Ecole Normale Supérieure de l'Enseignement Technique Mohammedia
Université Hassan II de Casablanca
ENSET
المدرسة العليا لأساتذة التعليم التقني المحمدية
جامعة الحسن الثاني بالدار البيضاء

Projet de Fin Module

Implémentation du Atelier Sécurité

Projet de Atelier Sécurité des endpoints et supervision SIEM

Réalisé par :
Abdelali Saadali

Encadré par :
Prof. Azeddine KHIAT

Année universitaire : 2025/2026

Introduction

Dans un contexte marqué par l'augmentation des cyberattaques ciblant les infrastructures Cloud et les systèmes hétérogènes, la mise en place de solutions de supervision et de détection centralisées devient indispensable. Les entreprises modernes s'appuient de plus en plus sur des plateformes SIEM et EDR afin de garantir la visibilité, la traçabilité et la détection proactive des incidents de sécurité.

Ce projet s'inscrit dans cette logique et consiste à la mise en œuvre d'une architecture de supervision de la sécurité des endpoints basée sur Wazuh, combinant les fonctionnalités SIEM (Security Information and Event Management) et EDR (Endpoint Detection and Response). Le lab a été déployé dans un environnement AWS Learner Lab, intégrant des systèmes Linux et Windows, afin de simuler un environnement réel multi-OS.

L'objectif principal est d'observer, centraliser et analyser en temps réel les événements de sécurité générés sur différents hôtes, tout en illustrant les concepts de sécurité des endpoints, gestion des identités et des accès (IAM/PAM) et threat detection / threat hunting.

1. Architecture générale du lab :

L'architecture du lab repose sur une infrastructure Cloud simple mais réaliste, composée de trois instances EC2 déployées dans le même VPC AWS.

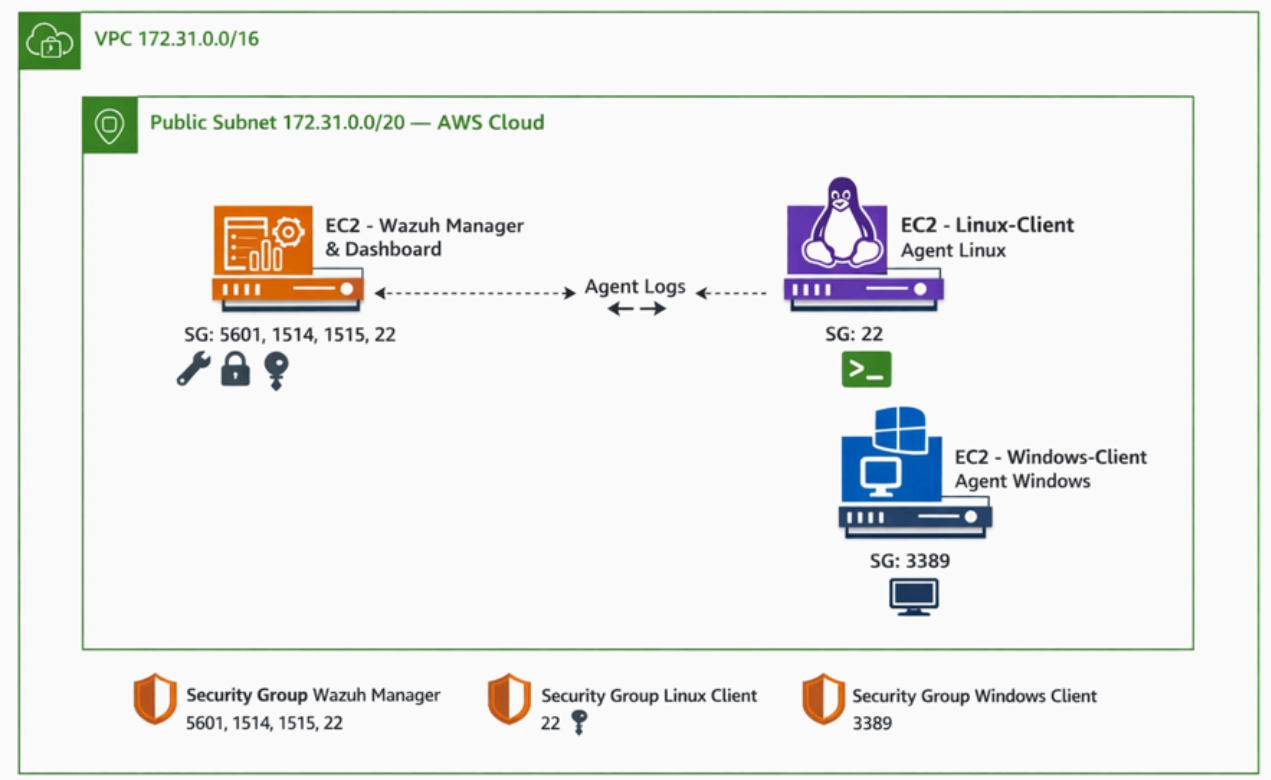
1.1 Composants de l'architecture :

- EC2-1 : Serveur Wazuh (Ubuntu 24.04 LTS)
  - Wazuh Manager
  - Wazuh Indexer
  - Wazuh Dashboard
  - Rôle : centralisation, corrélation, analyse et visualisation des événements
- EC2-2 : Client Linux (Ubuntu 24.04)
  - Wazuh Agent
  - Rôle : génération d'événements Linux (authentification, privilèges, intégrité)
- EC2-3 : Client Windows (Windows Server)
  - Wazuh Agent
  - Rôle : génération d'événements Windows Security et EDR

1.2 Flux réseau :

Les communications entre les composants sont basées sur les ports standards Wazuh :

- 1514/TCP : communication agent → serveur
- 1515/TCP : enrôlement automatique des agents
- 443/TCP (ou 5601) : accès au Dashboard Wazuh



2. Mise en place de l'environnement AWS :

Les trois instances EC2 ont été déployées dans le même VPC et le même subnet afin de garantir la communication directe entre les agents et le serveur Wazuh.

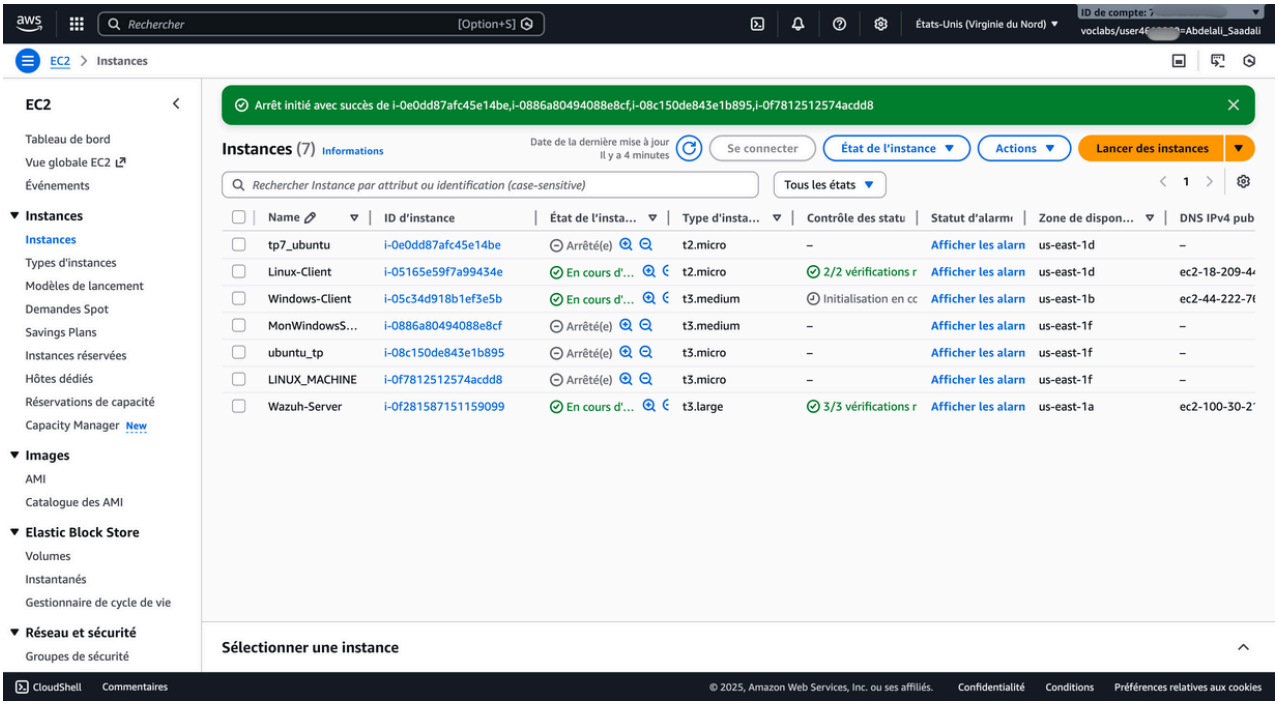
Un Security Group dédié a été configuré pour restreindre strictement les accès réseau, conformément aux bonnes pratiques de sécurité Cloud (principe du moindre privilège).

Accès SSH et RDP limités à l'adresse IP de l'administrateur

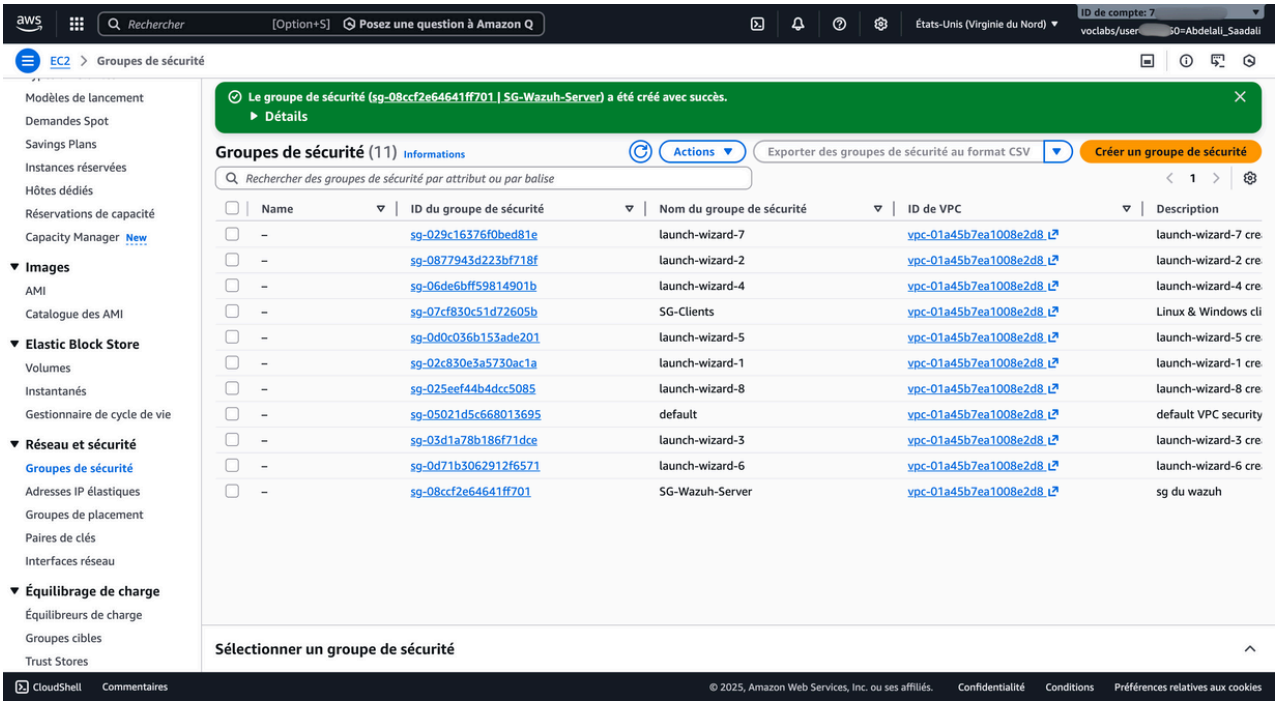
Ouverture des ports Wazuh uniquement entre les clients et le serveur

Cette configuration permet de simuler un environnement sécurisé proche d'un contexte professionnel.

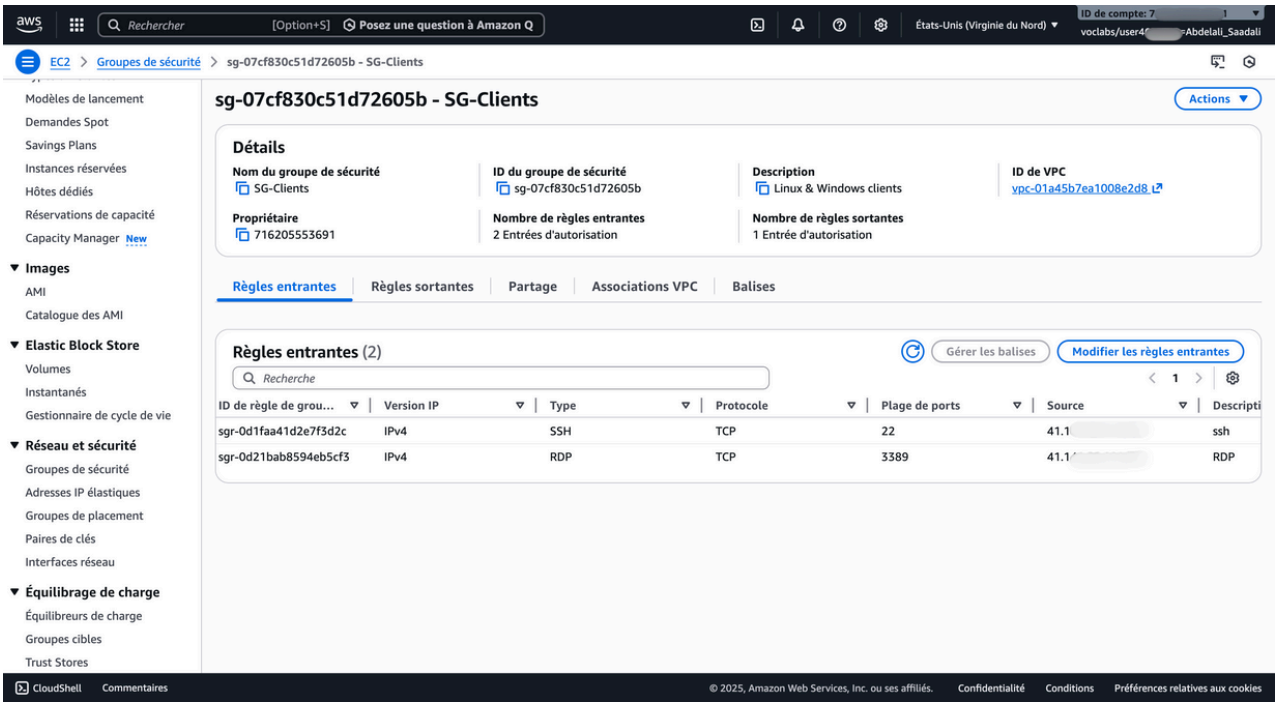
2.1 Les instances :



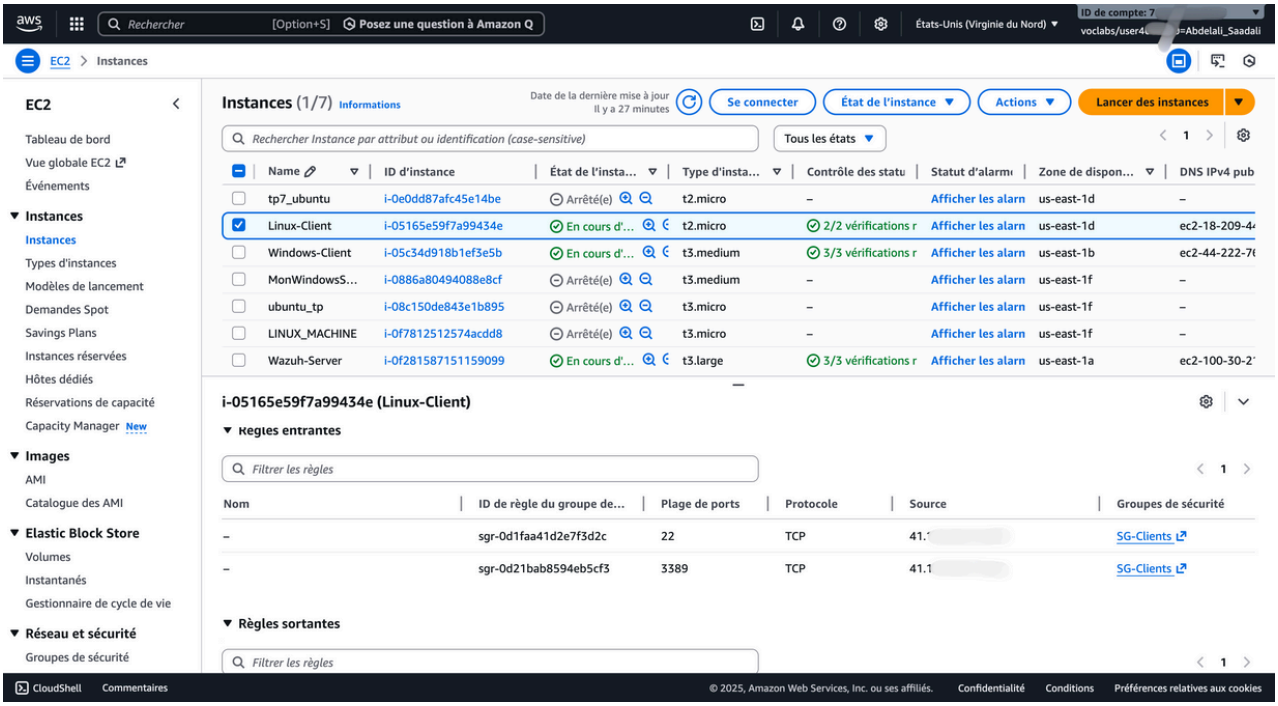
2.2 Groupe de sécurité :



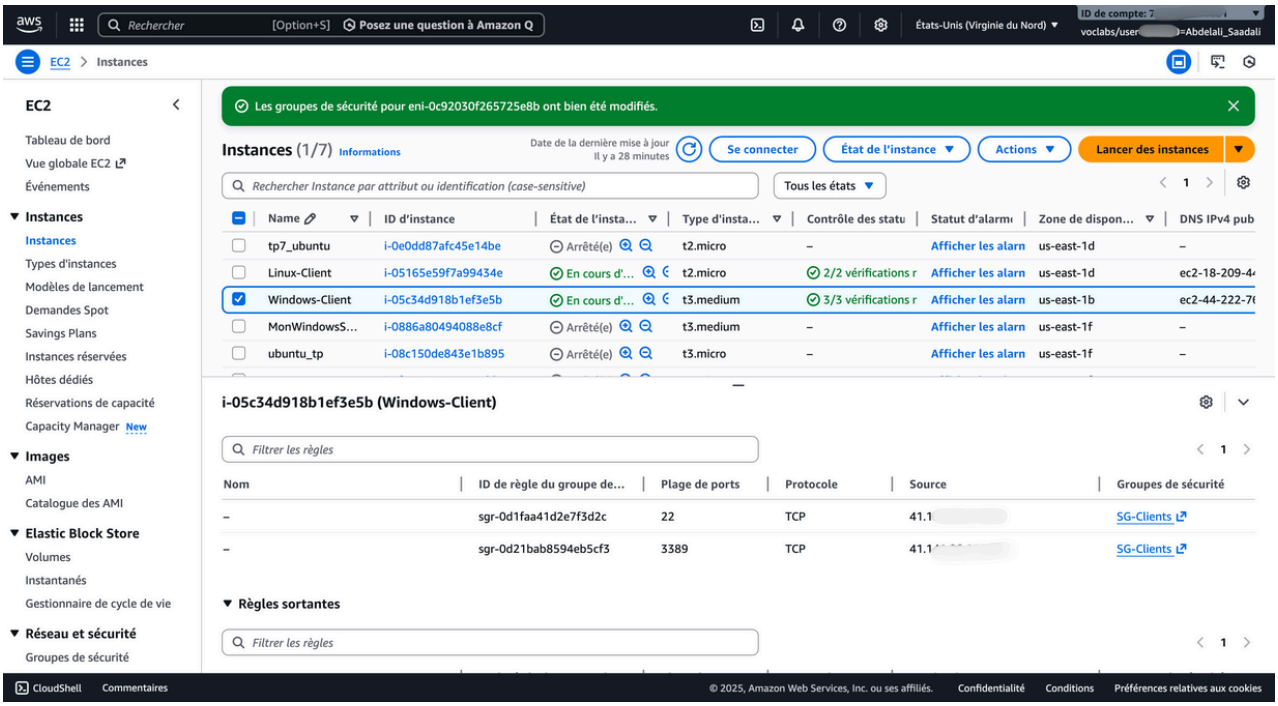
2.2.1 Groupe de sécurité des clients (Linux + Windows) :



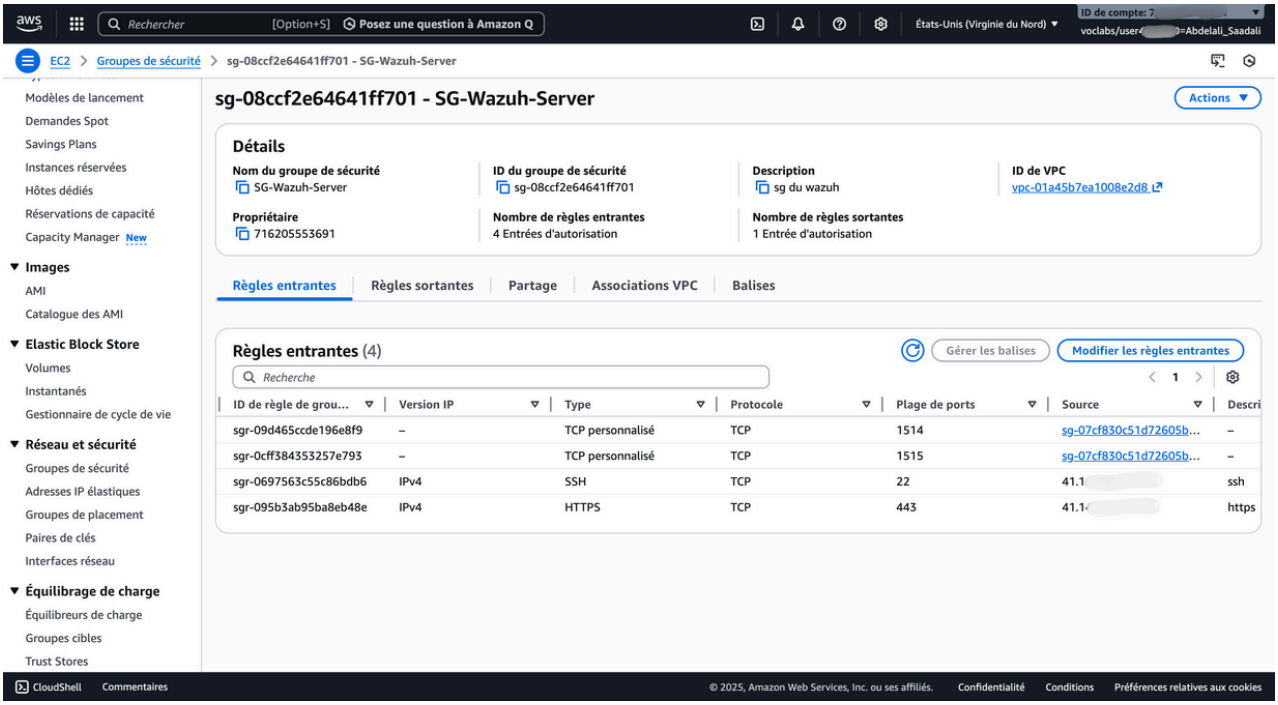
2.2.1.1 Client Linux :

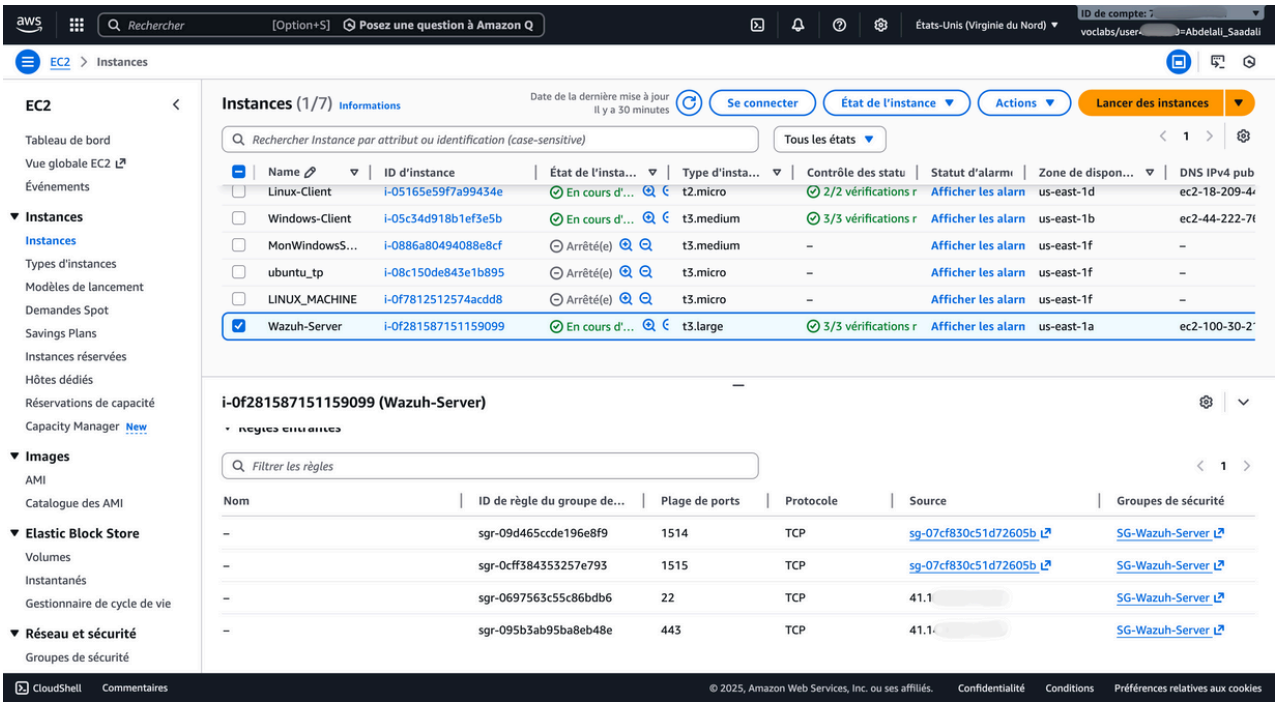


2.2.1.1 Client Windows :



2.2.2 Groupe de sécurité du seerveur Wazuh :





3. Installation de la plateforme Wazuh :

La plateforme Wazuh a été installée en mode All-in-One sur une instance Ubuntu 24.04. Cette installation regroupe le manager, l'indexer et le dashboard sur une seule machine, ce qui est adapté à un lab pédagogique.

Une fois l'installation terminée, l'accès au Dashboard Wazuh a permis de vérifier le bon fonctionnement des services et de commencer l'enrôlement des agents.

3.1 Connection ssh + mise a jour au système :

```
mac@MacBook-Pro-de-Abdelali Projet_de_fin_module %  ssh -i key-Wazuh-Server.pem ubuntu@100.30.218.189
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Dec 31 20:57:41 UTC 2025

  System load:  0.0               Temperature:           -273.1 C
  Usage of /:   6.2% of 28.02GB   Processes:             111
  Memory usage: 3%                Users logged in:       0
  Swap usage:   0%                IPv4 address for ens5: 172.31.46.35

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-46-35:~$ sudo apt update && sudo apt -y upgrade
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
```

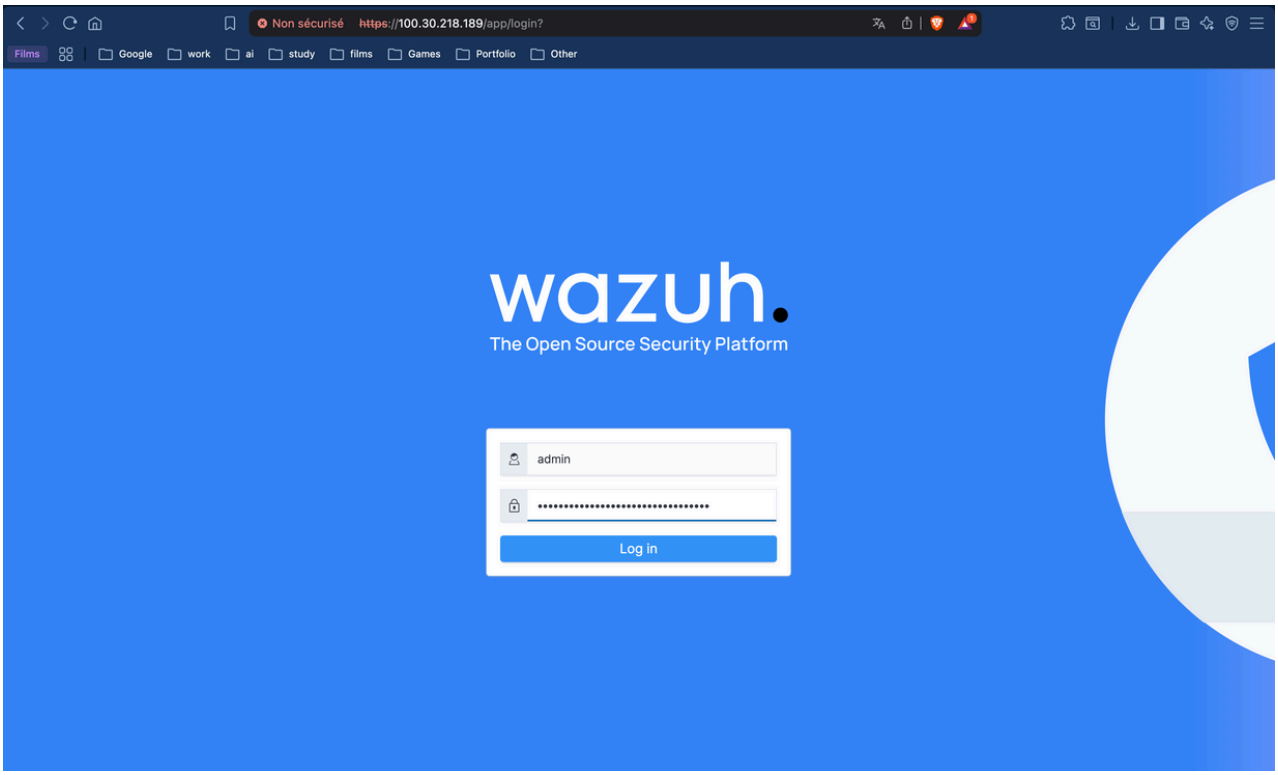
3.2 Installation du wazuh :

```
ubuntu@ip-172-31-46-35:~$ sudo bash wazuh-install.sh -a -i
31/12/2025 21:01:14 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
31/12/2025 21:01:14 INFO: Verbose logging redirected to /var/log/wazuh-install.log
31/12/2025 21:01:24 WARNING: Hardware and system checks ignored.
31/12/2025 21:01:24 INFO: Wazuh web interface port will be 443.
31/12/2025 21:01:30 INFO: --- Dependencies ----
31/12/2025 21:01:30 INFO: Installing apt-transport-https.
31/12/2025 21:01:36 INFO: Wazuh repository added.
31/12/2025 21:01:36 INFO: --- Configuration files ---
31/12/2025 21:01:36 INFO: Generating configuration files.
31/12/2025 21:01:38 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
31/12/2025 21:01:39 INFO: --- Wazuh indexer ---
31/12/2025 21:01:39 INFO: Starting Wazuh indexer installation.
31/12/2025 21:02:44 INFO: Wazuh indexer installation finished.
31/12/2025 21:02:44 INFO: Wazuh indexer post-install configuration finished.
31/12/2025 21:02:44 INFO: Starting service wazuh-indexer.
31/12/2025 21:03:05 INFO: wazuh-indexer service started.
31/12/2025 21:03:05 INFO: Initializing Wazuh indexer cluster security settings.
31/12/2025 21:03:16 INFO: Wazuh indexer cluster initialized.
31/12/2025 21:03:16 INFO: --- Wazuh server ---
31/12/2025 21:03:16 INFO: Starting the Wazuh manager installation.
31/12/2025 21:04:12 INFO: Wazuh manager installation finished.
31/12/2025 21:04:12 INFO: Starting service wazuh-manager.
31/12/2025 21:04:28 INFO: wazuh-manager service started.
31/12/2025 21:04:28 INFO: Starting Filebeat installation.
31/12/2025 21:04:38 INFO: Filebeat installation finished.
31/12/2025 21:04:38 INFO: Filebeat post-install configuration finished.
31/12/2025 21:04:38 INFO: Starting service filebeat.
31/12/2025 21:04:40 INFO: filebeat service started.
31/12/2025 21:04:40 INFO: --- Wazuh dashboard ---
31/12/2025 21:04:40 INFO: Starting Wazuh dashboard installation.
31/12/2025 21:05:26 INFO: Wazuh dashboard installation finished.
31/12/2025 21:05:26 INFO: Wazuh dashboard post-install configuration finished.
31/12/2025 21:05:26 INFO: Starting service wazuh-dashboard.
31/12/2025 21:05:26 INFO: wazuh-dashboard service started.
31/12/2025 21:06:04 INFO: Initializing Wazuh dashboard web application.
31/12/2025 21:06:05 INFO: Wazuh dashboard web application initialized.
31/12/2025 21:06:05 INFO: --- Summary ---
31/12/2025 21:06:05 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: v31N87G7aytg5ZnCUZY9vN+ZZtj4NzwA
31/12/2025 21:06:05 INFO: Installation finished.
ubuntu@ip-172-31-46-35:~$
```

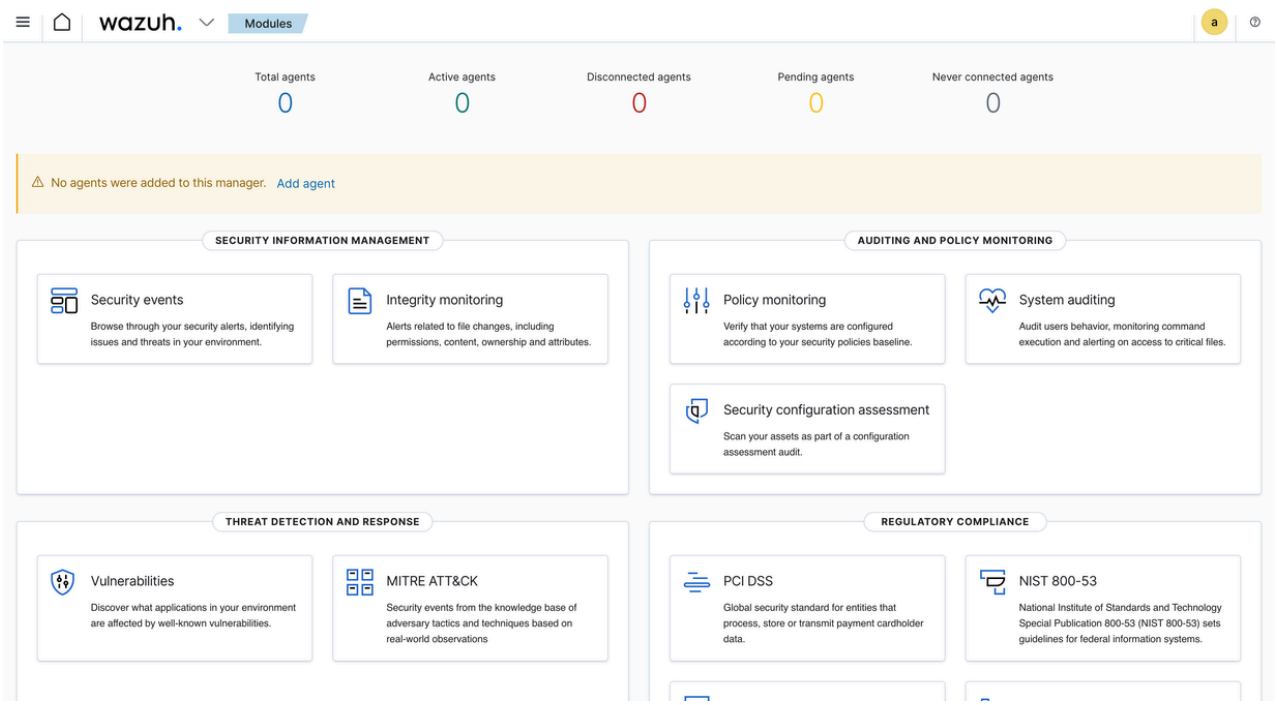
3.3 Verification :

```
Projet_de_fin_module — ubuntu@ip-172-31-46-35: ~ — ssh -i key-Wazuh...
ubuntu@ip-172-31-46-35:~$ sudo systemctl status wazuh-manager
sudo systemctl status wazuh-indexer
sudo systemctl status wazuh-dashboard
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; pr>
     Active: active (running) since Wed 2025-12-31 21:04:28 UTC; 4min 28s ago
      Tasks: 121 (limit: 9296)
     Memory: 377.0M (peak: 525.2M)
        CPU: 45.244s
     CGroup: /system.slice/wazuh-manager.service
             ├─58573 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─58612 /var/ossec/bin/wazuh-authd
             ├─58625 /var/ossec/bin/wazuh-db
             ├─58634 /var/ossec/bin/wazuh-execd
             ├─58645 /var/ossec/bin/wazuh-analysisd
             ├─58670 /var/ossec/bin/wazuh-syscheckd
             ├─58716 /var/ossec/bin/wazuh-remoted
             ├─58749 /var/ossec/bin/wazuh-logcollector
             ├─58769 /var/ossec/bin/wazuh-monitord
             ├─58771 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─58774 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             ├─58777 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr>
             └─58800 /var/ossec/bin/wazuh-modulesd
```

3.4 Login :



3.4 Dashboard :

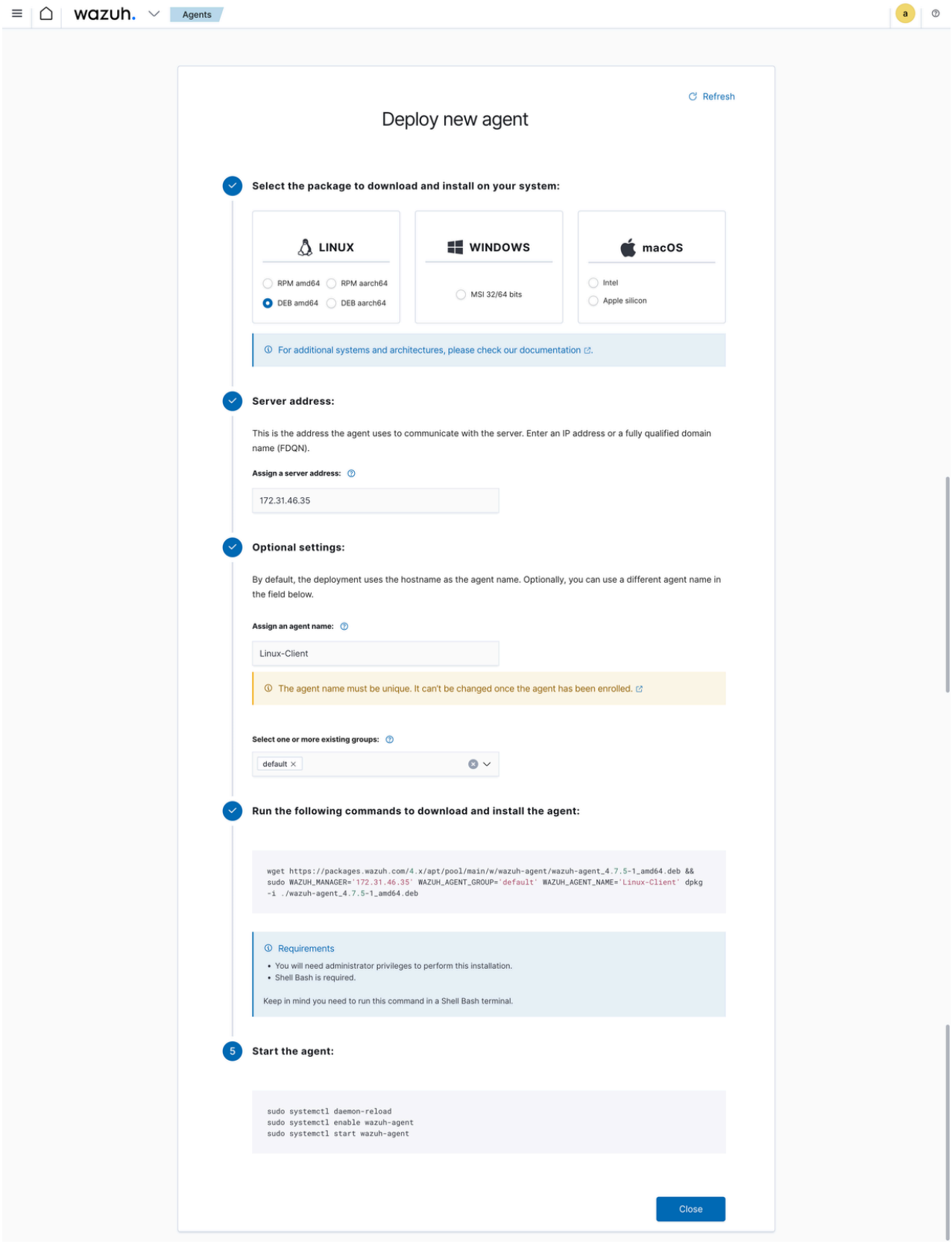


4. Enrôlement des agents Linux et Windows :

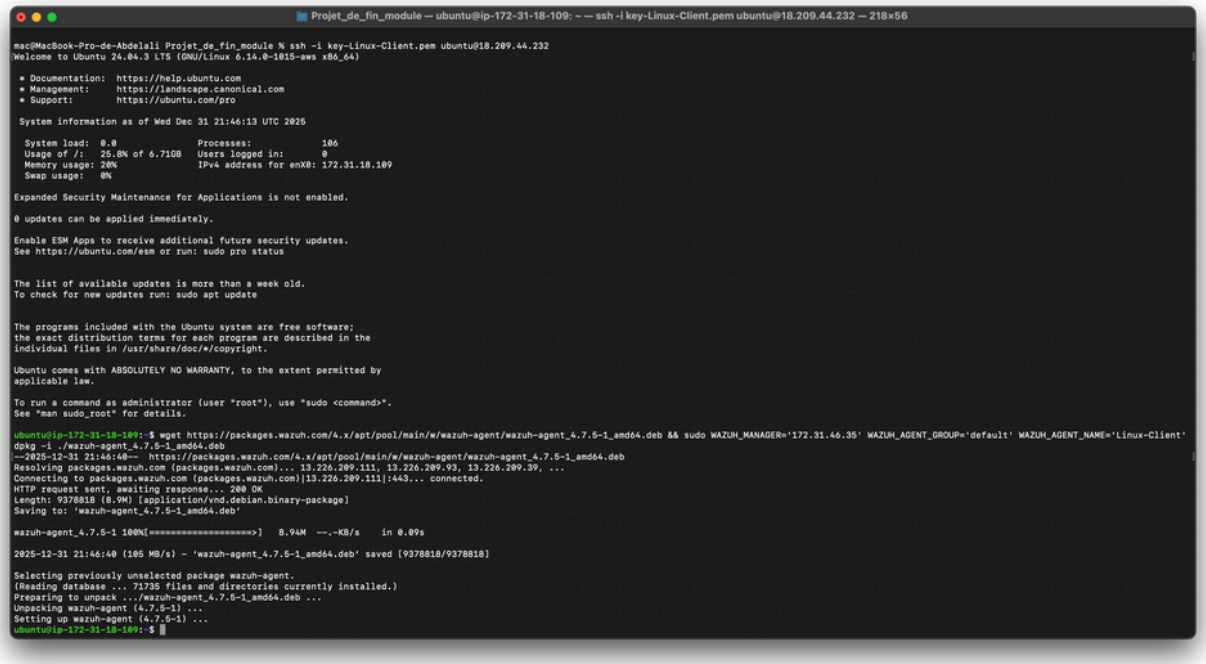
4.1 Agent Linux :

L'agent Wazuh a été déployé sur le client Linux via la fonctionnalité "Deploy new agent" du Dashboard.

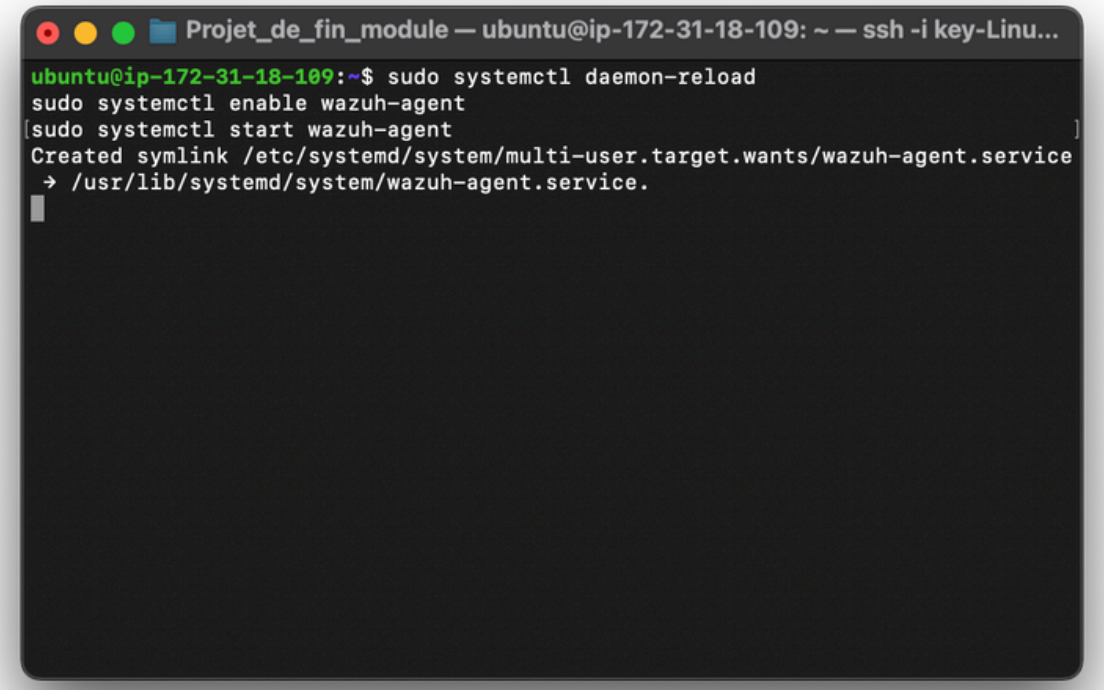
Après installation, l'agent apparaît comme actif et connecté, confirmant la bonne communication avec le serveur.



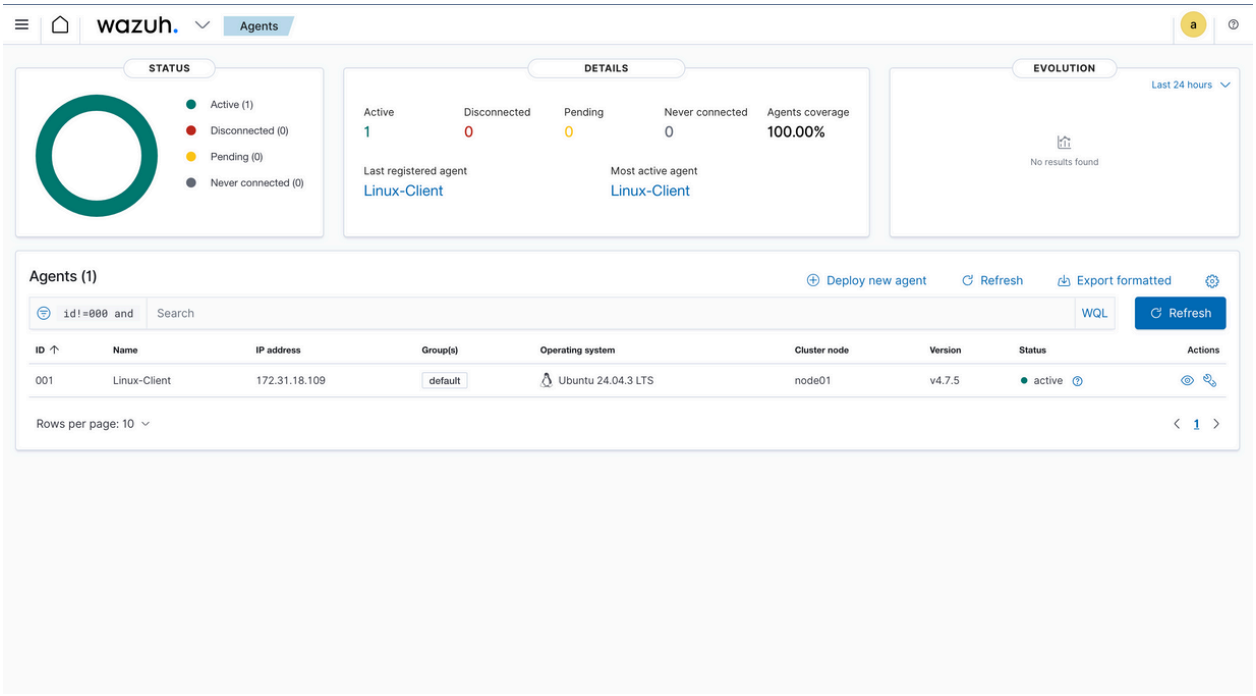
4.1.1 Installation d’agent :



4.1.2 Demmarage d’agent :



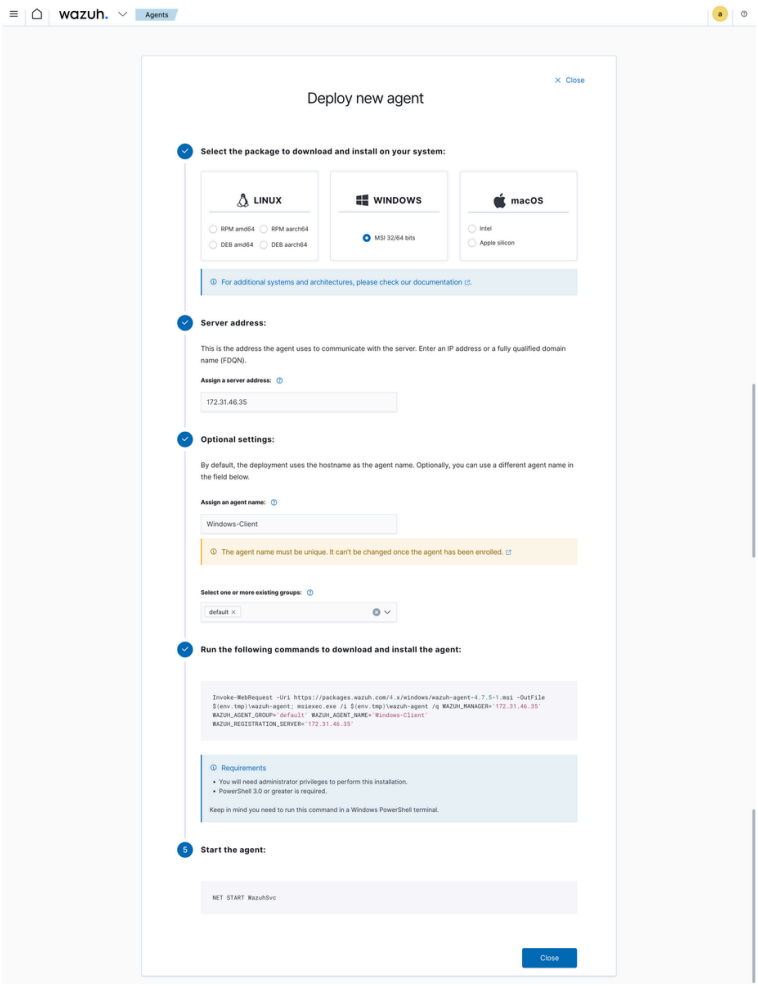
4.1.3 Affichage d’agent :



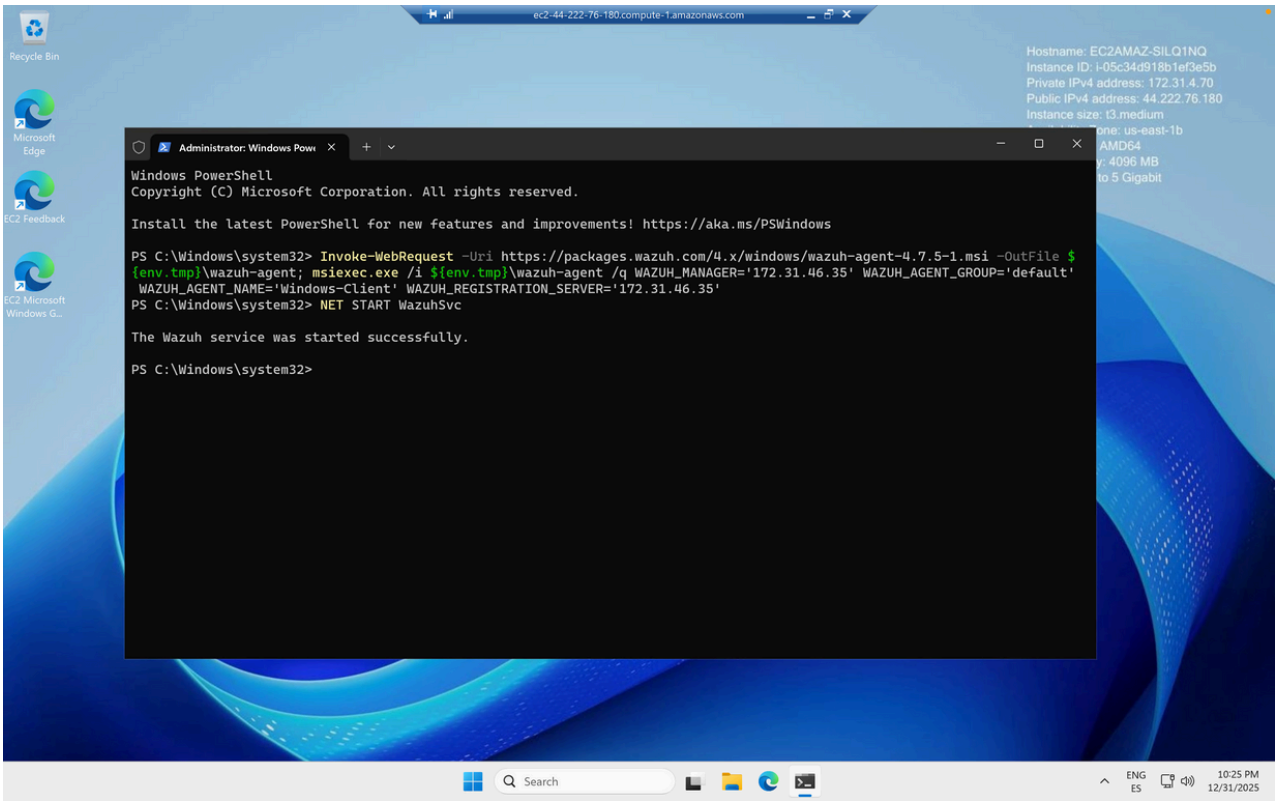
4.2 Agent Windows :

L’agent Wazuh a été installé sur le client Windows via PowerShell.

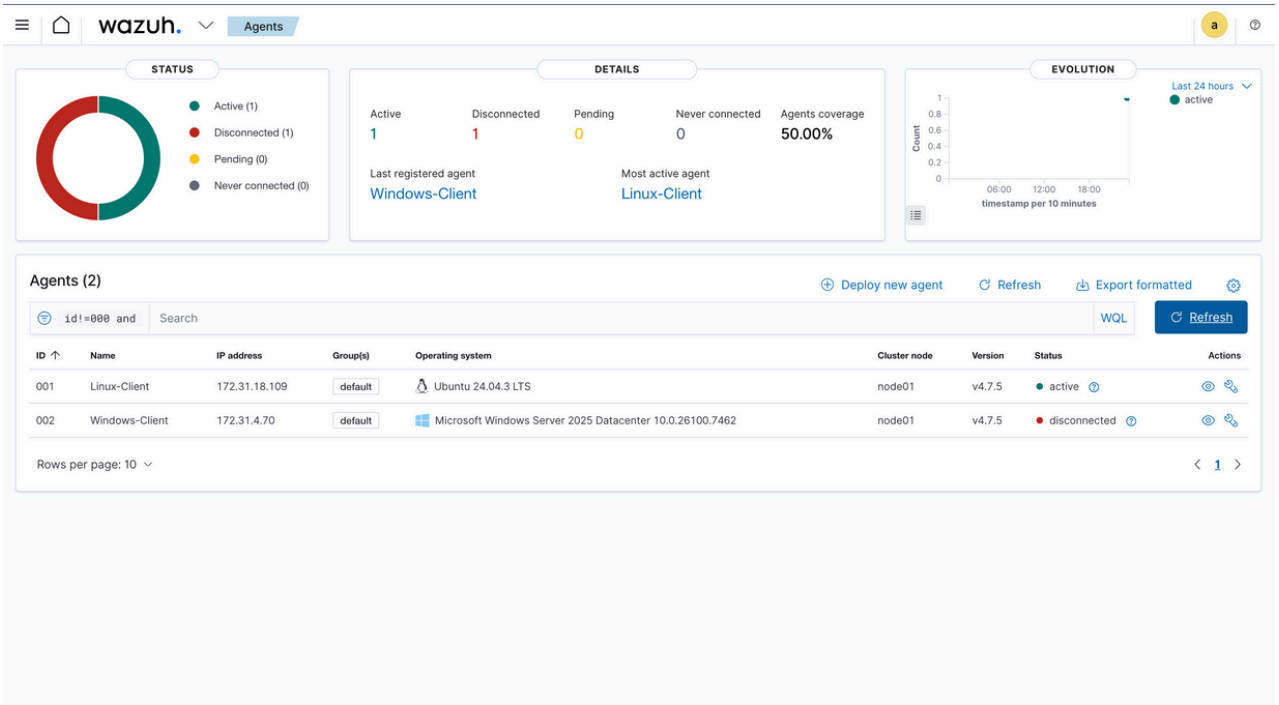
Le service Wazuh Agent est en état Running et les événements Windows sont correctement transmis au serveur.



4.2.1 Telechargement et demmarage d’agent :



4.2.2 Affichage d’agent :



5. Démonstrations SIEM et EDR :

Afin de valider le fonctionnement de la plateforme, plusieurs scénarios de sécurité ont été simulés.

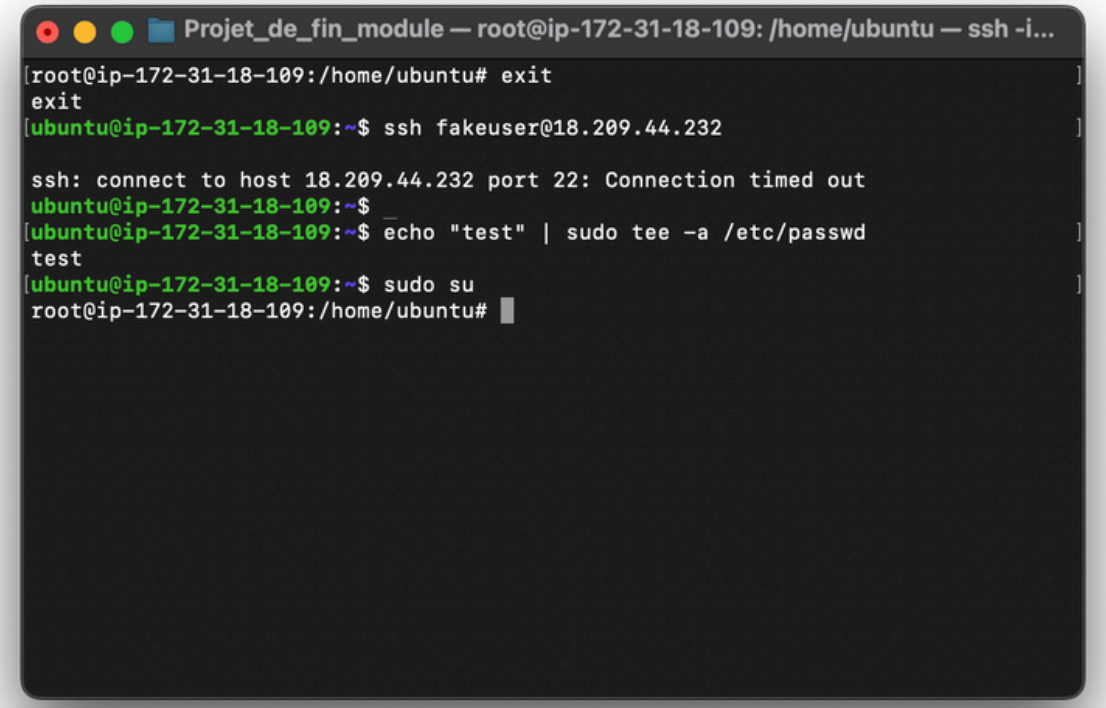
5.1 Scénarios SIEM – Linux :

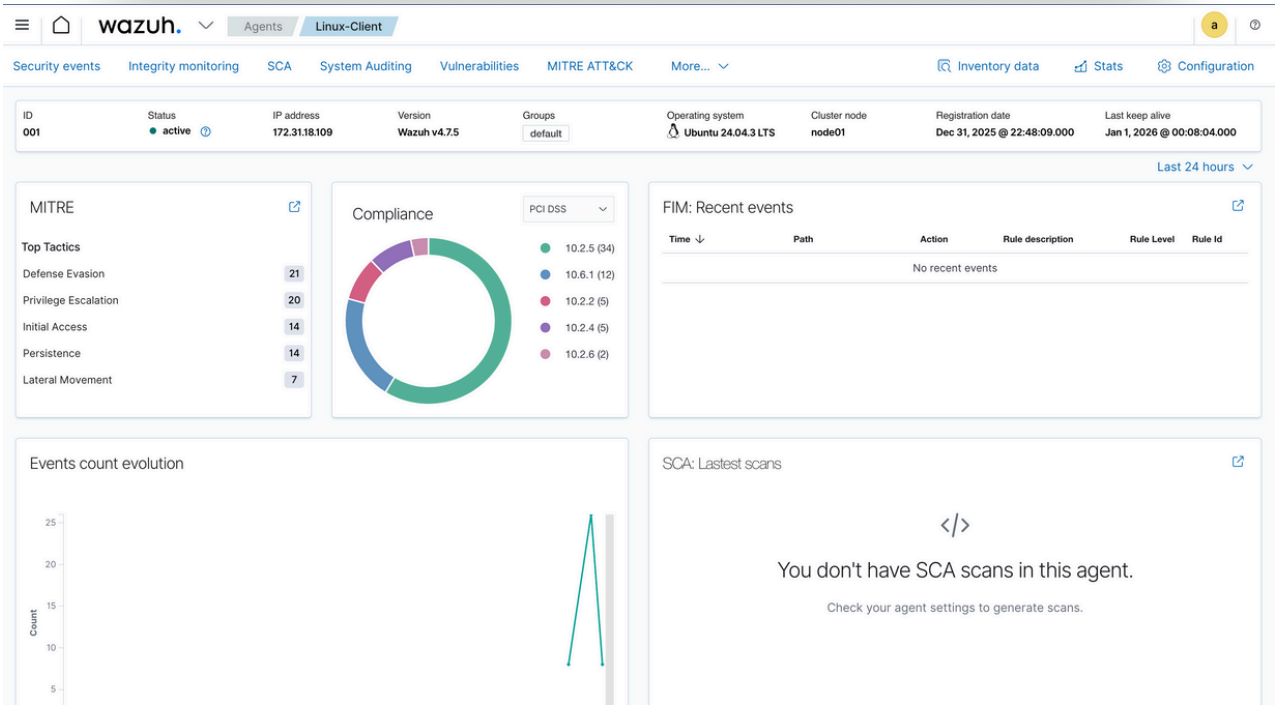
Tentatives de connexion SSH échouées (bruteforce simulé)

Élévation de privilèges via sudo

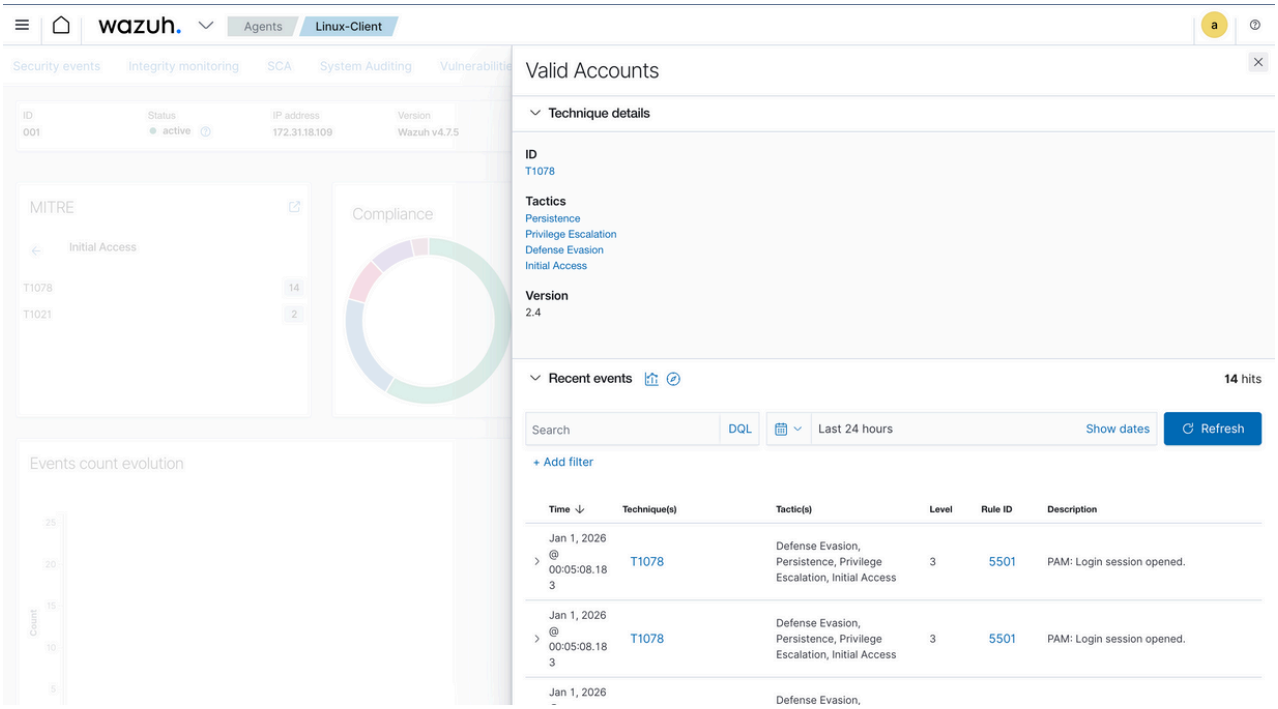
Modification d'un fichier sensible (/etc/passwd)

Ces actions ont généré des alertes visibles dans le Dashboard, notamment des événements liés à sshd, à l'authentification et au File Integrity Monitoring (FIM).

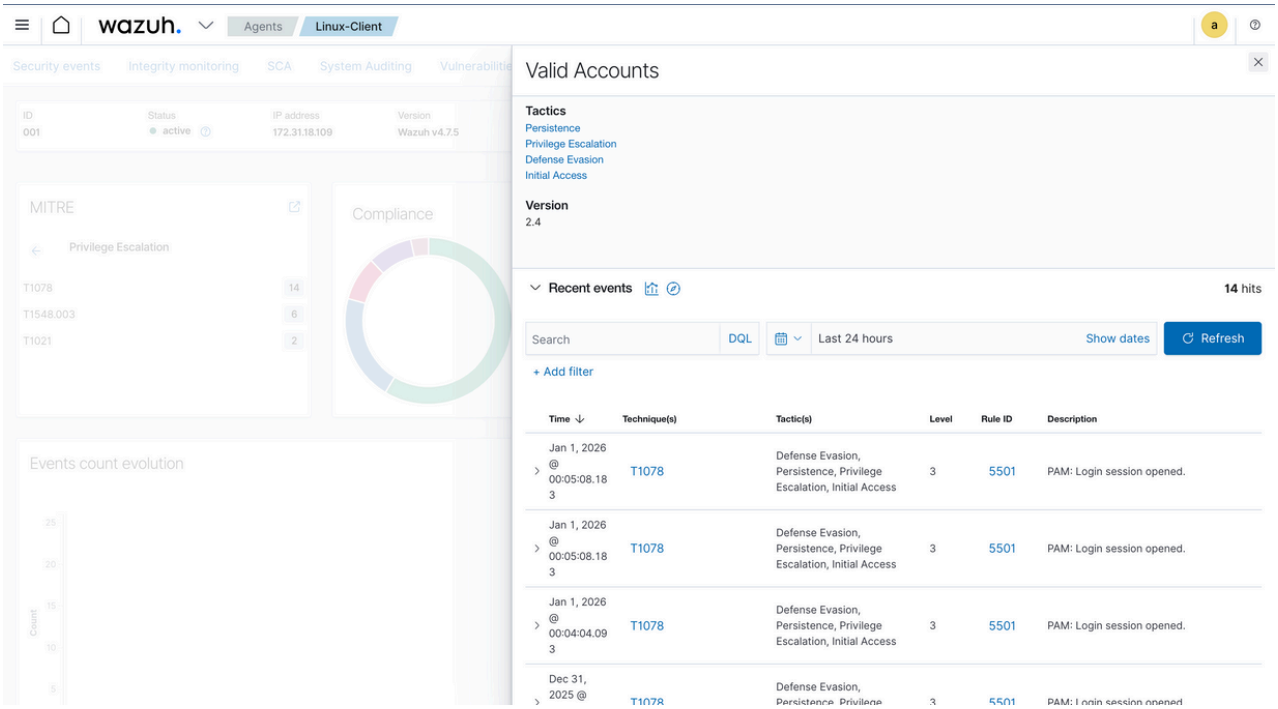




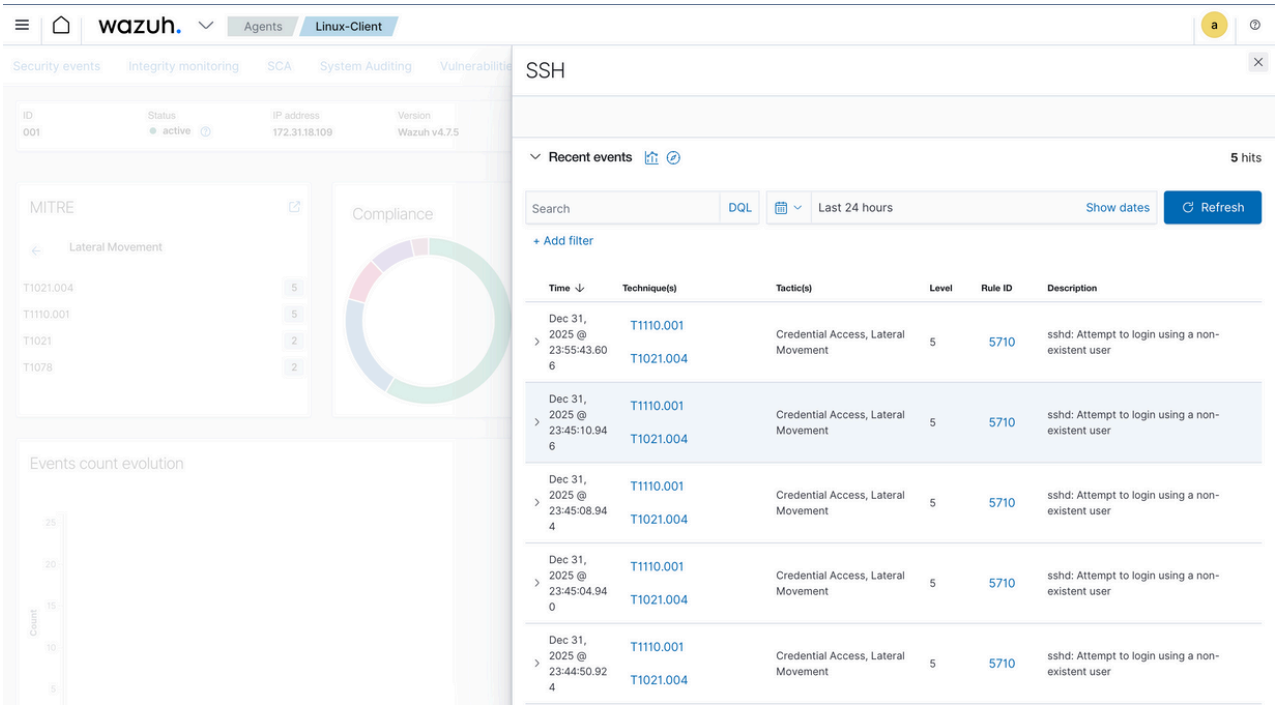
5.1.1 Tentatives SSH échouées (bruteforce simulé) :



5.1.2 Élévation de privilèges :



5.1.3 FIM (File Integrity Monitoring) :

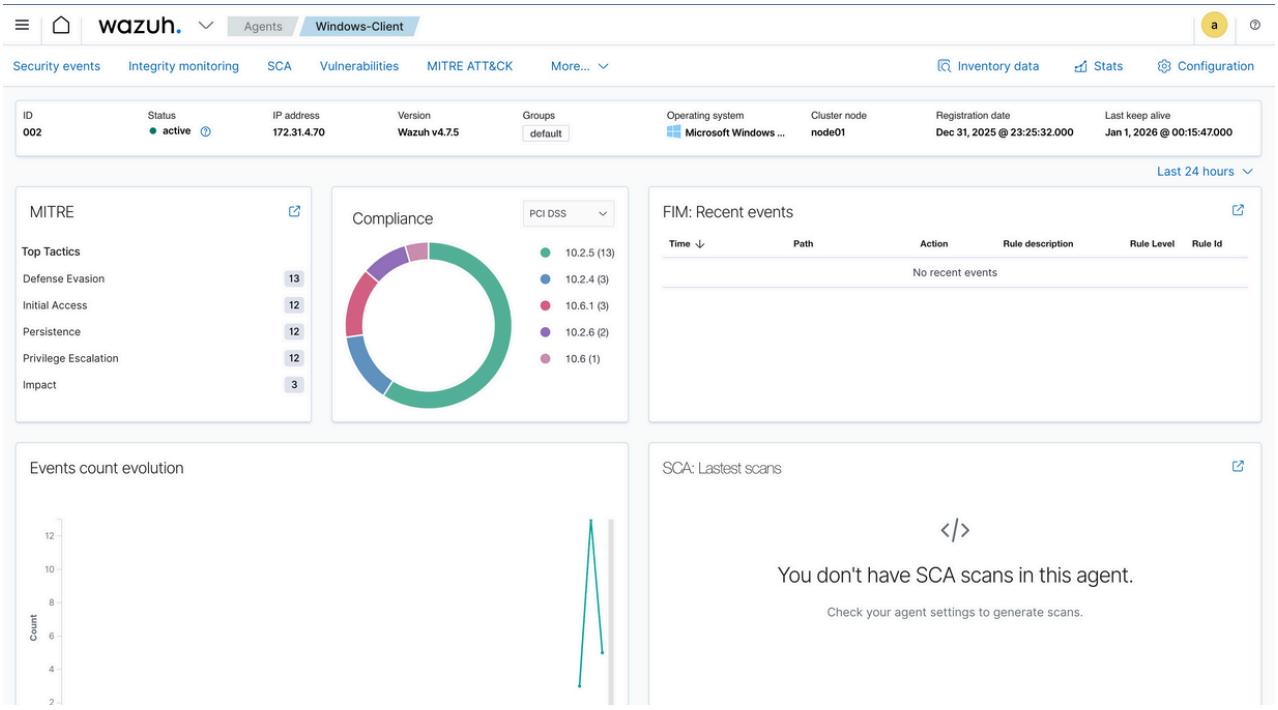


5.2 Scénarios EDR – Windows :

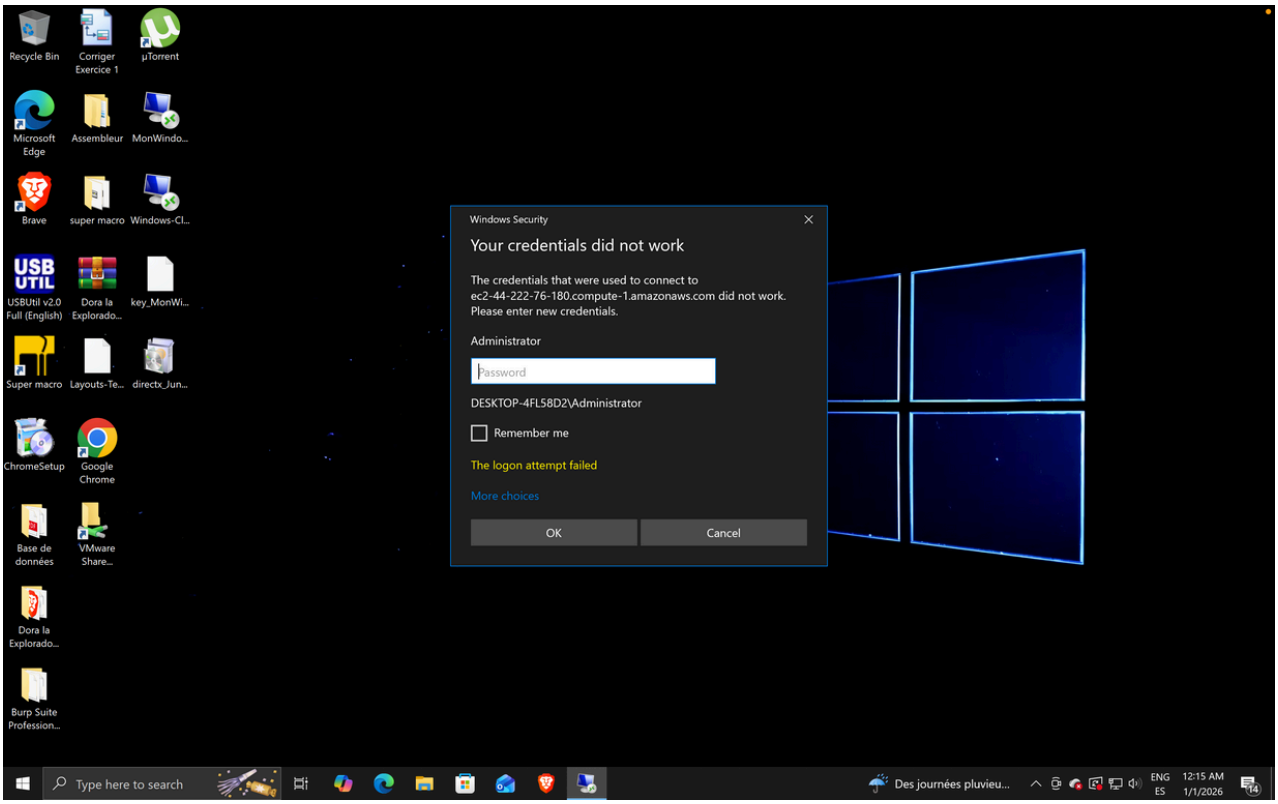
Échecs de connexion (Event ID 4625)

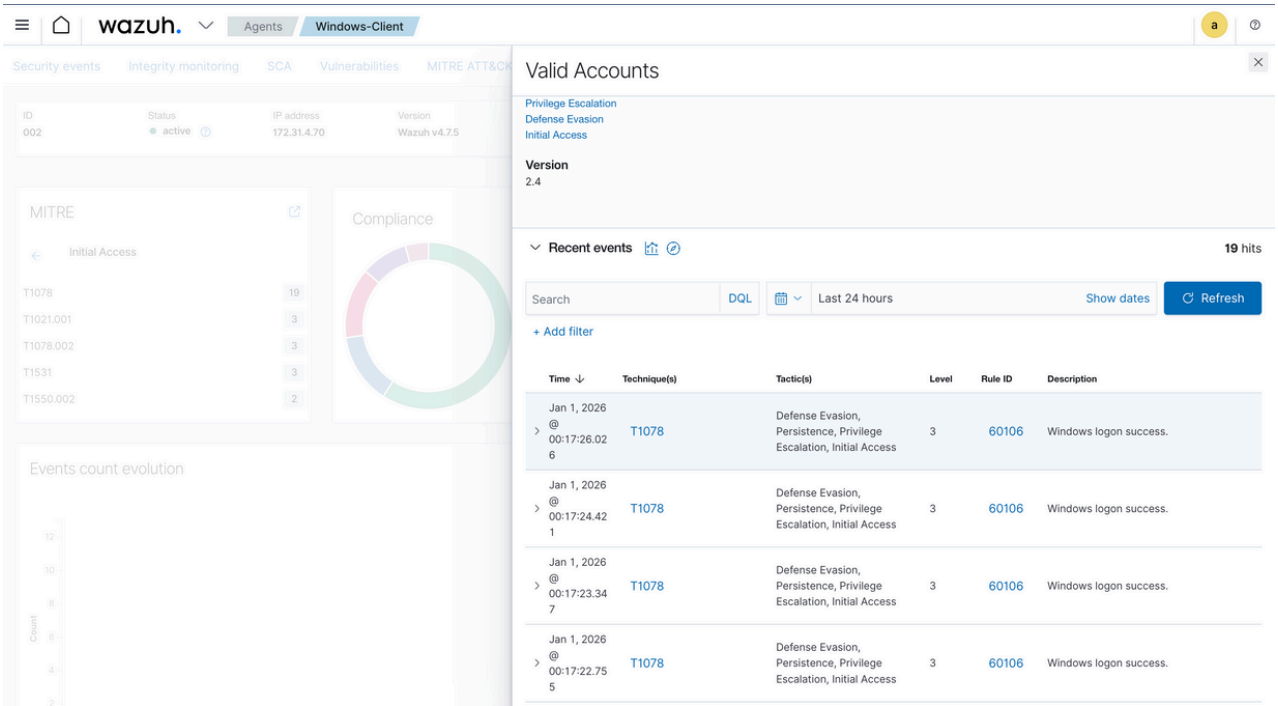
Création d'un utilisateur local et ajout au groupe Administrators

Ces événements ont été détectés par Wazuh et classifiés comme événements critiques liés à la gestion des identités et des privilèges.



5.2.1 Échecs de login (4625) :



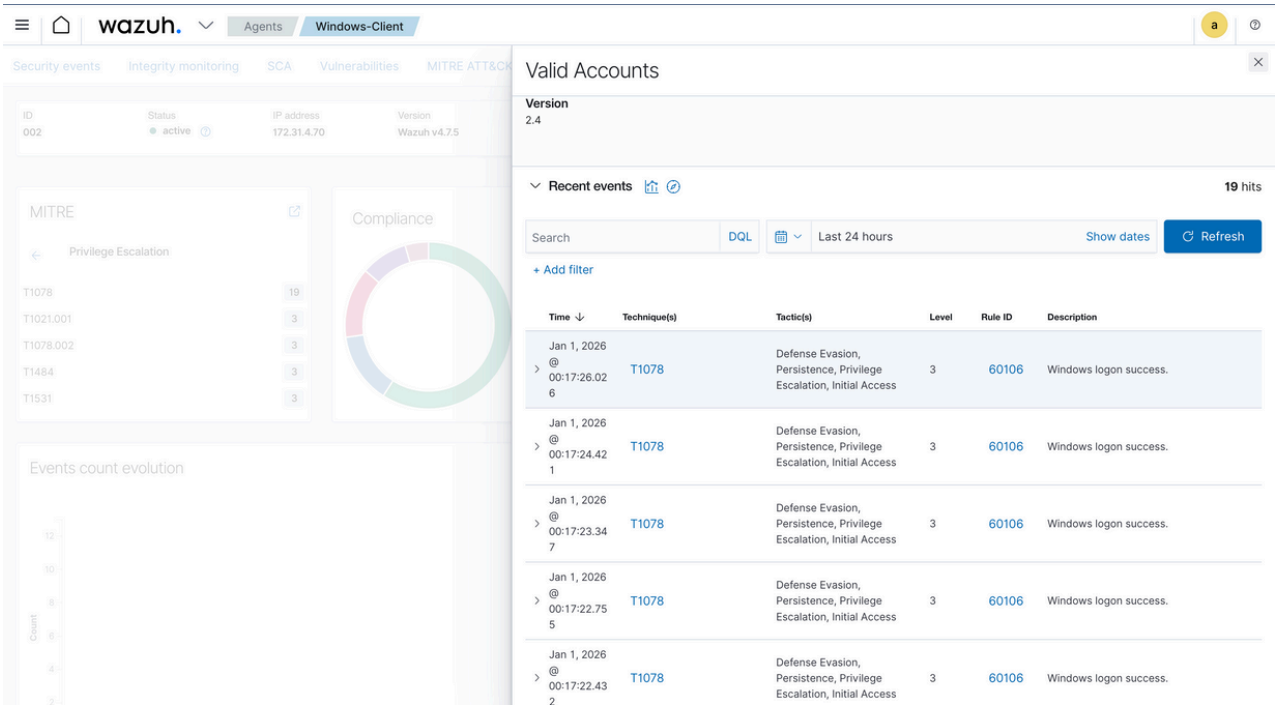


5.2.2 Création utilisateur (IAM) :

```
PS C:\Windows\system32> net user labuser P@ssw0rd! /add
The command completed successfully.

PS C:\Windows\system32> net localgroup administrators labuser /add
The command completed successfully.

PS C:\Windows\system32>
```



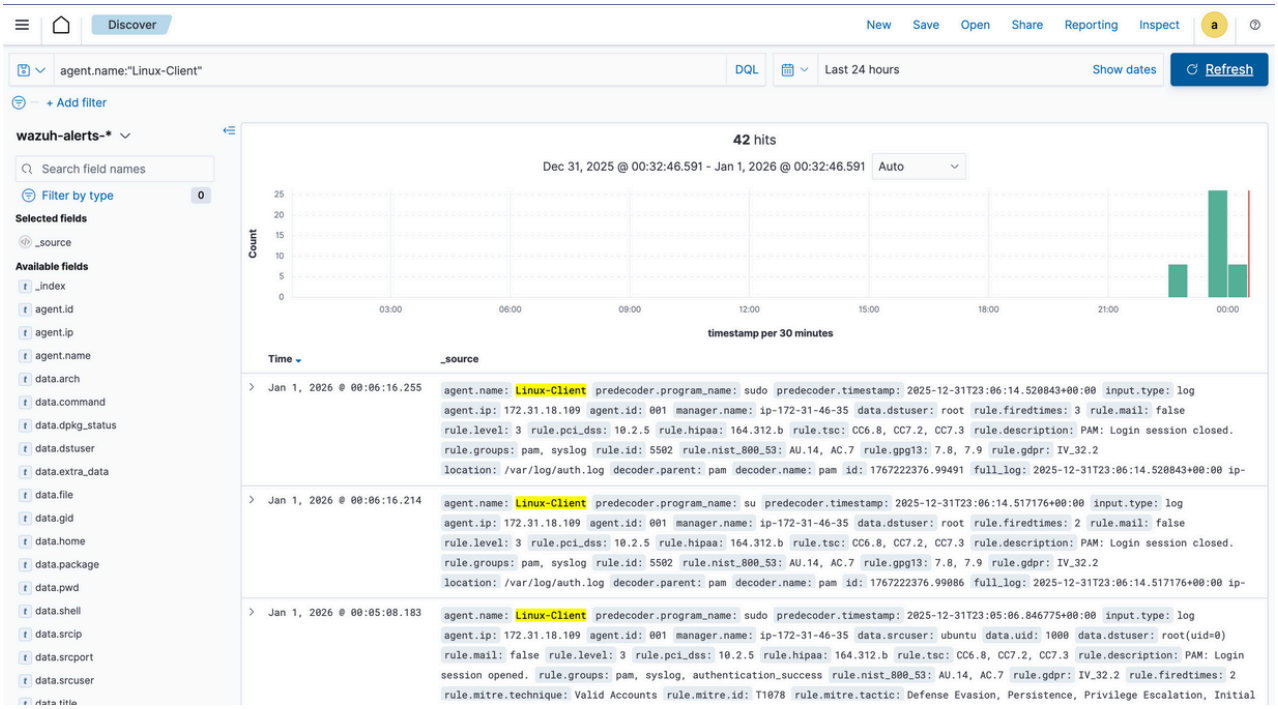
6. Analyse : SIEM, EDR et IAM :

SIEM : centralisation et corrélation des logs Linux et Windows
EDR : surveillance comportementale des endpoints (processus, utilisateurs, actions critiques)
IAM / PAM : détection des changements de privilèges et des tentatives d'accès non autorisées
Cette combinaison permet une visibilité complète sur les activités des systèmes et constitue la base d'un SOC moderne.

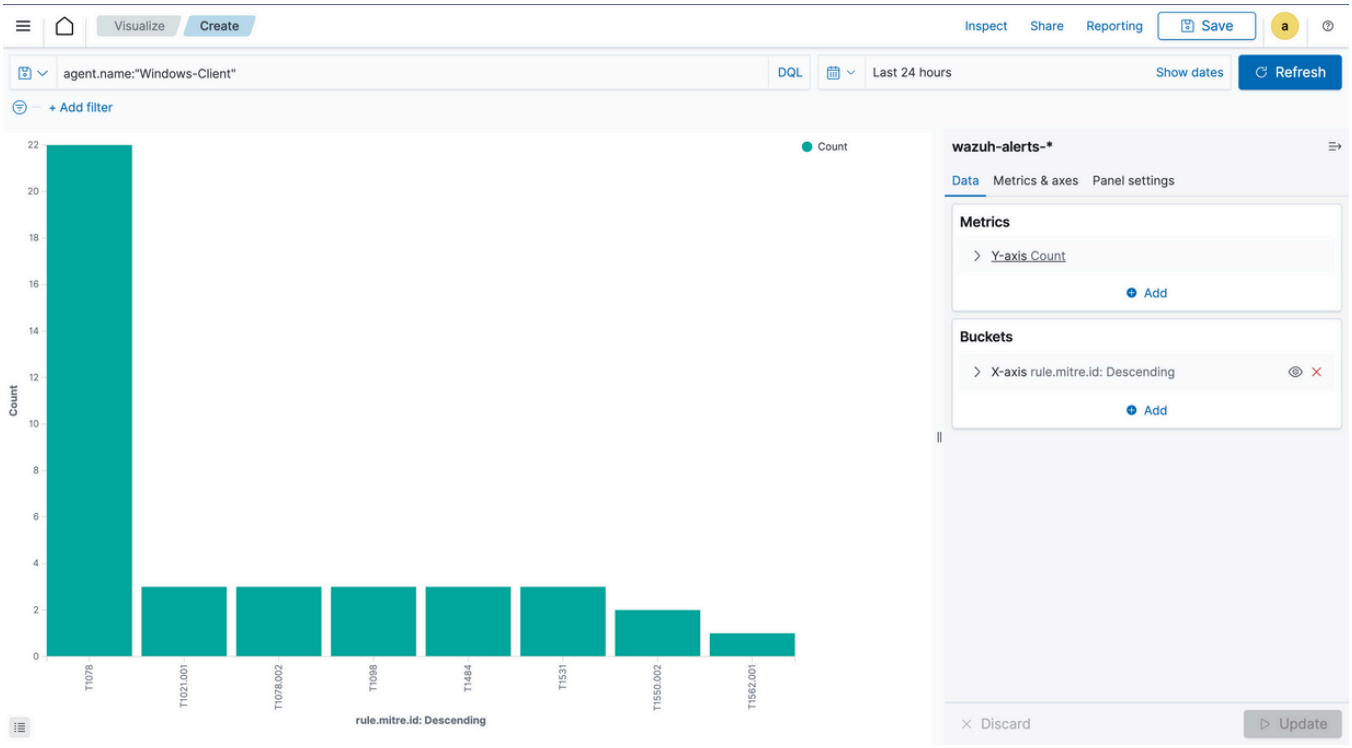
7. Security Monitoring et Threat Detection :

La plateforme Wazuh permet également de réaliser des requêtes de threat hunting, par exemple :
Recherche des tentatives d'authentification échouées répétées
Détection des créations de comptes administrateurs
Analyse des actions sensibles sur les fichiers système
Ces requêtes renforcent la capacité de détection proactive des menaces.

7.1 Dashboard + exemple d'un filtre :



7.2 Affichage en diagramme :



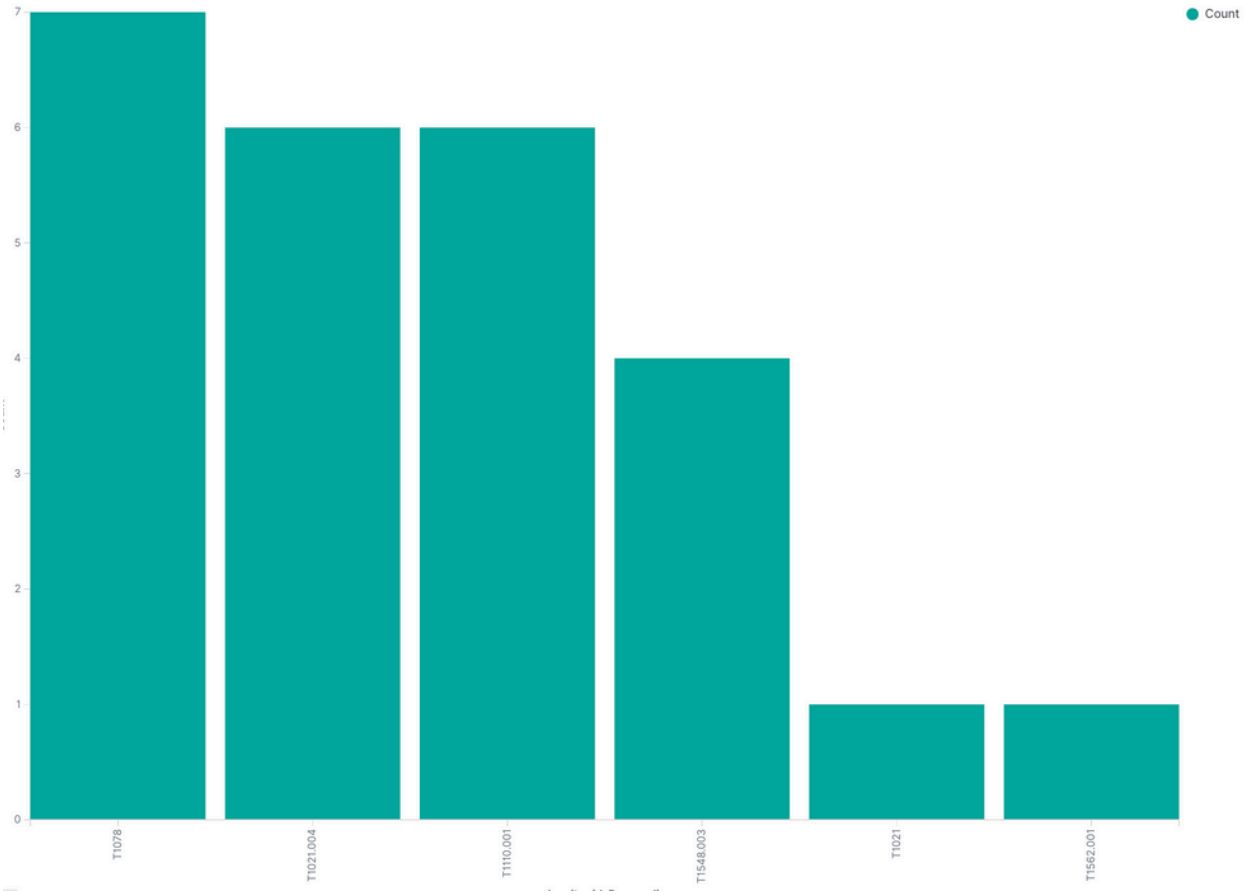
7.3 Threat Detection 1 :

7.3.1 Graphique des événements :

- Il affiche le nombre d'alertes classées par technique MITRE ATT&CK.
- Techniques les plus fréquentes

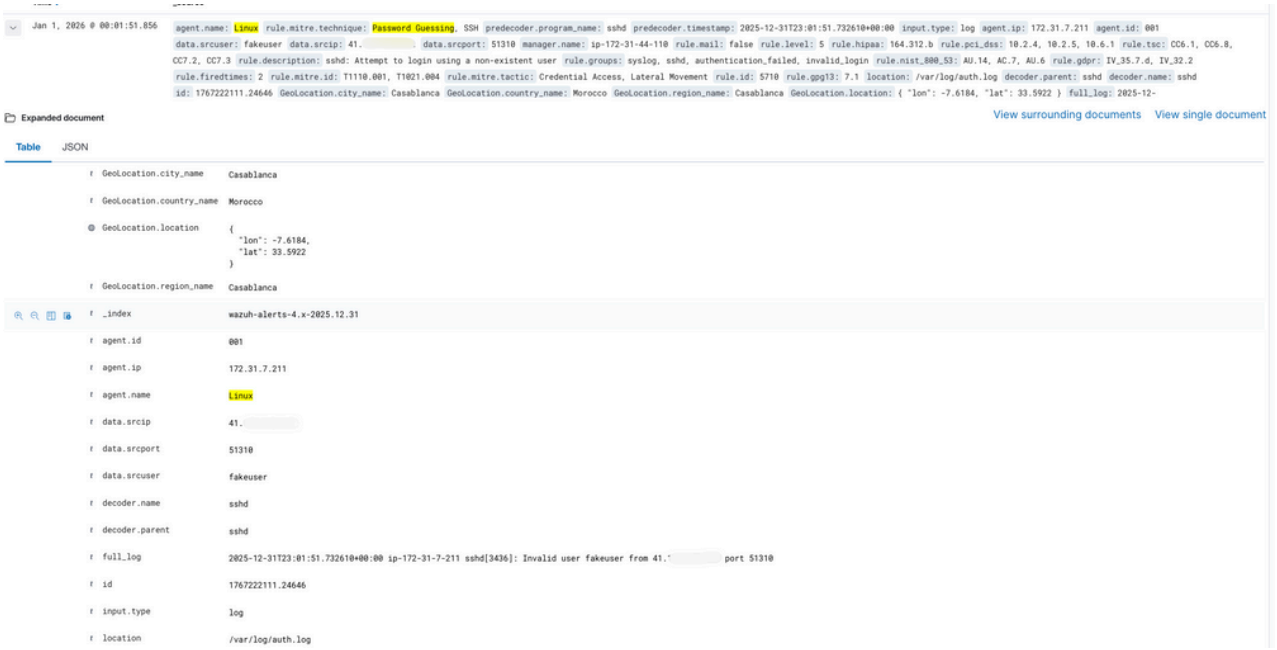
1. T1028 → ~7 événements (la plus élevée)
2. T1020.004 et T1100.001 → ~6 événements chacun
3. T1546.003 → ~4 événements
4. T1021 et T1569.001 → ~1 événement chacun

Ces techniques sont généralement liées à l'accès distant, l'exécution de code, la persistance ou le mouvement latéral dans un réseau.



2. Détail d'une alerte

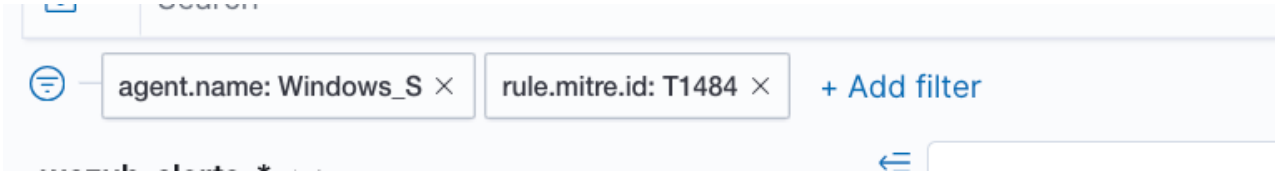
Type d'alerte : tentative de connexion SSH avec un utilisateur invalide ("Invalid user ... from ...").
Règle Wazuh déclenchée : ID 5719 (brute-force ou scan SSH classique).
IP source : 172.31.4.70 (adresse privée, donc probablement interne à un réseau/VPC).
Machine cible : serveur Linux (agent Wazuh ID 001, IP publique 41.141.x.x).
Géolocalisation de la machine cible : Casablanca, Maroc.
Date de l'événement : début décembre 2025.



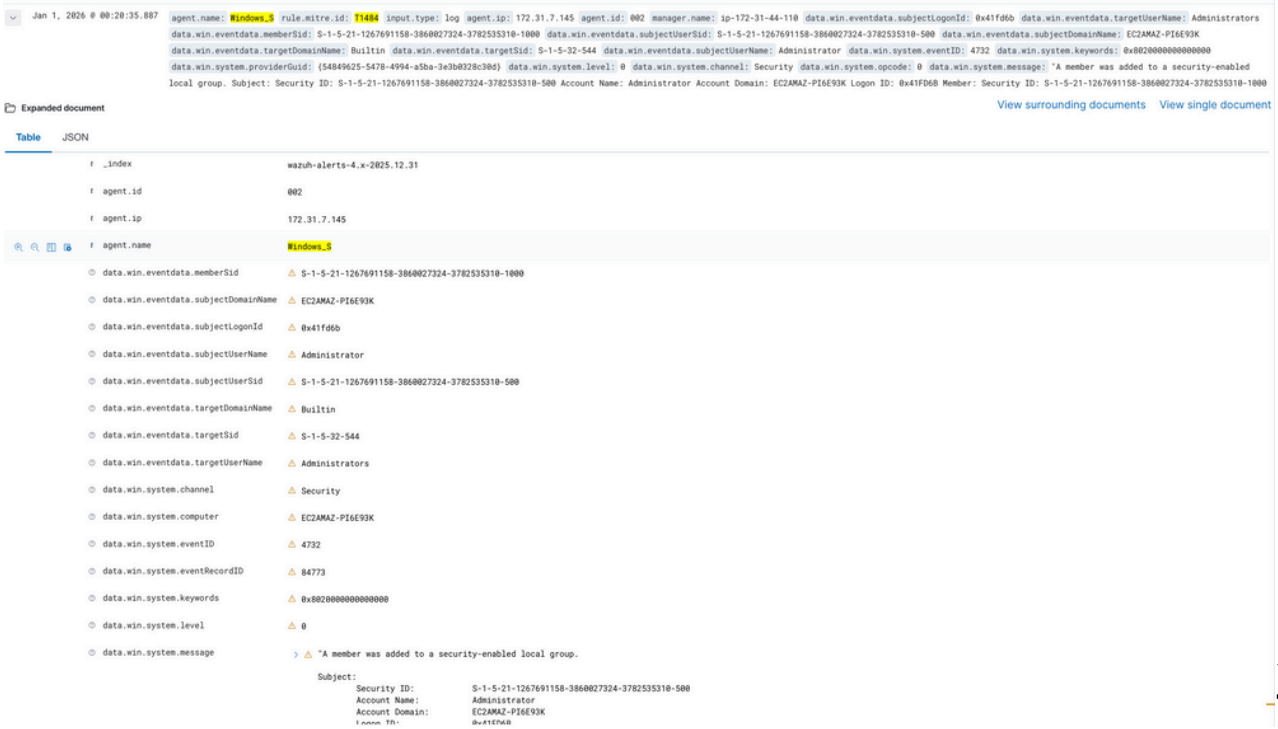
L’ensemble indique très probablement une tentative de brute-force SSH ou un scan automatisé visant ce serveur

7.4 Threat Detection 2:

une alerte de sécurité élevée dans Wazuh concernant une modification du groupe local "Administrators" sur une machine Windows. Cela correspond à l'ajout d'un membre à ce groupe privilégié



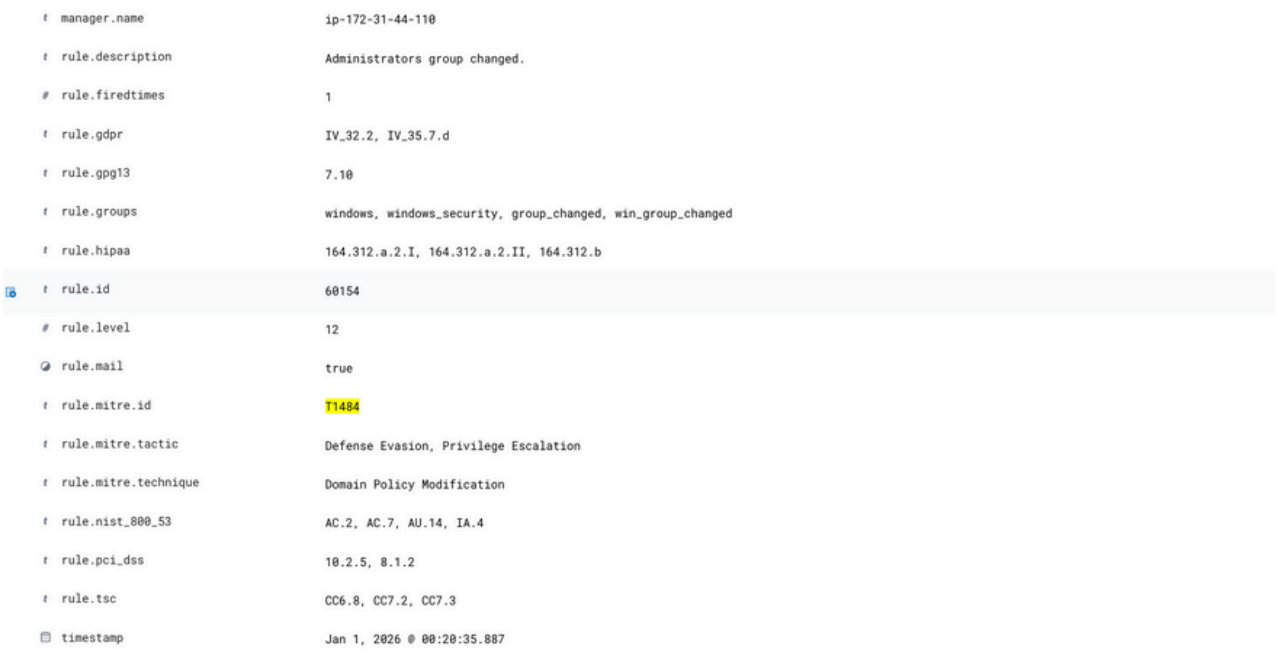
Détail de l’alerte



- Machine concernée : Agent Wazuh ID 002, nom "Windows_S", IP 172.31.4.70 (IP privée).
- Événement Windows : ID 4732 → "A member was added to a security-enabled local group".
- Groupe modifié : "Administrators" (groupe local Builtin des administrateurs).
- Compte ajouté : SID S-... (typiquement le compte Administrator du domaine).
- Compte qui a effectué l'action : Le même compte Administrator.

Technique MITRE ATT&CK

- ID : T1484
- Nom officiel (query name) : Domain or Tenant Policy Modification
- Sous-techniques possibles : T1484.001 (Group Policy Modification)
- Tactiques : Defense Evasion, Privilege Escalation



t	manager.name	ip-172-31-44-110
t	rule.description	Administrators group changed.
#	rule.firedtimes	1
t	rule.gdpr	IV_32.2, IV_35.7.d
t	rule.gpg13	7.10
t	rule.groups	windows, windows_security, group_changed, win_group_changed
t	rule.hipaa	164.312.a.2.I, 164.312.a.2.II, 164.312.b
t	rule.id	60154
#	rule.level	12
◕	rule.mail	true
t	rule.mitre.id	T1484
t	rule.mitre.tactic	Defense Evasion, Privilege Escalation
t	rule.mitre.technique	Domain Policy Modification
t	rule.nist_800_53	AC.2, AC.7, AU.14, IA.4
t	rule.pci_dss	10.2.5, 8.1.2
t	rule.tsc	CC6.8, CC7.2, CC7.3
🗓	timestamp	Jan 1, 2026 @ 00:20:35.887

- Règle Wazuh : ID 60154, niveau 12 (élevé).
- Description : "Administrators group changed."

Technique MITRE ATT&CK (confirmée)

ID : T1484
Nom officiel : Domain or Tenant Policy Modification
Tactique : Defense Evasion, Privilege Escalation
Technique détaillée : Domain Policy Modification (souvent via modification de Group Policy Objects - GPO).

7.5 Threat Detection 3 :

lertes sur une machine Windows cliente ("Windows-Client") indiquant une utilisation de comptes valides pour un mouvement latéral (probablement via RDP), combinée à une manipulation de compte et une authentification alternative (Pass the Hash). Cela s'inscrit dans une chaîne d'attaque potentielle

Requête de recherche

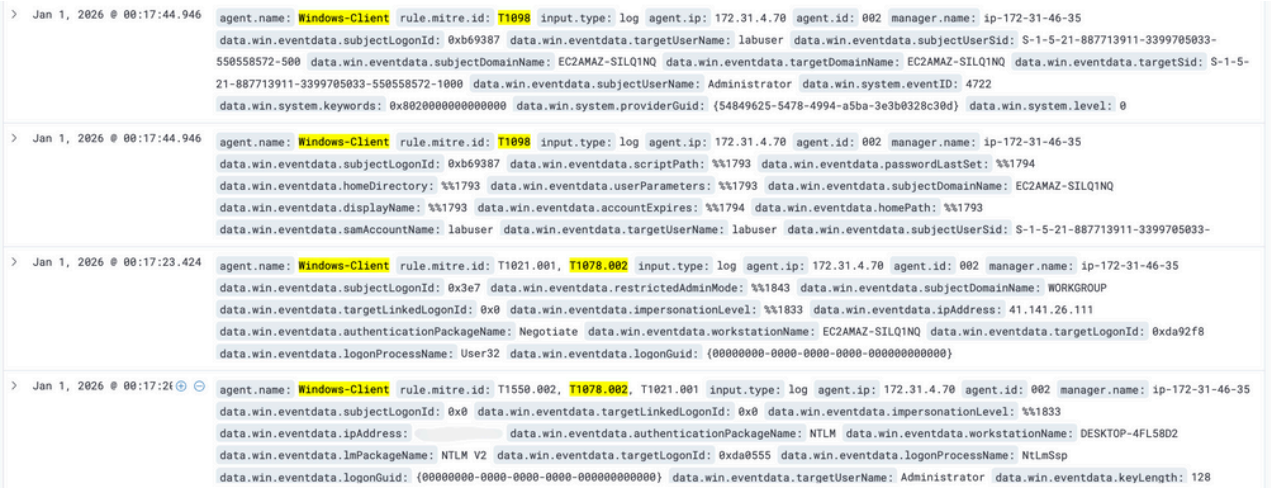
- Filtre appliqué : Agent nommé "Windows-Client" ET techniques MITRE T1098 OU T1078.002.
- Période : Dernières 24 heures.
- Cela cible spécifiquement les événements liés à la manipulation de comptes ou à l'abus de comptes de domaine.

Détails des alertes

Machine concernée :

Agent Wazuh ID 002, nom "Windows-Client", IP privée 172.31.4.70 (même sous-réseau 172.31.x.x que les alertes précédentes, typique d'un environnement lab/cloud)

Événements observés



1 Technique MITRE T1098 (deux alertes)

- Nom officiel : Account Manipulation
- Événement Windows ID 4722 : "A user account was enabled" (un compte utilisateur a été activé).
- Détails : Activation du compte local "labuser" par l'Administrator du domaine (EC2AMAZ-SIL01NQ).
- Paramètres suspects : home directory, script path, etc., définis avec des valeurs comme %1793 (potentiellement pour persistance ou backdoor).

2 Techniques MITRE T1021.001 + T1078.002

- T1021.001 : Remote Services: Remote Desktop Protocol
- T1078.002 : Valid Accounts: Domain Accounts
- Connexion RDP en Restricted Admin Mode (impersonation activée) depuis l'IP 41.x.x.x vers la machine cible

Conclusion

Ce projet a permis de mettre en œuvre une solution complète de supervision de la sécurité des endpoints dans un environnement Cloud réel. L'intégration de Wazuh avec des systèmes Linux et Windows a démontré l'efficacité des solutions SIEM et EDR pour la détection, l'analyse et la réponse aux incidents de sécurité.

Les résultats obtenus confirment l'importance de la centralisation des logs, de la surveillance des endpoints et de la gestion des identités dans la protection des infrastructures modernes.

Lien GitHub :

Le dépôt GitHub du projet, contenant la documentation, les fichiers de configuration et les captures d'écran, est disponible à l'adresse suivante :

https://github.com/AbdelaliSaadali/wazuh-siem-edr-cloud-lab.git