System Logs and the Syslog Standard

Logs are extremely helpful for troubleshooting or catching minor issues before they become major problems. Linux administrators should know where logs are stored and how to manage them.

Many programs use the syslog standard to write messages to logs. Log services that implement the syslog standard (like syslog, rsyslog, and syslog-ng) accept messages that are flagged with a facility and a priority - the category of the message and its level of importance. They use the facility and priority to determine what log file to store the message in.

Configuration location

Each syslog variant stores its main configuration in a different file.

Syslog variant	Main configuration file
syslog	/etc/syslog.conf
rsyslog	/etc/rsyslog.conf
syslog-ng	/etc/syslog-ng/syslog-ng.conf

The configuration sets which log file a message goes into based on factors like its facility and priority.

Log location

The log files on Linux systems are usually stored in the /var/log directory. Some examples of the log files you'll find there are listed in the following table.

Log name	Subject
messages or syslog	General system messages
dmesg or kern.log	Kernel and drivers
cron	Cron scheduler
httpd or apache2	Web server
maillog	Mail system
secure or auth.log	Security

Logger

The logger program lets users and scripts send log entries to syslog.

Format

```
logger <OPTIONS> [MESSAGE]
```

Options

Option	Description
-p	Specify either the priority or facility.priority. Default is “user.notice”
-n	Log to a remote server instead of the local syslog service
-t	Add a tag to the message (default is the username that ran logger)
-f	Read the log message from the specified file

If the message isn’t specified and -f isn’t used, then logger will read from standard input (hit Ctrl-D to end the message).

Logger example

This invocation of logger will log the message “System load is low” with the tag “SYSLOAD”, the facility “user”, and the priority “info”. Rather than logging to the local syslog, the log message is sent to the log server at logs.example.com.

```
logger -t SYSLOAD -p user.info -n logs.example.com System load is low
```

Logrotate

The logrotate program prunes logs on a regular basis to keep them from growing too large and filling the disk. When you install a program that generates its own log files instead of using syslog, the installer will usually put a file in the logrotate configuration directory here:

```
/etc/logrotate.d
```

Consider the configuration files in that directory to be examples that you can copy and modify for other programs so their logs don’t get out of control. Full documentation for the directives in the configuration file can be viewed by running man logrotate.conf.

Priorities

The priority of a syslog message indicates its severity. The lowest priority is “debug” (usually very detailed information used only when troubleshooting code), and the highest priority is “emerg” (emergency messages that indicate that the system must shut down).

Priority (low to high)	Description
debug	Debugging messages
info	Informational
notice	Normal but noteworthy
warning	Warnings
err	Errors
crit	Critical
alert	Needs immediate attention
emerg	Renders system unusable

Deprecated priorities that might show up on older systems include warn (same level as warning), err (same as error), and panic (same as emerg).

Facilities

The facility of a syslog message is used to categorize the message by topic. A message with the facility "mail" will usually be routed into the mail log, for example, while "authpriv" messages will be logged to a file that only root can access.

Facility	Associated system
auth	Security
authpriv	Root-only security (like login info)
cron	Cron scheduler
daemon	System daemons
ftp	FTP server
kern	Kernel
lpr	Printer daemon
mail	Mail system
news	NNTP system (Usenet)
syslog	Syslog
user	User-level
uucp	UUCP (old file copy protocol)
local0 to local7	Custom facilities for local use

Unlisted facilities are the security facility (which is deprecated - use auth instead) and the mark facility (only for internal syslog use).