This is what I see on my Centos system:

[root@LinuxServer-Class log]# ls -l /var/log

total 3276

drwxr-xr-x. 2 root root 4096 Jan 27 05:46 anaconda

drwx------. 2 root root 22 Aug 4 2017 audit

-rw-r--r--. 2 root root 12484 Mar 17 14:09 boot.log

-rw-r--r--. 1 root root 59050 Mar 12 14:24 boot.log-20180312

-rw-r--r--. 1 root root 76305 Mar 17 14:07 boot.log-20180317

-rw-------. 1 root utmp 2688 Mar 17 14:01 btmp

The who command output:

[root@LinuxServer-Class log]# who

greynolds pts/0 2018-03-17 14:10 (192.168.126.1)

The last command

[root@LinuxServer-Class log]# last | grep greynold

greynold pts/0 192.168.126.1 Sat Mar 17 14:10 still logged in

greynold tty1 Sat Mar 17 14:10 - 14:21 (00:10)

greynold tty1 Sat Mar 17 14:01 - 14:08 (00:07)

In my system, the output looked like this:

[root@LinuxServer-Class log]# lastlog

Username Port From Latest

root pts/0 Sat Mar 17 14:11:11 -0700 2018

bin \*\*Never logged in\*\*

daemon \*\*Never logged in\*\*

adm \*\*Never logged in\*\*

lp \*\*Never logged in\*\*

sync \*\*Never logged in\*\*

Output:

[root@LinuxServer-Class log]# tail /var/log/messages

Mar 17 14:28:01 [localhost] systemd: Started Session 75 of user pcp.

Mar 17 14:28:01 [localhost] systemd: Starting Session 75 of user pcp.

Mar 17 14:28:03 [localhost] systemd: Removed slice User Slice of pcp.

Mar 17 14:28:03 [localhost] systemd: Stopping User Slice of pcp.

Mar 17 14:30:01 [localhost] systemd: Created slice User Slice of root.

Mar 17 14:30:01 [localhost] systemd: Starting User Slice of root.

On my Centos Server the path location for rsyslog:

/etc/rsyslog.conf:

# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-\*/rsyslog\_conf.html

# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.

$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)

$ModLoad imjournal # provides access to the systemd journal

#$ModLoad imklog # reads kernel messages (the same are read from journald)

#$ModLoad immark # provides --MARK-- message capability

# Provides UDP syslog reception

#$ModLoad imudp

#$UDPServerRun 514

# Provides TCP syslog reception

#$ModLoad imtcp

#$InputTCPServerRun 514

Here is what it looks like in Centos:

/var/log/audit.log:

type=DAEMON\_START msg=audit(1517062275.400:2303): auditd start, ver=2.3.3 format=raw kernel=3.10.0-123.el7.x86\_64 auid=4294967295 pid=867 subj=system\_u:system\_r:auditd\_t:s0 res=success

type=CONFIG\_CHANGE msg=audit(1517062275.511:5): audit\_backlog\_limit=320 old=64 auid=4294967295 ses=4294967295 subj=system\_u:system\_r:auditctl\_t:s0 res=1

/var/log/secure

[root@LinuxServer-Class log]# view secure

Mar 12 14:24:48 moodle useradd[2242]: new group: name=Man, GID=1004

Mar 12 14:24:48 moodle useradd[2242]: new user: name=Man, UID=1004, GID=1004, home=/home/Man, shell=/bin/bash

Mar 12 14:24:48 moodle chage[2247]: changed password expiry for Man

Mar 12 14:24:48 moodle useradd[2250]: new group: name=Terry, GID=1005

Mar 12 14:24:48 moodle useradd[2250]: new user: name=Terry, UID=1005, GID=1005, home=/home/Terry, shell=/bin/bash

Mar 12 14:24:48 moodle chage[2255]: changed password expiry for Terry

Here is what it looks like in Centos:

[root@LinuxServer-Class etc]# logger -p local4.info " This is a info message from local 4"

[root@LinuxServer-Class etc]# less /var/log

[11]+ Stopped less /var/log

[root@LinuxServer-Class etc]# tail -f /var/log/local4info.log

Mar 17 16:00:48 [localhost] greynolds: This is a info message from local 4

Here is what it look like when I rotate logs in Centos:

rotating log /var/log/maillog, log->rotateCount is 4

dateext suffix '-20180317'

glob pattern '-[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]'

rotating log /var/log/messages, log->rotateCount is 4

dateext suffix '-20180317'

glob pattern '-[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]'

rotating log /var/log/secure, log->rotateCount is 4

dateext suffix '-20180317'

glob pattern '-[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]'