

Actividad 2

INSTALACIÓN Y CONFIGURACIÓN DE WAZUH

Miquel Rodríguez González

15 de mayo de 2024



wazuh.

Qué es Wazuh

Wazuh es un IDS de host de código abierto utilizado para la detección, visibilidad, y respuesta a amenazas de seguridad en entornos informáticos. Proporciona capacidades de monitoreo en tiempo real, análisis de registro, detección de intrusiones, y gestión de amenazas, entre otras funcionalidades.

Índice

1- Preparación.....	2
2- Creación de wazuh en la nube.....	2
3- Creación de agentes.....	6
3.1- Creación de un agente kali.....	6
3.1.1- Forzar eventos en kali.....	10
3.2- Creación de un agente windows 10.....	15
3.2.1- Forzar eventos en Windows 10.....	19
4- Conexiones extras.....	22

1- Preparación

- Tener un programa de virtualización
- Tener dos máquinas virtualizadas (1 kali linux y un windows 10 para este caso)
- Tener un correo corporativo (o correo temporal para pruebas)

2- Creación de wazuh en la nube

Estos pasos de creación de la página web, los podemos hacer directamente en nuestro equipo real, no hace falta hacerlo en ninguna máquina virtual.

Entramos a la página web de [wazuh](https://wazuh.com) y nos registramos. Necesitaremos un correo corporativo o un correo temporal en caso de que solo queramos hacer pruebas.

Create your account

Already have an account? [Log in](#)

First name
Pedro

Family name
Martnez

Business email
[Redacted]

Phone number
+34669669996

Password
@AVL8lyftotVB8Zym9CFqhGWIBkTkg35g

Company
ironhack

Country
Spain

Create account

Explore the potential of Wazuh Cloud

One new Cloud Console offers great advantages and flexibility for the users, making scalability options easier.

Processes are now greatly simplified and keeping track of your environments, invoices, and payments, is easier than ever.

Start your Free Trial

Get your 14 days trial. Sign up, register your first agent, and start enjoying Wazuh Cloud. You can cancel the trial at any time and **no credit card is required.**

[Learn more about Wazuh Cloud](#)

Verificamos nuestro email y ya podemos iniciar sesión

Cloud-delivered protection

Prevent, detect, and respond to threats in real time. Wazuh unifies historically separate functions into a single agent and platform architecture.

Email
[Redacted]

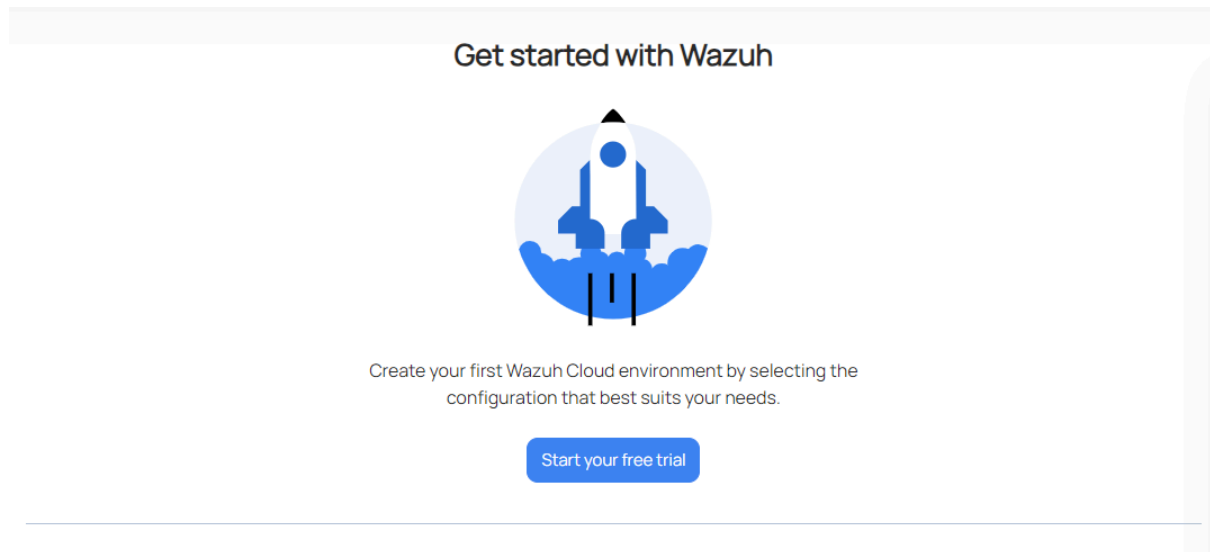
Password
[Masked]

Login

[Forgot your password?](#)

Don't have an account? [Sign up](#)

Empezamos con Wazuh



Configuramos nuestro entorno dándole un nombre, la región y todo lo necesario para crearlo

Create your environment

An environment contains all the Wazuh components ready for you to use. Once created, you only need to enroll your Wazuh agents to get started.

Name

mazhu2024

Region

Europe (Frankfurt)

Select your profile

Small

Medium

Large

Custom

Basic settings

- Active agents: Up to 100
- Indexed data retention: 1 month
- Archive data retention: 5 months
- Support plan: Standard support

Advanced settings

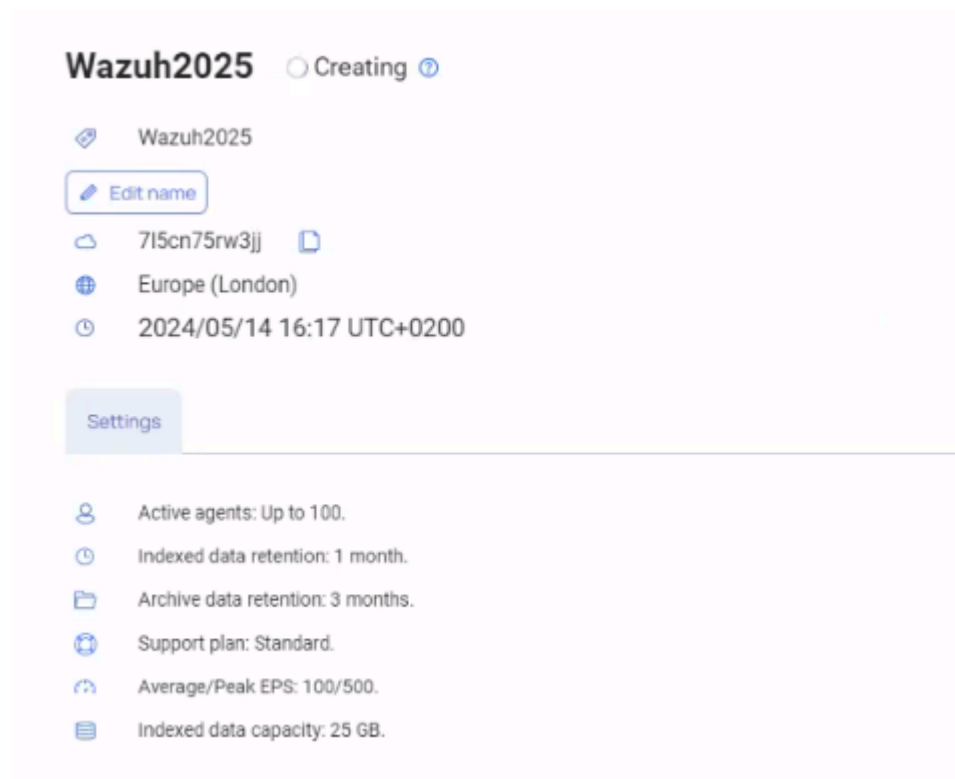
- Average/Peak EPS: 100 / 500 EPS
- Indexed data capacity: 25 GB

The recommended settings are based on our experience, but your workload may differ. Be sure to deploy, monitor, and adjust them as needed. [Read More](#).

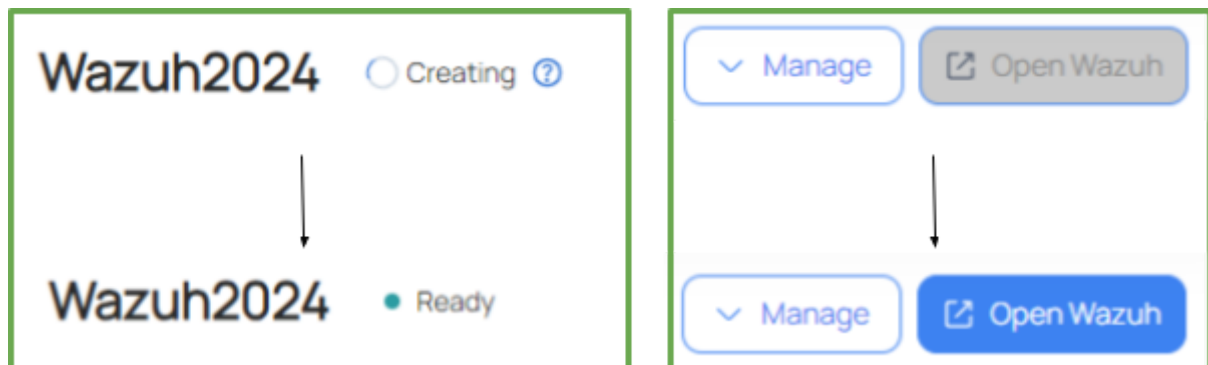
Iniciamos nuestra prueba gratuita

[Start your free trial](#)

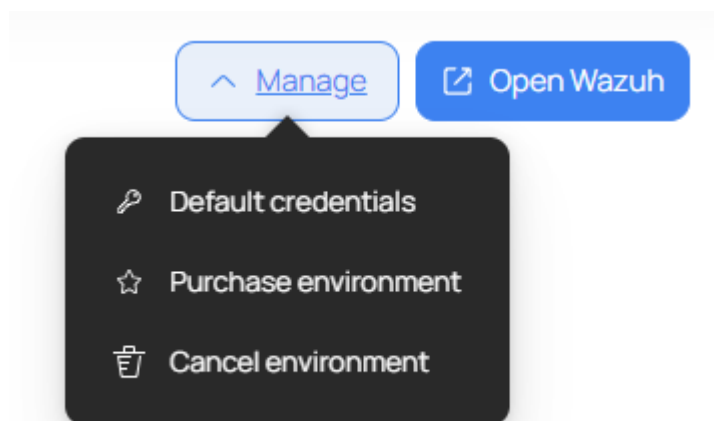
Una vez pulsado el botón wazuh creará nuestro entorno, esto puede tardar unos minutos



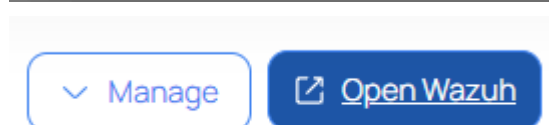
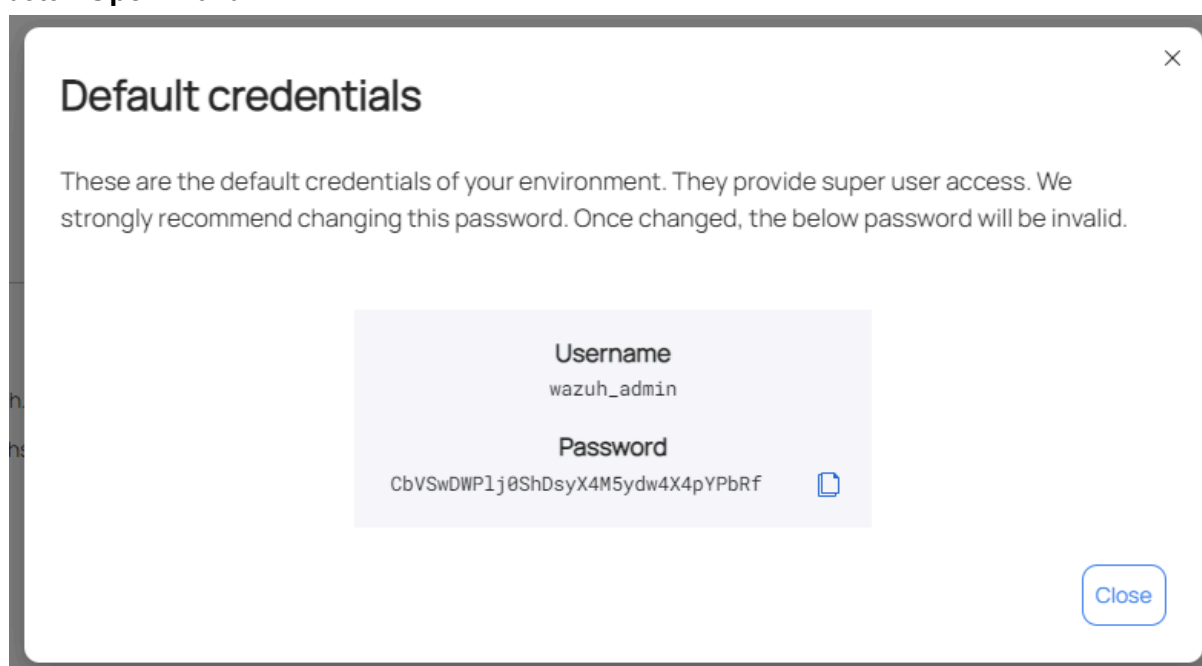
Tendremos que esperar que los siguientes cuadros se muestran como que el entorno ya ha sido creado



Para abrir wazuh lo primero que hacemos es ir a **Manage** y pulsar en **Default credentials**



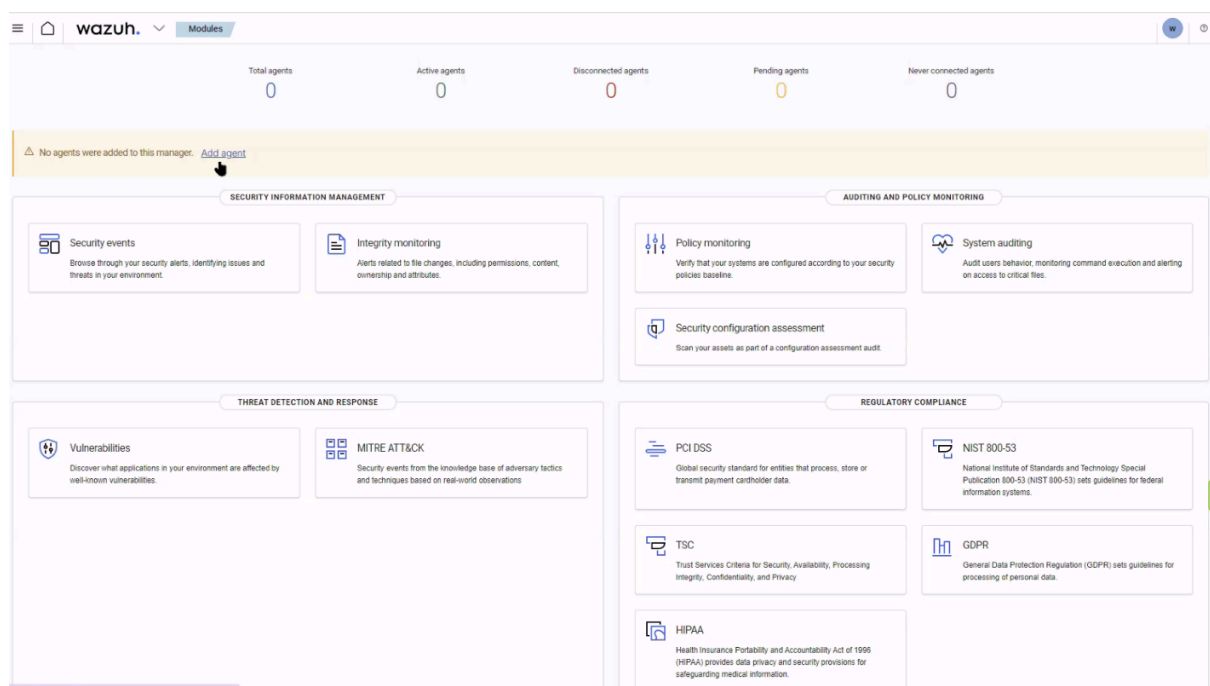
Este usuario y contraseña nos permitirán entrar en nuestro wazuh en cuanto pulsemos el botón **Open Wazuh**.



Iniciamos sesión con las credenciales anteriores



Aquí ya entramos en la página principal



3- Creación de agentes

3.1- Creación de un agente kali

En la parte superior podemos ver los distintos estados de los agents(equipos)

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	0


Vamos a añadir un nuevo agente a través de **Add agent**

⚠ No agents were added to this manager. [Add agent](#)


Seguimos los pasos para añadir un linux. En el caso de kali tenemos que seleccionar **DEB amd64**

✓


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 (FDQN).

Assign a server address: ?

gochyrrphzv5.cloud.wazuh.com

Le damos un nombre para poderlo diferenciarlo (**kaliLinux**)

✓

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: ?

KaliLinux

❗

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

Select one or more existing groups: ?

Default

Los siguientes pasos que nos indican los tendremos que hacer en el kali que queremos poner como agent

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

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb &&  
sudo WAZUH_MANAGER='gochyrrphzv5.cloud.wazuh.com'  
WAZUH_REGISTRATION_PASSWORD='$'*****' WAZUH_AGENT_NAME='KaliLinux' dpkg -  
i ./wazuh-agent_4.7.3-1_amd64.deb
```

☐ Show password

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.

5 Start the agent:

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

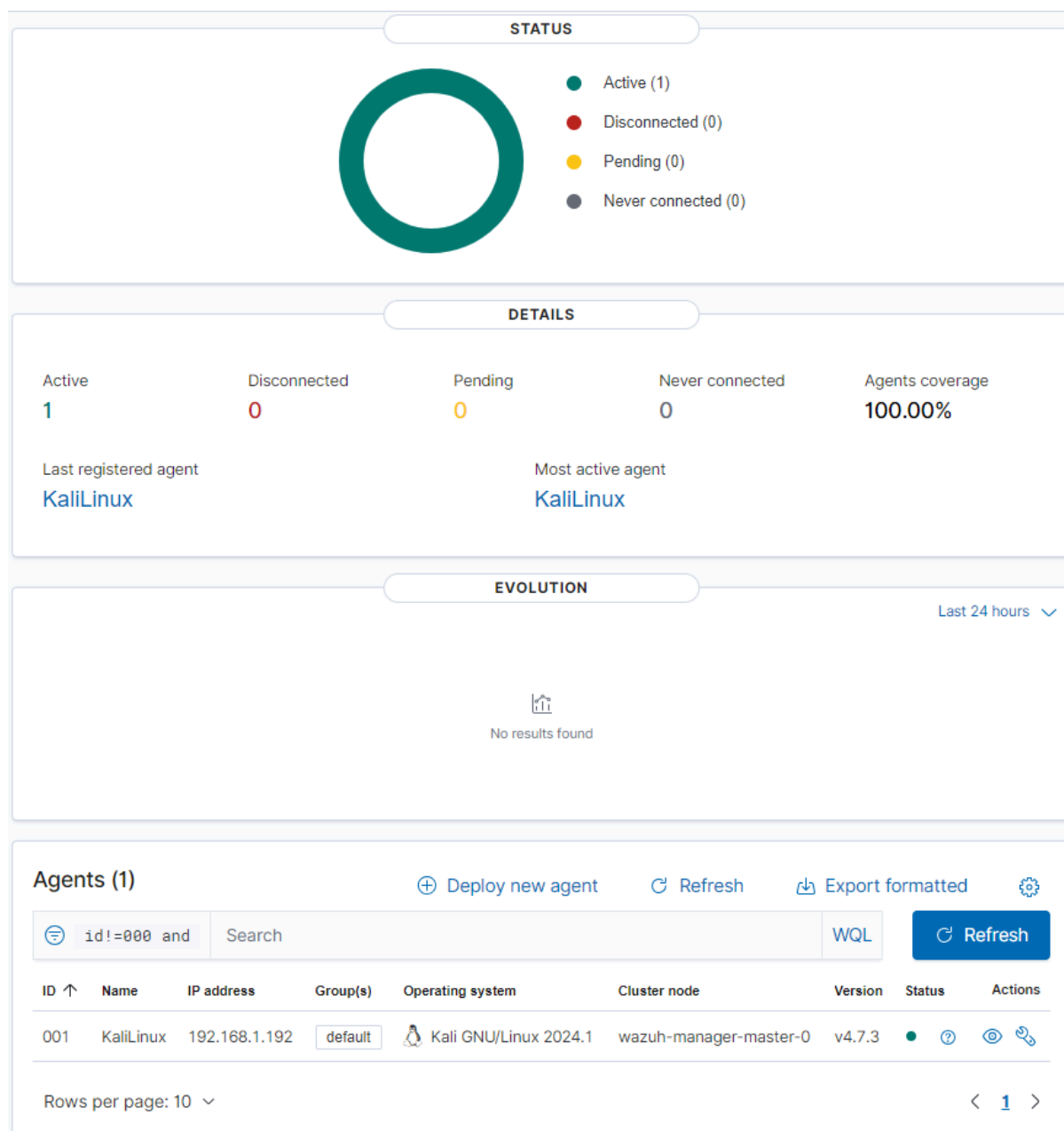
Abrimos nuestro Kali y ponemos el primer comando

```
(kali㉿kali)-[~]  
$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb && sudo WAZUH_MANAGER='gochyrrphzv5.cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='$'*****' WAZUH_AGENT_NAME='KaliLinux' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb  
--2024-05-16 10:08:11-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb  
Resolving packages.wazuh.com (packages.wazuh.com)... 18.154.48.95, 18.154.48.50, 18.154.48.117, ...  
Connecting to packages.wazuh.com (packages.wazuh.com)|18.154.48.95|:443 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 9362524 (8.9M) [binary/octet-stream]  
Saving to: 'wazuh-agent_4.7.3-1_amd64.deb'  
  
wazuh-agent_4.7.3-1_amd64.de 100%[=====>] 8.93M 4.68MB/s in 1.9s  
2024-05-16 10:08:13 (4.68 MB/s) - 'wazuh-agent_4.7.3-1_amd64.deb' saved [9362524/9362524]  
  
[sudo] password for kali:  
Selecting previously unselected package wazuh-agent.  
(Reading database ... 419534 files and directories currently installed.)  
Preparing to unpack .../wazuh-agent_4.7.3-1_amd64.deb ...  
Unpacking wazuh-agent (4.7.3-1) ...  
Setting up wazuh-agent (4.7.3-1) ...  
  
(kali㉿kali)-[~]  
$
```

Si todo ha salido correctamente vamos a por los siguiente comandos

```
(kali@kali)-[~]
$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
```

Si volvemos a la página de wazuh y acabamos el proceso de unir a kali como agent, podemos ver que efectivamente está unido



3.1.1- Forzar eventos en kali

Volvemos al kali e iniciamos distintos servicios. En el caso de este kali hago **systemctl start mariadb & systemctl start apache2 & a2enmod security2 & a2enmod headers**.

Con estos servicios iniciados vamos a intentar vulnerar una página web que tenemos en local.

[\(para más información puedes visitar la practica de modsecurity donde se utilizan estos servicios para hacer pruebas de seguridad en páginas web\)](#)

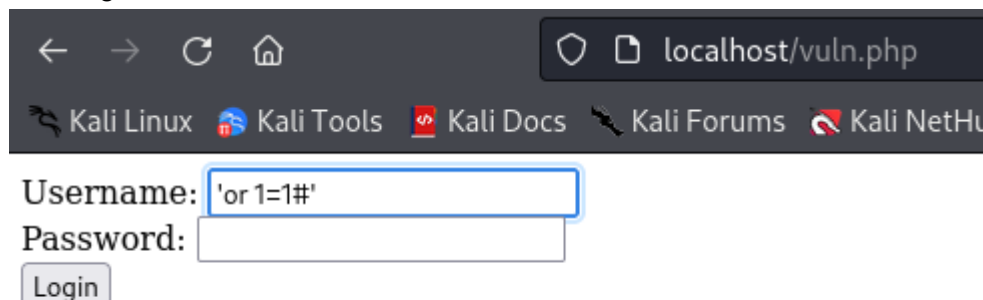
Si quieres saber qué servicios puedes activar en tu kali, puedes utilizar el comando **systemctl list-unit-files --type=service --state=disabled**

Si quieres ver los servicios activados utiliza **systemctl list-unit-files --type=service --state=enabled**

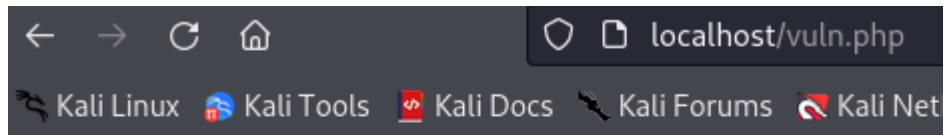
```
(kali㉿kali)-[~]
└─$ systemctl start mariadb & systemctl start apache2 & a2enmod security2 & a2enmod headers
[1] 9174
[2] 9175
[3] 9176
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
[3] + done          a2enmod security2
Module headers already enabled

(kali㉿kali)-[~]
└─$
[2] + done          systemctl start apache2
(kali㉿kali)-[~]
└─$
[1] + done          systemctl start mariadb
(kali㉿kali)-[~]
```

Abrimos una página que tenemos preparada con anterioridad y le hacemos una inyección de código con **'or 1=1#'**



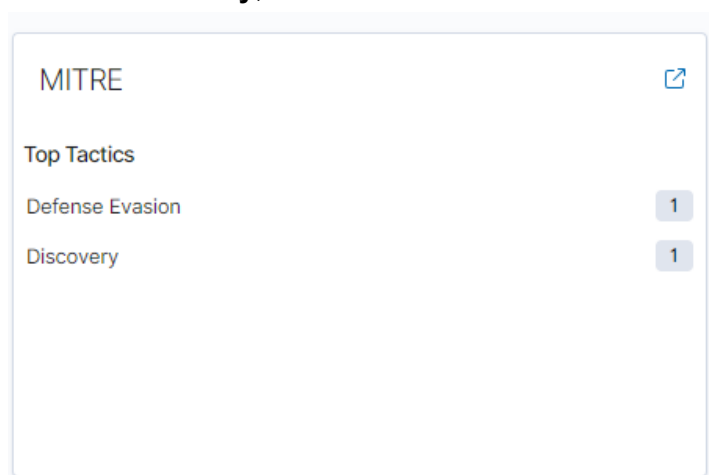
No nos deja pasar gracias al mod security que tenemos configurado



Forbidden

You don't have permission to access this resource.

Volvemos a la página de wazuh y refrescamos la página. podemos ver que hay un incidente llamado **Discovery**, entramos en el.



Hacemos click en el **T1083** que tenemos dentro.



Ahora podremos ver los detalles del incidente como en qué hora se ha producido, el nivel de amenaza, etc. También podemos ver que Modsecurity ha rechazado una query.

File and Directory Discovery

Technique details

ID

T1083

Tactics

Discovery

Version

1.4

Recent events

1 hits

Search

DQL

Last 24 hours

Show dates

Refresh

+ Add filter

Time	Technique(s)	Tactic(s)	Level	Rule ID	Description
May 16, 2024 @ 10:29:56.127	T1083	Discovery	7	30411	ModSecurity: Rejected a query

Rows per page: 10

< 1 >

Si nos dirigimos a **Modules** y **Security events** tendremos más información

Modules

Inventory data

Stats

Configuration

Security information management

Security events

Integrity monitoring

Threat detection and response

Vulnerabilities

MITRE ATT&CK

Auditing and Policy Monitoring

Policy Monitoring

System Auditing

Security configuration assessment

Regulatory Compliance

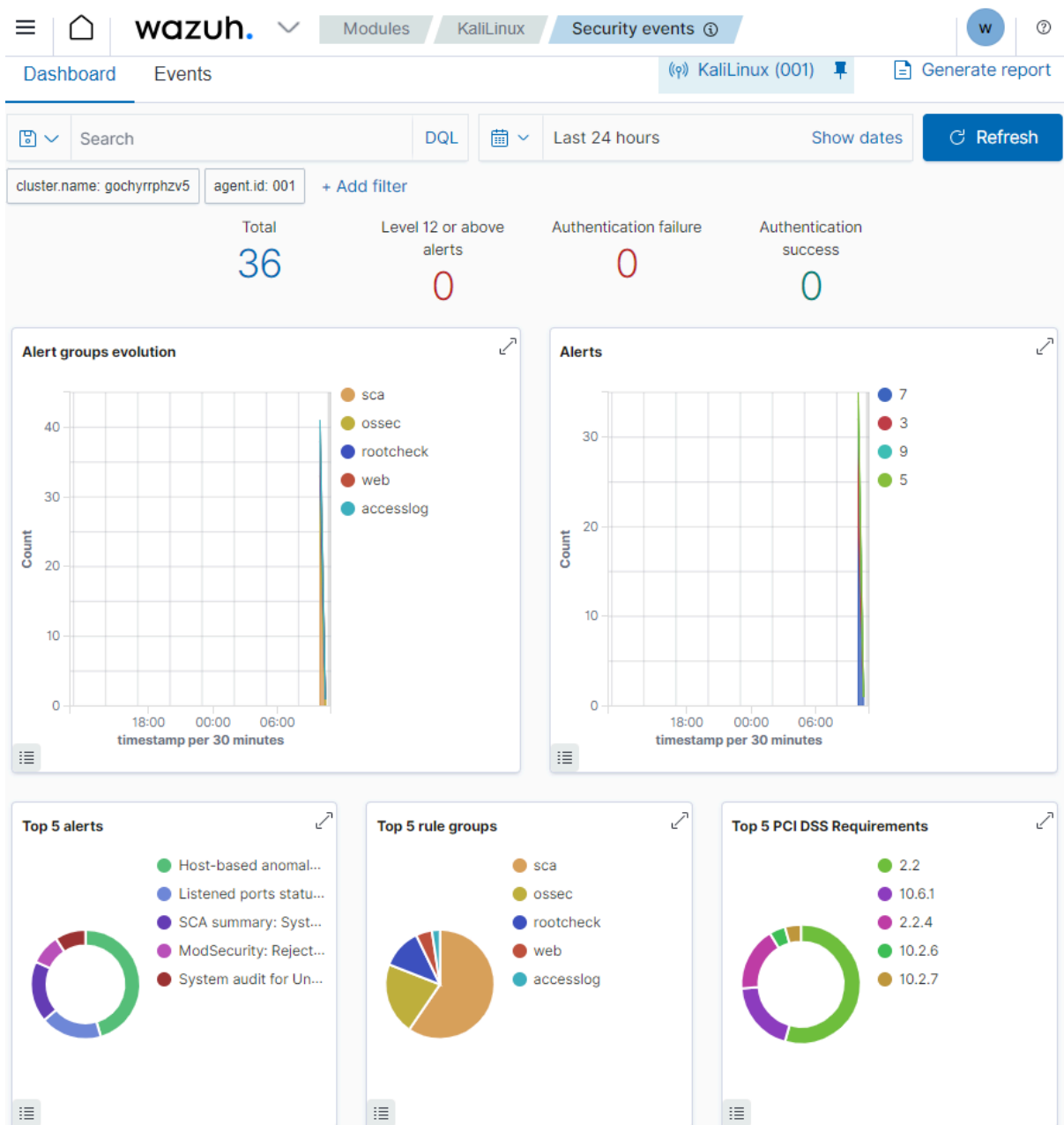
PCI DSS

GDPR

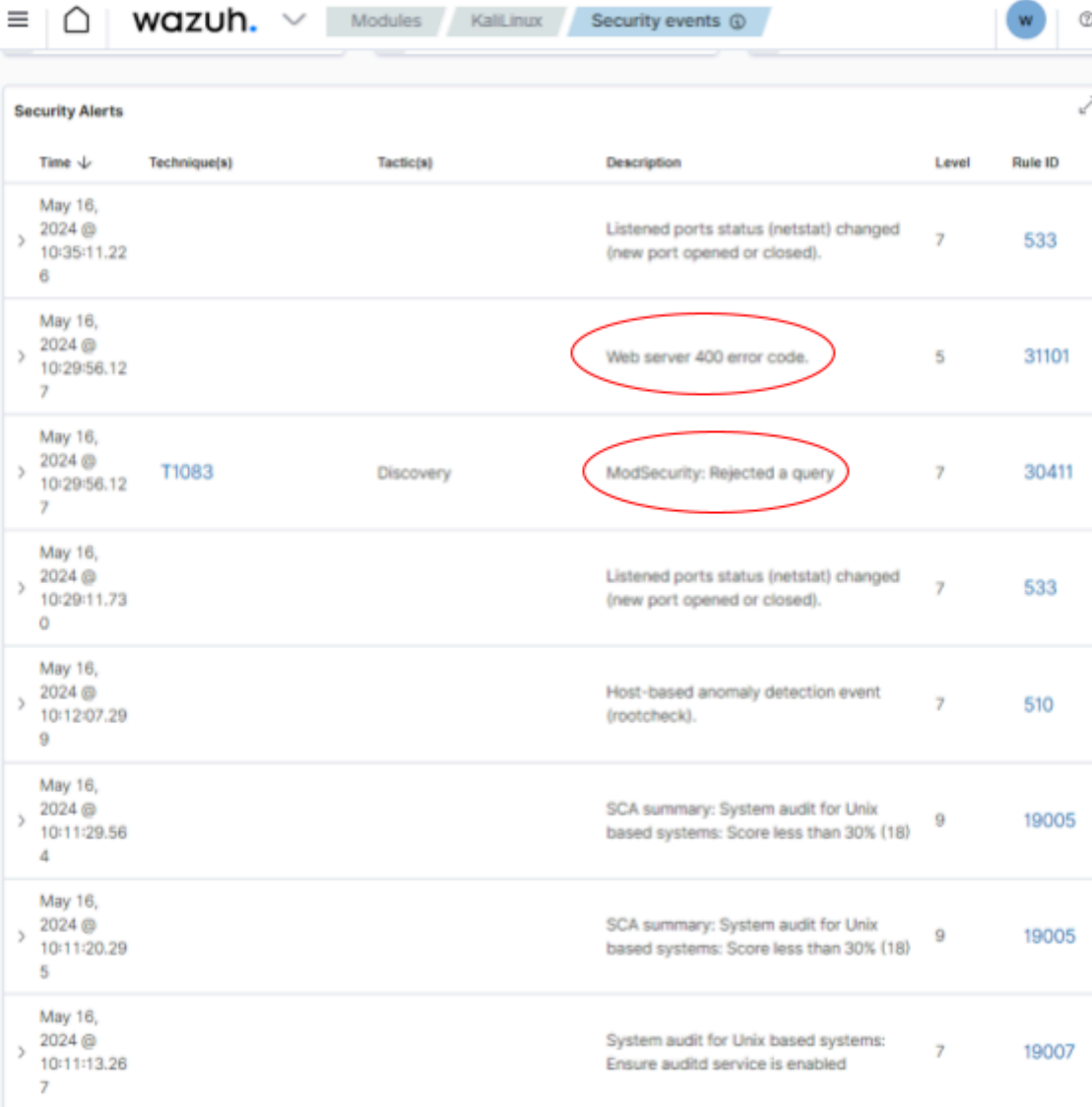
HIPAA

NIST 800-53

TSC



Si hacemos un poco de scroll tendremos todos los eventos, entre ellos podemos ver el evento lanzado por ModSecurity y el error 400

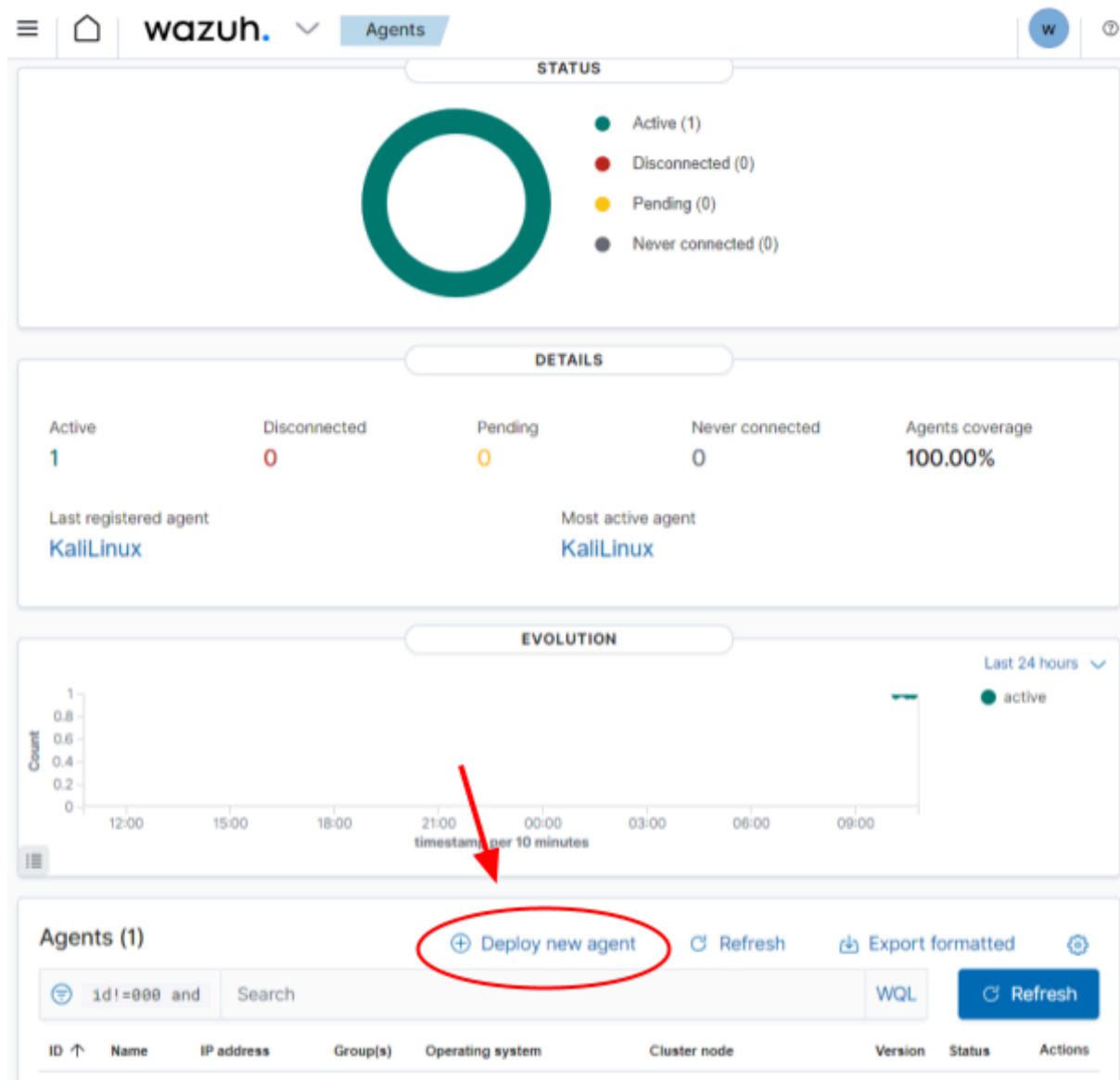


The screenshot shows the Wazuh Security Alerts interface. The top navigation bar includes the Wazuh logo, a dropdown menu, and tabs for 'Modules', 'Kali Linux', and 'Security events'. The 'Security events' tab is active. Below the navigation bar, there is a table titled 'Security Alerts'. The table has columns for 'Time', 'Technique(s)', 'Tactic(s)', 'Description', 'Level', and 'Rule ID'. The table contains eight rows of data. Two rows are circled in red: the second row with description 'Web server 400 error code.' and the third row with description 'ModSecurity: Rejected a query'.

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 16, 2024 @ 10:35:11.226			Listened ports status (netstat) changed (new port opened or closed).	7	533
May 16, 2024 @ 10:29:56.127			Web server 400 error code.	5	31101
May 16, 2024 @ 10:29:56.127	T1083	Discovery	ModSecurity: Rejected a query	7	30411
May 16, 2024 @ 10:29:11.730			Listened ports status (netstat) changed (new port opened or closed).	7	533
May 16, 2024 @ 10:12:07.299			Host-based anomaly detection event (rootcheck).	7	510
May 16, 2024 @ 10:11:29.564			SCA summary: System audit for Unix based systems: Score less than 30% (18)	9	19005
May 16, 2024 @ 10:11:20.295			SCA summary: System audit for Unix based systems: Score less than 30% (18)	9	19005
May 16, 2024 @ 10:11:13.267			System audit for Unix based systems: Ensure auditd service is enabled	7	19007




3.2- Creación de un agente windows 10

Volvemos a la pestaña de **Agents** y creamos uno nuevo para añadir un windows



Seleccionamos **MSI 32/64 bits**

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

 LINUX	 WINDOWS	 macOS
<div><input type="radio"/> RPM amd64</div> <div><input type="radio"/> RPM aarch64</div> <div><input type="radio"/> DEB amd64</div> <div><input type="radio"/> DEB aarch64</div>	<div><input checked="" type="radio"/> MSI 32/64 bits</div>	<div><input type="radio"/> Intel</div> <div><input type="radio"/> Apple silicon</div>

③ For additional systems and architectures, please check our documentation [↗](#).

Añadimos un nombre para poderlo identificarlo (**Windows 10**)

✓ **Server address:**

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

Assign a server address: [?](#)

gochyrphzv5.cloud.wazuh.com

✓ **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: [?](#)

Windows10

③ The agent name must be unique. It can't be changed once the agent has been enrolled. [↗](#)

Los siguiente comando tendremos que hacerlos dentro del windows10 que queremos añadir como agent

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

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi  
-OutFile ${env.tmp}\wazuh-agent; msixec.exe /i ${env.tmp}\wazuh-agent /q  
WAZUH_MANAGER='gochyrrphzv5.cloud.wazuh.com'  
WAZUH_REGISTRATION_PASSWORD='*****'  
WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='gochyrrphzv5.cloud.wazuh.com'
```

☐ Show password

Requirements

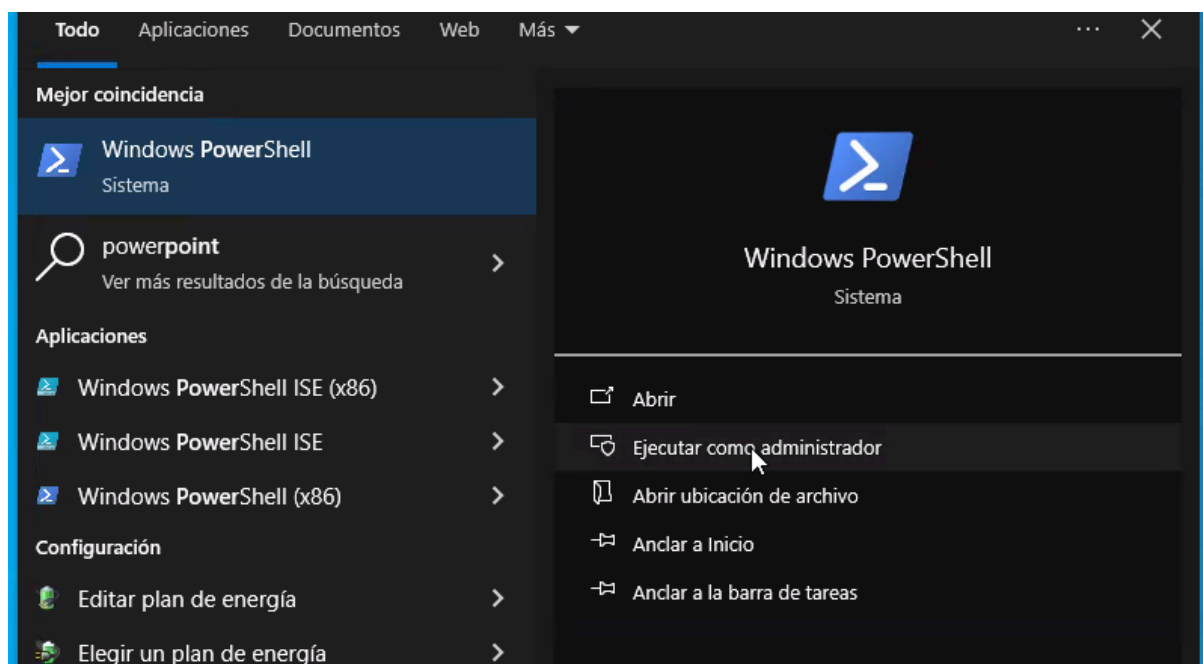
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

5 Start the agent:

```
NET START WazuhSvc
```

En el Windows10 buscamos **powershell** y haciendo click derecho le damos a **ejecutar como administrador**



Una vez abierta ponemos el primer comando indicado en las instrucciones

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\Administrador> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile ${env:tmp}\wazuh-agent; msixexec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='gochyrrphzv5.cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='RFvsHhZBbjmLTkeDK9SGrEtHZDFVNLvx' WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='gochyrrphzv5.cloud.wazuh.com'
```

Al ejecutar el comando:

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Escribiendo solicitud web
Escribiendo secuencia de solicitud... (Número de bytes escritos: 3499226)

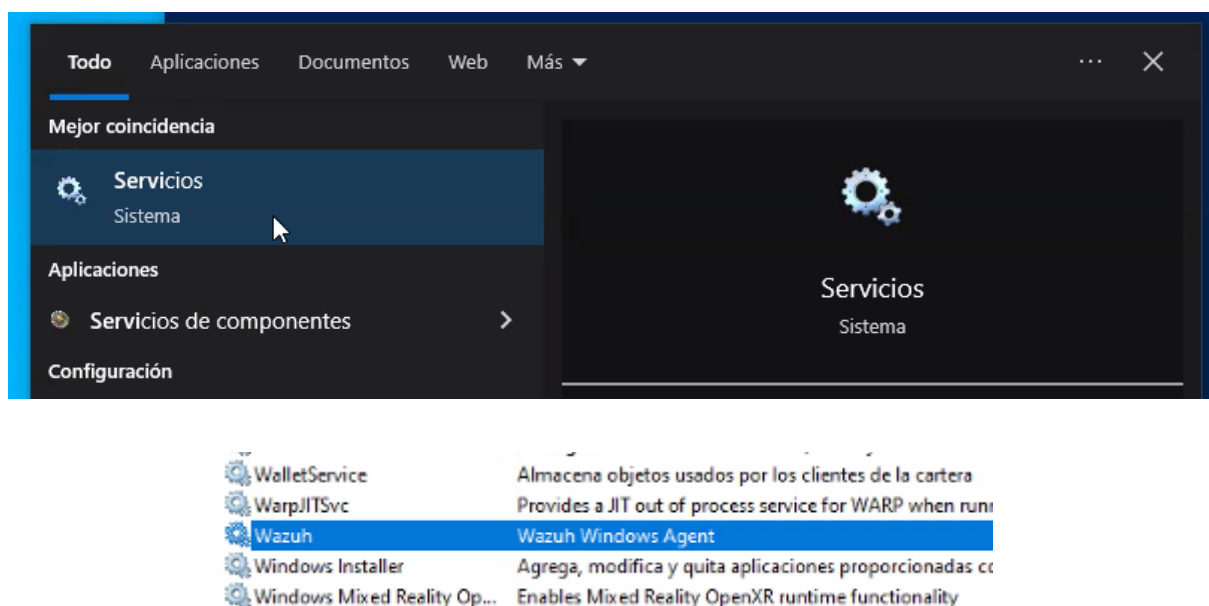
PS C:\Users\Administrador> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile ${env:tmp}\wazuh-agent; msixexec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='gochyrrphzv5.cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='RFvsHhZBbjmLTkeDK9SGrEtHZDFVNLvx' WAZUH_AGENT_NAME='Windows10' WAZUH_REGISTRATION_SERVER='gochyrrphzv5.cloud.wazuh.com'
```

Al completarse ponemos el segundo comando

```
PS C:\Users\Administrador> NET START WazuhSvc
El servicio de Wazuh está iniciándose.
El servicio de Wazuh se ha iniciado correctamente.

PS C:\Users\Administrador>
```

Podemos comprobar que tenemos el servicio de wazuh activado accediendo a servicios del sistema



Con esto hecho ya podemos volver a la página de wazuh y comprobar que tenemos el windows10 puesto como agent.

Agents (2)

⊕ Deploy new agent

🔄 Refresh

📄 Export formatted



⚙️

⊖ id!=000 and

Search

WQL

🔄 Refresh

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	KaliLinux x	192.168.1. 192	default	 Kali GNU/Linux 2024.1	wazuh-manager- master-0	v4.7.3	● ⓘ 👁 🔗	
002	Window s10	192.168.1. 195	default	 Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.587	wazuh-manager- master-0	v4.7.3	● ⓘ 👁 🔗	

Rows per page: 10 ▾

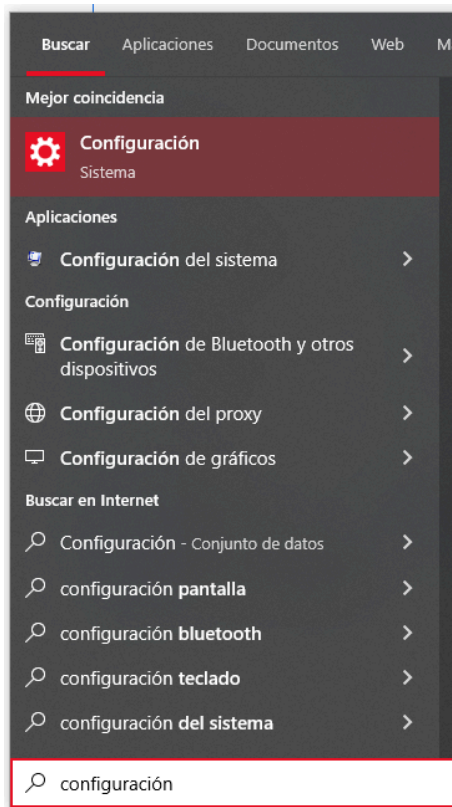
<

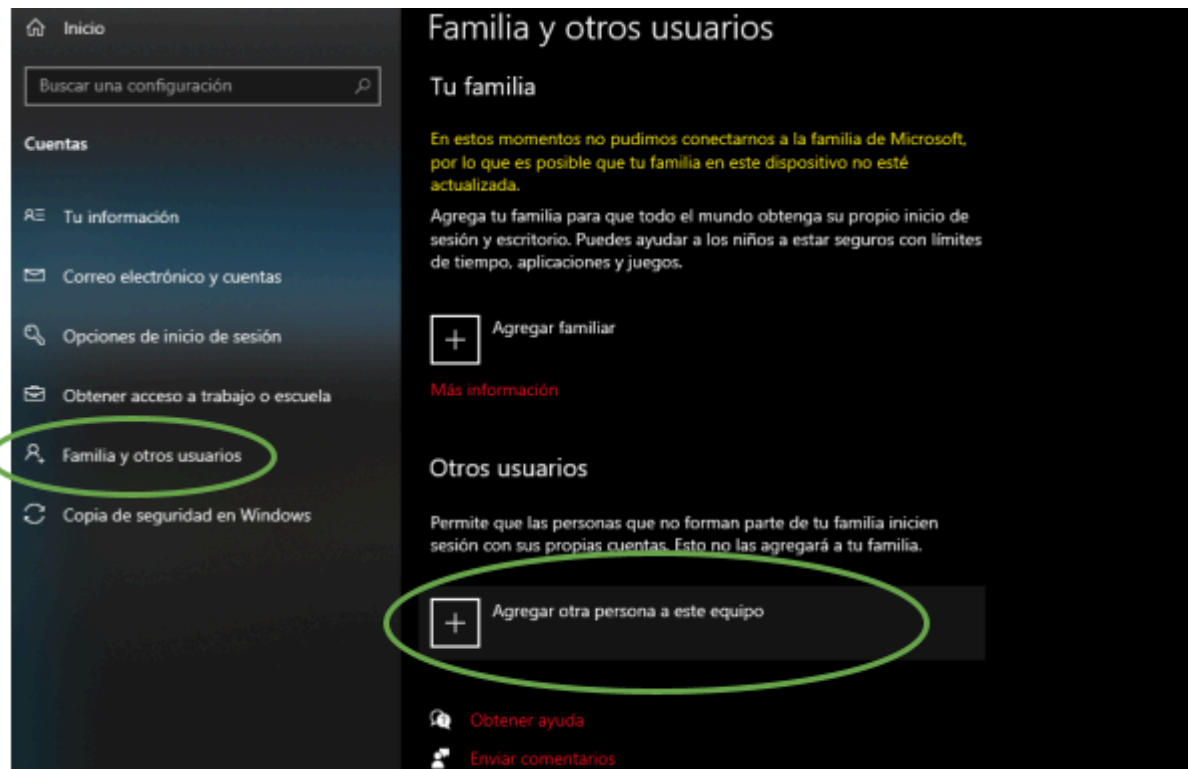
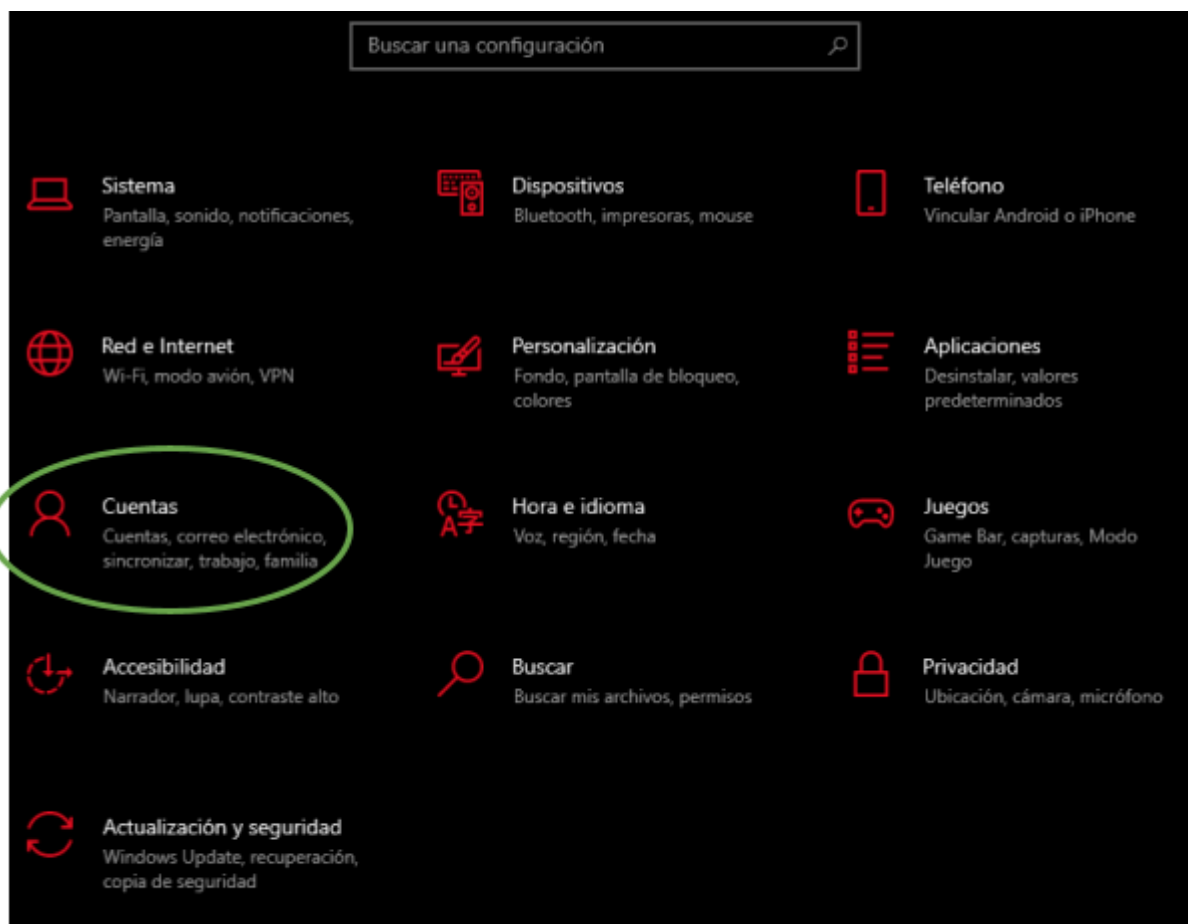
1

>

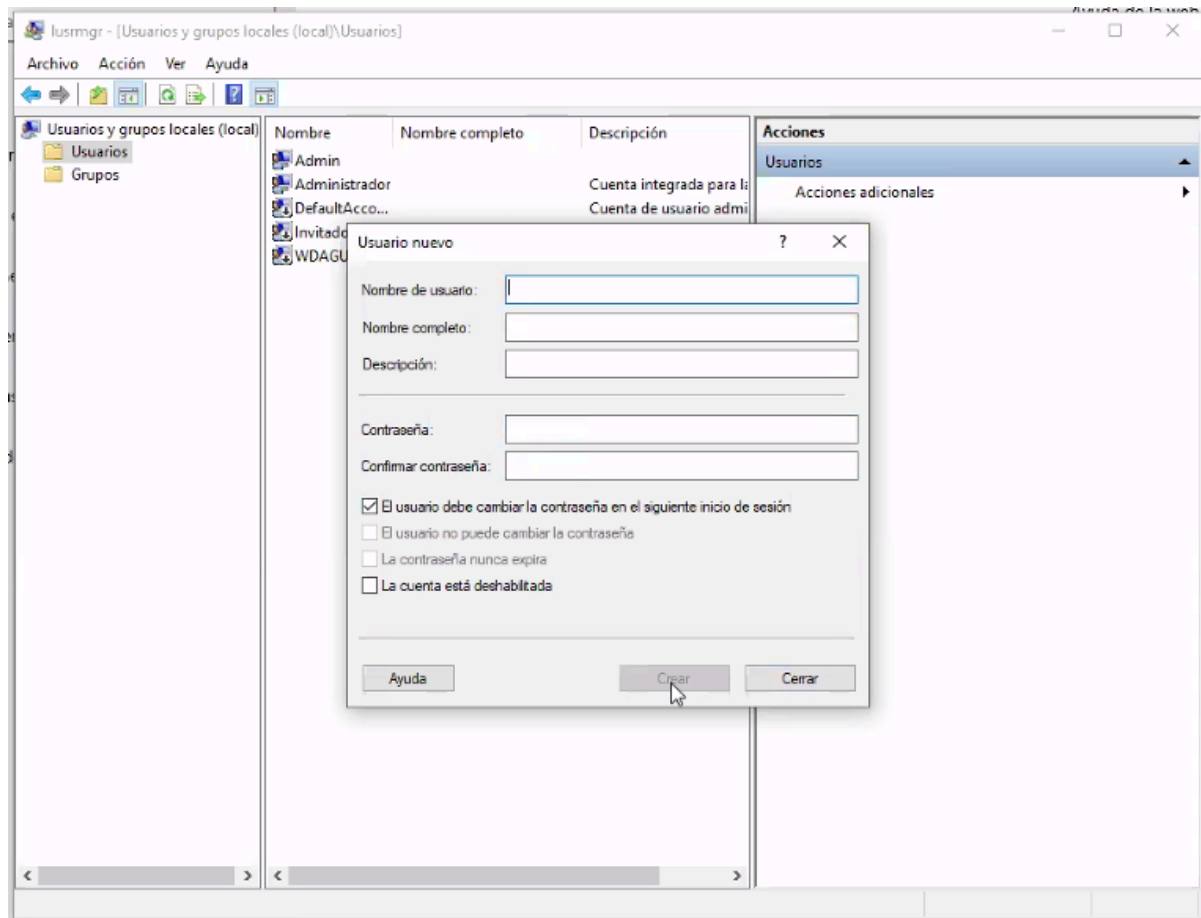
3.2.1- Forzar eventos en Windows 10

vamos a forzar una alerta por creación de usuario, para ello crearemos uno a través de **Configuración/Cuentas/Familia y otros usuarios**





Nos dirigimos a la carpeta de usuarios y creamos uno nuevo rellenando los campos a nuestro gusto



Volvemos a wazuh y entramos en el **agent windows10**, nos dirigimos a la pestaña de **Security events** donde podemos ver el evento de la creación del nuevo usuario

Recent events

Search

DQL

Last 24 hours

Show dates

+ Add filter

Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
> May 14, 2024 @ 17:15:21.346	T1098	Persistence	8	60110	User account changed.
> May 14, 2024 @ 17:15:21.216	T1098	Persistence	8	60110	User account changed.
> May 14, 2024 @ 17:15:21.170	T1098	Persistence	8	60110	User account changed.
> May 14, 2024 @ 17:15:21.144	T1098	Persistence	8	60109	User account enabled or created.
> May 14, 2024 @ 17:15:21.143	T1098	Persistence	8	60109	User account enabled or created.

Rows per page: 10

4- Conexiones extras

Para poder tener más alertas podemos conectar wazuh con cualquier servicio que tengamos. Algunos ejemplos podrían ser pfSense, suricata o snort. Solo tendremos que crear un agente de los equipos en los que están instalados y empezaremos a recibir sus eventos.