

Permisos para archivos especiales mediante (setuid, setgid y bit de permanencia).

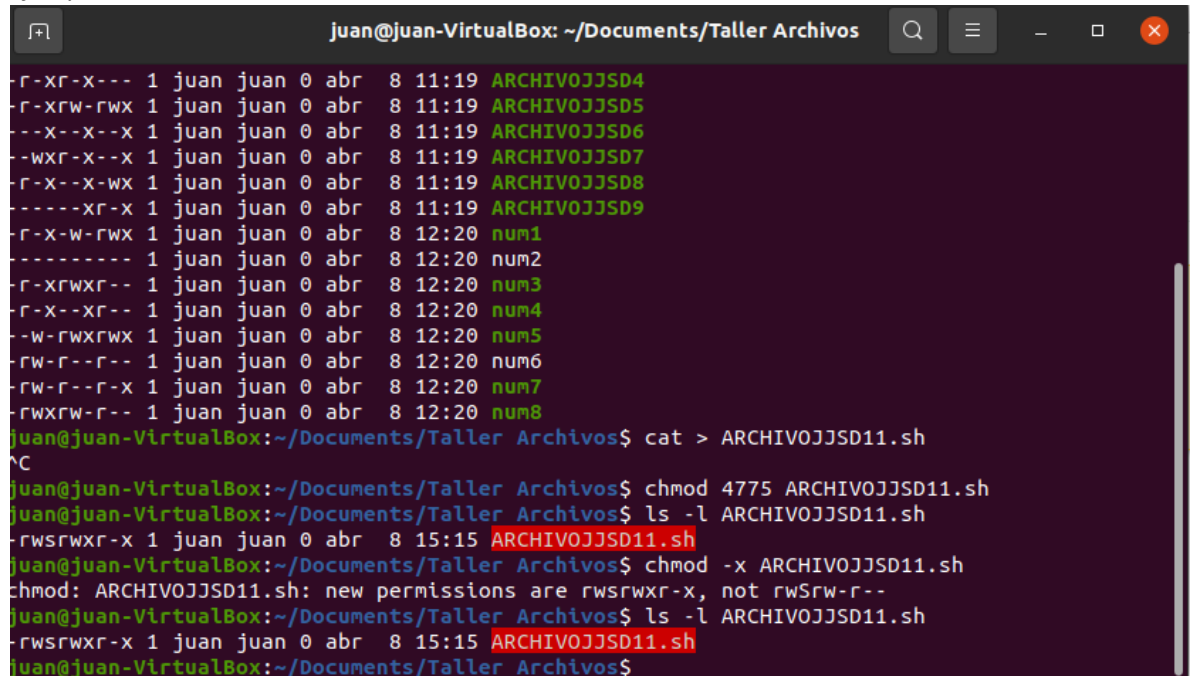
Cuando estos permisos se establecen, cualquier usuario que ejecuta ese archivo ejecutable asume el ID del propietario (o grupo) del archivo ejecutable.

1. **Permiso SETUID:** Cuando el permiso setuid se establece en un archivo ejecutable, se otorga acceso a el proceso que se ejecuta por medio de este archivo según el propietario del archivo. Este permiso especial permite a un usuario acceder a los archivos y directorios que, normalmente, están disponibles solo para el propietario.

Ejemplo en UNIX

```
-r-sr-sr-x 1 root sys 56808 Jun 17 12:02 /usr/bin/passwd
```

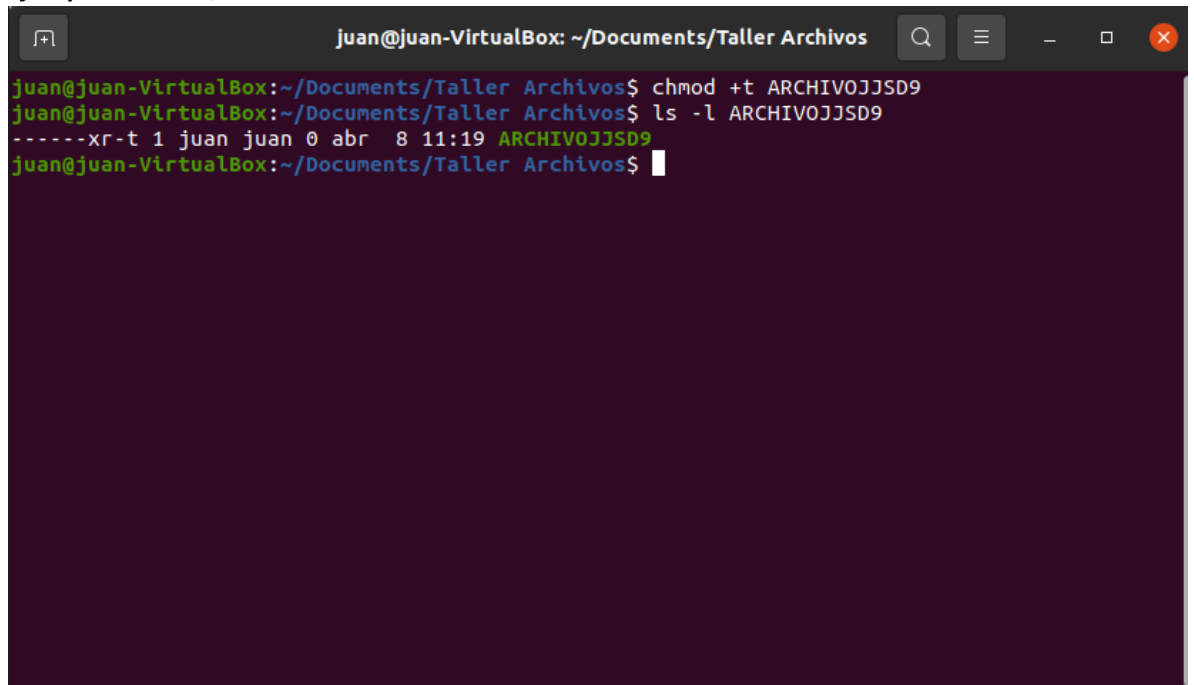
Ejemplo en Linux/Ubuntu



```
juan@juan-VirtualBox: ~/Documents/Taller Archivos
-r-xr-x--- 1 juan juan 0 abr 8 11:19 ARCHIVOJJSD4
-r-xrw-rwx 1 juan juan 0 abr 8 11:19 ARCHIVOJJSD5
---x--x--x 1 juan juan 0 abr 8 11:19 ARCHIVOJJSD6
-rwxr-x--x 1 juan juan 0 abr 8 11:19 ARCHIVOJJSD7
-r-x--x-wx 1 juan juan 0 abr 8 11:19 ARCHIVOJJSD8
-----xr-x 1 juan juan 0 abr 8 11:19 ARCHIVOJJSD9
-r-x-w-rwx 1 juan juan 0 abr 8 12:20 num1
----- 1 juan juan 0 abr 8 12:20 num2
-r-xrwxr-- 1 juan juan 0 abr 8 12:20 num3
-r-x--xr-- 1 juan juan 0 abr 8 12:20 num4
-r-w-rwxrwx 1 juan juan 0 abr 8 12:20 num5
-rw-r--r-- 1 juan juan 0 abr 8 12:20 num6
-rw-r--r-x 1 juan juan 0 abr 8 12:20 num7
-rwxrw-r-- 1 juan juan 0 abr 8 12:20 num8
juan@juan-VirtualBox:~/Documents/Taller Archivos$ cat > ARCHIVOJJSD11.sh
^C
juan@juan-VirtualBox:~/Documents/Taller Archivos$ chmod 4775 ARCHIVOJJSD11.sh
juan@juan-VirtualBox:~/Documents/Taller Archivos$ ls -l ARCHIVOJJSD11.sh
-rwsrwxr-x 1 juan juan 0 abr 8 15:15 ARCHIVOJJSD11.sh
juan@juan-VirtualBox:~/Documents/Taller Archivos$ chmod -x ARCHIVOJJSD11.sh
chmod: ARCHIVOJJSD11.sh: new permissions are rwsrwxr-x, not rwSrW-r--
juan@juan-VirtualBox:~/Documents/Taller Archivos$ ls -l ARCHIVOJJSD11.sh
-rwsrwxr-x 1 juan juan 0 abr 8 15:15 ARCHIVOJJSD11.sh
juan@juan-VirtualBox:~/Documents/Taller Archivos$
```

2. **Permiso SETGID:** este permiso se aplica a un directorio, los archivos que se crearon en ese directorio pertenecen al grupo correspondiente del directorio. Cualquier usuario que tiene permisos de escritura y ejecución en el directorio puede crear un archivo allí. Sin embargo, el archivo pertenece al grupo que posee el directorio, no al grupo al que pertenece el usuario.
3. **Bit de permanencia:** El bit de permanencia consiste en un bit de permiso que protege los archivos dentro de un directorio, de esta forma un archivo solo podrá ser suprimido por el propietario del archivo, el propietario del directorio o un usuario con privilegios

Ejemplo en Linux/Ubuntu



```
juan@juan-VirtualBox: ~/Documents/Taller Archivos
juan@juan-VirtualBox:~/Documents/Taller Archivos$ chmod +t ARCHIVOJJSD9
juan@juan-VirtualBox:~/Documents/Taller Archivos$ ls -l ARCHIVOJJSD9
-----xr-t 1 juan juan 0 abr  8 11:19 ARCHIVOJJSD9
juan@juan-VirtualBox:~/Documents/Taller Archivos$
```

The image shows a terminal window titled "juan@juan-VirtualBox: ~/Documents/Taller Archivos". The user has executed the command `chmod +t ARCHIVOJJSD9` to set the sticky bit on the file `ARCHIVOJJSD9`. The subsequent `ls -l ARCHIVOJJSD9` command shows the file's permissions as `-----xr-t 1`, indicating that the sticky bit is now set. The terminal output is displayed on a dark purple background with green and blue text.