System Log Files

Most log files are found in `/var/log` Checking logs are critical to see if things are working correctly

- Checking logs is critical to see if things are working correctly.
- Take a look at all the log files on scratch `ls /var/log`

Kernel Ring Buffer

The kernel ring buffer is something like a log file for the kernel; however, unlike other log files, it's stored in memory rather than in a disk file.

You can use the `dmesg` command to view it. Many times it is logged to `/var/log/dmesg` as well. It requires sudo privileges to read the /var/log/dmesg file, but not to run the dmesg command.

Viewing log files

There are a number of commands to view log files.

- `cat`
- `less`
- `head`
- `tail`

Anytime a new entry is added to a log file, it is appended to the end of the file. This is one of those times where `tail` is particularly useful. Usually when we want to look at log files we want to look at the most recent entries.

When organizing our viewing command - order matters. Most of the following commands produce different results. And all are useful depending on what type of results you want. Go through the thought process and figure out what each command does. Can you figure out which three produce identical results?

- `cat /var/log/syslog`
- `cat /var/log/syslog | grep daemon`
- `cat /var/log/syslog | grep daemon | tail -n 10`
- `cat /var/log/syslog | tail -n 10`
- `cat /var/log/syslog | tail -n 10 | grep daemon`
- `less /var/log/syslog`
- `less /var/log/syslog | tail -n 10 | grep daemon`
- `head -n 10 /var/log/syslog`
- `head -n 10 /var/log/syslog | grep daemon`
- `tail -n 10 /var/log/syslog`
- `tail -n 10 /var/log/syslog | grep daemon`

If you add the -f option to the tail command it provides a live watch of the log file. This is helpful when trying to watch any error messages produced as you test certain functionality, such as logging in or running a specific program.

- Use `ctrl-c` to cancel the `tail -f` command.

Note that log files show info for all users and processes. If you are looking for something specific you may want refine your results with `grep`.

The log files

`/var/log/syslog` or `/var/log/messages`

- holds general purpose log files for many daemons and logs for processes that don't have their own log files. It contains General Message and system related stuff.
- If you are doing general troubleshooting start here first.

`/var/log/<some application>`

- (after installing a package like Apache web server, you would look in /var/log/apache2 to diagnose issues related to it.
- There are other log files that are important to troubleshoot other issues.

Log Files

Log files are frequently rotated or archived to keep the log files from getting too big and time-conuming to read. Meaning that the oldest log file is deleted, the latest log file is renamed with a date or number, and a new log file is created. For instance, if it’s rotated on December 1, 2012, /var/log/messages will become /var/log/messages-20121201, /var/log/messages-1.gz, or something similar, and a new /var/log/messages will be created. This practice keeps log files from growing too large.

Types of Log Files

Log Files found on Scratch

- /var/log/syslog - General message and system related stuff
- /var/log/dmesg - Kernel ring buffer log file
- /var/log/auth.log - authentication log
- /var/log/kern.log - kernel log
- /var/log/wtmp - login records file
- /var/log/dist-upgrade/ - distribution logs directory
- /var/log/dpkg.log - dpkg command log file
- /var/log/apt/ - apt command logs directory
- /var/log/fsck/ - file system check logs directory
- /var/log/upstart/ - upstart command logs directory (plug and play)
- /var/log/apache2 - apache2 access and error logs directory

Other log files not found on Scratch

- /var/log/cron.log - cron daemon log
- /var/log/boot.log - system boot log
- /var/log/messages - General message and system related stuff (CENTOS)
- /var/log/maillog - Mail server log
- /var/log/qmail/ - Qmail logs directory
- /var/log/httpd/ - Apache access and error logs directory
- /var/log/lightpd/ - Lighttpd access and error logs directory
- /var/log/mysqld.log - MySQL database server log file
- /var/log/secure - Authentication log
- /var/log/utmp - Login records file
- /var/log/yum.log - yum command log file (CENTOS)

Textbook Time

There is no textbook reading for this section
