

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
```