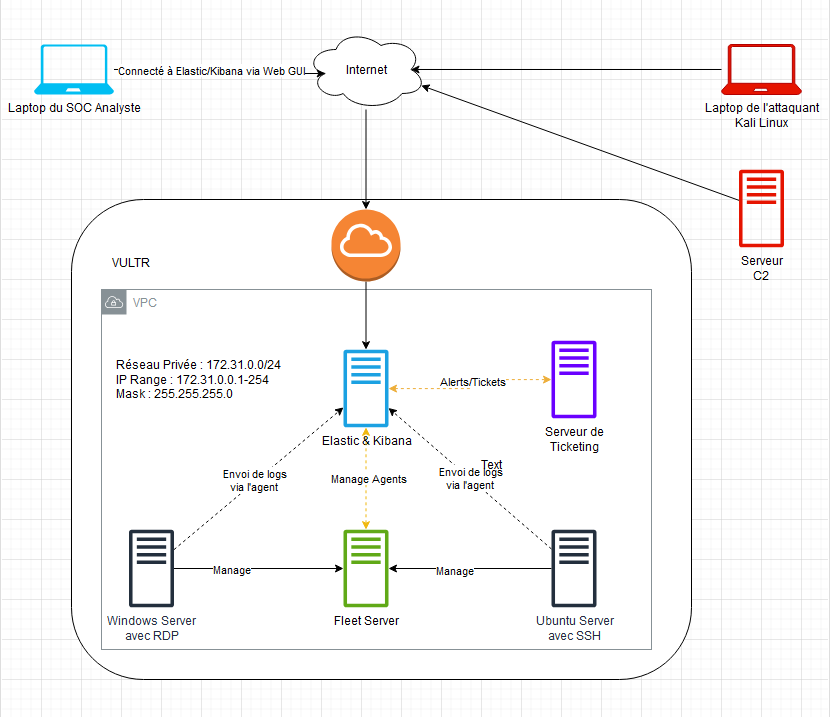
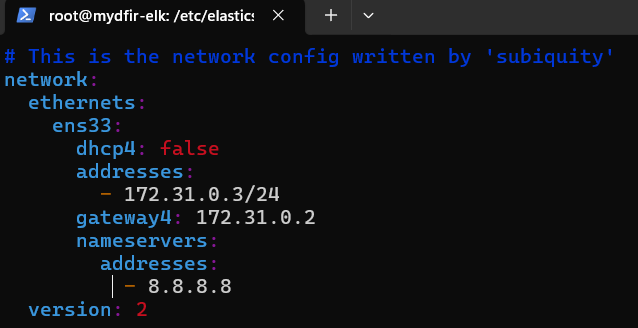
Topologie du Lab



* Installation d’Ubuntu Server et configuration de base
  + Hostname : mydfir-elk
  + vi /etc/netplan/00-installer-config.yaml
  + Assignation de l’adresse IP Statique : 172.31.0.3/24
  + Assignation du Gateway : 172.31.0.3/24
  + netplan apply



*Img1 : image du contenu du fichier de configuration /etc/netplan/00-installer-config.yaml*

Installation Elasticsearch

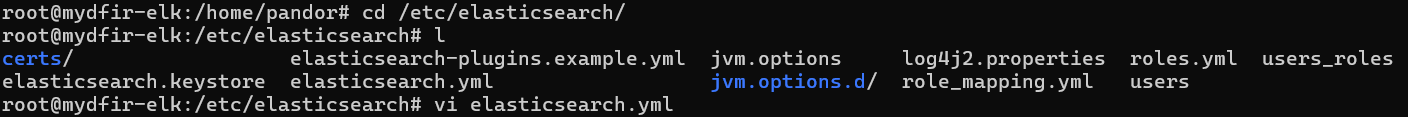
* Allez sur le site <https://www.elastic.co/fr/downloads/elasticsearch>
* Choisir la plateforme d’installation
* Copier le lien de téléchargement

Une image contenant texte, capture d’écran, logiciel

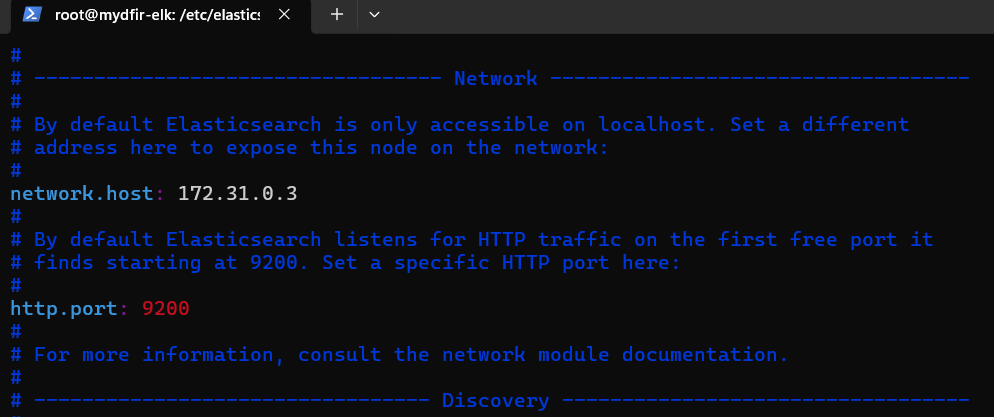
Description générée automatiquement

*Img2 : capture du processus d’installation dans le powershell*

* Enregistrer dans un bloc note la section qui parle de **Security autoconfiguration information**
* Se déplacer dans le répertoire **/etc/elasticsearch**



* Décommenter et modifier le **network.host** (Mettre l’IP du serveur actuel)
* Décommenter le **http.port**



* taper la commande pour rendre persistant le service
  + # systemctl daemon-reload
  + # systemctl enable elasticsearch.service
  + # systemctl start elasticsearch
* Vérifier l’état du service **elasticsearch** 
  + # systemctl status elasticsearch.service

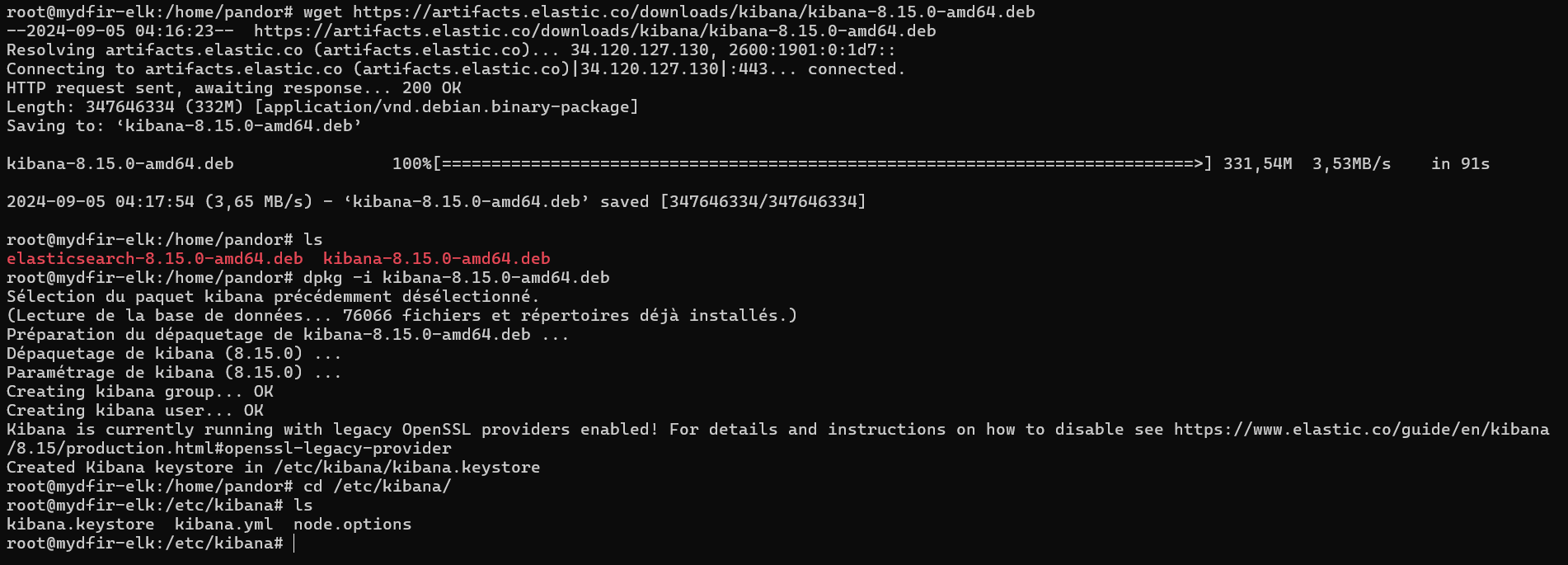
Une image contenant texte, capture d’écran, Police

Description générée automatiquement

*Img3 : capture d’écran qui montre que le processus est démarré*

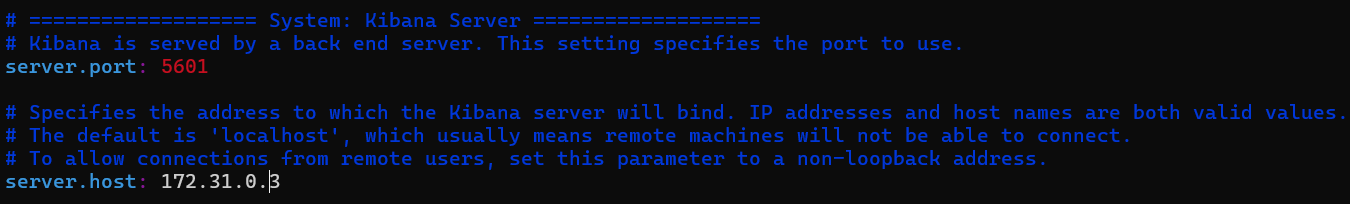
Installation de Kibana

* Aller sur <https://www.elastic.co/fr/downloads/kibana>
* Choisir la plateforme d’installation
* Copier le lien de téléchargement

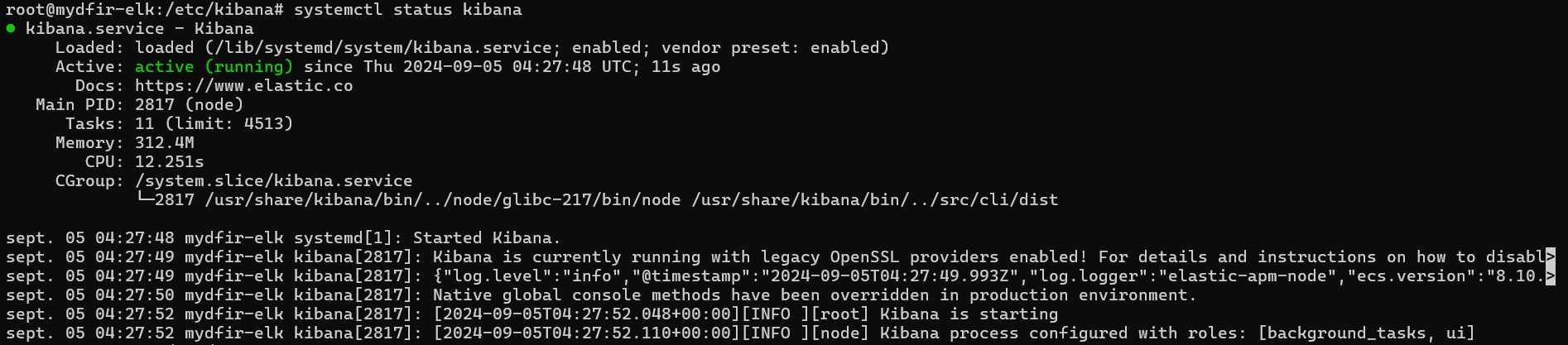


*Img4 : capture du processus d’installation dans le powershell*

* Se déplacer dans le répertoire **/etc/kibana**
* Editer le fichier /etc/kibana/kibana.yml
* Décommenter **server.port** et **server.host**



* # systemctl daemon-reload
* # systemctl enable kibana.service
* # systemctl start kibana
* # ufw allow 5601



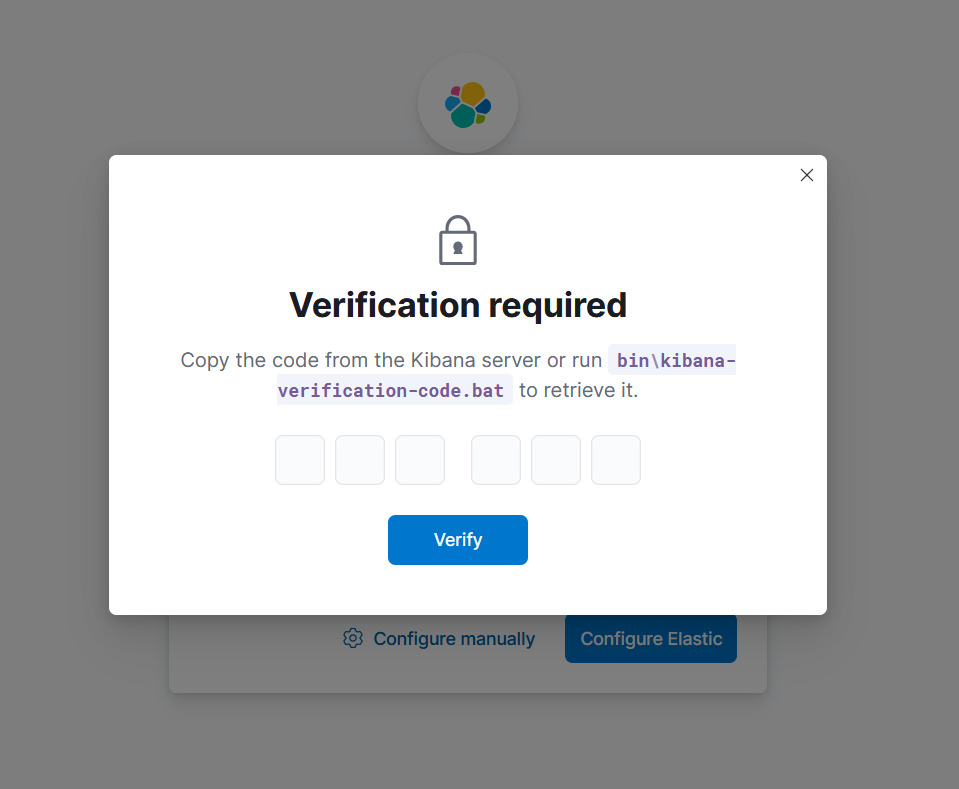
*Img5 : capture d’écran qui montre que le processus est démarré*

* On va générer un Token Elastisearch pour Kibana
  + # cd /usr/share/elasticsearch/bin/
  + # ./elasticsearch-create-enrollment-token --scope kibana
* Un Token sera généré
* Nous allons le copier dans Kibana
* D’abord accédons à Kibana par le navigateur : http://172.31.0.3:5601/

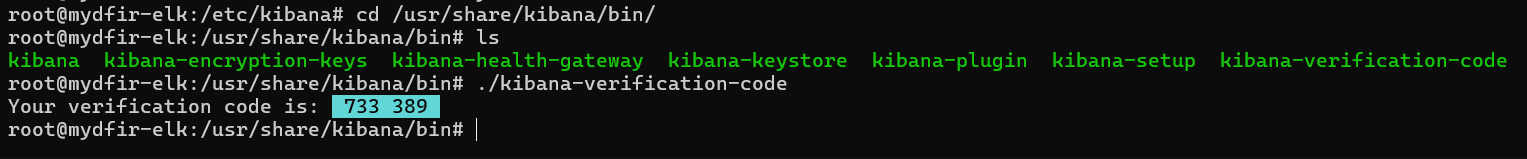
Une image contenant texte, capture d’écran, logiciel, ordinateur

Description générée automatiquement

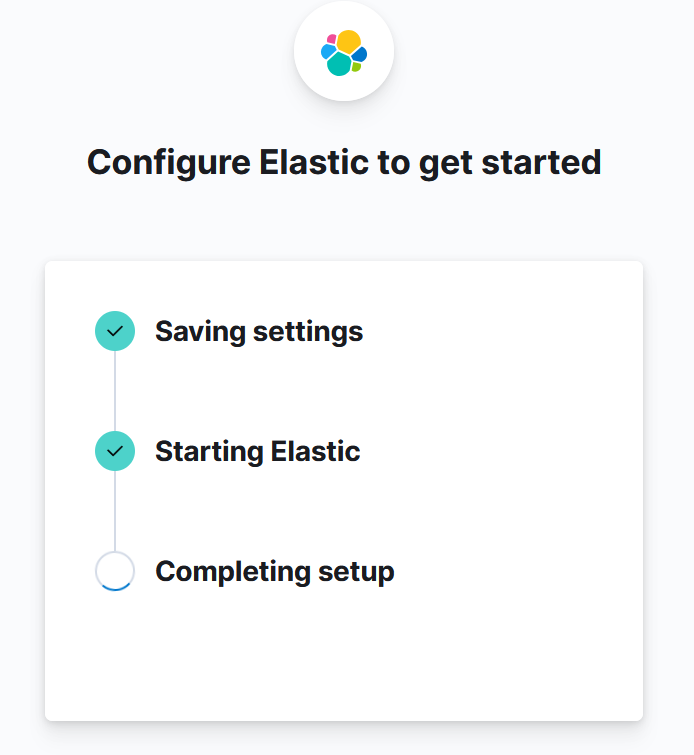
* On copie le Token généré précédemment puis on clique sur **Configure Elastic**
* On a ensuite l’image suivante



* On va chercher le code de vérification
  + # cd /usr/share/kibana/bin/
  + # ./kibana-verification-code



* La configuration de Kibana démarre

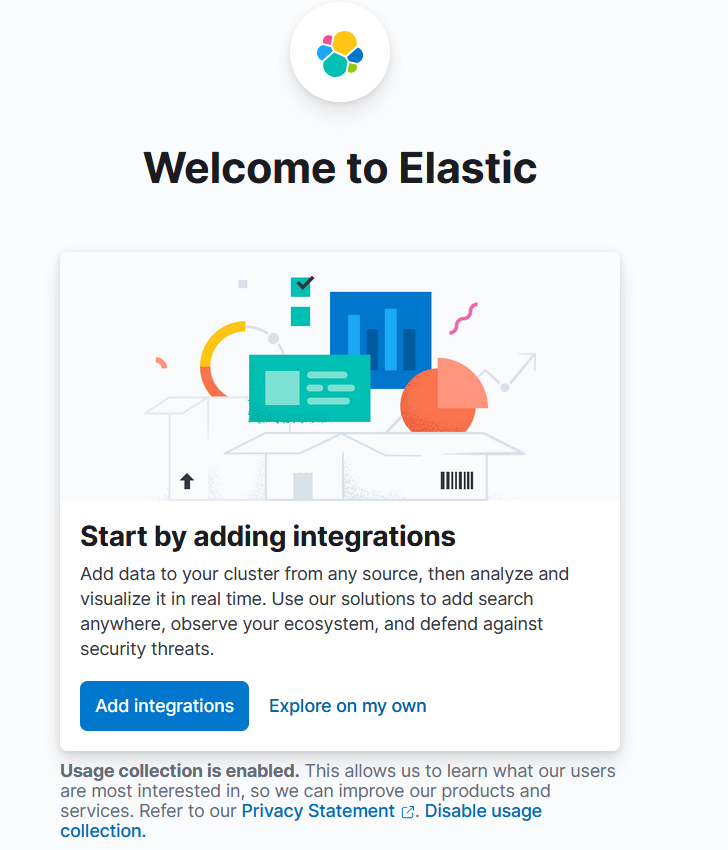


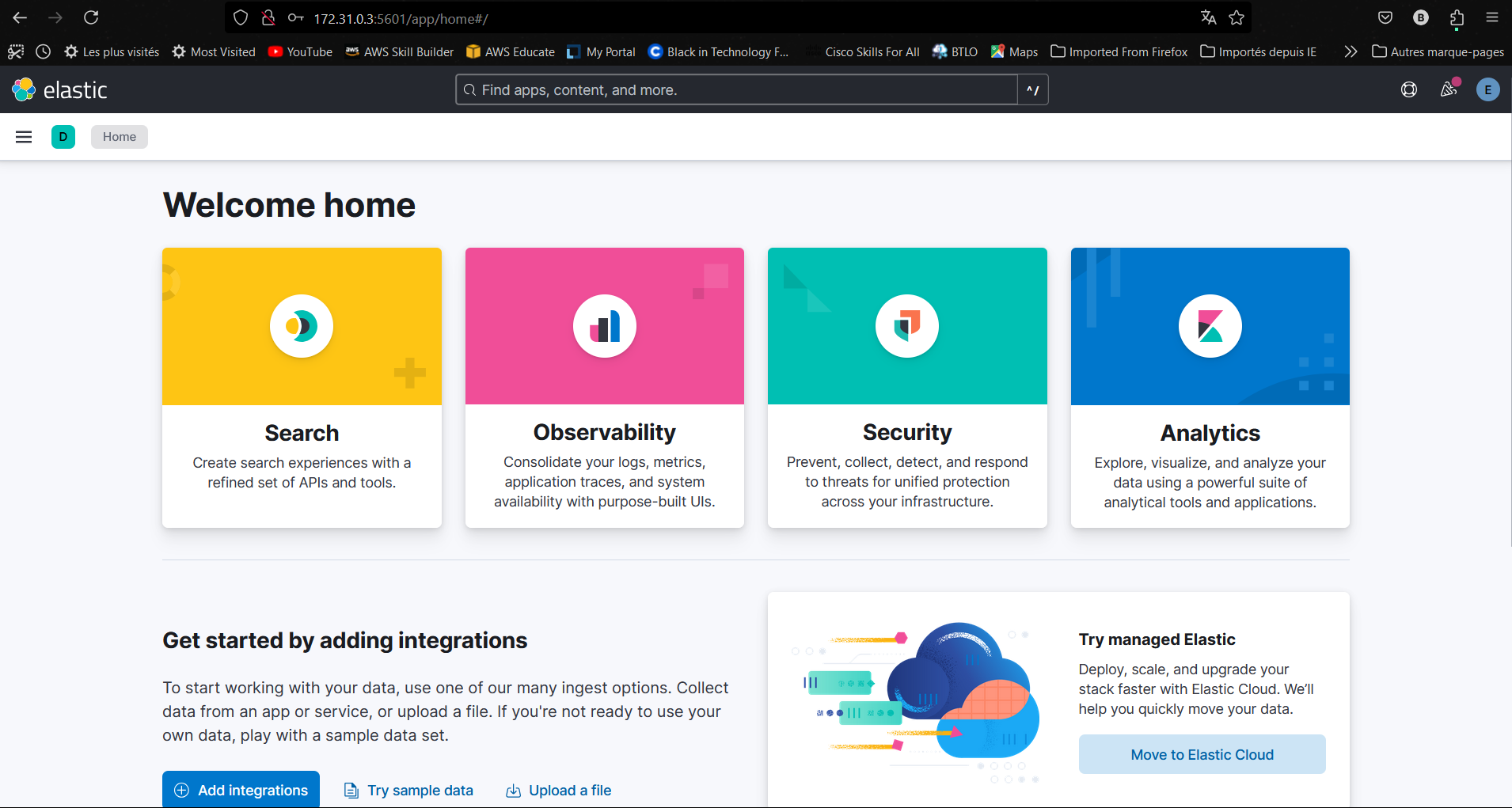
* Après la configuration nous seront appelé à entrer le Username et le Password (Ces informations sont stockées dans la section **Security autoconfiguration information** sauvegardé lors de l’instalation d’Elasticsearch cf : img2)

Une image contenant texte, capture d’écran, Police, Système d’exploitation

Description générée automatiquement

* Après avoir validé, on aura la page suivante. Puis on clique sur Explore on my own

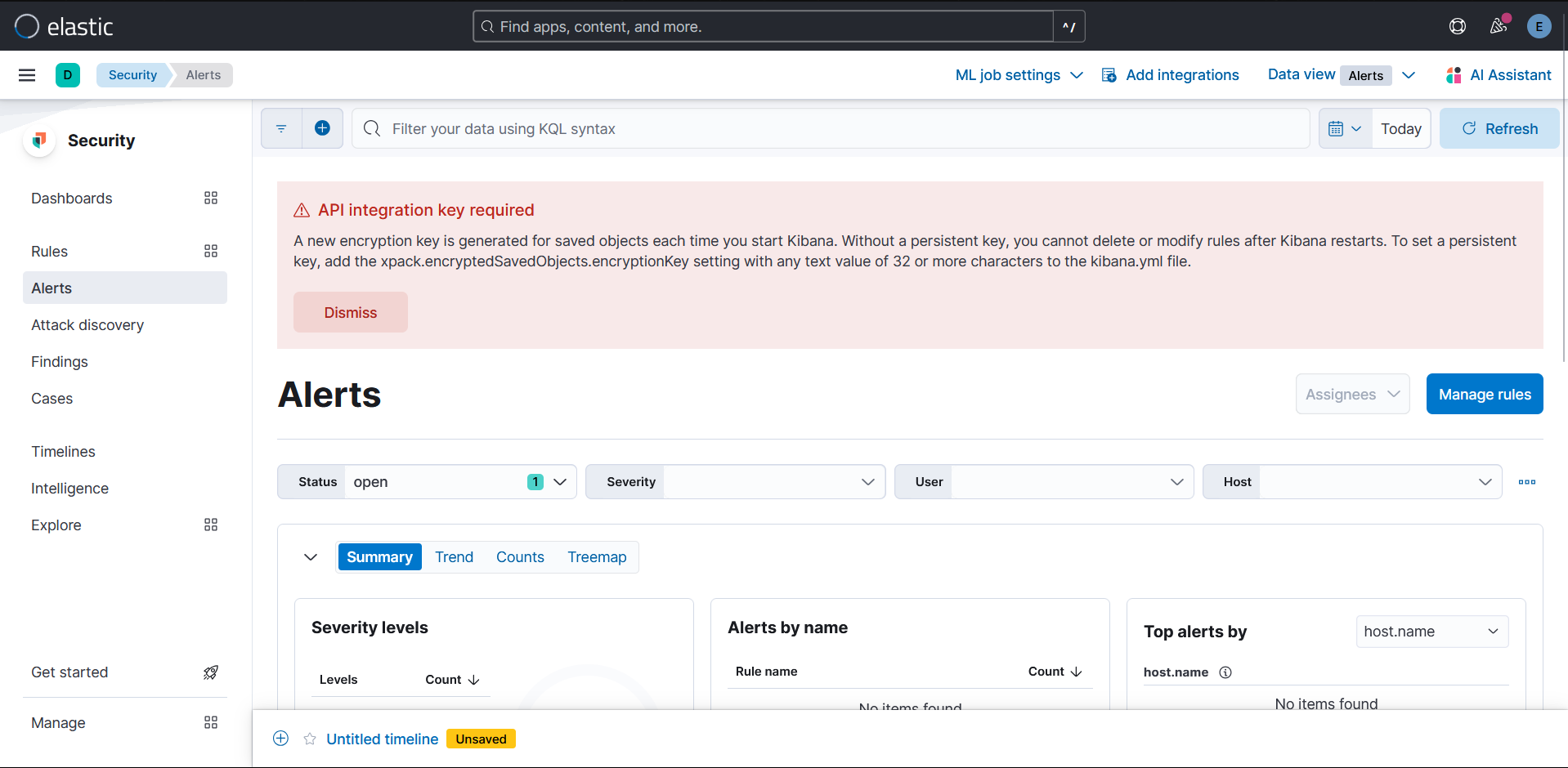




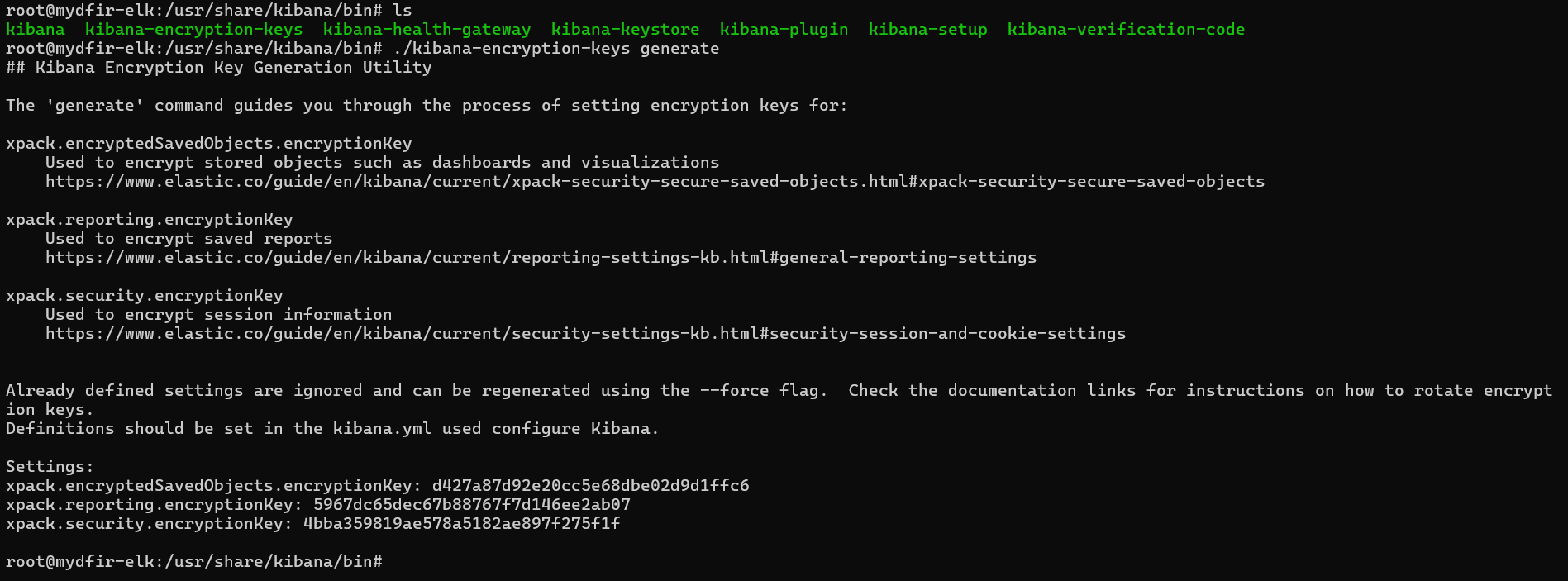
* Pour terminer l’installation nous allons ajouter le keystores

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

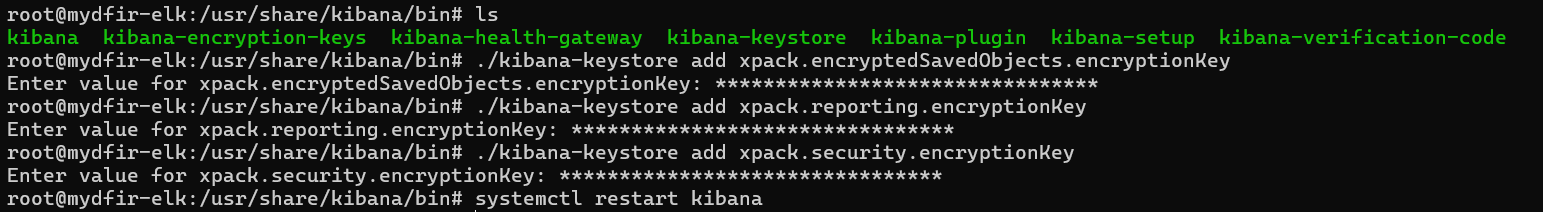
Description générée automatiquement



* Pour régler l’erreur affiché dessus, on va générer des clés de cryptage
  + # cd /usr/share/kibana/bin/
  + # ./kibana-encryption-keys generate
  + On copie la sortie dans un bloc note



* On suit les étapes de la capture d’écran suivante en fonction des clés générés puis on redémarre Kibana



* Nous n’avons plus l’erreur concernant le API Integration Required

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Kibana a été installé avec succès