CHAPTER 3

Viewing Events in EventVision

The events are displayed in an Events List log for each tab. These tabs reflect the different event categories and display event information related to the specific event category. The following tabs may be selected in the EventVision window:

- All Tab
- Audit Tab
- Provisioning Tab
- Security Tab
- Service Tab
- Syslog Tab
- System Tab
- Ticket Tab
- V1 Trap Tab
- V2 Trap Tab

The events are sorted according to date, where the latest event is displayed first and the oldest event is displayed last. You can define the filter to be used as well as the number of events to be displayed in the Events List using the EventVision Options dialog box. For more information see Setting EventVision Viewing Options, page 2-5.

The navigation toolbar enables you to navigate through all the EventVision log record pages.

Each page of the Events List displays the selected amount of events per page as defined in the EventVision Options dialog box. See Setting EventVision Viewing Options, page 2-5. You can use the **Go To** sub-menu options on the View menu or the respective toolbar buttons on the toolbar, to navigate between each displayed page.

All Tab

When you launch EventVision, the **All** tab is not displayed.

You can open this tab, as required, using the **Open All Tab** option on the File menu.

Note Opening the **All** tab may take some time to retrieve information from the Cisco ANA database for all category events.

The **All** tab displays information about all the events. Additional information specific to the event category can be viewed in the Events Properties dialog box or individual category tabs.

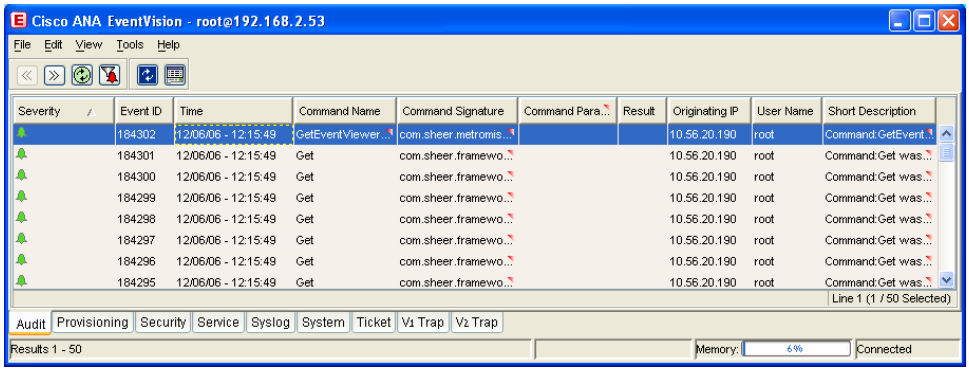
The following columns are displayed in the **All** tab:

- **Severity**—The severity of the ticket.
- **Event ID—**The sequential ID number of the event.
- **Short Description—**A description of the event, for example, device unreachable.
- **Time—**The date and time when the event occurred. The time is displayed in the following format MM/DD/YY HH:MM:SS.
- **Event Type—**The event type, namely, audit, system, ticket, provisioning, syslog, security, service, and traps.

Audit Tab

The **Audit** tab displays all the events generated for each command or request in Cisco ANA, for example, opening EventVision displays the following "GetEvent" in the Audit List:

Figure 3-1 Audit Tab



The following information is displayed in the **Audit** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the event (generated by Cisco ANA).
- **Time—**Logged and recorded at the time the event happened.
- **Command Name—**The audit specific command name, prefaced by, for example, Get…, Update…, Find…
- **Command Signature—**The actual command run by Cisco ANA, such as com.sheer.framework.
- **Command Parameter—**This parameter is currently unavailable in this version.
- **Result—**This parameter is currently unavailable in this version.
- **Originating IP—**The IP address of the client that issued the command.
- **User Name—**The name of the user who initiated the command.
- **Short Description—**An aggregation of portions of the same fields in the Audit Command fields.

The type of information displayed in the **Audit** tab can be audited by defining the appropriate registry keys and their values. The audit service enables you to audit all the commands executed in the system, for example, the Get command can be audited. The **Audit** tab then displays this information.

The following parameters can be controlled through the registry :

- Override the default auditing details level
- All or specific users
- Display only specific commands

The available values for these parameters are:

- **Concise—**Displays all (default) events besides the Command Parameters and Result column values.
- **Disable—**The commands will not be logged in the **Audit** tab events list.

For more information about the Registry Editor, refer to the *Cisco Active Network Abstraction Registry Editor Guide*.

Provisioning Tab

Events displayed in the **Provisioning** tab are events triggered during the configuration of a device. Cisco ANA sends an event explaining the configuration operation, for example, to configure the cross connect table in a device. The **Provisioning** tab displays detailed information specific to this event category. It contains events both from the Cisco ANA Command Builder and Cisco ANA Workflow Editor. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Provisioning** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the event.
- **Short Description—**A description of the event, for example, Script Show has failed.
- **User Name—**The name of the user who performed the provisioning operation.
- **Time—**Logged and recorded at the time the event happened.
- **Status—**The status, for example, success or fail.
- **Source—**The VNE key on which the provisioning operation succeeded or failed.

Security Tab

The **Security** tab displays detailed information specific to this event category. Security events are related to client login and user activity when managing the system and the environment. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Security** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the event.

- **Short Description—**A description of the event, for example, Successful login by root.
- **Location—**The entity that triggered the event, as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the event happened.
- **Client IP**—The IP address of the client where the event was triggered.
- **User Name**—The user name of the client where the event was triggered.
- **Client Type**—The type of client, namely, NetworkVision, EventVision, Cisco ANA Manage or Unknown (for example,BQL, Registry Editor and so on).
- **Auto Cleared**—Indicates whether the alarm is cleared automatically. The alarm is cleared when it is correlated to an alarm which has been cleared. If the alarm is cleared automatically it is defined as true.

Service Tab

The **Service** tab displays all the alarms generated by Cisco ANA, for example, link down. Service events are related to the alarms that are generated by the Cisco ANA system. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Service** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event, for example, Route entry restored.
- **Location—**The entity that triggered the alarm, as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the event happened.

Syslog Tab

The **Syslog** tab displays all the syslog events. These events are related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **Syslog** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the alarm, for example, Device configuration changed.
- **Location—**The entity that triggered the alarm, as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the alarm happened.

System Tab

The **System** tab displays all the system events related to the everyday working of the internal system and its components. These events may be related to the Cisco ANA and Cisco ANA Gateway resources, representing the system log. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **System** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Event ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event, for example, Dropped Events Report.
- **Location—**The entity that triggered the event.
- **Time—**Logged and recorded at the time the event happened.

Ticket Tab

The **Ticket** tab displays detailed information specific to this event category. A **ticket** event contains a single root alarm (the root-cause alarm can be of any alarm type, for example, syslog, service and so on), and all its subsequent correlated alarms. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The maximum number of open tickets (other tickets can be correlated to them) for the system is 5000.

This number is configurable in the registry, however we do not recommend increasing it.

Note Changes to the registry should only be carried out with the support of Cisco Professional Services.

A "`tickets capacity overflow, red threshold reached`" system alarm is generated when this number is exceeded. The alarm severity is defined as critical.

The following additional information is displayed in the **Ticket** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Ticket ID—**The sequential ID number of the ticket.
- **Short Description—**A description of the event, for example, Link Down.
- **Location—**The entity that triggered the ticket, as a hyperlink that opens the relevant location.
- **Last Modification Time—**The date and time when the ticket was last modified.
- **Time—**Logged and recorded at the time the first event happened.
- **Acknowledged—**The status of the ticket that is being handled, namely, true (acknowledged) or false (not acknowledged).
- **Affected Devices Count—**The number of devices affected by the ticket (the source(s) of the alarm and their subsequent alarms).

- **Correlation Count—**Displays the number of correlated alarms included in the ticket. For example, if in the **Correlation** tab of the Ticket Properties, there are 3 alarms correlated to the root-cause alarm, then the counter displays the number 3. If there are 2 alarms correlated to the root-cause alarm, and each alarm in turn has 2 alarms correlated to it, then the counter displays the number 4.
- **Reduction Count—**Displays the number of alarms included in the ticket. For example, nine alarms can be viewed in the **History** tab of the Ticket Properties window, but only a single ticket is displayed in the Ticket pane.
- **Duplication Count—**Displays the number of occurrences of the original root-cause alarm included in the ticket. For example, if the ticket was created by a link down root-cause alarm, and then the link goes up and down again quickly so that it is included in the same ticket, then the duplication counter displays the number 2, as the root-cause alarm occurred twice.

For information about viewing ticket properties, see Ticket Tab Properties, page 4-2.

V1 Trap Tab

This event is triggered when the network element sends a trap message to Cisco ANA because of a network event, for example, Link Down. The **V1 Trap** tab displays detailed information specific to this event category. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional is displayed in the **V1 Trap** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event, for example, enterprise generic trap.
- **Time—**Logged and recorded at the time the event happened.
- **Location—**The entity that triggered the trap, as a hyperlink that opens the relevant location.

V2 Trap Tab

The **V2 Trap** tab displays detailed information specific to this event category. Additional information specific to this event category can be viewed in the Events Properties dialog box.

The following additional information is displayed in the **V2 Trap** tab:

- **Severity—**Displays an icon of a bell, which is colored according to the severity of the alarm on the event (the color and type of alarm is displayed in the Properties pane's **Severity** field). See Color Coding of Events List Severity Icons, page 2-4.
- **Alarm ID—**The sequential ID number of the alarm.
- **Short Description—**A description of the event.
- **Location—**The entity that triggered the trap, such as a hyperlink that opens the relevant location.
- **Time—**Logged and recorded at the time the event happened.