11.1.2 Log File Facts

Log files can provide a system administrator with a wealth of information about how a Linux system is working.

This lesson covers the following topics:

- Common log files
- Centralized logging

Common Log Files

The following table describes the contents of commonly used log files.

File/Directory	Contents
/var/log/boot.log **/var/log/boot.msg**	The system writes messages generated during the boot process to either the boot.log or boot.msg file depending on the distribution.
/var/log/faillog **/var/log/btmp**	Login failures for user accounts are listed in either the faillog or btmp file, depending on the distribution.
/var/log/firewall **/var/log/firewalld**	Depending on the distribution, the system stores log entries for the host firewall.
/var/log/lastlog	The lastlog file holds information about the last time each user logged in.
/var/log/maillog	The maillog file contains reports on mail server status and messages related to incoming and outgoing mail.
/var/log/messages	The messages file is the default file for storing system messages. This file may include copies of messages that appear on the console, internal kernel messages, and messages sent by networking programs. The messages file is based on the init daemon, used on older Linux distributions
/var/log/warn	The warn file displays warning messages from many processes by default.
/var/log/wtmp	The wtmp file keeps track of all users who have logged into and out of the system as well as listing every connection and runlevel change.
/var/log/dmesg	The dmesg file is often called the kernel ring buffer. It reports messages received in the process of configuring hardware devices as the system boots.
/var/log/secure	The secure file logs any attempts to log in as the root user or attempts to use the **su** command. This file also contains information on remote logins and failed root user login attempts.
/var/log/sa	The **/var/log/sa** directory stores **/sa*[n]*** files, which contain all performance information for the day of the month indicated by ***[n]***. For example, **/var/log/sa/sa15** contains performance information for the fifteenth day of the month, and it will be overwritten on the fifteenth day of the next month.
/var/log/cron	The cron file stores messages related to tasks scheduled with cron. It keeps track of which tasks are run and when they were started.
/var/log/rpmpkgs	On Red Hat systems, the rpmpkgs file tracks installed packages. It also records all kernel packages on the system.
/tmp/install.log **/root/install.log**	The install.log may or may not be present, depending on the distribution. This file records messages related to the installation and can be useful for installation records for a computer.
/etc/rsyslog.conf	The rsyslog.conf file is the main configuration file for the rsyslogd which logs system messages on Linux systems. This file specifies rules for logging. For every log message received rsyslog looks at its configuration file, /etc/rsyslog.conf to determine how to handle that message. If no rule statement matches the message, Rsyslog discards it.
/var/log/kern.log	The var/log/kern.log file provides a detailed log of messages from the Linux kernel. These messages may prove useful for trouble-shooting a new or custom-built kernel
/var/log/*[application]*	Many applications also create logs in the /var/log directory. If you list the contents of your /var/log subdirectory, you will see familiar names, such as /var/log/apache2 representing the logs for the Apache 2 web server, or /var/log/samba, which

	contains the logs for the Samba server.

Centralized Logging

Since looking at individual log files can be cumbersome, especially if you have multiple servers or tiers in your architecture, a good practice is to centralize your logs in one place. With centralized logging, you are able to search through your logs quicker, which can help you solve issues faster. To take advantage of centralized logs, several third-party agents or daemons can be installed and used.

The following table list a few daemons used for centralizing logs:

Daemon	Description
rsyslog	A light-weight daemon installed on most common Linux distributions. It offers fast high-performance, great security features, and a modular design. It is able to accept inputs from a wide variety of sources, transform them, and output the result to diverse destination. This is the most popular daemon.
syslog-ng	syslog-ng collects logs from any source, process them in real time, and delivers them to a wide variety of destinations. syslog-ng also allows you to flexibly collect, parse, classify, rewrite and correlate logs from across your infrastructure and store or route them to log analysis tools.
Fluentd	Lets you unify the data collection and consumption for a better use and understanding of data. Fluentd tries to structure data as JSON as much as possible and has a flexible plug-in system that allows the community to extend its functionality.
logstash	A heavy-weight agent capable of performing more advanced processing and parsing. It is capable of obtaining data from a multitude of sources simultaneously, and after processing, it can then send it to your favorite “stash”.