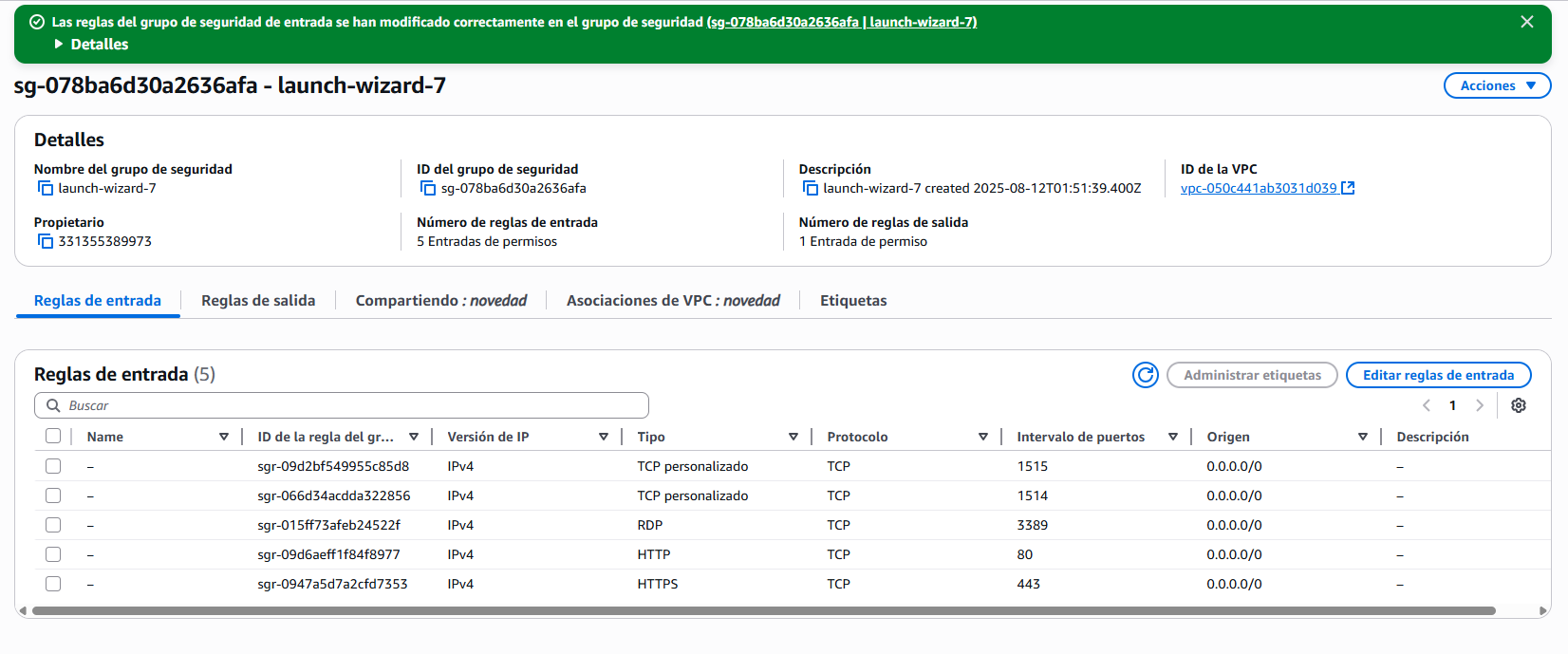
# **Desafio Diego Cabre 26489744-0**

# **1) (2 pts) Preparar/confirmar la VM Windows Server 2019 (AWS EC2)**

A. En la consola AWS → EC2 → Instances:

* Verifica AMI = *Windows Server 2019*
* Security Group: añade las reglas inbound:  
  + RDP TCP 3389 (tu IP).
  + Wazuh: TCP 1514 y TCP 1515 desde la IP pública privada del manager



B. Conectar por RDP:

* Obtén contraseña (EC2 → Actions → Get Windows password) y conéctate.

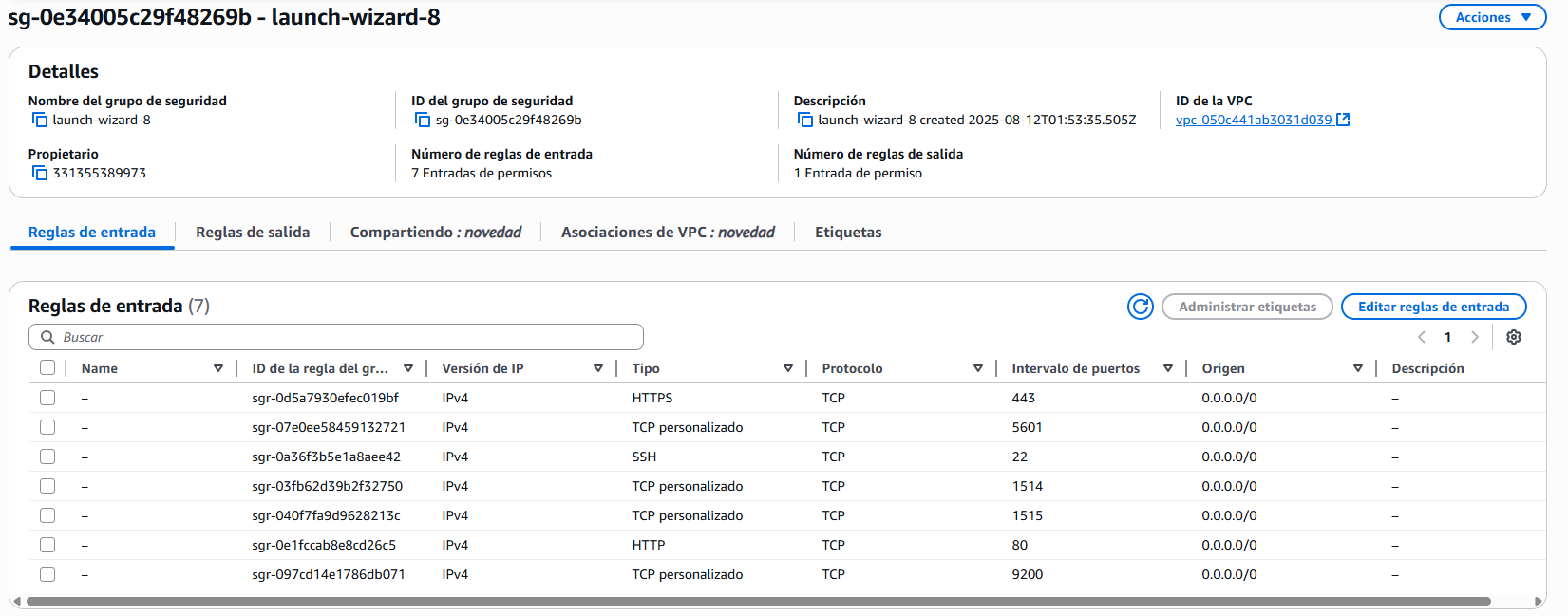
**2) Instalación de una máquina virtual con Sistema Operativo Fedora.**

En este caso use instancia de Ubuntu ya que la maquina virtual me corre muy lento

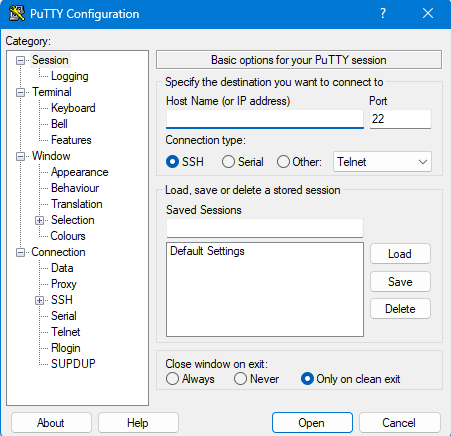
A. En la consola AWS → EC2 → Instances:

* Verifica AMI = Ubuntu 22.04
* Security Group: añade las reglas inbound:

Wazuh: TCP 1514 y TCP 1515 desde la IP pública privada del manager



por putty puedes conectarte mediante SSH con la clave guardada y la dirección pública

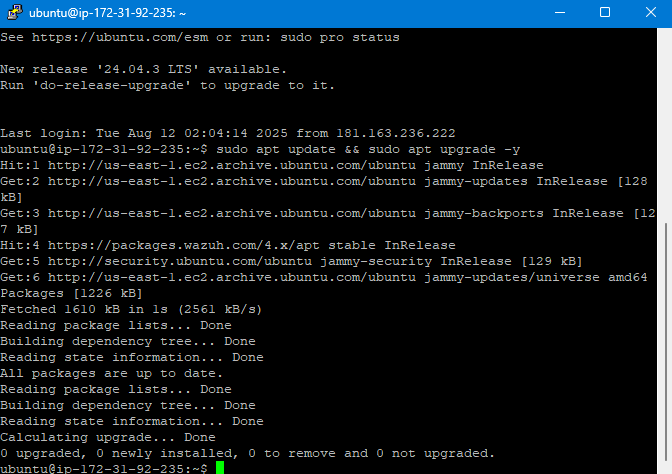


**3) Instalación de Wazuh en el Servidor con Ubuntu**

Usaremos el **Wazuh Installation Assistant** (instalación rápida *all-in-one*). Esto instala Wazuh indexer (buscador), manager y dashboard

Conéctate por SSH al servidor (Ubuntu) y ejecuta:

sudo apt update && sudo apt upgrade -y

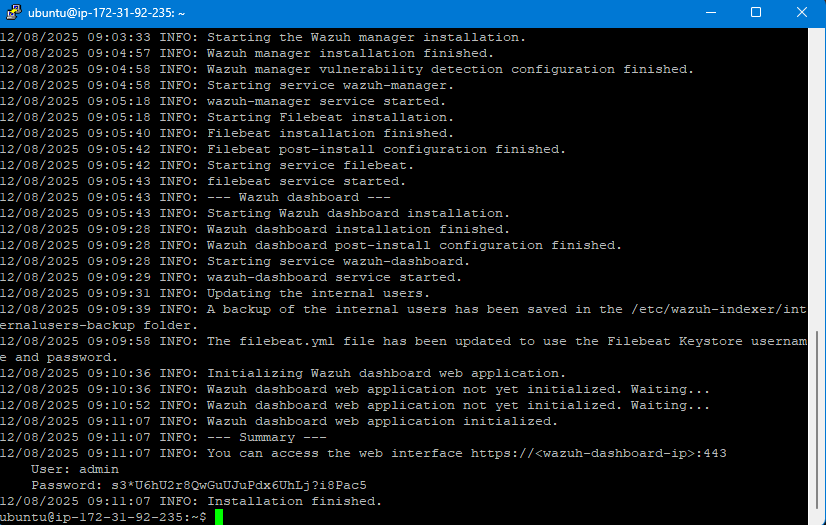


descargar el asistente (ejemplo con v4.12; la URL puede variar según versión)

curl -sO <https://packages.wazuh.com/4.12/wazuh-install.sh>

dar permisos y ejecutar la instalación all-in-one

sudo bash wazuh-install.sh -a



User: admin

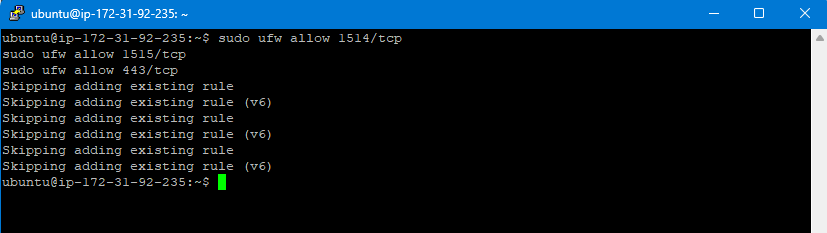
Password: s3\*U6hU2r8QwGuUJuPdx6UhLj?i8Pac5

Abrir puertos en el servidor

sudo ufw allow 1514/tcp

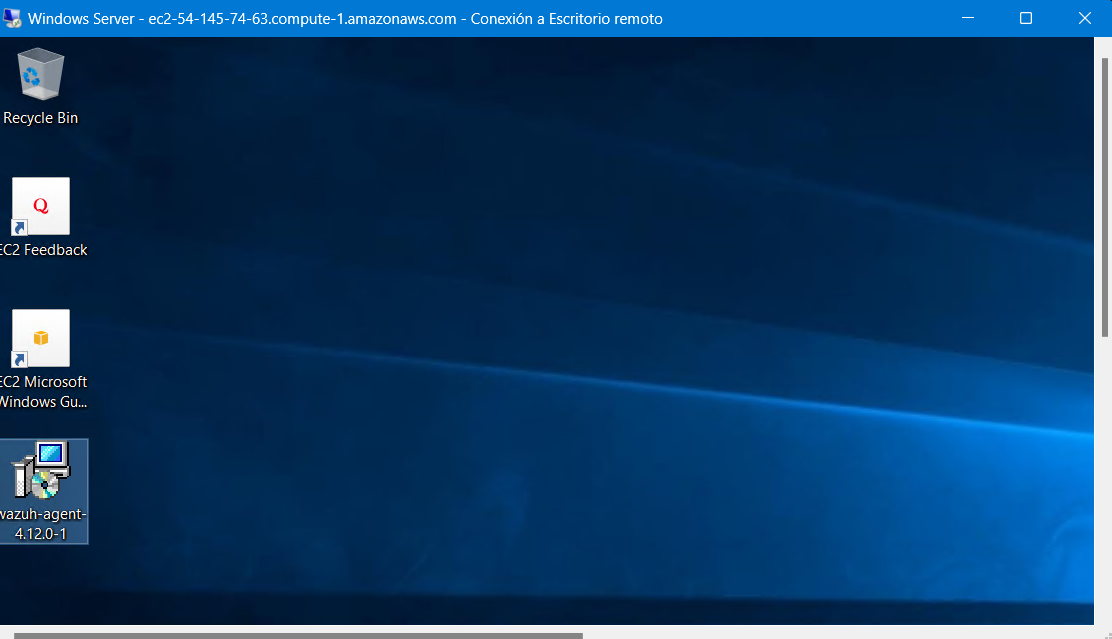
sudo ufw allow 1515/tcp

sudo ufw allow 443/tcp

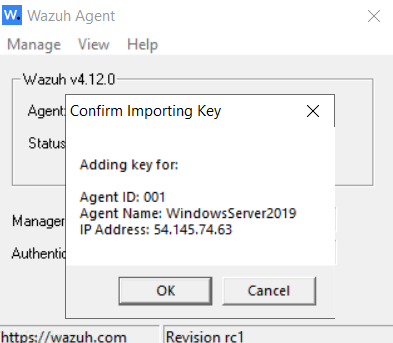


**4) Instalación del Wazuh Agent en Windows Server 2019**

Descargamos el agente en nuestro servidor Windows y le damos siguiente



en manager ip colocamos la ip pública o privada (si es un entorno de laboratorio) del servidor ubuntu



NOTA: LA clave de autenticación se obtiene de la siguiente forma:

Conéctate por SSH a tu máquina donde instalaste el **Wazuh Manager** y ejecuta:

sudo /var/ossec/bin/manage\_agents

Te saldrá un menú como este:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* Wazuh agent manager. \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Add an agent

2. Extract key for an agent

3. Remove an agent

4. List already added agents

5. Exit

### **Paso A: Añadir un agente nuevo**

Elige la opción **1** (*Add an agent*).

* Te pedirá el **nombre** (le coloque “WindowsServer2019”).
* IP del agente: puedes poner la IP privada de la instancia de Windows (si está en la misma VPC) o any.
* ID: lo asigna automáticamente.

### **Paso B: Obtener la clave**

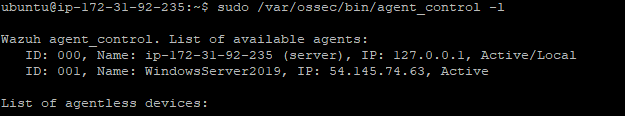
Después de crearlo, elige la opción **2** (*Extract key for an agent*).

* Selecciona el agente que acabas de crear.
* Copia la **Authentication key** que aparece (es una cadena larga de letras y números).

**5) Configurar Wazuh Agent para que se conecte con el servidor SIEM**

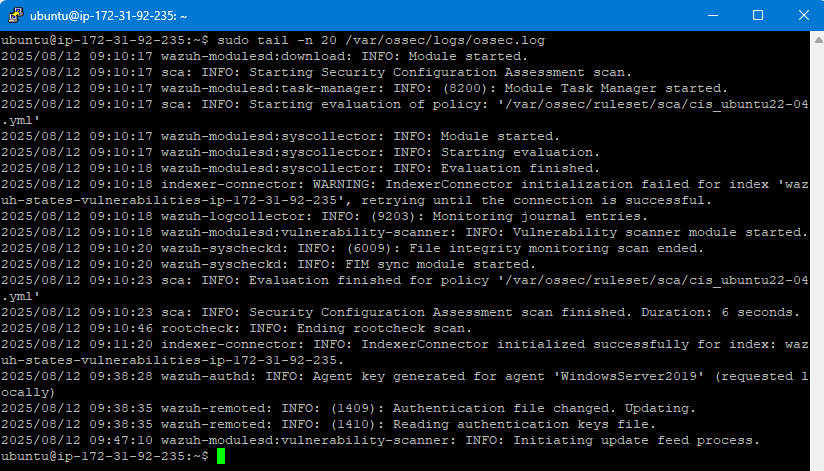
Para probar que tiene conexión, en ubuntu colocar el siguiente comando:

sudo /var/ossec/bin/agent\_control -l



podemos tambien ejecutar:

sudo tail -n 20 /var/ossec/logs/ossec.log



Registro en ossec.log que evidencia la generación de la clave y la actualización de archivo de autenticación para el agente WindowsServer2019 Agent key generated y Authentication file changed