TP5 : Démarrer avec Logstash

Vérification de l'installation

- Dézipper l'archive fournie et vérifier qu'il s'agit de la même version qu'ElasticSearch
- Placer vous dans *bin* et exécuter :
  `logstash -e 'input { stdin { } } output { stdout {} }'`

Traitement de logs Apache

Connexion FileBeat / Logstash

- Récupérer la distribution de FileBeat et dézipper
- Récupérer l'archive contenant les logs Apache et dézipper
- Dans le fichier de configuration filebeat.yml, mettre à jour la configuration avec les lignes suivantes :

```
filebeat.prospectors:
- type: log
  enabled : true
  paths:
    - /path/to/file/logstash-tutorial.log
output.logstash:
hosts: ["localhost:5044"]
```

- Démarrer filebeat avec la commande suivante :
  `./filebeat -e -c filebeat.yml -d "publish"`

- Créer un fichier de configuration de pipeline ***pipeline.conf*** comme suit :

```
input {
    beats {
        port => "5044"
    }
}
# The filter part of this file is commented out to indicate that it is
# optional.
# filter {
#
# }
output {
    stdout { codec => rubydebug }
}
```

Tester la configuration :

```
bin/logstash -t -f ./pipeline.conf
```

Démarrer logstash et observer la console :

```
bin/logstash -r -f ./pipeline .conf
```

Ajout filtre grok

- Modifier la configuration afin d'appliquer un filtre grok parsant les messages Apache

```
filter {
    grok {
        match => { "message" => "%{COMBINEDAPACHELOG}"}
    }
}
```

La configuration est automatique par contre il faut demander à *Filebeat* de retraiter le fichier Apache.

- Arrêter Filebeat et supprimer son registre avec la commande :

```
sudo rm data/registry
```

- Relancer Filebeat et observer la sortie sur la console de logstash.
  Quels sont les changement par rapport à tout à l'heure ?

Ajouter ensuite le filtre GeoIP

```
geoip {
        source => "clientip"
    }
```

- Recommencer le traitement et observer les changements

Alimentation d'ElasticSearrch

- Modifier la config afin que la sortie soit dirigée vers votre cluster ElasticSearch

```
output {
   elasticsearch {
        hosts => [ "localhost:9200" ]
    }
}
```

- Recommencer le traitement, vérifier la console d'ElasticSearch et trouver l'index créé.
- Effectuer une recherche afin de trouver des documents ElasticSearch