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

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

```
sysadmin@UbuntuDesktop:~/Projects/TarDocs$ sudo tar xvvf TarDocs.tar
```

```
sysadmin@UbuntuDesktop:~/Projects$ ls
TarDocs  TarDocs.tar
```

```
sysadmin@UbuntuDesktop:~/Projects$ cd TarDocs/
sysadmin@UbuntuDesktop:~/Projects/TarDocs$ ls
Documents  Financials  Movies  Pictures  Programs
sysadmin@UbuntuDesktop:~/Projects/TarDocs$ ls -l ~/Projects/TarDocs/Documents/
total 1512
-rwxr-xr-x 1 instructor instructor 1365983 Aug 10  2012 c++interviewquestions.pdf
drwxr-xr-x 2 instructor instructor    4096 Jan 12  2019 Design-Patterns
drwxr-xr-x 2 instructor instructor    4096 Jan 12  2019 Google-Maps-Hacks
-rwxr-xr-x 1 instructor instructor  161823 Oct  3  2015 IntelliJIDEA_ReferenceCard.pdf
drwxr-xr-x 5 instructor instructor    4096 Jan 13  2019 Java
drwxr-xr-x 2 instructor instructor    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:

```
sysadmin@UbuntuDesktop:~/Projects$ sudo tar cvvf Javaless_Docs.tar --exclude="TarDocs/Document
s/Java" TarDocs
```

```
sysadmin@UbuntuDesktop:~/Projects$ ls
Javaless_Docs.tar  TarDocs  TarDocs.tar
```

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

```
sysadmin@UbuntuDesktop:~/Projects$ tar tvvf Javaless_Docs.tar | grep -R 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:

```
sysadmin@UbuntuDesktop:~/Projects$ sudo tar czvvf logs_backup.tar.gz --listed-incremental=snapshot.fi
le /var/log
```

Critical Analysis Question

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

The -c option is to create the archive file and the -x tar option is to extract that existing file. Using both the -x and -c option will not work because it needs to have an existing tar file created.

Step 2: Create, Manage, and Automate Cron Jobs

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

```
# HW 5 => Create, Manage, and Automate Cron Jobs

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

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

```
sysadmin@UbuntuDesktop:~$ sudo mkdir ~/backups/{freemem,diskuse,openlist,freedisk}
```

Paste your system.sh script edits below:

#!/bin/bash

2.

```
#!/bin/bash

#Prints the amount of free memory on the system and saves it
free -mh > ~/backups/freemem/free_mem.txt

#Prints disk usage and saves it
du -h > ~/backups/diskuse/disk_usage.txt

#Lists all open files and saves it
lsof > ~/backups/openlist/open_list.txt

#Prints file system disk space statistics and saves it
df -h > ~/backups/freedisk/free_disk.txt
```

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

```
sysadmin@UbuntuDesktop:~$ chmod +x system.sh
sysadmin@UbuntuDesktop:~$ sudo ./system.sh
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
sysadmin@UbuntuDesktop:~$
```

Optional

- Commands to test the script and confirm its execution:

Bonus

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

```
sysadmin@UbuntuDesktop:~$ ls
backups                    Documents     Pictures  research          subpoena_request  text1
backup.sh                  Downloads     Projects  Security_scripts  sudo              Videos
Cybersecurity-Lesson-Plans  learning_awk  Public    shadow_copy       system.sh
Desktop                    Music         python    snap              Templates
sysadmin@UbuntuDesktop:~$ crontab -e
```

```
#HW 5 => Bonus -- automate script by adding it to the weekly system-wide cron directory
@weekly ~/system.sh
```

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

   - Add your config file edits below:

2.
```
/var/log/auth.log{
        weekly
        rotate 7
        notifempty
        compress
        delaycompress
        missingok
}
```

Bonus: Check for Policy and File Violations

1. Command to verify auditd is active:

```
sysadmin@UbuntuDesktop:~$ systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-10-06 00:41:30 EDT; 10h ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
  Process: 9956 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
  Process: 9940 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
 Main PID: 9947 (auditd)
    Tasks: 2 (limit: 4675)
   CGroup: /system.slice/auditd.service
           └─9947 /sbin/auditd

Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: backlog_wait_time 0
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: enabled 1
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: failure 1
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: pid 9947
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: rate_limit 0
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: backlog_limit 8192
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: lost 0
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: backlog 1
Oct 06 00:41:30 UbuntuDesktop augenrules[9956]: backlog_wait_time 0
Oct 06 00:41:30 UbuntuDesktop systemd[1]: Started Security Auditing Service.
sysadmin@UbuntuDesktop:~$
```

2. Command to set number of retained logs and maximum log file size:
    - Add the edits made to the configuration file below:

```
sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/auditd.conf
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$
```

3.
```
  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
```

4. 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:

```
sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/rules.d/audit.rules
sysadmin@UbuntuDesktop:~$
```

5.
```
-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
```

6. Command to restart auditd:

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

7. Command to list all auditd rules:

```
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
sysadmin@UbuntuDesktop:~$
```

8. Command to produce an audit report:

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

Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 10/06/2021 00:37:21 sysadmin ? /dev/pts/1 /usr/bin/sudo no 415
2. 10/06/2021 00:37:25 sysadmin ? /dev/pts/1 /usr/bin/sudo no 416
3. 10/06/2021 00:37:28 sysadmin ? /dev/pts/1 /usr/bin/sudo no 417
4. 10/06/2021 00:37:43 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 440
5. 10/06/2021 00:38:38 root UbuntuDesktop pts/1 /usr/bin/chfn yes 560
6. 10/06/2021 10:52:42 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 899
sysadmin@UbuntuDesktop:~$
```

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

```
sysadmin@UbuntuDesktop:~$ sudo useradd attacker
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$ sudo aureport -m

Account Modifications Report
================================================
# date time auid addr term exe acct success event
================================================
1. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 531
2. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 533
3. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 534
4. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 541
5. 10/06/2021 00:38:30 1000 UbuntuDesktop pts/1 /usr/bin/passwd criminal no 551
6. 10/06/2021 00:38:38 1000 UbuntuDesktop pts/1 /usr/bin/passwd criminal yes 557
7. 10/06/2021 11:01:53 1000 UbuntuDesktop pts/1 /usr/sbin/useradd attacker yes 2661
8. 10/06/2021 11:01:53 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 2665
sysadmin@UbuntuDesktop:~$
```

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

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

11. Command to verify auditd rules:

```
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
sysadmin@UbuntuDesktop:~$
```

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

Account Modifications Report
===============================================
# date time auid addr term exe acct success event
===============================================
1. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 531
2. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 533
3. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 534
4. 10/06/2021 00:38:21 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 541
5. 10/06/2021 00:38:30 1000 UbuntuDesktop pts/1 /usr/bin/passwd criminal no 551
6. 10/06/2021 00:38:38 1000 UbuntuDesktop pts/1 /usr/bin/passwd criminal yes 557
7. 10/06/2021 11:01:53 1000 UbuntuDesktop pts/1 /usr/sbin/useradd attacker yes 2661
8. 10/06/2021 11:01:53 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 2665
```

Bonus (Research Activity): Perform Various Log Filtering Techniques

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

```
sysadmin@UbuntuDesktop:~$ sudo journalctl -b -p "emerg.."err"
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Wed 2021-10-06 11:16:15 EDT. --
Oct 04 16:34:17 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log mes
Oct 04 16:34:17 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log mes
Oct 04 16:34:32 UbuntuDesktop spice-vdagent[2136]: Cannot access vdagent virtio channel /dev/virtio-p
Oct 04 16:34:50 UbuntuDesktop spice-vdagent[2620]: Cannot access vdagent virtio channel /dev/virtio-p
Oct 04 16:34:53 UbuntuDesktop pulseaudio[2474]: [pulseaudio] bluez5-util.c: GetManagedObjects() faile
Oct 04 16:52:36 UbuntuDesktop pulseaudio[2474]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to
Oct 04 16:52:36 UbuntuDesktop pulseaudio[2474]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this i
Oct 04 16:52:36 UbuntuDesktop pulseaudio[2474]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up w
Oct 04 17:01:58 UbuntuDesktop kernel: e1000 0000:00:03.0 enp0s3: Reset adapter
Oct 04 17:01:59 UbuntuDesktop kernel: usb 1-1: can't set config #1, error -32
Oct 05 22:16:56 UbuntuDesktop kernel: [drm:vmw_kms_check_display_memory [vmwgfx]] *ERROR* Combined ou
Oct 06 00:37:28 UbuntuDesktop sudo[9849]: sysadmin : 3 incorrect password attempts ; TTY=pts/1 ; PWD=
Oct 06 00:45:04 UbuntuDesktop kernel: usb 1-1: can't set config #1, error -32
Oct 06 11:01:18 UbuntuDesktop sudo[10333]: sysadmin : 1 incorrect password attempt ; TTY=pts/1 ; PWD=
Oct 06 11:01:58 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:01:58 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:01:58 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:19 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:19 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:19 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:30 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:30 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:30 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:36 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:36 UbuntuDesktop kernel: audit: backlog limit exceeded
Oct 06 11:03:36 UbuntuDesktop kernel: audit: backlog limit exceeded
lines 1-27/27 (END)
```

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

```
sysadmin@UbuntuDesktop:~$ sudo journalctl -b --disk-usage
Archived and active journals take up 416.0M in the file system.
sysadmin@UbuntuDesktop:~$
```

3. Comand to remove all archived journal files except the most recent two:

```
sysadmin@UbuntuDesktop:~$ sudo journalctl --vacuum-files=2
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@fed3c224181944cdb53
922cb4f90f935-0000000000000001-0005972d05e4b690.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@00059742ccf258c3-01
c663e4b24a6da1.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@00059742d126cbd8-8f
de5c3ef5545679.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7
ff3552ffd3eaf-0000000000000001-00059742d11d6f3f.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@893d6dd392f847ea
833abe05e03ef4dd-00000000000006dc-00059742d5b00913.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1001@0917458f902140a7
8012f13deaf5c5f1-0000000000000b12-00059742e0cf8cba.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7
ff3552ffd3eaf-0000000000001254-0005c25000d9c5de.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1001@0917458f902140a7
8012f13deaf5c5f1-00000000000014ae-0005c2500171b142.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7
ff3552ffd3eaf-00000000000014ba-0005c250017396e4.journal (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7
ff3552ffd3eaf-0000000000003885-0005c250472390b5.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1001@0917458f902140a7
8012f13deaf5c5f1-000000000000389b-0005c2504756e6f0.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7
ff3552ffd3eaf-0000000000003b9b-0005cb0f60c9871a.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1001@0917458f902140a7
8012f13deaf5c5f1-0000000000003e66-0005cb0f615ec0ae.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@7e858fb1ab9241558b7
ff3552ffd3eaf-0000000000003e74-0005cb0f615f8161.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005cc8b8c88921d-ed
5219b7e9b27603.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@0005cd603751c0fb
-e81660b2a3f1acac.journal~ (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005cd6034eeeb1e-a8
2eb15c9afabaab.journal~ (32.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@0005cd8cd6210728-a5
90364a0c684f56.journal~ (16.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/user-1000@a7f065ef60404ea7
91aafca18b0951fd-0000000000000528-0005cd603751aff5.journal (8.0M).
Deleted archived journal /var/log/journal/e5853fe375964d39b27025eb6608e969/system@4c278224b28848aab7e
ab184e5625285-0000000000000001-0005cd8cd61fc535.journal (128.0M).
Vacuuming done, freed 328.0M of archived journals from /var/log/journal/e5853fe375964d39b27025eb6608e
969.
sysadmin@UbuntuDesktop:~$
```

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

```
sysadmin@UbuntuDesktop:~$ sudo journalctl -p 0..2 > /home/sysadmin/Priority_High.txt
sysadmin@UbuntuDesktop:~$ ls
backups                    Downloads          Projects          shadow_copy       Templates
backup.sh                  learning_awk       Public            snap              text1
Cybersecurity-Lesson-Plans Music              python            subpoena_request  Videos
Desktop                    Pictures           research          sudo
Documents                  Priority_High.txt  Security_scripts  system.sh
sysadmin@UbuntuDesktop:~$ cat Priority_High.txt
-- Logs begin at Fri 2021-09-24 00:01:02 EDT, end at Wed 2021-10-06 11:37:29 EDT. --
-- No entries --
sysadmin@UbuntuDesktop:~$
```

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

```
sysadmin@UbuntuDesktop:~$ crontab -e
crontab: installing new crontab
sysadmin@UbuntuDesktop:~$
```

```
  GNU nano 2.9.3                    /tmp/crontab.z9kQPX/crontab                    M

# 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


# HW 5 => Create, Manage, and Automate Cron Jobs

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

#HW 5 => Bonus -- automate script by adding it to the weekly system-wide cron directory
@weekly ~/system.sh


#HW 5 => BONUS #2
@daily sudo journalctl -p "emerg.."crit" > /home/sysadmin/Priority_High.txt
```