Week 5 Homework Submission File: Archiving and Logging Data

Please edit this file by adding the solution commands on the line below the pr
ompt.

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 xvvf TarDocs.tar

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

```
sysadmin@UbuntuDesktop:~/Projects$ ls -al TarDocs/Documents/
total 1520
drwxr-xr-x 6 sysadmin sysadmin    4096 Jan 13  2019 .
drwxr-xr-x 7 sysadmin sysadmin    4096 Nov 18  2019 ..
-rwxr-xr-x 1 sysadmin sysadmin 1365983 Aug 10  2012 c++interviewquestions.pdf
drwxr-xr-x 2 sysadmin sysadmin    4096 Jan 12  2019 Design-Patterns
drwxr-xr-x 2 sysadmin sysadmin    4096 Jan 12  2019 Google-Maps-Hacks
-rwxr-xr-x 1 sysadmin sysadmin  161823 Oct  3  2015
IntelliJIDEA_ReferenceCard.pdf
drwxr-xr-x 5 sysadmin sysadmin    4096 Jan 13  2019 Java
drwxr-xr-x 2 sysadmin sysadmin    4096 Jan 12  2019 Music-Sheets

sysadmin@UbuntuDesktop:~/Projects$ tar --
exclude='/home/sysadmin/Projects/TarDocs/Documents/Java' -cvvf
Javaless_Docs.tar ~/Projects/TarDocs
```

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

```
sysadmin@UbuntuDesktop:~/Projects$ tar tvvf Javaless_Docs.tar | grep Java
**Bonus**
- Command to create an incremental archive called `logs_backup_tar.gz` with on
ly changed files to `snapshot.file` for the `/var/log` directory:

sysadmin@UbuntuDesktop:~/Projects$ sudo tar -czvvf logs_backup.tar.gz --
listed-incremental=logs_backup.snar --level=0 /var/log/
```

Critical Analysis Question

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

-c option is to create an archive and -x is to extract from archive Therefore these two functions cannot be execute at the same time
---

Step 2: Create, Manage, and Automate Cron Jobs

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

```
# m h  dom mon dow   command
0 6 * * 3 sudo 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:~$ mkdir { ~/backups/freemem ~/backups/diskuse
~/backups/openlist ~/backups/freedisk }
```
2. Paste your `system.sh` script edits below:

    ```bash
    #!/bin/bash


# free memory  output to backups/freemem
free -m >> ~/backups/freemem/free_mem.txt

# diskusage output to backups/freedisk
df -h >> ~/backups/diskuse/disk_usage.txt

# list of open files
lsof >> ~/backups/openlist/open_list.txt

# disk space stat
stat -f / >>  ~/backups/freedisk/free_disk.txt


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

```
sysadmin@UbuntuDesktop:~$ chmod u+x system.sh
Optional
- Commands to test the script and confirm its execution:
sysadmin@UbuntuDesktop:~$ ./system.sh

Bonus
- Command to copy `system` to system-wide cron directory:
cron
sysadmin@UbuntuDesktop:~$ sudo cp system.sh /etc/cron.weekly/
```
```

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:

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

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

Bonus: Check for Policy and File Violations

   1. Command to verify `auditd` is active:

```
sysadmin@UbuntuDesktop:~$ systemctl status auditd
```
2. Command to set number of retained logs and maximum log file size:
```
sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/auditd.conf
```
    - Add the edits made to the configuration file below:

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

```
#
# 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
```

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]
    ```

```
-w /etc/passwd -p wra -k hashpass_audit
-w /etc/shadow -p wra -k userpass_audit
-w /var/log/auth.log -p wra -k authlog_audit
```

4. Command to restart `auditd`:
sysadmin@UbuntuDesktop:~$ systemctl restart auditd

5. Command to list all `auditd` rules:
sysadmin@UbuntuDesktop:~$ sudo auditctl -l
-w /etc/passwd -p rwa -k hashpass_audit
-w /etc/shadow -p rwa -k userpass_audit
-w /var/log/auth.log -p rwa -k authlog_audit

6. Command to produce an audit report:
sysadmin@UbuntuDesktop:~$ sudo aureport

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

8. Command to use `auditd` to watch `/var/log/cron`:
sysadmin@UbuntuDesktop:~$ sudo auditctl -w /var/log/cron

9. Command to verify `auditd` rules:
sysadmin@UbuntuDesktop:~$ sudo auditctl -l
-w /etc/passwd -p rwa -k hashpass_audit
-w /etc/shadow -p rwa -k userpass_audit
-w /var/log/auth.log -p rwa -k authlog_audit
-w /var/log/cron -p rwxa

Bonus (Research Activity): Perform Various Log Filtering Techniques

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

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

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

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

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]
    ```
