Gabriel LIÉBAUT

Guide d’installation Wazuh

INFORMATION SUR L’INSTALLATION :

Wazuh **DOIT** être installé sur une VM séparée de Graylog/Elasticsearch.
Les ports 9200 et 9300 sont utilisés par les deux solutions — il y aurait un conflit fatal.

Information hardware de la VM

Composant	Valeur recommandée
OS	Debian 12
CPU	4 CPU minimum
RAM	16 Go recommandé
Disque	50 Go SSD minimum

Préparation du système

Mettez à jour le système et installez les dépendances nécessaires :

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

Installation de Wazuh

Téléchargez et lancez le script d'installation officiel Wazuh.

```
curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh
sudo bash ./wazuh-install.sh -a
```

Attention : l’installation prend 10 à 20 minutes selon la connexion internet.

À la fin de l'installation, le script affiche les identifiants. Si vous les avez manqués, extrayez-les avec :

```
sudo tar -xvf wazuh-install-files.tar
sudo cat wazuh-install-files/wazuh-passwords.txt
```

Se connecter à l'interface

Ouvrer un navigateur et connectez-vous à l'URL suivante :

https://<IP de la VM WAZUH>
Identifiant : admin
Mot de passe : MDP récupéré (wazuh-passwords)

Vérification des status

Vérifier l'état des services dans cette ordre précis :

```
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-indexer
sudo systemctl status wazuh-dashboard
```

Vérifier les ports ouverts :

```
sudo ss -tlnp | grep -E '443|1514|1515|9200'
```

Installer les agents Wazuh sur les machines à surveiller

Un agent Wazuh doit être installé sur chaque machine que vous souhaitez surveiller (VM Graylog, hôte Proxmox, autres VMs).

Télécharger l'agent sur chaque machine à surveiller

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-
agent_4.14.5-1_amd64.deb
```

Installer l'agent en pointant vers le manager Wazuh

```
sudo WAZUH_MANAGER='<IP_VM_WAZUH>' dpkg -i ./wazuh-agent_4.14.5-1_amd64.deb
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
sudo systemctl status wazuh-agent
```

Configurer lsb-release sur l'hôte Proxmox

Connectez-vous au Shell de votre hôte Proxmox et installez lsb-release :

```
apt update && apt install -y lsb-release
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.5-1_amd64.deb
WAZUH_MANAGER='<IP_VM_WAZUH>' dpkg -i ./wazuh-agent_4.14.5-1_amd64.deb
```

Activez et redémarrez le service lsb-release sur Proxmox :

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