Présentation et installation des outils

Guillaume.Fay@univ-paris1.fr

esup portail

Plan

- Elasticsearch
  - Présentation
  - Installation
  - Configuration
  - Plugin Kopf
- Logstash
- Kibana
- Filebeat

Présentation d'elasticsearch

- Elasticsearch a été créé en 2004 par Shay Banon, la version 1 sort en 2014
- Basé sur Apache Lucène (comme son concurrent Solr)
- Moteur de recherche distribué, scalable sur des centaines de serveurs
- API RESTful exposées par web services. Utilisable avec n'importe quel langage de programmation (avec JSON).
- Ils utilisent elasticsearch : Wikipedia, Stackoverflow, Github, ...

Pré-requis et conseils pour l'installation

- Requiert un JDK 7 ou supérieur (Elastic.co préconise un JDK 8 Oracle)
- Prévoir beaucoup de RAM
  - Ne pas allouer plus de 50 % de la RAM disponible à ES.
  - Ne pas allouer plus de 32 Go à ES
- CPU : Privilégier beaucoup de cœurs plutôt qu'une haute fréquence

Installation d’elasticsearch

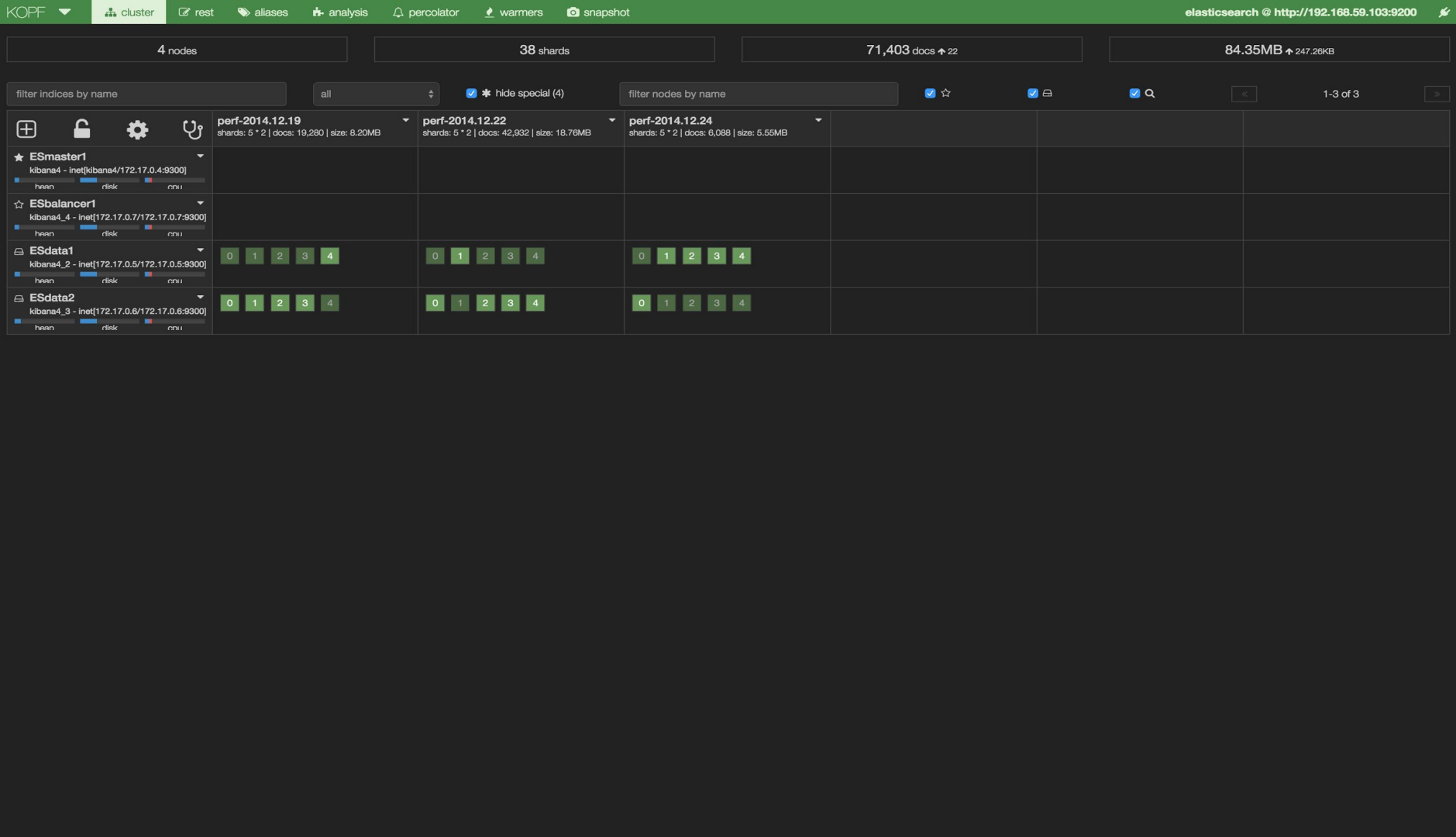
- Installation via dépôt (APT)
  - wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
  - echo "deb https://packages.elastic.co/elasticsearch/2.x/debian stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-2.x.list
  - sudo apt-get update && sudo apt-get install elasticsearch
- Installation manuelle
  - curl -L -O https://download.elastic.co/elasticsearch/release/org/elasticsearch/distribution/tar/elasticsearch/2.3.3/elasticsearch-2.3.3.tar.gz
  - tar -xvf elasticsearch-2.3.3.tar.gz

Configuration d'elasticsearch

- Fichier de configuration : /etc/elasticsearch/elasticsearch.yml
- cluster.name
  - Renseigne le nom du cluster, important pour la discovery.
- node.name
  - Renseigne le nom du nœud, par défaut un personnage Marvel choisi aléatoirement.
- indices.fielddata.cache.size
  - Permet de limiter l'espace mémoire alloué au fielddata cache (aggrégations, tris)
- path.data
  - Chemin de stockage des données du noeud
- path.repo
  - Chemin de stockage des snapshots du noeud

Le plugin Kopf

- Permet d'avoir une interface graphique pour monitorer le cluster
- Alternative : Marvel développé par Elastic.co
- Installation
  - $ES_HOME/bin/plugin --install lmenezes/elasticsearch-kopf
  - Fichier de configuration $ES_HOME/plugins/_site/kopf_external_settings.json
  - URL par défaut : http://localhost:9200/_plugin/kopf


KOPF
cluster
rest
aliases
analysis
percolator
warmers
snapshot
elasticsearch @ http://192.168.59.103:9200
4 nodes
38 shards
71,403 docs ↑ 22
84.35MB ↑ 247.26KB
filter indices by name
all
hide special (4)
filter nodes by name
1-3 of 3
perf-2014.12.19
shards: 5 * 2 | docs: 19,280 | size: 8.20MB
perf-2014.12.22
shards: 5 * 2 | docs: 42,932 | size: 18.76MB
perf-2014.12.24
shards: 5 * 2 | docs: 6,088 | size: 5.55MB
ESmaster1
kibana4 - inet[kibana4/172.17.0.4:9300]
heap
disk
cpu
ESbalancer1
kibana4_4 - inet[172.17.0.7/172.17.0.7:9300]
heap
disk
cpu
ESdata1
kibana4_2 - inet[172.17.0.5/172.17.0.5:9300]
heap
disk
cpu
0 1 2 3 4
0 1 2 3 4
0 1 2 3 4
ESdata2
kibana4_3 - inet[172.17.0.6/172.17.0.6:9300]
heap
disk
cpu
0 1 2 3 4
0 1 2 3 4
0 1 2 3 4

Logstash : Présentation

- Logiciel servant à parser les logs. On peut voir Logstash comme un tunnel dans lequel passe les logs.
- Une configuration Logstash est composée de trois éléments de base : input, filter et output.
    - Input : Source (un fichier, filebeat, elasticsearch)
    - Filter : Dans cette partie, on peut enrichir et travailler sur les logs.
    - Output : (elasticsearch, sdtout, ...)

Logstash : Installation

- Installation via dépôt (APT)
  - wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
  - echo "deb https://packages.elastic.co/logstash/2.3/debian stable main" | sudo tee -a /etc/apt/sources.list
  - sudo apt-get update && sudo apt-get install logstash
- Installation manuelle
  - Télécharger et décompresser logstash

Kibana : Présentation

- Kibana permet de créer des indicateurs et de consulter les données contenues dans elasticsearch
- Visualisation : tableaux, graphiques, cartes, ...
- Dashboard : regroupement de visualisations

Kibana : Installation

- Installation via un dépôt (APT)
  - wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
  - echo "deb http://packages.elastic.co/kibana/4.5/debian stable main" | sudo tee -a /etc/apt/sources.list
  - sudo apt-get update && sudo apt-get install kibana
- Installation manuelle
  - Télécharger et décompresser

Plugin Sense

- Le plugin Sense permet de faire des requêtes complexes en Query DSL.
- Coloration syntaxique et auto complétion
- Installation
  - ./bin/kibana plugin --install elastic/sense
  - ./bin/kibana

Server localhost:9200

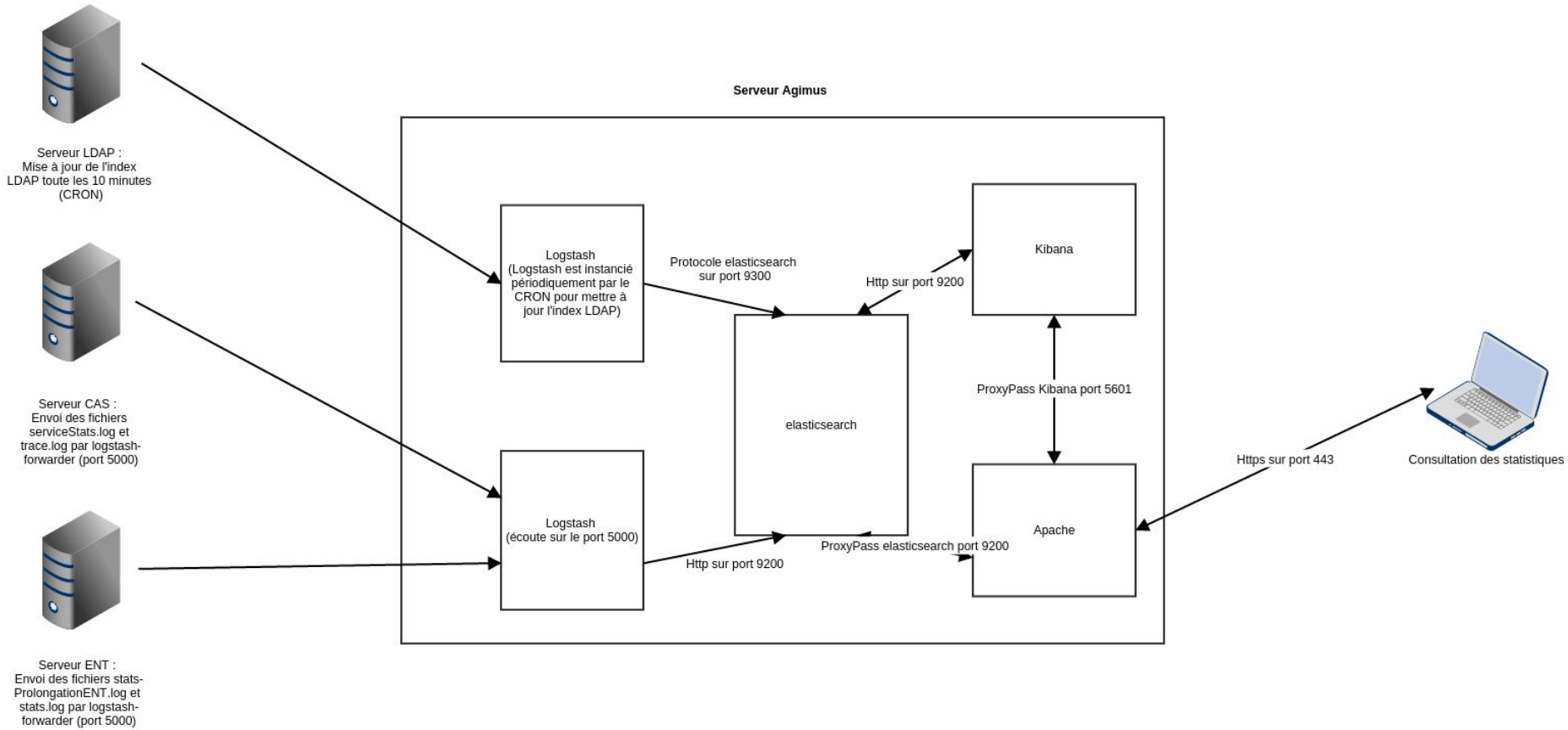
```
# Delete all data in the `website` index
DELETE /website

# Create a document with ID 123
PUT /website/blog/123
{
  "title": "My first blog entry",
  "text":  "Just trying this out...",
  "date":  "2014/01/01"
}

# Search!
GET website/_search
{
  "query": {
    "match": {
      "title": "blog"
    }
  }
}



# Delete all data in the `website` index
DELETE /website

# Create a document with ID 123
PUT /website/blog/123
{
  "title": "My first blog entry",
  "text":  "Just trying this out...",
  "date":  "2014/01/01"
}

# Search!
GET website/_search
{
```

Filebeat : Présentation

- Surveille un ou plusieurs fichiers et envoie les modifications vers un output.
- Permet de configurer avec précisions les informations à envoyer
- L'output peut être :
  - Logstash
  - Elasticsearch
  - Fichier
- Beaucoup plus fiable que son prédécesseur logstash-forwarder.

Filebeat : Installation

- Installation via dépôt
- Installation manuelle
  - curl -L -O https://download.elastic.co/beats/filebeat/filebeat_1.2.3_amd64.deb
  - sudo dpkg -i filebeat_1.2.3_amd64.deb


Serveur Agimus
Serveur LDAP :
Mise à jour de l'index LDAP toute les 10 minutes (CRON)
Serveur CAS :
Envoi des fichiers serviceStats.log et trace.log par logstash-forwarder (port 5000)
Serveur ENT :
Envoi des fichiers stats-ProlongationENT.log et stats.log par logstash-forwarder (port 5000)
Logstash
(Logstash est instancié périodiquement par le CRON pour mettre à jour l'index LDAP)
Logstash
(écoute sur le port 5000)
Protocole elasticsearch sur port 9300
Http sur port 9200
Http sur port 9200
ProxyPass elasticsearch port 9200
elasticsearch
Kibana
ProxyPass Kibana port 5601
Apache
Https sur port 443
Consultation des statistiques