



## Auteurs

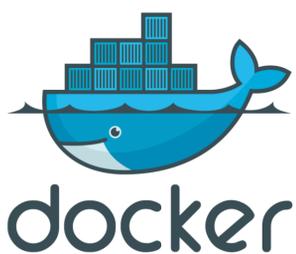
Effectué par :  
Khaled MOALLA  
Manel BEN FATMA

Encadré par:  
Luc CLEMENT  
Raphaëlle LOYER  
Walid GAALOU

## Partenaires



## Technologies phares



## Analyser les logs docker

un travail pénible

- Analyser une centaine de ligne de logs sans outil de filtrage et de recherche est un travail pénible.
- Les containers de production de UAVIA génèrent une centaine de logs par minutes et tirer profit de ces derniers nécessitent une interface meilleure qu'une simple ligne de commande.
- Plus la réaction à une erreur dans le log est plus lente ,plus l'impact est important.

```

khaled@khaled-HP-15-Notebook-PC: ~/juaviaPFE/docker-elk-master
Fichier  Edition  Affichage  Rechercher  Terminal  Aide
: [], "pid":1,"method":"post","statusCode":200,"req":{"url":"/elasticsearch/_msearch",
"method":"post","headers":{"host":"localhost:5601","connection":"keep-alive",
"content-length":"754","accept":"application/json, text/plain, */*","origin":"h
ttp://localhost:5601","kbn-version":"6.5.4","user-agent":"Mozilla/5.0 (X11; Linu
x x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.
36","content-type":"application/x-ndjson","referer":"http://localhost:5601/app/k
ibana"},"accept-encoding":"gzip, deflate, br","accept-language":"fr-FR,fr;q=0.9,a
r-TN;q=0.8,ar;q=0.7,en-US;q=0.6,en;q=0.5"},"remoteAddress":"172.19.0.1","userAge
nt":"172.19.0.1","referer":"http://localhost:5601/app/kibana"},"res":{"statusCod
e":200,"responseTime":3799,"contentLength":9},"message":"POST /elasticsearch/_ms
earch 200 3799ms - 9.0B"}
kibana_1 | {"type":"response","@timestamp":"2019-01-29T10:18:14Z","tags":
: [], "pid":1,"method":"post","statusCode":200,"req":{"url":"/elasticsearch/_msearch",
"method":"post","headers":{"host":"localhost:5601","connection":"keep-alive",
"content-length":"754","accept":"application/json, text/plain, */*","origin":"h
ttp://localhost:5601","kbn-version":"6.5.4","user-agent":"Mozilla/5.0 (X11; Linu
x x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.
36","content-type":"application/x-ndjson","referer":"http://localhost:5601/app/k
ibana"},"accept-encoding":"gzip, deflate, br","accept-language":"fr-FR,fr;q=0.9,a
r-TN;q=0.8,ar;q=0.7,en-US;q=0.6,en;q=0.5"},"remoteAddress":"172.19.0.1","userAge
nt":"172.19.0.1","referer":"http://localhost:5601/app/kibana"},"res":{"statusCod
e":200,"responseTime":925,"contentLength":9},"message":"POST /elasticsearch/_mse
arch 200 925ms - 9.0B"}

```

## La Solution Open source

Stack ELK & Pilote de logging Syslog



- Utilisation du pilote docker Syslog pour l'envoi des logs taggés via le réseau vers Logstash.
- Configuration des filtres et des ports Logstash pour améliorer le découpage du log en plusieurs champs plus significatifs.
- Configuration de la présentation des logs en utilisant Kibana.

## Résultats finaux

Des logs bien définies & une présentation ergonomique

- Découpage du log en des champs lisibles : Timestamp, log level, message ,hôte ...
- Filtrage très facile en utilisant l'interface Kibana.
- Des statistiques utiles sur les logs comme le nombre d'erreur ou de warnings.

