Chapter 14

Configuring System Logging for a C-series Platform

This chapter describes how to configure the system log server (also called a syslog server) on a C-series platform.Topics include:

Overview of the C-series Platform Log Server

The C-series platform includes a system log server that you can configure to manage messages generated on the system. These messages record events that occur to system processes and components.

You can configure the system log server on a C-series platform to send messages about events to:

- A local file
- Other hosts that are running a system log server
- Users who need to be notified about particular error conditions

You configure which groups of messages are to be forwarded by message type and severity level.

Message Groups

Message groups (also called facilities) define sets of messages generated by the same software process or concerned with a similar condition or activity (such as authentication attempts).

You can configure the following message groups for the system log server:

- any—Messages from all facilities.
- authorization—Authentication and authorization attempts.
- daemon—Actions performed or errors encountered by various system processes.
- ftp—Actions performed or errors encountered by an FTP process.
- kernel—Actions performed or errors encountered by the kernel.
- user—Actions performed or errors encountered by various user processes.
- local7—Actions performed or errors encountered by different SRC processes.

Severity Levels

You can specify the following severity levels for groups of messages to be forwarded:

- any—Messages for all severity levels.
- emergency—System panic or other condition that causes the system to stop functioning.
- alert—Conditions that require immediate correction.
- critical—Critical conditions, such as hard drive errors.
- error—Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- warning— Conditions that warrant monitoring.
- notice—Conditions that are not errors but might warrant special handling.
- info—Events or nonerror conditions of interest.
- none—Messages are not generated for any condition.

Before You Configure System Logging

Before you configure the syslog server on a C-series platform, you should be familiar with:

- The syslog protocol
- Logging for SRC components

  See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SRC Components*.

Configuration Statements for System Logging on a C-series Platform

Use the following configuration statements to configure the system log server at the [edit] hierarchy level.

system syslog file *file-name* (any | authorization | daemon | ftp | kernel | user | local7) {
(any | emergency | alert | critical | error | warning | notice | info | none);
}

system syslog host *log-host-name* (any | authorization | daemon | ftp | kernel | user | local7) {
(any | emergency | alert | critical | error | warning | notice | info | none);
}

system syslog user *user-name* (any | authorization | daemon | ftp | kernel | user | local7) {
(any | emergency | alert | critical | error | warning | notice | info | none);
}

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

Saving System Log Messages to a File

Use the following statements to configure the system log server to store messages in a file:

system syslog file *file-name* (any | authorization | daemon | ftp | kernel | user | local7) {
(any | emergency | alert | critical | error | warning | notice | info | none);
}

By default, message files are stored in the */var/log* directory. All log files are rotated daily. When a new log file is created, the previous day's file is compressed and saved. After rotation, the software retains only the last five compressed log files.

To configure the system log server to send messages to a file on the local C-series platform:

1. From configuration mode, access the configuration statement that configures the system log server.

   ```
   [edit]
   user@host# edit system syslog
   ```

2. Specify the name of the file to store messages, and group and severity level for the messages.

   ```
   [edit system syslog]
   user@host# set file file-name message-group severity
   ```

   For example, to configure the system log server to save critical messages generated by authentication and authorization attempts to the file named access:

   ```
   [edit system syslog]
   user@host# set file access authorization critical
   ```

Sending System Log Messages to Other Servers

Use the following statements to configure the system log server to send messages to another system log server:

```
system syslog host log-host-name (any | authorization | daemon | ftp | kernel | user |
local7) {
(any | emergency | alert | critical | error | warning | notice | info | none);
}
```

Before you configure the system log server to send messages to other system log servers, ensure that the remote system log server is configured to receive messages on the standard UDP port, 514.

To configure the system log server to send messages to another system log server:

1. From configuration mode, access the configuration statement that configures the system log server.

   ```
   [edit]
   user@host# edit system syslog
   ```

2. Specify the remote system log server to receive messages as well as the groups and severity level for those messages.

   [edit system syslog]
   user@host# **set host** *log-host-name message-group severity*

   For example, to configure the system log server to send error messages generated by processes on the C-series platform to my-syslog-server:

   [edit system syslog]
   user@host# **set my-syslog-server.mydomain.com local7 error**

Sending Notifications for System Log Messages to Users

Use the following statements to configure the system log server to send notifications to users:

system syslog user *user-name* (any | authorization | daemon | ftp | kernel | user | local7) {
(any | emergency | alert | critical | error | warning | notice | info | none);
}

To configure the system log server to send notifications to users:

1. From configuration mode, access the configuration statement that configures the system log server.

   [edit]
   user@host# **edit system syslog**

2. Specify the user to receive notifications and the types of notifications to be sent.

   [edit system syslog]
   user@host# **set user** *user-name message-group severity*

   For example, to configure the system log server to send notifications to admin for conditions that require immediate attention:

   [edit system syslog]
   user@host# **set user admin any critical**