TP6 : Configuration Pipeline Logstash

6.1 Traitement des logs apache

Nous voulons améliorer la pipeline logstash du TP précédent.
Le répertoire de logs Apache contient différents fichiers en fonction des virtual host configuré sur Apache.
La pipeline doit :

- Utiliser un input file traitant tous les fichiers d'un répertoire
- Alimenter des types de documents différents en fonction des noms des fichiers de trace
- Convertir le champ « bytes » en un type long
- Alimenter la géo-localisation à partir de l'IP du client
- Affecter le champ *timestamp* au champ *@timestamp*
- Créer des champs day,month,year qui isolera respectivement le jour, le mois et l'année de l'événement

Modifier le nom d el'index ElasticSerach vers lequel les documents sont acheminés.

6.2 Traitement des logs Jboss

L'objectif est de garder toutes les lignes :

- WARNING, ERROR ou FATAL
- Et les exceptions

6.3 Exécution simultanée des 2 pipelines

Mettre au point le fichier pipelines.yml qui configure les 2 pipelines précédentes.

Utiliser un modèle d'exécution différent pour chaque pipeline