Logging Files

coursera.org/learn/linux-for-developers/supplement/PSurX/logging-files

System log files are essential for monitoring and troubleshooting. In Linux, these messages appear in various files under **/var/log**.

Ultimate control of how messages are dealt with is controlled by the **syslogd** daemon (usually **rsyslogd** on modern systems) common to many UNIX-like operating systems. The newer systemd-based systems can use **journalctl** instead, but usually retain **syslogd** and cooperate with it.

Important messages are sent not only to the logging files, but also to the system console window; if you are not running X or are at a virtual terminal, you will see them directly there as well. In addition, these messages will be copied to **/var/log/messages** (or to **/var/log/syslog** on Ubuntu), but if you are running X, you have to take some steps to view them.

A good way to see them is to open a terminal window, and in that window, type **tail -f /var/log/messages**. On a GNOME desktop, you can also access the messages by clicking on *System* > *Administration* > *System Log or Applications* > *System Tools* > *Log File Viewer* in your Desktop menus, and other desktops have similar links you can locate.

In order to keep log files from growing without bound, the **logrotate** program is run periodically and keeps four previous copies (by default) of the log files (optionally compressed) and is controlled by **/etc/logrotate.conf**.

Here are some of the important log files found under **/var/log**:

File	Purpose
boot.log	System boot messages
dmesg	Kernel messages saved after boot. To see the current contents of the kernel message buffer, type **dmesg**
messages or **syslog**	All important system messages
secure	Security related messages