Instalación Wazuh Open Source security

Introducción.

Wazuh es una plataforma de seguridad gratuita y de código abierto que unifica las capacidades XDR y SIEM. Protege cargas de trabajo en entornos locales, virtualizados, en contenedores y basados en la nube.

Wazuh ayuda a organizaciones e individuos a proteger sus activos de datos contra amenazas a la seguridad. Es ampliamente utilizado por miles de organizaciones en todo el mundo, desde pequeñas empresas hasta grandes empresas.

Antes de realizar la instalación del Manager de Wazuh y los agentes se debe verificar que la lista de repositorios este actualizada ya que influye en los siguientes aspectos:

Seguridad:

- Corrección de vulnerabilidades: Los repositorios se actualizan constantemente para corregir vulnerabilidades de seguridad. Si no se actualiza, su sistema estará vulnerable a ataques.
- Software desactualizado: El software desactualizado puede tener vulnerabilidades de seguridad sin parches.

Estabilidad y rendimiento:

- Corrección de errores: Las actualizaciones de software corrigen errores que pueden causar inestabilidad o problemas de rendimiento.
- Mejoras de rendimiento: Las actualizaciones de software pueden mejorar el rendimiento general del sistema.

Nuevos paquetes y versiones:

- Acceso a nuevas funciones: Las actualizaciones de software agregan nuevas funciones y mejoras.
- Compatibilidad con hardware nuevo: Las actualizaciones de software pueden agregar compatibilidad con hardware nuevo.

Instalación de Wazuh.

La solución Wazuh se compone de tres componentes de plataforma central y un único agente universal. Para instalar Wazuh en tu infraestructura el inicio rápido es una forma automatizada de instalar Wazuh en tan solo unos minutos, es recomendable realizarlo desde la documentación oficial de Wazuh:

- https://documentation.wazuh.com/current/quickstart.html

Requisitos.

Hardware.

Los requisitos de hardware dependen en gran medida de la cantidad de puntos finales protegidos y cargas de trabajo en la nube. Este número puede ayudar a estimar cuántos datos se analizarán y cuántas alertas de seguridad se almacenarán e indexarán.

La siguiente tabla muestra el hardware recomendado para una implementación:

Agentes	UPC	RAM	Almacenamiento (90 días)
1–25	4 CPU virtuales	8GB	50GB
25–50	8 CPU virtuales	8GB	100GB
50-100	8 CPU virtuales	8GB	200GB

Compatibilidad del navegador.

Se admiten los siguientes navegadores web:

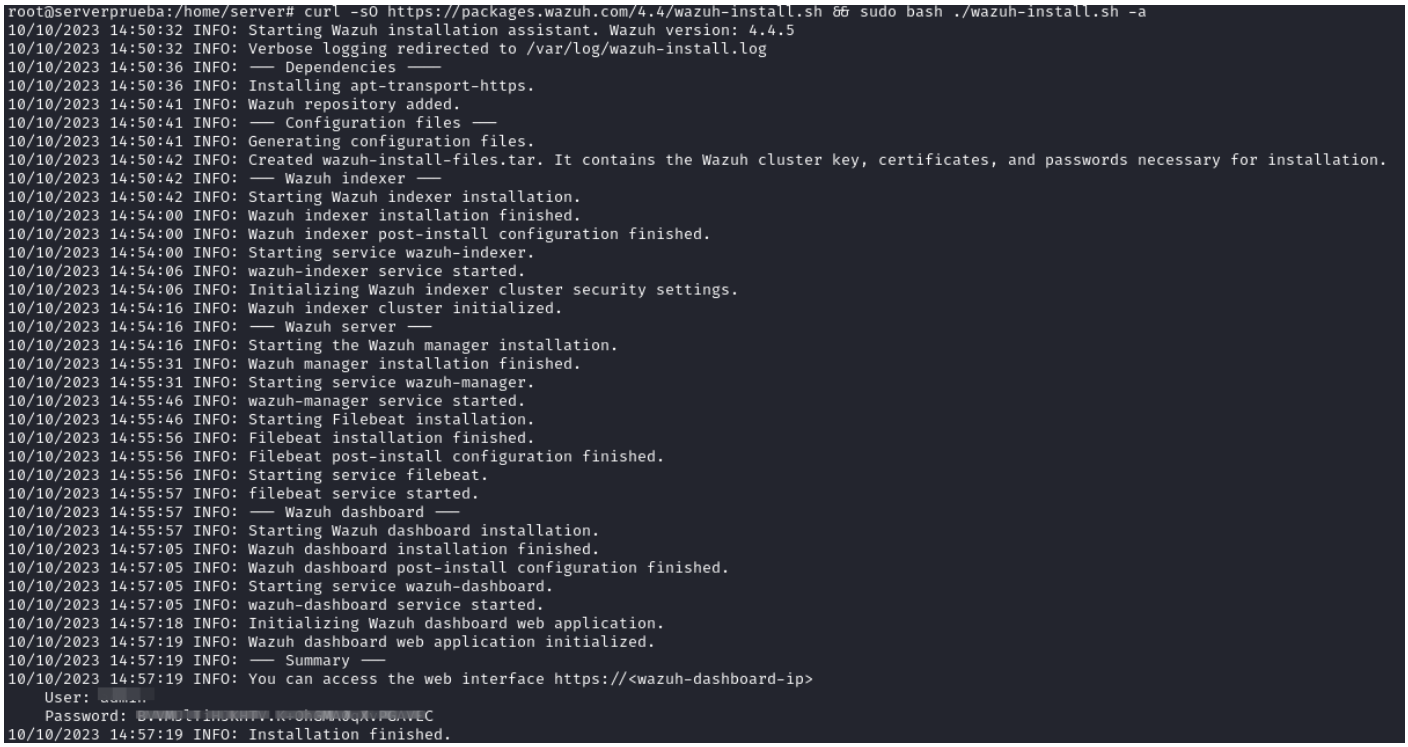
- Chrome 95 o posterior
- Firefox 93 o posterior
- Safari 13.7 o posterior

Es posible La funcionalidad en navegadores basados en Chromium.

Instalación rápida Wazuh Manager.

Ejecución del asistente de instalación de Wazuh.

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



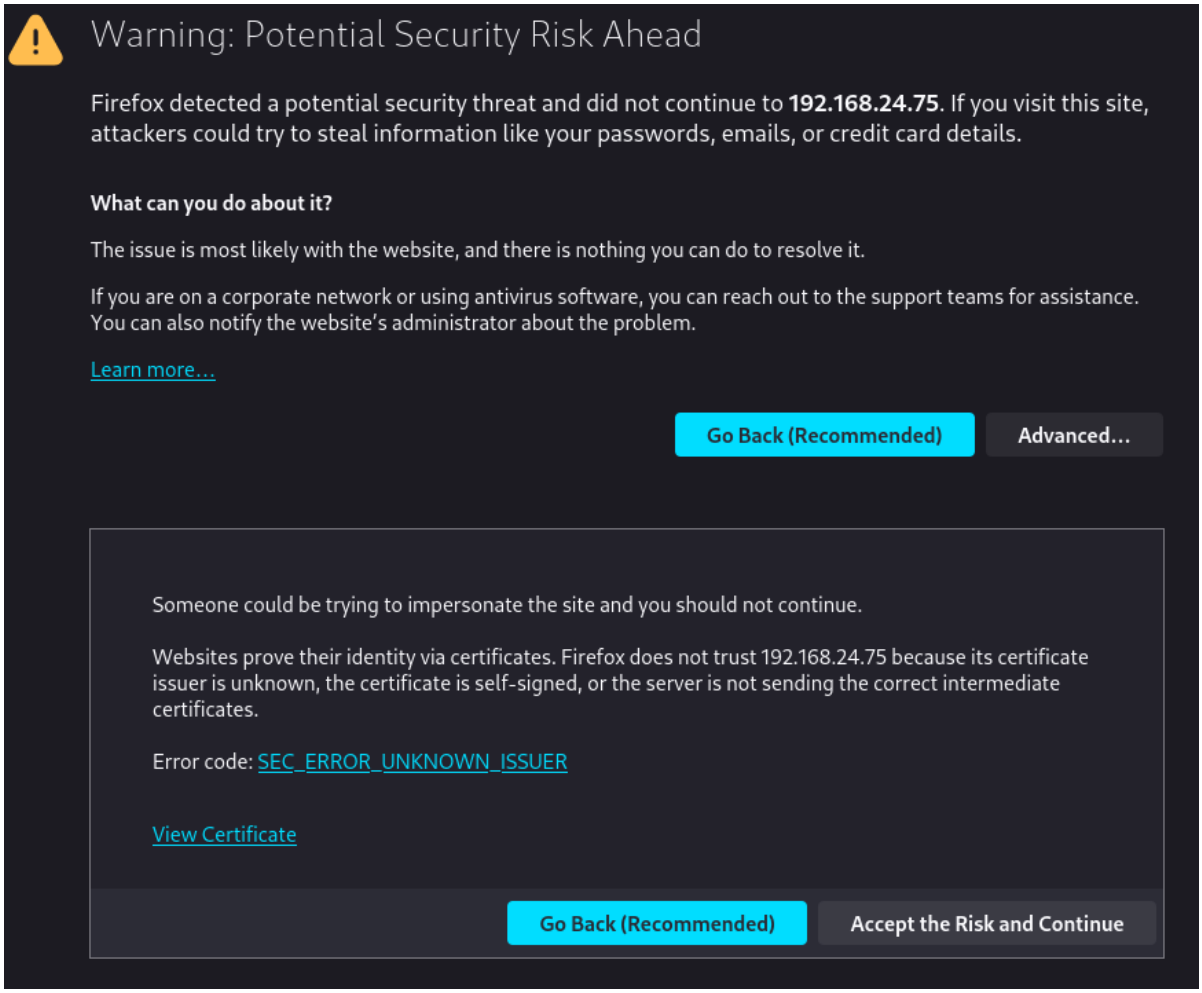
Una vez finalizada la instalación, el resultado muestra las credenciales de acceso y un mensaje que confirma que la instalación fue exitosa.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <CONTRASEÑA>
INFO: Installation finished.
```

Instalación y configuración exitosa de Wazuh. Para acceder a la interfaz web de Wazuh se utiliza: https://<wazuh-dashboard-ip> (con las respectivas credenciales)

```
Nombre de usuario: admin
Contraseña: <CONTRASEÑA>
```

Cuando accede al panel de Wazuh por primera vez, el navegador muestra un mensaje de advertencia que indica que el certificado no fue emitido por una autoridad confiable. Esto es lo esperado y el usuario tiene la opción de aceptar el certificado como una excepción o, alternativamente, configurar el sistema para usar un certificado de una autoridad confiable.



Almacenamiento de contraseñas.

Se puede encontrar las contraseñas de todos los usuarios del indexador de Wazuh y de la API de Wazuh en la página wazuh-passwords.txtarchivo dentro wazuh-install-files.tar.

Para imprimirlos, ejecute el siguiente comando:

```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

Instalación del agente de Wazuh.

En caso de no tener instalado el paquete 'curl' se debe proceder con la instalación del mismo para realizar la descarga de elementos.

```
sudo apt install curl
```

Instalación de claves GPG

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

Añadir el repositorio de Wazuh a las listas de repositorios.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

Actualizar la información de los paquetes.

```
apt-get update
```

DESPLIEGUE DEL AGENTE.

Se recomienda desplegar el agente de Wazuh desde el servidor en la web por la simplicidad de su ejecución.

Agregamos al nuevo agente:

Deploy a new agent

Refresh

1 Choose the operating system

Red Hat Enterpris... | CentOS | Ubuntu | Windows | macOS

Show less

AIX | Alpine | Amazon Linux | Debian | Fedora

HP-UX | openSUSE | Oracle Linux | Raspbian OS | Solaris

SUSE

2 Choose the version

Debian 7 | Debian 8 | Debian 9 +

3 Choose the architecture

i386 | x86_64 | armhf | aarch64 | PowerPC

4 Wazuh server address

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

192.168.24.75

4 Wazuh server address

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

192.168.24.75

5 Optional settings

The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set the agent name below.

Assign an agent name

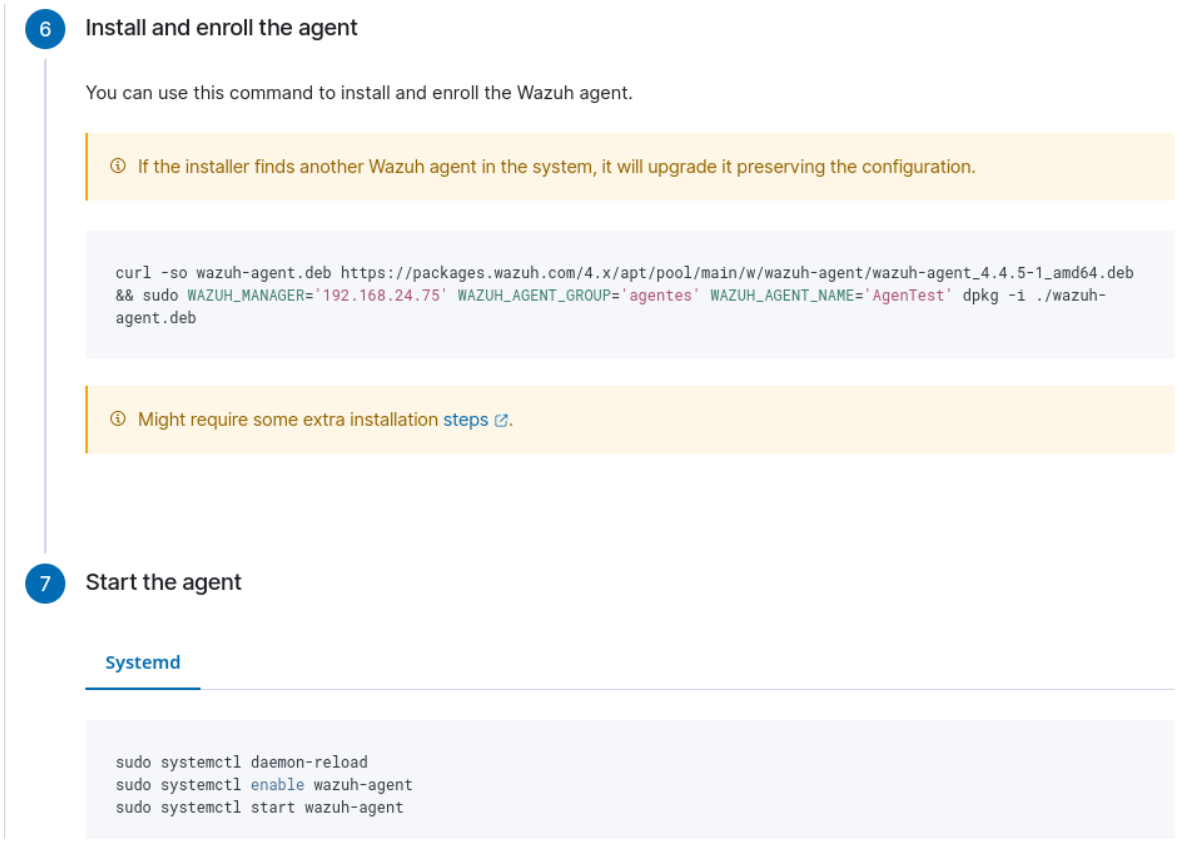
AgenTest

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

Select one or more existing groups

agentes ×

default



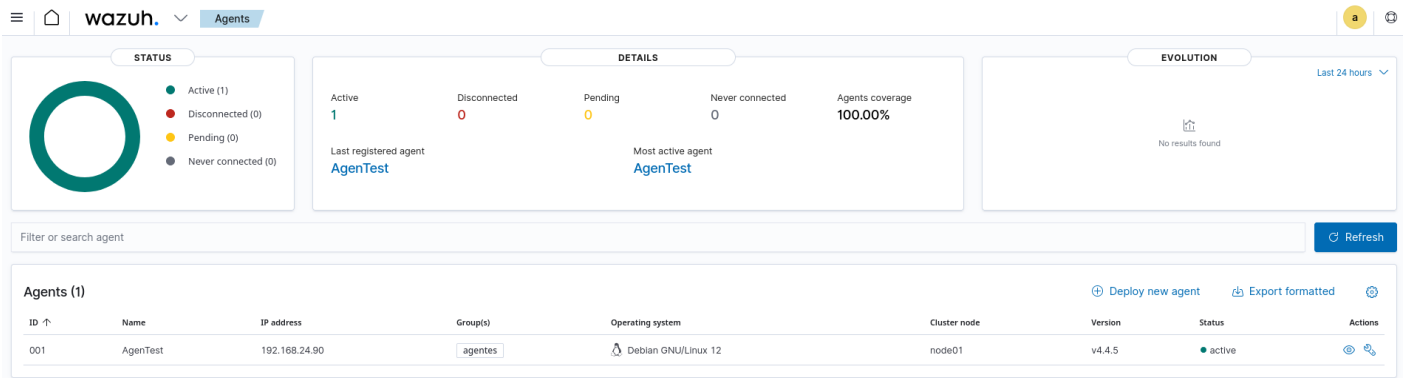
Con el asistente tenemos los comandos a insertar en el terminal del nuevo agente por lo que procedemos a copiar los comandos generados:

```
root@hostvictima:/home/victima# curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.4.5-1_amd64.deb && sudo WAZUH_MANAGER='192.168.24.75
' WAZUH_AGENT_GROUP='agentes' WAZUH_AGENT_NAME='AgenTest' dpkg -i ./wazuh-agent.deb
Selecting previously unselected package wazuh-agent.
(Reading database ... 160320 files and directories currently installed.)
Preparing to unpack ./wazuh-agent.deb ...
Unpacking wazuh-agent (4.4.5-1) ...
Setting up wazuh-agent (4.4.5-1) ...
```

```
root@hostvictima:/home/victima# sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Synchronizing state of wazuh-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@hostvictima:/home/victima# systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; preset: enabled)
     Active: active (running) since Tue 2023-10-10 11:46:03 EDT; 9s ago
    Process: 27279 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 27 (limit: 3490)
     Memory: 20.5M
        CPU: 199ms
     CGroup: /system.slice/wazuh-agent.service
             ├─27301 /var/ossec/bin/wazuh-execd
             ├─27312 /var/ossec/bin/wazuh-agentd
             ├─27325 /var/ossec/bin/wazuh-syscheckd
             ├─27337 /var/ossec/bin/wazuh-logcollector
             └─27354 /var/ossec/bin/wazuh-modulesd

Oct 10 11:45:56 hostvictima systemd[1]: Starting wazuh-agent.service - Wazuh agent...
Oct 10 11:45:56 hostvictima env[27279]: Starting Wazuh v4.4.5...
Oct 10 11:45:57 hostvictima env[27279]: Started wazuh-execd...
Oct 10 11:45:58 hostvictima env[27279]: Started wazuh-agentd...
Oct 10 11:45:59 hostvictima env[27279]: Started wazuh-syscheckd...
Oct 10 11:46:00 hostvictima env[27279]: Started wazuh-logcollector...
Oct 10 11:46:01 hostvictima env[27279]: Started wazuh-modulesd...
Oct 10 11:46:03 hostvictima env[27279]: Completed.
Oct 10 11:46:03 hostvictima systemd[1]: Started wazuh-agent.service - Wazuh agent.
```

Actualizamos el navegador y tenemos al agente desplegado.



Revision #13
Created 3 abril 2024 12:03:45 by Ricardo Chavez
Updated 10 abril 2024 11:05:56 by Ricardo Chavez