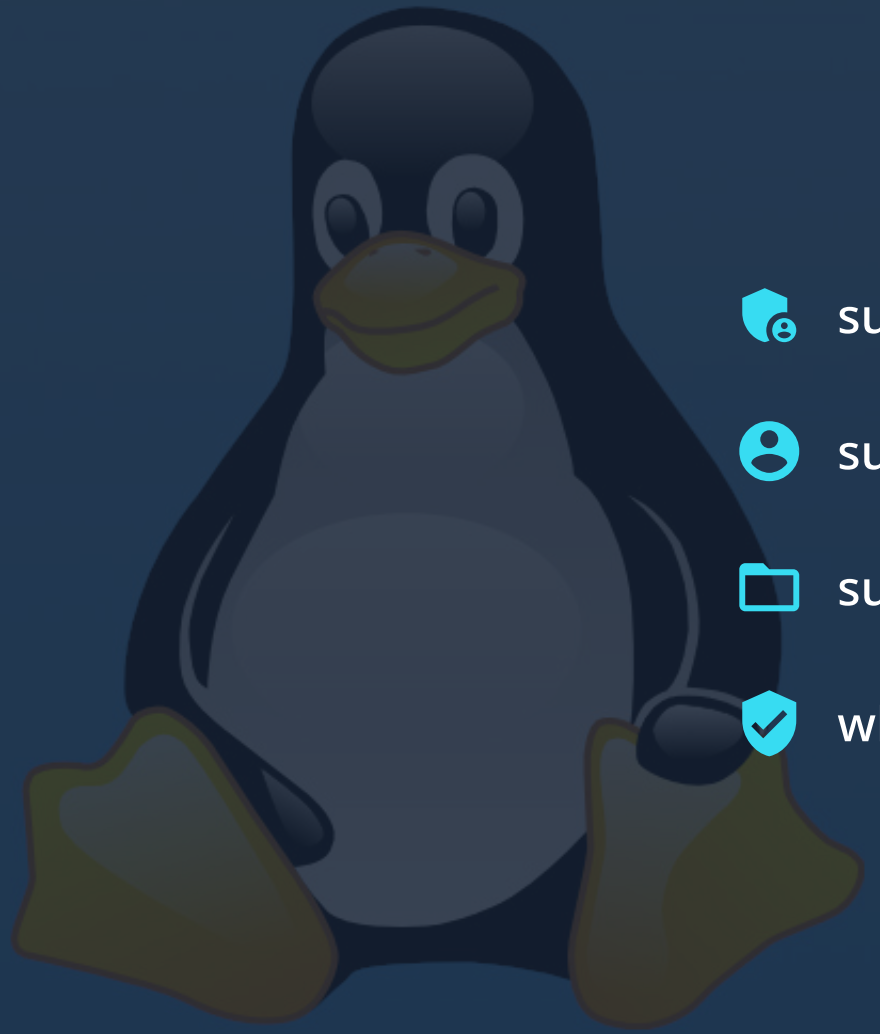
Escalada de Privilegios

Gestión de permisos en Linux



- sudo
- su
- sudoers
- wheel

¿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

Diferencias sudo vs su

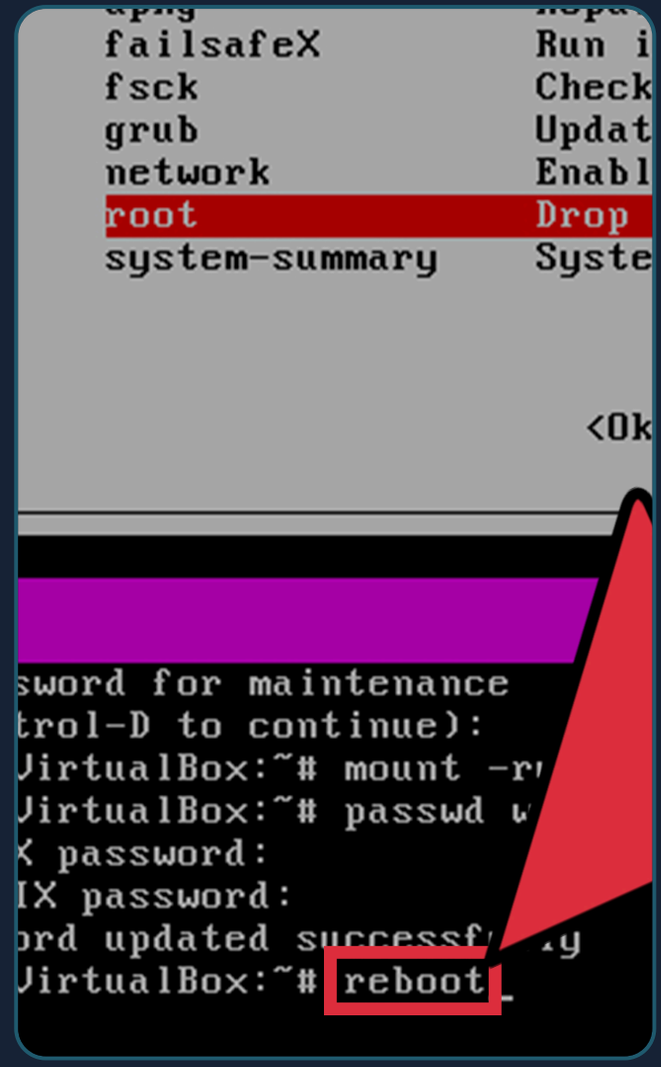
sudo

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



Fichero sudoers, grupos sudo y wheel

Fichero sudoers

Ruta: /etc/sudoers

Configura permisos sudo para usuarios y grupos

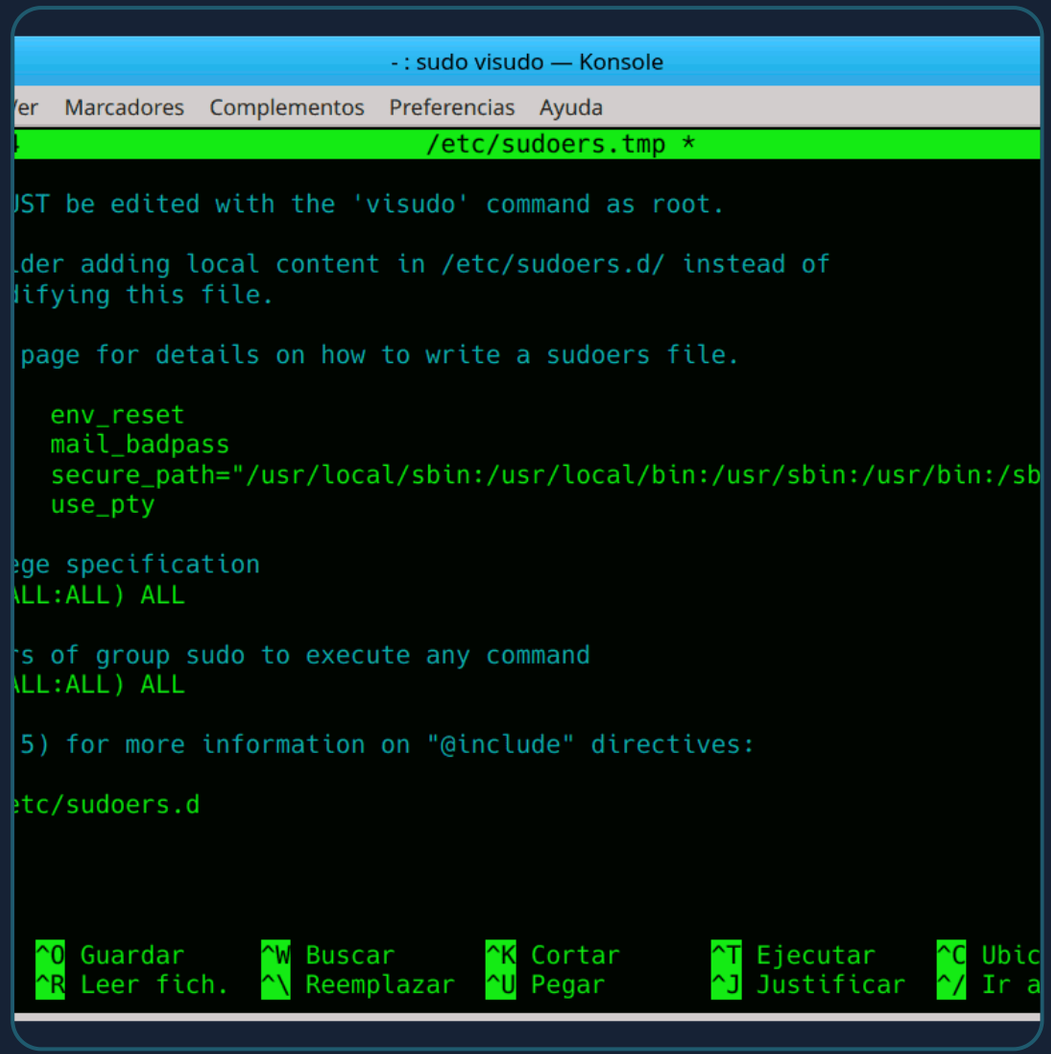
grupo sudo

Usuarios con permisos para usar sudo

grupo wheel

Grupo tradicional en distribuciones como RHEL/CentOS

Ambos grupos permiten escalada de privilegios según configuración



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/curso

Código de ejemplo

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

Usuario

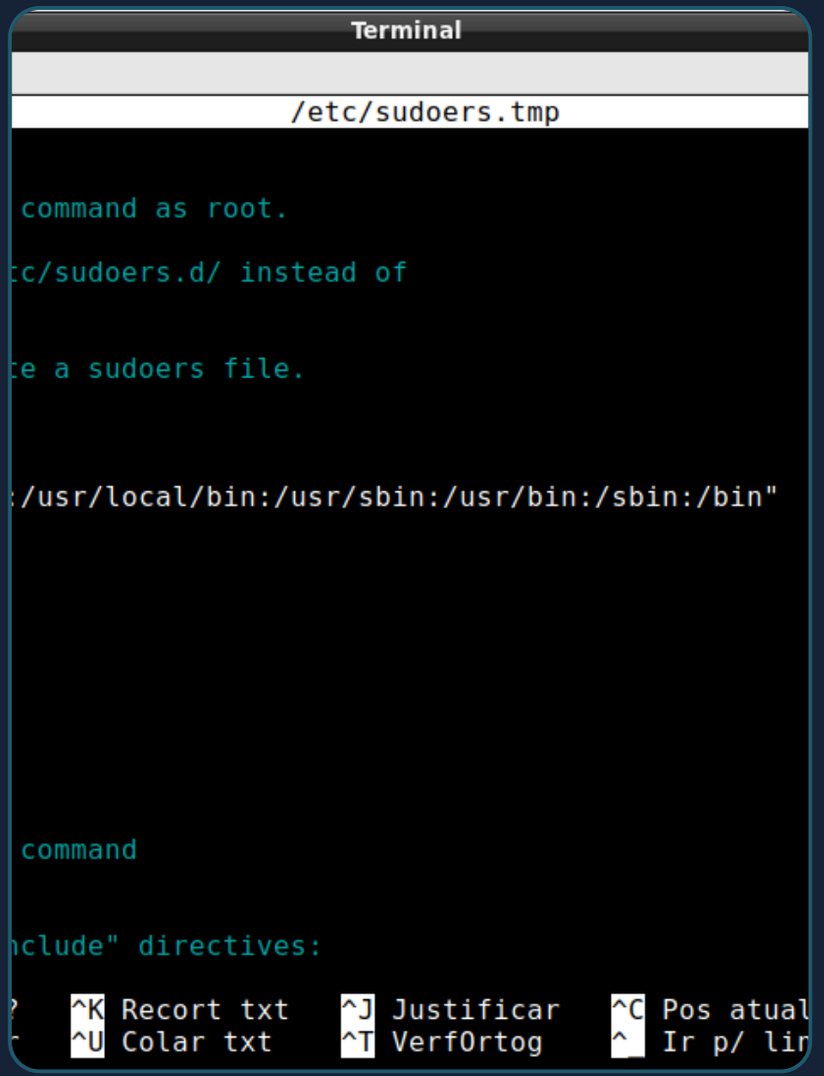
curso

NOPASSWD

Sin contraseña

Comandos

apt update/upgrade



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/?

a Almacenar ficheros de 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