

# UD3 – LINUX – ADMINISTRACIÓ I CONFIGURACIÓ-II

1º DAW - CFGS

Prof. Manuel Enguidanos  
*[menguidanos@fpmislata.com](mailto:menguidanos@fpmislata.com)*

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos

Cada usuario se identifica en el sistema de forma única con un número que lo identifica y diferencia de otro usuario. Ese número es el **UID** (***U**ser **ID***, identificador del usuario). Los usuarios deben pertenecer al menos a un grupo, al que se le llamará grupo primario o principal, y, además, pueden pertenecer a otros grupos, llamados grupos secundarios. Cada grupo en el sistema se identifica por un número llamado **GID** (***G**roup **ID***, identificador de grupo).

```
johndoe:x:1000:1000:John Doe,,:/home/helder:/bin/bash
```

UID

GID

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos

Existen tres tipos de usuarios:

- **Usuario *root*:** también llamado administrador del sistema o superusuario. Tiene todos los privilegios sobre el sistema y acceso a todo el sistema. Si se puede iniciar sesión con él hay que hacerlo con cautela. Su UID es el **0** y su directorio personal es **/root**.
- **Usuarios del sistema o especiales:** no son usuarios que van a iniciar sesión en el sistema. Tampoco son usuarios físicos. Suelen ser usuarios que necesitan ejecutar ciertos procesos y servicios a su nombre y ser propietarios de archivos. El UID de estos usuarios suele ser entre el 1 y el 999.
- **Usuarios estándar o normales:** usuarios que iniciarán sesión en el sistema, tienen un UID de 1000 en adelante, su directorio personal en donde tendrán todos los privilegios se ubica por defecto en una carpeta con su nombre dentro de `/home` y podrán tener diferentes tipos de permisos dentro del sistema.

## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos

### Gestión en el entorno gráfico

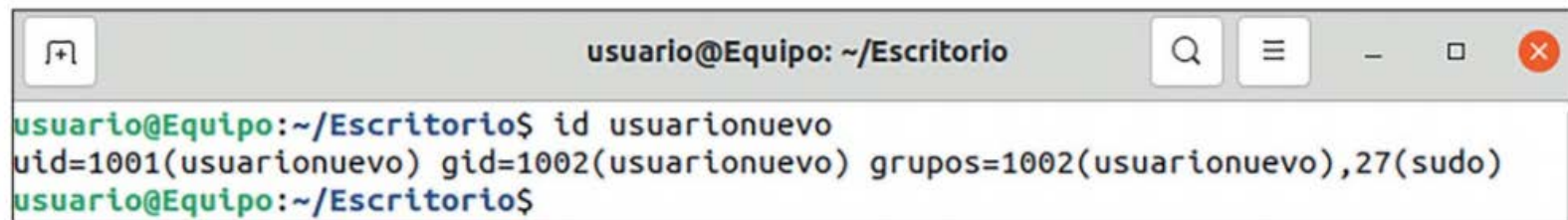
**Figura 3.18.** Usuario nuevo de tipo administrador al que se le permitirá establecer su contraseña en el siguiente inicio de sesión.

**Figura 3.17.** Para labores de administración el sistema puede solicitar de nuevo la contraseña al usuario por seguridad.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos

### ■■■ Gestión en el entorno gráfico



```
usuario@Equipo: ~/Escritorio
usuario@Equipo:~/Escritorio$ id usuarionuevo
uid=1001(usuarionuevo) gid=1002(usuarionuevo) grupos=1002(usuarionuevo),27(sudo)
usuario@Equipo:~/Escritorio$
```

**Figura 3.19.** Información del nuevo usuario creado, como su UID, su GID y los grupos a los que pertenece.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Gestión en el entorno gráfico

Para realizar la gestión desde el entorno gráfico de forma más completa debe instalarse la aplicación **Usuarios y grupos**, lo que puede hacerse desde el siguiente paquete:

```
sudo apt install gnome-system-tools
```

Una vez instalado, se accede a esta aplicación desde las aplicaciones (Figura 3.20).

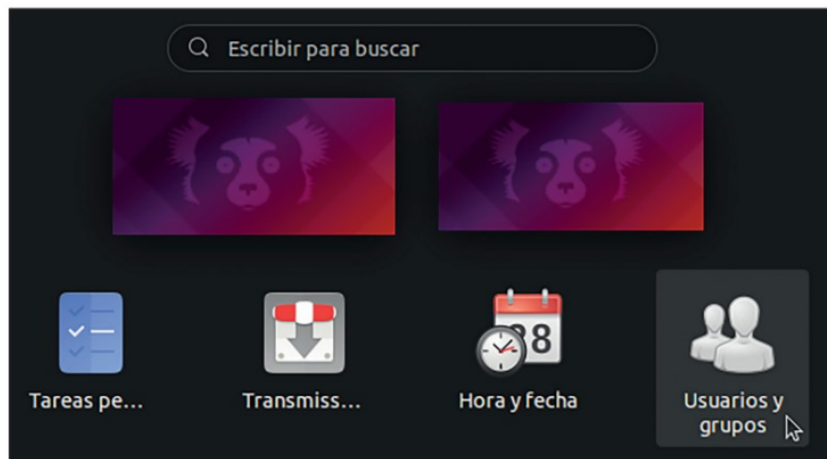


Figura 3.20. Acceso a la aplicación *Usuarios y grupos* una vez instalada.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■ ■ 3.3.1. Usuarios y grupos ■ ■ ■ Gestión en el entorno gráfico

Accediendo a **Mostrar aplicaciones** se puede buscar la aplicación **Usuarios y grupos**. Al hacer clic sobre el icono se abrirá la ventana que se muestra en la Figura 3.21.



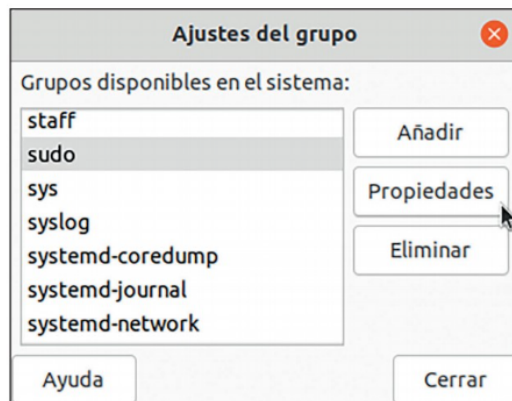
**Figura 3.21.** Ventana inicial de la aplicación Usuarios y grupos desde donde puede realizarse una gestión completa de los usuarios y los grupos.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos

### ■■■ Gestión en el entorno gráfico

Desde aquí se pueden añadir y eliminar usuarios, con los botones **Añadir** y **Eliminar**, respectivamente. Si se pulsa sobre **Gestionar grupos** (Figura 3.21) se muestra una ventana con todos los grupos disponibles en el sistema y se puede pulsar sobre **Añadir** o **Eliminar** para agregar o borrar grupos, respectivamente. Si se selecciona un grupo y se pulsa sobre **Propiedades** se puede modificar el grupo (Figura 3.22).



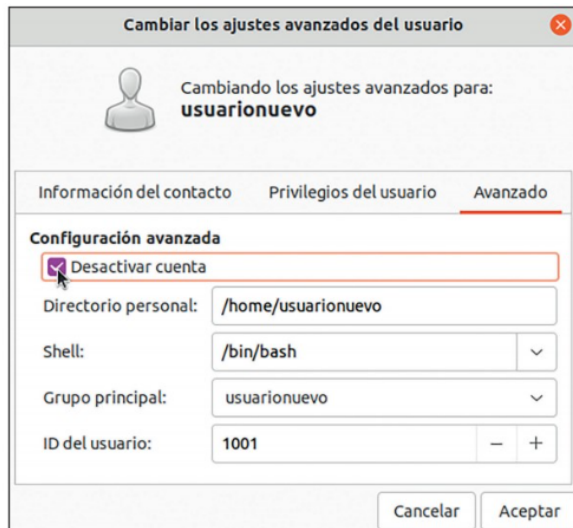
*Figura 3.22. Ventana para gestionar los grupos, donde pueden añadirse, eliminarse o consultar sus propiedades.*



## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos

### ■■■ Gestión en el entorno gráfico



*Figura 3.23. Desactivación de la cuenta de un usuario. El usuario no podrá volver a iniciar sesión hasta que no se le active de nuevo.*

También se puede desactivar la cuenta del usuario marcando sobre **Desactivar cuenta** y después seleccionando **Aceptar**. El efecto será modificar el campo de la contraseña en el fichero `/etc/shadow` añadiéndole el carácter de exclamación **!** al inicio del campo.

## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos Comandos relacionados con la gestión de usuarios y grupos

#### adduser

Añade un usuario al sistema. También se puede utilizar para añadir un usuario a un grupo existente.

Sintaxis:

```
adduser [opciones]... usuario
adduser [opciones]... usuario grupo
```

Opciones:

`--system`

Crea un usuario del sistema.

`--home DIR`

Crea el directorio personal donde se indique en *DIR*.

`--shell SHELL`

La *shell* del usuario predeterminada será la indicada en *SHELL*.

`--no-create-home`

No crea directorio personal al usuario.

`--uid ID`

El UID del usuario será el indicado en *ID*.

`--ingroup GROUP` | `--gid ID`

Especifica el grupo primario del usuario, que se puede indicar mediante el nombre del grupo en *GROUP* o mediante su GID en *ID*.

Ejemplos:

```
sudo adduser usuarioNuevo
```

Crea un usuario llamado **usuarioNuevo**.

```
sudo adduser --system usuariosistema
```

Crea un usuario del sistema.

```
sudo adduser --uid 1010 usuario2
```

Crea un usuario llamado **usuario2** con el UID **1010**.

```
sudo adduser --home /home/claseA/alumno1 alumno1
```

Crea un usuario llamado **alumno1** y crea el directorio personal **/home/claseA/alumno1** para ese usuario.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Comandos relacionados con la gestión de usuarios y grupos

#### addgroup

Añade un grupo al sistema.

Sintaxis:

```
addgroup [opciones]... grupo
```

Opciones:

`--system`

Añade un grupo del sistema.

`--gid ID`

El GID del grupo será el indicado en *ID*.

Ejemplos:

```
sudo addgroup gruponuevo
```

Crea el grupo **gruponuevo**.

```
sudo adduser usuarionuevo gruponuevo
```

Añade un usuario al grupo.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Comandos relacionados con la gestión de usuarios y grupos

`deluser`

Elimina un usuario del sistema.

Sintaxis:

`deluser [opciones] usuario`

Opciones:

`--remove-home`

Elimina el directorio personal del usuario eliminado.

`--remove-all-files`

Elimina todos los ficheros del sistema que pertenezcan a ese usuario.

Ejemplo:

`sudo deluser --remove-home usuariounuevo` Borra el usuario y su directorio personal.

## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos    Comandos relacionados con la gestión de usuarios y grupos

`delgroup`

Elimina un grupo de usuarios.

Sintaxis:

```
delgroup [opciones] grupo
```

Opciones:

`--only-if-empty`

Elimina el grupo solo si no tiene ningún usuario que pertenezca a él.

Ejemplo:

```
sudo delgroup --only-if-empty usuario
```

Muestra el mensaje de que el grupo **usuario** aún tiene al usuario **usuario** como grupo primario y no lo borra.

# 3.3. Gestión de usuarios y grupos locales

## 3.3.1. Usuarios y grupos Comandos relacionados con la gestión de usuarios y grupos

### usermod

Modifica la cuenta de un usuario.

Sintaxis:

```
usermod [opciones] usuario
```

Opciones:

<code>-d, --home HOME_DIR</code>	Cambia el directorio personal del usuario.
<code>-m, --move-home</code>	Mueve el contenido del directorio personal al nuevo.
<code>-a, --append</code>	Añade el usuario a los grupos que se indique con <code>-G</code> .
<code>-G, --groups GRUPOS...</code>	Lista de grupos separados por comas.
<code>-l, --login NEW_LOGIN</code>	Cambia el nombre del usuario.
<code>-s, --shell SHELL</code>	Cambia la <i>shell</i> de inicio del usuario.
<code>-L, --lock NOMBRE</code>	Bloquea la cuenta de usuario añadiendo <code>!</code> al inicio de su campo de contraseña en el fichero <code>/etc/shadow</code> .
<code>-U, --unlock NOMBRE</code>	Desbloquea la cuenta de usuario.

Ejemplos:

```
sudo usermod usuario2 -l alumno2
```

 Cambia el nombre de **usuario2** a **alumno2**.

```
sudo usermod alumno2 -d /home/claseA/alumno2
```

Cambia el directorio personal de **alumno2** a `/home/claseA/alumno2` y mueve los ficheros que tuviese en el directorio anterior al nuevo.

```
sudo usermod -a -G sudo,sambashare alumno2
```

Añade el usuario **alumno2** a los grupos **sudo** y **sambashare** como grupos secundarios.

## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos

#### Comandos relacionados con la gestión de usuarios y grupos

##### groupmod

Modifica un grupo.

Sintaxis:

```
groupmod [opciones] grupo
```

Opciones:

`-g, --gid GID`

Modifica el GID del grupo.

`-n, --new-name nuevo_grupo`

Modifica el nombre del grupo.

##### chsh

Cambia la *shell* de inicio del usuario.

Sintaxis:

```
chsh [-s shell] [usuario]
```

Opciones:

`-s shell`

Cambia la *shell* por la que se indique en esta opción.

Ejemplo:

```
chsh -s /bin/sh usuario
```

# 3.3. Gestión de usuarios y grupos locales

## 3.3.1. Usuarios y grupos    Comandos relacionados con la gestión de usuarios y grupos

`id`

Muestra información sobre el usuario con su UID y los grupos del usuario con su GID. Con las opciones `-un` ofrece la misma información que el comando `whoami`.

Sintaxis:

```
id [opciones]... [usuario]...
```

Opciones:

<code>-g, --group</code>	Muestra solo el grupo principal.
<code>-G, --groups</code>	Muestra los GID de los grupos a los que pertenece.
<code>-u, --user</code>	Muestra el UID.
<code>-n, --name</code>	Muestra el nombre en vez de los números.

Ejemplo:

<code>id -un</code>	Muestra el nombre del usuario que ejecuta el comando.
<code>id -u</code>	Muestra el UID del usuario que ejecuta el comando.



## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos    Comandos relacionados con la gestión de usuarios y grupos

#### groups

Muestra los grupos a los que pertenece el usuario. Si no se especifica ningún usuario muestra la información sobre el usuario que ejecuta el comando.

Sintaxis:

```
groups [opciones]... [usuario]...
```

#### chown

Cambia el propietario y el grupo de uno o varios archivos.

Sintaxis:

```
chown [opciones]... [propietario[:][grupo]] fichero...
```

Opciones:

**-R, --recursive**    Cambia los subdirectorios de forma recursiva.

Ejemplo:

```
chown usuario fichero.txt
```

Cambia el propietario a **fichero.txt**.

```
chown usuario:grupo fichero.txt
```

Cambia el propietario y el grupo.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Comandos relacionados con la gestión de usuarios y grupos

`chgrp`

Cambia el grupo de uno o varios archivos.

Sintaxis:

```
chgrp [opciones]... grupo fichero...
```

Opciones:

`-R, --recursive` Cambia los subdirectorios de forma recursiva.

Ejemplo:

```
chgrp --recursive grupo ~/trabajos
```

Cambia el grupo de la carpeta **trabajos** y todas las subcarpetas.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos

### ■■■ Seguridad en el sistema y en las contraseñas

Se pueden establecer ciertas restricciones y atributos a las contraseñas directamente en el fichero `/etc/login.defs`, o bien utilizar **PAM** (*Pluggable Authentication Modules*, módulos de autenticación conectables), que es una librería para gestionar la autenticación en el sistema de forma flexible y centralizada. En `/etc/pam.d/common-password` se recogen las reglas que se aplican en las contraseñas.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Seguridad en el sistema y en las contraseñas

En el fichero `/etc/security/pwquality.conf` se puede configurar la política de contraseñas para exigir unos requisitos de mayor complejidad. Cada línea del fichero está comentada, es decir, empieza por el carácter `#`. Al descomentarla se utilizará esa restricción. Algunas de las restricciones que se pueden configurar son las siguientes:

- **difok** (número de caracteres diferentes a la contraseña anterior).
- **minlen** (longitud mínima de la cadena).
- **ucrcdit** (número mínimo, si es negativo, o máximo de letras mayúsculas).
- **lccredit** (número mínimo, si es negativo, o máximo de letras minúsculas).
- **dcrcdit** (número mínimo, si es negativo, o máximo de dígitos).
- **maxrepeat** (número máximo de veces que se puede repetir un solo carácter).
- **retry** (máximo número de veces que se puede intentar acceder).

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Seguridad en el sistema y en las contraseñas

El módulo **pam\_pwquality** se encarga de controlar estos requisitos. Si no está instalado, es posible instalarlo junto con el paquete de herramientas siguiente:

```
sudo apt install libpam-pwquality libpwquality-tools -y
```

El fichero **/etc/pam.d/common-password** debe contener la siguiente línea:

```
password    requisite    pam_pwquality.so retry=3 (aquí se pueden añadir también  
                                las restricciones).
```

Con la aplicación **pwscore** se puede comprobar previamente la robustez y la validez de la contraseña.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Ficheros de configuración

Los ficheros de configuración se encuentran repartidos en varios lugares de la estructura del sistema y contienen información necesaria para la configuración del sistema operativo. A través de estos ficheros se puede modificar el comportamiento del sistema.

#### **/etc/login.defs**

Este fichero contiene los valores predeterminados que tendrá el usuario nuevo, como el método de cifrado de la contraseña (ENCRYPT\_METHOD SHA512), la máscara predeterminada (UMASK 022), los permisos de los directorios personales de los usuarios (HOME\_MODE 0750) y el número de intentos permitidos (LOGIN\_RETRIES 5), entre otros parámetros.



## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos      Ficheros de configuración

`/etc/passwd`

En cada una de las líneas de este fichero se encuentra información sobre los usuarios del sistema. La información de cada usuario se organiza en varios campos separados por el carácter de los dos puntos (:). Cada línea del fichero tiene la siguiente estructura:

login:x:UID:GID:información:directorio_personal:shell_de_inicio						
1	2	3	4	5	6	7

- 1: nombre del usuario que utiliza para acceder al sistema.
- 2: una x indica que hay una contraseña encriptada en el fichero `/etc/shadow`.
- 3, 4: identificadores del usuario y del grupo principal del usuario.
- 5: información sobre el usuario (campos GECOS).
- 6: directorio personal del usuario, donde tiene los permisos.
- 7: *shell* que se ejecutará por defecto cuando el usuario inicie la sesión.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Ficheros de configuración

#### /etc/shadow

Fichero que contiene información sobre la contraseña de cada usuario, así como la contraseña cifrada. Este fichero no debe poder ser accesible por los usuarios que no sean administradores o *root*, por motivos de seguridad. Cada línea contiene información sobre la contraseña de cada usuario en 9 campos separados por el carácter de los dos puntos (:):

```
login:$6$xxxx...:999999:0:99999:9:::
```

La información que contiene es el nombre del usuario, la contraseña cifrada con el método de cifrado que se indique en el fichero **login.defs** (si empieza por \$6\$ estará codificada en SHA512) y diversa información sobre la fecha del último cambio de la contraseña, el tiempo que hay que esperar antes de cambiarla, la antigüedad máxima permitida, advertencias sobre el cambio, advertencias sobre inactividad y el tiempo que queda para que expire la contraseña.



## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Ficheros de configuración

#### **/etc/group**

En cada una de las líneas de este fichero se encuentra información sobre los grupos definidos en el sistema. Los usuarios deben pertenecer a un grupo primario o principal y además pueden pertenecer a otros llamados grupos secundarios. El grupo principal de cada usuario es el grupo cuyo GID viene en el fichero **/etc/passwd**. Cada línea del fichero tiene la siguiente estructura formada por el nombre del grupo, la **x**, que hace referencia a la contraseña del grupo en el fichero **/etc/gshadow**, el GID del grupo y una lista separada por comas de los nombres de los usuarios que pertenezcan a este grupo, pero que no sea su grupo primario, es decir, los usuarios que lo tengan como grupo secundario.

***grupo:x:GID:usuarios***

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Ficheros de configuración

#### **/etc/gshadow**

Fichero donde se guardan las contraseñas de los grupos del sistema. Aunque las contraseñas no se utilicen para los grupos, es necesario el fichero para proteger el grupo. Al igual que **shadow**, solo **root** tiene permiso de lectura sobre el fichero. Cada línea del fichero tiene la siguiente estructura formada por el nombre del grupo, la contraseña, la lista separada por comas de los usuarios administradores del grupo y la lista separada por comas de los demás miembros del grupo:

```
nombre:contraseña:administradores:miembros
```

#### **/etc/deluser.conf**

Fichero que contiene la configuración con los parámetros predeterminados cuando se utilizan los comandos **deluser** y **delgroup**.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Ficheros de configuración

#### **/etc/adduser.conf**

Fichero que contiene la configuración con los parámetros predeterminados cuando se utilizan los comandos `adduser` y `addgroup`. Por ejemplo, `DSHELL=/bin/bash` (shell por defecto), `DHOME=/home` (directorio predeterminado que contendrá los directorios personales de los usuarios), `SKEL=/etc/skel` (directorio `skel` predeterminado), o los primeros y últimos UID y GID por defecto de los usuarios del sistema y de las cuentas usuarios.

#### **/etc/skel**

Este directorio tiene el contenido del directorio de los usuarios que se añadan al sistema. Al crear un usuario nuevo, se le copia el contenido de este directorio en su carpeta personal, de manera que cualquier fichero o carpeta que se añada a este directorio se añadirá a los directorios personales de los usuarios que se añadan al sistema a partir de ese momento.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Ficheros de configuración

#### `/etc/shells`

Contiene la ruta de las *shells* o intérpretes de comandos válidos. Puede tener los siguientes o algunos más que se hayan instalado:

- `/bin/sh` Bourne **Shell** es la *shell* disponible desde UNIX.
- `/bin/bash` Bourne-**Again Shell** es la *shell* que suele venir por defecto y se diseñó como reemplazo de la anterior.
- `/bin/rbash` Restricted **bash** es una *shell* más restringida que la anterior, a la que para hacerla más segura se le quitan características como poder cambiar el directorio, las redirecciones, las variables de entorno, etcétera.
- `/bin/dash` Debian Almquist **Shell** es una *shell* compatible con `sh` que es más rápida que `bash` al ser más pequeña y consumir menos recursos.

Si se da el caso de que un usuario no tiene una *shell* válida o tiene de *shell* `/bin/false` o `/usr/sbin/nologin`, será un usuario que no podrá iniciar sesión en el sistema.

## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Cambiar de usuario o ejecutar comandos con privilegios de otro usuario

`su`

Cambia de usuario. Si no se indica nada entra como usuario *root*. Antes de iniciar la sesión como el usuario que se indique habrá que escribir su contraseña correctamente.

Sintaxis:

```
su [-l, --login, -] [usuario]
```

Opciones:

`-`, `-l`, `--login`

Ejecuta los *scripts* de inicio de sesión del usuario.

Ejemplos:

```
su
```

Inicia sesión como usuario *root*.

```
su -l
```

Inicia sesión como usuario *root* ejecutando los *scripts* de inicio de sesión de *root*.

```
su -l usuario2
```

Inicia sesión como usuario **usuario2** ejecutando los *scripts* de inicio de sesión.

## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos

Cambiar de usuario o ejecutar comandos con privilegios de otro usuario

#### sudo

Permite ejecutar comandos con permisos o privilegios del usuario *root* o superusuario, por defecto, o por otro usuario que se especifique. Previamente el usuario deberá estar configurado en el fichero **/etc/sudoers** como usuario que puede tener privilegios de *root*, o bien pertenecer al grupo **sudo**, ya que en ese fichero se indica que un usuario que pertenezca a ese grupo tendrá todos los privilegios.

El ejecutar un comando con **sudo** solicita la clave del usuario antes de ejecutarlo, como medida de seguridad. Después se puede seguir utilizándolo sin que vuelva a pedir la clave durante un tiempo. También es posible configurar el fichero **/etc/sudoers** para poder ejecutar comandos con **sudo** y que no pida la clave.

Sintaxis:

```
sudo [-u usuario] [-i | --login] [comando]
sudo -e [-u usuario] fichero
sudo [-l | --list]
```

# 3.3. Gestión de usuarios y grupos locales

## 3.3.1. Usuarios y grupos

### Cambiar de usuario o ejecutar comandos con privilegios de otro usuario

#### sudo

Sintaxis:

```
sudo [-u usuario] [-i | --login] [comando]
sudo -e [-u usuario] fichero
sudo [-l | --list]
```

Opciones:

`-i, --login`

Ejecuta los *scripts* de inicio de sesión del usuario. Si no se indica ningún comando abre la terminal como el usuario que se indique o como *root* (sería similar a escribir `su -l`).

`-l, --list`

Si no se indica comando muestra qué tiene permitido hacer el usuario.

`-u <usuario>, --user=<usuario>`

Realiza la acción como el usuario indicado en vez de como superusuario o *root*.

`-e, --edit`

Edita un fichero con privilegios de *root* o del usuario especificado.

Ejemplos:

```
sudo -i
sudo -e /etc/passwd
sudo --list

sudo -u usuario2 whoami
```

Inicia sesión como *root* y ejecuta sus scripts de inicio.

Edita el fichero `/etc/passwd` con privilegios de superusuario. Muestra los comandos que tiene permitidos y prohibidos el usuario.

Muestra por pantalla usuario2 porque se está ejecutando el comando `whoami` como **usuario2**.

# 3.3. Gestión de usuarios y grupos locales

## 3.3.1. Usuarios y grupos

### Cambiar de usuario o ejecutar comandos con privilegios de otro usuario

#### visudo

Editor para el contenido del fichero `/etc/sudoers`. La primera vez que se use preguntará qué editor se quiere utilizar y recomienda abrirlo con **nano**. Este fichero suele tener las siguientes líneas, entre otras:

```
root ALL=(ALL:ALL) ALL    Indica que el usuario root puede ejecutar cualquier comando,
                           como cualquier usuario y grupo y desde cualquier equipo, es
                           decir, tiene todos los privilegios.

%sudo ALL=(ALL:ALL) ALL    Indica que los usuarios del grupo sudo pueden tener todos
                           los privilegios de root (cuando se utilice el comando sudo). Se
                           indica que es un grupo por el carácter % al inicio de la línea.
```

El significado de cada línea sería el siguiente:

```
usuario hosts=(usuarios:grupos) comandos
%grupo hosts=(usuarios:grupos) comandos
```

Donde **usuario** o **%grupo** indica el usuario o el grupo respectivamente al que se le va a dar permiso para poder ejecutar el comando **sudo**; **hosts** indica los equipos permitidos desde los que puede acceder (se puede utilizar una lista separada por comas de nombres de equipos, direcciones IP, redes o bien **ALL** para indicar desde todos los equipos); (**usuarios:grupos**) son las listas separadas por comas de usuarios o grupos que se pueden utilizar para ejecutar comandos en su nombre o bien **ALL** para indicar todos; y, finalmente, **comandos** indica una lista de comandos que pueden ejecutarse o bien **ALL** para indicar todos los comandos. Para especificar las listas de usuarios, equipos y comandos se pueden crear alias de diferentes tipos, como **User\_Alias** (usuarios), **Runas\_Alias** (ejecutar como un usuario y grupo), **Host\_Alias** (equipos) y **Cmnd\_Alias** (comandos). Por ejemplo:

```
User_Alias    USUARIOS = usuario1, usuario2, usuario3
```



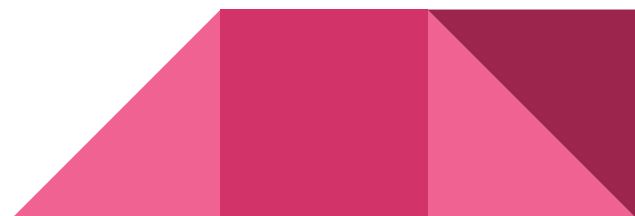
## ■ 3.3. Gestión de usuarios y grupos locales

### ■■ 3.3.1. Usuarios y grupos ■■■ Directorio personal del usuario e inicio de sesión

Cada usuario en el sistema tiene asignado un directorio personal al que accede por defecto al iniciar sesión. Este directorio se crea por defecto al crear el usuario, a menos que se indique lo contrario dentro del directorio **/home**.

`/home/<nombre_usuario>`

donde **<nombre\_usuario>** será el nombre que cada usuario tendrá y que utilizará para iniciar sesión en el sistema.



## 3.3. Gestión de usuarios y grupos locales

### 3.3.1. Usuarios y grupos      Directorio personal del usuario e inicio de sesión

El usuario *root* tiene su directorio personal en `/root`.

Al entrar el usuario en el sistema se ejecutan una serie de *scripts* de inicio de sesión. Existen *scripts* que se ejecutarán cada vez que se inicie el sistema y otros cada vez que un usuario inicie su sesión de alguna de estas formas:

```
su -  
su -l  
su -login
```

Para entrar como usuario *root* desde la cuenta de otro usuario si no se conoce la contraseña de *root* pero el usuario pertenece al grupo **sudo**, se puede escribir en una terminal lo siguiente:

```
sudo su    o    sudo -l
```

En este caso el sistema preguntará por la contraseña del usuario que ejecuta el comando `sudo` (no la de *root*) y a continuación se iniciará sesión como usuario *root*. Es una forma de poder acceder como usuario *root* sin necesidad de saber la contraseña de este, por lo que hay que tener precaución con los usuarios a los que se les permite usar el comando `sudo`.



# Realitzar Practica 2 y 3



# UD3 – LINUX – ADMINISTRACIÓ I CONFIGURACIÓ-II

1º DAW - CFGS

Prof. Manuel Enguidanos  
*[menguidanos@fpmislata.com](mailto:menguidanos@fpmislata.com)*