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) Telecharger Wazuh en ligne de commande sur debian

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

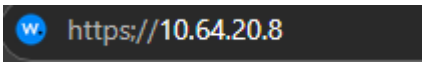
2. Télécharger les agents Wazuh

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

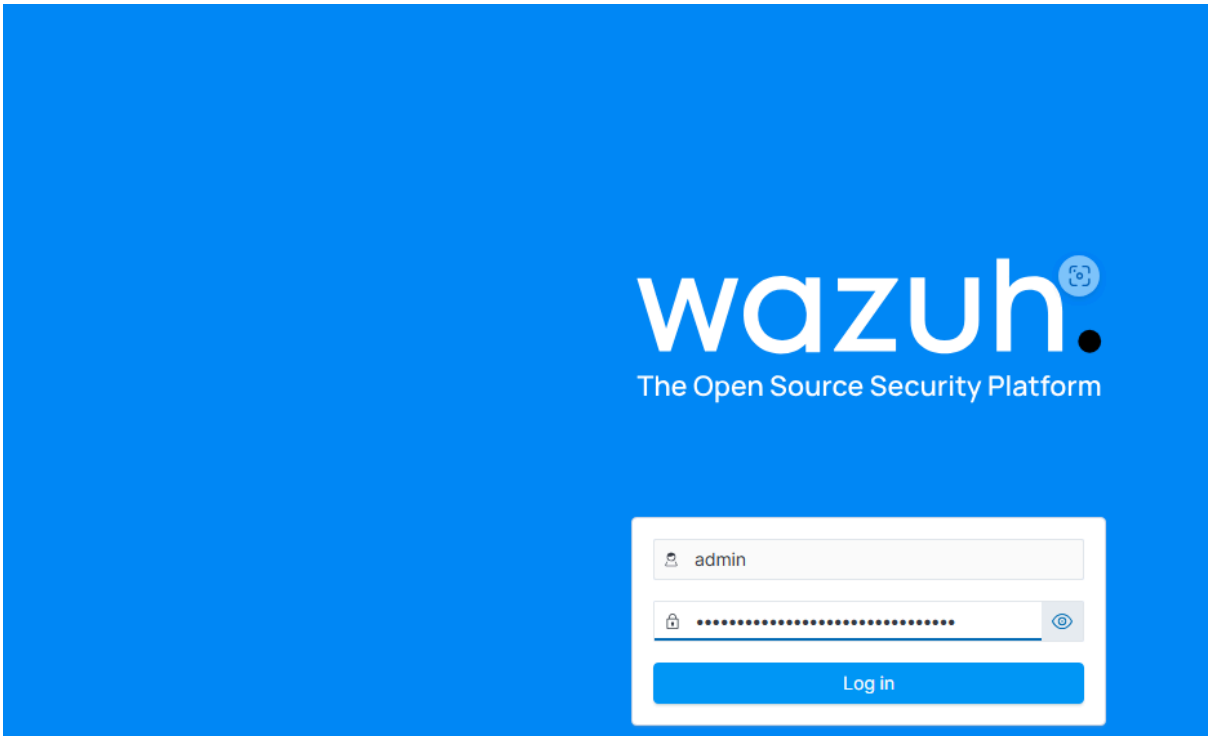
Linux
Windows
macOS

3. Accéder au tableau de bord Wazuh

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



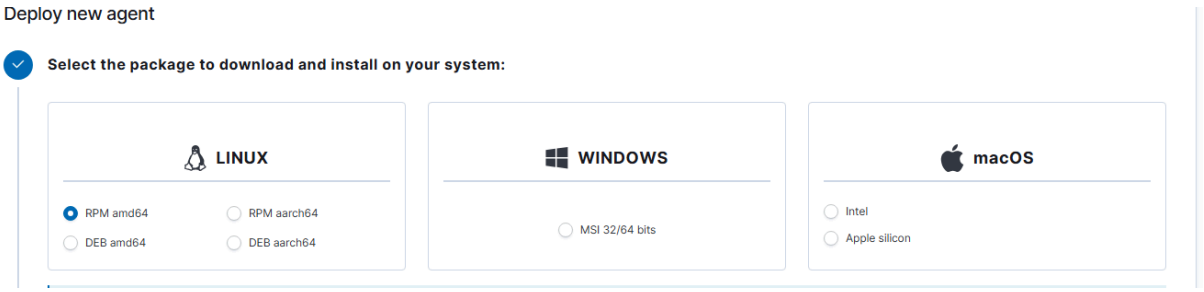
Connectez-vous avec les identifiants fournis lors de l'installation.

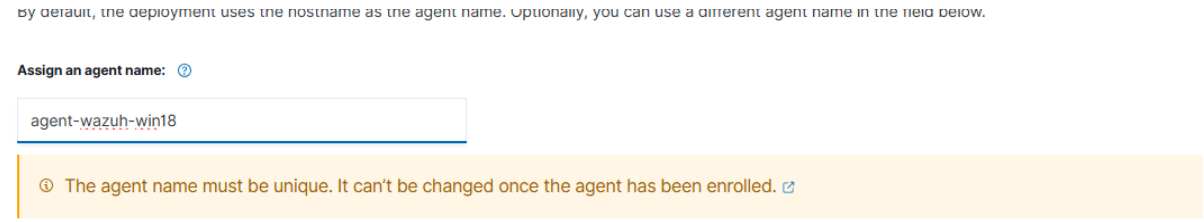


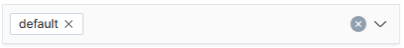
2) Pour déployer un agent

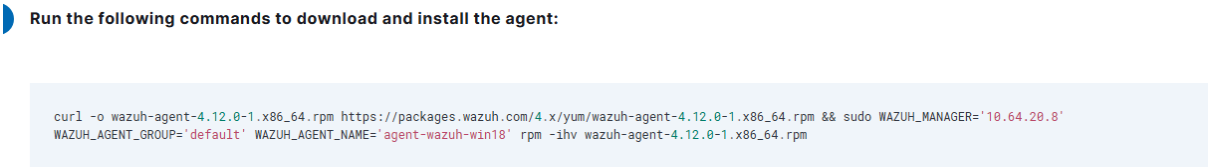
1. Connecte-toi à l’interface web Wazuh.
2. Dans le menu, clique sur Agents > Deploy new agent.
3. Sélectionne le système d’exploitation de la machine cible (Linux, Windows, etc.).

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









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