GLOSARIO

- **Background:** ejecución de procesos en segundo plano.
- **Cuantum:** espacio de tiempo asignado a cada proceso para ocupar la CPU.
- **GID:** número de identificación de grupo único en sistemas Linux.
- **Linux-PAM:** sistema centralizado de autenticación de usuarios en Linux.
- **Login:** nombre que se emplea para acceder al sistema operativo.
- **Máscara de permisos:** privilegios de los que dispone el propietario, el grupo y el resto de usuarios sobre un objeto del sistema de archivos en sistemas Linux.
- **Modo kernel en ejecución:** capacidad de ejecución en modo privilegiado sobre el sistema operativo.
- **PCB:** bloque de control del proceso.
- **PID:** identificador del proceso.
- **Proceso:** instancia de un programa en ejecución.
- **Prompt:** línea de petición de órdenes en el intérprete de comandos.
- **Shell:** intérprete de comandos que actúa de interfaz entre el sistema operativo y los usuarios.
- **Superusuario:** usuario con mayor privilegio sobre un sistema Linux.
- **UID:** número de identificación de usuario único en sistemas Linux.

GESTIÓN DE USUARIOS POR LÍNEA DE COMANDO DE LINUX

Los usuarios y grupos de Linux se gestionan a través de los archivos ***/etc/passwd*** y ***/etc/group***, principalmente, además de otros ficheros como ***/etc/sudoers*** o ***/etc/shadow***.

Por usuario administrador en Linux entendemos aquel que tiene capacidad de gestión en el sistema, sin ser necesariamente el superusuario (*root*). Esta capacidad puede ser desarrollada si dispone de privilegios gracias al **comando *sudo*** o si se encuentra en grupos de usuarios con privilegios sobre determinados archivos o comandos de gestión.

El fichero de configuración de grupos ***/etc/group*** centraliza la gestión de grupos en el sistema. Cada usuario ha de pertenecer a un grupo principal (cuarto campo del fichero */etc/passwd*), pero, además, puede pertenecer a varios grupos secundarios, especificándose en */etc/group*.

Los usuarios disponen de ***login*** y ***UID*** únicos y necesarios para identificarse en el sistema y poder operar en él. El ***superusuario***, por defecto, no está habilitado para evitar acciones perjudiciales de manera inconsciente, debido al enorme control que posee sobre el sistema.

El directorio ***/etc/skel*** contiene los archivos de configuración por defecto que se añaden al directorio de trabajo de un usuario cuando este es creado con las opciones adecuadas. En otras palabras, contiene la plantilla de creación de perfiles de usuarios.

COMANDOS:

- ***sudo:*** permite ejecutar comandos en nombre de otros usuarios, siempre que el usuario y el comando que se va a ejecutar estén permitidos gracias al archivo de configuración */etc/sudoers*.
- ***su:*** cambiar de usuario.

- ***useradd:*** crea una nueva entrada en */etc/passwd* y copia todo lo que hay por defecto en el fichero *etc/skel* al directorio de usuario.
- ***userdel:*** eliminar usuario.
- ***usermod:*** modificar usuario.
- ***who:*** ver usuarios conectados.
- ***groupadd:*** añadir nuevo grupo al sistema.
- ***groupdel:*** eliminar un grupo del sistema.
- ***groupmod:*** modificar un grupo del sistema.
- ***adduser:*** añadir un usuario a un grupo.
- ***deluser:*** eliminar un usuario de un grupo.

Grupos predeterminados (***root*** es el más importante):

Grupos	Descripción
adm	Grupo de administración que permite accesos a archivos de registro y comandos como *sudo* y *su*
users	Grupo de usuarios estándar
nobody	Sin privilegios
root	Administración sin restricciones sobre todo el sistema
tty	Aporta privilegios sobre algunos dispositivos, como /dev/tty
lpadmin	Confiere privilegios sobre dispositivos de puerto paralelo

COMANDOS:

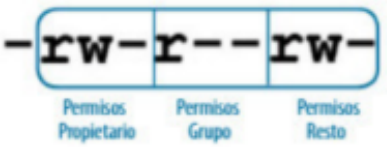
- ***chown:*** modificar el propietario de un archivo.
- ***chgrp:*** modificar el grupo de un archivo.

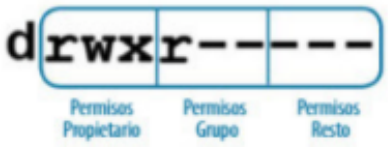
Las contraseñas se guardan en ***/etc/shadow***, del que Linux-PAM hace uso. Cuando se crea un usuario con *useradd*, no se le asigna una contraseña por defecto y tampoco se le solicita al usuario en cuestión, por lo que este no puede acceder al sistema. Por ende, un administrador del sistema, el usuario *root* o aquel que disponga de privilegios mediante *sudo*, podrá asignar contraseñas a usuarios.

COMANDOS:

- ***passwd:*** permite cambiar la contraseña ya existente de un usuario o generar una por primera vez. Esta se encripta y se almacena en */etc/shadow*. (Ejemplo: *sudo passwd usuario*).
- ***openssl passwd:*** permite generar contraseñas hash.
- ***chage:*** gestionar y establecer políticas de caducidad de contraseñas, modificando así valores del archivo de configuración */etc/shadow*.

ACCESO A RECURSOS Y PERMISOS LOCALES





Tipos de archivo (primer campo):

- **'-':** archivo regular.
- **'d':** directorio.

Permisos sobre archivos y carpetas

Permisos	Archivos	Carpetas
Permiso de lectura (r)	Puede ser leído o visualizado.	Se puede visualizar su contenido, mostrando los archivos o carpetas que contenga.
Permiso de escritura (w)	Pueden modificar su contenido, sus permisos, el propietario y el grupo.	Permite modificar el contenido, creando o eliminando archivos o carpetas en ella.
Permiso de ejecución (x)	Permite ejecutarlo.	Permite acceder a ella.

Existen unos bits llamados "raros" que se asocian a unos modos especiales:

- ***Set-uid:*** cuando está activo, se simboliza con una **s** en lugar de una **x** en los bits de la máscara de permisos del propietario. Si el archivo no es ejecutable y dispone de *set-uid*, se representará con una **S**.
- ***Set-gid:*** cuando está activo, se simboliza con una **s** en lugar de una **x** en los bits de la máscara de permisos del grupo. Si el archivo o directorio no es ejecutable y dispone de *set-gid*, se representará con una **S**.
- ***Sticky-bit* o bit de permanencia:** cuando está activo, se simboliza con una **t** en lugar de una **x** en los bits de la máscara de permisos del resto de usuarios. Si el archivo o directorio no es ejecutable y dispone de *sticky-bit*, se representará con una **T**.

Tipos de modificación de permisos:

- **Octal:** activando o desactivando cada bit sobre los permisos en binario mediante un 1 o un 0, respectivamente. Una vez obtenido el código en binario, se debe pasar a octal con la máscara de permisos.
- **Simbólico:** es una manera más sencilla de aplicar una máscara de permisos, especialmente al modificarla con relación a su valor actual.

COMANDOS:

- ***chmod:*** para modificar los permisos.
- ***umask:*** modificar permisos por defecto.

GESTIÓN DE USUARIOS POR INTERFAZ GRÁFICA DE WINDOWS

Crear cuentas de administrador, invitado o usuario estándar a través de la interfaz gráfica, incluyendo cuentas administrativas deshabilitadas por defecto.

GESTIÓN DE PROCESOS POR LÍNEA DE COMANDOS DE LINUX

Figura 4.12
Ciclo de vida de un proceso.

COMANDOS de gestión de procesos:

- ***ps***
- ***top***
- ***htop***
- ***kill***

GESTIÓN DE PROCESOS POR INTERFAZ GRÁFICA DE WINDOWS

Administrador de tareas (mirar actividad): herramienta principal para la supervisión y control de procesos, con funcionalidades para finalizar procesos, cambiar prioridades y establecer afinidades de CPU.

AUTOMATIZACIÓN DE TAREAS EN LINUX

- ***at:*** lanzar órdenes en una fecha y hora concretas. Requiere previa instalación (*sudo apt install at*).
- ***batch:*** ejecutar una serie de comandos que se hayan escrito previamente.

RENDIMIENTO DEL SISTEMA

- ***vmstat***

Mirar actividades.

APLICACIONES DE MANTENIMIENTO Y OPTIMIZACIÓN

- **Actualización de Drivers:** uso de aplicaciones como *Drives Cloud* o *Driver Booster* para mantener los drivers actualizados.
- **Backup y Sincronización:** herramientas como *EaseUS Todo Backup Free*, *Clonezilla* y *FreeFileSync* para la creación de copias de seguridad y sincronización de archivos.
- **Antivirus:** importancia de programas antivirus de empresas como *Avira, Panda, Bitdefender, Kaspersky, AVG* o *Avast*.
- **Optimización del Sistema:** uso de herramientas como *CCleaner* y *Stacer* para la limpieza y optimización de sistemas Windows y Linux.