

LABWAZUH 1 – Instalación y configuración de Wazuh

1. Objetivo. – Implementar y configurar la plataforma de seguridad Wazuh en Linux y agentes en Windows, con el propósito de conocer el procedimiento correcto de su instalación y utilizar sus funcionalidades en próximos laboratorios.

2. Herramientas. - Para este laboratorio se utilizarán:

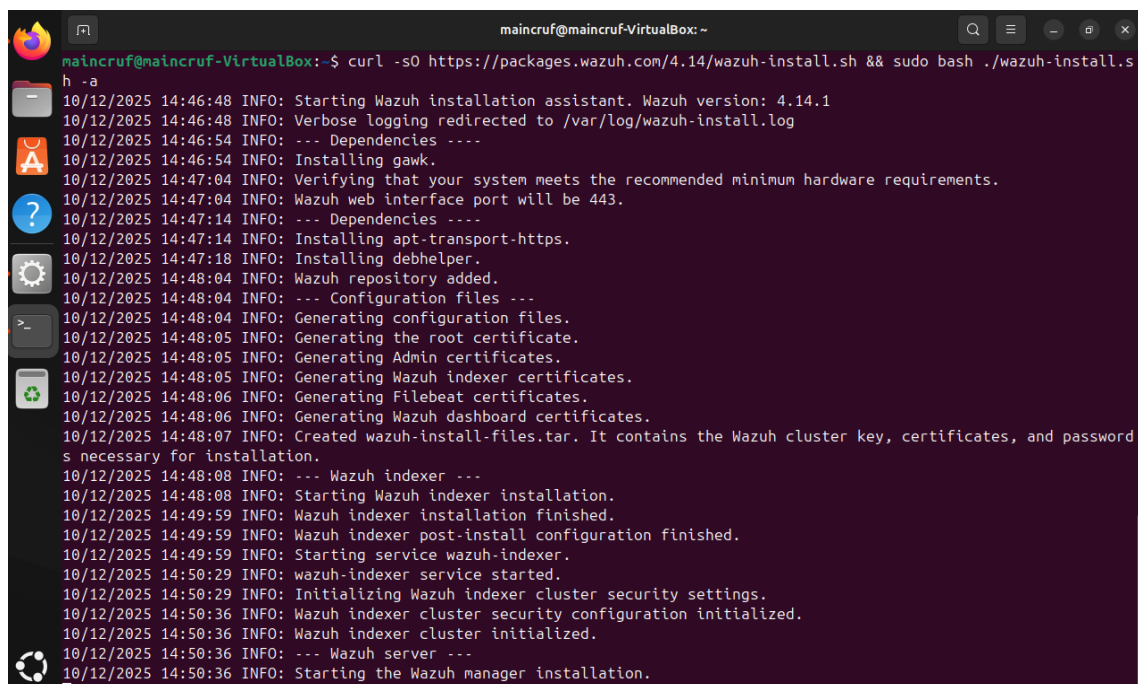
- Oracle VirtualBox.
- Maquina Windows y Cliente Ubuntu (máquina virtual)
- Wazuh.

3. Procedimiento

3.1 Instalación y configuración pfSense

1. Para realizar la instalación de Wazuh en Linux, se utiliza el comando provisto en su pagina web oficial y se lo ejecuta en la terminal, después de varios minutos la instalación se completa correctamente. (ver Figura 1)

2. Una vez instalado correctamente, Wazuh otorga un usuario y una contraseña, que permitirá y facilitara el acceso a todas sus herramientas y funcionalidades. (ver Figura 2).



```
maincruf@maincruf-VirtualBox: ~  
maincruf@maincruf-VirtualBox:~$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.s  
h -a  
10/12/2025 14:46:48 INFO: Starting Wazuh installation assistant. Wazuh version: 4.14.1  
10/12/2025 14:46:48 INFO: Verbose logging redirected to /var/log/wazuh-install.log  
10/12/2025 14:46:54 INFO: --- Dependencies ---  
10/12/2025 14:46:54 INFO: Installing gawk.  
10/12/2025 14:47:04 INFO: Verifying that your system meets the recommended minimum hardware requirements.  
10/12/2025 14:47:04 INFO: Wazuh web interface port will be 443.  
10/12/2025 14:47:14 INFO: --- Dependencies ---  
10/12/2025 14:47:14 INFO: Installing apt-transport-https.  
10/12/2025 14:47:18 INFO: Installing debhelper.  
10/12/2025 14:48:04 INFO: Wazuh repository added.  
10/12/2025 14:48:04 INFO: --- Configuration files ---  
10/12/2025 14:48:04 INFO: Generating configuration files.  
10/12/2025 14:48:05 INFO: Generating the root certificate.  
10/12/2025 14:48:05 INFO: Generating Admin certificates.  
10/12/2025 14:48:05 INFO: Generating Wazuh indexer certificates.  
10/12/2025 14:48:06 INFO: Generating Filebeat certificates.  
10/12/2025 14:48:06 INFO: Generating Wazuh dashboard certificates.  
10/12/2025 14:48:07 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and password  
s necessary for installation.  
10/12/2025 14:48:08 INFO: --- Wazuh indexer ---  
10/12/2025 14:48:08 INFO: Starting Wazuh indexer installation.  
10/12/2025 14:49:59 INFO: Wazuh indexer installation finished.  
10/12/2025 14:49:59 INFO: Wazuh indexer post-install configuration finished.  
10/12/2025 14:49:59 INFO: Starting service wazuh-indexer.  
10/12/2025 14:50:29 INFO: wazuh-indexer service started.  
10/12/2025 14:50:29 INFO: Initializing Wazuh indexer cluster security settings.  
10/12/2025 14:50:36 INFO: Wazuh indexer cluster security configuration initialized.  
10/12/2025 14:50:36 INFO: Wazuh indexer cluster initialized.  
10/12/2025 14:50:36 INFO: --- Wazuh server ---  
10/12/2025 14:50:36 INFO: Starting the Wazuh manager installation.
```

Figura 1. Instalación de Wazuh

```
10/12/2025 15:17:45 INFO: Starting Wazuh dashboard installation.
10/12/2025 15:28:18 INFO: Wazuh dashboard installation finished.
10/12/2025 15:28:19 INFO: Wazuh dashboard post-install configuration finished.
10/12/2025 15:28:19 INFO: Starting service wazuh-dashboard.
10/12/2025 15:28:20 INFO: wazuh-dashboard service started.
10/12/2025 15:28:22 INFO: Updating the internal users.
10/12/2025 15:28:31 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
10/12/2025 15:28:59 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
10/12/2025 15:29:38 INFO: Initializing Wazuh dashboard web application.
10/12/2025 15:29:38 INFO: Wazuh dashboard web application not yet initialized. Waiting...
10/12/2025 15:29:55 INFO: Wazuh dashboard web application not yet initialized. Waiting...
10/12/2025 15:30:10 INFO: Wazuh dashboard web application initialized.
10/12/2025 15:30:10 INFO: --- Summary ---
10/12/2025 15:30:10 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: NOT5fDd*julemlwhGLRvFp0*CL7UBzm0
10/12/2025 15:30:10 INFO: Installation finished.
root@maincruf-VirtualBox: /home/maincruf#
```

Figura 2. Instalación completa de Wazuh y credenciales recibidas.

3.2 Acceso a Wazuh

Para el acceso a este SIEM, necesitamos seguir los siguientes pasos.

1. Instalado Wazuh, se procede a abrir el navegador web, y escribir la ip de la maquina que servirá de servidor en la barra de búsqueda, en este caso es 192.168.0.6.
2. Al colocar las credenciales dadas por Wazuh, se dará acceso y se mostrara el overview de Wazuh. (ver Figura 3)

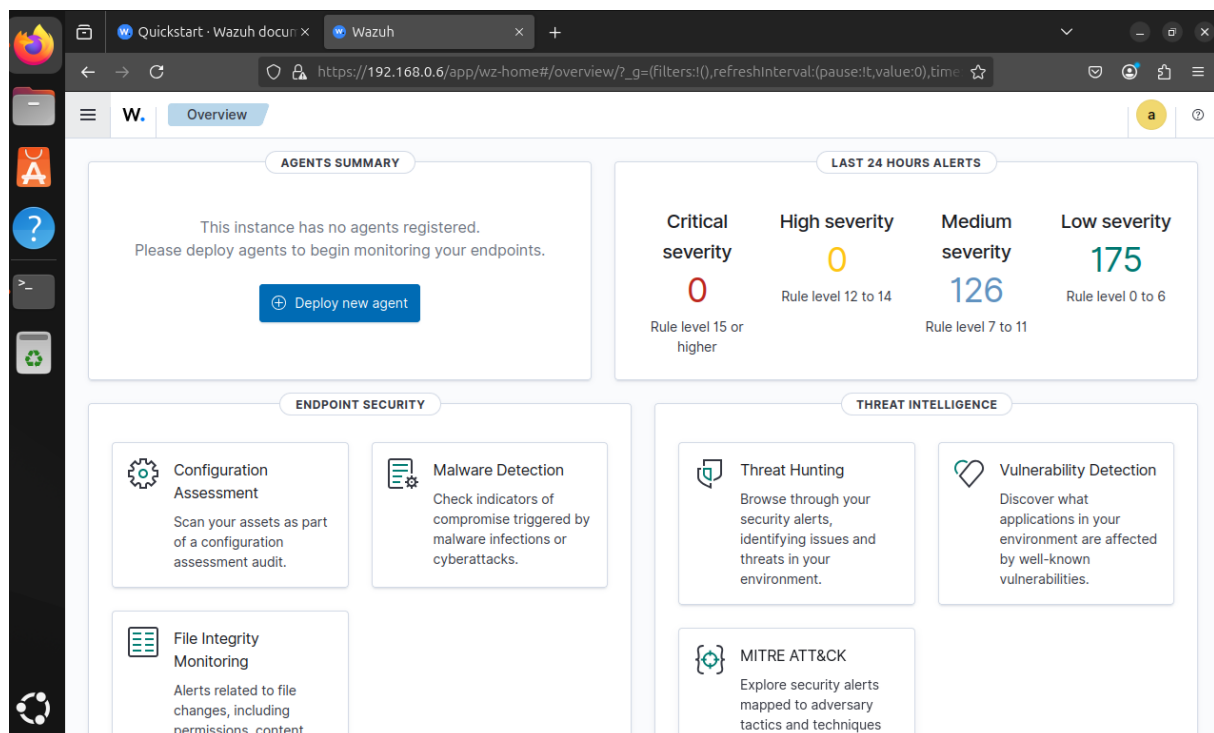


Figura 3. Overview de Wazuh.

3.3 Creación del agente de Wazuh

1. Para monitorear o recibir alertas de otros equipos se necesita crear “agentes”, para esto existe la opción “Deploy New Agent”, que permite establecer agentes fácilmente en distintos sistemas operativos, eligiendo para este laboratorio un equipo Windows. (ver Figura 4)

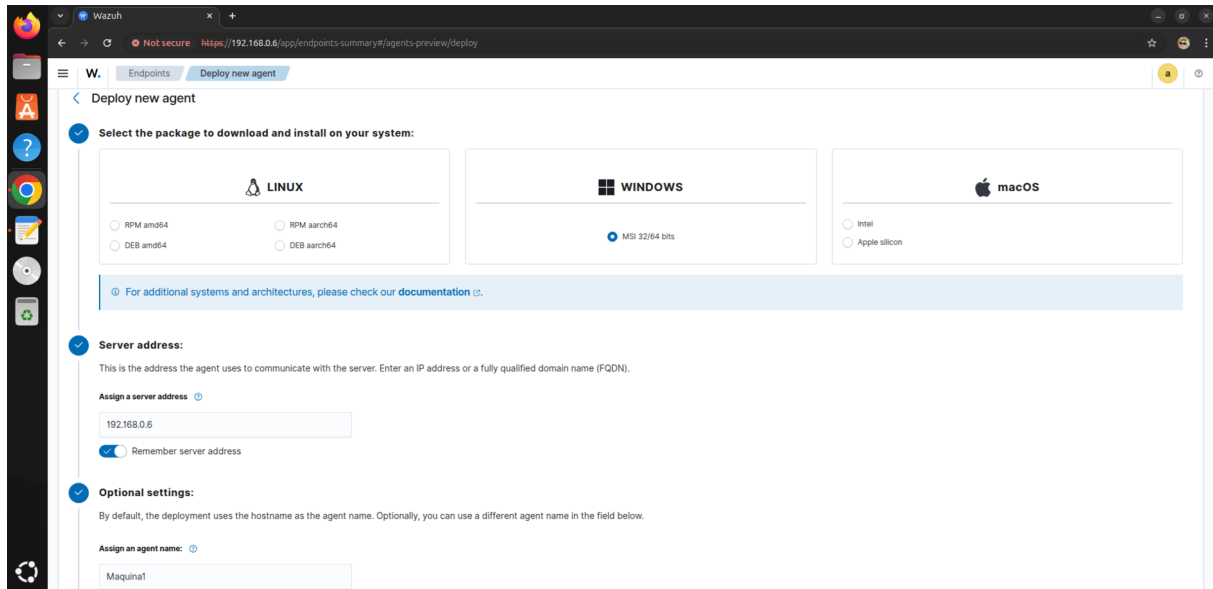


Figura 4. Creando un agente en Linux para Windows.

2. Ya creado el agente, Wazuh dará un comando para ejecutarlo en modo administrador en Windows PowerShell, de modo de que el servicio comience y así sincronizar el servidor con su agente. (ver Figura 5)

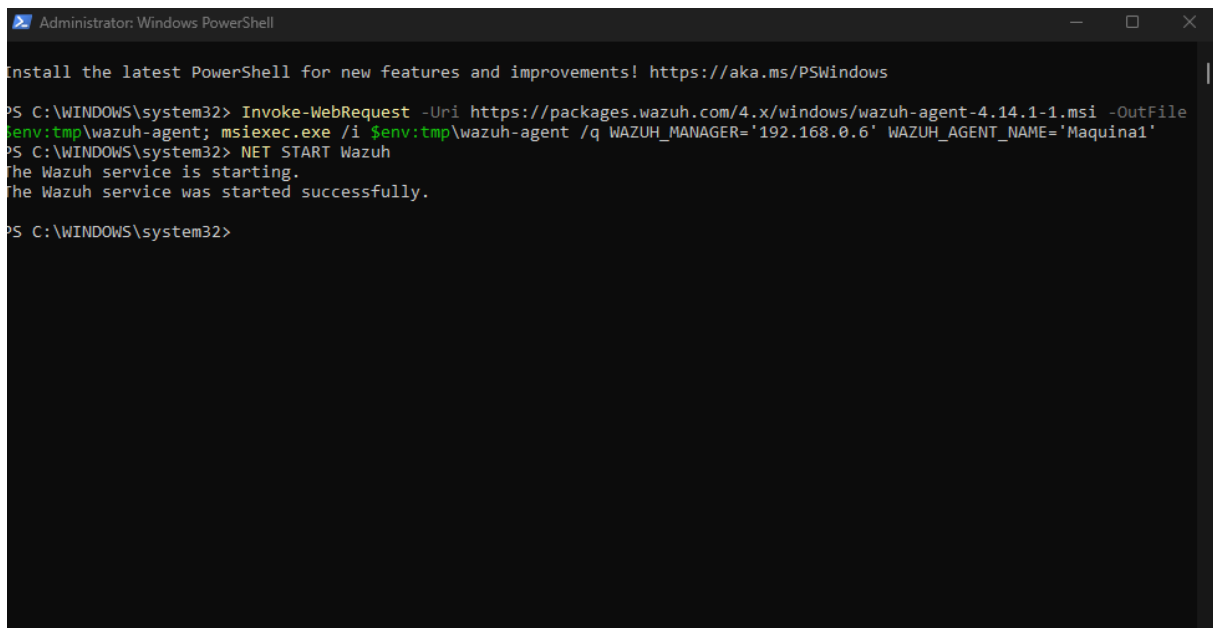


Figura 5. Instalación y funcionamiento del agente en Windows.

3. Dentro de la interfaz de Wazuh, se logra ver que el agente Windows se sincronizó correctamente con el servidor Wazuh Linux, permitiendo monitorizar y recibir alertas de ese equipo. (ver Figura 6)

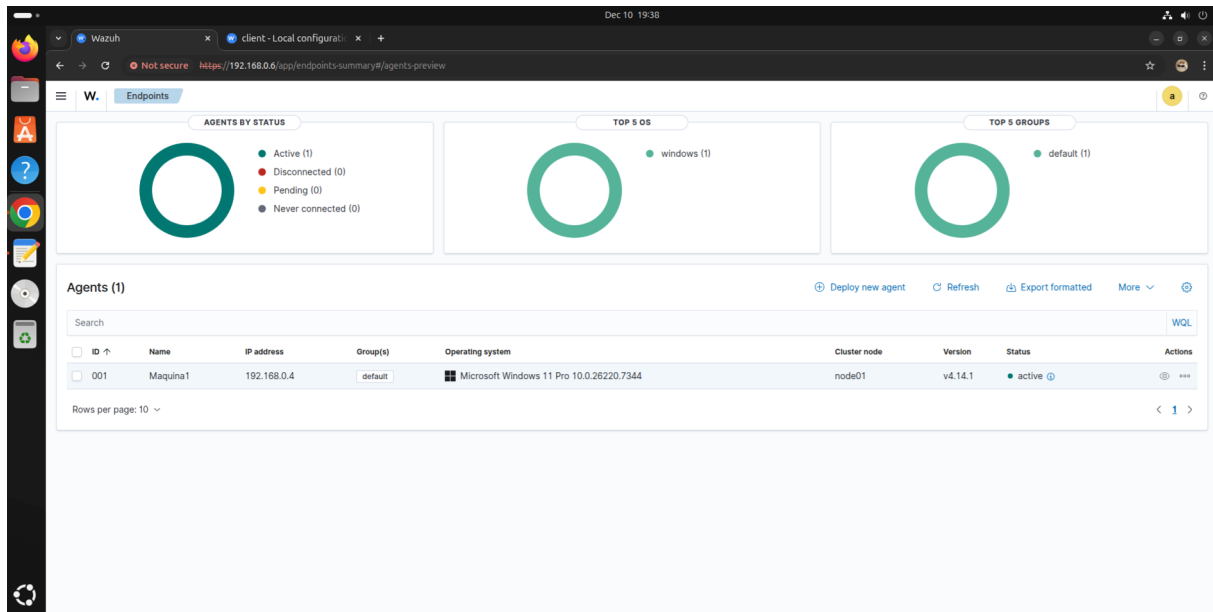


Figura 6. Agente correctamente conectado con el servidor Wazuh.

4. Resultados Obtenidos. - Durante el laboratorio se logró realizar satisfactoriamente el proceso de instalación y configuración de la plataforma SIEM. Asimismo, se implementó el agente en el equipo de Windows para permitir su monitorización, verificando la conexión entre el agente y el servidor, confirmando que el SIEM es capaz de recibir los eventos y alertas generados.

5. Reflexión final. - Este laboratorio me permitió comprender como funciona la instalación de un SIEM, y la importancia de una correcta configuración de sus agentes. Aprendiendo el valor de estas herramientas en el ámbito de la ciberseguridad, ya que permiten monitorear amenazas en tiempo real y fortalecer distintos entornos como empresas, bancos o centros educativos.