

1. Installation de Wazuh

Prérequis :

- 3 Virtual machine (vm) en IP statique

Nous allons premièrement récupérer les certificats nécessaires :

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

Modifiez le fichier `./config.yml` et remplacez les noms des nœuds ainsi que les valeurs des adresses IP par les noms et adresses IP correspondants. Vous devez effectuer cette modification pour tous les nœuds Wazuh server, Wazuh indexer et Wazuh dashboard. Ajoutez autant de champs de nœuds que nécessaire.

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "IP_MACHINE_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: "IP_MACHINE_2"
      node_type: master
    - name: wazuh-2
      ip: "IP_MACHINE_3"
      node_type: worker
    #- name: wazuh-3
    # ip: "<wazuh-manager-ip>"
```

```
# node_type: worker

# Wazuh dashboard nodes
dashboard:
  - name: dashboard
    ip: "IP_MACHINE_1"
```

Exécutez le script `./wazuh-certs-tool.sh` pour créer les certificats. Dans le cas d'un cluster multi-nœuds, ces certificats devront ensuite être déployés sur toutes les instances Wazuh de votre cluster.

```
bash ./wazuh-certs-tool.sh -A
```

Compressons ensuite nos fichiers et supprimons `./wazuh-certifications`.

```
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
rm -rf ./wazuh-certificates
```

Enfin installons les paquets manquants :

```
apt-get install debconf adduser procps
```

Passons à l'installation de la clef GPG:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

Ajoutons ensuite le repo à nos sources.list avec le certificat en question :

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

Update :

```
apt-get update
```

Installons enfin wazuh-indexer :

```
apt-get -y install wazuh-indexer
```

Modifiez le fichier de configuration `/etc/wazuh-indexer/opensearch.yml` et remplacez les valeurs suivantes :

- **network.host** : Définit l'adresse de ce nœud pour le trafic HTTP et transport. Ce nœud utilisera cette adresse comme adresse de liaison et d'annonce. Vous pouvez renseigner une adresse IP ou un nom d'hôte.
- **Utilisez la même adresse du nœud que celle définie dans le fichier `config.yml` pour créer les certificats SSL.**
- **node.name** : Nom du nœud Wazuh Indexer tel que défini dans le fichier `config.yml`. Par exemple, `node-1`.

“ Envoyons nos certificats a nos serveurs :

```
scp wazuh-certificates.tar <USER>@<IP>:/home/<USER>/wazuh-certificates.tar
```

Exemple pour un cluster multi-nœuds

cluster.initial_master_nodes : Liste des noms des nœuds éligibles pour devenir maîtres. Ces noms sont définis dans le fichier `config.yml`. Décommentez les lignes pour `node-2` et `node-3`, modifiez les noms ou ajoutez-en d'autres, selon vos définitions dans `config.yml` :

```
cluster.initial_master_nodes:
```

```
- "node-1"  
- "node-2"  
- "node-3"
```

discovery.seed_hosts : Liste des adresses des nœuds éligibles pour devenir maîtres. Chaque élément peut être une adresse IP ou un nom d'hôte. Laissez cette configuration commentée si vous configurez le Wazuh Indexer en tant que nœud unique. Pour une configuration multi-nœuds, décommentez cette section et ajoutez les adresses IP de chaque nœud éligible :

```
discovery.seed_hosts:
```

```
- "10.0.0.1"  
- "10.0.0.2"  
- "10.0.0.3"
```

plugins.security.nodes_dn : Liste des noms distingués (DN) des certificats de tous les nœuds du cluster Wazuh Indexer. Décommentez les lignes pour `node-2` et `node-3` et modifiez les noms communs (CN) et les valeurs selon vos paramètres et vos définitions dans `config.yml` :

```
plugins.security.nodes_dn:
```

- "CN=node-1,OU=Wazuh,O=Wazuh,L=California,C=US"
- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"

Ces modifications permettent de configurer correctement un cluster Wazuh Indexer multi-nœuds avec les adresses IP et noms de nœuds définis dans `config.yml`.

Revision #4

Created 28 January 2025 11:11:32 by Admin

Updated 29 January 2025 09:32:31 by Admin