

Déploiement des agents Wazuh

NOM: KOUASSI

PRENOM: GLOHNDY JEAN-MARIE

ETABLISSEMENT: ORT-TOULOUSE



Sommaire

1. Introduction
2. Pré-requis
3. Ajout d' un agent depuis le Dashboard
4. Installation et configuration de l' agent
 - Agent Debian 12
 - Agent Windows 10
5. Démarrage de l' agent
6. Vérification et surveillance
7. Conclusion

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.

The screenshot shows the Wazuh Dashboard Overview page. The top navigation bar includes a menu icon, the Wazuh logo, and the 'Overview' tab. A yellow notification bubble with the letter 'a' and a help icon are in the top right. The main content area is divided into two main sections: 'AGENTS SUMMARY' and 'LAST 24 HOURS ALERTS'. The 'AGENTS SUMMARY' section shows a line graph icon and the text 'No results' with the message 'No results were found.' The 'LAST 24 HOURS ALERTS' section displays four severity levels: Critical severity (0), High severity (0), Medium severity (0), and Low severity (0), each with a corresponding rule level range. Below these sections is a yellow banner with a warning icon and the text 'No agents were added to this manager. Add agent'. The bottom section is divided into two columns: 'ENDPOINT SECURITY' and 'THREAT INTELLIGENCE'. The 'ENDPOINT SECURITY' column contains three cards: 'Configuration Assessment' (Scan your assets as part of a configuration assessment audit.), 'Malware Detection' (Verify that your systems are configured according to your security policies baseline.), and 'File Integrity Monitoring' (Alerts related to file changes, including permissions, content.). The 'THREAT INTELLIGENCE' column contains three cards: 'Threat Hunting' (Browse through your security alerts, identifying issues and threats in your environment.), 'Vulnerability Detection' (Discover what applications in your environment are affected by well-known vulnerabilities.), and 'MITRE ATT&CK' (Security events from the knowledge base of adversary). The 'VirusTotal' card is partially visible at the bottom right, showing 'Alerts resulting from VirusTotal analysis of suspicious files via an'.

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.

The screenshot displays the Wazuh dashboard interface in a web browser. The top navigation bar includes the Wazuh logo and the 'Endpoints' tab. Below the navigation bar, there are three summary cards: 'AGENTS BY STATUS' showing 1 Active agent, 'TOP 5 OS' showing 1 Debian agent, and 'TOP 5 GROUPS' showing 1 default group. The main section is titled 'Agents (1)' and includes a search filter 'status=active'. Below the filter is a table with the following data:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	debianglpi	192.168.111.63	default	Debian GNU/Linux 12	node01	v4.13.1	active	

The bottom of the dashboard shows pagination controls for 10 rows per page.

4. Installation et configuration de l' agent (suite)

4.2 Agent Windows 10

Étapes d'installation

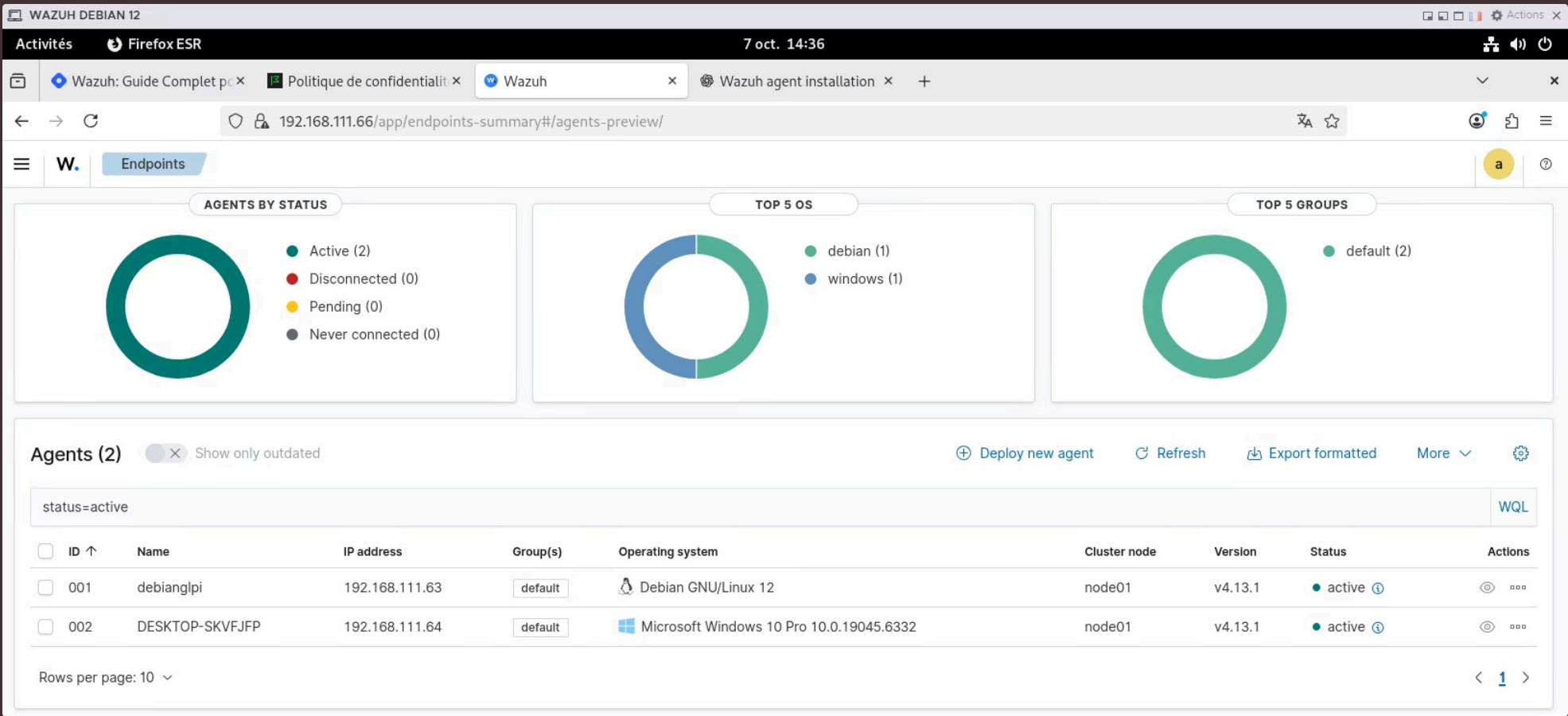
- Copier le script généré depuis le Dashboard.
- Ouvrir l' invite de commandes en mode Administrateur.
- Coller et exécuter le script.

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.