Installation de Wazuh sur Ubuntu avec agent Windows

1. Contexte et objectif

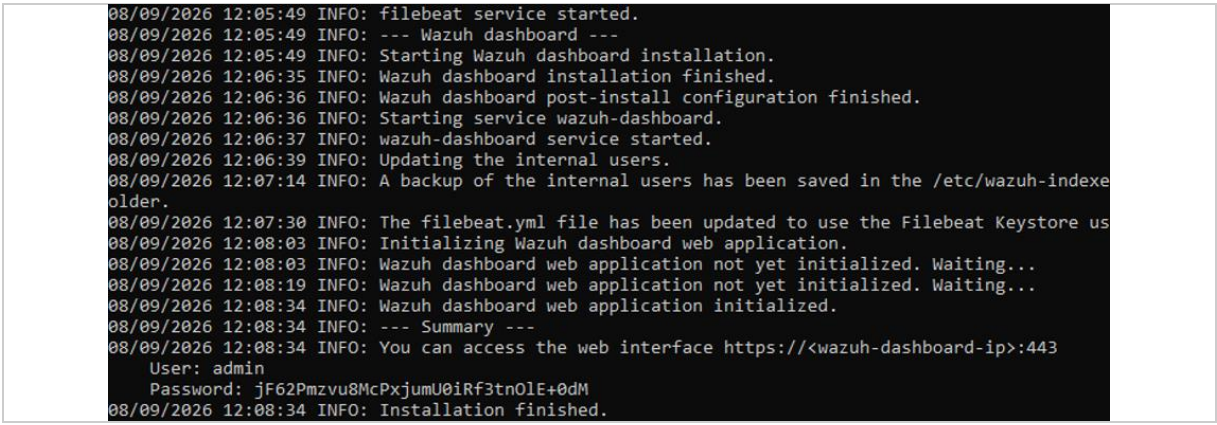
Wazuh est une plateforme open source de sécurité unifiée (SIEM/XDR). Elle centralise la collecte et l'analyse des événements de sécurité provenant des équipements d'un réseau : journaux système, alertes, détection d'intrusion, surveillance de l'intégrité des fichiers, évaluation de la conformité et threat intelligence. Elle est utilisée pour détecter les menaces, répondre aux incidents et superviser la posture de sécurité d'un parc informatique.

2. Installation de Wazuh sur Ubuntu

Wazuh propose un script d'installation officiel qui déploie automatiquement l'ensemble des composants en une seule commande. Le script est téléchargé depuis le dépôt officiel, puis exécuté avec l'option -a (all-in-one) :

```
cd /tmp
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh
sudo bash ./wazuh-install.sh -a
```

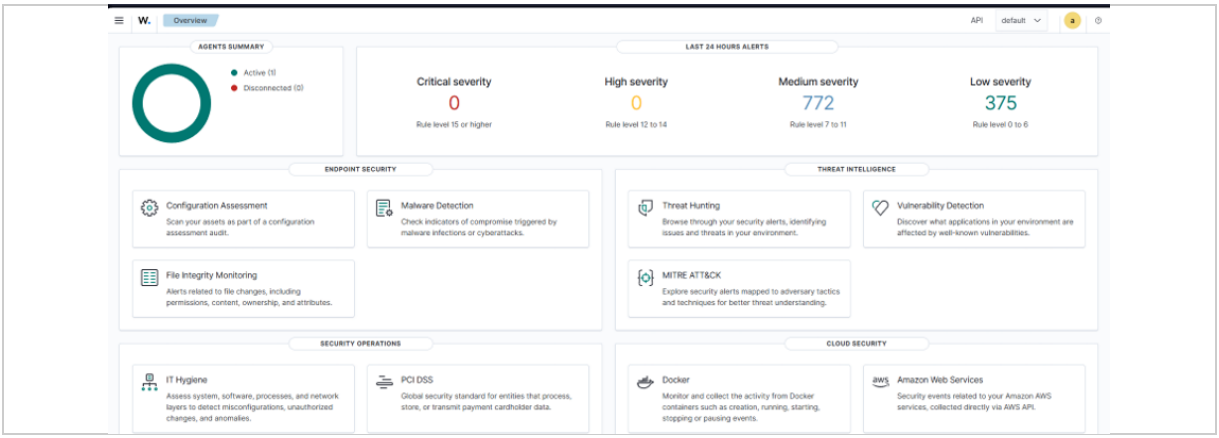
L'installation est entièrement automatisée et dure plusieurs minutes. A la fin du processus, le script affiche un résumé avec l'URL d'accès et les identifiants générés automatiquement.



3. Accès au dashboard Wazuh

Le dashboard Wazuh est accessible depuis un navigateur à l'adresse https://IP_SERVEUR:443. La connexion s'effectue avec le compte admin et le mot de passe affiché à la fin de l'installation. Le certificat SSL est auto-signé : il faut accepter l'exception de sécurité dans le navigateur lors du premier accès.

La page d'accueil Overview affiche un résumé de la posture de sécurité : nombre d'agents actifs/déconnectés, alertes des dernières 24h par niveau de sévérité (critique, élevé, moyen, faible) et l'ensemble des modules disponibles.



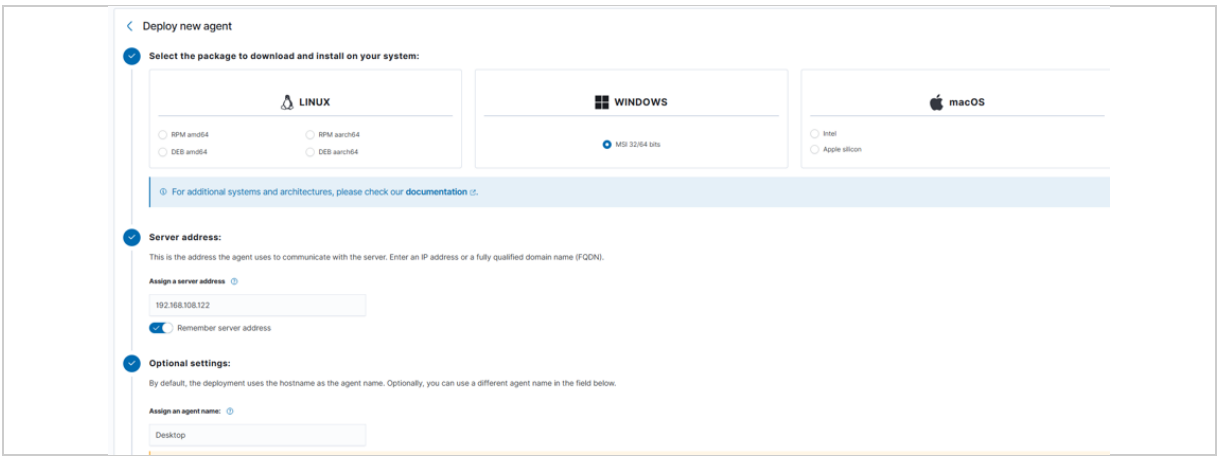
4. Déploiement de l'agent Wazuh sur un poste Windows

L'agent Wazuh est un service installé sur les postes clients. Il collecte les événements de sécurité (logs Windows, modifications de fichiers, tentatives de connexion, etc.) et les envoie au Manager Wazuh pour analyse et corrélation.

4.1 Génération de la commande d'installation

Dans le dashboard Wazuh, l'assistant de déploiement est accessible via le menu Endpoints → Deploy new agent. Il génère automatiquement la commande d'installation adaptée à la plateforme choisie. Les paramètres configurés sont :

- Système cible : Windows (MSI 32/64 bits)
- Adresse du serveur Wazuh : 192.168.108.122
- Nom de l'agent : Desktop (identifiant du poste dans le dashboard)

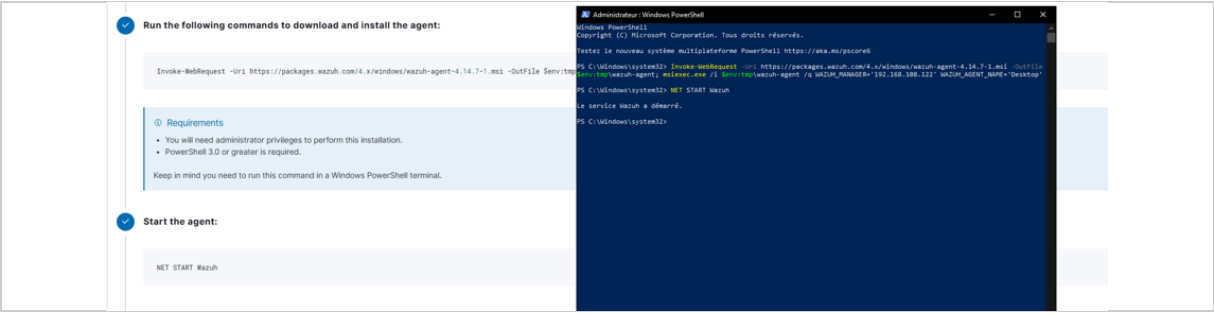


4.2 Installation et démarrage sur Windows

L'assistant fournit une commande PowerShell complète qui télécharge et installe l'agent en une seule étape. La commande est exécutée dans un terminal PowerShell en mode administrateur :

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.7-1.msi `
  -OutFile $env:tmp\wazuh-agent.msi; msiexec.exe /i $env:tmp\wazuh-agent.msi `
  /q WAZUH_MANAGER='192.168.108.122' WAZUH_AGENT_NAME='Desktop'
NET START Wazuh
```

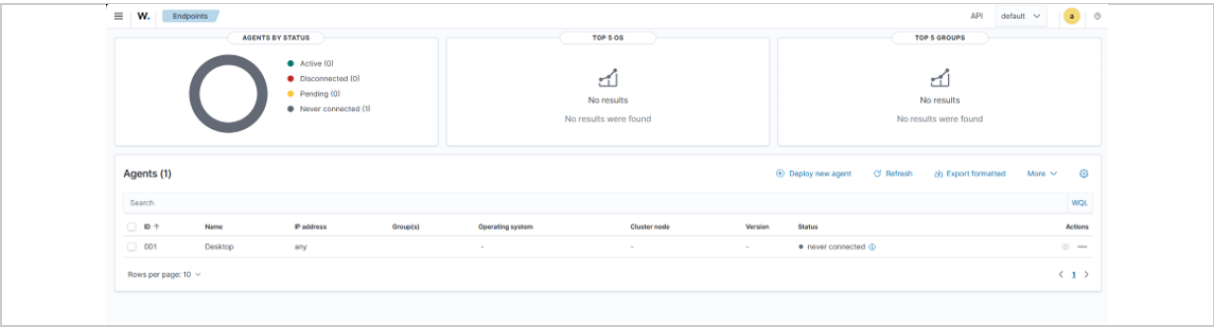
La première commande télécharge et installe silencieusement l'agent MSI avec les paramètres du Manager. La seconde démarre le service Wazuh immédiatement. Le service peut aussi être démarré ou redémarré via PowerShell avec Start-Service WazuhSvc.



5. Vérification dans le dashboard

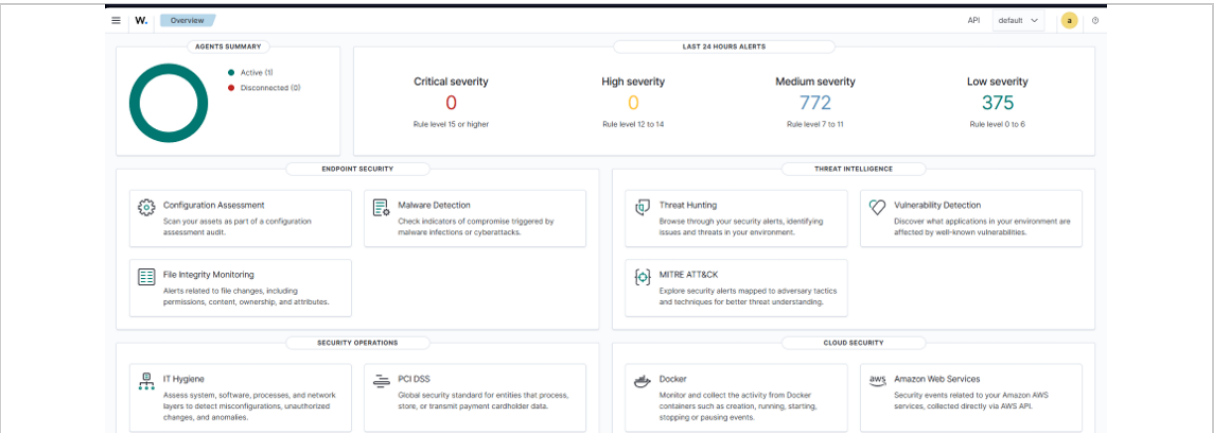
5.1 Liste des endpoints

Dans Wazuh, la section Endpoints affiche la liste de tous les agents enregistrés. Après l'installation, le poste Desktop apparaît avec son identifiant (001), son adresse IP et son statut. Au premier enregistrement, le statut est "never connected" jusqu'à ce que la première connexion soit établie, puis il passe à "Active".



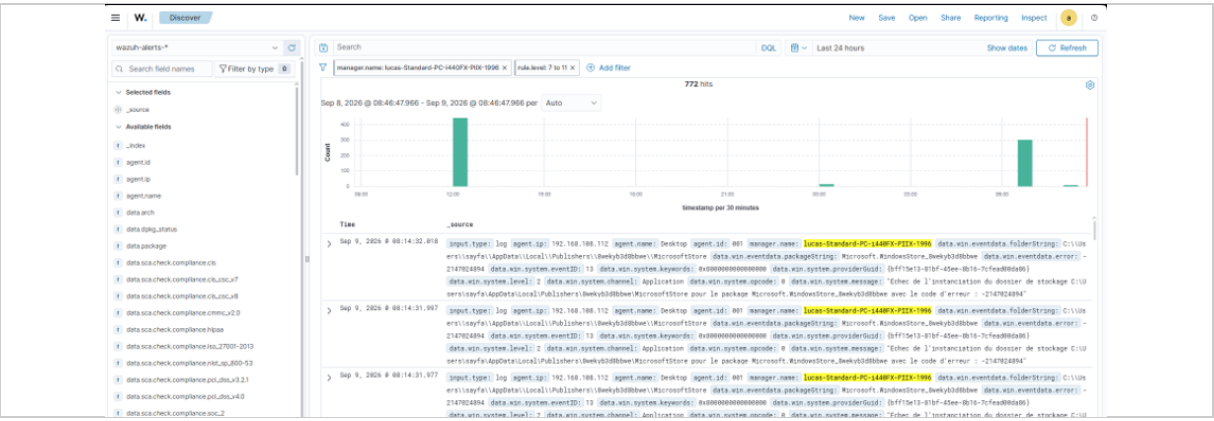
5.2 Alertes en temps réel

Une fois l'agent actif (statut Active), les événements collectés sur le poste Windows sont transmis au Manager Wazuh et indexés. Dans Wazuh, la vue Overview affiche 1 agent actif et le total des alertes des dernières 24h réparties par sévérité. Sur ce poste, 772 alertes de niveau moyen et 375 de niveau faible ont été générées, principalement liées aux activités système et applicatives normales de Windows.



5.3 Exploration des logs avec Discover

Le module Discover (anciennement accessible via l'Indexer) permet d'explorer en détail les événements collectés par l'agent. Les alertes sont filtrables par machine (manager.name), par niveau de règle (rule.level), par date et par n'importe quel champ des événements Windows. Chaque log affiche des informations détaillées : IP de l'agent, EventID Windows, canal (Application/Système/Sécurité), message et métadonnées associées.



6. Modules de sécurité disponibles

Le dashboard Wazuh propose de nombreux modules couvrant différents aspects de la sécurité :

- Endpoint Security : évaluation de configuration, détection de malwares, surveillance de l'intégrité des fichiers (FIM)
- Threat Intelligence : threat hunting, détection de vulnérabilités, corrélation MITRE ATT&CK
- Security Operations : IT Hygiene, conformité PCI DSS
- Cloud Security : Docker, Amazon Web Services

Ces modules fonctionnent automatiquement dès que l'agent est actif, sans configuration supplémentaire pour les cas d'usage de base.