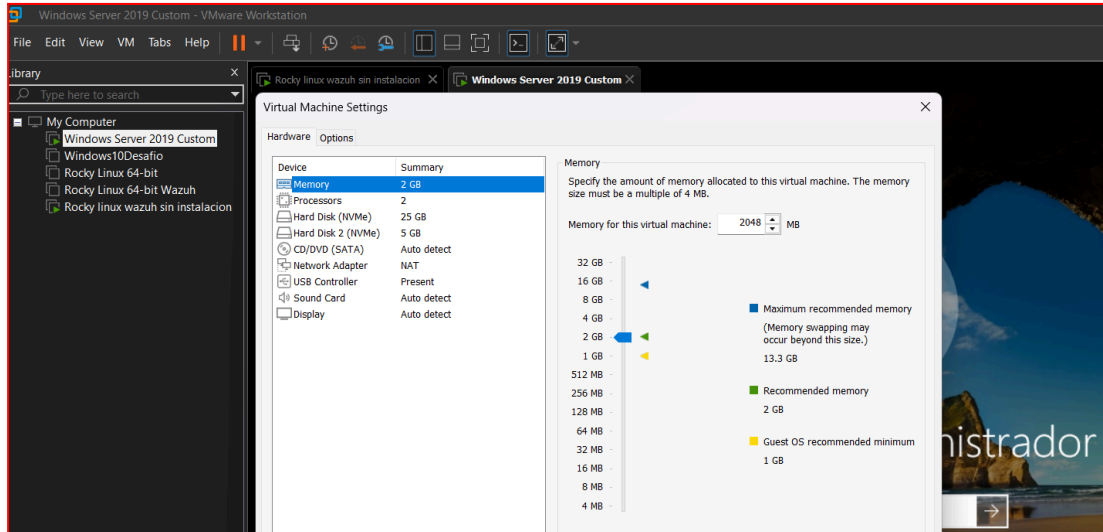


Desafío - Instalación de Wazuh

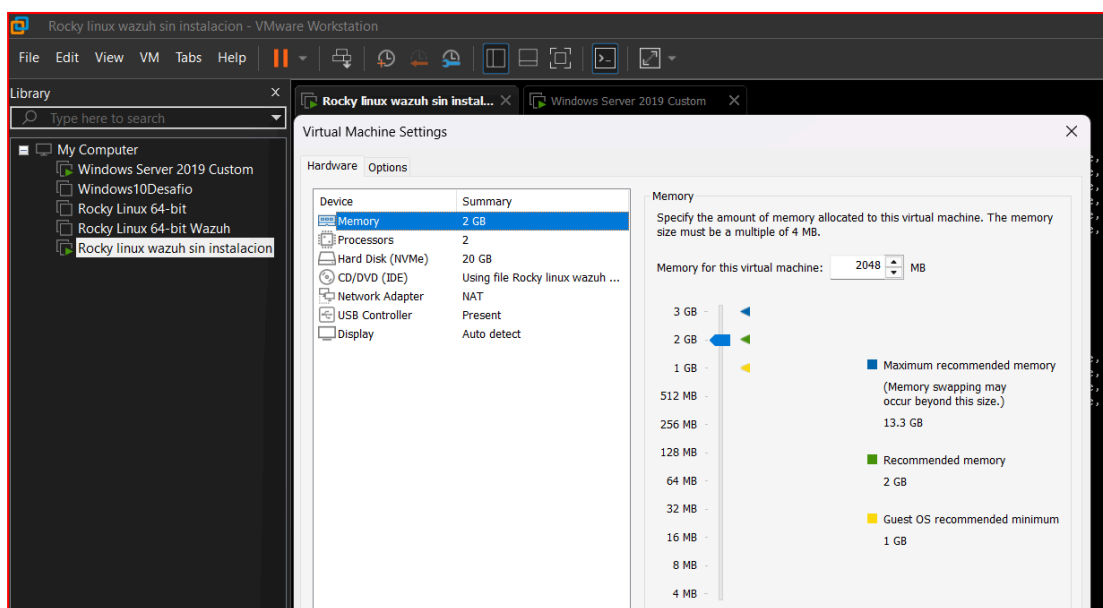
1. Instalación de una máquina virtual con Sistema Operativo Windows Server. (2 puntos)

En este desafío se utilizara una máquina virtual con Windows Server 2019, la cual ya se encuentra previamente configurada y ha sido utilizada durante el desarrollo del curso.



2. Instalación de una máquina virtual con Sistema Operativo Fedora. (2 puntos)

En este desafío se utilizara una máquina virtual con Rocky Linux release 9.5 (Blue Onyx), la cual ya se encuentra previamente configurada y ha sido utilizada durante el desarrollo del curso.



3. Instalación de Wazuh en el Servidor con Fedora. (2 puntos)

Se instaló la versión 4.7, la cual no presentó inconvenientes durante el proceso de instalación (ignorando las características del equipo con la opción -i), y se utilizó el siguiente comando:

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -o -i
```

El cual descarga el script de instalación y lo ejecuta.

```
[root@192 ~]# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -o -i
20/08/2025 16:20:59 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
20/08/2025 16:21:00 INFO: Verbose logging redirected to /var/log/wazuh-install.log
20/08/2025 16:21:11 INFO: --- Removing existing Wazuh installation ---
20/08/2025 16:21:11 INFO: Removing Wazuh manager.
20/08/2025 16:21:40 INFO: Wazuh manager removed.
20/08/2025 16:21:40 INFO: Removing Wazuh indexer.
20/08/2025 16:21:41 INFO: Wazuh indexer removed.
20/08/2025 16:21:41 INFO: Installation cleaned.
20/08/2025 16:21:44 INFO: --- Dependencies ---
20/08/2025 16:21:44 INFO: Installing tar.
20/08/2025 16:21:47 INFO: Installing lsof.
20/08/2025 16:21:49 WARNING: Hardware and system checks ignored.
20/08/2025 16:21:49 INFO: Wazuh web interface port will be 443.
20/08/2025 16:21:50 WARNING: The system has FirewallD enabled. Please ensure that traffic is allowed on these ports: 1515, 1514, 443.
20/08/2025 16:21:50 INFO: Wazuh repository added.
20/08/2025 16:21:51 INFO: --- Configuration files ---
20/08/2025 16:21:51 INFO: Generating configuration files.
20/08/2025 16:21:51 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
20/08/2025 16:21:52 INFO: --- Wazuh indexer ---
20/08/2025 16:21:52 INFO: Starting Wazuh indexer installation.
20/08/2025 16:26:54 INFO: Wazuh indexer installation finished.
20/08/2025 16:26:58 INFO: Wazuh indexer post-install configuration finished.
20/08/2025 16:26:58 INFO: Starting service wazuh-indexer.
20/08/2025 16:27:09 INFO: wazuh-indexer service started.
20/08/2025 16:27:09 INFO: Initializing Wazuh indexer cluster security settings.
20/08/2025 16:27:19 INFO: Wazuh indexer cluster initialized.
20/08/2025 16:27:19 INFO: --- Wazuh server ---
20/08/2025 16:27:19 INFO: Starting the Wazuh manager installation.
20/08/2025 16:28:27 INFO: Wazuh manager installation finished.
20/08/2025 16:28:27 INFO: Starting service wazuh-manager.
20/08/2025 16:28:37 INFO: wazuh-manager service started.
20/08/2025 16:28:37 INFO: Starting Filebeat installation.
20/08/2025 16:28:42 INFO: Filebeat installation finished.
20/08/2025 16:28:43 INFO: Filebeat post-install configuration finished.
20/08/2025 16:28:43 INFO: Starting service filebeat.
20/08/2025 16:28:44 INFO: filebeat service started.
20/08/2025 16:28:44 INFO: --- Wazuh dashboard ---
20/08/2025 16:28:44 INFO: Starting Wazuh dashboard installation.
20/08/2025 16:30:25 INFO: Wazuh dashboard installation finished.
20/08/2025 16:30:25 INFO: Wazuh dashboard post-install configuration finished.
20/08/2025 16:30:25 INFO: Starting service wazuh-dashboard.
20/08/2025 16:30:25 INFO: wazuh-dashboard service started.
20/08/2025 16:30:50 INFO: Initializing Wazuh dashboard web application.
20/08/2025 16:30:51 INFO: Wazuh dashboard web application initialized.
20/08/2025 16:30:51 INFO: --- Summary ---
20/08/2025 16:30:51 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: K4Ghxyosv.zr0Lss2vIE4uINhu6XqEQ8
20/08/2025 16:30:51 INFO: --- Dependencies ---
20/08/2025 16:30:51 INFO: Removing tar.
20/08/2025 16:30:52 INFO: Removing lsof.
20/08/2025 16:30:54 INFO: Installation finished.
```

4. Instalación de Wazuh Agent en el Servidor Windows Server. (2 puntos)

Para instalar el agente en el servidor (Windows Server 2019), primero es necesario descargarlo. En este caso, se utilizó la versión 4.7.5-1, la cual es compatible con la versión 4.7 de Wazuh instalada en Rocky Linux. La descarga se realizó desde la página oficial

<https://documentation.wazuh.com/4.7/installation-guide/wazuh-agent/wazuh-agent-package-windows.html>.

Note To perform the installation, administrator privileges are required.

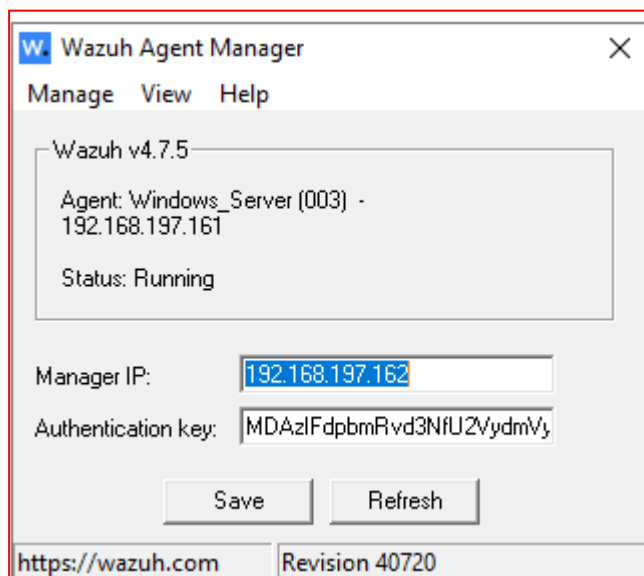
1. To start the installation process, download the [Windows installer](#).

A continuación, se ejecuta el comando de instalación desde la consola CMD, considerando la dirección IP del servidor en el que se encuentra instalado Wazuh.

```
wazuh-agent-4.7.5-1.msi /q WAZUH_MANAGER=192.168.197.162
```

5. Configurar Wazuh Agent para que se conecte con el servidor SIEM. (2 puntos)

Para la configuración del agente, se puede ejecutar la aplicación `win32ui`, ubicada en la ruta `C:\Program Files (x86)\ossec-agent`, una vez finalizada la instalación del agente, en el paso anterior.



La aplicación solicitará la dirección IP del servidor y la llave de autenticación, la cual debe obtenerse desde el servidor Wazuh.

Para obtener la clave, es necesario que el agente esté registrado con anterioridad. Este proceso se gestiona mediante el siguiente comando:

```
/var/ossec/bin/manage_agents
```

Al ejecutar este comando, y tomando la primera opción (Add an agente), se solicitará la dirección IP del agente, además de un nombre identificador para el mismo.

```
*****
* Wazuh v4.7.5 Agent manager.          *
* The following options are available:  *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
  * A name for the new agent: Windows_Server
  * The IP Address of the new agent: 192.168.197.161
Confirm adding it?(y/n): y
Agent added with ID 003.
```

Con el agente registrado, podemos obtener la key de autenticación, con el comando

```
/var/ossec/bin/manage_agents -e 003
```

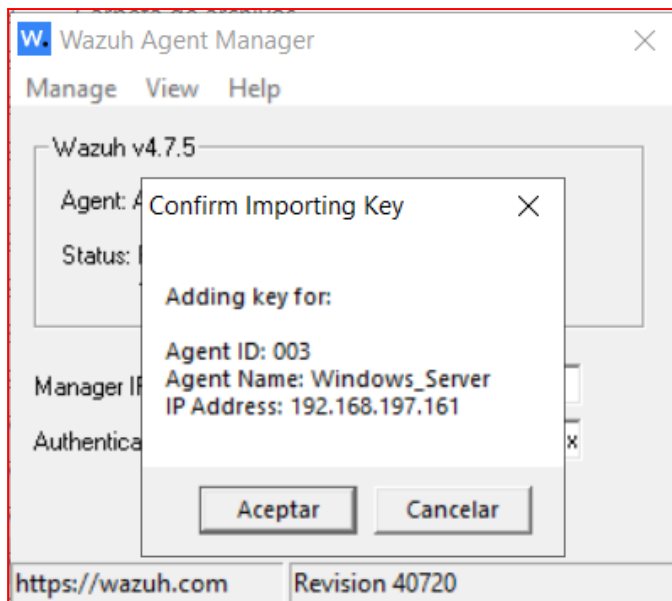
```
[root@localhost ~]# ./var/ossec/bin/manage_agents -e 003
```

Agent key information for '003' is:

MDAIZfDpbmRvd3Nfu2YydmVvIDE5MjI4XzJlZGUtMTk3LjE2MSAwN2EyMGY1MmMxOTIzM2E0ZmI5OTQ3ZjhZbnVmNEU5ODVmOTU1NjkvNztCZTgzODFyZTgzNjIzYzA5ZA5TAzY2I2

Es importante, tener claro el ID del agente, en mi caso el 003.

Una vez ingresados la dirección IP del servidor y la clave obtenida en la aplicación del agente en Windows Server, se puede inicializar el agente directamente desde la misma aplicación.



Posteriormente, la validación se realiza accediendo desde el navegador a la dirección del servidor con el puerto 443, en mi caso <https://192.168.197.162:443>

