



## Event Analytics

This section contains the following topics:

- [Alarms, on page 1](#)
- [Events, on page 9](#)
- [Accounting, on page 13](#)
- [Remote Clusters, on page 13](#)

## 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**

After you create a new alarm policy, navigate to **Alarms Raised** tab, click **Refresh** icon to view the created alarm.

Click on required **Severity** column, a slide-in pane appears with policy severity details and description.

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

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



**Note** For link-down events, you must setup an external visible IP address for SNMP trap receiver, and configure switch to send SNMP trap to NDFC. Otherwise, the port state change can only be done through polling, which is every 5 minutes.

## 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.
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.

Field	Description
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 <b>Delete</b> to delete the cleared alarm

## Monitoring and Adding Alarm Policies

In Cisco Nexus Dashboard Fabric 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 Nexus Dashboard Fabric Controller Server to bring this into effect.

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

You can forward alarms to registered SNMP listeners in Nexus Dashboard Fabric Controller. From Cisco Nexus Dashboard Fabric 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 > Alarm 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: <ul style="list-style-type: none"> <li>• Activated</li> <li>• Deactivated</li> </ul>

Field	Description
Policy type	Specifies the type of the policy: <ul style="list-style-type: none"> <li>• Device Health Policy</li> <li>• Interface Health Policy</li> <li>• Syslog Alarm Policy</li> </ul>
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 <a href="#">Create new alarm policy</a> section.
Edit	Select a policy and choose <b>Edit</b> to edit the alarm policy.
Delete	Select a policy and choose <b>Delete</b> to delete the alarm policy.
Activate	Select a policy and choose <b>Activate</b> to activate and apply the alarm policy.
Deactivate	Select a policy and choose <b>Deactivate</b> to disable and deactivate the alarm policy.
Import	Select to import alarm policies in bulk from a .csv file.
Export	Select to export alarm policies in bulk from a .csv 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.

## Create new alarm policy

You can add alarm policies for the following:

- Device Health Policy
- Interface Health Policy
- Syslog Alarm Policy

### Device Health Policy

Device health policies enable you to create alarms when Device ICMP Unreachable, Device SNMP Unreachable, or Device SSH Unreachable. 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.

### 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.

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

- 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 Cisco Nexus Dashboard Fabric 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 Cisco Nexus Dashboard Fabric Controller Web UI, choose **Settings > Server Settings > Events**. Configure the SMTP parameters, click **Save**, and restart Cisco Nexus Dashboard Fabric Controller services.
- Linkstate: Choose linkstate option to check for the interface link up or down. For the link-down you can raise an alarm and the link-up clear the alarms.
- Bandwidth (In/Out) -
- Inbound errors
- Outbound errors
- Inbound Discards
- Outbound Discards

### 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 Cisco Nexus Dashboard Fabric 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 Cisco Nexus Dashboard Fabric Controller Web UI, choose **Settings > Server Settings > Events**. Configure the SMTP parameters, click **Save**, and restart Cisco Nexus Dashboard Fabric 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

Identifier	ID1-ID2
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

## Endpoint Locator Alarms

Alarms are registered and created under the External alarm category by the Endpoint Locator (EPL).

### Alarm Policy

The EPL external alarm category policy is activated when EPL is enabled on a fabric. Alarms are raised for issues such as Duplicate IP addresses, Duplicate MAC addresses, Endpoints appearing on a VRF and Endpoints disappearing from a VRF, Endpoints moving within a fabric, loss of Route Reflector connectivity, and restoration of Route Reflector connectivity. Depending on the issue, the severity level of the alarm policy can be CRITICAL or MINOR.

Alarms are raised and categorized as CRITICAL for the following events:

- Route Reflector disconnection
- Detection of a duplicate IP address
- Detection of a duplicate MAC address

Alarms are raised and categorized as MINOR for the following events:

- Movement of an endpoint
- Appearance of a new VRF in a fabric
- Number of endpoints in a fabric goes down to 0
- Number of endpoints in a VRF goes down to 0
- Disappearance of all endpoints from a switch
- Connection of a Route Reflector (RR)

CRITICAL alarms are cleared automatically when the condition is corrected. For example, when the connectivity between NDFC and RR is lost, a CRITICAL alarm is generated. This alarm is automatically cleared when the connectivity between NDFC and RR is restored. Other MINOR alarms are automatically cleared after 30 minutes have passed since the alarm was generated.




---

**Note** You must clear the duplicate MAC and duplicate IP alarms after the condition is resolved.

---

Choose **Event Analytics > Alarms > Alarm Policies** to display the EPL alarm policies. These alarm policies are not editable on the web UI. Choose **Actions > Activate** or **Deactivate** to activate or deactivate the selected policy.

In case an alarm policy is deleted using the NDFC Web UI, any alarms created or cleared for that policy will not be displayed in the **Event Analytics > Alarms > Alarm Policies** tab. To delete a policy, select the checkbox next to the policy and click **Delete**. However, we recommend not deleting a policy from the NDFC Web UI. When a fabric is deleted, the alarm policy along with all the active alarms for the devices in that fabric are deleted.

### Endpoint Locator: Active Alarms

Choose **Event Analytics > Alarms > Alarms Raised** to display the active alarms.

To clear active alarms, select the checkbox next to the alarm, click **Actions > Clear**.

The screenshot shows the 'Event Analytics' interface with the 'Alarms Raised' tab selected. A table displays several alarms. The first row is selected, and the 'Ack Us' column has a dropdown menu open with 'Clear' highlighted.

Severity	Source	Name	Category	Creation Time	Updated Time	Policy	Message	Ack Us
Minor	172.28.10.39	es-leaf3	HW_MODULES_PS	4/5/2022, 4:41:07 AM	5/5/2022, 11:25:04 PM	discovery	Power Supply powersupply-1 updated(470) in undesired state offEnvPower	<input checked="" type="checkbox"/> Acknowledge <input type="checkbox"/> Unacknowledge <input type="checkbox"/> Clear <input type="checkbox"/> Delete Alarm
Minor	172.28.10.37	es-leaf1	HW_MODULES_PS	4/5/2022, 4:41:07 AM	5/5/2022, 11:25:04 PM	discovery	Power Supply powersupply-1 updated(470) in undesired state offEnvPower	<input type="checkbox"/> Acknowledge <input type="checkbox"/> Unacknowledge <input type="checkbox"/> Clear <input type="checkbox"/> Delete Alarm
Minor	172.28.10.100	es-spine	HW_MODULES_PS	4/5/2022, 4:41:07 AM	5/5/2022, 11:25:04 PM	discovery	Power Supply powersupply-1 updated(470) in undesired state offEnvPower	<input type="checkbox"/> Acknowledge <input type="checkbox"/> Unacknowledge <input type="checkbox"/> Clear <input type="checkbox"/> Delete Alarm
Minor	172.28.10.38	es-leaf2	HW_MODULES_PS	4/5/2022, 4:41:07 AM	5/5/2022, 11:25:04 PM	discovery	Power Supply powersupply-1 updated(470) in undesired state offEnvPower	<input type="checkbox"/> Acknowledge <input type="checkbox"/> Unacknowledge <input type="checkbox"/> Clear <input type="checkbox"/> Delete Alarm

To delete active alarms, select the checkbox next to the alarm and click **Actions > Delete**.

### Endpoint Locator: Cleared Alarms

To view the cleared alarms, navigate to **Event Analytics > Alarms > Alarms Cleared**.

Click on required **Cleared** status column to display detailed information about the required alarm.



The screenshot displays the 'Event Analytics' interface. On the left, there is a navigation menu with options: Alarms, Events, Accounting, and Remote Clusters. Under 'Alarms', there are sub-sections for 'Alarms Raised', 'Alarms Cleared', and 'Alarm Policies'. The main area shows a table of cleared alarms with columns for Status, Source, Name, Category, and Creation Time. A 'Filter by attributes' box is visible above the table. On the right, a detailed view of an 'Alarm Cleared' event is shown, including metadata like Source Name, Category, Policy, Interface, Acknowledged User, Sensor Index, Cleared By, and Cleared At. Below this is a 'Related History' table with columns for Severity, Value, Recieved At, Seen By, and Description.

Severity	Value	Recieved At	Seen By	Description
Critical	DOWN	4/25/2022, 11:25:01 AM	POLL	Switch ICMP Unreachable:172.28.10.39(es-leaf3)
Cleared	UP	4/25/2022, 11:29:52 AM	POLL	Switch ICMP Reachable:172.28.10.39(es-leaf3)

To delete a cleared alarm from the list of cleared alarms, select the checkbox next to the alarm and click **Actions > Delete**.

For more information on Alarms and Policies, refer [Alarms](#).

## 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 <b>Acknowledge</b> 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 <b>Unacknowledge</b> icon to acknowledge the event information for the fabric.
Delete	Select an event and choose <b>Delete</b> to delete the event.
Event Setup	Allows you to setup new event. For more information, see <a href="#">Event Setup, on page 10</a> .

## 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 > Event Setup**. From the **Actions** menu drop-down list, choose **Event Setup**.
- Step 2** In the Receiver tab, perform the following steps:
- Use the toggle button to enable this feature.
  - Select **Copy Syslog Messages to DB** and click **Apply** to copy the syslog messages to the database. If this option is not selected, the events will not be displayed in the events page of the Web client. The columns in the second table display the following:
    - Switches sending traps
    - Switches sending syslog
    - Switches sending syslog accounting
    - Switches sending delayed traps

- c) In the Sources tab, the table displays fabrics and switches associate with it. It also displays information about traps and syslogs.

**Step 3**

To add and remove notification forwarding for system messages from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Cisco Nexus Dashboard Fabric Controller Web UI forwards fabric events through email or SNMPv1 traps. Some SMTP servers may require addition of authentication parameters to emails that are sent from Nexus Dashboard Fabric Controller to the SMTP servers. You can add authentication parameters to the emails that are sent by Nexus Dashboard Fabric Controller to any SMTP server that requires authentication. Enable this feature on **Settings > Server Settings > Events** tab.

- a) Choose **Settings > Server Settings > Events** tab. Check **Enable Event forwarding** check box to enable events forwarding. The events forwarding scope, the recipient email address, severity of the event and type of the event is displayed. The description Regexp field is applicable only when the forwarding source is selected as Syslog while adding the events forwarder.
- b) Specify the **SMTP Server** details and the **From** email address. Configure the **Snooze** and **Event Count** filter.
- c) Click **Save**.
- d) Choose **Operations > Event Analytics**. From the Actions drop-down list, choose **Add Rule**.
- e) In the Forwarding Method, choose either **E-mail** or **Trap**.

If you choose **Trap**, **Address** and **Port** field is added to the dialog box.

- f) If you choose the **E-mail** forwarding method, enter the IP address in the Email Address field. If you choose the **Trap** method, enter the trap receiver IP address in the Address field and specify the port number.

You can either enter an IPv4 or IPv6 addresses or DNS server name in the Address field.

- g) In the **Fabric** field, choose all groups or specific fabric for notification. For SAN Installer, select **VSAN Scope**. You can either choose **All** or **List** option. If you select List, provide the list of VSANs for notification.
- h) In the Source field, select Nexus Dashboard Fabric Controller or **Syslog**.
  - If you select Nexus Dashboard Fabric Controller, then:
    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.
    3. From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
    4. Click **Add** to add the notification.
  - If you select Syslog, then:
    1. In the **Facility** list, select the syslog facility.
    2. Specify the syslog **Type**.
    3. In the **Description Regexp** field, specify a description that matches with the event description.
    4. From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
    5. Click **Add** to add the notification.

**Note** The Minimum Severity option is available only if the Event Type is set to **All**.

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
```

i) Click **Add Rule**.

**Step 4** To add rules to the Event Suppression from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

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

You can view, add, modify, and delete suppressor rules from the table. You can create a suppressor rule from the existing event table. Select a given event as the template and invoke the rule dialog window. Event details are automatically ported from the selected event in the event table to the input fields of the rule creation dialog window.

**Note** You cannot suppress EMC Call Home events from the Cisco Nexus Dashboard Fabric Controller Web UI.

- a) Specify the **Name** for the rule.
- b) Select the required **Scope** for the rule that is based on the event source.

In the **Scope** drop-down list, the LAN groups and the port groups are listed separately. You can choose **SAN/LAN, Port Groups** or **Any**. 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 suppressor rule is applied globally.

- c) Enter the **Facility** name or choose from the SAN/LAN Switch Event Facility List.

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

- d) From the drop-down list, select 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** box and select a valid time range during which the event is suppressed.

By default, the time range is not enabled, i.e., the rule is always active.

**Note** In general, you must not suppress accounting events. Suppressor rule for Accounting events can be created only for certain rare situations where Accounting events are generated by actions of Nexus Dashboard Fabric Controller or switch software. For example, lots of '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 the Suppressor table and invoke the Add Event Suppressor Rule dialog window.

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 <b>Delete</b> 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.

