

## ## Week 5 Homework Submission File: Archiving and Logging Data

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

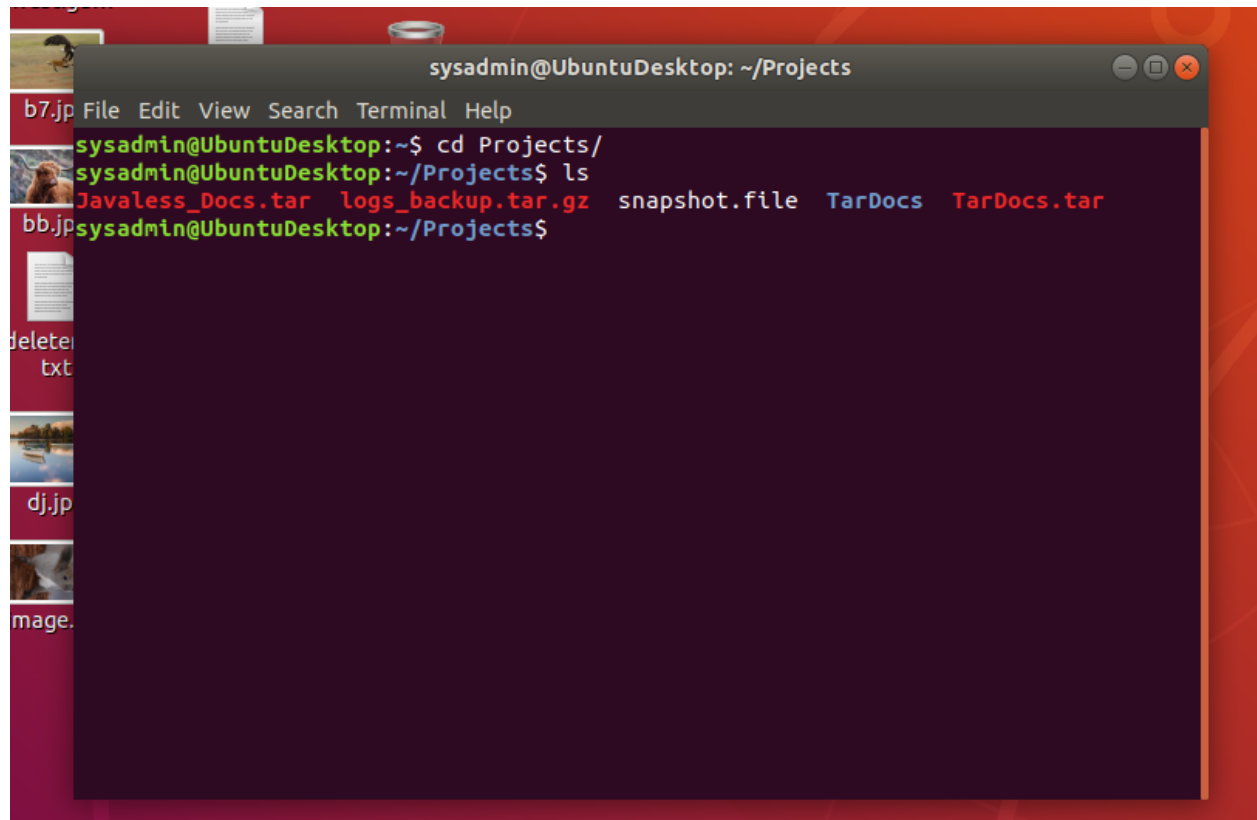
Save and submit the completed file for your homework submission.

---

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

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

**tar xvf TarDocs.tar**



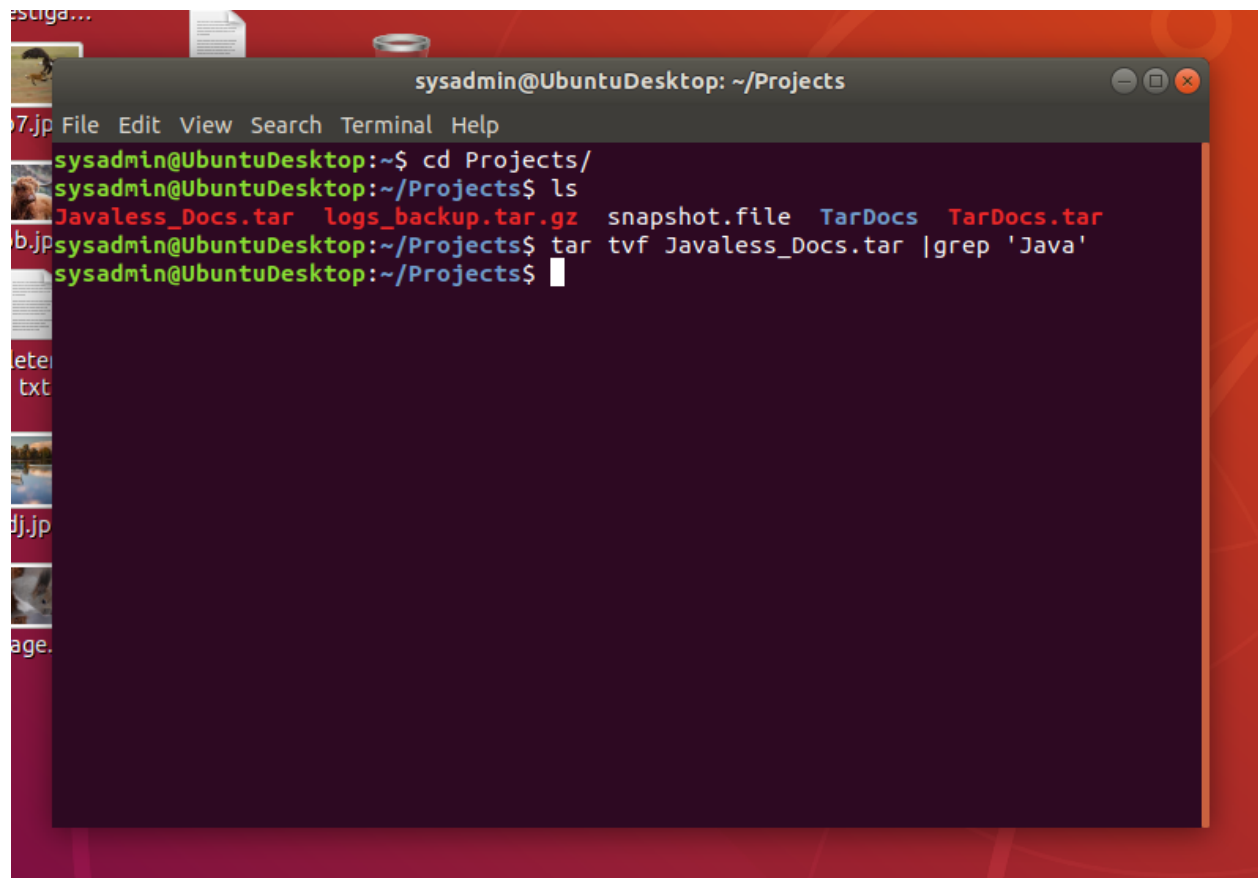
2. Command to **\*\*create\*\*** the `Javaless\_Doc.tar` archive from the `TarDocs/` directory, while excluding the `TarDocs/Documents/Java` directory:

**tar cvvf Javaless\_Docs.tar --exclude="Java" TarDocs**

```
sysadmin@UbuntuDesktop: ~/Projects
File Edit View Search Terminal Help
adrilateralCowboy/
drwxr-xr-x sysadmin/sysadmin      0 2019-01-12 19:40 TarDocs/Programs/Qu
adrilateralCowboy/base/
drwxr-xr-x sysadmin/sysadmin      0 2019-01-12 19:40 TarDocs/Programs/Qu
adrilateralCowboy/base/maps/
-rwxr-xr-x sysadmin/sysadmin 1665359 2018-01-12 22:45 TarDocs/Programs/Qu
adrilateralCowboy/base/maps/train.cm
-rwxr-xr-x sysadmin/sysadmin 228516082 2016-09-30 17:10 TarDocs/Programs/Qu
adrilateralCowboy/base/pak000.pk4
-rwxr-xr-x sysadmin/sysadmin 2905088 2016-09-30 17:00 TarDocs/Programs/Qu
adrilateralCowboy/base/gamex86.dll
-rwxr-xr-x sysadmin/sysadmin 15163 2016-04-02 00:17 TarDocs/Programs/Qu
adrilateralCowboy/icon.ico
-rwxr-xr-x sysadmin/sysadmin 4488192 2016-09-30 17:01 TarDocs/Programs/Qu
adrilateralCowboy/qc.exe
-rwxr-xr-x sysadmin/sysadmin 749568 2015-01-23 10:04 TarDocs/Programs/Qu
adrilateralCowboy/SDL2.dll
-rwxr-xr-x sysadmin/sysadmin 1128882 2016-07-16 00:14 TarDocs/Programs/Qu
adrilateralCowboy/quadrilateralcowboy_manual.pdf
-rwxr-xr-x sysadmin/sysadmin 2136 2018-01-12 22:45 TarDocs/Programs/Qu
adrilateralCowboy/unins000.dat
-rwxr-xr-x sysadmin/sysadmin 735909 2018-01-12 22:44 TarDocs/Programs/Qu
adrilateralCowboy/unins000.exe
sysadmin@UbuntuDesktop:~/Projects$ ls
Javaless_Docs.tar TarDocs TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$
```

3. Command to ensure `Java/` is not in the new `Javaless\_Docs.tar` archive:

```
tar tvf Javaless_Docs.tar |grep 'Java'
```

A terminal window titled 'sysadmin@UbuntuDesktop: ~/Projects' is shown. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows the user navigating to the 'Projects' directory and listing files. The files listed are 'Javaless\_Docs.tar', 'logs\_backup.tar.gz', 'snapshot.file', 'TarDocs', and 'TarDocs.tar'. The user then runs a command to search for 'Java' in 'Javaless\_Docs.tar' using 'tar tvf' and 'grep', but no output is shown.

```
sysadmin@UbuntuDesktop: ~$ cd Projects/
sysadmin@UbuntuDesktop: ~/Projects$ ls
Javaless_Docs.tar  logs_backup.tar.gz  snapshot.file  TarDocs  TarDocs.tar
sysadmin@UbuntuDesktop: ~/Projects$ tar tvf Javaless_Docs.tar |grep 'Java'
sysadmin@UbuntuDesktop: ~/Projects$
```

**\*\*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 cvf logs_backup.tar.gz --listed-incremental=snapshot.file /var/log/
```

```
sysadmin@UbuntuDesktop: ~/Projects
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ cd Projects/
sysadmin@UbuntuDesktop:~/Projects$ ls
Javaless_Docs.tar logs_backup.tar.gz snapshot.file TarDocs TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ tar tvf Javaless_Docs.tar |grep 'Java'
sysadmin@UbuntuDesktop:~/Projects$ cat snapshot.file
GNU tar-1.29-2
1634492862567826045016339486703473276012049273568/var/log/aptYeipp.log.xzYhistor
eteY.logYhistory.log.1.gzYhistory.log.2.gzYhistory.log.3.gzYhistory.log.4.gzYterm.l
xtogYterm.log.1.gzYterm.log.2.gzYterm.log.3.gzYterm.log.4.gz0162102426489416955204
9408219/var/log/samba/coresDnmbdDsmbd016210240518353428832049405615/var/log/unat
tended-upgradesYunattended-upgrades-shutdown.logYunattended-upgrades-shutdown.lo
g.1.gzYunattended-upgrades.logYunattended-upgrades.log.1.gz015735945124240000002
049405612/var/log/journalDe5853fe375964d39b27025eb6608e9690157359445954302946320
49393232/var/log/installerYcasper.logYdebugYinitial-status.gzYmedia-infoYpartman
YsyslogYtelemetryYversion0156503172002049405611/var/log/hpDtmp016340216567417296
22049404797/var/log/auditYaudit.logYaudit.log.1Yaudit.log.2Yaudit.log.3Yaudit.lo
g.40155056520602049405610/var/log/gdm30154879772102049402704/var/log/chkrootkit0
ge.1621024264894169552049658575/var/log/samba/cores/nmbd016344920505231800182049529
794/var/log/apache2Yaccess.logYerror.logYerror.log.1Yerror.log.2.gzYerror.log.3.
gzYerror.log.4.gzYerror.log.5.gzYerror.log.6.gzYerror.log.7.gzYerror.log.8.gzYer
ror.log.9.gzYother_vhosts_access.log0152041070202049405616/var/log/hp/tmp0163137
94356507519122049274178/var/log/nginxYaccess.logYerror.logYerror.log.10156096299
602049273570/var/log/dist-upgrade016344917802681243042049393242/var/log/journal/
e5853fe375964d39b27025eb6608e969Ysystem.journalYsystem@00059742ccf258c3-01c663e4
```

#### #### Critical Analysis Question

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

--- because you would be creating and extracting at the same time.

#### ### Step 2: Create, Manage, and Automate Cron Jobs

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

```
sysadmin@UbuntuDesktop: ~/Projects
File Edit View Search Terminal Help
GNU nano 2.9.3 /tmp/crontab.WjUmSC/crontab Modified
# 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 18 * * * /home/sysadmin/cleanup.sh
0 23 * * 5 tar cvvf ~/Documents/MedicalArchive/Medical_backup.tar.gz ~/research
5 23 * * 5 tar tvvWf ~/Documents/MedicalArchive/Medical_backup.tar.gz |less
0 4 * * * ls -l ~/Downloads > ~/Documents/Medical_files_list.txt
0 6 * * 3 tar cvvf /auth_backup.tgz /var/log/auth.log

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

### ### Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}  
sysadmin@UbuntuDesktop:~$ ls  
backups Downloads Pictures security  
cleanup.sh for_loops.sh Projects Security_scripts  
current_running_processes letter_script.sh Public system.sh  
Cybersecurity-Lesson-Plans month_script.sh python Templates  
Desktop Music research Videos  
Documents package_script.sh scripts  
sysadmin@UbuntuDesktop:~$ ls backups/  
diskuse freedisk freemem openlist  
sysadmin@UbuntuDesktop:~$
```

2. Paste your `system.sh` script edits below:

```
```bash  
#!/bin/bash  
[Your solution script contents here]  
```
```

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 system.sh
#!/bin/bash
sudo free -h >> ~/backups/freemem/free_mem.txt
sudo du -h >> ~/backups/diskuse/disk_usage.txt
sudo lsof >> ~/backups/openlist/open_list.txt
sudo df -h >> ~/backups/openlist/free_disk.txt

[ Read 6 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Linter ^_ Go To Line
```

3. Command to make the `system.sh` script executable:

`chmod +x system.sh`

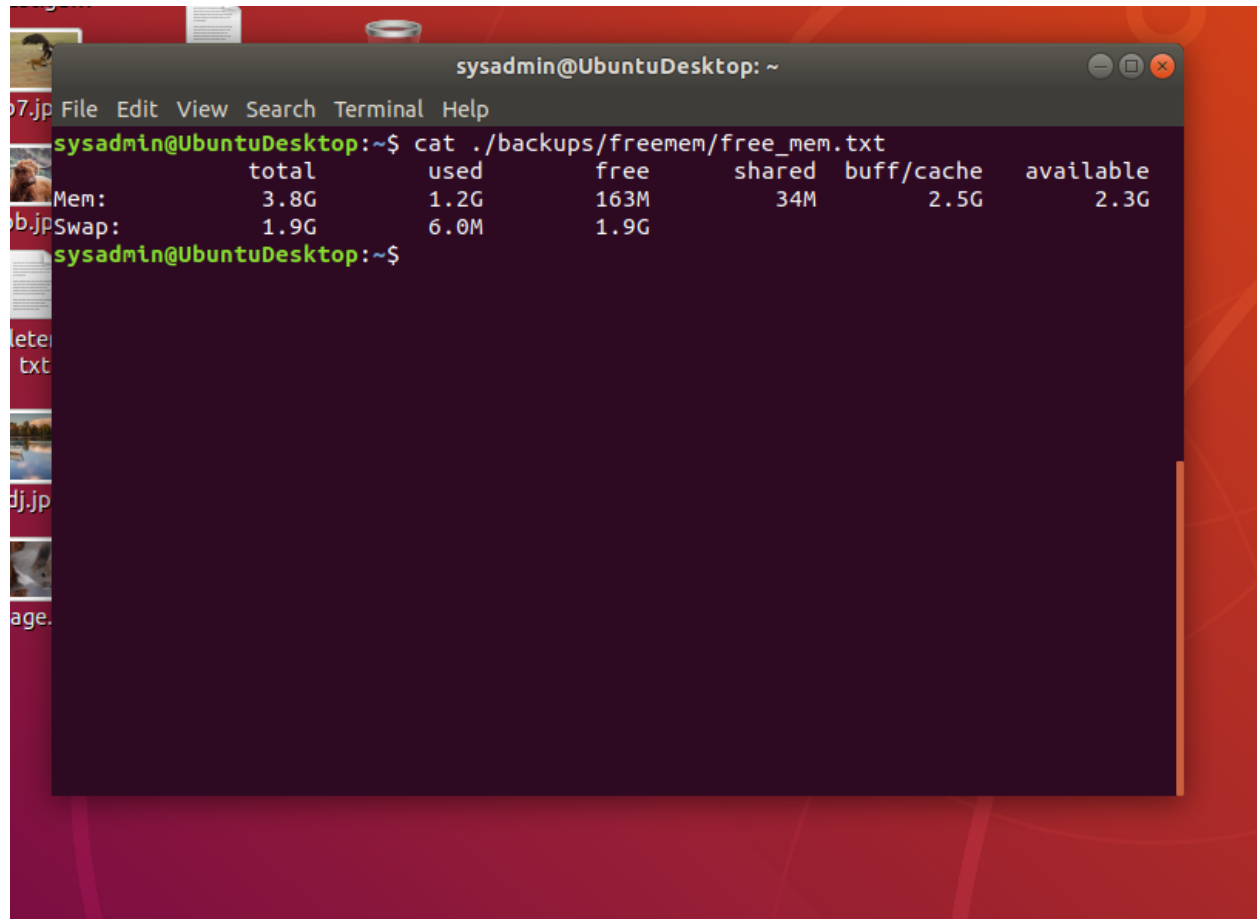
**\*\*Optional\*\***

- Commands to test the script and confirm its execution:

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ ls
backups Downloads Pictures security
cleanup.sh for_loops.sh Projects Security_scripts
current_running_processes letter_script.sh Public system.sh
Cybersecurity-Lesson-Plans month_script.sh python Templates
Desktop Music research Videos
Documents package_script.sh scripts
sysadmin@UbuntuDesktop:~$
```

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ sudo ./system.sh
ls: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
sysadmin@UbuntuDesktop:~$
```



A terminal window titled 'sysadmin@UbuntuDesktop: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is 'sysadmin@UbuntuDesktop:~\$'. The command 'cat ./backups/freemem/free\_mem.txt' has been executed, displaying memory statistics. The output shows 'Mem:' with 3.8G total, 1.2G used, 163M free, 34M shared, 2.5G buff/cache, and 2.3G available. 'Swap:' shows 1.9G total, 6.0M used, and 1.9G free. The prompt returns to 'sysadmin@UbuntuDesktop:~\$'.

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ cat ./backups/freemem/free_mem.txt
      total      used      free      shared  buff/cache   available
Mem:    3.8G    1.2G    163M        34M        2.5G        2.3G
Swap:   1.9G    6.0M    1.9G
sysadmin@UbuntuDesktop:~$
```

**\*\*Bonus\*\***

- Command to copy `system` to system-wide cron directory:

`sudo cp system.sh /etc/cron.weekly`

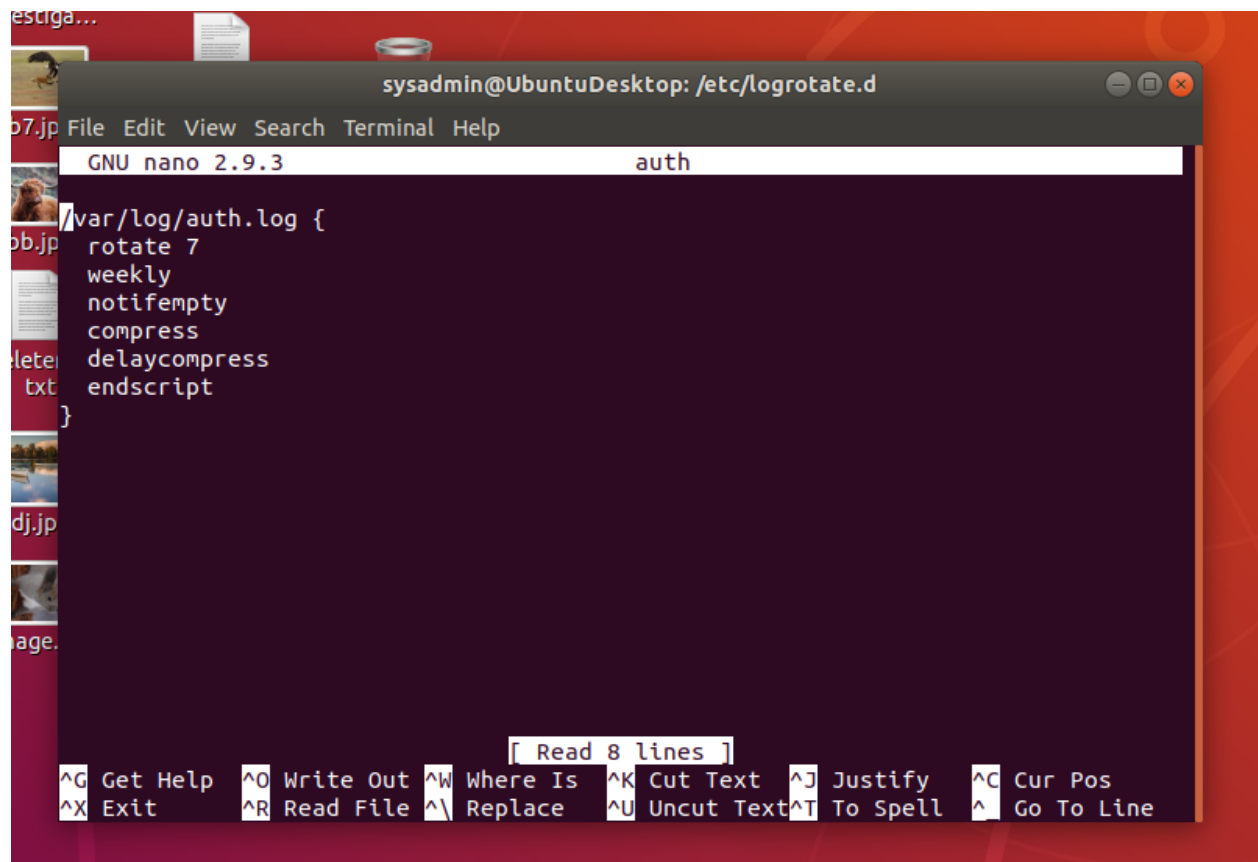
```
sysadmin@UbuntuDesktop: /etc/cron.weekly
b7.jp File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ cp system.sh /etc/cron.weekly
cp: cannot create regular file '/etc/cron.weekly/system.sh': Permission denied
sysadmin@UbuntuDesktop:~$ sudo cp system.sh /etc/cron.weekly
sysadmin@UbuntuDesktop:~$ etc
sysadmin@UbuntuDesktop:/etc$ cd cron.weekly/
sysadmin@UbuntuDesktop:/etc/cron.weekly$ ls
anacron  lynis-system.sh  system.sh  update.sh
backup.sh  man-db  update-notifier-common
sysadmin@UbuntuDesktop:/etc/cron.weekly$
```

---

### ### Step 4. Manage Log File Sizes

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

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



```
sysadmin@UbuntuDesktop: /etc/logrotate.d
GNU nano 2.9.3 auth
/var/log/auth.log {
  rotate 7
  weekly
  notifempty
  compress
  delaycompress
  endscrip
}

[ Read 8 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

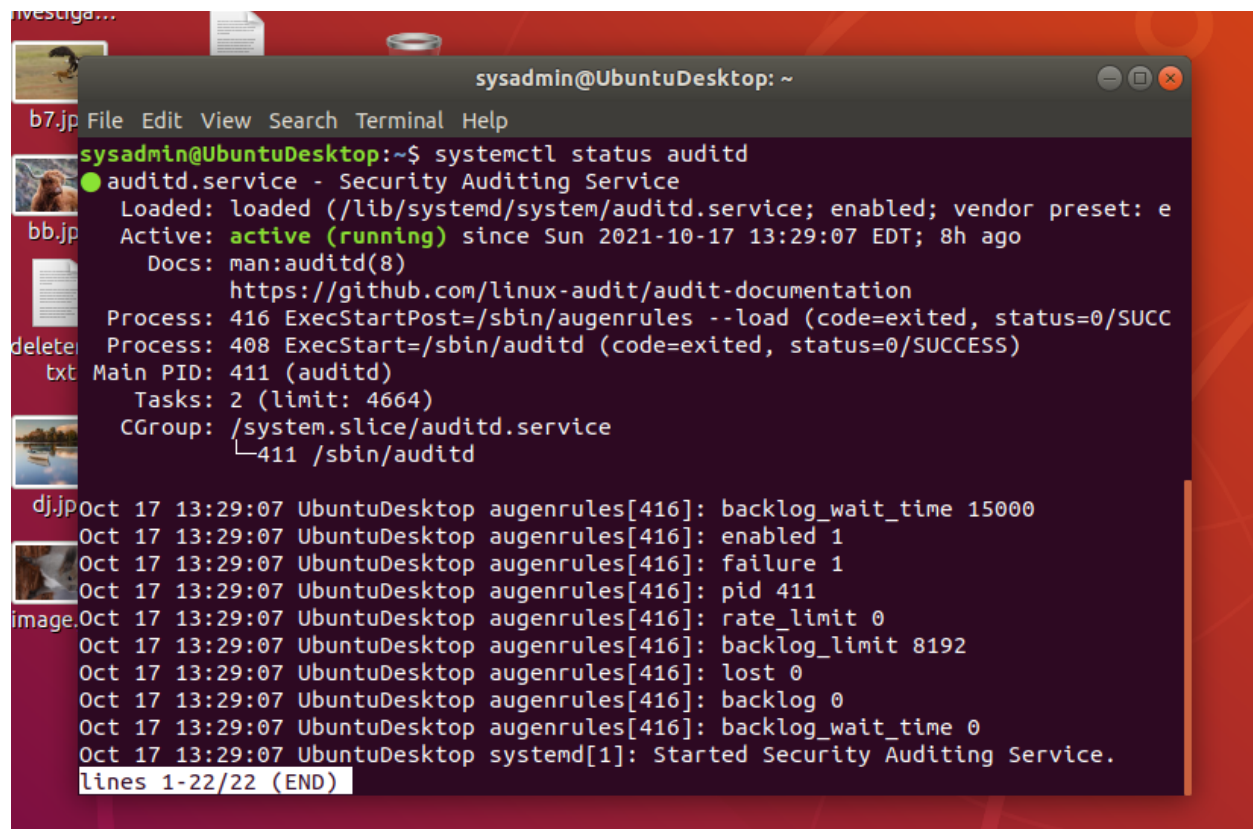
- Add your config file edits below:

```
```bash
[Your logrotate scheme edits here]
```
```

---

### Bonus: Check for Policy and File Violations

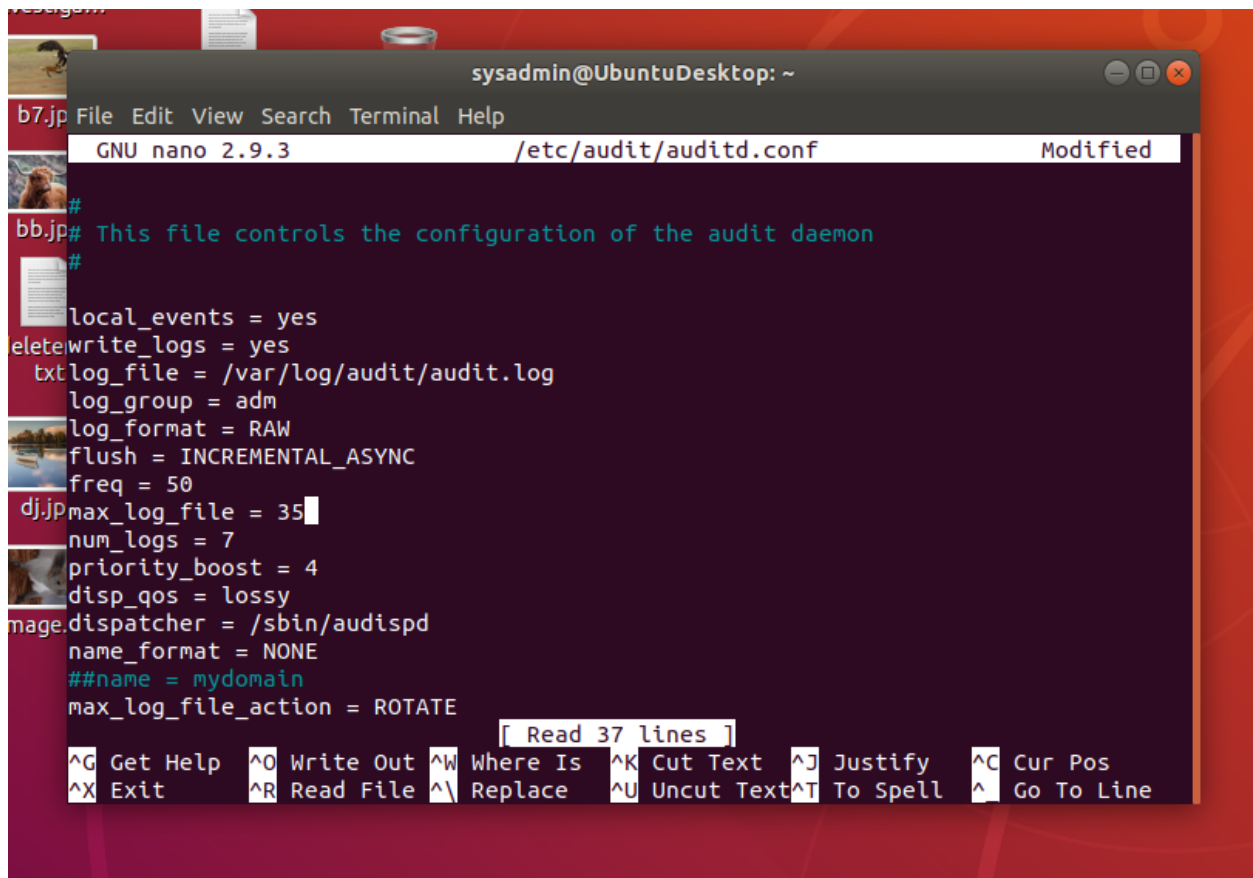
1. Command to verify `auditd` is active:

A terminal window titled 'sysadmin@UbuntuDesktop: ~' is open on a desktop background. The window shows the output of the 'systemctl status auditd' command. The output indicates that the 'auditd.service' is active and running. It provides details about the service's loaded state, active status, documentation link, process information, and various audit rules. The terminal text is as follows:

```
sysadmin@UbuntuDesktop:~$ systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: e
   Active: active (running) since Sun 2021-10-17 13:29:07 EDT; 8h ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 416 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCC
   Process: 408 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Main PID: 411 (auditd)
       Tasks: 2 (limit: 4664)
      CGroup: /system.slice/auditd.service
              └─411 /sbin/auditd

Oct 17 13:29:07 UbuntuDesktop augenrules[416]: backlog_wait_time 15000
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: enabled 1
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: failure 1
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: pid 411
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: rate_limit 0
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: backlog_limit 8192
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: lost 0
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: backlog 0
Oct 17 13:29:07 UbuntuDesktop augenrules[416]: backlog_wait_time 0
Oct 17 13:29:07 UbuntuDesktop systemd[1]: Started Security Auditing Service.
lines 1-22/22 (END)
```

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

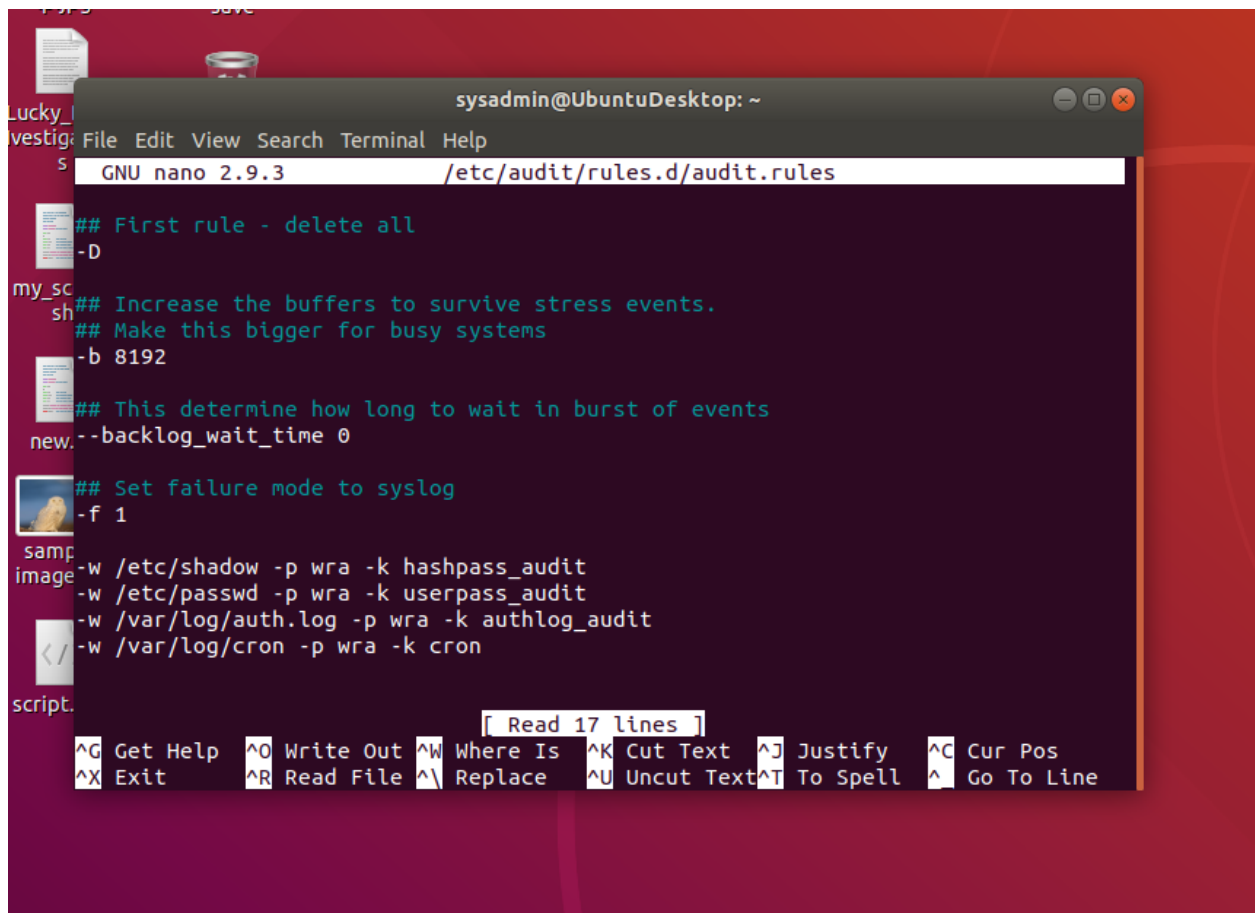


```
sysadmin@UbuntuDesktop: ~
b7.jp File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/audit/auditd.conf Modified
#
bb.jp# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
dj.jpmax_log_file = 35
num_logs = 7
priority_boost = 4
disp_qos = lossy
mage.dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
[ Read 37 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

- Add the edits made to the configuration file below:

```
```bash
[Your solution edits here]
```
```

3. Command using `auditd` to set rules for `/etc/shadow`, `/etc/passwd` and `/var/log/auth.log`:  
`sudo nano /etc/audit/rules.d/audit.rules`



```
sysadmin@UbuntuDesktop: ~
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

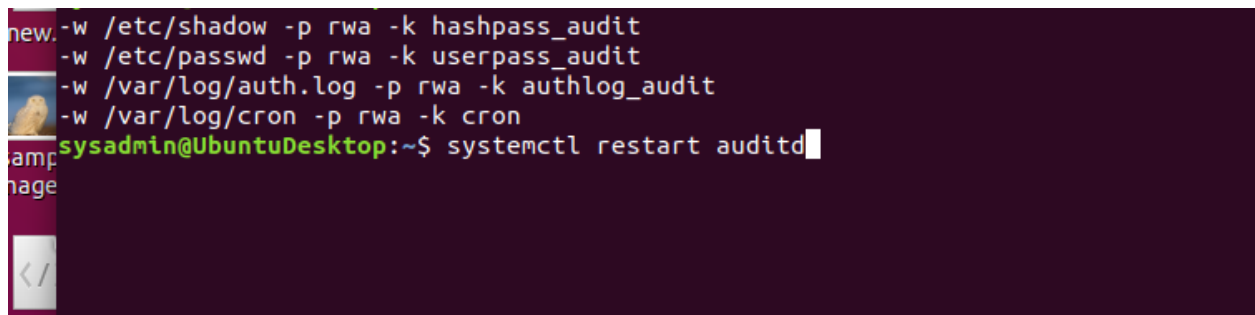
-w /etc/shadow -p wra -k hashpass_audit
-w /etc/passwd -p wra -k userpass_audit
-w /var/log/auth.log -p wra -k authlog_audit
-w /var/log/cron -p wra -k cron

[ Read 17 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

- Add the edits made to the `rules` file below:

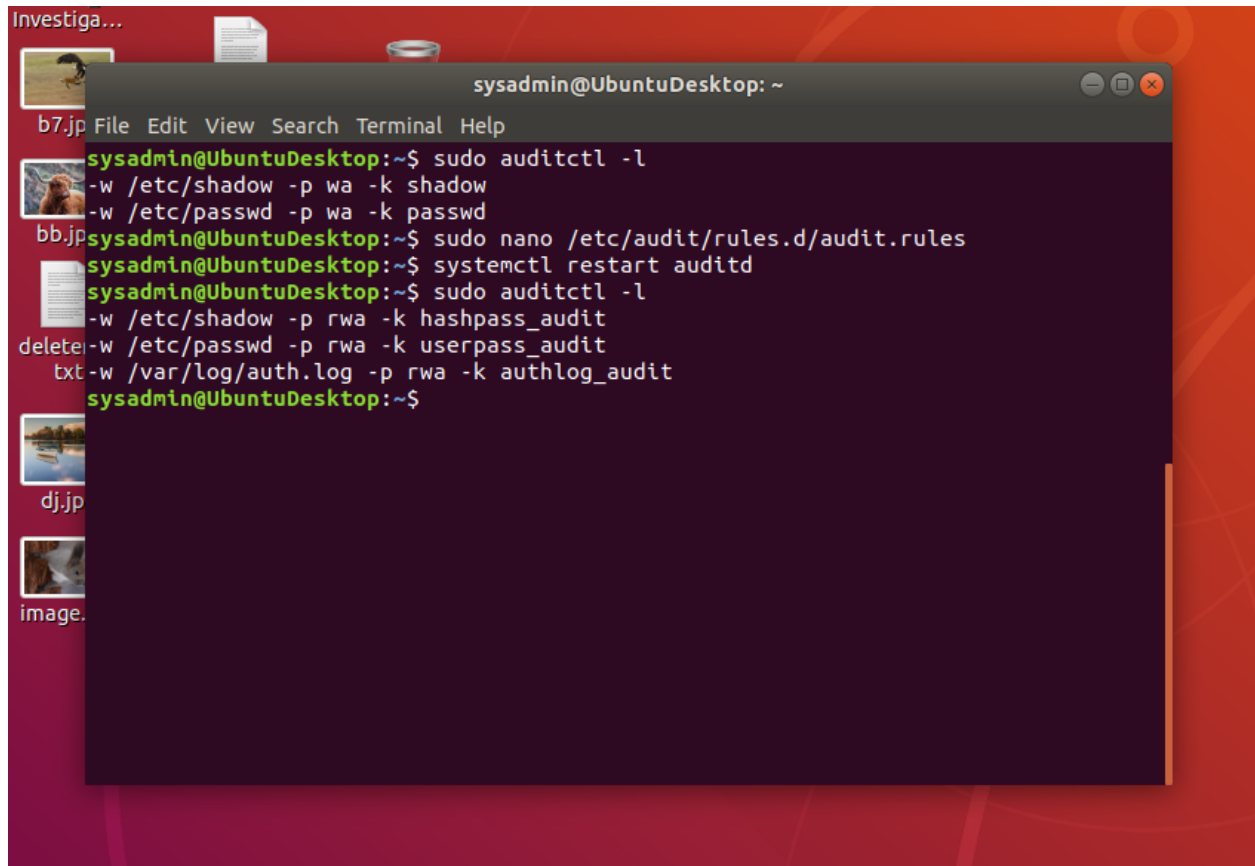
```
```bash
[Your solution edits here]
```
```

4. Command to restart `auditd`:



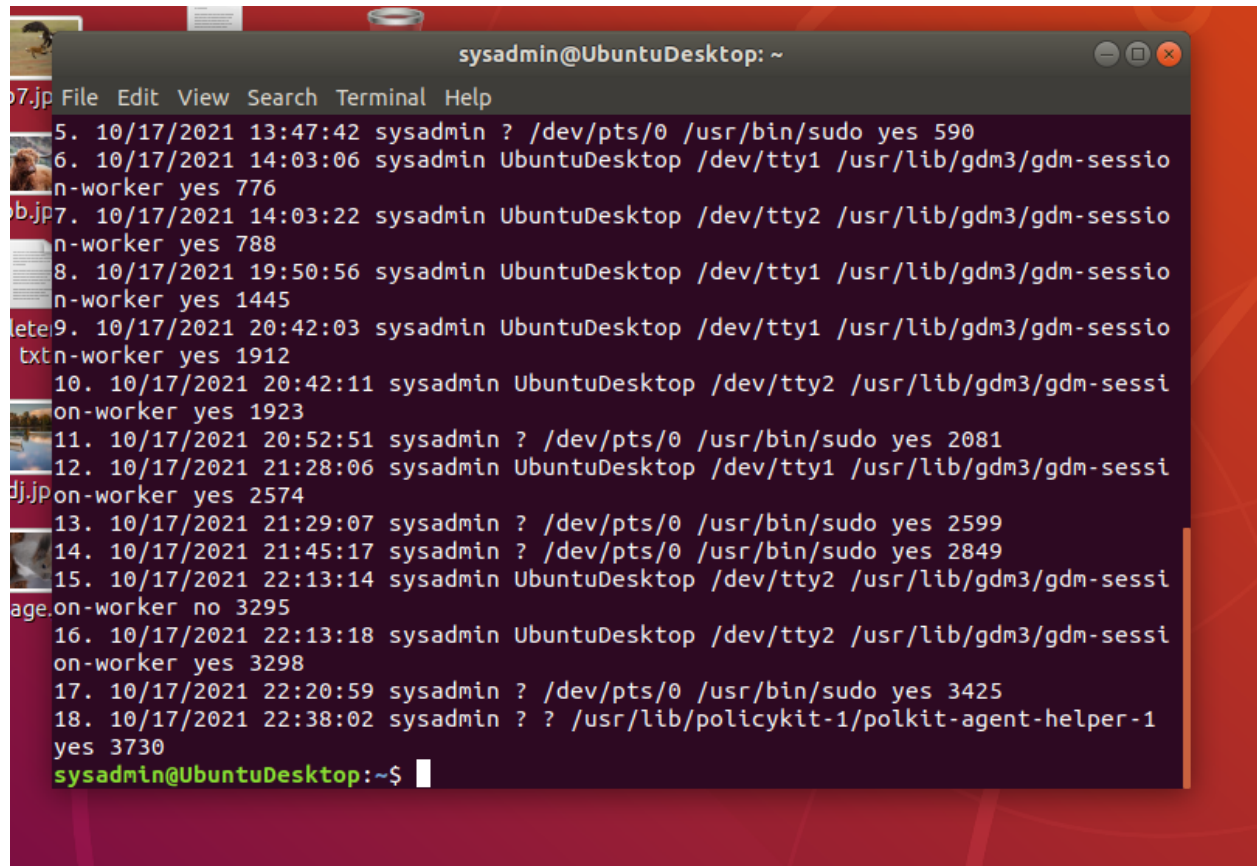
```
sysadmin@UbuntuDesktop:~$ systemctl restart auditd
```

5. Command to list all `auditd` rules:



6. Command to produce an audit report:

`sudo aureport -au -i`



```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
5. 10/17/2021 13:47:42 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 590
6. 10/17/2021 14:03:06 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 776
7. 10/17/2021 14:03:22 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 788
8. 10/17/2021 19:50:56 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 1445
9. 10/17/2021 20:42:03 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 1912
10. 10/17/2021 20:42:11 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1923
11. 10/17/2021 20:52:51 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 2081
12. 10/17/2021 21:28:06 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 2574
13. 10/17/2021 21:29:07 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 2599
14. 10/17/2021 21:45:17 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 2849
15. 10/17/2021 22:13:14 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 3295
16. 10/17/2021 22:13:18 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 3298
17. 10/17/2021 22:20:59 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 3425
18. 10/17/2021 22:38:02 sysadmin ? ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 3730
sysadmin@UbuntuDesktop:~$
```

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

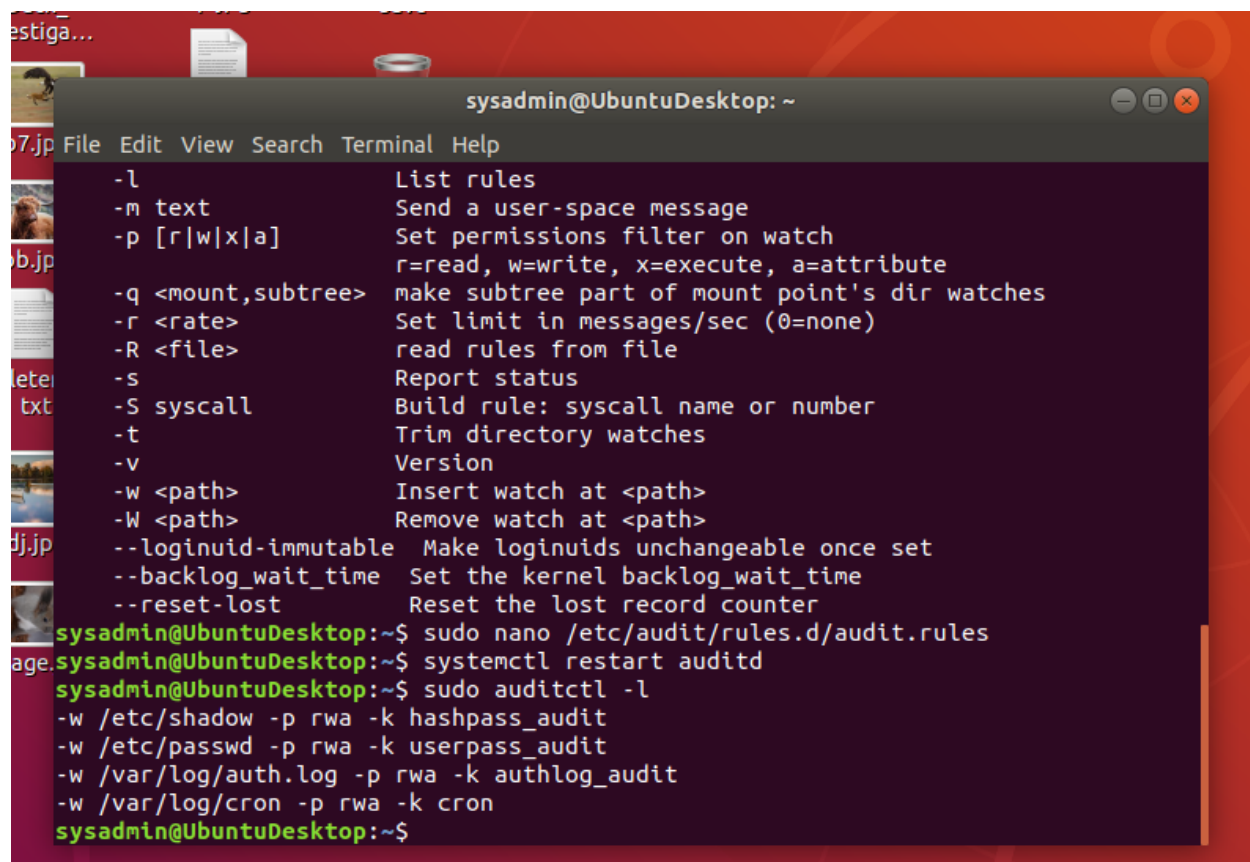
`sudo aureport -m`

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

`-w /var/log/cron -p rwa -k cron`

9. Command to verify `auditd` rules:





```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
-l List rules  
-m text Send a user-space message  
-p [r|w|x|a] Set permissions filter on watch  
r=read, w=write, x=execute, a=attribute  
-q <mount,subtree> make subtree part of mount point's dir watches  
-r <rate> Set limit in messages/sec (0=none)  
-R <file> read rules from file  
-s Report status  
-S syscall Build rule: syscall name or number  
-t Trim directory watches  
-v Version  
-w <path> Insert watch at <path>  
-W <path> Remove watch at <path>  
--loginuid-immutable Make loginuids unchangeable once set  
--backlog_wait_time Set the kernel backlog_wait_time  
--reset-lost Reset the lost record counter  
sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/rules.d/audit.rules  
sysadmin@UbuntuDesktop:~$ systemctl restart auditd  
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 rwa -k cron  
sysadmin@UbuntuDesktop:~$
```

---

### ### Bonus (Research Activity): Perform Various Log Filtering Techniques

1. Command to return `journalctl` messages with priorities from emergency to error:

```
Mon 09:15
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

sysadmin@UbuntuDesktop:~$ journalctl -p err -b
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Mon 2021-10-18 09:15:17 EDT. --
Oct 17 13:29:08 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Oct 17 13:29:08 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Oct 17 13:29:11 UbuntuDesktop systemd[1]: Failed to mount /vagrant.
Oct 17 13:29:17 UbuntuDesktop spice-vdagent[2175]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 13:29:42 UbuntuDesktop spice-vdagent[2672]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 13:36:06 UbuntuDesktop pulseaudio[2536]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not re
Oct 17 14:02:57 UbuntuDesktop systemd[1]: systemd-resolved.service: Watchdog timeout (limit 3min)!
Oct 17 14:02:57 UbuntuDesktop systemd[1]: systemd-udev.service: Watchdog timeout (limit 3min)!
Oct 17 14:02:57 UbuntuDesktop systemd[1]: snapd.service: Watchdog timeout (limit 5min)!
Oct 17 14:02:57 UbuntuDesktop systemd[1]: systemd-logind.service: Watchdog timeout (limit 3min)!
Oct 17 14:02:58 UbuntuDesktop gnome-session-binary[2327]: Unrecoverable failure in required component org.gnome.Shell.desktop
Oct 17 14:02:58 UbuntuDesktop gnome-session-binary[2327]: CRITICAL: We failed, but the fail whale is dead. Sorry....
Oct 17 14:03:08 UbuntuDesktop spice-vdagent[5260]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 14:09:51 UbuntuDesktop pulseaudio[5161]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not re
Oct 17 14:09:51 UbuntuDesktop pulseaudio[5161]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write new data to the device, but there was actu
Oct 17 14:09:51 UbuntuDesktop pulseaudio[5161]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a bug in the ALSA driver 'snd_intel8x0'. Please
Oct 17 14:23:12 UbuntuDesktop kernel: e1000 0000:00:03:00 enp0s3: Reset adapter
Oct 17 19:50:40 UbuntuDesktop systemd[1]: snapd.service: Watchdog timeout (limit 5min)!
Oct 17 19:50:40 UbuntuDesktop systemd[1]: systemd-logind.service: Watchdog timeout (limit 3min)!
Oct 17 19:50:58 UbuntuDesktop spice-vdagent[6776]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 19:51:22 UbuntuDesktop pulseaudio[6633]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not re
Oct 17 20:00:02 UbuntuDesktop pulseaudio[6633]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write new data to the device, but there was actu
Oct 17 20:00:02 UbuntuDesktop pulseaudio[6633]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a bug in the ALSA driver 'snd_intel8x0'. Please
Oct 17 20:00:02 UbuntuDesktop pulseaudio[6633]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up with POLLOUT set -- however a subsequent snd_pcm_a
Oct 17 20:41:54 UbuntuDesktop systemd[1]: systemd-resolved.service: Watchdog timeout (limit 3min)!
Oct 17 20:41:54 UbuntuDesktop systemd[1]: snapd.service: Watchdog timeout (limit 5min)!
Oct 17 20:41:54 UbuntuDesktop systemd[1]: systemd-udev.service: Watchdog timeout (limit 3min)!
Oct 17 20:41:54 UbuntuDesktop systemd[1]: systemd-logind.service: Watchdog timeout (limit 3min)!
Oct 17 20:42:04 UbuntuDesktop spice-vdagent[8123]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 20:42:28 UbuntuDesktop pulseaudio[7977]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not re
Oct 17 20:44:08 UbuntuDesktop pulseaudio[7977]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write new data to the device, but there was actu
Oct 17 20:44:08 UbuntuDesktop pulseaudio[7977]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a bug in the ALSA driver 'snd_intel8x0'. Please
Oct 17 20:44:08 UbuntuDesktop pulseaudio[7977]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up with POLLOUT set -- however a subsequent snd_pcm_a
lines 1-39...skipping...
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Mon 2021-10-18 09:15:17 EDT. --
Oct 17 13:29:08 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Oct 17 13:29:08 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Oct 17 13:29:11 UbuntuDesktop systemd[1]: Failed to mount /vagrant.
Oct 17 13:29:17 UbuntuDesktop spice-vdagent[2175]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 13:29:42 UbuntuDesktop spice-vdagent[2672]: Cannot access vdagnt virtio channel /dev/virtio-ports/com.redhat.spice.0
Oct 17 13:36:06 UbuntuDesktop pulseaudio[2536]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not re
```

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

```
Mon 09:17
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

sysadmin@UbuntuDesktop:~$ journalctl --disk-usage
Archived and active journals take up 2.6G in the file system.
sysadmin@UbuntuDesktop:~$
```

1. Command to remove all archived journal files except the most recent two:

```
File Edit View Search Terminal Help

sysadmin@UbuntuDesktop:~$ sudo journalctl --vacuum-time=2d
[sudo] password for sysadmin:
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@fed3c224181944cbb53922cb4f90f935-0000000000000001-0005972d05e4b690.j
ournal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@00059742d5b110d-5b03e094f05bdaab.journal- (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@00059742ccf258c3-01c663e4b24a6da1.journal- (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@00059742d126cb08-8fde5c3ef5545679.journal- (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7ff3552ffdd3eaf-0000000000000001-00059742d11d6f3f.j
ournal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@0893d6dd392f847ea833abe05e03ef4dd-000000000000006dc-00059742d5b0091
journal (128.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@f0872ed68b9f4da396ada2a217be9ebb-000000000000c5f37-0005ce225057eaf
f.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005ce8fc3ffcd64-d60cc0e388bc0314.journal- (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@0005ce8fc5f38b1e-a9fde92022d182be.journal- (8.0M).
Vacuuming done, freed 1.1G of archived journals from /var/log/journal/e5853fe375964d39b27025eb6608e969.
Vacuuming done, freed 0B of archived journals from /var/log/journal.
sysadmin@UbuntuDesktop:~$
```

1. Command to filter all log messages with priority levels between zero and two, and save output to `~/home/sysadmin/Priority\_High.txt`:

```
sysadmin@UbuntuDesktop: /etc/cron.daily
File Edit View Search Terminal Help
GNU nano 2.9.3 priority.sh
^I/bin/bash
journalctl -p crit -b >> /home/student/Priority_High.txt
```

1. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:

```
sysadmin@UbuntuDesktop:/etc$ cd cron.daily/
sysadmin@UbuntuDesktop:/etc/cron.daily$ ls
anacron  apt-compat  chkrootkit  google-chrome  man-db  popularity-contest  samba
apache2  aptitude   cracklib-runtime  logrotate  mlocate  priority.sh  update-notifier-common
sysadmin@UbuntuDesktop:/etc/cron.daily$
```

```
sysadmin@UbuntuDesktop: /etc/cron.daily
File Edit View Search Terminal Help
GNU nano 2.9.3 priority.sh
^I/bin/bash
journalctl -p crit -b >> /home/student/Priority_High.txt
```

```
```bash
[Your solution cron edits here]
```
```

---