

452 - LINUX Y UBUNTU

Vigila tus archivos clave en Ubuntu con auditd

Recibe un registro de quién toca los archivos de usuarios y contraseñas de tu sistema para detectar cambios no autorizados.



NIVEL
Avanzado

TIEMPO
25 min

CATEGORÍA
Linux y Ubuntu

WEB
soporteinformatico360.com

auditd es el sistema de auditoría de Linux. Le dices qué archivos importantes quieres vigilar y anota cada cambio con fecha, usuario y programa. Es una forma sencilla de bastionar tu Ubuntu y saber si alguien ha tocado lo que no debe.

■ Qué necesitas

- ✓ Un equipo con Ubuntu (la última versión LTS)
- ✓ Un usuario con permisos sudo
- ✓ Conexión a Internet
- ✓ La terminal (Ctrl + Alt + T)

■ Paso a paso

01

Instala auditd

Abre la terminal e instala el paquete. El servicio arranca solo al terminar.

```
Terminal
$ sudo apt update
$ sudo apt install auditd -y
$
```

02

Comprueba que está activo

Debe aparecer como active (running). Pulsa q para salir.

```
Terminal
$ sudo systemctl status auditd
$
```

03

Vigila los archivos sensibles

Añade una regla para el archivo de usuarios y otra para sudoers. La letra w vigila escrituras y la a cambios de permisos.

```
Terminal
$ sudo auditctl -w /etc/passwd -p wa -k usuarios
$ sudo auditctl -w /etc/sudoers -p wa -k sudo
$
```

04

Haz una prueba

Crea un usuario de prueba y busca el rastro con la etiqueta usuarios. Verás quién hizo el cambio y con qué programa.

Terminal

```
$ sudo adduser prueba
$ sudo ausearch -k usuarios -i
$ █
```

05

Hazlo permanente

Copia las dos reglas (sin auditctl delante) en el archivo `/etc/audit/rules.d/vigilancia.rules` y cárgalas con `sudo augenrules --load`.



06

Limpia y revisa

Borra el usuario de prueba con `sudo deluser prueba`. De vez en cuando, mira el resumen de archivos vigilados con `sudo aureport -f`.

■ Consejos

CONSEJO 1

Vigila pocos archivos importantes: demasiadas reglas llenan el registro.

CONSEJO 2

Pon etiquetas (-k) claras para encontrar los eventos rápido.

CONSEJO 3

Combínalo con `journalctl` y `Lynis` para tener una visión completa.



Importante: Cambia solo equipos que administres. Si editas reglas en un servidor de empresa, avisa antes al responsable y haz copia de la configuración.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar.
En taller, a domicilio en Madrid o por asistencia remota.

910 117 112

soporte@soporteinformatico360.com
soporteinformatico360.com