

204 - Permisos avançats

Curs 2020 - 2021

ASIX M01-ISO UF1-A01-03 Permisos avançats: SetUID / SetGID / Stickybit

Permisos	1
Descripció	1
Permisos avançats	1
Funcionament dels permisos avançats	1
Establiment de permisos avançats	4
Exercicis d'exemple	6

Permisos

Descripció

Conceptes clau:

- ☐ SetUID
- ☐ SetGID
- ☐ Stickybit

Ordres a treballar:

- ☐ chmod

Permisos avançats

Funcionament dels permisos avançats

Fins ara hem vist que els permisos el GNU/Linux s'estructuren en tres blocs corresponents a *propietari*, *grup* i *altres*. Per cada grup es poden establir els permisos de *r read*, *w write*, *x execute* i *- cap*.

Anem a presentar nous permisos que es poden establir a fitxers i directoris, que anomenem permisos avançats. Aquests permisos actuen de manera diferent si s'apliquen a fitxers o directoris.

Permisos avançats i la seva funció:

SetUID

- ❑ fitxers: aplicat aquest permís a fitxers executables fa que el fitxer s'executi amb els permisos efectius del propietari del fitxer en lloc dels permisos corresponents a l'usuari que executa l'ordre.
- ❑ directoris: aquest permís no té sentit aplicat a directoris.
- ❑ aquest permís s'aplica al bloc de permisos del propietari i es mostra com una s minúscula. És obligatori per ser funcional que també estigui concedit el permís x (és a dir, calen els dos permisos). Si el permís x no està concedit es mostrarà com una S majúscula indicant que el permís no és vàlid.

```
$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 27872 12 abr 2018 /usr/bin/passwd

$ cp /usr/bin/date ladata
$ chmod 4755 ladata
$ ls -la ladata
-rwsr-xr-x 1 ecanet ecanet 106928 21 des 10:18 ladata

$ chmod 4655 ladata
$ ls -la ladata
-rwsr-xr-x 1 ecanet ecanet 106928 21 des 10:18 ladata
```

- en el primer exemple es visualitza l'ordre passwd del sistema que té el SetUID activat (una s minúscula a la part dels permisos del propietari).
- en el segon exemple es fa una còpia local de l'ordre data i s'anomena ladata i se li assignen els permisos d'execució activant el SetUID (més endavant es veurà com fer-ho). Altre cop podem observar que els permisos d'usuari indiquen que el SetUID està actiu (rws).
- finalment es modifiquen els permisos de l'ordre ladata establint una combinació errònia que aplica la s però no aplica la x. Es pot observar del llistat que el permís SetUID està mal aplicat perquè la s apareix en majúscules (rWS).

SetGID

- ❑ fitxers: aplicat a fitxers executables provoca que l'ordre s'executi amb els permisos efectius del grup del fitxer en lloc dels permisos corresponents a l'usuari que executa l'ordre.
- ❑ directoris: aplicat a un directori provoca que el contingut que es genera nou dins del directori passa a ser automàticament del mateix grup que el directori. Tot el contingut del directori hereta el grup del directori.
- ❑ aquest permís s'aplica al bloc de permisos del grup i es mostra com una s minúscula. És obligatori per ser funcional que també estigui concedit el permís x (és a dir, calen els dos permisos). Si el permís x no està concedit es mostrarà com una S majúscula indicant que el permís no és vàlid.

```

$ ls -l /usr/bin/write
-rwxr-sr-x 1 root tty 19584 27 mar 2018 /usr/bin/write

$ chmod 2755 ladata
$ ls -l ladata
-rwxr-sr-x 1 ecanet ecanet 106928 21 des 10:18 ladata

$ chmod 2745 ladata
$ ls -l ladata
-rwxr-Sr-x 1 ecanet ecanet 106928 21 des 10:18 ladata

```

- primerament es llista l'ordre executable del sistema write i s'observa que és una ordre que té el SetGID activat. Al bloc de permisos del grup es pot observar la s minúscula (r-s) que indica que el permís és actiu.
- es modifica el permís a una ordre propia anomenada ladata i se li assigna permisos d'execució i s'activa el SetGID. Es pot observar del llistat dels permisos que per al grup d'apliquen els permisos r, x i s. Que la s sigui minúscula indica que el permís x també està concedir.
- finalment s'agina a la ordre local ladata uns permisos errònis on s'activa el SetGID però no s'acompanya del permís x. Per això el llistat mostra r-S amb la S majúscula indicat que el permís SetGID no està ben assignat (falta la x).

```

$ mkdir projecte
$ ls -ld projecte/
drwxrwxr-x 2 ecanet ecanet 40 21 des 10:31 projecte/

$ chgrp sintesi projecte/
$ chmod 2770 projecte/
$ ls -ld projecte/
drwxrws--- 2 ecanet sintesi 40 21 des 10:31 projecte/

$ chmod 2760 projecte/
$ ls -ld projecte/
drwxrws--- 2 ecanet sintesi 40 21 des 10:31 projecte/

```

- primerament es crea un directori projecte que es genera amb els permisos per defecte segons la umask de l'usuari.
- s'assigna el directori projecte al grup d'usuaris sintesi.
- es modifiquen els permisos del directori concedint permís total pel propietari i grup i cal pels altres. També 'assigna el SetGID com es pot observar del llistat, que al bloc de permisos del grup mostra rws. També es pot observar que el directori ara pertany al grup sintesi.
- finalment es fa un exemple de mostrar una incorrecta assignació del permís de SetGID. S'aplica el permís s però no el permís x i com es pot observar del listat es mostra rwS on la S majúscula indica que el SetGID no és efectiu.

Sticky Bit

- ❑ fitxers: actualment aquest permís aplicat a fitxers no té sentit pràctic. originàriament marcava el fitxer per quedar resident a memòria.

- ❑ directoris: aplicat a un directori provoca que els usuaris tot i tenir permís w no puguin esborrar el contingut que no sigui seu. Així s'evita que els usuaris puguin esborrar contingut d'altres usuaris.
- ❑ aquest permís s'aplica al bloc de permisos de altres i es mostra com una t minúscula. És obligatori per ser funcional que també estigui concedit el permís x (és a dir, calen els dos permisos) però de fet el més lògic per al seu funcionament és assignar rwx. Si el permís x no està concedit es mostrarà com una T majúscula indicant que el permís no és vàlid.

```
$ ls -ld /tmp/ /var/tmp/
drwxrwxrwt 16 root root 380 21 des 10:38 /tmp/
drwxrwxrwt 15 root root 4096 21 des 10:16 /var/tmp/

$ chmod 1777 projecte/
$ ls -ld projecte/
drwxrwsrwt 2 ecanet sintesi 40 21 des 10:31 projecte/

$ chmod 1776 projecte/
$ ls -ld projecte/
drwxrwsrwt 2 ecanet sintesi 40 21 des 10:31 projecte/
```

- primerament els mostren els directoris temporals del sistema /tmp i /var/tmp que són dos directoris que per defecte tenen l'Sticky Bit activat. Es pot observar que el llistat mostra rwt.
- s'assigna al directori projectes control total per a tothom i s'activa l'Sticky Bit. Es pot observar que al bloc de permisos de altres es mostra rwt amb la t minúscula indicant que el permís és efectiu.
- finalment s'assignen uns permisos incorrectes al directori projecte perquè s'assigna l'Sticky Bit però no el permís x. El llistat mostra els permisos rwT amb la t majúscula indicant que el permís Sticky Bit està mal concedit (falta la x).

****nota**** el els propers documents s'explica com funcionen, per a què serveixen, els permisos avançats. En aquest capítol simplement aprenem a establir-los.

Establiment de permisos avançats

Hi ha dos mecanismes per establir els permisos amb **chmod**, la notació **octal** i la notació **simbòlica**. Usualment s'utilitza la notació octal quan a un element li volem assignar tots els permisos de cop. En canvi s'utilitza la notació simbòlica quan es vol modificar només algun permís respectant l'estat dels altres.

Octal

Per assignar permisos avançats cal un nou octet a l'esquerra del tot (de més pès) que indica amb el seu valor si es concedeix el permís SetUID, SetGID o Sticky Bit.

avançat propietari grup altres

- 4** SetUID
- 2** SetGID
- 1** Sticky Bit

Exemples d'assignació de permisos vàlids:

`chmod 4755 programa`
assigna a programa els permisos `rws r-x r-x`. El **4** inicial assigna el `setuid`, `755` assigna control total per al propietari i lectura i execució per al grup i altres.

`chmod 2755 programa`
assigna a programa els permisos `rwxr-sr-x`. El **2** inicial assigna el permís `setgid`, el `755` assigna control total per al propietari i lectura i execució per al grup i altres.

`chmod 2750 directori`
assigna al directori els permisos `rwxr-s---`. El **2** inicial assigna el permís `setgid`, el `750` assigna control total per al propietari i lectura i execució per al grup i cap permís per a altres.

`chmod 1777 directori`
assigna al directori els permisos `rwrxrwxrwx`. El **1** inicial assigna el permís sticky bit, el `777` assigna control total a tothom.

`chmod 3773 directori`
assigna al directori els permisos `rwxrws-wt`. El **3** inicial activa el `setgid` i l'sticky bit. Els altres permisos serien `rwrxwx-wx` però cal aplicar-los els dos permisos especials i es transforma en `rwxrws-wt`.

`chmod 6755 programa`
assigna a programa els permisos `rwsr-sr-x`. El **6** inicial activa el `setuid` i el `setgid`. La resta de permisos serien `rw-x-r-xr-x` i quan se'ls aplica el **6** inicial queden `rwsr-sr-x`.

Exemples de permisos mal assignat:

`chmod 4655 programa`
assigna els permisos `rwSr-xr-x`. El **4** inicial assigna el `setuid` però els permisos `655` corresponien a `rw-r-xr-x`. En aplicar el `setuid` sense la `x` es mostra la `S` majúscules indicant la ineffectivitat del permís.

`chmod 7666 directori`
assigna els permisos `rwSrwSrwT` que no tenen ni cap ni peus!

`chmod 1666 directori`
assigna els permisos `rw-rw-rwT` al directori. Podem observar que l'sticky bit no està correctament assignat.

Simbòlic

Per establir els permisos en simbòlic cal usar els caràcters s i t. Cal posar atenció amb la s perquè serveix tant per a setuid com per setgid.

s *setuid* | *setgid* per assignar aquest permís segons correspongui al bloc de permisos propietari o grup
t *sticky bit* per assignar aquest permís al bloc altres.

Exemples d'assignació de permisos:

chmod u+s programa
assigna a programa el setuid

chmod ug+s programa
assigna al propietari i grup el setuid i setgid.

chmod g-s directori
elimina el permís setgid del directori

chmod +t directori
assigna el permís sticky bit al directori

chmod -t directori
elimina el permís de sticky bit de directori

chmod u=rws programa
assigna al bloc de permisos del propietari els permisos rws.

Exercicis d'exemple

1. Llista els directoris /tmp i /var/tmp i digues quin permís especial tenen activat.

```
$ ls -ld /tmp/ /var/tmp/  
drwxrwxrwt 16 root root 380 21 des 10:38 /tmp/  
drwxrwxrwt 15 root root 4096 21 des 10:16 /var/tmp/
```

- tenen activat el permís de sticky bit.

2. Llista del directori /usr/bin tots els fitxers amb permisos de propietari rws.

```
$ ls -l /usr/bin/ | grep "rws"  
-rwsr-xr-x. 1 root root 52984 2 ago 2017 at  
-rwsr-xr-x. 1 root root 73864 14 ago 2017 chage  
-rws--x--x. 1 root root 27992 27 mar 2018 chfn  
-rws--x--x. 1 root root 23736 27 mar 2018 chsh
```

```
-rwsr-xr-x. 1 root root 57608 2 ago 2017 crontab
-rwsr-xr-x. 1 root root 32040 7 ago 2017 fusermount
-rwsr-xr-x. 1 root root 31992 14 oct 2018 fusermount-glusterfs
-rwsr-xr-x. 1 root root 78432 14 ago 2017 gpasswd
-rwsr-xr-x. 1 root root 61336 23 abr 2018 ksu
-rwsr-xr-x. 1 root root 36064 27 mar 2018 mount
-rwsr-xr-x. 1 root root 39000 14 ago 2017 newgidmap
-rwsr-xr-x. 1 root root 41920 14 ago 2017 newgrp
-rwsr-xr-x. 1 root root 39000 14 ago 2017 newuidmap
-rwsr-xr-x. 1 root root 27872 12 abr 2018 passwd
-rwsr-xr-x. 1 root root 27688 11 jul 2018 pkexec
-rwsr-xr-x. 1 root root 32136 27 mar 2018 su
-rwsr-xr-x. 1 root root 27880 27 mar 2018 umount
```

3. Llista els permisos de l'ordre passwd. Quins permisos especials té activats?

```
$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 27872 12 abr 2018 /usr/bin/passwd
```

4. Copia l'ordre /usr/bin/cal al teu directori home i anomena-la calendari. Assignar-li el permís setuid i setgid. Fes-ho en octal.

```
$ cp /usr/bin/cal calendari
$ chmod 6755 calendari
$ ls -l calendari
-rwsr-sr-x 1 ecanet ecanet 57704 21 des 11:35 calendari
```

5. Desactiva del programa calendari el permisos setuid i setgid.

```
$ chmod ug-s calendari
$ ls -l calendari
-rwxr-xr-x 1 ecanet ecanet 57704 21 des 11:35 calendari
```

6. Activa al programa calendari el permís setgid usant notació simbòlica.

```
$ chmod g+s calendari
$ ls -l calendari
-rwxr-sr-x 1 ecanet ecanet 57704 21 des 11:35 calendari
```

7. Crea un directori anomenat testdir i assigna permisos 750 i també el setgid usant notació octal.

```
$ mkdir testdir
$ chmod 2750 testdir/
$ ls -ld testdir/
drwxr-s--- 2 ecanet ecanet 40 21 des 11:40 testdir/
```

8. Activa en el directori testdir el permís sticky bit usant notació simbòlica (aplica només la t no la x). Com es mostra el permís t?

```
$ chmod +t testdir/
```

```
$ ls -ld testdir/  
drwsr-s--T 2 ecanet ecanet 40 21 des 11:40 testdir/
```

- el permís t està mal concedit perquè falta la x i per això no és efectiu i es mostra amb la lletra T majúscula.

9. Usant notació simbòlica desactiva el setgid del directori testdir i activa la wx (a més de l'sticky bit) a altres.

```
$ chmod g-s,o+wx testdir/
```

```
$ ls -ld testdir/  
drwsr-x-wT 2 ecanet ecanet 40 21 des 11:40 testdir/
```

10. Amb notació simbòlica elimina la x dels permisos de propietari del directori testdir. Què passa amb el permís setuid? És rellevant?

```
$ chmod u-g testdir/
```

```
$ ls -ld testdir/  
d-wSr-x-wT 2 ecanet ecanet 40 21 des 11:40 testdir/
```

- en eliminar la x el permís de setuid queda mal aplicat i es mostra la S en majúscula.
- de totes maneres no és significatiu perquè el permís setuid aplicat a fitxers executables no té sentit, no és aplicable.