**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**

Home Dircetory:

sysadmin@ubuntuDesktop:~$ pwd

/home/sysadmin/

mkdir Projects

Download files “TarDocs.tar from firefox browser.

~/Projects/TarDocs.tar

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

$ cd Projects

$ sudo tar tvvf TarDocs.tar | more (Verify the files insides the tar)

$ sudo tar xvvf Project/TarDocs.tar -C Projects/

$ ls Projects/

TarDocs TarDocs.tar

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

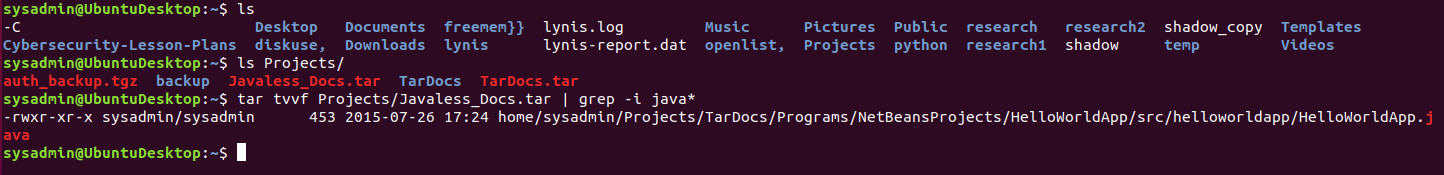
First verify the file location:

$ ls Projects/TarDocs/

Documents Financials Movies Pictures Programs (These folders are inside the TarDocs)

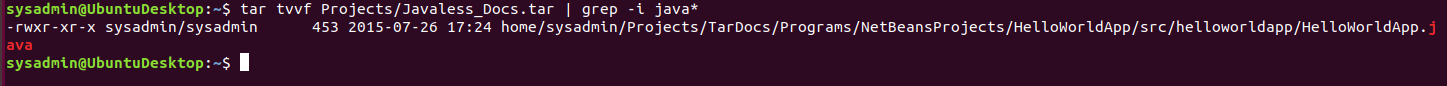
$ **sudo tar cvvWf Projects/Javaless\_Docs.tar --exclude=”Projects/TarDocs/Documents/Java” ~/Projects/TarDocs/**

$ tar tvvf Javaless\_Docs.tar | more



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

$ 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:

$ sudo tar zcvf Projects/logs\_backup.sun.tar.gz - -listed-incremental=Projects/logs\_backup.snar –level=0 /var/log



For Incremental:

$ sudo tar zcvf Projects/logs\_backup.mon.tar.gz - -listed-incremental=Projects/logs\_backup.mon.snar /var/log



**Critical Analysis Question**

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

-x : Extracts the archive

-c : Create archive

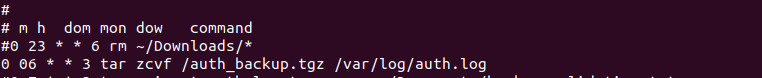
**Step 2: Create, Manage, and Automate Cron Jobs**

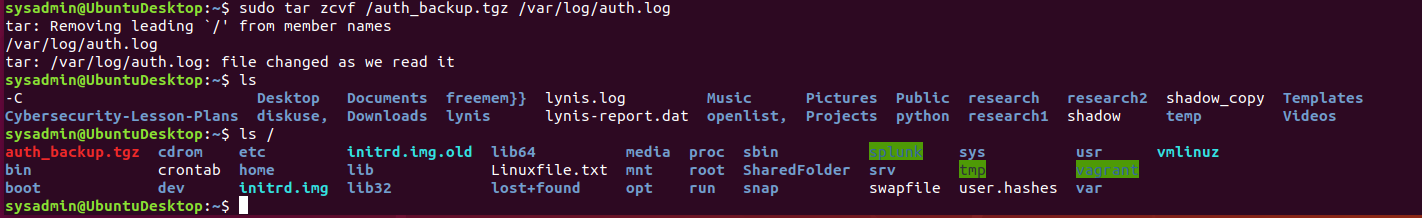
1. Cron job for backing up the /var/log/auth.log file:

Verify in linux command first and make the corntab job.

**$ sudo tar zcvf /auth\_backup.tgz /var/log/auth.log**

**$crontab -e**

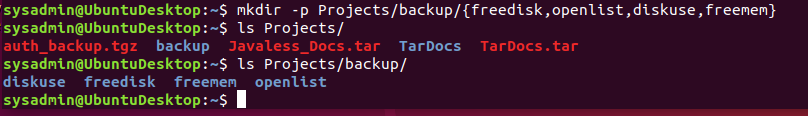




**Step 3: Write Basic Bash Scriptsauth\_backup.tgp**

1. Brace expansion command to create the four subdirectories:

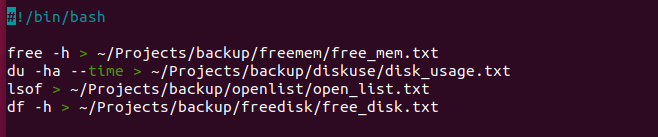
$ mkdir -p Projects/backup/{freedisk,openlist,diskuse,freemem}



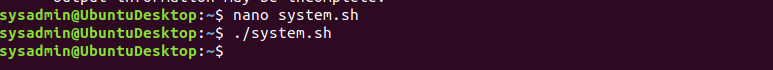
1. Paste your system.sh script edits below:

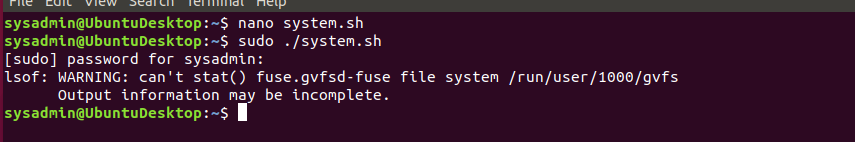
#!/bin/bash

[Your solution script contents here]



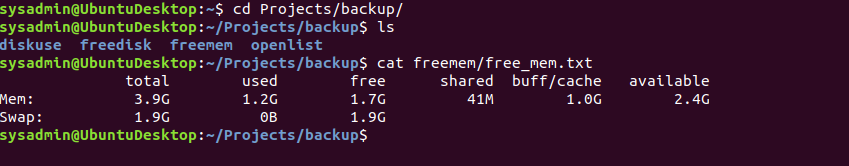
1. Command to make the system.sh script executable:





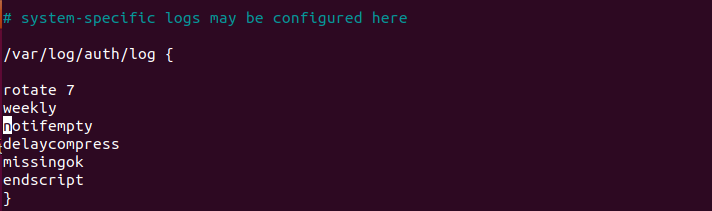
**Optional**

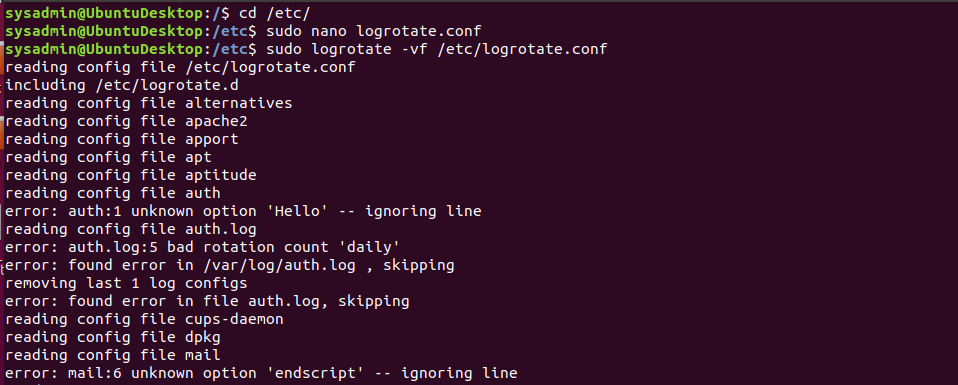
* Commands to test the script and confirm its execution:



**Step 4. Manage Log File Sizes**

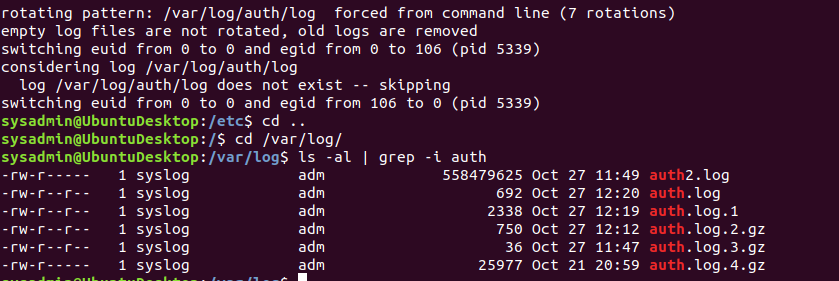
1. Run sudo nano /etc/logrotate.conf to edit the logrotate configuration file.

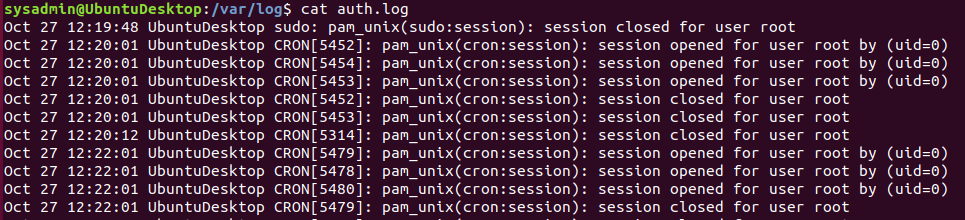




Configure a log rotation scheme that backs up authentication messages to the /var/log/auth.log.

* + Add your config file edits below:



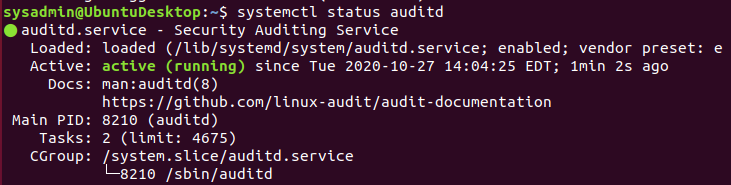


[Your logrotate scheme edits here]

**Bonus: Check for Policy and File Violations**

1. Command to verify auditd is active:

$ systemctl status auditd



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

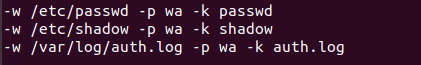


[Your solution edits here]

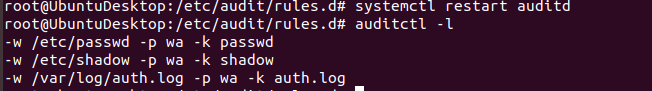
1. Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log:
   * Add the edits made to the rules file below:

# cd /etc/audit/rules.d/

#nano audit.rules



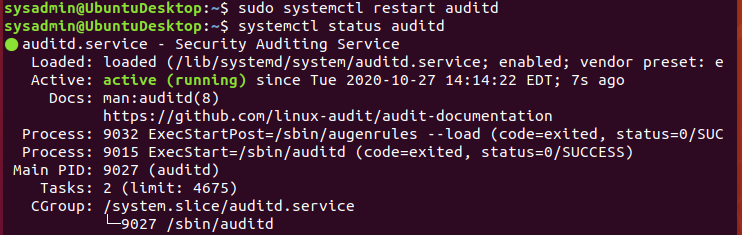
#systemctl restart auditd



[Your solution edits here]

1. Command to restart auditd:

$ sudo systemctl restart auditd



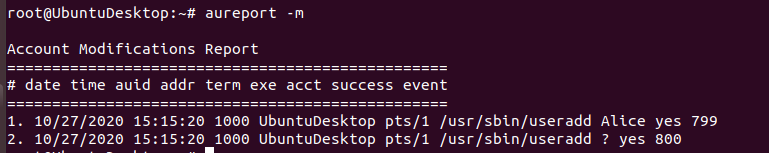
1. Command to list all auditd rules:

#auditctl -l

1. Command to produce an audit report:

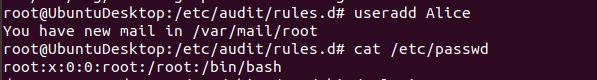
#aureport

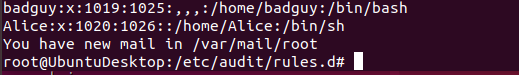
#aureport -m



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

root@ubuntDesktop: /etc/audit/rules.d# useradd Alice





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

#auditctl -w /var/log/cron

#auditctl -l

1. Command to verify auditd rules:

#auditctl -l

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

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

$ journalctl -p 0

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

$ journalctl –disk-usage



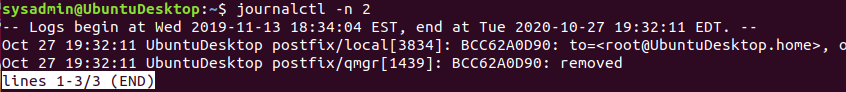
$ journalctl -ef

$journalctl -b

$ journalctl –list-boots

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

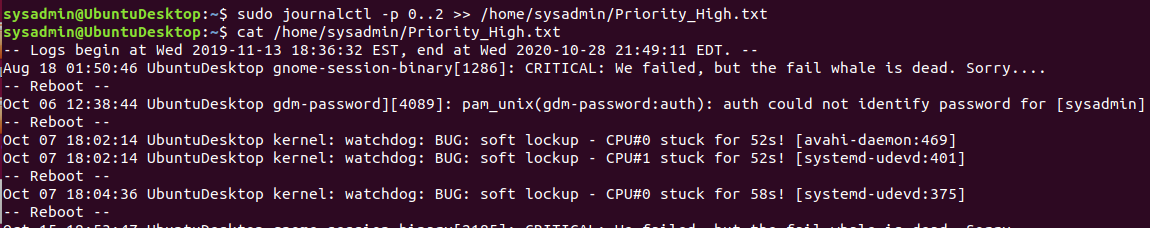
$ journalctl -n 2



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

Commands for: journalctl -p o (Emergency) , journalctl -p 1 (Alert), journalctl -p 2 (Critical)

$ sudo journalctl -p 0..2 >> /home/sysadmin/Priority\_High.txt



Thank you so much for your time,

Dhawal Pandya