Events and Audit Logs

About Events

Note For detailed reference information about faults, events, errors, and system messages, see the *Cisco ACI System Messages Reference Guide* or the *Cisco APIC Management Information Model Reference*, which is a web-based application.

The Application Policy Infrastructure Controller (APIC) maintains a comprehensive, up-to-date run-time representation of the administrative and operational state of the Cisco Application Centric Infrastructure (ACI) fabric system in a collection of managed objects (MOs). Any configuration or state change in any MO is considered an event. Most events are part of the normal workflow and there is no need to record their occurrence or to bring them to the attention of the user unless they meet one of the following criteria:

- The event is defined in the model as requiring notification.
- The event follows a user action that is required to be auditable.

Event Objects and Logs

In the *Cisco APIC Management Information Model Reference*, the **event** package contains general event-related object classes, although some event types are found in other packages.

A loggable event is represented by an event record object, which is an immutable, stateless, and persistent MO created by the system to record the occurrence of a specific set of conditions at a given point in time. Although an event record MO is usually triggered by conditions in another MO, it is not contained by that MO but is contained in an event log.

Each new event record MO is added to one of three separate event logs, depending on the cause of the event:

- Audit log—Holds objects that are records of user-initiated events such as logins and logouts (`aaa:SessionLR`) or configuration changes (`aaa:ModLR`) that are required to be auditable.

- Health score log—Holds records of changes in the health score (`health:Record`) of the system or components.
- Event log—Holds records of other system-generated events (`event:Record`) such as link state transitions.

Each log collects and retains event records. An event MO remains in the log until it is purged when the log reaches capacity and space is needed for new event records. The retention and purge behavior for each log is specified in a record retention policy (`event:ARetP`) object associated with each log.

The creation of an event record object can also trigger the export of record details to an external destination by syslog, SNMP trap, or other methods.

Event Properties

The system provides detailed information about each event object. This table describes the event properties:

Property	Description
code	The event code.
id	The unique identifier assigned to the event.
affected	The MO associated with the event.
cause	The probable cause category (for example, transition).
trigger	The generating activity for the event (for example, user, operation, or session).
severity	The severity level of the event. Events are of severity level 'info.'
created	The day and time when the event occurred.
descr	The description of the event.

Event Life Cycle

APIC event MOs are stateless. An event MO created by the APIC is never modified or cleared. An event MO is deleted by the rotation of the event log as newer events are added and log space is needed.

Event Descriptions

The *Cisco APIC Management Information Model Reference*, a Web-based application, contains a list of events with descriptions and attributes. In the **Navigation** frame of the application, select the **Events** tab to view the event list.

This example shows an event description from the *Cisco APIC Management Information Model Reference*:

```
Event ifc:policymgr:user|creation||aaa:User|User $name$ created

Rule ID:7475

Raised on MO: aaa:User
Name: user_creation__aaa_User_User__name__created
Code: E4201779
Cause: transition
```

```
Severity: info
Trigger: USER
Message: User name created

Triggered By:
```

Viewing Events

Viewing Events Using the GUI

Logged events are presented in many places in the GUI, filtered to show only those events relevant to the current GUI context. Wherever a **History** tab appears in the GUI **Work** pane, you can view the relevant log entries from the event log, health log, or audit log. This procedure shows how to view Authentication, Authorization, and Accounting (AAA) events as an example.

Procedure

Step 1 In the menu bar, click **Admin**.

Step 2 In the submenu bar, click **AAA**.

Step 3 In the **Navigation** pane, choose **AAA Authentication**.

Step 4 In the **Work** pane, click the **History** tab.

Step 5 Under the **History** tab, click the **Events** subtab to view the event log.

Step 6 Under the **History** tab, click the **Audit Log** subtab to view the audit log.

Step 7 Double-click a log entry to view additional details about the event.

Viewing Events Using the API

In the *Cisco APIC Management Information Model Reference*, the **event** package contains the event-related object classes except for audit log classes, which are contained in the **aaa** package.

You can view events using the API query methods to search for specific system event MOs (`event:Record`) or audit log event MOs (`aaa:ModLR`). Every event MO contains a property (`affected`) that shows the DN of the affected MO.

This example shows how to view a Tenant object and the associated audit logs. The query asks for the audit logs for tenant 't6' and the response shows the log entry for creation of the tenant.

```
GET http://192.0.20.123/api/node/mo/uni/tn-t6.xml?rsp-subtree-include=audit-logs

RESPONSE:
<fvTenant
.
. [PROPERTIES TRUNCATED FOR READABILITY]
.
>
   <aaaModLR
     affected="uni/tn-t6"
```

```
    cause="transition"
    changeSet="name:t6"
    childAction=""
    code="E4206326"
    created="2014-07-24T03:01:54.440+00:00"
    descr="Tenant t6 created"
    id="4294968636"
    ind="creation"
    modTs="never"
    rn="mod-4294968636"
    severity="info"
    status=""
    trig="config"
    txId="576460752303423731"
    user="admin"/>
</fvTenant>
```

This example shows how to request all event logs associated to a tunnel interface object:

```
GET http://192.0.20.123/api/node/mo/topology/pod-1/node-1019/sys/tunnel-[tunnel7].xml
?rsp-subtree-include=event-logs
```

For detailed information about configuring the APIC REST API, see the *Cisco APIC REST API Configuration Guide*.

External Reporting of Events

The APIC can report events asynchronously to external systems through the following mechanisms:

- Syslog

Note Beginning with Cisco ACI 3.1(1) release, an enhancement is introduced to add the time accuracy by including the sub-second information in the timestamp field of the Syslog messages.

For example, the **Creation Time** now includes the milliseconds information, for example, (.817) in the Syslog output.

```
Here is an example:

Severity        : info
Affected Object : topology/pod-1/node-101/sys/hsrp/inst-default
Code            : E4210476
ID              : 4294970360
Cause           : admin-state-change
Description     : HSRP instance is administratively Enabled
Creation Time   : 2017-09-13T10:17:11.817-07:00
```

- Cisco Call Home
- API subscriptions
- SNMP
    - Beginning with Cisco APIC Release 1.2(1), the APIC controller supports SNMP for APIC-related events.

- SNMP messages for ACI leaf and spine switches are sent by the switches themselves, but APIC can configure SNMP trap destinations for SNMP traps sent by ACI switches.
- For a list of SNMP MIBs and traps supported by ACI, see the *Cisco ACI MIB Support List*.

For information on configuring external reporting, see the following documents:

- *Cisco APIC Troubleshooting Guide*
- *Cisco APIC REST API Configuration Guide*

Changing the Severity or Squelching an Event

Every APIC event has a default severity. In some circumstances, an event might be considered more or less severe than the default level. In some cases, you might want to ignore a particular event and squelch (suppress) it from appearing in event reports or status dashboards. APIC provides two locations from which you can change the severity of an event type:

- In a monitoring policy (beginning with Cisco APIC Release 3.2(1))
- Directly from the **Events** tab under a component in the APIC GUI (beginning with Cisco APIC Release 4.2(1))

Note When you change the severity or choose to ignore an event type, the change applies only to newly created events. Existing event records are not affected.

Changing Event Severity or Squelching an Event from the Events Tab

In the **Events** tab of an APIC GUI component, you can change the severity of a displayed event or you can suppress (squelch) it altogether.

Note The option to directly change the severity or squelch an event from a component **Events** tab was introduced in Cisco APIC Release 4.2(1).

Tip For squelching an event, we recommend using this procedure instead of the procedure described in Changing Event Severity or Squelching an Event in the Monitoring Policy, on page 6. This simple procedure eliminates the need to look up the event code or the relevant monitoring policy. We do recommend, however, that you remember which monitoring policy (by default, Tenant common, Fabric, or Access Monitoring default) is modified by the operation in case you want to unsquelch the event type at a later time. The affected monitoring policy is displayed when you select the **Ignore Event** action.

Procedure

Step 1 Navigate to the **Events** tab that currently displays an instance of the event.

Step 2 Choose one of the following actions:

- To change the severity of these events, right-click the row of the desired event code, select **Change Severity**, select the desired severity level, and click **Change Severity**.
- To prevent these events from appearing in event reports (squelching the event), right-click the row of the desired event code, select **Ignore Event**, then click **Ignore Event**.

With either of these actions, a dialog box appears in which you can confirm the selected action. In both cases, the dialog box displays the path to the **Affected Monitoring Policy**, which will be automatically modified as a result of the action. To undo the action later, you can navigate to this policy and manually modify it as described in Changing Event Severity or Squelching an Event in the Monitoring Policy, on page 6.

This change will be applied for all future events with this event code that occur as a result of the displayed **Affected Monitoring Policy**.

What to do next

When you squelch an event code, a squelch policy is automatically created and added to a monitoring policy. If you want the future event instances to appear again, you must locate and delete that squelch policy. Depending on the `monPolDn` property of the parent MO, the auto-created event squelch policy can be stored in the **Event Severity Assignment Policies** under one of the following:

- **Tenants > common > Policies > Monitoring > default**
- **Fabric > Access Policies > Policies > Monitoring > default**
- **Fabric > Fabric Policies > Policies > Monitoring > default**
- **Fabric > Fabric Policies > Policies > Monitoring > Common Policy**

If you have created and applied a non-default monitoring policy (not one of the four default policies mentioned above) to the parent MO that has the event code, you must access that non-default monitoring policy when you want to undo the squelch policy.

When you have located the squelch policy, follow the procedure in Changing Event Severity or Squelching an Event in the Monitoring Policy, on page 6 to delete the entry for the event code or change the severity to a setting other than **squelched**.

Changing Event Severity or Squelching an Event in the Monitoring Policy

You can change the severity of an event type or suppress (squelch) it altogether by modifying the **Event Severity Assignment Policies** in the monitoring policy.

Note The option to directly change the severity or squelch an event from a monitoring policy was introduced in Cisco APIC Release 3.2(1).

Procedure

Step 1 Navigate to the monitoring policy that is affected by the event.

Step 2 Expand the monitoring policy and select **Event Severity Assignment Policies**.

Step 3 From the **Monitoring Object** drop-down list, select the object that contains the event to be changed.

If the desired object does not appear in the list, follow these steps:

a) Click the pencil icon next to the list.
b) Check the box for the desired object.
c) Click **Submit** to add the object to the **Monitoring Object** list.

Step 4 In the task bar at the top of the policy table, click the + sign.

A form row appears in the table.

Step 5 Select the desired event code in the **Code** drop-down list.

Step 6 Select the desired severity level in the **Severity** drop-down list.

To prevent the event from appearing in event reports, select **squelched**.

Step 7 (Optional) To make a notation about the change, you can add a comment in the **Description** text box.