

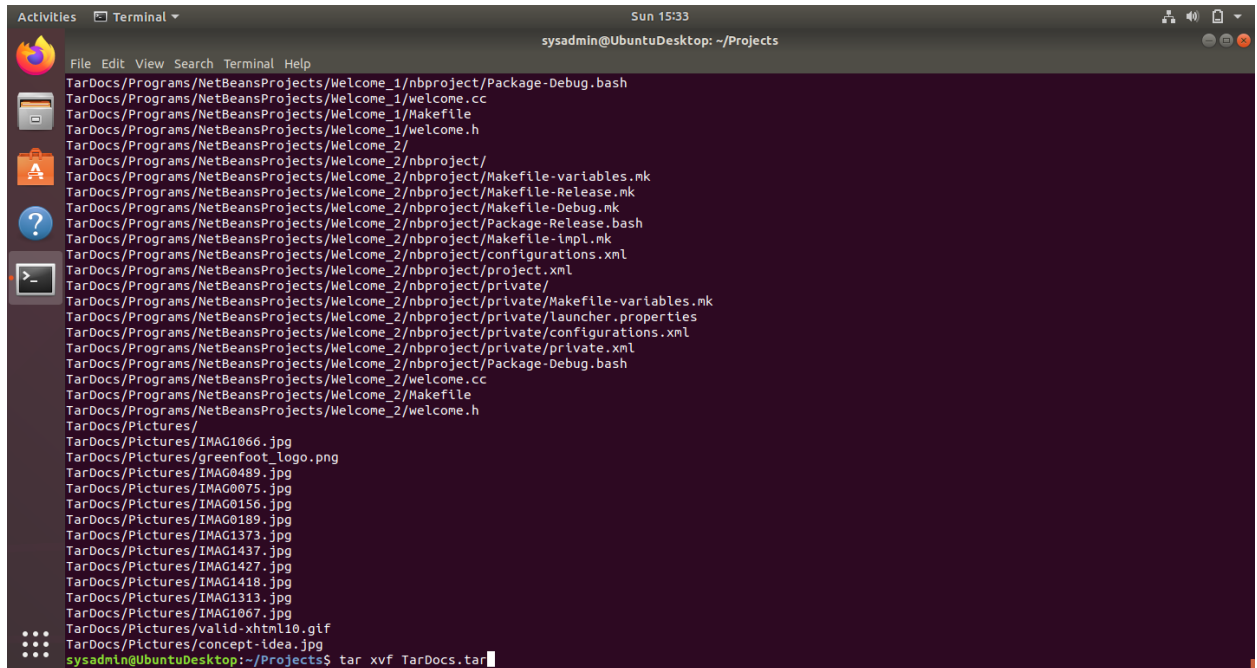
# Week 5 Homework Submission File: Archiving and Logging Data

---

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

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

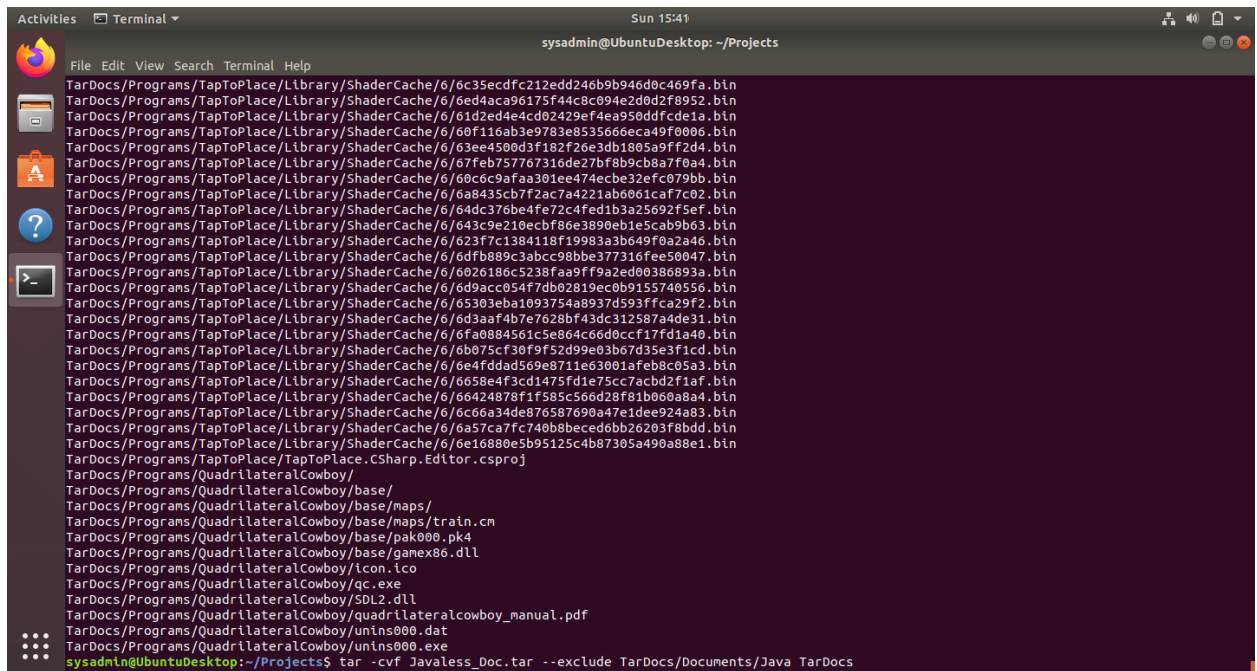
`tar xvf TarDocs.tar`



A terminal window titled "Terminal" with a dark background. The window shows the output of the command `tar xvf TarDocs.tar`. The output lists the contents of the archive, including files and directories such as `TarDocs/Programs/NetBeansProjects/Welcome_1/nbproject/Package-Debug.bash`, `TarDocs/Pictures/IMAG1066.jpg`, and `TarDocs/Pictures/valid-xhtml10.gif`. The terminal window also shows the command prompt `sysadmin@UbuntuDesktop: ~/Projects` and the command `tar xvf TarDocs.tar` being executed.

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

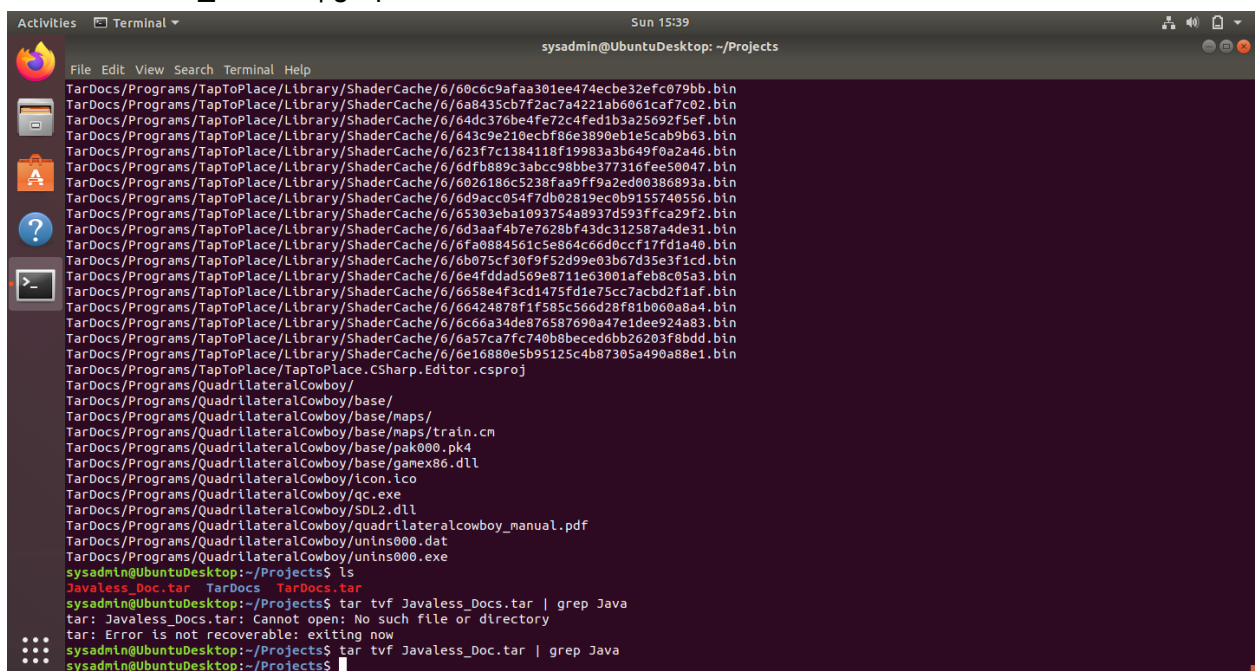
tar -cvf Javaless\_Doc.tar - --exclude TarDocs/Documents/Java TarDocs



```
Activities Terminal Sun 15:41
sysadmin@UbuntuDesktop: ~/Projects
File Edit View Search Terminal Help
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6c35ecdfc212edd246b9b946d0c469fa.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6ed4aca96175f44c8c094e2d0d2f8952.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/61d2ed4e4cd02429ef4ea95dddfcde1a.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/60f116ab3e9783e853566eca49f0006.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/63ee4500d3f182f26e3db1805a9ff2d4.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/67feb757767316de27bf8b9cb8a7f0a4.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/60c6c9afaa301ee474ecbe32efc079bb.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6a8435cb7f2ac7a4221ab6061caf7c02.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/64dc376be4fe72c4fed1b3a25692f5ef.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/643c9e210ecbf86e3890eb1e5cab9b63.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/623f7c1384118f19983a3b649f0a2a46.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6dfb889c3abcc98bbe377316fee50047.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6026186c5238faa9ff9a2ed00386893a.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6d9acc054f7db02819ec0b9155740556.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/65303eba1093754a8937d593ffca29f2.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6d3aaf4b7e7628bf43dc312587a4de31.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6fa0884561c5e864c66d0ccf17fd1a40.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6b075cf30f9f52d99e03b67d35e3f1cd.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6e4fddad569e8711e63001afeb8c05a3.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6658e4f3cd1475fd1e75cc7acbd2f1af.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/66424878f1f585c566d28f81b060a8a4.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6c66a34de876587690a471dee924a83.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6a57ca7fc740b8beced6bb26203f8bdd.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6e16880e5b95125c4b87305a490a88e1.bin
TarDocs/Programs/TapToPlace/TapToPlace.CSharp.Editor.csproj
TarDocs/Programs/QuadrilateralCowboy/
TarDocs/Programs/QuadrilateralCowboy/base/
TarDocs/Programs/QuadrilateralCowboy/base/maps/
TarDocs/Programs/QuadrilateralCowboy/base/maps/train.cm
TarDocs/Programs/QuadrilateralCowboy/base/pak000.pk4
TarDocs/Programs/QuadrilateralCowboy/base/gamex86.dll
TarDocs/Programs/QuadrilateralCowboy/icon.ico
TarDocs/Programs/QuadrilateralCowboy/qc.exe
TarDocs/Programs/QuadrilateralCowboy/SDL2.dll
TarDocs/Programs/QuadrilateralCowboy/quadrilateralcowboy_manual.pdf
TarDocs/Programs/QuadrilateralCowboy/unins000.dat
TarDocs/Programs/QuadrilateralCowboy/unins000.exe
sysadmin@UbuntuDesktop:~/Projects$ tar -cvf Javaless_Doc.tar --exclude TarDocs/Documents/Java TarDocs
```

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

tar tvf Javaless\_Doc.tar | grep Java



```
Activities Terminal Sun 15:39
sysadmin@UbuntuDesktop: ~/Projects
File Edit View Search Terminal Help
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/60c6c9afaa301ee474ecbe32efc079bb.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6a8435cb7f2ac7a4221ab6061caf7c02.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/64dc376be4fe72c4fed1b3a25692f5ef.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/643c9e210ecbf86e3890eb1e5cab9b63.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/623f7c1384118f19983a3b649f0a2a46.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6dfb889c3abcc98bbe377316fee50047.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6026186c5238faa9ff9a2ed00386893a.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6d9acc054f7db02819ec0b9155740556.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/65303eba1093754a8937d593ffca29f2.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6d3aaf4b7e7628bf43dc312587a4de31.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6fa0884561c5e864c66d0ccf17fd1a40.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6b075cf30f9f52d99e03b67d35e3f1cd.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6e4fddad569e8711e63001afeb8c05a3.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6658e4f3cd1475fd1e75cc7acbd2f1af.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/66424878f1f585c566d28f81b060a8a4.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6c66a34de876587690a471dee924a83.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6a57ca7fc740b8beced6bb26203f8bdd.bin
TarDocs/Programs/TapToPlace/Library/ShaderCache/6/6e16880e5b95125c4b87305a490a88e1.bin
TarDocs/Programs/TapToPlace/TapToPlace.CSharp.Editor.csproj
TarDocs/Programs/QuadrilateralCowboy/
TarDocs/Programs/QuadrilateralCowboy/base/
TarDocs/Programs/QuadrilateralCowboy/base/maps/
TarDocs/Programs/QuadrilateralCowboy/base/maps/train.cm
TarDocs/Programs/QuadrilateralCowboy/base/pak000.pk4
TarDocs/Programs/QuadrilateralCowboy/base/gamex86.dll
TarDocs/Programs/QuadrilateralCowboy/icon.ico
TarDocs/Programs/QuadrilateralCowboy/qc.exe
TarDocs/Programs/QuadrilateralCowboy/SDL2.dll
TarDocs/Programs/QuadrilateralCowboy/quadrilateralcowboy_manual.pdf
TarDocs/Programs/QuadrilateralCowboy/unins000.dat
TarDocs/Programs/QuadrilateralCowboy/unins000.exe
sysadmin@UbuntuDesktop:~/Projects$ ls
Javaless_Doc.tar TarDocs TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ tar tvf Javaless_Docs.tar | grep Java
tar: Javaless_Docs.tar: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
sysadmin@UbuntuDesktop:~/Projects$ tar tvf Javaless_Doc.tar | grep Java
sysadmin@UbuntuDesktop:~/Projects$
```

## Bonus

- Command to create an incremental archive called logs\_backup\_tar.gz with only changed files to snapshot.filefor the /var/log directory:

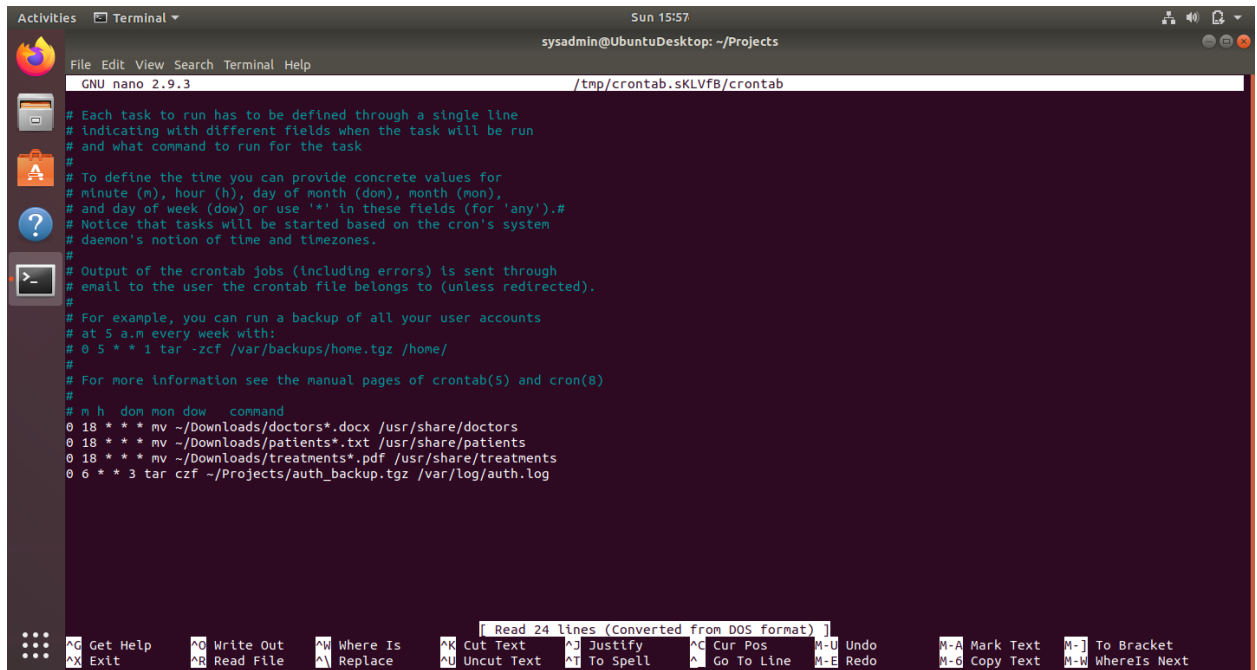
## Critical Analysis Question

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

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

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

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



```
Activities  Terminal  Sun 15:57
sysadmin@UbuntuDesktop: ~/Projects

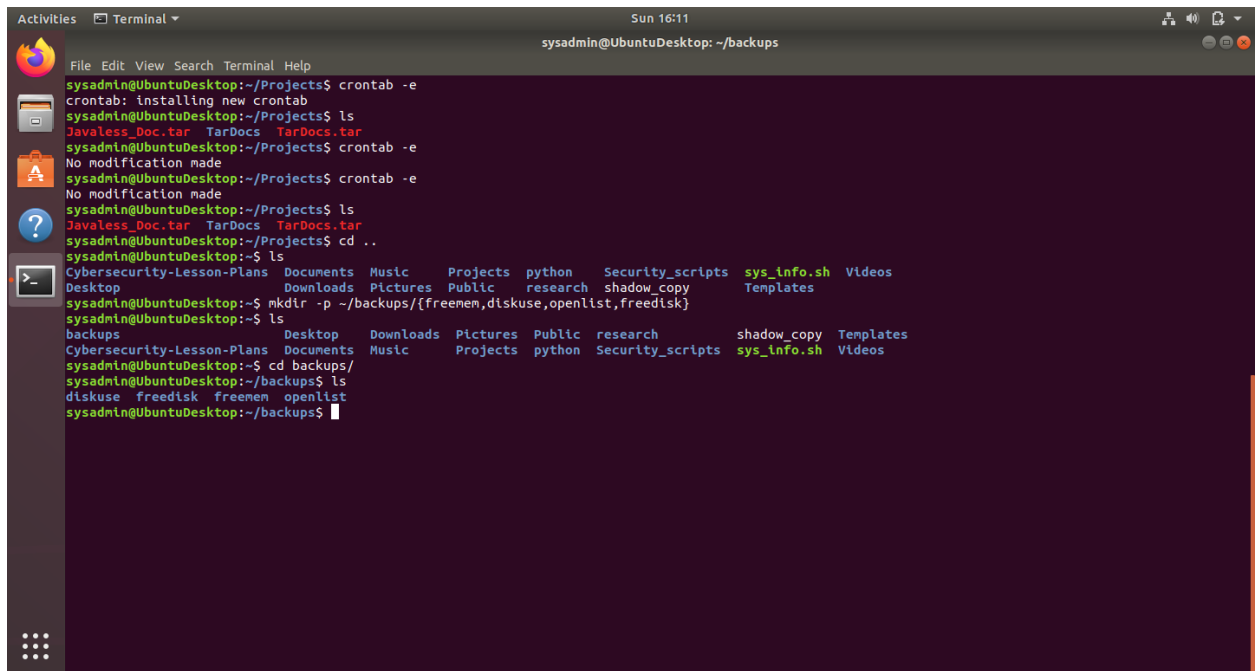
File Edit View Search Terminal Help
GNU nano 2.9.3 /tmp/crontab.sKLVFB/crontab

# 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 18 * * * mv ~/Downloads/doctors*.docx /usr/share/doctors
0 18 * * * mv ~/Downloads/patients*.txt /usr/share/patients
0 18 * * * mv ~/Downloads/treatments*.pdf /usr/share/treatments
0 6 * * 3 tar czf ~/Projects/auth_backup.tgz /var/log/auth.log
```

## Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

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

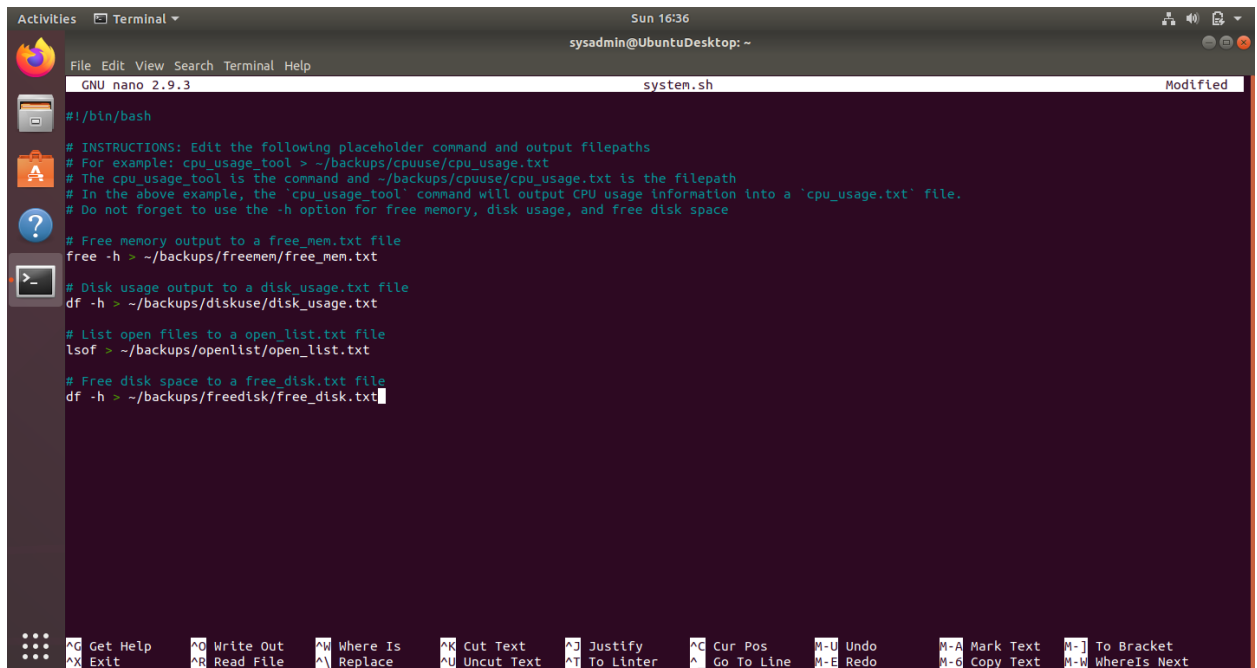


```
sysadmin@UbuntuDesktop: ~/backups
sysadmin@UbuntuDesktop:~/Projects$ crontab -e
crontab: installing new crontab
sysadmin@UbuntuDesktop:~/Projects$ ls
Javaless_Doc.tar  TarDocs  TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ crontab -e
No modification made
sysadmin@UbuntuDesktop:~/Projects$ crontab -e
No modification made
sysadmin@UbuntuDesktop:~/Projects$ ls
Javaless_Doc.tar  TarDocs  TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ cd ..
sysadmin@UbuntuDesktop:~$ ls
Cybersecurity-Lesson-Plans  Desktop  Downloads  Music  Projects  python  Security_scripts  sys_info.sh  Videos
sysadmin@UbuntuDesktop:~$ mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}
sysadmin@UbuntuDesktop:~$ ls
backups  Desktop  Downloads  Pictures  Public  research  shadow_copy  Templates
sysadmin@UbuntuDesktop:~$ cd backups/
sysadmin@UbuntuDesktop:~/backups$ ls
diskuse  freemem  freemem  openlist
sysadmin@UbuntuDesktop:~/backups$
```

Paste your system.sh script edits below:

`#!/bin/bash`

2. [Your solution script contents here]



```
GNU nano 2.9.3 system.sh Modified
#!/bin/bash

# INSTRUCTIONS: Edit the following placeholder command and output filepaths
# For example: cpu_usage_tool > ~/backups/cpuuse/cpu_usage.txt
# The cpu_usage_tool is the command and ~/backups/cpuuse/cpu_usage.txt is the filepath
# In the above example, the 'cpu_usage_tool' command will output CPU usage information into a 'cpu_usage.txt' file.
# Do not forget to use the -h option for free memory, disk usage, and free disk space

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

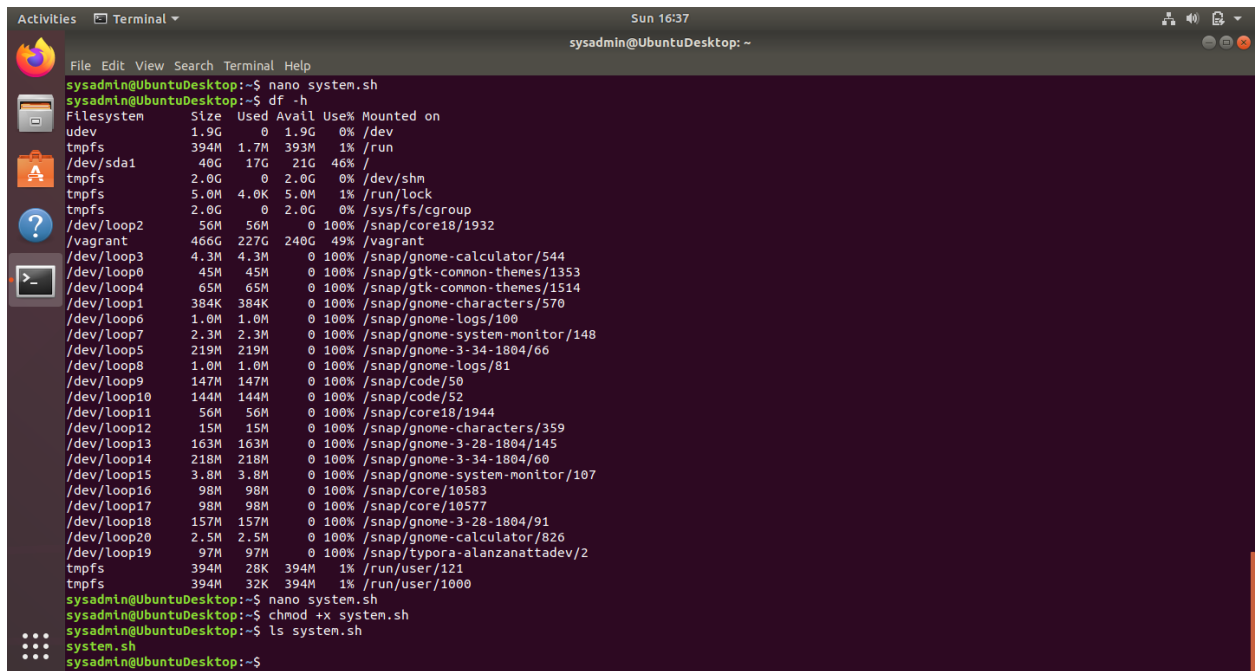
# Disk usage output to a disk_usage.txt file
df -h > ~/backups/diskuse/disk_usage.txt

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

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

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

chmod +x system.sh



The screenshot shows a terminal window with the following commands and output:

```
sysadmin@UbuntuDesktop:~$ nano system.sh
sysadmin@UbuntuDesktop:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M   1.7M  393M   1% /run
/dev/sda1       46G    17G   21G  46% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M   4.0K  5.0M   1% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop2      56M    56M   0 100% /snap/core18/1932
/vagrant        466G  227G  240G  49% /vagrant
/dev/loop3      4.3M   4.3M   0 100% /snap/gnome-calculator/544
/dev/loop6      45M    45M   0 100% /snap/gtk-common-themes/1353
/dev/loop4      65M    65M   0 100% /snap/gtk-common-themes/1514
/dev/loop1     384K   384K   0 100% /snap/gnome-characters/570
/dev/loop6      1.0M   1.0M   0 100% /snap/gnome-logs/100
/dev/loop7      2.3M   2.3M   0 100% /snap/gnome-system-monitor/148
/dev/loop5     219M  219M   0 100% /snap/gnome-3-34-1804/66
/dev/loop8      1.0M   1.0M   0 100% /snap/gnome-logs/81
/dev/loop9     147M  147M   0 100% /snap/code/50
/dev/loop10    144M  144M   0 100% /snap/code/52
/dev/loop11     56M   56M   0 100% /snap/core18/1944
/dev/loop12     15M   15M   0 100% /snap/gnome-characters/359
/dev/loop13    163M  163M   0 100% /snap/gnome-3-28-1804/145
/dev/loop14    218M  218M   0 100% /snap/gnome-3-34-1804/60
/dev/loop15     3.8M   3.8M   0 100% /snap/gnome-system-monitor/107
/dev/loop16     98M   98M   0 100% /snap/core/10583
/dev/loop17     98M   98M   0 100% /snap/core/10577
/dev/loop18    157M  157M   0 100% /snap/gnome-3-28-1804/91
/dev/loop20     2.5M   2.5M   0 100% /snap/gnome-calculator/826
/dev/loop19     97M   97M   0 100% /snap/typora-alanzanattadev/2
tmpfs          394M   28K  394M   1% /run/user/121
tmpfs          394M   32K  394M   1% /run/user/1000
sysadmin@UbuntuDesktop:~$ nano system.sh
sysadmin@UbuntuDesktop:~$ chmod +x system.sh
sysadmin@UbuntuDesktop:~$ ls system.sh
system.sh
sysadmin@UbuntuDesktop:~$
```

## Optional

- Commands to test the script and confirm its execution: `./system.sh`

## Bonus

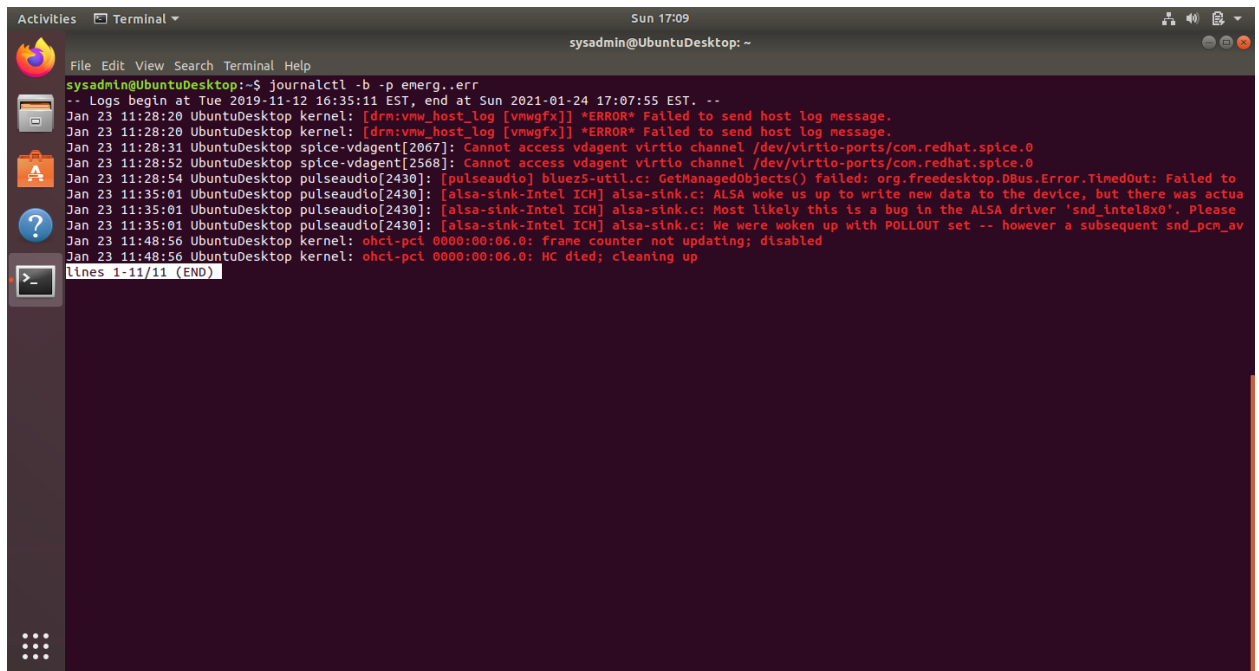
- Command to copy system to system-wide cron directory:

---

## Step 4: Perform Various Log Filtering Techniques

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

journalctl -b -p emerg..err

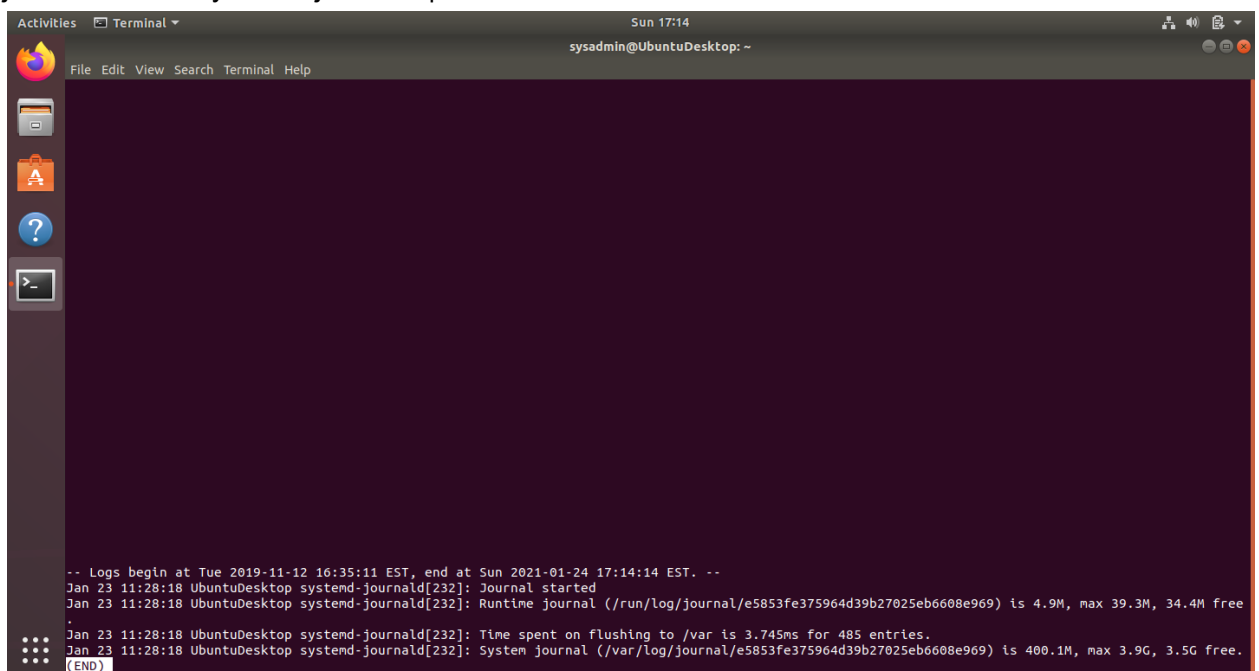


A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Sun 17:09, sysadmin@UbuntuDesktop: ~). The terminal shows the command `journalctl -b -p emerg..err` and its output, which lists emergency logs from January 23, 2021. The logs include errors from the kernel and pulseaudio, such as 'Failed to send host log message' and 'Cannot access vagent virtio channel'. The output ends with 'lines 1-11/11 (END)'.

```
sysadmin@UbuntuDesktop:~$ journalctl -b -p emerg..err
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Sun 2021-01-24 17:07:55 EST. --
Jan 23 11:28:20 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Jan 23 11:28:20 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Jan 23 11:28:31 UbuntuDesktop spice-vdagent[2567]: Cannot access vagent virtio channel /dev/virtio-ports/com.redhat.spice.0
Jan 23 11:28:52 UbuntuDesktop spice-vdagent[2568]: Cannot access vagent virtio channel /dev/virtio-ports/com.redhat.spice.0
Jan 23 11:28:54 UbuntuDesktop pulseaudio[2430]: [pulseaudio] bluez5-uttl.c: GetManagedObjects() failed: org.freedesktop.DBus.Error.TimedOut: Failed to
Jan 23 11:35:01 UbuntuDesktop pulseaudio[2430]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write new data to the device, but there was actua
Jan 23 11:35:01 UbuntuDesktop pulseaudio[2430]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a bug in the ALSA driver 'snd_intel8x0'. Please
Jan 23 11:35:01 UbuntuDesktop pulseaudio[2430]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up with POLLOUT set -- however a subsequent snd_pcm_av
Jan 23 11:48:56 UbuntuDesktop kernel: ohci-pci 0000:00:06.0: frame counter not updating; disabled
Jan 23 11:48:56 UbuntuDesktop kernel: ohci-pci 0000:00:06.0: HC died; cleaning up
lines 1-11/11 (END)
```

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

journalctl -b -u systemd-journald | less



A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Sun 17:14, sysadmin@UbuntuDesktop: ~). The terminal shows the command `journalctl -b -u systemd-journald | less` and its output, which displays the disk usage of the system journal. The output includes the command `journalctl -b -u systemd-journald` and the resulting disk usage statistics, such as 'Runtime journal (/run/log/journal/e5853fe375964d39b27025eb6608e969) is 4.9M, max 39.3M, 34.4M free'. The output ends with 'lines 1-11/11 (END)'.

```
sysadmin@UbuntuDesktop:~$ journalctl -b -u systemd-journald | less
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Sun 2021-01-24 17:14:14 EST. --
Jan 23 11:28:18 UbuntuDesktop systemd-journald[232]: Journal started
Jan 23 11:28:18 UbuntuDesktop systemd-journald[232]: Runtime journal (/run/log/journal/e5853fe375964d39b27025eb6608e969) is 4.9M, max 39.3M, 34.4M free
Jan 23 11:28:18 UbuntuDesktop systemd-journald[232]: Time spent on flushing to /var is 3.745ms for 485 entries.
Jan 23 11:28:18 UbuntuDesktop systemd-journald[232]: System journal (/var/log/journal/e5853fe375964d39b27025eb6608e969) is 400.1M, max 3.9G, 3.5G free.
lines 1-11/11 (END)
```

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

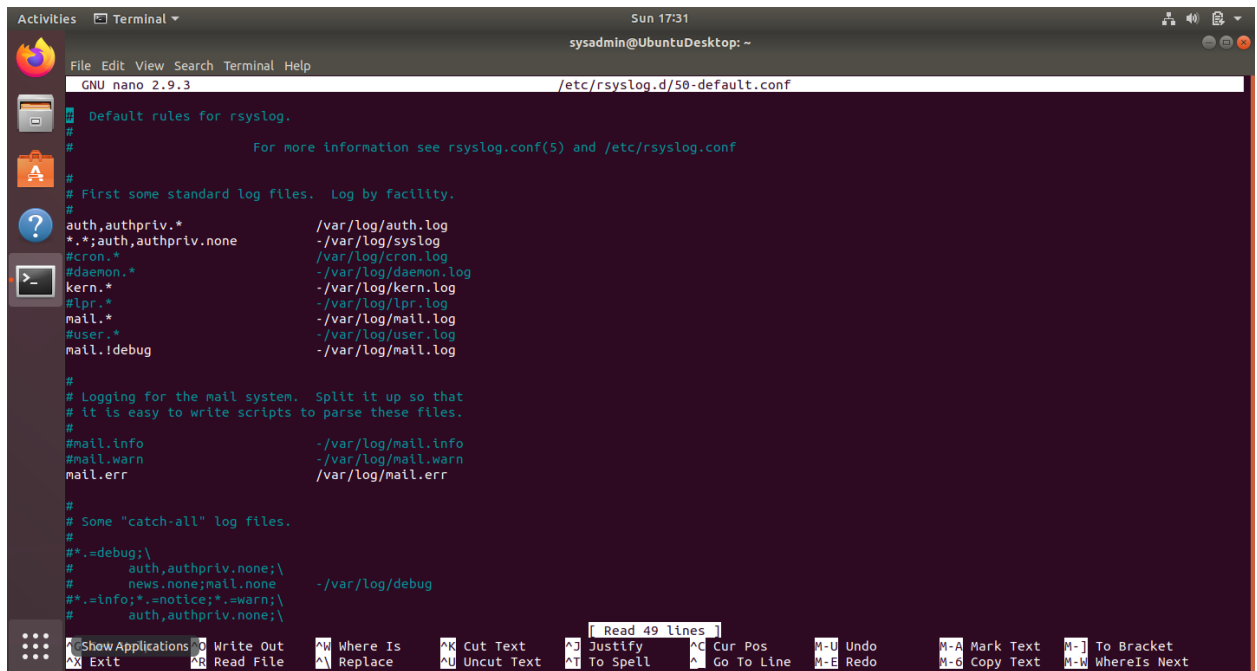
[illegible]

- Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:
- Command to automate the last command in a daily cronjob:
- Add the edits made to the crontab file below:  
[Your solution cron edits here]

1. Command to record all mail log messages, except for debug, to `/var/log/mail.log`:
  - Add the edits made to the configuration file below:

```
mail.!debug      -/var/log/mail.log
```

## 2. [Your solution edits here]



```
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/rsyslog.d/50-default.conf

# Default rules for rsyslog.
#
# For more information see rsyslog.conf(5) and /etc/rsyslog.conf
#
# First some standard log files.  Log by facility.
#
auth,authpriv.*      /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.*              /var/log/cron.log
#daemon.*            /var/log/daemon.log
#kern.*               /var/log/kern.log
#lpr.*                /var/log/lpr.log
#mail.*               /var/log/mail.log
#user.*               /var/log/user.log
mail.!debug           /var/log/mail.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info            /var/log/mail.info
#mail.warn            /var/log/mail.warn
mail.err              /var/log/mail.err
#
# Some "catch-all" log files.
#
#*.debug;\
#   auth,authpriv.none;\
#   news.none;mail.none -/var/log/debug
#*.info;*.notice;*.warn;\
#   auth,authpriv.none;\
#   mail.none;mail.err   /var/log/debug
#
# Show Applications Write Out Where Is Cut Text Justify Cur Pos M-U Undo M-A Mark Text M-J To Bracket
# Exit Read File Replace Uncut Text To Spell Go To Line M-E Redo M-C Copy Text M-W WhereIs Next
```

## Bonus

- Command to record all boot log messages, except for info and debug, to /var/log/boot.log:
  - Add the edits made to the configuration file below:
- [Your solution edits here]

## Step 6. 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.
  - Add your config file edits below:

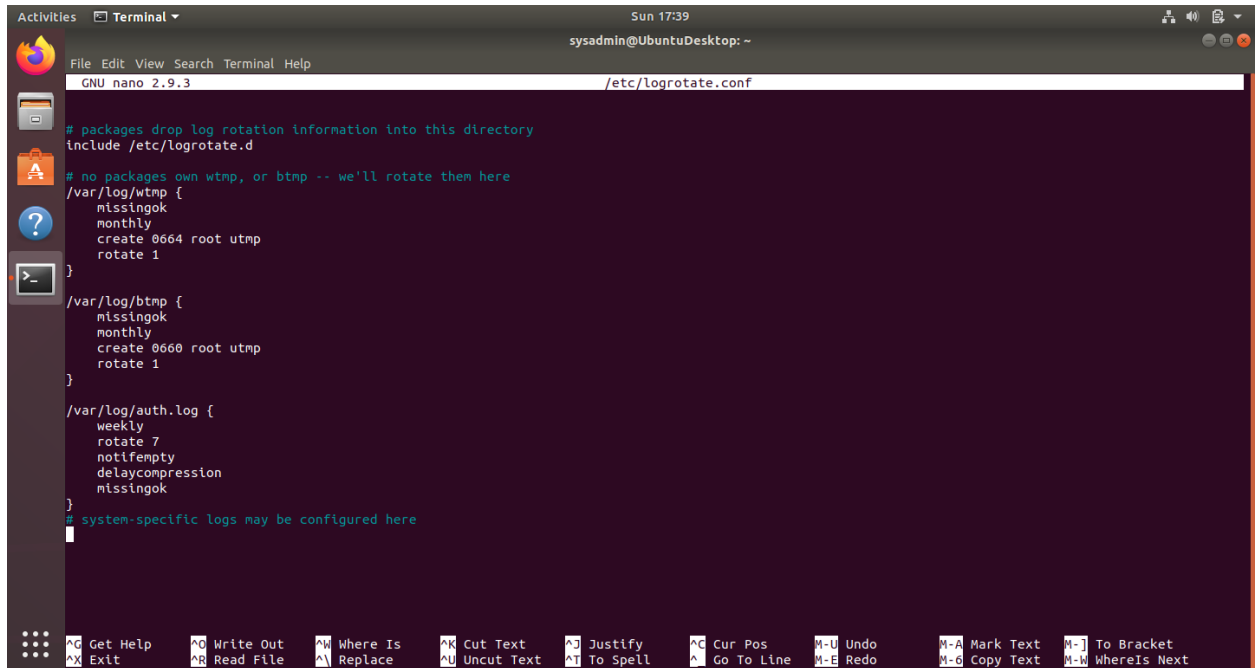
```
/var/log/auth.log {  
  
    weekly  
  
    rotate 7  
  
    notifempty  
  
    delaycompression
```



Missingok

}

## 2. [Your logrotate scheme edits here]



The screenshot shows a terminal window titled 'Terminal' with the user 'sysadmin@UbuntuDesktop: ~'. The terminal is running the nano text editor on the file '/etc/logrotate.conf'. The file content is as follows:

```
# 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
}

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

# system-specific logs may be configured here
```

The terminal window includes a menu bar with options: File, Edit, View, Search, Terminal, Help. The status bar at the bottom shows various keyboard shortcuts for nano editor operations.

## Bonus: Check for Policy and File Violations

1. Command to verify auditd is active:
2. Command to set number of retained logs and maximum log file size:
  - o Add the edits made to the configuration file below:
3. [Your solution edits here]
4. Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log:
  - o Add the edits made to the rules file below:
5. [Your solution edits here]
6. Command to restart auditd:
7. Command to list all auditd rules:
8. Command to produce an audit report:
9. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:
10. Command to use auditd to watch /var/log/cron:
11. Command to verify auditd rules: