

# Bootcamp Analista SOC Nivel 1

3° Edición

Módulo IV

Taller: Implementación de Wazuh

**Elaborado por:**

Sheyla Leacock



**COMUNIDAD  
DOJO**

## Objetivos del taller:

- ☐ Crear un HomeLab para el análisis de eventos de seguridad.
- ☐ 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 Windows y 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 y / o una máquina virtual con Windows 10.

\*Nota: Tomar de referencia la guía del CyberHomeLab desarrollado en la primera clase:

<https://github.com/WOSECPA/AnalistaSOC2022/blob/main/CyberHomeLab/Creando%20tu%20HomeLab.pdf>

## 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>

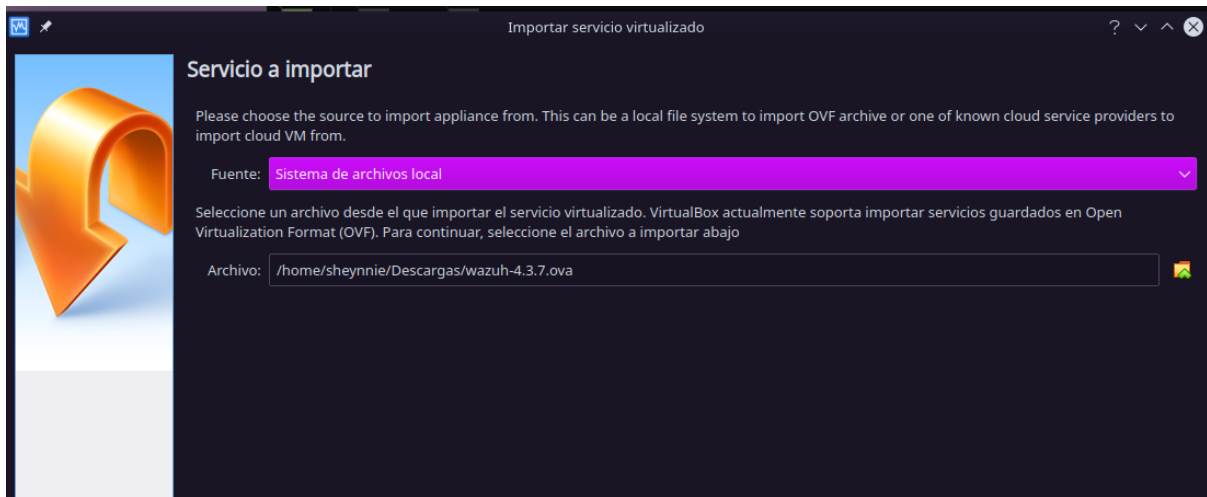
### Virtual Machine (OVA)

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](#).

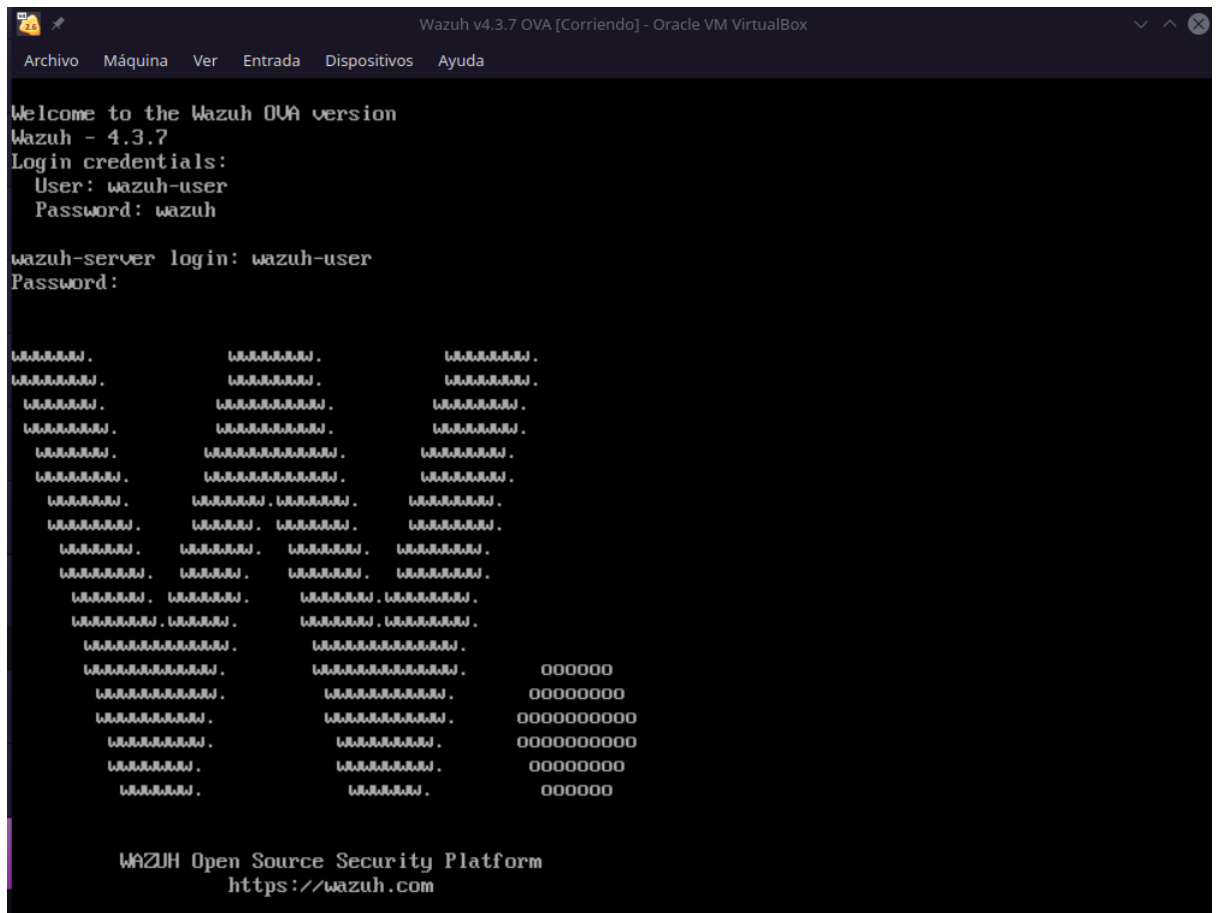
Download the [virtual appliance \(OVA\)](#), which contains the following components:

- 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**

```
Wazuh v4.3.7 OVA [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[wazuh-user@wazuh-server ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:eb:ad:a3 brd ff:ff:ff:ff:ff:ff
    inet 10.45.1.7/24 brd 10.45.1.255 scope global dynamic eth0
        valid_lft 86286sec preferred_lft 86286sec
    inet6 fe80::a00:27ff:feeb:ada3/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

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](https://<wazuh_ip>/app/login)**

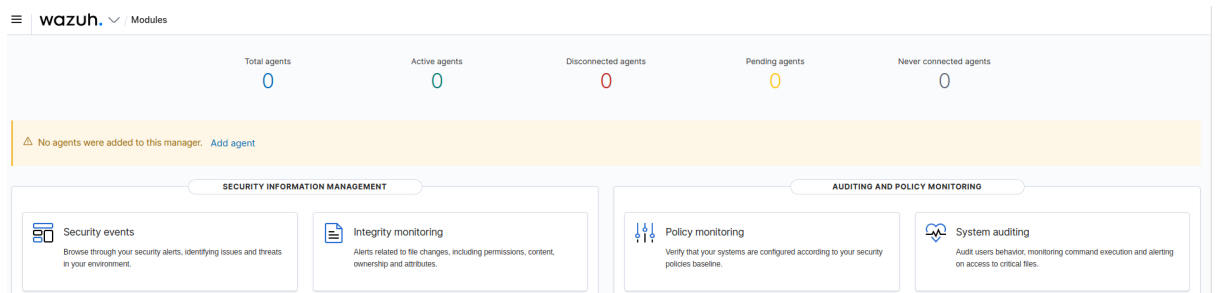
y nos logueamos con los siguientes datos:

user: **admin**

password: **admin**



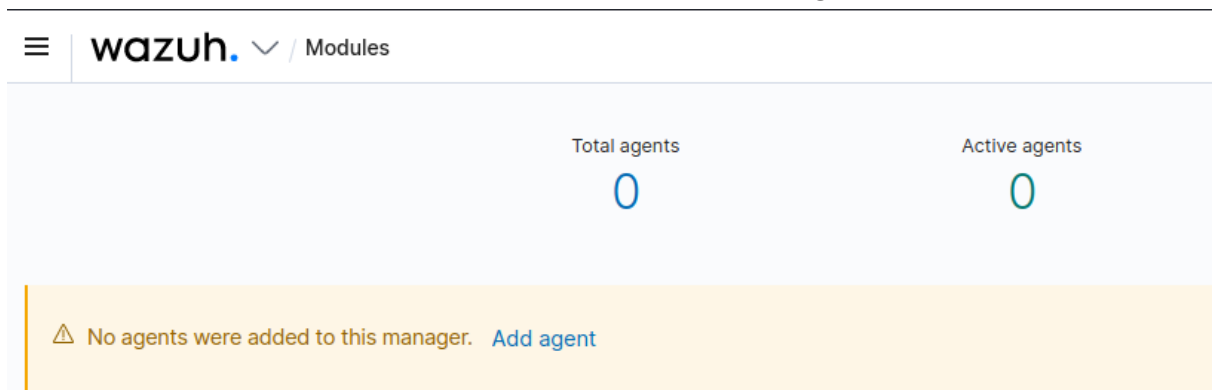
6. Una vez wazuh culmine el healthcheck nos mostrará el panel inicial



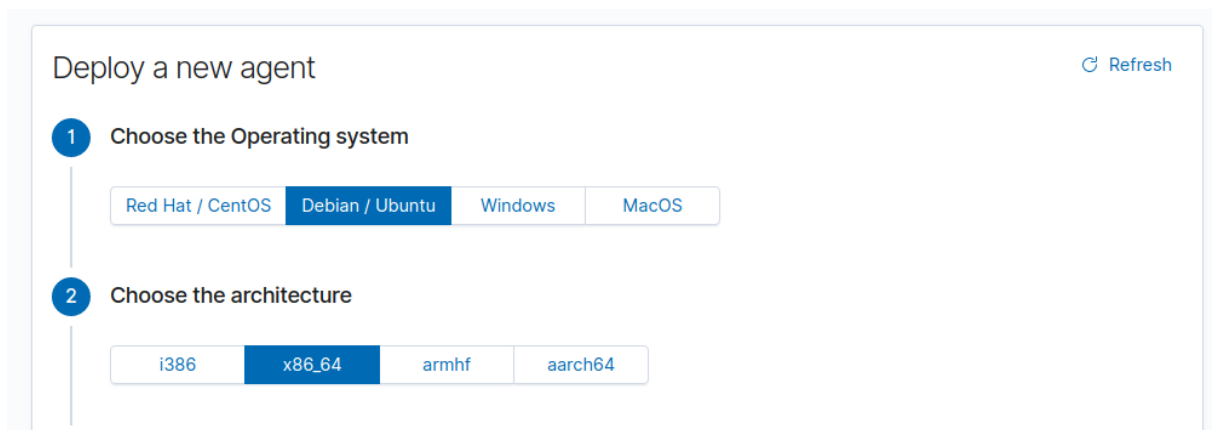
# Parte II - Instalación de agentes de recolección de logs

## Opción 1: Desde el servidor de Wazuh

1. Desde el apartado de module, seleccionamos la opción **Add agent**



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



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

**3 Wazuh server address**

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

4. En la opción 4 indicamos el grupo **default** que se encuentra creado.

**4 Assign the agent to a group**

Select one or more existing groups



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

**5 Install and enroll the agent**

You can use this command to install and enroll the Wazuh agent in one or more hosts.

① If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

```
curl -so wazuh-agent-4.3.7.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.3.7-1_amd64.deb && sudo WAZUH_MANAGER='10.45.1.7' WAZUH_AGENT_GROUP='default' dpkg -i ./wazuh-agent-4.3.7.deb
```

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

**6 Start the agent**

**Systemd** SysV Init

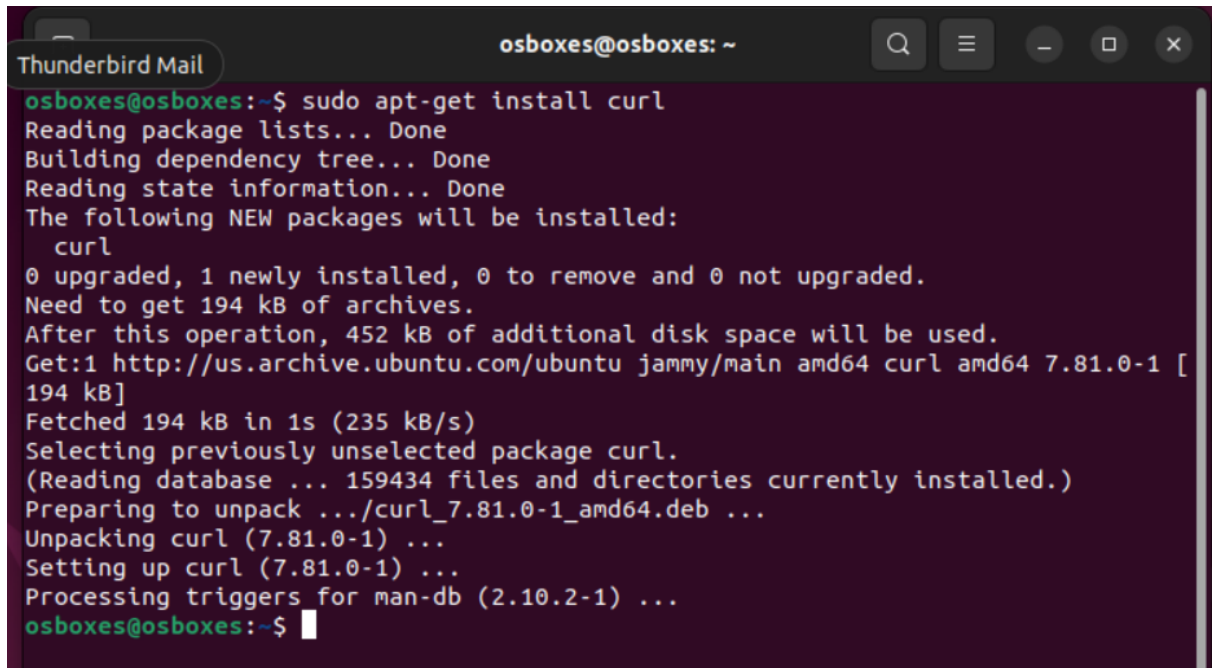
```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Copy command

To verify the connection with the Wazuh server, please follow this [document](#).

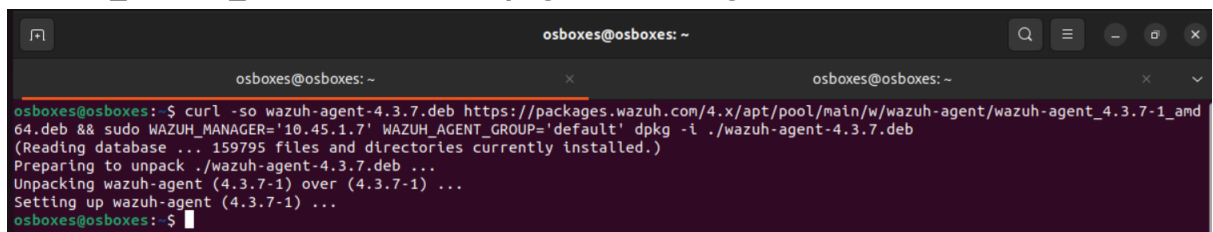
7. Iniciamos la máquina Ubuntu y desde la terminal instalaremos primero el paquete curl que utilizaremos para instalar el agente. Utilizamos el comando: **sudo apt-get install curl**





```
osboxes@osboxes: ~  
osboxes@osboxes:~$ sudo apt-get install curl  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  curl  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 194 kB of archives.  
After this operation, 452 kB of additional disk space will be used.  
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 curl amd64 7.81.0-1 [194 kB]  
Fetched 194 kB in 1s (235 kB/s)  
Selecting previously unselected package curl.  
(Reading database ... 159434 files and directories currently installed.)  
Preparing to unpack .../curl_7.81.0-1_amd64.deb ...  
Unpacking curl (7.81.0-1) ...  
Setting up curl (7.81.0-1) ...  
Processing triggers for man-db (2.10.2-1) ...  
osboxes@osboxes:~$
```

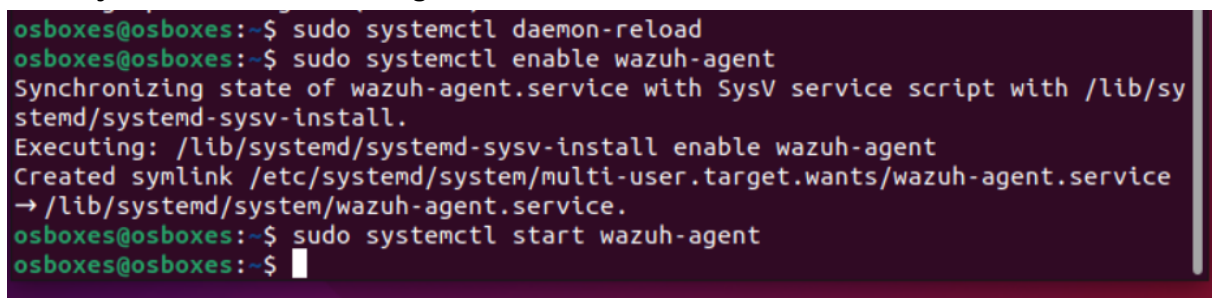
8. Ahora si, copiaremos y pegaremos el comando indicado para instalar el agente: ***curl -so wazuh-agent-4.3.7.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent\_4.3.7-1\_amd64.deb && sudo WAZUH\_MANAGER='IP' WAZUH\_AGENT\_GROUP='default' dpkg -i ./wazuh-agent-4.3.7.deb***



```
osboxes@osboxes: ~  
osboxes@osboxes:~$ curl -so wazuh-agent-4.3.7.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.3.7-1_amd64.deb && sudo WAZUH_MANAGER='10.45.1.7' WAZUH_AGENT_GROUP='default' dpkg -i ./wazuh-agent-4.3.7.deb  
(Reading database ... 159795 files and directories currently installed.)  
Preparing to unpack ./wazuh-agent-4.3.7.deb ...  
Unpacking wazuh-agent (4.3.7-1) over (4.3.7-1) ...  
Setting up wazuh-agent (4.3.7-1) ...  
osboxes@osboxes:~$
```

9. 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***



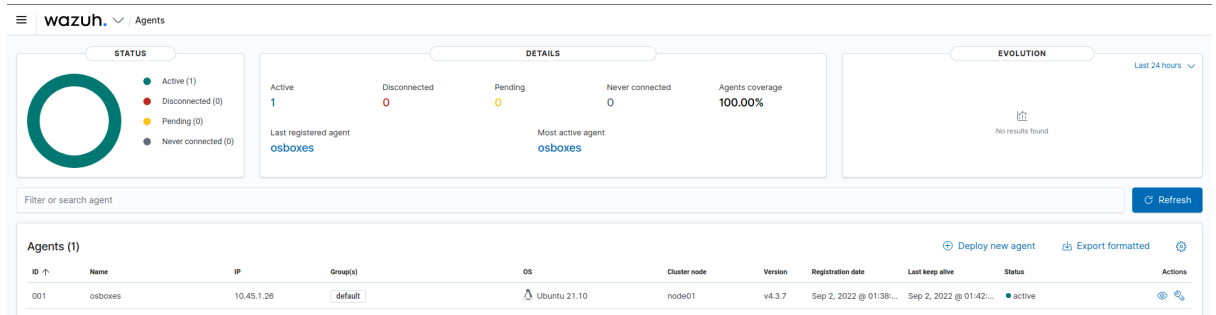
```
osboxes@osboxes:~$ sudo systemctl daemon-reload  
osboxes@osboxes:~$ sudo systemctl enable wazuh-agent  
Synchronizing state of wazuh-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable wazuh-agent  
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.  
osboxes@osboxes:~$ sudo systemctl start wazuh-agent  
osboxes@osboxes:~$
```

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

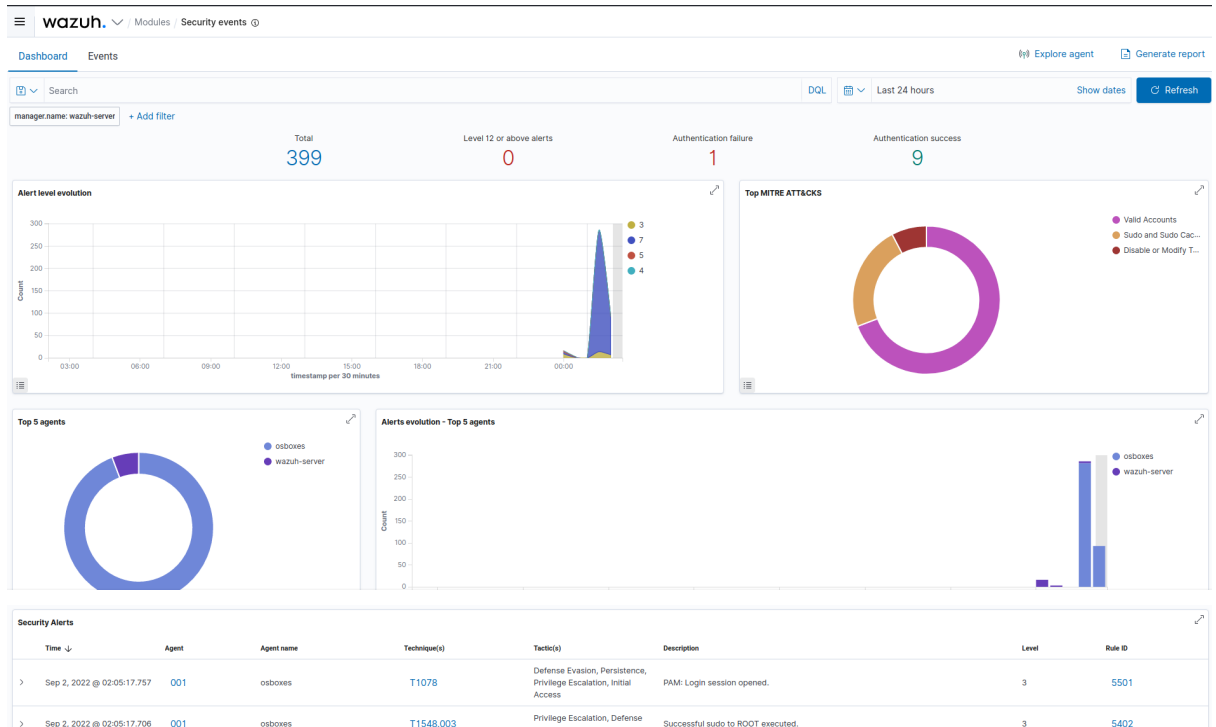
10. Luego de esto, regresamos al servidor de wazuh para validar que se encuentra un agente conectado



y si damos click a dicho número veremos el detalle de los agentes



11. Desde la opción Module/Security Events podemos visualizar los eventos de seguridad registrados



## Opción 2: Mediante el paquete de instalación

- Desde la máquina donde instalaremos el agente, en este caso, la máquina con Windows 10, nos dirigimos al sitio oficial de paquetes de instalación de wazuh: <https://documentation.wazuh.com/current/installation-guide/packages-list.html>

### Wazuh manager and Wazuh agent

#### Linux

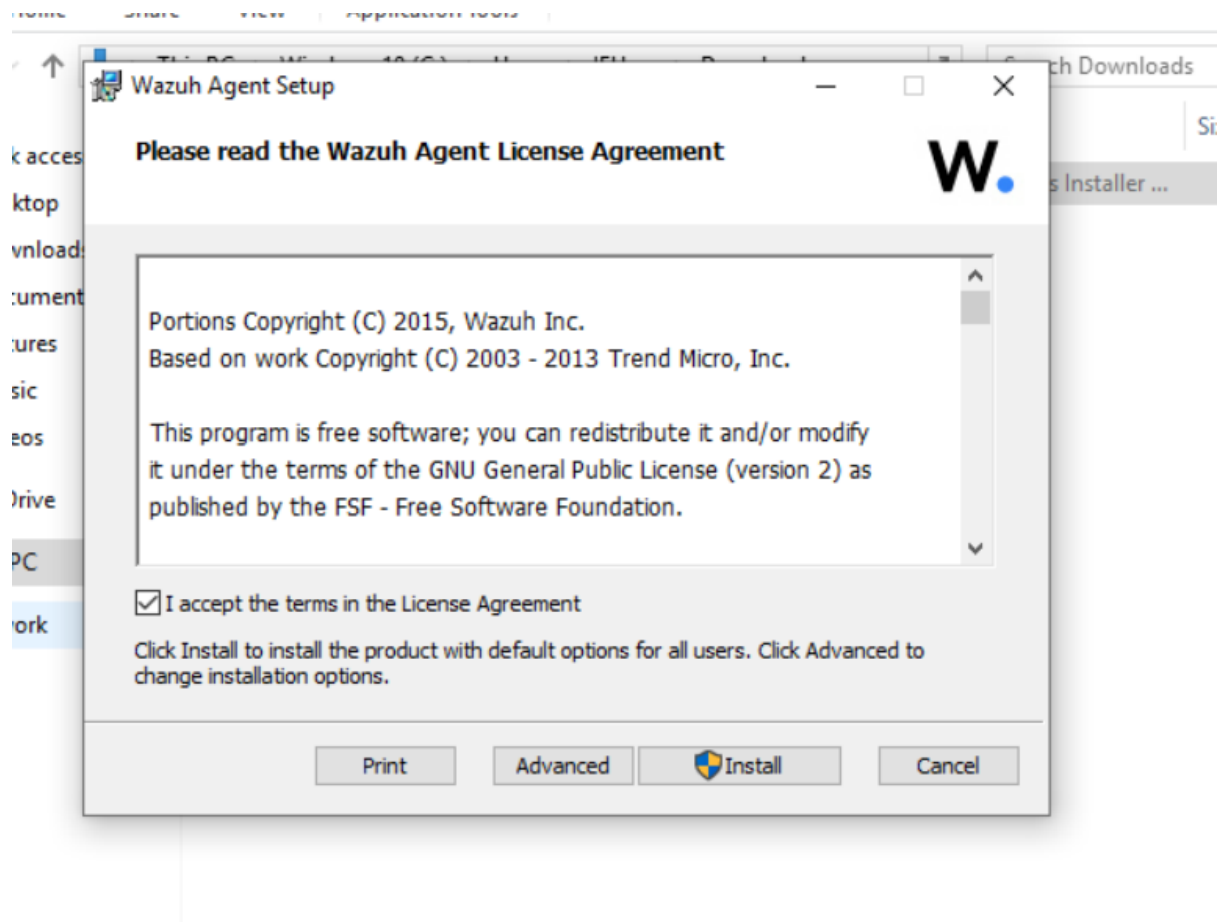
Distribution	Version	Architecture	Package
Amazon Linux	1 and 2	i386	wazuh-agent-4.3.7-2.i386.rpm (sha512)
		x86_64	wazuh-agent-4.3.7-2.x86_64.rpm (sha512)
			wazuh-manager-4.3.7-2.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.3.7-2.aarch64.rpm (sha512)
			wazuh-manager-4.3.7-2.aarch64.rpm (sha512)
		armhf	wazuh-agent-4.3.7-2.armv7hl.rpm (sha512)
	7 or later	powerpc	wazuh-agent-4.3.7-2.ppc64le.rpm (sha512)
	6 or later	i386	wazuh-agent-4.3.7-2.i386.rpm (sha512)
		x86_64	wazuh-agent-4.3.7-2.x86_64.rpm (sha512)
			wazuh-manager-4.3.7-2.x86_64.rpm (sha512)

- Descargamos el paquete que cumpla con la distribución y arquitectura de la máquina a utilizar, para efectos de este laboratorio utilizaremos la versión de windows

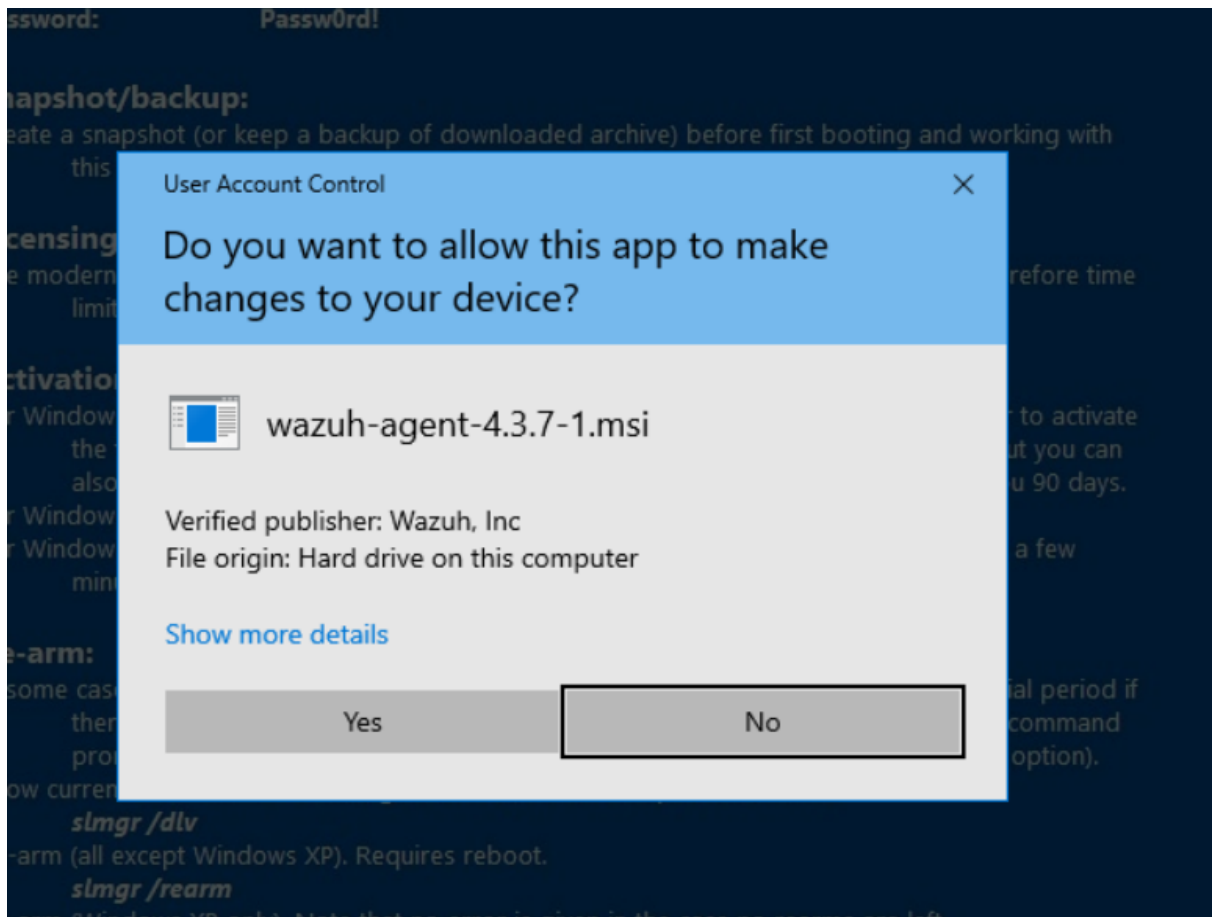
#### Windows

Version	Architecture	Package
XP or later	32/64bits	wazuh-agent-4.3.7-1.msi (sha512)

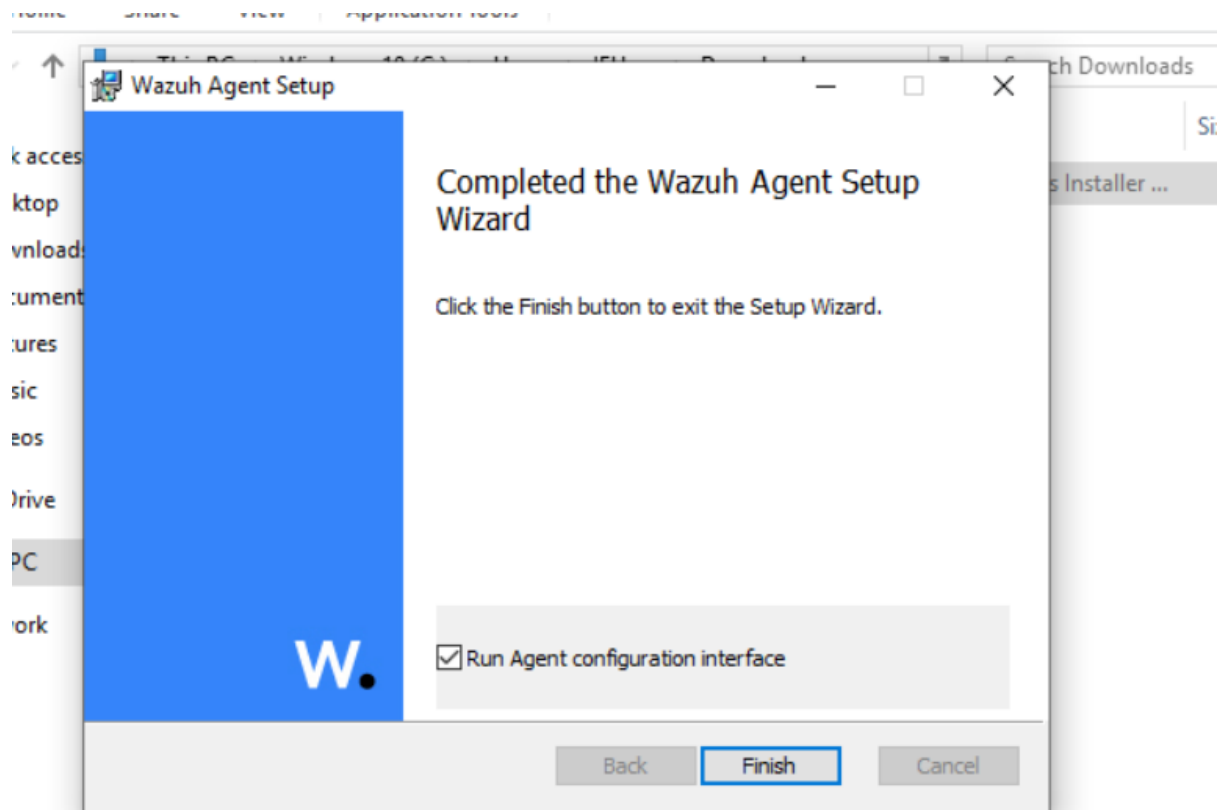
- Una vez descargado le damos doble click para ejecutarlo. En la ventana que aparece aceptamos los términos y le damos a instalar.



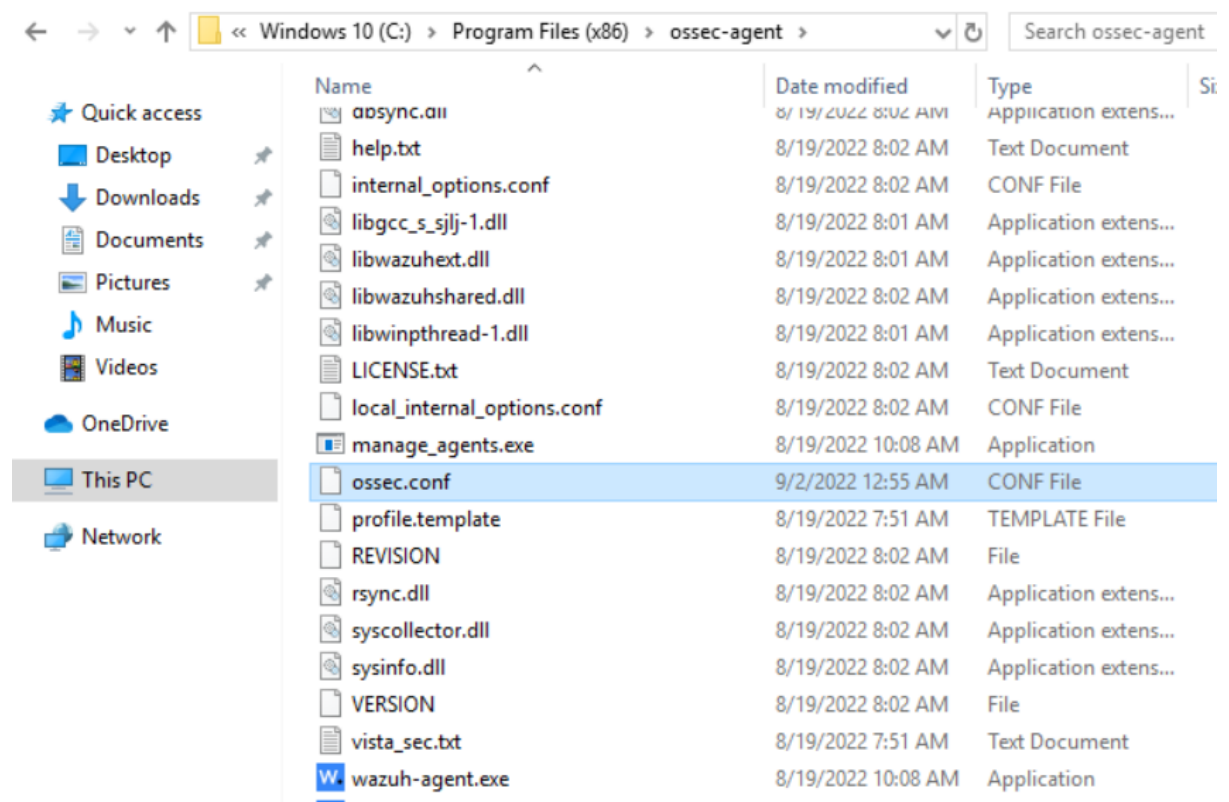
4. Al siguiente mensaje que aparece le damos click en **Si** para aceptar los cambios en el dispositivo.



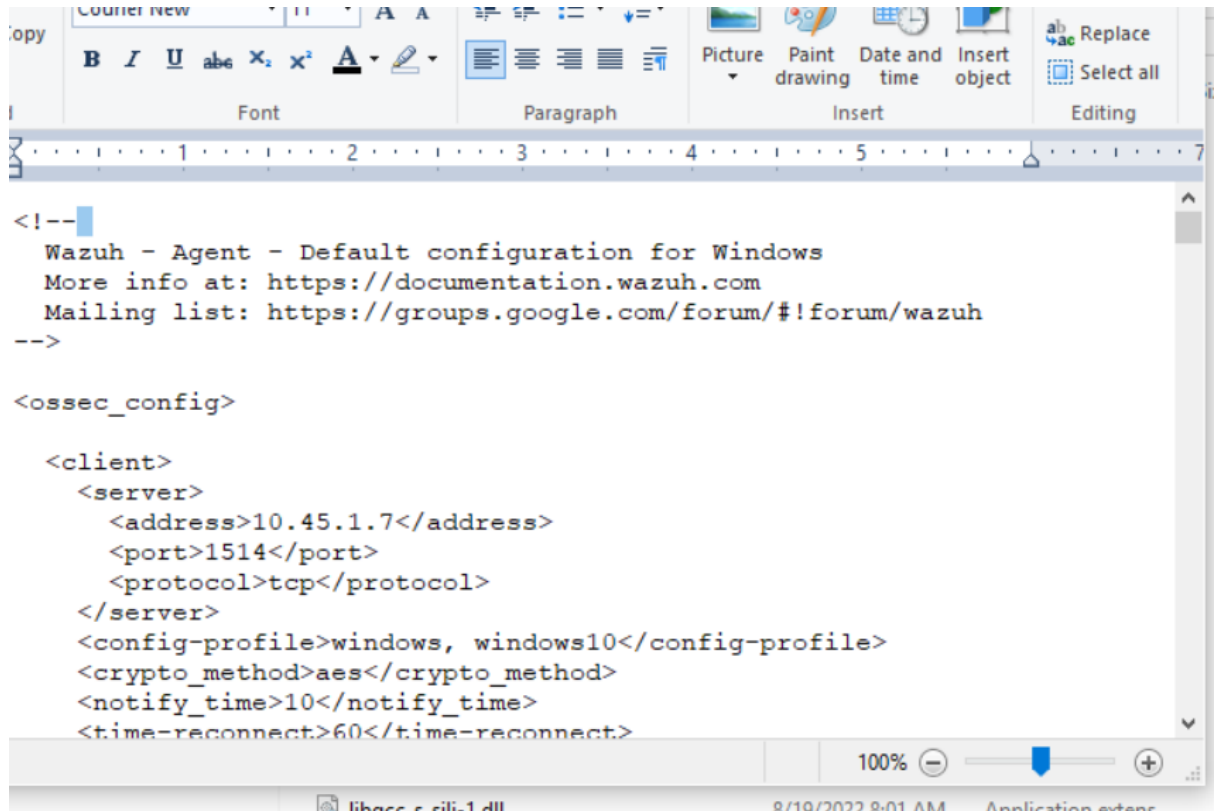
5. Al completar el setup le damos en la casilla de ejecutar interfaz del agente y luego damos click a **Finalizar**.



6. Ahora nos dirigimos a la carpeta **C:\Program Files (x86)\ossec-agent** y ubicamos el archivo **ossec.conf**



7. Abrimos el archivo con un editor de texto como wordpad y cambiamos la línea identificada bajo el tag **<address>** reemplazando el valor 0.0.0.0 por el valor de la ip del servidor de Wazuh.  
Guardamos los cambios.



8. Luego de esto, podemos visualizar el agente registrado y activo desde el servidor de Wazuh.

Agents (3)										
ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
003	MSEDOEWIN10	10.45.1.10	default	Microsoft Windows 10 Enterpr...	node01	v4.3.7	Sep 2, 2022 @ 03:21...	Sep 2, 2022 @ 03:22...	active	<a href="#">Refresh</a> <a href="#">Delete</a>
001	osboxes	10.45.1.26	default	Ubuntu 21.10	node01	v4.3.7	Sep 2, 2022 @ 01:38...	Sep 2, 2022 @ 02:09...	disconnected	<a href="#">Refresh</a> <a href="#">Delete</a>
002	fedora	10.45.1.14	default	Fedora 34	node01	v4.3.7	Sep 2, 2022 @ 02:21...	Sep 2, 2022 @ 02:24...	disconnected	<a href="#">Refresh</a> <a href="#">Delete</a>

\*Nota: Si el agente no aparece registrado debemos revisar y modificar las reglas del firewall de windows para permitir el tráfico de salida a los puertos utilizados para la conexión entre el agente y el servidor de Wazuh:

**1514/TCP** para la comunicación del agente.

**1515/TCP** para la inscripción mediante solicitud automática de agente.

**55000/TCP** para la inscripción vía la API del servidor.