

Sécurisation des Flux par VPN

Dans le cadre de la sécurisation de vos infrastructures il vous est demandé de pouvoir anticipé et agir en cas de soucis.

Auteur

Roblot Jean-Philippe - jroblot.simplon@proton.me

Version

29/02/2024 - V1R0

Releases

Ubuntu Server LTS22.04 Ubuntu Desktop LTS22.04 Windows Server 2019 Windows 10 22H2 Wazuh 4.7

Powered by <https://shields.io>

Contexte

En tant que administrateur Cybersécurité, mise en place d'un serveur EDR et ajout d'agent sur les serveurs et clients de l'infrastructure.

Questions

1. Qu'est-ce que l'Endpoint Detection and Response (EDR) et quel est le rôle de Wazuh dans ce domaine ?

Les solutions de sécurité EDR peuvent détecter les comportements suspects du système sur les hôtes et les terminaux, collecter des données sur les points de terminaison et analyser les événements individuels, puis enquêter sur la cause première du comportement malveillant. Leurs principales fonctions :

- Détection automatisée des cybermenaces
- Intégration de la Threat Intelligence
- Surveillance continue en temps réel et visibilité historique
- Enquête rapide sur les menaces

Wazuh se compose de différents composants :

- Les agents Wazuh, déployés sur les hôtes à surveiller, collectant des données sur les activités du système et des journaux pour les analyser et détecter les comportements suspects ou les signes d'intrusion.
- Le serveur Wazuh, qui agit comme un centre de contrôle, recevant et analysant les données des agents. Le serveur Wazuh est l'élément central où se déroule la corrélation des événements, la détection d'anomalies et la réponse aux incidents.
- Interface utilisateur (UI) et API : Pour la gestion et la visualisation des données, l'interface utilisateur offre des tableaux de bord, des alertes et des rapports. L'API permet l'intégration avec

d'autres outils et systèmes existants.

Ses fonctionnalités :

- Détection des menaces :
- Analyse des journaux
- Conformité et gestion des vulnérabilités
- Réponse aux incidents

2. Quels sont les principaux avantages de l'utilisation de Wazuh comme solution EDR pour la détection et la réponse aux menaces sur les endpoints ?

- Open Source : Étant une solution open source, Wazuh est accessible à tous, favorisant la transparence et permettant à la communauté de contribuer à son développement.
- Flexibilité et extensibilité : Wazuh peut s'intégrer à d'autres outils et solutions de sécurité, offrant ainsi une plus grande flexibilité pour répondre aux besoins spécifiques de chaque environnement.
- Surveillance centralisée : Avec un serveur central, il est possible de surveiller et de gérer un grand nombre d'agents, ce qui en fait une solution adaptable aux réseaux de toute taille.
- Corrélation avancée des événements : La capacité de corréler les événements à partir de multiples sources permet une détection plus précise des menaces.

3. Quels sont les prérequis matériels et logiciels nécessaires pour déployer Wazuh en tant que solution EDR ?

- Matériel :
 - 2 coeurs CPU, 4Go de RAM et 3Go de stockage pour le serveur (ou plus selon le nombre d'agents)
- Logiciels
 - Navigateur : Chrome 95 or later, Firefox 93 or later, Safari 13.7 or later
 - L'agent est pris en charge pour Linux, Windows, MacOS, Docker et Kubernetes

4. Comment configurer les agents Wazuh sur les endpoints et quels types de données sont collectés pour l'analyse ?

La configuration des agents est centralisée via le fichier **agent.conf**.

Sont paramétrables à distance :

- Surveillance de l'Intégrité des Fichiers (syscheck) : Vérifie les modifications de fichiers sur les points d'extrémité.
- Détection de Rootkits (rootcheck) : Identifie les rootkits et les comportements suspects.
- Collecte de Données de Journal (localfile) : Collecte les journaux système et d'application.
- Surveillance des Politiques de Sécurité (wodle name="open-scap", wodle name="cis-cat") : Vérifie la conformité aux politiques de sécurité.
- Commandes à Distance (wodle name="command") : Permet d'exécuter des commandes à distance sur les agents.
- Étiquettes pour les Alertes des Agents (labels) : Ajoute des étiquettes aux alertes générées par les agents.

- Évaluation de la Configuration de Sécurité (sca) : Évalue la configuration de sécurité des points d'extrémité.
- Inventaire Système (syscollector) : Collecte des informations sur les logiciels installés, les utilisateurs, etc.
- Éviter les Inondations d'Événements (client_buffer) : Gère le flux d'événements.
- Configuration osquery (wodle name="osquery") : Intègre osquery pour collecter des données supplémentaires.
- Intervalle de Reconnexion Forcée (client) : Configure l'intervalle de reconnexion forcée des agents.

5. Quels sont les mécanismes de détection de Wazuh pour identifier les menaces et les comportements suspects sur les endpoints ?

Wazuh utilise des règles, des analyses de vulnérabilités et des mécanismes de surveillance pour identifier les menaces et les comportements anormaux sur les points d'extrémité, renforçant ainsi la sécurité globale du réseau.

6. Comment configurer des alertes dans Wazuh pour être informé en temps réel des activités malveillantes sur les endpoints ?

On peut générer des alertes via les règles de détection des menaces prédéfinies de Wazuh, en créant des règles personnalisées et via la surveillance de l'intégrité des fichiers (FIM).

L'intégration avec VirusTotal et Yara renforce la capacité de Wazuh à identifier les menaces.

Déploiement du serveur Zabbix

- Déployer une VM Ubuntu Server LTS 22.04 (dans notre cas dans Azure)

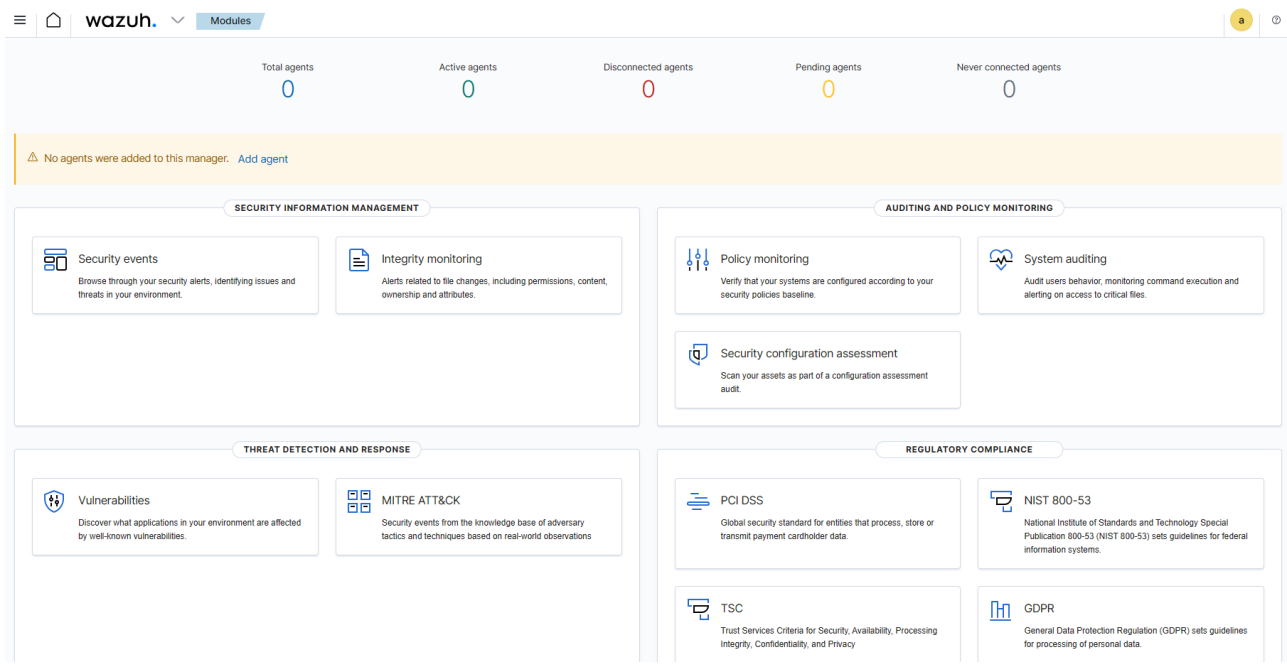
The screenshot displays the Azure portal interface for a virtual machine named 'vmwazuh'. The left sidebar contains navigation options such as 'Vue d'ensemble', 'Journal d'activité', 'Contrôle d'accès (IAM)', 'Étiquettes', 'Diagnosticuer et résoudre les problèmes', 'Se connecter', 'Mise en réseau', 'Paramètres', and 'Disponibilité + mise à l'échelle'. The main content area shows the 'Bases' (Basics) tab, which includes details about the operating system (Linux (ubuntu 22.04)), size (Standard D2s v3), and network configuration. Below this, the 'Propriétés' (Properties) tab is active, showing the 'Machine virtuelle' (Virtual machine) section with details like 'Nom de l'ordinateur' (vmwazuh), 'Système d'exploitation' (Linux (ubuntu 22.04)), 'Éditeur de l'image' (canonical), 'Offre d'image' (0001-com-ubuntu-server-jammy), 'Plan d'image' (22_04-lts-gen2), 'Génération de machine virtuelle' (V2), 'Architecture de machine virtuelle' (x64), 'État de l'agent' (Ready), and 'Version de l'agent' (2.9.1.1). The 'Mise en réseau' (Networking) section shows the public IP address (74.235.201.188) and the private IP address (10.6.0.4).

- Installer W.Indexer, W.Server, W.Dashboard

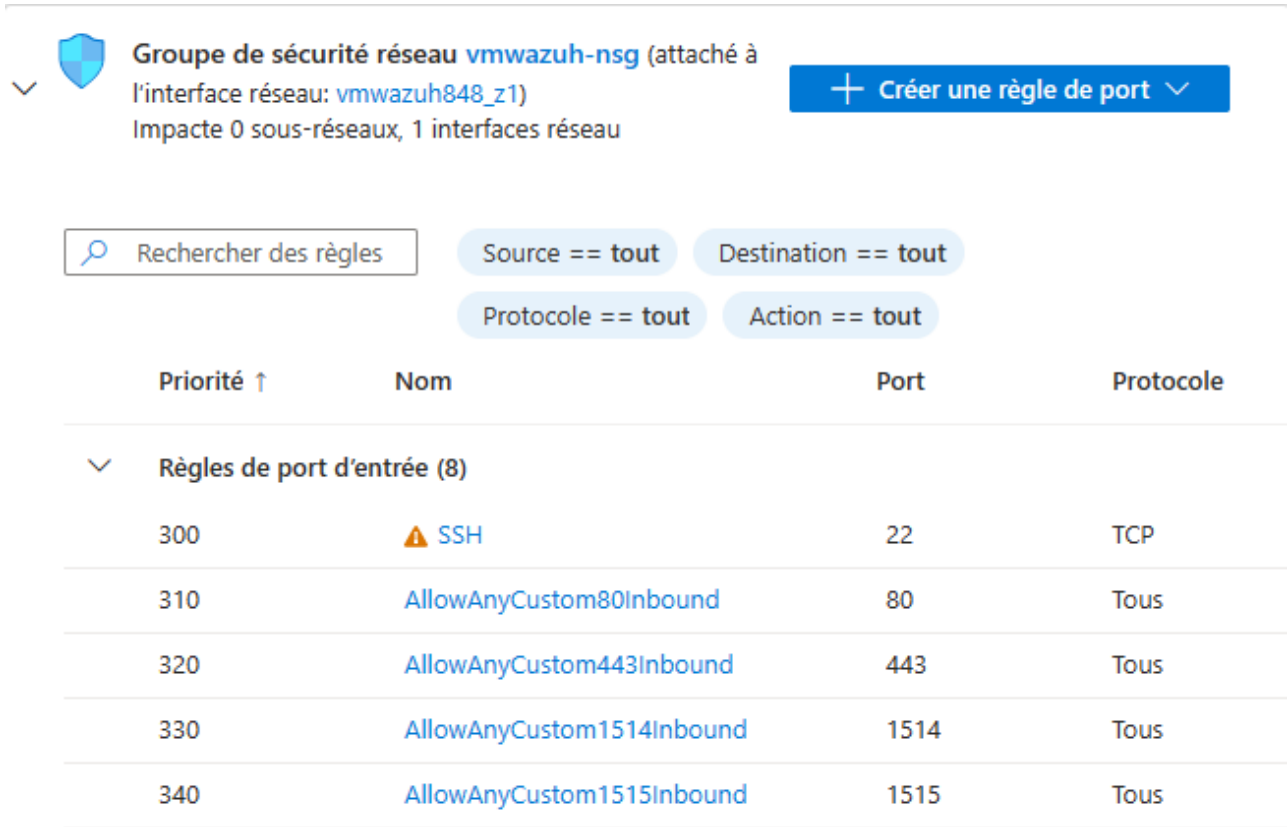
```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash
./wazuh-install.sh -a
```

```
29/02/2024 10:47:51 INFO: --- Summary ---
29/02/2024 10:47:51 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: yuLibYou6T6Ogyep4?HDWuNzk6TRb0Y4
29/02/2024 10:47:51 INFO: Installation finished.
```

- Via le navigateur, se connecter au dashboard avec les identifiants fournis lors de l'installation



- Le manager utiliser les ports 1514 et 1515 pour récupérer les données des agents. Ils faut donc ouvrir les ports du serveur



Ajouter l'agent pour Windows


- Via PowerShell**
Dans le portail Wazuh, cliquer sur "add an agent"

Agents

Deploy new agent

✓

Select the package to download and install on your system:


 LINUX

☐ RPM amd64


☐ RPM aarch64

☐ DEB amd64

☐ DEB aarch64

 WINDOWS

☒ MSI 32/64 bits

 macOS

☐ Intel

☐ Apple silicon

ⓘ

For additional systems and architectures, please check our documentation [↗](#).

✓

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: ⓘ

74.235.201.188

Windows-Client-Agent

ⓘ

The agent name must be unique. It can't be changed once the agent has been enrolled. [↗](#)

Select one or more existing groups: ⓘ

Default

▼

4

Run the following commands to download and install the agent:

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.2-1.msi -OutFile \${env.tmp}\wazuh-agent; msexec.exe /i \${env.tmp}\wazuh-agent /q WAZUH_MANAGER='74.235.201.188' WAZUH_AGENT_NAME='Windows-Client-Agent' WAZUH_REGISTRATION_SERVER='74.235.201.188'

ⓘ

Requirements

You will need administrator privileges to perform this installation.

PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

5

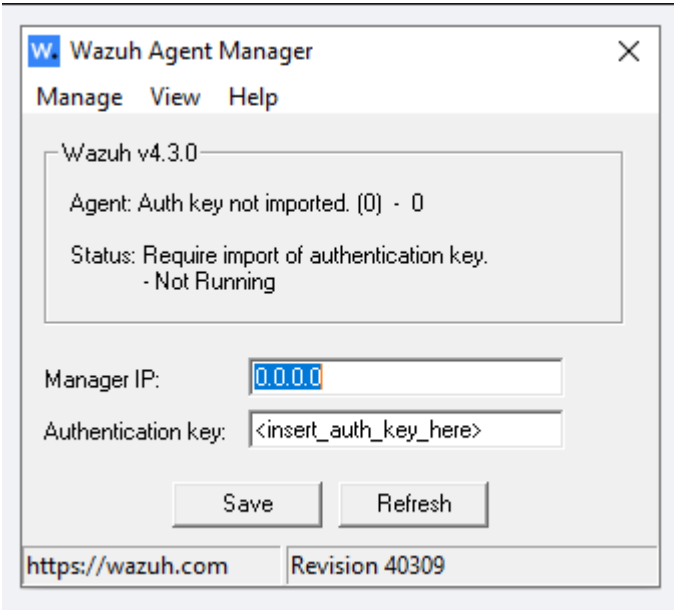
Start the agent:

NET START WazuhSvc

• Via GUI

6 / 8

- Télécharger l'installer sur le poste client via [le site officiel](#)
- Lancer l'assistant d'installation



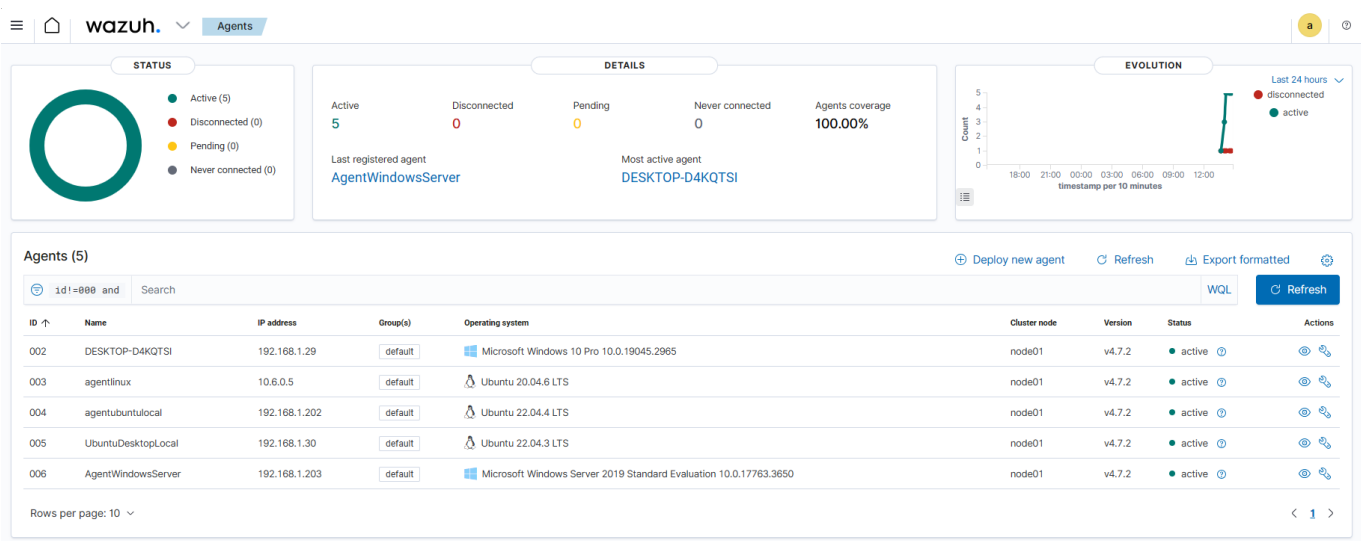
Ajouter l'agent pour Linux

- Procéder de la même façon que précédemment sur le portail Wazuh, spécifier l'agent correspondant à votre distribution (ici DEB amd64)

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.2-1_amd64.deb && sudo WAZUH_MANAGER='74.235.201.188' WAZUH_AGENT_NAME='ubuntu' dpkg -i ./wazuh-agent_4.7.2-1_amd64.deb

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

Visualiser nos agents



Retirer un agent de la liste

- Sur le serveur Wazuh

```

modo@vmwazuh:~$ sudo /var/ossec/bin/manage_agents ## Retirer un agent de la liste
1  # Sécurisation des Flux par VPN
88  ## Ajouter l'agent pour Windows
***** poste client via [le site
* Wazuh v4.7.2 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: r
Available agents:
ID: 001, Name: Windows-Client-Agent, IP: any
ID: 002, Name: DESKTOP-D4KQTSI, IP: any
ID: 003, Name: agentlinux, IP: any
ID: 004, Name: agentubuntulocal, IP: any
ID: 005, Name: UbuntuDesktopLocal, IP: any
ID: 006, Name: AgentWindowsServer, IP: any
Provide the ID of the agent to be removed (or '\q' to quit): 001
Confirm deleting it?(y/n): y
Agent '001' removed.

```