R5.Cyber.11

Modou Diop

RT3

1/ Un compte rendu d'installation de votre suite elastic sur Ubuntu. **(SAE5.Cyber.03)**

SAE 5. Cyber.11

Objectif général :

Configurer, déployer, et utiliser la suite Elastic pour la supervision, l'analyse de logs et la surveillance de systèmes, services, et équipements réseaux dans le cadre de scénarios pratiques

Sommaire :

C’est quoi Elasticsearch

Elasticsearch est un moteur de recherche et d’analyse distribué, basé sur Apache Lucene, conçu pour traiter rapidement de grandes quantités de données en temps réel.

Il est souvent utilisé pour des cas d'utilisation tels que la recherche plein texte, l'analyse de journaux, la surveillance, et bien plus encore.

Téléchargement des fichiers d’installation

Je vais décrire le processus d’installation d’Elasticsearch, composant central de la suite Elastic, sur un système Ubuntu.

Récupérer l'archive d’installation :

Je vais utiliser la commande `wget` pour récupérer des fichiers depuis un serveur distant sur Internet. La première commande récupère un fichier tar.gz (`elasticsearch-8.10.4-linux-x86_64.tar.gz`), qui est une archive compressée contenant les fichiers nécessaires pour installer Elasticsearch sur un système Linux 64 bits.

```
root@rt-mv:/home/administrateur# wget https://artifacts.elastic.co/downloads/el
asticsearch/elasticsearch-8.10.4-linux-x86_64.tar.gz
--2025-01-23 16:49:33--  https://artifacts.elastic.co/downloads/elasticsearch/e
lasticsearch-8.10.4-linux-x86_64.tar.gz
Résolution de cache-etu.univ-artois.fr (cache-etu.univ-artois.fr)… 193.49.62.52
Connexion à cache-etu.univ-artois.fr (cache-etu.univ-artois.fr)|193.49.62.52|:3
128… connecté.
requête Proxy transmise, en attente de la réponse… 200 OK
Taille : 611633882 (583M) [application/x-gzip]
Enregistre : ‘elasticsearch-8.10.4-linux-x86_64.tar.gz’
Corbeille
earch-8.10. 100%[==================>] 583,30M  54,3MB/s    ds 13s

2025-01-23 16:49:47 (46,4 MB/s) - ‘elasticsearch-8.10.4-linux-x86_64.tar.gz’ en
registré [611633882/611633882]

root@rt-mv:/home/administrateur#
```

```
root@rt-mv:/home/administrateur# wget https://artifacts.elastic.co/downloads/el
asticsearch/elasticsearch-8.10.4-linux-x86_64.tar.gz.sha512
--2025-01-23 16:51:13--  https://artifacts.elastic.co/downloads/elasticsearch/e
lasticsearch-8.10.4-linux-x86_64.tar.gz.sha512
Résolution de cache-etu.univ-artois.fr (cache-etu.univ-artois.fr)… 193.49.62.52
Connexion à cache-etu.univ-artois.fr (cache-etu.univ-artois.fr)|193.49.62.52|:3
128… connecté.
requête Proxy transmise, en attente de la réponse… 200 OK
Taille : 171 [binary/octet-stream]
Enregistre : ‘elasticsearch-8.10.4-linux-x86_64.tar.gz.sha512’

elasticsearch-8.10. 100%[==================>]     171  --.-KB/s    ds 0s

2025-01-23 16:51:13 (142 MB/s) - ‘elasticsearch-8.10.4-linux-x86_64.tar.gz.sha5
12’ enregistré [171/171]

root@rt-mv:/home/administrateur#
```

Vérification de l’intégrité du fichier

La **vérification de l’intégrité du fichier** et l'utilisation de la somme de contrôle SHA512 sont des étapes cruciales pour s'assurer que le fichier téléchargé n'est pas corrompu ou modifié.

```
root@rt-mv:/home/administrateur# shasum -a 512 -c elasticsearch-8.10.4-linux-x8
6_64.tar.gz.sha512
elasticsearch-8.10.4-linux-x86_64.tar.gz: OK
root@rt-mv:/home/administrateur#
```

Résultat : message `OK`, confirmant que l’archive est intacte et n’a pas été altérée

Extraction de l’archive

Ensuite l’extraction d'une archive avec la commande tar pour accéder aux fichiers compressés dans des formats comme `.tar.gz`.

```
root@rt-mv:/home/administrateur# tar -xzf elasticsearch-8.10.4-linux-x86_64.tar
.gz
root@rt-mv:/home/administrateur#
```

```
root@rt-mv:/home/administrateur/elasticsearch-8.10.4# wget https://artifacts.el
astic.co/downloads/elasticsearch/elasticsearch-8.10.4-amd64.deb
--2025-01-23 17:06:50--  https://artifacts.elastic.co/downloads/elasticsearch/e
lasticsearch-8.10.4-amd64.deb
Résolution de cache-etu.univ-artois.fr (cache-etu.univ-artois.fr)… 193.49.62.52
Connexion à cache-etu.univ-artois.fr (cache-etu.univ-artois.fr)|193.49.62.52|:3
128… connecté.
requête Proxy transmise, en attente de la réponse… 200 OK
Taille : 611691748 (583M) [binary/octet-stream]
Enregistre : ‘elasticsearch-8.10.4-amd64.deb’

elasticsearch-8.10. 100%[==================>] 583,35M  10,7MB/s    ds 52s

2025-01-23 17:07:43 (11,3 MB/s) - ‘elasticsearch-8.10.4-amd64.deb’ enregistré [
611691748/611691748]

root@rt-mv:/home/administrateur/elasticsearch-8.10.4# sudo dpkg -i elasticsearc
h-8.10.4-amd64.deb
Sélection du paquet elasticsearch précédemment désélectionné.
(Lecture de la base de données... 208063 fichiers et répertoires déjà installés
.)
Préparation du dépaquetage de elasticsearch-8.10.4-amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Dépaquetage de elasticsearch (8.10.4) ...
Paramétrage de elasticsearch (8.10.4) ...
--------------------------- Security autoconfiguration information ------------
```

Résultat : les fichiers d’Elasticsearch ont été extraits dans le répertoire correspondant.

Configuration d’Elasticsearch

1. Accès au répertoire d’Elasticsearch

```
Afficher les applications nistrateur# cd elasticsearch-8.10.4/
root@rt-mv:/home/administrateur/elasticsearch-8.10.4#
```

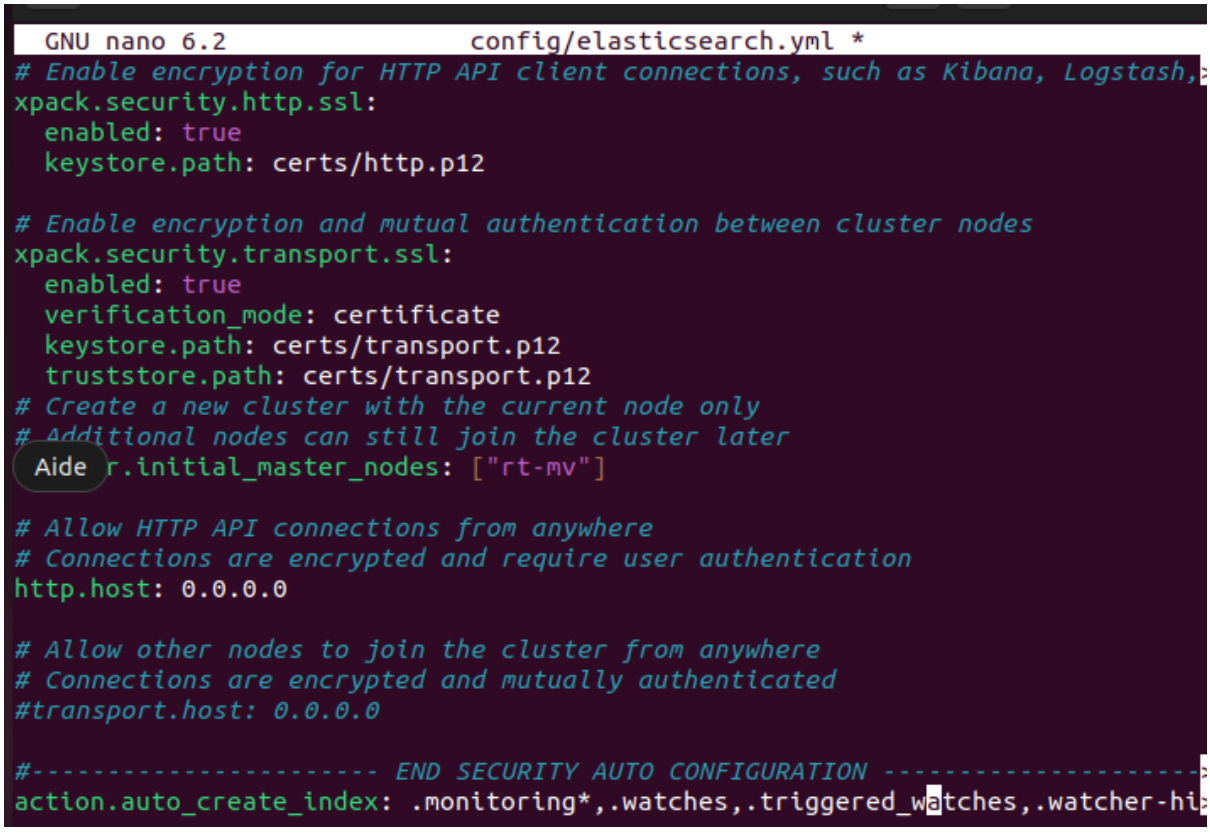
Ensuite Je me déplace sur le répertoire --- > cd elasticsearch-8.10.4

Puis éditer le fichier de configuration principal d'Elasticsearch pour ajuster certains paramètres avant son démarrage.

Ce fichier contient les paramètres essentiels pour la configuration d'Elasticsearch, notamment :

- Les options de cluster.
- Les paramètres de réseau.
- La gestion des indices.

nano config/elasticsearch.yml



action.auto_create_index: . monitoring*,.watches,.triggered_watches,.watcher-history*,.ml*

Cela garantit que seuls ces indices spécifiques peuvent être créés automatiquement, tout en désactivant la création automatique pour d'autres indices. C'est utile pour éviter la prolifération d'indices non désirés.

2. Activation du service

Activez le service pour qu'il démarre au démarrage, démarrage Elasticsearch et Vérifiez l'état du service

```
root@rt-mv:/home/administrateur/elasticsearch-8.10.4# sudo systemctl enable ela
sticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.servi
ce → /lib/systemd/system/elasticsearch.service.
root@rt-mv:/home/administrateur/elasticsearch-8.10.4#
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.servi
ce → /lib/systemd/system/elasticsearch.service.
root@rt-mv:/home/administrateur/elasticsearch-8.10.4# sudo systemctl start elas
ticsearch
root@rt-mv:/home/administrateur/elasticsearch-8.10.4#
```

```
root@rt-mv:/home/administrateur/elasticsearch-8.10.4# sudo systemctl status ela
sticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendo>
     Active: active (running) since Thu 2025-01-23 17:11:26 CET; 1min 3s ago
       Docs: https://www.elastic.co
   Main PID: 37868 (java)
      Tasks: 73 (limit: 2878)
     Memory: 1.5G
        CPU: 40.231s
     CGroup: /system.slice/elasticsearch.service
             ├─37868 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:>
             ├─37926 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress>
             └─37946 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux>

janv. 23 17:11:05 rt-mv systemd[1]: Starting Elasticsearch...
janv. 23 17:11:08 rt-mv systemd-entrypoint[37868]: janv. 23, 2025 5:11:08 PM s>
janv. 23 17:11:08 rt-mv systemd-entrypoint[37868]: WARNING: COMPAT locale prov>
janv. 23 17:11:26 rt-mv systemd[1]: Started Elasticsearch.
lines 1-17/17 (END)
```

3. Configuration des droits

S'assurer que l'utilisateur actuel a les droits nécessaires pour lire et exécuter les fichiers même en root.

sudo chown -R administrateur:administrateur /home/administrateur/elasticsearch-8.10.4
sudo chmod -R u+rwx /home/administrateur/elasticsearch-8.10.4

Exécution Elasticsearch

```
✅ Elasticsearch security features have been automatically configured!
✅ Authentication is enabled and cluster connections are encrypted.

ℹ️  Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):
  dhnekYVehgL7+Tjbewwv

ℹ️  HTTP CA certificate SHA-256 fingerprint:
  9666e2755a2c2aeef31b66cfc22245fe2bc0440bc431cc88f00a06005d70eb13

ℹ️  Configure Kibana to use this cluster:
• Run Kibana and click the configuration link in the terminal when Kibana starts.
• Copy the following enrollment token and paste it into Kibana in your browser (valid for the next 30 minutes):
  eyJ2ZXIiOiI4LjEwLjQiLCJhZHIiOlsiMTcyLjMxLjE5LjU0OjkyMDAiXSwiZmdyIjoiOTY2NmUyNzU1YTJjMmFlZWYzMWI2NmNmYzIyMjQ1ZmUyYmMwNDQwYmM0MzFjYzg4ZjAwYTA2MDA1ZDcwZWIxMyIsImtleSI6ImY2cWlsNVFCV1I3MUY1dFFBa055Okt4M3c2YzNlUnl1RFB5SHlrQWFYZFEifQ==

ℹ️  Configure other nodes to join this cluster:
• On this node:
  - Create an enrollment token with `bin/elasticsearch-create-enrollment-token -s node`.
  - Uncomment the transport.host setting at the end of config/elasticsearch.yml.
  - Restart Elasticsearch.
• On other nodes:
  - Start Elasticsearch with `bin/elasticsearch --enrollment-token <token>`, using the enrollment token that you generated.
```

✅ Elasticsearch security features have been automatically configured!

✅ Authentication is enabled and cluster connections are encrypted.

ℹ️ Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):

dhnekYVehgL7+Tjbewwv

ℹ️ HTTP CA certificate SHA-256 fingerprint:
9666e2755a2c2aeef31b66cfc22245fe2bc0440bc431cc88f00a06005d70eb13

ℹ️ Configure Kibana to use this cluster:
• Run Kibana and click the configuration link in the terminal when Kibana starts.

- Copy the following enrollment token and paste it into Kibana in your browser (valid for the next 30 minutes):

eyJ2ZXIiOiI4LjEwLjQiLCJhZHIiOlsiMTcyLjMxLjE5LjU0OjkyMDAiXSwiZmdyIjoiOTY2NmUyN
zU1YTJjMmFlZWYzMWI2NmNmYzIyMjQ1ZmUyYmMwNDQwYmM0MzFjYzg4ZjAwYTA2MDA1ZDcwZWIxMyIsImtleSI6ImY2cWlsNVFCV1I3MUY1dFFBa055Okt4M3c2YzNlUnl1RFB5 SHlrQWFYZFEifQ==

- Les fonctionnalités de sécurité d'Elasticsearch ont été configurées automatiquement.
- L'authentification est activée, et les connexions au cluster sont sécurisées.

Le mot de passe pour l'utilisateur par défaut (`elastic`) a été généré automatiquement :
dhnekYVehgL7+Tjbewwv

Toutes les étapes ont été réalisées sans erreurs, comme le montrent les messages dans le terminal.

Les étapes initiales de téléchargement, vérification et extraction ont permis de préparer l’environnement pour Elasticsearch. L’étape suivante consistera à configurer et lancer Elasticsearch, puis vérifier son bon fonctionnement.

curl -u elastic:dhnekYVehgL7+Tjbewwv https://localhost:9200 -k

```
administrateur@rt-mv:~/elasticsearch-8.10.4$ curl -u elastic:dhnekYVehgL7+Tjbewwv https://localhost:9200 -k
{
  "name" : "rt-mv",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "KeEaSPymQUSPUxznvTtAYQ",
  "version" : {
    "number" : "8.10.4",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "b4a62ac808e886ff032700c391f45f1408b2538c",
    "build_date" : "2023-10-11T22:04:35.506990650Z",
    "build_snapshot" : false,
    "lucene_version" : "9.7.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
administrateur@rt-mv:~/elasticsearch-8.10.4$
```

C’est quoi Kibana

Kibana est un outil open-source de visualisation et d'analyse de données conçu pour fonctionner avec **Elasticsearch**, une base de données puissante utilisée pour la recherche et l'analyse.

Rapport entre Elasticsearch et Kibana

Kibana et Elasticsearch sont étroitement liés et fonctionnent ensemble comme des composants complémentaires de la **suite Elastic Stack**.

- **Kibana dépend d’Elasticsearch :**

Sans Elasticsearch, Kibana ne peut pas fonctionner, car il n’a pas de données à afficher ou analyser.
Kibana envoie des requêtes à Elasticsearch pour récupérer les données.

- **Interface pour Elasticsearch :**

Elasticsearch est puissant mais fonctionne principalement via des API REST et des requêtes en JSON. Kibana simplifie ce processus avec une interface intuitive.

> Exemple : Au lieu d’écrire une requête complexe en JSON pour chercher des logs, tu peux utiliser Kibana pour filtrer ou cliquer sur un bouton.

- **Visualisation des résultats d'Elasticsearch :**

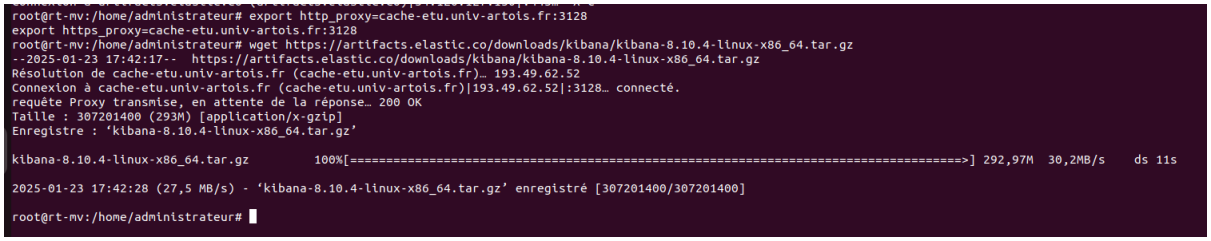
Elasticsearch analyse les données, mais les résultats sont souvent difficilement lisibles sous leur forme brute. Kibana présente ces résultats sous forme de graphiques, de cartes ou de tableaux.

Téléchargement des fichiers d’installation

Je vais décrire le processus d’installation de Kibana, composant central de la suite Kibana, sur un système Ubuntu.

Récupérer l'archive d’installation :

Je vais utiliser la commande `wget` pour récupérer des fichiers depuis un serveur distant sur Internet.



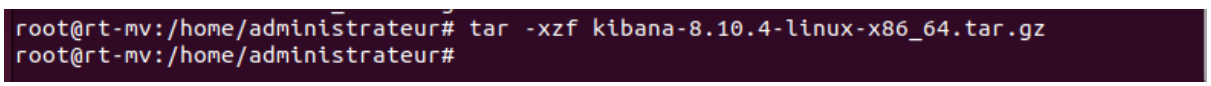
Vérification de l’intégrité du fichier

La **vérification de l’intégrité du fichier** et l'utilisation de la somme de contrôle SHA512 sont des étapes cruciales pour s'assurer que le fichier téléchargé n'est pas corrompu ou modifié.

Résultat : message `OK`, confirmant que l’archive est intacte et n’a pas été altérée

Extraction de l’archive

Ensuite l’extraction d'une archive avec la commande tar pour accéder aux fichiers compressés dans des formats comme `.tar.gz`.



Résultat : les fichiers de kibana ont été extraits dans le répertoire correspondant.

Accès au répertoire de Kibana

Ensuite Je me déplace sur le répertoire ----> cd kibana-8.10.4/

```
root@rt-mv:/home/administrateur# cd kibana-8.10.4/
root@rt-mv:/home/administrateur/kibana-8.10.4#
```

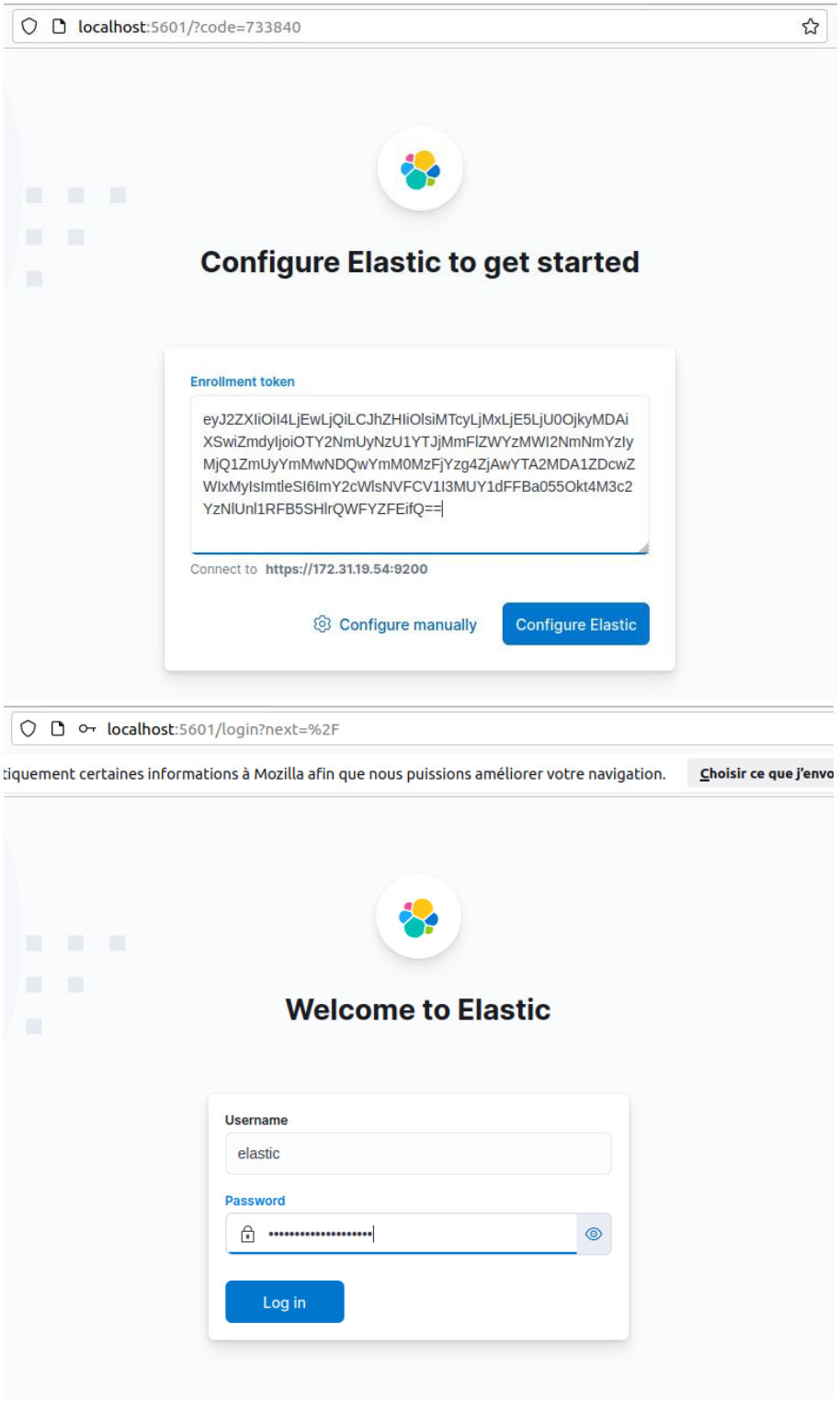
Exécution de Kibana

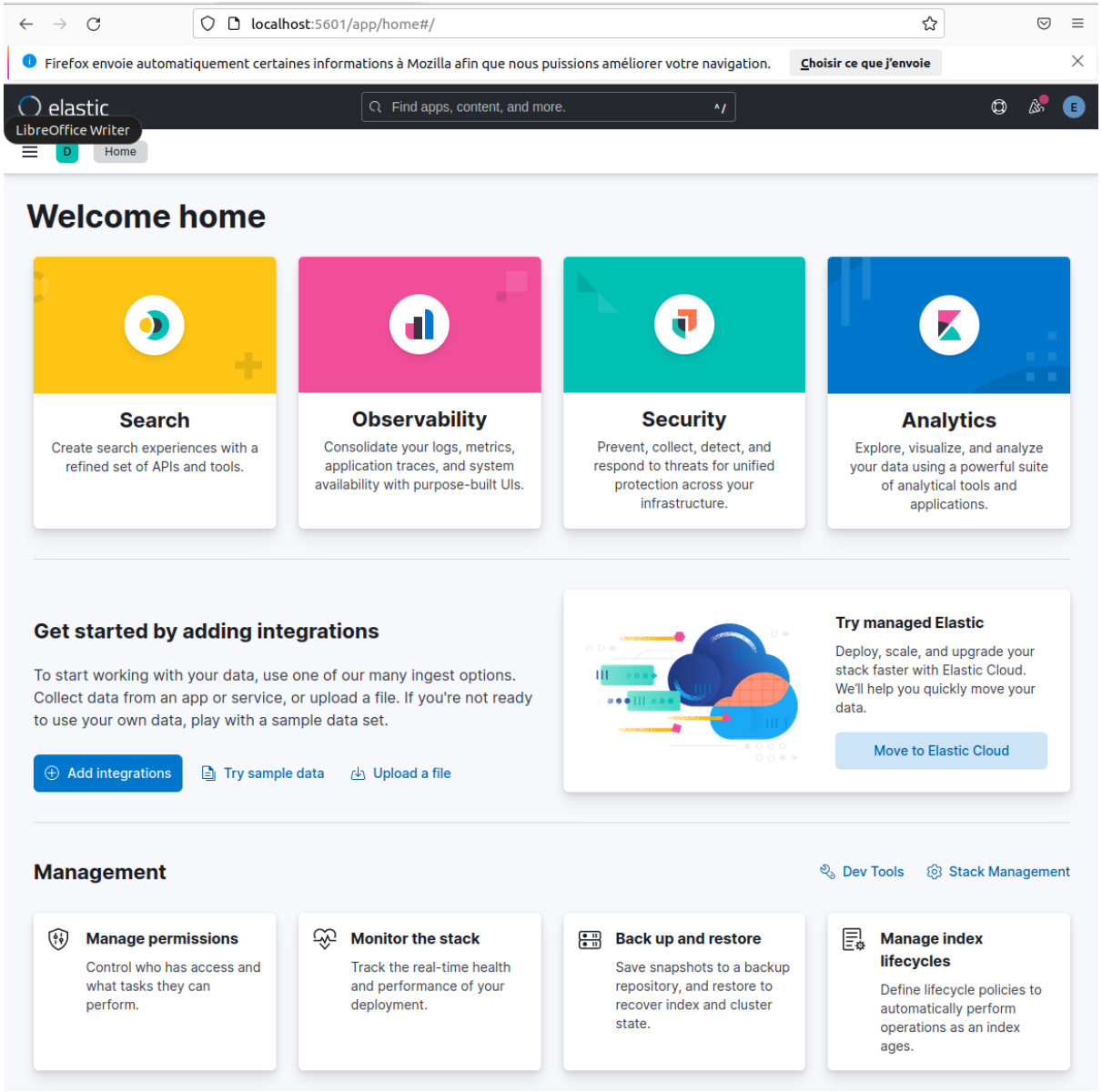
La commande utilisée est : `./bin/kibana`, que Kibana est démarré manuellement à partir du répertoire

```
administrateur@rt-mv:~/kibana-8.10.4$ ./bin/kibana
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://ww
w.elastic.co/guide/en/kibana/8.10/production.html#openssl-legacy-provider
{"log.level":"info","@timestamp":"2025-01-24T09:50:47.224Z","log":{"logger":"elastic-apm-node"},"agentVersion":"3.49.1","env":{"
pid":6707,"proctitle":"./bin/../node/bin/node","os":"linux 5.19.0-35-generic","arch":"x64","host":"rt-mv","timezone":"UTC+0100",
"runtime":"Node.js v18.17.1"},"config":{"serviceName":{"source":"start","value":"kibana","commonName":"service_name"},"serviceVe
rsion":{"source":"start","value":"8.10.4","commonName":"service_version"},"serverUrl":{"source":"start","value":"https://kibana-
cloud-apm.apm.us-east-1.aws.found.io/","commonName":"server_url"},"logLevel":{"source":"default","value":"info","commonName":"lo
g_level"},"active":{"source":"start","value":true},"contextPropagationOnly":{"source":"start","value":true},"environment":{"sour
ce":"start","value":"production"},"logUncaughtExceptions":{"source":"start","value":true},"globalLabels":{"source":"start","valu
e":[["git_rev","976088dd04c6fd3b907fd2bb92af306e7d77ce4c"]],"sourceValue":{"git_rev":"976088dd04c6fd3b907fd2bb92af306e7d77ce4c"}
},"secretToken":{"source":"start","value":"[REDACTED]","commonName":"secret_token"},"breakdownMetrics":{"source":"start","value"
:false},"captureSpanStackTraces":{"source":"start","sourceValue":false},"centralConfig":{"source":"start","value":false},"metric
sInterval":{"source":"start","value":120,"sourceValue":"120s"},"propagateTracestate":{"source":"start","value":true},"transactio
nSampleRate":{"source":"start","value":0.1,"commonName":"transaction_sample_rate"},"captureBody":{"source":"start","value":"off"
,"commonName":"capture_body"},"captureHeaders":{"source":"start","value":false}},"activationMethod":"require","ecs":{"version":"
1.6.0"},"message":"Elastic APM Node.js Agent v3.49.1"}
[2025-01-24T10:50:50.025+01:00][INFO ][root] Kibana is starting
[2025-01-24T10:50:50.199+01:00][INFO ][node] Kibana process configured with roles: [background_tasks, ui]
[2025-01-24T10:51:12.433+01:00][INFO ][plugins-service] Plugin "cloudChat" is disabled.
[2025-01-24T10:51:12.439+01:00][INFO ][plugins-service] Plugin "cloudExperiments" is disabled.
[2025-01-24T10:51:12.439+01:00][INFO ][plugins-service] Plugin "cloudFullStory" is disabled.
[2025-01-24T10:51:12.440+01:00][INFO ][plugins-service] Plugin "cloudGainsight" is disabled.
[2025-01-24T10:51:12.599+01:00][INFO ][plugins-service] Plugin "profiling" is disabled.
[2025-01-24T10:51:12.650+01:00][INFO ][plugins-service] Plugin "securitySolutionServerless" is disabled.
[2025-01-24T10:51:12.650+01:00][INFO ][plugins-service] Plugin "serverless" is disabled.
[2025-01-24T10:51:12.650+01:00][INFO ][plugins-service] Plugin "serverlessObservability" is disabled.
[2025-01-24T10:51:12.651+01:00][INFO ][plugins-service] Plugin "serverlessSearch" is disabled.
[2025-01-24T10:51:12.960+01:00][INFO ][http.server.Preboot] http server running at http://localhost:5601
[2025-01-24T10:51:13.122+01:00][INFO ][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
[2025-01-24T10:51:13.124+01:00][INFO ][preboot] "interactiveSetup" plugin is holding setup: Validating Elasticsearch connection
configuration…
[2025-01-24T10:51:13.165+01:00][INFO ][root] Holding setup until preboot stage is completed.


i Kibana has not been configured.

Go to http://localhost:5601/?code=733840 to get started.
```

Le navigateur ouvert sur http://localhost:5601.

- Cette page correspond à l’interface graphique de Kibana.
- Une invite initiale est visible, permettant de configurer Kibana et de l'associer à un cluster Elasticsearch.





C’est quoi Logstash

Logstash est un outil open-source de la suite Elastic conçu pour **ingérer, transformer et envoyer des données** vers Elasticsearch ou d'autres destinations.

Il agit comme un **pipeline de traitement de données** qui collecte des données de plusieurs sources, les transforme (via des filtres), puis les transmet à une destination (généralement Elasticsearch).

Rapport entre Logstash et Elasticsearch

- **Traitement des données avant indexation :**

Logstash nettoie, structure et transforme les données avant de les envoyer à Elasticsearch.

- Exemple : Si tu as des fichiers journaux non structurés, Logstash peut les formater en JSON pour qu'Elasticsearch puisse les indexer correctement.

- **Sources multiples :**

Elasticsearch est puissant, mais il n'ingère pas directement toutes les données. Logstash agit comme un **intermédiaire**, capable de collecter des données de plusieurs sources, de les harmoniser, puis de les transmettre à Elasticsearch.

- **Pipeline de traitement :**

Logstash rend le projet plus flexible, permettant d'ajouter des étapes de traitement, comme la détection d'erreurs ou l'ajout de nouvelles données contextuelles avant l'analyse dans Elasticsearch.

Pourquoi intégrer Logstash dans ton projet ?

Logstash serait particulièrement utile si ton projet traite :

Des logs ou journaux non structurés : par exemple, des fichiers journaux d'applications ou des logs réseau.

Des sources multiples de données : comme des bases de données, des fichiers CSV, ou des métriques système.

Des pipelines complexes : où les données doivent être enrichies, nettoyées ou regroupées avant d'être indexées dans Elasticsearch.

Installation et configuration de Logstash

```
administrateur@rt-mv:~/kibana-8.10.4$ sudo apt-get update && sudo apt-get install logstash
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Réception de :2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10,4 kB]
Réception de :3 https://artifacts.elastic.co/packages/8.x/apt stable/main i386 Packages [6 730 B]
Réception de :4 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [133 kB]
Atteint :5 http://security.ubuntu.com/ubuntu jammy-security InRelease
150 ko réceptionnés en 1s (124 ko/s)
Lecture des listes de paquets... Fait
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  dns-root-data
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les NOUVEAUX paquets suivants seront installés :
  logstash
0 mis à jour, 1 nouvellement installés, 0 à enlever et 4 non mis à jour.
Il est nécessaire de prendre 436 Mo dans les archives.
Après cette opération, 715 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.17.1-1 [436 MB]
436 Mo réceptionnés en 21s (20,4 Mo/s)
Sélection du paquet logstash précédemment désélectionné.
(Lecture de la base de données... 208074 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../logstash_1%3a8.17.1-1_amd64.deb ...
Dépaquetage de logstash (1:8.17.1-1) ...
Paramétrage de logstash (1:8.17.1-1) ...
administrateur@rt-mv:~/kibana-8.10.4$ service logstash start
administrateur@rt-mv:~/kibana-8.10.4$ service logstash status
● logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; disabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-01-24 11:23:30 CET; 10s ago
   Main PID: 40311 (java)
      Tasks: 21 (limit: 2878)
     Memory: 329.6M
        CPU: 15.683s
     CGroup: /system.slice/logstash.service
             └─40311 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.comp>

janv. 24 11:23:30 rt-mv systemd[1]: Started logstash.
janv. 24 11:23:30 rt-mv logstash[40311]: Using bundled JDK: /usr/share/logstash/jdk
lines 1-12/12 (END)
```

Ensuite voici les contenus des fichiers nécessaires pour recréer la configuration rapidement.

Fichier 1 : /etc/logstash/conf.d/02-beats-input.conf

```
  GNU nano 6.2                          /etc/logstash/conf.d/02-beats-input.conf *
input {
  beats {
    port => 5044
  }
}
```

Fichier 2 : **/etc/logstash/conf.d/30-elasticsearch-output.conf**

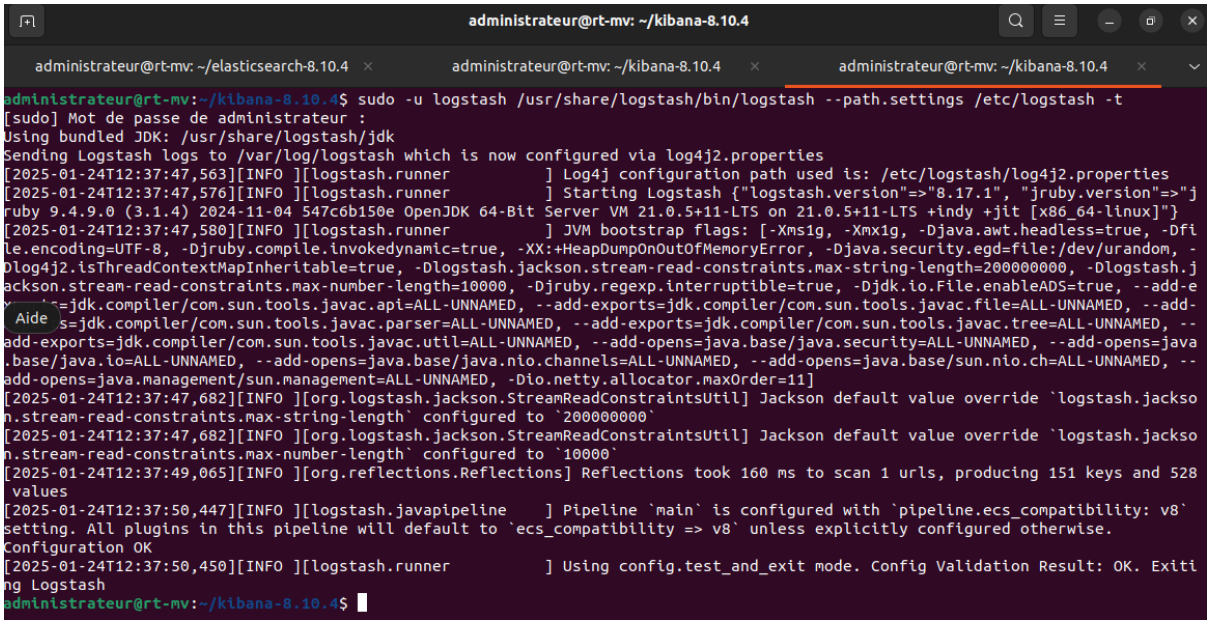
```
  GNU nano 6.2                        /etc/logstash/conf.d/30-elasticsearch-output.conf *
output {
  if [@metadata][pipeline] {
    elasticsearch {
      hosts => ["localhost:9200"]
      manage_template => false
      index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
      pipeline => "%{[@metadata][pipeline]}"
    }
  } else {
    elasticsearch {
      hosts => ["localhost:9200"]
      manage_template => false
      index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    }
  }
}
```

Ensuite nous procédons à :

L'exécution de Logstash en utilisant l'utilisateur `logstash` ;

Charger les paramètres et configurations définis dans `/etc/logstash` ;

Vérifier (sans démarrer Logstash) si la configuration est valide et renvoie les erreurs éventuelles.



Puis :

Redémarrer le service Logstash. Avec **`service logstash restart`**

Activer le démarrage automatique du service Logstash au démarrage du système avec **`service logstash enable`**