Installation de wazuh

installation server

1. ouvrir le terminal
2. entrer

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

le logiciel va automatiquement installer indexer, server et dashboard Le mot de passe administrateur sera donner a la fin de l'isntallation, `n'oubliez pas de le noter`

installation agent

agent windows

1. telecharge le .msi sur https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi
2. ouvrir powershell en tant que administrateur et coller

```
./wazuh-agent-4.7.3-1.msi /q WAZUH_MANAGER='addresse.ip.du.server'
WAZUH_AGENT_NAME='CHANGE_MOI'
WAZUH_REGISTRATION_SERVER='addresse.ip.du.server'
```

1. puis pour demarrer le service

```
NET START Wazuh_
```

agent linux

1. ```
   wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb && sudo WAZUH_MANAGER='addresse.ip.du.server' WAZUH_AGENT_NAME='CHANGE_MOI' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb_
   ```

2. demarrer l'agent avec:

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

Certificat SSL pour le dashboard

Pour ajouter un certificat ssl

1. Copier les fichiers (clé, certificat, certificat CA) dans /etc/wazuh-dashboard/certs
2. Modifier les droits

```
chmod 500 /etc/wazuh-dashboard/certs
chmod 400 /etc/wazuh-dashboard/certs/*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

3. Editer le fichier de configuration

```
nano /etc/wazuh-dashboard/opensearch_dashboards.yml
```

Et rajouter ceci:

opensearch_dashboards.yml

```
opensearch.ssl.verificationMode: none
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/srv-
sec1.company.lan.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/srv-
sec1.company.lan.crt"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-
dashboard/certs/company-ca.crt"]
```