40Z Exploitation de journaux d'application

Solution étudiée: suite ELK

Équipe E16, alias *CASIment l'UML*:

- Baptiste BILLARD
- Théo LARCHER
- Simon LEBEAUD

Problématique

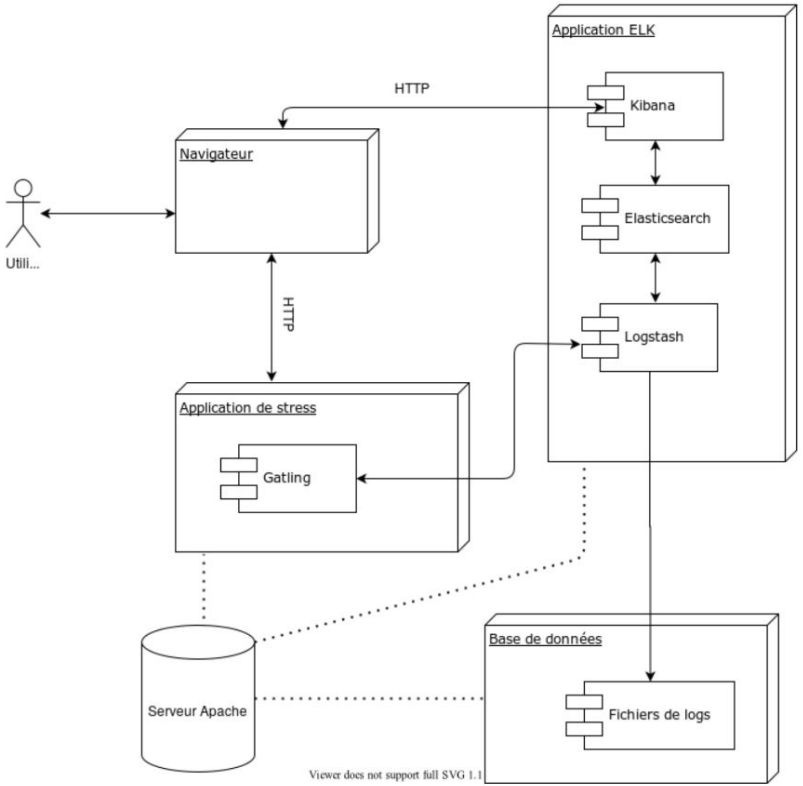
- Stockage, collecte et analyse d’une grande quantité de journaux (**logs**)
- Permettre la gestion d’une architecture logicielle complexe grâce à cette analyse

Les solutions retenues

- Loggly (équipe B)
- **Suite ELK**
- Loki (équipe C)
- Solr (équipe D)

La suite ELK: Logstash - Elasticsearch - Kibana

Architecture de la solution



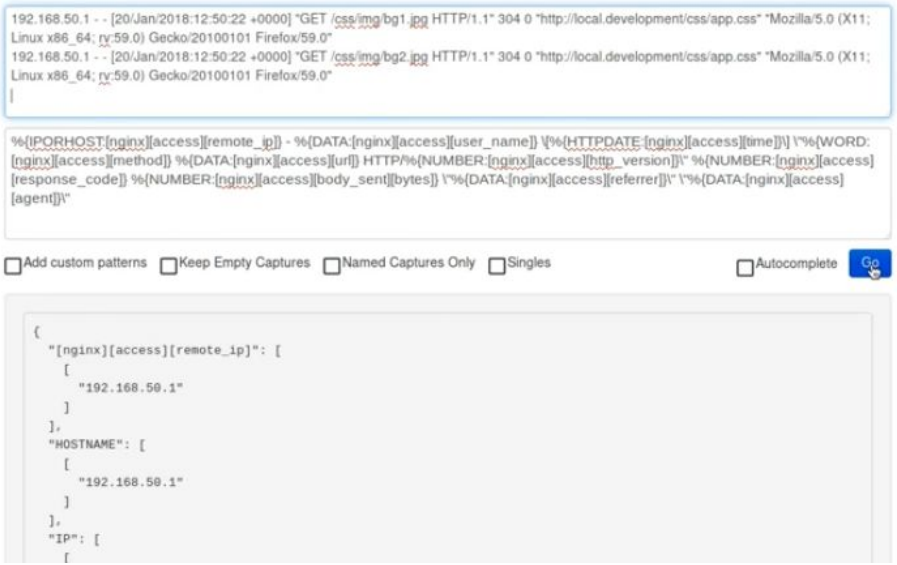
Le pattern mis en oeuvre : *ConversionPattern*

Formater un évènement de log pour le convertir en string.

Log

Conversion specifier

Result



“Démonstration”

Les critères de qualité surveillés

- **Tolérance aux erreurs:**
  - Recenser et être robuste aux erreurs de mémoire
  - Possibilité aux utilisateurs de signaler des données imprécises
- **Efficacité:**
  - Le temps et les ressources attribué est-il convenable pour notre utilisation
  - Mesurer le nombre de lignes de logs
  - Temps d'exécution d'une requête court
- **Nombre d'échecs:** Comparer le ratio *logs mal analysés / total logs* sur les différentes solutions sur un même ensemble de logs

Merci de votre attention.