soundtraining.net
accelerated i.t. training

Documentation

www.soundtraining.net
(206) 988-5858

# Configuring syslogd

*By Don R. Crawley, CCNA Security, Linux+*

syslogd is the Linux logging daemon. As with nearly everything in Linux, it is highly configurable. syslogd can track almost anything you wish on your Linux system from kernel messages to logins to mail usage. You can configure syslogd by modifying /etc/syslog.conf on most Linux systems. If you don't find syslog.conf under /etc, try "whereis syslog.conf" to locate it.

syslog.conf controls the type of messages that are logged, the level of logging, and where messages are stored. syslog.conf is usually commented extensively and fairly easy to understand. The format of syslog.conf is divided into two parts: selectors and actions. Selectors is also divided into two parts: facility and level and they're separated by a period. Selectors and actions are separated by a tab:

```
facility.level action
```

Facility is the source of the logging messages, level is the amount of logging, and action is where to send the messages. For example:

```
mail.info /var/log/maillog
```

tells syslogd to log messages concerning mail using a level of "info" to /var/log/maillog. The available levels, in order of decreasing severity, are emerg, alert, crit, err, warning, notice, info, and debug. (debug provides the greatest amount of information; emerg provides the least.) You can also use wildcards in syslog.conf. For example:

```
*.emerg /dev/console
```

would send all messages of emerg level straight to the console. Another example:

```
kern.* /dev/console
```

would send all kernel messages to the console. Similarly, this example:

```
kern.* *
```

would send emergency level messages to all users. For more information, read the man page for syslog.conf:

```
#man syslog.conf
```

## *Viewing System Logs*

You can view system logs by navigating to /var/log and viewing the file ŧmessagesŧ. Each line of the log can be broken down into five parts:

1. The date and time the message was received
2. The name of the computer that generated the message
3. The service or program associated with the message
4. The PID of the program or service
5. The message itself

It's often helpful to use a grep filter to limit the number of log messages viewed. For example, if youɫre having problems with secure shell, you might start your troubleshooting by using a command similar to this:

```
#less /var/log/messages | grep sshd
```

**soundtraining.net**
Accelerated, task-based training for IT pros
On the web: www.soundtraining.net
On the phone: (206) 988-5858