

Chapter 22

Configure System Logging

System logging operations use a syslog-like mechanism to record systemwide, high-level operations, such as interfaces' going up or down and users' logging into 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);
  }
  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;
  }
  console {
    facility level;
  }
}
```

You can log system logging information to one or more destinations. The destinations can be one or more files, one or more remote hosts, the terminals of one or more users if they are logged in, and the system console.

For each place where you can log system logging information, you specify the class (*facility*) of messages to log and the minimum severity level (*level*) of the message.

Table 10 lists the system logging facilities, and Table 11 lists the system logging severity levels.

Table 10: System Logging Facilities

Facility	Description
any	Any facility
authorization	Any authorization attempt
change-log	Any change to the configuration
cron	Cron daemon
daemon	Various system daemons
interactive-commands	Commands executed in the CLI
kernel	Messages generated by the JUNOS kernel
user	Messages from random user processes

Table 11: System Logging Severity Levels

Severity Level (from Highest to Lowest Severity)	Description
emergency	Panic or other conditions that cause the system to become unusable.
alert	Conditions that should be corrected immediately, such as a corrupted system database.
critical	Critical conditions, such as hard drive errors.
error	Standard error conditions.
warning	System warning messages.
notice	Conditions that are not error conditions, but that might warrant special handling.
info	Informational messages. This is the default.
debug	Software debugging messages.

A common set of operations to log is when users log into 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.

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 modify 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 modify 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.

Overriding the Facility

When sending messages to a remote host, you can override the facility. For example, you can configure all messages from a single router to go to a single log file on the remote host. You can also configure different routers to send messages to different log files on the same remote host, to, for example, segregate messages representing different regions of the country.

To override the facility, include the `facility-override` statement at the `[edit system syslog host hostname]` hierarchy level.

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

Table 12 lists the system logging facilities that you can specify on the `facility-override` statement.

Table 12: System Logging Facilities That You Can Specify on the `facility-override` Statement

Facility	Description
authorization	Any authorization attempt
cron	Cron daemon
daemon	Various system daemons
kernel	Messages generated by the JUNOS kernel
local0	Local logging option number 0
local1	Local logging option number 1
local2	Local logging option number 2
local3	Local logging option number 3
local4	Local logging option number 4
local5	Local logging option number 5
local6	Local logging option number 6
local7	Local logging option number 7
user	Messages from random user processes

Configure Log Message Prefixes

You can configure a string to be prepended to every log message sent to the remote host, which is useful for identifying the router from which it came. The string cannot contain spaces, equal signs (=), or colons (:). To prepend a string to log messages sent to a remote host, include the `log-prefix` statement at the `[edit system syslog host hostname]` hierarchy level.

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

A colon and a space are appended to the string when the syslog messages are written to the log. For example, if the string is configured as `JNPR`:

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

Examples: Configure System Logging

Log system logging information to two files, one remote host, the user Alex's terminal, and the system console:

```
[edit system]
syslog {
  /* send all security-related information to file "security" */
  file security {
    authorization info;
    interactive-commands info;
  }
  /* send generic messages (authorization at level notice and above,
  the rest at level warning and above) to file "messages" */
  file messages {
    authorization notice;
    any warning;
  }
  /* send any critical messages to alex if he is logged in */
  user alex {
    any critical;
  }
  /* send all daemon level info and above, or anything warning and above, to
  the host junipero.berry.net */
  host junipero.berry.net {
    daemon info;
    any warning;
  }
  /* send any error messages, or higher, to the system console */
  console {
    any error;
  }
}
```

Log all CLI commands entered by all users and all authorization attempts to a file and to the terminals of all users who are logged in:

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

Log all CLI commands entered by any user to the user Philip's terminal and log only the rollback and commit commands entered by any user to the user Darius' terminal:

```
[edit system]
syslog {
  user philip {
    interactive-commands any;
  }
  user darius {
    any notice;
  }
}
```



Log the changing of alarms:

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