

## USUARIOS Y GRUPOS.

Como ya se ha afirmado Linux es un sistema multiusuario, lo cual permite que varios usuarios puedan conectarse y trabajar en él de forma simultánea. Las conexiones como ya se ha visto se pueden realizar a través de varias terminales locales o utilizando servicios de red como el Telnet y SSH.

Un usuario se caracteriza por su login el cual debe indicar para conectarse al sistema, y por su password o contraseña. Además, puede poseer un conjunto de datos adicionales como el domicilio, teléfono, etc.

El usuario con más privilegios en Linux es **root**. Este es el único con derechos suficientes para crear o eliminar a otros usuarios, además de acceder a todo el sistema de ficheros sin ninguna restricción.

En Linux existen grupos de usuarios que permiten otorgar los mismos privilegios a un conjunto de usuarios. Siempre que se añada un usuario al sistema se creará un grupo con su mismo nombre, llamado grupo primario. Durante la creación o posteriormente, se podrá incorporar el usuario a otros grupos secundarios. Así cuando creamos el usuario Olegario, el sistema creará automáticamente un grupo llamado Olegario que contará como único miembro con el usuario creado.

Tanto los usuarios como los grupos se identifican por el sistema a través de un identificador (ID) numérico. El usuario root siempre tiene el ID cero. Cada usuario cuando se conecta al sistema posee un identificador de usuario asociado (uid) y uno o varios identificadores de grupo (gid).

Al añadir un usuario también se creará un directorio base para el mismo con el nombre de su login. Este directorio se coloca por defecto en el directorio */home/nombredelusuario* excepto para root, cuyo directorio base es */root*.

La información asociada a los usuarios en un sistema Linux se guarda en el fichero **/etc/passwd** y las contraseñas y datos afines en **/etc/shadow**. Por su parte la información de los grupos, sus miembros y passwords están en **/etc/group** y **/etc/gshadow** respectivamente. (Vemos a la derecha un ejemplo del fichero **/etc/passwd**).

Para crear un usuario se usa el comando **useradd**, aunque es mucho mejor usar un script que viene instalado en Linux, que se llama **adduser**. Este script controla como funciona useradd y permite realizar funciones avanzadas, como crear automáticamente el directorio del usuario, configurar su perfil, etc.

```
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
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
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:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

## FICHERO DE USUARIOS: /ETC/PASSWD

Este fichero consta de 7 campos separados por el símbolo dos puntos (:).

Nombre	Contraseña	UID	GID	Información	Dir. Personal	Shell
--------	------------	-----	-----	-------------	---------------	-------

- **Nombre:** Indica el nombre de la cuenta de usuario.
- **Contraseña:** indica una X siempre, ya que en los sistemas operativos modernos la contraseña no se almacena en este mismo fichero, ya que sería un fallo de seguridad muy grande. En su lugar la contraseña se almacena en el fichero /etc/shadow.
- **UID:** es el número que se le asigna a cada usuario en el sistema.
- **GID:** es el número del grupo principal al que pertenece este usuario. (El grupo principal suele tener el mismo nombre del usuario).
- **Información:** varios campos separados por coma, y se utilizan a título informativo, no tienen ningún significado propio importante.
- **Dir. Personal:** directorio donde se almacenará el perfil del usuario (sus documentos y configuraciones). Suele ser habitual que sea /home/*Nombredelusuario*.
- **Shell:** el programa que se debe ejecutar para ofrecerle un terminal de acceso al sistema a este usuario, normalmente es el bash ya que es el shell que utilizamos por defecto. Si no queremos que un usuario pueda tener acceso a estos terminales, bastaría con indicarle aquí un nombre falso, como por ejemplo /bin/false y de este modo este usuario no podría interactuar con el sistema aunque realizara correctamente el login.

Vemos aquí un ejemplo de las últimas 5 líneas de un fichero /etc/passwd.

```
usuario@debian740:~$ tail -5 /etc/passwd
saned:x:111:117::/home/saned:/bin/false
Debian-gdm:x:112:118:Gnome Display Manager:/var/lib/gdm3:/bin/false
usuario:x:1000:1000:usuario,,,:/home/usuario:/bin/bash
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
mysql:x:114:121:MySQL Server,,,:/nonexistent:/bin/false
usuario@debian740:~$
```

## EL FICHERO DE CONTRASEÑAS /ETC/SHADOW.

Este fichero consta de 8 campos separados por dos puntos.

Nombre	Contraseña	Ult. cambio	Mínimo	Máximo	Aviso	Inactivo	Caducidad
--------	------------	-------------	--------	--------	-------	----------	-----------

- **Nombre:** Nombre del usuario.
- **Contraseña:** es la contraseña del usuario encriptada. Esta contraseña hoy en día se representa en tres partes distintas, separadas por el símbolo del dólar (\$).
  - Id. Esto nos indica el método de encriptación que fue utilizado. Un valor de 1 indica MD5, un valor de 2 Blowfish, 3 es NT Hash, 5 es SHA-256 y 6 es SHA-512.
  - Salt. Este valor se usa por los algoritmos de encriptación y puede ser de hasta 16 caracteres. Este valor se crea aleatoriamente en cada generación de contraseña.
  - Hash. La contraseña en sí misma. MD5 usa 22 caracteres, SHA-256 usa 43, y SHA-512 usa 86.

Si nos encontramos con un asterisco en este campo significa que la cuenta está bloqueada. Lo mismo se puede conseguir colocando una exclamación (!) al principio de la contraseña. Una cuenta sin contraseña la veremos o bien con todo este campo en blanco, o bien con dos exclamaciones consecutivas (!!).

- **Ult. Cambio:** indica el día en que se cambió la contraseña por última vez. (Este número indica los días que han transcurrido desde el 1-1-1970).
- **Mínimo:** El mínimo número de días que hay que esperar para cambiar la contraseña.
- **Máximo:** El máximo número de días antes de que la contraseña caduque.
- **Aviso:** Antes de que la contraseña caduque, avisaremos al usuario al llegar a este número de días.
- **Inactivo:** Una vez que la contraseña caduque esperaremos este número de días antes de bloquearla definitivamente.
- **Caducidad:** Es una fecha, en la cual la cuenta automáticamente quedará bloqueada. (Este número indica los días que han transcurrido desde el 1-1-1970).

```
root@debian740:/home/usuario# tail -5 /etc/shadow
saned*:16186:0:99999:7:::
Debian-gdm*:16186:0:99999:7:::
usuario:$6$0aLI6P1D$G8TcjA3i0De0J4sQ6JmGy1nmKJwYlw0.0JNREi4dbv3a48b02EBLNw8Bt2C/
VKuaqwxw83aTLuIyhhzm1n2IOG/:16186:0:99999:7:::
hplip*:16372:0:99999:7:::
mysql:!:16393:0:99999:7:::
root@debian740:/home/usuario#
```

Dado que estos campos son un poco especiales, es más fácil consultarlos con el comando chage.

```
chage -l usuario
```

---

### EL FICHERO DE GRUPOS /ETC/GROUP.

Este fichero consta de 4 campos separados por dos puntos.

Nombre	Contraseña	GID	Miembros
--------	------------	-----	----------

- **Nombre:** Es el nombre del grupo
- **Contraseña:** al igual que ocurre con los usuarios, los grupos también pueden tener contraseña, y lo normal es no incluir esta contraseña en este fichero, sino en su propio fichero `/etc/gshadow`.
- **GID:** Es el identificador numérico del grupo.
- **Miembros:** Los nombres de los miembros del grupo separados por coma.

```
root@debian740:/home/usuario# tail -5 /etc/group
usuario:x:1000:
lpadmin:x:119:
ssl-cert:x:120:
mysql:x:121:usuario,margarita
margarita:x:1001:
root@debian740:/home/usuario#
```

---

### EL FICHERO DE CONTRASEÑAS DE GRUPOS /ETC/GSHADOW.

Este fichero consta de 4 campos separados por dos puntos.

Nombre	Contraseña	Administradores	Miembros
--------	------------	-----------------	----------

- **Nombre:** El nombre del grupo.
- **Contraseña:** Una contraseña encriptada con las mismas características que la existente en el fichero shadow. Si existe una contraseña en un grupo, un usuario que se quiera introducir como miembro del grupo tendrá que saber dicha contraseña ya que el sistema se la pedirá (comando `newgrp`). Si un grupo no tiene una contraseña, solo el root o los administradores del grupo podrán asignar miembros a dicho grupo.
- **Administradores.** Una lista de usuarios separados por coma que pueden añadir o eliminar miembros al grupo.
- **Miembros:** Una lista de usuarios separados por coma. Estos son los usuarios que pueden acceder al grupo sin que se le pida la contraseña. Esta lista debe ser la misma que la que se encuentra en `/etc/group`.

- Miembros. Lista de miembros del grupo separados por coma.

```
root@debian740:/home/usuario# tail -5 /etc/gshadow
usuario:::
lpadmin:::
ssl-cert:::
mysql:::usuario,margarita
margarita:::
root@debian740:/home/usuario#
```

---

#### OTROS FICHEROS IMPORTANTES.

A parte de los ficheros anteriores debemos tener en cuenta los siguientes:

- **/etc/default/useradd**: contiene los valores por defecto a la hora de añadir un usuario al sistema con el comando **useradd**.
- **/etc/adduser.conf**: contiene los valores por defecto a la hora de añadir un usuario al sistema con el comando **adduser**.
- **/etc/deluser.conf**: contiene los valores por defecto a la hora de eliminar un usuario del sistema con el comando **deluser**.
- **/etc/shells**: el fichero de shells contiene una lista de shells válidas. Si la Shell de usuario no está en este fichero no puede acceder al sistema mediante login.
- **/etc/skel**: directorio que almacena el contenido del directorio de los nuevos usuarios que se vayan añadiendo al sistema.