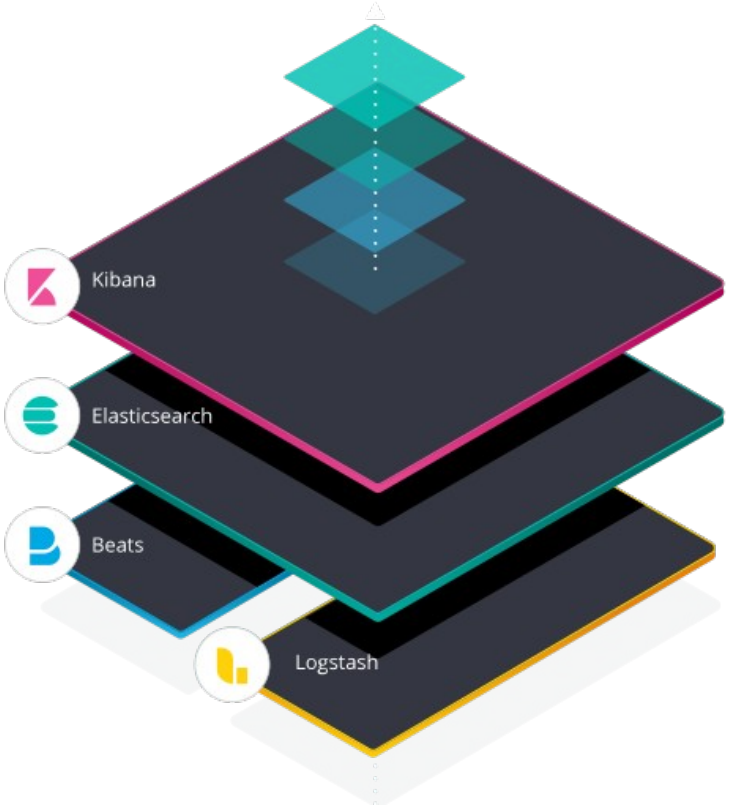
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

Elastic Stack

Céline Lambert / Adrien Contesse

Université de Toulouse

Elastic Stack



Présentation d'Elastic Stack

Trois projets opensource intégrés

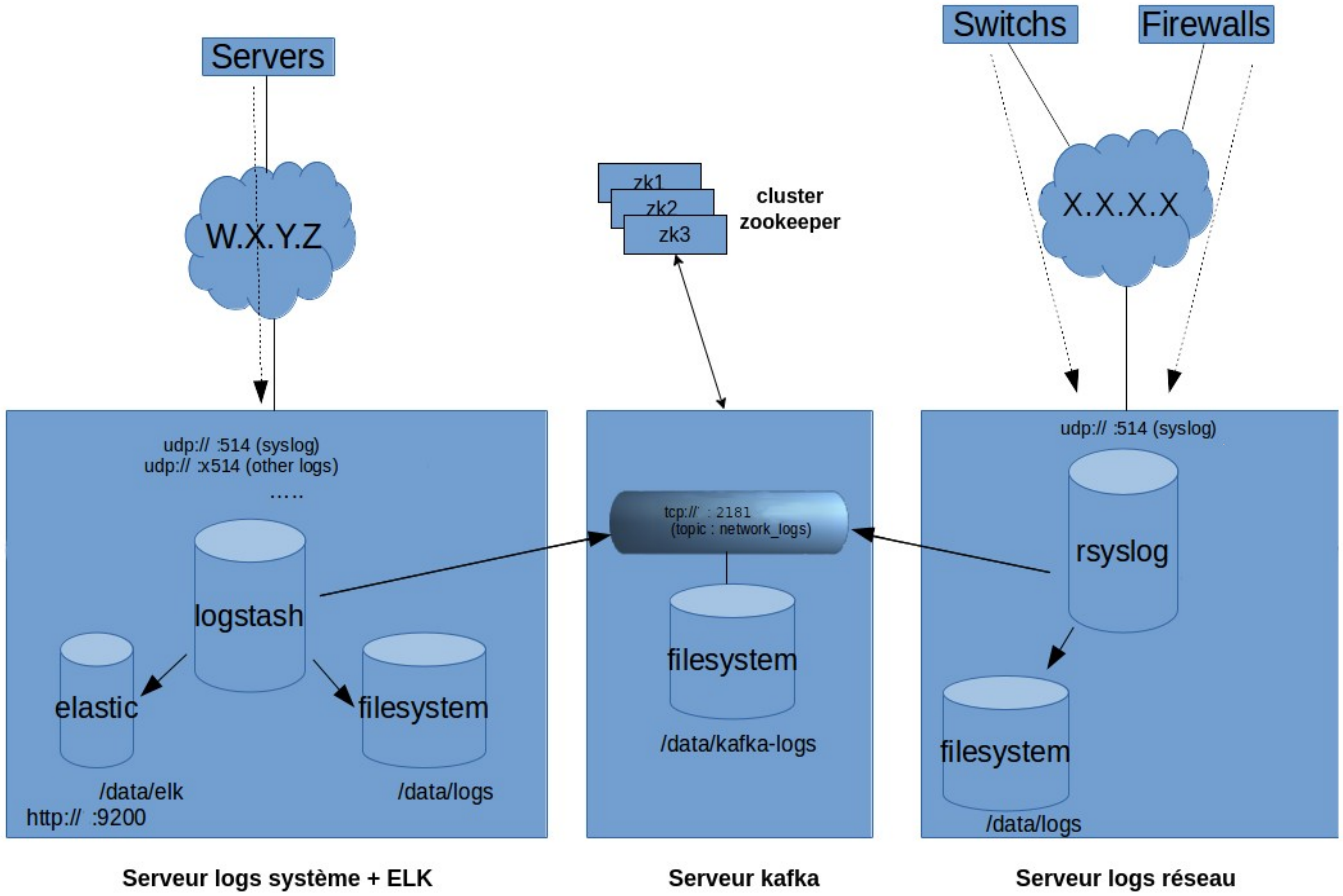

Elasticsearch : moteur de recherche


Logstash/Beats : pipeline coté serveur

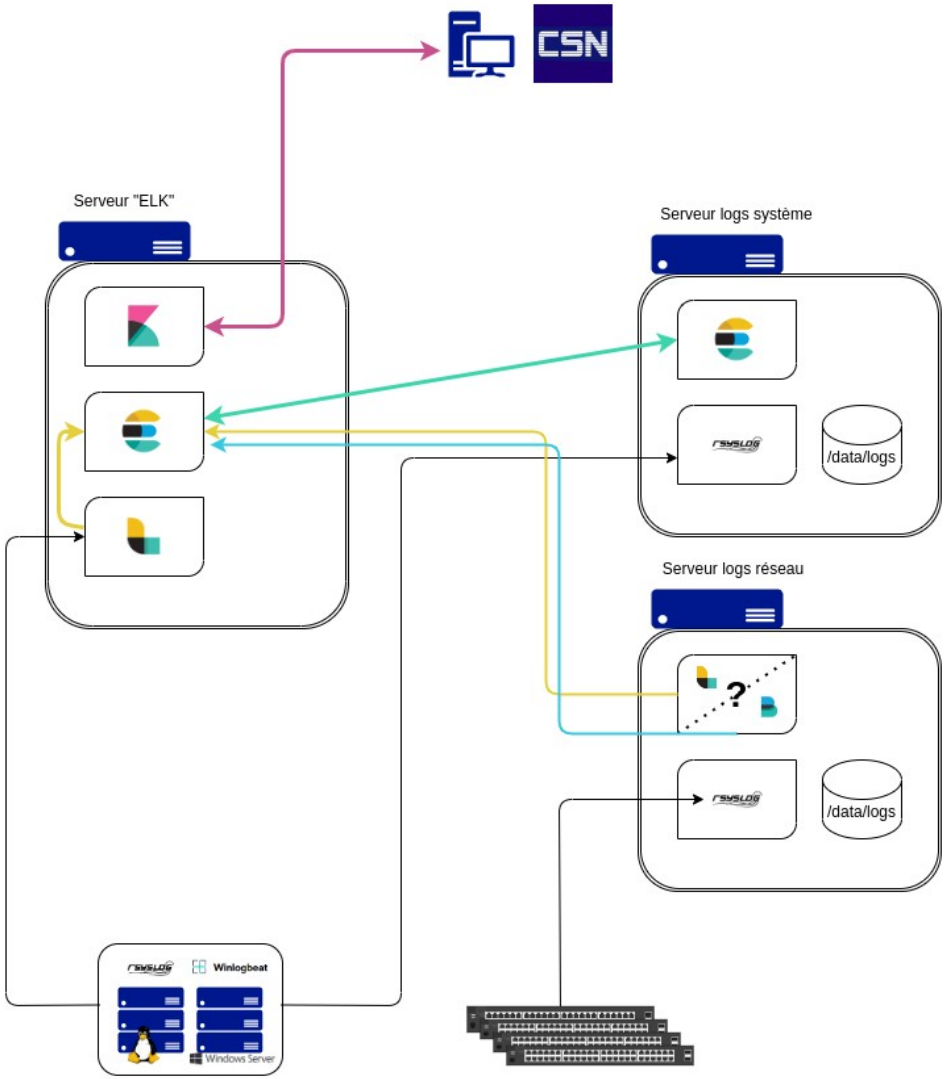

Kibana : interface de visualisation web

- Utilise diverses technos opensource : Lucene, Json, NoSQL.
- Propose une API Rest
- Moteur de recherche d'entreprise le plus populaire

Architecture précédente



Evolution de l’architecture



Installation de la stack

- Repository debian fourni par elastic
- Sélection de la version 8.6
- Configuration simple (YAML)
- Sécurisation des échanges entre les briques de la stack par certificats, tokens, clés d’API, authentification

Comparatif filebeat vs logstash

- Filbeat : « prêt à porter »,
  facile et rapide
  Communication directe possible avec Kibana.
- Logstash : « sur mesure »

  plus complexe (patterns grok).
  Extraction précise des infos utiles.
- Kibana permet d'agréger les données des deux solutions.

Difficultés rencontrées

- Problème de clés sur le repository en Ubuntu 18.04
- Difficultés de mise en place de la sécurisation :

  Certificat auto-signé.

  Intégration du 2d nœud au cluster,

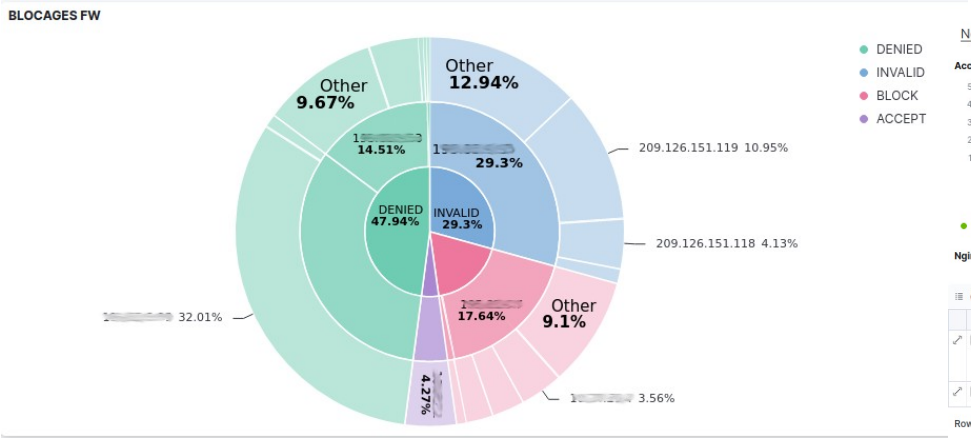
  Un utilisateur par brique avec des privilèges différents.

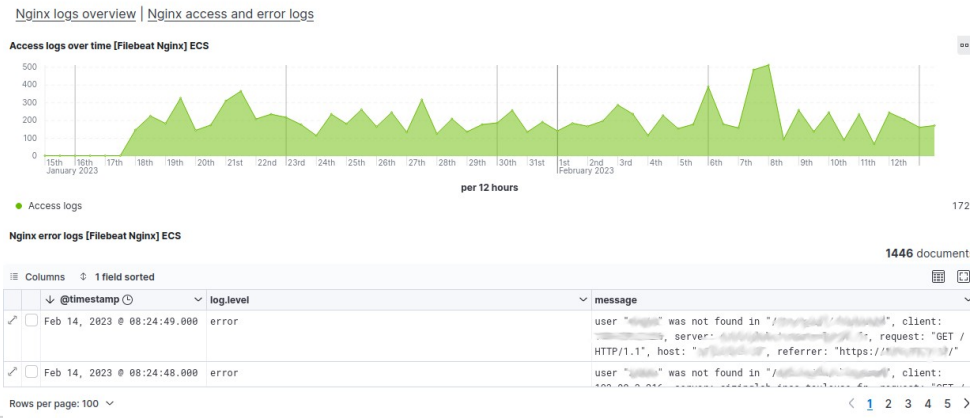
  Méthodes d’authentification différentes selon les briques

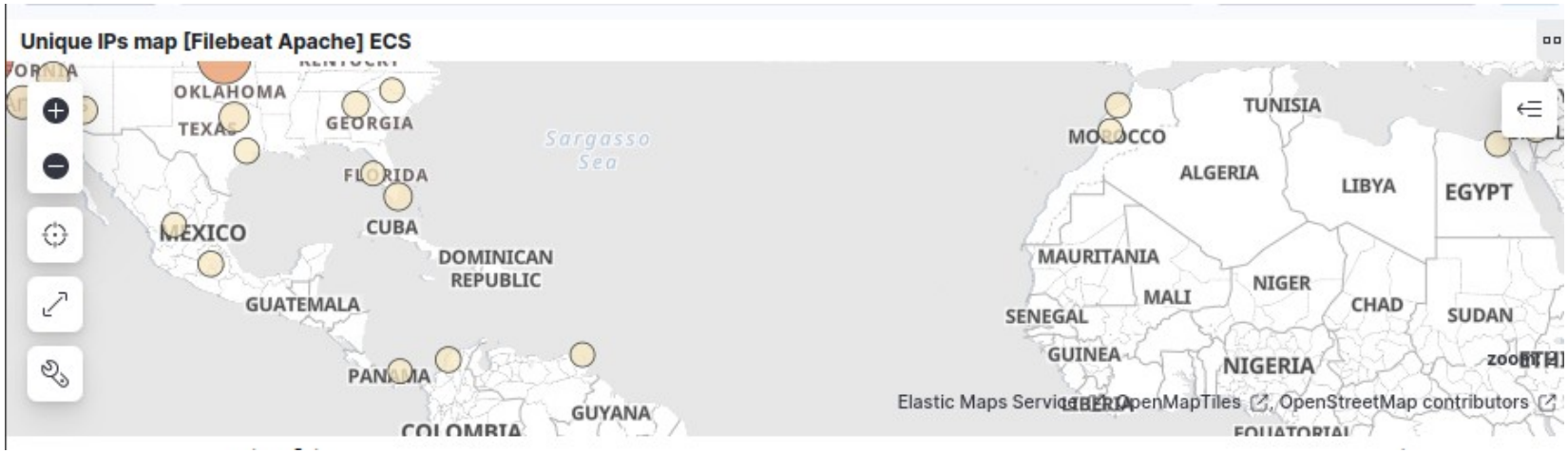
Difficultés rencontrées (2)

- Documentation parfois cryptique
- Complexité/exotisme des patterns grok (ruby) => débogueur recommandé.

Conclusion


BLOCAGES FW
Other
9.67%
Other
12.94%
14.51%
29.3%
DENIED
47.94%
INVALID
29.3%
17.64%
Other
9.1%
4.27%
209.126.151.119 10.95%
209.126.151.118 4.13%
32.01%
3.56%
DENIED
INVALID
BLOCK
ACCEPT


Nginx logs overview | Nginx access and error logs
Access logs over time [Filebeat Nginx] ECS
per 12 hours
Access logs
Nginx error logs [Filebeat Nginx] ECS
1446 document
Columns
1 field sorted
@timestamp
log.level
message
Feb 14, 2023 @ 08:24:49.000
error
Feb 14, 2023 @ 08:24:48.000
error
Rows per page: 100


Unique IPs map [Filebeat Apache] ECS
OKLAHOMA
TEXAS
GEORGIA
FLORIDA
CUBA
MEXICO
DOMINICAN
REPUBLIC
GUATEMALA
GUYANA
Sargasso
Sea
TUNISIA
ALGERIA
LIBYA
EGYPT
MAURITANIA
MALI
NIGER
CHAD
SUDAN
SENEGAL
GUINEA
NIGERIA
Elastic Maps Service
OpenMapTiles
OpenStreetMap contributors


ELK