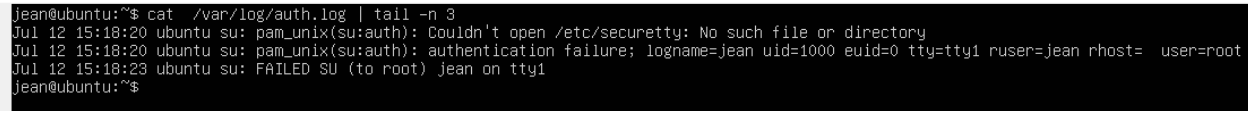
Exercise 12-Logs

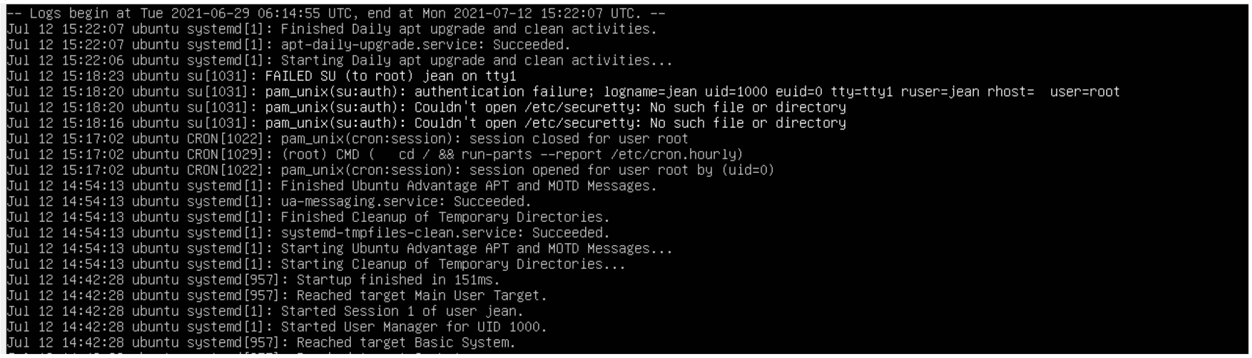
1. Change your user to another (for example from regular user to root) and input a wrong password. How and from what log file in /var/log path you can retrieve the information from this failed login attempt?



```
jean@ubuntu:~$ cat  /var/log/auth.log | tail -n 3
Jul 12 15:18:20 ubuntu su: pam_unix(su:auth): Couldn't open /etc/securetty: No such file or directory
Jul 12 15:18:20 ubuntu su: pam_unix(su:auth): authentication failure; logname=jean uid=1000 euid=0 tty=tty1 ruser=jean rhost=  user=root
Jul 12 15:18:23 ubuntu su: FAILED SU (to root) jean on tty1
jean@ubuntu:~$
```

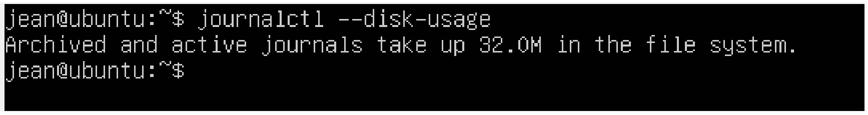
2. How do you retrieve the logged information from journald from last 24 hours so that newest entries are displayed first (at the top)?

With the command **journalctl –reverse**



```
-- Logs begin at Tue 2021-06-29 06:14:55 UTC, end at Mon 2021-07-12 15:22:07 UTC. --
Jul 12 15:22:07 ubuntu systemd[1]: Finished Daily apt upgrade and clean activities.
Jul 12 15:22:07 ubuntu systemd[1]: apt-daily-upgrade.service: Succeeded.
Jul 12 15:22:06 ubuntu systemd[1]: Starting Daily apt upgrade and clean activities...
Jul 12 15:18:23 ubuntu su[1031]: FAILED SU (to root) jean on tty1
Jul 12 15:18:20 ubuntu su[1031]: pam_unix(su:auth): authentication failure; logname=jean uid=1000 euid=0 tty=tty1 ruser=jean rhost=  user=root
Jul 12 15:18:20 ubuntu su[1031]: pam_unix(su:auth): Couldn't open /etc/securetty: No such file or directory
Jul 12 15:18:16 ubuntu su[1031]: pam_unix(su:auth): Couldn't open /etc/securetty: No such file or directory
Jul 12 15:17:02 ubuntu CRON[1022]: pam_unix(cron:session): session closed for user root
Jul 12 15:17:02 ubuntu CRON[1029]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Jul 12 15:17:02 ubuntu CRON[1022]: pam_unix(cron:session): session opened for user root by (uid=0)
Jul 12 14:54:13 ubuntu systemd[1]: Finished Ubuntu Advantage APT and MOTD Messages.
Jul 12 14:54:13 ubuntu systemd[1]: ua-messaging.service: Succeeded.
Jul 12 14:54:13 ubuntu systemd[1]: Finished Cleanup of Temporary Directories.
Jul 12 14:54:13 ubuntu systemd[1]: systemd-tmpfiles-clean.service: Succeeded.
Jul 12 14:54:13 ubuntu systemd[1]: Starting Ubuntu Advantage APT and MOTD Messages...
Jul 12 14:54:13 ubuntu systemd[1]: Starting Cleanup of Temporary Directories...
Jul 12 14:42:28 ubuntu systemd[957]: Startup finished in 151ms.
Jul 12 14:42:28 ubuntu systemd[957]: Reached target Main User Target.
Jul 12 14:42:28 ubuntu systemd[1]: Started Session 1 of user jean.
Jul 12 14:42:28 ubuntu systemd[1]: Started User Manager for UID 1000.
Jul 12 14:42:28 ubuntu systemd[957]: Reached target Basic System.
```

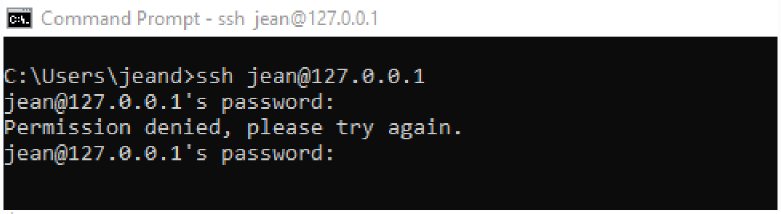
3. How much do stored journal files take up disk space?



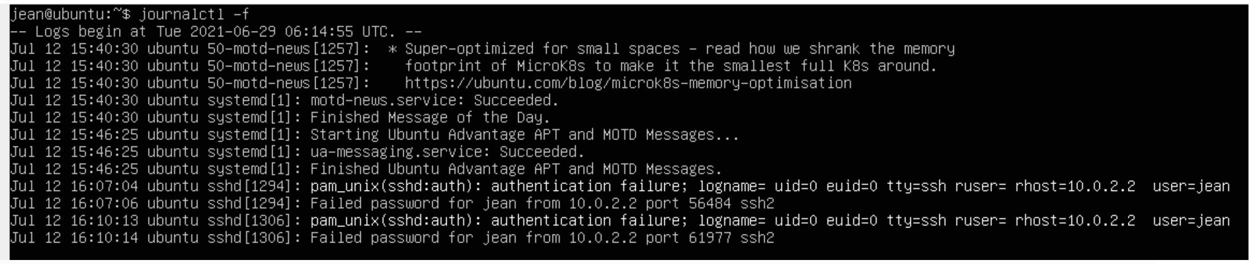
```
jean@ubuntu:~$ journalctl --disk-usage
Archived and active journals take up 32.0M in the file system.
jean@ubuntu:~$
```

4. Open journald for real-time logging. Now open SSH connection to your Ubuntu (refer to Putty guide in here). Try to login by typing first the invalid and then the correct password. How are these entries logged?

Failed Login

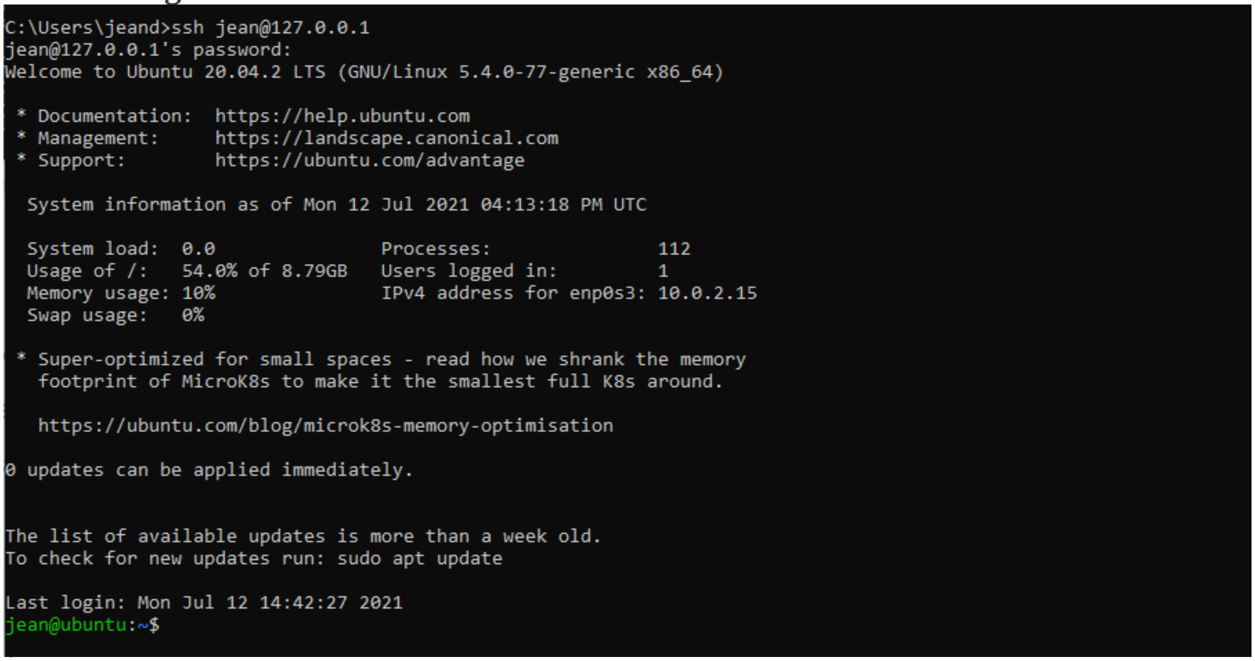


```
C:\Users\jeand>ssh jean@127.0.0.1
jean@127.0.0.1's password:
Permission denied, please try again.
jean@127.0.0.1's password:
```

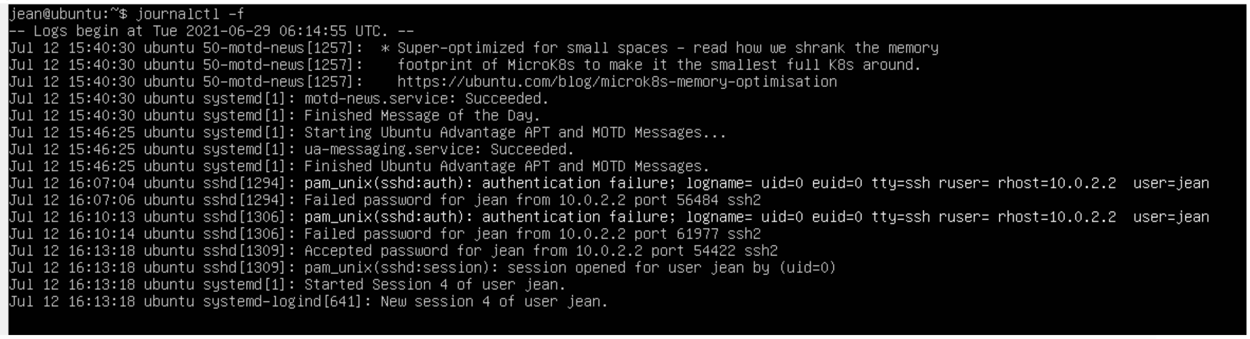


```
jean@ubuntu:~$ journalctl -f
-- Logs begin at Tue 2021-06-29 06:14:55 UTC. --
Jul 12 15:40:30 ubuntu 50-motd-news[1257]:  * Super-optimized for small spaces - read how we shrank the memory
Jul 12 15:40:30 ubuntu 50-motd-news[1257]:    footprint of MicroK8s to make it the smallest full K8s around.
Jul 12 15:40:30 ubuntu 50-motd-news[1257]:    https://ubuntu.com/blog/microk8s-memory-optimisation
Jul 12 15:40:30 ubuntu systemd[1]: motd-news.service: Succeeded.
Jul 12 15:40:30 ubuntu systemd[1]: Finished Message of the Day.
Jul 12 15:46:25 ubuntu systemd[1]: Starting Ubuntu Advantage APT and MOTD Messages...
Jul 12 15:46:25 ubuntu systemd[1]: ua-messaging.service: Succeeded.
Jul 12 15:46:25 ubuntu systemd[1]: Finished Ubuntu Advantage APT and MOTD Messages.
Jul 12 16:07:04 ubuntu sshd[1294]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2  user=jean
Jul 12 16:07:06 ubuntu sshd[1294]: Failed password for jean from 10.0.2.2 port 56484 ssh2
Jul 12 16:10:13 ubuntu sshd[1306]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2  user=jean
Jul 12 16:10:14 ubuntu sshd[1306]: Failed password for jean from 10.0.2.2 port 61977 ssh2
```

Success Login

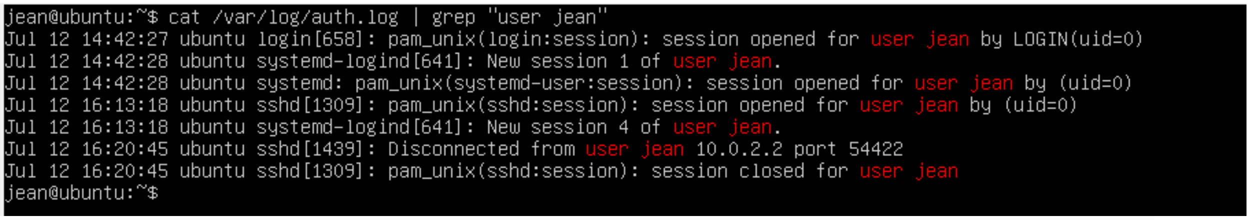


```
C:\Users\jeand>ssh jean@127.0.0.1
jean@127.0.0.1's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 12 Jul 2021 04:13:18 PM UTC

  System load:  0.0               Processes:               112
  Usage of /:   54.0% of 8.79GB   Users logged in:         1
  Memory usage: 10%               IPv4 address for enp0s3: 10.0.2.15
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jul 12 14:42:27 2021
jean@ubuntu:~$
```



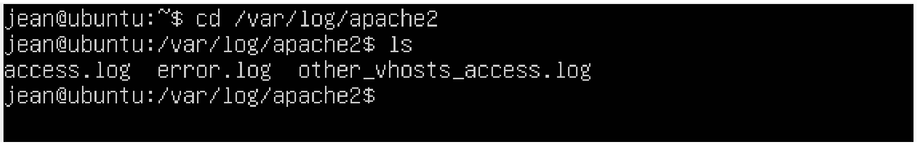
```
jean@ubuntu:~$ journalctl -f
-- Logs begin at Tue 2021-06-29 06:14:55 UTC. --
Jul 12 15:40:30 ubuntu 50-motd-news[1257]:  * Super-optimized for small spaces - read how we shrank the memory
Jul 12 15:40:30 ubuntu 50-motd-news[1257]:    footprint of MicroK8s to make it the smallest full K8s around.
Jul 12 15:40:30 ubuntu 50-motd-news[1257]:    https://ubuntu.com/blog/microk8s-memory-optimisation
Jul 12 15:40:30 ubuntu systemd[1]: motd-news.service: Succeeded.
Jul 12 15:40:30 ubuntu systemd[1]: Finished Message of the Day.
Jul 12 15:46:25 ubuntu systemd[1]: Starting Ubuntu Advantage APT and MOTD Messages...
Jul 12 15:46:25 ubuntu systemd[1]: ua-messaging.service: Succeeded.
Jul 12 15:46:25 ubuntu systemd[1]: Finished Ubuntu Advantage APT and MOTD Messages.
Jul 12 16:07:04 ubuntu sshd[1294]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2  user=jean
Jul 12 16:07:06 ubuntu sshd[1294]: Failed password for jean from 10.0.2.2 port 56484 ssh2
Jul 12 16:10:13 ubuntu sshd[1306]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2  user=jean
Jul 12 16:10:14 ubuntu sshd[1306]: Failed password for jean from 10.0.2.2 port 61977 ssh2
Jul 12 16:13:18 ubuntu sshd[1309]: Accepted password for jean from 10.0.2.2 port 54422 ssh2
Jul 12 16:13:18 ubuntu sshd[1309]: pam_unix(sshd:session): session opened for user jean by (uid=0)
Jul 12 16:13:18 ubuntu systemd[1]: Started Session 4 of user jean.
Jul 12 16:13:18 ubuntu systemd-logind[641]: New session 4 of user jean.
```

5. Open authentication log file (auth.log) and check the content. How can you print only lines from this log file to the CLI containing new sessions from your user (tip: use grep)?



```
jean@ubuntu:~$ cat /var/log/auth.log | grep "user jean"
Jul 12 14:42:27 ubuntu login[658]: pam_unix(login:session): session opened for user jean by LOGIN(uid=0)
Jul 12 14:42:28 ubuntu systemd-logind[641]: New session 1 of user jean.
Jul 12 14:42:28 ubuntu systemd: pam_unix(systemd-user:session): session opened for user jean by (uid=0)
Jul 12 16:13:18 ubuntu sshd[1309]: pam_unix(sshd:session): session opened for user jean by (uid=0)
Jul 12 16:13:18 ubuntu systemd-logind[641]: New session 4 of user jean.
Jul 12 16:20:45 ubuntu sshd[1439]: Disconnected from user jean 10.0.2.2 port 54422
Jul 12 16:20:45 ubuntu sshd[1309]: pam_unix(sshd:session): session closed for user jean
jean@ubuntu:~$
```

6. In previous exercise (EX-11) you installed Apache2 web server (if you haven’t, install it with sudo apt install apache2). What log files does this service have (see /var/log directory)?



```
jean@ubuntu:~$ cd /var/log/apache2
jean@ubuntu:/var/log/apache2$ ls
access.log  error.log  other_vhosts_access.log
jean@ubuntu:/var/log/apache2$
```