

3.33pt

Gestió dels usuaris

René Serral-Gracià¹

¹Universitat Politècnica de Catalunya (UPC)

February 11, 2022

Temari

- 1 Introducció a l'Administració de Sistemes
- 2 Instal·lació del Sistema Operatiu
- 3 **Gestió d'usuaris**
- 4 Gestió d'aplicacions
- 5 Monitorització del sistema
- 6 Manteniment del sistema de fitxers
- 7 Serveis locals
- 8 Serveis de xarxa
- 9 Protecció i seguretat
- 10 Virtualització

Outline

3.33pt

- 1 Introducció
- 2 Les bases de dades del sistema
- 3 Desactivació i baixa d'usuaris
- 4 Procés de Login
- 5 Permisos i proteccions

Outline

3.33pt

- 1 Introducció
 - Objectius
- 2 Les bases de dades del sistema
- 3 Desactivació i baixa d'usuaris
- 4 Procés de Login
- 5 Permisos i proteccions

Objectius

Coneixements

- Conèixer les bases de dades del sistema
- Permisos i proteccions de fitxers i directoris
 - Els bits de SetUID/SetGID

Habilitats

- Tasques de gestió d'usuaris
 - Alta d'usuaris
 - Creació de grups i assignació d'usuaris a grups
 - Desactivació i baixa d'usuaris

Comandes i fitxers

- `chmod`, `chown`, `id`, `useradd`, `userdel`, `umask`
- `/etc/passwd`, `/etc/group`, `/etc/shadow`

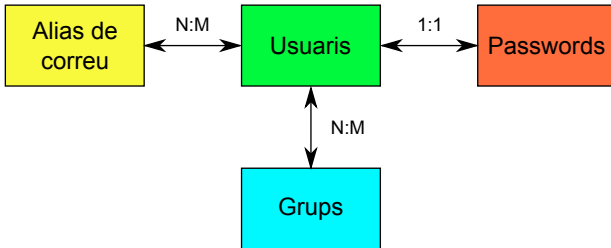
Outline

3.33pt

- 1 Introducció
- 2 Les bases de dades del sistema
- 3 Desactivació i baixa d'usuaris
- 4 Procés de Login
- 5 Permisos i proteccions

Bases de dades del sistema

- /etc/passwd
- /etc/group
- /etc/shadow
- /etc/aliases



/etc/passwd

- Accessible per lectura a tots els usuaris

Format

```
username:passwd:uid:gid:real_name:homedir:shell
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
nobody:x:99:99:Nobody:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
aramirez:x:500:500:Alex Ramirez, C6117, 54040:/home/aramirez:/bin/bash
```

Més sobre Usuaris

Usuaris especials

- root
 - UID 0 (no importa el username)
- ftp
 - Accés per FTP anònim (sense password)
- nobody
 - Usuari especial per NFS — i altres serveis

Usuaris del sistema

- Usats per executar serveis sense privilegis de superusuari
- No tenen shell assignat — Ni password
- Conjunt de privilegis que permeten realitzar les tasques

/etc/group

- Un grup pot tenir molts usuaris
- Cada usuari té un grup principal (/etc/passwd)
- Cada grup té una llista de membres

Format

groupname:passwd:gid:username,username,...

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
```

```
wheel:x:10:root
Mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
ftp:x:50:
nobody:x:99:
users:x:100:aramirez
aramirez:x:500:
```

Més sobre grups

Grups amb significat especial — dependent de la configuració

- `wheel`
 - Grup d'usuaris amb privilegis d'administració
- `nobody`
 - Grup especial per NFS
- `users`
 - Tots els usuaris hi pertanyen

/etc/shadow

- Accessible únicament per root
 - Password encriptat
 - Política d'expiració de passwords

Format

username:passwd:política d'expiració de passwords

- passwd: per canviar el password
- chage: permet canviar la política d'expiració
 - Temps mínim/màxim entre canvis de passwords
 - Data d'expiració d'un compte

```
root:$1$iVKd84gQ$IV7vHG0CHdIGGnYnNs00E/:12260:0:99999:7:::  
bin:*:12260:0:99999:7:::  
daemon:*:12260:0:99999:7:::  
...  
aramirez:$1$jGmk47hy$6Lkk.QYrMI67qPqvhTCdS.:12262::99999:::
```

/etc/aliases

- Base de dades d'alias de e-mail

- Permet redireccionar el mail
- Dels pseudo-usuaris
 - a l'administrador
 - a programes
 - a l'exterior

```
# Basic system aliases -- these MUST be present.
mailer-daemon: postmaster
postmaster: root

# General redirections for pseudo accounts.
bin: root
webmaster: root
support: postmaster

# Person who should get root e-mail
root: aduran, xavim@ac.upc.edu
```

Activitat

Individualment

- Detalleu el procés d'alta d'un usuari
- Modificació de les bases de dades
- Creació de directoris
- Fitxers per defecte
- ...

En grup

- Posta en comú i discussió
- Programació de la comanda useradd (pseudocodi)

Gestió d'usuaris – Comandes bàsiques

Gestió d'usuaris

- `useradd (adduser) userdel`
- `usermod` — Permet modificar tot menys el username
- `passwd`
- `newusers`
- `vipw`

Gestió de grups

- `groupadd groupdel`
- `groupmod`
- `gpasswd (passwd -g)`
- `newgrp, sg`
- `vigr`

Outline

3.33pt

- 1 Introducció
- 2 Les bases de dades del sistema
- 3 Desactivació i baixa d'usuaris**
 - Desactivació
 - Baixa d'usuaris
 - Polítiques de gestió d'usuaris
- 4 Procés de Login
- 5 Permisos i proteccions

Desactivació

Eliminar un usuari de forma temporal

→ Cal impedir l'accés de l'usuari al sistema

- ❶ Invalidar el password
 - Afegir un caràcter il·legal (*)
 - Permet recuperar el password antic en cas de necessitat
- ❷ Invalidar el seu intèrpret de comandes
 - Canviar-lo per un altre (`/bin/false`, `/bin/nologin`)
 - Informa l'usuari que ha estat desactivat
 - Avisa l'administrador si l'usuari intenta accedir al sistema

Baixa d'usuari

Quan estem segurs que un usuari no necessita el seu compte...

- 1 Desactivar compte (invalidant el password)
- 2 Comprovar que l'usuari no estigui treballant a la màquina
- 3 Fer un backup de les seves dades
- 4 Esborrar les dades
- 5 Eliminar l'usuari de les bases de dades del sistema
 - /etc/shadow
 - /etc/passwd
 - /etc/group
- 6 Afegir una redirecció del seu correu electrònic
 - /etc/aliases

Polítiques de gestió d'usuaris

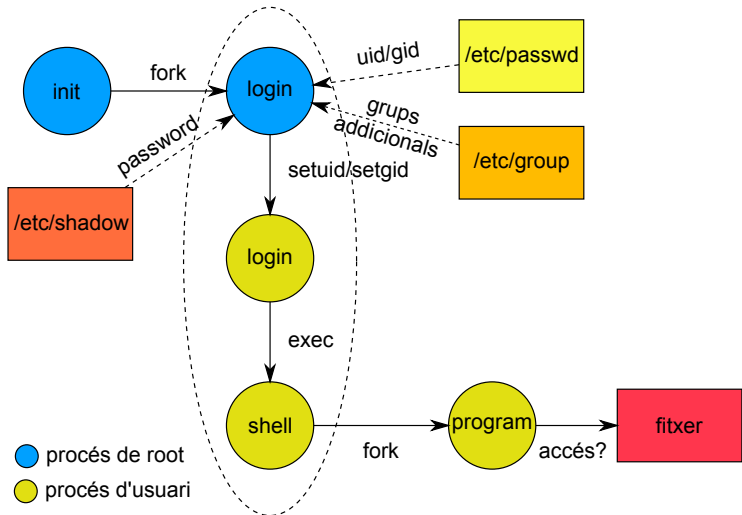
- Assignació de UIDs
 - No reciclar mai els UIDs
- Assignació de username
 - Guardar despatx i telèfon de contacte dels usuaris
- Organització de `/home`
 - Plana
 - Tots els usuaris (`/home/...`)
 - Jeràrquica, creant diferents nivells de directoris
 - Per departaments... pisos... despatxos...
(`/home/ac/user`)
 - ... en múltiples discos

Outline

3.33pt

- 1 Introducció
- 2 Les bases de dades del sistema
- 3 Desactivació i baixa d'usuaris
- 4 Procés de Login**
- 5 Permisos i proteccions

Procés de Login



Elevació de privilegis

Es realitza mitjançant crides a SetUID/SetGID

- Treballar com a root es perillós — i de cops innecessari
 - Millor tenir un usuari administrador i elevar els privilegis quan sigui necesari
- `su [usuari] [-c comanda]`
 - Permet canviar d'usuari (per defecte a root)
- `sudo [comanda]`
 - Permet executar una comanda com un altre usuari
 - L'administrador pot restringir quines comandes pot executar cada usuari

Outline

3.33pt

- 1 Introducció
- 2 Les bases de dades del sistema
- 3 Desactivació i baixa d'usuaris
- 4 Procés de Login
- 5 Permisos i proteccions

Permisos i proteccions

```
(-,d) rwx rwx rwx propietari grup
```

- 3 tipus de permisos
 - Lectura, escriptura i execució (rwx)
 - En fitxers normals...
 - En directoris...
- 3 àrees on s'apliquen
 - Propietari, grup, altres (ugo)
- Comandes:
 - `chown`: per canviar el propietari
 - `chgrp`: per canviar el grup d'un fitxer
 - `chmod`: per canviar els permisos
- Bit Set-UID/Set-GID (s)
- Bit Sticky (t) només a directoris

Permisos i proteccions

| | Fitxers | Directoris |
|------------|------------------------------------|---|
| r | Llegir els continguts | Llistar els continguts |
| w | Escriure/Modificar les continguts | Afegir/esborrar fitxers |
| x | Executar | Accedir al directori |
| SetUID | S'executa amb l'UID del propietari | No té efecte |
| SetGID | S'executa amb l'GID del propietari | Els fitxers es creen amb el mateix grup propietari que el directori |
| Sticky Bit | No té efecte | Només els propietaris dels fitxers el poden esborrar |

Activitat – En grup

- Assigneu les proteccions a directoris i fitxers per tal que el fitxer...

```
$ ls -l ./dirdades/dades.txt  
-rw-rw-r-- 1 aso01 aso01 9778 Nov 28 18:10 ./dirdades/dades.txt
```

- Només el pugui modificar el propietari
- El pugui llegir tot el grup
- Només el pugui esborrar el propietari
- Només el propietari pugui fer un “ls” del directori

Activitat – En grup

- Assigneu les proteccions a directoris i fitxers per tal que el fitxer...

```
$ ls -l ./dirdades/dades.txt  
-rw-rw-r-- 1 aso01 aso01 9778 Nov 28 18:10 ./dirdades/dades.txt
```

- Només el pugui modificar el propietari
 - `-w- - - - -`
- El pugui llegir tot el grup
 - `- - - r - - - - + dir - - - - -x - - -`
- Només el pugui esborrar el propietari
 - `dir → -w- - - - -`
- Només el propietari pugui fer un “ls” del directori
 - `dir → rw- - - - -`

```
$ ls -la ./dirdades/dades.txt  
drwx--x--- 1 aso01 aso01 1024 Nov 28 18:11 .  
-rw-r----- 1 aso01 aso01 9778 Nov 28 18:11 ./dirdades/dades.txt
```

Permisos per defecte

En la creació d'un fitxer/directori. . .

- El propietari el determina l'usuari i grup actuals
 - `id` informa de l'usuari/grup actual
 - `newgrp` canvia el grup actual de l'usuari
- Els permisos els determina la variable `umask`: user mask
 - Indica quins permisos **NO** es posen per defecte a nous fitxers o directoris

```
022: rwx r-x r-x
027: rwx r-x ---
```

Treball Personal

Tipus d'instal.lació d'aplicacions

- Formats de distribució de software
 - tar, gz, rpm, deb, zip. . .