



## Module 5 Challenge Submission File

### Archiving and Logging Data

Make a copy of this document to work in, and then for each step, add the solution command below the prompt. Save and submit this completed file as your Challenge deliverable.

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

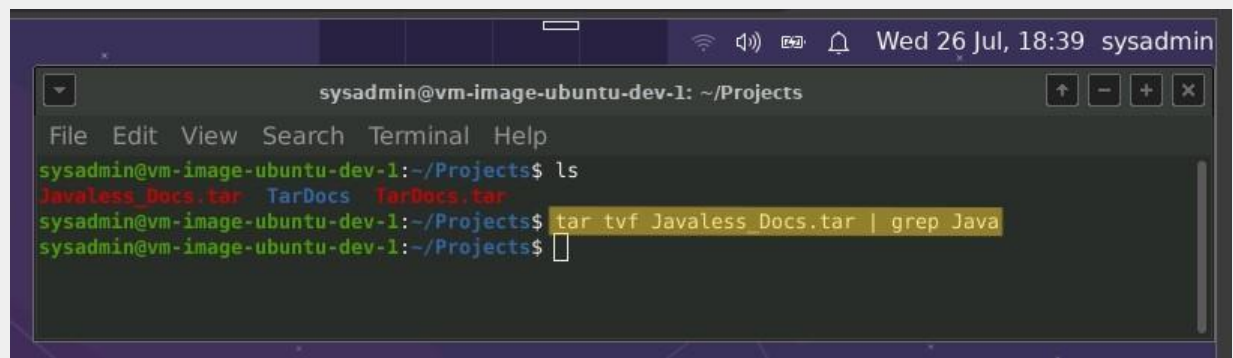
1. Command to **extract** the `TarDocs.tar` archive to the current directory:

```
sysadmin@vm-image-ubuntu-dev-1: ~/Projects
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~/Projects$ sudo tar -xvf TarDocs.tar
[sudo] password for sysadmin:
TarDocs/
TarDocs/Movies/
TarDocs/Movies/ZOE_0004.mp4
TarDocs/Movies/ZO_0001.mp4
TarDocs/Movies/ZOE_0003.mp4
TarDocs/Movies/ZOE_0002.mp4
TarDocs/Financials/
TarDocs/Financials/investments1.txt
TarDocs/Financials/Assests_2.txt
TarDocs/Financials/Assests_1.txt
```

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

```
sysadmin@vm-image-ubuntu-dev-1: ~/Projects
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~/Projects$ sudo tar cvf Javaless_Doc.tar --exclude=TarDocs/Documents/Java TarDocs
[sudo] password for sysadmin:
TarDocs/
TarDocs/Programs/
TarDocs/Programs/TapToPlace/
TarDocs/Programs/TapToPlace/.vs/
TarDocs/Programs/TapToPlace/.vs/TapToPlace/
TarDocs/Programs/TapToPlace/.vs/TapToPlace/v14/
TarDocs/Programs/TapToPlace/.vs/TapToPlace/v14/.suo
TarDocs/Programs/TapToPlace/TapToPlace.CSharp.csproj
TarDocs/Programs/TapToPlace/WindowsStoreApp/
TarDocs/Programs/TapToPlace/WindowsStoreApp/.vs/
```

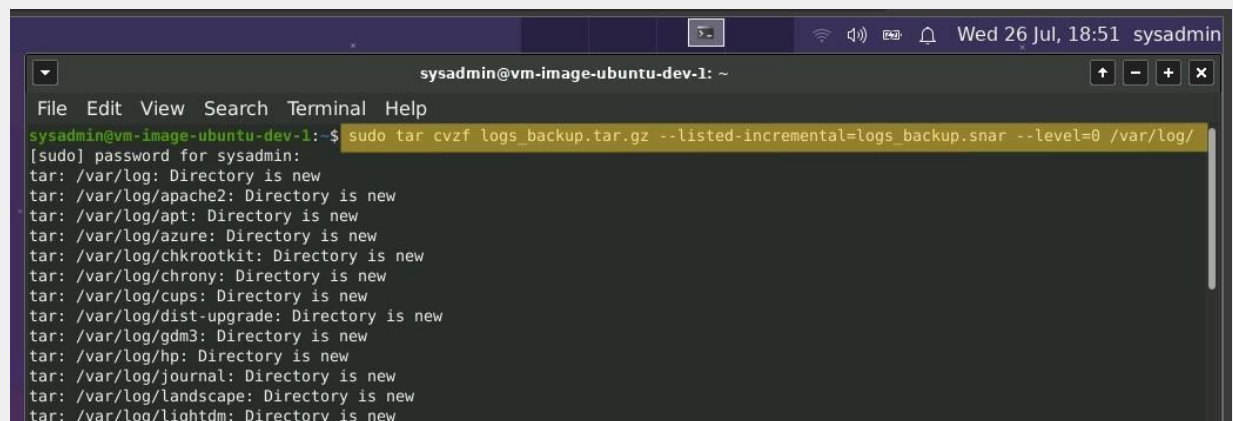
3. Command to ensure `Java/` is not in the new `Javaless_Docs.tar` archive:



```
sysadmin@vm-image-ubuntu-dev-1: ~/Projects
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~/Projects$ ls
Javaless_Docs.tar  TarDocs  TarDocs.tar
sysadmin@vm-image-ubuntu-dev-1:~/Projects$ tar tvf Javaless_Docs.tar | grep Java
sysadmin@vm-image-ubuntu-dev-1:~/Projects$
```

## Optional

4. Command to create an incremental archive called `logs_backup.tar.gz` with only changed files to `snapshot.file` for the `/var/log` directory:



```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo tar cvzf logs_backup.tar.gz --listed-incremental=logs_backup.snar --level=0 /var/log/
[sudo] password for sysadmin:
tar: /var/log: Directory is new
tar: /var/log/apache2: Directory is new
tar: /var/log/apt: Directory is new
tar: /var/log/azure: Directory is new
tar: /var/log/chkrootkit: Directory is new
tar: /var/log/chrony: 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/journal: Directory is new
tar: /var/log/landscape: Directory is new
tar: /var/log/lightdm: Directory is new
```

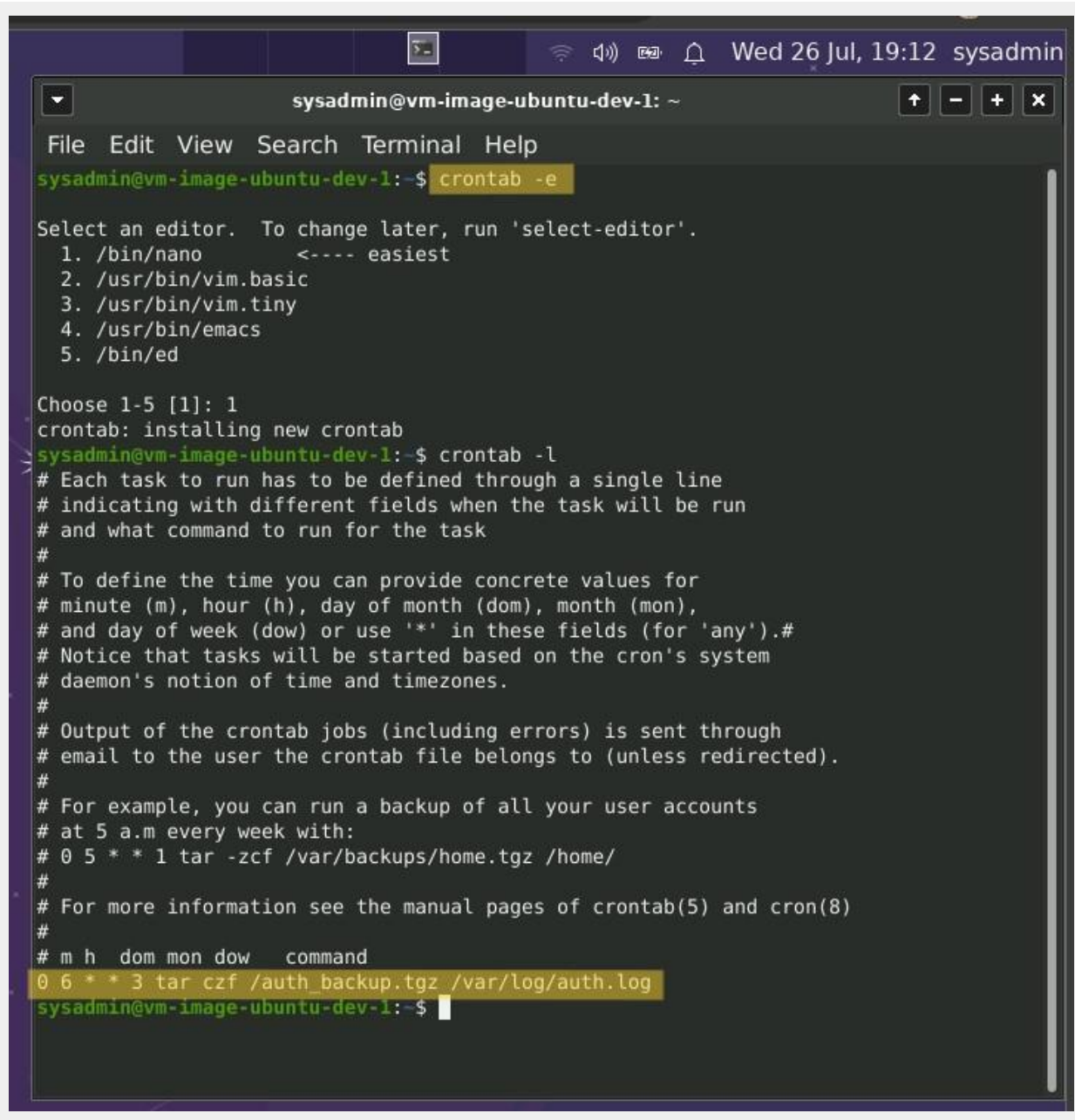
## Critical Analysis Question

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

I would not use `-x` and `-c` at the same time with `tar` because you cannot create and extract an archive in one command line.

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

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



The screenshot shows a terminal window titled "sysadmin@vm-image-ubuntu-dev-1: ~". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the user running `crontab -e`, which opens an editor selection menu. The user chooses option 1, `/bin/nano`. The terminal then shows the user running `crontab -l`, which displays the current crontab contents. The user then adds a new cron job entry: `0 6 * * 3 tar czf /auth_backup.tgz /var/log/auth.log`. The terminal prompt returns to `sysadmin@vm-image-ubuntu-dev-1:~$`.

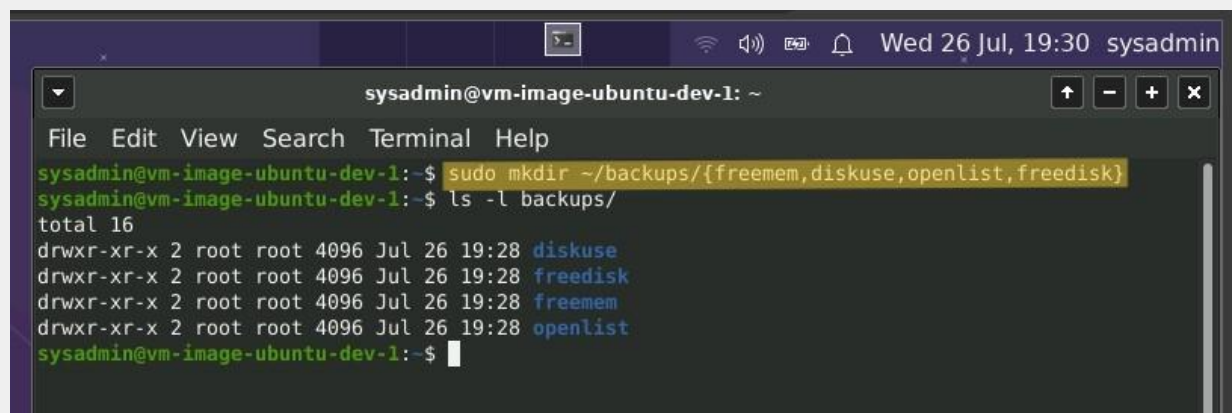
```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ crontab -e

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano          <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny
 4. /usr/bin/emacs
 5. /bin/ed

Choose 1-5 [1]: 1
crontab: installing new crontab
sysadmin@vm-image-ubuntu-dev-1:~$ 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 tar czf /auth_backup.tgz /var/log/auth.log
sysadmin@vm-image-ubuntu-dev-1:~$
```

## Step 3: Write Basic Bash Scripts

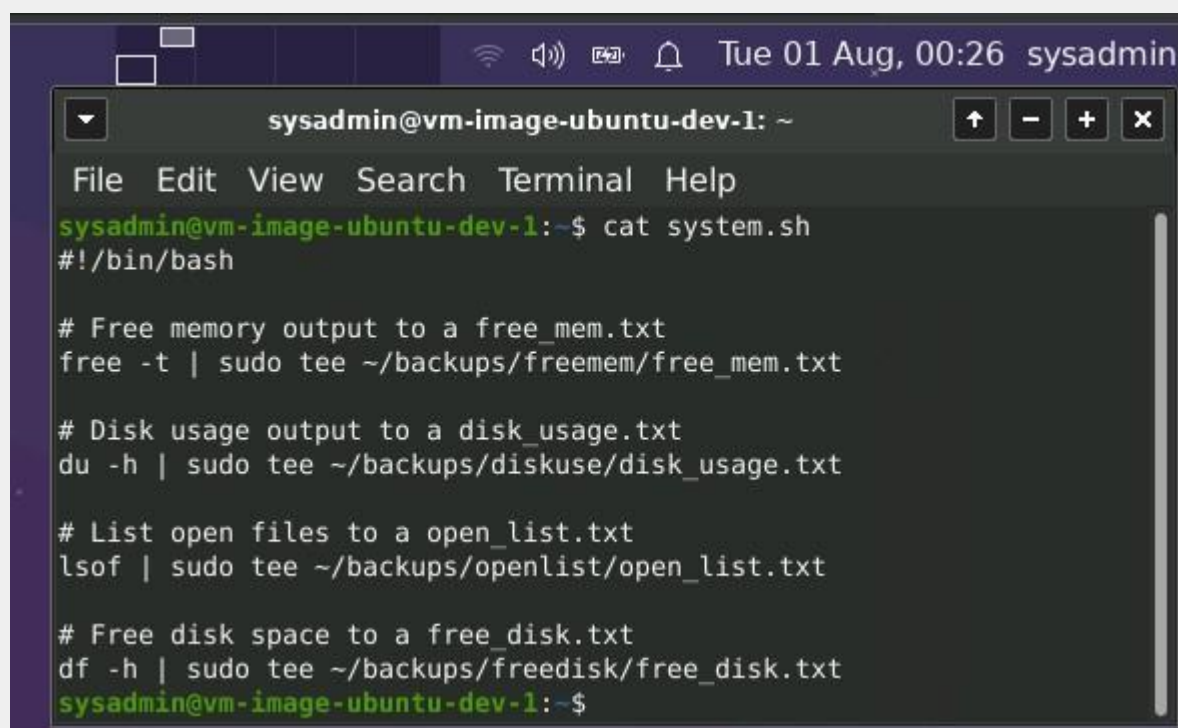
1. Brace expansion command to create the four subdirectories:



A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo mkdir ~/backups/{freemem,diskuse,openlist,freedisk}
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l backups/
total 16
drwxr-xr-x 2 root root 4096 Jul 26 19:28 diskuse
drwxr-xr-x 2 root root 4096 Jul 26 19:28 freedisk
drwxr-xr-x 2 root root 4096 Jul 26 19:28 freemem
drwxr-xr-x 2 root root 4096 Jul 26 19:28 openlist
sysadmin@vm-image-ubuntu-dev-1:~$
```

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



A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
sysadmin@vm-image-ubuntu-dev-1:~$ cat system.sh
#!/bin/bash

# Free memory output to a free_mem.txt
free -t | sudo tee ~/backups/freemem/free_mem.txt

# Disk usage output to a disk_usage.txt
du -h | sudo tee ~/backups/diskuse/disk_usage.txt

# List open files to a open_list.txt
lsof | sudo tee ~/backups/openlist/open_list.txt

# Free disk space to a free_disk.txt
df -h | sudo tee ~/backups/freedisk/free_disk.txt
sysadmin@vm-image-ubuntu-dev-1:~$
```

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

```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ nano system.sh
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l system.sh
-rw-rw-r-- 1 sysadmin sysadmin 332 Jul 28 17:52 system.sh
sysadmin@vm-image-ubuntu-dev-1:~$ sudo chmod +x system.sh
[sudo] password for sysadmin:
sysadmin@vm-image-ubuntu-dev-1:~$ ls -l system.sh
-rwxrwxr-x 1 sysadmin sysadmin 332 Jul 28 17:52 system.sh
sysadmin@vm-image-ubuntu-dev-1:~$
```

Optional

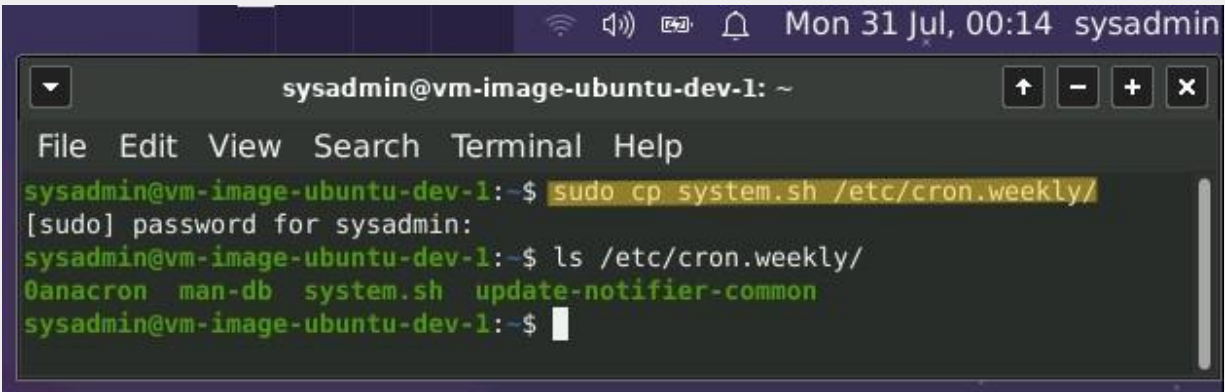
4. Commands to test the script and confirm its execution:

```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ ./system.sh
[sudo] password for sysadmin:
```

```
ns: sysadmin@vm-ima...
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ head -5 ~/backups/freemem/free_mem.txt
total      used      free      shared  buff/cache   available
Mem:      8129836 1901892 1111600    416040    5116344    5495784
Swap:      0         0         0
Total:    8129836 1901892 1111600
sysadmin@vm-image-ubuntu-dev-1:~$ head -5 ~/backups/freedisk/free_disk.txt
Filesystem      Size  Used Avail Use% Mounted on
/dev/root        29G   24G   5.6G   81% /
devtmpfs        3.9G     0   3.9G    0% /dev
tmpfs            3.9G     0   3.9G    0% /dev/shm
tmpfs            794M   1.8M   793M    1% /run
sysadmin@vm-image-ubuntu-dev-1:~$ head -5 ~/backups/diskuse/disk_usage.txt
36K ./Lucky_Duck_Investigations/Roulette_Loss_Investigation/Player_Dealer_Correlation
16K ./Lucky_Duck_Investigations/Roulette_Loss_Investigation/Player_Analysis
16K ./Lucky_Duck_Investigations/Roulette_Loss_Investigation/Dealer_Analysis
72K ./Lucky_Duck_Investigations/Roulette_Loss_Investigation
76K ./Lucky_Duck_Investigations
sysadmin@vm-image-ubuntu-dev-1:~$ head -5 ~/backups/openlist/open_list.txt
COMMAND  PID  TID TASKCMD  USER  FD  TYPE  DEVICE SIZE/OFF  NODE NAME
systemd  1    1    systemd  root  cwd  unknown  /proc/1/cwd (readlink: Permission denied)
systemd  1    1    systemd  root  rtd  unknown  /proc/1/root (readlink: Permission denied)
systemd  1    1    systemd  root  txt  unknown  /proc/1/exe (readlink: Permission denied)
systemd  1    1    systemd  root  NOFD  /proc/1/fd (opendir: Permission denied)
sysadmin@vm-image-ubuntu-dev-1:~$
```

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





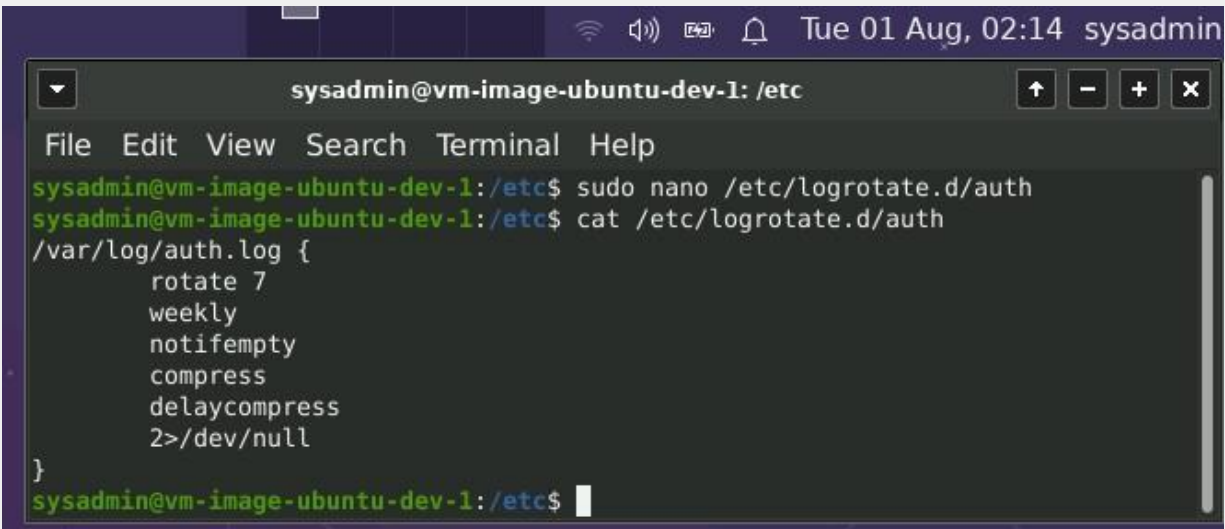
```
Mon 31 Jul, 00:14 sysadmin
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo cp system.sh /etc/cron.weekly/
[sudo] password for sysadmin:
sysadmin@vm-image-ubuntu-dev-1:~$ ls /etc/cron.weekly/
0anacron  man-db  system.sh  update-notifier-common
sysadmin@vm-image-ubuntu-dev-1:~$
```

## 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`.

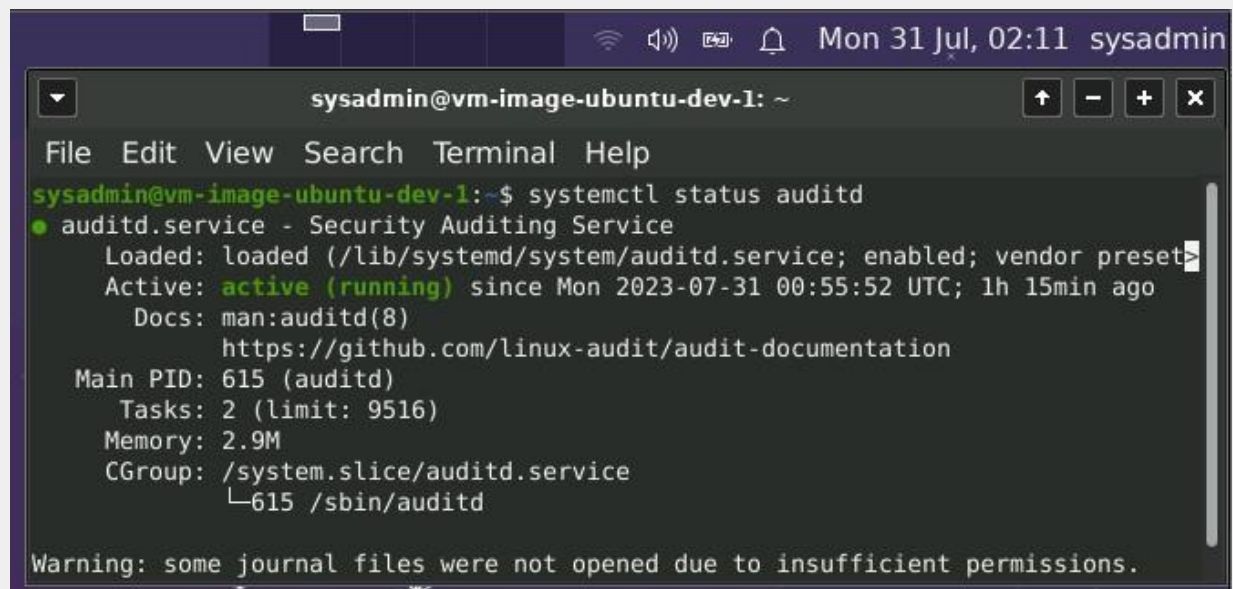
- a. Add your config file edits:



```
Tue 01 Aug, 02:14 sysadmin
sysadmin@vm-image-ubuntu-dev-1: /etc
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:/etc$ sudo nano /etc/logrotate.d/auth
sysadmin@vm-image-ubuntu-dev-1:/etc$ cat /etc/logrotate.d/auth
/var/log/auth.log {
    rotate 7
    weekly
    notifempty
    compress
    delaycompress
    2>/dev/null
}
sysadmin@vm-image-ubuntu-dev-1:/etc$
```

## Optional Additional Challenge: Check for Policy and File Violations

1. Command to verify `auditd` is active:



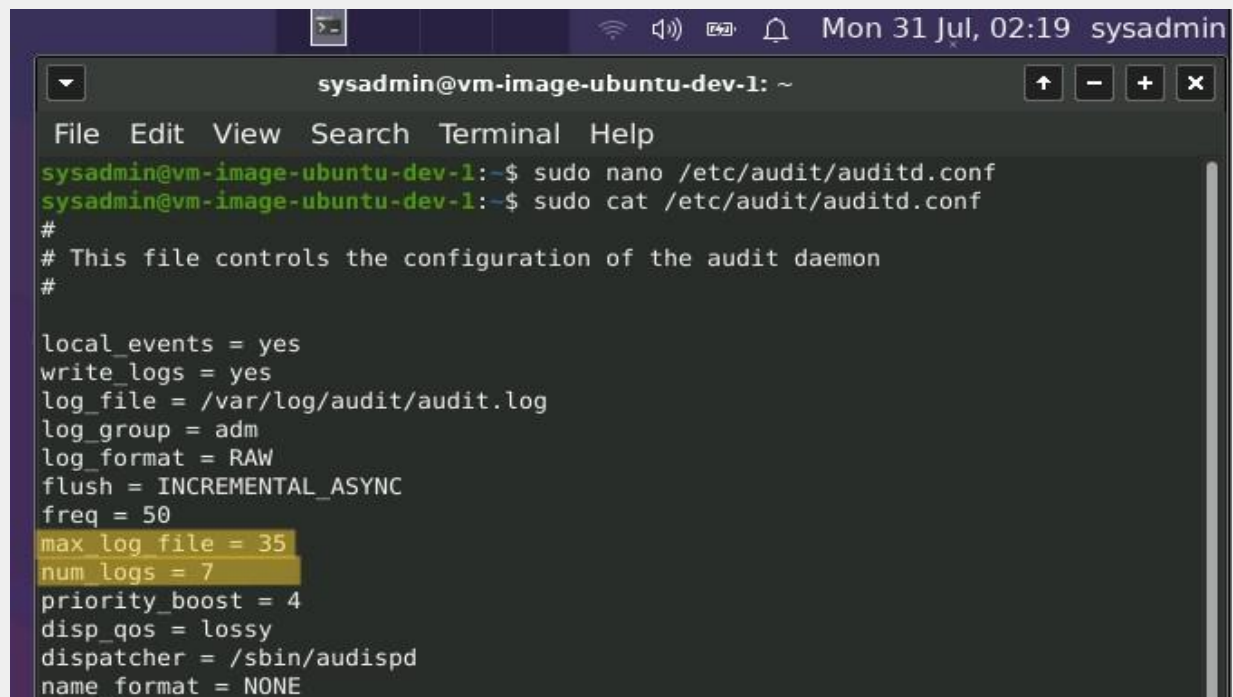
```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset:
   Active: active (running) since Mon 2023-07-31 00:55:52 UTC; 1h 15min ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Main PID: 615 (auditd)
     Tasks: 2 (limit: 9516)
    Memory: 2.9M
     CGroup: /system.slice/auditd.service
             └─615 /sbin/auditd

Warning: some journal files were not opened due to insufficient permissions.
```

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

```
sudo nano /etc/audit/auditd.conf
```

Add the edits made to the configuration file:

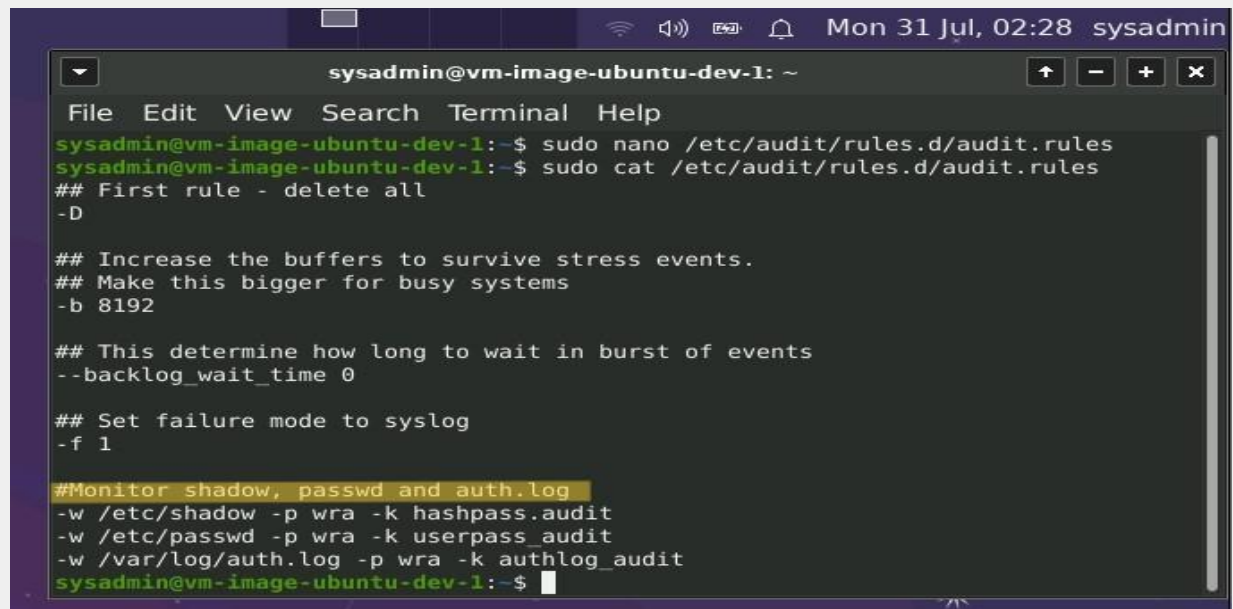


```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo nano /etc/audit/auditd.conf
sysadmin@vm-image-ubuntu-dev-1:~$ sudo cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = 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
```

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
```

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



A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo nano /etc/audit/rules.d/audit.rules
sysadmin@vm-image-ubuntu-dev-1:~$ sudo cat /etc/audit/rules.d/audit.rules
## First rule - delete all
-D

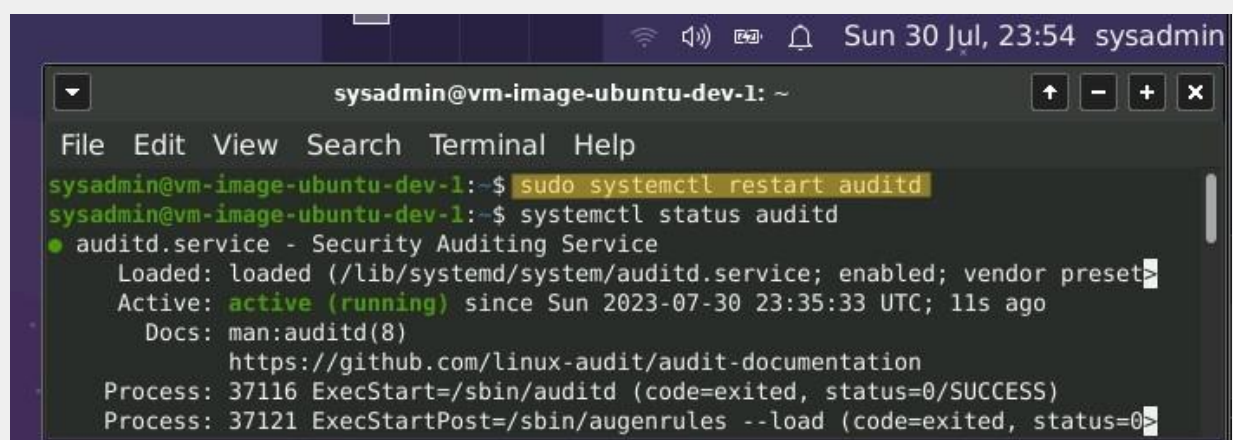
## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

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

## Set failure mode to syslog
-f 1

#Monitor shadow, passwd and auth.log
-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
sysadmin@vm-image-ubuntu-dev-1:~$
```

4. Command to restart `auditd`:

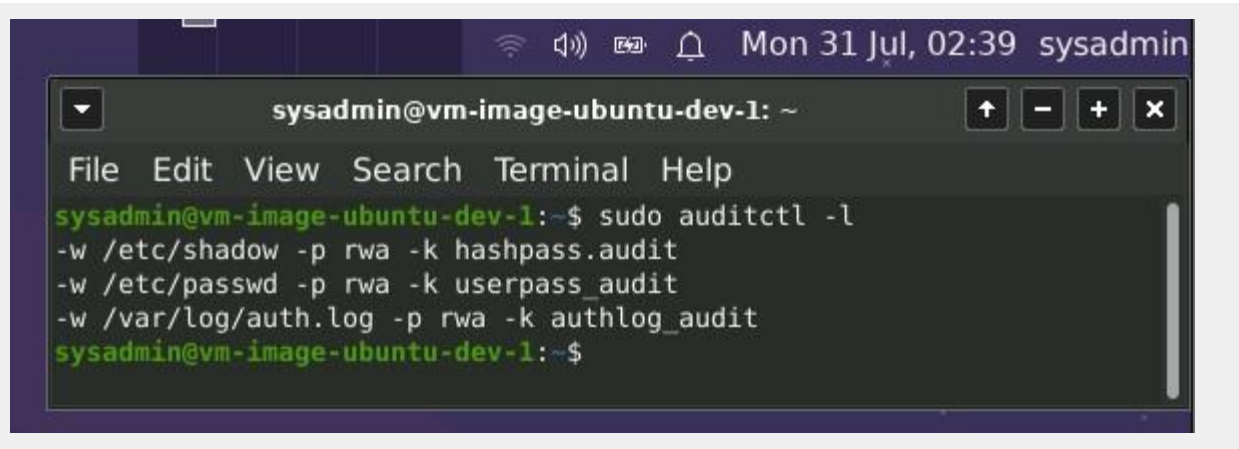


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo systemctl restart auditd
sysadmin@vm-image-ubuntu-dev-1:~$ systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset:
   Active: active (running) since Sun 2023-07-30 23:35:33 UTC; 11s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 37116 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Process: 37121 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/
```

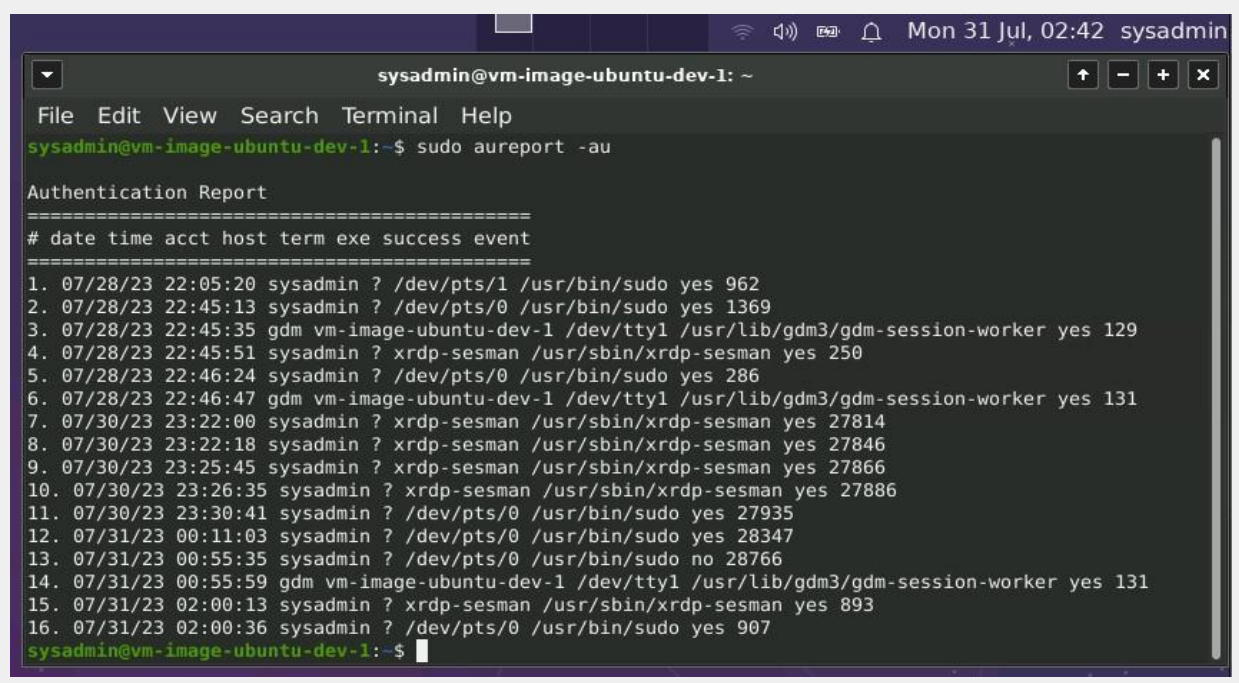
5. Command to list all `auditd` rules:





```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ 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@vm-image-ubuntu-dev-1:~$
```

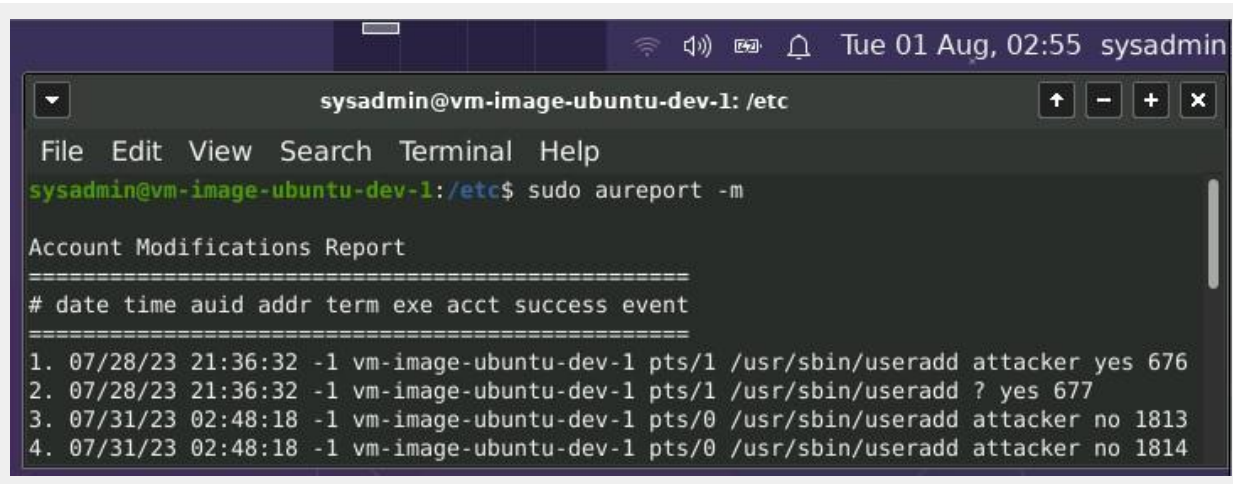
6. Command to produce an audit report:



```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo aureport -au

Authentication Report
=====
# date time acct host term exe success event
=====
1. 07/28/23 22:05:20 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 962
2. 07/28/23 22:45:13 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 1369
3. 07/28/23 22:45:35 gdm vm-image-ubuntu-dev-1 /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 129
4. 07/28/23 22:45:51 sysadmin ? xrdp-sesman /usr/sbin/xrdp-sesman yes 250
5. 07/28/23 22:46:24 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 286
6. 07/28/23 22:46:47 gdm vm-image-ubuntu-dev-1 /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 131
7. 07/30/23 23:22:00 sysadmin ? xrdp-sesman /usr/sbin/xrdp-sesman yes 27814
8. 07/30/23 23:22:18 sysadmin ? xrdp-sesman /usr/sbin/xrdp-sesman yes 27846
9. 07/30/23 23:25:45 sysadmin ? xrdp-sesman /usr/sbin/xrdp-sesman yes 27866
10. 07/30/23 23:26:35 sysadmin ? xrdp-sesman /usr/sbin/xrdp-sesman yes 27886
11. 07/30/23 23:30:41 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 27935
12. 07/31/23 00:11:03 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 28347
13. 07/31/23 00:55:35 sysadmin ? /dev/pts/0 /usr/bin/sudo no 28766
14. 07/31/23 00:55:59 gdm vm-image-ubuntu-dev-1 /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 131
15. 07/31/23 02:00:13 sysadmin ? xrdp-sesman /usr/sbin/xrdp-sesman yes 893
16. 07/31/23 02:00:36 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 907
sysadmin@vm-image-ubuntu-dev-1:~$
```

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

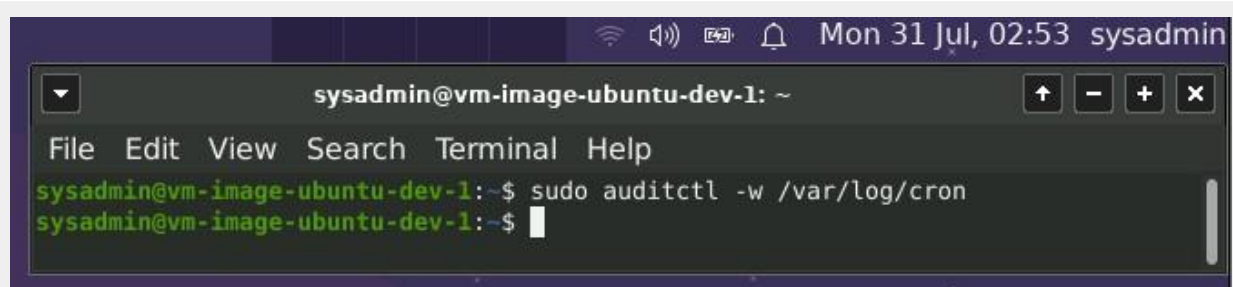


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: /etc' showing the output of the command 'sudo aureport -m'. The output is an 'Account Modifications Report' with a table of audit events. The table has columns: #, date, time, auid, addr, term, exe, acct, success, and event. It lists four events related to user additions.

```
sysadmin@vm-image-ubuntu-dev-1: /etc$ sudo aureport -m

Account Modifications Report
=====
# date time auid addr term exe acct success event
=====
1. 07/28/23 21:36:32 -1 vm-image-ubuntu-dev-1 pts/1 /usr/sbin/useradd attacker yes 676
2. 07/28/23 21:36:32 -1 vm-image-ubuntu-dev-1 pts/1 /usr/sbin/useradd ? yes 677
3. 07/31/23 02:48:18 -1 vm-image-ubuntu-dev-1 pts/0 /usr/sbin/useradd attacker no 1813
4. 07/31/23 02:48:18 -1 vm-image-ubuntu-dev-1 pts/0 /usr/sbin/useradd attacker no 1814
```

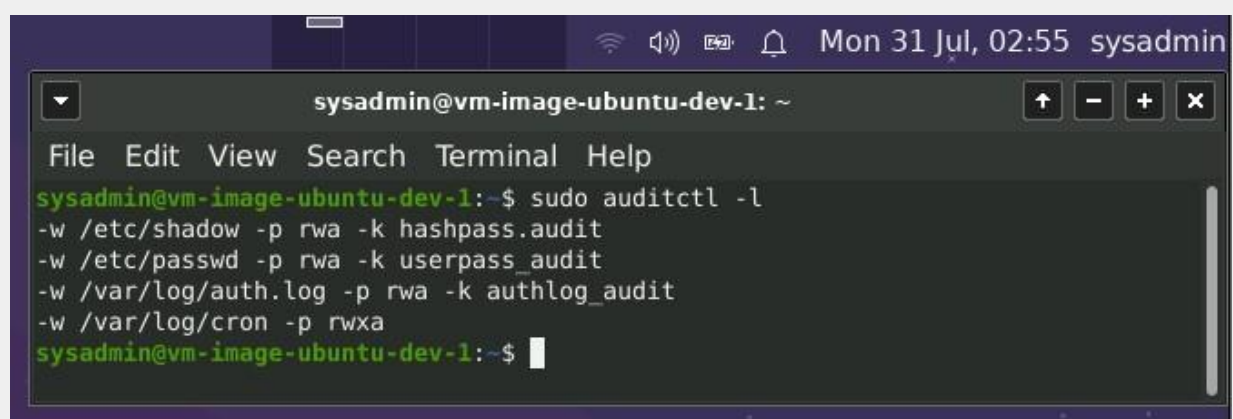
8. Command to use auditd to watch /var/log/cron:



A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' showing the command 'sudo auditctl -w /var/log/cron' being executed.

```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo auditctl -w /var/log/cron
sysadmin@vm-image-ubuntu-dev-1:~$
```

9. Command to verify auditd rules:

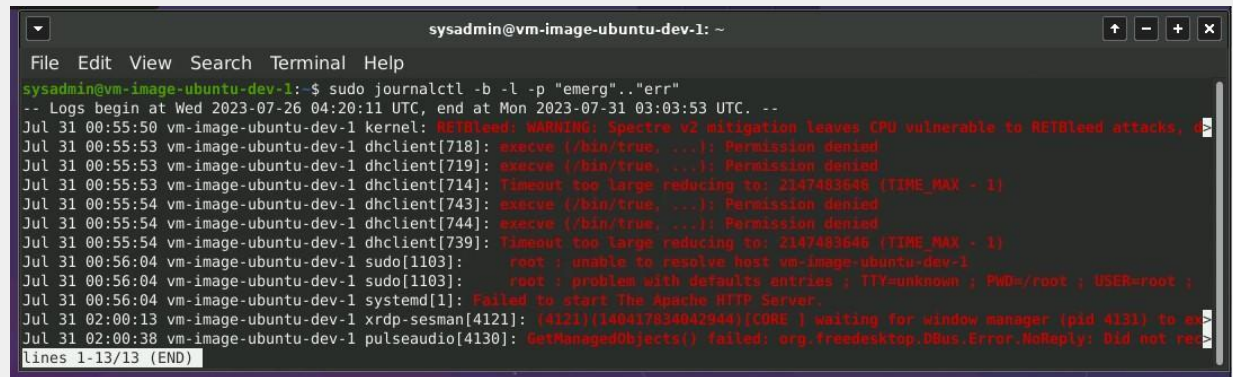


A terminal window titled 'sysadmin@vm-image-ubuntu-dev-1: ~' showing the command 'sudo auditctl -l' and its output, which lists the current audit rules.

```
sysadmin@vm-image-ubuntu-dev-1:~$ 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 rwx
```

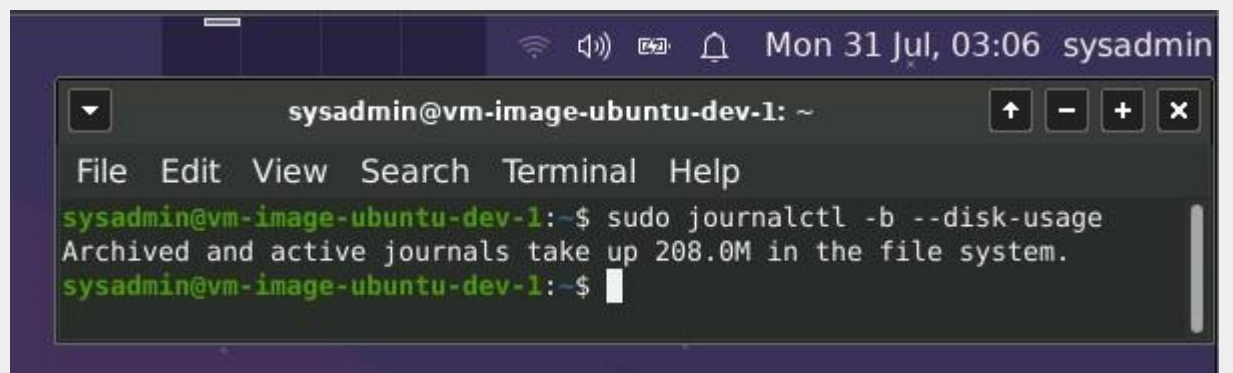
## Optional (Research Activity): Perform Various Log Filtering Techniques

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



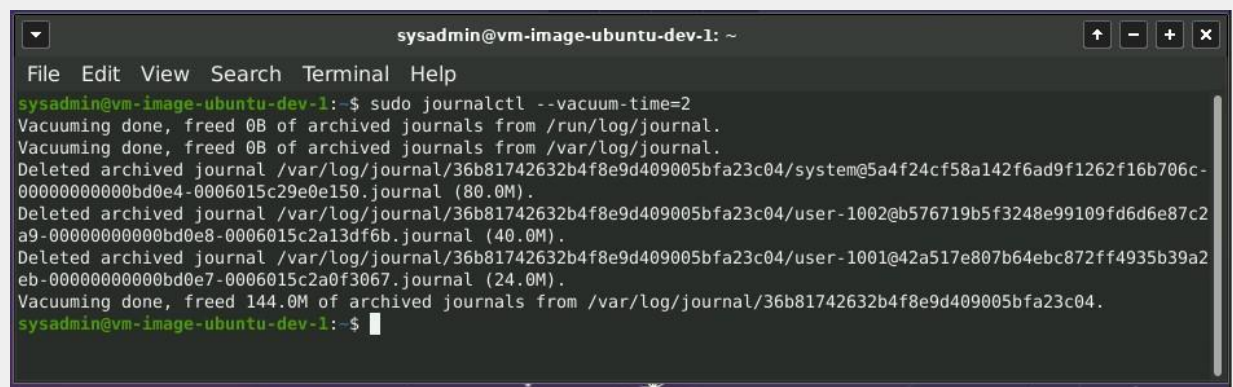
```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ sudo journalctl -b -l -p "emerg".. "err"  
-- Logs begin at Wed 2023-07-26 04:20:11 UTC, end at Mon 2023-07-31 03:03:53 UTC. --  
Jul 31 00:55:50 vm-image-ubuntu-dev-1 kernel: RETbleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to RETbleed attacks, d  
Jul 31 00:55:53 vm-image-ubuntu-dev-1 dhclient[718]: execve (/bin/true, ...): Permission denied  
Jul 31 00:55:53 vm-image-ubuntu-dev-1 dhclient[719]: execve (/bin/true, ...): Permission denied  
Jul 31 00:55:53 vm-image-ubuntu-dev-1 dhclient[714]: Timeout too large reducing to: 2147483646 (TIME_MAX - 1)  
Jul 31 00:55:54 vm-image-ubuntu-dev-1 dhclient[743]: execve (/bin/true, ...): Permission denied  
Jul 31 00:55:54 vm-image-ubuntu-dev-1 dhclient[744]: execve (/bin/true, ...): Permission denied  
Jul 31 00:55:54 vm-image-ubuntu-dev-1 dhclient[739]: Timeout too large reducing to: 2147483646 (TIME_MAX - 1)  
Jul 31 00:56:04 vm-image-ubuntu-dev-1 sudo[1103]: root : unable to resolve host vm-image-ubuntu-dev-1  
Jul 31 00:56:04 vm-image-ubuntu-dev-1 sudo[1103]: root : problem with defaults entries ; TTY=unknown ; PWD=/root ; USER=root ;  
Jul 31 00:56:04 vm-image-ubuntu-dev-1 systemd[1]: Failed to start The Apache HTTP Server.  
Jul 31 02:00:13 vm-image-ubuntu-dev-1 xrdp-sesman[4121]: (4121)(140417834042944)(CORE) waiting for window manager (pid 4131) to ex  
Jul 31 02:00:38 vm-image-ubuntu-dev-1 pulseaudio[4130]: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not re  
Lines 1-13/13 (END)
```

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



```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ sudo journalctl -b --disk-usage  
Archived and active journals take up 208.0M in the file system.  
sysadmin@vm-image-ubuntu-dev-1:~$
```

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



```
sysadmin@vm-image-ubuntu-dev-1: ~  
File Edit View Search Terminal Help  
sysadmin@vm-image-ubuntu-dev-1:~$ sudo journalctl --vacuum-time=2  
Vacuuming done, freed 0B of archived journals from /run/log/journal.  
Vacuuming done, freed 0B of archived journals from /var/log/journal.  
Deleted archived journal /var/log/journal/36b81742632b4f8e9d409005bfa23c04/system@5a4f24cf58a142f6ad9f1262f16b706c-  
0000000000bd0e4-0006015c29e0e150.journal (80.0M).  
Deleted archived journal /var/log/journal/36b81742632b4f8e9d409005bfa23c04/user-1002@b576719b5f3248e99109fd6d6e87c2  
a9-0000000000bd0e8-0006015c2a13df6b.journal (40.0M).  
Deleted archived journal /var/log/journal/36b81742632b4f8e9d409005bfa23c04/user-1001@42a517e807b64ebc872ff4935b39a2  
eb-0000000000bd0e7-0006015c2a0f3067.journal (24.0M).  
Vacuuming done, freed 144.0M of archived journals from /var/log/journal/36b81742632b4f8e9d409005bfa23c04.  
sysadmin@vm-image-ubuntu-dev-1:~$
```

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



```
sysadmin@vm-image-ubuntu-dev-1: ~
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:~$ sudo journalctl --priority="emerg".. "crit" > /home/sysadmin/Priority_High.txt
sysadmin@vm-image-ubuntu-dev-1:~$
```

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

```
sysadmin@vm-image-ubuntu-dev-1: /
File Edit View Search Terminal Help
sysadmin@vm-image-ubuntu-dev-1:/$ crontab -e
crontab: installing new crontab
sysadmin@vm-image-ubuntu-dev-1:/$ 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 tar czf /auth backup.tgz /var/log/auth.log
0 0 * * * journalctl --priority="emerg".. "crit" > /home/sysadmin/Priority_High.txt
sysadmin@vm-image-ubuntu-dev-1:/$
```