

INSTALLATION DE WAZUH

Wazuh est une plateforme de sécurité qui offre une protection XDR et SIEM unifiée pour les terminaux et les charges de travail cloud. La solution se compose d'un agent universel unique et de trois composants centraux : le serveur Wazuh, l'indexeur Wazuh et le tableau de bord Wazuh.

Wazuh est gratuit et open source. Ses composants sont conformes à la Licence Publique Générale GNU, version 2 , et à la Licence Apache, version 2.0 (ALv2).

Exigence Matériel

Les exigences matérielles dépendent fortement du nombre de terminaux protégés et de charges de travail cloud. Ce nombre permet d'estimer la quantité de données à analyser et le nombre d'alertes de sécurité à stocker et indexer.

Le démarrage rapide implique le déploiement du serveur Wazuh, de l'indexeur Wazuh et du tableau de bord Wazuh sur le même hôte. Cela suffit généralement à surveiller jusqu'à 100 points de terminaison et à gérer 90 jours de données d'alerte indexées et interrogeables. Le tableau ci-dessous présente le matériel recommandé pour un déploiement rapide :

Agents	processeur	BÉLIER	Stockage (90 jours)
1–25	4 vCPU	8 Gio	50 Go
25–50	8 vCPU	8 Gio	100 Go
50–100	8 vCPU	8 Gio	200 Go

Pour les environnements plus vastes, nous recommandons un déploiement distribué. Une configuration de cluster multi-nœuds est disponible pour le serveur et l'indexeur Wazuh, offrant une haute disponibilité et un équilibrage de charge.

Système opérateur

Les composants centraux de Wazuh nécessitent un processeur Intel ou AMD Linux 64 bits (architecture x86_64/AMD64). Wazuh recommande l'une des versions de système d'exploitation suivantes :

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

L'installation de wazuh se fait en 3 principales étapes qui sont :

- **L'installation de l'indexeur wazuh,**
- **L'installation du serveur wazuh**
- **L'installation du tableau de bord wazuh.**

Pour installer wazuh, il faut s'assurer que la machine sur laquelle on souhaite l'installer répond aux exigences minimales en termes de système d'exploitation et de ressources système. Il existe plusieurs façons d'installer Wazuh :

Installation à partir des packages précompilés : Wazuh fournit des packages précompilés pour différents systèmes d'exploitation, tels que des packages DEB pour Ubuntu/Debian, des paquets MSI pour Windows, etc.

Installation à partir des sources : Si on souhaite personnaliser l'installation ou si vous utilisez un système d'exploitation pour lequel il n'y a pas de package précompilé disponible, on peut installer Wazuh à partir des sources.

Conteneurisation : Wazuh fournit des images Docker officielles qui peuvent être utilisées pour créer des conteneurs et les déployer facilement dans l'environnement si on utilise des conteneurs Docker ou Kubernetes.

Voici les étapes à suivre pour une installation à partir des ressources :

➤ **Installation de l'indexeur Wazuh :**

Installez et configurez l'indexeur Wazuh en cluster mono-nœud ou multi-nœuds en suivant les instructions étape par étape. L'indexeur Wazuh est un moteur de recherche en texte intégral hautement évolutif qui offre une sécurité avancée, des alertes, une gestion d'index, une analyse approfondie des performances et plusieurs autres fonctionnalités.

Le processus d'installation est divisé en trois étapes.

➤ **Création de certificats**

1. Téléchargez le **wazuh-certs-tool.sh** script et le config.yml fichier de configuration. Cela crée les certificats qui chiffrent les communications entre les composants centraux de Wazuh.

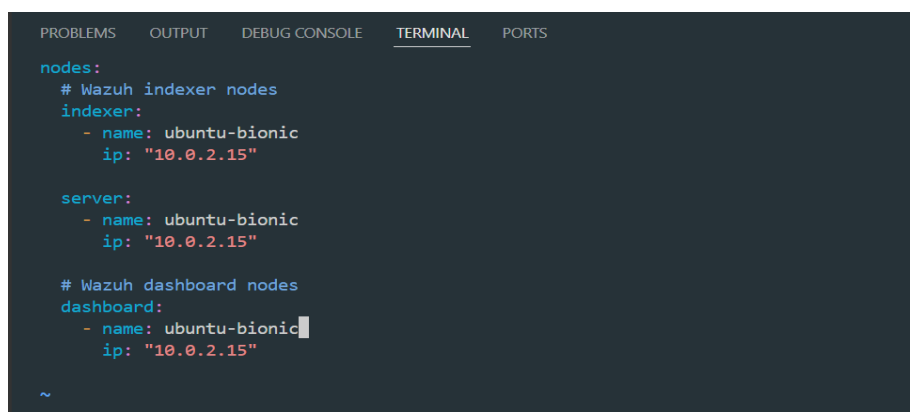
```
curl -sO https://packages.wazuh.com/4.11/wazuh-certs-tool.sh
```

```
curl -sO https://packages.wazuh.com/4.11/config.yml
```

```
vagrant@ubuntu-bionic:~$ sudo -i
root@ubuntu-bionic:~# curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
onfig.ymlroot@ubuntu-bionic:~# curl -sO https://packages.wazuh.com/4.11/config.yml
```

Image 1 : téléchargements des paquets d'installation

2. Modifiez config.yml et remplacez les noms et les adresses IP des nœuds par les noms et adresses IP correspondants. Cette opération est nécessaire pour tous les nœuds du serveur Wazuh, de l'indexeur Wazuh et du tableau de bord Wazuh. Ajoutez autant de champs de nœud que nécessaire. Dans notre cas nous avons utilisé un nœud



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

nodes:
# Wazuh indexer nodes
indexer:
- name: ubuntu-bionic
  ip: "10.0.2.15"

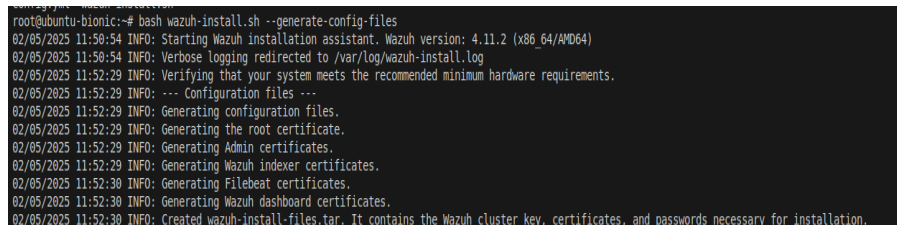
server:
- name: ubuntu-bionic
  ip: "10.0.2.15"

# Wazuh dashboard nodes
dashboard:
- name: ubuntu-bionic
  ip: "10.0.2.15"
```

Image2 : configuration des nœuds d'installations

3. Exécutez l'assistant d'installation de Wazuh avec l'option **--generate-config-files** permettant de générer la clé de cluster, les certificats et les mots de passe Wazuh nécessaires à l'installation. Vous trouverez ces fichiers dans ./wazuh-install-files.tar.

bash wazuh-install.sh --generate-config-files



```
root@ubuntu-bionic:~# bash wazuh-install.sh --generate-config-files
02/05/2025 11:58:54 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
02/05/2025 11:58:54 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/05/2025 11:52:29 INFO: Verifying that your system meets the recommended minimum hardware requirements.
02/05/2025 11:52:29 INFO: --- Configuration files ---
02/05/2025 11:52:29 INFO: Generating configuration files.
02/05/2025 11:52:29 INFO: Generating the root certificate.
02/05/2025 11:52:29 INFO: Generating Admin certificates.
02/05/2025 11:52:29 INFO: Generating Wazuh indexer certificates.
02/05/2025 11:52:30 INFO: Generating Filebeat certificates.
02/05/2025 11:52:30 INFO: Generating Wazuh dashboard certificates.
02/05/2025 11:52:30 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
```

Image3 : génération de la clé de cluster

4. Exécutez l'assistant d'installation de Wazuh avec l'option **--wazuh-indexer** et le nom du nœud pour installer et configurer l'indexeur Wazuh. Le nom du nœud doit être identique à celui utilisé lors **config.yml** de la configuration initiale.

Assurez-vous qu'une copie de **wazuh-install-files.tar**, créée lors de l'étape de configuration initiale, est placée dans votre répertoire de travail et dans notre cas nous avons exécuter **bash wazuh-install.sh --wazuh-indexer ubuntu-bionic**

```
root@ubuntu-bionic:~# bash wazuh-install.sh --wazuh-indexer ubuntu-bionic
02/05/2025 12:12:00 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
02/05/2025 12:12:00 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/05/2025 12:12:07 INFO: Verifying that your system meets the recommended minimum hardware requirements.
02/05/2025 12:12:16 INFO: Wazuh repository added.
02/05/2025 12:12:17 INFO: --- Wazuh indexer ---
02/05/2025 12:12:17 INFO: Starting Wazuh indexer installation.
02/05/2025 12:26:10 INFO: Wazuh indexer installation finished.
02/05/2025 12:26:10 INFO: Wazuh indexer post-install configuration finished.
02/05/2025 12:26:10 INFO: Starting service wazuh-indexer.
02/05/2025 12:26:31 INFO: wazuh-indexer service started.
02/05/2025 12:26:31 INFO: Initializing Wazuh indexer cluster security settings.
02/05/2025 12:26:33 INFO: Wazuh indexer cluster initialized.
02/05/2025 12:26:33 INFO: Installation finished.
```

Image4 : installation de l'indexeur wazuh

5. L'étape finale de l'installation du cluster à nœud unique ou à nœuds multiples de l'indexeur Wazuh consiste à exécuter le script d'administration de sécurité.

Exécutez l'assistant d'installation Wazuh avec l'option **--start-cluster** sur n'importe quel nœud d'indexation Wazuh pour charger les nouvelles informations de certificats et démarrer le cluster. **bash wazuh-install.sh --start-cluster**

6. Test de l'installation du cluster via la commande. Elle est exécutée pour obtenir le mot de passe de l'utilisateur

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P
""\admin\" -A 1
```

```
root@ubuntu-bionic:~# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\admin\" -A 1
indexer_username: 'admin'
indexer_password: 'MT3XTbsax3oI2fh+IVlllGJidv8AKWP8'
```

Image5: génération du nom utilisateur et du mot de passe

7. Exécuter la commande suivante pour confirmer la réussite de l'installation

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200
```

Bien évidemment remplacer ADMIN_PASSWORD par le mot de passe et WAZUH_INDEXER_IP par votre adresse IP.

```
root@ubuntu-bionic:~# curl -k -u admin:MT3XTbsax3oI2fh+IVlllGJidv8AKWP8 https://10.0.2.15:9200
{
  "name" : "ubuntu-bionic",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "mlaUrOmTe6rlin7IjVMNQ",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "e5a68d19815af94a9883fead7927edb40181f32d",
    "build_date" : "2025-03-26T19:08:40.098412Z",
    "build_snapshot" : false,
    "lucene version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Image6 : confirmation de réussite de l'installation

➤ Installation du serveur Wazuh :

Le serveur Wazuh analyse les données reçues des agents et déclenche des alertes lorsqu'il détecte des menaces et des anomalies. Ce composant central inclut le gestionnaire Wazuh et Filebeat.

Exécutez l'assistant d'installation de Wazuh avec l'option --wazuh-server suivie du nom du nœud pour installer le serveur Wazuh. Le nom du nœud doit être identique à celui utilisé lors config.yml de la configuration initiale.

```
bash wazuh-install.sh --wazuh-server ubuntu-focal
```

```

root@ubuntu-bionic:~# bash wazuh-install.sh --wazuh-server ubuntu-bionic
02/05/2025 12:35:25 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
02/05/2025 12:35:25 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/05/2025 12:35:34 INFO: Verifying that your system meets the recommended minimum hardware requirements.
02/05/2025 12:35:41 INFO: Wazuh repository added.
02/05/2025 12:35:41 INFO: --- Wazuh server ---
02/05/2025 12:35:41 INFO: Starting the Wazuh manager installation.
02/05/2025 12:46:39 INFO: Wazuh manager installation finished.
02/05/2025 12:46:39 INFO: Wazuh manager vulnerability detection configuration finished.
02/05/2025 12:46:39 INFO: Starting service wazuh-manager.
02/05/2025 12:47:05 INFO: wazuh-manager service started.
02/05/2025 12:47:05 INFO: Starting Filebeat installation.
02/05/2025 12:59:57 INFO: Filebeat installation finished.
02/05/2025 13:00:27 INFO: Filebeat post-install configuration finished.
02/05/2025 13:01:02 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
02/05/2025 13:01:58 INFO: Starting service filebeat.
02/05/2025 13:01:58 INFO: filebeat service started.
02/05/2025 13:01:58 INFO: Installation finished.

```

Image7: installation du serveur wazuh

➤ Installation du tableau de bord Wazuh :

Le tableau de bord Wazuh est une interface web flexible et intuitive permettant d'explorer et de visualiser les événements et archives de sécurité.

Exécutez l'assistant d'installation de Wazuh avec l'option `--wazuh-dashboard` et le nom du nœud pour installer et configurer le tableau de bord Wazuh. Le nom du nœud doit être identique à celui utilisé lors `config.yml` de la configuration initiale

```
bash wazuh-install.sh --wazuh-dashboard ubuntu-bionic
```

```

vagrant@ubuntu-focal:~$ sudo -i
root@ubuntu-focal:~# bash wazuh-install.sh --wazuh-dashboard ubuntu-focal
03/05/2025 02:46:50 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
03/05/2025 02:47:11 INFO: --- Wazuh dashboard ---
03/05/2025 02:47:11 INFO: Starting Wazuh dashboard installation.
03/05/2025 02:49:49 INFO: Wazuh dashboard installation finished.
03/05/2025 02:49:49 INFO: Wazuh dashboard post-install configuration finished.
03/05/2025 02:49:49 INFO: Starting service wazuh-dashboard.
03/05/2025 02:49:49 INFO: wazuh-dashboard service started.
03/05/2025 02:50:08 INFO: Initializing Wazuh dashboard web application.
03/05/2025 02:50:08 INFO: Wazuh dashboard web application initialized.
03/05/2025 02:50:08 INFO: --- Summary ---
03/05/2025 02:50:08 INFO: You can access the web interface https://10.0.2.15:443
    User: admin
    Password: Iv?cgby3Trr51QcFJFvf3auMyNHGW00d
03/05/2025 02:50:08 INFO: Installation finished.

```

Image8 : installation du Dashboard wazuh

Accédez à l'interface web de Wazuh avec vos **admin** identifiants utilisateur. Il s'agit du compte administrateur par défaut de l'indexeur Wazuh et il vous permet d'accéder au tableau de bord Wazuh.

URL: https://<**WAZUH_DASHBOARD_IP_ADDRESS**>

Nom d'utilisateur : admin

Mot de passe : <**ADMIN_PASSWORD**>

Lorsque vous accédez au tableau de bord Wazuh pour la première fois, le navigateur affiche un message d'avertissement indiquant que le certificat n'a pas été émis par une autorité de confiance. Une exception peut être ajoutée dans les options avancées du navigateur. Pour plus de sécurité, le **root-ca.pem** fichier précédemment généré peut être importé dans le gestionnaire de certificats du navigateur. Il est également possible de configurer un certificat provenant d'une autorité de confiance.

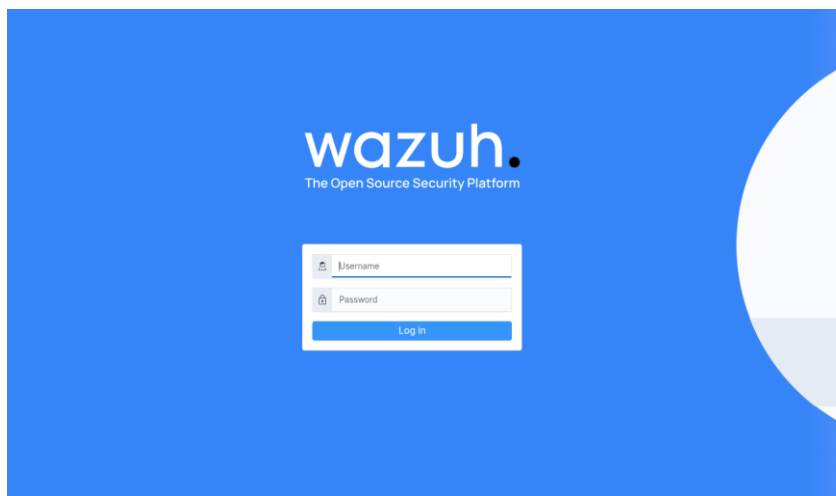


Image9 : page de connexion de wazuh

Après une authentification réussie nous obtenons un Dashboard comme suit :

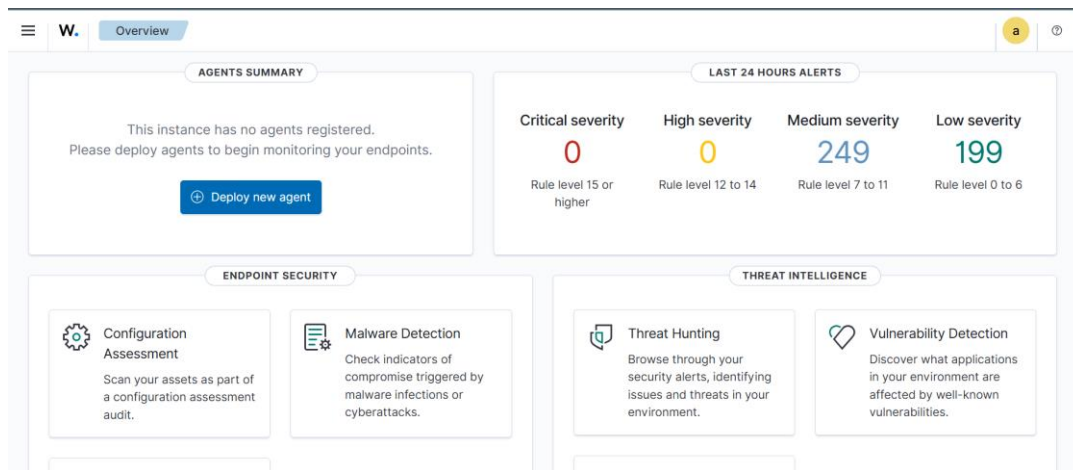


Image10 : tableau de bord de wazuh

LANCEMENT D'UN AGENT WAZUH

L'agent Wazuh est multiplateforme et s'exécute sur les terminaux que l'utilisateur souhaite surveiller. Il communique avec le serveur Wazuh et envoie des données en temps quasi réel via un canal chiffré et authentifié.

L'agent a été développé pour répondre à la nécessité de surveiller une grande variété de terminaux sans impacter leurs performances. Il est compatible avec les systèmes d'exploitation les plus courants et nécessite en moyenne 35 Mo de RAM.

L'agent Wazuh fournit des fonctionnalités clés pour améliorer la sécurité de votre système.

Collecteur de journaux	Exécution de la commande
Surveillance de l'intégrité des fichiers (FIM)	Évaluation de la configuration de sécurité (SCA)
Inventaire du système	Détection de logiciels malveillants
Réponse active	Sécurité des conteneurs
Sécurité du cloud	

L'installation de l'agent Wazuh dépend du système d'exploitation et pour chaque système il y'a une méthode définie pour cela.

Dans notre cas nous l'avons déployé sur des terminaux linux

➤ **Déploiement d'agents Wazuh sur des terminaux linux**

L'agent s'exécute sur l'hôte que vous souhaitez surveiller et communique avec le serveur Wazuh, envoyant des données en temps quasi réel via un canal crypté et authentifié. Le déploiement d'un agent Wazuh sur un système Linux utilise des variables de déploiement qui facilitent l'installation, l'enregistrement et la configuration de l'agent.

Dans notre cas nous allons configurer une machine Windows comme un agent wazuh

- Choisir le système sur lequel on veut déployer l'agent wazuh (Dans notre cas Windows)

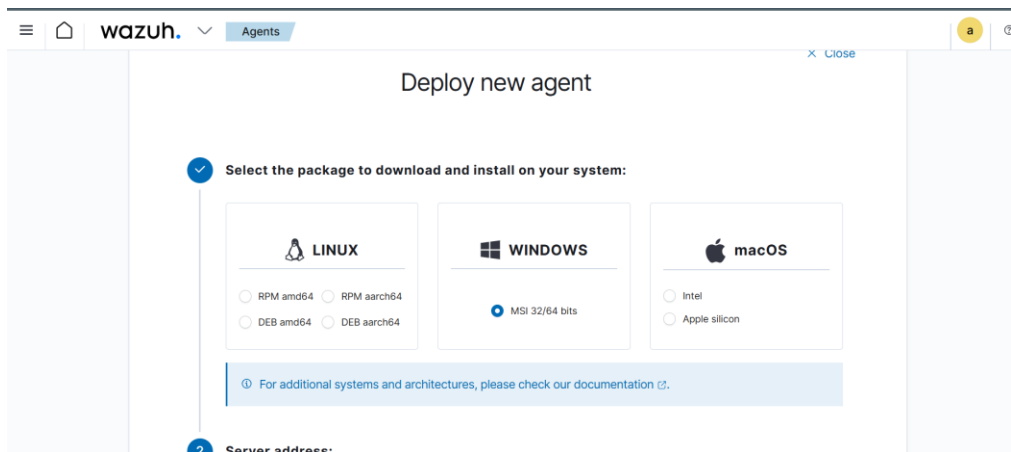


Image11 : choix du système pour le lancement de l'agent

- Renseigner l'adresse IP sur serveur wazuh (qui doit être dans le même réseau que celui de l'adresse IP de l'agent) et ensuite renseigner l'host Name de la machine qui joue le rôle d'agent et choisir le groupe (Optionnel)

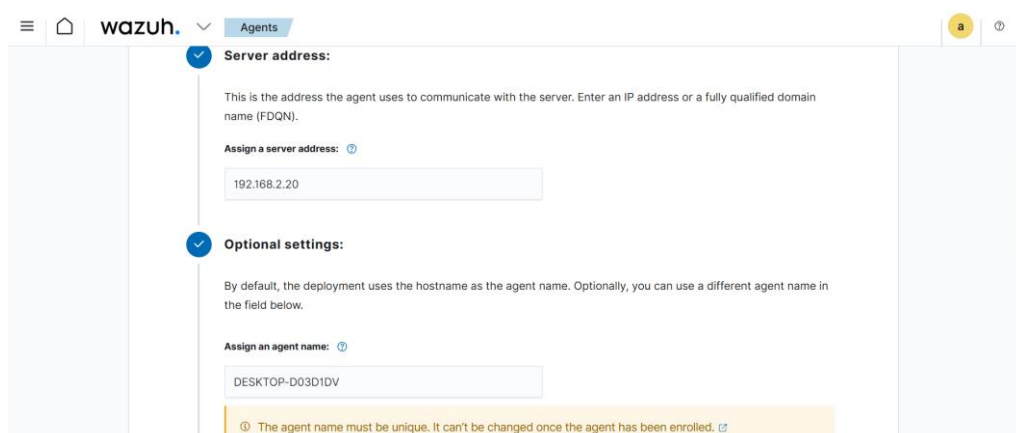


Image12 : configuration des adresses IP et des host Name

- Une commande sera générée automatiquement et une fois exécuter dans le terminal de la machine Windows l'agent sera configurer et s'affichera dans le serveur wazuh

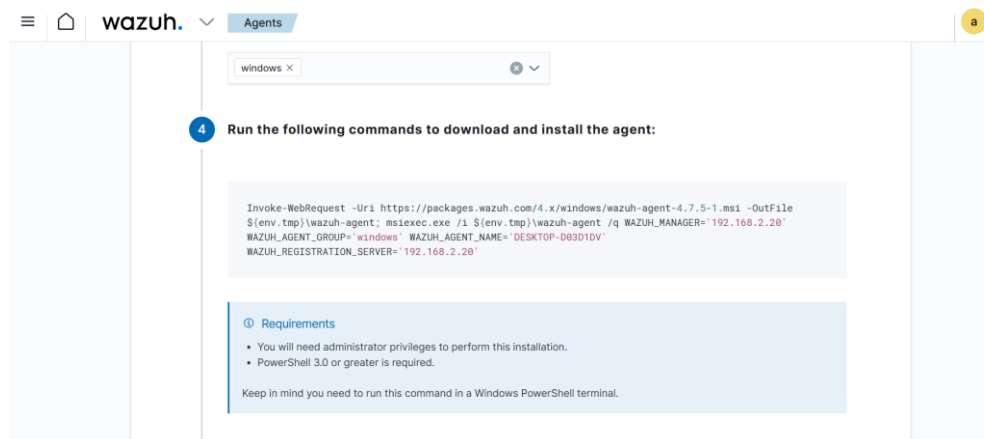


Image13 : génération de la commande

```
PS C:\Users\DELL> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $env:tmp\wazuh-agent; msexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.2.20' WAZUH_AGENT_GROUP='windows' WAZUH_AGENT_NAME='DESKTOP-D03D1DV' WAZUH_REGISTRATION_SERVER='192.168.2.20'
PS C:\Users\DELL> NET START WazuhSvc
Le service demandé a déjà été démarré.

Vous obtiendrez une aide supplémentaire en entrant NET HELPMSG 2182.
PS C:\Users\DELL>
```

Image14 : lancement de l'agent wazuh sur Windows

- Lancer l'agent WAZUH grâce à la commande **NET START WazuhSvc**

Après une exécution correcte de ces étapes nous pourrions voir l'agent wazuh Windows apparaitre et être opérationnel dans notre serveur wazuh

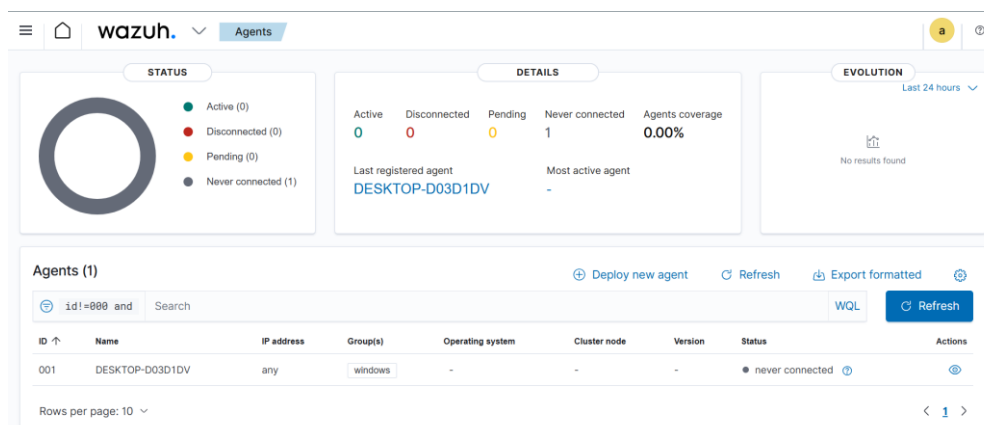


Image14 : présentation de l'agent wazuh