SIEM - Wazuh (dashboard/indexer/master/worker)

Dans le cadre de la sécurisation des systèmes d’information, le déploiement d’une solution SIEM (Security Information and Event Management) est essentiel pour collecter, analyser et corréler les événements provenant de différents environnements. Ce projet documente l’implémentation de Wazuh, une solution SIEM open-source, en décrivant les rôles de ses différents composants : Dashboard, Indexer, Master et Worker.

1. Installation de Wazuh

Prérequis :

- 3 Virtual machine (vm) en IP statique

Nous allons premièrement récupéré 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`.

2. Wazuh indexer

Pré-requis :

- Assurez-vous qu'une copie du fichier `wazuh-certificates.tar`, créé lors de l'étape de configuration initiale, se trouve dans votre répertoire de travail actuel.

Étapes à suivre

1. Remplacez `<INDEXER_NODE_NAME>` par le nom du nœud Wazuh Indexer tel que défini dans votre fichier `config.yml` (par exemple, `node-1`).
2. Exécutez les commandes suivantes :

```
# Remplacez par le nom du nœud (par exemple, node-1)
NODE_NAME=node-1

# Créez le répertoire des certificats
mkdir /etc/wazuh-indexer/certs

# Décompressez les certificats spécifiques au nœud dans le répertoire
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem
./admin.pem ./admin-key.pem ./root-ca.pem

# Renommez les fichiers pour qu'ils correspondent au format attendu par le Wazuh Indexer
mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem /etc/wazuh-indexer/certs/indexer.pem
mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem

# Définissez les permissions pour sécuriser les certificats
chmod 500 /etc/wazuh-indexer/certs
chmod 400 /etc/wazuh-indexer/certs/*

# Assurez-vous que les certificats appartiennent à l'utilisateur et au groupe Wazuh Indexer
chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

3. Si aucun autre composant Wazuh (comme un manager ou un dashboard) ne sera installé sur ce nœud, supprimez le fichier `wazuh-certificates.tar` pour renforcer la sécurité :

```
rm -f ./wazuh-certificates.tar
```

Vous devez maintenant exécuter ceci sur votre master ainsi que votre worker :

Configurer les permissions Une fois les certificats décompressés et placés, définissez les permissions appropriées :

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

Démarrage du service Wazuh Indexer

1. Activez et démarrez le service Wazuh Indexer :

```
systemctl enable wazuh-indexer
systemctl start wazuh-indexer
```

2. Vérifiez que le service fonctionne correctement :

```
systemctl status wazuh-indexer
```

Action recommandée : Désactiver les mises à jour de Wazuh

Il est recommandé de désactiver les dépôts de paquets Wazuh après l'installation afin d'éviter des mises à jour accidentelles qui pourraient perturber l'environnement.

Exécutez la commande suivante pour désactiver le dépôt Wazuh :

```
sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list
apt update
```

3. Cluster initialization

Exécutez le script **indexer-security-init.sh** de l'indexeur Wazuh sur n'importe quel nœud de l'indexeur Wazuh pour charger les nouvelles informations des certificats et démarrer le cluster en mode nœud unique ou multi-nœuds.

```
/usr/share/wazuh-indexer/bin/indexer-security-init.sh
```

Essayons ensuite de nous connecter :

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

Après connexion via 'admin' 'admin' vous aurez un retour comme ceci :


```
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "095jEW-oRJSFKLz5wmo5PA",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
    "build_date" : "2023-06-03T06:24:25.112415503Z",
    "build_snapshot" : false,
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

4. Wazuh serveur

1. Installation et configuration du serveur Wazuh en mode mono-nœud ou cluster multi-nœuds

Suivez ces instructions étape par étape pour installer et configurer le serveur Wazuh en tant que nœud unique ou en cluster multi-nœuds. Le serveur Wazuh est un composant central qui comprend le **gestionnaire Wazuh** et **Filebeat**.

- **Le gestionnaire Wazuh** collecte et analyse les données des agents Wazuh déployés. Il déclenche des alertes en cas de détection de menaces ou d'anomalies.
- **Filebeat** transfère en toute sécurité les alertes et les événements archivés vers l'indexeur Wazuh.

Processus d'installation

L'installation est divisée en deux étapes principales :

1. **Installation du nœud du serveur Wazuh**
2. **Configuration du cluster pour un déploiement multi-nœuds**

> **Remarque**
> **Vous devez avoir les privilèges root pour exécuter toutes les commandes décrites ci-dessous.`**

1. Installation du nœud du serveur Wazuh

Ajout du dépôt Wazuh

> **Remarque**
> Si vous installez le serveur Wazuh sur le même hôte que l'indexeur Wazuh, vous pouvez ignorer cette étape, car le dépôt Wazuh pourrait déjà être ajouté.

1. Téléchargeons nos paquets :

```
apt-get install gnupg apt-transport-https curl
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
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
apt-get update
```

2. Nous pouvons ensuite installer wazuh-manager et filebeat:

```
apt-get -y install wazuh-manager
apt-get -y install filebeat
```

> ### *Qu'est-ce que Filebeat ?*
>
> ***Filebeat** est un expéditeur léger de logs (log shipper) développé par **Elastic**. Il est utilisé pour **collecter, traiter et transférer des journaux** depuis différentes sources vers une destination, comme **Elasticsearch**, **Logstash**, ou d'autres systèmes de stockage et d'analyse.*
>
> *Dans le cas de **Wazuh**, **Filebeat joue un rôle essentiel** :*
>
> - *Il récupère **les alertes et les événements archivés** du gestionnaire Wazuh.*
> - *Il **les transmet en toute sécurité** à l'indexeur Wazuh (basé sur OpenSearch ou Elasticsearch).*
> - *Il garantit **une transmission fiable** des logs, même en cas de panne temporaire.*

Configuration de Filebeat pour Wazuh :

1. Installons désormais la pré configuration de filebeat :

```
curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.10/tpl/wazuh/filebeat/filebeat.yml
```

1. Modifier le fichier de configuration Filebeat

Éditez le fichier de configuration `/etc/filebeat/filebeat.yml` et remplacez la valeur des hôtes (**hosts**) comme suit :

- **Définir les nœuds de l’indexeur Wazuh**
  Vous pouvez utiliser soit des **adresses IP**, soit des **noms d’hôte**.
  Par défaut, l’hôte est **localhost** (`127.0.0.1:9200`). Remplacez cette valeur par l'adresse de votre indexeur Wazuh.
- **Si vous avez plusieurs nœuds d’indexation**, séparez les adresses par des virgules :

```
# Wazuh - Configuration de Filebeat
output.elasticsearch:
  hosts: ["10.0.0.1:9200", "10.0.0.2:9200", "10.0.0.3:9200"]
  protocol: https
  username: ${username}
  password: ${password}
```

2. Sécuriser les identifiants avec un keystore Filebeat

Créez un **keystore** Filebeat pour stocker les identifiants d’authentification de manière sécurisée :

```
filebeat keystore create
```

Ajoutez le **nom d’utilisateur et le mot de passe** par défaut (`admin:admin`) au keystore sécurisé :

```
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin --force
```

3. Télécharger le modèle d’alertes pour l’indexeur Wazuh

Exécutez la commande suivante pour télécharger le fichier **wazuh-template.json**, qui est utilisé pour structurer les alertes dans l’indexeur Wazuh :

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.10.1/extensions/elasticsearch/7.x/wazuh-template.json
```

Donnez les **autorisations de lecture** pour que Filebeat puisse l’utiliser :

```
chmod go+r /etc/filebeat/wazuh-template.json
```

4. Installer le module Wazuh pour Filebeat

Le module Wazuh permet à **Filebeat** de récupérer correctement les alertes du gestionnaire Wazuh.

Installez-le avec la commande suivante :

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

5. Redémarrer Filebeat

Une fois la configuration terminée, redémarrez **Filebeat** pour appliquer les modifications :

```
systemctl restart filebeat
systemctl status filebeat
```

> **Filebeat est maintenant configuré pour envoyer les alertes Wazuh à votre indexeur Wazuh !**

2 : Déploiement des certificats et configuration de la connexion à l’indexeur Wazuh

1. Déploiement des certificats

> **Remarque**
> Assurez-vous qu'une copie du fichier `wazuh-certificates.tar`, créé lors de l’étape initiale de configuration, est placée dans votre répertoire de travail.

1. **Remplacez** `<SERVER_NODE_NAME>` par le nom du certificat de votre serveur Wazuh. Ce nom doit être le même que celui utilisé dans `config.yml` lors de la création des certificats.
2. **Déplacez les certificats dans leurs emplacements correspondants** :

```
NODE_NAME=<SERVER_NODE_NAME>


# Créer le répertoire des certificats pour Filebeat
mkdir /etc/filebeat/certs
```

```
# Extraire uniquement les certificats nécessaires depuis l'archive
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem

# Renommer les certificats pour qu'ils correspondent à Filebeat
mv -n /etc/filebeat/certs/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem

# Sécuriser les permissions des certificats
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/*

# Définir le propriétaire des fichiers comme root
chown -R root:root /etc/filebeat/certs
```

2. Configuration de la connexion à l’indexeur Wazuh

> **Remarque**
> Vous pouvez ignorer cette étape si vous **n'utilisez pas** la fonctionnalité de détection des vulnérabilités.

1. **Enregistrez les identifiants de connexion à l’indexeur dans le keystore de Wazuh** :

```
echo '<INDEXER_USERNAME>' | /var/ossec/bin/wazuh-keystore -f indexer -k username
echo '<INDEXER_PASSWORD>' | /var/ossec/bin/wazuh-keystore -f indexer -k password
```

> **Remarque**
> Lors d’une installation standard, les identifiants par défaut sont :
> **Utilisateur :** `admin`
> **Mot de passe :** `admin`

---

3. Modification du fichier de configuration `ossec.conf`

Éditez le fichier **`/var/ossec/etc/ossec.conf`** pour configurer la connexion à l’indexeur Wazuh.

- **Par défaut**, la configuration de l’indexeur est définie avec une seule adresse `0.0.0.0`, comme indiqué ci-dessous :

```
<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://0.0.0.0:9200</host>
  </hosts>
  <ssl>
    <certificate_authorities>
      <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificate_authorities>
    <certificate>/etc/filebeat/certs/filebeat.pem</certificate>
    <key>/etc/filebeat/certs/filebeat-key.pem</key>
  </ssl>
</indexer>
```

- **Remplacez** `0.0.0.0` par **l'adresse IP ou le nom d’hôte de votre nœud d’indexeur Wazuh**.
  Vous pouvez trouver cette valeur dans le fichier de configuration Filebeat **`/etc/filebeat/filebeat.yml`**.

4. Configuration en mode cluster multi-nœuds

Si vous utilisez **un cluster d'indexeurs Wazuh**, ajoutez une entrée `<host>` pour chaque nœud :

```
<hosts>
  <host>https://10.0.0.1:9200</host>
  <host>https://10.0.0.2:9200</host>
</hosts>
```

> **Remarque**
> La **détection des vulnérabilités** privilégie le premier nœud de la liste pour l’envoi des rapports.
> Si ce nœud n'est pas disponible, Wazuh passe automatiquement au suivant.

La connexion sécurisée entre Filebeat et l’indexeur Wazuh est maintenant configurée !

3. Démarrage du gestionnaire Wazuh et de Filebeat

1. Démarrer le gestionnaire Wazuh

Activez et démarrez le service **Wazuh Manager** avec les commandes suivantes :

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

Vérifiez ensuite son statut pour vous assurer qu'il fonctionne correctement :

```
systemctl status wazuh-manager
```

2. Démarrer le service Filebeat

Activez et démarrez le service **Filebeat** :

```
systemctl daemon-reload
systemctl enable filebeat
systemctl start filebeat
```

Vérifiez que Filebeat est correctement installé et qu'il peut se connecter à l'indexeur Wazuh :

```
filebeat test output
```

3. Vérification de la connexion Filebeat - Wazuh Indexer

L'exécution de la commande précédente devrait afficher une réponse semblable à celle-ci :

```
elasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
```

```
  security: server's certificate chain verification is enabled
  handshake... OK
  TLS version: TLSv1.3
  dial up... OK
talk to server... OK
version: 7.10.2
```

> Si vous obtenez une sortie similaire, cela signifie que **Filebeat est bien connecté à l'indexeur Wazuh** et que tout fonctionne correctement.

4. Finalisation de l’installation du serveur Wazuh

Votre nœud serveur Wazuh est maintenant installé avec succès !

Si vous utilisez **un cluster Wazuh multi-nœuds**, **répétez cette étape pour chaque nœud serveur Wazuh** avant de passer à la configuration du cluster.

Si vous souhaitez un **serveur Wazuh en mode mono-nœud**, l’installation est terminée et vous pouvez **passer directement à l’installation du Wazuh Dashboard**.

5. Désactiver les mises à jour automatiques de Wazuh (recommandé)

> **Remarque :**
> Nous **recommandons de désactiver les mises à jour automatiques** des paquets Wazuh après l'installation.
> Cela évite **les mises à jour accidentelles** qui pourraient causer des problèmes de compatibilité.

Désactivez les mises à jour automatiques du dépôt Wazuh avec la commande suivante :

```
sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list
apt update
```

> **Votre serveur Wazuh est maintenant prêt à l’emploi ! **
> Vous pouvez maintenant passer à l’**installation du Wazuh Dashboard** pour une gestion et une visualisation centralisée.