# Déploiement des agents Wazuh

NOM: KOUASSI

PRENOM: GLOHNDY JEAN-MARIE

ETABLISSEMENT: ORT-TOULOUSE

# Sommaire

# 1. Introduction

Après avoir installé le serveur Wazuh, l’ indexeur et le dashboard (TP1), l’ objectif est de déployer des agents Wazuh sur les terminaux clients afin de collecter les logs et événements de sécurité.

# 2. Pré-requis

### TP1 terminé

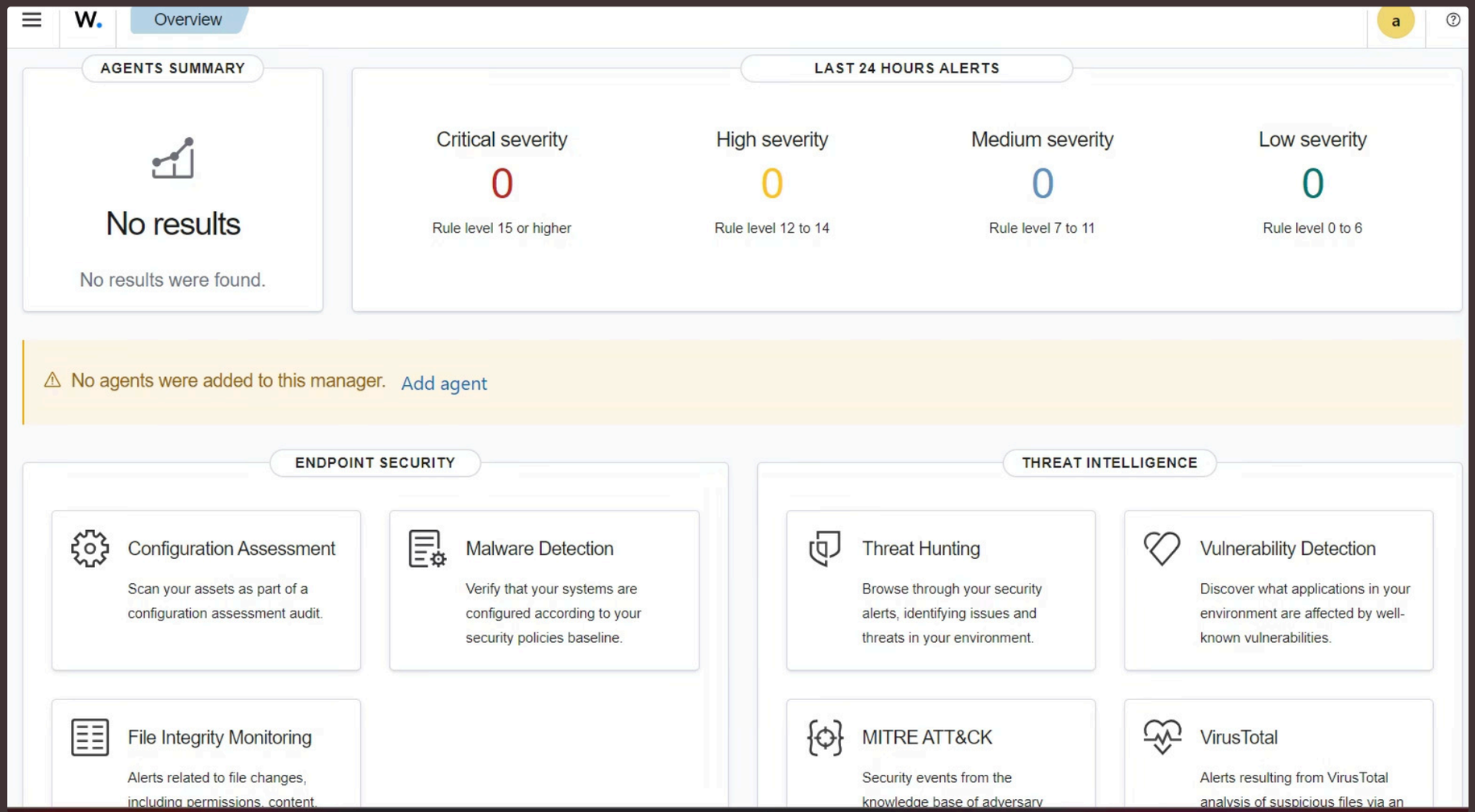
Wazuh manager, indexeur et dashboard installés.

### Accès au Dashboard

Accès au Wazuh Dashboard.

### Machines clientes

Machines clientes : Debian 12 et Windows 10.



# 3. Ajout d’ un agent depuis le Dashboard

## Se connecter au Dashboard

https://:5601

## Créer un nouvel agent

Cliquer sur “Add agent” pour créer un nouvel agent.

## Choisir le système

Choisir le type de système : Linux (Debian 12) ou Windows 10.

## Entrer l’ adresse IP

Entrer l’ adresse IP du serveur Wazuh (où le manager est installé).

## Génération du script

Le Dashboard génère un script d’ installation spécifique pour chaque machine.

# 4. Installation et configuration de l’agent

## 4.1 Agent Debian 12

### Étapes d'installation

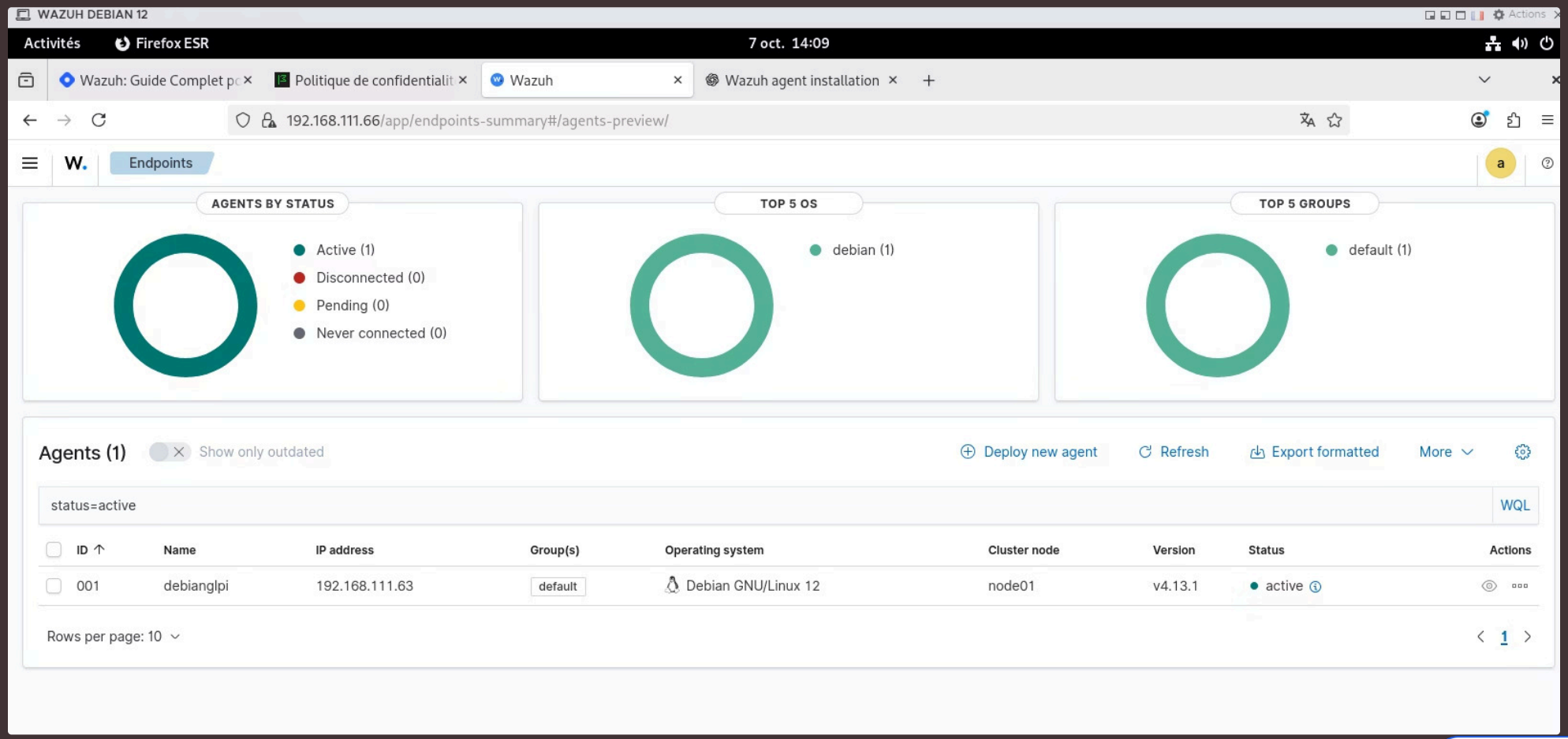
- Copier le script généré depuis le Dashboard.
- Ouvrir un terminal sur Debian 12 et exécuter le script avec les droits administrateur (`sudo`).

### Démarrage de l’agent

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

### Explications des commandes

- **daemon-reload** : recharge les services système.
- **enable wazuh-agent** : active le démarrage automatique de l’agent au boot.
- **start wazuh-agent** : démarre l’agent immédiatement.



# 4. Installation et configuration de l’agent (suite)

## 4.2 Agent Windows 10

### Étapes d'installation

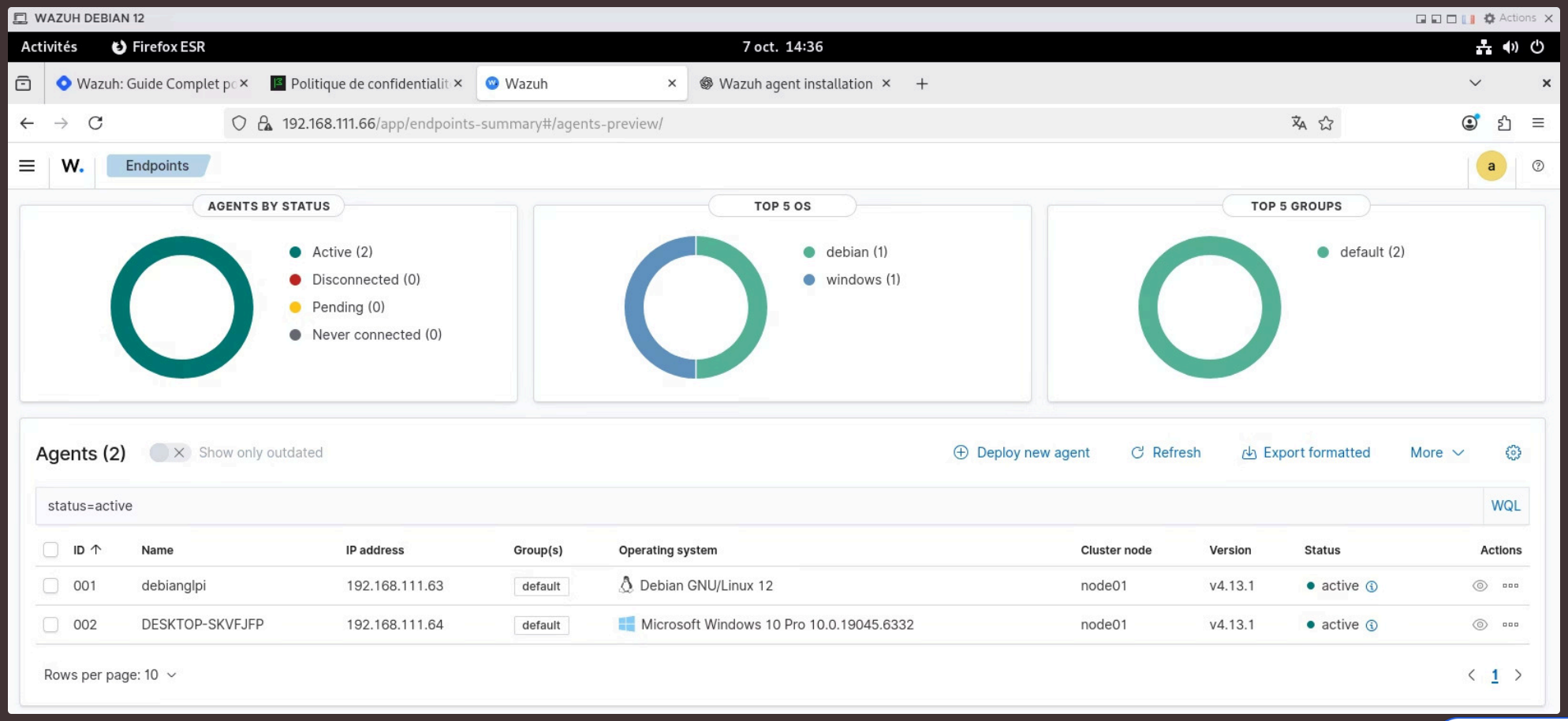
- Copier le script généré depuis le Dashboard.
- Ouvrir l’invite de commandes en mode Administrateur.
- Coller et exécuter le script.

### Démarrage de l’agent

```
NET START WazuhSvc
```

### Explications

Démarre le service `WazuhSvc` qui correspond à l’agent Wazuh sur Windows.



# 5. Vérification et surveillance

Les agents installés apparaissent dans le Dashboard Wazuh.

💡 Les logs sont remontés en temps réel du Debian 12 et du Windows 10 vers le serveur Wazuh.

### Blocage d’ acteurs malveillants

### Surveillance de l’ intégrité des fichiers (FIM)

### Détection de tentatives de connexion échouées répétées

### Analyse des comportements réseau

### Réponse automatisée aux incidents

# 6. Conclusion

Le TP2 montre comment déployer facilement les agents Wazuh sur Debian 12 et Windows 10.

### Collecte Sécurisée

Chaque agent assure la collecte et le transfert sécurisé des logs vers le manager Wazuh.

### Supervision Centralisée

Après installation, le Dashboard permet une supervision centralisée et réactive de tous les terminaux.