"Elastic Security"

Jean-Marc Pouchoulon

octobre 2023

Elastic security est une suite de sécurité qui permet de collecter des logs, de les analyser et de les visualiser. La suite est libre sauf pour certaines fonctionnalités avancées comme le "machine learning" et intègre des dashboards sécurité. Les logs sont collectées dans le but de permettre la détection d'intrusion à l'aide de règles fournies par Elastic ou par la communauté et vos propres règles.

1 Mise en place d'un environnement Elastic Security

Docker doit être installé sur votre machine. L'environnement Elastic est composée de plusieurs conteneurs docker.

Faire un "git clone `https://github.com/pushou/siem.git`" afin d'installer "elastic SIEM" , l'IDS "Suricata", Evebox, et Zeek. La configuration nécessaire est musclée et une machine avec 16Go de Ram est un minimum. Vous obtiendrez de l'aide en lançant la commande "make help".

Modifiez le fichier /etc/sysctl.conf

```
vm.max_map_count=262144
```

Puis

```
systctl -p
```

Vous lancerez les commandes suivantes pour installer les différents composants.

```
make es (attendez que la procédure soit terminée, les autres "containers" en ont besoin pour démarrer)
make siem
make fleet
```

"make pass" vous permettra de visualiser le mot de passe pour l'utilisateur "elastic" qui est le super utilisateur de la suite.

Vous pouvez vous connecter à l'interface web de la suite à l'adresse `http://ip_de_votre_machine:5601` avec le compte "elastic" et le mot de passe obtenu précédemment. La stack elastic que vous venez d'installer est composée des qui éléments suivants:

— Une instance d'Elasticsearch: moteur de recherche et de stockage des données qui écoute sur le port 9200 en TLS sur votre hôte.

— Un Kibana: interface web pour visualiser les données qui écoute sur le port 5601 en TLS sur votre hôte.

— fleet: interface web pour gérer les agents Elastic ou Beats qui écoute sur le port 8220 en TLS sur votre hôte.

Un IPS est auu

2 Configuration de fleet

2.1 Configuration de l'url de fleet

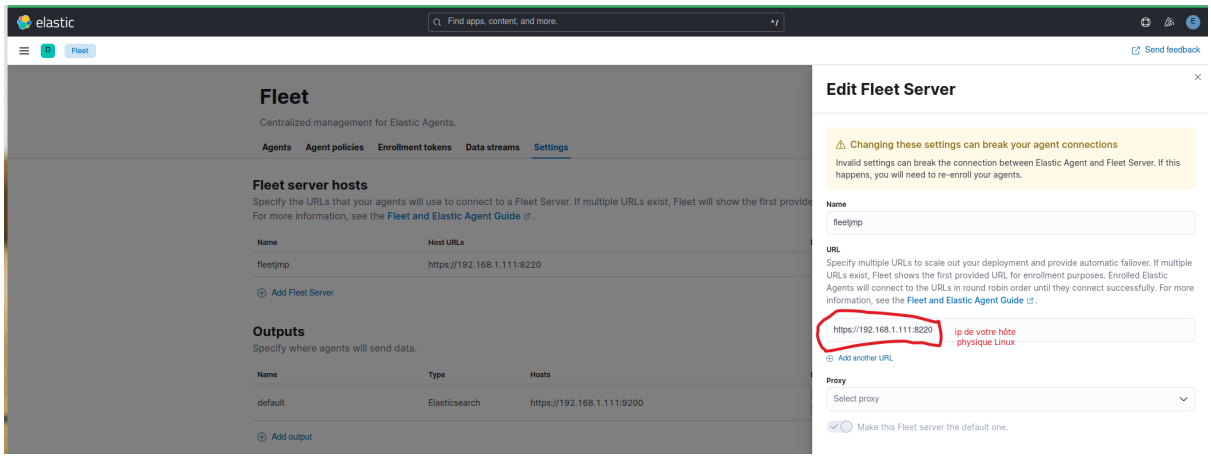

FIGURE 1 – Configuration de l'url de fleet.

2.2 Configuration des "outputs" de fleet

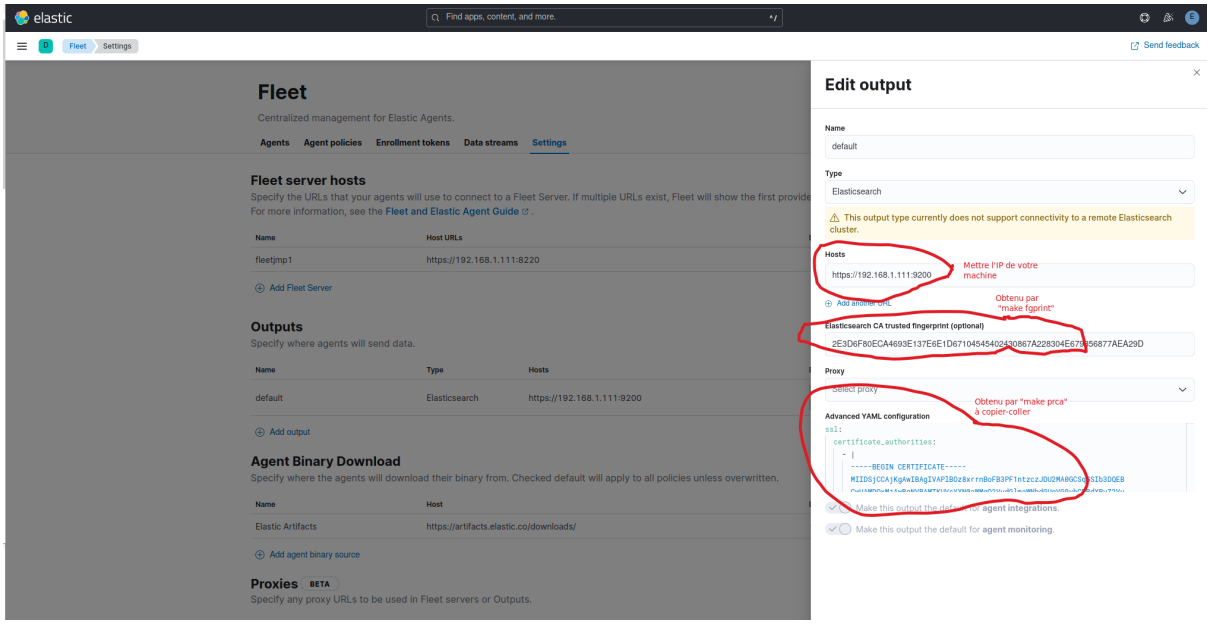

FIGURE 2 – Configuration des "outputs" de fleet.

3 Agent Elastic sur un poste Windows

3.1 Installation de l'agent Elastic sur un poste Windows

Vous désactivez le pare-feu de votre poste Windows et "defender".

Installer l'agent sur un poste windows (VM ou physique du CloudLab) et connectez-le à votre "fleet server". Pour cela, suivez le menu "add agent" de fleet. Vous créerez une policy "Windows" standard et vous l'appliquerez à votre agent.

Vous installez l'agent sur votre poste Windows en suivant les instructions de fleet en Powershell.

3.2 Déploiement des intégrations pour Windows

Charger les deux intégrations suivantes:

— titre "Windows"

— titre "Elastic Defend"

Vous appliquerez ces deux intégrations à l'agent déployé.

Pour "elastic defend" l'agent refuse de se connecter au serveur fleet car il cherche à vérifier le certificat du serveur avec l'IP. Il faut donc désactiver la vérification du hostname du certificat par "defend" dans la configuration avancée de l'intégration.

3.3 Configuration de l'"intégration" de "defend"

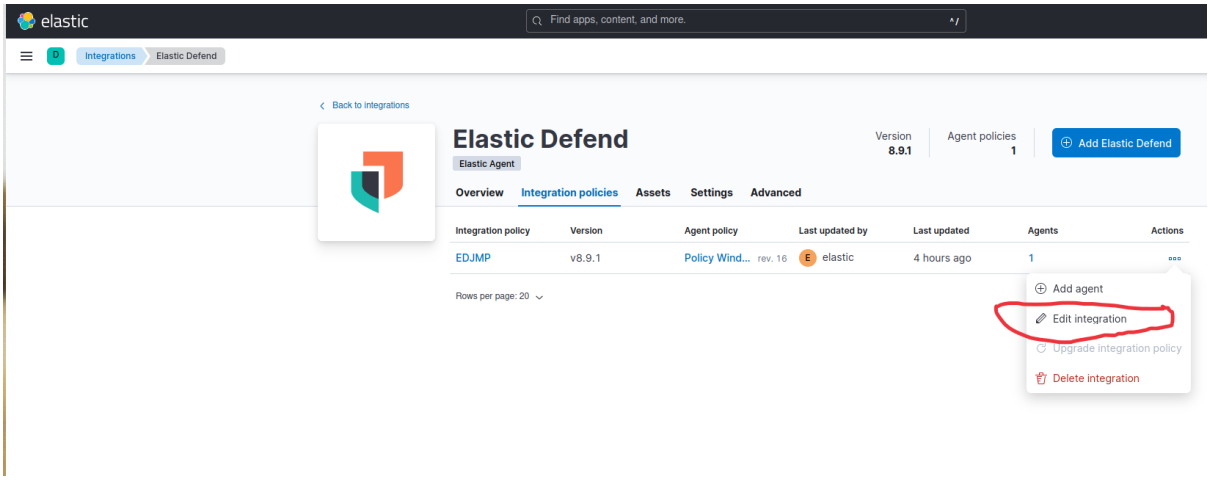

FIGURE 3 – Configuration de l'"intégration" de defend 1.

Faites apparaître la configuration avancée de cette intégration. Passez à "false" le flag et redéployez l'intégration.

3.4 Configuration de l'"intégration" de "defend"

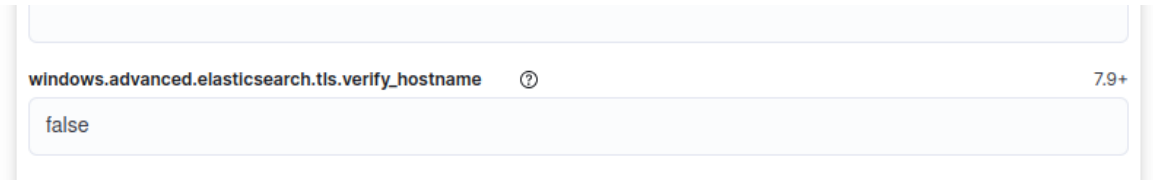

FIGURE 4 – Configuration de l'"intégration" de defend 1.

3.5 Retrouvez des informations sur votre poste Windows

1. Retrouvez les métriques systèmes de votre poste Windows dans Kibana (voir "hosts).
2. Retrouvez les métriques sur les services de votre machine Windows.
3. Retrouvez les pourcentages des différents type d'évènements windows ("security" , "sysmon" ...) de votre machine dans Kibana.
4. Dans un premier temps passer defend en mode "detect".

3.6 Lancez et détectez une simulation d'attaques

1. Chargez et "enable" toutes les règles de détection fournies en standard par Elastic. Seules celles nécessitant un abonnement ne seront pas activées. Vous pouvez activer pour un quelques jours le mode "payant" en test.
2. Déployez le "repository" suivant dans votre machine windows:`https://github.com/NextronSystems/APTSimulator`.
3. Lancez le script "APTSimulator.bat" en mode administrateur et lancez toutes les simulations d'attaques pour faire réagir l'agent.
4. Vérifiez que vous avez bien des alertes dans la partie "Security" de Kibana.
5. Créez une timeline sur l'alerte "process creation". Analyser cet évènement avec Kibana pour obtenir un joli graphique.
6. Remettez "defend" en mode "prevent" et relancez les simulations d'attaques. Vérifiez que les attaques sont bloquées.

4 Agent Elastic sur un poste Linux