Thierno Cherif HANE

Mise en place d'une solution de sécurité avec Wazuh sur Debian

Réalisé par :

Thierno Cherif HANE

Encadré par :

Mr Massamba LO

thane@groupeisi.com

Thierno Cherif HANE

PLAN DU PROJET : Mise en place d'une solution de sécurité avec Wazuh

I. Introduction

- Présentation du projet
- Objectifs du projet
- Technologies utilisées

II. Présentation des outils

- Wazuh : Manager, Agents, Dashboard
- Debian : système pour le serveur
- Windows et Linux : clients pour les tests de surveillance

III. Configuration du serveur Wazuh sur Debian

- Étape 1 : Mise à jour du système
- Étape 2 : Génération des certificats
- Étape 3 : Ajout de la clé GPG
- Étape 4 : Installation des composants Wazuh
- Étape 5 : Vérification de l'indexeur
- Étape 6 : Configuration de Filebeat
- Étape 7 : Ajout du template et du module Wazuh
- Étape 8 : Sécurisation des identifiants Filebeat
- Étape 9 : Démarrage et test de Filebeat
- Accès au Dashboard

IV. Ajout et configuration des agents

A. Agent Linux

- Ajout de la clé GPG
- Ajout du dépôt
- Mise à jour et installation
- Activation et démarrage du service

B. Agent Windows

- Téléchargement et installation de l'agent

thane@groupeisi.com

- Ajout de l'agent via le manager (manage_agents)
- Configuration du client avec l'IP du manager et la clé
- Démarrage du service

V. Conclusion

Thierno Cherif HANE

I. Introduction

❖ Présentation du projet

Ce projet consiste à mettre en place une solution de sécurité avec la plateforme **Wazuh**, installée sur un serveur **Debian**. Deux ordinateurs (un sous **Linux** et un autre sous **Windows**) sont connectés au serveur grâce à l'installation d'agents Wazuh pour permettre leur surveillance.

❖ Objectifs du projet

- Surveiller en temps réel les activités des deux machines clientes.
- Centraliser la collecte des journaux système (logs), des fichiers et des processus.
- Détecter les tentatives d'intrusion grâce aux alertes générées automatiquement par Wazuh.

❖ Technologies utilisées

- **Wazuh** : outil de surveillance, d'analyse de journaux et de détection d'intrusions.
- **Debian** : système d'exploitation utilisé pour installer le serveur principal (Wazuh Manager).
- **Windows et Linux** : systèmes d'exploitation utilisés sur les deux machines clientes pour tester les agents Wazuh.

II. Présentation des outils

➢ Wazuh

Wazuh est une plateforme de sécurité libre (open source) qui permet de surveiller des systèmes informatiques en temps réel. Elle est composée de trois éléments principaux :

- **Wazuh Manager** : il s'agit du cœur du système qui reçoit, analyse et stocke les données envoyées par les machines clientes.
- **Agents Wazuh** : installés sur les ordinateurs à surveiller, ils envoient les journaux d'activité au manager.
- **Dashboard** : une interface web qui permet de visualiser les alertes, les statistiques et les événements de manière claire.

➢ Debian (serveur)

Debian est un système d'exploitation Linux utilisé ici pour faire tourner le serveur Wazuh. Il est réputé pour sa stabilité, sa sécurité, et son efficacité dans les environnements professionnels. Toutes les étapes de configuration ont été réalisées sous Debian.

thane@groupeisi.com

- **Windows et Linux (clients)**

Ces deux systèmes ont été choisis pour représenter différents environnements de travail :

- **Client Linux** : pour tester la surveillance des systèmes basés sur Unix.
- **Client Windows** : pour voir comment Wazuh gère les événements propres à l'environnement Windows (comme les journaux système et le registre).

III. Configuration du serveur Wazuh sur Debian

ÉTAPE 1 : Préparation du système

apt update -y

Met à jour la liste des paquets pour s'assurer que le système est prêt.

```
root@debian11:~# apt update -y
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
root@debian11:~# apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian11:~#
```

ÉTAPE 2 : Préparation des certificats de sécurité

curl -sO https://packages.wazuh.com/4.12/wazuh-certs-tool.sh

curl -sO https://packages.wazuh.com/4.12/config.yml

vim config.yml

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

tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .

rm -rf ./wazuh-certificates

Ces commandes font :

- Le téléchargement du script et du fichier de configuration.
- L'édition de config.yml pour renseigner les IP/noms.
- La génération des certificats pour tous les composants.

Thierno Cherif HANE

- L'archivage et nettoyage des fichiers générés.

```
root@debian11:~# curl -sO https://packages.wazuh.com/4.12/wazuh-certs-tool.sh
root@debian11:~# curl -sO https://packages.wazuh.com/4.12/config.yml
root@debian11:~#
```

```
       valid_lft forever preferred_lft
root@debian11:~# vim config.yml
root@debian11:~#
```

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "<192.168.1.1>"
    #- 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: "<192.168.1.1>"
    #  node_type: master

    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "<192.168.1.1>"
~
```

```
root@thierno:~# bash ./wazuh-certs-tool.sh -A
26/06/2025 16:35:01 INFO: Verbose logging redirected to /root/wazuh-certificates
-tool.log
26/06/2025 16:35:01 INFO: Generating the root certificate.
26/06/2025 16:35:01 INFO: Generating Admin certificates.
26/06/2025 16:35:02 INFO: Admin certificates created.
26/06/2025 16:35:02 INFO: Generating Wazuh indexer certificates.
26/06/2025 16:35:02 INFO: Wazuh indexer certificates created.
26/06/2025 16:35:02 INFO: Generating Filebeat certificates.
26/06/2025 16:35:02 INFO: Wazuh Filebeat certificates created.
26/06/2025 16:35:02 INFO: Generating Wazuh dashboard certificates.
26/06/2025 16:35:03 INFO: Wazuh dashboard certificates created.
root@thierno:~#
```

```
root@thierno:~# tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
./
./wazuh-1-key.pem
./admin-key.pem
./node-1.pem
./admin.pem
./root-ca.key
./node-1-key.pem
./dashboard-key.pem
./dashboard.pem
./root-ca.pem
./wazuh-1.pem
```

thane@groupeisi.com

```
root@thierno:~# rm -rf ./wazuh-certificates
root@thierno:~#
```

ÉTAPE 3 : Ajout de la clé GPG Wazuh

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

Permet de vérifier l'authenticité des paquets téléchargés via APT.

```
root@thierno:~# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-
default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && c
hmod 644 /usr/share/keyrings/wazuh.gpg
gpg: le porte-clefs « /usr/share/keyrings/wazuh.gpg » a été créé
gpg: répertoire « /root/.gnupg » créé
gpg: /root/.gnupg/trustdb.gpg : base de confiance créée
gpg: clef 96B3EE5F29111145 : clef publique « Wazuh.com (Wazuh Signing Key) <supp
ort@wazuh.com> » importée
gpg:       Quantité totale traitée : 1
gpg:                     importées : 1
root@thierno:~#
```

ÉTAPE 4 : Installation de Wazuh
Ajoute les lignes suivantes :

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

apt update

apt install wazuh-manager wazuh-dashboard wazuh-indexer -y

Installe les 3 composants Wazuh :

- wazuh-manager (le moteur)
- wazuh-dashboard (interface web)
- wazuh-indexer (moteur OpenSearch)

ÉTAPE 5 : Vérification de l'indexer

curl -k -u admin:admin https://10.5.20.12:9200

Vérifie que l'indexeur OpenSearch est bien accessible.

Thierno Cherif HANE

```
oot@thierno:~# curl -k -u admin:admin https://10.5.20.12:9200

 "name" : "node-1",
 "cluster_name" : "wazuh-cluster",
 "cluster_uuid" : "zaMT-uMoTFC3tduMiq36BQ",
 "version" : {
   "number" : "7.10.2",
   "build_type" : "deb",
   "build_hash" : "dae2bfc93896178873b43cdf4781f183c72b238f",
   "build_date" : "2025-04-30T10:51:28.815931460Z",
   "build_snapshot" : false,
   "lucene_version" : "9.12.1",
   "minimum_wire_compatibility_version" : "7.10.0",
   "minimum_index_compatibility_version" : "7.0.0"
 },
 "tagline" : "The OpenSearch Project: https://opensearch.org/"
```

ÉTAPE 6 : Configuration de Filebeat

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.12/tpl/wazuh/filebeat/filebeat.yml

vim /etc/filebeat/filebeat.yml

Télécharge un fichier de configuration prêt à l'emploi et le modifie si besoin.

```
oot@thierno:~# curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4
12/tpl/wazuh/filebeat/filebeat.yml
oot@thierno:~# ls
onfig.yml  direct     isi.ldif                wazuh-certificates-tool.log
levstack   info.ldif  wazuh-certificates.tar  wazuh-certs-tool.sh
oot@thierno:~# vim /etc/filebeat/filebeat.yml
oot@thierno:~# filebeat keystore create
reated filebeat keystore
oot@thierno:~# echo admin | filebeat keystore add username --stdin --force
uccessfully updated the keystore
oot@thierno:~# echo admin | filebeat keystore add password --stdin --force
uccessfully updated the keystore
oot@thierno:~# curl -so /etc/filebeat/wazuh-template.json https://raw.githubuse
content.com/wazuh/wazuh/v4.12.0/extensions/elasticsearch/7.x/wazuh-template.jsc

oot@thierno:~# chmod go+r /etc/filebeat/wazuh-template.json
oot@thierno:~#

oot@thierno:~# vim /etc/filebeat/filebeat.yml
oot@thierno:~#
```

ÉTAPE 7 : Template et module Wazuh pour Filebeat

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-template.json -o /etc/filebeat/wazuh-template.json

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

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

Configure Filebeat pour qu'il comprenne les logs Wazuh correctement.

thane@groupeisi.com

```
root@thierno:~# chmod go+r /etc/filebeat/wazuh-template.json
root@thierno:~# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0
.4.tar.gz | tar -xvz -C /usr/share/filebeat/module
wazuh/
wazuh/alerts/
wazuh/alerts/config/
wazuh/alerts/config/alerts.yml
wazuh/alerts/ingest/
wazuh/alerts/ingest/pipeline.json
wazuh/alerts/manifest.yml
wazuh/module.yml
wazuh/_meta/
wazuh/_meta/docs.asciidoc
wazuh/_meta/config.yml
wazuh/_meta/fields.yml
wazuh/archives/
wazuh/archives/config/
wazuh/archives/config/archives.yml
wazuh/archives/ingest/
wazuh/archives/ingest/pipeline.json
wazuh/archives/manifest.yml
root@thierno:~#
```

ÉTAPE 8 : Sécurisation des identifiants Filebeat

filebeat keystore create

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

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

Crée un keystore sécurisé pour stocker les identifiants d'accès à l'indexeur.

ÉTAPE 9 : Démarrage et test de Filebeat

systemctl start filebeat

filebeat test output

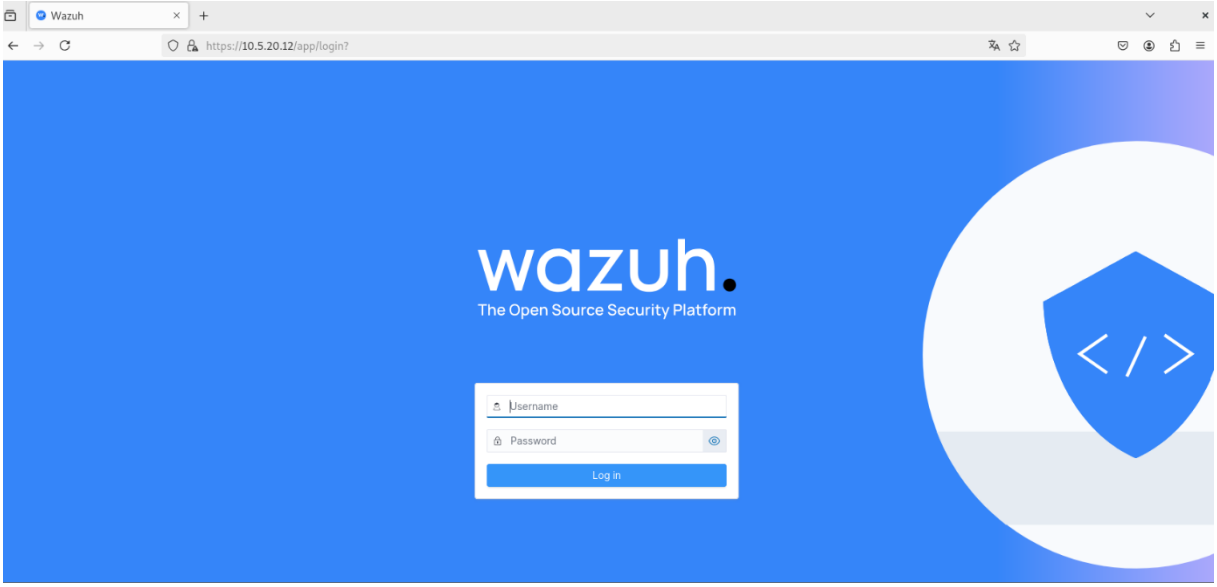
Démarre Filebeat et teste s'il parvient à se connecter à l'indexeur.

```
root@thierno:~# systemctl start filebeat
root@thierno:~# filebeat test output
elasticsearch: https://10.5.20.12:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 10.5.20.12
    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
```

RÉSULTAT FINAL

Thierno Cherif HANE

Accès au tableau de bord via :
https://10.5.20.12/app/login
Identifiants par défaut : admin / admin



IV. Ajout et configuration des agents

A. Agent Linux

Pour permettre la supervision d'une machine Linux depuis le serveur Wazuh, on installe l'**agent Wazuh** sur le poste client. Cet agent collecte les journaux système et les envoie au **manager**

1. Installer la clé GPG du dépôt Wazuh

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

Explication :

- curl -s https://... : télécharge silencieusement la clé GPG.
- gpg --no-default-keyring ... --import : importe cette clé dans un fichier spécifique.
- chmod 644 : donne les bonnes permissions pour que le système puisse l'utiliser.

Cette clé permet de **vérifier que les paquets Wazuh sont authentiques et sûrs**.

2. Ajouter le dépôt APT de Wazuh

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

thane@groupeisi.com

Explication :

- Cette commande ajoute **le dépôt officiel de Wazuh** à la liste des sources APT.
- signed-by=... : indique à APT d'utiliser la clé GPG précédemment installée.
- Le fichier wazuh.list est utilisé pour séparer les sources de manière propre.

3. Mettre à jour la base de données des paquets

apt-get update

Explication :

- Met à jour la liste des paquets disponibles en tenant compte du nouveau dépôt.

4. Installer l'agent Wazuh en spécifiant l'adresse IP du serveur

WAZUH_MANAGER="192.168.1.1" apt-get install wazuh-agent

Explication :

- L'agent est installé via APT.
- La variable WAZUH_MANAGER définit l'**adresse du serveur** à contacter une fois l'agent lancé.

5. Activer et démarrer le service

- systemctl daemon-reload
- systemctl enable wazuh-agent
- systemctl start wazuh-agent

Explication de chaque ligne :

- systemctl daemon-reload : recharge les services après l'installation.
- systemctl enable wazuh-agent : active l'agent au démarrage du système.
- systemctl start wazuh-agent : démarre immédiatement le service.

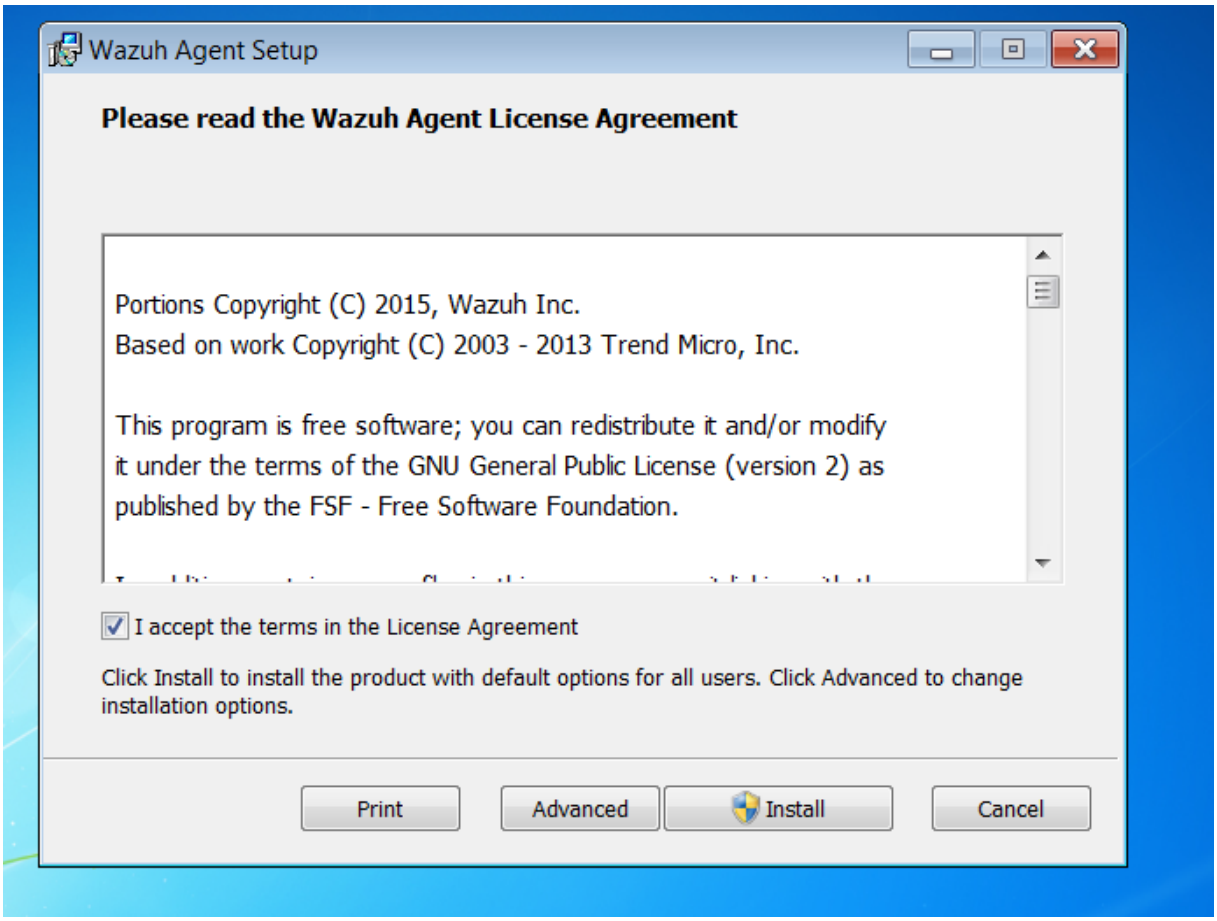
B. Ajout et configuration d'un agent Wazuh sur Windows

Pour permettre la supervision d'un poste Windows (dans mon cas, avec l'IP 10.5.20.12), j'ai installé et configuré **l'agent Wazuh pour Windows**.

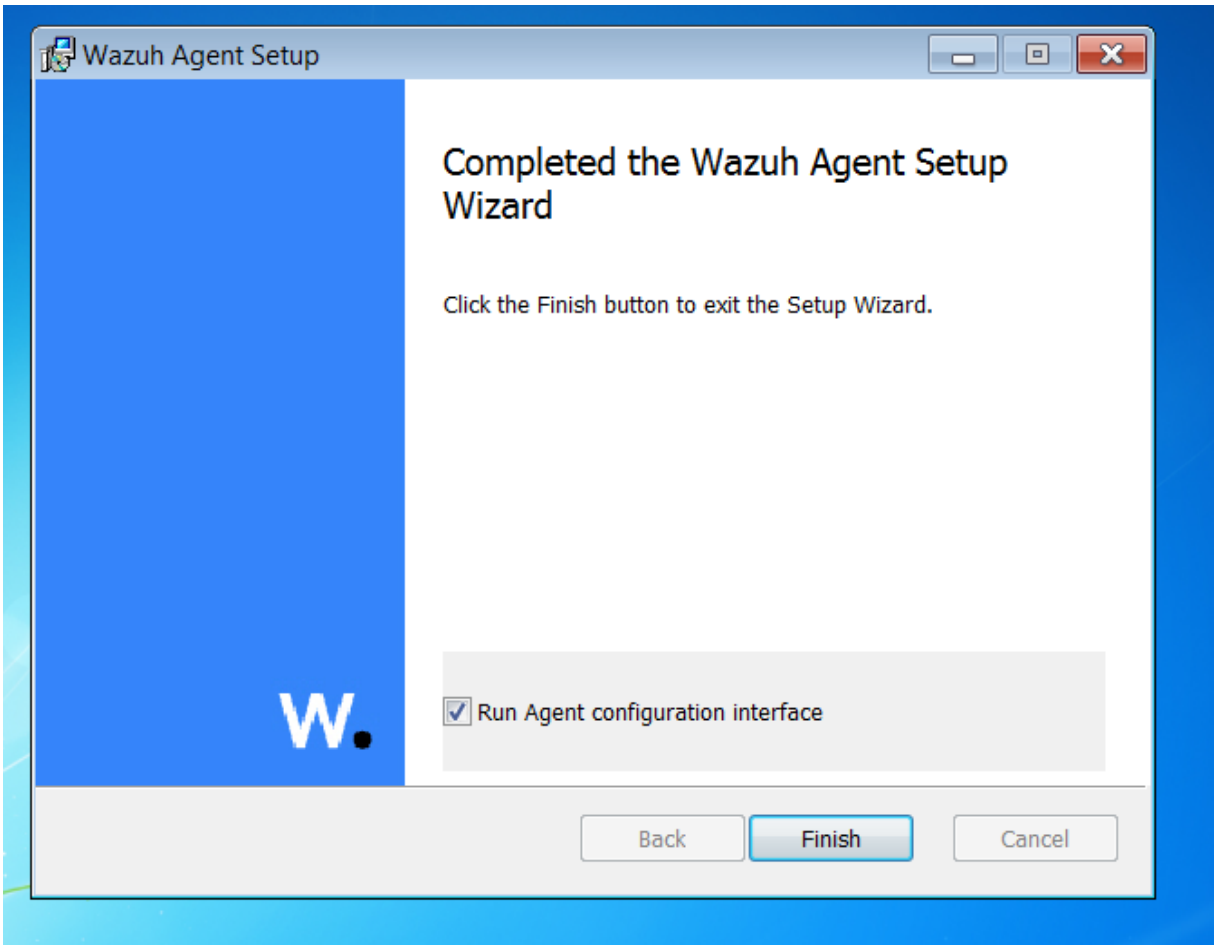
1. Téléchargement et installation de l'agent

J'ai téléchargé le fichier wazuh-agent-4.12.0.msi depuis le site officiel https://wazuh.com puis j'ai lancé l'installation graphique (**setup** classique sous Windows).

Thierno Cherif HANE



thane@groupeisi.com



2. Configuration de l'agent

Ouvrir un terminal sur le serveur Wazuh

Exécuter l'outil de gestion des agents :

/var/ossec/bin/manage_agents

```
root@debian11:~# /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.12.0 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: agent-win7
   * The IP Address of the new agent: 10.5.20.10
Confirm adding it?(y/n): y
Agent added with ID 001.
```

Ensuite, on dois extraire la clé d'authentification :

Toujours dans le menu, on tape :

E

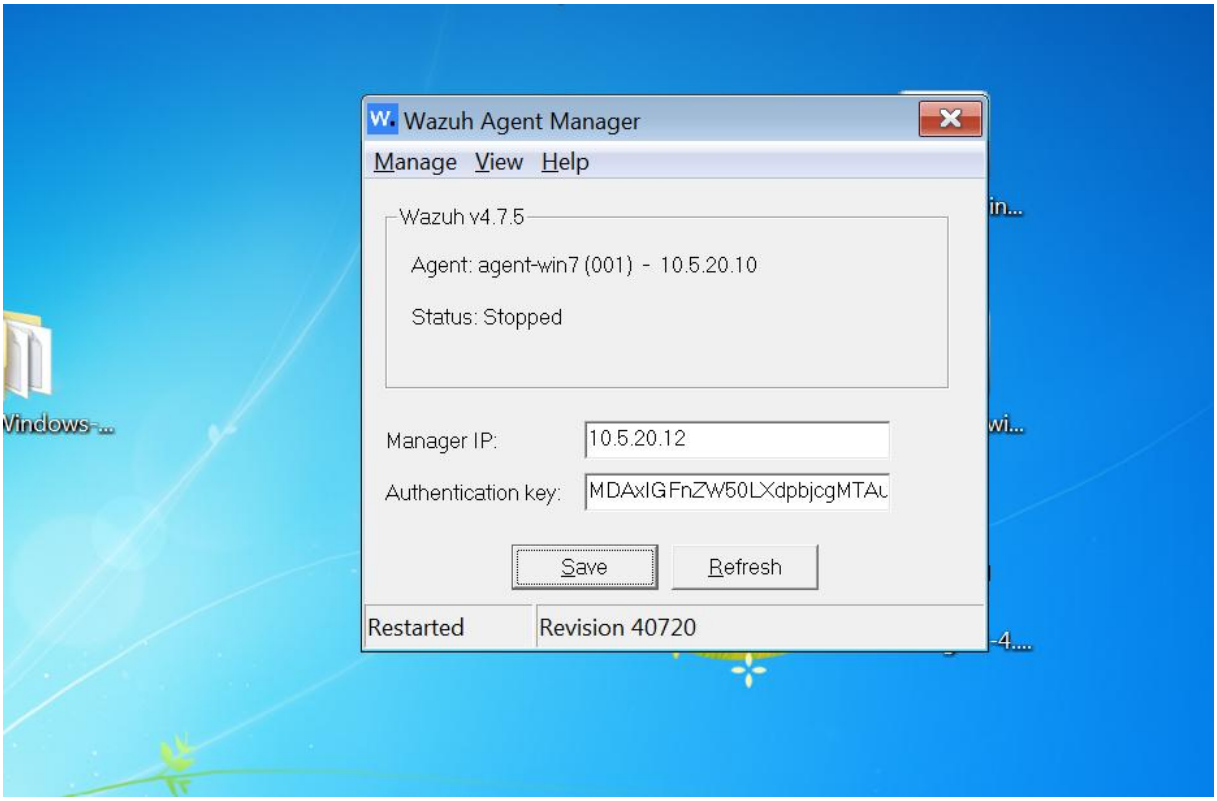
- Choisis l'ID de l'agent à extraire (par exemple 001)
- La clé te sera affichée : **copie-la** pour la coller ensuite sur l'agent Windows.

```
****************************************
* Wazuh v4.12.0 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: agent-win7, IP: 10.5.20.10
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIGFnZW50LXdpbjcgMTAuNS4yMC4xMCAzZWQ5YWQyYTEwZGJkYjhhZDU0YjU3NTVlMzE3OGQ4YjcyOTM5MjE2YzUwMDA3NDdiZTQ3NThkZTFjZjUyZWJm

** Press ENTER to return to the main menu.
```

Après suis allé sur la machine cliente j'ai ouvert le programme « Wazuh Agent » j'ai rempli les champs suivants :

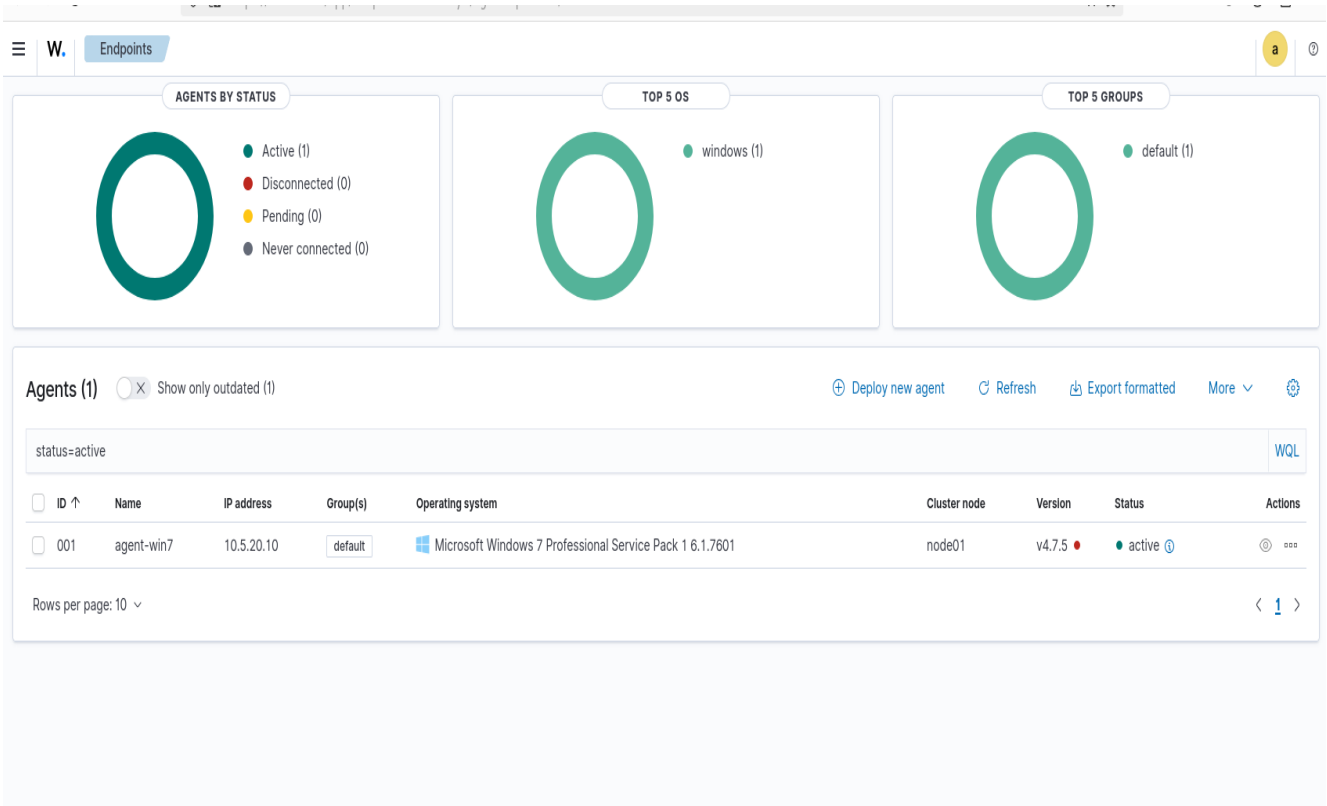
- **Manager IP** : 10.5.20.10 (adresse de mon serveur Wazuh)
- **Authentication key** : j'ai copié la clé fournie par le manager via /var/ossec/bin/manage_agents

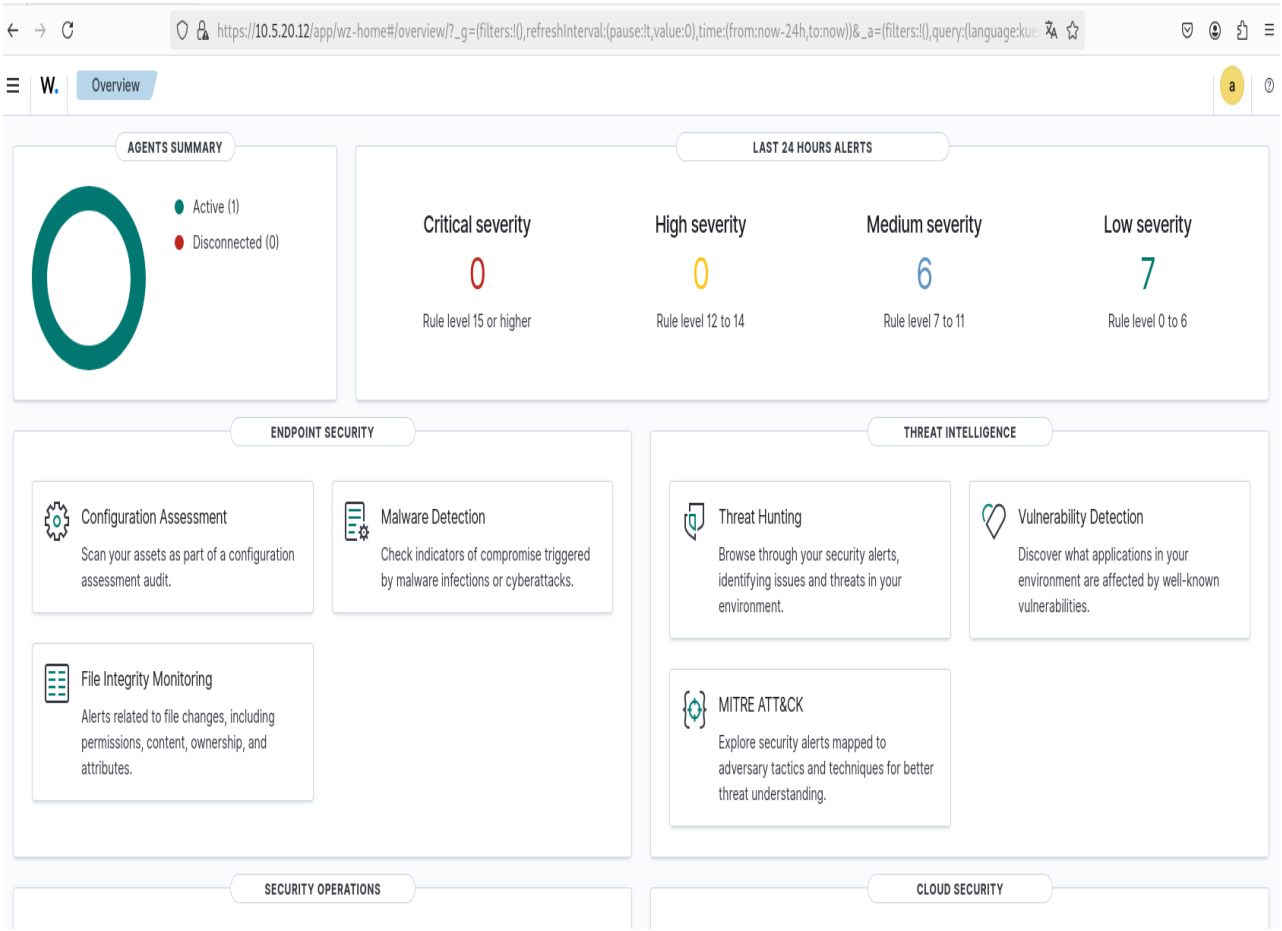
Thierno Cherif HANE



thane@groupeisi.com

Thierno Cherif HANE





thane@groupeisi.com

Thierno Cherif HANE

V. Conclusion

Ce projet m'a permis de mettre en place une solution de supervision avec Wazuh sur un serveur Debian, ainsi que deux agents sous Linux et Windows. Grâce à cette installation, j'ai pu centraliser les journaux et détecter d'éventuelles intrusions. Ce travail m'a aidé à mieux comprendre les bases de la sécurité réseau et l'importance de la surveillance des systèmes.

thane@groupeisi.com