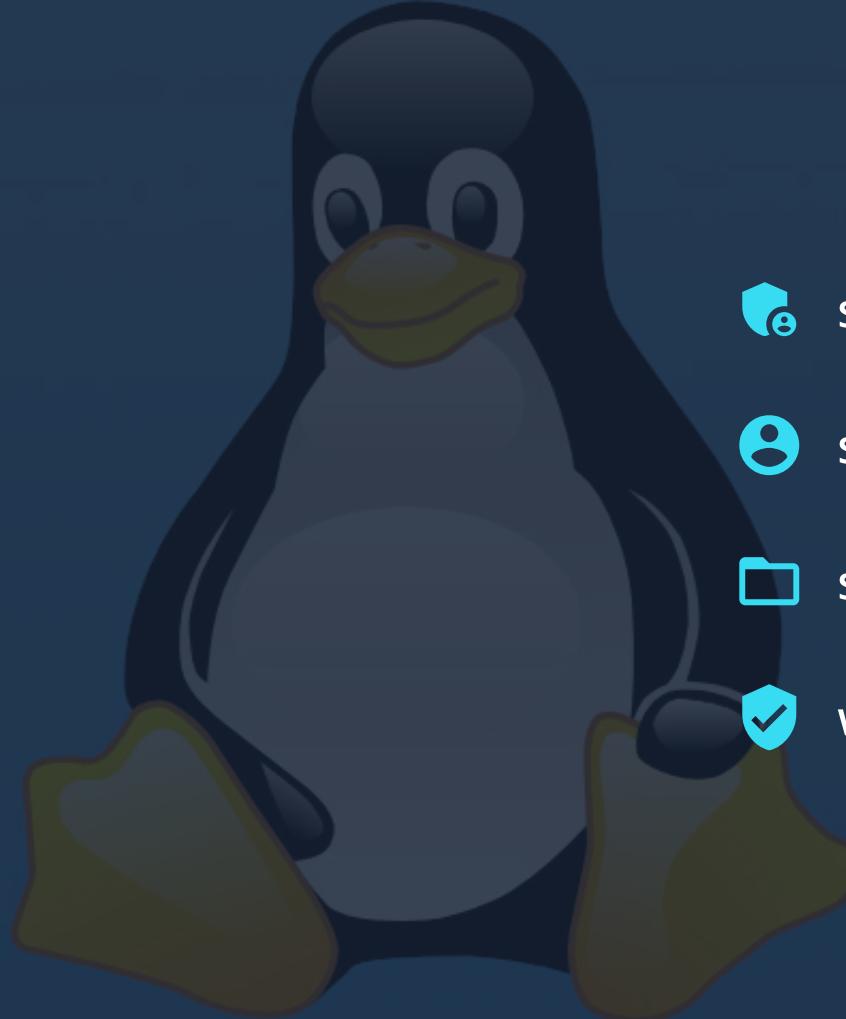




# Escalada de Privilegios

---

Gestión de permisos en Linux



sudo



su



sudoers



wheel

# ⑧ ¿Qué es sudo?

## ⌚ Definición

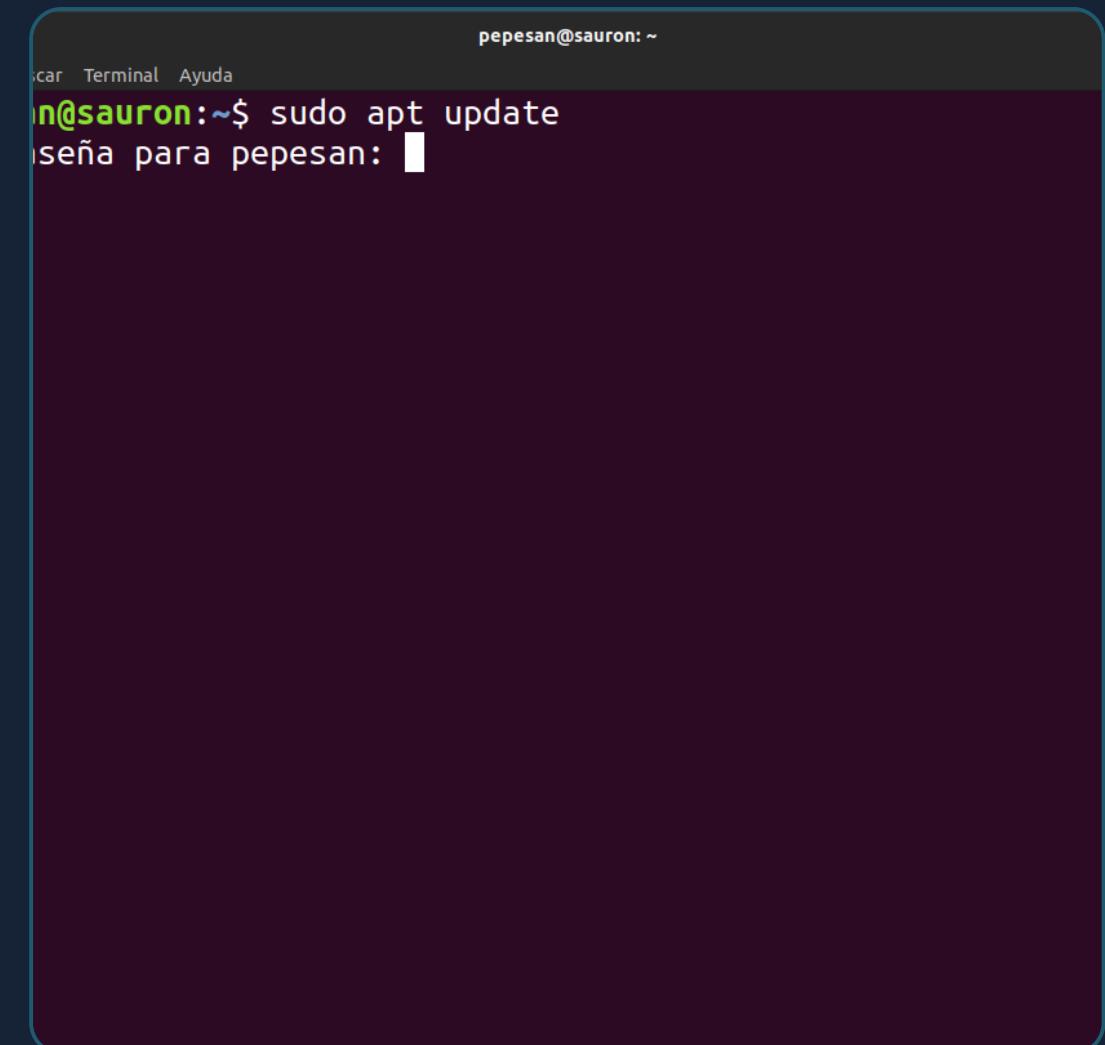
Aplicación de escalada de privilegios en sistemas Unix/Linux

## ⬇ Instalación

No está presente en todos los sistemas por defecto

## ✓ Funcionalidad

Permite ejecutar comandos con privilegios de superusuario



A screenshot of a terminal window titled 'pepesan@sauron: ~'. The window shows a command-line interface with the following text:  
pepesan@sauron:~\$ sudo apt update  
Contraseña para pepesan: █

# → Diferencias sudo vs su

## sudo

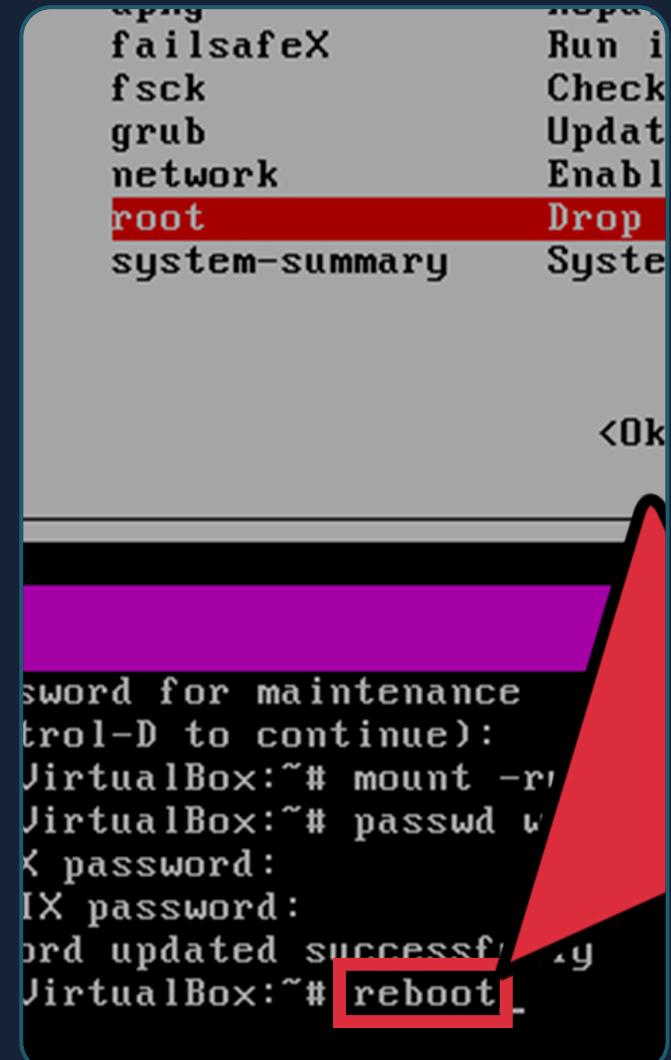
- ✓ Contraseña del usuario actual
- ✓ Ejecuta solo un comando
- ✓ Registra acciones en logs
- ✓ Más seguro y granular

## su

- ✓ Contraseña del usuario objetivo
- ✓ Cambia de usuario
- ✓ Sin registro de logs
- ✓ Menos control granular



Cuándo **sudo**: Para tareas específicas • **su**: Para sesiones usar prolongadas



The terminal window shows the following content:

```
^P^S failsafeX Run i
      fsck Check
      grub Updat
      network Enabl
      root Drop
      system-summary Syste
<0k

sword for maintenance
trol-D to continue):
JirtualBox:~# mount -r
JirtualBox:~# passwd v
x password:
IX password:
ord updated successfully.
JirtualBox:~# reboot
```

A red box highlights the command "reboot" at the bottom of the terminal output.

# ★ Fichero sudoers, grupos sudo y wheel

## Fichero sudoers

Ruta: /etc/sudoers

Configura permisos sudo para usuarios y grupos

### grupo sudo

Usuarios con permisos para usar sudo

### grupo wheel

Grupo tradicional en distribuciones como RHEL/CentOS

**i** Ambos grupos permiten escalada de privilegios según configuración

```
- : sudo visudo — Konsole
Fer Marcadores Complementos Preferencias Ayuda
/etc/sudoers.tmp *

#ST be edited with the 'visudo' command as root.

#der adding local content in /etc/sudoers.d/ instead of
#ifying this file.

page for details on how to write a sudoers file.

env_reset
mail_badpass
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
use_pty

#ge specification
ALL:ALL ) ALL

#rs of group sudo to execute any command
ALL:ALL ) ALL

5) for more information on "@include" directives:
/etc/sudoers.d

^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubic
^R Leer fich. ^Y Reemplazar ^U Pegar ^J Justificar ^/ Ir a
```

## 📁 Fichero sudoers.d/

### 📄 ¿Qué es?

Directorio [/etc/sudoers.d/](#) que permite configuraciones adicionales sin editar el fichero principal sudoers

### ⭐ Ventajas

- ✓ Más seguro
- ✓ Modular
- ✓ Fácil de mantener
- ✓ Evita errores en fichero principal

### ⚙️ Estructura

Cada fichero en [sudoers.d/](#) se incluye automáticamente en la configuración sudo



# <> Ejemplo de configuración para usuario curso

## Crear fichero en /etc/sudoers.d/

```
sudo visudo -f /etc/sudoers.d/curs
```

## Código de ejemplo

```
curso ALL=(ALL) NOPASSWD: /usr/bin/apt  
update,  
/usr/bin/apt upgrade
```



curso



NOPASSWD  
Sin contraseña



Comandos  
apt  
update/upgrade

```
Terminal  
/etc/sudoers.tmp  
  
command as root.  
etc/sudoers.d/ instead of  
te a sudoers file.  
  
:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"  
  
command  
include" directives:  
? ^K Recort txt ^J Justificar ^C Pos atual  
^U Colar txt ^T VerfOrtog ^I Ir p/ lir
```

# Preguntas tipo test

1. ¿Qué comando permite ejecutar comandos con privilegios de superusuario en Linux?

- a** sudo
- b** su
- c** chmod
- d** chown

2. ¿Cuál es la ubicación del fichero principal sudoers?

- a** /etc/sudoers
- b** /etc/sudoers.conf
- c** /etc/sudoers.d/
- d** /var/sudoers

3. ¿Qué grupo tradicional en RHEL/CentOS permite escalada de privilegios?

- a** sudo
- b** wheel
- c** admin
- d** root

4. ¿Cuál es la principal diferencia entre sudo y su?

- a** sudo requiere contraseña de root
- b** su solo ejecuta un comando
- c** sudo registra acciones en logs
- d** su es más seguro

5. ¿Para qué sirve el directorio /etc/sudoers.d/?

Almacenar ficheros de configuración adicionales

- a** configuración adicionales
- b** Guardar logs de sudo

6. ¿Qué opción permite a un usuario ejecutar sudo sin contraseña?

- a** NOPASSWD
- b** NOLOG
- c** NOAUTH
- d** NOPWD