

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.

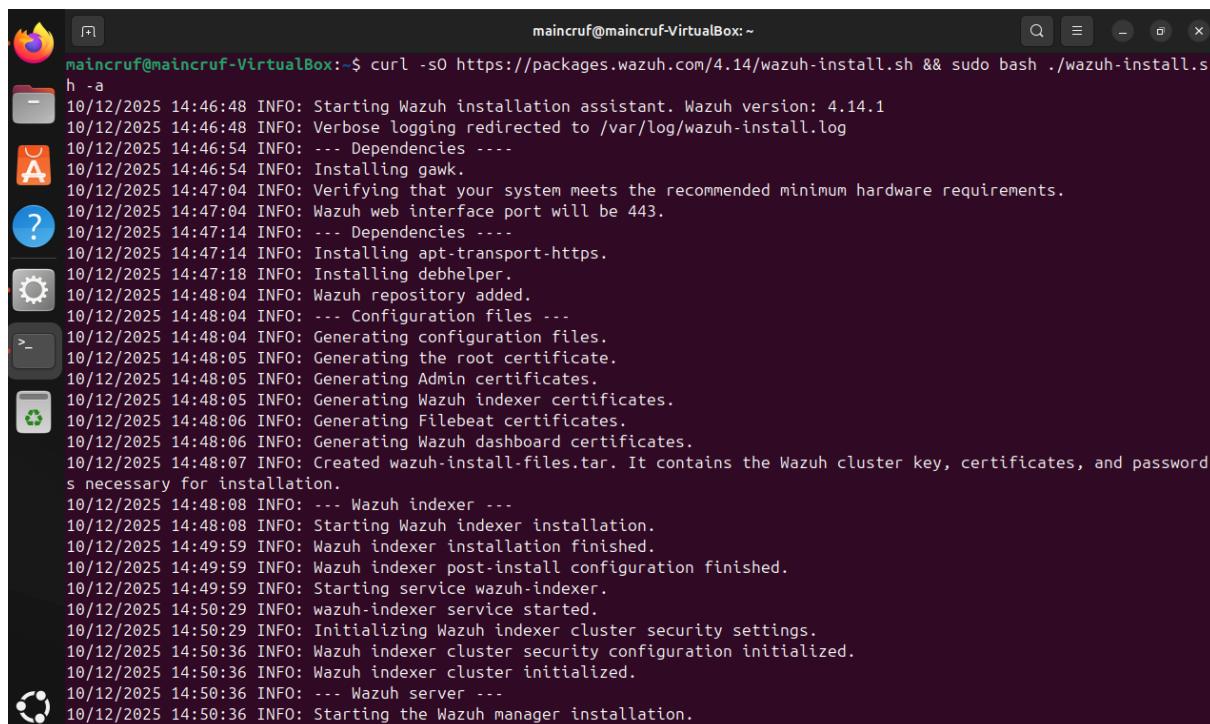
2. Herramientas. - Para este laboratorio se utilizaron:

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

3. Configuración

3.1 Servidor Wazuh

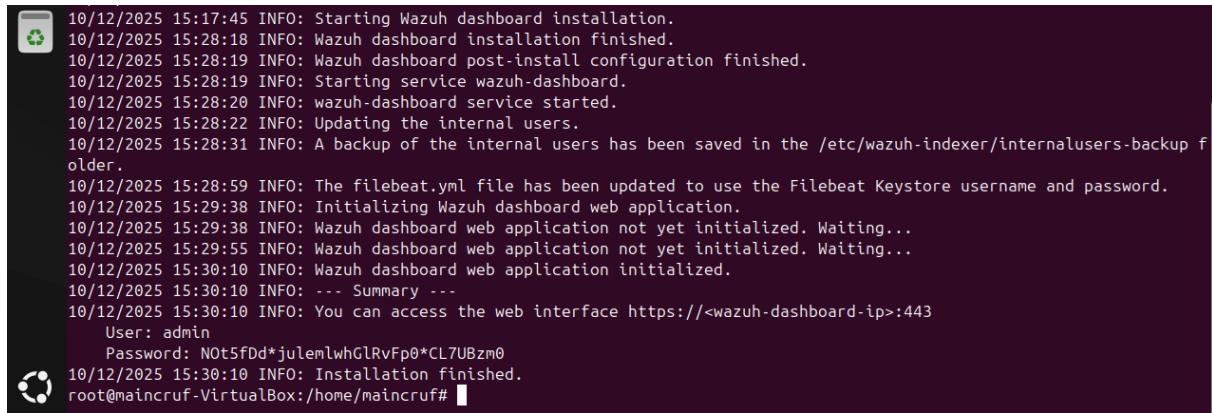
Se instaló el servidor Wazuh en Linux mediante la ejecución del comando de instalación provisto en la página web oficial de Wazuh. Después de varios minutos de espera, la instalación se completó correctamente. (ver Figura 1)



```
maincruf@maincruf-VirtualBox:~$ curl -s0 https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -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

Una vez finalizada la instalación, Wazuh facilitó un usuario y contraseña, con el propósito de facilitar el acceso a todas sus herramientas y funcionalidades. (ver Figura 2)



```

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@mainercru-VirtualBox:/home/mainercru# 
```

Figura 2. Instalación completa de Wazuh y credenciales recibidas.

3.2 Agente Wazuh

Para monitorear o recibir alertas de otros equipos se necesita crear “agentes”. Se accedió a la interfaz de Wazuh e ingresó a la opción “Deploy New Agent” (ver Figura 6). Esta opción permite establecer agentes fácilmente en distintos sistemas operativos, eligiendo para este laboratorio un equipo Windows. (ver Figura 3)

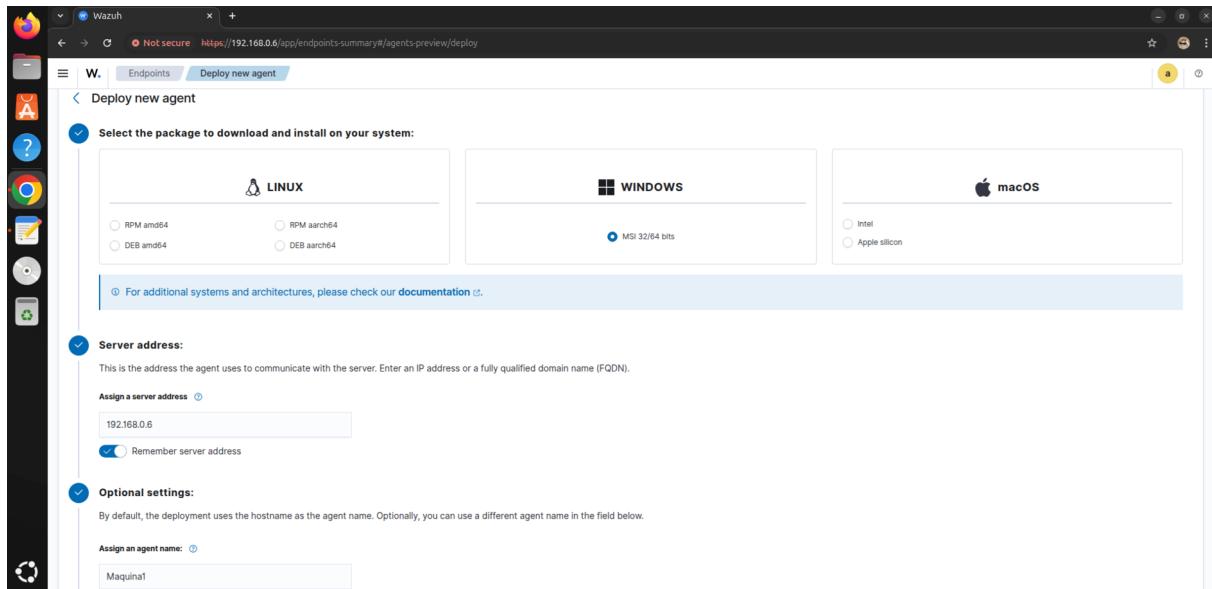
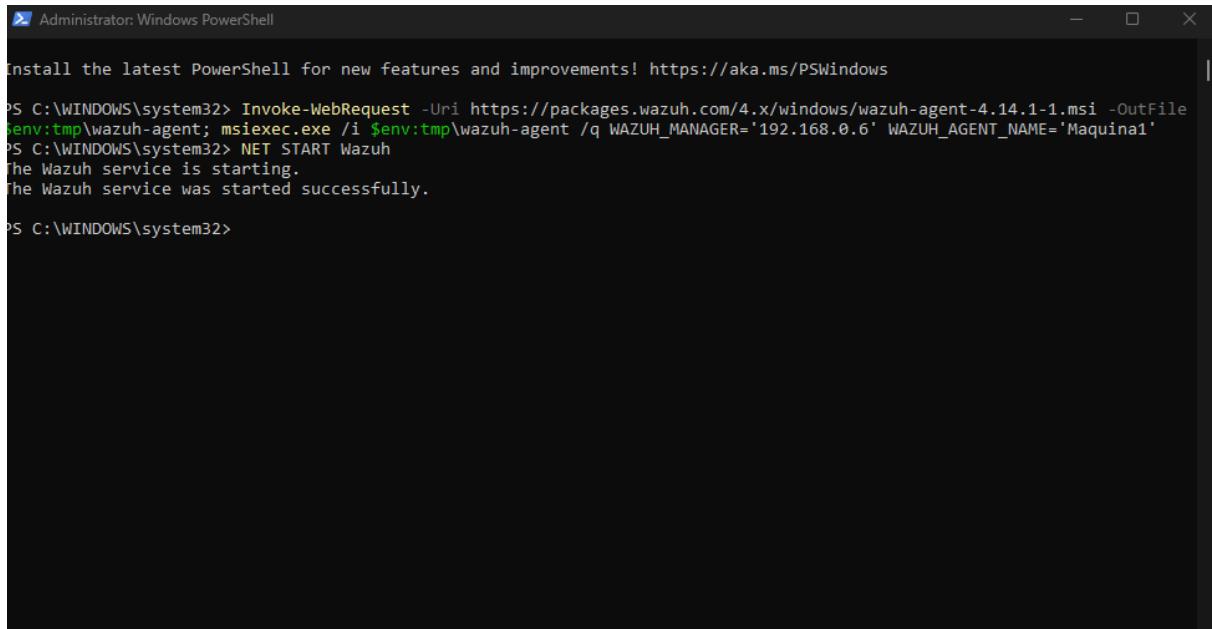


Figura 3. Creando un agente en Linux para Windows.

Configurado el agente en la interfaz, Wazuh proveyó un comando y se lo ejecutó en modo administrador en Windows PowerShell, para que de esta forma el servicio comience y se sincronice el servidor con el agente. (ver Figura 4)



```
Administrator: Windows PowerShell

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

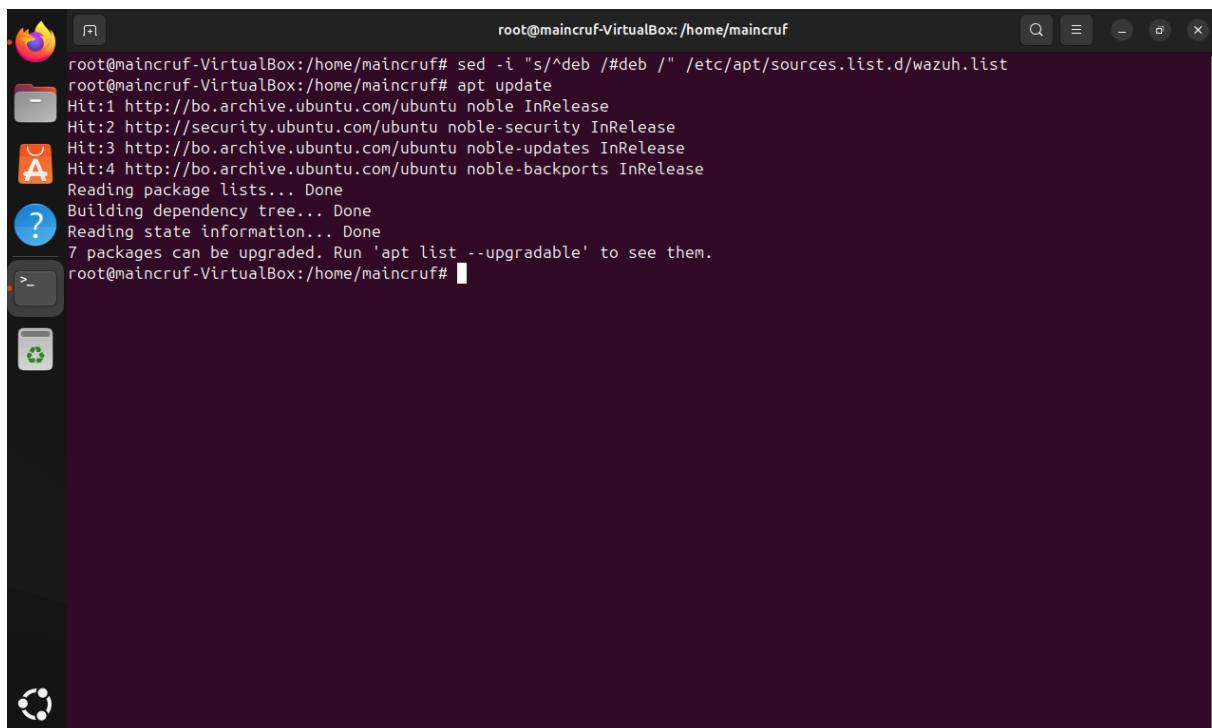
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.0.6' WAZUH_AGENT_NAME='Maquina1'
PS C:\WINDOWS\system32> NET START Wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```

Figura 4. Instalación y funcionamiento del agente en Windows.

3.3 Desactivación de actualizaciones

Se desactivaron las actualizaciones con el objetivo de evitar fallos de versiones entre el agente Wazuh y el servidor. (ver Figura 5)



```
root@maincruf-VirtualBox:/home/maincruf# sed -i "s/^deb /\#deb /" /etc/apt/sources.list.d/wazuh.list
root@maincruf-VirtualBox:/home/maincruf# apt update
Hit:1 http://bo.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://bo.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://bo.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@maincruf-VirtualBox:/home/maincruf#
```

Figura 5. Desactivación de actualizaciones automáticas en Wazuh

4. Verificación Técnica

4.1 Acceso a Wazuh

Se accedió a este SIEM, siguiendo los siguientes pasos.

1. Se abrió el navegador web, y se escribió la IP de la máquina que servirá de servidor en la barra de búsqueda, en este caso es 192.168.0.6.
2. Tras colocar las credenciales dadas por Wazuh, se permitió el acceso y se mostró la vista general (overview) de Wazuh. (ver Figura 6)

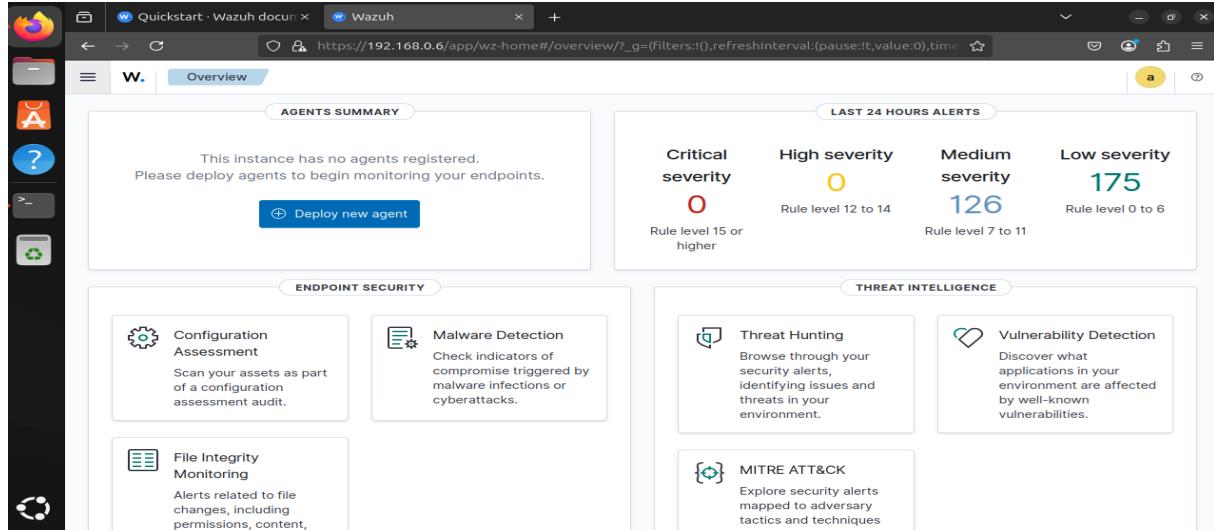


Figura 6. Overview de Wazuh.

4.2 Verificación agente Wazuh

Dentro de la interfaz de Wazuh, se logró ver que el agente Windows se sincronizó correctamente con el servidor en Linux, permitiendo monitorizar y recibir alertas de ese equipo. (ver Figura 7)

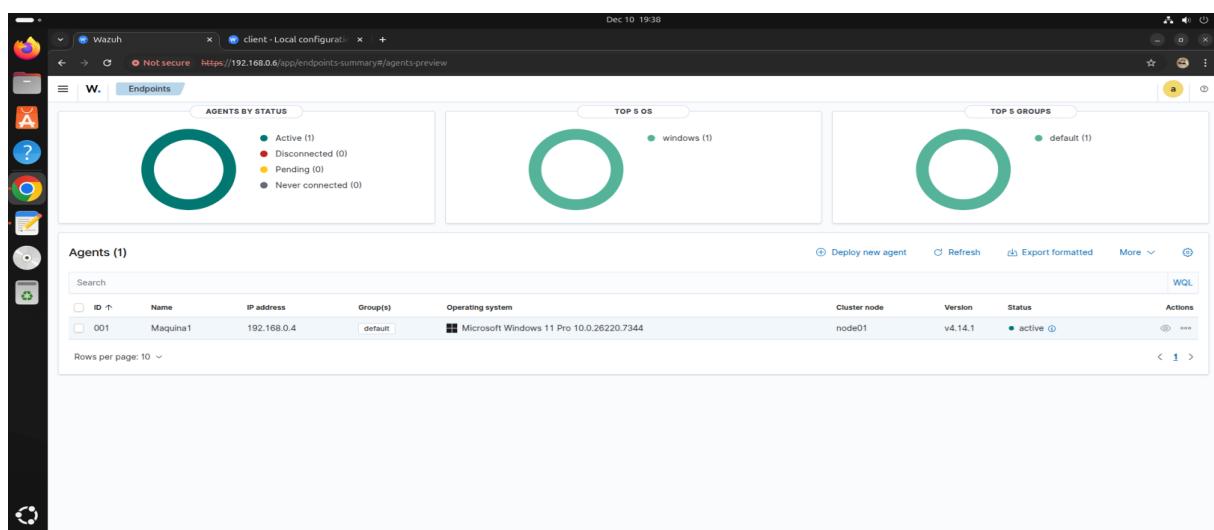


Figura 7. Agente correctamente conectado con el servidor Wazuh.