

wazuh.

The Open Source Security Platform



Wazuh : Comment mettre en place un serveur SIEM et IDS avec Wazuh

Responsable	Lucas GRANDVAUX
Tags	Guides et procédures Résolutions



Ce tutoriel a pour but de mettre en place une solution de sécurité capable de centraliser les journaux système, détecter les comportements suspects et renforcer la protection de l'infrastructure de l'entreprise Cyna. Il s'appuie sur un outil combinant les fonctions d'un SIEM, d'un système de détection d'intrusion (IDS), et d'une solution de réponse aux menaces (XDR). L'objectif est de collecter, corrélérer et analyser en temps réel les données de sécurité afin de détecter des activités anormales, améliorer la visibilité sur le système d'information et réagir efficacement en cas de menace.

- [1. Mise à jours des paquets debian](#)
- [2. Installation de wazuh](#)
 - [2.1 Interface web d'administration](#)
 - [2.2 Les agents](#)
 - [2.2.1 Linux](#)
 - [2.2.2 Windows](#)
- [3. Test de bon fonctionnement](#)

1. Mise a jours des paquets debian

Mettre a jours les paquets Debian avec la commande suivante :

```
sudo apt update && sudo apt upgrade -y
```

installez les paquets nécessaires suivants :

```
sudo apt install vim git sudo curl -y
```

2. Installation de wazuh

Téléchargez et exécutez l'assistant d'installation Wazuh avec cette commande :

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./w
```

Une fois l'assistant terminé l'installation, la sortie affiche les informations d'identification d'accès et un message confirmant que l'installation a réussi.

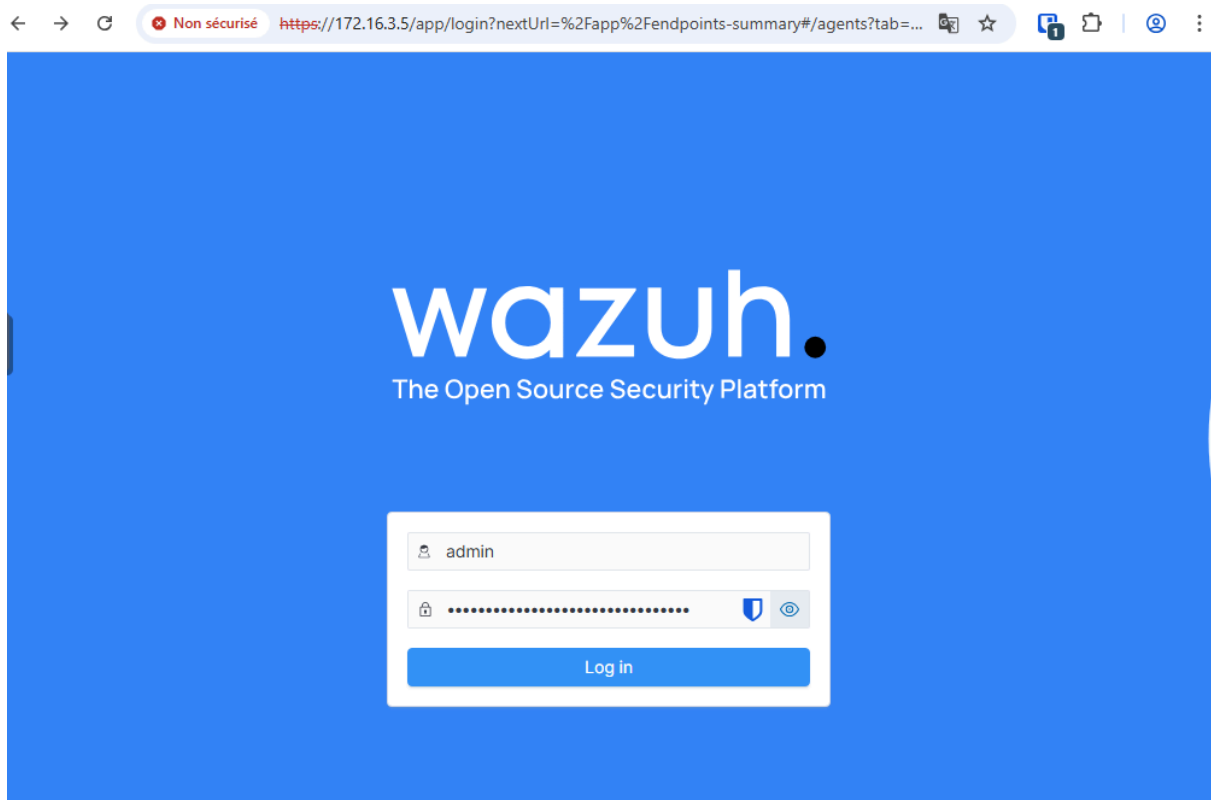
```
INFO: --- Summary ---  
INFO: You can access the web interface https://172.16.3.5/  
User: admin  
Password: <ADMIN_PASSWORD>  
INFO: Installation finished.
```

Vous avez maintenant installé et configuré Wazuh.

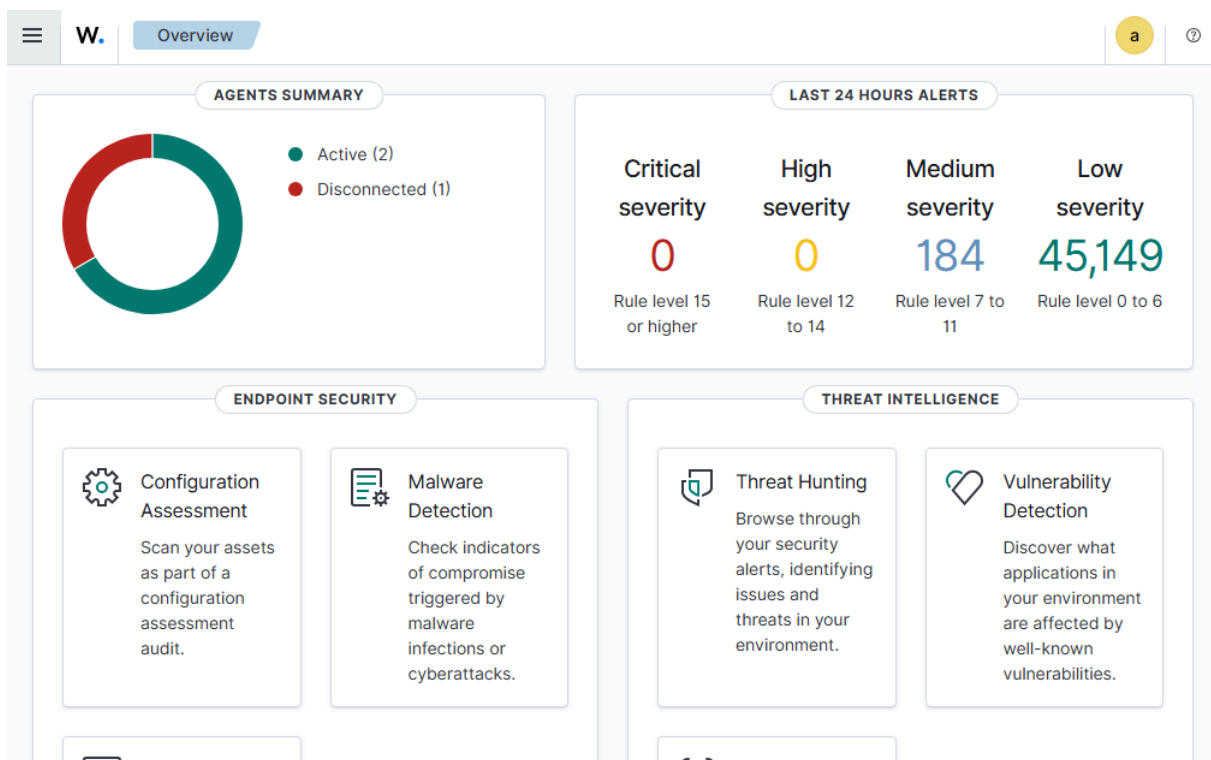
2.1 Interface web d'administration

Maintenant, il faut accéder à l'interface Web de Wazuh avec `https://172.16.3.5` et l'identifiants :

- **Nom d'utilisateur :** `admin`
- **Mot de passe :** `<ADMIN_PASSWORD>`



Voici la page d'accueil de Wazuh :



2.2 Les agents

Afin de surveiller et remonter les différentes informations, il va falloir mettre en place et installer les agents sur les différents serveurs (Windows, Linux, etc...).


2.2.1 Linux

Pour déployer un nouvelle agent, aller dans Agents management > Summary > Deploy a new agent

Deploy new agent

✓

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

①

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 (FQDN).

Assign a server address ①

✓

Remember server address

Sélectionner l'architecture de votre machine Linux, dans mon cas c'est une **DEB amd64**, puis dans l'adresse IP, y insérer celle de votre serveur Wazuh.

Puis dans **Optional settings**, renseigner le nom de l'agent, par exemple si l'agent sera sur mon serveur NTP, je peux le nommer NTP. Puis sélectionner un groupe, je vais choisir en fonction des VLAN, vu que le serveur NTP se situe dans le VLAN DMZ, j'ai créer en amont pour chaque VLAN son groupe, je vais donc l'ajouter dans le groupe **DMZ**.



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: [?](#)

NTP

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

Select one or more existing groups: [?](#)

DMZ x



Enfin dans l'étape 4, il y est inscrit une commande, cette commande il faudra l'exécuter sur le serveur cible, donc le serveur NTP, une fois la commande exécuter, il faudra relancer le démon, puis activer et démarrer l'agent wazuh. Une fois cette étape terminer, votre agent wazuh est installer et configurer sur votre serveur NTP.

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_4.12.0-1_amd64.deb && sudo WAZUH_MANAGER='172.16.3.5' WAZUH_AGENT_GROUP='DMZ' WAZUH_AGENT_NAME='NTP' dpkg -i ./wazuh-agent_4.12.0-1_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.

5

Start the agent:


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


2.2.2 Windows


Pour déployer un nouvelle agent, aller dans Agents management > Summary > Deploy a new agent

Deploy new agent

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

① 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 (FQDN).

Assign a server address ①

☒ Remember server address

Sélectionner l'architecture **MSI 32/64 bits**, puis dans l'adresse IP, y insérer celle de votre serveur Wazuh.

Puis dans **Optional settings**, renseigner le nom de l'agent, par exemple si l'agent sera sur mon serveur Windows Server ou est hébergé dessus SharePoint Server 2019, je peux le nommer SharePoint. Puis sélectionner un groupe, je vais choisir en fonction des VLAN, vu que le serveur SharePoint Server 2019 se situe dans le VLAN Serveurs, je vais donc l'ajouter dans le groupe **Servers**.

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: ①

① The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Select one or more existing groups: ①



Enfin dans l'étape 4, il y est inscrit une commande, cette commande il faudra l'exécuter sur le serveur cible, donc le serveur Windows Server ou est héberger SharePoint Server, une fois la commande exécuter, il faudra simplement démarrer l'agent wazuh. Une fois cette étape terminer, votre agent wazuh est installer et configurer sur votre serveur Windows Server.

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

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='172.16.3.5' WAZUH_AGENT_GROUP='Servers' WAZUH_AGENT_NAME='SharePoint'
```

③ 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
```

3. Test de bon fonctionnement

Nous allons créer un nouveau utilisateurs et lui attribué des privilèges élevé sudo sur la machine virtuelle Trésorerie ou un agent y est deja installé, une fois les commandes executé nous pourrons directement l'apercevoir sur **Agents management > Summary >** cliquer sur l'agent **Tresorerie >**

Ou aller dans **Explore > Discover >** filtré avec le nom d'utilisateurs **demo-admin-02**

Nous pouvons donc apercevoir que l'information a l'issu de la création d'un utilisateur a bien



Puis dans **Agents management > Summary** > cliquer sur l'agent **Tresorerie** > nous pouvons retrouver sur les 5 dernières minutes, différents graphiques et données, ou l'on retrouve notamment l'élévation de privilège "**sudo**" d'un compte utilisateurs, et la création d'un compte

