1. The main log file

a) /var/log/messages – Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.

2. Access and authentication

a) /var/log/auth.log – Contains system authorization information, including user logins and authentication machinsm that were used.

b) /var/log/lastlog – Displays the recent login information for all the users. This is not an ascii file. You should use lastlog command to view the content of this file.

c) /var/log/btmp – This file contains information about failed login attemps. Use the last command to view the btmp file. For example, “last -f /var/log/btmp | more”

d) /var/log/wtmp or /var/log/utmp – Contains login records. Using wtmp you can find out who is logged into the system. who command uses this file to display the information.

e) /var/log/faillog – Contains user failed login attemps. Use faillog command to display the content of this file.

f) /var/log/secure – Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login.

3. Package install/uninstall

a) /var/log/dpkg.log – Contains information that are logged when a package is installed or removed using dpkg command

b) /var/log/yum.log – Contains information that are logged when a package is installed using yum

4. System

a) /var/log/daemon.log – Contains information logged by the various background daemons that runs on the system

b) /var/log/cups – All printer and printing related log messages

c) /var/log/cron – Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file

5. Applications

b) /var/log/maillog /var/log/mail.log – Contains the log information from the mail server that is running on the system. For example, sendmail logs information about all the sent items to this file

b) /var/log/Xorg.x.log – Log messages from the XWindows system

Information

There are lots of log files located in **/var/log/** on any Linux machine. What do they mean and what do they log?

Details

The following log files are located in the **/var/log/** directory and while this list is comprehensive, it is by no means every possible log file that can exist in this location.

The logs are managed by the syslog facility and the various facilities can log to one or more of the log files listed. In addition, the user can turn off logging of a specific facility.

The facilities are typically:

```
kern.*
*.info
mail.*
authpriv.*
cron.*
*.emerg
```

These are set up, on a RHEL system in **/etc/syslog.conf** file.

Here are a list of the log files and what they mean or do:

/var/log/messages - This file has all the global system messages located inside, including the messages that are logged during system startup. Depending on how the syslog config file is sent up, there are several things that are logged in this file including mail, cron, daemon, kern, auth, etc.

/var/log/dmesg - Contains kernel ring buffer. This file is overwritten when the system is rebooted.

/var/log/auth.log - System authorization information is included in this file, along with user logins and the authentication mechanism that were used.

/var/log/boot.log - Contains information that are logged when the system boots

/var/log/daemon.log - The various system background daemons that are running will log information to this file.

/var/log/kern.log - Contains information logged by the kernel. Helpful to troubleshoot a custom-built kernel.

/var/log/lastlog - Displays the recent login information for all the users. This is not an ascii file. An admin can use the lastlog command to view the content of this file.

/var/log/maillog /var/log/mail.log - Logs information from the mail server that is running on the system. For example, sendmail logs information about all the sent items to this file.

/var/log/user.log - Contains information about all user level logs.

/var/log/Xorg.x.log - Log messages from the X server to this file.

/var/log/btmp - This file contains information about failed login attempts. Use the last command to view the btmp file. For example, `last -f /var/log/btmp | more`.

/var/log/cups /var/log/spooler - All printer and printing related log messages.

/var/log/anaconda.log - While installing Linux, all installation related messages are stored in this log file.

/var/log/yum.log - Contains information that are logged when a package is installed using yum. This file can be referenced in the event a packages is removed that has dependencies.

/var/log/cron - Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file

/var/log/secure - Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login.

/var/log/wtmp - The wtmp file records all logins and logouts.

/var/log/utmp - The utmp file allows one to discover information about who is currently using the system.

/var/log/faillog - Contains failed user login attempts. Use faillog command to display the content of this file.

/var/log/httpd/ - Contains the apache web server access_log and error_log and related virtual hosts logs if set up to log here.

/var/log/apache2 - Contains the apache web server access_log and error_log and related virtual hosts logs if set up to log here.

/var/log/conman/ - Log files for ConMan client. conman connects remote consoles that are managed by conmand daemon.

/var/log/mail/ - This subdirectory contains additional logs from the mail server. For example, sendmail stores the collected mail statistics in /var/log/mail/statistics file

/var/log/audit/ - Contains logs information stored by the Linux audit daemon (auditd).

/var/log/setroubleshoot/ - SELinux uses setroubleshootd (SE Trouble Shoot Daemon) to notify about issues in the security context of files and logs those information in this log file.

/var/log/samba/ - Contains log information stored by samba, which is used to connect Windows to Linux.

/var/log/sa/ - Contains the daily sar files that are collected by the sysstat package.