Special Permission

Types of Special permissions :

1.Setuid (SUID) - 4
2.Setgid (SGID) - 2
3.Sticky Bit - 1

/usr/sbin/ - contains the executable files of root user

/usr/bin - contains the executable files of normal user

1. Set User ID/SETUID :

Set uid – give the permission to who can use the commands

Numeric values of Set Uid is 4

Example :

Useradd can be done only by root by default.
Special Permission (SUID) changes any user can add user .

```
[root@localhost ~]# ls -li /usr/sbin/useradd
33823508 -rwxrwx---. 1 root root 141128 Jul 21  2022 /usr/sbin/useradd
```

i) We can see no other user can add new user :

```
[root@localhost ~]# su - ipl
[ipl@localhost ~]$ useradd WPL
-bash: /usr/sbin/useradd: Permission denied
```

ii) Now we are giving Suid for useradd command.

```
[root@localhost ~]# chmod 4777 /usr/sbin/useradd
[root@localhost ~]# ls -li /usr/sbin/useradd
33823508 -rwsrwxrwx. 1 root root 141128 Jul 21  2022 /usr/sbin/useradd
```

iii) Now any user can add new user ;

```
[root@localhost ~]# su - ipl
[ipl@localhost ~]$ useradd mani
sss_cache must be run as root
sss_cache must be run as root
```

Same for Userdel :

```
[root@localhost ~]# ls -li /usr/sbin/userdel
33823509 -rwxr-xr-x. 1 root root 90968 Jul 21  2022 /usr/sbin/userdel
[root@localhost ~]# chmod u+s /usr/sbin/userdel
[root@localhost ~]# ls -li /usr/sbin/userdel
33823509 -rwsr-xr-x. 1 root root 90968 Jul 21  2022 /usr/sbin/userdel
```

Result that any user can delete any user

```
[root@localhost home]# su - markets
[markets@localhost ~]$ userdel subha
sss_cache must be run as root
sss_cache must be run as root
```

GUID :

 All files or directories created inside that directory will be owned by the same common group.

 Its numeric value is 2.

```
drwxr-xr-x. 2 root root 6 Jun  6 03:21 example
[root@localhost /]# chgrp tamilnadu example
[root@localhost /]# ls -ld example
drwxr-xr-x. 2 root tamilnadu 6 Jun  6 03:21 example
[root@localhost /]# chmod 2755 example
[root@localhost /]# ls -ld example
drwxr-sr-x. 2 root tamilnadu 6 Jun  6 03:21 example
[root@localhost /]# cd example
[root@localhost example]# mkdir karuna
[root@localhost example]# ls -ld karuna
drwxr-sr-x. 2 root tamilnadu 6 Jun  6 03:23 karuna
[root@localhost example]# cd karuna
[root@localhost karuna]# mkdir praveena
[root@localhost karuna]# ls -ld praveena
drwxr-sr-x. 2 root tamilnadu 6 Jun  6 03:24 praveena
```

STICKY BITS :

The sticky bit permission set, then the file can be deleted only by the REAL owner of the file/directory or the root user.

 Its numeric value is 1.

i) Creating a directory in /

```
[root@localhost /]# mkdir maha
```

ii) Adding a file in a created directory:

```
drwxr-xr-x. 2 root root 6 Jun  6 04:25 maha
[root@localhost /]# cd maha
[root@localhost maha]# touch logitha
```

iii) Giving sticky bits special permission ;

```
[root@localhost /]# chmod 1777 maha
```

iv) Result that only owner can remove the file :

```
[chennai@localhost ~]$ cd /maha
[chennai@localhost maha]$ ls
logitha
[chennai@localhost maha]$ rm -rf logitha
rm: cannot remove 'logitha': Operation not permitted
```