

Administración de redes Linux

Gestión de usuarios

Iria Estévez Ayres

uc3m

Universidad **Carlos III** de Madrid

Departamento de Ingeniería Telemática

Marzo 2025

Índice

- 1 Cuentas de usuario
 - Concepto
 - Formas de acceso al sistema
- 2 Generación de claves ssh
- 3 Configuración de usuarios y grupos
 - Configuración de usuarios
 - Configuración de grupos
- 4 Permisos

Apartado 1

Cuentas de usuario

Cuentas de usuario

Linux es multiusuario:

- Usuario administrador (`root`)
 - Acceso total a todos los recursos.
 - Administración e instalación del equipo.
 - Establece claves y contraseñas
- Usuario normal (ej. `iria`)
 - Usan los recursos del sistema (los programas instalados).
 - Tienen unos recursos propios (cuenta).
 - Puede ser `sudoer` (gana permisos para hacer determinadas acciones).

¿Quién está conectado ahora?

```
telematica@debian-mini:~$ w
 00:55:10 up 1:45, 1 user, load average: 0,00, 0,00, 0,00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
telemati  tty1    -             23:09    3.00s  1.04s  0.00s w
telematica@debian-mini:~$ who
telematica tty1          2020-03-03 23:09
telematica@debian-mini:~$
```

Formas de acceso al sistema

Para acceder al sistema se pide nombre y palabra de paso de acceso (login y passwd):

- Consolas virtuales
 - Modo texto CTRL+Alt+F1 F4
 - Modo gráfico CTRL+Alt+F7
- Conexión serie COM1 (ttyS0), COM2 (ttyS1),
 - Conectar un módem, null modem o un dumb terminal. Para identificar los puertos serie:

```
$ dmesg | grep ttyS
[1.285839] 0000:00:16.3: ttyS4 at I/O 0xf0a0 (irq = 19, base_baud = 115200)
is a 16550A
$ sudo setserial -g /dev/ttyS4
/dev/ttyS4, UART: 16550A, Port: 0xf0a0, IRQ: 19
```

- Desde red (telnet, **ssh**)

Apartado 2

Generación de claves ssh

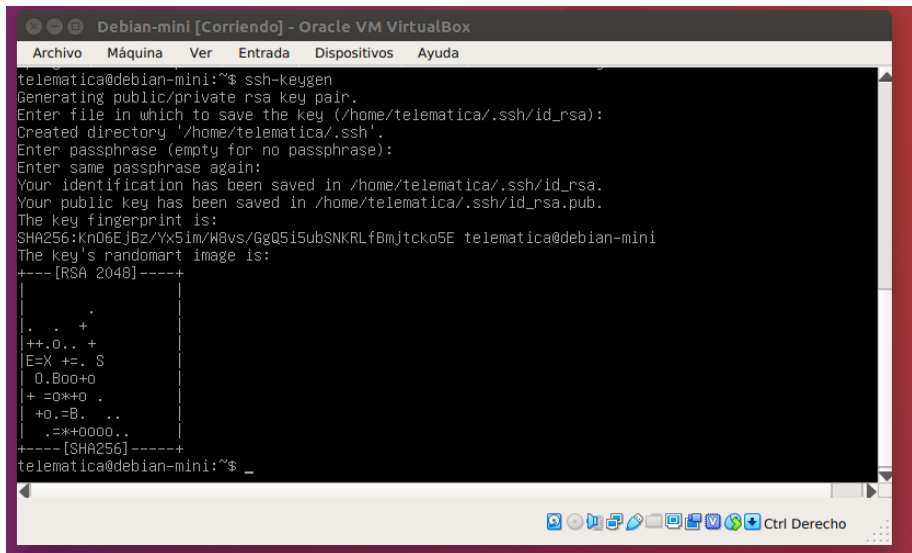
¿Qué es ssh-keygen?

- El protocolo SSH usa criptografía de clave pública para autenticar host y usuarios.
- Las claves de autenticación se crean usando un programa de generación de claves como `ssh-keygen`.
 - Estos pares de claves se suelen usar para logins automáticos, single sign-on y para autenticar hosts.
- No hace falta guardar las passwords en ficheros (se evita así que en un servidor comprometido, se robe la password del usuario).
- Debéis usarlas como si fuesen passwords y eliminarlas cuando ya no las necesitéis.

¿Cómo usar ssh-keygen?

- Forma más sencilla de generar un par de claves para autenticación de usuarios: ejecutar `ssh-keygen` sin argumentos.
- El par de claves se guardarán debajo del directorio `.ssh`
- Como por defecto el algoritmo es RSA, los nombres suelen ser `id_rsa.pub` e `id_rsa`
- Importante: la *passphrase* debe ser robusta.

Creando par de claves ssh para autenticación



```
Debian-mini [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

telematica@debian-mini:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/telematica/.ssh/id_rsa):
Created directory '/home/telematica/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/telematica/.ssh/id_rsa.
Your public key has been saved in /home/telematica/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:Kn06EjBz/Yx5im/W8vs/GgQ5iSubSNKRLfBmjtkco5E telematica@debian-mini
The key's randomart image is:
+---[RSA 2048]-----+
|
|  .
|.. . +
|++.. +
|E=X +=. S
| 0.B00+0
|+ =0*+0 .
|+0.=B. ..
| .=*+0000..
+---[SHA256]-----+
telematica@debian-mini:~$ _
```

The screenshot shows a terminal window titled "Debian-mini [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The terminal output shows the execution of the "ssh-keygen" command. It prompts for a file name to save the key, creates the directory "/home/telematica/.ssh", and asks for a passphrase (which is left empty). It then displays the key fingerprint: "SHA256:Kn06EjBz/Yx5im/W8vs/GgQ5iSubSNKRLfBmjtkco5E telematica@debian-mini". Below the fingerprint, it shows a randomart image for the RSA 2048 key. The prompt "telematica@debian-mini:~\$" is shown at the bottom of the terminal.

Clave pública generada

La clave pública tendrá esta pinta:

```
telematica@debian-mini:~$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDQJF2F5TDrvbrU0/jBCP48jUJpeiLRREbAaDjh5QKTvdAQQtKimg+etusuvW2
pquefyTzSxuxrYKJrOUQD1M9+UhmSV0eE3U33VAY2F1j1+K36BkuIJ4Uqoe7MBdcn0FLdGD79DPcH3ZwRapsCj10YxaCkaJ6UTJR
TxTntQYtbSqCYjEPSyZTgRP0IY3rB59czUncWbFFfr4D1nM19I1RyXgXR2Zq6bN29JfU6gX2H20bAjhTG+4aCdHHX27V64/Whh0G
xIWJvTXNFSNhM/3TyaQ07JFip0uY+TI4a1wR2fS1HupTZ8Zn8b41FNPGgdXgiqm+mfIC54Id5qQcieoV telematica@debian-m
ini
telematica@debian-mini:~$ _
```

Para poder usarla para autenticarte en un servidor:

- Puedes editar el fichero `authorized_keys` del servidor
- O usar el comando `ssh-copy-id`

Copiando la clave pública a un servidor

```
telematica@debian-mini:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub labgastt@monitor01.lab.it.uc3m.es
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/telematica/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install all the new keys
labgastt@monitor01.lab.it.uc3m.es's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'labgastt@monitor01.lab.it.uc3m.es'"
and check to make sure that only the key(s) you wanted were added.

telematica@debian-mini:~$ _
```

En el ejemplo, se copia a monitor01.lab.it.uc3m.es con la cuenta de una asignatura. Intenta hacer lo mismo, pero con tu usuario de los laboratorios del Departamento de Ingeniería Telemática.

Fichero authorized_keys

Después de hacer ssh al servidor, podemos comprobar el contenido de `.ssh/authorized_keys`:

```
monitor01:~> cd .ssh/  
monitor01:~/.ssh> ls  
authorized_keys  known_hosts  
monitor01:~/.ssh> cat authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDQJFZ2F5TDrvbrU0/jBCP48jUJpeiLRREbAaDjh5QKTvdAQQztKimg+etusuvW2  
pquefyTzSxuxrYKJrOUQD1M9+UhmSVDeE3U33VAYZF1j1+K36BkuIJ4Uqoe7MBdcn0FLdGD79DPch3ZwRapsCj10YxaCkaj6UTjR  
TxTntQYtbSqCYJEPsyZTgRP0IY3rB59czUncWbfFfr4D1nM19I1RyXgXR22q6bN29JfU6gX2H20bAjhTG+4aCdHHX27V64/Whh0G  
xIWJvTXNFSnHm/3TYaQ07JFip0uY+TI4a1wR2fS1HupT282N8b41FNPGgdXgigq+mfIC54Id5qQcieoV telematica@debian-m  
ini  
monitor01:~/.ssh>
```

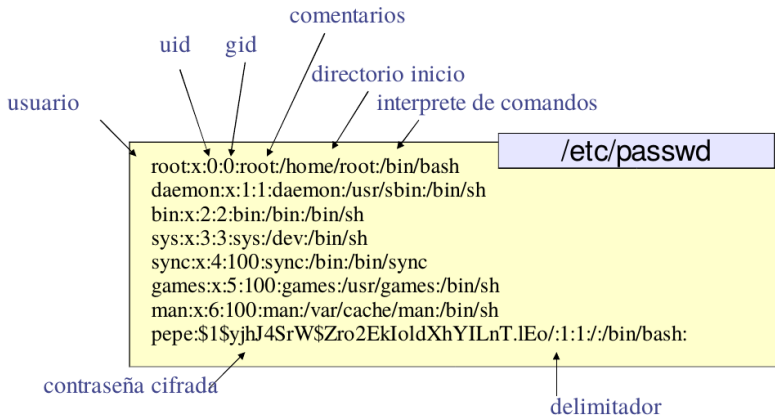
Apartado 3

Configuración de usuarios y grupos

Configuración de cuentas

- Ficheros clave
 - /etc/passwd : lista de todos los usuarios **locales**.
 - /etc/shadow (cuando hay shadow passwd).
 - /etc/group
 - /etc/gshadow (cuando hay shadow passwd).
- Comandos para la gestión de usuarios.
 - getent, compgen
 - passwd
 - groups, id
 - adduser, deluser

Estructura de /etc/passwd



Estructura de `/etc/passwd`

- La contraseña ya no se guarda en `/etc/passwd`. Se guarda:
 - `x` si está guardada en `/etc/shadow` (sólo tiene acceso el usuario `root`)
 - `!` el usuario está inhabilitado. No puede hacer login
- En el campo intérprete de comandos:
 - `/bin/false`: el usuario no puede acceder al sistema.
 - `/sbin/nologin`: el usuario no puede acceder y le aparece un mensaje indicándoselo (sistema creado en los 90, mucho después de la convención de `/bin/false`).

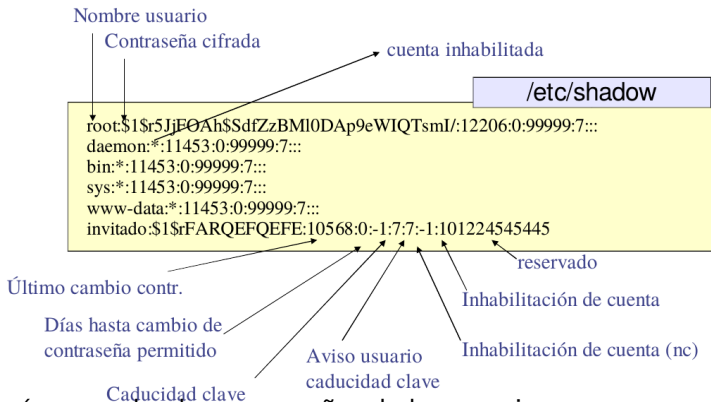
Usando getent

```
telematica@debian-mini:~$ getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/ssh:/usr/sbin/nologin
telematica:x:1000:1000:telematica,,:/home/telematica:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
telematica@debian-mini:~$ getent passwd telematica
telematica:x:1000:1000:telematica,,:/home/telematica:/bin/bash
telematica@debian-mini:~$ _
```

Usando compgen para saber qué usuarios hay

```
telematica@debian-mini:~$ compgen -u
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
Lapt
systemd-timesync
systemd-network
systemd-resolve
messagebus
avahi-autoipd
sshd
telematica
systemd-coredump
telematica@debian-mini:~$
```

Estructura de /etc/shadow



- Aquí se guardan las contraseñas de los usuarios.
- Sólo tiene acceso el root a este fichero.
- Al principio del campo contraseña viene indicado también el algoritmo de cifrado: `1` es MD5; `$2a$` es Blowfish; `$2y$` es Blowfish; `5` es SHA-256; `6` es SHA-512.

Nuestro /etc/shadow

```
telematica@debian-mini:~$ sudo cat /etc/shadow
root:$6$SArGzImseE0pobHJ$JkFEAbXhZ9ESxIaN48ck10VH1oSD0Ebxc0164Lf7ItQQHNIudMGWKSyfatUbRychgUiHEm9Jnytrf7b/6fI7q1:18283:0:99999:7:::
daemon:*:18283:0:99999:7:::
bin:*:18283:0:99999:7:::
sys:*:18283:0:99999:7:::
sync:*:18283:0:99999:7:::
games:*:18283:0:99999:7:::
man:*:18283:0:99999:7:::
lp:*:18283:0:99999:7:::
mail:*:18283:0:99999:7:::
news:*:18283:0:99999:7:::
uucp:*:18283:0:99999:7:::
proxy:*:18283:0:99999:7:::
www-data:*:18283:0:99999:7:::
backup:*:18283:0:99999:7:::
list:*:18283:0:99999:7:::
irc:*:18283:0:99999:7:::
gnats:*:18283:0:99999:7:::
nobody:*:18283:0:99999:7:::
_apt:*:18283:0:99999:7:::
systemd-timesync:*:18283:0:99999:7:::
systemd-network:*:18283:0:99999:7:::
systemd-resolve:*:18283:0:99999:7:::
messagebus:*:18283:0:99999:7:::
avahi-autoipd:*:18283:0:99999:7:::
sshd:*:18283:0:99999:7:::
telematica:$6$siBtT2uRhVdoulJP$dFyI4sGu4d92gKx7bXLdCtYPAmT.1ZuWqVTIPl4uwV.GgPRIC5hgP/SFyt/trFfT3U8pF0rmdmoclRvna810.:18283:0:99999:7:::
systemd-coredump:!:18283:0:99999:7:::
telematica@debian-mini:~$ _
```

- El SALT de la contraseña aparece entre \$\$

Cambiar la contraseña

- Debemos usar el comando `passwd`
 - Para cambiar nuestra contraseña, sin argumentos.
 - Para cambiar la de otros usuarios, `passwd nombreUsuario`
- Cambiando nuestra contraseña, comprobad cómo cambian los campos

```
telematica:$6$s1btT2wRhVdoulJP$dFyI4sGu4d92gKx7bXLdCtYPAmT.i2uWqVT1Pt4wwV.GgPRIC5hgP/SFyt/tRFfT3U8pF
OrmmdocLtRvna810.:18283:0:99999:7:::
systemd-coredump:!!:18283::::::
telematica@debian-mini:~$ passwd
Cambiando la contraseña de telematica.
Current password:
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
telematica@debian-mini:~$ sudo cat /etc/shadow | grep telematica
telematica:$6$tzJkizrx2X.K1020$a0zAbqKkdBy0b4qzSLdq31kPbIQz8zuEy0PA5dcAG8X8jdxp30xR5PvNmMcGG2amJLTrB
n80021tpBxQ/0eo3/:18325:0:99999:7:::
telematica@debian-mini:~$ _
```

Cambio de información de la edad para una contraseña

Usando el comando `chage`.

```
telematica@debian-mini:~$ sudo chage telematica
Cambiando la información de la edad para telematica
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado

    Duración mínima de la contraseña [0]:
    Duración máxima de la contraseña [99999]:
    Último cambio de contraseña (AAAA-MM-DD) [2020-03-04]:
    Aviso de caducidad de la contraseña [7]:
    Contraseña inactiva [-1]:
    Fecha de caducidad de la cuenta (AAAA-MM-DD) [-1]:
telematica@debian-mini:~$ _
```

Verificando la integridad de las contraseñas

- El comando `pwck` verifica la integridad de los usuarios y la información de autenticación (consistencia de los ficheros).
- Comprueba todas las entradas en `/etc/passwd` y `/etc/shadow` tienen el formato adecuado y contienen datos válidos.
- Se pide al usuario que borre las entradas que no tienen un formato adecuado o que tienen otros errores no corregibles.

Añadiendo usuarios al sistema

Podemos añadir nuevos usuarios locales al sistema mediante los comandos:

- `adduser` Herramienta interactiva de alto nivel
- `useradd` Herramienta de bajo nivel

adduser

```
$ sudo adduser perico
Adding user 'perico' ...
Adding new group 'perico' (1004) ...
Adding new user 'perico' (1004) with group 'perico' ...
Creating home directory '/home/perico' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for perico
Enter the new value, or press ENTER for the default
Full Name []: Perico
Room Number []: comedor
Work Phone []: 666666666
Home Phone []: 111111111
Other []:
Is the information correct? [Y/n] y
$ sudo grep perico /etc/passwd
perico:x:1004:1004:Perico,comedor,666666666,111111111:/home/perico:/bin/bash
$ ls -ld /home/perico
drwxr-xr-x 2 perico perico 4096 Mar  3 13:05 /home/perico
```

deluser herramienta análoga para borrar usuarios

useradd

```
$ sudo useradd frederico
$ sudo grep frederico /etc/passwd
frederico:x:1005:1005::/home/frederico:/bin/sh
$ ls -ld /home/frederico /home/perico
ls: cannot access '/home/frederico': No such file or directory
```

userdel herramienta análoga para borrar usuarios.

PAM

- En Linux la autenticación del sistema la rige un sistema modular muy flexible denominado PAM.
- La autenticación usuario/contraseña que hemos explicado es el módulo por defecto de PAM: `pam_unix.so`.
- Pero es solo una de las posibilidades, el paquete `libpam-modules` instala muchos módulos distintos que se pueden ver en `/var/lib/dpkg/info/libpam-modules.list`
- Si queremos cambiar el módulo de autenticación lo tenemos que configurar en el fichero `/etc/nsswitch.conf` (Name Service Switch)
- Veremos en una práctica como utilizar LDAP con PAM.

Name Service Switch

- Muchas funciones en la biblioteca GNU C (glibc) necesitan configurarse para trabajar correctamente en el entorno local.
- Esto es lo que hace el fichero de configuración `/etc/nsswitch.conf`: especifica los servicios (módulos) para acceder a una *base de datos*.

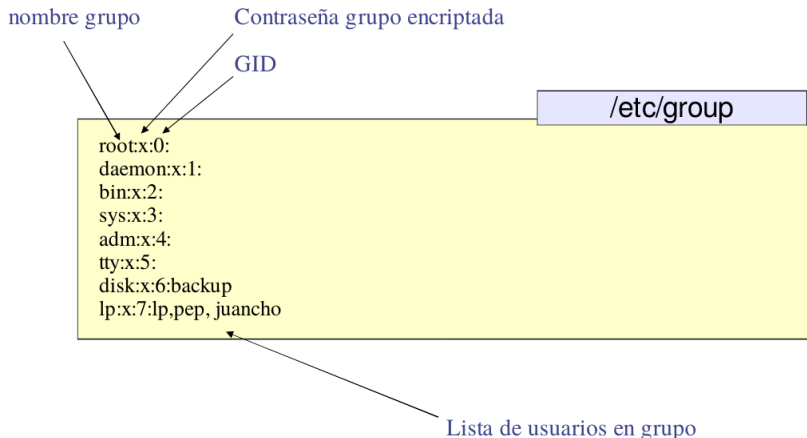
```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap
gshadow:     files
hosts:       files mdns4_minimal dns [NOTFOUND=return] mdns4 winbind
networks:    files
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files
netgroup:    nis
```

- Además de los módulos permite especificar condiciones (ej. NOTFOUND) y las acciones a tomar (ej. return).
- Cuando se ponen varios módulos se van probando en la secuencia indicada.
- Toda la información está en el paquete `glibc-doc-reference`.

¿Por qué grupos de usuarios?

- Facilita la gestión de instalaciones grandes de Linux (UNIX).
- Facilita compartir archivos u otros recursos con un pequeño número de usuarios.
- Facilita la gestión y monitorización de los usuarios.
- La pertenencia a un grupo da al usuario acceso especial a los archivos y directorios o dispositivos que están permitidos a ese grupo.

Estructura de /etc/group



Información acerca de los grupos de un usuario (I)

- Listado de todos los grupos a los que pertenece: `groups`, `groups usuario`

```
telematica@debian-mini:~$ groups
telematica cdrom floppy audio dip video plugdev netdev bluetooth
telematica@debian-mini:~$ groups telematica
telematica : telematica cdrom floppy audio dip video plugdev netdev bluetooth
telematica@debian-mini:~$ groups root
root : root
telematica@debian-mini:~$
```

- Imprimir sus identificadores:
 - Identificador de grupo principal: `id -g`, `id -g usuario`
 - Nombre de su grupo principal: `id -gn`, `id -gn usuario`
 - Todos los grupos a los que pertenece: `id -G`, `id -G usuario`

Información acerca de los grupos de un usuario (y II)

```
$ id
uid=1000(telematica) gid=1000(telematica) grupos=1000(telematica),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
$ id -g
1000
$ id -g telematica
1000
$ id -gn
telematica
$ id -g root
0
$ id -gn root
root
$ id -G telematica
1000 24 25 29 30 44 46 109 111
$ id -Gn telematica
telematica cdrom floppy audio dip video plugdev netdev bluetooth
$ id -Gn root
root
$
```

Gestionando grupos de usuarios

- Para añadir un nuevo grupo: `groupadd nombreGrupo`.
- Para añadir un usuario a un grupo (diferentes formas): `useradd` (bajo nivel), `gpasswd -a nombreUsr nombreGrupo`, `usermod -a -G nombreGrupo nombreUsr`
- Modificar definición de un grupo `groupmod`
 - Ejemplo: para cambiar el nombre de un grupo
`groupmod -n nuevoNombre nombreViejo`
- Borrar un grupo `groupdel nombredeGrupo`

```
$ id -Gn perico
perico
$ sudo groupadd futbol
$ sudo gpasswd -a perico futbol
Añadiendo al usuario perico al grupo futbol
$ id -Gn perico
perico futbol
$
```

- Se puede cambiar el grupo de un usuario temporalmente durante sólo una sesión: comando `newgrp` (crea un nuevo hijo, la shell donde se ha cambiado el grupo).

Apartado 4

Permisos

Permisos especiales

- SUID
 - Cambia el propietario en tiempo de ejecución.
 - Ejemplo passwd.
- SGID
 - Cambia el grupo del fichero cuando se ejecuta
- Bit persistencia
 - Si está activo sólo el propietario puede borrar el fichero
 - Utilidad en ficheros temporales en /tmp

Permisos por defecto

- Un fichero se crea por defecto con los permisos dados por el complemento a 1 de `umask`.
 - Si la máscara vale 777: ningún permiso a ningún usuario.
 - Si la máscara vale 000: todos los permisos a todos los usuarios.
- Se puede cambiar `umask` de forma temporal en una sesión.

```
$umask
0022
$umask 777
$touch sinPermisos
$ls -l sinPermisos
----- 1 perico perico sinPermisos
```

Cambio de la propiedad de un fichero: chown, chgrp

- Cambiar el usuario al que pertenece: chown
- Cambiar al grupo al que pertenece: chgrp

```
$ ls -l prueba
-rw-r--r-- 1 perico perico 0 mar  4 17:26 prueba
$ sudo chgrp telematica prueba
[sudo] password for telematica:
$ ls -l
total 0
-rw-r--r-- 1 perico telematica 0 mar  4 17:26 prueba
$ sudo chown root prueba
$ ls -l
total 0
-rw-r--r-- 1 root telematica 0 mar  4 17:26 prueba
$
```

Administración de redes Linux

Gestión de usuarios

Iria Estévez Ayres

uc3m

Universidad **Carlos III** de Madrid

Departamento de Ingeniería Telemática

Marzo 2025