

# 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





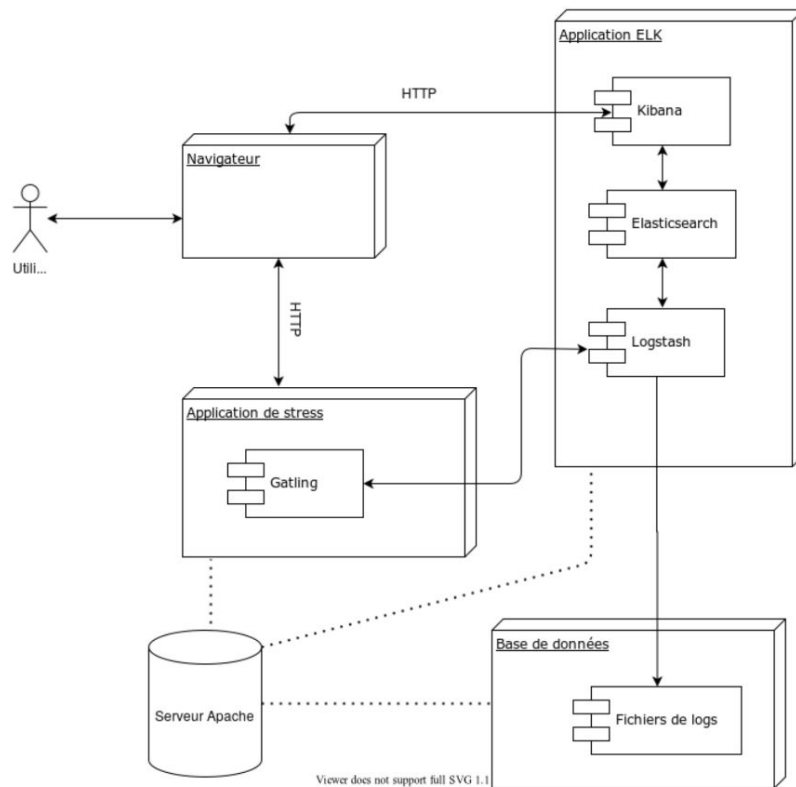
## Les solutions retenues

- 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

```
192.168.50.1 - - [20/Jan/2018:12:50:22 +0000] "GET /css/img/bg1.jpg HTTP/1.1" 304 0 "http://local.development/css/app.css" "Mozilla/5.0 (X11; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0"
192.168.50.1 - - [20/Jan/2018:12:50:22 +0000] "GET /css/img/bg2.jpg HTTP/1.1" 304 0 "http://local.development/css/app.css" "Mozilla/5.0 (X11; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0"
|
```

Conversion  
specifier

```
%([PORTHOST:[nginx][access][remote_ip]] - %([DATA:[nginx][access][user_name]] \[%([HTTPDATE:[nginx][access][time]]) \[%([WORD:[nginx][access][method]] %([DATA:[nginx][access][url]] HTTP/%([NUMBER:[nginx][access][http_version]]) \[%([NUMBER:[nginx][access][response_code]] %([NUMBER:[nginx][access][body_sent][bytes]] \[%([DATA:[nginx][access][referrer]] \[%([DATA:[nginx][access][agent]] \%
```

☐ Add custom patterns ☐ Keep Empty Captures ☐ Named Captures Only ☐ Singles

☐ Autocomplete 

Result

```
{
  "[nginx][access][remote_ip]": [
    [
      "192.168.50.1"
    ]
  ],
  "HOSTNAME": [
    [
      "192.168.50.1"
    ]
  ],
  "IP": [
    [
```



# **“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.**

