Understanding SAN Fabrics, Release 12.2.1

Table of Contents

New and Changed Information

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

Release Version	Feature	Description
There were no major changes from the previous release.		

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.

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 > Manage > 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 **Manage > Fabrics > Fabrics**.

Action Item	Description
Add Fabric	From the **Actions** drop-down list, select **Add Fabric**. For more instructions, see Adding a Fabric.
Edit Fabrics	Select a fabric to edit. From the **Actions** drop-down list, select **Edit Fabrics**. Make the necessary changes and click **Apply**. For more instructions, see Editing a Fabric.
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.
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.

Action Item	Description
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.
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 *Backup and Restore* in the *Cisco NDFC SAN Controller Configuration Guide*.

Adding a Fabric

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

1. Choose **Manage > Fabrics > SAN Fabrics**.
2. Choose **Actions > Add Fabrics**.
3. In the **Fabric Name** field, enter a unique name for the fabric.
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.

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.

      

      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.

        

        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.

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. 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.

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

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.

- 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 the Cisco Nexus Dashboard Deployment Guide.

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

1. Log into your **vSphere** Client.
2. Navigate to the ESXi host.
3. Right-click the host and choose **Settings**.

   A sub-menu appears.
4. Choose **Networking > Virtual Switches**.

   All the virtual switches appear as blocks.
5. Click **Edit Settings** of the VM Network.
6. Navigate to the **Security** tab.
7. Update the **Promiscuous mode** settings as follows:
   - Check the **Override** check box.
   - Choose **Accept** from the drop-down list.
8. Click **OK**.

Editing a Fabric

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

1. Choose **Manage > Fabrics > SAN Fabrics**.
2. Choose check box to edit required fabric name, choose the **Actions > Edit Fabrics**.
3. In the **Edit Fabrics** window, you can edit only one fabric at a time.
4. Enter a new fabric **Fabric Name**.
5. (Optional) Check the **SNMPV3** check box. If you check SNMPV3, the **Community** field changes to **Username** and **Password**.
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.
7. Change the status to **Managed**, **Unmanaged**, or **Managed Continuously**.
8. (Optional) Check the **Use UCS Credentials** check box if you want to modify UCS credentials.
9. Enter the **Username** and **Password**.
10. Click **Apply** to save the changes.

Deleting a Fabric

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

1. Choose **Manage > Fabrics > SAN Fabrics**.
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:

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

1. Choose **Manage > Fabrics**.
2. Choose the check box next to the fabric you want to purge.
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.

1. Choose **Manage > Fabrics**.
2. Choose the check box next to the fabric you want to configure performance collections.
3. Choose **Action > Configure Performance**.

   The **Performance Data Collection Settings** window appears.
4. Choose check box **Performance Collection**, to enable other check boxes.
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 **Admin > System Settings > Server Settings > PM**.
   b. On **PM** tab, choose check box for **Enable SAN Sensor Discovery** and **Collect Temperature for SAN Switches**.
6. Click **Apply** to save the configuration.
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 **Admin > System 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.

Copyright