

Rapport de stage

Abderrahim Khantouch

BTS SIO 1^{ère} Année



27/05/24 – 29/06/24
Nougaro

Lycée Claude

Contexte

Dans le cadre réglementaire de mon stage de 1^{ère} année de BTS SIO option SLAM, j'ai passé cinq semaines de stage à l'entreprise 3R à Montauban, du 27 mai au 28 juin 2024.

Les objectifs qui m'ont été assignés pendant ces cinq semaines ont été le déploiement, la compréhension et la documentation de l'outil de cybersécurité, Wazuh.

Pendant cinq semaines, j'ai essayé de maîtriser cet outil et transmettre mes connaissances à travers la documentation que j'ai rédigée, afin que l'outil soit déployé à grande échelle dans tout le parc réseau de l'entreprise par mon tuteur de stage et par le responsable informatique de l'entreprise.

Ce rapport de stage condense les difficultés et les accomplissements que j'ai pu expérimenter pendant mon stage, le but étant de résumer mon expérience de la manière la plus limpide possible.

Description de l'entreprise

Nom : 3R

Statut : SAS

Activité : Vente de machine d'essais

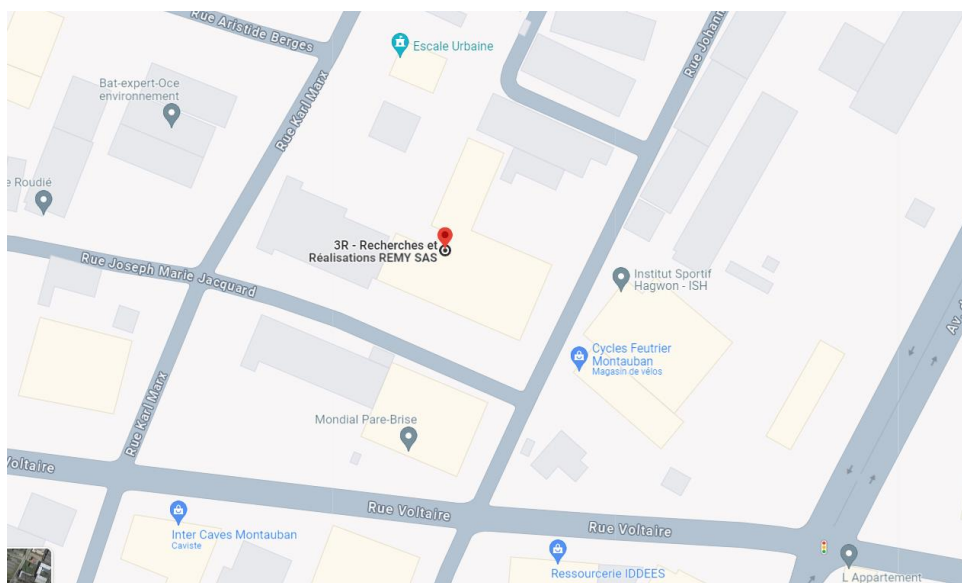
Nombre de salariés :

Horaire de travail :

- 8h – 12h00 | 13h00 – 17h00
Du lundi au vendredi

Adresse de l'entreprise :

1 Rue Joseph Marie Jacquard, 82000 Montauban



Clients de l'entreprise :

Les entreprises du BTP et les établissements scolaires

Rayon d'action de l'entreprise :

Portée Nationale

Conditions de réalisation

Horaires de travail personnel :

- 8h – 12h00 | 13h00 – 17h00

Du lundi au jeudi

- 8h – 11h00

Vendredi

Objectifs :

- Déployer Wazuh sur un serveur et sur des hôtes pour pouvoir le tester
- Tester Wazuh avec des tests de base pour voir les alertes que cela déclenche
- Ecrire une documentation qui retrace tous ce que j'ai fait pour que les deux étapes précédentes s'accomplissent correctement

Environnement de travail :

Pour pouvoir faire tout ça, j'ai bénéficié d'un environnement de travail avec un serveur de test, qui m'a permis de simuler les tests qui se feront plus tard lorsque ma documentation sera utilisée par l'entreprise.

Limitations :

Pour le côté limitation, je ne pouvais pas avoir accès à Internet via toutes les VM que j'ai utilisé pour installer le serveur Wazuh et les agents, ce qui fait que j'ai dû souvent jongler entre la désactivation d'Internet et la réactivation d'Internet sur certaines VM pour pouvoir installer des paquets et en même temps détecter les autres hôtes.

La raison étant que, d'après le responsable informatique de l'entreprise et mon tuteur, utiliser sur une VM le réseau Internet de l'entreprise sans qu'ils ne me donnent l'autorisation de le faire peut créer un doublon d'adresses IP totalement identique à une autre sur le réseau.

Créant des dysfonctionnements plus ou moins susceptibles de parasiter le réseau.

Et je ne pouvais pas avoir un suivi en profondeur de mes travaux puisque mon tuteur me laissait la plupart du temps en grande autonomie, ce qui fait que certaines notions ont peut-être pu m'échapper au vu de mon expérience dans le secteur de la cybersécurité.

Outils

Serveur de test (accès à Internet) :

- Gestionnaire Hyper-V
 - VM Ubuntu
 - VM Amazon Linux 2
 - VM Windows
 - VM Kali Linux
- VirtualBox
- Disque dur

Poste de travail :

- Word
- Google
 - Documentation Wazuh

Gestionnaire Hyper-V :

Technologie Microsoft qui permet de créer des environnements informatiques virtuels, un équivalent de VirtualBox ou VMWare.

Serveur Wazuh :

Un serveur qui s'occupe de recevoir tous les événements envoyés par un agent, afin que les données des événements soient consultables depuis l'API de Wazuh (ex : un échec d'authentification).

Agent Wazuh :

Un outil qui, lorsqu'il est installé dans un système d'exploitation, envoie tous les événements qui se déroulent sur sa machine au serveur Wazuh.

Installation et Déploiement de Wazuh

Serveur Wazuh

Pour commencer le déploiement de Wazuh, il faut choisir comment installer le serveur Wazuh sur l'une des VM et sur quelle VM.

Mais avant de faire ce choix, j'ai dû créer avec Hyper-V les VM qui me permettront d'installer le serveur Wazuh et les différents agents.

Une fois fait, voici ce que cela donne.

Nom	État
3RU0VIRWDOM02 - 2024...	Désactivé
Kali-Linux	Désactivé
Linux_Agent	Désactivé
vmsylob	Désactivé
WazuhServ	Désactivé

Seule la VM WazuhServ avait un accès direct à Internet, ce qui fait que c'est avec cette VM que j'ai décidé d'y mettre le serveur Wazuh.

Pour ce faire, avec le conseil de mon tuteur de stage, j'ai décidé d'installer le serveur Wazuh avec un fichier .ova qui contient tous les composants du serveur (plus communément appelé une appliance).

Depuis le site de Wazuh, j'ai installé le fichier avec mon serveur de test

Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. This can be directly imported to VirtualBox or other OVA compatible virtualization systems. Take into account that this VM only runs on 64-bit systems. It does not provide high availability and scalability out of the box. However, these can be implemented by using [distributed deployment](#).

Download the [virtual appliance \(OVA\)](#), which contains the following components:

- Amazon Linux 2
- Wazuh manager 4.8.0
- Wazuh indexer 4.8.0
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.8.0

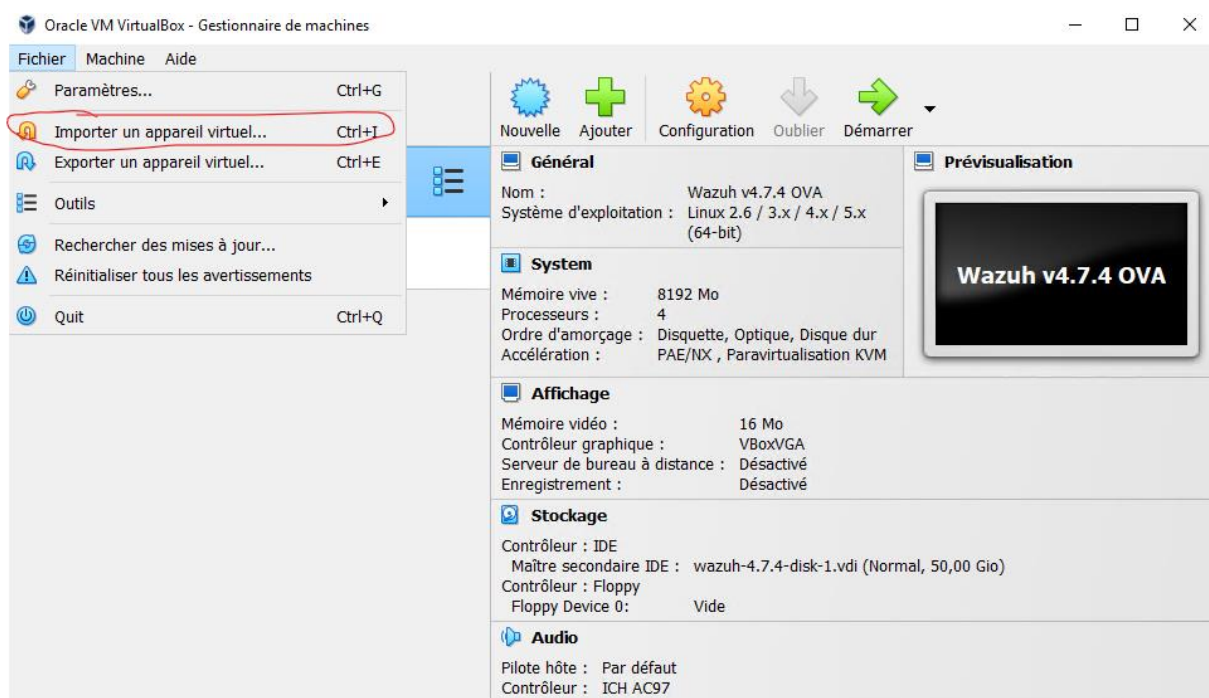
J'ai ensuite installé VirtualBox pour pouvoir convertir le fichier en vhd, afin qu'il soit importable sur Hyper-V.

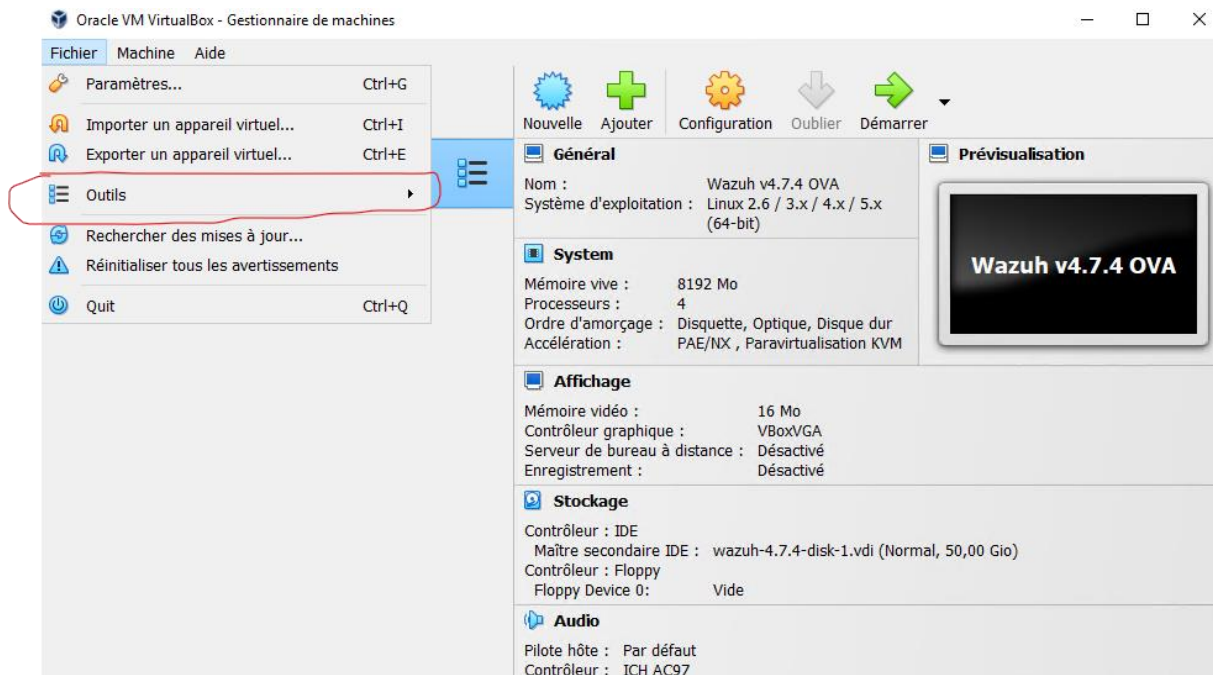
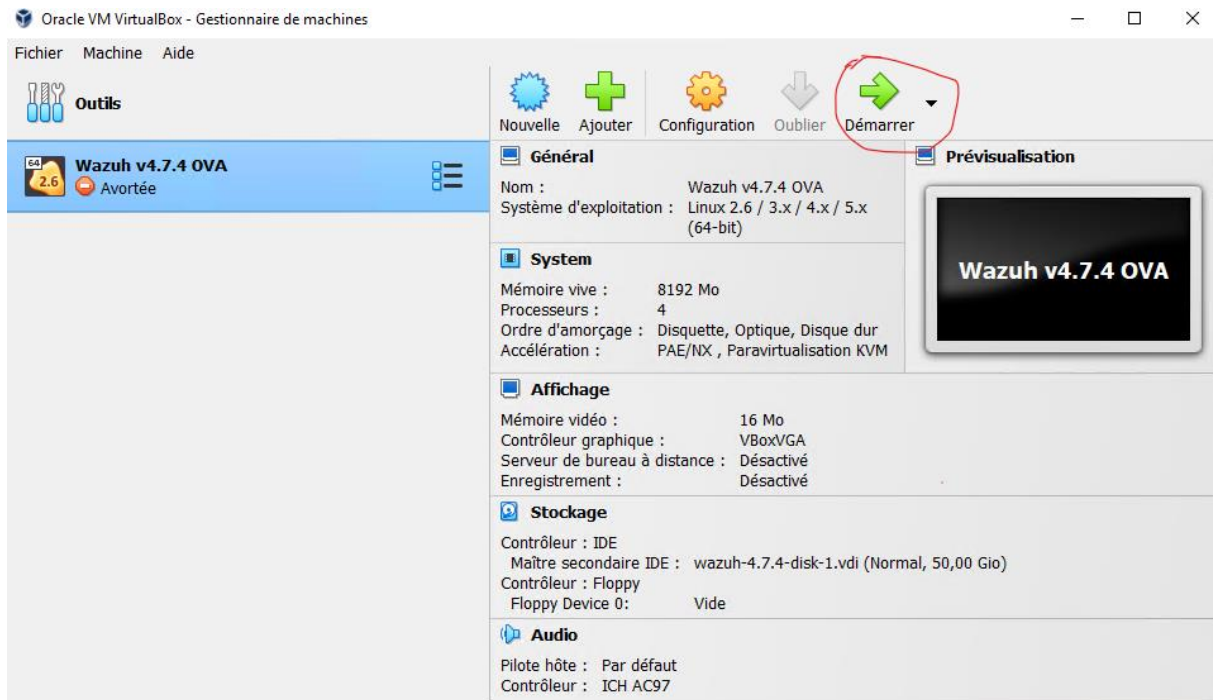
Dès que ça été fait, j'ai suivi les instructions dans un site web que voici, pour que je puisse convertir le fichier ova en vhd.

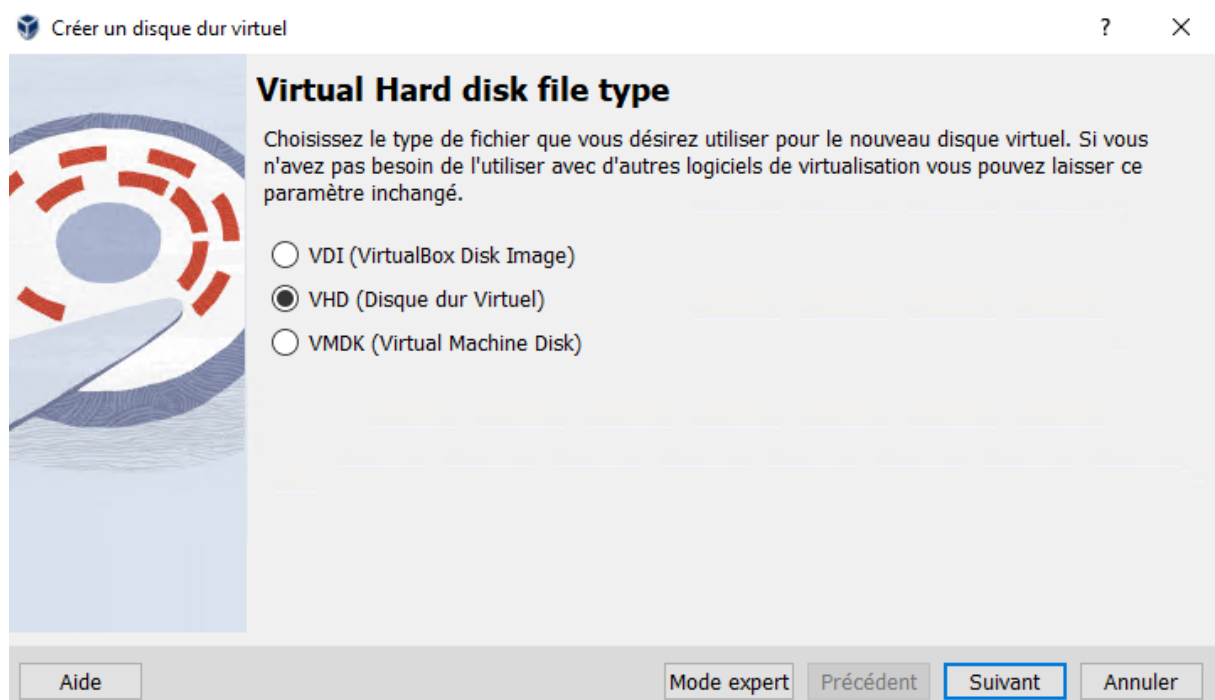
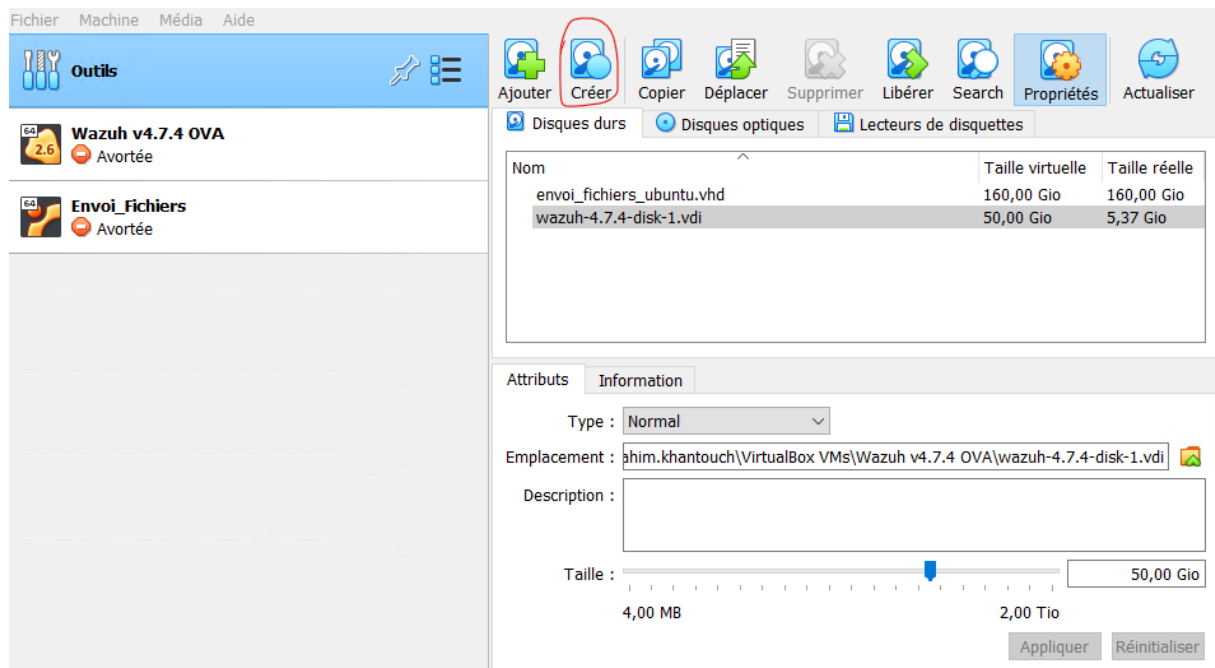
<https://akril.net/convertir-le-disque-dur-virtuel-dune-vm-virtualbox-de-vdi-vers-vhd-ou-vhdx-pour-hyper-v/>

Dans l'ordre j'ai importé le fichier dans VirtualBox puis j'ai démarré la VM nouvellement créé.

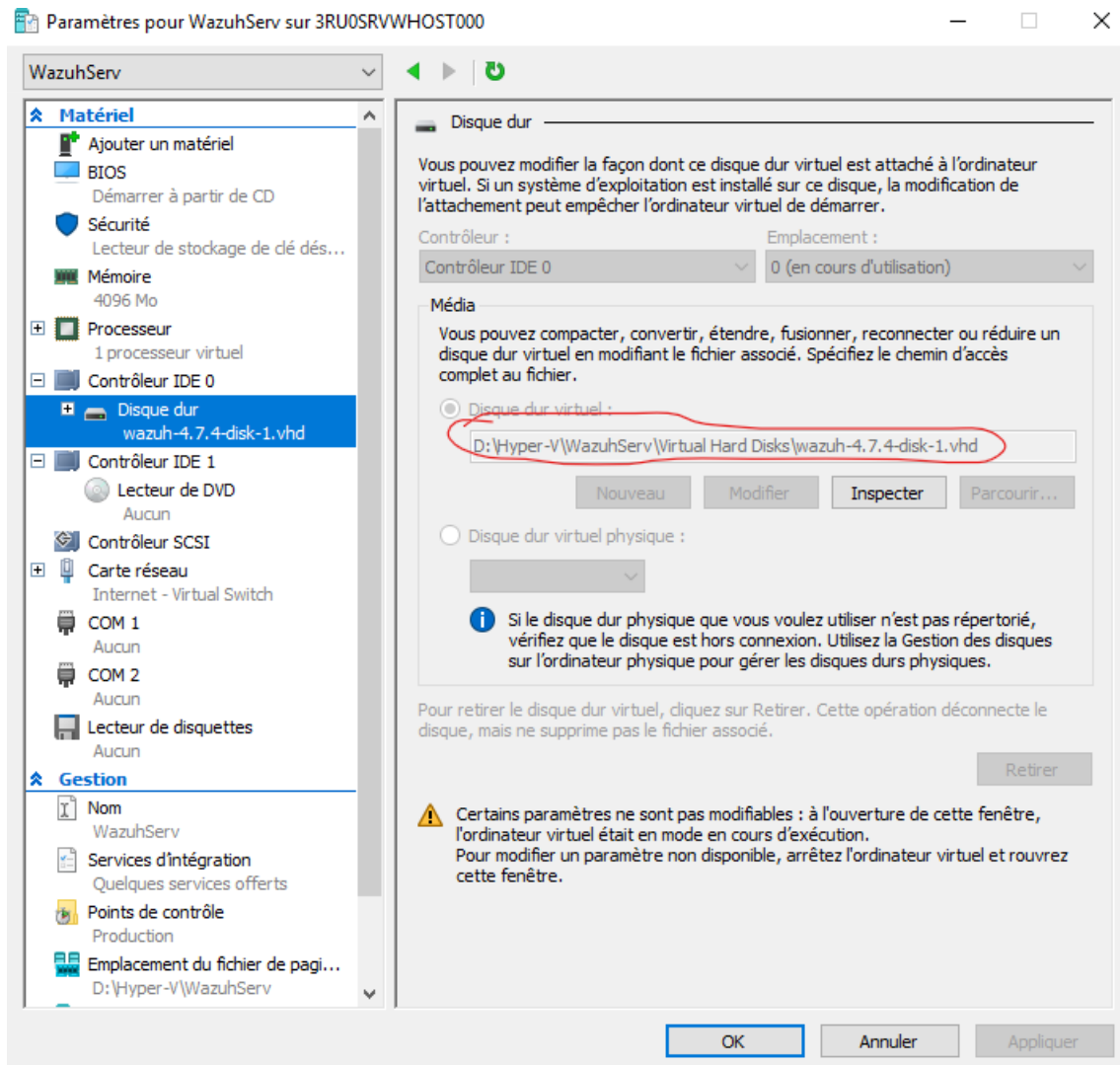
Ensuite, je suis allé dans Outils puis dans Gestionnaire de médias Virtuels pour convertir le fichier cette fois transformé en fichier .vdi en fichier .vhd



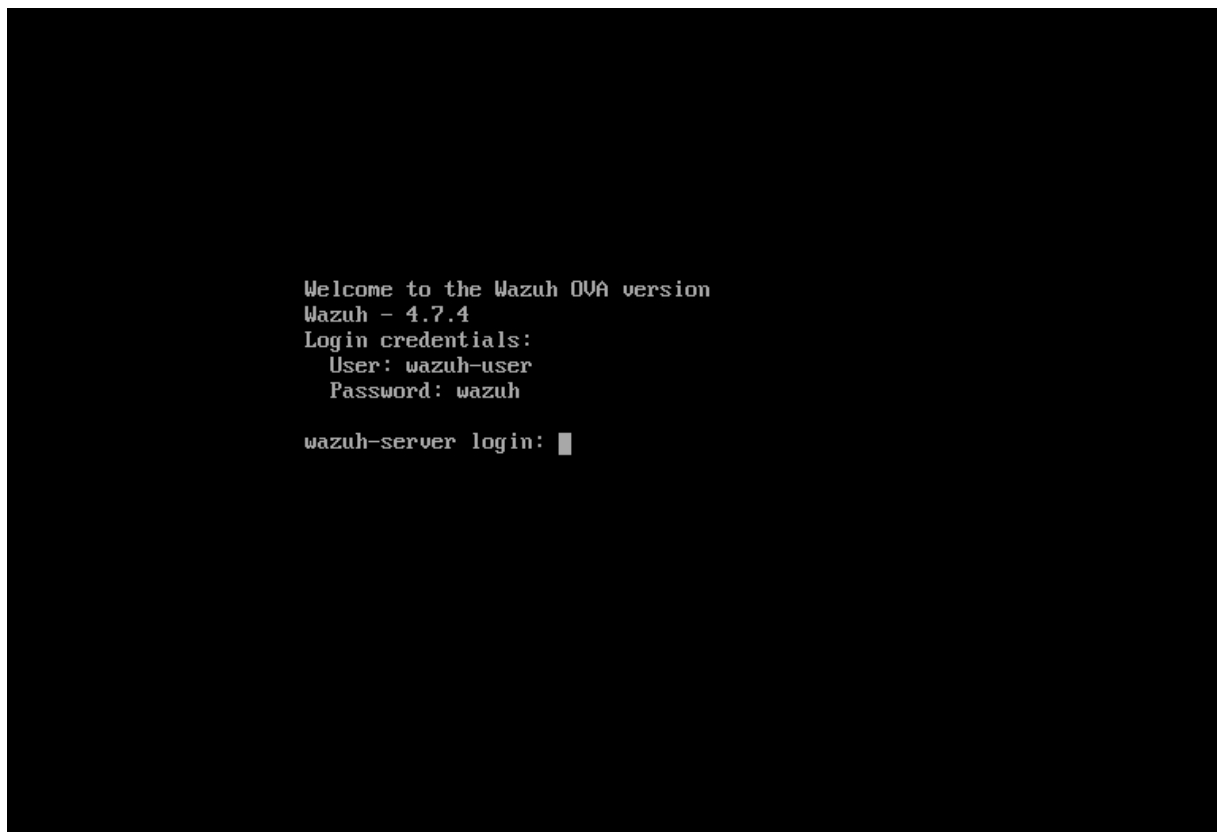




J'ai ensuite importé le fichier créé dans les paramètres de la VM WazuhServ.



Une fois fini, en démarrant la VM j'ai pu confirmer que l'installation s'est bien passé avec l'affichage suivant.

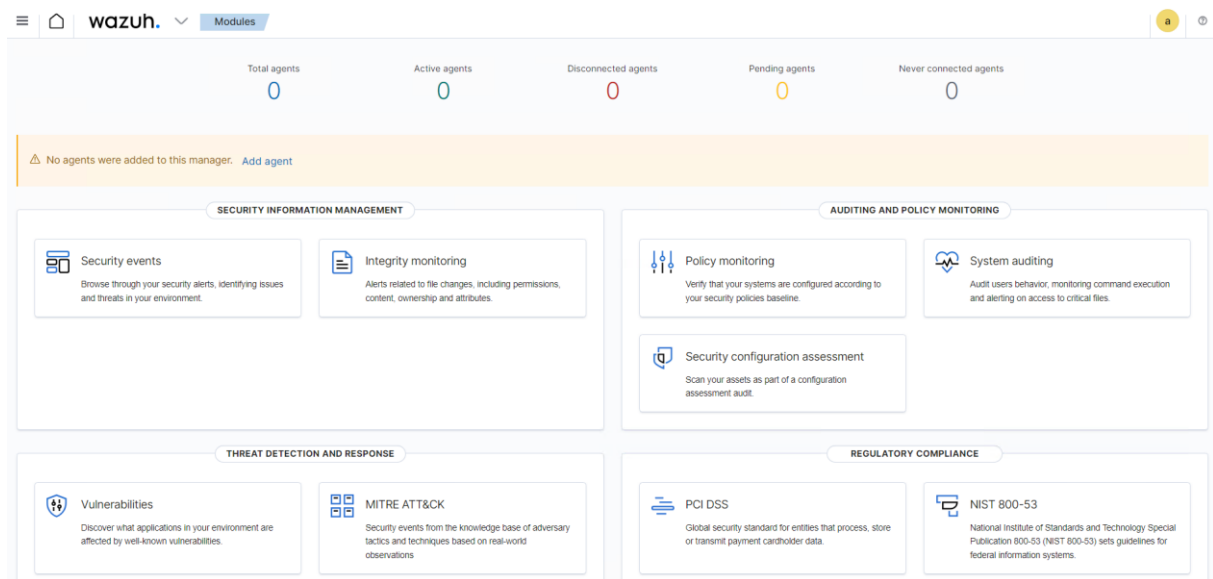


Voilà, le serveur Wazuh est mis en place.

L'appliance Wazuh a automatiquement fait en sorte que le système d'exploitation soit Linux et que le distro soit Amazon Linux 2, ça veut dire donc que si je veux voir l'API de Wazuh directement, j'ai besoin de le faire sur une autre VM en me connectant sur le même réseau interne que le serveur Wazuh ou le faire depuis le serveur de test.

Ce que j'ai fait, c'est taper dans le navigateur Internet de mon serveur de test, l'adresse IP du serveur pour afficher l'API.





Maintenant que c'est fini, il ne me manquait plus qu'à ajouter des agents pour que le serveur Wazuh commence à montrer des évènements.

Installation des agents

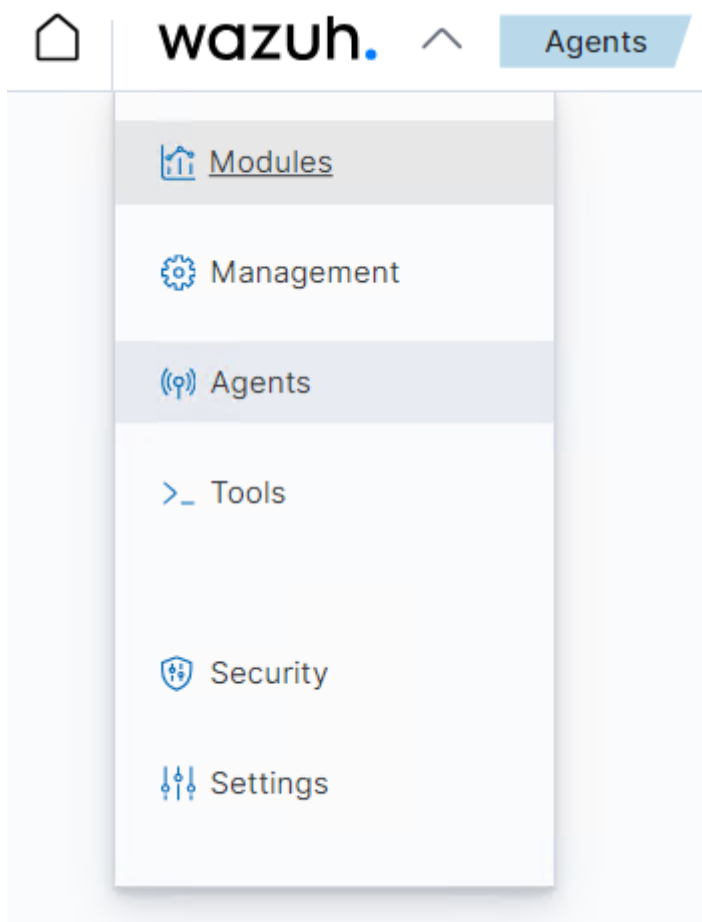
Ubuntu

En Hors Ligne (réseau privé) :

Mise en exécution impossible


Connecté à Internet (réseau Ethernet) :

Pour le coup c'est assez simple, il suffit d'aller dans la partie Agent de Wazuh




✓


Select the package to download and install on your system:

 **LINUX**

☐ RPM amd64 ☐ RPM aarch64
☒ DEB amd64 ☐ DEB aarch64

 **WINDOWS**

☐ MSI 32/64 bits

 **macOS**

☐ Intel
☐ Apple silicon

🔗

For additional systems and architectures, please check our documentation [🔗](#).

✓

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: ?

192.168.1.27

✓

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: ?

Cliquez sur Deb amd64, renseignez l'adresse IP du serveur Wazuh, renseignez le nom qu'aura l'agent de votre distribution Linux, sélectionnez le filtre Default en appuyant sur l'option Groupes existants

Assign an agent name: ?

Test

ⓘ

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

Select one or more existing groups: ?

Default

4

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_4.7.4-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.1.27' WAZUH_AGENT_NAME='Test' dpkg -i ./wazuh-agent_4.7.4-1_amd64.deb
```

ⓘ 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.

5

Start the agent:

Quand c'est fait, il suffit de copier/coller le script généré par Wazuh et les scripts de lancement de l'agent dans votre terminal Ubuntu pour que l'agent se mette en place

Il y' a d'autres méthodes pour pouvoir installer l'agent mais celle-là est de très loin la plus rapide et la plus simple d'exécution

Windows

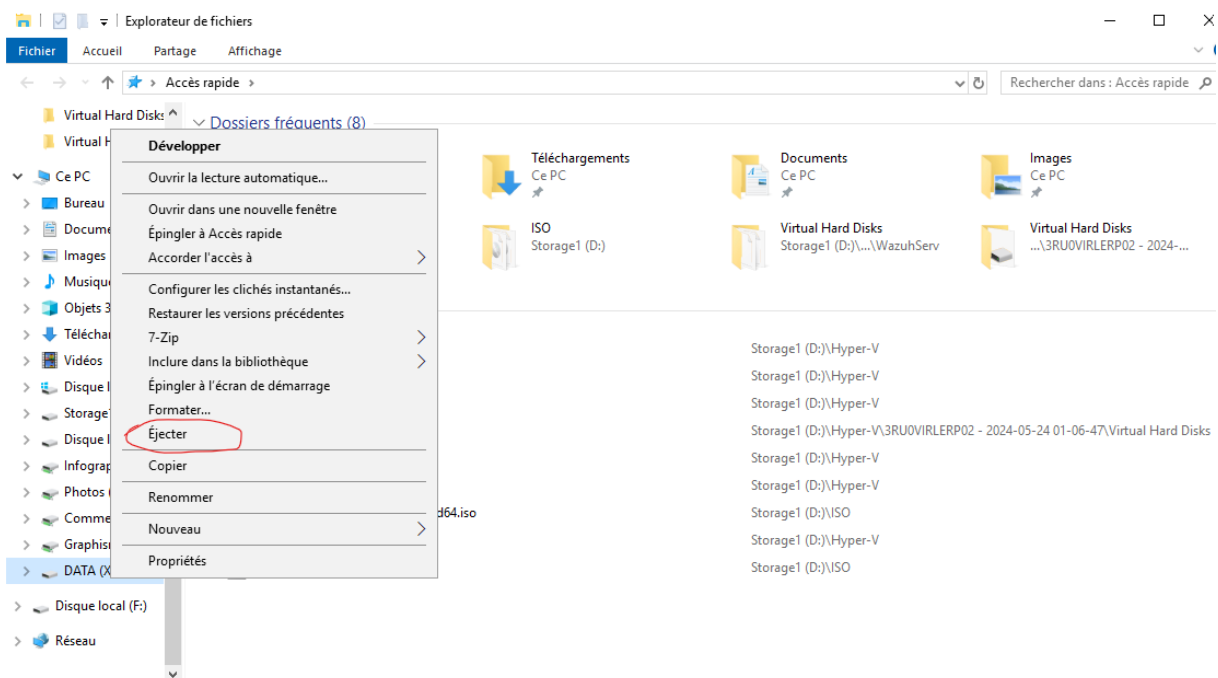
Hors Ligne :

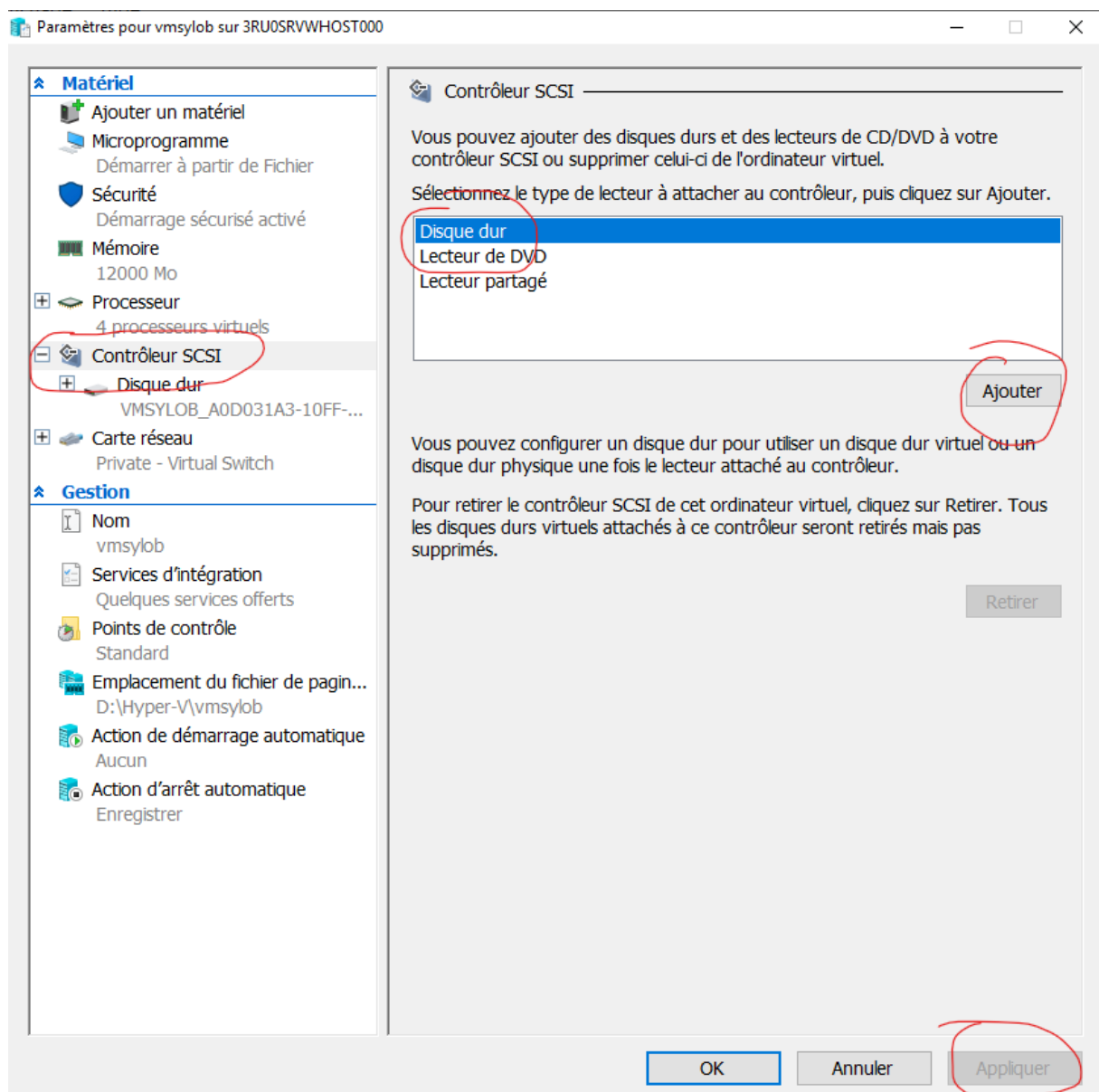
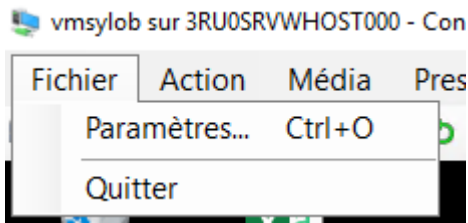
Cette méthode d'installation est tout aussi rapide et efficace que la précédente

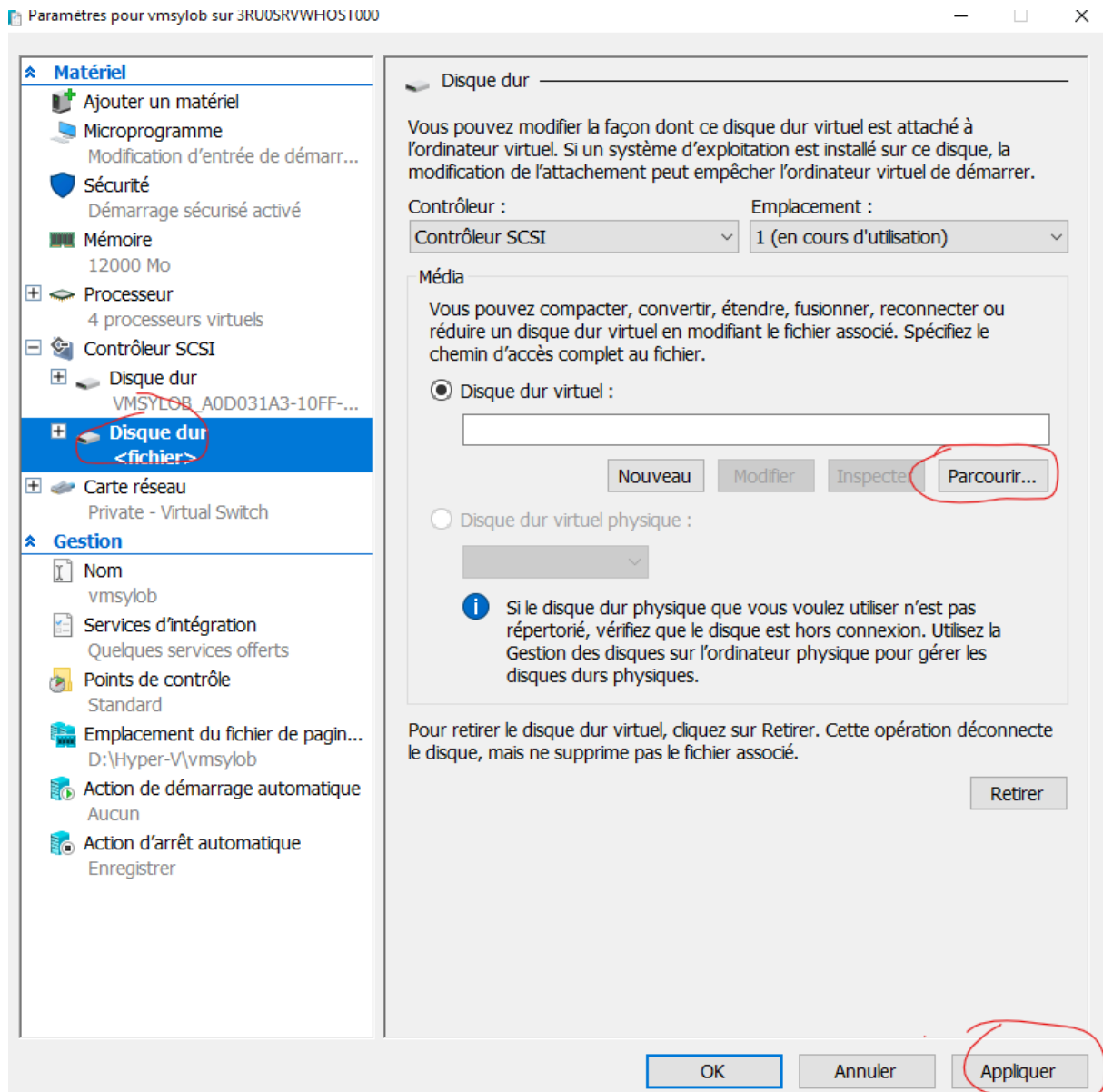
Vous téléchargez depuis la documentation Wazuh le package d'installation de l'agent Windows et vous le transférez sur un disque

- <https://documentationwazuh.com/current/installation-guide/packages-list.html>

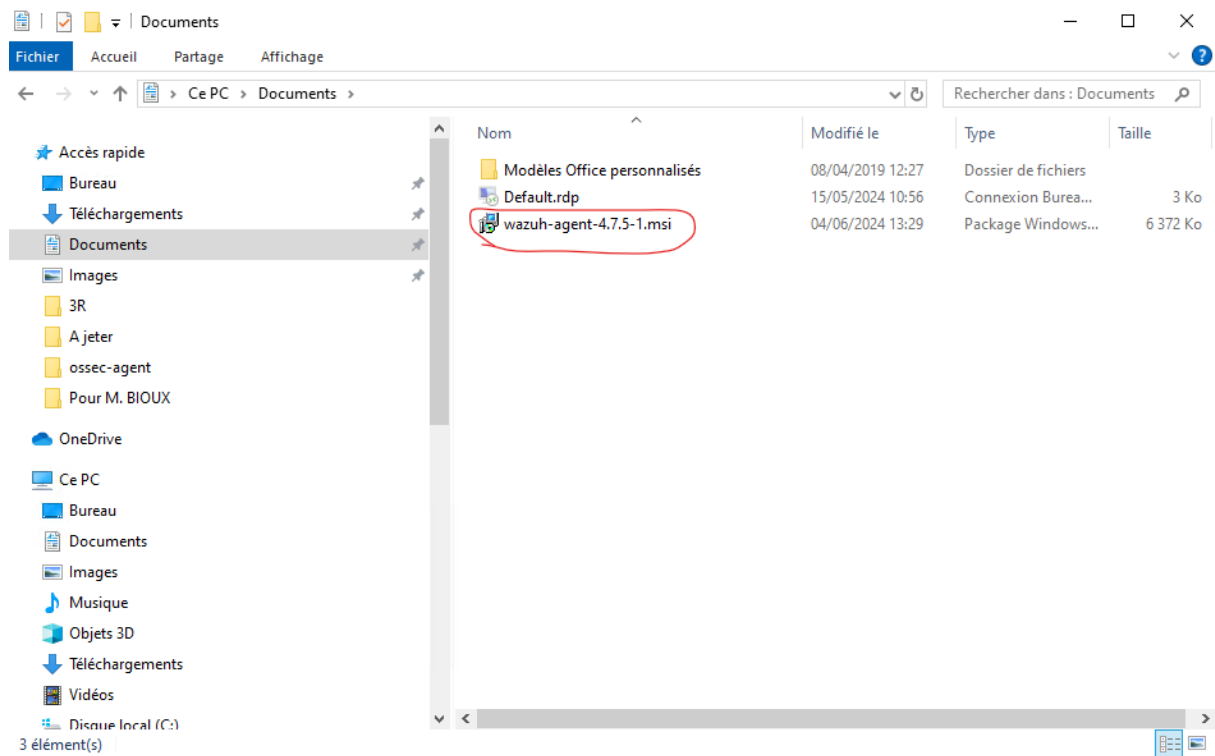
Il faudra ensuite Ejecter le disque pour qu'il puisse être utilisé dans la VM Windows (Si l'option n'apparaît pas, c'est soit parce que le disque n'est pas monté ou que vous ne l'avez pas sélectionné depuis la barre du Menu Rapide, je vous invite à faire un clic droit au même type d'emplacement que dans l'image ci-dessous)





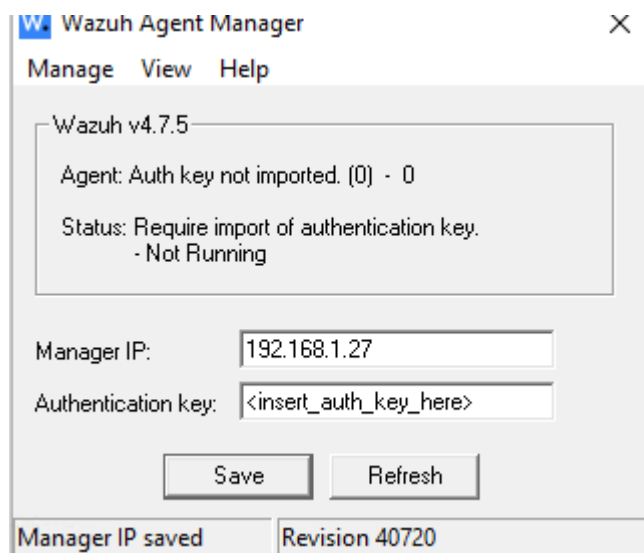


Après que le disque a bien été implémenté, plus qu'à utiliser le fichier d'installation dans la VM Windows



Cliquez dessus dès qu'il est présent dans votre VM

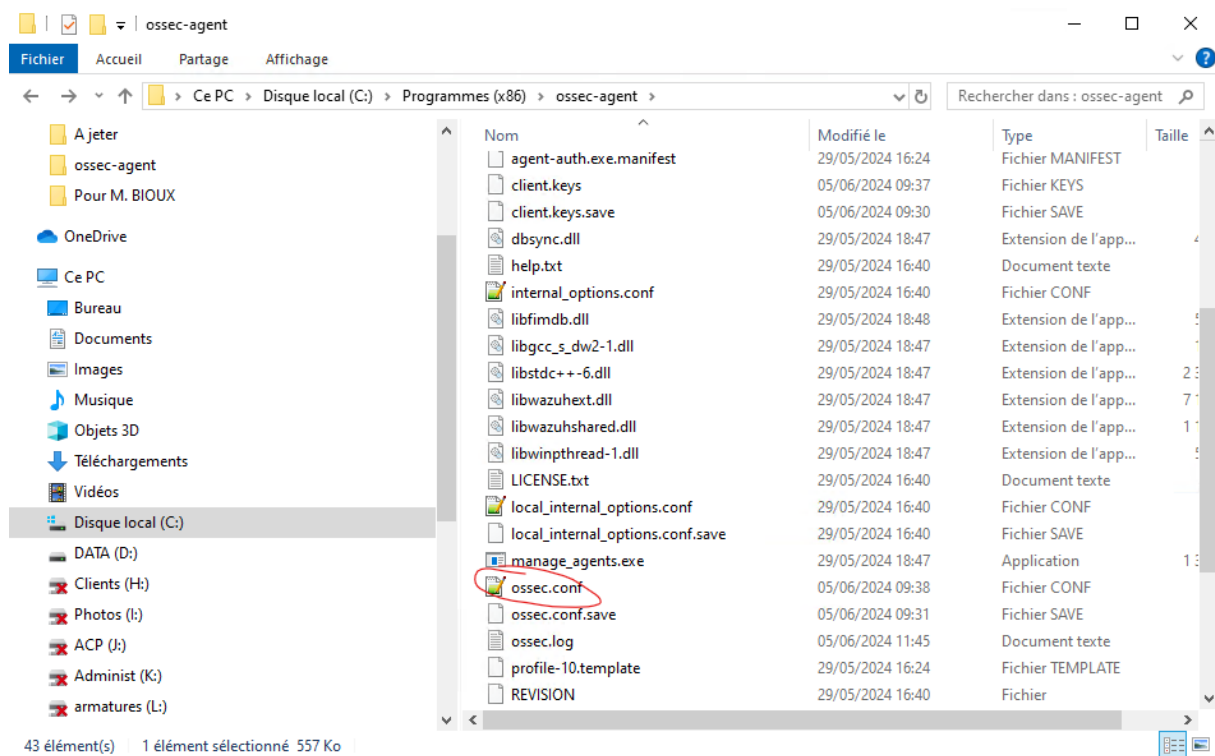
Vous vous retrouverez ensuite sur le launcher de l'agent Wazuh, il faudra cocher l'option Run Agent Configuration Interface et renseigner ensuite l'adresse IP du serveur Wazuh sans mettre la clé d'authentification



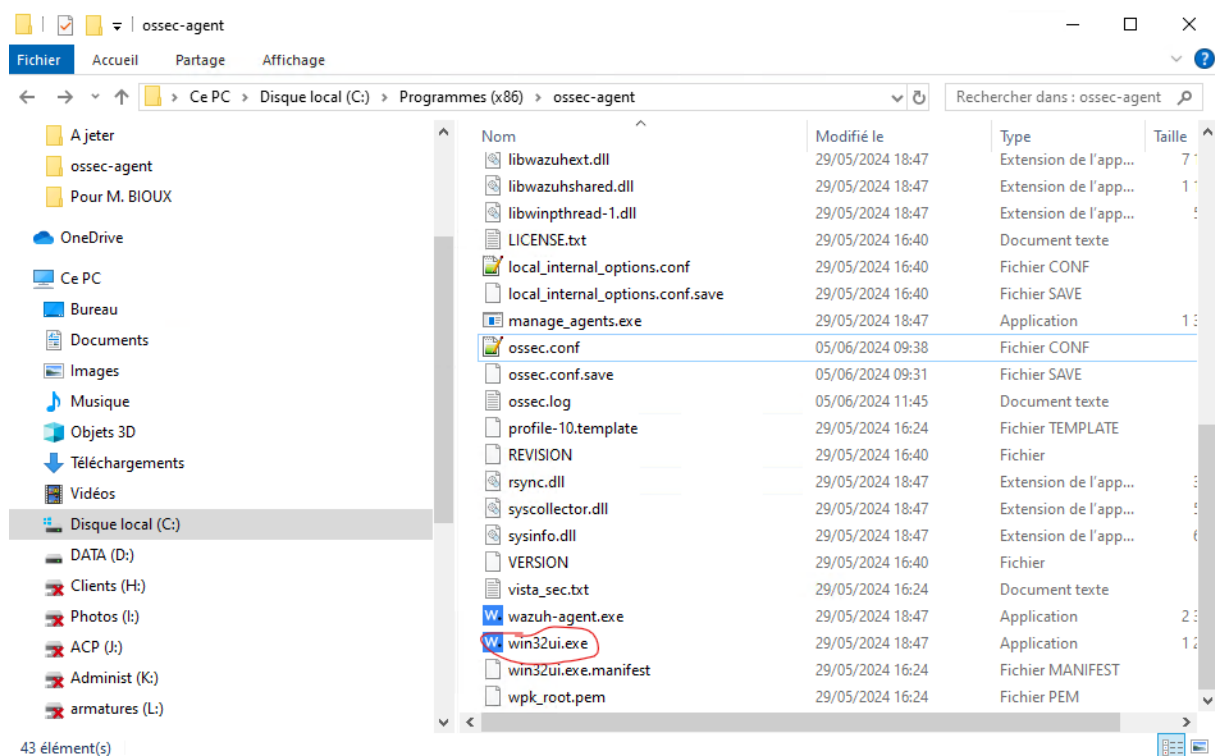
Cliquez sur Save, sur Manage, Start et c'est fini pour la partie installation

Si vous n'avez pas coché l'option Run Agent Configuration Interface, vous pouvez soit aller renseigner l'adresse IP du serveur dans le fichier ossecconf entre ces balises <address> </address>

C:\Program Files (86)\ossec-agent

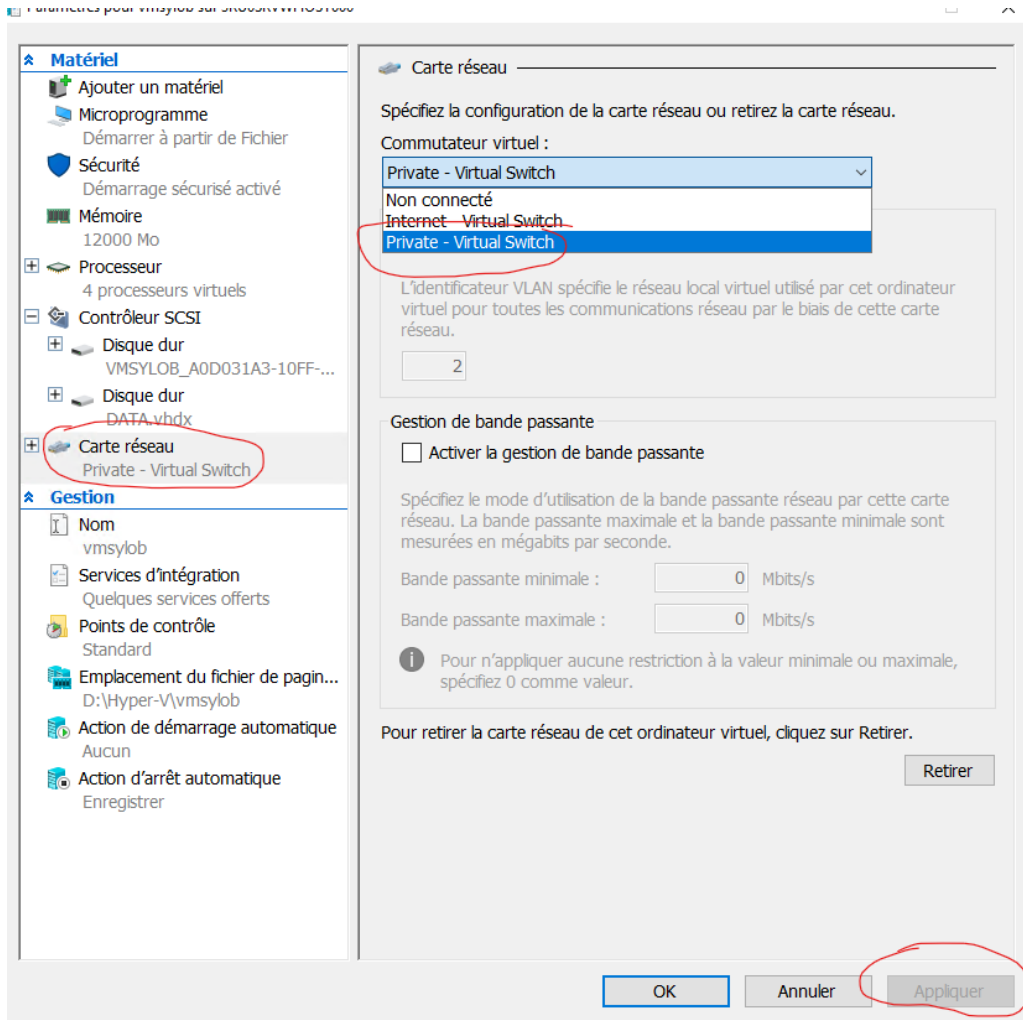


Ou vous pouvez cliquer sur le fichier win32uiexe qui est ici dans le même dossier



Ensuite, pour que l'agent Windows soit reconnu, il faut connecter le serveur Wazuh et la VM Windows vers le même switch dans les paramètres pour qu'ils soient dans le même réseau privé


Dans les deux parties, vous faites la même chose





Ensuite vous attendez quelques secondes, le temps que l'agent soit reconnu par le serveur, dès que c'est fini vous pourrez refaire basculer le serveur Wazuh vers le switch connecté au réseau Ethernet

Connecté au réseau Ethernet :

Il suffit de refaire la même manipulation que pour l'agent sur Ubuntu, en cochant cette fois l'option MSI 32/64 bits

**LINUX**
☐ RPM amd64 ☐ RPM aarch64
☐ DEB amd64 ☐ DEB aarch64

**WINDOWS**
☒ MSI 32/64 bits

**macOS**
☐ Intel
☐ Apple silicon

[① For additional systems and architectures, please check our documentation.](#)

2

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: [?](#)

Server address

3

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: [?](#)

Agent name

Il suffit ensuite de copier les deux requêtes générées grâce au nom de l'agent, à l'adresse IP du serveur Wazuh et le filtre Default tout comme pour l'agent Ubuntu

Pour exécuter les requêtes, utilisez au choix Powershell ou cmd en mode administrateur