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:

```
sysadmin@UbuntuDesktop:~/Projects$ tar xvf TarDocs.tar
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
TarDocs/Financials/investments3.txt
TarDocs/Financials/investments2.txt
TarDocs/Documents/
TarDocs/Documents/Music-Sheets/
TarDocs/Documents/Music-Sheets/Stairway-to-heaven-piano-guitar-A-minor.pdf
TarDocs/Documents/Music-Sheets/Stairway-to-heaven-guitar.pdf
TarDocs/Documents/Music-Sheets/Stairway-to-heaven-bass-tab.pdf
TarDocs/Documents/Music-Sheets/Thumbs.db
TarDocs/Documents/Java/
```

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

- **tar -cvvWf Javaless_Docs.tar . --exclude="/TarDocs/Documents/Java" > ~/Projects/Javaless_Docs.txt**

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

- **tar -tvf Javaless_Docs.tar | grep 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 -cvzf logs_backup.tar.gz --listed-incremental=logs_backup.snar --level=0 /var/log**

```
-rw-r--r--  1 root     root     87917602 Dec 29 16:46 logs_backup.tar.gz
-rw-r--r--  1 root     root         3717 Dec 29 16:46 logs_backup.snar
-rw-r-----  1 syslog   adm        909282 Dec 29 16:46 auth.log
sysadmin@UbuntuDesktop:/var/log$ sudo tar -cvzf logs_backup.tar.gz  --listed-incremental=logs_backup.snar --level=0 /var/lo
```

Critical Analysis Question

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

- **-x : extracts the tar archive**
- **-c : creates the tar archive**

The two options conflict with one another

Step 2: Create, Manage, and Automate Cron Jobs

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

- **sudo tar -cvzf /home/sysadmin/authlogs_backup.tgz /home/sysadmin/authlogs_backup.tar >> /home/sysadmin/compressauth.txt**

```
-rw-r--r-- 1 root     root       46819 Dec 29 17:29 authlogs_backup.tgz
sysadmin@UbuntuDesktop:~$ sudo tar -cvzf /home/sysadmin/authlogs_backup.tgz /home/sysadmin/authlogs_backup.tar >> /home/sysadmin/compressaut
h.txt
```

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

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

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

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

```bash
#!/bin/bash
[Your solution script contents here]
```

```
# 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
du -h > ~/backups/diskuse/disk_usage.txt

# List open files to a open_list.txt file
lsof -L | wc -l > ~/backups/openlist/open_list.txt

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

# CPU Usuage to a cpu_usage.txt file
top -c > ~/backups/cpuuse/cpu_usage.txt
sysadmin@UbuntuDesktop:~$
```

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

```
sysadmin@UbuntuDesktop:~$ chmod +x system.sh
```

Optional
- Commands to test the script and confirm its execution:
 cat the log files produced from the script
cat <filename> | head|less|more|

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

sudo cp system.sh /etc/cron/cron.daily/

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:

```
sysadmin@UbuntuDesktop: /etc/logrotate.d
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    /etc/logrotate.conf                    Modified

# see "man logrotate" for details
# rotate log files weekly
weekly

# use the syslog group by default, since this is the owning group
# of /var/log/syslog.
su root syslog

# keep 4 weeks worth of backlogs
rotate 1

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
compress

# will not rotate if empty
notifempty

# if logs are missing, ignore error message and move on to the next log
missingok

# packages drop log rotation information into this directory
include /etc/logrotate.d
```

```bash
[Your logrotate scheme edits here]
```

```
sysadmin@UbuntuDesktop:/etc/logrotate.d$ sudo cat auth
/var/log/auth.log {
        Rotate 7
        weekly
        notifempty
        compress
        delaycompress
        missingok
        endscript
}
sysadmin@UbuntuDesktop:/etc/logrotate.d$
```

Bonus: Check for Policy and File Violations

1. Command to verify `auditd` is active:

```
sysadmin@UbuntuDesktop:/etc/logrotate.d$ sudo systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-12-26 14:38:36 EST; 1 day 4h ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
  Process: 361 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
  Process: 350 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
 Main PID: 355 (auditd)
    Tasks: 2 (limit: 4666)
   CGroup: /system.slice/auditd.service
           └─355 /sbin/auditd

Dec 26 14:38:36 UbuntuDesktop augenrules[361]: backlog_wait_time 15000
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: enabled 1
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: failure 1
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: pid 355
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: rate_limit 0
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: backlog_limit 8192
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: lost 0
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: backlog 0
Dec 26 14:38:36 UbuntuDesktop augenrules[361]: backlog_wait_time 0
Dec 26 14:38:36 UbuntuDesktop systemd[1]: Started Security Auditing Service.
```

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

- Add the edits made to the configuration file below:

```
sysadmin@UbuntuDesktop:/etc$ 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
##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
sysadmin@UbuntuDesktop:/etc$
```

```bash
[Your solution edits here]
```

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:

```bash
[Your solution edits here]
```

```
sysadmin@UbuntuDesktop:/etc$ 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

-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@UbuntuDesktop:/etc$
```

4. Command to restart `auditd`:

```
sudo systemctl restart auditd
```

5. Command to list all `auditd` rules:

```
sysadmin@UbuntuDesktop:/var/log$ sudo !!
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 rwa -k cron_audit
sysadmin@UbuntuDesktop:/var/log$
```

6. Command to produce an audit report:

```
sysadmin@UbuntuDesktop:/var/log$ sudo aureport -au

Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 12/17/2020 21:02:00 sysadmin ? ? /usr/lib/policykit-1/polkit-agent-helper-1 yes 173
2. 12/17/2020 21:18:47 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 371
3. 12/17/2020 21:18:52 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 373
4. 12/17/2020 21:21:49 sysadmin ? /dev/pts/1 /usr/bin/sudo no 561
5. 12/17/2020 21:21:58 sysadmin ? /dev/pts/1 /usr/bin/sudo no 562
6. 12/17/2020 21:22:03 sysadmin ? /dev/pts/1 /usr/bin/sudo no 583
7. 12/17/2020 21:22:42 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 686
8. 12/17/2020 21:23:01 root ? /dev/pts/1 /bin/su yes 710
9. 12/17/2020 21:23:13 sysadmin ? /dev/pts/1 /bin/su yes 833
10. 12/17/2020 21:23:33 root ? /dev/pts/1 /bin/su yes 893
11. 12/17/2020 21:24:03 root UbuntuDesktop pts/1 /usr/bin/chfn yes 990
12. 12/17/2020 21:33:49 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1237
13. 12/22/2020 13:00:43 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 8119
14. 12/22/2020 14:07:13 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 8758
15. 12/22/2020 14:07:18 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 8759
16. 12/22/2020 14:08:24 sysadmin ? /dev/pts/1 /bin/su yes 8781
17. 12/22/2020 14:32:12 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 9007
18. 12/22/2020 15:19:28 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 9447
19. 12/22/2020 16:00:39 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 9830
20. 12/22/2020 16:00:49 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 9831
21. 12/22/2020 18:08:01 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 11044
22. 12/22/2020 18:54:57 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 11469
23. 12/22/2020 18:56:01 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 11471
24. 12/22/2020 18:56:06 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 11489
25. 12/22/2020 18:59:03 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 11512
26. 12/22/2020 18:59:03 root ? /dev/pts/1 /bin/su yes 11517
27. 12/22/2020 18:59:21 sysadmin ? /dev/pts/1 /bin/su yes 11522
28. 12/22/2020 20:04:17 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 12152
29. 12/22/2020 20:10:37 root ? /dev/pts/1 /bin/su no 12209
30. 12/22/2020 20:11:00 root ? /dev/pts/1 /bin/su no 12211
31. 12/22/2020 20:11:11 root ? /dev/pts/1 /bin/su no 12213
32. 12/22/2020 20:11:23 sysadmin ? /dev/pts/1 /usr/bin/sudo yes 12215
33. 12/22/2020 20:11:23 root ? /dev/pts/1 /bin/su yes 12220
34. 12/22/2020 20:11:43 sysadmin ? /dev/pts/1 /bin/su yes 12228
35. 12/22/2020 20:57:33 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 12652
36. 12/22/2020 20:57:38 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 12654
37. 12/22/2020 20:57:44 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 12656
```

```
63. 12/26/2020 23:29:04 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 5772
64. 12/26/2020 23:30:45 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 5793
65. 12/27/2020 00:14:04 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 6230
66. 12/27/2020 00:28:46 sysadmin ? /dev/pts/0 /usr/bin/sudo no 6367
67. 12/27/2020 00:28:53 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 6368
68. 12/27/2020 00:29:04 root ? /dev/pts/0 /bin/su yes 6374
69. 12/27/2020 15:38:34 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 14911
70. 12/27/2020 15:45:36 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 14968
71. 12/27/2020 15:45:44 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 14970
72. 12/27/2020 15:45:49 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 14972
73. 12/27/2020 15:55:07 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 15065
74. 12/27/2020 15:57:35 sysadmin ? /dev/pts/0 /bin/su yes 15087
75. 12/27/2020 15:57:50 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 15091
76. 12/27/2020 15:58:31 sysadmin ? /dev/pts/0 /bin/su no 15114
77. 12/27/2020 15:58:43 sysadmin ? /dev/pts/0 /bin/su yes 15116
78. 12/27/2020 16:38:16 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 15510
79. 12/27/2020 16:38:19 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 15512
80. 12/27/2020 19:08:14 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 16919
81. 12/27/2020 19:08:23 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 16921
82. 12/27/2020 19:09:20 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 16924
83. 12/27/2020 19:37:22 root ? /dev/pts/0 /bin/su yes 17244
84. 12/27/2020 20:09:12 attacker ? /dev/pts/0 /bin/su no 17981
85. 12/27/2020 20:09:23 attacker ? /dev/pts/0 /bin/su no 17988
86. 12/27/2020 20:09:29 attacker ? /dev/pts/0 /bin/su no 17995
87. 12/27/2020 20:20:50 root ? /dev/pts/0 /bin/su no 21114
88. 12/27/2020 20:20:57 root ? /dev/pts/0 /bin/su no 21121
```

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

```
sysadmin@UbuntuDesktop:/etc$ sudo useradd attacker
sysadmin@UbuntuDesktop:/etc$ sudo attacker
sudo: attacker: command not found
sysadmin@UbuntuDesktop:/etc$ su attacker
Password:
su: Authentication failure
sysadmin@UbuntuDesktop:/etc$ su attacker
Password:
su: Authentication failure
sysadmin@UbuntuDesktop:/etc$ su attacker
Password:

su: Authentication failure
```

```
sysadmin@UbuntuDesktop:/var/log$ sudo aureport -m

Account Modifications Report
===============================================
# date time auid addr term exe acct success event
===============================================
1. 12/17/2020 21:23:51 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 947
2. 12/17/2020 21:23:51 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 949
3. 12/17/2020 21:23:51 1000 UbuntuDesktop pts/1 /usr/sbin/groupadd ? yes 950
4. 12/17/2020 21:23:51 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 957
5. 12/17/2020 21:24:03 1000 UbuntuDesktop pts/1 /usr/bin/passwd criminal yes 987
6. 12/26/2020 14:38:45 -1 ? ? /usr/sbin/useradd vboxadd no 222
7. 12/26/2020 14:38:45 -1 ? ? /usr/sbin/useradd vboxadd no 223
8. 12/26/2020 14:38:45 -1 ? ? /usr/sbin/useradd vboxadd no 224
9. 12/26/2020 14:38:45 -1 ? ? /usr/sbin/useradd vboxadd no 225
10. 12/27/2020 20:08:16 1000 UbuntuDesktop pts/0 /usr/sbin/useradd attacker yes 17949
11. 12/27/2020 20:08:16 1000 UbuntuDesktop pts/0 /usr/sbin/useradd ? yes 17953
sysadmin@UbuntuDesktop:/var/log$
```

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

```
sysadmin@UbuntuDesktop:/etc$ 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:/etc$
```

9. Command to verify `auditd` rules:

```
You must be root to run this program.
sysadmin@UbuntuDesktop:/etc$ 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:/etc$
```

Bonus (Research Activity): Perform Various Log Filtering Techniques

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

```
sysadmin@UbuntuDesktop:~$ cat journalctlauto.sh
#!/bin/bash

# utilizing journalctl log filtering to assess if a breach has occurred

# log search that returns all messages since last boot, with priorities from emergency to error
sudo journalctl -r -p err -b >> /home/sysadmin/allmessages.txt

# Disk usage output since last reboot
sudo journalctl --disk-usage >> /home/sysadmin/diskusage.txt

# removes all archived journal reports except for last since the last reboot
sudo journalctl --vacuum-time=2d >> /home/sysadmin/archiveremoval.txt
sudo journalctl -S -2d -U today -n 15 >> /home/sysadmin/retain2days.txt

# filters all log message with priority levels between zero and two
sudo journalctl -p 0..2 -n 15  >> /home/sysadmin/Priority_High.txt
```

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

SEE Screenshot above

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

SEE Screenshot above

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

SEE Screenshot above

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

```bash
[Your solution cron edits here]
```

```
# Need to Verify if this is correct
0 6 7 * 3 tar cf /aut_backup.tgz /var/log/auth.log

# Need to Verify if this is correct
15 6 7 * 3 gzip -t /aut_backup.tgz >> /compressauth.txt


# move below cron to /etc/cron/cron.daily/ - need to create separate script
0 5 * * * ~/home/sysadmin/journalctlauto.sh >> journalctlauto.txt


sysadmin@UbuntuDesktop:~$
```

```
root@UbuntuDesktop:/etc/cron.daily# ls journal*
journalctlPriority.sh
root@UbuntuDesktop:/etc/cron.daily# cat journa*
#!/bin/bash

# utilizing journalctl log filtering to assess if a breach has occurred
#Bonus Daily.Cron

# filters all log message with priority levels between zero and two
sudo journalctl -p 0..2 -n 15  >> ~/home/sysadmin/Priority_High.txt
root@UbuntuDesktop:/etc/cron.daily#
```

```
-rwxr-xr-x 1 root root  239 Jan  5 16:35 journalctlPriority.sh
root@UbuntuDesktop:/etc/cron.daily# pwd
/etc/cron.daily
root@UbuntuDesktop:/etc/cron.daily#
```