Doc Wazuh

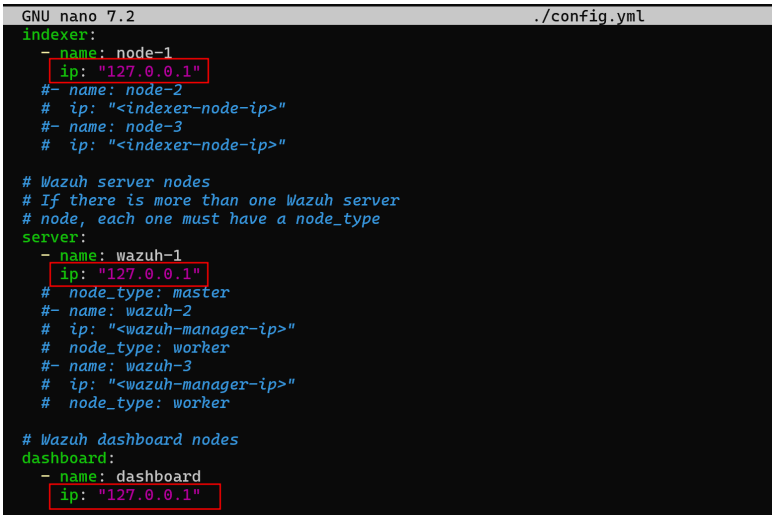
Installation du cluster d'indexation WAZUH

> ⚠️ **Cette partie de l'installation est à effectué sur une première machine Linux.**
>
> **4Go de RAM sont requis pour le bon fonctionnement du serveur.**

Tout d'abord installons l'assistant d'installation Wazuh ainsi que le fichier de configuration :

```
curl -sO https://packages.wazuh.com/4.10/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.10/config.yml
```

Modifiez le fichier `./config.yml` et remplacez les adresses IP par votre adresse IP correspondante.



Exécutez ensuite l'assistant d'installation précédemment téléchargé

```
bash wazuh-install.sh --generate-config-files
```

Installation des nœuds d'indexation Wazuh

Téléchargez l'assistant d'installation Wazuh

```
curl -sO https://packages.wazuh.com/4.10/wazuh-install.sh
```

Exécutez ensuite l'assistant d'installation

```
bash wazuh-install.sh --wazuh-indexer node-1
#Notez que "node-1" doit être potentiellement remplacé par le nom que vous
#à votre indexer lors de la modification du fichier config.yml
```

⚠️ Cette étape doit être répéter autant de fois qu'il y a de noeuds

Initialisation du cluster

Vous pouvez dès à présent lancer le cluster

```
bash wazuh-install.sh --start-cluster
```

Pour récupérer le mot de passe admin exécutez la commande

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | g
```

Pour finir entrez la commande

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200
#Remplacez <ADMIN_PASSWORD> par votre mot de passe admin
#Remplacez <WAZUH_INDEXER_IP> par l'adresse IP de votre indexeur
```

Installation du serveur Wazuh

Téléchargez l’assistant d’installation Wazuh

```
curl -sO https://packages.wazuh.com/4.10/wazuh-install.sh
```

Démarrez l’installation

```
bash wazuh-install.sh --wazuh-server wazuh-1
#Notez que "wazuh-1" doit être potentiellement remplacé par le nom que vous
#à votre serveur lors de la modification du fichier config.yml
```

⚠️ Si vous voulez faire un cluster de serveurs à plusieurs noeuds, répétez l'opération en **changeant le nom du noeud** à chaque fois.

Installation du tableau de bord Wazuh

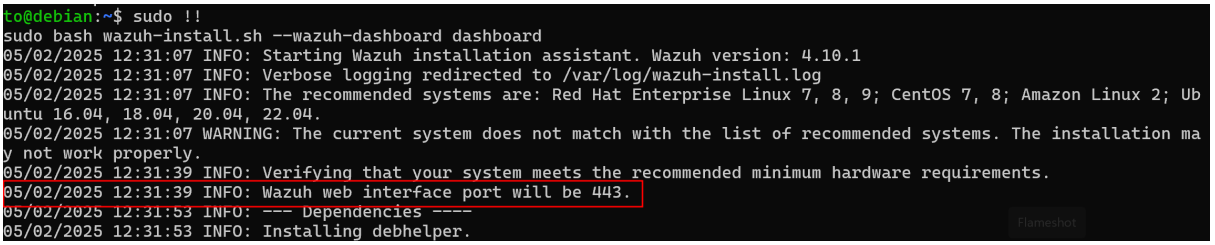
Téléchargez l'assistant d'installation Wazuh

```
curl -sO https://packages.wazuh.com/4.10/wazuh-install.sh
```

Démarrez l'installation

```
bash wazuh-install.sh --wazuh-dashboard dashboard
#Notez que "dashboard" doit être potentiellement remplacé par le nom que vo
#à votre serveur lors de la modification du fichier config.yml
```

💡 Durant l'installation, le port de l'interface web est indiqué. Par défaut, le port 443 est utilisé.



Si l'installation s'est correctement effectuée, vous devriez voir ce message dans votre terminal.

```
05/02/2025 12:41:06 INFO: Wazuh dashboard web application initialized.
05/02/2025 12:41:06 INFO: --- Summary ---
05/02/2025 12:41:06 INFO: You can access the web interface https://192.168.56.102:443
    User: admin
    Password: c8S*RHAZe6u5VTc.Nu2sbp133ljZ*saT
05/02/2025 12:41:06 INFO: Installation finished.
to@debian:~$
```

Récupérez maintenant les mots de passe générés par Wazuh

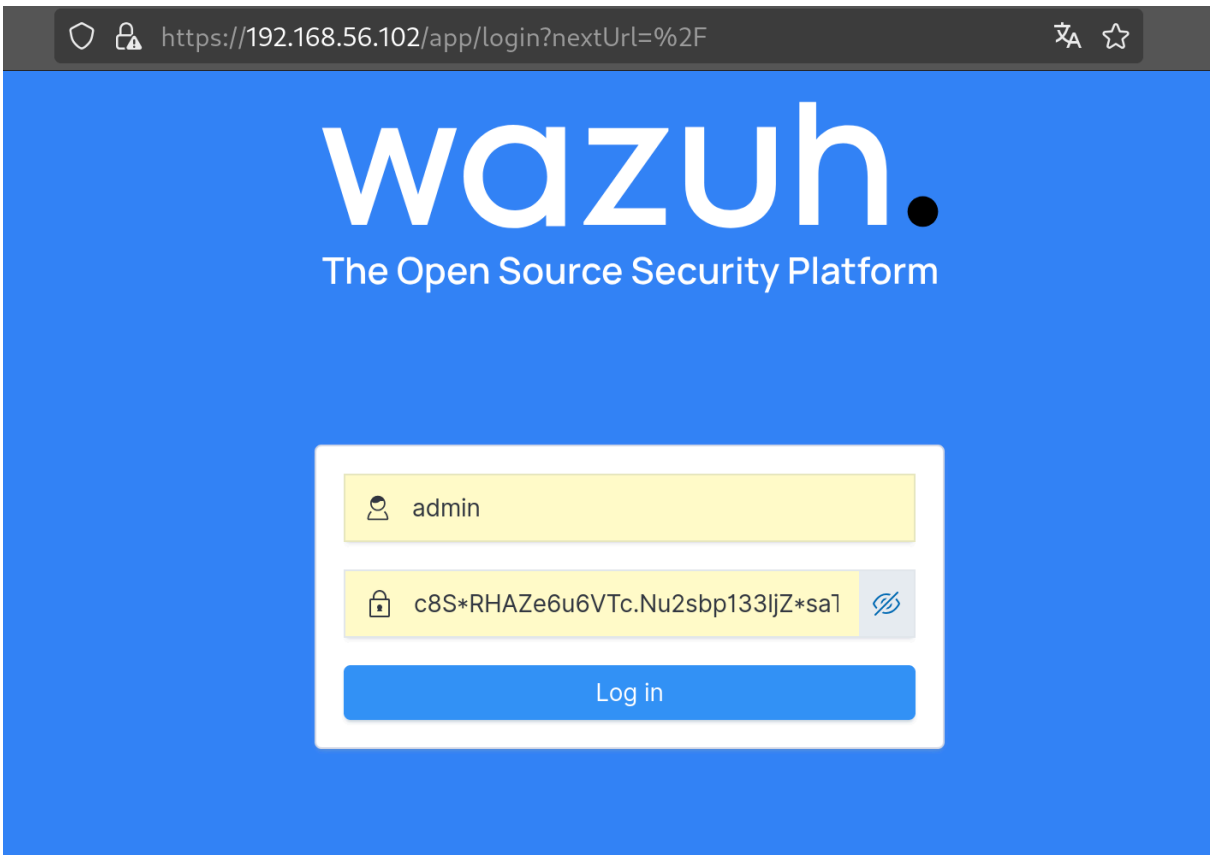
```
tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

Vous pouvez dès à présent vous connecter au tableau de bord depuis une autre machine.

URL : https://<ADRESSE_IP_TABLEAUDEBORD>

Utilisateur : admin

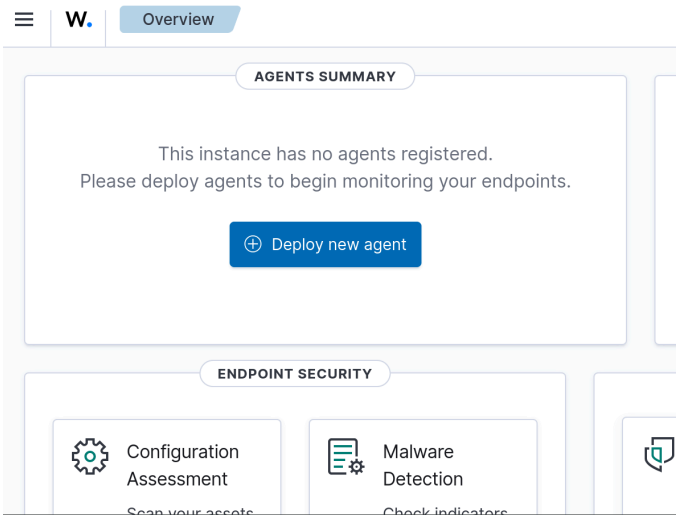
Mot de passe : le mot de passe précédemment récupéré.



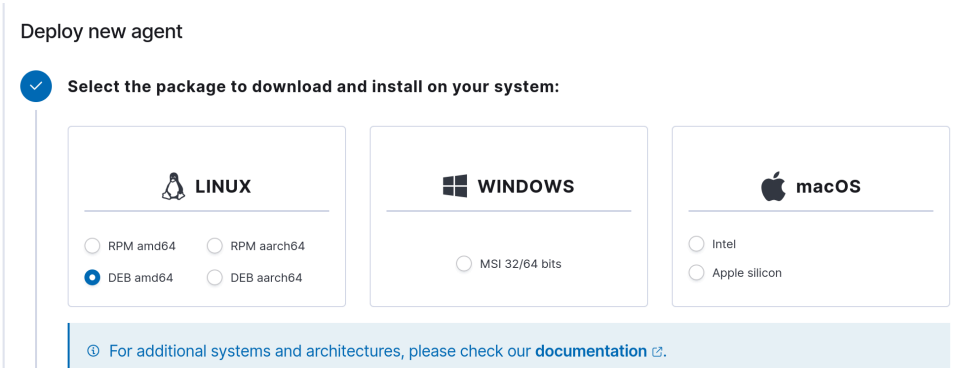
Installation de l’agent Wazuh

> ⚠️ **Installez l’agent sur la machine que vous souhaitez surveiller.**

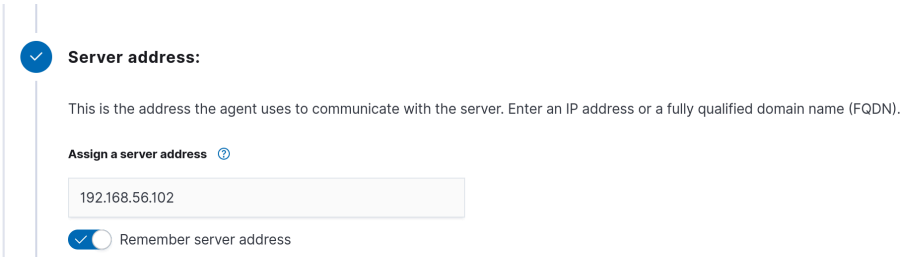
Rendez vous sur votre tableau de bord Wazuh, puis cliquez sur **“Deploy new agent”**



Sélectionnez **la version du système sur lequel vous souhaitez installer l’agent.**



Renseignez ensuite **l’adresse IP utilisée lors de la création du serveur Wazuh**



Une commande propre à vos choix sera disponible, celle-ci doit être exécutée sur la machine sur laquelle vous souhaitez installé l'agent

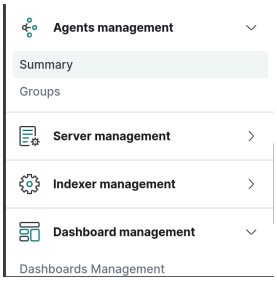
```
#Exemple de commande
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-
&& sudo WAZUH_MANAGER='192.168.56.102' WAZUH_AGENT_NAME='Agent-
```

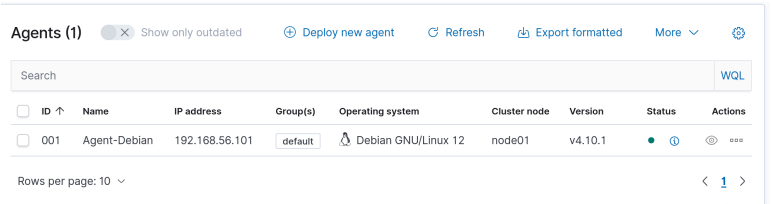
Démarrez maintenant l'agent en effectuant les commandes suivantes

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent #Sert à activer le lancement automatique
sudo systemctl start wazuh-agent #Lance le service de l'agent.
```

L'agent est désormais installé et lancé, vous pouvez accéder aux informations de la machine en vous rendant sur le tableau de bord.

Si l'installation et le démarrage ont été correctement effectués, vous pourrez apercevoir votre machine en vous rendant dans **"Agents Management"** puis **"Summary".**





Documentation créée par Théo BRET