Wazuh

Índex

Cicle formatiu: CFGM Sistemes Microinformàtics i Xarxes (SMX) / CFGS Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0226 - Seguretat Informàtica (RA3) / 0378 - Seguretat i alta disponibilitat (RA2)

Sistema operatiu: Ubuntu Server 26.04 LTS

Figura 1: Wazuh logo

1. Introducció

Wazuh és una plataforma de codi font obert que combina **SIEM** (Security Information and Event Management) i **XDR** (Extended Detection and Response). Permet monitorar servidors i endpoints per detectar activitat sospitosa, verificar la integritat de fitxers, escanejar vulnerabilitats i complir normatives de seguretat.

Aquest document mostra la instal·lació **all-in-one** (tots els components en una sola màquina) sobre **Ubuntu Server 26.04 LTS**, adequada per a un entorn de laboratori o per a monitorar fins a un centenar d'agents.

AVÍS

A la data de creació d'aquest document, la documentació oficial de Wazuh encara llista com a sistemes suportats oficialment Ubuntu 16.04 fins a 24.04. El suport per a Ubuntu 26.04 està en fase de suport preliminar (hi ha tasques obertes al dipòsit de Wazuh per validar-lo tant a l'agent com als components centrals). A la pràctica, els paquets `.deb` genèrics funcionen sense problemes perquè Wazuh no depèn de particularitats de la versió d'Ubuntu més enllà de `systemd` i `apt`, però en un entorn de producció convé revisar l'estat de suport oficial abans de desplegar-hi. Per a un lab docent, com el que es descriu aquí, no hi ha cap inconvenient.

2. Wazuh dins el context SIEM

Un **SIEM** és una plataforma que centralitza la recollida, l'anàlisi i la correlació de dades de seguretat provinents de múltiples fonts (firewalls, IDS/IPS, servidors, aplicacions, dispositius de xarxa i endpoints), amb l'objectiu de detectar amenaces, respondre a incidents i facilitar el compliment normatiu. Combina dues funcions:

- **SIM** (Security Information Management): emmagatzematge i anàlisi a llarg termini dels registres, útil per a investigacions forenses i auditories.
- **SEM** (Security Event Management): monitoratge i correlació en temps real per detectar anomalies de manera immediata.

El flux habitual d'un SIEM és: recollida de dades → normalització → correlació d'esdeveniments → generació d'alertes → emmagatzematge/anàlisi històrica → visualització → (opcionalment) resposta automatitzada. Wazuh és una de les solucions SIEM de codi font obert més utilitzades, juntament amb alternatives comercials com Splunk, Elastic SIEM o Datadog SIEM, gràcies al seu baix cost i a la integració nativa amb capacitats XDR.

3. Arquitectura

Wazuh es compon de tres serveis centrals, que en aquesta instal·lació conviuran en el mateix host:

Component	Funció	Port
Wazuh indexer	Emmagatzematge i cerca (fork d'OpenSearch)	9200/TCP
Wazuh server	Motor d'anàlisi, regles i gestió d'agents	1514, 1515, 1516, 55000/TCP
Wazuh dashboard	Interfície web (basada en OpenSearch Dashboards)	443/TCP

Els **agents** són programes lleugers instal·lats a cada màquina monitorada, que envien dades cap al servidor a través del port 1514 (esdeveniments) i s'enrolen pel port 1515.

4. Requisits

- Ubuntu Server 26.04 LTS (64 bits), instal·lació neta
- Mínim: 4 GB de RAM (l'indexer, per si sol, ja vol 2 GB); recomanat 8 GB o més per anar còmode.
- Mínim 40 GB de disc; l'emmagatzematge d'alertes creix ràpidament amb la retenció.
- Accés `root` o `sudo`.
- Nom d'host resoluble o IP estàtica.
- Ports oberts: 443/TCP (dashboard), 1514/TCP (esdeveniments d'agents), 1515/TCP (enrollment), 55000/TCP (API, opcional si es vol accedir-hi des de fora).

Si a la màquina hi ha hagut prèviament una instal·lació d'OpenSearch, Elasticsearch o MongoDB, cal purgar-la abans, ja que l'instal·lador de Wazuh no conviu bé amb restes d'aquests serveis.

Comprova la RAM disponible:

```
free -h
```

5. Wazuh manager per dins

Wazuh manager (el “cervell” del servidor) no és un únic procés, sinó un conjunt de dimonis especialitzats que treballen coordinats:

Dimoni	Funció
`wazuh-remoted`	Rep i xifra la comunicació amb els agents
`wazuh-analysisd`	Descodifica els esdeveniments i els contrasta amb el conjunt de regles per generar alertes
`wazuh-syscheckd`	Motor de monitoratge d'integritat de fitxers (FIM)
`wazuh-authd`	Gestiona el registre (enrollment) de nous agents
`filebeat`	Reenvia els esdeveniments processats cap al Wazuh indexer

Quan un agent detecta un esdeveniment (un canvi a un fitxer, un intent d'autenticació fallit, una entrada de log sospitosa…), l'envia xifrat al manager. Aquest el descodifica, l'analitza contra milers de regles predefinides (i personalitzables) per detectar patrons d'atac, escalades de privilegis o comportaments anòmals, i si hi ha coincidència genera una alerta amb informació de severitat i context. Aquesta alerta s'envia a l'indexer per quedar emmagatzemada i visible al tauler de control. Opcionalment, el manager pot executar una **resposta activa** (bloquejar una IP, tancar una sessió, executar un script de remediació) sense intervenció manual.

El manager pot funcionar en clúster (múltiples nodes) per a alta disponibilitat, tot i que en aquest tutorial es fa servir la configuració d'un sol node, adequada per a un lab.

6. Prepara el sistema

Actualitza la llista de paquets:

```
sudo apt update
```

Actualitza els paquets:

```
sudo apt upgrade
```

Instal·la les dependències bàsiques:

```
sudo apt install curl apt-transport-https unzip wget libcap2-bin
```

L'indexer (OpenSearch) necessita augmentar el límit de `mmap` per funcionar correctament:

```
cat << 'EOF' | sudo tee /etc/sysctl.d/99-wazuh.conf
# Augmenta les àrees de memòria virtual per a l'indexer de Wazuh
vm.max_map_count=262144
EOF
```

Recarrega tots els paràmetres del kernel definits als fitxers de configuració de `sysctl`, aplicant-los en calent sense necessitat de reiniciar:

```
sudo sysctl --system
```

```
* Applying /usr/lib/sysctl.d/10-apparmor.conf ...
* Applying /usr/lib/sysctl.d/10-coredump-debian.conf ...
* Applying /usr/lib/sysctl.d/50-default.conf ...
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...
* Applying /usr/lib/sysctl.d/55-bufferbloat.conf ...
* Applying /usr/lib/sysctl.d/55-console-messages.conf ...
* Applying /usr/lib/sysctl.d/55-ipv6-privacy.conf ...
* Applying /usr/lib/sysctl.d/55-kernel-hardening.conf ...
* Applying /usr/lib/sysctl.d/55-magic-sysrq.conf ...
* Applying /usr/lib/sysctl.d/55-map-count.conf ...
* Applying /usr/lib/sysctl.d/55-network-security.conf ...
* Applying /usr/lib/sysctl.d/55-ptrace.conf ...
* Applying /usr/lib/sysctl.d/55-zeropage.conf ...
* Applying /etc/sysctl.d/99-wazuh.conf ...
kernel.apparmor_restrict_unprivileged_userns = 1
kernel.apparmor_restrict_unprivileged_unconfined = 1
kernel.core_pattern = core
kernel.sysrq = 0x01b6
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.enp0s3.rp_filter = 2
net.ipv4.conf.enp0s8.rp_filter = 2
net.ipv4.conf.lo.rp_filter = 2
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.enp0s3.accept_source_route = 0
net.ipv4.conf.enp0s8.accept_source_route = 0
net.ipv4.conf.lo.accept_source_route = 0
net.ipv4.conf.default.promote_secondaries = 1
net.ipv4.conf.enp0s3.promote_secondaries = 1
net.ipv4.conf.enp0s8.promote_secondaries = 1
net.ipv4.conf.lo.promote_secondaries = 1
net.ipv4.ping_group_range = 0 2147483647
net.core.default_qdisc = fq_codel
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
fs.protected_regular = 2
fs.protected_fifos = 1
vm.max_map_count = 1048576
kernel.pid_max = 4194304
net.core.default_qdisc = fq_codel
kernel.printk = 4 4 1 7
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
kernel.kptr_restrict = 1
kernel.sysrq = 176
vm.max_map_count = 1048576
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
kernel.yama.ptrace_scope = 1
vm.mmap_min_addr = 65536
```

```
vm.max_map_count = 262144
```

Consulta el valor actual del paràmetre del kernel `vm.max_map_count`:

```
sysctl vm.max_map_count
```

Sortida esperada:

```
vm.max_map_count = 262144
```

7. Instal·la amb l'assistent oficial (mètode recomanat)

Wazuh proporciona un script assistit que instal·la i configura automàticament els tres components. És el mètode més ràpid per a un lab d'un sol node. Descarrega l'script d'instal·lació:

```
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh
```

Executa l'script en mode "**all-in-one**":

- Wazuh manager (el servidor central que rep i analitza els esdeveniments).
- Wazuh indexer (basat en OpenSearch, on es guarden i indexen les dades).
- Wazuh dashboard (la interfície web, basada en Kibana/OpenSearch Dashboards).

```
sudo bash ./wazuh-install.sh -a
```

El procés triga entre 15 i 20 minuts. Es pot seguir el progrés en directe amb `sudo tail -f /var/log/wazuh-install.log`

```
09/07/2026 09:02:47 INFO: Starting Wazuh installation assistant. Wazuh
 ↪  version: 4.14.6
09/07/2026 09:02:47 INFO: Verbose logging redirected to
 ↪  /var/log/wazuh-install.log
09/07/2026 09:02:48 INFO: The recommended systems are: Red Hat
 ↪  Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Amazon
 ↪  Linux 2023; Ubuntu 16.04, 18.04, 20.04, 22.04; Rocky Linux 9.4.
09/07/2026 09:02:48 WARNING: The current system does not match with
 ↪  the list of recommended systems. The installation may not work
 ↪  properly.
09/07/2026 09:02:51 INFO: Verifying that your system meets the
 ↪  recommended minimum hardware requirements.
09/07/2026 09:02:51 INFO: Wazuh web interface port will be 443.
09/07/2026 09:02:55 INFO: --- Dependencies ----
09/07/2026 09:02:55 INFO: Installing debhelper.
09/07/2026 09:03:37 INFO: Wazuh repository added.
09/07/2026 09:03:37 INFO: --- Configuration files ---
```

```
09/07/2026 09:03:37 INFO: Generating configuration files.
09/07/2026 09:03:38 INFO: Generating the root certificate.
09/07/2026 09:03:38 INFO: Generating Admin certificates.
09/07/2026 09:03:38 INFO: Generating Wazuh indexer certificates.
09/07/2026 09:03:39 INFO: Generating Filebeat certificates.
09/07/2026 09:03:39 INFO: Generating Wazuh dashboard certificates.
09/07/2026 09:03:40 INFO: Created wazuh-install-files.tar. It
 ↪  contains the Wazuh cluster key, certificates, and passwords
 ↪  necessary for installation.
09/07/2026 09:03:40 INFO: --- Wazuh indexer ---
09/07/2026 09:03:40 INFO: Starting Wazuh indexer installation.
09/07/2026 09:04:10 INFO: Wazuh indexer installation finished.
09/07/2026 09:04:10 INFO: Wazuh indexer post-install configuration
 ↪  finished.
09/07/2026 09:04:10 INFO: Starting service wazuh-indexer.
09/07/2026 09:04:23 INFO: wazuh-indexer service started.
09/07/2026 09:04:23 INFO: Initializing Wazuh indexer cluster security
 ↪  settings.
09/07/2026 09:04:28 INFO: Wazuh indexer cluster security configuration
 ↪  initialized.
09/07/2026 09:04:28 INFO: Wazuh indexer cluster initialized.
09/07/2026 09:04:28 INFO: --- Wazuh server ---
09/07/2026 09:04:28 INFO: Starting the Wazuh manager installation.
09/07/2026 09:09:56 INFO: Wazuh manager installation finished.
09/07/2026 09:09:56 INFO: Wazuh manager vulnerability detection
 ↪  configuration finished.
09/07/2026 09:09:56 INFO: Starting service wazuh-manager.
09/07/2026 09:10:10 INFO: wazuh-manager service started.
09/07/2026 09:10:10 INFO: Starting Filebeat installation.
09/07/2026 09:10:18 INFO: Filebeat installation finished.
curl: (22) The requested URL returned error: 429
09/07/2026 09:10:28 INFO: Filebeat post-install configuration
 ↪  finished.
09/07/2026 09:10:28 INFO: Starting service filebeat.
09/07/2026 09:10:29 INFO: filebeat service started.
09/07/2026 09:10:29 INFO: --- Wazuh dashboard ---
09/07/2026 09:10:29 INFO: Starting Wazuh dashboard installation.
09/07/2026 09:17:39 INFO: Wazuh dashboard installation finished.
09/07/2026 09:17:39 INFO: Wazuh dashboard post-install configuration
 ↪  finished.
09/07/2026 09:17:39 INFO: Starting service wazuh-dashboard.
09/07/2026 09:17:40 INFO: wazuh-dashboard service started.
09/07/2026 09:17:41 INFO: Updating the internal users.
09/07/2026 09:17:45 INFO: A backup of the internal users has been
 ↪  saved in the /etc/wazuh-indexer/internalusers-backup folder.
09/07/2026 09:17:57 INFO: The filebeat.yml file has been updated to
 ↪  use the Filebeat Keystore username and password.
09/07/2026 09:18:24 INFO: Initializing Wazuh dashboard web
 ↪  application.
09/07/2026 09:18:25 INFO: Wazuh dashboard web application initialized.
09/07/2026 09:18:25 INFO: --- Summary ---
09/07/2026 09:18:26 INFO: You can access the web interface
 ↪  https://<wazuh-dashboard-ip>:443
```

```
    User: admin
    Password: xr3O4YCjzax9C15.2Re4yg4dIuO3gRkx
09/07/2026 09:18:26 INFO: Installation finished.
ramon@server:~$
```

NOTA

En Ubuntu 26.04, l'script de detecció del sistema operatiu pot no reconèixer explícitament la versió i mostrar un avís. En la majoria de casos es pot continuar sense problemes, ja que el que realment importa és que la família és Debian/Ubuntu amb `systemd`. Si el procés s'atura per aquest motiu, es pot forçar la comprovació amb la variable `WAZUH_INSTALL_SKIP_OS_CHECK=1` abans de l'ordre `sudo bash ./wazuh-install.sh -a`, o instal·lar pas a pas seguint la guia oficial per a “step by step” enllaçada als recursos. Un altre avís habitual és el de “discrepància de versions entre l'API i el tauler de control” (*API and dashboard version mismatch*), que apareix quan el dipòsit APT ha instal·lat una versió menor diferent per a `wazuh-manager` i `wazuh-dashboard`. Es corregeix fixant la mateixa versió als dos paquets amb `apt-mark hold` un cop acabada la instal·lació.

En acabar, l'script mostra l'URL del tauler de control i les credencials generades automàticament. **Cal guardar aquesta contrasenya**, ja que només es mostra una vegada. Si es perd, es pot recuperar del fitxer de credencials generat durant la instal·lació:

```
sudo tar -O -xvf wazuh-install-files.tar
 ↪  wazuh-install-files/wazuh-passwords.txt
```

8. Accedeix al tauler de control

Des d'un navegador, dins la mateixa xarxa:

```
https://<IP_DEL_SERVIDOR_WAZUH>
```

Cal iniciar sessió amb l'usuari `admin` i la contrasenya recuperada al pas anterior. El navegador mostrarà un avís de certificat no confiable perquè, per defecte, s'utilitza un certificat autosignat; per a un entorn de producció es recomana substituir-lo per un certificat vàlid (per exemple, via Let's Encrypt).

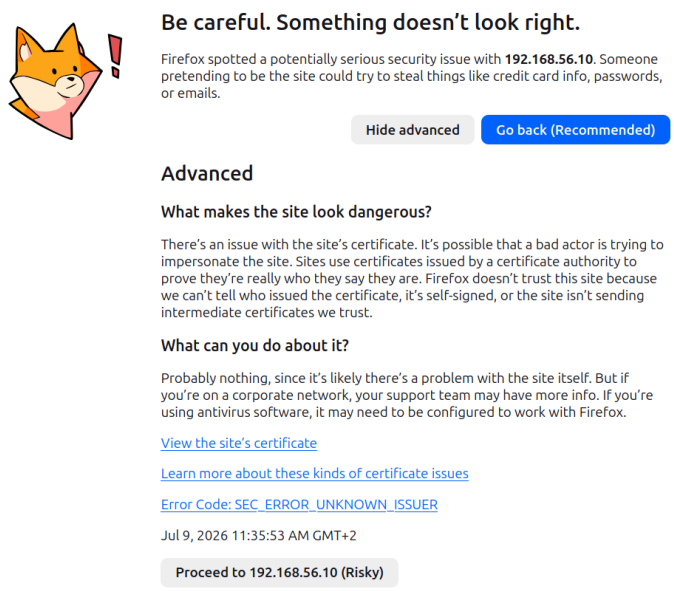

Figura 2: Avís de certificat no confiable

Figura 3: Inici de sessió

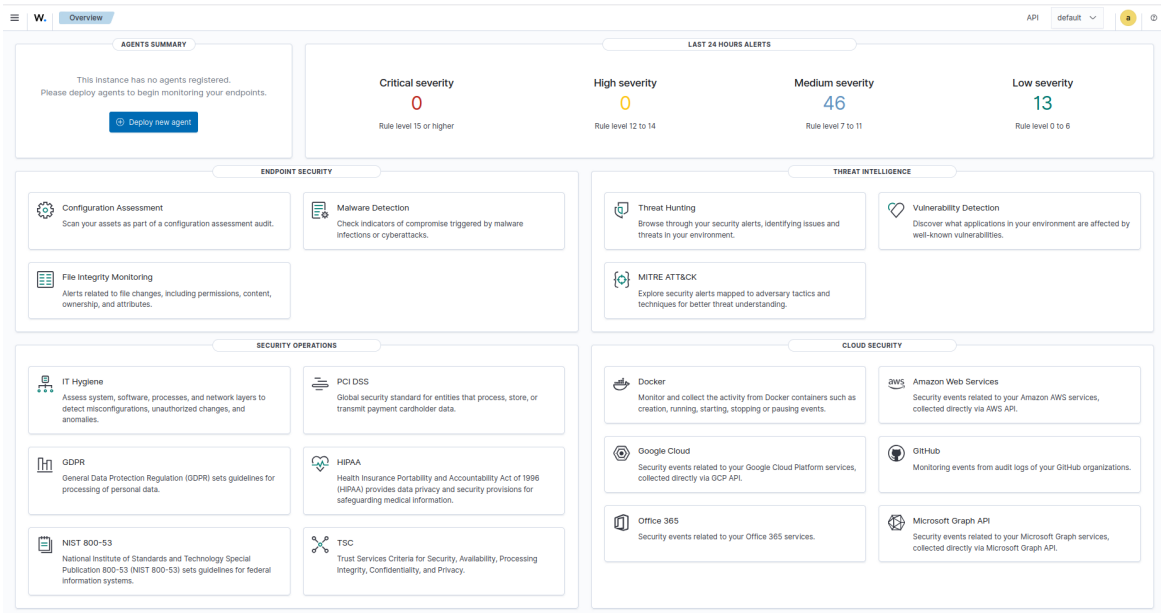

Figura 4: Tauler de control

AVÍS

Cal canviar la contrasenya per defecte de seguida. No es recomana deixar un desplegament actiu amb les credencials generades automàticament.

Per canviar la contrasenya de l'usuari `admin` s'utilitza l'script oficial de gestió de contrasenyes. La contrasenya ha de tenir una longitud entre 8 i 64 caracters i contenir com a mínim una majúscula, una minúscula, un número i un símbol(.*+?-)

En aquest exemple s'utilitza la contrasenya **+vpeMq100v** que compleix tots els requisits i resulta fàcil de recordar: *Más vale pájaro en mano que ciento volando*. ;-)

```
sudo bash /usr/share/wazuh-indexer/plugins/opensearch-security/tools
 ↪  /wazuh-passwords-tool.sh -u admin -p '+vpeMq100v'
```

```
09/07/2026 09:43:55 INFO: Updating the internal users.
09/07/2026 09:43:57 INFO: A backup of the internal users has been
 ↪  saved in the /etc/wazuh-indexer/internalusers-backup folder.
09/07/2026 09:44:01 INFO: The filebeat.yml file has been updated to
 ↪  use the Filebeat Keystore username and password.
09/07/2026 09:44:21 WARNING: Password changed. Remember to update the
 ↪  password in the Wazuh dashboard, Wazuh server, and Filebeat nodes
 ↪  if necessary, and restart the services.
```

9. Desplega un agent GNU/Linux

Els agents es despleguen a cada màquina que es vulgui monitorar. Des del mateix tauler de control (menú **Endpoints summary → Deploy new agent**) es pot generar l'ordre exacta segons el sistema operatiu i la IP del servidor. De manera manual, en un client Debian/Ubuntu.

Descarrega la clau pública GPG de Wazuh, i desa-la en un keyring propi del sistema, per poder verificar la signatura dels paquets:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH \
  | sudo gpg --no-default-keyring \
  --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import
```

```
gpg: keyring '/usr/share/keyrings/wazuh.gpg' created
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key)
 ↪  <support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Canvia els permisos:

```
sudo chmod 644 /usr/share/keyrings/wazuh.gpg
```

Crea el fitxer de definició del dipòsit APT de Wazuh, indicant a apt on trobar els paquets i amb quina clau verificar-los:

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
 ↪  https://packages.wazuh.com/4.x/apt/ stable main" | \
  sudo tee /etc/apt/sources.list.d/wazuh.list
```

Actualitza la llista de paquets:

```
sudo apt update
```

Instal·la el paquet de l'agent de Wazuh (no el manager), passant-li com a variable d'entorn la IP del servidor Wazuh al qual s'ha de connectar:

```
sudo WAZUH_MANAGER='<IP_DEL_SERVIDOR_WAZUH>' apt install -y
 ↪  wazuh-agent
```

Fes que systemd rellegeixi els `unit files` (.service, .socket, etc.) del disc:

```
sudo systemctl daemon-reload
```

Configura el servei `wazuh-agent` perquè s'engegui automàticament en arrencar el sistema i l'arrenca ara mateix:

```
sudo systemctl enable --now wazuh-agent
```

Al cap d'uns segons, l'agent hauria d'aparèixer com a **actiu** al tauler de control, dins de l'apartat d'endpoints.

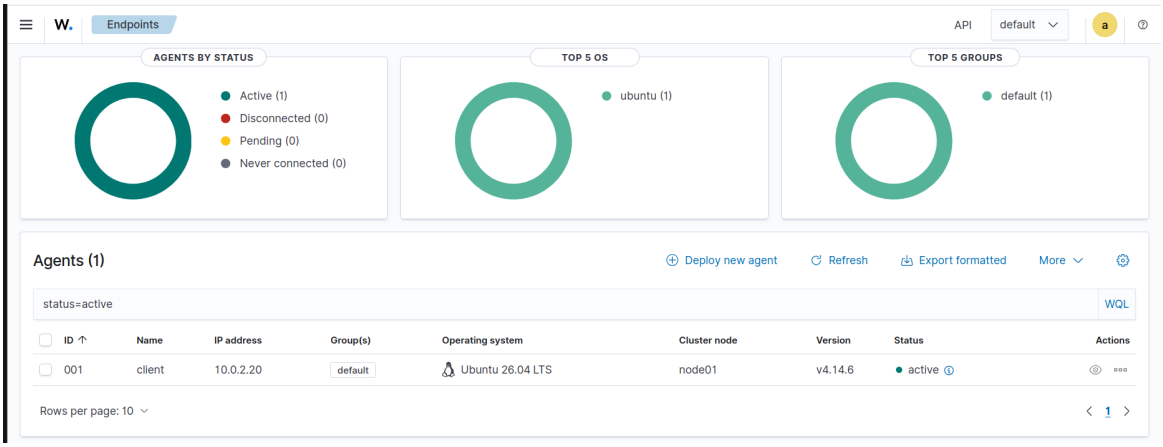

Figura 5: Endpoints

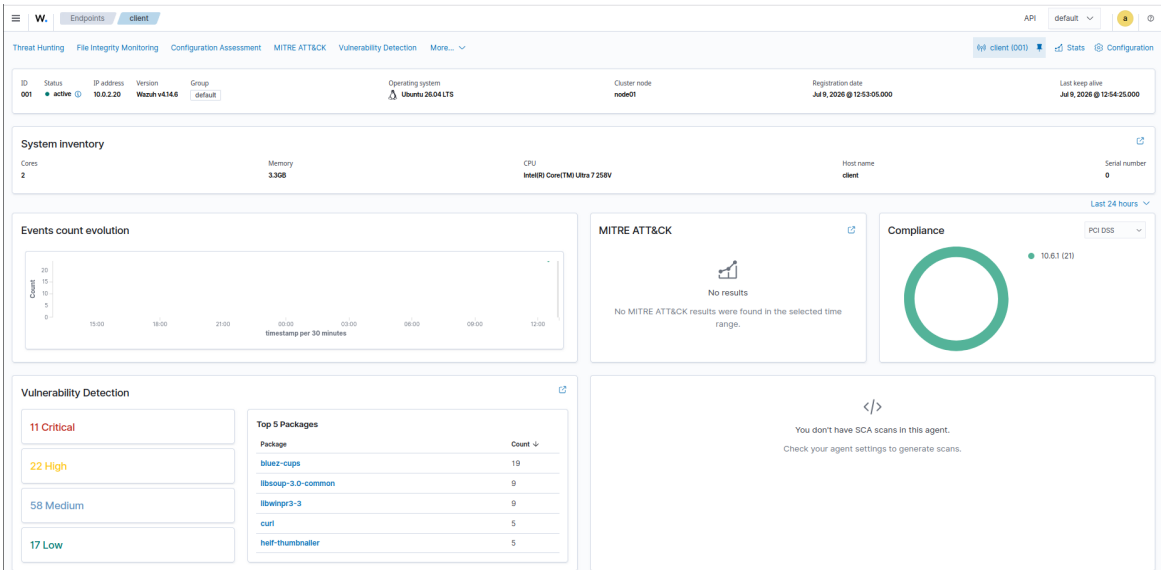

Figura 6: Informació de l'endpoint

10. Verificació bàsica

Comprova l'estat dels serveis al servidor:

```
sudo systemctl status wazuh-indexer
```

```
sudo systemctl status wazuh-manager
```

```
sudo systemctl status wazuh-dashboard
```

```
sudo systemctl status filebeat
```

NOTA

Filebeat és l'agent d'enviament de logs de l'stack Elastic/OpenSearch, i Wazuh l'utilitza internament com a mecanisme de transport: l'agent Wazuh no envia les dades directament a l'indexer, sinó que el manager (o en instal·lacions “all-in-one”, el mateix node) fa servir Filebeat per enviar els esdeveniments processats des del manager cap al Wazuh indexer (OpenSearch).

Verifica que Filebeat es connecta correctament a l'indexer:

```
sudo filebeat test output
```

11. Monitoratge d'integritat de fitxers (FIM)

Una de les funcionalitats més útils és el **File Integrity Monitoring**. S'activa a l'agent editant `/var/ossec/etc/ossec.conf`:

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<syscheck>
  <disabled>no</disabled>
  <frequency>43200</frequency>
  <directories check_all="yes"
 ↪  realtime="yes">/etc,/var/www,/etc/bind,/etc/kea</directories>
</syscheck>
```

Reinicia l'agent perquè apliqui els canvis:

```
sudo systemctl restart wazuh-agent
```

Qualsevol modificació dins d'aquests directoris (per exemple, un canvi no autoritzat a la configuració de BIND9 o de Kea) generarà una alerta al tauler de control.

12. Aplicació pràctica al laboratori

Aquesta plataforma es pot integrar directament amb la infraestructura de xarxa ja muntada:

- Desplegar un agent al **DC de Samba AD** per monitorar intents d'autenticació fallits i canvis a fitxers crítics.
- Desplegar un agent al servidor **Kea DHCP + BIND9** per vigilar canvis no autoritzats a les zones DNS o a la configuració DHCP-DDNS.
- Activar el mòdul de **detecció de vulnerabilitats**, que compara els paquets instal·lats amb bases de dades CVE, útil com a exercici pràctic del mòdul de seguretat.

13. Recursos addicionals

- Documentació oficial (índex complet): https://documentation.wazuh.com/current/index.html
- Guia d'inici ràpid: https://documentation.wazuh.com/current/quickstart.html
- Components i arquitectura: https://documentation.wazuh.com/current/getting-started/components/index.html
- Desplegament d'agents: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html
- Casos d'ús (FIM, detecció de vulnerabilitats, threat hunting, compliance…): https://documentation.wazuh.com/current/getting-started/use-cases/index.html
- Guia de proves de concepte (PoC): https://documentation.wazuh.com/current/proof-of-concept-guide/index.html --- exercicis pràctics guiats com detectar un atac de força bruta o una injecció SQL, ideals per a pràctiques d'aula.
- Wazuh manager (referència de dimonis i configuració): https://documentation.wazuh.com/current/user-manual/manager/wazuh-manager.html
- Sistemes operatius suportats (comprovar l'estat actualitzat d'Ubuntu 26.04): https://documentation.wazuh.com/current/installation-guide/wazuh-server/index.html

Índex de figures

Versions d'aquest document

- HTML
- PDF
- ODT
- MD