

Control de Usuarios, Permisos y Grupos en Entornos Linux Multiusuario

26/06/2025

Angel Moreno García

CodeArts Solutions

Madrid

Introducción

Esta guía documenta la implementación técnica de un sistema organizado de usuarios, grupos y permisos en Linux. El objetivo es garantizar un entorno seguro, estructurado y fácil de administrar, aplicando buenas prácticas de control de acceso mediante permisos clásicos y ACLs, junto con políticas básicas de seguridad.

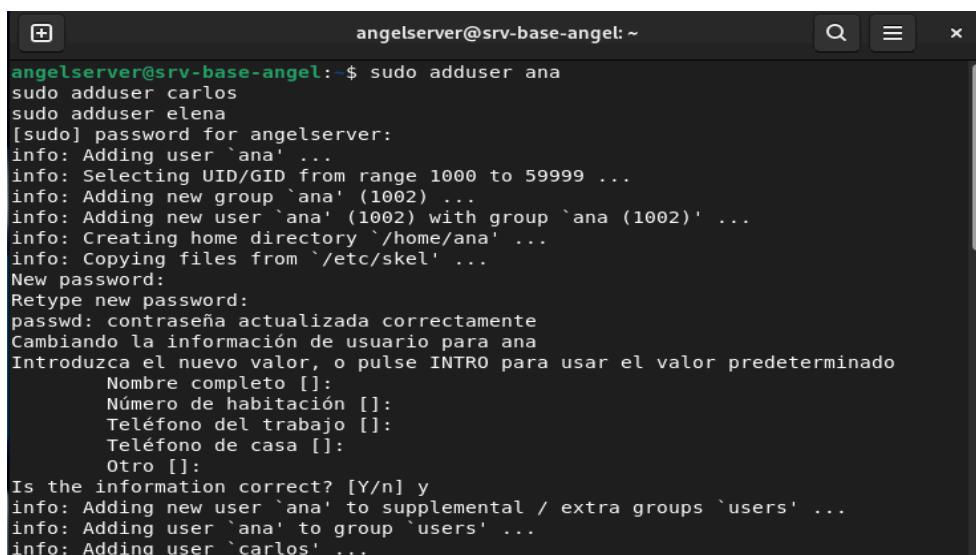
Fase 1: Creación y organización de usuarios

Crearemos usuarios individuales y los asignaremos a grupos para organizarlos.

Objetivos

1. Crear usuarios individuales
2. Crear grupos funcionales
3. Asignar correctamente usuarios a grupos

Primero, crearemos y configuraremos los usuarios *ana*, *carlos* y *elena* de usuarios usaremos: ***sudo adduser ana***, ***sudo adduser carlos*** y ***sudo adduser elena***. Y también crearemos los grupos *webdev*, *infra* y *docs* con: ***sudo groupadd webdev***, ***sudo groupadd infra***, ***sudo groupadd docs***.



```
angelserv@srv-base-angel:~$ sudo adduser ana
sudo adduser carlos
sudo adduser elena
[sudo] password for angelserv:
info: Adding user `ana' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ana' (1002) ...
info: Adding new user `ana' (1002) with group `ana (1002)' ...
info: Creating home directory `/home/ana' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para ana
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
  Nombre completo []:
  Número de habitación []:
  Teléfono del trabajo []:
  Teléfono de casa []:
  Otro []:
Is the information correct? [Y/n] y
info: Adding new user `ana' to supplemental / extra groups `users' ...
info: Adding user `ana' to group `users' ...
info: Adding user `carlos' ...
```



```
angelserv@srv-base-angel:~$ sudo groupadd webdev
sudo groupadd infra
sudo groupadd docs
angelserv@srv-base-angel:~$
```

Asignaremos los usuarios previamente creados a los grupos correspondientes, para ello usaremos los comandos:

sudo usermod -aG webdev ana, sudo usermod -aG infra carlos, sudo usermod -aG docs elena

```
angelserv@srv-base-angel:~$ sudo usermod -aG webdev ana
sudo usermod -aG infra carlos
sudo usermod -aG docs elena
angelserv@srv-base-angel:~$
```

Cambiaremos las contraseñas de los usuarios para aportar mayor seguridad y emplearemos una *mayúscula*, *una minúscula*, *un número* y *un carácter especial*. Haremos esto con cada usuario usando los comandos: ***sudo passwd ana ,sudo passwd carlos y sudo passwd elena***

```
angelserv@srv-base-angel:~$ sudo passwd ana
sudo passwd carlos
sudo passwd elena
New password:
Retype new password:
passwd: contraseña actualizada correctamente
New password:
Retype new password:
passwd: contraseña actualizada correctamente
New password:
Retype new password:
passwd: contraseña actualizada correctamente
angelserv@srv-base-angel:~$
```

Fase 2: Estructura de directorios y control de acceso

Para la estructura apropiada de los directorios primero debemos crear las carpetas, después asignar el propietario de la carpeta y su grupo.

Usaremos: ***sudo mkdir -p /grupos/web /grupos/infra /grupos/docs*** para crear la carpeta, ***sudo chown :webdev /grupos/web***, ***sudo chown :infra /grupos/infra***, , ***sudo chown :docs /grupos/docs*** para asignar los propietarios y grupos.

Al terminar estableceremos el **permiso 770** (*solo propietario y grupo pueden acceder*) y activaremos el bit *setgid* para heredar grupo automáticamente, emplearemos el comando: ***sudo chmod 770 /grupos/web /grupos/infra /grupos/docs*** y después ***sudo chmod g+s /grupos/web /grupos/infra /grupos/docs*** para activar el bit.



```
angelserv@srv-base-angel:~$ sudo mkdir -p /grupos/web /grupos/infra /grupos/docs
angelserv@srv-base-angel:~$ sudo chown :webdev /grupos/web
sudo chown :infra /grupos/infra
sudo chown :docs /grupos/docs
angelserv@srv-base-angel:~$ sudo chmod 770 /grupos/web /grupos/infra /grupos/docs
angelserv@srv-base-angel:~$ sudo chmod g+s /grupos/web /grupos/infra /grupos/docs
angelserv@srv-base-angel:~$
```

Fase 3: Configuración avanzada de permisos y restricciones

Para la configuración avanzada de los permisos, aplicaremos permisos de lectura a todos los usuarios y verificaremos los permisos. Primero crearemos el archivo, después crearemos el grupo compartido y por último aplicaremos las ACLs.

Objetivos

- Gestionar permisos específicos en un archivo
- Usar ACLs para acceso fino

Usaremos los comandos para crear el archivo:

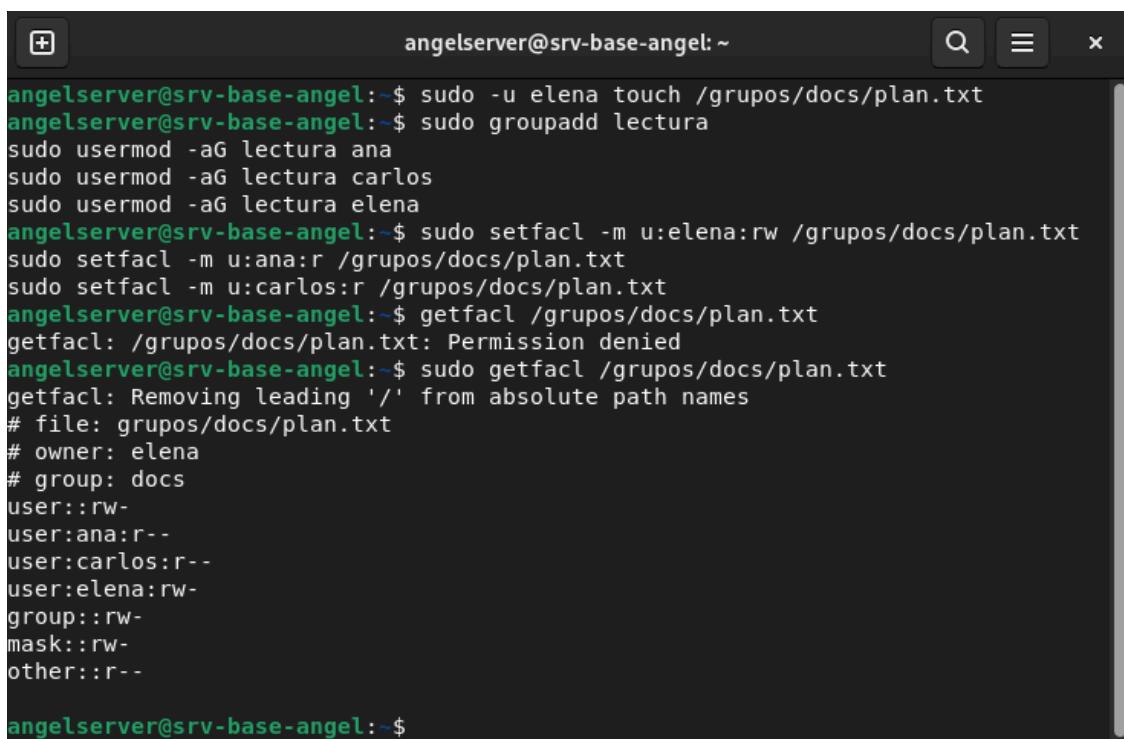
sudo touch /grupos/docs/plan.txt, sudo chown elena:docs /grupos/docs/plan.txt

Para crear el grupo compartido usaremos en la consola:

sudo groupadd lectura, sudo usermod -aG lectura ana, sudo usermod -aG lectura carlos, sudo usermod -aG lectura elena

Para aplicar las ACLs

sudo setfacl -m g:lectura:r-- /grupos/docs/plan.txt, sudo setfacl -m u:elena:rw- /grupos/docs/plan.txt



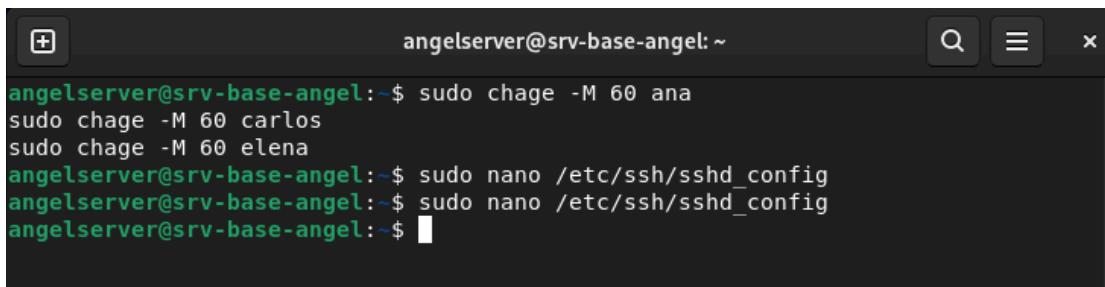
```
angelserv@srv-base-angel:~$ sudo -u elena touch /grupos/docs/plan.txt
angelserv@srv-base-angel:~$ sudo groupadd lectura
sudo usermod -aG lectura ana
sudo usermod -aG lectura carlos
sudo usermod -aG lectura elena
angelserv@srv-base-angel:~$ sudo setfacl -m u:elena:rw /grupos/docs/plan.txt
sudo setfacl -m u:ana:r /grupos/docs/plan.txt
sudo setfacl -m u:carlos:r /grupos/docs/plan.txt
angelserv@srv-base-angel:~$ getfacl /grupos/docs/plan.txt
getfacl: /grupos/docs/plan.txt: Permission denied
angelserv@srv-base-angel:~$ sudo getfacl /grupos/docs/plan.txt
getfacl: Removing leading '/' from absolute path names
# file: grupos/docs/plan.txt
# owner: elena
# group: docs
user::rw-
user:ana:r--
user:carlos:r--
user:elena:rw-
group::rw-
mask::rw-
other::r--

angelserv@srv-base-angel:~$
```

Fase 4: Buenas prácticas y seguridad básica

Establecer caducidad de las contraseñas

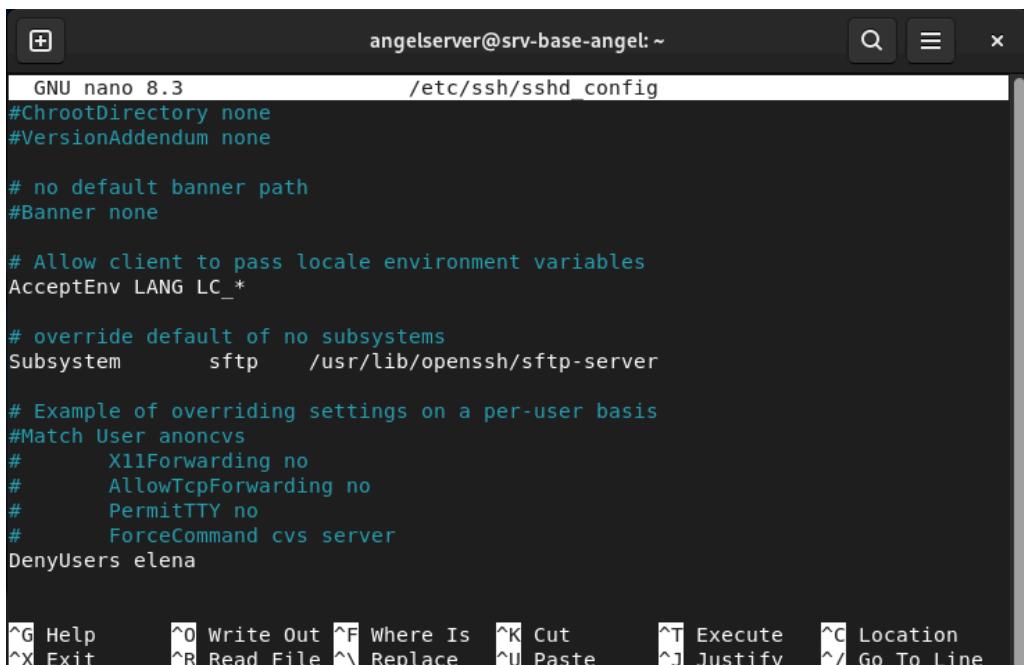
Estableceremos la caducidad de las contraseñas en 60 días, para ello usaremos el comando en la consola: ***sudo chage -M 60 ana, sudo chage -M 60 carlos y sudo chage -M 60 elena***



```
angelsrv@srv-base-angel:~$ sudo chage -M 60 ana
sudo chage -M 60 carlos
sudo chage -M 60 elena
angelsrv@srv-base-angel:~$ sudo nano /etc/ssh/sshd_config
angelsrv@srv-base-angel:~$ sudo nano /etc/ssh/sshd_config
angelsrv@srv-base-angel:~$
```

Bloquear accesos SSH

Después bloquearemos el acceso SSH a elena, para ello necesitaremos editar el archivo sshd_config con el comando: ***sudo nano /etc/ssh/sshd_config***. Al final del archivo añadiremos: ***DenyUsers elena***. Al terminar, reiniciamos el servicio SSH con: ***sudo systemctl restart ssh***



```
GNU nano 8.3                               /etc/ssh/sshd_config
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp      /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
DenyUsers elena

^G Help      ^O Write Out ^F Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit     ^R Read File ^\ Replace   ^U Paste   ^J Justify  ^/ Go To Line
```

Alias de bienvenida a nuevos usuarios

Para terminar, añadiremos un nuevo alias de bienvenida para los usuarios con el comando:
`echo "echo ' Bienvenido al sistema, recuerda usar contraseñas seguras.'" | sudo tee -a /etc/skel/.bashrc`



The screenshot shows a terminal window titled "angelserver@srv-base-angel: ~". The user has run several commands to manage user accounts and update the welcome message:

```
angelserv...$ sudo chage -M 60 ana
sudo chage -M 60 carlos
sudo chage -M 60 elena
angelserv...$ sudo nano /etc/ssh/sshd_config
angelserv...$ sudo systemctl restart ssh
angelserv...$ echo "echo ' Bienvenido al sistema, recuerda usa
r contraseñas seguras.'" | sudo tee -a /etc/skel/.bashrc
echo ' Bienvenido al sistema, recuerda usar contraseñas seguras.'
angelserv...$
```

Conclusión

Se ha implementado con éxito una estructura de usuarios, grupos y permisos en un entorno **Linux**. El sistema garantiza un acceso controlado a los recursos, separación de funciones y aplicación de medidas de seguridad básicas. El uso de ACLs y setgid proporciona una gestión granular, mientras que las restricciones SSH y políticas de contraseñas refuerzan la protección del sistema.