



CHAPTER 11

Generating Reports

Overview

You can configure the Cisco Security Agent to log an event each time a system action triggers a rule.

You can use the event logging data received from agents to generate reports that indicate overall network health. Using these reports, you can monitor how your current rule sets are working and adjust them, if necessary.

You can also generate reports related to configuration information.

This section contains the following topics.

- [Types of Reports, page 11-2](#)
- [Viewing Reports, page 11-2](#)
- [Generating Reports, page 11-3](#)
- [Events by Severity, page 11-3](#)
- [Events by Group, page 11-5](#)
- [Host Detail, page 11-6](#)
- [Policy Detail, page 11-8](#)
- [Group Detail, page 11-9](#)

Types of Reports

CSA MC lets you generate reports using various criteria. For example, you can create reports based on event severity level, on the group that generated the event, and on the individual host systems producing events. You can sort by other parameters such as time frame, host, and event code that you configure separately.

Viewing Reports

When you generate your reports, you're given the option of selecting the type of viewer through which to display the report. From the Viewer type pulldown menu, you can select the following.

- **PDF:** This option will generate the complete report as a PDF file that can be viewed, printed, and saved using the browser PDF plug-in. If you do not have a PDF plug-in installed on your browser, you will have to install a PDF browser plug-in to view this report type.
- **HTML:** This option breaks the report into individual HTML pages which can be viewed one page at a time in a browser window. Only the currently viewed report page can be printed. (Supported by Internet Explorer 6.0 or higher and FireFox 1.5.0.x or higher.)

When you print reports, the formatting will vary depending on which view type you have selected and the printer settings on the printer you're using.

**Caution**

When you print reports, it is recommended that you print using Landscape mode. Reports do not print correctly using Portrait mode.

**Caution**

CSA MC requires and installs Sun JRE (Java Runtime Environment) to generate reports using the Jasper reporting tool. If you remove the Java directory from the CSA MC system, you cannot generate reports.

Generating Reports

You generate reports by selecting various sorting options in the CSA MC report configuration views. When you are finished selecting sorting parameters, you can generate your report.

Events by Severity

You can generate reports using various selection and sorting criteria. In this case, you are creating a report based on event severity levels.

To generate an Events by Severity report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Severity** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Events by Severity report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** From the pulldown list, select an **Event Filter**. This is an Event Set you create from the Events> Event Sets configuration view (see [Event Sets, page 10-36](#)).
 - Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents (see [Figure 11-1](#)).
 - Step 6** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 7** Select a **Viewer type**, PDF or HTML.
 - Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

Figure 11-1 Events by Severity Report Configuration

The screenshot shows the Management Center for Cisco Security Agents V5.2 interface in a Microsoft Internet Explorer browser. The address bar shows the URL: `https://biohazard/csamc52/webadmin`. The page title is "Management Center for Cisco Security Agents V5.2". The navigation menu includes "Events", "Systems", "Configuration", "Analysis", "Maintenance", "Reports", and "Search Help". The current page is "Reports" > "Events by Severity" > "IIS Events by severity".

The configuration form includes the following fields:

- Name:** IIS Events by severity
- Description:** IIS Events by severity report
- Criteria:**
 - Event Filter: IIS events critical and emergency [New|View]
 - Sort by: Time [Ascending]
 - Filter out similar events: Yes
 - Viewer type: HTML Frame

At the bottom of the form, there are buttons for "Save", "View report", and "Delete". A status bar indicates "17 rule changes pending" and a "Generate rules" button. The user is logged in as "admin".

191591

Events by Group

You can generate reports using various selection and sorting criteria. In this case, you are creating a report based on the groups that have generated the events.

To generate an Events by Group report, do the following.

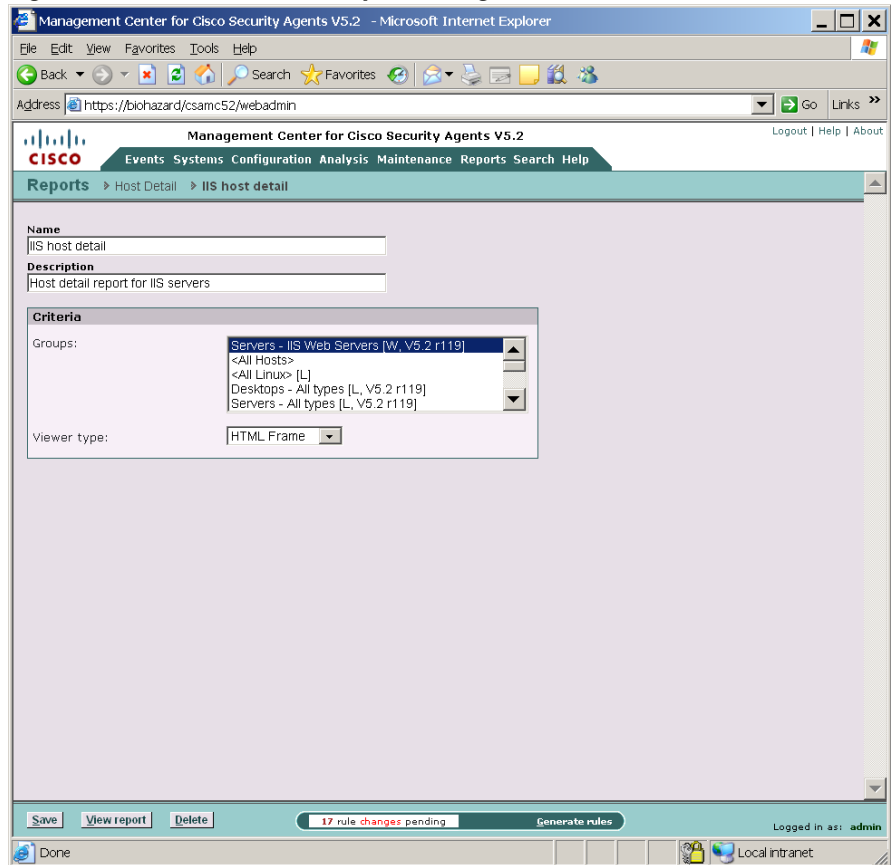
-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Group** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Events by Group report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** From the pulldown list, select an **Event Filter**. This is an Event Set you create from the Events> Event Sets configuration view (see [Event Sets, page 10-36](#)).
 - Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents.
 - Step 6** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 7** Select a **Viewer type**, PDF or HTML.
 - Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 9** Click the **View Report** button and the report is automatically displayed in a new window.

Host Detail

You can generate reports based on hosts in specific groups you select as part of the report. A host detail report provides in-depth information on the hosts in the groups you select for the report.

To generate a host detail report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Host Detail** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Host Detail report configuration view (see [Figure 11-2](#)), enter a **Name** and a **Description** for the report.
 - Step 4** Select the **Groups** for which you want to generate a report. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the **Ctrl** key when you click on the item in question. Press the **Shift** key to select multiple successive items. You can also select **All Hosts** here to generate a report for all registered hosts.
 - Step 5** Select a **Viewer type**, PDF or HTML.
 - Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 7** Click the **View Report** button and the report is automatically displayed in a new browser window.

Figure 11-2 Host Detail Report Configuration

191592

Policy Detail

You can generate reports by selected policies. A policy report provides in-depth information on the policies you select for the report.

To generate a policy detail report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar and select **Policy Detail** from the drop-down list that appears.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Policy Detail report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** Select the **Policies** for which you want to generate a report. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the **Ctrl** key when you click on the item in question. Press and hold the **Shift** key to select multiple successive items.
 - Step 5** Select a **Viewer type**, PDF or HTML.
 - Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 7** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Group Detail

You can generate reports by a selected group or groups. A group report provides in-depth information on the groups you select for the report.

To generate a group detail report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar and select **Group Detail** from the drop-down list that appears.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Group Detail report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** Select the **Groups** for which you want to generate a report. To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the **Ctrl** key when you click on the item in question. Press and hold the **Shift** key to select multiple successive items.
 - Step 5** Select a **Viewer type**, PDF or HTML.
 - Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 7** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

