



About Fabric Overview for SAN
Operational Mode Setups, Release
12.1.3

Table of Contents

New and Changed Information	1
Fabric Overview	2
Fabric Summary	3
Switches	4
Viewing Module Inventory	5
Viewing Interfaces	6
VSANs	8
Default VSAN Settings	9
Create VSAN Wizard	9
Delete VSAN	12
Field and Descriptions for VSANs	12
Switches Tab	13
ISL Tab	13
Host Ports Tab	14
Storage Ports Tab	14
Attributes Tab	14
Domain ID Tab	16
VSAN Membership Tab	16
Device Aliases	17
Configuring Device Aliases	17
CFS	18
Event Analytics	20
Performing Backup actions	21
Name Server	23
Configuration Monitor	24
Viewing of Port Usage	26
Metrics	27
Congestion Analysis	29
Congestion Visualization	29
DIRL	31
DIRL Congestion Management Visualization	32
Rate Limit Events	33
Copyright	35

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
NDFC release 12.1.3	Reorganized content	Content within this document was originally provided in the <i>Cisco NDFC-Fabric Controller Configuration Guide</i> or the <i>Cisco NDFC-SAN Controller Configuration Guide</i> . Beginning with release 12.1.3, this content is now provided solely in this document and is no longer provided in those documents.

Fabric Overview

The **Actions** drop-down list at the Fabric level allows you to configure backup, Refer to the section "Configuring Fabric Backup" in [Backing Up and Restoring SAN Operational Mode Setups](#) 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 the section "Tech Support" in Add Switches for SAN Operational Mode .
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 the section "Execute CLI" in Add Switches for SAN Operational Mode .

Viewing Module Inventory

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

1. In Cisco Nexus Dashboard Fabric Controller, choose **SAN > Fabric**.
2. Double-click on the required fabric to open the **Fabric Overview** page and click on the **Modules** tab.

The **Modules** tab displays 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**.

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

Viewing Interfaces

1. In Cisco Nexus Dashboard Fabric Controller, choose **SAN > Fabric**.
2. Double-click on the required fabric to open the **Fabric Overview** page and click on the **Interfaces** tab. The **Interfaces** tab displays a list of all the interfaces in the selected fabric.

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

Field	Description
Switch Name	Specifies the name of the switch the interface belongs to.
Interface Name	Specifies the name of the interface. The Show 24hr chart icon to the left of the interface name opens the Interface Details and Performance Chart dialog box for the selected interface. It displays details about the interface and a performance chart that depicts the traffic details through the interface. This chart is available only for interfaces that are connected to another interface.
Admin. Status	Specifies the administration status of the interface.
Oper. Status	Specifies the operational status of the interface.
Reason	Specifies the reason for failure.
Admin. Speed	Specifies the configured speed of the interface in Gbs.
Oper. Speed	Specifies the current operational speed of the interface in Gbs.
Mode	Specifies the mode of the interface.
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 description that you have added about the interface.
Owner	Specifies the name of the port owner.
Port Group	Specifies the port group number to which the interface belongs to.

3. To perform no shutdown for an interface, check the check box for the required interface and choose **Actions > No Shutdown**. Click **Confirm** in the warning window that appears.
4. To shutdown an interface, check the check box for the required interface and choose **Actions > Shutdown**. Click **Confirm** in the warning window that appears.
5. To assign a port owner for an interface, do the following:
 - a. Check the check box for the required interface and choose **Actions > Owner**.

You can select multiple interfaces while assigning the port owner, if required.
 - b. In the **Set Port Owner** dialog box that appears, enter a required name and click **Apply**.

6. To add description for an interface, do the following:

- a. Check the check box for the required interface and choose **Actions > Description**.



You can add description for multiple interfaces, simultaneously.

- b. In the **Set Port Description** dialog box, enter the description and click **Apply**.

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

VSANs

You can configure and manage Virtual SANs (VSANs) from Cisco Nexus Dashboard Fabric Controller. Go to **SAN > Fabrics**, then double-click on a fabric to view the **Fabric Overview** page. Click on the **VSANs** tab to view VSAN information. You can view or configure VSAN for the discovered fabrics, with either **Manageable** or **Manage Continuously** status. For a selected fabric, a VSAN Scope tree is displayed in the left panel.

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



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

The VSANs tab displays the following fields.

Field	Description
VSAN Name	<p>Displays the VSAN name.</p> <p>The information that is associated with the selected VSAN scope appears in the right panel. If a VSAN is segmented, each individual segmented VSAN is a VSAN scope. For every selected VSAN scope, you can view information in tabs.</p> <ul style="list-style-type: none">▪ Switches Tab▪ ISL Tab▪ Host Ports Tab▪ Storage Ports Tab▪ Attributes Tab▪ Domain ID Tab▪ VSAN Membership Tab
VSAN ID	Specifies the VSAN ID.
Segments	Specifies the Segments on this VSAN. Click on segments to open a slide-in pane to view summary information about each segment.
Status	Specifies if VSAN is Up or Down .

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

Action Item	Description
Create VSAN	Allows you to launch wizard to create VSAN. For more information, click Create VSAN Wizard .

Delete VSAN	Select the VSAN and click Delete VSAN to delete the VSAN. For more information, click Delete VSAN .
-------------	---



When changing VSAN of the Switch port in Nexus Dashboard Fabric Controller, If the port was associated with Isolated VSAN, then the previous VSAN column will be blank. For description on all fields that appear on the tabs, refer [Field and Descriptions for VSANs](#).

Default VSAN Settings

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

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

Create VSAN Wizard

The VSAN Creation Wizard workflow includes these steps:

- VSAN ID and name
- Select Switches
- Configure VSAN Attributes
- Configure VSAN Domain
- Configure Port Membership

Go to **SAN > Fabrics**, then double-click on a fabric to view the **Fabric Overview** page. Click on the **VSANs** tab to view VSAN information. Click **Actions > Create VSAN**. The **Create New VSAN** screen of the wizard is displayed.



Ensure that the VSAN is not already created.

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

Before you begin:

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

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



The suspended VSANs are not managed.

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

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

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

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



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

- d. Click the FICON check box to enable FICON on the switch.
- e. Click Next.

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

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

Click **Next**.

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



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

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

The following types are available:

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



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

b. In InterOp, select an interoperability value.

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

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

- InterOp-3: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.
- InterOp-4: implies that the VSAN can interoperate with specific Fibre Channel vendor devices for basic to advanced functionalities.



InterOp isn't supported on FICON VSAN.

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

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

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



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

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

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

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

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

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

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

g. Click **Next**.

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

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

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

c. For every switch in the table, enter the domain ID from the list of available Domain IDs.

d. Click **Next**.

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



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

Click **Next**.

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

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

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



After the VSAN is created, it will take few minutes for the new VSAN to appear in the VSAN scope tree.
If the switch port is associated with Isolated VSAN then the previous VSAN information will be blank.

Delete VSAN

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

1. Go to **SAN > Fabrics**, then double-click on a fabric to view the **Fabric Overview** page.
2. Click on the **VSANS** tab to view VSAN information.

The **VSANS** window is displayed.

3. Select the VSAN that you want to delete and click **Actions > Delete VSAN**.

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

4. Select all of the switches or select a specific switch to delete the VSAN from those switches, then click **Delete VSAN**.

A confirmation window appears.

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



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


Field and Descriptions for VSANs

The Field and Descriptions for all the tabs that are displayed on **SAN > Fabrics > Fabric Overview > VSANs** are explained in the following sections:

- [Switches Tab](#)
- [ISL Tab](#)
- [Host Ports Tab](#)
- [Storage Ports Tab](#)
- [Attributes Tab](#)
- [Domain ID Tab](#)

Switches Tab

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

Field	Description
Name	Specifies the name of the switch in the VSAN. Click the name to view the switch summary. Click Show more Details to view complete information.
Domain ID	Specifies an insistent domain ID.
VSAN WWN	Specifies the world wide name (WWN) of the VSAN.
Principal WWN	Specifies the world wide name (WWN) of the switch.  For the principal switch, the value is <i>self</i> .
Model	Specifies the model name of the switch.
Release	Specifies the NX-OS version on the switch.
Up Time	Specifies the time from which the switch is up.

ISL Tab

This tab displays information about the ISLs about the switches in the VSAN scope. The following table describes the fields that appear on the ISLs tab.

If the VSAN is configured on both the switches across the ISL and if VSAN is not enabled on the ISL, Nexus Dashboard Fabric Controller considers VSAN as segmented. Therefore, add the VSAN to the trunked VSANs across the ISL to clear the warning message. Alternatively, you can ignore this warning message.

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

Host Ports Tab

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

Field	Description
Enclosure	The name of the enclosure.
Device Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
Fcid	The FC ID assigned for this host.
Switch Interface	Interface on the switch that is connected with the end device.
Link Status	The operational status of the link.
Vendor	Specifies the name of the vendor.
Serial Number	Specifies the serial number of the enclosure.
Model	Specifies the name of the model.
Firmware	The version of the firmware that is executed by this HBA.
Driver	The version of the driver that is executed by this HBA.
Additional Info	The information list corresponding to this HBA.


Storage Ports Tab

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

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


Attributes Tab

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

Field	Description
Edit	<p>Click Edit to modify the attributes of the VSAN and to push the same VSAN attributes to the selected switches.</p> <p>If the VSAN is FICON VSAN in any selected switch, the following fields won't appear on the UI, as they can't be modified for the FICON VSAN.</p> <ul style="list-style-type: none"> • vsanLoadBalancing • InterOp • Inorder Delivery <p>After modify the attributes, you can click Save to save changes or Cancel to discard.</p>
Switch Name	Displays the name of the switch that is associated with the VSAN.
VSAN Name	Displays the name of the VSAN.
Admin	<p>Specifies if the status of the Admin is either Active or Suspend.</p> <ul style="list-style-type: none"> • Active implies that the VSAN is configured and services for the VSAN is activated. • Down implies that the VSAN is configured; however, the service for the VSAN is deactivated. You can use set this state to preconfigure all the VSAN parameters by using the CLI only. <div style="display: flex; align-items: center; margin-top: 10px;">  <p>If you suspend a VSAN, it's removed from Cisco Nexus Dashboard Fabric Controller as well.</p> </div>
Oper	The operational state of the VSAN.
MTU	Displays the MTU for the switch.
Load Balancing	<p>Specifies the load-balancing type that is used in the VSAN.</p> <p>The type of load balancing used on this VSAN.</p> <ul style="list-style-type: none"> • srcId/DestId-use source and destination ID for path selection • srcId/DestId/OxId-use source, destination, and exchange IDs
InterOp	<p>The interoperability mode of the local switch on this VSAN.</p> <ul style="list-style-type: none"> • default • interop-1 • interop-2 • interop-3
Inorder Delivery	The Inorder Delivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it's not guaranteed.
FICON	True if the VSAN is FICON-enabled.


Domain ID Tab

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

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

VSAN Membership Tab

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

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

Device Aliases

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

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

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

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**.



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:

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.

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



If you close the Add device alias window before applying the device aliases to the

switches, the changes will be discarded and the device alias will not be created.

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



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.



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.
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.



Deleting the device alias may cause traffic interruption.

- b. Click **Yes** to delete the device alias.
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.
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:

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

The CFS configuration for this switch is committed.

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

The CFS configuration for this switch is aborted.

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: See the " Alarms" section in [Event Analytics](#)
- Events: See the " Events" section in [Event Analytics](#)
- Accounting: See the " Accounting" section in [Event Analytics](#)


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	<ul style="list-style-type: none">• Choose Backup now. <p>The Create new backup window appears.</p> <ul style="list-style-type: none">• Enter name in Backup tag field. If required choose check box Mark backup as golden. <p>For more information on golden backup, refer to the section "Golden Backup" in Backing Up and Restoring SAN Operational Mode Setups.</p> <ul style="list-style-type: none">• Click OK.
Copy to bootflash	<p>Choose Copy to bootflash. A confirmation window appears, click OK.</p> <p>For more information on bootflash, see the section "Copy Bootflash" in About Switch Overview for SAN Operational Mode Setups.</p>
Compare	<p>Choose required switch names to compare configuration of switches, choose Compare.</p> <p>You can select only two switches at an instance.</p> <p>Compare Config window appears, displaying the difference between the two configuration files.</p> <p>The Source and Target configuration files content is displayed in two columns.</p> <p>The differences in the configuration file are show in the table, with legends.</p> <ul style="list-style-type: none">• Red: Deleted configuration details.• Green: New added configuration.• Blue: Modified configuration details.

Actions	Descriptions
Export	<p>Click Export.</p> <p>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.</p>
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	<p>To delete existing backups, choose Delete a confirmation window appears, click Confirm.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>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.</p> </div>

Name Server

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

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

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

Field	Description
VSAN ID	Specifies the VSAN ID for the selected Fabric.
FC ID	Specifies the associated interface FCID.
Switch	Specifies the name of the switch. Click on the switch name to view the switch summary information. Double click on the switch name to launch the Switch Overview screen.
Port	Specifies the interface port.
Device Alias	Displays the alias retrieved from the switch. A device aliases is a user-friendly name for a port WWN. Device alias name can be specified when configuring features.
Type	The options are N and NL .
Port Name	Specifies the name of the port.
Node Name	Specifies the name of the node.
FC4Type:Feature	Specifies the FC Type that the port is using. This includes which protocol or state the port is in, that is, scsi-fcp, nvme, npv and whether it is an initiator or target. The following are the sample values: <ul style="list-style-type: none">▪ scsi-fcp:target▪ scsi-fcp,nvme:init,init▪ scsi-fcp:both▪ nvme:target,disc

Configuration Monitor

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

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

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

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


The Configuration Monitor tab displays the following fields.

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

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

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

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

Action Item	Description
Enable Fabric Monitoring	Allows you to enable fabric monitoring on all switches in the fabric.
Disable Fabric Monitoring	<p>Allows you to disable monitoring the entire fabric. Note that if you disable fabric monitoring, the configuration drift data will not be captured and there will be no data to display on this tab.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>If you Disable Fabric Monitoring for the fabric, all the alarms are moved to Alarms Cleared tab.</p> </div>
Reset Baseline Configuration	<p>Allows you to reset baseline configuration.</p> <p>Select the switch and choose Reset Baseline Configuration to purge all the configurations into Baseline Configuration.</p>

Viewing of Port Usage

You can view the following information on Port Usage tab.

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

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

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

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

Metrics

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

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

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

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

Fields	Descriptions
Switch Name	Specifies the name of switch.
Avg. Rx	Specifies the average Rx value.
Peak Rx	Specifies the peak Rx value.
Avg. Tx	Specifies the average Tx value.
Peak Tx	Specifies the peak Tx value.
Avg. Rx+Tx	Specifies the average of Rx and Tx value.
Avg. Errors	Specifies the average error value.
Peak Errors	Specifies the peak error value.
Avg. Discards	Specifies the average discard value.
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 ©	Specifies the lowest temperature value.
Avg. Value ©	Specifies the average temperature value.
High Value ©	Specifies the high temperature value.
Show last day	Click Show last day to view data for selected day, week, month, and year.

Congestion Analysis

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



- The jobs run in the background, even after you log off.
- Starting with NDFC release 12.1.3:
 - For the Cisco MDS 9000 Series switches running on NX-OS version 9 and later, performance monitoring data is polled using NX-API for the fiber channel (FC) ports, and the NX-API feature is automatically enabled if it's not already enabled. For Cisco MDS 9000 Series switches running on NX-OS version 8 and earlier, SNMP is used instead.
 - Slow drain job page is removed because the slow drain job is integrated into PM and it runs together with the PM collection for 24 hours by default.

1. Choose **SAN > Fabrics**.
2. From the list of fabrics, double-click on a fabric to view the **Fabric Summary**.
3. Click the **Congestion Analysis** tab.

The **Congestion Analysis** window shows the congestion data for the fabric directly for the last 24 hours. You can change the time scope to see the history data up to two weeks.

4. Determine the type of information that you want to have displayed in the **Device Interfaces** table.
 - Select **Only Rows With Data** to filter and display the nonzero entries in the statistics.
 - Select **Show All Rows** to show all entries in the table, regardless of their values.
5. Click a switch name in the **Switch Name** column of the **Device Interfaces** table to display the switch's health.
6. Click an interface name in the **Interface** column of the **Device Interfaces** table to display the slow drain value for the switch port in a chart format.

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

Congestion Visualization

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

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

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

A switch color represents the highest level Congestion that is found on any link to switch. The maximum value is 3 and the minimum value is 1. A switch has two colors if overutilized. The right half of the switch is colored in light blue to represent the overutilization. A number on the switch represents the number of F ports with Congestion. The color around the number represents the highest level Congestion that is found on F ports of the switch. Click the switch to bring in a sliding window, which shows the switch details. Double-click on the switch to view congestion data by filtering on the switch name.

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



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

DIRL

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

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

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

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

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

The following are the different transition states of DIRL:

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

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

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



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

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

DIRL Congestion Management Visualization

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

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



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

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

1. Choose **SAN > Fabrics**.
2. From the list of Fabrics, double click on the fabric to view **Fabric Summary**.
3. Click **DIRL** tab.
4. Click **Start DIRL data collection** to begin collection.
5. Click **Cancel/Abort** to stop the collection.

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

An entry in the table below shows that following fields:

Field	Description
Switch	Specifies the switch on which the analysis is collected. Click on the Switch to view a slide-in pane displaying the summary. Click on the launch icon to view Switch Overview .
Interface	<p>Specifies the interface on which the analysis is collected.</p> <ul style="list-style-type: none"> Click the trend icon to view the chart for DIRL events on the interface. The graph provides information about Ingress, Egress, DIRL counter(s) values of the current DIRL with event timestamps for the selected DIRL interface. <p>The graph also shows set of Falling/Rising threshold of each DIRL counter; the threshold is based on the active edge type Port Monitor policy at the time of the DIRL status collection.</p> <ul style="list-style-type: none"> Click on the interface name to view interface summary. Click VSAN value to view the related VSANs. Click DIRL Events to view Rate Limit Events. The table displays the events of this interface from the CLI command output show fpm ingress-rate-limit events.
Current rate limit (%)	Specifies the % indicating the current rate limit.
Previous action	Specifies the previous action performed to control the rate limit.
Last updated time	Displays the time stamp at which the event occurred.

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

Rate Limit Events

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

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

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

Field	Description
Fabric	Specifies the Fabric to which the switch belongs.
Switch	Specifies the fabric for which the DIRL congestion is visualized.
Interface	Specifies the interface on which the events are visualized.
Last collection at	Specifies the date and time at which the DIRL status was collected.

Field	Description
Counter	Specifies if the counter is for txwait or tx-datarate or tx-datarate-burst .
Event	Specifies the event.
Counter Value %	Specifies the value of the counter.
Action	Specifies the action which triggered the event,
Operating port speed (Mbps)	Specifies the speed of the operating port.
Input rate (Mbps)	Specifies the input rate.
Output rate (Mbps)	Specifies the output rate.
Current rate limit (%)	Specifies the current rate limit.
Applied rate limit (%)	Specifies the applied rate limit.
Time	Specifies the time at event was triggered.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017–2024 Cisco Systems, Inc. All rights reserved.