Gestión de Usuarios y Grupos.

En Linux, un usuario puede representar tanto a una persona (usuario real) como a una entidad encargada de gestionar un servicio o aplicación (usuario lógico). Cada usuario definido en el sistema se asocia con un identificador único (UID) y una cuenta que almacena sus datos personales en una zona reservada del disco. Los usuarios cuentan con restricciones específicas que les impiden ejecutar comandos que puedan comprometer la integridad del sistema, alterar su configuración de manera accidental o afectar servicios en segundo plano, así como los permisos y ubicaciones de archivos y directorios del sistema. Solo el usuario root dispone de privilegios sin restricciones para gestionar el sistema en su totalidad.

Un grupo, por su parte, es una estructura lógica identificada por un nombre y un identificador único (GID). Sirve para agrupar múltiples cuentas con un propósito común, permitiéndoles compartir los mismos permisos de acceso a ciertos recursos. Toda cuenta debe pertenecer al menos a un grupo, conocido como su grupo primario. Aunque un sistema pueda tener un único usuario, es crucial evitar utilizar la cuenta root para tareas diarias; esta cuenta debe reservarse exclusivamente para actividades administrativas.

Características principales de una cuenta de usuario:

1. Identificación: Tiene un nombre y un UID únicos en el sistema.
2. Pertenencia: Forma parte de un grupo primario y puede pertenecer a otros grupos adicionales.
3. Información asociada: Puede incluir datos relevantes sobre el propietario de la cuenta.
4. Directorio personal: Cada usuario dispone de un directorio personal para almacenar sus datos.
5. Intérprete de comandos: Está asociado a un shell que permite ejecutar aplicaciones y utilidades del sistema operativo.
6. Seguridad: Requiere una contraseña robusta y difícil de adivinar.
7. Entorno personalizado: Posee un perfil de entrada que define las características iniciales de su entorno operativo.
8. Control de acceso: Puede incluir una fecha de caducidad para la cuenta.
9. Cuotas de disco: Es posible asignar límites de uso de disco por sistema de archivos.
10. Auditoría: Se pueden habilitar sistemas que registren las actividades del usuario.

Linux ofrece múltiples métodos para gestionar usuarios que acceden al sistema. El enfoque más común es definir las cuentas y grupos localmente en cada servidor. Sin embargo, también es posible implementar sistemas de autenticación externos que permitan compartir configuraciones de usuarios entre varias máquinas.

Archivos clave en la gestión de usuarios y grupos:

`/etc/passwd`

Contiene la descripción básica de los usuarios locales, incluyendo:

Nombre de usuario. UID y GID. Descripción del usuario. Directorio personal. Shell predeterminado. /etc/shadow Fichero oculto que gestiona las contraseñas y restricciones, como:

Contraseña cifrada. Fecha de creación. Reglas para cambio de contraseña (frecuencia, aviso, bloqueo, expiración).

`/etc/group`

Define los grupos de usuarios, con:

Nombre del grupo. GID. Miembros del grupo.

`/etc/gshadow`

Fichero oculto y opcional que almacena contraseñas de grupos privados, con campos para:

Nombre del grupo. Contraseña. Administradores y miembros del grupo.

Usuarios y Grupos predefinidos

En todos los sistemas linux existen usuarios y grupos predefinidos por el sistema operativo, que se utilizan para la gestión y el control de los distintos servicios que se ejecutan.

El usuario especial root, tiene el UID 0 y GID 0 es el administrador del equipo con un control total sobre el sistema. Existe también un grupo root, con características administrativas al que pertenece el citado usuario.

En la siguiente tabla se muestra algunos de los usuarios y grupos predefinidos.

Usuario	**UID**	**GID**	**Descripción**
root	0	0	Administrador con control total.
bin	1	1	Propietario de las utilidades del Sistema Operativo
daemon	2	2	Gestor de servicios generales.
adm	3	4	Propietario de los archivos de registros históricos y administrativos
lp	4	7	Administrador de los servicios de impresión.
ftp	14	50	Controlador del acceso al servicio de FTP anónimo.
nobody	99	99	Gestor de servicios varios.
www-data	48	48	Propietario de los ficheros y directorios del Servidor Web.

Los usuarios que gestionan los servicios, deben tener deshabilitada la opción de inicio de sesión, esto se logra asignando /sbin/nologin como el intérprete de comandos de la cuenta de usuario.

Gestión de usuarios

Para la gestión de usuarios se utilizan los siguientes comandos que deben ser ejecutados desde la terminal: `useradd`, `passwd`, `usermod`, `groupmod`.

Para crear una nueva cuenta de usuario, se utiliza el comando `useradd` seguido del nombre del usuario como argumento. Ejemplos:

• Para crear un usuario llamado pedro:

```
# useradd pedro
```

• Crea un usuario llamado teo con el directorio home en /tmp/teo, expira el 31/12/2022

```
# useradd –d /tmp/teo –e 20221231 teo
```

• Crea un nuevo usuario en el grupo admins al usuario raul

```
# useradd –G admins raul
```

• modificar el directorio home del usuario raul a la ruta /nuevo/home moviendo además todo su contenido del home actual.

```
# usermod –d -m /nuevo/home/ raul
```

• Agregar al grupo root al usuario raul

```
# usermod –G root -a raul
```

• Eliminar el usuario ehenry borrando tambien su directorio personal.

```
# userdel –r ehenry
```

• Quitar la contraseña del usuario cornelio

```
# passwd -d cornelio
```

• Crear un nuevo grupo llamado gadminred.

```
# groupadd gadminred
```

• Eliminar del grupo gadminred al usuario ricardo.

```
# gpasswd -d Ricardo gadminred
```

• Cambiar de dueño de archivo al nuevo usuario y grupo `www-data`

```
# mkdir sitioweb
# chown www-data:www-data sitioweb
```