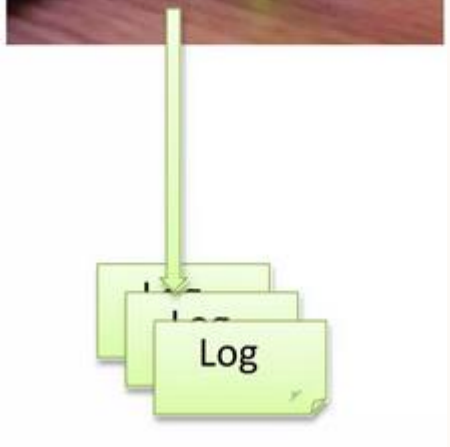
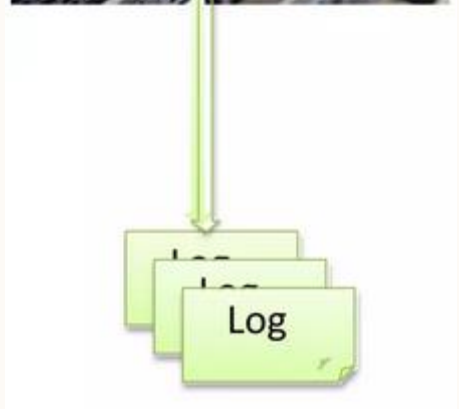
ELK STACK

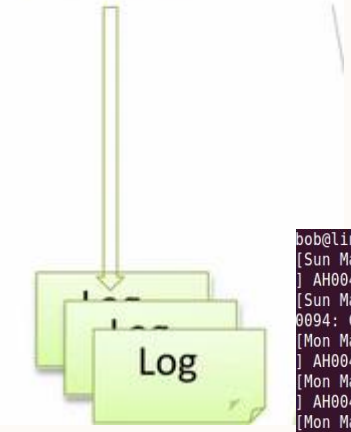
Introduction à ElasticSearch, Logstash et Kibana

SOMMAIRE

- Pourquoi ?
- La Stack
  - ElasticSearch
  - Logstash
  - Kibana
- Démo







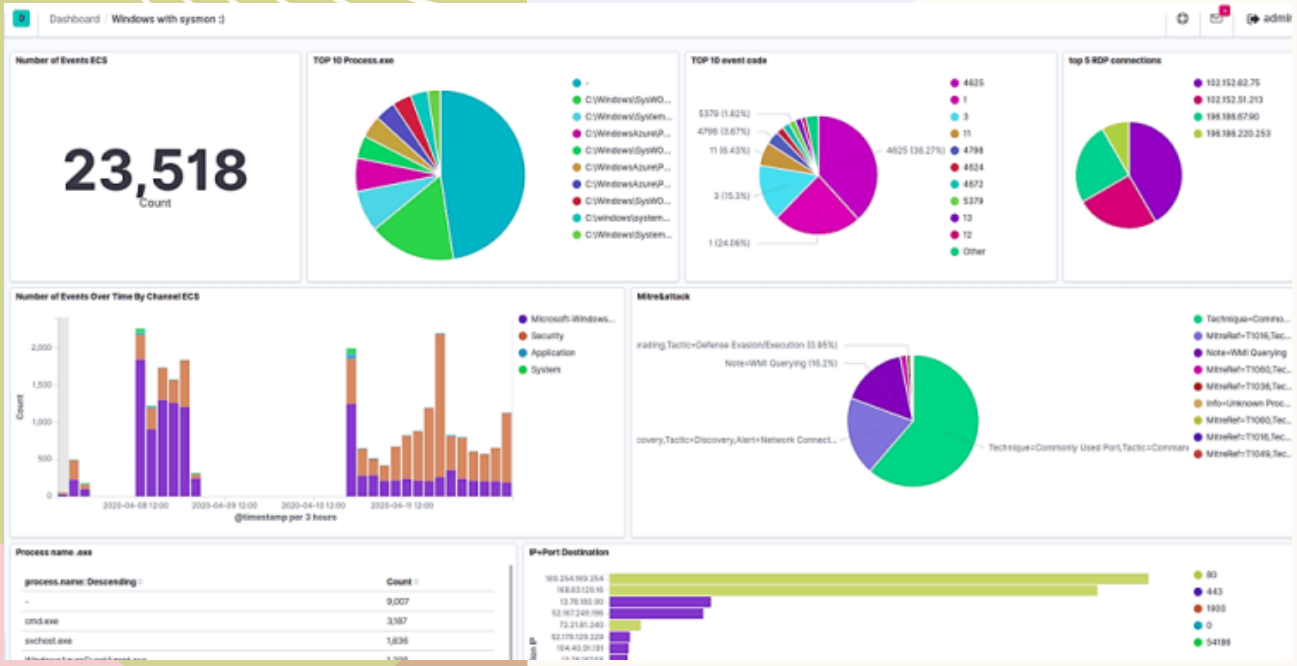

```
bob@linux-ub:/var/www/html$ cat /var/log/apache2/error.log
[Sun Mar 27 20:27:00.269176 2016] [mpm_event:notice] [pid 23343:tid 140057225037696
] AH00489: Apache/2.4.7 (Ubuntu) configured -- resuming normal operations
[Sun Mar 27 20:27:00.269264 2016] [core:notice] [pid 23343:tid 140057225037696] AH0
0094: Command line: '/usr/sbin/apache2'
[Mon Mar 28 17:51:40.796855 2016] [mpm_event:notice] [pid 23343:tid 140057225037696
] AH00491: caught SIGTERM, shutting down
[Mon Mar 28 17:51:41.849873 2016] [mpm_event:notice] [pid 52009:tid 140535007307648
] AH00489: Apache/2.4.7 (Ubuntu) configured -- resuming normal operations
[Mon Mar 28 17:51:41.849978 2016] [core:notice] [pid 52009:tid 140535007307648] AH0
0094: Command line: '/usr/sbin/apache2'
[Mon Mar 28 17:53:49.477402 2016] [mpm_event:notice] [pid 52009:tid 140535007307648
] AH00491: caught SIGTERM, shutting down
[Mon Mar 28 17:53:49.530379 2016] [mpm_event:notice] [pid 53542:tid 140182453340032
] AH00489: Apache/2.4.7 (Ubuntu) configured -- resuming normal operations
[Mon Mar 28 17:53:49.530507 2016] [core:notice] [pid 53542:tid 140182453340032] AH0
0094: Command line: '/usr/sbin/apache2'
[Tue Mar 29 20:52:09.189540 2016] [mpm_event:notice] [pid 53542:tid 140182453340032
] AH00491: caught SIGTERM, shutting down
```

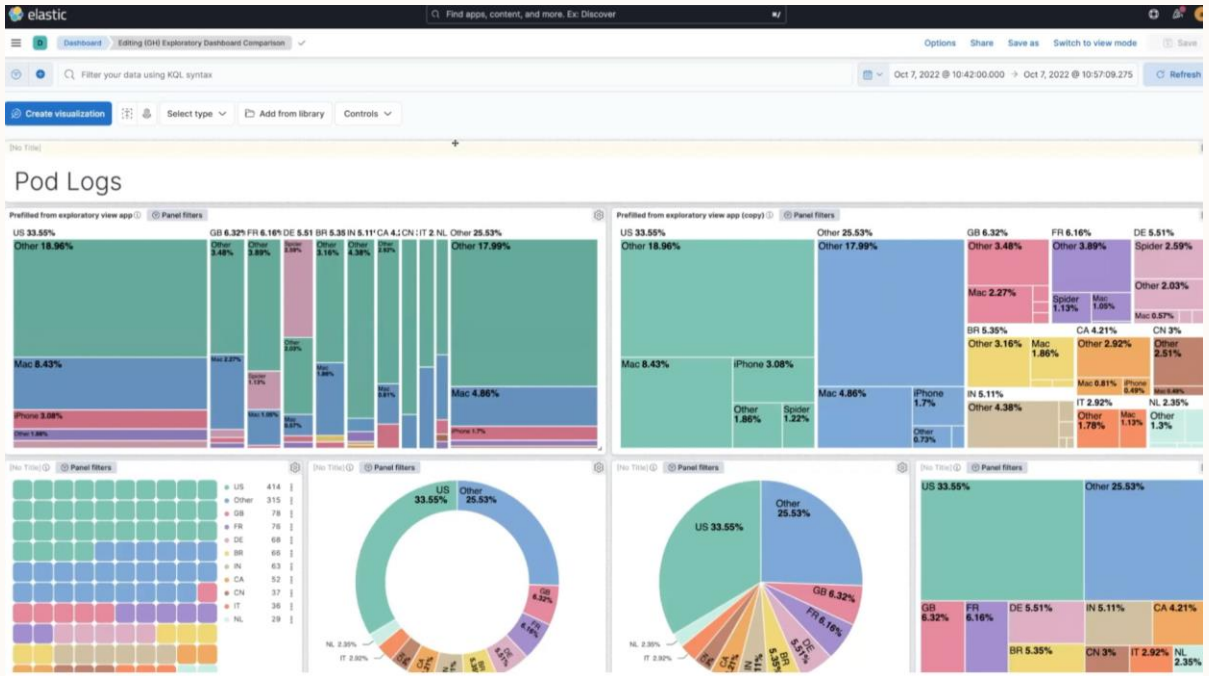
POURQUOI ?

« Tu peux me trouver les logs qu'il y a eu hier entre 15h02 et 15h07 stp ? »

LA SOLUTION ?

Visualisation > Texte brut



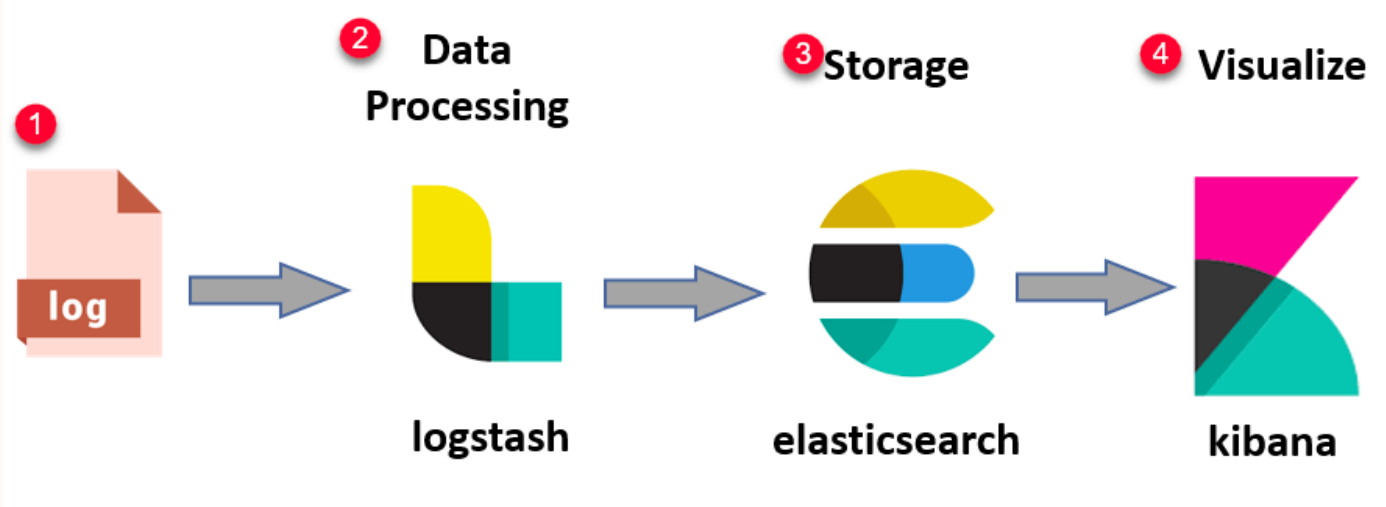


LA STACK ELK

La stack ELK est le produit de 3 outils « source-available »:

- Elasticsearch
- Logstash
- Kibana

Les 3 étant développés par Elastic

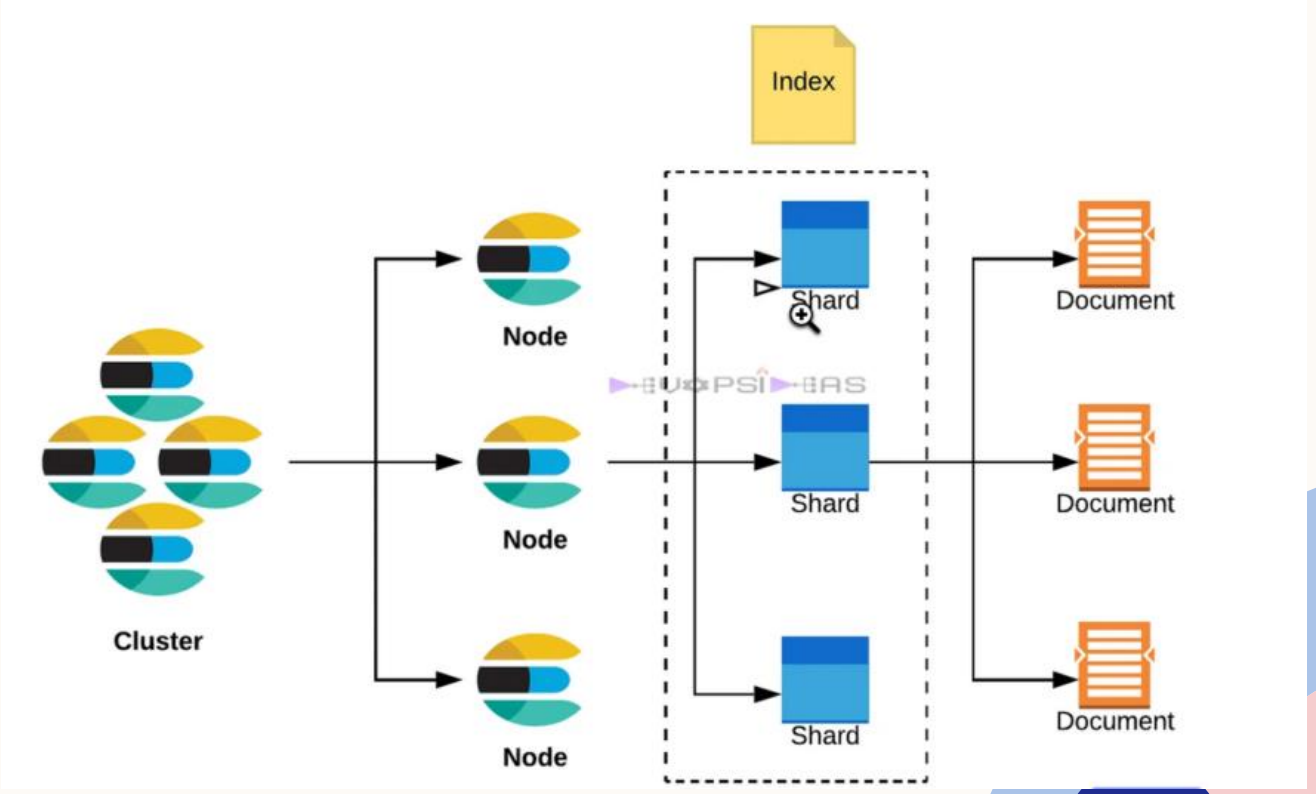


QUI UTILISE ELK ?

ELASTIC

ElasticSearch est le moteur de recherche.

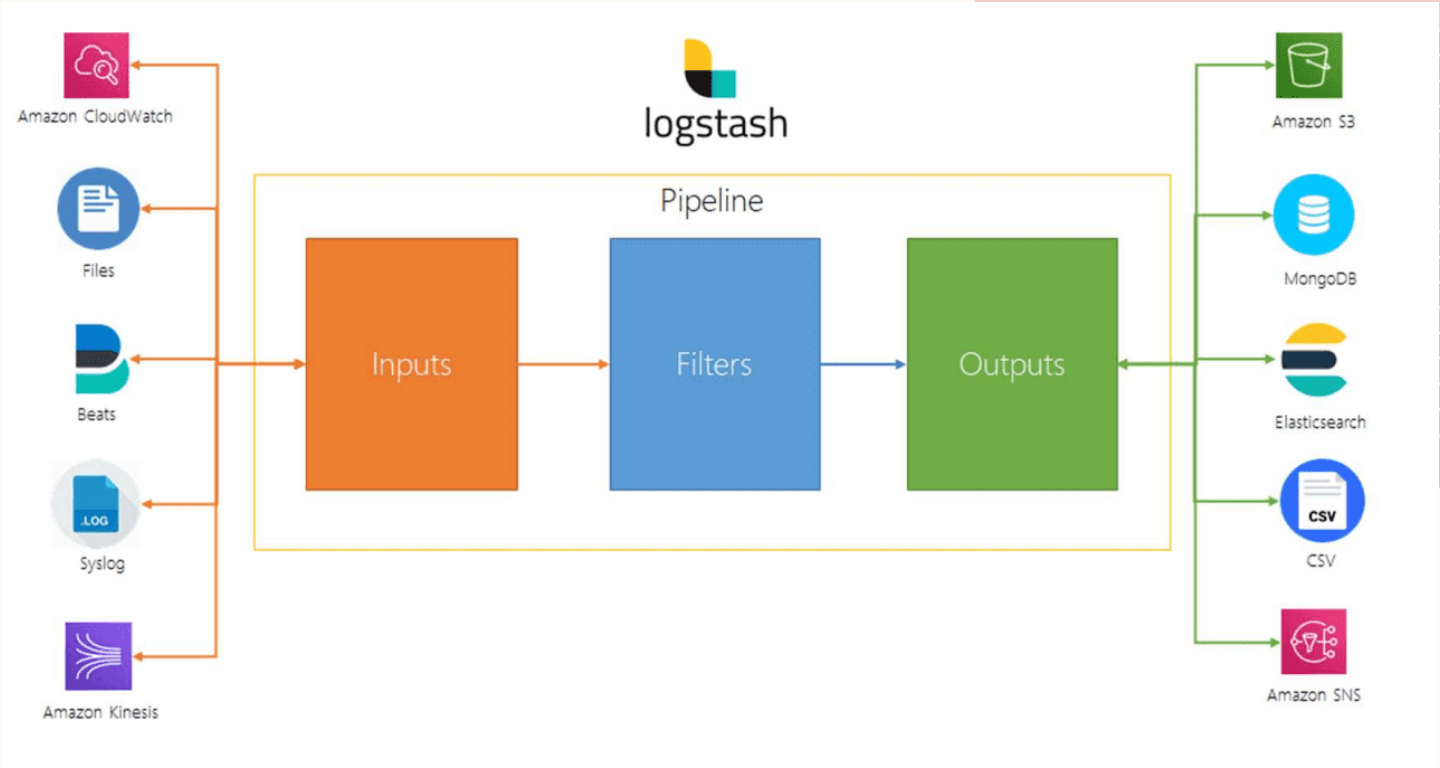
- Multi-tenant
- Recherche fulltext
- Scalable
- Distribué



LOGSTASH

Logstash s'occupe de collecter et d'ingérer les données.

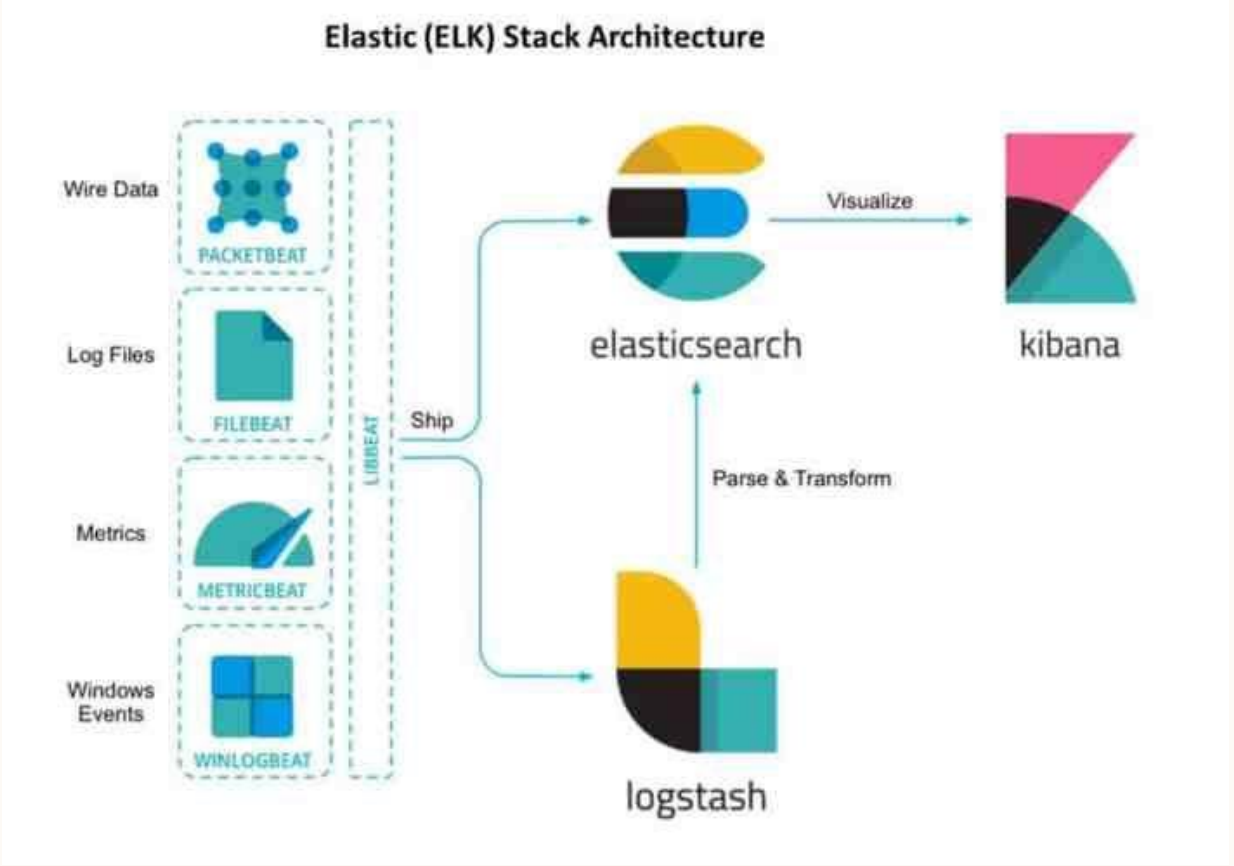
- ETL (Extract-Transform-Load)
- Centralisation de donnée
- Peut lire tout types de logs (système, web, erreurs, applicatifs)



KIBANA

Kibana est le GUI

- Visualisation de données
- Création de dashboard interractifs
- Peut utiliser d'énormes volumes de données



Kibana possède un équivalent open-source « OpenSearch » sponsorisé par AWS développé après que Elastic ait enlevé l'open-source du projet

MERCI

Maintenant, démo tp etc…