Table des matières

Wazuh HIDS

Installation

Indexer

Mini RAM (Go)	Mini CPU (Cores)	Reco RAM (Go)	Reco CPU (Cores)
4	2	16	8

Pour 80 Pc, 10 serveurs, 10 équipements réseaux prévoir 230 Go d'espace disque.

Assistant

Télécharger le Script et le fichier de configuration .yml

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.3/config.yml
```

Éditer le ficher de Config “config.yml”

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: <indexer-node-ip>
    #- 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: <wazuh-manager-ip>
```

```
    #  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: <dashboard-node-ip>
```

Changer les noms et ip des serveurs de votre infra.

Exécutez l'assistant avec l'option –generate-config-files pour générer la clé de cluster Wazuh, les certificats et les mots de passe nécessaires à l'installation. Vous pouvez trouver ces fichiers dans ./wazuh-install-files.tar.

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

Ajouter l'option -i pour toutes vos commandes d'installation si vous utiliser une distro Debian

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

Ceci afin d'ignorer le check de config.

Copiez le fichier wazuh-install-files.tar sur tous les serveurs du déploiement distribué, y compris le serveur Wazuh, l'indexeur Wazuh et les nœuds du tableau de bord Wazuh. Cela peut être fait en utilisant l'utilitaire scp.

Lancer l'installation du noeud indexer.

```
bash wazuh-install.sh --wazuh-indexer node-1
```

node-1 correspond à votre nom de server dans le fichier .yml.

Initialiser votre Cluster

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

Tester l'installation de votre cluster.
Executer cette commande pour extraire le mot de passe Amin de l'archive des fichiers de conf.

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'admin\'" -A 1
```

Tester que votre serveur réponde bien.

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200
```

Server

Mini RAM (Go)	Mini CPU (Cores)	Reco RAM (Go)	Reco CPU (Cores)
2	2	4	8

Pour 80 Pc, 10 serveurs, 10 équipements réseaux prévoir 10 Go d'espace disque.

Assistant

Télécharger le Script d'installation.

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
```

Assurer vous d'avoir copié sur votre serveur le fichier wazuh-install-files.tar depuis l'indexer via la commande SCP.
Lancer l'installation de votre serveur.

```
bash wazuh-install.sh --wazuh-server wazuh-1
```

Modifier l'entrée wazuh-1 par le nom donnée à votre serveur dans le ficher de conf.

Noublier pas l'option -i lors de l'installation si vous opter pour une distro debian.

Dashboard

Indexer

Mini RAM (Go)	Mini CPU (Cores)	Reco RAM (Go)	Reco CPU (Cores)
4	2	8	4

Assistant

Télécharger le Script et le fichier de configuration .yml

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
```

Assurer vous d'avoir copié sur votre serveur le fichier wazuh-install-files.tar depuis l'indexer via la commande SCP. \ **Lancer l'installation de votre serveur dashboard.**

```
bash wazuh-install.sh --wazuh-dashboard dashboard
```

Une fois l'installation terminée:

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
   User: admin
   Password: <ADMIN_PASSWORD>

INFO: Installation finished.
```

Vous avez maintenant installé et configuré Wazuh. Tous les mots de passe générés par l'assistant d'installation de Wazuh se trouvent dans le fichier wazuh-passwords.txt à l'intérieur de l'archive wazuh-install-files.tar. Pour les imprimer, exécutez la commande suivante :

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

Web UI

```
URL: https://<wazuh-dashboard-ip>

Username: admin

Password: <ADMIN_PASSWORD>
```

Paramètrages

Password Enrollement

Wazuh Manager

Pour permettre à l'agent de s'enrôler avec un mot de passe d'hautentification:
Activez l'option d'authentification par mot de passe en ajoutant la configuration mise en évidence ci-dessous à la section <auth> du fichier de configuration du serveur manager dans /var/ossec/etc/ossec.conf.

```
<auth>
  <use_password>yes</use_password>
```

```
</auth>
```

```
<!-- Configuration for wazuh-authd -->
  <auth>
    <disabled>no</disabled>
    <port>1515</port>
    <use_source_ip>no</use_source_ip>
    <purge>yes</purge>
    <use_password>yes</use_password>
    <ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>
    <!-- <ssl_agent_ca></ssl_agent_ca> -->
    <ssl_verify_host>no</ssl_verify_host>
    <ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
    <ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
    <ssl_auto_negotiate>no</ssl_auto_negotiate>
  </auth>
```

Définissez un mot de passe à utiliser avec l'inscription de l'agent. Ceci peut être réalisé de deux manières:

Recommandé - Définir votre propre mot de passe. Cela se fait en créant le fichier /var/ossec/etc/authd.pass sur le manager avec votre mot de passe.

Remplacez <CUSTOM_PASSWORD> par le mot de passe d'inscription de l'agent que vous avez choisi et exécutez la commande suivante:

```
echo "<CUSTOM_PASSWORD>" > /var/ossec/etc/authd.pass
```

Modifier les autorisations et la propriété du fichier authd.pass.

```
chmod 640 /var/ossec/etc/authd.pass
chown root:wazuh /var/ossec/etc/authd.pass
```

Redémarrer le service wazuh pour prendre effet.

```
systemctl restart wazuh-manager
```

Autoriser le service d'inscription à définir un mot de passe aléatoire. Un nouveau mot de passe aléatoire est généré à chaque redémarrage du service Wazuh manager.

Redémarrez le gestionnaire afin que le service d'inscription génère un mot de passe aléatoire. Ce mot de passe est stocké dans /var/ossec/logs/ossec.log.

```
systemctl restart wazuh-manager
```

Exécutez la commande suivante pour obtenir le mot de passe d'inscription de l'agent :

```
grep "Random password" /var/ossec/logs/ossec.log
```

Sortie:

```
2022/01/11 12:41:35 wazuh-authd: INFO: Accepting connections on port 1515.
Random password chosen for agent authentication:
6258b4eb21550e4f182a08c10d94585e
```

Certificate Enrollement

Wazuh Manager

En l'absence d'une autorité de certification déjà configurée, exécutez la commande suivante sur le serveur Wazuh pour l'utiliser comme autorité de certification :

```
openssl req -x509 -new -nodes -newkey rsa:4096 -keyout rootCA.key -out
rootCA.pem -batch -subj "/C=FR/ST=LYS/O=Wazuh"
```

1. Générez une demande de signature de certificat (CSR) pour l'agent Wazuh sur le serveur Wazuh :

- Vérification de l'agent Wazuh sans validation de l'hôte : Ceci est effectué sans spécifier l'adresse IP ou le nom d'hôte de l'agent Wazuh.

```
openssl req -new -nodes -newkey rsa:4096 -keyout sslagent.key -out
sslagent.csr -batch
```

- Vérification de l'agent Wazuh avec validation de l'hôte : cela se fait en spécifiant l'adresse IP ou le nom d'hôte de l'agent Wazuh.

```
openssl req -new -nodes -newkey rsa:4096 -keyout sslagent.key -out
sslagent.csr -subj '/C=FR/CN=<agent_IP>'
```

- sslagent.csrest le CSR à soumettre à l'autorité de certification.
- sslagent.keyest la clé privée CSR générée.

1. Signez le CSR de l'agent généré à l'aide des clés CA :

```
openssl x509 -req -days 365 -in sslagent.csr -CA rootCA.pem -CAkey
rootCA.key -out sslagent.cert -CAcreateserial
```

- sslagent.csrest le CSR à soumettre à l'autorité de certification.
- sslagent.certest le certificat SSL signé par le CSR.
- rootCA.pemest le certificat racine de l'autorité de certification.
- rootCA.keyest la clé privée du certificat racine de l'autorité de certification.

Copier le rootCA.pem dans le répertoire **/var/ossec/etc/** de votre serveur Wazuh.

Editer le fichier de configuration **/var/ossec/etc/ossec.conf** en ajouter le chemin du **rootCA.pem**

```
<auth>
   ...
   <ssl_agent_ca>/var/ossec/etc/rootCA.pem</ssl_agent_ca>
</auth
```

Redemarrer le service wazuh-manager:

```
systemctl restart wazuh-manager
```

Clients Windows

Mot de passe

Sur le client windows créer un fichier authd.pass.
C:\Program Files (x86)\ossec-agent pour les OS 64-bit
C:\Program Files\ossec-agent pour les OS 32-bit

```
echo “<CUSTOM_PASSWORD>” > "C:\Program Files (x86)\ossec-agent\authd.pass"
```

Noter en lieux et place de <CUSTOM_PASSWORD> saisisser le mot de passe venant du manager.

Ajouter l'adress ip et les infos d'enrôlement du Wazuh manager dans le fichier de conf du client:

```
C:\Program Files (x86)\ossec-agent\ossec.conf
```

```
<client>
   <server>
       <address>MANAGER_IP</address>
      ...
   </server>
.......
<enrollment>
   <enabled>yes</enabled>
   <manager_address>ip_manager</manager_address>
   <groups>Windows</groups>
</enrollment>
</client>
```

Relancer le service en PowerShell:

```
Restart-Service -Name wazuh
```

Déploiement

Pour déployer un client en ligne de commande (Powershell)

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.9-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.9.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.9.msi /q WAZUH_MANAGER='ip_manager' WAZUH_REGISTRATION_SERVER='ip_manager' WAZUH_REGISTRATION_PASSWORD='************' WAZUH_AGENT_GROUP='Windows'
```

Compléter avec les paramètre de votre serveur Wazuh.

Certificats

Assurez-vous que le certificat SSL signé et les fichiers de clés (**sslagent.certet sslagent.key**) ont été copiés sur le poste.
Idéalement dans le profile de l'utilisateur (administrateur ou assimilé)

Modifiez le fichier de configuration de l'agent Wazuh situé dans "**C:\Program Files (x86)\ossec-agent\ossec.conf**" et incluez les éléments suivants :

```
<client>
   <server>
      <address>WAZUH_MANAGER_IP</address>
   </server>
   <enrollment>
<agent_certificate_path>C:\Users\agent\sslagent\sslagent.cert</agent_certificate_path>
      <agent_key_path>C:\Users\agent\sslagent\sslagent.key</agent_key_path>
   </enrollment>
</client>
```

Relancer le service de l'agent ossec via PowerShell :

```
Restart-Service -Name wazuh
```

Si tout est Ok! vous devriez voir ceci dans votre fichier de log:

```
wazuh-agent: INFO: Valid key received
wazuh-agent: INFO: Waiting 20 seconds before server connection
wazuh-agent: INFO: Evaluation finished.
```

Depuis votre console Wazuh:

Client Linux

Déploiement

```
curl -so wazuh-agent-4.3.9.deb
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-
agent_4.3.9-1_amd64.deb && sudo WAZUH_MANAGER='10.99.30.24'
WAZUH_REGISTRATION_PASSWORD='*********' WAZUH_AGENT_GROUP='Linux' dpkg -i
./wazuh-agent-4.3.9.deb
```

Mot de passe

Créer le fichier contenant le mot de passe d'enrôlement.

```
echo "<CUSTOM_PASSWORD>" > /var/ossec/etc/authd.pass
```

Fixer les droits sur le fichier.

```
chmod 640 /var/ossec/etc/authd.pass
chown root:wazuh /var/ossec/etc/authd.pass
```

configuration de l'agent:

```
nano / etc/ossec/etc/ossec.conf
```

Applique la configuration comme suit:

```
<client>
    <server>
      <address>ip_manager</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>debian, debian11</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
<enrollment>
   <enabled>yes</enabled>
   <manager_address>ip_manager</manager_address>
<authorization_pass_path><PATH_TO_PASSWORD_FILE></authorization_pass_path>
   <groups>Linux</groups>
```

```
</enrollment>
</client>
```

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

Certificate Enrollement

A l'aide de la commande SCP copier les fichiers **sslagent.key** et **sslagent.cert** sur le poste client. Editer le fichier de configuration sur le poste client **/var/ossec/etc/ossec.conf** et modifier la section <client></client> comme dans l'exemple ci dessous:

```
<client>
   <server>
      <address><WAZUH_MANAGER_IP></address>
   </server>
   <enrollment>
<agent_certificate_path>/<PATH_TO>/sslagent.cert</agent_certificate_path>
      <agent_key_path>/<PATH_TO>/sslagent.key</agent_key_path>
   </enrollment>
</client>
```

Redemarrer lagent wazuh sur le poste client:

```
systemctl restart wazuh-agent
```

Activer Vulnérabilitées

Serveur Wazuh

Pour activer la prise en charge des vulnérabilitées sur le serveur:

```
nano /var/ossec/etc/ossec.conf
```

```
 <vulnerability-detector>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <min_full_scan_interval>6h</min_full_scan_interval>
    <run_on_start>yes</run_on_start>

    <!-- Ubuntu OS vulnerabilities -->
    <provider name="canonical">
```

```
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>stretch</os>
    <os>buster</os>
    <os>bullseye</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- RedHat OS vulnerabilities -->
  <provider name="redhat">
    <enabled>yes</enabled>
    <os>5</os>
    <os>6</os>
    <os>7</os>
    <os>8</os>
    <os>9</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Amazon Linux OS vulnerabilities -->
  <provider name="alas">
    <enabled>no</enabled>
    <os>amazon-linux</os>
    <os>amazon-linux-2</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Arch OS vulnerabilities -->
  <provider name="arch">
    <enabled>no</enabled>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Windows OS vulnerabilities -->
  <provider name="msu">
    <enabled>yes</enabled>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Aggregate vulnerabilities -->
  <provider name="nvd">
```

```
      <enabled>yes</enabled>
      <update_from_year>2010</update_from_year>
      <update_interval>1h</update_interval>
    </provider>

  </vulnerability-detector>
```

Client Linux

Editer la config et modifier comme suit:

```
/var/ossec/etc/ossec.conf
```

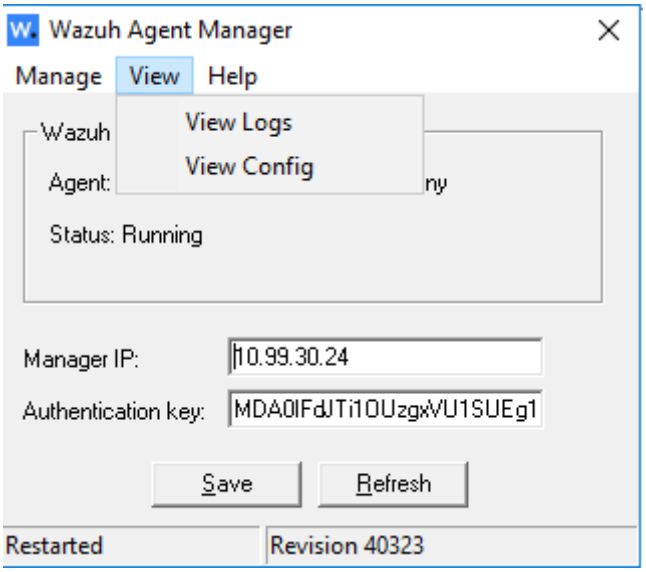
```
<!-- System inventory -->
  <wodle name="syscollector">
    <disabled>no</disabled>
    <interval>1h</interval>
    <scan_on_start>yes</scan_on_start>
    <hardware>yes</hardware>
    <os>yes</os>
    <network>yes</network>
    <packages>yes</packages>
    <ports all="no">yes</ports>
    <processes>yes</processes>

    <!-- Database synchronization settings -->
    <synchronization>
      <max_eps>10</max_eps>
    </synchronization>
  </wodle>
```

Relancer le service !

Client Windows

Sur le client Wazuh Windows éditer la config (attention executer le binaire en mode administrateur).



Ajouter la ligne: “<hotfixes>yes</hotfixes>” pour l'analyse.

```
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>
  <hotfixes>yes</hotfixes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>
```

Relancer le service!!

Changé le certificat auto signé

Si vous souhaitez changer les certificat par défaut par les votres.

```
cp /my-path/my certificat.pem /etc/wazuh-dashboard/certs/dashboard.pem
cp /my-path/my certificat-key.pem /etc/wazuh-dashboard/certs/dashboard-
key.pem
chmod 500 /etc/wazuh-dashboard/certs
```

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

Aplliquer vos changement sur chaque serveur de votre infa.

Manage Agent

```
/var/ossec/bin/manage_agents
```

```
****************************************
* Wazuh v4.3.9 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: L
```

Remove agent

```
/var/ossec/bin/manage_agents -r 00x
```

Aller Plus Loins !
