

Event Analytics

This section contains the following topics:

- Alarms, on page 1
- Events, on page 11
- Accounting, on page 15
- Remote Clusters, on page 16

Alarms

This tab displays the alarms that are generated for various categories. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Last Updated (optional), Policy, and Message. You can specify the Refresh Interval in this tab. You can select one or more alarms and then acknowledge or unacknowledge their status using the Change Status drop-down list. In addition, you can select one or more alarms and then click the Delete button to delete them.

Alarms Raised

UI Path: **Operations > Event Analytics > Alarms**

1. Click the **Alarms Raised** tab to view the alarm policies that were triggered by an alarm.
2. Click on the **Severity** in the Alarms table to view the history of the alarms raised due to the same policy on the same ITL/ITN flow.
3. Click on policy ID in **ID** column to view the charts.

   A slide-in pane appears with charts.
4. Choose required **Metrics** from drop-down list to view the graph.

Note These metrics can be viewed only for SAN Insights Anomaly Policy.

The following table describes the fields that appear on **Operations > Event Analytics > Alarms > Alarms Raised**.

Field	Description
Severity	Specifies the severity of the alarm
Source	Specifies the name of the source.
Name	Specifies the name of the alarm
Category	Specifies the category of the alarm
Creation Time	Specifies the time at which the alarm was created
Policy	Specifies the policy of the alarm
Message	Displays the message.
Ack User	Displays the username who acknowledged the alarm.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Alarms Raised** tab.

Action Item	Description
Acknowledge	Choose one or multiple alarms and choose **Acknowledge**. Allows you to bookmark the alarms and adds ack user name to **Acknowledged** column.
Unacknowledge	Choose one or multiple alarms and choose **Unacknowledge** to remove the bookmarked alarms. **Note** Only acknowledged alarms can be unacknowledged.
Clear	Choose alarm and choose **Clear** to clear the alarm policy manually. The cleared alarms will be moved to **Alarm Cleared** tab.
Delete Alarm	Choose an alarm and choose **Delete** to delete the alarm.

Alarms Cleared

UI Path: **Operations > Event Analytics > Alarms > Alarms Cleared**

Alarms Cleared tab has the list of alarms which are cleared in the **Alarms Raised** tab. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Cleared At (optional), Cleared By, Policy, and Message. You can view the cleared alarm details for maximum of 90 days.

You can choose one or more alarms and click the **Actions > Delete** to delete them.

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

Field	Description
Severity	Specifies the severity of the alarm.
Source	Specifies the IP Address of source alarm.

Field	Description
Name	Specifies the name of the alarm.
Category	Specifies the category of the alarm.
Creation Time	Specifies the time at which the alarm was created.
Cleared Time	Specifies the time at which the alarm was cleared.
Cleared By	Specifies the user who cleared the alarm.
Policy	Specifies the policy of the alarm.
Message	Specifies the CPU utilization and other details of alarm
Ack User	Specifies the acknowledged user role name.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Alarms Cleared** tab.

Action Item	Description
Delete Alarm	Select an alarm and choose **Delete** to delete the cleared alarm

Monitoring and Adding Alarm Policies

In Cisco SAN Controller to enable alarms, Navigate to **Operations** > **Event Analytics** > **Alarms**, click **Alarm Policies** on vertical tab. Ensure that the Enable external alarms check box is selected. You must restart SAN Controller Server to bring this into effect.

You can forward alarms to registered SNMP Listeners in SAN Controller. From Cisco SAN Controller web UI, choose **Settings > Server Settings > Alarms**, ensure that the **Enable external alarms** check box is selected. You must restart SAN Controller Server to bring this into effect.

You can forward alarms to registered SNMP Listeners in SAN Controller. From Cisco SAN Controller web UI, choose **Settings > Server Settings > Alarms**, enter an external port address in alarm.trap.listener.address field, click **Apply Changes**, and restart SAN Controller.



Note Ensure that you select **Forwarding** check box in **Alarm Policy creation** dialog window to enable forwarding alarms to external SNMP Listener.

The following table describes the fields that appear on **Operations > Event Analytics > Alarms > Alarms Policies**.

Field	Description
Name	Specifies the name of the alarm policy
Description	Specifies the description of the alarm policy
Status	Specifies the status of the alarm policy: • Activated • Deactivated

Field	Description
Policy type	Specifies the type of the policy: • Device Health Policy • Interface Health Policy • Syslog Alarm Policy • Hardware Health Policy • SAN Insights Anomaly
Devices	Specifies the devices to which the alarm policy is applied.
Interfaces	Specifies the interfaces.
Details	Specifies the details of the policy.

The following table describes the action items, in the **Actions** menu drop-down list that appear on **Operations > Event Analytics > Alarms > Alarms Policies**.

Action Item	Description
Create new alarm policy	Choose to create a new alarm policy. See Create new alarm policy section.
Edit	Select a policy and choose **Edit** to edit the alarm policy.
Delete	Select a policy and choose **Delete** to delete the alarm policy.
Activate	Select a policy and choose **Activate** to activate and apply the alarm policy.
Deactivate	Select a policy and choose **Deactivate** to disable and deactivate the alarm policy.
Import	Select to import alarm policies from a .txt file.
Export	• Click the box next to a specific alarm policy, then click **Export** to export that alarm policy as a .txt file. • Select or deselect all the boxes next to the alarm policies, then click **Export** to export all the alarm policies as a .txt file.

You can add alarm policies for the following:

- **Device Health Policy**: Device health policies enable you to create alarms when Device SNMP Unreachable, or Device SSH Unreachable. Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.
- **Interface Health Policy**: Interface health policies enable you to monitor Up or Down, Packet Discard, Error, Bandwidth details of the interfaces. By default all interfaces are selected for monitoring.
- **Syslog Alarm Policy**: Syslog Alarm Policy defines a pair of syslog messages formats; one which raises the alarm, and one which clears the alarm.
- **Hardware Health Policy**: The hardware health policy is used to raise hardware-related alarms for different parameters, such as fan status, power supply, modular status and all interface-related alarms.

- **San Insights Anomaly Policy**: SAN Insights Anomaly Policy enables you to create customized alarms to identify issues in the fabric using SAN Insight data.

  From Cisco Nexus Dashboard SAN Controller Release 12.1.2e, you can modify or activate or use data of pre-provisioned SAN Insights anomaly policies which is in **Not Active** state by default.

Create new alarm policy

You can add alarm policies for the following:

- Device Health Policy
- Interface Health Policy
- Syslog Alarm Policy
- Hardware Health Policy
- SAN Insights Anomaly

After you create a new alarm policy, in the **Alarm Policies** tab, click **Refresh** to view the newly-created alarm policy.

Device Health Policy

Device health policies enable you to create alarms when certain conditions are met. By default, all devices are selected for monitoring.

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: You can forward alarms to registered SNMP listeners in SAN Controller. From the Web UI, choose **Settings** > **Server Settings** > **Events**.



Note Ensure that you select **Forwarding** check box while configuring alarm policies to forward alarms to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From SAN Controller Web UI, choose **Settings** > **Server Settings** > **Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.
- Specify the CPU utilization parameters, memory utilization parameters, and environmental temperature parameters.
- **Device Availability**: Device health policies enable you to create alarms in the following situations:
  - **Device Access**: When device SNMP or device SSH is unnreachable.
  - **Peripherals**: When fan, power supply, or module is unnreachable.

Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.

Select the devices for which you want to create policies. Specify the policy name, description, CPU Utilization parameters, Memory Utilization parameters, Environment Temperature parameters, device availability, and device features.

Interface Health Policy

Interface health policies enable you to monitor the interface status, packet discards, errors and bandwidth details of the interfaces. By default, all interfaces are selected for monitoring.

Select the devices for which you want to create policies and then specify the following parameters:

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: You can forward alarms to registered SNMP listeners in SAN Controller. From the Web UI, choose **Settings** > **Server Settings** > **Events**.



Note Ensure that you select **Forwarding** check box while configuring alarm policies to forward alarms to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From SAN Controller Web UI, choose **Settings** > **Server Settings** > **Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.
- **Linkstate**: Choose linkstate option to check for the interface link status. You can generate an alarm whenever a link is down and clear the alarms when the link is up.
- **Bandwidth (In/Out)**: Allows you to set the maximum bandwidth allowed in inbound and outbound directions. The system generates alarms when the bandwidth exceeds the specified values.
- **Inbound Errors**: Allows you to set thresholds for the number of inbound errors that are discarded after which it generates an alarm.
- **Outbound Errors**: Allows you to set thresholds for the number of outbound errors that are discarded after which it generates an alarm.
- **Inbound Discards**: Allows you to set thresholds for the number of inbound packets that are discarded after which it generates an alarm.
- **Outbound Discards**: Allows you to set thresholds for the number of outbound packets that are discarded after which it generates an alarm.

Syslog Alarm

Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one which clears the alarm.

Select the devices for which you want to create policies and then specify the following parameters:

- Devices: Define the scope of this policy. Select individual devices or all devices to apply this policy.
- Policy Name: Specify the name for this policy. It must be unique.
- Description: Specify a brief description for this policy.

- Forwarding: You can forward alarms to registered SNMP listeners in SAN Controller. From Web UI, choose **Settings > Server Settings > Events**.



Note Ensure that you select **Forwarding** check box in Alarm Policy creation dialog window to enable forwarding alarms to external SNMP listener.

- Email: You can forward alarm event emails to recipient when alarm is created, cleared or severity changed. From SAN Controller Web UI, choose **Settings > Server Settings > Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.
- Severity: Define the severity level for this syslog alarm policy. Choices are: Critical, Major, Minor, and Warning.
- Identifier: Specify the identifier portions of the raise & clear messages.
- Raise Regex: Define the format of a syslog raise message. The syntax is as follows: Facility-Severity-Type: Message
- Clear Regex: Define the format of a syslog clear message. The syntax is as follows: Facility-Severity-Type: Message

The Regex definitions are simple expressions but not a complete regex. Variable regions of text are noted using $(LABEL) syntax. Each label represents a regex capture group (.+), which corresponds to one or more characters. The variable texts found in both raise and clear messages are used to associate the two messages. An Identifier is a sequence of one or more labels that appear in both messages. An Identifier is used to match a clear syslog message to the syslog message that raised the alarm. If the text appears only in one of the messages, it can be noted with a label and exclude it from the identifier.

Example: A policy with "Value": "ID1-ID2",

```
"syslogRaise": "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"
"syslogClear": "SVC-5-UP: $(ID1) module $(ID2) is up."
```

In the example, ID1 and ID2 labels can be marked as an identifier to find the alarm. This identifier will be found in corresponding syslog messages. Label “REASON” is in the raise but not in the clear message. This label can be excluded from the identifier, as it has no impact on the syslog message to clear the alarm.

Table 1: Example 1

Identifier	**ID1-ID2**
Raise Regex	ETHPORT-5-IF_ADMIN_UP: Interface Ethernet15/1 is admin up .
Clear Regex	ETHPORT-5-IF_DOWN_NONE: Interface Ethernet15/1 is down (Transceiver Absent)

In the above example, the regex expressions are part of the syslog messages that appear in the terminal monitor.

Table 2: Example 2

Identifier	**ID1-ID2**
Raise Regex	ETH_PORT_CHANNEL-5-PORT_DOWN: $(ID1): $(ID2) is down
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP: $(ID1): $(ID2) is up

Table 3: Example 3:

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning cleared

Hardware Health Policy

The hardware health policy is used to raise hardware-related alarms for different parameters, such as fan status, power supply, modular status and all interface-related alarms.

By default, there is a hardware policy called as discovery that is standard with the NDFC installation. This hardware policy defines various conditions for different parameters. You can also create custom hardware policies for the parameters listed above and define regex expressions based on which alarms are raised.

By default, the **All Devices** option is selected automatically.

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: You can forward alarms to registered SNMP listeners in SAN Controller. From the Web UI, choose **Settings** > **Server Settings** > **Events**.



Note Ensure that you select **Forwarding** check box while configuring alarm policies to forward alarms to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From SAN Controller Web UI, choose **Settings** > **Server Settings** > **Events**. Configure the SMTP parameters, click **Save**, and restart SAN Controller services.

Hardware alarms are raised based on regex expressions that you enter when you are creating the policy.

In the **Alarms** area, create a hardware health policy to raise alarms for the following parameters:

- **Fan**: Define the severity for fan-related alarms and determine the condition for the alarms.
  1. Click the toggle switch next to **Fan** to enable the fan-related alarms.
  2. Select the severity of the alarm:
     - Critical
     - Major
     - Minor
     - Warning
     - Cleared
  3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status is not that value.

For example, if you enter `ok` in the **Trigger alarm when status is not** field, NDFC will raise an alarm for any status other than `ok`, such as N/A.

4. Click **Save**.

- **Power Supply**: Define the severity for power supply-related alarms and determine the condition for the alarms.
  1. Click the toggle switch next to **Power Supply** to enable the power supply-related alarms.
  2. Select the severity of the alarm:
     - Critical
     - Major
     - Minor
     - Warning
     - Cleared
  3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status is not that value.

     For example, if you enter `ok` in the **Trigger alarm when status is not** field, NDFC will raise an alarm for any status other than `ok`, such as failed, OffEnvpower, OffDenied, and so on.
  4. Click **Save**.
- **Module**: Define the severity for module-related alarms and determine the condition for the alarms.
  1. Click the toggle switch next to **Module** to enable the module-related alarms.
  2. Select the severity of the alarm:
     - Critical
     - Major
     - Minor
     - Warning
     - Cleared
  3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status matches that value.

     For example, if you were to enter the following value in the **Trigger alarm when status matches regex** field, as shown in the information (i) button:

     ```
     ^(?!ok|poweredDown|okButDiagFailed).*$
     ```

     NDFC will raise an alarm when modules are in states other than ok, poweredDown, and OkButDiag failed.
  4. Click **Save**.
- **Interface Status**: Define the severity for interface-related alarms and determine the condition for the alarms.

1. Click the toggle switch next to **Interface Status** to enable the interface-related alarms.
2. Click one or more toggle switches next to the appropriate severity to select the severity of the alarm:
   - Critical
   - Major
   - Minor
   - Warning
   - Cleared
3. Click **Edit Regex**, then enter the value that will trigger the alarm when the status matches that value. The provided regex expression is matched against the combined field of `admin_status:oper_status:status_reason`.

   For example, if you were to enter the following value in the **Trigger alarm when status matches regex** field:

   ```
   ^up:down:(?!Link not connected|XCVR not inserted|sfpNotPresent|Channel admin down).*$
   ```

   NDFC will raise an alarm when interfaces are in states that match these values.
4. Click **Save**.

SAN Insights Anomaly Policy

From Cisco Nexus Dashboard SAN Controller Release 12.0(1), a new policy type saninsights is added. This new policy type can be customized to identify issues. You can create an alarm policy, based on specific flows to retain per interval data for analysis. If selected flow matches alarm policy, maintain the flow based on the parameters defined by the policy.

Procedure

Step 1 Choose **Operations** > **Event Analytics** > **Alarms**.

Step 2 Choose **Alarm Policies** in the **Alarms** tab.

Step 3 Choose **Actions** > **Create new alarm policy**.

Step 4 Use the **San Insights Anomaly Policy** radio button.

Step 5 Specify details for below parameters:

- **Policy Name**: Specify the name for this policy. It must be unique.
- **Description**: Specify a brief description of this policy.
- **Forwarding**: Choose checkbox, to enable forwarding alarms to external SNMP listener.
- **Email**: Choose checkbox, to send mail updates on this policy to mail id.

Step 6 Select time from drop-down list to define **Capture Time** and **Retention Time**.

- **Capture Time**: Specifies the length of time to capture per-interval data for each flow matching the given policy.

- **Retention Time**: Specifies the length of time to keep that data (before it is deleted).

Step 7 Select time or interval from the drop-down list to define **Analysis Level** and select severity level from drop-down list to define the **Severity** of this policy.

- **Analysis Level**: Specifies which aggregation of flow data must be checked for the given policy. Some policy types such as aborts or failures policy are logic to match when it happens instantly (Interval level). Some policy types are as an anomaly policy when they are sustained above a threshold. For example, a momentary ECT or DAL spike in level is not alarming, but if that same spike level is continued for a period (5 minutes or 1 hour) then it must be investigated.
- **Severity**: Specifies the severity that will be associated with any alarms that are raised due to this policy.

Step 8 You can define a new rule, click **Add new rule** and specify mandatory fields and then click **Create new policy**.

Note
- You can define one or more new rules and match criteria to identify a flow and create a new policy.
- All policies are matched against each ITL/ITN flow records streamed to the receiver from the switches.

You can view the created alarms in the **Alarms** tab.

Events

This tab displays the events that are generated for the switches. This tab displays information such as Ack, Acknowledged user, Group, Switch, Severity, Facility, Type, Count, Last Seen, and Description. You can select one or more events and then acknowledge or unacknowledge their status using the Change Status drop-down list. In addition, you can select one or more alarms and then click the Delete button to delete them. If you want to delete all events, click the Delete All button.

The following table describes the fields that appear on **Operations > Event Analytics > Events**.

Field	Description
Group	Specifies the Fabric
Switch	Specifies the hostname of the switch
Severity	Specifies the severity of the event
Facility	Specifies the process that creates the events. The event facility includes two categories: NDFC and syslog facility. Nexus Dashboard Fabric Controller facility represents events generated by Nexus Dashboard Fabric Controller internal services and SNMP traps generated by switches. Syslog facility represents the machine process that created the syslog messages.
Type	Specifies how the switch/fabric are managed

Field	Description
Count	Specifies the number of times the event has occurred
Creation Time	Specifies the time when the event was created
Last Seen	Specifies the time when the event was run last
Description	Specifies the description provided for the event
Ack	Specifies if the event is acknowledged or not

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Operations > Event Analytics > Events**.

Action Item	Description
Acknowledge	Select one or more events from the table and choose **Acknowledge** icon to acknowledge the event information for the fabric. After you acknowledge the event for a fabric, the acknowledge icon is displayed in the Ack column next to the Group.
Unacknowledge	Select one or more events from the table and choose **Unacknowledge** icon to acknowledge the event information for the fabric.
Delete	Select an event and choose **Delete** to delete the event.
Add Suppressor	Select an event and choose **Add Suppressor** to add a rule to the event. You can provide name to the rule. Using the **Scope** options, you can add this rule to all the Fabrics, or particular elements or all elements.
Event Setup	Allows you to setup new event. For more information, see Event Setup, on page 12.

Event Setup

To setup an event using the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **Operations** > **Event Analytics** and click on the **Events** tab.

Step 2 From the **Actions** drop-down list, select **Event Setup**.
The **Receiver** tab displays the following details:

- **Syslog Receiver enabled**: Displays the status of the syslog server.
- **SNMP Trap Receiver**: Displays the details of SNMP traps received, processed and dropped.
- **Syslog Receiver**: Displays the details of syslog messages received, processed and dropped.

Step 3 Navigate to the **Sources** tab, to view a list of fabrics and its associated switches.
The **Sources** tab displays all the fabrics and the associated switches in tabular format. It also displays if traps and syslogs have been configured on the switches.

Step 4 Perform the following steps to create rules for forwarding email notifications or traps for events:

Cisco Nexus Dashboard Fabric Controller Web UI forwards fabric events through email or SNMPv1 or SNMPv2c traps. Some SMTP servers may require adding authentication parameters to the emails that are sent from Nexus Dashboard Fabric Controller to the SMTP servers.

a) Ensure that you have configured SMTP parameters before configuring rules for forwarding event notifications through emails. To verify SMTP configuration, navigate to **Settings** > **Server Settings** > **SMTP** and verify that you have configured the required fields.

a) To enable events forwarding, choose **Settings** > **Server Settings** > **Events** and configure the fields as described in the following table.

Table 4: Configure Events Forwarding

Field	Description
Enable Event forwarding	Check the checkbox to enable events forwarding feature.
Email Forwarding From Email List	Specifies the email address from which the forwarding messages arrive.
Snooze Event Forwarding	Snoozes an event from forwarding for the given time range.
Maximum Number of Repeats in Event Forwarding	Stops forwarding an event after the specified time. 0 indicates unlimited time.
Maximum Number in Events/Traps/Syslog Queue	Specifies the maximum number in the queue before dropping the incoming events/traps/syslog.

b) To configure rules, choose **Operations** > **Event Analytics**.

c) Navigate to the **Forwarding** tab and choose **Actions** > **Add Rule** and configure the fields as described in the following table.

Table 5: Configure Rules

Field	Description
Forwarding Method	Chooose one of the forwarding methods: • **E-Mail** • **Trap**
Email Address	This field appears if you select **E-mail** as the forwarding method. Enter an email address for forwarding the event notifications.

Field	Description
Address	This field appears if you select **Trap** as the forwarding method. Enter the IP address of the SNMP trap receiver. You can either enter an IPv4 or IPv6 address or a DNS server name.
Port	Enter the port to which the traps are forwarded.
Forwarding Scope	Maximum number in queue before dropping the incoming events/traps/syslog messages.
Fabric	Select **All Fabrics** or a specific fabric for notification.
VSAN Scope	For SAN Installer, select the VSAN scope. You can either choose **All** or **List**.
VSAN List	If you select **List**, provide the list of VSANs for notification.
Source	Select **DCNM** or **Syslog**. If you select **DCNM**, do the following: **1.** From the **Type** drop-down list, choose an event type. **2.** Check the **Storage Ports Only** check box to select only the storage ports. This check box is enabled only for port related events. If you select **Syslog**, do the following: **1.** In the **Facility** list, select the syslog facility. **2.** In the **Type** field, enter the syslog type. **3.** In the **Description Regex** field, enter a description that matches with the event description.

d) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.

The traps that are transmitted by Cisco Nexus Dashboard Fabric Controller correspond to the severity type. A text description is also provided with the severity type.

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

e) Click **Add Rule**.

Step 5 Perform the following steps to create rules for suppressing events:

Nexus Dashboard Fabric Controller allows you to suppress specified events based on user-specified rules. Such events will not be displayed on the Nexus Dashboard Fabric Controller Web UI and SAN Client. The events will neither be added to the Nexus Dashboard Fabric Controller database, nor forwarded via email or as SNMP traps.

You can view, add, modify, and delete rules from the table. You can create a rule from the existing events. Select an existing event as the template and open the **Add Rule** window by navigating to **Operations** > **Event Analytics** > **Events** page, select the event and choose **Actions** > **Add Suppresor**. The details are automatically ported from the selected event in the events table to the fields of the **Add Rule** window.

a) In the **Name** field, enter a name for the rule.
b) In the **Scope** field, select one of the following options - **SAN**, **Port Groups** or **Any**.

In the **Scope** field, the LAN/SAN groups and the port groups are listed separately. For SAN and LAN, select the scope of the event at the fabric or group or switch level. You can only select groups for port group scope. If use select **Any** as the scope, the suppression rule is applied globally.

c) In the **Facility** field, enter the name or choose from the SAN/LAN switch event facility list.

If you do not specify a facility, a wildcard is applied.

d) In the **Type** field, enter the event type.

If you do not specify the event type, wildcard is applied.

e) In the **Description Matching** field, specify a matching string or regular expression.

The rule matching engine uses regular expression that is supported by Java Pattern class to find a match against an event description text.

f) Check the **Active Between** check box and select a valid time range during which the event is suppressed.

By default, the time range is not enabled.

Note
In general, you must not suppress accounting events. Suppression rule for Accounting events can be created only for certain situations where accounting events are generated by actions of Nexus Dashboard Fabric Controller or switch software. For example, 'sync-snmp-password' AAA syslog events are automatically generated during the password synchronization between Nexus Dashboard Fabric Controller and managed switches. To suppress accounting events, navigate to **Operations** > **Event Analytics** > **Events** page, select the event and choose **Actions** > **Add Suppressor**.

g) Click **Add Rule**.

Accounting

You can view the accounting information on Cisco Nexus Dashboard Fabric Controller Web UI.

The following table describes the fields that appear on **Operations > Event Analytics > Accounting**.

Field	Description
Source	Specifies the source
User Name	Specifies the user name.
Time	Specifies the time when the event was created
Description	Displays the description.
Group	Specifies the name of the group.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Operations > Event Analytics > Accounting**.

Action Item	Description
Delete	Select a row and choose **Delete** to delete accounting information from the list.

Remote Clusters

This tab displays the clusters and the number of Fabrics in each cluster in your setup.

Click on the Cluster Name to see the summary information. You can click on the launch icon to view the detailed summary of the Cluster.