

Cisco NDFC-SAN Controller Configuration Guide, Release 12.1.1e

First Published: 2022-07-07

Last Modified: 2022-12-16

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Overview** 1

Know your Web UI 1

CHAPTER 2 **New and Changed Information** 3

New and Changed Information 3

CHAPTER 3 **Dashboard** 5

Overview 5

Host 7

Viewing Host Enclosures 9

Viewing CPU & Memory and Disk I/O Charts 9

Storage 10

Viewing Storage Enclosure 11

SAN Insights 12

Viewing SAN Insights 12

Viewing Custom Graphing 15

Viewing Custom Graph and Table 16

Monitoring Metrics 17

Viewing IT Pairs 19

CHAPTER 4 **Topology** 21

Searching Topology 22

Viewing Topology 22

Viewing Elements in SAN Topology 23

Zooming, Panning, and Dragging 24
Layouts 25
Status 25

PART I SAN 27

CHAPTER 5 Fabrics 29
Fabrics 29
Adding a Fabric 30
Editing a Fabric 31
Deleting a Fabric 32
Rediscovering a Fabric 32
Purging a Fabric 32
Configuring Performance 33
SAN Insights 33
Prerequisites 34
Configuring Persistent IP Address 34
Guidelines and Limitations 35
Server Properties for SAN Insights 35
Configuring SAN Insights 37
Configuring Fabric Backup 43
Golden Backup 44
Fabric Overview 45
Fabric Summary 45
Switches 45
Modules 46
Viewing Interface 47
VSANs 48
Default VSAN Settings 49
Create VSAN Wizard 50
Delete VSAN 53
Field and Descriptions for VSANs 53
Device Aliases 58
Configuring Device Aliases 58

CFS 60
Event Analytics 61
Performing Backup actions 61
Viewing of Port Usage 62
Metrics 63
Congestion Analysis 64
Congestion Visualization 65
DIRL 66
DIRL Congestion Management Visualization 67
Rate Limit Events 68

CHAPTER 6 Switches 71
Switches 71
Device Manager 72
Tech Support 72
Execute CLI 72
Enhanced Role-based Access Control 73
Nexus Dashboard Security Domains 77
Switch Overview 79
Viewing Switch Summary 79
Modules 79
Viewing Interface 80
Viewing Switch Licenses 81
Event Analytics 82
Viewing Backup 82
Copy Bootflash 83
Compare Configuration Files 83
Export Configuration 84
Viewing of Port Usage 85
Viewing Bootflash 85
Device Manager 85
Blades 85

CHAPTER 7 SAN Links 87

SAN Links 87
ISL and Port Channels 87
Configuring FCIP 87
Port Channels 89
Create Port Channel Wizard 101
Edit Existing Port Channel 102
NPV Links 103

CHAPTER 8 Interfaces 105
Interfaces 105
FC Ports 105
Viewing Inventory Information for FC Ports 105
Viewing Performance Information for FC Ports 106
Viewing Transceiver Information for FC Ports 107
Viewing FC FICON Ports 108
Viewing Performance Information for Ethernet Ports 109
Viewing Performance Information for Port Groups 110
Port Group Member 110
Viewing Performance Information for Optics 111
Custom Port Groups 112
Viewing Performance of Custom Port Groups 112
Configuring Custom Port Groups 113

CHAPTER 9 End Devices 115
Devices 115
Enclosures 116
Inventory 116
Inventory – Host Enclosures 116
Inventory – Storage Enclosures 118
Performance 119
Performance – Host Enclosures 119
Performance – Storage Enclosures 119
Enclosure Members 120

CHAPTER 10 **Host Path Redundancy** 121
Host Path Redundancy 121
Diagnostic Test 121
Hostpath Errors 122
Ignored Host 123
Ignored Storage 123
Ignored Host Storage Pair 123

CHAPTER 11 **Port Monitoring** 125
Port Monitoring Policy 125
Configuring SFP Counters 130

CHAPTER 12 **Active Zones** 133
Regular Zones 133
IVR Zones 134

CHAPTER 13 **Storage** 135
Storage Arrays 135
storageName Enclosure 135
Storage SMI-S Provider 136
Adding SMI-S Provider 138

PART II **Virtual Management** 139

CHAPTER 14 **Zoning** 141
Zoning 141
Enhanced Zoning 143
CFS 144
Zonesets 146
Zones 148
FC Aliases 149
Members 150

CHAPTER 15 **Virtual Infrastructure Manager** 153
Virtual Infrastructure Manager 153
Support for Cisco UCS B-Series Blade Servers 154
Configuring Routes IP Address 155
Adding vCenter Visualization 156

PART III **Settings** 159

CHAPTER 16 **Server Settings** 161
Server Settings 161

CHAPTER 17 **Feature Management** 163
Feature Management 163
Choosing Feature Set 163
Features with each Persona 164
Changing across Feature-Set 165

CHAPTER 18 **Credentials Management** 167
SAN Credentials Management 167

PART IV **Operations** 169

CHAPTER 19 **Event Analytics** 171
Alarms 171
Alarms Raised 171
Alarms Cleared 172
Monitoring and Adding Alarm Policies 173
Create new alarm policy 175
Events 181
Event Setup 182
Accounting 185
Remote Clusters 186

CHAPTER 20 **Image Management** 187

Image Management 187

Overview 188

Staging an Image 188

Validating an Image 189

Upgrading an Image 190

Modifying a Policy 191

Recalculating Compliance 192

Images 192

Uploading an Image 194

Image Policies 195

Creating an Image Policy 195

History 196

CHAPTER 21 **Programmable Reports** 199

Create Report 200

Report Templates 201

Report Definitions 201

Reports 203

CHAPTER 22 **License Management** 205

Overview 205

NDFC Server Licenses 206

Smart Licensing 207

Switch Licenses 210

Smart Licensing using Policy to Establish Trust with CSSM 211

Switch License Files 212

Adding Switch License Files 213

CHAPTER 23 **Templates** 215

Templates 215

Creating a New Template 218

Editing a Template 219

Importing a Template 220
Installing POAP Templates 221
Template Structure 221
Template Format 222
Template Variables 228
Variable Meta Property 230
Variable Annotation 237
Templates Content 240
Advanced Features 242
Report Template 244

CHAPTER 24 Backup and Restore 247
Scheduler 248
Restore 249
Backup Now 251

CHAPTER 25 NXAPI Certificates 253
Certificate Generation and Management 253
Switch Certificates 254
CA Certificates 256

PART V Service Integration 259

CHAPTER 26 One View Dashboard 261
One View Dashboard 261

CHAPTER 27 Device Manager 263
Device Manager 263
Physical 263
Inventory 263
Modules - Status and Config 263
Power Supplies 264
Temperature Sensors 265
Fan 265

Switches 265
ISLs 266
NP Link 267
ISL's Statistics 267
Hosts 268
Enclosures 268
Device Manager - Preferences 269
Interface 269
Virtual Interface Groups 269
Virtual FC Interfaces 270
Ethernet Interfaces 271
Virtual FC Ethernet 272
Quick Configuration Tool 272
Ethernet Interface 273
Ethernet Interfaces iSCSI 274
Ethernet Interfaces iSCSI TCP 275
Ethernet Interfaces VLAN 275
Ethernet VLAN 276
FC Interface Monitor Traffic 276
FC Interface Monitor Protocol 277
FC Interface Monitor Discards 277
FC Interface Monitor Link Errors 278
FC Interface Monitor Frame Errors 278
FC Interface Monitor Class 2 Traffic 279
FC Interface Monitor Class 2 Errors 279
FC Interface Monitor FICON 279
Check Oversubscription 279
Virtual FC Interface Monitor Traffic 280
Virtual FC Interface Monitor Discards 280
Virtual FC Interface Monitor Errors 280
Ethernet Interface Dot3Stats 280
Interface Monitor 281
Ethernet PortChannels 282
Ethernet Interface Monitor iSCSI Connections 282

Ethernet Interface Monitor TCP 282
FCIP Monitor 283
Monitor SVC Interface 283
Monitor SVC NPorts 284
Monitor SVC Session FCP 284
Monitor SVC Session Other 285
FCIP Interfaces 285
System Timeout 286
Interface License 286
General 287
FC Interfaces General 287
FC Interfaces Rx BB Credit 289
FC Interfaces Other 290
FC Interfaces FLOGI 290
FC Interfaces ELP 291
FC Interfaces Trunk Config 293
FCIP Interfaces Trunk Failures 293
FC Interfaces IP 293
FC Interfaces Physical 294
FC Interfaces Capability 294
FC Interfaces FICON Peer 295
Interfaces NPorts (SVC) 295
Interfaces Sessions 296
IP Statistics TCP 296
Port Channels Ethernet Interfaces 296
Port Channels FC Interfaces 297
Port Channels General 297
FlexAttach Global 298
FlexAttach Virtual PWWN 298
FlexAttach Physical to Virtual WWNs 299
FIPS 299
FCIP FICON Configuration 299
Port Channels AutoCreate 300
SPAN Sessions 300

Span Global 300
SPAN Source Interfaces 300
Port Tracking Dependencies 300
Port Tracking Force Shut 301
Port Guard 301
Bandwidth Reservation: 48-Port 96-Gbps Fibre Channel module 301
Bandwidth Reservation: 48-Port 48-Gbps Fibre Channel module 301
Bandwidth Reservation: 24-Port 48-Gbps Fibre Channel module 302
Bandwidth Reservation: 48-Port 256-Gbps Fibre Channel module 302
Bandwidth Reservation: 32-Port 256-Gbps Fibre Channel module 303
DS-X9448-768K9 (Luke) Line Card Bandwidth Reservation 303
FC 303
VSAN General 303
VSAN Membership 304
VSAN Interop-4 WWN 304
VSAN Timers 305
VSAN Default Zone Policies 305
IVR Local Topology 305
IVR Fabric ID 305
IVR Default Fabric ID 305
IVR Action 306
IVR RDI VSANs 306
IVR Active Topology 306
IVR Zoneset Status 306
IVR Discrepancies 307
IVR Domains 307
IVR FCID 308
IVR Zoneset Active Zones 308
IVR Zoneset Active Zones Attributes 308
IVR Zoneset Name 308
DPVM Actions 309
DPVM Config Database 309
DPVM Active Database 310
Domain Manager Running 310

Domain Manager Configuration 310
Domain Manager Domains 312
Domain Manager Statistics 312
Domain Manager Interfaces 312
Domain Manager Persistent FcIds 313
Domain Manager Allowed DomainIds 313
Zoneset Active Zones 313
Zoneset Unzoned 313
Zoneset Status 314
Zoneset Policies 314
Zoneset Active Zones Attributes 315
Zoneset Enhanced 315
Zoneset Read Only Violations 316
Zoneset Statistics 316
Zoneset LUN Zoning Statistics 316
Zoneset Members 317
Fabric Config Server Discovery 317
Fabric Config Server Interconnect Elements 317
Fabric Config Server Platforms (Enclosures) 318
Fabric Config Server Fabric Ports 318
FC Routes 318
FDMI HBAs 319
FDMI Ports 319
FDMI Versions 319
Flow Statistics 320
FCC 320
Diagnostics 320
FSPF General 321
FSPF Interfaces 321
FSPF Interface Stats 322
SDV Virtual Devices 323
SDV Real Devices 323
LUN Discover 324
LUN Targets 324

LUNs 324
Device Alias 325
Device Alias Configuration 325
Device Alias Mode 325
Device Alias Discrepancies 325
Name Server General 325
Name Server Advanced 326
Name Server Proxy 326
Name Server Statistics 326
Preferred Path Maps and Routes 327
Preferred Path Maps Active 327
Preferred Path All Match Criteria 327
Preferred Path Active Match Criteria 328
Preferred Path All Sets 328
RSCN Nx Registrations 329
RSCN Multi-PID Support 329
RSCN Event 329
RSCN Statistics 329
Multicast Root 330
QoS Policy Maps 330
QoS Class Maps 330
QoS Match Statements 330
QoS Class Maps by Policy Maps 330
QoS Policy Maps by VSAN 331
QoS DWRR 331
QoS Rate Limit 331
Timers and Policies 331
WWN Manager 332
NPV Traffic Map 332
NPV Load Balance 333
NPV External Interface Usage 333
NP Link 333
FCoE 333
Config 333

VSAN-VLAN Mapping 334
VLAN-VSAN Mapping 334
FCoE Statistics 334
Ficon 335
FICON VSANs 335
FICON VSANs Files 336
Global 336
FICON Port Attributes 336
FICON Port Configuration 337
FICON Port Numbers 337
FICON VSANs Director History 338
Fabric Binding Actions 338
Fabric Binding Config Database 339
Fabric Binding Active Database 339
Fabric Binding Database Differences 339
Fabric Binding Violations 339
Fabric Binding Statistics 340
Fabric Binding EFMD Statistics 340
IP Storage 341
FCIP Profiles 341
FCIP Tunnels 342
FCIP Tunnels (Advanced) 342
FCIP Tunnels (FICON TA) 343
FCIP Tunnels Statistics 343
FCIP XRC Statistics 343
iSCSI Connection 344
iSCSI Initiators 344
iSCSI Session Initiators 345
Module Control 345
iSCSI Global 345
iSCSI Session Statistics 346
iSCSI Targets 346
iSCSI iSLB VRRP 347
iSCSI Initiator Access 347

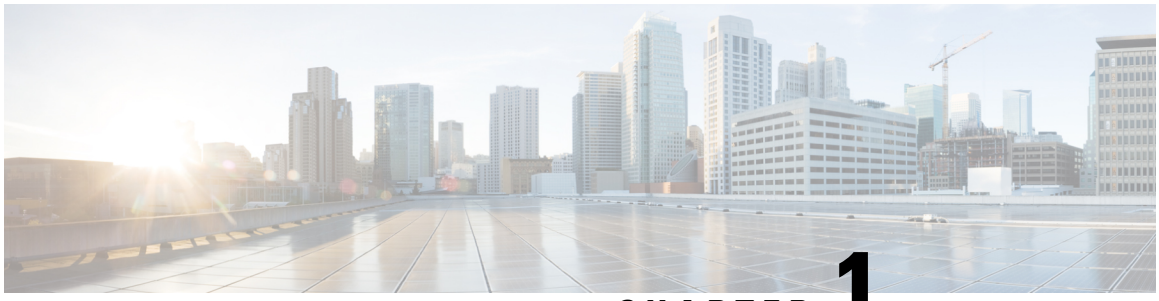
Initiator Specific Target 347
iSCSI Initiator PWWN 348
iSCSI Sessions 348
iSCSI Sessions Detail 348
IP Services 349
IP Routes 349
IP Statistics ICMP 349
IP Statistics IP 350
IP Statistics SNMP 351
IP Statistics UDP 353
mgmt0 Statistics 353
TCP UDP TCP 353
TCP UDP UDP 353
VRRP General 353
VRRP IP Addresses 354
VRRP Statistics 354
CDP General 355
CDP Neighbors 355
iSNS Profiles 356
iSNS Servers 356
iSNS Entities 357
iSNS Cloud Discovery 357
iSNS Clouds 357
iSNS Cloud Interfaces 357
Monitor Dialog Controls 357
iSNS Details iSCSI Nodes 358
iSNS Details Portals 359
Security 359
Security Roles 359
Security Role Rules 359
Feature Group Manager 360
AAA LDAP Servers 360
AAA Server Groups 361
AAA Search Map 361

AAA Applications 361
AAA Defaults 362
AAA General 362
AAA Statistics 363
iSCSI User 365
Common Roles 365
SNMP Security Users 366
SNMP Security Communities 366
Security Users Global 366
FC-SP General/Password 367
FC-SP Interfaces 367
FC-SP Local Passwords 368
FC-SP Remote Passwords 368
FC-SP Statistics 368
FC-SP SA (Security Association) 368
FC-SP ESP Interfaces 368
PKI General 369
PKI RSA Key-Pair 369
PKI Trust Point 369
PKI Trust Point Actions 370
PKI LDAP 371
PKI Certificate Map 371
PKI Certificate Map - Application 371
PKI Trust Point Detail 371
IKE Global 372
IKE Pre-Shared AuthKey 373
IKE Policies 373
IKE Initiator Version 373
IKE Tunnels 373
IPSEC Global 374
IPSEC Transform Set 374
IPSEC CryptoMap Set Entry 374
IPSEC Interfaces 375
IPSEC Tunnels 375

IP ACL Profiles 375
IP ACL Interfaces 376
IP Filter Profiles 376
SSH/Telnet 377
Port Security Actions 378
Port Security Config Database 379
Port Security Active Database 379
Port Security Database Differences 380
Port Security Violations 380
Port Security Statistics 380
IPsec 381
Events 381
Call Home General 381
Call Home Destinations 381
Call Home Email Setup 381
Call Home Alerts 382
Call Home HTTP Proxy Server 382
Call Home SMTP Servers 383
Call Home User Defined Command 383
Delayed Traps 383
Call Home Profiles 383
Event Destinations Addresses 383
Event Destinations Security (Advanced) 384
Event Filters General 384
Event Filters Interfaces 385
Event Filters Control 385
Link Incident History 385
RMON Thresholds Controls 386
RMON Thresholds 64bit Alarms 386
RMON Thresholds 32bit Alarms 387
RMON Thresholds Events 388
RMON Thresholds Log 388
Admin 388
Copy Configuration 388

Flash Files 389
Compact Flash 389
License Features 389
License Manager Keys 389
License Manager Install 390
License Manager Usage 391
Port Licensing 391
Feature Set 392
Feature Control 392
NTP Servers 392
NTP General 393
Running Processes 393
Show Startup/Running Config 393
Show EPLD Version 393
Copy Flash Files 394
Generate TAC Pac File 394
Show Tech Support 395
Show Image Version 395
Show Onboard Log 395
Summary View 395
RLIR ERL 396
Preferred Host 397
Preferred Path 397
Edit iSCSI Advertised Interfaces 397
DNS General 397
DNS Servers 398
Cisco Fabric Services (CFS) Features 398
Cisco Fabric Services (CFS) IP Multicast 399
Cisco Fabric Service (CFS) IP Static Peers 400
Cisco Fabric Services (CFS) Feature by Region 400
Cisco Fabric Services (CFS) All Region 400
Cisco Fabric Services (CFS) Owner 400
Cisco Fabric Services (CFS) Merge 400
Logs 401

SysLog (Since Reboot) 401
SysLog (Severe Events) 401
Accounting Log 401
Switch Logging 402
Syslog Severity Levels 402
Syslog Servers 402
End Devices - Hosts 402
Intelligent Features – Summary 403
Data Mobility Manager – Modules 403
Storage Media Encryption 404
Members 404
Interfaces 404
Hosts 404
SSM Features 405
Summary 405
FCWA 405
SSM 406
MSM 406
SANTap CVT 406
SANTap DVT 406
NASB 407
NASB Target 407
Virtual Initiator 407
DMM Rate 407
FCWA Config Status 408
Statistics Status 408
Statistics I/O Traffic 408
Statistics I/O Traffic Details 408
Statistics SCSI Commands 409
Statistics SCSI Errors 409
Statistics SCSI Sense Errors 409
Compact 410



CHAPTER 1

Overview

- Know your Web UI, on page 1

Know your Web UI

When you launch the Cisco Nexus Dashboard Fabric Controller Web UI for the first time, the **Feature Management** window opens. After you choose a deployment type, the left pane displays menu relevant to the personality.

The top pane displays the following UI elements:

- **Home** icon – Click to view One view on the Nexus Dashboard setup.
- **Nexus Dashboard** – Click to view One view on the Nexus Dashboard setup.
- **Help** – Click on **Help** to see a drop-down list with the following options:
  - **About Nexus Dashboard** – Displays the version of the Cisco Nexus Dashboard on which Cisco Nexus Dashboard Fabric Controller is deployed.
  - **Welcome Screen** – Displays What's New information. You can choose to see this page every time you launch the Web UI.
  - **Help Center** – Click to view the Help Center page. You can access various product documents from this page.

    Scroll to the end of the page to view the services installed on Nexus Dashboard. Click on the Service to view **Help Center**.

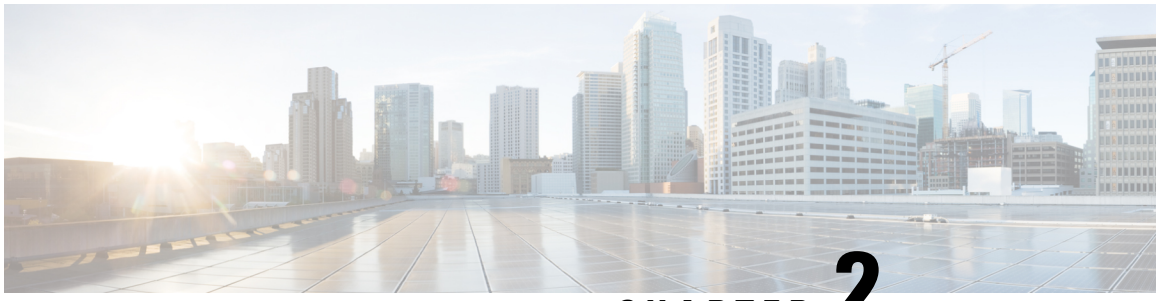
- **User Role** – Displays the role of the user who is currently logged in, for example, **admin**. Click on the username to see a drop-down list with the following options:
  - **User Preferences** – Allows you to view the Welcome screen on every login.
  - **Change Password** – Allows you to change the password for the current logged-in user.

    If you are a network administrator user, you can modify the passwords of other users.
  - **Manage API Keys** – Click to manage API keys. Click on **Add API Key** to generate API key. Click on **Edit** icon to provide **Name** and modify **API Key**. Click **Save**.
  - **Logout** – Allows you to terminate the Web UI and return to the login screen.

- **Cisco Nexus Dashboard Fabric Controller Persona** – Specifies the deployment persona – **Fabric Controller** or **SAN Controller** or **Fabric discovery**.
- **View Alarms** – Click the bell icon to view the **Alarms**. You can also view this page from **Operations > Event Analytics > Alarms** from the left pane.
- **Help** icon – Click to view help pages or information about Cisco NDFC.
  - Select **Help** to view the context-sensitive help for the UI page.
  - Select **About NDFC** to view the version number and copyright information.

General icons on UI:

- **Hamburger** icon – Click on **Hamburger** icon adjacent to product name on home screen to minimize the menu items on home screen or to view menu items in details.
- **Refresh** icon – Click refresh icon to refresh and load screen.



CHAPTER 2

New and Changed Information

- New and Changed Information, on page 3

New and Changed Information

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features in this release.

The following tables provide information about the new and changed features in Cisco NDFC.

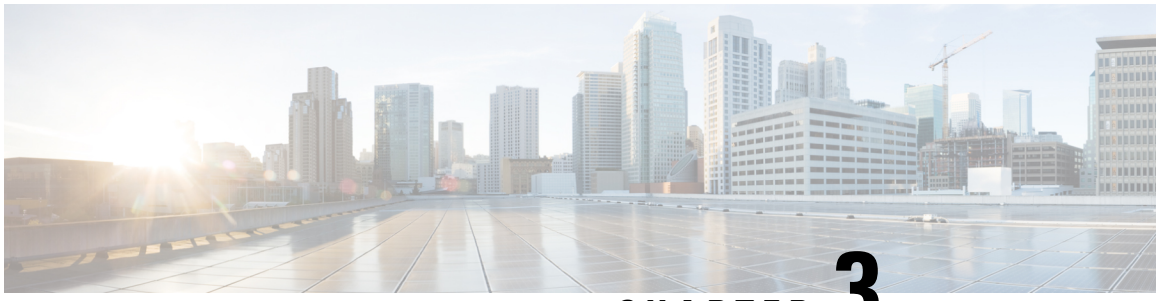
Table 1: New and Enhanced features for all personas in NDFC Release 12.1.1e

Feature	Description	Where Documented
Support NDFC with Nexus Dashboard on KVM	NDFC can be installed on virtual Nexus Dashboard cluster running on top of KVM hypervisor. This is supported for Fabric Controller, Fabric Discovery and SAN Controller modes.	Cisco Nexus Dashboard Deployment Guide

Table 2: New and Enhanced features in SAN Fabrics in Cisco NDFC Release 12.1.1e

Feature	Description	Where Documented
NDFC delivered on RHEL for SAN deployments	Nexus Dashboard can be deployed on Red Hat Enterprise Linux and allows you to install NDFC SAN Controller persona.	Cisco Nexus Dashboard Deployment Guide
DIRL Congestion Management Visualization	Beginning from Release 12.1.1e, NDFC provides visualization of DIRL information to highlight congestion points within a SAN fabric.	DIRL, on page 66

Feature	Description	Where Documented
One View for multiple SAN Controllers	This feature provides a single pane of glass for multiple NDFC SAN Controller instances. It provides information about the status of switches, ports, and fabrics across multiple controllers.	One View Dashboard, on page 261
Interface to execute CLI Commands	With this release, NDFC provides an interface to execute CLI commands on multiple Cisco MDS 9000 Series Switches simultaneously.	Execute CLI, on page 72
Smart Licensing using Policy support for Cisco MDS 9000 Series Switches	NDFC allows you to discover Cisco MDS 9000 Series Switches that are configured with Smart Licensing using Policy.	Smart Licensing using Policy for Cisco NDFC
Endpoint Visibility	You can now view transceiver information in Fibre Chanel interfaces.	Viewing Transceiver Information for FC Ports, on page 107
Enhancement to SAN Insights	• Enhanced SAN Insights scale now supports up to 500K ITLs/ITNs. • Support for SAN Insights for 64G modules	Fabrics, on page 29



CHAPTER 3

Dashboard

The intent of the **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 various scopes that are available on the Cisco SAN Controller Web UI are:

- Overview, on page 5
- Host, on page 7
- Storage, on page 10
- SAN Insights, on page 12

Overview

By default, a subset of the available dashlets are automatically displayed in the **Overview** of dashboard.

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

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

Dashlet	Description
Fabrics	Displays details of Fabrics such as name, state, and health status of the fabric. To view more information about the fabric, click the fabric name (link) to open the **Fabric** slide-in pane. Click the **Launch** icon. Alternatively, double-click the fabric name. The **Fabric Overview** window appears.
Event Analytics	Displays events with **Critical**, **Major**, **Minor**, and **Warning** severity. Click the severity level or the sectors on the pie chart to view more information about the severity of events and alarms in the **Event Analytics** window.
Links	Displays a diagram of Inter-Switch Link (ISL) and NPV Links for transmitting and receiving in the data

Dashlet	Description
	center. Click the sectors on the pie chart to view more information in the **SAN Links** window.
Switches	**Switch Health** - Displays the switch's health status in the form of chart with colors and health condition names with total number of switches in the brackets. 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. **Switch Status** - Displays the status of the switch. **Switch Release Versions** - Displays the switch release versions. **Switch Models** - Displays the models of switches. Click the sectors on the pie chart, the severity, status, versions, or the models to view more information in the **Switches** window.
Modules	Displays the switches on which the modules are discovered, the models name and the count.
Port Usage	Displays the ports inventory summary information.
Performance Collector	Displays the performance collection information. • Click **Stop collector** to stop performance collection information. • Click **Start collector** to restart the performance collection information.
Top ISL	Displays data for top 10 performing ISLs. Each entry shows device name, specifies the average of Rx traffic and Tx traffic in percentage. Click the **chart** icon next to the device name to view more details.

Dashlet	Description
Top SAN End Ports	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. Click the **chart** icon next to the device name to view more details.
TOP FICON End Ports	Displays data for top 10 performing FICON host and control unit 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. Click the **chart** icon next to the device name to view more details.
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. Click the **chart** icon to view more details.
TOP Optics	Displays data for top 10 optics. You can sort optics by hotest SPFs, coldest SPFs, lowers Rx Power, and lowest Tx Power. Click the **chart** icon next to the switch interfaces view more details.
TOP CPU/Temperature	Displays the data for top CPU and temperature details of switches. Click the **chart** icon next to the switch to view more details.
TOP Error And Discard	Displays the top error packets that are discarded for the selected interface. Click the **chart** icon to view more details.

Host

UI Path: **Dashboards** > **Host**

Host dashboard provides information that is 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 **Host** dashboard consists of four panels:

- **Enclosures** panel - Lists the hosts and their network attributes.
  - The **Host Enclosure Name** column lists all the hosts.

    Click **i** icon for relevant host enclosure to view the **SAN Insights Monitor** page. See Monitor Metrics for more information.

    Click the host name to view the summary information of a host.
  - **Member WWNs** displays the World-Wide Name of the member devices. It is a 64-bit identifier and is unique world-wide.
  - **#VMs** displays SAN host VM details. Click **#VMs** to view the **SAN Host VM Screen** and **Enclosures** information.
- **Traffic Chart** — Provides the I/O statistics, CPU and memory information, and disk latency of individual hosts or virtual machines.
- **Events Table** — Provides information about events of all the switch ports that are configured within a specific host enclosure.
- **Topology** - 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 the data paths.

Click a **Host Enclosure Name** to display a slide-out panel that displays the following details about the host device. The details displayed may vary depending on the device type.

Field	Description
IP Address	Displays the IP address of the switch.
MAC Address	Displays the MAC addresses.
WWN	Displays the port WWN.
FCIDs	Specifies the associated FCID.
OS Version	Displays the OS details.
#VMs	Displays the number of VMs.
VHost Name	Displays the name of the virtual host.
VHost IP	Displays the name of the virtual host IP Address.
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 NDFC using SAN Insights.

Note 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.

Viewing Host Enclosures

To view the host enclosures from the SAN Controller 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 on **i** icon of host enclosure.

The **SAN Insights Monitor** window appears.

Step 3 On **SAN Insights Monitor** window, click on required host name.

The Host enclosure slide-in pane appears.

Step 4 Click on **Launch** icon to view Host Enclosure page.

The Host Enclosure window appears.

The Host Enclosure window displays the Initiator-Target (IT) pairs, Topology, average ECT/DAL/read/write times, and Switch Interface for the selected host.

- **Initiator Target Pairs** - 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.
- **Topology** - Provides an end-to-end topology layout and path information between host enclosures. On **View** card click **+** or **-** to zoom-in and zoom-out. Similarly, you can use the mouse scroll wheel to zoom-in and zoom-out. Click **Refresh** icon to refresh the topology view. Choose **Select layout** drop-down list to view topology. This can be either **Hierachical** or **Hierachical Left-Right** view .
- The first table in below row shows the details of all metrics on ECT/DAL/read/write times, active I/Os, IOPS, Throughput, etc. along with their 1-hour average and the baseline information.
- **Switch Interface** - Click on topology to view associated switch name and the interface name in the last row in table.

Viewing CPU & Memory and Disk I/O Charts

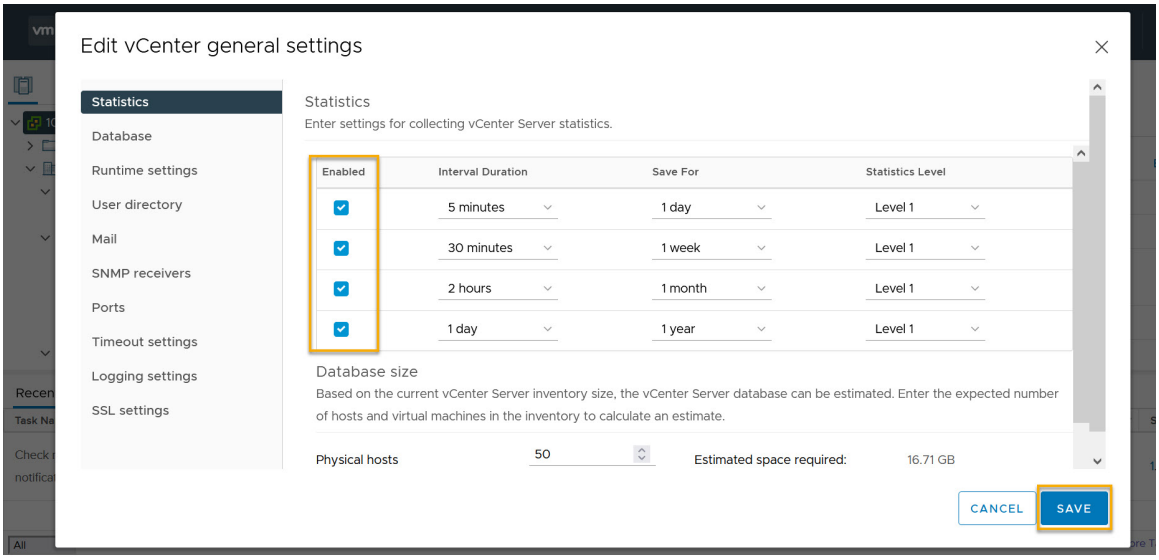
To view the SAN host enclosures from the NDFC SAN Controller Web UI, perform the following steps:

Before you begin

To view VM charts for **CPU & Memory** and **Disk I/O**, you must edit vCenter settings on the vSphere vCenter and enable statistics manually.

To enable statistics manually on the vSphere vCenter, perform the following steps:

1. Login to vSphere vCenter. (Click on the appropriate **Host**.)
2. Click **Configure** > **EDIT**. The **Edit vCenter general settings** screen appears.
3. On **Statistics** tab, check all the check boxes and click **SAVE**.



Procedure

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

The list of hosts in the Enclosures table is displayed.

Step 2 Click the host name.

The **Host** slide-in pane displays general information.

Step 3 Click on **#VMs** to view the required virtual machine (VM) details.

The **SAN Host VM Screen** is displayed.

Select an Enclosure to view **CPU & Memory** and **Disk I/O** charts on the right pane.

Storage

To access the **Storage** dashboard, choose **Dashboards** > **Storage**.

The **Storage** dashboard consists of the following:

- **Enclosures**: Lists the storage and their network attributes.
  - The **Storage Enclosure Name** column lists all the storage devices.
  - **Member WWNs** displays the World-Wide Name of the member storage devices. It's a 64-bit identifier and is unique world-wide.
- **Traffic Chart** area: Provides the I/O statistics, CPU and memory information, and disk latency of individual storage device or virtual machines.
- **Events Table** area: Provides information about the events of all the ports that are configured within a specific storage device enclosure.
- **Topology**: Provides end-to-end topology layout and path information of 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.

Viewing Storage Enclosure

SAN Controller 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 **Settings** > **Server Settings** > **Insights**. Ensure that you restart the SAN Insights service to use the new properties.

To view the storage enclosure from the SAN Controller Web UI, perform the following steps:

Procedure

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

The list of storage in the storage enclosures table is displayed.

Step 2 Click **i** icon to view SAN Insights Monitor page. On **SAN Insights Monitor** window, click on required storage name. Refer to Monitor Metrics for more information.

Step 3 Click on **Launch** icon to view Storage Enclosure window.

The **Storage Enclosure** window appears.

The Storage Enclosure window displays the Initiator-Target (IT) pairs, Topology, average ECT/DAL/read/write times, and Switch Interface for the selected host.

- **Initiator Target Pairs** - This table lists all the initiator-target pairs for the selected storage. 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.
- **Topology** - Provides an end-to-end topology layout and path information between host enclosures. On **View** card click **+** or **-** to zoom-in and zoom-out. Similarly, you can use the mouse scroll wheel to zoom-in and zoom-out. Click **Refresh** icon to Refresh the topology view. Choose **Select layout** drop-down list to view topology. This can be either **Hierachical** or **Hierachical Left-Right** view.
- The flow table shows the details of all metrics on ECT/DAL/read/write times, active I/Os, IOPS, Throughput etc. along with their 1-hour average and the baseline information.

- **Switch Interface** - This table displays data for the last hour period that is selected for the interface. The switch name and the interface name are displayed on top of the switch interface table.

SAN Insights

SAN Insights visually displays fabric-level information in a holistic view from end-to-end.

On 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 the selected scope.

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.

SAN Controller allows you to view SAN Insights metrics based on fabrics, switches, and two protocols namely SCSI and NVMe.

Ensure that you have enabled SAN Insights feature for SAN Controller. Choose **Settings** > **Feature Management**, choose check box **SAN Insights**.

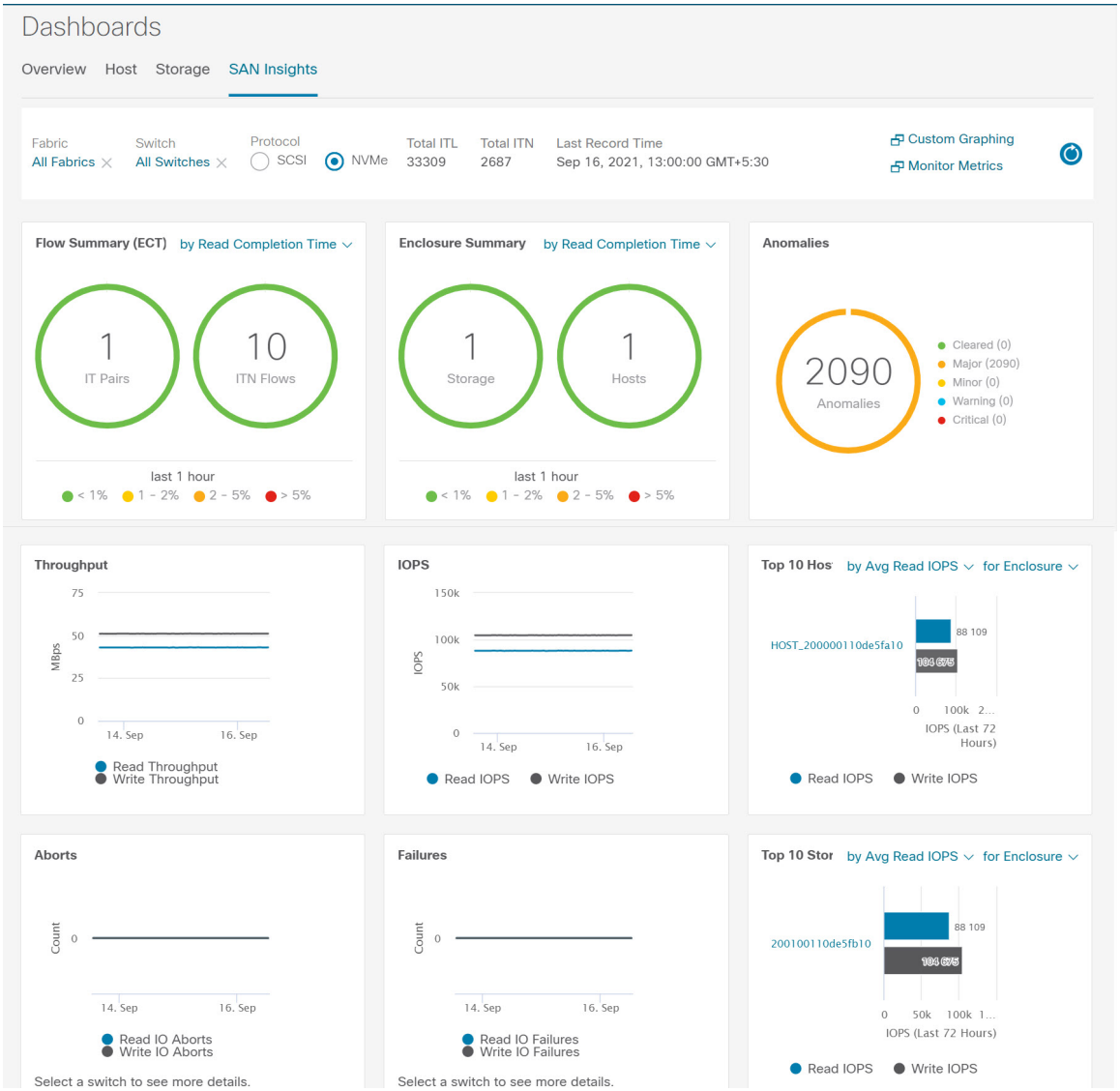
Ensure that you have configured SAN Insights, to view information on Dashboard. See Configuring SAN Insights, on page 37.

Viewing SAN Insights

To view the SAN Insights Dashboard, choose **Dashboard** > **SAN Insights**. The SAN Insights Dashboard provides visibility for overall read/write IO operations/latency.

Table 3: SAN Insights Dashboard

Field	Description
Fabric	Click **Fabric**, to select required fabric, and click **Save**.
Switch	Click **Switch**, to select required switch.
Protocol	Choose **SCSI** or **NVMe** check box to select required protocol. By default, **SCSI** protocol is selected,
Total ITL	Displays total ITL value for selected options.
Total ITN	Displays total ITN value for selected options.
Last Record Time	Displays last record time for selected options.
Custom Graphing	Click **Custom Graphing**, SAN Insights Metrics Custom Graphing window is displayed. For more information, see Custom Graphing.
Monitor Metrics	Click **Monitor Metrics**, SAN Insights Monitor window is displayed. For more information, see Monitor Metrics.
Refresh	Click **Refresh** icon to Refresh and load screen.



Ensure that you restart the SAN Insights service to use the new properties.

The total distinct ITL and ITN counts from the trained baseline is displayed at top center of 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.

- Anomalies

  Displays the number of anomalies policy and their severity levels in pie-chart and list. The pie chart displays the severity levels in different color modes and the list next to the chart displays the severity level and the number of anomaly policies in that level.

  You can edit, manage, view, acknowledge, and clear these anomalies. Choose **Operations** > **Event Analytics** > **Alarms**.

- 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.

  Select a switch to see 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.

  Select a switch to see 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/WWN/Device Alias in the selected Protocol/Fabric/Switch scope based on the metric that is 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/WWN/Device Alias in the selected Protocol/Fabric/Switch scope based on the metric that is 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 Host** 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.
- In the **Top 10 Host** and **Top 10 Storage** dashlets, the bars for the write metrics do not display the value always due to restricted space. To view all the values on the graph, you can either hover the mouse over the bar or hide the read or the write bar using the legend at the bottom of the dashlet.

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.

Ensure that you have configured Syslog on the SAN Controller Device Manager, to capture NPU and ITL Loads. Choose **SAN** > **Switches**. Click on the switch, a slide-panel is displayed, click **Launch** icon to view switch information, click **Device Manager**. 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 SAN Controller server.

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 Custom Graphing

To view the SAN Insights metrics, choose **Dashboard** > **SAN Insights**. The SAN Insights Dashboard page appears. Click **View Custom Graphing** to view SAN Insights Metrics Custom Graphing window.

The dashboard displays the data over the last 72 hours. However, the Flow Summary and the Enclosure Summary donuts display the last hour aggregation from the latest updated time. The top 10 hosts/storage, throughput, IOPS, Aborts, Failures, graph display respective data.

Note The refresh interval for Custom Graphing page is 5 minutes. Click on the **Play** icon to refresh every 5 minutes automatically.

Cisco SAN Controller 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 on the **Web UI** > **Settings** > **Server Settings** > **Insights**.

Ensure that you restart the SAN Insights service to use the new properties.

Viewing Custom Graph and Table

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

You can also add multiple graphs for comparison by clicking on the **Add Graph** the top right.

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

SAN Insights Metrics has two tabs.

- Graph
- Table

Graph



The graph is plotted with corresponding metrics with from and to date selected. 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. Click **Add Graph** to create graph. You can add maximum of three graphs at a time on this page.

SAN Controller allows the user to view data for more than two weeks' timeframe (up to a default maximum of 90 days. You can configure this timeframe in the server properties. Click drop down button next to Time Range and select date.

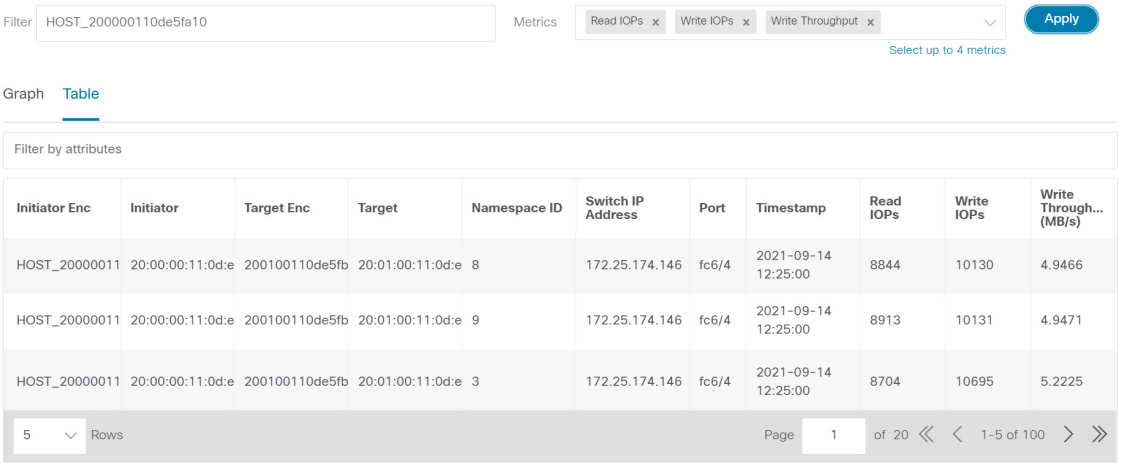
The Custom graphing metrics are enhanced to include the Write IO Failures, Read IO Failures, Write IO Aborts and Read IO Aborts to the drop-down metrics list.

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.

Table



When you select a failure or abort from **Metrics** 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 that 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.

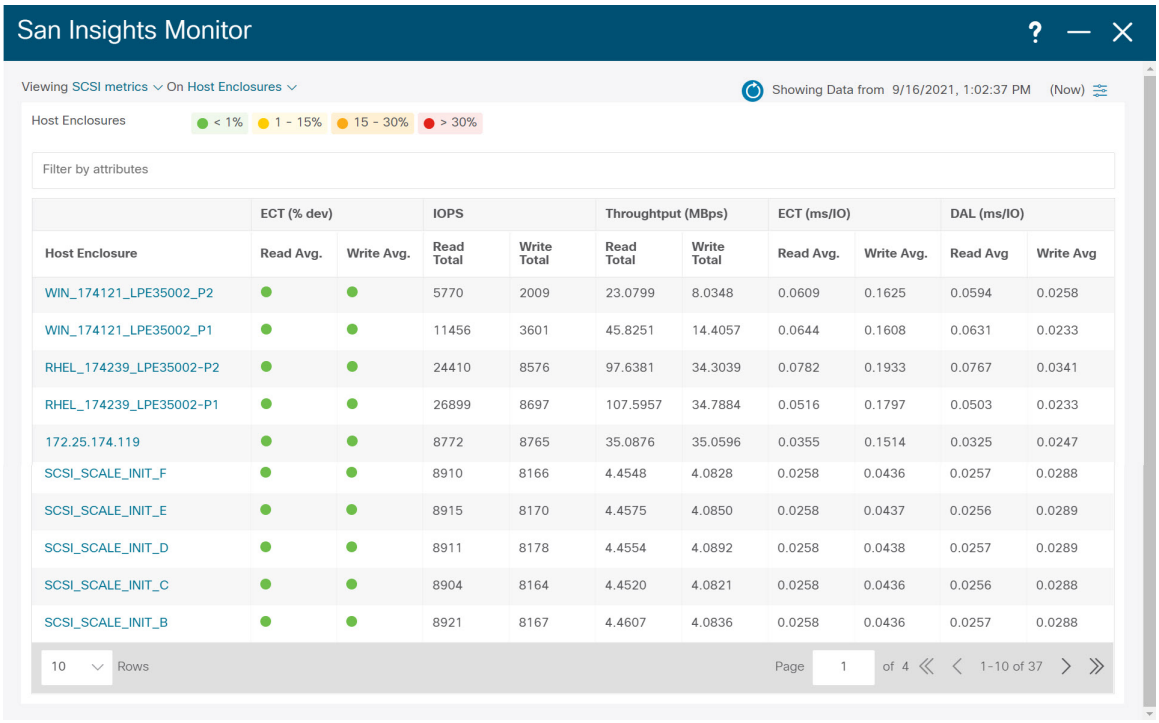
To view, input any of the seven dimensions (Initiator Enc, Initiator, Target Enc, Target, LUN, Switch IP Address, Port, Timestamp, Read IOPs, Write IOPs) in the filter by attributes field (separated by comma), and select an associated metric.

Monitoring Metrics

UI Path: **Dashboard** > **SAN Insights** > **Monitor Metrics**

The SAN Insights Monitor 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.

SAN Controller allows you to view SAN Insights monitor based on two protocols, SCSI and NVMe. By default, the SCSI protocol is selected. However, you can change this setting from the **Settings** > **Server Settings** > **Insights**.



From Release 12.0.1a, you can view SAN Insights Monitor on dashboard. From SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard** > **SAN Insights** .

Step 2 Click **Monitor Metrics**.

The **SAN Insights Monitor** window is displayed.

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

Step 3 Choose **SCSI** or **NVMe** metrics using **Viewing** drop-down list to view to select the data type.

Step 4 Choose **Host Enclosure**, **Storage Enclosure**, or **IT Pairs** using **On** drop-down list to view required data.

Step 5 Click **Refresh** icon, to view current time.

The system time is displayed at the right corner of the window.

Specify a time interval using the time setting icon. Click **Setting** icon, enter appropriate time in hours and click **Apply** to view data of selected time.

The switch interface counters display when you choose green circle icon on the switch on the topology page.

Step 6 Click on the required name to view details.

A slide-in panel is displayed with the associated I-T pairs.

Step 7 Click **Launch** icon to view the window.

Similarly, you can click thrice on the name to navigate to the detailed view.

The SAN Insights Monitor page displays the initiator-target pairs for the selected enclosure or IT Pairs. The flow table shows the details of all metrics on ECT/DAL/read/write times, ECT (%dev), IOPS, throughput information.

Similarly, you can view SAN Insights Monitor, from host and storage tabs on dashboard.

- Choose **Dashboard > Host**, click **i** icon on required host name. For more information on host enclosure, refer to Viewing Host Enclosures section.
- Choose **Dashboard > Storage**, click **i** icon on required storage name. For more information on storage enclosure, refer to Viewing Storage Enclosures section.

For more information on Initiator-Target (IT) Pairs, refer to Viewing IT Pairs, on page 19 section.

Viewing IT Pairs

Cisco Nexus Dashboard Fabric Controller 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 **Settings** > **Server Settings** > **Insights**. Ensure that you restart the SAN Insights service to use the new properties

To view the IT Pair from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

UI Path: **Dashboard** > **SAN Insights** > **Monitor Metrics**

Procedure

Step 1 Choose **Dashboard** > **SAN Insights** > **Monitor Metrics**

The SAN Insights Monitor page appears. Refer to Monitor Metrics for more information.

Step 2 Choose **SCSI** or **NVMe** metrics using **Viewing** drop-down list to view to select the data type.

Step 3 Choose **IT Pairs** using **On** drop-down list to view data.

Step 4 Click on required IT pair name.

The IT pair slide-in panel appears.

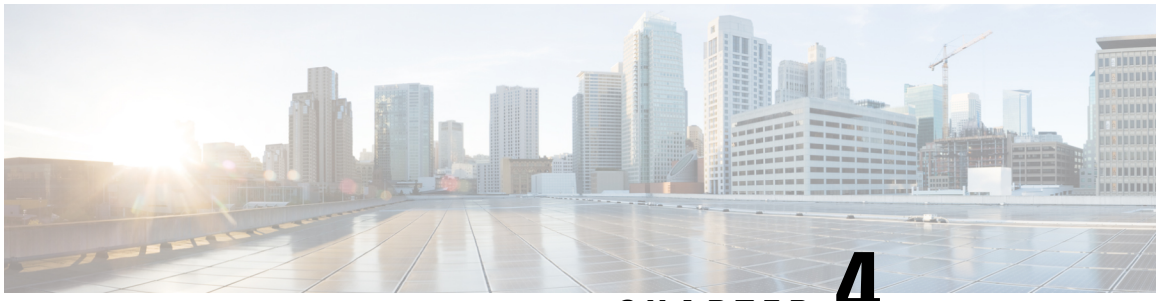
Step 5 Click on **Launch** icon to view IT pairs window.

The IT pairs window appears.

The IT pair window displays the Initiator-Target (IT) pairs, Topology, average ECT/DAL/read/write times, and Switch Interface for the selected IT pair.

- **Initiator Target Pairs** - This table lists all the IT pairs for the selected IT pair name. 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.

- **Topology** - Provides an end-to-end topology layout and path information between IT pairs. On **View** card click **+** or **-** to zoom-in and zoom-out. Similarly, you can use the mouse scroll wheel to zoom-in and zoom-out. Click **Refresh** icon to refresh the topology view. Choose **Select layout** drop-down list to view topology. This can be either **Hierachical** or **Hierachical Left-Right** view.
- The flow table shows the details of all metrics on ECT/DAL/read/write times, active I/Os, IOPS, Throughput etc. along with their 1-hour average and the baseline information.
- **Switch Interface** - This 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.



CHAPTER 4

Topology

UI Navigation - Click **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. Use this window to perform the following tasks:

- To view more information about each of these elements, hover your cursor over the corresponding element.
- To view your navigation in the topology, view the breadcrumb at the top.
- When you click the device or the element, a slide-in pane appears from the right that displays more information about the device or the element. To view more information in the topology, double-click a node to open the node topology. For example, to view the fabric topology and its components in the **Topology** window, double-click the fabric node and then double-click an element that you want to view such as a host, a multicast group or a multicast flow, as applicable to the fabric type, and view the respective topology.
- If you want to view the fabric summary for the fabrics, click the fabric node. From the **Fabric Summary** slide-in pane, open the **Fabric Overview** window. Alternatively, you can right-click a fabric and choose **Detailed View** to open the **Fabric Overview** window. For more information about fabric overview window, see Fabric Overview, on page 45.
- Similarly, you can click on a 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 in the **Switch** slide-in pane. To view more information, click the **Launch** icon to open the **Switch Overview** window. For more information about switch overview window, see Switch Overview, on page 79.

  SAN switches have only two roles, Core Router and Edge Router.
- Choose an action from the **Actions** drop-down list to perform various actions based on the element you select in the topology.
- To perform actions on the elements in the topology, other than the ones listed in the actions drop-down list, right-click the element. This opens the appropriate windows and allows you to perform tasks based on the elements. For example, if you right-click a fabric, you can perform tasks such as various configurations, delete the fabric, backup and restore, and many more.

This section contains the following:

- Searching Topology, on page 22

• Viewing Topology, on page 22

Searching Topology

Use a combination of search attributes and search criteria in the search bar for an effective search. As you enter a combination of search attribute and search criteria in the search bar, the corresponding devices are highlighted in the topology.

You can apply the search criteria such as equals (**=**), does not equal (**!=**), contains (**contains**), and does not contain (**!contains**).

The search attribute that you can use for SAN fabric is fabric name.

When a device is displayed on the topology, double-click it to navigate further into the topology. For example, when the fabric that you searched is displayed on the topology, double-click on the fabric (cloud icon) to navigate inside its topology. Furthermore, after the fabric is displayed on the topology, you can continue to search based on a combination of a criteria and various search attributes such as switch name, IP address, model, serial, software version, and up time.



Note Certain levels of the topology allow filters only, that is, filters take the place of Search. The topology listing for these levels display a limited number of entities.

Viewing Topology

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.

In case of multiple selection of switch, you must release the modifier keys (cmd/ctrl) before releasing mouse drag to end the switch selection.

You can view the following information of the devices and links in the **View** pane:

- Layout options - You can zoom in, zoom out, or adjust the layout to fit the screen. You can also refresh the topology or save any changes to the topology. For more information, see Zooming, Panning, and Dragging, on page 24.
- Select Layout drop-down list - Choose the layout for your topology from this drop-down list, and click **Save Topology Layout** in the layout options. For more information, see Layouts, on page 25.
- Status - The status of every device or link is represented by different colors. You can view the configurational status and operational status as well for LAN topologies. For more information, see Status, on page 25.

Topology for a node is displayed at multiple scope. Each scope is shown in the hierarchical order. The scope hierarchy is shown as breadcrumbs and can be navigated to required scope. Scopes are as follows:

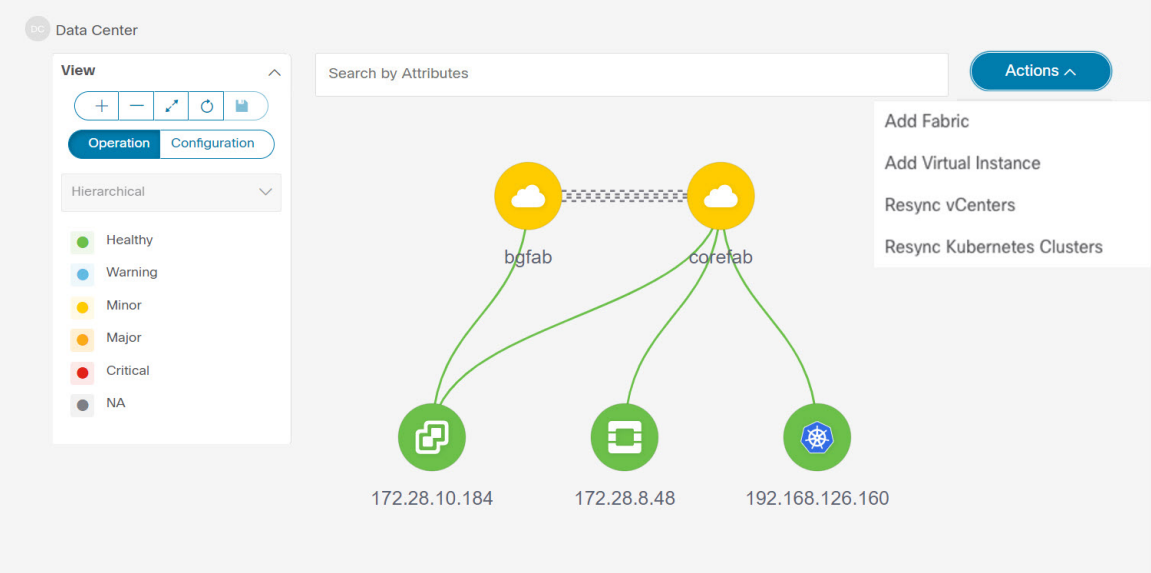
- Data Center
- Cluster (vCenter)
- Resource List (DVS, Compute, and VM)

- Resource

Note

- In the **Topology** window, FEX appears in gray (**Unknown** or **NA**) because Operation and Configuration status 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. Right-click on the link and delete it if the removal was intentional. A manual Rediscover of the switch will also delete and re-learn all links to that switch.

When a Multi-Site Domain (MSD) fabric is deployed with the child fabrics, to view multi-site topology, double-click on a fabric node, and then choose MSD scope or double click on the gray MSD node to view the MSD topology.



Viewing Elements in SAN Topology

UI Navigation - Click **Topology**.

This section provides information about various elements or entities displayed in the **Topology** window for SAN fabrics.

VSAN

In the **Topology** window, double-click on the fabric to view the fabric topology. A SAN fabric contains VSAN node and switches. The VSAN node has a number displayed in brackets, which indicates the number of VSANs in the fabric. Double-click on the VSAN node to view the individual VSANs in the VSAN node topology.

The VSAN topology displays zones and switches connected to the VSAN. Double-click on a VSAN to open the VSAN topology and view the zones and switches. However, the switches must have the VSAN configured and have links with VSAN membership.

Zone

Double-click on the VSAN node, VSAN zone is displayed. The switches in that VSAN and a Zones node show the number of zones. Double click on that zones node, which displays individual zone nodes. Double click on zone node display switches in that zone and its connectivity (ISL) with end devices that are a member of the selected zone.

Hosts and Storage

The zone topology displays hosts and storage devices pertaining to the zone and connected to a switch. In the **Topology** window, double-click on a zone to view hosts and storage devices.

Alternatively, to view the switch topology, you can directly click on a switch in the fabric topology. The switch topology displays the hosts and storage devices connected to the switch.

Hosts

Click on the host device to view more information about the host in the slide-in pane. From the slide-in pane, you can open the host dashboard. Alternatively, you can right-click on the host device and click **Detailed View** to open the host dashboard.

Storage

Click on the storage device to view more information about storage in the slide-in pane. From the slide-in pane, you can open the storage dashboard. Alternatively, you can right-click on the storage device and click **Detailed View** to open the storage dashboard.

Links

In the switch topology, click on the link that connects two devices, for example, the switch and the storage to open the **Link** slide-in pane. This pane displays the details related to the last polling of the performance data. However, you must have configured performance monitoring for the fabric in **Performance Data Collection Settings**. This allows the Nexus Dashboard Fabric Controller to collect the traffic information and the aggregated information is displayed along with a graph showing traffic utilization. The Nexus Dashboard Fabric Controller updates the last poll metric every 5 minutes for all the ports, links, and so on for all the switches in the fabric. If the date and time displayed in this pane is current, then the last poll metric details are up to date. The details provided in this slide-in pane are as follows:

- General information such as link capacity, VSAN, and status.
- Information about the traffic for the last 24 hours with details such as average, maximum, and minimum Rx and Tx in Bytes.
- The last poll metrics such as Time, Rx, and Tx can be viewed in a graph on the **Graph** tab and in a table format on the **Table** tab. Note that the table is paginated.

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.

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, Nexus Dashboard Fabric Controller splits your leaf-tier every 16 switches.

- **Circular** and **Tiered-Circular** - Draw nodes in a circular or concentric circular pattern.
- **Random** - Nodes are placed randomly on the window. Nexus Dashboard Fabric Controller tries to make a guess and intelligently place nodes that belong together in close proximity.
- **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, Nexus Dashboard Fabric Controller will draw the nodes based on your last saved layout positions.

Before a layout is chosen, Nexus Dashboard Fabric Controller checks if a custom layout is applied. If a custom layout is applied, Nexus Dashboard Fabric Controller uses it. If a custom layout is not applied, Nexus Dashboard Fabric Controller 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.

Status

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

- Green - Indicates that the element is in good health and functioning as intended.
- Blue - Indicates that the element is in a warning state and requires attention to prevent any further problems.
- Yellow - Indicates that the element has minor issues.
- Orange - Indicates that the element has major issues 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.

The configurational colors and what they indicate are described in the following list:

- Green - Indicates that the element is element is In-Sync with the intended configuration.
- Blue - Indicates that the element has pending deployments.

- Yellow - Indicates that active deployments are in-progress.
- Red - Indicates that the element is Out-of-Sync with the intended configuration.
- Gray: Indicates lack of information or no support for Configuration Sync calculation.



Note

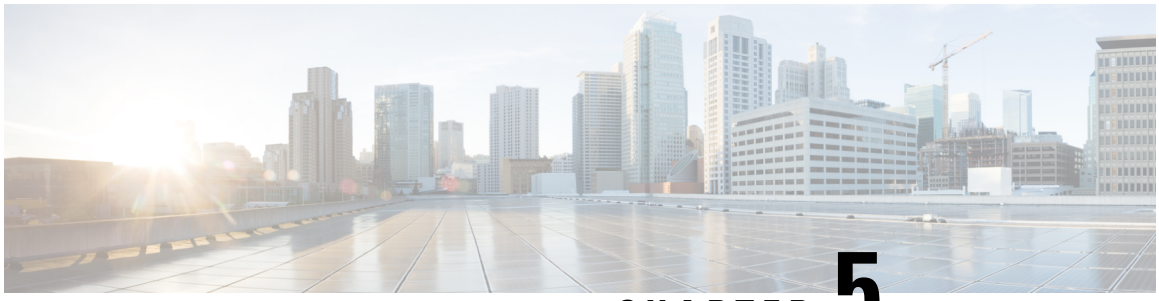
- In the **Topology** window, FEX appears in gray (**Unknown** or **n/a**) because Operation and Configuration status is not calculated for FEX.
- After moving a cable from one port to another port, the old fabric link is retained in the **Topology** window, and it is shown in the red color indicating that the link is down. Right-click on the link and delete it if the removal was intentional. A manual Rediscover of the switch will also delete and re-learn all links to that switch.



PART I

SAN

- Fabrics, on page 29
- Switches, on page 71
- SAN Links, on page 87
- Interfaces, on page 105
- End Devices, on page 115
- Host Path Redundancy, on page 121
- Port Monitoring, on page 125
- Active Zones, on page 133
- Storage, on page 135



CHAPTER 5

Fabrics

- Fabrics, on page 29
- Fabric Overview, on page 45

Fabrics

From Release 12.0.1a, SAN Controller allows you to create SAN Fabrics.

The following table describes the fields that appear on **SAN Controller > SAN > Fabrics > Fabrics**.

Field	Description
Fabric Name	Specifies the name of the fabric.
Seed Switch	Specifies the seed switch used to discover switches in the fabric.
State	Specifies the state of the fabric.
SNMPv3/SSH	Specifies if SNMP and SSH access is allowed.
User/Community	Specifies the role of the user who created the fabric.
Auth/Privacy	Displays the authentication type.
Licensed	Specifies if all the switches in the fabric are licensed or not.
Health	Displays the health of the fabric.
Performance Collection	Specifies if performance collection is enabled or disabled on the fabric.
Updated Time	Specifies the time when the fabric was created or updated.
Incl. VSANS	Specifies the VSANS included with the fabric.
Excl. VSANS	Specifies the excluded VSANS.

The following table describes the action items, in the Actions menu drop-down list, that appear on **SAN > Fabrics > Fabrics**.

Action Item	Description
Add Fabric	From the **Actions** drop-down list, select **Add Fabric**. For more instructions, see Adding a Fabric .
Edit Fabrics	Select a fabric to edit. From the **Actions** drop-down list, select **Edit Fabrics**. Make the necessary changes and click **Apply**. For more instructions, see Editing a Fabric, on page 31.
Delete Fabrics	Select one or more fabrics to delete. From the **Actions** drop-down list, select **Delete Fabrics**. Click **Confirm** to delete the fabrics. For more instructions, see Deleting a Fabric, on page 32.
Rediscover Fabrics	Allows you to rediscover the switches, links, and end devices associated with the fabric. Select one or more fabrics to rediscover. From the **Actions** drop-down list, select **Rediscover Fabrics**. A progress bar in the **State** column displays the rediscovery progress. For more instructions, see Rediscovering a Fabric, on page 32.
Purge Fabrics	Allows you to purge non-existent switches, links, and end devices of the fabric. Select one or more fabrics to purge. From the **Actions** drop-down list, select **Purge Fabrics**. For more instructions, see Purging a Fabric, on page 32.
Configure Performance	Allows you to enable performance monitoring on links, switch interfaces, and end devices associated with the fabric. Select one or more fabrics for performance monitoring. From the **Actions** drop-down list, select **Configure Performance**. Make the necessary changes and click **Apply**. For more instructions, see Configuring Performance.
Configure SAN Insights	Allows you configure SAN Insights on the selected fabric. For more instructions, see Configure SAN Insights.
Configure Backup	Allows you to configure and schedule backup for the fabric data. For more instructions, see Configuring Fabric Backup, on page 43.

This chapter contains below sections:

Adding a Fabric

To create a fabric using Cisco SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN** > **Fabrics** > **SAN Fabrics**.

Step 2 Choose **Actions** > **Add Fabrics**.

Step 3 In the **Fabric Name** field, enter a unique fabric name.

Step 4 In the Fabric Seed Switch field, enter the IP address of the seed switch.

You can also enter the DNS name of the seed switch.

Step 5 Check **SNMPv3/SSH** check box to enable access.

Step 6 From the **Authentication / Privacy** drop-down list, choose appropriate authentication for switch discovery.

Step 7 In the **User Name** and **Password** fields, enter appropriate details to access the seed switch.

Step 8 To discover switches using VSANs only, check the **Limit Discovery by VSAN** check box.

You can choose to discover switches that are associated with VSANs or not associated with VSANs.

- Select **Included VSAN List** to discovery switches included in VSANs.
- Select **Excluded VSAN List** to discovery switches excluded in VSANs.
- Enter the included or excluded VSANs in the **VSAN List** field.

Step 9 (Optional) To discover switches using UCS credentials, check the **Use UCS Credentials** check box.

- Enter the appropriate **UCS CLI Credentials** in the username and password fields.
- To use the same SNMP credentials, check the **Use same SNMP Credentials for UCS** check box.

  You must provide different SNMP details if you uncheck this check box.
- To use SNMP for UCS, check the **Use SNMPv3 for UCS** check box.
- Enter appropriate community string in the **UCS SNMP Community String** field.

Step 10 Click **Add** to add a Fabric.

Editing a Fabric

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

Procedure

Step 1 Choose **SAN > Fabrics > SAN Fabrics**.

Step 2 Choose check box to edit required fabric name, choose the **Actions > Edit Fabrics**.

Step 3 You see the **Edit Fabrics** window. You can edit only one fabric at a time.

Step 4 Enter a new fabric **Fabric Name**

Step 5 (Optional) Check the **SNMPV3** check box. If you check SNMPV3, the **Community** field change to **Username** and **Password**.

Step 6 Enter the **Username** and **Password**, privacy and specify how you want SAN Controller Web Client to manage the fabric by selecting one of the status options.

Step 7 Change the status to **Managed**, **Unmanaged**, or **Managed Continuously**.

Step 8 (Optional) Check the **Use UCS Credentials** check box. If you want to modify UCS credentials.

Step 9 Enter the **Username** and **Password**

Step 10 Click **Apply** to save the changes.

Deleting a Fabric

To delete a fabric using SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN > Fabrics > SAN Fabrics**.

Step 2 Choose **Actions** > **Delete Fabrics** to remove the fabric from the data source and to discontinue data collection for that fabric.

Rediscovering a Fabric

To discover a fabric using Cisco SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN > Fabrics > SAN Fabrics**.

Step 2 Choose check box to rediscover required fabric name, choose the **Actions** > **Rediscover Fabrics**.

Step 3 Click **Yes** in the dialog box.

In a fabric window, **State** column displays the progress of rediscovery for selected fabric.

The **Fabric** is rediscovered.

Purging a Fabric

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

Procedure

Step 1 Choose **SAN > Fabrics**.

Step 2 Choose the check box next to the fabric you want to purge.

Step 3 Choose **Action** > **Purge Fabrics**.

The Fabric is purged.

From SAN Controller Release 12.0.1a, you can purge fabric on Topology window.

- Choose **Topology**, choose a fabric, Right-click on fabric, choose **Purge Down Fabric**.

  The **Fabric** is purged.

Configuring Performance

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 SAN Controller 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.

Procedure

Step 1 Choose **SAN > Fabrics**.

Step 2 Choose the check box next to the fabric you want to configure performance collections.

Step 3 Choose **Action** > **Configure Performance**.

The **Performance Data Collection Settings** window appears.

Step 4 Choose check box **Performance Collection**, to enable other check boxes.

Step 5 Choose required **ISL/NPV Links**, **Hosts**, **Storage**, and **FC Ethernet**, or choose box **Select All** to enable performance collection for these data types.

a) To collect temperature data for SAN devices, choose **Settings** > **Server Settings** > **PM**.

b) On **PM** tab, choose check box for **Enable SAN Sensor Discovery** and **Collect Temperature for SAN Switches**.

Step 6 Click **Apply** to save the configuration.

Step 7 In the confirmation dialog box, click **Yes** to restart the performance collector.

What to do next

After upgrading to Nexus Dashboard Fabric Controller, to view the restored old Performance Manager and high chart data, you must manually enable Performance Manager for each fabric. However, any old Temperature data is not restored.

To begin collecting Temperature data on the upgraded Nexus Dashboard Fabric Controller setup, go to **Settings > Server Settings PM** tab. Check **Collect Temperature for LAN Switches** checkbox and click **Save**.. Note that **Enable LAN Sensor Discovery** checkbox is enabled by default.

SAN Insights

The SAN Insights feature enables you to configure, monitor, and view the flow analytics in fabrics. SAN Insights features of SAN Controller enable 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.

SAN Controller 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, see Required System Memory for SAN Controller deployment. Ensure that the system RAM, vCPU, and SSDs are used for deploying SAN Insights. Use of NTP is recommended to maintain time synchronization between the SAN Controller and the switches. Enable PM collection for viewing counter statistics.

From Release 12.0.1a, you can create policy based alarms generation for SAN ITL/ITN flow. From Web UI, choose **Operations** > **Event Analytics** > **Alarms** > **Alarm Policies** to create policies.

Prerequisites

- SAN Insights is supported on virtual-data node and physical node.
- The SAN Insights feature isn't supported on app-node deployment for Nexus Dashboard.
- Single node and three nodes deployments of Nexus Dashboard are supported for deploying SAN Insights.
- If SAN Insights streaming was configured with KVGPB encoding using versions of Cisco SAN Insights older than 11.2(1), the switch continues to stream with KVGPB encoding while configuring streaming with SAN Insights versions 11.2(1) and above. Compact GPB streaming configuration for SAN Insights is supported starting from SAN Controller 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 SAN Controller Web UI, choose **SAN** > **Fabrics**, select a fabric, choose **Actions** > **Configure SAN Insights** and click **Next**. On the Switch Configuration screen, select required switch, choose **Actions** > **Disable Analytics** to clear all the analytics and telemetry configuration on the selected switches.
- The SAN Insights feature is supported for Cisco MDS NX-OS Release 8.3(1) and later.

Configuring Persistent IP Address

Before you install or upgrade to SAN Controller Release 12.1.1e, you must configure persistent IP addresses on Cisco Nexus Dashboard.

Ensure that the services are allocated with IP pool addresses on the Cisco Nexus Dashboard. For more information, refer to *Cluster Configuration* section in Cisco Nexus Dashboard User Guide.



Note To configure SAN Insights on one node for SAN Controller deployment, the SAN Insights receiver requires one available Persistent IP. Similarly, to configure SAN Insights on three nodes for SAN Controller deployment, it requires three available Persistent IP addressees.

To configure Persistent IP addresses on Cisco Nexus Dashboard, perform the following steps:

Procedure

Step 1 Choose **Infrastructure** > **Cluster Configuration**.

Step 2 On General tab, in External Service Pools card, click **Edit** icon.

The **External Service Pools** window appears.

Step 3 To configure IP addresses for SAN Controller, in Data Service IP's, click **Add IP Address**, enter required IP addresses and click **check** icon.

Step 4 Click **Save**.

Guidelines and Limitations

- Ensure that the time configurations in SAN Controller 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 SAN Controller.
- To modify the streaming interval, use the CLI from the switch, and remove the installed query for SAN Controller. Modify the **san.telemetry.streaming.interval** property in the SAN Controller 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. You can change the default value while configuring SAN Insights. On **Switch configuration** wizard in **Interval(s)** column select required value from drop-down list.
- The port sampling window on the switch side should have all ports (default).
- 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, see Configuring SAN Insights.

Server Properties for SAN Insights

To modify server settings values, navigate to **Settings** > **Server Settings** > **Insights** on the Web UI.

Note If you change the server properties, ensure that you restart the SAN Controller to use the new properties value.

The following table describes the field names, descriptions, and its default values.

Table 4: Server Properties for SAN Insights

Field Name	Description	Default Value
Telemetry pages default protocol scsi/nvme	Specifies the required default protocol selection in the SAN Insights UI pages to view corresponding data: SCSI or NVMe.	SCSI

Field Name	Description	Default Value
SAN Insights ECT thread count	Specifies number of threads to use for ECT queries.	4
Max. Aggregation bucket size	Specifies maximum number of buckets to use for aggregation queries.	40,000
Data table download size	Specifies number of records for table download.	1000
ECT Data limit	Specifies the ECT Data limit.	14 **Note** The value of ECT data limit must be less than or equal to the value of SAN Telemetry retention policy - baseline / post processed.
SAN Telemetry deviation low threshold	Specifies the value that is the change point between normal and low.	1
SAN Telemetry deviation med threshold	Specifies the value that is the change point between low and medium.	15
SAN Telemetry deviation high threshold	Specifies the value that is the change point between medium and high.	30
SAN Telemetry deviation low threshold for NVMe	Specifies the value that is the change point between normal and low for NVMe.	1
SAN Telemetry deviation med threshold for NVMe	Specifies the value that is the change point between low and medium for NVMe.	2
SAN Telemetry deviation high threshold for NVMe	Specifies the value that is the change point between medium and high for NVMe.	5
SAN Telemetry training timeframe	Specifies the training time frame for flows ECT baseline.	7 days
SAN Telemetry training reset timeframe	Specifies the time duration to periodically restart the ECT baseline training after number of days.	14 days
SAN Telemetry retention policy - baseline / post processed	Specifies the retention policy - baseline / post processed.	14
SAN Telemetry retention policy - hourly rollups	Specifies the retention policy - hourly rollups	90
Telemetry Gap Reset Interval	Specify maximum valid time gap between records (before drop) time is in seconds	750
Active Anomaly Capture	Specify maximum number of actively tracked anomalies per post processor.	500

Field Name	Description	Default Value
Baseline training include NOOP frames	Specify if the baseline learning should reference noop frames.	Not selected
Baseline training includes negative deviation	Specify if the baseline deviation must include negatives.	Selected
Use telemetry Gap Reset Interval	Specifies the use telemetry reset based on time gap between records	Selected

The following table describes the system requirement for installation of SAN Controller:

Table 5: Required System Memory for SAN Controller with SAN Insights

Node Type	vCPUs	Memory	Storage
Virtual Data Node	32	128 GB	3 TB SSD
Physical Data Node	40	256 GB	4*2.2 TB HDD, 370G SSD, 1.5 TB NVMe

Table 6: Verified limit for SAN Insights deployment

Deployment Type	Verified Limit[1] [2]
Cisco Virtual Nexus Dashboard (1 Node)	80K ITLs/ITNs
Cisco Physical Nexus Dashboard (1 Node)	120K ITLs/ITNs
Cisco Virtual Nexus Dashboard (3 Node)	150K ITLs/ITNs
Cisco Physical Nexus Dashboard (3 Node)	250K ITLs/ITNs

1 Initiator-Target-LUNs (ITLs)
2 Initiator-Target-Namespace ID (ITNs)

Configuring SAN Insights

From SAN Controller Release 12.0.1a, you can configure SAN fabrics on topology window, apart from configuring on fabric window.

On topology window, right-click on a SAN fabric, choose **Configure SAN Insights** and follow procedure to configure.

To configure SAN Insights on the SAN Controller Web UI, perform the following steps:

Before you begin

Ensure that you configure persistent IP addresses, before you configure SAN Insights. Refer to Configuring persistent IP addresses.

Ensure that you have enabled SAN Insights feature for SAN Controller. Choose **Settings** > **Feature Management**, choose check box **SAN Insights**.

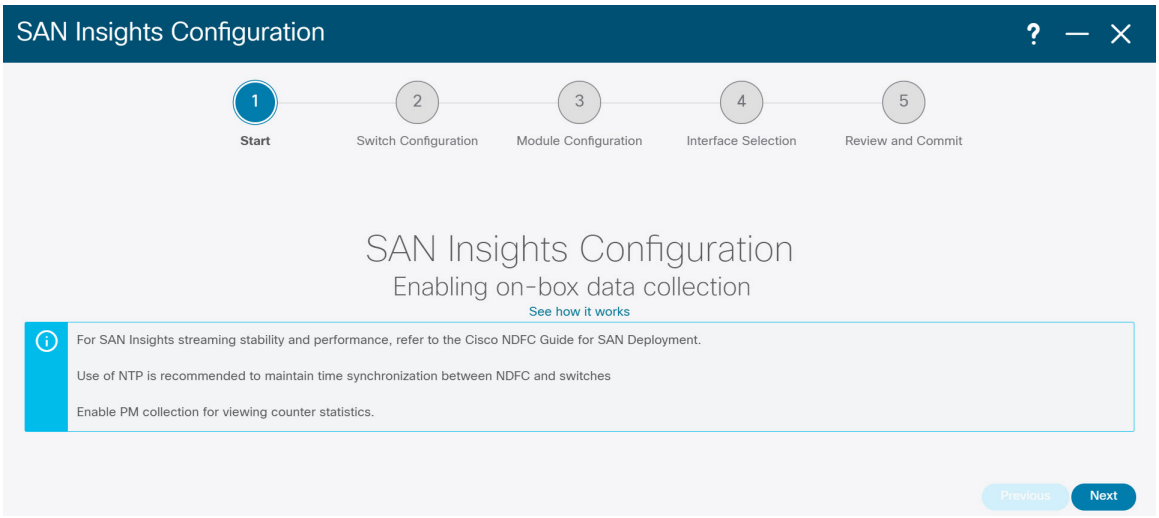
Note You must configure with sufficient system requirements and IP addresses. For more information on scale limits, refer to table Required System Memory for SAN deployment in Server Properties for SAN Insights.

Procedure

Step 1 Choose **SAN** > **Fabrics**.

Step 2 Choose required fabric, click **Actions** > **Configure SAN Insights**.

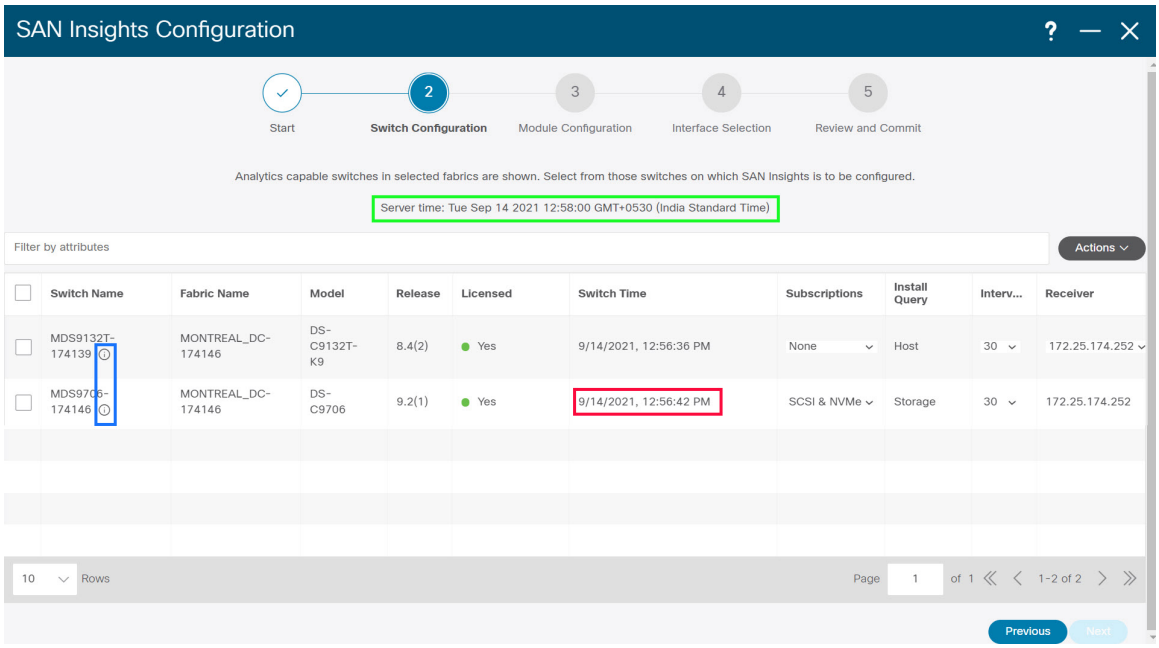
The **SAN Insights Configuration** wizard appears.



Step 3 In the **SAN Insights Configuration** wizard, click **Next**.

The **Switch Configuration** wizard appears.

Step 4 Select the switches where SAN Insights analytics and telemetry streaming need to be configured, after you select the appropriate values from the drop-down list as mentioned below.



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.

Note
SAN Controller time is displayed on this UI and switch time is marked in RED if the switch time is found to be deviating from the SAN Controller time.

For the selected SAN Controller 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 SAN Controller server to receive SCSI telemetry and another SAN Controller server to receive NVMe telemetry.

In SAN Controller deployment, the IP address assigned to eth0 or eth1 can be used for receiving SAN Insights streaming from the switch. However, ensure that streaming is configured to the SAN Controller 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 Controller for streaming analytics data from the switch.

You can provide management IP eth0 and data IP eth1 for fabric access to bootstrap the SAN Controller. Therefore, the streaming must be configured to the persistent IP assigned in the data-IP subnet. Refer to the Configuring Persistent IP Address, on page 34 section for more information.

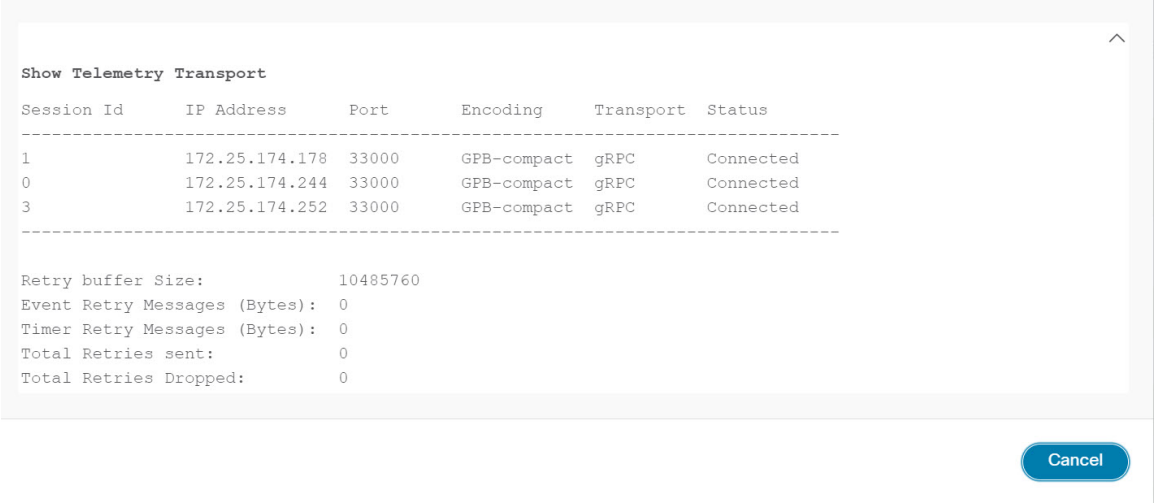
For NDFC to run on top of the virtual Nexus Dashboard (vND) instance, you must enable promiscuous mode on port groups that are associated with Nexus Dashboard interfaces where External Service IP addresses are specified. vND comprises of Nexus Dashboard management interface and data interface. By default, for LAN deployments, 2 external service IP addresses are required for the Nexus Dashboard management interface subnet. Therefore, you must enable promiscuous mode for the associated port-group. If inband management or Endpoint Locator (EPL) is enabled, you must specify External Service IP addresses in the Nexus Dashboard data interface subnet. You must also enable the promiscuous mode for the Nexus Dashboard data/fabric interface port-group. For NDFC SAN Controller, promiscuous mode must be enabled only on the Nexus Dashboard data interface associated port-group. For NDFC SAN Controller, promiscuous mode only needs to be enabled on the Nexus Dashboard data interface associated port-group. For more information, refer to Cisco Nexus Dashboard Deployment Guide.

To configure promiscuous mode to have multiple persistent IPs reachable on the same port group. See *Cluster Configuration section in Nexus Dashboard Guide.*

The Subscription column allows you to specify which protocol to which the Receiver subscribes. You can choose from SCSI, NVMe, both or none from drop-down list.

Note
If you choose **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 **i** icon in the **Switch Name** 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.

Note
If there is more than a single receiver for an example in a cluster mode, click dropdown icon next to the receiver to select required receiver.

Step 5 Click **Next**. The switches that are capable of streaming analytics are listed in the **Select Switches** page.

Step 6 Select the switches on which SAN Insights must be configured.

Note
Both SAN Controller and Switch time are recorded and displayed when you navigate to the **Select Switches** page. This helps you to ensure that the clocks of SAN Controller and switch are in sync.

Choose single or multiple switches, click **Actions** > **Disable Analytics** to clear all the analytics and telemetry configuration on the selected switches.

Compact GPB streaming configuration for SAN Insights is supported. To stream using Compact GPB, the old KVGPB streaming must be disabled and removed before configuring SAN Insights, newly after the upgrade.

In the **Install Query** column, type of port per switch is displayed. The port types are:**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
ISL based queries must be added when you use the ISL query installation type for the switches that has connected to storage (storage-edge switches).

Note
SAN Controller 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.

When the administrator selects the ISL\Host\Storage on the configure wizard, the respective ports are filtered and listed on the next step.

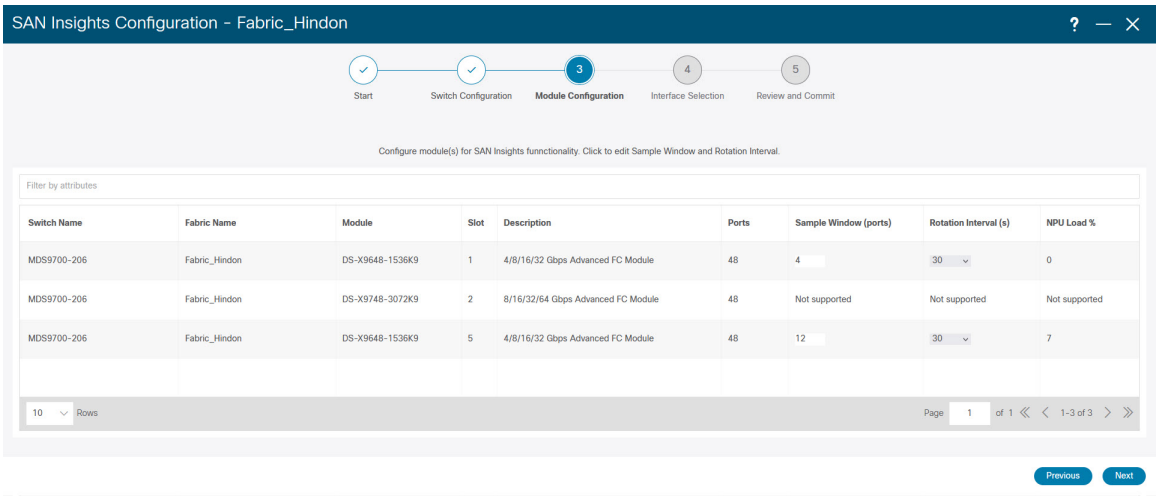
Step 7 Click **Next**.

You can see all the analytics supported modules on the switches selected in the previous view, listed with the respective instantaneous NPU load in the last column. Port-sampling configuration (optional) and port-sampling rotation interval 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.

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.

Step 8 In the **Module Configuration** tab, configure the module(s) for SAN Insights functionality.

Beginning with Release 12.1.1e, Cisco NDFC supports discovery of 64G modules and can be selected during SAN Insights configuration. 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.



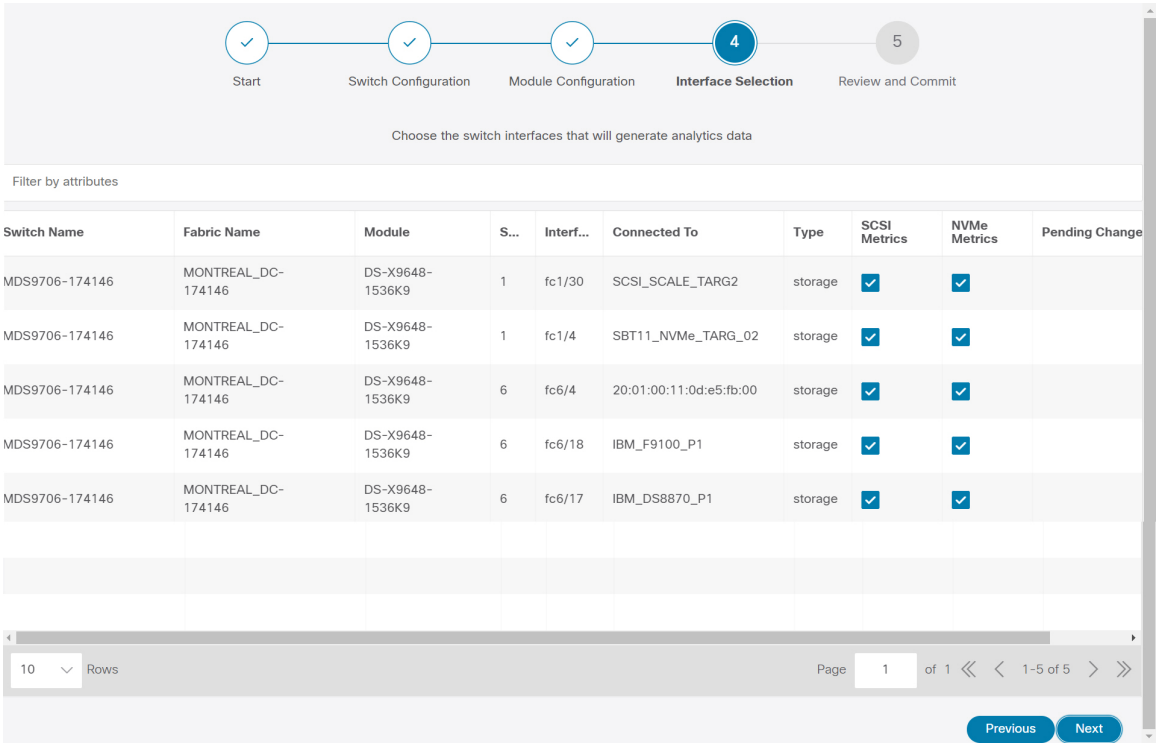
To change the values for **Sample Window (ports)** and **Rotation Interval (seconds)**, click the row and enter the desired values.

- To undo the changes, click **Cancel**.
- To save changes, click **Save**.

The **NPU Load** column displays the network processing unit (NPU) within a module.

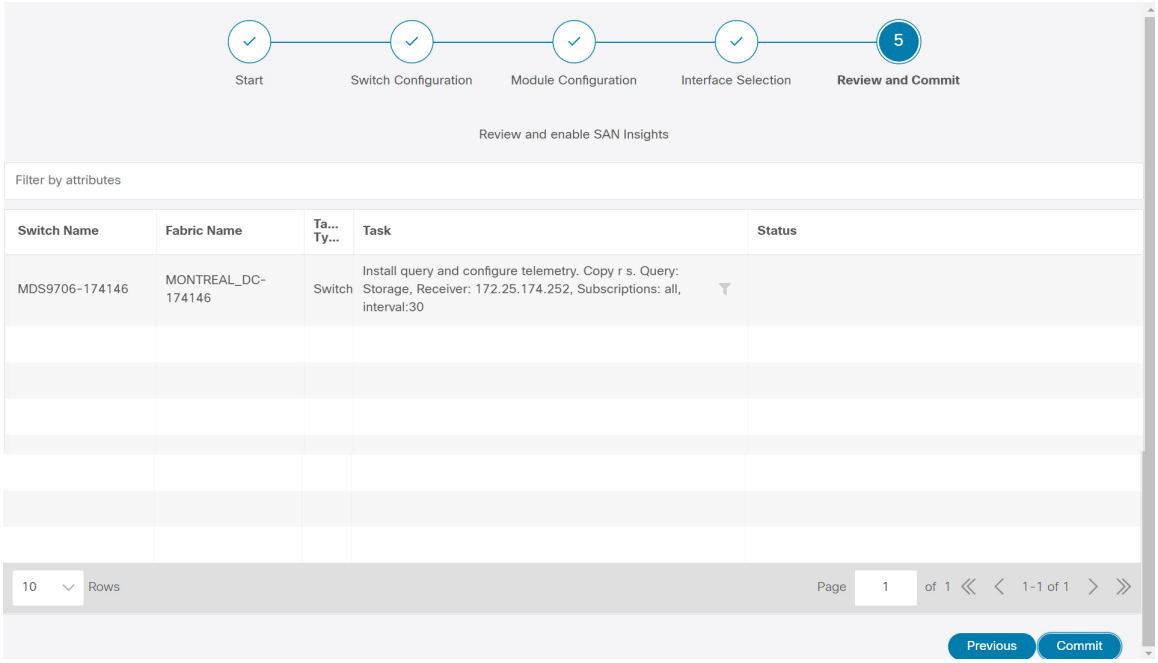
Step 9 Click **Next**.

Step 10 In the **Interface Selection** tab, select the interfaces that generate analytics data within the fabric.



For each interface, you can enable or disable metrics. Choose check box in SCSI Metrics and NVMe Metrics column to enable or disable analytics on the desired port.

Step 11 Click **Next**, and then review the changes that you have made.



Step 12 Click **Commit**. The CLI is executed on the switch.

Step 13 Review the results and see that the response is successful.

Note
Some SAN Insights window can take up to 2 hours to display data.

Step 14 Click **Close** to return to the home page.

Close icon appears only after all CLI commands are executed on the switch.

Navigate to the **SAN** > **Fabrics** or topology page again, to modify the SAN Insights configurations.

Configuring Fabric Backup

You can configure backup for selected fabric, from Fabric window, similarly you can configure backup on **Fabric Overview** window. Choose **Fabric Overview** > **Actions** on main window, click **Configure Backup**.

You can back up all fabric configurations and intents automatically or manually. You can save configurations in SAN Controller, which are the intents. The intent may or may not be pushed on to the switches.

SAN Controller doesn't back up the following fabrics:

- External fabrics in monitor-only mode: You can take a backup of external fabrics in monitor-only mode, but can't restore them. You can restore this backup when the external fabric isn't in monitor-only mode.

- Parent MSD fabric: You can take backups of MSD fabrics. When you initiate a backup from the parent fabric, the backup process is applicable for the member fabrics as well. However, SAN Controller stores all the backed-up information of the member fabrics and the MSD fabric together in a single directory.

The backed-up configuration files can be found in the corresponding directory with the fabric name. Each backup of a fabric is treated as a different version, regardless if it is backed up manually or automatically. You can find all versions of the backup in the corresponding fabric directories.

You can enable scheduled backup for fabric configurations and intents.

The backup has the information related to intent and fabric configurations in addition to associated state of the resource manager in terms of used resources on fabrics. SAN Controller backs up only when there's a configuration push. SAN Controller triggers the automatic backup only if you didn't trigger any manual backup after the last configuration push.

Golden Backup

You can now mark the backups that you don't want to delete even after you reach the archiving limit. These backups are the golden backups. You can't delete golden backups of fabrics. However, SAN Controller archives only up to 10 golden backups. You can mark a backup as golden backup while restoring the fabric. To mark a backup as golden backup, perform the following steps from the Web UI:

Procedure

Step 1 Choose a fabric and choose **Fabrics > Fabric Overview > Backup**.

The **Backup** tab appears.

Step 2 On main window, choose **Actions** > **Configure Backup**.

The **Scheduled Archive** window appears.

Step 3 Choose the time period from where you want to choose the backup.

Valid values are **1m**, **3m**, **6m**, **YTD**, **1y**, and **All**. You can zoom into the graph. By default the backup information for **1m**, which is one month, appears. You can also choose a custom date range. The backup information includes the following information:

- Backup date
- Total number of devices
- Number of devices in sync
- Number of devices out of sync

Step 4 Choose the backup you want to mark as golden by clicking the backup.

You can choose the automatic or manual backup. These backups are color-coded. Automatic backups are indicated in blue color. Manual backups are indicated in midnight blue color. Golden backups are indicated in orange color. The automatic backups have only the versions in their names. Whereas the manual backups have tag names, which you gave when you initiated a manual backup, along with the version in the backup name. Hover over a backup to see the name. The automatic backup is initiated from the **Backup** tab in the

Fabric Overview window. The manual backup is initiated by clicking **Backup Now** from the **Actions** pane in the backup tab.

Step 5 Navigate to switch window, choose check box for required switch name, choose **Switch** > **Switch Overview** > **Backup** > **Actions** > **Mark as golden backup** to mark golden backup.

A confirmation dialog box appears.

Step 6 Click **Yes**.

Step 7 Continue with rest of the fabric restore procedure as mentioned in the *Restoring Fabrics* section or exit the window.

Fabric Overview

The **Actions** drop-down list at the Fabric level allows you to Configure backup, Refer Configuring Fabric Backup, on page 43 for more information.

Fabric Overview contains tabs that allows you view and perform the below operations on the fabric:

Fabric Summary

Click on a fabric to open the side kick panel. The following sections display the summary of the fabric:

- **Health** - Shows the health of the Fabric.
- **Alarms** - Displays the alarms based on the categories.
- **Fabric Info** - Provides basic about the Fabric.
- **Inventory** - Provides information about Switch Configuration and Switch Health.

Click the **Launch** icon to the right top corner to view the Fabric Overview.

Switches

The following table describes the fields that appear on **Switches** window.

Field	Description
Switch Name	Specifies name of the switch.
IP Address	Specifies IP address of the switch.
Fabric Name	Specifies the associated fabric name for the switch.
Status	Specifies the status of the switch.

Field	Description
Health	Specifies the health status of the switch. The following are health status: • Healthy • Critical • Warning • OK
Ports	Specifies the total number of ports on switch.
Used Ports	Specifies the total number of used ports on switch.
Model	Specifies the switch model.
Serial Number	Specifies the serial number of the switch.
Release	Specifies the release number of the switch.
Up Time	Specifies the switch up time details.

The following table describes the action items, in the Actions menu drop-down list, that appear on **SAN > Switches > Switches**.

Action Item	Description
Device Manager	You can log in to Device Manager for required switch. The **Device Manager** login window appears, enter credentials and log in. See Device Manager, on page 263 to view descriptions and instructions for using the Cisco MDS 9000 Device Manager.
Tech Support	Allows you to initiate log collection. For more information, see Tech Support, on page 72.
Execute CLI	Allows you to run multiple CLI commands on multiple switches and collect output as zipped text file for each switch. For more information, see Execute CLI, on page 72.

Modules

To view the inventory information for modules from the SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN > Switch > Switch Overview > Modules**. Similarly you can view modules from fabric overview window, **SAN > Fabric > Fabric Overview > Modules**

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

You can view required information in table, enter details in **Filter by Attributes**.

Step 2 You can view the following information.

- **Name** displays the module name.
- **Model** displays the model name.
- **Serial Number** column displays the serial number.
- **Type** column displays the type of the module.
- **Oper. Status** column displays the operation status of the module.
- **Slot** column displays the slot number.
- **HW Revision** column displays the hardware version of the module.
- **Software Revision** column displays the software version of the module.
- **Asset ID** column displays the asset id of the module.

Viewing Interface

UI Path: **SAN** > **Switch** > **Switch Overview** > **Interface**

Similarly you can view interface on fabric overview window.

SAN > **Fabric** > **Fabric Overview** > **Interface**

The following table describes the fields that appear on the **Interfaces** tab.

Field	Description
Name	Specifies the interface name.
Admin. Status	Specifies the administration status of the interface.
Oper. Status	Specifies the operational status of the interface.
Reason	Specifies the reason for failure.
Speed	Specifies the speed of the interface in Gbs.
Mode	Specifies the mode of the interface.
Switch	Specifies the name of the switch.
VSAN	Specifies the name of the connected VSAN.
Connected To	Specifies the connection details.
Connected To Type	Specifies the type of connection.

Field	Description
Description	Specifies the details about the interface.
Owner	Specifies the port owner name.
Port Group	Specifies the port group number for the interface connected.

To perform various operations on the inventory tab, follow the below procedures:

Procedure

Step 1 To perform no shutdown for an interface, select the check box for the required interface and choose **Actions** > **No Shutdown**.

A warning window appears, click **Confirm**.

Step 2 To shutdown an interface, select the check box for the required interface and choose **Actions** > **Shutdown**.

A warning window appears, click **Confirm**.

Step 3 To assign a port owner for an interface, do the following:

a) Select the check box for the required interface and choose **Actions** > **Owner**.

b) In the **Set Port Owner** dialog box that appears, enter a required name and click **Apply**.

Step 4 To set up diagnostic for an interface, select the check box for the required interface and choose **Actions** > **Link Diagnostics**.

VSANs

You can configure and manage Virtual SANs (VSANs) from Cisco Nexus Dashboard Fabric Controller. From the menu, choose **Virtual Management > VSANS** to view VSAN information. You can view or configure VSAN for the discovered fabrics, with either **Manageable** or **Manage Continuously** status. For a 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 Series 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 Nexus Dashboard Fabric Controller does not discover, nor display any suspended VSAN.

The VSANs tab displays the following fields.

Field	Description
VSAN Name	Displays the VSAN name. 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 • ISLs • Host Ports • Storage Ports • Attributes • Domain ID • VSAN Membership
VSAN ID	Specifies the VSAN ID.
Segments	Specifies the Segments on this VSAN. Click on segments to open a slide-in pane to view summary information about each segment.
Status	Specifies if VSAN is **Up** or **Down**.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Fabrics Overview** > **VSANs** tab.

Action Item	Description
Create VSAN	Allows you to launch wizard to create VSAN. For more information, click Create VSAN Wizard, on page 50.
Delete VSAN	Select the VSAN and click Delete VSAN to delete the VSAN. For more information, click Delete VSAN, on page 53.

Note When changing VSAN of the Switch port in Nexus Dashboard Fabric Controller, If the port was associated with Isolated VSAN, then the previous VSAN column will be blank.

For description on all fields that appear on the tabs, refer Field and Descriptions for VSANs, on page 53.

This section includes the following topics:

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 workflow includes:

- Specify VSAN ID and name.
- Select Switches.
- Specify VSAN attributes.
- Specify VSAN Domain.
- Specify VSAN Members.

Choose **Virtual Management > VSANS**. After you select a Fabric from the drop-down list, click **Create New VSAN** icon. The Welcome screen of the wizard is displayed.

Note Ensure that the VSAN is not already created.

To create and configure VSANs from the Cisco Nexus Dashboard Fabric Controller 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 is not already created. Do not create the VSAN in suspended state.

Note The suspended VSANs are not managed.

Procedure

Step 1 In the 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 VSAN 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 the FICON check box to enable FICON on the switch.
e) Click Next.

Step 2 In the Select Switches screen, click the check box next to the Switch Name, to create the VSAN.

If the switch name is grayed out, it implies that the switch is already part of a 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 3 In the Configure VSAN Attributes screen, configure the VSAN attributes.

Note
If you create a VSAN in a suspended state, it doesn't appear on the Cisco Nexus Dashboard Fabric Controller as it doesn't manage suspended VSANs.

a) In Load Balancing, select the load balancing type to be used on the VSAN.

The following types are available:

- Src ID/Dest ID: Based on only source ID (Src_ID) and destination ID (Dest_ID).
- Src ID/Dest ID/Ox ID (default): Originator exchange ID (Ox_ID) is also used for load balancing, in addition to Src_ID and Dest_ID. 0x_ID is an exchange ID assigned by the originator Interconnect Port for an exchange with the target Interconnect Port.

Note
Src ID/Dest ID/0x ID is the default Load Balancing type for non-FICON VSAN and it isn't available for FICON VSAN, Src ID/Dest ID is the default for FICON VSAN.

b) In InterOp, select an interoperability value.

The InterOp value is used to interoperate with different vendor devices. You can choose from one of the following:

- Default: implies that the interoperability is disabled.
- InterOp-1: implies that the VSAN can interoperate with all the Fibre Channel vendor devices.
- InterOp-2: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-3: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-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 Admin State, 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
  Nexus Dashboard Fabric Controller doesn't manage a suspended VSAN, and therefore it does not appear in the VSAN scope.

d) Check the InOrder delivery check box 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) Check the Add Fabric Binding DB check box if you want to enable the fabric binding for the FICON VSAN.

If the check box is selected, all the peers in the selected switches are added to each switch in the selected list.

f) Check the All Port Prohibited check box if you want to prohibit all the ports for FICON VSAN.

If the check box is selected, the FICON VSAN is created as all Ports prohibited, by default.

g) Click **Next**.

Step 4 In the Configure VSAN Domain screen, configure the static domain IDs for FICON VSAN.

a) Check the Use Static Domain IDs check box 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 **Automatically 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 5 In the Configure Port 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 6 In the Review screen, verify if you have configured the VSAN correctly.

Click **Previous** to navigate to the earlier screen and modify 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 Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Virtual Management > VSANS**.

The **VSANS** window is displayed.

Step 2 From the Select a 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 VSANS area.

Step 3 Expand the Fabric and click the delete icon next to the VSAN.

The Delete VSAN screen appears, showing the switches associated with the VSAN.

Note
You can't delete Segmented VSAN.

Step 4 Select the check box of the Switch for which you want to remove the VSAN.

Click **Delete VSAN**.

A confirmation window appears.

Step 5 Click **Confirm** to confirm the deletion or click **Cancel** 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 **Virtual Management > VSANS** are explained in the following tables.

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 7: 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. Click **Show more Details** to view complete information.

Field	Description
Domain ID	Specifies an insistent domain ID.
VSAN WWN	Specifies the world wide name (WWN) of the VSAN.
Principal WWN	Specifies the world wide 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.
Up Time	Specifies the time from which the switch is up.

ISLs Tab

This tab displays information about the ISLs about the switches in the VSAN scope. 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, Nexus Dashboard Fabric Controller 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 8: Field and Description on ISL 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.
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 the ISL is a Port Channel.
Additional Info	Additional information for this ISL, such as, TE/TF/TNP ISL.

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 9: Field and Description on Host Ports Tab

Field	Description
Enclosure	The name of the enclosure.
Device Alias	The device alias of this entry.

Field	Description
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.
Serial Number	Specifies the serial number of the enclosure.
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.

Storage Ports 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 10: Field and Description on Storage 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.

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 11: 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. • vsanLoadBalancing • InterOp • Inorder Delivery After modify the attributes, you can click **Save** to save changes or **Cancel** to discard.
Switch Name	Displays the name of the switch that is associated with the VSAN.
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. • **Down** 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 Nexus Dashboard Fabric Controller as well.
Oper	The operational state of the VSAN.
MTU	Displays the MTU for the switch.
Load Balancing	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/Oxld—use source, destination, and exchange IDs
InterOp	The interoperability mode of the local switch on this VSAN. • default • interop-1 • interop-2 • interop-3

Field	Description
Inorder Delivery	The Inorder Delivery 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.

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 12: Field and Description on Domain ID Tab

Field	Description
Edit	Select a switch and click the 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	Specifies the configuration.
Config Type	Specifies the usage of the domain ID type—**preferred** or **static**.
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 13: Field and Description on VSAN Membership Tab

Field	Description
Edit	Select a switch and click the Edit icon to modify Port VSAN Membership for selected VSAN and selected switch. Port VSAN Membership is presented by different types including FC (physical), Port Channel, 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

Device Aliases

A device aliases 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.

The following table describes the fields that appear under **Device Aliases** tab.

Field	Description
Switch	Displays the device alias switch name.
Device Alias	Displays the alias retrieved from the switch.
pWWN	Displays the port WWN

This section contains the following:

Configuring Device Aliases

Click a required Fabric from Fabrics table, a Slide-in panel is displayed. Click Launch icon to view Fabric Overview window, and click **Device Aliases** tab.

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 SAN Controller Web UI, the fabric must be configured as Device Alias enhanced mode.

To add, or edit, or delete device aliases, perform the following steps:

Procedure

Step 1 Choose check box next to the switch column for which you need to add the device alias

a) Click **Actions > Add device alias**.

The **Add device alias** windows appears.

All the provisioned port WWNs are populated in the table.

b) Enter a device alias name in the **Device Alias** field to indicate to create a device alias for the selected pWWN.
c) Click **Save** to exit the inline editor mode.
d) 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 **+** icon of Pre-provision device aliases to create a new table row in inline editor mode.
b) In the **pWWN** field, enter the non-provisioned port WWN and device alias 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 2 To edit the device alias, choose the check box next to the switch column, and then click **Actions > Edit device aliases**.

Note
You can select multiples switches to edit device aliases.

The **Edit device aliases** windows appears.

All the selected port WWNs are populated in the table.

a) Click **Edit** icon next to the pWWN column.
b) Enter a required device alias name in the Device Alias field and click **tick** icon to save the name.
c) Repeat the same procedure to edit other device alias names.
d) Click **Apply** to save edited device aliases to the switches.

Note
When you rename a device alias, a warning message appears that editing device alias causes traffic interruption and to review the zone member type. For Cisco NX-OS Releases in:

- 7.x releases - before 7.3(0) releases
- 6.x releases - before 6.2(15) releases

e) Click **Cancel** to discard changes or click **Confirm** to save changes.

Step 3 Choose check box next to the switch column for which you need to delete the device alias.

a) Click **Actions** > **Delete device alias**.

A confirmation window appears.

Note
Deleting the device alias may cause traffic interruption.

b) Click **Yes** to delete the device alias.

Step 4 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 a 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 created. In case of failure, you must troubleshoot and fix the problem.

CFS

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.

The following table describes the columns that appears on **CFS** tab:

Fields	Descriptions
Switch	Specifies the name of switch.
Feature	Specifies the feature on the switch.
Last Action	Specifies the last action performed on the switch.
Result	Specifies the action performed is success or unsuccessful.
Lock Owner Switch	Specifies whether the switch is locked or not.
Lock Owner User	Specifies the user role name if the switch is locked.
Merge Status	Specifies the merge status of the switch.

To view CFS information from the SAN Controller Web UI, perform the following steps:

Procedure

Step 1 To commit the CFS configuration, choose the **Switch** radio button, click **Commit**.

The CFS configuration for this switch is committed.

Step 2 To abort the CFS configuration, choose the **Switch** radio button, click **Abort**.

The CFS configuration for this switch is aborted.

Step 3 To clear the lock on the CFS configuration, choose 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.

Event Analytics

Event Analytics includes the following topics:

- Alarms, on page 171
- Events, on page 181
- Accounting, on page 185

Performing Backup actions

The following table describes the columns that appears on **Backup** tab.

Fields	Descriptions
Switch	Specifies the name of switch.
Backup Date	Specifies the backup date.
Backup Tag	Specifies the backup name.
Backup Type	Specifies the backup type, whether it is a golden backup.
Configuration Files	Specifies the configuration files details.

The following table describes the fields and descriptions that appears on **Action** tab.

Actions	Descriptions
Backup now	• Choose **Backup now**. The **Create new backup** window appears. • Enter name in **Backup tag** field. If required choose check box **Mark backup as golden**. For more information on golden backup, refer to Golden Backup, on page 44. • Click **OK**.
Copy to bootflash	Choose **Copy to bootflash**. A confirmation window appears, click **OK**. For more information on bootflash, check Copy Bootflash, on page 83.

Actions	Descriptions
Compare	Choose required switch names to compare configuration of switches, choose **Compare**. You can select only two switches at an instance. **Compare Config** window appears, displaying the difference between the two configuration files. The Source and Target configuration files content is displayed in two columns 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.
Export	Click **Export**. 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.
Edit tag	Click **Edit tag** to change the backup tag name.
Mark as golden	To mark existing backup as golden backup, choose **Mark as golden**, a confirmation window appears, click **Confirm**.
Remove as golden	To remove existing backup from golden backup, choose **Remove as golden**, a confirmation window appears, click **Confirm**.
Delete	To delete existing backups, choose **Delete** a confirmation window appears, click **Confirm**. **Note** • If you have marked backup as golden backup. make sure that the golden backup is removed, else error appears you can't delete existing backup. • You can delete one backup at a time.

Viewing of Port Usage

You can view the following information on Port Usage tab.

- **Port Speed** column displays the speed of the port.
- **Used Ports** column displays the total ports with the mentioned port speed.
- **Available Ports** column displays the available ports for the port speed.
- **Total Ports** column displays the total ports with the mentioned speed.
- **Estimated Day Left** column displays the estimated days left for the ports.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

Used ports displays the total used ports for the selected switch.**Total ports** displays the total available ports for the selected switch.

Metrics

The Metric tab displays the infrastructure health and status. You can view CPU utilization, Memory utilization, Traffic, and Temperature details.

The following table describes the columns that appears on **CPU** and **Memory** tab.

Fields	Descriptions
Switch Name	Specifies the name of switch.
IP Address	Specifies the switch IP address.
Low Value (%)	Specifies the lowest CPU utilization value on the switch.
Avg. Value (%)	Specifies the average CPU utilization value on the switch.
High Value (%)	Specifies the high CPU utilization value on the switch.
Range Preview	Specifies the linear range preview.
Last Update Time	Specifies the last updated time on the switch.
Show last day	Click **Show last day** to view data for selected day, week, month, and year.

The following table describes the columns that appears on **Traffic** tab.

Fields	Descriptions
Switch Name	Specifies the name of switch.
Avg. Rx	Specifies the average Rx value.
Peak Rx	Specifies the peak Rx value.
Avg. Tx	Specifies the average Tx value.
Peak Tx	Specifies the peak Tx value.
Avg. Rx+Tx	Specifies the average of Rx and Tx value.
Avg. Errors	Specifies the average error value.
Peak Errors	Specifies the peak error value.
Avg. Discards	Specifies the average discard value.
Peak Discards	Specifies the peak discard value.
Last Update Time	Specifies the last updated time.
Show last day	Click **Show last day** to view data for selected day, week, month, and year.

The following table describes the columns that appears on **Temperature** tab.

Fields	Descriptions
Switch Name	Specifies the name of switch.
IP Address	Specifies the switch IP address.
Temperature Module	Specifies the module of temperature.
Low Value (C)	Specifies the lowest temperature value.
Avg. Value (C)	Specifies the average temperature value.
High Value (C)	Specifies the high temperature value.
Show last day	Click **Show last day** to view data for selected day, week, month, and year.

Congestion Analysis

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

To enable SAN Congestion to collect statistics on ports, navigate to **Server Settings** > **PM** and check **Slowdrain Collect on All Ports** check box.

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

Procedure

Step 1 Choose **SAN > Fabrics**.

Step 2 From the list of Fabrics, double click on the fabric to view **Fabric Summary**.

Click **Congestion Analysis** tab.

Step 3 Select a fabric from the **Fabric** drop-down list.

Step 4 From the **Duration** drop-down list, select **Once** or **Daily** for the scheduled job. **Once** includes intervals such as 10 minutes, 30 minutes, 1 hour, and custom hours and runs 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.

Step 5 Click **Start Analysis** to begin polling.

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

Step 6 Click **Stop Analysis** 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 7 The **Fabric**, **Status** of polling, **Start**, **End**, and **Duration** columns for each fabric is displayed.

Step 8 Select a fabric and click **Delete All** or **Stop** to delete or stop a job respectively.

A detailed view of the fabric will appear when you click a fabric name and displays Congestion details for the fabric. See Congestion Visualization, on page 65 for more information.

Step 9 Click a switch name in the **Switch Name** column of the **Device Interfaces** table to display the switch's health.

Step 10 Click an interface name in the **Interface** column of the **Device Interfaces** table to display the slow drain value for the switch port in a chart format.

Use the **Filter by attributes** option to display the details based on the defined value for each column.

Select the **Only Rows With Data** option to filter and display the nonzero entries in the statistics.

Congestion Visualization

A topology of the selected fabric appears when you click a fabric name and displays Congestion details for the fabric. 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 more information. The links and switches are color-coded. Enable performance collections and SNMP traps to view the Congestion information on the topology.

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

Table 14: Color Description

Color	Name	Description
Blue (light)	High Utilization	High utilization tx-datarate >= 80%
Green	Normal	No Congestion 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 Congestion 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 Congestion. The color around the number represents the highest level Congestion that is found on F ports of the switch. Click the switch to see more Congestion details.

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

Note The highest Congestion level a link can have is **Level 3**. Valid colors for a link are Green, Red, Orange, Yellow (dark), Yellow (light), and Gray (light).

DIRL

Dynamic Ingress Rate Limiting (DIRL) is used to automatically limit the rate of ingress commands and other traffic to reduce or eliminate the congestion that is occurring in the egress direction. DIRL does this by reducing the rate of IO solicitations such that the data generated by these IO solicitations matches the ability of the end device to process the data without causing any congestion. As the device's ability to handle the amount of solicited data changes, DIRL, will dynamically adjust seeking to supply it with the maximum amount of data possible without the end device causing congestion. After the end device recovers from congestion, DIRL will automatically stop limiting the traffic that is sent to the switch port.

In case of slow drain and over utilization, the assumption is that if the rate of IO solicitation requests is reduced then this will make a corresponding reduction in the amount of data solicited and being sent to the end device. Reducing the amount of data will resolve both the slow drain and over utilization cases.

DIRL is comprised of two functions and can perform equally well on congestion caused both slow drain and over utilization:

- **Port monitor**: Detects slow drain and overutilization conditions and if the port guard action is set as DIRL, it notifies FPM. Port monitor port guard action DIRL can be configured on the following counters:
  - **txwait**: Use for detection of slow drain.
  - **tx-datarate**: Used for detection of overutilization.
  - **tx-datarate-burst**: Use for detection of overutilization.
- **FPM**: DIRL actions are taken by FPM as notified by port monitor. On detecting a rising threshold from port monitor, FPM does rate reduction causing the rate of ingress traffic to be reduced. On detecting the value of a counter being below the falling threshold continuously for the DIRL recovery interval, FPM does rate recovery.

After the port monitor policy is configured with the DIRL portguard action and activated, all non- default F ports are monitored by default, and FPM is notified if congestion is detected on any of these ports. However, you can manually exclude certain interfaces from being monitored.

The following are the different transition states of DIRL:

- **Normal**: The state in which a port is functioning normally and state before it enters DIRL Rate Reduction. After full recovery, the port returns to the Normal state.
- **DIRL Rate Reduction**: The state in which an event rising threshold triggers the DIRL rate reduction process.
- **DIRL Rate Reduction Maximum**: The state in which the DIRL rate reduction has reached its maximum value and more rising thresholds events are detected.

- **DIRL Status**: The state in which an event below the rising threshold and above the falling threshold is detected. This state will transition to the DIRL Recovery state when an event below the falling threshold is detected for the configured recovery-interval.
- **DIRL Rate Recovery**: The state in which the DIRL rate recovery happens on detecting an event below the falling threshold for the configured recovery-interval. This state will transition to the Normal state after the port recovers completely from DIRL.

  This state is a recurring state and there will be multiple rate recoveries before the ports are completely recovered from DIRL. This state will transition to the DIRL Stasis state when an event below the rising threshold and above the falling threshold is detected.

The following are the actions that are initiated by DIRL depending on the type of event detected on the port:

Note The events are listed in reverse chronological order with the most current event at the top.

- An event rising threshold is detected on the port and DIRL is initiated for the port. The port ingress traffic rate is reduced to 50% of its current rate.
- In the next polling interval, the recovery-interval expires without detecting a rising threshold. The port ingress traffic is increased by 25% of its current capacity.
- In the next polling interval, the recovery-interval expires without detecting a rising threshold. The port ingress traffic is increased by 25% of its current capacity..
- In the next polling interval, the recovery-interval expires without detecting a rising threshold. The port ingress traffic is increased by 25% of its current capacity.
- In the next polling interval, the recovery-interval expires without detecting a rising threshold. The port ingress traffic is increased by 25% of its current capacity.
- In the next polling interval, an event rising threshold is detected on the port, and DIRL is initiated for the port. The port ingress traffic is reduced again to 50% of its current rate.

DIRL Congestion Management Visualization

Dynamic Ingress Rate Limiting (DIRL) analysis is an on-demand job executed on the selected Fabric. It displays the DIRL status and events on all the switches in the fabric. The following commands are executed on the switches and the output is collected as a snapshot.

- **show fpm ingress-rate-limit status**
- **show fpm ingress-rate-limit events**

Note DIRL Visualization is supported on Cisco MDS Series switches with Release 9.2(1) and later.

To view the DIRL analysis on Cisco NDFC SAN Controller UI, perform the following:

1. Choose **SAN** > **Fabrics**.
2. From the list of Fabrics, double click on the fabric to view **Fabric Summary**.

Click **DIRL** tab.

3. Click **Start DIRL data collection** to begin collection.

   Click **Cancel/Abort** to stop the collection.

A status message appears to show that the collection is in progress. It also displays the time stamp at which the analysis began. After the Analysis is complete, information is populated in the table below. A status message appears to indicate that the collection is complete. It also displays the time stamp at which the analysis was completed.

An entry in the table below shows that following fields:

Field	Description
Switch	Specifies the switch on which the analysis is collected. Click on the Switch to view a slide-in pane displaying the summary. Click on the launch icon to view **Switch Overview**.
Interface	Specifies the interface on which the analysis is collected. Click on the interface to view the **Rate Limit events**. The table displays the events of this interface from the CLI command output **show fpm ingress-rate-limit events**.
Current rate limit (%)	Specifies the % indicating the current rate limit.
Previous action	Specifies the previous action performed to control the rate limit.
Last updated time	Displays the time stamp at which the event occurred.

Click **DIRL Past Events** to view the DIRL events for all the interfaces in this fabric, except the current DIRL interfaces. The table displays events from CLI command output **show fpm ingree-rate-limit events**.

Rate Limit Events

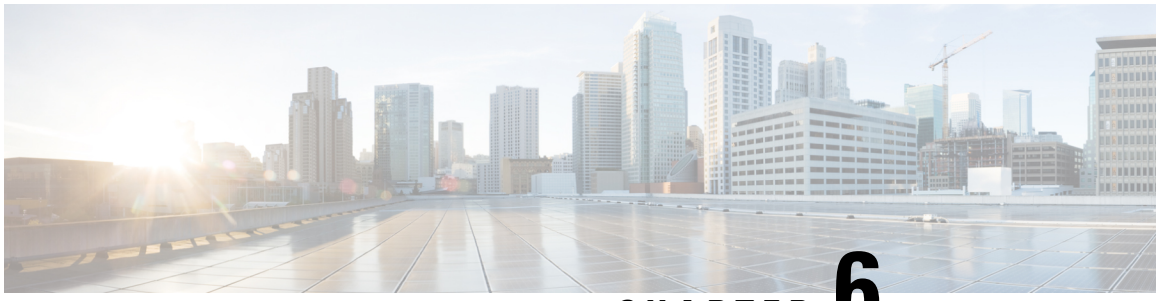
Double click on the Fabric to view the **Fabric Overview**. On the **DIRL** tab, after the DIRL status is collected on the switches, the data is displayed in the table below.

Click **DIRL Events** in the Interface column to view the rate limit events for that interface on the switch.

The following table provides information about the fields and table items that appear on this screen.

Field	Description
Fabric	Specifies the Fabric to which the switch belongs.
Switch	Specifies the fabric for which the DIRL congestion is visualize
Interface	Specifies the interface on which the events are visualized.
Last collection at	Specifies the date and time at which the DIRL status was colle
Counter	Specifies if the counter is for **txwait** or **tx-datarate** or **tx-datarate-burst**.
Event	Specifies the event.

Field	Description
Counter Value %	Specifies the value of the counter.
Action	Specifies the action which triggered the event,
Operating port speed (Mbps)	Specifies the speed of the operating port.
Input rate (Mbps)	Specifies the input rate.
Output rate (Mbps)	Specifies the output rate.
Current rate limit (%)	Specifies the current rate limit.
Applied rate limit (%)	Specifies the applied rate limit.
Time	Specifies the time at event was triggered.



CHAPTER 6

Switches

- Switches, on page 71
- Switch Overview, on page 79

Switches

The following table describes the fields that appear on **Switches** window.

Field	Description
Switch Name	Specifies name of the switch.
IP Address	Specifies IP address of the switch.
Fabric Name	Specifies the associated fabric name for the switch.
Status	Specifies the status of the switch.
Health	Specifies the health status of the switch. The following are health status: • Healthy • Critical • Warning • OK
Ports	Specifies the total number of ports on switch.
Used Ports	Specifies the total number of used ports on switch.
Model	Specifies the switch model.
Serial Number	Specifies the serial number of the switch.
Release	Specifies the release number of the switch.
Up Time	Specifies the switch up time details.

The following table describes the action items, in the Actions menu drop-down list, that appear on **SAN > Switches > Switches**.

Action Item	Description
Device Manager	You can log in to Device Manager for required switch. The **Device Manager** login window appears, enter credentials and log in. See Device Manager, on page 263 to view descriptions and instructions for using the Cisco MDS 9000 Device Manager.
Tech Support	Allows you to initiate log collection. For more information, see Tech Support, on page 72.
Execute CLI	Allows you to run multiple CLI commands on multiple switches and collect output as zipped text file for each switch. For more information, see Execute CLI, on page 72.

Device Manager

See Device Manager, on page 263 chapter for descriptions and instructions for using the Cisco MDS 9000 Device Manager.

Note Device Manger session is terminated when you navigate to another tab on the **Switch Overview** screen.

Tech Support

From the **Actions** drop-down list, select **Tech Support** to initiate log collection. A window appears.

- Enter time in **Session timeout** field in minutes, by default time is 20 minutes.
- Enter the command in **Command** text field and click **Run**.
- A confirmation window appears stating 'Data submitted successfully, tech support starting', click **Confirm** and status changes to **Completed**.
- You can download the report, click **Download Tech Support**.

Execute CLI

From Release 12.1.1e, Cisco NDFC SAN Controller allows you to execute CLI commands on switches. You can collect the output from the CLI commands in `.zip` file for each switch.

To execute CLI commands on switches, do the following:

1. On the Cisco NDFC UI, choose **SAN > Switches > Switches**.
2. Select the switches on which you want to execute the CLI commands.

   You can select more than one switch to run the set of CLI commands simultaneously.

3. From the **Actions** drop-down list, choose **Execute CLI** .

   The **Execute Switch CLI** screen is displayed.

4. On the **Configure** tab, click on the hyperlink under **Selected Switches** to view the selected switches on which the CLIs will be executed.

5. In the **CLI Commands** text box, enter the CLI commands to be executed on the switches.

   Ensure that you enter one command per line.

6. Click **Execute**.

   A **Success** confirmation message appears.

7. On the **Execute** tab, the tables displays switch, associated fabric and the CLI execution status.

8. Click on **Download output** to download the command output.

Note If switch is not reachable via CLI then the output in zip file will indicate an error.

Enhanced Role-based Access Control

Starting from SAN Controller Release 12.0.1(a), all RBAC is in Nexus Dashboard. User-roles and access are defined from Nexus Dashboard for fabrics on NDFC.

Nexus Dashboard admin role is considered as Network-admin role in NDFC.

DCNM had five roles to perform various access and operations. If a user is access a fabric with network stage role has access to all other fabrics as a network stage role. Therefore, a username is restricted with their role in DCNM.

Cisco NDFC Release 12.0.1(a) has same five roles but you can do granular RBAC with integration of Nexus Dashboard. If a user accesses a fabric as a network stage role, the same user can access different fabric with other user role such as admin or operator role. Therefore, a user can have different access on the different fabrics in NDFC.

NDFC RBAC supports following roles:

- NDFC Access Admin
- NDFC Device Upgrade Admin
- NDFC Network Admin
- NDFC Network Operator
- NDFC Network Stager

The following table describes the user roles and their privileges in NDFC.

Roles	Privileges
NDFC Access Admin	Read/Write See

Roles	Privileges
NDFC Device Upgrade Admin	Read/Write
NDFC Network Admin	Read/Write
NDFC Network Operator	Read
NDFC Network Stager	Read/Write

The following roles are supported on DCNM for backward compatibility:

- SAN admin (mapped to network-admin)
- Global-admin (mapped to network-admin)
- SAN network-admin (mapped to network-admin)
- Server-admin (mapped to network-admin)



Note In any window, the actions that are restricted by the user role that is logged in are grayed out.

NDFC Network Admin

A user with the **NDFC Network Admin** role can perform all the operations in SAN Controller.

From Cisco Nexus Dashboard Fabric Controller Release 12.1.1e, a user with this role can perform all operations for MSD fabrics in Networks and VRFs.

You can freeze a particular fabric or all fabrics in SAN Controller if you are a user with the **NDFC Network Admin** role.



Note Make sure that the switch user role for discovery or add switches or LAN credentials for NDFC must have the network-admin role.

NDFC Device Upgrade Admin

A user with the **NDFC Device Upgrade Admin** role can perform operations only in **Image Management** window.

See the Image Management section for more information.

NDFC Access Admin

A user with the **NDFC Access Admin** role can perform operations only in **Interface Manager** window for all fabrics.

An NDFC access admin can perform the following actions:

- Add, edit, delete and deploy layer 2 port channels, and vPC.

- Edit host vPC, and ethernet interfaces.
- Save, preview, and deploy from management interfaces.
- Edit interfaces for LAN classic, and IPFM fabrics.

  Apart from nve, management, tunnel, subinterface, SVI, interface grouping, and loopback interfaces

However, a user with the SAN Controller access admin role can't perform the following actions:

- Cannot edit layer 3 port channels, ST FEX, AA FEX, loopback interfaces, nve interfaces, and subinterfaces.
- Cannot edit member interfaces and port channels of Layer 3, ST FEX, AA FEX.
- Cannot edit interfaces with policy associated from underlay and link for easy fabrics.
- Cannot edit peer link port channel.
- Cannot edit management interface.
- Cannot edit tunnel.



Note The icons and buttons are grayed out for this role when the fabric or SAN Controller is in deployment-freeze mode.

NDFC Network Stager

A user with the **NDFC Network Stager** role can make configuration changes on SAN Controller. A user with the **NDFC Network Admin** role can deploy these changes later. A network stager can perform the following actions:

- Edit interface configurations
- View or edit policies
- Create interfaces
- Change fabric settings
- Edit or create templates

However, a network stager cannot perform the following actions:

- Cannot make any configuration deployments to switches.
- Cannot perform deployment-related actions from the SAN Controller Web UI or the REST APIs.
- Cannot access the administration options like licensing, creating more users, and so on.
- Cannot move switches in and out of maintenance mode.
- Cannot move fabrics in and out of deployment-freeze mode.
- Cannot install patches.
- Cannot upgrade switches.

- Cannot create or delete fabrics.
- Cannot import or delete switches.

NDFC Network Operator

A network operator can view fabric builder, fabric settings, preview configurations, policies, and templates. However, a network operator cannot perform the following actions:

- Cannot change expected configurations of any switch within any fabric.
- Cannot deploy any configurations to switches.
- Cannot access the administration options like licensing, creating more users, and so on.

The difference between a network operator and a network stager is that, as a network stager you can only define intent for existing fabrics, but cannot deploy those configurations.

Only a network admin can deploy the changes and edits that are staged by a user with the network stager role.

Choosing Default Authentication Domain

By default login screen on Nexus Dashboard chooses the local domain for authentication. You can change domain at login time by choosing available domains from drop-down list.

Nexus Dashboard supports local and remote authentication. The remote authentication providers for Nexus Dashboard include RADIUS, and TACACS. For more information on authentication support, refer https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-211.pdf.

The following table describes RBAC comparison between DCNM and NDFC access:

DCNM 11.5(x)	NDFC 12.0.x and 12.1.x
• User has a single role. • All APIs and resources are accessed with this single role.	• User can have a different role in different Nexus Dashboard for sec domains. • Security domain contains single Nexus Dashboard, and each Ne Dashboard contains single NDFC Fabric.
A single role is associated with the user by disabling or restricting the access to options in DCNM.	A single role displays only privileged resources on the selected page restricted access are grayed out based on security domain associated selected resource on further options on NDFC.
DCNM AV Pair format with shells, roles, and optional access constraints.	Nexus Dashboard AV Pair format with shells, domains.
Supported roles based on deployment type LAN, SAN, or PMN.	Supported roles such as network-admin, network-operator, device-upg-admin, network-stager, access-admin are in NDFC. Support for legacy roles for backward compatibility. Nexus Dashboa admin role as network-admin of DCNM.

The following table describes DCNM 11.5(x) AV Pair format:

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell Cisco-AV-Pair Value
Network-Operator	shell:roles = "network-operator" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-oper dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1group2 group5"	cisco-av-pair=shell:roles="network-adm dcnm-access="group1 group2 group5"

The following table describes NDFC 12.x AV Pair format:

User Role	AVPair Value
NDFC Access Admin	Access-admin
NDFC Device Upgrade Admin	Device-upg-admin
NDFC Network Admin	Network-admin
NDFC Network Operator	Network-operator
NDFC Network Stager	Network-stager

The AV pair string format differs when configuring a read/write role, read-only role, or a combination of read/write and read-only roles for a specific user. A typical string includes the domain, followed by the read-write roles separated from the read-only roles using the slash (/) character; individual roles are separated by the pipe (|) character:

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

Nexus Dashboard Security Domains

Access control information about a user login contains authentication data like user ID, password, and so on. Based on the authorization data, you can access resources accordingly. Admins in Cisco Nexus Dashboard can create security domains and group various resource types, resource instance, and map them into a security domain. The admins define an AV-pair for each user, which defines the access privileges for users to different resources in Cisco Nexus Dashboard. When you create a fabric, a site is created in Nexus Dashboard with the same fabric name. You can create and view these sites from **Nexus Dashboard > Sites**.

The SAN Controller REST APIs use this information to perform any action by checking the authorization.

Note When accessing REST APIs, you can verify passed payload in JSON format. Ensure that the payload is an appropriate JSON format.

When you upgrade from SAN Controller Release 11.x, each fabric is mapped to an autogenerated site of the same name. All these sites are mapped into the **all** security domain in Nexus Dashboard.

All resources are placed in **all** domain before they are assigned or mapped to other domains. The all security domain does not include all the available security domains in Nexus Dashboard.

AV-Pairs

A group of security domains along with read and write roles for each domain are specified using AV-pairs. Administrators define AV-pair for each user. The AV-pair defines the access privileges to users across various resources in Nexus Dashboard.

The AV-pair format is as follows:

```
"avpair":
"shell:domains=security-domain/write-role-1|write-role-2,security-domain/write-role-1|write-role2/read-role-1|read-role-2"
```

```
For example: "avpair":
```

```
"shell:domains=all/network-admin/app-user|network-operator". "all/admin/" makes user
super-user and it's best to avoid examples with all/admin/"
```

The write role is inclusive of read role as well. Hence, `all/network-admin/` and `all/network-admin/network-admin` are the same.

Note From SAN Controller Release 12.0.1a supports the existing AV-pair format that you created in SAN Controller Release 11.x. However, if you are creating a new AV-pair, use the format that is mentioned above. Ensure that the shell: domains must not have any spaces.

Specifying Cisco NX-OS User Roles and SNMPv3 Parameters on AAA Servers

You can use the VSA cisco-AV-pair on AAA servers to specify user role mapping for the Cisco NX-OS device using this format:

```
shell:roles="roleA roleB …"
```

If you do not specify the role option in the cisco-AV-pair attribute, the default user role is network-operator.

You can also specify your SNMPv3 authentication and Privacy protocol attributes as follows:

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The Privacy protocol options are AES-128 and DES. If you do not specify these options in the cisco-AV-pair attribute, MD5 and DES are the default authentication protocols.

Creating a Security Domain

To create a security domain from Cisco Nexus Dashboard, perform the following steps:

1. Log into Cisco Nexus Dashboard.
2. Choose **Administrative > Security**.
3. Navigate to **Security Domains** tab.
4. Click **Create Security Domain**.
5. Enter the required details and click **Create**.

Creating a User

To create a user from Cisco Nexus Dashboard, perform the following steps:

1. Log into Cisco Nexus Dashboard.
2. Choose **Administrative > Users**.
3. Click **Create Local User**.
4. Enter the required details and click **Add Security Domain**.
5. Choose a domain from the drop-down list.
6. Assign a SAN Controller service read or write role by checking the appropriate check box.
7. Click **Save**.

Switch Overview

UI Path: **SAN** > **Switches** > **Switch Overview**

The Switch Overview menu includes the following sub menus:

Viewing Switch Summary

You can view information about switch along with the switch summary on **Switch Overview** tab. Navigate **SAN** > **Switches**, click on required switch. A slide-in pane appears. Click **Launch** icon to view the **Switch Overview** window.

The following are the default cards that appear in the **Summary** tab:

Card	Description
Switch Information	Displays details of switch such as name, health status, IP address, model, version and other switch information.
Event Analytics	Displays events with **Critical**, **Major**, **Minor**, and **Warning** severity. In this card, click **Launch** icon to navigate to events tab for more information.
Resources	Displays the resource utilization of switch in the graph form.
Modules	Displays the switches on which the modules are discovered, the models name and the count.
Interfaces	Displays the switch interface summary information.
Port Usage	Displays the ports inventory summary information.

Modules

To view the inventory information for modules from the SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN > Switch > Switch Overview > Modules**. Similarly you can view modules from fabric overview window, **SAN > Fabric > Fabric Overview > Modules**

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

You can view required information in table, enter details in **Filter by Attributes**.

Step 2 You can view the following information.

- **Name** displays the module name.
- **Model** displays the model name.
- **Serial Number** column displays the serial number.
- **Type** column displays the type of the module.
- **Oper. Status** column displays the operation status of the module.
- **Slot** column displays the slot number.
- **HW Revision** column displays the hardware version of the module.
- **Software Revision** column displays the software version of the module.
- **Asset ID** column displays the asset id of the module.

Viewing Interface

UI Path: **SAN** > **Switch** > **Switch Overview** > **Interface**

Similarly you can view interface on fabric overview window.

SAN > **Fabric** > **Fabric Overview** > **Interface**

The following table describes the fields that appear on the **Interfaces** tab.

Field	Description
Name	Specifies the interface name.
Admin. Status	Specifies the administration status of the interface.
Oper. Status	Specifies the operational status of the interface.
Reason	Specifies the reason for failure.
Speed	Specifies the speed of the interface in Gbs.
Mode	Specifies the mode of the interface.
Switch	Specifies the name of the switch.

Field	Description
VSAN	Specifies the name of the connected VSAN.
Connected To	Specifies the connection details.
Connected To Type	Specifies the type of connection.
Description	Specifies the details about the interface.
Owner	Specifies the port owner name.
Port Group	Specifies the port group number for the interface connected.

To perform various operations on the inventory tab, follow the below procedures:

Procedure

Step 1 To perform no shutdown for an interface, select the check box for the required interface and choose **Actions** > **No Shutdown**.

A warning window appears, click **Confirm**.

Step 2 To shutdown an interface, select the check box for the required interface and choose **Actions** > **Shutdown**.

A warning window appears, click **Confirm**.

Step 3 To assign a port owner for an interface, do the following:

a) Select the check box for the required interface and choose **Actions** > **Owner**.
b) In the **Set Port Owner** dialog box that appears, enter a required name and click **Apply**.

Step 4 To set up diagnostic for an interface, select the check box for the required interface and choose **Actions** > **Link Diagnostics**.

Viewing Switch Licenses

You can view the following information on Licenses tab.

- **Feature** column displays the feature names of the selected switch.
- **Status** column displays the status of licenses. Status will be either **In Use** or **Unused**.
- **Type** column displays the type of the licenses.
- **Warnings** column displays the grace period of licenses and its expiry date.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

Event Analytics

Event Analytics includes the following topics:

- Alarms, on page 171
- Events, on page 181
- Accounting, on page 185

Viewing Backup

You can view the following information on Backup tab.

- **Switch** column displays the switch name.
- **Backup Date** column displays the backup date.
- **Backup Tag** column displays the backup tag name.
- **Backup Type** column displays the type of backup.
- **Configuration File** column displays the configuration files that are archived for that device.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

The following table describes the actions you can perform in this tab:

Action	Description
Copy to bootflash	Refer to Copy Bootflash, on page 83.
Compare	Refer to Compare.
Export	Refer to Export.
Edit tag	To edit a tag of a switch. Choose check box for a required switch, choose **Actions** > **Edit tag** and click **OK**.
Mark as golden	To mark switch as a golden backup. Choose check box for a required switch, choose **Actions** > **Mark as golden**. A confirmation window appears, click **Confirm**. Refer to Golden backup section for more information.
Remove as golden	To remove switch from a golden backup. Choose check box for a required switch, choose **Actions** > **Remove as golden**. A confirmation window appears, click **Confirm**.

Action	Description
Delete	To delete switch from a backup. Choose check box for a required switch, choose **Actions** > **Delete**. A confirmation window appears, click **Confirm**.

This sections contains the following:

Copy Bootflash

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 SAN Controller home page, choose **SAN> Switch > Switch Overview > Backup**.

Step 2 Click **Copy to bootflash**.

Copy to bootflash page appears, displaying the **Source Configuration Preview** and **Selected Devices** area.

Source 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.

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 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 2 Navigate to **SAN> Switch > Switch Overview > Compare**.

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**: Diff 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.
- Golden Config—Specifies the version of the destination configuration.
- 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 SAN Controller server. Perform the following task to export a configuration file.

Procedure

Step 1 From SAN Controller 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.

Viewing of Port Usage

You can view the following information on Port Usage tab.

- **Port Speed** column displays the speed of the port.
- **Used Ports** column displays the total ports with the mentioned port speed.
- **Available Ports** column displays the available ports for the port speed.
- **Total Ports** column displays the total ports with the mentioned speed.
- **Estimated Day Left** column displays the estimated days left for the ports.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

Used ports displays the total used ports for the selected switch.**Total ports** displays the total available ports for the selected switch.

Viewing Bootflash

You can view the following information on Bootflash tab.

- **Primary Bootflash Summary** card displays the total, used and available space.
- **Secondary Bootflash Summary** card displays the total, used and available space.
- **Directory Listing** area displays check box for **Primary Bootflash** and **Secondary Bootflash**.

  This area shows the filename, size, and last modified date for all the files and directories on the switch bootflash. Choose **Actions > Delete** to delete files to increase the available space on the switch.

Device Manager

See Device Manager, on page 263 chapter for descriptions and instructions for using the Cisco MDS 9000 Device Manager.

Note Device Manger session is terminated when you navigate to another tab on the **Switch Overview** screen.

Blades

You can view the interfaces of the UCS switches through **SAN > Switches > Switch Overview**, on the SAN Controller Web UI.

Note Ensure that the UCS switches are listed on SAN Controller and the status of these switches are correct. You can view these tabs only for UCS switches.

Blades tab displays information of all server blades attached to the UCS FI.

The UCS has three tabs namely:

- Blades
- vNICs
- vHBAs

The blades tab displays all blade information as cards. Click **More Details** icon on each blade area to view details on the side panel of the selected blade.

You can click **Collapse All** or **Expand All** icon to collapse all or expand all blade areas respectively.

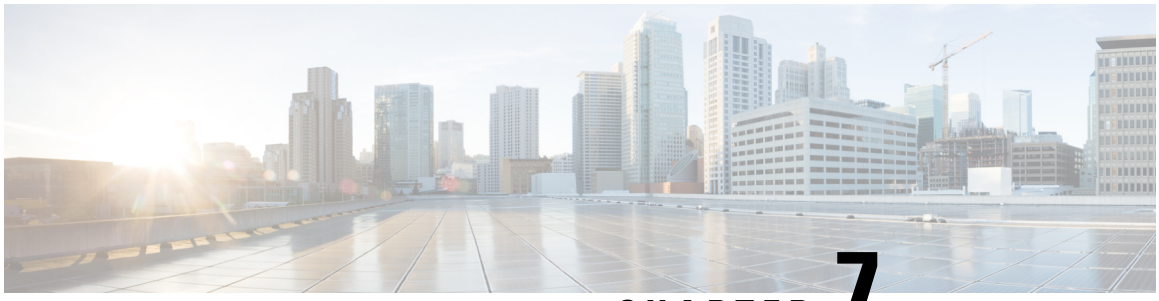
Blades tab displays information of all server blades attached to the UCS FI. Primary UCS FI only in redundancy setup or standalone UCS FI are displayed.

vNICs

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

vHBAs

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



CHAPTER 7

SAN Links

• SAN Links, on page 87

SAN Links

Cisco SAN Controller allows you to configure FCIP, Port channels on SAN Fabrics. You can also monitor the ISL traffic and errors, and view the performance of NPV links from the Cisco Nexus Dashboard Fabric Controller Web UI.

This section contains the following topics:

ISL and Port Channels

The ISL Traffic and Errors window is displayed. The table shows the ISLs and Port channels configured on SAN Fabrics. You can use the drop-down to filter the view by 24 hours, Week, Month, and Year.

Click on the trend icon in the Name column to view the graphical representation.

You can perform the following operations from the Actions drop-down list:

Configuring FCIP

To configure FCIP, perform the following steps:

Procedure

Step 1 Choose **Actions** > **Configure FCIP**.

The page displays the tasks to configure FCIP using the FCIP Wizard.

Note
FCIP is not supported on Cisco MDS 9000 24/10-Port SAN Extension Module.

Step 2 On the **Select Switch Pair** screen, select two MDS switches from the list to connect via FCIP.

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 3 Click **Next** to select the Ethernet ports.

Step 4 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 5 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 6 Click **Next** to specify Tunnel properties.

Step 7 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 8 Click **Next** to create FCIP ISL.

Step 9 Enter the **Profile ID** and **Tunnel ID** for the switch pair, and select the **FICON Port Address** from the list.

To configure FICON port numbers for FCIP ISLs, ensure that the **active equals saved** command is enabled on at least one of the FICON-enabled VSANs in the fabric. The **active equals saved** command is enabled by default when FICON is enabled on a VSAN. If not, you can still configure the ISL. However, you must manually add the FICON specific configuration details later.

Step 10 Click **View Configured** to display the **Profiles** and **Tunnels** information.

Step 11 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 12 Click **Next** to go to the summary page.

The **Summary** page displays what you have selected in the previous steps.

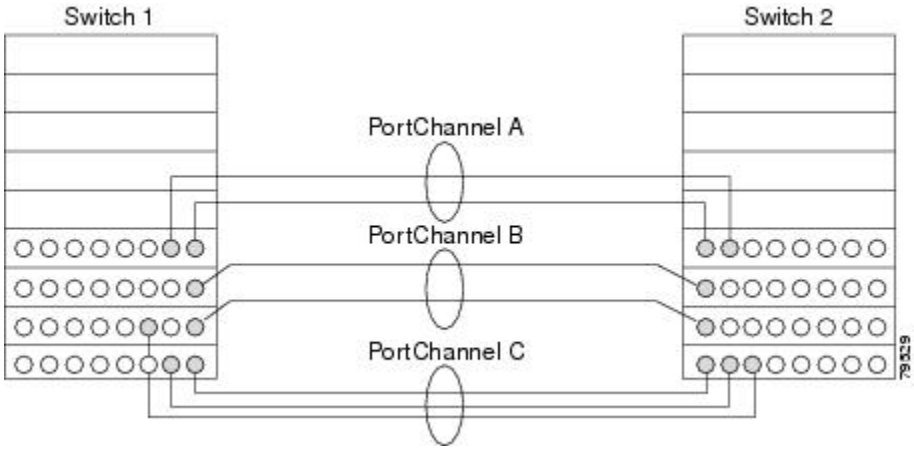
Step 13 Click **Finish** to configure FCIP.

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 1: 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 2: Trunking Only, on page 90 and Figure 3: Port Channeling and Trunking, on page 90).

Figure 2: Trunking Only

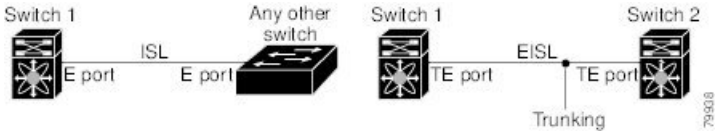
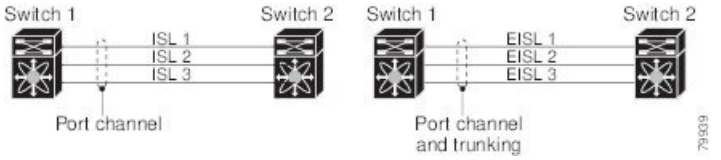


Figure 3: Port Channeling and Trunking



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.

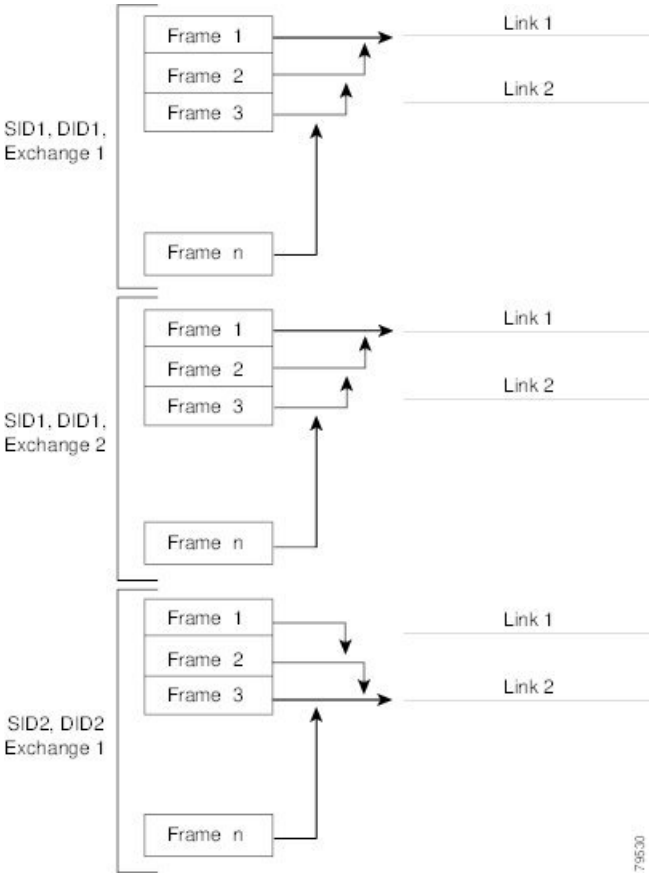
Load Balancing

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.

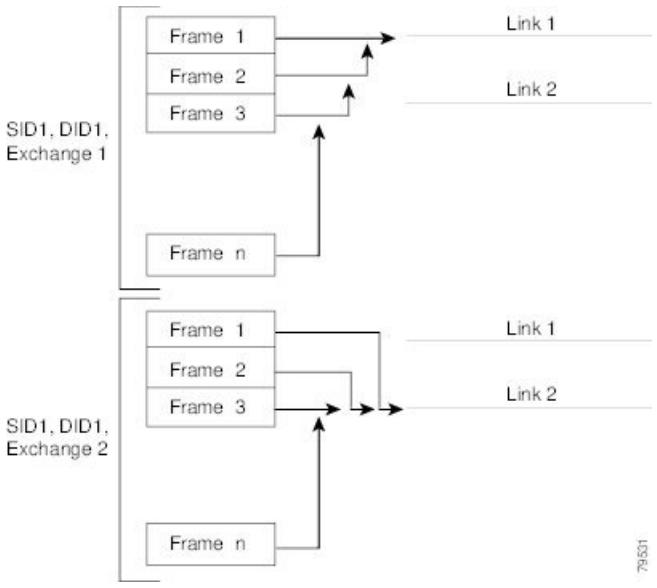
The following figure illustrates how a source ID 1 (SID1) and destination ID1 (DID1)-based load balancing works. When the first frame in a flow is received on an interface for forwarding, link 1 is selected. Each subsequent frame in that flow is sent over the same link. No frame in SID1 and DID1 utilizes link 2.

Figure 4: 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 5: 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 15: Channel Group Configuration Differences

ON Mode	ACTIVE Mode
No protocol is exchanged.	A Port Channel protocol negotiation is performed with the peer ports.

ON Mode	ACTIVE Mode
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.

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.

The following table describes 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

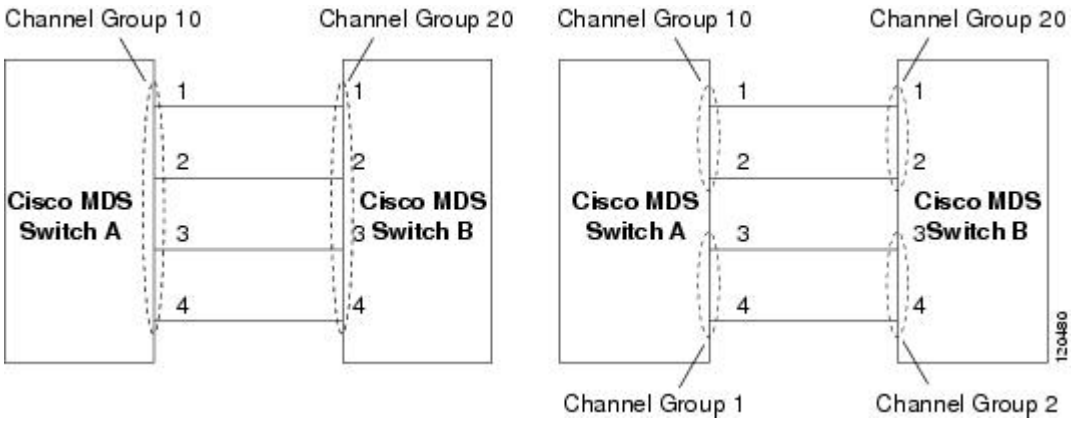
The following guidelines and restrictions are applicable for F and TF Port Channels:

- 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

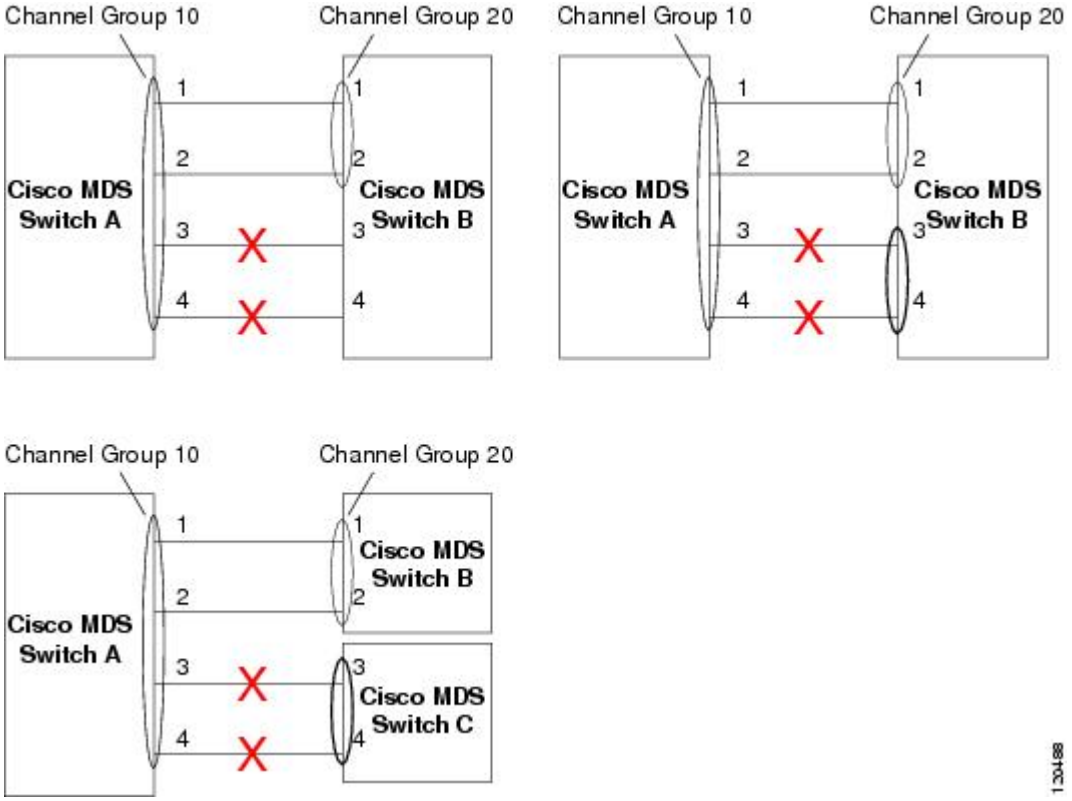
Port Channels are created with default values. You can change the default configuration just like any other physical interface. The following figure provides examples of valid Port Channel configurations.

Figure 6: 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 7: Misconfigured Configurations



Default Settings

The following table lists the default settings for Port Channels.

Table 16: 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 Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Navigate to **SAN** > **Links**.

Step 2 On the **ISLs** tab, choose **Actions** > **Create a new Port Channel**.

The **Create new port channel** wizard opens.

Step 3 In the **Select Switch Pair** screen, perform the following steps:

a) Select the appropriate fabric from the **Fabric** list.

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 4 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 5 In the **Configure 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 list, select the appropriate FICON port address on the switch. Select the port address that you want to assign to the Port Channel port.

To configure FICON port numbers for the Port Channel, ensure that the **active equals saved** command is enabled on at least one of the FICON-enabled VSANs in the fabric. **active equals saved** command is enabled by default. If not, you can still configure the port channel. However, you must manually add the FICON specific configuration details later.

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 **Non Trunk** 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) The 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 **Non Trunk** 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** check box 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 6 Click **Previous** to return to the previous screen and edit the settings. Click **Create new port channel** to configure the Port Channel.

A success message appears.

Edit Existing Port Channel

To edit a Port Channel using the Edit Port Channel Wizard on the Nexus Dashboard Fabric Controller Web UI, follow these steps:

Procedure

Step 1 Choose **Edit Port Channel** from the **Actions** drop-down list.

Click **Edit Port Channel** to launch the Create 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, choose 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 check box is enabled.

b) If you do not choose any ISL, check the **Delete Port Channel if Empty** check box to delete the port channel.

c) Check the **Force admin**, **trunk**, **speed**, **VSAN attributes to be identical** check box to choose identical values for admin, trunk, speed and VSAN attributes.

d) Click **Next**.

Step 5 Click **Save port channel** to apply the changes.

NPV Links

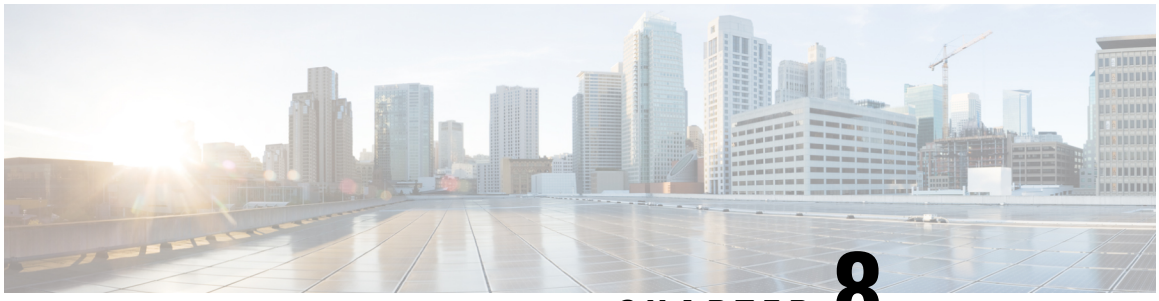
The NPV Links window is displayed. The table shows the performance of NPV links on SAN Fabrics. You can use the drop-down to filter the view by 24 hours, Week, Month, and Year.

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

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.



CHAPTER 8

Interfaces

- Interfaces, on page 105

Interfaces

This section provides information about SAN interfaces, such as, FC ports, Ethernet ports, port groups, and so on.

FC Ports

Choose **SAN > Interfaces > FC Ports** to view information about FC ports.

Viewing Inventory Information for FC Ports

Choose **SAN > Interfaces > FC Ports > Inventory** tab to display the list of Fibre Chanel interfaces.

The following table describes the fields that appear on **SAN > Interfaces > FC Ports > Inventory**.

Field	Description
Status	Specifies the status of the interface.
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Enclosure	Specifies the enclosure.
Device Name	Specifies the device name.
VSAN	Specifies the VSAN to which the interface belongs to.
Switch interface	Specified the interface name.
Type	Specifies the interface type.
Port WWN	Specifies the port world wide name (pWWN).

Field	Description
Speed	Specifies the interface speed.
FCID	Specifies the interface FCID.

Viewing Performance Information for FC Ports

Choose **SAN > Interfaces > FC Ports > Performance** tab to view the performance of Fibre Chanel interfaces.

The following table describes the fields that appear on **SAN > Interfaces > FC Ports > Performance**. You can filter the data using the **Day, Week, Month**, and **Year** options from the **Show last day** drop-down list. You can also filter for **Host Ports** and **Storage Ports** using **Show Host Ports** drop-down list.

To enable Performance, navigate to the **Fabric** window, choose the required fabric, and choose **Actions > Configure Performance**.

Field	Description
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Name	Specifies the interface name. Click the chart icon in the **Name** column to view a graph of the traffic on that device according to the selected timeline. You can filter the data using the **Day, Week, Month**, and **Year** options.
VSAN	Specifies the VSAN to which the interface belongs to.
Switch interface	Specified the interface name.
Speed	Specifies the interface speed.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Avg %	Specifies the average percentage of receiving or transmitting speed.
Peak	Specifies the peak utilization of the receiving or transmitting speed.
Peak %	Specifies the peak utilization percentage of the receiving or transmitting speed.
Rx + Tx	Specifies the sum of Rx and Tx speeds.
Errors/Discards	

Field	Description
In Avg	Specified the average of incoming errors or discards.
Out Avg	Specified the average of outgoing errors or discards.
In Peak	Specified the peak of incoming errors or discards.
Out Peak	Specified the peak of outgoing errors or discards.

Viewing Transceiver Information for FC Ports

Choose **SAN > Interfaces > FC Ports > Transceiver** tab to view the transceivers in Fibre Chanel interfaces.

The following table describes the fields that appear on **SAN > Interfaces > FC Ports > Transceiver**.

Field	Description
Enclosure	Specifies the enclosure name.
Device Alias	Displays the alias retrieved from the switch. A device aliases is a user-friendly name for a port WWN. Device alias name can be specified when configuring features.
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Port WWN	Specifies the port world wide name (pWWN).
Fcid	Specifies the associated interface FCID.
Switch interface	Specified the interface name.
Link Status	Displays the operational status of the link.
Vendor	Specifies the name of the vendor.
Serial Number	Specifies the serial number of the enclosure.
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.

Viewing FC FICON Ports

Choose **SAN** > **Interfaces** > **FC Ports** > **FICON** to display the list of Fiber Channel FICON interfaces.

The following table describes the fields that appear on the **FICON** page. Use the **Show last day** drop-down list to filter the view by **Day**, **Week**, **Month**, and **Year**.

Field	Description
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Switch interface	Specifies the switch interface.
Description	Specifies the interface description.
FCID	Specifies the associated interface FCID.
Mode	Specifies the interface mode.
FICON ID	Specifies the FICON ID.
Connected To	Specifies where the interface is connected to.
VSAN	Specifies the VSAN to which the interface belongs to.
Speed	Specifies the interface speed.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Avg %	Specifies the average percentage of receiving or transmitting speed.
Peak	Specifies the maximum utilization of the receiving or transmitting speed.
Peak %	Specifies the maximum utilization in percentage of the receiving or transmitting speed.
Rx + Tx	Specifies the sum of Rx and Tx speeds.
Errors/Discards	
In Avg	Specifies the average of incoming errors or discards.
Out Avg	Specifies the average of outgoing errors or discards.
In Peak	Specifies the maximum number of incoming errors or discards.

Field	Description
Out Peak	Specifies the maximum number of outgoing errors or discards.

Viewing Performance Information for Ethernet Ports

Choose **SAN > Interfaces > Ethernet** tab to display the list of Ethernet interfaces.

The following table describes the fields that appear on **SAN > Interfaces > Ethernet**. Use the **Show last day** menu drop-down list to filter the view by **Day**, **Week**, **Month**, and **Year**.

Field	Description
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Name	Specifies the interface name. Click the chart icon in the **Name** column to view a graph of the traffic on that device according to the selected timeline. You can filter the data using the **Day**, **Week**, **Month**, and **Year** options.
Description	Specifies the interface description.
Speed	Specifies the interface speed.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Avg %	Specifies the average percentage of receiving or transmitting speed.
Peak	Specifies the peak utilization of the receiving or transmitting speed.
Peak %	Specifies the peak utilization percentage of the receiving or transmitting speed.
Rx + Tx	Specifies the sum of Rx and Tx speeds.
Errors/Discards	
In Avg	Specified the average of incoming errors or discards.
Out Avg	Specified the average of outgoing errors or discards.
In Peak	Specified the peak of incoming errors or discards.
Out Peak	Specified the peak of outgoing errors or discards.

Viewing Performance Information for Port Groups

Choose **SAN > Interfaces > Port Groups** tab to display the list of port groups.

The following table describes the fields that appear on **SAN > Interfaces > Port Groups**. Use the **Show last 24 hours** menu drop-down list to filter the view by **24 Hours**, **Week**, **Month**, and **Year**.

Field	Description
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Port Group Name	Specifies the port group name. Click the name to display the port group members.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Peak	Specifies the peak utilization of the receiving or transmitting speed.
Rx + Tx	Specifies the sum of Rx and Tx speeds.
Errors/Discards	
In Avg	Specified the average of incoming errors or discards.
In Peak	Specified the peak of incoming errors or discards.
Last Updated	Specifies when the information was last updated.

Port Group Member

Choose **SAN > Interfaces > Port Groups** and click a port group name to view the port group members.

The following table describes the fields that appear on **Port Group Member**.

Field	Description
Port Group Member	Specifies the port group member. Click the chart icon to view a graph of the traffic for the port group member according to the selected timeline. You can filter the data using the **Day**, **Week**, **Month**, and **Year** options.
Speed	Specifies the speed for the port group member.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.

Field	Description
Peak	Specifies the peak utilization of the receiving or transmitting speed.
Rx + Tx	Specifies the sum of Rx and Tx speeds.
Errors/Discards	
In Avg	Specified the average of incoming errors or discards.
In Peak	Specified the peak of incoming errors or discards.
Last Updated	Specifies when the information was last updated.

Viewing Performance Information for Optics

Choose **SAN > Interfaces > Optics** tab to display the list of optics.

The following table describes the fields that appear on **SAN** > **Interfaces** > **Optics**.

Field	Description
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Switch	Specifies the switch name.
Interface	Specifies the interface name. Click the chart icon in the **Interface** column to view a graph of the optics parameters on that device according to the selected timeline. You can filter the data using the **Day**, **Week**, **Month**, and **Year** options.
Temperature (C)	Specifies the average, minimum, and maximum temperature.
Current (mA)	Specifies the average, minimum, and maximum current.
OpRxPower (dBm)	Specifies the average, minimum, and maximum optic Rx power.
OpTxPower (dBm)	Specifies the average, minimum, and maximum optic Tx power.
Voltage (V)	Specifies the average, minimum, and maximum voltage.

To view the optic metric information of devices that are connected to all the FC ports from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **SAN** > **Interfaces** > **Optics**.

   The **Optics** window is displayed.

2. You can sort the table using **Filter by attributes** field to enable filtering by **Fabric**, **Switch**, **Interface**, **Temperature**, **Current**, **Power**, and **Voltage**.
3. You can use **Show last day** drop-down to filter the view by **Day**, **Week**, **Month**, and **Year**.
4. Click a fabric name to display the fabric health status on the right-side of the page.
5. Click the **Launch** icon on fabric window to navigate to the fabric overview page.

Custom Port Groups

Choose **SAN > Interfaces > Custom Port Groups** tab to view and create custom port groups.

The following table describes the fields that appear on **SAN > Interfaces > Custom Port Groups**.

Field	Description
Group Name	Specifies the port group name. Click the name to view the performance and configure the port group. For more information, see Viewing Performance of Custom Port Groups , on page 112 and Configuring Custom Port Groups, on page 113.
Devices	Specifies the number of devices.
Interfaces	Specifies the number of interfaces.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **SAN > Interfaces > Custom Port Groups**.

Action Item	Description
Create Port Group	Select a port group from the table, choose **Create Port Group**, provide a port group name, and click **Save & Exit** to create a custom port group.
Edit port group	Select a port group from the table and choose **Edit port group** to edit port group.
Delete	Select a port group from the table and choose **Delete** to delete the port group.

Viewing Performance of Custom Port Groups

Choose **SAN > Interfaces > Custom Port Groups** and click a port group name to view the performance of the port group.

The following table describes the fields that appear on the **Performance** tab of Custom Port Groups.

Field	Description
Device	Specifies the device name.
Connected To	Specifies where the interface is connected to.
Speed	Specifies the interface speed.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Peak	Specifies the peak utilization of the receiving or transmitting speed.
Rx + Tx	Specifies the sum of Rx and Tx speeds.
Errors/Discards	
Avg	Specified the average of incoming errors or discards.
Peak	Specified the peak of incoming errors or discards.
Last Updated	Specifies when the information was last updated.

Use the **Show last day** menu drop-down list to filter the view by Day, Week, Month, and Year.

Configuring Custom Port Groups

Choose **SAN > Interfaces > Custom Port Groups**, click a port group name, and click the **Configuration** tab to configure the custom port group.

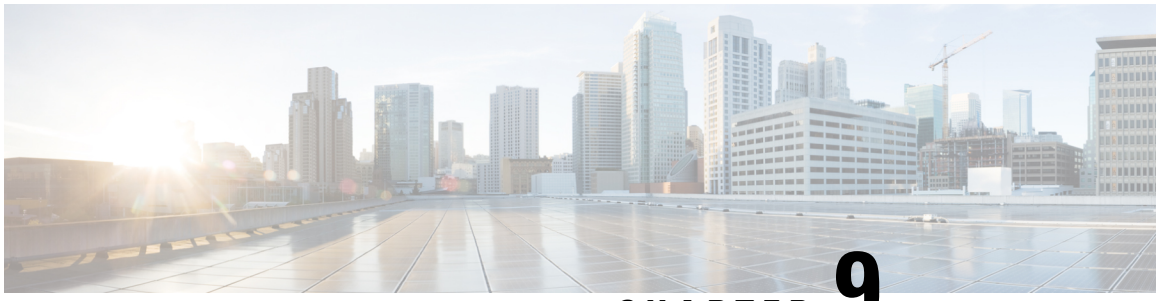
The following table describes the fields that appear on the **Configuration** tab of Custom Port Groups.

Field	Description
Device	Specifies the device name. Click the device name to display the device status on the right-side of the page.
Connected To	Specifies where the interface is connected to.
Description	Specifies the interface description.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on the **Configuration** tab.

Action Item	Description
Add Interfaces	Choose **Add Interfaces** to add interfaces to the port group. In the Add Interfaces window, select a device and click **Next Step - Add Interfaces.** Select the interfaces that you want to add to the port group and click **Save & Exit**.

Action Item	Description
Delete	Select a port group from the table and choose **Delete** to delete the port group.



CHAPTER 9

End Devices

- Devices, on page 115
- Enclosures, on page 116

Devices

Choose **SAN > End Devices > Devices** tab to display the list of host and storage devices.

The following table describes the fields that appear on **SAN > End Devices > Devices**.

Use the **Show last day** menu drop-down list to filter the view by **Day**, **Week**, **Month**, and **Year**.

Use the **Show Host Ports** menu drop-down list to filter the view by **Host Ports** and **Storage Ports**.

Field	Description
Fabric	Specifies the fabric name. Click the fabric name to display the fabric status on the right-side of the page. Click the **Launch** icon on the top-right side of the pane to see Fabric Overview. For information on Fabric Overview, see Fabric Overview, on page 45.
Enclosure Name	Specifies the enclosure name.
Device Alias	Specifies the device alias. Click the chart icon in the **Device Alias** column to view a graph of the traffic on that device according to the selected timeline. You can filter the data using the **Day**, **Week**, **Month**, and **Year** options.
FCID	Specifies the associated FCID.
Switch interface	Specifies the switch interface.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Avg %	Specifies the average percentage of receiving or transmitting speed.

Field	Description
Peak	Specifies the peak utilization of the receiving or transmitting speed.
Peak %	Specifies the peak utilization percentage of the receiving or transmitting speed.
Errors/Discards	
In Avg	Specified the average of incoming errors or discards.
Out Avg	Specified the average of outgoing errors or discards.
In Peak	Specified the peak of incoming errors or discards.
Out Peak	Specified the peak of outgoing errors or discards.

Enclosures

Choose **SAN > End Devices > Enclosures** tab to display the host and storage enclosures.

Cisco Nexus Dashboard Fabric Controller extends the fabric visibility up to the server and allows you to discover and search the end devices, SAN Storage Enclosures, and Storage Systems that are attached to the network.

Click an enclosure name in the table to view more information about the enclosure.

This section includes the following topics:

Inventory

Choose **SAN > End Devices > Enclosures> Inventory > Host Enclosures** tab to display the host and storage inventory enclosures.

This section includes the following topics:

Inventory – Host Enclosures

The following table describes the fields that appear on **SAN > End Devices > Enclosures> Inventory > Host Enclosures**.

Field	Description
Enclosure	Specifies the enclosure name. Click the enclosure name for more information.
OS	Specifies the OS details.
IP Address	Specifies the IP address of the switch.
WWNs	Specifies the number of World Wide Names (WWNs).

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **SAN > End Devices > Enclosures> Inventory > Host Enclosures**.

Action Item	Description
Edit	Select an enclosure from the table and choose **Edit** to update the enclosure information.
Change to Storage Enclosure	Select an enclosure from the table and choose **Change to Storage Enclosure** to change the selected enclosure to storage enclosure.

Importing or Exporting Inventory Enclosures data

From Release 12.1.2e, you can import and export enclosures data to a `.txt` file. This feature allows you to edit the exported file, and import the data to NDFC. You can either choose to export **All** or **Only Host Enclosures** or **Only Storage Enclosures** data. You can also choose one Fabric or All fabrics' data while exporting.

To export Inventory Enclosures data, perform the following steps:

1. On either **Host Enclosures** or **Storage Enclosures** tab, from the Actions drop-down list, select **Export**.
2. Select the enclosures to export data. You can choose **All** or **Only Host Enclosures** or **Only Storage Enclosures**.
3. In the Exported File Name field, provide the name of the exported file.

Note The export file is of **.txt** format only.

4. From **Fabric scope** drop-down list, choose **All Fabrics** or specific Fabric from which you must export enclosures data.
5. Click **Export** to download the enclosures data.

   Save the exported file to a local directory.

To import Inventory Enclosures data, perform the following steps:

1. On either **Host Enclosures** or **Storage Enclosures** tab, from the Actions drop-down list, select **Import**.
2. Upload the data file from your local directory. You can either drag and drop the file, or browse to upload the data file.

Note You can import data from **.txt** file format only.

   The uploaded file appears in the Import Enclosures area.

3. Click **OK** to import the enclosures data. Click **Cancel** the discard.

Inventory – Storage Enclosures

The following table describes the fields that appear on **SAN > End Devices > Enclosures> Inventory > Storage Enclosures**.

Field	Description
Enclosure	Specifies the enclosure name. Click the enclosure name for more information.
IP Address	Specifies the IP address of the switch.
WWNs	Specifies the number of World Wide Names (WWNs).

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **SAN > End Devices > Enclosures> Inventory > Storage Enclosures**.

Action Item	Description
Edit	Select an enclosure from the table and choose **Edit** to update the enclosure information.
Change to Host Enclosure	Select an enclosure from the table and choose **Change to Host Enclosure** to change the selected enclosure to host enclosure.

Importing or Exporting Inventory Enclosures data

From Release 12.1.2e, you can import and export enclosures data to a `.txt` file. This feature allows you to edit the exported file, and import the data to NDFC. You can either choose to export **All** or **Only Host Enclosures** or **Only Storage Enclosures** data. You can also choose one Fabric or All fabrics' data while exporting.

To export Inventory Enclosures data, perform the following steps:

1. On either **Host Enclosures** or **Storage Enclosures** tab, from the Actions drop-down list, select **Export**.
2. Select the enclosures to export data. You can choose **All** or **Only Host Enclosures** or **Only Storage Enclosures**.
3. In the Exported File Name field, provide the name of the exported file.

Note The export file is of **.txt** format only.

4. From **Fabric scope** drop-down list, choose **All Fabrics** or specific Fabric from which you must export enclosures data.
5. Click **Export** to download the enclosures data.

   Save the exported file to a local directory.

To import Inventory Enclosures data, perform the following steps:

1. On either **Host Enclosures** or **Storage Enclosures** tab, from the Actions drop-down list, select **Import**.
2. Upload the data file from your local directory. You can either drag and drop the file, or browse to upload the data file.



Note You can import data from **.txt** file format only.

The uploaded file appears in the Import Enclosures area.

3. Click **OK** to import the enclosures data. Click **Cancel** the discard.

Performance

Choose **SAN > End Devices > Enclosures> Performance > Host Enclosures** tab to display the host and storage performance enclosures.

This section includes the following topics:

Performance – Host Enclosures

The following table describes the fields that appear on **SAN > End Devices > Enclosures > Performance > Host Enclosures**. Use the **Show last day** menu drop-down list to filter the view by **Day**, **Week**, **Month**, and **Year**.

Field	Description
Enclosure Name	Specifies the enclosure name. Click the enclosure name to view more information. Click the chart icon to view a graph of the traffic on that device according to the selected timeline. You can filter the data using the **Day**, **Week**, **Month**, and **Year** options.
Rx/Tx/Errors/Discards	
Avg	Specifies the average receiving, transmitting, errors, or discards speed.
Peak	Specifies the peak utilization of the receiving, transmitting, errors, or discards speed.
Rx + Tx	Specifies the sum of receiving and transmitting speeds.
Last Updated	Specifies the last updated time.

Performance – Storage Enclosures

The following table describes the fields that appear on **SAN > End Devices > Enclosures> Inventory > Storage Enclosures**.

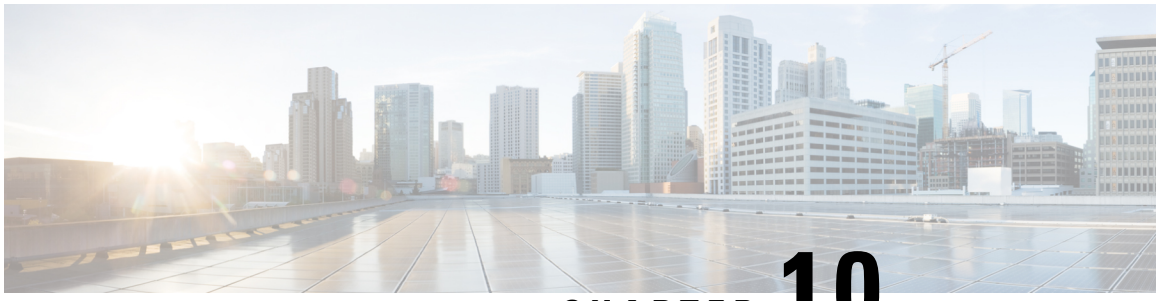
Field	Description
Enclosure Name	Specifies the enclosure name.
Rx/Tx/Errors/Discards	
Avg	Specifies the average receiving, transmitting, errors, or discards speed.
Peak	Specifies the peak utilization of the receiving, transmitting, errors, or discards speed.
Last Updated	Specifies the last updated time.

Use the **Show last day** menu drop-down list to filter the view by Day, Week, Month, and Year.

Enclosure Members

The following table describes the fields that appear on **SAN > End Devices > Enclosures > Performance**. Enclosure members can be viewed for Host and Storage performance enclosures. Use the **Show last day** menu drop-down list to filter the view by **Day**, **Week**, **Month**, and **Year**.

Field	Description
Fabric	Specifies the fabric name. Click the name to view information about fabric health on the right-side of the page.
Device	Specifies the device name.
Speed	Specifies the device speed.
Rx/Tx	
Avg	Specifies the average receiving or transmitting speed.
Avg %	Specifies the average percentage of receiving or transmitting speed.
Peak	Specifies the peak utilization of the receiving, or transmitting speed.
Peak %	Specifies the peak utilization percentage of the receiving or transmitting speed.
Errors/Discards	
Avg	Specifies the average errors or discards speed.
Peak	Specifies the peak utilization of the errors or discards speed.
Last Updated	Specifies the last updated time.



CHAPTER 10

Host Path Redundancy

• Host Path Redundancy, on page 121

Host Path 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 Nexus Dashboard Fabric Controller 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 NDFC. 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 NDFC, in order for Host Path Redundancy and other features to consider them the same device.

Choose **SAN > Host Path Redundancy**.

This section includes the following topics:

Diagnostic Test

Procedure

Step 1 Choose **SAN > Host Path Redundancy > Diagnostic Test**.

Step 2 Under the **Diagnostic Test** tab, use the check boxes to select the host redundancy optional checks.

Step 3 Check the **Automatically run tests 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 perform 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 relevant tabs that are next to the **Diagnostic Test** tab.

Hostpath Errors

Choose **SAN > Host Path Redundancy > Hostpath Errors** tab to display the host path redundancy errors table. The top of the table displays the colored **Good**, **Errored**, and **Skipped** host enclosure counts.

The following table describes the fields that appear on **SAN > Host Path Redundancy > Hostpath Errors**.

Field	Description
Host Enclosure	Specifies the hosts that contain the errors. These are counts of each path in the host enclosures seeing an error.
Storage Enclosure	Specifies the connected storage that is encountering the error.
Description	Specifies the description of the error.
Fix	Specifies a solution to fix the error. Point to the error to view a solution to fix the error.
First Seen	Specifies when the error was first seen.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **SAN > Host Path Redundancy > Hostpath Errors**.

Action Item	Description
Ignore Host	Select a row from the table and choose **Ignore Host** 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.
Ignore Storage	Select a row from the table and choose **Ignore Storage** to add the selected rows storage enclosure to an exclusion list.
Ignore Host Storage Pair	Select a row from the table and choose **Ignore Host Storage Pair** to add the selected rows host-storage pair enclosure to an exclusion list.
Clear Results	Select a row from the table and choose **Clear Results** to clear the results.

Ignored Host

Choose **SAN > Host Path Redundancy > Ignored Host** tab to display the list of host enclosures that have been skipped or ignored by the redundancy check along with the reason for skipping.

The following table describes the fields that appear on **SAN > Host Path Redundancy > Ignored Host**. Select a host enclosure and click **Unignore** to remove the host from the ignored list and begin receiving errors about the host you had chosen to ignore.

Field	Description
Host Enclosure	Specifies the hosts that contain the errors.
Ignore Reason	Specifies the reason for which the host was ignored. 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.**

Ignored Storage

Choose **SAN > Host Path Redundancy > Ignored Storage** tab to display the list of storage enclosures that have been selected to be ignored during the redundancy check.

The following table describes the fields that appear on **SAN > Host Path Redundancy > Ignored Storage**. Select a storage enclosure and click **Unignore** to remove the storage from the ignored list and begin receiving errors about the storage you had chosen to ignore.

Field	Description
Storage Enclosure	Specifies the connected storage that is encountering the error.
Ignore Reason	Specifies the reason for which the storage was ignored.

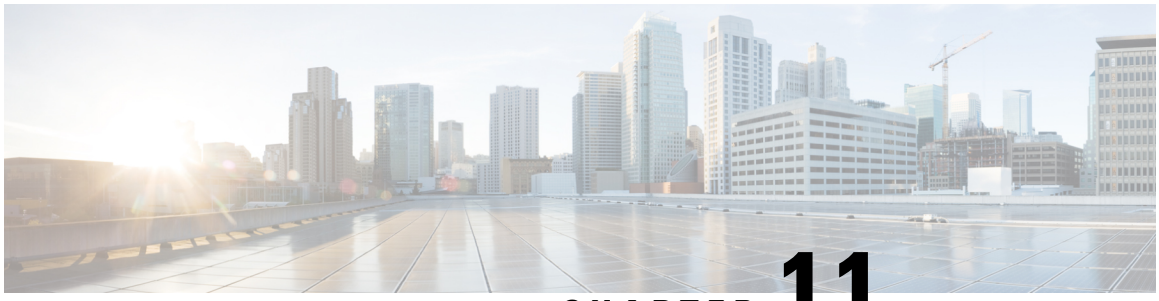
Ignored Host Storage Pair

Choose **SAN > Host Path Redundancy > Ignored Host Storage Pair** tab to display the list of host-storage pairs that have been selected to be ignored during the redundancy check.

The following table describes the fields that appear on **SAN > Host Path Redundancy > Ignored Host Storage Pair**. Select a row and click **Unignore** to remove the host-storage pair from the ignored list.

Field	Description
Host Enclosure	Specifies the hosts that contain the errors.

Field	Description
Storage Enclosure	Specifies the connected storage that is encountering the error.
Ignore Reason	Specifies the reason for which the storage was ignored.



CHAPTER 11

Port Monitoring

- Port Monitoring Policy, on page 125
- Configuring SFP Counters, on page 130

Port Monitoring Policy

This feature allows you to save custom Port Monitoring policies in the Cisco SAN Controller 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 SAN Controller user can select the MDS switch to push the policy.

Cisco SAN Controller provides 12 templates to customize the policy. The user-defined policies are saved in the Cisco SAN Controller database. You can select any template or customized policy to push to the selected fabric or switch with the desired port type.

From Cisco SAN Controller Release 12.0.1a, a new port monitory policy **fabricmon_edge_policy** is added.

Note You can edit only user-defined policies.

The following table describes the fields that appear on Cisco Fabric Controller **SAN** > **Port Monitoring**.

Field	Description
Selected Port Monitoring Policy	This drop-down list shows the following templates for policies: • Normal_edgePort • Normal_allPort • Normal_corePort • Aggressive_edgePort • Aggressive_allPort • Aggressive_corePort • Most-Aggressive_edgePort • Most-Aggressive_allPort • Most-Aggressive_corePort • default • slowdrain • fabricmon_edge_policy
Logical Type	Specifies the type of port for selected policies. The available port types are: • Core • Edge • All
Save	Allows you to save your changes for the user-defined policies. **Note** You cannot save configuration changes for default templates.
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. To create new policy: • Choose required port monitoring policy, click **Save As**. The **New Port Monitoring Policy** pop window appears. • Enter new policy name and select required logical type and click **Save**.
Delete	Allows you to delete any user-defined policies.

Field	Description
Push to switches	

Field	Description
	Allows you to select a fabric or switch and push the selected policies with the desired port type. The following policies select the Core policy type: • Normal_corePort • Aggressive_corePort • Most-Aggressive_corePort The following policies select the edge policy type: • Normal_edgePort • Aggressive_edgePort • Most-Aggressive_edgePort • fabricmon_edge_policy • slowdrain The following policies select all policy types: • Normal_allPort • Aggressive_allPort • Most-Aggressive_allPort • default Select the parameters and click **Push** to push the policies to the switches in the fabric. For SAN Controller from Release 12.0.1a, you can change required port type for selected policy apart from the pre-defined port. • Choose required policy, click **Push to Switches**. The **Push to Switches** pop up window appears. • Choose required port type and click **Push**. If there is an active policy with the same or common port type, the push command configures the same policy on the selected devices. This policy replaces the existing active policy with the same or common port type. A warning message is displayed for replacing the existing policy. Click **Confirm** to rewrite the policy. A confirmation message is displayed for policy pushed to switches. Click View logs to view log details on the switch or click **OK** to return to the home page. If you click **Push to Switches** while the policy is edited, the customized policy will not be saved.

Field	Description
	SAN Controller enables Fabric Performance Monitor (FPM) feature when you push and activate the edge logical-type policy with FPIN or DIRL port guard. **Note** If you select Cisco MDS 9250i Multiservice Fabric Switch for policy with FPIN or DIRL feature counter, a warning window appears.
Description	Move the pointer to the "i" icon next to the description to view detailed information. Beginning with SAN Controller Release 12.0.1a, the following new counters are introduced: • Rx Datarate Burst • Tx Datarate Burst • SFP Rx Power Low Warning • SFP Tx Power Low Warning • Input Errors
Rising Threshold	Specifies the upper threshold limit for the counter type.
Rising Event	Specifies the type of event to be generated when the rising threshold is reached or crossed.
Falling Threshold	Specifies the lower threshold limit for the counter type.
Alerts	Specifies type of alert for the port. The alerts are syslog, rmon, and oblf. Alert is applicable for Cisco MDS switches with release 8.5(1) only.
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". From Cisco SAN Controller Release 12.0.1a, new port guards **FPIN**, **DIRL**, and **cong-isolate-recover** are added for edge port type only. **Note** DIRL is a preview feature in Cisco SAN Controller 12.0.1a. It is recommended not to use in production environment.
Congestion- signal Warning	Indicates the building congestion between ports. This is available only for **TxWait (%)** counter only.

Field	Description
Congestion- signal Alarm	Indicates the critical congestion between ports. This is available only for Tx-Wait counter.
Monitor	Indicates the value either true or false.
Edit	Click to edit above details for each row and click tick mark to save configuration changes. **Note** You can overwrite configuration changes saved using Save and Save As option when you edit the configuration for each row.

Configuring SFP Counters

From Cisco MDS NX-OS Release 8.5(1), the SFP counters allow you to configure the low warning thresholds for Tx Power and Rx Power for SFPs. You will receive syslog when these threshold values drop below the configured values.

SFPs are monitored once in every 10 minutes. The rising threshold is the count of Rx or Tx Power times. This power time is less than or equal to the SFPs Rx or Tx Power low warning threshold multiplied by the percentage. Accordingly, you can increment the rising threshold once every 10 minutes. Configuring a rising threshold value that is more than the 600 multiple of the poll interval displays an error.

For example, for a polling interval of 1200, the rising threshold will be 2 (1200/600) and must be more than 2. The SFP counters are not included in the default policy and the only alert action that is available is syslog. You can configure the polling interval using the port monitor counter command.

You can choose one of the following to configure SFP counters, perform the following options:

- Configuring a low warning threshold percentage of 100% allows this counter to trigger when the Rx Power is less than or equal to the SFP's Rx Power low warning threshold.
- Configuring a low warning threshold percentage less than 100% allows this counter to trigger when the Rx Power is above the SFP's Rx Power low warning threshold.
- Configuring a low warning threshold percentage of greater than 100% allows this counter to trigger when the Rx Power is less than the SFP's Rx Power low warning threshold (between low warning and low alarm).

The following are the SFP counters:

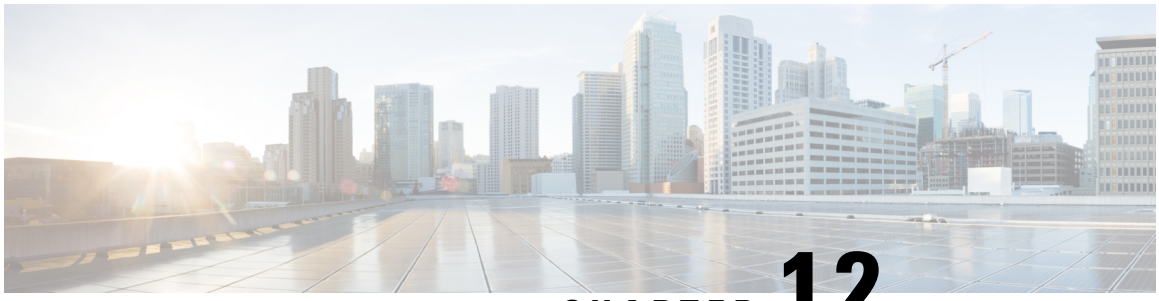
- **sfp-rx-power-low-warn**

  Specifies the number of times a SFP's port reached a percentage of the SFP's Rx Power's low warning threshold. This threshold varies depending on the type, speed, and manufacturer of the SFP and this is displayed via show interface transceiver details command. This value is percentage of each individual SFP's Rx Power low warning threshold and not the perfect value. This percentage can be configured in the range of 50 to 150% to allow for alerting at values less than the Rx Power low warning threshold or greater than the Rx Power low warning threshold. This is an perfect value and varies between 50% to 150%. The low warning threshold value is calculated as the actual low warning threshold value of the SFP times the specified percentage. If the Rx power is lesser than or equal to the low warning threshold value, then this counter is incremented.

- **sfp-tx-power-low-warn**

  Specifies the number of times a SFP's port reached a percentage of the SFP's Tx Power's low warning threshold. This threshold varies depending on the type, speed, and manufacturer of the SFP and this is displayed via show interface transceiver details command. This value is percentage of each individual SFP's Tx Power low warning threshold and not the perfect value. This percentage can be configured in the range of 50 to 150% to allow for alerting at values less than the Tx Power low warning threshold or greater than the Tx Power low warning threshold. This is an perfect value and varies between 50% to 150%. The low warning threshold value is calculated as the actual low warning threshold value of the SFP times the specified percentage. If the Tx power is lesser than or equal to the low warning threshold value, then this counter is incremented.

From Cisco MDS NX-OS Release 8.5(1), the datarate burst counters monitor the number of times the datarate crosses the configured threshold datarate in one second intervals. If the number crosses the configured number for rising threshold, the configured alert actions are taken as the condition is met. Datarate burst counters are polled every second. The datarate burst counters are not included in the default policy. For configuring the datarate burst counters, see *Configuring a Port Monitor Policy* section in *Cisco MDS 9000 Series Interfaces Configuration Guide.*



CHAPTER 12

Active Zones

- Regular Zones, on page 133
- IVR Zones, on page 134

Regular Zones

You can view all the Regular Zones that are configured on SAN Controller. Choose **SAN** > **Active Zones** > **Regular Zones** tab. The following table describes the fields that appear on this screen.

Table 17:

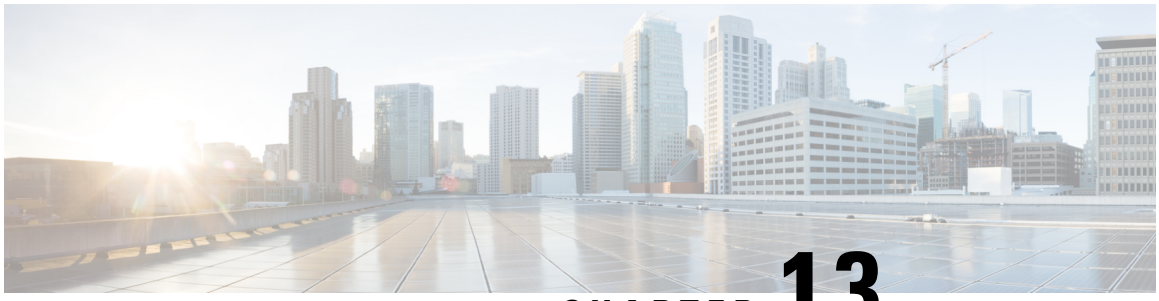
Field	Description
Group	Specifies the name of the fabric.
VSANS	Specifies the number of VSANS configured on this Zone.
Zone Sets	Specifies the name of zone set to which the zone belongs.
Zone	Displays the zone under which this member is present. **Note** You cannot save any changes made to topology layout from this screen.
Switch Interface/WWN	Specifies the switch interface or WWN of the switch that the zone member is attached to.
PWWN	Specifies the associated pWWN to the switch.
Member Name	Displays the name of the zone member.
Zoned By	Displays the type of zoning. You can search by type of zoning such as WWN, FCID, fcAlias, or iSCSI.

IVR Zones

You can view all the IVR Zones configured on SAN Controller. Choose **SAN > Active Zones > IVR Zones** tab. The following table describes the fields that appear on this screen.

Table 18:

Field	Description
Group	Specifies the fabric name.
VSANS	Specifies the number of VSANS configured on this Zone.
Zone Sets	Specifies the name of Zone set to which the zone belongs.
Zone	Displays the zone under which this member is present.
Switch Interface/WWN	Specifies the switch interface or WWN of the switch that the zone member is attached to.
PWWN	Specifies the associated pWWN to the switch.
Member Name	Displays the name of the zone member.
Zoned By	Displays the type of zoning. You can search by type of zoning such as WWN, FCID, fcAlias, or iSCSI.



CHAPTER 13

Storage

- Storage Arrays, on page 135
- Storage SMI-S Provider, on page 136

Storage Arrays

This tab displays information about storage arrays.

The following table describes the fields that appear on **SAN > Storage > Storage Arrays**.

Field	Description
storageName	Specifies the storage name. Click on the **storageName** to view the **Storage Enclosure** details. For more information on the tabs displayed, refer to storageName Enclosure, on page 135.
WWN	Specifies the world wide name (WWN) of the storage device. Only storage array PWWN that are discovered via fabric discovery are displayed. However, storage array may have more ports than specified here.

storageName Enclosure

Click on the **storageName** item to view the detailed information about each storage array.

The details of a Storage Array depends on the type of array discovered, and the provider's adherence to the SMI-S standards. Click of the array to load the inventory page, starting with a summary tab, and other context specific tabs based on the type of array.

The following tabs provide relevant information:

- **Summary**

  This table provides information about the provider. Storage array **Serial Number**, **Storage type** and **Number of Physical Disks** in the array are also displayed.

- **Components**

This tab lists all the components in the Storage.

Click on the component **Name** to view total storage capacity, usage details, and physical disks details.

- **Pools**

  This tab lists all the pools, their status and Raw capacity. Click on **POOL Name** to view the pool details.

- **LUNs**

  This tab lists all the LUNs in the storage array. It provides **LUN ID**, **WWN**, **Status**, and **Capacity** details for each LUN. Click on **LUN Name** to view further details about each LUN. You can also view the **Host LUN Access** information in the **LUN Detail** view.

  Host Port PWWN, **Host Interface**, **Zoning**, and **Storage Interface** values in **Host LUN Access** table is displayed only if the host accessing this LUN is a part of the NDFC discovered fabric.

- **Host**

  This tab lists all the hosts in the selected storage. It provides the **Host name**, **Node WWN**, and **WWN** details for each host in the Storage array. Click on a **Host Name** to view details about the host. You can view the relevant details on the **LUNs** tab and **Ports** tab within the **Host Detail** view.

  Host Interface, **Zoning**, and **Storage Interface** values in **LUNs Tab > Host LUN Access** table is displayed only if the host accessing this LUN is part of the NDFC discovered fabric.

  Fabric and **Host Interface** values in **Host Ports** table is displayed only if **Host Port WWN** is part of the NDFC discovered fabric.

- **Processors**

  This tab lists all the Processors and their Status. It also shows the number of adapters for each processor. Click on a **Processor Name** to view the details.

- **Ports**

  This tab lists all the Ports within the Storage array. Click on **Port Name** to view details about the port.

  Host Interface, **Zoning**, and **Storage Interface** values in the **Host LUN Access** table is displayed only if Host accessing the LUN in **LUN ID** column is part of the NDFC discovered fabric.

Storage SMI-S Provider

This tab displays the SMI-S provider information.

The following table describes the fields that appear on **SAN > Storage > Storage SMIS Provider**.

Field	Description
Vendor	Specifies the vendor. Cisco NDFC supports the following vendors: • EMC • NetApp • IBM • HDS • PureStorage • HP • Other
Provider URL	Specifies SMI-S provider URL.
Name Space	Specifies name space.
Interop Name Space	Specifies interop name space.
Port	Specifies the port.
Status	Specifies the status.
Secure	Specifies if it is a secure connection.
Discovery Status	Specifies the discovery status.
Last Updated Time	Specifies the last updated time.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **SAN > Storage > Storage SMIS Provider**.

Action Item	Description
Add Provider	Adds an SMI-S provider. For instructions, refer to Adding SMI-S Provider, on page 138.
Edit Provider	Select a provider from the table and choose **Edit Provider** to update the provider information.
Delete Provider	Select a provider from the table and choose **Delete Provider** to delete the provider.
Rediscover Provider	Select a provider from the table and choose **Rediscover Provider** to scan for any changes. This triggers the discovery cycle outside its normal periodic polling.

Action Item	Description
Purge Provider	Select a provider from the table and choose **Purge Provider** to purge the provider information. This removes elements no longer present from discovery.

Adding SMI-S Provider

To add an SMI-S provider from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN > Storage > Storage SMIS Provider**.

The **Storage SMIS Provider** tab is displayed.

Step 2 Click the **Actions** menu drop-down list and click **Add Provider**.

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

Step 3 Use the drop-down to select a **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
A minimum of one valid Nexus Dashboard Fabric Controller license must be provisioned before adding the data sources for SMI-S storage discovery.

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

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

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

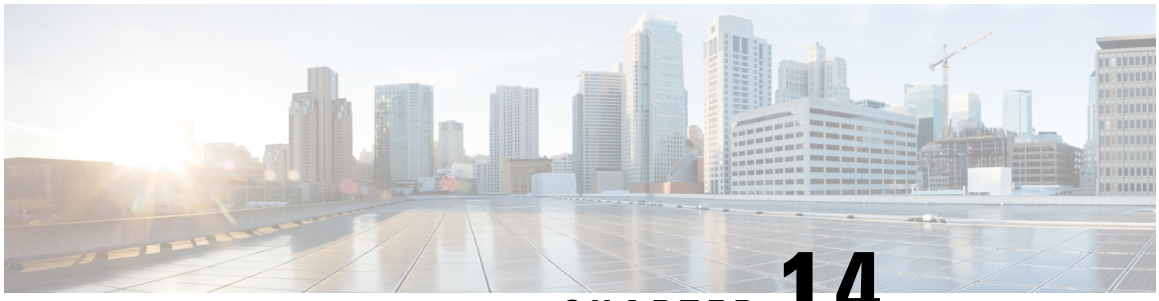
The credentials are validated and the storage discovery starts if the credentials is valid. If the credentials check fails, you will be prompted to enter valid credentials.



PART II

Virtual Management

- Zoning, on page 141
- Virtual Infrastructure Manager, on page 153



CHAPTER 14

Zoning

- Zoning, on page 141

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.

From SAN Controller Release 12.0.1a, Regular zones, and IVR zones are merged into a single zoning page.

Note When device aliases are used for zoning in Web UI, 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 SAN Controller **Virtual Management** > **Zoning** tab.

Field	Description
Zoning Type	Choose radio button next to **Regular** or **IVR** to select required zoning type.
Fabric	From the Fabric drop-down list, you can choose the fabric for which you are configuring or viewing the Zoning. If admin role locks the fabric, you can view lock icon next to the fabric field.
VSAN	Choose Regular Zoning type to view VSAN field. From the VSAN drop-down list, you can choose the VSAN for which you are configuring regular zones.
Region ID	Choose IVR Zoning type to view Region ID field. From the Region ID drop-down list, you can choose the region name for which you are configuring IVR zones.

Field	Description
Enhanced Zoning	Click **configurations** icon next to **VSAN** text field to view Enhanced zoning window. **Note** Enhanced Zoning is supported only for Regular zone. For more details, refer to Enhanced Zoning section.
Cisco Fabric Services (CFS)	Click **set-up assistant** icon next to the **Region ID** field to view CFS window. **Note** CFS is supported only for IVR Zoning. For more details, refer to CFS section.
Switch	From the Switch drop-down list, select the switch to which you want to configure.
Action	On Zoning field, click **Actions** to view the following items: • Changes • Database • Clear Server Cache • Discovery Sync
Changes	On Zoning field, click **Actions** > **Changes**. • Enable smart zoning - Enables smart zoning configuration for all the switches. • 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. • Discard Pending - Discards the changes in progress.
Database	On Zoning field, click **Actions** > **Database**. • Backup database – Choose Backup Database, the **Backup Database** window is displayed. Enter a name and click **Backup**. • Restore database – Choose Restore Database, the **Restore Database** window is displayed. Upload appropriate file and click **Restore**.
Clear Server Cache	On Zoning area, choose **Actions** > **Clear Server Cache**. Clears the cache on the server.
Discovery Sync	On Zoning area, choose **Actions** > **Discovery Sync**. To synchronize zoning modules with discovery.

This chapter contains the following sections:

Enhanced Zoning

From SAN Controller Release 12.0.1a, Enhanced Zoning feature is added for Regular Zoning type.

Enhanced zoning performs all configurations within a single configuration session for regular zoning. When you begin a session, the switch locks the entire fabric to implement the changes.

Choose **Regular** radio button on Zoning type, Click **configurations** icon next to **VSAN** field to view Enhanced zoning window.

The **Enhanced Zoning** window has the following fields and their descriptions.

Field	Description
Switch	Specifies IP address of the switch.
Mode	Displays mode of the switch, that can be one of the following: • Basic • Enhanced
Result	Displays the activation results, which can be one of the following: • Success • Failed
Config DB locked by	Displays the role name of locked configuration database.
Action	Displays the action on the switch, that can be one of the following: • No operation • Commit changes • Cleanup Click **edit** icon on last column to select required action and click check mark icon to save.
Last Action Results	Displays status of last configuration database.
Enforce full DB merge	Displays status as enabled or disabled. Click **edit** icon on last column to select required action and click check mark icon to save. Enabling it ensures that both the active and local zones are merged and are identical on all switches for a VSAN.

Field	Description
Read from	For enhanced zones or IVR CFS enabled zones when a change is made to zoning DB on a switch, all zone data is pushed into a pending database, until commit command is issued. This flag helps user to get data either from pending zone DB (Copy DB) or regular zone DB (Effective DB). Click **edit** icon on last column to select required action and click check mark icon to save.
Activation Date	Specifies date of the zoneset activated.

To perform various operations on Enhanced Zoning window from SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Virtual Management** > **Zoning**, choose required **Zone Type**, **Fabric**, and **VSAN**.

Step 2 Click **configurations** icon adjacent **VSAN** field

The **Enhanced Zoning** window is displayed.

Step 3 Click **Edit** icon next to **Read from** column, to select required database and click **Tick** icon to save.

Step 4 To change the mode from basic to enhanced, choose **Actions** > **Set Mode to Enhanced**, and click **Apply**.

Step 5 You can follow the same procedure to set mode from enhanced to basic, choose **Actions** > **Set Mode to Basic**, and click **Apply**.

CFS

Cisco Fabric Services (CFS) provides a common infrastructure for automatic configuration synchronization in the fabric for IVR zoning. When a CFS is configured on one switch and same properties can be transmitted on other switches. You can enable or disable IVR on the switch. Furthermore, you can enable or disable both CFS and global CFS on the selected switch.

Choose **IVR** radio button on Zoning type, Click **set-up assistant** icon next to **VSAN** field to view CFS window.

You can view below tabs on CFS window:

- Control
- IVR
- Action

The following table describes the fields that appear on **Control** tab.

Fields	Description
Switch	Specifies IP address of the switch.

Fields	Description
IVR Status	Displays whether IVR is enabled or disabled on the switch.
Edit	Click **Edit** icon to enable or disable IVR on the switch and click tick mark to save changes.
Refresh	Click **Refresh** icon to refresh table.
Apply	Click **Apply** to save changes for each modification on the switch.
Done	Click **Done** to save all changes and to exit from CFS window.

The following table describes the fields and descriptions that appears on **IVR** tab.

Fields	Description
Switch	Specifies IP address of the switch.
CFS Status	Specifies whether CFS status is enabled or disabled.
Global CFS	Specifies whether this feature is enabled or disabled on the switch.
Read from	Specifies status: • Effective DB • Copy DB
Lock Owner	Specifies switch is locked by admin.
Merge Status	Specifies fabric merge that occurred.
Region ID	Specifies the region id of the switch.
Edit	Click **Edit** icon to perform changes in Read from and Region ID column for selected row.
Apply	Click **Apply** to save changes for each modification on the switch
Refresh	Click **Refresh** icon to refresh table.
Done	Click **Done** to save all changes and to exit from CFS window.

To perform various operations on a switch in the IVR tab from SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Select a switch, choose **Actions** > **Commit** and click **Apply** to enable IVR on a switch.

Note
You can commit changes only CFS is enabled on selected switch.

Step 2 Select a switch, choose **Actions** > **Abort** and click **Apply** to disable IVR on a switch.

Step 3 Select a switch, choose **Actions** > **Clear** and click **Apply** to clear IVR information on a switch.

Step 4 Select a switch, choose **Actions** > **Enable CFS** and click **Apply** to enable CFS on a switch.

Step 5 Select a switch, choose **Actions** > **Disable Global CFS** and click **Apply** to enable CFS globally on a switch.

The following table describes the fields and descriptions that appears on **Action** tab.

Actions	Description
Switch	Specifies IP address of the switch.
Active	Specifies switch active status is true or false.
Activation Time	Specifies the activation date and time.
IVR NAT Status	Specifies IVR status is enabled or disabled.
Auto Discover Topology	Specifies whether auto discover topology status is true or false
Edit	Click **Edit** icon to perform changes in IVR NAT Status and Auto Discover Topology columns for selected row.
Region ID	Specifies the region id of the switch.
Edit	Click **Edit** icon to perform changes in Read from and Region ID column for selected row.
Apply	Click **Apply** to save changes for each modification on the switch
Refresh	Click **Refresh** icon to refresh table.
Done	Click **Done** to save all changes and to exit from CFS window.

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.

The following table describes the fields and descriptions that appear on SAN Controller **Virtual Management** > **Zoning** Zonesets table.

Field	Description
Zoneset Name	Lists all the names that are configured under the selected Zoneset. Click on the Zoneset name to view the summary information in a slide-in pane. Click **Edit Zoning** to edit and activate zoneset.
Modified	Displays if the zoneset is modified or not.
Zones	Lists all the Zones that are configured under the selected Zoneset.
Members	Lists the members present in the selected Zone.
Activation Date	Specifies date of the zoneset activated.

Procedure

Step 1 To create zonesets from SAN Controller Web UI, choose **Actions** > **Create Zoneset**.

The **Create Zoneset** window appears.

Step 2 Enter a valid name for the zoneset, and click **Create zoneset**.

A zoneset is created and is listed in the **Zoneset** area.

Step 3 To Copy/Clone zonesets, choose radio button and choose **Actions** > **Copy / Clone Zoneset** or click **ellipse** icon in last column on required zone name.

The **Clone or Copy Zoneset** window shows two options.

Choose the appropriate radio button. You can choose one 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 names** or **Append names** 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 **Copy zoneset** 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 next to **Zoneset Name** column and choose **Actions** > **Delete Zoneset**.

A confirmation window appears. Click **Yes** to delete the zoneset.

Step 5 To edit the zone name, choose the zone radio button next to the **Zoneset Name** column and choose **Actions>** > **Edit zones & members** or click **ellipse** icon in last column on required zone name.

The **Zoneset** page for the selected fabric is displayed.

Choose check box next to **Zone Name** column, choose **Actions** > **Rename zone**.

Enter the new name for the zoneset. Click **Rename**.

Step 6 To deactivate a zoneset, choose the zoneset radio button next to the **Zoneset Name** column and click **Actions** > **Deactivate**.

A confirmation window appears. Click **Yes** to deactivate the zoneset.

Step 7 To activate a zoneset, choose radio button next to the **Zoneset Name** column and click **Activate**.

The **Zoneset Differences** window shows the changes made to the zoneset since it was activated previously. Click **Activate**.

Zones

UI Path: **Virtual Management > Zoning**. Select a zone member, a slide-in panel appears. Click on **Launch** icon to view **Zones** window.

Based on the Zoneset that is selected, the zones that are configured under that zoneset are displayed in the **Zones** area. To view Zones tab, click on a radio button for a zoneset, choose **Actions** > **Edit zones & members**. A **Zoneset** window is displayed. It also displays true or false only when the VSAN has smart zone that is enabled.

You can create, copy, delete, or clone, and rename the zones. It also displays true or false only when the VSAN has smart zone that is enabled. 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 Zones area has the following fields and their descriptions.

Field	Description
Filter by Attribute	You can search by specifying the required zone name or zoneset and members.
Add to zoneset	You can select zone name and click **Add to zoneset.**
Refresh	Click **Refresh** icon to refresh table.
Zone Name	Displays the name of the zone. You can search by specifying the zone name. **Note** You cannot save any changes made to topology layout from this screen. Select the zone name to view the members of the zoneset.
In Zoneset	Specifies whether a zone is part of a zoneset. 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.
Members	Specifies the zone members of the zone. You can search by specifying the member.

Procedure

Step 1 To create zones, choose **Virtual Management > Zoning**.

Step 2 In the **Zonesets** area, choose required Zoneset Name.

A slide-in panel is displayed.

a) Click **Edit Zoning** or **launch** icon to view Zoneset window.

By default, Zones tab is displayed.

Step 3 To create a zone, choose **Actions** > **Create new zone**.

a) In the **Create new zone**, enter a valid name for the Zone, and click **Create**.
b) Click **Create new zone**.
c) Choose select box next to **Smart Zoning**, to enable smart zoning for new zone.

A zone is created and is listed in the **Zones** area.

Step 4 To enable a smart zone, choose required check box next to **Zone Name**, choose **Actions** > **Enable smart zoning**.

You can view smart zone column only if smart zoning is enabled for VSAN.

Step 5 To disable a smart zone, choose required check box next to **Zone Name**, choose **Actions** > **Disable smart zoning**.

Step 6 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 7 To rename a zone from a zoneset, choose required check box next to **Zone Name**, choose **Actions** > **Rename zone**.

In the **Name** field, enter the new name for the zone, and click **Rename**.

Step 8 To remove a zone from a zoneset, choose required check box next to **Zone Name**, choose **Actions** > **Remove from 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 9 To delete a zone from a zoneset, choose required check box next to **Zone Name**, choose **Actions** > **Delete zone(s)**.

You can select single or multiple zones to delete at an instant.

Note
You cannot delete a zone that is a member of the selected zoneset. Remove the zone from the zoneset to delete it.

FC Aliases

Navigation Path: **Virtual Management >** > **Zoning** > **Zone Sets** > **Members**

From SAN Controller Release 12.0.1a, FC Aliases feature is supported for regular zones. It is used to associate with one or more pWWNs to a required name. When you add a zone member, you can add FC Alias or delete existing FC Alias. FC Aliases tab displays below fields:

- FC Alias – Specifies the name of FC Alias.
- Member – Specifies members associated with FC Alias.

To do FCAliases operations, perform the following steps:

Procedure

Step 1 Choose **Virtual Management** > **Regular Zones**, click required Zoneset Name.

A slide-in panel window appears.

Step 2 Click **Edit Zoning** or **Launch** icon to view **Zoneset** page.

The Zoneset window is displayed.

Step 3 Click **FC Aliases** tab to view the FC Aliases area.

Step 4 To create a new FC alias, choose **Actions** > **Create new FC Alias**.

The **Create new FC Alias** window is displayed.

a) Enter a valid name in a text field and click **Create FC Alias**.

An FC alias is created and is listed in the FC Aliases area.

Step 5 To delete a new FC alias, select required check box next to the **FC Alias** column, choose **Actions** > **Delete FC Alias**.

Members

UI Path: **Virtual Management** > **Zoning** > **Zone Sets** > **Members**

Based on the selected zoneset and zone, the **Members** area displays the zone members and their status. Enter required field name in **Filter by attributes** text field to view member details.

The Members area has the following fields and their descriptions.

Field	Description
Parent	Displays the name of the zone member. You can search by specifying the zone name.
Member	Displays the member name for the zone.
Switch	Specifies the switch that the zone member is linked. You can search by specifying the switch.
Interface	Specifies the interface that the zone member is attached to. You can search by specifying the interface.
Status	Specifies the status of zone.
Zoned By	Displays the type of zoning. You can search by type of zoning such as WWN, FCID, FC Alias, or iSCSI, FWWN, Device Alias, IP Subnet and many more.

Field	Description
FCID	Specifies the FCID associated with the zone member. You can search by specifying the FCID associated with the zone member.
pWWN	Specifies the pWWN of the switch. You can search by specifying the WWN of the switch.

You can add or remove members from the zoneset. Furthermore, you can also add existing members and add existing FC Alias to members.

From SAN Controller Web UI, choose **Virtual Management** > **Zoning** > **Zoneset** > **Members** to view Members area on **Zoneset** window.

Select a zoneset and zones to view the list of zone members.

Procedure

Step 1 To create new member, In **Members** area, choose **Actions** > **Create new member**.

In the **Create and Add a new Member** window, choose radio button of the appropriate zone.

Enter a valid name in text field and click **Create Member**.

Based on Zone by radio button section, the new name is only for the selected zone by and not for all the zone. For example, when you choose WWN zone by, the name in the text field is for WWN zone. Similarly, when you choose **Domain & Port zone** by, the Domain ID number and Switch Interface name.

The Create new Member allows you to add a member to a zone that does not exist in the fabric, currently. This feature can 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 a zone member, choose check box next to **Parent** column and then click **Actions** > **Remove Member from zone(s)**

You can select multiple zones in an instance to remove.

Step 3 To add existing member, choose **Actions** > **Add existing members**.

The **Add existing members** window is displayed.

This window has the following fields and their descriptions.

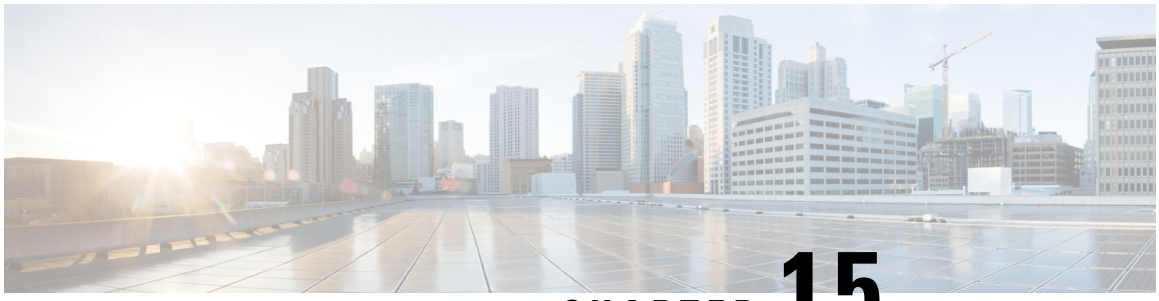
Field	Description
Zone By	The **Zone by** feature determines if the device must be added to the zone using the device WWN or device alias. If you choose **Zone By: End Ports**, the devices are added to the zones by WWN. Similarly, for Device Alias and FC Alias the devices are added to the zones by Device Alias and FC Alias respectively. Based on the zone by you choose, the devices are displayed.

Field	Description
Member Name	Displays the name of the zone. You can search by specifying the zone name.
Type	Specifies the switch is storage or host.
Switch	Specifies the switch that the zone member is linked. You can search by specifying the switch.
Interface	Specifies the interface that the zone member is attached to. You can search by specifying the interface.
pWWN	Specifies the pWWN of the switch. You can search by specifying the pWWN of the switch.
VSAN	Specifies the VSAN the zone member is in.

Step 4 Select the appropriate **Zone by** option and select required **Member Name**.

Step 5 Click **Add members**.

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.



CHAPTER 15

Virtual Infrastructure Manager

- Virtual Infrastructure Manager, on page 153
- **Adding vCenter Visualization**, on page 156

Virtual Infrastructure Manager

UI Path: **Virtual Management** > **Virtual Infrastructure Manager**

Note Ensure that you have enabled Network visualization of Virtual Machines feature for Cisco Nexus Dashboard Fabric Controller.

The following table describes the fields that appear on Virtual Infrastructure Manager window:

Field	Description
Server	Specifies the Server IP Address.
Managed	Specifies the status of the cluster either Managed or Unmanaged.
Status	Specifies the status of the added cluster.
User	Specifies the user created the cluster.
LastUpdated Time	Specifies the last updated time for the cluster.

Note Click **Refresh** icon to refresh the Virtual Infrastructure Manager table.

The following table describes the action items, in the Actions menu drop-down list, that appear on Virtual Infrastructure Manager window:

Action Item	Description
Add Instance	From the **Actions** drop-down list, choose **Add Instance**. For more instructions, see Adding an Instance. **Note** Ensure that you have configured same IP address on Routes. Refer to Configuring Routes IP Address.
Edit Instance	Choose an instance to edit. From the **Actions** drop-down list, choose **Edit Instance**. Make the necessary changes and click **Save**. Click **Cancel** to discard the changes.
Delete Instance(s)	Choose one or more required instance to delete. From the **Actions** drop-down list, choose **Delete Instance(s)**. Click **Confirm** to delete the instance. Click **Cancel** to discard the delete.
Rediscover Instance(s)	Choose one or more required instance to rediscover. From the **Actions** drop-down list, choose **Rediscover Instance(s)**. A confirmation message appears.

For more information:

Support for Cisco UCS B-Series Blade Servers

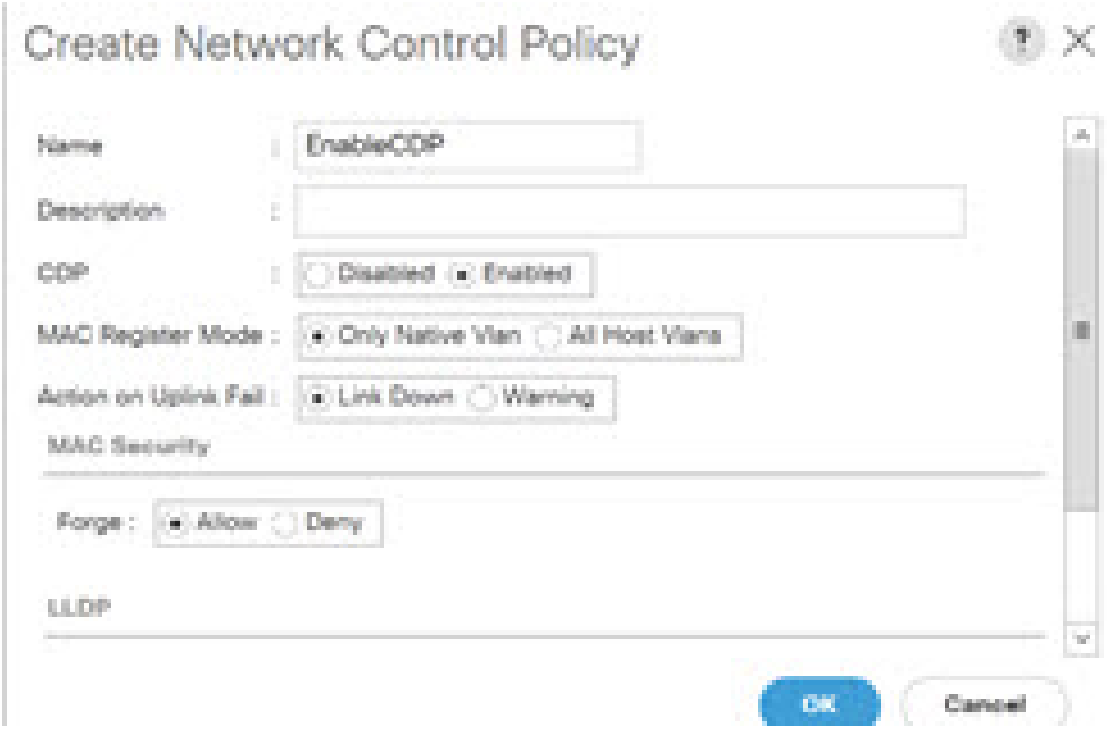
NDFC supports hosts running on UCS type B (chassis UCS) that are behind the Fabric interconnect. You must enable CDP of the vNIC on Cisco UCSM to use this feature.

Note By default, CDP is disabled on Cisco UCSM.

Let us consider two VMMs, VMM-A and VMM-B, for reference. After the discovery of Cisco UCS UCS B-Series Blade Servers, the Topology displays the blue colored VMM-A and VMM-B are fabric interconnect nodes. A sample topology is as shown in the figure below.

To enable CDP on UCSM, you must create a new Network Control policy using the following steps:

1. On the USCM, choose **LAN** and expand the policies.
2. Right-click on the **Network Control Policies** to create a new policy.
3. In the Name field, enter the policy name as **EnableCDP**.
4. Choose **enabled** option for CDP.



5. Click **OK** to create the policy.

To apply the new policy to the ESX NICs, perform the following steps:

- If you are using updated vNIC templates, choose each vNIC template for your ESXi vNICs, and apply the EnableCDP policy from the Network Control Policy drop-down list.
- If you are not using any vNIC templates, use the updated Service Profile Template. Apply EnableCDP policy on each of the service profile template.
- If you are using one-off Service Profiles (i.e., if each server using its own service profile), then you must go to every Service Profile and enable EnableCDP policy on every vNIC.

For more information about Cisco UCSM, refer to Cisco UCSM Network Management Guide.

Configuring Routes IP Address

Before you add IP address to vCenter, you must configure same IP address on Cisco Nexus Dashboard.

To configure Routes on Cisco Nexus Dashboard, perform the following steps:

Procedure

Step 1 Choose **Infrastructure** > **Cluster Configuration**.

Step 2 On **General** tab, in **Routes** card, click **Edit** icon.

The **Routes** window appears.

Step 3 To configure IP addresses, click **Add Management Network Routes**, enter required IP addresses, and click **check** icon.

Step 4 Click **Save**.

The route configuration is governed by following two scenarios:

a. For vCenter, which is an application server is typically reachable over mgmt network.

b. The ESXi servers that are managed by vCenters and the baremetal servers hosting the K8s instances and/or OpenStack instances would be connected to the fabric network directly. Hence, they will be reachable over data networks.

Adding vCenter Visualization

You can perform various actions in the **Actions** menu drop-down list, that appear on **Virtual Management > Virtual Infrastructure Manager.**

Procedure

Step 1 Choose **Actions** > **Add Instance**.

The **Add Instance** window appears.



Step 2 Choose **vCenter** from Select Type drop-down list.

Enter required IP address or Domain name and password in the respective fields.

Step 3 Click **Add**.

You can view added vCenter cluster in the **Virtual Infrastructure Manager** window.

Step 4 To edit an instance**,** choose required vCenter, choose **Actions > Edit Instance** and click **Save** changes.

You can update password for the selected vCenter cluster and change the admin status to Managed or Unmanaged and vice-versa.

Note
For the vCenter cluster in Unmanaged status, you cannot view the topology and vCenter cluster details on dashboard.

Step 5 To delete one or more vCenter cluster, choose the required vCenter, choose **Actions** > **Delete Instance(s)** and click **Confirm** changes.

Note
All the data will be deleted if you delete the Cluster. The Cluster will be removed from the Topology view also.

Step 6 To rediscover one or more vCenter cluster, choose the required vCenter, choose **Actions > Rediscover Instance(s)**.

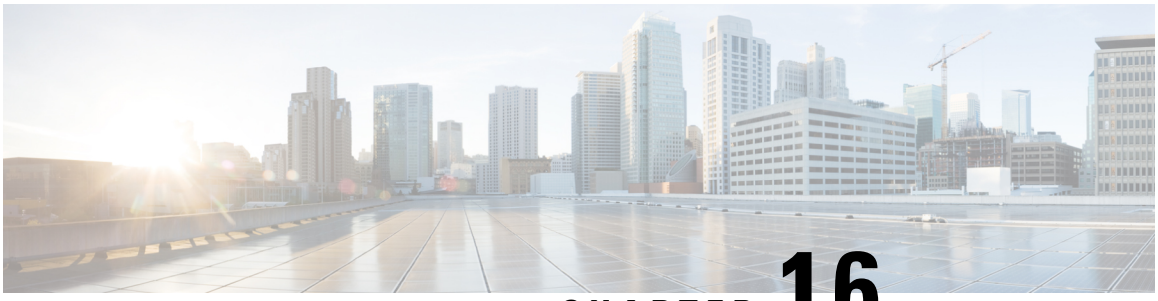
A confirmation message appears.



PART III

Settings

- Server Settings, on page 161
- Feature Management, on page 163
- Credentials Management, on page 167



CHAPTER 16

Server Settings

• Server Settings, on page 161

Server Settings

You can set the parameters that are populated as default values.

To set the parameters of the Nexus Dashboard Fabric Controller server from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Choose **Settings > Server Settings**.

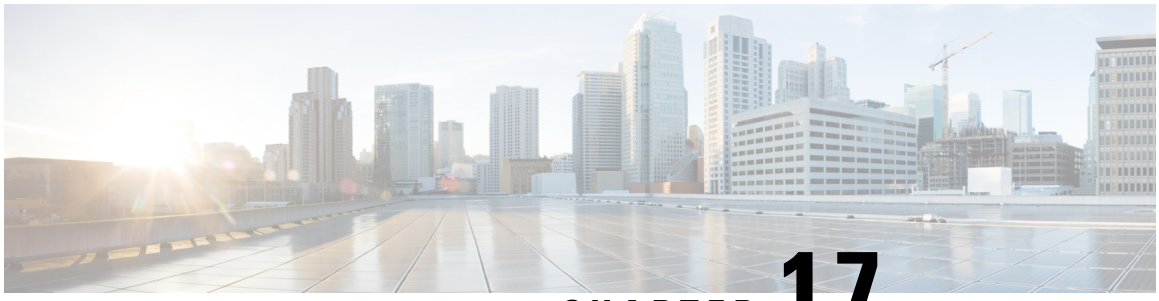
   Server settings are classified under different tabs,

2. Modify the settings based on the requirement.
3. Click **Save** to apply the new modified settings.

Each microservice of enabled features has other tabs and properties other than listed below. Each field has short description. If there is error during configuring any features, corresponding tab is highlighted in red, and **Save** button is disabled till the errors are resolved. Comprehensive checks are performed in NDFC server by the microservices, if there are any errors is displayed on NDFC UI. Server settings supported for 'all-or-none' to save properties and it doesn't support partial updates.

Note You can modify required properties in server settings without support of Cisco TAC.

Note If Nexus Dashboard is rebooted, NDFC services are down for some time.



CHAPTER 17

Feature Management

• Feature Management, on page 163

Feature Management

In Cisco DCNM Release 11.x, you must choose the install mode while installing the DCNM. From Release 12.0.1a, Cisco Nexus Dashboard Fabric Controller allows you to install the service on the Nexus Dashboard. After you launch the Nexus Dashboard Fabric Controller UI, you will see three different Install modes on the Feature Management page.

Nexus Dashboard Fabric Controller 12 allows you to dynamically enable the feature set and scale applications. Choose **Settings > Feature Management** to choose the installer type and enable or disable few features on the selected deployment.

When you launch Nexus Dashboard Fabric Controller for the first time from Cisco Nexus Dashboard, the Feature Management screen appears. You can perform only Backup and Restore operations before you choose the feature set.

On the Feature Management page, you can choose one of the following install modes:

- Fabric Discovery
- Fabric Controller
- SAN Controller

After you select a Feature Set, from the next login, Dashboard page opens when you launch Cisco Nexus Dashboard Fabric Controller from Nexus Dashboard.

Choosing Feature Set

When you launch Cisco Nexus Dashboard Fabric Controller 12 for the first time, none of the feature set is enabled. During this state, you can perform Backup and Restore to restore the DCNM 11.5(x) data on Nexus Dashboard Fabric Controller 12. Nexus Dashboard Fabric Controller will read the data from the backup file and select the installer type accordingly.

To deploy feature-set from Cisco Nexus Dashboard Fabric Controller Web UI perform the following steps:

Procedure

Step 1 Choose **Settings** > **Feature Management**.

Step 2 Select a persona to view the default set of features.

For information about the features available in Cisco NDFC personas, see Features with each Persona, on page 164.

Step 3 In the table below, select the check box against the feature name available with the feature set.

Step 4 Click **Apply**.

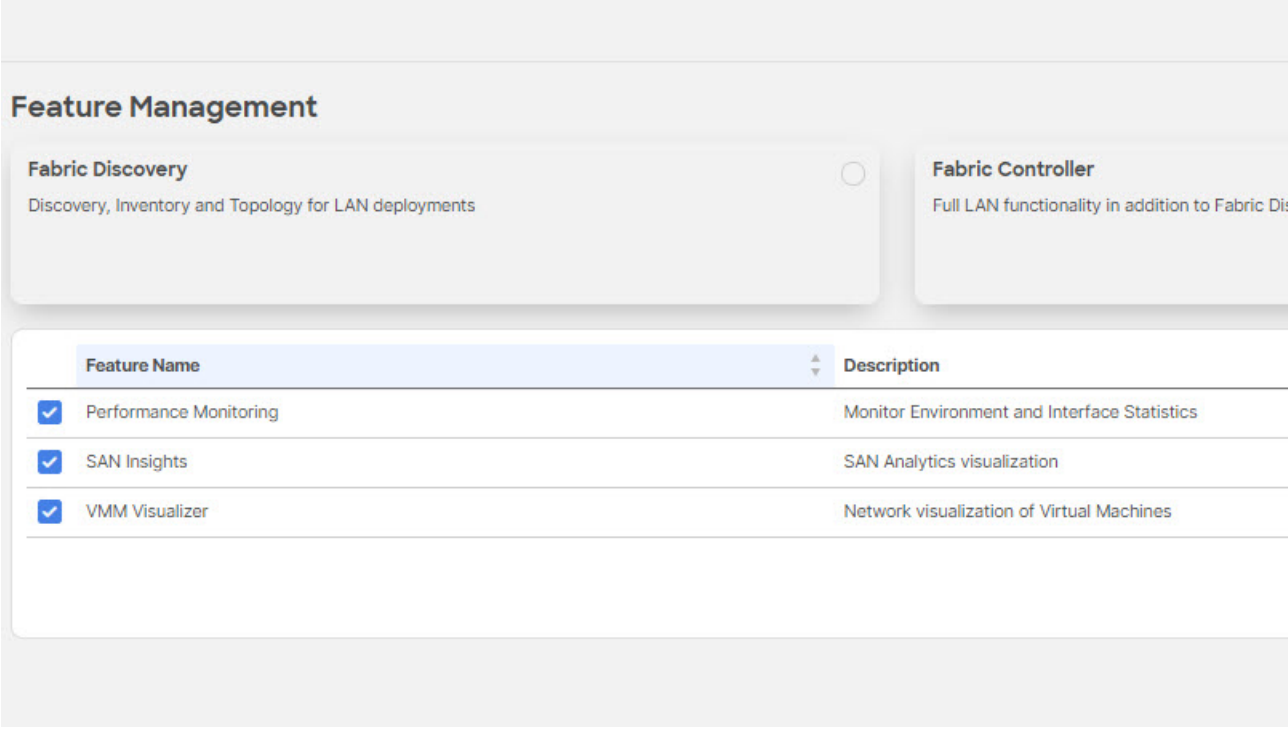
The feature-set will be deployed. The selected applications will be enabled. A message appears that the feature set is installed, and you must refresh to take effect.

Step 5 Refresh the browser to deploy Nexus Dashboard Fabric Controller with the selected feature set and applications.

The left pane shows the features supported specifically with the deployed feature set.

Features with each Persona

SAN Controller



Performance Monitoring

Enable this feature to monitor performance of fabrics in NDFC. See Configuring Performance for more information.

SAN Insights

The SAN Insights feature enables you to configure, monitor, and view the flow analytics in fabrics. SAN Insights features of SAN Controller enable you to visualize the health-related indicators in the interface so that you can quickly identify issues in fabrics. See SAN Insights for more information.



Note Before you install or upgrade to SAN Controller Release 12.1.1e, ensure that you configure persistent IP address on Cisco Nexus Dashboard.

VMM Visualizer

Enable this feature to configure network visualization of Virtual Machines on fabrics. See Virtual Infrastructure Manager, on page 153 for more information.



Note SAN Insights and VMM Visualizer features are not enabled after restore. You must choose check boxes on **Settings** > **Feature Management** and click **Save** to enable these features after restore.

Changing across Feature-Set

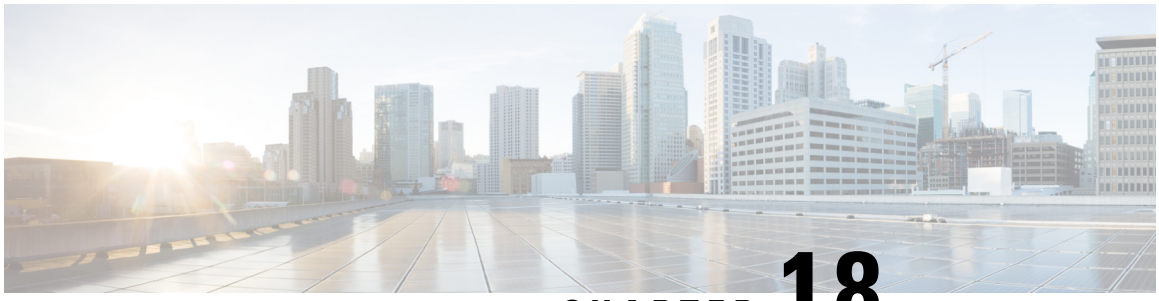
Nexus Dashboard Fabric Controller 12 allows you to switch from one feature set to another. Choose **Settings** > **Feature Management**. Select the desired feature set and applications in the table below. Click **Save & Continue**. Refresh the browser to begin using Cisco Nexus Dashboard Fabric Controller with the new feature set and applications.

There are a few features/applications supported with specific deployments. When you change the feature set, some of these features are not supported in the new deployment. The following table provides details about the pre-requisites and criteria based on which you can change the feature set.

Table 19: Supported Switching between deployments

From/To	Fabric Discovery	Fabric Controller	SAN Controller
Fabric Discovery	-	Only monitor mode fabric is supported in Fabric Discovery deployment. When you change the feature set, the fabric can be used in the Fabric Controller deployment.	Not supported
Fabric Controller	You must delete the existing fabrics before changing the fabric set.	If you're changing from Easy Fabric to IPFM fabric application, you must delete the exiting fabrics.	Not supported

From/To	Fabric Discovery	Fabric Controller	SAN Controller
SAN Controller	Not supported	Not supported	-



CHAPTER 18

Credentials Management

• SAN Credentials Management, on page 167

SAN Credentials Management

Choose **Settings > SAN Credentials Management** to display 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 Nexus Dashboard Fabric Controller has the following fields:

Field	Description
Seed Switch	IP address of the switch.
Username	Specifies the username of the Cisco Nexus Dashboard Fabric Controller 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 Nexus Dashboard Fabric Controller 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.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Settings > SAN Credentials Management**.

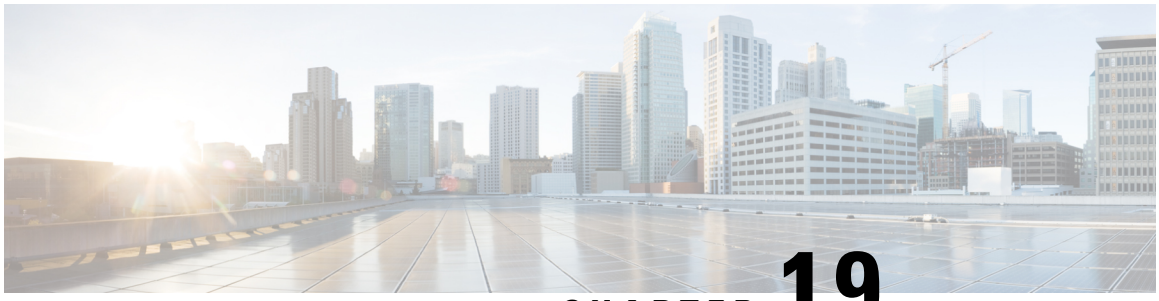
Action Item	Description
Edit	Select a row from the table and choose **Edit** to update the switch credentials information.
Clear	Clears the switch credentials.
Validate	Revalidates the switch credentials.



PART IV

Operations

- Event Analytics, on page 171
- Image Management, on page 187
- Programmable Reports, on page 199
- License Management, on page 205
- Templates, on page 215
- Backup and Restore, on page 247
- NXAPI Certificates, on page 253



CHAPTER 19

Event Analytics

This section contains the following topics:

- Alarms, on page 171
- Events, on page 181
- Accounting, on page 185
- Remote Clusters, on page 186

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.

Alarms Raised

UI Path: **Operations > Event Analytics > Alarms**

1. Click the **Alarms Raised** tab to view the alarm policies that were triggered by an alarm.
2. Click on the **Severity** in the Alarms table to view the history of the alarms raised due to the same policy on the same ITL/ITN flow.
3. Click on policy ID in **ID** column to view the charts.

   A slide-in pane appears with charts.
4. Choose required **Metrics** from drop-down list to view the graph.



Note These metrics can be viewed only for SAN Insights Anomaly Policy.

The following table describes the fields that appear on **Operations > Event Analytics > Alarms > Alarms Raised**.

Field	Description
Severity	Specifies the severity of the alarm
Source	Specifies the name of the source.
Name	Specifies the name of the alarm
Category	Specifies the category of the alarm
Creation Time	Specifies the time at which the alarm was created
Policy	Specifies the policy of the alarm
Message	Displays the message.
Ack User	Displays the username who acknowledged the alarm.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Alarms Raised** tab.

Action Item	Description
Acknowledge	Choose one or multiple alarms and choose **Acknowledge**. Allows you to bookmark the alarms and adds ack user name to **Acknowledged** column.
Unacknowledge	Choose one or multiple alarms and choose **Unacknowledge** to remove the bookmarked alarms. **Note** Only acknowledged alarms can be unacknowledged.
Clear	Choose alarm and choose **Clear** to clear the alarm policy manually. The cleared alarms will be moved to **Alarm Cleared** tab.
Delete Alarm	Choose an alarm and choose **Delete** to delete the alarm.

Alarms Cleared

UI Path: **Operations > Event Analytics > Alarms > Alarms Cleared**

Alarms Cleared tab has the list of alarms which are cleared in the **Alarms Raised** tab. 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 view the cleared alarm details for maximum of 90 days.

You can choose one or more alarms and click the **Actions > Delete** to delete them.

The following table describes the fields that appear on **Alarms Cleared** tab.

Field	Description
Severity	Specifies the severity of the alarm.
Source	Specifies the IP Address of source alarm.

Field	Description
Name	Specifies the name of the alarm.
Category	Specifies the category of the alarm.
Creation Time	Specifies the time at which the alarm was created.
Cleared Time	Specifies the time at which the alarm was cleared.
Cleared By	Specifies the user who cleared the alarm.
Policy	Specifies the policy of the alarm.
Message	Specifies the CPU utilization and other details of alarm
Ack User	Specifies the acknowledged user role name.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Alarms Cleared** tab.

Action Item	Description
Delete Alarm	Select an alarm and choose **Delete** to delete the cleared alarm

Monitoring and Adding Alarm Policies

In Cisco SAN Controller to enable alarms, Navigate to **Operations** > **Event Analytics** > **Alarms**, click **Alarm Policies** on vertical tab. Ensure that the Enable external alarms check box is selected. You must restart SAN Controller Server to bring this into effect.

You can forward alarms to registered SNMP Listeners in SAN Controller. From Cisco SAN Controller web UI, choose **Settings > Server Settings > Alarms**, ensure that the **Enable external alarms** check box is selected. You must restart SAN Controller Server to bring this into effect.

You can forward alarms to registered SNMP Listeners in SAN Controller. From Cisco SAN Controller web UI, choose **Settings > Server Settings > Alarms**, enter an external port address in alarm.trap.listener.address field, click **Apply Changes**, and restart SAN Controller.

Note Ensure that you select **Forwarding** check box in **Alarm Policy creation** dialog window to enable forwarding alarms to external SNMP Listener.

The following table describes the fields that appear on **Operations > Event Analytics > Alarms > Alarms Policies**.

Field	Description
Name	Specifies the name of the alarm policy
Description	Specifies the description of the alarm policy
Status	Specifies the status of the alarm policy: • Activated • Deactivated

Field	Description
Policy type	Specifies the type of the policy: • Device Health Policy • Interface Health Policy • Syslog Alarm Policy • Hardware Health Policy • SAN Insights Anomaly
Devices	Specifies the devices to which the alarm policy is applied.
Interfaces	Specifies the interfaces.
Details	Specifies the details of the policy.

The following table describes the action items, in the **Actions** menu drop-down list that appear on **Operations > Event Analytics > Alarms > Alarms Policies**.

Action Item	Description
Create new alarm policy	Choose to create a new alarm policy. See Create new alarm policy section.
Edit	Select a policy and choose **Edit** to edit the alarm policy.
Delete	Select a policy and choose **Delete** to delete the alarm policy.
Activate	Select a policy and choose **Activate** to activate and apply the alarm policy.
Deactivate	Select a policy and choose **Deactivate** to disable and deactivate the alarm policy.
Import	Select to import alarm policies from a .txt file.
Export	• Click the box next to a specific alarm policy, then click **Export** to export that alarm policy as a .txt file. • Select or deselect all the boxes next to the alarm policies, then click **Export** to export all the alarm policies as a .txt file.

You can add alarm policies for the following:

- **Device Health Policy**: Device health policies enable you to create alarms when Device SNMP Unreachable, or Device SSH Unreachable. Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.
- **Interface Health Policy**: 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 Policy**: Syslog Alarm Policy defines a pair of syslog messages formats; one which raises the alarm, and one which clears the alarm.
- **Hardware Health Policy**: The hardware health policy is used to raise hardware-related alarms for different parameters, such as fan status, power supply, modular status and all interface-related alarms.

- **San Insights Anomaly Policy**: SAN Insights Anomaly Policy enables you to create customized alarms to identify issues in the fabric using SAN Insight data.

Create new alarm policy

You can add alarm policies for the following:

- Device Health Policy
- Interface Health Policy
- Syslog Alarm Policy
- Hardware Health Policy
- SAN Insights Anomaly

After you create a new alarm policy, in the **Alarm Policies** tab, click **Refresh** to view the newly-created alarm policy.

Device Health Policy

Device health policies enable you to create alarms when certain conditions are met. By default, all devices are selected for monitoring.

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: You can forward alarms to registered SNMP listeners in SAN Controller. From the Web UI, choose **Settings** > **Server Settings** > **Events**.



Note Ensure that you select **Forwarding** check box while configuring alarm policies to forward alarms to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From SAN Controller Web UI, choose **Settings** > **Server Settings** > **Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.
- Specify the CPU utilization parameters, memory utilization parameters, and environmental temperature parameters.
- **Device Availability**: Device health policies enable you to create alarms in the following situations:
  - **Device Access**: When device SNMP or device SSH is unnreachable.
  - **Peripherals**: When fan, power supply, or module is unnreachable.

Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.

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.

Interface Health Policy

Interface health policies enable you to monitor the interface status, packet discards, errors and bandwidth details of the interfaces. By default, all interfaces are selected for monitoring.

Select the devices for which you want to create policies and then specify the following parameters:

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: You can forward alarms to registered SNMP listeners in SAN Controller. From the Web UI, choose **Settings** > **Server Settings** > **Events**.



Note Ensure that you select **Forwarding** check box while configuring alarm policies to forward alarms to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From SAN Controller Web UI, choose **Settings** > **Server Settings** > **Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.
- **Linkstate**: Choose linkstate option to check for the interface link status. You can generate an alarm whenever a link is down and clear the alarms when the link is up.
- **Bandwidth (In/Out)**: Allows you to set the maximum bandwidth allowed in inbound and outbound directions. The system generates alarms when the bandwidth exceeds the specified values.
- **Inbound Errors**: Allows you to set thresholds for the number of inbound errors that are discarded after which it generates an alarm.
- **Outbound Errors**: Allows you to set thresholds for the number of outbound errors that are discarded after which it generates an alarm.
- **Inbound Discards**: Allows you to set thresholds for the number of inbound packets that are discarded after which it generates an alarm.
- **Outbound Discards**: Allows you to set thresholds for the number of outbound packets that are discarded after which it generates an alarm.

Syslog Alarm

Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one which clears the alarm.

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.
- Forwarding: You can forward alarms to registered SNMP listeners in SAN Controller. From Web UI, choose **Settings > Server Settings > Events**.

Note Ensure that you select **Forwarding** check box in Alarm Policy creation dialog window to enable forwarding alarms to external SNMP listener.

- Email: You can forward alarm event emails to recipient when alarm is created, cleared or severity changed. From SAN Controller Web UI, choose **Settings > Server Settings > Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.
- 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 20: 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 21: 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 22: 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

Hardware Health Policy

The hardware health policy is used to raise hardware-related alarms for different parameters, such as fan status, power supply, modular status and all interface-related alarms.

By default, there is a hardware policy called as discovery that is standard with the NDFC installation. This hardware policy defines various conditions for different parameters. You can also create custom hardware policies for the parameters listed above and define regex expressions based on which alarms are raised.

By default, the **All Devices** option is selected automatically.

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: You can forward alarms to registered SNMP listeners in SAN Controller. From the Web UI, choose **Settings** > **Server Settings** > **Events**.

Note Ensure that you select **Forwarding** check box while configuring alarm policies to forward alarms to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From SAN Controller Web UI, choose **Settings** > **Server Settings** > **Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.

Hardware alarms are raised based on regex expressions that you enter when you are creating the policy.

In the **Alarms** area, create a hardware health policy to raise alarms for the following parameters:

- **Fan**: Define the severity for fan-related alarms and determine the condition for the alarms.
  1. Click the toggle switch next to **Fan** to enable the fan-related alarms.
  2. Select the severity of the alarm:
     - Critical
     - Major
     - Minor
     - Warning
     - Cleared
  3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status is not that value.

For example, if you enter `ok` in the **Trigger alarm when status is not** field, NDFC will raise an alarm for any status other than `ok`, such as N/A.

4. Click **Save**.

- **Power Supply**: Define the severity for power supply-related alarms and determine the condition for the alarms.
  1. Click the toggle switch next to **Power Supply** to enable the power supply-related alarms.
  2. Select the severity of the alarm:
     - Critical
     - Major
     - Minor
     - Warning
     - Cleared
  3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status is not that value.

     For example, if you enter `ok` in the **Trigger alarm when status is not** field, NDFC will raise an alarm for any status other than `ok`, such as failed, OffEnvpower, OffDenied, and so on.
  4. Click **Save**.
- **Module**: Define the severity for module-related alarms and determine the condition for the alarms.
  1. Click the toggle switch next to **Module** to enable the module-related alarms.
  2. Select the severity of the alarm:
     - Critical
     - Major
     - Minor
     - Warning
     - Cleared
  3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status matches that value.

     For example, if you were to enter the following value in the **Trigger alarm when status matches regex** field, as shown in the information (i) button:

     ```
     ^(?!ok|poweredDown|okButDiagFailed).*$
     ```

     NDFC will raise an alarm when modules are in states other than ok, poweredDown, and OkButDiag failed.
  4. Click **Save**.
- **Interface Status**: Define the severity for interface-related alarms and determine the condition for the alarms.

1. Click the toggle switch next to **Interface Status** to enable the interface-related alarms.
2. Click one or more toggle switches next to the appropriate severity to select the severity of the alarm:
   - Critical
   - Major
   - Minor
   - Warning
   - Cleared
3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status matches that value. The provided regex expression is matched against the combined field of `admin_status:oper_status:status_reason`.

   For example, if you were to enter the following value in the **Trigger alarm when status matches regex** field:

   ```
   ^up:down:(?!Link not connected|XCVR not inserted|sfpNotPresent|Channel admin down).*$
   ```

   NDFC will raise an alarm when interfaces are in states that match these values.
4. Click **Save**.

SAN Insights Anomaly Policy

From Cisco Nexus Dashboard SAN Controller Release 12.0(1), a new policy type saninsights is added. This new policy type can be customized to identify issues. You can create an alarm policy, based on specific flows to retain per interval data for analysis. If selected flow matches alarm policy, maintain the flow based on the parameters defined by the policy.

Procedure

Step 1 Choose **Operations** > **Event Analytics** > **Alarms**.

Step 2 Choose **Alarm Policies** in the **Alarms** tab.

Step 3 Choose **Actions** > **Create new alarm policy**.

Step 4 Use the **San Insights Anomaly Policy** radio button.

Step 5 Specify details for below parameters:

- **Policy Name**: Specify the name for this policy. It must be unique.
- **Description**: Specify a brief description of this policy.
- **Forwarding**: Choose checkbox, to enable forwarding alarms to external SNMP listener.
- **Email**: Choose checkbox, to send mail updates on this policy to mail id.

Step 6 Select time from drop-down list to define **Capture Time** and **Retention Time**.

- **Capture Time**: Specifies the length of time to capture per-interval data for each flow matching the given policy.

- **Retention Time**: Specifies the length of time to keep that data (before it is deleted).

Step 7 Select time or interval from the drop-down list to define **Analysis Level** and select severity level from drop-down list to define the **Severity** of this policy.

- **Analysis Level**: Specifies which aggregation of flow data must be checked for the given policy. Some policy types such as aborts or failures policy are logic to match when it happens instantly (Interval level). Some policy types are as an anomaly policy when they are sustained above a threshold. For example, a momentary ECT or DAL spike in level is not alarming, but if that same spike level is continued for a period (5 minutes or 1 hour) then it must be investigated.
- **Severity**: Specifies the severity that will be associated with any alarms that are raised due to this policy.

Step 8 You can define a new rule, click **Add new rule** and specify mandatory fields and then click **Create new policy**.

Note
- You can define one or more new rules and match criteria to identify a flow and create a new policy.
- All policies are matched against each ITL/ITN flow records streamed to the receiver from the switches.

You can view the created alarms in the **Alarms** tab.

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.

The following table describes the fields that appear on **Operations > Event Analytics > Events**.

Field	Description
Group	Specifies the Fabric
Switch	Specifies the hostname of the switch
Severity	Specifies the severity of the event
Facility	Specifies the process that creates the events. The event facility includes two categories: NDFC and syslog facility. Nexus Dashboard Fabric Controller facility represents events generated by Nexus Dashboard Fabric Controller internal services and SNMP traps generated by switches. Syslog facility represents the machine process that created the syslog messages.
Type	Specifies how the switch/fabric are managed

Field	Description
Count	Specifies the number of times the event has occurred
Creation Time	Specifies the time when the event was created
Last Seen	Specifies the time when the event was run last
Description	Specifies the description provided for the event
Ack	Specifies if the event is acknowledged or not

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Operations > Event Analytics > Events**.

Action Item	Description
Acknowledge	Select one or more events from the table and choose **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 Group.
Unacknowledge	Select one or more events from the table and choose **Unacknowledge** icon to acknowledge the event information for the fabric.
Delete	Select an event and choose **Delete** to delete the event.
Event Setup	Allows you to setup new event. For more information, see Event Setup, on page 182.

Event Setup

To setup an event using the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Operations** > **Event Analytics** and click on the **Events** tab.

Step 2 From the **Actions** drop-down list, select **Event Setup**.
The **Receiver** tab displays the following details:

- **Syslog Receiver enabled**: Displays the status of the syslog server.
- **SNMP Trap Receiver**: Displays the details of SNMP traps received, processed and dropped.
- **Syslog Receiver**: Displays the details of syslog messages received, processed and dropped.

Step 3 Navigate to the **Sources** tab, to view a list of fabrics and its associated switches.
The **Sources** tab displays all the fabrics and the associated switches in tabular format. It also displays if traps and syslogs have been configured on the switches.

Step 4 Perform the following steps to create rules for forwarding email notifications or traps for events:

Cisco Nexus Dashboard Fabric Controller Web UI forwards fabric events through email or SNMPv1 or SNMPv2c traps. Some SMTP servers may require adding authentication parameters to the emails that are sent from Nexus Dashboard Fabric Controller to the SMTP servers.

a) Ensure that you have configured SMTP parameters before configuring rules for forwarding event notifications through emails. To verify SMTP configuration, navigate to **Settings** > **Server Settings** > **SMTP** and verify that you have configured the required fields.

a) To enable events forwarding, choose **Settings** > **Server Settings** > **Events** and configure the fields as described in the following table.

Table 23: Configure Events Forwarding

Field	Description
Enable Event forwarding	Check the checkbox to enable events forwarding feature.
Email Forwarding From Email List	Specifies the email address from which the forwarding messages arrive.
Snooze Event Forwarding	Snoozes an event from forwarding for the given time range.
Maximum Number of Repeats in Event Forwarding	Stops forwarding an event after the specified time. 0 indicates unlimited time.
Maximum Number in Events/Traps/Syslog Queue	Specifies the maximum number in the queue before dropping the incoming events/traps/syslog.

b) To configure rules, choose **Operations** > **Event Analytics**.

c) Navigate to the **Forwarding** tab and choose **Actions** > **Add Rule** and configure the fields as described in the following table.

Table 24: Configure Rules

Field	Description
Forwarding Method	Chooose one of the forwarding methods: • **E-Mail** • **Trap**
Email Address	This field appears if you select **E-mail** as the forwarding method. Enter an email address for forwarding the event notifications.
Address	This field appears if you select **Trap** as the forwarding method. Enter the IP address of the SNMP trap receiver. You can either enter an IPv4 or IPv6 address or a DNS server name.

Field	Description
Port	Enter the port to which the traps are forwarded.
Forwarding Scope	Maximum number in queue before dropping the incoming events/traps/syslog messages.
Fabric	Select **All Fabrics** or a specific fabric for notification.
VSAN Scope	For SAN Installer, select the VSAN scope. You can either choose **All** or **List**.
VSAN List	If you select **List**, provide the list of VSANs for notification.
Source	Select **DCNM** or **Syslog**. If you select **DCNM**, do the following: **1.** From the **Type** drop-down list, choose an event type. **2.** Check the **Storage Ports Only** check box to select only the storage ports. This check box is enabled only for port related events. If you select **Syslog**, do the following: **1.** In the **Facility** list, select the syslog facility. **2.** In the **Type** field, enter the syslog type. **3.** In the **Description Regex** field, enter 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.

The traps that are transmitted by Cisco Nexus Dashboard Fabric Controller 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
```

e) Click **Add Rule**.

Step 5 Perform the following steps to create rules for suppressing events:

Nexus Dashboard Fabric Controller allows you to suppress specified events based on user-specified rules. Such events will not be displayed on the Nexus Dashboard Fabric Controller Web UI and SAN Client. The

events will neither be added to the Nexus Dashboard Fabric Controller database, nor forwarded via email or as SNMP traps.

You can view, add, modify, and delete rules from the table. You can create a rule from the existing events. Select an existing event as the template and open the **Add Rule** window by navigating to **Operations** > **Event Analytics** > **Events** page, select the event and choose **Actions** > **Add Suppresor**. The details are automatically ported from the selected event in the events table to the fields of the **Add Rule** window.

a) In the **Name** field, enter a name for the rule.
b) In the **Scope** field, select one of the following options - **SAN**, **Port Groups** or **Any**.

   In the **Scope** field, the LAN/SAN groups and the port groups are listed separately. 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 select **Any** as the scope, the suppression rule is applied globally.

c) In the **Facility** field, enter the name or choose from the SAN/LAN switch event facility list.

   If you do not specify a facility, a wildcard is applied.

d) In the **Type** field, enter the event type.

   If you do not specify the event type, wildcard is applied.

e) 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.

f) Check the **Active Between** check box and select a valid time range during which the event is suppressed.

   By default, the time range is not enabled.

   Note
   In general, you must not suppress accounting events. Suppression rule for Accounting events can be created only for certain situations where accounting events are generated by actions of Nexus Dashboard Fabric Controller or switch software. For example, 'sync-snmp-password' AAA syslog events are automatically generated during the password synchronization between Nexus Dashboard Fabric Controller and managed switches. To suppress accounting events, navigate to **Operations** > **Event Analytics** > **Events** page, select the event and choose **Actions** > **Add Suppressor**.

g) Click **Add Rule**.

Accounting

You can view the accounting information on Cisco Nexus Dashboard Fabric Controller Web UI.

The following table describes the fields that appear on **Operations > Event Analytics > Accounting**.

Field	Description
Source	Specifies the source
User Name	Specifies the user name.
Time	Specifies the time when the event was created

Field	Description
Description	Displays the description.
Group	Specifies the name of the group.

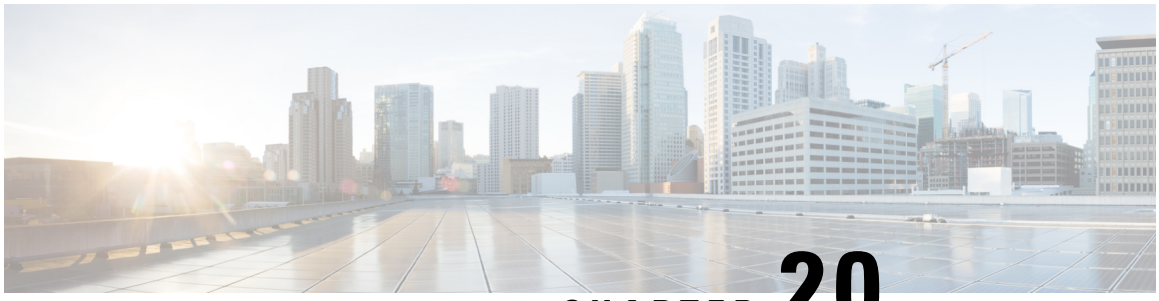
The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Operations > Event Analytics > Accounting**.

Action Item	Description
Delete	Select a row and choose **Delete** to delete accounting information from the list.

Remote Clusters

This tab displays the clusters and the number of Fabrics in each cluster in your setup.

Click on the Cluster Name to see the summary information. You can click on the launch icon to view the detailed summary of the Cluster.



CHAPTER 20

Image Management

- Image Management, on page 187

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.

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.
- In order to execute any ISSU operations, any new NDFC user must first set the necessary device credentials under the Credential Management page. You will not be able to execute ISSU operations without first setting the proper device credentials.

The **Image Management** window has the following tabs and you can perform the operations listed in the Actions column.

Tabs	Actions
Overview	Stage Image Validate Upgrade Apply Policy Recalculate Compliance
Images	Upload
Image Policies	Create
History	History, on page 196

Ensure that your user role is **network-admin** or **device-upg-admin** and you didn't freeze the Nexus Dashboard Fabric Controller to perform the following operations:

- Upload or delete images.
- Install, delete, or finish installation of an image.
- Install or uninstall packages and patches.
- Activate or deactivate packages and patches.
- Add or delete image management policies (applicable only for network-admin user role).
- View management policies.

You can view any of the image installations or device upgrade tasks if your user role is **network-admin**, **network-stager**, **network-operator**, or **device-upg-admin**. You can also view them if your Nexus Dashboard Fabric Controller is in freeze mode.

Here's the process to upgrade the switch image:

1. Discover the switches into Nexus Dashboard Fabric Controller.
2. Upload images.
3. Create image policies.
4. Attach the image policies to the switches.
5. Stage the images on switches.
6. (Optional) Validate if the switches support non-disruptive upgrade.
7. Upgrade the switches accordingly.

Overview

The Overview window displays all the switches that you discover in the Cisco Nexus Dashboard Fabric Controller. You can view information like the current version of the switch, policy attached to it, status, and other image-related information. You can filter and sort the entries.

Nexus Dashboard Fabric Controller UI Navigation

- Choose **Operations > Image Management > Overview.** Click Actions to perform various operations.

Based on the actions you perform, the value under the Reason column is updated.

You can perform the following actions in the **Overview** window:

Staging an Image

After attaching an image policy to a switch, stage the image. When you stage an image, the files are copied into the bootflash.

To stage an image from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

- Attach a policy to the selected devices before staging an image on the device.
- The minimum supported NX-OS image version in SAN Controller is 6.1(2)I1(1).

  To stage an image on Cisco Nexus 9000 or Nexus 3000 switches running NX-OS version earlier than the version mentioned above, you must set **Use KSTACK to SCP on N9K, N3K** value to False. On the Web UI, choose **Settings > Server Settings > SSH** tab. Uncheck the **Use KSTACK to SCP on N9K, N3K** check box. If you're staging supported image versions, check this check box.

Procedure

Step 1 Choose **Operations > Image Management > Overview**.

Step 2 Choose a switch by checking the check box.

Note
You can choose more than one switch to stage an image.

Step 3 Click **Actions** and choose **Stage Image**.

The **Select Images to Install window** appears.

In this window, you can view how much space is available on the switch and how much space is required.

Step 4 (Optional) Click the hyperlink under the Files For Staging column to view the files that are getting copied to the bootflash.

Step 5 Click **Stage**.

You will be diverted to the Overview tab under the Image Management window.

Step 6 (Optional) You can view the status under the Image Staged column.

Step 7 (Optional) Click the hyperlink under the Reason column to view the log.

Validating an Image

Before you upgrade the switches, you can validate if they support non-disruptive upgrade. To validate an image from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Operations > Image Management > Overview**.

Step 2 Choose a switch by checking the check box.

Note
You can choose more than one switch to stage an image.

Step 3 Click **Actions** and choose **Validate**.

The **Validate** dialog box appears.

Step 4 Check the Confirm non disruptive upgrade check box.

Step 5 Click **Validate**.

You'll return to the Overview tab under the Image Management window.

Step 6 (Optional) You can view the status under the Validated column.

Step 7 (Optional) Click the hyperlink under the Reason column to view the log.

Upgrading an Image

You can upgrade or uninstall a switch. Upgrade Groups option allows you to trigger image upgrade on multiple switches at an instant. This option can be selected for upgrade/downgrade options.



Note It is recommended to perform upgrade for maximum of twelve switches at once. If you choose more than twelve switches, the upgrade happens sequentially.

Upgrade Options for NX-OS Switches

- Disruptive: Choose this option for disruptive upgrades.
- Allow Non-disruptive: Choose this option to allow non-disruptive upgrades. When you choose **Allow Non Disruptive** option and if the switch does not support non-disruptive upgrade, then it will go through a disruptive upgrade. When you choose **Force Non Disruptive** and 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.
- When you select multiple switches with different roles to upgrade, a warning message appears to review the switch selection, click **Confirm** to upgrade or click **Cancel**.

  Ensure that the below limitation is applicable while adding devices in a same group, else a warning message is displayed to review the switch selection:

  - For all Peers, Spines, Borders, Border Gateways, RPs, or RRs in a fabric, if more than one switch is with same role in a fabric.



Note The upgrade groups are automatically deleted, if the attached devices are detached from the created or upgrade or modify group.

To upgrade a switch image from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Operations** > **Image Management** > **Overview**.

Step 2 Choose a switch by checking the check box.

Step 3 Click **Actions** and choose **Upgrade**.

The **Upgrade/Uninstall** window appears.

Step 4 Choose the type of upgrade by checking the check box.

The valid options are NXOS, EPLD, and Packages (RPM/SMU).

Step 5 Choose NXOS, EPLD, or Packages:

a) Choose an upgrade option from the drop-down list based on how you want to upgrade.
b) (Optional) Check the BIOS Force check box.

You can view thee validation status of all the devices.

c) Check the **Golden** check box to perform a golden upgrade.
d) Enter the module number in the **Module Number** field.

You can view the module status below this field.

Note

- If you choose **Packages**, you can view the package details too.
- You can uninstall the packages by selecting the **Uninstall** radio button.

Step 6 Click **Upgrade**.

Note
Upgrade status takes 30 - 40 minutes to update, if multiple switches are upgraded.

Modifying a Policy

You can update the image policy that you have attached to a switch. You can change an image policy for multiple switches at the same time.

To attach or change an image policy attached to a switch from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Operations > Image Management > Overview**.

Step 2 Choose a switch by checking the check box.

Step 3 Click **Actions** and choose **Modify Policy**.

The **Modify Policy** dialog box appears.

Step 4 You can either attach or detach a policy, choose required check box.

Step 5 Choose a policy from the Policy drop-down list.

Step 6 Click required **Attach** or **Detach**.

Step 7 (Optional) Click the hyperlink under the Reason column to view the changes.

Step 8 (Optional) Click the hyperlink under thee Status column to view the current and expected image versions.

If the switch is in **Out-Of-Sync** status, view the expected image versions and upgrade the switch accordingly.

Recalculating Compliance

To recalculate the configuration compliance of a switch from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Operations > Image Management > Overview**.

Step 2 Choose a switch by checking the check box.

Step 3 Click **Actions** and choose **Recalculate Compliance**.

Step 4 Click the hyperlink under the Reason column to view the changes.

Images

You can view the details of the images and the platform under this tab. You can upload or delete images to a device.

The following table describes the fields that appear on **Operations > Image Management > Images**.

Field	Description
Platform	Specifies the name of the platform. Images, RPMs, or SMUs are categorized as follows: • N9K/N3k • N6K • N7K • N77K • N5K • Other • Third Party The images are the same for N9K and N3K platforms. The platform is **Other** if the uploaded images are not mapped to any of the existing platforms. The platform is **Third Party** for RPMs.
Bits	Specifies the bits of the image

Field	Description
Image Name	Specifies the filename of the image, RPM, or SMU that you uploaded.
Image Type	Specifies the file type of the image, EPLD, RPM, or SMU.
Image Sub Type	Specifies the file type of the image, EPLD, RPM, or SMU. The file type EPLDs are **epld**. The file types of images are **nxos**, **system** or **kickstart**. The file type for RPMs is **feature** and for SMUs the file type is **patch**.
NXOS Version	Specifies the NXOS image version for only Cisco switches.
Image Version	Specifies the image version for all devices, including the non-Cisco devices as well.
Size (Bytes)	Specifies the size of the image, RPM, or SMU files in bytes.
Checksum	Specifies the checksum of the image. The checksum checks if there's any corruption in the file of the image, RPM, or SMU. You can validate the authenticity by verifying if the checksum value is same for the file you downloaded from the Cisco website and the file you upload in the **Image Upload** window.

The following table describes the action items, in the **Actions** menu drop-down list, that appears on **Operations > Image Management > Images**.

Action Item	Description
Refresh	Refreshes the Images table.
Upload	Click to upload a new image. For instructions, see Uploading an Image, on page 194.
Delete	Allows you to delete the image from the repository. Choose an image, click **Actions**, and choose **Delete**. A confirmation window appears. Click **Yes** to delete the image. **Note** Before deleting an image, ensure that the policy attached to the image, is not attached to any switches. **Note** If you delete an image on a switch in switch console, allow maximum of 24 hours to refresh and view update on NDFC. Else, on NDFC UI, navigate **LAN** > **Fabrics** > **Switches**, choose switch for which image is deleted and click **Actions** > **Discover** > **Rediscover** to view updates.

Uploading an Image

You can upload 32-bit and 64-bit images. To upload different types of images to the server from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Note Devices use these images during POAP or image upgrade. All the images, RPMs, and SMUs are used in the **Image Policies** window.

Your user role should be **network-admin**, or **device-upg-admin** to upload an image. You can't perform this operation with the **network-stager** user role.

Procedure

Step 1 Choose **Operations > Image Management > Images**.

Step 2 Click **Actions** and choose **Upload**.

The **Upload Image** 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 **OK**.

You can upload a ZIP or TAR file as well. Cisco Nexus Dashboard Fabric Controller processes and validate the image file and categorize it under the existing platforms accordingly. If it doesn't fall under **N9K/N3K**, **N6K**, **N7K**, **N77K**, or **N5K** platforms, the image file is categorized under **Third Party** or **Other** platform. The **Third Party** platform is applicable only for RPMs.

Step 5 Click **OK**.

The EPLD images, RPMs, and SMUs are uploaded to the repository in the following path: `/var/lib/dcnm/upload/<platform_name>`.

Note
If only EPLD files are uploaded, you cannot create policy as Release drop-down list is empty for EPLD images.

All NX-OS, kickstart and system images are uploaded to the repository in the following paths: `/var/lib/dcnm/images and/var/lib/dcnm/upload/<platform_name>`

The upload takes some time depending on the file size and network bandwidth.

Note
You can upload images for all Cisco Nexus Series Switches.

You can upload EPLD images only for Cisco Nexus 9000 Series Switches.

If your network speed is slow, increase the wait time of Cisco Nexus Dashboard Fabric Controller to 1 hour so that the image upload is complete. To increase the wait time from Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

a) Choose **Settings > Server Settings**.
b) Search for the **csrf.refresh.time** property, and set the value as **60**.

The value is in minutes.

c) Click **Apply Changes**.
d) Restart the Nexus Dashboard Fabric Controller server.

Image Policies

The image management policies will have the information of intent of NX-OS images along with RPMs or SMUs. The policies can belong to a specific platform. Based on the policy applied on a switch, Cisco Nexus Dashboard Fabric Controller checks if the required NXOS and RPMs or SMUs are present on the switch. If there is any mismatch between the policy and images on the switch, a fabric warning is generated.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Operations > Image Management > Image Policies**.

Action Item	Description
Create	Allows you to create a policy that can be applied to images. See Creating an Image Policy, on page 195 section.
Delete	Allows you to delete the policy. Choose a policy, click **Actions**, and choose **Delete**. A confirmation window appears. Click **Confirm** to delete the **policy**. **Note** An error message appears if you try to delete a policy that is attached to a device.
Edit	Allows you to edit the policy.

Creating an Image Policy

To create an image policy from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

Upload the images under the **Images** tab before creating an image policy. See the Uploading an Image, on page 194 for more information about uploading images.

Procedure

Step 1 Choose **Operations > Image Management > Image Policies**.

Step 2 Click **Actions > Create**.

The **Create Image Management Policy** dialog box appears.

Step 3 Enter information for the required fields.

The following fields appear in the **Create Image Management Policy** dialog box.

Fields	Actions
Policy Name	Enter the policy name.
Platform	Choose a platform from the Platform drop-down list. The options will be populated based on the images you upload in the **Images** window. The options for the **Release** drop-down list will be autopopulated based on the platform you choose.
Release	Choose the NX-OS version from the **Release** drop-down list. The release versions of 64-bit images are appended with 64bit in the image name. **Note** If only EPLD files are uploaded, you cannot create policy as Release drop-down list is empty for EPLD images.
Package Name	(Optional) Choose the packages. before choose Packages, View All Packages check box to display all uploaded packages for a given platform (its version agnostic).
Policy Description	(Optional) Enter a policy description.
EPLD	(Optional) Check the EPLD check box if the policy is for an EPLD image.
Select EPLD	(Optional) Choose the EPLD image.
RPM Disable	(Optional) Check this check box to uninstall the packages.
RPMs To Be Uninstalled	(Optional) Enter the packages to be uninstalled separated by commas. You can enter the package names only if you check the RPM Disable checkbox.

Step 4 Click **Save**.

What to do next

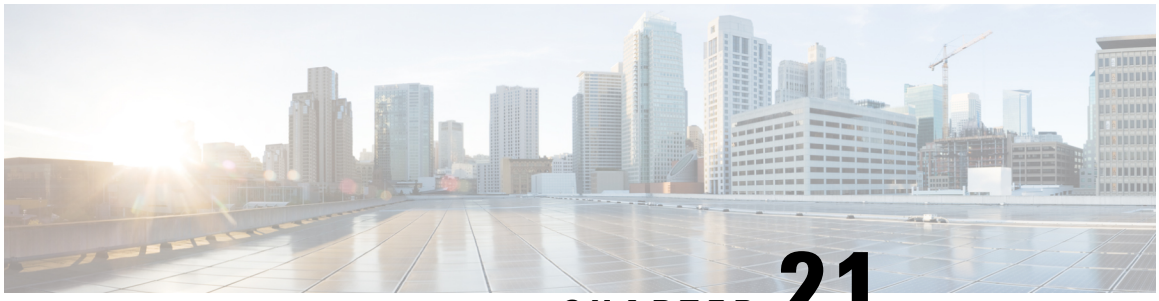
- Attach the policy to a device. See Modifying a Policy, on page 191 section for more information.
- To edit an image policy after you've created it, click **Actions** > **Edit**.
- To delete an image policy, click **Actions** > **Delete**.

History

You can view the history of all the Image Management operations from **Operations** > **Image Management** > **History** tab.

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

Field	Description
ID	Specifies the ID number.
Device Name	Specifies the device name.
Version	Specifies the version of the image on the device.
Policy Name	Specifies the policy name attached to the image.
Status	Displays if the operation was a success or failure.
Reason	Specifies the reason for the operation to fail.
Operation Type	Specifies the type of operation performed.
Fabric Name	Specifies the name of the Fabric.
Created By	Specifies the user name who performed the operation.
Timestamp	Specifies the time when the operation was performed.



CHAPTER 21

Programmable Reports

The **Programmable Reports** application enables the generation of reports using Python 2.7 scripts. Report jobs are run to generate reports. Each report job can generate multiple reports. You can schedule the report to run for a specific device or fabric. These reports are analyzed to obtain detailed information about the devices.

The **REPORT** template type is used to support the **Programmable Reports** feature. This template has two template subtypes, **UPGRADE** and **GENERIC**. For more information on the REPORT template, refer Report Template, on page 244. A python SDK is provided to simplify report generation. This SDK is bundled with Nexus Dashboard Fabric Controller.

Note A Jython template supports a maximum file size of 100k bytes. In case any report template exceeds this size, Jython execution may fail.

Nexus Dashboard Fabric Controller UI Navigation

To launch programmable reports on the Cisco Nexus Dashboard Fabric Controller Web UI, choose **Operations** > **Programmable Reports**.

The **Reports** window is displayed. This window has **Report Definitions** and **Reports** tabs. You can create reports from both the tabs by clicking **Create Report**. For information on creating a report job, refer *Creating a Report Job*. Refresh the window by clicking the **Refresh** icon.

Note Report jobs and SAN user defined reports are not migrated when upgraded from Cisco DCNM 11.5(x) to Nexus Dashboard Fabric Controller Release 12.0.1a. You must create them again manually.

This chapter contains the following sections:

- Create Report, on page 200
- Report Definitions, on page 201
- Reports, on page 203

Create Report

Choose **Operations** > **Programmable Reports**. Click **Create Report**. The **Create Report** wizard appears.

To create a report job, perform the following steps:

Procedure

Step 1 Enter a name for the report job in the **Report Name** field.

Step 2 Click **Select a template**.

Step 3 Choose a report template from the drop-down list and click **Select**.

Based on the template you've chosen, provide required values to the fields that appear on the screen.

Step 4 Click **Next** to move to the **Source & Recurrence** step.

Step 5 Choose the frequency at which the report job should be run.

The following table shows the options available and their description.

Available Option	Description
Now	The report is generated now.
Daily	The report is generated daily at a specified time between the Start Date and End Date.
Weekly	The report is generated once a week at a specified time between the Start Date and End Date.
Monthly	The report is generated once a month at a specified time between the Start Date and End Date.
Periodic	The report is generated periodically in a time period between the specified Start Date and End Date. The interval of time between the reports can be specified in minutes or hours.

Note
When you are creating a Periodic NVE VNI Counters report, the report generation frequency has to be set to 60 minutes or more. If the frequency is less than 60 minutes, an error message is displayed.

Step 6 In the **Email Report To** field, enter an email ID or mailer ID if you want the report in an email.

You must configure SMTP settings in **Settings > Server Settings > SMTP** tab. If the Data service IP address is in private subnet, the static management route for SMTP server must be added in Cisco Nexus Dashboard cluster configuration.

Step 7 Choose the devices, fabrics, or VSANs in the **Select device(s)**, **Select fabric(s)**, or **Select VSAN(s)** area.

Note
Based on the template you choose, the devices, fabrics, or VSANs are populated.

Step 8 Click **Save**.

A new report and repot definitions are created and appears on the **Reports** and **Report Definitions** tab respectively.

Report Templates

Each report template has some data associated with it. Depending on the features you have enabled in Nexus Dashboard Fabric Controller, some of the report templates available are

- Inventory_Report
- Performance_Report
- Switch_Performance_Report
- fabric_cloudsec_oper_status
- fabric_macsec_oper_status
- fabric_nve_vni_counter
- fabric_resources
- sfp_report
- switch_inventory

In addition to the templates listed above, any other templates that have been created by you will also be listed here. For more information on default templates and creating customized templates, refer to Templates, on page 215. Templates are listed based on the associated tags.

Performance_Report and **Switch_Performance_Report** are used for performance management reports.

Report Definitions

The **Report Definitions** tab displays the report jobs which are created by a user.

You can view the following information in this tab:

Field	Description
Title	Specifies the title of the report job.
Template	Specifies the name of the template.
Scope	Specifies the scope of the report.
Scope Type	Specifies if the report is generated for a device or a fabric.

Field	Description
Status	Specifies the status of the report. The status messages are as follows: • Success: Report is generated successfully. • Scheduled: A report generating schedule is set. • Running: A report job is running. • Failed: Report execution failed for one or more selected switches/fabrics or an issue occurred during running of the report job. • Unknown: Job state could not be identified.
Last Run Time	Specifies the time at which the report was last generated.
User	Specifies the user who has initiated the report generation.
Recurrence	Specifies the frequency at which the reports are generated.
Internal	Specifies if the report is run generated by a user or by Nexus Dashboard Fabric Controller. The value is **false** if the report is generated by a user.

You can perform the following actions in this tab:



Note You cannot perform these actions on internal report definitions.

Action	Description
Edit	Allows you to edit a report. **Note** You cannot change the report name and template.
Re-run Report	Allows you to rerun a report. You can use the re-run option to generate a report before the scheduled execution time.

Action	Description
History	Allows you to view report job history. The **Job History** window is displayed. You can view several entries per report job. **Note** The number of definitions displayed is defined by the following settings on **Settings > Server Settings > Reports** tab. Based on these values, the reports and history is purged. • Max number of history across report definition • Max number of reports per report definition
Delete	Allows you to delete a report job.

Reports

The **Reports** tab displays the reports which are run by a user.

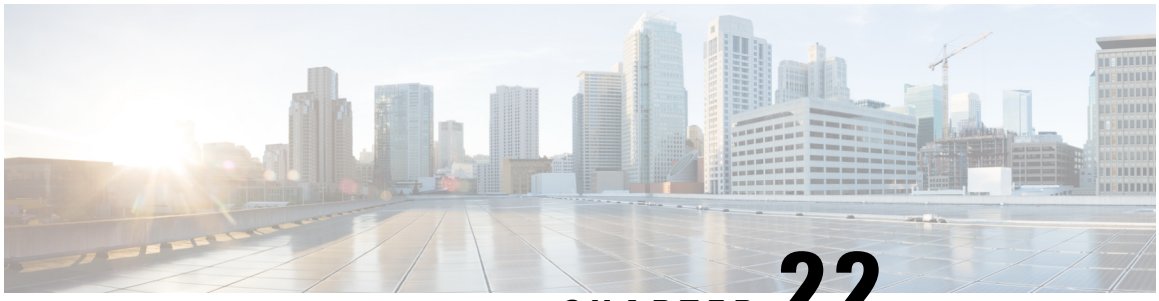
You can view the following information in this tab:

Field	Description
Title	Specifies the title of the report. • Single click on the report title opens a slide in summary panel. • Double click on the report title opens the Details and Commands window.
Template	Specifies the name of the template.
Scope	Specifies the scope of the report.
Scope Type	Specifies if the report is generated for a device or a fabric.

Field	Description
Status	Specifies the status of the report. The status messages are as follows: • COMPLETED • SUCCESS • RUNNING • FAILED • WARNING • SCHEDULED • UNKNOWN
User	Specifies the user who has initiated the report generation.
Recurrence	Specifies the frequency at which the reports are generated.
Created At	Specifies when the report is created.
Internal	Specifies if the report was created by a user or Nexus Dashboard Fabric Controller. The value is false if the report is created by a user.

You can perform the following actions in this tab:

Action	Description
Delete	Allows you to delete a report. **Note** You cannot delete internal reports.
Compare (2 Reports)	Allows you to compare two reports side by side. The report detail is logically grouped into sections. The commands are displayed based on the templates and the API that is used to run the commands on the device. For example, in the switch_inventory template, the show version, show inventory and show license usage commands are run to retrieve information. Note that the commands are displayed only if the show_and_store API is used to run the commands on the device.
Download	Allows you to download a report. You cannot choose more than one report to download.



CHAPTER 22

License Management

Beginning with Cisco Nexus Dashboard Fabric Controller Release 12.0.1a, support is removed for the following:

- Eval license state is not supported.
- Server License files are not supported.

  You must convert existing server license files to smart licenses on Cisco Smart Software Manager (CSSM). For more information, see Cisco Smart Software Manager

This chapter contains the following topics:

- Overview, on page 205
- NDFC Server Licenses, on page 206
- Smart Licensing, on page 207
- Switch Licenses, on page 210
- Switch License Files, on page 212

Overview

You can view the existing Cisco Nexus Dashboard Fabric Controller licenses by choosing **Operations** > **License Management** > **Overview**. You can view and assign licenses in the following tabs:

- **NDFC**
- **Smart**
- **Switch License Files**

Note By default, the **Overview** tab appears.

The **Overview** tab has three cards namely NDFC, Switch, and Smart. These cards display the total number of licenses to purchase and the total number of licenses expiring.

To enable Smart Licensing on switches, click **Setup Smart Licensing**. For more information on Smart Licensing, check Smart section.

NDFC Server Licenses

On NDFC tab, you can review the status of NDFC licenses for each switch. These license may be provisioned on the device, or a Smart License, or an Honor License or Unlicensed device.

Choose one or multiple switches, click **Actions** > **Assign** or **Assign All**.

When you assign a license to a device, the NDFC license service assigns the available license, based on availability on the device, status of smart licensing, and other factors.

Server based smart license is supported for Cisco MDS switches, and Nexus 9000, 3000 7000, and 5000 series of switches.



Note You cannot install a license for fabrics with brocade switch, although the install license option is displayed.

To add license from your local directory:

1. Click **Add license**.

   The **Add License File** window appears.

2. Click **Select License File** and choose appropriate files from your local directory.

3. Click **Upload** and click **Refresh** icon to refresh table and to view uploaded license files.

   The license filename, type of license, and expiration date details are extracted from the imported license file and listed in the table.

The following table displays the fields that appear on **License Management** > **NDFC**.

Field	Description
Switch Name	Displays the name of the switch.
License Type	Displays the license type of the switch that can be one of the following: • Switch • Smart • Switch Smart
State	Displays the license type of the switch that can be one of the following: • Permanent • Unlicensed • Smart • Expired • Not Applicable • Invalid

Field	Description
Expiration Date	Specifies the expiration date of license.
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.
Fabric	Specifies the name of the fabric.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **License Management** > **NDFC**.

Action Item	Description
Assign	Choose a switch, from the **Actions** drop-down list, select **Assign**. A confirmation message appears.
Unassign	Choose a switch, from the **Actions** drop-down list, select **UnAssign**. A confirmation message appears.
Assign All	• To assign license to all switches in the table, from the **Actions** drop-down list, choose **Assign All**. A confirmation message appears • Click **OK** to refresh table.
Unassign All	• To unassign license to all switches in the table, from the **Actions** drop-down list, choose **UnAssign All**. A confirmation message appears • Click **OK** to refresh table.

Smart Licensing

Cisco Nexus Dashboard Fabric Controller allows you to configure Smart Licensing and you can use the Smart Licensing feature to manage licenses at device-level and renew them if required.

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**: Cisco License Central 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 Licensing Central. For a more detailed overview on Cisco Licensing, visit the Licencing Hub.

Smart License Management

This policy runs in the license microservice and provides the ability to manage the licenses for NDFC using CSSM. From this release, you can register smart licensing OnPrem, or offline mode.

When you register smart licensing on NDFC directly with internet access, Cisco Nexus Dashboard uses IP addresses to access the smart license instead of hostname and displays an error.

Ensure that subnets for IP addresses on `smartreceiver.cisco.com` are added to the routing IP address in Cisco Nexus Dashboard.

To add IP addresses, On Cisco Nexus Dashboard Web UI, navigate to **Admin Console**, **Infrastructure** > **Cluster Configuration** > **Routes** area. Click the edit icon and add IP addresses for **Management Network Routes**. Click **Save** to confirm.

The **Smart** page shows the following cards:

- **Enable Smart Licensing**

  Use the toggle switch to enable Smart Licensing. Once enabled, Smart License can assign in two ways, **Establish Trust** or **Offline Mode**.

- **Trust Status**

  Click on **Establish Trust** to establish trust. You can view two options **Transport Gateway - OnPrem with CSLU** and connecting through CSSM either directly with Cisco's licensing servers or **Proxy - Proxy via intermediate HTTP or HTTPS proxy**.

  On the **Establish Trust for Smart License** window, select the transport type to use when establishing trust with the Smart Licensing agent.

  - Choose **Default** to communicate directly with the Cisco Licensing Server.
  - Choose **Transport Gateway - OnPrem with CSLU** and enter appropriate URL.

    You don't require trust token to enable licensing. The trust is established between CSSM and the OnPrem CSLU. From NDFC and OnPrem CSLU, trust is constant, as it expected to be a local connection.
  - Choose **Proxy - Proxy via intermediate HTTP or HTTPS proxy** to transport using the proxy server. Enter the URL and Port details to access via the proxy server. For more information, refer to Smart Licensing using Policy to Establish Trust with CSSM, on page 211.

  If using the default Transport, enter the registration token obtained from CSSM.



Note After Smart Licensing is registered, you must manually assign licenses to the existing switches. For all switches discovered after registration, smart licenses are automatically assigned to the switches.

- **Offline Mode**

  In Offline mode you can share data in alternative between NDFC instance and CSSM. Operating in an air-gap or disconnected environment, use of Offline mode allows you to export state, upload it to CSSM, and import a response back to NDFC.

  To export license data and to import the response from CSSM, follow below perform the following steps:

  1. On **Trust Status** click **Switch to Offline mode** to enable offline mode.
  2. In offline mode with one or moe licenses assigned, click **Export License Data**.
  3. On https://software.cisco.com/software/csws/ws/platform/home, navigate to smart licensing section, click **Reports** tab, and choose subsequent usage data files tab. The usage report from NDFC can be uploaded and after few minutes a response can be downloaded and imported to NDFC.
  4. Click **Import License Data** and upload the CSSM acknowledge file on NDFC.

- **License Status**

  Specifies the status of the licensing on NDFC. 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 **IN USE** or **NOT IN USE** 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.

  Click **Policy Details**, to view smart license policy details. You can view the default smart license policy of initial 90 days and ongoing reporting within 365 days of that report.



Note You can view reports after 30 days of initial registering.

Resync

When the total number of NDFC license are not same as CSSM license counts, click **Resync**, to refresh the license counts.

Resync causes a local audit of the NDFC licenses in the switch inventory and updates the smart license counts for reporting

CSSM allows you to convert traditional licenses to Smart Licenses. For instructions, refer to https://www.cisco.com/c/dam/en/us/products/se/2020/8/Collateral/brownfield-conversion-qrg.pdf.

To migrate from Smart Licensing to Smart Licensing using Policy, launch Cisco Nexus Dashboard Fabric Controller. On the Web UI, choose **Operations > License Management > Smart** tab. Establish trust with CCSM using SLP. For instructions, refer to Smart Licensing using Policy to Establish Trust with CSSM, on page 211.

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.

Field	Description
Status	Specifies the status of the licenses used. Valid values are **IN USE** and **NOT IN USE**.
Description	Specifies the type and details of the license.

To upload or download license reports, go to https://software.cisco.com/, navigate to **Smart Software Licensing > Reports**. On **Usage Data Files** tab, click **Upload Usage Data** to upload Usage Report from NDFC. After few minutes of uploading the report, click **Download** in the **Acknowledgment** column to download a response brought back to the NDFC and imported.

Switch Licenses

If the switch is pre-configured with a smart license, Nexus Dashboard Fabric Controller validates and assigns a switch smart license. To assign licenses to switch using the Cisco Nexus Dashboard Fabric Controller UI, choose **Operations** > **License Management** > **Smart**. Click **Enable Smart Licensing** toggle button to enable smart licensing feature.

Switch based smart license is supported for MDS switches, and Nexus 9000, and 3000 Series of switches.

Note For the switches which are in managed mode, switch smart license must be assigned through Nexus Dashboard Fabric Controller.

To enable switch smart license on Nexus Dashboard Fabric Controller:

- 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 id token command. Use **EXEC** option in Nexus Dashboard Fabric Controller to push token.

Click **Refresh** icon to refresh table.

The following table displays the fields that appear on **License Management** > **Switch**.

Field	Description
Switch	Displays the name of the switch.
Features	Displays the features on the switch.
Status	Displays the status of switch is in use or not. • Unused • In Use • Out Of Compliance

Field	Description
Type	Displays the license type of the switch that can be one of the following: • Temporary • Permanent • Smart • Counter Permanent • Unlicensed • Counted
Warnings	Specifies the warnings about license, such as expiration date and time.
Group	Specifies the fabric or LAN name.

Smart Licensing using Policy to Establish Trust with CSSM

To establish trust with CSSM using the Smart Licensing using Policy on Cisco Nexus Dashboard Fabric Controller, perform the following steps:

Before you begin

- Ensure that there is network reachability between Cisco Nexus Dashboard and CSSM. To configure network reachability, launch **Cisco Nexus Dashboard Web UI**. On **Admin Console**, choose **Infrastructure** > **Cluster Configuration** > **General** tab. In **Routes** area, click the edit icon, and add IP addresses for Data Network Routes. Click **Save** to confirm.
- Ensure that you have obtained the Token from CSSM.

Procedure

Step 1 Choose **Operations** > **License Management** > **Smart** tab.

Step 2 Use the **Enable Smart Licensing** toggle button to enable smart licensing.

Step 3 On the **Trust Status** card, click **Establish Trust**.

The **Establish Trust for Smart License** window appears.

Step 4 Select the **Transport** option to register Smart License Agent.

The options are:

- **Default - NDFC communicates directly with Cisco's licensing servers**

  This option uses the following URL: https://smartreceiver.cisco.com/licservice/license.

- **Transport Gateway – OnPrem with CSLU option**

  Enter the CSLU transport URL.

Note
You must configure the license smart URL on the product to use the CSLU transport URL.

- **Proxy - Proxy via intermediate HTTP or HTTPS proxy**

  Enter the URL and the port if you select this option.

Step 5 In the **Token** field, paste the token that you have obtained from CSSM to establish trust for Smart Licenses.

Step 6 Click **Establish Trust**.

A message appears as confirmation.

The status changes from UNTRUSTED to TRUSTED. The name, count, and status of switch licenses appear.

Click on **TRUSTED** to see the details. 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.

Step 7 Click **NDFC** tab.

Step 8 From the Actions drop-down list, select **Assign All**.

The **Status** of the server licenses shows **InCompliance**.

If the status shows **OutofComplaince**, visit the CSSM portal to acquire the required licenses.

For all other statuses, contact Cisco Technical Assistance Center (TAC).

Switch License Files

Cisco Nexus Dashboard Fabric Controller allows you to upload multiple licenses at a single instance. Nexus Dashboard Fabric Controller 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.

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

Field	Description
Switch	Specifies the switch name.
Switch IP	Specifies the switch IP address.
License File	Specifies the type of license file.
Status	Specifies the status of license.
Result Message	Specifies the license details.
Last Upload Time	Specifies the date and time uploaded on server.
Features	Specifies the license features.

Adding Switch License Files

To bulk install licenses to the switches on the Cisco Nexus Dashboard Fabric Controller Web Client UI, perform the following steps:

Procedure

Step 1 Choose **Operations** > **License Management** > **Switch License Files**.

The **Switch License File** window appears.

Step 2 On the Switch License File tab, click **Add License** to upload the appropriate license file.

The **Add License File** window appears.

Step 3 In the Add License File, click **Select License File**.

Navigate and choose the appropriate license file located in your local directory.

Step 4 Click **Upload**.

The License file is uploaded to the Nexus Dashboard Fabric Controller. The following information is extracted from the license file.

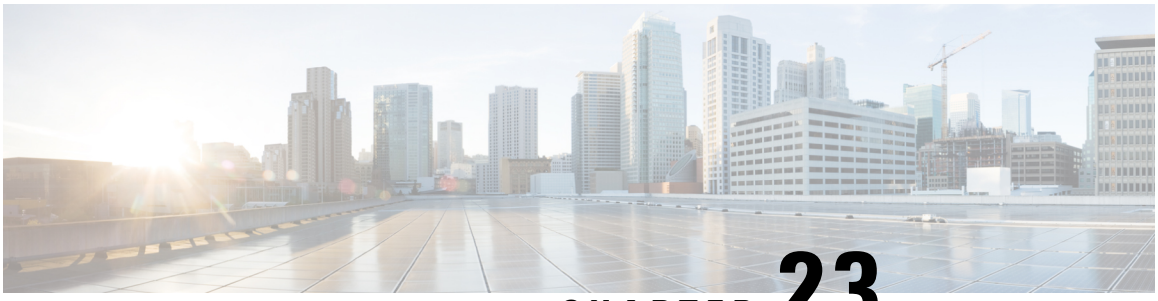
- Switch IP – IP Address of the switch to which this license is assigned.
- License File – filename of the license file
- Features List –list of features supported by the license file

Step 5 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.

Step 6 Click **Actions** > **Install** to 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.

Step 7 After the license matches with respective devices and installs, the **Status** column displays the status.



CHAPTER 23

Templates

- Templates, on page 215

Templates

UI Navigation

- Choose **Operations** > **Templates**.

You can add, edit, or delete templates that are configured across different Cisco Nexus, IOS-XE, IOS-XR, and Cisco MDS platforms using Cisco Nexus Dashboard Fabric Controller Web client. The following parameters are displayed for each template that is configured on Cisco Nexus Dashboard Fabric Controller 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.

Table 25: Template Table Fields and Description

Field	Description
Name	Specifies the template name.
Supported Platforms	Specifies the platforms that the template support.
Type	Specifies the template type.
Sub Type	Specifies the template sub type.
Modified	Specifies the date and time of the template modification.
Tags	Specifies if the template is tagged to a fabric or a device.
Description	Specifies the template description.
Reference Count	Specifies the number of times a template is used.

Click the table header to sort the entries in alphabetical order of that parameter.

Note Templates with errors are not listed in the Templates window. You cannot import templates with errors. To import such templates, fix the errors, and import them.

The following table describes the action items, in the **Actions** drop-down list, that appears in the **Templates** window.

Table 26: Templates Actions and Description

Actions	Description
Create new template	Allows you to create a new template. For more information, see Creating a New Template, on page 218.
Edit template properties	Allows you to edit the template properties. You can edit only one template at a time. For more information, see Editing a Template, on page 219.
Edit template content	Allows you to edit the template content. You can edit only one template at a time. For more information, see Editing a Template, on page 219.
Duplicate template	Allows you to duplicate the selected template with a different name. You can edit the template as required. You can duplicate only one template at a time. To duplicate a template, select the check box next to the template that you want to duplicate and choose **Duplicate template**. The **Duplicate Template** window appears. Specify a name for the duplicated template. For more information about editing the duplicated template, see Editing a Template, on page 219.

Actions	Description
Delete template	Allows you to delete a template. You can delete more than one template in a single instance. You can delete the user-defined templates. However, you cannot delete the predefined templates To delete a template, select the check box next to the template that you want to delete and choose **Delete template**. A warning message appears. If you are sure you want to delete the template, click **Confirm**. If not, click **Cancel**. If the template is in use or is a shipping template, you cannot delete it, and an error message appears. **Note** Select multiple templates to delete them at the same instance. To delete the template permanently, delete the template that is located in your local directory: `Cisco Systems\dcn\ndfc\data\templates\`.
Import	Allows you to import a template from your local directory, one at a time. For more information, see Importing a Template, on page 220.
Import as Zip	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. For more information, see Importing a Template, on page 220 **Note** To install POAP templates for the Nexus Dashboard Fabric Controller Virtual Appliance (OVA or ISO), see Installing POAP Templates, on page 221. .
Export	Allows you to export the template configuration to a local directory location. You can export only one template at a time. To export a template, use the check box next to it to select it and choose **Export**. Select a location on your local system directory to store the template file. Click **Save**. The template file is exported to your local directory.

You can only view templates with the **network-operator** role. You cannot create, edit, or save templates with this role. However, you can create or edit templates with the **network-stager** role.

This section contains the following:

Creating a New Template

Nexus Dashboard Fabric Controller UI Navigation

- Choose **Operations** > **Templates**.

To create user-defined templates and schedule jobs from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 In the **Templates** window, from the **Actions** drop-down list, choose **Create new template**.

The **Create Template** window appears.

Step 2 In the **Template Properties** page of the window, specify a template name, description, tags, and choose supported platforms for the new template. Next, choose a template type and a sub template type from the drop-down lists. Choose a content type for the template from the drop-down list.

Note
The base templates are CLI templates.

Step 3 Click **Next** to continue editing the template or click **Cancel** to discard the changes.

The edited template properties are displayed in the **Template Content** page of the **Edit Template** window. For information about the structure of the Configuration Template, see the *Template Structure* section.

Step 4 Click **Validate** to validate the template syntax.

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 5 Click **Help** to open the **Editor Help** pane on the right.

This window contains more information about the format, variables, content and data types used to build the template. Close the **Editor Help** pane.

Step 6 Click **Errors** and **Warnings** if the links are displayed. If there are no errors or warnings, the links are not available. If errors or warnings are present, and you click the links, the **Errors & Warnings** pane appears on the right displaying the errors and warnings. Close the **Errors & Warnings** pane.

Step 7 To build the template content, select the required theme, key binding, and font size from the drop-down list.

Step 8 Click **Finish** to complete editing of the template, click **Cancel** to discard the changes, click **Previous** to go to the **Template Properties** page.

The page with the message that the template was created appears. The page also displays the template name, type, and sub type, and the platforms. You can also click **Create another template** to create one more template or click **Edit <template name> template** to edit the template that was just edited.

Step 9 Close the **Edit Template** window or Click **Back to template library** to go back to the **Templates** window.

Editing a Template

Nexus Dashboard Fabric Controller UI Navigation

- Choose **Operations** > **Templates**.

You can edit the user-defined templates. However, the predefined templates and templates that are already published cannot be edited.

Use the **Edit Template** window to first edit the template properties and then edit the template content. Furthermore, you can edit either only the template properties using the **Edit template properties** action or only the template content using the **Edit template content** action. In other words, you can edit the template properties at one instance, and then, edit the template content at another instance. You can also use this window to view the template properties and content.

Perform the following steps to edit the template properties and then edit the template content:

Procedure

Step 1 In the **Templates** window, select a template. From the **Actions** drop-down list, choose **Edit template properties**.

The **Edit Template** window appears.

Step 2 In the **Template Properties** page of the window displays the name of the template along with its description, supported platforms, tags, and content type. You can edit the template description and tags. To edit the supported platforms, clear the selected check boxes to select other switches. Next, choose a template type and a sub template type from the drop-down lists.

Step 3 Click **Next** to continue editing the template or click **Cancel** to discard the changes.

The edited template properties are displayed in the **Template Content** page of the **Edit Template** window.

Step 4 Click **Validate** to validate the template syntax.

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 5 Click **Help** to open the **Editor Help** pane on the right.

This window contains more information about the format, variables, content and data types used to build the template. Close the **Editor Help** pane.

Step 6 Click **Errors** and **Warnings** if the links are displayed. If there are no errors or warnings, the links are not available. If errors or warnings are present, and you click the links, the **Errors & Warnings** pane appears on the right displaying the errors and warnings. Close the **Errors & Warnings** pane.

Step 7 To build the template content, select the required theme, key binding, and font size from the drop-down list.

Step 8 Click **Finish** to complete editing of the template, click **Cancel** to discard the changes, click **Previous** to go to the **Template Properties** page.

The page with the message that the template is saved appears. The page also displays the template name, type, and sub type, and the platforms. You can also click **Create another template** to create one more template or click **Edit <template name> template** to edit the template that was just edited.

Step 9 Close the **Edit Template** window or Click **Back to template library** to go back to the **Templates** window.

Importing a Template

Nexus Dashboard Fabric Controller UI Navigation

- Choose **Operations** > **Templates**.

Follow the same procedure while importing zipped templates.

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.

Note You can install POAP templates for the Nexus Dashboard Fabric Controller Virtual Appliance (OVA or ISO). For more information, see Installing POAP Templates, on page 221.

To import a template from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 In the **Templates** window, from the **Actions** drop-down list, choose **Import template**.

The **Import Template** window appears.

Step 2 Browse and select the template that is saved on your computer.

Step 3 Click **OK** to import the template or click **Cancel** to discard the template.

Note
After importing a zipped template file, either a successful or error message appears. Click **OK**.

Step 4 You can edit the template parameters and content, if necessary. For more information, see Editing a Template, on page 219.

Note
When importing a zipped template file, the **Edit Template** window may not appear. However, you can edit the template parameters and content, if necessary, using the **Edit Template** action.

Step 5 If you do not want to edit the template properties or content, then keep clicking **Next**, then **Finish** and **Back to template library** to go back to the **Templates** window.

Installing POAP Templates

UI Navigation

- Choose **Operations** > **Templates**.

Cisco Nexus Dashboard Fabric Controller allows you to add, edit, or delete user-defined templates that are configured across different Cisco Nexus platforms. From Cisco Nexus Dashboard Fabric Controller 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 Nexus Dashboard Fabric Controller 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 Nexus Dashboard Fabric Controller.

Procedure

Step 1 Navigate to https://software.cisco.com/download/release.html, and download the file.

You can choose one of the following:

- `ndfc_ip_vxlan_fabric_templates.10.0.1a.zip`
- `ndfc_fabricpath_fabric_templates.10.0.1a.zip file`

Step 2 Unzip and extract the files to the local directory on your computer.

Step 3 Click **Import Template** from the **Actions** drop-down list.

Step 4 Browse and select the template that is saved on your computer. You can edit the template parameters, if necessary.

Step 5 Check **POAP** and **Publish** check box to designate these templates as POAP templates.

Step 6 Click **Validate Template Syntax** to validate the template.

Step 7 Click **Save** to save the template or **Save and Exit** to save the template and exit.

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, N6K, N7K, N9K, MDS, VDC, N9K-9000v, IOS-XE, IOS-XR, Others, All Nexus Switches list separated by comma.	No
templateType	Specifies the type of Template used.	• CLI • POAP **Note** POAP option is not applicable for Cisco Nexus Dashboard Fabric Controller LAN Fabric deployment. • POLICY • SHOW • PROFILE • FABRIC • ABSTRACT • REPORT	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 **Note** POAP option is not applicable for Cisco Nexus Dashboard Fabric Controller LAN Fabric deployment. • 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	

Property Name	Description	Valid Values	Optional?
		• INTERFACE • SHOW • VLAN • INTERFACE_VLAN • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORTCHANNEL • 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 • REPORT • UPGRADE • GENERIC	

Property Name	Description	Valid Values	Optional?
contentType		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI **Note** POAP option is not applicable for Cisco Nexus Dashboard Fabric Controller LAN Fabric deployment. • POLICY • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • PROFILE • TEMPLATE_CLI • PYTHON • FABRIC • PYTHON • ABSTRACT • TEMPLATE_CLI • PYTHON • REPORT • PYTHON	Yes
implements	Used to implement the abstract template.	Text	Yes
dependencies	Used to select the specific feature of a switch.	Text	Yes

Property Name	Description	Valid Values	Optional?
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

Variable Type	Valid Value	Iterative?

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

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

Variable Type	Valid Value	Iterative?
string[]	Example: {a,b,c,str1,str2}	Yes

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 Nexus Dashboard Fabric Controller 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
ipAddrList	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: [redacted] Example 3: 172.22.31.97, 172.22.31.99, [redacted], 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
ipAddressWithSubnet	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											
iSCSIAddress	Example: [illegible]												
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 shellcmd { [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>; ….. } [structarray1] [, structarray2] [, structarray3 []>];`												
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”	
IsSourceSwitchName	“true” or “false”	

Annotation Key	Valid Values	Description
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.

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]**

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.

Report Template

The template type of REPORT template is python, and it has two subtypes, UPGRADE and GENERIC.

UPGRADE

The UPGRADE template is used for pre-ISSU and post-ISSU scenarios. These templates are listed in the ISSU wizard.

Refer to the default upgrade template packaged in Nexus Dashboard Fabric Controller for more information on pre-ISSU and post-ISSU handling. The default upgrade template is issu_vpc_check.

GENERIC

The GENERIC template is used for any generic reporting scenarios, such as, collecting information about resources, switch inventory, SFPs, and NVE VNI counters. You can also use this template to generate troubleshooting reports.

Resources Report

This report displays information about resource usage for a specific fabric.

The **Summary** section shows all resource pools with the current usage percentages. Use the horizontal scroll bar at the bottom of the window to display more columns.

POOL NAME: Specifies the name of the pool.

POOL RANGE: Specifies the IP address range of the pool.

SUBNET MASK: Specifies the subnet mask.

MAX ENTRIES: Specifies the maximum number of entries that can be allocated from the pool.

USAGE INSIDE RANGE: Specifies the current number of entries allocated inside the pool range.

USAGE OUTSIDE RANGE: Specifies the current number of entries set outside the pool range.

USAGE PERCENTAGE: This is calculated by using the formula: (Usage Inside Range/Max Entries) *100.

Click **View Details** to display a view of resources allocated or set in each resource pool. For example, the detailed section for a SUBNET has information about the resources that have been allocated within the subnet.

Switch Inventory Report

This report provides a summary about the switch inventory.

Click **View Details** to display more information about the modules and licenses.

SFP Report

This report provides information about utilization of SFPs at a fabric and device level.



Note The switch inventory and SFP reports are supported only on Cisco Nexus devices.

Troubleshooting Reports

These reports are generated to help in troubleshooting scenarios. Currently, the **NVE VNI Counters** report is the only pre-defined troubleshooting report. Generating **NVE VNI Counters** reports involves performing periodic checks to identify the VNIs that are among the top hits based on network traffic. In a large-scale setup, we recommend limiting the report generation frequency to a minimum of 60 minutes.

NVE VNI Counters Report

This report collects the **show nve vni counters** command output for each VNI in the fabric.

After comparing the oldest report and the newest report, the **Summary** section shows the top-10 hit VNIs. The top hit VNIs are displayed in these categories:

- L2 or L3 VNIs for unicast traffic
- L2 or L3 VNIs for multicast traffic
- L2 only VNIs for unicast traffic
- L2 only VNIs for multicast traffic
- L3 only VNIs for unicast traffic
- L3 only VNIs for multicast traffic

The oldest report refers to the first report that is saved in the current reporting task. If you want to select a specific report as the first report against which the current report has to be compared, delete all reports that are older than the one selected so that the selected report becomes the first and oldest report.

For example, three reports were run yesterday at 8:00 a.m, 4:00 p.m. and 11:00 p.m. If you want to use the report at 11:00 p.m. as the first and oldest report for today’s reporting, delete the two reports that were run yesterday at 8:00 a.m. and 4:00 p.m.

For a periodic report, the oldest report is the first report that is run at the start time of a period. For daily and weekly reports, the current report is compared against the previously generated report.

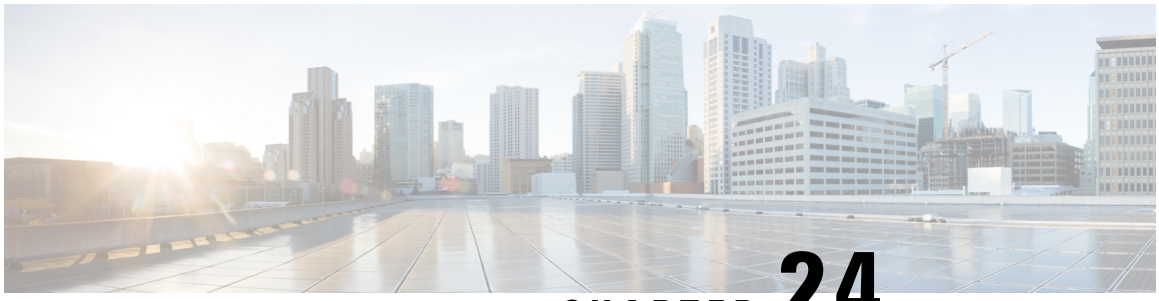
The **Summary** section displays a column-wise report with information about the total transmitted bytes and the VNIs. Use the horizontal scroll bar at the bottom of the window to display more columns.



Note The **Summary** section in the NVE VNI Counters report displays negative numbers in the TOTAL TX BYTES column if a report is generated after a switch reload or after clearing the counters on the switch. The numbers are displayed correctly in the subsequent reports. As a workaround, we recommend deleting all old reports or creating a new job before reloading switches or clearing counters.

Click **View Details** to display more information. This section shows NVE VNIs and counters on a per-switch basis.

For more information on how the reports are displayed, refer *Programmable Reports* chapter.



CHAPTER 24

Backup and Restore

You can take a backup manually anytime. You can also configure a scheduler to backup all fabric configurations and intents.

You can backup and restore using any of the following formats:

- **Config only**: A Config only backup is smaller. It contains the intent, dependent data, discovery information, credentials, and policies. A restore from this backup has functional fabrics, switch discovery, expected configurations, and other settings.
- **Full**: A Full backup is large. It contains current data, historical data, alarms, host information, and everything in a Config only backup. A restore from this backup has functional historical reports, metrics charts, and all base functionality.

You can restore a config-only backup or a full backup.

When restoring a backup, you can choose to do a config only restore or a full restore. A config only restore will restore only the configuration (intent, discovery information, credentials, and policies) and can be done using both config only backups and full backups. A full restore will restore the configuration and any current and historical data, charts, etc. and can be done using only full backups.

Note Wait for minimum of 20 minutes after fresh installation before restoring the backup data. Some applications may not be operational if the backup is restored immediately in the freshly installed setup.

Feature Compatibility Post Upgrade

The following table lists caveats associated with features that are restored from DCNM 11.5(x) backup after upgrade to NDFC, Release 12.1.1e.

Note 11.5(x) includes Releases 11.5(1), 11.5(2), only. Upgrade from 11.5(4) to 12.1.1e is not supported.

Feature in DCNM 11.5(x)	Upgrade Support
VMM Visibility with vCenter	Supported
Preview features configured	Not supported

Feature in DCNM 11.5(x)	Upgrade Support
LAN switches in SAN installations	Not supported
Switches discovered over IPv6	Not supported
DCNM Tracker	Not supported
Fabric Backups	Not supported
Report Definitions and Reports	Not supported
Switch images and Image Management policies	Not supported
SAN CLI templates	Not carried over from 11.5(x) to 12.1.1e
Switch images/Image Management data	Not carried over from 11.5(x) to 12.1.1e
Slow drain data	Not carried over from 11.5(x) to 12.1.1e
Alarm Policy configuration	Not carried over from 11.5(x) to 12.1.1e
Performance Management data	CPU/Memory/Interface statistics up to 90 days is restored post upgrade.



Note SAN Insights and VMM Visualizer features are not enabled after restore. You must choose check boxes on **Settings** > **Feature Management** and click **Save** to enable these features after restore.

This section includes the following:

- Scheduler, on page 248
- Restore, on page 249
- Backup Now, on page 251

Scheduler

The purpose of the scheduler is to take backups of the system, if a system needs to be restored. You must backup to a remote location.

To schedule a backups of application and configuration data from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

If there are no scheduled backup jobs, **No Schedule set** is displayed.

Procedure

Step 1 Click on **No Schedule set**.

The **Scheduler** window appears.

Step 2 Check the **Enable scheduled backups** check box.

Step 3 Under **Type**, select your desired format to restore.

- Choose **Config only** or **Full**.

Step 4 In the **Destination** field, click and choose **Export to SCP Server** or **Export to SFTP Server** from the drop-down list.

Step 5 In the **Server** field, provide the Server IP Address.

Step 6 In the **File Path** field, provide the absolute path of the directory to store the backup file.

Step 7 Enter **Username** and **Password** to the backup directory.

Step 8 Enter the **Encryption Key** to the backup file.

You must have an Encryption Key in order to restore from the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

Step 9 In the **Run on days** field, select the check box to schedule the backup job on one or more days.

Step 10 In the **Start at** field, use the time picker to schedule the backup at a particular time.

The time picker is a 12-hour clock.

Step 11 Click **Schedule backup** to run the backup job as per schedule.

Restore

Note Wait for minimum of 20 minutes after fresh installation before restoring the backup data. Some applications may not be operational if the backup is restored immediately in the freshly installed setup.

Guidelines

You can do a restore only on a freshly installed Nexus Dashboard Fabric Controller with no features enabled.

When you migrate from L2 HA to L3 HA, check the Ignore External Service IP Configuration check box to ensure that the persistent IPs in the backup are ignored and it selects new ones during the restore. Rest of the data will be restored.

Note During disaster recovery, NDFC allows you to restore only on the same version on which the backup was taken.

To restore application and configuration data from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Click **Restore**.

The **Restore now** window appears.

Step 2 Under **Type**, select your desired format to restore.

- Choose **Config only** or **Full**.

Step 3 In the **Source** field, click and choose the appropriate source where you have stored the backup file.

- Choose **Upload File** if the file is stored in a local directory.
  - **a.** Open the directory where you've saved the backup file.
  - **b.** Drag and drop the backup file to the **Restore now** window.

    or

    Click Browse. Navigate to the directory where you've saved the backup file. Select the backup file and click Open.
  - **c.** Enter the **Encryption Key** to the backup file.

    Note
    You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

- Choose **Import from SCP Server** or **Import from SFTP Server** if the backup file is stored in a remote directory.
  - **a.** In the **Server** field, provide the Server IP Address.
  - **b.** In the **File Path** field, provide the relative file path to the backup file.
  - **c.** In the **Username** and **Password** fields, enter appropriate details.
  - **d.** In the **Encryption Key** field, enter the Encryption Key to the backup file.

    Note
    You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

Step 4 (Optional) Check the **Ignore External Service IP Configuration** check box.

If the **Ignore External Service IP Configuration** check box is selected, then the external service IP configuration is ignored. This selection allows you to take a backup on a system and restore it on a different system, with different management and/or data subnets.

This option does not have any impact during an upgrade from Cisco DCNM 11.5(x) to Cisco NDFC.

Step 5 Click **Restore**.

The backup file appears in the table on the Backup & Restore window. The time required to restore depends on the data in the backup file.

Backup Now

To take a backup of application and configuration data from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Click **Backup now**.

Step 2 Under **Type**, select your desired format to restore.

- Choose **Config only** or **Full**.

Step 3 In the **Destination** field, click and choose the appropriate destination to store the backup file.

- Choose **Local Download** to store the backup in a local directory.

  a. Enter the **Encryption Key** to the backup file.

  Note
  You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

  b. Click **Backup**.

  After the backup is complete, the backup file available for download from the **Backup & Restore** screen.

  c. In the Actions column, you can click on Download icon to save the backup to a local directory.

  Click on **Delete** icon to delete the backup.

  Note
  You must delete the backups that are taken with **Local Download** options as soon as possible due to the limited amount of allocated disk space.

- Choose **Export to SCP Server** or **Export to SFTP Server** to store the backup file in a remote directory.

  You must specify the file name if you choose the **Export to SFTP Server** option for backup. You do not need to specify the file name for the **Export to SCP Server** option. The file name should contain *path/filename.tar.gz*.

  a. In the **Server** field, provide the Server IP Address.

  b. In the **File Path** field, provide the relative file path to the backup file.

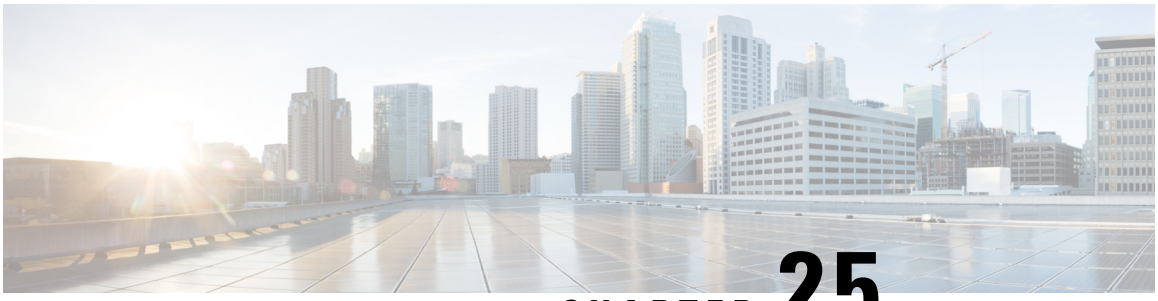
  c. In the **Username** and **Password** fields, enter appropriate details.

d. In the **Encryption Key** field, enter the Encryption Key to the backup file.

Note
You must have an Encryption Key in order to restore the backup. The Encryption Key is used to encrypt a portion of the backup file that has sensitive information.

e. Click **Backup**.

After the backup is complete, the backup file is saved in the remote directory.



CHAPTER 25

NXAPI Certificates

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 or use Cisco Nexus Dashboard Fabric Controller to install these on switches.

Cisco Nexus Dashboard Fabric Controller provides a Web UI framework to upload NX-API certificates to Nexus Dashboard Fabric Controller. Later, you can install the certificates on the switches that are managed by Nexus Dashboard Fabric Controller.

Note This feature is supported on switches running on Cisco NXOS version 9.2(3) or higher.

• Certificate Generation and Management, on page 253

Certificate Generation and Management

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 Nexus Dashboard Fabric Controller also supports a single certificate file that contains an embedded key file, that is, the `.crt/.cer/.pem` file, which can also contain the contents of the `.key` file.

Nexus Dashboard Fabric Controller doesn't support binary encoded certificates, that is, the certificates with the `.der` extension are not supported. You can protect the key file with a password for encryption. Cisco Nexus Dashboard Fabric Controller does not mandate encryption; however, as this is stored on Nexus Dashboard Fabric Controller, we recommend that you encrypt the key file. Nexus Dashboard Fabric Controller supports AES encryption.

You can either choose CA-signed certificates or self-signed certificates. Cisco Nexus Dashboard Fabric Controller does not mandate the signing; however, the security guidelines suggest you use the CA-signed certificates.

You can generate multiple certificates meant for multiple switches, to upload to Nexus Dashboard Fabric Controller. Ensure that you name the certificates appropriately, to help you choose the switch meant for that certificate.

You can upload one certificate and the 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, Nexus Dashboard Fabric Controller 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 Nexus Dashboard Fabric Controller will not be able to install the certificate on the switch.

Cisco Nexus Dashboard Fabric Controller 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 the 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 Nexus Dashboard Fabric Controller 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, Nexus Dashboard Fabric Controller doesn't enforce it; switches may choose to accept or reject a certificate based on the parameters in the certificate.

NX-API Certificate Verification by Cisco Nexus Dashboard Fabric Controller

From release 12.0.1a onwards, Cisco Nexus Dashboard Fabric Controller supports a capability to verify NX-API certificates offered by switches. The NX-API requests done by Cisco Nexus Dashboard Fabric Controller require SSL connection, and switches act like SSL server and offer server certificate as part of SSL negotiations. If provided a corresponding CA certificate, Cisco Nexus Dashboard Fabric Controller can verify it.



Note By default, NX-API certificate verification is not enabled because it requires all switches in the data center to have the CA-signed certificates installed, and Cisco Nexus Dashboard Fabric Controller is fed all the corresponding CA certificates.

Cisco Nexus Dashboard Fabric Controller NX-API certificate management provides two functionalities named as Switch Certificates and CA Certificates to manage the same.

Switch Certificates

Uploading Certificates

To upload the certificates onto Nexus Dashboard Fabric Controller, perform the following steps:

1. Click **Upload Certificate** to upload the appropriate certificate file.

2. Browse your local directory and choose the certificate key pair that you must upload to Nexus Dashboard Fabric Controller.

   You can choose certificates with extension `.cer/.crt/.pem + .key` file separately.

   Cisco Nexus Dashboard Fabric Controller also allows you to upload a single certificate file that contains an embedded key file. The key file is automatically derived after upload.

3. Click **Upload** to upload the selected files to Nexus Dashboard Fabric Controller.

   A successful upload message appears. The uploaded certificates are listed in the table.

   The table shows the Status as UPLOADED. If the certificate is uploaded without the key file, the status shows KEY_MISSING.

Assigning Switches and Installing Certificates

To install certificates on the switches using Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

1. Select one or multiple certificates check box.
2. From the **Actions** drop-down list, select **Assign Switch & Install**.
3. In the **NX API Certificate Credentials** field, provide the password which was used to encrypt the key while generating the certificates.

   The **Password** field is mandatory, however, if the keys were not encrypted using a password, any random string you can enter, for example, test, install, and so on. In case of unencrypted files, passwords are not used, but you still need to enter any random string because it is bulk mode.



Note 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.

4. For each certificate, click on the **Assign** arrow and select the switch to associate with the certificate.
5. Click **Install Certificates** to install all the certificates on their respective switches.

Unlinking and Deleting Certificates

After the certificates are installed on the switch, Nexus Dashboard Fabric Controller cannot uninstall the certificate from Nexus Dashboard Fabric Controller. 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 Nexus Dashboard Fabric Controller.



Note Unlinking the certificate from the switch does not delete the certificate on the switch. The certificate still exists on the switch. Cisco Nexus Dashboard Fabric Controller cannot delete the certificate on the Switch.

To delete certificates from Nexus Dashboard Fabric Controller repository, perform the following steps:

1. Select the certificate(s) that you need to delete.
2. From the **Actions** drop-down list, select **Unlink**.

   A confirmation message appears.
3. Click **OK** to unlink the selected certificates from the switches.

   The status column shows UPLOADED. The Switch column shows NOT_INSTALLED.
4. Select the certificate that is now unlinked from the Switch.
5. From the **Actions** drop-down list, select **Delete**.

   The certificate is deleted from Nexus Dashboard Fabric Controller.

CA Certificates

Uploading Certificates

To upload the certificates onto Nexus Dashboard Fabric Controller, perform the following steps:

1. On **CA Certificates** tab, click **Upload Certificate** to upload the appropriate license file.
2. Browse your local directory and choose the certificate-key pair that you must upload to Nexus Dashboard Fabric Controller.

   You can upload certificates with the `.cer/.crt/.pem` file extensions.



Note The CA Certificates are public certificates and do not contain any keys; also, keys are not needed for this operation. This is the certificate which Cisco Nexus Dashboard Fabric Controller must verify the NX-API certificates offered by the switches. In other words, the CA certificates are consumed by Cisco Nexus Dashboard Fabric Controller and never installed on the switches.

3. Click **Upload** to upload the selected files to Nexus Dashboard Fabric Controller.

   A successful upload message appears. The uploaded certificates are listed in the table.

Deleting Certificates

To delete CA certificates, choose **Actions** from drop-down list, click **Delete**.

Enabling NX-API Certificate Verification

The NX-API certificate verification is enabled using the toggle button on the CA Certificates page. However, this must be done only after all the switches managed by Cisco Nexus Dashboard Fabric Controller are installed with CA-signed certificates and the corresponding CA Root certificates (one or more) are uploaded to Cisco Nexus Dashboard Fabric Controller. When this is enabled, the Cisco Nexus Dashboard Fabric Controller SSL client starts verifying the certificates that are offered by the switches. If the verification fails, the NX-API calls will also fail.

Note

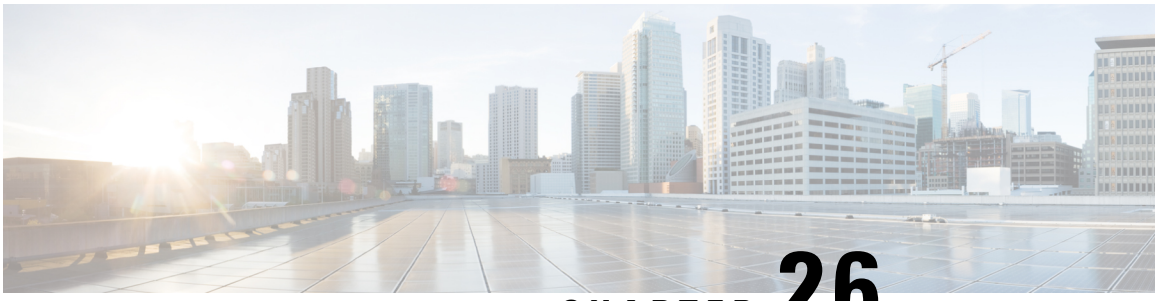
- Verification of the NX-API certificates cannot be enforced per switch; it is for either all or none. Hence, it is important that the verification is enabled only when all the switches have their corresponding CA-signed certificates installed.
- It is also required that all the CA certificates are installed on the Cisco Nexus Dashboard Fabric Controller.
- When an NX-API call fails for a given switch because of verification issues, you can use the toggle button to disable enforcement, and all goes back to the previous state without any consequences.
- Because of the above points, you must enable the enforcement during a maintenance window.



PART V

Service Integration

- One View Dashboard, on page 261
- Device Manager, on page 263



CHAPTER 26

One View Dashboard

• One View Dashboard, on page 261

One View Dashboard

One View dashboard displays many dashlets showing summary information about all the sites. By default, a subset of the available dashlets are automatically displayed in the overview of dashboard.

From the left menu bar, choose **SAN Controller > One View > One View Dashboard**. The **Overview** window displays the default dashlets. You can also click on the refresh icon to manually refresh the dashboard.

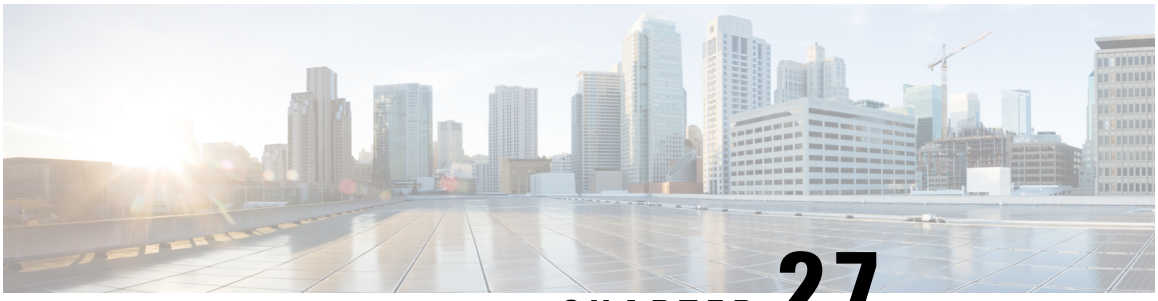
Click on the one view icon on the top bar to view **Select NDFC** screen. Click on **One View** to view the controller information and their status. Click on each of the controllers in the left pane to view specific information about that controller in federation.

You can also view the NDFC service and Nexus Dashboard status for each federated node.

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

Dashlet	Description
Summary	Displays the following in a horizontal pane. • Number of SAN Controllers in Federation setup • Total number of fabrics • Total number of discovered switches
Fabric Health	Displays the fabric's health status in the form of chart with colors and health condition severity with total number of fabrics in the brackets.
Switch Health	Displays the switch's health status in the form of chart with colors and health condition severity with total number of switches in the brackets.
Switch Release Versions	Displays the NX-OS version in the form of chart with colors with total number of switches with each version in the brackets.

Dashlet	Description
Switch Models	Displays the switch PIDs in the form of chart with colors with total number of switches with each version in the brackets.
Fabrics	Displays all the fabrics and their associated controller. It also displays the state of operation and health of each fabric.
Switches	Displays all the switches and their associated controller and fabrics. It also displays the health of each switch.
Controllers	Displays Fabric Health, Switch Health, Switch Release Versions, and Switch models for each controller in the federation setup.



CHAPTER 27

Device Manager

• Device Manager, on page 263

Device Manager

This chapter contains help information for Device Manager. This chapter contains the following sections:

Physical

This section includes the physical attributes for the DCNM SAN setup:

Inventory

Field	Description
Name	Field Replaceable Unit (FRU) name.
ModelName	Model name identifier.
SerialNumber	Primary and secondary serial numbers.
HardwareRevision	Hardware revision.
SoftwareRevision	The release version of Cisco NX-OS software.
Alias	Alias name as specified by a network manager.
AssetID	User-assigned asset tracking identifier as specified by a network manager.

Modules - Status and Config

Field	Description
Name	Module description.
Module	Module name identifier.
OperStatus	Module's operational state.
Reset	Click to reboot the module.

Field	Description
RateModeOverSubscriptionLimit	Select this option to control the restriction on the oversubscription ratio on modules that support it. By default, the restriction is enabled. If you disable this option, all the interfaces on the module are capable of operating at maximum admin speed, regardless of the available bandwidth.
BandwidthFairnessConfig	Select this option to control bandwidth fairness on modules that support it. By default, bandwidth fairness is enabled.
BandwidthFairnessOper	Shows if bandwidth fairness is enabled or disabled. By default, bandwidth fairness is enabled.
X2 xcvrFrequency Config	Specifies the transceiver frequency of the module. • notApplicable - Select this when the module does not support this configuration. • xcvrFreqX2FC - Select this to set the module's FC transceiver frequency to10 Gigabyte. • xcvrFreqX2Eth - Select this to set the module's Ethernet transceiver frequency to10 Gigabyte.
ResetReasonDescription	Why module was last reset.
Local Switching Mode	Shows the status of the local switching modules.
StatusLastChangeTime	When OperStatus was changed.
Power Admin	Allows you to power on and off the Field Replaceable Unit (FRU).
Power Oper	Field Replaceable Unit (FRU) operational power state.
Current	Current supplied by the Field Replaceable Unit (FRU).

Power Supplies

Field	Description
Name	Power supply location.
TotalPowerAvailable	Shows the available power. In combined mode, the total available power is twice the lesser of the two power supplies.
Redundant/Combined	Select to determine how the power supplies are configured. Redundant mode provides a backup power supply if one should fail, but the total power available is less.
ModelName	The model identifier.
OperStatus	Operational power state.
TotalAvailable	Total power available for power supply usage. When Mode is redundant, the total power available will be the lesser power capacity of the power supplies. When Mode is combined, the total power available will be twice the lesser of the power capacities of the operating power supplies.
TotalReserved	Total current drawn by powered-on FRUs

Note If the power supply to the Uros and Paradise is either interrupted or turned off, the OperStatus in the power supply table displays "offEnvOther". However, the corresponding entry for the powered down device the inventory table will remain.

Temperature Sensors

Field	Description
Name	Sensor location.
Threshold Major	Major temperature threshold.
Threshold Minor	Minor temperature threshold.
Current	Most recent measurement seen by the sensor.
Status	The present operational status of the sensor.

Fan

Field	Description
Name	Fan location.
ModelName	The model identifier.
OperStatus	The current operating status.

Switches

Field	Description
Description	A description of the switch and software.
UpTime	The time since the network management portion of the system was last re-initialized.
Name	An administratively-assigned name for this switch.
Location	The physical location of this switch (e.g., `telephone closet, 3rd floor').
Contact	The contact person for this switch, together with information on how to contact this person.
SwitchWWN	The World-Wide Name of this switch.
ClockDateAndTime	The current local date and time for the system. Setting this is equivalent to setting an automated clock and calendar.
TimeZone	The current local time zone for the system. The time zone must be entered in the format GMT, which is the number of hours difference between your time zone and GMT (Greenwich Mean Time).

Field	Description
ProcessorRAM	Total number of bytes of RAM available on the Processor.
NVRAM	Total number of bytes of NVRAM in the entity.
NVRAMUsed	Number of bytes of NVRAM in use.
FIPSModeActivation	Enable or disable FIPS mode on the device. FIPS 140-2 is a set of security requirements for cryptographic modules and it details the U.S. Government requirements for cryptographic modules. A module will comprise both hardware and software such as a data center switching or routing module. The module is said to be in FIP- enabled mode when a request is recieved to enable the FIPS mode and a set of self-tests are successfully run in response to the request. If the self-tests fail, then an appropriate error is returned.
CPUUtilization	The average utilization of CPU on the active supervisor.
MemoryUtilization	The average utilization of memory on the active supervisor.
FlashPartitionSize	Flash partition size.
FlashPartitionFreeSpace	Free space within a Flash partition.
Status	The overall status of the switch.
Vendor	Switch vendor's name, such as Cisco, McData, or Brocade.
Model	Switch model name, such as MDS 9134 or MDS 9124.
Release	Switch software version.
NumFCPorts	Number of physical FC ports in the switch.
WWN	MAC address for the Ethernet VDCs that are discovered.
VDCId	Unique IDs for the Ethernet VDCs that are discovered.
FCoE Enabled	If true, FCoE is enabed for the Ethernet VDCs that are discovered.

ISLs

Field	Description
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.
To Interface	The port index of destination E_port of the link.
Status	The operational status of the link.

NP Link

Field	Description
NPIV (Core)	The NPIV core switch.
F Port	The connected F Port on the NPIV core switch.
NPV	NPV Switch.
NP Port	The connected port on the NPV switch.
Status	The operational status of the link.

ISL's Statistics

Field	Description
Description	An alias name for the interface, as specified by a network manager. For Port Channel and FCIP, this field will always show members if they are available. For FCIP, this field will show compress if compressed.
VSAN(s)	VSAN membership.
Mode	Operating mode of the port> (See Legend).
Connected To	Attached port. This could be a host, storage, or switch port.
Speed	Maximum bandwidth in Gbps.
Rx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Rx Comp	The IP Copmression ratio for received packets on the FCIP device.
Tx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Tx Comp	The IP Copmression ratio for transmitted packets on the FCIP device
Errors	Total number of Rx and Tx errors on the interface. Types of Rx errors include CRC errors, fragmented framed, unsupported class frames, runt frames, jabber frames, and giant Frames. Types of Tx errors are generally CRC errors, but these are rare. If the Errors field is not empty, there are probably Rx errors. For a more detailed breakdown of the error count, check the Monitor dialog box for appropriate interface.

Discards	Total number of Rx and Tx discards on the interface. Rx frames discarded are generally due to protocol errors. On rare occasions, a frame is received without any hardware errors, but a filtering rule set for the MAC address discards the frame due to a mismatch. Discarded Tx frames can be timeout frame discards (port is offline or not up), or timeout frames that are not sent back to the supervisor (class F/2 frames). If the Discards field is not empty, it is probably due to timeout frames.
Log	If checked, writes the record into the message log on each poll interval.

Hosts

Field	Description
Enclosure Name	The name of the enclosure.
Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
FcId	The FC ID assigned for this host.
Link Status	The operational status of the link.
Serial Number	Serial number.
Model	Model name.
Firmware Ver	The version of the firmware executed by this HBA.
Driver Ver	The version of the firmware executed by this HBA.
Information	The information list corresponding to this HBA.
Switch Interface	Interface on the switch that is connected with the end device.

Enclosures

Field	Description
IP Address	The IP address of the enclosure.
Elem. Mgr Use HTTP	Use HTTP to launch the local enclosure.
Elem. Mgr URL/Path	Use a URL to launch the local enclosure
Device Type	If host, it is HBA. If storage, it is the SCSI target.
Vendor	If host, it is HBA. If storage, it is the SCSI target.
Model	If host, it is HBA. If storage, it is the SCSI target.
Firmware Ver	The version of the firmware executed by this HBA.
Driver Ver	The version level of the driver software controlling this HBA.
OS	The type and version of the operating system controlling this HBA

Field	Description
Other Info	The information list corresponding to this HBA.

Device Manager - Preferences

Field	Description
Retry Requests # time(s) after #sec timeout	The number of retries to be attempted after time out (seconds).
Enable Status Polling	Check to enables status polling in every (specified number of) seconds
Trace SNMP packets in Message Log	Check to enable tracing SNMP packets in the message log.
Register for Events after Open, listen on Port 1163	Check to automatically register for events.
Show WWN Vendor	Check to enable showing the WWN vendor name. • Replace - Replace the existing vendor name with the new one. • Prepend - Attach the new vendor name to the beginning of the current vendor name.
Show Timestamps as Date/Time	Check for displaying the time stamp in the Date/Time format.
Telnet Path	Path to the telnet client.
Use Secure Shell instead of Telnet	Check to use secure shell.
CLI Session Timeout	Time interval for the CLI session (in seconds). Enter ‘0’ to disable CLI timeout.
Show Tooltips in Physical View	Check to show tooltips.
Label Physical View Ports with	• FICON - Displays FICON as label for the ports on the device view. • Interface - Displays Interface as label for the ports on the device view.
Export Table	• Tab-Delimited - Exports the table to tab-delimited text file. • XML - Exports the table to xml file.

Interface

The following sections:

Virtual Interface Groups

The Bound Ethernet Interface field in the table can be modified. The remaining fields are for information only.

Field	Description
Switch	Name of the switch hosting this virtual interface group (VIG).
VIG Id	Virtual interface group identifier.
Bound Eth Interface	Physical Ethernet interface associated with this VIG.
Virtual Eth Interfaces	The virtual Ethernet interface bound to this VIG.
Virtual FC Interfaces	The virtual FC interface bound to this VIG.
Operational Status	The current operational state of the VIG.
CreationTime	Date and time when the VIG was created.



Note This table applies only to N5k switches running version less than 4.0(1a).

Virtual FC Interfaces

The following fields in the table can be modified: Description, Bind Type, Bind Interface, Bind MAC Address, FCF Priority, VSAN ID Port, Mode Admin, Status Admin. The remaining fields are for information only.

Field	Description
Switch	Name of the switch hosting this interface.
Interface	Interface name.
Description	Text description of the interface as specified by a network manager.
VIG Id	Virtual interface group to which this virtual FC interface is bound.
Bind Type	The type of interface associated with this virtual FC interface - physical Ethernet interface or MAC address of the FCoE Node (ENode).
Bind Interface	Physical Ethernet interface or Ethernet port channel associated with this virtual FC interface.
Bind MACAddress	MAC address of an FCoE Node (ENode) or a remote Fibre Channel Forwarder (FCF) identified by the virtual FC interface.
FCF Priority	The FCoE Initialization Protocol (FIP) priority value advertised by the FCF to ENodes.
VSAN ID Port	VSAN ID to which this interface is statically assigned.
VSAN Id Dynamic	Index of the VSAN to which this interface is statically assigned.
Mode Admin	The port mode configured by the user. Virtual FC interfaces support only fabric port (F Port) mode.
Rate Mode	Specifies the interface as dedicated mode or shared mode.
Speed Oper	Operational speed.
Mode Oper	The current operating mode of the port.

Field	Description
Speed Admin	The port speed configured by the user.
Status Service	Specifies whether the interface is in service or out of service.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
Status FailureCause	The cause of current operational state of the port.
Status LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.



Note VIG Id field applies only to N5k switches running version less than 4.0(1a).

Ethernet Interfaces

The Description and Admin fields in the table can be modified. The remaining fields are for information only.

Field	Description
Switch	Name of the switch hosting this interface.
Interface	Interface name.
Description	Text description of the interface as specified by a network manager.
VIG Id	Virtual interface group to which this virtual interface is bound.
Bound Eth Interface	Physical Ethernet interface associated with this virtual Ethernet interface.
Admin	The desired state of the interface.
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
CDP (Enable)	Indicates whether the Cisco Discovery Protocol is currently running on this interface.
Duplex Status	The current mode of operation of the MAC entity. The status 'unknown' indicates that the current duplex mode could not be determined.
Enable Link Trap	Specifies whether Link Up or Link Down traps should be generated for this interface.



Note This table applies only to N5k switches running version less than 4.0(1a).

Virtual FC Ethernet

Field	Description
Switch	Name of the switch hosting this interface.
Interface	Displays the name of the vFC interface and its association with other interfaces.
Description	Text description of the interface as specified by a network manager.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
Speed Oper	Operational speed of the interface
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.

Quick Configuration Tool

Field	Description
Show All Interfaces	Check this checkbox to show all the available interfaces including the interfaces that are not available for binding to a vFC.
Auto Assigin vFC Id	Check this checkbox to select vFC Id automatically. If you do not select this option you must manually enter a valid vFC Id.
Switch Operational Type	Click **Ethernet Switch** if you are not configuring any Fibre Channel interfaces on the switch. Click **FCoE Switch** if you are configuring Fibre Channel and FCoE interfaces.
Interface	Name of the physical Ethernet interface. If you hover the cursor over a physical Ethernet interface, any associated virtual interfaces are displayed in the tooltip.
FCoE VLAN(VSAN)	FCoE VLAN (VSAN) mapping to be used by the interface.
Admin Mode	Admin mode of the vFC interface, i.e. F or E
Eth Only	Configures the physical Ethernet without any virtual interfaces. Click the **Eth Only** button in the column header to set all the interfaces to this value.
vEth Only	Configures the physical Ethernet to have an associated VIG and a virtual Ethernet interface. Click the **vEth Only** button in the column header to set all the interfaces to this value.
vFC Only	Configures the physical Ethernet to have an associated VIG and a virtual FC interface. Click the **vFC Only** button in the column header to set all the interfaces to this value.
vFC	Configures the physical Ethernet to have an associated VIG and a virtual FC interface. Click the **vFC** button in the column header to set all the interfaces to this value.
vEth + vFC	Configures the physical Ethernet to have an associated VIG, a virtual Ethernet interface and a virtual FC interface. Click the **vEth + vFC** button in the column header to set all the interfaces to this value.

Field	Description
Configure Action Status	Displays the current status of the requested configuration changes.

Note vEth only, vFC only, vEth + vFC columns are not applicable for N5K switches running version 4.0(1a)N1

Note vFC column is applicable only for N5K switches running version 4.0(1a)N1

Note For earlier configured ports, mapping details will not be displayed in VLAN(VSAN) Mapping column.

Ethernet Interface

Field	Description
Description	An `alias' name for the interface as specified by a network manager.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
Speed Oper	Operational speed of the interface.
Speed Admin	• notApplicable - The Speed change is not applicable for that port. • oneGigSpeed - The IPStorage port is configured as 1G. • tenGigSpeed - The IPStorage port is configured as 10G.
Failure Cause	Causes of the failures.
PhysAddress	The interface's MAC address.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
ConnectorPresent	True if the connector is detected.
CDP (Enable)	An indication of whether the Cisco Discovery Protocol is currently running on this interface.
IscsiAuthMethod	The authentication method.

Field	Description
Promiscuous Mode	Checking or unchecking this option dictates the destination of the packets/frames. If this option is checked, then this interface accepts packets/frames that are addressed to this station. If this option is not selected, then packets accepted by the station are transmitted on the media. Checking or unchecking this option does not affect the reception of broadcast and multicast packets/frames by the interface.
AutoNegotiate	Select this option to enable auto negotiation.
Beacon Mode	In beacon mode, an interface LED is assigned a flashing mode for identification. Select this option to enable beacon mode.
IPAddress/Mask	IP address and subnet mask for the interface.

Note SAN Admin users cannot change the ethernet interfaces settings in Cisco Nexus 5000 Series switches using Device Manager.

Ethernet Interfaces iSCSI

Field	Description
Description	An `alias' name for the interface as specified by a network manager.
Speed	Operational speed.
PhysAddress	The interface's WWN.
Admin	The desired state of the interface.
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value contains a N/A value.
PortVSAN	The VSAN that the interface belongs to.
ForwardingMode	Use Store and Forward if the HBA has problems with Passthrough.
Initiator ID Mode	How the initiator is identified on this interface, either by its iSCSI name (name) or by its IP address (ipaddress).
Enable	The intiator proxy mode for this interface. If true, then all the initiators coming on this interface would use the intiator configuration provided by this interface. The initiator configuration include port WWN and node WWN.
Assignment	How the initiator proxy mode FC addresses are assigned. If `auto', then the FC addresses are automatically assigned. If it is `manual', then they have to be manually configured.
Port WWN	The Port FC address used by the intiators on this interface when the intiator proxy mode is on.

Field	Description
Node WWN	The Node FC address used by the initiators on this interface when the initiator proxy mode is on.

Ethernet Interfaces iSCSI TCP

Field	Description
Local Port	Local interface TCP port.
SACK	Indicates if the Selective Acknowledgement (SACK) option is enabled or not.
KeepAlive	The TCP keep alive timeout for this iSCSI interface. If the value is 0, the keep-alive timeout feature is disabled.
MinTimeout	The TCP minimum retransmit time.
Max	The TCP maximum retransmissions.
SendBufferSize	The TCP send buffer size.
MinBandwidth	The TCP minimum bandwidth.
MaxBandwidth	The TCP maximum bandwidth.
Estimated Round Trip	The estimated round trip delay of network pipe used for B-D product computation. The switch can use this to derive the TCP window to advertise.
QoS	The TCP QoS code point.
PMTU Enable	Indicates if the Path MTU discovery option is enabled or not.
PMTU Reset Timeout	The PMTU reset timeout.
Connections Normal	The number of normal iSCSI connections.
Connections Discovered	The number of discovery iSCSI connections.
CWM Enable	If true, congestion window monitoring is enabled. If false, it is disabled.
CWM Burst Size	The maximum burst sent after a TCP sender idle period.
Max Jitter	The maximum delay variation (not due to congestion) that can be experienced by TCP connections on this interface.
Port	The local TCP port of this interface.

Ethernet Interfaces VLAN

Field	Description
Switch	Name of the switch.
Interface	Name of the interface.

Field	Description
VLAN mode	The mode in which this VLAN is configured. Static—A port with static VLAN membership directly assigned to a single VLAN. Dynamic—A port with dynamic VLAN membership assigned to a single VLAN based on the content of packets received on the port via VQP queries to VMPS. multiVLAN—A port with multiple VLAN memberships that are directly assigned to one or more VLANs.
VLAN list	The list of VLANs which are allowed on the switch.

Ethernet VLAN

Field	Description
Switch	Name of the switch.
ID	Switch ID
Trunk Mode	Specifies whether the mode is access or trunk.
Trunk Status	Ttrunking status of the port.
Native VLAN	Native VLANs
Allowed VLAN List	The list of VLANs which are allowed to be received/transmitted on the port.
Active VLAN List	The list or range of VLANs that are active on the switch.

FC Interface Monitor Traffic

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
C3 Rx Bytes	The number of Class 3 bytes, including the frame delimiters, received by this port from its attached Nx_Port.
C3 Rx Frames	The number of Class 3 frames, including the frame delimiters, received by this port from its attached Nx_Port.
C3 Tx Bytes	The number of Class 3 bytes, including the frame delimiters, transmitted by this port to its attached Nx_Port.
C3 Tx Frames	The number of Class 3 frames, including the frame delimiters, transmitted by this port to its attached Nx_Port.
CF Rx Bytes	The number of Class F bytes, including the frame delimiters, received by this port from its attached Nx_Port.
CF Rx Frames	The number of Class F frames, including the frame delimiters, received by this port from its attached Nx_Port.
CF Tx Bytes	The number of Class F bytes, including the frame delimiters, transmitted by this port to its a attached Nx_Port.

Field	Description
CF Tx Frames	The number of Class F frames, including the frame delimiters, transmitted by this port to its attached Nx_Port.

FC Interface Monitor Protocol

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
LRRIn	The number of Link reset responses received by the FC-port.
LRROut	The number of Link reset responses transmitted by the FC-port.
OlsIns	The number of Offline Sequence errors received by the FC-Port.
OlsOuts	The number of Offline Sequence errors issued by the FC-Port.
NOSIn	The number of Non-Operational Sequences received by the FC-port.
NOSOut	The number of Non-Operational Sequences transmitted by the FC-port.
LinkResetIns	The number of link reset protocol errors received by the FC-Port from the attached FC-port.
LinkResetOuts	The number of link reset protocol errors issued by the FC-Port to the attached FC-Port.
TxWaitCount	The number of times the FC-port waited due to lack of transmit credits.
RxBBCredit	The maximum number of receive buffers available for holding Class 2, Class 3 received from the logged-in Nx_Port. It is for buffer-to-buffer flow control in the incoming direction from the logged-in Nx_Port to FC-port.
TxBBCredit	The total number of buffers available for holding Class 2, Class 3 frames to be transmitted to the logged-in Nx_Port. It is for buffer-to-buffer flow control in the direction from FC-Port to Nx_Port.
BBCreditTransitionFromZero	The number of transitions of BB credit out of zero state.

FC Interface Monitor Discards

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Class2	The number of Class 2 frames discarded by this port.
Class3	The number of Class 3 frames discarded by this port.
ClassF	The number of Class F frames discarded by this port.
EISL	The number of Enhanced Inter Switch Link (EISL) frames discarded by the FC-port. EISL frames carry an EISL header containing VSAN among other information.
InDiscards	The total number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.

Field	Description
OutDiscards	The total number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

FC Interface Monitor Link Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
LinkFailures	The number of link failures detected by the FC-Port.
SigLosses	The number of signal losses detected by the FC-Port.
SyncLosses	The number of loss of synchronization failures detected by the FC-Port.
InvalidTxWords	The number of invalid transmission words detected by the FC-Port.
DelimiterErrors	The number of Delimiter Errors detected by the FC-Port.
AddressIdErrors	The number of address identifier errors detected by the FC-Port.

FC Interface Monitor Frame Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InvalidCrcs	The number of invalid CRCs detected by the FC-Port. Loop ports should not count CRC errors passing through when monitoring.
ELPFailures	The number of Exchange Link Parameters Switch Fabric Internal Link service request failures detected by the FC-Port. This is applicable to only Interconnect_Port, which are E_Port or B_Port.
Frags	The number of fragmented frames received by the FC-port.
Runts	The number of frames received by the FC-port that are shorter than the minimum allowable frame length regardless if the CRC is good or not.
Jabbers	The number of frames received by the FC-port that are longer than a maximum frame length and also have a CRC error.
TooLongs	The number of frames received by the FC-port where the frame length was greater than what was agreed to in FLOGI/PLOGI. This could be caused by losing the end of frame delimiter.
TooShorts	The number of frames received by the FC-port where the frame length was less than the minimum indicated by the frame header (normally 24 bytes), but it could be more if the DFCTL field indicates an optional header should be present.
Unknowns	The number of unknown class frames received by FC-port.
EOFa	The number of frames received by FC-port with EOF aborts.
Framing	The number of framing errors. This denotes that the FC-port detected an inconsistency of frame structure.

FC Interface Monitor Class 2 Traffic

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
In Octets/In Frames	The number of Class 2 frame bytes and frames, including the frame delimiters, received by this port from its attached Nx_Port.
Out Octets/Out Frames	The number of Class 2 frame bytes and frames, including the frame delimiters, delivered through this port to its attached Nx_Port.

FC Interface Monitor Class 2 Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
FBSY	The number of busy frame responses.
FRJT	The number of F_RJT frames generated by this port against Class 2 frames.
PBSY	The number of times that port busy was returned to this port as result of a class 2 frame that could not be delivered to the other end of the link. This occurs if the destination Nx_Port is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection).
PRJT	The number of times that port reject was returned to this port as a result of a class 2 frame that was rejected at the destination Nx_Port.

FC Interface Monitor FICON

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
FramePacingTime	Number of 2.5 microsecond units that frame transmission is blocked due to zero credit.
DispErrorsInFrame	Number of frames with disparity errors.
EOFErrs	Number of frames with EOF errors.
DispErrsOutOfFrame	Number of frames with OOF errors.
InvalidOrderSets	Number of invalid or unrecognizable Order Sets outside of frames.

Check Oversubscription

Field	Description
Interval	
Elapsed	Time elapsed.
Interface	Name of the interface
InOctectRate	
OutOctectRate	

Virtual FC Interface Monitor Traffic

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
RxBytes	The number of bytes, including the frame delimiters, received by this port from its attached N_Port.
RxFrames	The number of frames, including the frame delimiters, received by this port from its attached N_Port.
TxBytes	The number of bytes, including the frame delimiters, transmitted by this port to its attached N_Port.
TxFrames	The number of frames, including the frame delimiters, transmitted by this port to its attached N_Port.

Virtual FC Interface Monitor Discards

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InDiscards	The total number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
OutDiscards	The total number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Virtual FC Interface Monitor Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InErrors	The number of incoming errors detected by the virtual FC port.
OutErrors	The number of outgoing errors detected by the virtual FC port.

Ethernet Interface Dot3Stats

Field	Description
Interface	Name of the interface.
Alignment Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
FCS Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Multiple Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collisions.

Field	Description
SQE Test Errors	The number of times the PLS sublayer generated the SQE TEST ERROR message for a particular interface.
Deferred Transmissions	The count of the number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Late Collisions	The number of times that a collision is detected on a particular interface later than one slot time into the transmission of a packet.
Excessive Collisions	The count of the number of frames for which transmission on a particular interface failes because of excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal Mac Transmit Errors	The count of the number of frames for which transmission on a particular interface fails because of an internal MAC sublayer transmit error.
Carrier Sense Errors	The number of times that a carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Longs	The count of number of frames received on a particular interface that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The count of number of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error.
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present

Interface Monitor

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Rx Bytes	The total number of bytes received on the interface, including framing characters.
RxFrames	The number of frames received on the interface.
Rx Multicast Frames	(Nexus 5000 Series only) The number of multicast frames received on the interface.
Rx Broadcast Frames	(Nexus 5000 Series only) The number of broadcast frames received on the interface.
TxBytes	The total number of bytes transmitted out of the interface, including framing characters.
TxFrames	The total number of frames transmitted out of this interface.
Tx Multicast Frames	(Nexus 5000 Series only) The number of multicast frames transmitted out of this interface.
Tx Broadcast Frames	(Nexus 5000 Series only) The number of multicast frames transmitted out of this interface.
RxErrors	The number of inbound frames that contained errors preventing them from being deliverable to a higher-layer protocol.
TxErrors	The number of outbound frames that could not be transmitted because of errors.

Field	Description
RxDiscards	The number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
TxDiscards	The number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Ethernet PortChannels

Field	Description
Description	Alias name for the interface as specified by a network manager.
Members	Members of this Ethernet port channel.
Oper Speed	Operational speed of the interface.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
PhysAddress	The interface's MAC address.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.

Ethernet Interface Monitor iSCSI Connections

Field	Description
RxBytes	Total number of bytes received on an iSCSI session.
TxBytes	Total number of bytes transmitted on an iSCSI session.
IPSEC	A collection of objects for iSCSI connection statistics.

Ethernet Interface Monitor TCP

Field	Description
Opens	The number of times connections have been opened.
Accepts	The number of times connections have been accepted.
Failed	The number of times connections have failed.
RxResets	The number of times connections have been reset.
Est	The number of connections that have been established.
RxSegs	The total number of segments received on established connections, including those received in error.
TxSegs	The total number of segments sent, except for those containing retransmitted bytes.

Field	Description
ReTxSegs	The total number of segments retransmitted.
BadSegs	The total number of segments received in error (e.g., bad checksums).
TxSegResets	The number of segments sent containing the "reset" flag.
SplitSeg	The number of segments sent which were less than the minimum.
DupACKs	The number of duplicate ACKs received.
RxBytes	The number of header and data bytes received.
TxBytes	The number of header and data bytes sent.

FCIP Monitor

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
C3 Rx Bytes	The number of incoming bytes of data traffic.
C3 Tx Bytes	The number of outgoing bytes of data traffic.
CF Rx Bytes	The number of incoming bytes of control traffic.
CF Tx Bytes	The number of outgoing bytes of control traffic.
Rx Error	The number of inbound frames that contained errors preventing them from being deliverable to a higher-layer protocol.
Tx Error	The number of outbound frames that could not be transmitted because of errors.
RxDiscard	The number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
TxDiscard	The number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Monitor SVC Interface

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Rx Bytes	Number of incoming bytes.
Rx Frames	Number of incoming frames.
Tx Bytes	Number of outgoing bytes.
Tx Frames	Number of outgoing frames.
Rx Errors	Number of incoming errors.

Field	Description
Tx Errors	Number of outgoing errors.
Rx Discards	Number of incoming discards.
Tx Discards	Number of outgoing discards.

Monitor SVC NPorts

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Rx Bytes	Number of incoming bytes on this virtual N-port.
Rx Frames	Number of incoming frames on this virtual N-port.
Tx Bytes	Number of outgoing bytes on this virtual N-port.
Tx Frames	Number of outgoing frames on this virtual N-port.
Rx Bytes	Number of incoming bytes on this virtual N-port.
Rx Frames	Number of incoming frames on this virtual N-port.
Tx Bytes	Number of outgoing bytes on this virtual N-port.
Tx Frames	Number of outgoing frames on this virtual N-port.

Monitor SVC Session FCP

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Cmds	Number of incoming FCP Command frames in this session.
XferRdys	Number of incoming FCP Transfer Ready frames in this session.
DataFrames	Number of incoming FCP Data frames.
Status	Number of incoming FCP status frames.
DataBytes	Number of incoming FCP Data bytes.
OverRuns	Number of incoming FCP Overrun frames in this session.
UnderRuns	Number of incoming FCP Underrun frames in this session.
Cmds	Number of outgoing FCP Command frames in this session.
XferRdys	Number of outgoing FCP Transfer Ready frames in this session.
DataFrames	Number of outgoing FCP Data frames.

Field	Description
Status	Number of outgoing FCP status frames.
DataBytes	Number of outgoing FCP Data bytes.
OverRuns	Number of outgoing FCP OverRun frames in this session.
UnderRuns	Number of outgoing FCP UnderRun frames in this session.

Monitor SVC Session Other

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InELSFrames	Number of incoming Extended Link Service frames in this session.
InBLSFrames	Number of incoming Basic Link Service frames in this session.
OutELSFrames	Number of outgoing Extended Link Service frames in this session.
OutBLSFrames	Number of outgoing Basic Link Service frames in this session.
InAborts	Number of incoming aborted frames in this session.
OutAborts	Number of outgoing aborted frames in this session.
OpenXchanges	Number of Open Exchanges in this session.
InBadFc2Drops	Number of FC2 dropped frames in this session.
InBadFcPDrops	Number of FCP dropped frames.
InFCPDataExcess	Number of FCP Data Excess frames in this session.

FCIP Interfaces

Field	Description
Description	Alias name for the interface as specified by a network manager.
PortVsan	The VSAN ID to which this interface is statically assigned.
Oper Mode	The current operating mode of the port.
AutoChannelCreate	If checked, automatically create the PortChannel.
Admin	The desired state of the interface.
Oper Status	The current operational state of the interface.
FailureCause	The cause of current operational state of the port.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
FICON Address	The FICON port address of this port.

System Timeout

If frames residing in the switch for a long time, they should be regarded as congestion drop. If there is continuously no tx/rx credits received, it should be regarded as no credit drop. You can configure the timeout value of congestion drop and no credit drop in the Device Manager client. To configure the slow port monitor timeout, please go to **Admin > System Timeout**.

Field	Description
E port Congestion Drop	Specify the time for E port congestion drop. Or click on default to input a default value. The unit is ms.
F port Congestion Drop	Specify the time for F port congestion drop. Or click on default to input a default value. The unit is ms.
F port NoCredit Drop	Specify the time for no credit drop. Click on disable if you do not want to drop the frames without tx/rx credits or click on default to input a default value. The unit is ms.
E Port slowport-monitor	Specify the slowport-monitor timeout value for E port. Click on disable to disable slowport monitoring. Or click on default to input a default value. The unit is ms.
F Port slowport-monitor	Specify the slowport-monitor timeout value for F port. Click on disable to disable slowport monitoring. Or click on default to input a default value. The unit is ms.

Note To configure the slow port monitor time out values from SAN client, go to **Physical Attributes > Switches > System> Timeout**.

Interface License

Field	Description
Type	Specifies the license that can be acquired for a given interface. Currently, the Port Activation license can be defined.
Config	Displays the license for which an interface is eligible. An interface which is not eligible for any type of license will not be displayed.
Oper	The current state of port license on the interface is displayed.

General

Field	Description
Description	An `alias' name for the interface as specified by a network manager.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
Oper	Operational speed
PhysAddress	The interface's MAC address.
Admin	State of the admin.
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state.
CDP	Enable or disable CDP.
Default Gateway	The IP address of the default gateway.

FC Interfaces General

The following variables are not supported by all interfaces: PortVSAN, Port Mode Admin and Oper, Admin Speed, and FailureCause.

Field	Description
Description	Alias name for the interface as specified by a network manager.
VSAN Id Port	VSAN ID to which this interface is statically assigned.
VSAN Id Dynamic	The VSAN ID that this interface has been dynamically assigned (
CDP (Enable)	An indication of whether the Cisco Discovery Protocol is currentl interface.
Promiscuous Mode	Checking or unchecking this option dictates the destination of the option is checked, then this interface accepts packets/frames that a station. If this option is not selected, then packets accepted by the on the media. Checking or unchecking this option does not affect the reception of l packets/frames by the interface9.
Auto Negotiate	An indication of whether auto-negotiation of speed and duplex m this interface.
Beacon Mode	In beacon mode, an interface LED is assigned a flashing mode fo this option to enable beacon mode.

Field	Description
Mode Admin	The port mode configured by the user. Modes are: • auto - If the user configured the port as auto, then the port initial determines the mode of the port. • F Port - In fabric port mode, an interface functions as a fabric po be connected to a peripheral device (host or disk) operating as a • FL Port - In fabric loop port mode, an interface functions as a fa port may be connected to one or more NL ports (including FL port to form a public arbitrated loop. • E Port - In expansion port mode, an interface functions as a fabr This port may be connected to another E port to create an Inter-S between two switches. E ports carry frames between switches fo fabric management. • FX Port - Interfaces configured as Fx ports can operate in either mode. The Fx port mode is determined during interface initializa the attached N port or NL port. This administrative configuration to operate in any other mode—for example, preventing an interf another switch. • SD Port - In SPAN destination port mode, an interface functions analyzer (SPAN). The SPAN feature is specific to switches in th Family. It monitors network traffic that passes though a Fibre Cl • TL Port - In translative loop port mode, an interface functions as port. It may be connected to one or more private loop devices. T specific to Cisco MDS 9000 family switches and have similar pro • ST Port - In the SPAN tunnel port (ST port) mode, an interface fu point port in the source switch for the RSPAN Fibre Channel tun mode and the remote SPAN (RSPAN) feature are specific to swi MDS 9000 Family. When configured in ST port mode, the interfac to any device, and thus cannot be used for normal Fibre Channe • TE Port - In trunking E port mode, an interface functions as a tru port. It may be connected to another TE port to create an Extend between two switches. TE ports are specific to Cisco MDS 9000 • B Port - While E ports typically interconnect Fibre Channel swit extender devices, such as Cisco's PA-FC-1G Fibre Channel port a bridge port model to connect geographically dispersed fabrics. this port type is "read only" and it cannot be set. • TF Port - Trunking f_Port • TNP Port - Trunking N Proxy port mode applicable only to N-por • NP Port - N Proxy port mode applicable only to N-port Virtualiz
Mode Oper	The current operating mode of the port.
SpeedGroup	Specifies the current speed group configuration on the given interfac • None—The interface speed group configuration on this interfac It is a read-only value. • 10G—The interface speed group configuration on this interface • 1/2/4/8G—The interface speed group configuration on this interfac

Field	Description
Speed Admin	The port speed configured by the user. The port speed values are a 8Gb, 10Gb, autoMax2G, and autoMax4G. **Note** On a Cisco Nexus 5000 Series switch that runs Cisco NX-O can configure the 8-Gbps administrative speed only on an M1060 can configure the speed to 1 Gbps, 2 Gbps, or 4 Gbps on all switc Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(2)
Speed Oper	Operational speed.
RateMode	Specifies the interface as dedicated mode or shared mode.
Status Service	Specifies whether the interface is in service or out of service.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
Status FailureCause	The cause of current operational state of the port.
StatusWasEnabled	If true, this port successfully completed a link initialization.
Status LastChange	When the interface entered its current operational state. If the cur prior to the last re-initialization of the local network management value is N/A.
Port Owner	Administratively assigned name of the current owner of the interf

FC Interfaces Rx BB Credit

Field	Description
Oper	The receive buffer-to-buffer credits configured for the operational port mode.
Model	The BB_Credit model used by the FC-port. The alternate BB_Credit management model can be used in the arbitrated loop topology to manage the flow of frames between the two ports participating in the current loop circuit. Since this is a characteristic of a physical port, this is not applicable for Port Channel ports.
Admin	The receive buffer-to-buffer credits configured for this port.
Extended	The extended BB credits that can be configured on an FC port (in the range 256 through 4095). The acceptable value depends on the BB credit configuration of other ports on the module. This value can only be modified on modules that support the extended BB credit feature.
AdminISL	The receive buffer-to-buffer credits configured for this port to be used if it is operating in xE_port mode.
AdminFx	The receive buffer-to-buffer credits configured for this port to be used if it is operating in Fx mode.

Field	Description
PerfBuffer Admin	The performance buffers configured for this port. These buffers in addition to the buffer-to-buffer credits are used to improve the performance of a port. If a value of 0 is set, then the module uses the built-in algorithm to calculate the number of performance buffers to be used.
PerfBuffer Oper	The performance buffers presently operational on this port.
Oper Rx	The maximum number of receive buffers available for holding Class 2, Class 3, Class F frames received from the peer Interconnect_Port.
Oper Tx	The total number of buffers available for holding Class 2, Class 3, Class F frames to be transmitted to the peer Interconnect_Port.
Current Rx	The current value of receive buffer-to-buffer credits for this port.
Current Tx	The current value of transmit buffer-to-buffer credits for this port.
BbScn Notify	Indicates whether the Buffer-to-buffer State Change Number (BB_SC_N) mode is enabled. If checked, BB_SC_N mode is enabled. If unchecked, BB_SC_N mode is disabled.

FC Interfaces Other

Field	Description
PortChannel Id	The port channel that this interface belongs to.
Fabric WWN	The world wide name given to this interface.
Mtu bytes	The size of the largest frame which can be sent/received on the interface, specified in bytes.
RxDataFieldSize bytes	The largest Data_Field size for an FT_1 frame that can be received by this port.
HoldTime us	The maximum time that the FC-Port shall hold a frame in the transmitter buffer before discarding it, if it is unable to deliver the frame.
Auto Port Channel	Check if you want the PortChannel to be created automatically.
FEC Admin	Specifies the port FEC state configured.
FEC Oper	Specifies the current operating FEC state of the port.

FC Interfaces FLOGI

Field	Description
FcId	The address identifier that has been assigned to the logged-in Nx_Port.
PortName	The world wide name of the logged-in Nx_Port.
NodeName	The world wide name of the Remote Node the logged-in Nx_Port belongs to.
Original PWWN	The original port WWN for this interface

Field	Description
Version	The version of FC-PH that the Fx_Port has agreed to support from the Fabric Login.
BBCredit Rx	The maximum number of receive buffers available for holding Class 2, Class 3 received from the logged-in Nx_Port. It is for buffer-to-buffer flow control in the incoming direction from the logged-in Nx_Port to FC-port.
BBCredit Tx	The total number of buffers available for holding Class 2, Class 3 frames to be transmitted to the logged-in Nx_Port. It is for buffer-to-buffer flow control in the direction from FC-Port to Nx_Port. The buffer-to-buffer flow control mechanism is indicated in the respective BbCreditModel.
CoS	The classes of services that the logged-in Nx_Port has requested the FC-Port to support and the FC-Port has granted the request.
Class2 RxDataSize	The Class 2 Receive Data Field Size of the logged-in Nx_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Nx_Port.
Class2 SeqDeliv	Whether the FC-Port has agreed to support Class 2 sequential delivery during the Fabric Login. This is meaningful only if Class 2 service has been agreed. This is applicable only to Fx_Ports.
Class3 RxDataSize	The Class3 Receive Data Field Size of the logged-in Nx_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Nx_Port.
Class3 SeqDeliv	Whether the FxPort has agreed to support Class 3 sequential delivery during the Fabric Login. This is meaningful only if Class 3 service has been agreed. This is applicable only to Fx_Ports.

FC Interfaces ELP

Field	Description
Neighbor Port	The port world wide name of the peer Interconnect_Port.
Neighbor Switch	The node world wide name of the peer Node.
BBCredit Rx	The maximum number of receive buffers available for holding Class 2, Class 3, Class F frames received from the peer Interconnect_Port. It is for buffer-to-buffer flow control in the incoming direction from the peer Interconnect_Port to local Interconnect_Port. The buffer-to-buffer flow control mechanism is indicated in the respective BbCreditModel.

Field	Description
BBCredit Tx	The total number of buffers available for holding Class 2, Class 3, Class F frames to be transmitted to the peer Interconnect_Port. It is for buffer-to-buffer flow control in the direction from the local Interconnect_Port to peer Interconnect_Port. The buffer-to-buffer flow control mechanism is indicated in the corresponding BbCreditModel.
CoS	The classes of services that the peer Interconnect_Port has requested the local Interconnect_Port to support and the local Interconnect_Port has granted the request.
Class2 SeqDeliv	Whether the local Interconnect_Port has agreed to support Class 2 sequential delivery during the Exchange Link Parameters Switch Fabric Internal Link Service request. This is meaningful only if Class 2 service has been agreed.
Class2 RxDataSize	The Class 2 Receive Data Field Size of the peer Interconnect_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Interconnect_Port. This is meaningful only if Class 2 service has been agreed.
Class3 SeqDeliv	Whether the local Interconnect_Port has agreed to support Class 3 sequential delivery during the Exchange Link Parameters Switch Fabric Internal Link Service request. This is meaningful only if Class 3 service has been agreed.
Class3 RxDataSize	The Class 3 Receive Data Field Size of the peer Interconnect_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Interconnect_Port. This is meaningful only if Class 3 service has been agreed.
ClassF X_ID	When true indicates that the peer Interconnect_Port supplying this parameter requires that an interlock be used during X_ID assignment in Class F. This is meaningful only if Class F service has been agreed.
ClassF RxDataSize	The Class F Receive Data Field Size of the peer Interconnect_Port. Class F service is always agreed between two Interconnect_Ports. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Interconnect_Port.
ClassF ConSeq	The number of sequence status blocks provided by the Interconnect_Port supplying the parameters for tracking the progress of a sequence as a sequence recipient. The maximum number of concurrent sequences that can be specified is 255. A value of N/A in this field is reserved.
ClassF EECredit	The maximum number of Class F data frames which can be transmitted by an Interconnect_Port without receipt of accompanying ACK or Link_Response frames. The minimum value of end-to-end credit is one. The end-to-end credit field specified is associated with the number of buffers available for holding the Data_Field of a Class F frame and processing the contents of that Data_Field by the Interconnect_Port supplying the parameters.

Field	Description
ClassF OpenSeq	The open sequences per exchange shall specify the maximum number of sequences that can be open at one time at the recipient between a pair of Interconnect_Ports for one exchange. This value is used for exchange and sequence tracking.

FC Interfaces Trunk Config

Field	Description
Admin	The trunking mode configured by the user. • When set to nonTrunk, the port negotiates and converts the link into non-trunking mode. This port and the peer port's OperTrunkMode will not carry multiple VSAN traffic. • When set to trunk, the port negotiates and converts the link into trunking mode only if the peer port is trunk or auto. • When set to auto, the port is willing to convert the link to a trunk link only if the peer port is trunk.
Oper	The current trunking mode of the port.
Allowed VSANs	The list of VSANs which are allowed to be received/transmitted on the port when the port is operating in trunking mode. Only ports operating in trunk mode can belong to multiple VSANs.
Up VSANs	The list of VSANs whose operational state is up, that this port is associated with. Only ports operating in trunk mode can be associated to multiple VSANs. This is applicable to only ports operating in trunk mode.

FCIP Interfaces Trunk Failures

Field	Description
FailureCause	An entry is shown in this table if there is an error in the trunk status for the given VSAN.

FC Interfaces IP

Field	Description
Switch	The name of the switch.
Ethernet Interface	A unique value that identifies the ethernet interface.
Ethernet Status	The current operational state of the ethernet interface.
Ethernet IP Address	The Internet address for this entity.
Peer IP Address	The Internet address for this entity
Port	The Port ID string as reported in the most recent CDP message.
Peer Interface	A unique value that identifies the peer interface on this device to which this link pertains.

Field	Description
Peer Device Id	The Peer Device ID string as reported in the most recent CDP message.
IP Security Enabled	Specifies whether the IP Security is turned on or not.

FC Interfaces Physical

Field	Description
BeaconMode	If enabled, an interface LED is put into flashing mode for easy identification of a particular interface.
ConnectorPresent	If true, there is a physical connector.
ConnectorType	The module type of the port connector.
TransmitterType	The technology of the port transceiver.
Vendor	The connector unit vendor.
PartNumber	The connector unit part number.
Revision	The port revision of the connector unit.
SerialNo	The serial number of the connector unit.

FC Interfaces Capability

Field	Description
FC-PH Vers Low	The lowest version of FC-PH that the FC-Port is capable of supporting.
FC-PH Vers High	The highest version of FC-PH that the FC-Port is capable of supporting.
RxDataSize Min	The minimum size in bytes of the Data Field in a frame that the FC-Port is capable of receiving from its attached FC-port.
RxDataSize Max	The maximum size in bytes of the Data Field in a frame that the FC-Port is capable of receiving from its attached FC-port.
HoldTime Min	The minimum holding time (in microseconds) that the FC-Port is capable of supporting.
HoldTime Max	The maximum holding time (in microseconds) that the FC-Port is capable of supporting.
CoS	The Bit mask indicating the set of Classes of Service that the FC-Port is capable of supporting.
ServiceStateCapable	Indicates whether this interface is capable of handling service state change.
PortRateMode Capable	Indicates whether this interface is capable of being configured as dedicated or shared port rate modes.

Field	Description
AdminRxBbCreditExtendedCapable	If true, it is capable of changing the extended buffer-to-buffer credits on the interface. The user can configure the object fcIfAdminRxBbCreditExtended on this interface
Class2Seq Deliv	The flag indicating whether or not the FC-Port is capable of supporting Class 2 Sequential Delivery.
Class3Seq Deliv	The flag indicating whether or not the FC-Port is capable of supporting Class 3 Sequential Delivery.

FC Interfaces FICON Peer

Field	Description
TypeNumber	The type number of the peer node. For example, the type number could be 002105.
SerialNumber	The sequence number assigned to the peer node during manufacturing. For example, the serial number could be 000000023053.
Tag	The identifier of the port in the peer node connected to this port.
FcId	Address Identifier assigned to NX-Port
Status	Specifies the status of the row, is valid, invalid or old.
Name	Name of this port.
Manufacturer	The name of the company that manufactured the peer node. For example, the manufacturer info could be HTC.
ModelNumber	The model number of the peer node. For example, the model number could be F20.
PlantOfMfg	The plant code that identifies the plant of manufacture of the peer node. For example, the plant code of manufacture could be 00.
UnitType	The type of the peer node that this port is communicating.
Alert	The type of link incident that occurred on this interface.

Interfaces NPorts (SVC)

Field	Description
Pwwn	The WWN (Worldwide Name) of the virtual N-port.
FcId	Fibre Channel Identifier of the virtual N-port.
State	The operational state of the virtual N-port.
DownReason	If the state of the N-port is 'down' as depicted by the instance of State, this value denotes the reason why this N-port is 'down'.

Interfaces Sessions

Field	Description
NportPwwn	The WWN of the N-port that belongs to this session.
PeerPwwn	The WWN of the remote N-port for this session.
PeerNwwn	The WWN of the remote N-port for this session.
PeerFcId	Fibre Channel Identifier of the remote port for this session.

IP Statistics TCP

Field	Description
AttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
InErrs	The total number of segments received in error (e.g., bad TCP checksums).
ActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
EstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
InSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted bytes.
RetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted bytes.
OutRsts	The number of TCP segments sent containing the RST flag.

Port Channels Ethernet Interfaces

Field	Description
Description	Alias name for the interface as specified by a network manager.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
PhysAddress	The interface's address at its protocol.
Admin	The desired state of the interface.
Oper	The current operational state of the interface.

Field	Description
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
IPAddress/Mask	The IP address and mask of the interface.
iSCSI AuthMethod	The authentication method for this interface.
iSNS ProfileName	The iSNS server profile name for this interface.

Port Channels FC Interfaces

Field	Description
PortVsan	VSAN to which this interface is statically assigned.
Description	Alias name for the interface as specified by a network manager.
Admin Mode	The port mode configured by the user. If the user configured the port as auto(1), then the port initialization scheme determines the mode of the port. In this case the user can look at OperMode to determine the current operating mode of port. Only auto(1) or ePort(4) is allowed.
Oper Mode	The current operating mode of the port.
Admin Speed	The port speed configured by the user.
Oper Speed	The interface's current bandwidth per second.
Admin Status	The desired state of the interface.
Oper Status	The current operational state of the interface.
FailureCause	The cause of current operational state of the port.
LastChange	The time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the switch, then this is a zero or N/A value.

Port Channels General

Field	Description
Admin Mode	The channel mode desired by the network manager.
Oper Mode	The current operating channel mode of the port.

Field	Description
Force	The method to add port(s) to a Port Channel port. • If unchecked, then a compatibility check is done on the parameters of the port(s) being added to this Port Channel. The port(s) being added must have the same physical and configured parameters as the Port Channel port. • If checked, a compatibility check is done on only physical parameters. The port(s) being added to this Port Channel port must have same physical parameters. The operation will fail only if the physical parameters are not same. The configured parameters of the port(s) being added are overwritten by configured parameters of this Port Channel port.
MemberList By Interface	The list of the E_ports that are members of this Port Channel port.
MemberList By FICON	The list of the E_ports that are members of this Port Channel port.
MemberList LoadBalanced	Those ports which are actively participating in the PortChannel.
LastAction Status	The status of the last operation (add or remove a member) done to change the member list of a Port Channel Port. When no ports are added or the last operation is successful then this value is successful. If this value is failed then the user can look at LastAddStatusCause to find the reason of failure.
LastAction FailureCause	The cause of failure to last operation (add or remove a member) done to change the member list of a Port Channel port.
LastAction Time	The timestamp indicating the time of last action performed on this entry.
CreationTime	The timestamp of this entry's creation time.
FICON Address	The FICON port address. If empty, then this channel is not used by FICON. (This column is displayed if FICON is enabled. This column is grayed out if the Port Channel is auto-created.)

FlexAttach Global

Field	Description
VirtualPwwnauto	Enables automatic generation of Virtual WWNs on all the F_port interfaces. If the value of VirtualPWWNauto is set to 'true', the value of VirtualWWN Auto of all the entries in the VirtualWWN table is implicitely set to true.

FlexAttach Virtual PWWN

Field	Description

virtual pWWN	This is the virtual port WWN for this interface. If the value of VirtualWwnAuto is 'true', then value of this virtual pWWWN is automatically generated by the device.If value of this pWWWN is set explicitely, then value of VirtualWwnAuto is implicitely set to 'false'. If length of pWWWN is zero, then automatic virtual WWN generation is disabled. This pWWWN can not be set to length zero
Auto	Enable automatic generation of Virtual WWNs on this interface.If the value of VirtualWwnPwwn is set explicitely, then the value of Auto will be implicitely set to false. Also, if this Auto is set to 'true', then value of VirtualWwnPwwn is overwritten with auto generated virtual port WWN.
LastChange	The value of sysUpTime at the time of the last change to this Virtual WWN Entry.

FlexAttach Physical to Virtual WWNs

Field	Description
virtual pWWN	This is the virtual port WWN for this device port WWN. In order to minimize WWN collision, no two instances of this Virtual pWWN can have same value. **Note** :The Virtual pWWN cannot be changed when corresponding device is logged in.
LastChange	The value of sysUpTime at the time of the last change to this Virtual WWN Entry.

FIPS

Field	Description
ModeActivation	To enable/disable FIPS mode on the device. FIPS 140-2 is a set of security requirements for cryptographic modules and it details the U.S. Government requirements for cryptographic modules. A module will comprise both hardware and software, eg a datacenter switching or routing module. The module is said to be in FIPS enabled mode when a request is recieved to enable the FIPS mode and a set of self-tests are successfully run in response to the request. If the self-tests fail, then an appropriate error is returned

FCIP FICON Configuration

Field	Description
Interface	This is a unique value that identifies the interface on this FCIP device to which this link pertains.
VSAN List Admin	This is the list of VSANs (in the range 1 through 2047) for which Ficon Tape Acceleration is configured. Only VSANs with a cficonVsanEntry of CISCO-FICON-MIB present can be configured for Ficon Tape Acceleration.

Field	Description
VSAN List Oper	This is the list of VSANs (in the range 1 through 2047) for which Ficon Tape Acceleration is operationally "ON".

Port Channels AutoCreate

Field	Description
Channel	The channel group mode of this PortChannel.
Persistent	True if the PortChannel is persistent.

SPAN Sessions

Field	Description
Dest Interface	The Span Destination port interface.
Filter VSAN List	The VSANs that are assigned to this session.
Status Admin	Suspend an active session or activate an inactive session.
Status Oper	The current state of the session.
Description	The description of the session status.
VSAN List	The VSANs that are assigned to this session.
Or Interface (Direction)	The destination port ID to be configured for the session.
Inactive Reason	Description of the reason why this session is not active.

Span Global

Field	Description
MaxQueuedSpanPackets	This field specifies the drop threshold packets for all span sessions.The MaxQueuedSpanPackets field is only available when no session is active.

SPAN Source Interfaces

Field	Description
Interface, Direction	The destination port ID configured for the session, and the direction of traffic.

Port Tracking Dependencies

Field	Description
Linked, Destination Interfaces	The interfaces that are doing the tracking.
VSAN Type	Whether a single VSAN or all VSANs are being tracked.

Field	Description
VSAN ID	If a single VSAN is being tracked, the ID of that VSAN.

Port Tracking Force Shut

Field	Description
Interface	The interface of the port to be configured for the forced-shut mode.
Force Shut	If true, the port is brought down administratively, and you must bring the port up manually. If false, the port is brought down operationally only, and is brought up again as soon as any one of the tracked ports comes up.

Port Guard

Field	Description
Interface	Name of the interface
Enable	Specifies whether an interface can be stopped from changing between up and down states or allowed to change states continuously.
Duration (sec)	Specifies the time duration in which a port is allowed to change states.
Number of Flaps	Specifies the number of times the port can flap in the time specified in the Duration.
Oper	Operational state of the interface.

Bandwidth Reservation: 48-Port 96-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 4 Gbps on the first port of each group and the remaining ports 8 Gbps shared	Allocates a rate mode and admin speed of 4 Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports
Dedicated 8 Gbps on the first port of each group and the remaining ports 8 Gbps shared	Allocates a rate mode and admin speed of 8 Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports
Shared 8 Gbps on all ports (initial & default settings)	Allocates a rate mode and admin speed of 8 Gbps on all the available ports. This is the default setting.

Bandwidth Reservation: 48-Port 48-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 2 Gbps on the first port of each group and the remaining ports 4 Gbps shared	Allocates a rate mode and admin speed of 2Gbps on the first port of each group and the remaining ports share 4 Gbps depending on the operational speed of the ports

RateMode Config Macro	Description
Dedicated 8 Gbps on the first port of each group and the remaining ports 4 Gbps shared	Allocates a rate mode and admin speed of 8 Gbps on the first port of each group and the remaining ports share 4 Gbps depending on the operational speed of the ports
Shared Auto with Maximum of 4 Gbps on all ports (initial & default settings)	Allocates a maximum rate mode and admin speed of 4Gbps on all the available ports. This is the default setting.

Bandwidth Reservation: 24-Port 48-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 8 Gbps on the first port of each group and the remaining ports 8G shared	Allocates a rate mode and admin speed of 8Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports
Shared Auto on all ports (initial & default settings)	Allocates a rate mode and admin speed of 8 Gbps on all the available ports. This is the default setting.

Bandwidth Reservation: 48-Port 256-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 8 Gbps on the first 4 ports in each 6-port port group and the remaining ports 8G shared	Allocates a rate mode and admin speed of 8Gbps on the first 4 ports in each 6-port port group and the remaining ports share 8 Gbps depending on the operational speed of the ports.
Dedicated 8 Gbps on the first port of each group and the remaining ports 8G shared	Allocates a rate mode and admin speed of 8 Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports.
Shared 8G 0n all ports	Allocates a rate mode and admin speed of 8 Gbps on all the available ports. This is the default setting.
Dedicated 4G 0n all ports	Allocates a rate mode and admin speed of 4Gbps on all the available ports.
Dedicated 10G on following ports: • 4,5,6,7,8,10 (ports 1,2,3,9,11,12 disabled) • 16, 17, 18, 19, 20, 22 (ports 13,14,15, 21,23,24 disabled) • 28,29,30,31,32,34 (ports 25,26,27,33,35,36 disabled) • 40,41,42,43,44,46 (ports 37,38, 39 45, 47, 48 disabled)	Allocates a rate mode and admin speed of 10Gbps on the following ports.

Bandwidth Reservation: 32-Port 256-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 8 Gbps on on all ports	Allocates a rate mode and admin speed of 8 Gbps on all the available ports.
Shared 8 Gbps on on all ports — initial and default settings.	Allocates a rate mode and admin speed of shared 8 Gbps on all the available ports.
Dedicated 10G on following ports: • 2,3,4,5,6,8 (ports 1 and 7 disabled) • 10,11,12,13,14,16 (ports 9 and 15 disabled) • 18,19,20,21,22,24 (ports 17 and 23 disabled) • 26,27,28,29,30,32 (ports 25 and 31 disabled)	Allocates a rate mode and admin speed of 10Gbps on the specified ports.

DS-X9448-768K9 (Luke) Line Card Bandwidth Reservation

RateMode Config Macro	Description
Dedicated 10G on the following ports: • Ports 1-8 • Ports 9-16 • Ports 17-24 • Ports 25-32 • Ports 33-40 • Ports 41-48	Allocates dedicated rate mode and admin speed of 10 Gbps on the specified ports.
Unconfigure 10G on the following ports: • Ports 1-8 • Ports 9-16 • Ports 17-24 • Ports 25-32 • Ports 33-40 • Ports 41-48	Reverts to default rate mode and admin speed on the specified ports. Transceiver frequencey is set to FC. This operation is disruptive.

FC

This section includes the following:

VSAN General

Field	Description
Name	The name of the VSAN. Note that default value will be the string VSANxxxx where xxxx is value of vsanIndex expressed as 4 digits. For example, if vsanIndex is 23, the default value is VSAN0023.
Mtu	The MTU of the VSAN. Normally, this is 2112.

Field	Description
LoadBalancing	The type of load balancing used on this VSAN. • srcdst - use source and destination ID for path selection • srcdst 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
AdminState	The state of this VSAN.
OperState	The operational state of the VSAN.
InOrderDelivery	The InorderDelivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it is not guaranteed.
DomainId	Specifies an insistent domain ID.
FICON	True if the VSAN is FICON-enabled.
Network Latency	Network latency of this switch on this VSAN. This is the time interval after which the frames are dropped if they are not delivered in the order they were transmitted.

VSAN Membership

Field	Description
Switch	Name of the switch
Ports	FC Ports in VSAN
Channels	PortChannels in VSAN
FCIP	FCIP Interfaces in VSAN
iSCSI	iSCSI Interfaces in VSAN
FICON	Interfaces in VSAN by FICON
FC Virtual Interface	Virtual FC interfaces in VSAN

VSAN Interop-4 WWN

Field	Description
VSAN ID	The ID of the VSAN containing the McData switch.
WWN	The WWN of the McData switch.

VSAN Timers

Field	Description
VSAN Id	The ID of the VSAN.
R_A_TOV	The Resource_Allocation_Timeout Value used for FxPorts as the timeout value for determining when to reuse an NxPort resource such as a Recovery_Qualifier. It represents E_D_TOV plus twice the maximum time that a frame may be delayed within the Fabric and still be delivered. Note that all switches in a fabric should be configured with the same value of this timeout.
D_S_TOV	The Distributed_Services_Timeout Value which indicates that how long a distributed services requestor will wait for a response.
E_D_TOV	The Error_Detect_Timeout Value used for FxPorts as the timeout value for detecting an error condition. Note that all switches in a fabric should be configured with the same value of this timeout. Note that value must be less than value of D_S_TOV.
NetworkDropLatency	Network latency of this switch on this VSAN.

VSAN Default Zone Policies

Field	Description
Zone Behavior	Represents the initial value for default zone behavior on a VSAN when it is created. If a VSAN were to be deleted and re-created again, the default zone behavior will be set to the value specified for this object.
Propagation Mode	Represents the initial value for zone set propagation mode on a VSAN when it is created. If a VSAN were to be deleted and re-created again, the zone set propagation mode will be set to the value specified for this object.

IVR Local Topology

Field	Description
VSAN List	The list of configured VSANs that are part of IVR topology on this device.

IVR Fabric ID

Field	Description
VSAN List	The list of configured VSANs that are part of IVR topology on this device.

IVR Default Fabric ID

Field	Description
Fabric Id	The configured Default Autonomous Fabric ID of this switch.

IVR Action

Field	Description
Activate Local Topology	Setting this object to activate is a request for the configured IVR topology to be activated on this device. i.e., for the current configuration of IVR topology to be cloned, with the clone becoming the active IVR topology.
IsActive	This object indicates of IVR topology is active or not. If true, the IVR topology is active. If false, the IVR topology is not active.
Activation Time	When the IVR topology was most recently activated. If the IVR topology has not been activated prior to the last re-initialization of the local network management system, then this value will be N/A.
Enable IVR NAT	Enable FCID and VSAN identifier translation across VSAN boundaries. If true, the VSAN identifier as well as the entire FCID of the end devices would be modified as frames cross VSAN boundaries.
Auto Discover Topology	Enable automatic VSAN topology discovery. If true, automatic VSAN topology discovery is turned on. IVR processes would communicate with each other to provide a global view of the physical topology to all the IVR enabled switches. If false, automatic VSAN topology discovery is turned off.

IVR RDI VSANs

Field	Description
Add Virtual Domain to FC Domain List	This object lists VSANs in which the virtual domains in a VSAN are added to the domain list in that VSAN.

IVR Active Topology

Field	Description
VSAN List	The list of VSANs that are part of IVR topology on this device.

IVR Zoneset Status

Field	Description
Status	Status of the active IV Zoneset on this VSAN.

- idle - Idle
- active - Active
- deactive - Deactive
- defaultZoneDeny - Activation failed because of default zone behavior is deny and there is no regular active zoneset.
- activationFailed - Activation failed
- deactivationFailed - Deactivation failed
- activationNotInitiated - Activation not initiated
- activationFailedFabricChgFailed - Activation failed because of fabric change failed.
- deactivationNotInitiated - Deactivation not initiated.
- deactivationFailedFabChgFailed - Deactivation failed because of fabric change failed.
- deactivationNotInitiated - Deactivation not initiated.
- deactivationFailedFabChgFailed - Deactivation failed because of fabric changing.
- activating - Activation in progress.
- activatingWaitForLowestSwwn - Activation in progress; waiting for the lowest switch WWN switch to add IV zoneset to the regular active zoneset.
- activatingFabricChanging - Activation in progress; fabric is changing.
- deactivating - Deactivation in progress.
- deactivatingWaitForLowestSwwn - Deactivation in progress; waiting for the lowest switch WWN switch to delete IVR zoneset from the regular active zoneset.
- deactivatingFabricChanging - Deactivation in progress; fabric is changing.
- defaultZonePermit - Activation failed because of default zone behavior is permit.
- defaultZonePermitNoForce - Activation failed because of default zone behavior is permit with no force option.
- defaultZonePermitActZsNoForce - Activation failed because of default zone behavior is permit and with regular activate zoneset and no force option.
- denyNoActiveZoneset - Activation failed because there is no active zoneset.
- activationFailedLowestWwnWait - Activation failed waiting for the switch with lowest wwn to activate this zoneset.
- deactivationFailedLowestWwnWait - Deactivation failed waiting for switch with lowest wwn to deactivate this zoneset.
- activationFailedZoneNmCtnsIlChar - Activation fails because one of the zone names in zoneset that is being activated contains illegal character.

IVR Discrepancies

Field	Description
Discrepancy	The checksum of the enforced (active) IV zoneset.
RegionID	Identifies the CFS configuration supported region.

IVR Domains

Field	Description
Domain Id	The FC domain ID that will be used to represent the VSAN.

IVR FCID

Field	Description
FCID	The FCID to be used by IVR to represent the device.

IVR Zoneset Active Zones

Field	Description
VSAN Id	IVR VSAN ID.
Zone	Active IVR zone name.
Fabric Id	Autonomous fabric ID.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
LUNs	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

IVR Zoneset Active Zones Attributes

Field	Description
Zone	Active IVR zone name.
QoS	True if QoS enabled, otherwise false.
QoS Priority	QoS priority value (Low, Medium, or High).
Broadcast	Specifies if broadcast zoning is enabled on this default zone on this VSAN. If true, then it is enabled. If false, then it is disabled.

IVR Zoneset Name

Field	Description
VSAN Id	IVR VSAN ID.
Zone	Active IVR zone name.
Fabric Id	Autonomous fabric ID.

Field	Description
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
Luns	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

DPVM Actions

Field	Description
Action	Helps in activating the set of bindings.
Result	Indicates the outcome of the activation.
Status	Indicates the state of activation. If true, then activation has been attempted as the most recent operation. If false, then an activation has not been attempted as the most recent operation.
CopyActive to Config	When set to copy(1), results in the active (enforced) binding database to be copied on to the configuration binding database. The learned entries are also copied.
Auto Learn Enable	Helps to learn the configuration of devices logged into the local device on all its ports and the VSANs to which they are associated.
Auto Learn Clear	Assists in clearing the auto-learnt entries.
Clear WWN	Represents the Port WWN (pWWN) to be used for clearing its corresponding auto-learnt entry.

DPVM Config Database

Field	Description
Switch	Name of the switch.
Type	Specifies the type of the corresponding instance of device.
WWN or Name or MAC	Represents the logging in device. The value depends on the corresponding device type (PWWN, NWWN or MAC).
VSAN Id	Represents the VSAN to be associated to the port on the local device on which the device represented by cdpvmLoginDev logs in.
Switch Interface	Represents the device alias.

DPVM Active Database

Field	Description
Type	Specifies the type of the corresponding instance of cdpvmEnfLoginDev.
WWN or Name or MAC	Represents the logging in device. The value depends on the corresponding device type (PWWN, NWWN or MAC).
VSAN Id	Represents the VSAN of the port on the local device through which the device represented by cdpvmEnfLoginDev logs in.
Interface	Represents the device alias.
IsLearnt	Indicates whether this is a learnt entry or not. If true, then it is a learnt entry. If false, then it is not.

Domain Manager Running

Field	Description
State	The state of the Domain Manager on the local switch on this VSAN.
DomainId	The Domain ID of the local switch on this VSAN or 0 if no Domain ID has been assigned.
Local Switch WWN	The WWN of the local switch on this VSAN.
Local Priority	The running priority of the local switch on this VSAN.
Principal Switch WWN	The WWN of the principal switch on this VSAN, or empty string if the identity of the principal switch is unknown.
Principal Priority	The running priority of the principal switch on this VSAN.

Domain Manager Configuration

Field	Description
Enable	Enables the Domain Manager on this VSAN. If enabled on an active VSAN, the switch will participate in principal switch selection. If disabled, the switch will participate in neither the principal switch selection nor domain allocation. Thus, Domain ID needs to be configured statically.

Field	Description
Running DomainId	The configured Domain ID of the local switch on this VSAN or 0 if no Domain ID has been configured. The meaning depends on DomainIdType. If Type is 'preferred', then domain ID configured is called 'preferred Domain ID'. The valid values are between 0 and 239. In a situation where this domain could not be assigned, any domain ID would be acceptable. The value '0' means any domain ID. If Type is 'static' (insistent), then domain ID is called 'static Domain ID' and valid values are between 1 and 239. In a situation where this domain was non-zero but could not be assigned, no other domain ID would be acceptable. If the Domain Manager is enabled on the VSAN, then a RDI (Request Domain ID) will be sent requesting this Domain ID. If no Domain ID can be granted in the case of 'preferred' or if the configured 'static' (insistent) domain ID cannot be not granted then, it is an error condition. When this error occurs, the E_ports on that VSAN will be isolated. If the domain manager is not enabled, then the static (insistent) Domain ID is assumed to be granted, if it has been configured (to a valid number). If either of the domain IDs are not configured with a non-zero value on this VSAN and if the domain manager is not enabled, then - switch will isolate all of its E_ports on this VSAN.
DomainId Type	Type of configured Domain ID.
FabricName	The WWN that is used for fabric logins on this VSAN. This is used only if Enable is false. If Enable is true, then principal switch WWN is used. It is automatically set to the default value when set to zero-length value.
Priority	Priority of the switch to be used in principal switch selection process.
Contiguous Allocation	Determines how the switch behaves when elected as the principal switch. If true, switch won't accept non-contiguous domain IDs in RDIs and will try to replace all the Domain IDs in the list with contiguous domain IDs if a RDI for a contiguous Domain ID can not be fulfilled. If false, then the switch acts normally in granting the Domain IDs even if they are not contiguous.
Auto Reconfigure	Determines how the switch responds to certain error conditions. The condition that can cause these errors is merging of two disjoint fabrics that have overlapping Domain ID list. If true, the switch will send a RCF (ReConfigureFabric) to rebuild the Fabric. If false, the switch will isolate the E_ports on which the errors happened.
Persistent FcId	If true, then all the FC ID assigned on this VSAN are made persistent on this VSAN. If false, then all the entries on VSAN in PersistencyTable are deleted.
Purge FcIds?	Tells the Domain Manager to purge the FC IDs on this VSAN in the FC ID persistency database.
Restart?	Tells the Domain Manager to rebuild the Domain ID tree all over again. If 'disruptive', then a RCF (ReConfigure Fabric) is generated in the VSAN in order for the fabric to recover from the errors. If nonDisruptive, then a BF (Build Fabric) is generated in the VSAN.

Field	Description
Optimization	You need to click the field to select one of the following. To disable turbo mode, do not select anything. • Fast-Restart- Set the optimization type to fast restart. • Selective-Restart- Set the optimization type to selective restart.

Domain Manager Domains

Field	Description
SwitchWWN	The WWN of the switch to which the corresponding value of DomainId is currently assigned for the particular VSAN.

Domain Manager Statistics

Field	Description
Prin. Sel Total	The number of principal switch selections on this VSAN.
Prin. Sel Local	The number of times the local switch became the principal switch on this VSAN.
Fabric Builds (BF)	The number of BuildFabrics (BFs) that have occurred on this VSAN.
Fabric Reconfigures (Rcf)	The number of ReconfigureFabrics (RCFs) that have occurred on this VSAN.
FcIds Free	The number of FC IDs that are unassigned on this VSAN.
FcIds Assigned	The number of FC IDs that are assigned on this VSAN.
FcIds Reserved	The number of FC IDs that are reserved on this VSAN.

Domain Manager Interfaces

Field	Description
Role	One of the following: • nonPrincipal - non-principal interface • principalUpstream - upstream principal interface • principalDownsteam - downstream principal interface • isolated - isolated interface • down - down interface unknown • unknown - unknown interface
RcfReject	Determines if the incoming ReConfigure Fabric (RCF) messages on this interface on this VSAN is accepted or not. If true, then the incoming RCF is rejected. If false, incoming RCF is accepted. Note that this does not apply to the outgoing RCFs generated by this interface.

Domain Manager Persistent FcIds

Field	Description
FcId	The FC ID assigned for this WWN on this VSAN. The third octet must be 0x00 if value of PersistencyNum is area.
Mask	The number of FC IDs starting from PersistencyFcId which are assigned either statically or dynamically for this WWN on this VSAN. The value one means just one FC ID is assigned. The value area means all the FC IDs in the area that is specified in the second octet of FcId are assigned. Typically, 256 FC IDs are assigned for an area. This value cannot be changed if the value of Used is true.
Used	Indicates if this FC ID is used or not.
Assignment	The type of persistency of this FC ID.

Domain Manager Allowed DomainIds

Field	Description
List	Provides the lists of domains that are allowed. A domain is allowed in this VSAN if the corresponding bit has a value of 1. If it has a value which is less than 32 bytes long, then the domains which are not represented are not considered to be in the list. If this object is a zero-length string, then no domains are allowed in this VSAN.

Zoneset Active Zones

Field	Description
Zone	Zone name.
Type	Zone member type.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
LUNs	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. • Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

Zoneset Unzoned

Field	Description
Name	Zone member name.

Field	Description
WWN	Zone member WWN.
FcId	Zone member FC ID.

Zoneset Status

Field	Description
Status	Indicates the outcome of the most recent activation/deactivation.
Activation Time	When this entry was most recently activated. If this entry has been activated prior to the last re-initialization of the local network management system, then this value will be N/A.
FailureCause	The reason for the failure of the zoneset activation/deactivation.
FailedSwitch	The domain ID of the device in the fabric that has caused the Change Protocol to fail.
Active == Local?	Indicates whether the enforced database is the same as the local database on this VSAN. If true, then they are the same. If false, then they are not the same.
Active Zoneset	The name of the enforced IV zoneset.
Hard Zoning	Indicates whether the hard zoning is enabled on this VSAN. Hard zoning is a mechanism by which zoning is enforced in hardware. If true, then hard zoning is enabled on this VSAN. If false, then hard zoning is not enabled on this VSAN.

Zoneset Policies

Field	Description
Default Zone Behavior	Controls the behavior of the default zone on this VSAN. If it is set to permit, then the members of the default zone on this VSAN can communicate with each other. If it is set to deny, then the members of the default zone on this VSAN cannot communicate with each other.
Default Zone ReadOnly	Indicates whether SCSI read operations are allowed on members of the default zone which are SCSI targets, on this VSAN. If true, then only SCSI read operations are permitted. So, this default zone becomes a read-only default zone on this VSAN. If false, then both SCSI read and write operations are permitted.
Default Zone QoS	Specifies whether the QoS attribute for the default zone on this VSAN is enabled. If true, then QoS attribute for the default zone on this VSAN is enabled. If false, then the QoS attribute for the default zone on this VSAN is disabled.
Default Zone QoS Priority	Specifies the QoS priority value.
Default Zone Broadcast	Specifies if broadcast zoning is enabled on this default zone on this VSAN. If true, then it is enabled. If false, then it is disabled.
Propagation	Controls the way zoneset information is propagated during Merge/Change protocols on this VSAN

Field	Description
Read From	Specifies whether the management station wishes to read from the effective database or from the copy database.

Zoneset Active Zones Attributes

Field	Description
Name	Zone name.
Read Only	Indicates if only SCSI read operations are allowed on members of the default zone which are SCSI targets on this VSAN. If true, then only SCSI read operations are permitted. So, this default zone becomes a read-only default zone on this VSAN. If false, then both SCSI read and write operations are permitted.
QoS	Specifies whether the QoS attribute for the default zone on this VSAN is enabled. If true, then QoS attribute for the default zone on this VSAN is enabled. If false, then the QoS attribute for the default zone on this VSAN is disabled.
QoS Priority	Specifies QoS priority value (Low, Medium, or High).
Broadcast	Specifies if broadcast zoning is enabled on this default zone on this VSAN. If true, then it is enabled. If false, then it is disabled.

Zoneset Enhanced

Field	Description
Action	When set to basic(1), results in the zone server operating in the basic mode as defined by FC-GS4 standards. When set to enhanced(2), results in the zone server operating in the enhanced mode as defined by FC-GS4 standards.
Result	The outcome of setting the mode of operation of the local Zone Server on this VSAN.
Config DB Locked By	Specifies the owner for this session.
Config DB Discard Changes	Assists in committing or clearing the contents of the copy database on this session.
Config DB Result	Indicates the outcome of setting the corresponding instance of czseSessionCntl to commitChanges(1).
Enforce Full DB Merge	Controls the zone merge behavior. If this object is set to allow, then the merge takes place according to the merge rules. If set to restrict, then if the merging databases are not exactly identical, the Inter-Switch Link (ISL) between the devices is isolated.
Read From	Specifies whether the management station wishes to read from the effective database or from the copy database.

Zoneset Read Only Violations

Field	Description
Violations	The number of Data protected Check Condition error responses sent by the local Zone Server.

Zoneset Statistics

Field	Description
Merge Req Tx	The number of Merge Request Frames sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Merge Req Rx	The number of Merge Request Frames received by this Zone Server from other Zone Servers in the fabric on this VSAN.
Merge Acc Tx	The number of Merge Accept Frames sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Merge Acc Rx	The number of Merge Accept Frames received by this Zone Server from other Zone Servers in the fabric on this VSAN.
Change Req Tx	The number of Change Requests sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Change Req Rx	The number of Change Requests received by this Zone Server from other Zone Servers in the fabric on this VSAN.
Change Acc Tx	The number of Change Responses sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Change Acc Rx	The number of Change Responses received by this Zone Server from other Zone Servers in the fabric on this VSAN.
GS3 Rej Tx	The number of GS3 requests rejected by this Zone Server on this VSAN.
GS3 Req Rx	The number of GS3 requests received by this Zone Server on this VSAN.

Zoneset LUN Zoning Statistics

Field	Description
INQUIRY	The number of SCSI INQUIRY commands that have been received by the local zone server.
REPORT LUN	The number of SCSI Report LUNs commands that have been received by the local zone server. Typically the Report LUNs command is sent only for LUN 0.
SENSE	The number of SCSI SENSE commands that have been received by the local zone server.
Other Cmds	The number of SCSI Read, Write, Seek, etc., commands received by the local zone server.
BadInquiry Errors	The number of No LU error responses sent by the local zone server.
Illegal Errors	The number of Illegal Request Check Condition responses sent by the local zone server.

Zoneset Members

Field	Description
Zone	Default zone.
Type	FCID.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
Luns	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

Fabric Config Server Discovery

Field	Description
Status	The status of the discovery on the local switch. Initially when the switch comes up, this will be set to databaseInvalid state on all VSANs. This indicates that a discovery needs to be done. The state will be set to inProgress for this VSAN during the discovery. Once the discovery is completed on this VSAN, this will be set to completed. After the discovery is completed for the specified list of VSANs, the data is cached for an interval of time. Once this interval of time expires, the data is lost and this will be set to databaseInvalid state for the specified list of VSANs.
CompleteTime	When the last discovery was completed on this VSAN. This value is N/A before the first discovery on this VSAN.

Fabric Config Server Interconnect Elements

Field	Description
Type	The type of this Interconnect Element.
DomainId	The Domain Id of this Interconnect Element. If the Domain Id has not been configured, then this value is 0.
MgmtId	The management identifier of this Interconnect Element. If the Interconnect Element is a switch, then this will be the Domain Controller identifier of the switch.
FabricName	The fabric name of this Interconnect Element.

Field	Description
LogicalName	The logical name of this Interconnect Element.
Vendor, Model, Release, WWN	The information list corresponding to this Interconnect Element.
MgmtAddrList	The management address list corresponding to this Interconnect Element.

Fabric Config Server Platforms (Enclosures)

Field	Description
Name	The name of this platform.
Type	The type of this platform.
ConfigSource	The source of configuration of this entry. Note that an entry which is configured via GS3 cannot be deleted through SNMP.
NodeList	The node name list corresponding to this platform.
MgmtAddrList	The management address list corresponding to this Platform.

Fabric Config Server Fabric Ports

Field	Description
Type	The type of this port.
TXType	The TX type of this port.
ModuleType	The module type of this port.
Interface	The physical number corresponding to this port entry.
State	The state of this port.
AttachedPortList	The attached port name list corresponding to this port.

FC Routes

Field	Description
Preference	The value used to select one route over another when more than one route to the same destination is learned from different protocols, peers, or static routes. The preference value is an arbitrarily assigned value used to determine the order of routes to the same destination in a single routing database (RIB). The active route is chosen by the lowest preference value.
LastChangeTime	The last time a row was created, modified, or deleted in the FC route table.
DomainId	The domain ID of next hop switch. However, when read, this value could be N/A if the value of fcRouteProto is local.
Metric	The routing metric for this route. The use is dependent on fcRouteProto used.

Field	Description
Type	The type of route. • local(1): refers to a route for which the next hop is the final destination. • remote(2): refers to a route for which the next hop is not the final destination. This is not relevant for multicast and broadcast route entries.

FDMI HBAs

Field	Description
Sn	The serial number of this HBA.
Model	The model of this HBA.
ModelDescr	The model description.
OSInfo	The type and version of the operating system controlling this HBA.
MaxCTPayload	The maximum size of the Common Transport (CT) payload including all CT headers but no FC frame header(s), that may be send or received by application software resident in the host containing this HBA.

FDMI Ports

Field	Description
SupportedFC4Type	The supported FC-4 types attribute registered for this port on this VSAN.
SupportedSpeed	The supported speed registered for this port on this VSAN.
CurrentSpeed	The current speed registered for this port on this VSAN.
MaxFrameSize	The maximum frame size attribute registered for this port on this VSAN.
OsDevName	The OS Device Name attribute registered for this port on this VSAN.
HostName	The name of the host associated with this port.

FDMI Versions

Field	Description
Hardware	The hardware version of this HBA.
DriverVer	The version level of the driver software controlling this HBA.
OptROMVer	The version of the Option ROM or the BIOS of this HBA.
Firmware	The version of the firmware executed by this HBA.

Flow Statistics

Field	Description
Type	The matching criteria by which flows are selected to be included in the traffic which is instrumented by the ingress traffic counters.
VsanId	The id of VSAN.
DestId	The destination fibre channel address ID.
SrcId	The source fibre channel address ID.
Mask	The mask for source and destination fibre channel address ID.
Frames	The number of received frames for the flow created by the network manager.
Bytes	The number of received frame bytes for the flow created by the network manager.
CreationTime	The timestamp indicating the time the row was created or modified.

FCC

Field	Description
Enable	Enable Fabric Congestion Control
Priority	Specifies the priority level for the frames.
EdgeQuenchPktsRecd	The number of Edge Quench packets received and processed on this port.
EdgeQuenchPktsSent	The number of Edge Quench packets generated on this Port as result of congestion.
PathQuenchPktsRecd	The number of Path Quench packets received and processed on this port.
PathQuenchPktsSent	The number of Path Quench packets generated on this Port as result of congestion.
CurrentCongestionState	The current FCC congestion state of this Port indicating the severity of the congestion.
LastCongestedTime	When the congestion state of the Port changed to noCongestion from some other value. N/A if the congestion state of the Port has never transitioned to noCongestion since the last restart of the device.
LastCongestionStartTime	When the congestion state of the port changed from noCongestion to some other value.
IsRateLimitingApplied	If true, rate limiting is currently being applied on this port.

Diagnostics

Field	Description
Value	Displays the most recent measurement seen by the sensor.

Field	Description
Alarms High and Low	Represents the severity level of the SFP diagnostic information of an interface for temperature, voltage, current, optical transmit and receive power. It ranges from 1 to 6, with 6 being highest severity.
Warnings High and Low	

FSPF General

Field	Description
AdminStatus	The desired state of FSPF on this VSAN.
OperStatus	State of FSPF on this VSAN.
SetToDefault	Enabling this changes each value in this row to its default value. If all the configuration parameters have their default values and if the VSAN is suspended, then the row is deleted automatically.
RegionId	The autonomous region of the local switch on this VSAN.
DomainId	The Domain Id of the local switch on this VSAN.
SpfHoldTime	The minimum time between two consecutive SPF computations on this VSAN. The smaller value means that routing will react to the changes faster but the CPU usage is greater.
SpfDelay	The time between when FSPF receives topology updates and when it starts the Shortest Path First (SPF) computation on this VSAN. The smaller value means that routing will react to the changes faster but the CPU usage is greater.
MinLsArrival	The minimum time after accepting a Link State Record (LSR) on this VSAN before accepting another update of the same LSR on the same VSAN. An LSR update that is not accepted because of this time interval is discarded.
MinLsInterval	The minimum time after this switch sends an LSR on this VSAN before it will send another update of the same LSR on the same VSAN.
LsRefreshTime	The interval between transmission of refresh LSRs on this VSAN.
LSRMaxAge	The maximum age an LSR will be retained in the FSPF database on this VSAN. It is removed from the database after MaxAge is reached.
CreateTime	When this entry was last created.
CheckSum	The total checksum of all the LSRs on this VSAN.

FSPF Interfaces

Field	Description
SetToDefault	Enabling this changes each value in this row to its default value. If all the configuration parameters have their default values and if the interface is down, then the row is deleted automatically.

Field	Description
Cost	The administrative cost of sending a frame on this interface on this VSAN. The value 0 means that the cost has not been configured. Once the value has been configured, the value can not again be 0; so, obviously the value can not be set to 0. If the value is 0 and the corresponding interface is up, the agent sets a value calculated using the ifSpeed of the interface. Otherwise, the value is used as the cost. Note that following formula is used to calculate the link cost. Link Cost = { fspfIfCost if fspfIfCost > 0 {(1.0625e12 / Baud Rate) if fspfIfCost == 0 where Baud Rate is the ifSpeed of the interface.
AdminStatus	The desired state of FSPF on this interface on this VSAN.
HelloInterval	Interval between the periodic HELLO messages sent on this interface on this VSAN to verify the link health. Note that this value must be same on both the interfaces on each end of the link on this VSAN.
DeadInterval	Maximum time for which no HELLO messages can be received on this interface on this VSAN. After this time, the interface is assumed to be broken and removed from the database. Note that this value must be greater than the HELLO interval specified on this interface on this VSAN.
RetransmitInterval	Time after which an unacknowledged link update is retransmitted on this interface on this VSAN.
Neighbour State	The state of FSPF's neighbor state machine, which is the operational state of the interaction with the neighbor's interface which is connected to this interface.
Neighbour DomainId	The Domain ID of the neighbor on this VSAN.
Neighbour PortIndex	The index, as known by the neighbor, of the neighbor's interface which is connected to this interface on this VSAN.
CreateTime	When this entry was last created.

FSPF Interface Stats

Field	Description
CreateTime	When this entry was last created.
ErrorRxPkts	Number of invalid FSPF control frames received on this interface on this VSAN since the creation of the entry.
InactivityExpirations	Number of times the inactivity timer has expired on this interface on this VSAN since the creation of the entry.
LsuRxPkts	Number of Link State Update (LSU) frames received on this interface on this VSAN since the creation of the entry.
LsuTxPkts	Number of Link State Update (LSU) frames transmitted on this interface on this VSAN since the creation of the entry.

Field	Description
RetransmittedLsuTxPkts	Number of LSU frames retransmitted on this interface on this VSAN since the creation of the entry.
LsaRxPkts	Number of Link State Acknowledgement (LSA) frames received on this interface on this VSAN since the creation of the entry.
LsaTxPkts	Number of Link State Acknowledgement (LSA) frames transmitted on this interface on this VSAN since the creation of the entry.
HelloTxPkts	Number of HELLO frames transmitted on this interface on this VSAN since the creation of the entry.
HelloRxPkts	Number of HELLO frames received on this interface on this VSAN since the creation of the entry.

SDV Virtual Devices

Field	Description
Name	Represents the name of this virtual device.
Virtual Domain	The user preference for a persistent Domain ID for this virtual device to indicate a specific partition (domain) of the fabric that this virtual device should belong to.
Virtual FCID	The user preference for a persistent FCID for this virtual device.
Port WWN	The assigned PWWN for this virtual device. The agent assigns this value when the configuration is committed.
Node WWN	The assigned NWWN for this virtual device. The agent assigns this value when the configuration is committed.
Assigned FCID	The assigned FCID of this virtual device. The agent assigns this value when the configuration is committed and the real device that this virtual device virtualizes is on-line.
Real Device Map List	The set of real device(s) that this virtual device virtualizes in this VSAN.

SDV Real Devices

Field	Description
Type	The type of real device identifier represented by the value of the corresponding instance of cFcSdvVirtRealDeviceId that this virtual device virtualizes to.
Name	Represents a real device(s) identifier that this virtual device virtualizes.
Map Type	The mapping association type of the real device(s) (initiator/target).

LUN Discover

Field	Description
StartDiscovery	If Local, then only the directly attached SCSI target devices/ports and LUNs associated with them on all VSANs will be discovered. If Remote, then all SCSI target devices/ports and LUNs associated with them on all VSANs in the whole fabric, except the directly attached ones, will be discovered.
Type	Selecting targets results in only targets being discovered, without the NS results in both targets and LUNs being discovered.
OS	Specifies the operating system on which the LUNs need to be discovered.
Status	Indicates the outcome of the LUN discovery on the local switch. Contains the status of the most recent discovery. • inProgress(1) - indicates that the discovery is still in progress. • completed(2) - indicates that the discovery is complete. • failure(3) - indicates that the discovery encountered a failure.
CompleteTime	When the last discovery was completed. The value will be zero or N/A, if discovery has not been performed since the last system restart.

LUN Targets

Field	Description
VsanId	The VSAN to which this target belongs to.
Port WWN	The name of this authorized/discovered target device or port.
DevType	The device type of the SCSI target.
VendorId	The vendor Id of the SCSI target.
ProductId	The product Id of the SCSI target.
RevLevel	The product revision level of the SCSI target.
OtherInfo	The bytes from 0 to 7 in the INQUIRY command response data.

LUNs

Field	Description
Id	The number of this LUN.
Capacity (MB)	The capacity of this LUN.
SerialNum	The serial number of this LUN.
OS	The operating system for which this LUN was discovered.
FC ID	The Fibre Channel ID for this LUN.

Device Alias

Field	Description
Alias	The device alias of this entry. A device can have only one alias configured.
WWN	The Fibre Channel device which is given a device alias.

Device Alias Configuration

Field	Description
Device Alias	The device alias of this entry. A device can have only one alias configured.
WWN	The Fibre Channel device which is given a device alias.

Device Alias Mode

Field	Description
ConfigMode	Specifies the mode in which the device aliases can be configured. When it is set to basic, the device aliases operate in basic mode of operation. When basic mode is turned on, all MIBs which are using device aliases should internally convert them to their equivalent pWWNs and use the pWWNs. The mechanism to be followed for this conversion is implementation specific. When it is set to enhanced, the Device aliases operate in enhanced mode of operation. When enhanced mode is turned on, all MIBs which are using device aliases should use them as is without any conversion. Since the device aliases are used directly without any conversion, this is the native mode of operation of device aliases.

Device Alias Discrepancies

Field	Description
Discrepancy	Represents the checksum computed over the database represented by cfdaConfigTable and the cfdaConfigMode object. This object is used by a network manager to check if the above mentioned objects have changed on the local device. The method used to compute the checksum is implementation specific.

Name Server General

Field	Description
VSAN Id / FcId	The ID of the VSAN or FC.
Type	The port type of this port.
PortName	The fibre channel Port_Name (WWN) of this Nx_port.
NodeName	The fibre channel Node_Name (WWN) of this Nx_port.
FC4Type/Features	The FC-4 Features associated with this port and the FC-4 Type. Refer to FC-GS3 specification for the format.
FC4 Features	The FC-4 Features associated with this port.

Field	Description
ProcAssoc	The Fibre Channel initial process associator.
FabricPortName	The Fabric Port Name (WWN) of the Fx_port to which this Nx_port is attached.

Name Server Advanced

Field	Description
ClassOfSvc	The class of service indicator.
PortIpAddress	Contains the IP address of the associated port.
NodeIpAddress	The IP address of the node of this Nx_port, as indicated by the Nx_Port in a GS3 message that it transmitted.
SymbolicPortName	The user-defined name of this port.
SymbolicNodeName	The user-defined name of the node of this port.
HardAddress	Extended Link Service (FC-PH-2). Hard Address is the 24-bit NL_Port identifier which consists of - the 8-bit Domain Id in the most significant byte - the 8-bit Area Id in the next most significant byte - the 8-bit AL-PA(Arbitrated Loop Physical Address) which an NL_port attempts acquire during FC-AL initialization in the least significant byte. If the port is not an NL_Port, or if it is an NL_Port but does not have a hard address, then all bits are reported as 0s.
ProcAssoc	The Fibre Channel initial process associator (IPA).
PermanentPortName	The Permanent Port Name of this Nx port. If multiple port names are associated with this Nx port via FDISC (Discover F Port Service Parameters), the Permanent Port Name is the original port name associated with this Nx port at login.

Name Server Proxy

Field	Description
PortName	Name of the proxy port which can register/de-register for other ports on this VSAN. Users can enable third party registrations by setting this value.

Name Server Statistics

Field	Description
Queries Rx	The total number of Get Requests received by the local switch on this VSAN.
Queries Tx	The total number of Get Requests sent by the local switch on this VSAN.
Requests Rx Reg	The total number of Registration Requests received by the local switch on this VSAN.

Field	Description
Requests Rx DeReg	The total number of De-registration Requests received by the local switch on this VSAN.
RSCN Rx	The total number of RSCN commands received by the local switch on this VSAN.
RSCN Tx	The total number of RSCN commands sent by the local switch on this VSAN.
Rejects Tx	The total number of requests rejected by the local switch on this VSAN.

Preferred Path Maps and Routes

Field	Description
VSAN Id, Route Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map.
Map Active	Allows the activation/de-activation of all the routes within an FC route map. If true, then all the routes within this FC route map will be activated. If false, then all routes within this FC route map will be de-activated.
Route Strict Preference	Allows changes to the way the preferred path selection logic will select the preferred path. Setting it to true makes the preferred path to select the outgoing interface strictly based on the preference set using the cPrefPathRMapSetIntfPref. When it is set to false, then the preferred path selection logic only performs selection only when the current outgoing interface goes down.
Route Active	Allows the activation/de-activation of the route within an FC route map. If true, then the route will be activated. If false, then the route will be de-activated.
RouteActive	Allows the activation/de-activation of the route within an FC route map. If true, then the route will be activated. If false, then the route will be de-activated.

Preferred Path Maps Active

Field	Description
VSAN Id	The VSAN ID of this FC route map.
GlobalActive	Allows the activation/de-activation of all the routes within an FC route map.

Preferred Path All Match Criteria

Field	Description
VSAN Id, Route Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map.
Source FcId	The FC ID that needs to be matched with a source address in a frame for flow classification.

Field	Description
Source Information	Represents the mask associated with the source address.
Source Serial Number	Represents the source serial number.
Source Unit Type	The unit type of the source.
Source Tag	Unique identifier for the source address.
Dest FcId	The FC ID that needs to be matched with a destination address in a frame for flow classification.
Dest Information	Represents the mask associated with the destination address.
Dest Serial Number	Represents the destination serial number.
Dest Unit Type	The unit type of the destination.
Dest Tag	Unique identifier for the destination address.

Preferred Path Active Match Criteria

Field	Description
VSAN Id, Route Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map.
Source FcId	The FC ID that needs to be matched with a source address in a frame for flow classification.
Source Information	Represents the mask associated with the source address.
Source Serial Number	Represents the source serial number
Source Unit Type	The unit type of the source.
Source Tag	Unique identifier for the source address.
Dest FcId	The FC ID that needs to be matched with a destination address in a frame for flow classification.
Dest Information	Represents the mask associated with the destination address.
Dest Serial Number	Represents the destination serial number.
Dest Unit Type	The unit type of the source.
Dest Tag	Unique identifier for the destination address.

Preferred Path All Sets

Field	Description
VSAN Id, Route Id, Preference	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map. Preference level, which indicates the metric or cost of the preferred path. The lower the number the higher the preference.

Field	Description
Interface	Represents an interface on the local device on which the matched or classified frame will be forwarded.
IVR Nexthop VSAN	Represents the IVR next hop VSAN ID.

RSCN Nx Registrations

Field	Description
RegType	Indicates the type of registration desired by the subscriber. • 'fromFabricCtrlr' indicates RSCNs generated by the Fabric Controller. • 'fromNxPort' indicates RSCNs generated by Nx_Ports. • 'fromBoth' indicates RSCNs generated by Fabric Controller and Nx_Ports.

RSCN Multi-PID Support

Field	Description
Enable	Specifies whether the multi-pid option is enabled on this VSAN.

RSCN Event

Field	Description
TimeOut (msec)	The time (in seconds) before the RSCN event times out.

RSCN Statistics

Field	Description
SCR Rx	The number of SCRs received from Nx_Ports on this VSAN.
SCR RJT	The number of SCR rejected on this VSAN.
RSCN Rx	The number of RSCNs from Nx_Ports received on this VSAN.
RSCN Tx	The total number of RSCNs transmitted on this VSAN.
RSCN RJT	The number of RSCN requests rejected on this VSAN.
SW-RSCN Rx	The number of Inter-Switch Registered State Change Notifications (SW_RSCN) received on this VSAN from other switches.
SW-RSCN Tx	The number of Inter-Switch Registered State Change Notifications (SW_RSCN) transmitted on this VSAN to other switches.
SW-RSCN RJT	The number of SW_RSCN requests rejected on this VSAN.

Multicast Root

Field	Description
DomainId	The domain ID of the multicast root on this VSAN.
ConfigMode	The configured multicast root mode on this VSAN.
OperMode	The operational multicast root mode on this VSAN.

QoS Policy Maps

Field	Description
Name	The name of this classifier entry. The name should be unique.

QoS Class Maps

Field	Description
Name	The name of this filter entry. The name should be unique.
Match	Specifies how the filter should be applied. If true, then all the match statements associated with this filter must be satisfied in order for this filter match to be considered successful. If false, then even if any one of the criteria associated with this filter is satisfied, then the filter match is considered successful.

QoS Match Statements

Field	Description
SrcAddr	An FC address that needs to be matched with the source address in a FC frame.
DstAddr	An FC address that needs to be matched with the destination address in a FC frame.
Interface	An FC interface on the local device on which a frame should arrive in order to be classified by this filter. A value of zero indicates that no interface is configured.
WildCard	Specifies whether the wild-card option has been set. If true, then the wild-card option is set and all the FC traffic will be considered to match the corresponding multi-field classifier. If false, then the wild-card option is not set.

QoS Class Maps by Policy Maps

Field	Description
Class Map ID	Identifies a Fibre Channel filter.
Priority	Specifies priority value.

QoS Policy Maps by VSAN

Field	Description
VSAN Id, Direction	Specifies the direction of traffic flow on this VSAN.
Policy Map Id	Selects the first Differentiated Services Classifier Element to handle traffic on this VSAN.

QoS DWRR

Field	Description
Weight	The weight associated with this queue.

QoS Rate Limit

Field	Description
Percent	Specifies the rate-limit factor on this interface.

Timers and Policies

Field	Description
R_A_TOV	The Resource_Allocation_Timeout Value used for FxPorts as the timeout value for determining when to reuse an NxPort resource such as a Recovery_Qualifier.
D_S_TOV	The Distributed_Services_Timeout Value which indicates how long a distributed services requester will wait for a response.
E_D _TOV	The Error_Detect_Timeout Value used for FxPorts as the timeout value for detecting an error condition.
F_S_TOV	The Fabric_Stability_Timeout Value used to ensure that fabric stability has been achieved during fabric configuration.
Network Drop Latency	Network latency of this switch. This is the time interval after which the frames are dropped if they are not delivered in the order they were transmitted. Note that network latency is always greater than switch latency.
Switch Drop Latency	The switch latency of this switch. This is the time interval after which a switch drops the undelivered frames on a link which went down after delivering some frames to the next hop. This way the undelivered frames can be transmitted on a new link if there is one available.
InOrderDelivery	The InOrderDelivery guarantee flag of device. If true, then the InOrder Delivery is guaranteed. If false, it is not guaranteed.

Field	Description
TrunkProtocol	Enables or disables the trunking protocol for the device. The trunking protocol is used for negotiating trunk mode and calculating operational VSANs on an EISL link. It also performs port VSAN consistency checks. On non-trunking ISL links, if the port VSANs are different, the E ports will be isolated. To avoid this isolation, this should be set to disable.

WWN Manager

Field	Description
SwitchWWN	The World-Wide Name of this fabric element. It's a 64-bit identifier and is unique worldwide.
Type 1 WWNs	
Max	Maximum number of NAA Type 1 WWNs that are available for assignment to internal entities.
Available	Number of NAA Type 1 WWNs that are currently available for assignment to internal entities.
Reserved	Number of NAA Type 1 WWNs that are reserved for internal purposes.
Type 2 & 5 WWNs	
Max	Maximum number of total WWNs of types NAA Type 2 and Type 5 WWNs available for assignment to internal entities.
Available	Sum of number of NAA Type 2 and Type 5 WWNs currently available for assignment to the internal entities.
Reserved	Number of total WWNs of types NAA Type 2 and Type 5 WWNs reserved for internal purposes.
Enable Secondary when more WWWNs needed	
BaseMacAddress	The first MAC address used for generating World Wide Names (WWNs) when the default range of WWNs generated from supervisor MAC address are exhausted.
MacAddressRange	The number of secondary MAC Addresses starting from and including the wwnmSecondayBaseMacAddress.

NPV Traffic Map

Field	Description
Switch	Name of the switch
Server Interface	Name of the server interface.
External Interface List	The list of interfaces to which the traffic needs to be mapped to.

NPV Load Balance

Field	Description
Switch	Name of the switch.
Enable	Enable or disable displaying NPV related per server interface information

NPV External Interface Usage

Field	Description
Switch	Name of the switch
Server Interface	Interface on the NPV Device that connects to end devices such as hosts or disks. It is also known as F-port, as it operates in F port mode.
External Interface In Use	Interface on the NPV Device that connects to the NPV Core Switch. It is also known as NP-port as it operates in NP port mode.

NP Link

Field	Description
NPIV (core)	Name of the NPIV core switch.
F port	The F port that is connected to the NPIV core switch
NPV	Name of the NPV switch
Speed	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of `n' then the speed of the interface is between `n-500,000' to `n+499,999'.
Rx Util%	Received traffic Utilization %, total number of octets received on the interface over the speed configured on the interface, including framing characters
Rx Bytes	The total number of octets received on the interface, including framing characters
Tx Util%	Recetransmittedived traffic Utilization %, total number of octets transmitted ou of the interface over the speed configured on the interface, including framing characters.
Tx Bytes	The total number of octets transmitted out of the interface, including framing characters.

FCoE

Config

Field	Description
FC Map	The FCoE Mac Address Prefix used to associate the FCoE Node (ENode).
Default FCF Priority	The default FCoE Initialization Protocol (FIP) priority value advertised by the Fibre Channel Forwarder (FCF) to ENodes.

Field	Description
FKA Adv. Period (sec)	The time interval at which FIP Keep Alive (FKA) messages are transmitted to the MAC address of the ENode.

VSAN-VLAN Mapping



Note This table applies only to N5k switches running version 4.0(1a) and greater.

Field	Description
VSAN Id	The ID of the VSAN.
VLAN Id	The ID of the VLAN.
Oper State	Shows the operational state of this VLAN-VSAN association entry.

VLAN-VSAN Mapping

Field	Description
VSAN Id	The ID of the VSAN.
VLAN Id	The ID of the VLAN.
Oper State	Shows the operational state of this VLAN-VSAN association entry.

FCoE Statistics

Field	Description
Alignment Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
FCS Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Multiple Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collisions.
SQE Test Errors	The number of times the PLS sublayer generated the SQE TEST ERROR message for a particular interface.
Deferred Transmissions	The count of the number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.

Field	Description
Late Collisions	The number of times that a collision is detected on a particular interface later than one slot time into the transmission of a packet.
Excessive Collisions	The count of the number of frames for which transmission on a particular interface failes because of excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal Mac Transmit Errors	The count of the number of frames for which transmission on a particular interface fails because of an internal MAC sublayer transmit error.
Carrier Sense Errors	The number of times that a carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Longs	The count of number of frames received on a particular interface that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The count of number of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error.
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present

Ficon

FICON VSANs

Field	Description
VSAN ID	Uniquely identifies a VSAN within a fabric.
Host Can Offline SW	If true, it allows the host to put the system offline.
Host Can Sync Time	If true, the host can set the system time.
Port Control by Host	If true, the host is allowed to alter FICON Director connectivity parameters.
Port Control by SNMP	If true, SNMP manager is allowed to alter FICON director connectivity parameters.
CUP Name	The name of the Control Unit Device.
CUP Enable	Indicates whether the Control Unit Device is enabled.
Domain ID	Specifies the domain ID of the switch.
CodePage	The Code Page used in this VSAN.
Character Set	Character set for the code page used in this VSAN.
Active=Saved	If true, the active to saved mode is enabled. All changes will be saved to NVRAM.
User Alert Mode	If true, FICON management stations will prompt on changes.

Field	Description
Device Allegiance	If CUP is in allegiance state with a channel, it cannot accept any commands from any logical paths. A CUP goes in an allegiance state when it accepts command from a channel and forms 'an allegiance' with it until the successful completion of the channel program, at which point the CUP goes in a an 'unlocked' mode.
VSAN Time	The system time in the VSAN. This could be set either by the host or be the default global time in the FICON Director. The default global time is the local time in the FICON Director.
VSAN State	Controls the state of the ports belonging to a VSAN in the context of the FICON functionality.
VSAN Serial Number	The serial number of the FICON director for this VSAN.

FICON VSANs Files

Field	Description
Description	Configuration file description.
CUP Name	The name of the Control Unit Device.
Status	Locked indicates no change allowed. Unlocked indicates change allowed.
LastAccessed	The time this file was last accessed.
UserAlertMode	If true, director user alert mode is enabled.

Global

Field	Description
Default Port Prohibited	Check this option to block the default port.

FICON Port Attributes

Field	Description
TypeNumber	The type number for this FICON Director.
SerialNumber	The sequence number assigned to this FICON Director during manufacturing.
Tag	This is the identifier of the peer port. • If the peer port's unit type is channel, then PortId will be the CHPID (Channel Path Identifier) of the channel path that contains this peer port. • If the peer port is controlUnit, then PortId will be 0. • If the peer port is fabric, then PortId will be port address of the interface on the peer switch.

Field	Description
FcId	The fabric Id of the other side port (initiator /target). This will be filled only in the case of Fabric ports.
Status	'valid' - if this information is current. 'old' - if this information is cached. Click Clear Old Attributes to clear the cache.
Name	The FICON port name.
Manufacturer	The name of the company that manufactured this FICON Director.
ModelNumber	The model number for this FICON Director.
PlantOfMfg	The plant code that identifies the plant of manufacture of this FICON Director.
UnitType	The peer type of the port that this port is communicating. ==Channel - host ==Control Unit - disk == Fabric - ISL
Alert	Displays one of the following: • bitErrThreshExceeded, • lossOfSignalOrSync, • nosReceived, • primitiveSeqTimeOut, • invalidPrimitiveSeq Click Clear to acknowledge and clear this alert.

FICON Port Configuration

Field	Description
Show Installed Ports Only	If true, only physically available ports will be listed in the table.
ESCON Style	ESCON Style Port Configuration display is the Port Configuration table in DM displaying the ESCON Style Ports. In the table, A represents the available ports and P represents the prohibited ports.
Port/ Prohibit	Enter the FICON address of the port and the prohibited list. (This is an alternative to the table grid.)
Name	The port name of this port.
Block	If true, this port will be isolated.
Prohibit Grid	Click on the grid to add or remove the ability of ports to communicate with each other.

FICON Port Numbers

Field	Description
Module	The number of the module in the chassis.

Field	Description
Reserved Port Numbers (Physical)	The reserved port numbers for the module.
NumPorts	The number of ports reserved for that module.
Module Name	The name of the module.
Reserved Port Numbers (Logical)	Chassis slot port numbers. Reserved port numbers for one chassis slot. There can be up to 64 port numbers reserved for each slot in the chassis.

FICON VSANs Director History

To view the latest FICON information, you must click the Refresh button.

Field	Description
KeyCounter	The key counter.
Ports Address Changed	The list of ports that have configuration change for a value of KeyCounter.

Fabric Binding Actions

Field	Description
VSANId	Specifies the unique identifier for a VSAN within a fabric.
Activate	• activate - results in the valid fabric bindings on this VSAN/VLAN being activated. • force activate - results in forced activation, even if there are errors during activation and the activated fabric bindings will be copied to the active database. • deactivate - results in deactivation of currently activated valid fabric bindings (if any), on this VSAN/VLAN. Currently active entries (if any), which would have been present in the active database, will be removed. • no-selection -
Enabled	The state of activation on this VSAN/VLAN. If true, then an activation has been attempted as the most recent operation on this VSAN/VLAN. If false, then an activation has not been attempted as the most recent operation on this VSAN/VLAN.
Result	Indicates the outcome of the most recent activation/deactivation.
LastChange	When the valid fabric bindings on this VSAN/VLAN were last activated. If the last activation took place prior to the last re-initialization of the agent, then this value will be N/A.
CopyActToConfig	If enabled, results in the active fabric binding database to be copied on to the configuration database on this VSAN/VLAN. Note that the learned entries are also copied.

Fabric Binding Config Database

Field	Description
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.
Peer WWN (Name)	Specifies the switch WWN of a switch that can be part of the fabric.
DomainId	Specifies an insistent domain ID.

Fabric Binding Active Database

Field	Description
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.
Peer WWN	Specifies the switch WWN of a switch that can be part of the fabric.
DomainId	Specifies the insistent domain ID of the switch represented by the corresponding instance of the WWN of a switch.

Fabric Binding Database Differences

Field	Description
VSAN	From the drop down list, select the number VSANs to be compared.
Compare With	Choose the database for comparison: • Active - compares the fabric bind active database with respect to configuration database on this VSAN/VLAN. So, the configuration database will be the reference database and the results of the difference operation will be with respect to the configuration database. • Config - compares the fabric bind configuration database with respect to active database on this VSAN/VLAN. So, the active database will be the reference database and the results of the difference operation will be with respect to the active database.
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.
Peer WWN	Specifies the device WWN of a device that can be part of the fabric.
DomainId	Specifies the insistent domain ID of the switch represented by the corresponding instance of the WWN of a switch.
Reason	Indicates the reason for the difference between the databases being compared, for this entry.

Fabric Binding Violations

Field	Description
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.

Field	Description
Peer WWN	The sWWN (switch WWN) of the device that was denied entry into the fabric on one of the local device's ports.
DomainId	The domain ID of the device that was denied entry into the fabric on one of the local device's ports. A value of zero indicates that the switch WWN of the device was not present in the enforced fabric bindings.
DenialTime	When the denial took place.
DenialCount	The number of times this switch has been denied entry into the fabric on one of the local device's ports.
DenialReason	The reason for which the device was denied entry into the fabric on one of the local device's ports.

Fabric Binding Statistics

Field	Description
AllowedReqs	The number of requests from switches to become part of the fabric that have been allowed on this VSAN/VLAN.
DeniedReqs	The number of requests from switches to become part of the fabric that have been denied on this VSAN/VLAN.
Clear	When set to clear, it results in fabric bind statistic counters being cleared on this VSAN/VLAN.

Fabric Binding EFMD Statistics

Field	Description
TxMergeReqs	The number of EFMD Merge Requests transmitted on this VSAN by the local device.
RxMergeReqs	The number of EFMD Merge Requests received on this VSAN by the local device.
TxMergeAccs	The number of EFMD Merge accepts transmitted on this VSAN by the local device.
RxMergeAccs	The number of EFMD Merge accepts received on this VSAN by the local device.
TxMergeRejs	The number of EFMD Merge rejects transmitted on this VSAN by the local device.
RxMergeRejs	The number of EFMD Merge rejects received on this VSAN by the local device.
TxMergeBusys	The number of EFMD Merge Busys transmitted on this VSAN by the local device.
RxMergeBusys	The number of EFMD Merge Busys received on this VSAN by the local device.

Field	Description
TxMergeErrs	The number of EFMD Merge Errors transmitted on this VSAN by the local device.
RxMergeErrs	The number of EFMD Merge Errors received on this VSAN by the local device

IP Storage

FCIP Profiles

Field	Description
IP Address	The Internet address for this entity.
Port	A TCP port other than the FCIP well-known port on which the FCIP entity listens for new TCP connection requests.
SACK	Whether the TCP Selective Acknowledgement Option is enabled to allow the receiver end to acknowledge multiple lost frames in a single ACK, enabling faster recovery.
KeepAlive (s)	The TCP keep alive timeout for all links within this entity.
ReTrans MinTimeout (ms)	The TCP minimum retransmit timeout for all the links on this entity.
ReTrans Max	The Maximum number of times that the same item of data will be retransmitted over a TCP connection. If delivery is not acknowledged after this number of retransmissions then the connection is terminated.
Send BufSize (KB)	The aggregate TCP send window for all TCP connections on all Links within this entity. This value is used for Egress Flow Control. When the aggregate of the data queued on all connections within this entity reaches this value, the sender is flow controlled.
Bandwidth Max (Kb)	This is an estimate of the Bandwidth of the network pipe used for the B-D product computation, which lets us derive the TCP receive window to advertise.
Bandwidth Min (Kb)	The minimum available bandwidth for the TCP connections on the Links within this entity.
Est Round Trip Time (us)	This is an estimate of the round trip delay of the network pipe used for the B-D product computation, which lets us derive the TCP receive window to advertise.
PMTU Enable	The path MTU discovery.
PMTU ResetTimeout (sec)	The time interval for which the discovered pathMTU is valid, before MSS reverts back to the negotiated TCP value.
CWM Enable	If true, congestion window monitoring is enabled.
CWM BurstSize (KB)	The maximum burst sent after a TCP sender idle period.
Max Jitter	The maximum delay variation (not due to congestion) that can be experienced by TCP connections on this interface.

FCIP Tunnels

Field	Description
Interface	This identifies the interface on this FCIP device to which this link pertains.
Attached	The interface on which this FCIP link was initiated.
B Port Enable	If true, the B port mode is enabled on the local FCIP link.
B Port KeepAlive	If true, a message is sent in response to a (Fibre Channel) ELS Echo frame received from the peer. Some B Port implementations use ELS Echo request/response frames as Link Keep Alive.
Remote IP Address	The Internet address for the remote FCIP entity.
Remote TCP Port	The remote TCP port to which the local FCIP entity will connect if and when it initiates a TCP connection setup for this link.
Spc Frames Enable	If true, the TCP active opener initiates FCIP special frames and the TCP passive opener responds to the FCIP special frames. If it is set to false, the FCIP special frames are neither generated nor responded to.
Spc Frames RemoteWWN	The World Wide Name of the remote FC Fabric Entity. If this is a zero length string then this link would accept connections from any remote entity. If a WWN is specified then this link would accept connections from a remote entity with this WWN.
Spc Frames Remote Profile Id	The remote FCIP entity's identifier.

FCIP Tunnels (Advanced)

Field	Description
Interface	The interface on which this FCIP link was initiated.
Timestamp Enable	If true, the timestamp in FCIP header is to checked.
Timestamp Tolerance	The accepted time difference between the local time and the timestamp value received in the FCIP header. By default this value will be EDTOV/2. EDTOV is the Error_Detect_Timeout Value used for Fibre channel Ports as the timeout value for detecting an error condition.
Number Connections	The maximum number of TCP connections allowed on this link.
Passive	If false, this link endpoint actively tries to connect to the peer. If true, the link endpoint waits for the peer to connect to it.
QoS Control	The value to be set for the ToS field in IP header for the TCP control connection.
QoS Data	The value to be set for the ToS field in IP header for the TCP Data connection.
IP Compression	What algorithm is used, if any.
Write Accelerator	The Write accelerator allows for enhancing SCSI write performance.
Tape Accelerator	If true, the tape accelerator (which allows for enhancing Tape write performance) is enabled.

Field	Description
Tape Accelerator Oper	Write Acceleration is enabled for the FCIP link.
TapeRead Accelerator Oper	Enabled automatically when the Tape Accelerator Oper is active.
FlowCtrlBufSize Tape (KB)	The size of the flow control buffer (64K to 32MB). If set to 0, flow control buffer size is calculated automatically by the switch.
IPSec	Indicates whether the IP Security has been turned on or off on this link.
XRC Emulator	Check to enable XRC Emulator. It is disabled by default.
XRC Emulator Oper	Indicates the operational status of XRC Emulator.

FCIP Tunnels (FICON TA)

Field	Description
Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
VSAN List Admin	The list of VSANs for which FICON Tape Acceleration is configured.
VSAN List Oper	The list of VSANs for which FICON Tape Acceleration is operationally on.

FCIP Tunnels Statistics

Field	Description
Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
Rx IPCompRatio	The IP compression ratio for received packets on the FCIP device. The value of this object will be presented as a floating point number with two digits after the decimal point.
Tx IPCompRatio	The IP compression ratio for transmitted packets on the FCIP device. The value of this object will be presented as a floating point number with two digits after the decimal point.

FCIP XRC Statistics

Field	Description
ProfileId	Unique ID of the profile.
Interface	Name of the interface.
RRSAccelerated	The number of read record set IUs accelerated.
RRSForwarded	Number of read record set IUs forwarded.
BusyStatus	Number of instances of busy status received from the control unit.
UnitCheckStatus	Number of instances of unit check status received from the control unit.

Field	Description
cfmFcipLinkExtXRCEStatsSelReset	Number of selective resets processed.
BufferAllocErrors	Number of buffer allocation errors.

iSCSI Connection

Field	Description
LocalAddr	The local Internet Network Address used by this connection.
RemoteAddr	The remote Internet Network Address used by this connection.
CID	The iSCSI Connection ID for this connection.
State	The current state of this connection, from an iSCSI negotiation point of view. • login - The transport protocol connection has been established, but a valid iSCSI login response with the final bit set has not been sent or received. • full - A valid iSCSI login response with the final bit set has been sent or received. • logout - A valid iSCSI logout command has been sent or received, but the transport protocol connection has not yet been closed.
MaxRecvDSLen	The maximum data payload size supported for command or data PDUs in use within this connection. Note that the size of reported in bytes even though the negotiation is in 512k blocks.
SendMarker	Indicates whether or not this connection is inserting markers in its outgoing data stream.
HeaderDigest	The iSCSI header digest scheme in use within this connection.
DataDigest	The iSCSI data digest scheme in use within this connection.

iSCSI Initiators

Field	Description
Name or IP Address	A character string that is a globally unique identifier for the node represented by this entry.
VSAN Membership	The list of configured VSANs the node represented by this entry can access.
Dynamic	If true, then the node represented by this entry is automatically discovered.
Initiator Type	Indicates whether the node is a host that participates in iSCSI load-balancing.
Persistent Node WWN	If true, then the same FC address is assigned to the node if it were to be represented again in the FC domain with the same node name. Note that the node FC address is either automatically assigned or manually configured.
SystemAssigned Node WWNN	If true, the FC address is automatically assigned to this node. If false, then the FC address has to be configured manually.

Field	Description
Node WWN	The persistent FC address of the node.
Persistent Port WWN	If true, then the same FC address is assigned to the ports of the node if it were to be represented again in the FC domain with the same node name.
Port WWN	All the FC port addresses associated with this node.
AuthUser	This is the only CHAP user name that the initiator is allowed to log in with.
Target UserName	(Optional) The user name to be used for login. If you do not supply a username, the global user name is used.
Target Password	(Optional) The password to be used for login. If you do not supply a password, the global password is used.
Load Metric	A configured load metric of this iSCSI initiator for the purpose of iSCSI load balancing.
Auto Zone Name	The zone name that is used when the system creates automatic zone for this initiator's specific list of targets.

iSCSI Session Initiators

Field	Description
Name or IP Address	The name or IP address of the initiator port.
Alias	The initiator alias acquired at login.

Module Control

Field	Description
Module Id	ID of the module.
Admin Status	Enables or disables the iSCSI feature for the module.
OperStatus	Shows whether the iSCSI interface is enabled or disabled for the module.

iSCSI Global

Field	Description
AuthMethod	The authentication method.
InitiatorIdleTimeout	The time for which the gateway (representing a FC target) waits from the time of last iSCSI session to a iSCSI initiator went down, before purging the information about that iSCSI initiator.
iSLB ZonesetActivate	Checking this option performs automatic zoning associated with the initiator targets

Field	Description
DynamicInitiator	This field determines how dynamic iSCSI initiators are created. Selecting the iSCSI option (default) creates dynamic iSCSI initiators. If you select iSLB then the an iSLB dynamic initiator is created. Selecting the deny option does not allow dynamic creation of the initiators.
Target UserName	The default user name used for login. If an initiator user name is specified, that user name is used instead.
Target Password	The default password used for login. If an initiator password is specified, that password is used instead.

iSCSI Session Statistics

Field	Description
PDU Command	The count of Command PDUs transferred on this session.
PDU Response	The count of Response PDUs transferred on this session.
Data Tx	The count of data bytes that were transmitted by the local iSCSI node on this session.
Data Rx	The count of data bytes that were received by the local iSCSI node on this session.
Errors Digest	Authentication errors.
Errors CxnTimeout	Connection timeouts.

iSCSI Targets

Field	Description
Dynamically Import FC Targets	Check this option to dynamically import FC targets into the iSCSI domain. A target is not imported if it already exists in the iSCSI domain.
iSCSI Name	The iSCSI name of the node represented by this entry.
Dynamic	Indicates if the node represented by this entry was either automatically discovered or configured manually.
Primary Port WWN	The FC address for this target.
Secondary Port WWN	The optional secondary FC address for this target. This is the FC address used if the primary cannot be reached.
LUN Map iSCSI	The configured default Logical Unit Number of this LU.
LUN Map FC Primary	The Logical Unit Number of the remote LU for the primary port address.
LUN Map FC Secondary	The Logical Unit Number of the remote LU for the secondary port address.
Initiator Access All	If true, then all the initiators can access this target even those which are not in the initiator permit list of this target. If false, then only initiators which are in the permit list are allowed access to this target.

Field	Description
Initiator Access List	Lists all the iSCSI nodes that are permitted to access the node represented by this entry. If AllAllowed is false and the value of List is empty, then no initiators are allowed to access this target.
Advertised Interfaces	Lists all the interfaces on which the target could be advertised.
Trespass Mode	The trespass mode for this node. Every iSCSI target represents one or more port(s) on the FC target. If true, the node instructs the FC node to present all LUN I/O requests to secondary port if the primary port is down.
RevertToPrimaryPort	Indicates if it is required to revert back to primary port if the FC target comes back online.

iSCSI iSLB VRRP

Field	Description
VrId, IpVersion	The virtual router number and the IP version (IPv4, IPv6, or DNS).
Load Balance	Indicates whether load balancing is enabled.

iSCSI Initiator Access

Field	Description
Initiator Name	The iSCSI node name.

Initiator Specific Target

Field	Description
Name	A globally unique identifier for the node.
Port WWN(s) Primary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
Port WWN(s) Secondary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
LUN Map (Hex) iSCSI	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
LUN Map (Hex) FC Primary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
LUN Map (Hex) FC Secondary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
No AutoZone Creation	Indicates if a FibreChannel zone is automatically created for this iSCSI initiator-target and the iSCSI initiator. If true the zone is not automatically created. If false (default) the zone is automatically created.

Field	Description
Trespass Mode	The trespass mode for this node. If true the FC node instance presents all LUN I/O requests to the secondary port (fcSecondaryAddress) if the primary port (fcAddress) is down.
Revert to Primary Port	The revert to primary mode for this node. If true the FC node instance presents all LUN I/O requests to the primary port fcAddress) when the primary port comes back online.
Primary PWWN VSAN	Indicates the VSAN into which the auto zone is placed for this initiator target. If this object is not set then the VSAN is determined by querying the name server.
Secondary PWWN VSAN	Indicates the VSAN into which the auto zone is placed for this initiator target. If this object is not set then the VSAN is determined by querying the name server.

iSCSI Initiator PWWN

Field	Description
Port WWN	The FC address for this entry.

iSCSI Sessions

Field	Description
Type	Type of iSCSI session: • normal - session is a normal iSCSI session • discovery - session is being used only for discovery.
TargetName	If Direction is Outbound, this will contain the name of the remote target.
Vsan ID	The VSAN to which this session belongs to.
ISID	The initiator-defined portion of the iSCSI Session ID.
TSIH	The target-defined identification handle for this session.

iSCSI Sessions Detail

Field	Description
ConnectionNumber	The number of transport protocol connections that currently belong to this session.
ImmediateData	Whether the initiator and target have agreed to support immediate data on this session.
Initial	If true, the initiator must wait for a Ready-To-Transfer before sending to the target. If false, the initiator may send data immediately, within limits set by FirstBurstSize and the expected data transfer length of the request.

Field	Description
MaxOutstanding	The maximum number of outstanding Ready-To-Transfers per task within this session.
First	The maximum length supported for unsolicited data sent within this session.
Max	The maximum number of bytes which can be sent within a single sequence of Data-In or Data-Out PDUs.
Sequence	If false, indicates that iSCSI data PDU sequences may be transferred in any order. If true indicates that data PDU sequences must be transferred using continuously increasing offsets, except during error recovery.
PDU	If false, iSCSI data PDUs within sequences may be in any order. If true indicates that data PDUs within sequences must be at continuously increasing addresses, with no gaps or overlay between PDUs.

IP Services

IP Routes

Field	Description
Routing Enabled	When this check box is enabled, the switch is acting as in IP router.
Destination, Mask, Gateway	The value that identifies the local interface through which the next hop of this route should be reached.
Metric	The primary routing metric for this route.
Interface	The local interface through which the next hop of this route should be reached.
Active	Indicates whether the route is active.

IP Statistics ICMP

Field	Description
InParmProbs	The number of ICMP Parameter Problem messages received.
OutParmProbs	The number of ICMP Parameter Problem messages sent.
InSrcQuenchs	The number of ICMP Source Quench messages received.
InRedirects	The number of ICMP Redirect messages received.
InEchos	The number of ICMP Echo (request) messages received.
InEchoReps	The number of ICMP Echo Reply messages received.
InTimestamps	The number of ICMP Timestamp (request) messages received.
InTimestampReps	The number of ICMP Timestamp Reply messages received.
InAddrMasks	The number of ICMP Address Mask Request messages receiv
InAddrMaskReps	The number of ICMP Address Mask Reply messages received

Field	Description
InDestUnreachs	The number of ICMP Destination Unreachable messages received
InTimeExcds	The number of ICMP Time Exceeded messages received.
OutSrcQuenchs	The number of ICMP Source Quench messages sent.
OutRedirects	The number of ICMP Redirect messages sent. For a host, this value since hosts do not send redirects.
OutEchos	The number of ICMP Echo (request) messages sent.
OutEchoReps	The number of ICMP Echo Reply messages sent.
OutTimestamps	The number of ICMP Timestamp (request) messages sent.
OutTimestampReps	The number of ICMP Timestamp Reply messages sent.
OutAddrMasks	The number of ICMP Address Mask Request messages sent.
OutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.
OutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
OutTimeExcds	The number of ICMP Time Exceeded messages sent.

IP Statistics IP

Field	Description
InHdrErrors	The number of input data grams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
InAddrErrors	The number of input data grams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. For entities which are not IP routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
InUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP data grams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such frames met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any frames counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default routers are down.
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.

Field	Description
ReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The total number of IP datagrams which local IP user- protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any data grams counted in ipForwDatagrams.
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP routers, this counter will include only those frames which were Source-Routed via this entity, and the Source-Route option processing was successful.
FragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully re-assembled.

IP Statistics SNMP

Field	Description
BadVersions	The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
BadCommunityNames	The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
BadCommunityUses	The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
ASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
TooBigs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.

Field	Description
SilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
ProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned.
NoSuchNames	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
BadValues	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
ReadOnlys	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value readOnly in the error-status field, as such this is provided as a means of detecting incorrect implementations of the SNMP.
GenErrs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
Pkts	The total number of messages delivered to the SNMP entity from the transport service.
GetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
GetNexts	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.
SetRequests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.
OutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.
OutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.
OutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
TotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
TotalSetVars	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

IP Statistics UDP

Field	Description
InErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
InDatagrams	The total number of UDP datagrams delivered to UDP users.
OutDatagrams	The total number of UDP datagrams sent from this entity.
NoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

mgmt0 Statistics

Field	Description
InErrors	Total number of received errors on the interface.
OutErrors	Total number of transmitted errors on the interface.
InDiscards	Total number of received discards on the interface.
OutDiscards	Total number of transmitted discards on the interface.
TotalRxBytes	Total number of bytes received.
TxBytes	Total number of bytes transmitted.
RxFrames	Total number of frames received.
TxFrames	Total number of frames transmitted.

TCP UDP TCP

Field	Description
State	The state of this TCP connection.

TCP UDP UDP

Field	Description
Port	The local port number for this UDP listener.

VRRP General

Field	Description
IP Address Type, VrId, Interface	The IP address type (IPv4, IPv6, or DNS), the virtual router ID, and the interface.
Admin	The admin state of the virtual router (active or notInService).

Field	Description
Oper	The current state of the virtual router. There are three defined values: • `initialize', which indicates that all the virtual router is waiting for a startup event. • `backup', which indicates the virtual router is monitoring the availability of the master router. • master', which indicates that the virtual router is forwarding frames for IP addresses that are associated with this router.
Priority	Specifies the priority to be used for the virtual router master election process. Higher values imply higher priority. A priority of '0' is sent by the master router to indicate that this router has ceased to participate in VRRP and a backup virtual router should transition to become a new master. A priority of 255 is used for the router that owns the associated IP address(es).
AdvInterval	The time interval, in seconds, between sending advertisement messages. Only the master router sends VRRP advertisements.
PreemptMode	Controls whether a higher priority virtual router will preempt a lower priority master.
UpTime	When this virtual router transitioned out of `initialized'.
Version	The VRRP version on which this VRRP instance is running.
AcceptMode	Controls whether a virtual router in Master state will accept packets addressed to the address owner's IPv6 address as its own if it is not the IPv6 address owner. If true, the virtual router in Master state will accept. If false, the virtual router in Master state will not accept.

VRRP IP Addresses

Field	Description
Interface, VRRP ID, IP Address	Interface, Virtual Router Redundancy Protocol ID, and associated IP address

VRRP Statistics

Field	Description
IP Address Type, VrId, Interface	The IP address type (IPv4, IPv6, or DNS), the virtual router ID, and the interface.
LastAdvRx	The total number of VRRP advertisements received by this virtual router.
Protocol Traffic MasterIpAddr	The master router's real (primary) IP address. This is the IP address listed as the source in VRRP advertisement last received by this virtual router.
Protocol Traffic BecomeMaster	The total number of times that this virtual router's state has transitioned to MASTER.

Field	Description
Priority 0 Rx	The total number of VRRP frames received by the virtual router with a priority of '0'.
Priority 0Tx	The total number of VRRP frames sent by the virtual router with a priority of '0'.
AuthErrors InvalidType	The total number of frames received with an unknown authentication type.
Other Errors dvIntervalErrors	The total number of VRRP advertisement frames received for which the advertisement interval is different than the one configured for the local virtual router.
Other Errors IpTtlErrors	The total number of VRRP frames received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
Other Errors InvalidTypePktsRcvd	The number of VRRP frames received by the virtual router with an invalid value in the type field.
Other Errors AddressListErrors	The total number of frames received for which the address list does not match the locally configured list for the virtual router.
OtherErrors PacketLengthErrs	The total number of frames received with a frame length less than the length of the VRRP header.
RefreshRate	The interval of time between refreshes.

CDP General

Field	Description
Enable	Whether the Cisco Discovery Protocol is currently running. Entries in CacheTable are deleted when CDP is disabled.
MessageInterval sec	The interval at which CDP messages are to be generated. The default value is 60 seconds.
HoldTime sec	The time for the receiving device holds CDP message. The default value is 180 seconds.
LastChange	When the cache table was last changed.
Supported DeviceId Format	Indicates the Device-ID format capability of the device.
DeviceId Format	An indication of the format of Device-ID contained in the corresponding instance of the supported device.

CDP Neighbors

Field	Description
Switch	The Internet address for this entity.
Local Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.

Field	Description
DeviceName	The remote device's name. By convention, it is the device's fully qualified domain name.
DeviceID	The device ID string as reported in the most recent CDP message.
DevicePlatform	The version string as reported in the most recent CDP message.
Interface	The port ID string as reported in the most recent CDP message.
IPAddress	The (first) network-layer address of the device's SNMP-agent as reported in the address TLV of the most recently received CDP message.
NativeVLAN	The remote device's interface's native VLAN, as reported in the most recent CDP message. The value 0 indicates no native VLAN field (TLV) was reported in the most recent CDP message.
PrimaryMgmtAddr	Indicates the (first) network layer address at which the device will accept SNMP messages as reported in the most recently received CDP message.
SecondaryMgmtAddr	Indicates the alternate network layer address at which the device will accept SNMP messages as reported in the most recently received CDP message.

iSNS Profiles

Field	Description
Addr	The address of the iSNS server.
Port	The TCP port of the iSNS server.

iSNS Servers

Field	Description
Name	The name of the iSNS Server.
TcpPort	The TCP port used for iSNS messages. If TCP is not supported by this server, the value is 0.
Uptime	The time the server has been active.
ESI Non Response Threshold	The number of ESI messages that will be sent without receiving a response before an entity is de-registered from the iSNS database.
# Entities	The number of entities registered in iSNS on the server.
# Portals	The number of portals registered in iSNS on the server.
# Portal Groups	The number of portal groups registered in iSNS on the server.
# iSCSI Devices	The number of iSCSI Nodes registered in iSNS on the server.

iSNS Entities

Field	Description
Entity ID	The iSNS entity identifier for the entity.
Last Accessed	The time the entity was last accessed.

iSNS Cloud Discovery

Field	Description
AutoDiscovery	Whether automatic cloud discovery is turned on or off.
DiscoveryDelay	Time duration between successive IP cloud discovery runs.
Discovery	The IP network discovery command to be executed. • all - Run IP network discovery for all the gigabit ethernet interfaces in the fabric. • noOp (default) - no operation is performed.
CommandStatus	The status of the license install / uninstall / update operation. • success - discovery operation completed successfully • nProgress - discovery operation is in progress • none - no discovery operation is performed • NoIpNetworkNameSpecified - ipCloud name not specified • invalidNetworkName - ipCloud is not configured • NoIPSPortNameSpecified - gigE port ifindex not specified • invalidIPSPortName - invalid gigE port interface • generalISNSFailure - General ISNS Server Failure

iSNS Clouds

Field	Description
Id	The ID of the IP cloud.
Switch WWN	The WWN of the switch in this table.

iSNS Cloud Interfaces

Field	Description
Name, Switch WWN, Interface, Address	The name, Switch WWN, interface, and address of the cloud.

Monitor Dialog Controls

Field	Description
Line Chart	Opens a new window with a line chart representation of the data.

Field	Description
Area Chart	Opens a new window with an area chart representation of the data.
Bar Chart	Opens a new window with a bar chart representation of the data.
Pie Chart	Opens a new window with a pie chart representation of the data.
Reset Cumulative Counters	Resets the counters to 0 if the Column Data display mode is set to Cumulative.
Export to File	Opens a standard Save dialog box. The data is saved as a.TXT file.
Print	Opens a standard Print dialog box.
Update Frequency	The interval at which the data is updated in the monitor dialog.
Column Data	Specifies the type of data that is displayed in the monitor dialog. • Absolute Value - Displays the total amount since the switch was booted. This is the default for error monitoring. • Cumulative - Displays the total amount since the dialog was opened. You can reset the counters by clicking the Reset Cumulative Counters button, to gather a new set of cumulative data. • Minimum/sec - Displays the minimum value per second at every refresh interval. • Maximum/sec - Displays the maximum value per second at every refresh interval. • Last Value/sec - Displays the most recent value per second at every refresh interval. This is the default setting for traffic monitoring.
Elapsed	The amount of time that has elapsed since the dialog was opened. You can reset this counter by clicking the Reset Cumulative Counters button, to gather a new set of cumulative data.

iSNS Details iSCSI Nodes

Field	Description
Name	The iSCSI Name of the initiator or target associated with the storage node.
Type	The Node Type bit-map defining the functions of this iSCSI node, where 31 is a Target, 30 is an Initiator, 29 is a Control, and all others are reserved.
Alias	The Alias name of the iSCSI node.
ScnBitmap	The State Change Notification (SCN) bitmap for a node.
WWN Token	An optional globally unique 64-bit integer value that can be used to represent the World Wide Node Name of the iSCSI device in a Fibre Channel fabric.
AuthMethod	The iSCSI authentication method enabled for this iSCSI Node.

iSNS Details Portals

Field	Description
Addr	The Internet address for this portal.
TcpPort	The port number for this portal.
SymName	The optional Symbolic Name for this portal.
EsiInterval	The Entity Status Inquiry (ESI) Interval for this portal.
TCP ESI	The TCP port number used for ESI monitoring.
TCP Scn	The TCP port used to receive SCN messages from the iSNS server.
SecurityInfo	Security attribute settings for the portal as registered in the Portal Security Bitmap attribute.

Security

Security Roles

Field	Description
Name	Name of the role. Click the **Create** button to define a new role. Click the **Rules** button to define the rules for this role.
Description	Text description of the user role.
VSAN Scope Enable	Enables the ability to limit the role to specified VSANs.
VSAN Scope List	Specify a list of VSANs to which the role is allowed access.
Interface Scope Enable	(Nexus 5000 Series only) Enables the ability to limit the role to specified interfaces.
Interface Scope List	(Nexus 5000 Series only) Specify a list of interfaces to which the role is allowed access.

Security Role Rules

Note This table applies only to Nexus 5000 Series switches.

Field	Description
Rule Order	The rules are applied in numerical order.
Permit?	Indicates whether the rule will permit or deny the operation.
Rule Operation	The rule can specify read-only access or read-write access to the operation.
Rule Element Type	The rule can be applied to a command, a feature, feature group or all. Select **all** to apply the rule to all commands and features.

Field	Description
Rule Element	The rule element specifies the command, feature or feature group to which the rule applies.
Features/Groups	Click the **Features/Groups** button to open the feature group manager.

Feature Group Manager



Note This table applies only to Nexus 5000 Series switches.

Field	Description
Name	The name of the feature group.
Add	To create a new feature group, enter a new feature group name in the Name field, and click **Add**.
Add Feature	To add features to feature groups, select one or more feature group names in the Feature Groups panel, select features in the Features panel, and click **Add Feature**.
Apply	To save changes, click the **Apply** button

AAA LDAP Servers

Field	Description
IP Address Type	The IP address type (IPv4, IPv6, or DNS).
Name or IP Address	The name or IP address of the AAA server.
AuthPort	The Authentication port of the AAA server.
TimeOut(s)	The time in seconds between retransmissions to the AAA server.This value overrides value set in the timeout set in the Features tab for this server. If this value is zero, then the value set in the Features tab will be used.
Retransmits	The additional number of times the AAA server should be tried by the AAA client before giving up on the server. This value overrides value set in the Features tab. If this value is zero, then the value set in the Features tab will be used.
Idle Time (m)	The time interval in minutes, at which the system periodically tests the AAA Server by sending test packets to the server. The default value of 0 means that the AAA server is not tested periodically.
TestUser	The user name to be used in the test packets sent to the AAA Server, to test if the server responds to the requests.
TestPassword	The password to be used in test packets sent to the AAA Server to test if the server responds to the requests.

Field	Description
RootDN	The root name that is used for authenticating access to LDAP server database.
RootDNPasswordEncrType	Type of encryption that is used for the RootDNPassword password.
RootDNPassword	The RootDN password to use if you want to perform root binding. Anonymous bind will be performed if you do not enter a RoodDN password.
SSL Mode	Specifies whether the TLS tunnel needs be setup or not, before binding with the LDAP server.

AAA Server Groups

Field	Description
Name	The name of the server group.
Protocol	The AAA protocol to which this server group belongs to.
ServerIdList	This represents ordered list of AAA Servers which form this Server Group. The order in which servers occur within the value determines the Server priority in that group. The first one will be 'Primary' and the rest are secondary (others). A Server Group can not exist without any members.
DeadTime	The DeadTime setting for AAA Server Group. This indicates the length of time in minutes that the system will mark the server dead when a AAA server does not respond to an authentication request. During the interval of the dead time, any authentication request that comes up would not be sent to that AAA server that was marked as dead. The default value of 0 means that the AAA servers will not be marked dead if they do not respond.

AAA Search Map

Field	Description
BaseDN	Specifies the name of the base entry in the LDAP hierarchy from where begins the search while processing the authorization request.
Filter	Specifies the name of the LDAP filter to be used for searching the user e database.
Attribute	Specifies the LDAP attribute to be used as user profile private attribute.

AAA Applications

Field	Description
ServerGroupIdList	This represents ordered list of AAA server groups that are configured for this application to perform AAA functions. The order in which server groups occur within the value determines the Server Group priority in the list.

Field	Description
Local	The 'Local' AAA means all the AAA functions are performed using the local AAA service provided in the device. If enabled, is used only after trying all the server groups in the server group list.
Trivial	'Trivial' AAA is used only after trying all the server groups and 'Local' AAA (if configured). Trivial AAA corresponds to one of the following based on the value of corresponding instance of AAAFunction. • User name based authentication, if 'AAAFunction' value is 'authentication' • No Authorization check, if 'AAAFunction' value is 'authorization' • No accounting, if 'AAAFunction' value is 'accounting'.

AAA Defaults

Field	Description
KeyEncrType	The encryption type of the server key.
AuthKey	The key used in encrypting the frames passed between the AAA server and the client.This key must match the one configured on the server.
TimeOut	The time in seconds between retransmissions to the AAA server.
Retransmits	The additional number of times the AAA server should be tried by the AAA client before giving up on the server.
DirectReq	Specifies whether you can choose an AAA server for authentication during login. If true, you can specify the remote AAA server for authentication during login. If you specify the login name as username@hostname, then the authentication request is sent to the remote AAA server hostname with the user name as user name. If false, you cannot specify the remote AAA server for authentication during login.
DeadTime (m)	The DeadTime setting for AAA server group. This indicates the length of time in minutes that the system will mark the server dead when a AAA server does not respond to an authentication request. During the interval of the dead time, any authentication request that comes up would not be sent to that AAA server that was marked as dead. The default value of 0 means that the AAA servers will not be marked dead if they do not respond.

AAA General

Field	Description
AuthTypeMSCHAP	Indicates whether the MSCHAP authentication mechanism should be used for authenticating the user through the remote AAA server during login. If true, MSCHAP authentication is used. If false, the default authentication mechanism is used.

Field	Description
AuthTypeMSCHAPv2	Indicates whether the MSCHAPv2 authentication mechanism should be used for authenticating the user through remote AAA Server during login. If true, MSCHAP authentication is used. If false, the default authentication mechanism is used.



Note You are recommended to change one authentication mechanism at a time otherwise there might be an error. For example, if you want to change MSCHAP to MSCHAPv2, please choose MSCHAP and apply, and then choose MSCHAPv2 and apply.

AAA Statistics

Field	Description
Authentication	
Requests	The number of authentication requests sent to this server since it was made active. Retransmissions due to request timeouts are counted as distinct requests.
Timeouts	The number of authentication requests which have timed out since the server was made active.
Unexpected	The number of unexpected authentication responses received from this server since it was made active.
Errors	The number of server ERROR authentication responses received from this server since it was made active.
Incorrect	The number of authentication responses which could not be processed since the server was made active.
ResponseTime	Average response time for authentication requests sent to this server, excluding timeouts, since system re-initialization.
Successes	The number of authentication transactions with this server which succeeded since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction is successful if the server responds with either an authentication pass or fail.
Failures	The number of authentication transactions with this server which failed since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction failure occurs if maximum resends have been met or the server aborts the transaction.
Authorization	
Requests	The number of authorization requests sent to this server since it was made active. Retransmissions due to request timeouts are counted as distinct requests.
Timeouts	The number of authorization requests which have timed out since the server was made active. A timeout results in a retransmission of the request. If the maximum number of attempts has been reached, no further retransmissions will be attempted.

Field	Description
Unexpected	The number of unexpected authorization responses received from this server since it was made active. An example is a delayed response to a request which had already timed out.
Errors	The number of server ERROR authorization responses received from this server since it was made active. These are responses indicating that the server itself has identified an error with its authorization operation.
Incorrect	The number of authorization responses which could not be processed since the server was made active. Reasons include inability to decrypt the response, invalid fields, or the response is not valid based on the request.
ResponseTime	Average response time for authorization requests sent to this server, excluding timeouts, since system re-initialization.
Successes	The number of authorization transactions with this server which succeeded since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction is successful if the server responds with either an authorization pass or fail.
Failures	The number of authorization transactions with this server which failed since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction failure occurs if maximum resends have been met or the server aborts the transaction.
Accounting	
Requests	The number of accounting requests sent to this server since system re-initialization. Retransmissions due to request timeouts are counted as distinct requests.
Timeouts	The number of accounting requests which have timed out since system re-initialization. A timeout results in a retransmission of the request If the maximum number of attempts has been reached, no further retransmissions are attempted.
Unexpected	The number of unexpected accounting responses received from this server since system re-initialization. An example is a delayed response to a request which had already timed out.
Errors	The number of server ERROR accounting responses received from this server since system re-initialization. These are responses indicating that the server itself has identified an error with its accounting operation.
Incorrect	The number of accounting responses which could not be processed since system re-initialization. Reasons include inability to decrypt the response, invalid fields, or the response is not valid based on the request.
ResponseTime	Average response time for accounting requests sent to this server, since system re-initialization excluding timeouts.
Successes	The number of accounting transactions with this server which succeeded since system re-initialization. A transaction may include multiple request retransmissions if timeouts occur. A transaction is successful if the server responds with either an accounting pass or fail.

Field	Description
Failures	The number of accounting transactions with this server which failed since system re-initialization. A transaction may include multiple request retransmissions if timeouts occur. A transaction failure occurs if maximum resends have been met or the server aborts the transaction.
Statistics	
State	Current state of the server. • up - Server responding to requests • dead - Server failed to respond A server is marked dead if it does not respond after maximum retransmissions. A server is marked up again either after a waiting period or if some response is received from it
Duration Current (csec)	The elapsed time the server has been in its current state.
Duration Previous (csec)	This object provides the elapsed time the server was been in its previous state prior to the most recent state. This value is zero if the server has not changed state.
TotalDeadTime	The total elapsed time this server's state has had the value dead since system re-initialization.
DeadCount	The number of times this server's state has transitioned to dead since system re-initialization

iSCSI User

Field	Description
iSCSI User	The name of the iSCSI user.
Password	The password of the iSCSI user.

Common Roles



Note Common Roles is not available in displayFCoE mode (use Security Roles).

Field	Description
Description	Description of the common role.
Enable	This specifies whether the common Role has a VSAN restriction or not.
List	List of VSANs user is restricted to.

SNMP Security Users

Field	Description
Role	The user in Security Model independent format.
Password	Password of the common user. For SNMP, this password is used for both authentication and privacy. For CLI and XML, it is used for authentication only.
Digest	The type of digest authentication protocol which is used.
Encryption	The type of encryption authentication protocol which is used.
ExpiryDate	The date on which this user will expire.
SSH Key File Configured	Specifies whether the user is configured with SSH public key.
SSH Key File	The name of the file storing the SSH public key. The SSH public key is used to authenticate the SSH session for this user. Note that this applies to only CLI user. The format can be one of the following: • SSH Public Key in OpenSSH format • SSH Public Key in IETF SECSH (Commercial SSH public key format) • SSH Client Certificate in PEM (privacy-enhanced mail format) from which the public key is extracted • SSH Client Certificate DN (Distinguished Name) for certificate based authentication
Creation Type	The type of the credential store of the user. When a row is created in this table by a user, the user entry is created in a credential store local to the device. In case of remote authentication mechanism like AAA Server based authentication, credentials are stored in other (remote) system/device.
Expiry Date	The date on which this user will expire.

SNMP Security Communities

Field	Description
Community	The community string.
Role	The Security Model name.

Security Users Global

Field	Description
Enforce SNMP Privacy Encryption	Specifies whether the SNMP agent enforces the use of encryption for SNMPv3 messages globally on all the users in the system.
Cache Timeout	This specifies maximum timeout value for caching the user credentials in the local system.

Note The privacy password and authentication password are required for an administrator to create a new user or delete an existing user in Device Manager. However, if the administrator does not provide these credentials at the time of creating a new user, Device Manager uses the authentication password of the administrator as the privacy password. If the privacy protocol defined for the user is not DES (default), the SNMP Agent in the MDS will not be able to decrypt the packet and the SNMP Agent times out. If the privacy protocol defined for the user is not DES, the user needs to provide both the privacy password and the protocol when logging in.

FC-SP General/Password

Field	Description
Timeout	Timeout period for FC-SP messages
HashList	Contains a proposed hash mechanism, in the order of preference. The first is the most preferred and the last contains the least preferred.
GroupList	Each ':' separated token contains a value, corresponding to a Diffie-Hellman group identifier.
GenericPasswd	Password for the switch

FC-SP Interfaces

Field	Description
Mode	The FC-SP mode on this interface. • If autoPassive, a port would not initiate any FC-SP authentication exchange but would always take part in FC-SP authentication exchange initiated by the other side. • If autoActive, a port would always try to initiate FC-SP authentication exchange after ESC. If other side does not support FC-SP authentication port will still be brought up. • If on, port would always try to initiate FC-SP authentication exchange and authentication is done before the port becomes up. If other side does not support FC-SP authentication, port will not be brought up. • If off, port would never initiate FC-SP authentication exchange and send reject to any FC-SP authentication message started from other end. If this is not 'off', then port has to support at least one FC-SP authentication protocol. **Note** You need to configure the FC-SP DHCHAP mode individually on each switch to avoid the timeout error from DCNM.
Reauthenticate Interval (hr)	The time (in hours) for which a port has to wait before trying to re-authenticate the other end.
Reauthenticate Start	Re-authenticate the other end, if this is set to enable.

Field	Description
Auth Successes	The number of times the FC-SP authentication succeeded on this interface.
Auth Fails	The number of times the FC-SP authentication failed on this interface.
Auth Bypasses	The number of times the FC-SP authentication was bypassed on this interface.

FC-SP Local Passwords

Field	Description
Local WWN	The World Wide Name of the local host.
Password	Password of the local switch.

FC-SP Remote Passwords

Field	Description
Remote WWN	The World Wide Name of the remote host.
Password	Password of the remote switch.

FC-SP Statistics

Field	Description
Auth Succeeded	The number of times the FC-SP authentication succeeded on this interface.
Auth Failed	The number of times the FC-SP authentication failed on this interface.
Auth ByPassed	The number of times the FC-SP authentication was bypassed on this interface.
EspSpiMismatch	The number of frames received with a mismatched SPI.
EspAuthFailed	The number of frames received that failed ESP authentication check.

FC-SP SA (Security Association)

Field	Description
SPI	Displays the Security Parameter Index value.
Salt	Salt used for encryption.
Key	Key used for encryption and authentication.

FC-SP ESP Interfaces

Field	Description
Interface	Name of the interface.

Field	Description
ESP Mode	Specifies the ESP mode as one of the following: • None-ESP is not running on the link. • Gcm- Link needs to be encrypted and authenticated. • Gmac-Link needs to be authenticated
EgressSA	Specifies the egress security association to be used. Valid values are between 256 and 65536.
IngressSA1	Specifies the ingress security association to be used. Valid values are between 256 and 65536.
IngressSA2	Specifies the ingress security association to be used. Valid values are between 256 and 65536.
EspFailureReason	Displays the reason of failure. “None” indicates that no error.

PKI General

Field	Description
Switch	Name of the switch.
CertStoreConfig	The certificate store configuration used by the system for authentication.

PKI RSA Key-Pair

Field	Description
Name	The name or label of a key-pair.
Size	The size of the key. The following modulus sizes are defined: • 512-bit, 768-bit, 1024-bit, 1536-bit and 2048-bit. Once created, the size cannot be changed. After a key-pair has been deleted through row deletion, the entry can be created again with another size.
FileName	The name of the file storing the RSA private key. This filename is automatically generated from the key-pair name. It is a unix style '/' separated string representing the absolute path of the file in the file system of the device.
Exportable	The key-pair is exportable through the exportpkcs12 PKI support action. Once created, the exportable flag value cannot be changed. After a key-pair has been deleted through row deletion, the entry can be created again with another value for the exportable flag.

PKI Trust Point

Field	Description
Name	The name or label of a trust point.

Field	Description
KeyPair Name	The name of the associated key-pair from a key-pair table. If a key-pair is not yet associated, the value will be a zero length string.
Revoke CheckMethods	Revocation checking methods list which is an ordered list of certificate revocation checking methods to be employed while verifying peer certificates issued by the CA corresponding to this trust point entry. The value of this object is a ordered list of one or more 1-octet values, where each 1-octet value corresponds to a method in the revocation checking method enumeration: • none (1) - No revocation status checking needed; instead consider the certificate as not revoked. • crl (2) - Use CRL for checking the revocation status of certificates. • ocsp (3) - Use OCSP for checking the revocation status of certificates. If none occurs in the list, it should be the last value. The octets after the last value in the ordered list should be zero octets. The order in which the revocation checking methods occur within the value of this object determines the order the revocation checking methods are attempted during the verification of a peer certificate. The default value (after row creation) contains only the revocation checking method crl.
OCSPurl	The contact http url of the external OCSP server for certificate revocation checking using OCSP protocol. The default value (after row creation) s a zero length string.

PKI Trust Point Actions

Field	Description
Name	The name or label of the trust point action.
Command	The PKI support action to be triggered for this trust point entry.
Url	Indicates the file name containing the input or output certificate data needed for the PKI support action being triggered on this entry. The file name should be specified as bootflash:<filename> and it should be available on bootflash or get created on bootflash depending upon the action being triggered.
Password	Indicates the password required to perform the PKI support action being triggered. This password is required to be specified only for certreq, importpkcs12 and exportpkcs12 actions. For security reasons, the value, whenever it is retrieved by the management protocol, is always the zero length string.
Last Command	The PKI support action attempted last. The value attempted to be set for cpkiAction object last. If no action has been triggered for the trust point after its creation, then retrieving the value of this object will return none.
Result	The result of the execution of the last PKI support action.

PKI LDAP

Field	Description
Switch	Name of the switch.
Store Type	The type of remote certificate store.
CRL Timer (hrs)	The time interval based on which the CRL's corresponding to the CA certificates are updated. The CA certificates and the corresponding CRL's are fetched from remote certstore for authenticaion are stored in local cache to avoid time delays for subsequent authentication.
Server Group Name	The name of the server group that is used for the remote certstore operations.

PKI Certificate Map

Field	Description
Switch	Name of the switch
Filter Name	The unique name of the mapping filter
Subject Name	The subject name of the CA certificate.
Alternate Name Email	AltNameEmail is another unique field and is a part of the subject name, that is used for authentication.
Alternate Name Universal Principal Name	UPN is another unique field and is a part of the subject name, that is used for authentication.

PKI Certificate Map - Application

Field	Description
Switch	Name of the switch.
Purpose / Issuer Name	The issuer name of the certificate
Map Name 1	The name of the first filtering map that will be applied to the certificate with a given purose and an issuer name.
Map Name 2	The name of the second filtering map that will be applied to the certificate with a given purose and an issuer name.

PKI Trust Point Detail

Field	Description
Name	The name or label of the key-pair.
IdCert FileName	The name of the file storing the identity certificate. It is a unix style '/' separated string representing the absolute path of the file in the file system of the device. If there is no identity certificate obtained as yet, the value will be a zero length string.

Field	Description
IdCert SubjName	The subject name of the identity certificate. If there is no certificate or no subject name in the certificate, the value of this object will be a zero length string.
IdCert SerialNum	The serial number of the identity certificate. If there is no certificate, the value of this object will be a zero length string.
IdCert StartDate	The time when the identity certificate starts to be valid, corresponding to the notBefore field in the certificate. If there is no certificate, the value of this object will be a zero length string.
IdCert EndDate	The time when the identity certificate validity ends, corresponding to the notAfter field in the certificate. If there is no certificate, the value of this object will be a zero length string.
IdCert FingerPrint	The MD5 fingerprint of the identity certificate in HEX string format. If there is no certificate, the value of this object will be a zero length string.
IssuerCert FileName	The name of the file storing the issuer certificate. It is a unix style '/' separated string representing the absolute path of the file in the file system of the device. If there is no issuer certificate obtained yet, the value of this object will be a zero length string.
IssuerCert SubjName	The issuer name (subject name in issuer certificate which will be the same as the issuer name in the identity certificate if present). If there is no certificate, the value will be a zero length string.
IssuerCert SerialNum	The serial number of the issuer certificate. If there is no certificate, the value will be a zero length string.
IssuerCert StartDate	The time when the issuer certificate starts to be valid, corresponding to the notBefore field in the certificate. If there is no certificate, the value will be a zero length string.
IssuerCert EndDate	The time when the issuer certificate validity ends, corresponding to the notAfter field on in the certificate. If there is no certificate, the value will be a zero length string.
IssuerCert FingerPrint	The MD5 fingerprint of the issuer's certificate in HEX string format. If there is no certificate, the value of this object will be a zero length string.

IKE Global

Field	Description
RemIdentity	Displays the keep alive interval in seconds used by the IKE entity on the managed device with all the peers for the DOI corresponding to this conceptual row.
Key	Displays the type of keep alives to be used by the IKE entity on the managed device with all the peers for the DOI corresponding to this conceptual row.

IKE Pre-Shared AuthKey

Field	Description
KeepAliveInterval (sec)	The Phase 1 ID identity of the peer for which this pre-shared key is configured on the local entity.
IdentityType	The pre-shared authorization key used in authenticating the peer corresponding to this conceptual row.

IKE Policies

Field	Description
Priority	The priority of this ISAKMP Policy entry. The policy with lower value would take precedence over the policy with higher value in the same DOI.
Encr	The encryption transform specified by this ISAKMP policy specification. The Internet KeyExchange (IKE) tunnels setup using this policy item would use the specified encryption transform to protect the ISAKMP PDUs.
Hash	The hash transform specified by this ISAKMP policy specification. The IKE tunnels setup using this policy item would use the specified hash transform to protect the ISAKMP PDUs.
Auth	The peer authentication method specified by this ISAKMP policy specification. If this policy entity is selected for negotiation with a peer, the local entity would authenticate the peer using the method specified by this object.
DHGroup	Specifies the Oakley group used for Diffie Hellman exchange in the Main Mode. If this policy item is selected to negotiate Main Mode with an IKE peer, the local entity chooses the group specified by this object to perform Diffie Hellman exchange with the peer.
Lifetime (sec)	Specifies the lifetime in seconds of the IKE tunnels generated using this policy specification.

IKE Initiator Version

Field	Description
Address	The address of the remote peer corresponding to this conceptual row. This object cannot be modified while the corresponding value of cicIkeCfgInitiatorStatus is equal to active.
Version	The IKE protocol version used when connecting to a remote peer specified in cicIkeCfgInitiatorPAddr. This object cannot be modified while the corresponding value of cicIkeCfgInitiatorStatus is equal to active.

IKE Tunnels

Field	Description
LocalAddress	The address of the local endpoint for the Phase-1 tunnel.

Field	Description
RemoteAddresss	The address of the remote endpoint of the Phase-1 tunnel.
AuthMethod	The authentication method used in Phase-1 negotiations on the control tunnel corresponding to this conceptual row.
Action	The action to be taken on this tunnel. If clear, then this tunnel is cleared. If re-key, then re-keying is forced on this tunnel. The value none would be returned on doing read of this object.

IPSEC Global

Field	Description
Lifetime (sec)	The default lifetime (in seconds) assigned to an IPSEC tunnel as a global policy (maybe overridden in specific cryptomap definitions).
Lifesize (KB)	The default life size in KBytes assigned to an IPSEC tunnel as a global policy (unless overridden in cryptomap definition).

IPSEC Transform Set

Field	Description
Id	This is the sequence number of the transform set that uniquely identifies the transform set. Distinct transform sets must have distinct sequence numbers.
Protocol	Represents the suite of Phase-2 security protocols of this transform set.
ESP Encryption	Represents the transform used for ESP encryption.
ESP Authentication	Represents the transform used to implement integrity check with ESP protocol.
Mode	Represents the encapsulation mode of the transform set.

IPSEC CryptoMap Set Entry

Field	Description
IpFilter	Specifies an IP protocol filter to be secured using this cryptomap entry. When it has a value of zero-length string, it is not valid/applicable.
TransformSetIdList	The list of cipsXformSetId that are members of this CipsStaticCryptomapEntry. The value of this object is a concatenation of zero ormore 4-octet strings, where each 4-octet string contains a 32-bit cipsXformSetId value in network byte order. A zero length string value means this list has no members.
AutoPeer	If true the destination address is taken as the peer address, while creating the tunnel.
Peer Address	The IP address of the peer to which this cryptomap entry is currently connected.

Field	Description
PFS	Identifies whether the tunnels instantiated due to this policy item should use Perfect Forward Secrecy (PFS) and if so, what group of Oakley they should use.
LifeTime	Specifies the lifetime of the IPsec Security Associations (SA) created using this IPsec policy entry.
Lifesize Value	Identifies the life size (maximum traffic in bytes that may be carried) of the IPSec SAs created using this IPSec policy entry. When a Security Association (SA) is created using this IPsec policy entry, its life size takes the value of this object.

IPSEC Interfaces

Field	Description
CryptomapName	The index of the static cryptomap table. The value of the string is the name string assigned by the NMS when defining a cryptomap set.
InterfaceList	Interfaces belong to the cryptomap.

IPSEC Tunnels

Field	Description
Local Address	The IP address of the local endpoint for the IPsec Phase-2 tunnel.
RemoteAdddress	The type of the IP address of the remote endpoint for the IPsec Phase-2 tunnel.
ESP Encryption	The encryption algorithm used by the outbound security association of the IPsec Phase-2 tunnel.
ESP Encryption KeySize	The key size in bits of the negotiated key to be used with the algorithm denoted by ceipSecTunOutSaEncryptAlgo. For DES and 3DES the key size is respectively 56 and 168. For AES, this will denote the negotiated key size.
ESP Authentication	The authentication algorithm used by the inbound encapsulation security protocol (ESP) security association of the IPsec Phase-2 tunnel.
LifeSize (KB)	The negotiated life size of the IPSEC Phase-2 tunnel in kilobytes.
LifeTime (sec)	The negotiated lifetime of the IPSEC Phase-2 tunnel in seconds. If the tunnel was setup manually, the value of this MIB element should be 0.
Action	The status of the MIB table row.

IP ACL Profiles

Field	Description
Name	This is the unique IP protocol filter profile identifier.
Type	This object determines the usage type for this filter profile. This usage type cannot be changed after the profile has been created.

IP ACL Interfaces

Field	Description
ProfileName	This is the unique IP protocol filter profile identifier.

IP Filter Profiles

Field	Description
Action	If it is set to deny, all frames matching this filter will be discarded and scanning of the remainder of the filter list will be aborted. If it is set to permit, all frames matching this filter will be allowed for further bridging or routing processing.
Protocol	This filter protocol value matches the Internet Protocol Number in the frames. These IP numbers are defined in the Network Working Group Request for Comments (RFC) documents. Setting this to '-1' will make the filtering match any IP number.
Address	The source IP address to be matched for this filter. A value of 0 causes all source address to match.
Mask	This is the wildcard mask for the SrcAddress bits that must match. 0 bits in the mask indicate the corresponding bits in the SrcAddress must match in order for the matching to be successful, and 1 bits are don't care bits in the matching. A value of 0 causes only IP frames of source address the same as SrcAddress to match.
PortLow	If Protocol is UDP or TCP, this is the inclusive lower bound of the transport-layer source port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or less than the value specified for this entry in SrcPortHigh.
PortHigh	If Protocol is UDP or TCP, this is the inclusive upper bound of the transport-layer source port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or greater than the value specified for this entry in SrcPortLow. If this value is '0', the UDP or TCP port number is ignored during matching.
Address	The destination IP address to be matched for this filter. A value of 0 causes all source address to match.
Mask	This is the wildcard mask for the DestAddress bits that must match. 0 bits in the mask indicate the corresponding bits in the DestAddress must match in order for the matching to be successful, and 1 bits are don't care bits in the matching. A value of 0 causes only IP frames of source address the same as SrcAddress to match.
PortLow	If Protocol is UDP or TCP, this is the inclusive lower bound of the transport-layer destination port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or less than the value specified for this entry in PortHigh.

Field	Description
PortHigh	If Protocol is UDP or TCP, this is the inclusive upper bound of the transport-layer destination port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or greater than the value specified for this entry in DestPortLow. If this value is '0', the UDP or TCP port number is ignored during matching.
Precedence	The IP traffic precedence parameters in each frame are used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Most network treats high precedence traffic as more important than other traffic. The IP Precedence value ranges from '0' to '7', with '7' the highest precedence and '0' the lowest precedence. The value '-1' means to match frames of any IP precedence. In other words, the IP precedence parameter will not to checked if this value is '-1'. The precedence level are: • routine(0) - Routine traffic precedence • priority(1) - Priority traffic precedence • immediate(2) - Immediate traffic precedence • flash(3) - Flash traffic precedence • flashOverride(4) - Flash-override traffic precedence • critical(5) - Critical precedence • internet(6) - Internetwork control traffic precedence • network(7) - Network control traffic precedence.
TOS	The Type of Service (TOS) of the frame. The TOS values ranges from '0' to '15'. The value '-1' matches any TOS value.
ICMPType	This filter specifies the ICMP message type to be matched. Setting this value to '-1' will make the filtering match any ICMP message type.
ICMPCode	This filter specifies the ICMP message code to be matched. Setting this value to '-1' will make the filtering match any ICMP code.
TCPEstablished	This filter if true specifies that for TCP protocol, in an established connection, a match occurs if the TCP datagram has the ACK,FIN,PSH,RST,SYN or URG control bits set. If false, a match will occur for any TCP datagram.
LogEnabled	Specifies whether filtered frames will be logged by the filtering subsystem or not. If true, then all frames will be logged. If false, then no frame will be logged.

SSH/Telnet

Field	Description
Enable SSH/Telnet	Check to enable SSH and/or Telnet.
NumBits	The number of bits provided to generate the key. This determines the length of the key string generated by the SSH.
Key	The SSH key string that is generated.

Field	Description
LastCreationTime	The time of the last creation of the key.
Enable	Enables or disables the Secure Shell (SSH) service on the device.

Port Security Actions

Field	Description
Activation	
Action	• activate - results in the valid port bindings on this VSAN/VLAN being activated. • activate (Turn LearningOff) - results in the valid port bindings on this VSAN/VLAN being activated and copied to the active database and will also result in auto learn being turned off on this VSAN/VLAN, once the activation is complete. • force activate - results in forced activation, even if there are errors during activation and the activated port bindings will be copied to the active database. • force activate (Turn Learning Off) - results in forced activation along with turning auto learn off after activation and the activated port bindings will be copied to the active database. • deactivate - results in deactivation of currently activated valid port bindings (if any), on this VSAN/VLAN. Currently active entries (if any), which would have been present in the active database, will be removed. • Activation will not be allowed on a VSAN if auto-learn is enabled on that VSAN
Enabled	The state of activation on this VSAN/VLAN. If true, then an activation has been attempted as the most recent operation on this VSAN/VLAN. If false, then an activation has not been attempted as the most recent operation on this VSAN/VLAN.
Result	Indicates the outcome of the most recent activation/deactivation.
Last Change	When the valid port bindings on this VSAN/VLAN were last activated. If the last activation took place prior to the last re-initialization of the agent, then this value will be N/A.
CopyActiveToConfig	If enabled, results in the active port binding database to be copied on to the configuration database on this VSAN/VLAN. Note that the learned entries are also copied.
AutoLearn	Helps to learn the valid port binding configuration of devices/ports logged into the local device on all its ports and populate the above active database with the same. This mechanism of 'learning' the configuration of devices/ports logged into the local device over a period of time and populating the configuration is a convenience mechanism for users. If enabled on a particular VSAN, all subsequent logins (FLOGIs) on that VSAN will be populated in the enforced port binding database, provided it is not in conflict with existing enforced port bindings on that VSAN. When disabled, the mechanism of learning is stopped. The learned entries will however be in the active database.

Field	Description
Clear AutoLearned	
Action	• Clear VSAN results in port bind auto-learnt entries being cleared on this VSAN. • Clear Interface(s) results in port bind auto-learnt entries being cleared on the interface specified on this VSAN.
Interface	Specifies the interface(s) on which the port bind auto-learnt entries need to be cleared.

Port Security Config Database

Field	Description
Interface or fWWN	Represents the address of the port on the local device through which the device specified can FLOGI. • If fwwn, then the value is the fabric WWN of a port on the local device • If intfIndex, then a port on the local device is being represented by its interface. • If wildCard, then it represents a wild-card entry. The wild-card represents any port on the local device.
Type	The mechanism to identify a switch port.
WWN	Represents the logging-in device address

Port Security Active Database

Field	Description
Interface or fWWN	The address of a port on the local device.
Type	The mechanism to identify a switch port.== fwwn - the local switch port is identified by Fabric WWN(fWWN). == intfIndex - the local switch port is identified by ifIndex. == wildCard - wild card (any switch port on local device).
WWN	Represents the logging in device address.
IsLearnt	Indicates if this entry is a learnt entry or not.

Port Security Database Differences

Field	Description
CompareWith	Specifies the database for the comparison. • configDb - compares the configuration database with respect to active database on this VSAN/VLAN. So, the active database will be the reference database and the results of the difference operation will be with respect to the active database. • activeDb - compares the active database with respect to configuration database on this VSAN/VLAN. So, the configuration database will be the reference database and the results of the difference operation will be with respect to the configuration database.
VSANId	The ID of the VSAN to compare against.
Interface/fWWN	The address of a port on the local device.
Type	The mechanism to identify a switch port. • fwwn - the local switch port is identified by Fabric WWN(fWWN). • intfIndex - the local switch port is identified by ifIndex. • wildCard - wild card (any switch port on local device).
WWN	Represents the logging in device address.
Reason	Indicates the reason for the difference between the databases being compared, for this entry.

Port Security Violations

Field	Description
Interface	The fWWN of the port on the local device where the login was denied.
End Device	The pWWN of the device that was denied FLOGI on one of the local device's ports.
Or Switch	The sWWN of the device (if the device happens to be a switch), that was denied entry on one of the local device's ports.
Time	When the login denial took place.
Count	The number of times this particular pWWN/nWWN or sWWN has been denied login on this particular local interface.

Port Security Statistics

Field	Description
AllowedLogins	The number of FLOGI requests that have been allowed on this VSAN/VLAN.
DeniedLogins	The number of FLOGI requests that have been denied on this VSAN/VLAN.
Clear	When set to clear, it results in port bind statistic counters being cleared on this VSAN/VLAN.

IPsec

Field	Description
Interface, CryptomapName	The binding of cryptomap sets to the interfaces of the managed entity.

Events

Call Home General

Field	Description
Contact	The contact person for this switch, together with information on how to contact this person.
PhoneNumber	The phone number of the contact person. The phone number must start with '+' and contains only numeric characters except for space and '-'. Some valid phone numbers are +44 20 8332 9091 +45 44886556 +81-46-215-4678 +1-650-327-2600.
EmailAddress	The email address of the contact person. Some valid email addresses are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
StreetAddress	The mailing address of this switch.
CustomerId	A string, in whatever format is appropriate, to identify the customer.
ContractId	A string, in whatever format is appropriate, to identify the support contract between the customer and support partner.
SiteId	A location identifier of this device.
DeviceServicePriority	The service priority of the device. This determines how fast the device has to be serviced.
Enable	Enables or disables the CallHome infrastructure on the local device.

Call Home Destinations

Field	Description
ProfileName,ID	The destination profile name and identifier.
Type	Transmission method type.
EmailAddress	The email address associated this destination profile. Some examples are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
Http Url	The HTTP URL associated with this destination profile.

Call Home Email Setup

Field	Description
From	The email address that is to be used in the From field when sending the email using SMTP. Some examples are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.

Field	Description
ReplyTo	The email address that is to be used in the Reply-To field when sending the email using SMTP. Some examples are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
IP Address Type	The IP address type (IPv4, IPv6, or DNS).
Name or IP Address	Name or IP address of the SMTP server.
Port	TCP port of the SMTP server.

Call Home Alerts

Field	Description
Action	Test - sends a Call Home message TestWithInventory - sends a message with inventory details.
Status	The status of the last callhome action invocation.
FailureCause	The failure cause for the last callhome test invocation.
LastTimeSent	When the last CallHome alert was sent.
NumberSent	The number of CallHome alerts sent.
Every	Time frame for sending the periodic software inventory Call Home message.
Throttling Enable	If checked, enables the message throttling mechanism implemented on the system, to limit the number of callhome messages for a alert type within a time frame. The maximum is 30 in a 2-hour time frame, and any further messages for that alert type are discarded.
Enable	If checked, enables the sending of periodic software inventory callhome messages on the system.

Call Home HTTP Proxy Server

Field	Description
Master	Name of the switch.
Address Type	The type of the HTTP proxy server as represented by the value in the HTTP proxy server address.
Address	The address of the HTTP proxy server.
Port	The port of the HTTP proxy server.
Enable	Enable or disable the use of HTTP proxyserver configured for sending callhome messages over HTTP.

Call Home SMTP Servers

Field	Description
Address Type, Address	IP address of the SMTP server.
Port	TCP port of the SMTP server.
Priority	Priority value

Call Home User Defined Command

Field	Description
User Defined Command	Used to configure user defined commands for the callhome alert group types.

Delayed Traps

Field	Description
Enable	Enable or disable delay traps.
Delay	Delay interval in minutes (valid values are between 1 to 60)

Call Home Profiles

Field	Description
MsgFormat	XML, full text, or short text.
MaxMsgSize	Maximum message size that can be sent to destination pointed to by this destination profile.
MsgLevel	Threshold level, used for filtering alert messages sent to a destination. Callhome alert message with severity level lower than the configured threshold level would not be sent. The default threshold level is debug (1), which means all the alert messages will be sent.
AlertGroups	The list of configured alert groups for this destination profile.

Event Destinations Addresses

Field	Description
Address/Port	IP Address and Port to send event.
Security Name	The SNMP parameters to be used when generating messages to be sent to this address.
Security Model	Is used when generating SNMP messages using this entry.
Inform Type	• Trap - unacknowledged event • Inform - acknowledged event.

Field	Description
Inform Timeout	This expected maximum round trip time for communicating with the address.
RetryCount	The number of retries to be attempted when a response is not received for a generated message.
Status	• Active—Port is active. • NotInService—Port is out of service.

Event Destinations Security (Advanced)

Field	Description
MPModel	The Message Processing Model to be used when generating SNMP messages using this entry.
SecurityModel	The Security Model to be used when generating SNMP messages using this entry.
SecurityName	Identifies the Principal on whose behalf SNMP messages will be generated using this entry.
SecurityLevel	The Level of Security to be used when generating SNMP messages using this entry.

Event Filters General

Field	Description
FSPF - Nbr State Changes	Specifies whether or not the local switch should issue notification when the local switch learns of a change in the Neighbor's state (state in the FSPF Neighbor Finite State Machine) on an interface on a VSAN.
Domain Mgr - ReConfig Fabrics	Specifies whether or not the local switch should issue a notification on sending or receiving ReConfigureFabric (RCF) on a VSAN.
Zone Server - Request Rejects	Specifies if the Zone Server should issue a notification on rejects.
Zone Server - Merge Failures	Specifies if the zone server should issue a notification on merge failures.
Zone Server - Merge Successes	Specifies if the zone server should issue a notification on merge successes.
Zone Server - Default Zone Behavior Change	Specifies if the zone server should issue a notification if the propagation policy changes.
Zone Server - Unsupp Mode	Specifies if the zone server should issue a notification on unsupp mode changes
FabricConfigServer - Request Rejects	Specifies if the Fabric Configuration Server should issue a notification on rejects.
RSCN - ILS Request Rejects	Specifies if the RSCN module should generate notifications when a SW_RSCN request is rejected.

Field	Description
RSCN - ILS RxRequest Rejects	Specifies if the RSCN module should generate notifications when a SW_RSCN request is rejected.
RSCN - ELS Request Rejects	Specifies if the RSCN module should generate notifications when a SCR or RSCN request is rejected.
FRU Changes	A false value will prevent Field Replaceable Unit (FRU) notifications from being generated by this system.
SNMP - Community Auth Failure	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps.
VRRP	Indicates whether the VRRP-enabled router will generate SNMP traps for events defined in this MIB.
FDMI	Specifies if the FDMI should generate notifications when a registration request is rejected.
License Manager	Indicates whether the system should generate notifications.
Port/Fabric Security	Specifies if the system should generate notifications when a port/fabric security issue arises.
FCC	Specifies whether the agent should generate notifications.
Name Server	If checked, the Name Server generates a notification when a request is rejected. If false, the notification is not generated.

Event Filters Interfaces

Field	Description
EnableLinkTrap	Indicates whether linkUp/linkDown traps should be generated for this interface.

Event Filters Control

Field	Description
Variable	Represents the notification to be controlled.
Descr	Description about the notification.
Enabled	Check to enable notification of the control. Shows the status of the control.



Note You see the Descr column only on switches that runs Cisco NX-OS release 5.0 or later.

Link Incident History

Field	Description
Host Time	The local time on the host.

Field	Description
Switch Time	The local time on the switch.
Port	The port number for the link incidents.
Interface	The Fibre Channel interface in the specified port.
Link Incident	The type of incident that occurred.

RMON Thresholds Controls

Field	Description
AlarmEnable	If true, the RMON alarm feature is enabled. If the RMON feature is disabled, all the RMON alarm related polling are stopped. Note that this is only intended for temporary disabling of RMON alarm feature to ensure that the CPU usage by RMON alarms is not detrimental. For permanent disabling on this feature, it suggested that all the entries in the alarmTable are removed.
MaxAlarms	The maximum number of entries allowed in the alarmTable.

RMON Thresholds 64bit Alarms

Field	Description
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. When setting this variable, care should be taken in the case of deltaValue sampling - the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2^31 - 1 during a single sampling interval.
Variable	The variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.
SampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value is absoluteValue, the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value is deltaValue, the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
Value	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes.
StartupAlarm	The alarm that may be sent when this entry is first set to valid.

Field	Description
Rising Threshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.
Rising EventId	The ID of the eventEntry that is used when a rising threshold is crossed.
Falling Threshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated.
Falling EventId	The ID of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of eventIndex. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is N/A, no associated event will be generated, as N/A is not a valid event index.
FailedAttempts	The number of times the alarm variable was polled (in the active state) and no response was received.
Owner	The ID of the user who configured this entry.

RMON Thresholds 32bit Alarms

Field	Description
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. When setting this variable, care should be taken in the case of deltaValue sampling - the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2^31 - 1 during a single sampling interval.
Variable	The variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.
SampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Value	The value of the statistic during the last sampling period.
StartupAlarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.
Rising EventId	The ID of the eventEntry that is used when a rising threshold is crossed.
Falling Threshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated.
Falling EventId	The ID of the eventEntry that is used when a falling threshold is crossed.

Field	Description
FailedAttempts	The number of times the alarm variable was polled (in the active state) and no response was received.
Owner	The ID of the user who configured this entry.

RMON Thresholds Events

Field	Description
Description	A comment describing this event entry.
Type	The type of notification that the probe will make about this event. In the case of log, an entry is made in the log table for each event. In the case of SNMP-trap, an SNMP trap is sent to one or more management stations.
Community	The community string.
LastTimeSent	When this event entry last generated an event. If this entry has not generated any events, this value will be N/A.
Owner	The entity that configured this entry and is therefore using the resources assigned to it.

RMON Thresholds Log

Field	Description
Time	When this log entry was created.
Description	A description of the event that activated this log entry.

Admin

Copy Configuration

Field	Description
From	Specifies the type of file to copy from.
To	Specifies the type of file to copy to.
ServerAddress	The IP address of the server from (or to) which to copy the configuration file.
FileName	The file name (including the path, if applicable) of the file.
Protocol	The protocol to be used for any copy.
UserName	Remote user name.
UserPassword	Remote user password
CopyState	Specifies the state of this config-copy request. The value of this object is instantiated only after the row has been instantiated. For example, after the CopyEntryRowStatus has been made active.

Field	Description
CopyFailCause	The reason why the config-copy operation failed. This object is instantiated only when the CopyState for this entry is in the failed state.

Flash Files

Field	Description
Name	Flash file name as specified by the user copying in the file.
Size (B)	Size of the file in bytes. Note that this size does not include the size of the file system file header.
Modified	Date and time the file was last modified.

Compact Flash

Field	Description
Device	Name of the device.
Partition	Flash partition name used to refer to a partition.
Size	Size of the partition.

License Features

Field	Description
Missing	Represents the number of missing usage licenses of this feature, when one or more installed license files containing this feature's license, are missing in the local system. Under normal condition, the value is 0.
Installed Type	A combination of demo, permanent, counted, unlicensed, inGracePeriod for that license.
Installed Count	Maximum number of concurrent usages of this license feature. This is the cumulative license usage count for this feature from all the installed license files, containing this feature's license information.
Status	Represents the number of current usages of this licensed feature.
ExpiryDate	Expiry date of the licensed feature.
GracePeriod	Represents the grace period left for this feature, in days/seconds. Grace period is the number of seconds either an unlicensed feature or a feature whose license has expired is allowed to run.
Errors	Errors, if any.
DefaultLicenses	The maximum number of concurrent usages of this license feature that is included by default.

License Manager Keys

Field	Description
LastModified	Represents the time when the license file contents was last modified.

Field	Description
Feature	Specifies the installed license file name.
Version	The version number of the license file.
Type	• permanent - Indicates permanent license
Count	• uncounted - Specified the uncounted license for this feature. • counted - Indicates the maximum number of concurrent uses of this licensed feature.

License Manager Install

Field	Description
HostId	Contains the License hostid of the local system. It is used to identify the local system when requesting license(s) for this system.
URI	Represents the location on the local system, from which the license file will be picked for installation. User should have copied the license file provided by CISCO-CCO, by some other means (for example, through CLI) to this location. For example, the value could be 'bootflash:licfile1'. This MUST be set to a valid value before 'install'. For uninstall operation the value is irrelevant.
Target Filename	Represents either the name with which the license file will be installed, or the name of the license file for uninstall.

Status	The status of the license install/uninstall operation: • success (1) - install/uninstall operation completed successfully. InProgress (2) - License install/uninstall operation is in progress. • corruptedLicenseFile (3) - License file content is Invalid/Corrupted. • targetLicenseFileAlreadyExist (4) - Target license file name already exist. • invalidLicenseFileName (5) - License file does not exist. • duplicateLicense (6) - License file is already installed. • licenseInUse (7) - Can't uninstall a license file which is in use. • generalLicensingFailure (8) - General error from license Manager. • none (9) - no install/uninstall operation is performed. • licenseExpiryConflict(10) - License exist with a different expiration date for the feature. • invalidLicenseCount(11) - License count is invalid for the feature. • notThisHost (12) - License host-id in the license file doesn't match. • licenseInGraceMore (13) - Number of licenses in grace period exceeds the number in install license file. • licenseFileNotFound (14) - License file not found, for install / uninstall / update operation. • licenseFileMissing (15) - A previously installed license file is found missing. • licenseFileMissing (15) - A previously installed license file is found missing. • invalidLicenseFileExtension (16) - License file does not have a.lic extension. • invalidURI (17) - Invalid license file URI, specified for install operation. • noDemoLicenseSupport (18) - Demo License Not Supported. • invalidPlatform (19) - Invalid Platform

License Manager Usage

Field	Description
Name	Represents the name of the application which has checked out the feature.
Application	The application which has checked out the feature.

Port Licensing

Field	Description
Id	Displays the License host ID of the local system. It is used to identify the local system when requesting licenses.
Max	Maximum number of concurrent usages of this license.
Used	Represents the current number of usages of this licensed feature.

Feature Set

Field	Description
Name	The name of the feature set.
OpStatus	The current operating status of the feature.
Action	The action executed against the feature set.
LastCommand	The last action triggered for the feature set.
Result	The result of the last action that was applied to the feature set.

Feature Control

Field	Description
Feature Name	The name of the feature.
Status	The current operating status of the feature.
Action	Enable or disable a feature.
LastCommand	The result of the last action for the feature.
Result	The failure reason description for the failed execution of last action triggered for the feature.

NTP Servers

Field	Description
IP Address Type	The IP address type (IPv4 or IPv6) of the peer.
Name or IP Address	The name or IP address of the peer.
Mode	The association mode of the NTP server, with values coded as follows: Peer - A host operating in this mode sends periodic messages regardless of the reachability state or stratum of its peer. By operating in this mode the host, usually a LAN workstation, announces its willingness to be synchronized by, but not to synchronize the peer. Server - This type of association is ordinarily created upon arrival of a client request message and exists only in order to reply to that request, after which the association is dissolved. By operating in this mode the host, usually a LAN time server, announces its willingness to synchronize, but not to be synchronized by the peer.
Preferred	Specifies whether this peer is the preferred one over the others. By default, NTP chooses the peer with which to synchronize the time on the local system. If true, NTP will choose the corresponding peer to synchronize the time with. If multiple entries are true, NTP will choose the first one to be set.

NTP General

Field	Description
Leap	Two-bit code warning of an impending leap second to be inserted in the NTP timescale.
RootDelay	A signed fixed-point number indicating the total round-trip delay in seconds, to the primary reference source at the root of the synchronization subnet.
RootDispersion	The maximum error in seconds, relative to the primary reference source at the ro of the synchronization subnet.

Running Processes

Field	Description
Name	The name associated with this process. If the name is longer than 32 characters, it will be truncated to the first 31 characters, and a `*' will be appended as the last character to imply this is a truncated process name.
MemAllocated (B)	The sum of all the dynamically allocated memory that this process has received from the system. This includes memory that may have been returned.
CPU Time (us)	The amount of CPU time the process has used, in microseconds.

Show Startup/Running Config

Field	Description
Startup	Backs up startup configuration of the switch to another computer with the specified file name.
Running	Backs up running configuration of the switch to another computer with the specified file name.
TCP Timeout	The value (in seconds) to wait for establishing TCP connection before timing out. Valid values are 1 to 120. A timeout results in abortion of the back up action.
FileName	To specify the name of the file where backup details are stored.
Compress File	Check the **Compress File** check box to compress the backup log file.

Show EPLD Version

Field	Description
Image URI	URI of the image.
Result	Version of the the image specified in the URI.

Copy Flash Files

Field	Description
Direction	Specifies the direction for file transfer.
Protocol	The protocol to be used for copy.
ServerAddress	The server address to be used.
RemoteUserName	Remote user name for protocols FTP, SFTP, and SCP.
RemotePassword	Remote user password used by FTP, SFTP or SCP.
Server File	Server file name, either in Flash or on a server, depending on the type of copy command. Mandatory. For a copy from Flash: File name must be of the form [device>:][:] where is a value obtained from FlashDeviceName, is obtained from FlashPartitionName and is the name of a file in Flash. If you copy files using xFTP protocol, server files may need to be located in a path that is relative to xFTP root path. **Note** You may need to manually modify the file path if required.
Switch File	Switch file name. For a copy to Flash: File name must be of the form {device>:][:] where is a value obtained from FlashDeviceName, is obtained from FlashPartitionName and is any character string that does not have embedded colon characters.

Generate TAC Pac File

You can download Tac-Pac in .zip format file.

Field	Description
Protocol	
TCP Timeout	The value (in minutes) to wait for establishing TCP connection before timing out. Valid values are 1 to 60. A timeout results in abortion of the back up action.
Management Interface	Allows you to choose the type of interface. The available options are: • default • vrf management • vrf default
ServerAddress	The server address to be used.
UserName	Remote user name.
UserPassword	Remote user password
FileName	The name of the file where the show tech support information will be captured.

Show Tech Support

Field	Description
TCP Timeout	The number (in seconds) to wait for the CLI before timing out.
FileName	The name of the file where the show tech support information will be captured.
Compress File	Check this check box to compress the text file into a ZIP file.

Show Image Version

Field	Description
Image URL	The URL of the image.
Result	The version of the image at the specified URL.

Show Onboard Log

Field	Description
Filter Log By	
Module Number	Slot number of the card in the chassis.
Start Date	Specify a start time.
End Date	Specify an end time.
Capture Show Onboard Log Output to File	
TCP Timeout	Specify a time-out interval from the drop-down list.
FileName	Name of the log file.
Compress File	Check the **Compress File** check box to compress the log file.

Summary View

Field	Description
Description	An alias name for the interface, as specified by a network manager. For Port Channel and FCIP, this field will always show members if they are available. For FCIP, this field will show compress if compressed.
VSAN(s)	VSAN membership.
Mode	Operating mode of the port> (See Legend).

Field	Description
Connected To	Attached port. This could be a host, storage, or switch port. **Note** Device Manager connects and manages one switch at a time. If the switch with NPV switch connection information is stored in the core switch and the NPV switch is selected to view, the **Connected To** information will not be displayed.
Speed	Maximum bandwidth in Gbps.
Rx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Tx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Errors	Total number of Rx and Tx errors on the interface. Types of Rx errors include CRC errors, fragmented framed, unsupported class frames, runt frames, jabber frames, and giant Frames. Types of Tx errors are generally CRC errors, but these are rare. If the Errors field is not empty, there are probably Rx errors. For a more detailed breakdown of the error count, check the Monitor dialog box for appropriate interface.
Discards	Total number of Rx and Tx discards on the interface. Rx frames discarded are generally due to protocol errors. On rare occasions, a frame is received without any hardware errors, but a filtering rule set for the MAC address discards the frame due to a mismatch. Discarded Tx frames can be timeout frame discards (port is offline or not up), or timeout frames that are not sent back to the supervisor (class F/2 frames). If the Discards field is not empty, it is probably due to timeout frames.
Log	If checked, writes the record into the message log on each poll interval.

RLIR ERL

Field	Description
Vsan ID	VSAN Identifier of the port.
FC ID	Fibre Channel identifier of the subscribing Nx_Port.
Format	The device type for which the Nx_Port receives RLIR ELS."

Field	Description
RegType	The subscriber's registration type. • ConditionalRx - The Nx_Port will be the recipient of a link incident record only if no other recipients from the ERL on the VSAN is chosen. • AlwaysRx - The Nx_Port will be always chosen as the recipient of a link incident records.

Preferred Host

Field	Description
Vsan ID	VSAN Identifier of the port.
PreFcid	Preferred Fibre Channel identifier of the subscribing Nx_Port.

Preferred Path

Field	Description
Interface	Represents an interface on the local device on which the matched or classified frame will be forwarded.
VSAN Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map. Preference level, which indicates the metric or cost of the preferred path. The lower the number the higher the preference.
DestinationDomain	
FCID	The FC ID that needs to be matched with a source address in a frame for flow classification.
Description	
Primary ISL	
Secondary ISL	

Edit iSCSI Advertised Interfaces

Field	Description
Num	The number of the iSCSI target.
Interface	The interface over which the target is to be advertised.

DNS General

Field	Description
Enable	Enables or disables DNS configuration.
Domain Name	The name of the domain where the DNS server is enabled.

DNS Servers

Field	Description
IP Address	The IP Address of the DNS server.

Cisco Fabric Services (CFS) Features

Field	Description
Globally Enabled	Check this box to allow CFS on this switch to distribute feature configurations to other switches. Uncheck the box to prevent CFS from distributing the configuration to other switches.
Feature	The name of the CFS-capable feature.
Status	Status of the CFS-capable feature.
Command	The action to be triggered for the feature. Actions include: • noop - No operation. • enable - Enable CFS distribution on the switch. • disable - Disable CFS distribution on the switch. • commit - Commit changes made since the session began. • abort - Discard changes made, and close the session. • clear - Discard changes made without closing the session.
Type	The last CFS feature scope type used.
VSAN Id	The ID of the VSAN on which this feature is running.
RegionId	The distribution region ID that this CFS capable feature maps to. This region is required to be defined prior to its usage.
View Config Changes As	Determines whether to view the changes as running or pending. A pending configuration exists until a Commit or Abort action is triggered for that feature. If the value is running then all subsequent configuration retrieval for this feature will be from the running configuration on the local device. If the value is pending then all subsequent configuration retrieval for this feature will be from the pending configuration on the local device.
LastCommand	The last action performed on this feature.
Result	Result of the action performed on the CFS-capable feature.
Scope	The value of this object represents the attributes of a CFS-capable feature as registered with the CFS infrastructure. • fcFabric - indicates that the CFS based distribution for a feature spans the entire FC (Fibre Channel) fabric • ipNetwork - indicates that the CFS based distribution for a feature spans the entire IP network • vsanScope - indicates that the CFS based distribution for a feature is done on per VSAN basis and restricted to a specific VSAN in a FC (Fibre Channel) fabric

Field	Description
PendingConfOwnerAddr	The address of the device in the fabric where the pending configuration exists for the feature.
Lock Owner Switch	The address of the device in the fabric where the pending configuration exists for the feature within this scope.
Lock Owner UserName	The name of the device in the fabric where the pending configuration exists for the feature within this scope.
Merge Status	The result of the last fabric merge for this feature within the context of the combination of scope type and scope value in the system. The following are the results: • Success—Fabric merge completed successfully. • InProgress—Fabric merge in progress. You may get this status when the local device that is a part of fabric engaged in the process of merging with another fabric. • Failure—Fabric merge failed. • Waiting—Waiting for existing merge to complete while the conflicts are being cleared. You may get this status when the local device that is a part of fabric waiting for any conflicts to be resolved before initiating a new instance of fabric merge. • Other—None of the other values of this enumeration.
Master	Select the CFS Master switch.

Cisco Fabric Services (CFS) IP Multicast

Field	Description
IP Address Type	The IP address type (IPv4, IPv6, or DNS).
Multicast Address Domain	The multicast address domain to which the CFS distribution is restricted. There is a default multicast address for both IPv4 and IPv6 through which the keep-alive messages are sent and received to discover the CFS capable switches over IP. All switches with similar multicast address form one CFS-over-IP fabric. The default multicast address for IPv4 is 239.255.70.83 and range supported is [239.255.0.0 - 239.255.255.255] The default multicast address for IPv6 is ff13::7743:4653 and the supported range is [ff13::0000:0000 - ff13::ffff:ffff]
Action	Specifies the current operating mode employed in CFS for distribution over the corresponding type of Internet address. By setting the value of this object to 'enable', CFS will enable its capability to distribute the application data across the fabric over the corresponding type of Internet address. By setting the value of this object to 'disable', CFS will disable its capability to distribute the data across the fabric over the corresponding type of Internet address.

Cisco Fabric Service (CFS) IP Static Peers

Field	Description
IP Static Peer	Specifies the address of a CFS peer device intended for distribution.
DiscStatus	Specifies a a user defined peer device intended for CFS distribution.

Cisco Fabric Services (CFS) Feature by Region

Field	Description
Feature	Identifies the name of a CFS-capable feature within a distribution region.
RegionId	Identifies a CFS distribution region.

Cisco Fabric Services (CFS) All Region

Field	Description
RegionId	Identifies a CFS distribution region.

Cisco Fabric Services (CFS) Owner

Field	Description
Feature, VSAN	The name of the CFS-capable feature, and the VSAN in which the feature is enabled or committed.
Name or IP Address	The name or IP address of the switch on which the feature is enabled or committed.
UserName	The name of the user who enabled or committed the feature.
Type	The last CFS feature scope type used.

Cisco Fabric Services (CFS) Merge

Field	Description
Feature	The name of the CFS-capable feature.
CFS Merge Status Value	The result of the last fabric merge that occurred.

Logs

SysLog (Since Reboot)

Note To see the latest logs, please close and launch the Log dialog. 'Refresh' option is not available for page by page dialog.

Field	Description
Switch Time	The local time on the switch.
Facility	Name of the facility that generated the message.
Severity	The severity of the message.
Event	The name of the event being logged
VSAN Id	The VSAN on which the event occurred.
Host Time	The local time on the host.
Description	A description of the event being logged.

SysLog (Severe Events)

Field	Description
Switch Time	The local time on the switch.
Facility	Name of the facility that generated the message.
Severity	The severity of the message.
Event	The name of the event being logged
VSAN Id	The VSAN on which the event occurred.
Host Time	The local time on the host.
Description	A description of the event being logged.

Accounting Log

Note To see the latest logs, please close and launch the Log dialog. 'Refresh' option is not available for page by page dialog.

Field	Description
Switch Time	The local time on the switch.

Field	Description
Action	The action that occurred (start, stop, or update).
Protocol & Source	The protocol and the IP address of the source switch.
User	The name of the user.
Description	A description of the action, if applicable.

Switch Logging

Field	Description
ConsoleEnable	Indicate whether the Syslog messages should be sent to the console.
ConsoleMsgSeverity	Minimum severity of the message that are sent to the Console.
TerminalEnable	Indicate whether the Syslog messages should be sent to the terminals.
TerminalMsgSeverity	Minimum severity of the message that are sent to the terminals.
LinecardEnable	Indicate whether the Syslog messages should be generated at the line cards.
LinecardMsgSeverity	Minimum severity of the message that are sent from linecards.
LogFileMsgSeverity	Minimum severity of the message that are sent to the log file.
SyslogLogFileName	Name of file to which the Syslog messages are logged.

Syslog Severity Levels

Field	Description
Facility	Batch process that generates messages.
Severity	Minimum severity of the message that are generated by this Syslog message facility.

Syslog Servers

Field	Description
IPAddress Type	The IP address type (IPv4, IPv6, or DNS).
Name or IP Address	The address of the Syslog server.
MsgSeverity	Minimum severity of the message that are sent to this Syslog ser
Facility	The facility to be used when sending Syslog messages to this ser

End Devices - Hosts

Field	Description
Host Enclosure	Name of the host enclosure
Name	Name of the VMware

Field	Description
IP Address	IP Address of the VMware
CPU Count	CPU Count of the VMware
Memory Size	Memory Size of the VMware
Status	Current status of the VMware.
OS	OS of the VMware.
Data Store	Name of the VMware datastore.
Last Update Time	Time at which the DCNM-SAN Server last updated the VMware.

Intelligent Features – Summary

Field	Description
Switch	IP address of the switch.
Module	Name of the module.
Name	Name of the switch.
IOA	Display enabled if the IOA feature is enabled. The field will be blank i disabled.
DMM	Display enabled if the DMM feature is enabled. The field will be blank disabled.
SANTap	Display enabled if the SANTap feature is enabled. The field will be bla disabled.

Data Mobility Manager – Modules

Field	Description for a Job Row	Description for a Session
Name	The name of the job.	This field is blank.
ID	System-assigned unique identifier for the job.	The session number with
Mode	Server mode or storage mode.	This field is blank.
Existing Storage	Alias name of the port on the existing storage.	LUN number on the exist
New Storage	Alias name of the port on the new storage.	LUN number on the new
Status	Status of the job. A created or scheduled job has not yet started. An in-progress job is currently performing the migration. A completed or verified job has finished successfully. A stopped, failed or reset job has finished unsuccessfully.	Status of the session.

Field	Description for a Job Row	Description for a Session Ro
Time	Date and time that the job is scheduled to start. This field is blank if the job has not been scheduled. If the job is in progress, this field displays the date and time that the job started.	If the session is in progress, t displays the estimated durati remaining until the session c Otherwise, the field is blank.
SSM1	Switch number and slot of the SSM executing the migration job.	Displays **On SSM 1** if the s executing on SSM 1.
SSM2	Switch number and slot of the SSM executing the migration job.	Displays **On SSM 2** if the s executing on SSM 2.
Type	Online or offline migration.	This field is blank.
Rate	Best effort, slow, medium or fast. You set the rate when you configure the migration job.	This field is blank.

Storage Media Encryption

Members

Field	Description
Cluster	SME cluster name.
State	The operational state of the SME cluster.
Master	Identifies the SME cluster master's IP address.
Members	Identifies the IP address of the switch that is a member of the SME cluster.
IsLocal?	Identifies if the switch is a local or remote member of this cluster.

Interfaces

Field	Description
Cluster	Identifies the cluster to which this SME interface belongs.
Interfaces	Identifies the SME interface.
State	Operational state of this SME interface.

Hosts

Field	Description
Host	Fibre-channel port name (P_WWN) of the host Nx_Port.
Cluster	Identifies the cluster to which this host port belongs.

SSM Features

Summary

Field	Description
Switch	Name of the switch on the intelligent module.
Module	Slot number of the intelligent module.
Name	Name of the intelligent module.
IOA	IOA state of the intelligent module.
DMM	DMM state of the intelligent module.
SANTap	SANTap state of the intelligent module.
SE	SE state of the intelligent module.

FCWA

Field	Description
Flow Id	Represents the flow identifier.
Init WWN	Represents the pWWN of the initiator in the flow.
Init VSAN	The VSAN ID of the initiator on which the flow is configured.
Target WWN	Represents the pWWN of the target in the flow.
TargetVSAN	The VSAN ID of the target on which the flow is configured.
WriteAcc	Specifies if write-acceleration feature is enabled for this flow. If set to true it is enabled. If set to false, it is disabled.
BufCount	It specifies the number of buffers to be used for write-acceleration.
Stats Enable	Specifies if the statistics gathering needs to be enabled for this flow. If set to true, then it is enabled. If it is set to false, then it is disabled.
Stats Clear	Assists in clearing the statistics for this flow.
Init Verification	The verification status of the initiator device corresponding to the SCSI flow.
Init Module	The status of the linecard where the SCSI flow initiator device is located.
Target Verification	The verification status of the target device corresponding to the SCSI flow.
Target Module	The status of the linecard where the SCSI flow target device is located.

SSM

Field	Description
StartPort, EndPort, Feature	A table containing feature related information for interfaces. This table gives a list of interfaces that are assigned to different features. The interfaces supported are of the type Fibre Channel.
PartnerImageURI	A collection of objects related to SSM Feature to interface mapping.

MSM

Field	Description
Switch	Name of the switch on the MSM module.
Module, StartNode, EndNode, Feature	A table containing the feature related information, such as the MSM module number, the node range that are assigned to different features.



Note The difference between MSM (Multiservice Modules) and SSM (Services Module) is that SSM could enable the features per port range on a card. For MSM you have to enabled it on the whole card.

SANTap CVT

Field	Description
Node WWN	Represents the node world wide name of the CVT created on the module.
Port WWN	Represents the port world wide name of the CVT created on the module.
Name	The administratively assigned name for this CVT.

SANTap DVT

Field	Description
VSAN Id, Port WWN	Represents the port world wide name of the created DVT. It will be the same as the port world wide name of the real target for which data is to be replicated.
Interface	Represents the port on the module where the DVT will be created.
Target VSAN Id	Represents the VSAN of the real target for which this DVT is being created.
Name	The administratively assigned name for this DVT.
LUNSize Handling	Indicates whether the DVT should use the real target LUN size for the virtual LUN or the max LUN size supported which is 2TB.
IO Timeout (sec)	Represents the IO timeout value associated with the DVT. This object should be set during the DVT creation time and cannot be modified later.
Target IO Timeout (sec)	Represents the target IO timeout value associated with the DVT.

NASB

Field	Description
Control	Specifies the device type for the LUNs exposed by the TPC target. A value of 1 sets the device type to the default value of disk. A value of 2 sets the device type to storage array controller. Other values are reserved for future changes.
Multiple	Specifies whether the TPC target is operating in a single LUN or multi-LUN mode. A value of 1 sets the default mode which is single LUN. A value of 2 sets multi LUN mode in which the TPC target exposes 10 LUNs.

NASB Target

Field	Description
Module, VSAN Id, Processor Id	The unique ID number associated with the TPC target. This ID number is unique within the VSAN in which the TPC target is configured.
Virtual Target Node WWN	The TPC target's node world wide name.
Virtual Target Port WWN	The TPC target's port world wide name.
State	The current state of the TPC target.
XCOPY Num	The total number of xcopy commands processed by the TPC target since the module on which this target has been configured has been online.
XCOPY MinData (KB)	The smallest amount of data in kilobytes transferred by the TPC target in a single xcopy command since the module on which this target has been configured has been online.
XCOPY MaxData (KB)	The largest amount of data in kilobytes transferred by the TPC target in a single xcopy command since the module on which this target has been configured has been online.
XCOPY Avgthruput (KBps)	The average kilobytes per second throughput of the TPC target in processing the xcopy commands.

Virtual Initiator

Field	Description
Processor Id	The DPP ID.
Control	If false, it’s the data path. If true, it’s the control path.

DMM Rate

Field	Description
Fast(MBps)	Specifies the migration rate value for the fast attribute for a specific module.
Medium(MBps)	Specifies the migration rate value for the medium attribute for a specific module.
Slow(MBps)	Specifies the migration rate value for the slow attribute for a specific module.

FCWA Config Status

Field	Description
Overall	The configuration status for write-acceleration feature for this flow.
Initiator	The initiator configuration status for write-acceleration feature for this flow.
Target	The target configuration status for write-acceleration feature for this flow.

Statistics Status

Field	Description
Overall	The configuration status for statistics feature for this flow.
Initiator	The initiator configuration status for statistics feature for this flow.
Target	The target configuration status for statistics feature for this flow.

Statistics I/O Traffic

Field	Description
IOs Read	The total number of SCSI read operations on this LUN on this flow.
IOs Write	The total number of SCSI write operations on this LUN on this flow.
Blocks Read	The total number of blocks that have been read on this LUN on this flow.
Blocks Write	The total number of blocks that have been written on this LUN on this flow.
Bytes Rx	The total number of octets received in link-level frames on this LUN on this flow.
Bytes Tx	The total number of octets transmitted in link-level frames on this LUN on this flow.
Frames Rx	The total number of link-level FC frames received on this LUN on this flow.
Frames Tx	The total number of link-level frames transmitted on this LUN on this flow.

Statistics I/O Traffic Details

Field	Description
Timeouts Read	The total number of SCSI read operations that have timed out on this LUN on this flow.
Timeouts Write	The total number of SCSI write operations that have timed out on this LUN on this flow.
MaxBlocks Read	The maximum number of blocks read across all read operations on this LUN on this flow.
MaxBlocks Write	The total number of blocks that have been written on this LUN on this flow.
MaxTime Read	The maximum response time over all read operations on this LUN on this flow.

Field	Description
MaxTime Write	The maximum response time over all write operations on this LUN on this flow.
MinTime Read	The minimum response time over all read operations on this LUN on this flow.
MinTime Write	The minimum response time over all write operations on this LUN on this flow.
Active Read	The number of read operations that are currently active on this LUN on this flow.
Active Write	The number of write operations that are currently active on this LUN on this flow.

Statistics SCSI Commands

Field	Description
TestUnitRdys	The number of test unit ready SCSI commands sent on this LUN on this flow.
RepLuns	The number of report LUN SCSI commands sent on this LUN on this flow.
Inquirys	The number of SCSI inquiry commands sent on this LUN on this flow.
RdCapacitys	The number of read capacity SCSI commands sent on this LUN on this flow.
ModeSenses	The number of mode sense SCSI commands sent on this LUN on this flow.
ReqSenses	The number of request sense SCSI commands sent on LUN on this flow.

Statistics SCSI Errors

Field	Description
BusyStatuses	The number of busy SCSI statuses received on this LUN on this flow.
StatusResvConfs	The number of reservation conflicts SCSI status received on this LUN on this flow.
TskSetFulStatuses	The number of task set full SCSI statuses received on this LUN on this flow
AcaActiveStatuses	The number of ACA active statuses received on this LUN on this flow.

Statistics SCSI Sense Errors

Field	Description
NotRdyErrs	The number of NOT READY SCSI SENSE key errors received on this LUN on this flow. This indicates that the logical unit being addressed cannot be accessed.
MedErrs	The number of MEDIUM ERROR SCSI SENSE key errors received on this LUN on this flow. This indicates that the command terminated with a non-recovered error condition possibly caused by a flaw in the medium.

Field	Description
HwErrs	The number of HARDWARE ERROR SCSI SENSE key errors received on this LUN on this flow. This indicates that the target detected a non-recoverable hardware failure.
IllReqErrs	The number of ILLEGAL REQUEST SCSI SENSE key errors received on this LUN on this flow.
UnitAttErrs	The number of UNIT ATTENTION SCSI SENSE key errors received on this LUN on this flow.
DatProtErrs	The number of DATA PROTECT SCSI SENSE key errors received on this LUN on this flow.
BlankErrs	The number of BLANK CHECK SCSI SENSE key errors received on this LUN on this flow.
CpAbrtErrs	The number of COPY ABORTED SCSI SENSE key errors received on this LUN on this flow.
AbrtCmdErrs	The number of ABORTED COMMAND SCSI SENSE key errors received on this LUN on this flow.
VolFlowErrs	The number of VOLUME OVERFLOW SCSI SENSE key errors received on this LUN on this flow.
MiscmpErrs	The number of VOLUME OVERFLOW SCSI SENSE key errors received on this LUN on this flow.

Compact

Field	Description
Device	This is the flash device sequence number to index, used within the table of initialized flash devices. The lowest value should be 1. The highest should be less than or equal to the value of the ciscoFlashDevicesSupported object
Partition	This is the flash partition name used to refer to a partition by the system. This can be any alpha-numeric character string of the form AAAAAAAAnn, where A represents an optional alpha character and n a numeric character. Any numeric characters must always form the trailing part of the string. The system will use only the numeric portion to map to a partition index. Flash operations get directed to a device partition based on this name. The system has a concept of a default partition. This would be the first partition in the device. The system directs an operation to the default partition whenever a partition name is not specified. The partition name is therefore mandatory except when the operation is being done on the default partition, or the device has just one partition (is not partitioned).
Size	This is the flash partition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize.