El sistema d'auditoria de Linux: auditd

Índex

`auditd` (*Linux Audit Daemon*) és el dimoni del sistema d'auditoria del kernel de Linux. Permet registrar esdeveniments del sistema de manera detallada: accés a fitxers, crides al sistema, canvis de privilegis, connexions de xarxa, modificacions de configuració, etc.

És una eina fonamental per a:

- **Seguretat:** detectar intrusions i comportaments anòmals.
- **Compliment normatiu:** PCI-DSS, HIPAA, ISO 27001, SOX, GDPR.
- **Investigació forense:** reconstruir què va passar en un incident.
- **Auditoria d'administració:** saber qui va fer què i quan.

L'arquitectura es basa en dos components:

- **Kernel:** el subsistema d'auditoria intercepta esdeveniments i els envia al dimoni.
- **`auditd`:** recull els esdeveniments del kernel i els escriu al log.

1. Instal·lació

```
# Debian/Ubuntu
sudo apt install auditd audispd-plugins

# Fedora/RHEL/CentOS
sudo dnf install audit audit-libs

# Arch/Manjaro
sudo pacman -S audit
```

1.1. Habilitar i iniciar el servei

```
sudo systemctl enable --now auditd
sudo systemctl status auditd
```

2. Arquitectura i components

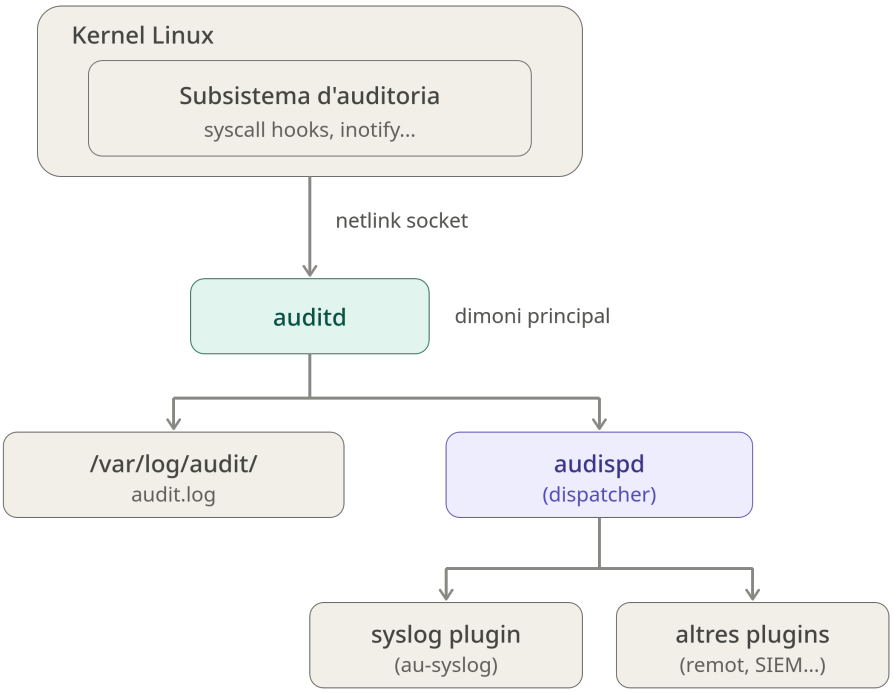

Figura 1: Arquitectura d'auditd

2.1. Components principals

Component	Descripció
`auditd`	Dimoni principal que recull i escriu els esdeveniments
`auditctl`	Eina per gestionar les regles d'auditoria en temps real
`ausearch`	Cerca i filtra esdeveniments als logs d'auditoria
`aureport`	Genera informes resumits dels logs
`autrace`	Traça les crides al sistema d'un procés (similar a strace)
`audispd`	Dispatcher: distribueix esdeveniments a connectors externs
`augenrules`	Compila les regles de `/etc/audit/rules.d/` en un fitxer únic

3. Fitxers de configuració

3.1. `/etc/audit/auditd.conf`

Configuració principal del dimoni:

```
# Fitxer de log
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root

# Mida màxima del log (MB)
max_log_file = 50

# Acció quan s'arriba a la mida màxima
# ROTATE, SYSLOG, SUSPEND, KEEP_LOGS, IGNORE
max_log_file_action = ROTATE

# Nombre de fitxers de log a conservar
num_logs = 10

# Acció quan l'espai en disc és baix
# SYSLOG, SUSPEND, SINGLE, HALT
space_left = 75
space_left_action = SYSLOG
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND

# Flux d'esdeveniments per segon (0 = sense límit)
rate_limit = 0

# Mode de prioritat (0=normal, 1=alta, 2=temps real)
priority_boost = 4
```

3.2. `/etc/audit/audit.rules` i `/etc/audit/rules.d/`

Les regles d'auditoria es poden definir a:

- **`/etc/audit/audit.rules`**: fitxer únic (generat per `augenrules`).
- **`/etc/audit/rules.d/*.rules`**: fitxers individuals que `augenrules` compila.

Estructura recomanada a `rules.d/`:

```
/etc/audit/rules.d/
├── 10-base-config.rules
├── 20-dont-audit.rules
├── 30-stig.rules
├── 40-local.rules
├── 50-identity.rules
```

```
├── 70-system-local.rules
└── 99-finalize.rules
```

4. Regles d'auditoria

4.1. Tipus de regles

Tipus	Descripció
Regles de control	Configuren el comportament del subsistema d'auditoria
Regles de sistema de fitxers	Vigilen accés a fitxers i directoris (watches)
Regles de crides al sistema	Vigilen syscalls específiques

4.2. Sintaxi amb `auditctl`

```
auditctl [opcions]
```

Opcions de control

```
# Veure les regles actives
sudo auditctl -l

# Veure l'estat del subsistema
sudo auditctl -s

# Eliminar totes les regles
sudo auditctl -D

# Bloquejar les regles (immutable, requereix reinici per canviar)
sudo auditctl -e 2

# Activar/desactivar l'auditoria
sudo auditctl -e 1    # activar
sudo auditctl -e 0    # desactivar
```

Regles de vigilància de fitxers (`-w`)

```
# Sintaxi
auditctl -w RUTA -p PERMISOS -k CLAU

# Permisos:
#   r = lectura
#   w = escriptura
#   x = execució
#   a = canvi d'atributs

# Vigilar lectura i escriptura de /etc/passwd
sudo auditctl -w /etc/passwd -p rwa -k canvi_usuaris

# Vigilar el directori /etc/
sudo auditctl -w /etc/ -p wa -k canvi_configuracio

# Vigilar execució d'un binari
sudo auditctl -w /usr/bin/sudo -p x -k us_sudo

# Vigilar /var/log/
sudo auditctl -w /var/log/ -p wa -k canvi_logs
```

Regles de crides al sistema (`-a`)

```
# Sintaxi
auditctl -a LLISTA,ACCIÓ -S SYSCALL [-F CAMP=VALOR] -k CLAU

# Llistes: task, exit, user, exclude
# Accions: always, never

# Auditar tots els intents d'obertura de fitxers fallits
sudo auditctl -a always,exit -F arch=b64 -S open -F exit=-EACCES -k
 ↪  acces_denegat
sudo auditctl -a always,exit -F arch=b32 -S open -F exit=-EACCES -k
 ↪  acces_denegat

# Auditar canvis de privilegis (setuid, setgid)
sudo auditctl -a always,exit -F arch=b64 -S setuid -S setgid -k
 ↪  canvi_privilegis

# Auditar creació i eliminació de fitxers
sudo auditctl -a always,exit -F arch=b64 -S creat -S unlink -S
 ↪  unlinkat -k gestio_fitxers

# Auditar modificacions del sistema de fitxers
sudo auditctl -a always,exit -F arch=b64 -S chmod -S chown -S fchmod
 ↪  -k canvi_permisos

# Auditar muntatge de sistemes de fitxers
```

```
sudo auditctl -a always,exit -F arch=b64 -S mount -S umount2 -k
 ↪  muntatge

# Auditar accions d'un usuari concret (uid=1000)
sudo auditctl -a always,exit -F arch=b64 -F uid=1000 -S all -k
 ↪  usuari_ramon

# Excloure esdeveniments d'un procés (reduir soroll)
sudo auditctl -a never,exit -F arch=b64 -F exe=/usr/sbin/crond
```

4.3. Camps de filtratge (`-F`)

Camp	Descripció	Exemple
`arch`	Arquitectura (b32/b64)	`-F arch=b64`
`uid`	ID d'usuari	`-F uid=1000`
`gid`	ID de grup	`-F gid=0`
`euid`	UID efectiu	`-F euid=0`
`auid`	UID d'auditoria (inici de sessió original)	`-F auid=1000`
`pid`	ID de procés	`-F pid=1234`
`ppid`	ID del procés pare	`-F ppid=1`
`exe`	Ruta de l'executable	`-F exe=/bin/bash`
`path`	Ruta del fitxer afectat	`-F path=/etc/passwd`
`exit`	Codi de retorn de la syscall	`-F exit=-EACCES`
`success`	Èxit (1) o fallada (0) de la syscall	`-F success=0`
`key`	Clau de filtratge	`-F key=clau`

5. Fitxers de regles predefinides

RHEL/Fedora i altres distribucions inclouen conjunts de regles predefinides:

```
# Localització habitual
ls /usr/share/audit/sample-rules/
ls /usr/share/doc/audit/

# Regles STIG (Security Technical Implementation Guide)
# Regles PCI-DSS
# Regles NISPOM
```

5.1. Exemple de fitxer de regles complet (`/etc/audit/rules.d/40-local.rules`)

```
# Eliminar regles existents
-D

# Mida del buffer (esdeveniments pendents)
-b 8192

# Acció si el kernel no pot enviar esdeveniments
 ↪  (0=silent,1=printk,2=panic)
-f 1

# ── Identitat i autenticació ──────────────────────────
-w /etc/passwd -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/group -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/sudoers -p wa -k sudoers
-w /etc/sudoers.d/ -p wa -k sudoers

# ── SSH ───────────────────────────────────────────────
-w /etc/ssh/sshd_config -p wa -k sshd_config

# ── Fitxers de log ────────────────────────────────────
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
-w /var/log/lastlog -p wa -k session

# ── Execució de sudo ──────────────────────────────────
-w /usr/bin/sudo -p x -k sudo_exec
-w /bin/su -p x -k su_exec

# ── Canvis de xarxa ───────────────────────────────────
-w /etc/hosts -p wa -k network
-w /etc/network/ -p wa -k network
-w /etc/sysconfig/network -p wa -k network

# ── Cron ──────────────────────────────────────────────
-w /etc/cron.d/ -p wa -k cron
-w /etc/cron.daily/ -p wa -k cron
-w /etc/cron.weekly/ -p wa -k cron
-w /var/spool/cron/ -p wa -k cron

# ── Mòduls del kernel ─────────────────────────────────
-w /sbin/insmod -p x -k moduls_kernel
-w /sbin/rmmod -p x -k moduls_kernel
-w /sbin/modprobe -p x -k moduls_kernel
-a always,exit -F arch=b64 -S init_module -S delete_module -k
 ↪  moduls_kernel

# ── Syscalls de privilegis ────────────────────────────
```

```
-a always,exit -F arch=b64 -S setuid -S setgid -S seteuid -S setegid
 ↪  -k setuid
-a always,exit -F arch=b32 -S setuid -S setgid -S seteuid -S setegid
 ↪  -k setuid

# ── Accés denegat ──────────────────────────────────
-a always,exit -F arch=b64 -S open -S openat -F exit=-EACCES -k
 ↪  acces_denegat
-a always,exit -F arch=b64 -S open -S openat -F exit=-EPERM -k
 ↪  acces_denegat

# ── Bloquejar regles (immutable) ──────────────────
# -e 2
```

6. Format del log d'auditoria

Els esdeveniments es desen a `/var/log/audit/audit.log` en format de text pla:

```
type=SYSCALL msg=audit(1717920000.123:456): arch=c000003e syscall=2
 ↪  success=yes exit=3 a0=7f1234 a1=0 a2=1fffff a3=0 items=1 ppid=1234
 ↪  pid=5678 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000
 ↪  fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=1
 ↪  comm="cat" exe="/usr/bin/cat" subj=unconfined_u:unconfined_r
 ↪  key="acces_fitxer"

type=CWD msg=audit(1717920000.123:456): cwd="/home/ramon"

type=PATH msg=audit(1717920000.123:456): item=0 name="/etc/passwd"
 ↪  inode=131073 dev=08:01 mode=0100644 ouid=0 ogid=0 rdev=00:00
 ↪  obj=system_u:object_r:passwd_file_t nametype=NORMAL
```

6.1. Camps principals d'un esdeveniment SYSCALL

Camp	Descripció
`type`	Tipus d'esdeveniment (SYSCALL, PATH, CWD, USER_AUTH…)
`msg`	Timestamp i número de sèrie de l'esdeveniment
`syscall`	Número de la crida al sistema
`success`	Si la syscall va tenir èxit
`pid`	PID del procés
`auid`	UID d'auditoria (usuari que va iniciar sessió)
`uid/gid`	UID/GID real del procés
`comm`	Nom del procés
`exe`	Ruta completa de l'executable
`key`	Clau de la regla que ha generat l'esdeveniment

6.2. Tipus d'esdeveniments habituals

Tipus	Descripció
`SYSCALL`	Crida al sistema
`PATH`	Fitxer o directori afectat
`CWD`	Directori de treball actual
`EXECVE`	Execució d'un programa
`USER_AUTH`	Intent d'autenticació
`USER_LOGIN`	Inici de sessió d'usuari
`USER_LOGOUT`	Tancament de sessió
`ADD_USER`	Creació d'un usuari
`DEL_USER`	Eliminació d'un usuari
`CRYPTO_KEY_USER`	Ús de claus criptogràfiques
`AVC`	Denegació de SELinux/AppArmor
`CONFIG_CHANGE`	Canvi de configuració de l'auditoria

7. `ausearch`: cercar esdeveniments

```
# Cercar per clau
sudo ausearch -k identity
sudo ausearch -k sudo_exec

# Cercar per usuari
sudo ausearch -ua ramon
sudo ausearch -ui 1000        # Per UID

# Cercar per executable
sudo ausearch -x /usr/bin/sudo

# Cercar per tipus d'esdeveniment
sudo ausearch -m USER_LOGIN
sudo ausearch -m SYSCALL

# Cercar per interval de temps
sudo ausearch --start today
sudo ausearch --start yesterday --end today
sudo ausearch --start "06/09/2025 08:00:00" --end "06/09/2025
 ↪  18:00:00"

# Cercar esdeveniments fallits
sudo ausearch --success no

# Cercar per PID
sudo ausearch -p 1234

# Format llegible
sudo ausearch -k identity -i          # Interpreta UIDs, syscalls...
sudo ausearch -k identity --format text  # Format text pla

# Combinar criteris
```

```
sudo ausearch -k sudoers -ua ramon --start today -i
```

8. `aureport`: informes

```
# Resum general
sudo aureport

# Informe d'autenticacions
sudo aureport -au
sudo aureport --auth

# Informe d'inicis de sessió
sudo aureport -l
sudo aureport --login

# Informe d'execucions
sudo aureport -x
sudo aureport --executable

# Informe de fitxers accedits
sudo aureport -f
sudo aureport --file

# Informe d'errors/fallades
sudo aureport --failed

# Informe d'anomalies
sudo aureport -a
sudo aureport --anomaly

# Informe per interval de temps
sudo aureport --start today
sudo aureport --start this-week

# Informe d'usuaris
sudo aureport -u
sudo aureport --user

# Informe de claus (keys)
sudo aureport -k
sudo aureport --key

# Informe resum (estadístiques)
sudo aureport --summary
```

Exemple de sortida de `aureport`:

```
Summary Report
======================
```

```
Range of time in logs: 09/06/2025 00:00:01.000 - 09/06/2025
 ↪  23:59:59.000
Selected time for report: 09/06/2025 00:00:01 - 09/06/2025
 ↪  23:59:59.000
Number of changes in configuration: 4
Number of changes to accounts, groups, or roles: 0
Number of logins: 12
Number of failed logins: 3
Number of authentications: 18
Number of failed authentications: 5
Number of users: 3
Number of terminals: 4
Number of host names: 2
Number of executables: 35
Number of commands: 28
Number of files: 47
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 8
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 2
Number of keys: 6
Number of process IDs: 124
Number of events: 892
```

9. `autrace`: traçar un procés

```
# Traçar l'execució d'una ordre
sudo autrace /usr/bin/ls /etc

# Veure els resultats
sudo ausearch -p PID -i

# Netejar les regles temporals d'autrace
sudo autrace --stop
```

10. Integració amb `syslog` i SIEM

10.1. Enviar esdeveniments a syslog

Editar `/etc/audisp/plugins.d/syslog.conf` (o `/etc/audit/plugins.d/syslog.conf`):

```
active = yes
direction = out
path = builtin_syslog
type = builtin
args = LOG_INFO
format = string
```

10.2. Enviar esdeveniments a un servidor remot

```
# /etc/audisp/audisp-remote.conf
remote_server = 192.168.1.50
port = 60
transport = tcp
```

```
# /etc/audisp/plugins.d/au-remote.conf
active = yes
direction = out
path = /sbin/audisp-remote
type = always
format = string
```

11. Bones pràctiques

1. **Definir una política clara** abans de configurar regles: quins esdeveniments són rellevants.
2. **Usar claus descriptives** (`-k`) per facilitar la cerca posterior.
3. **Separar les regles en fitxers** a `/etc/audit/rules.d/` per organització.
4. **Incloure arquitectures b32 i b64** en les regles de syscalls per cobrir tots els casos.
5. **Monitorar l'espai en disc:** els logs d'auditoria poden créixer ràpidament.
6. **Configurar rotació de logs** (`max_log_file`, `num_logs`, `max_log_file_action = ROTATE`).
7. **Enviar logs a un servidor centralitzat** per evitar que un atacant pugui esborrar-los.
8. **Revisar periòdicament** els informes amb `aureport --summary`.
9. **Bloquejar les regles** amb `auditctl -e 2` en producció per evitar modificacions no autoritzades.
10. **Excloure soroll** amb regles `never` per a processos de sistema molt actius (cron, auditd mateix).
11. **Correlacionar amb altres logs** (`/var/log/auth.log`, `journalctl`) per a investigació forense.

12. Casos d'ús habituals

Detectar qui ha modificat `/etc/passwd`

```
sudo auditctl -w /etc/passwd -p wa -k passwd_change
sudo ausearch -k passwd_change -i
```

Detectar execucions de sudo

```
sudo auditctl -w /usr/bin/sudo -p x -k sudo_exec
sudo ausearch -k sudo_exec -i --start today
```

Detectar intents d'accés denegat

```
sudo auditctl -a always,exit -F arch=b64 -S open,openat -F
 ↪  exit=-EACCES -k acces_denegat
sudo ausearch -k acces_denegat --success no -i
```

Informe d'inicis de sessió fallits del dia

```
sudo aureport --auth --failed --start today
```

Investigar activitat d'un usuari concret

```
sudo ausearch -ua ramon --start today -i | less
```

13. Resum d'ordres

```
# Estat del subsistema
auditctl -s

# Llistar regles actives
auditctl -l

# Afegir vigilància de fitxer
auditctl -w /etc/passwd -p rwa -k passwd

# Afegir regla de syscall
```

```
auditctl -a always,exit -F arch=b64 -S execve -k exec

# Eliminar totes les regles
auditctl -D

# Cercar per clau
ausearch -k passwd -i

# Cercar per usuari avui
ausearch -ua usuari --start today -i

# Informe general
aureport --summary

# Informe d'autenticacions fallides
aureport --auth --failed

# Recarregar regles
augenrules --load
service auditd restart
```

14. Referències

- `man auditd` --- Manual del dimoni
- `man auditctl` --- Manual de gestió de regles
- `man ausearch` --- Manual de cerca
- `man aureport` --- Manual d'informes
- `man audit.rules` --- Format dels fitxers de regles
- `man auditd.conf` --- Configuració del dimoni
- Linux Audit Documentation
- Arch Wiki: Audit framework
- Red Hat: Auditing the system

Versions d'aquest document

- HTML - auditd.html
- PDF - auditd.pdf
- ODT - auditd.odt
- MD - auditd.md