Add Switches for SAN Operational Mode, Release 12.1.3

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 nor of the new features up to this release.

Release Version	Feature	Description
NDFC release 12.1.3	Reorganized content	Content within this document was originally provided in the *Cisco NDFC-Fabric Controller Configuration Guide* or the *Cisco NDFC-SAN Controller Configuration Guide*. Beginning with release 12.1.3, this content is now provided solely in this document and is no longer provided in those documents.
NDFC release 12.1.3	Enhancements to the Execute CLI feature.	The Execute CLI feature has been enhanced to include a Session Timeout field, and to provide additional options when providing the CLI commands to be executed on the switches and for viewing the Execute CLI output.

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.
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.
Migrate Brocade Parameters	

Device Manager

The Device Manager provides a graphical representation of the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

In addition to the Device Manager service available on the switch dashboard, beginning with Cisco Nexus Dashboard Fabric Controller Release 12.1.3, you can download and install standalone Device Manager application on your local system.

Download Device Manager

Before you begin

The client computer is installed with Windows or Linux operating system.

This section describes the steps to download Device manager to your local system.

1. In Cisco Nexus Dashboard Fabric Controller, choose **SAN > Switches**

   The switch dashboard displays.

2. From the **Actions** drop-down list, choose **Device Manager**.

   This will download the device manager client file in *tar.gz* format to your system. You can then extract the archive file to view its contents.

3. Depending on the operating system installed, run the script or the batch file to install Device Manager application on your system.

   On a Linux system, the script file (*.sh) file resides in the */bin directory*.

   On a Windows system, the script file (*.bat) file resides in the */bin directory*.

   The Device Manager login dialog box appears.

4. Log on to the Device Manager application.

   The system downloads Device Manager as a standalone application on your local system.

   See Device Manager to view descriptions and instructions for using the Cisco MDS 9000 Device Manager.

Tech Support

From the **Actions** drop-down list, select **Tech Support** to initiate log collection. A window appears.

- Enter time in **Session timeout** field in minutes, by default time is 20 minutes.
- Enter the command in **Command** text field and click **Run**.
- A confirmation window appears stating 'Data submitted successfully, tech support starting', click **Confirm** and status changes to **Completed**.
- You can download the report, click **Download Tech Support**.

Execute CLI

Cisco NDFC SAN Controller allows you to execute CLI commands on switches. You can collect the output from the CLI commands in a zip file for each switch.

To execute CLI commands on switches, do the following:

1. On the Cisco NDFC UI, choose **SAN > Switches**.
2. Select the switches on which you want to execute the CLI commands.

   You can select more than one switch to run the set of CLI commands simultaneously.

3. From the **Actions** drop-down list, choose **Execute CLI** .

   The **Execute Switch CLI** screen is displayed.

4. On the **Configure** tab, click on the hyperlink under **Selected Switches** to view the selected switches on which the CLIs will be executed.
5. In the **Session Timeout** area, enter the length of time before the session timeout.

   Valid options are 2-10 minutes. The default entry is 5 minutes.

6. Determine how you will provide the CLI commands to be executed on the switches.

   - Enter the CLI commands to be executed on the switches in the **CLI Commands** text box, or
   - Click on the **Read Commands File** button and upload a file with a .txt extension that has a list of CLI commands to be executed.

   Ensure that you enter one command per line in the **CLI Commands** text box or in the .txt file.

7. Click **Execute**.

   When the command execution is completed on all the switches, a popup window appears, showing the **Execute CLI Output**.

8. Click **Close**.

   You are returned to the **Execute Switch CLI** window, where the table displays the switch, the associated fabric and the CLI execution status.

   - Click on **Show Output** to bring up the popup window again, showing the **Execute CLI Output**.

     When an output is larger than a few MB, the **show output** is truncated. In that case, you must download the file to see the complete output. **Show output** is meant for light output to allow for faster debugging with little to display, and is not meant for offline debugging done with a downloaded file.

   - Click on **Download output** to download the command output as a zip file.
   - Click **Done** when you are finished with the procedures in this window.

If the switch is not reachable via CLI, then the output in the zip file will indicate an error.

Enhanced Role-based Access Control

Starting from SAN Controller Release 12.0.1(a), all RBAC is in Nexus Dashboard. User-roles and access are defined from Nexus Dashboard for fabrics on NDFC.

Nexus Dashboard admin role is considered as Network-admin role in NDFC.

DCNM had five roles to perform various access and operations. If a user is access a fabric with network stage role has access to all other fabrics as a network stage role. Therefore, a username is restricted with their role in DCNM.

Cisco NDFC Release 12.0.1(a) has same five roles but you can do granular RBAC with integration of Nexus Dashboard. If a user accesses a fabric as a network stage role, the same user can access different fabric with other user role such as admin or operator role. Therefore, a user can have different access on the different fabrics in NDFC.

NDFC RBAC supports following roles:

- NDFC Access Admin
- NDFC Device Upgrade Admin
- NDFC Network Admin
- NDFC Network Operator
- NDFC Network Stager

The following table describes the user roles and their privileges in NDFC.

Roles	Privileges
NDFC Access Admin	Read/Write
NDFC Device Upgrade Admin	Read/Write
NDFC Network Admin	Read/Write
NDFC Network Operator	Read
NDFC Network Stager	Read/Write

The following roles are supported on DCNM for backward compatibility:

- SAN admin (mapped to network-admin)
- Global-admin (mapped to network-admin)
- SAN network-admin (mapped to network-admin)
- Server-admin (mapped to network-admin)

In any window, the actions that are restricted by the user role that is logged in are grayed out.

NDFC Network Admin

A user with the **NDFC Network Admin** role can perform all the operations in SAN Controller.

From Cisco Nexus Dashboard Fabric Controller Release 12.1.1e, a user with this role can perform all operations for MSD fabrics in Networks and VRFs.

You can freeze a particular fabric or all fabrics in SAN Controller if you are a user with the **NDFC Network Admin** role.

Make sure that the switch user role for discovery or add switches or LAN credentials for NDFC must have the network-admin role.

NDFC Device Upgrade Admin

A user with the **NDFC Device Upgrade Admin** role can perform operations only in **Image Management** window.

See the [Image Management] section for more information.

NDFC Access Admin

A user with the **NDFC Access Admin** role can perform operations only in the **Interface Manager** window for all fabrics.

An NDFC access admin can perform the following actions:

- Add, edit, delete and deploy layer 2 port channels, and vPC.
- Edit host vPC, and ethernet interfaces.
- Save, preview, and deploy from management interfaces.
- Edit interfaces for LAN classic, and IPFM fabrics.

  Apart from nve, management, tunnel, subinterface, SVI, interface grouping, and loopback interfaces

However, a user with the SAN Controller access admin role can't perform the following actions:

- Cannot edit layer 3 port channels, ST FEX, AA FEX, loopback interfaces, nve interfaces, and subinterfaces.
- Cannot edit member interfaces and port channels of Layer 3, ST FEX, AA FEX.
- Cannot edit interfaces with policy associated from underlay and link for easy fabrics.
- Cannot edit peer link port channel.
- Cannot edit management interface.
- Cannot edit tunnel.

The icons and buttons are grayed out for this role when the fabric or SAN Controller is in deployment-freeze mode.

NDFC Network Stager

A user with the **NDFC Network Stager** role can make configuration changes on SAN Controller. A

user with the **NDFC Network Admin** role can deploy these changes later. A network stager can perform the following actions:

- Edit interface configurations
- View or edit policies
- Create interfaces
- Change fabric settings
- Edit or create templates

However, a network stager cannot perform the following actions:

- Cannot make any configuration deployments to switches.
- Cannot perform deployment-related actions from the SAN Controller Web UI or the REST APIs.
- Cannot access the administration options like licensing, creating more users, and so on.
- Cannot move switches in and out of maintenance mode.
- Cannot move fabrics in and out of deployment-freeze mode.
- Cannot install patches.
- Cannot upgrade switches.
- Cannot create or delete fabrics.
- Cannot import or delete switches.

NDFC Network Operator

A network operator can view fabric builder, fabric settings, preview configurations, policies, and templates. However, a network operator cannot perform the following actions:

- Cannot change expected configurations of any switch within any fabric.
- Cannot deploy any configurations to switches.
- Cannot access the administration options like licensing, creating more users, and so on.

The difference between a network operator and a network stager is that, as a network stager you can only define intent for existing fabrics, but cannot deploy those configurations.

Only a network admin can deploy the changes and edits that are staged by a user with the network stager role.

Choosing Default Authentication Domain

By default login screen on Nexus Dashboard chooses the local domain for authentication. You can change domain at login time by choosing available domains from drop-down list.

Nexus Dashboard supports local and remote authentication. The remote authentication providers for Nexus Dashboard include RADIUS, and TACACS. For more information on authentication support, refer the Cisco Nexus Dashboard User Guide, Release 2.1.x.

The following table describes RBAC comparison between DCNM and NDFC access:

DCNM 11.5(x)	NDFC 12.0.x and 12.1.x
• User has a single role. • All APIs and resources are accessed with this single role.	• User can have a different role in different Nexus Dashboard for security domains. • Security domain contains single Nexus Dashboard, and each Nexus Dashboard contains single NDFC Fabric.
A single role is associated with the user by disabling or restricting the access to options in DCNM.	A single role displays only privileged resources on the selected page and restricted access are grayed out based on security domain associated with selected resource on further options on NDFC.
DCNM AV Pair format with shells, roles, and optional access constraints.	Nexus Dashboard AV Pair format with shells, domains.
Supported roles based on deployment type LAN, SAN, or PMN.	Supported roles such as network-admin, network-operator, device-upg-admin, network-stager, access-admin are in NDFC.Support for legacy roles for backward compatibility. Nexus Dashboard admin role as network-admin of DCNM.

The following table describes DCNM 11.5(x) AV Pair format:

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell Cisco-AV-Pair Value
Network-Operator	shell:roles = "network-operator" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1group2 group5"	cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"

The following table describes NDFC 12.x AV Pair format:

User Role	AVPair Value
NDFC Access Admin	Access-admin
NDFC Device Upgrade Admin	Device-upg-admin
NDFC Network Admin	Network-admin
NDFC Network Operator	Network-operator
NDFC Network Stager	Network-stager

The AV pair string format differs when configuring a read/write role, read-only role, or a combination of read/write and read-only roles for a specific user. A typical string includes the domain, followed by

the read-write roles separated from the read-only roles using the slash (/) character; individual roles are separated by the pipe (|) character:

shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>

Nexus Dashboard Security Domains

Access control information about a user login contains authentication data like user ID, password, and so on. Based on the authorization data, you can access resources accordingly. Admins in Cisco Nexus Dashboard can create security domains and group various resource types, resource instance, and map them into a security domain. The admins define an AV-pair for each user, which defines the access privileges for users to different resources in Cisco Nexus Dashboard. When you create a fabric, a site is created in Nexus Dashboard with the same fabric name. You can create and view these sites from **Nexus Dashboard > Sites**.

The SAN controller REST APIs use this information to perform any action by checking the authorization.

When accessing REST APIs, you can verify passed payload in JSON format. Ensure that the payload is an appropriate JSON format. When you upgrade from SAN Controller Release 11.x, each fabric is mapped to an autogenerated site of the same name. All these sites are mapped into the **all** security domain in Nexus Dashboard.

All resources are placed in **all** domain before they are assigned or mapped to other domains. The all security domain does not include all the available security domains in Nexus Dashboard.

AV-Pairs

A group of security domains along with read and write roles for each domain are specified using AV-pairs. Administrators define AV-pair for each user. The AV-pair defines the access privileges to users across various resources in Nexus Dashboard.

The AV-pair format is as follows:

" avpair" : " shell:domains=security-domain/write-role-1|write-role-2,security-domain/write-role-1|write-role2/read-role-1|read-role-2"

Example: " avpair" : " shell:domains=all/network-admin/app-user|network-operator"

all/admin/ makes the user super-user and it's best to avoid examples with all/admin/. The write role is inclusive of read role as well. Hence, all/network-admin/ and all/network-admin/network-admin are the same.

From SAN Controller Release 12.0.1a supports the existing AV-pair format that you created in SAN Controller Release 11.x. However, if you are creating a new AV-pair, use the format that is mentioned above. Ensure that the shell: domains must not have any spaces.

Specifying Cisco NX-OS User Roles and SNMPv3 Parameters on AAA Servers

You can use the VSA cisco-AV-pair on AAA servers to specify user role mapping for the Cisco NX-OS device using this format:

```
shell:roles=" roleA roleB ..."
```

If you do not specify the role option in the cisco-AV-pair attribute, the default user role is network-operator.

You can also specify your SNMPv3 authentication and Privacy protocol attributes as follows:

```
shell:roles=" roleA roleB..."  snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The Privacy protocol options are AES-128 and DES. If you do not specify these options in the cisco-AV-pair attribute, MD5 and DES are the default authentication protocols.

Creating a Security Domain

To create a security domain from Cisco Nexus Dashboard, perform the following steps:

1. Log into Cisco Nexus Dashboard.
2. Choose **Administrative > Security**.
3. Navigate to **Security Domains** tab.
4. Click **Create Security Domain**.
5. Enter the required details and click **Create**.

Creating a User

To create a user from Cisco Nexus Dashboard, perform the following steps:

1. Log into Cisco Nexus Dashboard.
2. Choose **Administrative > Users**.
3. Click **Create Local User**.
4. Enter the required details and click **Add Security Domain**.
5. Choose a domain from the drop-down list.
6. Assign a SAN Controller service read or write role by checking the appropriate check box.
7. Click **Save**.

Copyright