



# Doc Wazuh

## Installation du cluster d'indexation WAZUH



**Cette partie de l'installation est à effectuer 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.

```
GNU nano 7.2                               ./config.yml
indexer:
- name: node-1
  ip: "127.0.0.1"
#- name: node-2
# ip: "<indexer-node-ip>"
#- name: node-3
# ip: "<indexer-node-ip>"

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
- name: wazuh-1
  ip: "127.0.0.1"
  node_type: master
#- name: wazuh-2
# ip: "<wazuh-manager-ip>"
# node_type: worker
#- name: wazuh-3
# ip: "<wazuh-manager-ip>"
# node_type: worker

# Wazuh dashboard nodes
dashboard:
- name: dashboard
  ip: "127.0.0.1"
```

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 choisissez pour votre indexer lors de la modification du fichier config.yml



Cette étape doit être répétée autant de fois qu'il y a de nœuds

## 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
```

```
to@debian:~$ sudo tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "'admin'" -A 1
indexer_username: 'admin'
indexer_password: '4lBnWx?1.nU.8ED6IoLNLFpHPpnbDZwm' mot de passe
to@debian:~$
```

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 nœuds, répétez l'opération en **changeant le nom du nœud** 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 vous avez donné 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.

```
to@debian:~$ sudo !!
sudo bash wazuh-install.sh --wazuh-dashboard dashboard
05/02/2025 12:31:07 INFO: Starting Wazuh installation assistant. Wazuh version: 4.10.1
05/02/2025 12:31:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
05/02/2025 12:31:07 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04.
05/02/2025 12:31:07 WARNING: The current system does not match with the list of recommended systems. The installation may not work properly.
05/02/2025 12:31:39 INFO: Verifying that your system meets the recommended minimum hardware requirements.
05/02/2025 12:31:39 INFO: Wazuh web interface port will be 443.
05/02/2025 12:31:53 INFO: --- Dependencies ---
05/02/2025 12:31:53 INFO: Installing debhelper.
```

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

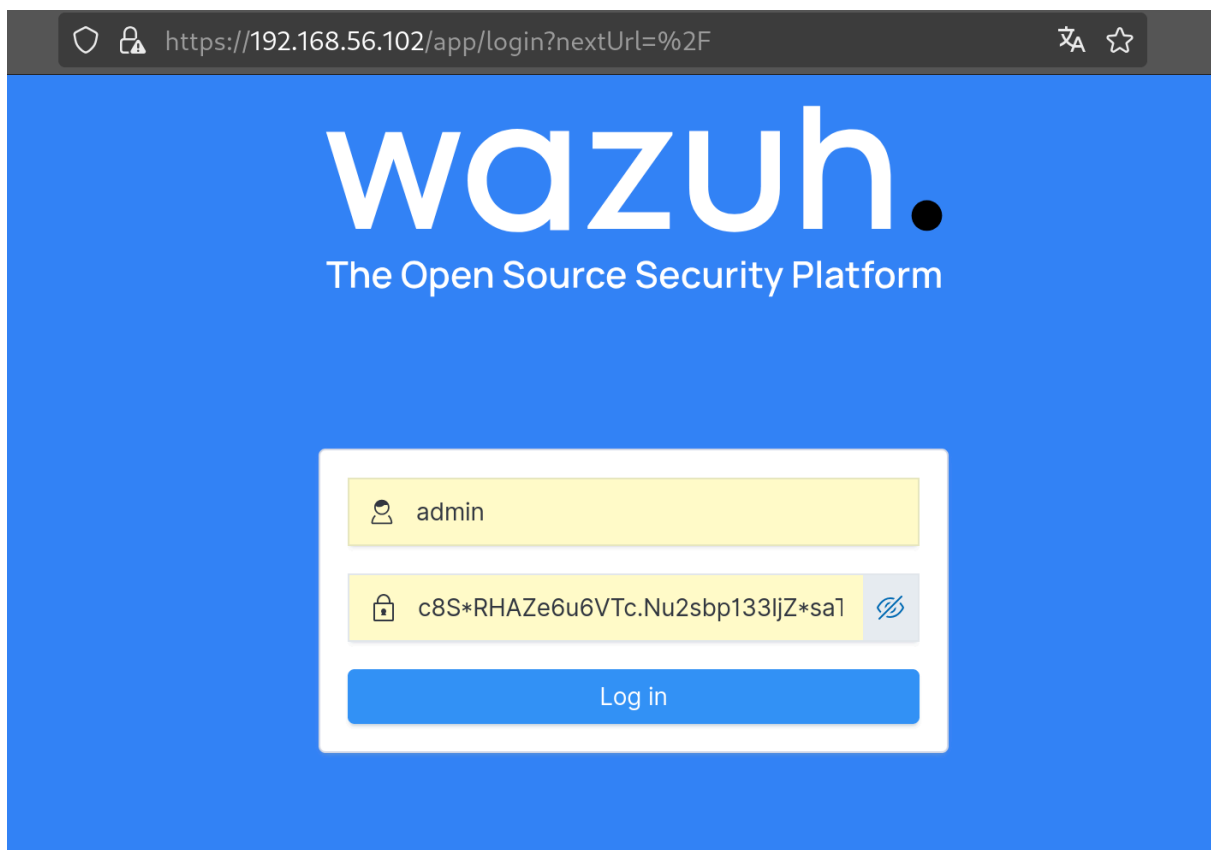
```
tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

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.

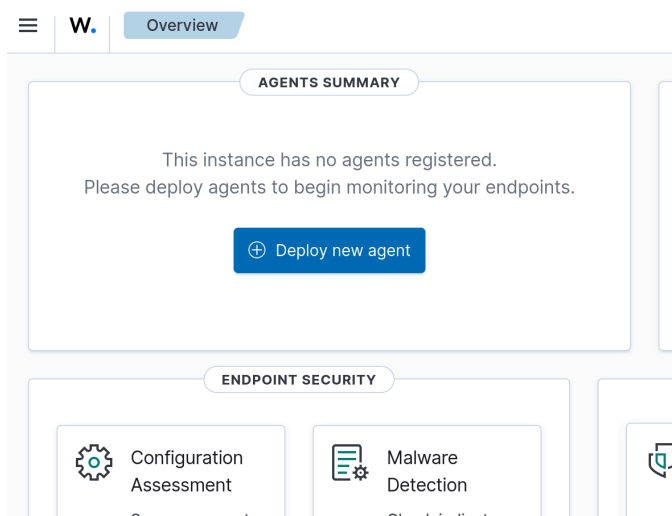


# Installation de l'agent Wazuh

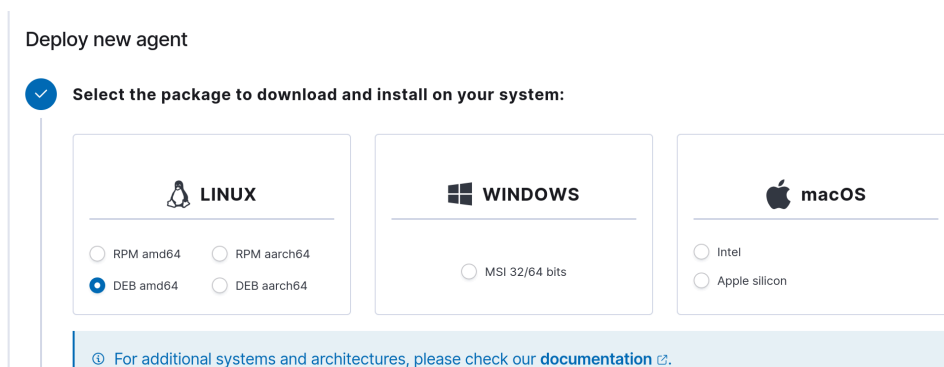


**Installez l'agent sur la machine que vous souhaitez surveiller.**

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

✓

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 [?](#)

192.168.56.102

✓

Remember server address

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"**.

Agents management

Summary

Groups

Server management

Indexer management

Dashboard management

Dashboards Management

Agents (1)

Show only outdated

Deploy new agent

Refresh

Export formatted

More

WQL

Search

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Agent-Debian	192.168.56.101	default	Debian GNU/Linux 12	node01	v4.10.1	<span>●</span> <span>ⓘ</span>	<span>⋮</span>

Rows per page: 10

< 1 >

*Documentation créée par Théo BRET*