

Installation d'un SIEM - Wazuh Server

Introduction :

L'installation de Wazuh se fait en installant ses 3 composants principaux :

- Wazuh Server : Il s'agit du système qui analyse toutes les données qu'il reçoit via les agents et qui déclenche les alertes.
- Wazuh Indexer : Il s'occupe comme son nom l'indique d'indexer et d'analyser en temps réel les données transmises par le composant Wazuh Server pour ensuite pouvoir être facilement récupéré par le dernier composant suivant. L'indexer stocke les data sous forme de documents JSON et sont associés avec des clés, des noms et des attributs pour pouvoir trier et chercher plus facilement les données qui nous intéressent.
- Wazuh Dashboard : Le dernier composant est donc le dashboard qui est une interface Web utile à la visualisation de data et d'analyse par un opérateur humain. Il est basé sur Kibana, qui est une partie de la stack très connue Elastik (ELK). Il se base sur les documents préalablement triés par l'indexeur.

Schéma explicatif :

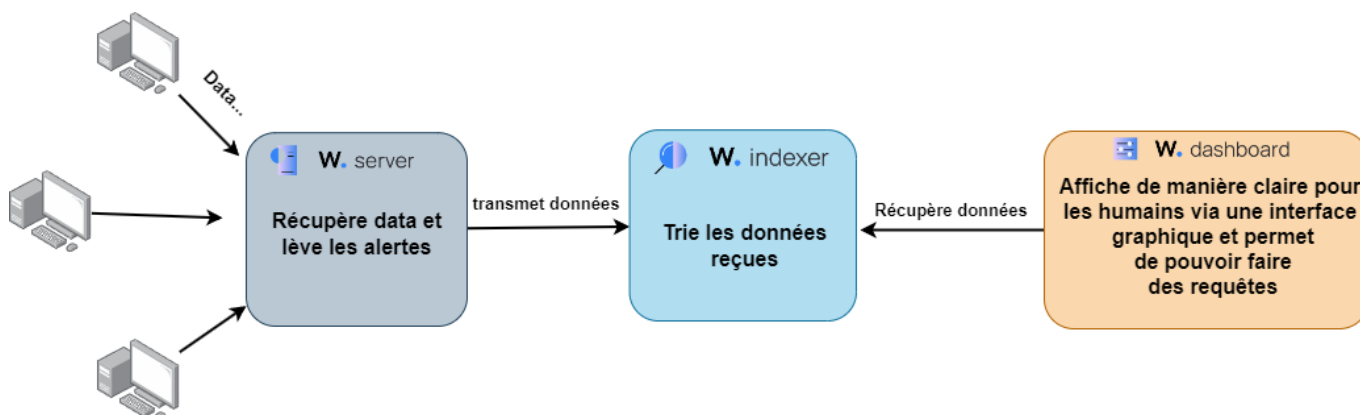


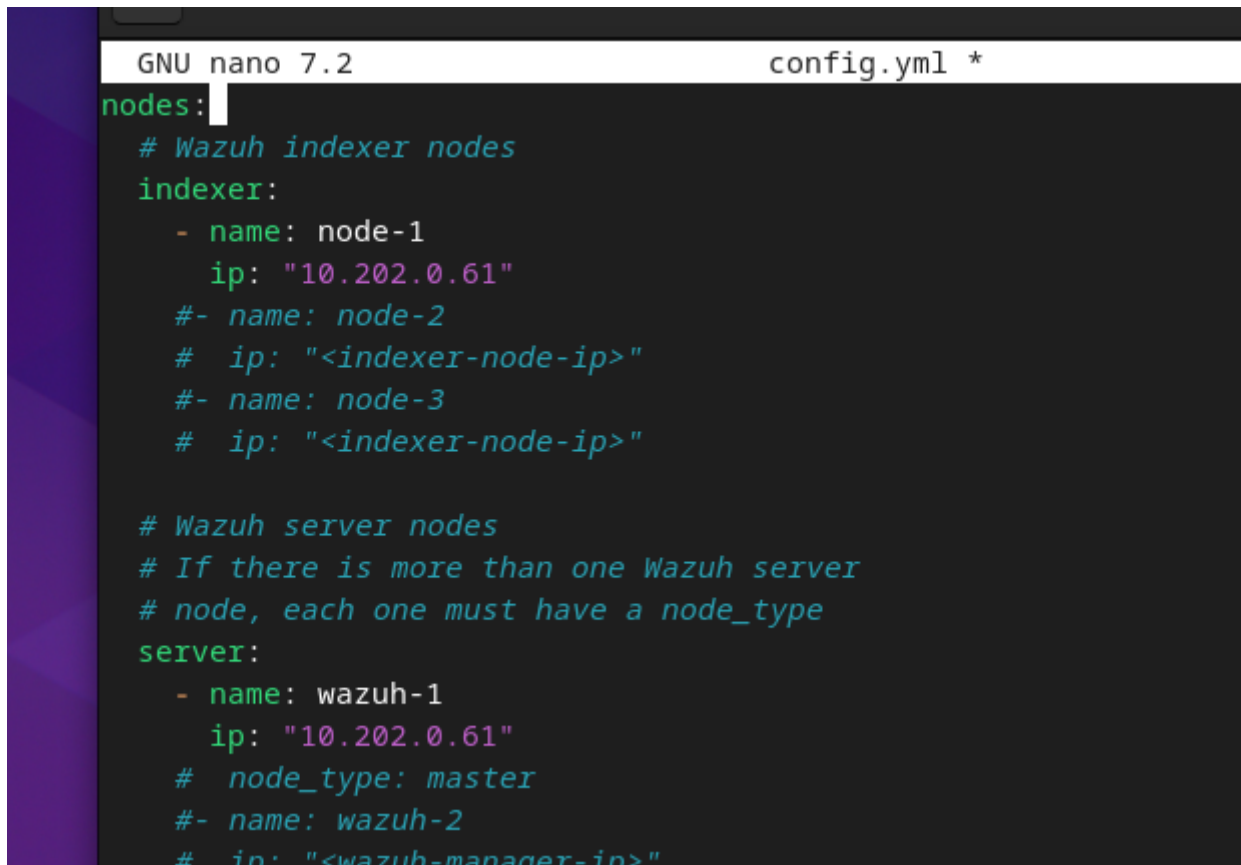
Schéma très bien fait, parce que c'est moi qui l'ai fait

Installation sur un Debian 12 :

L'installation va donc s'effectuer en installant les 3 composants un par un, en commençant par le Wazuh Indexer comme ceci :

```
apt install -y curl sudo && mkdir wazuh && cd wazuh && curl -sO
https://packages.wazuh.com/4.6/wazuh-install.sh && curl -sO
https://packages.wazuh.com/4.6/config.yml && nano config.yml
```

Dans le fichier de configuration, on rentre les IP de notre serveur :

A screenshot of a terminal window with a dark background and light-colored text. The window title is "GNU nano 7.2" and the file being edited is "config.yml *". The content of the file is a YAML configuration for Wazuh nodes and servers. It includes comments in French and configuration details for an indexer and a server. The configuration is as follows:

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "10.202.0.61"
    #- 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: "10.202.0.61"
      # node_type: master
    #- name: wazuh-2
    # ip: "<wazuh-manager-ip>"
```

On peut ensuite lancer le script d'auto-configuration et création des certificats avec le script fourni par Wazuh :

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

On peut ensuite lancer l'assistant d'installation :

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

On peut terminer par lancer l'installation du Cluster :

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

On récupère le mot de passe admin généré précédemment :

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

On peut tester la connexion soit avec un navigateur, soit directement avec l'utilitaire Curl :

```
curl -k -u admin:MDP https://IP:9200
```

```
root@Wazuh-Serv:~/wazuh/wazuh# curl -k -u admin:x66RYlrx?fxAAjzy5Xwv6Hk3Y+U4x.RQ https://10.202.0.98:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "yDxDCKLjRda1EiZAP05Dvg",
  "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/"
}
root@Wazuh-Serv:~/wazuh/wazuh#
```

Une réponse valide quand l'installation fonctionne.

On peut maintenant lancer l'installation du composant Wazuh Server :

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

Puis on peut lancer l'installation du dashboard :

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

On peut récupérer les mots de passes générés avec la commande suivante :

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

Puis aller sur notre nouveau dashboard généré :

```
firefox https://IP/
```

wazuh.

Modules

Total agents

0

Active agents

0

Disconnected agents

0

Pending agents

0

Never connected agen

0

No agents were added to this manager. [Add agent](#)

SECURITY INFORMATION MANAGEMENT

Security events

Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring

Verify that your systems are configured according to your security policies baseline.

Security configuration assessment

Scan your assets as part of a configuration assessment audit.

Syst

Audit execu

4 / 4