ECOLE NORMALE SUPÉRIEURE DE L'ENSEIGNEMENT
TECHNIQUE DE MOHAMMEDIA
UNIVERSITÉ HASSAN II DE CASABLANCA

Département Mathématique et Informatique

Filière : Génie de logiciel et système informatique distribuée

Compte rendu

Atelier_Sécurité des endpoints et supervision SIEM : étude de cas multi-OS (Linux & Windows)

Réalisé par :

Chaimae Mouhssine

Encadré par :

Pr. Azeddine KHIAT

Table of content

1. Introduction

Dans un contexte où les cyberattaques ciblant les endpoints sont de plus en plus fréquentes et sophistiquées, la mise en place de solutions de supervision et de détection avancée devient indispensable.
Cet atelier a pour objectif la mise en œuvre complète d'une plateforme de sécurité basée sur Wazuh, combinant les approches SIEM (Security Information and Event Management) et EDR (Endpoint Detection and Response), déployée dans un environnement Cloud AWS.

L'atelier s'appuie sur un laboratoire multi-systèmes **(Linux et Windows)** afin de reproduire un contexte réaliste proche de celui rencontré en entreprise ou dans un SOC (Security Operations Center).

2. Objectifs pédagogiques de l'atelier

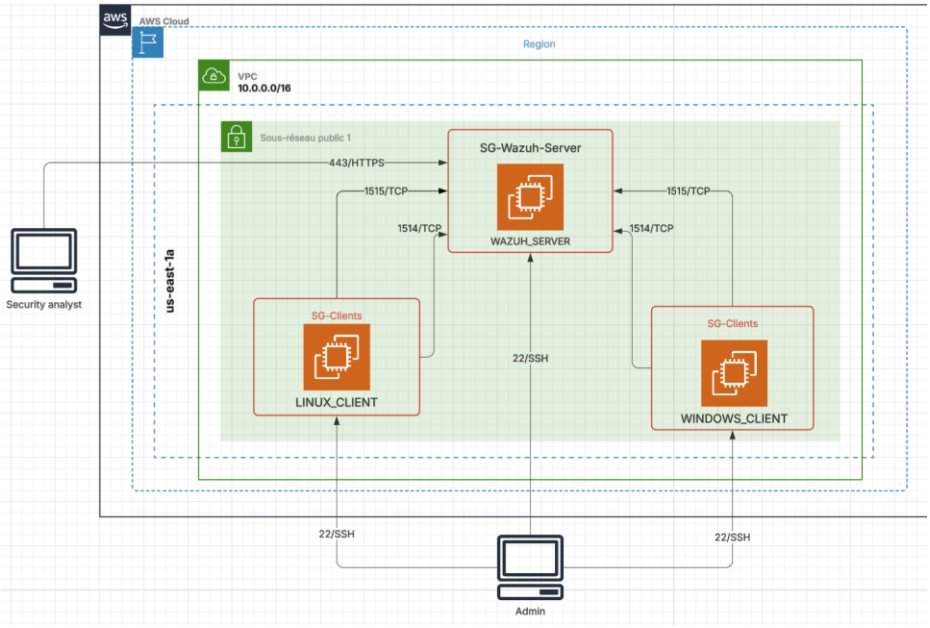
Les objectifs principaux de cet atelier sont :

- Concevoir une architecture Cloud sécurisée sur AWS
- Créer et configurer un réseau virtuel isolé (VPC)
- Déployer une solution SIEM & EDR centralisée avec Wazuh
- Superviser et analyser des événements de sécurité réels
- Comprendre la corrélation des événements multi-OS
- Mettre en évidence les capacités de détection et de réponse aux incidents

3. Architecture du laboratoire

L'architecture déployée est composée des éléments suivants :

- **EC2-1 (Ubuntu 22.04)** : Serveur Wazuh (Manager, Indexer, Dashboard)
- **EC2-2 (Ubuntu 22.04)** : Client Linux avec agent Wazuh
- **EC2-3 (Windows Server)** : Client Windows avec agent Wazuh et option Sysmon



Flux réseau principaux :

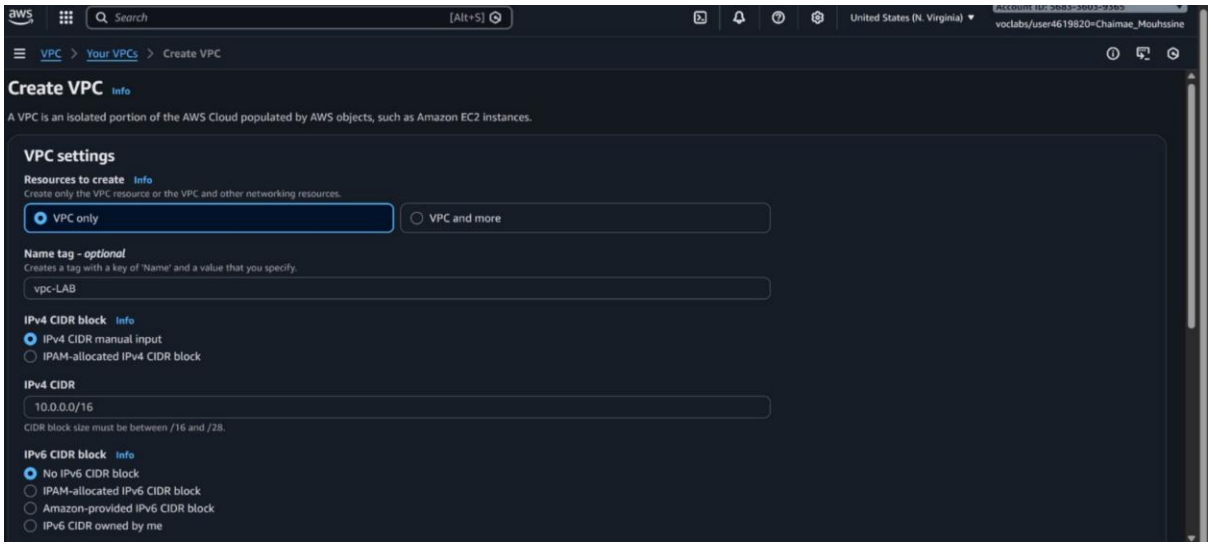
- Agents → Serveur Wazuh : 1514/TCP
- Enrôlement des agents : 1515/TCP
- Accès au Dashboard Wazuh : 443/TCP (HTTPS)

4. Mise en place de l'infrastructure Cloud AWS

4.1 Création d'un VPC personnalisé

Afin d'isoler totalement l'environnement du laboratoire et de maîtriser le réseau, **un VPC dédié a été créé manuellement**.

- **Nom du VPC** : VPC-SIEM-LAB
- **Plage CIDR** : 10.0.0.0/16

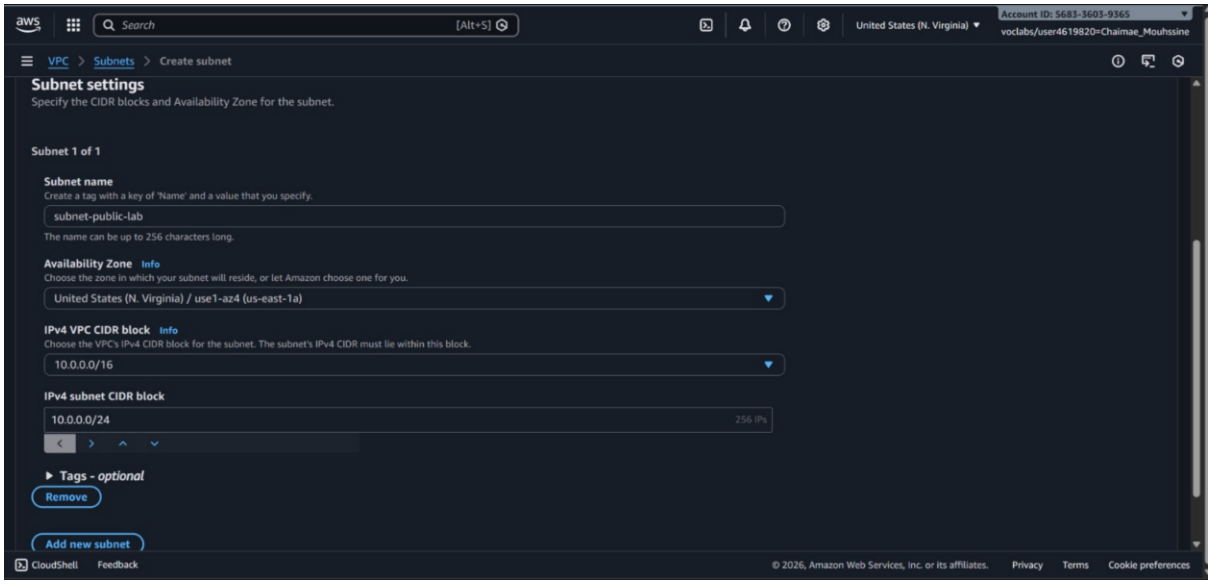


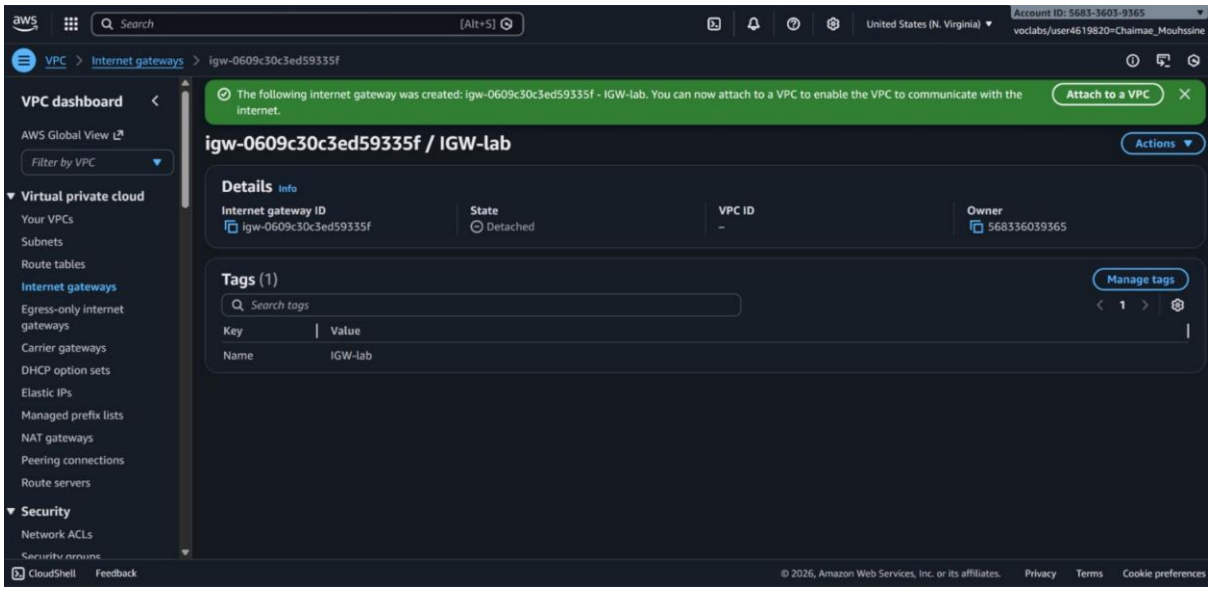
La création d'un VPC personnalisé permet d'éviter l'utilisation du VPC par défaut d'AWS et offre un meilleur contrôle sur le routage, la sécurité et l'isolation réseau. 4.2 Création du subnet public

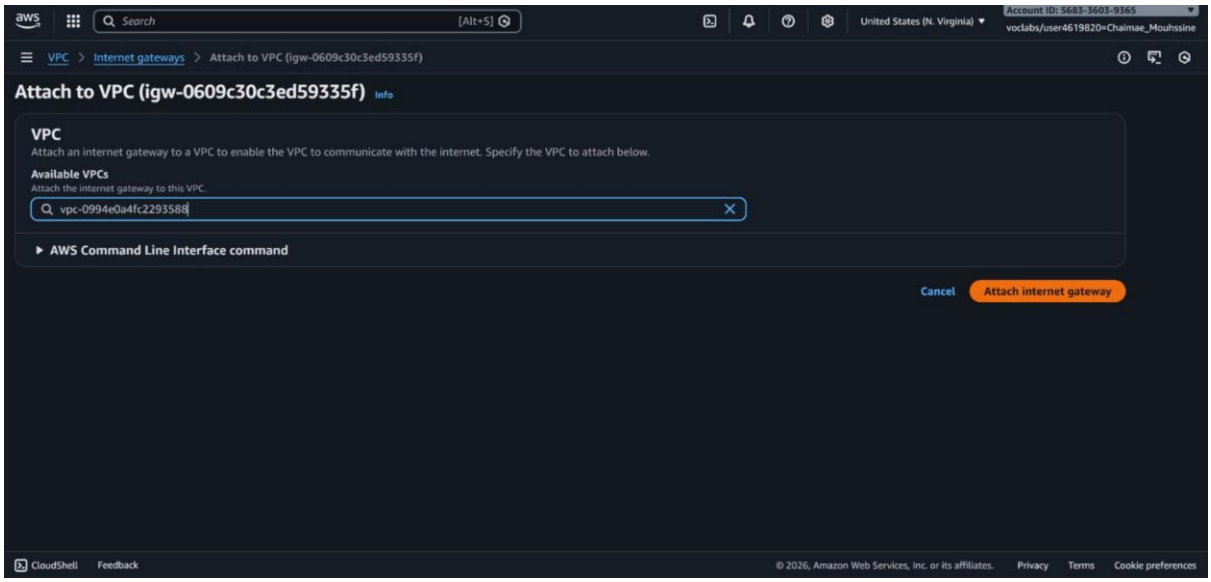
4.2 Création du subnet public

Un subnet public a été configuré pour héberger toutes les instances EC2.

- **Nom du subnet** : Subnet-Public-SIEM
- **CIDR** : 10.0.1.0/24
- **Attribution automatique d'IP publique** : activée





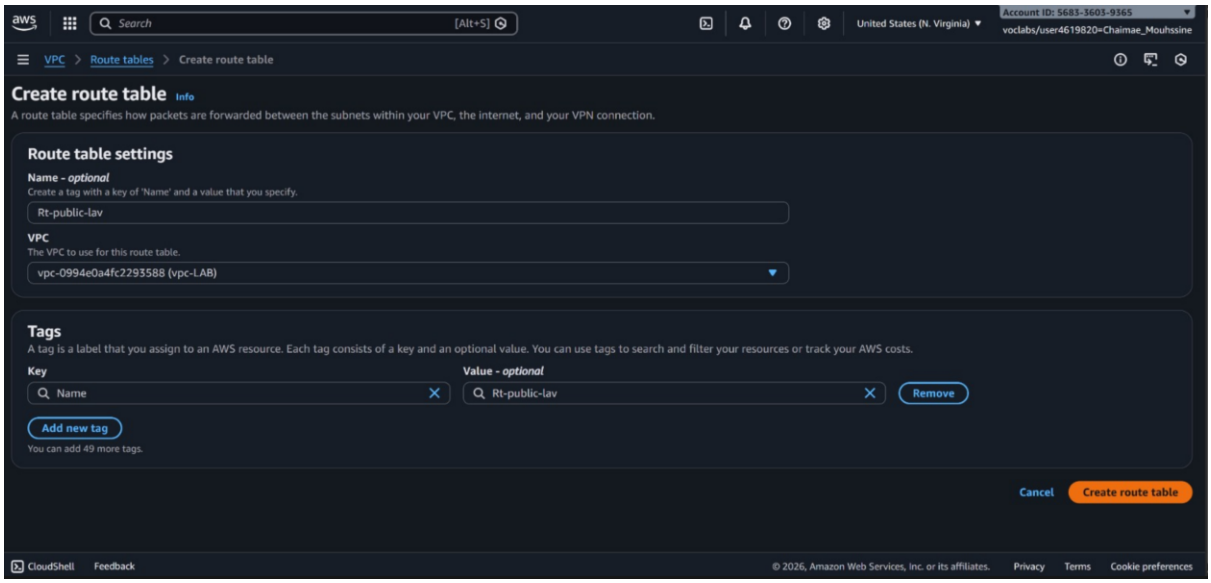


Ce choix simplifie la communication entre les instances et permet l'accès externe au dashboard Wazuh et aux services distants (SSH / RDP).

4.3 Internet Gateway et table de routage

- Création d'une Internet Gateway (IGW)
- Association de l'IGW au VPC
- Création d'une table de routage publique

Ajout de la route:

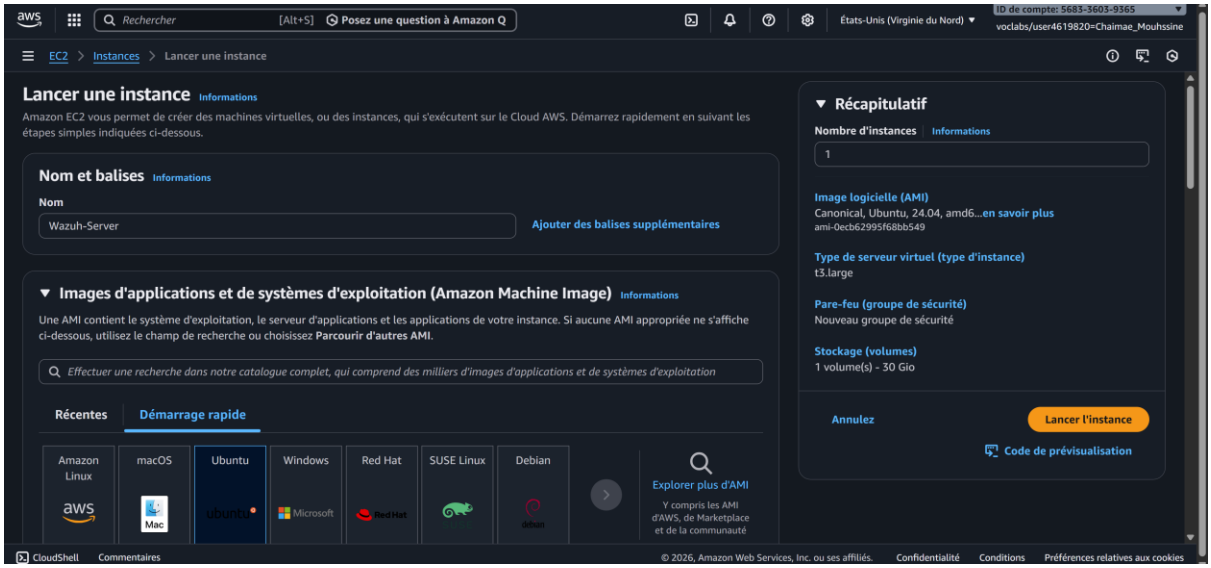


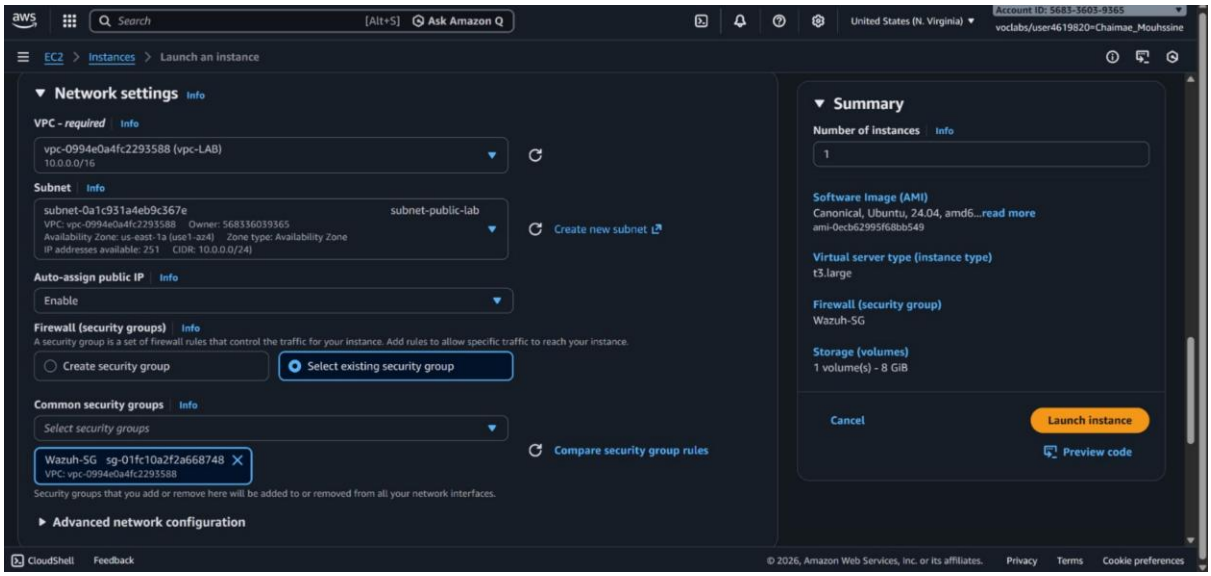
Cette configuration garantit l'accès Internet pour les instances tout en conservant une architecture réseau simple et efficace.

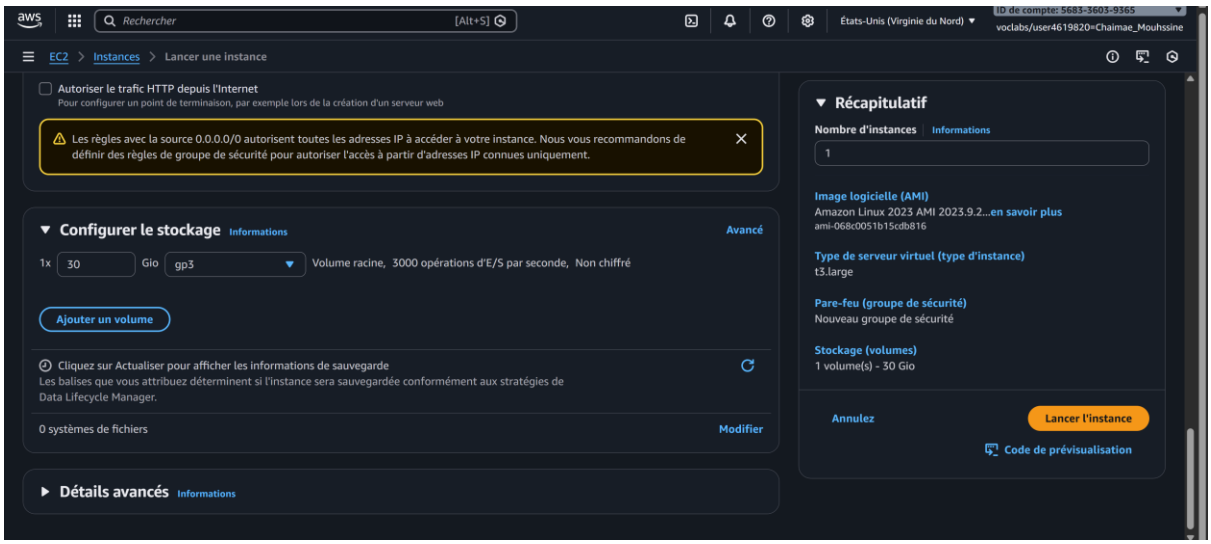
5. Déploiement des instances EC2 dans le VPC

Toutes les instances ont été déployées dans le même VPC et le même subnet, assurant une communication privée directe.

5.1 Serveur Wazuh

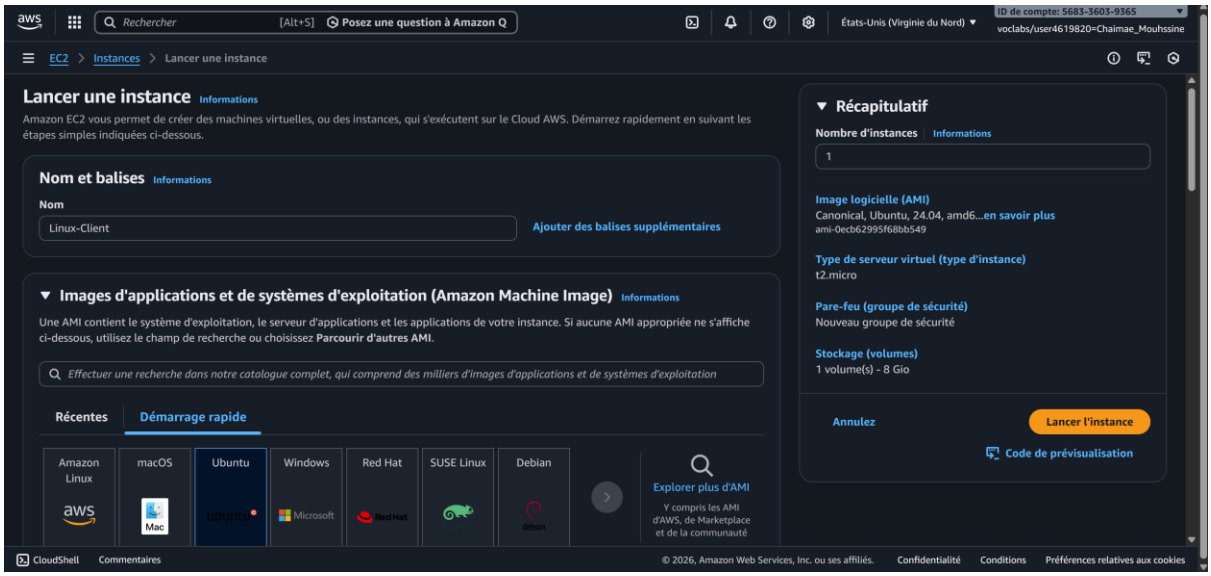


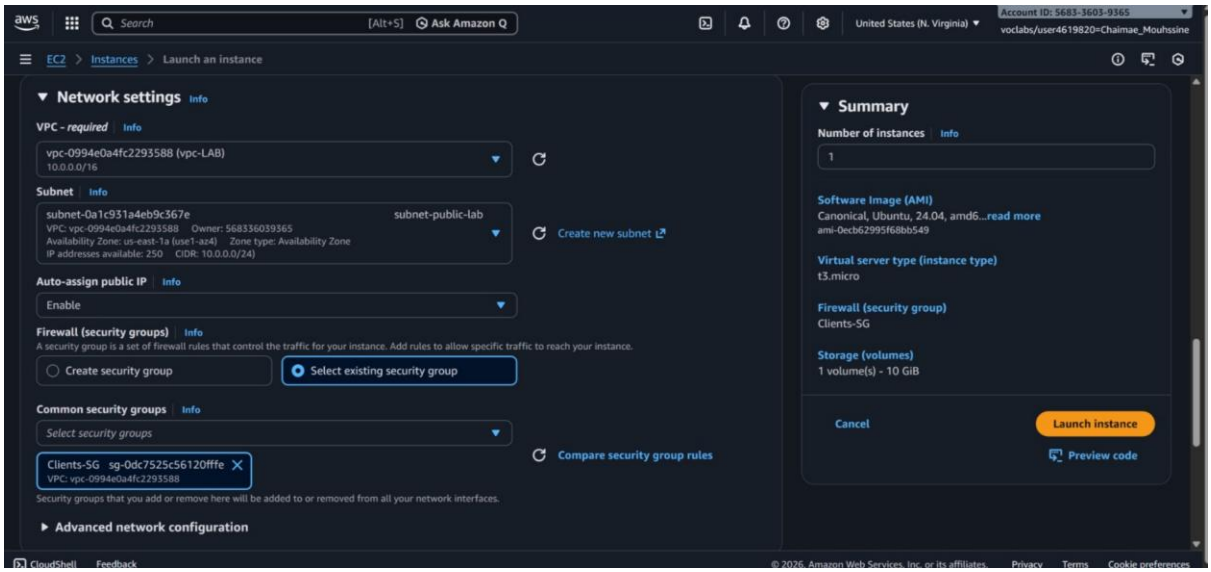




5.1 Client Linux

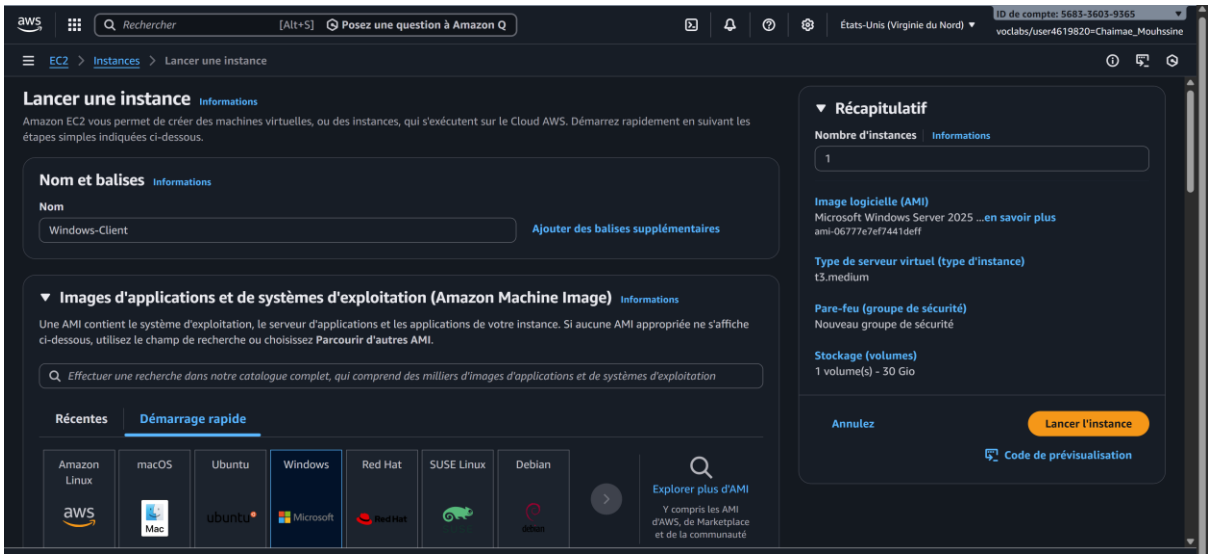
- Ubuntu 22.04 (t2.micro)

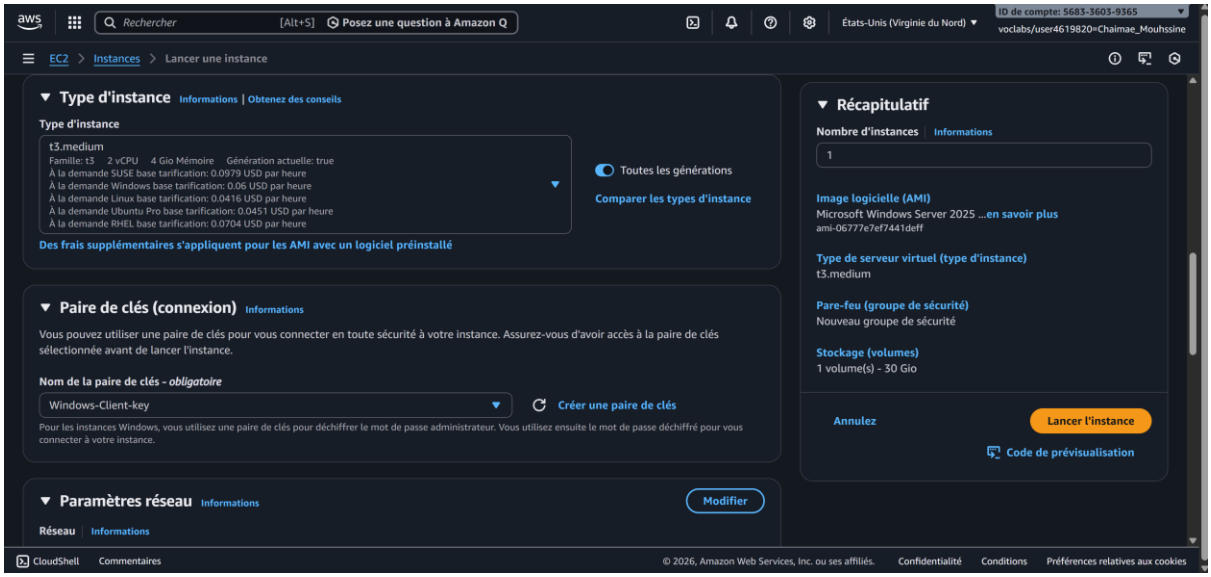




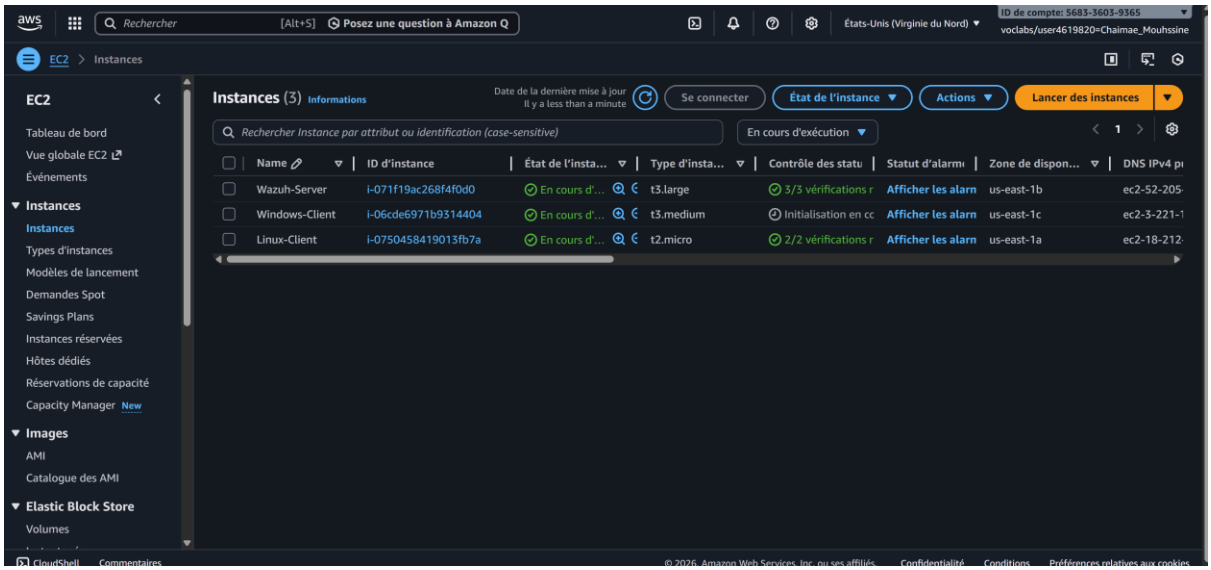
5.2 Windows Client

- Windows Server (t3.medium)

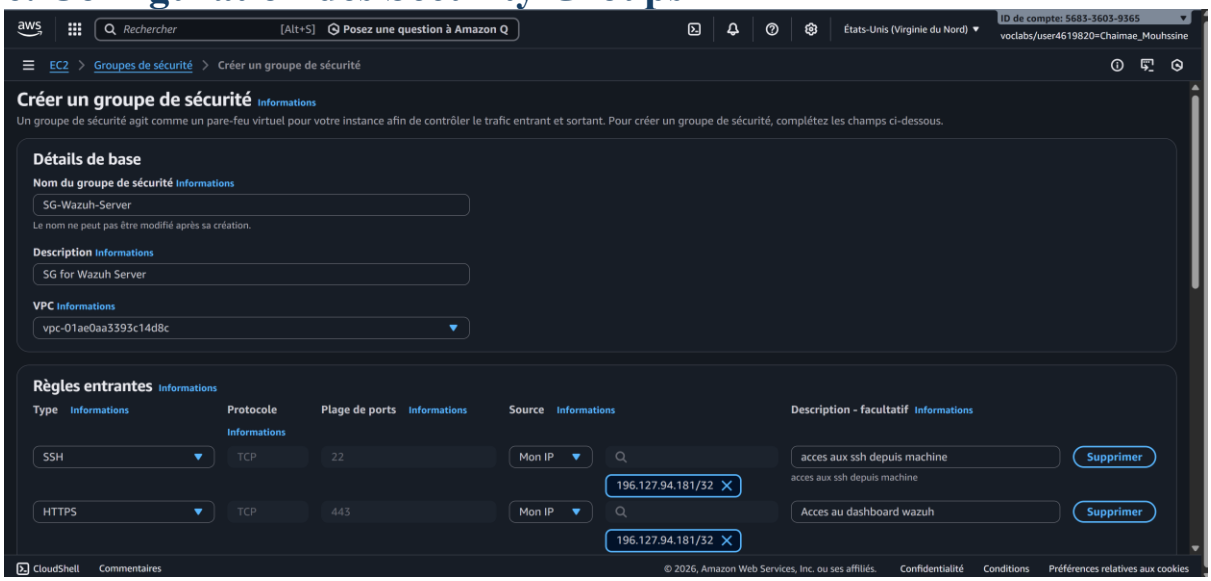


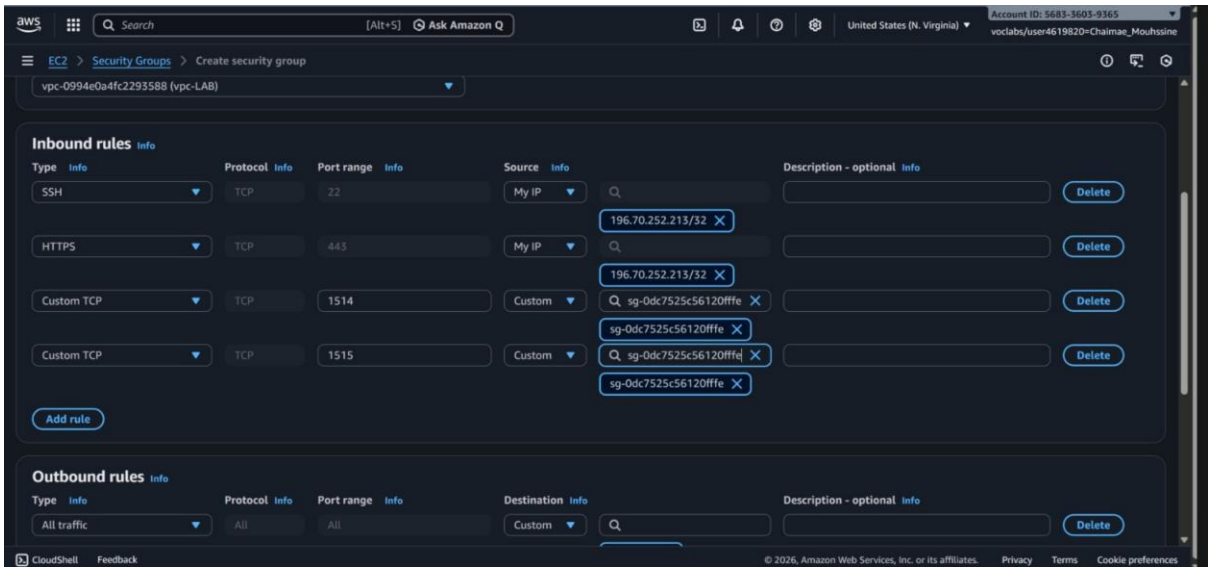


Les instances sont créé avec succès



6. Configuration des Security Groups





7. Installation et configuration de Wazuh All-in-One

- Enrôlement via le **Dashboard Wazuh**

sudo apt update && sudo apt -y upgrade

```
ubuntu@ip-10-0-0-20:~$
ubuntu@ip-10-0-0-20:~$ sudo apt update && sudo apt -y upgrade
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [3161 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [484 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [19.0 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [5043 kB]
```

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

```
ubuntu@ip-10-0-0-20:~$
ubuntu@ip-10-0-0-20:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
ubuntu@ip-10-0-0-20:~$
```

sudo bash wazuh-install.sh -a

```
ubuntu@ip-10-0-0-20:~$
ubuntu@ip-10-0-0-20:~$ sudo bash wazuh-install.sh -a
04/01/2026 10:26:31 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
04/01/2026 10:26:31 INFO: Verbose logging redirected to /var/log/wazuh-install.log
04/01/2026 10:26:40 INFO: Wazuh web interface port will be 443.
04/01/2026 10:26:45 INFO: --- Dependencies ----
04/01/2026 10:26:45 INFO: Installing apt-transport-https.
04/01/2026 10:26:50 INFO: Wazuh repository added.
04/01/2026 10:26:50 INFO: --- Configuration files ---
04/01/2026 10:26:50 INFO: Generating configuration files.
04/01/2026 10:26:52 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and password
s necessary for installation.
04/01/2026 10:26:53 INFO: --- Wazuh indexer ---
04/01/2026 10:26:53 INFO: Starting Wazuh indexer installation.
04/01/2026 10:27:55 INFO: Wazuh indexer installation finished.
04/01/2026 10:27:55 INFO: Wazuh indexer post-install configuration finished.
04/01/2026 10:27:55 INFO: Starting service wazuh-indexer.
04/01/2026 10:28:15 INFO: wazuh-indexer service started.
04/01/2026 10:28:15 INFO: Initializing Wazuh indexer cluster security settings.
04/01/2026 10:28:27 INFO: Wazuh indexer cluster initialized.
04/01/2026 10:28:27 INFO: --- Wazuh server ---
04/01/2026 10:28:27 INFO: Starting the Wazuh manager installation.
04/01/2026 10:29:20 INFO: Wazuh manager installation finished.
04/01/2026 10:29:20 INFO: Starting service wazuh-manager.
04/01/2026 10:29:37 INFO: wazuh-manager service started.
04/01/2026 10:29:37 INFO: Starting Filebeat installation.
04/01/2026 10:29:46 INFO: Filebeat installation finished.
04/01/2026 10:29:47 INFO: Filebeat post-install configuration finished.
04/01/2026 10:29:47 INFO: Starting service filebeat.
04/01/2026 10:29:48 INFO: filebeat service started.
04/01/2026 10:29:48 INFO: --- Wazuh dashboard ---
04/01/2026 10:29:48 INFO: Starting Wazuh dashboard installation.
04/01/2026 10:30:41 INFO: Wazuh dashboard installation finished.
04/01/2026 10:30:42 INFO: Wazuh dashboard post-install configuration finished.
04/01/2026 10:30:42 INFO: Starting service wazuh-dashboard.
04/01/2026 10:30:42 INFO: wazuh-dashboard service started.
04/01/2026 10:31:17 INFO: Initializing Wazuh dashboard web application.
04/01/2026 10:31:17 INFO: Wazuh dashboard web application not yet initialized. Waiting...
04/01/2026 10:31:33 INFO: Wazuh dashboard web application not yet initialized. Waiting...
04/01/2026 10:31:48 INFO: Wazuh dashboard web application initialized.
04/01/2026 10:31:48 INFO: --- Summary ---
04/01/2026 10:31:48 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: QFsi?vvUedlsgXbupZ*RVaixAf5oYhN4
04/01/2026 10:31:48 INFO: Installation finished.
ubuntu@ip-10-0-0-20:~$
```

À la fin, le script fournit :

- **URL du dashboard:** https://54.196.16.171:443
- **Utilisateur : admin**
- **Mot de passe :** CsJpEbgRNAZR495aMkkvukVUceUvdv+9

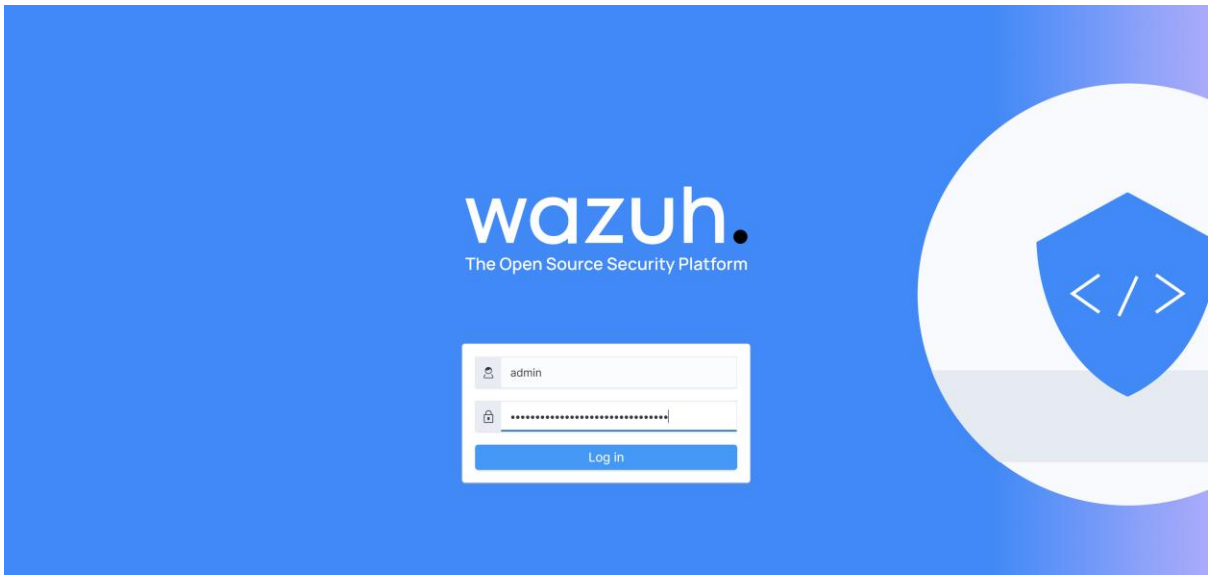
Vérification des services :

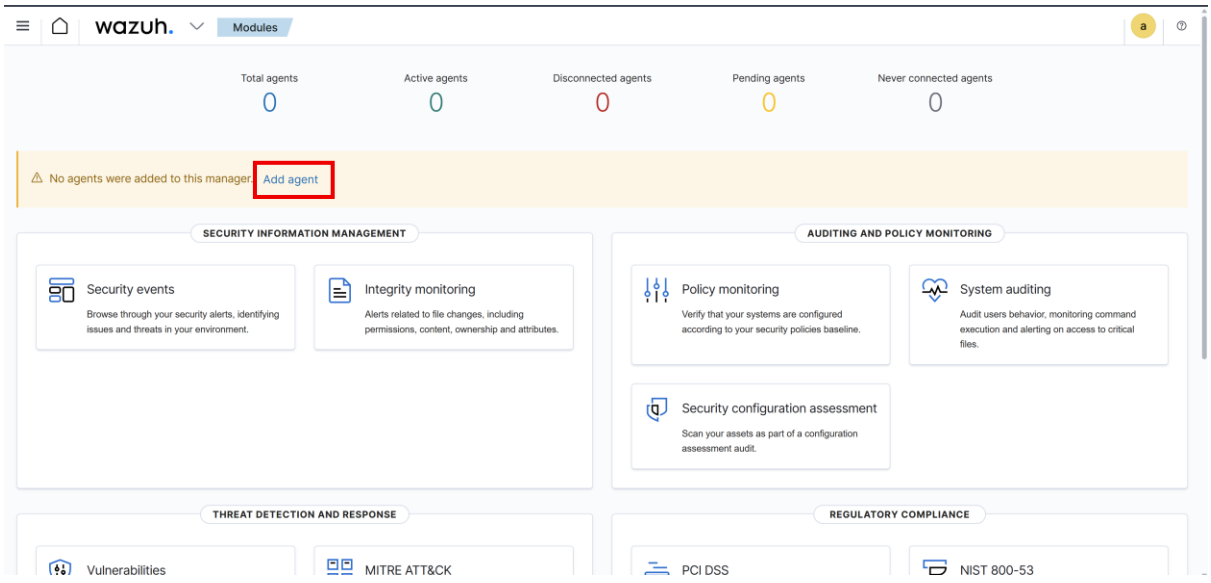
```
ubuntu@ip-10-0-0-20: ~
ubuntu@ip-10-0-0-20:~$
ubuntu@ip-10-0-0-20:~$ sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2026-01-04 10:29:37 UTC; 28min ago
      Tasks: 121 (limit: 4580)
     Memory: 266.3M
        CPU: 48.378s
     CGroup: /system.slice/wazuh-manager.service
             ├─58728 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─58767 /var/ossec/bin/wazuh-authd
             ├─58781 /var/ossec/bin/wazuh-db
             ├─58804 /var/ossec/bin/wazuh-execd
             ├─58815 /var/ossec/bin/wazuh-analysisd
             ├─58859 /var/ossec/bin/wazuh-syscheckd
             ├─58875 /var/ossec/bin/wazuh-remoted
             ├─58898 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─58901 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─58904 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─58917 /var/ossec/bin/wazuh-logcollector
             ├─58936 /var/ossec/bin/wazuh-monitord
             └─58958 /var/ossec/bin/wazuh-modulesd

Jan 04 10:29:29 ip-10-0-0-20 env[58672]: Started wazuh-db...
Jan 04 10:29:29 ip-10-0-0-20 env[58672]: Started wazuh-execd...
Jan 04 10:29:30 ip-10-0-0-20 env[58672]: Started wazuh-analysisd...
Jan 04 10:29:31 ip-10-0-0-20 env[58672]: Started wazuh-syscheckd...
Jan 04 10:29:32 ip-10-0-0-20 env[58672]: Started wazuh-remoted...
Jan 04 10:29:33 ip-10-0-0-20 env[58672]: Started wazuh-logcollector...
Jan 04 10:29:34 ip-10-0-0-20 env[58672]: Started wazuh-monitord...
Jan 04 10:29:35 ip-10-0-0-20 env[58672]: Started wazuh-modulesd...
Jan 04 10:29:37 ip-10-0-0-20 env[58672]: Completed.
Jan 04 10:29:37 ip-10-0-0-20 systemd[1]: Started Wazuh manager.

ubuntu@ip-10-0-0-20:~$
```

```
ubuntu@ip-10-0-0-20:~$ sudo systemctl status wazuh-indexer
● wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2026-01-04 10:28:15 UTC; 34min ago
       Docs: https://documentation.wazuh.com
   Main PID: 15204 (java)
      Tasks: 74 (limit: 4580)
     Memory: 2.2G
        CPU: 1min 32.390s
     CGroup: /system.slice/wazuh-indexer.service
             └─15204 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopen>

Jan 04 10:27:55 ip-10-0-0-20 systemd[1]: Starting Wazuh-indexer...
Jan 04 10:27:58 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: A terminally deprecated method in java.lang.System has>
Jan 04 10:27:58 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: System::setSecurityManager has been called by org.open>
Jan 04 10:27:58 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: Please consider reporting this to the maintainers of o>
Jan 04 10:27:58 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: System::setSecurityManager will be removed in a future>
Jan 04 10:28:00 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: A terminally deprecated method in java.lang.System has>
Jan 04 10:28:00 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: System::setSecurityManager has been called by org.open>
Jan 04 10:28:00 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: Please consider reporting this to the maintainers of o>
Jan 04 10:28:00 ip-10-0-0-20 systemd-entrypoint[15204]: WARNING: System::setSecurityManager will be removed in a future>
Jan 04 10:28:15 ip-10-0-0-20 systemd[1]: Started Wazuh-indexer.

ubuntu@ip-10-0-0-20:~$
```

```
ubuntu@ip-10-0-0-20:~$
ubuntu@ip-10-0-0-20:~$ sudo systemctl status wazuh-dashboard
● wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2026-01-04 10:31:04 UTC; 34min ago
   Main PID: 61046 (node)
      Tasks: 11 (limit: 4580)
     Memory: 210.0M
        CPU: 12.710s
     CGroup: /system.slice/wazuh-dashboard.service
             └─61046 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-rejecti>

Jan 04 10:31:15 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:15Z","tags":["info",>
Jan 04 10:31:15 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:15Z","tags":["info",>
Jan 04 10:31:15 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:15Z","tags":["info",>
Jan 04 10:31:15 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:15Z","tags":["info",>
Jan 04 10:31:16 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:16Z","tags":["info",>
Jan 04 10:31:16 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:16Z","tags":["info",>
Jan 04 10:31:16 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:16Z","tags":["info",>
Jan 04 10:31:17 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:17Z","tags":["listen>
Jan 04 10:31:17 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"log","@timestamp":"2026-01-04T10:31:17Z","tags":["info",>
Jan 04 10:31:33 ip-10-0-0-20 opensearch-dashboards[61046]: {"type":"response","@timestamp":"2026-01-04T10:31:32Z","tags":[],>

ubuntu@ip-10-0-0-20:~$
```

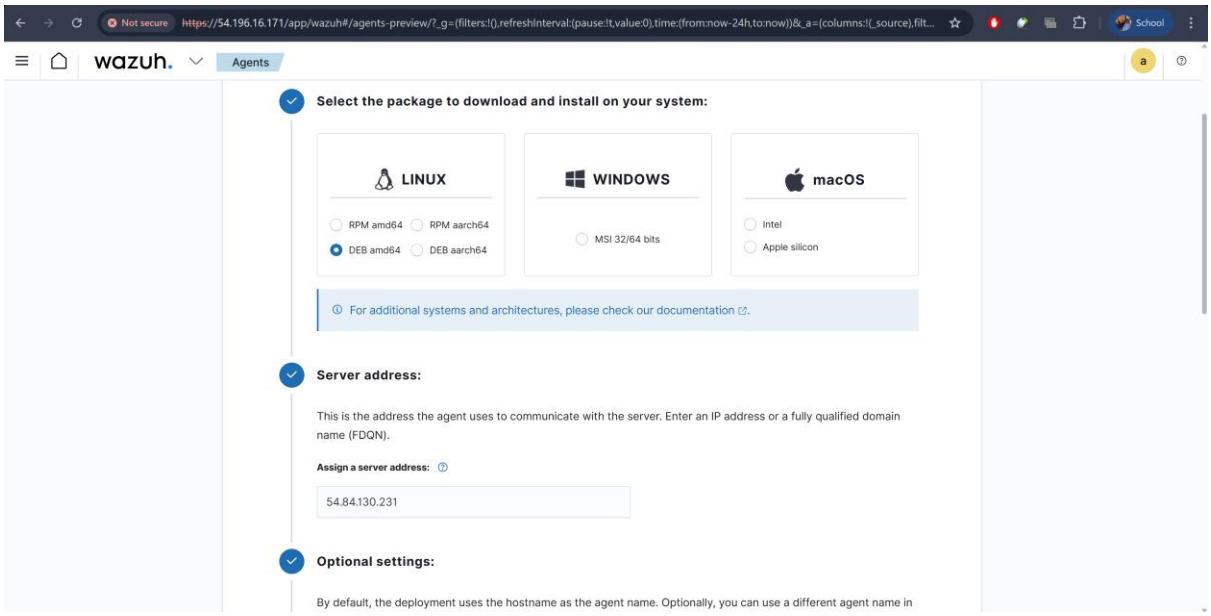
- Connexion à l'interface Wazuh

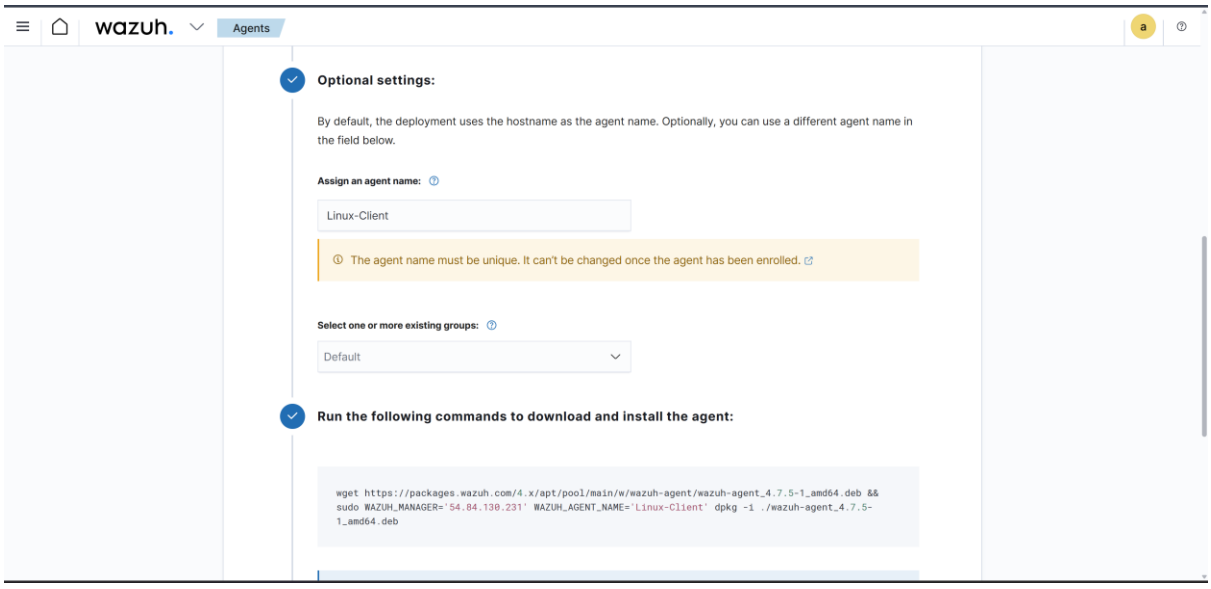


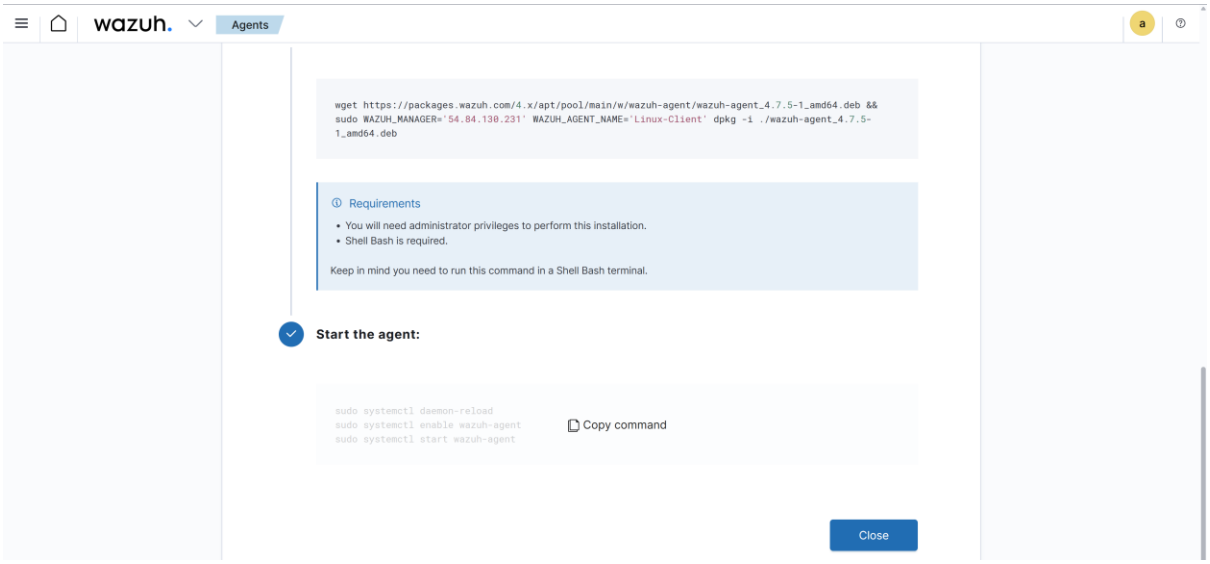


8.Enrôler le client Linux et Windows

- Via le dashboard Wazuh → Agents management → Deploy new agent

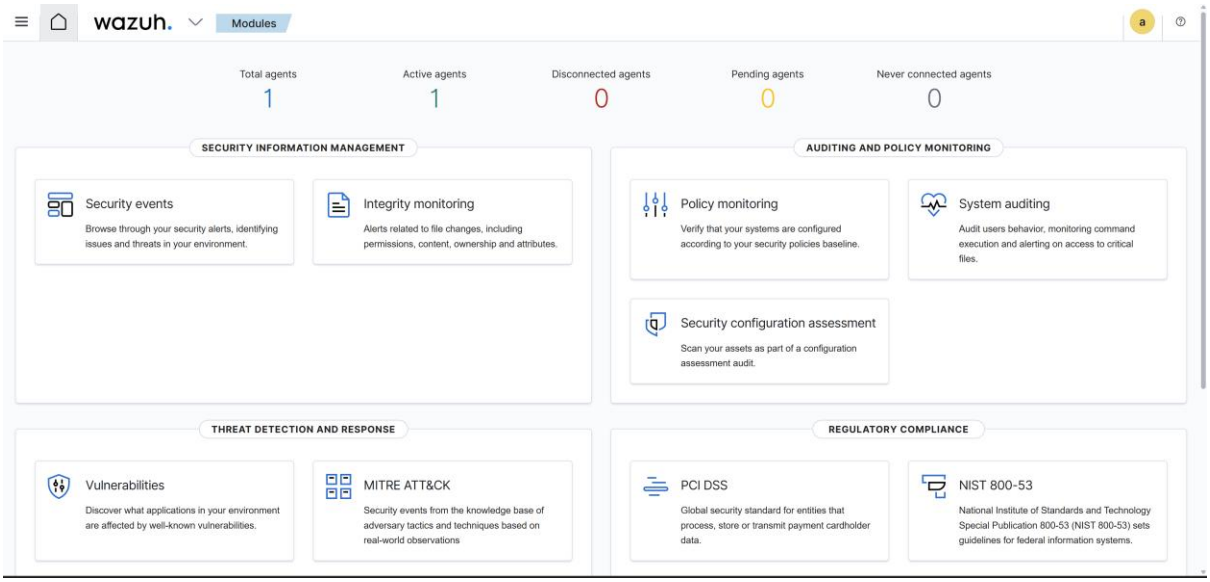


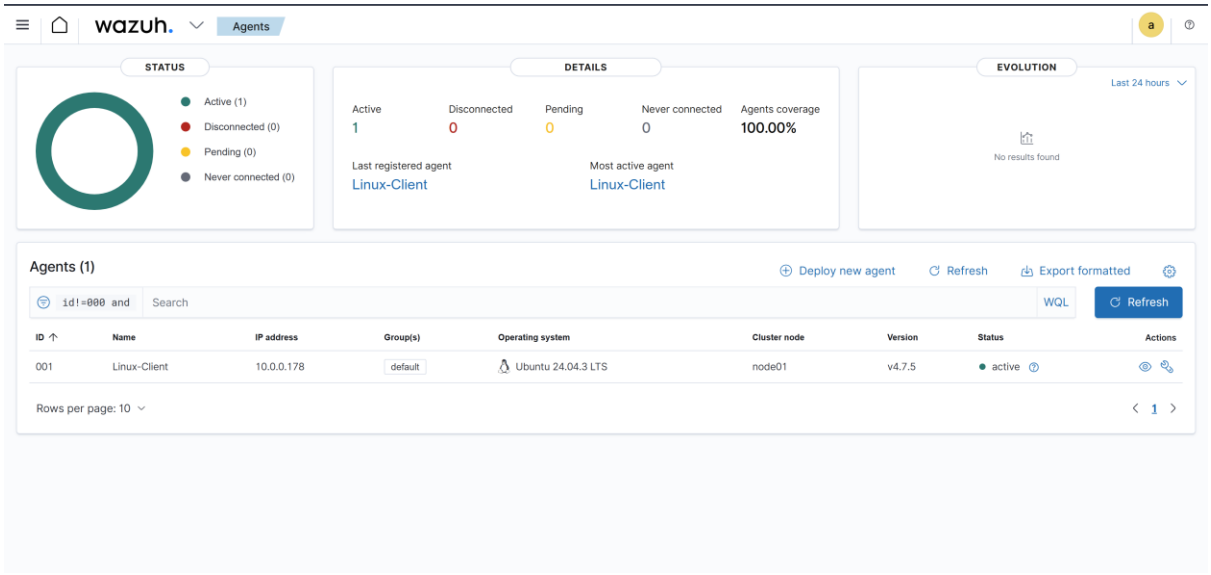


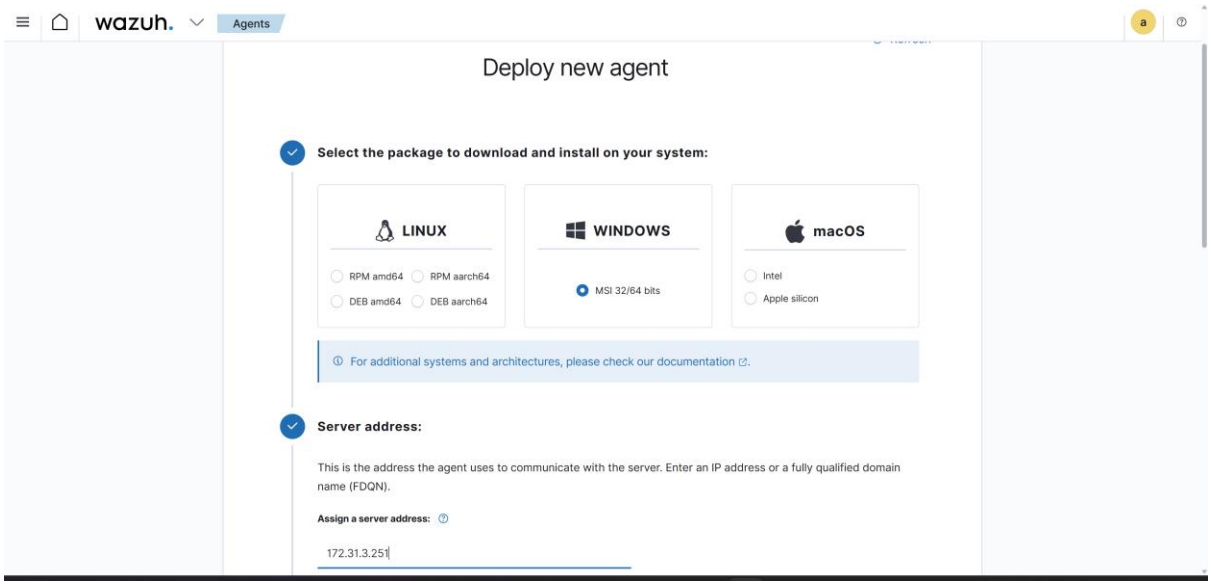


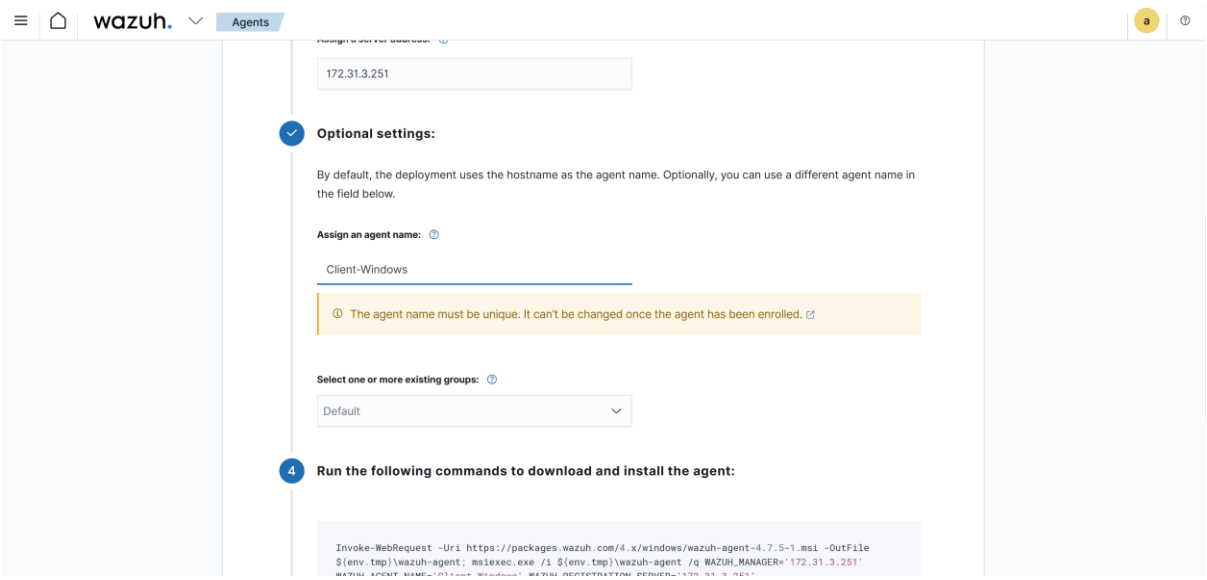
➢ Sélection Linux → Copier commandes et exécuter sur le client

```
ubuntu@ip-10-0-0-178:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb &&
 sudo WAZUH_MANAGER='34.229.165.166' WAZUH_AGENT_NAME='Linux-Client' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
--2026-01-06 14:40:06--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 13.226.209.39, 13.226.209.78, 13.226.209.111, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|13.226.209.39|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9378818 (8.9M) [application/vnd.debian.binary-package]
Saving to: ‘wazuh-agent_4.7.5-1_amd64.deb’

wazuh-agent_4.7.5-1_amd64.deb 100%[=============================================>]   8.94M  51.7MB/s    in 0.2s

2026-01-06 14:40:07 (51.7 MB/s) - ‘wazuh-agent_4.7.5-1_amd64.deb’ saved [9378818/9378818]

Selecting previously unselected package wazuh-agent.
(Reading database ... 71735 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.5-1_amd64.deb ...
Unpacking wazuh-agent (4.7.5-1) ...
Setting up wazuh-agent (4.7.5-1) ...
ubuntu@ip-10-0-0-178:~$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
ubuntu@ip-10-0-0-178:~$
```



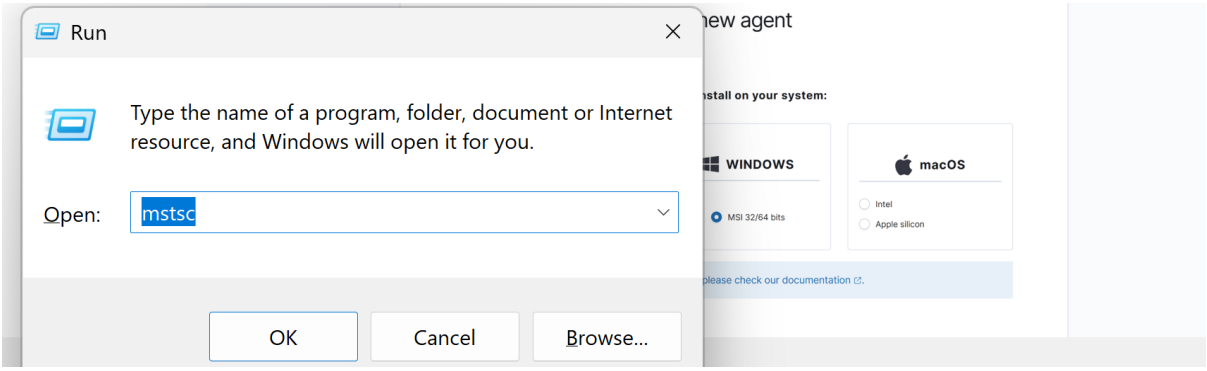

wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active 1
Disconnected 0
Pending 0
Never connected 0
Agents coverage 100.00%
Last registered agent
Linux-Client
Most active agent
Linux-Client
EVOLUTION
Last 24 hours
No results found
Agents (1)
Deploy new agent
Refresh
Export formatted
id!=000 and
Search
WQL
Refresh
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
001
Linux-Client
10.0.0.178
default
Ubuntu 24.04.3 LTS
node01
v4.7.5
active
Rows per page: 10
1

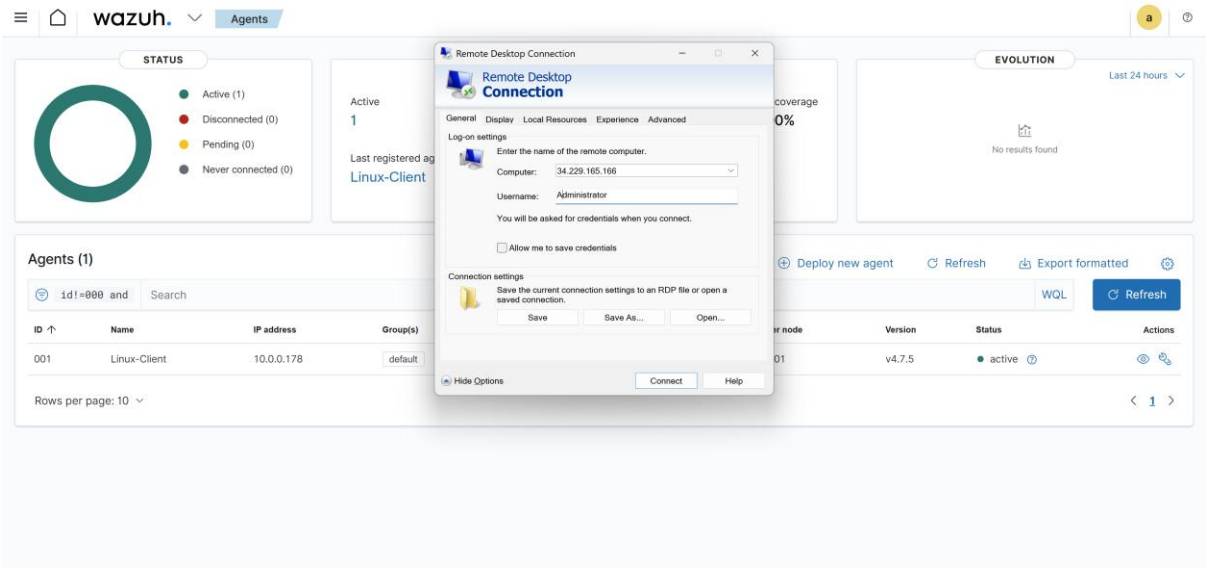

wazuh.
Agents
Deploy new agent
Select the package to download and install on your system:
LINUX
RPM amd64
RPM aarch64
DEB amd64
DEB aarch64
WINDOWS
MSI 32/64 bits
macOS
Intel
Apple silicon
For additional systems and architectures, please check our documentation.
Server address:
This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).
Assign a server address:
172.31.3.251

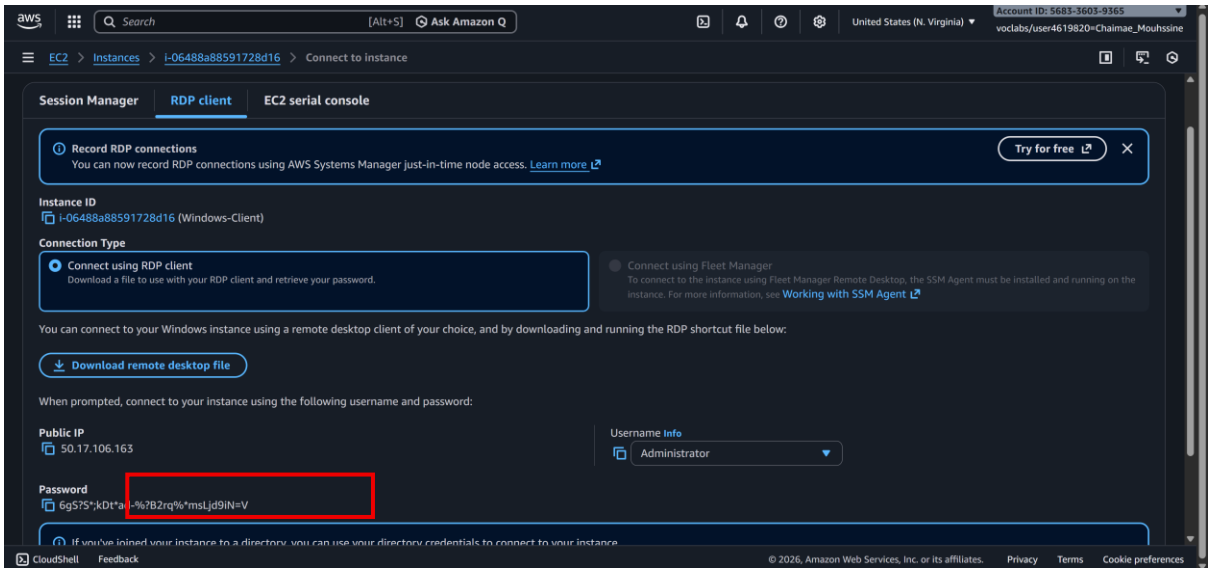


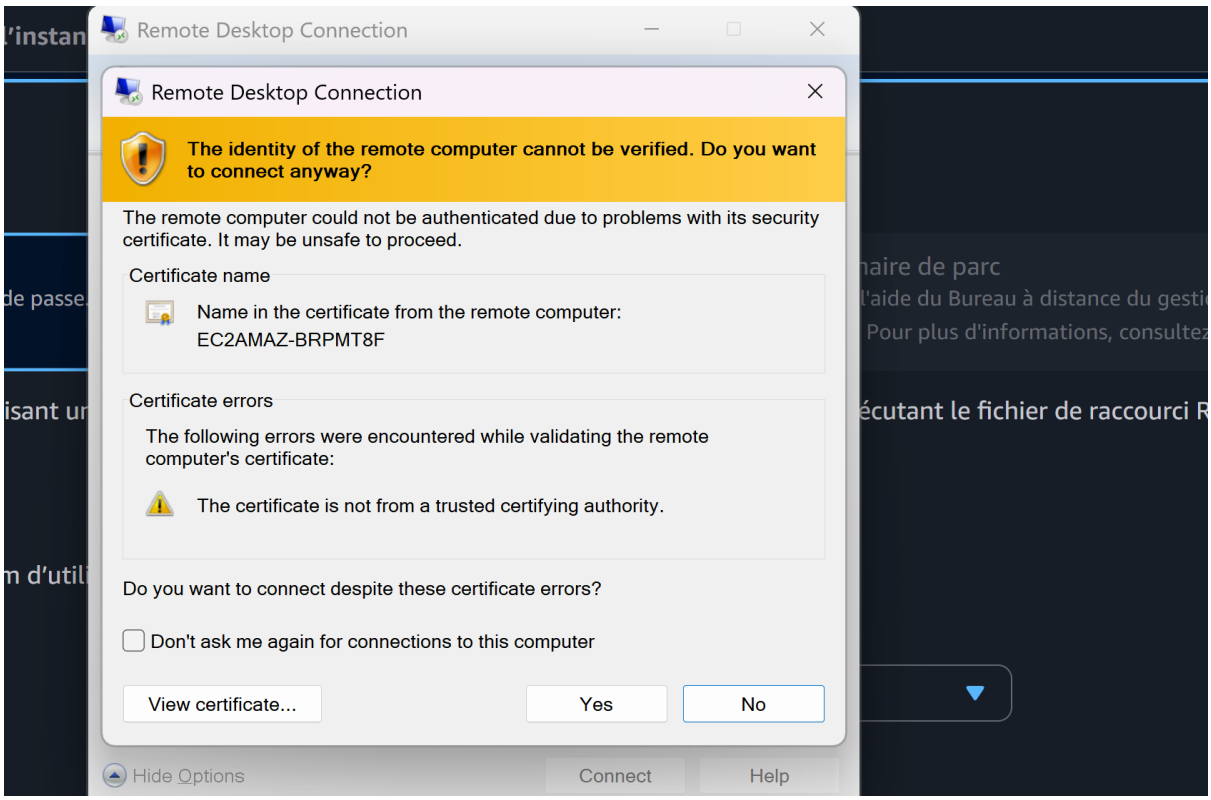
Connexion au EC2 WINDOWS_CLIENT via RDP

- On ouvre cmd+r et on tape la commande : mstsc



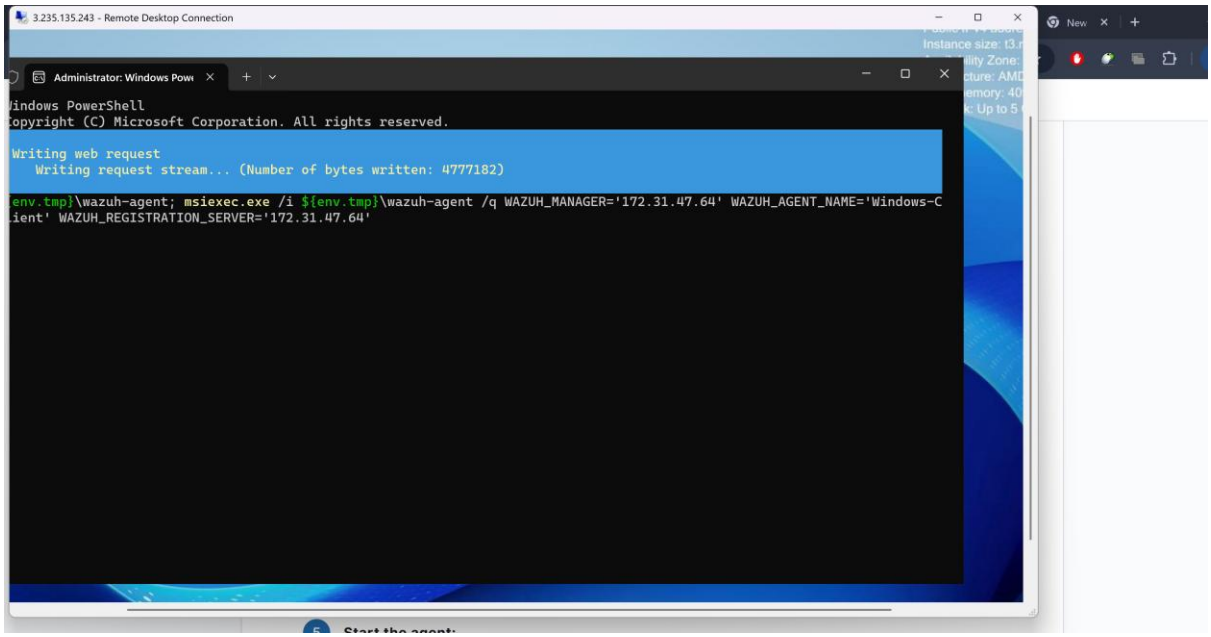


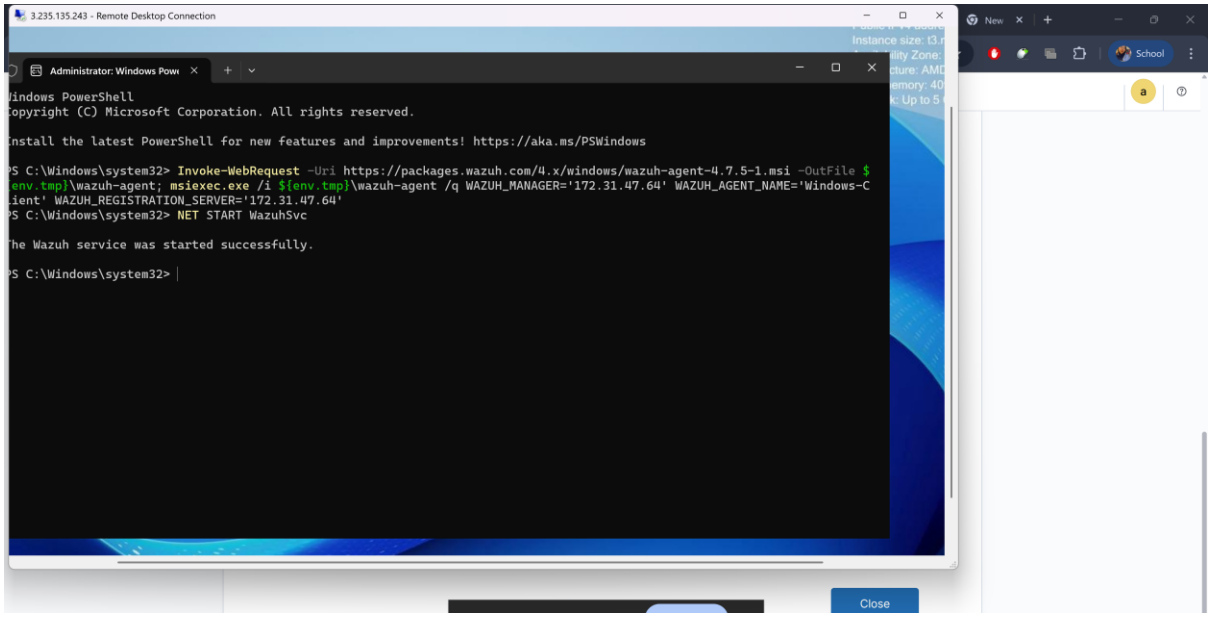


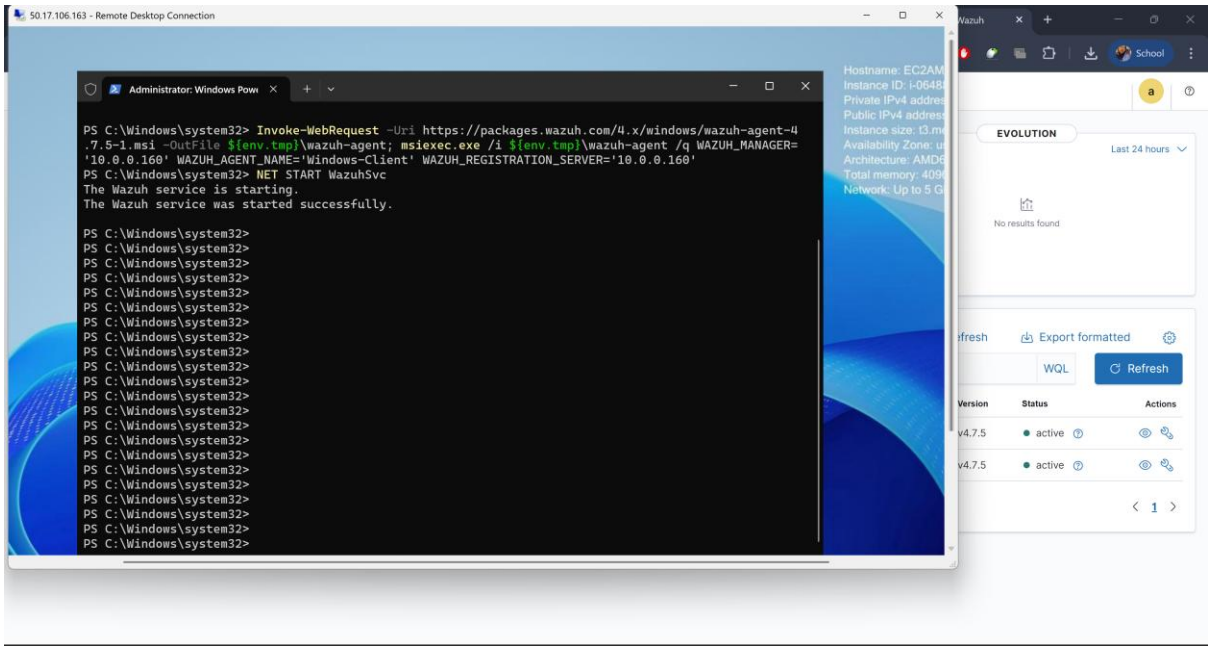


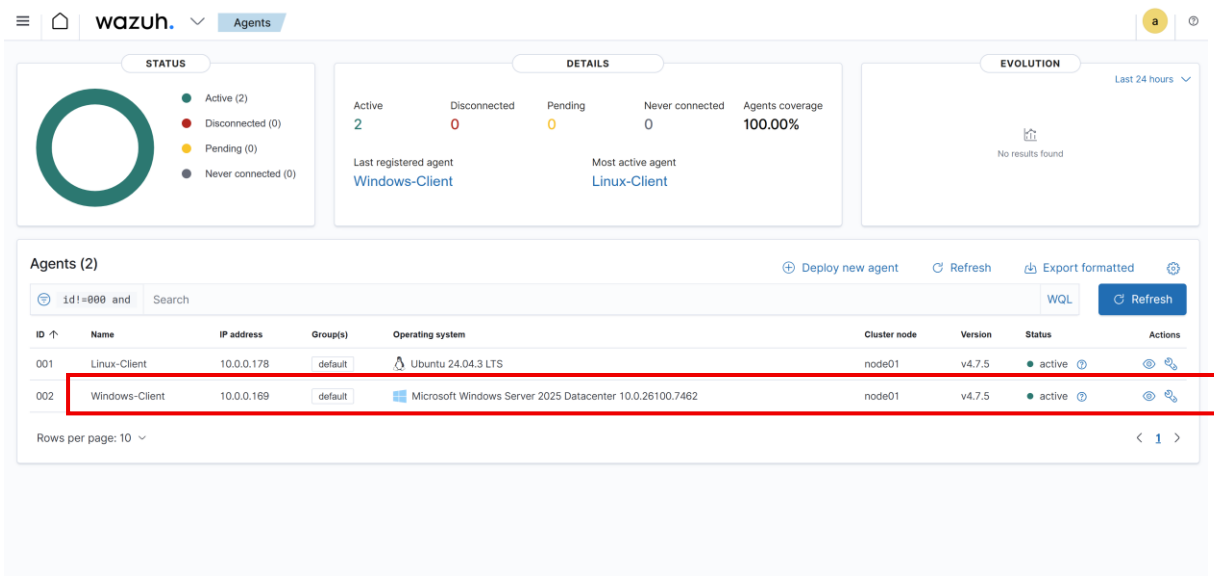
Passer dans powershell :

- Installation agent depuis dashboard (PowerShell)


3.235.135.243 - Remote Desktop Connection
Administrator: Windows Powe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Writing web request
Writing request stream... (Number of bytes written: 4777182)
env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='172.31.47.64' WAZUH_AGENT_NAME='Windows-C
lient' WAZUH_REGISTRATION_SERVER='172.31.47.64'
New


3.235.135.243 - Remote Desktop Connection
Administrator: Windows Powe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $
env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='172.31.47.64' WAZUH_AGENT_NAME='Windows-C
lient' WAZUH_REGISTRATION_SERVER='172.31.47.64'
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service was started successfully.
PS C:\Windows\system32>
New
School
Close





L'enrôlement centralisé facilite la gestion des endpoints à grande échelle.

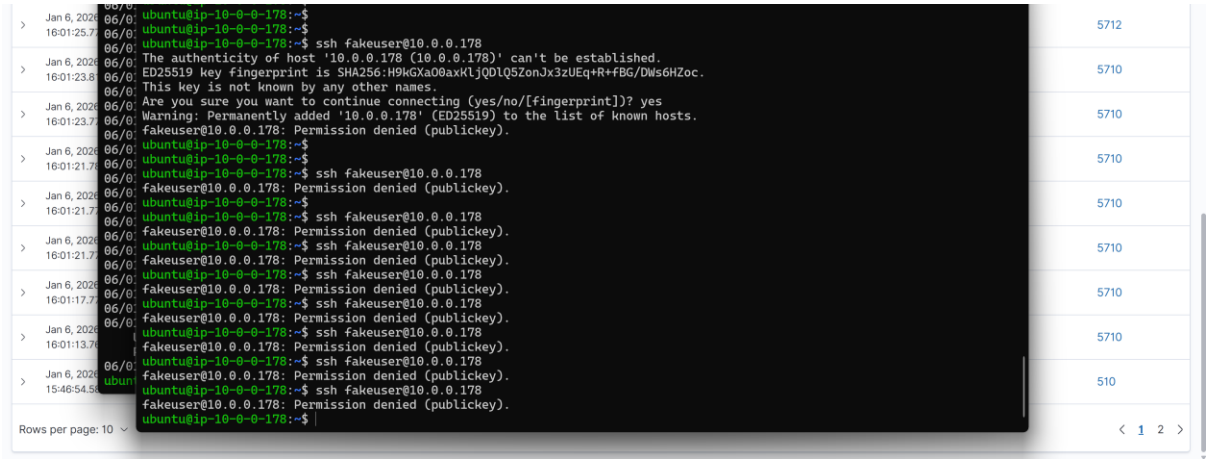
9. Scénarios de démonstration SIEM & EDR

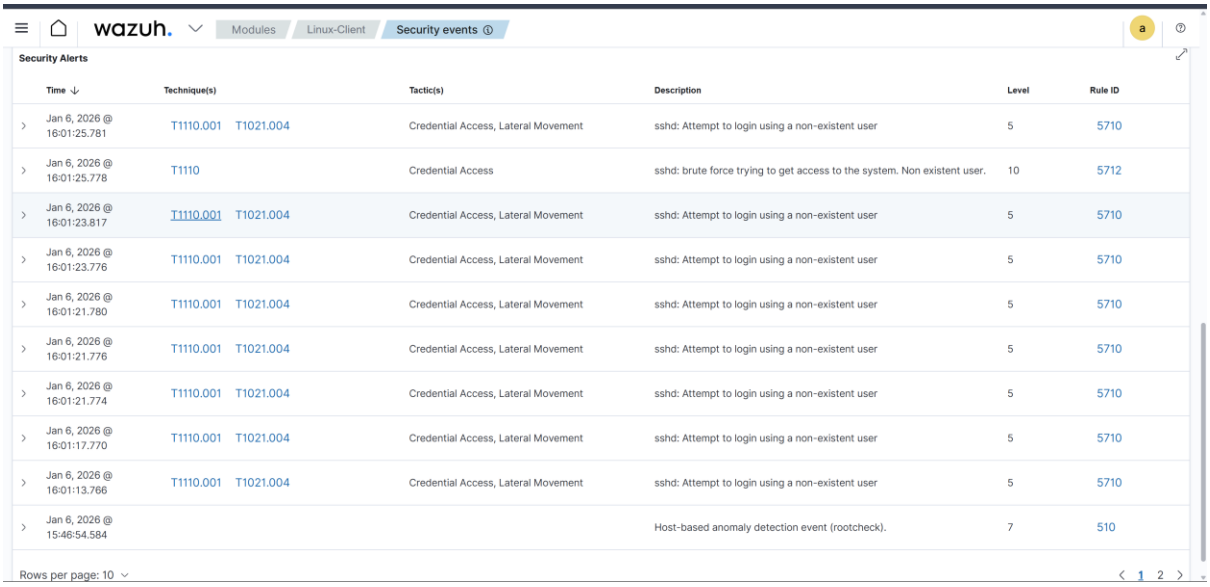
9.1 Côté Linux

9.1.1 Scénario 1 — Tentatives SSH échouées (bruteforce simulé)

Sur Linux-Client (ou depuis une autre machine), fais plusieurs tentatives de login SSH invalides :

ssh fakeuse@10.0.0.178

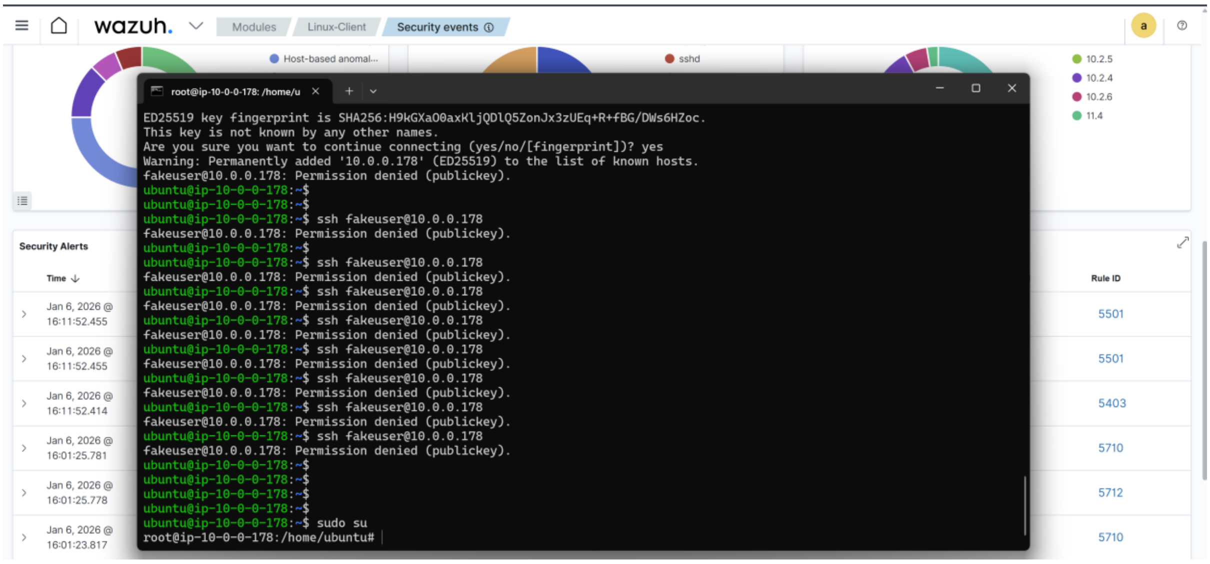


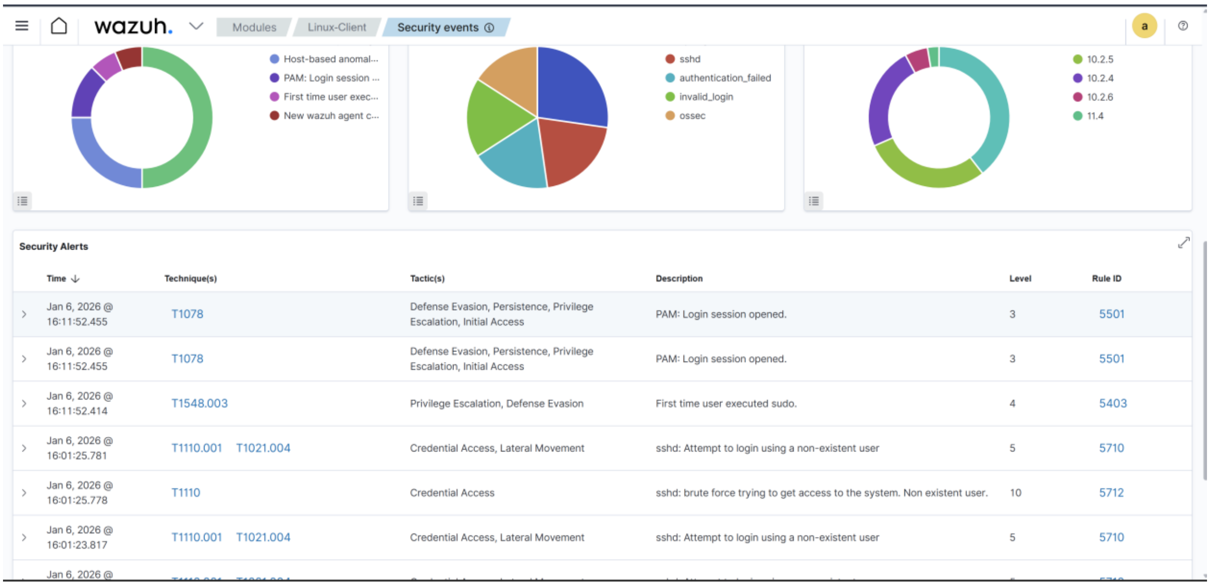


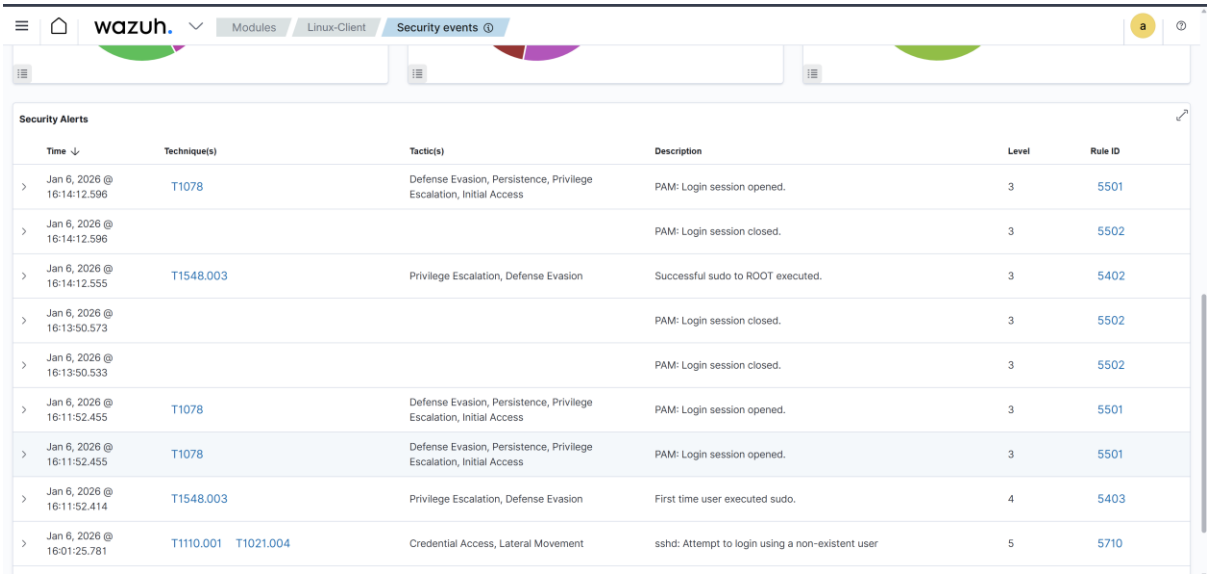
- Tentatives SSH échouées
- Élévation de privilèges
- Modification de fichiers sensibles (FIM)

9.1.2 Scénario 2 — Élévation de privileges

sudo su



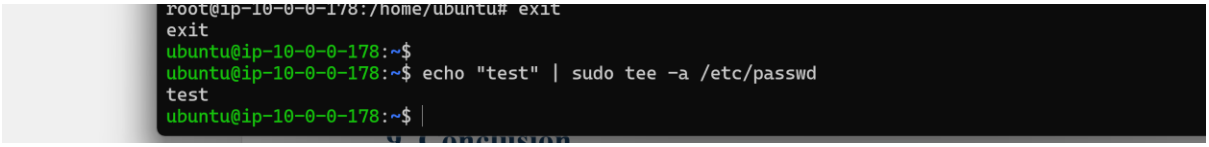




Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 6, 2026 @ 16:14:12.596	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 6, 2026 @ 16:14:12.596			PAM: Login session closed.	3	5502
Jan 6, 2026 @ 16:14:12.555	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Jan 6, 2026 @ 16:13:50.573			PAM: Login session closed.	3	5502
Jan 6, 2026 @ 16:13:50.533			PAM: Login session closed.	3	5502
Jan 6, 2026 @ 16:11:52.455	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 6, 2026 @ 16:11:52.455	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 6, 2026 @ 16:11:52.414	T1548.003	Privilege Escalation, Defense Evasion	First time user executed sudo.	4	5403
Jan 6, 2026 @ 16:01:25.781	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

9.1.3 Scénario 3 — Modification fichier sensible

echo "test" | sudo tee -a /etc/passwd

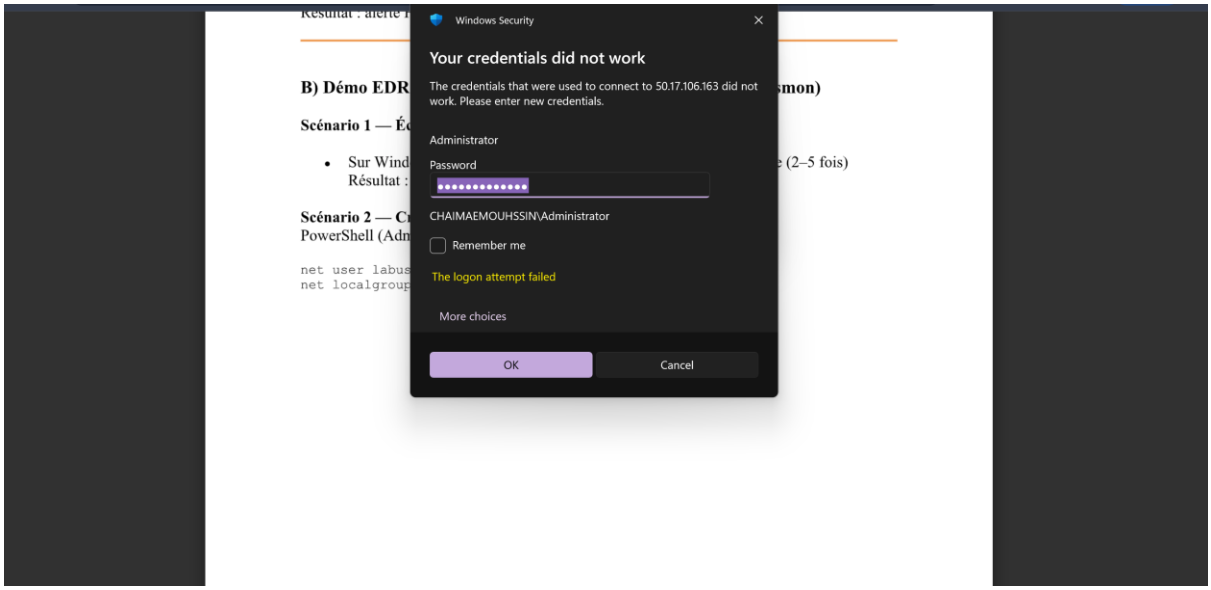


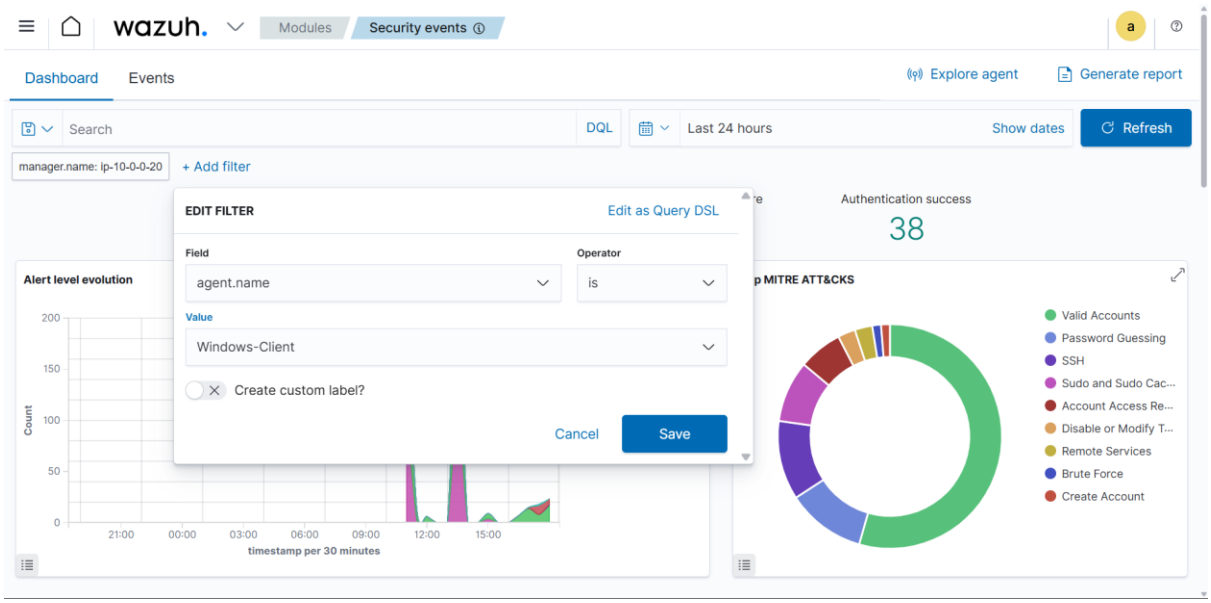
Jan 6, 2026 @ 16:11:52.455	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 6, 2026 @ 16:11:52.455	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
Jan 6, 2026 @ 16:11:52.414	T1548.003	Privilege Escalation, Defense Evasion	First time user executed sudo.	4	5403

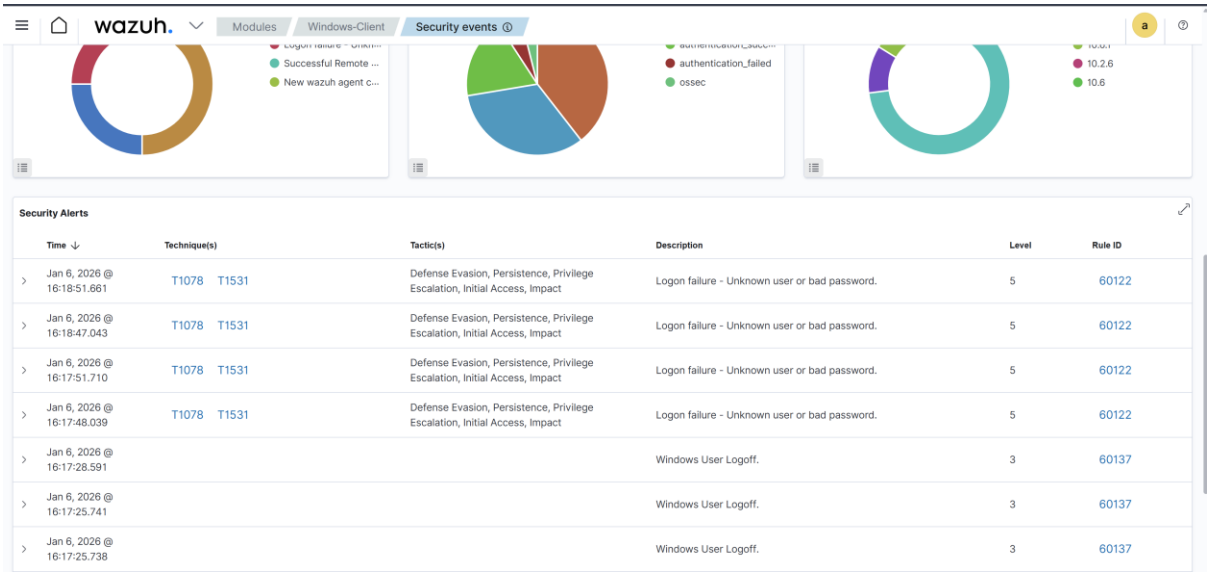
9.2 Scénarios côté Windows

9.2.1 Scénario 1 — Échecs de login

Sur Windows : on realise des connexions RDP avec mauvais mot de passe







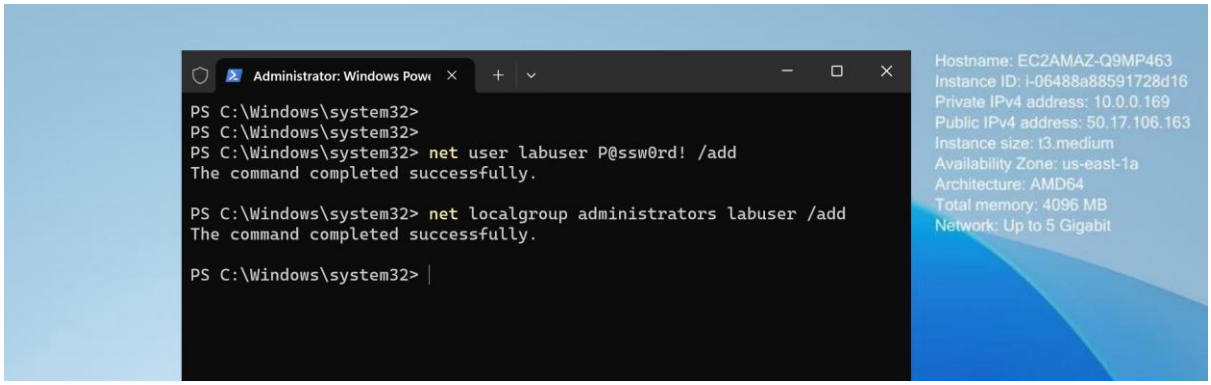
Security Alerts

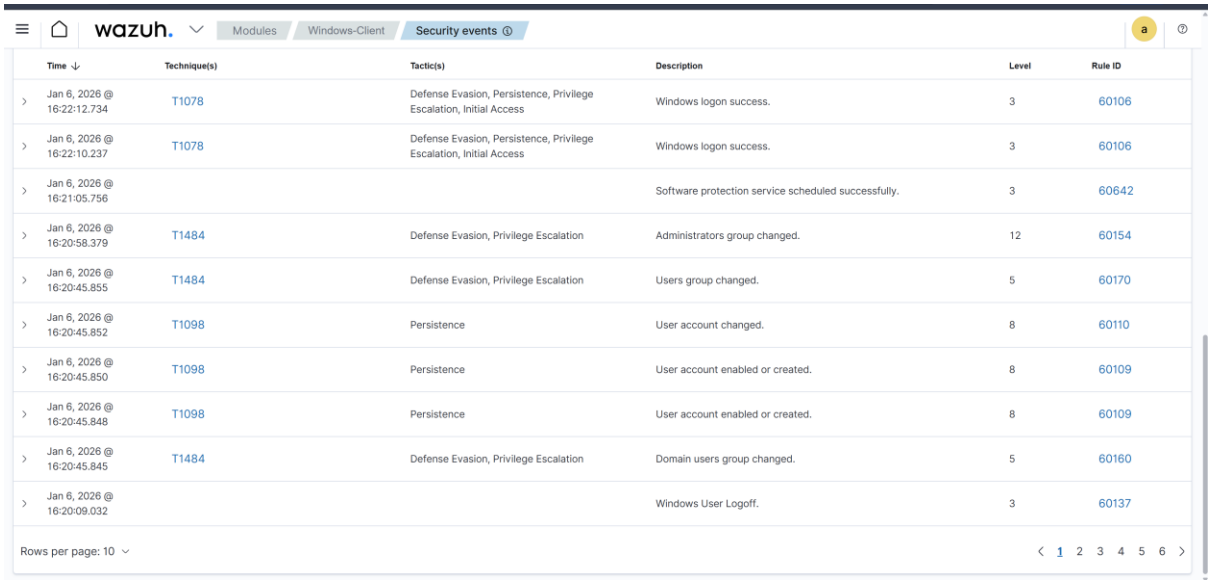
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 6, 2026 @ 16:18:51.661	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Jan 6, 2026 @ 16:18:47.043	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Jan 6, 2026 @ 16:17:51.710	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Jan 6, 2026 @ 16:17:48.039	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Jan 6, 2026 @ 16:17:28.591			Windows User Logoff.	3	60137
Jan 6, 2026 @ 16:17:25.741			Windows User Logoff.	3	60137
Jan 6, 2026 @ 16:17:25.738			Windows User Logoff.	3	60137

9.2.2 Scénario 2 — Création d'un utilisateur local

PowerShell (Admin) :

- net user labuser P@ssw0rd! /add
- net localgroup administrators labuser /add





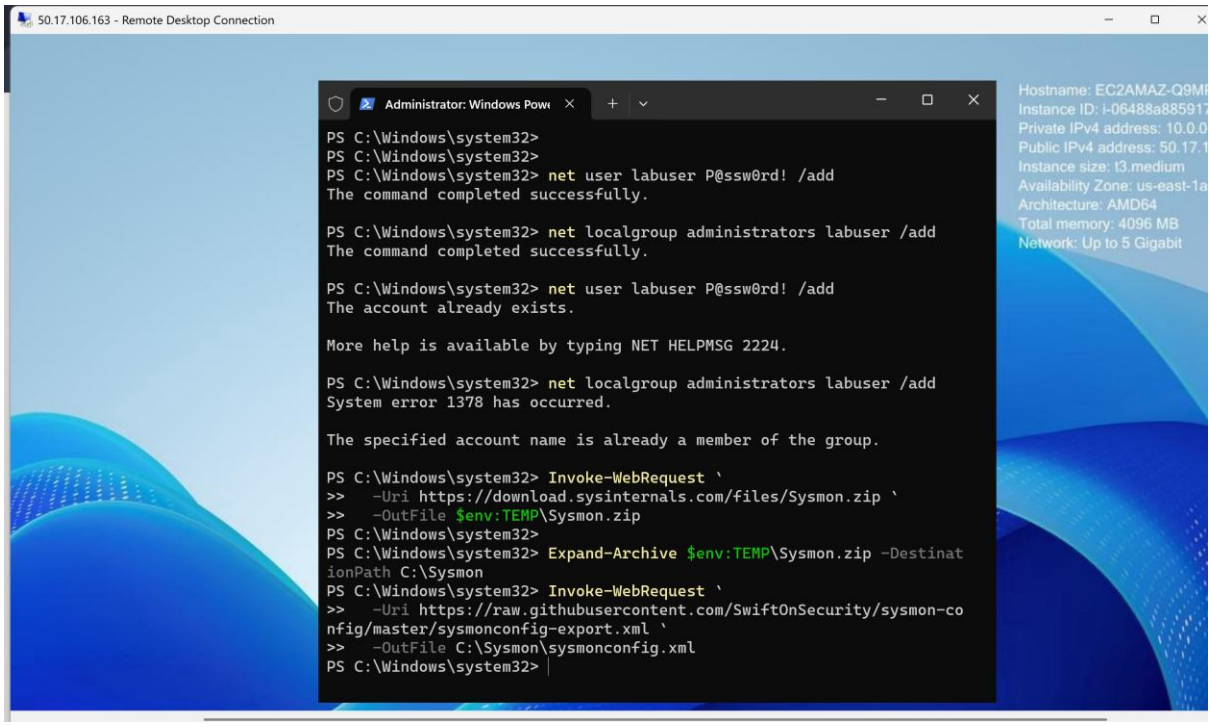
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 6, 2026 @ 16:22:12.734	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jan 6, 2026 @ 16:22:10.237	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jan 6, 2026 @ 16:21:05.756			Software protection service scheduled successfully.	3	60642
Jan 6, 2026 @ 16:20:58.379	T1484	Defense Evasion, Privilege Escalation	Administrators group changed.	12	60154
Jan 6, 2026 @ 16:20:45.855	T1484	Defense Evasion, Privilege Escalation	Users group changed.	5	60170
Jan 6, 2026 @ 16:20:45.852	T1098	Persistence	User account changed.	8	60110
Jan 6, 2026 @ 16:20:45.850	T1098	Persistence	User account enabled or created.	8	60109
Jan 6, 2026 @ 16:20:45.848	T1098	Persistence	User account enabled or created.	8	60109
Jan 6, 2026 @ 16:20:45.845	T1484	Defense Evasion, Privilege Escalation	Domain users group changed.	5	60160
Jan 6, 2026 @ 16:20:09.032			Windows User Logoff.	3	60137

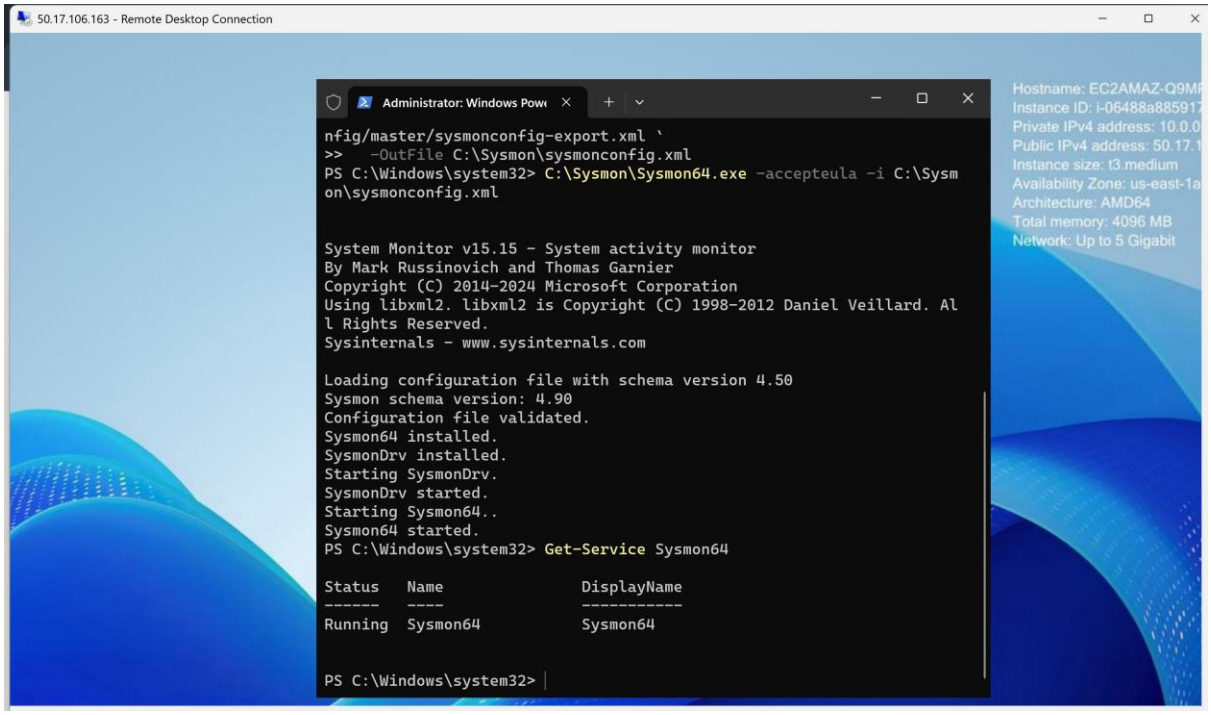
Rows per page: 10 1 2 3 4 5 6

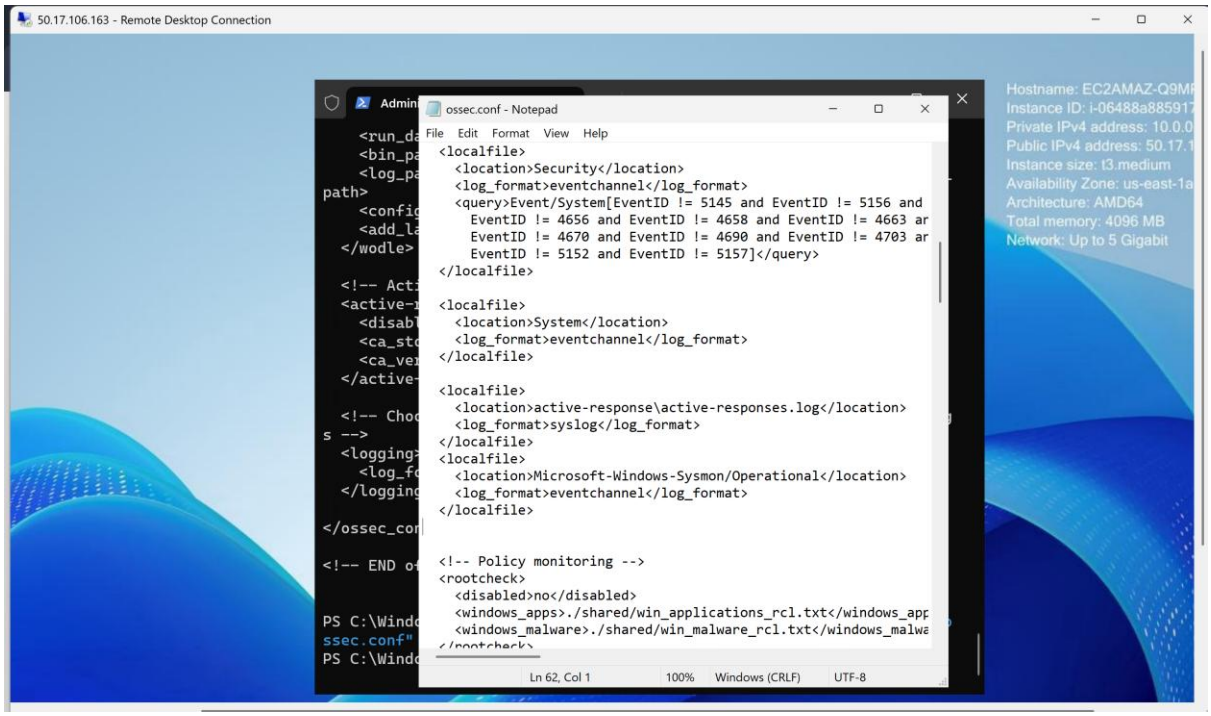
9.2.3 Scénario 3— Option "EDR plus riche": installer Sysmon

Installation Sysmon

- Invoke-WebRequest -Uri https://download.sysinternals.com/files/Sysmon.zip -OutFile C:\Sysmon.zip
- Expand-Archive -Path C:\Sysmon.zip -DestinationPath C:\Sysmon

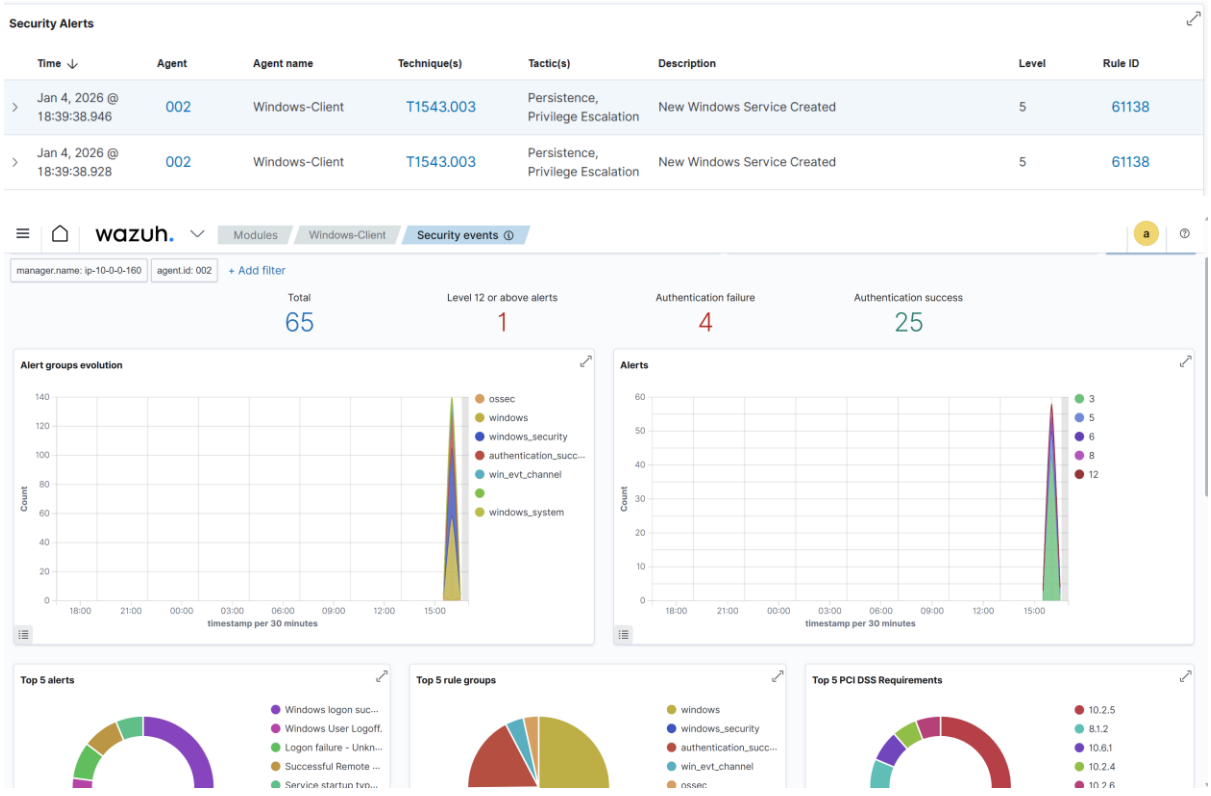

50.17.106.163 - Remote Desktop Connection
Administrator: Windows Powe
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> net user labuser P@ssw0rd! /add
The command completed successfully.
PS C:\Windows\system32> net localgroup administrators labuser /add
The command completed successfully.
PS C:\Windows\system32> net user labuser P@ssw0rd! /add
The account already exists.
More help is available by typing NET HELPMSG 2224.
PS C:\Windows\system32> net localgroup administrators labuser /add
System error 1378 has occurred.
The specified account name is already a member of the group.
PS C:\Windows\system32> Invoke-WebRequest `
>> -Uri https://download.sysinternals.com/files/Sysmon.zip `
>> -OutFile $env:TEMP\Sysmon.zip
PS C:\Windows\system32>
PS C:\Windows\system32> Expand-Archive $env:TEMP\Sysmon.zip -Destinat
ionPath C:\Sysmon
PS C:\Windows\system32> Invoke-WebRequest `
>> -Uri https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-co
nfig/master/sysmonconfig-export.xml `
>> -OutFile C:\Sysmon\sysmonconfig.xml
PS C:\Windows\system32>
Hostname: EC2AMAZ-Q9M
Instance ID: i-06488a885917
Private IPv4 address: 10.0.0.
Public IPv4 address: 50.17.1
Instance size: t3.medium
Availability Zone: us-east-1a
Architecture: AMD64
Total memory: 4096 MB
Network: Up to 5 Gigabit


50.17.106.163 - Remote Desktop Connection
Administrator: Windows Powe
nfig/master/sysmonconfig-export.xml `
>> -OutFile C:\Sysmon\sysmonconfig.xml
PS C:\Windows\system32> C:\Sysmon\Sysmon64.exe -accepteula -i C:\Sysm
on\sysmonconfig.xml
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. Al
l Rights Reserved.
Sysinternals - www.sysinternals.com
Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Windows\system32> Get-Service Sysmon64
Status Name DisplayName
------ ---- -----------
Running Sysmon64 Sysmon64
PS C:\Windows\system32>
Hostname: EC2AMAZ-Q9M
Instance ID: i-06488a885917
Private IPv4 address: 10.0.0.
Public IPv4 address: 50.17.1
Instance size: t3.medium
Availability Zone: us-east-1a
Architecture: AMD64
Total memory: 4096 MB
Network: Up to 5 Gigabit



Ces scénarios démontrent la capacité de Wazuh à détecter des comportements suspects et à générer des alertes pertinentes.

10. Visualisation dans le Dashboard Wazuh



11. Conclusion

Cet atelier a permis de mettre en œuvre une plateforme SIEM & EDR complète, intégralement conçue et configurée en détail, depuis la création du réseau Cloud jusqu'à l'analyse avancée des événements de sécurité.

La création d'un VPC personnalisée, le déploiement multi-OS et la configuration fine des règles de sécurité illustrent une démarche professionnelle conforme aux standards des infrastructures modernes.

Wazuh s'impose comme une solution robuste, capable de fournir une vision centralisée, proactive et corrélée des événements de sécurité, renforçant ainsi significativement la posture de sécurité globale.

Webographie

https://github.com/CHAIMAEMOUHSSINE/Security-Lab-Endpoints-Supervision-SIEM-Multi-OS-Linux-Windows-.git