Tutoriel Installation SIEM Wazuh sur Docker

Tutoriel par Samuel Desbiens

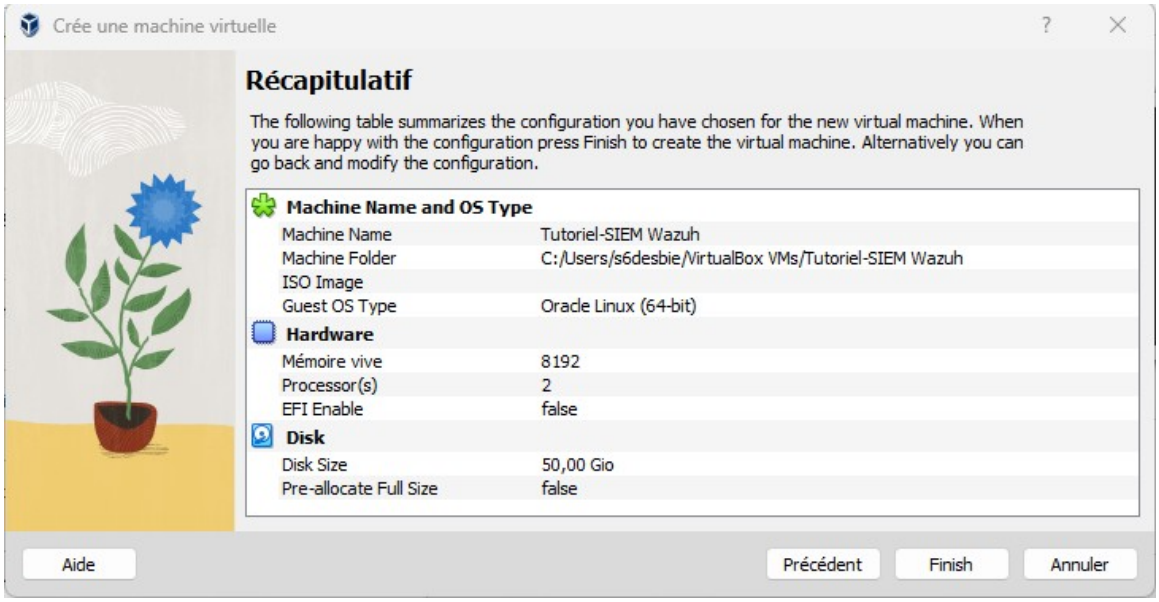
Ce dont que vous allez avoir besoin :

Une machine VirtualBox ;

Docker;

Tout d'abord, veuillez crée une machine virtuelle avec les options suivantes :

Au moins 8192 mb de RAM, 2 cœurs pour le processeur et au moins 50 Gb d'espace disque.



Installez par la suite la distribution Linux de votre choix (Ubuntu Server dans ce tutoriel, vous pouvez y aller avec la distribution que vous voulez).

Une fois l'installation complété et que vous vous êtes connecté sur votre machine virtuelle, faire les fameuses mises à jour et upgrade de la machine (ex : ***sudo apt-get update && sudo apt-get upgrade***).

Après avoir installé les mises à jour, il va être temps d'installer Docker et Docker Compose.

Docker :

> ***sudo curl -sSL https://get.docker.com/ | sh***
> ***sudo systemctl start docker***
> ***sudo systemctl enable docker***

Docker Compose:

s***udo curl -L https://github.com/docker/compose/releases/download/v2.23.3/docker-compose-linux-x86_64 -o /usr/local/bin/docker-compose***

sudo chmod +x /usr/local/bin/docker-compose
sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
docker-compose –version

```
samuel@tuto-wazuh:~$ docker-compose --version
Docker Compose version v2.23.3
```

Vous êtes supposé de voir ça à la fin de la suite de commande si tout s'est bien passé.

Par la suite, faire la commande suivante afin que docker utilise 6 Gb de RAM (d'où pourquoi j'ai mentionné 8 Gb plus haut, pour se laisser une marge de manœuvre).

sudo sysctl -w vm.max_map_count=262144

Et maintenant, le programme principal de ce tutoriel : Wazuh. Nous allons le faire exécuter sur Docker. Pour l'installation, faire la commande suivante :

git clone https://github.com/wazuh/wazuh-docker.git -b v4.2.6 --depth=1

Une fois ceci installé, il va falloir générer des certificats SSL pour sécuriser le traffic réseau de Elasticsearch, Kibana et Nginx :

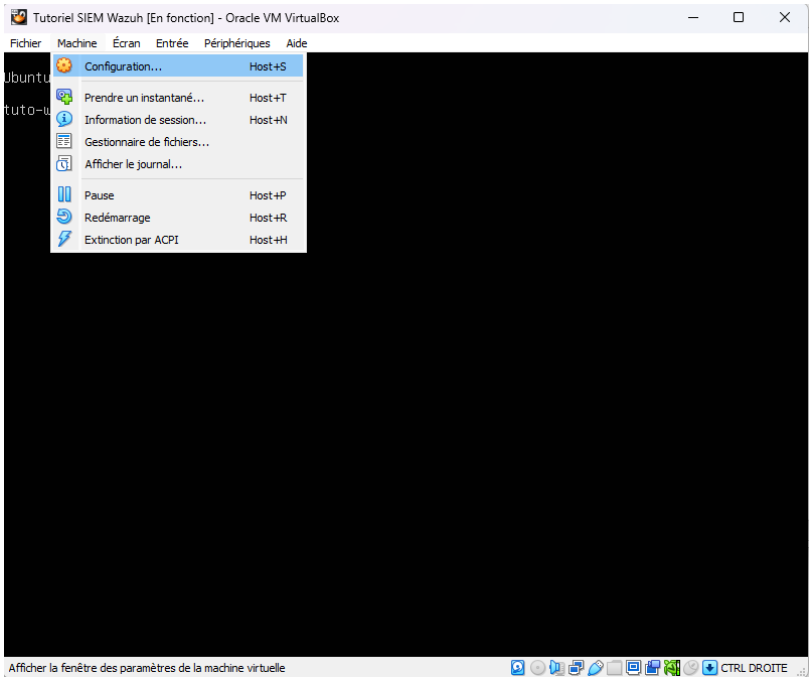
sudo docker-compose -f wazuh-docker/generate-opendistro-certs.ylm run --rm generator
sudo bash ./wazuh-docker/production_cluster/kibana_ssl/generate-self-signed-cert.sh
sudo bash ./wazuh-docker/production_cluster/nginx/ssl/generate-self-signed-cert.sh

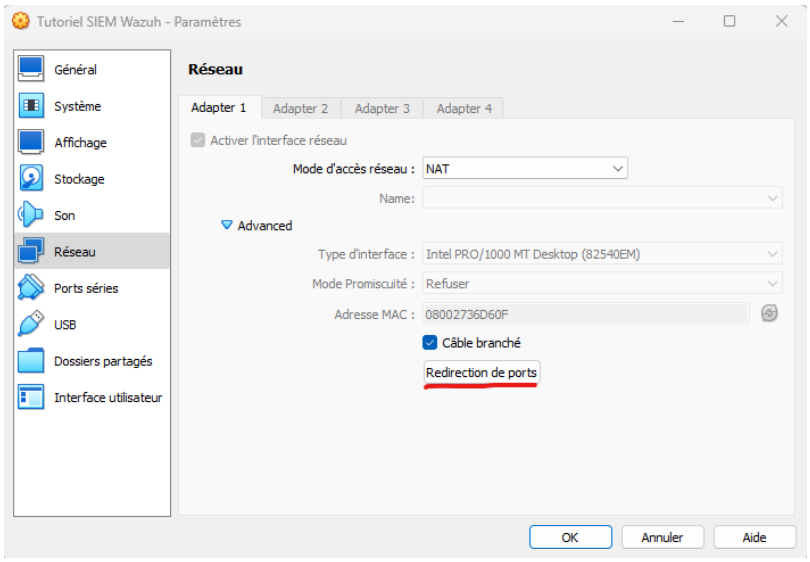
Pour finir avec la partie installation, nous allons déployer notre environnement avec la commande suivante :

sudo docker-compose -f wazuh-docker/production.yml up -d

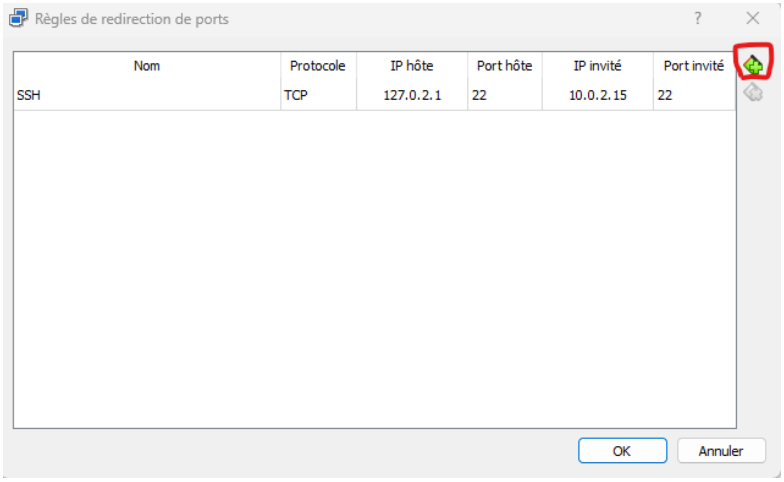
(Prendre note que la première initialisation de l'environnement va prendre plusieurs minutes, ne stressez pas avec ça!)

Pour la connexion au site web, nous allons faire une redirection de port de notre machine physique vers la machine virtuelle. Pour ce faire, aller dans « Machine » → « Configuration » → « Réseau » → « Redirection de ports »

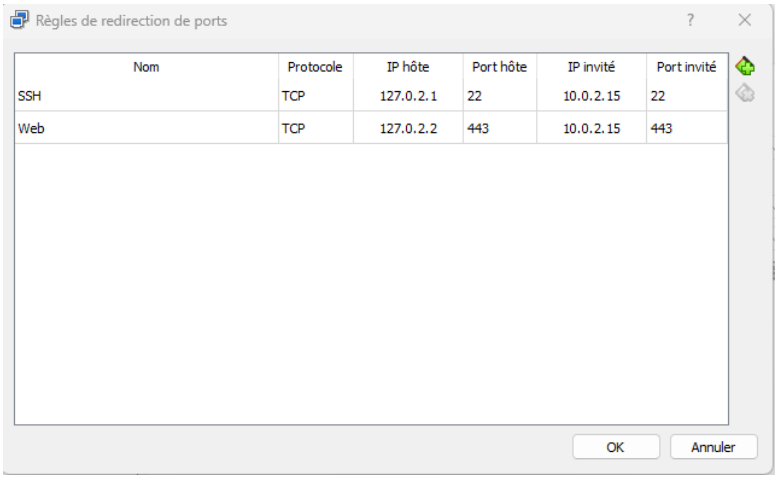




Vous allez ensuite cliquer sur le petit carré vert avec un + vert :



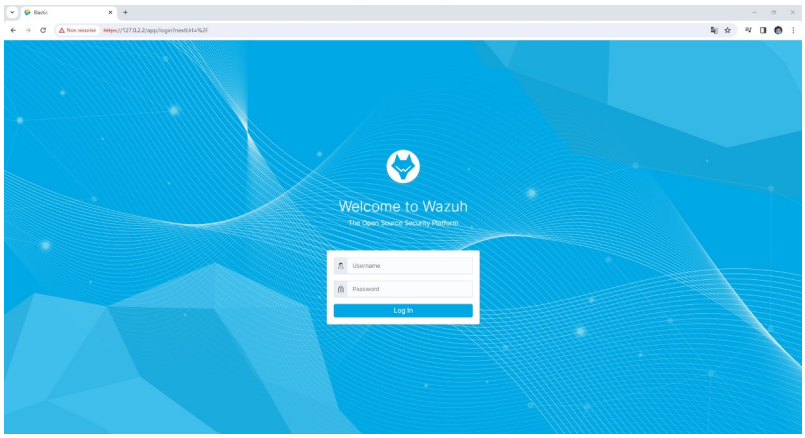
Ensuite, veuillez rentrer la ligne en bas (l'adresse IP hôte peut varier, mais essayer de rester dans le réseau 127.0.XXX.XXX car ce sont des IP local)



Une fois ceci complété, cliquez sur « OK » et encore « OK » pour revenir à la machine virtuelle.

Ouvrez votre navigateur web sur votre machine physique et aller à l'adresse IP que vous avez écrit dans votre redirection de ports (dans mon cas : https://127.0.2.2:443).

Vous allez avoir une alerte de certificat auto-signé, dépendamment de votre navigateur, trouver l'option de continuer à naviguer sur le site.

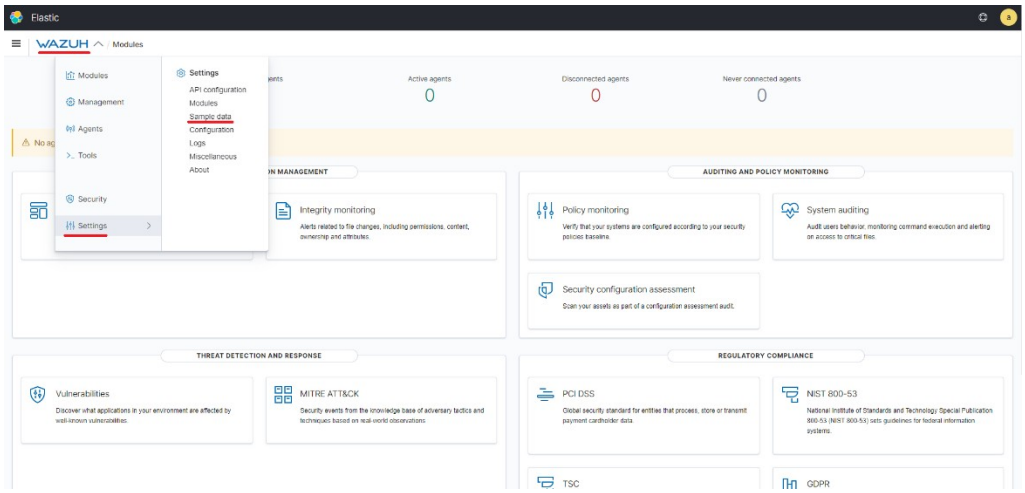


Ta-dam! Vous pouvez maintenant vous connecter avec les identifiants par défaut suivant :
Username : **admin**

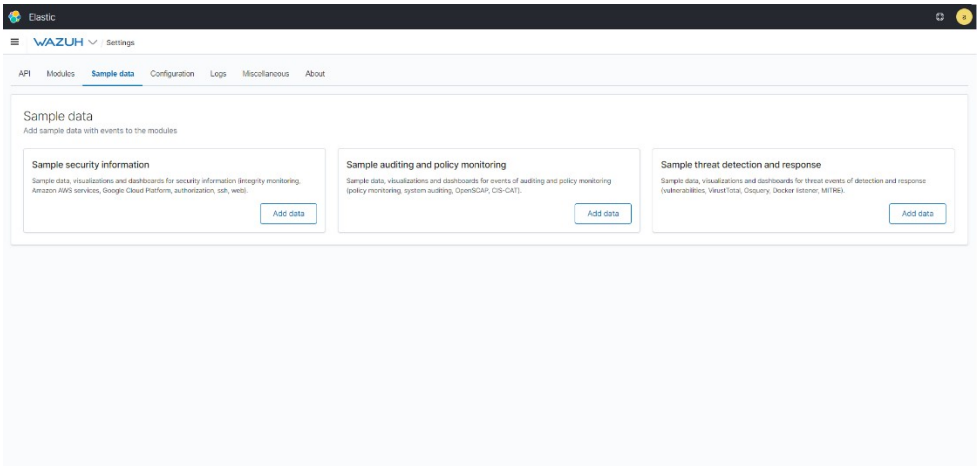
Password : **SecretPassword**

Maintenant que nous sommes connectés, il va falloir générer des données. Bonne nouvelle! Il existe des échantillons de données dans Wazuh.

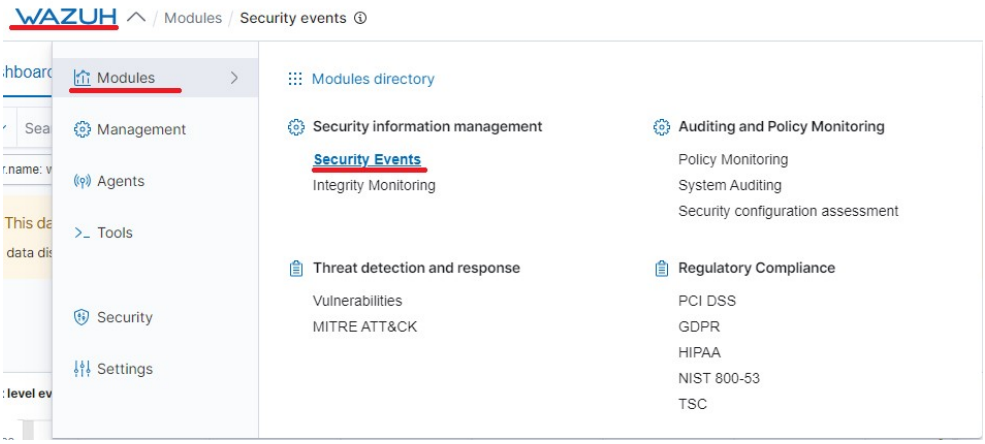
Pour se faire, cliquez sur le mot « Wazuh » en haut à gauche de votre écran, suivit de « Settings » et finalement « Sample data »



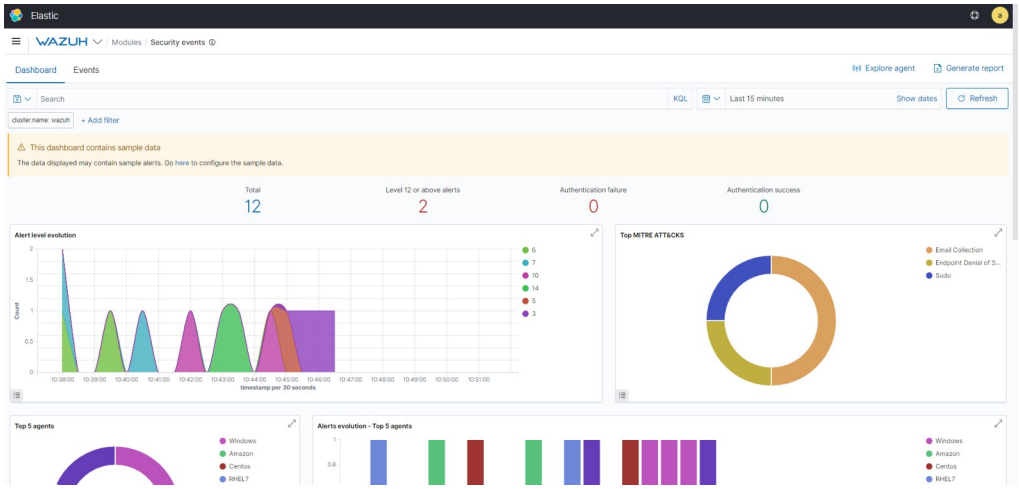
Rendu sur la page suivante, juste choisir les données que vous voulez selon vos besoins en cliquant sur « Add data ».



Une fois les données générées, Cliquez sur « Wazuh » → « Modules » → « Security Events » :



Vous allez arriver sur une page ressemblant à ceci :



Félicitations! Vous avez installé un SIEM et généré des données, maintenant à vous de vous amusez avec Wazuh! Vous pouvez changer la zone de temps des événements à afficher, voir plus bas sur la page les détails des alertes, vous pouvez voir les statistiques en rapport au events, etc.

Liens utiles :

Le tutoriel fut fait à l'aide de ce site web :

https://socfortress.medium.com/easiest-siem-install-wazuh-elasticsearch-kibana-and-filebeat-docker-install-26f9c35762bc

Lien pour Wazuh sur GitHub :

https://github.com/wazuh/wazuh-docker