Week 5 Homework Submission File: Archiving and Logging Data

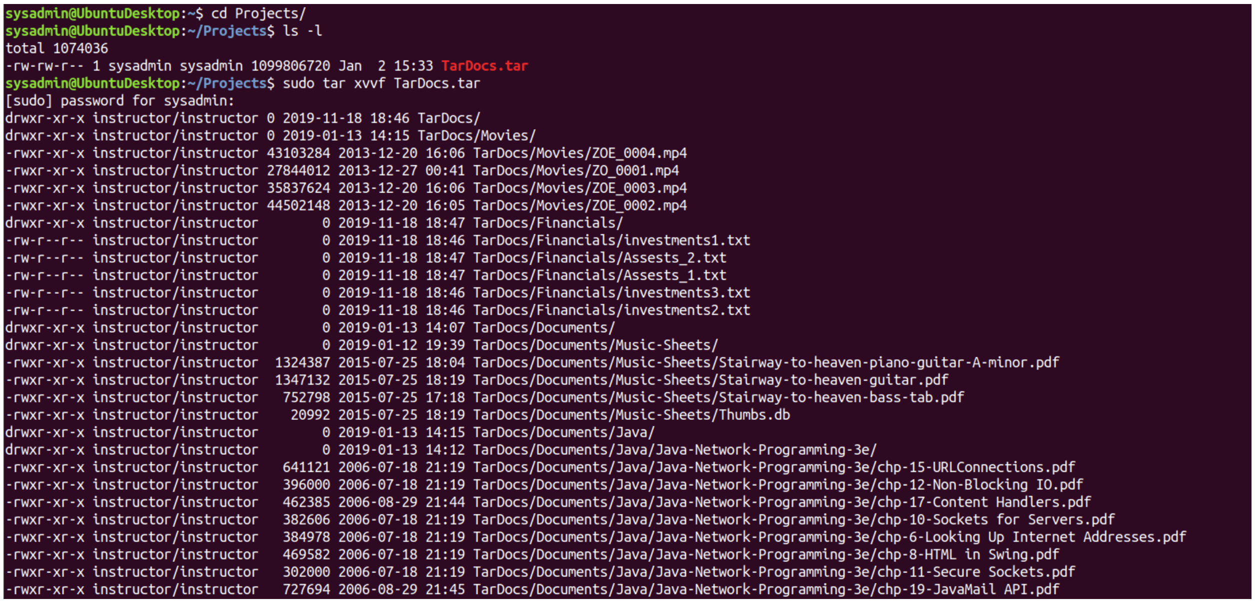
Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

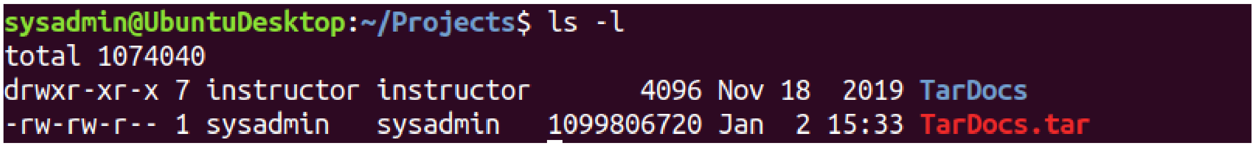
Step 1: Create, Extract, Compress, and Manage tar Backup Archives

1. Command to **extract** the TarDocs.tar archive to the current directory:

   sudo tar xvvf TarDocs.tar



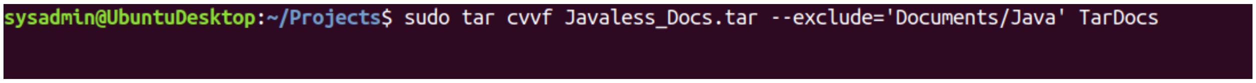
```
sysadmin@UbuntuDesktop:~$ cd Projects/
sysadmin@UbuntuDesktop:~/Projects$ ls -l
total 1074036
-rw-rw-r-- 1 sysadmin sysadmin 1099806720 Jan  2 15:33 TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ sudo tar xvvf TarDocs.tar
[sudo] password for sysadmin:
drwxr-xr-x instructor/instructor 0 2019-11-18 18:46 TarDocs/
drwxr-xr-x instructor/instructor 0 2019-01-13 14:15 TarDocs/Movies/
-rwxr-xr-x instructor/instructor 43103284 2013-12-20 16:06 TarDocs/Movies/ZOE_0004.mp4
-rwxr-xr-x instructor/instructor 27844012 2013-12-27 00:41 TarDocs/Movies/ZO_0001.mp4
-rwxr-xr-x instructor/instructor 35837624 2013-12-20 16:06 TarDocs/Movies/ZOE_0003.mp4
-rwxr-xr-x instructor/instructor 44502148 2013-12-20 16:05 TarDocs/Movies/ZOE_0002.mp4
drwxr-xr-x instructor/instructor        0 2019-11-18 18:47 TarDocs/Financials/
-rw-r--r-- instructor/instructor        0 2019-11-18 18:46 TarDocs/Financials/investments1.txt
-rw-r--r-- instructor/instructor        0 2019-11-18 18:47 TarDocs/Financials/Assests_2.txt
-rw-r--r-- instructor/instructor        0 2019-11-18 18:47 TarDocs/Financials/Assests_1.txt
-rw-r--r-- instructor/instructor        0 2019-11-18 18:46 TarDocs/Financials/investments3.txt
-rw-r--r-- instructor/instructor        0 2019-11-18 18:46 TarDocs/Financials/investments2.txt
drwxr-xr-x instructor/instructor        0 2019-01-13 14:07 TarDocs/Documents/
drwxr-xr-x instructor/instructor        0 2019-01-12 19:39 TarDocs/Documents/Music-Sheets/
-rwxr-xr-x instructor/instructor  1324387 2015-07-25 18:04 TarDocs/Documents/Music-Sheets/Stairway-to-heaven-piano-guitar-A-minor.pdf
-rwxr-xr-x instructor/instructor  1347132 2015-07-25 18:19 TarDocs/Documents/Music-Sheets/Stairway-to-heaven-guitar.pdf
-rwxr-xr-x instructor/instructor   752798 2015-07-25 17:18 TarDocs/Documents/Music-Sheets/Stairway-to-heaven-bass-tab.pdf
-rwxr-xr-x instructor/instructor    20992 2015-07-25 18:19 TarDocs/Documents/Music-Sheets/Thumbs.db
drwxr-xr-x instructor/instructor        0 2019-01-13 14:15 TarDocs/Documents/Java/
drwxr-xr-x instructor/instructor        0 2019-01-13 14:12 TarDocs/Documents/Java/Java-Network-Programming-3e/
-rwxr-xr-x instructor/instructor   641121 2006-07-18 21:19 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-15-URLConnections.pdf
-rwxr-xr-x instructor/instructor   396000 2006-07-18 21:19 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-12-Non-Blocking IO.pdf
-rwxr-xr-x instructor/instructor   462385 2006-08-29 21:44 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-17-Content Handlers.pdf
-rwxr-xr-x instructor/instructor   382606 2006-07-18 21:19 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-10-Sockets for Servers.pdf
-rwxr-xr-x instructor/instructor   384978 2006-07-18 21:19 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-6-Looking Up Internet Addresses.pdf
-rwxr-xr-x instructor/instructor   469582 2006-07-18 21:19 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-8-HTML in Swing.pdf
-rwxr-xr-x instructor/instructor   302000 2006-07-18 21:19 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-11-Secure Sockets.pdf
-rwxr-xr-x instructor/instructor   727694 2006-08-29 21:45 TarDocs/Documents/Java/Java-Network-Programming-3e/chp-19-JavaMail API.pdf
```



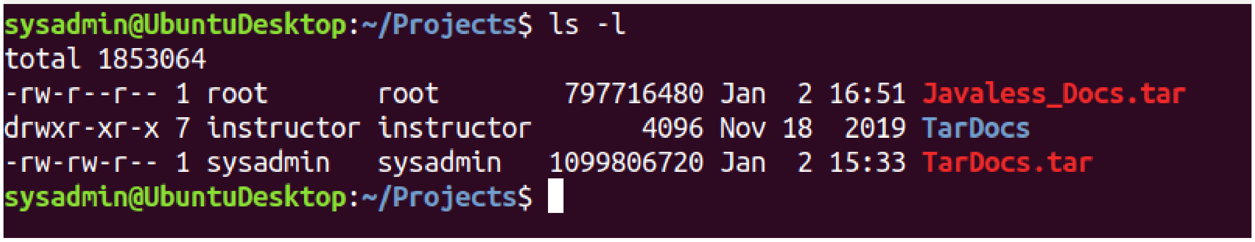
```
sysadmin@UbuntuDesktop:~/Projects$ ls -l
total 1074040
drwxr-xr-x 7 instructor instructor       4096 Nov 18  2019 TarDocs
-rw-rw-r-- 1 sysadmin   sysadmin   1099806720 Jan  2 15:33 TarDocs.tar
```

2. Command to **create** the Javaless_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:

   sudo tar cvvf Javaless_Docs.tar --exclude='Documents/Java' TarDocs



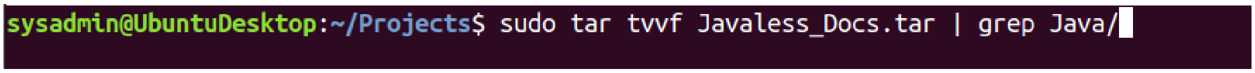
```
sysadmin@UbuntuDesktop:~/Projects$ sudo tar cvvf Javaless_Docs.tar --exclude='Documents/Java' TarDocs
```



```
sysadmin@UbuntuDesktop:~/Projects$ ls -l
total 1853064
-rw-r--r-- 1 root       root        797716480 Jan  2 16:51 Javaless_Docs.tar
drwxr-xr-x 7 instructor instructor       4096 Nov 18  2019 TarDocs
-rw-rw-r-- 1 sysadmin   sysadmin   1099806720 Jan  2 15:33 TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ 
```

3. Command to ensure Java/ is not in the new Javaless_Docs.tar archive:

   sudo tar tvvf Javaless_Docs.tar | grep Java/

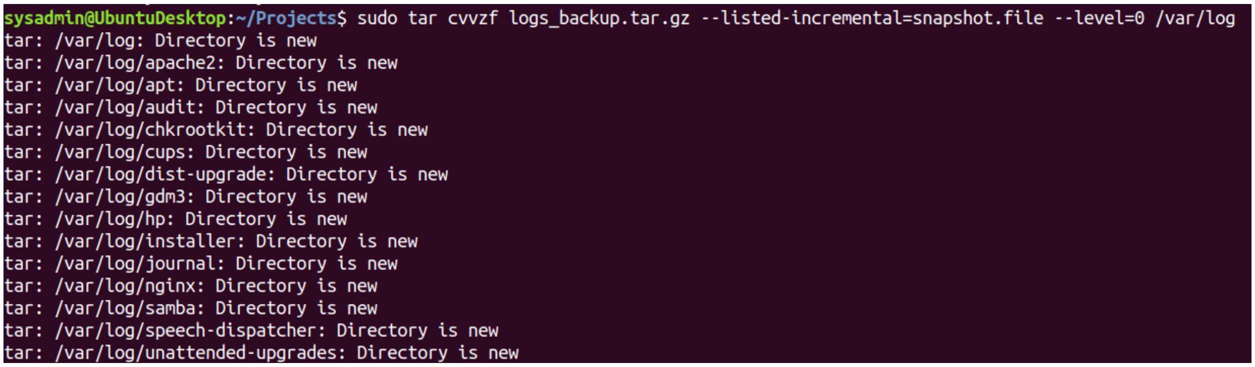


```
sysadmin@UbuntuDesktop:~/Projects$ sudo tar tvvf Javaless_Docs.tar | grep Java/
```

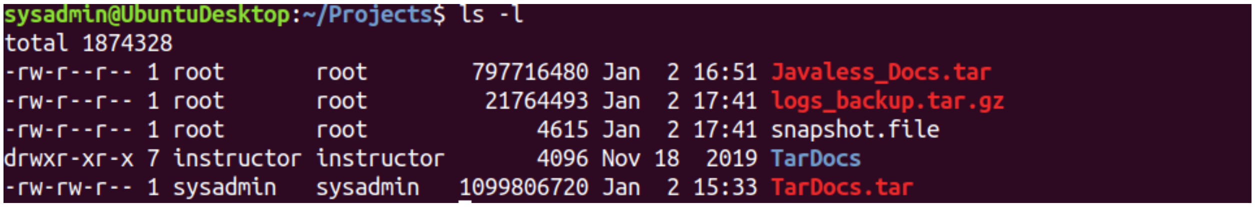
Bonus

- Command to create an incremental archive called logs_backup_tar.gz with only changed files to snapshot.file for the /var/log directory:

  sudo tar cvzf logs_backup.tar.gz --listed-incremental=snapshot.file --level=0 /var/log



```
sysadmin@UbuntuDesktop:~/Projects$ sudo tar cvvzf logs_backup.tar.gz --listed-incremental=snapshot.file --level=0 /var/log
tar: /var/log: Directory is new
tar: /var/log/apache2: Directory is new
tar: /var/log/apt: Directory is new
tar: /var/log/audit: Directory is new
tar: /var/log/chkrootkit: Directory is new
tar: /var/log/cups: Directory is new
tar: /var/log/dist-upgrade: Directory is new
tar: /var/log/gdm3: Directory is new
tar: /var/log/hp: Directory is new
tar: /var/log/installer: Directory is new
tar: /var/log/journal: Directory is new
tar: /var/log/nginx: Directory is new
tar: /var/log/samba: Directory is new
tar: /var/log/speech-dispatcher: Directory is new
tar: /var/log/unattended-upgrades: Directory is new
```



```
sysadmin@UbuntuDesktop:~/Projects$ ls -l
total 1874328
-rw-r--r-- 1 root       root        797716480 Jan  2 16:51 Javaless_Docs.tar
-rw-r--r-- 1 root       root         21764493 Jan  2 17:41 logs_backup.tar.gz
-rw-r--r-- 1 root       root             4615 Jan  2 17:41 snapshot.file
drwxr-xr-x 7 instructor instructor       4096 Nov 18  2019 TarDocs
-rw-rw-r-- 1 sysadmin   sysadmin   1099806720 Jan  2 15:33 TarDocs.tar
```

Critical Analysis Question

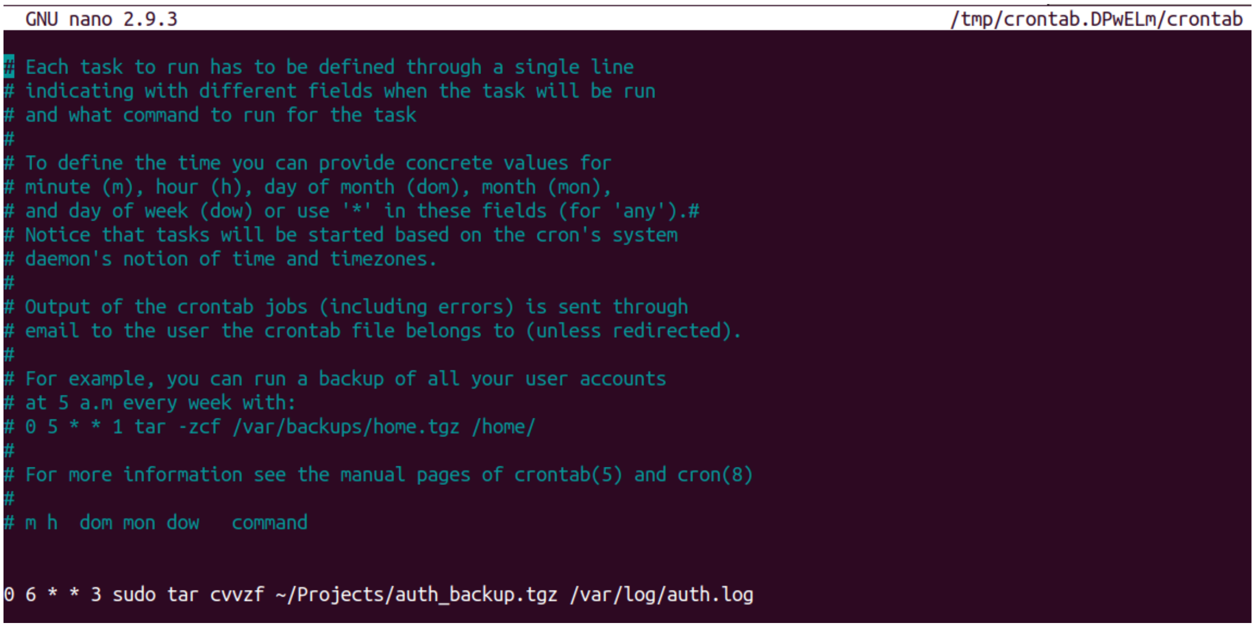
- Why wouldn't you use the options -x and -c at the same with tar?

  We do not use the options -x and -c at the same time with tar because "-c" refers to creating an archive file and "-x" refers to extracting an archive file. We can only only extract a file after archiving it.

Step 2: Create, Manage, and Automate Cron Jobs

1. Cron job for backing up the /var/log/auth.log file:

   *0 6 * * 3 sudo tar cvvzf ~/Projects/auth_backup.tgz /var/log/auth.log*

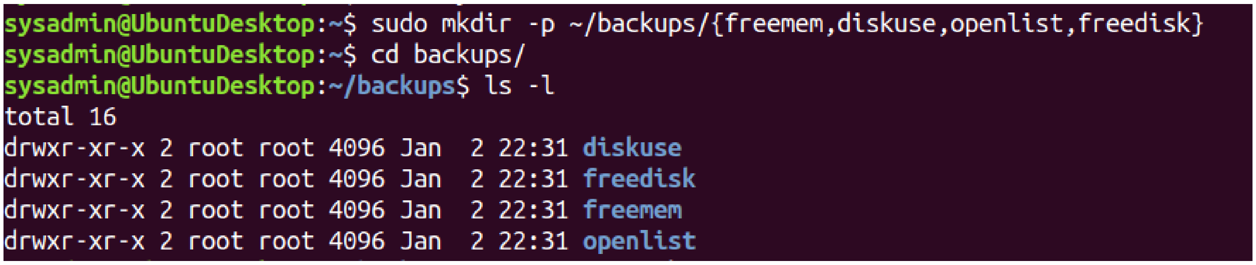


```
  GNU nano 2.9.3                                                                                      /tmp/crontab.DPwELm/crontab

# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command


0 6 * * 3 sudo tar cvvzf ~/Projects/auth_backup.tgz /var/log/auth.log
```

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

   sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}



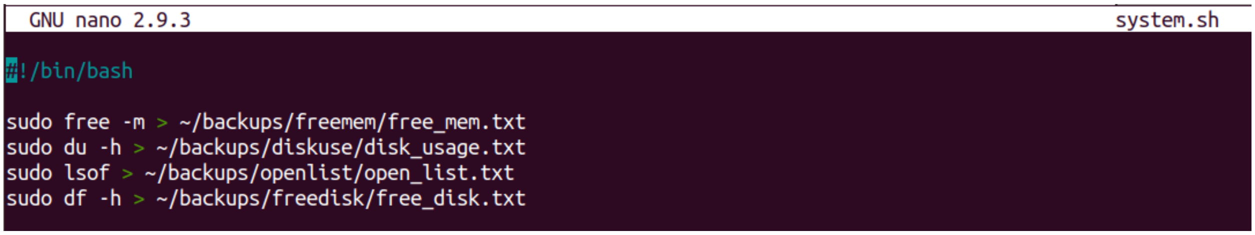
```
sysadmin@UbuntuDesktop:~$ sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}
sysadmin@UbuntuDesktop:~$ cd backups/
sysadmin@UbuntuDesktop:~/backups$ ls -l
total 16
drwxr-xr-x 2 root root 4096 Jan  2 22:31 diskuse
drwxr-xr-x 2 root root 4096 Jan  2 22:31 freedisk
drwxr-xr-x 2 root root 4096 Jan  2 22:31 freemem
drwxr-xr-x 2 root root 4096 Jan  2 22:31 openlist
```

Paste your system.sh script edits below:

nano system.sh

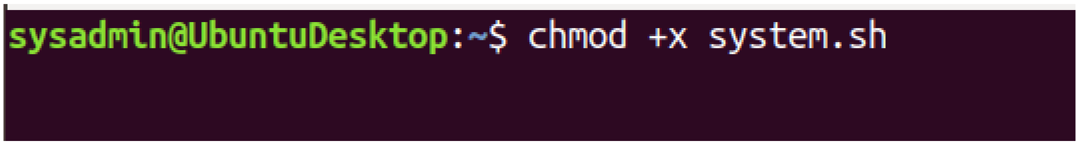
#!/bin/bash

sudo free -m > ~/backups/freemem/free_mem.txt
sudo du -h > ~/backups/diskuse/disk_usage.txt
sudo lsof > ~/backups/openlist/open_list.txt
sudo df -h > ~/backups/freedisk/free_disk.txt

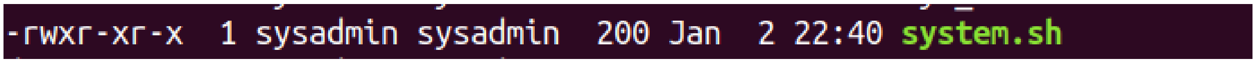


```
  GNU nano 2.9.3                                                                              system.sh

#!/bin/bash

sudo free -m > ~/backups/freemem/free_mem.txt
sudo du -h > ~/backups/diskuse/disk_usage.txt
sudo lsof > ~/backups/openlist/open_list.txt
sudo df -h > ~/backups/freedisk/free_disk.txt
```

2. Command to make the system.sh script executable:
   chmod +x system.sh



```
sysadmin@UbuntuDesktop:~$ chmod +x system.sh
```



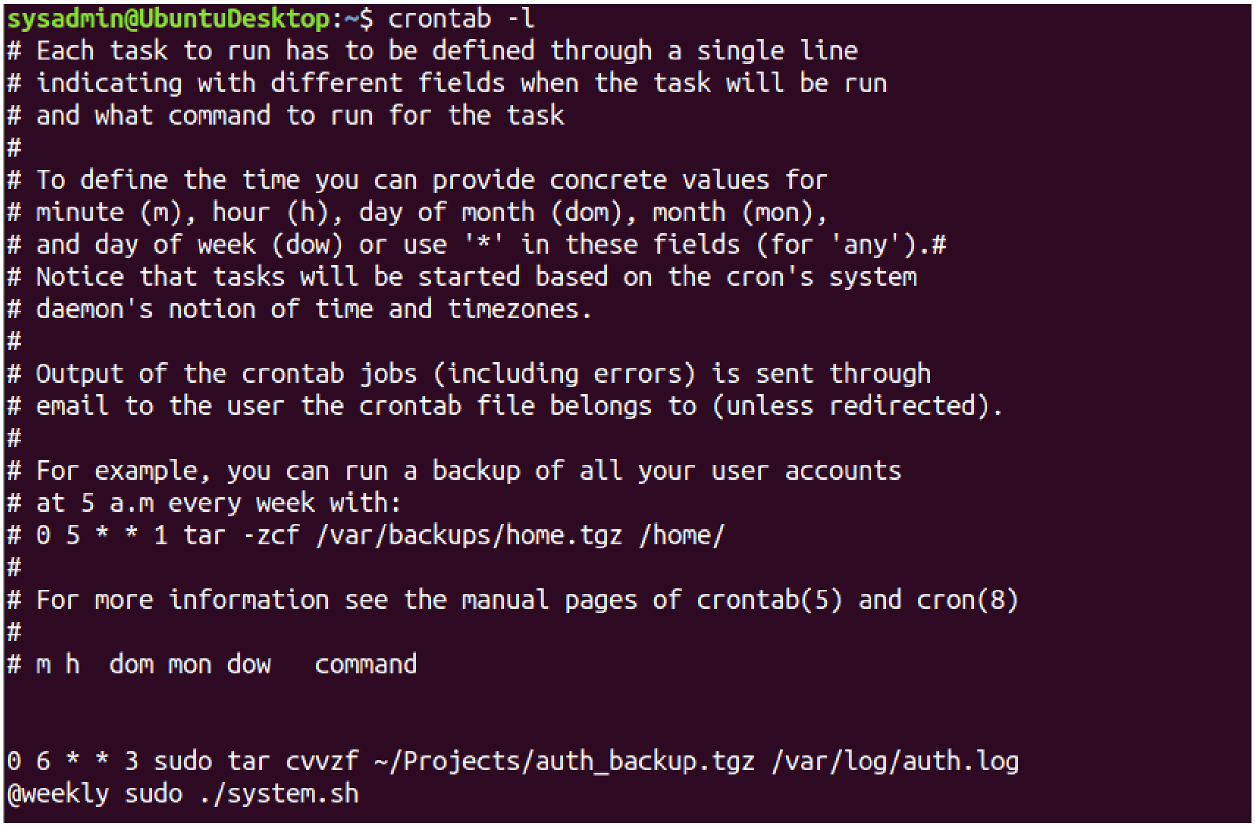
```
-rwxr-xr-x  1 sysadmin sysadmin  200 Jan  2 22:40 system.sh
```

Optional

- Commands to test the script and confirm its execution:

Bonus

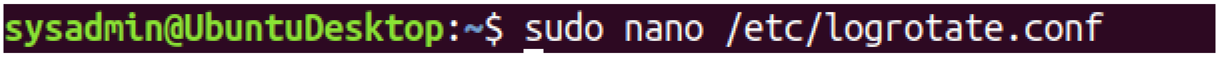
- Command to copy system to system-wide cron directory:
  @weekly sudo ./system.sh



```
sysadmin@UbuntuDesktop:~$ crontab -l
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command


0 6 * * 3 sudo tar cvvzf ~/Projects/auth_backup.tgz /var/log/auth.log
@weekly sudo ./system.sh
```

Step 4. Manage Log File Sizes

1. Run sudo nano /etc/logrotate.conf to edit the logrotate configuration file.
   sudo nano /etc/logrotate.conf

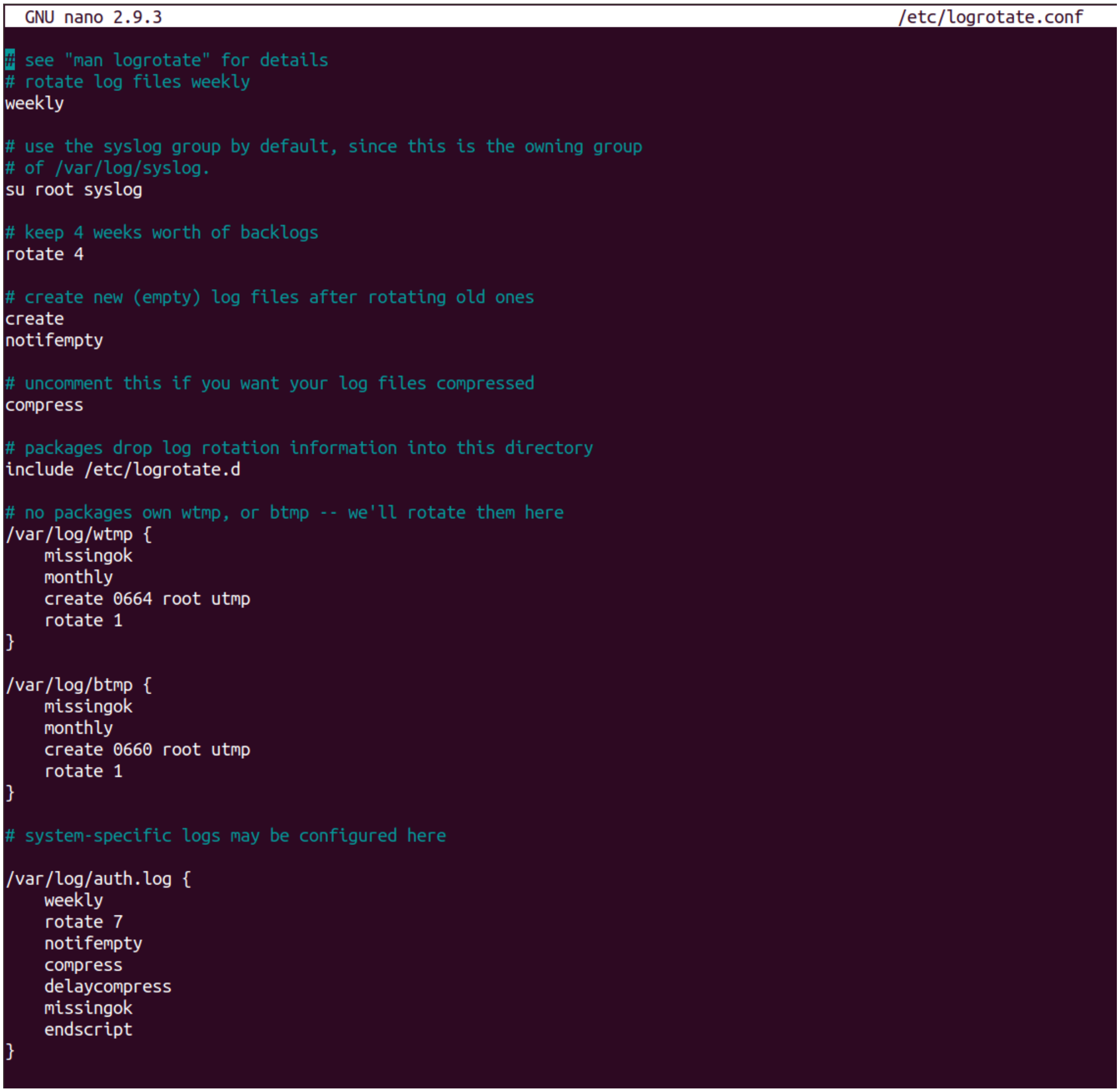


```
sysadmin@UbuntuDesktop:~$ sudo nano /etc/logrotate.conf
```

Configure a log rotation scheme that backs up authentication messages to the /var/log/auth.log.

- Add your config file edits below:

```
/var/log/auth.log {
        weekly
        rotate 7
        notifempty
        compress
        delaycompress
        missingok
        endscript
}
```

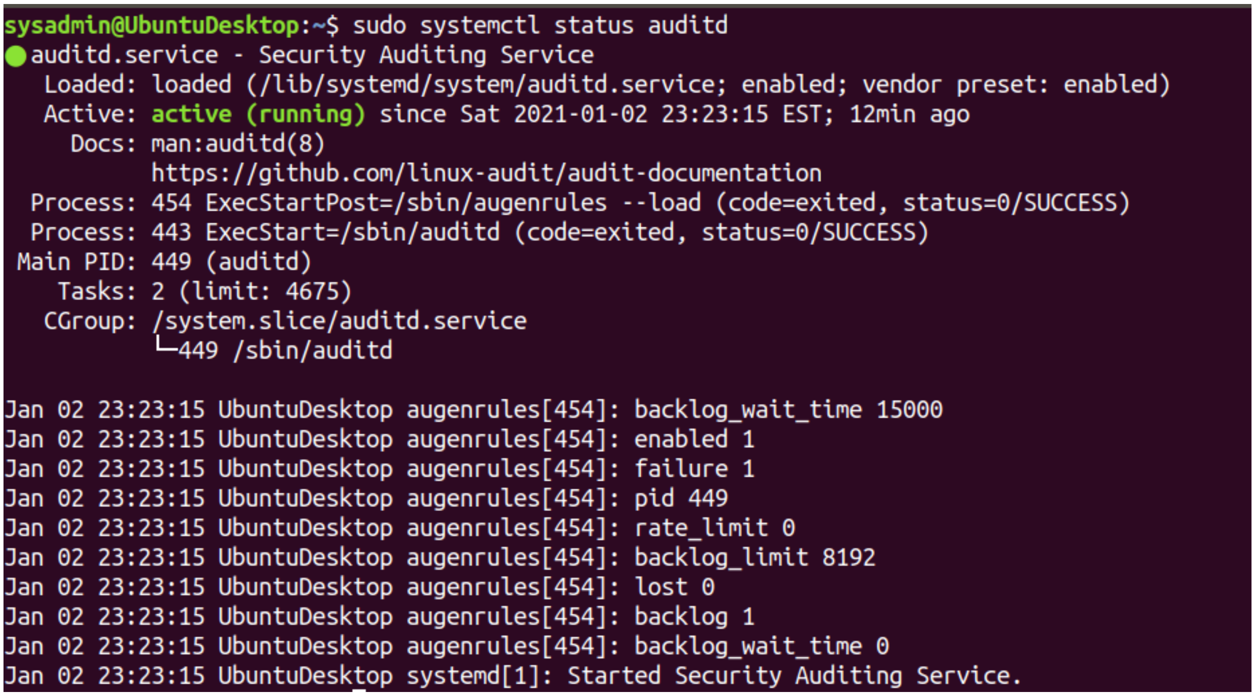


```
# see "man logrotate" for details
# rotate log files weekly
weekly

# use the syslog group by default, since this is the owning group
# of /var/log/syslog.
su root syslog

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create
notifempty

# uncomment this if you want your log files compressed
compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

# system-specific logs may be configured here

/var/log/auth.log {
    weekly
    rotate 7
    notifempty
    compress
    delaycompress
    missingok
    endscript
}
```

Bonus: Check for Policy and File Violations

1. Command to verify auditd is active:

   sudo systemctl status auditd

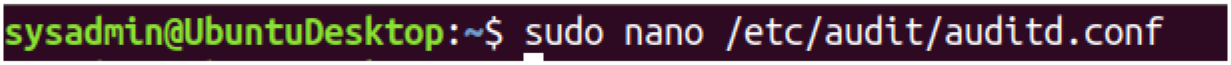


```
sysadmin@UbuntuDesktop:~$ sudo systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-01-02 23:23:15 EST; 12min ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
  Process: 454 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
  Process: 443 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
 Main PID: 449 (auditd)
    Tasks: 2 (limit: 4675)
   CGroup: /system.slice/auditd.service
           └─449 /sbin/auditd

Jan 02 23:23:15 UbuntuDesktop augenrules[454]: backlog_wait_time 15000
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: enabled 1
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: failure 1
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: pid 449
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: rate_limit 0
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: backlog_limit 8192
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: lost 0
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: backlog 1
Jan 02 23:23:15 UbuntuDesktop augenrules[454]: backlog_wait_time 0
Jan 02 23:23:15 UbuntuDesktop systemd[1]: Started Security Auditing Service.
```

2. Command to set number of retained logs and maximum log file size:

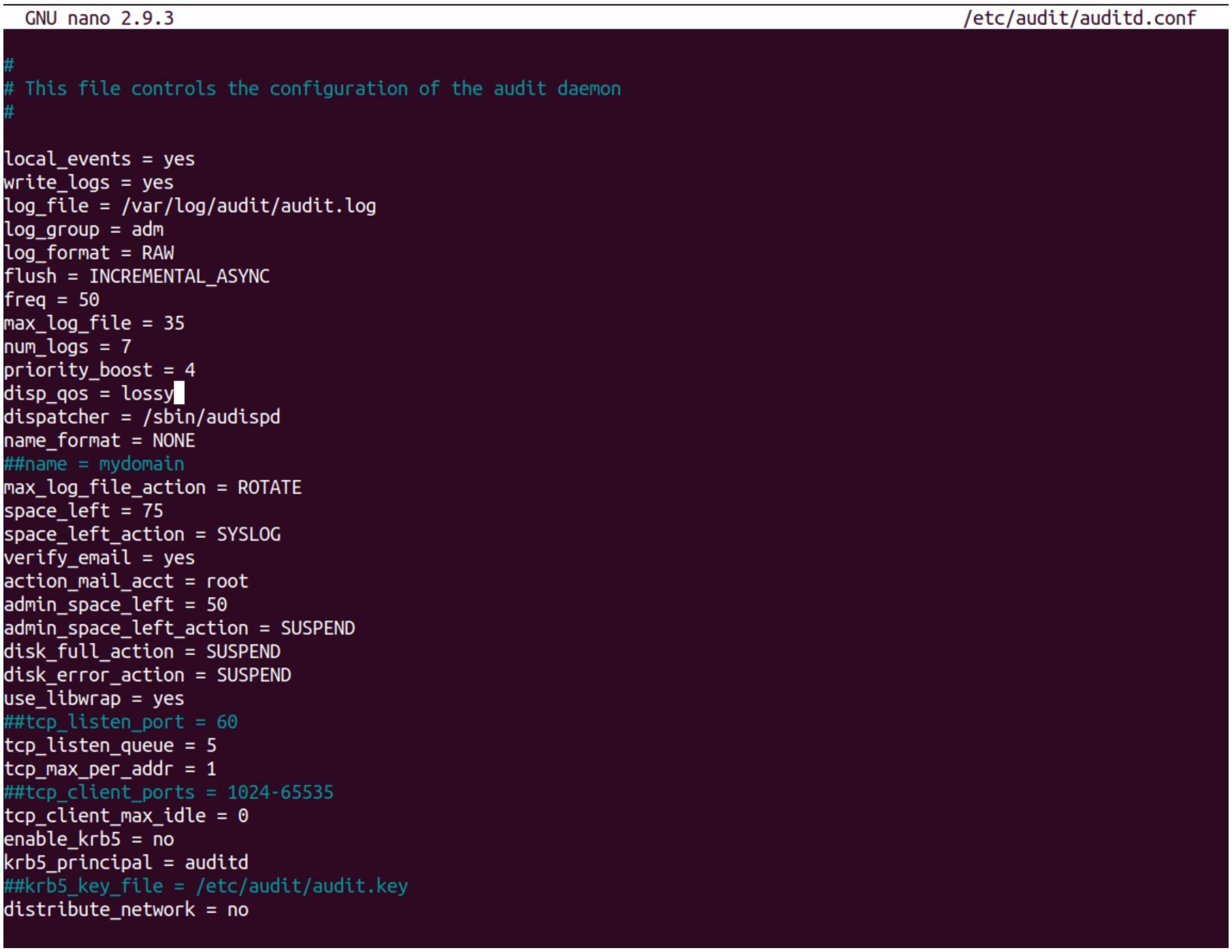
   sudo nano /etc/audit/auditd.conf

   Max_log_file = 35
   num_logs = 7



```
sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/auditd.conf
```

   ○ Add the edits made to the configuration file below:

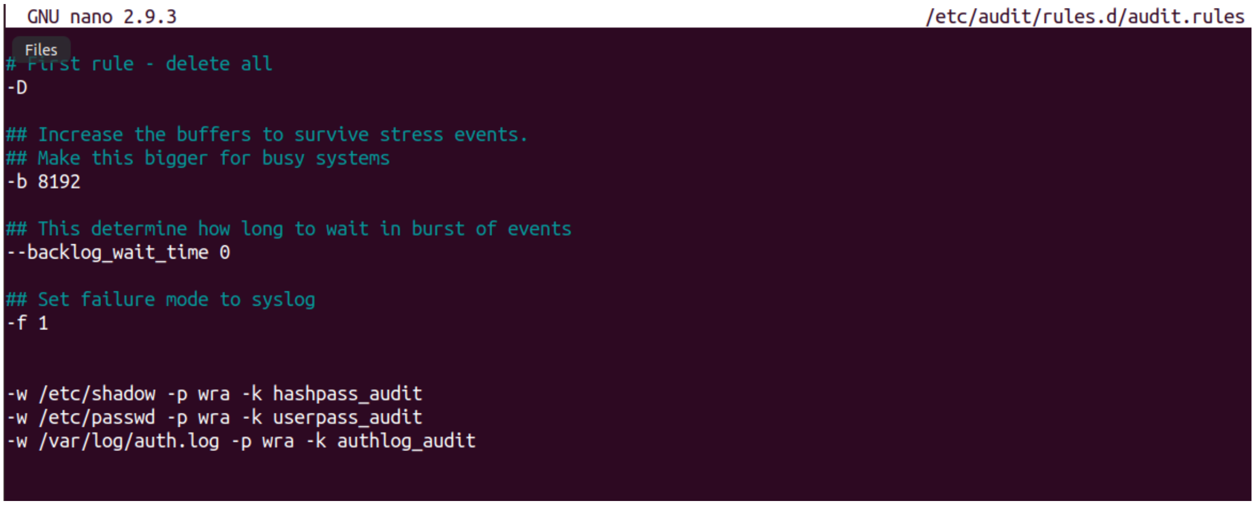


```
GNU nano 2.9.3                                                    /etc/audit/auditd.conf

#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 35
num_logs = 7
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
```

3. Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log:

   ○ Add the edits made to the rules file below:

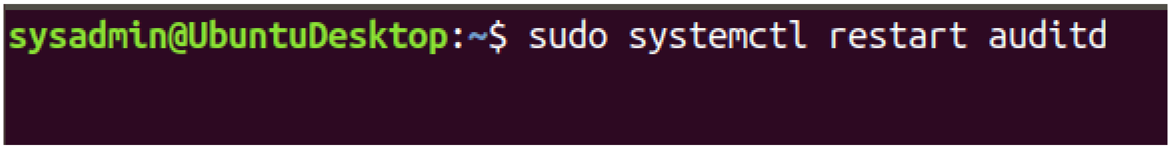
     -w /etc/shadow -p wra -k hashpass_audit
     -w /etc/passwd -p wra -k userpass_audit
     -w /var/log/auth.log -p wra -k authlog_audit



```
  GNU nano 2.9.3                                                          /etc/audit/rules.d/audit.rules

# First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 0

## Set failure mode to syslog
-f 1


-w /etc/shadow -p wra -k hashpass_audit
-w /etc/passwd -p wra -k userpass_audit
-w /var/log/auth.log -p wra -k authlog_audit
```

4. Command to restart auditd:

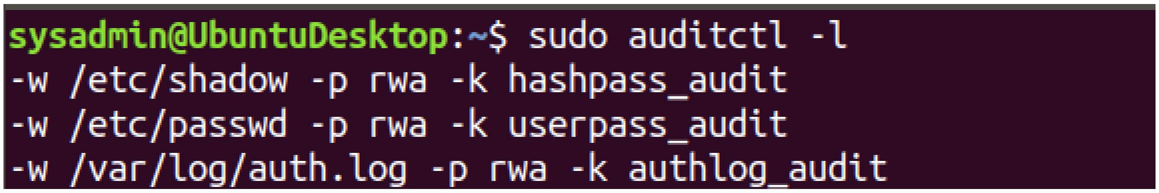
   sudo systemctl restart auditd



```
sysadmin@UbuntuDesktop:~$ sudo systemctl restart auditd
```

5. Command to list all auditd rules:

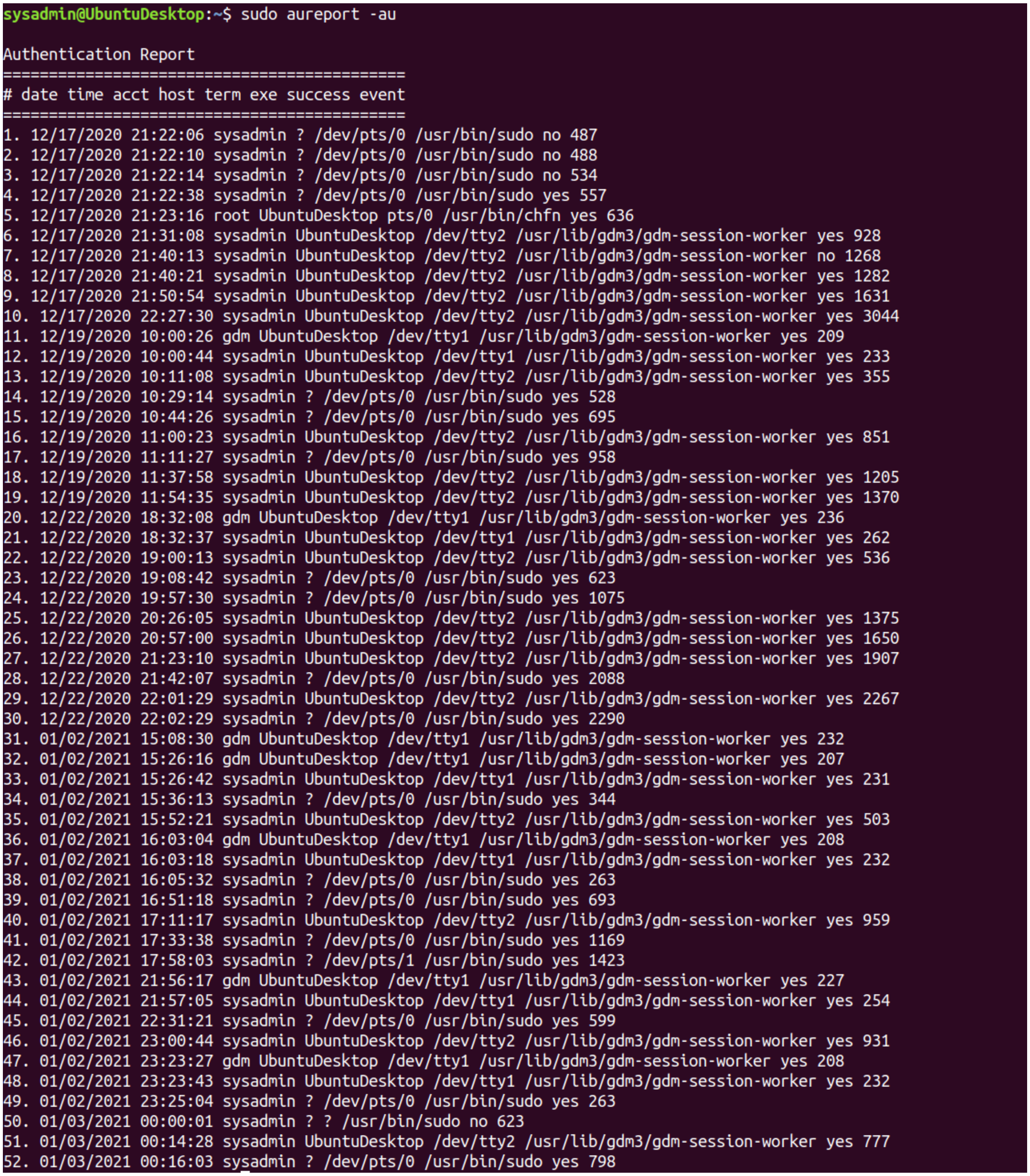
   sudo auditctl -l



```
sysadmin@UbuntuDesktop:~$ sudo auditctl -l
-w /etc/shadow -p rwa -k hashpass_audit
-w /etc/passwd -p rwa -k userpass_audit
-w /var/log/auth.log -p rwa -k authlog_audit
```

6. Command to produce an audit report:

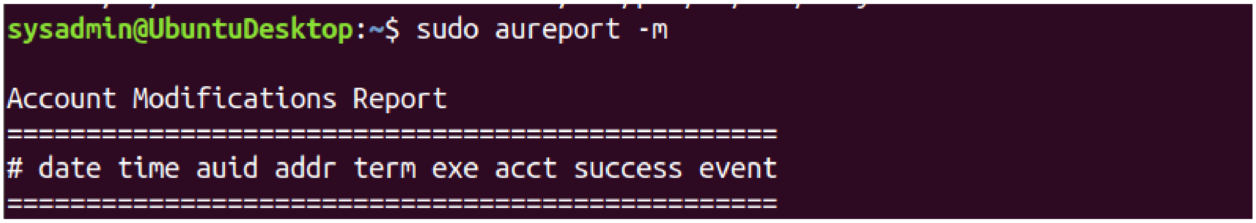
   sudo aureport -au



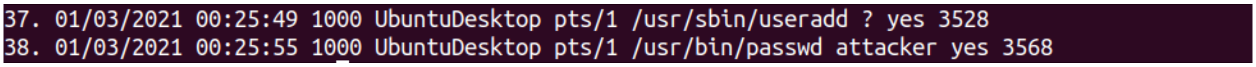
```
sysadmin@UbuntuDesktop:~$ sudo aureport -au

Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 12/17/2020 21:22:06 sysadmin ? /dev/pts/0 /usr/bin/sudo no 487
2. 12/17/2020 21:22:10 sysadmin ? /dev/pts/0 /usr/bin/sudo no 488
3. 12/17/2020 21:22:14 sysadmin ? /dev/pts/0 /usr/bin/sudo no 534
4. 12/17/2020 21:22:38 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 557
5. 12/17/2020 21:23:16 root UbuntuDesktop pts/0 /usr/bin/chfn yes 636
6. 12/17/2020 21:31:08 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 928
7. 12/17/2020 21:40:13 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 1268
8. 12/17/2020 21:40:21 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1282
9. 12/17/2020 21:50:54 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1631
10. 12/17/2020 22:27:30 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 3044
11. 12/19/2020 10:00:26 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 209
12. 12/19/2020 10:00:44 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 233
13. 12/19/2020 10:11:08 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 355
14. 12/19/2020 10:29:14 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 528
15. 12/19/2020 10:44:26 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 695
16. 12/19/2020 11:00:23 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 851
17. 12/19/2020 11:11:27 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 958
18. 12/19/2020 11:37:58 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1205
19. 12/19/2020 11:54:35 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1370
20. 12/22/2020 18:32:08 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 236
21. 12/22/2020 18:32:37 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 262
22. 12/22/2020 19:00:13 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 536
23. 12/22/2020 19:08:42 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 623
24. 12/22/2020 19:57:30 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 1075
25. 12/22/2020 20:26:05 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1375
26. 12/22/2020 20:57:00 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1650
27. 12/22/2020 21:23:10 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1907
28. 12/22/2020 21:42:07 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 2088
29. 12/22/2020 22:01:29 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 2267
30. 12/22/2020 22:02:29 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 2290
31. 01/02/2021 15:08:30 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 232
32. 01/02/2021 15:26:16 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 207
33. 01/02/2021 15:26:42 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 231
34. 01/02/2021 15:36:13 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 344
35. 01/02/2021 15:52:21 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 503
36. 01/02/2021 16:03:04 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 208
37. 01/02/2021 16:03:18 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 232
38. 01/02/2021 16:05:32 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 263
39. 01/02/2021 16:51:18 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 693
40. 01/02/2021 17:11:17 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 959
41. 01/02/2021 17:33:38 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 1169
42. 01/02/2021 17:58:03 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 1423
43. 01/02/2021 21:56:17 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 227
44. 01/02/2021 21:57:05 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 254
45. 01/02/2021 22:31:21 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 599
46. 01/02/2021 23:00:44 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 931
47. 01/02/2021 23:23:27 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 208
48. 01/02/2021 23:23:43 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 232
49. 01/02/2021 23:25:04 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 263
50. 01/03/2021 00:00:01 sysadmin ? ? /usr/bin/sudo no 623
51. 01/03/2021 00:14:28 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 777
52. 01/03/2021 00:16:03 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 798
```

7. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

   sudo aureport -m



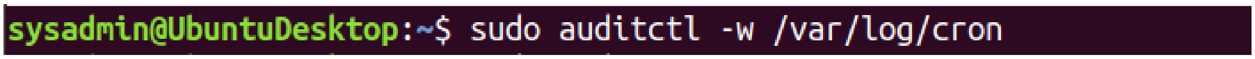
```
sysadmin@UbuntuDesktop:~$ sudo aureport -m

Account Modifications Report
=================================================
# date time auid addr term exe acct success event
=================================================
```



```
37. 01/03/2021 00:25:49 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 3528
38. 01/03/2021 00:25:55 1000 UbuntuDesktop pts/1 /usr/bin/passwd attacker yes 3568
```

8. Command to use auditd to watch /var/log/cron:

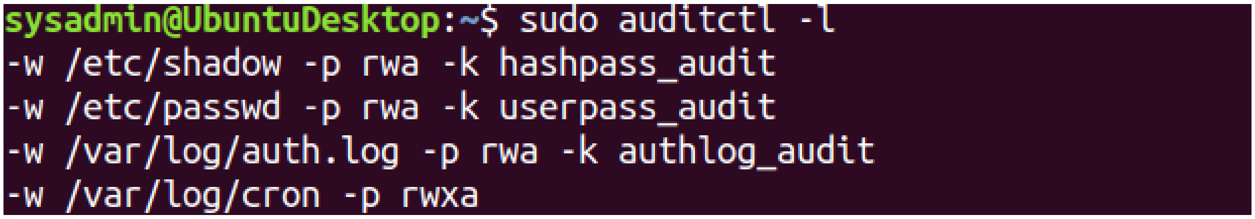
   sudo auditctl -w /var/log/cron



```
sysadmin@UbuntuDesktop:~$ sudo auditctl -w /var/log/cron
```

9. Command to verify auditd rules:

   sudo auditctl -l

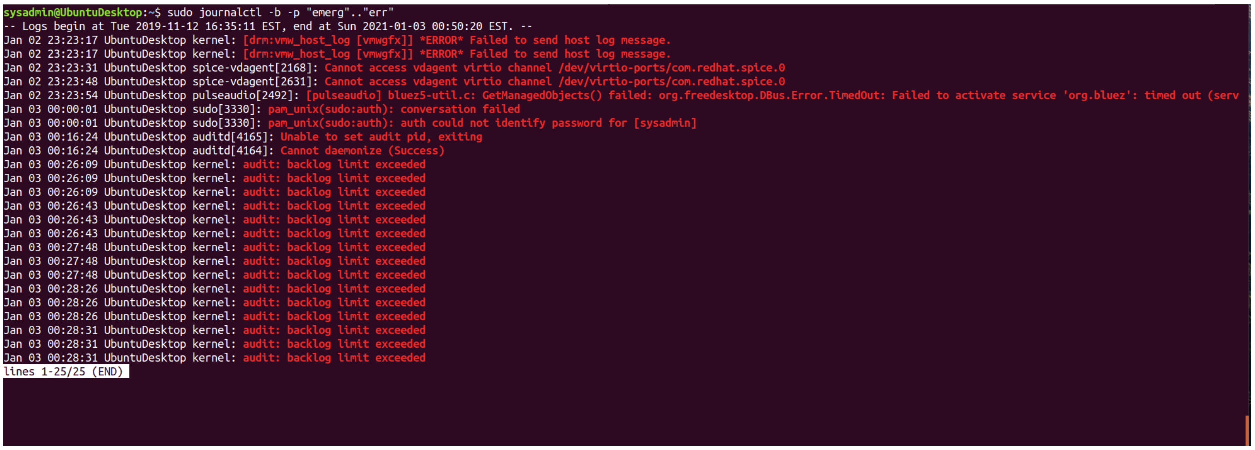


```
sysadmin@UbuntuDesktop:~$ sudo auditctl -l
-w /etc/shadow -p rwa -k hashpass_audit
-w /etc/passwd -p rwa -k userpass_audit
-w /var/log/auth.log -p rwa -k authlog_audit
-w /var/log/cron -p rwxa
```

Bonus (Research Activity): Perform Various Log Filtering Techniques

1. Command to return journalctl messages with priorities from emergency to error: **(enlarge screenshot to view)**

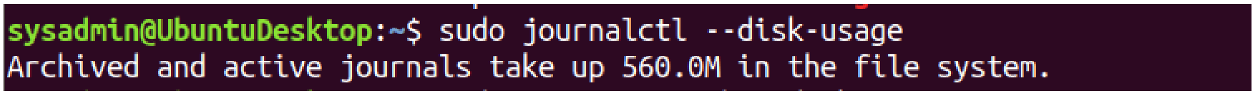
   sudo journalctl -b -p “emerg”..”err”



```
sysadmin@UbuntuDesktop:~$ sudo journalctl -b -p "emerg".."err"
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Sun 2021-01-03 00:50:20 EST. --
Jan 02 23:23:17 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Jan 02 23:23:17 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Jan 02 23:23:31 UbuntuDesktop spice-vdagent[2168]: Cannot access vdagent virtio channel /dev/virtio-ports/com.redhat.spice.0
Jan 02 23:23:48 UbuntuDesktop spice-vdagent[2631]: Cannot access vdagent virtio channel /dev/virtio-ports/com.redhat.spice.0
Jan 02 23:23:54 UbuntuDesktop pulseaudio[2492]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.TimedOut: Failed to activate service 'org.bluez': timed out (serv
Jan 03 00:00:01 UbuntuDesktop sudo[3330]: pam_unix(sudo:auth): conversation failed
Jan 03 00:00:01 UbuntuDesktop sudo[3330]: pam_unix(sudo:auth): auth could not identify password for [sysadmin]
Jan 03 00:16:24 UbuntuDesktop auditd[4165]: Unable to set audit pid, exiting
Jan 03 00:16:24 UbuntuDesktop auditd[4164]: Cannot daemonize (Success)
Jan 03 00:26:09 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:26:09 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:26:09 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:26:43 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:26:43 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:26:43 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:27:48 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:27:48 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:27:48 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:28:26 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:28:26 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:28:26 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:28:31 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:28:31 UbuntuDesktop kernel: audit: backlog limit exceeded
Jan 03 00:28:31 UbuntuDesktop kernel: audit: backlog limit exceeded
lines 1-25/25 (END)
```

2. Command to check the disk usage of the system journal unit since the most recent boot:

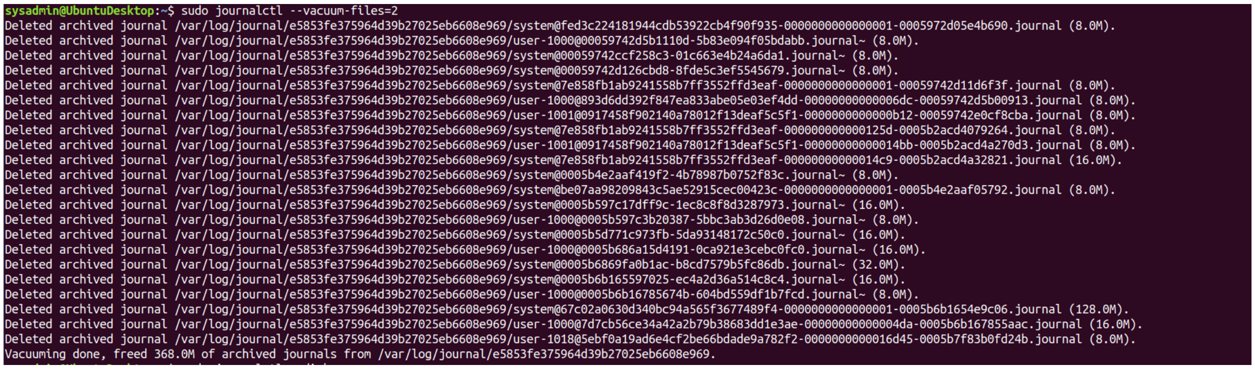
   sudo journalctl --disk-usage



```
sysadmin@UbuntuDesktop:~$ sudo journalctl --disk-usage
Archived and active journals take up 560.0M in the file system.
```

3. Command to remove all archived journal files except the most recent two: **(enlarge screenshot to view)**

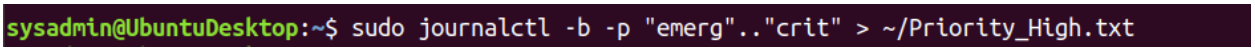
   sudo journalctl --vacuum-files=2



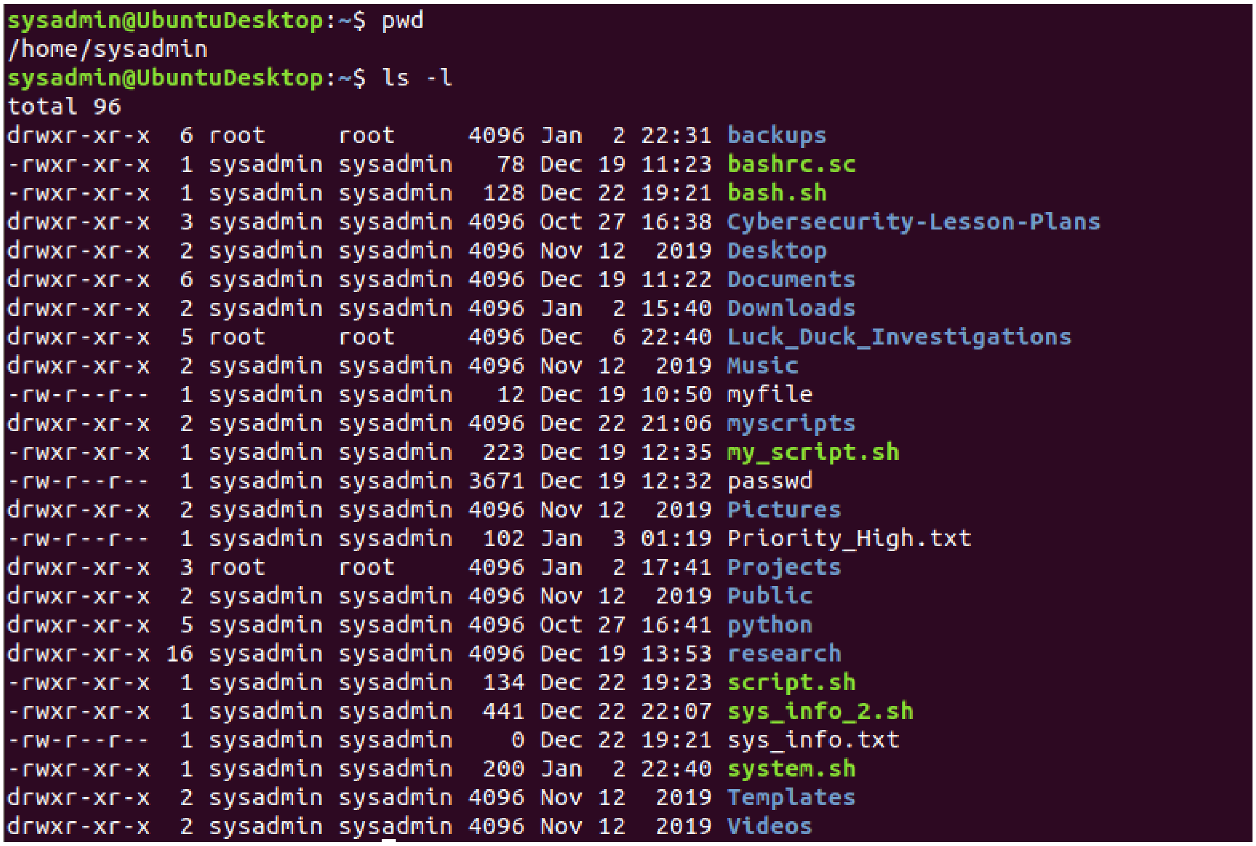
```
sysadmin@UbuntuDesktop:~$ sudo journalctl --vacuum-files=2
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@fed3c224181944cdb53922cb4f90f935-0000000000000001-0005972d05e4b690.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@00059742d5b1110d-5b83e094f05bdabb.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@00059742ccf258c3-01c663e4b24a6da1.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@00059742d126cbd8-8fde5c3ef5545679.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7ff3552ffd3eaf-0000000000000001-00059742d11d6f3f.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@893d6dd392f847ea833abe05e03ef4dd-00000000000006dc-00059742d5b00913.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1001@0917458f902140a78012f13deaf5c5f1-0000000000000b12-00059742e0cf8cba.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7ff3552ffd3eaf-000000000000125d-0005b2acd4079264.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1001@0917458f902140a78012f13deaf5c5f1-00000000000014bb-0005b2acd4a270d3.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7ff3552ffd3eaf-00000000000014c9-0005b2acd4a32821.journal (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005b4e2aaf419f2-4b78987b0752f83c.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@be07aa98209843c5ae52915cec00423c-0000000000000001-0005b4e2aaf05792.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005b597c17dff9c-1ec8c8f8d3287973.journal~ (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@0005b597c3b20387-5bbc3ab3d26d0e08.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005b5d771c973fb-5da93148172c50c0.journal~ (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@0005b686a15d4191-0ca921e3cebc0fc0.journal~ (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005b6869fa0b1ac-b8cd7579b5fc86db.journal~ (32.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005b6b165597025-ec4a2d36a514c8c4.journal~ (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@0005b6b16785674b-604bd559df1b7fcd.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@67c02a0630d340bc94a565f3677489f4-0000000000000001-0005b6b1654e9c06.journal (128.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@7d7cb56ce34a42a2b79b38683dd1e3ae-00000000000004da-0005b6b167855aac.journal (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1018@5ebf0a19ad6e4cf2be66bdade9a782f2-0000000000016d45-0005b7f83b0fd24b.journal (8.0M).
Vacuuming done, freed 368.0M of archived journals from /var/log/journal/e5853fe375964d39b27025eb6608e969.
```

4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority_High.txt:

   sudo journalctl -b -p “emerg”..”crit” > ~/Priority_High.txt



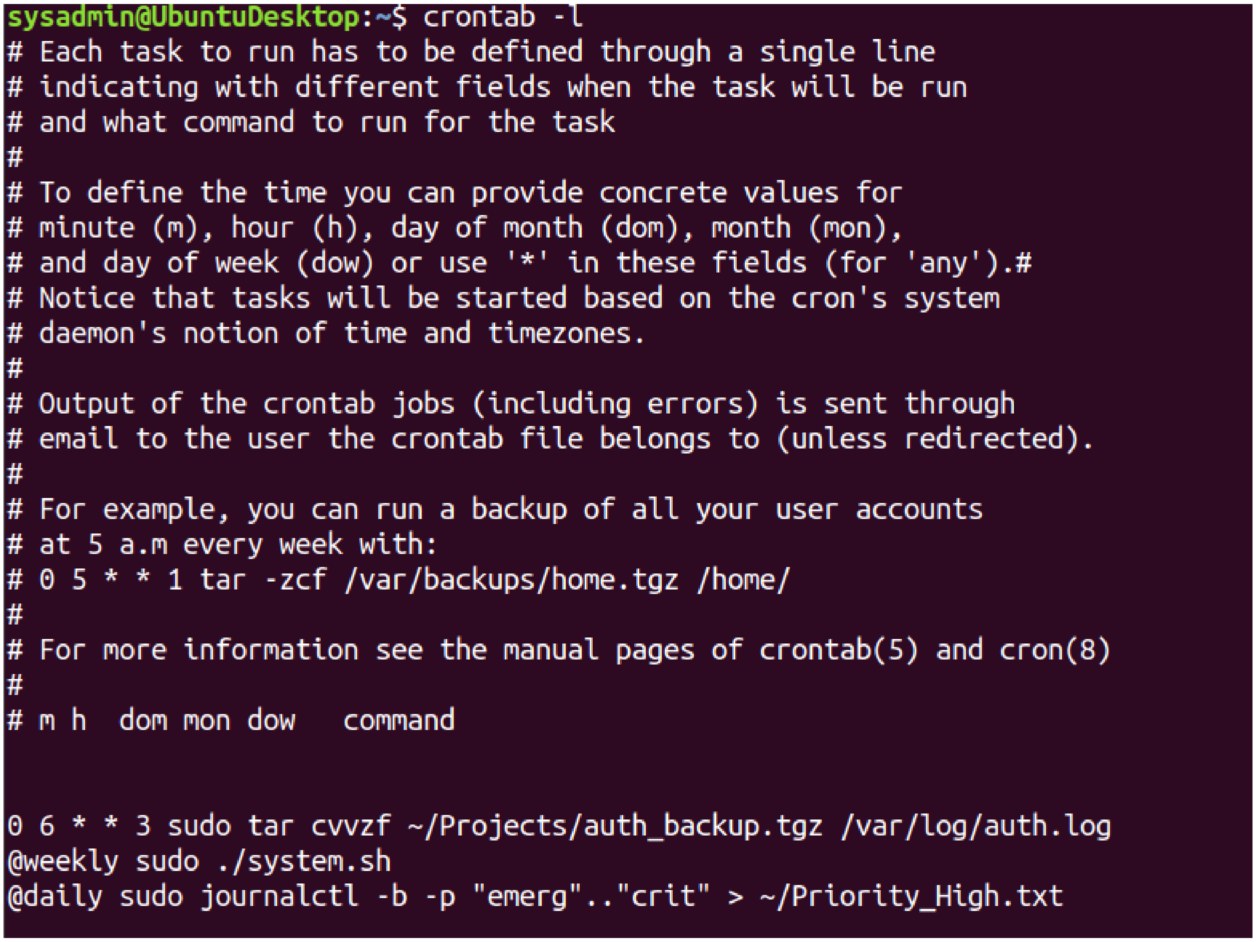
```
sysadmin@UbuntuDesktop:~$ sudo journalctl -b -p "emerg".."crit" > ~/Priority_High.txt
```



```
sysadmin@UbuntuDesktop:~$ pwd
/home/sysadmin
sysadmin@UbuntuDesktop:~$ ls -l
total 96
drwxr-xr-x  6 root     root     4096 Jan  2 22:31 backups
-rwxr-xr-x  1 sysadmin sysadmin   78 Dec 19 11:23 bashrc.sc
-rwxr-xr-x  1 sysadmin sysadmin  128 Dec 22 19:21 bash.sh
drwxr-xr-x  3 sysadmin sysadmin 4096 Oct 27 16:38 Cybersecurity-Lesson-Plans
drwxr-xr-x  2 sysadmin sysadmin 4096 Nov 12  2019 Desktop
drwxr-xr-x  6 sysadmin sysadmin 4096 Dec 19 11:22 Documents
drwxr-xr-x  2 sysadmin sysadmin 4096 Jan  2 15:40 Downloads
drwxr-xr-x  5 root     root     4096 Dec  6 22:40 Luck_Duck_Investigations
drwxr-xr-x  2 sysadmin sysadmin 4096 Nov 12  2019 Music
-rw-r--r--  1 sysadmin sysadmin   12 Dec 19 10:50 myfile
drwxr-xr-x  2 sysadmin sysadmin 4096 Dec 22 21:06 myscripts
-rwxr-xr-x  1 sysadmin sysadmin  223 Dec 19 12:35 my_script.sh
-rw-r--r--  1 sysadmin sysadmin 3671 Dec 19 12:32 passwd
drwxr-xr-x  2 sysadmin sysadmin 4096 Nov 12  2019 Pictures
-rw-r--r--  1 sysadmin sysadmin  102 Jan  3 01:19 Priority_High.txt
drwxr-xr-x  3 root     root     4096 Jan  2 17:41 Projects
drwxr-xr-x  2 sysadmin sysadmin 4096 Nov 12  2019 Public
drwxr-xr-x  5 sysadmin sysadmin 4096 Oct 27 16:41 python
drwxr-xr-x 16 sysadmin sysadmin 4096 Dec 19 13:53 research
-rwxr-xr-x  1 sysadmin sysadmin  134 Dec 22 19:23 script.sh
-rwxr-xr-x  1 sysadmin sysadmin  441 Dec 22 22:07 sys_info_2.sh
-rw-r--r--  1 sysadmin sysadmin    0 Dec 22 19:21 sys_info.txt
-rwxr-xr-x  1 sysadmin sysadmin  200 Jan  2 22:40 system.sh
drwxr-xr-x  2 sysadmin sysadmin 4096 Nov 12  2019 Templates
drwxr-xr-x  2 sysadmin sysadmin 4096 Nov 12  2019 Videos
```

5. Command to automate the last command in a daily cron job. Add the edits made to the crontab file below:

   Crontab -e
   @daily sudo journalctl -b -p “emerg”..”crit” > ~/Priority_High.txt



```
sysadmin@UbuntuDesktop:~$ crontab -l
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command


0 6 * * 3 sudo tar cvvzf ~/Projects/auth_backup.tgz /var/log/auth.log
@weekly sudo ./system.sh
@daily sudo journalctl -b -p "emerg".."crit" > ~/Priority_High.txt
```