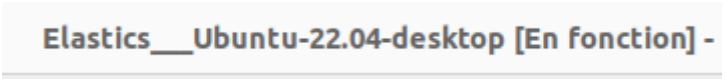
Gavin Nshimirimana

R5.Cyber.11

Compte Rendu	Outil Associé
1. Compte rendu d'installation de votre suite Elastic sur Ubuntu	Elasticsearch, Kibana
2. Compte rendu de supervision avec votre suite Elastic d'une machine Ubuntu	Elasticsearch, Kibana, filebeat, metricbeat
3. Compte rendu de supervision avec votre suite Elastic d'un service web (Apache, Nginx, ...)	Elasticsearch, Kibana, filebeat, metricbeatLogstash
4. Compte rendu de supervision d'équipement(s) Cisco	Elasticsearch, Kibana, filebeat, metricbeat
5. Compte rendu de supervision d'un autre service/équipement	Elasticsearch, Kibana, filebeat, metricbeat
6. Comptes rendus de vos analyses de logs des TP0 à TP5	Elasticsearch, Kibana, filebeat, metricbeat



Compte rendu n°0

Installation de votre suite Elastic sur Ubuntu

Installation de la suite Elastic sur Ubuntu

Choix de la méthode d'installation

Il existe deux méthodes principales pour installer Elasticsearch :

1. **Archives Linux (tar.gz)** :
    - **Flexibilité** : Ce format contient les fichiers d'Elasticsearch compressés et peut être utilisé sur n'importe quelle distribution Linux ou sur macOS. L'installation se fait manuellement, ce qui nécessite de décompresser l'archive et de placer les fichiers où je le souhaite. Cela implique une gestion plus active du démarrage/arrêt du service, des mises à jour et de la configuration.
    - **Pas d'intégration automatique** : Les dépendances ne sont pas installées automatiquement, et je dois enregistrer Elasticsearch en tant que service système manuellement.

2. **Packages Debian (deb)** :
    - **Simplicité d'utilisation** : Le fichier .deb est conçu spécifiquement pour les systèmes basés sur Debian comme Ubuntu. L'installation se fait via un gestionnaire de paquets (apt), ce qui permet de résoudre automatiquement les dépendances et d'intégrer Elasticsearch en tant que service système.
    - **Mises à jour facilitées** : Grâce à apt, les mises à jour sont simples à réaliser, et les conflits de dépendances sont gérés par le gestionnaire de paquets.

Pour la mise en place de la suite Elastic, j'ai choisi d'utiliser l'archive Linux (tar.gz) plutôt que le package Debian (.deb). Ce choix m'offre un meilleur contrôle sur l'emplacement des fichiers et la configuration, permettant ainsi une personnalisation adaptée.

Téléchargement et installation

J'ai donc commencé par télécharger les fichiers nécessaires depuis le site officiel d'Elastic. Voici les liens utilisés :

Téléchargement d'Elasticsearch
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.10.4-linux-x86_64.tar.gz

Checksum pour validation
https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.10.4-linux-x86_64.tar.gz.sha512

Après avoir téléchargé l'archive, j'ai décompressé le fichier à l'aide de la commande suivante
tar -xzf elasticsearch-8.10.4-linux-x86_64.tar.gz

Je me suis ensuite rendu dans le répertoire d'Elasticsearch
cd elasticsearch-8.10.4

```
administrateur@rt-mv:~$ cd Téléchargements/
administrateur@rt-mv:~/Téléchargements$ ls
elasticsearch-8.10.4-linux-x86_64.tar.gz  elasticsearch-8.10.4-linux-x86_64.tar.gz.sha512
administrateur@rt-mv:~/Téléchargements$ shasum -a 512 -c elasticsearch-8.10.4-linux-x86_64.tar.gz.sha512
elasticsearch-8.10.4-linux-x86_64.tar.gz: OK
administrateur@rt-mv:~/Téléchargements$ ^[[200~tar -xzf elasticsearch-8.10.4-linux-x86_64.tar.gz~
tar : commande introuvable
administrateur@rt-mv:~/Téléchargements$ tar -xzf elasticsearch-8.10.4-linux-x86_64.tar.gz
administrateur@rt-mv:~/Téléchargements$ cd elasticsearch-8.10.4/
administrateur@rt-mv:~/Téléchargements/elasticsearch-8.10.4$ S
```

La commande : *shasum -a 512 -c elasticsearch-8.10.4-linux-x86_64.tar.gz.sha512* est utilisée pour **vérifier l'intégrité** du fichier téléchargé en comparant son empreinte (ou somme de contrôle) avec celle fournie dans le fichier `.sha512`

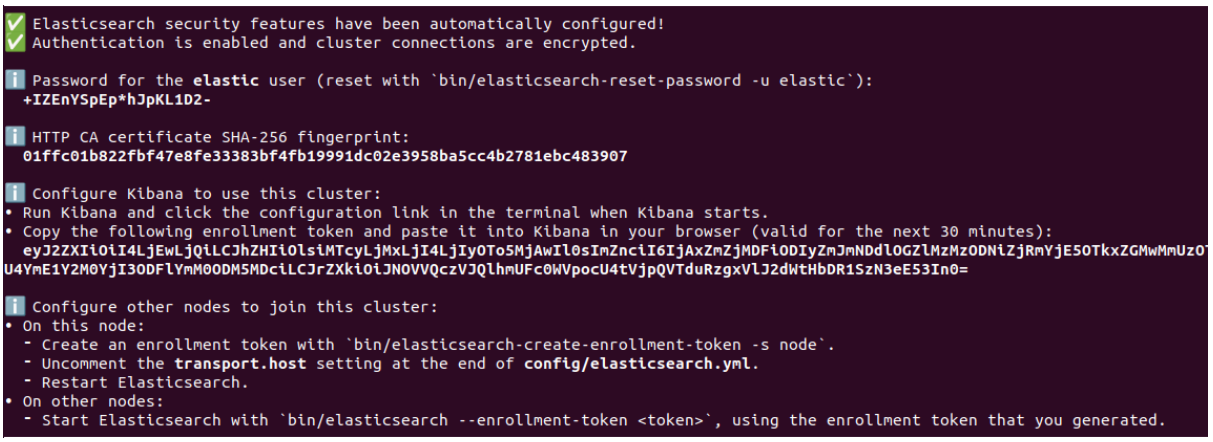
Le message **OK** signifie que l'intégrité du fichier `elasticsearch-8.10.4-linux-x86_64.tar.gz` est confirmée ! Le fichier téléchargé n'a pas été modifié ou corrompu, et correspond exactement à l'original distribué par Elastic.

Pour démarrer le service, j'ai exécuté la commande suivante : ./bin/elasticsearch

Authentification

Lors du premier démarrage, j'ai reçu un nom d'utilisateur et un mot de passe nécessaires pour me connecter à Elasticsearch :

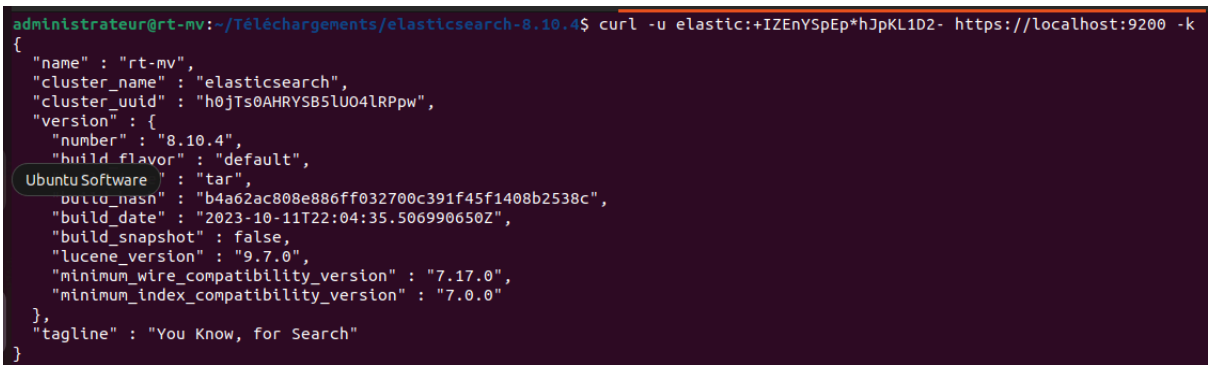
- **Nom d'utilisateur** : `elastic`
- **Mot de passe** : `+IZEnYSpEp*hJpKL1D2-` (Ce mot de passe est affiché dans le terminal au démarrage d'Elasticsearch.)



Pour se connecter à Elasticsearch il existe deux méthodes :

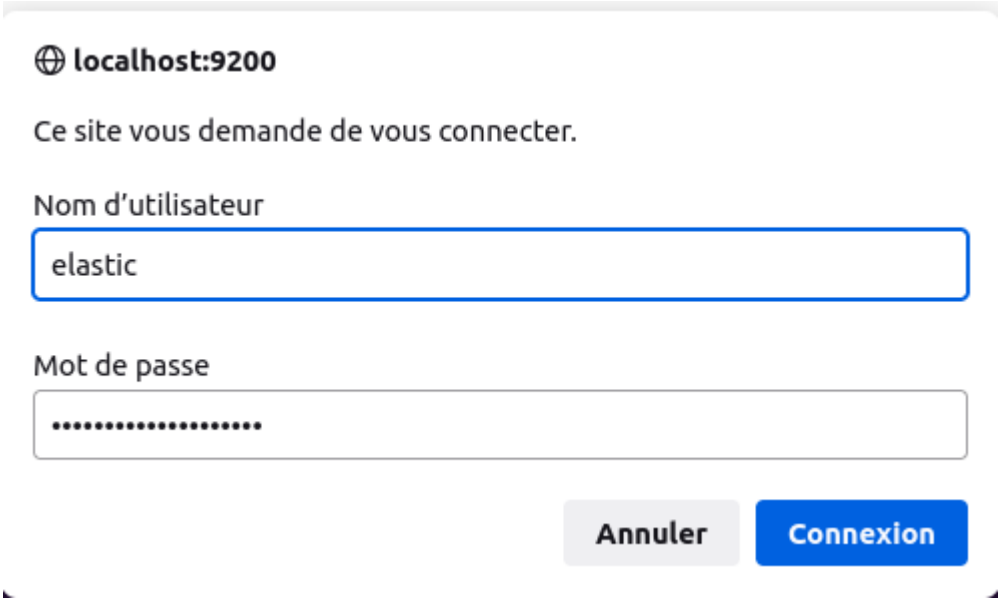
Ligne de commande :

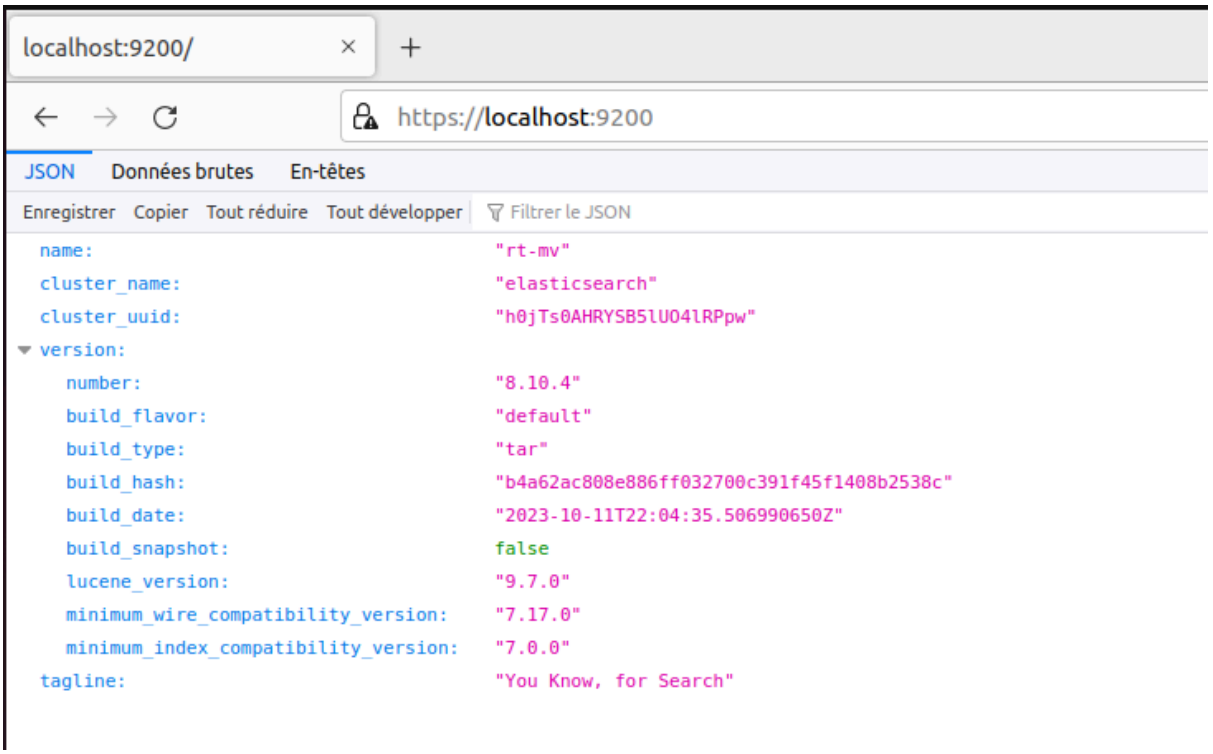
curl -u elastic:+IZEnYSpEp*hJpKL1D2- https://localhost:9200 -k



Navigateur Web :

En accédant à l'URL suivante : https://localhost:9200/.





Une fois connecter ont peut donc visualiser les informations sur le cluster.

Détails du Cluster

- **Nom de l'instance** : `rt-mv`
- **Nom du cluster** : `elasticsearch`
- **UUID du cluster** : `h0jTs0AHRYSB5lUO4lRPpw`
- **Version d'Elasticsearch** : `8.10.4`

Mise en place de l'interface Web avec Kibana

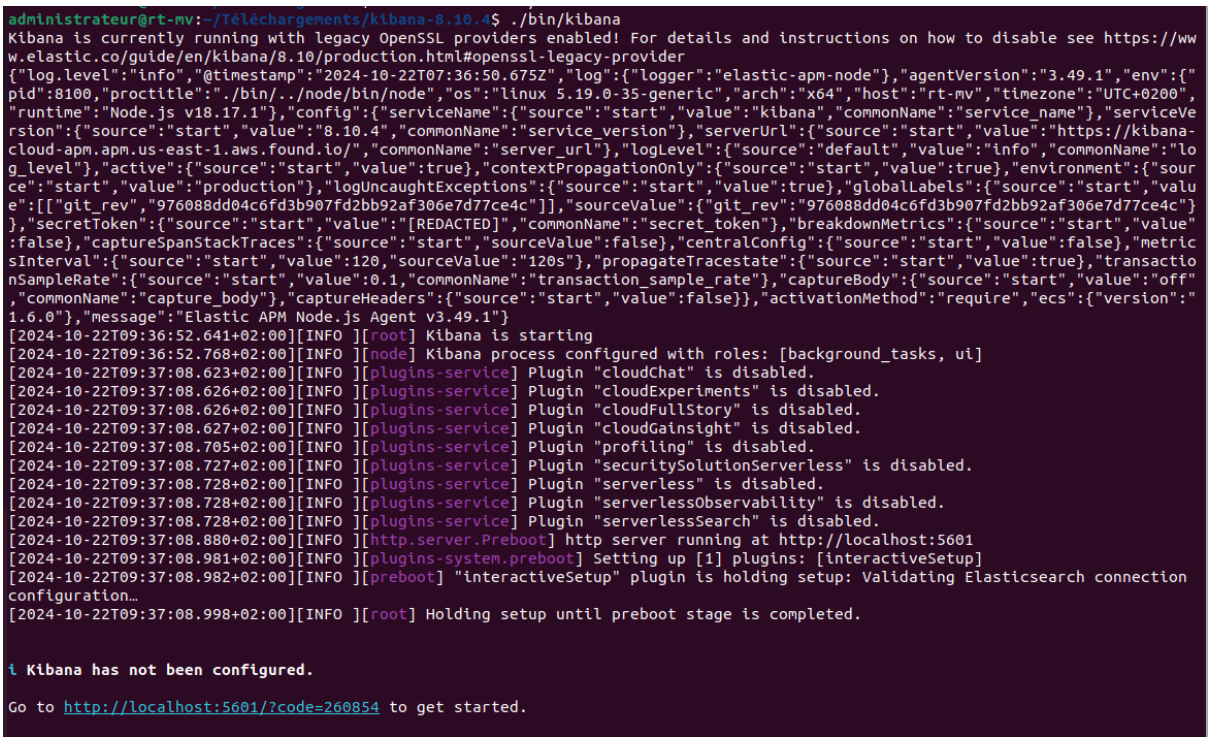
Pour avoir une interface graphique pour visualiser et interagir avec mes données, j'ai installé Kibana. Voici les étapes suivies pour l'installation :

Téléchargement et décompression de Kibana

J'ai téléchargé Kibana avec les commandes suivantes :

curl -O https://artifacts.elastic.co/downloads/kibana/kibana-8.10.4-linux-x86_64.tar.gz
curl https://artifacts.elastic.co/downloads/kibana/kibana-8.10.4-linux-x86_64.tar.gz.sha512 | shasum -a 512 -c -
tar -xzf kibana-8.10.4-linux-x86_64.tar.gz
cd kibana-8.10.4/

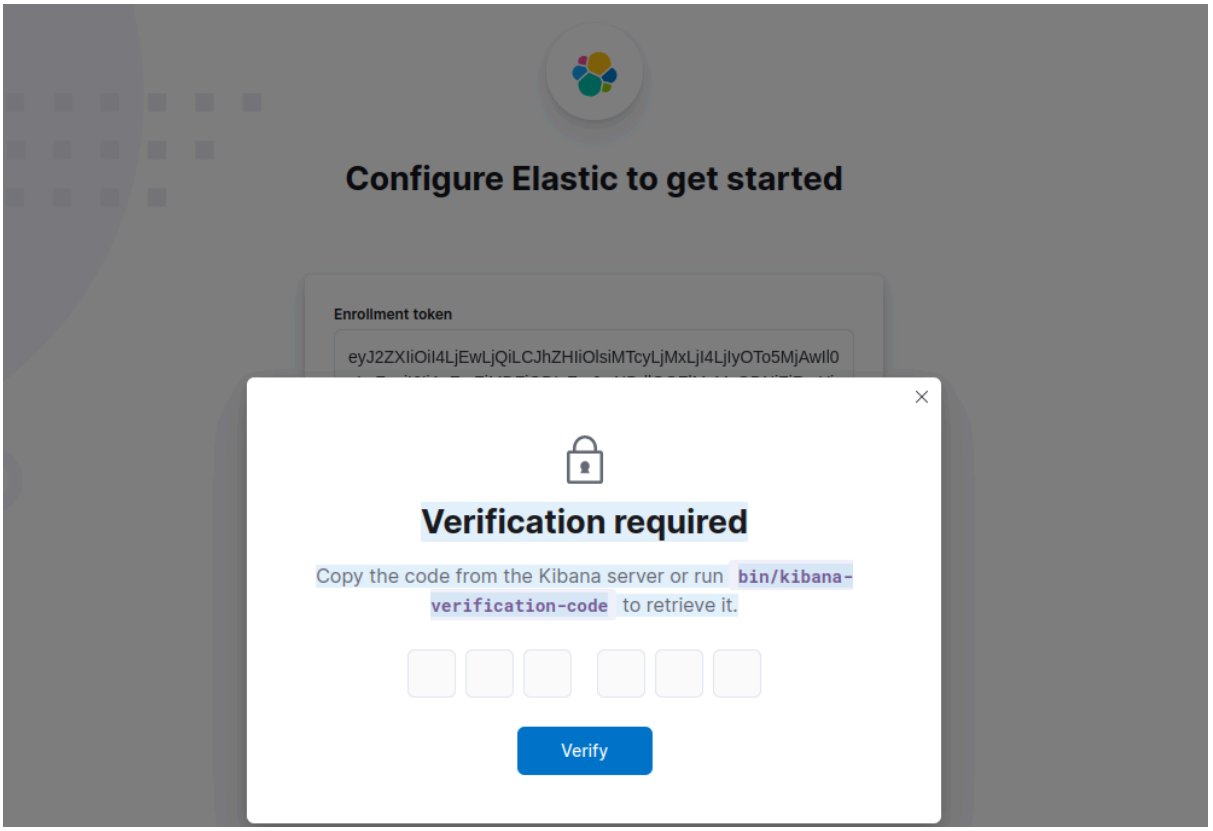
Après la décompression, j'ai lancé Kibana. J'ai ensuite accédé à l'interface web pour remplir les informations requises afin de finaliser l'installation.

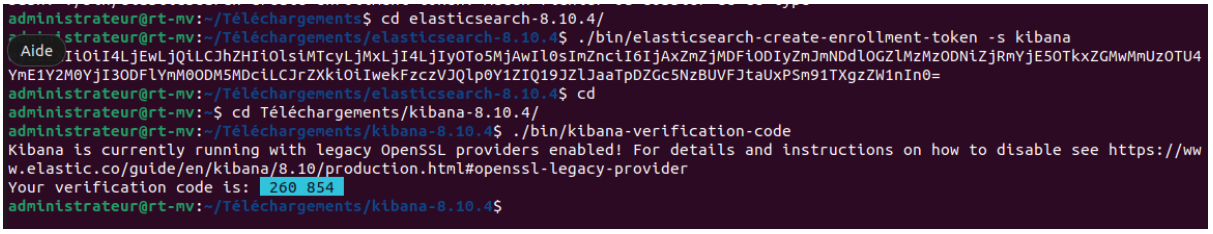


Une fois kibana décompressé lancer je me rend sur l'interface web et rempli ce qui est demandé afin de terminer l'installation,

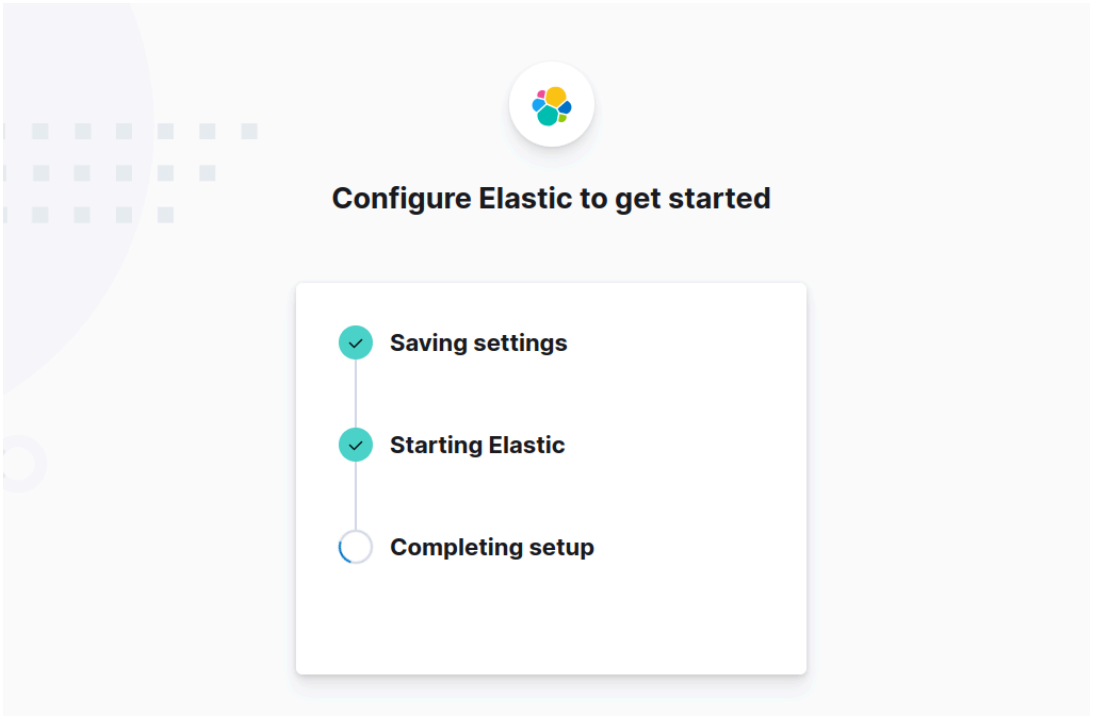
Configuration de Kibana

Kibana demande une authentification en deux étapes : un token d'enrôlement et un code de vérification,

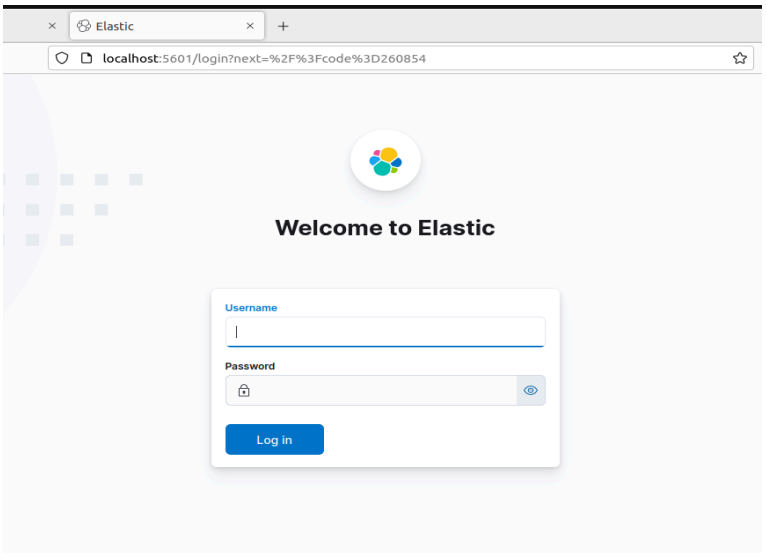




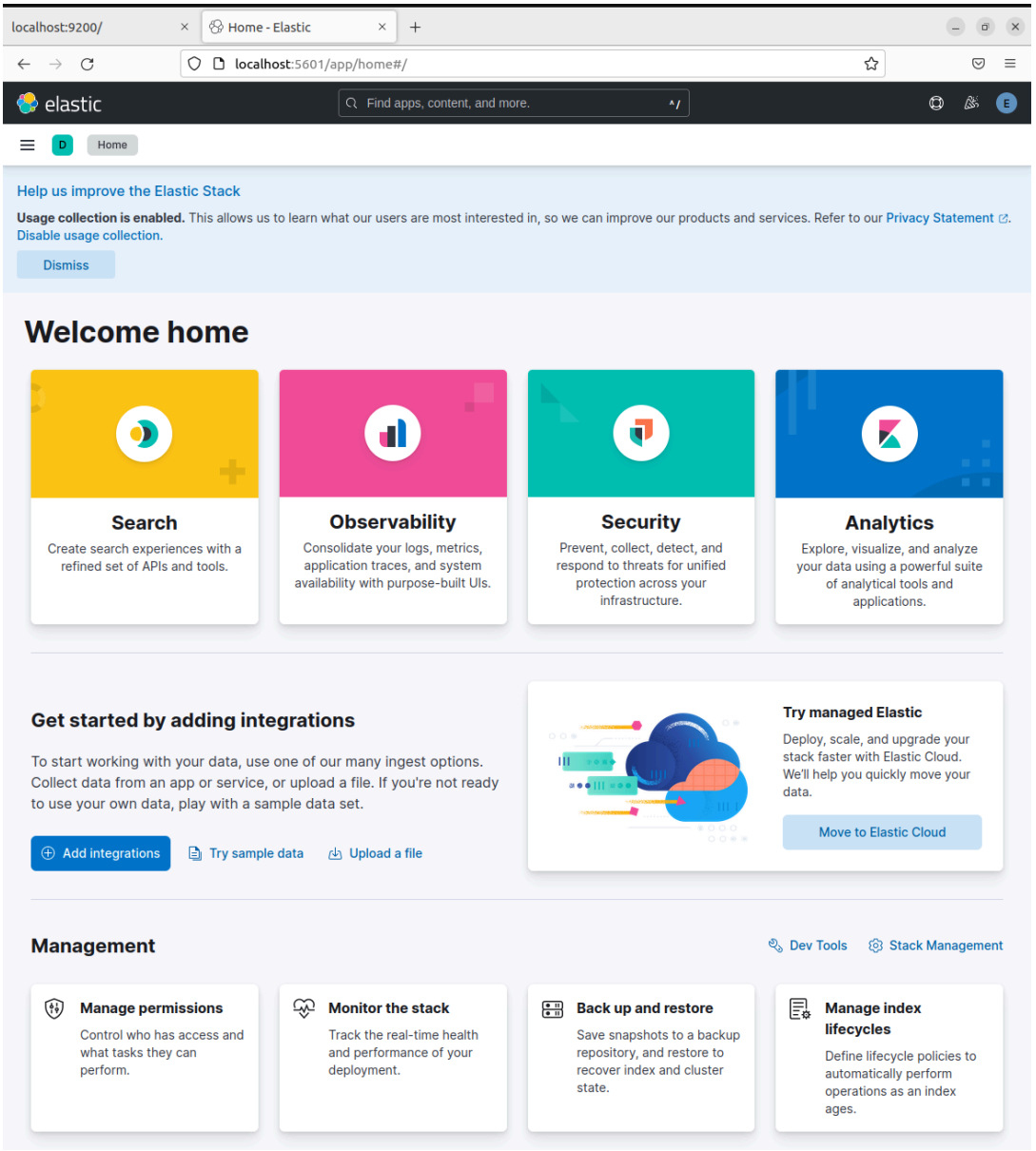
Une fois ces étapes réalisées, Kibana s'est installé automatiquement et j'ai attendu que la configuration se termine.



À la fin de ce processus, une nouvelle demande d'authentification est apparue pour finaliser la configuration de Kibana.



Enfin voici à quoi ressemble l’interface d’élastics une fois que kibana est installé



Résumé de l'installation

Après toutes ces étapes, j'ai pu accéder à deux outils essentiels :

- **Elasticsearch**, qui fonctionne par défaut sur le port 9200 pour les requêtes HTTP.
- **Kibana**, qui fonctionne sur le port 5601, servant d'interface web pour interagir avec Elasticsearch.

En accédant à Kibana via http://localhost:5601, j'utilise l'interface graphique qui se connecte à Elasticsearch en arrière-plan via le port 9200. Si je souhaite interagir directement avec Elasticsearch, je peux continuer à utiliser les requêtes sur http://localhost:9200.