HOMEWORK WEEK 5 SUBMISSION

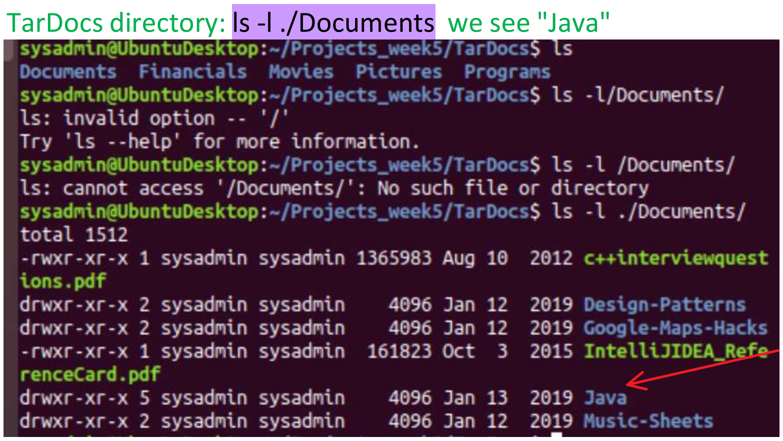
Sunday, January 16, 2022 7:45 PM

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.

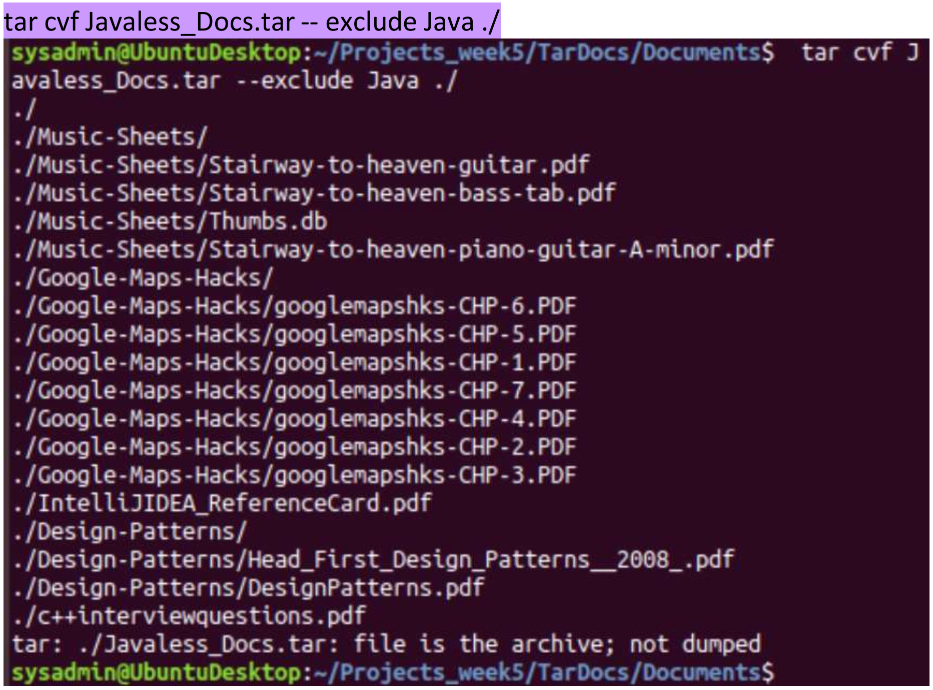
Step 1: Create, Extract, Compress, and Manage tar Backup Archives

1. Command to **extract** the TarDocs.tar archive to the current directory:
   tar xvvf TarDocs.tar
   VERIFYING THERE IS A JAVA SUBDIRECTORY:
   in the TarDocs directory: ls -l ./Documents we see "Java"



```
sysadmin@UbuntuDesktop:~/Projects_week5/TarDocs$ ls
Documents  Financials  Movies  Pictures  Programs
sysadmin@UbuntuDesktop:~/Projects_week5/TarDocs$ ls -l/Documents/
ls: invalid option -- '/'
Try 'ls --help' for more information.
sysadmin@UbuntuDesktop:~/Projects_week5/TarDocs$ ls -l /Documents/
ls: cannot access '/Documents/': No such file or directory
sysadmin@UbuntuDesktop:~/Projects_week5/TarDocs$ ls -l ./Documents/
total 1512
-rwxr-xr-x 1 sysadmin sysadmin 1365983 Aug 10  2012 c++interviewquest
ions.pdf
drwxr-xr-x 2 sysadmin sysadmin    4096 Jan 12  2019 Design-Patterns
drwxr-xr-x 2 sysadmin sysadmin    4096 Jan 12  2019 Google-Maps-Hacks
-rwxr-xr-x 1 sysadmin sysadmin  161823 Oct  3  2015 IntelliJIDEA_Refe
renceCard.pdf
drwxr-xr-x 5 sysadmin sysadmin    4096 Jan 13  2019 Java
drwxr-xr-x 2 sysadmin sysadmin    4096 Jan 12  2019 Music-Sheets
```

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



```
sysadmin@UbuntuDesktop:~/Projects_week5/TarDocs/Documents$  tar cvf J
avaless_Docs.tar --exclude Java ./
./
./Music-Sheets/
./Music-Sheets/Stairway-to-heaven-guitar.pdf
./Music-Sheets/Stairway-to-heaven-bass-tab.pdf
./Music-Sheets/Thumbs.db
./Music-Sheets/Stairway-to-heaven-piano-guitar-A-minor.pdf
./Google-Maps-Hacks/
./Google-Maps-Hacks/googlemapshks-CHP-6.PDF
./Google-Maps-Hacks/googlemapshks-CHP-5.PDF
./Google-Maps-Hacks/googlemapshks-CHP-1.PDF
./Google-Maps-Hacks/googlemapshks-CHP-7.PDF
./Google-Maps-Hacks/googlemapshks-CHP-4.PDF
./Google-Maps-Hacks/googlemapshks-CHP-2.PDF
./Google-Maps-Hacks/googlemapshks-CHP-3.PDF
./IntelliJIDEA_ReferenceCard.pdf
./Design-Patterns/
./Design-Patterns/Head_First_Design_Patterns__2008_.pdf
./Design-Patterns/DesignPatterns.pdf
./c++interviewquestions.pdf
tar: ./Javaless_Docs.tar: file is the archive; not dumped
sysadmin@UbuntuDesktop:~/Projects_week5/TarDocs/Documents$
```

3. Command to ensure Java/ is not in the new Javaless_Docs.tar archive:
   tar tvf Javaless_Docs.tar shows that there is no Java in the list as I read through it.
   and I piped grep to the end of it to make sure there were no instances of 'Java':
   tar tvvf Javaless_Docs.tar | grep -i java

Bonus

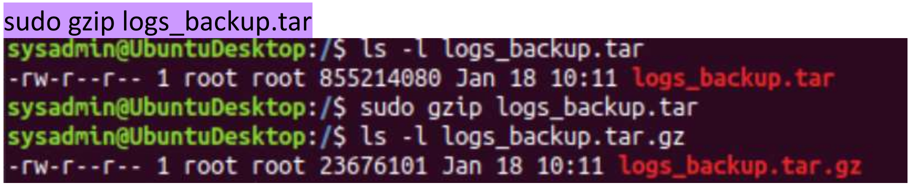
- Command to create an incremental archive called logs_backup_tar.gz with only changed files to snapshot.file for the /var/log directory:

  from root directory:

  ```
  sudo tar cvvWf logs_backup.tar --listed-incremental=snapshot.file --level=0 /var/log
  ```

  then gzip the file:

  ```
  sudo gzip logs_backup.tar
  ```



```
sysadmin@UbuntuDesktop:/$ ls -l logs_backup.tar
-rw-r--r-- 1 root root 855214080 Jan 18 10:11 logs_backup.tar
sysadmin@UbuntuDesktop:/$ sudo gzip logs_backup.tar
sysadmin@UbuntuDesktop:/$ ls -l logs_backup.tar.gz
-rw-r--r-- 1 root root 23676101 Jan 18 10:11 logs_backup.tar.gz
```

Critical Analysis Question

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

c creates, x extracts. I think that it wouldn't make sense to extract something you are creating simultaneously. If you are extracting, you want to take something OUT OF tar format. If you are creating you want to put something INTO tar format.

Step 2: Create, Manage, and Automate Cron Jobs

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

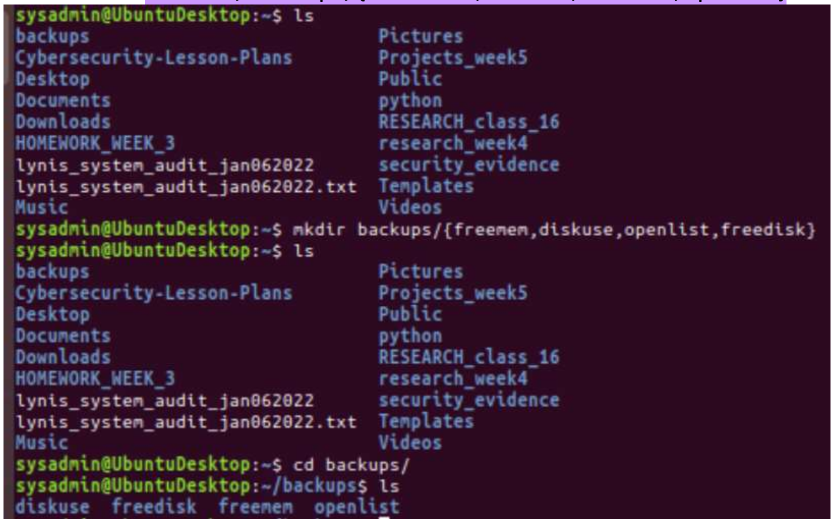
   ```
   0 6 * * 3 tar cvf /auth_backup.tgz /var/log/auth.log
   ```

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

   first: `mkdir backups`

   then: `mkdir ~/backups/{freemem,diskuse,freedisk,openlist}`

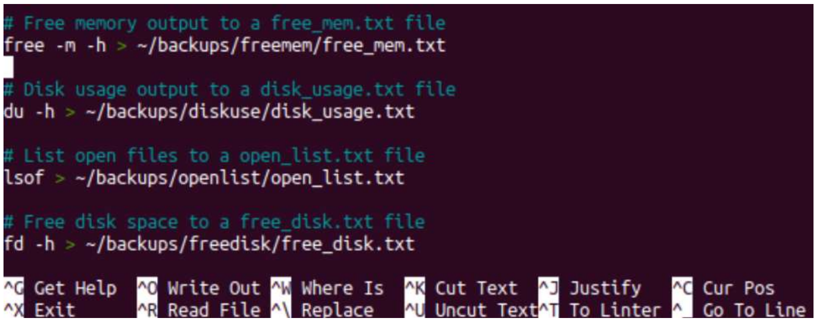


```
sysadmin@UbuntuDesktop:~$ ls
backups                             Pictures
Cybersecurity-Lesson-Plans          Projects_week5
Desktop                             Public
Documents                           python
Downloads                           RESEARCH_class_16
HOMEWORK_WEEK_3                     research_week4
lynis_system_audit_jan062022        security_evidence
lynis_system_audit_jan062022.txt    Templates
Music                               Videos
sysadmin@UbuntuDesktop:~$ mkdir backups/{freemem,diskuse,openlist,freedisk}
sysadmin@UbuntuDesktop:~$ ls
backups                             Pictures
Cybersecurity-Lesson-Plans          Projects_week5
Desktop                             Public
Documents                           python
Downloads                           RESEARCH_class_16
HOMEWORK_WEEK_3                     research_week4
lynis_system_audit_jan062022        security_evidence
lynis_system_audit_jan062022.txt    Templates
Music                               Videos
sysadmin@UbuntuDesktop:~$ cd backups/
sysadmin@UbuntuDesktop:~/backups$ ls
diskuse  freedisk  freemem  openlist
```

2. Paste your system.sh script edits below:

   ```
   #!/bin/bash

   # Free memory output to a free_mem.txt file
   free -m -h > ~/backups/freemem/free_mem.txt

   # Disk usage output to a disk_usage.txt file
   du -h > ~/backups/diskuse/disk_usage.txt

   # List open files to a open_list.txt file
   ```

```
lsof > ~/backups/openlist/open_list.txt

# Free disk space to a free_disk.txt file
fd -h > ~/backups/freedisk/free_disk.txt
```



```
# Free memory output to a free_mem.txt file
free -m -h > ~/backups/freemem/free_mem.txt

# Disk usage output to a disk_usage.txt file
du -h > ~/backups/diskuse/disk_usage.txt

# List open files to a open_list.txt file
lsof > ~/backups/openlist/open_list.txt

# Free disk space to a free_disk.txt file
fd -h > ~/backups/freedisk/free_disk.txt
```

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

```
chmod +x system.sh
```

Optional

```
sudo sh system.sh
```

then can check the files using cat or nano:

example:

```
cd backups/freemem
cat free_mem.txt
```

…etc for the other 3

Bonus

- Command to copy system.sh to system-wide cron directory:

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

Step 4. Manage Log File Sizes

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

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

Bonus: Check for Policy and File Violations

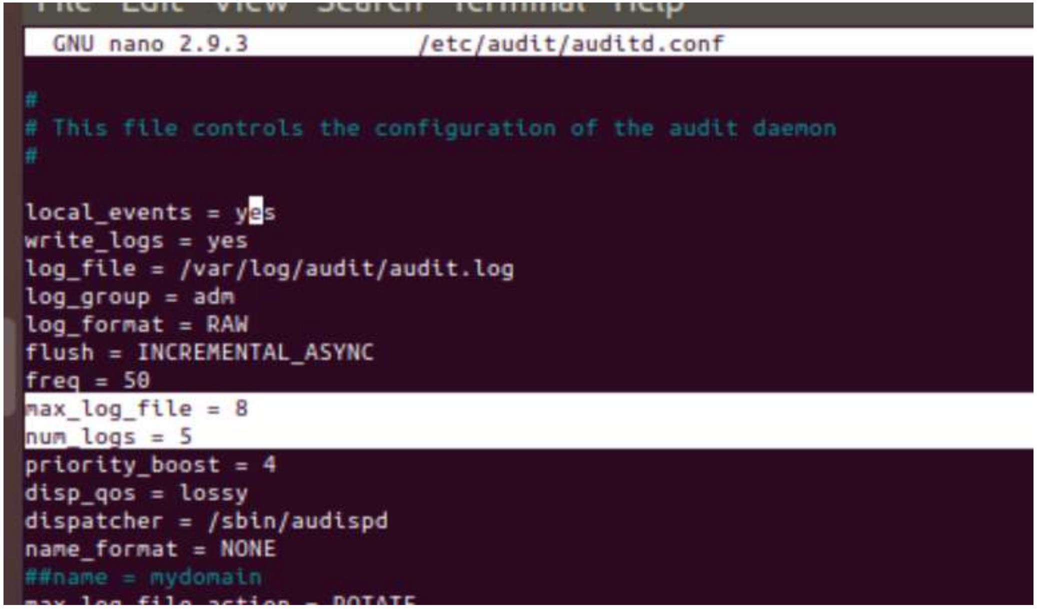
1. Command to verify auditd is active:$ systemctl status auditd
2. Command to set number of retained logs and maximum log file size:

THIS IS WHAT WAS IN THE etc/audit/auditd.conf file:

```
#
# 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
```

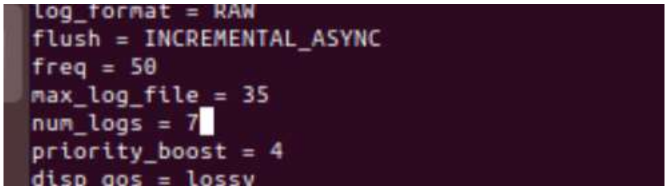
```
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE

##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
```

- ○ Add the edits made to the configuration file below: we want to change the number of retained logs to 7 and the maximum log size to 35, so I edited these two lines:



```
  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 = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
```

To max_log_file = 35 and num_logs = 7:



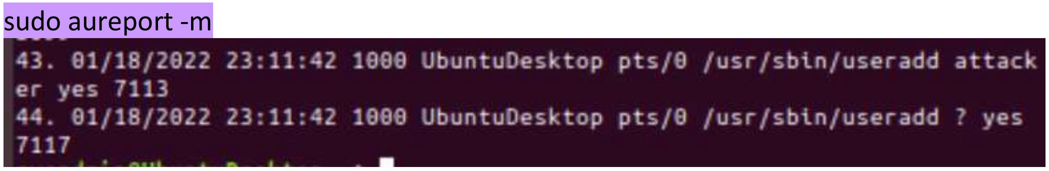
```
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 35
num_logs = 7
priority_boost = 4
disp_qos = lossy
```

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 -pwra -khashpass_audit
     -w/etc/passwd -pwra -kuserpass_audit
     -w/var/log/auth.log -pwra -kauthlog.audit

4. Command to restart auditd:
   $ systemctl stop auditd
   Then
   $ systemctl start auditd
   (can instead: sudo systemctl restart auditd)

5. Command to list all auditd rules: $ sudo auditctl -l

6. Command to produce an audit report:
   sudo aureport -au
7. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:
   sudo aureport -m



```
43. 01/18/2022 23:11:42 1000 UbuntuDesktop pts/0 /usr/sbin/useradd attack
er yes 7113
44. 01/18/2022 23:11:42 1000 UbuntuDesktop pts/0 /usr/sbin/useradd ? yes
7117
```

8. Command to use auditd to watch /var/log/cron:
   $: sudo auditctl -w /var/log/cron
9. Command to verify auditd rules:
   sudo auditctl -l

Bonus (Research Activity): Perform Various Log Filtering Techniques

1. Command to return journalctl messages with priorities from emergency to error:
   $ journalctl -b -1 -p "emerg".."crit"

   **From <https://www.loggly.com/ultimate-guide/using-journalctl/>

   SO…

   I would try: journalctl -b -1 -p "emerg"…"error" DOESN'T WORK
   tried:
   journalctl -b -1 -p "emerg".."err" WORKS!

2. Command to check the disk usage of the system journal unit since the most recent boot:
   journalctl --disk-usage
3. Command to remove all archived journal files except the most recent two:
4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority_High.txt:
5. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:
   [Your solution cron edits here]