

Chapter 24

System Log Messages Overview

The JUNOS software generates system log messages to record events that occur on the router, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency, or a user logging in to the configuration database

- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process

- Emergency or critical conditions, such as router power-down due to excessive temperature

Each system log message identifies the software process that generated the message and briefly describes the operation or error that occurred.

The chapter discusses the following topics:

- System Logging Configuration Guidelines on page 314

- Minimum System Logging Configuration on page 315

- Configure System Logging

- Direct Messages to a Log File on page 317

- Direct Messages to a User Terminal on page 317

- Direct Messages to the Console on page 318

- Archive System Logs on page 318

- Direct Messages to a Remote Machine on page 319

Go to page 322 for system logging configuration examples. For more information about system logging, see the *JUNOS Internet Software System Log Messages Reference*.

System Logging Configuration Guidelines

System logging operations use a system logging mechanism to record systemwide, high-level operations, such as interfaces' going up or down and users' logging in to or out of the router.

To control system logging and how much information the system should log, include the `syslog` statement at the `[edit system]` hierarchy level:

```
[edit system]
syslog {
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
  console {
    facility level;
  }
  file filename {
    facility level;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
  host hostname {
    facility level;
    facility-override facility;
    log-prefix string;
  }
  user (username | *) {
    facility level;
  }
}
```

Minimum System Logging Configuration

For the JUNOS software processes to generate system log messages, you must include the `syslog` statement at the `[edit system]` hierarchy level. Specify at least one destination for system log messages, as described in Table 15.

Table 15: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration
File	<pre>[edit system syslog] file filename { facility level; }</pre>
Remote machine	<pre>[edit system syslog] host hostname { facility level; }</pre>
Router console	<pre>[edit system syslog] console { facility level; }</pre>
Terminal session of one, several, or all users	<pre>[edit system syslog] user (username *) { facility level; }</pre>

Configure System Logging

The JUNOS system logging utility is similar to the UNIX `syslogd` utility, and includes the following features:

You can direct messages to one or more destinations:

To a named file in a local file system (when you include the `file` statement). See “Direct Messages to a Log File” on page 317.

To the terminal sessions of one or more specific users (or all users) when they are logged into the router (when you include the `user` statement). See “Direct Messages to a User Terminal” on page 317.

To the router console (when you include the `console` statement). See “Direct Messages to the Console” on page 318.

To a remote machine that is running the `syslog` utility, by configuring the `host` statement. See “Direct Messages to a Remote Machine” on page 319.

Each message is assigned to a *facility*, which is a group of messages that are either generated by the same software process or associated with a similar condition or activity (such as authentication attempts). To log the messages belonging to one or more facilities to a particular destination, specify each facility name as a separate statement within the set of statements for the destination. Table 16 lists the JUNOS system logging facilities.

Table 16: System Logging Facilities

Facility	Type of Event or Error
any	Any (includes messages from all facilities)
authorization	Authentication and authorization attempts
change-log	Change to the JUNOS configuration
conflict-log	Configuration that is inconsistent with router hardware
cron	Actions performed or errors encountered by the cron daemon
daemon	Actions performed or errors encountered by various system daemons
firewall	Packet filtering actions performed by a firewall filter
interactive-commands	Commands issued at the JUNOS command-line interface (CLI) operational mode prompt
kernel	Actions performed or errors encountered by the JUNOS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
user	Actions performed or errors encountered by various user-space processes

Each message is assigned a *severity level*, which indicates how seriously the triggering event affects router functions. When you configure logging for a facility and destination, you specify a severity level for each facility; messages that belong to the facility and are rated at that level or higher are logged to the destination. Table 17 lists the severity levels in order from highest to lowest.

Table 17: System Log Message Severity Levels

Severity Level	Description
emergency	System panic or other condition that causes the router to stop functioning.
alert	Conditions that require immediate correction, such as a corrupted system database.
critical	Critical conditions, such as hard disk 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 non-error conditions of interest.
debug	Software debugging messages. Specify this level only when so directed by a technical support representative.

To prevent log files from growing too large, the JUNOS system logging utility by default writes messages to a sequence of files of a defined size. You can configure the number of files, their maximum size, and who can read them. For more information, see “Archive System Logs” on page 318.

When directing messages to a remote machine, you can configure features that make it easier to separate JUNOS-specific messages or messages generated on particular routers. For more information, see “Direct Messages to a Remote Machine” on page 319.

A common set of operations to log is when users log on to the router and when they issue CLI commands. To configure this type of logging, specify the interactive-commands facility and one of the following severity levels:

info—Log all top-level CLI commands, including the configure command, and all configuration mode commands.

notice—Log the configuration mode commands rollback and commit.

warning—Log when any software process restarts.

Another common operation to log is when users enter authentication information. To configure this type of logging, specify the authorization facility.

Direct Messages to a Log File

To direct system log messages to a file on the local disk of the router, include the file statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
file filename {
  facility level;
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
}
```

The default directory for log files is `/var/log`; to specify a different directory on the local disk, include the complete pathname. For the list of logging facilities and severity levels, see Table 16 and Table 17 respectively.

You can also include the archive statement to configure the number, size, and permissions for a log file. For more information, see “Archive System Logs” on page 318.

Direct Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged into the router, include the user statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
user (username | *) {
  facility level;
}
```

Specify one or more JUNOS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged into the router. For the list of logging facilities and severity levels, see Table 16 and Table 17 respectively.

Direct Messages to the Console

To direct system log messages to the router console, include the console statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
console {
  facility level;
}
```

For the list of logging facilities and severity levels, see Table 16 and Table 17 respectively.

Archive System Logs

Logging information is saved to one or more files. By default, the software stores the logging information in up to ten 128-KB files, and by default, these files can be read by a limited group of users. To configure the number and size of all system log files, as well as who can read them, include the archive option at the [edit system syslog] hierarchy level:

```
[edit system]
syslog {
  archive {
    files number;
    size size;
    (world-readable | no-world-readable);
  }
}
```

To configure the number and size of a particular system log file, as well as who can read it, include the archive option at the [edit system syslog file filename] hierarchy level:

```
[edit system]
syslog {
  file filename {
    facility level;
    archive {
      files number;
      size size;
      (world-readable | no-world-readable);
    }
  }
}
```

You can configure any number of files in the range 1 through 1000, and they can be any size in the range 64 KB (64k) through 1 GB (1g).

To allow any user to read the log file, include the world-readable option.

Direct Messages to a Remote Machine

By default, messages directed to a remote machine retain the facility to which they belong on the local machine. In other words, the logging utility on the remote machine handles the messages in the same way as messages that belong to that facility even if they are generated on the remote machine.

To direct system log messages to a remote machine, include the host statement at the [edit system syslog] hierarchy level:

```
[edit system syslog]
host hostname {
  facility level;
  facility-override facility;
  log-prefix string;
}
```

Specify the remote machine's IP address or fully qualified hostname. The remote machine must be running either the standard syslogd utility or the JUNOS software, but we do not recommend directing messages to another router. For the list of logging facilities and severity levels, see Table 18 and Table 17 respectively.

The JUNOS logging utility includes the following features to help you separate, aggregate, and label messages directed to a remote machine:

Assign an Alternate Facility on page 319

Prepend a Prefix on page 321

For examples of system logging configurations, see “Examples: Configure System Logging” on page 322.

Assign an Alternate Facility

By default, messages directed to a remote machine are handled in the same way as messages that are generated on the remote machine. For example, suppose you configure the following statements on local-router to write messages from the authorization facility to a remote machine called monitor:

```
[edit system syslog]
host monitor {
  authorization info;
}
```

If the logging utility on monitor is configured to write messages belonging to the authorization facility to the file /var/log/auth-attempts, the file will contain the messages generated when users log on to local-router and the messages generated when users log on to monitor. Although the name of the source machine appears in each system log message, mixing messages from multiple machines can make it more difficult to analyze the contents of the auth-attempts file.

To assign all messages sent to a remote machine to a different facility on that machine, include the `facility-override` and `facility` statements at the `[edit system syslog host hostname]` hierarchy level:

```
[edit system syslog host hostname]
  facility level;
  facility-override facility;
```

On the remote machine, you must also configure the logging utility to handle the messages assigned to the alternate facility in the desired manner.

Table 18 shows the facilities for the `facility-override` statement.

Table 18: Facilities for the `facility-override` Statement

Facility	Description
authorization	Authentication and authorization attempts
cron	Actions performed or errors encountered by the cron daemon
daemon	Actions performed or errors encountered by various system daemons
kernel	Actions performed or errors encountered by the JUNOS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by various user-space processes

Examples: Assign an Alternate Facility

Log all messages generated on the local router at the error level or higher to the local0 facility on the remote machine called monitor:

```
[edit system syslog]
  host monitor {
    any error;
    facility-override local0;
  }
```

In the following example, a single remote machine called `central-logger` handles log messages about configuration changes for two routers located in California and two routers located in New York. The messages from California are aggregated into one facility (`local1`) and the messages from New York into another facility (`local2`).

Configure California routers to aggregate messages in the local1 facility:

```
[edit system syslog]
host central-logger {
  change-log info;
  facility-override local1;
}
```

Configure New York routers to aggregate messages in the local2 facility:

```
[edit system syslog]
host central-logger {
  change-log info;
  facility-override local2;
}
```

On central-logger, you could then configure the system logging utility to write messages from the local1 facility to the /var/log/california-config file and the messages from the local2 facility to the /var/log/new-york-config file.

Prepend a Prefix

To prepend a string to every system log message sent to a remote machine, include the log-prefix and *facility* statements at the [edit system syslog host *hostname*] hierarchy level:

```
[edit system syslog host hostname]
facility level;
log-prefix string;
```

The log-prefix string can contain any alphanumeric character except spaces, equal signs (=), or colons (:). A colon and a space are appended to the string when the system log messages are written to the log.

Example: Prepend a Prefix

Prepend the string M40 to all messages generated on the router to indicate that the router is an M40, and send the messages to the remote machine hardware-logger:

```
[edit system syslog]
host hardware-logger {
  any info;
  log-prefix M40;
}
```

When these configuration statements are included on the router original1, a message in the system logging file on hardware-logger looks like the following:

```
Mar 9 17:33:23 original1 M40: mgd[477]: UI_CMDLINE_READ_LINE: user 'root', command
'run show version'
```

Examples: Configure System Logging

Configure how various types of messages are handled, as described in the comments. Information is logged to two files, a remote machine, the terminal of user alex, and to the console:

```
[edit system]
syslog {
/* write all security-related messages to file "security" */
  file security {
    authorization info;
    interactive-commands info;
  }
/* write messages about potential problems to file "messages": messages */
/* from "authorization" facility at level "notice" and above, messages from */
/* all other facilities at level "warning" and above */
  file messages {
    authorization notice;
    any warning;
  }
/* write all messages at level "critical" and above to terminal of user "alex" if she */
/* is logged in */
  user alex {
    any critical;
  }
/* write all messages from the "daemon" facility at level "info" and above, and messages
*/
/* from all other facilities at level "warning" and above, to the machine junipero.berry.net */
  host junipero.berry.net {
    daemon info;
    any warning;
  }
/* write all messages at level "error" or above to the system console */
  console {
    any error;
  }
}
```

Configure the handling of messages generated when users issue JUNOS CLI commands, as described in the comments:

```
[edit system]
syslog {
/* write messages to file "user-actions" when users issue any CLI command */
  file user-actions {
    interactive-commands info;
  }
/* write messages to terminal of user "philip" when users issue "rollback"*/
/* or "commit" command */
  user philip {
    interactive-commands notice;
  }
/* write messages to console when users issue commands that restart */
/* a JUNOS software process*/
  console {
    interactive-commands warning;
  }
}
```

Write messages about all CLI commands entered by users, and all authentication or authorization attempts to the file `cli-commands` and to the terminal of any user who is logged in:

```
[edit system]
syslog {
  file cli-commands {
    interactive-commands info;
    authorization info;
  }
  user * {
    interactive-commands info;
    authorization info;
  }
}
```

Write all changes to the state of alarms to the file `alarms`:

```
[edit system]
syslog {
  file alarms {
    kernel warning;
  }
}
```

