11.1.7 Log File Display Facts

As a system administrator, you will encounter both binary and text-based log files. You should be familiar with working with both types of files.

This lesson covers the following topics:

- Viewing and managing text-based log files
- Viewing and managing binary log files

View and Manage Text-based Log Files

The following table describes commands to view and manage text-based log files:

Command	Use To	Function
cat	Views the contents of a log file.	**cat /var/log/messages** shows the entire text of the messages log.
grep	Filters text from a text file.	**cat /var/log/messages | grep ftp** filters the output of the cat command to show only lines that contain the term *ftp*.
tail	Shows the last 10 lines of a file. Be aware of the following options: • **-f** displays additions to the log in real time. • **-n**# specifies the number of lines to display.	**tail /var/log/messages** shows the last 10 lines of the messages log. **tail -f /var/log/messages** displays the real-time entries of the messages log as they are updated.
head	Shows the first 10 lines of a file.	**head /var/log/messages** shows the first 10 lines of the messages log.
less **more**	Scrolls through individual pages of a file.	**less /var/log/messages** allows you to scroll through each page of the file.
vi **gedit**	Opens text files for editing.	**vi less /var/log/messages** opens the messages log for editing.

View and Manage Binary Log Files

The following table lists several commands used to view and manage binary log files:

Command	Function
dmesg	Views the boot logs and troubleshoots hardware errors. The **dmesg** command shows information about all the hardware controlled by the kernel and displays error messages as they occur.
dmesg -n #	Controls which error messages are sent to the console. For example, **dmesg -n 1** sends only the most critical errors (0 and 1) to the console. Other messages are still logged in the log files.
last	Shows all users who have logged in to and out of the system as well as listing every connection and runlevel change (for example, the contents of the **/var/log/wtmp** file).
faillog **lastb**	Shows all failed login attempts on the system (for example, the contents of the **/var/log/btmp** file or **/var/log/faillog** file, depending on the distribution).
lastlog	Shows a list of the dates and times for the last login for each user.
logger	Changes the message severity and where logged messages are sent.
logrotate	Manages, compresses, renames, and deletes log files based on specific criteria (such as size or date).
sar	Views system statistics. **sar** is short for System Activity Report. It comes as part of the **sysstat** (System Statistics) package. When used alone, it returns CPU statistics. Common options include the following: • **-A** displays all information. • **-b** displays I/O statistics. • **-B** displays swap statistics. • **-f /var/log/sa** *filename* displays information from the specified file.