Response Automation for System Events

This chapter describes how to configure the Embedded Event Manager (EEM).

- About the EEM, on page 1
- Guidelines for the EEM, on page 2
- Configure the EEM, on page 3
- Monitoring the EEM, on page 6
- History for the EEM, on page 6

About the EEM

The EEM service enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions.

Supported Events

The EEM supports the following events:

- Syslog—The ASA uses syslog message IDs to identify syslog messages that trigger an event manager applet. You may configure multiple syslog events, but the syslog message IDs may not overlap within a single event manager applet.
- Timers—You may use timers to trigger events. You may configure each timer only once for each event manager applet. Each event manager applet may have up to three timers. The three types of timers are the following:
  - Watchdog (periodic) timers trigger an event manager applet after the specified time period following the completion of the applet actions and restart automatically.
  - Countdown (one-shot) timers trigger an event manager applet once after the specified time period and do not restart unless they are removed, then re-added.
  - Absolute (once-a-day) timers cause an event to occur once a day at a specified time, and restart automatically. The time-of-day format is in hh:mm:ss.

    You may configure only one timer event of each type for each event manager applet.

- None—The none event is triggered when you run an event manager applet manually using the CLI or ASDM.
- Crash—The crash event is triggered when the ASA crashes. Regardless of the value of the **output** command, the **action** commands are directed to the crashinfo file. The output is generated before the **show tech** command.

Actions on Event Manager Applets

When an event manager applet is triggered, the actions on the event manager applet are performed. Each action has a number that is used to specify the sequence of the actions. The sequence number must be unique within an event manager applet. You may configure multiple actions for an event manager applet. The commands are typical CLI commands, such as **show blocks**.

Output Destinations

You may send the output from the actions to a specified location using the **output** command. Only one output value may be enabled at any one time. The default value is **output none**. This value discards any output from the **action** commands. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled. You may send the output of the **action** CLI commands to one of three locations:

- **None**, which is the default and discards the output
- **Console**, which sends the output to the ASA console
- **File**, which sends the output to a file. The following four file options are available:
  - **Create a unique file**, which creates a new, uniquely named file each time that an event manager applet is invoked
  - **Create/overwrite a file**, which overwrites a specified file each time that an event manager applet is invoked.
  - **Create/append to a file**, which appends to a specified file each time that an event manager applet is invoked. If the file does not yet exist, it is created.
  - **Create a set of files**, which creates a set of uniquely named files that are rotated each time that an event manager applet is invoked.

Guidelines for the EEM

This section describes guidelines and limitations that you should check before configuring the EEM.

Context Mode Guidelines

Not supported in multiple context mode.

Additional Guidelines

- During a crash, the state of the ASA is generally unknown. Some commands may not be safe to run during this condition.
- The name of an event manager applet may not contain spaces.
- You cannot modify the None event and Crashinfo event parameters.
- Performance may be affected because syslog messages are sent to the EEM for processing.
- The default output is **output none** for each event manager applet. To change this setting, you must enter a different output value.
- You may have only one output option defined for each event manager applet.

Configure the EEM

Configuring the EEM consists of the following tasks:

Procedure

Step 1 Create an Event Manager Applet and Configure Events, on page 3.
Step 2 Configure an Action and Destinations for Output from an Action, on page 4.
Step 3 Run an Event Manager Applet, on page 5.
Step 4 Track Memory Allocation and Memory Usage, on page 5.

Create an Event Manager Applet and Configure Events

To create an event manager applet and configure events, perform the following steps:

Procedure

Step 1 In ASDM, choose **Configuration** > **Device Management** > **Advanced** > **Embedded Event Manager**.
Step 2 Click **Add** to display the **Add Event Manager Applet** dialog box.
Step 3 Enter the name of the applet (without spaces) and describe what it does. The description may be up to 256 characters long. You may include spaces in description text if it is placed within quotes.
Step 4 Click **Add** in the **Events** area to display the **Add Event Manager Applet Event** dialog box.
Step 5 Choose the event type that you want to configure from the **Type** drop-down list. The available options are **crashinfo**, **None**, **Syslog**, **Once-a-day timer**, **One-shot timer**, and **Periodic** timer.

- **Syslog**: Enter a single syslog message or a range of syslog messages. If a syslog message occurs that matches the specified individual syslog message or range of syslog messages, an event manager applet is triggered. (Optional) Enter the number of times in the **occurrences** field that the syslog message must occur for an event manager applet to be invoked. The default is 1 occurrence every 0 seconds. Valid values are from 1 - 4294967295. (Optional) Enter the number of seconds in the **period** field within which

the syslog messages must occur to invoke the action. This value limits how frequently an event manager applet is invoked to at most once in the configured period. Valid values are from 0 - 604800. A value of 0 means that no period is defined.

- **Periodic**: Enter the time period in seconds. The number of seconds may range from 1- 604800.
- **Once-a-day timer**: Enter the time of day in hh:mm:ss. The time range is from 00:00:00 (midnight) to 23:59:59.
- **One-shot timer**: Enter the time period in seconds. The number of seconds may range from 1- 604800.
- **None**: Choose this option to invoke an event manager applet manually.
- **crashinfo**: Choose this option to trigger a crash event when the ASA crashes.

Configure an Action and Destinations for Output from an Action

To configure an action and specific destinations for sending output from an action, perform the following steps:

Procedure

Step 1 Click **Add** to display the **Add Event Manager Applet** dialog box.

Step 2 Enter the name of the applet (without spaces) and describe what it does. The description may be up to 256 characters long.

Step 3 Click **Add** in the **Actions** area to display the **Add Event Manager Applet Action** dialog box.

Step 4 Enter the unique sequence number in the **Sequence #** field. Valid sequence numbers range from 0 - 4294967295.

Step 5 Enter the CLI command in the **CLI Command** field. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled.

Step 6 Click **OK** to close the **Add Event Manager Applet Action** dialog box.

The newly added action appears in the **Actions** list.

Step 7 Click **Add** to open the **Add Event Manager Applet** dialog box.

Step 8 Choose one of the available output destination options:

- Choose the **None** option from the **Output Location** drop-down list to discard any output from the **action** commands. This is the default setting.
- Choose the **Console** option from the **Output Location** drop-down list to sends the output of the **action** commands to the console.

  Note Running this command affects performance.

- Choose the **File** option from the **Output Location** drop-down list to send the output of the **action** commands to a new file for each event manager applet that is invoked. The **Create a unique file** option is automatically selected as the default.

  The filename has the format of eem-*applet-timestamp*.log, in which *applet* is the name of the event manager applet and *timestamp* is a dated time stamp in the format of YYYYMMDD-hhmmss.

- Choose the **File** option from the **Output Location** drop-down list, then choose the **Create a set of files** option from the drop-down list to create a set of rotated files.

  When a new file is to be written, the oldest file is deleted, and all subsequent files are renumbered before the first file is written. The newest file is indicated by 0, and the oldest file is indicated by the highest number. Valid values for the rotate value range from 2 - 100. The filename format is eem-*applet*-*x*.log, in which *applet* is the name of the applet, and *x* is the file number.

- Choose the **File** option from the **Output Location** drop-down list, then choose the **Create/overwrite a file option** from the drop-down list to write the **action** command output to a single file, which is overwritten every time.

- Choose the **FileFile** option from the **Output Location** drop-down list, then choose the **Create/append a file** option from the drop-down list to writes the **action** command output to a single file, but that file is appended to every time.

Step 9 Click **OK** to close the **Add Event Manager Applet** dialog box.

The specified output destination appears in the **Embedded Event Manager** pane.

Run an Event Manager Applet

To run an event manager applet, perform the following steps:

Procedure

Step 1 In the **Embedded Event Manager** pane, select an event manager applet from the list that has been configured with the **None** event.

Step 2 Click **Run**.

Track Memory Allocation and Memory Usage

To log memory allocation and memory usage, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Advanced** > **Embedded Event Manager**.

Step 2 Click **Add** to display the **Add Event Manager Applet** dialog box.

Step 3 Click **Add** again to display the **Add Event Manager Applet Event** dialog box.

Step 4 Choose **memory-logging-wrap** from the drop-down list.

Step 5 Click **OK** to add it to the **Events** list.

Step 6 Click **OK** again to add it to the **Applets** list.

Monitoring the EEM

See the following commands to monitor the EEM.

- **Monitoring > Properties > EEM Applets**

  This pane shows the list of EEM applets and their hit count value.

- **Tools > Command Line Interface**

  This pane allows you to issue various non-interactive commands and view results.

History for the EEM

Table 1: History for the EEM

Feature Name	Platform Releases	Description
Embedded Event Manager (EEM)	9.2(1)	The EEM service enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions. We introduced the following screens: **Configuration > Device Management > Advanced > Embedded Event Manager, Monitoring > Properties > EEM Applets**.
Memory tracking for the EEM	9.4(1)	We have added a new debugging feature to log memory allocations and memory usage, and to respond to memory logging wrap events. We modified the following screen: **Configuration > Device Management > Advanced > Embedded Event Manager > Add Event Manager Applet > Add Event Manager Applet Event**.