click **Next**.

Step 5 In the Config VSAN Domain screen, configure the static domain IDs for FICON VSAN.

a) Select the Use Static Domain IDs field, to configure the domain ID for the switches in the VSAN.
b) The Available Domain IDs field shows all the available Domain IDs in the Fabric.

Click **Apply Available Domain IDs** to assign the domain ID for every switch that is selected to be a part of the VSAN.

c) For every switch in the table, enter the domain ID from the list of available Domain IDs.
d) Click **Next**.

Step 6 In the Config Port VSAN Membership screen, for every switch in the VSAN, configure the interfaces, as the member of the new VSAN.

Note Modifying the Port VSAN may affect the I/O of the interface.

Click **Next**.

Step 7 In the Summary screen, verify if you have configured the VSAN correctly.

Click **Previous** to navigate to the earlier screen and modify the configuration.

Click **Cancel** to discard the configuration.

Click **Finish** to confirm and configure the VSAN. The VSAN creation result is displayed at the bottom of the window.

Note After the VSAN is created, it will take few minutes for the new VSAN to appear in the VSAN scope tree.

Note If the switch port is associated with Isolated VSAN then the previous VSAN information will be blank.

Delete VSAN

To delete a VSAN and its attributes from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **SAN** > **VSAN**.

The **VSAN** window is displayed.

Step 2 From the Fabric drop-down list, select the Fabric to which the VSAN is associated.

The VSAN scope tree for the selected Fabric is displayed in the VSAN area.

Step 3 Expand the Fabric and select the VSAN that you want to delete.

Note You can’t delete Segmented VSAN.

Step 4 Click the **Delete VSAN** icon.

The Delete VSAN screen appears, showing the switches associated with the VSAN.

Step 5 Select the checkbox of the Switch for which you want to remove the VSAN.

Click **Delete**.

A confirmation window appears.

Step 6 Click **Yes** to confirm the deletion or click **No** to close the dialog box without deleting the VSAN.

Note After the VSAN is deleted, it will take few minutes for the new VSAN to disappear from the VSAN scope tree.

Field and Descriptions for VSANs

The Field and Descriptions for all the tabs that are displayed on **Cisco Web UI** > **SAN** > **VSAN** are explained in the following tables.

- Switches tab, on page 219
- ISLs Tab, on page 219
- Host Ports Tab, on page 220
- Storage Tab, on page 220
- Attributes Tab, on page 221
- Domain ID Tab, on page 222

- VSAN Membership Tab, on page 223

Switches tab

This tab displays Switches in the VSAN scope. Click the Switch name to view the summary information of the switch. The following table describes the fields that appear on the Switches tab.

Table 22: Field and Description on Switches Tab

Field	Description
Name	Specifies the name of the switch in the VSAN. Click the name to view the switch summary. For description about the fields in the Switch Summary, refer to Viewing Inventory Information for Switches, on page 45. Click **Show more Details** to view complete information.
Domain ID	Specifies an insistent domain ID.
VSAN WWN	Specifies the WorldWide Name (WWN) of the VSAN.
Principal WWN	Specifies the WorldWide Name (WWN) of the switch. **Note** For the principal switch, the value is "self".
Model	Specifies the model name of the switch.
Release	Specifies the NX-OS version on the switch.
Uptime	Specifies the time from which the switch is up.
Icons	
Total	The number next to Total specifies the entries under this tab.
Refresh	Click the Refresh icon to refresh the entries.

ISLs Tab

This tab displays information about the ISLs about the switches in the VSAN scope. Click the Switch name to view the summary information. **Click Show more details** to view complete information on the selected switch. The following table describes the fields that appear on the ISLs tab. If the VSAN is configured on both the switches across the ISL and if VSAN is not enabled on the ISL, DCNM considers VSAN as segmented. Therefore, add the VSAN to the trunked VSANs across the ISL to clear the warning message. Alternatively, you can ignore this warning message.

Table 23: Field and Description on ISLs Tab

Field	Description
VSANs	All VSANs which this ISL runs traffic on.
From Switch	The source switch of the link.
From Interface	The port index of source E_port of the link.
To Switch	The switch on the other end of the link.

Field	Description
To Interface	The port index of destination E_port of the link.
Speed	The speed of this ISL.
Status	The operational status of the link.
Port Channel Members	The member of Port Channel if ISL is a Port Channel.
Additional Info	Additional information for this ISL, e.g., TE/TF/TNP ISL
Icons	
Total	The number next to Total specifies the entries under this tab.
Refresh Icon	Click the Refresh icon to refresh the entries.

Host Ports Tab

This tab displays information about the host ports on the switches in the VSAN scope. The following table describes the fields that appear on the Host Ports tab.

Table 24: Field and Description on Host Ports Tab

Field	Description
Enclosure	The name of the enclosure.
device Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
FcId	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.
Vendor	Specifies the name of the vendor.
Model	Specifies the name of the model.
Firmware	The version of the firmware that is executed by this HBA.
Driver	The version of the driver that is executed by this HBA.
Additional Info	The information list corresponding to this HBA.
Icons	
Total	The number next to Total specifies the entries under this tab.
Refresh	Click the Refresh icon to refresh the entries.

Storage Tab

This tab displays information about the storage ports on the switches in the VSAN scope. The following table describes the fields that appear on the Storage Ports tab.

Table 25: Field and Description on Storage Tab

Field	Description
Enclosure	The name of the enclosure.
device Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
FcId	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.
Icons	
Total	The number next to Table specifies the entries under this tab.
Refresh	Click the Refresh icon to refresh the entries.

Attributes Tab

This tab displays the attributes of all the switches in the VSAN scope. The following table describes the fields that appear on the Attributes tab.

Table 26: Field and Description on Attributes Tab

Field	Description
Edit	Click **Edit** to modify the attributes of the VSAN and to push the same VSAN attributes to the selected switches. If the VSAN is FICON VSAN in any selected switch, the following fields won't appear on the UI, as they can't be modified for the FICON VSAN. • Load-balancing • InterOp • InorderDelivery After modify the attributes, you can click **Apply** to save changes or **Cancel** to discard.
Switch Name	Displays the name of the switch that is associated with the VSAN.
Name	Displays the name of the VSAN.
Admin	Specifies if the status of the Admin is either Active or Suspend. • **active** implies that the VSAN is configured and services for the VSAN is activated. • **suspended** implies that the VSAN is configured; however, the service for the VSAN is deactivated. You can use set this state to preconfigure all the VSAN parameters by using the CLI only. **Note** If you suspend a VSAN, it's removed from Cisco DCNM as well.

Field	Description
Oper	The operational state of the VSAN.
MTU	Displays the MTU for the switch.
LoadBalancing	Specifies the load-balancing type that is used in the VSAN. The type of load balancing used on this VSAN. • srcId/DestId—use source and destination ID for path selection • srcdId/DestId/0xld—use source, destination, and exchange IDs
InterOp	The interoperability mode of the local switch on this VSAN. • standard • interop-1 • interop-2 • interop-3
InorderDelivery	The InorderDelivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it's not guaranteed.
FICON	True if the VSAN is FICON-enabled.
Icons	
Total	The number next to Table specifies the entries under this tab.
Refresh Icon	Click the Refresh icon to refresh the entries.

Domain ID Tab

This tab displays information about the VSAN domain and its parameters. The following table describes the fields that appear on the Domain ID tab.

Table 27: Field and Description on Domain ID Tab

Field	Description
Edit	Click Edit icon to modify the Domain ID information for the selected switch.
Switch Name	Specifies the switch name in the VSAN. **Note** NPV switches aren't listed in this column. However, the NPV switches exist in this VSAN fabric.
State	Specifies the state of the Switch.
Enable	Specifies if the Domain ID is enabled or disabled.
Running	Specifies the running domain.
Config Type	Specifies the usage of the domain ID type—**preferred** or **static**.

Field	Description
Icons	
Total	The number next to Table specifies the entries under this tab.
Refresh Icon	Click the Refresh icon to refresh the entries.

VSAN Membership Tab

This tab displays information about the interfaces on the switches that form the VSAN. The following table describes the fields that appear on the VSAN Membership tab.

Table 28: Field and Description on VSAN Membership Tab

Field	Description
Edit	Click Edit icon to modify Port VSAN Membership for selected VSAN and selected switch. Port VSAN Membership is presented by different types including FC (physical), PortChannel, FCIP, iSCSI, VFC (slot/port), VFC (ID), VFC (Channel), VFC FEX, and VFC Breakout, PortChooser is provided for each type to show all existing interfaces on a selected switch for the user to choose from. **Note** If you modify Post VSAN Membership for any operational trunking port or port channel members, a warning appears. Use the Device Manager to change Allowed VSAN List for Trunking Interface.
Switch Name	Name of the switch
Interfaces	FC Ports in VSAN
Icons	
Total	The number next to Table specifies the entries under this tab.
Refresh Icon	Click the Refresh icon to refresh the entries.

SAN Zoning

Zoning enables you to set up access control between storage devices or user groups. If you have administrator privileges in your fabric, you can create zones to increase the network security and to prevent data loss or corruption. Zoning is enforced by examining the source-destination ID field.

Note When device aliases are used for zoning in web GUI/SAN Client, end devices must be logged into the fabric thus web GUI can configure zoning using device aliases. If end nodes are not logged in, PWWN can be used for zoning.

The following table describes the fields and icons that appear on Cisco DCNM **Configure** > **SAN** > **Zoning** tab.

Field	Description
Fabric	From the Fabric drop-down list, you can choose the fabric for which you are configuring or viewing the SAN Zoning.
VSAN	From the VSAN drop-down list, you can choose the VSAN for which you are configuring zoning.
Switches	From the Switch drop-down list, select the switch to which you want to configure.
Commit Changes	Commits the Zoning configuration changes to all the switches. This field is only applicable when a zone is in the enhanced or smart mode.
Distribute	Distributes the Zoning configuration to all the switches. This field is only applicable when a zone is in the basic mode.
Export All	You can export the Zoning configurations to a .csv file, and save it on your local directory.
Zonesets	Lists all the Zoneset configured for the selected Fabric, VSAN, and the Switch.
Zones	Lists all the Zones that are configured under the selected Zoneset.
Zone Members	Lists the members present in the selected Zone.
Available to Add	Lists the available devices to add to the Zones.
Clear Server Cache	Clears the cache on the Cisco DCNM server.
Discard Pending Changes	Discards the changes in progress.

This section contains the following:

Zonesets

Based on the selected Fabric, VSAN and Switch, the Zoneset area displays the configured zonesets and their status. You can create, copy, delete or edit the zonesets. Further, the zonesets can be activated or deactivated.

Procedure

Step 1 To create zonesets from Cisco DCNM Web UI, choose **Configure > SAN Zoning > Zonesets** and click **Create Zoneset** icon.

The **Create Zoneset** window appears.

Step 2 Enter a valid name for the zoneset, and click **Create**.

A zoneset is created and is listed in the **Zoneset** area.

Step 3 Choose the zone radio button and click **Clone\Copy Zoneset** icon to clone or copy zonesets.

The Clone or Copy Zoneset window shows two options.

- Choose the appropriate **Action** radio button. You can choose of the of the following:
  - **Copy**: Creates a new zoneset that consists copies of the zones in the initial zoneset.

    You can prepend or append a string to identify the copied zoneset. Enter a valid string in the **Tag** field, and choose the **Prepend** or **Append** radio button.
  - **Clone**: To create a new zoneset with a new name consisting of the same zones as the source zoneset.

    In the **Name** field, enter a valid name for the new zoneset.
- Click **OK** to clone or copy the zoneset.

  The cloned or the copied zoneset appears in the **Zoneset** area.

Step 4 To delete the zoneset, choose the zoneset radio button and click delete zoneset icon.

A confirmation window appears. Click **Yes** to delete the zoneset.

Step 5 To edit the zone name, choose the zone radio button and click **Rename Zoneset** icon.

In the **Name** field, enter the new name for the zoneset. Click **Rename**.

Step 6 To activate a zoneset, choose the zoneset radio button and click **Activate**.

The **Zoneset Differences** window shows the changes made to the zoneset since it was activated previously. Click **Activate**.

Step 7 To deactivate a zoneset, choose the zoneset radio button and click **Deactivate**.

A confirmation window appears. Click **Yes** to deactivate the zoneset.

Zones

Based on the Zoneset that is selected, the zones that are configured under that zoneset are displayed in the **Zones** area. It also displays true or false only when the VSAN has smart zone that is enabled. You can create, copy, delete, or edit the zones. Furthermore, the zones can be added to or removed from the selected Zoneset. You can also enable or disable the smart zone on the zone table.

Note Select the **Zoneset** for which you must alter the zones.

Select **Zoneset** radio button in the Zonesets area. The zones that are configured on the selected Zoneset and zones on the switch are displayed. The zones that are a part of the Zone are marked with a green check mark.

The Zones area has the following fields and their descriptions.

Field	Description
In Zoneset	Specifies whether a zone is part of a zoneset.

Field	Description
	Displays **true** if the zone is part of a zoneset. Otherwise, displays **false**. You can search by choosing true or false from the **In Zoneset** drop-down list.
Zone Name	Displays the name of the zone. You can search by specifying the zone name.
Smart Zone	Specifies whether a zone is a smart zone. Displays **true** if the zone is a smart zone. Otherwise, displays **false**. You can search this field by choosing **true** or **false** from the **Smart Zone** drop-down list. This field only shows that up when the VSAN has smart zone that is enabled.

Procedure

Step 1 To create zones, choose **Configure** > **SAN** > **Zoning** > **Zones**, click **Create** icon.

a) In the Create Zone window, enter a valid name for the Zone, and click **Create**.

A zone is created and is listed in the **Zones** area.

Step 2 To Clone Zones, choose **Configure** > **SAN** > **Zoning** > **Zones**, select the **Zone** radio button and click **Clone Zone** icon.

The **Clone Zone** window is displayed.

a) In the Name field, enter a valid name for the new zoneset.
b) Click **Clone** to clone the zone.

The cloned zones appear in the **Zones** area.

Step 3 To add zone to a zoneset, choose **Configure** > **SAN Zoning** > **Zones**, select the zone that is not a part of the zoneset. Click **Add Zone** icon. You can select more than one zone to be added to the Zoneset.

The zone is added to the selected Zoneset. A green tick mark appears next to the Zone name to indicate that the zone is added to the zoneset.

Step 4 To remove zone from a zoneset, choose **Configure** > **SAN Zoning** > **Zones**, check the **Zone** check box. Click **Remove Zone** icon. You can select more than one Zone to be deleted from the Zoneset.

The zone is removed from the selected Zoneset. A green tick mark disappears next to the Zone name to indicate that the zone is removed from the zoneset.

Step 5 To Delete Zones, choose **Configure** > **SAN Zoning** > **Zones**, check the **Zone** check box. Click **Delete Zone** icon.

A confirmation window appears.

Click **Yes** to delete the selected zones.

Note You cannot delete a zone that is a member of the selected zoneset. Remove the zone from the zoneset to delete it.

Step 6 To edit the zone name, choose **Configure > SAN Zoning > Zones**, select the **Zone** radio button. Click **Rename Zone** icon.

In the Name field, enter the new name for the zone.

Click **Rename**.

Step 7 To enable smart zone, choose **Configure > SAN Zoning > Zones**, select the **Zone** radio button. Click **Enable Smart Zone** icon.

Under the **Smart Zone** column, it displays True.

Step 8 To disable smart zone, choose **Configure > SAN Zoning > Zones**, select the **Zone** radio button. Click **Disable Smart Zone** icon.

Under the **Smart Zone** column, it displays false.

Zone Members

Based on the selected Zoneset and the Zone, the Zone Members area displays the zone members and their status. You can create, or remove members from the Zoneset.

The Zone Members area has the following fields and their descriptions.

Field	Description
Zone	Displays the Zone under which this member is present. You can search by zone name in this field.
Zoned By	Displays the type of zoning. You can search by type of zoning such as WWN, FCID, fcAlias, or iSCSI.
Device Type	Displays the smart zoning device type. The applicable values are **Host**, **Storage**, or **Both**. You can search this field by choosing **Host**, **Storage** or **Both** from the **Device Type** drop-down list. This field only shows up when the VSAN has smart zone that is enabled.
Name	Displays the name of the zone member. You can search by specifying the zone name.
Switch Interface	Specifies the switch interface that the zone member is attached to. You can search by specifying the switch interface.

Field	Description
FcId	Specifies the FcID associated with the zone member. You can search by specifying the FcID associated with the zone member.
WWN	Specifies the WWN of the switch. You can search by specifying the WWN of the switch.

Procedure

Step 1 To create zone members, from Cisco DCNM **Web Client > Configure > SAN Zoning > Zone Members**, click Create icon.

a) In the **Create and Add Member** window, enter the WWN name or Device Alias for the zone member.

Note You can add only offline members for the device alias zone.

b) Click **Create and Add**.

The create and add feature allows you to add a member to a zone that does not exist in the fabric, currently. This feature can also be utilized when the device discovery did not discover all the devices. With the Available to add feature, you can add a discovered device to the zone.

Step 2 To Remove Zone Member, from Cisco DCNM **Web Client > Configure > SAN Zoning > Zone Members**, check the **Zone Member** check box. Click **Remove Member** icon.

You can remove more than one zone member at a time, for deletion.

Available to Add

The **Available to Add** area has the following fields and their descriptions.

Field	Description
Type	Displays the smart zoning device type. The applicable values are **Host** or **Storage**. You can search this field by choosing **Host**or **Storage** from the **Type** drop-down list.
Name	Displays the name of the zone. You can search by specifying the zone name.
Switch Interface	Specifies the switch interface that the zone member is attached to. You can search by specifying the switch interface.
FcId	Specifies the FcID associated with the zone member.

Field	Description
	You can search by specifying the FcID associated with the zone member.
WWN	Specifies the WWN of the switch. You can search by specifying the WWN of the switch.

To add discovered devices to one or more zones from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > SAN > Zoning > Available to Add**.

Step 2 In the **Zone by area**, select the Ports or Device radio buttons.

The **Zone by** feature determines if the device must be added to the zone using the device WWN or Device alias.

A window appears showing the list of End Ports or Devices available to add.

If you choose **Zone By: End Port**, the devices are added to the zones by WWN. If you choose **Zone By: Device Alias**, the devices are added to the zones by Device Alias. Based on the zone by option you choose, the devices are displayed.

Step 3 Select the devices to add to a zone.

Step 4 Click **Add** to add the selected devices to the zone.

Note You can select more than one zone. A dialog appears that shows a list of all the zones that are currently selected on the zone table.

IVR Zoning

From Cisco DCNM Release 11.0(1), IVR Zoning feature is supported. You can use IVR Zoning to create, edit, copy, or delete IVR zones in the web client.

The IVR Zoning page is launched from Cisco DCNM **Configure** > **SAN** > **IVR Zoning** menu item. After you launch the IVR Zoning page, you will see the following fields and sections:

- Fabric
- Region ID
- Switches
- Commit Changes
- Export All
- Clear Server Cache
- Discard Pending Changes

- Zonesets
- Zone Members
- Zones
- Available to Add

The following table describes the fields and icons on Cisco DCNM **Configure** > **SAN** > **IVR Zoning** tab.

Field	**Description**
Fabric	From the Fabric drop-down list, you can choose the fabric for which you are configuring or viewing the IVR Zoning. You must select a fabric to view the options of Region ID and Switches.
Region ID	From the Region ID drop-down list, you can choose the region for a switch.
Switches	From the Switch drop-down list, select the switch to which you want to configure. Zone Seed switch is selected by default.
Commit Changes	Commits the IVR zoning configuration changes to all the switches. This field is only applicable when a zone is in the enhanced or smart mode.
Export All	You can export the IVR zoning configurations to a .csv file, and save it on your local directory.
Clear Server Cache	Clears the discovered zoning cache on the Cisco DCNM server.
Discard Pending Changes	Discards the changes in progress.

To display the zone sets, you need to select the desired fabric, region ID, and switch. This is different from regular zoning, which needs the fabric, VSAN, and switch.

Three checks are made when a switch is selected and can result in a warning dialog including one or more of the following warnings:

- Check for IVR Cisco Fabric Services enabled.
- Check for NAT and Auto Topology Enabled.
- Check if there is an existing IVR zone merge failure.

If the IVR Cisco Fabric Services feature is not enabled, then **Activate**, **Deactivate**, **Commit Changes**, and **Discard Pending Changes**are blocked. If IVR NAT and IVR Auto Topology are not enabled, you will get a warning to enable them.

This section contains the following:

Zonesets

Based on the selected fabric, region and switch, the **Zoneset** area displays the configured zonesets and their status. You can create, copy or clone, delete, rename, activate, or deactivate a zoneset.

The following table describes the fields and icons that appear on **Cisco DCNM Web Client** > **Configure** > **SAN** > **IVR Zoning** > **Zonesets** area.

Fields	Description
Create Zoneset	Creates a zoneset.
Copy\Clone Zoneset	• Copy—Creates a zoneset and copies of zones in the original zoneset. The copied names are the existing names that are prepended or appended with a specified string. • Clone—Creates only a zoneset with a new name consisting the same zones as the original zoneset.
Delete Zoneset	Deletes the selected zoneset.
Rename Zoneset	Renames the selected zoneset.
Zoneset	Lists all the zonesets that is configured for the selected fabric, region ID, and the switch.
Status	Displays if the zoneset is active or not.
Modified	Displays if the zoneset is modified or not.

Procedure

Step 1 To create zonesets, choose **Configure > SAN > IVR Zoning > Zonesets**. Click **Create Zoneset** icon.

a) In the Create Zoneset window, enter a valid name for the zoneset.

b) Click **Create**.

A zoneset is created and is listed in the **Zoneset** area.

Step 2 To clone or copy zonesets, choose **Configure > SAN > IVR Zoning > Zonesets**. Select the radio button of the zoneset to be copied or cloned. Click **Clone\Copy Zoneset** icon.

The **Clone\Copy Zoneset** window shows two options.

a) Click the appropriate Action radio button.

You can choose one of the following:

- **Copy**—You can prepend or append a string to identify the copied zoneset. Enter a valid string in the **Tag** field, and select the **Prepend** or **Append** radio button.
- **Clone**—In the Name field, enter a valid name for the new zoneset.

b) Click **OK** to clone or copy the zoneset.

The cloned or the copied zoneset appears in the Zoneset area.

Step 3 To delete the zoneset, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**. Select the **Zoneset** radio button. Click **Delete Zoneset** icon.

A confirmation window appears.

Click **Yes** to delete the zoneset.

Step 4 To rename the zonset name, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**. Select the zoneset radio button. Click **Rename Zoneset** icon.

In the Name field, enter the new name for the zoneset.

Click **Rename**.

Step 5 To activate a zoneset, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**. Select the zoneset radio button. Click **Activate**.

The Zoneset Differences window shows the changes that are made to the zoneset after the previous activation.

Click **Activate**.

Step 6 To deactivate a zoneset, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**. Select the zoneset radio button. Click **Deactivate**.

A confirmation window appears.

Click **Yes** to deactivate the zoneset.

Zones

All zones that are configured appear under **Zones** when a zoneset is selected. The zones that belong to the selected zoneset have a green check box. You can create, copy, delete, or edit zones. Furthermore, the zones can be added to or removed from the selected zoneset. You can also enable or disable the smart zone on the zone table.

The following table describes the fields and icons that appear on Cisco DCNM **Configure** > **SAN** > **IVR Zoning** > **Zones**:

Fields	Description
Create Zone	Creates a zone.
Clone Zone	Creates a zone with a new name consisting the same zone members as the source zone.
Add Zone	Adds a zone to the selected zoneset.
Remove Zone	Removes the selected zones from a zoneset.
Delete Zone	Deletes the selected zones that do not belong to a zoneset.
Rename Zone	Renames the selected zone.

Fields	Description
In Zoneset	Specifies whether a zone is part of a zoneset. The check box is selected if the zone is part of a zoneset. You can search by choosing true or false from the **In Zoneset** drop-down list.
Zone Name	Displays the name of the zone. You can search by specifying the zone name.
Smart Zone	Specifies whether a zone is a smart zone. Displays **true** if the zone is a smart zone. Otherwise, displays **false**. You can search this field by choosing **true** or **false** from the **Smart Zone** drop-down list. This field only is displayed when the VSAN has smart zone that is enabled.

Procedure

Step 1 To create a zone, choose **Configure** > **SAN** > **IVR Zoning** > **Zones**.

Step 2 Click **Create Zone**.

a) In the **Create Zone** window, enter a valid name for the zone.
b) Click **Create**.

A zone is created and is listed in the **Zones** area.

Step 3 To clone a zone, **Configure** > **SAN** > **IVR Zoning** > **Zones**, select a zoneset.

All the zones in the fabric appear under **Zones**. From **Zones**, select a zone and click **Clone Zone**.

Note You can clone only one zone at a time.

a) In the **Clone Zone** window, enter a valid name for the new zone.
b) Click **Clone**.

The cloned zones appear under **Zones**.

Step 4 To add a zone that is not part of a zoneset, choose **Configure** > **SAN** > **IVR Zoning** > **Zoneset**, select a zoneset.

All the zones in the fabric appear under **Zones**. From **Zones**, select a zone that is not part of the zoneset. Click **Add Zone** icon.

You can select more than one zone to be added to the zoneset.

The zone are added to the selected zoneset. A green check mark appears next to the zone name to indicate that the zone is added to the zoneset.

Step 5 To remove a zone from a zoneset, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**. Select a zoneset.

All the zones in the fabric appear under **Zones**. From **Zones**, select a zone that belongs to the selected zoneset and click **Remove Zone**.

The zone is removed from the selected zoneset. The green check mark next to the zone name disappears to indicate that the zone is removed from the zoneset.

Step 6 To delete a zone from a zoneset, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**, select a zoneset.

All the zones in the fabric appear under **Zones**. From **Zones**, select a zone that does not belong to the selected zoneset and click **Delete Zone**.

A confirmation window appears. Click **Yes** to delete the selected zones.

Note You cannot delete a zone that is a member of the selected zoneset. Remove the zone from the zoneset to delete it.

Step 7 To rename a zone, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**, select a zoneset. From **Zones**, select the zone to be renamed and click **Rename Zone**.

In the **Name** field, enter the new name for the zone.

Click **Rename**.

Step 8 To enable a smart zone, choose **Configure** > **SAN** > **IVR Zoning** > **Zones**. Select a zoneset.

From **Zones**, select a zone, and click **Enable Smart Zone**.

Under the **Smart Zone** column, it displays **True**.

Step 9 To disable a smart zone, choose **Configure** > **SAN** > **IVR Zoning** > **Zonesets**, select a zoneset.

From **Zones**, select a zone, and click **Disable Smart Zone**.

Under the **Smart Zone** column, it displays **False**.

Zone Members

Based on the selected zoneset and zone, the **Zone Members** area displays the zone members and their status.

The following table describes the fields and icons that appear on Cisco DCNM **Configure** > **SAN** > **IVR Zoning** > **Zone Members** area.

Field	Description
Create and Add Member to Zone	Creates a zone member and adds it to a zone.
Remove Member	Removes a zone member. You can remove more than one member at a time.
Zone	Displays the zone under which this member is present. You can search by zone name in this field.
Zoned By	Displays the type of zoning.

Field	Description
	You can search by type of zoning such as WWN, FCID, fcAlias, or iSCSI.
Name	Displays the name of the zone member. You can search by specifying the zone name.
Switch Interface	Specifies the switch interface that the zone member is attached to. You can search by specifying the switch interface.
VSAN	Specifies the VSAN the zone member is in.
FcId	Specifies the FcID associated with the zone member. You can search by specifying the FcID associated with the zone member.
WWN	Specifies the WWN of the switch. You can search by specifying the WWN of the switch.

To add or remove members from the zoneset from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Select a zoneset and zones to view the list of zone members.

Procedure

Step 1 To create and add zone members, choose **Configure > SAN > IVR Zoning > Zone Members**. Click **Create and Add Member to Zone**.

a) In the **Create and Add Member** window, enter the WWN name or Device Alias and VSAN for the zone member.

   You can enter the WWN name with or without colons.

   Note You can add only offline members for the device alias zone.

b) Click **Create and Add**.

The Create and Add feature allows you to add a member to a zone that does not exist in the fabric, currently. This feature can be also utilized when the device discovery did not discover all the devices. With the Available to add feature, you can add a discovered device to the zone.

Step 2 To remove a zone member, choose **Configure > SAN > IVR Zoning > Zone Members**, select a zone member. Click **Remove Member**.

Available to Add

You can add discovered devices to the zones using **Available to Add** option. The **Add Member** dialog has an additional field for VSAN to be entered, which is only visible when launched from the IVR Zoning page and not the regular Zoning page.

The following table describes the fields and icons that appear on Cisco DCNM **Configure > SAN > IVR Zoning > Available to Add**.

Field	Description
Add Member	Adds a device to a zone.
Zone By	The **Zone by** feature determines if the device must be added to the zone using the device WWN or device alias. If you choose **Zone By: End Ports**, the devices are added to the zones by WWN. If you choose **Zone By: Device Alias**, the devices are added to the zones by device alias.
Type	Displays the smart zoning device type. The applicable values are **Host** or **Storage**. You can search this field by choosing **Host**or **Storage** from the **Type** drop-down list.
Name	Displays the name of the zone. You can search by specifying the zone name.
Switch Interface	Specifies the switch interface that the zone member is attached to. You can search by specifying the switch interface.
VSAN	Specifies the VSAN the zone member is in.
FcId	Specifies the FcID associated with the zone member. You can search by specifying the FcID associated with the zone member.
WWN	Specifies the WWN of the switch. You can search by specifying the WWN of the switch.

Procedure

Step 1 Choose **Configure > SAN > IVR Zoning > Available to Add**.

Step 2 In the **Zone by** field, select **End Ports** or **Device Alias** radio button.

A window appears showing the list of end ports or devices available to add.

Step 3 Select the devices to be added to a zone.

Step 4 Click **Add**.

Note Specify the device type for smart zoning if smart zone is enabled for that zone.

You can select more than one zone. When this occurs, a dialog appears that shows a list of all the zones that are currently selected on the zone table.

Configuring FCIP

Cisco DCNM allows you to create FCIP links between Gigabit Ethernet ports, enables Fibre Channel write acceleration and IP compression.

To configure FCIP from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > SAN > FCIP**.

The Welcome page displays the tasks to configure FCIP using the FCIP Wizard.

Step 2 Click **Next** to select the switch pair.

Note FCIP is not supported on Cisco MDS 9000 24/10-Port SAN Extension Module.

Step 3 Select two MDS switches to connect via FCIP for **Between Switch** and **Switch** from the drop-down list.

Each switch must have an Ethernet port that is connected to an IP network to function correctly.

Note In the case of a federation setup, both switches must belong to the fabrics that are discovered or managed by the same server.

Step 4 Click **Next** to select the Ethernet ports.

Step 5 Select the Ethernet ports to be used in FCIP ISL between the selected switches.

Down ports must be enabled to function correctly. Security can be enforced for unconfigured 14+2, 18+4, 9250i and SSN16 Ethernet ports.

Step 6 Click **Next** to specify the IP addresses and add an IP route.

Step 7 Enter the Ethernet ports IP addresses and specify the IP Routes if the port addresses are in a different subnet.

Note Click **Next** to apply the changes to IP Address and IP Route.

Step 8 Click **Next** to specify Tunnel properties.

Step 9 Specify the following parameters to tunnel the TCP connections.

Enter the parameters.

- **Max Bandwidth**: Enter the number between 1 to 10000. The unit is **Mb**.
- **Min Bandwidth**: Enter the minimum bandwidth value. The unit is **Mb**.
- **Estimated RTT(RoundTrip Time)**—Enter the number between 0 to 300000. The unit is **us**. Click **Measure** to measure the roundtrip time.

- **Write Acceleration**: Check the check box to enable the write acceleration.

  Note If Write Acceleration is enabled, ensure that flows will not load balance across multiple ISLs.

- **Enable Optimum Compression**: Check the check box to enable the optimum compression.
- **Enable XRC Emulator**: Check the check box to enable XRC emulator.
- **Connections**: Enter the number of connections from 0 to 100.

Step 10 Click **Next** to create FCIP ISL.

Step 11 Enter the **Profile ID** and **Tunnel ID** for the switch pair, and select the **FICON Port Address** from the drop-down list.

Step 12 Click **View Configured** to display the **Profiles** and **Tunnels** information.

Step 13 Select the **Trunk Mode** from **non-Trunk**, **trunk**, and **auto**. Specify the **Port VSAN** for **non-Trunk** and **auto**, and allowed **VSAN List** for Trunk tunnel.

Step 14 Click **Next** to the last summary page.

The **Summary** view displays what you have selected in the previous steps.

Step 15 Click **Deploy** to configure FCIP or click **Finish** complete the configuration and deploy later.

Port Channels

Port Channels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy. Port Channels can connect to interfaces across switching modules, so a failure of a switching module cannot bring down the Port Channel link.

Beginning with Cisco Data Center Network Manager 11.0(1), you can configure and edit Port Channels. Navigate to **Configure > SAN > Port Channel** to create or edit Port Channels.

Click **Create New Port Channel** to launch the wizard to create new Port Channel.

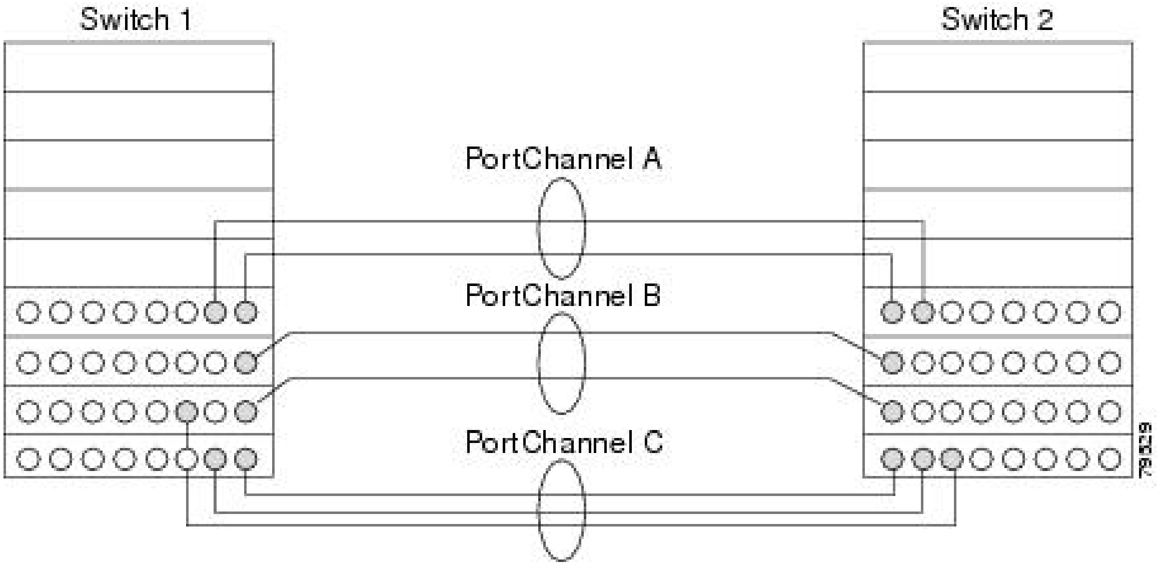
Click **Edit Existing Port Channel** to launch the wizard to edit an existing Port Channel.

Information About Configuring Port Channels

Port Channels Overview

Port Channels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy (See below figure). Port Channels can connect to interfaces across switching modules, so a failure of a switching module cannot bring down the Port Channel link.

Figure 4: Port Channel Flexibility



Port Channels on Cisco MDS 9000 Family switches allow flexibility in configuration. This illustrates three possible Port Channel configurations:

- Port Channel A aggregates two links on two interfaces on the same switching module at each end of a connection.
- Port Channel B also aggregates two links, but each link is connected to a different switching module. If the switching module goes down, traffic is not affected.
- Port Channel C aggregates three links. Two links are on the same switching module at each end, while one is connected to a different switching module on switch 2.

Port Channeling and Trunking

Trunking is a commonly used storage industry term. However, the Cisco NX-OS software and switches in the Cisco MDS 9000 Family implement trunking and Port Channeling as follows:

- Port Channeling enables several physical links to be combined into one aggregated logical link.
- Trunking enables a link transmitting frames in the EISL format to carry (trunk) multiple VSAN traffic. For example, when trunking is operational on an E port, that E port becomes a TE port. A TE port is specific to switches in the Cisco MDS 9000 Family. An industry standard E port can link to other vendor switches and is referred to as a nontrunking interface (See Figure 5: Trunking Only, on page 239 and Figure 6: Port Channeling and Trunking, on page 240).

Figure 5: Trunking Only

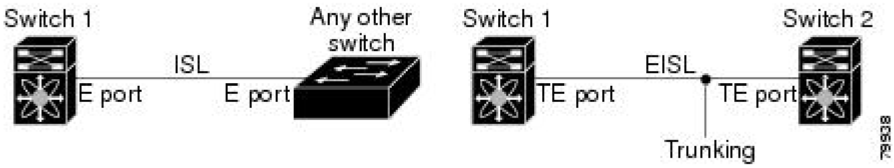
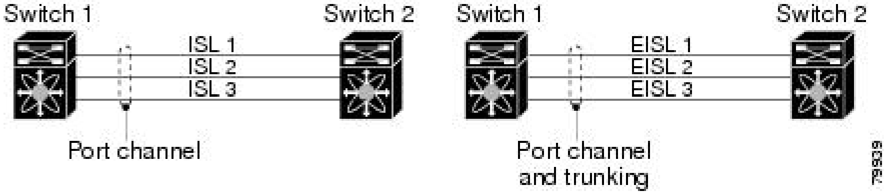


Figure 6: Port Channeling and Trunking



Port Channeling and trunking are used separately across an ISL.

- Port Channeling—Interfaces can be channeled between the following sets of ports:
  - E ports and TE ports
  - F ports and NP ports
  - TF ports and TNP ports
- Trunking—Trunking permits carrying traffic on multiple VSANs between switches.
- Both Port Channeling and trunking can be used between TE ports over EISLs.

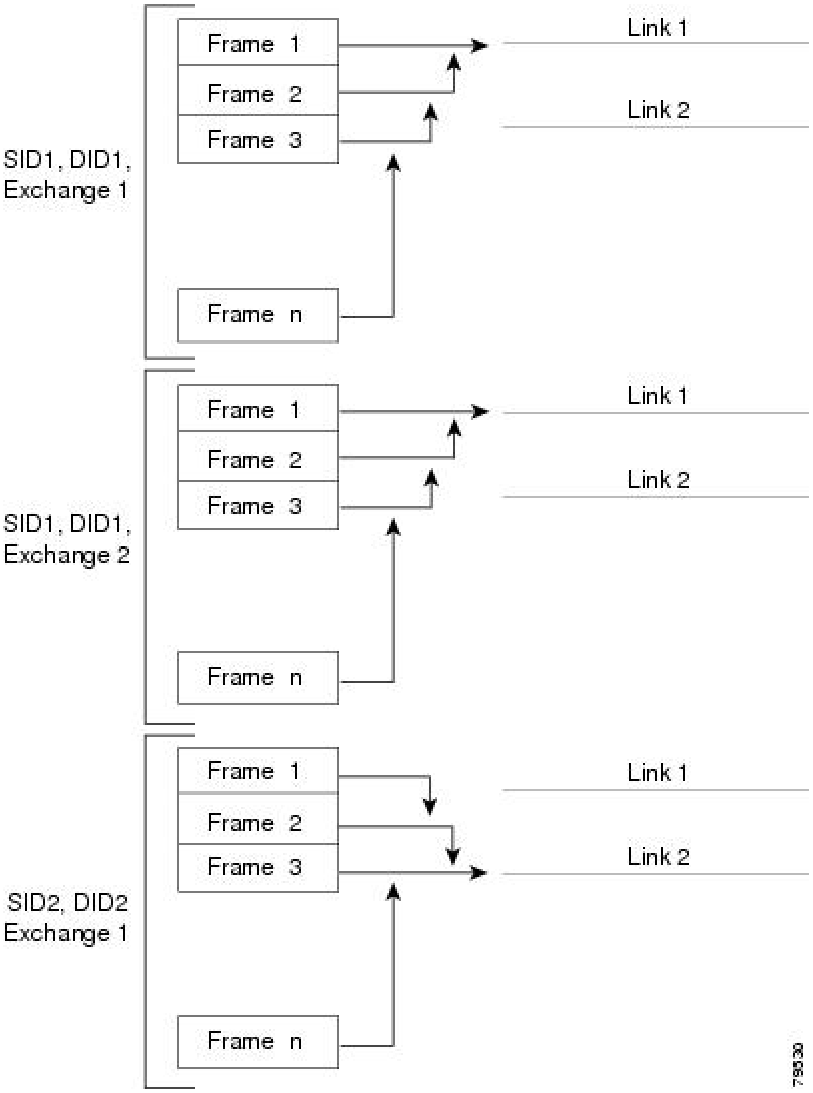
Load Balancing

Two methods support the load-balancing functionality:

- Flow-based—All frames between a source and destination follow the same links for a given flow. That is, whichever link is selected for the first exchange of the flow is used for all subsequent exchanges.
- Exchange-based—The first frame in an exchange picks a link and subsequent frames in the exchange follow the same link. However, subsequent exchanges can use a different link. This provides more granular load balancing while preserving the order of frames for each exchange.

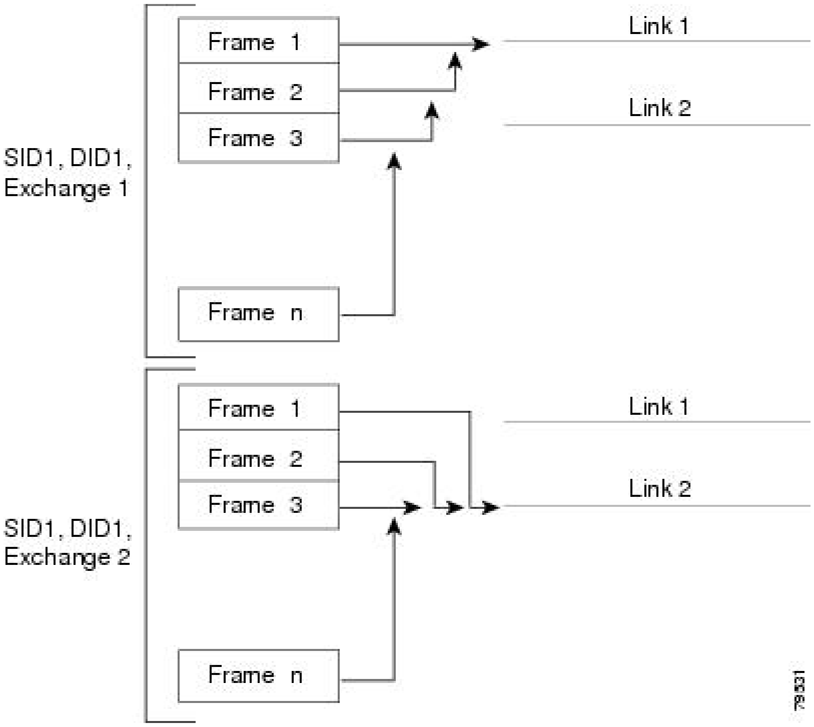
The following figure illustrates how a source ID 1 (SID1) and destination ID1 (DID1)-based load balancing works. When the first frame in a flow is received on an interface for forwarding, link 1 is selected. Each subsequent frame in that flow is sent over the same link. No frame in SID1 and DID1 utilizes link 2.

Figure 7: SID1 and DID1-Based Load Balancing



The following figure illustrates how exchange-based load balancing works. When the first frame in an exchange is received for forwarding on an interface, link 1 is chosen by a hash algorithm. All remaining frames in that particular exchange are sent on the same link. For exchange 1, no frame uses link 2. For the next exchange, link 2 is chosen by the hash algorithm. Now all frames in exchange 2 use link 2.

Figure 8: SID1, DID1, and Exchange-Based Load Balancing



Port Channel Modes

You can configure each Port Channel with a channel group mode parameter to determine the Port Channel protocol behavior for all member ports in this channel group. The possible values for a channel group mode are as follows:

- ON (default)—The member ports only operate as part of a Port Channel or remain inactive. In this mode, the Port Channel protocol is not initiated. However, if a Port Channel protocol frame is received from a peer port, the software indicates its nonnegotiable status. This mode is backward compatible with the existing implementation of Port Channels in releases prior to Release 2.0(1b), where the channel group mode is implicitly assumed to be ON. In Cisco MDS SAN-OS Releases 1.3 and earlier, the only available Port Channel mode was the ON mode. Port Channels that are configured in the ON mode require you to explicitly enable and disable the Port Channel member ports at either end if you add or remove ports from the Port Channel configuration. You must physically verify that the local and remote ports are connected to each other.
- ACTIVE—The member ports initiate Port Channel protocol negotiation with the peer ports regardless of the channel group mode of the peer port. If the peer port, while configured in a channel group, does not support the Port Channel protocol, or responds with a nonnegotiable status, it defaults to the ON mode behavior. The ACTIVE Port Channel mode allows automatic recovery without explicitly enabling and disabling the Port Channel member ports at either end.

The following table compares ON and ACTIVE modes.

Table 29: Channel Group Configuration Differences

ON Mode	ACTIVE Mode
No protocol is exchanged.	A Port Channel protocol negotiation is performed with the peer ports.
Moves interfaces to the suspended state if its operational values are incompatible with the Port Channel.	Moves interfaces to the isolated state if its operational values are incompatible with the Port Channel.
When you add or modify a Port Channel member port configuration, you must explicitly disable (shut) and enable (no shut) the Port Channel member ports at either end.	When you add or modify a Port Channel interface, the Port Channel automatically recovers.
Port initialization is not synchronized.	There is synchronized startup of all ports in a channel across peer switches.
All misconfigurations are not detected as no protocol is exchanged.	Consistently detect misconfigurations using a Port Channel protocol.
Transitions misconfigured ports to the suspended state. You must explicitly disable (shut) and enable (no shut) the member ports at either end.	Transitions misconfigured ports to the isolated state to correct the misconfiguration. Once you correct the misconfiguration, the protocol ensures automatic recovery.

Port Channel Deletion

When you delete the Port Channel, the corresponding channel membership is also deleted. All interfaces in the deleted Port Channel convert to individual physical links. After the Port Channel is removed, regardless of the mode used (ACTIVE and ON), the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down.

If you delete the Port Channel for one port, then the individual ports within the deleted Port Channel retain the compatibility parameter settings (speed, mode, port VSAN, allowed VSAN, and port security). You can explicitly change those settings as required.

- If you use the default ON mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the ACTIVE mode, then the Port Channel ports automatically recover from the deletion.

Interfaces in a Port Channel

You can add or remove a physical interface (or a range of interfaces) to an existing Port Channel. The compatible parameters on the configuration are mapped to the Port Channel. Adding an interface to a Port Channel increases the channel size and bandwidth of the Port Channel. Removing an interface from a Port Channel decreases the channel size and bandwidth of the Port Channel.

This section describes interface configuration for a Port Channel and includes the following topics:

Interface Addition to a Port Channel

You can add a physical interface (or a range of interfaces) to an existing Port Channel. The compatible parameters on the configuration are mapped to the Port Channel. Adding an interface to a Port Channel increases the channel size and bandwidth of the Port Channel.

A port can be configured as a member of a static Port Channel only if the following configurations are the same in the port and the Port Channel:

- Speed
- Mode
- Rate mode
- Port VSAN
- Trunking mode
- Allowed VSAN list or VF-ID list

After the members are added, regardless of the mode (ACTIVE and ON) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down (see the "Generation 1 Port Channel Limitations" section on page -12).

Compatibility Check

A compatibility check ensures that the same parameter settings are used in all physical ports in the channel. Otherwise, they cannot become part of a Port Channel. The compatibility check is performed before a port is added to the Port Channel.

The check ensures that the following parameters and settings match at both ends of a Port Channel:

- Capability parameters (type of interface, Gigabit Ethernet at both ends, or Fibre Channel at both ends).
- Administrative compatibility parameters (speed, mode, rate mode, port VSAN, allowed VSAN list, and port security).

Note Ports in shared rate mode cannot form a Port Channel or a trunking Port Channel.

- Operational parameters (remote switch WWN and trunking mode).

A port addition procedure fails if the capability and administrative parameters in the remote switch are incompatible with the capability and administrative parameters in the local switch. If the compatibility check is successful, the interfaces are operational and the corresponding compatibility parameter settings apply to these interfaces.

Suspended and Isolated States

If the operational parameters are incompatible, the compatibility check fails and the interface is placed in a suspended or isolated state based on the configured mode:

- An interface enters the suspended state if the interface is configured in the ON mode.
- An interface enters the isolated state if the interface is configured in the ACTIVE mode.

Forcing an Interface Addition

You can force the port configuration to be overwritten by the Port Channel. In this case, the interface is added to a Port Channel.

- If you use the default ON mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You have to explicitly enable those ports again.
- If you use the ACTIVE mode, then the Port Channel ports automatically recover from the addition.

Note When Port Channels are created from within an interface, the force option cannot be used.

After the members are forcefully added, regardless of the mode (ACTIVE and ON) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down.

Interface Deletion from a Port Channel

When a physical interface is deleted from the Port Channel, the channel membership is automatically updated. If the deleted interface is the last operational interface, then the Port Channel status is changed to a down state. Deleting an interface from a Port Channel decreases the channel size and bandwidth of the Port Channel.

- If you use the default ON mode to avoid inconsistent states across switches and to maintain consistency across switches, then the ports shut down. You must explicitly enable those ports again.
- If you use the ACTIVE mode, then the Port Channel ports automatically recover from the deletion.

After the members are deleted, regardless of the mode (ACTIVE and ON) used, the ports at either end are gracefully brought down, indicating that no frames are lost when the interface is going down.

Port Channel Protocols

In earlier Cisco SAN-OS releases, Port Channels required additional administrative tasks to support synchronization. The Cisco NX-OS software provides robust error detection and synchronization capabilities. You can manually configure channel groups or they can be automatically created. In both cases, the channel groups have the same capability and configurable parameters. Any change in configuration that is applied to the associated Port Channel interface is propagated to all members of the channel group.

A protocol to exchange Port Channel configurations is available in all Cisco MDS switches. This addition simplifies Port Channel management with incompatible ISLs. An additional autocreation mode enables ISLs with compatible parameters to automatically form channel groups without manual intervention.

The Port Channel protocol is enabled by default.

The Port Channel protocol expands the Port Channel functional model in Cisco MDS switches. It uses the exchange peer parameters (EPP) services to communicate across peer ports in an ISL. Each switch uses the information that is received from the peer ports along with its local configuration and operational values to decide if it should be part of a Port Channel. The protocol ensures that a set of ports is eligible to be part of the same Port Channel. They are only eligible to be part of the same Port Channel if all the ports have a compatible partner.

The Port Channel protocol uses two subprotocols:

- Bringup protocol—Automatically detects misconfigurations so you can correct them. This protocol synchronizes the Port Channel at both ends so that all frames for a given flow (as identified by the source FC ID, destination FC ID and OX_ID) are carried over the same physical link in both directions. This helps make applications such as write acceleration, work for Port Channels over FCIP links.
- Autocreation protocol—Automatically aggregates compatible ports into a Port Channel.

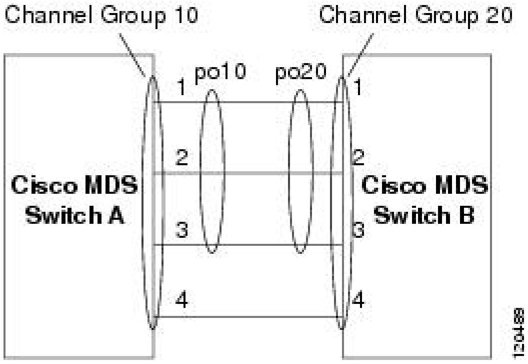
This section describes how to configure the Port Channel protocol and includes the following sections:

Channel Group Creation

Note Channel groups are not supported on internal ports in the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeSystem.

Assuming link A1-B1 comes up first (see Figure 1-9), that link is operational as an individual link. When the next link comes up, for example, A2-B2, the Port Channel protocol identifies if this link is compatible with link A1-B1 and automatically creates channel groups 10 and 20 in the respective switches. If link A3-B3 can join the channel groups (the Port Channels), the respective ports have compatible configurations. If link A4-B4 operates as an individual link, it is because of the incompatible configuration of the two end ports with the other member ports in this channel group.

Figure 9: Autocreating Channel Groups



The channel group numbers are selected dynamically, and as such, the administrative configuration of the ports forming the channel group at either end are applicable to the newly created channel group. The channel group number being chosen dynamically may be different across reboots for the same set of Port Channels based on the order of ports that are initialized in the switch.

Table 1-10 identifies the differences between user-configured and auto-configured channel groups.

User-Configured Channel Group	Autocreated Channel Group
Manually configured by the user.	Created automatically when compatible links come up between two compatible switches, if channel group autocreation is enabled in all ports at both ends.
Member ports cannot participate in autocreation of channel groups. The autocreation feature cannot be configured.	None of these ports are members of a user-configured channel group.
You can form the Port Channel with a subset of the ports in the channel group. Incompatible ports remain in a suspended or isolated state depending on the ON or ACTIVE mode configuration.	All ports included in the channel group participate in the Port Channel—no member port becomes isolated or suspended; instead, the member port is removed from the channel group when the link is found to be incompatible.

Any administrative configuration that is made to the Port Channel is applied to all ports in the channel group, and you can save the configuration for the Port Channel interface.	Any administrative configuration that is made to the Port Channel is applied to all ports in the channel group, but the configurations are saved for the member ports; no configuration is saved for the Port Channel interface. You can explicitly convert this channel group, if required.
You can remove any channel group and add members to a channel group.	You cannot remove a channel group, or add/remove any of its members. The channel group is removed when no member ports exist.

Autocreation

The autocreation protocol has the following functionality:

- A port is not allowed to be configured as part of a Port Channel when the autocreation feature is enabled. These two configurations are mutually exclusive.
- Autocreation must be enabled in both the local and peer ports to negotiate a Port Channel.
- Aggregation occurs in one of two ways:
  - A port is aggregated into a compatible autocreated Port Channel.
  - A port is aggregated with another compatible port to form a new Port Channel.
- Newly created Port Channels are allocated from the maximum Port Channel (128 for Generation 1 or a combination of Generation 1 and Generation 2 switches, or 256 for Generation 2 switches) in a decreasing order based on availability. If all 128 (or 256) numbers are used up, aggregation is not allowed.
- You cannot change the membership or delete an autocreated Port Channel.
- When you disable autocreation, all member ports are removed from the autocreated Port Channel.
- Once the last member is removed from an autocreated Port Channel, the channel is automatically deleted and the number is released for reuse.
- An autocreated Port Channel is not persistent through a reboot. An autocreated Port Channel can be manually configured to appear the same as a persistent Port Channel. Once the Port Channel is made persistent, the autocreation feature is disabled in all member ports.
- You can enable or disable the autocreation feature on a per-port basis or for all ports in the switch. When this configuration is enabled, the channel group mode is assumed to be active. The default for this task is disabled.
- If autocreation of channel groups is enabled for an interface, you must first disable autocreation before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.

Note When enabling autocreation in any switch in the Cisco MDS 9000 Family, we recommend that you retain at least one interconnected port between the switches without any autocreation configuration. If all ports between two switches are configured with the autocreation feature at the same time, you may face a possible traffic disruption between these two switches as the ports are automatically disabled and reenabled when ports are added to an autocreated Port Channel.

Manually Configured Channel Groups

A user-configured channel group cannot be converted to an autocreated channel group. However, you can convert an autocreated channel group to a manual channel group. Once performed, this task is irreversible. The channel group number does not change, but the member ports operate according to the properties of the manually configured channel group, and the autocreation of channel group is implicitly disabled for all member ports.

Tip If you enable persistence, be sure to enable it at both ends of the Port Channel.

Prerequisites for Configuring Port Channels

Before configuring a Port Channel, consider the following guidelines:

- Configure the Port Channel across switching modules to implement redundancy on switching module reboots or upgrades.
- Ensure that one Port Channel is not connected to different sets of switches. Port Channels require point-to-point connections between the same set of switches.

On switches with Generation 1 switching modules, or a combination of Generation 1 and Generation 2 switching modules, you can configure a maximum of 128 Port Channels. On switches with only Generation 2 switching modules, or Generation 2 and Generation 3 switching modules, you can configure a maximum of 256 Port Channels.

If you misconfigure Port Channels, you may receive a misconfiguration message. If you receive this message, the Port Channel’s physical links are disabled because an error has been detected.

A Port Channel error is detected if the following requirements are not met:

- Each switch on either side of a Port Channel must be connected to the same number of interfaces.
- Each interface must be connected to a corresponding interface on the other side (see Figure 1-11 for an example of an invalid configuration).
- Links in a Port Channel cannot be changed after the Port Channel is configured. If you change the links after the Port Channel is configured, be sure to reconnect the links to interfaces within the Port Channel and reenable the links.

If all three conditions are not met, the faulty link is disabled.

Enter the show interface command for that interface to verify that the Port Channel is functioning as required.

Guidelines and Limitations for Configuring Port Channels

This section includes the guidelines and limitations for this feature:

General Guidelines for Cisco MDS 9000 Series Switches

Cisco MDS 9000 Family switches support the following number of Port Channels per switch:

- Switches with only Generation 1 switching modules do not support F and TF Port Channels.

- Switches with Generation 1 switching modules, or a combination of Generation 1 and Generation 2 switching modules, support a maximum of 128 Port Channels. Only Generation 2 ports can be included in the Port Channels.
- Switches with only Generation 2 switching modules or Generation 2 and Generation 3 modules support a maximum of 256 Port Channels with 16 interfaces per Port Channel.
- A Port Channel number refers to the unique identifier for each channel group. This number ranges from of 1 to 256.

Generation 1 Port Channel Limitations

This section includes the restrictions on creation and addition of Port Channel members to a Port Channel on Generation 1 hardware:

- The 32-port 2-Gbps or 1-Gbps switching module.
- The MDS 9140 and 9120 switches.

When configuring the host-optimized ports on Generation 1 hardware, the following Port Channel guidelines apply:

- If you execute the write erase command on a 32-port switching module, and then copy a saved configuration to the switch from a text file that contains the no system default switchport shutdown command, you have to copy the text file to the switch again for the E ports to come up without manual configuration.
- Any (or all) full line rate ports in the Cisco MDS 9100 Series can be included in a Port Channel.
- The host-optimized ports in the Cisco MDS 9100 Series are subject to the same Port Channel rules as 32-port switching modules; only the first port of each group of four ports is included in a Port Channel.
    - You can configure only the first port in each 4-port group as an E port (for example, the first port in ports 1–4, the fifth port in ports 5–8, and so on). If the first port in the group is configured as a Port Channel, the other three ports in each group (ports 2–4, 6–8, and so on) are not usable and remain in the shutdown state.
    - If any of the other three ports are configured in a no shutdown state, you cannot configure the first port to be a Port Channel. The other three ports continue to remain in a no shutdown state.

F and TF Port Channel Limitations

The following guidelines and restrictions are applicable for F and TF Port Channels:

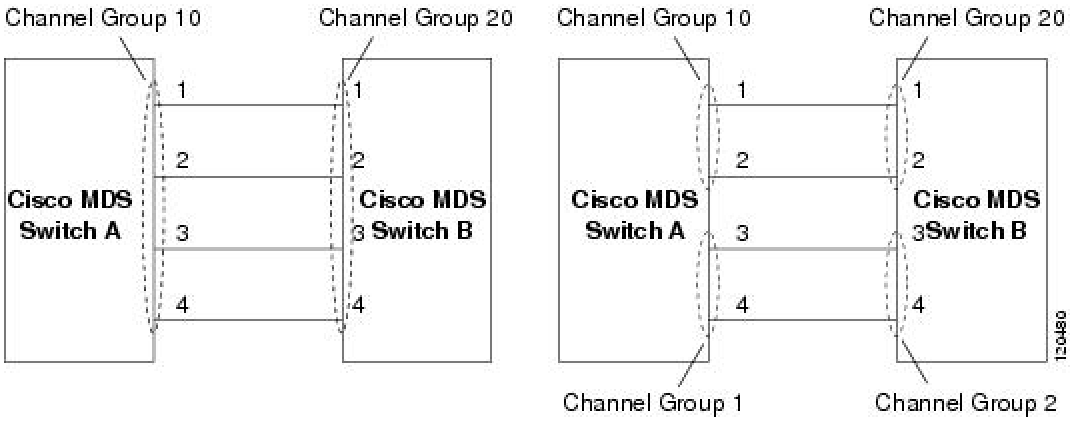
- The ports must be in F mode.
- Automatic creation is not supported.
- The Port Channel interface must be in ACTIVE mode when multiple FCIP interfaces are grouped with WA.
- ON mode is not supported. Only ACTIVE-ACTIVE mode is supported. By default, the mode is ACTIVE on the NPV switches.
- Devices that are logged in through F Port Channel on an MDS switch are not supported in IVR non-NAT configuration. The devices are supported only in IVR NAT configuration.

- Port security rules are enforced only on physical pWWNs at the single link level.
- FC-SP authenticates only the first physical FLOGI of every Port Channel member.
- Since the FLOGI payload carries only the VF bits to trigger the use of a protocol after the FLOGI exchange, those bits will be overridden. In the case of the NPV switches, the core has a Cisco WWN and tries to initiate the PCP protocol.
- The name server registration of the N ports logging in through an F Port Channel uses the fWWN of the Port Channel interface.
- DPVM configuration is not supported.
- The Port Channel port VSAN cannot be configured using DPVM.
- The Dynamic Port VSAN Management (DPVM) database is queried only for the first physical FLOGI of each member, so that the port VSAN can be configured automatically.
- DPVM does not bind FC_IDs to VSANs, but pWWNs to VSANs. It is queried only for the physical FLOGI.

Valid and Invalid Port Channel Examples

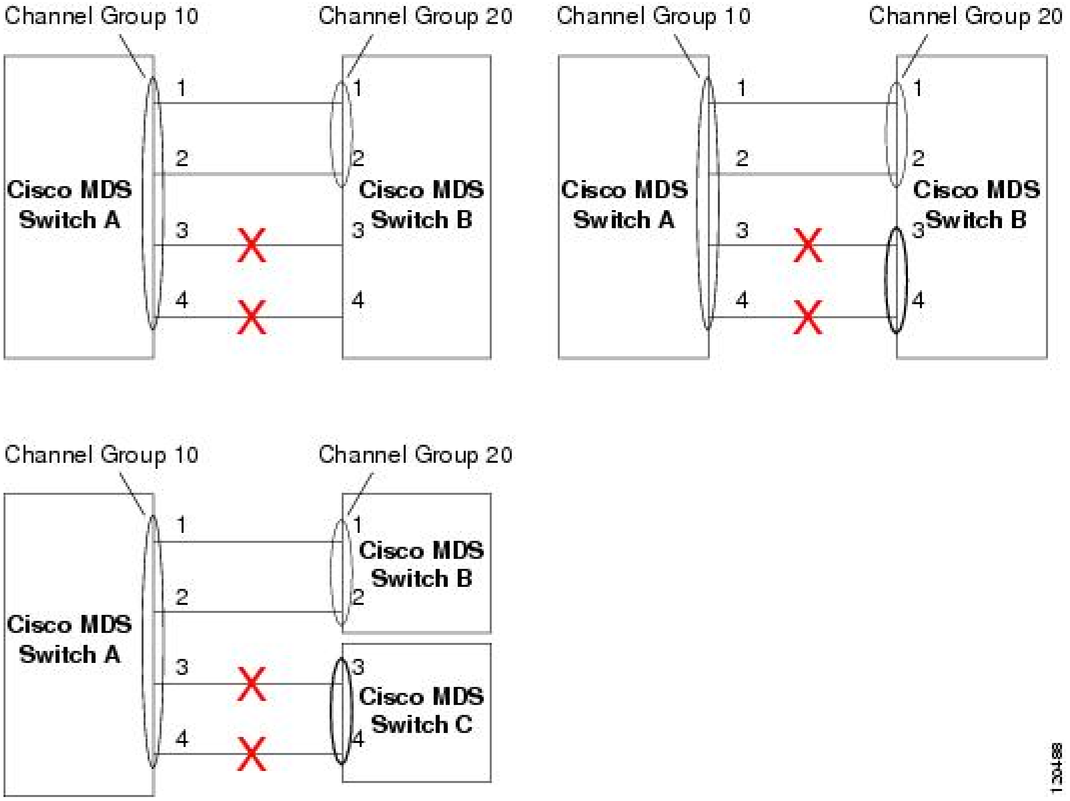
Port Channels are created with default values. You can change the default configuration just like any other physical interface. The following figure provides examples of valid Port Channel configurations.

Figure 10: Valid Port Channel Configurations



The following figure provides examples of invalid configurations. Assuming that the links are brought up in the 1, 2, 3, 4 sequence, links 3 and 4 will be operationally down as the fabric is misconfigured.

Figure 11: Misconfigured Configurations



Default Settings

The following table lists the default settings for Port Channels.

Table 30: Default Port Channel Parameters

Parameters	Default
Port Channels	FSPF is enabled by default.
Create Port Channel	Administratively up.
Default Port Channel mode	ON mode on non-NPV and NPIV core switches. ACTIVE mode on NPV switches.
Autocreation	Disabled.

Create Port Channel Wizard

To create a Port Channel using the Create New Port Channel Wizard on the DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > SAN > Port Channel**.

Click **Create New Port Channel** to launch the Create Port Channel Wizard.

Step 2 In the Select Switch Pair screen, perform the following steps:

a) Select the appropriate fabric from the Fabric drop-down.

   The list contains switch pairs in the fabric that have an ISL between them, that is not already in a port channel.

b) Select a switch pair to be linked by an FC Port Channel.

   If there are NPV links between NPIV-core and NPV switches, you must enable F Port Trunking and Channeling Protocol using the **feature fport-channel-trunk** command on the NPIV switch in order to see the switch-pair and the number of NPV links.

c) Click **Next**.

Step 3 In the Select ISLs screen, select one or more ISLs or Links to create a new Channel between the switch pair.

a) From the list of ISLs in the Available area, select and click right arrow to move the ISL to the Selected area.
b) Click **Next**.

Step 4 In the Create Port Channel screen, define, or edit the channel attributes.

a) Channel ID field is populated with the next unused channel ID. Change the channel ID or description for each switch, if necessary.

   The range of the channel ID is from 1 to 256.

b) FICON Port Address is only enabled if the switches are FICON enabled. From the drop-down list, select the appropriate FICON port address on the switch. Select the port address that you want to assign to the Port Channel port.
c) In the Channel Attributes area, to configure the speed, click the appropriate radio button.
d) Select the appropriate Trunk Mode radio button to enable trunking on the links in the Port Channel.

   - Select **trunk** if your link is between TE ports.
   - Select **nonTrunk** if your link is between E ports.
   - Select **auto** if you are not sure.

e) In the Port VSAN field, enter the interface ID for port VSAN which must be used when trunking is not enabled.

   Every interface must have a port VSAN even if trunking is enabled. If trunking is enabled, this port VSAN is not used. However, the switch must configure the port, so that the network knows what VSAN to use by default, if trunking is disabled.

f) VSAN list field provides a list of VSANs you want to allow the port channel to use for trunking.

   This field is disabled if the Trunk Mode is set to **nonTrunk** or **auto**.

g) In the Core Switch Bandwidth field, select dedicated or shared radio button to allocate the switch bandwidth.

   This bandwidth is applicable only for port channels between an NPIV and NPV switch.

h) Check the **Force Admin**, **Trunk**, **Speed**, and **VSAN attributes to be identical** checkbox to ensure that the same parameter settings are used in all physical ports in the channel. If these settings are not identical, the ports cannot become part of the Port Channel.

Step 5 Click **Previous** to return to the previous screen and edit the settings. Click **Finish** to configure the Port Channel.

A success message appears.

Step 6 Click **Close** to close the Create Port Channel Wizard.

Edit Existing Port Channel

To edit a Port Channel using the Edit Port Channel Wizard on the DCNM Web UI, follow these steps:

Procedure

Step 1 From the Cisco DCNM Web UI, navigate to **Configure > SAN > Port Channel**.

Click on **Edit Existing Port Channel** to launch the Edit Port Channel Wizard.

Step 2 In the Select Switch Pair screen, do the following:

a) Select the appropriate fabric from the Fabric drop-down list.

The switch pairs that have port channels between them are listed in the area below.

b) Select a switch pair to edit the port channel.
c) Click **Next**.

Step 3 In the Select Port Channel screen, select a Port Channel to edit.

Click **Next**.

Step 4 In the Edit Port Channel screen, select the desired ISL.

a) Click the right and left arrow to select the available ISLs.

Note The selected ISLs are contained in the Port Channel after you save the changes. If the Selected ISLs list is empty, the Delete Port Channel is Empty checkbox is enabled.

b) If you do not choose any ISL, check the **Delete Port Channel if Empty** checkbox to delete the port channel.
c) Check the **Force admin**, **trunk**, **speed**, **VSAN attributes to be identical** checkbox to choose identical values for admin, trunk, speed and VSAN attributes.
d) Click **Next**.

Step 5 Click **Finish** to apply the changes.

Click **Previous** to go back to the previous screen and edit the values.

Click **Cancel** to abort the changes.

Device Alias

A device alias is a user-friendly name for a port WWN. Device alias name can be specified when configuring features such as zoning, QoS, and port security. The device alias application uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management and fabric-wide distribution.

This section contains context-sensitive online help content under **Configure** > **SAN** > **Device Alias**.

The following table describes the fields that appear under **Configure > SAN > Device Alias**.

Field	Description
Seed Switch	Displays the device alias seed switch name.
Device Alias	Displays the alias retrieved from the seed switch.
pWWN	Displays the port WWN.

This section contains the following:

Configuration

Select the Fabric from the Fabric drop-down list. The list of device aliases existing on the fabric will be retrieved and displayed.

Before performing any Device Alias configuration, check the status on the **CFS** tab, to ensure that the status is "success".

Note To perform Device Alias configuration from the Cisco DCNM Web client, the fabric must be configured as Device Alias enhanced mode.

Procedure

Step 1 To delete the device alias, Cisco DCNM **Web Client** > **Configure** > **SAN** > **Device Alias** > **Configuration** tab, check the device alias you need to delete.

a) Click **Delete**.

A confirmation message appears.

Note Deleting the device alias may cause traffic interruption.

b) Click **Yes** to delete the topic alias.

Step 2 To create the device alias, from Cisco DCNM **Web Client** > **Configure** > **SAN** > **Device Alias** > **Configuration** tab, click **Create**.

The Add Device Alias windows appears.

All the provisioned port WWNs are populated in the table.

a) Enter a device alias name in the **Device Alias** field to indicate to create a device alias for the selected pWWN.

b) Click **Save** to exit the inline editor mode.
c) Click **Apply** to assign the device alias to the switches.

You can also create a device alias with a non-provisioned port WWN.

a) Click **New Alias** to create a new table row in inline editor mode.
b) In the **pWWN** field, enter the non-provisioned port WWN for the new alias.
c) Click **Save** to exit the inline editor mode.
d) Click **Apply** to assign the device alias and the associated pWWN to the switches.

Note If you close the Add Device Alias window before applying the device alias to the switches, the changes will be discarded and the device alias will not be created.

Step 3 For end devices with an attached service profile, the service profile name is populated to the **Device Alias** field. This allows the service profile name as device alias name for those devices.

Device Alias creation is CFS auto-committed after clicking Apply. Click **CFS** tab to check if CFS is properly performed after the device alias was created. In case of failure, you must troubleshoot and fix the problem.

CFS

Select the Fabric from the Fabric drop-down list. The list of device aliases existing on the fabric is retrieved and displayed.

CFS information is listed for all the eligible switches in the fabric. Before performing any Device Alias configuration, check the status on the **CFS** tab to ensure that the status is "success". If the CFS is locked by another user, or if the previous operation failed, ensure that the CFS session is unlocked.

To view CFS information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **SAN** > **Device Alias** > **CFS**.

Step 2 To commit the CFS configuration, select the **Switch** radio button.

Click **Commit**.

The CFS configuration for this switch is committed.

Step 3 To abort the CFS configuration, select the **Switch** radio button.

Click **Abort**.

The CFS configuration for this switch is aborted.

Step 4 To clear the lock on the CFS configuration of the switch, select the **Switch** radio button.

Click **Clear Lock**.

If the CFS is locked by another user, or if the previous operation failed, ensure that the CFS session is unlocked.

Port Monitoring

This feature allows you to save custom Port Monitoring policies in the Cisco DCNM database. It allows you to push the selected custom policy to one or more fabrics or Cisco MDS 9000 Series Switches. The policy is designated as active Port-Monitor policy in the switch.

This feature is supported only on the Cisco MDS 9000 SAN Switches and therefore the Cisco DCNM user is allowed to select the MDS switch to push the policy.

Cisco DCNM provides five templates to customize the policy. The user-defined policies are saved in the Cisco DCNM database. You can select any template or customized policy to push to the selected fabric or switch with the desired port type.

Note You can edit only user-defined policies.

The following table describes the fields that appear on Cisco DCNM **Configure > SAN > Port Monitoring**.

Field	Description
Templates	This drop-down list shows the following templates for policies: • Normal_accessPort • Normal_allPort • Normal_trunksPort • Aggressive_accessPort • Aggressive_allPort • Aggressive_trunksPort • Most-Aggressive_accessPort • Most-Aggressive_allPort • Most-Aggressive_trunksPort • default • slowdrain
Save	Allows you to save your changes for the user-defined policies.
Save As	Allows you to save an existing policy as a new policy with a different name. This creates another item in the templates as Custom Policy. The customized policy is saved under this category. If you click **Save As** while the policy is edited, the customized policy is saved.

Field	Description
	Note The port type of the customized policy will not be saved when Save As is selected.
Delete	Allows you to delete any user-defined policies.
Push to switches	Allows you to select a fabric or switch and push the selected policies with a desired port type. The available port types are: • trunks/Core • access-port/Edge • all **Note** If you choose trunks or all, the port guard is disabled. The following policies select the trunks/Core policy type: • Normal_trunksPort • Aggressive_trunksPort • Most-Aggressive_trunksPort The following policies select the access-port/Edge policy type: • Normal_accessPort • Aggressive_accessPort • Most-Aggressive_accessPort • slowdrain The following policies select the all policy type: • Normal_allPort • Aggressive_allPort • Most-Aggressive_allPort • default Select the parameters and click **Push** to push the policies to the switches in the fabric. If there is any active policy with the same or common port type, the push command configures the same policy on the selected devices. This policy replaces

Field	Description
	the existing active policy with the same or common port type. If you click **Push to Switches** while the policy is edited, the customized policy will not be saved.
Counter Description	Specifies the counter type. Move the pointer to the "i" icon next to the counter description to view detailed information.
Rising Threshold	Specifies the upper threshold limit for the counter type.
Rising Event	Specifies the type of event to be generated when rising threshold is reached or crossed.
Falling Threshold	Specifies the lower threshold limit for the counter type.
Falling Event	Specifies the type of event to be generated when falling threshold is reached or crossed.
Poll Interval	Specifies the time interval to poll for the counter value.
Warning Threshold	Allows you to set an optional threshold value lower than the rising threshold value and higher than the falling threshold value to generate syslogs. The range is 0–9223372036854775807.
Port Guard	Specifies if the port guard is enabled or disabled. The value can be false, flap, or errordisable. The default value is "false".
Monitor ?	The default value is "true".

SAN Insights - Overview

Introduction to SAN Insights

The SAN Insights feature enables you to configure, monitor, and view the flow analytics in fabrics. Cisco DCNM enables you to visualize the health-related indicators in the interface so that you can quickly identify issues in fabrics. Also, the health indicators enable you to understand the problems in fabrics. The SAN Insights feature also provides more comprehensive end-to-end flow-based data from the host to LUN.

From Release 11.2(1), Cisco DCNM supports SAN Telemetry Streaming (STS) using compact GPB transport, for better telemetry performance and to improve the overall scalability of SAN Insights.

For SAN insights streaming stability and performance, refer to System Requirements section in the *Cisco DCNM Installation Guide for SAN Deployment Guide* and the section Increasing Elasticsearch Database Heap Size of the *Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide*. Ensure system RAM is of adequate size. Use of NTP is recommended to maintain time synchronization between the DCNM and the switches. Enable PM collection for viewing counter statistics.

Prerequisites

- The SAN Insights feature is supported for Cisco MDS NX-OS Release 8.3(1) and later.
- The SAN Insights feature isn't supported on small deployment.
- Every Federation node must consist of three Large DCNM nodes.
- For SAN Insights streaming stability and performance, the recommended Elasticsearch heap size is 16GB. To increase the heap size, see Increasing Elasticsearch Database Heap Size, on page 267.
- If SAN Insights streaming was configured with KVGPB encoding using versions of Cisco DCNM SAN Insights older than 11.2(1), the switch continues to stream with KVGPB encoding while configuring streaming with DCNM versions 11.2(1) and above. Compact GPB streaming configuration for SAN Insights is supported starting from Cisco DCNM 11.2(1). To stream using Compact GPB, disable the old KVGPB streaming before configuring SAN Insights newly, after the upgrade. To disable analytics and telemetry, on the Cisco DCNM Web client, choose **Configure** > **SAN** > **SAN Insights**. Click **Continue**. Select the appropriate fabric and click **Continue**. On the Switch Selection screen, click **Disable Analytics** to clear all the analytics and telemetry configuration on the selected switches.

Guidelines and Limitations

- Ensure that the time configurations in Cisco DCNM and the supported switches are synchronized to the local NTP server for deploying the SAN Insights feature.
- Any applicable daylight time savings settings must be consistent across the switches and Cisco DCNM.
- To modify the streaming interval, use the CLI from the switch, and remove the installed query for Cisco DCNM. Modify the **san.telemetry.streaming.interval** property in the DCNM server properties. The allowed values for the interval are 30–300 seconds. The default value is 30 seconds. If there is an issue with the default value or to increase the value, set default value to 60 seconds.Again configure the same switch from Cisco DCNM to push the new streaming interval.
- Use the ISL query installation type only for the switches that have storage connected (storage-edge switches).
- For the ISL query installation type, in the Configure SAN Insights wizard, analytics can't be enabled on interfaces that are members of port-channel ISL to non-MDS platform switches.
- After installing the switch-based FM_Server_PKG license, the Configure SAN Insights wizard may take upto 5 minutes to detect the installed license.

For information about the SAN Insights dashboard, see SAN Insights Dashboard.

For information about configuring the SAN Insights dashboard, see Configuring SAN Insights, on page 261.

Server Properties for SAN Insights

The following table describes the property name and its default values. To modify these values, navigate to **Administration** > **DCNM Server** > **Server Properties** on the Web UI.

From Release 11.4(1), you need not stop/start the SAN Insights Post processing application and the SAN Insight Pipeline application from the **DCNM WebUI** > **Applications** > **Catalog** page, to refresh server properties. Click the Pause, and then Resume on the application icon to apply the modifications to the server properties.

Note After applying changes to the server properties, you must restart all the DCNM services.

For OVA Deployment—Restart the DCNM Services by using the following commands in the same sequence.

```
(dccnm-server)# sysadmin user
(dccnm-server)# appmgr stop dcnm
(dccnm-server)# appmgr start dcnm
```

After the applications are up and running, choose **Web UI** > **Applications** > **Catalog**. Restart **SAN Insight Pipeline Collector** and **SAN Insight Post Processor** applications.

Note If you change the server properties, ensure that you restart the Cisco DCNM to use the new properties value. Restart the SAN Insights service to use the new properties.

Table 31: Server Properties for SAN Insights

Property Name	Description	Default Value
san.telemetry.processing.interval	Specifies the SAN Insights processing interval.	300,000 milliseconds
san.telemetry.streaming.interval	Specifies the SAN Insights streaming interval.	30 seconds
san.telemetry.va.flow.limit	Specifies maximum number of unique flows (ITLs + ITCNs) taken for processing DCNM on virtual machine.	50,000
san.telemetry.pa.flow.limit	Specifies maximum number of unique flows (ITLs + ITCNs) taken for processing on Cisco Nexus Dashboard.	70,000
san.telemetry.use.noop.data	Specifies if the noop frames are used in ECT baseline training calculation.	TRUE
san.telemetry.log.dropped	Specifies log of all dropped flows explicitly	FALSE
san.telemetry.train.timeframe	Specifies the training time frame for flows ECT baseline.	7 days
san.telemetry.train.reset	Specifies the time duration to periodically restart the ECT baseline training after number of days.	14 days
san.telemetry.expire.flows	Specifies the retention policy after which the flows data is deleted.	2 days
san.telemetry.expire.flows	Specifies the retention policy after which the flows data is deleted.	7 days
san.telemetry.expire.baseline	Specifies the retention policy after which the post processed data is deleted.	14 days

Property Name	Description	Default Value
san.telemetry.expire.rollup	Specifies the retention policy after which the hourly rollups data is deleted.	90 days
san.telemetry.expire.train	Specifies time to keep unseen flow training data	14 days
san.telemetry.deviation.low	Specifies the deviation low mark for SCSI telemetry	10
san.telemetry.deviation.med	Specifies the deviation medium mark for SCSI telemetry	30
san.telemetry.deviation.high	Specifies the deviation high mark for SCSI telemetry	50
san.telemetry.nvme.deviation.low	Specifies the deviation low mark for NVMe/FC telemetry	0
san.telemetry.nvme.deviation.med	Specifies the deviation medium mark for NVMe/FC telemetry	2
san.telemetry.nvme.deviation.high	Specifies the deviation high mark for NVMe/FC telemetry	5
san.telemetry.default.protocol	Specifies the desired default protocol selection in the SAN Insights UI pages to view corresponding data: SCSI or NVMe.	SCSI
san.telemetry.gap.reset	Allows you to use telemetry reset based on time gap between records	true
san.telemetry.gap.reset.interval	Specifies the maximum valid time gap between records.	750 seconds

Configuring SAN Insights

To configure SAN insights from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Note From Release 11.3(1), the SAN Insights feature is supported on Cisco DCNM Deployment using OVA/ISO image with Huge deployment option only.

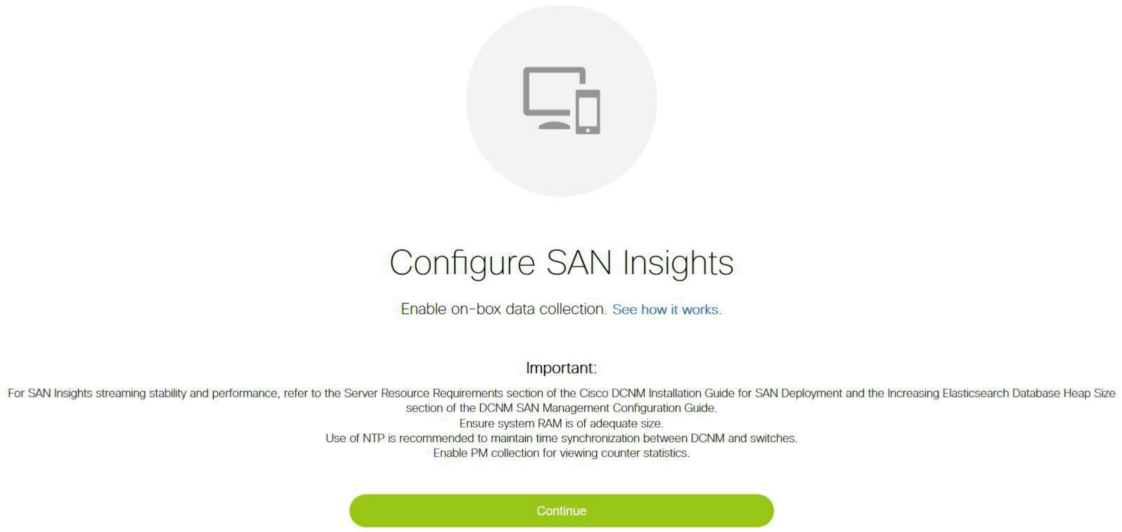
From Release 11.3(1), the Elasticsearch heap size is set to 25% of the total system RAM, up to a maximum of 32G heap size. SAN Insights require a minimum of 16GB Elasticsearch heap size for proper functioning. As Cisco DCNM SAN deployment with OVA/ISO is already configured with sufficient system requirements, you need not increase the Heap Size manually.

Refer to Increasing Elasticsearch Database Heap Size, on page 267 for more instructions.

Procedure

Step 1 Choose **Configure** > **SAN** > **SAN Insights**.

The **Configure SAN Insights** wizard appears.



Configure SAN Insights

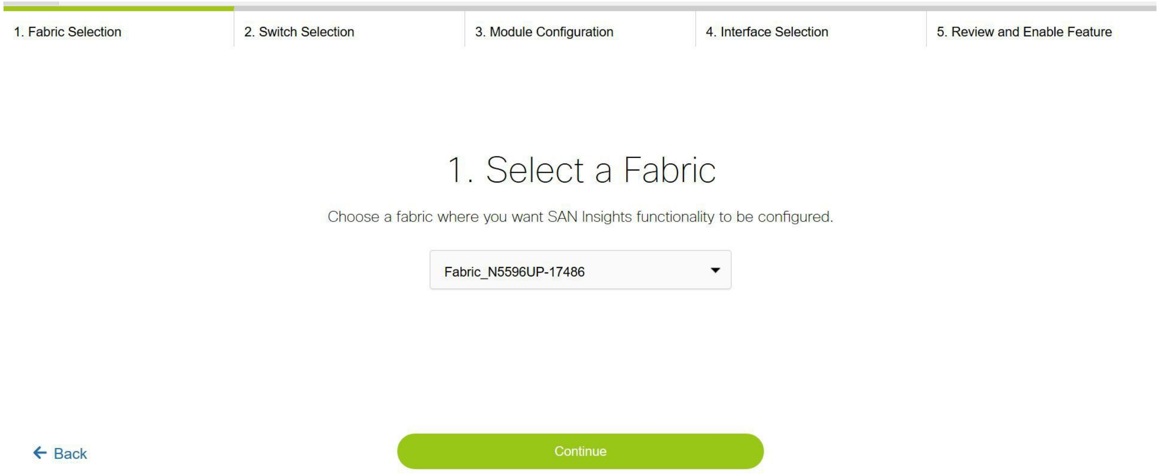
Enable on-box data collection. See how it works.

Important:

For SAN Insights streaming stability and performance, refer to the Server Resource Requirements section of the Cisco DCNM Installation Guide for SAN Deployment and the Increasing Elasticsearch Database Heap Size section of the DCNM SAN Management Configuration Guide.
Ensure system RAM is of adequate size.
Use of NTP is recommended to maintain time synchronization between DCNM and switches.
Enable PM collection for viewing counter statistics.

Step 2 In the **Configure SAN Insights** page, click **Continue**.

The **Fabric Selection** window appears.



1. Fabric Selection 2. Switch Selection 3. Module Configuration 4. Interface Selection 5. Review and Enable Feature

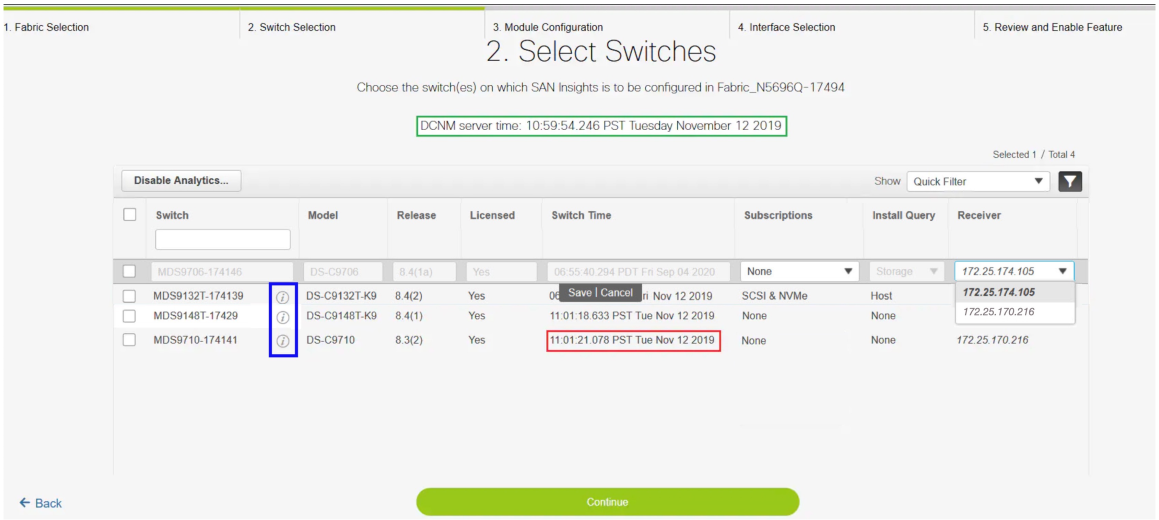
1. Select a Fabric

Choose a fabric where you want SAN Insights functionality to be configured.

Fabric_N5596UP-17486

Step 3 Select a fabric where you want the SAN Insights functionality to be configured. The wizard works with one fabric at a time.

If the switches don’t have SAN Insights license, the status in the Licensed column shows **No (install licenses)**. Click on **Install licenses** to apply license to the switch.



2. Select Switches

Choose the switch(es) on which SAN Insights is to be configured in Fabric_N5696Q-17494

DCNM server time: 10:59:54.246 PST Tuesday November 12 2019

Selected 1 / Total 4

□	Switch	Model	Release	Licensed	Switch Time	Subscriptions	Install Query	Receiver
□	MDS9706-174146	DS-C9706	8.4(1a)	Yes	06:55:40.294 PDT Fri Sep 04 2020	None	Storage	172.25.174.105
□	MDS9132T-174139 ⓘ	DS-C9132T-K9	8.4(2)	Yes	06 ri Nov 12 2019	SCSI & NVMe	Host	
□	MDS9148T-17429 ⓘ	DS-C9148T-K9	8.4(1)	Yes	11:01:18.633 PST Tue Nov 12 2019	None	None	
□	MDS9710-174141 ⓘ	DS-C9710	8.3(2)	Yes	11:01:21.078 PST Tue Nov 12 2019	None	None	172.25.170.216

Note The Cisco DCNM time is displayed and switch time is in RED if the switch time is found to be deviating from the DCNM time.

For the selected DCNM Receiver in the last column, the receiver can subscribe to telemetry: SCSI only, NVMe only, both SCSI & NVMe, or None. This allows you to configure one DCNM server to receive SCSI telemetry and another DCNM server to receive NVMe telemetry.

In Cisco DCNM SAN OVA/ISO deployments, the IP address that is assigned to eth0 or eth1 can be used for receiving SAN Insights streaming from the switch. However, ensure that streaming is configured to the DCNM interface having IP reachability from the respective switches. In the **Receiver** column all the discovered interfaces are listed. Choose the corresponding interface IP address that is configured while installing SAN OVA\ISO for streaming analytics data from the switch.

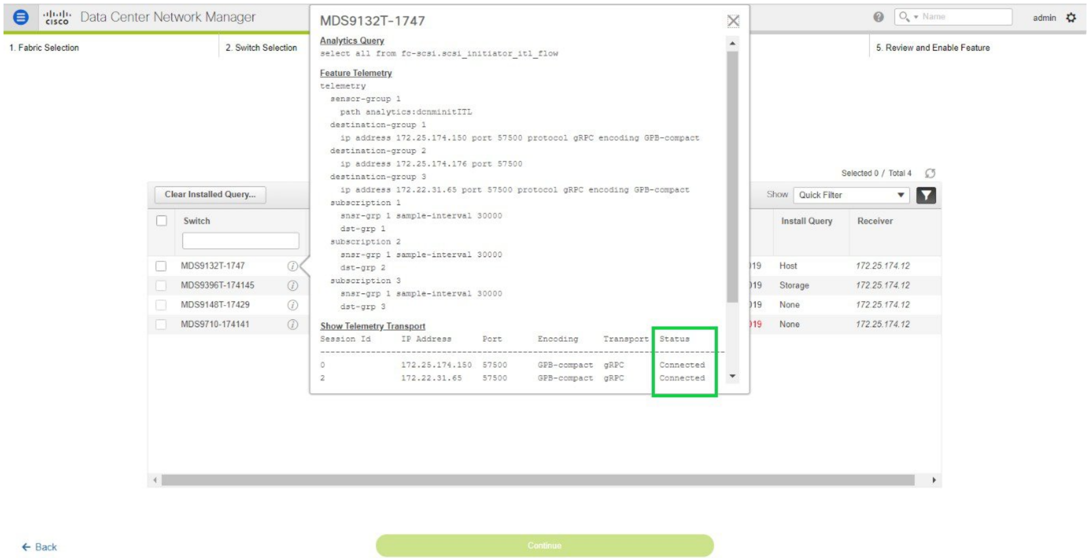
Beginning with Release 11.4(1), you can provide only the eth0 IP address to operate the DCNM OVA/ISO/SE. Therefore, the streaming must be configured to eth0 interface.

The Subscription column allows you to specify which protocol to which the Receiver subscribes. You can choose from SCSI, NVMe, both or none.

Note If you select **None for Subscription**, a warning message is displayed to select an appropriate Subscription before you proceed. Select the desired protocols for **Subscription**.

You can click the ⓘ (information) icon in the Switch column to get the configuration details for analytics and telemetry features from the switch (if Analytics Query and Telemetry features are configured).

If Analytics Query of either type (dcnminitITL, dcnmtgtITL, dcnmislpcITL, dcnminitITN, dcnmtgtITN, or dcnmislpcITN) isn’t configured on the switch, the telemetry configurations won’t be displayed.



Switch		Install Query	Receiver
MDS9132T-1747	)19	Host	172.25.174.12
MDS9396T-174145	)19	Storage	172.25.174.12
MDS9148T-17429	)19	None	172.25.174.12
MDS9710-174141	)19	None	172.25.174.12

MDS9132T-1747

Analytics Query

```
select all from fc-scsi.scsi_initiator_itl_flow
```

Feature Telemetry

```
telemetry
  sensor-group 1
    path analytics:dcnminitITL
  destination-group 1
    ip address 172.25.174.150 port 57500 protocol gRPC encoding GPB-compact
  destination-group 2
    ip address 172.25.174.176 port 57500
  destination-group 3
    ip address 172.22.31.65 port 57500 protocol gRPC encoding GPB-compact
  subscription 1
    snsr-grp 1 sample-interval 30000
    dst-grp 1
  subscription 2
    snsr-grp 1 sample-interval 30000
    dst-grp 2
  subscription 3
    snsr-grp 1 sample-interval 30000
    dst-grp 3
```

Show Telemetry Transport

```
Session Id    IP Address      Port     Encoding     Transport  Status
------------------------------------------------------------------------
0             172.25.174.150  57500    GPB-compact  gRPC       Connected
2             172.22.31.65    57500    GPB-compact  gRPC       Connected
```

Step 4 Click **Continue**. The switches that are capable of streaming analytics are listed in the **Select Switches** page.

Step 5 Select the switches on which SAN Insights must be configured.

Note Both Cisco DCNM and switch time are recorded and displayed when you navigate to the **Select Switches** page. This helps you to ensure that the clocks of Cisco DCNM and switch are in sync.

Click **Disable Analytics** to clear all the analytics and telemetry configuration on the selected switches.

If SAN Insights streaming was configured with KVGPB encoding using versions of Cisco DCNM SAN Insights older than 11.2(1), the switch continues to stream with KVGPB encoding while configuring streaming with DCNM versions 11.2(1) and above. From Cisco DCNM Release 11.2(1), Compact GPB streaming configuration for SAN Insights is supported. To stream using Compact GPB, the old KVGPB streaming must be disabled before configuring SAN Insights, newly after the upgrade.

In the **Install Query** column, choose one type of port per switch, and then click Save. You can choose from these options: **ISL**, **host**, or **storage**.

- **host**—lists all ports where hosts or initiators are connected on the switch.
- **storage**—lists all ports where storage or targets are connected on the switch.
- **ISL**—lists all ISL and port channel ISL ports on the switch.
- **None**—indicates that no query is installed.

The following queries are used:

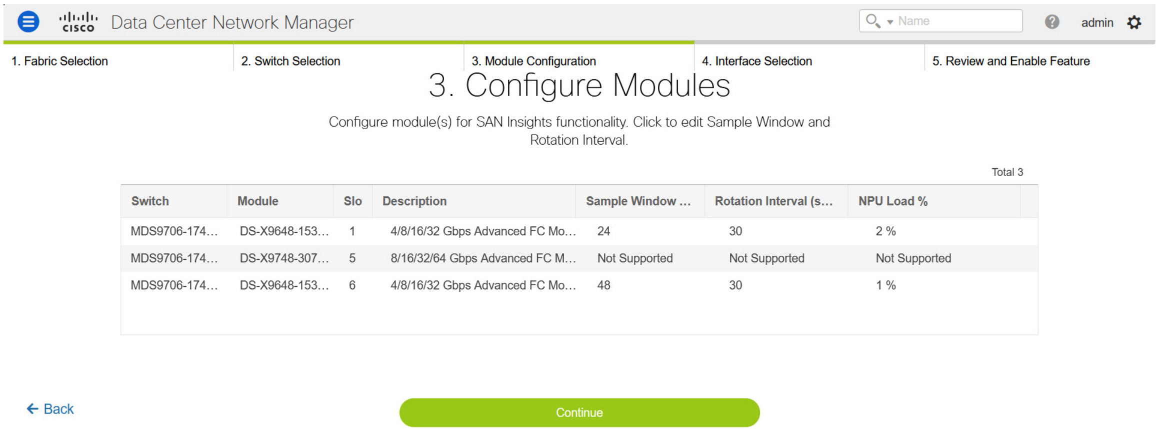
- dcnmtgtITL/dcnmtgtITN—This is the storage-only query.
- dcnminitITL/dcnminitITN—This is the host-only query.
- dcnmislpcITL/dcnmislpcITN—This is the ISL and pc-member query.

Note Cisco DCNM supports 20K (ITLs + ITNs) per DCNM server; however, it doesn't manage duplicate ITLs\ITNs. If you configure both host and storage queries (on the switches where their Hosts and Storage are connected respectively), the data is duplicated for the same ITL\ITN. This results in inconsistencies in the computed metrics.

Note From Cisco DCNM release 11.5(1), Cisco Nexus dashboard supports 60K (ITLs/ITNs), DCNM on OVA virtual appliances supports 40k ITLs/ITNs, and DCNM on Linux (RHEL) server supports 20K (ITLs/ITNs) for SAN deployments.

When the administrator selects the ISL\Host\Storage on the configure wizard, the respective ports are filtered and listed on the next step.

Step 6 Click **Continue**. You can see all the analytics supported modules on the switches that are selected in the previous view, which is listed with the respective instantaneous NPU load in the last column. Port-sampling configuration (optional) for the module can be specified in this step. The default configuration on the switch is to monitor all analytics-enabled ports on the switch for analytics.



3. Configure Modules

Configure module(s) for SAN Insights functionality. Click to edit Sample Window and Rotation Interval.

Total 3

Switch	Module	Slo	Description	Sample Window ...	Rotation Interval (s...	NPU Load %
MDS9706-174...	DS-X9648-153...	1	4/8/16/32 Gbps Advanced FC Mo...	24	30	2 %
MDS9706-174...	DS-X9748-307...	5	8/16/32/64 Gbps Advanced FC M...	Not Supported	Not Supported	Not Supported
MDS9706-174...	DS-X9648-153...	6	4/8/16/32 Gbps Advanced FC Mo...	48	30	1 %

Note If port sampling is enabled on multiple ISL ports with ISL query installed, the metrics aggregation isn't accurate. Because all exchanges won't be available at the same time, the metrics aggregation isn't accurate. We recommend that you don't use port sampling with ISL queries, with multiple ISLs.

Beginning with Release 11.5(4), Cisco DCNM supports discovery of 64G modules. Port-sampling is not supported on these modules and NPU load is not applicable for 64G SAN analytics. Therefore, you cannot configure sample window and rotation interval for 64G modules.

Note For 64G modules, you can edit the Sample Window field and enter the number of ports. However, the following error message appears:

```
Port sampling is not supported for this module.
```

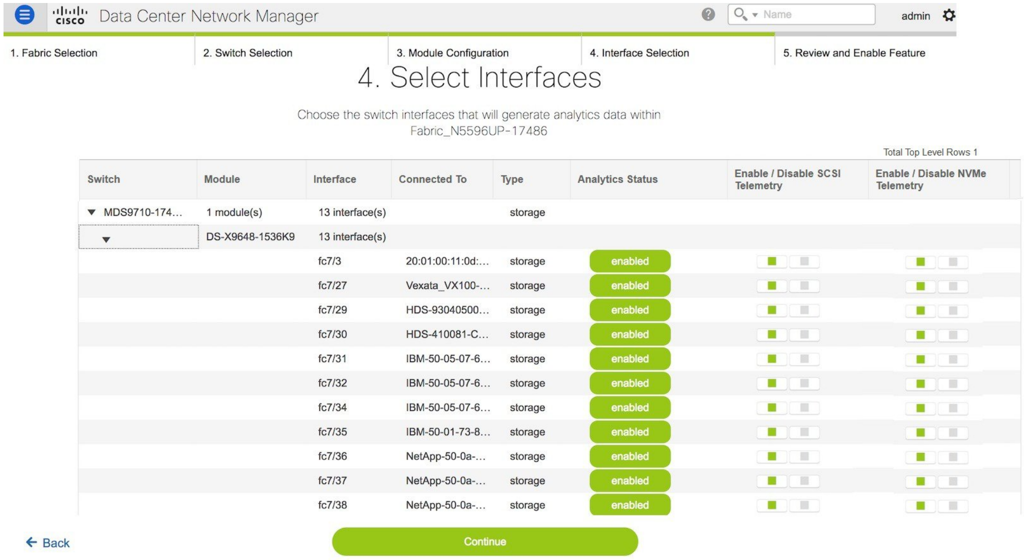
Step 7 In the **Configure Modules** tab, configure the module(s) for SAN Insights functionality.

To change the values for **Sample Window (ports)** and **Rotation Interval (seconds)**, click the row and enter the desired values.

- To undo the changes, click **Cancel**.
- To save changes, click **Save**.

The **NPU Load** column displays the Network Processing Unit (NPU) within a module.

Step 8 Click **Continue**.



4. Select Interfaces

Choose the switch interfaces that will generate analytics data within Fabric_N5596UP-17486

Total Top Level Rows 1

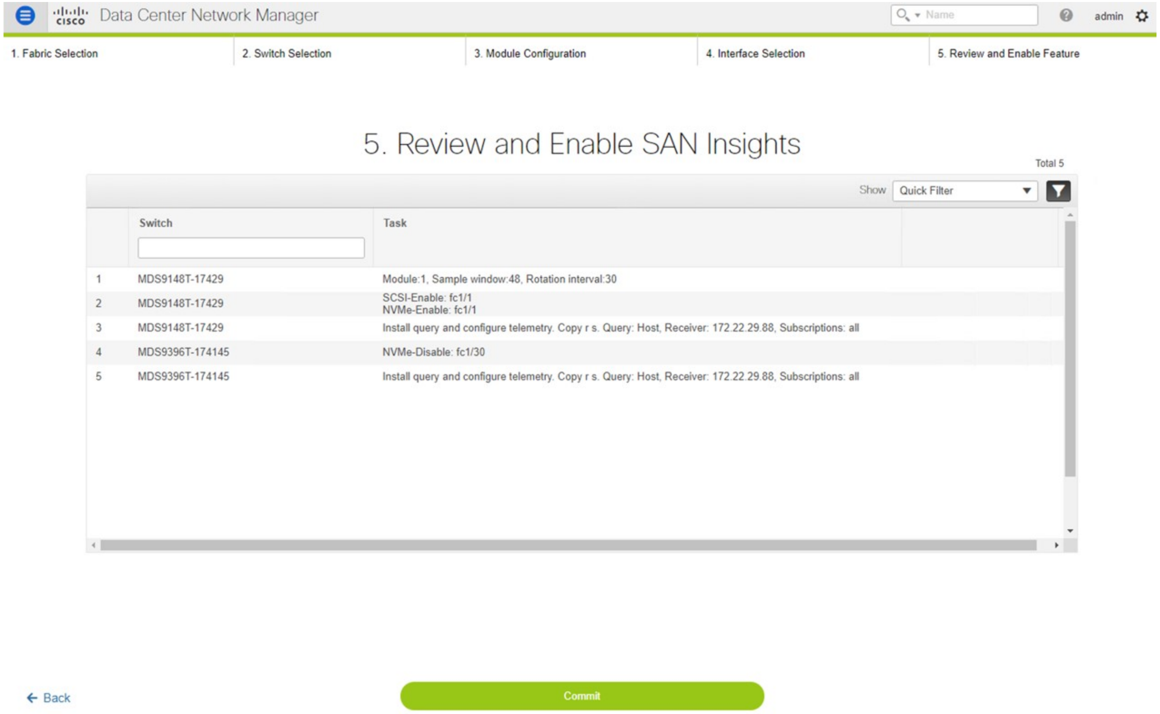
Switch	Module	Interface	Connected To	Type	Analytics Status	Enable / Disable SCSI Telemetry	Enable / Disable NVMe Telemetry
▼ MDS9710-174…	1 module(s)	13 interface(s)		storage			
▼	DS-X9648-1536K9	13 interface(s)					
		fc7/3	20:01:00:11:0d:…	storage	enabled	■ □	■ □
		fc7/27	Vexata_VX100-…	storage	enabled	■ □	■ □
		fc7/29	HDS-93040500…	storage	enabled	■ □	■ □
		fc7/30	HDS-410081-C…	storage	enabled	■ □	■ □
		fc7/31	IBM-50-05-07-6…	storage	enabled	■ □	■ □
		fc7/32	IBM-50-05-07-6…	storage	enabled	■ □	■ □
		fc7/34	IBM-50-05-07-6…	storage	enabled	■ □	■ □
		fc7/35	IBM-50-01-73-8…	storage	enabled	■ □	■ □
		fc7/36	NetApp-50-0a-…	storage	enabled	■ □	■ □
		fc7/37	NetApp-50-0a-…	storage	enabled	■ □	■ □
		fc7/38	NetApp-50-0a-…	storage	enabled	■ □	■ □

Step 9 In the **Select Interfaces** tab, select the interfaces that generate analytics data within the fabric.

For each interface, you can enable or disable telemetry by type: SCSI or NVMe enable SCSI only, NVMe only, both SCSI & NVMe, or None on each interface.

You can click the toggle button to enable or disable analytics on the desired port.

Step 10 Click **Continue**, and then review the changes that you have made.



5. Review and Enable SAN Insights

Total 5

	Switch	Task
1	MDS9148T-17429	Module:1, Sample window:48, Rotation interval:30
2	MDS9148T-17429	SCSI-Enable: fc1/1 NVMe-Enable: fc1/1
3	MDS9148T-17429	Install query and configure telemetry. Copy r s. Query: Host, Receiver: 172.22.29.88, Subscriptions: all
4	MDS9396T-174145	NVMe-Disable: fc1/30
5	MDS9396T-174145	Install query and configure telemetry. Copy r s. Query: Host, Receiver: 172.22.29.88, Subscriptions: all

Step 11 Click **Commit**. The CLI is executed on the switch.

Step 12 Review the results and see that the response is successful.

Note Some SAN Insights pages can take up to 2 hours to display data.

Step 13 Click **Close** to return to the home page. **Close** icon appears only after all CLI commands are executed on the switch.

Navigate to the **Configure** > **SAN Insights** page again, to modify the SAN Insights configurations.

Increasing Elasticsearch Database Heap Size

The Java heap size is the amount of memory allocated to applications running in the Java Virtual Machine used by DCNM server itself. Objects in heap memory can be shared between threads and improve performance. SAN Insights benefits from an appropriate quantity of heap.

From Release 11.3(1), the Elasticsearch heap size is set to 25% of the total system RAM for RHEL/OVA/ISO SAN deployments, up to a maximum of 32G heap size. SAN Insights require a minimum of 16GB Elasticsearch heap size for proper functioning. In Release 11.3(1), with adequate system RAM at the time of deployment, it won't be necessary to modify the Elasticsearch heap size.

To increase the Elasticsearch heap size for SAN OVA/ISO deployments, increase the total system RAM and restart the DCNM VM/Server. This increases the Elasticsearch heap size by 25% of the total system RAM.

Viewing Services

The SAN Insights feature uses PIPELINE and SanInsight process to listen to the switch port and collect data. These services are run on OVA as applications and are available on the **Web Client** > **Applications** > **Catalog**. They are identified as the SAN Insight Pipeline Collector, and SAN Insight Post Processor, respectively.

From Release 11.4(1), the San Insight Pipeline Collector and the SAN Insight Post Processing applications can only be paused and resumed from **Web UI** > **Applications** > **Catalog**.

CHAPTER 7

Administration

This chapter contains the following topics:

DCNM Server

The DCNM Server menu includes the following submenus:

Starting, Restarting, and Stopping Services

By default, the ICMP connectivity between DCNM and its switches validates the connectivity during Performance Management. If you disable ICMP, Performance Management data will not be fetched from the switches. You can configure this parameter in the **server properties**. To disable ICMP connectivity check from Cisco DCNM Web UI, choose **Administration** > **DCNM Server** > **Server Properties**, and set `skip.checkPingAndManageable` parameter value to `true`.

To clean up the performance manager database (PM DB) stale entries, start, restart, or stop a service, from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration** > **DCNM Server** > **Server Status**.

The **Status** window appears that displays the server details.

Step 2 In the **Actions** column, click the action you want to perform. You can perform the following actions:

- Start or restart a service.
- Stop a service.
- Clean up the stale PM DB entries.

- Reinitialize the Elasticsearch DB schema.

Step 3 View the status in the **Status** column.

What to do next

See the latest status in the **Status** column.

From Cisco DCNM Release 11.4(1), you can see the status of the following services as well:

Note The following services are available for OVA/ISO deployments only.

They are not applicable on Windows or Linux deployments.

- NTPD server: NTPD service running on DCNM OVA, the IP address, and the port to which the service is bound.
- DHCP server: DHCP service running on DCNM OVA, the IP address, and the port to which the service is bound.
- SNMP traps
- Syslog Receiver

The DCNM servers for these services are as follows:

Service Name	DCNM Server
NTPD Server	0.0.0.0:123
DHCP Server	0.0.0.0:67
SNMP Traps	0.0.0.0:2162
Syslog Server	0.0.0.0:514

Using the Commands Table

The commands table contains links to commands that launch new dialog boxes to provide information about the server status and server administrative utility scripts. You can execute these commands directly on the server CLI.

- **ifconfig**: click this link to view information about interface parameters, IP address, and netmask used on the Cisco DCNM server.
- **appmgr status all**: click this link to view the DCNM server administrative utility script that checks the status of different services currently running.
- **appmgr show vmware-info**: click this link to view information about the CPU and Memory of Virtual Machine.
- **clock**: click this link to view information about the server clock details such as time, zone information.

Note The commands section is applicable only for the OVA or ISO installations.

Customization

From Cisco DCNM Release 11.3(1), you can modify the background image and message on the Web UI login page. This feature helps you to distinguish between the DCNM instances, when you have many instances running at the same time. You can also use a company-branded background on the login page. Click on Restore Defaults to reset the customizations to their original default values.

To remove the customizations and restore to the default values, click **Restore defaults**.

Login Image

This feature allows you to change the background image on the Cisco DCNM Web UI login page. If you have many instances of DCNM, this will help you identify the correct DCNM instance based on the background image.

To edit the default background image for your Cisco DCNM Web UI login page, perform the following steps:

1. Choose **Administration > DCNM Server > Customization**.
2. In the Login Image area, click **Add (+)** icon.

   Browse for the image that you need to upload from your local directory. You can choose any of the following format images: JPG, GIF, PNG, and SVG.
3. Select the image and click **Open**.

   A status message appears on the right-bottom corner.

   ```
   Login image
   Upload Successful
   ```

   Note We recommend that you upload a scaled image for fast load times.

   The uploaded image is selected and applied as the background image.
4. To choose an existing image as login image, select the image and wait until you see the message on the right-bottom corner.
5. To revert to the default login image, click **Restore Defaults**.

Message of the day (MOTD)

This feature allows you to add a message to the Cisco DCNM Web UI login page. You can a list of messages that will rotate on the configured frequency. This feature allows you to convey important messages to the user on the login page.

To add or edit the message of the day on the Cisco DCNM Web UI login page, perform the following steps:

1. Choose **Administration > DCNM Server > Customization**.
2. In the **Message of the day (MOTD)** field, enter the message that must appear on the login page.
3. Click **Save**.

Viewing Log Information

You can view the logs for performance manager, SAN management server, SME server, web reports, web server, and web services. These processes have no corresponding GUI that allows you to view information about these log files. If you see errors, preserve these files for viewing.

Note Logs cannot be viewed from a remote server in a federation.

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

Procedure

Step 1 Choose **Administration > DCNM Server > Logs**.

You see a tree-based list of logs in the left column. Under the tree, there is a node for every server in the federation. The log files are under the corresponding server node.

Step 2 Click a log file under each node of the tree to view it on the right.

Step 3 Double-click the tree node for each server to download a ZIP file containing log files from that server.

Step 4 (Optional) Click **Generate Techsupport** to generate and download files required for technical support.

This file contains more information in addition to log files.

Note A TAR.GZ file will be downloaded for OVA and ISO deployments, and a ZIP file will be downloaded for all other deployments. You can use the use **appmgr tech_support** command in the CLI to generate the techsupport file.

Step 5 (Optional) Click the **Print** icon on the upper right corner to print the logs.

Server Properties

You can set the parameters that are populated as default values in the DCNM server.

To set the parameters of the DCNM server from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Server Properties**.

Step 2 Click **Apply Changes** to save the server settings.

Configuring SFTP/SCP Credentials

A file server is required to collect device configuration and restoring configurations to the device.

To configure the SFTP/SCP credentials for a file store from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Archive FTP Credentials**.

The **Archive FTP Credentials** window is displayed.

Note The credentials are auto-populated for fresh OVA and ISO installations.

Step 2 In the **Server Type** field, use the radio button to select **SFTP**.

Note

- You must have an SFTP server to perform backup operation. The SFTP server can be an external server. The SFTP directory must be an absolute Linux/SSH path format and must have read/write access to the SFTP User.
- If you are using an external server, enter its IP address in the **server.FileServerAddress** field in **Administration > DCNM Server > Server Properties**.
- If the **nat.enabled** field under **Administration > DCNM Server > Server Properties** is true, you must enter the NAT device IP in the **server.FileServerAddress** field and the SFTP server must be local.

a) Enter the **User Name** and **Password**.

Note From Release 11.3(1), for OVA/ISO installations, use the **sysadmin** user credentials to access the root directory.

b) Enter the **Directory** path.

The path must be in absolute Linux path format.

If SFTP is unavailable on your device, you can use third-party SFTP applications, such as, mini-SFTP, Solarwinds, and so on. When you use an external SFTP, you must provide the relative path in the STFP Directory Path. For example, consider the use cases at the end of this procedure.

Note From Release 11.3(1), for OVA/ISO installations, enter directory as `/home/sysadmin`.

c) From the **Verification Switches** drop-down list, select a switch.
d) Click **Apply** to save the credentials.
e) Click **Verify & Apply** to verify if SFTP and switch have connectivity and save the configuration.

If there are any failures during the verification, the new changes will not be stored.

f) Click **Clear SSH Hosts** to clear SSH hosts for all switches or selected switches.

If there is a failure in any of the switches, an error message appears. Navigate to **Configure > Backup > Switch Configuration > Archive Jobs > Job Execution Details** to view the number of successful and unsuccessful switches.

Step 3 In the **Server Type** field, use the radio button to select **TFTP**.

Cisco DCNM uses a local TFTP server for data transfer. Ensure that there is no external TFTP server running on the DCNM server.

Note Ensure that your switch user role includes the copy command. Operator roles receive a *permission denied* error. You can change your credentials in the **Discovery** window. Navigate to **Inventory > Discovery**.

a) From the **Verification Switch** drop-down list, select a switch.
b) Click **Apply** to save the credentials everywhere.
c) Click **Verify & Apply** to verify if TFTP and switch have connectivity and save the configuration.

If there are any failures during the verification, the new changes are not stored.

Step 4 In the **Server Type** field, use the radio button to select **SCP**.

Note

- You must have an SCP server to perform backup operation. The SCP server can be an external server. The SCP directory must be an absolute Linux/SSH path format and must have read/write access to the SCP User.
- If you are using an external server, enter its IP address in the **server.FileServerAddress** field under **Administration > DCNM Server > Server Properties**.
- If the **nat.enabled** field under **Administration > DCNM Server > Server Properties** is true, you must enter the NAT device IP in the **server.FileServerAddress** field and the server must be local.

a) Enter the **User Name** and **Password**.
b) Enter the **Directory** path.

The path must be in absolute Linux path format.

If SCP is unavailable on your device, use external SCP applications, such as, mini-SCP, Solarwinds, and so on. When you use an external SCP, you must provide the relative path in the SCP Directory Path. For example, consider the use cases at the end of this procedure.

c) From the **Verification Switches** drop-down, select the switch.
d) Click **Apply** to save the credentials everywhere.
e) Click **Verify & Apply** to verify if SCP and switch have connectivity and save the configuration. If there are any failures during the verification, the new changes will not be stored.
f) Click **Clear SSH Hosts** to clear SSH hosts for all switches or selected switches.

If there is a failure in any of the switches, an error message is displayed. To view the number of successful and unsuccessful switches, go to **Configure > Backup > Switch Configuration > Archive Jobs > Job Execution Details**.

Step 5 Choose **Configuration > Templates > Templates Library > Jobs** to view individual device verification status.

The configurations that are backed up are removed from the file server and are stored in the file system.

SFTP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms, like OVA, ISO, or Linux, and the test folder is located at `/test/sftp/`, you must provide the entire path of the SFTP directory. In the SFTP Directory field, enter `/test/sftp`.

Use Case 2:

If Cisco DCNM is installed on the Windows platform, and the test folder is located at `C://Users/test/sftp/`, you must provide the relative path of the SFTP directory. In the SFTP Directory field, enter `/`.

For Example:

- If the path in the external SFTP is `C://Users/test/sftp/`, then the Cisco DCNM SFTP Directory path must be `/`.
- If the path in the external SFTP is `C://Users/test`, then the Cisco DCNM SFTP Directory path must be `/sftp/`.

Examples for SCP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms, like OVA, ISO, or Linux, and the test folder is located at `/test/scp/`, you must provide the entire path of the SCP directory. In the **SCP Directory** field, enter `/test/scp`.

Use Case 2:

If Cisco DCNM is installed on the Windows platform, and the test folder is located at `C://Users/test/scp/`, you must provide the relative path of the SCP directory. In the **SCP Directory** field, enter `/`.

For Example:

- If the path in the external SCP is `C://Users/test/scp/`, then the Cisco DCNM SCP directory path must be `/`.
- If the path in the external SCP is `C://Users/test`, then the Cisco DCNM SCP directory path must be `/scp/`.

Modular Device Support

To support any new hardware that does not require many major changes, a patch can be delivered instead of waiting for the next DCNM release. **Modular Device Support** helps to deliver and apply the DCNM patch releases. An authorized DCNM administrator can apply the patch to the production setup. Patch releases are applicable for the following scenarios:

- Support any new hardware, like chassis or line cards

- Support latest NX-OS versions
- Support critical fixes as patches

To view the patch details from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration** > **DCNM Server** > **Modular Device Support**.

You see the **DCNM Servers** column on the left in the window and **Modular Device support information** window on the right.

Step 2 Expand **DCNM Servers** to view all the DCNM servers.

It includes the list of patches installed along with the version number, corresponding platforms supported, chassis supported, NX-OS version supported, PID supported, backup directory and the last patch deployment time in the **Modular Device support information** table.

What to do next

For more details about how to apply and rollback a patch, go to http://www.cisco.com/go/dcnm for more information.

Managing Switch Groups

You can configure switch groups by using Cisco DCNM Web UI. You can add, delete, or move a switch to a group, or move switches from a group to another group.

This section contains the following:

Adding Switch Groups

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

Procedure

Step 1 Choose **Administration** > **DCNM Server** > **Switch Groups**.

Step 2 Click the **Add** icon.

The **Add Group** window is displayed, that allows you to enter the name for the switch group.

Step 3 Enter the name of the switch group and click **Add** to complete adding the switch group.

The switch group name validation, and the maximum tree depth is 10. If you do not choose a parent group before adding a new switch group, the new group is added on the top of the hierarchy.

Removing a Group or a Member of a Group

You can delete a group or a member of the group from the Cisco DCNM Web UI. When you delete a group, the associated groups are deleted. The fabrics or ethernet switches of the deleted groups are moved to the default SAN or LAN.

To remove a group or a member of a group from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose the switch group or members of a group that you want to remove.

Step 2 Click the **Remove** icon.

A dialog box prompts you to confirm the deletion of the switch group or the member of the group.

Step 3 Click **Yes** to delete or **No** to cancel the action.

Moving a Switch Group to Another Group

To move a switch group to another group from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Select a switch or switch group.

Step 2 Drag the highlighted switch or switch group to another group.

To move multiple switches across different switch groups, use **Ctrl** key or **Shift** key.

You can see the switch or switch group. Users are not allowed to move multiple switches in the group level under the new group now.

Note It is not allowed to move multiple switches in the group level. You may not mix a group with switches.

Managing Custom Port Groups

Custom port groups aid you to test the performance of the interfaces in the group. You can view the defined custom ports and their configurations.

This section includes the following topics:

Adding Custom Port Groups

To add a custom port group from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Custom Port Groups**.

The **Custom Port Groups** window is displayed.

Step 2 In the **User-Defined Groups** block, click the **Add** icon.

Step 3 Enter the name for the custom port group in the **Add Group Dialog** window.

Step 4 Click **Add**.

A custom port group is created in the **User-Defined Groups** area.

Configuring Switch and Interface to the Port Group

To configure the custom port group to include switches and interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Custom Port Groups**.

Step 2 In the **User-Defined Groups** area, select the port group to add the switch and interfaces.

Step 3 In the **Configurations** area, click **Add Member**.

The **Port Configuration** window appears for the selected custom port group.

Step 4 In the **Switches** tab, select the switch to include in the custom port group.

The list of available **Interfaces** appears.

Step 5 Select all the interfaces to check the performance.

Step 6 Click **Submit**.

The list of interfaces is added to the custom port group.

Removing Port Group Member

To remove or delete a port group member in a custom port group from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Custom Port Groups**.

Step 2 In the **User Defined Groups** area, select a port group.

Step 3 In the **Configuration** area, select the switch name and interface that must be deleted.

Step 4 In the **User Defined Groups** area, select the group from which the member must be deleted.

Step 5 Click **Remove Member**.

A confirmation window appears.

Step 6 Click **Yes** to delete the member from the custom port group.

Removing Port Group

To remove or delete a port group from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Custom Port Groups**.

Step 2 In the **User Defined Groups** area, select the group which must be deleted.

Step 3 Click **Remove**.

A confirmation window appears.

Step 4 Click **Yes** to delete the custom group.

Viewing Server Federation

Note There must be a minimum of 3 nodes in the Federation set up for failover to function correctly. In a 2 node Federation setup, if one of the servers is down, the Elasticsearch cannot form the cluster, and therefore the Web UI may behave inconsistently. In the case of a 3 node Federation setup, if two servers are down, inconsistent behavior of the WebUI is seen.

Note Ensure that you clear your browser cache and cookies everytime after a Federation switchover or failover.

To view federation server information in Cisco DCNM, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Federation**.

The list of servers along with its IP address, status, location, local time, and data sources are displayed.

Step 2 Use the **Enable Automatic Failover** check box to turn on or turn off the failover functionality.

Step 3 In the **Location** column, double-click to edit the location.

If the status of one of the servers in the federation is **Inactive**, some functionality may not work unless the server status changes to **Active**.

Note Before upgrading Cisco DCNM, ensure that **Enable Automatic Failover** is unchecked. Otherwise, if one server within the federation is down, the devices are moved to the other DCNM server which comes up first after the upgrade. To prevent the automove for DCNM upgrade, you must disable the automove on all DCNMs within the federation, and upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.

Note In DCNM Federation, when **Enable Automatic Failover** is enabled, if a DCNM is down, the devices under its management is moved to the other DCNM. However after the DCNM is back, the devices will not move back.

Note When you upgrade Cisco DCNM Federation, you need to revisit the **Administration** > **DCNM Server** > **Federation** page, and run the Elasticsearch cluster sync command after the upgrade is complete. This will update the Elasticsearch configurations and restart performance monitoring. To run the Elasticsearch cluster sync command, you need to enable Elasticsearch clustering button in the **Administration** > **DCNM Server** > **Federation** page. To restart the performance monitoring, choose **Administration** > **DCNM Server** > **Server Status**, and click the green button.

The **ElasticSearch Cluster** section gives the details about the elastic search. It has the following fields:

Field	Description
Name	Specifies the name of the elastic search cluster.
Nodes	Specifies the number of instances clustered.
Status	Specifies if the cluster is enabled or not. If the cluster is not enabled, the status is yellow. If the cluster is enabled, the status is green.

Elasticsearch Clustering

Note The **ElasticSearch Clustering** sync-up option is available only on the Primary node in the Federation setup.

To sync each of the elastic search nodes that are associated with a federated server, into an elastic search cluster, perform the following steps:

Procedure

Step 1 In the **Federation** window, click **ElasticSearch Clustering**. The **Elastic Search Clustering** pop-up window appears.

Step 2 Click **Apply**.
This operation synchronizes each of the elastic search nodes that are associated with a federated server, into an elastic search cluster. The operation is disruptive to any features using elastic search as a data store. Some features are impacted by ongoing data synchronization operations after the elastic search services are resumed.

Multi Site Manager

Procedure

Step 1 Multi-Site-Manager (MsM) provides a single pane for users to search for switches that are managed by DCNM globally. MSM can do realtime search to find out which switch globally handles the traffic for a given virtual machine based on IP address, name or mac address, and supporting VXLAN basing on segment ID as well. It provides hyperlink to launch the switch only. This window also plays the role of remote site registration. The registration only allows the current DCNM server to access the remote DCNM server or site. For the remote site to access the current DCNM server, registration is required on the remote site as well.

Step 2 Choose **Administration > DCNM Server > Multi Site Manager**.

The MsM window displays the overall health or status of the remote site and the application health.

Step 3 You can search by **Switch, VM IP, VM Name, MAC**, and **Segment ID**.

Step 4 You can add a new DCNM server by clicking **+Add DCNM Server**. The **Enter Remote DCNM Server Information** window opens. Fill in the information that is required and click **OK** to save.

Step 5 Click **Refresh All Sites** to display the updated information.

Device Connector

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

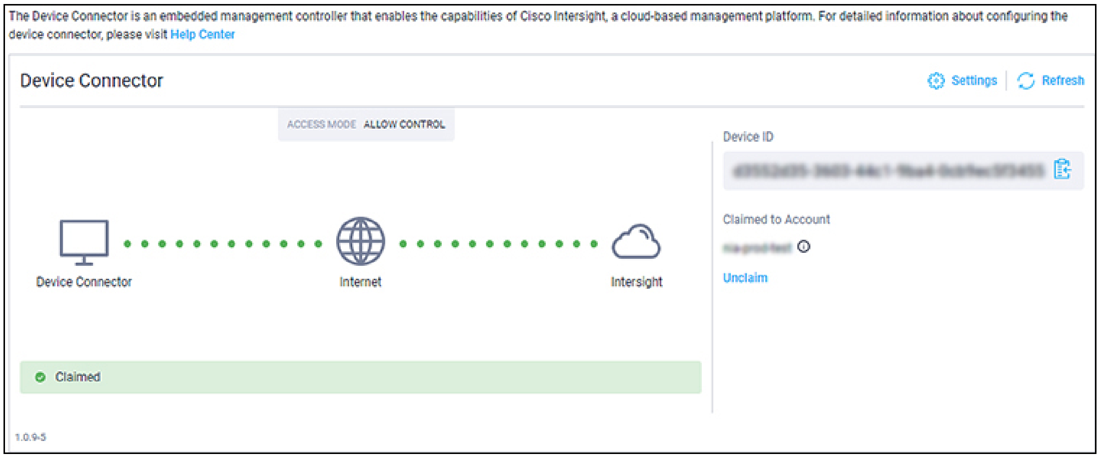
Networks Insights applications are connected to the Cisco Intersight cloud portal through a Device Connector which is embedded in the management controller of the Cisco DCNM platform. Cisco Intersight is a virtual appliance that helps manage and monitor devices through the Network Insights application. The Device Connector provides a secure way for connected DCNM to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

Configuring Device Connector

To configure the Device Connector from the Cisco DCNM Web UI, perform the following steps:

1. Choose **Administration > DCNM Server > Device Connector**.

   The Device Connector work pane appears.



The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

Device Connector

Device ID

[redacted]

Claimed to Account

[redacted]

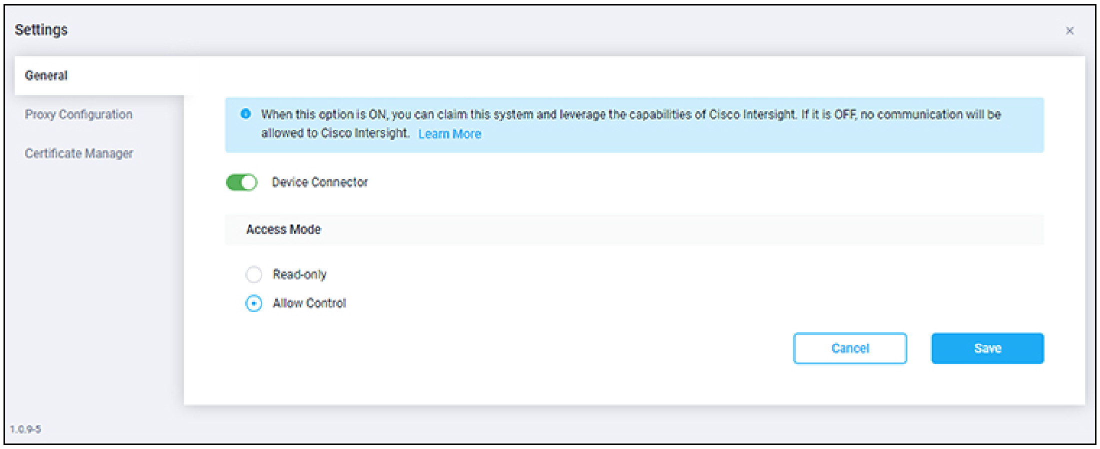
Claimed

1.0.9-5

307463

2. Click **Settings**.

The **Settings - General** window appears.



Settings

When this option is ON, you can claim this system and leverage the capabilities of Cisco Intersight. If it is OFF, no communication will be allowed to Cisco Intersight. Learn More

Device Connector: ON

Access Mode

○ Read-only

● Allow Control

1.0.9-5

307465

- **Device Connector (switch)**

  This is the main switch for the Device Connector communication with Cisco Intersight. When the switch is on (green highlight), the Device Connector claims the system and leverages the capabilities of the Cisco Intersight. If the switch is off (gray highlight), no communication can occur between Cisco DCNM and Cisco Intersight.

- **Access Mode**

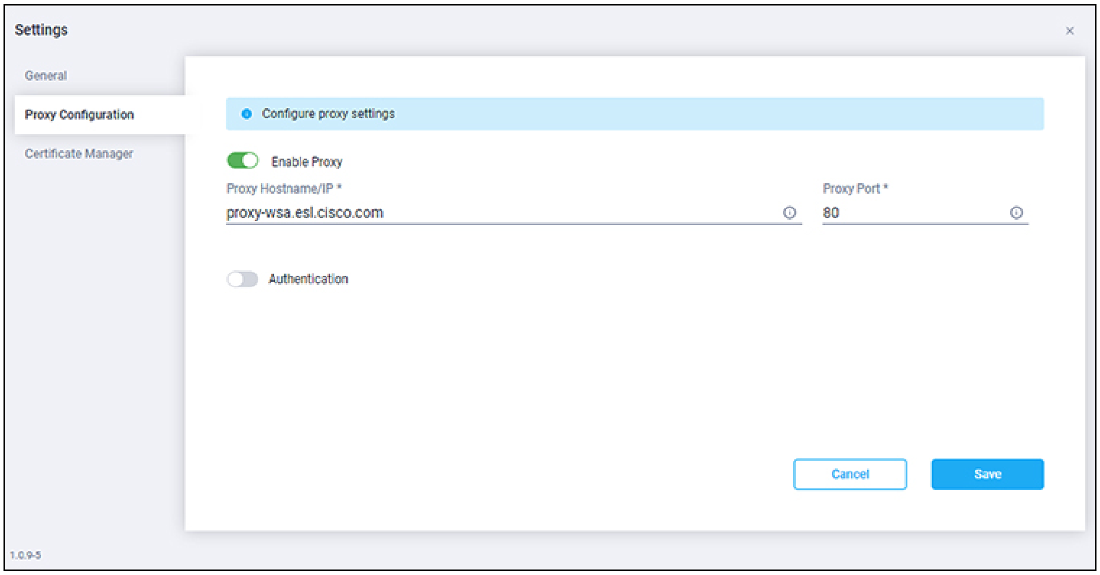
  - **Read-only**: This option ensures that there are no changes to this device from Intersight. For example, actions such as upgrading firmware or a profile deployment is not allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.

  - **Allow Control**: This option (selected by default) enables you to perform full read/write operations from the appliance, based on the features available in Cisco Intersight.

3. Set the Device Connector to on (green highlight) and choose **Allow Control**.

4. Click **Proxy Configuration**.

The **Settings - Proxy Configuration** window appears.



Configure proxy settings

Enable Proxy

Proxy Hostname/IP *: proxy-wsa.esl.cisco.com

Proxy Port *: 80

Authentication

- **Enable Proxy (switch)**

  Enable HTTPS Proxy to configure the proxy settings.

Note Network Insights requires Proxy settings.

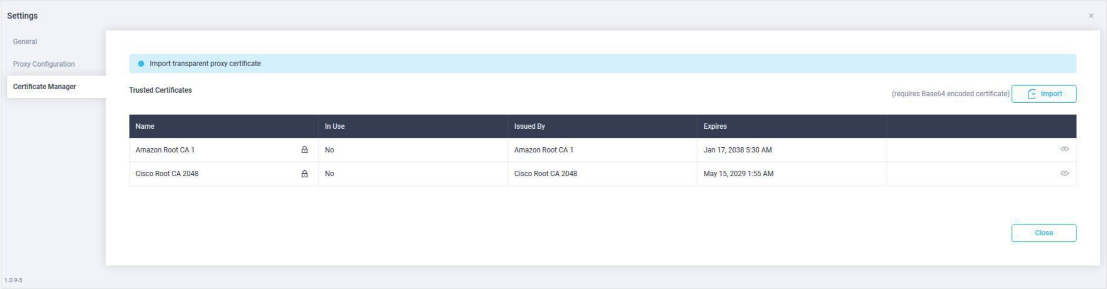
- **Proxy Hostname/IP* and Proxy Port***: Enter a proxy hostname or IP address, and a proxy port number.
- **Authentication (switch)**

  Enable proxy access through authentication. When the switch is on (green highlight), authentication to the proxy server is required. If the switch is off (gray highlight), it does not require authentication.

  Username* and Password: Enter a user name and password for authentication.

  The device connector does not mandate the format of the login credentials, they are passed as-is to the configured HTTP proxy server. The username must be a qualified domain name depending on the configuration of the HTTP proxy server.

5. Enable the proxy (green highlight) and enter a hostname and port number.
6. (Optional) If proxy authentication is required, enable it (green highlight) and enter a username and password.
7. Click **Save**.
8. Click **Certificate Manager**.



Name	In Use	Issued By	Expires	
Amazon Root CA 1	No	Amazon Root CA 1	Jan 17, 2038 5:30 AM	
Cisco Root CA 2048	No	Cisco Root CA 2048	May 15, 2029 1:55 AM	

The trusted certificates appear in the table.

A list of trusted certificates appears. You can import a valid trusted certificate.

- **Import**

  Browse the directory, choose, and import a CA signed certificate.

Note The imported certificate must be in the ***.pem (base64encoded)** format.

- You can view the list of certificates with the following information:
  - **Name**—Common name of the CA certificate.
  - **In Use**—Whether the certificate in the trust store is used to successfully verify the remote server.
  - **Issued By**—The issuing authority for the certificate.
  - **Expires**—The expiry date of the certificate.

Note You cannot delete bundled certificates.

NX-API Certificate Management for Switches

Cisco NX-OS switches require an SSL certificate to function in NX-API HTTPS mode. You can generate the SSL certificates and get it signed by your CA. You can install the certificates manually using CLI commands on switch console.

From Release 11.4(1), Cisco DCNM provides a Web UI framework to upload NX-API certificates to DCNM. Later, you can install the certificates on the switches that are managed by DCNM.

This feature is supported only on Cisco DCNM OVA/ISO deployments.

Note This feature is supported on switches running on Cisco NXOS version 9.2(3) or higher.

For each switch, the data center administrator generates an ASCII (base64) encoded certificate. This certificate comprises two files:

- `.key` file that contains the private key
- `.crt/.cer/.pem` file that contains the certificate

Cisco DCNM also supports a single certificate file that contains an embedded key file, that is, `.crt/.cer/.pem` file can also contain the contents of .key file.

DCNM doesn't support binary encoded certificates, that is, the certificates with `.der` extension are not supported. You can protect the key file with a password for encryption. Cisco DCNM does not mandate encryption; however, as this is stored on DCNM, we recommend that you encrypt the key file. DCNM supports AES encryption.

You can either choose CA-signed certificates or self-signed certificates. Cisco DCNM does not mandate the signing; however, the security guidelines suggest you use CA-signed certificates.

You can generate multiple certificates meant for multiple switches, to upload to DCNM. Ensure that you name the certificates appropriately, to help you choose the switch meant for that certificate.

You can upload one certificate and corresponding key file, or bulk upload multiple certificates and key files. After the upload is complete, you can view the upload list before installing these on the switches. If a certificate file that contains an embedded key file is uploaded, DCNM derives the key automatically.

Certificate and the key file must have the same filename. For example, if a certificate filename is `mycert.pem`, the key filename must be `mycert.key`. If the certificate and key pair filenames are not the same, then DCNM will not be able to install the certificate on the switch.

Cisco DCNM allows you to bulk install the certificates to the switches. Because bulk installation uses the same password, all encrypted keys must be encrypted with the same password. If the password is different for a key, you cannot install the certificate in bulk mode. Bulk mode installation allows you to install encrypted and unencrypted keys certificates together, but all encrypted keys must have the same password.

When you install a new certificate on the switch, it replaces the existing certificate and replaces it with the new certificate.

You can install the same certificate on multiple switches; however, you cannot use the bulk upload feature.

Note DCNM doesn't enforce the validity of certificates or options provided in it. It is up to you and the requirements on the switch to follow the convention. For example, if a certificate is generated for Switch-1 but it is installed on Switch-2, DCNM doesn't enforce it; switches may choose to accept or reject a certificate based on the parameters in the certificate.

On Cisco DCNM **Web UI > Administration > DCNM Server > NX API Certificates**, the following tables are displayed:

- **Certificate Installation Status table**: Displays the status of certificates last installed on the switches. It also displays the time when the certificates were updated previously.
- **Certificates Uploaded to DCNM table**: Displays the certificates uploaded on DCNM and any switch association.

  However, refer to the Certificate Installation Status table to see the certificate and switch association. Upload table is only meant for uploading certificates on DCNM and installing on the switches.

You can also watch the video that demonstrates how to use Switch NX-API SSL Certificate Management feature. See Video: Switch NX-API SSL Certificate Management.

Uploading the certificates on DCNM

To upload the certificates onto DCNM using the Cisco DCNM Web Client UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > NX API Certificates**.

Step 2 In the **Certificates Uploaded to DCNM** area, click **Upload Certificates** to upload the appropriate license file.

Step 3 Browse your local directory and choose the certificate key pair that you must upload to DCNM.

You can choose certificates with extension .cer/.crt/.pem + .key file separately.

Cisco DCNM also allows you to upload a single certificate file that contains an embedded key file. The key file is automatically derived after upload.

Step 4 Click **Open** to upload the selected files to DCNM.

A successful upload message appears. The uploaded certificates are listed in the **Certificates Uploaded to DCNM** area.

In the **Certificate Installation Status** area, the certificate appears, with Status as **UPLOADED**.

If the certificate is uploaded without the key file, the status shows **KEY_MISSING**.

Installing Certificates on Switches

To install certificates on the switches using Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > NX API Certificates**.

Step 2 In the **Certificate Installation Status** area, for each certificate, click on the **Switch** column.

Step 3 From the drop-down list, select the switch to associate with the certificate.

Click **Save**.

Step 4 Select the certificate that you need to install and click **Install Certificates on Switch**.

You can select multiple certificates to perform a bulk install.

Step 5 In the **Bulk Certificate Install** window, upload the certificates to DCNM. Perform the following steps:

You can install a maximum of 20 certificates at the same instance, using the Bulk Install feature.

a) Choose the file transfer protocol to upload the certificate to DCNM.

   You can choose either SCP or SFTP protocol to upload the certificates.

b) Check the VRF checkbox for the certificates to support the VRF configuration.

   Enter the VRF name that the switch uses to reach DCNM. Generally, DCNM is reached via management VRF of switches, but it can be any VRF that is configured on the switch that is used to reach DCNM.

c) In the NX-API Certificate Credentials, enter the password which was used to encrypt the key while generating the certificates.

Leave this field empty, if the key uploaded along with the certificate is not encrypted.

Note that you can install unencrypted and encrypted keys and a certificate in a single bulk install; however, you must provide the key password used for encrypted keys.

d) Click **Install**.

A notification message appears to confirm if the certificate was successfully installed on the specific switch.

In the Certificate Installation Status area, the Status of certificate now shows **INSTALLED**.

Unlinking and Deleting certificates

After the certificates are installed on the switch, DCNM cannot uninstall the certificate from DCNM. However, you can always install a new certificate on the switch. The certificates that are not installed on the switches can be deleted. To delete the certificate installed on the switch, you must unlink the certificate from the switch, and then delete it from DCNM.

Note Unlinking the certificate from the switch does not delete the certificate on the switch. The certificate still exists on the switch. Cisco DCNM cannot delete the certificate on the Switch.

To delete certificates from DCNM repository, using the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > NX API Certificates**.

Step 2 In the **Certificate Installation Status** area, select the certificate(s) that you need to delete.

Step 3 Click **Clear** Certificates.

A confirmation message appears.

Step 4 Click **OK** to clear the selected certificates.

The status column shows UPLOADED. The Switch column shows NOT_INSTALLED.

Step 5 Select the certificate and click **Clear Certificates**.

The Certificate is removed from the Certificate Installation Status table.

Step 6 In the Certificates Uploaded to DCNM area, select the certificate that is now unlinked from the Switch.

Click **Delete Certificates**.

The certificate is deleted from DCNM.

Troubleshooting NX API Certificate Management

While installing a certificate, you can encounter errors. The following sections provide information about troubleshooting the NX-API Certificate Management for switches.

COPY_INSTALL_ERROR

Problem Statement: Error message COPY_INSTALL_ERROR

Reason Cisco DCNM cannot reach the switch.

Solution:

- Verify if the switch is reachable from Cisco DCNM. You can perform an SSH login and ping the switch to verify.
- Switch connects to DCNM through it's management interface. Verify if you can ping DCNM from the Switch console. If the switch requires VRF, very if the correct vrf is provided.
- If the certificate private key is encrypted, ensure that you provide the correct password.
- Verify is the correct key file is uploaded with the certificate. Ensure that the certificate file and the key file have the same filename.

CERT_KEY_NOT_FOUND

Problem Statement: Error message CERT_KEY_NOT_FOUND

Reason: Key file was not uploaded while uploading the certificate (.cer, .crt, .pem).

Solution:

- Ensure that the certificate (.cer, .crt, or .pem) file and its corresponding .key file has the same filename

  For example: If the certificate file name is mycert.crt, the key file must be mycert.key.
- DCNM identifies key file with certificate file name, and therefore, it is necessary to have the key file with same filename.
- Upload the certificate and key file with same filename, and install the certificate.

Backing up DCNM

From Cisco DCNM, Release 11.5(1), you can trigger scheduled DCNM backups from the Cisco DCNM Web UI. When you trigger a backup from the Web UI, the **appmgr backup** command is run. You can see the following information under the **Server Backup Jobs** tab in the **Backup** window.

Table 32: Server Backup Jobs Tab

Parameters	Description
Node	Specifies if the backup is active or standby. For standalone nodes, it will appear as a localpath. **Note** For HA cluster, one active node and one standby node is created. However, you can choose only the active node for an HA cluster.
Schedule	Specifies when the scheduled backup is triggered.
Local Path	Specifies the local path, where the backup is stored.
Remote Destination	Specifies the username, host IP, and the remote destination, where the backup is stored. It is empty if you do not save the backup in a remote location. **Note** A copy of the backup is also stored in the local path.
Log Path	Specifies the path where the log entries are stored. You can use this information to troubleshoot any issues.
Saved Backups	Specifies the number of versions of a backup. The default value is 5.

You can perform the following actions in the **Backup** window:

Creating a Backup

To create a backup from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration** > **DCNM Server** > **Backup**.

The **Backup** window appears, which has all the information under the **Server Backup Schedules** area.

Step 2 Click **Add**.

The **Create Backup Schedule** dialog box appears.

Step 3 Choose the time using the **Start At** drop-down list under the **Schedule** area.

Step 4 Choose the frequency of the backup.

The valid options are:

- **Daily**: Select this radio button if you want to trigger the backup everyday.

- **Weekly**: Select this radio button if you want to trigger the backup once a week. If you select this radio button, you get options to choose the day.

Step 5 Enter the number of backups you want to save in the **Max # of Saved Backups** field under the **Destination** area.

You can save upto 10 backups and the default value is 5.

Step 6 (Optional) Check the **Remote Destination** check box to save the backup in a remote location.

The following fields will be available after you check the **Remote Destination** check box.

Fields	Descriptions
User	Enter the username.
Password	Enter the password. **Note** You don't have to enter the password if you have enabled the key-less configuration between your DCNM and the remote host.
Host IP	Enter the host IP address which is connected to your DCNM.
Path	Enter the remote destination path where you want to save the backup.

Note

- The backup files are huge, with the size in gigabytes.
- A copy of the backup will always be saved in the local destination as well.

Step 7 Click **Create**.

The **Backup** window is populated even when you run the **appmgr backup** command using the CLI. You can also view the backups, which you scheduled from the Web UI, in the CLI using the **appmgr backup schedule show** command.

Modifying a Backup

To modify a backup from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Backup**.

The **Backup** window appears, which has all the information under the **Server Backup Schedules** area.

Step 2 Click **Modify**.

The **Modify Backup Schedule** dialog box appears.

Step 3 Make the necessary changes.

Step 4 Click **Modify**.

Deleting a Backup

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

Procedure

Step 1 Choose **Administration** > **DCNM Server** > **Backup**.

The **Backup** window appears, which has all the information under the **Server Backup Schedules** area.

Step 2 Click **Delete**.

The confirmation dialog box appears.

Step 3 Click **Yes**.

Note If you run the **appmgr backup schedule none** command in the CLI, the backup is deleted. You can verify if the backup is deleted by refreshing the **Backup** window.

Job Execution Details

You can see the following information under the **Job Execution Details** tab in the **Backup** window.

Table 33: Server Backup Schedules Area

Parameters	Description
Node	Specifies if the node is active or standby. For standalone nodes, it will appear as a local node.
Backup File	Specifies the path, where the backup is stored.
Start Time	Specifies the time when the backup process started.
End Time	Specifies the time when the backup process ended.
Log File	Specifies the path where the log entries are stored. You can use this information to troubleshoot any issues.
Status	Specifies if the backup was a success or failed.
Error Message	Specifies error messages, if any, that appeared during the backup.

Manage Licensing

The Manage Licensing menu includes the following submenus:

Managing Licenses

You can view the existing Cisco DCNM licenses by choosing **Administration > Manage Licensing > DCNM**. You can view and assign licenses in the following tabs:

- **License Assignments**
- **Smart License**
- **Server License Files**

Note By default, the **License Assignments** tab appears.

The following table displays the SAN and LAN license information.

Field	Description
License	Specifies SAN or LAN.
Free/Total Server-based Licenses	Specifies the number of free licenses that are purchased out of the total number of licenses. The total number of licenses for new installations are 50. However, the total number of licenses continues to be 500 for inline upgrade.
Unlicensed/Total (Switches/VDCs)	Specifies the number of unlicensed switches or VDCs out of the total number of switches or VDCs.
Need to Purchase	Specifies the number of licenses to be purchased.

This section includes the following topics:

License Assignments

The following table displays the license assignment details for every switch or VDC.

Field	Description
Group	Displays if the group is fabric or LAN.
Switch Name	Displays the name of the switch.
WWN/Chassis ID	Displays the world wide name or Chassis ID.
Model	Displays the model of the device. For example, DS-C9124 or N5K-C5020P-BF.

Field	Description
License State	Displays the license state of the switch that can be one of the following: • Permanent • Eval • Unlicensed • Not Applicable • Expired • Invalid • Smart
License Type	Displays the license type of the switch that can be one of the following: • DCNM-Server • Switch • Smart • Honor • Switch-Smart
Expiration Date	Displays the expiry date of the license. **Note** Text under the **Expiration Date** column is in red for licenses, which expire in seven days.
Assign License	Select a row and click this option on the toolbar to assign the license.
Unassign License	Select a row and click this option on the toolbar to unassign the license. **Note** If you unassign licenses of all switches in a fabric, even the fabric is unlicensed. However, in a federated setup after you unassign the license for a fabric, restart the PM service so that the fabric is no longer listed in the **SAN Collections** window. Restarting the PM is required to move the fabric from one node to another node successfully.
Assign All	Click this option on the toolbar to refresh the table and assign the licenses for all the items in the table.
Unassign All	Click this option on the toolbar to refresh the table and unassign all the licenses.

Note You must have network administrator privileges to assign or unassign licenses.

When the fabric is first discovered and if the switch does not have a valid switch-based license, a license is automatically assigned to the fabric from the file license pool until no more licenses are left in the pool. If you have an existing fabric and a new switch is added to the fabric, the new switch is assigned a license if one is available in the file license pool and if it does not already have a switch-based license.

After you register smart license, if you click **Assign License** for a switch that does not have a permanent license, a smart license is assigned to the switch. The priority of licenses that are assigned are in the following order:

1. **Permanent**
2. **Smart**
3. **Eval**

To assign license to switches through POAP, refer to DCNM Licensing Guide.

Disabling smart licensing unassigns licenses of switches that were smart-licensed.

The evaluation license is assigned for switches that do not support smart licensing. The license state is **Eval** and the license type is **DCNM-Server**. See *Cisco DCNM Licensing Guide, Release 11.x* to view the list of switches that support smart licensing.

Smart License

From Cisco DCNM Release 11.1(1), you can use the smart licensing feature to manage licenses at device-level and renew them if required. From Cisco DCNM Web UI, choose **Administration** > **Manage Licensing** > **DCNM** > **Smart License**. You will see a brief introduction on Cisco smart licensing, a menu bar, and the **Switch Licenses** area.

Introduction to Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it’s secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation**: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management**: My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility**: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (https://software.cisco.com/software/csws/ws/platform/home).

For a more detailed overview on Cisco Licensing, go to https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html.

In the introduction, click **Click Here** to view the information on smart software licensing.

The menu bar has the following icons:

- **Registration Status**: Displays details of the current registration in a pop-up window when clicked. The value is **UNCONFIGURED** if the smart licensing is not enabled. After you enable the smart licensing without registering, the value is set to **DEREGISTERED**. The value is set to **REGISTERED** after you register. Click the registration status to view the last action, account details, and other registration details in the **Registration Details** pop-up window.

- **License Status**: Specifies the status of the license. The value is **UNCONFIGURED** if the smart licensing is not enabled. After you enable the smart licensing without registering, the value is set to **NO LICENSES IN USE**. The value is set to **AUTHORIZED** or **OUT-OF-COMPLIANCE** after registering and assigning licenses. Click the license status to view the last action, last authorization attempt, next authorization attempt, and the authorization expiry in the **License Authorization Details** pop-up window.
- **Control**: Allows you to enable or disable smart licensing, register tokens, and renew the authorization.

The following table describes the fields that appear in the **Switch Licenses** section.

Field	Description
Name	Specifies the license name.
Count	Specifies the number of licenses used.
Status	Specifies the status of the licenses used. Valid values are **Authorized** and **Out of Compliance**.
Description	Specifies the type and details of the license.
Last Updated	Specifies the timestamp when switch licenses were last updated.
Print	Allows you to print the details of switch licenses.
Export	Allows you to export the license details.

After you remove a product license from your account in Cisco Smart Software Manager, disable the smart licensing and register it again.

Enabling Smart Licensing

To enable smart licensing from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM > Smart License**.

Step 2 Click **Control** and choose **Enable** in the drop-down list to enable the smart licensing.

A confirmation window appears.

Step 3 Click **Yes**.

Instructions to register the DCNM instance appear.

The registration status changes from **UNCONFIGURED** to **DEREGISTERED**, and the license status changes from **UNCONFIGURED** to **No Licenses in Use**.

Registering a Cisco DCNM Instance

Before you begin

Create a token in Cisco Smart Software Manager.

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM > Smart License**.

Step 2 Click **Control** and choose **Register** in the drop-down list.

The **Register** window appears.

Step 3 Select the transport option to register the smart licensing agent.

The options are:

- **Default - DCNM communicates directly with Cisco's licensing servers**

  This option uses the following URL: https://tools.cisco.com/its/service/oddce/services/DDCEService

- **Transport Gateway - Proxy via Gateway or Satellite**

  Enter the URL if you select this option.

- **Proxy - Proxy via intermediate HTTP or HTTPS proxy**

  Enter the URL and the port if you select this option.

Step 4 Enter the registration token in the **Token** field.

Step 5 Click **Submit** to register the license.

The registration status changes from **DEREGISTERED** to **REGISTERED**. The name, count, and status of switch licenses appear.

Click **Registration Status: REGISTERED** to see the details of the registered token.

The switch details are updated under the **Switches/VDCs** section of the **License Assignments** tab. The license type and the license state of switches that are licensed using the smart license option are **Smart**.

What to do next

Troubleshoot communication errors, if any, that you encounter after the registration.

Troubleshooting Communication Errors

To resolve the communication errors during registration, perform the following steps:

Procedure

Step 1 Stop the DCNM service.

Step 2 Open the server properties file from the following path: /usr/local/cisco/dcm/fm/conf/server.properties

Note The server properties file for Windows will be in the following location: C:/Program Files/Cisco/dcm/fm/conf/server.properties

Step 3 Include the following property in the server properties file: `#cisco.smart.license.production=false`

`#smartlicense.url.transport=https://`*`CiscoSatellite_Server_IP`*`/Transportgateway/services/DeviceRequestHandler`

Step 4 Update the Cisco satellite details in Host Database in the /etc/hosts file in the following syntax:

`Satellite_Server_IP` `CiscoSatellite`

Step 5 Start the DCNM service.

Renew Authorization

You can manually renew the authorization only if you have registered. Automatic reauthorization happens periodically. Click **License Status** to view details about the next automatic reauthorization. To renew authorization from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration** > **Manage Licensing** > **DCNM** > **Smart License**.

Step 2 Click **Control** and choose **Renew Authorization** in the drop-down list to renew any licensing authorizations.

A request is sent to Cisco Smart Software Manager to fetch updates, if any. The **Smart Licenses** window is refreshed after the update.

Disabling Smart Licensing

To disable smart licensing from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration** > **Manage Licensing** > **DCNM** > **Smart License**.

Step 2 Select **Control** and select **Disable** to disable smart licensing.

A confirmation window appears.

Step 3 Click **Yes**.

The license status of the switches using this token, under the **License Assignments** tab, changes to **Unlicensed**. This token is removed from the list under the **Product Instances** tab in the Cisco Smart Software Manager.

If a smart license is not available and you disable smart licensing, release the license manually from the **License Assignments** tab.

Switch Smart License

If the switch is pre-configured with a smart license, DCNM validates and assigns a switch smart license. To assign licenses to switch using the Cisco DCNM UI, choose **Administration** > **Manage Licensing** >**Assign License** or, **AssignAll**.

Note From Cisco NX-OS Release 9.3(6), switch smart license is supported.

To enable switch smart license on DCNM:

- Enable smart license feature on the switch, using freeform CLI configuration.
- Configure smart licensing on the switch, using **feature license smart** or **license smart enable** command on the switch.
- Push token of your device to smart account using license smart register **idtoken** command. Use **EXEC** option in DCNM to push token. For more details, refer to Running EXEC Mode Commands in DCNM.

For unlicensed switches, licenses are assigned based on this priority:

1. DCNM Smart License
2. DCNM Server License
3. DCNM Eval License

Server License Files

From Cisco DCNM Web UI, choose **Administration** > **Manage Licensing** > **DCNM** > **Server License Files**. The following table displays the Cisco DCNM server license fields.

Field	Description
Filename	Specifies the license file name.
Feature	Specifies the licensed feature.
PID	Specifies the product ID.
SAN (Free/Total)	Displays the number of free versus total licenses for SAN.
LAN (Free/Total)	Displays the number of free versus total licenses for LAN.
Expiration Date	Displays the expiry date of the license. **Note** Text in the **Expiration Date** field is in Red for licenses that expires in seven days.

Adding Cisco DCNM Licenses

To add Cisco DCNM licenses from Cisco DCNM, perform the following steps:

Before you begin

You must have network administrator privileges to complete the following procedure.

Procedure

Step 1 Choose **Administration** > **Manage Licensing** > **DCNM** to start the license wizard.

Step 2 Choose the **Server License Files** tab.

The valid Cisco DCNM-LAN and DCNM-SAN license files are displayed.

Ensure that the security agent is disabled when you load licenses.

Step 3 Download the license pack file that you received from Cisco into a directory on the local system.

Step 4 Click **Add License File** and select the license pack file that you saved on the local machine.

The file is uploaded to the server machine, which is saved into the server license directory, and then loaded on to the server.

Note Ensure that you do not edit the contents of the .lic file or the Cisco DCNM software ignores any features that are associated with that license file. The contents of the file are signed and must remain intact. When you accidentally copy, rename, or insert the license file multiple times, the duplicate files are ignored, but the original is counted.

Switch Features—Bulk Install

From Release 11.3(1), Cisco DCNM allows you to upload multiple licenses at a single instance. DCNM parses the license files and extract the switch serial numbers. It maps the serial numbers in the license files with the discovered fabric to install the licenses on each switch. License files are moved to bootflash and installed.

To bulk install licenses to the switches on the Cisco DCNM Web Client UI, perform the following steps:

1. Choose **Administration** > **Manage Licensing** > **Switch features**.
2. In the Switch Licenses area, click **Upload License files** to upload the appropriate license file.

   The Bulk Switch License Install window appears.
3. In the Select file, click **Select License file(s)**.

   Navigate and choose the appropriate license file located in your local directory.

   Click **Open**.
4. Choose the file transfer protocol to copy the license file from the DCNM server to the switch.
   - Choose either **TFTP**, **SCP**, or **SFTP** protocol to upload the license file.

Note Not all protocols are supported for all platforms. TFTP is supported for Win/RHEL DCNM SAN installation only. However, SFTP/SCP supported for all installation types.

5. Check the **VRF** check box for the licenses to support VRF configuration.

   Enter the VRF name of one of their defined routes.

6. Check the **Overwrite file on Switch** checkbox, to overwrite the license file with the new uploaded license file.

   Note The overwrite command copies the new file over the existing one in boot flash. If the previous license was already installed, it won't override the installation.

7. In the DCNM Server credentials, enter the root username and password for the DCNM server.

   Enter the authentication credentials for access to DCNM. For DCNM Linux deployment, this is the username. For OVA\ISO deployments, use the credentials of the **sysadmin** user.

8. Click **Upload**.

   The License file is uploaded to the DCNM. The following information is extracted from the license file.

   - Switch IP – IP Address of the switch to which this license is assigned.
   - License File – filename of the license file
   - Features List –list of features supported by the license file

9. Select the set of licenses that you want to upload and install on their respective switches. A license file is applicable for a single specific switch.

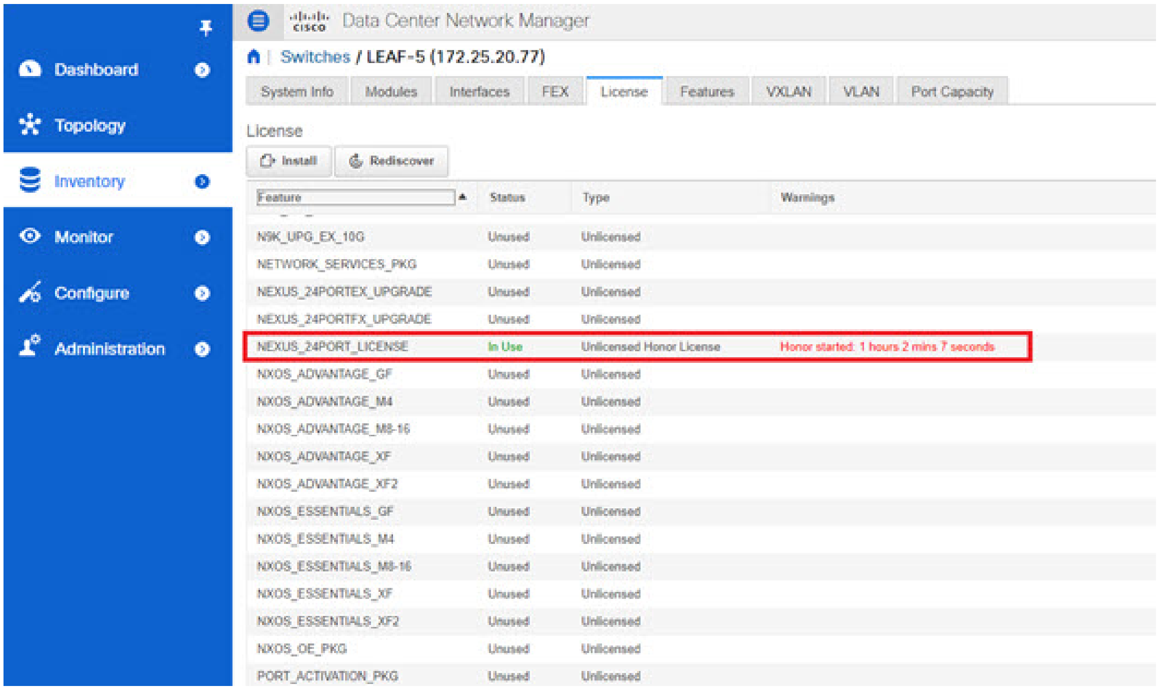
10. Click **Install Licenses**.

    The selected licenses are uploaded and installed on their respective switches. Status messages, including any issues or errors are updated for each file as it completes.

11. After the license matches with respective devices and installs, the **License Status** table displays the status.

Switch-based honor license support

On the DCNM **Web UI > Inventory > Switch > License**, the **Type** column displays “Unlicensed Honor License” and **Warnings** column displays **Honor started: …** with elapsed time since the license was changed to the Honor mode.

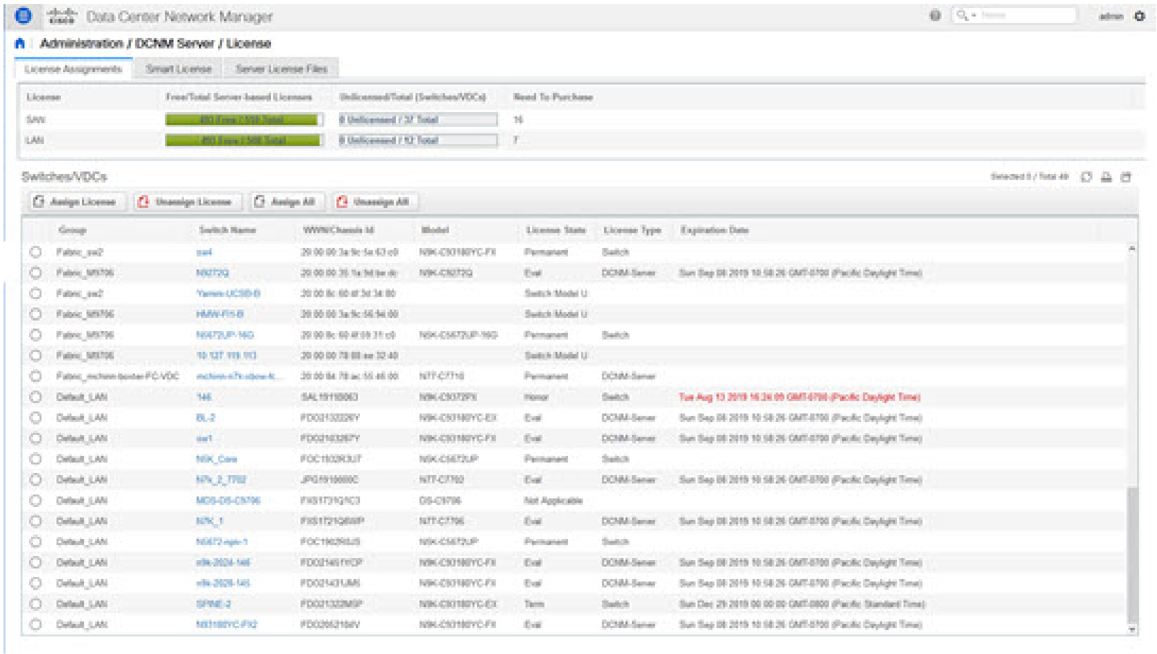


Switches / LEAF-5 (172.25.20.77)

License

Feature	Status	Type	Warnings
N9K_UPG_EX_10G	Unused	Unlicensed	
NETWORK_SERVICES_PKG	Unused	Unlicensed	
NEXUS_24PORTEX_UPGRADE	Unused	Unlicensed	
NEXUS_24PORTFX_UPGRADE	Unused	Unlicensed	
NEXUS_24PORT_LICENSE	In Use	Unlicensed Honor License	Honor started: 1 hours 2 mins 7 seconds
NXOS_ADVANTAGE_GF	Unused	Unlicensed	
NXOS_ADVANTAGE_M4	Unused	Unlicensed	
NXOS_ADVANTAGE_M8-16	Unused	Unlicensed	
NXOS_ADVANTAGE_XF	Unused	Unlicensed	
NXOS_ADVANTAGE_XF2	Unused	Unlicensed	
NXOS_ESSENTIALS_GF	Unused	Unlicensed	
NXOS_ESSENTIALS_M4	Unused	Unlicensed	
NXOS_ESSENTIALS_M8-16	Unused	Unlicensed	
NXOS_ESSENTIALS_XF	Unused	Unlicensed	
NXOS_ESSENTIALS_XF2	Unused	Unlicensed	
NXOS_OE_PKG	Unused	Unlicensed	
PORT_ACTIVATION_PKG	Unused	Unlicensed	

Note Switch-based honor licenses can’t be overwritten with server-based license files.

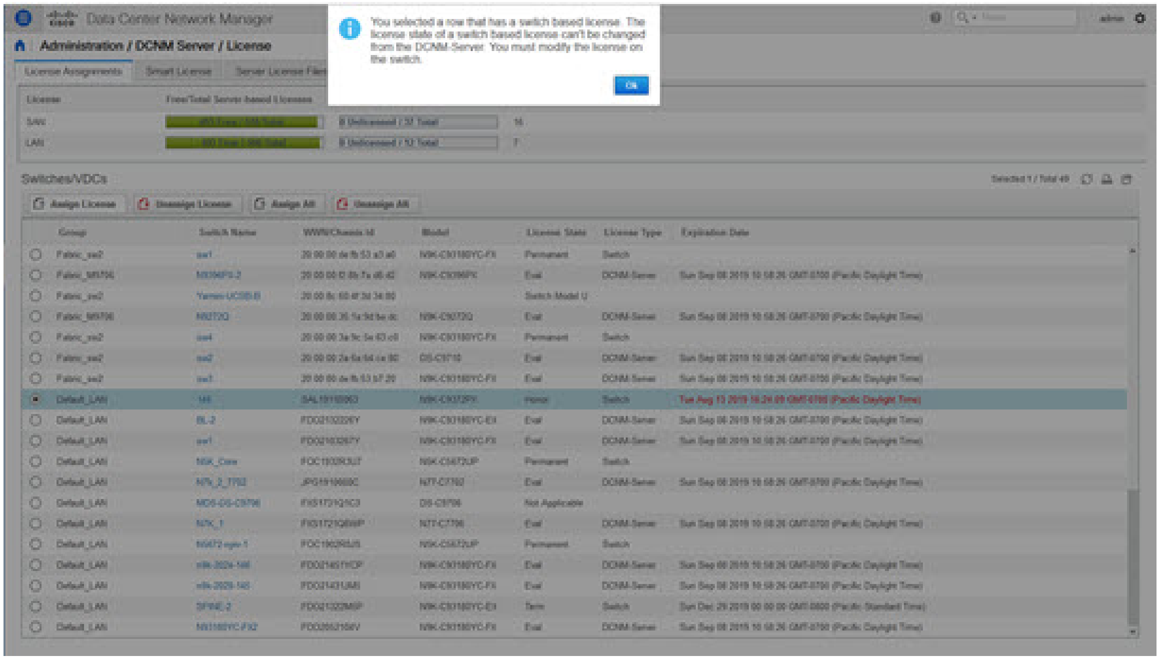


Administration / DCNM Server / License

License	Free/Total Server-based Licenses	Unlicensed/Total (Switches/VDCs)	Need To Purchase
SAN	493 Free / 500 Total	0 Unlicensed / 37 Total	16
LAN	493 Free / 500 Total	0 Unlicensed / 10 Total	7

Switches/VDCs

	Group	Switch Name	WWN/Chassis Id	Model	License State	License Type	Expiration Date
○	Fabric_sw2	sw4	20:00:00:3a:9c:5a:63:c0	N9K-C93180YC-FX	Permanent	Switch	
○	Fabric_M9706	N9272Q	20:00:00:35:1a:9d:be:dc	N9K-C9272Q	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Fabric_sw2	Yamen-UCSB-B	20:00:8c:60:4f:3d:34:80		Switch Model U		
○	Fabric_M9706	HMW-FI-B	20:00:00:3a:9c:56:94:00		Switch Model U		
○	Fabric_M9706	N5672UP-16G	20:00:8c:60:4f:59:31:c0	N5K-C5672UP-16G	Permanent	Switch	
○	Fabric_M9706	10.127.119.113	20:00:00:78:88:ee:32:40		Switch Model U		
○	Fabric_mchem-border-FC-VDC	mchem-n7k-xbow-b...	20:00:84:78:ac:55:46:00	N7T-C7718	Permanent	DCNM-Server	
○	Default_LAN	146	SAL19110063	N9K-C9372PX	Honor	Switch	Tue Aug 13 2019 16:24:05 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	BL-2	FDO2132226Y	N9K-C93180YC-EX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	sw1	FDO2103267Y	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	N5K_Core	FOC1502R3U7	N5K-C5672UP	Permanent	Switch	
○	Default_LAN	N7k_2_7702	JPG1916000C	N77-C7702	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	MDS-DS-C9706	FXS1731Q1C3	DS-C9706	Not Applicable		
○	Default_LAN	N7K_1	FXS1721Q6WP	N77-C7706	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	N5672-vpc-1	FOC1902R0J5	N5K-C5672UP	Permanent	Switch	
○	Default_LAN	n9k-2024-146	FDO21461YCP	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	n9k-2028-145	FDO21431UM6	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	SPINE-2	FDO21322MSP	N9K-C93180YC-EX	Term	Switch	Sun Dec 29 2019 00:00:00 GMT-0800 (Pacific Standard Time)
○	Default_LAN	N93180YC-FX2	FDO2002158V	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)



Administration / DCNM Server / License

You selected a row that has a switch based license. The license state of a switch based license can't be changed from the DCNM-Server. You must modify the license on the switch.

License	Free/Total Server-based Licenses		
SAN	493 Free / 500 Total	8 Unlicensed / 37 Total	16
LAN	500 Free / 500 Total	8 Unlicensed / 12 Total	7

Switches/VDCs

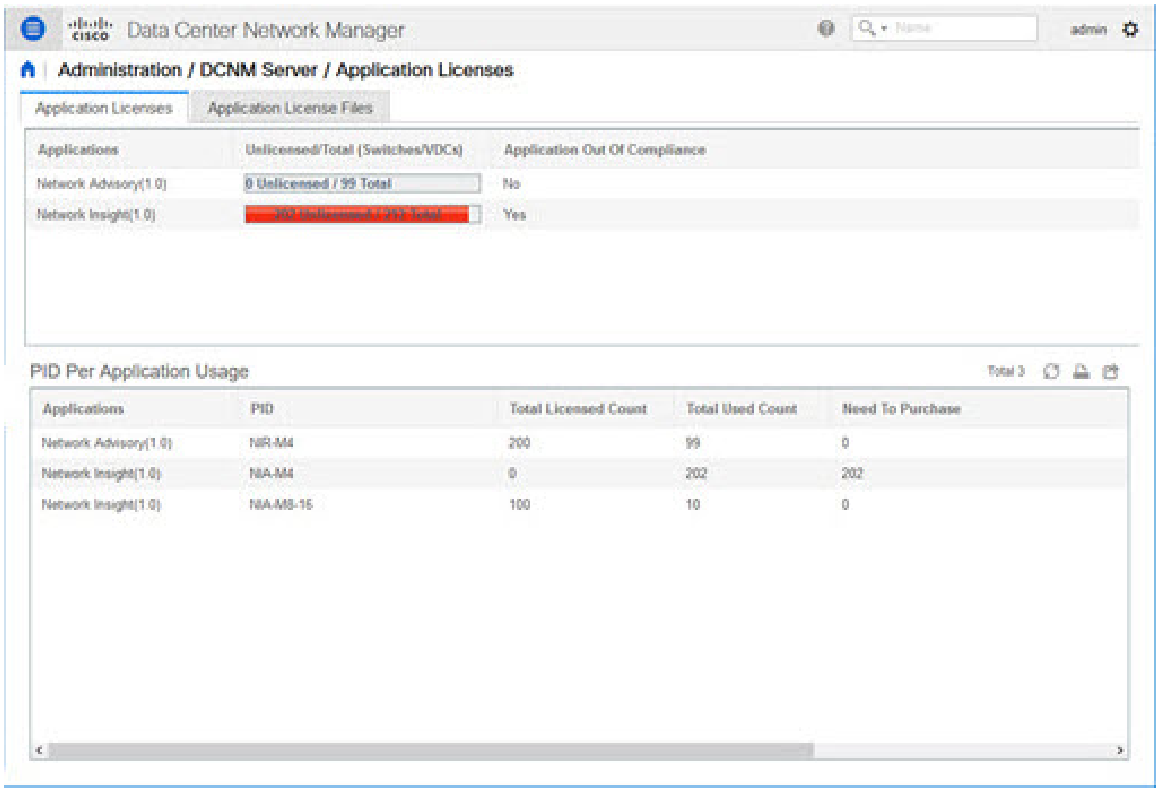
Selected 1 / Total 49

	Group	Switch Name	WWN/Chassis Id	Model	License State	License Type	Expiration Date
○	Fabric_sw2	sw1	20:00:00:de:fb:53:a3:a0	N9K-C93180YC-FX	Permanent	Switch	
○	Fabric_M9706	N9396PX-2	20:00:00:f2:8b:7a:d6:42	N9K-C9396PX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Fabric_sw2	Yamen-UCSB-B	20:00:8c:60:4f:3d:34:80		Switch Model U		
○	Fabric_M9706	N9272Q	20:00:00:35:1a:9d:be:dc	N9K-C9272Q	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Fabric_sw2	sw4	20:00:00:3a:9c:5a:63:c0	N9K-C93180YC-FX	Permanent	Switch	
○	Fabric_sw2	sw2	20:00:00:2a:6a:6d:ca:80	DS-C9710	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Fabric_sw2	sw3	20:00:00:de:fb:53:b7:20	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
●	Default_LAN	141	SAL19150903	N9K-C9372PX	Honor	Switch	Tue Aug 13 2019 16:24:09 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	BL-2	FDO2132226Y	N9K-C93180YC-EX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	sw1	FDO2103267Y	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	N5K_Core	FOC1932R3U7	N5K-C5672UP	Permanent	Switch	
○	Default_LAN	N7k_2_7702	JPG1910600C	N77-C7702	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	MDS-DS-C9706	FXS1721Q1C3	DS-C9706	Not Applicable		
○	Default_LAN	N7K_1	FXS1721Q6WP	N77-C7706	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	N5672-vpc-1	FOC1902R0U5	N5K-C5672UP	Permanent	Switch	
○	Default_LAN	n9k-2024-166	FDO21451YCP	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	n9k-2029-165	FDO2143UMI	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	SPINE-2	FDO21322M9P	N9K-C93180YC-EX	Term	Switch	Sun Dec 29 2019 00:00:00 GMT-0800 (Pacific Standard Time)
○	Default_LAN	N9180YC-FX2	FDO20521S6V	N9K-C93180YC-FX	Eval	DCNM-Server	Sun Sep 08 2019 10:58:26 GMT-0700 (Pacific Daylight Time)

Application Licenses

From Release 11.3(1), you can manage licenses for applications on the Cisco DCNM. Choose **Web UI** > **Administration** > **Manage Licensing** > **Applications** to view the Application Licenses.

The Application Licenses tab displays the DCNM Applications with a summary of their unlicensed/total switches and if they are out of compliance. The PID Per Application Usage table displays the actual counts per PID given to the server from the Application Framework. The PIDs that need to be purchased for each application is also listed.



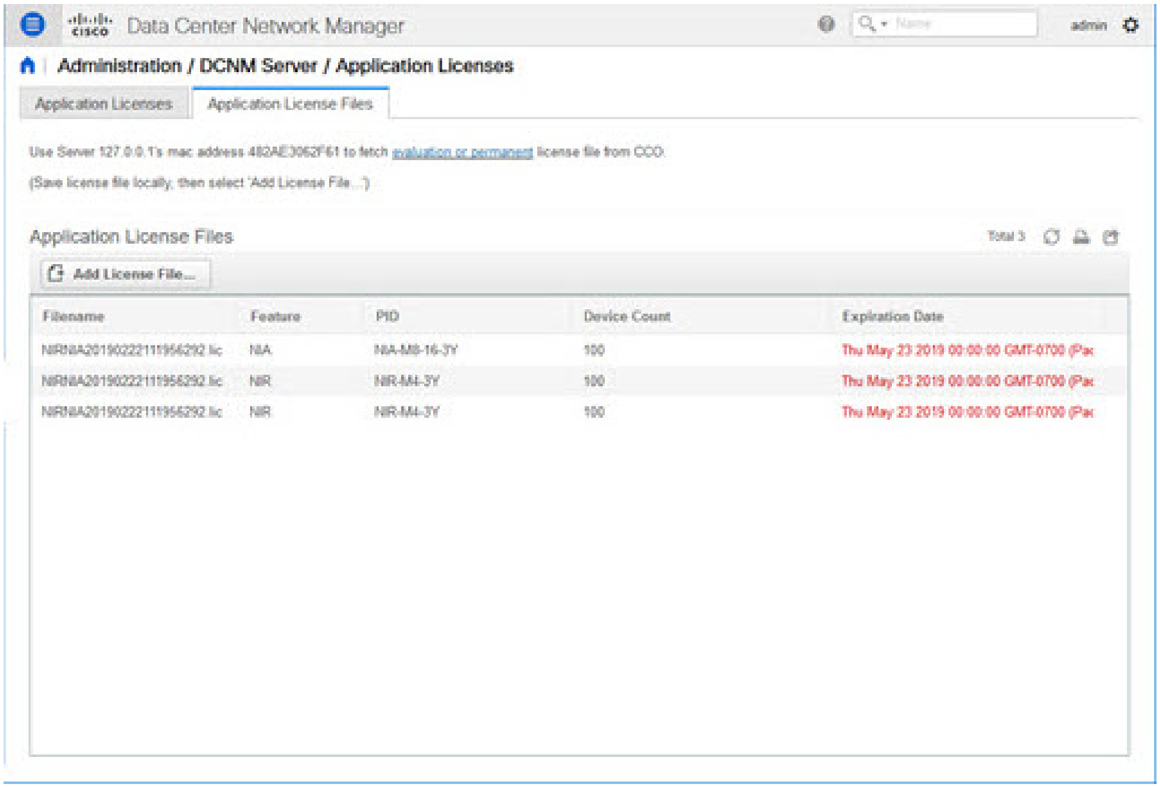
Administration / DCNM Server / Application Licenses

Applications	Unlicensed/Total (Switches/VDCs)	Application Out Of Compliance
Network Advisory(1.0)	0 Unlicensed / 99 Total	No
Network Insight(1.0)	202 Unlicensed / 212 Total	Yes

PID Per Application Usage

Applications	PID	Total Licensed Count	Total Used Count	Need To Purchase
Network Advisory(1.0)	NIR-M4	200	99	0
Network Insight(1.0)	NIA-M4	0	202	202
Network Insight(1.0)	NIA-M8-15	100	10	0

The Application License Files tab allows you to add license files for the applications. Click on Add license file to add license file from your local directory. The license filename, application name, PID, device count and expiration date details are extracted from the imported license file. If the license isn’t permanent or is eval or term, the expiration date is also listed.



Administration / DCNM Server / Application Licenses

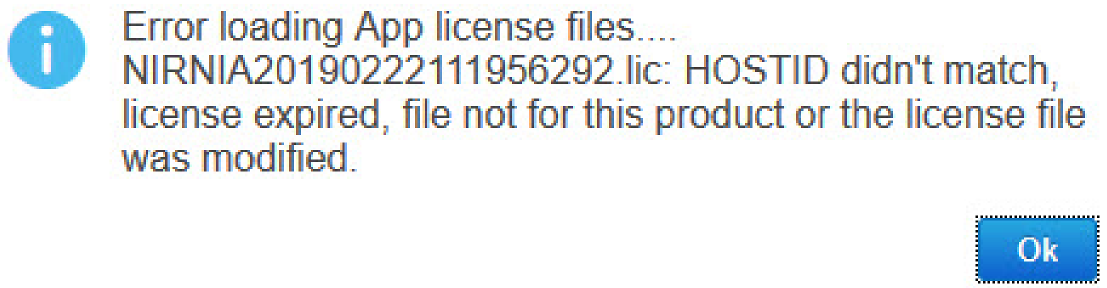
Use Server 127.0.0.1's mac address 482AE3062F61 to fetch evaluation or permanent license file from CCO.

(Save license file locally, then select 'Add License File...')

Application License Files

Filename	Feature	PID	Device Count	Expiration Date
NIRNIA20190222111956292.lic	NIA	NIA-M8-16-3Y	100	Thu May 23 2019 00:00:00 GMT-0700 (Pac
NIRNIA20190222111956292.lic	NIR	NIR-M4-3Y	100	Thu May 23 2019 00:00:00 GMT-0700 (Pac
NIRNIA20190222111956292.lic	NIR	NIR-M4-3Y	100	Thu May 23 2019 00:00:00 GMT-0700 (Pac

The following image shows a sample error message while uploading an application license file.


Error loading App license files.... NIRNIA20190222111956292.lic: HOSTID didn't match, license expired, file not for this product or the license file was modified.

Management Users

Note Every time you login to DCNM, the DCNM server fetches information from the ISE server for AAA authentication. The ISE server will not authenticate again, after the first login.

The Management Users menu includes the following submenus:

Remote AAA

To configure remote AAA from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Management Users > Remote AAA Properties**.

The AAA properties configuration window appears.

Step 2 Use the radio button to select one of the following authentication modes:

- Local: In this mode the authentication authenticates with the local server.
- Radius: In this mode the authentication authenticates against the RADIUS servers specified.
- TACACS+: In this mode the authentication authenticates against the TACACS servers specified.
- Switch: In this mode the authentication authenticates against the switches specified.
- LDAP: In this mode the authentication authenticates against the LDAP server specified.

Step 3 Click **Apply**.

Local

Procedure

Step 1 Use the radio button and select **Local** as the authentication mode.

Step 2 Click **Apply** to confirm the authentication mode.

Radius

Procedure

Step 1 Use the radio button and select **Radius** as the authentication mode.

Note When using the DCNM AAA or Radius authentication, you should not specify the hash (#) symbol at the beginning of a secret key. Otherwise, DCNM will try to use # as encrypted, and it will fail.

Step 2 Specify the Primary server details and click **Test** to test the server.

Step 3 (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.

Step 4 Click **Apply** to confirm the authentication mode.

TACACS+

Procedure

Step 1 Use the radio button and select **TACACS+** as the authentication mode.

Note When using the DCNM AAA or Radius authentication, you should not specify the hash (#) symbol at the beginning of a secret key. Otherwise, DCNM will try to use **#** as encrypted, and it will fail.

Step 2 Specify the Primary server details and click **Test** to test the server.

Step 3 (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.

Note For IPv6 transport, enter Physical and VIP address for AAA authentication as the order of addresses changes during failover situation.

Step 4 Click **Apply** to confirm the authentication mode.

Switch

Procedure

Step 1 Use the radio button to select **Switch** as the authentication mode.

DCNM also supports LAN switches with the IPv6 management interface.

Step 2 Specify the Primary Switch name and click **Apply** to confirm the authentication mode.

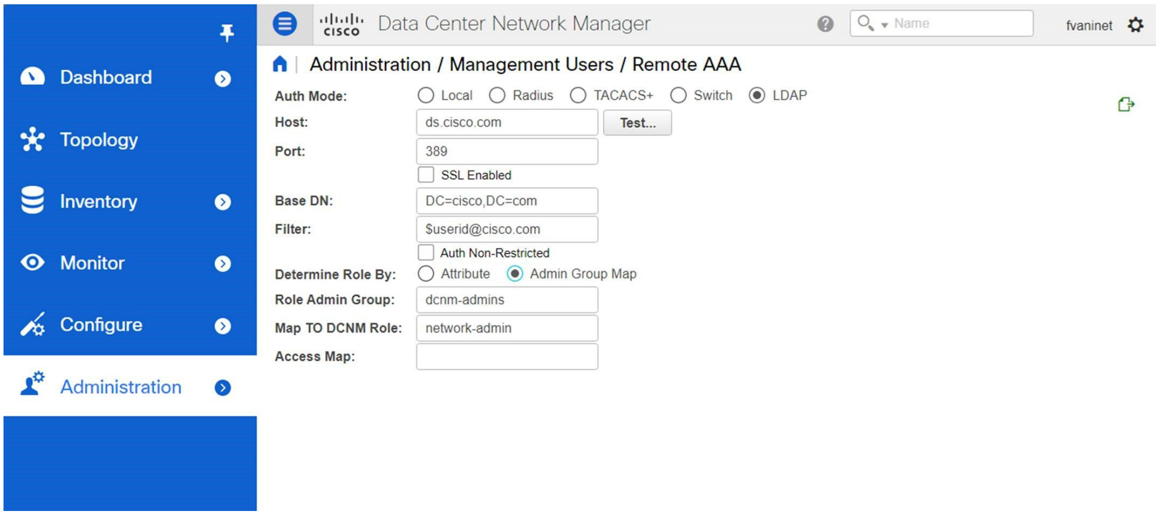
Step 3 (Optional) Specify the names for Secondary and Tertiary Switches.

Step 4 Click **Apply** to confirm the authentication mode.

LDAP

Procedure

Step 1 Use the radio button and select **LDAP** as the authentication mode.



Administration / Management Users / Remote AAA

Auth Mode: ○ Local ○ Radius ○ TACACS+ ○ Switch ● LDAP

Host: ds.cisco.com

Port: 389

□ SSL Enabled

Base DN: DC=cisco,DC=com

Filter: $userid@cisco.com

□ Auth Non-Restricted

Determine Role By: ○ Attribute ● Admin Group Map

Role Admin Group: dcnm-admins

Map TO DCNM Role: network-admin

Access Map:

Step 2 In the **Host** field, enter either the IPv4 or IPv6 address.

If DNS service is enabled, you can enter DNS address (hostname) of the LDAP server.

Step 3 In the **Port** field, enter a port number.

Enter 389 for non-SSL; enter 636 for SSL. By default, the port is configured for non-SSL.

Step 4 Select the **SSL Enabled** check box, if SSL is enabled on the AAA server.

Note You must enter **636** in the Port field, and select **SSL Enabled** check box to use LDAP over SSL.

This ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a SSL session, before sending the bind or search request.

Note Cisco DCNM establishes a secured connection with the LDAP server using TLS. Cisco DCNM supports all versions of TLS. However, the specific version of TLS is determined by the LDAP server.

For example, if the LDAP server supports TLSv1.2 by default, DCNM will connect using TLSv1.2.

Step 5 In the **Base DN** field, enter the base domain name.

The LDAP server searches this domain. You can find the base DN by using the **dsquery.exe user -name**<*display_name*> command on the LDAP server.

For example:

```
ldapserver# dsquery.exe users -name "John Smith"

CN=john smith,CN=Users,DC=cisco,DC=com
```

The Base DN is DC=cisco,DC=com.

Note Ensure that you enter the elements within the Base DN in the correct order. This specifies the navigation of the application when querying Active Directory.

Step 6 In the **Filter** field, specify the filter parameters.

These values are used to send a search query to the Active Directory. The LDAP search filter string is limited to a maximum of 128 characters.

For example:

- $userid@cisco.com

  This matches the user principal name.

- CN=$userid,OU=Employees,OU=Cisco Users

  This matches the exact user DN.

Step 7 Choose an option to determine a role. Select either **Attribute** or **Admin Group Map**.

- **Admin Group Map**: In this mode, DCNM queries LDAP server for a user based on the Base DN and filter. If the user is a part of any user group, the DCNM role will be mapped to that user group.
- **Attribute**: In this mode, DCNM queries for a user attribute. You can select any attribute. When you choose **Attribute**, the **Role Admin Group** field changes to **Role Attributes**.

Step 8 Enter value for either **Roles Attributes** or **Role Admin Group** field, based on the selection in the previous step.

- If you chose **Admin Group Map**, enter the name of the admin group in the **Role Admin Group** field.
- If you chose **Attribute**, enter the appropriate attribute in the **Attributes** field.

Step 9 In the **Map to DCNM Role** field, enter the name of the DCNM role that will be mapped to the user.

Generally, **network-admin** or **network-operator** are the most typical roles.

For example:

```
Role Admin Group: dcnm-admins
Map to DCNM Role: network-admin
```

This example maps the Active Directory User Group **dcnm-admins** to the **network-admin** role.

To map multiple Active Directory User Groups to multiple roles, use the following format:

```
Role Admin Group:
Map To DCNM Role: dcnm-admins:network-admin;dcnm-operators:network-operator
```

Note that **Role Admin Group** is blank, and **Map To DCNM Role** contains two entries delimited by a semicolon.

Step 10 In the **Access Map** field, enter the Role Based Access Control (RBAC) device group to be mapped to the user.

Step 11 Click **Test** to verify the configuration. The Test AAA Server window appears.

Step 12 Enter a valid **Username** and **Password** in the Test AAA Server window.

If the configuration is correct, the following message is displayed.

```
Authentication succeeded.
The cisco-av-pair should return 'role=network-admin' if this user needs to
see the DCNM Admin pages. 'SME' roles will allow SME page access. All other
roles - even if defined on the switches - will be treated
as network operator.
```

This message is displayed regardless of 'Role Admin Group' or 'Attribute' mode. It implies that Cisco DCNM can query your Active Directory, the groups, and the roles are configured correctly.

If the test fails, the LDAP Authentication Failed message is displayed.

Warning Don’t save the configuration unless the test is successful. You cannot access DCNM if you save incorrect configurations.

Step 13 Click **Apply Changes** icon (located in the right top corner of the screen) to save the configuration.

Step 14 Restart the DCNM SAN service.

- For Windows – On your system navigate to **Computer Management** > **Services and Applications** > **Services**. Locate and right click on the DCNM application. Select **Stop**. After a minute, right click on the DCNM application and select **Start** to restart the DCNM SAN service.
- For Linux – Go to **/etc/init.d/FMServer.restart** and hit return key to restart DCNM SAN service.

Managing Local Users

As an admin user, you can use Cisco DCNM Web UI to create a new user, assign the role and associate one or more groups or scope for the user.

This section contains the following:

Adding Local Users

Procedure

Step 1 From the menu bar, choose **Administration** > **Management Users** > **Local**. You see the **Local Users** page.

Step 2 Click **Add User**.

You see the **Add User** dialog box.

Step 3 Enter the username in the **User name** field.

Note The username is case sensitive, but the username guest is a reserved name, which is not case sensitive. The guest user can only view reports. The guest user cannot change the guest password, or access the Admin options in DCNM Web Client.

Step 4 From the **Role** drop-down list, select a role for the user.

Step 5 In the **Password** field, enter the password.

Note All special characters, except SPACE is allowed in the password.

Step 6 In the **Confirm Password** field, enter the password again.

Step 7 Click **Add** to add the user to the database.

Step 8 Repeat Steps 2 through 7 to continue adding users.

Deleting Local Users

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

Procedure

Step 1 Choose **Administration** > **Management Users** > **Local**.

The **Local Users** page is displayed.

Step 2 Select one or more users from the **Local Users** table and click the **Delete User** button.

Step 3 Click **Yes** on the warning window to delete the local user. Click **No** to cancel deletion.

Editing a User

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

Procedure

Step 1 Choose **Administration** > **Management Users** > **Local**.

Step 2 Use the checkbox to select a user and click the **Edit User** icon.

Step 3 In the **Edit User** window, the **Username** and **Role** are mentioned by default. Specify the **Password** and **Confirm Password**.

Step 4 Click **Apply** to save the changes.

User Access

You can select specific groups or fabrics that local users can access. This restricts local users from accessing specific groups or fabrics for which they have not been provided access. To do this, perform the following steps:

Procedure

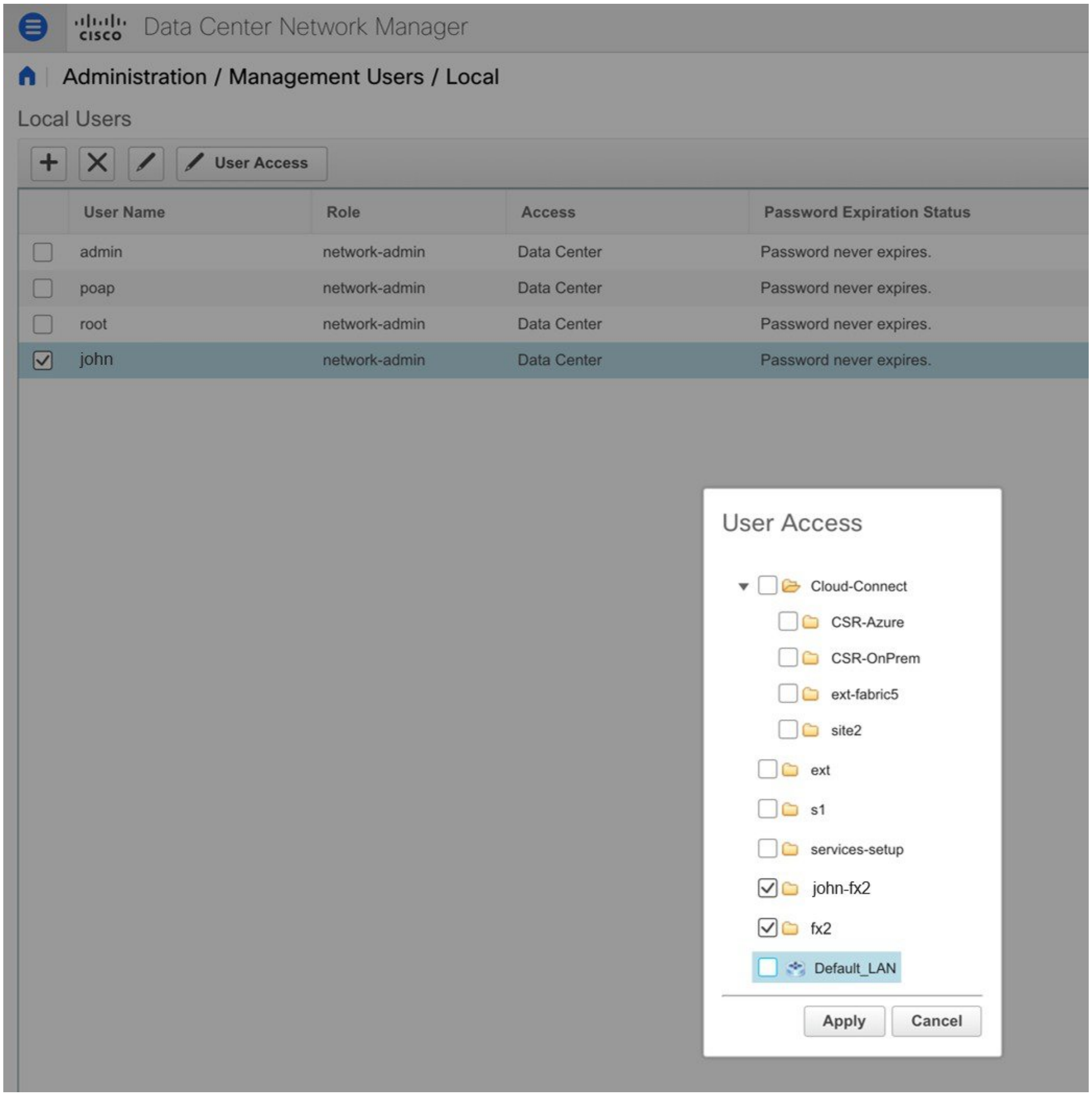
Step 1 Choose **Administration** > **Management Users** > **Local**.

The **Local Users** window is displayed.

Step 2 Select one user from the **Local Users** table. Click **User Access**.

The **User Access** selection window is displayed.

Step 3 Select the specific groups or fabrics that the user can access and click **Apply**.


Data Center Network Manager
Administration / Management Users / Local
Local Users
+
X
User Access

☐	User Name	Role	Access	Password Expiration Status
☐	admin	network-admin	Data Center	Password never expires.
☐	poap	network-admin	Data Center	Password never expires.
☐	root	network-admin	Data Center	Password never expires.
☑	john	network-admin	Data Center	Password never expires.

User Access

- ☐ Cloud-Connect
  - ☐ CSR-Azure
  - ☐ CSR-OnPrem
  - ☐ ext-fabric5
  - ☐ site2
- ☐ ext
- ☐ s1
- ☐ services-setup
- ☑ john-fx2
- ☑ fx2
- ☐ Default_LAN

Managing Clients

You can use Cisco DCNM to disconnect DCNM Client Servers.

Procedure

Step 1 Choose **Administration** > **Management Users** > **Clients**.

A list of DCNM Servers are displayed.

Step 2 Use the check box to select a DCNM server and click **Disconnect Client** to disconnect the DCNM server.

Note You cannot disconnect a current client session.

Performance Setup

The Performance Setup menu includes the following submenus:

Performance Setup LAN Collections

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM to add and remove performance collections. License the switch and kept it in the **Managed Continuously** state before creating a collection for the switch.

Note To collect Performance Manager data, ICMP ping must be enabled between the switch and DCNM server. Set **pm.skip.checkPingAndManageable** server property to true and then restart the DCNM. Choose Web **UI** > **Administration** > **DCNM Server** > **Server Properties** to set the server property.

To add a collection, follow these steps:

Procedure

Step 1 Choose **Administration > Performance Setup > LAN Collections**.

Step 2 For all the licensed LAN switches, use the check boxes to enable performance data collection for **Trunks**, **Access**, **Errors & Discards**, and **Temperature Sensor**.

Step 3 Use the check boxes to select the types of LAN switches for which you want to collect performance data.

Step 4 Click **Apply** to save the configuration.

Step 5 In the confirmation dialog box, click **Yes** to restart the Performance Manager. The Performance Manager has to be restarted for any new setting to take effect.

Performance Manager SAN Collections

If you are managing your switches with the performance manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM to add and remove performance collections. License the switch and keep it in the **managedContinuously** state before creating a collection for the switch. Only licensed fabrics appear in this window.

To add a collection, follow these steps:

Procedure

Step 1 Choose **Administration** > **Performance Setup** > **SAN Collections**.

Step 2 Select a fabric and select the **Name**, **ISL/NPV Links**, **Hosts**, **Storage**, **FC Flows**, and **FC Ethernet** to enable performance collection for these data types.

Step 3 Click **Apply** to save the configuration.

Step 4 In the confirmation dialog box, click **Yes** to restart the performance collector.

Performance Setup Thresholds

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM to add and remove performance collections. License the switch and keep it in the **Managed Continuously** state before creating a collection for the switch.

Procedure

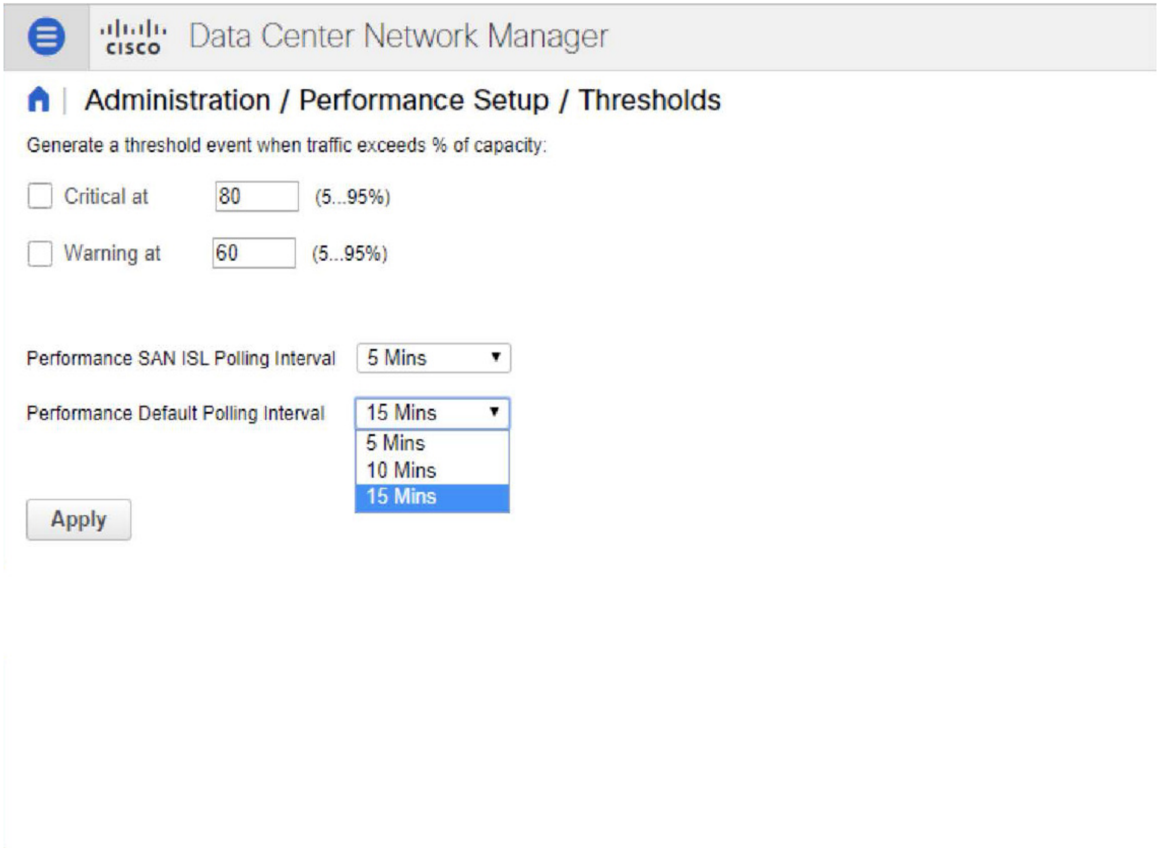
Step 1 Choose **Administration** > **Performance Setup** > **Thresholds**.

Step 2 Under **Generate a threshold event when traffic exceeds % of capacity**, use the check box to specify the **Critical at** and **Warning at** values. The range for **Critical at** is from 5 to 95, and the default is 80. The range for **Warning at** is from 5 to 95, and the default is 60.

Step 3 Select a value for **Performance SAN ISL Polling Interval** from the drop-down list. Valid values are **5 Mins**, **4 Mins**, **3 Mins**, **2 Mins**, **1 Min**, and **30 Sec**. The default is **30 Sec**.

Step 4 Select a value for **Performance Default Polling Interval** from the drop-down list. Valid values are **5 Mins** , **10 Mins**, and **15 mins**. The default value is **5 Mins**.

Step 5 Click **Apply**.



Data Center Network Manager

Administration / Performance Setup / Thresholds

Generate a threshold event when traffic exceeds % of capacity:

□ Critical at 80 (5...95%)

□ Warning at 60 (5...95%)

Performance SAN ISL Polling Interval: 5 Mins

Performance Default Polling Interval: 15 Mins

Configuring User-Defined Statistics

To configure user-defined statistics from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration** > **Performance Setup** > **User Defined**.

The User-Defined statistics window is displayed.

Step 2 Click **Add** icon.

The **Add SNMP Statistic to Performance Collection** window is displayed.

Step 3 From the **Switch** table, select the switch for which you want to add other statistics.

Step 4 From the **SNMP OID** drop-down list, select the OID.

Note For SNMP OID ModuleX_Temp,IFHCInOctets.IFINDEX,IFHCOutOctest.IFINDEX, selected from drop-down list, you must replace 'X' with correct module number or the corresponding IFINDEX.

Step 5 In the **Display Name** box, enter a new name.

Step 6 From the **SNMP Type** drop-down list, select the type.

Step 7 Click **Add** to add this statistic.

Event Setup

The Event Setup menu includes the following submenus:

Viewing Events Registration

To enable **Send Syslog**, **Send Traps** and **Delayed Traps** you must configure the following in the DCNM SAN client:

- Enabling **Send Syslog**: Choose **Physical Attributes > Events > Syslog > Servers**. Click **Create Row**, provide the required details, and click **Create**.
- Enabling **Send Traps**: Choose **Physical Attributes > Events > SNMP Traps > Destination**. Click **Create Row**, provide the required details, and click **Create**.
- Enabling **Delayed Traps**: Choose **Physical Attributes > Events > SNMP Traps > Delayed Traps**. In the **Feature Enable** column, use the check boxes to enable delayed traps for the switch and specify the delay in minutes.

Procedure

Step 1 Choose **Administration > Event Setup > Registration**.

The SNMP and Syslog receivers along with the statistics information are displayed.

Step 2 Check the **Enable Syslog Receiver** check box and click **Apply**, to enable the syslog receiver if it is disabled in the server property.

To configure event registration or syslog properties, choose **Administration > DCNM Server > Server Properties** and follow the on-screen instructions.

Step 3 Select **Copy Syslog Messages to DB** and click **Apply** to copy the syslog messages to the database.

If this option is not selected, the events will not be displayed in the events page of the Web client.

The columns in the second table display the following:

- Switches sending traps
- Switches sending syslog
- Switches sending syslog accounting
- Switches sending delayed traps

Notification Forwarding

You can use Cisco DCNM Web UI to add and remove notification forwarding for system messages.

This section contains the following:

Adding Notification Forwarding

Cisco DCNM Web UI forwards fabric events through email or SNMPv1 traps.

Some SMTP servers may require addition of authentication parameters to emails that are sent from DCNM to the SMTP servers. Starting from Cisco DCNM Release 11.4(1), you can add authentication parameters to the emails that are sent by DCNM to any SMTP server that requires authentication. This feature can be configured by setting up the **SMTP>Authentication** properties in the **Administration>DCNM Server>Server Properties** window. Enter **true** in the **server.smtp.authenticate** field, enter the required username in the **server.smtp.username** field, and enter the required password in the **server.smtp.password** field.

To add and remove notification forwarding for system messages from the Cisco DCNM Web UI, perform the following steps:

Note Test forwarding works only for the licensed fabrics.

Procedure

Step 1 Choose **Administration > Event Setup > Forwarding**.

The events forwarding scope, the recipient email address, severity of the event and type of the event is displayed. The description Regex field is applicable only when the forwarding source is selected as Syslog while adding the events forwarder.

Step 2 Check the **Enable** checkbox to enable events forwarding.

Step 3 Specify the **SMTP Server** details and the **From** email address.

Step 4 Click **Apply** to save the configuration.

Step 5 In the **Event Count Filter**, add a filter for the event count to the event forwarder.

The forwarding stops forwarding an event if the event count exceeds the limit as specified in the event count filter. In this field, you can specify a count limit. Before an event can be forwarded, the Cisco DCNM checks if its occurrence exceeds the count limit. If it does, the event will not be forwarded.

Step 6 Select the **Snooze** checkbox and specify the **Start** date and time and the **End** date and time. Click **Apply** to save the configuration.

Step 7 Under the **Event Forwarder Rules** table, click the **+** icon to add an event forwarder rule.

You see the **Add Event Forwarder Rule** dialog box.

Step 8 In the **Forwarding Method**, choose either **E-mail** or **Trap**. If you choose **Trap**, a **Port** field is added to the dialog box.

Step 9 If you choose the **E-mail** forwarding method, enter the IP address in the **Email Address** field. If you choose the **Trap** method, enter the trap receiver IP address in the **Address** field and specify the port number.

You can either enter an IPv4 or IPv6 addresses or DNS server name in the **Address** field.

Step 10 For **Forwarding Scope**, choose the **Fabric/LAN** or **Port Groups** for notification.

Step 11 In the **Source** field, select **DCNM** or **Syslog**.

If you select **DCNM**, then:

a) From the **Type** drop-down list, choose an event type.
b) Check the **Storage Ports Only** check box to select only the storage ports.
c) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
d) Click **Add** to add the notification.

If you select **Syslog**, then:

a) In the **Facility** list, select the syslog facility.
b) Specify the syslog **Type**.
c) In the **Description Regex** field, specify a description that matches with the event description.
d) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
e) Click **Add** to add the notification.

Note The **Minimum Severity** option is available only if the **Event Type** is set to All.

The traps that are transmitted by Cisco DCNM correspond to the severity type. A text description is also provided with the severity type.

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

Removing Notification Forwarding

You can remove notification forwarding.

Procedure

Step 1 Choose **Administration** > **Event Setup** > **Forwarding**.

Step 2 Select the check box in front of the notification that you want to remove and click **Delete**.

Configuring EMC CallHome

To configure EMC Call Home for EMC supported SAN switches from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Event Setup > EMC Call Home**.

Step 2 Select the **Enable** check box to enable this feature.

Step 3 Use the check box to select the fabrics or individual switches.

Step 4 Enter the general email information.

Step 5 Click the **Apply** to update the email options.

Step 6 Click **Apply and Test** to update the email options and test the results.

Event Suppression

Cisco DCNM allows you to suppress the specified events that are based on the user-specified suppressor rules. Such events will not be displayed on the Cisco DCNM Web UI and SAN Client. The events will neither be persisted to DCNM database, nor forwarded via email or SNMP trap.

You can view, add, modify, and delete suppressor rules from the table. You can create a suppressor rule from the existing event table. Select a given event as the template, and invoke the rule dialog window. Event details are automatically ported from the selected event in the event table to the input fields of the rule creation dialog window.

Note You cannot suppress EMC Call Home events from the Cisco DCNM Web UI.

This section includes the following:

Add Event Suppression Rules

To add rules to the Event Suppression from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Event Setup > Suppression**.

The **Suppression** window is displayed.

Step 2 Click the **Add** icon above the **Event Suppressors** table.

The **Add Event Suppressor Rule** window is displayed.

Step 3 In the **Add Event Suppressor Rule** window, specify the **Name** for the rule.

Step 4 Select the required **Scope** for the rule that is based on the event source.

In the Scope drop-down list, the LAN groups and the port groups are listed separately. You can choose **SANLAN, Port Groups** or **Any**. For **SAN** and **LAN**, select the scope of the event at the Fabric or Group or Switch level. You can only select groups for **Port Group** scope. If use selects **Any** as the scope, the suppressor rule is applied globally.

Step 5 Enter the **Facility** name or choose from the **SAN/LAN Switch Event Facility** List.

If you do not specify a facility, wildcard is applied.

Step 6 From the drop-down list, select the Event **Type**.

If you do not specify the event type, wildcard is applied.

Step 7 In the **Description Matching** field, specify a matching string or regular expression.

The rule matching engine uses regular expression that is supported by Java Pattern class to find a match against an event description text.

Step 8 Check the **Active Between** box and select a valid time range during which the event is suppressed.

By default, the time range is not enabled, i.e., the rule is always active.

Note In general, you must not suppress accounting events. Suppressor rule for Accounting events can be created only for certain rare situations where Accounting events are generated by actions of DCNM or switch software. For example, lots of '*sync-snmp-password*' AAA syslog events are automatically generated during the password synchronization between DCNM and managed switches. To suppress Accounting events, navigate to the **Suppressor table** and invoke the **Add Event Suppressor Rule** dialog window.

Note Choose **Monitor > Switch > Events** to create a suppressor rule for a known event. There is no such shortcut to create suppressor rules for Accounting events.

Delete Event Suppression Rule

To delete event suppressor rules from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Event Setup > Suppression** .

Step 2 Select the rule from the list and click **Delete** icon.

Step 3 Click **Yes** to confirm.

Modify Event Suppression Rule

To modify the event suppressor rules, do the following tasks:

Procedure

Step 1 Choose **Administration > Event Setup > Suppression**.

Step 2 Select the rule from the list and click **Edit**.

You can edit **Facility**, **Type**, **Description Matching** string, and **Valid time range**.

Step 3 Click **Apply** to save the changes,

Credentials Management

The Credential Management menu includes the following submenus:

SAN Credentials

The Cisco DCNM home page, choose **Administration > Credentials Management > SAN Credentials** displays the SNMP access details to the fabric seed switch. If the user has validated the access to all the fabrics, the SNMP credentials for all the seed switches of the fabrics is displayed.

The switch credentials window for the Cisco DCNM has the following fields:

Field	Description
Fabric Name	The fabric name to which the switch belongs.
Seed Switch	IP address of the switch.
User Name	Specifies the username of the Cisco DCNM user.
Password	Displays the encrypted form of the switch SNMP user.
SNMPv3/SSH	Specifies if the SNMP protocol is validated or not. The default value is **false**.
Auth/Privacy	Specifies the Authentication protocol The default value is **NOT_SET**.
Status	Displays the status of the switch

Before the Cisco DCNM user configures the fabric using SNMP, the user must furnish and validate SNMP credentials on the seed switch of the fabric. If the user does not provide valid credentials for the fabric seed switch, the Switch Credentials table shows the default values for SNMPv3/SSH and AuthPrivacy fields.

Click the switch row and enter correct credentials information. Click **Save** to commit the changes.

If the user changes the configuration, but does not provide a valid switch credential, the user action is rejected. Validate the switch credentials to commit your changes.

You can perform the following operations on this screen.

- To Revalidate the credentials:
  1. From the Cisco DCNM home page, choose **Administration > Credentials Management > SAN Credentials**, click the **Fabric Name** radio button to select a seed switch whose credentials needs to be validated.
  2. Click **Revalidate**.

     A confirmation message appears, stating if the operation was successful or a failure.

- To clear the switch credentials:

  1. From the Cisco DCNM home page, choose **Administration** > **Credentials Management** > **SAN Credentials**, click the **Fabric Name** radio button to select a seed switch to delete.
  2. Click **Clear**.

     A confirmation message appears.
  3. Click **Yes** to delete the switch credential from the DCNM server.

LAN Credentials

While changing the device configuration, Cisco DCNM uses the device credentials provided by you. However, if the LAN Switch credentials are not provided, Cisco DCNM prompts you to open the **Administration** > **Credentials Management** > **LAN Credentials** page to configure LAN credentials.

Cisco DCNM uses two sets of credentials to connect to the LAN devices:

- **Discovery Credentials**—Cisco DCNM uses these credentials during discovery and periodic polling of the devices.
- **Configuration Change Credentials**—Cisco DCNM uses these credentials when user tries to use the features that change the device configuration.

LAN Credentials Management allows you to specify configuration change credentials. Before changing any LAN switch configuration, you must furnish *Configuration Change* SSH credentials for the switch. If you do not provide the credentials, the configuration change action will be rejected.

These features get the device write credentials from LAN Credentials feature.

- Upgrade (ISSU)
- Maintenance Mode (GIR)
- Patch (SMU)
- Template Deployment
- POAP-Write erase reload, Rollback
- Interface Creation/Deletion/Configuration
- VLAN Creation/Deletion/Configuration
- VPC Wizard

You must specify the configuration change credentials irrespective of whether the devices were discovered initially or not. This is a one-time operation. Once the credentials are set, that will be used for any configuration change operation.

Default Credentials

Default credentials is used to connect all the devices that the user has access to. You can override the default credentials by specifying credentials for each of the devices in the Switch Table below.

Note After you enter appropriate credentials in **Password**, **Confirm Password** fields and click **Save**, the **Confirm Password** field is blank. A blank **Confirm Password** field implies that the password is saved successfully.

Cisco DCNM tries to use individual switch credentials in the Switch Table, to begin with. If the credentials (username/password) columns are empty in the Switch Table, the default credentials will be used.

Switch Table

Switch table lists all the LAN switches that user has access. You can specify the switch credentials individually, that will override the default credentials. In most cases, you need to provide only the default credentials.

You can perform the following operations on this screen.

- Edit Credentials, on page 322
- Validate Credentials, on page 322
- Clear Switch Credentials, on page 323
- Credentials Management with Remote Access, on page 323

The LAN Credentials for the DCNM User table has the following fields.

Field	Description
Switch	Displays the LAN switch name.
IP Address	Specifies the IP Address of the switch.
User Name	Specifies the username of the switch DCNM user.
Password	Displays the encrypted form of the SSH password.
Group	Displays the group to which the switch belongs.

Edit Credentials

Perform the following task to edit the credentials.

1. From the Cisco DCNM home page, choose **Administration** > **Credentials Management** > **LAN Credentials**, check the **Switch** check box for which you need to edit the credentials.
2. Click Edit icon.
3. Specify **User Name** and **Password** for the switch.

Validate Credentials

Perform the following task to validate the credentials.

1. From the **Administration** > **Credentials Management** > **LAN Credentials**, check the **Switch** check box for which you need to validate the credentials.
2. Click **Validate**.

A confirmation message appears, stating if the operation was successful or a failure.

Clear Switch Credentials

Perform the following task to clear the switch credentials.

1. From the **Administration** > **Credentials Management** > **LAN Credentials**, check the **Switch** check box for which you need to clear the credentials.
2. Click **Clear**.
3. Click **Yes** to clear the switch credentials from the DCNM server.

Credentials Management with Remote Access

DCNM allows you to authenticate users in different modes such as:

- Local Users - In this mode, you can use the Cisco DCNM Web UI to create a new user, assign a role, and provide access to one or more fabrics or groups for the user.
- Remote Users - In this mode, you can log in to DCNM. The DCNM server fetches information from the Remote Authentication server, for example, the Cisco Identity Services Engine (ISE), for AAA authentication. Cisco supports TACACS+, RADIUS, and LDAP options for remote authentication. For more information, see Remote AAA.

When you configure DCNM for remote authentication, the AAA server handles both authentication and authorization. DCNM forwards the entered user login and password to the AAA server to check for authentication. Post authentication, the AAA server returns the appropriate privileges/role assigned to the user through the **cisco-avpair** attribute. This attribute can contain the list of fabrics that a particular user can access. The supported roles for DCNM LAN deployments are as follows:

- network-admin
- network-operator

Both device discovery credentials and LAN credentials provide write access to the devices, but they differ—as the write operation is performed only with LAN credentials. Device discovery credentials are associated with each device and entered only once, that is, when you import the device into DCNM. DCNM uses these credentials for periodic rediscovery using a mix of SSH and SNMPv3 access to the device. However, LAN credentials are configured for every user on a per-user basis. If a user with an appropriate role has access to DCNM, then that user can enter the LAN credentials to get write access to the devices. The write operations use the LAN credentials to access the device, which allows for an appropriate audit trail of the changes made in DCNM by every user and the resultant changes in the device.

When you configure DCNM using Remote Authentication Methods such as TACACS+ or RADIUS, the users can set their LAN credentials as follows:

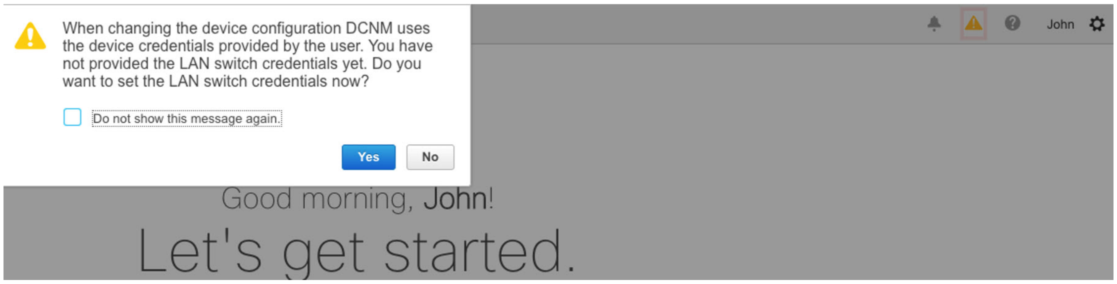
- Regular AAA Remote Authentication
- AAA Remote Authentication Passthrough Mechanism
- AAA Remote Authentication Using DCNM Service Account

Regular AAA Remote Authentication

Post authentication, when a user with an appropriate role logs in to DCNM for the first time, DCNM prompts the user to enter the LAN credentials. As mentioned earlier, DCNM uses these credentials to provide write access to the devices. All users must follow this process. Consider that an internal business policy requires the users to change password every 3-6 months. Then all the users must update their passwords for device access in the DCNM **LAN Credentials** window. Also, they must update their passwords in the AAA server.

For example, let us consider a user named John, who has authentication on the ISE server.

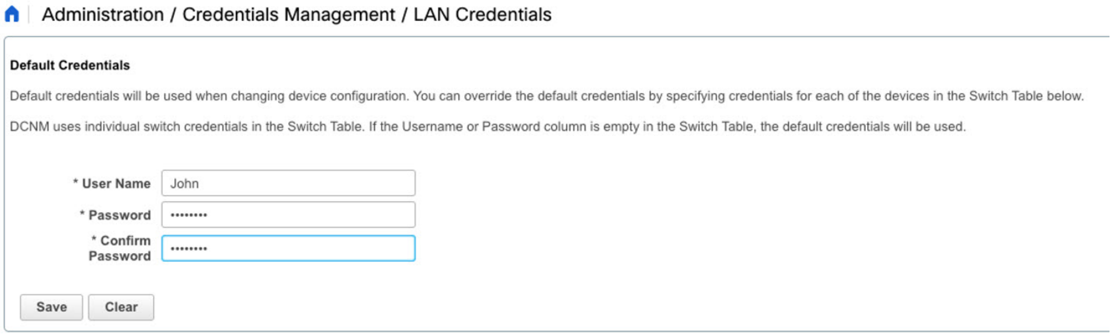
1. John logs in to DCNM with his user credentials.
2. The ISE server authenticates the user credentials of John, and DCNM displays a message to enter his LAN switch credentials. DCNM uses these credentials to perform various configurations and write operations on the devices.



When changing the device configuration DCNM uses the device credentials provided by the user. You have not provided the LAN switch credentials yet. Do you want to set the LAN switch credentials now?

□ Do not show this message again.

3. John enters his LAN switch credentials. DCNM uses the LAN switch credentials for all write operations triggered by John on all devices. However, John can also opt to enter LAN switch credentials on a per-device access basis. This per-device access option overrides the access provided by entering the default credentials.



Administration / Credentials Management / LAN Credentials

Default Credentials

Default credentials will be used when changing device configuration. You can override the default credentials by specifying credentials for each of the devices in the Switch Table below.

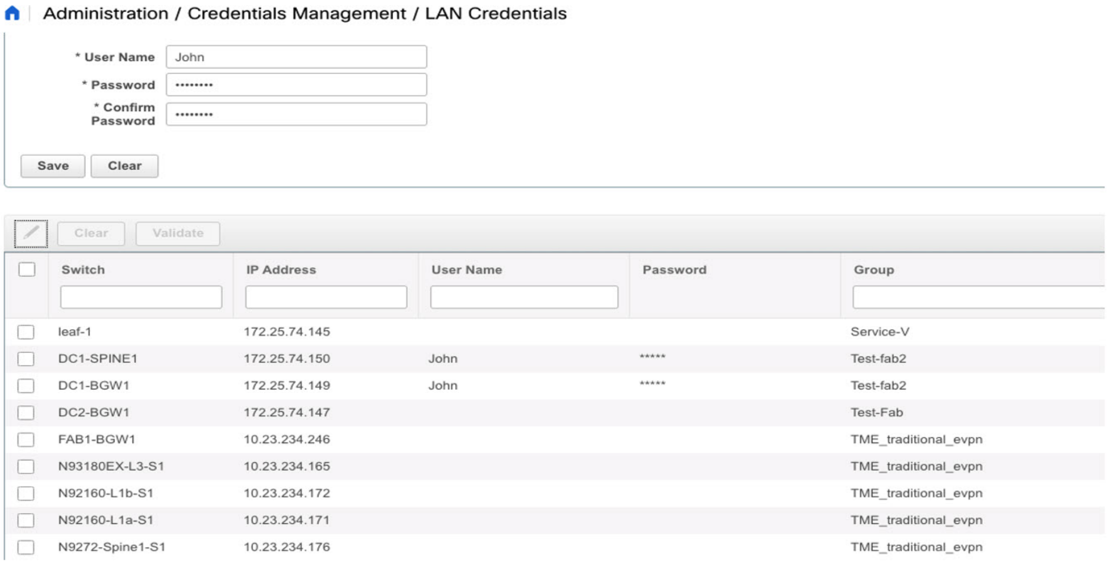
DCNM uses individual switch credentials in the Switch Table. If the Username or Password column is empty in the Switch Table, the default credentials will be used.

* User Name: John

* Password: ••••••••

* Confirm Password: ••••••••

When John logs in to DCNM again, DCNM doesn't display any message to enter the LAN switch credentials as it has already captured his LAN switch credentials. John uses the same credentials to log in to DCNM and to the devices that he can access.



Administration / Credentials Management / LAN Credentials

* User Name	John
* Password	••••••••
* Confirm Password	••••••••

☐	Switch	IP Address	User Name	Password	Group
☐	leaf-1	172.25.74.145			Service-V
☐	DC1-SPINE1	172.25.74.150	John	*****	Test-fab2
☐	DC1-BGW1	172.25.74.149	John	*****	Test-fab2
☐	DC2-BGW1	172.25.74.147			Test-Fab
☐	FAB1-BGW1	10.23.234.246			TME_traditional_evpn
☐	N93180EX-L3-S1	10.23.234.165			TME_traditional_evpn
☐	N92160-L1b-S1	10.23.234.172			TME_traditional_evpn
☐	N92160-L1a-S1	10.23.234.171			TME_traditional_evpn
☐	N9272-Spine1-S1	10.23.234.176			TME_traditional_evpn

4. Now, consider that after a few months, the Corporate IT policy changes. Then John must update his password in the Remote AAA server, and also perform Step 3 to allow DCNM to update his LAN switch credentials.

Thus, in this mode, when John logs in to the DCNM Web GUI with his updated password, DCNM doesn't display any message to enter LAN credentials. However, John must update the password in LAN Credentials. Updating the password is necessary as it allows DCNM to inherit the newly updated password and perform write operations on the devices.

AAA Remote Authentication Passthrough Mechanism

In this mode, when a user enters the username and password to log in to DCNM, DCNM automatically copies the user credentials to the Default Credentials in the LAN switch credentials settings for that user. As a result, when the user logs in for the first time, DCNM doesn't display the message to enter the LAN switch credentials.

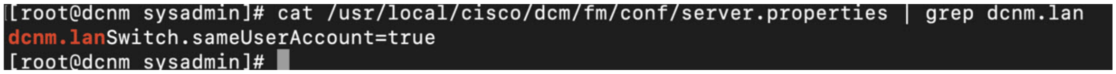
1. Use SSH to log in to DCNM as a sysadmin user.

2. Log in to the `/root/directory` using the **su** command.

3. Navigate to the `/usr/local/cisco/dcm/fm/conf/server.properties` file.

4. Add the following server property to the file and save the changes.

   dcnm.lanSwitch.sameUserAccount=true



```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep dcnm.lan
dcnm.lanSwitch.sameUserAccount=true
[root@dcnm sysadmin]#
```

5. Restart DCNM using the **service FMServer restart** command.

6. Now, John logs in to DCNM.

7. After successful authentication, DCNM doesn't display the message to update the LAN switch credentials, as it automatically copies this information to the LAN switch credentials.

8. Consider that after a few months, the Corporate IT policy changes. In this mode, John must update his password in the Remote AAA server. After that, when John logs in to DCNM, DCNM automatically copies the updated credentials to the Default LAN Credentials associated with the user John.

AAA Remote Authentication Using DCNM Service Account

Often, the customers prefer to track all the changes made from the DCNM controller with a common service account. In the following example, a user makes changes using the DCNM controller, which results in changes on the device. These changes are audit logged on the device, against a common service account. Thus, it is possible to distinguish the controller-triggered changes from other changes (also known as Out-of-Band changes) made by the user directly on the device. The Out-of-Band changes appear in the device accounting logs as made from the user account.

For example, create a service account with the name **Robot** on the remote AAA server. Using the corresponding credentials, the Robot user can log in to DCNM. The Robot user can enter the default LAN credentials to have write access to the devices. The DCNM network-admin enables a server property that automatically sets the default LAN credentials for all the users and inherits the default LAN credentials associated with Robot.

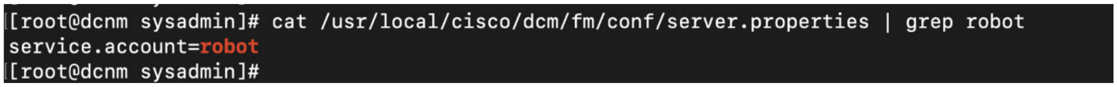
Therefore, when any user logs in to DCNM and makes any configuration changes, DCNM pushes the changes to the devices using the LAN credentials of Robot. The DCNM deployment history logs track the user who triggered the change and display the corresponding changes deployed from DCNM to the switch in the audit log with the user Robot.

To set up the service account on the DCNM, perform the following steps:

1. Use SSH to log in to DCNM as a sysadmin user.
2. Log in to the `/root/ directory` using the **su** command.
3. Navigate to the `/usr/local/cisco/dcm/fm/conf/server.properties` file.
4. Add the following server property to the file and save the changes.

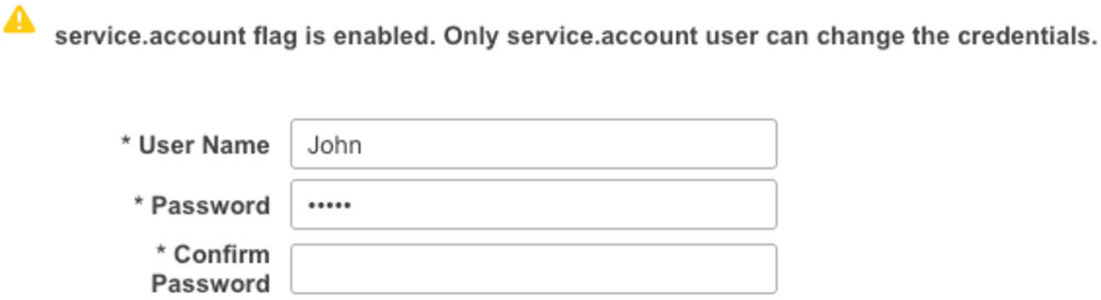
   service.account=robot

Note You can enable either an AAA passthrough account or a Service Account.



```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

5. Restart DCNM using the **service FMServer restart** command.
6. Now, John logs in to DCNM.
7. After successful authentication, DCNM doesn't display the message to update the LAN switch credentials. However, when John navigates to the **LAN Credentials** page, DCNM displays a message stating that the Service Account is enabled in DCNM and, hence, all LAN credentials will be inherited from the service account.



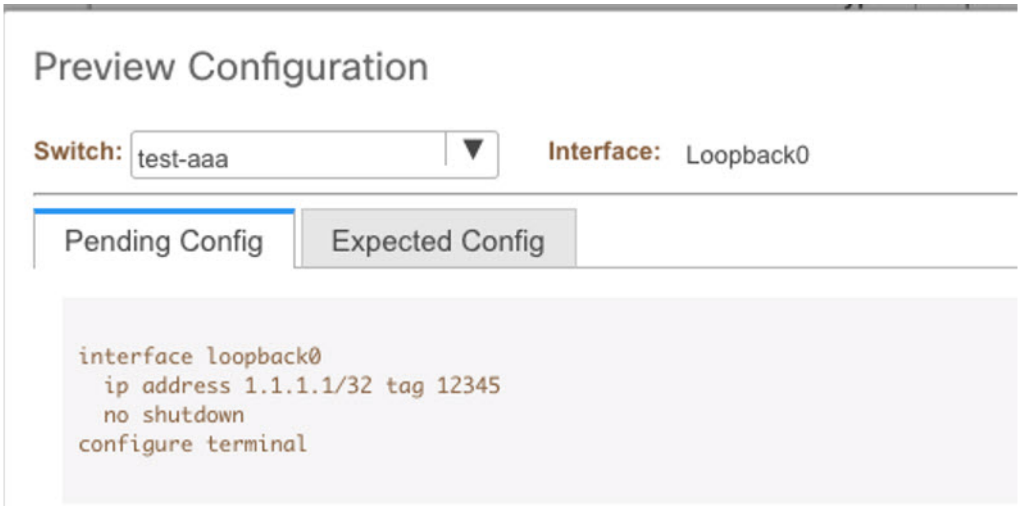
service.account flag is enabled. Only service.account user can change the credentials.

* User Name	John
* Password	•••••
* Confirm Password	

Service Account Configuration Audit

The following workflow example allows for verification of the configuration audit while using the DCNM service account feature. However, you must have completed the Service Account Activation procedure.

1. John creates a test loopback on a device.



Preview Configuration

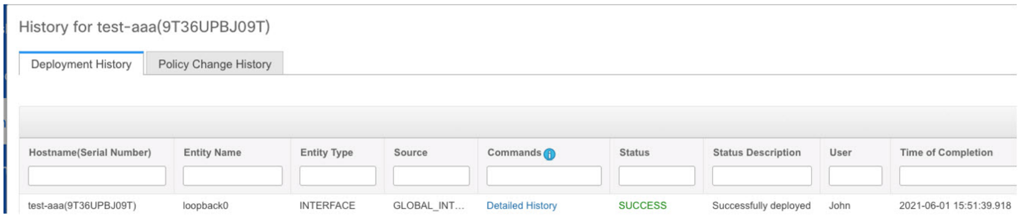
Switch: test-aaa

Interface: Loopback0

```
interface loopback0
  ip address 1.1.1.1/32 tag 12345
  no shutdown
configure terminal
```

2. John deploys the configuration using DCNM.

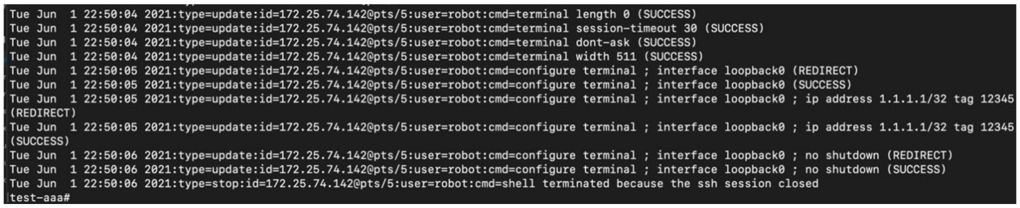
3. The DCNM Deployment history confirms that John made the recent configuration change.



History for test-aaa(9T36UPBJ09T)

Hostname(Serial Number)	Entity Name	Entity Type	Source	Commands	Status	Status Description	User	Time of Completion
test-aaa(9T36UPBJ09T)	loopback0	INTERFACE	GLOBAL_INT...	Detailed History	SUCCESS	Successfully deployed	John	2021-06-01 15:51:39.918

4. The accounting logs of the device indicate that the DCNM Service Account (that is, Robot, in this example) has triggered the changes on the NX-OS device.



```
Tue Jun  1 22:50:04 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=terminal length 0 (SUCCESS)
Tue Jun  1 22:50:04 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=terminal session-timeout 30 (SUCCESS)
Tue Jun  1 22:50:04 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=terminal dont-ask (SUCCESS)
Tue Jun  1 22:50:04 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=terminal width 511 (SUCCESS)
Tue Jun  1 22:50:05 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=configure terminal ; interface loopback0 (REDIRECT)
Tue Jun  1 22:50:05 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=configure terminal ; interface loopback0 (SUCCESS)
Tue Jun  1 22:50:05 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=configure terminal ; interface loopback0 ; ip address 1.1.1.1/32 tag 12345
(REDIRECT)
Tue Jun  1 22:50:05 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=configure terminal ; interface loopback0 ; ip address 1.1.1.1/32 tag 12345
(SUCCESS)
Tue Jun  1 22:50:06 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=configure terminal ; interface loopback0 ; no shutdown (REDIRECT)
Tue Jun  1 22:50:06 2021:type=update:id=172.25.74.142@pts/5:user=robot:cmd=configure terminal ; interface loopback0 ; no shutdown (SUCCESS)
Tue Jun  1 22:50:06 2021:type=stop:id=172.25.74.142@pts/5:user=robot:cmd=shell terminated because the ssh session closed
test-aaa#
```

CHAPTER 8

Applications

Cisco Data Center Network Manager (DCNM) uses the application framework to host various plugins and microservices to support operations and related features in Cisco DCNM.

The Applications Framework provides the following features:

- An infrastructure for hosting applications that require more system resources as the scale of the network increases.
- An independent application development-deployment-management lifecycle for applications.

Cisco DCNM Applications Framework supports two modes namely clustered mode and unclustered mode. In clustered mode, the compute nodes are clustered together whereas in the latter only the DCNM server nodes namely the active/standby exist. Most of the applications for ex: Network Insights require clustered setup to be ready before they can be uploaded and deployed using DCNM Applications Framework.

Application Framework User Interface

To use the Applications Framework feature, in the Cisco DCNM home page's left pane, click **Applications**.

The Applications window displays the following tabs:

- **Catalog**—This tab lists the applications that are used by Cisco DCNM. These applications for performing various functions within Cisco DCNM. For more information, see *Catalog*.
- **Compute**—This tab displays the existing compute nodes. The tab shows nodes that are part of the hosting infrastructure. The uptime indicates how long they have been part of the infrastructure. In a High Availability (HA) setup, both the active and the standby nodes appear as joined. For more information, see Compute, on page 336.

Note In the cluster mode, the Cisco DCNM servers will not appear under the Compute tab.

- **Preferences**—This tab is relevant to the cluster mode of deployment, where the application instances are placed. This tab enables you to compute the cluster connectivity and configure the Cluster Connectivity preferences. For more information, see Preferences, on page 337.

Cisco DCNM uses the following applications:

- Kibana: This is an open-source data-visualization plug-in for Elasticsearch, which provides visualization capabilities. Cisco DCNM uses the Kibana application for the Media Controller, and Endpoint Locator.
- San Insight Pipeline Collector(1.0)
- SAN Insight Post Processor(1.0)
- Health Monitor(2.0)

Catalog

The Catalog allows you to view all the applications that you have installed or enabled on the Cisco DCNM. Few applications are installed and are operational by default, when you install the Cisco DCNM.

The following applications appears based on the Cisco DCNM Deployments:

- Health Monitor (2.1)
- PTP Monitoring (1.1)
- Kibana (2.0)
- Programmable report (1.1.0)
- Elastic Service (1.1)
- Compliance (4.0.0)
- Debug Tools (2.1)
- IPAM Integrator (1.0)
- Endpoint Locator (2.1)
- Kubernetes Visualizer (1.1)
- vmmplugin (4.1)

Note The applications started by default, or also installed on the DCNM utilizes infrastructure services are operational, by default.

You can install more applications from the App Center, via the Web UI.

Health Monitor

The Health Monitor helps you to monitor the infrastructure health and status. You can monitor the Alerts, Service Utilization, and Compute Utilization using the Health Monitor application. When you install or upgrade to 11.2(1), the Health Monitor application is installed and operational, by default.

To launch the Health Monitor app, on the Cisco DCNM Web UI, choose **Applications**. On the Catalog tab, click on **Health Monitor** to launch the application.

Note Health Monitor application is installed by default in Cisco DCNM cluster mode.

Health Monitor app broadly monitors and alerts on the following metrics for Services, Computes and DCNM server:

- CPU utilization
- Memory utilization
- Network I/O (eth0)
- Disk I/O

You can monitor the following using the Health Monitor application:

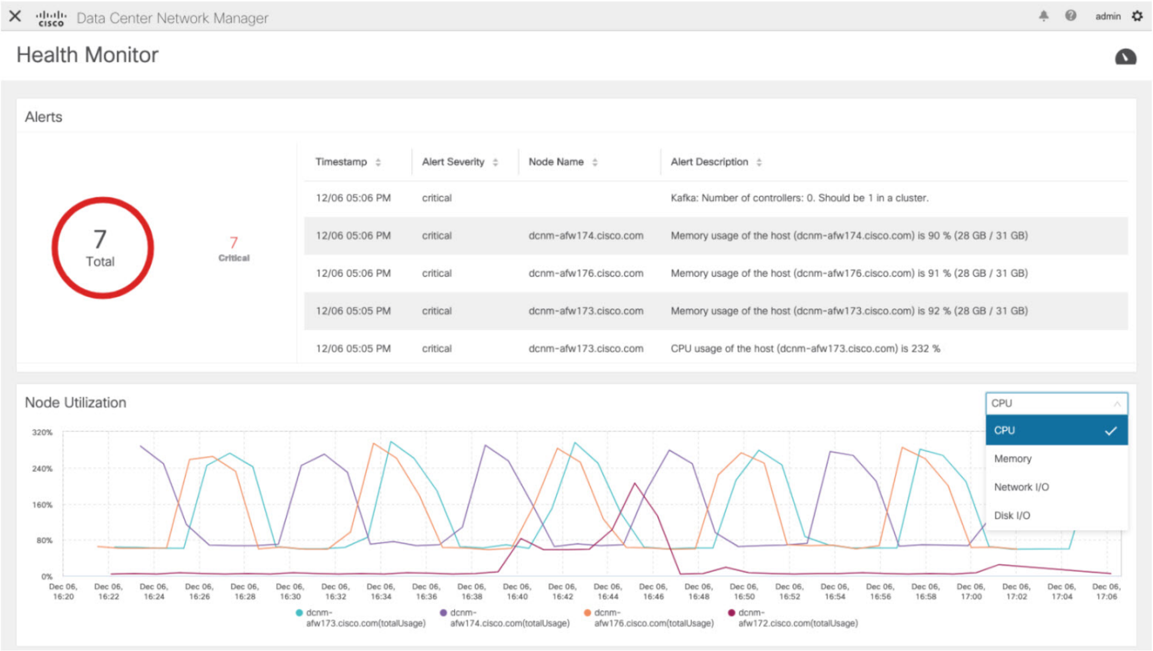
Alerts

The Alerts window provides information about the number of alerts that have occurred, from the specified date and time. You can view the alerts, based on the following categories, in the graphical view and the list view.

In the graphical view, the categories are:

- **Severity** displays the alerts, based on the severity: Critical/Major/Minor/Info.
- **Type** displays the alerts, based on the cluster type.
- **Compute** displays the alerts, for each compute node.
- **Service** displays the alerts, for all the services running on Cisco DCNM.

Click on the Refresh icon to refresh the alerts. Click on the list view icon to view the alerts in list format.



Timestamp	Alert Severity	Node Name	Alert Description
12/06 05:06 PM	critical		Kafka: Number of controllers: 0. Should be 1 in a cluster.
12/06 05:06 PM	critical	dcnm-afw174.cisco.com	Memory usage of the host (dcnm-afw174.cisco.com) is 90 % (28 GB / 31 GB)
12/06 05:06 PM	critical	dcnm-afw176.cisco.com	Memory usage of the host (dcnm-afw176.cisco.com) is 91 % (28 GB / 31 GB)
12/06 05:05 PM	critical	dcnm-afw173.cisco.com	Memory usage of the host (dcnm-afw173.cisco.com) is 92 % (28 GB / 31 GB)
12/06 05:05 PM	critical	dcnm-afw173.cisco.com	CPU usage of the host (dcnm-afw173.cisco.com) is 232 %

In the List View, alerts are displayed in tabular format with the following categories:

- **Timestamp** displays the time when the alert triggers. Format is MM/DD HH:MM AM/PM.
- **Alert Severity** displays the severity of alert.
- **Alert Type** displays the cluster alert type.
- **Node Name** displays the node name where the alert triggers.
- **Alert Description** displays the summary of the alert.

Click on the right or left navigation arrows to move to the next or the previous page.

You can also choose to set the number of items to view on page. Select a suitable number from the **Objects Per Page** drop-down list.

Click on the **Graphical representation** icon to go to the graphical view. Click on **Download Data** icon to download alerts information for troubleshooting purposes.

Health Monitor generates alerts for the following metrics:

- CPU utilization >= 65 %
- Memory utilization >= 65 %
- Disk utilization >= 65 %
- Elasticsearch cluster status: Red/yellow
- Elasticsearch unassigned shards > 0
- Elasticsearch JVM heap used >= 65 %
- Kafka partitions without leader: Controller offline partitions count > 0
- Kafka controllers count: Controller active controller count != 1

- Kafka partition leader: Controller unclear leader elections count > 0

Service Utilization

You can monitor all the services running on the Cisco DCNM on this window. Based on the time range and the service, the graphical view shows the CPU and Memory utilization for service. Click on the **Service Utilization** icon on the top-right corner to launch the CPU utilization graphical view.

From the **Time Range** drop-down list, choose the time range for which you want to view the utilization. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. You can also click the date on the calendar to set range. Click **Apply** to confirm the time range.

From the **Services** drop-down list, choose the service to view its Service utilization. This list comprises of all the services that are currently running on the Cisco DCNM.

Select the Time Range to view the **Service**, the **Cpu Utilization**, and **Memory Utilization** graphs. You can hover over specific points on the respective graphs for more information on CPU and Memory utilization at specific time.

The memory utilization graphical view depicts the actual memory consumption (RAM) in Gigabytes (GB).

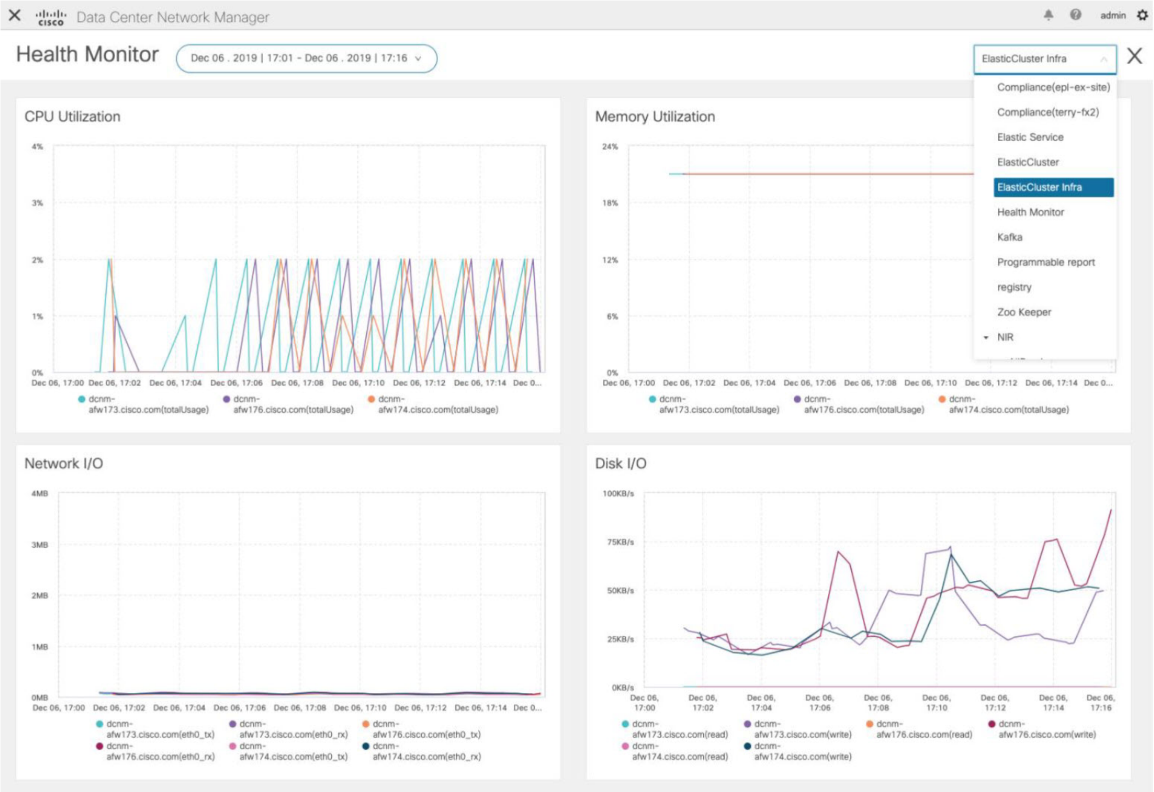
Click [**X**] icon on the top-right corner to close the Service Utilization window and revert to the Alerts window.

Guidelines and Limitations for Health Monitor in Service Utilization

- The CPU utilization for applications without a CPU limit, like Kafka, ElasticSearch, FMserver, and so on, may show 100% utilization in the graphs. 100% utilization is because this application uses one or more cores.
- The following alerts are triggered for the CPU utilization of applications:
  - Minor alert: 200-400 %

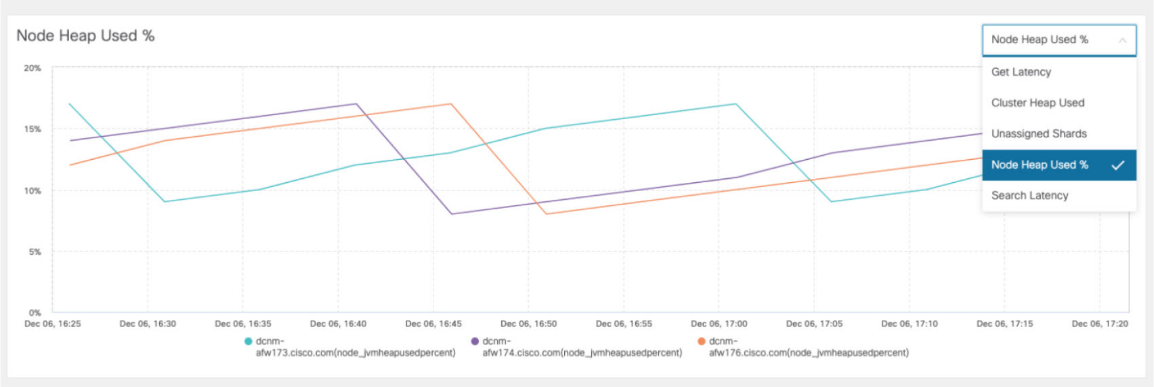
    Major alert: 400-600%

    Critical: > 600%
- The transient message for Kafka controller counts appears as a severe alert sometimes. You can ignore the alert if it clears within two minutes after refresh.
- The **Disk I/O** and **Memory Utilization** metrics are not available for Kafka and Elastic Service.
- The **Network I/O** metric is not available for **DCNM: FMServer** and **DCNM: Postgres**.
- The metrics does not auto-refresh. Navigate between different windows using the options in the drop-down list to refresh the metrics. Additionally, you can change the time range to refresh the metrics for a selected period.
- There might be duplicate alerts for the same feature.



The following additional metrics are collected for Elastic Cluster:

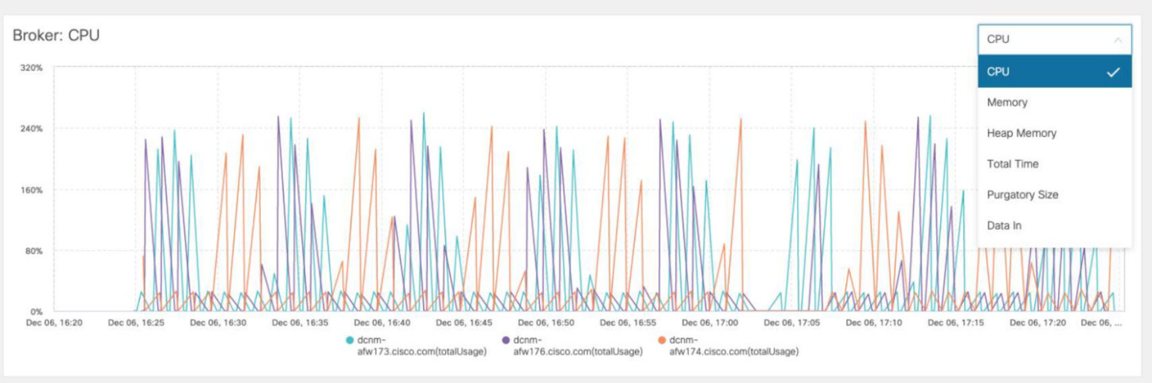
- Get latency: Latency for getting a single record by id
- Cluster heap used: Heap memory used by the cluster
- Unassigned shards: Count of unassigned shards
- Node heap used percentage: Percentage heap memory used by the node
- Search latency: Latency for getting a collection of records



The following additional metrics are collected for Kafka broker:

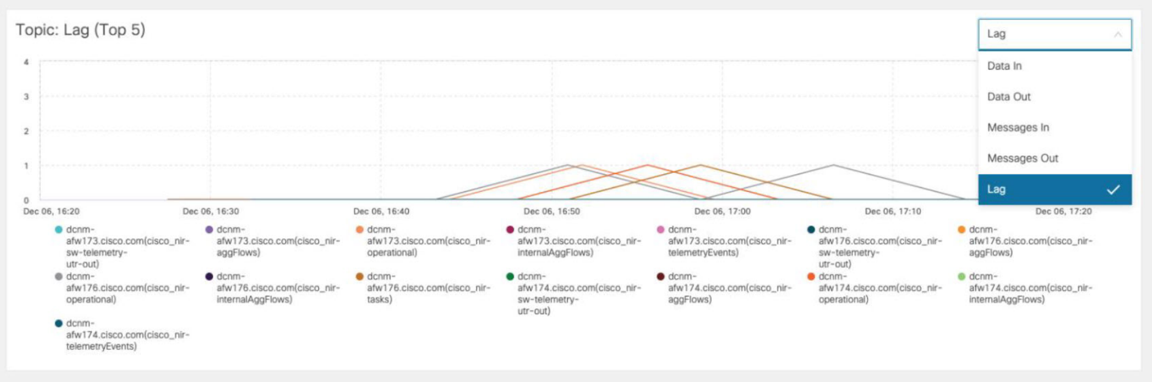
- CPU: CPU utilization of broker

- Memory: Memory utilization of broker
- Heap memory: Heap memory utilized by broker
- Total time: Network produce, network fetch follower, network fetch consumer time
- Purgatory size: Server fetch purgatory size, server produce purgatory size of broker
- Data in: Bytes in for the broker
- Data out: Bytes out for the broker
- Messages in: Messages received by the broker
- Fetch request: Total fetch requests for the broker
- ISR: In-sync-replicas expands and shrinks for the broker



The following additional metrics are collected for top 5 Kafka topics:

- Data in: Bytes in for the topic
- Data out: Bytes out for the topic
- Messages in: Message in count for topic
- Messages out: Message out count for topic
- Lag: Lag per topic


Topic: Lag (Top 5)
Lag
Data In
Data Out
Messages In
Messages Out
Lag ✓
4
3
2
1
0
Dec 06, 16:20
Dec 06, 16:30
Dec 06, 16:40
Dec 06, 16:50
Dec 06, 17:00
Dec 06, 17:10
Dec 06, 17:20
● dcnm-afw173.cisco.com(cisco_nir-sw-telemetry-utr-out)
● dcnm-afw173.cisco.com(cisco_nir-aggFlows)
● dcnm-afw173.cisco.com(cisco_nir-operational)
● dcnm-afw173.cisco.com(cisco_nir-internalAggFlows)
● dcnm-afw173.cisco.com(cisco_nir-telemetryEvents)
● dcnm-afw176.cisco.com(cisco_nir-sw-telemetry-utr-out)
● dcnm-afw176.cisco.com(cisco_nir-aggFlows)
● dcnm-afw176.cisco.com(cisco_nir-operational)
● dcnm-afw176.cisco.com(cisco_nir-internalAggFlows)
● dcnm-afw176.cisco.com(cisco_nir-tasks)
● dcnm-afw174.cisco.com(cisco_nir-sw-telemetry-utr-out)
● dcnm-afw174.cisco.com(cisco_nir-aggFlows)
● dcnm-afw174.cisco.com(cisco_nir-operational)
● dcnm-afw174.cisco.com(cisco_nir-internalAggFlows)
● dcnm-afw174.cisco.com(cisco_nir-telemetryEvents)

Compute Utilization

You can monitor all the computes installed with the Cisco DCNM. Based on the time range and the service, the graphical view shows the CPU and Memory utilization for service. Click on the **Compute Utilization** icon on the top-right corner to launch the CPU utilization graphical view.

From the **Time Range** drop-down list, choose the time range for which you want to view the utilization. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. You can also click the date on the calendar to set range. Click **Apply** to confirm the time range.

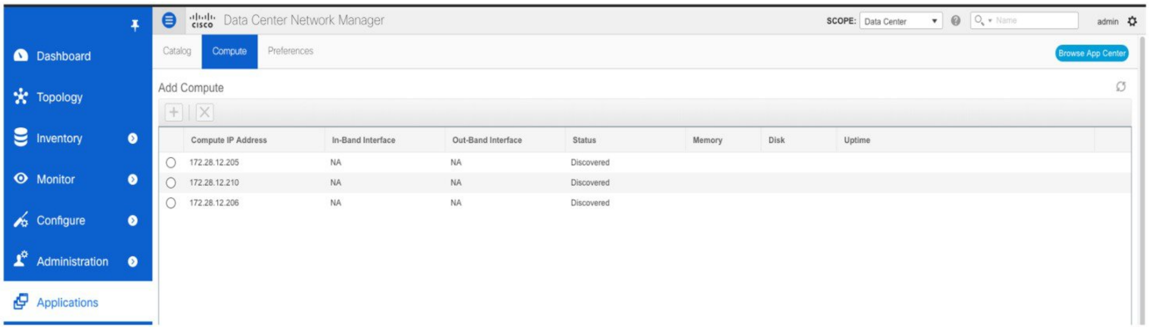
Select the Time Range to view the **Service**, the **Cpu Utilization**, and **Memory Utilization** graphs. You can hover over specific points on the respective graphs for more information on CPU and Memory utilization at specific time.

The memory utilization graphical view depicts the actual memory consumption (RAM) in Gigabytes (GB).

Click [**X**] icon on the top-right corner to close the Service Utilization window and revert to the Alerts window.

Compute

This tab displays the existing compute nodes. The tab shows nodes that are part of the hosting infrastructure. The uptime indicates how long they have been part of the infrastructure. In a High Availability (HA) setup, both the active and the standby nodes appear as joined. In clustered mode, the compute nodes status indicate if the nodes are joined or discovered.



Add Compute

	Compute IP Address	In-Band Interface	Out-Band Interface	Status	Memory	Disk	Uptime
○	172.28.12.205	NA	NA	Discovered			
○	172.28.12.210	NA	NA	Discovered			
○	172.28.12.206	NA	NA	Discovered			

Note If the NTP server for compute nodes is not synchronized with the NTP server for DCNM Servers (Active and Standby) and Computes, you cannot configure a cluster.

The certificates are generated with a timestamp. If you configure the Compute nodes using a different NTP server, the mismatch in timestamp will not allow to validate the certificates. Therefore, if the compute cluster is configured despite of a mismatch of NTP server, the applications will not function properly.

Note In clustered mode, the Cisco DCNM servers will not appear under the Compute tab.

The following table describes the fields that appear on **Applications** > **Compute**.

Table 34: Field and Description on Compute Tab

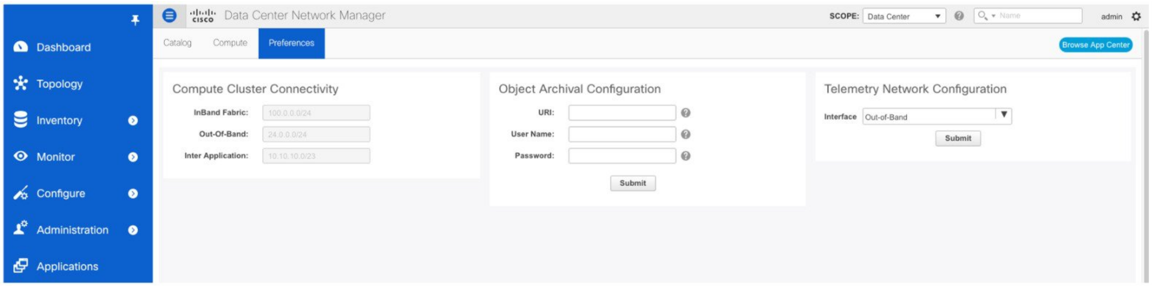
Field	Description
Compute IP Address	Specifies the IP Address of the Compute node.
In-Band Interface	Specifies the in-band management interface.
Out-Band Interface	Specifies the out-band management interface.
Status	Specifies the status of the Compute node. • Joined • Discovered • Failed • Offline
Memory	Specifies the memory that is consumed by the node.
Disk	Specifies the disk space that is consumed on the compute node.
Uptime	Specifies the duration of the uptime for a compute node.

When you install a compute node with correct parameters, it appears as **Joined** in the Status column. However, the other two computes appears as Discovered.

To configure or modify the Cluster Connectivity preferences, see Preferences, on page 337.

Preferences

This tab is relevant to the cluster mode of deployment, where the application instances are placed. This tab enables you to compute cluster connectivity and configure the Cluster Connectivity preferences.



Compute Cluster Connectivity

InBand Fabric: 100.0.0.0/24

Out-Of-Band: 24.0.0.0/24

Inter Application: 10.10.10.0/23

Object Archival Configuration

URI:

User Name:

Password:

Telemetry Network Configuration

Interface: Out-of-Band

Note This deployment does not support the compute cluster connectivity. The **Compute Cluster Connectivity** fields are grayed out for this deployment.

Object Archival Configuration

The NIA application collects tech support logs for all switches in Fabric, and determines the advisory, based on the data. The logs are saved on the Cisco DCNM server for further analysis or troubleshooting. If you need to download these logs before their life span ends or to create some space on the DCNM server, you can move the logs to a remote server.

In the **URI** field, enter the relative path to the archive folder, in the format `host[:port]/[path to archive]`. Enter the username and password to access the URI, in the **username** and **Password** field. Click **Submit** to configure the remote server.

CHAPTER 9

DCNM Integration with ServiceNow

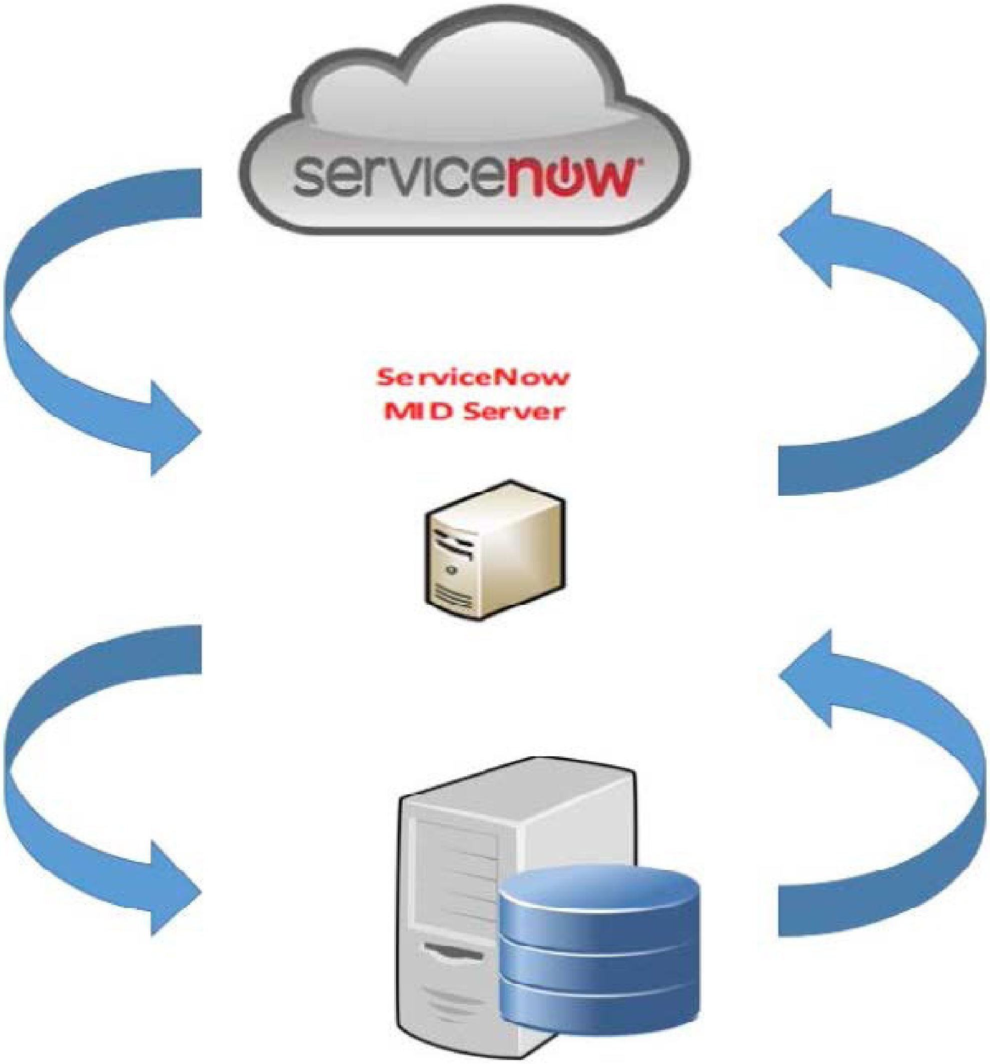
DCNM Integration with ServiceNow

ServiceNow offers applications for IT Service Management (ITSM) and IT Operations Management (ITOM). There are four primary modules - inventory discovery, incident management, event management & change management workflows. Starting from Cisco DCNM Release 11.3(1), we provide Cisco DCNM integration with ServiceNow. This enables you to integrate end-user IT data with the ServiceNow platform. The integration provides a default set of ServiceNow custom tables which are populated with configuration data.

To utilize this functionality, install the DCNM application in the ServiceNow customer instance and provide the DCNM mid-server details. Information or data regarding switch details, port details, and alarms, is retrieved to the ServiceNow Configuration Management Database (CMDB) tables. By default, data is retrieved every 15 minutes and displayed.

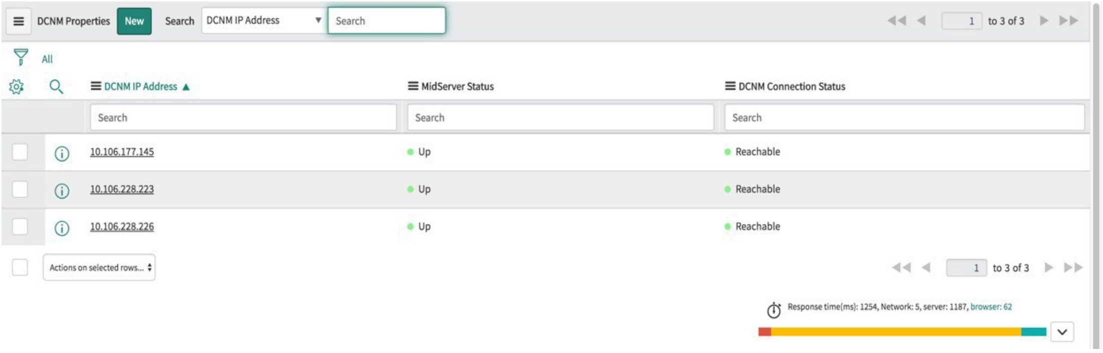
Details about the switches and ports of each switch are collected from the DCNM inventory. The alarms are collected by polling DCNM. Alarms are then filtered and categorized based on their type, such as, CPU, MEMORY, POWER, LINKSTATE, EXTERNAL, ICMP, SNMP, and SSH. The alarms are then stored in an Events table. These events are then used to generate incidents for the CPU, MEMORY, SNMP, and SSH categories. The source, description, severity and category of each alarm is stored. However, when an alarm ceases to exist in DCNM, the incident that was raised for it is not updated or cleared on the DCNM ServiceNow application. When polling of alarms is initiated for the first time, the alarms that were raised in the last seven days are pulled in from DCNM.

The DCNM application on ServiceNow runs scheduled scripts and connects with the mid-server which in turn connects with DCNM to retrieve data. DCNM sends the requested data to the mid-server which then passes on the data to the DCNM application on ServiceNow. The tables in the DCNM instance on ServiceNow are then populated with this retrieved data.



Guidelines and Limitations of DCNM Integration with ServiceNow

- In the ServiceNow Cisco DCNM Application version 1.0, details about only one MID server can be added in the **Cisco DCNM>Properties** table. Starting from Cisco DCNM Application version 1.1, multiple MID servers can be added in the **Cisco DCNM>Properties** table. This means that data can be retrieved from multiple DCNM setups at the same time. In the ServiceNow GUI, data from each DCNM is distinguished by the DCNM IP address.


DCNM Properties
New
Search
DCNM IP Address
Search
1 to 3 of 3
All
Actions on selected rows...
1 to 3 of 3
Response time(ms): 1254, Network: 5, server: 1187, browser: 62

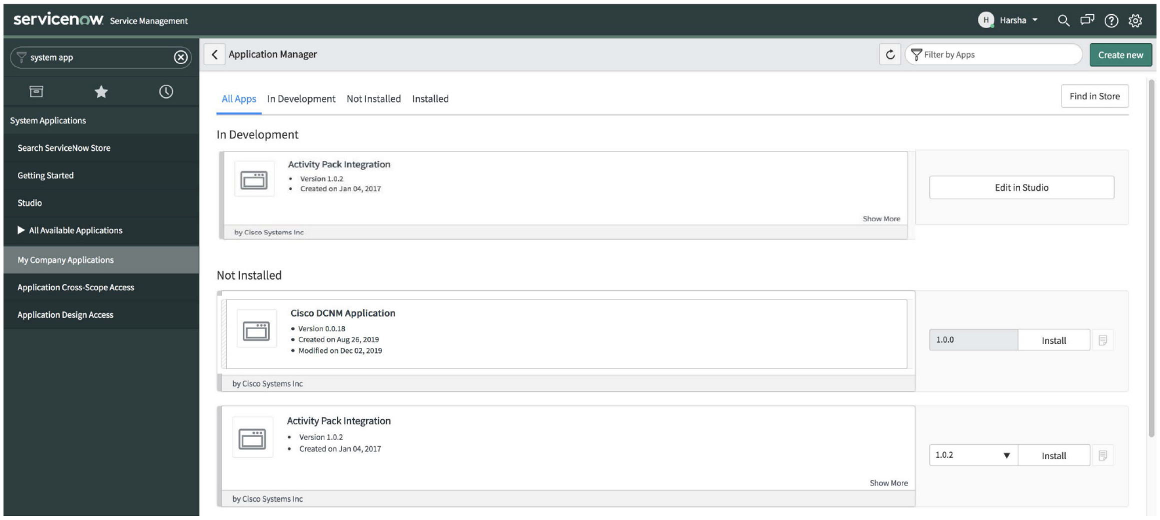
DCNM IP Address ▲	MidServer Status	DCNM Connection Status
10.106.177.145	Up	Reachable
10.106.228.223	Up	Reachable
10.106.228.226	Up	Reachable

- Scheduled scripts to retrieve data are run only after insertion of a server record in the **Cisco DCNM>Properties** table.
- In case the mid-server IP Address and credentials in the **Cisco DCNM>Properties** table are changed, the data that was imported using the previous mid-server is deleted from the application scope tables. However, data that was imported to the ServiceNow CMDB (global scope) remains and is not deleted.
- To ensure optimal performance in the ServiceNow database, each entry is matched with the switch database ID and IP Address ensuring that there is no duplication of entries.
- Entries in the cmdb_ci_ip_switch table have to be manually deleted in case a new server is added in the **Cisco DCNM>Properties** table.

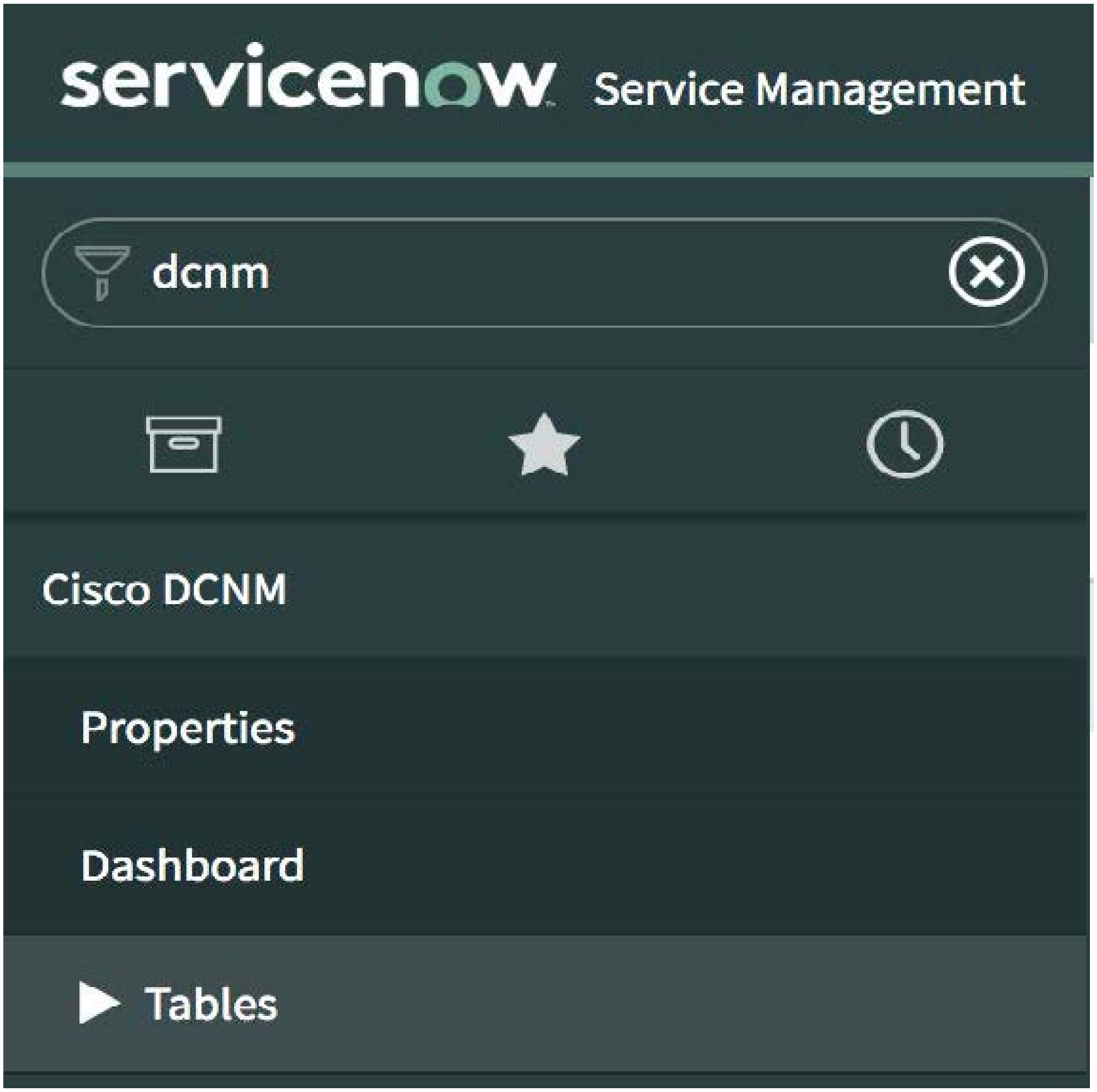
Installing and Configuring the Cisco DCNM Application on ServiceNow

Procedure

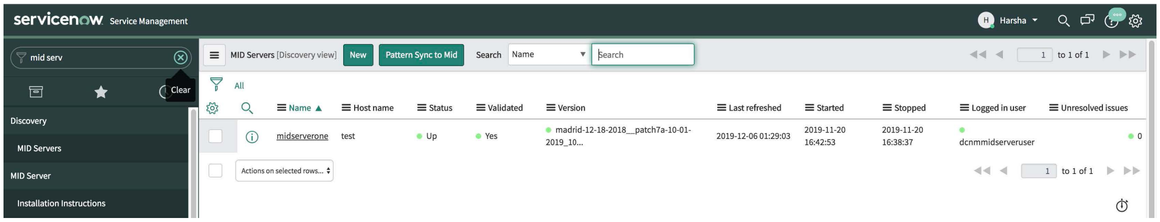
Step 1 Log in to https://dcnm1.service-now.com. Select **System Applications** > **Applications**. Install the **Cisco DCNM Application** from the **All Apps** tab.



Step 2 After installation is complete, verify that the Cisco DCNM Properties and Dashboard tabs are appearing in the application.



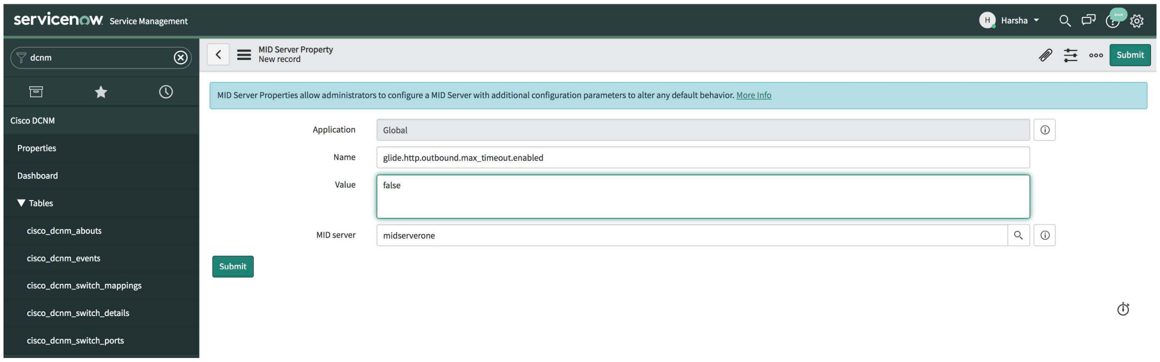
Step 3 Choose **MID Servers** and click the MID Server that is used for DCNM integration.


servicenow Service Management
Harsha
mid serv
Clear
Discovery
MID Servers
MID Server
Installation Instructions
MID Servers [Discovery view]
New
Pattern Sync to Mid
Search
Name
Search
1 to 1 of 1
All
Actions on selected rows...

Name ▲	Host name	Status	Validated	Version	Last refreshed	Started	Stopped	Logged in user	Unresolved issues
midserverone	test	● Up	● Yes	● madrid-12-18-2018__patch7a-10-01-2019_10...	2019-12-06 01:29:03	2019-11-20 16:42:53	2019-11-20 16:38:37	● dcnmmidserveruser	● 0

Step 4 Scroll down and click the **Properties** tab. Click **New** and add the property given below in the **MID Server Property New record** window. Click **Submit**.

Name	Type	Value
glide.http.outbound.max_timeout.enabled	True/false	False



MID Server Property
New record

MID Server Properties allow administrators to configure a MID Server with additional configuration parameters to alter any default behavior. More Info

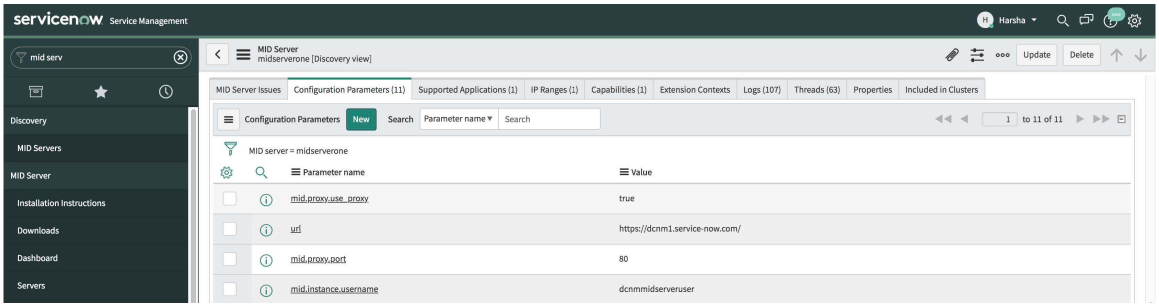
Application: Global

Name: glide.http.outbound.max_timeout.enabled

Value: false

MID server: midserverone

Step 5 Now, select the **Configuration Parameters** tab.



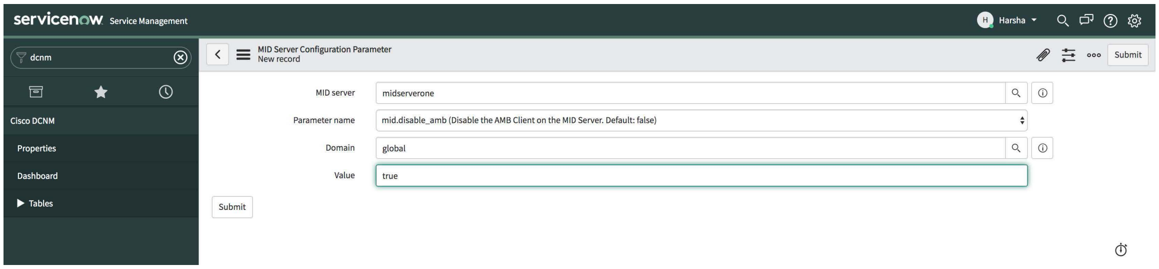
MID Server
midserverone [Discovery view]

Configuration Parameters

MID server = midserverone

Parameter name	Value
mid.proxy.use_proxy	true
url	https://dcnm1.service-now.com/
mid.proxy.port	80
mid.instance.username	dcnmmidserveruser

Step 6 In the **Configuration Parameters** tab, click **New**. Enter the required details in the fields.



MID Server Configuration Parameter
New record

MID server: midserverone

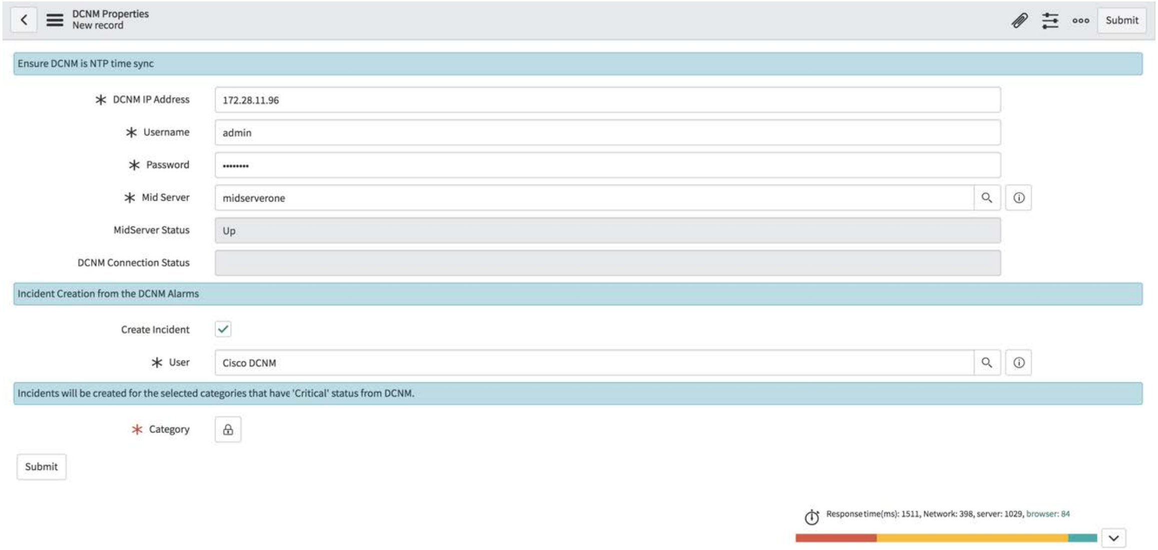
Parameter name: mid.disable_amb (Disable the AMB Client on the MID Server. Default: false)

Domain: global

Value: true

Step 7 Click **Submit** to set up the MID Server.

Step 8 Choose **Cisco DCNM > Properties**. Click **New Server**. Enter the required parameters.



DCNM Properties
New record
Submit

Ensure DCNM is NTP time sync

* DCNM IP Address	172.28.11.96
* Username	admin
* Password	••••••••
* Mid Server	midserverone
MidServer Status	Up
DCNM Connection Status	

Incident Creation from the DCNM Alarms

Create Incident	☑
* User	Cisco DCNM

Incidents will be created for the selected categories that have 'Critical' status from DCNM.

* Category 🔒

Submit
Response time(ms): 1511, Network: 398, server: 1029, browser: 84

DCNM IP Address - IP Address of the DCNM.

Username - Enter the username used to log in to DCNM.

Password - Enter the password used to log in to DCNM.

Note Access should be provided only for DCNM admins.

Mid server - Specify the name of the mid server to be used. The name is auto-populated as you type. You can also click the search icon next to this field to bring the MID Servers window. You can then select a MID Server from the list that is displayed.

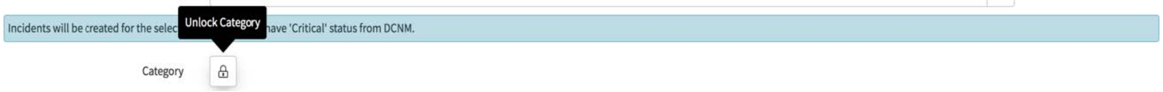
MidServer Status - Indicates whether the MID server is up or down.

DCNM Connection Status - Indicates whether the DCNM IP address that has been provided is reachable or not to retrieve data. This status field is populated when you click **Submit** after you have entered the required information. **Reachable** is displayed on successful communication with DCNM, and **Unreachable**, in case the connection is unsuccessful.

Create Incident - Select this checkbox in case you need incidents to be raised automatically for alarm events.

User - Create a new user and add the user name in this field. The Caller field in the incidents that are created is populated with this user name. This field is auto-populated as you type. You can also click the search icon next to this field to bring the Users window. You can then select a user from the list that is displayed.

Category - Click the lock icon 🔒 to create incidents automatically for specific categories only.



Incidents will be created for the selec… have 'Critical' status from DCNM.

Select the required category for which incidents have to be created from the drop-down list below the **Category** window. The available categories for creation of incidents are CPU, DEVICE_ACCESS_SNMP,DEVICE_ACCESS_SSH, and MEMORY. Refer the following table for more information on this.

Table 35: Events & Incidents

Category	Data Collection in ServiceNow	Incident Raised	Incident Rule	ServiceNow Incident details

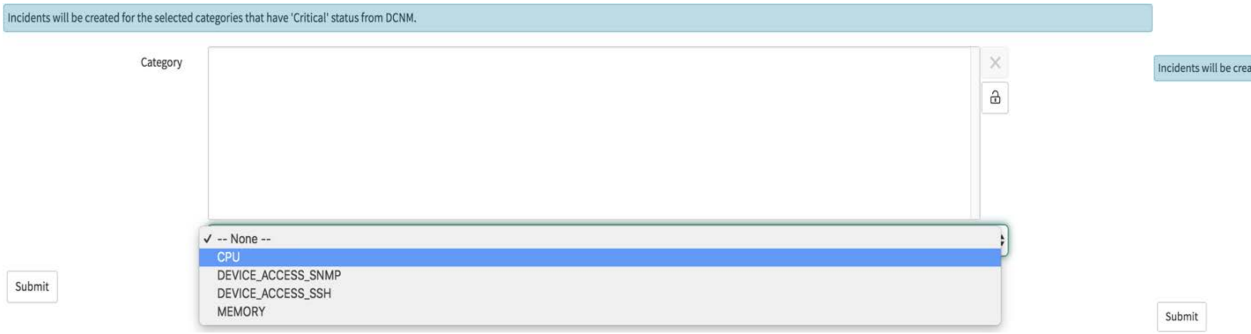
CPU	Yes	Yes	DCNM Alarm severity = 'Critical'	Priority = 2
				Urgency = 2
				Impact = 2

Memory	Yes	Yes	DCNM Alarm severity = 'Critical'	Priority = 2
				Urgency = 2
				Impact = 2

Power	Yes	No	NA	NA
Linkstate	Yes	No	NA	NA
ICMP	Yes	No	NA	NA

SNMP	Yes	Yes	DCNM Alarm severity = 'Critical'	Priority = 2
				Urgency = 2
				Impact = 2

SSH	Yes	Yes	DCNM Alarm severity = 'Critical'	Priority = 2
				Urgency = 2
				Impact = 2

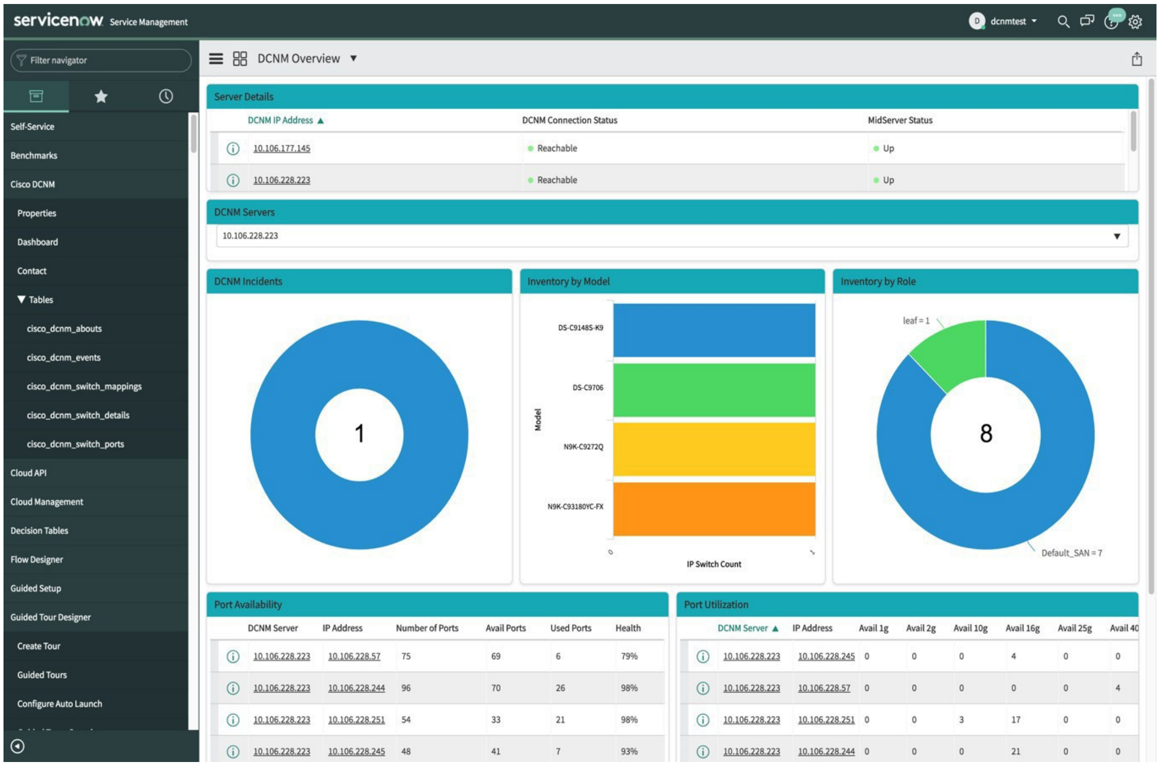


Incidents will be created for the selected categories that have 'Critical' status from DCNM.

Now, click **Submit**.

Viewing the Dashboard

Choose **Cisco DCNM>Dashboard** to display the dashboard. The **DCNM IP Address**, the **DCNM Connection Status** and the **MidServer Status** are displayed at the top of the dashboard.



Server Details

DCNM IP Address ▲	DCNM Connection Status	MidServer Status
10.106.177.145	● Reachable	● Up
10.106.228.223	● Reachable	● Up

DCNM Servers

10.106.228.223 ▼

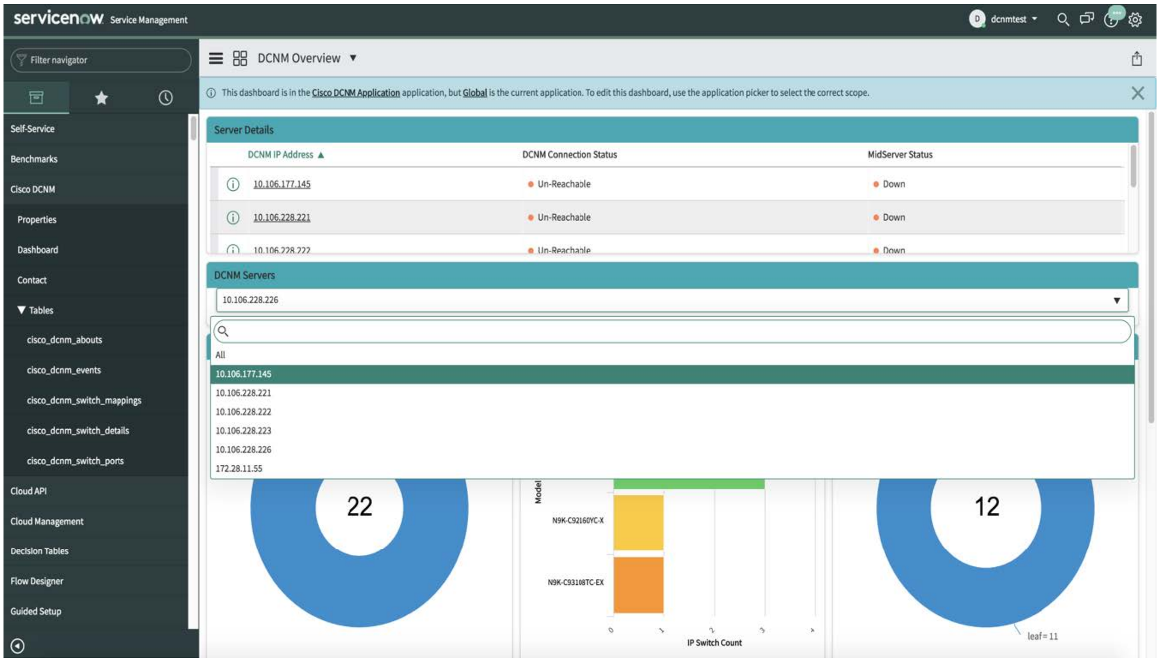
Port Availability

DCNM Server	IP Address	Number of Ports	Avail Ports	Used Ports	Health
10.106.228.223	10.106.228.57	75	69	6	79%
10.106.228.223	10.106.228.244	96	70	26	98%
10.106.228.223	10.106.228.251	54	33	21	98%
10.106.228.223	10.106.228.245	48	41	7	93%

Port Utilization

DCNM Server ▲	IP Address	Avail 1g	Avail 2g	Avail 10g	Avail 16g	Avail 25g	Avail 40
10.106.228.223	10.106.228.245	0	0	0	4	0	0
10.106.228.223	10.106.228.57	0	0	0	0	0	4
10.106.228.223	10.106.228.251	0	0	3	17	0	0
10.106.228.223	10.106.228.244	0	0	0	21	0	0

The **DCNM Servers** section displays the IP address of the DCNM server from which the data is being retrieved and displayed. Click the dropdown list to select any other DCNM server as per your requirement.



This dashboard is in the Cisco DCNM Application application, but Global is the current application. To edit this dashboard, use the application picker to select the correct scope.

Server Details

DCNM IP Address ▲	DCNM Connection Status	MidServer Status
10.106.177.145	● Un-Reachable	● Down
10.106.228.221	● Un-Reachable	● Down
10.106.228.222	● Un-Reachable	● Down

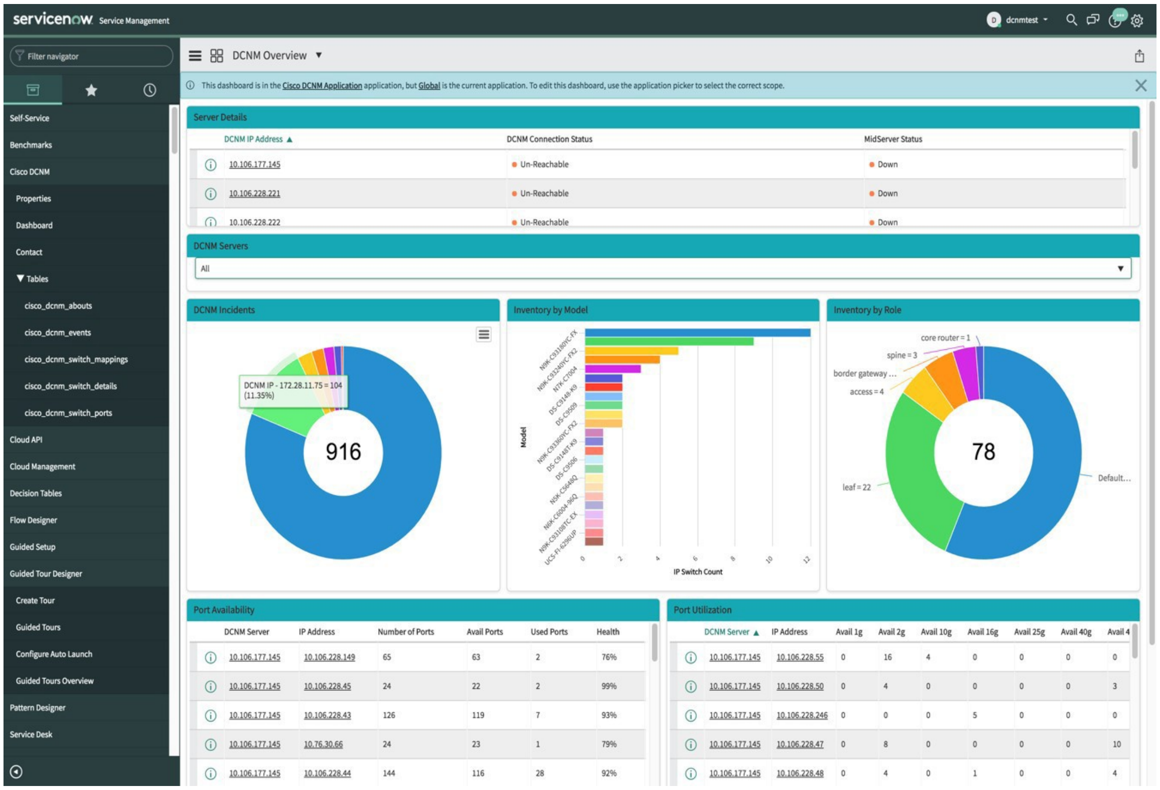
DCNM Servers

10.106.228.226 ▼

All
10.106.177.145
10.106.228.221
10.106.228.222
10.106.228.223
10.106.228.226
172.28.11.55

Click **All** to retrieve and display data from all the DCNM Servers that are displayed in the dropdown list. When the **All** option is selected, the number of incidents that are displayed in the DCNM Incidents donut are color-coded and displayed based on the different DCNM server IP addresses. The Inventory by Model and

Inventory by Role donuts also display data from all the DCNM servers. The Port Availability and Port Utilization donuts display data along with the DCNM Server that each IP address belongs to.



This dashboard is in the Cisco DCNM Application application, but Global is the current application. To edit this dashboard, use the application picker to select the correct scope.

Server Details

	DCNM IP Address ▲	DCNM Connection Status	MidServer Status
ⓘ	10.106.177.145	● Un-Reachable	● Down
ⓘ	10.106.228.221	● Un-Reachable	● Down
ⓘ	10.106.228.222	● Un-Reachable	● Down

DCNM Servers

All ▼

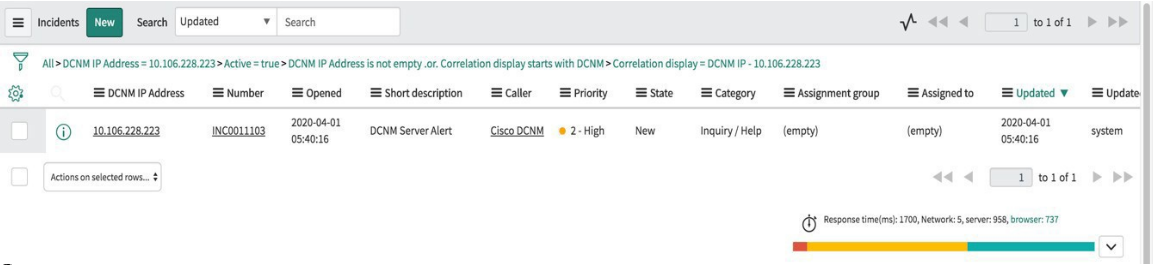
Port Availability

	DCNM Server	IP Address	Number of Ports	Avail Ports	Used Ports	Health
ⓘ	10.106.177.145	10.106.228.149	65	63	2	76%
ⓘ	10.106.177.145	10.106.228.45	24	22	2	99%
ⓘ	10.106.177.145	10.106.228.43	126	119	7	93%
ⓘ	10.106.177.145	10.76.30.66	24	23	1	79%
ⓘ	10.106.177.145	10.106.228.44	144	116	28	92%

Port Utilization

	DCNM Server ▲	IP Address	Avail 1g	Avail 2g	Avail 10g	Avail 16g	Avail 25g	Avail 40g	Avail 4
ⓘ	10.106.177.145	10.106.228.55	0	16	4	0	0	0	0
ⓘ	10.106.177.145	10.106.228.50	0	4	0	0	0	0	3
ⓘ	10.106.177.145	10.106.228.246	0	0	0	5	0	0	0
ⓘ	10.106.177.145	10.106.228.47	0	8	0	0	0	0	10
ⓘ	10.106.177.145	10.106.228.48	0	4	0	1	0	0	4

DCNM Incidents - This displays the number of incidents that have been raised based on the alarms retrieved from DCNM. Click the donut for more details about the

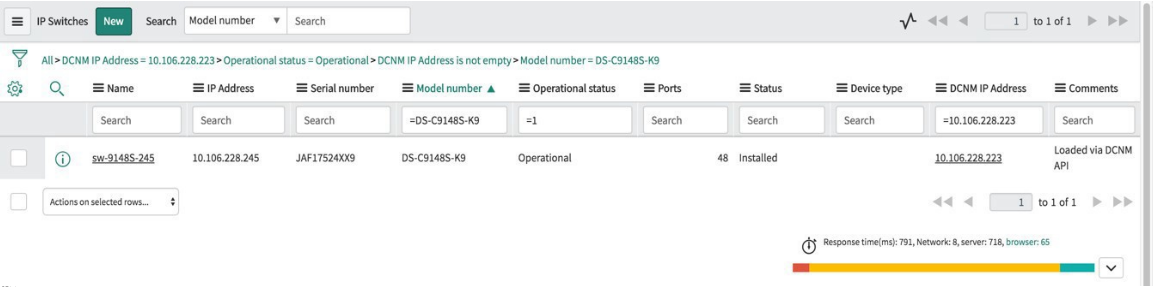


All > DCNM IP Address = 10.106.228.223 > Active = true > DCNM IP Address is not empty .or. Correlation display starts with DCNM > Correlation display = DCNM IP - 10.106.228.223

		DCNM IP Address	Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated ▼	Update
□	ⓘ	10.106.228.223	INC0011103	2020-04-01 05:40:16	DCNM Server Alert	Cisco DCNM	● 2 - High	New	Inquiry / Help	(empty)	(empty)	2020-04-01 05:40:16	system

Response time(ms): 1700, Network: 5, server: 958, browser: 737

Inventory by Model - This displays the number and type of switches present in DCNM. Each band represents a device model. Click a band for more



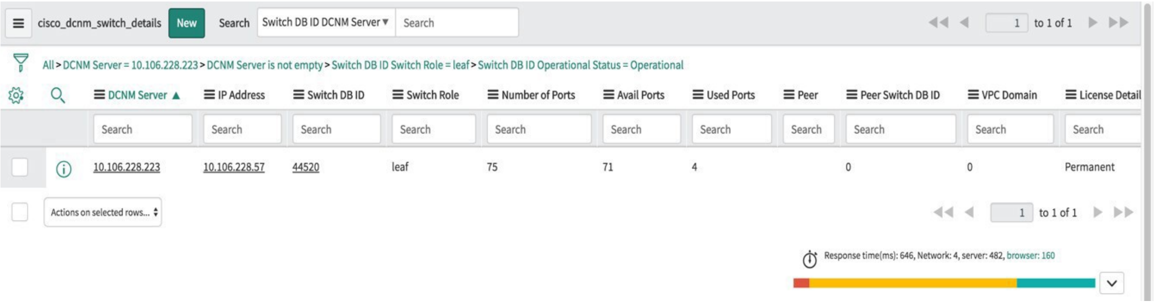
All > DCNM IP Address = 10.106.228.223 > Operational status = Operational > DCNM IP Address is not empty > Model number = DS-C9148S-K9

		Name	IP Address	Serial number	Model number ▲	Operational status	Ports	Status	Device type	DCNM IP Address	Comments
		Search	Search	Search	=DS-C9148S-K9	=1	Search	Search	Search	=10.106.228.223	Search
□	ⓘ	sw-9148S-245	10.106.228.245	JAF17524XX9	DS-C9148S-K9	Operational	48	Installed		10.106.228.223	Loaded via DCNM API

Response time(ms): 791, Network: 8, server: 718, browser: 65

Inventory by Role - This displays the number and types of switch roles present in DCNM. Click the required section to display the number of roles that are operational and click on that pictorial representation to display more details about the roles.

Note The number that is displayed in the Inventory by Role donut does not change in case switches are removed from DCNM. The switches that are removed are displayed as Non Operational and there is no change in the number that is displayed in the donut.



cisco_dcnm_switch_details
New
Search
Switch DB ID DCNM Server ▾
Search
1 to 1 of 1

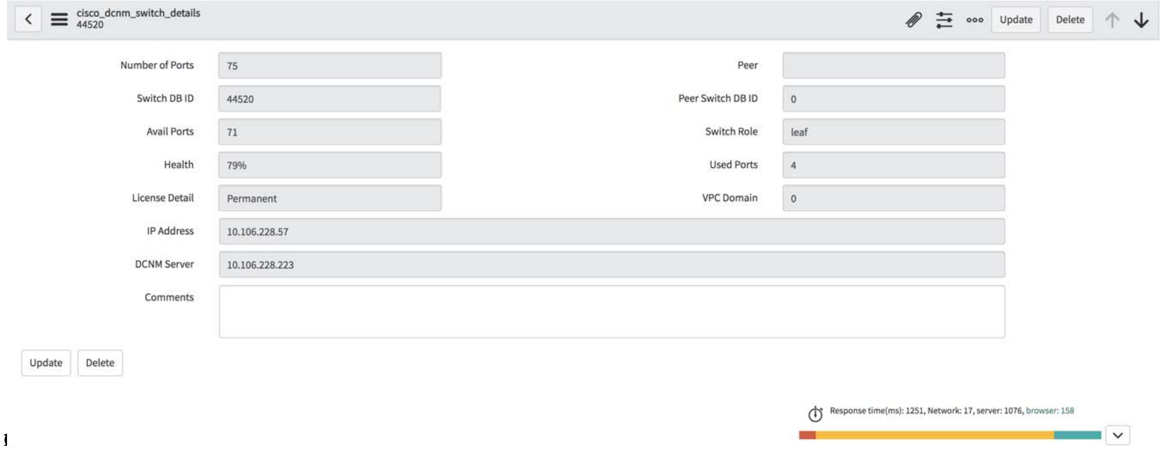
All > DCNM Server = 10.106.228.223 > DCNM Server is not empty > Switch DB ID Switch Role = leaf > Switch DB ID Operational Status = Operational

DCNM Server ▲	IP Address	Switch DB ID	Switch Role	Number of Ports	Avail Ports	Used Ports	Peer	Peer Switch DB ID	VPC Domain	License Detail
10.106.228.223	10.106.228.57	44520	leaf	75	71	4		0	0	Permanent

Actions on selected rows...
1 to 1 of 1

Response time(ms): 646, Network: 4, server: 482, browser: 160

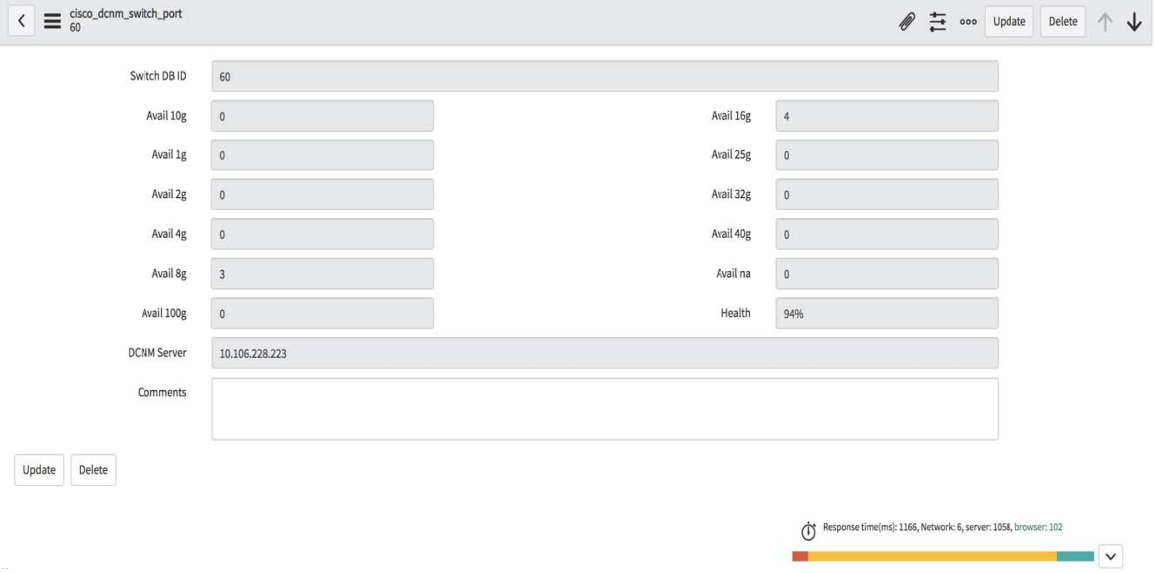
Port Availability - This displays information about port availability. The DCNM server and IP address along with the total number of ports, available ports, used ports and health of the switch is displayed. Click an IP address to display more



Number of Ports	75	Peer	
Switch DB ID	44520	Peer Switch DB ID	0
Avail Ports	71	Switch Role	leaf
Health	79%	Used Ports	4
License Detail	Permanent	VPC Domain	0
IP Address	10.106.228.57		
DCNM Server	10.106.228.223		
Comments			

Response time(ms): 1251, Network: 17, server: 1076, browser: 158

Port Utilization - This displays information about port utilization based on each IP address. The number of ports having 1G, 2G, 4G, 8G, 10G, 16G, 25G, 32G, 40G, and 100G availability, are displayed. Click an IP address to display more

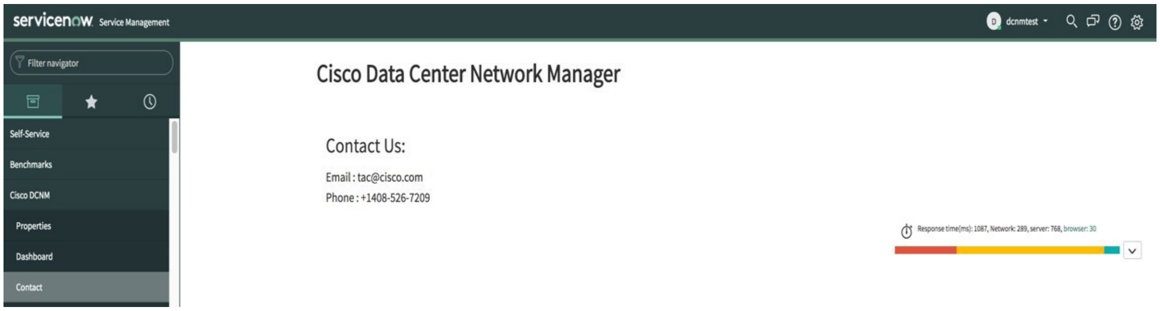


Switch DB ID	60		
Avail 10g	0	Avail 16g	4
Avail 1g	0	Avail 25g	0
Avail 2g	0	Avail 32g	0
Avail 4g	0	Avail 40g	0
Avail 8g	3	Avail na	0
Avail 100g	0	Health	94%
DCNM Server	10.106.228.223		
Comments			

Response time(ms): 1166, Network: 6, server: 1058, browser: 102

Contact Us

Choose **Cisco DCNM>Contact** to display an email address and a telephone number that can be used to contact Cisco Systems for any queries.



Cisco Data Center Network Manager

Contact Us:

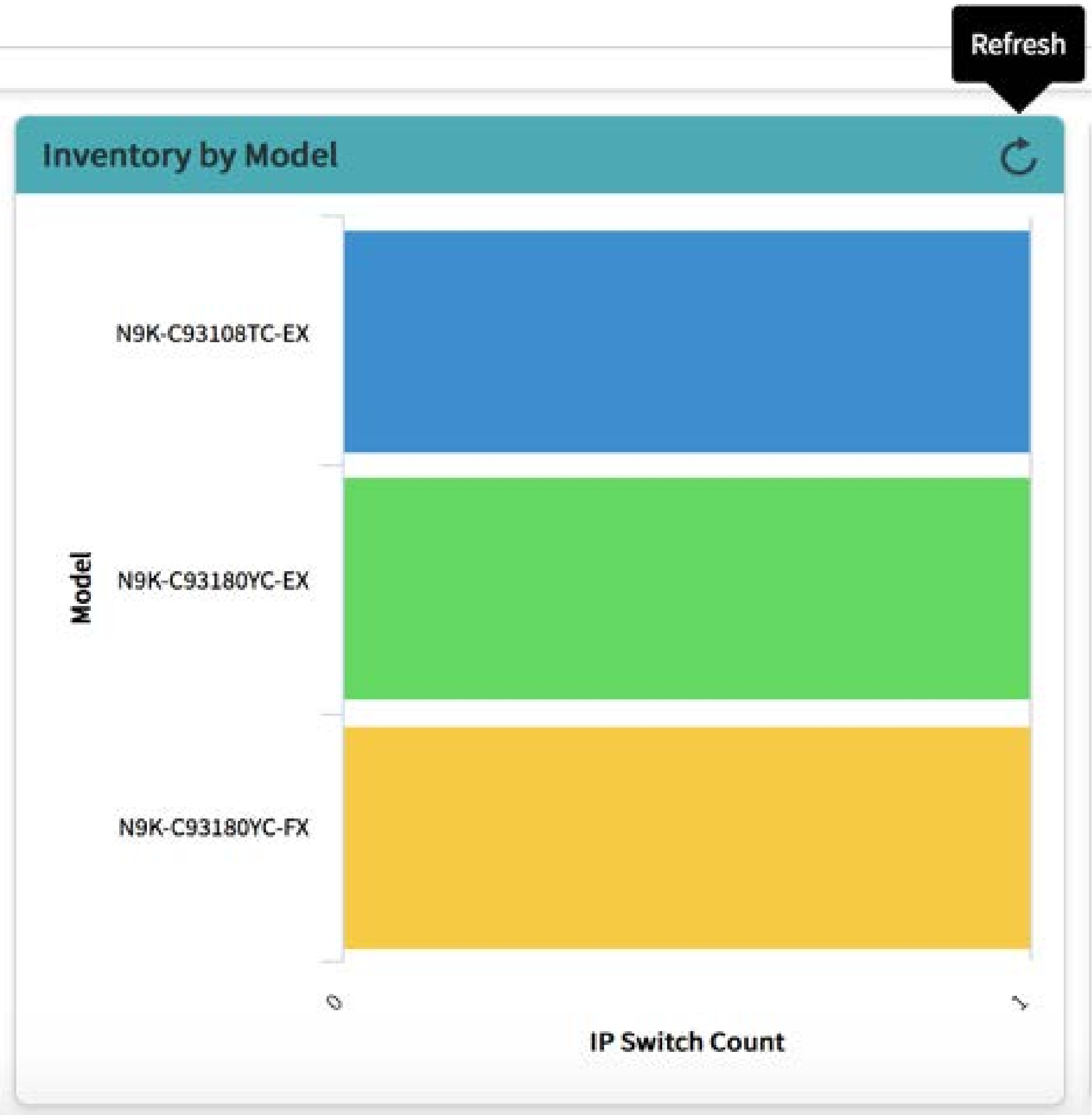
Email : tac@cisco.com
Phone : +1408-526-7209

Response time(ms): 1087, Network: 289, server: 768, browser: 30

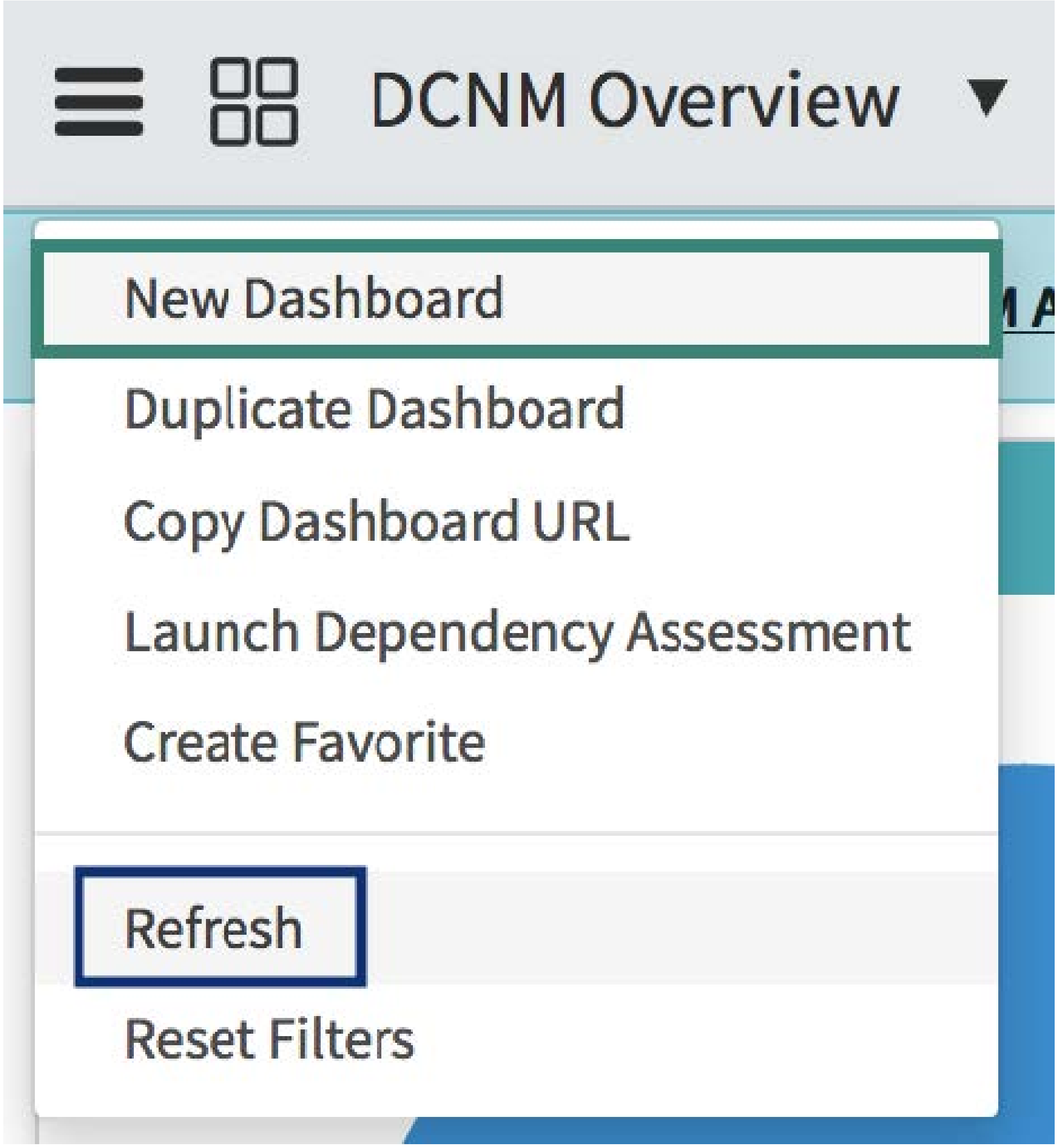
Troubleshooting DCNM Integration with ServiceNow

In case data is not being retrieved in the ServiceNow table:

- Check if the MID server is up or down.
- Check for information entries in system logs with the source “x_caci_cisco_dcnm”.
- Check the login credentials added in Cisco DCNM Properties.
- Consider a scenario in which data is being displayed on the ServiceNow dashboard for the selected DCNM server and then you want to display data for another DCNM server. In such a scenario, the ServiceNow dashboard may take some time to load data from the other DCNM server due to a delay in refreshing the cache. To refresh the data manually, click the **Refresh** icon that appears on the top right corner of the individual tiles when you hover the cursor over the tiles.



You can also refresh the whole dashboard by clicking on the **Dashboard Controls** icon ≡ and then clicking **Refresh** to load the reports correctly.



For more information on DCNM application integration with ServiceNow, click here.