Administración básica del Sistema Operatiu. Gestión d'usuaris local en Linux.

Archivos de administración y control de usuarios

.bash_logout	Se ejecuta cuando el usuario abandona la sesión.
.bash_profile	Se ejecuta cuando el usuario inicia la sesión.
.bashrc	Se ejecuta cuando el usuario inicia la sesión.
/etc/group	Usuarios y sus grupos.
/etc/gshadow	Contraseñas encriptadas de los grupos.
/etc/login.defs	Variables que controlan los aspectos de la creación de usuarios.
/etc/passwd	Usuarios del sistema.
/etc/shadow	Contraseñas encriptadas y control de fechas de usuarios del sistema.

Comandos de administración y control de usuarios

adduser	Ver useradd
chage	Permite cambiar o establecer parámetros de las fechas de control de la contraseña.
chpasswd	Actualiza o establece contraseñas en modo batch, múltiples usuarios a la vez. (se usa junto con newusers)
id	Muestra la identidad del usuario (UID) y los grupos a los que pertence.
gpasswd	Administra las contraseñas de grupos (/etc/group y /etc/gshadow).
groupadd	Añade grupos al sistema (/etc/group).
groupdel	Elimina grupos del sistema.
groupmod	Modifica grupos del sistema.
groups	Muestra los grupos a los que pertence el usuario.
newusers	Actualiza o crea usuarios en modo batch, múltiples usuarios a la vez. (se usa junto chpasswd)
pwconv	Establece la protección shadow (/etc/shadow) al archivo /etc/passwd.
pwunconv	Elimina la protección shadow (/etc/shadow) al archivo /etc/passwd.
useradd	Añade usuarios al sistema (/etc/passwd).
userdel	Elimina usuarios del sistema.
usermod	Modifica usuarios.

Adició de nous usuaris

Línia de comandes	**useradd, adduser, newusers, chpassw**
Manual	Modificació de l'arxiu **etc/passwd**; creació del directori inici; copia d'arxius de configuració al directori personal (.bash_profile,...); assignació de la contrasenya, ...
Per lots	**newusers, chpasswd**
Per entorn gràfic	**users-admin**
Eines gràfiques basades en entorn Web	**webmin**

Copia i explica tots el camps corresponents a un registre de l'arxiu **/etc/passwd**.

usuario:x:UID:GID:Comentarios:Directorio Home:Shell

- **usuario**: identificador de usuario en el sistema.
- **x**: contraseña, pero en su lugar aparece una 'x', ya que la contraseña se encuentra cifrada en /etc/shadow
- **UID**: número de identidad del usuario. Es un valor único. Suele ser mayor o igual que 100, ya que el 0 se reserva para el root y del 1 al 99 para tareas del sistema.
- **GID**: número de identidad de grupo. Al igual que ocurre con el UID, el cero se reserva para el grupo root.
- **comentarios**: nombre real u otros comentarios sobre el usuario (puede contener espacios).
- **directorio_home**: directorio de casa del usuario
- **shell**: intérprete de comandos (normalmente bash). En caso de que se encuentre en este campo /bin/false, el usuario no podrá ejecutar ningún comando del sistema.

Copia i explica tots el camps corresponents a un registre de l'arxiu **/etc/group**.

grupo:x:GID:Lista de usuarios

- **grupo**: identificador de grupo en el sistema.
- **x**: contraseña, aunque lo más común es que este campo aparezca vacío (el grupo no necesita contraseña).
- **GID**: número de identidad de grupo.
- **lista_usuarios**: lista de usuarios que pertenecen al grupo separados por comas. También se pueden añadir usuarios de otros grupos, con lo que tendrían todos los privilegios de este grupo.

Copia i explica tots el camps corresponents a un registre de l'arxiu **/etc/shadow**.

usuario: contraseña_cifrada: d1: d2: d3: d4: d5: d6: reservado

donde cada uno de los campos es:

- **usuario**: es el login o nombre de usuario (el mismo que en /etc/passwd)
- **x**: contraseña: aparece una x; la contraseña se encuentra cifrada en /etc/shadow.

- **d1**: nº de días desde el 01/01/1970 hasta último cambio de la contraseña.
- **d2**: nº de días que deben pasar hasta que se pueda cambiar la contraseña.
- **d3**: nº de días que deben pasar para que caduque la contraseña y deba ser cambiada.
- **d4**: nº de días de antelación con los que avisará el sistema de la caducidad de la contraseña.
- **d5**: nº de días con contraseña caducada antes de deshabilitar la cuenta.
- **d6**: nº de días desde el 01/01/1970 y el día en que se deshabilitó la cuenta.

Archivos de administración y control de usuarios

etc/passwd	Archivo que contiene los usuarios del sistema. Cada línea guarda información sobre un usuario. La información se organiza en campos separados por el carácter ":"
/etc/group	Archivo que contiene los grupos del sistema y usuarios que pertenecen a cada grupo
/etc/shadow	Archivo que contiene las contraseñas cifradas y control de fechas de usuarios del sistema. Los algoritmos de encriptación más utilizados en Linux son **DES** (en desuso por su poca seguridad), **MD-5**, **SHA-256** y **SHA-512**.
/etc/gshadow	Archivo que contiene las contraseñas cifradas de los grupos.
/etc/skel	Directorio que contiene los archivos de inicio y cierre de sesión de los usuarios. Se utiliza de plantilla para copiarlos en la creación de nuevos usuarios
.bash_logout	Se ejecuta cuando el usuario abandona la sesión.
.bash_profile	Se ejecuta cuando el usuario inicia la sesión.
.bashrc	Se ejecuta cuando el usuario inicia la sesión.
/etc/default/useradd	Archivo que contiene las variables que controlan los aspectos de la creación de usuarios. Contiene los valores por defecto a la hora de añadir un usuario al sistema con el comando **useradd**
/etc/login.defs	Archivo que contiene las variables que controlan los aspectos de la creación de usuarios. Si se utiliza el sistema de contraseñas encriptadas, este archivo define algunos valores por defecto sobre la encriptación de contraseñas y otros parámetros al generar un nuevo usuario. Contendrá el algoritmo de encriptación utilizado para las contraseñas (línea ENCRYPT_METHOD) si se va a permitir o no usar la encriptación con el algoritmo MD5 (MD5_CRYT_ENAB), establecer algunas variables del sistema y otros parámetros
/etc/adduser.conf	Contiene los valores por defecto cuando se añaden usuarios con el comando **adduser**
/etc/deluser.conf	Contiene los valores por defecto cuando se eliminan usuarios con el comando **deluser**
/etc/shells	Contiene la lista de shells válidos. Si el shell del usuario no está en el fichero, o bien el usuario tiene la shell **/bin/false**, no podrá acceder al sistema mediante **login**

Comandos de administración y control de usuarios

adduser	Añade usuarios al sistema (/etc/passwd) en modo interactivo
chage	Permite cambiar o establecer parámetros de las fechas de control de la contraseña
chpasswd	Actualiza o establece contraseñas en modo batch, múltiples usuarios a la vez. (se usa junto con newusers)
id	Muestra la identidad del usuario (UID) y los grupos a los que pertenece.
gpasswd	Administra las contraseñas de grupos (/etc/group y /etc/gshadow)
groupadd	Añade grupos al sistema (/etc/group)
groupdel	Elimina grupos del sistema
groupmod	Modifica grupos del sistema
groups	Muestra los grupos a los que pertenece el usuario
newusers	Actualiza o crea usuarios en modo batch, múltiples usuarios a la vez. (se usa junto chpasswd)
pwconv	Establece la protección shadow (/etc/shadow) al archivo /etc/passwd
pwunconv	Elimina la protección shadow (/etc/shadow) al archivo /etc/passwd
useradd	Añade usuarios al sistema (/etc/passwd)
userdel	Elimina usuarios del sistema
usermod	Modifica usuarios
mkpasswd	Genera contraseñas encriptadas
gpasswd	

Más información sobre los comandos y ficheros de administración y control de usuarios y grupos

Son los ficheros que el sistema lee o modifica a la hora de gestionar los usuarios y los grupos

/etc/passwd

Contiene en cada una de sus líneas información sobre un usuario. La información se organiza en campos separados por el carácter "**:**"

Cada línea del fichero tiene la siguiente estructura:

/etc/shadow

En este fichero se almacenan las contraseñas **encriptadas** de cada usuario. Dada la importancia de la información que almacena sólo el **root** o un usuario con privilegios de administrador puede tener permiso de lectura sobre él.

Cada vez que un usuario entra al sistema en este fichero se comprueba si la contraseña introducida es correcta.

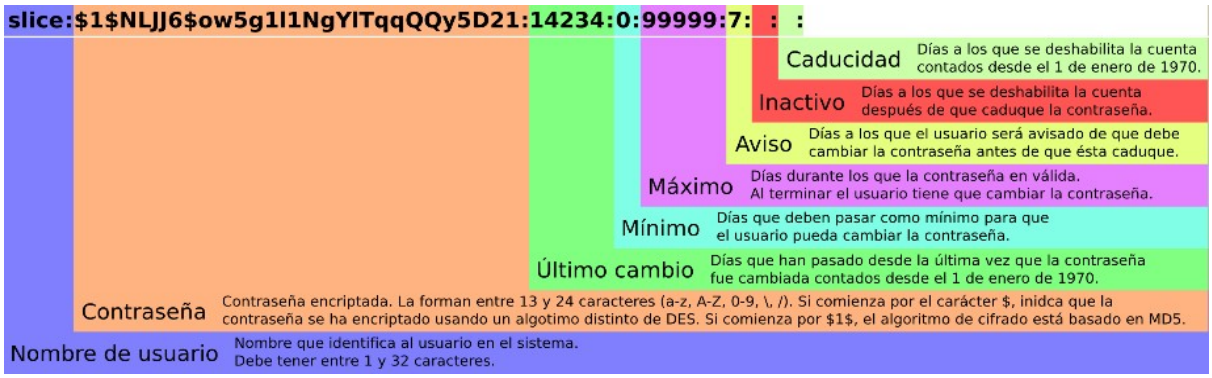
En sistemas Linux la contraseña encriptada se solía guardar en el campo **x** de **/etc/passwd**, utilizando el algoritmo de encriptación DES (Data Encryption Standard, Algoritmo Estándar de Encriptación. Por motivos de seguridad se empezó a utilizar el fichero **/etc/shadow** y algoritmos de encriptación más complejos. A la forma de utilizar este fichero para almacenar las contraseñas se le llama shadow password.

Los algoritmos de encriptación más utilizados en Linux son **DES** (en desuso por su poca seguridad), **MD-5**, **SHA-256** y **SHA-512**. Para saber cuál es el sistema de cifrado utilizado, se debe observar el primer número presente entre los símbolos **$** del archivo shadow:

- **DES**: son 13 caracteres, de los cuáles los 2 primeros son el valor del salt.
- **MD5**: si empieza por 1, el valor del salt está entre el segundo y tercer carácter '$' de la cadena, al igual que en los siguientes. **(22 caracteres)**
- **blowfish**

- **SHA-256**: si empieza por 5. **(43 Caracteres)**
- **SHA-512**: si empieza por 6. **(86 Caracteres)**

Cada línea del fichero **/etc/shadow** contiene campos separados por '**:**'. Tiene la siguiente estructura:



Al poner una contraseña a un usuario, una función hash la cifra con el algoritmo determinado según sea el cifrado. Toma un bloque arbitrario de datos y devuelve una cadena con una determinada longitud (valor hash). Los datos para ser codificados son denominados “el mensaje” y el valor hash se le denomina “message digest” o simplemente “digest”

Pero no es todo… pues si dos contraseñas fueran iguales o supiéramos el algoritmo usado quizás podríamos descifrarlo sabiendo unas cuantas contraseñas básicas y comparando el digest hasta sacar unas equivalencias.

Para evitar esto y cerrar completamente el cerco de seguridad de la contraseña, se le añaden los bit salt, que son datos al azar añadidos a la contraseña para posteriormente cifrar con el hash. Digamos que lo enmascaramos en más datos y así no sabremos qué parte es la contraseña real y cuales son los datos sin valor.

Los cifrado con bits salt se usan en muchos sistemas modernos, desde seguridad de credenciales a Seguridad en Internet. Hacen mucho más lentos los ataque por diccionario y de fuerta bruta para el crackeo.

Comando mkpasswd

El comando **mkpasswd**, genera contraseñas encriptadas. Algunas de sus opciones son:

- **mkpasswd -m help** → Muestra los algoritmos que podemos utilizar
- **mkpasswd -m des** → Pide contraseña y la encripta con dicho algoritmo.
- **mkpasswd -m md5**
- **mkpasswd -m sha-256**
- **mkpasswd -m sha-512 <palabra>** → Genera la contraseña cifrada de “palabra”con algoritmo sha-256 y usando salts aleatorios. Cada vez que se utiliza la misma “palabra” para ser encriptada se obtienen un resultado diferente, ya que se utiliza un “salt” aleatorio distinto.
- **mkpasswd -m sha-512 -S 1234567812345678** → Genera la contraseña cifrada de la palabra que pide a continuación, con algoritmo sha-256 y usando un salt el mismo salt de 8 bytes, por lo que el resultado obtenido serà siempre el mismo, ya que el “salt” no es aleatorio sino fijo.

/etc/group

Fichero en el que se encuentran definidos los grupos del sistema.

Cada usuario del sistema debe pertenecer obligatoriamente a un **grupo principal** o primario. El grupo principal de cada usuario es el grupo cuyo **GID** viene en el fichero indicado en el archivo **/etc/passwd**.

Además, un usuario puede pertenecer a otros grupos diferentes, llamados grupos secundarios.

Cada línea del fichero **/etc/group** tiene la siguiente estructura:

grupo:x:GID:usuarios

Ejemplo:

```
$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:ivan
...
aserrano:x:131:
```

El significado de cada campo es el siguiente:

- **nombre**: Contiene el nombre del grupo.
- **x**: Se utilizaba en los sistemas Unix para almacenar la contraseña del grupo. Actualmente no se suele utilizar, salvo para proteger ciertos grupos para evitar que un usuario que no pertenezca a él pueda convertirse en miembro del grupo con el comando **newgrp**, para lo que se añade ***** o **!** en el fichero **/etc/gshadow**, o bien se puede añadir una contraseña al grupo con el comando **gpasswd**.
- **GID**: Tiene el mismo significado que en el fichero **/etc/passwd**. Número que identifica al grupo del sistema.
- **usuarios**: Lista separada por comas de usuarios que tienen ese grupo como grupo secundario. Para saber el grupo primario deberemos mirar su GID en el fichero **/etc/passwd**.

/etc/gshadow

Fichero donde se guardan las contraseñas de los grupos del sistema. Aunque las contraseñas no se utilicen para los grupos, es necesario éste fichero para proteger al grupo. Al igual que shadow, sólo root tiene permiso de lectura sobre el fichero.

Cada línea del fichero tiene la siguiente estructura:

nombre:contraseña:

- **nombre**: Nombre del grupo
- **contraseña**: Puede ser una contraseña encriptada o bien los caracteres “*” o ”!”, dependiendo de si queremos utilizar las contraseñas de grupo o no.

/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 cuando se añaden usuarios con el comando **adduser**

/etc/deluser.conf

Contiene los valores por defecto cuando se eliminan usuarios con el comando **deluser**.

/etc/login.defs

Si se utiliza el sistema de contraseñas encriptadas, este archivo define algunos valores por defecto sobre la encriptación de contraseñas y otros parámetros cuando se genera un nuevo usuario. Contiene el algoritmo de encriptación utilizado para las contraseñas (línea ENCRYPT_METHOD), si se va a permitir o no usar la encriptación con el algoritmo MD5 (MD5_CRYT_ENAB), establecer algunas variables del sistema y otros parámetros.

Si buscamos dentro del fichero /etc/login.defs las cadenas de caracteres “encrypt method” y “md5” podemos ver el valor de dichos parámetros

```
$ grep -i "encrypt_method" /etc/login.defs
ENCRYPT_METHOD SHA512

$ grep -i "md5" /etc/login.defs
#MD5_CRYPT_ENAB          no
```

La opción **-i** hace que no diferencie entre mayúsculas y minúsculas.

/etc/shells

Contiene la lista de shells válidos. Si el shell del usuario no está en el fichero, o bien el usuario tiene la shell **/bin/false**, no podrá acceder al sistema mediante **login**

Directorios de configuración

/etc/skel

Directorio que contiene la plantilla con los archivos de inicio y finalización de sesión, para el directorio **home** de los nuevos usuarios que se vayan añadiendo al sistema.