5. Analyse de cause et corrélation des données des jobs

Les données disponibles sont :

- Le volume de transactions (KPI) sommé par minutes
- Logs applicatifs (messages textuels semi-structurés) du moteur de traitement des transactions
- Mesures de performance d'utilisation du réseau

5.1 Importer les données

KPI :
Créer l'index avec le bon mapping

```
PUT /it_ops_kpi
{
  "settings" : {
    "number_of_shards" : 1,
    "number_of_replicas" : 1
  },
  "mappings": {
     "doc" : {
      "properties" : {
        "@timestamp" : {
          "type" :  "date",
          "format": "epoch_millis"
        }
} } } }
```

Puis importer les données:

```
curl -X POST -H "Content-Type: application/json"
http://localhost:9200/it_ops_kpi/_bulk --data-binary "@it_ops_app_logs.json"
```

Traces du moteur

```
PUT /it_ops_app
{
  "settings" : {
    "number_of_shards" : 1,
    "number_of_replicas" : 1
  },
  "mappings": {
     "doc" : {
      "properties" : {
        "@timestamp" : {
          "type" :  "date",
```

```
          "format": "epoch_millis"
        }
} } } }
```

Importer les données avec :

```
curl -X POST -H "Content-Type: application/json"
http://localhost:9200/it_ops_app/_bulk --data-binary "@it_ops_app_logs.json"
```

Réseau

Créer l'index *pour les données réseau :*

```
PUT /it_ops_network
{
  "settings" : {
    "number_of_shards" : 1,
    "number_of_replicas" : 1
  },
  "mappings": {
     "doc" : {
      "properties" : {
        "@timestamp" : {
          "type" :  "date",
          "format": "epoch_millis"
        }
} } } }
```

Puis :

```
curl -X POST -H "Content-Type: application/json"
http://localhost:9200/it_ops_app/_bulk --data-binary "@it_ops_app_logs.json"
```

5.2 Jobs ML

Créer 3 jobs :

- Détection d'anomalie sur des nombre de transactions faibles
- Anomalie sur le décompte des messages de traces catégorisés
- Anomalies sur les performances réseau (moyennes sur les métriques)

Utiliser un bucket span de 15m et des influenceurs partagés (*hostname, physical host*)

5.3 Corrélation des analyses

Identifier la compagnie aérienne responsable de l'anomalie