**Sujet 1 :**  Mettre en œuvre une base de données dont l'objectif est d'héberger les journaux (logs) d'équipements, logiciels , systèmes d'exploitation, équipements dans le but de permettre l'analyse à froid et à chaud . Faire une démonstration sur un exemple concret (Cybersécurité : tentative d' intrusion ou dysfonctionnement pour analyse et correction de bugs , …)

Recherche de la techno à préconiser :

* MongoDB
* ElasticSearch
* Cassandra
* Mysql
* Neo4j

Pour être performant dans le stockage de logs, une base de données doit pouvoir couvrir ces différents points :

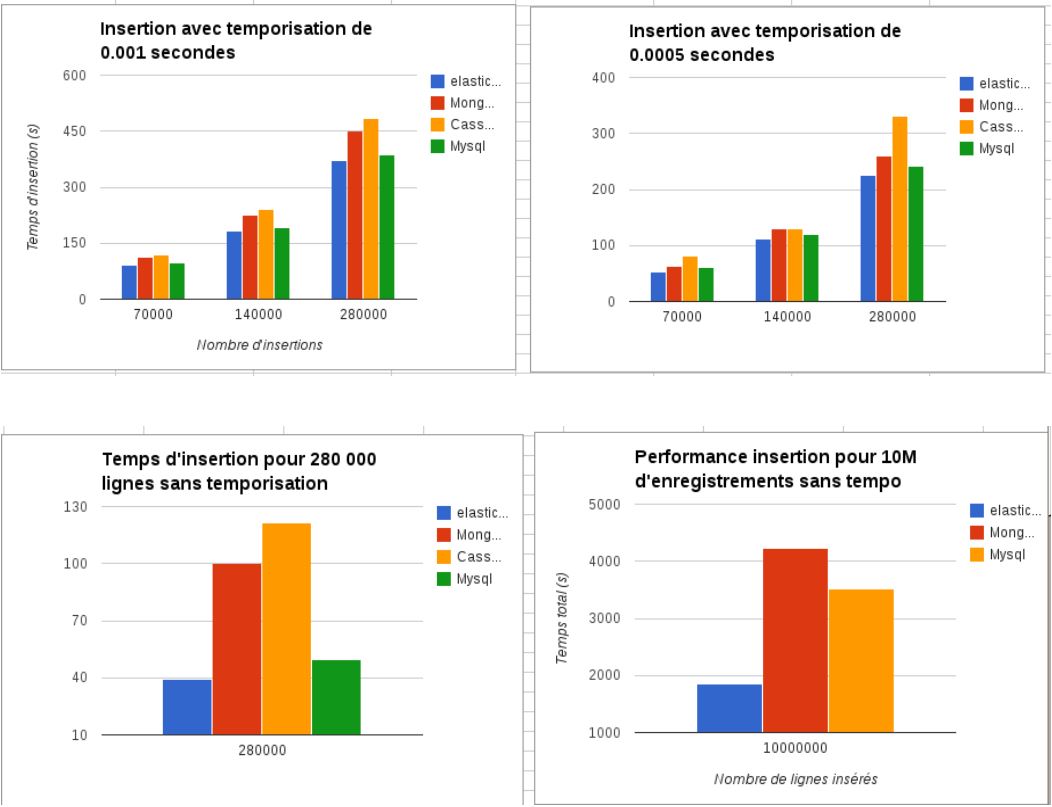
* Collection
* Transport
* Traitement
* Stockage
* Recherche
* Visualisation

MongoDB semble être la solution de base et répondre plutôt bien aux attentes, surtout en termes de stockage.

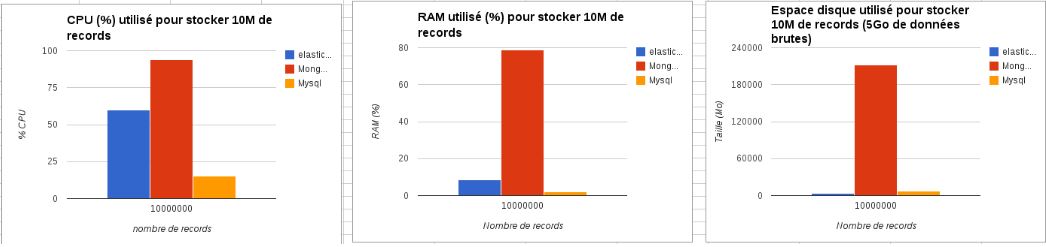
Un combo sort gagnant des recherches, cela implique **Logstash-Forwarder** pour la collecte et le transport, **Logstash et Riemann** pour le process, et **Kibana3** pour la visualisation.

Workbench: ElasticSearch – MongoDB – Cassandra – Mysql

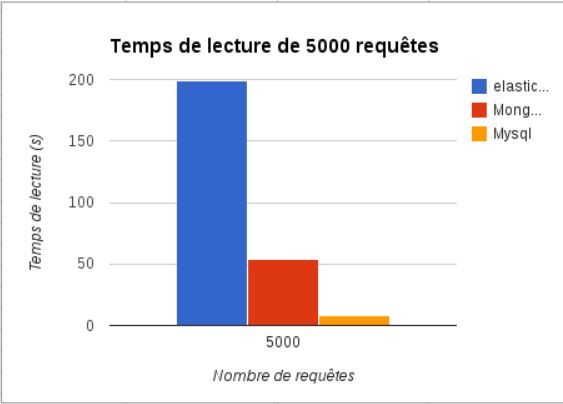
*Insertion*



*Consommation*



*Lecture*



Les tests ont été réalisé en essayant d’être cohérent pour un comparatif pertinent même si d’autres workbench dans d’autres circonstances et avec d’autres paramètres pourrait être très différents.

Au niveau des résultats, **Cassandra** sort gagnant avec des très bons temps de lecture et d’écriture tout en ayant une faible consommation. Malgré cela l’équipe qui a réalisé ces tests ont finalement décidé d’utiliser **ElasticSearch** pour leur projet, Les atouts sont la facilité de mise en place et les avantages liés au services annexes comme **Kibana**.

**Cas d’usage :**

Dans notre cas d’usage les logs seront probablement stockés en termes de jours, voir mois, avec une nécessitée de pouvoir facilement et rapidement accéder aux données pour une analyse en temps réel.

**Le Prof a validé aussi de partir sur ElasticSearch !**

**Progression :**

**ElasticSearch**, **kibana**, **logstash** et **filebeat** installés sur la machine distante, ports 9200 et 5601 ouverts, fichiers de config modifiés pour accepter les connexions remote via *10.8.2.35:5601*.

# Bibliographie

* Comparatif database: <https://eventuallycoding.com/2013/11/05/comparaison-de-moteurs-de-base-de-donnees-pour-du-stockage-de-logs/>
* Comparatif database: <https://dzone.com/articles/5-data-storages-for-better-log-management>
* Log monitoring: <https://www.elastic.co/fr/observability/log-monitoring>
* Tuto complet: <https://medium.com/@vitalypanukhin/elasticsearch-elk-stack-for-log-management-8f4e61a60239>
* Install ELK Ubuntu: <https://infosecwriteups.com/how-to-install-elastic-stack-on-ubuntu-22-04-lts-a2f1b00eced>