

Bootcamp Analista SOC Nivel 1

2025

SIEM, el corazón del SOC

Taller: Implementación de Wazuh

Elaborado por:

Sheyla Leacock



**COMUNIDAD
DOJO**

Objetivos del taller:

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

Disclaimer:

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

Metodología:

1. Se desplegará el SIEM Wazuh mediante una OVA en VirtualBox y se realizarán las configuraciones necesarias para su funcionamiento.
2. Se realizará la instalación de agentes de recolección de logs en sistemas Linux.
3. Se visualizarán las capacidades de la herramienta.

Prerrequisitos:

1. Tener instalado VirtualBox: <https://www.virtualbox.org/wiki/Downloads>
2. Tener una máquina virtual con Ubuntu.

Parte I - Importar la OVA de Wazuh

1. Descargar la OVA desde el sitio oficial de wazuh:

<https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html>

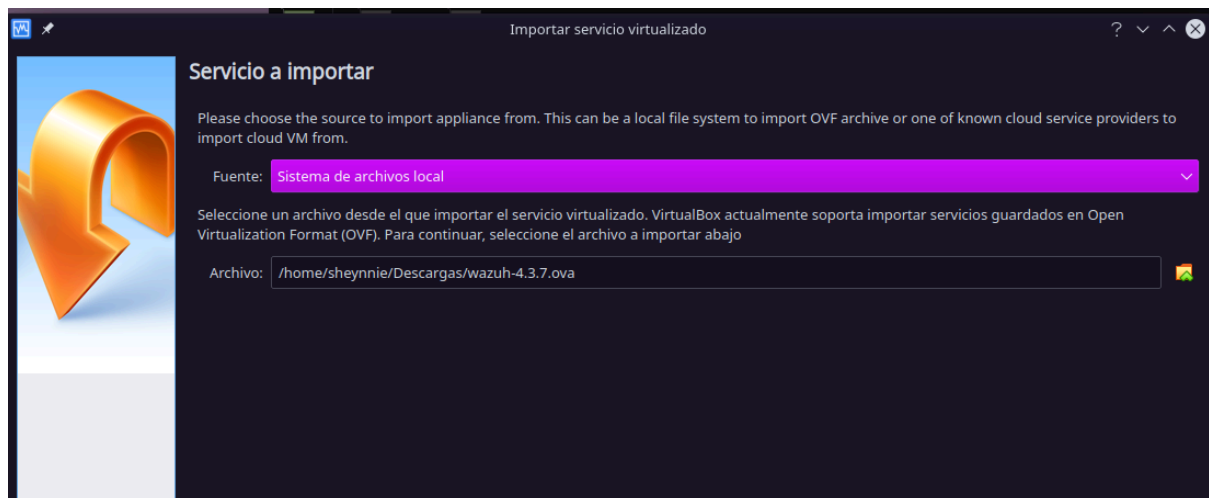
Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. This can be directly imported to VirtualBox or other OVA compatible virtualization systems. Take into account that this VM only runs on 64-bit systems. It does not provide high availability and scalability out of the box. However, these can be implemented by using [distributed deployment](#).

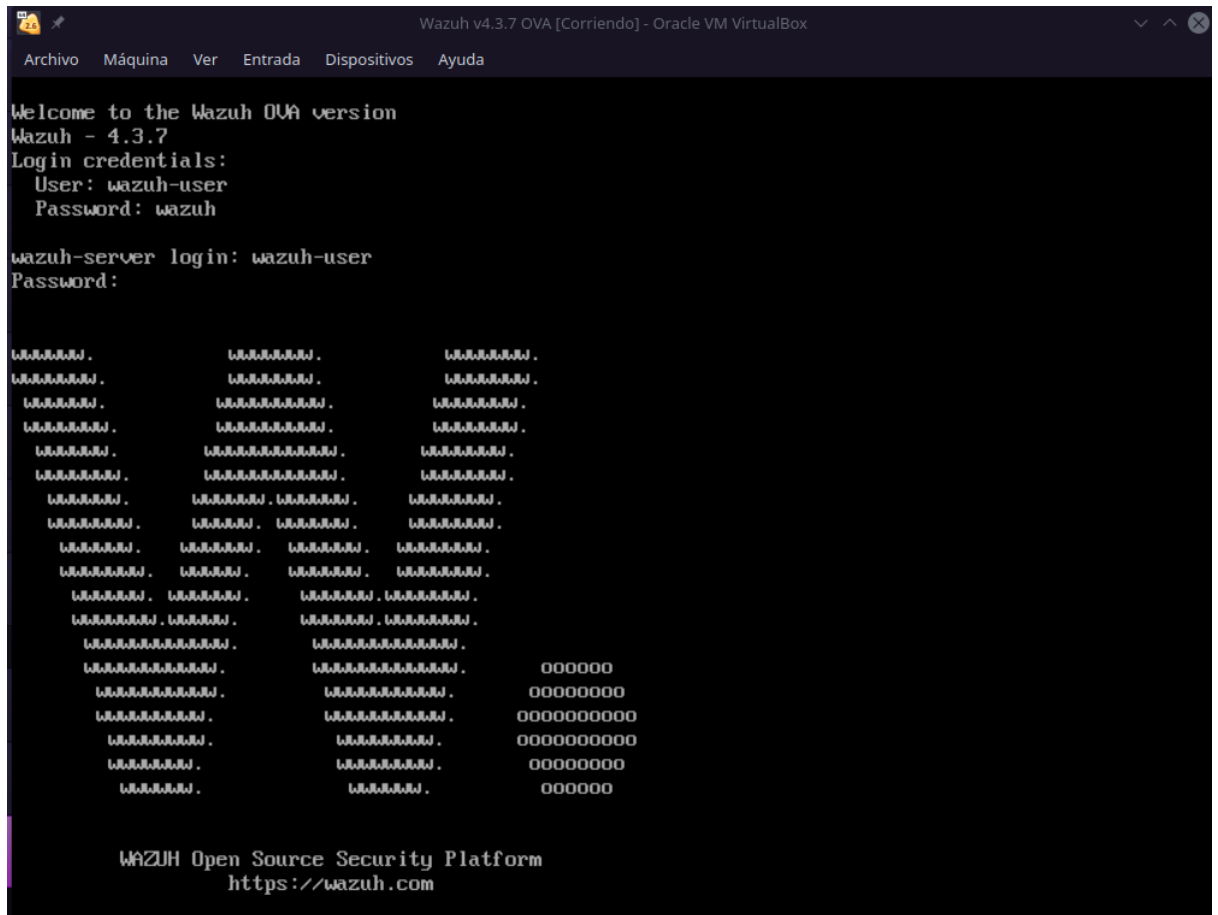
Download the [virtual appliance \(OVA\)](#), which contains the following components:

- CentOS 7
- Wazuh manager 4.3.7
- Wazuh indexer 4.3.7
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.3.7

2. Importar la ova desde Virtualbox



3. Iniciar la máquina virtual y loguearnos utilizando los datos de acceso:
user: **wazuh-user**
password: **wazuh**



4. Validamos la IP que mantiene la máquina de Wazuh con el comando: ***ip addr***



*Nota: la IP a utilizar es la identificada como inet en la interfaz eth0.

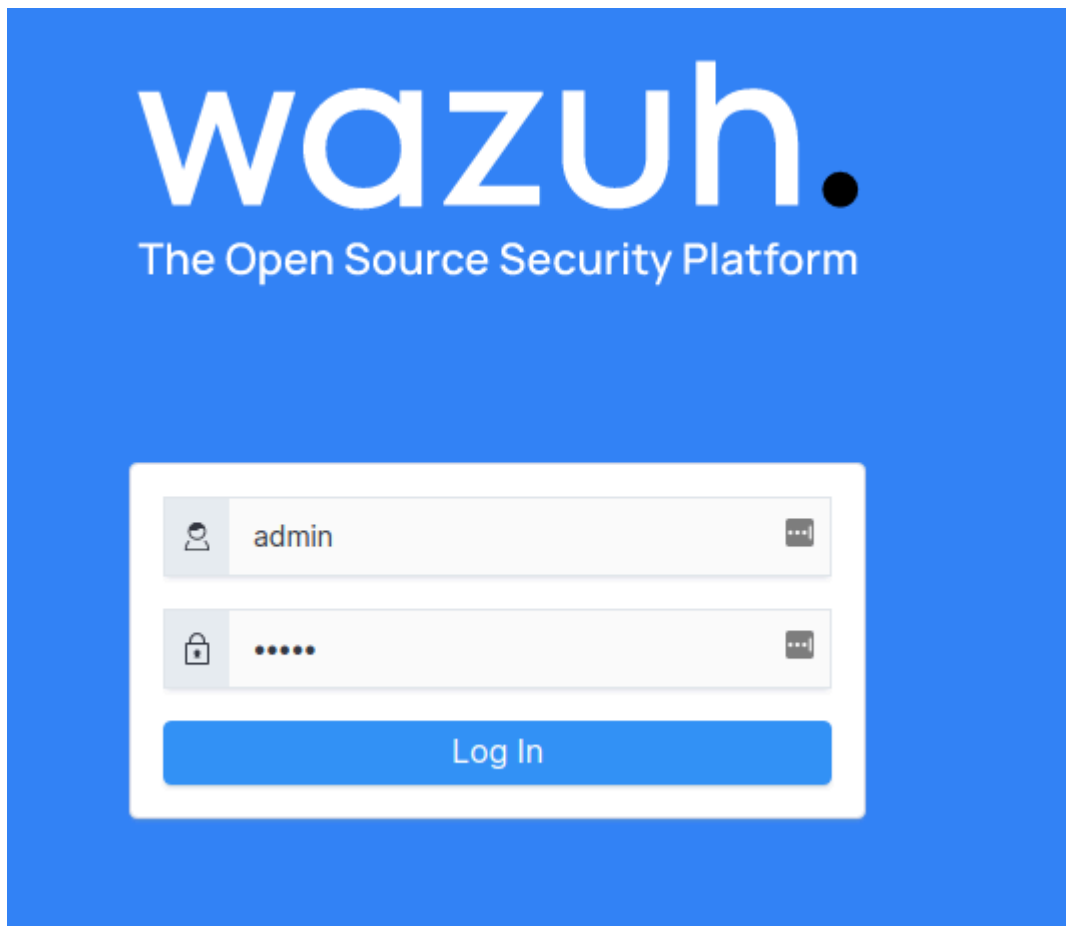
5. Accedemos desde el navegador web de nuestra máquina host a la URL de la IP del servidor de Wazuh utilizando protocolo https:

https://<wazuh ip>/app/login

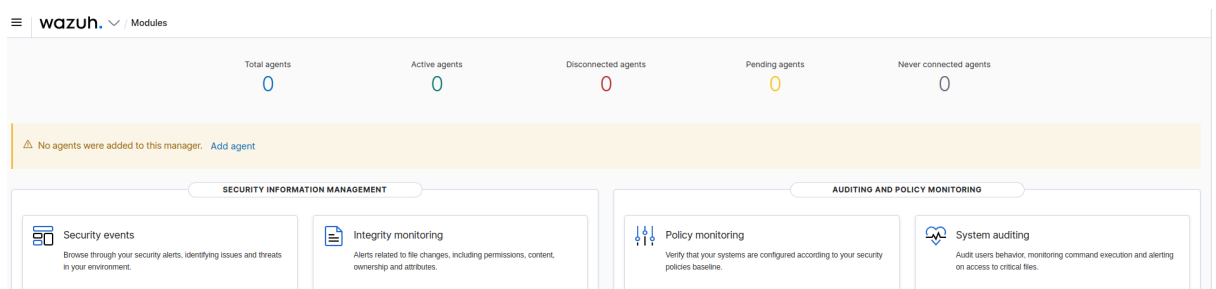
y nos logueamos con los siguientes datos:

```
user: admin
```

password: **admin**



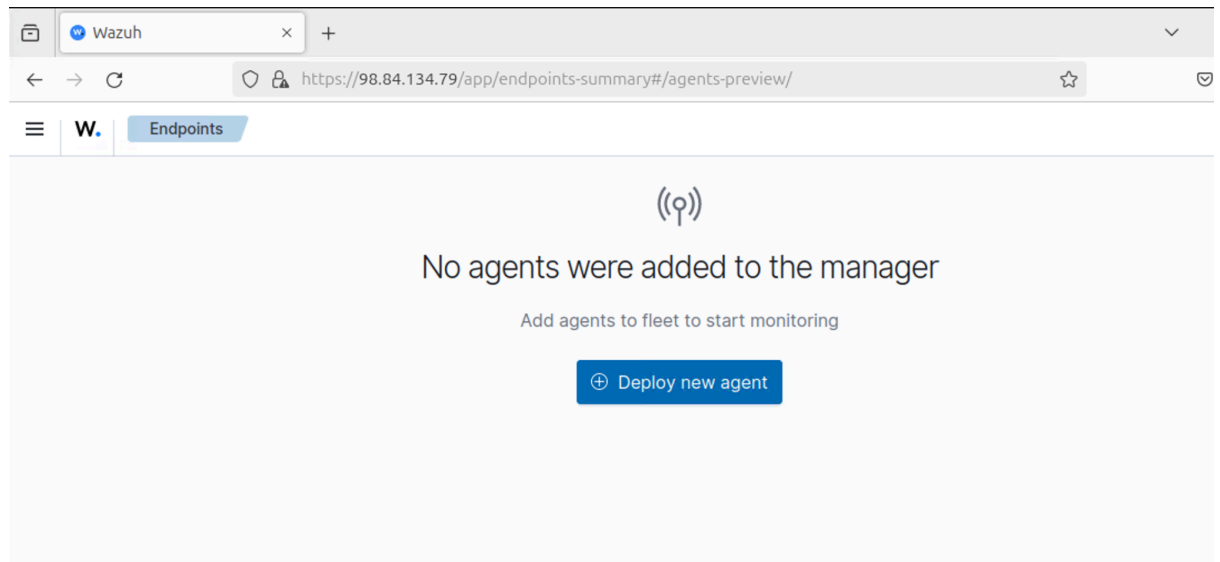
6. Una vez wazuh culmine el healthcheck nos mostrará el panel inicial



Parte II - Instalación de agentes de recolección de logs

Desde el servidor de Wazuh

1. Desde el apartado de Server Management -> Endpoint Summary, seleccionamos la opción ***Deploy new agent***




2. En la opción 1 indicamos los datos del sistema donde instalaremos el agente. Para efectos de este laboratorio seleccionaremos los datos de nuestra máquina Ubuntu o Windows 10.

W. Endpoints Deploy new agent


× Close

Deploy new agent


✓ Select the package to download and install on your system:

 **LINUX**

☐ RPM amd64 ☐ RPM aarch64
☐ DEB amd64 ☒ DEB aarch64

 **WINDOWS**

☐ MSI 32/64 bits

 **macOS**

☐ Intel
☐ Apple silicon

④ For additional systems and architectures, please check our [documentation](#).


✓ Server address:

3. En la opción 2 indicamos la IP del servidor de wazuh, es decir, la IP desde donde estamos ingresando estas configuraciones.


Deploy new agent

✓


Select the package to download and install on your system:

 **LINUX**

☒ RPM amd64 ☐ RPM aarch64
☐ DEB amd64 ☐ DEB aarch64

 **WINDOWS**

☐ MSI 32/64 bits

 **macOS**

☐ Intel
☐ Apple silicon

ⓘ

 For additional systems and architectures, please check our [documentation](#).

✓

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address ⓘ

100.24.192.255

☒ Remember server address

4. En la opción 3 podemos asignar un nombre al agente para identificarlo (opcional).

✓

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ⓘ

ubuntu24.02

ⓘ

 The agent name must be unique. It can't be changed once the agent has been enrolled. [↗](#)

5. En la opción 4 se nos mostrará el comando que podemos copiar y utilizar desde la máquina en la cual instalaremos el agente.

4 Run the following commands to download and install the agent:

```
curl -o wazuh-agent-4.9.0-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.9.0-1.x86_64.rpm && sudo WAZUH_MANAGER='100.24.192.255' WAZUH_AGENT_NAME='Ubuntu' rpm -ihv wazuh-agent-4.9.0-1.x86_64.rpm
```

④ Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

6. En la opción 5 se nos indican los comandos para iniciar el agente

✓ Start the agent:

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

7. Iniciamos la máquina Ubuntu y desde la terminal copiaremos y pegaremos el comando indicado para instalar el agente: ***curl -o wazuh-agent-4.9.0-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.9.0-1.x86_64.rpm && sudo WAZUH_MANAGER='<IP de wazuh manager>' WAZUH_AGENT_NAME='<nombre de agente wazuh>' rpm -ihv wazuh-agent-4.9.0-1.x86_64.rpm***

```
[ec2-user@ip-172-31-47-251 ~]$ curl -o wazuh-agent-4.9.0-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.9.0-1.x86_64.rpm && sudo WAZUH_MANAGER='100.24.192.255' WAZUH_AGENT_NAME='AGENT-LINUX' rpm -ihv wazuh-agent-4.9.0-1.x86_64.rpm
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 10.4M  100 10.4M    0     0  25.7M      0 --:--:-- --:--:-- --:--:-- 25.7M
Verifying... ##### [100%]
Preparing... ##### [100%]
package wazuh-agent-4.9.0-1.x86_64 is already installed
```

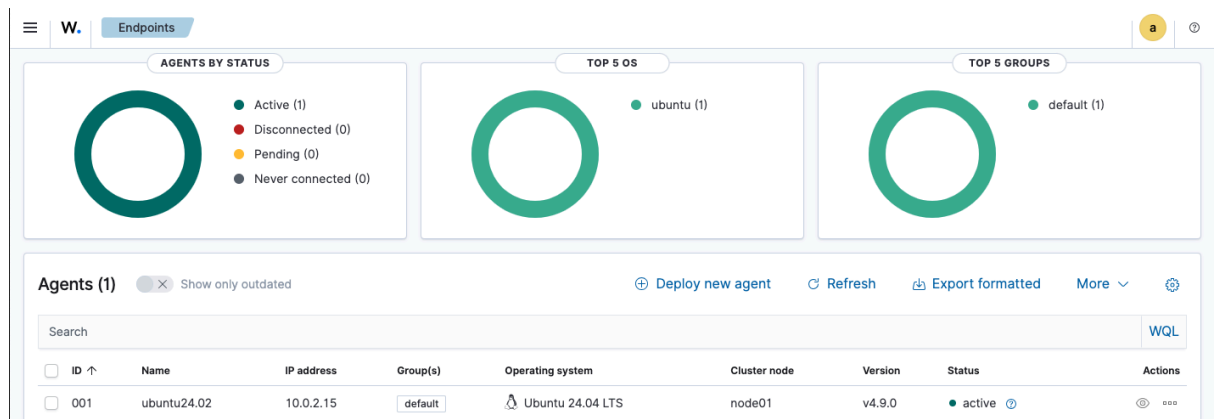
8. A continuación, ingresamos los comandos para habilitar e iniciar el servicio del agente:

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

```
[ec2-user@ip-172-31-47-251 ~]$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

*Nota: con el comando `sudo systemctl status wazuh-agent` podemos validar el estado del servicio.

9. Luego de esto, regresamos al servidor de wazuh para validar que se encuentra un agente conectado.



10. Desde la opción Threat Intelligence -> Threat Hunting podemos visualizar un Dashboard resumen y el detalle de los eventos de seguridad registrados

