ClamAV

Índex

ClamAV (Clam AntiVirus) és un motor antivirus de codi obert dissenyat principalment per a sistemes GNU/Linux, encara que és multiplataforma. És mantingut per Cisco Talos i distribuït sota la llicència GPL v2.

Figura 1: ClamAV logo

1. Història i origen

- Creat per Tomasz Kojm el **2002**.
- El nom “Clam” prové de “Clam AntiVirus”.
- El **2007** va ser adquirit per Sourcefire.
- El **2013** Sourcefire va ser adquirida per **Cisco**, que n'és l'actual mantenidora a través de l'equip **Cisco Talos**.
- És el motor antivirus de referència per a servidors de correu en entorns Linux.

2. Característiques principals

- Motor de detecció basat en **signatures** (fitxers `.cvd` i `.cld`).
- Suport per a **descompressió** automàtica: ZIP, RAR, 7z, TAR, GZ, BZ2, ARJ, CAB, i molts més.
- Anàlisi de fitxers **PE** (executables Windows), ELF (Linux), macOS Mach-O.
- Detecció de **programari maliciós en documents**: PDF, Office (OLE2, OOXML), RTF, HTML.
- Suport per a **correus electrònics** (MIME, eml, mbox).
- Motor d'**expressions regulars** per a heurístiques.
- Integració nativa amb **servidors de correu** (Postfix, Sendmail, Exim, etc.) via `clamav-milter` o `amavisd`.
- Interfície de **dimoni** (ClamD) per a escaneig en temps real d'alt rendiment.
- Actualització automàtica de bases de dades via **FreshClam**.
- Disponible per a Linux, macOS, Windows i FreeBSD.

3. Components principals

Component	Descripció
`clamscan`	Eina CLI per escaneig manual de fitxers i directoris
`clamd`	Dimoni en segon pla per a escaneig eficient
`clamdscan`	Client que envia fitxers al dimoni `clamd`
`freshclam`	Actualitzador automàtic de la base de dades de virus
`sigtool`	Eina per crear i verificar signatures
`clambc`	Compilador de bytecode per a regles avançades
`clamav-milter`	Integració amb MTA (Mail Transfer Agents)

4. Instal·lació

Debian / Ubuntu

```
sudo apt update
sudo apt install clamav clamav-daemon clamav-freshclam
```

Fedora / RHEL / CentOS

```
sudo dnf install clamav clamav-update clamd
```

Arch Linux / Manjaro

```
sudo pacman -S clamav
```

Des de codi font

```
# Dependències: cmake, openssl, libxml2, libpcre2, libbz2, zlib
git clone https://github.com/Cisco-Talos/clamav.git
cd clamav
mkdir build && cd build
cmake ..
make -j$(nproc)
sudo make install
```

5. Configuració inicial

5.1. Actualitzar la base de dades

Abans del primer ús cal baixar les signatures:

```
sudo systemctl stop clamav-freshclam   # si el servei ja corre
sudo freshclam
sudo systemctl start clamav-freshclam
```

5.2. Fitxers de configuració principals

Fitxer	Propòsit
`/etc/clamav/freshclam.conf`	Configuració de FreshClam
`/etc/clamav/clamd.conf`	Configuració del dimoni ClamD

5.3. Configuració mínima de `clamd.conf`

```
LocalSocket /var/run/clamav/clamd.ctl
User clamav
DatabaseDirectory /var/lib/clamav
LogFile /var/log/clamav/clamd.log
MaxFileSize 100M
MaxScanSize 400M
```

5.4. Configuració mínima de `freshclam.conf`

```
DatabaseOwner clamav
UpdateLogFile /var/log/clamav/freshclam.log
DatabaseMirror database.clamav.net
Checks 24
```

6. Ús de `clamscan`

6.1. Sintaxi bàsica

```
clamscan [opcions] [ruta]
```

6.2. Exemples habituals

```
# Escaneig d'un fitxer
clamscan fitxer.pdf

# Escaneig recursiu d'un directori
clamscan -r /home/usuari/

# Escaneig recursiu mostrant només fitxers infectats
clamscan -r --infected /home/

# Escaneig recursiu eliminant fitxers infectats
clamscan -r --remove /directori/

# Moure fitxers infectats a quarantena
clamscan -r --move=/var/quarantena /home/

# Escaneig de tot el sistema (excloent /proc, /sys, /dev)
clamscan -r --exclude-dir="^/proc" --exclude-dir="^/sys"
 ↪  --exclude-dir="^/dev" /

# Desar informe en fitxer de log
clamscan -r /home/ --log=/var/log/clamav/scan.log

# Escaneig amb múltiples fils (ClamAV >= 0.100)
clamscan -r --max-threads=4 /home/
```

6.3. Opcions més importants

Opció	Descripció
`-r`	Recursiu
`--infected` / `-i`	Mostra només fitxers infectats
`--remove`	Elimina fitxers infectats
`--move=DIR`	Mou fitxers infectats al directori especificat
`--copy=DIR`	Copia fitxers infectats (no els elimina)
`--log=FILE`	Desa el resultat al fitxer indicat
`--exclude=REGEX`	Exclou fitxers que coincideixen amb el patró
`--exclude-dir`	Exclou directoris
`--max-filesize=N`	Mida màxima de fitxer a escanejar
`--no-summary`	Suprimeix el resum final
`--bell`	Sona un avís quan troba una amenaça
`--stdout`	Envia resultats a stdout

`--quiet`	Silenciós (errors i infeccions)

7. Ús de `clamdscan` (amb dimoni)

`clamdscan` envia fitxers al dimoni `clamd`, que ja té les signatures carregades en memòria. És molt més ràpid que `clamscan` per a escaneigs repetitius.

```
# Iniciar el dimoni
sudo systemctl start clamav-daemon   # Debian/Ubuntu
sudo systemctl start clamd           # Fedora/RHEL

# Escaneig via dimoni
clamdscan /home/usuari/documents/

# Escaneig recursiu
clamdscan -r /home/

# Multifil
clamdscan --fdpass -r /home/
```

8. FreshClam --- Actualització de signatures

```
# Actualització manual
sudo freshclam

# Estat del servei d'actualització automàtica
sudo systemctl status clamav-freshclam

# Activar actualització automàtica a l'arrencada
sudo systemctl enable --now clamav-freshclam
```

8.1. Bases de dades oficials

Fitxer	Contingut
`main.cvd`	Signatures principals (estables)
`daily.cvd`	Signatures diàries (actualitzades contínuament)
`bytecode.cvd`	Regles de bytecode avançades

Ubicació per defecte: `/var/lib/clamav/`

9. Signatures personalitzades

ClamAV permet crear signatures pròpies.

9.1. Signature de cadena hexadecimal (`.hdb`)

```
# Format: MD5:tamany:NomSignatura
d41d8cd98f00b204e9800998ecf8427e:0:Fitxer_Buit_Test
```

9.2. Signature de patró (`sigtool`)

```
# Crear una signatura des d'un fitxer maliciós
sigtool --md5 fitxer_malicos.exe >> /etc/clamav/custom.hdb

# Verificar la signatura
sigtool --info /var/lib/clamav/daily.cvd
```

9.3. Regles YARA (ClamAV >= 0.99)

ClamAV suporta regles YARA directament:

```
rule ExempleRegla {
    meta:
        description = "Detecció de prova"
    strings:
        $a = "malware_string"
    condition:
        $a
}
```

Desa el fitxer com `.yara` o `.yar` al directori de bases de dades.

10. Integració amb correu electrònic

10.1. Amb Postfix + Amavisd-new

```
sudo apt install amavisd-new clamav-daemon
# Afegir a /etc/amavis/conf.d/15-content_filter_mode:
# @bypass_virus_checks_maps = (1);  # per desactivar
# @virus_scanners = ('ClamAV');
```

10.2. Amb clamav-milter (directe a Postfix)

```
sudo apt install clamav-milter
# /etc/clamav/clamav-milter.conf:
MilterSocket /var/spool/postfix/clamav/clamav.sock
```

11. OnAccessScanning --- Escaneig en temps real

Disponible a Linux via **fanotify** (nucli >= 3.8):

```
# /etc/clamav/clamd.conf
OnAccessIncludePath /home
OnAccessExcludeUname clamav
OnAccessPrevention yes
OnAccessExtraScanning yes
```

```
# Activar (requereix root i nucli compatible)
sudo clamonacc --config=/etc/clamav/clamd.conf
```

NOTA

L'escaneig en temps real consumeix recursos considerables. Recomanat només en servidors crítics.

12. Rendiment i ajustaments

Paràmetre (clamd.conf)	Recomanació
`MaxFileSize`	100M (ajustar segons necessitat)
`MaxScanSize`	400M
`MaxRecursion`	16
`MaxFiles`	10000
`StreamMaxLength`	100M
`MaxThreads`	10--20 (en servidors)
`ReadTimeout`	180
`IdleTimeout`	30

13. Automatització amb cron

```
# Escaneig diari a les 02:00 del directori /home
0 2 * * * root clamscan -r /home/ --infected
 ↪  --log=/var/log/clamav/scan_$(date +\%F).log

# Escaneig setmanal complet (diumenge a les 03:00)
0 3 * * 0 root clamscan -r / --exclude-dir="^/proc"
 ↪  --exclude-dir="^/sys" \
  --exclude-dir="^/dev" --infected
   ↪  --log=/var/log/clamav/full_scan_$(date +\%F).log
```

14. Codi de sortida (`exit codes`)

Codi	Significat
`0`	Cap amenaça trobada
`1`	Amenaça/es trobada/es
`2`	Error durant l'escaneig

Útil per a scripts:

```
clamscan -r /home/usuari/
if [ $? -eq 1 ]; then
    echo "ALERTA: virus detectat!" | mail -s "ClamAV Alert"
     ↪  admin@example.com
fi
```

15. Limitacions conegudes

- **No és un antivirus en temps real** per defecte (cal configurar OnAccess explícitament).
- La seva taxa de detecció és **inferior** a solucions comercials en amenaces de zero-day.
- El dimoni `clamd` pot consumir **molta memòria RAM** (400--800 MB) en carregar totes les signatures.
- No detecta amenaces noves sense actualitzar les bases de dades.
- En Windows, la protecció en temps real és molt limitada comparada amb AV comercials.

16. Alternatives i comparativa

Eina	Llicència	Temps real	Plataforma	Cas d'ús principal
ClamAV	GPL v2	Opcional	Multi	Servidors de correu, escaneig programat
Sophos (free)	Propietari	Sí	Linux/Mac	Estacions de treball corporatives
ESET NOD32	Propietari	Sí	Multi	Desktop/servidor corporatiu
Maldet (LMD)	GPL	No	Linux	Allotjament web compartit
Chkrootkit	GPL	No	Unix/Linux	Detecció de rootkits
Rkhunter	GPL	No	Unix/Linux	Detecció de rootkits

17. Recursos oficials

- **Web oficial:** https://www.clamav.net
- **Documentació:** https://docs.clamav.net
- **Codi font (GitHub):** https://github.com/Cisco-Talos/clamav
- **Bases de dades de signatures:** https://www.clamav.net/downloads
- **Fòrum i suport:** https://blog.clamav.net

Versions d'aquest document

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