Important Log File Locations and Using journalctl

Commands for viewing, including those with 'relevant command' listed: cat, tail, grep, less, zcat, zgrep, zmore, etc.

Log location	***Relevant command***	***Comments***
/**var/log/messages**		Includes some security related info- where PAM is logged (Ubuntu after Natty instead uses /var/log/syslog)
/var/log/boot.log		Self-explanatory see also boot.log.* for older logs
/var/log/wtmp	**last**	Successful (mnemonic "working") logins, logouts, reboots
(same as above)	**last reboot**	Shows just reboots, same with keyword logins, etc
/var/log/btmp	**lastb**	Shows history of failed login attempts (mnemonic "bad")
/var/log/lastlog	**lastlog**	Shows recent user logins
/var/log/secure		Authpriv messages, more
/var/log/dmesg	**dmesg**	Boot and dbus messages
/root/install.log		Is updated - good to keep copies after fresh installs of things
/var/log/anaconda.log		System installation info on Red Hat systems
/var/log/dpkg.log		dpkg logs for Debian installs/removes (see also /apt/ directory)
/var/log/yum.log		yum command log for Red Hat installs/removes
/var/log/kern.log		Kernel logs
/var/log/daemon.log		Info from various background daemons
/var/log/user.log		Information about all user level logs
/var/log/audit/		Audit daemon (auditd).
/var/log/setroubleshoot/		SELinux's setroubleshootd
/var/log/sssd/		System security services (remote directory access, auth)
/var/log/cron.log		Crond logs
/var/log/sa/		Daily sar files for systat
/var/log/maillog		Mail server logs (sendmail/ dovecot)
/var/log/qmail/		Qmail log directory
/var/log/httpd/		Apache access and error logs directory
/var/log/lighttpd/		Lighttpd access and error logs directory
/var/log/mysqld.log		MySQL database server log file
/var/log/cups		Printer and printing related log messages
/var/log/samba/		Samba info, Windows support

- For authenication, Debian-based use **/var/log/auth.log** while Red Hat-based use **/var/log/secure**
- **/var/log/faillog** - if available can also provide info on failed login attempts
- Similar to **wtmp**, but perhaps not as useful is **/var/log/utmp**

Remember the syslog standard levels/priorities:
0= emerg, 1=alert, 2=crit, 3= err, 4=warning, 5=notice, 6=info, 7=debug
Levels with a higher numerical level give less information (7 least, 0 most)

journald and journalctl options

-f	New log entries as they are added	journalctl -u mysql -f
-k	Kernel messages (example: 5 boots previous	journalctl -k -b -5
-u	Messages for specified systemd service	journalctl -u httpd
-b	Boot msgs; last boot, use -1; two boots ago -2; etc.	(see above -k example)
--list--boots	List system boots	
-r	Show in reverse order; most recent entries first	
-p	Display messages by priority	journalctl -p err
--since, --until	Time range; formats: 09:00; "1 hour ago", 2 days ago	journalctl --since "-2017-05-23 23:15:-00"
-o	Output options, includes short, verbose export > filename	journalctl -o json-pretty
_PID, _UID	Messages produced by a specific PID, UID, GID	journalctl _UID=100 (remember **id** command)
_COMM, etc.	Name of executable or path, hostname. Similar options	journalctl _HOSTNAME=my-host
	Various attributes supported- see man page for list	_SELINUX_CONTEXT= system_r:policykit_t

The journal is saved in the **/var/log/journal/**

Integrating and Configuring rsyslogd and journald

Rsyslog is still central to logging - journald doesn't have all the mechanisms to do things
journalctl: -b for booting info, --since=yesterday or , -o for verbose, u= service (or PID) for process
journalctl without options just dumps from the binary to screen.
/etc/systemd/journald.conf

Sending journald logs to rsyslog: *In **/etc/syslog.conf** add:*
$modload imuxsock - (input module unix socket)
$OmitLocalLogging off
- and -
*In **/etc/rsyslog.d/listend.conf**, add:* $SystemLogSocketName /run/systemd/journal/syslog

Sending rsyslog to journald *In **/etc/rsyslog.conf** add:*
$modload omjournal *.* :omjournal:
(this tells it, from any facility, and any priority, send to omjournal

Other input modules (Apache into rsyslog example)

```
$ModLoad imfile

$InputFileName /var/log/httpd/error_log
$InputFileTag apache-error:
$InputFileStateFile state-apache-error
$InputRunFileMonitor
```

Exporting to a DB using an output module:

```
$ModLoad ommysql

$ActionOmmysqlServerPort 1234
*.* :ommysql:database-servername,database-name,database-
userid,database-password
```

Enabling remote logging in /etc/rsyslog.conf (these are there for us in the file, just commented out)
Provides UDP syslog reception - classical method - best backward compat but you can lose messages
$ModLoad imudp
$UDPServerRun 514

Provides TCP syslog reception - the better option
$ModLoad imtcp
$TCPServerRun 514

For sending out, look at the forwarding rules and find this:
Replace remote-host with IP addy or servername in hosts files
. @@remote-host:514

Sample conf file lines. Basic syntax is facility.level … target

```
*.info:mail.none:authpriv.none:cron.none    /var/log/messages
        .none is exclusion, * is wildcard.  This line logs everything of level 1 or higher except as noted
 authpriv.*                 /var/log/secure
        This catches all messages from authpriv and puts into /secure
*.emerg                     *
        Sends all emergency messages to all tty's and logs (local- not remote)
uucp.news.crit              /var/log/spooler
        News errors using uucp facility
local7.*                    /var/log/boot.log
        local7 is a boot facility.  See more facilities in the syslog man page
```

Logrotate - /etc/logrotate.conf **-** Specifies to rotate logs, daily, weekly, monthly; how long to keep logs before deleting; a create directive to replace the moved log with a blank empty file to use; dateext directive to use date as a filename extension; compress or not
There is also an include directive pointing to /etc/logrotate.d as a place for specific RPMs to throw logs /etc/logrotate.d/ to hold more granular rule files for syslog, http, yum, up2date, samba, etc., processes).