

Permisos Especiales



Permisos especiales

SUID Set-User-ID

- Por default los archivos se ejecutan usando el user id.
- SUID permite correr un programa utilizando user id del dueño del archivo.
- Se define con la letra **s** en modo simbólico y el **4** en modo octal.

```
$ chmod u=rwxs,go=rx archivo
```

```
$ chmod 4755 archivo
```



Permisos especiales

SGID Set-Group-ID

- Funciona de igual manera que SUID, pero con privilegios de grupo.
- Se define utilizando la letra **s** en modo simbólico y **2** en modo octal.

```
$ chmod u=rwx,g=rxs,o=rx archivo
```

```
$ chmod 2755 archivo
```



Sticky bit

- Si un directorio tiene permiso de escritura y el sticky bit está definido, un proceso puede borrar o renombrar archivos si:
 - El usuario efectivo es el mismo que el dueño del archivo.
 - El usuario efectivo es el mismo que el dueño del directorio.
 - El usuario es el superusuario.

Sticky bit

- Si un archivo ordinario tiene definido el sticky bit y es un binario, se carga en memoria incrementando su velocidad de inicio al ser llamado por otro proceso. Este uso en los sistemas operativos modernos no incrementa significativamente la velocidad por lo cual prácticamente es obsoleto, pero se conserva por compatibilidad.

Sticky bit

- Se define con la letra **t** en modo simbólico y con el **1** en modo octal.

```
$ chmod a=rwx,+t /tmp  
$ chmod 1777 /tmp
```