Chapter 2

Configuring Logging for SRC Components

This chapter describes logging for SRC components and applications. Topics include:

Overview of Logging

SRC components and applications generate event messages that you can save in logs—either by writing the messages to text files or by using the system log (syslog) facilities. You can use these logs to monitor the SRC components and troubleshoot problems. By default, log files are stored in the */var/log* directory.

Each SRC component has its own logging configuration. For example, the license server, the NIC, the SAE, and SNMP each have logging configuration. The C-series platform includes a system log server that you can configure to manage messages generated on that platform.

You can use the CLI to configure logging on a C-series platform or on a Solaris platform and to configure the system log server on a C-series platform. You can also use SRC configuration applications to configure component logging on a Solaris platform. For the SNMP agent, you can also configure logging through the agent's local configuration tool.

Related Information

For additional information, see the following sources:

- *SRC-PE Getting Started Guide, Chapter 14, Configuring System Logging for a C-series Platform*
- The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)

- *SRC-PE Getting Started Guide, Chapter 23, Configuring and Starting the SNMP Agent with the SRC CLI*
- *SRC-PE Getting Started Guide, Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*

Categories and Severity Levels for Event Messages

In the logging configuration, you can specify a filter for each type of log. This filter can include an expression that defines the *categories* and *severity levels* of event messages that the software saves.

Defining Categories

The category of an event message defines the SRC component that generated the event message. If you want to view only event logs in a specific category, you can define a variable <category>, which is a text string that matches the name of a category. This variable is not case sensitive. To view the names of categories for event messages, view a log file for one of the default filters.

For example, the category Cops defines event messages generated by the COPS server. Similarly, the category CopsMsg defines a particular sort of event message that the COPS server generates.

Juniper Networks Customer Service can also provide names of categories, especially for troubleshooting purposes.

Defining Severity Levels

The event filter provides 128 levels of severity numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in Table 4.

CAUTION: Enabling the generation of debug log messages has a negative affect on system performance. Do not enable debug log messages unless you are instructed to do so by Juniper Networks Technical Assistance Center (JTAC).

Table 4: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70
emerg	80

Table 4: Named Severity Levels (continued)

Name	Severity Level
panic	90
logmax	127

You can define a severity level as follows:

- Specify an explicit severity. For example:
  - debug—Defines only debug messages
- Specify a minimum severity and a maximum severity. For example:
  - info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
  - Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:
  - info-—Defines messages of minimum severity level info and maximum severity level logmax
  - -warning—Defines messages of minimum severity level logmin and maximum severity level warning
- Specify no severities to log all event messages.

The syntax for the severity takes the format:

[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]

Use either the name or the number of a severity level shown in Table 4 for the variables in this syntax.

Defining Filters

You specify a filter by defining an expression with the following format:

singlematch [,singlematch]*

- singlematch—[!] (< category > | ([< category >]/[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]))
- !—Do not log matching events
- < category > —See *Defining Categories* on page 8
- [< severity >] | [< minimumSeverity >]-[< maximumSeverity >]—See *Defining Severity Levels* on page 8.

The software filters events by evaluating each subexpression in order from left to right. When the software determines that an event message matches a subexpression, the software logs or ignores the message accordingly. You can specify an unlimited number of subexpressions; however, the order in which you specify the subexpressions affects the result.

Table 5 shows some examples of filters.

Table 5: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
Cops/debug	Debug events from COPS category only
!Cops,/debug	All debug events except those from COPS category
CopsMsg/info-,!CopsMsg,Cops	All messages from COPS category, except those from CopsMsg category with level less than info

Rotation of Log Files

On C-series platforms, log files that contain entries are rotated daily when other daily system tasks run on the system. The system retails 5 log files for a component before overwriting the oldest file.

When a new log file is opened to replace a file from the previous day that contains content, a number (1–4) is appended to the name of the older file. For example, *sae_debug.log.4* would be the oldest file in the rotation, s*ae_debug.log.1* would be the newest file in the rotation; *sae_debug.log* would be the active log file for SAE.

On C-series platforms, the software compresses log files and appends the *.gz* suffix; for example, *sae_debug.log.4.gz*. Log files are stored in the */opt/UMC/component-name/var/log directory*; for example, */opt/UMC/sae/var/log*.

If you are using the SRC software on a Solaris platform, you can use **logadm** on Solaris version 9 or greater, or you can install the log rotate application from the following Web site:

http://www.sunfreeware.com