The bridge to possible

Monitoring and Alerting in SAN Fabric with Cisco MDS 9000 Series Switches and NDFC

This document provides step-by-step guidance to set up automated monitoring and alerting in a Cisco SAN fabric. The primary audience is first-time users of Cisco MDS 9000 switches, NX-OS, and Cisco Nexus Dashboard Fabric Controller (NDFC) SAN Controller but experienced users can also benefit from it.

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

Scope

The command outputs, screenshots, and capabilities that are described in this document are based on Cisco NX-OS 9.2(1) for MDS 9000 switches, Nexus Dashboard (ND) 2.2(1h), and Nexus Dashboard Fabric Controller (NDFC) 12.1.1e. Although the procedures and recommendations that are outlined in this document apply to most NX-OS releases for MDS 9000 switches and NDFC, we recommend referring to the release notes and the configuration guides for up-to-date information. Also, it is an overview document, primarily aimed at new users. For details on specific topics, refer to the white papers and configuration guides that are listed in the references section.

Overview

Cisco MDS 9000 switches have hardware and software sensors to collect metrics and logs in real time. The hardware sensors are integrated within all the components. For example:

1. Sensors on port-ASICs collect metrics from wire-data for congestion monitoring, utilization, link-integrity, and so on.
2. Sensors on port-modules, supervisor modules, and fabric modules monitor general health, temperature, hardware failures, and so on.
3. Sensors on power supplies, fan trays, and other hardware components monitor environmental conditions.

It is not an exhaustive list and is provided here for reference only. Cisco NX-OS collects the sensor data and listens for any events that are generated by the hardware sensors. Based on the severity, the events are categorized under various levels, for example, Emergency, Critical, Informational, and so on. Finally, the events can be sent to remote monitoring systems through notification mechanisms, for example, SNMP, Syslog, and Call Home.

While Cisco NX-OS manages, monitors, and generates alerts from a single switch, Cisco NDFC SAN Controller can do the same for multiple switches and fabrics. It offers an intuitive HTML5-based web UI to monitor the underlying SAN fabric. NDFC SAN Controller receives the hardware and software sensor data collected by Cisco NX-OS and MDS 9000 switches and maintains long-term trends and seasonality. Also, NDFC SAN Controller receives event notifications that are generated by the switches and can forward them to a compatible third-party application.

In addition to monitoring the health of a SAN fabric, it is possible to monitor the storage performance using Cisco SAN Analytics. The MDS 9000 switches inspect the end-to-end SCSI and NVMe transactions to collect performance metrics in real time. Finally, the metrics are exported over streaming telemetry to SAN Insights, which is an analytics engine within NDFC SAN Controller.

Introduction to Nexus Dashboard and NDFC

Nexus Dashboard (ND) is a hosting platform, whereas Nexus Dashboard Fabric Controller (NDFC) is a service or application that's hosted on ND. NDFC is the successor of the Data Center Network Manager (DCNM). ND and NDFC provide many benefits such as active-active clustering, higher scale, anomaly detection, event analytics, and so on, and thus we recommend upgrading from DCNM to NDFC.

For more details on ND and NDFC, refer to the references section.

Access Mechanisms in a Cisco SAN Fabric

The access mechanisms in a Cisco SAN fabric that are built using MDS 9000 switches can be used for the following functions.

- Configuration
- Monitoring
- Event notifications

The following subsections provide an overview of these functions.

Configuration

This section provides an overview of the commonly used mechanisms to make configuration changes on the MDS 9000 switches. Detailed configuration options are outside the scope of this document. For more details, refer to the references section to access the Cisco MDS 9000 Configuration guides.

Configuring an MDS 9000 switch requires read-write access to it.

Command Line Interface (CLI)

CLI access is achieved over an SSH session to make configuration changes using the Cisco NX-OS commands. For example, the following snippet displays the steps to enable a Fibre Channel interface on MDS 9000 switches.

```
[user@~]%ssh -l admin <management_ip_address_of_the_switch>

User Access Verification

Password:

<snip>

MDS-9710# configure

Enter configuration commands, one per line. End with CNTL/Z.

MDS-9710(config)# interface fc1/1

MDS-9710(config-if)# no shutdown

MDS-9710(config-if)# end

MDS-9710#
```

The preceding snippet shows accessing the NX-OS CLI from a Linux host using SSH. The same can be achieved from other types of hosts (for example, Windows) and SSH clients (for example PuTTY).

SNMP

It is possible to make configuration changes to MDS 9000 switches using SNMP MIBs with read-write access. For example, SNMP object zoneDefaultZoneBehaviour (OID: 1.3.6.1.4.1.9.9.294.1.1.1.1.1) can change the behavior of the default zone in a VSAN.

For more details, refer to the references section to access the Cisco MDS 9000 Series MIB Quick Reference Guide.

NX-API

NX-API provides programmable access to the MDS 9000 switches over HTTP or HTTPS. NX-API can be used to make configuration changes on the switches to achieve automation and programmability.

For more details, refer to the references section to access the Cisco MDS 9000 Series Programmability Guide.

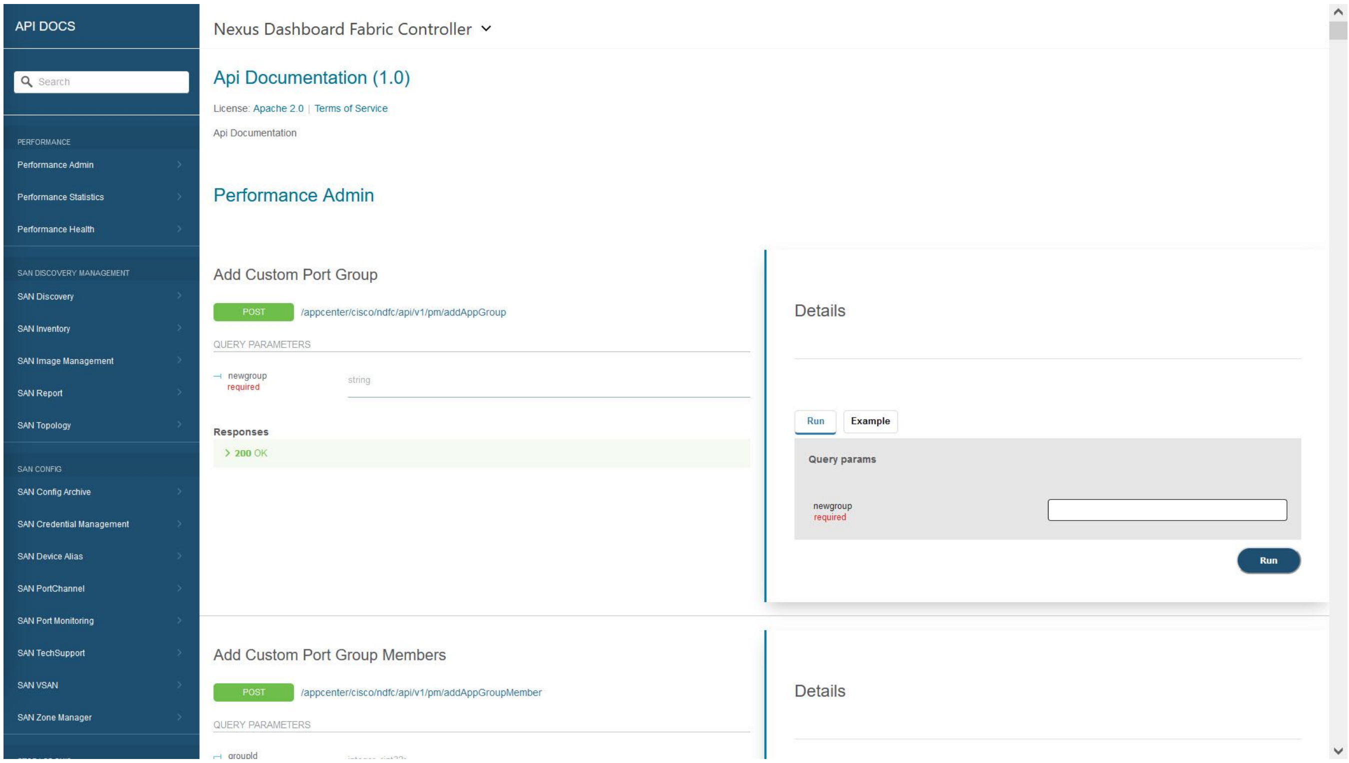
MDS 9000 Software Development Kit (SDK)

The SDK provides programmable access to the MDS 9000 switches. It leverages NX-API and CLI to communicate with the switches while abstracting the lower-level details from an end user. This SDK simplifies the rapid development of automation and programmable infrastructure to configure the SAN fabrics that are built using MDS 9000 switches.

For more details, refer to the references section to access the MDS SDK repository on GitHub and its documentation.

NDFC REST APIs

Cisco NDFC REST APIs enable programmable access to the managed SAN fabric. API information can be found either on **Nexus Dashboard** (or **NDFC**) > **Help Center** > **REST API** under the Programming options or from below URL https://[ND-mgmt-ip]/apidocs/ directly. Select **Nexus Dashboard Fabric Controller** from the drop-down list on the top of the page.



Api Documentation (1.0)

License: Apache 2.0 | Terms of Service

Api Documentation

Performance Admin

Add Custom Port Group

POST /appcenter/cisco/ndfc/api/v1/pm/addAppGroup

QUERY PARAMETERS

newgroup required string

Responses

200 OK

Details

Query params

newgroup required

Add Custom Port Group Members

POST /appcenter/cisco/ndfc/api/v1/pm/addAppGroupMember

QUERY PARAMETERS

groupId

Details

Figure 1. NDFC REST API

For more details, refer to the references section to access the Cisco ND/NDFC REST API Reference Guide.

Monitoring

This section provides an overview of the commonly used mechanisms to monitor the MDS 9000 switches. Monitoring an MDS 9000 switch requires read-only access to it.

Command Line Interface (CLI)

CLI access is achieved over an SSH session to monitor the hardware and the software components on MDS 9000 switches using the NX-OS *show* commands. For example, the following snippet displays the steps to monitor the input and output traffic rate on a Fibre Channel interface.

```
[user@~]%ssh -l admin <management_ip_address_of_the_switch>

User Access Verification

Password:

<snip>

MDS-9710# show interface fc1/1 counters brief


--------------------------------------------------------------------------------

Interface     Input (rate is 5 min avg)    Output (rate is 5 min avg)

          ----------------------------- -----------------------------

          Rate   Total         Rate   Total

          MB/s   Frames        MB/s   Frames

--------------------------------------------------------------------------------

fc1/1       182   1187625867862      245   181299685899

MDS-9710#
```

The preceding snippet shows accessing the NX-OS CLI from a Linux host using SSH. The same can be achieved from other types of hosts (for example, Windows) and SSH clients (for example PuTTY).

SNMP

SNMP provides an extensive set of MIBs to monitor hardware and software components on MDS 9000 switches. For example, SNMP object zoneNumber (OID: 1.3.6.1.4.1.9.9.294.1.1.6) can display the number of entries present in the zone table. Using SNMP, a remote monitoring agent can poll the switches (commonly known as SNMP polling) to monitor the switches. The frequency of polling the MDS 9000 switches depends upon the type of metric. For example, congestion (slow drain) metrics can be polled every few seconds, whereas memory utilization of a switch can be polled every few minutes.

For more details, refer to the references section to access the Cisco MDS 9000 Series MIB Quick Reference.

NX-API

NX-API provides programmable access to the MDS 9000 switches over HTTP or HTTPS. NX-API can be used to request the output of *show* commands in JSON or XML format. The recommended frequency of the request depends upon the type of metric. For example, congestion (slow drain) metrics can be requested every few seconds, whereas memory utilization of a switch can be requested every few minutes.

For more details, refer to the references section to access the Cisco MDS 9000 Series Programmability Guide.

MDS Software Development Kit (SDK)

The SDK provides programmable access to the MDS 9000 switches. It leverages NX-API and CLI to communicate with the switches while abstracting the lower-level details from an end user. This SDK simplifies the rapid development of automation and programmable infrastructure to monitor MDS 9000 fabrics.

For more details, refer to the references section to access the MDS SDK project on GitHub and its documentation.

Streaming Telemetry

Streaming Telemetry is a push mechanism for high-fidelity metric export from the MDS 9000 switches. The primary use-case is to export I/O flow metrics collected by Cisco SAN Analytics. For example, MDS 9700 directors running NX-OS 9.2(1) collect up to 70 metrics for 40,000 flows. This results in the export of 2.8 million metrics at every export interval of 30 seconds.

MDS 9000 switches support streaming telemetry using gRPC transport with (compact) GPB encoding. In addition to the I/O flow metrics collected by SAN Analytics, streaming telemetry can also export the interface metrics.

For more details, refer to the references section to access the Cisco MDS 9000 Series SAN Analytics and SAN Telemetry Streaming Configuration Guide.

NDFC APIs

It is possible to monitor various components of the managed SAN fabric using the NDFC REST APIs, for example, inventory, performance data, topology, and so on. API information can be found either on **Nexus Dashboard** (or **NDFC**) > **Help Center** > **REST API** under the Programming options or from below URL https://[ND-mgmt-ip]/apidocs/ directly. Select **Nexus Dashboard Fabric Controller** from the drop-down list on top of the page.

For more details, refer to the references section to access the Cisco ND/NDFC REST API Reference Guide.

Event notification

Cisco MDS 9000 switches can automatically send event notifications to a remote receiver in response to a local event.

It is possible to open a CLI session to MDS 9000 switches to display the events, as they are generated in real time. These events are called system messages. A limited number of system messages can be stored on the switch for a historic view. Although this approach is commonly used for active troubleshooting in real time, it is not strictly an unsolicited event notification mechanism to a remote agent.

For example, refer to the following snippet showing a system message when the operational state of an interface goes down.

```
2022 Apr 19 08:48:58 MDS-9710 %PORT-5-IF_DOWN_NONE: %$VSAN 1%$ Interface fc8/41 is down (None)
```

The printing of system messages on the console or terminal is disabled by default. To enable this functionality, use **`terminal monitor`** command.

A limited number of system messages are stored on the switch and can be displayed using the **`show logging [logfile | nvram]`** command, as shown in the following snippet.

```
MDS-9710# show logging nvram

2022 Apr 19 08:59:31 MDS-9710 %PLATFORM-2-PS_OK: Power supply 1 ok(Serial number DTM1626001B)
```

```
2022 Apr 19 08:59:31 MDS-9710 %PLATFORM-5-PS_STATUS: PowerSupply 1 current-status is PS_OK

2022 Apr 19 08:59:31 MDS-9710 %PLATFORM-2-PS_FANOK: Fan in Power supply 1 ok
<snip>
```

For more details, refer to the references section to access the Cisco MDS 9000 Series System Management Configuration Guide.

SNMP Traps and Informs

SNMP provides an extensive set of MIBs to notify a remote agent through traps and informs. These notifications are generated in response to a locally generated event. For example, SNMP object linkDown (OID: 1.3.6.1.2.1.11.0.2) is a trap to notify that the operational state of a switch port has gone down.

For more details, refer to the references section to access the Cisco MDS 9000 Series MIB Quick Reference.

Syslog

Events on MDS 9000 switch are logged as system messages carrying timestamp, device id, facility name, severity, and a text description of the event. These systems' messages can be sent to remote syslog servers.

The MDS 9000 switches support 8 levels of message severity, from level-0 (Emergency) to level-7 (Debug). By default, system messages with level-5 severity (Notifications) and lower are enabled. It is possible to customize the severity of the messages that are generated by a facility and, also control what is sent to a remote syslog server. For more details, refer to the references section to access the Cisco MDS 9000 Series System Management Configuration Guide.

Email

Critical events can be notified through emails, directly by the MDS 9000 switches using Call Home or by NDFC using event forwarding.

Call Home

MDS 9000 switches can send event notifications through email using the Call Home functionality.

For more details, refer to the references section to access the Cisco MDS 9000 Series System Management Configuration Guide.

NDFC Event Forwarding

NDFC acts as a centralized repository of all the events and can be the single source to generate emails to multiple destinations. The switches in the managed SAN fabric can send events to an NDFC server through any of the above-mentioned mechanisms, such as SNMP and Syslog. Based on the configured rule and filtering, NDFC can forward the events over email for urgent attention of the owners or for automated ticketing systems.

Best Practice

Use NDFC Event Forwarding to generate email notifications

Comparison and Usage recommendations

Choosing the correct mechanism for monitoring and event notification depends on the use-cases and the capability of the monitoring application. This section provides high-level guidelines about various available options.

Cisco SAN Fabric managed with NDFC

Cisco SAN fabric that is managed and monitored by NDFC is an end-to-end validated solution. The best monitored and notification mechanisms are used by default. For example, as of NDFC 12.1(1) and NX-OS 9.2(1):

1. Interface utilization is monitored using SNMP polling.
2. I/O flow metrics that are collected by SAN Analytics are received by streaming telemetry.
3. Events are received by SNMP traps or inform and Syslog.

The preceding is not an exhaustive list and is provided here for reference only.

Using Your Own or Third-Party Application

It is best to refer to the recommendations of the third-party vendor to choose the best metric export or notification mechanism. If you are building your app or customizing an existing app (for example, an open-source monitoring application), consider the following recommendations.

Feature Coverage

SNMP provides maximum coverage for monitoring and is widely supported by Cisco and third-party products. NX-API support was added on MDS 9000 switches in 2016. Commonly used features are available via NX-API at the time of writing this document, but the feature coverage is not as extensive as SNMP. Streaming telemetry supports the monitoring of I/O flow metrics and interface metrics only as of NX-OS 9.2(1) for MDS 9000 switches.

Performance

SNMP is known to be a resource-intensive protocol. The MDS 9000 switches have powerful CPUs. But high-frequency monitoring is best achieved by a newer and optimized mechanism like NX-API and streaming telemetry. It is fine to continue using SNMP with legacy applications because rewriting the application may not be worth the effort. However, for any newer implementations, we recommend using NX-API for high-frequency monitoring of the MDS 9000 switches.

Streaming telemetry is the best option to export millions of metrics with minimal load on the switch. But it requires a gRPC receiver which may not be worth the effort just for exporting interface metrics.

Industry-wide support

SNMP is widely supported. Newer monitoring applications support SNMP but also allow building custom receivers using the monitored agent APIs. NX-API can be used in such cases. Streaming telemetry is also a valid option, but it requires a dedicated gRPC receiver.

MDS 9000 switches, UCS Manager, and NDFC SAN Controller – Initial Setup

The initial setup of monitoring and alerting in a Cisco SAN fabric requires the following steps:

1. Set up MDS 9000 switches to be discovered by NDFC SAN Controller.

2. Set up UCS Manager to be discovered by NDFC SAN Controller. It is an optional step and is required only if you wish to monitor Cisco UCS Fabric Interconnect and servers using NDFC SAN Controller.
3. Set up NDFC SAN Controller.

The following subsections provide step-by-step details.

Initial setup of MDS 9000 switches and NX-OS before NDFC SAN Controller Discovery

As a first step, configure the network services like NTP, DNS, and so on, on the MDS 9000 switches. This step is important to keep correct timestamps in the outgoing event notifications, traffic utilization graphs on NDFC SAN Controller, streaming telemetry (if configured), and so on.

For more details on configuring the network services, refer to the references section to access the Cisco MDS 9000 Series Fundamentals Configuration Guide.

Best Practice

Use NTP to synchronize the clocks between the monitored SAN switches and the monitoring agent (NDFC).

Next, create snmp-user on MDS 9000 switches. NDFC SAN Controller requires the IP address of just a single switch (known as a seed switch) to discover the entire fabric but the user and the password must be the same on all the switches.

Cisco NDFC SAN Controller can monitor UCS Fabric Interconnects and the associated blade and rack servers when connected to a managed Cisco SAN fabric. This functionality requires the same snmp-user and password combination on the Cisco UCS Manager and SHA-AES authentication and Privacy mode. Due to this reason, we recommend using the same auth-privacy mode on the MDS switches also. Even if the SAN fabric may not have UCS servers connected today, it still is the best practice to avoid any changes in the future.

Best Practice

Use SHA-AES as authentication and privacy mode to discover SAN fabric via NDFC SAN Controller.

Creating a User on MDS Switches for NDFC SAN Controller Discovery

Use **snmp-server user** command to create a local user with SHA-AES authentication and Privacy mode. This user must have a **network-admin** role.

```
MDS-9710#configure

MDS-9710(config)#snmp-server user dcnmuser network-admin auth sha <> priv aes-128 <>

MDS-9710(config)#

MDS-9710(config)#end

MDS-9710# show running-config | inc dcnmuser

username dcnmuser password 5 $5$5Cht7P1y$ZaR6bDvAo5dSt7KUjr4H7qoaOQ/7cyUq98Av5k3jDF3 role
network-operator

username dcnmuser passphrase lifetime 269063912 warntime 279936932

snmp-server user dcnmuser network-admin auth sha 0x9eba83d512cd70bd34165e7f45af2962211c7be1
priv aes-128 0x9eba83d512cd70bd34165e7f45af2962211c7be1 localizedkey

MDS-9710#
```

Initial setup of Cisco UCS Manager before Discovering it by NDFC SAN Controller

NDFC SAN Controller can discover and monitor Cisco UCS Fabric Interconnects when connected to a managed Cisco SAN fabric. The discovery and monitoring are achieved via SNMP that is the same mechanism that is used to monitor the MDS 9000 switches. NDFC SAN Controller can monitor components beyond the Fabric Interconnects, for example, blade servers, vHBA, and vNICs. This enhanced monitoring is performed using UCS Manager APIs and requires a read-only user in Cisco UCS Manager. Overall, an SNMP user is required for the discovery and monitoring of the UCS Fabric Interconnects while a separate read-only user is required for monitoring vHBA and vNIC traffic.

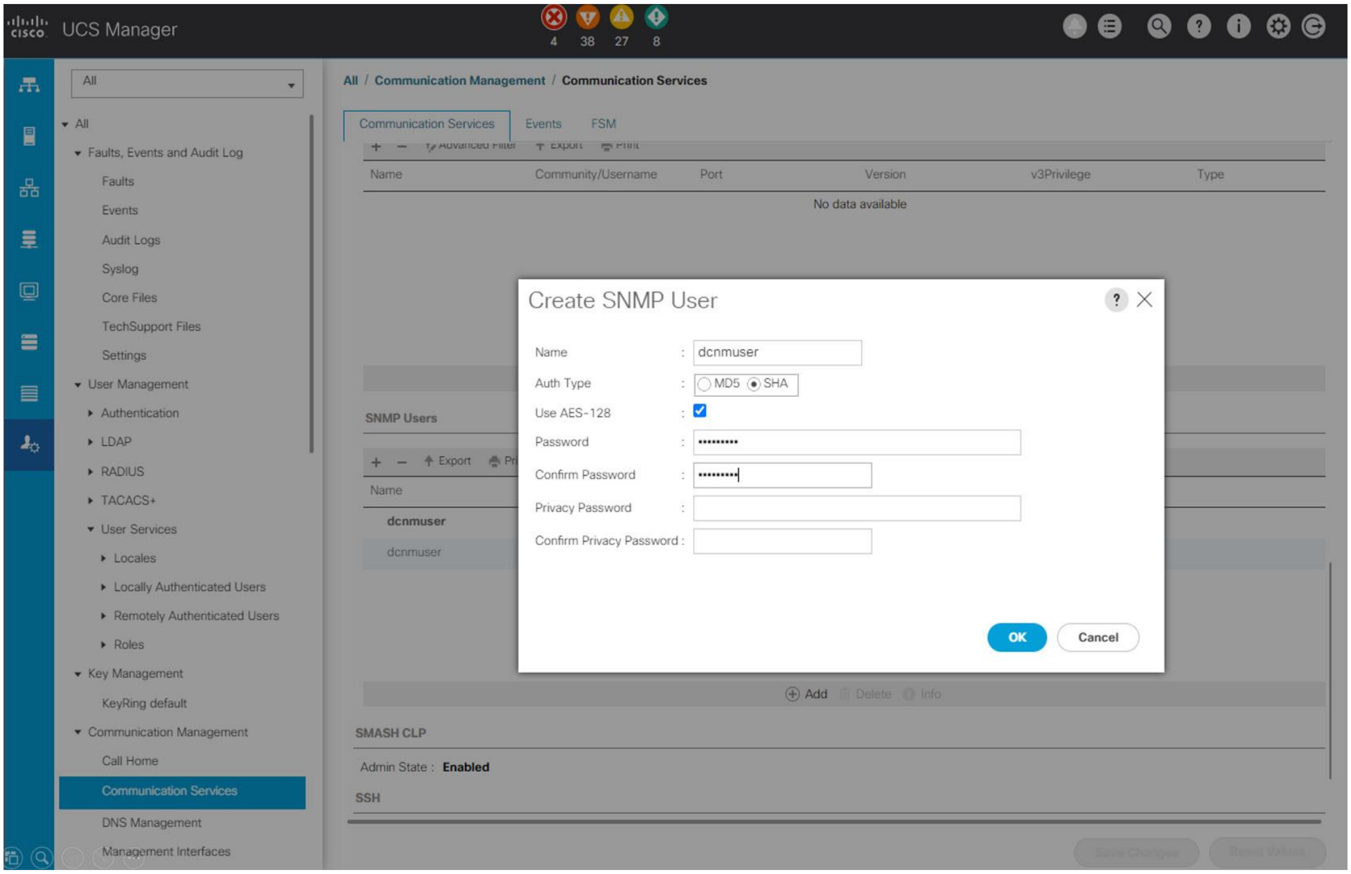
It is an optional step. Full functionality is available in NDFC SAN Controller if both the users are created and added correctly. If none of the users are created, NDFC SAN Controller can still discover the connected UCS Fabric Interconnects but is unable to show any more information on them. It is fine to reuse existing snmp-user and read-only user accounts if they exist on UCS Manager.

Before enabling the monitoring and alerting of a Cisco UCS domain, it is important to set up basic network services like NTP, DNS, and so on.

For more details, see references section to access the Cisco UCS Manager configuration guide.

Adding an SNMP User in Cisco UCS Manager

Navigate to **Admin tab > Communication Management > Communication Services**. Scroll down to the SNMP section and add a new SNMP user. For successful discovery by NDFC SAN Controller, it is mandatory to choose Auth Type as SHA and select the check box for AES-128. In some versions of UCS Manager, AES-128 is enabled by default. In such cases, no additional action is required by a user to select the Privacy mode.



Name	Community/Username	Port	Version	v3Privilege	Type
No data available					

SNMP Users

Name
dcnmuser
dcnmuser

Create SNMP User

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

SMASH CLP

Admin State : **Enabled**

Figure 2. Adding an SNMP user in Cisco UCS Manager

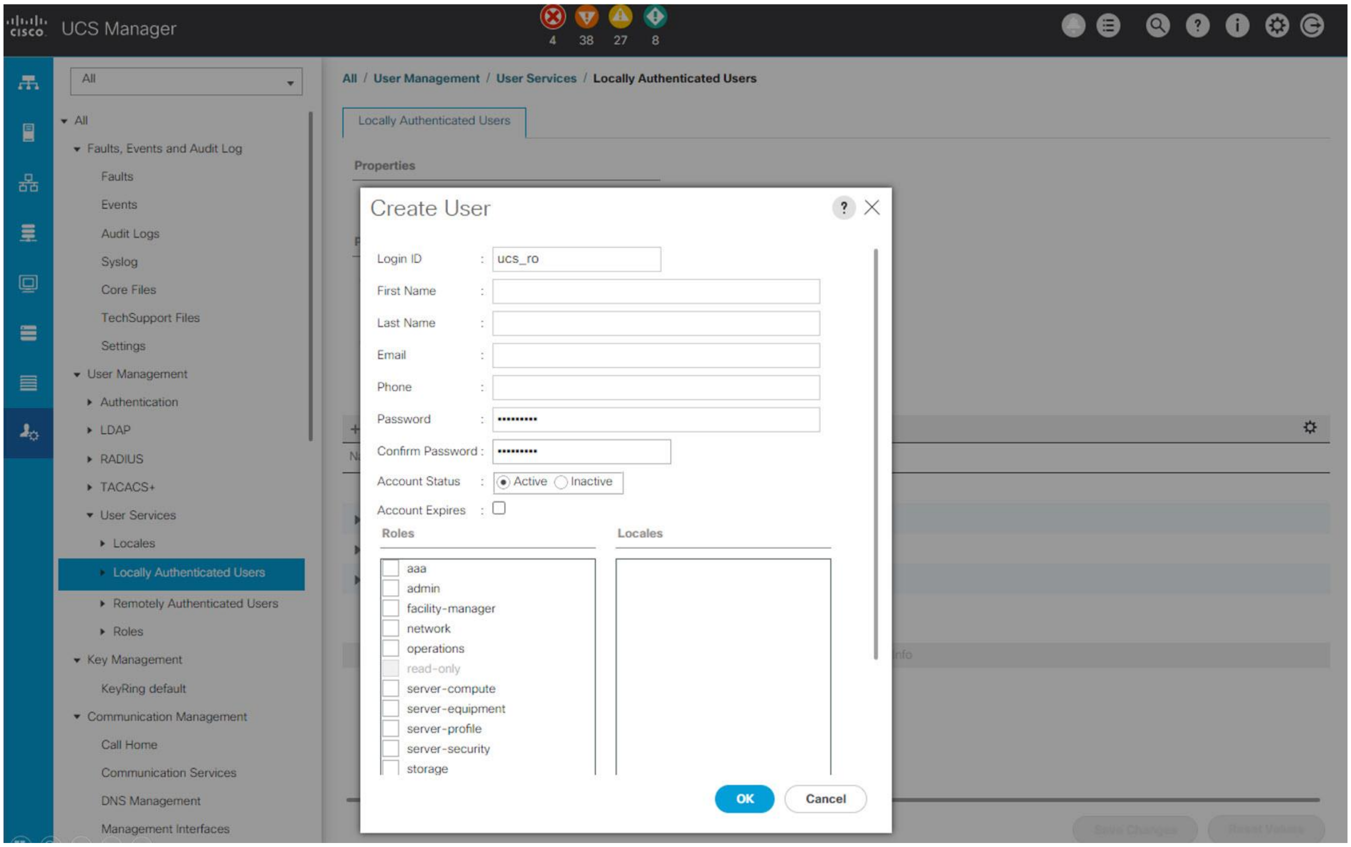
We recommend using different names for snmp-user and read-only user (for example, dcnmuser for SNMP access and ucs_ro for API access). This scheme helps in cleaner implementation and better troubleshooting if discovery does not work correctly in the future.

Best Practice

For NDFC SAN Controller discovery and monitoring of UCS, use different name strings for snmp-user and read-only user.

Adding a read-only User in Cisco UCS Manager

Navigate to **Admin** tab. Choose **User Management > User Services**. Go to locally authenticated users and add a new user. In Cisco UCS Manager, a user with no special roles is a read-only user.



Create User

Login ID : ucs_ro
First Name :
Last Name :
Email :
Phone :
Password : •••••••••
Confirm Password : •••••••••
Account Status : ● Active ○ Inactive
Account Expires : □

Roles
□ aaa
□ admin
□ facility-manager
□ network
□ operations
□ read-only
□ server-compute
□ server-equipment
□ server-profile
□ server-security
□ storage

Locales

Figure 3. Adding a read-only user in Cisco UCS Manager

Initial Setup of NDFC

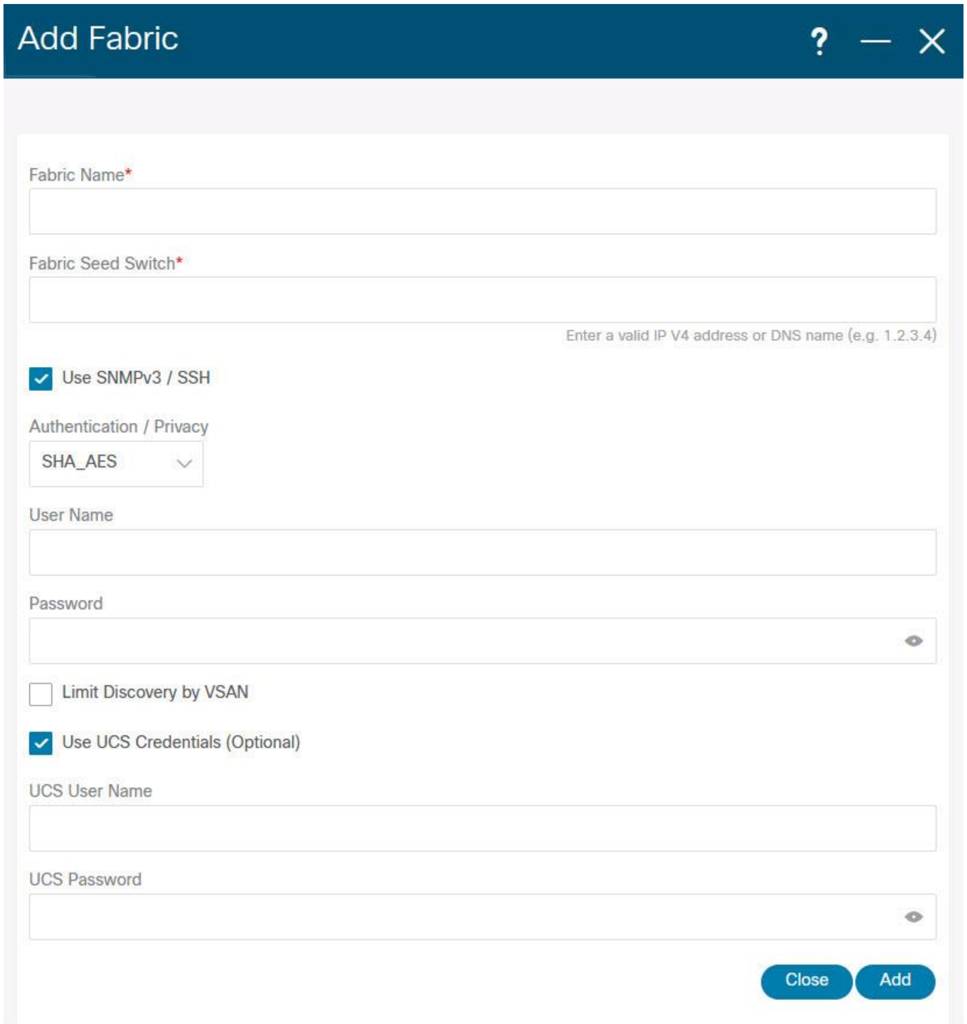
Before discovering a SAN fabric, Nexus Dashboard (ND) and NDFC must be correctly installed and set up for network services like DNS, NTP, and so on. For more details on ND and NDFC installation, refer to the references section to access the Cisco ND and NDFC Installation and Upgrade Guide for SAN Deployment.

Discovering a SAN fabric

Log in to NDFC SAN Controller. Navigate to Topology and click **Actions > Add Fabric**. In the **Fabric Name** field, enter an appropriate and relevant name for your fabric. In the Fabric Seed switch text box, enter the IP address of any switch in the fabric. Select SHA_AES from the Auth-Privacy drop-down list as per the above-mentioned best practice. This step assumes that the username and the password on the MDS 9000 switches have been created using the same auth and Privacy mode. Enable the ‘Use UCS Credentials’ check box to display text boxes for UCS username and UCS password. Under the UCS username, enter the read-only user (not the snmp-user) created in UCS Manager. The snmp-user in Cisco UCS Manager must be the same user as created on the MDS 9000 switches and already entered in the username field.

Click **Add**. It takes a few minutes to completely discover the fabric. Repeat the preceding steps for adding multiple fabrics.

Discovering a SAN fabric is a mandatory step for NDFC SAN Controller to manage that fabric. Adding UCS is optional (but highly recommended) and is required only if you wish to monitor the Fabric Interconnects, Servers, vHBA, and vNIC using NDFC SAN Controller.



Add Fabric

Fabric Name*

Fabric Seed Switch*

Enter a valid IP V4 address or DNS name (e.g. 1.2.3.4)

☑ Use SNMPv3 / SSH

Authentication / Privacy

SHA_AES

User Name

Password

□ Limit Discovery by VSAN

☑ Use UCS Credentials (Optional)

UCS User Name

UCS Password

Figure 4. Discovering a SAN fabric and the connected UCS domains in NDFC SAN Controller

Adding VMware vCenter

NDFC SAN Controller can detect the connected hypervisors (ESXi) and the hosted VMs. Navigate to **Virtual Management > Virtual Infrastructure Manager**, click **Actions > Add Instance** to add VMware vCenter Server. To view the connected hosts, navigate to **Dashboard > Hosts**. Select a hypervisor host to display the hosted VMs. Adding VMware vCenter to NDFC is an optional step but highly recommended.

Adding Storage Arrays

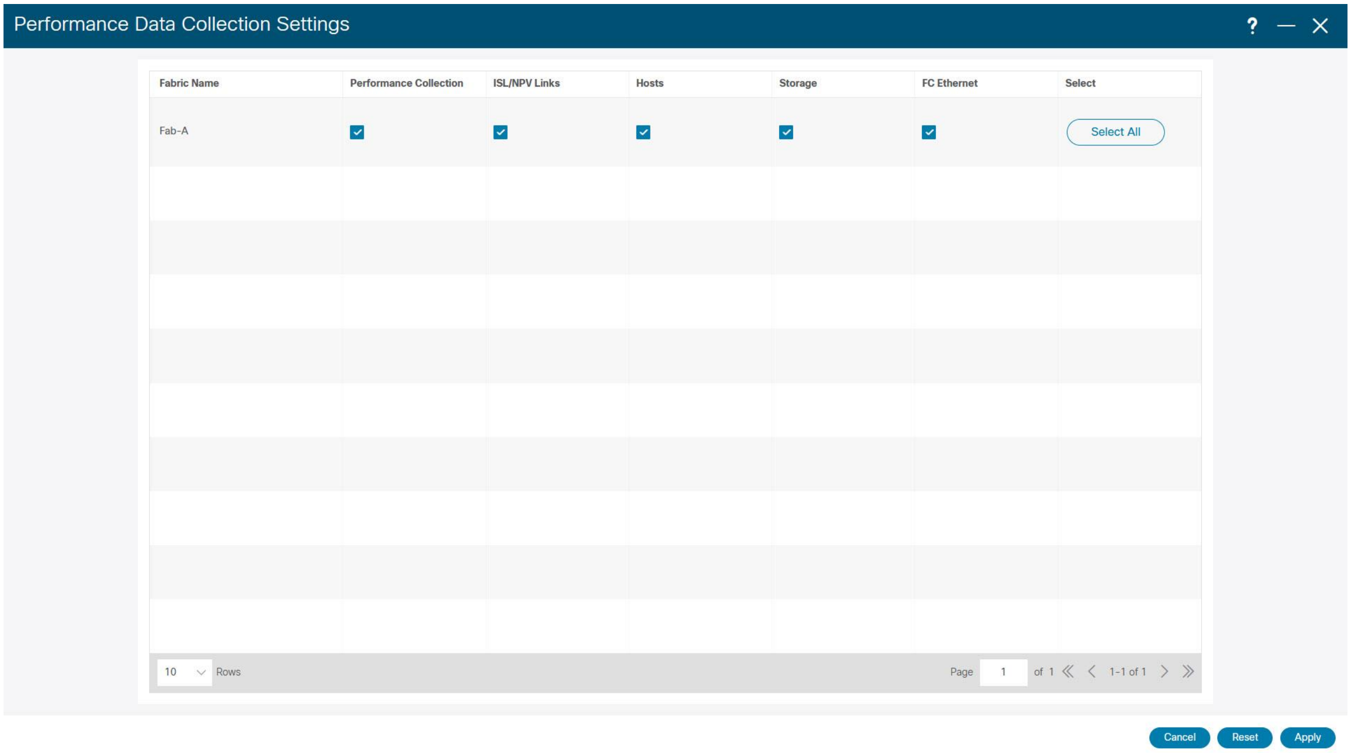
NDFC SAN Controller can detect and display information from storage arrays using SMI-S. Navigate to **SAN > Storage**. Click **Storage SMI-S Provider** and **Actions > Add Provider**. Select the storage array vendor from the drop-down list and enter all the required fields and click **Add**. The Storage SMI-S Provider details must be configured to see the storage array in NDFC SAN Controller. Adding storage arrays to NDFC is an optional step.

License Enablement

Navigate to **Operations > License Management** to install the appropriate licenses.

Enabling Performance Data Collection

Monitoring the performance of the switch ports (for example, traffic utilization) is disabled by default. To enable this functionality for specific fabrics, navigate to SAN > Fabrics. Select a fabric and click **Actions > Configure Performance** and select **Performance collections** and select **ISL/NPV Links**, **Hosts**, **Storage, and FC Ethernet** and click **Apply**. Repeat this step for all fabrics.



Fabric Name	Performance Collection	ISL/NPV Links	Hosts	Storage	FC Ethernet	Select
Fab-A	☑	☑	☑	☑	☑	Select All

Figure 5. Enabling the collection of performance data in NDFC SAN Controller

This step requires restarting the **Performance Collector** service. Click **Confirm.**

It takes a few minutes for the performance graphs to display the data in NDFC. Navigate to **SAN > Interfaces > FC Ports** and select the **Performance** tab to view the statistics. Selecting the small graph icon next to an interface name opens its graph.

It is a mandatory step to display switch port utilization graphs in NDFC SAN Controller.

Setting up Event Notifications on MDS 9000 Switches

NDFC SAN Controller uses SNMP to discover and monitor the MDS 9000 switches using the configured snmp-user. Discovering a SAN fabric by NDFC SAN Controller also sets itself as a receiver of the SNMP trap notifications but the Syslog notifications are not automatically enabled.

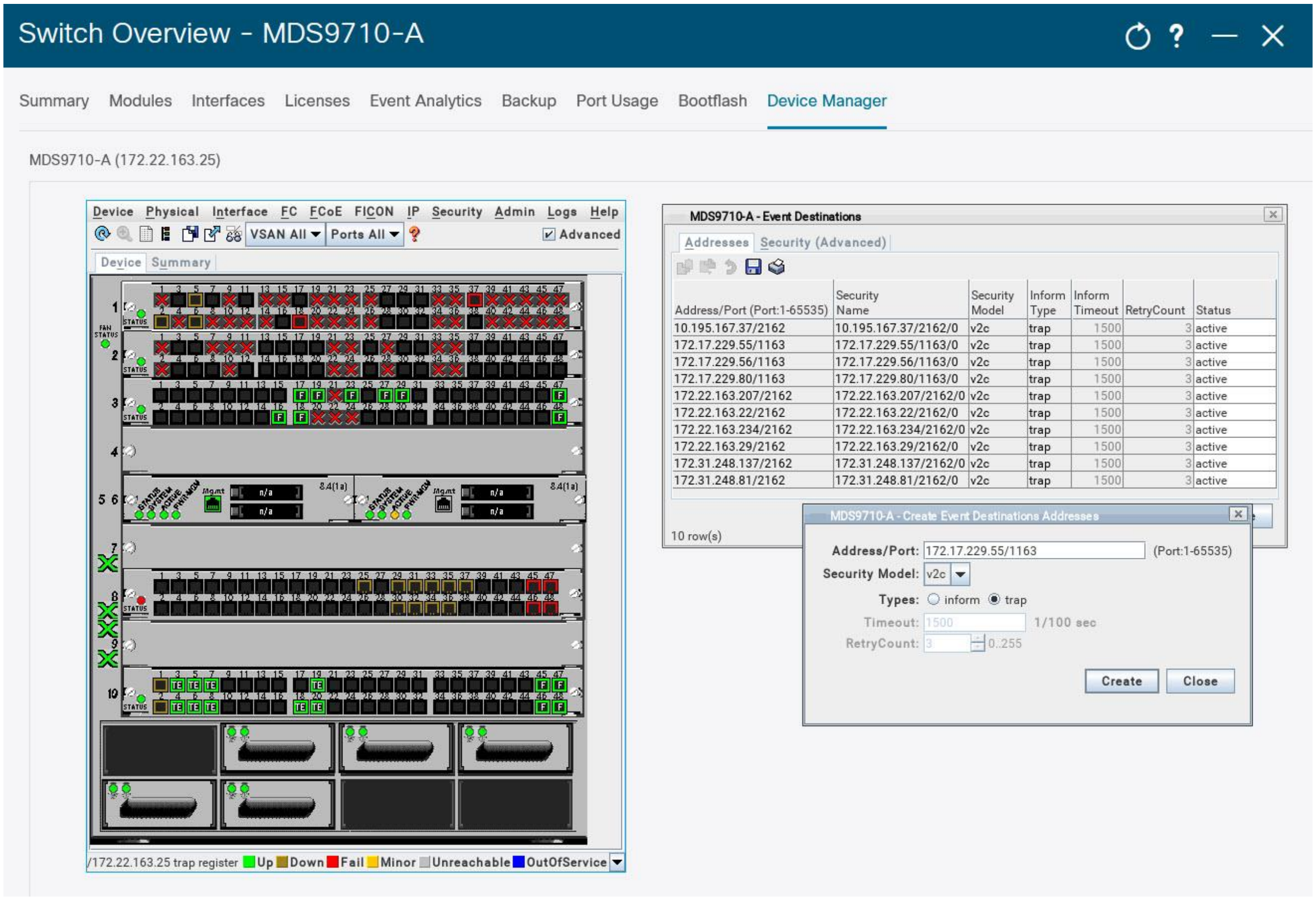
Best practice

Enable sending Syslog to NDFC SAN Controller for all the managed switches.

Setting up SNMP Traps and Informs Destination

SNMP trap and inform destinations can be configured by NX-OS CLI or using NDFC SAN Controller.

To configure using NDFC SAN Controller, navigate to **SAN > Switches**. Enable the check box to select a switch and click **Actions > Device Manager.** Enter the Device Manager of the switch by giving the correct credentials, and then select the **Admin > Events > Destinations**. Click **Create** and configure the IP address of the remote SNMP trap or inform destination. It can be the External IP address that is reserved for SNMP Trap and Syslog in the Nexus Dashboard server (you can see this in the **Nexus Dashboard Admin Console**, go to **Infrastructure > Cluster Configuration** and see **External Service Pools**). The SNMP trap or inform destination can also be any other compatible third-party application. NDFC SAN Controller configures itself as a receiver of SNMP trap when it discovers an MDS 9000 switch and starts managing it. No additional action is needed from a user.



MDS9710-A - Event Destinations

Addresses | Security (Advanced)

Address/Port (Port:1-65535)	Security Name	Security Model	Inform Type	Inform Timeout	RetryCount	Status
10.195.167.37/2162	10.195.167.37/2162/0	v2c	trap	1500	3	active
172.17.229.55/1163	172.17.229.55/1163/0	v2c	trap	1500	3	active
172.17.229.56/1163	172.17.229.56/1163/0	v2c	trap	1500	3	active
172.17.229.80/1163	172.17.229.80/1163/0	v2c	trap	1500	3	active
172.22.163.207/2162	172.22.163.207/2162/0	v2c	trap	1500	3	active
172.22.163.22/2162	172.22.163.22/2162/0	v2c	trap	1500	3	active
172.22.163.234/2162	172.22.163.234/2162/0	v2c	trap	1500	3	active
172.22.163.29/2162	172.22.163.29/2162/0	v2c	trap	1500	3	active
172.31.248.137/2162	172.31.248.137/2162/0	v2c	trap	1500	3	active
172.31.248.81/2162	172.31.248.81/2162/0	v2c	trap	1500	3	active

10 row(s)

MDS9710-A - Create Event Destinations Addresses

Address/Port: 172.17.229.55/1163 (Port:1-65535)
Security Model: v2c
Types: ○ inform ● trap
Timeout: 1500 1/100 sec
RetryCount: 3 0..255
Create | Close

Figure 6. Setting up SNMP trap or inform destinations in NDFC SAN Controller

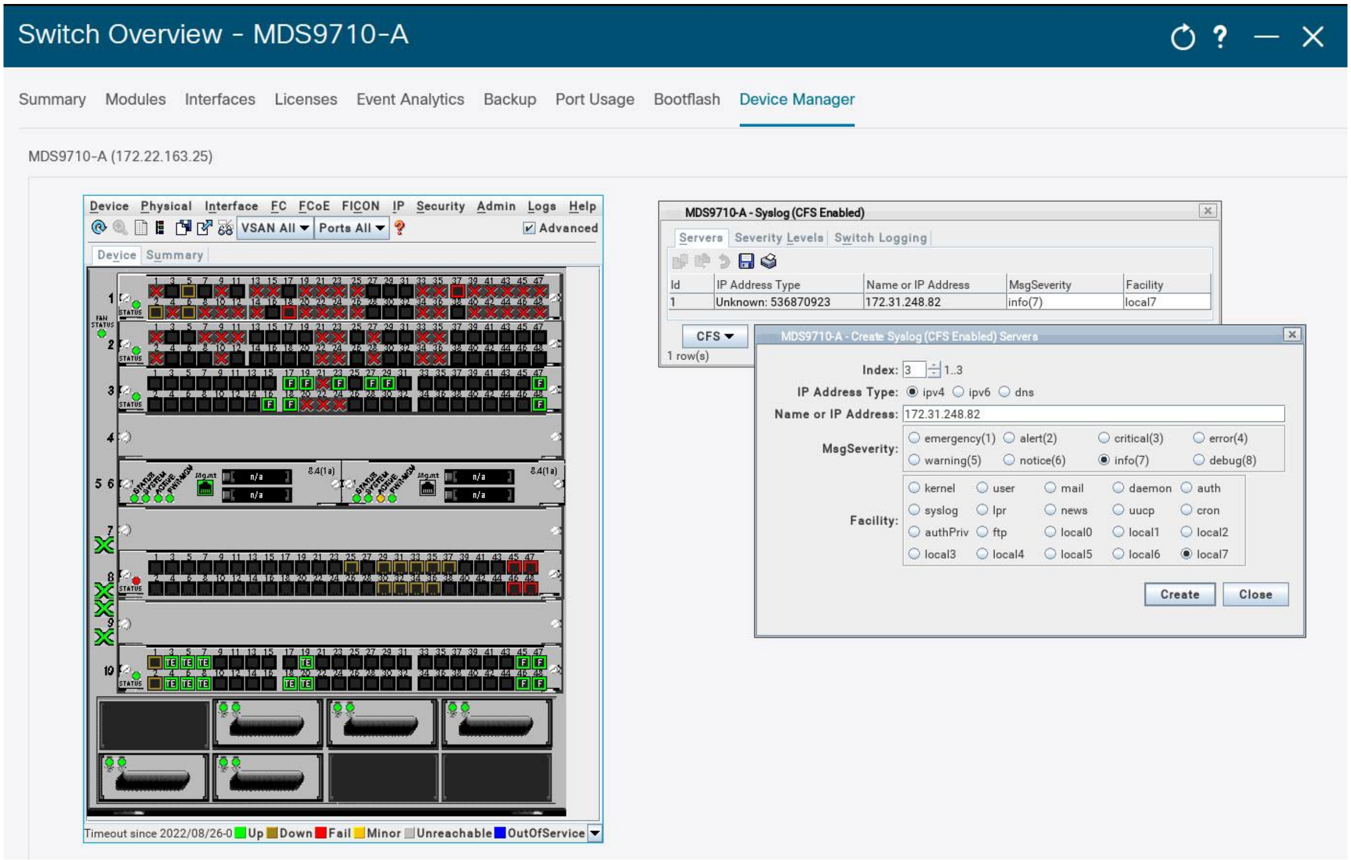
SNMP trap or inform destination can also be configured directly on the MDS 9000 switches using the `snmp-server host` command.

```
MDS-9710#configure

MDS-9710(config)# snmp-server host <destination> traps version 2c <community_string>

MDS-9710(config)# end

MDS-9710#
```

Setting up Syslog Destination

Syslog destinations can be configured by NX-OS CLI or using NDFC SAN Controller.

To configure using NDFC SAN Controller, navigate to **SAN > Switches**. Enable the check box to select a switch and click **Actions > Device Manager**. Enter the **Device Manager** of the switch by giving the correct credentials, and then select the **Logs tab > Syslog > Setup**. Click **Create** and configure the IP address of the remote Syslog destination. It can be the External IP address that is reserved for SNMP Trap and Syslog in the Nexus Dashboard server or any other compatible third-party application.



Switch Overview - MDS9710-A

MDS9710-A - Syslog (CFS Enabled)

Servers | Severity Levels | Switch Logging

Id	IP Address Type	Name or IP Address	MsgSeverity	Facility
1	Unknown: 536870923	172.31.248.82	info(7)	local7

CFS ▾

1 row(s)

MDS9710-A - Create Syslog (CFS Enabled) Servers

Index: 3 1..3

IP Address Type: ● ipv4 ○ ipv6 ○ dns

Name or IP Address: 172.31.248.82

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

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

Create | Close

Figure 7. Setting up Syslog destinations in NDFC SAN Controller

Syslog destination can also be configured directly on the MDS 9000 switches using the `logging server` NX-OS command.

```
MDS-9710#configure

MDS-9710(config)# logging server <destination>

MDS-9710(config)# end

MDS-9710#
```

It is possible to configure a syslog server on a single switch and distribute the same configuration to all the switches in the fabric using Cisco Fabric Services (CFS). It is the preferred approach in a larger environment. refer to the following snippet.

```
MDS-9710# configure

MDS-9710(config)# logging distribute (to all fabric switches via CFS)

MDS-9710(config)# logging commit
```

For more information on `logging distribute` command, refer to the references section to access the Cisco MDS 9000 Series System Management Configuration Guide.

Setting up Call Home

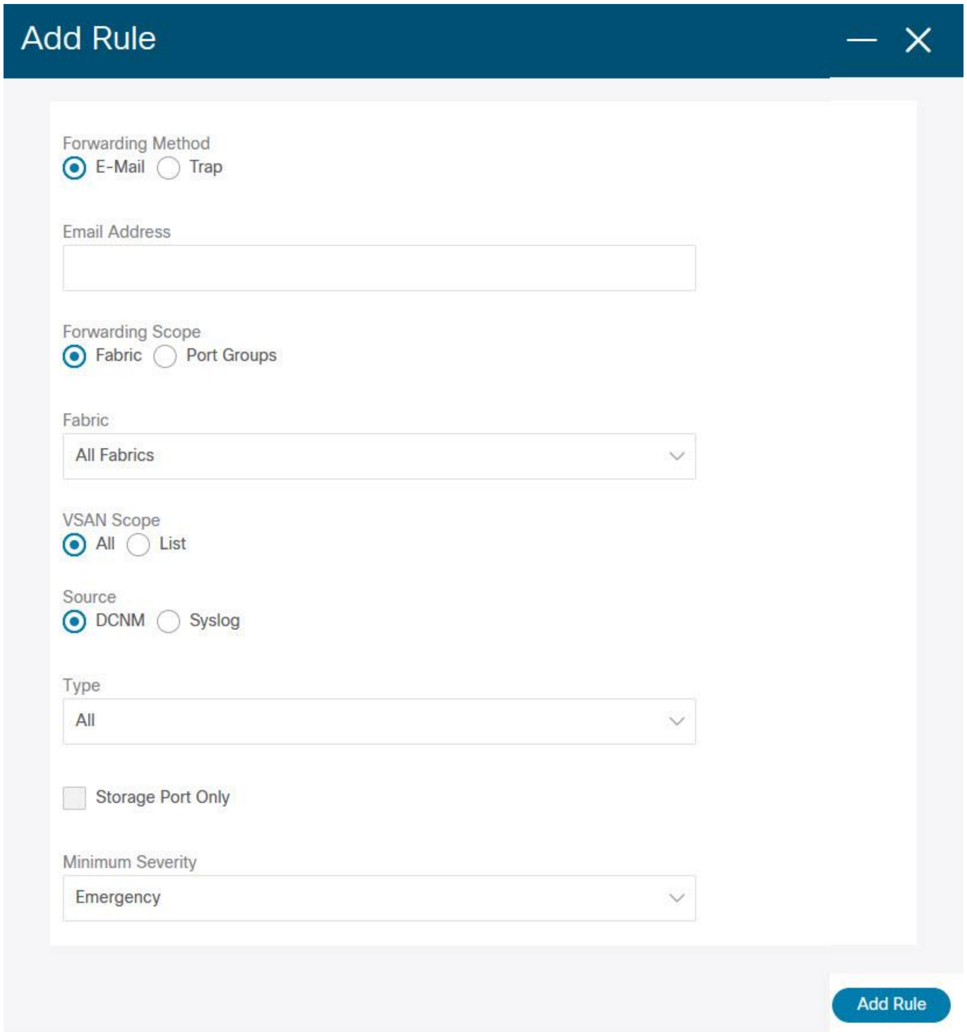
MDS 9000 switches can send event notifications over email using the Call Home functionality.

For details configuring Call Home, refer to the references section to access the Cisco MDS 9000 Series System Management Configuration Guide.

Setting up Event Notifications in NDFC SAN Controller

NDFC SAN Controller provides event forwarding using SNMP traps or informs and emails. A valid SMTP server is required for email forwarding. For configuring SMTP, navigate to Settings > Server Settings > SMTP tab.

Now, to configure event forwarding in NDFC SAN Controller, navigate to **Operations > Event Analytics > Events**. Click the **Actions > Event Setup**. Navigate to **Forwarding** tab and click **Actions > Add Rule** to configure specific rules.



Add Rule

Forwarding Method
● E-Mail ○ Trap

Email Address

Forwarding Scope
● Fabric ○ Port Groups

Fabric
All Fabrics

VSAN Scope
● All ○ List

Source
● DCNM ○ Syslog

Type
All

□ Storage Port Only

Minimum Severity
Emergency

Figure 8. Setting up Event Forwarding in NDFC SAN Controller

Number of Monitoring Agents, Traps or Informs, and Syslog Destinations

Multiple monitoring agents can simultaneously monitor the same MDS 9000 switches. Similarly, push notifications through SNMP traps and informs, Syslog, and Call Home can be sent to multiple destinations. Although NX-OS allows configuring many destinations, we recommend limiting it to 2 or 3 for avoiding extra load on the monitored switch.

Best Practice

Limit the number of monitoring agents, SNMP trap or inform and Syslog destinations to less than 3.

If more destinations are required, we recommend using the event forwarding feature of NDFC SAN Controller. Similar capability to relay the events is commonly available in other third-party applications also.

The destination of push notifications over SNMP or Syslog is explicitly configured on MDS 9000 switches. Hence, the number of destinations is known and can be limited by changing the configuration. On the contrary, the number of monitoring agents is not explicitly limited by an MDS 9000 switch. Many agents can simultaneously perform SNMP polling or send HTTP/HTTPs requests causing extra load on the switch. There is little reason for more than 3 agents to simultaneously monitor the same switch. Any such access should be limited by user credentials and other security mechanisms such as Access Control Lists (ACLs) or network firewalls.

Monitoring and Alerting of Specific Components

The following subsections explain monitoring and alerting of specific hardware and software components on MDS 9000 switches and NX-OS. Details are provided for using NDFC SAN Controller and a compatible third-party application.

SNMP MIBs

The correct interpretation of SNMP polling or to receive trap and inform notifications require the MIB file to be present on the monitoring agent. Cisco NDFC SAN Controller already carries all the MIB files and no additional action is required from a user. Using a third-party monitoring agent requires loading more MIB files into it. The required MIB files can be downloaded from the Cisco SNMP Object Navigator.

SNMP support is widely available across other Cisco and industry products. While using a generic SNMP MIB, be cautious before overwriting any existing MIB files. The generic services are common and do not require an MDS 9000 specific MIB. For example, `cseSysCPUUtilization` is a generic SNMP object to monitor the CPU utilization for many Cisco products. MDS 9000 switches are purposefully built for Fibre Channel and hence, carry specific MIBs for Fibre Channel services. Such MIB must be loaded in the monitoring agent in addition to the existing MIB files.

For more details, refer to the references section to access the Cisco MDS 9000 Family MIB Quick Reference. SNMP MIBs for specific components is provided in the following subsections.

For more details to translate OIDs into object names, their descriptions, browse OID trees, and to download the MIB files, refer to the references section to access the Cisco SNMP Object Navigator.

General Switch Health

General switch health can be monitored using the following NX-OS commands:

Table 1. NX-OS commands to check the overall switch health

NX-OS command	Description
show processes cpu <detailed | history | module | sort>	Check the control-plane CPU utilization of the switch
show processes memory <physical | shared | sort>	Check the memory utilization of the switch
show version	Check the NX-OS version, uptime, switch model, and so on.

NX-OS command	Description
show <environment | hardware>	Check the status of the hardware components of the switch

The output of the preceding commands is also available through NX-API when requested by a remote agent over HTTP or HTTPS.

SNMP MIBs can be used to poll the general health of the switch, especially the CPU, and memory utilization.

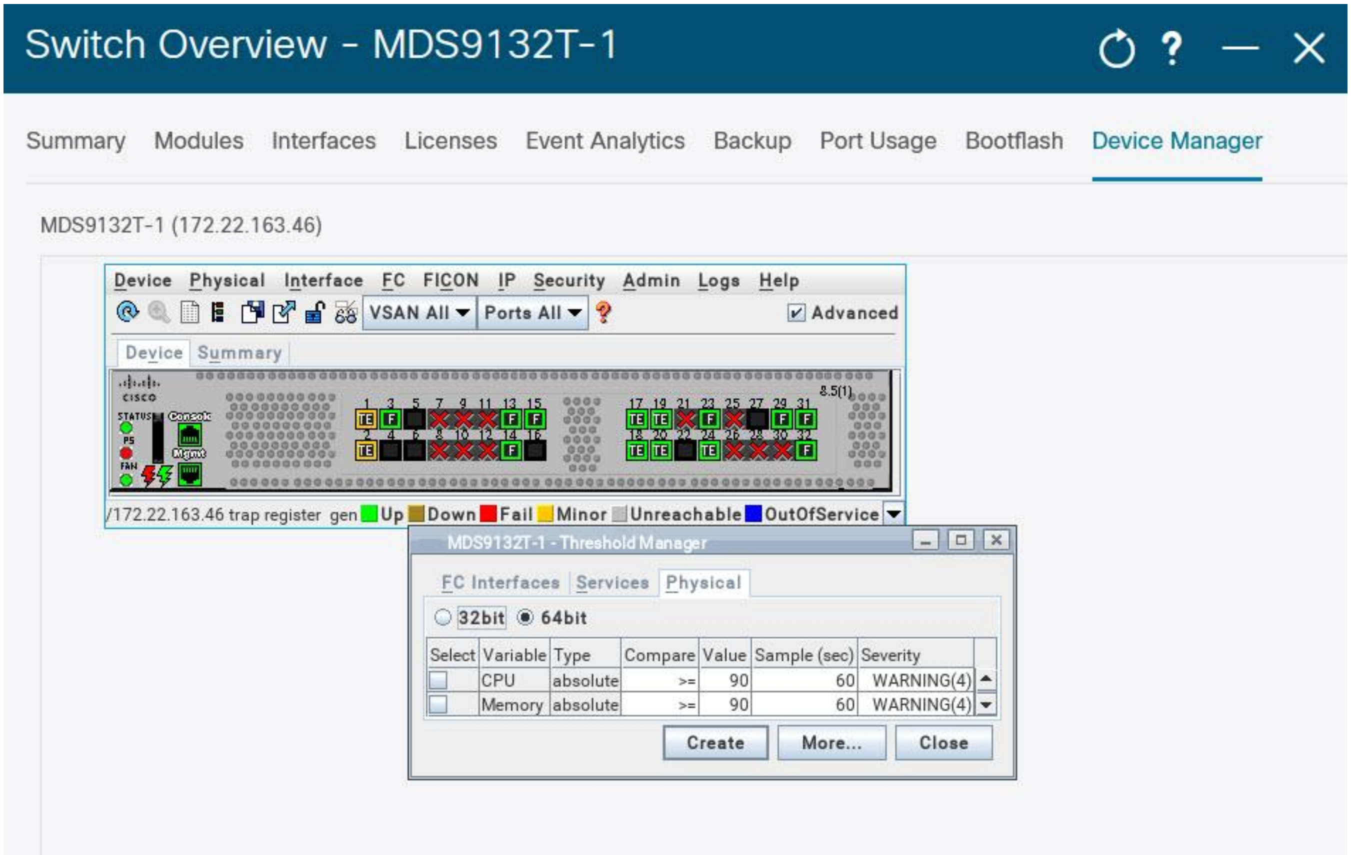
Table 2. General switch health SNMP Objects

SNMP Objects	OID	Description
cseSysMemoryUtilization	1.3.6.1.4.1.9.9.305.1.1.2	Percent utilization of memory
cseSysCPUUtilization	1.3.6.1.4.1.9.9.305.1.1.1	Percent utilization of CPU

Threshold-based Alerting from Common Switch Components

Use RMON to configure high-CPU, high-memory, and other similar alerts on MDS 9000 switch. RMON notifications are sent through SNMP trap or inform.

To configure RMON alerts from NDFC SAN Controller, navigate to **SAN > Switches**. Check the check box to select a switch and click **Actions > Device Manager**. Enter the **Device Manager** of the switch by giving the correct credentials and navigate to **Admin** tab **> Events > Threshold Manager**. Go to the **Physical** tab to set RMON alerts for high-CPU and high-Memory conditions.



○ 32bit ● 64bit

Select	Variable	Type	Compare	Value	Sample (sec)	Severity
☐	CPU	absolute	>=	90	60	WARNING(4)
☐	Memory	absolute	>=	90	60	WARNING(4)

Figure 9. Configuring RMON events in NDFC SAN Controller

Best Practice

Prefer NDFC SAN Controller over NX-OS CLI to configure threshold-based alerting using RMON.

It is possible to set RMON alerts through NX-OS CLI but NDFC SAN Controller is recommended because it automatically translates SNMP OID to a user-friendly string. refer to the following snippet to configure the high-CPU and high-Memory RMON alerts using NX-OS.

```
MDS-9710#configure

MDS-9710(config)# rmon hcalarm 1 1.3.6.1.4.1.9.9.305.1.1.1.0 60 absolute startupalarm 1
rising-threshold 90 4 falling-threshold 89 4 owner user_1_cseSysCPUUtilization

MDS-9710(config)# rmon hcalarm 2 1.3.6.1.4.1.9.9.305.1.1.2.0 60 absolute startupalarm 1
rising-threshold 90 4 falling-threshold 89 4 owner user_1_cseSysMemoryUtilization

MDS-9710#
```

The RMON events are sent to the configured SNMP trap or inform destination, which can be NDFC SAN Controller or a compatible third-party application.

Monitoring of Switch Hardware Components

Monitoring of switch hardware components is enabled by default. Notifications can be sent using Syslog and SNMP trap or inform. Email notifications can also be generated by MDS 9000 switches using Call Home or by NDFC SAN Controller event forwarding functionality.

The default enabled SNMP traps can be verified using **`show snmp trap`** command. refer to the following snippet.

```
MDS-9710# show snmp trap
--------------------------------------------------------------------------------
Trap type            Description          Enabled
--------------------------------------------------------------------------------
entity        : entity_mib_change        Yes
entity        : entity_module_status_change   Yes
entity        : entity_power_status_change   Yes
entity        : entity_module_inserted     Yes
entity        : entity_module_removed      Yes
entity        : entity_unrecognised_module   Yes
entity        : entity_fan_status_change    Yes
entity        : entity_power_out_change     Yes
link         : linkDown            Yes
link         : linkUp             Yes
link         : extended-linkDown        Yes
link         : extended-linkUp         Yes
link         : cieLinkDown           Yes
link         : cieLinkUp            Yes
link         : connUnitPortStatusChange    Yes
link         : delayed-link-state-change    Yes
callhome       : event-notify          No
callhome       : smtp-send-fail         No
cfs         : state-change-notif       No
cfs         : merge-failure          No
fcdomain       : dmNewPrincipalSwitchNotify   No
fcdomain       : dmDomainIdNotAssignedNotify   No
fcdomain       : dmFabricChangeNotify      No
rf          : redundancy_framework      Yes
aaa         : server-state-change       No
license       : notify-license-expiry      Yes
license       : notify-no-license-for-feature  Yes
license       : notify-licensefile-missing   Yes
license       : notify-license-expiry-warning  Yes
scsi         : scsi-lunDiscovery-complete   No
fcns         : reject-reg-req         No
fcns         : local-entry-change       No
fcns         : db-full             No
fcns         : remote-entry-change       No
rscn         : rscnElsRejectReqNotify     No
rscn         : rscnIlsRejectReqNotify     No
rscn         : rscnElsRxRejectReqNotify    No
rscn         : rscnIlsRxRejectReqNotify    No
```

```
fcs         : request-reject         No
fcs         : discovery-complete       No
fctrace       : route-test-complete       No
zone         : request-reject1         No
zone         : merge-success          No
zone         : merge-failure          No
zone         : default-zone-behavior-change  No
zone         : unsupp-mem           No
port-security    : fport-violation         No
port-security    : eport-violation         No
port-security    : fabric-binding-violation    No
vni         : virtual-interface-created    No
vni         : virtual-interface-removed    No
vsan         : vsanStatusChange        No
vsan         : vsanPortMembershipChange    No
fspf         : fspfNbrStateChangeNotify    No
upgrade       : UpgradeOpNotifyOnCompletion   Yes
upgrade       : UpgradeJobStatusNotify     Yes
feature-control   : FeatureOpStatusChange      No
vrrp         : cVrrpNotificationNewMaster   No
fdmi         : cfdmiRejectRegNotify      No
sysmgr        : cseFailSwCoreNotifyExtended   No
rmon         : risingAlarm           Yes
rmon         : fallingAlarm          Yes
rmon         : hcRisingAlarm          Yes
rmon         : hcFallingAlarm         Yes
config        : ccmCLIRunningConfigChanged   No
snmp         : authentication         No
link         : cisco-xcvr-mon-status-chg    No
vtp         : notifs             No
vtp         : vlancreate           No
vtp         : vlandelete           No
zone         : enhanced-zone-db-change     No
entity        : entity_sensor          Yes
entity        : cefcMIBEnableStatusNotification Yes
system        : Clock-change-notification    No
generic       : coldStart            Yes
generic       : warmStart            Yes
feature-control   : ciscoFeatOpStatusChange     No
syslog        : message-generated        No
entity        : cefcEnablePSOutputChangeNotif  Yes
vtp         : notifs             No
```

```
lldp         : lldpRemTablesChange       No
switchfabric     : fabric-crc           No
MDS-9710#
```

Traps and informs for more components can be enabled by **`snmp-server enable traps`** command. refer to the following snippet.

```
MDS-9710(config)# snmp-server enable traps ?
 <CR>
 aaa       Enable aaa traps
 callhome     Enable callhome traps
 cfs       Enable cfs traps
 config      Enable config traps
 entity      Enable entity traps
 fcdomain     Enable fcdomain traps
 fcns       Enable fcns traps
 fcs       Enable fcs traps
 fctrace     Enable fctrace traps
 fdmi       Enable fdmi traps
 feature-control Enable feature-control traps
 fspf       Enable fspf traps
 generic     Enable generic traps
 license     Enable license traps
 link       Enable link traps
 lldp       Enable lldp traps
 port-security  Enable port-security traps
 rf        Enable rf traps
 rmon       Enable rmon traps
 rscn       Enable rscn traps
 scsi       Enable scsi traps
 snmp       Enable snmp traps
 storm-control  Enable storm-control traps
 switchfabric   Enable switchfabric traps
 syslog      Enable syslog traps
 sysmgr      Enable sysmgr traps
 system      Enable system traps
 upgrade     Enable upgrade traps
 vni       Enable vni traps
 vrrp       Enable vrrp traps
 vsan       Enable vsan traps
 vtp       Enable vtp traps
 zone       Enable zone traps

MDS-9710(config)#
```

Hardware Misconfigurations

Hardware misconfigurations are automatically detected, and alerting is enabled by default. Notifications are sent using Syslog and SNMP traps or informs. For example, switches with the support of bidirectional airflow, a misconfiguration in the airflow direction is autodetected and a system message is generated, as shown below.

```
2022 Apr 19 16:07:08 MDS-9148 %KERN-0-SYSTEM_MSG: [ 152.729361] Airflow conflict is
detected. Incompatible PSU/ Fan found. Switch will be shutdown if compatible PSU/ Fan is not
installed. - kernel
```

Similar alerts are generated from other hardware components when a failure or misconfiguration is detected. No actions are required from a user.

High-Availability (HA) Monitoring

The high-availability state of MDS 9000 switches can be monitored using command **`show system redundancy ha status`**. refer to the following snippet.

```
MDS-9710# show system redundancy ha status
This supervisor             Other supervisor
---------------             ---------------
Active with HA standby         HA standby
MDS-9710#
MDS-9710# show system redundancy status
Redundancy mode
---------------
   administrative:  HA
     operational:  HA

This supervisor (sup-6)
-----------------------
  Redundancy state:  Active
  Supervisor state:  Active
   Internal state:  Active with HA standby

Other supervisor (sup-5)
------------------------
  Redundancy state:  Standby
  Supervisor state:  HA standby
   Internal state:  HA standby
MDS-9710#
```

The high-availability state of the MDS 9000 switches can also be monitored using CISCO-RF-MIB. For example, **`ciscoRFIssuStateNotif`** is generated to indicate a new state of the system. These state changes also generate system messages which can be sent to a remote agent using Syslog.

Email notifications can also be generated by MDS 9000 switches using Call Home or by NDFC SAN Controller event forwarding functionality.

SFP Monitoring and Alerting

Monitoring and alerting of SFPs on MDS 9000 switches are enabled by default. No action is required from a user. The alerting thresholds are pre-defined by the manufacturer based on the type of SFP.

CLI

Use the **`show interface transceiver details`** command to monitor the SFP.

```
MDS-9710# show interface fc1/17 transceiver details
fc1/17 sfp is present
  Name is CISCO-FINISAR
  Manufacturer's part number is FTLF8532P4BCV-C1
  Revision is B
  Serial number is FNS21280PRE
  Nominal bit rate is 28000 Mb/s
  Link length supported for 50/125um OM3 fiber is 70 m
  FC Transmitter type is short wave laser w/o OFC (SN)
  FC Transmitter supports short distance link length
  Transmission medium is multimode laser with 50 um aperture (M5)
  Supported speeds are - Min speed: 8000 Mb/s, Max speed: 32000 Mb/s
  Cisco extended id is unknown (0x0)
  Cisco part number is 10-3206-01
  Cisco pid is DS-SFP-FC32G-SW

  No tx fault, no rx loss, in sync state, diagnostic monitoring type is 0x68
  SFP Diagnostics Information:
----------------------------------------------------------------------------
                   Alarms         Warnings
                High    Low     High     Low
----------------------------------------------------------------------------
 Temperature  67.32 C     75.00 C   -5.00 C   70.00 C    0.00 C
 Voltage    3.35 V      3.63 V   2.97 V   3.46 V    3.13 V
 Current    7.57 mA     12.00 mA   1.00 mA  11.50 mA    2.00 mA
 Tx Power   -1.50 dBm     5.00 dBm -12.20 dBm  2.00 dBm   -8.20 dBm
 Rx Power    0.66 dBm     5.00 dBm -15.20 dBm  2.00 dBm  -11.20 dBm
 Transmit Fault Count = 0
----------------------------------------------------------------------------
 Note: ++ high-alarm; + high-warning; -- low-alarm; - low-warning
MDS-9710#
```

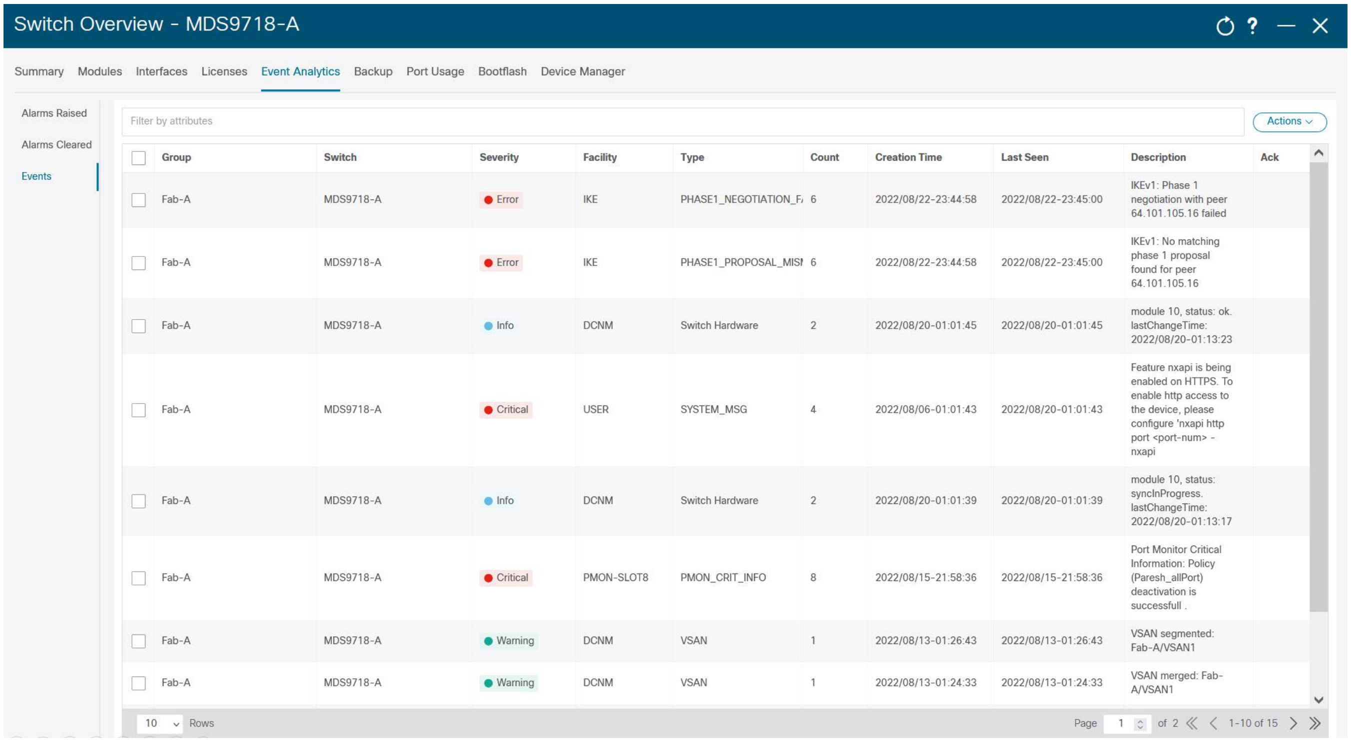
SFPs are monitored for:

- Temperature (Celsius)
- Voltage (Volts)
- Current ((milli) Ampere)

- Tx Power (dBm)
- Rx Power (dBm)
- Transmit Fault (count)

The preceding command output also displays the alarm and warning ranges. The monitoring of the SFPs is enabled by default and alerts are generated when thresholds are exceeded. Alerts based on custom threshold values can be generated using port-monitor feature on MDS switches. This event results in system messages (which can be sent to a remote agent using Syslog) and SNMP traps and informs.

This alert is also sent to NDFC SAN Controller and is accessible by navigating to SAN > Switches, selecting the respective switch and then navigating to Event Analytics > Events.



□	Group	Switch	Severity	Facility	Type	Count	Creation Time	Last Seen	Description	Ack
□	Fab-A	MDS9718-A	● Error	IKE	PHASE1_NEGOTIATION_F/	6	2022/08/22-23:44:58	2022/08/22-23:45:00	IKEv1: Phase 1 negotiation with peer 64.101.105.16 failed	
□	Fab-A	MDS9718-A	● Error	IKE	PHASE1_PROPOSAL_MISI	6	2022/08/22-23:44:58	2022/08/22-23:45:00	IKEv1: No matching phase 1 proposal found for peer 64.101.105.16	
□	Fab-A	MDS9718-A	● Info	DCNM	Switch Hardware	2	2022/08/20-01:01:45	2022/08/20-01:01:45	module 10, status: ok. lastChangeTime: 2022/08/20-01:13:23	
□	Fab-A	MDS9718-A	● Critical	USER	SYSTEM_MSG	4	2022/08/06-01:01:43	2022/08/20-01:01:43	Feature nxapi is being enabled on HTTPS. To enable http access to the device, please configure 'nxapi http port <port-num> -nxapi	
□	Fab-A	MDS9718-A	● Info	DCNM	Switch Hardware	2	2022/08/20-01:01:39	2022/08/20-01:01:39	module 10, status: syncInProgress. lastChangeTime: 2022/08/20-01:13:17	
□	Fab-A	MDS9718-A	● Critical	PMON-SLOT8	PMON_CRIT_INFO	8	2022/08/15-21:58:36	2022/08/15-21:58:36	Port Monitor Critical Information: Policy (Paresh_allPort) deactivation is successfull .	
□	Fab-A	MDS9718-A	● Warning	DCNM	VSAN	1	2022/08/13-01:26:43	2022/08/13-01:26:43	VSAN segmented: Fab-A/VSAN1	
□	Fab-A	MDS9718-A	● Warning	DCNM	VSAN	1	2022/08/13-01:24:33	2022/08/13-01:24:33	VSAN merged: Fab-A/VSAN1	

10 Rows Page 1 of 2 1-10 of 15

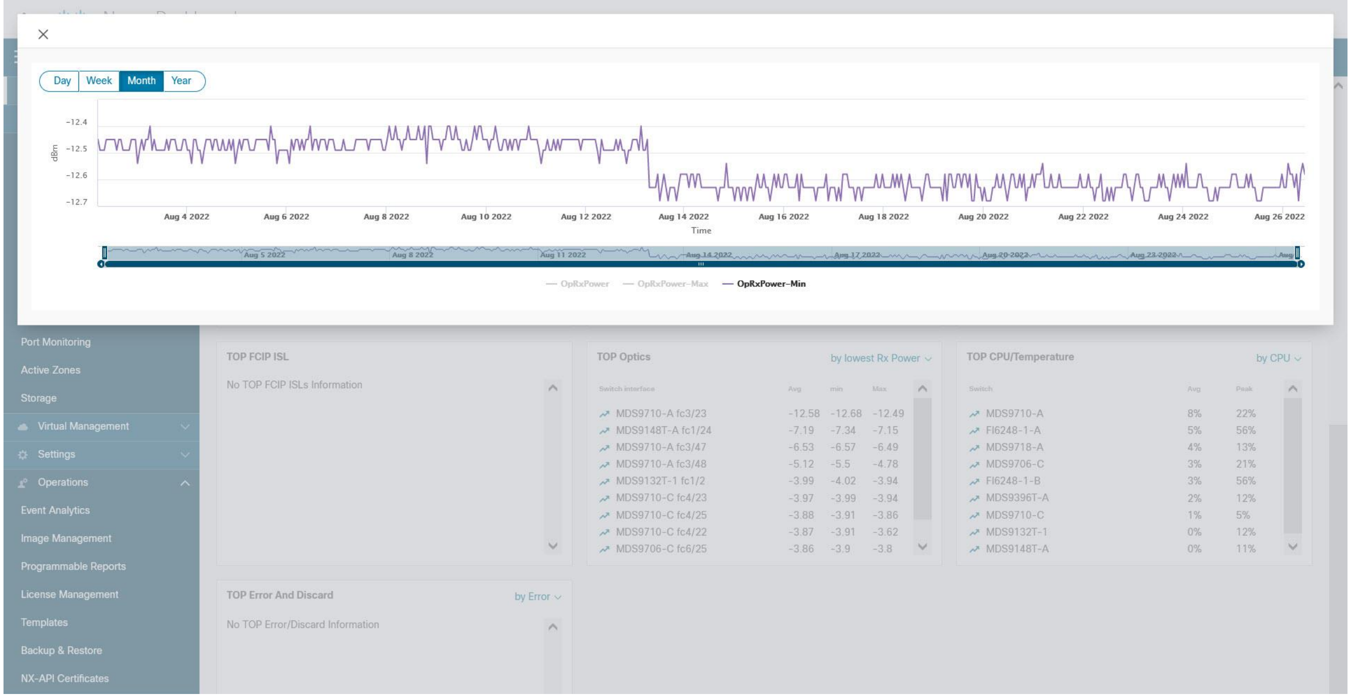
Figure 10. Viewing events in NDFC SAN Controller

NDFC SAN Controller

A dashlet for Optics health can be found on the NDFC SAN Controller dashboard. The dashlet gives data for top ten optics by the following parameters:

- Hottest SFPs
- Coldest SFPs
- Lowest Rx Power
- Lowest Tx Power

Clicking on the small graph icon next to an interface name will show the data in graph for a day/week/month/year.



TOP FCIP ISL

No TOP FCIP ISLs Information

TOP Optics

Switch interface	Avg	min	Max
MDS9710-A fc3/23	-12.58	-12.68	-12.49
MDS9148T-A fc1/24	-7.19	-7.34	-7.15
MDS9710-A fc3/47	-6.53	-6.57	-6.49
MDS9710-A fc3/48	-5.12	-5.5	-4.78
MDS9132T-1 fc1/2	-3.99	-4.02	-3.94
MDS9710-C fc4/23	-3.97	-3.99	-3.94
MDS9710-C fc4/25	-3.88	-3.91	-3.86
MDS9710-C fc4/22	-3.87	-3.91	-3.62
MDS9706-C fc6/25	-3.86	-3.9	-3.8

TOP CPU/Temperature

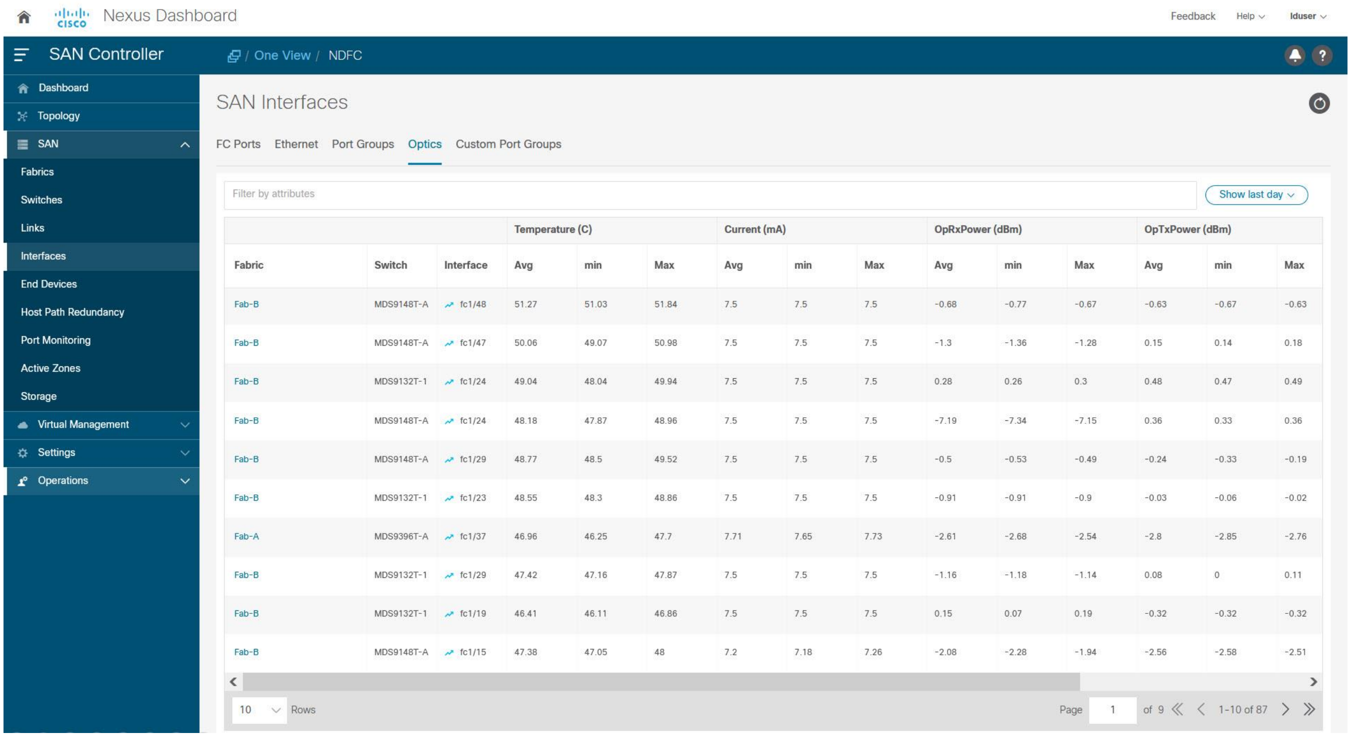
Switch	Avg	Peak
MDS9710-A	8%	22%
FI6248-1-A	5%	56%
MDS9718-A	4%	13%
MDS9706-C	3%	21%
FI6248-1-B	3%	56%
MDS9396T-A	2%	12%
MDS9710-C	1%	5%
MDS9132T-1	0%	12%
MDS9148T-A	0%	11%

TOP Error And Discard

No TOP Error/Discard Information

Figure 11. Optics dashlet and pop-up graph in NDFC SAN Controller

More optics information can be found at **SAN > Interfaces > Optics** tab.



			Temperature (C)			Current (mA)			OpRxPower (dBm)			OpTxPower (dBm)		
Fabric	Switch	Interface	Avg	min	Max	Avg	min	Max	Avg	min	Max	Avg	min	Max
Fab-B	MDS9148T-A	fc1/48	51.27	51.03	51.84	7.5	7.5	7.5	-0.68	-0.77	-0.67	-0.63	-0.67	-0.63
Fab-B	MDS9148T-A	fc1/47	50.06	49.07	50.98	7.5	7.5	7.5	-1.3	-1.36	-1.28	0.15	0.14	0.18
Fab-B	MDS9132T-1	fc1/24	49.04	48.04	49.94	7.5	7.5	7.5	0.28	0.26	0.3	0.48	0.47	0.49
Fab-B	MDS9148T-A	fc1/24	48.18	47.87	48.96	7.5	7.5	7.5	-7.19	-7.34	-7.15	0.36	0.33	0.36
Fab-B	MDS9148T-A	fc1/29	48.77	48.5	49.52	7.5	7.5	7.5	-0.5	-0.53	-0.49	-0.24	-0.33	-0.19
Fab-B	MDS9132T-1	fc1/23	48.55	48.3	48.86	7.5	7.5	7.5	-0.91	-0.91	-0.9	-0.03	-0.06	-0.02
Fab-A	MDS9396T-A	fc1/37	46.96	46.25	47.7	7.71	7.65	7.73	-2.61	-2.68	-2.54	-2.8	-2.85	-2.76
Fab-B	MDS9132T-1	fc1/29	47.42	47.16	47.87	7.5	7.5	7.5	-1.16	-1.18	-1.14	0.08	0	0.11
Fab-B	MDS9132T-1	fc1/19	46.41	46.11	46.86	7.5	7.5	7.5	0.15	0.07	0.19	-0.32	-0.32	-0.32
Fab-B	MDS9148T-A	fc1/15	47.38	47.05	48	7.2	7.18	7.26	-2.08	-2.28	-1.94	-2.56	-2.58	-2.51

Figure 12. Viewing Optics data in NDFC SAN Controller

SNMP Polling

The SFP parameters can be polled from the switches using SNMP (CISCO-ENTITY-SENSOR-MIB). Use this option to continuously monitor the SFP parameters for a long term trending and seasonality.

SNMP Notifications

The SNMP traps and informs for SFP alarm and warning notifications are sent via CISCO-INTERFACE-XCVR-MONITOR-MIB. The object is cIfXcvrMonStatusChangeNotif with following components:

- ifName
- cIfXcvrMonDigitalDiagTempAlarm
- cIfXcvrMonDigitalDiagTempWarning
- cIfXcvrMonDigitalDiagVoltAlarm
- cIfXcvrMonDigitalDiagVoltWarning
- cIfXcvrMonDigitalDiagCurrAlarm
- cIfXcvrMonDigitalDiagCurrWarning
- cIfXcvrMonDigitalDiagRxPwrAlarm
- cIfXcvrMonDigitalDiagRxPwrWarning
- cIfXcvrMonDigitalDiagTxPwrAlarm
- cIfXcvrMonDigitalDiagTxPwrWarning
- cIfXcvrMonDigitalDiagTxFaultAlarm

For more details to translate OIDs into object names, their descriptions, browse OID trees, and to download the MIB files, refer to the references section to access the Cisco SNMP Object Navigator.

Syslog notification

Following is a sample message when a low voltage warning is generated from SFP in port fc1/1.

```
%PORT-4-IF_SFP_WARNING: Interface fc1/1, Low Voltage Warning
```

Interface State and Performance Monitoring and Alerting

Hardware sensors on the port-ASICs on the Cisco MDS 9000 switches continuously collect the metrics at low granularity in real time. This section provides details to display the metrics using the NX-OS CLI or export them to a remote agent or generate automated alerting.

The monitoring of interfaces on MDS 9000 switches is enabled by default. Alerting of only major events is enabled by default, for example, link-up and link-down events. More alerts, if necessary, must be explicitly enabled, for example, high link utilization and B2B credit unavailability.

CLI

The interface counters are available under **`show interface <> counters`**, **`show interface <> counters brief`** and **`show interface <> counters detailed`** commands, as shown below.

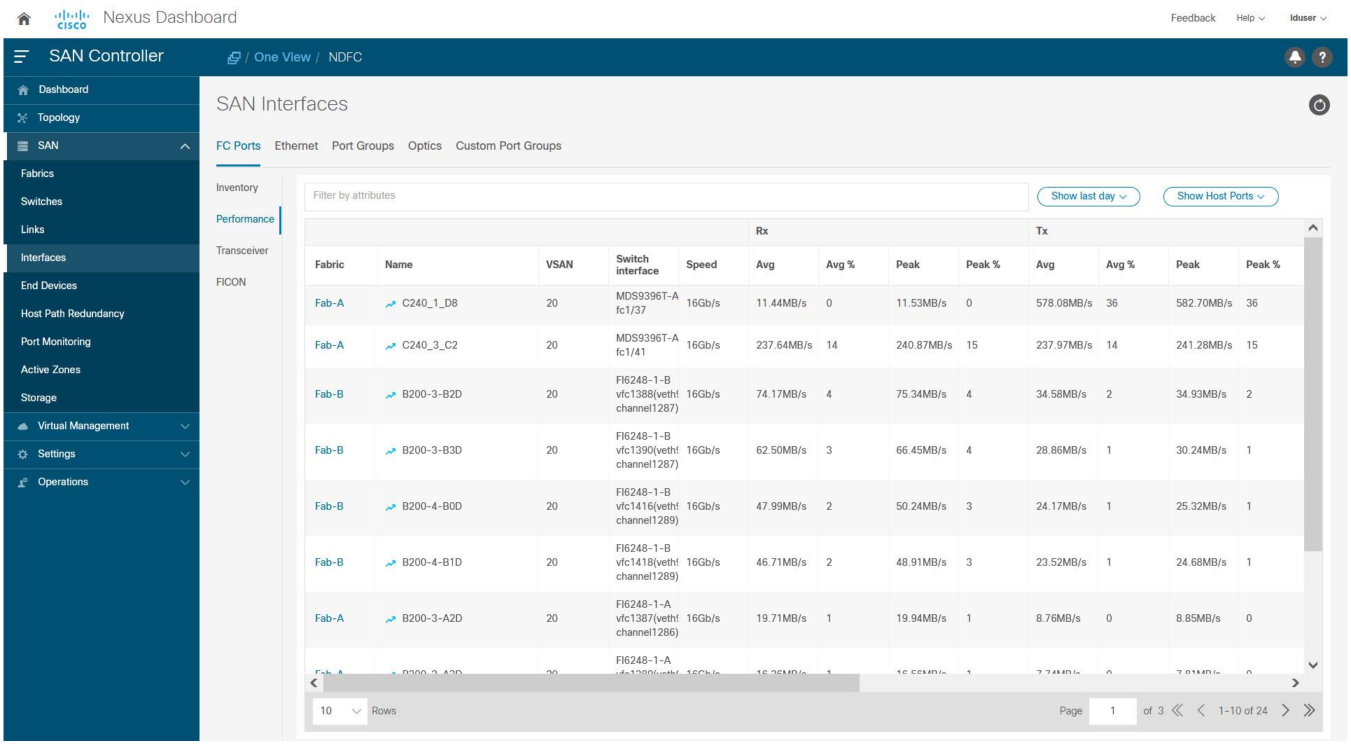
```
MDS9718-A# show interface fc1/15
fc1/15 is trunking
  Port description is to_MDS9706-C
  Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
  Port WWN is 20:0f:8c:60:4f:9e:2b:00
  Peer port WWN is 20:0f:8c:60:4f:54:51:00
  Admin port mode is auto, trunk mode is on
  snmp link state traps are enabled
  Port mode is TE
  Port vsan is 1
  Admin Speed is auto
  Operating Speed is 32 Gbps
  Rate mode is dedicated
  Port flow-control is ER_RDY

  Transmit B2B Credit for VL 0-3: 15, 15, 40, 430
  Receive B2B Credit for VL 0-3: 15, 15, 40, 430
  B2B State Change: Admin(on), Oper(up), Negotiated Value(14)
  Receive data field Size is 2112
  Beacon is turned off
  fec is enabled by default
  Logical type is core
  Belongs to port-channel2
  Trunk vsans (admin allowed and active) (1,20)
  Trunk vsans (up)            (1,20)
  Trunk vsans (isolated)         ()
  Trunk vsans (initializing)       ()
  5 minutes input rate 1446253536 bits/sec,180781692 bytes/sec, 135982 frames/sec
  5 minutes output rate 2023045760 bits/sec,252880720 bytes/sec, 194685 frames/sec
   1207557063868 frames input,1613205257783384 bytes
    0 discards,0 errors
    0 invalid CRC/FCS,0 unknown class
    0 too long,0 too short
   1727972173378 frames output,2257782335763584 bytes
    0 discards,0 errors
   7 input OLS,5 LRR,4 NOS,0 loop inits
   6 output OLS,10 LRR, 3 NOS, 0 loop inits
  Transmit B2B credit remaining for VL 0-3: 15, 15, 40, 429
  Receive B2B credit remaining for VL 0-3: 15, 15, 40, 430
  Last clearing of "show interface" counters: never

MDS9718-A#
MDS9718-A# show interface fc1/15 counters brief

-------------------------------------------------------------------------------
Interface     Input (rate is 5 min avg)   Output (rate is 5 min avg)
          ----------------------------- -----------------------------
          Rate   Total         Rate   Total
          MB/s   Frames        MB/s   Frames
-------------------------------------------------------------------------------
fc1/15       181   1207557888405     258   1727973322943
MDS9718-A#
MDS9718-A# show interface fc1/15 counters detailed
fc1/15
 Rx 5 min rate bit/sec:                      1455865440
 Tx 5 min rate bit/sec:                      2036661120
 Rx 5 min rate bytes/sec:                      181983180
 Tx 5 min rate bytes/sec:                      254582640
 Rx 5 min rate frames/sec:                       136454
 Tx 5 min rate frames/sec:                       195363

 Total Stats:
 Rx total frames:                        1207559175743
 Tx total frames:                        1727975142493
 Rx total bytes:                       1613208106752576
 Tx total bytes:                       2257786210241096
 Rx total multicast:                            0
```

```
Tx total multicast:                            0
Rx total broadcast:                            0
Tx total broadcast:                            0
Rx total unicast:                       1207559175627
Tx total unicast:                       1727975142384
Rx total discards:                             0
Tx total discards:                             0
Rx total errors:                              0
Tx total errors:                              0
Rx class-2 frames:                             0
Tx class-2 frames:                             0
Rx class-2 bytes:                             0
Tx class-2 bytes:                             0
Rx class-2 frames discards:                        0
Rx class-2 port reject frames:                       0
Rx class-3 frames:                       1207546927035
Tx class-3 frames:                       1727965551223
Rx class-3 bytes:                      1613207164103092
Tx class-3 bytes:                      2257785595672952
Rx class-3 frames discards:                        0
Rx class-f frames:                         12248475
Tx class-f frames:                          9591012
Rx class-f bytes:                         942649484
Tx class-f bytes:                         614568144
Rx class-f frames discards:                        0

Link Stats:
Rx Link failures:                             3
Rx Sync losses:                              0
Rx Signal losses:                             0
Rx Primitive sequence protocol errors:                   0
Rx Invalid transmission words:                       0
Rx Invalid CRCs:                              0
Rx Delimiter errors:                            0
Rx fragmented frames:                           0
Rx frames with EOF aborts:                         0
Rx unknown class frames:                          0
Rx Runt frames:                              0
Rx Jabber frames:                             0
Rx too long:                                0
Rx too short:                               0
Rx FEC corrected blocks:                          0
Rx FEC uncorrected blocks:                         0
Rx Link Reset(LR) while link is active:                  9
Tx Link Reset(LR) while link is active:                  1
Rx Link Reset Responses(LRR):                       5
Tx Link Reset Responses(LRR):                       10
Rx Offline Sequences(OLS):                         7
Tx Offline Sequences(OLS):                         6
Rx Non-Operational Sequences(NOS):                     4
Tx Non-Operational Sequences(NOS):                     3

Congestion Stats:
Tx Timeout discards:                            0
Tx Credit loss:                              0
BB_SCs credit resend actions:                       0
BB_SCr Tx credit increment actions:                    0
TxWait 2.5us due to lack of transmit credits for VL 0:           0
TxWait 2.5us due to lack of transmit credits for VL 1:           0
TxWait 2.5us due to lack of transmit credits for VL 2:           0
TxWait 2.5us due to lack of transmit credits for VL 3:           0
Percentage TxWait not available for last 1s/1m/1h/72h:      0%/0%/0%/0%
Rx B2B credit remaining for VL 0:                     15
Rx B2B credit remaining for VL 1:                     15
Rx B2B credit remaining for VL 2:                     40
Rx B2B credit remaining for VL 3:                    430
Tx B2B credit remaining for VL 0:                     15
Tx B2B credit remaining for VL 1:                     15
Tx B2B credit remaining for VL 2:                     40
Tx B2B credit remaining for VL 3:                    430
Rx B2B credit transitions to zero for VL 0:                10
Rx B2B credit transitions to zero for VL 1:                4
Rx B2B credit transitions to zero for VL 2:                4
Rx B2B credit transitions to zero for VL 3:              210513
Tx B2B credit transitions to zero for VL 0:                11
Tx B2B credit transitions to zero for VL 1:                5
Tx B2B credit transitions to zero for VL 2:                5
Tx B2B credit transitions to zero for VL 3:                5

Other Stats:
Zone drops:                                0
FIB drops for ports 1-16:                        20
XBAR errors for ports 1-16:                        0
Other drop count:                             0
```

```
 Last clearing of "show interface" counters :            never
```

```
MDS9718-A#
```

NDFC SAN Controller starts monitoring interface utilization after enabling Performance Collections for a fabric. Switch port utilization graphs are accessible by navigating to **SAN > Interfaces > FC Ports** and selecting the Performance tab to view the statistics. Selecting the small graph icon next to an interface name will open its graph.



					Rx				Tx			
Fabric	Name	VSAN	Switch interface	Speed	Avg	Avg %	Peak	Peak %	Avg	Avg %	Peak	Peak %
Fab-A	C240_1_D8	20	MDS9396T-A fc1/37	16Gb/s	11.44MB/s	0	11.53MB/s	0	578.08MB/s	36	582.70MB/s	36
Fab-A	C240_3_C2	20	MDS9396T-A fc1/41	16Gb/s	237.64MB/s	14	240.87MB/s	15	237.97MB/s	14	241.28MB/s	15
Fab-B	B200-3-B2D	20	FI6248-1-B vfc1388(veth! channel1287)	16Gb/s	74.17MB/s	4	75.34MB/s	4	34.58MB/s	2	34.93MB/s	2
Fab-B	B200-3-B3D	20	FI6248-1-B vfc1390(veth! channel1287)	16Gb/s	62.50MB/s	3	66.45MB/s	4	28.86MB/s	1	30.24MB/s	1
Fab-B	B200-4-B0D	20	FI6248-1-B vfc1416(veth! channel1289)	16Gb/s	47.99MB/s	2	50.24MB/s	3	24.17MB/s	1	25.32MB/s	1
Fab-B	B200-4-B1D	20	FI6248-1-B vfc1418(veth! channel1289)	16Gb/s	46.71MB/s	2	48.91MB/s	3	23.52MB/s	1	24.68MB/s	1
Fab-A	B200-3-A2D	20	FI6248-1-A vfc1387(veth! channel1286)	16Gb/s	19.71MB/s	1	19.94MB/s	1	8.76MB/s	0	8.85MB/s	0

10 Rows   Page 1 of 3   1-10 of 24

Figure 13. Monitoring performance of switch interfaces in NDFC SAN Controller

The interface metrics can be exported to a third-party application using SNMP, NX-API, or streaming telemetry.

For more details on NX-API, refer to the references section to access the Cisco MDS 9000 Series Programmability Guide.

For more details on streaming telemetry, refer to the references section to access the Cisco MDS 9000 Series SAN Analytics and SAN Telemetry Streaming Configuration Guide.

SNMP polling

IF-MIB is a commonly used MIB to monitor interface metrics. Table 3 provides a list of commonly used SNMB MIB objects for monitoring the interfaces on MDS 9000 switches.

Table 3. Commonly used MIBs for monitoring interfaces on MDS 9000 switches

S.No	MIB name	OID	Description
1	ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	Number of bytes received by the interface

S.No	MIB name	OID	Description
2	ifHCOutOctets	1.3.6.1.2.1.31.1.1.1.10	Number of bytes transmitted by the interface
3	fcIfTxWaitCount	1.3.6.1.4.1.9.9.289.1.2.1.1.15	TxWait, the number of 2.5µs when a switch port could not transmit due to 0 Tx B2B credits
4	fcHCIfBBCreditTransistionFromZero	1.3.6.1.4.1.9.9.289.1.2.1.1.40	Tx B2B credit transition to zero
5	fcIfBBCreditTransistionToZero	1.3.6.1.4.1.9.9.289.1.2.1.1.39	Rx B2B credit transition to zero
6	fcIfTxWtAvgBBCreditTransitionToZero	1.3.6.1.4.1.9.9.289.1.2.1.1.38	Number of 100ms when a switchport could not transmit due to 0 Tx B2B credits
7	fcIfCreditLoss	1.3.6.1.4.1.9.9.289.1.2.1.1.37	Credit Loss (recovery) - Represents extended period (1 or 1.5 seconds) of 0 Tx B2B credits
8	fcIfTimeOutDiscards	1.3.6.1.4.1.9.9.289.1.2.1.1.35	Timeout discards
9	fcIfOutDiscards	1.3.6.1.4.1.9.9.289.1.2.1.1.36	Total number of frames discarded in egress direction, which includes timeout discards
10	fcIfLinkResetIns	1.3.6.1.4.1.9.9.289.1.2.1.1.9	Number of link reset protocol errors that are received by an FC port from the attached FC port
11	fcIfLinkResetOuts	1.3.6.1.4.1.9.9.289.1.2.1.1.10	Number of link reset protocol errors issued by the FC port to the attached FC port.
12	fcIfSlowportCount	1.3.6.1.4.1.9.9.289.1.2.1.1.44	Duration for which Tx B2B credits were unavailable on a port
13	fcIfSlowportOperDelay	1.3.6.1.4.1.9.9.289.1.2.1.1.45	Number of times for which Tx B2B credits were unavailable on a port for a duration longer than the configured admin-delay value in slowport-monitor
14	fcIfInvalidCrcs	1.3.6.1.4.1.9.9.289.1.2.1.1.6	Number of invalid CRC packets detected by an FC port

For more details, refer to the references section to access the Cisco MDS 9000 Family MIB Quick Reference and Monitoring and Alerting in Cisco MDS Fabric white paper.

Alerting on Interface Metrics Using Port-monitor (PMON)

Port-monitor (PMON) feature on MDS 9000 switches proactively monitors the ports on a MDS 9000 switch and automatically generates alerts when the metrics exceed the configured thresholds. The port metrics are monitored in real time at a low granularity (as low as 2.5 microseconds). When PMON generates an event, the notification is sent using Syslog and SNMP traps or informs.

Configure PMON for proactive and automatic notifications to monitor the health of the switch ports.

Refer to the references section to access the Sample MDS Port-Monitor Policies. A sample port-monitor policy for core and edge ports is shown below.

```
!
port-monitor name CorePorts
 logical-type core
 counter link-loss poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter sync-loss poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter signal-loss poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter invalid-words poll-interval 60 delta rising-threshold 1 event 4 falling-threshold 0 event 4
 counter invalid-crc poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter tx-discards poll-interval 60 delta rising-threshold 100 event 3 falling-threshold 10 event 3
 counter lr-rx poll-interval 60 delta rising-threshold 5 event 2 falling-threshold 1 event 2
 counter lr-tx poll-interval 60 delta rising-threshold 5 event 2 falling-threshold 1 event 2
 counter timeout-discards poll-interval 60 delta rising-threshold 100 event 3 falling-threshold 10 event 3
 counter credit-loss-reco poll-interval 60 delta rising-threshold 1 event 2 falling-threshold 0 event 2
 counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 event 4
 counter tx-datarate poll-interval 10 delta rising-threshold 80 event 4 falling-threshold 79 event 4
 counter err-pkt-from-port poll-interval 60 delta rising-threshold 50 event 3 falling-threshold 0 event 3
 counter err-pkt-to-xbar poll-interval 60 delta rising-threshold 50 event 3 falling-threshold 0 event 3
 counter err-pkt-from-xbar poll-interval 60 delta rising-threshold 50 event 3 falling-threshold 0 event 3
 counter tx-slowport-oper-delay poll-interval 1 absolute rising-threshold 80 event 4 falling-threshold 0 event 4
 counter txwait poll-interval 1 delta rising-threshold 20 event 4 falling-threshold 0 event 4
 monitor counter err-pkt-from-port
 monitor counter err-pkt-to-xbar
 monitor counter err-pkt-from-xbar
 no monitor counter state-change
 no monitor counter rx-datarate
!
port-monitor activate CorePorts
```

```
!
port-monitor name EdgePorts
 logical-type edge
 counter link-loss poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter sync-loss poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter signal-loss poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter invalid-words poll-interval 60 delta rising-threshold 1 event 4 falling-threshold 0 event 4
 counter invalid-crc poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
 counter tx-discards poll-interval 60 delta rising-threshold 50 event 3 falling-threshold 10 event 3
 counter lr-rx poll-interval 60 delta rising-threshold 5 event 2 falling-threshold 1 event 2
 counter lr-tx poll-interval 60 delta rising-threshold 5 event 2 falling-threshold 1 event 2
 counter timeout-discards poll-interval 60 delta rising-threshold 50 event 3 falling-threshold 10 event 3
 counter credit-loss-reco poll-interval 60 delta rising-threshold 4 event 2 falling-threshold 0 event 2
 counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 event 4
 counter tx-datarate poll-interval 10 delta rising-threshold 80 event 4 falling-threshold 79 event 4
 counter tx-slowport-oper-delay poll-interval 1 absolute rising-threshold 50 event 4 falling-threshold 0 event 4
 counter txwait poll-interval 1 delta rising-threshold 20 event 4 falling-threshold 0 event 4
 no monitor counter err-pkt-from-port
 no monitor counter err-pkt-to-xbar
 no monitor counter err-pkt-from-xbar
 no monitor counter state-change
 no monitor counter rx-datarate
!
port-monitor activate EdgePorts
!
```

The preceding policy only triggers notifications. No port-guard actions are taken which can be configured for:

- Port flap
- Errodisable port (shutdown)
- Cong-isolate (Congestion Isolation)
- Cong-isolate-recover (Recover the port from a state of congestion isolation)
- FPIN (Send a Fabric Performance Impact Notification)

- DIRL (Prevent congestion using Dynamic Ingress Rate Limiting)

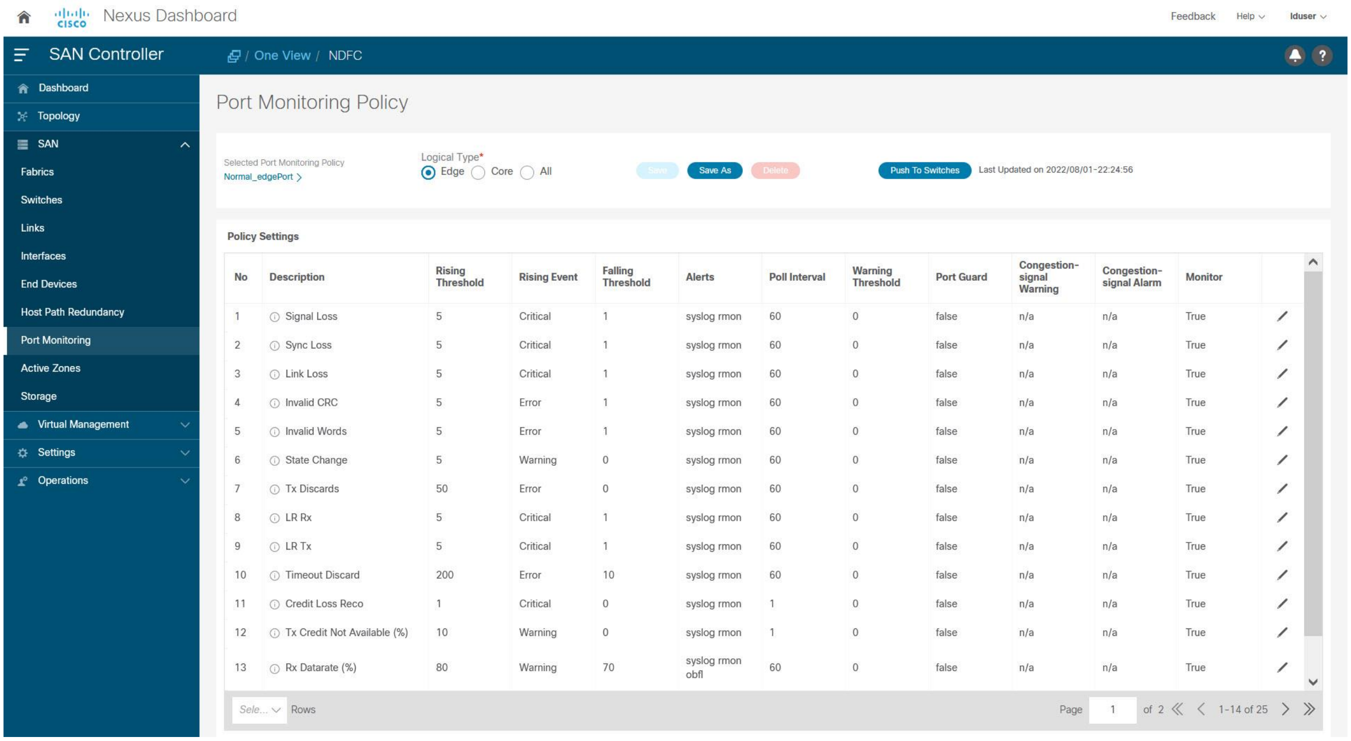
Enabling a port-guard action can be configured after a few initial weeks of soaking the thresholds values. Also, there is no single set of thresholds that fit all scenarios. The preceding policy is a good start. The aim should be to make the thresholds more aggressive if notifications are not received. When notifications are received, the root cause of the problem should be found and fixed before making the thresholds more aggressive.

We recommend configuring higher severity for important counters. For example, the impact due to a Link Reset (lr-rx and lr-tx) event is more severe than a condition when a port does not have enough transmitted B2B credits (txwait). Hence, the preceding sample policy configures lr-tx and lr-rx at severity level 2 and txwait to severity level 4.

Best Practice

Customize the severity of the PMON events for a higher level of attention at important events.

Port-monitor can also be configured by NDFC SAN Controller for a consistent policy across multiple switches and fabrics. Navigate to **SAN > Port Monitoring**. Select one of the existing policy templates or create your own by modifying and saving it with a custom name.



Port Monitoring Policy

Selected Port Monitoring Policy
Normal_edgePort

Logical Type* ● Edge ○ Core ○ All

Last Updated on 2022/08/01-22:24:56

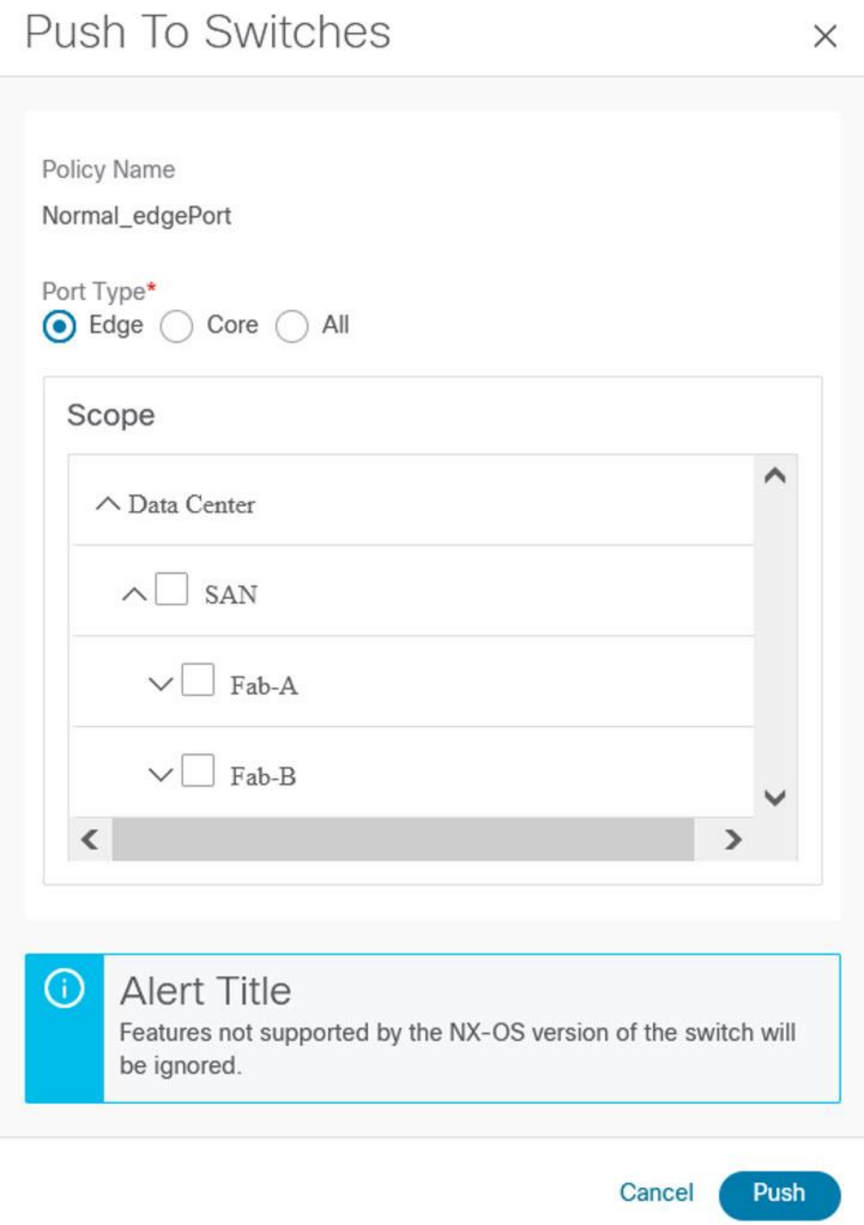
Policy Settings

No	Description	Rising Threshold	Rising Event	Falling Threshold	Alerts	Poll Interval	Warning Threshold	Port Guard	Congestion-signal Warning	Congestion-signal Alarm	Monitor
1	Signal Loss	5	Critical	1	syslog rmon	60	0	false	n/a	n/a	True
2	Sync Loss	5	Critical	1	syslog rmon	60	0	false	n/a	n/a	True
3	Link Loss	5	Critical	1	syslog rmon	60	0	false	n/a	n/a	True
4	Invalid CRC	5	Error	1	syslog rmon	60	0	false	n/a	n/a	True
5	Invalid Words	5	Error	1	syslog rmon	60	0	false	n/a	n/a	True
6	State Change	5	Warning	0	syslog rmon	60	0	false	n/a	n/a	True
7	Tx Discards	50	Error	0	syslog rmon	60	0	false	n/a	n/a	True
8	LR Rx	5	Critical	1	syslog rmon	60	0	false	n/a	n/a	True
9	LR Tx	5	Critical	1	syslog rmon	60	0	false	n/a	n/a	True
10	Timeout Discard	200	Error	10	syslog rmon	60	0	false	n/a	n/a	True
11	Credit Loss Reco	1	Critical	0	syslog rmon	1	0	false	n/a	n/a	True
12	Tx Credit Not Available (%)	10	Warning	0	syslog rmon	1	0	false	n/a	n/a	True
13	Rx Datarate (%)	80	Warning	70	syslog rmon obfl	60	0	false	n/a	n/a	True

Sele... Rows Page 1 of 2 1-14 of 25

Figure 14. Configuring port-monitor from NDFC SAN Controller

The threshold values can also be modified by clicking on the Edit option next to a specific policy row. Finally, click **Push To Switches** to configure the policy on one or multiple switches.



Push To Switches

Policy Name

Normal_edgePort

Port Type*

● Edge ○ Core ○ All

Scope

- Data Center
  - □ SAN
    - □ Fab-A
    - □ Fab-B

Alert Title

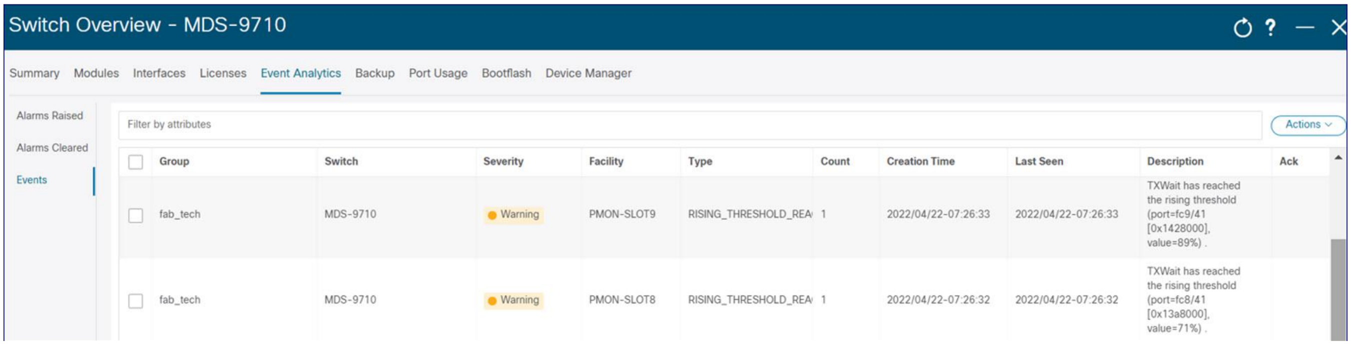
Features not supported by the NX-OS version of the switch will be ignored.

Figure 15. Configure Policy selected Switches

Following is a sample message that is generated by the port-monitor feature.

```
2022 Apr 22 07:26:31 MDS-9710 %PMON-SLOT9-4-RISING_THRESHOLD_REACHED_WARNING: TXWait has
reached the rising threshold (port=fc9/41 [0x1428000], value=89%) .
```

This alert is also sent to NDFC SAN Controller and is accessible by navigating to **SAN > Switches**, selecting the respective switch, and then navigating to **Event Analytics > Events**.



Switch Overview - MDS-9710

☐	Group	Switch	Severity	Facility	Type	Count	Creation Time	Last Seen	Description	Ack
☐	fab_tech	MDS-9710	● Warning	PMON-SLOT9	RISING_THRESHOLD_REA	1	2022/04/22-07:26:33	2022/04/22-07:26:33	TXWait has reached the rising threshold (port=fc9/41 [0x1428000], value=89%) .	
☐	fab_tech	MDS-9710	● Warning	PMON-SLOT8	RISING_THRESHOLD_REA	1	2022/04/22-07:26:32	2022/04/22-07:26:32	TXWait has reached the rising threshold (port=fc8/41 [0x13a8000], value=71%) .	

Figure 16. Viewing port-monitor events in NDFC SAN Controller

Monitoring and Alerting of Congestion and B2B credits

Cisco MDS 9000 switches and NDFC SAN Controller offer a strong feature-set to detect, troubleshoot, and automatically prevent SAN Congestion. An in-depth explanation of all the features is outside of the scope of this document. This section aims to help new users quickly get started with monitoring and automated alerting for congestion in a SAN fabric built using MDS 9000 switches. For more details, refer to the references section to access the Slow-Drain Device Detection, Troubleshooting, and Automatic Recovery white paper and Cisco MDS 9000 Series Interfaces Configuration Guide.

CLI

Monitoring of B2B credits and congestion is enabled by default on MDS 9000 switches. The metrics can be displayed by using **show interface <> counters detailed** command, as shown in the following snippet.

```
MDS-9710# show interface fc9/41 counters detailed
Fc9/41
<snip>
Congestion Stats:
 Tx Timeout discards:                            0
 Tx Credit loss:                              0
 TxWait 2.5us due to lack of transmit credits:         33174327296
 Percentage TxWait for last 1s/1m/1h/72h:          88%/89%/88%/31%
 Rx B2B credit remaining:                          0
 Tx B2B credit remaining:                          0
 Tx Low Priority B2B credit remaining:                   0
 Rx B2B credit transitions to zero:                7831888089
 Tx B2B credit transitions to zero:                9386174923
<snip>
 Last clearing of "show interface" counters :              never
MDS-9710#
```

The preceding command shows metrics in real time. A limited number of historic metrics and logs are stored in the persistent storage on the switch. This is called onboard failure logging (OBFL) and is accessible using **show logging onboard** command. For example, refer to the following snippet. The time at the execution of this command was 2022-04-25 09:17:32. The output displays that on Fri Apr 22 09:17:14 2022, interface fc9/41 was congested for 88% of the 20-seconds sampling period.

```
MDS9710-C# show logging onboard txwait
<snip>
---------------------------------
 Module: 9 txwait count
---------------------------------


----------------------------
Module: 9 show clock
----------------------------
2022-04-25 09:17:32


---------------------------------
Module: 9 txwait
---------------------------------
Notes:
   - Sampling period is 20 seconds
   - Only txwait delta >= 100 ms are logged


-----------------------------------------------------------------------------
| Interface | Delta TxWait Time   | Congestion | Timestamp        |
|      | 2.5us ticks | seconds |      |              |
-----------------------------------------------------------------------------
|  fc9/41 | 7088141   |  17   |   88%   | Fri Apr 22 09:17:14 2022 |
<snip>
```

For more details, refer to the references section to access the Cisco MDS 9000 Series System Management Configuration Guide.

In addition to the congestion, monitoring features that are enabled by default (for example, TxWait), the Slowport monitor is an important feature to detect Tx B2B credit unavailability duration on the ports of MDS 9000 switches.

Best Practice

Enable slowport-monitor for core and edge ports with 1-millisecond admin delay.

Slowport-monitor is not enabled by default. Enable it using **`system timeout slowport-monitor`** command.

```
MDS9718-A# conf t
MDS9718-A(config)# system timeout slowport-monitor 1 logical-type core
MDS9718-A(config)# system timeout slowport-monitor 1 logical-type edge
MDS9718-A(config)# end
MDS9718-A#
```

NDFC SAN Controller Slow Drain (Congestion) Analysis

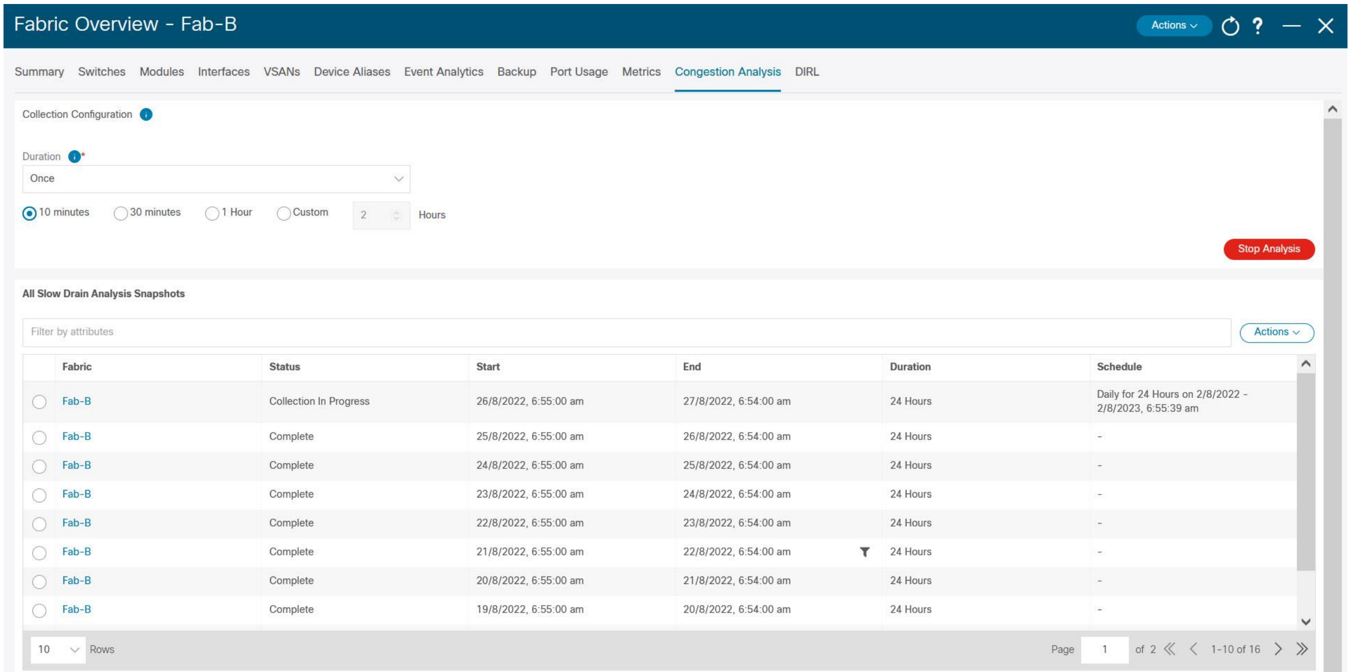
NDFC SAN Controller Slow Drain (Congestion) Analytics provides single-pane-of-glass visibility across the entire fabric. This feature is not enabled by default. Start the Slow Drain analysis in NDFC SAN Controller by navigating to **SAN > Congestion Analysis > Slow Drain** tab. Select a Fabric from the Fabric drop-down. Select **Daily** from the **Duration** drop-down. Select the **Custom** radio button and enter the number of hours to 24. Click the **Start Collection** button to start the Slow Drain Analysis.

In NDFC Release 12.1.1e, Slow Drain Analysis is renamed as Congestion Analytics and moved under Fabrics.

Best Practice

Schedule slow drain analysis on all the switches daily for 24 hours for always-on monitoring.

Repeat the same process for all the monitored fabrics. It is possible to visualize the results while the collection is in progress by selecting the Fabric under **All Slow Drain Analysis Snapshots**.



Collection Configuration

Duration*: Once

● 10 minutes ○ 30 minutes ○ 1 Hour ○ Custom 2 Hours

All Slow Drain Analysis Snapshots

Fabric	Status	Start	End	Duration	Schedule
Fab-B	Collection In Progress	26/8/2022, 6:55:00 am	27/8/2022, 6:54:00 am	24 Hours	Daily for 24 Hours on 2/8/2022 - 2/8/2023, 6:55:39 am
Fab-B	Complete	25/8/2022, 6:55:00 am	26/8/2022, 6:54:00 am	24 Hours	-
Fab-B	Complete	24/8/2022, 6:55:00 am	25/8/2022, 6:54:00 am	24 Hours	-
Fab-B	Complete	23/8/2022, 6:55:00 am	24/8/2022, 6:54:00 am	24 Hours	-
Fab-B	Complete	22/8/2022, 6:55:00 am	23/8/2022, 6:54:00 am	24 Hours	-
Fab-B	Complete	21/8/2022, 6:55:00 am	22/8/2022, 6:54:00 am	24 Hours	-
Fab-B	Complete	20/8/2022, 6:55:00 am	21/8/2022, 6:54:00 am	24 Hours	-
Fab-B	Complete	19/8/2022, 6:55:00 am	20/8/2022, 6:54:00 am	24 Hours	-

10 Rows

Figure 17. Slow Drain Analysis in NDFC SAN Controller

Metric Export using SNMP, NX-API, or Streaming Telemetry

The Congestion metrics that are collected by MDS 9000 switches can be exported to remote agents using SNMP, NX-API, or streaming Telemetry. Refer to Table 3 for a list of import SNMP MIB objects for Congestion monitoring.

NX-API monitoring can be used to request the output of `show interface counter detail` command which contains most of the congestion metrics. Streaming telemetry can be used to export the interface counters which contain congestion metrics also.

Congestion Alerting

Automatic alerting on SAN Congestion should be enabled using port-monitor. For more details and sample configuration, refer to the section on Interface State and Performance monitoring and Alerting.

Best Practice

Use Slow Drain Analysis in NDFC SAN Controller and port-monitor on MDS 9000 switches together.

We recommend using NDFC SAN Controller Slow Drain Analysis for fabric-wide monitoring. Proactive and automated alerting should be enabled using the port-monitor feature on the MDS 9000 switches. Both features serve different purposes and complement each other. When proactive notifications are received from PMON, historic trends and seasonality can be inspected using the NDFC SAN Controller slow drain analysis.

Fabric Services Monitoring and Alerting

Cisco MDS 9000 switches have more inbuilt monitoring for FC/FCoE services like FCNS database, zoning, VSAN, and so on. The notifications can be sent using Syslog and SNMP traps or informs. Email notifications can also be generated by MDS 9000 switches using Call Home or by NDFC SAN Controller using the event forwarding.

Fibre Channel Name Server (FCNS)

FCNS service can be monitored using CISCO-NS-MIB. The two important components of this MIB are

- **fcNameServerEntryAdd**: Name Server sends this notification whenever a new entry is added to the Name Server database.
- **fcNameServerEntryDelete**: Name Server sends this notification whenever an existing entry is deleted from the Name Server database.

Not all SNMP traps are enabled by default. If necessary, more traps can be enabled by using `snmp-server enable traps` command.

Also, RMON based alerting can be enabled on the switches using the Threshold Manager in Device Manager. For more details and examples, refer to the section on Threshold-based alerting from common switch components.

VSAN

VSAN service can be monitored using CISCO-VSAN-MIB, CISCO-VSAN-CAPABILITY, and CISCO-VLAN-MEMBERSHIP-MIB.

Like the FCNS traps, not all the SNMP traps are enabled by default. If necessary, more traps can be enabled by using `snmp-server enable traps` command.

Also, RMON based alerting can be enabled on the switches using the Threshold Manager in Device Manager. For more details and examples, refer to the section on Threshold-based alerting from common switch components.

Zoning

Zoning service can be monitored using CISCO-ZS-MIB and CISCO-ZS-EXT-MIB. Alerts are also generated using EEM. For example, `zone_members_max_per_sw` system policy generates a system message which can be sent via Syslog when the number of zones exceeds the maximum limit per switch.

Like the FCNS traps, not all SNMP traps are enabled by default. If necessary, more traps can be enabled by using `snmp-server enable traps` command.

Also, RMON based alerting can be enabled on the switches using the Threshold Manager in Device Manager. For more details and examples, refer to the section on Threshold-based alerting from common switch components.

NDFC One view

NDFC One view provides centralized management and visualization of multiple SAN environments that are managed by different NDFC servers. This single pane of glass provides insight into what is happening within the Fibre Channel SANs at multiple locations in one single view. These NDFC servers may be hosted on a one-node Nexus Dashboard or three-node Nexus Dashboard clusters that may be spread across the globe or managed by different teams within the same site. After creating multicluster connectivity among the Nexus Dashboard servers, a centralized dashboard provides a unified global view of the entire SAN install base. Also, single sign-on (SSO) allows seamless click-thru navigation to any of the servers that are participating within NDFC One view.

NDFC One view is available only for remote authentication users.

Best Practice

Use NDFC One view with remote authentication for centralized management of global SAN infrastructure

Nexus Dashboard One view and NDFC One view are different features. Nexus Dashboard One view (Figure 17) provides centralized management of Nexus Dashboard itself, which is a hosting platform in which applications such as NDFC can run. In contrast, NDFC One view provides centralized management of the SAN Infrastructure that's managed by different NDFC servers. NDFC One view is available with Release 12.1.1e onwards for SAN Controller only and is a no additional cost feature of NDFC.

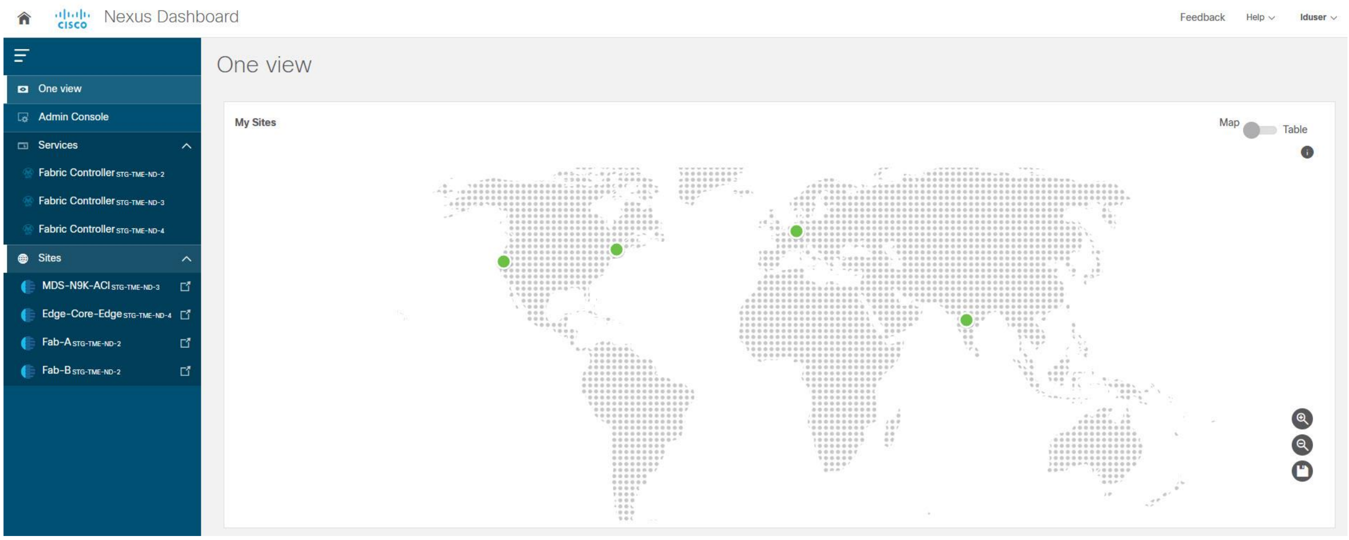
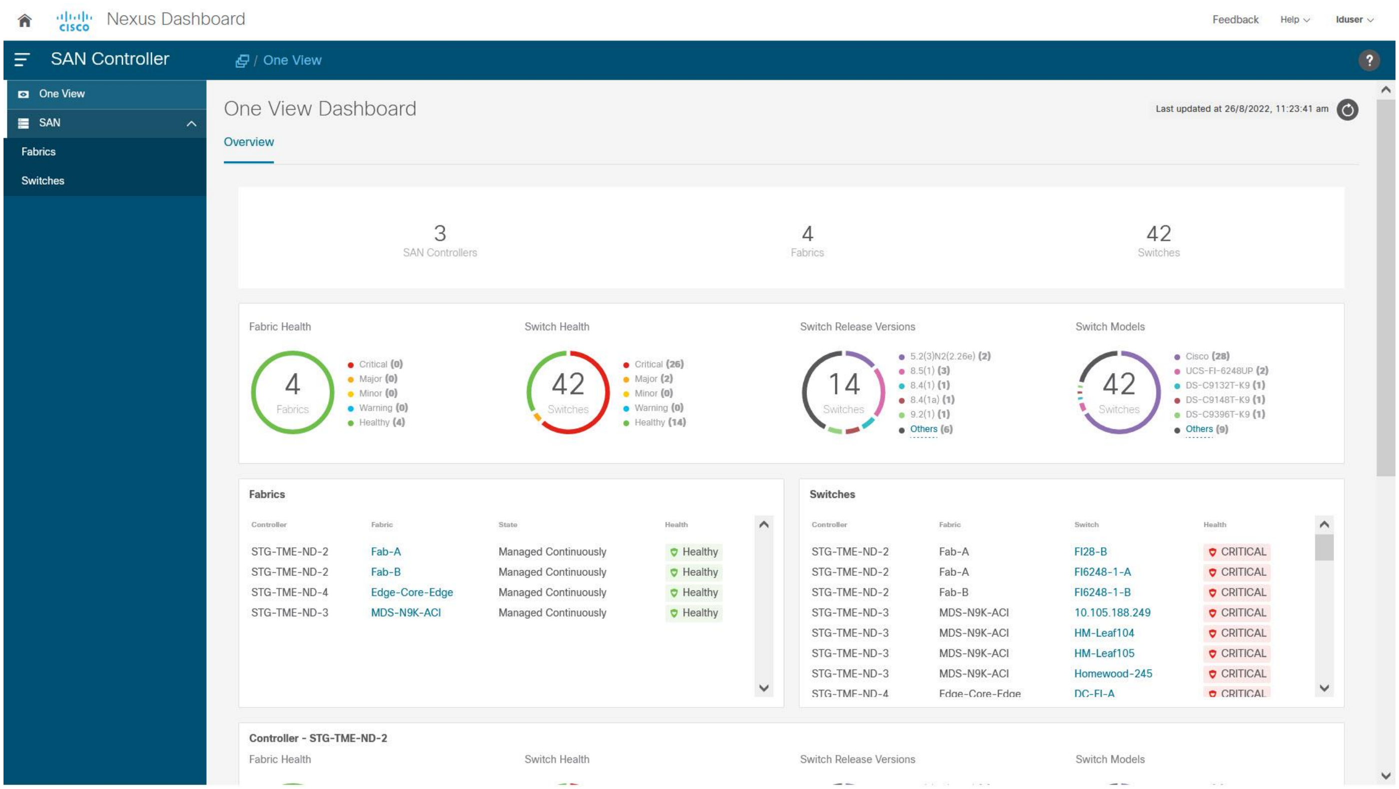


Figure 18. Nexus Dashboard One view



3 SAN Controllers | 4 Fabrics | 42 Switches

Fabric Health – 4 Fabrics: Critical (0), Major (0), Minor (0), Warning (0), Healthy (4)

Switch Health – 42 Switches: Critical (26), Major (2), Minor (0), Warning (0), Healthy (14)

Switch Release Versions – 14 Switches: 5.2(3)N2(2.26e) (2), 8.5(1) (3), 8.4(1) (1), 8.4(1a) (1), 9.2(1) (1), Others (6)

Switch Models – 42 Switches: Cisco (28), UCS-FI-6248UP (2), DS-C9132T-K9 (1), DS-C9148T-K9 (1), DS-C9396T-K9 (1), Others (9)

Fabrics

Controller	Fabric	State	Health
STG-TME-ND-2	Fab-A	Managed Continuously	Healthy
STG-TME-ND-2	Fab-B	Managed Continuously	Healthy
STG-TME-ND-4	Edge-Core-Edge	Managed Continuously	Healthy
STG-TME-ND-3	MDS-N9K-ACI	Managed Continuously	Healthy

Switches

Controller	Fabric	Switch	Health
STG-TME-ND-2	Fab-A	FI28-B	CRITICAL
STG-TME-ND-2	Fab-A	FI6248-1-A	CRITICAL
STG-TME-ND-2	Fab-B	FI6248-1-B	CRITICAL
STG-TME-ND-3	MDS-N9K-ACI	10.105.188.249	CRITICAL
STG-TME-ND-3	MDS-N9K-ACI	HM-Leaf104	CRITICAL
STG-TME-ND-3	MDS-N9K-ACI	HM-Leaf105	CRITICAL
STG-TME-ND-3	MDS-N9K-ACI	Homewood-245	CRITICAL
STG-TME-ND-4	Edge-Core-Edge	DC-FI-A	CRITICAL

Controller - STG-TME-ND-2

Fabric Health | Switch Health | Switch Release Versions | Switch Models

Figure 19. Nexus Dashboard Fabric Controller (NDFC) One view

Summary of Best Practices

Following is a summary of the best practices that are discussed in this document:

- We recommend using NTP to synchronize the clocks between the monitored SAN switches and the monitoring agent (NDFC SAN Controller) before setting up alerting and event notifications. It helps in having consistent timestamps on the events that are generated by the managed switches and as displayed by the monitored agent (NDFC).
- We recommend using SHA-AES as authentication and Privacy mode for NDFC SAN Controller to discover MDS 9000 SAN fabric and the connected UCS Fabric Interconnects.
- For NDFC SAN Controller to discover and monitor UCS Fabric Interconnects, servers, and traffic, we recommend using different name strings for snmp-user and read-only user in UCS Manager. This approach helps in better troubleshooting if any issues are found in the discovery process.
- We recommend enabling sending of syslog to NDFC SAN Controller. This functionality is not enabled by default and must be configured explicitly.
- We recommended using NDFC SAN Controller Event Forwarding to generate email notifications from a managed Cisco SAN Fabric. NDFC SAN Controller Event Forwarding acts as a single source to send email notifications using rule-based filtering on a central repository of the logs and events.
- We recommend limiting the number of agents monitoring the same MDS 9000 switch to less than 3. The monitoring agents can be Cisco NDFC SAN Controller or other third-party applications.

- We recommend limiting the number of event notification destinations (SNMP trap or inform, Syslog, and so on.) from an MDS 9000 switch to less than 3. The destinations of the events can be Cisco NDFC SAN Controller or other third-party applications.
- RMON threshold-based alerting is recommended to be configured using NDFC SAN Controller. Although the configuration is possible using NX-OS CLI, configuration from NDFC SAN Controller is easier and does not require knowing the exact SNMP OID.
- We recommend configuring the port-monitor (PMON) feature on MDS 9000 switches to generate proactive and automatic event notifications based on the health of the switch ports, for example, high utilization, CRC, congestion, and so on.
- In the port-monitor (PMON) policies, we recommend customizing the severity of events (using event-id) as per the severity of the monitored metric.
- We recommend configuring the slowport-monitor feature for core and edge ports with an admin delay of 1 millisecond. Enabling slowport-monitor can help to identify fabric level congestion. This functionality is not enabled by default and must be configured explicitly.
- We recommend running NDFC SAN Controller Slow Drain Analysis for always-on monitoring to help identify where slow drain symptoms are occurring within the fabric. To achieve this, schedule Slow drain analysis to run daily for 24 hours. This functionality is not enabled by default and must be configured explicitly on NDFC SAN Controller.
- We recommend using the Slow Drain Analysis in NDFC SAN Controller and port-monitor (PMON) on MDS 9000 switches. These features complement each other to help automatically identify fabric-level congestion symptoms.
- Use NDFC One view with remote authentication for centralized management of global SAN infrastructure

Conclusion

This document provides step-by-step guidance and best practices to configure automated monitoring and alerting in a Cisco SAN fabric. The hardware and the software components on the MDS 9000 switches collect the metrics and the logs in real time. In addition to the health of a SAN fabric, Cisco SAN Analytics provides at-the-scale visibility into the end-to-end I/O flows. The collected metrics and logs can be exported over SNMP, NX-API, Syslog, or streaming telemetry in an open format to a compatible third-party app or Cisco Nexus Dashboard Fabric Controller (NDFC) SAN Controller. The automated monitoring and alerting features available on MDS 9000 switches and NDFC SAN Controller help in achieving proactive operations, reduced downtimes, and improved SLAs.

References

- Cisco Nexus Dashboard Deployment Guide
- Cisco Nexus Dashboard Fabric Controller Installation and Upgrade Guide
- Cisco SNMP Object Navigator
- Cisco MDS 9000 Series Programmability Guide
- Cisco MDS 9000 Series SAN Analytics and SAN Telemetry Streaming Configuration Guide
- Slow-Drain Device Detection, Troubleshooting, and Automatic Recovery white paper

- Cisco MDS 9000 Family MIB Quick Reference
- Sample MDS Port-Monitor Policies
- Nexus Dashboard Fabric Controller (SAN) API
- MDS SDK Project on GitHub
- MDS SDK documentation
- Cisco UCS Manager configuration guide

Legal Information

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.