Creating and Editing SAN Fabrics, Release 4.2.1

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
Nexus Dashboard 4.2.1	There were no major changes from the previous release.	

View SAN fabrics

To view the SAN fabrics in your Nexus Dashboard:

1. Navigate to **Fabrics**:

   Manage > Fabrics

2. Review the information provided in Fabrics on the SAN fabrics that have been configured in your Nexus Dashboard.

   The following table describes the fields that appear in **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 in **Fabrics**.

Action Item	Description
Add Fabric	From the **Actions** drop-down list, select **Add Fabric**. For more instructions, see Add 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 Edit 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 Delete a fabric.

Action Item	Description
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 Rediscover a fabric.
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 Purge 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 Working with Reports for SAN Fabrics.
Configure SAN Insights	Allows you configure SAN Insights on the selected fabric. For more instructions, see SAN Insights.
Configure Backup	Allows you to configure and schedule backup for the fabric data. For more instructions, see Backing Up and Restoring Your SAN Fabric.

View SAN fabric summary information

To view SAN fabric summary information:

1. Navigate to **Fabrics**:

   Manage > Fabrics

2. Click on a SAN fabric to open a drawer with information on that SAN fabric.

   The following sections display the summary of the SAN fabric:

   - **Health** - Shows the health of the SAN fabric.
   - **Alarms** - Displays the alarms based on the categories.
   - **Switch Health**: Displays the number of switches in the SAN fabric and the switch health information.
   - **Switch Interfaces**: Displays the number of switch interfaces in the SAN fabric, along with this information:
     - **Oper. Status**:
     - **Admin Status**: Specifies the administration status of an interface, depending on the action taken on an interface. Possible states:
       - **Up**: Reflects the state of a switch interface where a No Shutdown action was performed (**Actions > No Shutdown**).
       - **Down**: Reflects the state of a switch interface where a Shutdown action was performed (**Actions > Shutdown**)

Click the **Launch** icon to the right top corner to view the **Fabric Overview** for a SAN fabric. See Understanding Fabric Overview for SAN Fabrics for more information.

Add a fabric

To add a SAN fabric:

1. Navigate to **Fabrics**:

   Manage > 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**.

   Nexus Dashboard 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.

      This is typically the IP address associated with its management interface (mgmt0).

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

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

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

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

   f. To discover UCS fabric interconnects (FIs) using UCS credentials, check the **Use UCS Credentials** check box.

      - Enter the appropriate **UCS CLI Credentials** in the **UCS User Name** and **UCS 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 Simple Network Management Protocol version 3 (SNMPv3) for UCS, check the **Use SNMPv3 for UCS** check box.
      - From the **UCS Authentication / Privacy** drop-down list, choose the appropriate

authentication with privacy for UCS fabric interconnect discovery.

> ℹ Cisco UCS Manager Release 3.2(3) and later releases do not support SNMPv3 users without Advanced Encryption Standard (AES) encryption, and it does not support Message-Digest Algorithm 5 (MD5) authentication if SNMPv3 is in Federal Information Processing Standards (FIPS) mode.

- In the **UCS SNMP User Name** and **UCS SNMP Password** fields, enter the appropriate details to access the UCS FIs if SNMPv3 is used.

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

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

g. To monitor metrics for the attached UCS FIs in IMM, check the **Monitor Intersight** checkbox. The Intersight credentials are necessary for obtaining inventory and metrics information. For more information, see Working with Cisco Intersight.

- Enter the Intersight region in the **Intersight Region** field.
- Generate the API key ID in Intersight > **API Keys** and add it to **API Key ID** in Nexus Dashboard. Save the secret key for uploading to Nexus Dashboard.
- Enter the **Account ID** in Nexus Dashboard that you obtained from Intersight > **Account Details**.
- Browse to and upload the saved secret key from Intersight to **Intersight Secret Key File** in Nexus Dashboard.
- Once configured and saved, you can view your Intersight integration on the Nexus Dashboard **Topology** page. You can view the associated blade servers, vNICs, and vHBAs.

6. If you chose **Non-Cisco** in the **Fabric Seed Switch Type**, follow these steps:

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 the appropriate authentication for switch discovery.

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

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

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

- Enter the appropriate **UCS CLI Credentials** in the **UCS Username** and **UCS 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 SNMPv3 for UCS, check the **Use SNMPv3 for UCS** check box.

  From the **UCS Authentication / Privacy** drop-down list, choose the appropriate authentication with privacy for discovery of UCS fabric interconnects.

  Enter the UCS SNMP username and password in the appropriate fields.

- If **Use SNMPv3 for UCS** is unchecked, enter the 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 is scheduled on Nexus Dashboard:
>
> - 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

You can run Nexus Dashboard 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.

Enabling promiscuous mode raises the risk of security issues in Nexus Dashboard, so we recommend that you set the default setting for promiscuous mode.

> - 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.

> The 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**.

Edit a fabric

To edit a SAN fabric:

1. Navigate to **Fabrics**:

   Manage > Fabrics

2. Choose a SAN fabric to edit.
3. Click **Actions > Edit Fabrics**.
4. In the **Edit Fabrics** window, you can edit only one fabric at a time.
5. Check the **Use SNMPv3 / SSH** check box, if applicable.

   - If you uncheck the **Use SNMPv3 / SSH** check box, the **Community String** field appears. Enter the appropriate community string in the **Community String** field.
   - If you check the **Use SNMPv3/SSH** check box, these fields appear:
     - **Authentication/Privacy**: From the **Authentication/Privacy** drop-down list, choose one of these options for switch discovery:
       - MD5
       - SHA
       - SHA2_224
       - SHA2_256
       - SHA2_384
       - SHA2_512
       - MD5_DES
       - MD5_AES
       - SHA_DES
       - SHA_AES
       - SHA2_224_AES
       - SHA2_256_AES
       - SHA2_384_AES
       - SHA2_512_AES

     ℹ The options with _DES or _AES are related to privacy. You need to select one of these options for enforcePriv or globalEnforcePriv. _AES only supports AES-128 encryption.

   - **Username** and **Password**: Enter the appropriate details to access the seed switch.

     ℹ The **Password** should be the same for both authentication and privacy.

6. Change the status to **Managed**, **Unmanaged**, or **Managed Continuously**, if necessary.
7. Check the **Use UCS Credentials** check box if you want to modify UCS credentials.

8. Check the **Monitor Intersight** option, if necessary.
9. Click **Apply** to save the changes.

Delete a fabric

When the orchestration feature is enabled on a fabric, the **Delete Fabric** option remains disabled. To delete a fabric, you must first disable its orchestration feature.

To delete a SAN fabric:

1. Navigate to **Fabrics**:

   Manage > Fabrics

2. Choose the SAN fabric that you want to delete.
3. Click **Actions > Delete Fabrics** to remove the fabric from the data source and to discontinue data collection for that fabric.

Rediscover a fabric

To rediscover a SAN fabric:

1. Navigate to **Fabrics**:

   Manage > Fabrics

2. Choose a SAN fabric to rediscover.
3. Click **Actions > Rediscover Fabrics**.
4. Click **Yes** in the dialog box.

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

   The SAN fabric is rediscovered.

Purge a fabric

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

1. Navigate to **Fabrics**:

   Manage > Fabrics

2. Choose a SAN fabric to purge.
3. Choose **Action > Purge Fabrics**.

   The SAN fabric is purged.

You can also purge a fabric from **Topology**:

1. Navigate to **Topology**:

   Home > Topology

2. Right-click on the SAN fabric that you want to purge, then click **Purge Down Fabric**.

   The SAN fabric is purged.

Copyright

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883