

Département Mathématique et Informatique

Filière : «BDCC2»

Virtualisation et Cloud Computing

Compte rendu

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

Réalisé par :

FENJIRO WIAM

Encadré par :

Pr. Azeddine KHIAT

Année Universitaire 2025-2026

Table des matières

Introduction.....	4
1. Présentation générale	4
1.1 Objectifs de l'activité	4
1.2 Présentation de Wazuh	5
1.3 Prérequis.....	5
2. Architecture du Lab Wazuh sur AWS.....	5
2.1 Vue générale de l'architecture	5
2.2 Composants de l'architecture	6
2.3 Rôle du serveur Wazuh (All-in-One).....	7
2.4 Rôle des endpoints supervisés	7
2.5 Flux réseau et communications.....	7
3. Description de l'activité.....	8
Etape 1 : Connexion à la console AWS	8
Etape 2 : Création de l'infrastructure du réseau.....	8
2.1 : création du VPC	8
2.2 : Création des groupes de sécurités	14
Etape 3 : Déploiement des instances EC2	19
3.1 : Serveur Wazuh (Ubuntu)	20
3.2 : Wazuh Linux Client	24
3.3 : Wazuh Windows Client.....	28
Etape 4 : Installation de Wazuh.....	33
4.1 Connexion SSH.....	33
4.2 Installation de Wazuh	33
4.3 Vérification des services	34
Étape 5 : Accès au Wazuh Dashboard	35
Étape 6 : Enrôlement du client Linux.....	38
6.1 Sélection du package à télécharger et à installer sur le système.....	39
6.2 Adresse du serveur	39
6.3 Paramètres optionnels	40
6.4 Exécution des commandes pour télécharger et installer l'agent (client Linux)	40

6.5 Démarrage de l'agent	42
Étape 7 : Enrôlement du client Windows	43
7.1 Sélection du package à télécharger et à installer sur le système	44
7.2 Adresse du serveur	44
7.3 Paramètres optionnels	44
7.4 Exécution des commandes pour télécharger et installer l'agent (client Windows).....	45
7.5 Démarrage de l'agent	51
Étape 8 : Scénarios de démonstration de sécurité (Démo SIEM + EDR : scénarios d'événements à générer)	51
8.1 Scénarios pour Linux Client (Démo SIEM côté Linux (rapide, visible tout de suite)).....	51
8.2 Scénarios pour Windows Client (Démo EDR côté Windows (événements sécurité + option Sysmon))	54
4. Analyse et résultats	57
4.1 Détection des événements de sécurité	57
4.1.1 Résultats côté client Linux	57
4.1.2 Résultats côté client Windows	58
4.2 Apport du SIEM dans la supervision.....	59
5. Apports de l'atelier : SIEM, EDR, IAM/PAM et Threat Hunting	60
5.1 Apport du SIEM dans l'atelier.....	60
5.2 Apport de l'EDR dans la sécurité des endpoints.....	61
5.3 Comparaison.....	62
5.4 IAM / PAM et contrôle des accès	62
5.5 Threat Hunting appliqué dans le lab	63
Conclusion	63

Introduction

La sécurité des systèmes d'information constitue aujourd'hui un enjeu majeur pour les organisations, en particulier dans des environnements Cloud de plus en plus distribués et exposés aux menaces.

Dans ce contexte, ce projet, intitulé « **Atelier_Sécurité des endpoints et supervision SIEM : étude de cas multi-OS (Linux & Windows)** », s'inscrit dans le cadre du module **Virtualisation et Cloud Computing**.

L'objectif principal de ce projet est de mettre en place une **plateforme opérationnelle de supervision et de protection des systèmes**, capable de collecter, centraliser et analyser les événements de sécurité sur des environnements Linux et Windows. Pour cela, j'ai utilisé **Wazuh**, une solution combinant les approches **SIEM (Security Information and Event Management)** et **EDR (Endpoint Detection and Response)**, déployée sur un environnement Cloud AWS.

Ce projet illustre concrètement le fonctionnement d'un **SOC moderne**, en montrant comment les événements de sécurité générés sur les endpoints sont centralisés sur le serveur Wazuh et analysés via le dashboard SIEM. Il couvre notamment trois axes principaux :

- **La sécurité des endpoints et le renforcement des systèmes,**
- **La gestion des identités et des accès (IAM / PAM),**
- **La supervision et la détection des menaces** avec des scénarios pratiques de threat hunting.

L'ensemble de la documentation du TP, incluant le rapport final, le schéma d'architecture ainsi que les captures d'écran des différentes étapes de réalisation, est disponible dans un dépôt GitHub public accessible à l'adresse suivante :

<https://github.com/WiamFen/Wazuh-SIEM-endpoints-AWS/>

1. Présentation générale

1.1 Objectifs de l'activité

Les objectifs principaux de ce projet sont :

- **Mettre en place une plateforme de supervision de sécurité** fonctionnelle sur AWS, intégrant Wazuh pour la collecte et l'analyse des événements.
- **Installer et configurer les agents Wazuh** sur des endpoints Linux et Windows pour assurer la surveillance des systèmes.
- **Observer et analyser les événements de sécurité** générés sur les endpoints en temps réel via le dashboard SIEM.
- **Comprendre le fonctionnement d'un SOC moderne**, avec l'intégration SIEM et EDR pour détecter et corrélérer les menaces.

- **Appliquer les bonnes pratiques de sécurité**, notamment la gestion des accès (IAM/PAM) et le renforcement des systèmes.
- **Réaliser des démonstrations concrètes** de détection de menaces sur Linux et Windows, illustrant le rôle des alertes et la réponse aux incidents.

1.2 Présentation de Wazuh

Wazuh est une solution open-source combinant :

- **SIEM (Security Information and Event Management)** pour la collecte, l'analyse et la corrélation des événements de sécurité.
- **EDR (Endpoint Detection and Response)** pour la surveillance des endpoints et la détection des menaces.
Dans cet atelier, Wazuh est déployé sur AWS dans un **VPC sécurisé**, avec :
 - Un serveur Ubuntu central hébergeant Wazuh (manager, indexer, dashboard).
 - Un client Linux et un client Windows supervisés par Wazuh.
Le serveur central collecte et analyse les événements remontés par les agents installés sur les clients.

1.3 Prérequis

Avant de commencer l'activité, les prérequis sont :

- Compte AWS actif avec accès au Learner Lab.
- Connaissances de base en **Linux, Windows et réseau**.
- Navigateur web pour accéder au dashboard Wazuh et à la console AWS.
- Connaissance des notions de base en **sécurité des systèmes et gestion des accès**.

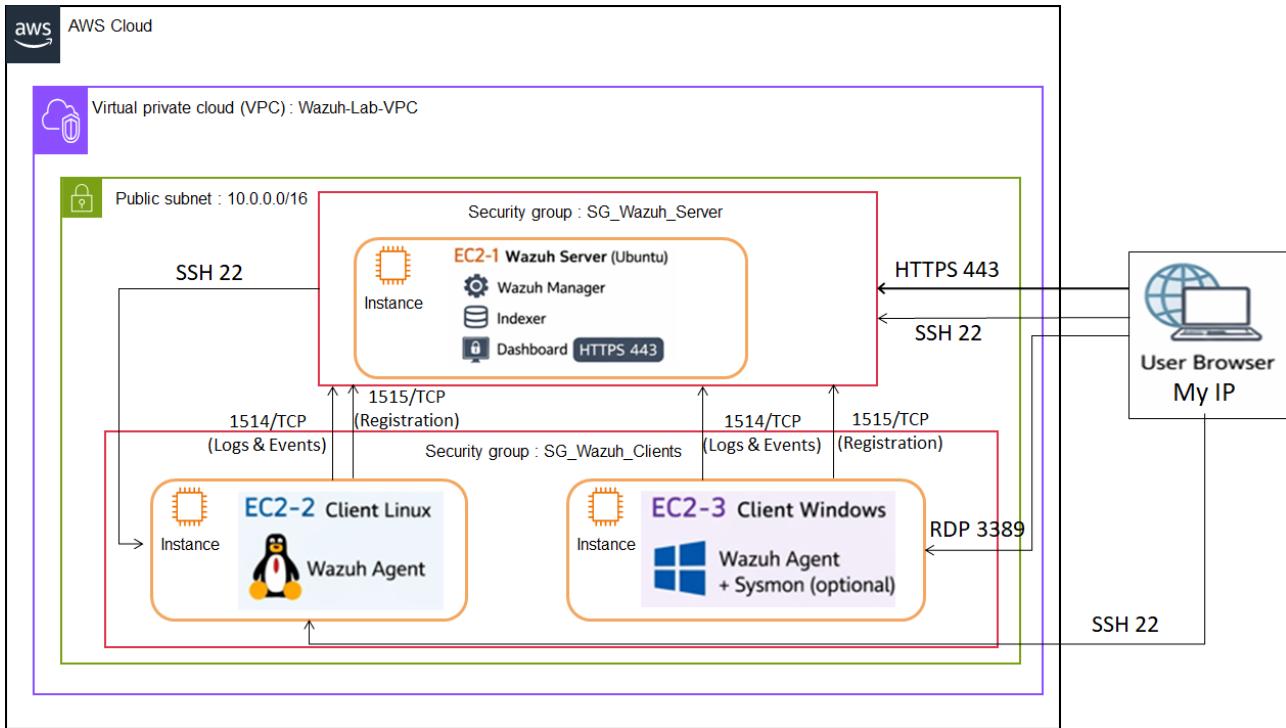
2. Architecture du Lab Wazuh sur AWS

2.1 Vue générale de l'architecture

L'architecture mise en place dans ce lab repose sur une plateforme centralisée de supervision de la sécurité, déployée sur AWS. Elle est composée de trois instances EC2 hébergées dans le même VPC, chacune ayant un rôle bien défini.

Le principe est le suivant :

les endpoints (Linux et Windows) génèrent des événements de sécurité qui sont collectés par les agents Wazuh, puis envoyés vers un serveur central Wazuh. Ce dernier assure la collecte, l'analyse, la corrélation des événements et leur visualisation via une interface web de type SIEM.



Un schéma de l'architecture globale du lab est présenté afin d'illustrer les interactions entre les différents composants.

2.2 Composants de l'architecture

L'architecture du lab est composée des éléments suivants :

Instance EC2	Système	Rôle principal	Description
EC2-1	Ubuntu	Wazuh All-in-One	Serveur central regroupant Wazuh Manager, Indexer et Dashboard
EC2-2	Ubuntu	Client Linux	Endpoint Linux supervisé par l'agent Wazuh
EC2-3	Windows Server / Windows 10-11	Client Windows	Endpoint Windows supervisé par l'agent Wazuh, avec option Sysmon pour enrichir les logs EDR

2.3 Rôle du serveur Wazuh (All-in-One)

Le serveur Wazuh constitue le cœur de la plateforme de supervision. Il regroupe plusieurs composants essentiels :

- **Wazuh Manager :**
Responsable de la réception des événements envoyés par les agents, de leur analyse et de la génération des alertes de sécurité.
- **Wazuh Indexer :**
Permet le stockage et l'indexation des événements pour faciliter la recherche, la corrélation et l'analyse.
- **Wazuh Dashboard :**
Interface web permettant de visualiser les alertes, les événements de sécurité et l'état des agents via des tableaux de bord SIEM.

2.4 Rôle des endpoints supervisés

Les endpoints représentent les systèmes à surveiller dans l'environnement :

- **Client Linux (Ubuntu) :**
Génère des événements liés à l'authentification, à l'élévation de privilèges, aux accès aux fichiers et aux activités système.
- **Client Windows :**
Génère des événements de sécurité Windows (logons, créations de comptes, modifications de privilèges).
L'installation optionnelle de **Sysmon** permet d'enrichir la détection EDR avec des événements avancés (processus, connexions réseau, etc.).

Ces événements sont collectés localement par les agents Wazuh puis transmis au serveur central.

2.5 Flux réseau et communications

Les communications entre les composants du lab reposent sur des flux réseau bien définis :

Source	Destination	Port	Description
Agents Linux / Windows	Wazuh Server	1514/TCP	Transmission des événements de sécurité
Agents Linux / Windows	Wazuh Server	1515/TCP	Enrôlement automatique des agents

Navigateur utilisateur	Wazuh Dashboard	443/TCP	Accès à l'interface web SIEM
------------------------	-----------------	---------	------------------------------

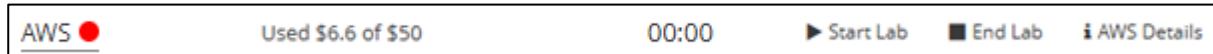
Ces flux sont contrôlés par des **Security Groups AWS**, garantissant que seules les communications nécessaires sont autorisées.

3. Description de l'activité

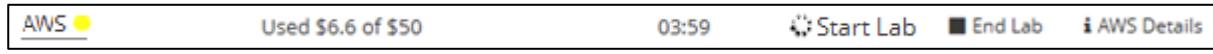
Etape 1 : Connexion à la console AWS

Dans cette étape, la connexion à la plateforme AWS Learner Lab a été effectuée. Le lab a été démarré en cliquant sur *Start Lab*, puis l'accès à la console AWS a été réalisé après validation de l'état actif de la session. Une fois la connexion établie, l'interface principale de la console AWS a été affichée.

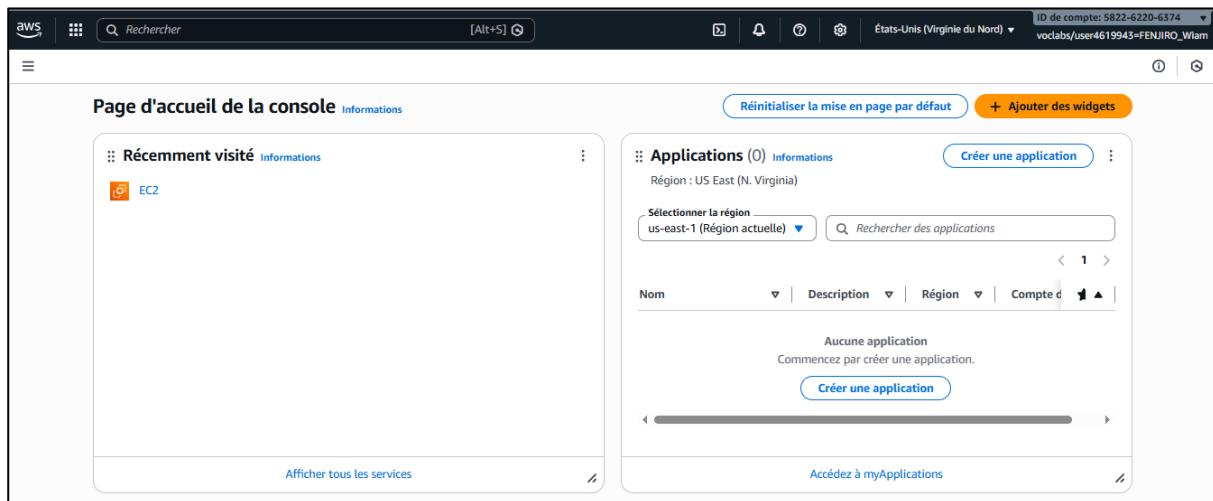
Démarrer le lab en cliquant sur **Start Lab**.



Attendre que l'icône à côté du lien AWS devienne **verte**, ce qui indique que la session est prête.



Cliquer sur le lien **AWS** en haut à gauche pour ouvrir la console dans un nouvel onglet.

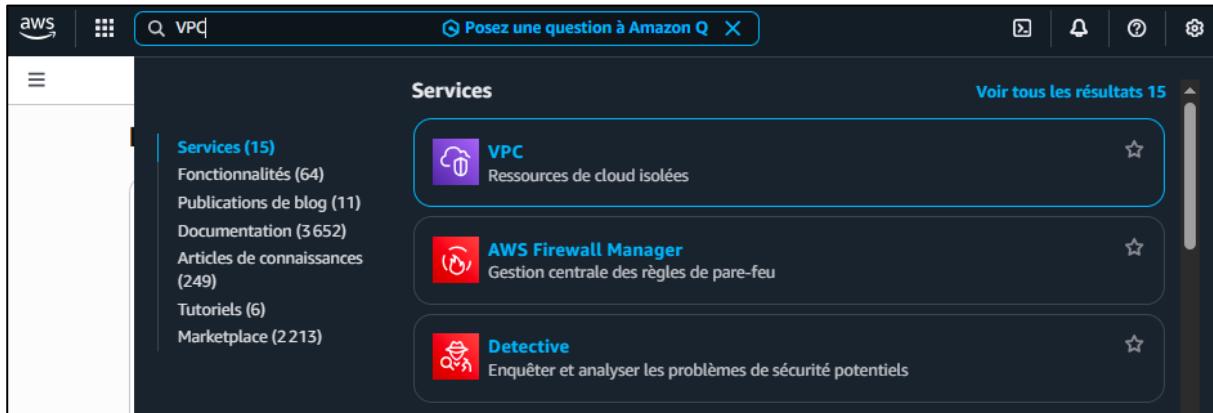


Etape 2 : Crédation de l'infrastructure du réseau

2.1 : création du VPC

J'ai créé le VPC en suivant ces étapes :

Chercher dans la barre de recherche des services : VPC

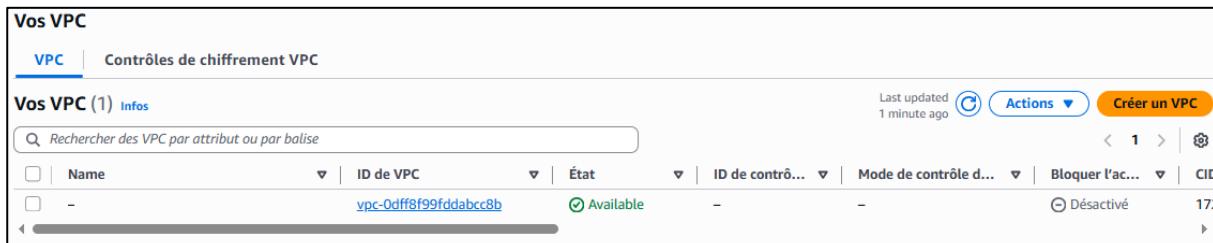


The screenshot shows the AWS CloudSearch interface with a search bar containing 'VPC'. Below the search bar, there is a navigation bar with icons for Home, Search, Notifications, and Settings. The main content area is titled 'Services' and shows a list of results. The first result is 'VPC' with a purple icon, followed by 'AWS Firewall Manager' with a red icon, and 'Detective' with an orange icon. Each result has a star icon to its right. A link 'Voir tous les résultats 15' is at the top right of the list.

Choisir VPC, puis à gauche cliquer sur 'Vos VPC'



The sidebar menu is titled 'Cloud privé virtuel' and contains three items: 'Vos VPC' (highlighted in blue), 'Sous-réseaux', and 'Tables de routage'.



The 'Vos VPC' page lists one item: 'Vos VPC (1)'. The table header includes columns for 'Name', 'ID de VPC', 'État', 'ID de contrô...', 'Mode de contrôle d...', 'Bloquer l'ac...', and 'CIE'. The single row shows 'vpc-0dff8f99fddabcc8b' in the ID column, 'Available' in the State column, and 'Désactivé' in the Block column. A 'Actions' button and a 'Créer un VPC' button are at the top right.



A large orange button labeled 'Créer un VPC' is shown, with a smaller 'Actions' button and a 'Last updated 1 minute ago' message above it.

Créer un VPC



The breadcrumb navigation shows the path: 'VPC > Vos VPC > Créer un VPC'.

Choisir : VPC et plus encore

Nom du VPC :VPC-Wazuh-Lab

Bloc d'adresses CIDR IPv4: 10.0.0.0/16

Créer un VPC Infos

Un VPC est une partie isolée du Cloud AWS remplie d'objets AWS, tels que des instances, des groupes de sécurité et des routes.

Paramètres VPC

Ressources à créer Infos

Créez uniquement la ressource VPC ou le VPC et d'autres ressources réseaux.

VPC uniquement

VPC et plus encore

Génération automatique d'identifications de noms Infos

Saisissez une valeur pour l'identification Nom. Cette valeur est utilisée pour générer automatiquement des identifications Noms pour toutes les ressources du VPC.

Génération automatique

VPC-Wazuh-Lab

Bloc d'adresses CIDR IPv4 Infos

Déterminez l'adresse IP de départ et la taille de votre VPC à l'aide de la notation CIDR.

10.0.0.0/16

65 536 IPs

La taille du bloc d'adresse CIDR doit être comprise entre /16 et /28.

Choisir le nombre de zones de disponibilité AZ: 1, nombre de sous réseaux publics : 1 et nombre de sous réseaux privés : 1

► Paramètres de chiffrement - *facultatif*

Nombre de zones de disponibilité (AZ) [Infos](#)

Choisissez le nombre de zones de disponibilité dans lesquelles mettre en service des sous-réseaux. Nous vous recommandons d'utiliser au moins deux zones de disponibilité pour avoir une haute disponibilité.

1 | 2 | 3

► Personnalisez les zones de disponibilité

Nombre de sous-réseaux publics [Infos](#)

Nombre de sous-réseaux publics à ajouter à votre VPC. Utilisez des sous-réseaux publics pour les applications web qui doivent être publiquement accessibles via Internet.

0 | **1**

Nombre de sous-réseaux privés [Infos](#)

Nombre de sous-réseaux privés à ajouter à votre VPC. Utilisez des sous-réseaux privés pour sécuriser les ressources backend qui n'ont pas besoin d'un accès public.

0 | **1** | 2

► Personnaliser les blocs d'adresse CIDR des sous-réseaux

Personnaliser les blocs d'adresse CIDR des sous-réseaux, et choisir pour celui de sous-réseaux public : 10.0.0.0/24 et pour celui de sous-réseaux privé : 10.0.1.0/24

▼ Personnaliser les blocs d'adresse CIDR des sous-réseaux

Bloc d'adresse CIDR de sous-réseau public dans us-east-1a

10.0.0.0/24 256 IPs

Bloc d'adresse CIDR de sous-réseau privé dans us-east-1a

10.0.1.0/24 256 IPs

Pour les passerelles : NAT, Zonal, dans une zone de disponibilité, et pour points de terminaison de VPC choisir aucune

Passerelles NAT (\$) - mises à jour [Infos](#)

La passerelle NAT permet aux ressources privées d'accéder à internet depuis n'importe quelle zone de disponibilité d'un VPC, fournissant ainsi un point de sortie internet géré unique pour l'ensemble de la région. Des frais supplémentaires s'appliquent.

[Aucune](#) | [Régional - nouveau](#) | **Zonal**

Présentation de la passerelle NAT régionale X

AWS propose désormais une passerelle NAT multi-AZ, éliminant ainsi le besoin de passerelles NAT distinctes entre les zones de disponibilité.

Passerelles NAT (\$) [Infos](#)

Choisissez le nombre de zones de disponibilité (AZ) dans lesquelles créer des passerelles NAT. Notez que chaque passerelle NAT est facturée.

Dans une zone de disponibilité

Une par zone de disponibilité

Points de terminaison d'un VPC [Infos](#)

Les points de terminaison peuvent aider à réduire les frais des passerelles NAT et à améliorer la sécurité en accédant directement à S3 depuis le VPC. Par défaut, une stratégie d'accès complet est utilisée. Vous pouvez personnaliser cette stratégie à tout moment.

[Aucune](#) | [Passerelle S3](#)

Activer les deux options DNS :

Options DNS [Infos](#)

- Activer les noms d'hôte DNS
- Activer la résolution DNS

▶ Identifications supplémentaires

[Annuler](#)

 [Prévisualiser le code](#)

Créer un VPC

Voici un aperçu du VPC à créer :



Cliquer sur Créer un VPC



Ressources et services VPC associés

Découvrez des ressources supplémentaires que vous pouvez lancer dans votre VPC pour créer votre architecture réseau. Des composants de sécurité aux services de connectivité, découvrez les éléments constitutifs disponibles pour votre infrastructure.



VPN client
Réseauage

AWS Client VPN est un service VPN géré basé sur le client qui vous permet d'accéder en toute sécurité aux ressources AWS et aux ressources de votre réseau sur site.

[Créer](#)

[Afficher le VPC](#)

Afficher le VPC :

[Afficher le VPC](#)

vpc-04691c8f428adbb05 / VPC-Wazuh-Lab-vpc

[Actions](#)

[Détails](#)

[Infos](#)

ID de VPC
[vpc-04691c8f428adbb05](#)

État

Bloquer l'accès public

Noms d'hôte DNS
Activé

Résolution DNS

Activé

Location

default

Jeu d'options DHCP

[dopt-0479c5e108d8420bb](#)

Table de routage principale

[rtb-04d432aca5c350740](#)

ACL réseau principal

[acl-0f42f6bcd293d072](#)

VPC par défaut

Non

CIDR IPv4

10.0.0.0/16

Groupe IPv6

–

CIDR IPv6 (groupe de bordure réseau)

–

Métriques d'utilisation d'adresses réseau

Désactivé

Groupes de règles du pare-feu DNS de

Route 53 Resolver

Échec du chargement des groupes de règles

ID de contrôle de chiffrement

–

Mode de contrôle de chiffrement

–

[Mappage des ressources](#)

[CIDR](#)

[Journaux de flux](#)

[Balises](#)

[Intégrations](#)

Vos VPC (2) [Infos](#)

Last updated
less than a minute ago



[Actions](#)

[Créer un VPC](#)

Rechercher des VPC par attribut ou par balise

<input type="checkbox"/> Name	ID de VPC	État	ID de contrô...	Mode de contrôle d...	Bloquer l'ac...
<input type="checkbox"/> –	vpc-0dff8f99fdabcc8b		–	–	
<input type="checkbox"/> VPC-Wazuh-Lab-vpc	vpc-04691c8f428adbb05		–	–	

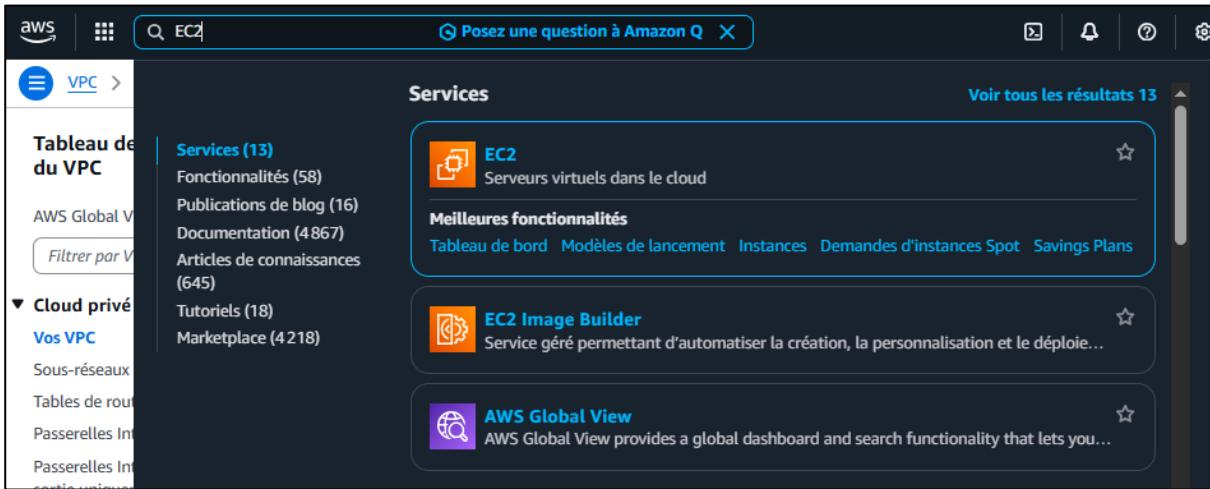
[Sélectionner un VPC ci-dessus](#)

Le nouveau VPC : VPC-Wazuh-Lab est créé avec succès

2.2 : Création des groupes de sécurités

Maintenant, je vais créer les groupes de sécurités pour le projet

Chercher dans la barre de recherche des services : EC2



The screenshot shows the AWS Management Console with the search bar set to 'EC2'. On the left sidebar, under 'VPC', there are sections for 'Tableau de bord du VPC' and 'Cloud privé'. Under 'Cloud privé', there is a 'Vos VPC' section with links for 'Sous-réseaux', 'Tables de route', 'Passerelles Internet', and 'Passerelles Intégrées'. The main content area is titled 'Services' and shows three results: 'EC2' (Serveurs virtuels dans le cloud), 'EC2 Image Builder' (Service géré permettant d'automatiser la création, la personnalisation et le déploiement d'images d'instance), and 'AWS Global View' (AWS Global View provides a global dashboard and search functionality that lets you...). A sidebar on the right lists 'Voir tous les résultats 13'.

Choisir EC2, puis à gauche cliquer sur ‘Groupes de sécurité’ dans Réseau et sécurité



The screenshot shows the 'Réseau et sécurité' section. Under 'Groupes de sécurité', there are links for 'Adresses IP élastiques', 'Groupes de placement', 'Paires de clés', and 'Interfaces réseau'.

Cliquer sur : Créer un groupe de sécurité



The screenshot shows a large orange button labeled 'Créer un groupe de sécurité'.

[☰ EC2 > Groupes de sécurité > Créer un groupe de sécurité](#)

2.2.1 Groupe de sécurité pour les clients de Wazuh (Linux + Windows)

Chaque endpoint utilise uniquement le protocole nécessaire à son administration : SSH pour le client Linux et RDP pour le client Windows. Bien qu'un groupe de sécurité unique soit appliqué aux deux instances, chaque système n'exploite que les règles qui lui sont pertinentes.

J'ai créé le nouveau groupe de sécurité avec les paramètres suivants :

- **Nom** : SG-Wazuh-Clients
- **Description** : SG clients Wazuh
- **VPC** : VPC-Wazuh-Lab

Créer un groupe de sécurité Informations

Un groupe de sécurité agit comme un pare-feu virtuel pour votre instance afin de contrôler le trafic

Détails de base

Nom du groupe de sécurité Informations

SG-Wazuh-Clients

Le nom ne peut pas être modifié après sa création.

Description Informations

SG clients Wazuh

VPC Informations

vpc-04691c8f428adbb05 (VPC-Wazuh-Lab-vpc)

Pour les règles de sécurités j'ai choisi 2 règles : SSH pour le client Linux et RDP pour le client Windows

Type	Port	Source
SSH	22	My IP
RDP	3389	My IP

Règles entrantes Informations

Type	Protocole	Plage de ports	Source	Description - facultatif
SSH	TCP	22	Mon IP	41.249.102.95/32
RDP	TCP	3389	Mon IP	41.249.102.95/32

[Ajouter une règle](#)

Créer le groupe de sécurité

Annuler

Créer un groupe de sécurité

Le groupe de sécurité SG-Wazuh-Clients est créé avec succès

⌚ Le groupe de sécurité ([sg-0e5f826079665b5a3](#) | SG-Wazuh-Clients) a été créé avec succès. X

▶ Détails

sg-0e5f826079665b5a3 - SG-Wazuh-Clients

[Actions ▾](#)

Détails			
Nom du groupe de sécurité <input checked="" type="checkbox"/> SG-Wazuh-Clients	ID du groupe de sécurité <input checked="" type="checkbox"/> sg-0e5f826079665b5a3	Description <input checked="" type="checkbox"/> SG clients Wazuh	ID de VPC <input checked="" type="checkbox"/> vpc-04691c8f428adbb05 ↗
Propriétaire <input checked="" type="checkbox"/> 582262206374	Nombre de règles entrantes 2 Entrées d'autorisation	Nombre de règles sortantes 1 Entrée d'autorisation	

[Règles entrantes](#) | [Règles sortantes](#) | [Partage](#) | [Associations VPC](#) | [Balises](#)

Règles entrantes (2)						
<input checked="" type="checkbox"/> Recherche					Gérer les balises	Modifier les règles entrantes
<input type="checkbox"/>	Name	ID de règle de grou...	Version IP	Type	Protocole	Plage de ports
<input type="checkbox"/>	-	sgr-093c82c1eeaaf4223	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-0ed93b8dcfe4d4ce0	IPv4	RDP	TCP	3389

2.2.2 Groupe de sécurité pour le serveur de Wazuh

Ce groupe de sécurité permet de contrôler les accès au serveur central Wazuh.

Il autorise uniquement les flux nécessaires à l'administration du serveur et à la communication avec les agents.

J'ai créé un nouveau groupe de sécurité avec les paramètres suivants :

- **Nom** : SG-Wazuh-Server
- **Description** : Groupe de sécurité du serveur Wazuh
- **VPC** : VPC-Wazuh-Lab

Créer un groupe de sécurité [Informations](#)

Un groupe de sécurité agit comme un pare-feu virtuel pour votre instance afin de contrôler le trafic

Détails de base

Nom du groupe de sécurité [Informations](#)

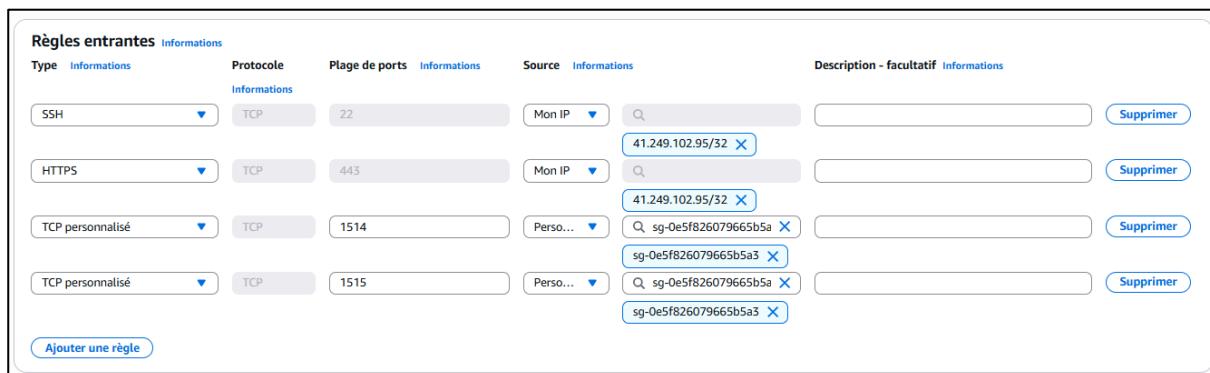
Le nom ne peut pas être modifié après sa création.

Description [Informations](#)

VPC [Informations](#)

Pour les règles de sécurité j'ai choisi les règles suivantes :

Type	Port	Source	Description
SSH	22	My IP	Accès administrateur au serveur
HTTPS	443	My IP	Accès au dashboard Wazuh
TCP personnalisé	1514	SG-Wazuh-Clients	Réception des événements des agents
TCP personnalisé	1515	SG-Wazuh-Clients	Enrôlement des agents



Créer le groupe de sécurité

Annuler Créer un groupe de sécurité

Le groupe de sécurité SG-Wazuh-Server est créé avec succès

✓ **Le groupe de sécurité (sg-0c4a1c596225b2689 | SG-Wazuh-Server) a été créé avec succès.** X

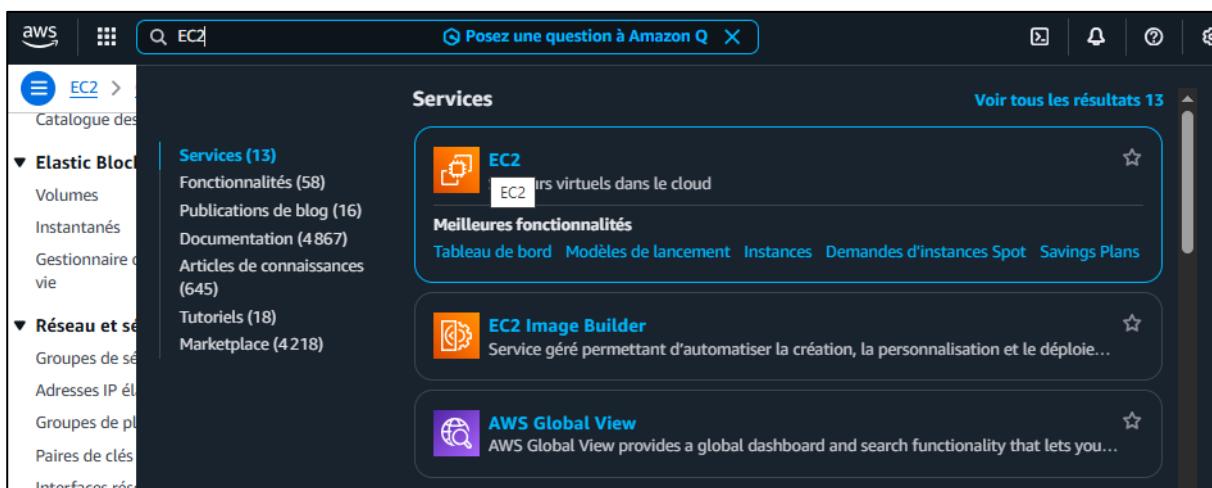
[EC2](#) > [Groupes de sécurité](#) > sg-0c4a1c596225b2689 - SG-Wazuh-Server

sg-0c4a1c596225b2689 - SG-Wazuh-Server				Actions
Détails				
Nom du groupe de sécurité sg-Wazuh-Server	ID du groupe de sécurité sg-0c4a1c596225b2689	Description SG serveur Wazuh	ID de VPC ypc-04691c8f428adbb05_1	
Propriétaire 582262206374	Nombre de règles entrantes 4 Entrées d'autorisation	Nombre de règles sortantes 1 Entrée d'autorisation		

Règles entrantes (4)						
	Name	ID de règle de groupe	Version IP	Type	Protocole	Plage de ports
<input type="checkbox"/>	-	sgr-02f5416e21110541b	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-0ed576ae89601cb0b	-	TCP personnalisé	TCP	1515
<input type="checkbox"/>	-	sgr-0b82b6ebc1ba2f64c	-	TCP personnalisé	TCP	1514
<input type="checkbox"/>	-	sgr-0854b21e3aeb9e3f4	IPv4	HTTPS	TCP	443

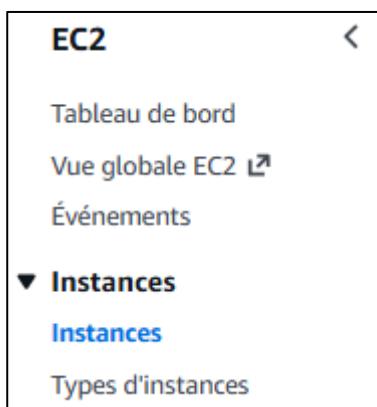
Etape 3 : Déploiement des instances EC2

Cette étape consiste à créer les différentes instances EC2 nécessaires au fonctionnement du lab : un serveur Wazuh et deux clients (Linux et Windows).



The screenshot shows the AWS CloudSearch interface. In the search bar at the top, 'EC2' is typed. Below the search bar, there's a sidebar with navigation links like 'Catalogue des services', 'Elastic Block Store', 'Réseau et sécurité', and 'Instances'. The main area displays search results under the heading 'Services'. The first result is 'EC2' with a sub-description 'Ils virtuels dans le cloud'. Below it are 'Meilleures fonctionnalités' and links to 'Tableau de bord', 'Modèles de lancement', 'Instances', 'Demandes d'instances Spot', and 'Savings Plans'. The second result is 'EC2 Image Builder' with a sub-description 'Service géré permettant d'automatiser la création, la personnalisation et le déploie...'. The third result is 'AWS Global View' with a sub-description 'AWS Global View provides a global dashboard and search functionality that lets you...'. There are also 'Voir tous les résultats 13' and a vertical scroll bar.

Choisir à gauche 'Instances'



The screenshot shows the AWS EC2 Instances menu. On the left, there's a sidebar with 'EC2' at the top, followed by 'Tableau de bord', 'Vue globale EC2', 'Événements', and 'Instances'. Under 'Instances', there are two sub-links: 'Instances' and 'Types d'instances'. The 'Instances' link is highlighted in blue.

Cliquer sur Lancer des instances

Lancer des instances ▼

3.1 : Serveur Wazuh (Ubuntu)

Le serveur Wazuh est l'élément central de l'architecture. Il héberge les composants SIEM et EDR.

Paramètres principaux :

- **Nom** : Wazuh_Server

Lancer une instance Informations

Amazon EC2 vous permet de créer des machines virtuelles, ou des instances, qui s'exécutent sur le Cloud AWS. Démarrer rapidement en suivant les étapes simples indiquées ci-dessous.

Nom et balises Informations

Nom

Wazuh_Server Ajouter des balises supplémentaires

- **AMI** : Ubuntu Server 22.04 LTS

Ubuntu Server 22.04 LTS(2+ filtré(s), 2 non filtré(s))

ubuntu Ubuntu Éligible à l'offre gratuite Fournisseur vérifié

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-0c398cb65a93047f2 (64 bits (x86)) / ami-0f14ad9f1d341c53d (64 bits (Arm))
Ubuntu Server 22.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).
Plateforme: ubuntu Type de périphérique racine: ebs Virtualisation: hvm ENA activé: Oui

Sélectionnez

64 bits (x86)
 64 bits (Arm)

▼ Images d'applications et de systèmes d'exploitation (Amazon Machine Image) [Informations](#)

Une AMI contient le système d'exploitation, le serveur d'applications et les applications de votre instance. Si aucune AMI appropriée ne s'affiche ci-dessous, utilisez le champ de recherche ou choisissez **Parcourir d'autres AMI**.

Effectuer une recherche dans notre catalogue complet, qui comprend des milliers d'images d'applications et de systèmes d'exploitation

AMI du catalogue

Récentes

Démarrage rapide

Nom

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Fournisseur vérifié

Éligible à l'offre gratuite



Explorer plus d'AMI

Y compris les AMI
d'AWS, de Marketplace
et de la communauté

Description

Ubuntu Server 22.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 22.04, amd64 jammy image

ID de l'image

ami-0c398cb65a93047f2

Nom d'utilisateur

ubuntu

Catalogue

AMI de démarrage
rapide

Publié

2025-10-
15T08:05:51.000Z

Architecture

x86_64

Virtualisation

hvm

Type de périphérique racine

ebs

ENA activé

Oui

- **Type d'instance : t3.large**

▼ Type d'instance [Informations](#) | [Obtenez des conseils](#)

Type d'instance

t3.large

Famille: t3 2 vCPU 8 Gio Mémoire Génération actuelle: true
 À la demande Linux base tarification: 0.0832 USD par heure
 À la demande Windows base tarification: 0.1108 USD par heure
 À la demande RHEL base tarification: 0.112 USD par heure
 À la demande SUSE base tarification: 0.1395 USD par heure
 À la demande Ubuntu Pro base tarification: 0.0867 USD par heure

Toutes les générations

[Comparer les types d'instance](#)

[Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé](#)

Créer une paire de clés : KEY_Wazuh_Server

Créer une paire de clés

Nom de la paire de clés
Les paires de clés vous permettent de vous connecter à votre instance en toute sécurité.

La longueur maximale du nom est de 255 caractères ASCII. Il ne peut pas inclure d'espaces avant ou après.

Type de paire de clés

RSA
Paire de clés privée et publique chiffrée RSA

ED25519
Paire de clés privée et publique chiffrée ED25519

Format de fichier de clé privée

.pem
À utiliser avec OpenSSH

.ppk
À utiliser avec PuTTY

⚠️ Lorsque vous y êtes invité, stockez la paire de clés dans un emplacement sécurisé et accessible sur votre ordinateur. Vous en aurez besoin ultérieurement pour vous connecter à votre instance. [En savoir plus ↗](#)

[Annulez](#) [Créer une paire de clés](#)



- **VPC : VPC-Wazuh-Lab**

▼ Paramètres réseau | Informations

VPC - obligatoire | Informations

vpc-04691c8f428adbb05 (VPC-Wazuh-Lab-vpc)
10.0.0.0/16

Sous-réseau | Informations

subnet-05b94a7165bd574a7 VPC-Wazuh-Lab-subnet-public1-us-east-1a
VPC: vpc-04691c8f428adbb05 Propriétaire: 582262206374
Zone de disponibilité: us-east-1a (use1-az2) Type de zone: Zone de disponibilité
Adresses IP disponibles: 250 CIDR: 10.0.0.0/24

Attribuer automatiquement l'adresse IP publique | Informations

Activer

- **Groupe de sécurité : SG-Wazuh-Server**

Pare-feu (groupes de sécurité) | Informations

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

Créer un groupe de sécurité Sélectionner un groupe de sécurité existant

Groupes de sécurité courants | Informations

Sélectionner les groupes de sécurité

SG-Wazuh-Server sg-0c4a1c596225b2689 X

Comparer les règles de groupe de sécurité

Les groupes de sécurité que vous ajoutez ou supprimez ici seront ajoutés ou supprimés de toutes vos interfaces réseau.

▶ Configuration réseau avancée

- **Stockage : 30 Go**

▼ Configurer le stockage | Informations

1x Gio Volume racine, Non chiffré

Lancer l'instance

Lancer l'instance

L'instance Wazuh server est lancée avec succès

 Succès

Lancement de l'instance réussi ([i-0603e89748ff9ff47](#))

Wazuh_Server i-0603e89748ff9ff47  En cours d'...   t3.large  3/3 vérifications r [Afficher les alarm](#) us-east-1a

3.2 : Wazuh Linux Client

Cette instance représente un endpoint Linux à surveiller.

 [EC2](#) > [Instances](#) > [Lancer une instance](#)

Paramètres principaux :

- **Nom** : Wazuh_Linux2_Client

Lancer une instance Informations

Amazon EC2 vous permet de créer des machines virtuelles, ou des instances, qui s'exécutent sur le Cloud AWS. Démarrez rapidement en suivant les étapes simples indiquées ci-dessous.

Nom et balises Informations

Nom

[Ajouter des balises supplémentaires](#)

- **AMI** : Ubuntu Server 22.04

▼ Images d'applications et de systèmes d'exploitation (Amazon Machine Image) [Informations](#)

Une AMI contient le système d'exploitation, le serveur d'applications et les applications de votre instance. Si aucune AMI appropriée ne s'affiche ci-dessous, utilisez le champ de recherche ou choisissez **Parcourir d'autres AMI**.

Effectuer une recherche dans notre catalogue complet, qui comprend des milliers d'images d'applications et de systèmes d'exploitation

[AMI du catalogue](#) | [Récentes](#) | [Démarrage rapide](#)

Nom

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Fournisseur vérifié

Éligible à l'offre gratuite



[Explorer plus d'AMI](#)

Y compris les AMI d'AWS, de Marketplace et de la communauté

Description

Ubuntu Server 22.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 22.04, amd64 jammy image

ID de l'image

ami-0c398cb65a93047f2

Nom d'utilisateur

ubuntu

Catalogue

AMI de démarrage rapide

Publié

2025-10-15T08:05:51.000Z

Architecture

x86_64

Virtualisation

hvm

Type de périphérique racine

ebs

ENA activé

Oui

- **Type d'instance : t3.micro**

▼ Type d'instance [Informations](#) | [Obtenez des conseils](#)

Type d'instance

t3.micro

Éligible à l'offre gratuite

Famille: t3 2 vCPU 1 Gio Mémoire Génération actuelle: true
 À la demande Ubuntu Pro base tarification: 0.0139 USD par heure
 À la demande SUSE base tarification: 0.0104 USD par heure
 À la demande Linux base tarification: 0.0104 USD par heure
 À la demande RHEL base tarification: 0.0392 USD par heure
 À la demande Windows base tarification: 0.0196 USD par heure

Toutes les générations

[Comparer les types d'instance](#)

Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé

Créer une paire de clés : KEY_Wazuh_Linux2_Client

Créer une paire de clés



Nom de la paire de clés

Les paires de clés vous permettent de vous connecter à votre instance en toute sécurité.

KEY_Wazuh_Linux2_Client

La longueur maximale du nom est de 255 caractères ASCII. Il ne peut pas inclure d'espaces avant ou après.

Type de paire de clés



RSA

Paire de clés privée et publique chiffrée RSA



ED25519

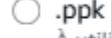
Paire de clés privée et publique chiffrée ED25519

Format de fichier de clé privée



.pem

À utiliser avec OpenSSH



.ppk

À utiliser avec PuTTY



Lorsque vous y êtes invité, stockez la paire de clés dans un emplacement sécurisé et accessible sur votre ordinateur. Vous en aurez besoin ultérieurement pour vous connecter à votre instance. [En savoir plus ↗](#)

Annulez

Créer une paire de clés



KEY_Wazuh_Linu
x2_Client.pem

▼ Paire de clés (connexion) Informations

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - *obligatoire*

KEY_Wazuh_Linux2_Client

 [Créer une paire de clés](#)

- **VPC : VPC-Wazuh-Lab**

▼ Paramètres réseau [Informations](#)

VPC - obligatoire | [Informations](#)

vpc-04691c8f428adbb05 (VPC-Wazuh-Lab-vpc)
10.0.0.0/16

Sous-réseau | [Informations](#)

subnet-05b94a7165bd574a7 VPC-Wazuh-Lab-subnet-public1-us-east-1a
VPC: vpc-04691c8f428adbb05 Propriétaire: 582262206374
Zone de disponibilité: us-east-1a (use1-az2) Type de zone: Zone de disponibilité
Adresses IP disponibles: 249 CIDR: 10.0.0.0/24

Attribuer automatiquement l'adresse IP publique | [Informations](#)

Activer

- **Groupe de sécurité : SG-Wazuh-Clients**

Pare-feu (groupes de sécurité) | [Informations](#)

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

Créez un groupe de sécurité Sélectionnez un groupe de sécurité existant

Groupes de sécurité courants | [Informations](#)

Sélectionnez les groupes de sécurité

SG-Wazuh-Clients sg-0e5f826079665b5a3 X
VPC: vpc-04691c8f428adbb05

Comparer les règles de groupe de sécurité

Les groupes de sécurité que vous ajoutez ou supprimez ici seront ajoutés ou supprimés de toutes vos interfaces réseau.

► Configuration réseau avancée

- **Stockage : 8 Go**

▼ Configurer le stockage [Informations](#) [Avancé](#)

1x Gio gp2 Volume racine, Non chiffré

[Ajouter un volume](#)

L'AMI sélectionnée contient des volumes de stockage d'instance, mais l'instance n'autorise aucun volume de stockage d'instance. Aucun des volumes de stockage d'instance provenant de l'AMI ne sera accessible depuis l'instance

ⓘ Cliquez sur Actualiser pour afficher les informations de sauvegarde
Les balises que vous attribuez déterminent si l'instance sera sauvegardée conformément aux stratégies de Data Lifecycle Manager.

0 systèmes de fichiers [Modifier](#)

Récapitulatif :

▼ Récapitulatif

Nombre d'instances | Informations

1

Image logicielle (AMI)
Ubuntu Server 22.04 LTS (HVM),...[en savoir plus](#)
ami-0c398cb65a93047f2

Type de serveur virtuel (type d'instance)
t3.micro

Pare-feu (groupe de sécurité)
SG-Wazuh-Clients

Stockage (volumes)
1 volume(s) - 8 Gio

[Annulez](#) [Lancer l'instance](#)

[Code de prévisualisation](#)

Lancer l'instance

L'instance Client Linux est lancée avec succès

Succès
Lancement de l'instance réussi ([i-0f34083a528bedd49](#))

<input type="checkbox"/> Wazuh_Linux2_Client	i-0f34083a528bedd49	<input checked="" type="checkbox"/> En cours d'... t3.micro	<input checked="" type="checkbox"/> 3/3 vérifications r	Afficher les détails
--	---------------------	--	---	--------------------------------------

3.3 : Wazuh Windows Client

Cette instance représente un endpoint Windows supervisé par Wazuh.

Paramètres principaux :

- **Nom** : Wazuh_Windows2_Client

Lancer une instance Informations

Amazon EC2 vous permet de créer des machines virtuelles, ou des instances, qui s'exécutent sur le Cloud AWS. Démarrez rapidement en suivant les étapes simples indiquées ci-dessous.

Nom et balises Informations

Nom

[Ajouter des balises supplémentaires](#)

Microsoft Windows Server 2022 Base(1+ filtré(s), 1 non filtré(s))



Microsoft Windows Server 2022 Base

ami-0fc8a85749a35ce56 (64 bits (x86))

Microsoft Windows 2022 Datacenter edition. [English]

Éligible à l'offre gratuite

Plateforme: windows

Type de périphérique racine: ebs

Virtualisation: hvm

ENA activé: Oui

[Sélectionnez](#)

64 bits (x86)

Fournisseur vérifié

- AMI : Windows Server 2022

▼ Images d'applications et de systèmes d'exploitation (Amazon Machine Image) Informations

Une AMI contient le système d'exploitation, le serveur d'applications et les applications de votre instance. Si aucune AMI appropriée ne s'affiche ci-dessous, utilisez le champ de recherche ou choisissez **Parcourir d'autres AMI**.

Effectuer une recherche dans notre catalogue complet, qui comprend des milliers d'images d'applications et de systèmes d'exploitation

[AMI du catalogue](#)

Récentes

Démarrage rapide

Nom

Microsoft Windows Server 2022 Base

Fournisseur vérifié

Éligible à l'offre gratuite



[Explorer plus d'AMI](#)

Y compris les AMI d'AWS, de Marketplace et de la communauté

Description

Microsoft Windows 2022 Datacenter edition. [English]

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

ID de l'image

ami-0fc8a85749a35ce56

Nom d'utilisateur

Administrator

Catalogue

AMI de démarrage rapide

Publié

2025-12-10T22:32:59.000Z

Architecture

x86_64

Virtualisation

hvm

Type de périphérique racine

ebs

ENA activé

Oui

- Type d'instance : t2.medium

Type d'instance [Informations](#) | [Obtenez des conseils](#)

Type d'instance

t2.medium

Famille: t2 2 vCPU 4 Gio Mémoire Génération actuelle: true
 À la demande Ubuntu Pro base tarification: 0.0499 USD par heure
 À la demande Linux base tarification: 0.0464 USD par heure
 À la demande RHEL base tarification: 0.0752 USD par heure
 À la demande Windows base tarification: 0.0644 USD par heure
 À la demande SUSE base tarification: 0.1464 USD par heure

Toutes les générations

[Comparer les types d'instance](#)

Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé

Créer une paire de clés : KEY_Wazuh_Windows2_Client

Créer une paire de clés

Nom de la paire de clés

Les paires de clés vous permettent de vous connecter à votre instance en toute sécurité.

KEY_Wazuh_Windows2_Client

La longueur maximale du nom est de 255 caractères ASCII. Il ne peut pas inclure d'espaces avant ou après.

Type de paire de clés

RSA
Paire de clés privée et publique chiffrée RSA

ED25519
Paire de clés privée et publique chiffrée ED25519 (non prise en charge pour les instances Windows)

Format de fichier de clé privée

.pem
À utiliser avec OpenSSH

.ppk
À utiliser avec PuTTY

⚠️ Lorsque vous y êtes invité, stockez la paire de clés dans un emplacement sécurisé et accessible sur votre ordinateur. **Vous en aurez besoin ultérieurement pour vous connecter à votre instance.** [En savoir plus ↗](#)

[Annulez](#) [Créer une paire de clés](#)



▼ Paire de clés (connexion) [Informations](#)

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - obligatoire

KEY_Wazuh_Windows2_Client

[Créer une paire de clés](#)

Pour les instances Windows, vous utilisez une paire de clés pour déchiffrer le mot de passe administrateur. Vous utilisez ensuite le mot de passe déchiffré pour vous connecter à votre instance.

- **VPC : VPC-Wazuh-Lab**

▼ Paramètres réseau [Informations](#)

VPC - obligatoire | [Informations](#)

vpc-04691c8f428adbb05 (VPC-Wazuh-Lab-vpc)
10.0.0.0/16

[Créer une nouvelle instance](#)

Sous-réseau | [Informations](#)

subnet-05b94a7165bd574a7 VPC-Wazuh-Lab-subnet-public1-us-east-1a
VPC: vpc-04691c8f428adbb05 Propriétaire: 582262206374
Zone de disponibilité: us-east-1a (use1-az2) Type de zone: Zone de disponibilité
Adresses IP disponibles: 248 CIDR: 10.0.0.0/24

[Créer un nouveau sous-réseau](#)

Attribuer automatiquement l'adresse IP publique | [Informations](#)

Activer

- **Groupe de sécurité : SG-Wazuh-Clients**

Pare-feu (groupes de sécurité) | [Informations](#)
 Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

Créez un groupe de sécurité Sélectionnez un groupe de sécurité existant

Groupes de sécurité courants | [Informations](#)

Sélectionnez les groupes de sécurité ▾

SG-Wazuh-Clients sg-0e5f826079665b5a3 X
VPC: vpc-04691c8f428adbb05

C [Comparer les règles de groupe de sécurité](#)

Les groupes de sécurité que vous ajoutez ou supprimez ici seront ajoutés ou supprimés de toutes vos interfaces réseau.

▶ **Configuration réseau avancée**

- **Stockage : 30 Go**

▼ **Configurer le stockage** [Informations](#) [Avancé](#)

1x 30 Gio gp2 ▾ Volume racine, Non chiffré

[Ajouter un volume](#)

Récapitulatif :

▼ **Récapitulatif**

Nombre d'instances | [Informations](#)

1

Image logicielle (AMI)
Microsoft Windows Server 2022 ...[en savoir plus](#)
ami-0fc8a85749a35ce56

Type de serveur virtuel (type d'instance)
t2.medium

Pare-feu (groupe de sécurité)
SG-Wazuh-Clients

Stockage (volumes)
1 volume(s) - 30 Gio

[Annulez](#) [Lancer l'instance](#)

 [Code de prévisualisation](#)

Lancer l'instance :

L'instance Client Windows est lancée avec succès

Succès
Lancement de l'instance réussi ([i-0df82d8910e4a62a5](#))

<input type="checkbox"/> Wazuh_Windows2_Client	i-0df82d8910e4a62a5	<input checked="" type="checkbox"/> En cours d'... t2.medium	<input checked="" type="checkbox"/> 2/2 vérifications r Afficher les alertes
--	---------------------	--	--

Etape 4 : Installation de Wazuh

4.1 Connexion SSH

La connexion au serveur Wazuh a été réalisée via SSH à l'aide de la clé de Wazuh Linux Client.

Se connecter [Informations](#)

Connectez-vous à une instance à l'aide du client basé sur un navigateur.

[EC2 Instance Connect](#) | [Session Manager](#) | **Client SSH** | [EC2 Serial Console](#)

ID d'instance
 i-0603e89748ff9ff47 (Wazuh_Server)

1. Ouvrez un client SSH.
2. Recherchez votre fichier de clé privée. La clé utilisée pour lancer cette instance est KEY_Wazuh_Server.pem
3. Exécuter, si nécessaire, cette commande pour vous assurer que votre clé n'est pas visible publiquement.
 chmod 400 "KEY_Wazuh_Server.pem"
4. Connectez-vous à votre instance à l'aide de son DNS public :
 ec2-100-24-23-249.compute-1.amazonaws.com

Commande copiée

ssh -i "KEY_Wazuh_Server.pem" ubuntu@ec2-100-24-23-249.compute-1.amazonaws.com

```
C:\Users\PC>ssh -i "KEY_Wazuh_Server.pem" ubuntu@ec2-100-24-23-249.compute-1.amazonaws.com
Warning: Identity file KEY_Wazuh_Server.pem not accessible: No such file or directory.
The authenticity of host 'ec2-100-24-23-249.compute-1.amazonaws.com (100.24.23.249)' can't be established.
ED25519 key fingerprint is SHA256:WV7hp2fRFx3Gsrn1AY5y8GLE9ey7mCR7z/KPITNWB2Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

4.2 Installation de Wazuh

L'installation de Wazuh a été effectuée à l'aide du script officiel, permettant une installation automatique de tous les composants.

```
ubuntu@ip-10-0-0-196:~$ sudo apt update && sudo apt -y upgrade  
/packages.wazuh.com/4.7/wazuh-install.sh  
sudo bash wazcurl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh  
sudo bash wazuh-install.sh -a
```

```
ubuntu@ip-10-0-0-196:~$ curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh  
ubuntu@ip-10-0-0-196:~$ sudo bash wazuh-install.sh -a  
04/01/2026 20:09:55 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5  
04/01/2026 20:09:55 INFO: Verbose logging redirected to /var/log/wazuh-install.log  
04/01/2026 20:10:04 INFO: Wazuh web interface port will be 443.  
04/01/2026 20:10:04 INFO: Wazuh web interface port will be 443.
```

```
ubuntu@ip-10-0-0-196:~$ sudo bash wazuh-install.sh -a  
04/01/2026 20:09:55 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5  
04/01/2026 20:09:55 INFO: Verbose logging redirected to /var/log/wazuh-install.log  
04/01/2026 20:10:04 INFO: Wazuh web interface port will be 443.  
04/01/2026 20:10:10 INFO: --- Dependencies ----  
04/01/2026 20:10:10 INFO: Installing apt-transport-https.  
04/01/2026 20:10:16 INFO: Wazuh repository added.  
04/01/2026 20:10:16 INFO: --- Configuration files ---  
04/01/2026 20:10:16 INFO: Generating configuration files.  
04/01/2026 20:10:18 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.  
04/01/2026 20:10:18 INFO: --- Wazuh indexer ---  
04/01/2026 20:10:18 INFO: Starting Wazuh indexer installation.  
04/01/2026 20:11:23 INFO: Wazuh indexer installation finished.  
04/01/2026 20:11:23 INFO: Wazuh indexer post-install configuration finished.  
04/01/2026 20:11:23 INFO: Starting service wazuh-indexer.  
^[[D^[[C04/01/2026 20:11:44 INFO: wazuh-indexer service started.  
04/01/2026 20:11:44 INFO: Initializing Wazuh indexer cluster security settings.  
^[[D^[[C04/01/2026 20:11:56 INFO: Wazuh indexer cluster initialized.  
04/01/2026 20:11:56 INFO: --- Wazuh server ---  
04/01/2026 20:11:56 INFO: Starting the Wazuh manager installation.
```

```
04/01/2026 20:14:48 INFO: --- Summary ---  
04/01/2026 20:14:48 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443  
    User: admin  
    Password: e?NRsITn3*ZyNCI2calde.Z8XEyvP3QN  
04/01/2026 20:14:48 INFO: Installation finished.  
ubuntu@ip-10-0-0-196:~$
```

Login et password récupérés.

4.3 Vérification des services

Après l'installation, les services Wazuh ont été vérifiés afin de s'assurer de leur bon fonctionnement.

```
ubuntu@ip-10-0-0-196:~$ 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 20:13:08 UTC; 1h 22min ago
     Tasks: 121 (limit: 9361)
    Memory: 382.0M
      CPU: 1min 6.357s
     CGroup: /system.slice/wazuh-manager.service
             └─58760 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
               ├─58801 /var/ossec/bin/wazuh-authd
               ├─58815 /var/ossec/bin/wazuh-db
               ├─58839 /var/ossec/bin/wazuh-execd
               ├─58843 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
               ├─58846 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
               ├─58849 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
               ├─58864 /var/ossec/bin/wazuh-analysisd
               ├─58906 /var/ossec/bin/wazuh-syscheckd
               ├─58922 /var/ossec/bin/wazuh-remoted
               ├─58955 /var/ossec/bin/wazuh-logcollector
               ├─58974 /var/ossec/bin/wazuh-monitord
               └─58996 /var/ossec/bin/wazuh-modulesd

Jan 04 20:12:59 ip-10-0-0-196 env[58704]: Started wazuh-db...
Jan 04 20:13:00 ip-10-0-0-196 env[58704]: Started wazuh-execd...
Jan 04 20:13:01 ip-10-0-0-196 env[58704]: Started wazuh-analysisd...
Jan 04 20:13:02 ip-10-0-0-196 env[58704]: Started wazuh-syscheckd...
Jan 04 20:13:03 ip-10-0-0-196 env[58704]: Started wazuh-remoted...
Jan 04 20:13:04 ip-10-0-0-196 env[58704]: Started wazuh-logcollector...
Jan 04 20:13:05 ip-10-0-0-196 env[58704]: Started wazuh-monitord...
Jan 04 20:13:06 ip-10-0-0-196 env[58704]: Started wazuh-modulesd...
Jan 04 20:13:08 ip-10-0-0-196 env[58704]: Completed.
Jan 04 20:13:08 ip-10-0-0-196 systemd[1]: Started Wazuh manager.
ubuntu@ip-10-0-0-196:~$
```

```
ubuntu@ip-10-0-0-196:~$ 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 20:11:44 UTC; 1h 25min ago
     Docs: https://documentation.wazuh.com
     Main PID: 15239 (java)
        Tasks: 75 (limit: 9361)
       Memory: 4.2G
         CPU: 2min 3.128s
        CGroup: /system.slice/wazuh-indexer.service
                  └─15239 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.
```

```
ubuntu@ip-10-0-0-196:~$ 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 20:14:32 UTC; 1h 23min ago
     Main PID: 61091 (node)
        Tasks: 11 (limit: 9361)
       Memory: 165.7M
         CPU: 17.612s
        CGroup: /system.slice/wazuh-dashboard.service
                  └─61091 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536
```

Étape 5 : Accès au Wazuh Dashboard

L'accès au dashboard Wazuh a été effectué via un navigateur web en utilisant l'adresse IP publique du serveur.

Lors du premier accès, un avertissement de sécurité du navigateur apparaît, car le certificat est auto-signé.

Il est alors nécessaire de continuer vers le site.

Copier l'adresse ipv4 publique de Wazuh Server



Résumé de l'instance pour i-0603e89748ff9ff47

Mis à jour il y a less than a minute

ID d'instance
i-0603e89748ff9ff47

Adresse IPv6
-

Informations

Adresse IPv4 publique copiée
34.201.58.28 | adresse ouverte ↗

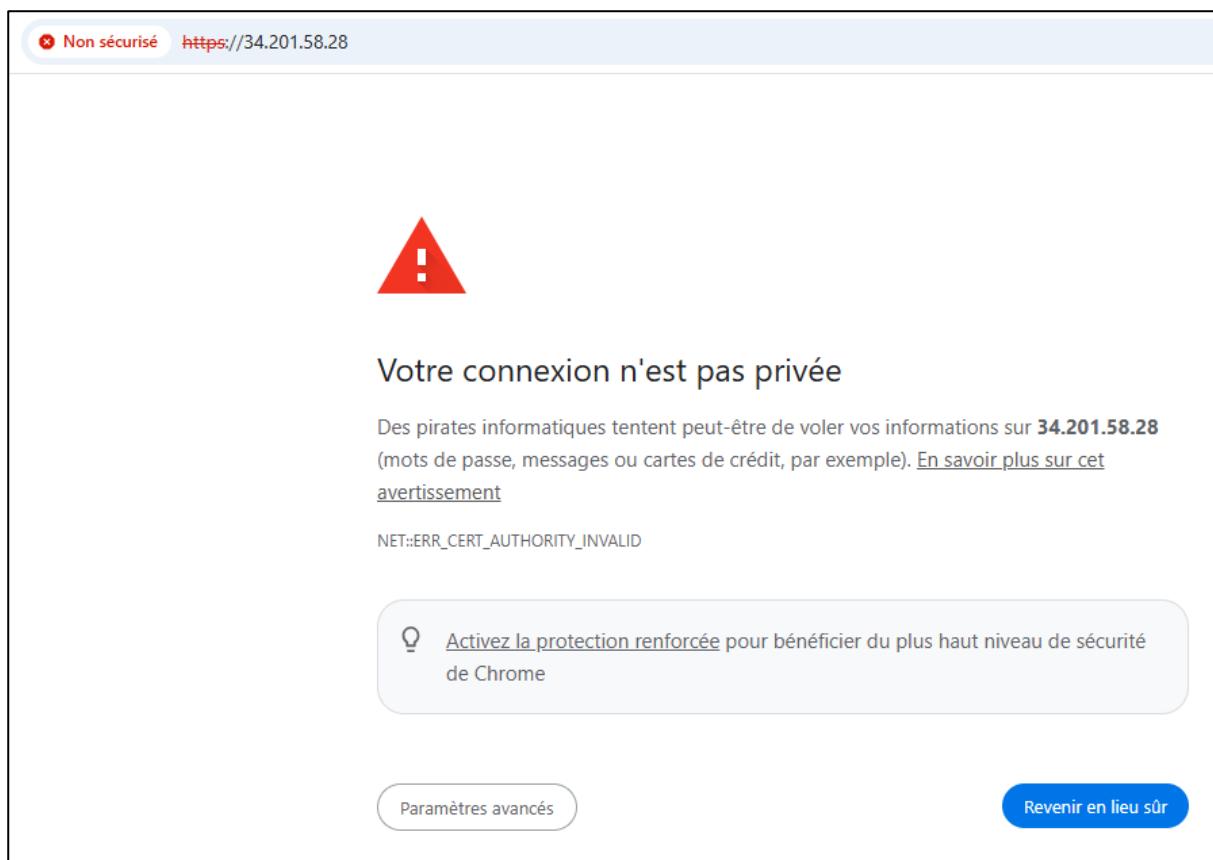
Adresse IPv4 privées
10.0.0.196

État de l'instance
En cours d'exécution

DNS public
ec2-34-201-58-28.compute-1.amazonaws.com | adresse ouverte ↗

Actions

Ouvrir dashboard Wazuh



Non sécurisé <https://34.201.58.28>

!

Votre connexion n'est pas privée

Des pirates informatiques tentent peut-être de voler vos informations sur **34.201.58.28** (mots de passe, messages ou cartes de crédit, par exemple). [En savoir plus sur cet avertissement](#)

NET::ERR_CERT_AUTHORITY_INVALID

Activez la protection renforcée pour bénéficier du plus haut niveau de sécurité de Chrome

Paramètres avancés Revenir en lieu sûr

Un message 'Votre connexion n'est pas privée' s'affiche, on clique sur paramètres avancés

Masquer les paramètres avancés

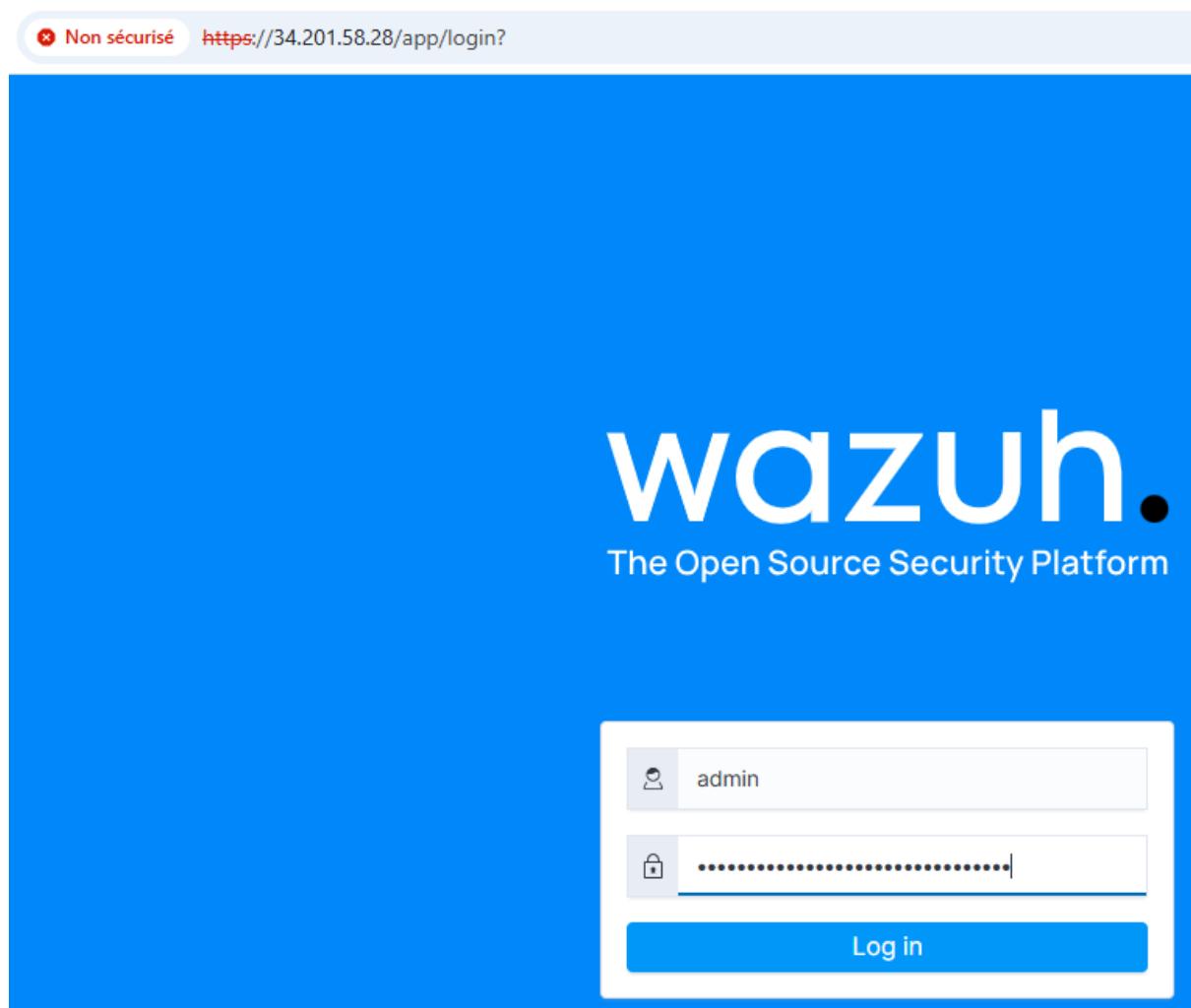
Revenir en lieu sûr

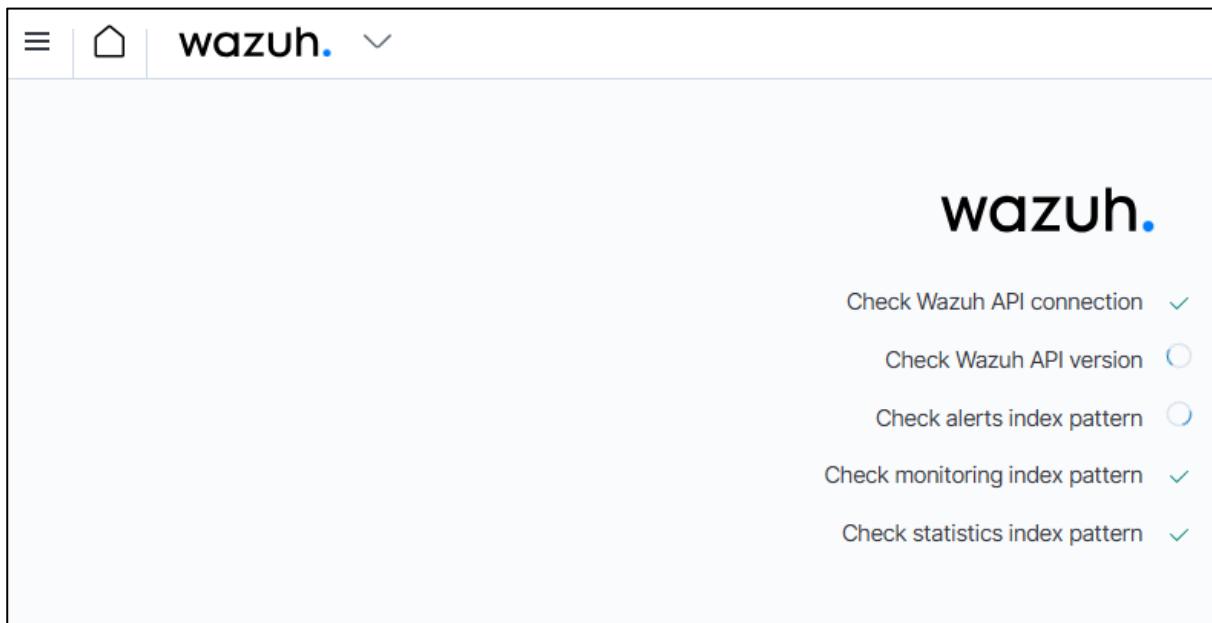
Impossible de vérifier sur le serveur qu'il s'agit bien du domaine **34.201.58.28**, car son certificat de sécurité n'est pas considéré comme fiable par le système d'exploitation de votre ordinateur. Cela peut être dû à une mauvaise configuration ou bien à l'interception de votre connexion par un pirate informatique.

[Continuer vers le site 34.201.58.28 \(dangereux\)](https://34.201.58.28/app/login?)

Et continuer vers le site

Une page login est ouverte, on entre login et password

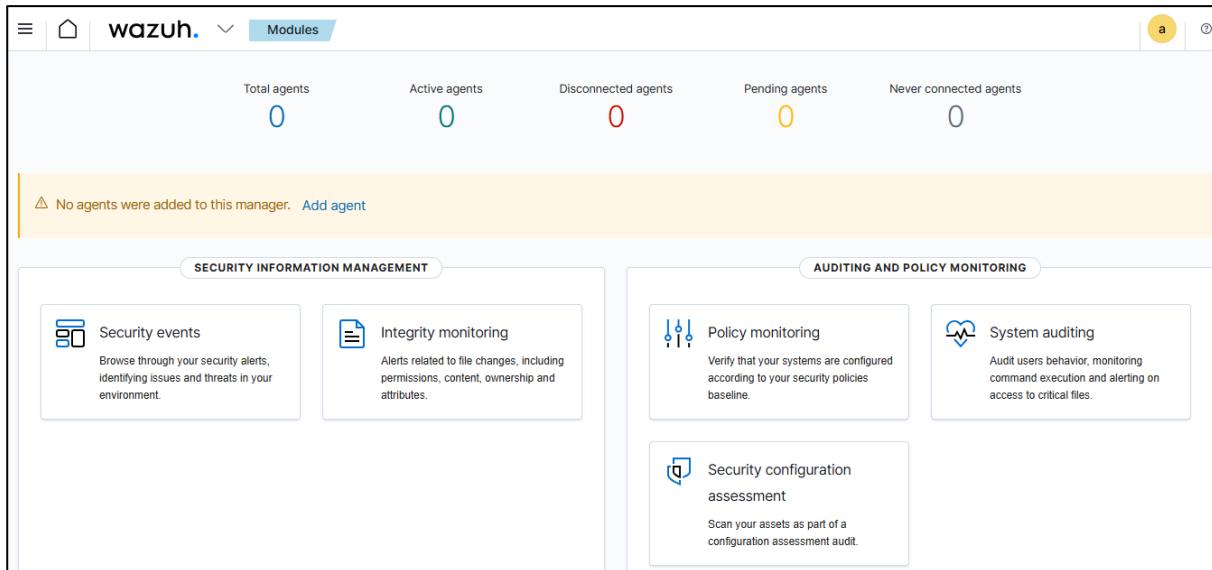




The dashboard shows a summary of Wazuh API connections and index patterns:

- Check Wazuh API connection: ✓
- Check Wazuh API version: ○
- Check alerts index pattern: ○
- Check monitoring index pattern: ✓
- Check statistics index pattern: ✓

Après l'authentification, la page d'accueil du dashboard Wazuh s'affiche. À ce stade, aucun agent n'est encore enrôlé dans la plateforme. Le tableau de bord indique donc un nombre d'agents égal à zéro et aucune alerte de sécurité n'est visible.



The dashboard displays the following agent counts:

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	0

A message indicates: "⚠ No agents were added to this manager. [Add agent](#)"

The dashboard is divided into two main sections:

- SECURITY INFORMATION MANAGEMENT** (Left):
 - Security events: Browse through your security alerts, identifying issues and threats in your environment.
 - Integrity monitoring: Alerts related to file changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING** (Right):
 - Policy monitoring: Verify that your systems are configured according to your security policies baseline.
 - System auditing: Audit users behavior, monitoring command execution and alerting on access to critical files.
 - Security configuration assessment: Scan your assets as part of a configuration assessment audit.

Étape 6 : Enrôlement du client Linux

Cette étape permet d'ajouter le client Linux à la plateforme de supervision Wazuh.

Déployer un nouvel agent soit en cliquant sur Add agent

⚠ No agents were added to this manager. [Add agent](#)

Ou cliquer sur Wazuh > Agent

The screenshot shows the Wazuh dashboard with the 'Modules' tab selected. On the left, there's a sidebar with icons for 'Management', 'Agents', 'Tools', 'Security', and 'Settings'. The main area is divided into several sections: 'Modules directory', 'Security information management' (with sub-options for 'Security Events' and 'Integrity Monitoring'), 'Auditing and Policy Monitoring' (with sub-options for 'Policy Monitoring', 'System Auditing', and 'Security configuration assessment'), 'Threat detection and response' (with sub-options for 'Vulnerabilities' and 'MITRE ATT&CK'), and 'Regulatory Compliance' (with sub-options for 'PCI DSS', 'GDPR', 'HIPAA', 'NIST 800-53', and 'TSC'). A message 'No agents found' is displayed in the top right corner.

6.1 Sélection du package à télécharger et à installer sur le système

Le package Linux a été sélectionné depuis le dashboard Wazuh.

The screenshot shows the 'Deploy new agent' page. At the top, there's a 'Refresh' button. Below it, the title 'Deploy new agent' is centered. A blue circular icon with a checkmark is followed by the instruction 'Select the package to download and install on your system:'. There are three boxes: 'LINUX' (selected), 'WINDOWS', and 'macOS'. The 'LINUX' box contains options for 'RPM amd64', 'RPM aarch64', 'DEB amd64' (selected), and 'DEB aarch64'. The 'WINDOWS' box contains 'MSI 32/64 bits'. The 'macOS' box contains 'Intel' and 'Apple silicon'. At the bottom, a note says 'For additional systems and architectures, please check our documentation' with a link icon.

6.2 Adresse du serveur

Copier l'adresse ipv4 privée du serveur Wazuh

Résumé de l'instance pour i-0603e89748ff9ff47 (Wazuh_Server) [Informations](#)

Mis à jour il y a 19 minutes

ID d'instance	<input checked="" type="checkbox"/> i-0603e89748ff9ff47	Adresse IPv4 publique	<input checked="" type="checkbox"/> 100.24.23.249 adresse ouverte ↗
Adresse IPv6	-	État de l'instance	<input checked="" type="checkbox"/> En cours d'exécution

Actions ▾

Adresse IPv4 privée copiée

Adresses IPv4 privées

10.0.0.196

DNS public

ec2-100-24-23-249.compute-1.amazonaws.com | [adresse ouverte ↗](#)

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: [?](#)

10.0.0.196

6.3 Paramètres optionnels

Entrer le nom de l'agent : Client-Linux

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [?](#)

Linux-Client

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

Select one or more existing groups: [?](#)

Default

6.4 Exécution des commandes pour télécharger et installer l'agent (client Linux)

6.4.1 Se connecter dans Wazuh-Linux-Client

Copier l'adresse ipv4 de Wazuh Linux client et se connecter via SSH

Se connecter Informations

Connectez-vous à une instance à l'aide du client basé sur un navigateur.

[EC2 Instance Connect](#)[Session Manager](#)[Client SSH](#)[EC2 Serial Console](#)

ID d'instance

[i-0f34083a528bedd49 \(Wazuh_Linux2_Client\)](#)

1. Ouvrez un client SSH.
2. Recherchez votre fichier de clé privée. La clé utilisée pour lancer cette instance est KEY_Wazuh_Linux2_Client.pem
3. Exécutez, si nécessaire, cette commande pour vous assurer que votre clé n'est pas visible publiquement.
 chmod 400 "KEY_Wazuh_Linux2_Client.pem"
4. Connectez-vous à votre instance à l'aide de son DNS public :

ec2-13-221-183-26.compute-1.amazonaws.com

Commande copiée

ssh -i "KEY_Wazuh_Linux2_Client.pem" ubuntu@ec2-13-221-183-26.compute-1.amazonaws.com

```
C:\Users\PC\Downloads>ssh -i "KEY_Wazuh_Linux2_Client.pem" ubuntu@ec2-13-221-183-26.compute-1.amazonaws.com
The authenticity of host 'ec2-13-221-183-26.compute-1.amazonaws.com (13.221.183.26)' can't be established.
ED25519 key fingerprint is SHA256:RADM12u9MdVcVgZuF2Tzk+c227UAMRx7UlvgZmcxsmw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-221-183-26.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1040-aws x86_64)

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

System information as of Wed Jan  7 19:25:13 UTC 2026

System load:  0.08      Processes:          104
Usage of /:   22.7% of 7.57GB  Users logged in:     0
Memory usage: 24%           IPv4 address for ens5: 10.0.0.206
Swap usage:   0%

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-10-0-0-206:~$
```

6.4.2 Copier le code de cette étape et l'exécuter



Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb &&
sudo WAZUH_MANAGER='10.0.0.196' WAZUH_AGENT_NAME='Linux-Client' dpkg -i ./wazuh-agent_4.7.5-
1_amd64.deb
```

① Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

```
ubuntu@ip-10-0-0-206:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-
agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='10.0.0.196' WAZUH_AGENT_NAME='Linux-Client' dpk
g -i ./wazuh-agent_4.7.5-1_amd64.deb
--2026-01-07 19:31:11-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-ag
ent_4.7.5-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 13.226.209.111, 13.226.209.39, 13.226.209
.93, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|13.226.209.111|: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  ---KB/s    in 0.02s

2026-01-07 19:31:11 (366 MB/s) - 'wazuh-agent_4.7.5-1_amd64.deb' saved [9378818/9378818]

Selecting previously unselected package wazuh-agent.
(Reading database ... 65993 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) ...
```

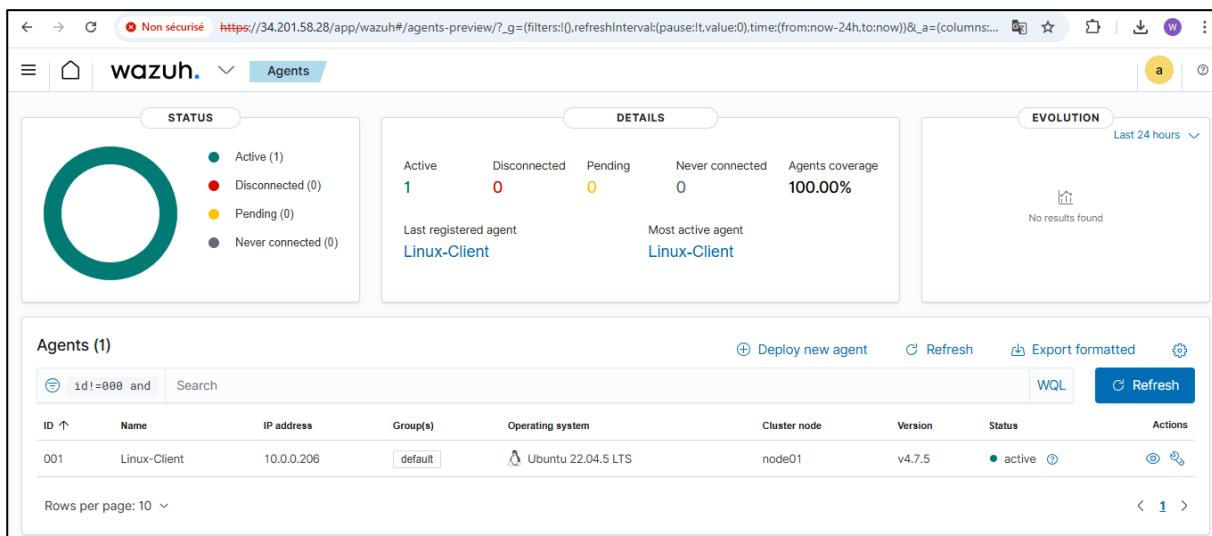
6.5 Démarrage de l'agent

Copier le code de cette étape



```
ubuntu@ip-10-0-0-206:~$ sudo systemctl daemon-reload
ubuntu@ip-10-0-0-206:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
ubuntu@ip-10-0-0-206:~$ sudo systemctl start wazuh-agent
ubuntu@ip-10-0-0-206:~$
```

Une fois démarré, l'agent apparaît comme **Active** dans le dashboard.



The dashboard shows the following details:

- STATUS:** Active (1), Disconnected (0), Pending (0), Never connected (0).
- DETAILS:** Last registered agent: Linux-Client, Most active agent: Linux-Client.
- EVOLUTION:** Last 24 hours, No results found.

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Linux-Client	10.0.0.206	default	Ubuntu 22.04.5 LTS	node01	v4.7.5	active	Edit Logs

Étape 7 : Enrôlement du client Windows

Cette étape permet d'ajouter l'endpoint Windows à Wazuh.

7.1 Sélection du package à télécharger et à installer sur le système

× Close

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 [↗](#).

7.2 Adresse du serveur

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: [?](#)

7.3 Paramètres optionnels

Entrer le nom de l'agent : Client-Windows

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ⓘ

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled. ↗

Select one or more existing groups: ⓘ

7.4 Exécution des commandes pour télécharger et installer l'agent (client Windows)

7.4.1 Se connecter à Wazuh Windows Client

La connexion à distance vers l'instance Windows a été réalisée à l'aide du protocole RDP afin d'accéder au système et installer l'agent Wazuh.



Récupérer le mot de passe

Cliquer sur Actions > Sécurité > Obtenir le mot de passe Windows

Actions ▲ **Lancer des instances ▼**

- Diagnostic des instances
- Paramètres de l'instance
- Mise en réseau
- Sécurité**
- Image et modèles
- Stockage
- Surveiller et dépanner

Tous les états ▼ < 1

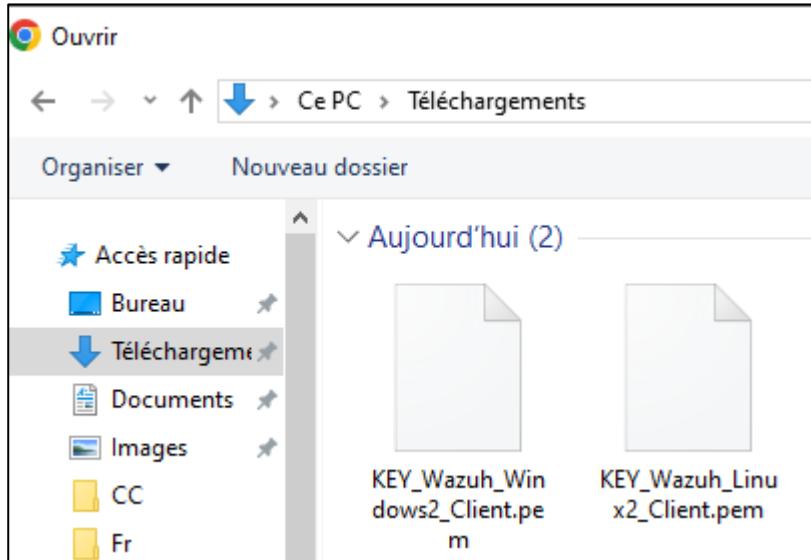
ta... | Contrôle des statu | Statut

ⓘ 3/3 vérifications r Affich

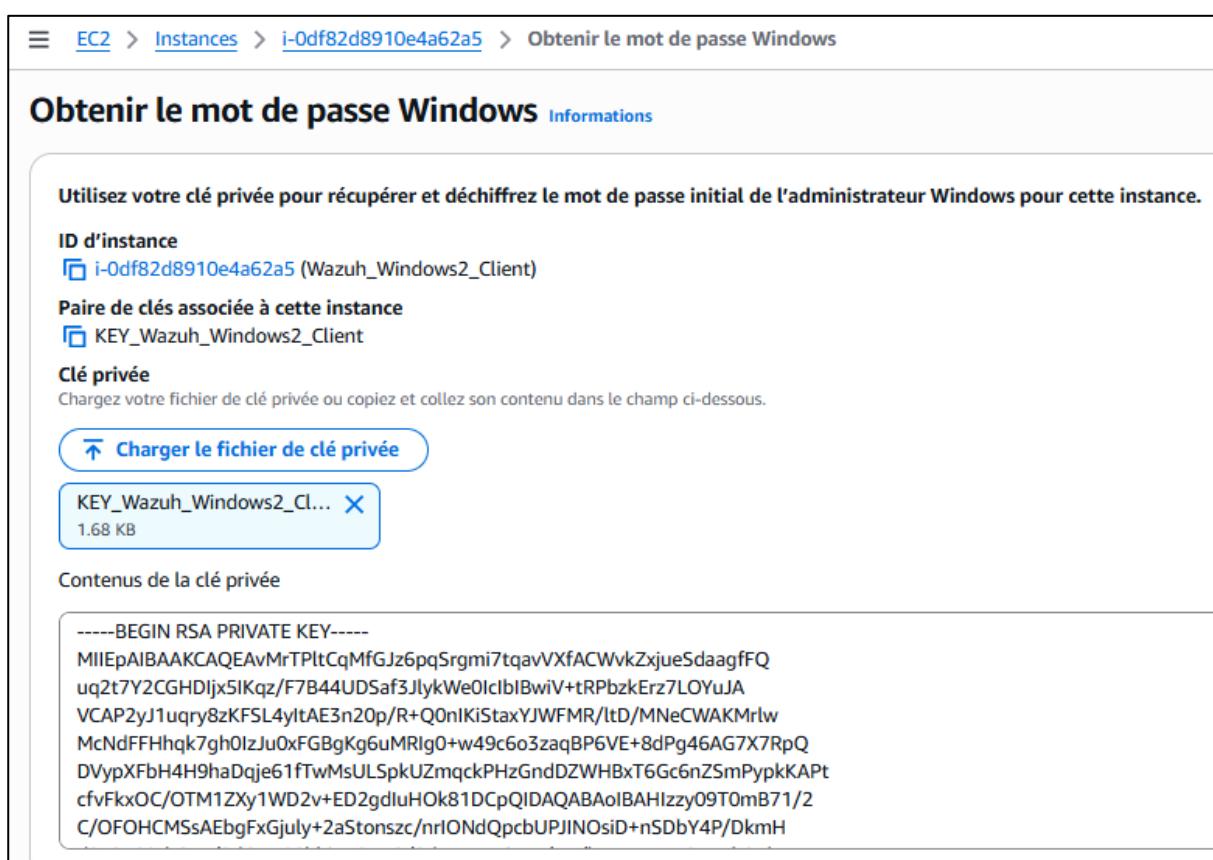
- Modifier les groupes de sécurité
- Obtenir le mot de passe Windows**
- Modifier le rôle IAM

ⓘ 2/2 vérifications r Affich

Charger la clé 'Wazuh_Windows2_Client.pem' depuis téléchargement



Nom du fichier : KEY_Wazuh_Windows2_Client.pem



Obtenir le mot de passe Windows Informations

Utilisez votre clé privée pour récupérer et déchiffrez le mot de passe initial de l'administrateur Windows pour cette instance.

ID d'instance
 i-0df82d8910e4a62a5 (Wazuh_Windows2_Client)

Paire de clés associée à cette instance
 KEY_Wazuh_Windows2_Client

Clé privée
 Chargez votre fichier de clé privée ou copiez et collez son contenu dans le champ ci-dessous.

KEY_Wazuh_Windows2_Cl...
 1.68 KB

Contenus de la clé privée

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAQCAQEAvMrTPltCqMfGJz6pqSrgmi7tqavVXfACWvkZxjueSdaagFFQ
uq2t7Y2CGHDlx5IKqz/F7B44UDSaf3JlykWe0lclbIBwiV+tRPbzkErz7LOYuJA
VCAP2yJ1uqry8zKFSL4yltAE3n20p/R+Q0nIKiStaxYWFMR/lD/MNeCWAKMrlw
McNdFFHhqk7gh0lJu0xFGBgKg6uMRlg0+w49c6o3zaqBP6VE+8dPg46AG7X7RpQ
DVypXFbH4H9haDqje61ftwMsULSpkUZmqckPHzGndDZWHBxT6Gc6nZSmPypkKAPt
cfvFkxOC/OTM1Zx1WD2v+ED2gdluHOk81DCpQIDAQABAoIBAHlzy09T0mB71/2
C/OFOHCMSSAEbgFxGJuly+2aStonszc/nrlONdQpcbUPJINOSiD+nSDbY4P/DkmH
```

Cliquer sur : déchiffrer le mot de passe

Annulez **Déchiffrer le mot de passe**

Obtenir le mot de passe Windows



Connectez-vous à votre instance Windows à l'aide des services Bureau à distance avec ces informations.

ID d'instance

i-0df82d8910e4a62a5 (Wazuh_Windows2_Client)

Adresse IP privée

10.0.0.12

Nom d'utilisateur

Administrator

Mot de passe

Ro.*fc1B;\$HB!MNOcdGG4hpYrd)\$@myl

ⓘ Changement de mot de passe recommandé

Nous vous recommandons de changer votre mot de passe par défaut.

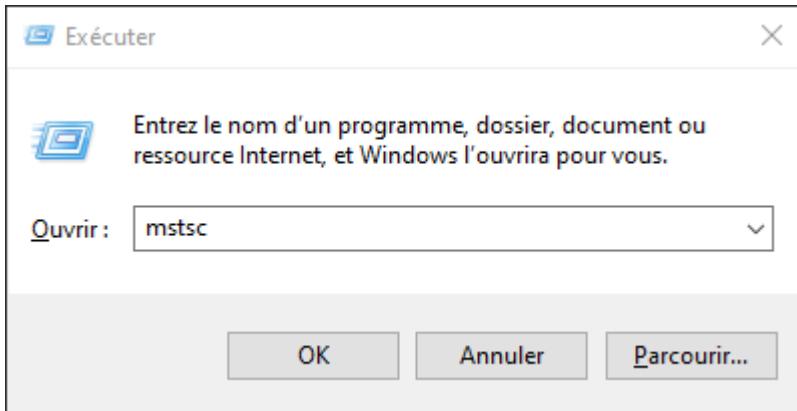
Remarque : un mot de passe par défaut modifié ne peut pas être récupéré à l'aide de cet outil. Il est important que vous choisissez un nouveau mot de passe dont vous vous souviendrez.

Annulez

OK

Se connecter à distance via le protocole RDP

Appuyer sur Windows + R puis Tapes : mstsc



Copier l'adresse ipv4 publique de Windows client

Résumé de l'instance pour i-0df82d8910e4a62a5 (Wazuh_Windows2_Client) [Informations](#)

[Se connecter](#) [État de l'instance](#) [Adresse IPv4 publique copiée](#)

Mis à jour il y a 2 minutes

ID d'instance [i-0df82d8910e4a62a5](#)

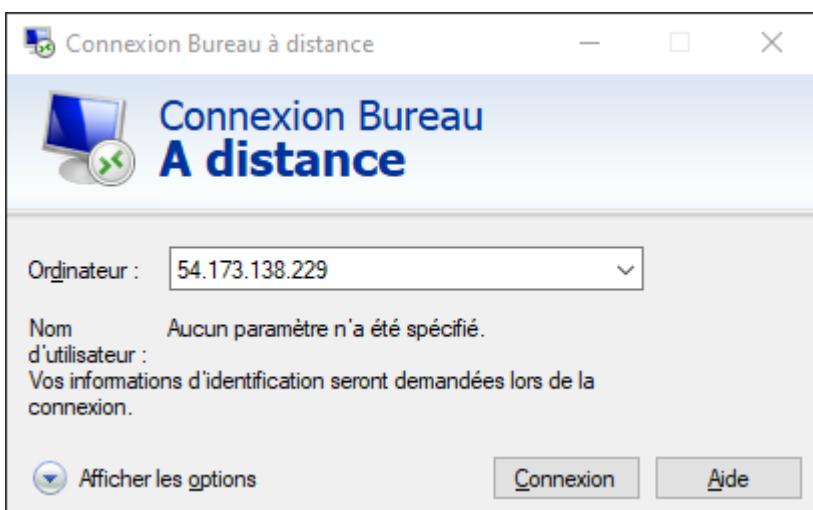
Adresse IPv6 -

Adresse IPv4 publique [54.173.138.229 | adresse ouverte ↗](#)

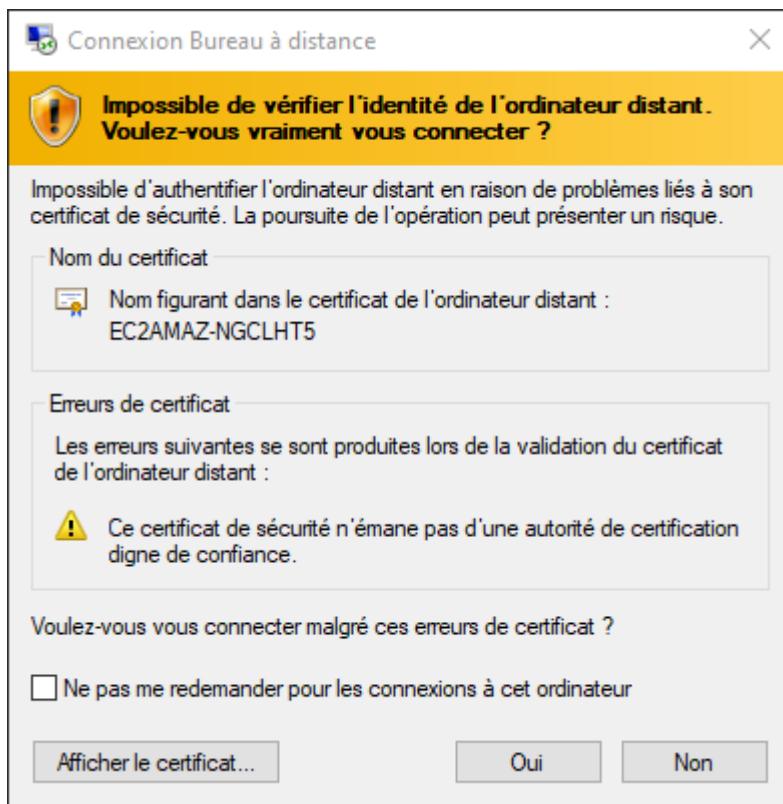
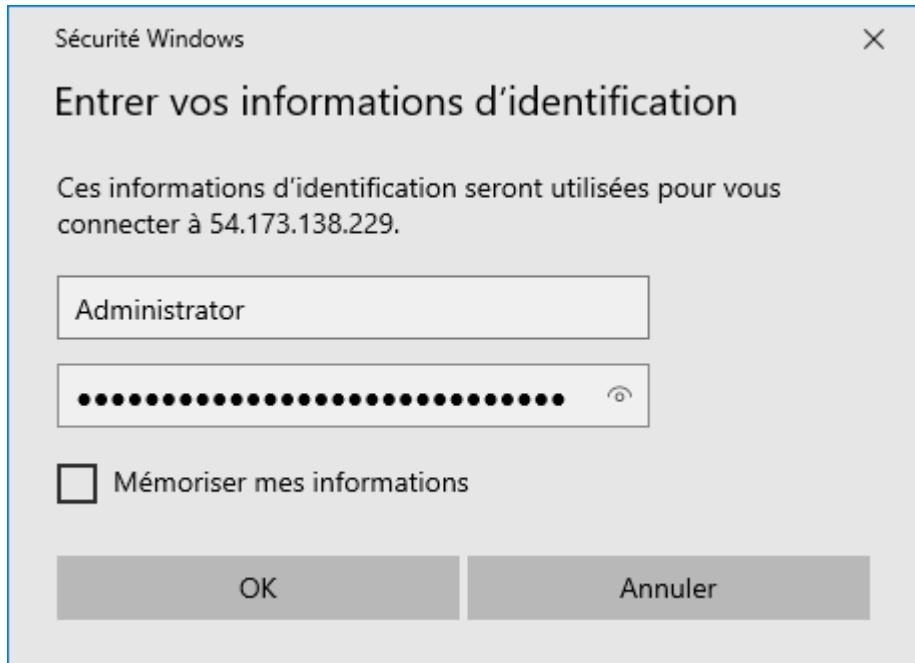
État de l'instance [En cours d'exécution](#)

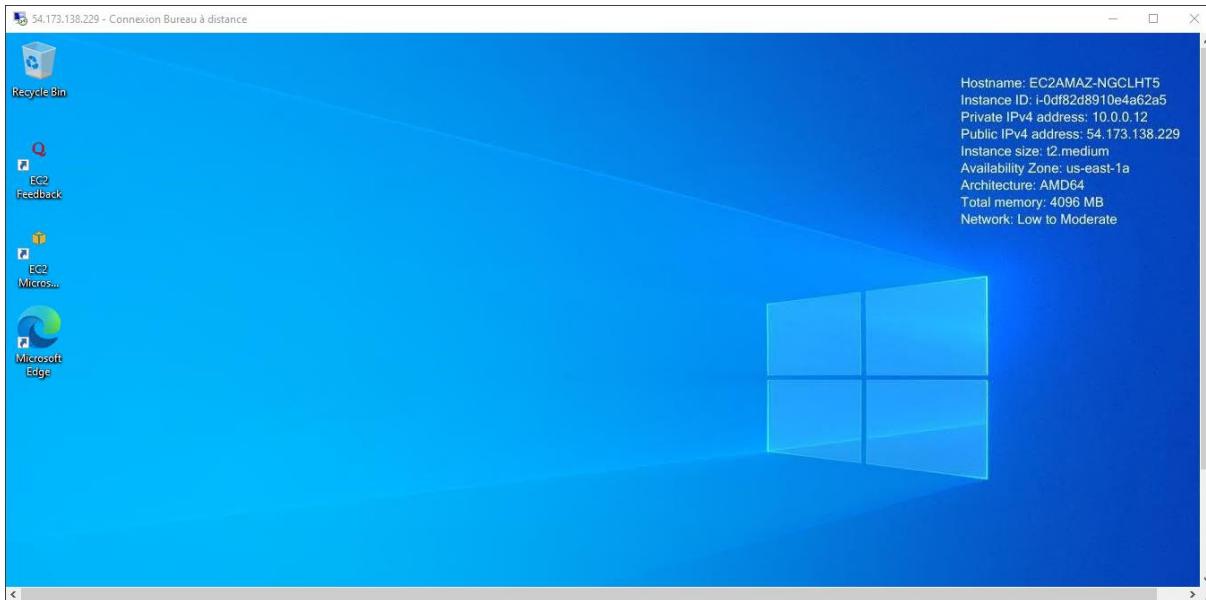
Adresses IPv4 privées [10.0.0.12](#)

DNS public [ec2-54-173-138-229.compute-1.amazonaws.com | adresse ouverte ↗](#)



Entrer Login et Password récupérés





7.4.2 Copier le code de cette étape et l'exécuter

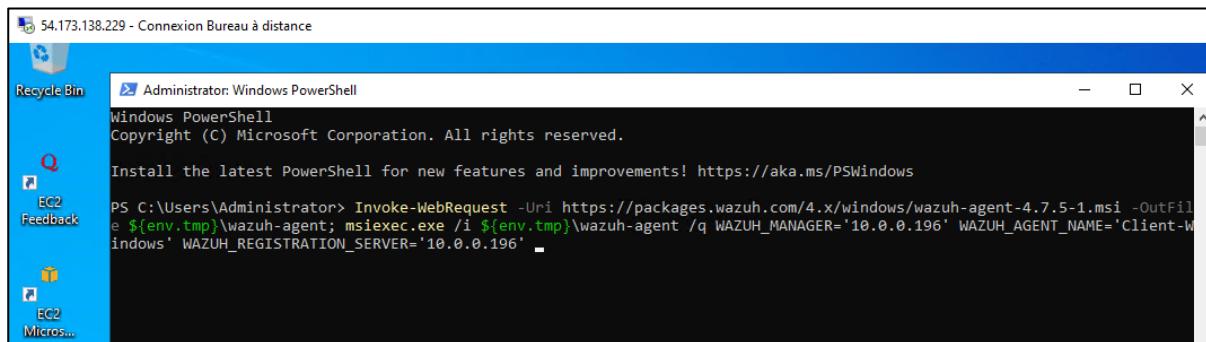
Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile ${env.tmp}\wazuh-agent; msieexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='10.0.0.196' WAZUH_AGENT_NAME='Client-Windows' WAZUH_REGISTRATION_SERVER='10.0.0.196'
```

① Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

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



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile ${env.tmp}\wazuh-agent; msieexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='10.0.0.196' WAZUH_AGENT_NAME='Client-Windows' WAZUH_REGISTRATION_SERVER='10.0.0.196'
PS C:\Users\Administrator>
```

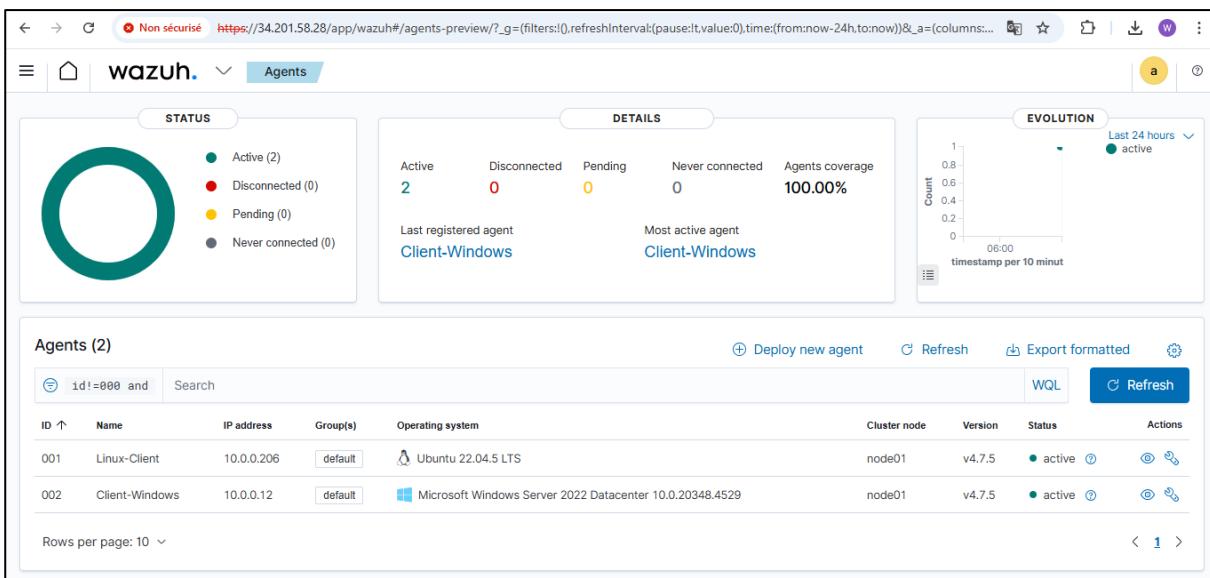
7.5 Démarrage de l'agent

Copier le code de cette étape et l'exécuter

```
PS C:\Users\Administrator> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Users\Administrator>
```

Après installation, le service Wazuh Agent a été démarré avec succès.



The screenshot shows the Wazuh Agents Preview interface. At the top, there's a summary section with a large green circle indicating all agents are active. Below it, a table lists two agents:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Linux-Client	10.0.0.206	default	Ubuntu 22.04.5 LTS	node01	v4.7.5	active	Details Logs
002	Client-Windows	10.0.0.12	default	Microsoft Windows Server 2022 Datacenter 10.0.20348.4529	node01	v4.7.5	active	Details Logs

At the bottom, there are buttons for 'Deploy new agent', 'Refresh', 'Export formatted', and 'WQL'. A small chart titled 'EVOLUTION' shows the count of active agents over the last 24 hours.

Étape 8 : Scénarios de démonstration de sécurité (Démo SIEM + EDR : scénarios d'événements à générer)

8.1 Scénarios pour Linux Client (Démo SIEM côté Linux (rapide, visible tout de suite))

8.1.1 Scénario 1 : Tentatives SSH échouées (bruteforce simulé)

Modifier les règles entrantes de SG-Wazuh-Clients

Règles entrantes (2)						
ID de règle de groupe	Version IP	Type	Protocole	Plage de ports	Source	
sgr-0ed93b8dcfe4d4ce0	IPv4	RDP	TCP	3389	41.249.7.13/32	
sgr-093c82c1eeaaf4223	IPv4	SSH	TCP	22	41.249.7.13/32	

Règles entrantes Informations						
ID de règle de groupe de sécurité	Type	Informations	Protocole	Informations	Plage de ports	Source
sgr-0ed93b8dcfe4d4ce0	RDP		TCP		3389	Mon IP
sgr-093c82c1eeaaf4223	SSH		TCP		22	Mon IP

Ajouter une autre règle ssh pour autoriser Wazuh-server à entrer (SSH , source : SG-wazuh-Server)

-	SSH		TCP		22	Perso...	41.249.7.13/32	
<input style="width: 100%;" type="text" value="sg-0c4a1c596225b2689"/> Utiliser : «sg-0c4a1c596225b2689» Blocs d'adresse CIDR Groupes de sécurité SG-Wazuh-Server sg-0c4a1c596225b2689 notifications								

Enregistrer les règles

⌚ Les règles de groupe de sécurité entrantes ont été modifiées avec succès sur le groupe de sécurité. (sg-0e5f826079665b5a3 | SG-Wazuh-Clients)

Règles entrantes						
Règles entrantes (3)						
ID de règle de groupe	Version IP	Type	Protocole	Plage de ports	Source	Description
-	IPv4	RDP	TCP	3389	41.249.7.13/32	-
-	IPv4	SSH	TCP	22	41.249.7.13/32	-
-	SSH		TCP		22	sg-0c4a1c596225b2689...

La commande ssh fakeuser@10.0.0.206 10 fois

```
ubuntu@ip-10-0-0-196:~$ ssh fakeuser@10.0.0.206
The authenticity of host '10.0.0.206 (10.0.0.206)' can't be established.
ED25519 key fingerprint is SHA256:RADMl2u9MdVcVgZuF2TZk+c227UAMrx7UlgZmcxsmw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.206' (ED25519) to the list of known hosts.
fakeuser@10.0.0.206: Permission denied (publickey).
ubuntu@ip-10-0-0-196:~$ ssh fakeuser@10.0.0.206
fakeuser@10.0.0.206: Permission denied (publickey).
```

Alerte :

Security events ⓘ							
> Jan 7, 2026 @ 21:36:13.956	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:11.956	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:11.954	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:09.952	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:07.950	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:03.946	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

8.1.2 Scénario 2 : Élévation de privilèges

sudo su

```
ubuntu@ip-10-0-0-196:~$ sudo su
root@ip-10-0-0-196:/home/ubuntu#
```

Alertes :

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 7, 2026 @ 21:43:01.879	000	ip-10-0-0-196	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
> Jan 7, 2026 @ 21:43:01.879	000	ip-10-0-0-196	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Jan 7, 2026 @ 21:43:01.879	000	ip-10-0-0-196	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501

8.1.3 Scénario 3 : Modification fichier sensible (FIM)

echo test | sudo tee -a /etc/passwd

```
ubuntu@ip-10-0-0-206:~$ echo test | sudo tee -a /etc/passwd
test
```

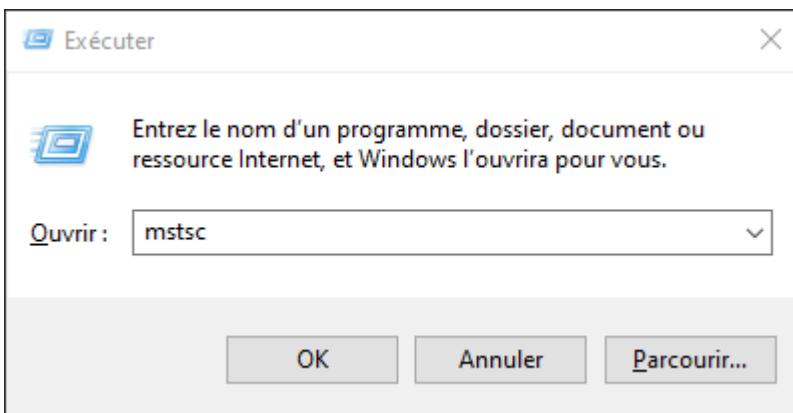
Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 7, 2026 @ 22:07:09.831	001	Linux-Client	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Jan 7, 2026 @ 22:07:09.831	001	Linux-Client			PAM: Login session closed.	3	5502
> Jan 7, 2026 @ 22:07:09.790	001	Linux-Client	T1548.003	Privilege Escalation, Defense Evasion	First time user executed sudo.	4	5403

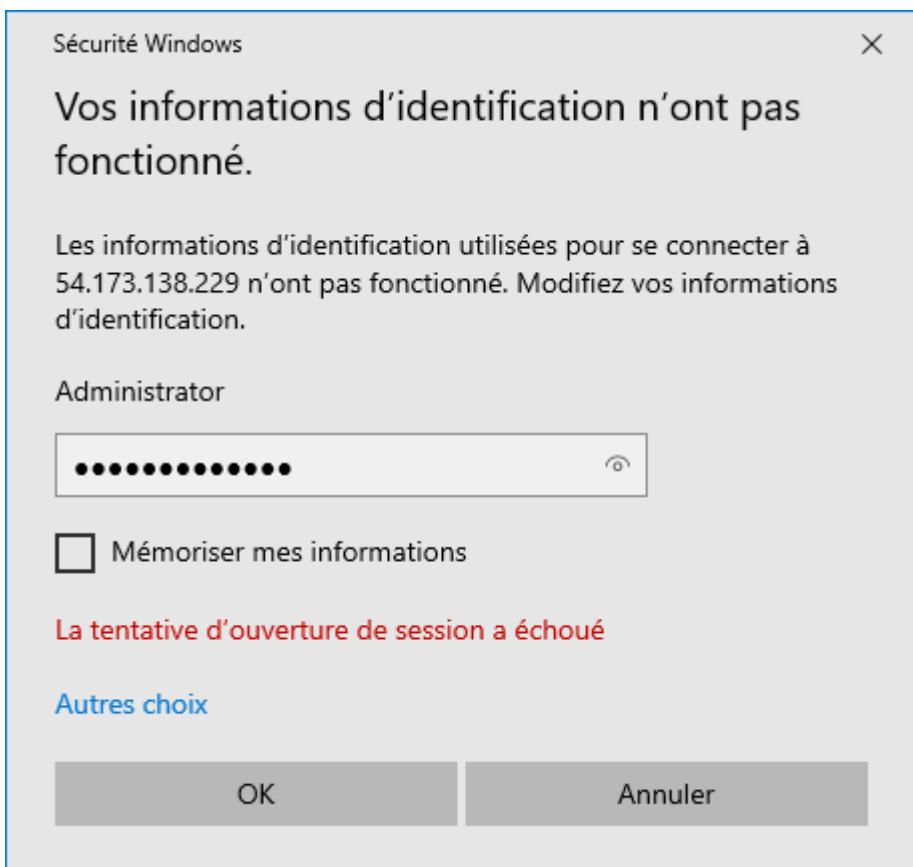
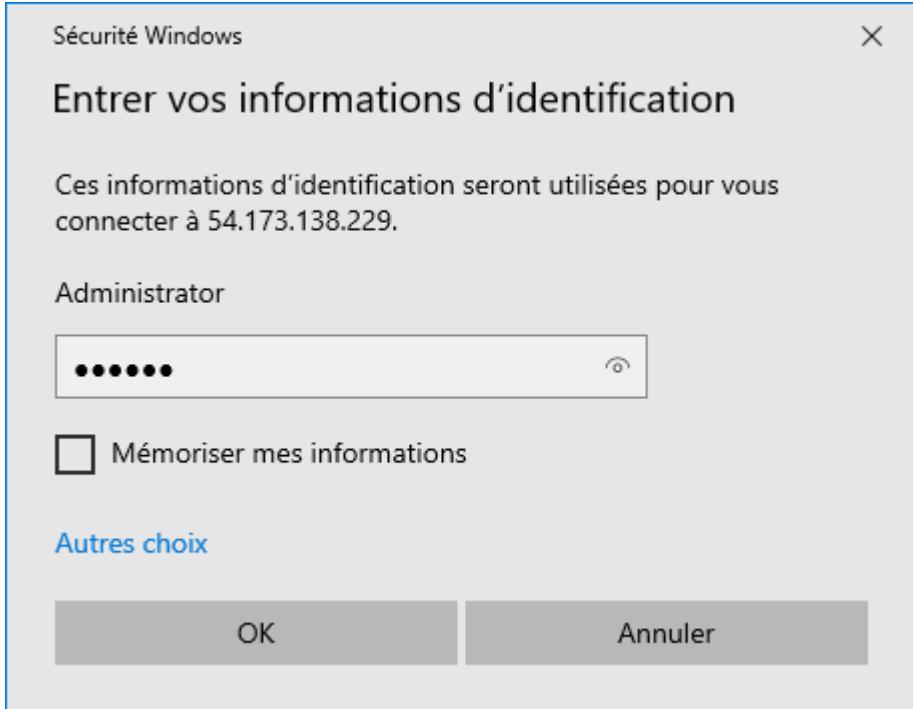
Pas d'alerte File Integrity Monitoring car elle n'est pas activé sur ce chemin

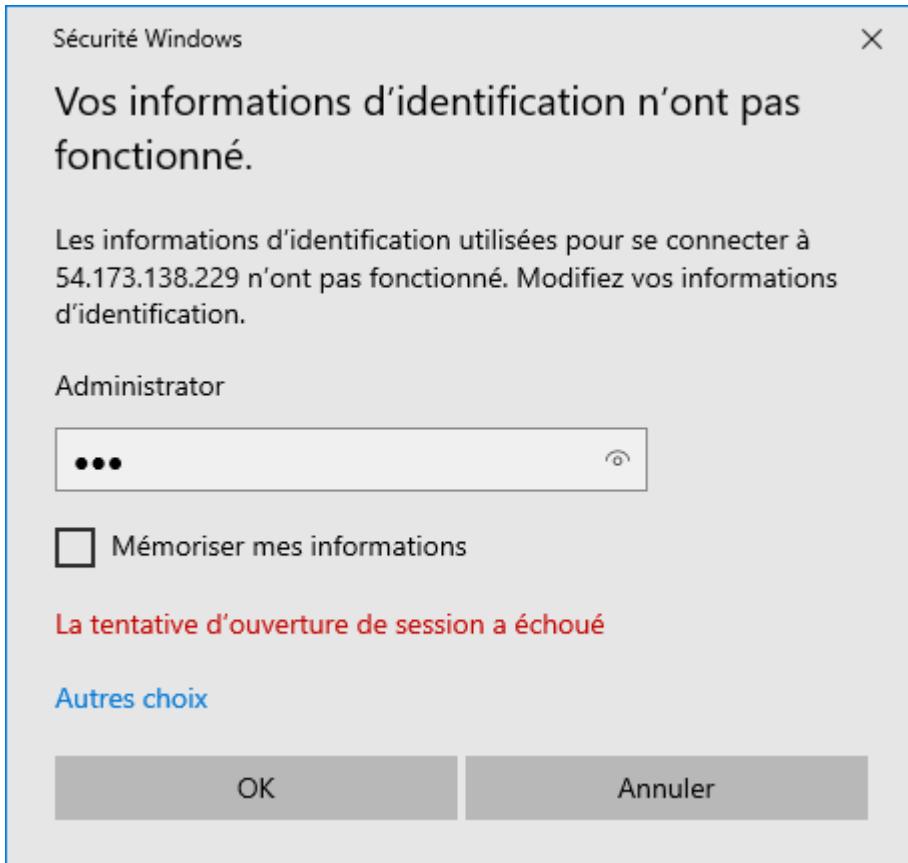
8.2 Scénarios pour Windows Client (Démo EDR côté Windows (événements sécurité + option Sysmon))

8.2.1 Scénario 1 : Échecs de login (4625)

Sur Windows : faire des connexions RDP avec mauvais mot de passe (3 fois)







Résultat : événements Windows Security (Failed login)

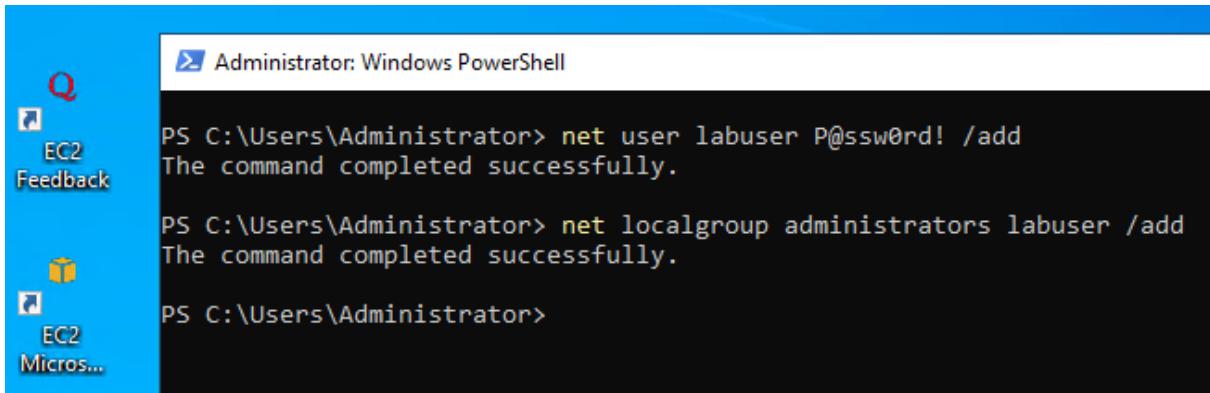
Security Alerts						
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID	
> Jan 7, 2026 @ 22:21:34.893	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122	
> Jan 7, 2026 @ 22:20:36.708	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122	
> Jan 7, 2026 @ 22:20:18.816	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122	

8.2.2 Scénario 2 : Création d'un utilisateur local

PowerShell (Admin) :

```
net user labuser P@sswOrd! /add
```

```
net localgroup administrators labuser /add
```



```

Administrator: Windows PowerShell

PS C:\Users\Administrator> net user labuser P@ssw0rd! /add
The command completed successfully.

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

PS C:\Users\Administrator>

```

Alertes :

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 7, 2026 @ 22:03:12.665	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Administrators group changed.	12	60154
> Jan 7, 2026 @ 22:02:47.805	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Users group changed.	5	60170
> Jan 7, 2026 @ 22:02:47.788	002	Client-Windows	T1098	Persistence	User account enabled or created.	8	60109
> Jan 7, 2026 @ 22:02:47.787	002	Client-Windows	T1098	Persistence	User account enabled or created.	8	60109
> Jan 7, 2026 @ 22:02:47.787	002	Client-Windows	T1098	Persistence	User account changed.	8	60110
> Jan 7, 2026 @ 22:02:47.747	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Domain users group changed.	5	60160

4. Analyse et résultats

4.1 Détection des événements de sécurité

Dans cette partie, l'objectif est de montrer que Wazuh détecte bien ce que tu as provoqué sur Linux et Windows.

4.1.1 Résultats côté client Linux

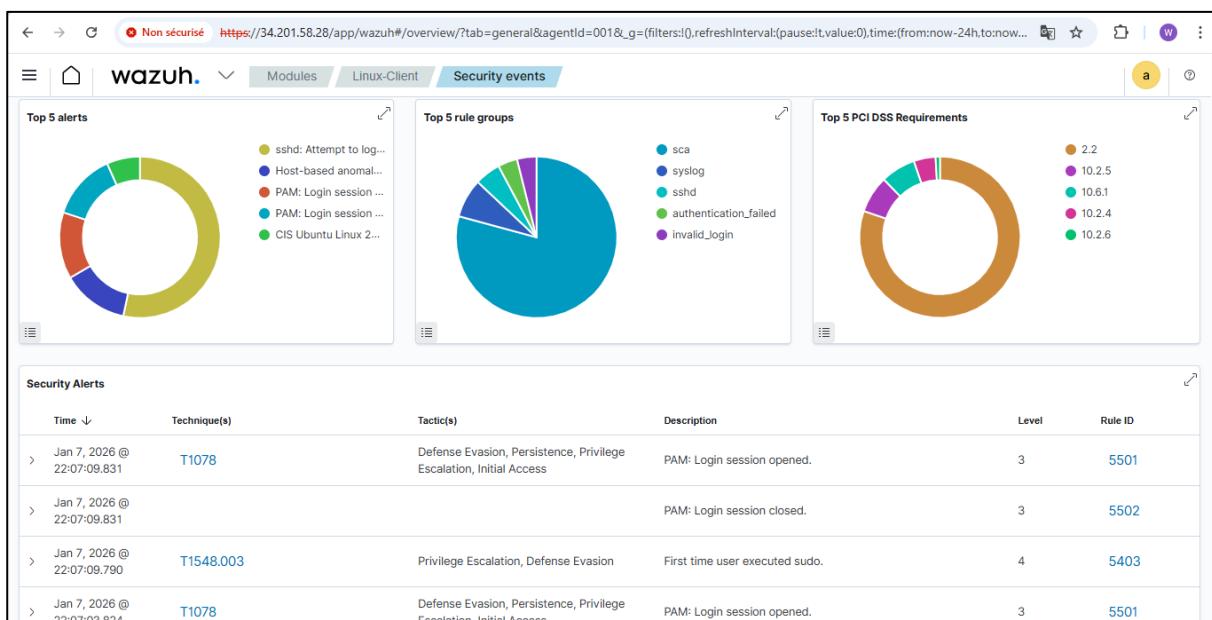
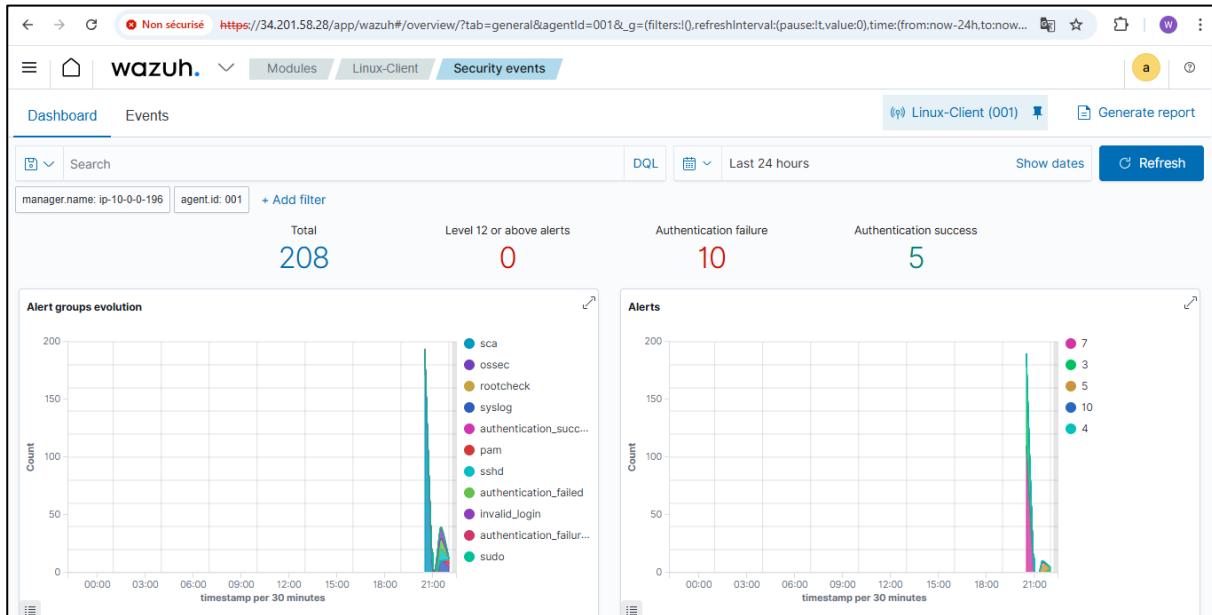
Alertes observées

Après l'exécution des scénarios de test sur le client Linux (tentatives SSH échouées, élévation de priviléges), plusieurs alertes ont été générées et remontées vers le serveur Wazuh.

Les événements détectés concernent principalement :

- Des tentatives d'authentification SSH échouées,
- Des actions nécessitant une élévation de priviléges (commande sudo).

Ces événements sont automatiquement analysés par Wazuh et classés selon leur niveau de严重性 (severity).



4.1.2 Résultats côté client Windows

Alertes observées

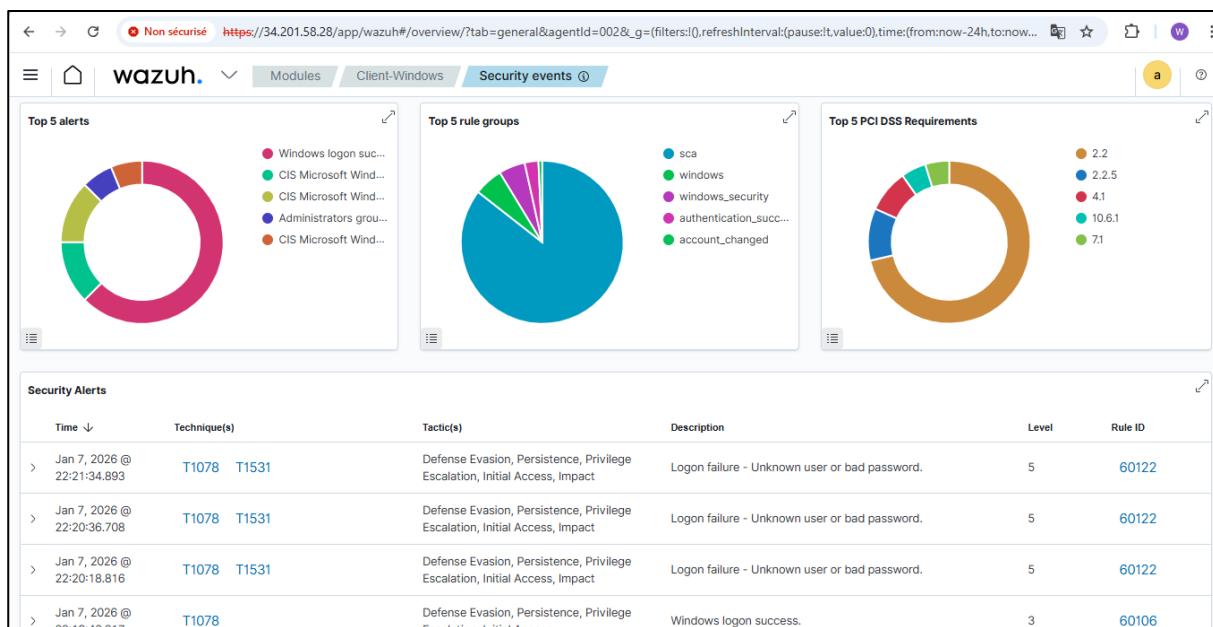
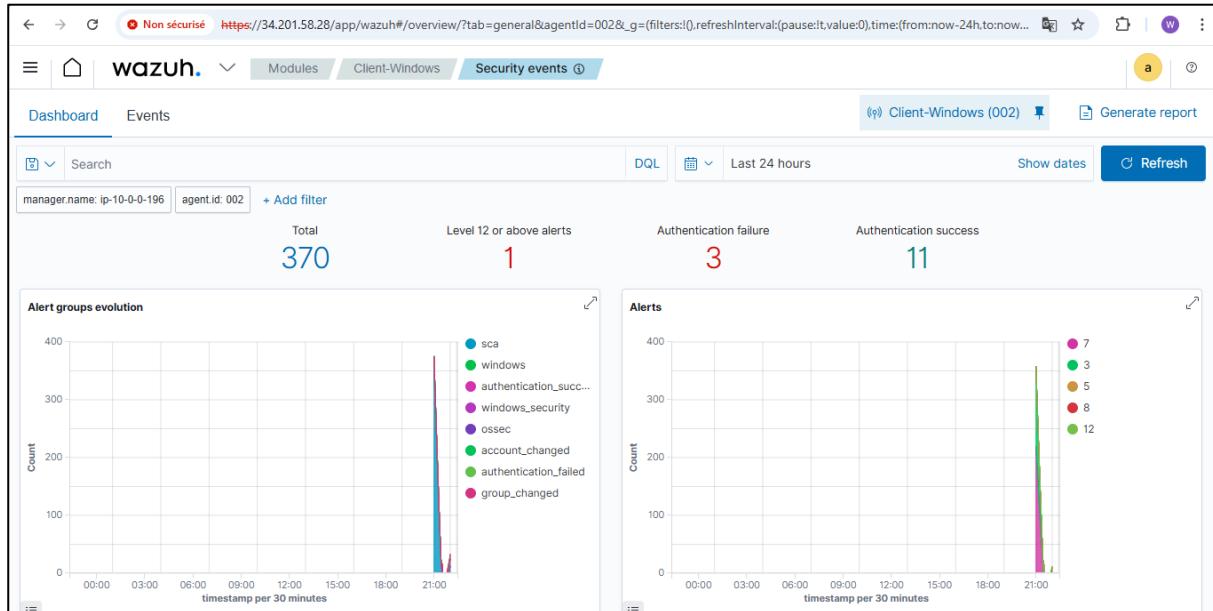
Sur le client Windows, les scénarios réalisés (échecs de connexion et création d'un utilisateur local) ont généré des événements de sécurité Windows.

Wazuh a permis de détecter :

- Des échecs de connexion (Event ID 4625),
- La création d'un nouvel utilisateur local,

- L'ajout de cet utilisateur au groupe Administrators.

Ces événements sont critiques dans un contexte de sécurité, car ils peuvent indiquer une tentative de compromission.



4.2 Apport du SIEM dans la supervision

L'utilisation d'une solution SIEM comme Wazuh permet de centraliser les événements de sécurité provenant de plusieurs systèmes dans une seule interface. Cela facilite la supervision globale de l'infrastructure et permet de détecter rapidement des comportements suspects.

Grâce au tableau de bord SIEM, il est possible d'analyser les alertes, de filtrer les événements par agent ou par type, et d'avoir une vision claire de l'état de sécurité des endpoints Linux et Windows.

Ce projet montre l'importance du SIEM dans un SOC moderne, en particulier dans un environnement Cloud où plusieurs systèmes doivent être surveillés en temps réel.

5. Apports de l'atelier : SIEM, EDR, IAM/PAM et Threat Hunting

Cette partie présente les principaux apports de l'atelier en termes de **supervision, sécurité des endpoints et analyse des menaces**, à travers les concepts de **SIEM, EDR, IAM/PAM et Threat Hunting**, illustrés par les scénarios réalisés dans le lab Wazuh.

5.1 Apport du SIEM dans l'atelier

Qu'est-ce qu'un SIEM ?

Un **SIEM (Security Information and Event Management)** est une solution qui permet de **centraliser, corréler et analyser** les événements de sécurité provenant de différentes sources d'un système d'information (serveurs, endpoints, applications, équipements réseau).

Rôle du SIEM dans ce projet

Dans ce lab, le rôle du SIEM est assuré par **Wazuh**, qui centralise les événements de sécurité générés par :

- Le client Linux (logs SSH, commandes sudo, activités système),
- Le client Windows (événements de sécurité Windows, connexions, comptes utilisateurs).

Le serveur Wazuh reçoit ces événements, les analyse et génère des **alertes de sécurité** visibles dans le **dashboard SIEM**.

Grâce au SIEM, il est possible de :

- Visualiser toutes les alertes dans une interface unique,
- Corréler des événements provenant de systèmes différents,
- Identifier rapidement des comportements suspects ou anormaux.

Exemple concret dans le lab

Lors des tests réalisés :

- Les tentatives SSH échouées sur le client Linux ont été détectées,
- Les événements Windows liés aux échecs de connexion et à la création de comptes ont été remontés,
- Toutes ces alertes ont été centralisées et visualisées dans le dashboard Wazuh.

wazuh. ▾ Modules Security events ⓘ							
> Jan 7, 2026 @ 21:36:13.956	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:11.956	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:11.954	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:09.952	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:07.950	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Jan 7, 2026 @ 21:36:03.946	001	Linux-Client	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

5.2 Apport de l'EDR dans la sécurité des endpoints

Qu'est-ce qu'un EDR ?

Un **EDR (Endpoint Detection and Response)** se concentre sur la **surveillance des endpoints** (postes utilisateurs et serveurs).

Il permet de détecter des comportements suspects directement au niveau du système local.

Rôle de l'EDR dans ce projet

Dans cet atelier, l'EDR est assuré par les **agents Wazuh installés sur les endpoints Linux et Windows**.

Ces agents permettent de détecter :

- Des élévations de privilèges (commande `sudo` sur Linux),
- Des tentatives d'accès non autorisées,
- La création et la modification de comptes utilisateurs sur Windows,
- Les échecs de connexion répétés.

Sur Windows, l'ajout optionnel de **Sysmon** permet d'enrichir la détection avec des informations plus détaillées sur les processus et les connexions.

Exemple concret dans le lab

- Sur Linux : détection des commandes exécutées avec privilèges élevés,
- Sur Windows : détection de la création d'un nouvel utilisateur et de son ajout au groupe Administrators

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 7, 2026 @ 21:43:01.879	000	ip-10-0-0-196	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
> Jan 7, 2026 @ 21:43:01.879	000	ip-10-0-0-196	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Jan 7, 2026 @ 21:43:01.879	000	ip-10-0-0-196	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 7, 2026 @ 22:03:12.665	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Administrators group changed.	12	60154
> Jan 7, 2026 @ 22:02:47.805	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Users group changed.	5	60170
> Jan 7, 2026 @ 22:02:47.788	002	Client-Windows	T1098	Persistence	User account enabled or created.	8	60109
> Jan 7, 2026 @ 22:02:47.787	002	Client-Windows	T1098	Persistence	User account enabled or created.	8	60109
> Jan 7, 2026 @ 22:02:47.787	002	Client-Windows	T1098	Persistence	User account changed.	8	60110
> Jan 7, 2026 @ 22:02:47.747	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Domain users group changed.	5	60160

5.3 Comparaison

Critère	SIEM	EDR
Focus principal	Infrastructure globale	Endpoints
Source des données	Logs multi-sources	Activités locales
Type de détection	Corrélation d'événements	Comportement local
Réponse	Alertes, analyse	Détection locale
Visibilité	Vue globale	Vue détaillée par machine
Exemple dans le lab	Centralisation Linux + Windows	Détection sudo, comptes Windows

Dans ce projet, **SIEM et EDR sont complémentaires :**

- Le SIEM offre une vision globale,
- L'EDR permet une analyse fine des actions locales.

5.4 IAM / PAM et contrôle des accès

Les scénarios réalisés dans cet atelier mettent en évidence l'importance de la gestion des identités et des priviléges (IAM / PAM).

Les actions suivantes ont été détectées :

- Tentatives de connexion échouées,
- Exécution de commandes avec priviléges élevés,
- Création et modification de comptes utilisateurs.

La supervision de ces événements permet de limiter les risques liés aux abus de priviléges et aux accès non autorisés.

Exemple du Lab : Alerte liée à une **création de compte Windows**

Security Alerts							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Jan 7, 2026 @ 22:03:12.665	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Administrators group changed.	12	60154
> Jan 7, 2026 @ 22:02:47.805	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Users group changed.	5	60170
> Jan 7, 2026 @ 22:02:47.788	002	Client-Windows	T1098	Persistence	User account enabled or created.	8	60109
> Jan 7, 2026 @ 22:02:47.787	002	Client-Windows	T1098	Persistence	User account enabled or created.	8	60109
> Jan 7, 2026 @ 22:02:47.787	002	Client-Windows	T1098	Persistence	User account changed.	8	60110
> Jan 7, 2026 @ 22:02:47.747	002	Client-Windows	T1484	Defense Evasion, Privilege Escalation	Domain users group changed.	5	60160

5.5 Threat Hunting appliqué dans le lab

Le threat hunting consiste à rechercher activement des comportements anormaux à partir des événements collectés.

Dans ce projet, plusieurs recherches ont été effectuées à partir du dashboard Wazuh, notamment :

- Filtrage des tentatives SSH échouées sur Linux,
- Analyse des événements Windows de type échec de connexion (Event ID 4625),
- Suivi des créations de comptes utilisateurs et des ajouts aux groupes sensibles.

Ces recherches permettent d'identifier des menaces potentielles avant qu'elles ne provoquent un incident majeur.

Conclusion

Ce projet a permis de mettre en place une plateforme complète de supervision de la sécurité basée sur Wazuh et AWS.

Il illustre le fonctionnement d'un SOC moderne, intégrant SIEM et EDR pour la détection et l'analyse des menaces sur des environnements Linux et Windows.