

Práctica BRS

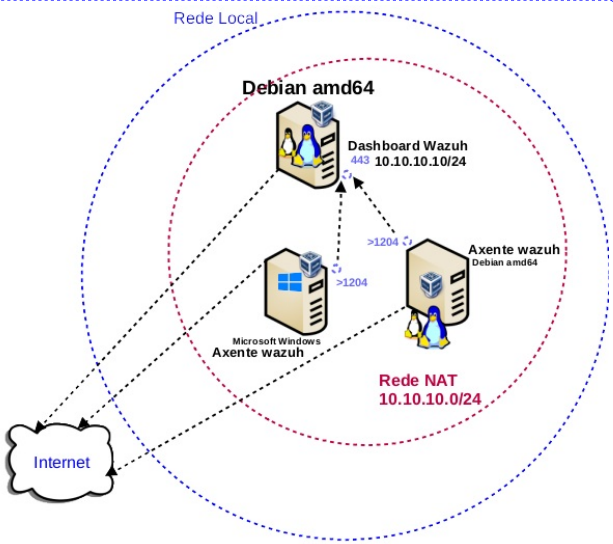
Auditoría, monitorización e protección de sistemas finais (endpoints): wazuh

ESCENARIO: wazuh

Wazuh → Máquina virtual Debian:
c Host
RAM ≥ 6144MB CPU ≥ 2
Disco duro: Debian amd64
docker
Wazuh: dashboard, manager, indexer
Rede: Rede NAT si-wazuh → 10.10.10.0/24
IP/MS: 10.10.10.10/24

Axente GNU/Linux
Máquina virtual Debian amd64:
c Host
RAM ≥ 2048MB CPU ≥ 2
Disco duro: Debian amd64
Rede: Rede NAT si-wazuh → 10.10.10.0/24
IP/MS: dinámica

Axente Microsoft Windows
Máquina virtual Microsoft Windows:
c Host
RAM ≥ 2048MB CPU ≥ 2
Disco duro: Windows amd64
Rede: Rede NAT si-wazuh → 10.10.10.0/24
IP/MS: dinámica



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- [1] wazuh (XDR, SIEM)
- [2] docker
- [3] docker hub
- [4] Cheat Sheet Docker A3
- [5] Explicacion Cheat-Sheet-Docker_A3
- [6] wazuh - docker

1. Configuración da rede según o escenario

Na contorna gráfica abrir un terminal e executar:

```
user@debian:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
user@debian:~$ su - #Acceder á consola de root(administrador) a través do comando su, o cal solicita o contrasinal do usuario root. Escribir o contrasinal de root para acceder.
```

```
root@debian:~# /etc/init.d/avahi-daemon stop || (systemctl stop avahi-daemon && systemctl stop avahi-daemon.socket) #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.
```

```
root@debian:~# systemctl disable avahi-daemon #Impide que o servizo avahi-daemon sexa iniciado no arranque xerando os links K* nos runlevels (/etc/rcX.d)
```

```
root@debian:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflito con este xestor.
```

```
root@debian:~# systemctl disable NetworkManager #Impide que o servizo NetworkManager sexa iniciado no arranque xerando os links K* nos runlevels (/etc/rcX.d)
```

```
root@debian:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de redes: loopback(lo) e a correspondente á Rede NAT(enp0s3).
```

```
$ man interfaces #Ver ás páxinas de manual referente ao ficheiro de configuración de rede /etc/network/interfaces
$ cat /etc/network/interfaces #Amosar o contido do ficheiro configuración de rede /etc/network/interfaces
$ ls -l /etc/network/interfaces.d #Listar de forma extendida o contido do directorio /etc/network/interfaces.d
```

```
root@debian:~# cat >> /etc/network/interfaces <<EOF
```

```
#Configuración interface enp0s3
```

```
auto enp0s3
```

```
iface enp0s3 inet static
```

```
address 10.10.10.24
```

```
gateway 10.10.10.1
```

```
EOF #Engadir ao ficheiro /etc/network/interfaces a configuración de enp0s3
```

```
root@debian:~# echo -e 'nameserver 8.8.8.8\nnameserver 8.8.4.4' > /etc/resolv.conf #Agregar servidores DNS para resolución de nomes.
```

```
root@debian:~# /etc/init.d/networking status #Comprobar o estado do demo networking, é dicir, comprobar se está activa a configuración de rede en /etc/network/interfaces (/etc/network/interfaces.d).
```

```
root@debian:~# /etc/init.d/networking restart || /etc/init.d/networking start #Arrancar o demo networking, é dicir, activar a configuración de rede en /etc/network/interfaces (/etc/network/interfaces.d).
```

```
root@debian:~# /etc/init.d/networking status #Comprobar o estado do demo networking, é dicir, comprobar se está activa a configuración de rede en /etc/network/interfaces (/etc/network/interfaces.d).
```

```
root@debian:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de redes: loopback(lo) e a correspondente á Rede NAT(enp0s3).
```

```
root@debian:~# ping -c4 10.10.10.10 #Comprobar mediante o comando ping a conectividade coa interface de rede local enp0s3
```

2. docker: Instalación e arranque

Executar no anterior terminal:

```
root@debian:~# apt update || apt-get update #Actualizar repositorios declarados no ficheiro /etc/apt/sources.list e nos ficheiros existentes no directorio /etc/apt/sources.list.d
```

Así, unha vez realizada a consulta dos ficheiros existentes nas rutas anteriores, descárganse uns ficheiros coas listas de paquetes posibles a instalar. Estes ficheiros son gardados en `/var/lib/apt/lists`

```
root@debian:~# apt -y install docker.io || apt-get -y install docker.io #Instalar o paquete de nome docker.io. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

```
root@debian:~# apt -y install docker-compose || apt-get -y install docker-compose #Instalar o paquete de nome docker-compose. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

```
root@debian:~# /etc/init.d/docker status || systemctl status docker #Comprobar o estado do demo docker
```

```
root@debian:~# /etc/init.d/docker start || systemctl start docker #Arrancar o demo docker
```

```
root@debian:~# /etc/init.d/docker status || systemctl status docker #Comprobar o estado do demo docker
```

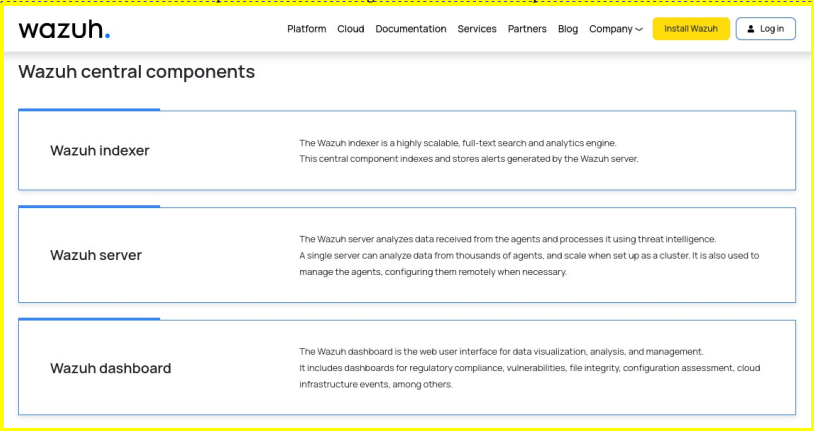
3. wazuh: Implantación en docker

Na contorna gráfica abrir un terminal e executar:

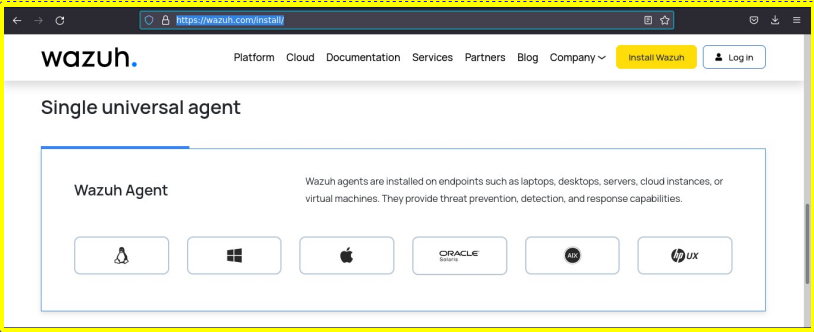
```
root@debian:~# git clone https://github.com/wazuh/wazuh-docker.git #Descargar wazuh dende github mediante git clone.
root@debian:~# cd wazuh-docker #Acceder ao directorio wazuh-docker
root@debian:~# git checkout tags/v4.9.2 -b wazuh-4.9.2 #Crear unha nova rama chamada wazuh-4.9.2 baseada na versión etiquetada v4.9.2.
```

Wazuh permite auditar, monitorizar e protexer sistemas finais ou endpoints. A solución Wazuh baséase no axente Wazuh, que se desprega nos puntos finais monitorizados, e en tres compoñentes centrais: o servidor Wazuh, o indexador de Wazuh e o panel de control de Wazuh:

- O indexador Wazuh é un motor de busca e análise de texto completo altamente escalable. Este compoñente central indexa e almacena as alertas xeradas polo servidor Wazuh.
- O servidor Wazuh analiza os datos recibidos dos axentes. Procésao mediante decodificadores e regras, utilizando intelixencia sobre ameazas para buscar indicadores de compromiso (IOC) coñecidos. Un único servidor pode analizar datos de centos ou miles de axentes e escalar horizontalmente cando se configura como un clúster. Este compoñente central tamén se utiliza para xestionar os axentes, configurándoos e actualizándoos de forma remota cando sexa necesario.
- O panel de control de Wazuh é a interface de usuario web para a visualización e análise de datos. Inclúe paneis listos para usar para eventos de seguridade, cumprimento normativo (por exemplo, PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), aplicacións vulnerables detectadas, datos de seguimento da integridade dos ficheiros, resultados da avaliación da configuración, seguimento da infraestrutura na nube, eventos e outros. Tamén se usa para xestionar a configuración de Wazuh e supervisar o seu estado.



Os axentes Wazuh instálanse en puntos finais(endpoints) como ordenadores portátiles, escritorios, servidores, instancias de nube ou máquinas virtuais. Ofrecen capacidades de prevención, detección e resposta de ameazas. Así, podemos desplegar **axentes wazuh (Single Universal Agent)** sobre sistemas operativos: GNU/Linux, Microsoft Windows, MacOS, Solaris, AIX, HP/UX.



```
root@debian:~# cd single-node #Acceder ao cartafol single-node.
root@debian:~# cat README.md #Ver o contido do ficheiro README.md que contén os pasos para o despregue de Wazuh en docker para a configuración nun único nodo (single node)
root@debian:~# sysctl -w vm.max_map_count=262144 #Incrementar o valor max_map_count: número máximo de mapas de memoria
root@debian:~# docker-compose -f generate-indexer-certs.yml run --rm generator #Xerar certificados para cada nodo para asegurar a comunicación entre os nodos.
root@debian:~# docker-compose up #Despregar os contenedores docker a través de docker-compose. Como non se indica coa opción -f un ficheiro, o ficheiro a interpretar será docker-compose.yml
```

```
root@debian:~# cat docker-compose.yml #Ver o contido do ficheiro wazuh-docker/single-node/docker-compose.yml
```

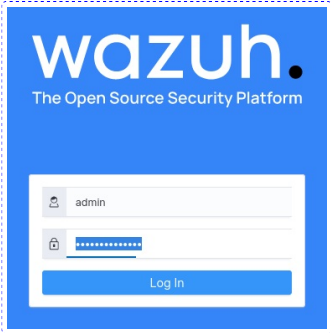
```
root@debian:~# docker container ls #Listar os contenedores docker activos.
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
b59ef4deef7a	wazuh/wazuh-dashboard:4.9.2	"/entrypoint.sh"	27 seconds ago	Up 24 seconds	443/tcp, 0.0.0.0:443->5601/tcp, :::443->5601/tcp	single-
node_wazuh_dashboard_1						
96ce4581a87b	wazuh/wazuh-indexer:4.9.2	"/entrypoint.sh open."	36 seconds ago	Up 27 seconds	0.0.0.0:9200->9200/tcp, :::9200->9200/tcp	single-
node_wazuh_indexer_1						
959ea21962e1	wazuh/wazuh-manager:4.9.2	"/init"	36 seconds ago	Up 27 seconds	0.0.0.0:1514-1515->1514-1515/tcp, :::1514-1515->1514-1515/tcp, 0.0.0.0:514->514/udp, :::514->514/udp, 0.0.0.0:55000->55000/tcp, :::55000->55000/tcp, 1516/tcp	single-
node_wazuh_manager_1						

Na contorna gráfica abrir outro terminal e executar:

user@debian:~\$ firefox https://localhost:443 & #Lanzar o navegador firefox na URL https://localhost:443 no porto TCP 443, realizando a execução em segundo plano (&), é dizer, acceder ao dashboard(panel de control) de wazuh.

Credenciais de acceso predeterminadas: admin/SecretPassword



Wazuh Overview dashboard showing security metrics and alerts.

AGENTS SUMMARY

No results

No results were found.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	47	144
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

- Configuration Assessment**
Scan your assets as part of a configuration assessment audit.
- Malware Detection**
Verify that your systems are configured according to your security policies baseline.
- File Integrity Monitoring**
Alerts related to file changes, including permissions, content.

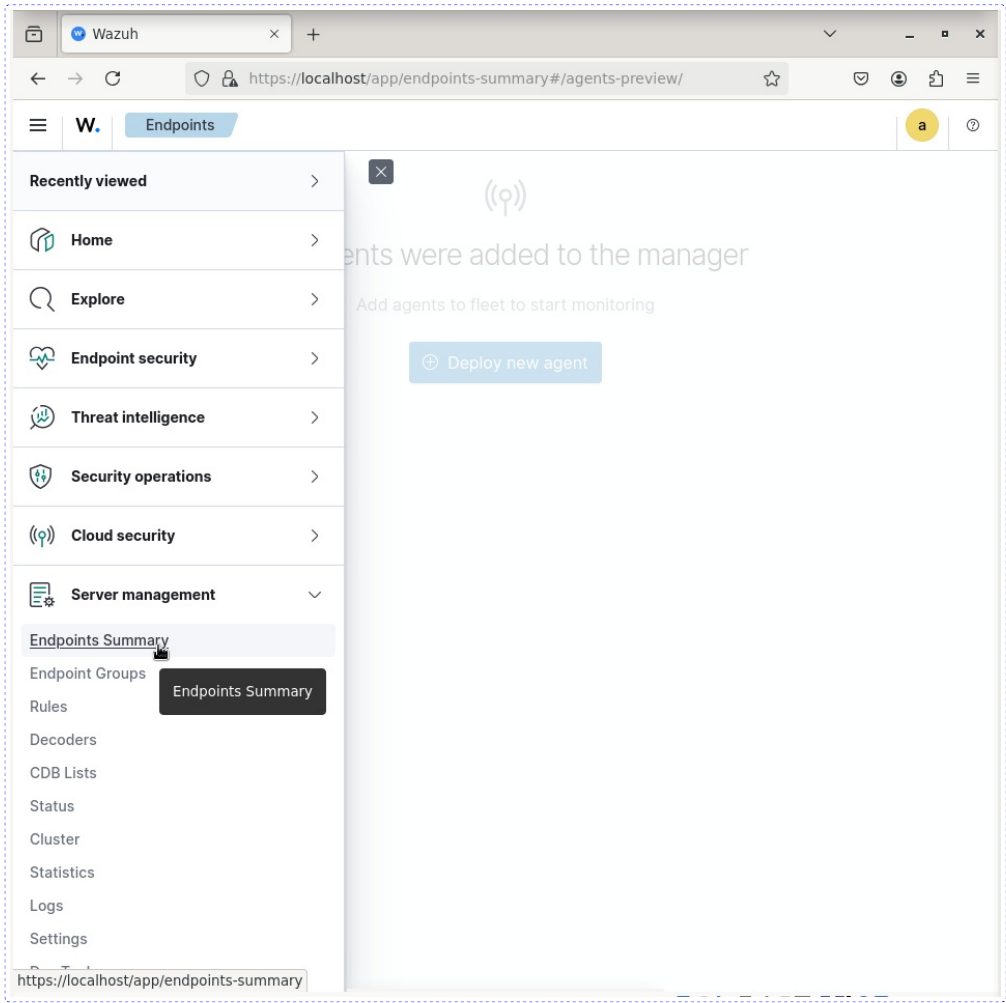
THREAT INTELLIGENCE

- Threat Hunting**
Browse through your security alerts, identifying issues and threats in your environment.
- Vulnerability Detection**
Discover what applications in your environment are affected by well-known vulnerabilities.
- MITRE ATT&CK**
Security events from the knowledge base of adversary.
- VirusTotal**
Alerts resulting from VirusTotal analysis of suspicious files via an

4. Engadir axentes

A. Debian GNU/Linux

1. Acceder a *Server management* → *Endpoints Summary*

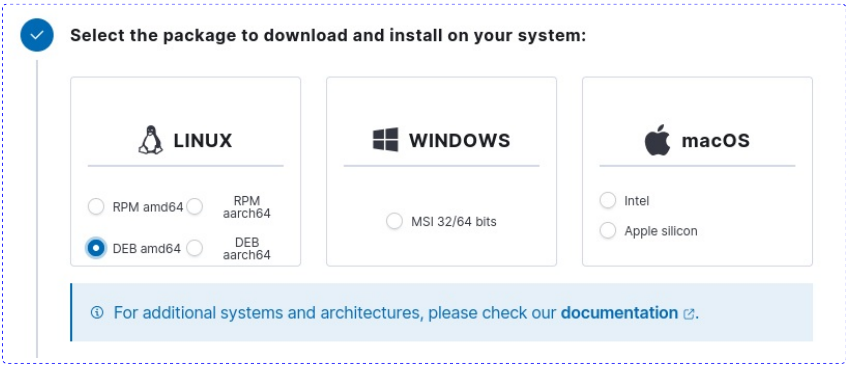


2. Acceder a Deploy new agent



3. Elixir:

- Sistema operativo e arquitectura: *LINUX* → *DEB amd64*



- Dirección IP/FQDN servidor wazuh: *wazuh-manager*

✓

Server address:

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

Assign a server address ⓘ

☐ ☒ Remember server address

- Asignar un nome e un grupo ao axente: *debian-axente1* → *default*

✓

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: ⓘ

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled. ⓘ

Select one or more existing groups: ⓘ

☒

- No apartado 4 (Instalar e engadir o axente) aparece un comando coas opcións escollidas. Este comando debe ser executado co usuario root no axente para engadilo como tal en wazuh:

✓

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_4.9.2-1_amd64.deb && sudo WAZUH_MANAGER='wazuh-manager' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='debian-axente1' dpkg -i ./wazuh-agent_4.9.2-1_amd64.deb
```

ⓘ 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.

- No apartado 5 aparecen os comandos necesarios, según o sistema Systemd, para recargar o servizo pertencente ao axente (wazuh-agent) e así poidamos ver no dashboard a este novo axente agregado.

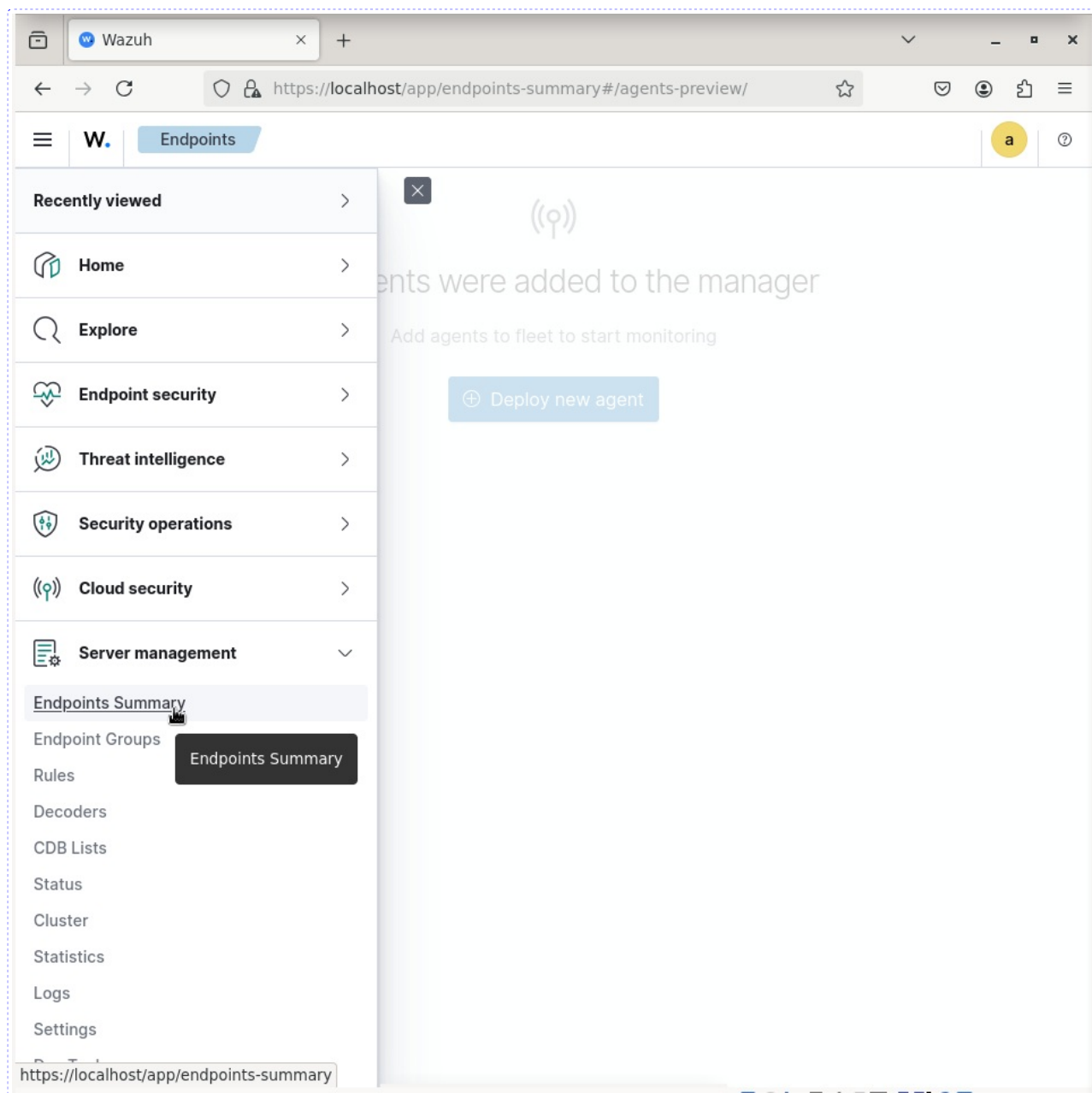
5

Start the agent:

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

B. Microsoft Windows

1. Acceder a *Server management* → *Endpoints Summary*

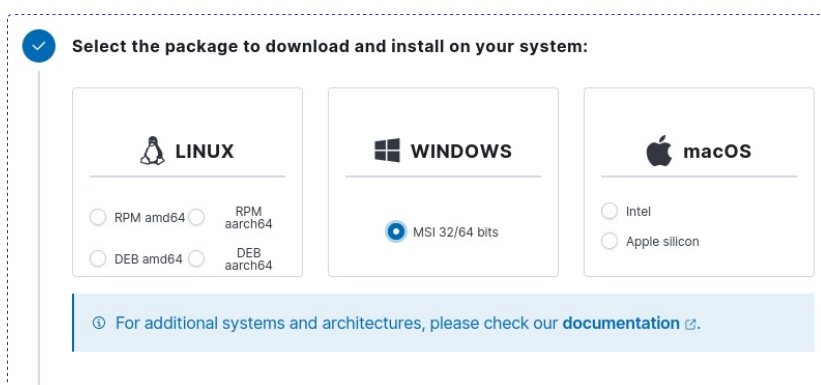


2. Acceder a *Deploy new agent*



3. Elixir:

- Sistema operativo: *Microsoft Windows*



- Dirección IP/FQDN servidor wazuh: 10.10.10.10

✓

Server address:

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

Assign a server address ⓘ

10.10.10.10|

☐ Remember server address

- Asignar un nome e un grupo ao axente: windows-axente1 → default

✓

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: ⓘ

windows-axente1

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

Select one or more existing groups: ⓘ

default × |

- No apartado 4 (Instalar e engadir o axente) aparece un comando coas opcións escollidas. Este comando debe ser executado co usuario administrador nunha consola de powershell no axente para engadilo como tal en wazuh:

4

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.2-1.msi -
OutFile $env:tmp\wazuh-agent; msixec.exe /i $env:tmp\wazuh-agent /q
WAZUH_MANAGER='10.10.10.10' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='windows-axente1'
```

ⓘ 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.

- No apartado 5 aparece o comando necesario para recargar o servizo pertencente ao axente (wazuh-agent) e así poidamos ver no dashboard a este novo axente agregado.

5

Start the agent:

```
NET START WazuhSvc
```


Máquinas virtuais axentes

5. Acceder ao axente Debian GNU/Linux: debianA

```
Executar nunha consola de comandos:
usuario@debianA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
usuario@debianA:~$ ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de redes: loopback(lo) e a correspondente á Rede NAT(enp0s3).
usuario@debianA:~$ ping -c4 10.10.10.10 #Comprobar mediante o comando ping a conectividade co servidor wazuh
root@debianA:~$ su - #Acceder á consola de root(administrador) a través comando su, o cal solicita o contrasinal do usuario root. Escribir o contrasinal de root para acceder.
root@debianA:~# echo '10.10.10.10 wazuh-manager' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome wazuh-manager,
para que atenda á IP 10.10.10.10
root@debianA:~# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.2-1_amd64.deb && sudo WAZUH_MANAGER='wazuh-
manager' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='debian-axente1' dpkg -i ./wazuh-agent_4.9.2-1_amd64.deb #Executar o comando do apartado 3.A.5
que nos ofrece wazuh para poder agregar este sistema operativo como axente de wazuh.
root@debianA:~# systemctl daemon-reload && systemctl enable wazuh-agent && systemctl start wazuh-agent Arrancar o servizo do axente para que poida ser visto no
dashboard de wazuh.
```

6. Acceder ao axente Microsoft Windows

```
Executar nun terminal:

> systeminfo #Amosar información de configuración detallada sobre o equipo e o seu sistema operativo.

> ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede.

> ping -c4 10.10.10.10 #Comprobar mediante o comando ping a conectividade co servidor wazuh
```

Executar en powershell con permisos de administrador:

```
> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.2-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-
agent /q WAZUH_MANAGER='10.10.10.10' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='windows-axente1' #Executar o comando do apartado 3.B.3 que nos
ofrece wazuh para poder agregar este sistema operativo como axente de wazuh.

> NET START WazuhSvc Arrancar o servizo do axente para que poida ser visto no dashboard de wazuh.
```

Dashboard: Máquina virtual Debian amd64

7. wazuh: Dashboard

A. Server Management → Endpoints Summary

Comprobar que os axentes engadidos aparecen no dashboard e que podemos acceder á súa monitorización:

Agents (2)

⊕ Deploy new agent

↻ Refresh

📄 Export formatted

More ▾

⚙️

Show only outdated

Search

WQL

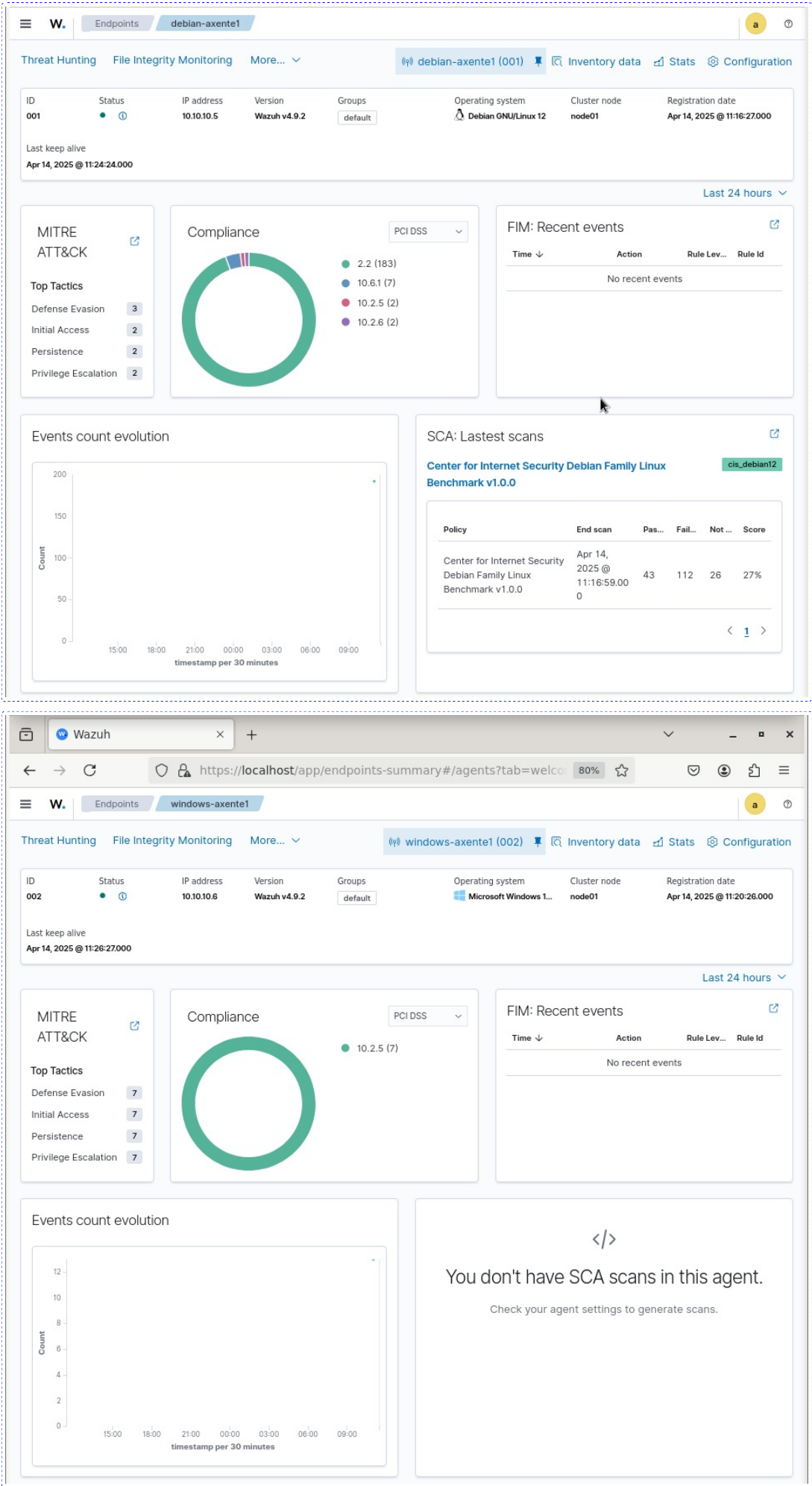
<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	debian-axente1	10.10.10.5	default	Debian GNU/Linux 12	node01	v4.9.2	● ⓘ 👁️ ⋮	
<input type="checkbox"/>	002	windows-axente1	10.10.10.6	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.2006	node01	v4.9.2	● ⓘ 👁️ ⋮	

Rows per page: 10 ▾

< 1 >

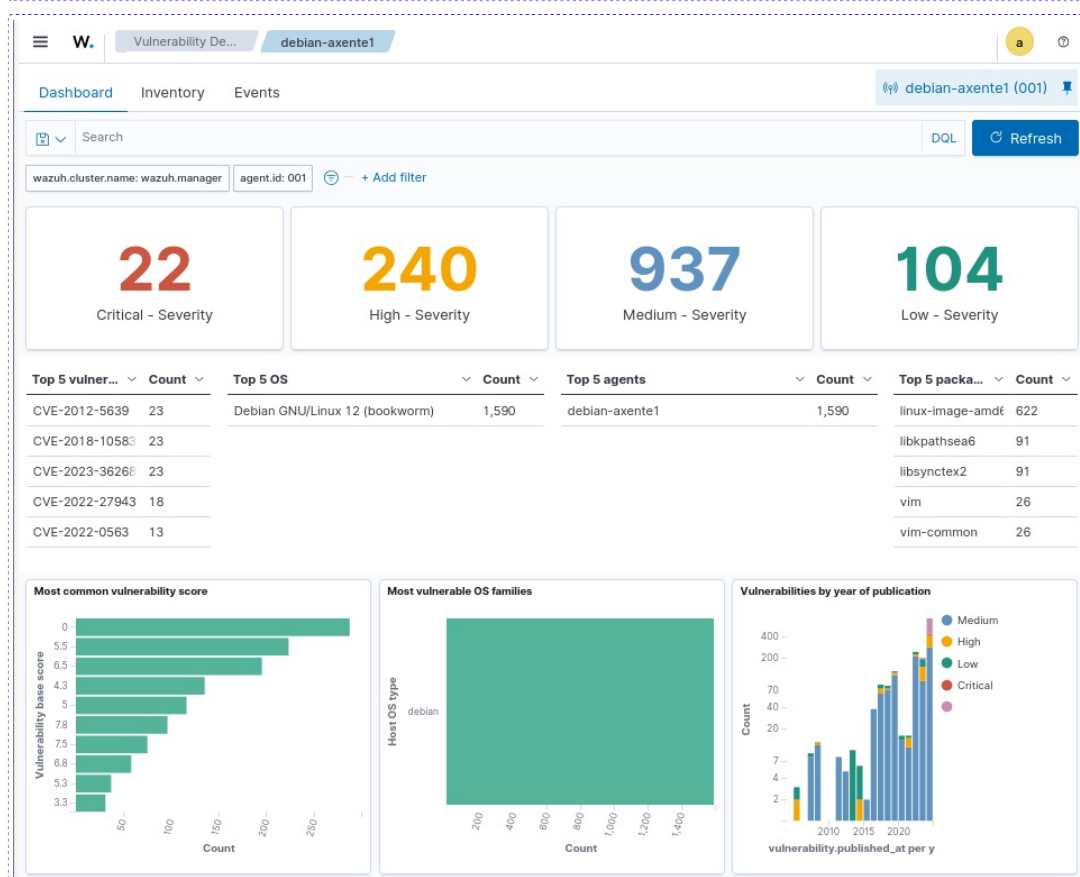
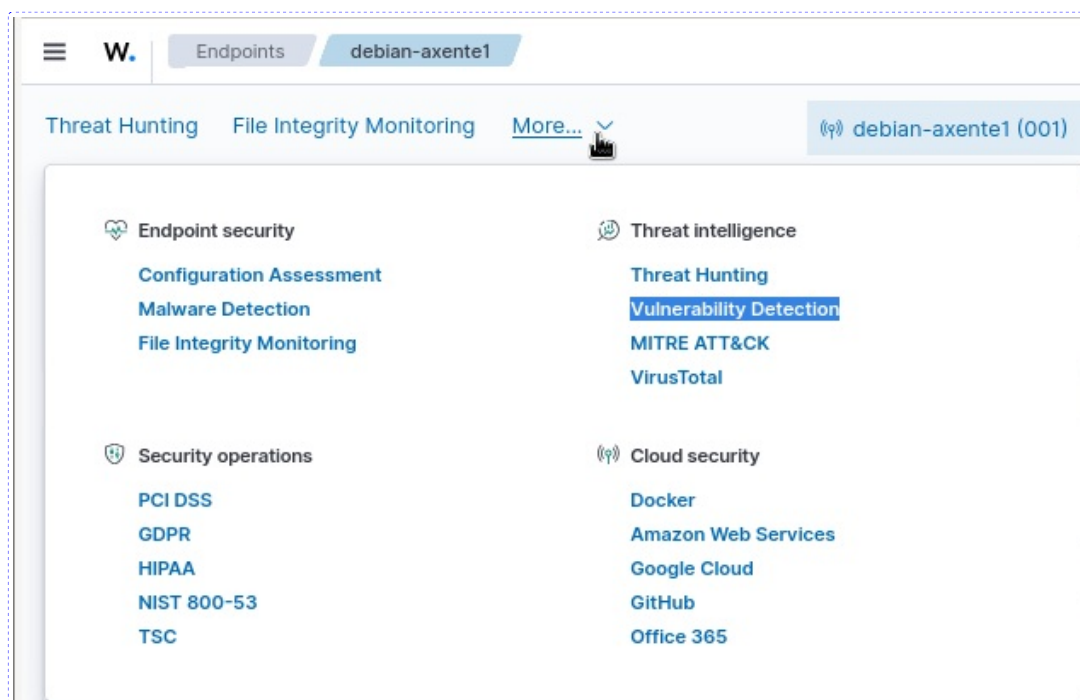
B. Panel de cada axente

Dende *Server Management* → *Endpoints Summary* ao premer en cada liña referente ao axente podemos acceder ao panel de cada axente:



```
root@debian:~# docker restart single-node_wazuh.manager_1
```

Agora podemos monitorizar os logs do contedor (usando `docker logs single-node_wazuh.manager_1`) e acceder no dashboard ao axente ao módulo **Vulnerability Detection**



E posible que o sistema operativo do axente non esté completamente actualizado. Así que accedemos a **debian-axente1** e actualizamos o sistema:

```
usuario@debian-axente1:~$ su -
```

```
root@debian-axente1:~# apt update && apt -y upgrade
```

Unha vez actualizado comprobamos de novo as vulnerabilidades existentes no sistema a través do módulo **Vulnerability Detection**

Accedemos á lapela **Inventory** para visualizar todas as vulnerabilidades. Unha vez dentro deste panel do dashboard podemos visualizar información sobre as vulnerabilidades premendo na icona lupa de cada liña.

The screenshot shows the Wazuh Inventory page for agent 'debian-axente1'. The interface includes a search bar, filters for 'wazuh.cluster.name: wazuh.manager' and 'agent.id: 001', and a 'Refresh' button. A table displays 1,590 hits with columns for agent, package, vulnerability details, and agent information. A tooltip 'Inspect vulnerability details' points to the magnifying glass icon in the first row of the table.

agent.n...	package...	package...	vul...	vulnera...	vulnera...	_index	agent.b...	agent.e...	agent.id	agent.ty...	age
debian-axen...	cups	2.4.2-3+de...	The browsi...	Medium	CVE-2014-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libglapi-me...	22.3.6-1+d...	Mesa 23.0...	High	CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libglapi-me...	22.3.6-1+d...	glx_pbuffer...		CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libglapi-me...	22.3.6-1+d...	Mesa v23...		CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libglapi-me...	22.3.6-1+d...	Mesa 23.0...	Medium	CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	mesa-vdpa...	22.3.6-1+d...	Mesa 23.0...	High	CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	mesa-vdpa...	22.3.6-1+d...	glx_pbuffer...		CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	mesa-vdpa...	22.3.6-1+d...	Mesa v23...		CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	mesa-vdpa...	22.3.6-1+d...	Mesa 23.0...	Medium	CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libthunarx...	4.18.4-1	Xfce Thuna...	Low	CVE-2018-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libreoffice...	4:7.4.7-1+...	An issue in ...	Medium	CVE-2023-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libreoffice...	4:7.4.7-1+...	LibreOffice...	Medium	CVE-2012-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libreoffice...	4:7.4.7-1+...	An informa...	Medium	CVE-2018-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	libcurl4	7.88.1-10+...	libcurl skip...		CVE-2024-...	wazuh-stat...			001	wazuh	v4.5
debian-axen...	cups-ipp-u...	2.4.2-3+de...	The browsi...	Medium	CVE-2014-...	wazuh-stat...			001	wazuh	v4.5

Tamén podemos xerar filtros de búsqueda para amosar vulnerabilidades, premendo **Add filter** e escollendo os criterios de búsqueda:

The screenshot shows the Wazuh Inventory page with the 'EDIT FILTER' dialog box open. The dialog allows creating a filter based on the field 'vulnerability.severity' using the operator 'is' and the value 'High'. There are options to 'Cancel' or 'Save' the filter, and a checkbox for 'Create custom label?'. The background table shows the same list of vulnerabilities as the previous screenshot.

Accedendo a información dunha vulnerabilidade podemos atopar documentación sobre esta.

Vulnerability details

Table

JSON

<div>f</div> <div>_index</div>	wazuh-states-vulnerabilities-wazuh.manager
<div>f</div> <div>agent.id</div>	001
<div>f</div> <div>agent.name</div>	debian-axente1
<div>f</div> <div>agent.type</div>	wazuh
<div>f</div> <div>agent.version</div>	v4.9.2
<div>f</div> <div>host.os.full</div>	Debian GNU/Linux 12 (bookworm)
<div>f</div> <div>host.os.kernel</div>	6.1.0-32-amd64
<div>f</div> <div>host.os.name</div>	Debian GNU/Linux
<div>f</div> <div>host.os.platform</div>	debian
<div>f</div> <div>host.os.type</div>	debian
<div>f</div> <div>host.os.version</div>	12
<div>f</div> <div>package.architecture</div>	amd64
<div>f</div> <div>package.description</div>	free implementation of the GL API -- shared library
<div>f</div> <div>package.name</div>	libglapi-mesa
<div>#</div> <div>package.size</div>	268
<div>f</div> <div>package.type</div>	deb
<div>f</div> <div>package.version</div>	22.3.6-1+deb12u1
<div>f</div> <div>vulnerability.category</div>	Packages
<div>f</div> <div>vulnerability.classification</div>	CVSS
<div>f</div> <div>vulnerability.description</div>	Mesa 23.0.4 was discovered to contain a NULL pointer dereference in check_xshm() for the has_error state. NOTE: this is disputed because there is no scenario in which the vulnerability was demonstrated.
<div>📅</div> <div>vulnerability.detected_at</div>	Apr 14, 2025 @ 17:17:57.059
<div>f</div> <div>vulnerability.enumeration</div>	CVE
<div>f</div> <div>vulnerability.id</div>	CVE-2023-45931
<div>📅</div> <div>vulnerability.published_at</div>	Mar 27, 2024 @ 05:15:11.000
<div>f</div> <div>vulnerability.reference</div>	https://gitlab.freedesktop.org/mesa/mesa/-/issues/9859 , https://seclists.org/fulldisclosure/2024/Jan/71
<div>f</div> <div>vulnerability.scanner.vendor</div>	Wazuh
<div>#</div> <div>vulnerability.score.base</div>	7.5
<div>f</div> <div>vulnerability.score.version</div>	3.1

E. SCA (Security Configuration Assessment)

O módulo *SCA (Security Configuration Assessment)* de Wazuh analiza a configuración de seguridade do sistema operativo e detecta desviacións respecto a estándares ou boas prácticas. A sección "Latest scans" mostra os resultados máis recentes destas análises, incluíndo regras superadas ou falladas.

No caso concreto de: **Center for Internet Security Debian Family Linux Benchmark v1.0.0** significa que o SCA está a aplicar as políticas de seguridade definidas polo **CIS Benchmark para sistemas Debian**, avaliando cousas como permisos de ficheiros, configuración de SSH, usuarios, auditoría, etc., para determinar se o sistema cumpre cos requisitos recomendados por este estándar de seguridade recoñecido internacionalmente.

SCA: Lastest scans

Center for Internet Security Debian Family Linux Benchmark v1.0.0

cis_debian12

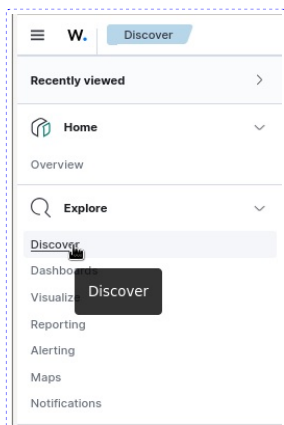
Policy	End scan	Pas...	Fail...	Not ...	Score
Center for Internet Security Debian Family Linux Benchmark v1.0.0	Apr 14, 2025 @ 11:16:59.000	43	112	26	27%

< 1 >

F. Discover

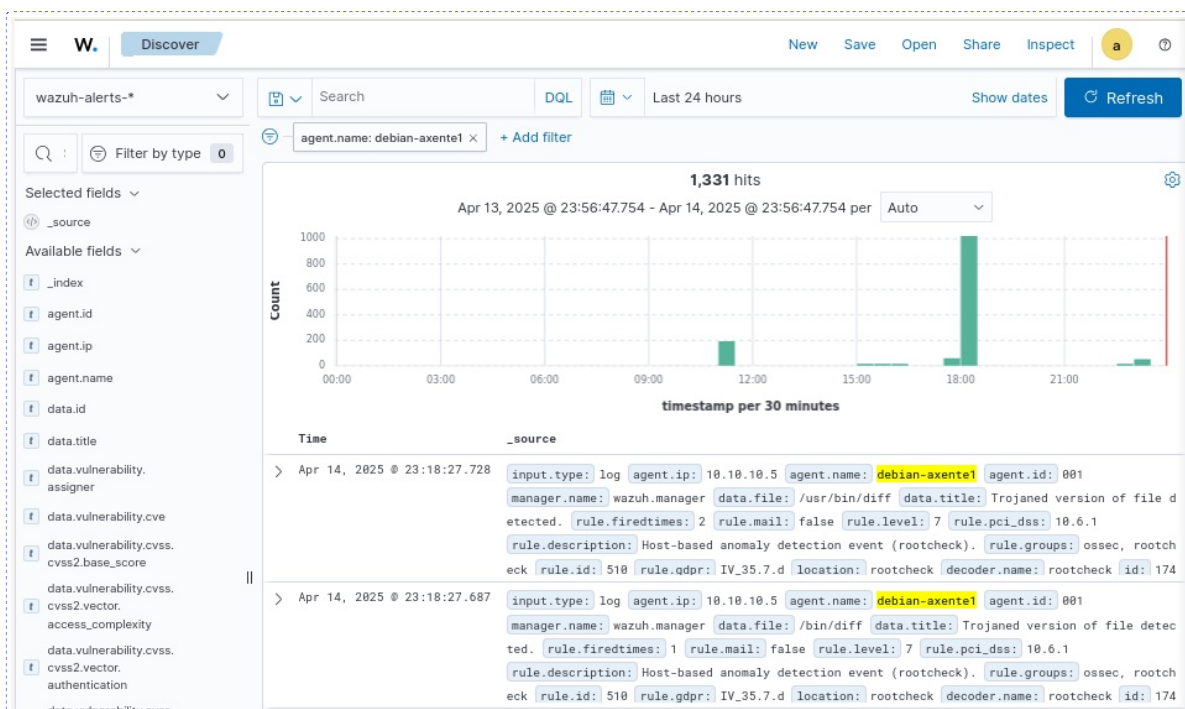
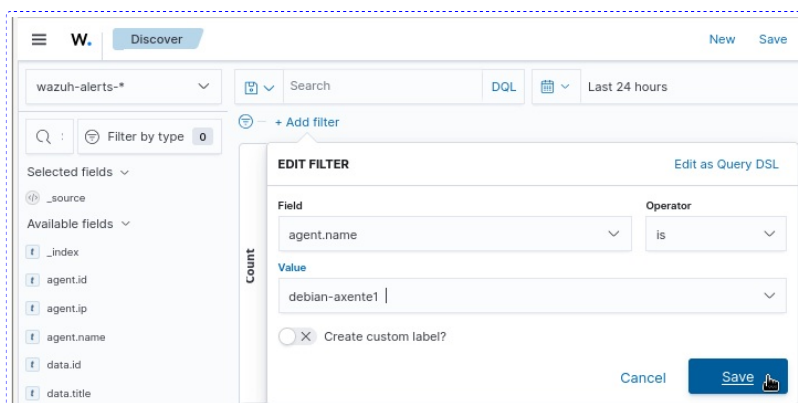
Wazuh 4.9.2 mostra os eventos de seguridade a través da vista de *Discover*. Estes eventos, detectados polos axentes ou polos módulos do manager, inclúen alertas de intrusión, cambios sospeitosos en ficheiros, execucións de procesos non autorizados, vulnerabilidades atopadas, detección de rootkits, entre outros. Baseándose nas regras do motor de análise de Wazuh, preséntanse con distintos niveis de severidade, o que permite ao administrador identificar, investigar e responder rapidamente ante posibles ameazas ou actividades anómalas na infraestrutura monitorizada.

Acceder ao dashboard, no menú lateral: *Explore* → *Discover*



Asegurarse que no buscador da parte superior, está seleccionado o índice: *wazuh-alerts-**. Pódese filtrar na parte de abaixo por: *Axente*, *Severidade* (*rule.level*), *Nome da regra* (*rule.description*), *ID de alerta*, etc. Así, por exemplo podemos filtrar para ver soamente eventos dun axente específico:

agent.name: "debian-axente1"



Exemplo: Ver eventos de SSH fallido

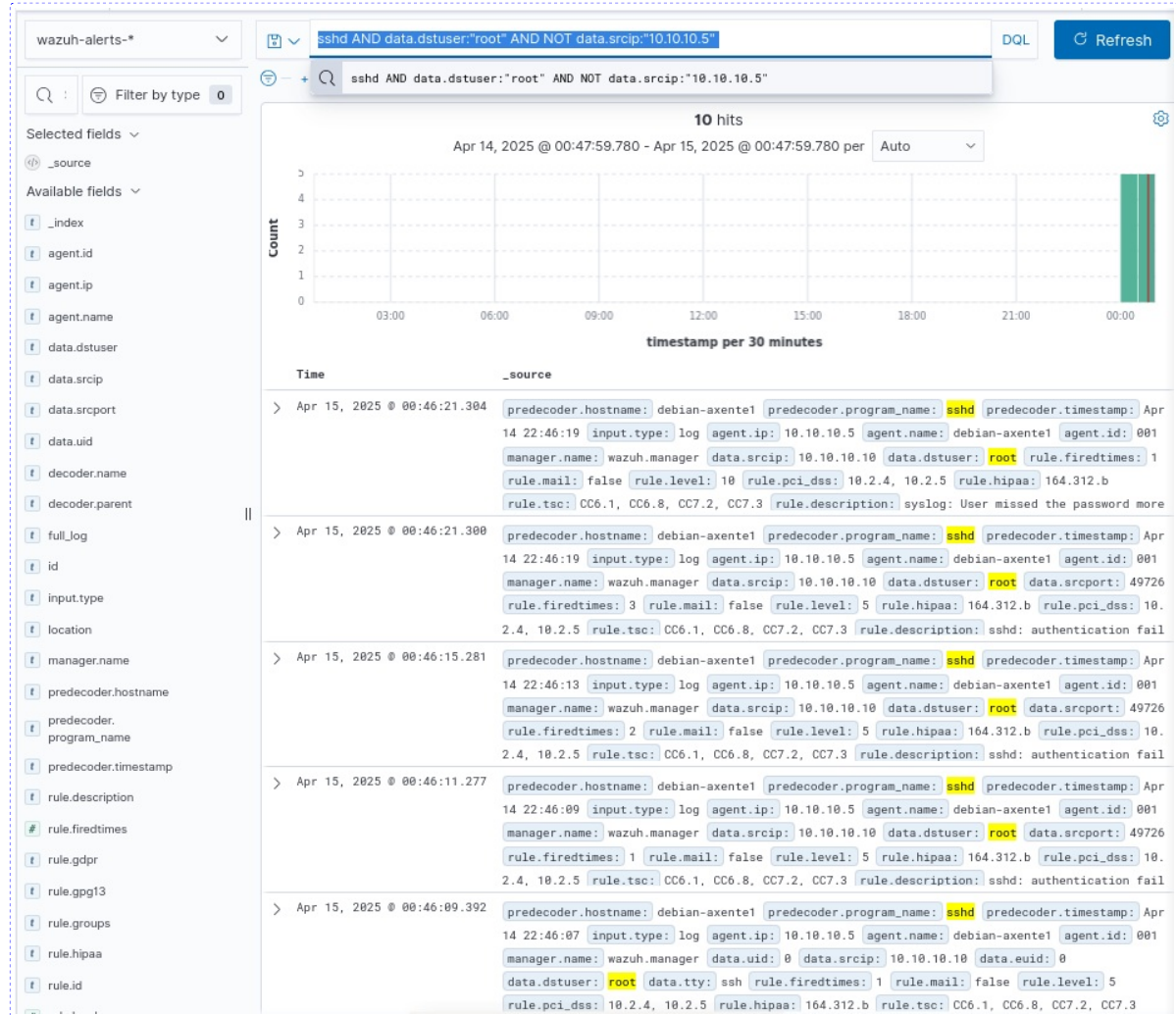
1. Acceder ao Dashboard: <https://localhost>
2. Ir ao menú lateral e acceder a *Explore* → *Discover*
3. Na barra de busca usar o seguinte filtro:

```
sshd AND data.dstuser:"root" AND NOT data.srcip:"10.10.10.5"
```

Explicación:

- sshd → eventos relacionados co servizo SSH.
- data.dstuser:"root" → intentos dirixidos ao usuario root
- AND NOT data.srcip:"10.10.10.5" → exclúe os eventos da IP 10.10.10.5

Este filtro mostra intentos de acceso a root por SSH desde calquera IP agás 10.10.10.5.



Exemplo: Regras de SSH fallido

A. Wazuh xa inclúe regras por defecto para SSH fallido.

A organización das regras evolucionou. Wazuh utiliza agora ficheiros con prefixos numéricos para establecer unha orde de carga e agrupación. As regras específicas para SSHD atópanse normalmente no ficheiro:

`/var/ossec/ruleset/rules/0095-sshd_rules.xml`

Este ficheiro contén as regras predeterminadas para analizar os eventos do daemon SSH (sshd), incluíndo:

- Intentos de inicio de sesión correctos.
- Intentos de inicio de sesión errados (contrasinal incorrecto, usuario inválido). (Regras como 5710, 5712, 5716, 5720 son comúns para isto).
- Erros de conexión.
- Cambios na configuración de SSH.
- Ataques de forza bruta (detectados mediante a correlación de múltiples fallos). (Regras como 5760, 5761).

Como verificalo no teu contedor:

Podes listar os ficheiros nesa carpeta ou buscar directamente o ficheiro:

1. Entra no contedor (se non estás dentro)

```
# docker exec -it single-node_wazuh.manager_1 bash
```

2. Dentro do contedor:

```
bash-5.2# find / -type f -iname "*sshd*rules*.xml" 2>/dev/null | (ls -l /var/ossec/ruleset/rules/ | grep sshd)
```

3. Exemplo de regra: `<rule id="5760" level="5"> <if_sid>5700,5716</if_sid> <match>Failed password|Failed keyboard|authentication error</match> <description>sshd: authentication failed.</description> <mitre> <id>T1110.001</id> <id>T1021.004</id> </mitre> <group>authentication_failed,gdpr_IV_35.7.d,gdpr_IV_32.2,pgp13_7.1,hipaa_164.312.b, nist_800_53_AU.14,nist_800_53_AC.7,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8, tsc_CC7.2,tsc_CC7.3,</group> </rule>`

B. Axente

Executar nunha consola de root no axente *debian-axente1*:

```
# NUM=$(grep -n '</ossec_config>' /var/ossec/etc/ossec.conf | head -1 | cut -d ':' -f1)
# sed -i "${NUM}d" /var/ossec/etc/ossec.conf
# NUM=$(grep -n '</ossec_config>' /var/ossec/etc/ossec.conf | tail -1 | cut -d ':' -f1)
# sed -i "${NUM}d" /var/ossec/etc/ossec.conf
# systemctl restart wazuh-agent.service
# systemctl status wazuh-agent.service --no-pager
```

C. Provocar o fallo de autenticación por SSH

Na máquina virtual Wazuh executar nunha consola:

`$ ssh root@10.10.10.5 #Acceder co usuario root mediante SSH ao axente debian-axente1 e provocar o fallo de autenticación SSH (por exemplo introducindo mal o contrasinal, aínda que o usuario root non ten permitido o acceso remoto por SSH no ficheiro de configuración /etc/ssh/sshd_config do axente: directiva PermitRootLogin) root@10.10.10.5's password:`

Permission denied, please try again.

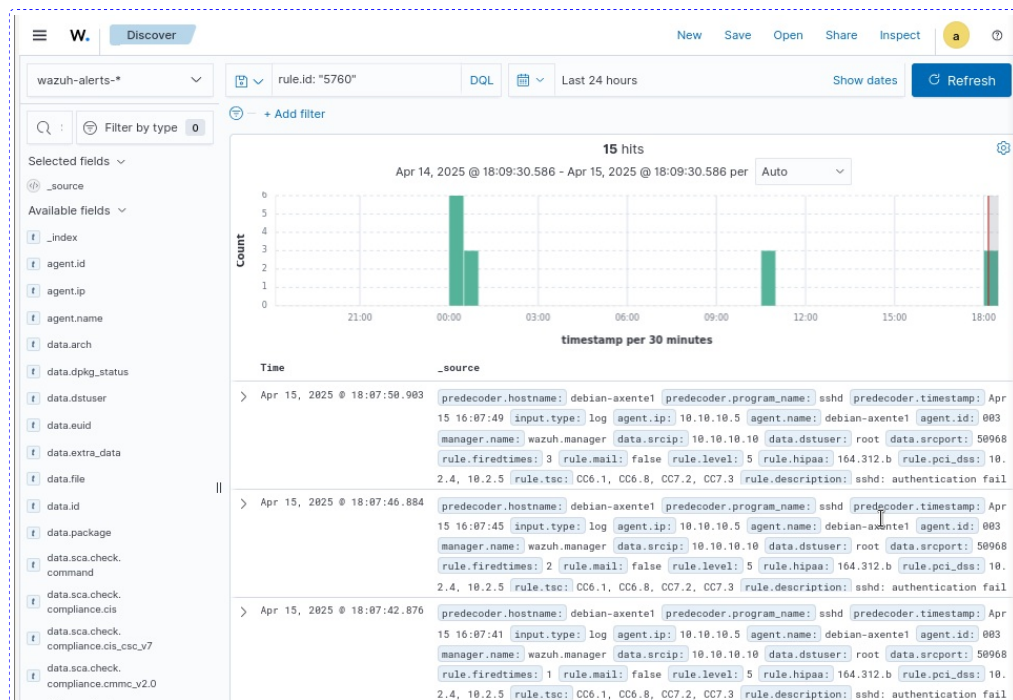
root@10.10.10.5's password:

Permission denied, please try again.

root@10.10.10.5's password:

root@10.10.10.5: Permission denied (publickey,password).

Verificar o filtro para a regra 5760 de SSH no Dashboard:



W. Discover

Apr 15, 2025 9 18:07:50.983

wazuh-alerts-*

Search

Filter by type 0

Selected fields

Available fields

predecoder.hostname: debian-axe1

predecoder.program_name: sshd

predecoder.timestamp: Apr 15 16:07:49

input.type: log

agent.id: 10.10.10.5

agent.name: debian-axe1

agent.id: 003

manager.name: wazuh.manager

data.scrip: 10.10.10.5

data.dstuser: root

data.srport: 50908

rule.firedtimes: 3

rule.mail: false

rule.level: 5

rule.hipsa: 104.3

rule.pci_dss: 10.2.4, 10.2.5

rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3

rule.description: sshd: authentication failed

rule.groups: syslog, sshd, authentication_failed

rule.id: 5768

rule.mist_800_53: AU.14, AC.7

rule.gdpr: IV_35.7.d

Expanded document

Table

JSON

f	_index	wazuh-alerts-4.x-2025.04.15
f	agent.id	003
f	agent.ip	10.10.10.5
f	agent.name	debian-axe1
f	data.dstuser	root
f	data.scrip	10.10.10.10
f	data.srport	50908
f	decoder.name	sshd
f	decoder.parent	sshd
f	full_log	Apr 15 16:07:49 debian-axe1 sshd[11244]: Failed password for root from 10.10.10.10 port 50908 ssh2
f	id	1744732270.724142
f	input.type	log
f	location	JournalId
f	manager.name	wazuh.manager
f	predecoder.hostname	debian-axe1
f	predecoder.program_name	sshd
f	predecoder.timestamp	Apr 15 16:07:49
f	rule.description	sshd: authentication failed.
#	rule.firedtimes	3
f	rule.gdpr	IV_35.7.d, IV_32.2
f	rule.gpg13	7.1
f	rule.groups	syslog, sshd, authentication_failed
f	rule.hipsa	104.312.b
f	rule.id	5768
#	rule.level	5
🔍	rule.mail	false
f	rule.mist_800_53	AU.14, AC.7
f	rule.pci_dss	10.2.4, 10.2.5

Exemplo: Activar resposta activa (IPS)

Imos configurar Wazuh para que executa automaticamente un script no axente *debian-axente1* ao detectar un posible ataque de Forza Bruta SSH (Regra 5760)

A. Configuración no Xestor (Manager) Wazuh

1. Editar o ficheiro de configuración principal do xestor:

O ficheiro `/root/wazuh-docker/single-node/config/wazuh_cluster/wazuh_manager.conf` é o que se carga dentro do contedor `docker single-node_wazuh.manager_1` en `/var/ossec/etc/ossec.conf`

```
# cd /root/wazuh-docker/single-node/config/wazuh_cluster/
# NUM=$(grep -n '<ossec_config>' wazuh_manager.conf | head -1 | cut -d ':' -f1)
# sed -i "${NUM}d" wazuh_manager.conf
# NUM=$(grep -n '<ossec_config>' wazuh_manager.conf | tail -1 | cut -d ':' -f1)
# sed -i "${NUM}d" wazuh_manager.conf
```

2. Engadir/Modificar o bloque `<active-response>`:

Sustitúe o comentario:

```
<!-- <active-response> active-response options here </active-response> -->
```

por:

```
<!-- ### RESPUESTA ACTIVA PARA BLOQUEO SSH ### -->
<active-response>
  <disabled>no</disabled>                                <!-- Activa esta resposta específica -->
  <command>script-ips.sh</command>                        <!-- Nome do script a enviar -->
  <location>local</location>                              <!-- Executar no axente que enviou o log -->
  <rules_id>5760</rules_id>                               <!-- ID da regra que dispara a resposta -->
  <timeout>600</timeout>                                  <!-- Tempo en segundos que durará o bloqueo (10 min) -->
</active-response>
```

- `no`: Habilita esta resposta.
- `script-ips.sh`: Nome do script a enviar.
- `local`: Executa no axente que orixinou o evento.
- `5760`: Actívase só coa regra 5760.
- `600`: Duración do bloqueo en segundos.

3. Verificar que o comando `script-ips.sh` está definido. Busca un bloque coma este dentro de `<ossec_config>`:

```
<command>
  <name>script-ips.sh</name>
  <executable>script-ips.sh</executable> <!-- Nome do script esperado no axente -->
  <timeout_allowed>yes</timeout_allowed> <!-- Indica que acepta timeout -->
</command>
```

Se non existe, engádeo.

4. Gardar o ficheiro

5. Reiniciar o Xestor Wazuh para aplicar os cambios:

```
bash-5.2# exit
# docker restart single-node_wazuh.manager_1
```

B. Configuración no Axente (*debian-axente1*)

O axente necesita ter a Resposta Activa habilitada e saber que script executar.

1. Verificar o ficheiro de configuración do axente: `/var/ossec/etc/ossec.conf`

Asegúrate de que a Resposta Activa estea habilitada globalmente. Busca o bloque `<active-response>` e verifica o valor `no` en `<disabled>`:

```
<active-response>
  <disabled>no</disabled>
  <!-- ... outras opcións ... -->
</active-response>
```

2. Verifica que o comando `script-ips.sh` está definido no axente. Busca un bloque `<command>` dentro de `<ossec_config>` con exactamente este contido (seguramente débese eliminar a liña relativa a *expect*):

```
<command>
  <name>script-ips.sh</name>                                <!-- Nome lóxico que chega do xestor -->
  <executable>script-ips.sh</executable> <!-- Script REAL que se executa no axente -->
  <timeout_allowed>yes</timeout_allowed> <!-- Debe ser 'yes' se o xestor envía timeout -->
</command>
```

Se non existe, engádeo. **Se é necesario gardar o ficheiro**

Un lugar lóxico para engadir bloques é despois da sección `<client_buffer>` e antes de seccións como `<rootcheck>` ou `<wodle>`. Non ten que ser estritamente aí, pero é un lugar común. O importante é que estea dentro do único bloque `<ossec_config>` válido.

C. Verificar o Script no Axente

1. Xerar o script `/var/ossec/active-response/bin/script-ips.sh`:

```
#!/bin/bash

read input
echo "$(date) - Script firewall-drop executado" >> /var/ossec/logs/active-responses.log
echo "$input" >> /var/ossec/logs/active-responses.log

# Extraer comando e IP
CMD=$(echo "$input" | grep -oP '"command"\s*:\s*\K[^\"]+')
IP=$(echo "$input" | grep -oP '"srcip"\s*:\s*\K[0-9.]+')

TABLE="inet"
CHAIN="filter"
CHAIN_INPUT="input"

if [ "$CMD" = "add" ]; then
    # Só engade se non existe
    nft list chain $TABLE $CHAIN $CHAIN_INPUT | grep -q "ip saddr $IP drop"
    if [ $? -ne 0 ]; then
        nft add rule $TABLE $CHAIN $CHAIN_INPUT ip saddr $IP drop
        echo "$(date) - IP bloqueada: $IP" >> /var/ossec/logs/active-responses.log

        # Eliminar a regra automaticamente despois de 600 segundos
        (
            sleep 600
            HANDLE=$(nft --handle list chain $TABLE $CHAIN $CHAIN_INPUT | grep "ip saddr $IP drop" | awk '{print $NF}')
            if [ -n "$HANDLE" ]; then
                nft delete rule $TABLE $CHAIN $CHAIN_INPUT handle $HANDLE
                echo "$(date) - IP desbloqueada AUTO: $IP (handle $HANDLE)" >> /var/ossec/logs/active-responses.log
            fi
        ) &
    fi
fi

elif [ "$CMD" = "delete" ]; then
    # Elimina regra asociada á IP se chega comando desde Wazuh Manager
    HANDLE=$(nft --handle list chain $TABLE $CHAIN $CHAIN_INPUT | grep "ip saddr $IP drop" | awk '{print $NF}')
    if [ -n "$HANDLE" ]; then
        nft delete rule $TABLE $CHAIN $CHAIN_INPUT handle $HANDLE
        echo "$(date) - IP desbloqueada MANUAL: $IP (handle $HANDLE)" >> /var/ossec/logs/active-responses.log
    fi
fi
```

2. Modificar os permisos:

```
# chmod 750 /var/ossec/active-response/bin/script-ips.sh
# chown root:wazuh /var/ossec/active-response/bin/script-ips.sh
```

D. Reiniciar o Axente Wazuh

Aplicar os cambios no axente:

```
# systemctl restart wazuh-agent
# systemctl status wazuh-agent --no-pager
```

E. Probar e Verificar

1. Activar o Firewall no Axente (Debian 12 usa nftables):

```
# nft list table inet filter; [ $? -ne 0 ] && systemctl enable nftables --now
# systemctl status nftables.service --no-pager
# nft list tables
```

2. Simula un ataque de forza bruta: Desde unha IP de proba, realiza varios intentos de login SSH errados contra debian-axente1

3. Monitoriza os Logs no axente:

- Revisa `/var/ossec/logs/active-responses.log`. Deberías ver a execución de `script-ips.sh` coa acción `add` e a IP atacante.

```
root@debian-axente1:~# tail -f -n2 /var/ossec/logs/active-responses.log
mar 15 abr 2025 23:03:13 CEST - IP bloqueada por script-ips.sh: 10.10.10.10
mar 15 abr 2025 23:03:13 CEST - IP bloqueada por script-ips.sh: 10.10.10.10
```

4. **Verifica o Firewall no Axente (Debian 12 usa nftables):** Busca unha regra que bloquee ('drop') a IP atacante na táboa filter, cadea input

```
root@debian-axente1:/var/ossec/active-response/bin# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority filter; policy accept;
        ip saddr 10.10.10.10 drop
    }

    chain forward {
        type filter hook forward priority filter; policy accept;
    }

    chain output {
        type filter hook output priority filter; policy accept;
    }
}
```

5. **Comproba o Bloqueo:** Intenta conectar por SSH desde a IP atacante; debería fallar.

```
usuario@computer:~$ nc -vz 10.10.10.5 22
10.10.10.5: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.5] 22 (ssh) : Connection timed out
usuario@computer:~$ ssh root@10.10.10.5
ssh: connect to host 10.10.10.5 port 22: Connection timed out
```

6. **Verifica o Desbloqueo Automático:**

- Agarda a que pase o tempo do timeout (10 minutos no exemplo).
- **No axente:**
 1. Revisa de novo `nft list ruleset`. A regra de bloqueo debería desaparecer.

```
root@debian-axente1:~# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority filter; policy accept;
    }

    chain forward {
        type filter hook forward priority filter; policy accept;
    }

    chain output {
        type filter hook output priority filter; policy accept;
    }
}
```

2. Comproba `/var/ossec/logs/active-responses.log` no axente para ver a acción delete.

```
root@debian-axente1:~# tail -f -n2 /var/ossec/logs/active-responses.log
mié 16 abr 2025 00:28:09 CEST - IP bloqueada: 10.10.10.10
mié 16 abr 2025 00:38:09 CEST - IP desbloqueada AUTO: 10.10.10.10 (handle 11)
```

Aviso Importante!

Ten coidado ao probar isto. Asegúrate de non bloquear accidentalmente unha IP que necesites para acceder ao sistema (como a túa propia IP de administración). Usa unha IP de proba específica para simular o ataque.