TP pour analyser les Logs avec Elasticsearch
Nom Complet : Sghiri Samir

Étape 1 : Lancer Elasticsearch avec Docker :

1) **Créez un fichier `docker-compose.yml` avec le contenu suivant :**

```yaml
version: '3'
services:
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.14.2
    container_name: elasticsearch
    environment:
      - discovery.type=single-node
      - xpack.security.enabled=false
      - xpack.security.transport.ssl.enabled=false
    ports:
      - "9200:9200"
      - "9300:9300"
    networks:
      - elastic
  kibana:
    image: docker.elastic.co/kibana/kibana:8.14.2
    container_name: kibana
    ports:
      - "5601:5601"
    environment:
      - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
    networks:
      - elastic
networks:
  elastic:
    driver: bridge
```

2) **Lancez Elasticsearch avec la commande suivante :**

docker-compose up -d

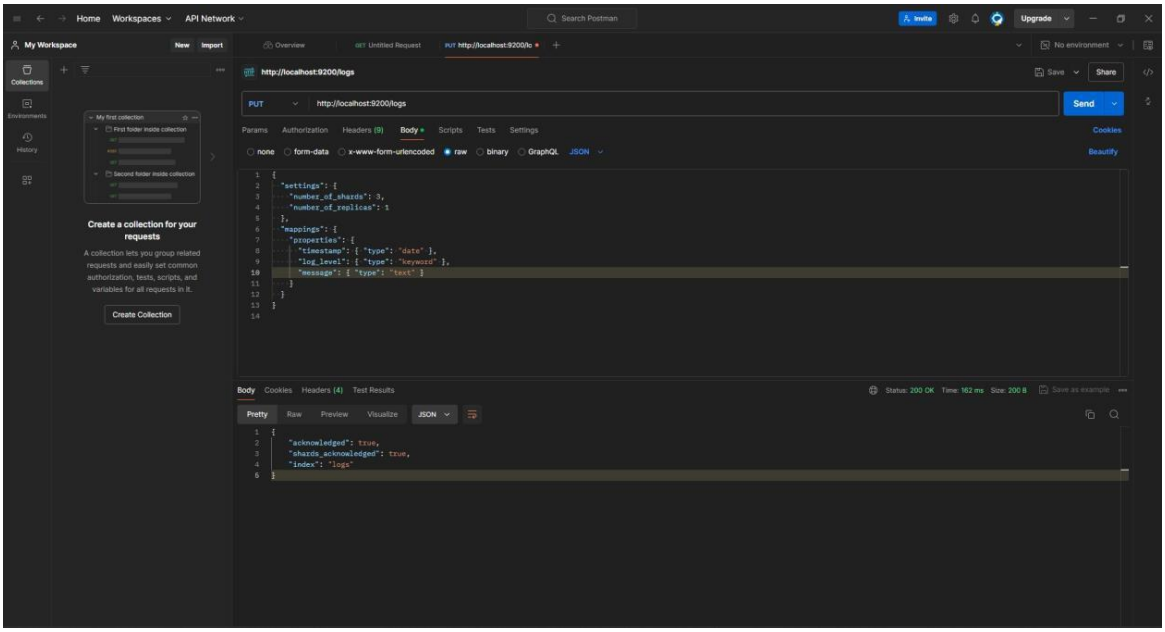
Étape 2 : Créer un Index "logs" :

1) **Créer un nouvel index "logs" :**

- Méthode : PUT

- URL : `http://localhost:9200/logs`
- Body :

```
{
"settings": {
"number_of_shards": 3,
"number_of_replicas": 1
},
"mappings": {
"properties": {
"timestamp": { "type": "date" },
"log_level": { "type": "keyword" },
"message": { "type": "text" }
}
}
}
```



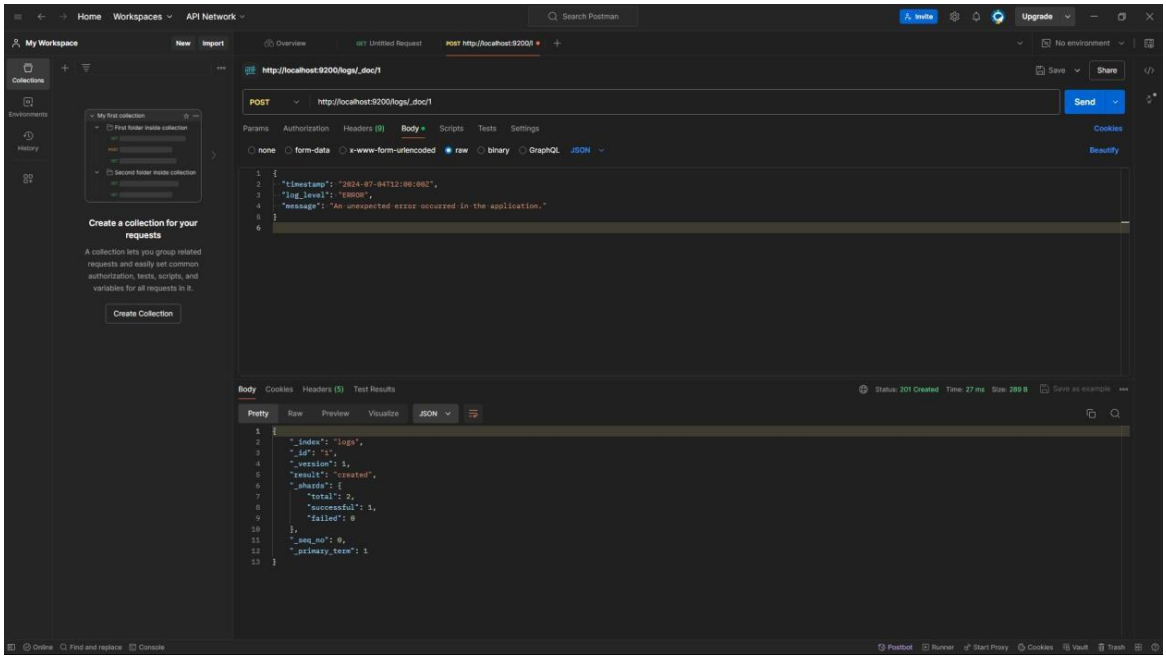
Étape 3 : Indexer des Logs :

1) Indexer un log d'erreur :

- Méthode : POST
- URL : `http://localhost:9200/logs/_doc/1`
- Body :

```
{
"timestamp": "2024-07-04T12:00:00Z",
"log_level": "ERROR",
```

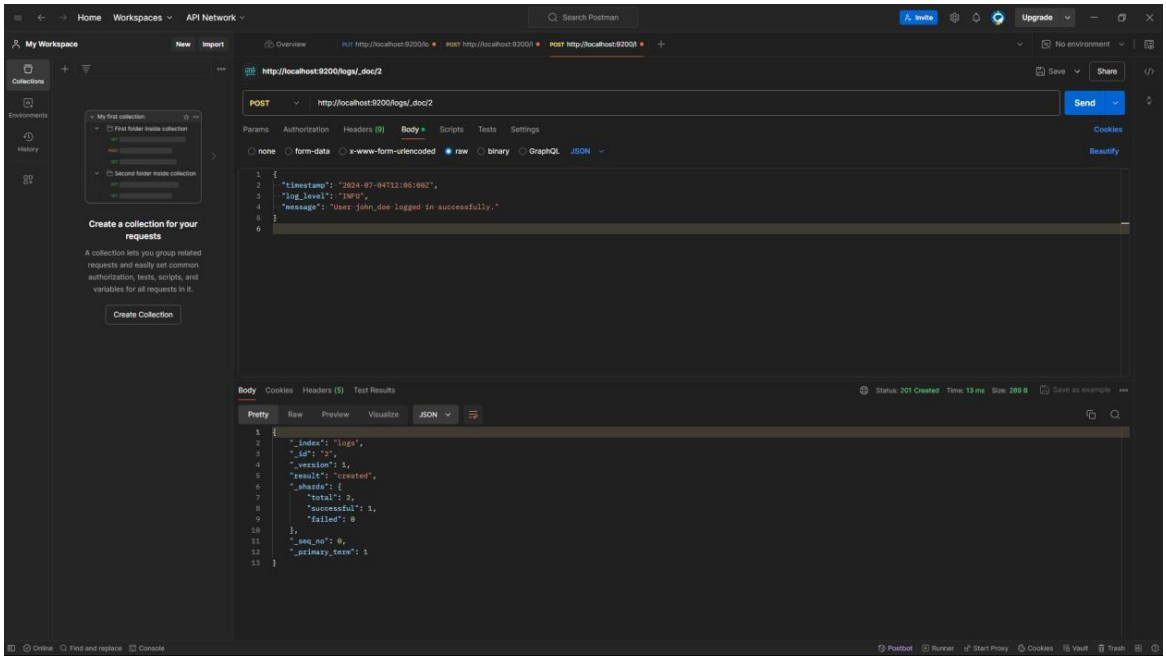
"message": "An unexpected error occurred in the application."
}



2) Indexer un log d'information :

- Méthode : POST
- URL : `http://localhost:9200/logs/_doc/2`
- Body :

{
"timestamp": "2024-07-04T12:05:00Z",
"log_level": "INFO",
"message": "User john_doe logged in successfully."
}

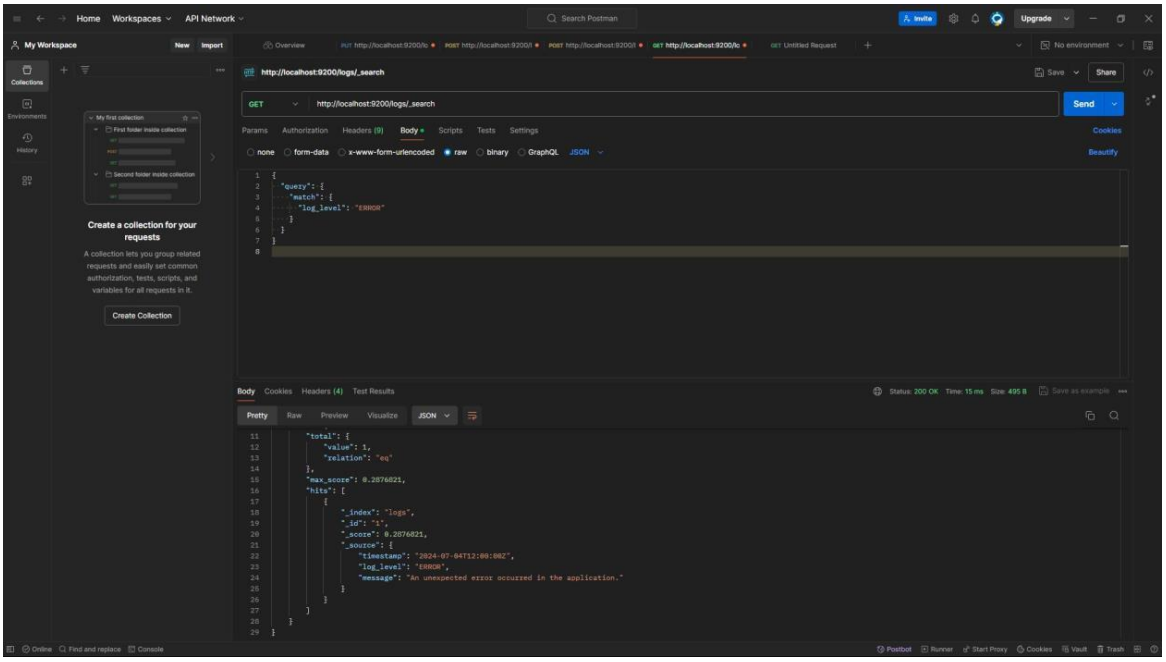


Étape 4 : Rechercher des Logs :

1) **Rechercher des logs par niveau de log :**

- Méthode : GET
- URL : `http://localhost:9200/logs/_search`
- Body :

```
{
"query": {
"match": {
"log_level": "ERROR"
}
}
}
```

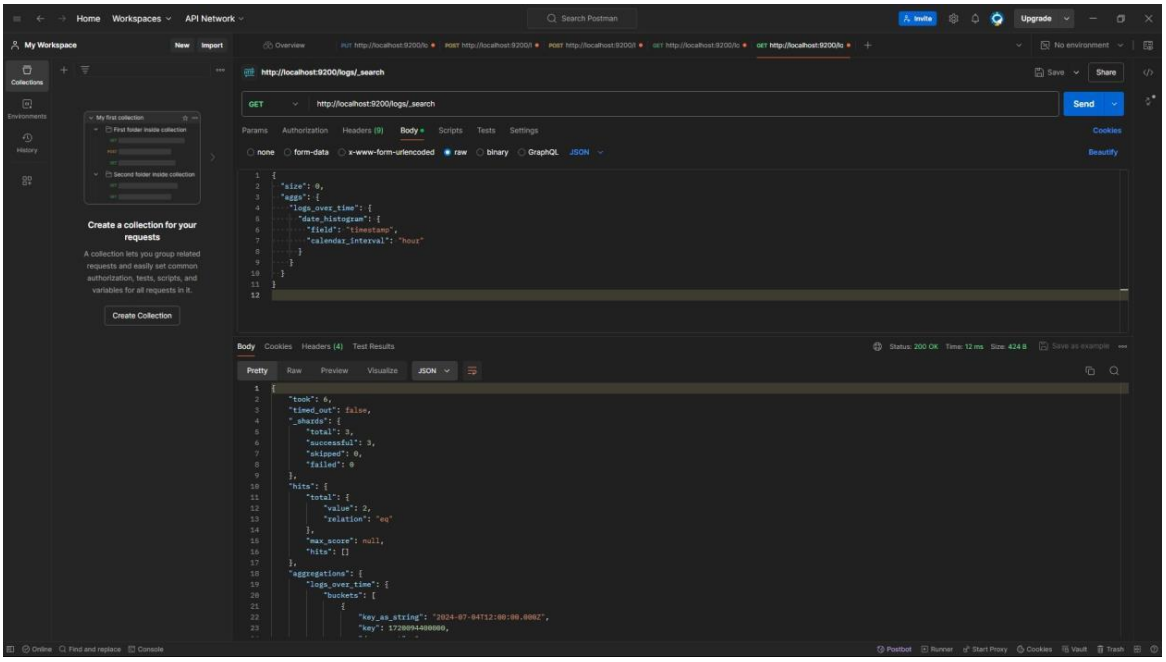


Étape 5 : Agrégations :

1) Histogramme de Dates : Regrouper les logs par date et heure.

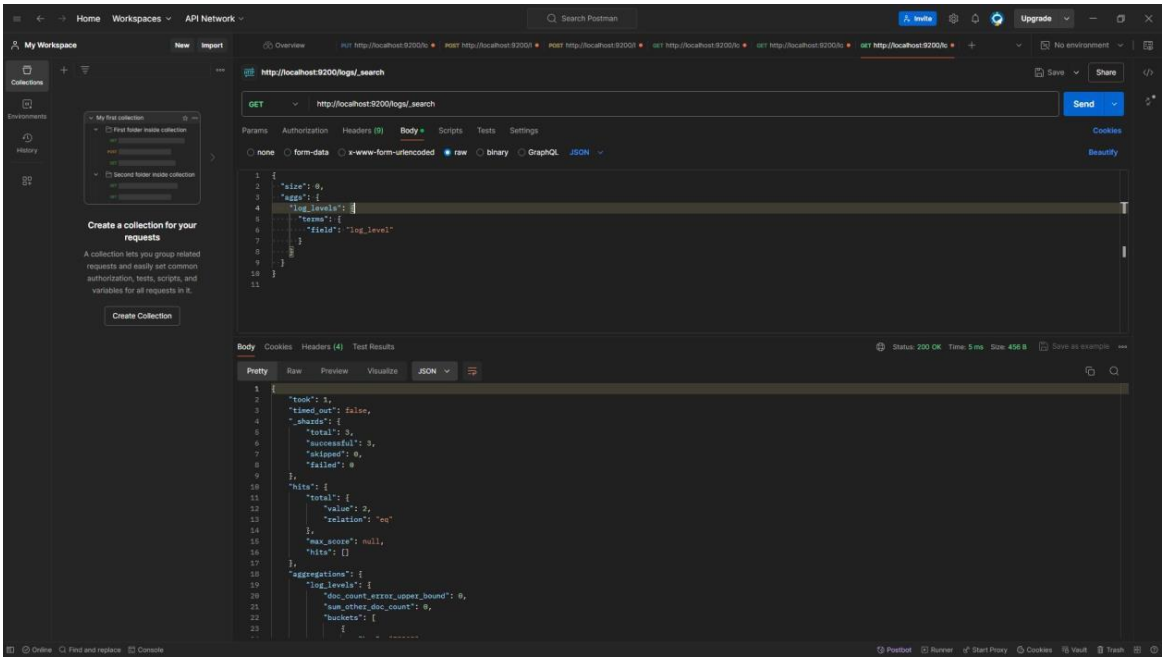
- Méthode : GET
- URL : `http://localhost:9200/logs/_search`
- Body :

```
{
"size": 0,
"aggs": {
"logs_over_time": {
"date_histogram": {
"field": "timestamp",
"calendar_interval": "hour"
}
}
}
}
```



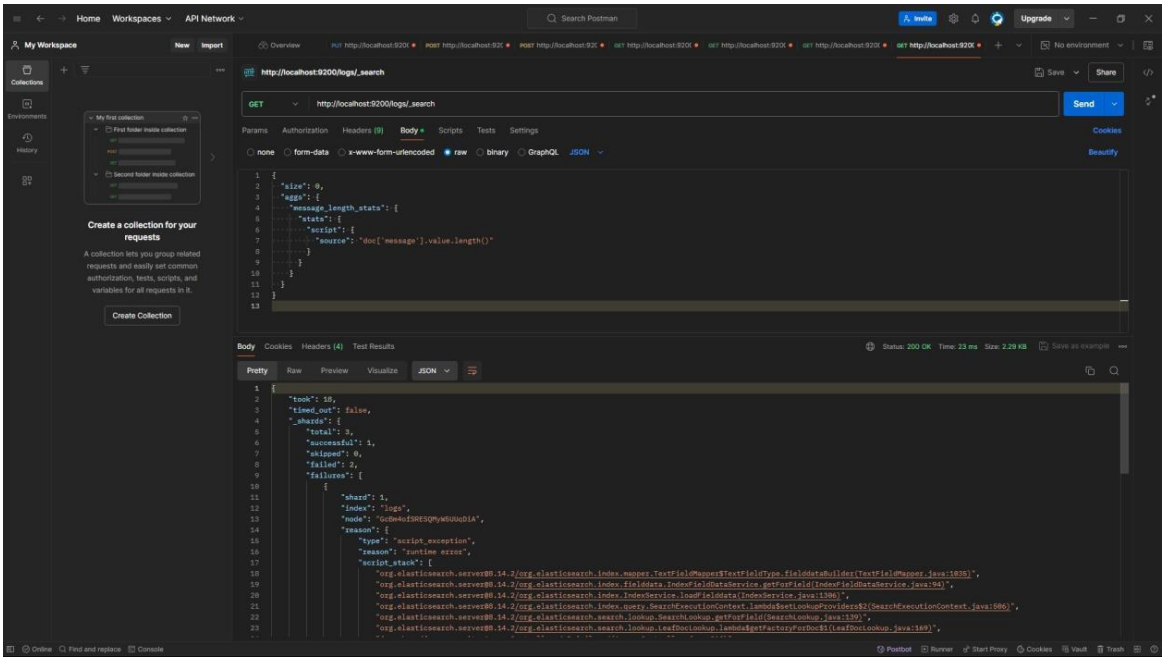
2) **Fréquence des Niveaux de Log : Compter le nombre de logs par niveau de log.**
   - Méthode : GET
   - URL : `http://localhost:9200/logs/_search`
   - Body :

```
{
"size": 0,
"aggs": {
"log_levels": {
"terms": {
"field": "log_level"
}
}
}
}
```



3) **Statistiques sur la Longueur des Messages : Calculer les statistiques sur la longueur des messages de logs.**
    - Méthode : GET
    - URL : `http://localhost:9200/logs/_search`
    - Body :

```
{
"size": 0,
"aggs": {
"message_length_stats": {
"stats": {
"script": {
"source": "doc['message'].value.length()"
}
}
}
}
}
```


Home
Workspaces
API Network
Search Postman
Invite
Upgrade
My Workspace
New
Import
Collections
Environments
History
Create a collection for your requests
A collection lets you group related requests and easily set common authorization, tests, scripts, and variables for all requests in it.
Create Collection
http://localhost:9200/logs/_search
GET
http://localhost:9200/logs/_search
Send
Save
Share
Params
Authorization
Headers (9)
Body
Scripts
Tests
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Beautify
{
"size": 0,
"aggs": {
"message_length_stats": {
"stats": {
"script": {
"source": "doc['message'].value.length()"
}
}
}
}
}
Body
Cookies
Headers (4)
Test Results
Status: 200 OK
Time: 23 ms
Size: 2.29 KB
Save as example
Pretty
Raw
Preview
Visualize
JSON
{
"took": 18,
"timed_out": false,
"_shards": {
"total": 2,
"successful": 1,
"skipped": 0,
"failed": 2,
"failures": [
{
"shard": 1,
"index": "logs",
"node": "GcBm4ofSRESQMyW5UUqDiA",
"reason": {
"type": "script_exception",
"reason": "runtime error",
"script_stack": [
"org.elasticsearch.server@8.14.2/org.elasticsearch.index.mapper.TextFieldMapper$TextFieldType.fielddataBuilder(TextFieldMapper.java:1035)",
"org.elasticsearch.server@8.14.2/org.elasticsearch.index.fielddata.IndexFieldDataService.getForField(IndexFieldDataService.java:94)",
"org.elasticsearch.server@8.14.2/org.elasticsearch.index.IndexService.loadFielddata(IndexService.java:1306)",
"org.elasticsearch.server@8.14.2/org.elasticsearch.index.query.SearchExecutionContext.lambda$setLookupProviders$2(SearchExecutionContext.java:686)",
"org.elasticsearch.server@8.14.2/org.elasticsearch.search.lookup.SearchLookup.getForField(SearchLookup.java:129)",
"org.elasticsearch.server@8.14.2/org.elasticsearch.search.lookup.LeafDocLookup.lambda$getFactoryForDoc$1(LeafDocLookup.java:169)",
Online
Find and replace
Console
Postbot
Runner
Start Proxy
Cookies
Vault
Trash