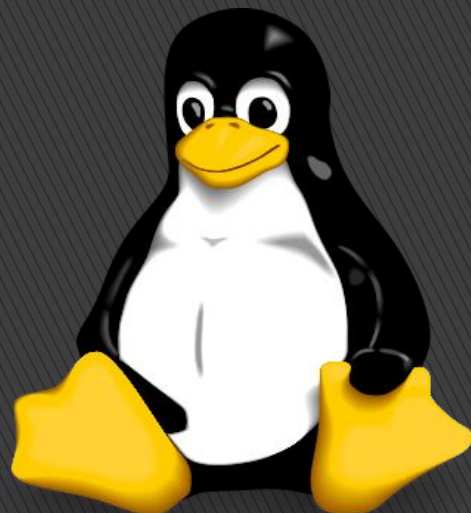
Special Permission

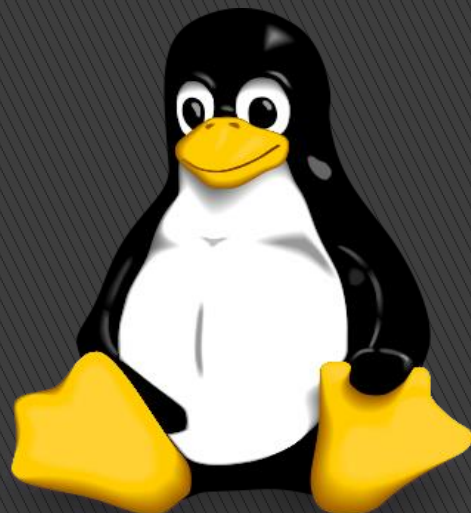
Special Permission

Special permissions are available for executable files and directory.



Three Type of Special Permission

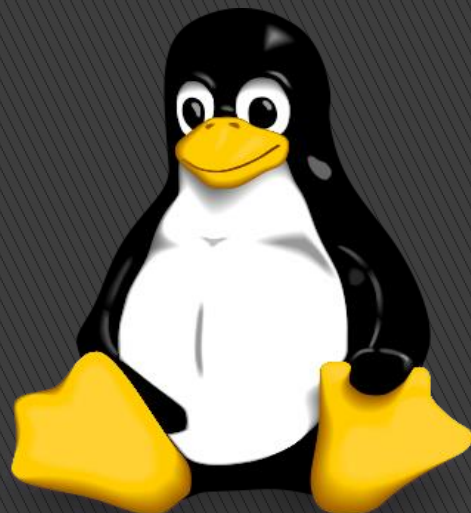
1. SUID
2. SGID
3. Sticky Bit



1. Set User ID (SUID)

The suid/setuid bit is represented by ”**s**” **(4).**

This special permission allows a user to access files and directories that are normally only available to the owner.



SUID

For set suid permission

```
#chmod     u+s          sample.txt
```

Or

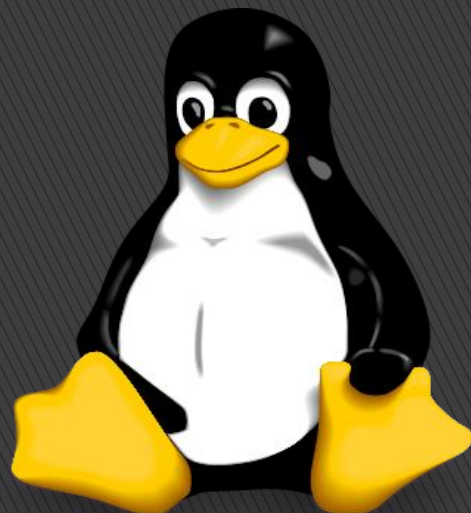
```
#chmod    4644          sample.txt
```

For Check

```
#ls          -l     sample.txt
```

For remove suid permission

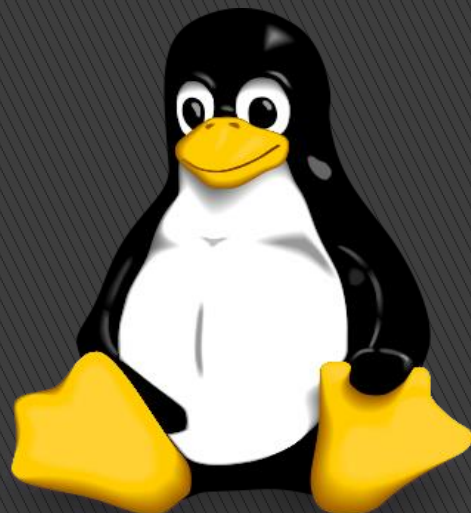
```
#chmod              u-s          sample.txt
```



2. Set Group ID (SGID)

When sgid permission is applied to a directory, all sub directories and files created inside this directory will get the same group ownership as main directory

The octal digit for the sgid is 2.



SGID

For set sgid permission

#chmod g+s /india

Or

#chmod 2755 /india

For Check:

#ls -ld /india

For remove sgid permission

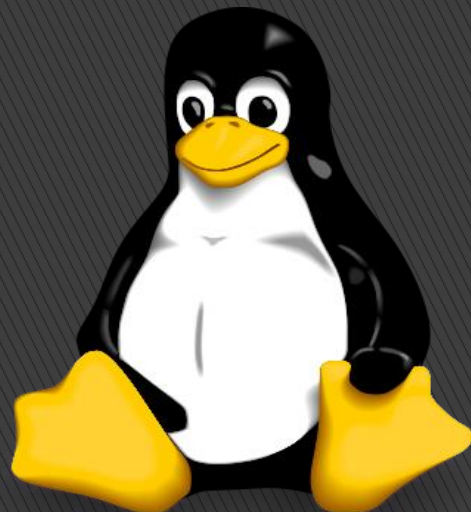
#chmod g-s /india

3. Sticky Bit

The sticky bit is represented by **t and octed digit 1.**

It is mainly used to protect files within a directory.

If a directory has the sticky bit set, a file can be deleted only by the owner of the file, the owner of the directory, or by root. This is useful for publically accessible directories.



Sticky Bit

For set sticky bit permission

```
#chmod          +t              /share
```

Or

```
#chmod          1770            /share
```

For Check :

```
#ls             -ld             /share
```

For remove sticky bit permission

```
#chmod          -t              /share
```