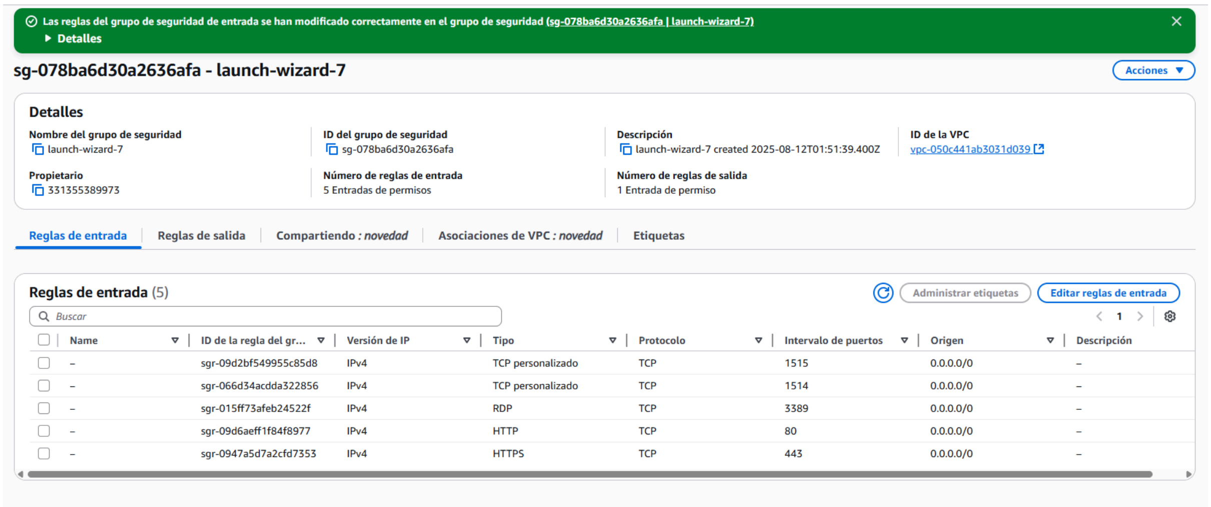
Desafio Diego Cabre 26489744-0

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



Las reglas del grupo de seguridad de entrada se han modificado correctamente en el grupo de seguridad (sg-078ba6d30a2636afa | launch-wizard-7)

▸ Detalles

sg-078ba6d30a2636afa - launch-wizard-7

Detalles

Nombre del grupo de seguridad: launch-wizard-7

ID del grupo de seguridad: sg-078ba6d30a2636afa

Descripción: launch-wizard-7 created 2025-08-12T01:51:39.400Z

ID de la VPC: vpc-050c441ab3031d039

Propietario: 331355389973

Número de reglas de entrada: 5 Entradas de permisos

Número de reglas de salida: 1 Entrada de permiso

Reglas de entrada (5)

□	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
□	–	sgr-09d2bf549955c85d8	IPv4	TCP personalizado	TCP	1515	0.0.0.0/0	–
□	–	sgr-066d34acdda322856	IPv4	TCP personalizado	TCP	1514	0.0.0.0/0	–
□	–	sgr-015ff73afeb24522f	IPv4	RDP	TCP	3389	0.0.0.0/0	–
□	–	sgr-09d6aeff1f84f8977	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-0947a5d7a2cfd7353	IPv4	HTTPS	TCP	443	0.0.0.0/0	–

B. Conectar por RDP:

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

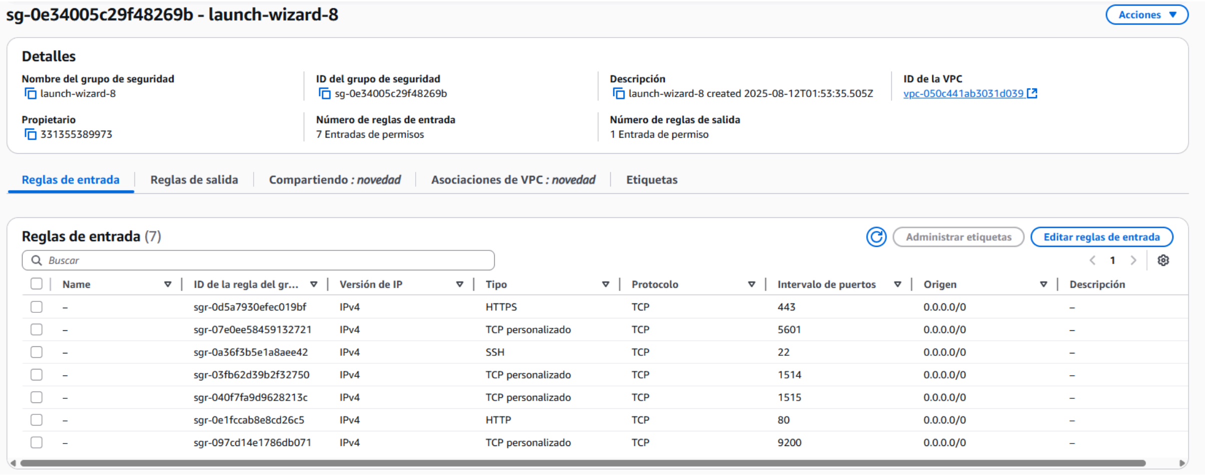
2) Instalación de una máquina virtual con Sistema Operativo Fedora.

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



sg-0e34005c29f48269b - launch-wizard-8

Detalles

Nombre del grupo de seguridad: launch-wizard-8

ID del grupo de seguridad: sg-0e34005c29f48269b

Descripción: launch-wizard-8 created 2025-08-12T01:53:35.505Z

ID de la VPC: vpc-050c441ab3031d039

Propietario: 331355389973

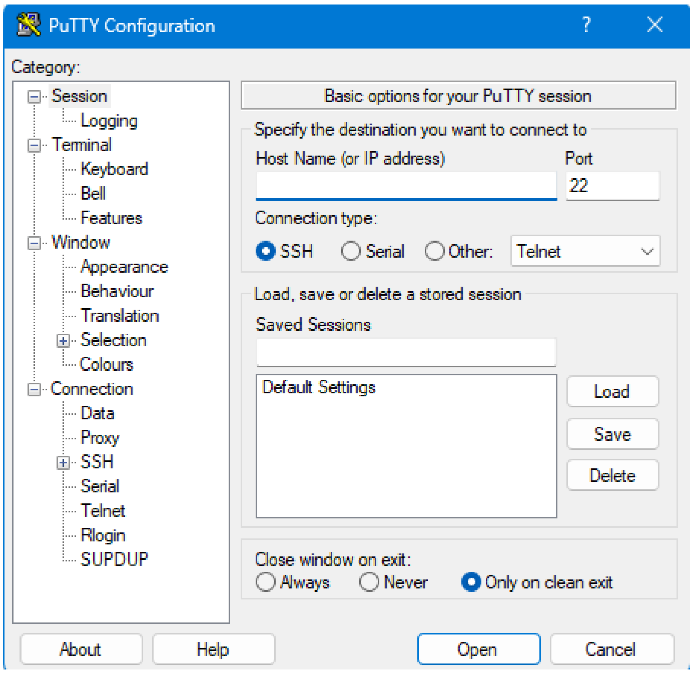
Número de reglas de entrada: 7 Entradas de permisos

Número de reglas de salida: 1 Entrada de permiso

Reglas de entrada (7)

□	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
□	–	sgr-0d5a7930efec019bf	IPv4	HTTPS	TCP	443	0.0.0.0/0	–
□	–	sgr-07e0ee58459132721	IPv4	TCP personalizado	TCP	5601	0.0.0.0/0	–
□	–	sgr-0a36f3b5e1a8aee42	IPv4	SSH	TCP	22	0.0.0.0/0	–
□	–	sgr-03fb62d39b2f32750	IPv4	TCP personalizado	TCP	1514	0.0.0.0/0	–
□	–	sgr-040f7fa9d9628213c	IPv4	TCP personalizado	TCP	1515	0.0.0.0/0	–
□	–	sgr-0e1fccab8e8cd26c5	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-097cd14e1786db071	IPv4	TCP personalizado	TCP	9200	0.0.0.0/0	–

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



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions:

Default Settings

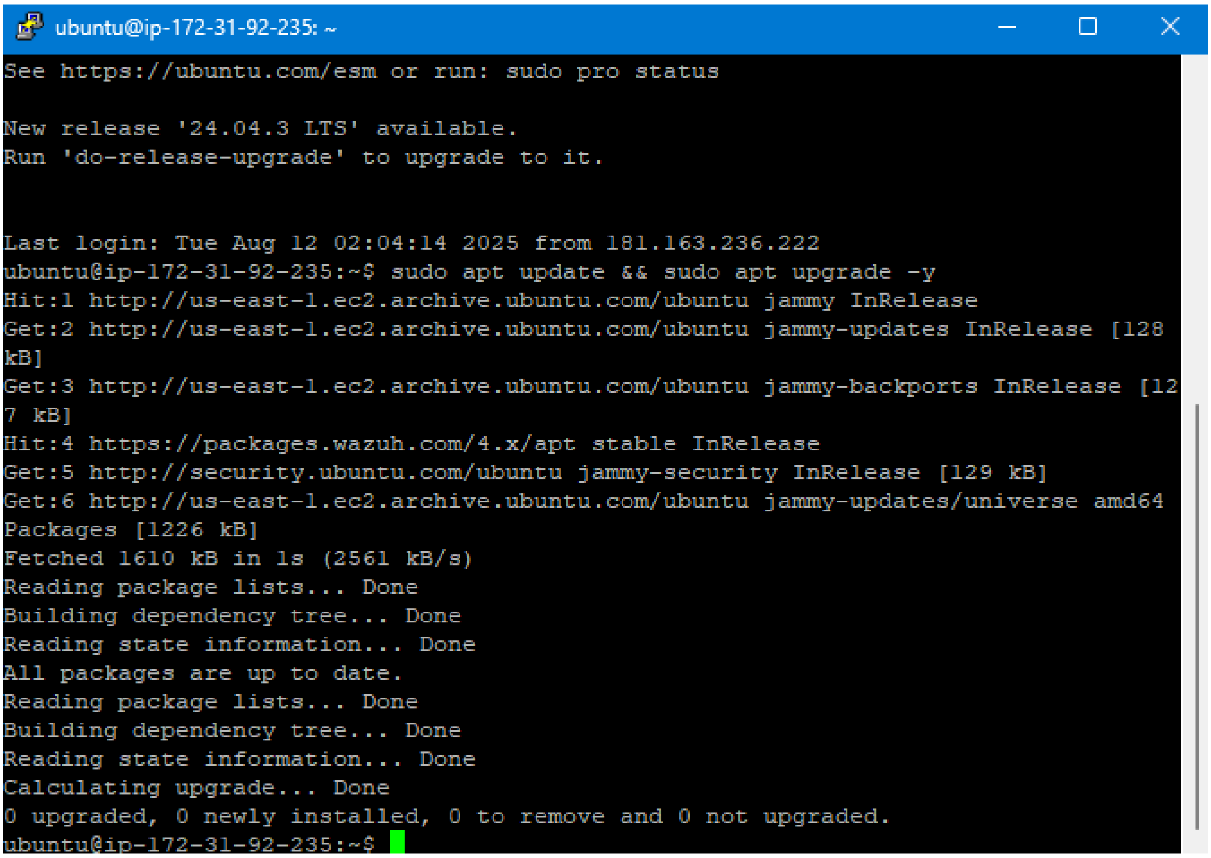
Close window on exit: ○ Always ○ Never ● Only on clean exit

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
```



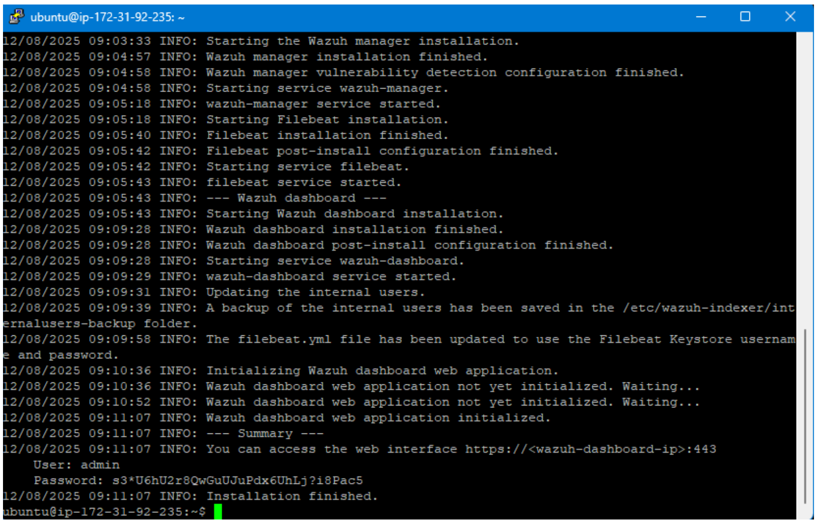
```
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Aug 12 02:04:14 2025 from 181.163.236.222
ubuntu@ip-172-31-92-235:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128
kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [12
7 kB]
Hit:4 https://packages.wazuh.com/4.x/apt stable InRelease
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64
Packages [1226 kB]
Fetched 1610 kB in 1s (2561 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-92-235:~$
```

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



```
12/08/2025 09:03:33 INFO: Starting the Wazuh manager installation.
12/08/2025 09:04:57 INFO: Wazuh manager installation finished.
12/08/2025 09:04:58 INFO: Wazuh manager vulnerability detection configuration finished.
12/08/2025 09:04:58 INFO: Starting service wazuh-manager.
12/08/2025 09:05:18 INFO: wazuh-manager service started.
12/08/2025 09:05:18 INFO: Starting Filebeat installation.
12/08/2025 09:05:40 INFO: Filebeat installation finished.
12/08/2025 09:05:42 INFO: Filebeat post-install configuration finished.
12/08/2025 09:05:42 INFO: Starting service filebeat.
12/08/2025 09:05:43 INFO: filebeat service started.
12/08/2025 09:05:43 INFO: --- Wazuh dashboard ---
12/08/2025 09:05:43 INFO: Starting Wazuh dashboard installation.
12/08/2025 09:09:28 INFO: Wazuh dashboard installation finished.
12/08/2025 09:09:28 INFO: Wazuh dashboard post-install configuration finished.
12/08/2025 09:09:28 INFO: Starting service wazuh-dashboard.
12/08/2025 09:09:29 INFO: wazuh-dashboard service started.
12/08/2025 09:09:31 INFO: Updating the internal users.
12/08/2025 09:09:39 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/int
ernalusers-backup folder.
12/08/2025 09:09:58 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore usernam
e and password.
12/08/2025 09:10:36 INFO: Initializing Wazuh dashboard web application.
12/08/2025 09:10:36 INFO: Wazuh dashboard web application not yet initialized. Waiting...
12/08/2025 09:10:52 INFO: Wazuh dashboard web application not yet initialized. Waiting...
12/08/2025 09:11:07 INFO: Wazuh dashboard web application initialized.
12/08/2025 09:11:07 INFO: --- Summary ---
12/08/2025 09:11:07 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: s3*U6hU2r8QwGuUJuPdx6UhLj?i8Pac5
12/08/2025 09:11:07 INFO: Installation finished.
ubuntu@ip-172-31-92-235:~$
```

User: admin

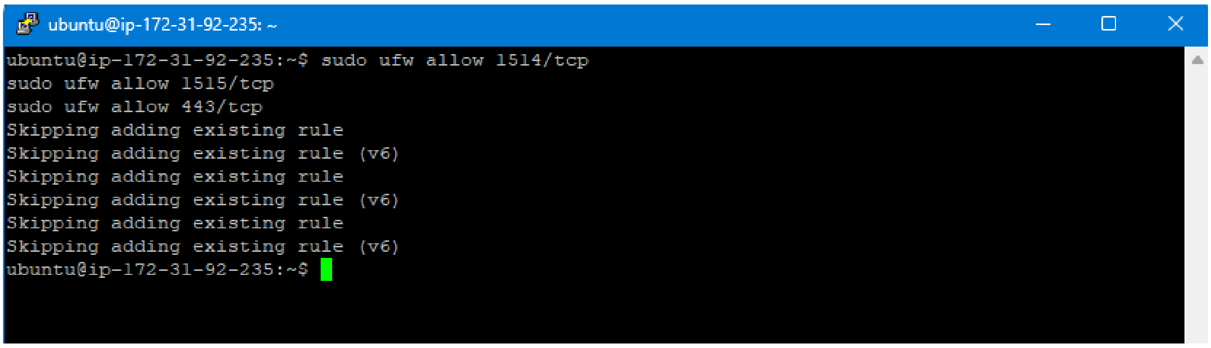
Password: s3*U6hU2r8QwGuUJuPdx6UhLj?i8Pac5

Abrir puertos en el servidor

sudo ufw allow 1514/tcp

sudo ufw allow 1515/tcp

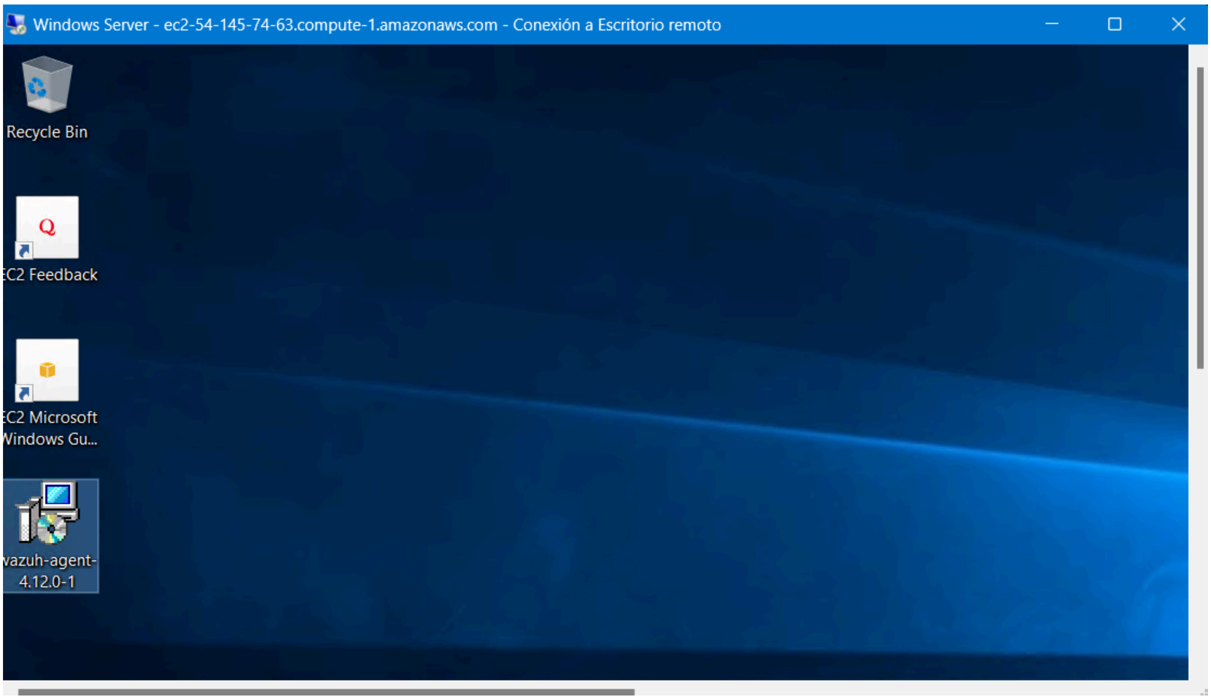
sudo ufw allow 443/tcp



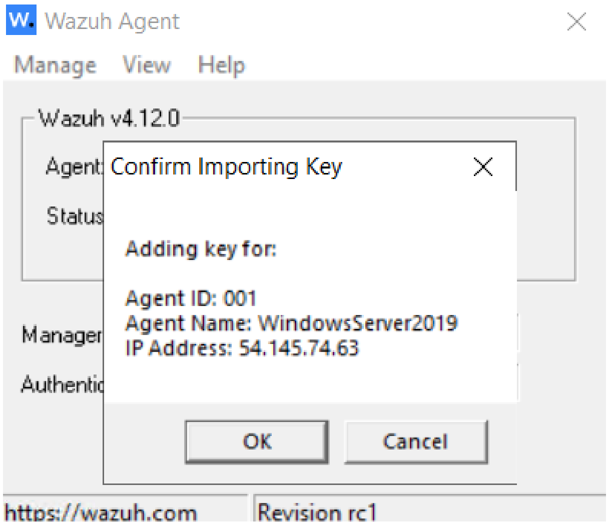
```
ubuntu@ip-172-31-92-235:~$ sudo ufw allow 1514/tcp
sudo ufw allow 1515/tcp
sudo ufw allow 443/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
Skipping adding existing rule
Skipping adding existing rule (v6)
Skipping adding existing rule
Skipping adding existing rule (v6)
ubuntu@ip-172-31-92-235:~$
```

4) Instalación del Wazuh Agent en Windows Server 2019

Descargamos el agente en nuestro servidor Windows y le damos siguiente


Windows Server - ec2-54-145-74-63.compute-1.amazonaws.com - Conexión a Escritorio remoto
Recycle Bin
EC2 Feedback
EC2 Microsoft Windows Gu...
wazuh-agent-4.12.0-1

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



Confirm Importing Key

Adding key for:

Agent ID: 001
Agent Name: WindowsServer2019
IP Address: 54.145.74.63

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

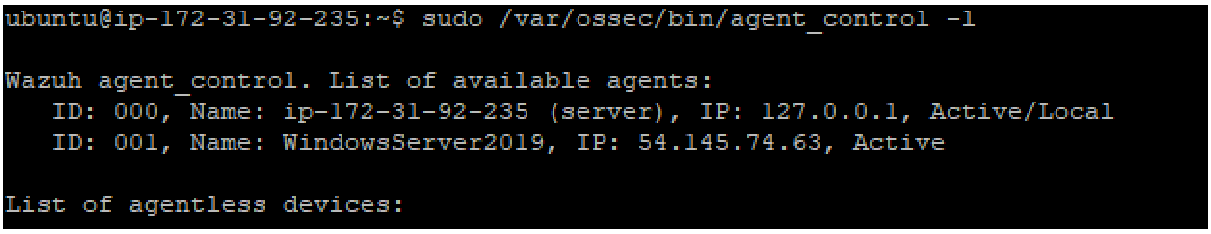
Después de crearlo, elige la opción **2** (*Extract key for an agent*).

- 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:

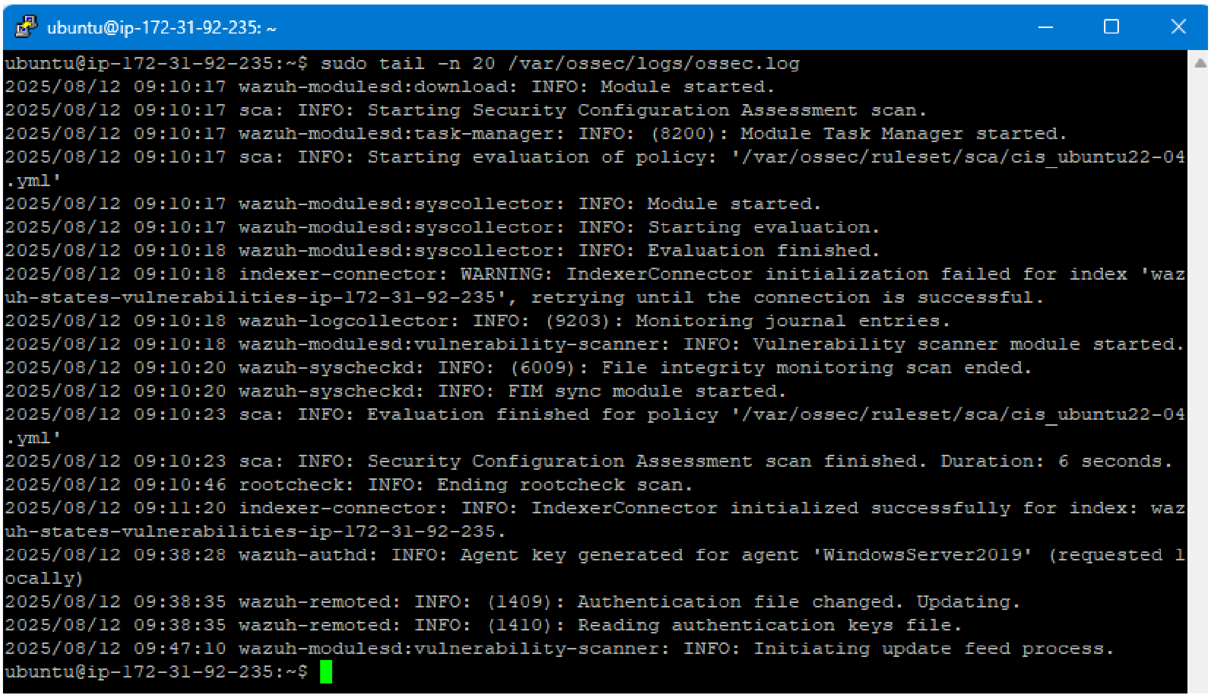
sudo /var/ossec/bin/agent_control -l



```
ubuntu@ip-172-31-92-235:~$ sudo /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
   ID: 000, Name: ip-172-31-92-235 (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: WindowsServer2019, IP: 54.145.74.63, Active

List of agentless devices:
```

podemos tambien ejecutar:

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



```
ubuntu@ip-172-31-92-235:~$ sudo tail -n 20 /var/ossec/logs/ossec.log
2025/08/12 09:10:17 wazuh-modulesd:download: INFO: Module started.
2025/08/12 09:10:17 sca: INFO: Starting Security Configuration Assessment scan.
2025/08/12 09:10:17 wazuh-modulesd:task-manager: INFO: (8200): Module Task Manager started.
2025/08/12 09:10:17 sca: INFO: Starting evaluation of policy: '/var/ossec/ruleset/sca/cis_ubuntu22-04
.yml'
2025/08/12 09:10:17 wazuh-modulesd:syscollector: INFO: Module started.
2025/08/12 09:10:17 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2025/08/12 09:10:18 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/08/12 09:10:18 indexer-connector: WARNING: IndexerConnector initialization failed for index 'waz
uh-states-vulnerabilities-ip-172-31-92-235', retrying until the connection is successful.
2025/08/12 09:10:18 wazuh-logcollector: INFO: (9203): Monitoring journal entries.
2025/08/12 09:10:18 wazuh-modulesd:vulnerability-scanner: INFO: Vulnerability scanner module started.
2025/08/12 09:10:20 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2025/08/12 09:10:20 wazuh-syscheckd: INFO: FIM sync module started.
2025/08/12 09:10:23 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/cis_ubuntu22-04
.yml'
2025/08/12 09:10:23 sca: INFO: Security Configuration Assessment scan finished. Duration: 6 seconds.
2025/08/12 09:10:46 rootcheck: INFO: Ending rootcheck scan.
2025/08/12 09:11:20 indexer-connector: INFO: IndexerConnector initialized successfully for index: waz
uh-states-vulnerabilities-ip-172-31-92-235.
2025/08/12 09:38:28 wazuh-authd: INFO: Agent key generated for agent 'WindowsServer2019' (requested l
ocally)
2025/08/12 09:38:35 wazuh-remoted: INFO: (1409): Authentication file changed. Updating.
2025/08/12 09:38:35 wazuh-remoted: INFO: (1410): Reading authentication keys file.
2025/08/12 09:47:10 wazuh-modulesd:vulnerability-scanner: INFO: Initiating update feed process.
ubuntu@ip-172-31-92-235:~$
```

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`