

GNU/Linux. Usuarios y grupos

[Información sobre el documento.....1](#)

[1. - Usuarios y grupos.....1](#)

[El usuario administrador.....1](#)

[Cambio de usuario al usuario root.....2](#)

[2. -Usuarios. Ficheros y comandos.....2](#)

[Comandos.....2](#)

[Fichero /etc/passwd.....3](#)

[Fichero /etc/shadow.....4](#)

[Ejemplo.....5](#)

[Fichero /etc/group.....6](#)

Información sobre el documento

El objetivo de este documento es enseñar, compartir conocimientos para facilitar el aprendizaje. Este documento es mejorable, y será actualizado si es preciso.

Este documento puede ser utilizado para uso personal, no comercial, como se presenta, respetando una serie de **condiciones de uso basadas en Licencia Creative Commons, como aparece en el logotipo, que se describe a continuación**



- El **documento se proporciona como está**, por tanto *no se pueden realizar modificaciones*, ni en el **formato** ni en el **contenido**, ni trabajos derivados, sin la autorización expresa del autor.
- Se debe **mencionar al autor** del mismo, por supuesto sin modificar los enlaces o imágenes introducidas por éste en el documento.
- **No se puede utilizar** este material **con fines lucrativos, comerciales o cualquier uso que pueda proporcionar, directa o indirectamente, un beneficio económico de terceros**, sin la autorización expresa del autor.
- Si se desea publicar el documento en algún sitio web, se debe hacer a través de un **enlace al documento en el sitio del autor** (www.educatica.es o cursos.educatica.es)

Si se desea publicar como un recurso dentro de un sitio web, sin utilizar un enlace al material en el sitio web del autor, se debe solicitar autorización expresa y, en cualquier caso, referenciar el sitio web del autor (www.educatica.es).

Espero sea de provecho ;)

1. - Usuarios y grupos

Básicamente, hay dos tipos de usuarios en los sistemas basados en GNU/Linux o Unix: el administrador (root) y el resto de usuarios.

Nos vamos a centrar en sistemas basados en GNU/Linux, en concreto utilizaremos Ubuntu. Sin embargo, la mayor parte de lo explicado se puede utilizar en cualquier sistema GNU/Linux o Unix.

El usuario administrador

El usuario root es el usuario utilizado para administrar el sistema. Este usuario puede realizar cualquier tarea de administración sobre el sistema. Es decir, este usuario puede hacer cualquier cosa con el sistema.



Este “poder” es peligroso, porque cualquier fallo ocasionado con la cuenta de root puede afectar a la seguridad de todo el sistema. Hay que tener en cuenta, que cualquier aplicación que se ejecute con la cuenta de root, tendrá los mismos permisos que root, por tanto podrá hacer cualquier cosa en el sistema. Por tanto es necesario tomar una serie de medidas de seguridad para evitar problemas con el uso de la cuenta de root.

Veamos algunas de estas medidas de seguridad.

- **Usar la cuenta de root solo cuando sea necesario.** Para ello, el administrador del sistema deberá contar con una cuenta de usuario normal, que será la que utilice para trabajar con el sistema. Cuando necesite realiza alguna tarea de administración, se cambiará a la cuenta de root para llevarla a cabo. Una vez terminada la tarea de administración, vuelve a su cuenta normal.
- **No permitir inicio de sesión con la cuenta root.** Aunque esta medida no es necesaria, si está siendo utilizada cada vez más. De esta forma, se obliga a que el administrador del sistema tenga que tener una cuenta de usuario normal y acceder al sistema a través de ésta. Es una manera de forzar el cambio a root solo cuando sea necesario.

Cambio de usuario al usuario root

El sistema proporciona una serie de mecanismos para poder cambiar al usuario root desde una cuenta de usuario normal o para ejecutar comandos como usuario root. Por supuesto, solo podrá hacer este cambio aquel o aquellos usuarios que queramos que tengan permisos de administración.

Para ello, hay dos técnicas de protección básicas: conocer la contraseña de root e iniciar sesión como root o configurar el sistema para que ciertos usuarios puedan ejecutar comandos como si fueran root.

La primera opción, proporcionar la contraseña de root e iniciar sesión, conlleva proporcionar cierta información sensible a uno o varios usuarios. Con esta técnica no se puede tener control sobre qué usuarios (administradores) han realizado ciertas operaciones. Por ejemplo, un usuario podría cambiar la contraseña de root, impidiendo acceder al resto.

La segunda opción se basa en mantener una lista con los usuarios que pueden ejecutar tareas como root. De tal forma que, cuando un usuario quiera realizar una operación de administración, se comprueba si ese usuario pertenece o no a la lista de usuarios con permisos de administración. Si pertenece, se comprueba si realmente es quien dice ser, pidiendo una contraseña. Esta opción es más fácil de mantener y permite realizar, hasta cierto punto, seguimiento de las operaciones realizadas.

2. -Usuarios. Ficheros y comandos

Comandos

adduser	Añade un usuario al sistema
deluser	Elimina un usuario del sistema
usermod	Modifica la cuenta de un usuario en el sistema.

Toda la información de configuración de usuarios y grupos se almacena en ficheros. El S.O. Utiliza ficheros de texto plano para gestionar las cuentas de usuario y grupos. De hecho, en gneral, tanto el S.O. como las aplicaciones utilizan para su configuración ficheros de texto plano, que pueden editarse directamente, aunque no siempre es la mejor opción.

Los ficheros de configuración que se utilizan para gestionar usuarios y grupos son:

/etc/passwd	Información de configuración sobre las cuentas de usuario del sistema.
/etc/shadow	Contraseñas de las cuentas de usuario
/etc/group	Información sobre los grupos del sistema.

Fichero /etc/passwd

Este fichero almacena la información necesaria para gestionar cuentas de usuario en el sistema. En cada línea de este fichero se guarda información de una cuenta de usuario. Vamos a ver el contenido de este fichero.

```
javier@smr01Profesor:~$ cat /etc/passwd
....
pepito:x:1002:1002:Jose Manuel Andrade,Dpto. Informática,,,:/home/pepito:/bin/bash
pepita:x:1003:1004:Jose Manela Andrade,,,:/home/pepita:/bin/bash
maria:x:1004:1006:María Andrade,,,:/home/maria:/bin/bash
ramon:x:1005:1007:Ramón Roman,,,:/home/ramon:/bin/bash
```

Con el comando `cat` se muestra el contenido del fichero `/etc/passwd`. Como puedes observar, cada línea almacena información de una cuenta de usuario. En cada línea, se almacenan una serie de campos (7) con información del usuario, separados por un carácter de separación ":".

Si queremos obtener más información sobre el fichero `/etc/passwd` podemos consultar su manual.

```
javier@smr01Profesor:~$ man passwd
Nos dará información sobre el comando passwd
NOMBRE
    passwd - cambia contraseñas
....
FICHEROS
    /etc/passwd
        El archivo que contiene las contraseñas.
VÉASE TAMBIÉN
    group(5), passwd(5), shadow(5)
...
```

Para consultar información sobre el fichero `/etc/passwd` tenemos que consultar la sección 5 del manual de `passwd`.

```
javier@smr01Profesor:~$ man 5 passwd
...
```

Existen 7 campos para cada cuenta de usuario:

Nombre usuario	Nombre con el que se identifica al usuario en el sistema.
Contraseña	En este fichero NO se almacena la contraseña del usuario. Para ésto se utiliza, por motivos de seguridad otro fichero (/etc/shadow).
UID	Identificador numérico del usuario. Este número es usado por el sistema para identificar a los usuarios.
GID	Identificador numérico del grupo principal del usuario. Todo usuario debe tener un grupo principal, pudiendo pertenecer a varios grupos más, pero solo uno principal.
Información general	Datos sobre el usuario. No es obligatorio.
Directorio de Inicio	Ruta del directorio de inicio del usuario.
Interprete de comandos	Ruta del interprete de comandos que utilizará el usuario.

Fichero /etc/shadow

El fichero /etc/shadow almacena las contraseñas de las cuentas de usuario. Se utiliza este fichero por seguridad.

Esto es debido a que es necesario que cualquier usuario pueda leer información de cuentas de usuario, que se almacenan en /etc/passwd. Si las contraseñas se almacenaran en el fichero /etc/passwd, cualquier usuario del sistema tendría acceso a las contraseñas (cifradas).

La solución, guardar las contraseñas en un fichero al que solo puede acceder el usuario root.

```
javier@smr01Profesor:~$ cat /etc/shadow
cat: /etc/shadow: Permiso denegado
javier@smr01Profesor:~$ sudo cat /etc/shadow
...
pepito:$1$GeYcB$uo.yrKAWYXffHcQqkn.a1.:14715:0:99999:7:::
pepita:$1$b9lwK1t0$7CguRqM2yin72JKKRC/n70:14715:0:99999:7:::
maria:$1$Rxr4IClP$ruhndnFzF40gDLtTPZFe5F.:14718:0:99999:7:::
ramon:$1$on5bv0Gu$qWlRj7Fp8Y/Umazwe8Ifo/:14718:0:99999:7:::
```

Si queremos obtener información sobre lo que almacena /etc/shadow, consultamos su página de manual.

Como se puede intuir, estos dos ficheros son complementarios. En /etc/passwd se almacena la información de las cuentas de usuario y en /etc/shadow se almacenan las contraseñas de cada cuenta de usuario.

El formato básico del fichero es el siguiente:

Nombre de usuario	(Obligatorio) Identifica al usuario para el que se almacena la contraseña.
Contraseña cifrada	Contraseña cifrada del usuario.
Información de edad	El resto de campos almacena información para gestionar la caducidad de las contraseñas.

Ejemplo

Vamos a crear un usuario con una contraseña. Usuario rosa y contraseña rosa.

```
javier@smr01Profesor:~$ sudo adduser rosa
Añadiendo usuario 'rosa' ...
Agregando nuevo grupo `rosa' (1008) ...
Agregando nuevo usuario `rosa' (1006) con grupo `rosa' ...
Creando el directorio personal '/home/rosa' ...
Copiando archivos desde '/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para rosa
Introduzca el nuevo valor, o presione ENTER para el predeterminado
    Nombre completo []: Rosa Martín
    Número de habitación []:
    Teléfono del trabajo []:
    Teléfono de casa []:
    Otro []: Dpto. Contabilidad
¿Es correcta la información? [y/N] y
javier@smr01Profesor:~$
```

Ahora vamos a mostrar el contenido del fichero que guarda información sobre los usuarios (/etc/passwd)

```
javier@smr01Profesor:~$ cat /etc/passwd
...
rosa:x:1006:1008:Rosa Martín,,Dpto. Contabilidad:/home/rosa:/bin/bash
```

Vamos a mostrar información de la contraseña del usuario rosa. Para ello mostramos el fichero que contiene la información de contraseña de los usuarios (/etc/shadow).

```
javier@smr01Profesor:~$ sudo cat /etc/shadow
...
rosa:$1$rXPKi8do$fTn/wJ2Xnh04feT1h9EsG.:14725:0:99999:7:::
```

Vamos a cambiar la contraseña del usuario rosa. Ahora será: "asor".

```
javier@smr01Profesor:~$ sudo passwd rosa
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
```

Ahora comprobamos que el fichero /etc/shadow se ha actualizado:

```
javier@smr01Profesor:~$ sudo cat /etc/shadow
...
rosa:$1$EVHSXpBt$3TYAvdG8neKC38GtY1tC20:14725:0:99999:7:::
```

Si comparamos la línea actual del fichero /etc/shadow de la inicial, vemos como ha cambiado la contraseña

```
rosa:$1$rXPKi8do$fTn/wJ2Xnh04feT1h9EsG.:14725:0:99999:7:::
rosa:$1$EVHSXpBt$3TYAvdG8neKC38GtY1tC20:14725:0:99999:7:::
```

Vamos a poner de nuevo la contraseña inicial y mostramos el fichero de contraseña.

```
javier@smr01Profesor:~$ sudo passwd rosa
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
javier@smr01Profesor:~$ sudo cat /etc/shadow | grep rosa
rosa:$1$6Rp5/ZbV$hBz8t1wx.B9nTtYWuqhYN.:14725:0:99999:7:::
```

Fichero /etc/group

Se trata del fichero donde se guarda información de los grupos a los que pertenecen los usuarios del sistema. En cada línea se almacena información de un grupo. Los campos son los siguientes:

Nombre grupo	identifica al grupo.
Contraseña	No se suele utilizar.
GID	Identificador numérico del grupo
Lista de miembros	Nombres de usuarios separados por coma que pertenecen al grupo.