RETOUR D'EXPERIENCE SUR NOTRE STACK DE LOGS

On va se dire les vrais affaires

QUI SUIS-JE ?

Julien Maitrehenry

DevOps at PetalMD

jmaitrehenry.ca
https://github.com/jmaitrehenry
@jmaitrehenry

AGENDA

- Contexte
- Notre stack
- Elasticsearch
- Les problèmes que l'on a eu
- Bonnes pratiques pour la stack ELK
- Démo

CONTEXTE

Des metrics, y'a qu'ça d'vrai !

CONTEXTE

- Rails web app log: ~2.3 millions docs/jour
  - 1 index daily
- Frontend monitoring: ~700k docs/jour
  - 1 index daily
- nginx: ~3.6 millions docs/jour
  - 1 index daily
- Sidekiq log: ~1.5 million docs/jour
  - 2 indexes weekly
- Quelques autres petits indexes

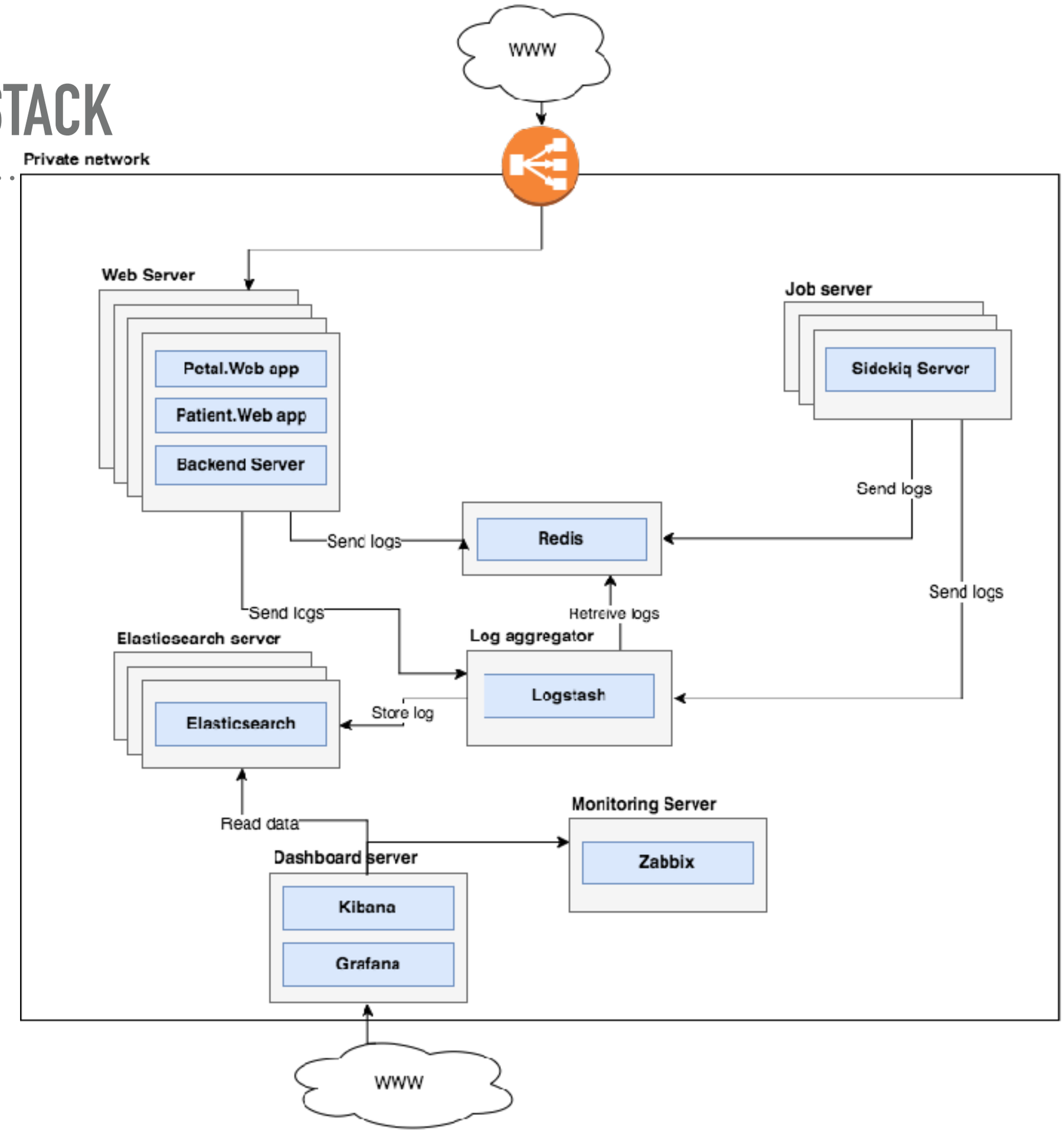
NOTRE STACK

La plus belle du monde et plus encore !

NOTRE STACK

- Applicatif
  - Serveurs web nginx pour les apps frontend
  - Serveur web nginx+passenger pour ruby
  - Serveur Sidekiq pour les background jobs
- Logs
  - Logstash + redis
  - Logstash as rsyslog server
  - Elasticsearch as storage engine
- Visualisation
  - Kibana
  - Grafana

NOTRE STACK


WWW
Private network
Web Server
Petal.Web app
Patient.Web app
Backend Server
Job server
Sidekiq Server
Send logs
Redis
Send logs
Send logs
Retreive logs
Send logs
Elasticsearch server
Elasticsearch
Store log
Log aggregator
Logstash
Read data
Monitoring Server
Zabbix
Dashboard server
Kibana
Grafana
WWW

ELASTICSEARCH

C'est quoi cette bête ?

ELASTICSEARCH – ELASTIC STACK

ELASTICSEARCH – HISTORY

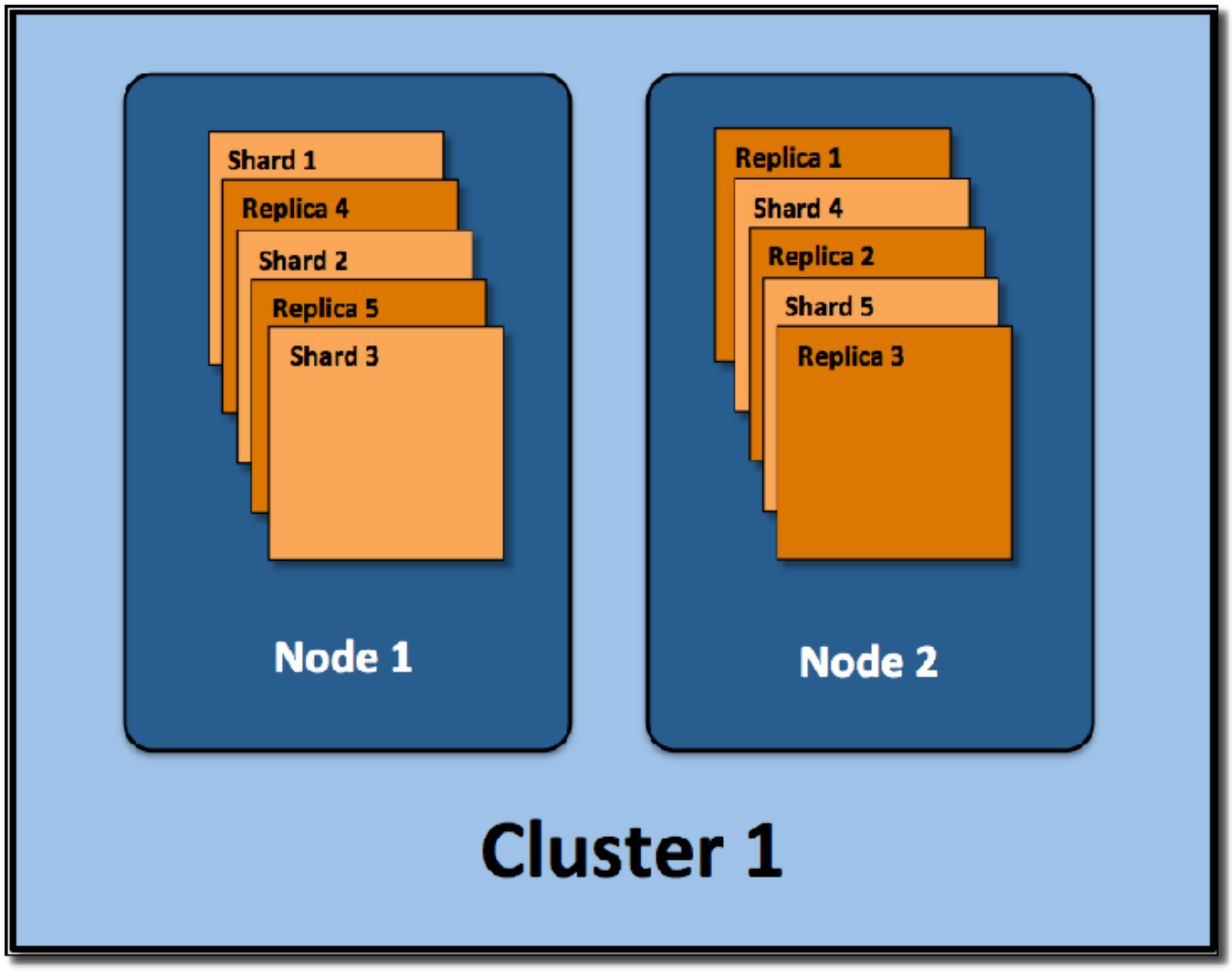
- 0.4: first version was released in February 2010
- 1.0: released in 2014
- 2.0: released in 2015
- 5.0: released in 2016

- Open Source
  - Apache License

ELASTICSEARCH – C'EST QUOI

- Distributed data storage & information retrieval plateform
  - Search Engine / aggregation engine / analytics
  - Suggestions / percolation / highlighting / geo
  - Document store
  - Horizontally distributed
  - Highly available
  - Real time / Near real time
  - Simple RestFull API

ELASTICSEARCH



LES PROBLÈMES QUE L'ON A EU

Y'en aura pas d'problèmes qu'ils disaient ! Y'en aura pas…

LES PROBLÈMES

- Pas de sécurité / authentification
- Trop lent à faire des rapports sur 3 mois
- Too many open files (Même après avoir une limite à 64k)

LES PROBLÈMES – PAS DE SÉCURITÉ

- Il ne possède pas :
  - de système d'encryption node <> client
  - d'encryption node <> node
  - de système d'authentification client <> node
  - de système d'authentification node <> node

- Existe des plugins:
  - X-Pack, anciennement Shield - $$$
  - ARMOR, open source, peu de support

LES PROBLÈMES – TROP LENT À FAIRE DES RAPPORTS

- Faire des rapports sur plusieurs mois était vraiment lent voir planté
- En relançant plusieurs fois le même rapport, il pouvait fonctionner

- Voir le problème Too many open files

PROBLÈMES – TOO MANY OPEN FILES

- Mon problème préféré ! Et le plus tough à fixer.
- Impossible de mettre *nofile* à *unlimited* avec centos, ES l'override
- 1 index = 5 shards + 5 shards de replica (by default)
- 1 shard = 1 process lucene = plusieurs file descriptor
- Fail random après un certain temps, ça peut être le port 9200 qui plante…
- *Si ça vous arrive, on pourra discuter de ma solution un peu pas propre du tout.*

BONNES PRATIQUES

Un peu découvert sur le tas

BONNES PRATIQUES – CLUSTER DE LOGS

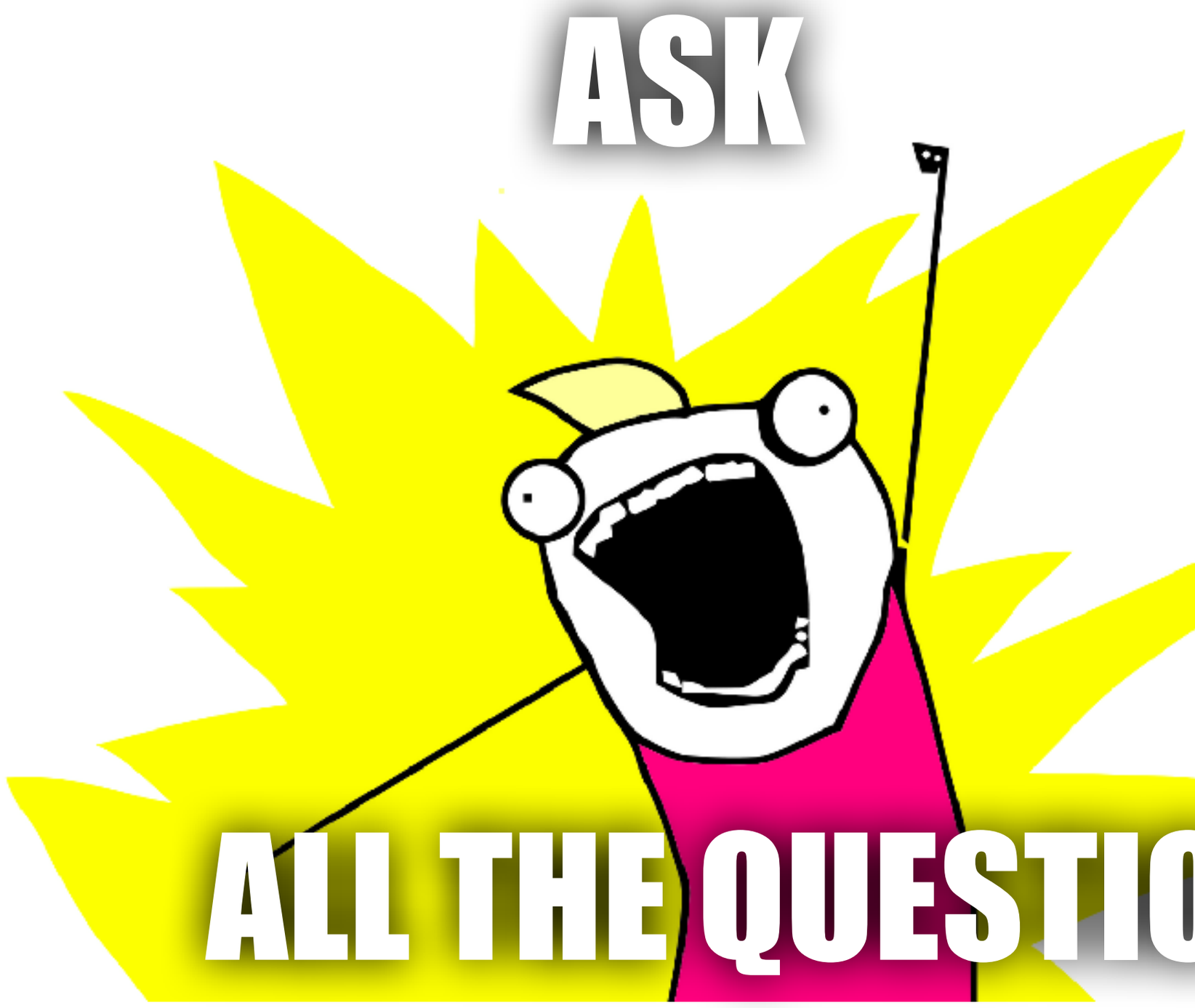
- **Avoir minimum 3 nodes (HA)**
- Augmenter de 2 ensuite
- **Avant 10 nodes, les nodes devrait être toute master=true et data=true**
- Choisir des serveurs moyen au lieu de gros serveurs
- Désactiver le Raid, ne pas utiliser de SAN / NAS
  - ES le gère pour nous, c'est une perte d'espace

BONNES PRATIQUES – CLUSTER DE LOGS

- Bien configurer le nombre de shards
  - On peut le réduire par après (ES >= 5.0) mais pas l'augmenter
  - **Ne pas mettre trop de shard !**
- Bien configurer la granularité de nos indexes (daily / weekly /…)
  - **Pour des logs, ne jamais utiliser qu'un seul index**
- Réduire le nombre de shard et d'index avec le temps
  - Si le nombre de document est assez faible 1 shard + 1 replica par index
  - Regrouper les daily en weekly, weekly en monthly suivant le volume

DEMO

Vas-y ! Envoie la sauce !



Mais pas trop là, j'fais que présenter la job des autres