Test Paper – 2 (TR – 1,2)

Permissions, Manage Packages, Processes, Service & Daemon

Note:- Each Question carry 5 Marks. **Total Marks - 75**

1. What is suid,sgid & sticky bit permissions. Explain in brief .

Soln>

These are the special permissions which are used with the normal permissions like read, write and execute

These permission are used to set special permissions to the files or directories.

suid – this is used to set the permission of file for other users because the problem is that the other user which has no execute permission can also delete the file so to overcome this we use the suid it's numerical representation is 4 and is append with other permissions using + operator and can also used with other permissions.

Eg. When a user sets the the permission of file he uses the representation of the normal permission which is like

777 so to user suid we add new bit at first of numeric permissions eg. X777

Here x is the suid permission

Here s represents execute permission with other permission

And S – represents no execute permission with other permission

```
[root@localhost ~]# pwd
/root
[root@localhost ~]# mkdir special_per
[root@localhost ~]# touch /root/special_per/suid
[root@localhost ~]# ls -l /root/special_per/
total 0
-rw-r--r--. 1 root root 0 Feb  1 10:11 suid
[root@localhost ~]# chmod 4777 /root/special_per/
[root@localhost ~]# ls -l /root/special_per/
total 0
-rw-r--r--. 1 root root 0 Feb  1 10:11 suid
[root@localhost ~]# chmod 4777 /root/special_per/suid
[root@localhost ~]# ls -l /root/special_per/
total 0
-rwsrwxrwx. 1 root root 0 Feb  1 10:11 suid
```

sgid – It is the special group command which is used the access of a group over a file the group users can also deletes the files so to stop that ie only the owner of the file can delete it we use the guid

Its numerical value is 2

And we can also append this with + operator.

Eg if a user want to append the permission to other permissions

By numerical way he can use 2xxx where x is other permissions

Or they can use g+s

```
[root@localhost ~]# chmod 2777 /root/special_per/guid
[root@localhost ~]# ls -l /root/special_per/
total 0
-rwxrwsrwx. 1 root root 0 Feb  1 10:18 guid
-rwsrwxrwx. 1 root root 0 Feb  1 10:11 suid
```

Sticky bit- It is used on directory so that any user other than owner cannot delete the directory content

Its numerical value is 1

Eg. to add this permission use 1xxx where x is other permissions or append +t

```
[root@localhost ~]# touch /root/special_per/sticky
[root@localhost ~]# ls -l /root/special_per/
total 0
-rwxrwsrwx. 1 root root 0 Feb  1 10:18 guid
-rw-r--r--. 1 root root 0 Feb  1 10:24 sticky
-rwsrwxrwx. 1 root root 0 Feb  1 10:11 suid
[root@localhost ~]# chmod 1777 /root/special_per/sticky
[root@localhost ~]# ls -l /root/special_per/
total 0
-rwxrwsrwx. 1 root root 0 Feb  1 10:18 guid
-rwxrwxrwt. 1 root root 0 Feb  1 10:24 sticky
-rwsrwxrwx. 1 root root 0 Feb  1 10:11 suid
```

2. (A) The permission -rwSr--r-- represented in octal expression will be?

(B) What is the difference between **t** and **T** when applying thesticky bit Permission?

Soln>

a> 4644

b> t – means the users other than owner cannot modify the directory and has execute permission on directory

```
[root@localhost ~]# ls -l /root/special_per/
total 0
-rwxrwsrwx. 1 root root 0 Feb  1 10:18 guid
-rwxrwxrwt. 1 root root 0 Feb  1 10:24 sticky
-rwsrwxrwx. 1 root root 0 Feb  1 10:11 suid
```

and T – means there is no execute permission on the directory.

```
[root@localhost ~]# ls -l /root/special_per/
total 0
-rwxrwsrwx. 1 root root 0 Feb  1 10:18 guid
-rw-rwxrwT. 1 root root 0 Feb  1 10:24 sticky
-rwsrwxrwx. 1 root root 0 Feb  1 10:11 suid
```

3. Create a collaborative directory **"/common/admin"** with the following characteristics:

(A) Group ownership of **/common/admin** is sysadmin.

(B) The directory should be readable, writable, and accessible to members of sysadmin, but not to any other user.

(C) Files created in **/common/admin** automatically have group ownership set to the sysadmin group.

Soln>

```
[root@localhost ~]# mkdir -p /common/admin
[root@localhost ~]# chown :sysadmin /common/admin
[root@localhost ~]# chmod 2770 /common/admin
[root@localhost ~]# ls -l /common/admin
total 0
[root@localhost ~]# ls -l /common/
total 0
drwxrws---. 2 root sysadmin 6 Feb  1 10:43 admin
```

4. A user is unable to rename a file in their home directory despite having full permissions on the file. What might be the reason for this issue?

Soln>

The permission of directory is read only.

5. Difference between default ACL and recursive ACL. Write the command to set it.

Soln>

ACL – it is used to see or set the access control list of a single file

Recursice ACL – it is used to set/see the recursive or the all files or derectories exists in the given directory

Eg

getfacl

```
[root@localhost /]# getfacl common
# file: common
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```

getfacl -R used for recursive call

```
[root@localhost /]# getfacl -R common/
# file: common/
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

# file: common//admin
# owner: root
# group: sysadmin
# flags: -s-
user::rwx
group::rwx
other::---
```

6. You are required to configure the **AlmaLinux 9** repository on your system using the following repository URLs:

- **AppStream:** https://repo.almalinux.org/almalinux/9/AppStream/x86_64/os
- **BaseOS:** https://repo.almalinux.org/almalinux/9/BaseOS/x86_64/os

Before configuring the new repositories, ensure that **all existing repositories are removed** from the system.

Tasks:

1. **Remove all existing repositories** from the system.
2. **Create new repository configuration files** for AlmaLinux 9 AppStream and BaseOS.
3. **Verify that the new repositories are properly configured and working.**

Soln>

1. To remove all existing repos we use: rm -f /etc/yum.repos.d/*.repo
   Here rm – remove cmd
   -f – forcefully remove all the content of a given dir
   yum.repos.d – path of dir where repos present
   * - used to select all the files of similar format

7. What are jobs. (Processes)

Soln>

Processes are the intermediators which used between a command and a file.

Processes are created when a command is run then according to the cmd the process contains the info of cmd and related files so it validates all the permission of directories and files then allow the file for certain operation and return a required output or error.

A process is a work which help the system security and privacy.

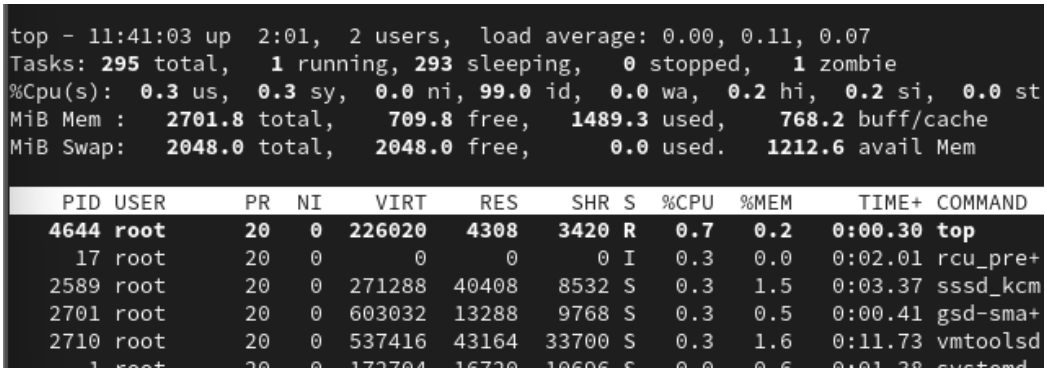
8. (A) What is the diffrence b/w ps -aux and top.

(B) How to filter out processes by memroy utilization.

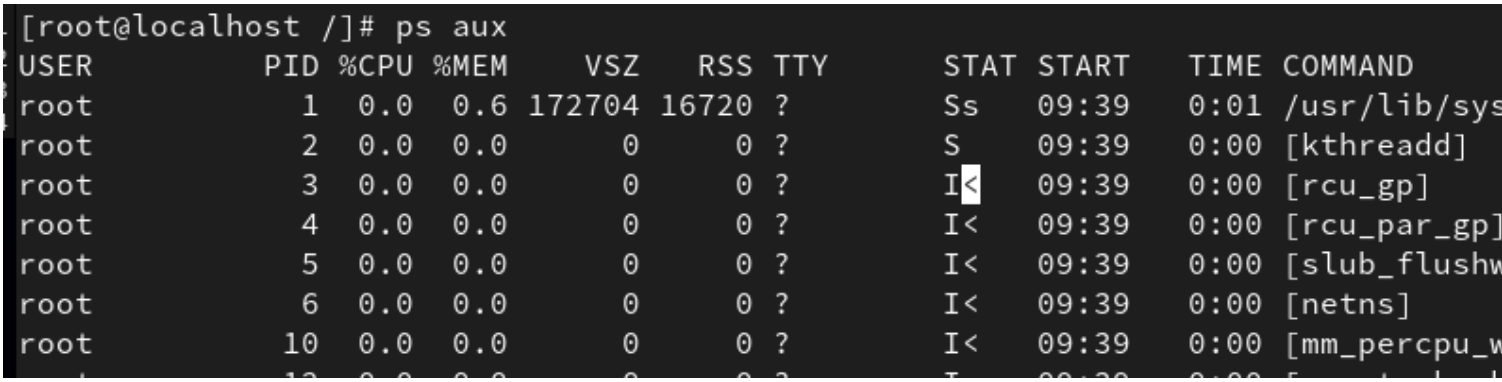
Soln>

Top – it gives all running processes with information and also it updates in every 3 second and displays new running precesses

The top program provides a dynamic real-time view of a running system.



ps -aux - it only shows the process completed till now after terminal starts



9. (A) What is the default signal to terminate a process.

Soln> ctrl+z

(B) What is the signal to forcefully terminate a process.

10. (A) Write shortcut keys to interrupt a process.

    (B) How to display that how many users are logged into system.

Soln>

a. Ctrl + c is used to interrupt a process
b. Using command: "**w**" we can display all user info. That who is loged in to which termina etc.

```
[root@localhost /]# w
 11:22:23 up  1:43,  2 users,  load average: 0.08, 0.03, 0.00
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
root     seat0     10:05    0.00s  0.00s  0.00s /usr/libexec/gdm-wayla
root     tty2      10:05    1:43m  0.01s  0.01s /usr/libexec/gnome-ses
```

11. (A) What is zombie process.

    (B) How to kill all process running by a particular user .

    (C) How to kill all process running in a particular terminal .

Soln>

a. A child process tells it parent process that It is going to be terminated so that process is a zombie process
   To see that which and how many zombie processes are running we use command: **top**

```
[root@localhost /]# top

top - 11:24:32 up  1:45,  2 users,  load average: 0.01, 0.02, 0.00
Tasks: 290 total,   1 running, 289 sleeping,   0 stopped,   0 zombie
%Cpu(s):  1.0 us,  1.0 sy,  0.0 ni, 96.9 id,  0.0 wa,  0.0 hi,  1.0 si,  0.
MiB Mem :   2701.8 total,    677.5 free,   1522.5 used,    766.4 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   1179.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMM
   2589 root      20   0  271288  40408   8532 S   2.1   1.5   0:02.79 ssso
   3899 root      20   0  226020   4308   3420 R   2.1   0.2   0:00.04 top
      1 root      20   0  172484  16696  10696 S   0.0   0.6   0:01.18 syst
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthr
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_
```

b. We use kill with the uid of the user to kill all process running of a user
c. We close the terminal to kill that terminal process using init0