# Module majeur

## ELK : c’est quoi ?

ELK est un ensemble de 3 outils qui travaillent ensemble pour gérer des logs (messages d’activité des applis, serveurs, etc.) :

1. Elasticsearch (E)
   → la base de données spécialisée dans la recherche.
   Il stocke les logs et permet de les retrouver hyper vite (par mot, par date, par champ, etc.).
2. Logstash (L)
   → le tuyau d’ingestion.
   Il reçoit des logs (par TCP, fichiers, etc.), les transforme (ajoute des champs, formate les dates…) et les envoie dans Elasticsearch.
3. Kibana (K)
   → l’interface web.
   Il se connecte à Elasticsearch pour afficher les logs sous forme de tableaux, graphiques, dashboards, etc.

## Comment ça s’articule

**Imagine un pipeline :**

**Applications / Services → Logstash → Elasticsearch → Kibana**

- **Les applis écrivent des logs (ex : {"msg":"erreur sur le serveur"}).**
- **Logstash reçoit ces logs (ici sur le port 5000), les nettoie (ajoute @timestamp, service, etc.) et les envoie dans Elasticsearch.**
- **Elasticsearch les range dans des “index” (comme des dossiers horodatés, ex : ftt-logs-2025.09.02).**
- **Kibana vient lire ces index et te permet de chercher, filtrer, et visualiser.**

## Commencer lancer un dashboard

- Apres un make, aller sur le navigateur : http://localhost:5601 (**Utilisateur** : `elastic` **Mot de passe** : `elastic`)
- Menu général sur la gauche, tout en bas : `Management / Stack Management`
- Toujours sur le menu de gauche en bas : `Kibana / Save objects`
- `Import`
- Importer `ft_transcendence/elk/export.ndjson`
- Aller dans le menu général `Analytics / Dashboard`

***User et mots de passe***

*Elasticsearch :*

***User : elastic  Mdp : elastic***

***Kibana** Il sert uniquement en interne **User kibana_system  mdp : kibana***

## Comment tester chaque service

# 1) Elasticsearch

Navigateur : `http://localhost:9200`

Terminal :

```
curl -u elastic:elastic http://localhost:9200/_cluster/health?pretty
```

✅ tu vois un JSON avec `"status":"yellow"` ou `"green"`.
❌ problème Elasticsearch (regarde `docker compose ps` et `docker compose logs elasticsearch`).

## 2) Kibana

Vérifier que Kibana est en ligne :

Navigateur : http://localhost:5601 (**Utilisateur** : `elastic`  **Mot de passe** : `elastic`)

`Terminal : curl -i http://localhost:5601/status`

❌ Si ça échoue → regarde les logs : `docker compose logs -f kibana`

## 3) Logstash

Terminal :

Tester que Logstash écoute bien sur le port TCP 5000 :

```
nc -v localhost 5000
```

✅ Réponse `succeeded!` → le port est ouvert.

Envoyer un log de test :

```
printf
'{"ts":"2025-09-02T12:00:00Z","service":"demo","env":"dev","level":"
info","msg":"hello logstash"}\n' \
```

```
| nc -v localhost 5000
```

Puis vérifier dans Elasticsearch que le log est bien indexé :

```
curl -u elastic:elastic 'http://localhost:9200/_cat/indices?v'
```

```
curl -u elastic:elastic
'http://localhost:9200/ftt-logs-*/_search?size=1&sort=@timestamp:des
c&pretty'
```

✅ Si ça marche → tu vois un index `ftt-logs-YYYY.MM.dd` et le dernier document inséré.
❌ Si ça échoue → regarde les logs de Logstash :

```
docker compose logs -f logstash
```

## 🛠️ Diagnostic rapide (en cas de souci)

1. **Qui tourne ?**

```
docker compose ps
```

2. **Regarder les logs**

```
docker compose logs -f elasticsearch
```

```
docker compose logs -f kibana
```

```
docker compose logs -f logstash
```

→ Les erreurs y sont en clair (auth, mot de passe, crash JVM, etc.).

3. **Tester l'auth**

Avec `elastic/elastic` :

```
curl -u elastic:elastic
http://localhost:9200/_security/_authenticate?pretty
```

- doit renvoyer `username":"elastic"`.

Avec `kibana_system/kibana` :

```
curl -u kibana_system:kibana
http://localhost:9200/_security/_authenticate?pretty
```

- doit renvoyer `username":"kibana_system"`.

## 📌 Résumé en 3 commandes

**ES OK ?**

```
curl -u elastic:elastic http://localhost:9200/_cluster/health?pretty
```

**Kibana OK ?**

```
curl -i http://localhost:5601/status
```

**Logstash OK ?**

```
printf '{"msg":"hello"}\n' | nc -v localhost 5000
```

```
curl -u elastic:elastic 'http://localhost:9200/ftt-logs-*/_search?size=1&sort=@timestamp:desc&pretty'
```