[Date]

Mise en place de Wazuh (Debian)

SIEM

Mamadou CAMARA
[NOM DE LA SOCIETE]

SOMMAIRE

1. Présentation : 2

2. Indexeur Wazuh 2

2.1 Installation de l'indexeur Wazuh à l'aide de la méthode d'installation ssistée 2

2.2 Installation du cluster d'indexation Wazuh 2

2.2.1 Configuration initiale 2

2.2.2 Installation des nœuds d'indexation Wazuh 3

2.2.3 Initialisation du cluster 4

2.2.4 Test de l'installation du cluster 4

3. Serveur Wazuh 6

3.1 Installation du serveur Wazuh à l'aide de la méthode d'installation assistée 6

3.1.1 Installation du cluster de serveurs Wazuh 6

4. Tableau de bord Wazuh 6

4.1 Installation du tableau de bord Wazuh à l'aide de la méthode d'installation assistée 6

4.1.1 Installation du tableau de bord Wazuh 6

5. Interface Graphique : 9

6. Agent wazuh sur les client Linux 10

A. Ajoutez le référentiel Wazuh pour télécharger les packages officiels. 10

B. Déployer un agent Wazuh 10

b1. Activez et démarrez le service agent Wazuh 11

1. Présentation :

Wazuh est une plateforme de sécurité SI tout-en-un, open source et puissante, conçue pour protéger les organisations contre les menaces cybernétiques. Elle se distingue par plusieurs fonctionnalités essentielles :

- **Détection d'Intrusions (IDS/IPS)**
- **Corrélation des Événements**
- **Analyse des Logs**
- **Gestion de Vulnérabilités**
- **Conformité et Rapports**
- **Extensibilité et Intégrations**

2. Indexeur Wazuh

L'indexeur Wazuh est un moteur de recherche et d'analyse plein texte hautement évolutif. Ce composant central de Wazuh indexe et stocke les alertes générées par le serveur Wazuh et offre des capacités de recherche et d'analyse de données en temps quasi réel.

2.1 Installation de l'indexeur Wazuh à l'aide de la méthode d'installation ssistée

Nous allons installer et configurer l'indexeur Wazuh en cluster mono-nœud sur une architecture 64 bits (x86_64/AMD64) grâce à la méthode d'installation assistée.

2.2 Installation du cluster d'indexation Wazuh

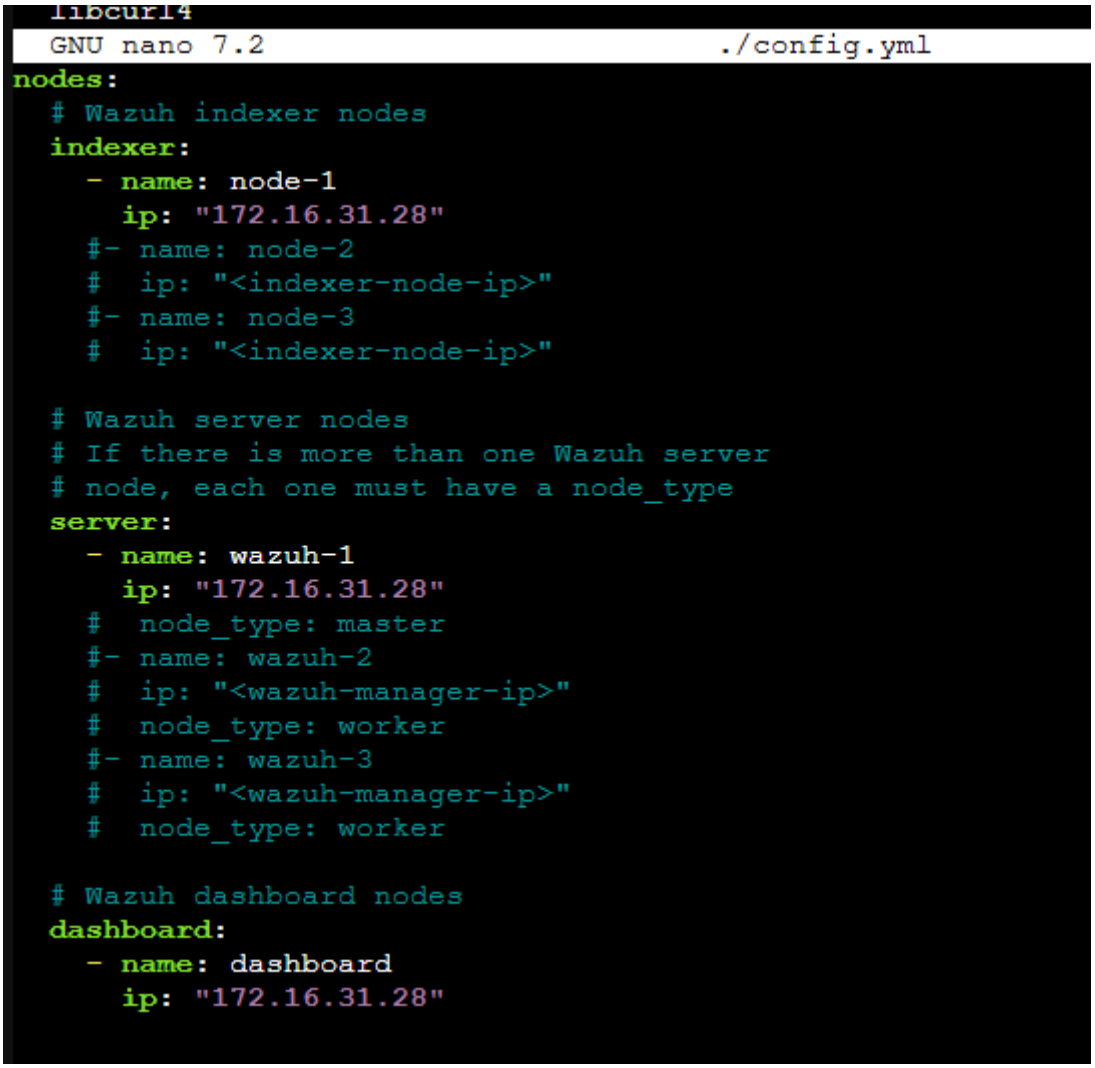
2.2.1 Configuration initiale

Indiquez votre configuration de déploiement, créez les certificats SSL pour crypter les communications entre les composants Wazuh et générez des mots de passe aléatoires pour sécuriser votre installation.

- Téléchargez l'assistant d'installation Wazuh et le fichier de configuration.

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.11/config.yml
```

- Modifiez ./config.yml et remplacez les noms et les adresses IP des nœuds par les noms et adresses IP correspondants. Cette opération est nécessaire pour tous les nœuds du serveur Wazuh, de l'indexeur Wazuh et du tableau de bord Wazuh. Ajoutez autant de champs de nœud que nécessaire.



- Exécutez l'assistant d'installation de Wazuh avec l'option --generate-config-files permettant de générer la clé de cluster, les certificats et les mots de passe Wazuh nécessaires à l'installation. Ces fichiers se trouvent dans ./wazuh-install-files.tar.

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

2.2.2 Installation des nœuds d'indexation Wazuh

Installez et configurez les nœuds d'indexation Wazuh.

- Téléchargez l'assistant d'installation de Wazuh.

  ```
  curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
  ```

- Exécutez l'assistant d'installation de Wazuh avec l'option --wazuh-indexer et le nom du nœud pour installer et configurer l'indexeur Wazuh. Le nom du nœud doit

être identique à celui utilisé lors config.yml de la configuration initiale, par exemple node-1

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

2.2.3 Initialisation du cluster

L'étape finale de l'installation du cluster à nœud unique de l'indexeur Wazuh consiste à exécuter le script d'administration de sécurité.

- Exécutez l'assistant d'installation Wazuh avec l'option --start-cluster sur n'importe quel nœud d'indexation Wazuh pour charger les nouvelles informations de certificats et démarrer le cluster

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

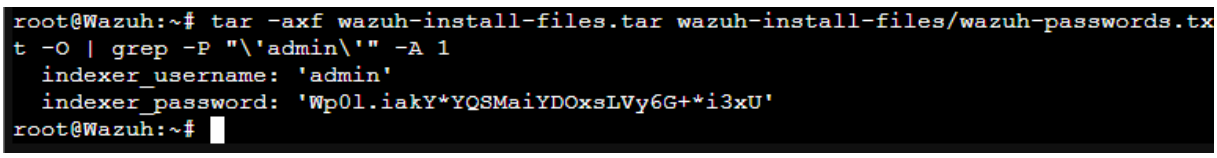
2.2.4 Test de l'installation du cluster

Exécutez la commande suivante pour obtenir le mot de passe *administrateur* :

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

Sortie :

```
indexer_username: 'admin'

 indexer_password: 'Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU'
```



Exécutez la commande suivante pour confirmer la réussite de l'installation. Remplacez- <ADMIN_PASSWORD> par le mot de passe obtenu à partir de la sortie de la commande précédente. Remplacez <WAZUH_INDEXER_IP> par l'adresse IP configurée de l'indexeur Wazuh

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

root@Wazuh:~# curl -k -u admin:Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU https://172.16.31.30:9200


```
{
 "name" : "node-1",
 "cluster_name" : "wazuh-indexer-cluster",
 "cluster_uuid" : "wiTTj681SD-aT1e7Ft9Spg",
 "version" : {
  "number" : "7.10.2",
  "build_type" : "deb",
  "build_hash" : "8f728199af83591b03e787621cb12b1e3437ae90",
  "build_date" : "2025-02-14T14:08:33.049199Z",
  "build_snapshot" : false,
  "lucene_version" : "9.11.1",
  "minimum_wire_compatibility_version" : "7.10.0",
  "minimum_index_compatibility_version" : "7.0.0"
 },
 "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```


```
root@Wazuh:~# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'admin\'" -A 1
  indexer_username: 'admin'
  indexer_password: 'Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU'
root@Wazuh:~# curl -k -u admin:Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU https://172.16.31.30:
9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "wiTTj681SD-aT1e7Ft9Spg",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "8f728199af83591b03e787621cb12b1e3437ae90",
    "build_date" : "2025-02-14T14:08:33.049199Z",
    "build_snapshot" : false,
    "lucene_version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
root@Wazuh:~# curl -k -u admin:Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU https://172.16.31.30:
9200/_cat/nodes?v
ip           heap.percent ram.percent cpu load_1m load_5m load_15m node.role node.roles                              cluster_manager name
172.16.31.30           63          99  38   24.65   21.61    24.64 dimr      data,ingest,master,remote_cluster_client *               node-1
root@Wazuh:~#
```

3. Serveur Wazuh

Le serveur Wazuh analyse les données reçues des agents Wazuh et déclenche des alertes en cas de détection de menaces ou d'anomalies. Il permet également de gérer à distance la configuration des agents et de surveiller leur état.

3.1 Installation du serveur Wazuh à l'aide de la méthode d'installation assistée

3.1.1 Installation du cluster de serveurs Wazuh

- Exécutez l'assistant d'installation de Wazuh avec l'option –wazuh-server suivie du nom du nœud pour installer le serveur Wazuh. Le nom du nœud doit être identique à celui utilisé lors config.yml de la configuration initiale, par exemple wazuh-1.

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

4. Tableau de bord Wazuh

4.1 Installation du tableau de bord Wazuh à l'aide de la méthode d'installation assistée

4.1.1 Installation du tableau de bord Wazuh

- Téléchargez l'assistant d'installation de Wazuh. Vous pouvez ignorer cette étape si vous avez déjà installé l'indexeur Wazuh sur le même serveur

```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
```

- Exécutez l'assistant d'installation de Wazuh avec l'option --wazuh-dashboard et le nom du nœud pour installer et configurer le tableau de bord Wazuh. Le nom du nœud doit être identique à celui utilisé lors config.yml de la configuration initiale, par exemple dashboard.

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

Le port par défaut de l'interface utilisateur Web Wazuh est le 443, utilisé par le tableau de bord Wazuh. Vous pouvez modifier ce port à l'aide du paramètre facultatif . Les ports 8443, 8444, 8080, 8888 et 9000 sont recommandés.-p|--port <PORT_NUMBER>

Une fois l'installation de Wazuh terminée, la sortie affiche les informations d'identification d'accès et un message confirmant que l'installation a réussi.

```
INFO: --- Summary ---

INFO: You can access the web interface https://<WAZUH_DASHBOARD_IP_ADDRESS>

  User: admin

  Password: <ADMIN_PASSWORD>


INFO: Installation finished.
```

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

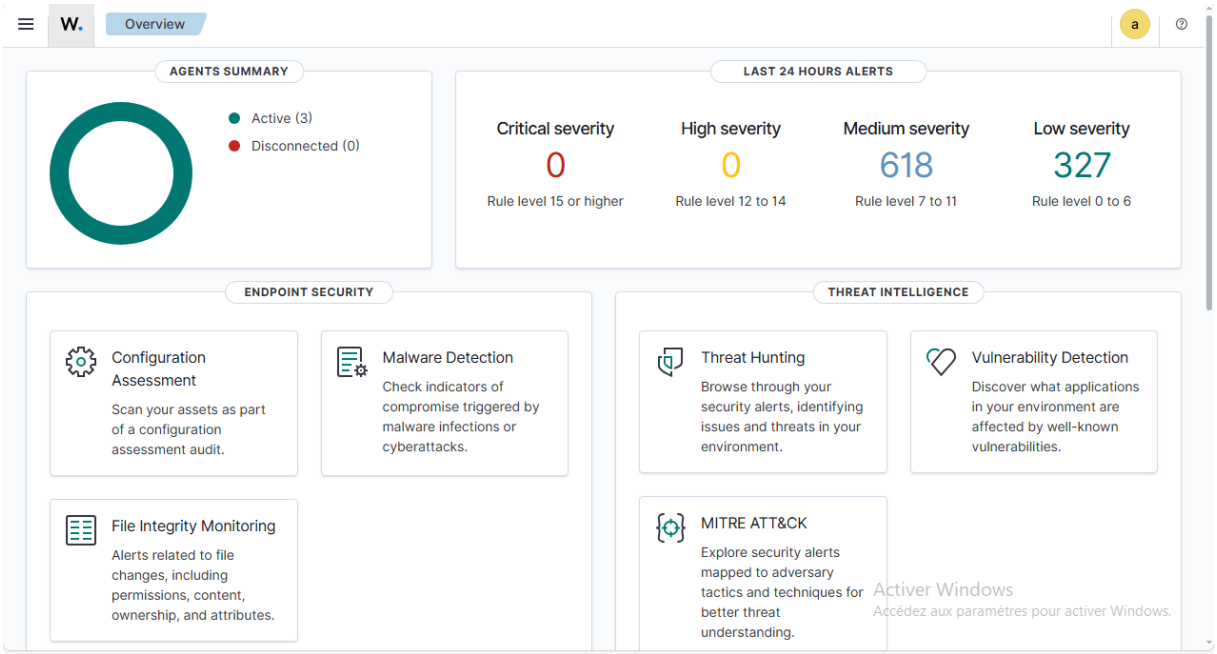
```
tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

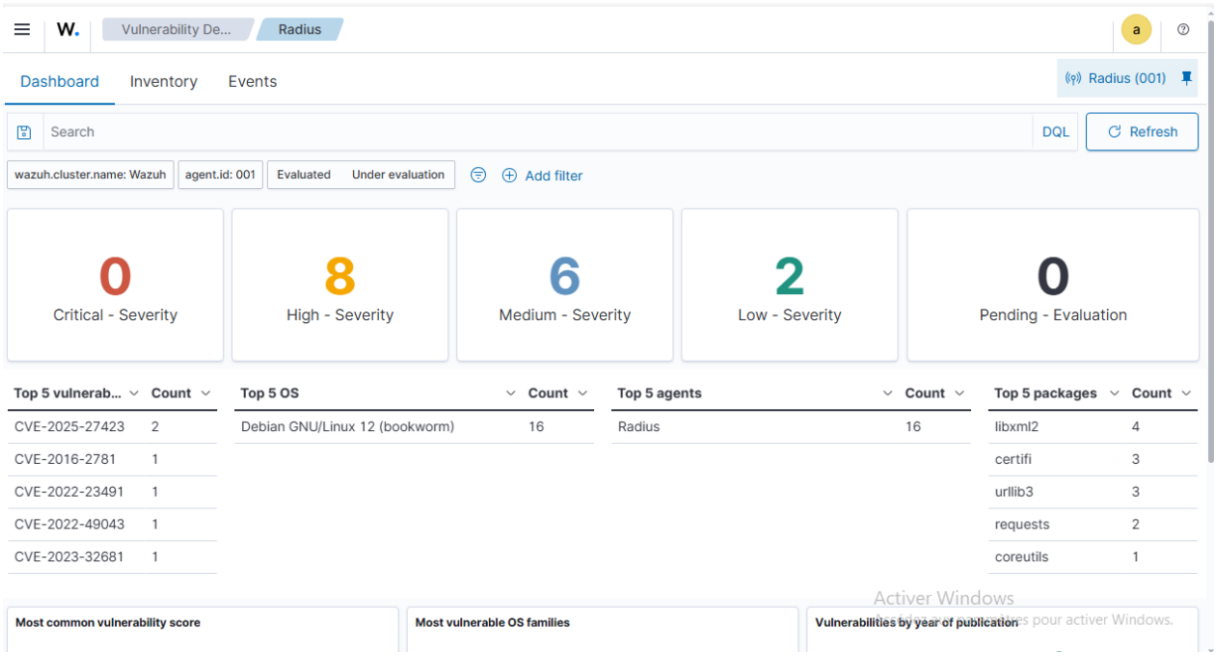
```
root@Wazuh:~# tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt

wazuh-install-files/wazuh-passwords.txt

# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard

  indexer_username: 'admin'

  indexer_password: 'Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU'


# Anomaly detection user for the web user interface

  indexer_username: 'anomalyadmin'

  indexer_password: 'Tz?EKw0UFzJh3Ynt*4Zqj6q95xh2qhKh'


# Wazuh dashboard user for establishing the connection with Wazuh indexer

  indexer_username: 'kibanaserver'

  indexer_password: 'CE*RuwscAoCJ2Q79W+4uN2*Ov5Sww8g9'
```

```
# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: '*2Q8G*uy5r?0j**0r*qJUT*lKn0HSzPM'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: 'an.NOJCB3Y4U5n+1km4e?cm9RgucXBLx'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: 'eAnhVZzRM2YA22A6HQgG3OASy97+.d??'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: '3jlPKroVnuztP3ccQ2psf+Y*0I8wBzF1'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: 'aTz0O?Gb*b7?6Hg8eC86Fj9uA9wEa+Nv'

# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
  api_password: 'Lx8*VJ43II4rB1.v1DOIIX3ffsen6Lg4'

root@Wazuh:~#
```

```
root@Wazuh:~# tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: 'Wp0l.iakY*YQSMaiYDOxsLVy6G+*i3xU'

# Anomaly detection user for the web user interface
  indexer_username: 'anomalyadmin'
  indexer_password: 'Tz?EKw0UFzJh3Ynt*4Zqj6q95xh2qhKh'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: 'CE*RuwscAoCJ2Q79W+4uN2*Ov5Sww8g9'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: '*2Q8G*uy5r?0j**0r*qJUT*lKn0HSzPM'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: 'an.NOJCB3Y4U5n+1km4e?cm9RgucXBLx'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: 'eAnhVZzRM2YA22A6HQgG3OASy97+.d??'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: '3jlPKroVnuztP3ccQ2psf+Y*0I8wBzF1'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: 'aTz0O?Gb*b7?6Hg8eC86Fj9uA9wEa+Nv'

# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
  api_password: 'Lx8*VJ43II4rB1.v1DOIIX3ffsen6Lg4'

root@Wazuh:~#
```

5. Interface Graphique :





6. Agent wazuh sur les client Linux

A. Ajoutez le référentiel Wazuh pour télécharger les packages officiels.

- Installer la clé 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
```

- Ajouter le référentiel :

```
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
```

- Mettre à jour les informations du package :

```
apt-get update
```

B. Déployer un agent Wazuh

```
root@ns0:~# WAZUH_MANAGER="172.16.31.30" apt-get install wazuh-agent^C
root@ns0:~# WAZUH_MANAGER="172.16.31.30" apt-get install wazuh-agent
```

```
deb https://packages.wazuh.com/4.x/apt/ stable main
root@ns0:~# WAZUH_MANAGER="172.16.31.30" apt-get install wazuh-agent
E: Conflicting values set for option Signed-By regarding source https://packages.wazuh.com/4.x/apt/ stable: /usr/share/keyring
s/wazuh.gpg !=
E: The list of sources could not be read.
root@ns0:~#
```

Solution

sudo rm -f /usr/share/keyrings/wazuh.gpg

sudo rm -f /etc/apt/sources.list.d/wazuh.list

b1. Activez et démarrez le service agent Wazuh

systemctl daemon-reload

systemctl enable wazuh-agent

systemctl start wazuh-agent