



# GESTIÓN DE USUARIOS

Laboratorio de Sistemas Operativos II



*GNU/Linux es un sistema operativo multiusuario y multitarea, esto significa que un **usuario** puede trabajar en simultáneo con otros, ejecutando una o más tareas a la vez.*

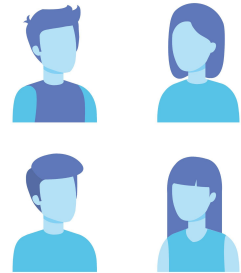


# Gestión de usuarios

La gestión de usuarios es la tarea de definir un perfil de privilegios para quienes operan con un sistema multiusuario. Incluye crear, modificar privilegios, asignar permisos y eliminar usuarios.

# Usuarios

- ▷ Pueden corresponder a personas o programas que hacen uso del sistema.
- ▷ Cada usuario del sistema tiene una cuenta asignada.
- ▷ Las cuentas se usan para identificar unívocamente a los usuarios del sistema.



# Cuenta de usuario



- ▷ Conjunto de información que indica al S.O. el tipo de usuario, los accesos permitidos, los privilegios y permisos en general.
- ▷ Se identifica con el nombre de usuario y contraseña
- ▷ Los usuarios se comunican con el sistema a través de una “interfaz de usuario”
- ▷ Proceso de conexión al sistema o **login**
- ▷ Proceso de desconexión al sistema o **logout**

# Usuarios en GNU/Linux

- ▷ Los usuarios están reunidos en grupos de acuerdo a un propósito común. Los grupos son expresiones lógicas de organización.
- ▷ Los usuarios tienen
  - Identificación única (User ID): **UID**
  - Grupo principal de usuario (Group ID): **GID**
- ▷ Un usuario puede pertenecer a varios grupos, además de su principal.

# Tipos de usuarios en GNU/Linux

 **root**

Superusuario o administrador del sistema operativo

 **especiales o de servicio**

Corresponden a cuentas del sistema operativo

 **normales**

Corresponden a personas físicas

# root

- ▷ UID = 0
- ▷ Tiene privilegios sobre todo el sistema.
- ▷ Acceso total a todos los archivos y directorios con independencia de propietarios y permisos.
- ▷ Gestiona cuentas de usuarios
- ▷ Ejecuta tareas de mantenimiento
- ▷ Puede detener el sistema
- ▷ Puede instalar software
- ▷ Puede modificar el kernel



**root@server: /#**



# Usuarios especiales

- ▷ UID entre 1 y 999 (en /etc/login.defs)
- ▷ Ejemplos: bin, daemon, adm, lp, sync, shutdown, mail, squid, apache, etc.
- ▷ Asumen distintos privilegios de root, no todos para proteger.
- ▷ No tienen contraseñas, no están diseñadas para iniciar sesiones (nologin).
- ▷ Muchas se crean durante de la instalación de Linux o de la aplicación.



# Usuarios normales

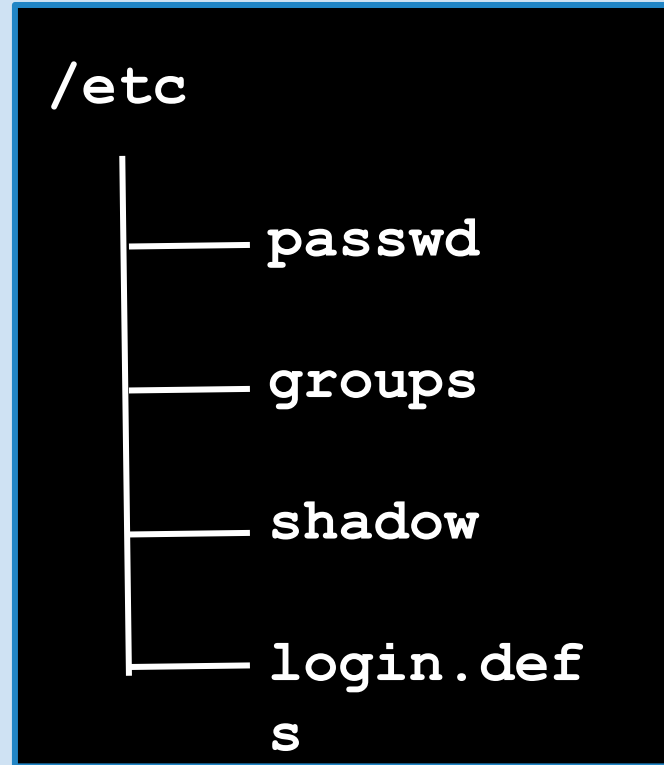
- ▶ UID desde 1000 (en /etc/login.defs)
- ▶ Se usan para usuarios individuales.
- ▶ Cada usuario dispone de un directorio de trabajo, ubicado generalmente en /home.
- ▶ Cada usuario puede personalizar su entorno de trabajo.
- ▶ Tienen solo privilegios completos en su directorio de trabajo o HOME.



**usuario@server:~\$**

# Archivos de configuración importantes

- `/etc/passwd`
- `/etc/groups`
- `/etc/shadow`
- `/etc/login.defs`



# /etc/passwd

- ▷ Todos los tipos de usuario tiene su cuenta definida en este archivo.
- ▷ Es de texto tipo ASCII, se crea durante la instalación con root y las cuentas especiales, y otros usuarios normales indicados.
- ▷ Contiene una línea para cada usuario y se actualiza a medida que se crean, modifican o eliminan usuarios.
- ▷ Las líneas tienen el formato siguiente, con 7 campos separados por el símbolo :

```
root:x:0:0:root:/root:/bin/bash
```

```
sergio:x:501:500:Sergio González:/home/sergio:/bin/bash
```

# Campos de /etc/passwd

<b>Campo 1</b>	Es el nombre del usuario, identificador de inicio de sesión (login). Único.
<b>Campo 2</b>	La 'x' indica la contraseña encriptada del usuario, además también indica que se está haciendo uso del archivo /etc/shadow, si no se hace uso de este archivo, este campo se vería algo así como: 'ghy675gjuXCc12r5gt78uuu6R'.
<b>Campo 3</b>	Número de identificación del usuario (UID). único.
<b>Campo 4</b>	Numeración de identificación del grupo (GID). Puede repetirse.
<b>Campo 5</b>	Comentarios o el nombre completo del usuario.
<b>Campo 6</b>	Directorio de trabajo (Home) donde se sitúa al usuario después del login.
<b>Campo 7</b>	Shell que va a utilizar el usuario de forma predeterminada.

# /etc/group

- ▷ Es un archivo de texto ASCII que guarda información de los grupos a los que pertenecen los usuarios del sistema.
- ▷ Contiene una línea para cada usuario con tres o cuatro campos por usuario:

```
nombre_grupo:contraseña:GID:lista_usuarios
```

# Campos de /etc/group

<b>Campo 1</b>	Nombre del grupo
<b>Campo 2</b>	Contraseña: del grupo (encriptada). Si este campo está vacío, no se utiliza ninguna contraseña.
<b>Campo 3</b>	Número de identificación del grupo (GID). único.
<b>Campo 4</b>	Lista de nombres de usuarios de todos los miembros del grupo, separados por comas.

# /etc/shadow

- ▷ Antes las contraseñas cifradas se almacenaban en el mismo `/etc/passwd`. El problema es que 'passwd' es un archivo que puede ser leído por cualquier usuario del sistema, aunque solo puede ser modificado por root.
- ▷ El archivo 'shadow' fue creado para resolver el problema, ya que solo puede ser leído y modificado por root.
- ▷ Almacena la contraseña encriptada de cada usuario y tiene otros campos de control de contraseñas.



# Campos de /etc/shadow

root:\$6\$RSX9ggySG4XhWqS35kkjDQF7p.HhN0:17399:0:99999:7:::

prueba:\$6\$3ZXePzr2U9z7KGWgMwCD7OZMSDHzb1:18385:0:15:7::18503:

Campo 1	Nombre de la cuenta del usuario.
Campo 2	Contraseña cifrada o encriptada, un '*' indica cuenta de 'nologin'.
Campo 3	Días transcurridos desde el 1/ene/1970 hasta la fecha en que la contraseña fue cambiada por última vez.
Campo 4	Número de días que deben transcurrir hasta que la contraseña se pueda volver a cambiar.
Campo 5	Número de días tras los cuales hay que cambiar la contraseña. (-1 significa nunca). A partir de este dato se obtiene la fecha de expiración de la contraseña.
Campo 6	Número de días antes de la expiración de la contraseña en que se le avisará al usuario al inicio de la sesión.
Campo 7	Días después de la expiración en que la contraseña se inhabilitara, si es que no se cambio.
Campo 8	Fecha de caducidad de la cuenta. Se expresa en días transcurridos desde el 1/Enero/1970 (epoch).
Campo 9	Reservado.

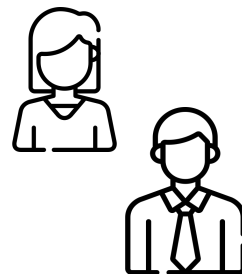
# /etc/login.defs

- ▷ Están definidas las variables que controlan los aspectos de la creación de usuarios y de los campos de shadow usada por defecto. Algunos son:
  - Número máximo de días que una contraseña es válida **PASS\_MAX\_DAYS**
  - El número mínimo de caracteres en la contraseña **PASS\_MIN\_LEN**
  - Valor mínimo para usuarios normales cuando se usa useradd **UID\_MIN**
- ▷ El valor umask por defecto **UMASK**
  - Si el comando useradd crea el directorio home por defecto **CREATE\_HOME**
- ▷ Lo definido se usará al momento de crear o modificar usuarios.

# USUARIOS Y GRUPOS

## Herramientas para gestionarlos

# Comando adduser (ver man)



- ▶ Crear un usuario nuevo

```
#adduser usuario
```

- ▶ Agregar un usuario existente a un grupo existente

```
#adduser usuario grupo
```

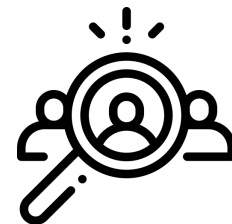
- ▶ Agregar usuario nuevo con UID = 1050

```
#adduser usuario --uid nro_id
```

- ▶ Otorgar privilegios de root a un usuario existente

```
#adduser usuario sudo
```

# Otras operaciones de usuarios



- ▷ Ver información de un usuario

```
#id usuario
```

```
#lslogins usuario
```

```
#finger usuario      (instalar finger)
```

- ▷ Eliminar un usuario

```
#userdel usuario
```

- ▷ Eliminar un usuario y sus archivos asociados

```
#userdel -rf usuario
```

# Comando usermod

- ▷ Cambiar el directorio personal de un usuario y mover su contenido

```
#usermod -d nuevodir -m usuario
```

- ▷ Cambiar grupo principal de un usuario

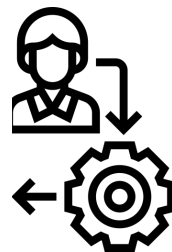
```
#usermod -g nuevogruppo usuario
```

- ▷ Cambiar nombre de usuario

```
#usermod -l nuevonombre usuario
```

- ▷ Bloquear la cuenta de un usuario

```
#usermod -L usuario
```



# Gestión de claves de usuario

- ▷ Modificar/asignar clave a un usuario (¡cuidado!)

```
#passwd usuario
```

- ▷ Ver información de claves de un usuario

```
#chage -l usuario
```

- ▷ Cambiar fecha de expiración de clave de un usuario

```
#chage -E AAAA-MM-DD usuario
```

- ▷ Obligar a cambiar la clave en el próximo login

```
#chage -d 0 usuario
```

# Gestión de grupos



- ▷ Crear un grupo nuevo

```
#addgroup grupo
```

- ▷ Eliminar un grupo

```
#groupdel grupo
```

- ▷ Modificar atributos de grupos, por ejemplo cambiar su nombre

```
#groupmod -n nuevogrupo grupo
```



# PERMISOS

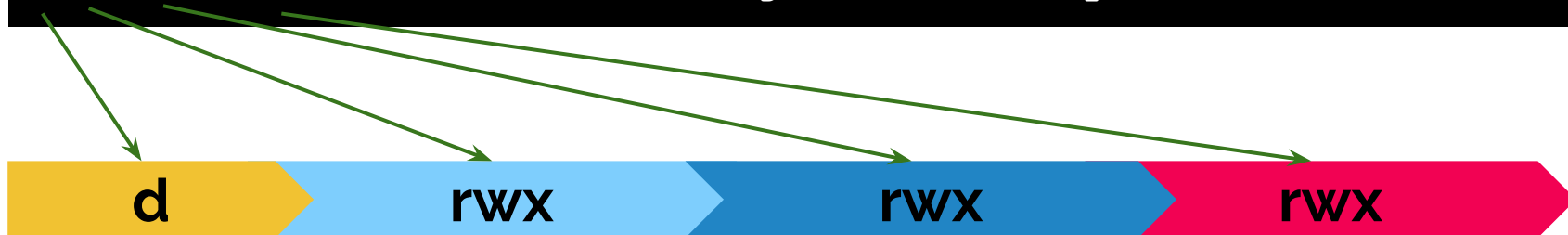
Herramientas para gestionarlos

# Permisos en GNU/Linux



# VER PERMISOS: #ls -l

```
root@nuna:~# ls -l /etc/apt
drwxr-xr-x 2 root root 4096 abr 14 2019 apt.conf.d
-rw-r--r-- 1 root root 104 jun 26 2017 listchanges.conf
drwxr-xr-x 2 root root 4096 jun 1 2017 preferences.d
```



## Tipo de archivo

d: directorio

- : artchivo

l : enlace

## Permisos de

usuario o dueño.

Un guión es la

ausencia del

permiso.

## Permisos de

grupo. Un guión

es la ausencia del

permiso.

## Permisos de otros

usuarios. No incluye

dueño ni grupo. Un

guión es la ausencia

del permiso.

# Gestión de Permisos con chmod

## ▷ Sintaxis

`#chmod a-quien operación permisos archivos`

## ▷ Ejemplos:

- Añade a **u**usuario dueño y **g**grupo el permiso de lectura sobre el archivo carta

`#chmod ug+r /home/alumno/carta`

- Añade permiso de ejecución a todos los usuarios del sistema (**a**= all)

`#chmod a+x /opt/programa.sh`

# Chmod en formato octal

## ▷ Valor de permisos

**Lectura = 4    //    Escritura = 2    //    Ejecución = 1**

## ▷ Ejemplos:

- Asigna a **u**usuario dueño y **g**grupo el permiso de lectura y elimina todos los permisos de los **o**tros usuarios sobre el archivo carta
- Asigna todos los permisos al **u**usuario dueño y al **g**grupo, y el permiso de lectura y ejecución a los **o**tros usuarios.

```
#chmod 440 /home/alumno/carta
```

```
#chmod 775 /opt/programa.sh
```

# ¡Gracias!

## ¿Preguntas?

Referencias:

[https://www.linuxtotal.com.mx/index.php?cont=info\\_admon\\_008](https://www.linuxtotal.com.mx/index.php?cont=info_admon_008)

<https://rm-rf.es/>