Galaxy Swiss Bourdin

Sommaire

I. Introduction 2

1. Contexte 2

2. Besoin 2

II. Solution 3

1. Choix de la technologie 3

2. Analyse comparative 3

III. Wazuh 5

1. Qu'est-ce que Wazuh ? 5

2. Origines de Wazuh 5

3. Les avantages de Wazuh 6

IV. Infrastructure 6

1. Schéma réseau actuel 6

2. Tableau d'Adressage IP des VLAN 7

3. Schéma réseau de la réalisation professionnelle 8

4. Matériel à disposition 9

V. Mise en place de Wazuh 10

1. Installation 10

2. Configuration 14

3. Test 19

VI. Évolution possible 25

1. Mise en place de la réponse automatisée (Active Response) 25

VII. Conclusion 25

I. Introduction

1. Contexte

Le laboratoire Galaxy Swiss Bourdin (GSB), issu de la fusion entre Galaxy et Swiss Bourdin, est devenu un leader mondial en 2009. Basé à Paris, GSB a choisi la France pour améliorer le suivi de ses activités de visite médicale, tout en ayant son siège social à Philadelphie, aux États-Unis. J'interviens en tant qu'administrateur système et réseau au sein de ce groupe.

2. Besoin

Le laboratoire Galaxy Swiss Bourdin (GSB) souhaite mettre en place un outil de supervision centralisée de la sécurité (SIEM/XDR) afin de protéger efficacement son système d'information et ses données stratégiques. Cet outil devra permettre :

- **Détection proactive et surveillance :**
  Collecter et analyser en temps réel les journaux d'événements de l'ensemble du parc informatique, incluant les serveurs centraux et les équipements des visiteurs médicaux. Cela permet d'identifier rapidement les comportements suspects, les anomalies et les tentatives d'intrusion sur le réseau.
- **Réponse automatisée aux incidents :**
  Apporter une capacité de réponse active pour bloquer automatiquement les menaces ou isoler les machines compromises. Cette réactivité immédiate permet de limiter l'impact d'une cyberattaque (comme un rançongiciel) sans attendre l'intervention manuelle des équipes informatiques.
- **Gestion des vulnérabilités :**
  Scanner en continu l'infrastructure pour identifier les failles de sécurité connues sur les systèmes et logiciels installés. Cela facilite la priorisation des correctifs et garantit le respect des politiques internes concernant la protection des données à caractère personnel.

En somme, GSB requiert un outil qui garantit la disponibilité, l'intégrité et la confidentialité de ses services informatiques face aux cyberattaques. L'objectif est de centraliser les alertes de sécurité, de réduire le temps de réponse aux incidents et d'obtenir une visibilité totale sur la posture de défense de l'infrastructure, sans générer de coûts de licence supplémentaires.

II. Solution

1. Choix de la technologie

Grâce à ce type de plateforme, nous bénéficions d'une vue centralisée sur les événements de sécurité, les journaux système et les activités suspectes, et nous pouvons être avertis rapidement lorsqu'un comportement anormal, une tentative d'intrusion ou une vulnérabilité est détecté sur un serveur ou un équipement informatique.

La supervision de sécurité des serveurs est le processus qui permet de surveiller en continu l'état des machines, de détecter les incidents potentiels, d'analyser les risques et d'assurer une meilleure protection des serveurs physiques ou virtuels ainsi que des données sensibles de l'entreprise.

2. Analyse comparative

Je souhaite choisir une solution de supervision de sécurité et de détection des menaces qui réponde précisément aux besoins de mon infrastructure. Pour cela, je me suis intéressé(e) aux outils les plus répandus et les plus éprouvés dans le domaine du SIEM, du XDR et de la surveillance des hôtes, afin de disposer d'une plateforme capable de centraliser les événements de sécurité et de signaler rapidement les comportements suspects ou les vulnérabilités détectées sur les serveurs et équipements informatiques.

Mon objectif est de bénéficier d'une solution offrant une vue centralisée sur les journaux système, les alertes de sécurité et l'état global du parc informatique, tout en assurant une détection rapide des incidents pouvant affecter la disponibilité, l'intégrité et la confidentialité du système d'information.

Cette analyse va ainsi comparer plusieurs solutions, en tenant compte de la facilité de mise en œuvre, de la richesse fonctionnelle, de la capacité de détection, de la gestion des vulnérabilités, de la performance, ainsi que du coût et de la scalabilité. Les principaux points forts et les limites de chacune seront détaillés dans le tableau suivant, afin de m'aider à déterminer laquelle convient le mieux à mon environnement et à mes priorités en matière de cybersécurité.

Critère	Wazuh	Splunk	Chef	SaltStack
Facilité d'utilisation	★★★★★ (5/5)	★★★ (3/5)	★★★ (3/5)	★★★★ (4/5)
	Agent léger, interface web ELK/Wazuh intuitive	Interface puissante mais complexe à maîtriser	Kibana très fluide, mais configuration de base complexe	Interface simple et efficace pour la gestion des logs
Communauté et écosystème	★★★★★ (5/5)	★★★★ (4/5)	★★★★ (4/5)	★★★ (3/5)
	Forte communauté open source, très documenté	Communauté entreprise massive (Splunk Answers)	Énorme communauté autour de la stack Elastic	Bonne communauté mais moins étendue qu'ELK ou Wazuh
Performance	★★★★ (4/5)	★★★★ (4/5)	★★★★ (4/5)	★★★★★ (5/5)
	Très performant (jusqu'à 30k événements/sec)	Excellente (plus de 100k événements/sec)	Très haute performance de traitement et d'indexation	Excellente (plus de 50k événements/sec)
Modèle d'architecture	Agent/Manager Analyse centralisée sur le Manager	Forwarder/Indexer/Search Head Architecture distribuée	Beats/Logstash/Elasticsearch Orienté traitement de données	Agent (Sidecar)/Server/OpenSearch Orienté collecte de logs
Sécurité et Conformité	Règles MITRE ATT&CK, PCI-DSS, RGPD intégrées	Solutions premium (Enterprise Security) très complètes	Bonnes fonctionnalités SIEM, mais moins "clé en main"	Très bonne gestion des gros volumes de logs
Scalabilité	★★★★★ (5/5)	★★★★ (4/5)	★★★★ (4/5)	★★★★ (4/5)
	Jusqu'à 14 000 agents par manager, clusterisable	Conçu pour de très grands environnements	Hautement scalable via le clustering Elasticsearch	Bonne gestion des environnements distribués
Coût	★★★★★ (5/5)	★ (1/5)	★★★ (3/5)	★★★★ (4/5)
	Gratuit (open source)	Très cher (licence au volume de données, $/Go)	Freemium (Core gratuit, fonctionnalités avancées tes) payan	Version Open Source gratuite, options Enterprise payantes

Au terme de cette analyse, j'opte pour Wazuh : sa spécialisation en cybersécurité, sa centralisation des journaux et des alertes, ainsi que sa gratuité répondent parfaitement à mes besoins de supervision et de protection de l'infrastructure. De plus, ses fonctionnalités de détection d'intrusion, d'analyse des vulnérabilités et de conformité facilitent la surveillance continue du système d'information, faisant de Wazuh le choix évident pour renforcer la sécurité des serveurs et des données sensibles de GSB.

III. Wazuh

1. Qu’est-ce que Wazuh ?

Wazuh est une plateforme open source de supervision de sécurité et de détection des menaces, reposant principalement sur une architecture de type Manager/Agent, qui permet de surveiller en continu les machines du système d’information. Il centralise les journaux, analyse les événements de sécurité et détecte des comportements anormaux, des tentatives d’intrusion ou des vulnérabilités présentes sur les serveurs et postes supervisés. Sa mise en œuvre permet d’obtenir une visibilité globale sur l’état de sécurité de l’infrastructure, tout en facilitant la conformité et le suivi des incidents grâce à des règles de détection et des tableaux de bord centralisés. Wazuh permet ainsi de renforcer la protection des serveurs physiques ou virtuels, d’améliorer la réactivité face aux cyberattaques et de mieux sécuriser les données sensibles de l’entreprise.

2. Origines de Wazuh

Wazuh s’inscrit dans la logique des solutions open source dédiées à la supervision de sécurité et à la détection des menaces sur les systèmes d’information. Son développement répond au besoin de disposer d’une plateforme centralisée capable de collecter les journaux, d’analyser les événements de sécurité et de détecter rapidement les comportements suspects sur les machines supervisées.

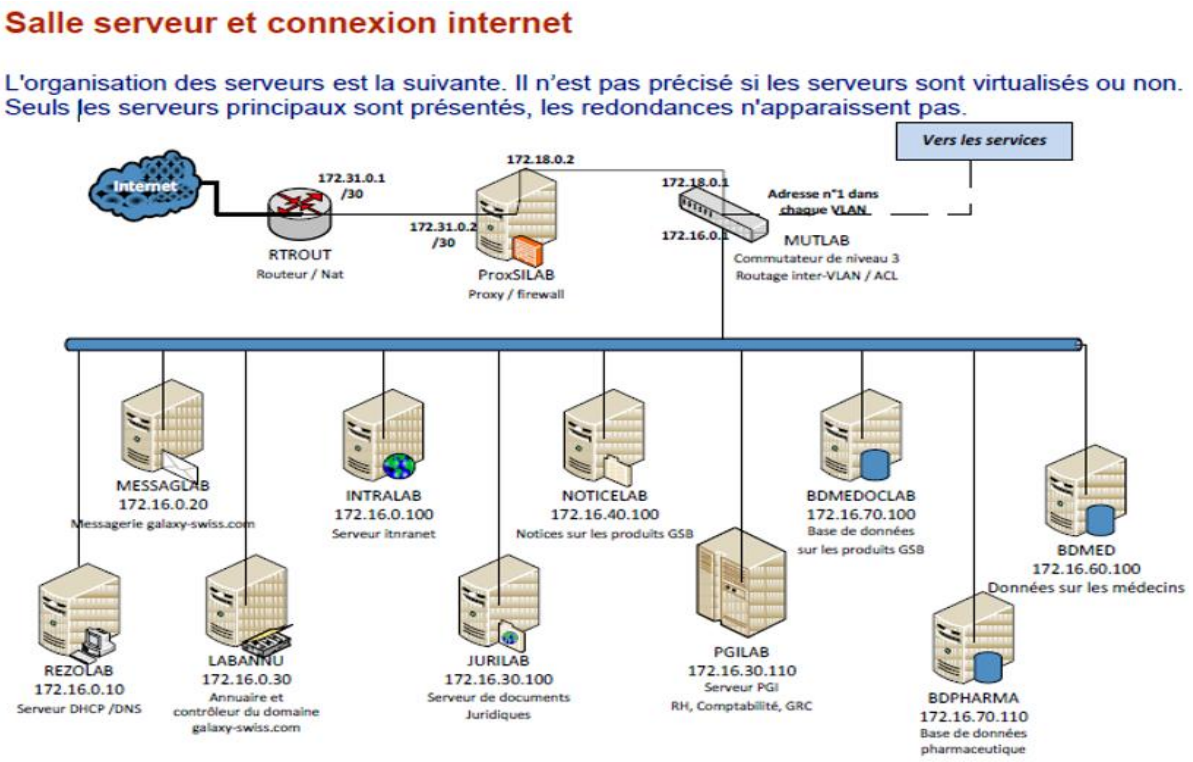
Contrairement à un simple outil de collecte de logs, Wazuh a été pensé pour renforcer la protection des infrastructures grâce à des fonctions de détection d’intrusion, d’analyse de vulnérabilités et de conformité. Son architecture de type Manager/Agent permet de superviser efficacement un grand nombre d’équipements tout en centralisant les alertes au sein d’une même interface.

3. Les avantages de Wazuh

- **Visibilité et centralisation :** L'interface unifiée permet de regrouper la collecte de logs, la détection d'intrusions et l'analyse de vulnérabilités sur une seule plateforme, simplifiant ainsi la gestion quotidienne de la sécurité.
- **Réponse automatisée (Active Response) :** En cas de détection d'une menace ou d'un comportement anormal, Wazuh peut exécuter automatiquement des actions correctives (comme le blocage d'une adresse IP malveillante), réduisant considérablement le temps de réaction.
- **Flexibilité et couverture étendue :** Qu'il s'agisse d'environnements physiques, virtuels ou cloud, Wazuh s'adapte facilement. Ses agents légers et multiplateformes (Linux, Windows, macOS) en font un choix idéal pour sécuriser l'ensemble d'un parc informatique hétérogène.

IV. Infrastructure

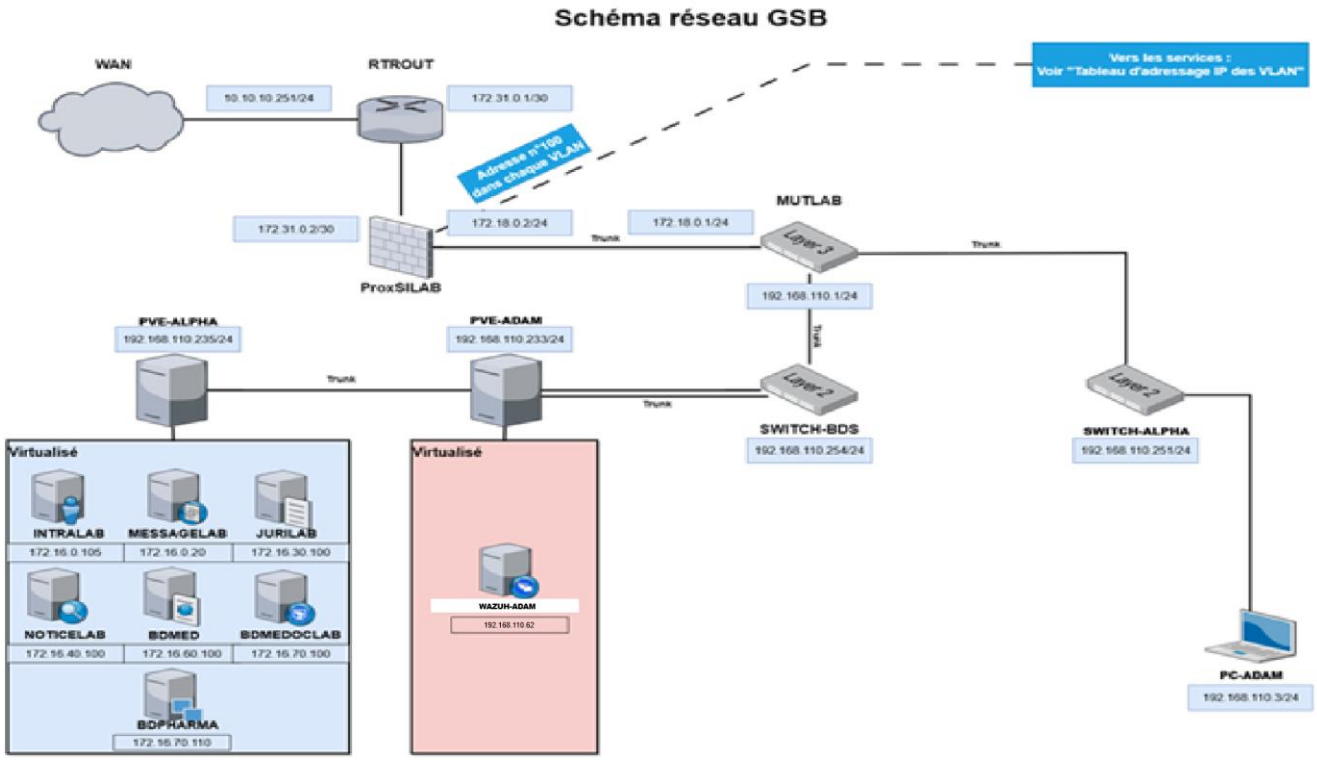
1. Schéma réseau actuel



2. Tableau d'Adressage IP des VLAN

VLAN	Service(s)	Passerelle VLAN
110	Réseau & Système	192.168.110.0/24
20	Direction / DSI	192.168.20.0/24
30	RH / Compta / Juridique / Secrétariat	192.168.30.0/24
40	Communication / Rédaction	192.168.40.0/24
50	Développement	192.168.50.0/24
60	Commercial	192.168.60.0/24
70	Labo-Recherche	192.168.70.0/24
100	Accueil	192.168.100.0/24
150	Visiteurs	192.168.150.0/24
200	Démonstration	192.168.200.0/24
300	Serveurs	172.16.0.0/17
400	Sortie	172.18.0.0/30

3. Schéma réseau de la réalisation professionnelle



4. Matériel à disposition

Dans la mise en place de ma réalisation professionnelle, voici le matériel mis à ma disposition par le groupe GSB :

- **Cisco Catalyst 3560G (MUTLAB)**
- **Cisco Catalyst 3750G (SW-RS-ALPHA)**
- **Cisco Catalyst 2960-S (SWITCH-BDS)**
- **Un routeur Cisco (RTROUT)**
- **Un routeur/pare-feu pfSense (ProxSilab)**
- **Hyperviseur de type 1 (PVE-ALPHA)**
- **Hyperviseur de type 1 (PVE-ADAM)**
- **Un point d'accès Wi-Fi**

V. Mise en place de Wazuh

1. Installation

1. Configuration de ma VM DEBIAN-ADAM

Sur une VM Debian 13 existante sur mon environnement, je créé un utilisateur wazuh

‘adduser wazuh’

```
root@DEBIAN-ADAM:~# adduser wazuh
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour wazuh
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Is the information correct? [Y/n]
```

J’ajoute cet utilisateur au groupe sudo

‘usermod -aG sudo wazuh’

```
root@DEBIAN-ADAM:~# usermod -aG sudo wazuh
```

2. Renommage la VM

Je lui attribue un nouveau nom pour la différencier des autres VMs. Pour ce faire, j'édite les fichier '/etc/hosts' et '/etc/hostname' :

```
wazuh@DEBIAN-ADAM:~$ sudo nano /etc/hosts
```

```
  GNU nano 8.4                                                /etc/hosts *
127.0.0.1       localhost
127.0.1.1       WAZUH-ADAM.gsb.lan      WAZUH-ADAM

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
wazuh@DEBIAN-ADAM:~$ sudo nano /etc/hostname
```

```
  GNU nano 8.4                                          /etc/hostname *
WAZUH-ADAM
```

3. Configuration d'une adresse IP fixe

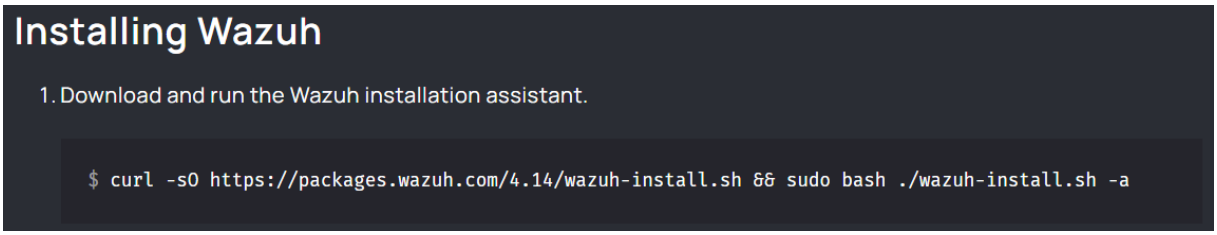
Pour que ma nouvelle VM ait une adresse IP fixe, je modifie la configuration réseau. J'ajuste les paramètres réseau dans le fichier `/etc/network/interfaces` :

```
wazuh@DEBIAN-ADAM:~$ sudo nano /etc/network/interfaces
```

```
  GNU nano 8.4                                  /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
        address 192.168.110.70
        gateway 255.255.255.0
        dns-nameserver 192.168.110.101 8.8.8.8 1.1.1.1
```

4. Installation d'Ansible

Je vais ensuite procéder à l'installation de Wazuh sur la VM. Afin d'obtenir la version la plus récente, je suis les recommandations d'installation sur la documentation d'Ansible :



J'utilise les commandes suivantes afin de compléter mon installation :

apt update && apt upgrade -y

```
wazuh@WAZUH-ADAM:~$ sudo apt update && sudo apt upgrade -y
Atteint : 1 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 2 http://deb.debian.org/debian trixie InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
49 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
Mis à jour :
  apache2          e2fsprogs          libext2fs2t64          openssh-client
  apache2-bin      grub-common        libfreetype6           openssh-server
  apache2-data     grub-pc            libgnutls30t64         openssh-sftp-server
  apache2-doc      grub-pc-bin        libpng16-16t64         openssl
  apache2-utils    grub2-common       libsqlite3-0           openssl-provider-legacy
  base-files       ifupdown           libss2                 python3-requests
  bash             inetutils-telnet   libssl3t64             python3-urllib3
  bind9-dnsutils   libc-bin           libtiff6               sqv
  bind9-host       libc-l10n          linux-base             sudo
  bind9-libs       libc6              linux-image-amd64      tzdata
  busybox          libcap2            linux-sysctl-defaults
  dhcpcd-base      libcap2-bin        locales
  dpkg             libcom-err2        logsave
```

curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -asudo apt update && sudo apt install ansible

```
wazuh@WAZUH-ADAM:~$ sudo curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Note à savoir : Il faut préalablement installer curl si se n'est pas déjà fait :

sudo apt install curl

L’assistant d’installation s’occupe de tout :

```
10/04/2026 14:02:57 INFO: Starting Wazuh installation assistant. Wazuh version: 4.14.4
10/04/2026 14:02:57 INFO: Verbose logging redirected to /var/log/wazuh-install.log
10/04/2026 14:02:57 INFO: The recommended systems are: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Amazon Linux 2023;
 Ubuntu 16.04, 18.04, 20.04, 22.04; Rocky Linux 9.4.
10/04/2026 14:02:57 WARNING: The current system does not match with the list of recommended systems. The installation may not work prope
rly.
```

Une fois qu’il a fini, un message apparait avec l’adresse IP pour accéder à l’interface web, sans oublier l’utilisateur et le mot de passe généré automatiquement.

Je vais également désactiver les mises à jour automatiques pour éviter de causer des instabilités systèmes ou des problèmes de compatiblité avant que celles-ci ne soient stables :

```
wazuh@DEBIAN-ADAM:~$ sudo sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list
```

L’installation est maintenant terminée, je passe à la configuration.

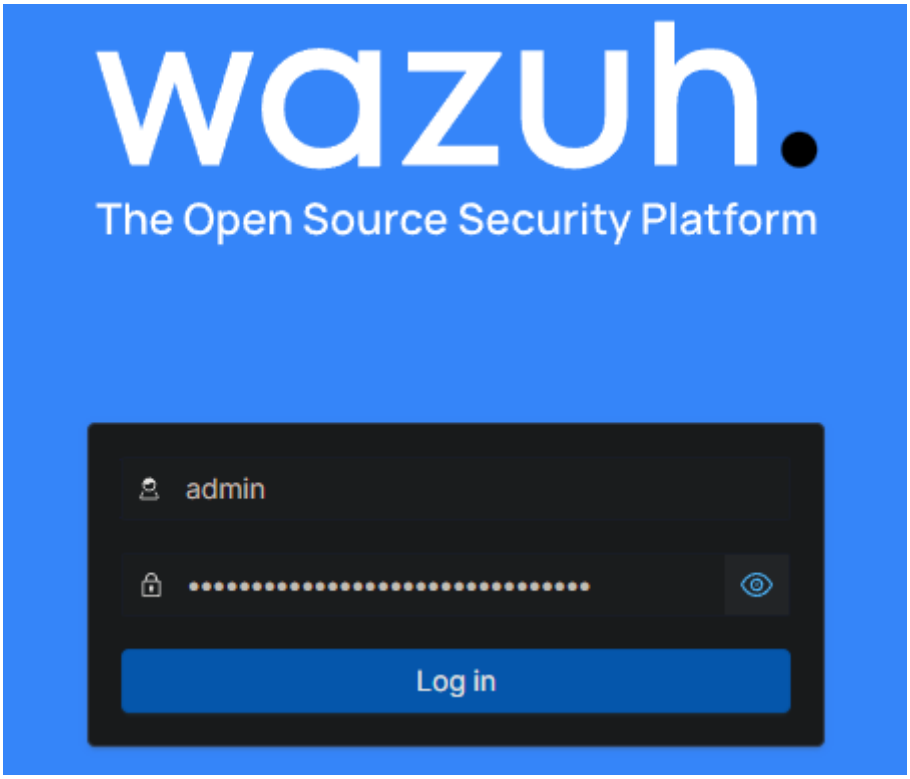
2. Configuration

1. Accès à l'interface web

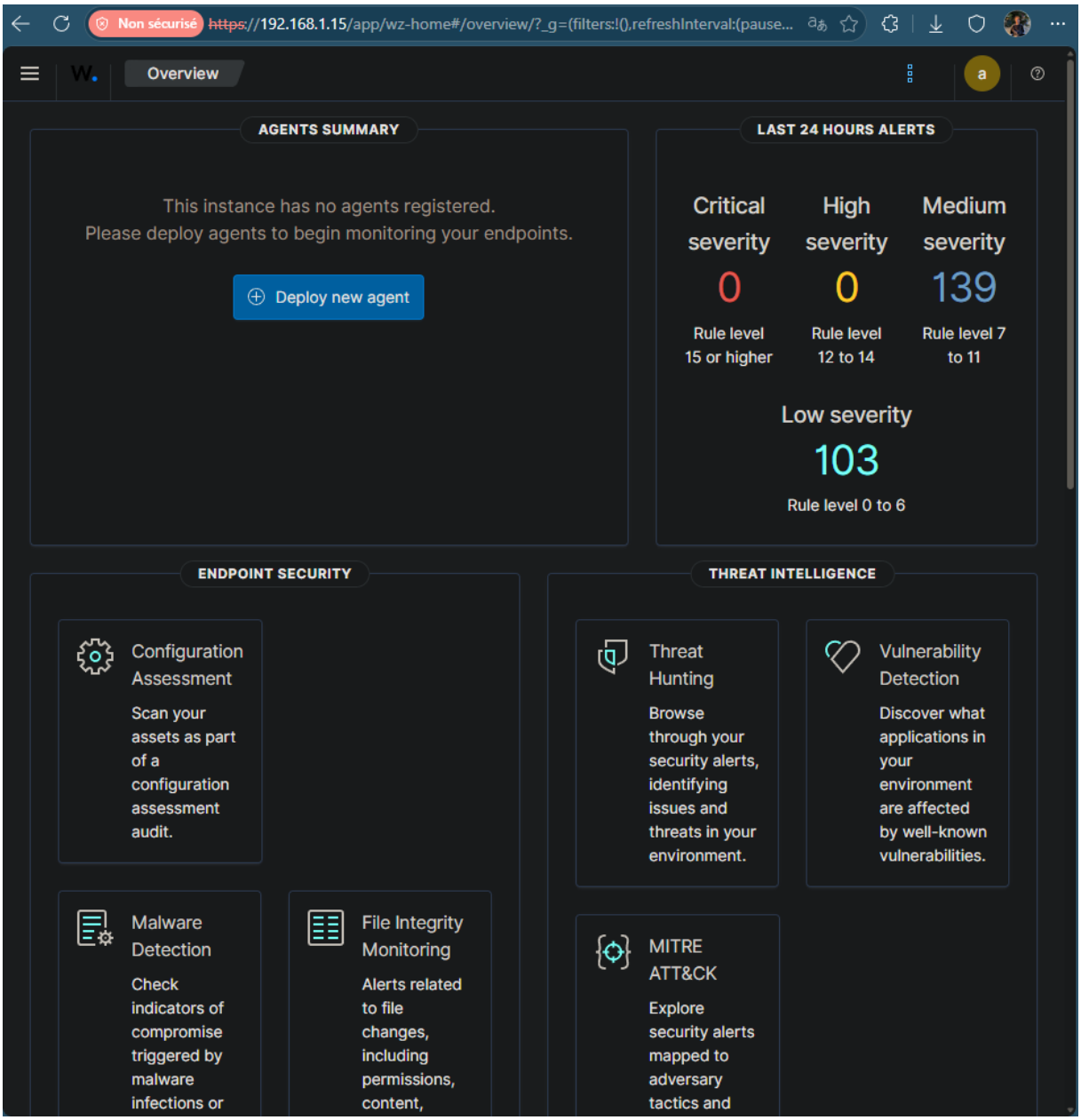
Suite à l'installation terminée, je me connecte via un navigateur internet avec l'IP du serveur Wazuh :

2. Connexion à l'interface

Je rentre ensuite le nom d'utilisateur et le mot de passe qu'on m'a donné durant l'installation :



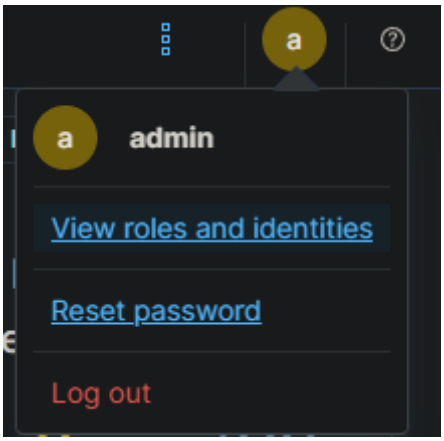
Une fois connecté, Wazuh se présente comme ceci :



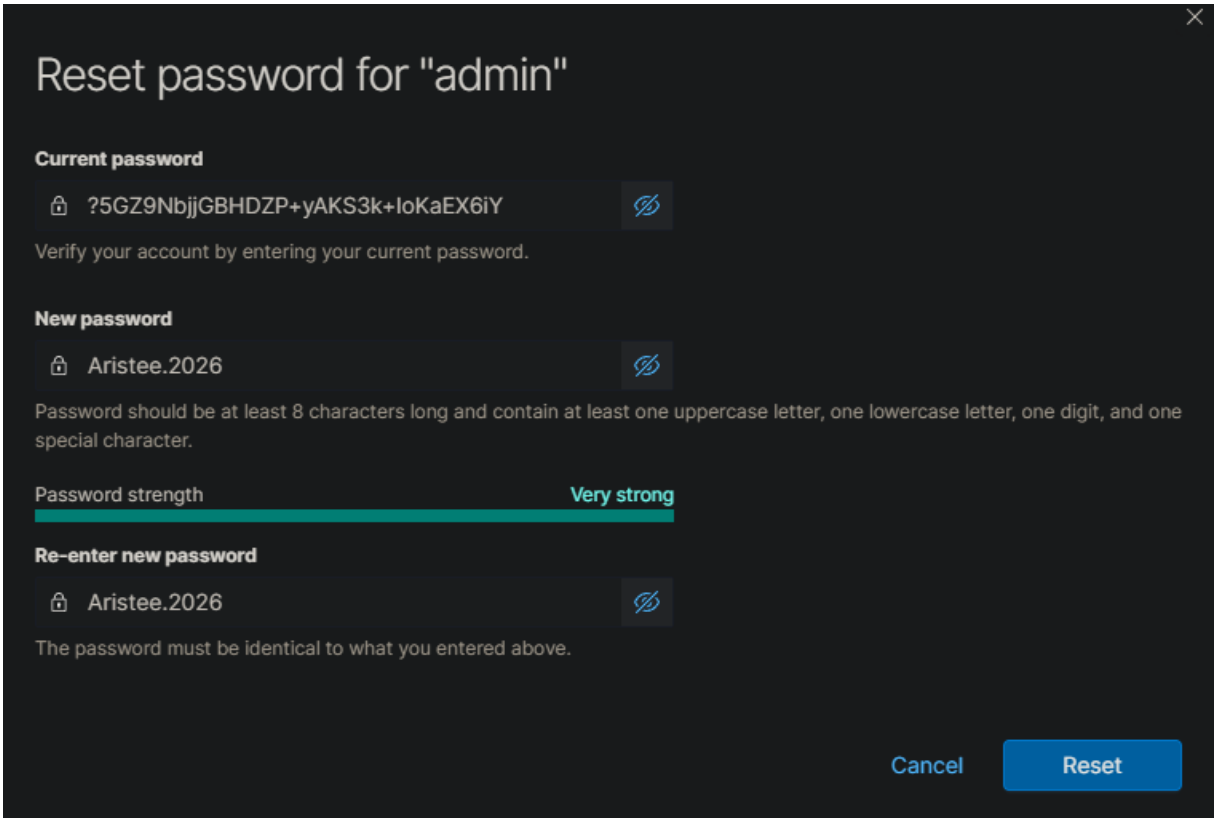
3. Changer le mot de passe

Imaginons que le mot de passe ne soit pas rigide, ou à contrario beaucoup trop compliqué à retenir comme ici, je vais changer le mot de passe par défaut.

Cliquer en haut à droite sur l'icône utilisateur :



Et tout simplement changer le mot de passe par 'Aristee.2026' :



Je peux aussi voir grâce à une commande la liste des utilisateurs et leur mot de passe en cas d'un oubli total sur un compte 'important', comme un administrateur par exemple :

```
wazuh@DEBIAN-ADAM:~$ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
[sudo] Mot de passe de wazuh :
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: '?5GZ9NbjjGBHDZP+yAKS3k+IoKaEX6iY'

# Anomaly detection user for the web user interface
  indexer_username: 'anomalyadmin'
  indexer_password: 'y2V76R3O?*XymUFwTgTOMt4RKcuv++Y0'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
  indexer_username: 'kibanaserver'
  indexer_password: 'CKac*NUn*3HIK03gZl5*G+0WaIMgV9P4'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
  indexer_username: 'kibanaro'
  indexer_password: 'wIxDkoT1nU0RPqmUqDP1+14nwx4YGgn*'

# Filebeat user for CRUD operations on Wazuh indices
  indexer_username: 'logstash'
  indexer_password: 'CVlL5iY9.+N1Qg8KbIrfMIU?.yMF6EvV'

# User with READ access to all indices
  indexer_username: 'readall'
  indexer_password: '.0W0mFs*aJ59oj5AX5JOe1mN3KEWf?*H'

# User with permissions to perform snapshot and restore operations
  indexer_username: 'snapshotrestore'
  indexer_password: '?my6sF8v0nr.TP.brzGHGfsq3J9m6qkz'

# Password for wazuh API user
  api_username: 'wazuh'
  api_password: 'xO+1Vawt?+7LlJm.PBfCLQxRS61EbeEE'

# Password for wazuh-wui API user
  api_username: 'wazuh-wui'
  api_password: 'Md4q0EYAjyYO8q8yYtxN+h?78x0QkAVj'
```

3. Test

1. Ajouter le dépôt Wazuh

Pour déployer et installer l'agent Wazuh sur une autre machine, ici une VM sous Debian 13, je dois d'abord passer par quelques étapes :

Installer les paquets suivants s'il en manque : apt-get install gnupg apt-transport-https

Installer la clé GPG : 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

```
root@DEBIAN-ADAM:~# 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
gpg: répertoire « /root/.gnupg » créé
gpg: /root/.gnupg/trustdb.gpg : base de confiance créée
gpg: clef 96B3EE5F29111145 : clef publique « Wazuh.com (Wazuh Signing Key) <support@wazuh.com> » importée
gpg:       Quantité totale traitée : 1
gpg:                    importées : 1
```

Ajouter le dépôt : 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

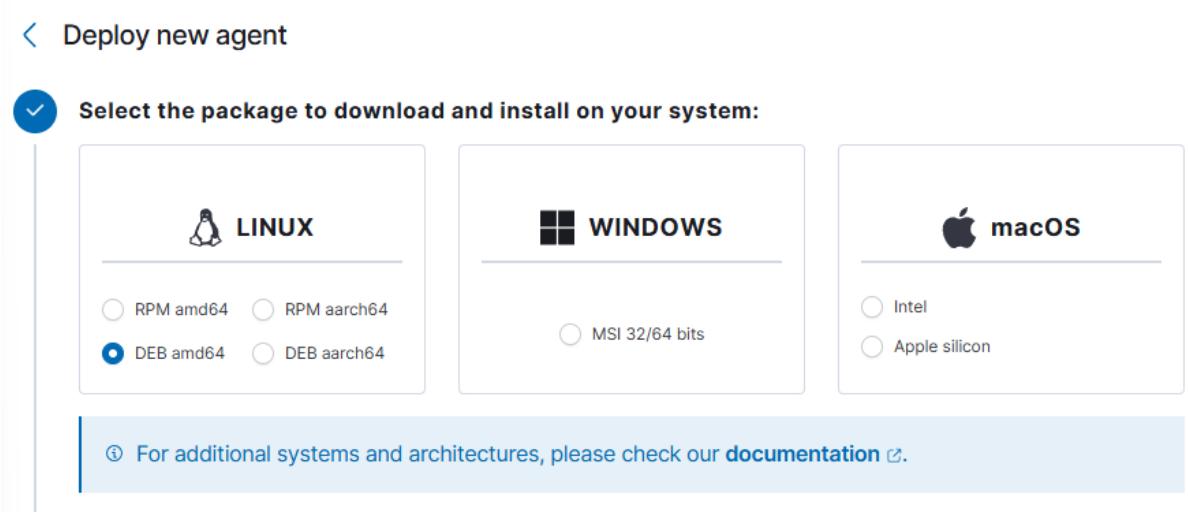
```
root@DEBIAN-ADAM:~# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" |
 tee -a /etc/apt/sources.list.d/wazuh.list
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
```

Puis mettre à jour les informations des paquets : apt update

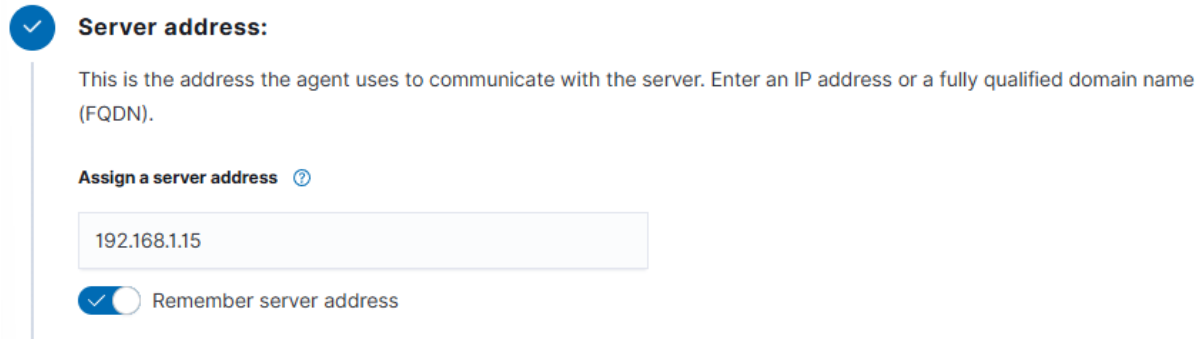
2. Configurer l'agent Wazuh

Dans le menu déroulant en haut à gauche de l'interface web, je vais dans 'Agents management' puis dans 'Summary'. Je clique sur déployer un nouvel agent, et je paramètre la bonne configuration.

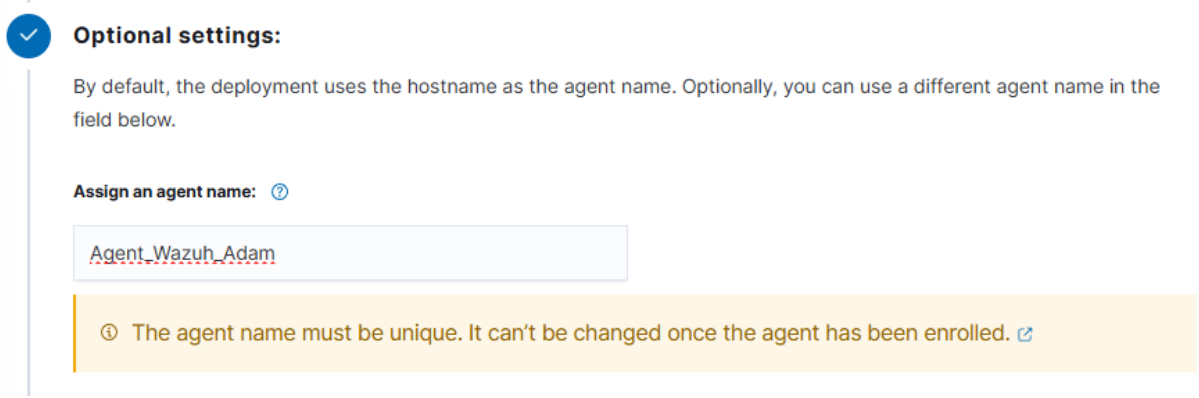
Dans un premier temps, choisir le système d'exploitation



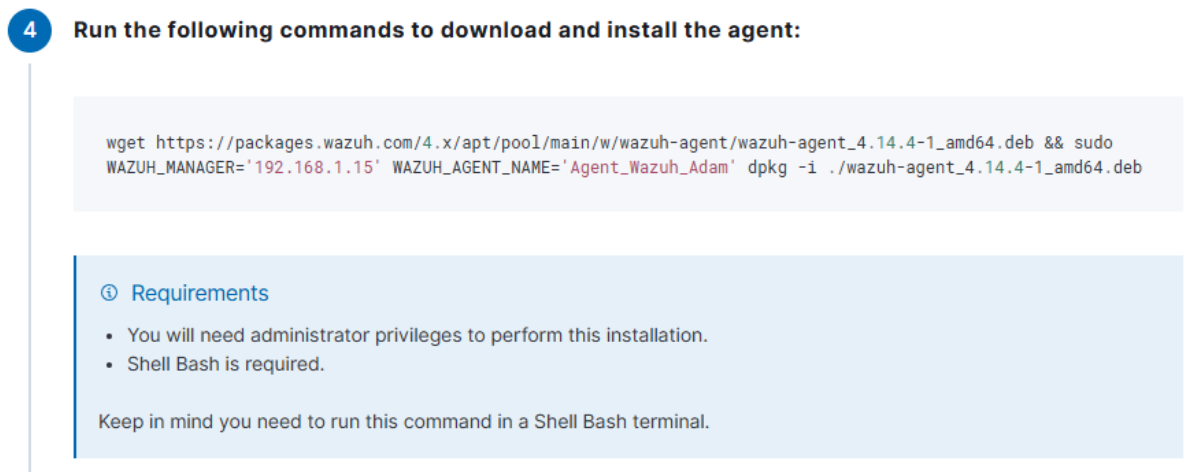
Renseigner l'adresse du serveur Wazuh (pour l'exemple, je vais mettre 192.168.1.15)



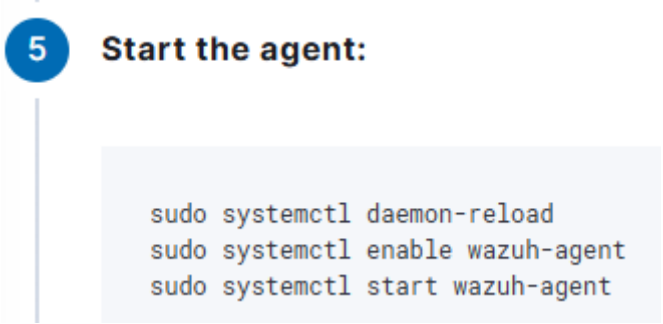
Je peux personnaliser le nom de l'agent lors de sa création si je le souhaite



Puis j'obtiens une commande personnalisée avec ce que j'ai enseigné précédemment



Et pour finir, l'activation / redémarrage des services pour l'Agent Wazuh



Je vais maintenant déployer l'agent Wazuh sur cette même VM Debian. Il faut absolument changer l'IP de la commande en mettant celle qui correspond au serveur Wazuh. Je peux même changer le nom de l'agent, ici 'WAZUH_MANAGER', mais je le laisse tel quel :
WAZUH_MANAGER="10.0.0.2" apt-get install wazuh-agent

```
root@DEBIAN-ADAM:~# WAZUH_MANAGER="192.168.110.70" apt-get install wazuh-agent
```

Puis je vais activer et relancer le service d'agent Wazuh :

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

```
root@DEBIAN-ADAM:~# systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-agent.service' → '/usr/lib/systemd/system/wazuh-agent.s
ervice'.
```

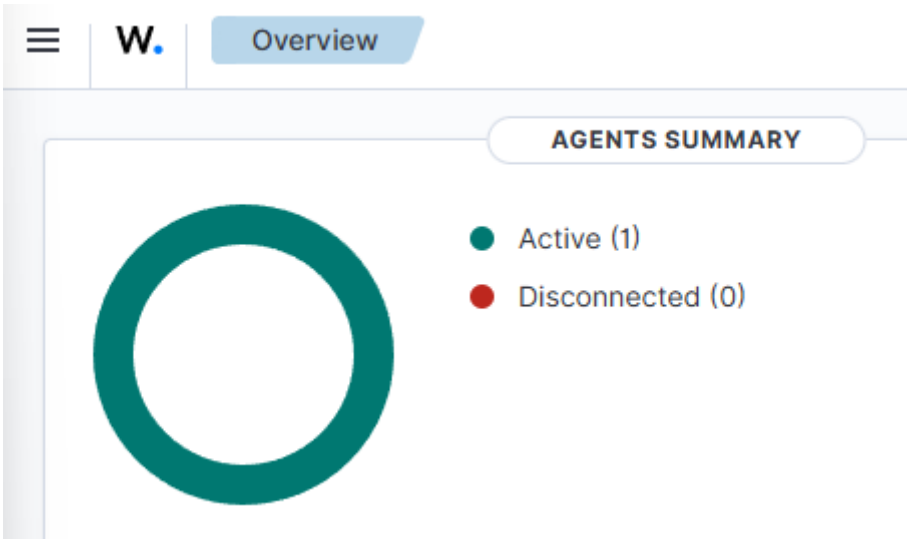
Et comme sur le serveur Wazuh, je vais désactiver les mises à jour automatiques pour garder une stabilité système, puis actualiser la liste :

sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
apt-get update

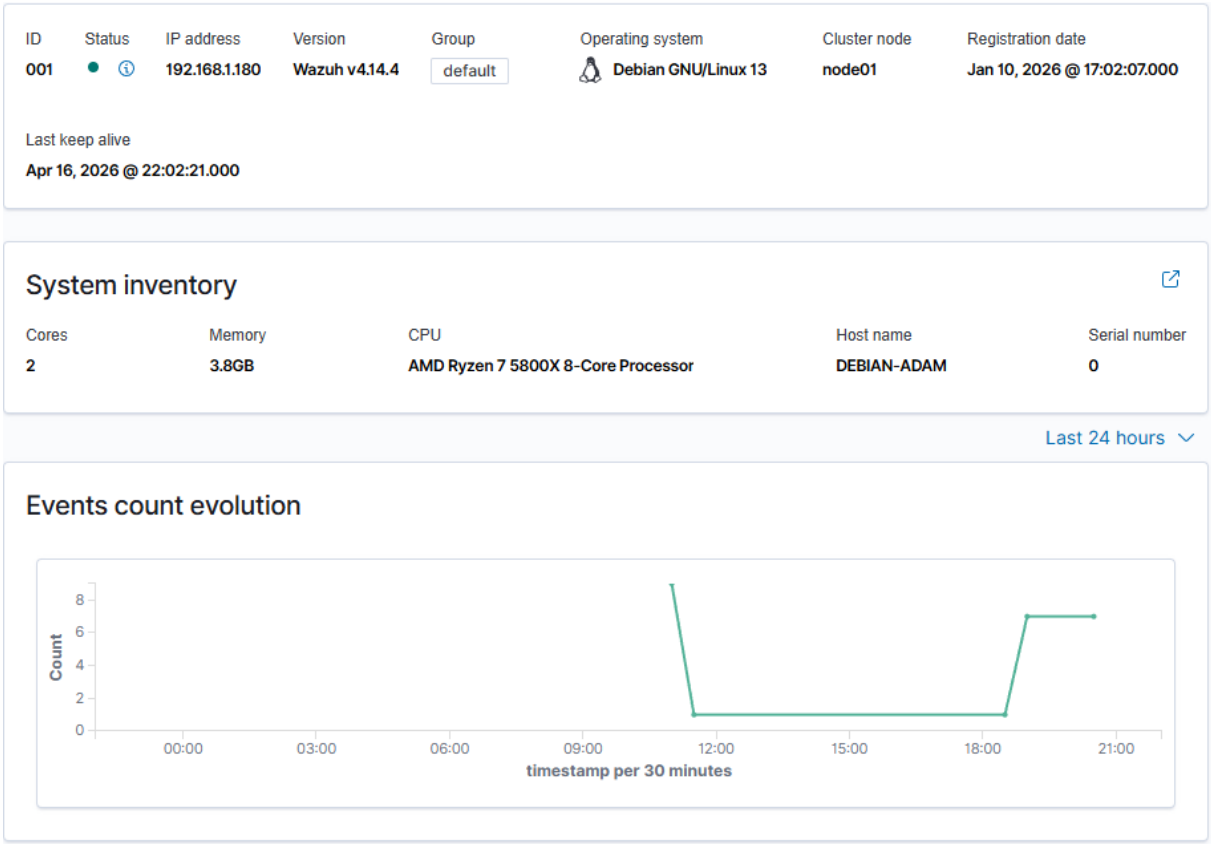
```
root@DEBIAN-ADAM:~# sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
apt-get update
Atteint : 1 http://security.debian.org/debian-security trixie-security InRelease
Atteint : 2 http://deb.debian.org/debian trixie InRelease
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease
Lecture des listes de paquets... Fait
```

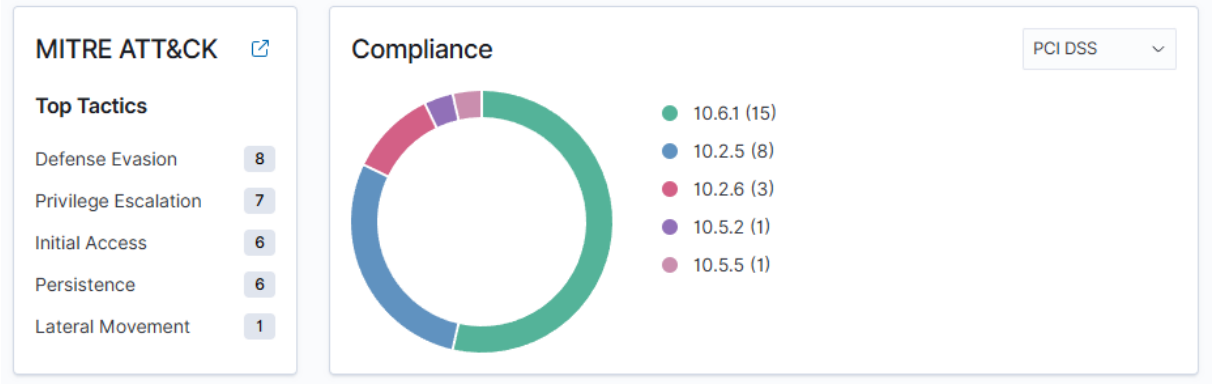
3. Résultat des données de l'agent

Maintenant, quand je suis sur la page d'accueil du site, je peux voir qu'il y a un agent actif



En cliquant dessus, je peux donc voir des informations sur ma machine :





Vulnerability Detection

0 Critical

57 High

104 Medium

1 Low

Top 5 Packages

Package	Count ↓
linux-image-amd64	348
amd64-microcode	10
vim-common	6
vim-tiny	6
libde265-0	2

Security Configuration Assessment

Policy	End scan	Passed	Failed	Not applic...	Score
Center for Internet Security Debian Linux 13 Benchmark	Apr 16, 2026 @ 19:08:45.000	67	115	25	36%

< 1 >

VI. Évolution possible

1. Mise en place de la réponse automatisée (Active Response)

En activant et configurant le module Active Response de Wazuh, GSB peut automatiser la réaction immédiate face aux menaces détectées sur ses serveurs et postes de travail. Cela inclut le déclenchement de scripts correctifs dès qu'une alerte critique est levée, comme le blocage automatique d'une adresse IP malveillante au niveau du pare-feu, la suspension d'un compte utilisateur suspect ou l'arrêt d'un processus lié à un logiciel malveillant.

Intérêts pour GSB :

- Réduire drastiquement le temps de réaction face aux cyberattaques sans attendre l'intervention humaine.
- Limiter les risques de propagation d'une menace (comme un ransomware) sur le reste du réseau d'entreprise.
- Garantir une protection continue (24h/24) des serveurs critiques hébergeant les données de recherche et de santé du laboratoire.

VII. Conclusion

L'adoption de Wazuh au sein du laboratoire Galaxy Swiss Bourdin (GSB) s'avère être une décision stratégique, permettant de superviser efficacement la sécurité du système d'information, de détecter les menaces et d'analyser les vulnérabilités.

Cette solution permet de centraliser les journaux et les alertes de sécurité, tout en améliorant la réactivité face aux incidents grâce à une surveillance continue des serveurs et des équipements.

En définitive, Wazuh se positionne comme un levier essentiel pour renforcer la sécurité, protéger les données sensibles et améliorer la qualité de service au sein de l'infrastructure GSB