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 Fabrics .
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 3.
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 4.
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 4.
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 4.
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 16.

This chapter contains below sections:

Adding a Fabric

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Editing a Fabric

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

Procedure

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

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

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

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

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

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

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

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

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

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

Deleting a Fabric

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

Procedure

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

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

Rediscovering a Fabric

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

Procedure

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

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

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

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

The **Fabric** is rediscovered.

Purging a Fabric

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

Procedure

Step 1 Choose **SAN > Fabrics**.

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

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

The Fabric is purged.

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

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

The **Fabric** is purged.

Configuring Performance

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

Procedure

Step 1 Choose **SAN > Fabrics**.

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

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

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

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

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

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

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

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

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

What to do next

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

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

SAN Insights

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

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

For SAN Insights streaming stability and performance, see 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**.

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

Field Name	Description	Default Value
Max. Aggregation bucket size	Specifies maximum number of buckets to use for aggregation queries.	40,000
Data table download size	Specifies number of records for table download.	1000
ECT Data limit	Specifies the ECT Data limit.	14 **Note** The value of ECT data limit must be less than or equal to the value of SAN Telemetry retention policy - baseline / post processed.
SAN Telemetry deviation low threshold	Specifies the value that is the change point between normal and low.	1
SAN Telemetry deviation med threshold	Specifies the value that is the change point between low and medium.	15
SAN Telemetry deviation high threshold	Specifies the value that is the change point between medium and high.	30
SAN Telemetry deviation low threshold for NVMe	Specifies the value that is the change point between normal and low for NVMe.	1
SAN Telemetry deviation med threshold for NVMe	Specifies the value that is the change point between low and medium for NVMe.	2
SAN Telemetry deviation high threshold for NVMe	Specifies the value that is the change point between medium and high for NVMe.	5
SAN Telemetry training timeframe	Specifies the training time frame for flows ECT baseline.	7 days
SAN Telemetry training reset timeframe	Specifies the time duration to periodically restart the ECT baseline training after number of days.	14 days
SAN Telemetry retention policy - baseline / post processed	Specifies the retention policy - baseline / post processed.	14
SAN Telemetry retention policy - hourly rollups	Specifies the retention policy - hourly rollups	90

Field Name	Description	Default Value
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)	80K ITLs/ITNs
Cisco Physical Nexus Dashboard (1 Node)	120K ITLs/ITNs
Cisco Virtual Nexus Dashboard (3 Node)	150K ITLs/ITNs
Cisco Physical Nexus Dashboard (3 Node)	250K ITLs/ITNs

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

Configuring SAN Insights

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

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

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

Before you begin

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

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

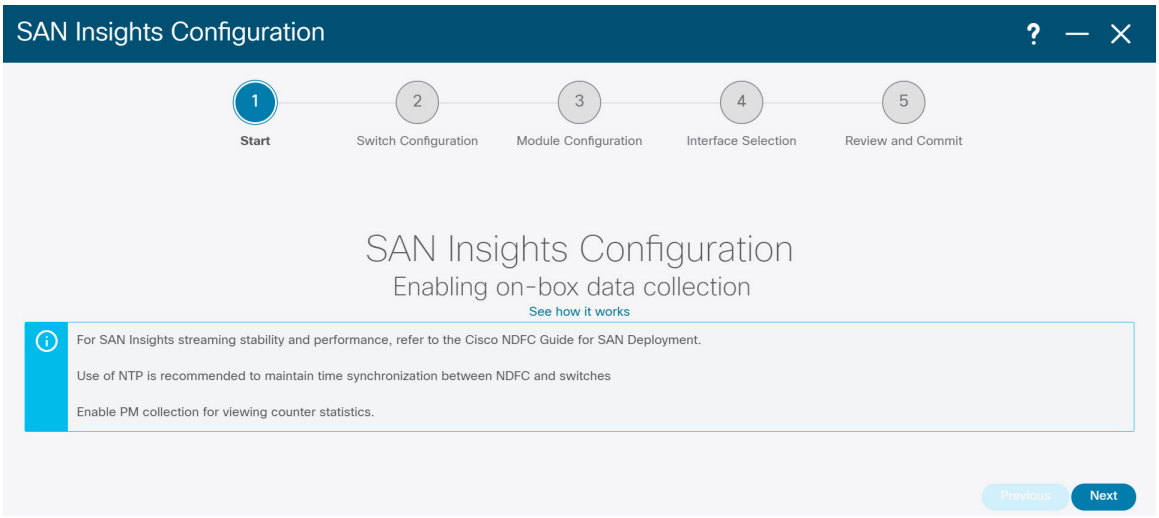
Note You must configure with sufficient system requirements and IP addresses. For more information on scale limits, refer to table Required System Memory for SAN deployment in Server Properties for SAN Insights.

Procedure

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

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

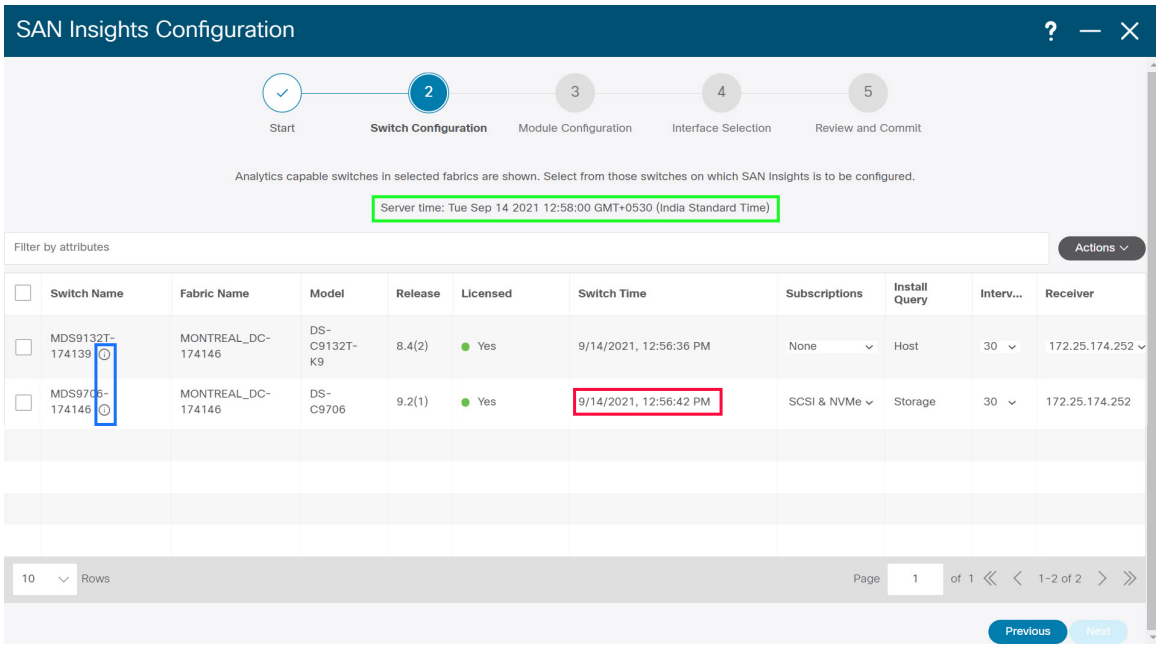
The **SAN Insights Configuration** wizard appears.



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 6 section for more information.

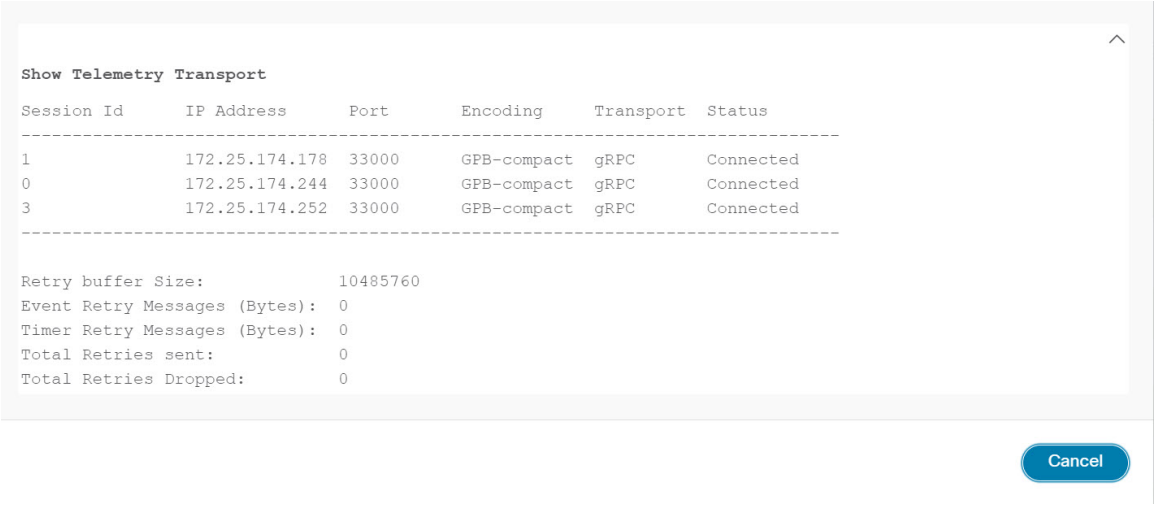
For NDFC to run on top of the virtual Nexus Dashboard (vND) instance, you must enable promiscuous mode on port groups that are associated with Nexus Dashboard interfaces where External Service IP addresses are specified. vND comprises of Nexus Dashboard management interface and data interface. By default,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

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

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

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

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



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

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

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

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

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

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

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

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

- **host**—lists all ports where hosts or initiators are connected on the switch.
- **storage**—lists all ports where storage or targets are connected on the switch.
- **ISL**—lists all ISL and port channel ISL ports on the switch.

- **None**—indicates that no query is installed.

The following queries are used:

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

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

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

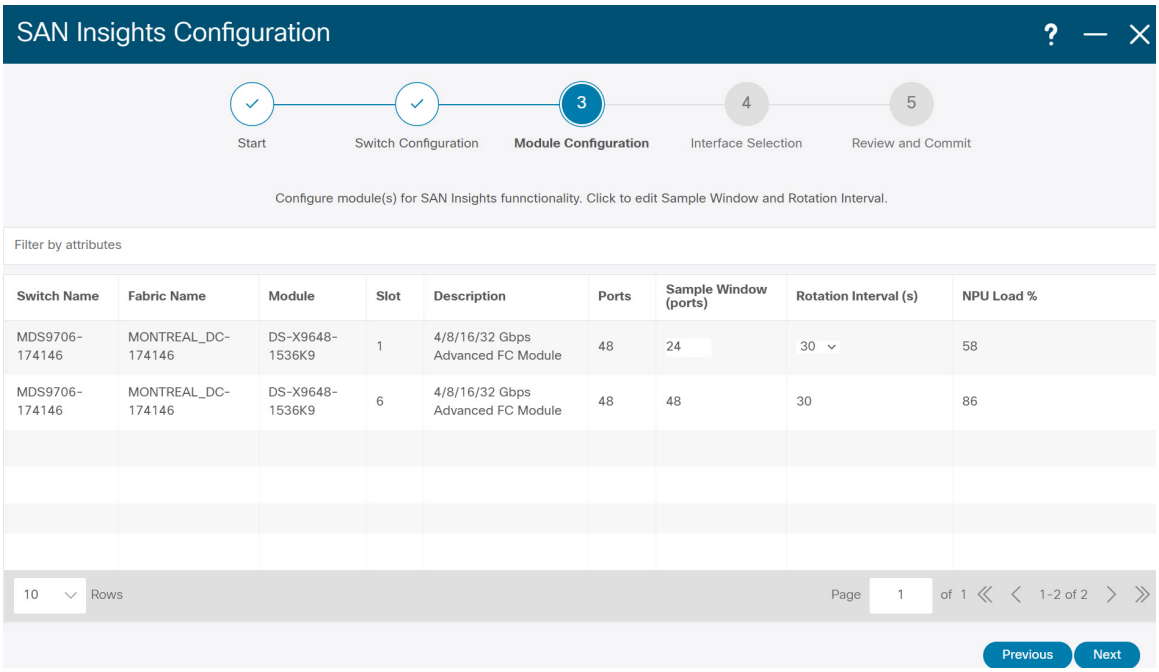
When the administrator selects the ISL\Host\Storage on the configure wizard, the respective ports are filtered and listed on the next step.

Step 7 Click **Next**.

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

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

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



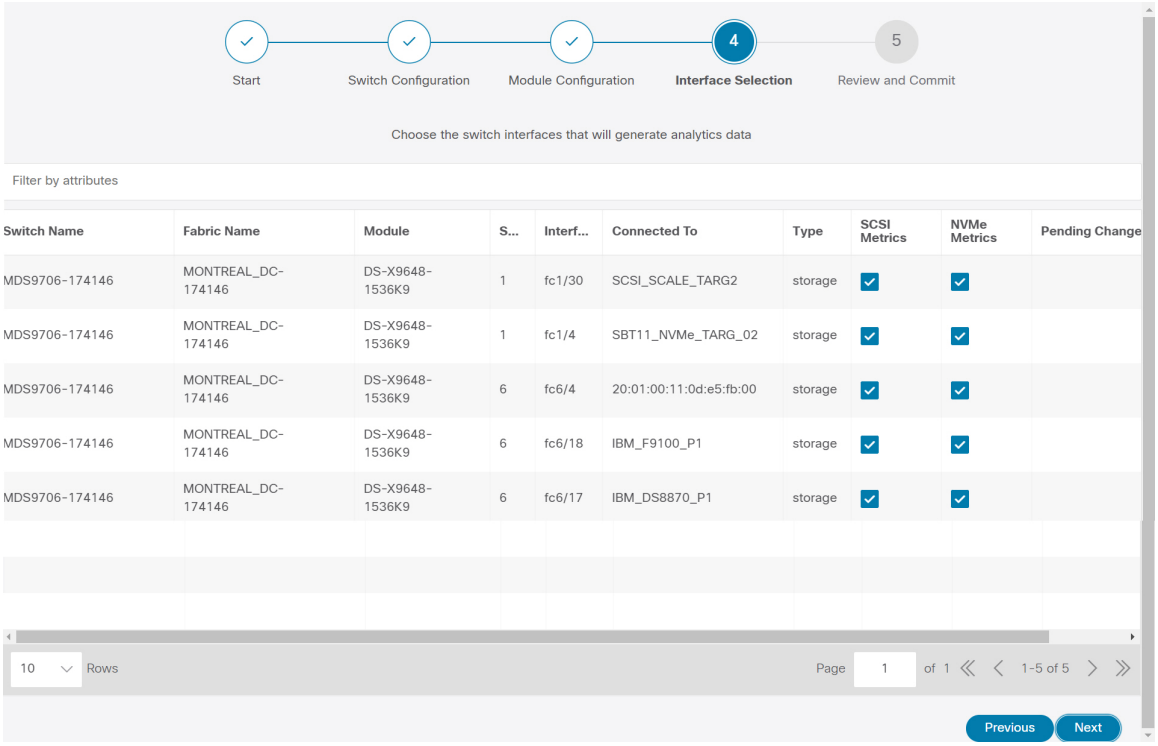
To change the values for **Sample Window (ports)** and **Rotation Interval (seconds)**, click the row and enter the desired values.

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

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

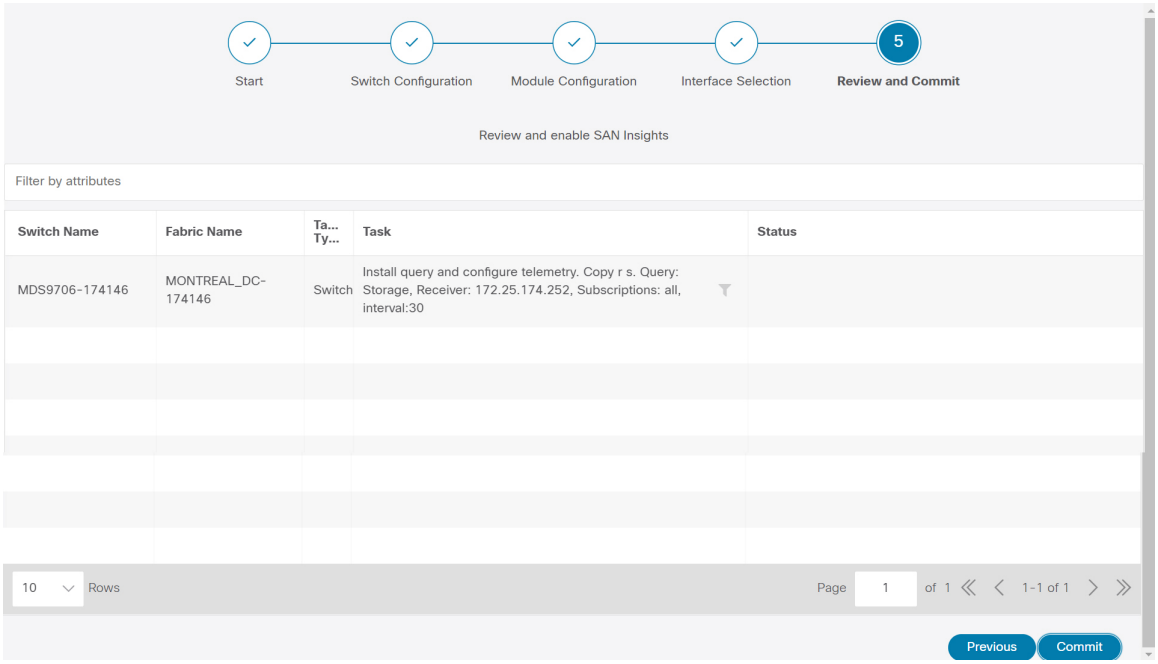
Step 9 Click **Next**.

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 16 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.
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.

Action Item	Description
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.
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**.

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 16. • 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.

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.

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

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

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