ELK

Objectifs:

- **Maitriser les concepts ELK ;**
- **Explorer les concepts du monitoring temps réel.**
- **Analyse des Logs**

Ce projet est à rendre le lundi 27 octobre avant 23h55 en binôme de deux. Produire un rapport.

-

1. Travail à faire

Partie 1

Dans un écosystème informatique de plus en plus complexe, le monitoring est devenu un levier clé pour suivre la performance et la fiabilité des infrastructures matérielles et applicatives. La pile ELK propose l'ingestion en temps réel de Stream de données et l'analyse d'un un vaste volume de données de télémétrie. Beaucoup de logiciels propriétaires (tel que Splunk) sont basés sur ELK pour fournir des fonctionnalités de monitoring et de suivi des performances. Ces informations indexées en temps réel peuvent être enrichies par l'intelligence artificielle (IA) et le machine learning (ML) pour offrir un environnement de diagnostic en temps réel.

Ce projet vise à indexer et explorer les journaux de build pour le logiciel Firefox produit par Mozilla. Il s'agit d'indexer les fichiers logs en temps réel et de fournir un tableau de bord pour le suivi des indicateurs de performance et des anomalies.

- Vous avez le choix d'utiliser logstash ou kafka pour l'ingestion des données en temps réel. Un guide d'installation et d'utilisation de Logstash et filebit se trouve dans le dossier « Project » ;
- Les données des logs sont fournies dans le dossier « Project ». Bien que ces données soient fournis de façon statique, il faut simuler l'ajout de données à ces logs en temps réel.

Travail à faire :

- Créer un Mapping adéquat dans Elasticsearch pour indexer les données des logs ;
- Configurer Filebit / Logstash OU KAFKA pour une ingestion automatisée des données (des logs vers l'index) ;
- Analyser les données et produire un tableau de bord ;
- Intégrer un module de machine learning pour détecter les anomalies dans les fichiers logs.