Zolux.com
ZOLUX SAINTES (F)
141 cours Paul Doumer - 17100 Saintes - France
contact@zolux.com – Tel : +33 (0)5 46 74 17 98

Groupe Emetteur : Service informatique
Objet : Utilisation ElasticSearch
Application : **Rédacteur : MÉNARD Lucas** **Date : Responsables : Romain BERTIN**
Ordre de classement de la procédure :
Destinataires

Indice	Date	Libellé de la procédure	Pages Modifiées
V1.0		**Utilisation de Elasticsearch**	

Nature de la dernière modification :

Veuillez détruire l'exemplaire à l'indice précédent

VERIFICATEUR : **Date :**	**APPROBATEUR :** **Date :**

Table des matières

Comment utilisé ElasticSearch ?

Utilité ? :

Elasticsearch agit comme un moteur de recherche puissant qui organise et indexe les données contenues dans les fichiers de logs. Une fois ces index établis, Grafana peut les exploiter pour générer des visualisations informatives et interactives, offrant ainsi une compréhension approfondie des informations contenues dans les logs.
.

Indexation :

Vérification des index déjà présent :

Commande pour vérifier les index créer dans elasticsearch :

curl -X GET "http://192.168.xxx.xxx:9200/_cat/indices?v"

Création d'un index :

Commande pour créer un index :

curl -X PUT "http://192.168.xxx.xxx:9200/logstest" -H 'Content-Type: application/json' -d '{"settings": {"number_of_shards": 1,"number_of_replicas": 0}}'

(Remplacer "logstest" par le nom d'index à créer)
(ElasticSearch accepte uniquement les noms d'index en minuscule)

Indexer des logs depuis un fichier jsonl

Commande pour indexer des logs depuis un fichier :

curl -H 'Content-Type: application/x-ndjson' -X POST 'http://192.168.xxx.xxx:9200/logstest/_bulk' --data-binary @logs.jsonl

(Remplacer "logstest" par le nom d'index créer)

Supprimer des index

Commande pour supprimer un index :

curl -X DELETE "http://192.168.xxx.xxx:9200/logstest"

(Remplacer “logstest” par le nom d’index a supprimé)

Indexation avec un script :

Script pour relier un fichier a un index :

```
nano ‘nom_au_choix’
```

Coller le script si dessous et ensuite faites « CTRL+S et CTRL+X »

```
#!/bin/bash

# Adresse d'Elasticsearch

ELASTICSEARCH_URL="http://192.168.xxx.xxx:9200"

# Nom de l'index

INDEX_NAME="logstest"

# Chemin vers le fichier de logs JSON Lines

LOGS_FILE="logs.jsonl"

# Lire le fichier ligne par ligne et indexer chaque document

while IFS= read -r line; do

# Indexer le document dans Elasticsearch

  curl -H 'Content-Type: application/json' -X POST
"$ELASTICSEARCH_URL/$INDEX_NAME/_doc" -d "$line"

done < "$LOGS_FILE"
```