

Wazuh

Wazuh est une plateforme open-source de sécurité utilisée pour la détection d'intrusions, la surveillance de l'intégrité des fichiers, l'analyse des journaux, et la gestion des vulnérabilités. Elle permet de centraliser les données de sécurité, de détecter les comportements suspects et de renforcer la protection des systèmes informatiques.

Les agents Wazuh sont des programmes installés sur les machines à surveiller (serveurs, postes clients, etc.). Ils collectent des données de sécurité comme les journaux système, les changements de fichiers, et les tentatives d'accès. Ces informations sont ensuite envoyées au serveur Wazuh pour être analysées et détecter d'éventuelles menaces.

1) Télécharger Wazuh en ligne de commande sur debian

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

2. Télécharger les agents Wazuh

Les agents Wazuh sont disponibles pour plusieurs systèmes d'exploitation : documentation.wazuh.com

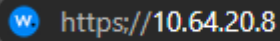
Linux

Windows

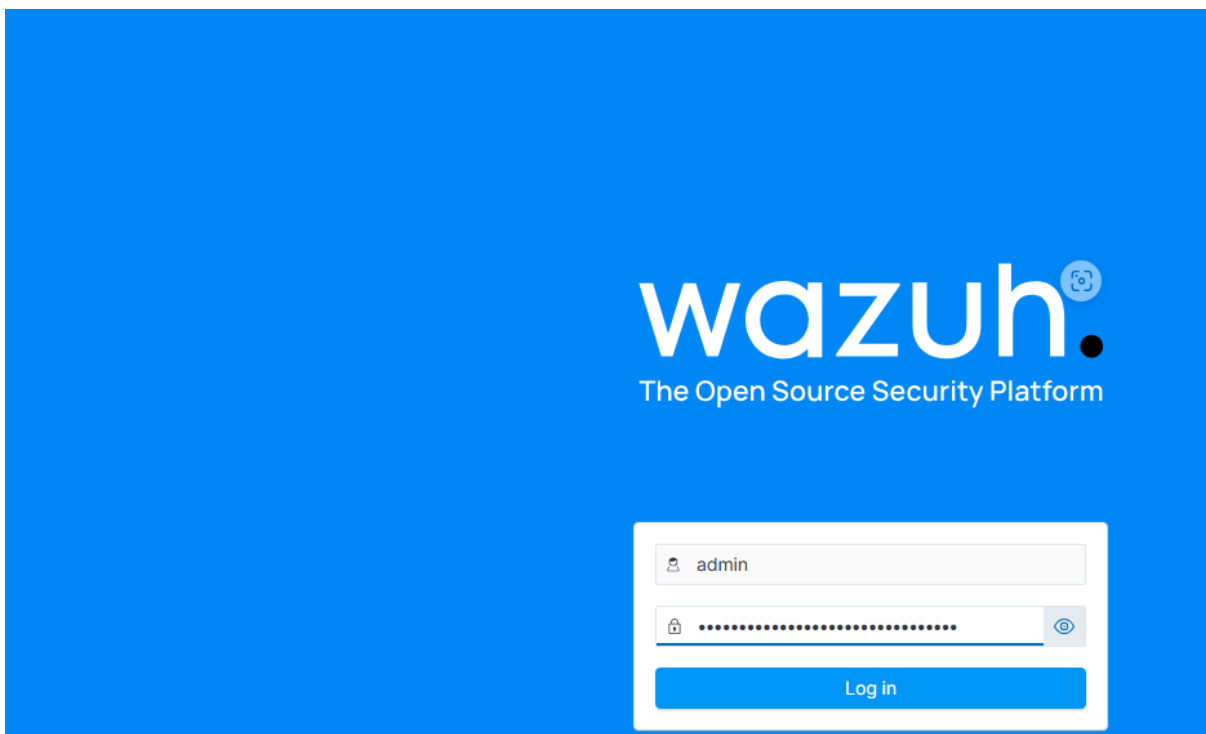
macOS

3. Accéder au tableau de bord Wazuh

Après l'installation, le tableau de bord Wazuh est accessible via un navigateur web à l'adresse

 https://10.64.20.8

Connectez-vous avec les identifiants fournis lors de l'installation.






2) Pour déployer un agent

1. Connecte-toi à l'interface web Wazuh.
2. Dans le menu, clique sur Agents > Deploy new agent.
3. Sélectionne le système d'exploitation de la machine cible (Linux, Windows, etc.).

4. Suis les instructions fournies pour l'installation et la configuration de l'agent.

Deploy new agent

Select the package to download and install on your system:

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

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 [?](#)

10.64.20.8

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: [?](#)

agent-wazuh-win18

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

default

Run the following commands to download and install the agent:

```
curl -o wazuh-agent-4.12.0-1.x86_64.rpm https://packages.wazuh.com/4.x/yum/wazuh-agent-4.12.0-1.x86_64.rpm && sudo WAZUH_MANAGER='10.64.20.8' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='agent-wazuh-win18' rpm -ihv wazuh-agent-4.12.0-1.x86_64.rpm
```

Sur linux a la fin :
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent