Incidentes de ciberseguridad

Wazuh

Jennifer

Instrucciones

Instalar y configurar Wazuh para gestionar y monitorizar incidentes de ciberseguridad mediante un sistema centralizado con manager y agentes.

Requisitos previos

Máquinas virtuales una para manager y otra agente linux

Es importante que tanto los agentes y el manager tengan la misma version para ello podemos consultar que version hay en esta pagina https://documentation.wazuh.com/current/release-notes/index-4x.html

1. **Descargar el instalador de Wazuh- manager**
   Es importante que estén los siguientes paquetes instalados y la máquina actualizada:
   sudo apt install vim curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg2
   wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo tee /etc/apt/trusted.gpg.d/elasticsearch.asc
   sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'
   sudo apt update
   sudo apt install elasticsearch
   sudo systemctl enable elasticsearch
   sudo systemctl start elasticsearc
   Este script automático instala el servidor Wazuh completo (manager, dashboard y Elasticsearch):
   curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

```
jennga@ububast:~$ curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
[sudo] password for jennga:
26/03/2025 11:12:19 INFO: Starting Wazuh installation assistant. Wazuh version: 4.5.4
26/03/2025 11:12:19 INFO: Verbose logging redirected to /var/log/wazuh-install.log
26/03/2025 11:12:29 INFO: Wazuh web interface port will be 443.
26/03/2025 11:12:31 INFO: --- Dependencies ----
26/03/2025 11:12:31 INFO: Installing apt-transport-https.
26/03/2025 11:12:35 INFO: Wazuh repository added.
26/03/2025 11:12:35 INFO: --- Configuration files ---
26/03/2025 11:12:35 INFO: Generating configuration files.
26/03/2025 11:12:36 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords n
ecessary for installation.
26/03/2025 11:12:36 INFO: --- Wazuh indexer ---
26/03/2025 11:12:36 INFO: Starting Wazuh indexer installation.
26/03/2025 11:13:27 INFO: Wazuh indexer installation finished.
26/03/2025 11:13:27 INFO: Wazuh indexer post-install configuration finished.
26/03/2025 11:13:27 INFO: Starting service wazuh-indexer.
26/03/2025 11:13:37 INFO: wazuh-indexer service started.
26/03/2025 11:13:38 INFO: Initializing Wazuh indexer cluster security settings.
26/03/2025 11:13:48 INFO: Wazuh indexer cluster initialized.
26/03/2025 11:13:48 INFO: --- Wazuh server ---
26/03/2025 11:13:48 INFO: Starting the Wazuh manager installation.
26/03/2025 11:15:02 INFO: Wazuh manager installation finished.
26/03/2025 11:15:02 INFO: Starting service wazuh-manager.
26/03/2025 11:15:18 INFO: wazuh-manager service started.
26/03/2025 11:15:18 INFO: Starting Filebeat installation.
26/03/2025 11:15:23 INFO: Filebeat installation finished.
26/03/2025 11:15:24 INFO: Filebeat post-install configuration finished.
26/03/2025 11:15:24 INFO: Starting service filebeat.
26/03/2025 11:15:25 INFO: filebeat service started.
26/03/2025 11:15:25 INFO: --- Wazuh dashboard ---
26/03/2025 11:15:25 INFO: Starting Wazuh dashboard installation.
26/03/2025 11:16:38 INFO: Wazuh dashboard installation finished.
26/03/2025 11:16:38 INFO: Wazuh dashboard post-install configuration finished.
26/03/2025 11:16:38 INFO: Starting service wazuh-dashboard.
26/03/2025 11:16:38 INFO: wazuh-dashboard service started.
26/03/2025 11:17:38 INFO: Initializing Wazuh dashboard web application.
26/03/2025 11:17:40 INFO: Wazuh dashboard web application initialized.
26/03/2025 11:17:40 INFO: --- Summary ---
26/03/2025 11:17:40 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: 676sf1NtxH.X.maDmhE0UNRFG2aMmx*p
```

   User: admin
   Password: 676sf1NtxH.X.maDmhE0UNRFG2aMmx*p

2. **Configuracion del manager**

   Es importante cambiar las credenciales que nos dieron en la hora de la instalación también que este apuntando a localhost

   sudo nano /etc/wazuh-dashboard/opensearch_dashboards.yml

```
  GNU nano 6.2                          /etc/wazuh-dashboard/opensearch_dashboards.ym
server.host: 0.0.0.0
opensearch.hosts: ["https://127.0.0.1:9200"]
server.port: 443
opensearch.ssl.verificationMode: certificate
opensearch.username: admin
opensearch.password: "676sf1NtxH.X.maDmhE0UNRFG2aMmx*p"
opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/wazuh-dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wazuh
opensearch_security.cookie.secure: true
```

Reiniciar Wazuh Dashboard:

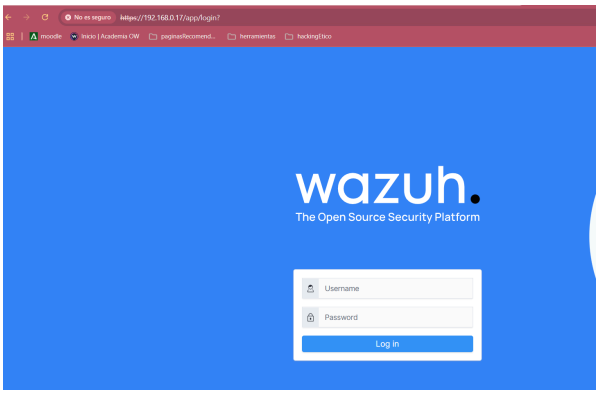
sudo systemctl restart wazuh-dashboard

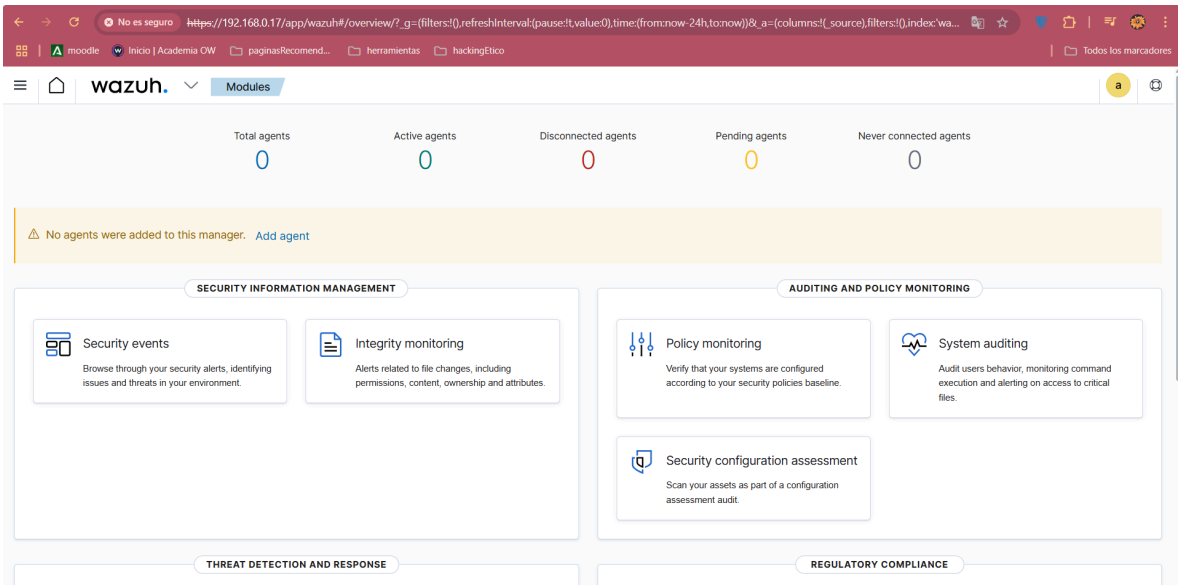
Verificar que este activo

sudo systemctl status wazuh-dashboard

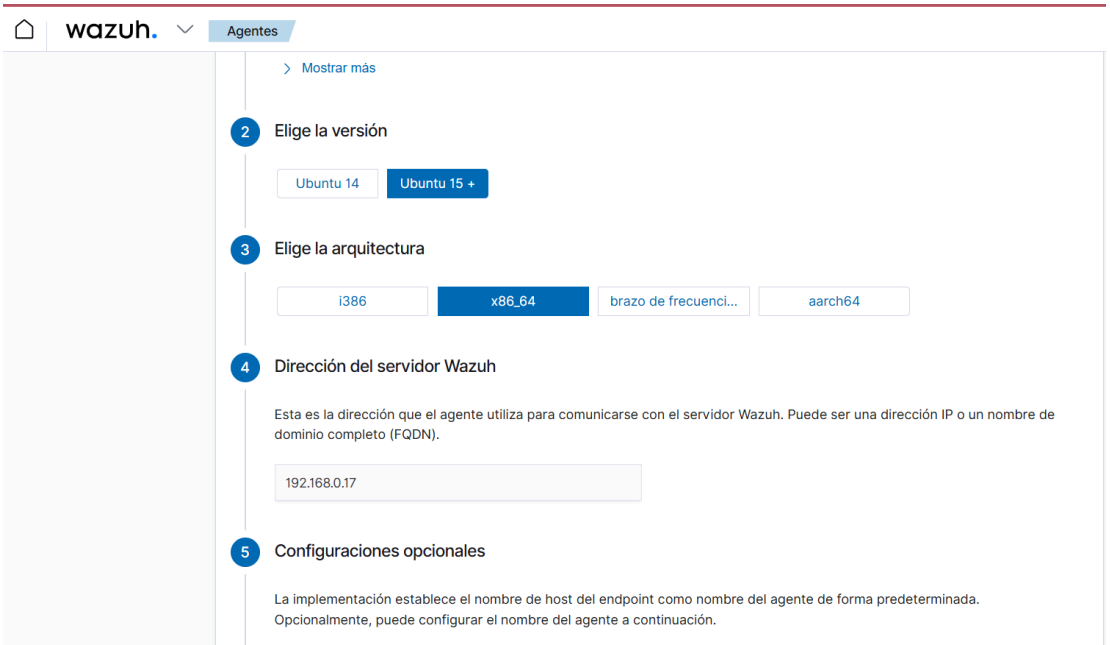
```
root@ububast:/home/jennga# sudo systemctl status wazuh-dashboard
● wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-03-26 08:56:03 UTC; 6min ago
   Main PID: 50740 (node)
      Tasks: 11 (limit: 4506)
     Memory: 148.7M
        CPU: 6.448s
     CGroup: /system.slice/wazuh-dashboard.service
             └─50740 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-rejec>

mar 26 08:56:07 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:07Z","tags":["info","pl>
mar 26 08:56:07 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:07Z","tags":["info","pl>
mar 26 08:56:07 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:07Z","tags":["info","pl>
mar 26 08:56:07 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:07Z","tags":["info","pl>
mar 26 08:56:07 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:07Z","tags":["info","sa>
mar 26 08:56:08 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:08Z","tags":["info","sa>
mar 26 08:56:08 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:08Z","tags":["info","pl>
mar 26 08:56:08 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:08Z","tags":["listening>
mar 26 08:56:08 ububast opensearch-dashboards[50740]: {"type":"log","@timestamp":"2025-03-26T08:56:08Z","tags":["info","ht>
mar 26 08:56:16 ububast opensearch-dashboards[50740]: {"type":"response","@timestamp":"2025-03-26T08:56:14Z","tags":[],"pi>
lines 1-20/20 (END)
```

Accedemos por el navegador poniendo la ip

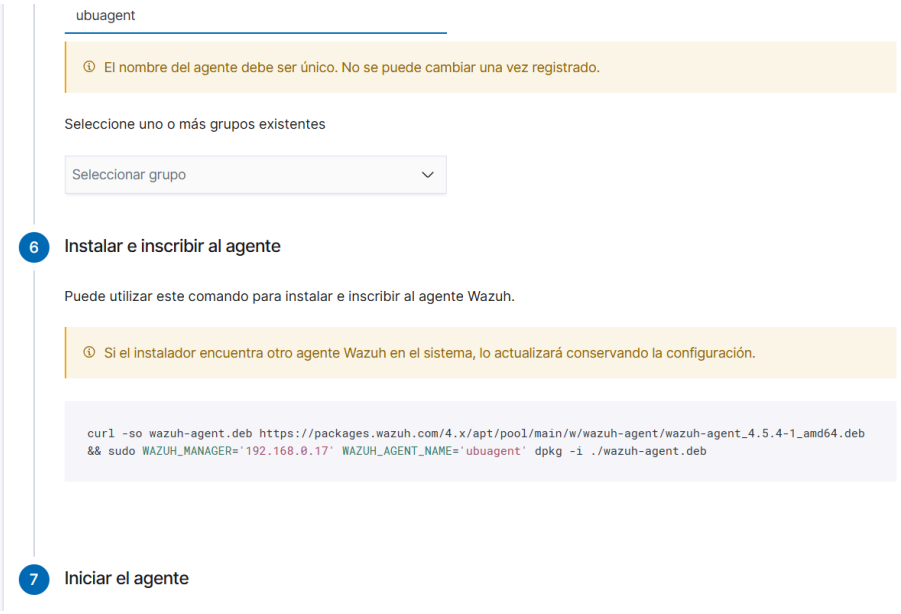




Configuramos el servidor para que pueda comunicarse con el agente en la pestaña de agente buscando Implementar un nuevo agente



nos copiamos la url que nos da para que el la maquina del agente se lo peguemos:



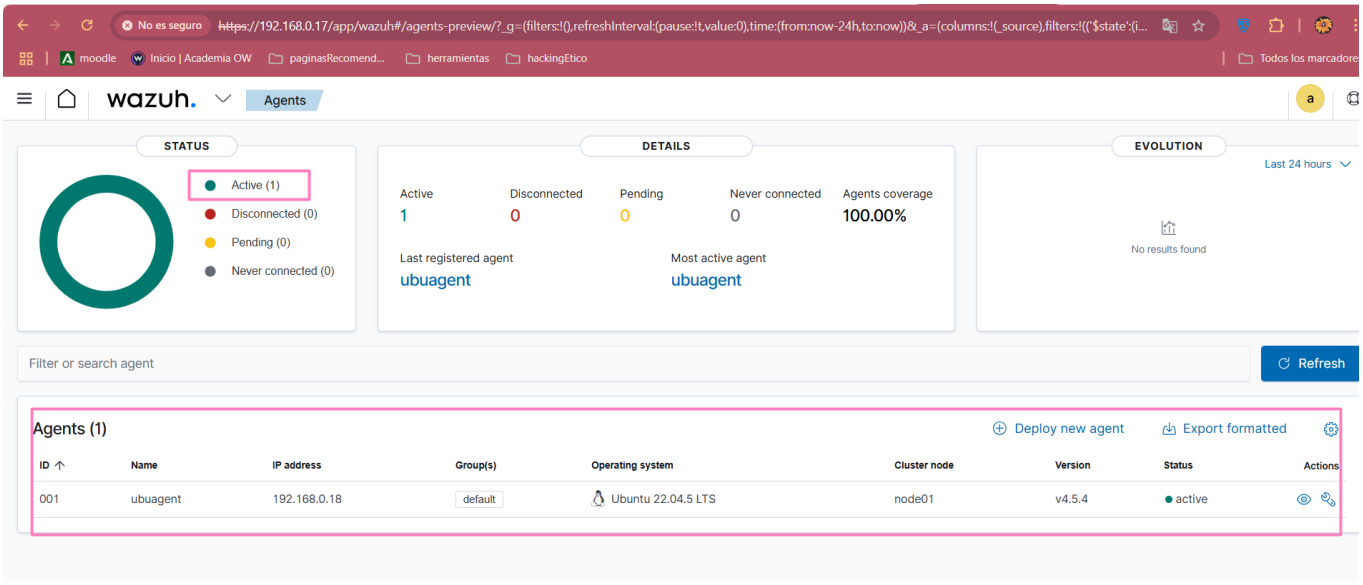
curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.5.4-1_amd64.deb && sudo WAZUH_MANAGER='192.168.0.17' WAZUH_AGENT_NAME='ubuagent' dpkg -i ./wazuh-agent.deb

3. **Instalación de los agentes Wazuh**
   Abrimo la máquina y pegamos el comando que nos puso la app:
   curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.5.4-1_amd64.deb && sudo WAZUH_MANAGER='192.168.0.17' WAZUH_AGENT_NAME='ubuagent' dpkg -i ./wazuh-agent.deb

```
jennga@ububast:~$ curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.5.4-1_a
md64.deb && sudo WAZUH_MANAGER='192.168.0.17' WAZUH_AGENT_NAME='ubuagent' dpkg -i ./wazuh-agent.deb
[sudo] password for jennga:
Seleccionando el paquete wazuh-agent previamente no seleccionado.
(Leyendo la base de datos ... 110374 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar ./wazuh-agent.deb ...
Desempaquetando wazuh-agent (4.5.4-1) ...
Configurando wazuh-agent (4.5.4-1) ...
jennga@ububast:~$
```

Después inicializamos el agente
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent

4. **En la app refrescamos la página y nos muestra lo siguiente**



Fuentes

https://github.com/hernandopena/Wazuh
https://medium.com/@fransk.roman.cambara/como-instalar-wazuh-2023-en-ubuntu-22-04-instalaci%C3%B3n-de-agentes-50cae9e23b35