SISTEMAS INFORMÁTICOS UD-4

SISTEMAS OPERATIVOS. GESTION DE USUARIOS Y PROCESOS

GESTIÓN DE USUARIOS Y GRUPOS EN LINUX

ÍNDICE

[INTRODUCCIÓN 3](#_Toc126955578)

[ARCHIVOS Y DIRECTORIOS IMPORTANTES EN LA GESTIÓN DE USUARIOS 3](#_Toc126955579)

[A. ARCHIVO /etc/passwd 3](#_Toc126955580)

[B. ARCHIVO /etc/group 3](#_Toc126955581)

[C. ARCHIVO /etc/shadow 4](#_Toc126955582)

[D. ARCHIVO /etc/gshadow 4](#_Toc126955583)

[E. ARCHIVO /etc/sudoers 5](#_Toc126955584)

[F. DIRECTORIO /etc/skel/ 5](#_Toc126955585)

[G. ARCHIVO /etc/default/useradd 6](#_Toc126955586)

[USUARIO ADMINISTRADOR 6](#_Toc126955587)

[A. SUPERUSUARIO (root) 6](#_Toc126955588)

[B. sudo 7](#_Toc126955589)

[C. su 7](#_Toc126955590)

[USUARIOS Y GRUPOS PREDETERMINADOS 7](#_Toc126955591)

# INTRODUCCIÓN

En Linux se gestionan los usuarios mediante archivos de configuración que son sólo accesibles por usuarios administradores.

# ARCHIVOS Y DIRECTORIOS IMPORTANTES EN LA GESTIÓN DE USUARIOS

## ARCHIVO /etc/passwd

Este archivo almacena las cuentas de los usuarios del sistema.

Texto

Descripción generada automáticamente

Se compone de 7 columnas separadas por “:”:

1. Login de usuario o nombre de acceso al sistema.
2. Password de autenticación (aparece con un valor “x” ya que el valor encriptado se encuentra en el archivo /etc/shadow).
3. UID (User IDentification) o número de identificación de usuario único.

* El 0 corresponde al superusuario (root).
* Del 1 al 99 son para cuentas predeterminadas.
* Del 100 al 999 son para cuentas administrativas del sistema.
* A partir del 1000 corresponden a los nuevos usuarios.

1. GID (Group IDentification) o número de identificación del grupo principal del usuario.
2. Información personal del usuario (nombre, teléfono, oficina, etc.).
3. /home o directorio de trabajo, es decir, el directorio inicial del usuario cuando se conecta al sistema.
4. Shell o intérprete de comandos empleado por el usuario cuando inicia el sistema.

## ARCHIVO /etc/group

Es el fichero de configuración de grupos y centraliza la gestión de grupos en el sistema.

Texto

Descripción generada automáticamente

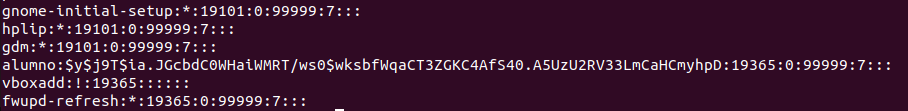
Se compone de 4 columnas separadas por “:”:

1. Nombre del grupo asociado al identificador del grupo.
2. Contraseña (aparece con un valor “x” ya que el valor encriptado se encuentra en el archivo /etc/gshadow).
3. Identificador de grupo (GID).
4. Lista de usuarios pertenecientes al grupo identificado como grupo secundario.

Todo usuario debe pertenecer a un grupo principal y, además, puede pertenecer a uno o varios grupos secundarios (o a ninguno).

## ARCHIVO /etc/shadow

Almacena la contraseña encriptada de los usuarios.



## ARCHIVO /etc/gshadow

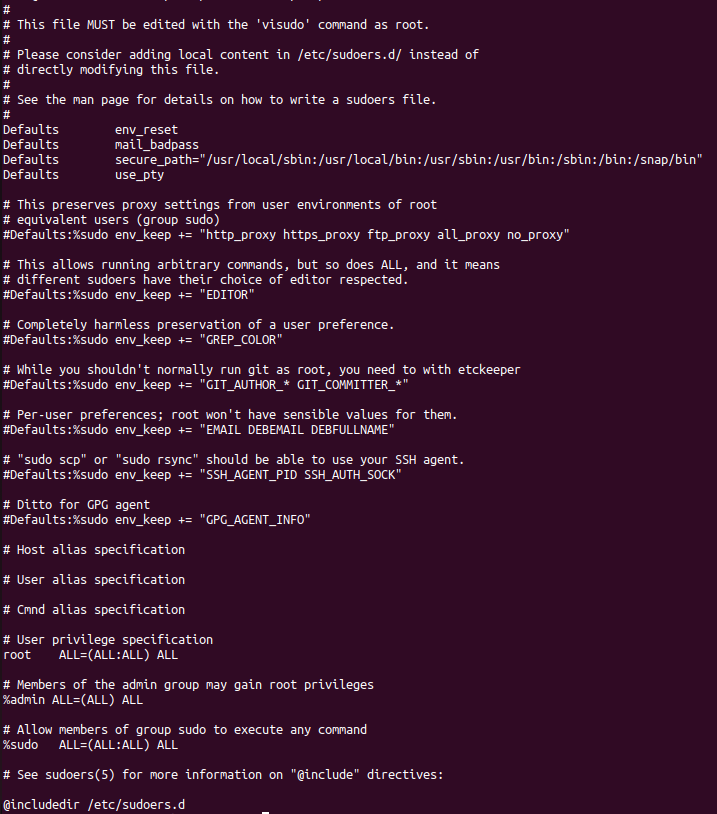
Almacena la contraseña encriptada de los grupos.

Texto

Descripción generada automáticamente

## ARCHIVO /etc/sudoers

Es un archivo que incluye una lista de los usuarios que pueden usar el comando sudo para obtener privilegios root.



## DIRECTORIO /etc/skel/

En este directorio que 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 (es decir, cuando se utiliza el comando useradd con la opción -m).

Texto

Descripción generada automáticamente

## ARCHIVO /etc/default/useradd

Es un archivo que contiene los valores por defecto que se asignan a un usuario creado con useradd.

Texto

Descripción generada automáticamente

# USUARIO ADMINISTRADOR

Es aquel que tiene capacidad de gestión en el sistema sin ser necesariamente el superusuario (root). Esta capacidad puede adquirirse mediante el comando sudo o si se encuentra en grupos de usuarios con privilegios sobre determinados archivos o comandos de gestión.

## SUPERUSUARIO (root)

Por defecto está deshabilitado para evitar acciones perjudiciales de manera inconsciente.

El prompt o línea de petición de órdenes varía según el usuario activo en él. Para superusuario es # (almohadilla) y para el resto de los usuarios es $ (símbolo del dólar), pero es posible modificar dichos caracteres editando las variables PS1 y PS2.

Para habilitar el usuario root le tenemos que asignar una contraseña mediante la orden: sudo passwd root.

Una vez indicada, podemos cambiar al usuario root mediante: su root.

## sudo

El comando sudo permite ejecutar comandos en nombre de otros usuarios, siempre que tanto el usuario como el comando que se va a ejecutar estén permitidos gracias al archivo de configuración /etc/sudoers.

Cuando ejecutamos sudo, éste solicita la contraseña del usuario que lo ejecuta. Queda almacenada durante unos minutos y, pasado este tiempo, si se vuelve a emplear, deberá introducirse de nuevo.

La sintaxis es: sudo -u usuario comando.

Texto

Descripción generada automáticamente

## su

Otra forma de ejecutar acciones de otro usuario es cambiando de usuario directamente mediante el comando su. Su sintaxis es: su [-] [usuario].

El – es opcional y permite cargar las preferencias del usuario al iniciar su sesión (por ejemplo, el /home)

En caso de no especificar un usuario será por defecto el root.

Para salir de la sesión de usuario con su debemos escribir exit.

# USUARIOS Y GRUPOS PREDETERMINADOS

En Linux además del usuario predeterminado root, existen una serie de grupos por defecto que sirven para otorgar permisos para facilitar la administración del sistema:

1. **adm**: Es el grupo de administradores que permite accesos a archivos de registro y comandos como sudo y su.
2. **users:** Es el grupo de usuarios estándar.
3. **nobody**: Es un grupo sin privilegios.
4. **root**: Administración sin restricciones sobre todo el sistema.
5. **tty**: Aporta privilegios sobre algunos dispositivos como /dev/tty (teclado y ratón).
6. **lpadmin**: Confiere privilegios sobre dispositivos de puerto paralelo.