Chapter 8

Configuring the SNMP Traps with the SRC CLI

This chapter describes how to use the SRC CLI to configure traps with the Simple Network Management Protocol (SNMP) agent. You can use the CLI to configure traps on a Solaris platform or on a C-series platform.

You can also use configuration applications to configure traps on a Solaris platform. See *Chapter 9, Configuring the SNMP Traps on a Solaris Platform*.

Topics in this chapter include:

Overview of SNMP Traps

The SNMP agent provides network management systems with SNMP trap notifications in case of component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB).

The SNMP agent can be run on each SRC host. It can monitor any SRC process running on the host and is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components.

MIBs

The SNMP agent monitors MIB variables. Most variables measure the performance of the system. Some variables are counters, such as the saeLogins variable, which counts the total number of subscriber logins since startup. Some variables are gauges, and their numbers go up and down, such as the saeHeapUsed variable, which measures the Java Virtual Machine heap that is currently in use.

A MIB defines a trap type that is associated with many MIB variables. For traps based on counters, the SNMP agent periodically polls each specified variable. It takes the difference between the previous and current values of the variable and compares that difference with the threshold. If the difference has moved up across thresholds, the SNMP agent sends a trap raising an alarm (minor, major, or critical) for the highest threshold crossed to all configured receivers. If the difference has moved down across thresholds, the agent sends a trap clearing the alarm of the lowest threshold crossed.

You can configure the polling interval between samples. If you change the polling interval, also adjust the thresholds. For instance, if the critical threshold for SAE logins is 1,000 and the interval is 60 seconds, then a critical alarm is raised if there are more than 1,000 logins in 60 seconds. But if you change the interval to 600 seconds, then you would need to change the threshold to 10,000 to have the same meaning.

For traps based on gauges, the previous value is not needed; the current value is compared with the thresholds.

In the trap tables, there is a field named R/AV, where R means rate, and AV means absolute value. Rate is used for variables that are counters, and it measures the rate of change of the counter. Absolute value is used for variables that are gauges.

For a list of all traps, see *Chapter 10, Understanding Traps*.

Traps

Traps are individual events that the SNMP agent can monitor, such as the number of timeouts or errors that have occurred or connections that have opened or closed. There are two types of traps:

- Performance traps—Traps that poll MIB variables associated with the trap to determine whether a variable has crossed configured thresholds. If the variable crosses a threshold, an alarm is triggered and a trap is sent to the list of configured receivers.

- Event traps—Traps that are sent when an event occurs; for example, when a connection is established or closed.

For a list and description of all traps, see *Chapter 10, Understanding Traps*.

SNMP Traps and Informs

SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. The standard and enterprise-specific traps are compiled into the network management software. For more information on the SRC traps, see *Chapter 10, Understanding Traps*. For information on system logging severity levels for SNMP traps, see ***Chapter 2, Configuring Logging for SRC Components***.

With traps, the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. With an inform, the receiver acknowledges the message with a response. For information about configuring SNMP notification handling, see *SRC-PE Getting Started Guide, Chapter 23, Configuring and Starting the SNMP Agent with the SRC CLI*.

Configuration Statements for the SNMP Traps

Use the following configuration statements to configure the SNMP traps at the [edit] hierarchy level.

snmp notify alarm category *category-name* ...

```
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
    minor minor;
}
```

snmp notify event category *category-name* ...

snmp notify event category *category-name* event *event-name* ...

For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring Performance Traps

Use the following configuration statements to configure performance traps:

snmp notify alarm category *category-name* ...

```
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
    minor minor;
}
```

To configure performance traps:

1. From configuration mode, access the configuration statement that configures the type of performance trap.

   ```
   [edit]
   user@host# edit snmp notify
   ```

2. Specify the type of trap and the trap name.

   ```
   [edit snmp notify]
   user@host# set alarm category category-name alarm alarm-name
   ```

   You can select from the list of trap types and their associated traps or create new traps.

3. (Optional) Specify the interval at which the variable associated with the trap is polled.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set interval interval
   ```

4. Specify the threshold above which a critical alarm is generated.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set critical critical
   ```

5. Specify the threshold above which a major alarm is generated.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set major major
   ```

6. Specify the threshold above which a minor alarm is generated.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set minor minor
   ```

Configuring Event Traps

Use the following configuration statements to configure event traps:

snmp notify event category *category-name* ...

snmp notify event category *category-name* event *event-name* ...

To configure event traps:

1. From configuration mode, access the configuration statement that configures the type of event trap.

   ```
   [edit]
   user@host# edit snmp notify
   ```

2. Specify the type of trap and the trap name.

   ```
   [edit snmp notify]
   user@host# set event category category-name event event-name
   ```

   You can select from the list of trap types and their associated traps or create new traps.