Fabrics

Fabrics

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

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

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

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

Action Item	Description
Add Fabric	From the **Actions** drop-down list, select **Add Fabric**. For more instructions, see Adding a Fabric, on page 2.
Edit Fabrics	Select a fabric to edit. From the **Actions** drop-down list, select **Edit Fabrics**. Make the necessary changes and click **Apply**. For more instructions, see Editing a Fabric, on page 5.
Delete Fabrics	Select one or more fabrics to delete. From the **Actions** drop-down list, select **Delete Fabrics**. Click **Confirm** to delete the fabrics. For more instructions, see Deleting a Fabric, on page 6.
Rediscover Fabrics	Allows you to rediscover the switches, links, and end devices associated with the fabric. Select one or more fabrics to rediscover. From the **Actions** drop-down list, select **Rediscover Fabrics**. A progress bar in the **State** column displays the rediscovery progress. For more instructions, see Rediscovering a Fabric, on page 6.
Purge Fabrics	Allows you to purge non-existent switches, links, and end devices of the fabric. Select one or more fabrics to purge. From the **Actions** drop-down list, select **Purge Fabrics**. For more instructions, see Purging a Fabric, on page 6.
Configure Performance	Allows you to enable performance monitoring on links, switch interfaces, and end devices associated with the fabric. Select one or more fabrics for performance monitoring. From the **Actions** drop-down list, select **Configure Performance**. Make the necessary changes and click **Apply**. For more instructions, see Configuring Performance.
Configure SAN Insights	Allows you configure SAN Insights on the selected fabric. For more instructions, see Configuring SAN Insights.
Configure Backup	Allows you to configure and schedule backup for the fabric data. For more instructions, see Configuring Fabric Backup, on page 17.

This chapter contains below sections:

Adding a Fabric

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

Procedure

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

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

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

Step 4 Select the **Fabric Seed Switch Type**.

From Release 12.1.2e, NDFC allows you to discover **Cisco** and **Non-Cisco** switches to SAN Fabrics.

Step 5 If you chose **Cisco** in the **Fabric Seed Switch Type**, perform the following:

a) In the **Fabric Seed Switch** field, enter the IP address of the seed switch.

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

b) Check the **SNMPv3/SSH** check box to enable access.

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

d) In the **User Name** and **Password** fields, enter appropriate details to access the seed switch if SNMPv3 is used.

Note If SNMPv3/SSH is not used, enter appropriate community string in the **Community String** field.

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

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

f) To discover switches using UCS credentials, check the **Use UCS Credentials** check box.

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

  You must provide different SNMP details if you uncheck this check box.
- To use SNMP for UCS, check the **Use SNMPv3 for UCS** check box.
- In the **User Name** and **Password** fields, enter appropriate details to access the seed switch if SNMPv3 is used.

  Note If SNMPv3/SSH is not used, enter appropriate community string in the **UCS SNMP Community String** field.

- Enter appropriate community string in the **UCS SNMP Community String** field, if SNMPv3 is not used.

Step 6 If you chose **Non-Cisco** in the **Fabric Seed Switch Type**, perform the following:

a) In the **Fabric Seed Switch** field, enter the IP address of the seed switch.

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

b) Check the **SNMPv3/SSH** check box to enable access.

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

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

e) In the **Non-Cisco Switch CLI Credentials**, provide appropriate username and password to access non-Cisco seed switch.

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

- Enter the appropriate **UCS CLI Credentials** in the username and password fields.

- To use the same SNMP credentials, check the **Use same SNMP Credentials for UCS** check box.

  You must provide different SNMP details if you uncheck this check box.

- To use SNMP for UCS, check the **Use SNMPv3 for UCS** check box.

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

  Enter UCS SNMP username and password in appropriate fields.

- If **Use SNMPv3 for UCS** is unchecked, enter appropriate community string in the **UCS SNMP Community String** field.

Step 7 Click **Add** to add a Fabric.

Note When you start SAN fabric discovery, after 15 minutes of fabric discovery the following process are scheduled on NDFC:

- If the fabric is licensed, Performance Manager (PM) collection is initiated.
- The Congestion Analysis job is scheduled to run continuously for a year. This job run will initiate after an hour of the schedule.

ESXi Networking for Promiscuous Mode

From Cisco NDFC Release 12.1.2e, you can run NDFC on top of virtual Nexus Dashboard (vND) instance with promiscuous mode that is disabled on port groups that are associated with Nexus Dashboard interfaces where External Service IP addresses are specified. vND comprises Nexus Dashboard management interface and data interface. By default, for fabric controller persona, two external service IP addresses are required for the Nexus Dashboard management interface subnet.

Before the NDFC Release 12.1.2e, if Inband management or Endpoint Locator or POAP feature was enabled on NDFC, you must also enable promiscuous mode for the Nexus Dashboard data or fabric interface port-group. This setting was mandatory for traffic flow that is associated for these features.

Enabling promiscuous mode raise risk of security issues in NDFC, it is recommended to set default setting for promiscuous mode.

Note

- Disabling promiscuous mode is supported from Cisco Nexus Dashboard Release 2.3.1c.
- You can disable promiscuous mode when Nexus Dashboard nodes are layer-3 adjacent on the Data network, BGP is configured, and fabric switches are reachable through the data interface.
- You can disable promiscuous mode when Nexus Dashboard interfaces are layer-2 adjacent to switch mgmt0 interface.

If Inband management or EPL is enabled, you must specify External Service IP addresses in the Nexus Dashboard data interface subnet. You can disable promiscuous mode for the Nexus Dashboard data or fabric interface port-group. For more information, refer to Cisco Nexus Dashboard Deployment Guide

Note Default option for promiscuous mode is **Reject**.

Procedure

Step 1 Log into your **vSphere** Client.

Step 2 Navigate to the ESXi host.

Step 3 Right-click the host and choose **Settings**.

A sub-menu appears.

Step 4 Choose **Networking** > **Virtual Switches**.

All the virtual switches appear as blocks.

Step 5 Click **Edit Settings** of the VM Network.

Step 6 Navigate to the **Security** tab.

Step 7 Update the **Promiscuous mode** settings as follows:

- Check the **Override** check box.
- Choose **Accept** from the drop-down list.

Step 8 Click **OK**.

Editing a Fabric

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

Procedure

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

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

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

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

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

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

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

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

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

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

Deleting a Fabric

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

Procedure

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

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

Rediscovering a Fabric

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

Procedure

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

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

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

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

The **Fabric** is rediscovered.

Purging a Fabric

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

Procedure

Step 1 Choose **SAN > Fabrics**.

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

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

The Fabric is purged.

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

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

The **Fabric** is purged.

Configuring Performance

If you are managing your switches with the performance manager, you must set up an initial set of flows and collections on the switch. You can use SAN Controller to add and remove performance collections. License the switch and keep it in the **managedContinuously** state before creating a collection for the switch. Only licensed fabrics appear in this window.

Procedure

Step 1 Choose **SAN > Fabrics**.

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

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

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

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

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

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

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

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

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

What to do next

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

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

SAN Insights

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

SAN Controller supports SAN Telemetry Streaming (STS) using compact GPB transport, for better telemetry performance and to improve the overall scalability of SAN Insights.

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

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

Prerequisites

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

Configuring Persistent IP Address

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

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

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

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

Procedure

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

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

The **External Service Pools** window appears.

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

Step 4 Click **Save**.

Changing Persistent IP Address

From Cisco NDFC Release 12.1.2e, you can change persistent IP addresses which are assigned for mandatory pods such as POAP-SCP and SNMP trap. To change the persistent IP address, perform the following steps:

Procedure

Step 1 On Cisco NDFC Web UI, navigate to **Settings** > **Server Settings** > **Admin** under **LAN Device Management Connectivity** drop-down list change **Management** to **Data** or conversely.

Changing option results in migration of SNMP and POAP-SCP pods to the persistent IP addresses associated with **External Service Pool** on Nexus Dashboard connected with the new **LAN Device Management Connectivity** option. After the completion of this process, the following message is displayed:

Some features have been updated. Reload the page to see latest changes.

Click **Reload the page**.

Step 2 On Cisco Nexus Dashboard Web UI, navigate to **Infrastructure** > **Cluster Configuration** > **General**, in **External Service Pools** card, change the required IP addresses for **Management Service IP Usage** or **Data Service IP Usage**.

Step 3 Navigate to NDFC Web UI **Server Settings** page, change the option in **LAN Device Management Connectivity** drop-down list to its initial selection.

Restoring this option to initial settings, results in migration of the SNMP and POAP-SCP pods to use the updated persistent IP address from the appropriate External Service IP pool.

Guidelines and Limitations

- Ensure that the time configurations in SAN Controller and the supported switches are synchronized to the local NTP server for deploying the SAN Insights feature.
- Any applicable daylight time savings settings must be consistent across the switches and SAN Controller.
- To modify the streaming interval, use the CLI from the switch, and remove the installed query for SAN Controller. Modify the **san.telemetry.streaming.interval** property in the SAN Controller server properties. The allowed values for the interval are 30–300 seconds. The default value is 30 seconds. If there is an issue with the default value or to increase the value, set default value to 60 seconds. You can change the default value while configuring SAN Insights. On **Switch configuration** wizard in **Interval(s)** column select required value from drop-down list.
- The port sampling window on the switch side should have all ports (default).
- Use the ISL query installation type only for the switches that have storage connected (storage-edge switches).

- For the ISL query installation type, in the Configure SAN Insights wizard, analytics can't be enabled on interfaces that are members of port-channel ISL to non-MDS platform switches.
- After installing the switch-based FM_Server_PKG license, the Configure SAN Insights wizard may take upto 5 minutes to detect the installed license.

For information about the SAN Insights dashboard, see SAN Insights Dashboard.

For information about configuring the SAN Insights, see Configuring SAN Insights.

Server Properties for SAN Insights

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

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

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

Table 1: Server Properties for SAN Insights

Field Name	Description	Default Value
Telemetry pages default protocol scsi/nvme	Specifies the required default protocol selection in the SAN Insights UI pages to view corresponding data: SCSI or NVMe.	SCSI
SAN Insights ECT thread count	Specifies number of threads to use for ECT queries.	4
Max. Aggregation bucket size	Specifies maximum number of buckets to use for aggregation queries.	40,000
Data table download size	Specifies number of records for table download.	1000
ECT Data limit	Specifies the ECT Data limit.	14 **Note** The value of ECT data limit must be less than or equal to the value of SAN Telemetry retention policy - baseline / post processed.

Field Name	Description	Default Value
SAN Telemetry deviation low threshold	Specifies the value that is the change point between normal and low.	1
SAN Telemetry deviation med threshold	Specifies the value that is the change point between low and medium.	15
SAN Telemetry deviation high threshold	Specifies the value that is the change point between medium and high.	30
SAN Telemetry deviation low threshold for NVMe	Specifies the value that is the change point between normal and low for NVMe.	1
SAN Telemetry deviation med threshold for NVMe	Specifies the value that is the change point between low and medium for NVMe.	2
SAN Telemetry deviation high threshold for NVMe	Specifies the value that is the change point between medium and high for NVMe.	5
SAN Telemetry training timeframe	Specifies the training time frame for flows ECT baseline.	7 days
SAN Telemetry training reset timeframe	Specifies the time duration to periodically restart the ECT baseline training after number of days.	14 days
SAN Telemetry retention policy - baseline / post processed	Specifies the retention policy - baseline / post processed.	14
SAN Telemetry retention policy - hourly rollups	Specifies the retention policy - hourly rollups	90
Telemetry Gap Reset Interval	Specify maximum valid time gap between records (before drop) time is in seconds	750
Active Anomaly Capture	Specify maximum number of actively tracked anomalies per post processor.	500
Baseline training include NOOP frames	Specify if the baseline learning should reference noop frames.	Not selected
Baseline training includes negative deviation	Specify if the baseline deviation must include negatives.	Selected
Use telemetry Gap Reset Interval	Specifies the use telemetry reset based on time gap between records	Selected

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

Table 2: Required System Memory for SAN Controller with SAN Insights

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

Table 3: Verified limit for SAN Insights deployment

Deployment Type	Verified Limit[1] [2]
Cisco Virtual Nexus Dashboard (1 Node)	1M ITLs/ITNs 80K ITLs/ITNs
Cisco Physical Nexus Dashboard (1 Node)	120K ITLs/ITNs
Cisco Virtual Nexus Dashboard (3 Node)	150K ITLs/ITNs
Cisco Physical Nexus Dashboard (3 Node)	500K ITLs/ITNs

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

Note For one Node vND to support 1M ITLs/ITNs, it requires 3TB of SSD and 128 GB of memory Nexus Dashboard as system requirement.

Configuring SAN Insights

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

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

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

Before you begin

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

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

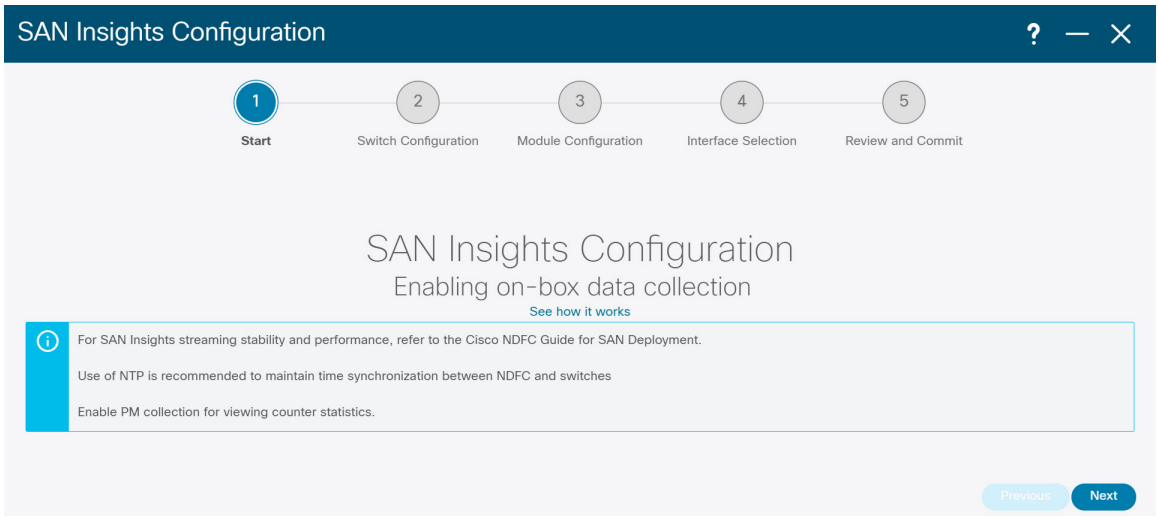
Note You must configure with sufficient system requirements and IP addresses. For more information on scale limits, refer to table Required System Memory for SAN deployment in Server Properties for SAN Insights.

Procedure

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

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

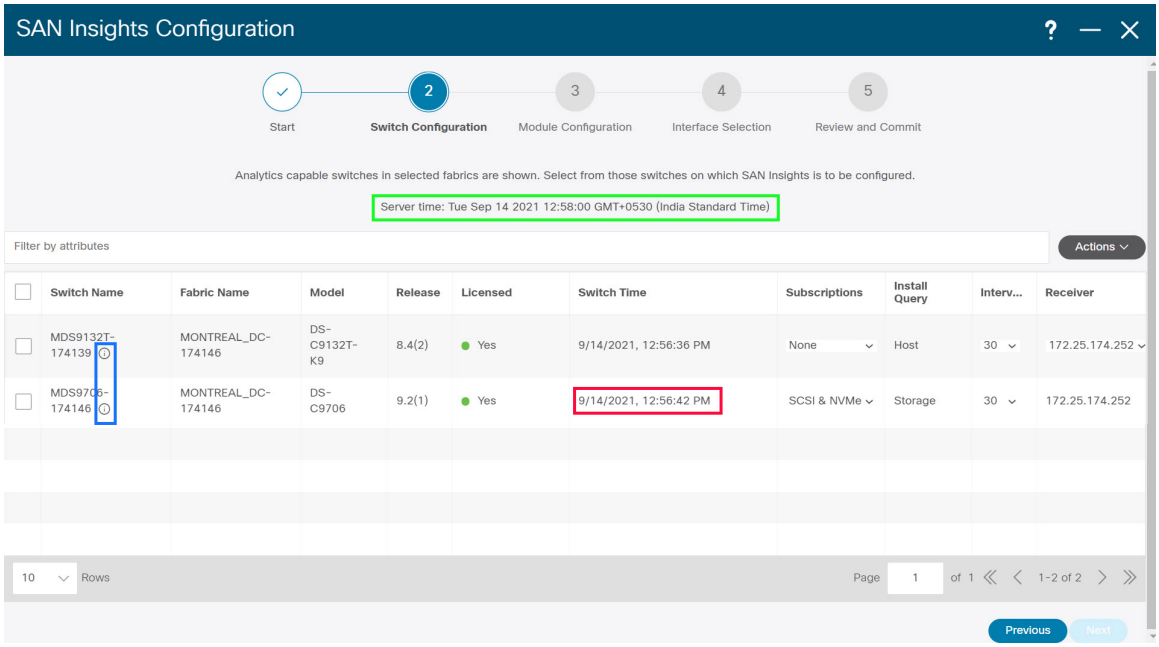
The **SAN Insights Configuration** wizard appears.



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

The **Switch Configuration** wizard appears.

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



If the switches don't have SAN Insights license, the status in the Licensed column shows **No (install licenses)**. Click on **Install licenses** to apply license to the switch.

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

For the selected SAN Controller Receiver in the last column, the receiver can subscribe to telemetry: SCSI only, NVMe only, both SCSI & NVMe, or None. This allows you to configure one SAN Controller server to receive SCSI telemetry and another SAN Controller server to receive NVMe telemetry.

In SAN Controller deployment, the IP address assigned to eth0 or eth1 can be used for receiving SAN Insights streaming from the switch. However, ensure that streaming is configured to the SAN Controller interface having IP reachability from the respective switches. In the **Receiver** column all the discovered interfaces are listed. Choose the corresponding interface IP address that is configured while installing SAN Controller for streaming analytics data from the switch.

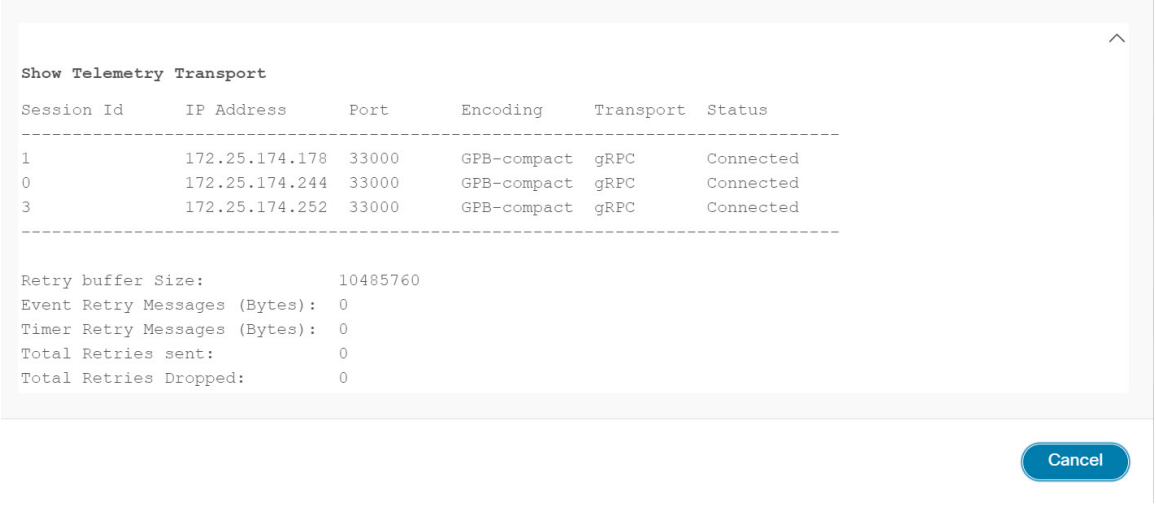
You can provide management IP eth0 and data IP eth1 for fabric access to bootstrap the SAN Controller. Therefore, the streaming must be configured to the persistent IP assigned in the data-IP subnet. Refer to the Configuring Persistent IP Address, on page 8 section for more information.

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

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

Note If you choose **None for Subscription**, a warning message is displayed to select an appropriate Subscription before you proceed. Select the desired protocols for Subscription.

You can click the **i** icon in the **Switch Name** column to get the configuration details for analytics and telemetry features from the switch (if Analytics Query and Telemetry features are configured).



If Analytics Query of either type (dcnminitITL, dcnmtgtITL, dcnmislpcITL, dcnminitITN, dcnmtgtITN, or dcnmislpcITN) isn't configured on the switch, the telemetry configurations won't be displayed.

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

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

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

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

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

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

In the **Install Query** column, type of port per switch is displayed. The port types are:**ISL**, **host**, or **storage**.

- **host**—lists all ports where hosts or initiators are connected on the switch.
- **storage**—lists all ports where storage or targets are connected on the switch.
- **ISL**—lists all ISL and port channel ISL ports on the switch.
- **None**—indicates that no query is installed.

The following queries are used:

- dcnmtgtITL/dcnmtgtITN—This is the storage-only query.
- dcnminitITL/dcnminitITN—This is the host-only query.
- dcnmislpcITL/dcnmislpcITN—This is the ISL and pc-member query.

Note ISL based queries must be added when you use the ISL query installation type for the switches that has connected to storage (storage-edge switches).

Note SAN Controller doesn't manage duplicate ITLs\ITNs. If you configure both host and storage queries (on the switches where their Hosts and Storage are connected respectively), the data is duplicated for the same ITL\ITN. This results in inconsistencies in the computed metrics.

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

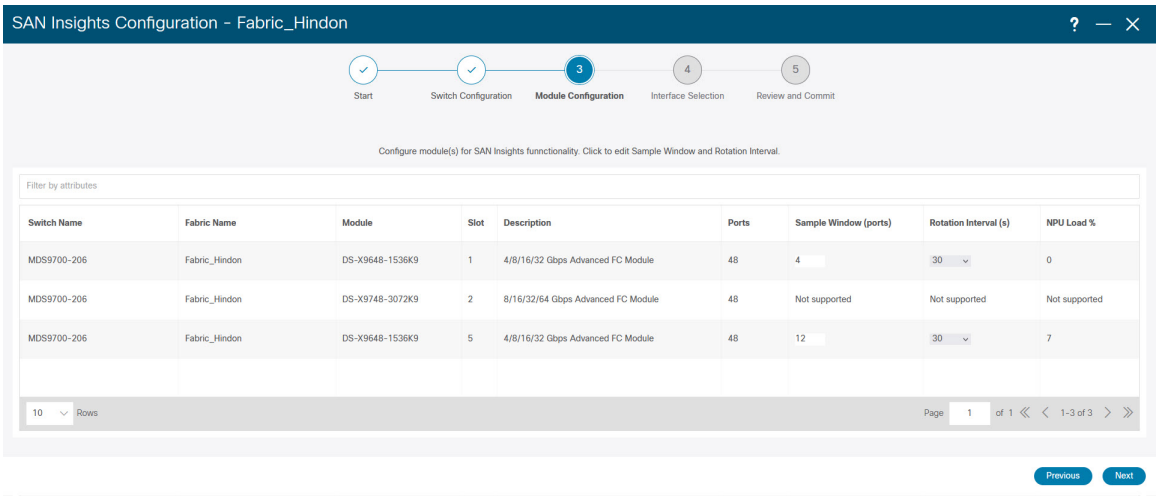
Step 7 Click **Next**.

You can see all the analytics supported modules on the switches selected in the previous view, listed with the respective instantaneous NPU load in the last column. Port-sampling configuration (optional) and port-sampling rotation interval for the module can be specified in this step. The default configuration on the switch is to monitor all analytics-enabled ports on the switch for analytics.

Note If port sampling is enabled on multiple ISL ports with ISL query installed, the metrics aggregation isn’t accurate. Because all exchanges won’t be available at the same time, the metrics aggregation isn’t accurate. We recommend that you don’t use port sampling with ISL queries, with multiple ISLs.

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

Beginning with Release 12.1.1e, Cisco NDFC supports discovery of 64G modules and can be selected during SAN Insights configuration. Port-sampling is not supported on these modules and NPU load is not applicable for 64G SAN analytics. Therefore, you cannot configure sample window and rotation interval for 64G modules.



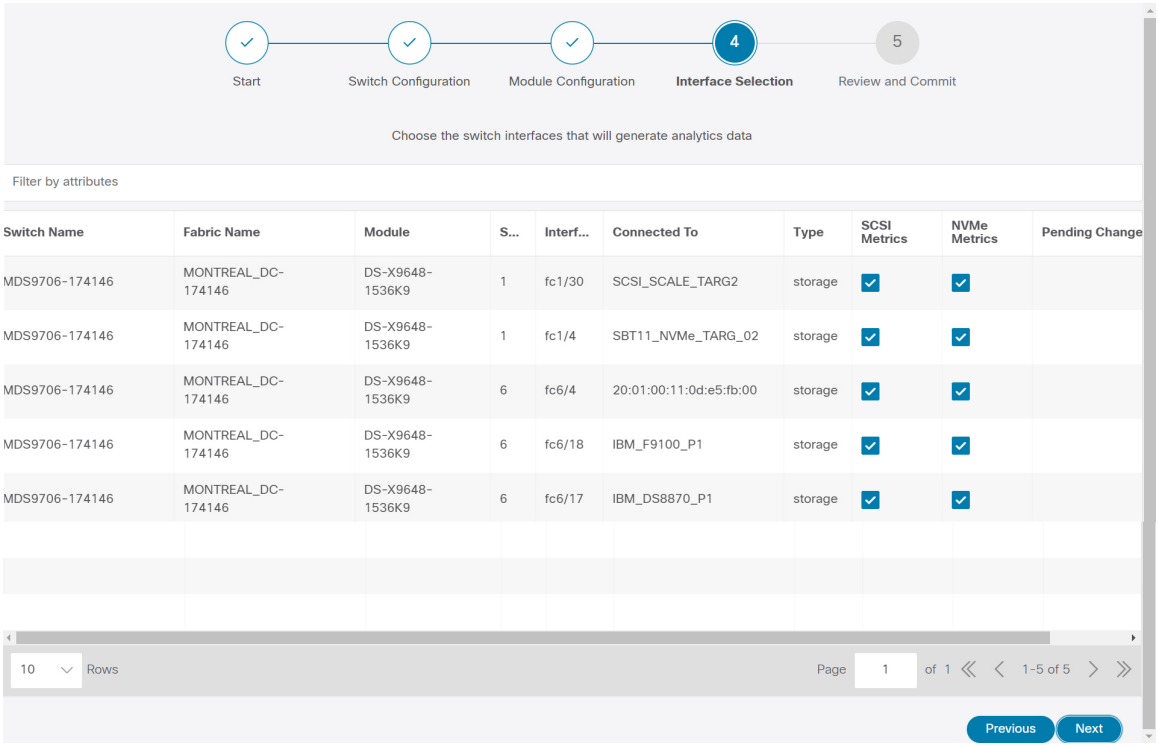
To change the values for **Sample Window (ports)** and **Rotation Interval (seconds)**, click the row and enter the desired values.

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

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

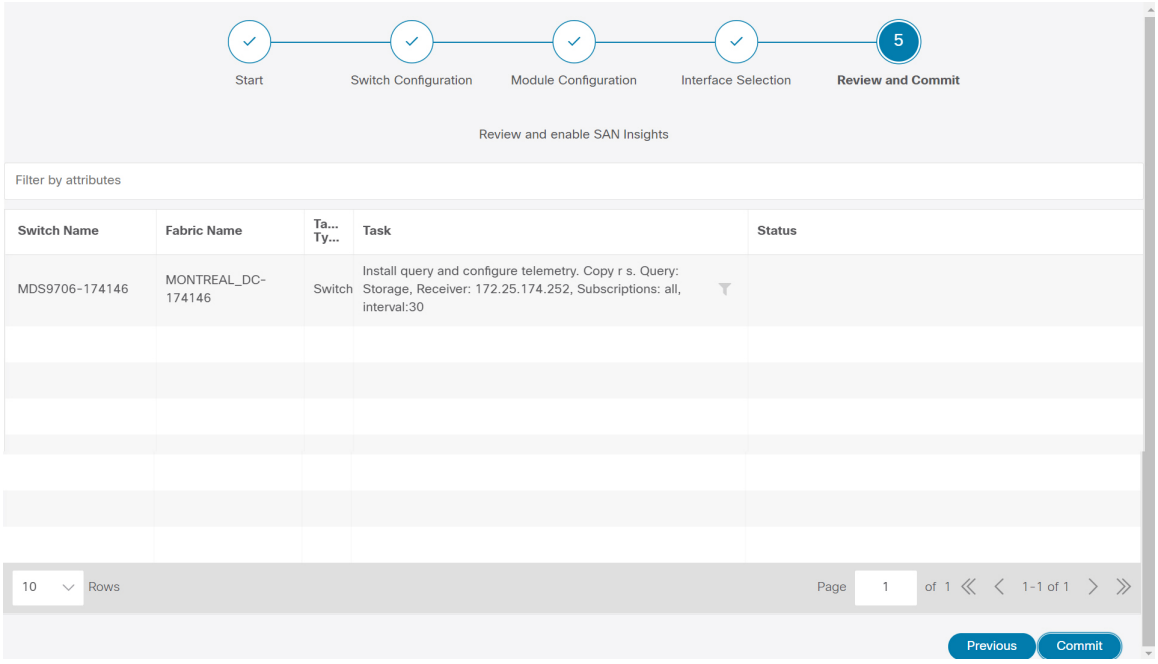
Step 9 Click **Next**.

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



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

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



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

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

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

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

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

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

Configuring Fabric Backup

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

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

SAN Controller doesn't back up the following fabrics:

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

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

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

You can enable scheduled backup for fabric configurations and intents.

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

Golden Backup

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

Procedure

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

The **Backup** tab appears.

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

The **Scheduled Archive** window appears.

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

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

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

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

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

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

A confirmation dialog box appears.

Step 6 Click **Yes**.

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

Fabric Overview

The **Actions** drop-down list at the Fabric level allows you to Configure backup, Refer Configuring Fabric Backup, on page 17 for more information.

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

Fabric Summary

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

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

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

Switches

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

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

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

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

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

Modules

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

Procedure

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

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

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

Step 2 You can view the following information.

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

Viewing Interface

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

Similarly you can view interface on fabric overview window.

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

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

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

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

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

Procedure

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

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

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

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

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

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

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

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

VSANs

You can configure and manage Virtual SANs (VSANs) from Cisco Nexus Dashboard Fabric Controller. From the menu, choose **Virtual Management > VSANS** to view VSAN information. You can view or configure VSAN for the discovered fabrics, with either **Manageable** or **Manage Continuously** status. For a selected fabric, a VSAN Scope tree is displayed in the left panel.

You can achieve higher security and greater stability in Fibre Channel fabrics by using virtual SANs (VSANs) on Cisco Data Center Switches and Cisco MDS 9000 Series switches. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs, you can create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FC IDs) to be used simultaneously in different VSANs.

Note Cisco Nexus Dashboard Fabric Controller does not discover, nor display any suspended VSAN.

The VSANs tab displays the following fields.

Field	Description
VSAN Name	Displays the VSAN name. The information that is associated with the selected VSAN scope appears in the right panel. If a VSAN is segmented, each individual segmented VSAN is a VSAN scope. For every selected VSAN scope, you can view information in tabs. • Switches Tab • ISLs Tab • Host Ports Tab • Storage Ports Tab • Attributes Tab • Domain ID Tab • VSAN Membership Tab
VSAN ID	Specifies the VSAN ID.
Segments	Specifies the Segments on this VSAN. Click on segments to open a slide-in pane to view summary information about each segment.
Status	Specifies if VSAN is **Up** or **Down**.

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

Action Item	Description
Create VSAN	Allows you to launch wizard to create VSAN. For more information, click Create VSAN Wizard, on page 24.
Delete VSAN	Select the VSAN and click Delete VSAN to delete the VSAN. For more information, click Delete VSAN, on page 26.

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

For description on all fields that appear on the tabs, refer Field and Descriptions for VSANs, on page 27.

This section includes the following topics:

Default VSAN Settings

The following table lists the default settings for all configured VSANs.

Parameters	Default
Default VSAN	VSAN 1.
State	Active State
Name	Concatenation of VSAN and a four-digit string representing the VSAN ID. For example, VSAN 3 is VSAN0003.
Load-balancing attribute	OX ID (src-dst-ox-id).

Create VSAN Wizard

VSAN Creation Wizard workflow includes:

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

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

Note Ensure that the VSAN is not already created.

To create and configure VSANs from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Before you begin

You cannot configure any application-specific parameters for a VSAN before creating the VSAN.

Ensure that the VSAN is not already created. Do not create the VSAN in suspended state.

Note The suspended VSANs are not managed.

Procedure

Step 1 In the VSAN ID and Name window, perform the following steps:

a) Ensure that the correct Fabric is against the Fabric field.
b) In the VSAN ID field, select VSAN ID from the drop-down list.

The range is 2–4094. Create the list of VSAN ID in at least one Switch in the Fabric. VSAN ID 4079 is for reserved VSAN.

c) In the VSAN Name field, enter a name for VSAN.

Note If the field is left blank, the Switch assigns a default name to the VSAN.

d) Click the FICON check box to enable FICON on the switch.

e) Click Next.

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

If the switch name is grayed out, it implies that the switch is already part of a VSAN. It may also imply that the switch doesn't have FICON feature enabled, if FICON is checked in the previous step.

Click **Next**.

Step 3 In the Configure VSAN Attributes screen, configure the VSAN attributes.

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

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

The following types are available:

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

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

b) In InterOp, select an interoperability value.

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

- Default: implies that the interoperability is disabled.
- InterOp-1: implies that the VSAN can interoperate with all the Fibre Channel vendor devices.
- InterOp-2: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-3: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-4: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.

Note InterOp isn't supported on FICON VSAN.

c) In Admin State, select the configurable state for this VSAN.

- Active: implies that the VSAN is configured and services for this VSAN is activated.
- Suspended: implies that the VSAN is configured, but the service for this VSAN is deactivated.

Choose this state to preconfigure all the VSAN parameters for the whole Fabric.

Note Nexus Dashboard Fabric Controller doesn't manage a suspended VSAN, and therefore it does not appear in the VSAN scope.

d) Check the InOrder delivery check box to allow in-order delivery.

When the value of fcInorderDelivery is changed, the value of this object is set to the new value of that object.

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

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

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

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

g) Click **Next**.

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

a) Check the Use Static Domain IDs check box to configure the domain ID for the switches in the VSAN.
b) The Available Domain IDs field shows all the available Domain IDs in the Fabric.

Click **Automatically apply available domain IDs** to assign the domain ID for every switch that is selected to be a part of the VSAN.

c) For every switch in the table, enter the domain ID from the list of available Domain IDs.
d) Click **Next**.

Step 5 In the Configure Port Membership screen, for every switch in the VSAN, configure the interfaces as the member of the new VSAN.

Note Modifying the Port VSAN may affect the I/O of the interface.

Click **Next**.

Step 6 In the Review screen, verify if you have configured the VSAN correctly.

Click **Previous** to navigate to the earlier screen and modify the configuration.

Click **Finish** to confirm and configure the VSAN. The VSAN creation result is displayed at the bottom of the window.

Note After the VSAN is created, it will take few minutes for the new VSAN to appear in the VSAN scope tree.

Note If the switch port is associated with Isolated VSAN then the previous VSAN information will be blank.

Delete VSAN

To delete a VSAN and its attributes from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

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

The **VSANS** window is displayed.

Step 2 From the Select a fabric drop-down list, select the Fabric to which the VSAN is associated.

The VSAN scope tree for the selected Fabric is displayed in the VSANS area.

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

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

Note You can't delete Segmented VSAN.

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

Click **Delete VSAN**.

A confirmation window appears.

Step 5 Click **Confirm** to confirm the deletion or click **Cancel** to close the dialog box without deleting the VSAN.

Note After the VSAN is deleted, it will take few minutes for the new VSAN to disappear from the VSAN scope tree.

Field and Descriptions for VSANs

The Field and Descriptions for all the tabs that are displayed on **Virtual Management > VSANS** are explained in the following tables.

Switches Tab

This tab displays Switches in the VSAN scope. Click the Switch name to view the summary information of the switch. The following table describes the fields that appear on the Switches tab.

Table 4: Field and Description on Switches Tab

Field	Description
Name	Specifies the name of the switch in the VSAN. Click the name to view the switch summary. Click **Show more Details** to view complete information.
Domain ID	Specifies an insistent domain ID.
VSAN WWN	Specifies the world wide name (WWN) of the VSAN.
Principal WWN	Specifies the world wide name (WWN) of the switch. **Note** For the principal switch, the value is *self*.
Model	Specifies the model name of the switch.

Field	Description
Release	Specifies the NX-OS version on the switch.
Up Time	Specifies the time from which the switch is up.

ISLs Tab

This tab displays information about the ISLs about the switches in the VSAN scope. The following table describes the fields that appear on the ISLs tab. If the VSAN is configured on both the switches across the ISL and if VSAN is not enabled on the ISL, Nexus Dashboard Fabric Controller considers VSAN as segmented. Therefore, add the VSAN to the trunked VSANs across the ISL to clear the warning message. Alternatively, you can ignore this warning message.

Table 5: Field and Description on ISL Tab

Field	Description
VSANs	All VSANs which this ISL runs traffic on.
From Switch	The source switch of the link.
From Interface	The port index of source E_port of the link.
To Switch	The switch on the other end of the link.
To Interface	The port index of destination E_port of the link.
Speed	The speed of this ISL.
Status	The operational status of the link.
Port Channel Members	The member of Port Channel if the ISL is a Port Channel.
Additional Info	Additional information for this ISL, such as, TE/TF/TNP ISL.

Host Ports Tab

This tab displays information about the host ports on the switches in the VSAN scope. The following table describes the fields that appear on the Host Ports tab.

Table 6: Field and Description on Host Ports Tab

Field	Description
Enclosure	The name of the enclosure.
Device Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
Fcid	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.
Vendor	Specifies the name of the vendor.

Field	Description
Serial Number	Specifies the serial number of the enclosure.
Model	Specifies the name of the model.
Firmware	The version of the firmware that is executed by this HBA.
Driver	The version of the driver that is executed by this HBA.
Additional Info	The information list corresponding to this HBA.

Storage Ports Tab

This tab displays information about the storage ports on the switches in the VSAN scope. The following table describes the fields that appear on the Storage Ports tab.

Table 7: Field and Description on Storage Ports Tab

Field	Description
Enclosure	The name of the enclosure.
Device Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
Fcid	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.

Attributes Tab

This tab displays the attributes of all the switches in the VSAN scope. The following table describes the fields that appear on the Attributes tab.

Table 8: Field and Description on Attributes Tab

Field	Description
Edit	Click **Edit** to modify the attributes of the VSAN and to push the same VSAN attributes to the selected switches. If the VSAN is FICON VSAN in any selected switch, the following fields won't appear on the UI, as they can't be modified for the FICON VSAN. • vsanLoadBalancing • InterOp • Inorder Delivery After modify the attributes, you can click **Save** to save changes or **Cancel** to discard.

Field	Description
Switch Name	Displays the name of the switch that is associated with the VSAN.
VSAN Name	Displays the name of the VSAN.
Admin	Specifies if the status of the Admin is either Active or Suspend. • **Active** implies that the VSAN is configured and services for the VSAN is activated. • **Down** implies that the VSAN is configured; however, the service for the VSAN is deactivated. You can use set this state to preconfigure all the VSAN parameters by using the CLI only. **Note** If you suspend a VSAN, it's removed from Cisco Nexus Dashboard Fabric Controller as well.
Oper	The operational state of the VSAN.
MTU	Displays the MTU for the switch.
Load Balancing	Specifies the load-balancing type that is used in the VSAN. The type of load balancing used on this VSAN. • srcId/DestId—use source and destination ID for path selection • srcdId/DestId/Oxld—use source, destination, and exchange IDs
InterOp	The interoperability mode of the local switch on this VSAN. • default • interop-1 • interop-2 • interop-3
Inorder Delivery	The Inorder Delivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it's not guaranteed.
FICON	True if the VSAN is FICON-enabled.

Domain ID Tab

This tab displays information about the VSAN domain and its parameters. The following table describes the fields that appear on the Domain ID tab.

Table 9: Field and Description on Domain ID Tab

Field	Description
Edit	Select a switch and click the Edit icon to modify the Domain ID information for the selected switch.

Field	Description
Switch Name	Specifies the switch name in the VSAN. **Note** NPV switches aren't listed in this column. However, the NPV switches exist in this VSAN fabric.
State	Specifies the state of the Switch.
Enable	Specifies if the Domain ID is enabled or disabled.
Running	Specifies the running domain.
Config	Specifies the configuration.
Config Type	Specifies the usage of the domain ID type—**preferred** or **static**.
Icons	
Total	The number next to Table specifies the entries under this tab.
Refresh Icon	Click the Refresh icon to refresh the entries.

VSAN Membership Tab

This tab displays information about the interfaces on the switches that form the VSAN. The following table describes the fields that appear on the VSAN Membership tab.

Table 10: Field and Description on VSAN Membership Tab

Field	Description
Edit	Select a switch and click the Edit icon to modify Port VSAN Membership for selected VSAN and selected switch. Port VSAN Membership is presented by different types including FC (physical), Port Channel, FCIP, iSCSI, VFC (slot/port), VFC (ID), VFC Channel, VFC FEX, and VFC Breakout, PortChooser is provided for each type to show all existing interfaces on a selected switch for the user to choose from. **Note** If you modify Post VSAN Membership for any operational trunking port or port channel members, a warning appears. Use the Device Manager to change Allowed VSAN List for Trunking Interface.
Switch Name	Name of the switch
Interfaces	FC Ports in VSAN

Device Aliases

A device aliases is a user-friendly name for a port WWN. Device alias name can be specified when configuring features such as zoning, QoS, and port security. The device alias application uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management and fabric-wide distribution.

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

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

This section contains the following:

Configuring Device Aliases

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

Before performing any Device Alias configuration, check the status on the CFS tab, to ensure that the status is **success**.

Note To perform Device Alias configuration from the SAN Controller Web UI, the fabric must be configured as Device Alias enhanced mode.

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

Procedure

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

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

The **Add device alias** windows appears.

All the provisioned port WWNs are populated in the table.

b) Enter a device alias name in the **Device Alias** field to indicate to create a device alias for the selected pWWN.
c) Click **Save** to exit the inline editor mode.
d) Click **Apply** to assign the device alias to the switches.

You can also create a device alias with a non-provisioned port WWN.

a) Click **+** icon of Pre-provision device aliases to create a new table row in inline editor mode.
b) In the **pWWN** field, enter the non-provisioned port WWN and device alias for the new alias.
c) Click **Save** to exit the inline editor mode.
d) Click **Apply** to assign the device alias and the associated pWWN to the switches.

Note If you close the Add device alias window before applying the device alias to the switches, the changes will be discarded and the device alias will not be created.

Step 2 To edit the device alias, choose the check box next to the switch column, and then click **Actions > Edit device aliases**.

Note You can select multiples switches to edit device aliases.

The **Edit device aliases** windows appears.

All the selected port WWNs are populated in the table.

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

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

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

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

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

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

A confirmation window appears.

Note Deleting the device alias may cause traffic interruption.

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

Step 4 For end devices with an attached service profile, the service profile name is populated to the **Device Alias** field. This allows the service profile name as a device alias name for those devices.

Device Alias creation is CFS auto committed after clicking **Apply**. Click **CFS** tab to check if CFS is properly performed after the device alias created. In case of failure, you must troubleshoot and fix the problem.

CFS

CFS information is listed for all the eligible switches in the fabric. Before performing any Device Alias configuration, check the status on the **CFS** tab to ensure that the status is "success". If the CFS is locked by another user, or if the previous operation failed, ensure that the CFS session is unlocked.

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

Fields	Descriptions
Switch	Specifies the name of switch.
Feature	Specifies the feature on the switch.

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

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

Procedure

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

The CFS configuration for this switch is committed.

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

The CFS configuration for this switch is aborted.

Step 3 To clear the lock on the CFS configuration, choose the **Switch** radio button, click **Clear lock**.

If the CFS is locked by another user, or if the previous operation failed, ensure that the CFS session is unlocked.

Event Analytics

Event Analytics includes the following topics:

- Alarms
- Events
- Accounting

Performing Backup actions

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

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

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

Actions	Descriptions
Backup now	• Choose **Backup now**. The **Create new backup** window appears. • Enter name in **Backup tag** field. If required choose check box **Mark backup as golden**. For more information on golden backup, refer to Golden Backup, on page 18. • Click **OK**.
Copy to bootflash	Choose **Copy to bootflash**. A confirmation window appears, click **OK**. For more information on bootflash, check Copy Bootflash.
Compare	Choose required switch names to compare configuration of switches, choose **Compare**. You can select only two switches at an instance. **Compare Config** window appears, displaying the difference between the two configuration files. The Source and Target configuration files content is displayed in two columns The differences in the configuration file are show in the table, with legends. • **Red**: Deleted configuration details. • **Green**: New added configuration. • **Blue**: Modified configuration details.
Export	Click **Export**. The files are downloaded in your local system. You can use the third-party file transfer tools to transfer these files to an external server.
Edit tag	Click **Edit tag** to change the backup tag name.
Mark as golden	To mark existing backup as golden backup, choose **Mark as golden**, a confirmation window appears, click **Confirm**.
Remove as golden	To remove existing backup from golden backup, choose **Remove as golden**, a confirmation window appears, click **Confirm**.
Delete	To delete existing backups, choose **Delete** a confirmation window appears, click **Confirm**. **Note** • If you have marked backup as golden backup. make sure that the golden backup is removed, else error appears you can't delete existing backup. • You can delete one backup at a time.

Name Server

Name Server stores name entries for all hosts in the FCNS database. The name server permits an Nx port to register attributes during a PLOGI (to the name server) to obtain attributes of other hosts. These attributes are deregistered when the Nx port logs out either explicitly or implicitly. In a multiswitch fabric configuration, the name server instances running on each switch shares information in a distributed database. One instance of the name server process runs on each switch.

Double click on the Fabric to view the Fabric Overview screen. Beginning with Release 12.1.2e, the **Name Server** tab displays name server entries for the selected Fabric. Note that this data is pulled from the Switches discovery, and therefore, the duplicate entries are removed.

The **Name Server** tab displays the following fields.

Field	Description
VSAN ID	Specifies the VSAN ID for the selected Fabric.
FC ID	Specifies the associated interface FCID.
Switch	Specifies the name of the switch. Click on the switch name to view the switch summary information. Double click on the switch name to launch the Switch Overview screen.
Port	Specifies the interface port.
Device Alias	Displays the alias retrieved from the switch. A device aliases is a user-friendly name for a port WWN. Device alias name can be specified when configuring features.
Type	The options are **N** and **NL**.
Port Name	Specifies the name of the port.
Node Name	Specifies the name of the node.
FC4Type:Feature	Specifies the FC Type that the port is using. This includes which protocol or state the port is in, that is, scsi-fcp, nvme, npv and whether it is an initiator or target. The following are the sample values: • scsi-fcp:target • scsi-fcp,nvme:init,init • scsi-fcp:both • nvme:target,disc

Configuration Monitor

From Release 12.1.2e, NDFC SAN Controller allows you to monitor the changes in configuration as compared to the baseline configuration.

After fabric discovery, configuration monitor saves the baseline configuration for all the switches in the fabric. The following parameters are monitored:

- NTP_TimeZone
- NTP_TimeServer
- AAA Config
- SYSLOG
- SNMP Host
- ACL
- Users

The monitoring job is executed once a day, everyday, to check for differences in baseline configuration and current configuration. Configuration Drift displays **Yes** when there is a difference between baseline and current configuration and an alarm is raised. You can view the Alarms raised on Cisco NDFC **Web UI > Event Analytics > Alarms > Alarms Raised**.

The Configuration Monitor tab displays the following fields.

Field	Description
Switch Name	Displays the switches discovered in the fabric. You can click on the switch name to view the summary information in a slide-in pane.
IP Address	Specifies the IP address of the switch.
Baseline Configuration Time	Specifies the time at which the baseline configuration was generated.
Baseline Configuration	Click **View** to view the baseline configuration for the specific switch. Click **Close** to return to the initial view.

Field	Description
Configuration Drift	Specifies if there is a difference in the current configuration, as compared to the baseline configuration. **N/A** specifies that NDFC failed to collect the switch baseline configuration due to SSH or reachability issue. **No** specifies that there is not configuration difference. **Yes** specifies that there is configuration drift as compared to the baseline configuration. Click **Yes** to view the configuration difference. On the **Configuration Differences** screen, **Baseline** and Current configurations are displayed side-by-side in two columns. The newly configuration Is highlighted in green color, and the deleted configuration lines are highlighted in red color.

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

For every event, an alarm is triggered and recorded on **Event Analytics > Alarms > Alarms Raised** page. If you **Disable Fabric Monitoring**, all the alarms are moved to **Alarms Cleared**.

Action Item	Description
Enable Fabric Monitoring	Allows you to enable fabric monitoring on all switches in the fabric.
Disable Fabric Monitoring	Allows you to disable monitoring the entire fabric. Note that if you disable fabric monitoring, the configuration drift data will not be captured and there will be no data to display on this tab. **Note** If you **Disable Fabric Monitoring** for the fabric, all the alarms are moved to **Alarms Cleared** tab.
Reset Baseline Configuration	Allows you to reset baseline configuration. Select the switch and choose **Reset Baseline Configuration** to purge all the configurations into Baseline Configuration.

Viewing of Port Usage

You can view the following information on Port Usage tab.

- **Port Speed** column displays the speed of the port.
- **Used Ports** column displays the total ports with the mentioned port speed.

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

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

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

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

Metrics

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

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

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

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

Fields	Descriptions
Switch Name	Specifies the name of switch.
Avg. Rx	Specifies the average Rx value.
Peak Rx	Specifies the peak Rx value.
Avg. Tx	Specifies the average Tx value.
Peak Tx	Specifies the peak Tx value.
Avg. Rx+Tx	Specifies the average of Rx and Tx value.
Avg. Errors	Specifies the average error value.
Peak Errors	Specifies the peak error value.
Avg. Discards	Specifies the average discard value.

Fields	Descriptions
Peak Discards	Specifies the peak discard value.
Last Update Time	Specifies the last updated time.
Show last day	Click **Show last day** to view data for selected day, week, month, and year.

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

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

Congestion Analysis

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

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

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

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

Procedure

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

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

Click **Congestion Analysis** tab.

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

Step 4 From the **Duration** drop-down list, select **Once** or **Daily** for the scheduled job. **Once** includes intervals such as 10 minutes, 30 minutes, 1 hour, and custom hours and runs the job immediately. **Daily** allows you to select a start time, and run the job for the selected interval. Use the radio button to select the desired interval to collect data.

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

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

Step 6 Click **Stop Analysis** to stop polling.

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

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

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

A detailed view of the fabric will appear when you click a fabric name and displays Congestion details for the fabric. See Congestion Visualization, on page 41 for more information.

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

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

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

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

Congestion Visualization

A topology of the selected fabric appears when you click a fabric name and displays Congestion details for the fabric. The topology window shows color-encoded nodes and links that correspond to various network elements. For each of the elements, you can hover over to fetch more information. The links and switches are color-coded. Enable performance collections and SNMP traps to view the Congestion information on the topology.

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

Table 11: Color Description

Color	Name	Description
Blue (light)	High Utilization	High utilization tx-datarate >= 80%
Green	Normal	No Congestion found
Red	Level 3	Credit loss recovery
Orange	Level 2	Drops
Yellow (dark)	Level 1.5	txwait >= 30%
Yellow (light)	Level 1	txwait < 30%

Color	Name	Description
Gray (light)	No Data	No Data

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

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

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

DIRL

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

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

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

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

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

The following are the different transition states of DIRL:

- **Normal**: The state in which a port is functioning normally and state before it enters DIRL Rate Reduction. After full recovery, the port returns to the Normal state.
- **DIRL Rate Reduction**: The state in which an event rising threshold triggers the DIRL rate reduction process.
- **DIRL Rate Reduction Maximum**: The state in which the DIRL rate reduction has reached its maximum value and more rising thresholds events are detected.
- **DIRL Status**: The state in which an event below the rising threshold and above the falling threshold is detected. This state will transition to the DIRL Recovery state when an event below the falling threshold is detected for the configured recovery-interval.
- **DIRL Rate Recovery**: The state in which the DIRL rate recovery happens on detecting an event below the falling threshold for the configured recovery-interval. This state will transition to the Normal state after the port recovers completely from DIRL.

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

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

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

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

DIRL Congestion Management Visualization

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

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

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

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

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

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

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

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

An entry in the table below shows that following fields:

Field	Description
Switch	Specifies the switch on which the analysis is collected. Click on the Switch to view a slide-in pane displaying the summary. Click on the launch icon to view **Switch Overview**.
Interface	Specifies the interface on which the analysis is collected. • Click the trend icon to view the chart for DIRL events on the interface. The graph provides information about Ingress, Egress, DIRL counter(s) values of the current DIRL with event timestamps for the selected DIRL interface. The graph also shows set of Falling/Rising threshold of each DIRL counter; the threshold is based on the active edge type Port Monitor policy at the time of the DIRL status collection. • Click on the interface name to view interface summary. Click VSAN value to view the related VSANs. • Click **DIRL Events** to view Rate Limit Events. The table displays the events of this interface from the CLI command output **show fpm ingress-rate-limit events**.
Current rate limit (%)	Specifies the % indicating the current rate limit.
Previous action	Specifies the previous action performed to control the rate limit.
Last updated time	Displays the time stamp at which the event occurred.

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

Rate Limit Events

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

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

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

Field	Description
Fabric	Specifies the Fabric to which the switch belongs.
Switch	Specifies the fabric for which the DIRL congestion is visua
Interface	Specifies the interface on which the events are visualized.
Last collection at	Specifies the date and time at which the DIRL status was co
Counter	Specifies if the counter is for **txwait** or **tx-datarate** or **tx-datarate-burst**.
Event	Specifies the event.
Counter Value %	Specifies the value of the counter.
Action	Specifies the action which triggered the event,
Operating port speed (Mbps)	Specifies the speed of the operating port.
Input rate (Mbps)	Specifies the input rate.
Output rate (Mbps)	Specifies the output rate.
Current rate limit (%)	Specifies the current rate limit.
Applied rate limit (%)	Specifies the applied rate limit.
Time	Specifies the time at event was triggered.