Implementación de Wazuh

Taller Práctico en VirtualBox 7.2.0

Bootcamp Analista SOC Nivel 1 - 2025

SIEM: El Corazón del SOC

Nombre: Eduardo Jurado
Correo: eduardoj2056@gmail.com
Fecha: 15 de agosto de 2025
Entorno: VirtualBox 7.2.0
OVA: Wazuh 4.7.3

Índice

1. Introducción

Wazuh es una plataforma de seguridad open source que ofrece:

- Detección de intrusiones
- Monitorización de integridad de archivos
- Análisis de vulnerabilidades
- Respuesta a incidentes

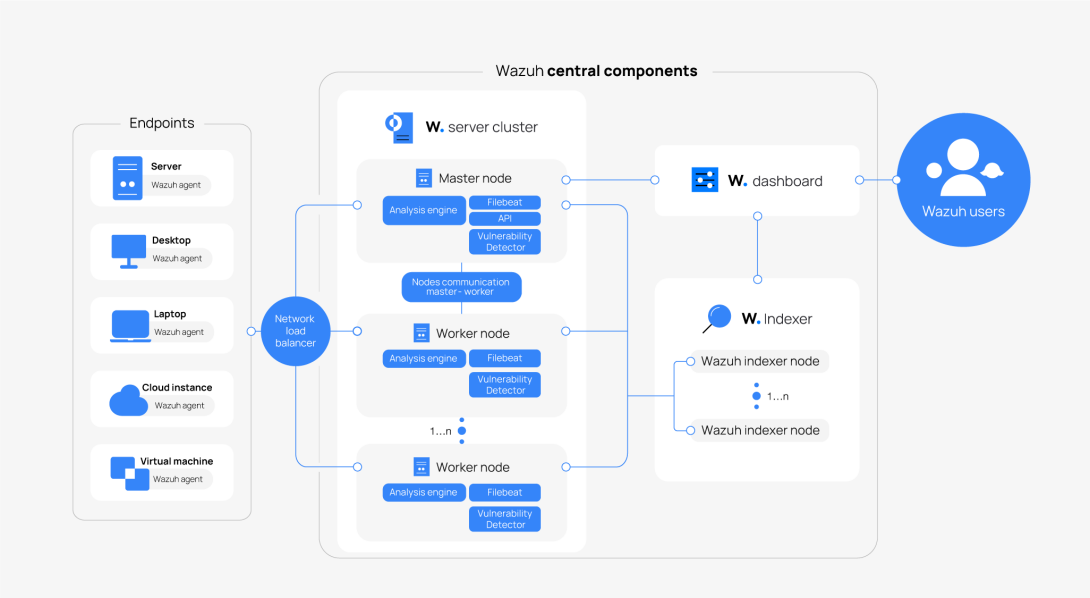

Figura 1: Arquitectura de Wazuh (Fuente: documentación oficial)

2. Objetivos del Taller

- Implementar el SIEM opensource Wazuh en un entorno local
- Instalar agentes de recolección de logs
- Relacionarse con las principales funcionalidades del SIEM

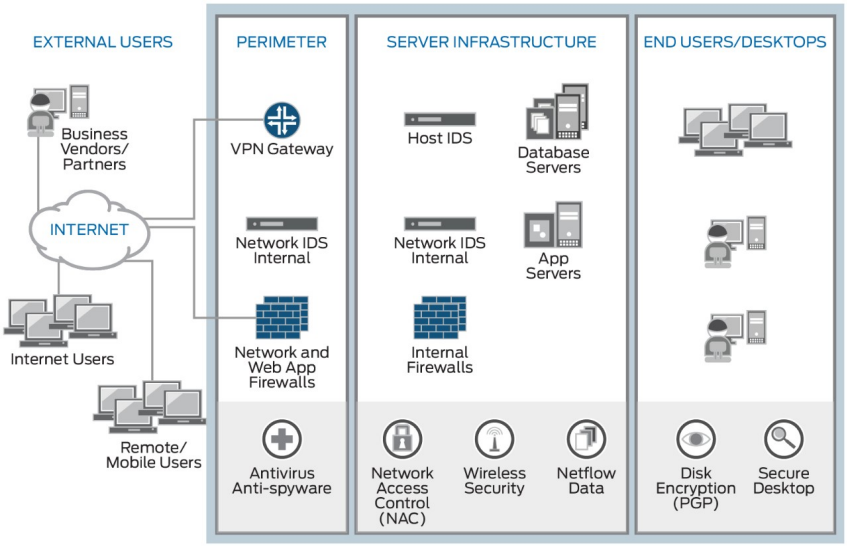

Figura 2: Flujo de trabajo de un SIEM

3. Disclaimer

Este laboratorio se realiza sólamente con fines educativos y de aprendizaje, con el fin de brindar información que permita mejorar las defensas en ciberseguridad.

4. Metodología

1. Despliegue del SIEM Wazuh mediante OVA en VirtualBox
2. Configuración del entorno
3. Instalación de agentes en sistemas Linux
4. Exploración de capacidades

5. Prerrequisitos

5.1. Requisitos Técnicos

- VirtualBox 7.2.0+ instalado
- 8GB RAM mínimo (16GB recomendado)
- 50GB de espacio libre
- Conexión a Internet estable

Figura 3: Página de descarga de VirtualBox

5.2. Descargas Necesarias

- OVA de Wazuh: `https://documentation.wazuh.com/current/installation-guide/wazuh-virtual-machine.html`
- Ubuntu Server 22.04 LTS (para agentes)

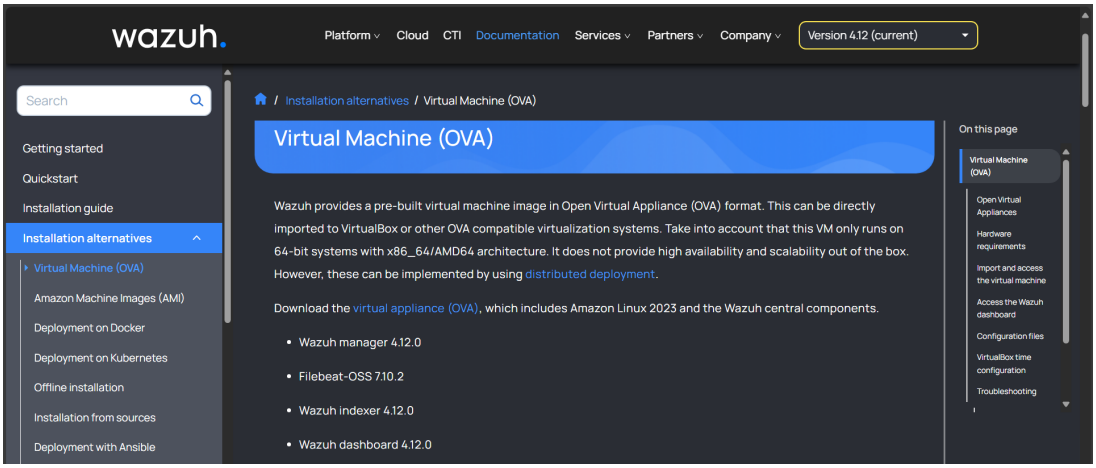

Figura 4: Página de descarga de la OVA Wazuh

6. Preparación del Entorno VirtualBox

6.1. Importación de la OVA

1. Abrir VirtualBox y seleccionar **Archivo → Importar servicio virtualizado**

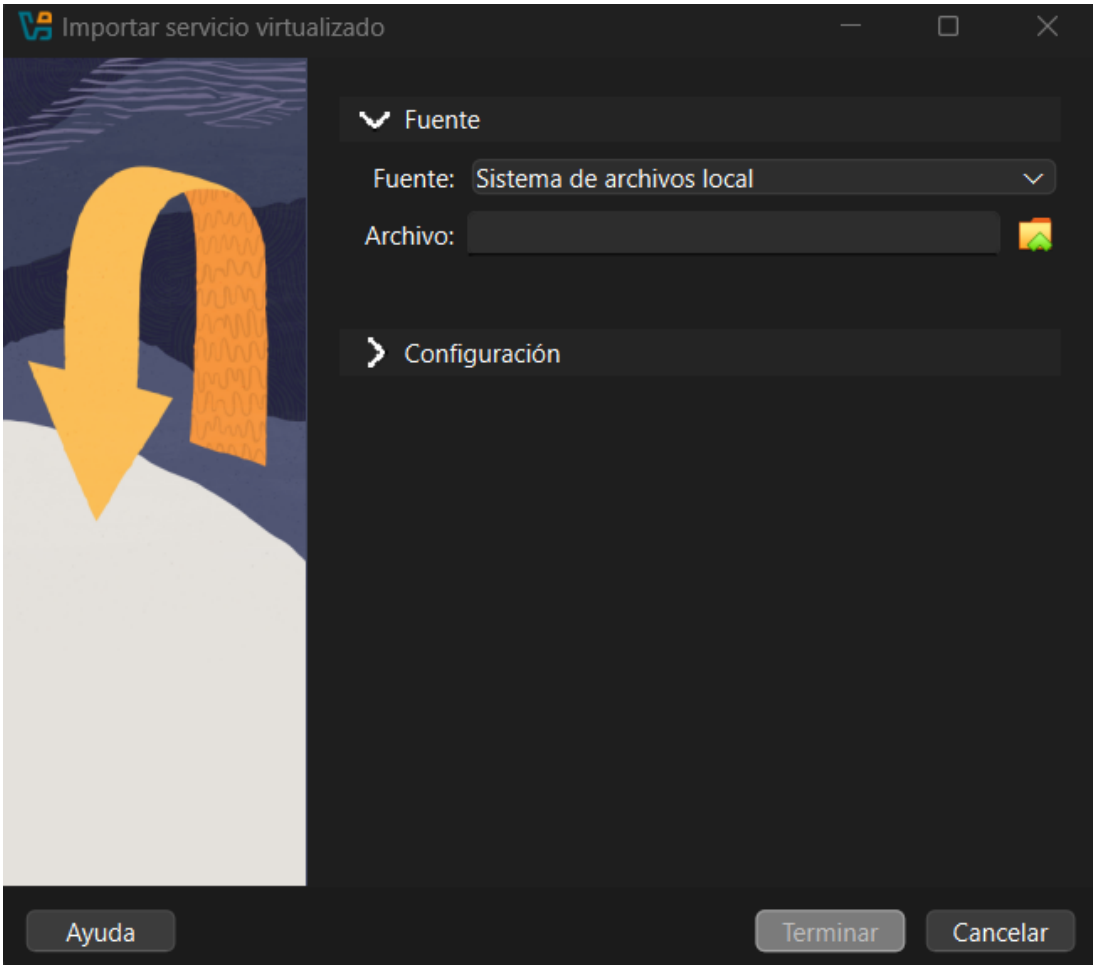

Figura 5: Menú de importación en VirtualBox

2. Seleccionar el archivo OVA descargado

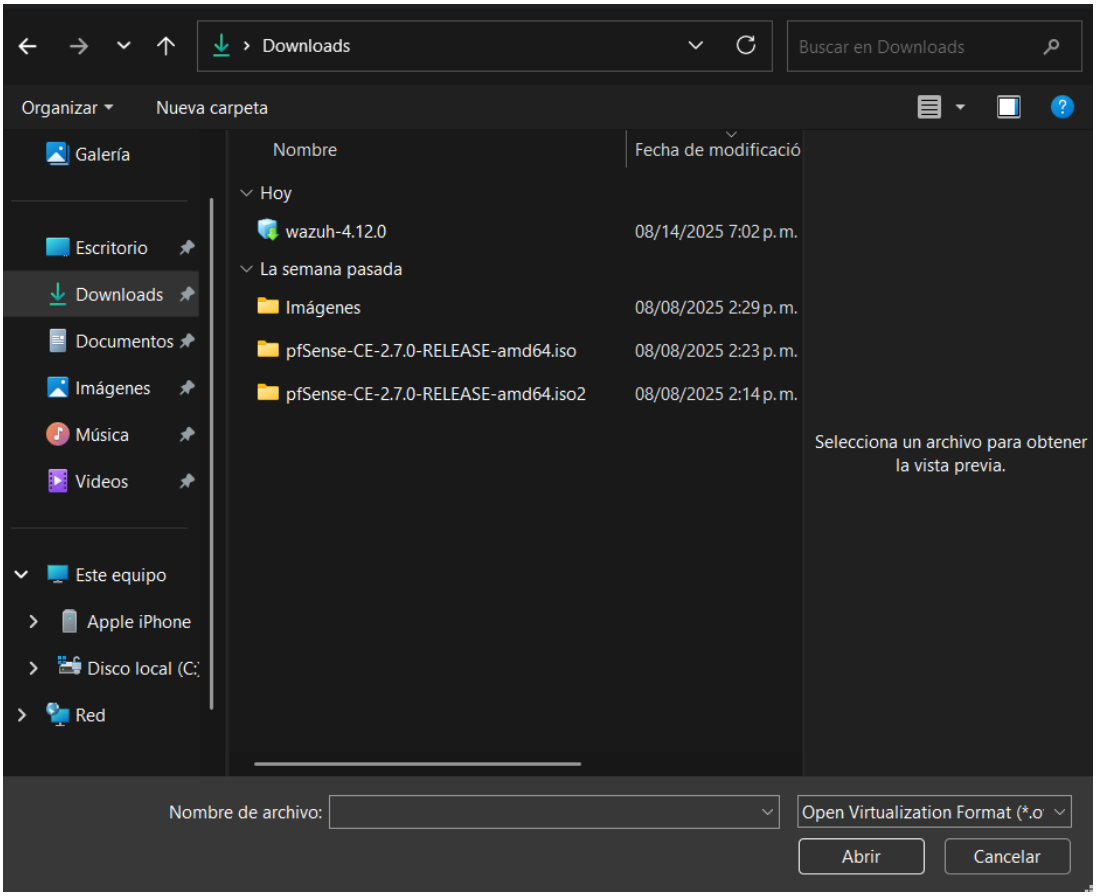

Figura 6: Selección del archivo OVA

3. Configuración recomendada:

```
# En el host (Windows/Linux/Mac):
systeminfo | find "Memoria"   # Windows
free -h                       # Linux/Mac
```

Listing 1: Comandos para verificar recursos

6.2. Configuración de la VM

- Ajustar recursos asignados:
  - 4 CPUs virtuales
  - 8GB RAM
  - Adaptador puente (Bridge)

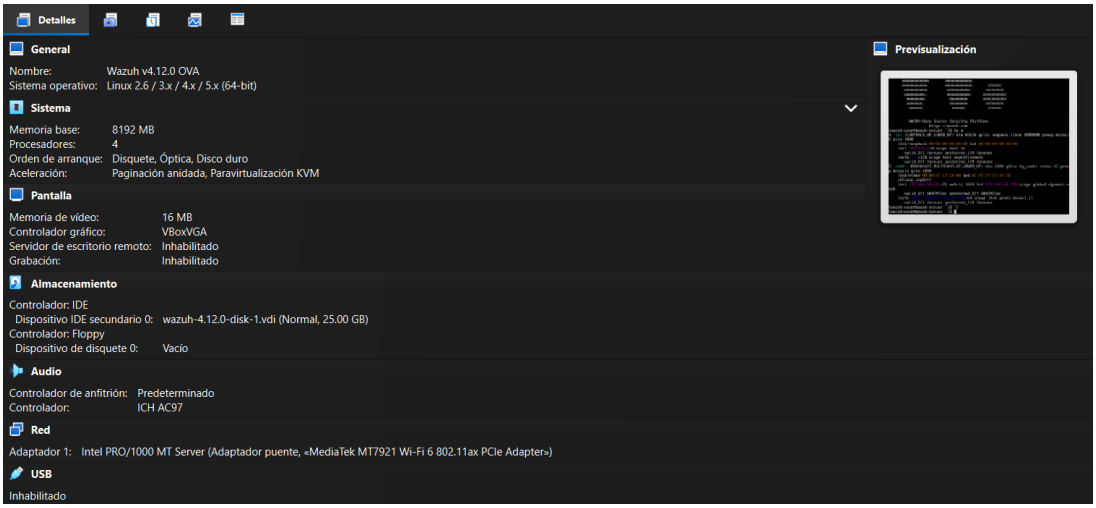

Figura 7: Configuración de recursos de la VM

7. Configuración Inicial

7.1. Primer Arranque

1. Iniciar la máquina virtual
2. Esperar a que complete el arranque (2-3 minutos)
3. Credenciales iniciales:

```
Usuario: wazuh-user
Contrase a: wazuh
```

Listing 2: Acceso inicial

7.2. Obtención de la IP

```
# Opci n 1 (recomendada):
sudo ip addr show | grep "inet␣" | grep -v "127.0.0.1"

# Opci n 2 (alternativa):
sudo nmcli device show | grep IP4.ADDRESS
```

Listing 3: Comandos para obtener IP

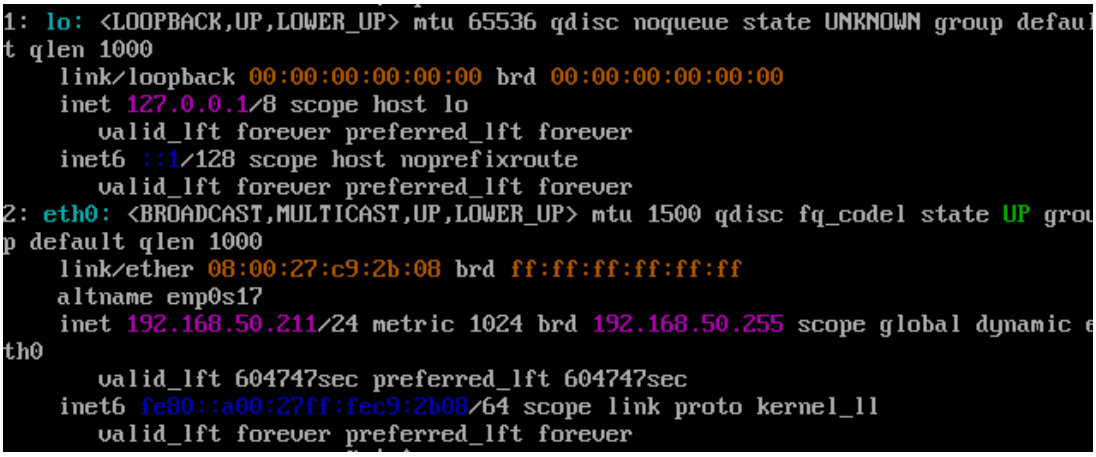

Figura 8: Obtención de la dirección IP desde terminal

8. Acceso al Dashboard

- URL: `https://https://192.168.50.211/`
- Credenciales predeterminadas:

```
Usuario: admin
Contrase a: admin
```

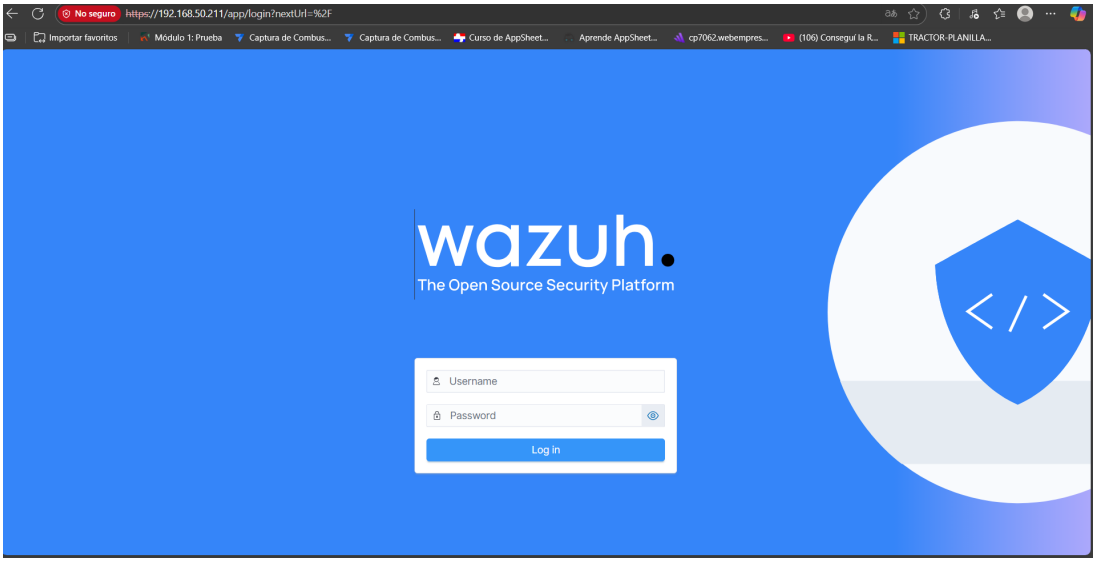

Figura 9: Pantalla de login del Wazuh Dashboard

9. Instalación de Agentes

9.1. En Sistema Linux

1. Conectarse al servidor Wazuh:

```
ssh wazuh-user@192.168.50.211
```

Listing 4: Conexión al servidor

sudo systemctl daemon-reload sudo systemctl enable wazuh-agent sudo systemctl start wazuh-agent

2. Generar clave de agente:

```
sudo /var/ossec/bin/manage_agents -l
```

3. Instalar agente en cliente Linux:

```
curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/
    main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb \\
&& sudo WAZUH_MANAGER='192.168.50.211' dpkg -i ./wazuh-agent.deb
```

```
root@debian:/home/debian# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/s

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt stable main" | sudo te
.list

sudo apt update
sudo apt install wazuh-agent -y
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt stable main
Hit:1 http://deb.debian.org/debian trixie InRelease
Hit:2 http://security.debian.org/debian-security trixie-security InRelease
Hit:3 http://deb.debian.org/debian trixie-updates InRelease
Get:4 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:5 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [46.2 kB]
Fetched 63.5 kB in 0s (129 kB/s)
1 package can be upgraded. Run 'apt list --upgradable' to see it.
Upgrading:
  wazuh-agent

Summary:
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 0
  Download size: 12.0 MB
  Space needed: 12.5 MB / 13.6 GB available

Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.12.0-1 [12.0 MB]
Fetched 12.0 MB in 1s (10.8 MB/s)
```

Figura 10: Proceso de instalación del agente en Linux

10. Exploración de Funcionalidades

10.1. Monitorización Básica

```
# Ver estado de servicios
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-indexer

# Ver logs en tiempo real
```

```
sudo tail -f /var/ossec/logs/alerts/alerts.log
```

Listing 5: Comandos útiles

11. Conclusión

- La OVA incluye:
  - Wazuh Manager 4.7.3
  - Wazuh Indexer 4.7.3
  - Dashboard 4.7.3
- Comandos clave para mantenimiento:

```
# Reiniciar servicios
sudo systemctl restart wazuh-manager

# Actualizar agentes
sudo apt update && sudo apt upgrade wazuh-agent
```