



Agimus-NG : Workshop

Julien Marchal
Guillaume Colson



Nicolas CAN
Ines Wallon



Sommaire

- ▶ Principe de fonctionnement
- ▶ Installation des briques nécessaires
- ▶ Configuration et prise en main d'Elasticsearch
- ▶ Création de graphiques et de tableaux de bord
- ▶ Discussion autour de la démarche d'indicateur



Principe de fonctionnement



Principe de fonctionnement

Principe de fonctionnement

► Documentation Wiki :

<https://www.esup-portail.org/wiki/x/BIC0GQ>



Principe de fonctionnement

► Modification du serveur CAS

► TRACE-ME

<https://www.esup-portail.org/wiki/display/AGIMUSNG/1+-+Modification+du+serveur+CAS>

- ajout du cookie lors de l'authentification
- stockage de la paire cookie<->uid



Principe de fonctionnement

► Modification du serveur CAS

► TRACE-ME

► Suivi des logs applicatifs (facultatif)

Nouveau fichier de logs contenant ID et service

Intégré dans

<https://github.com/EsupPortail/cas-toolbox-new>



Principe de fonctionnement

- ▶ Modification du serveur CAS
 - ▶ Enrichissement des logs avec vos données avec logstash
 - ▶ Modification des applications
- ajout du cookie dans les logs :
- ▶ Pour apache → `%{AGIMUS}C`
 - ▶ Pour lighttpd → `%{Cookie}i`



Principe de fonctionnement

- ▶ Modification du serveur CAS
- ▶ Enrichissement des logs avec vos données avec logstash
 - ▶ Modification des applications
 - ▶ Récupération des logs
 - ▶ Modification ou création de la configuration logstash
 - ▶ Enrichissement
 - ▶ Anonymisation



Principe de fonctionnement

- ▶ Modification du serveur CAS
- ▶ Enrichissement des logs avec vos données avec logstash
- ▶ Stockage dans elasticsearch
 - ▶ Un index par jour
 - ▶ Un type par application

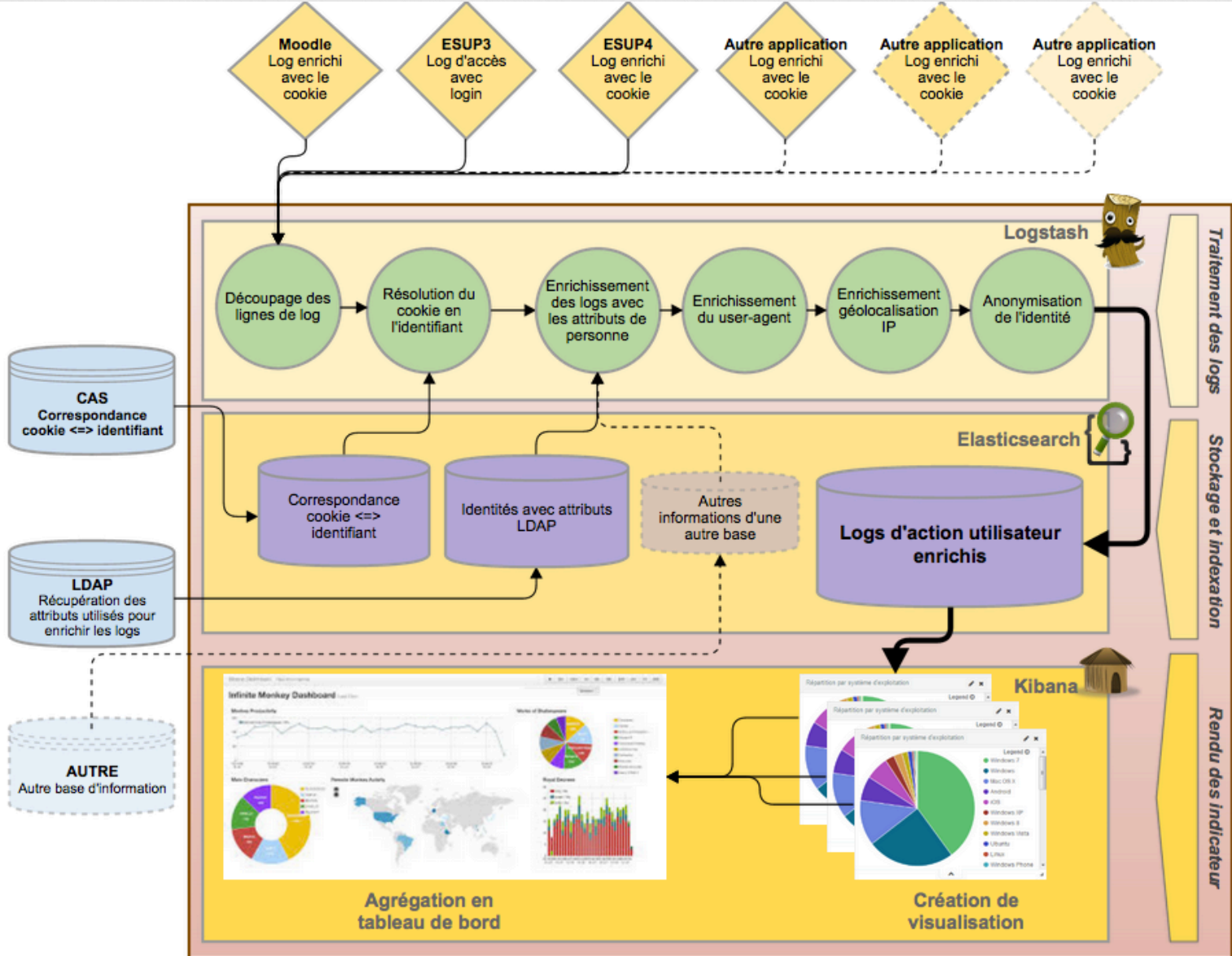


Principe de fonctionnement

- ▶ Modification du serveur CAS
- ▶ Enrichissement des logs avec vos données avec logstash
- ▶ Stockage dans elasticsearch
- ▶ Agrégation et affichage dans kibana
 - ▶ Basé sur les agrégations elasticsearch
 - ▶ Modifier ou créer les graphiques à partir de vos index



Principe de fonctionnement



Installation des briques nécessaires



Installations des briques nécessaires

Installation des briques nécessaires

► Installation spécifique à la machine virtuelle

► Attributs LDAP disponibles :

- eduPersonPrimaryAffiliation
- supannAffectation
- supannOrganisme

► Documentation en ligne :

<https://www.esup-portail.org/wiki/x/BoC0GQ>



Installation des briques nécessaires

► Installations des rpm Agimus-ng

```
[agimus@agimus ~]$ sudo yum install agimus-ng-demo
```

► Lancement des services

```
[agimus@agimus ~]$ sudo service slapd start  
[agimus@agimus ~]$ sudo service elasticsearch start  
[agimus@agimus ~]$ sudo service kibana start
```

► Accès au répertoire de travail

```
[agimus@agimus ~]$ cd /opt/agimus-ng  
[agimus@agimus agimus-ng]$ sudo chown -R agimus: .
```



Installation des briques nécessaires

► Vérification

```
[agimus@agimus agimus-ng]$ curl -XGET "localhost:9200"
{
  "status" : 200,
  "name" : "Awesome Android",
  "cluster_name" : "Agimus-ng",
  "version" : {
    "number" : "1.4.5",
    "build_hash" :
"2aaf797f2a571dcb779a3b61180afe8390ab61f9",
    "build_timestamp" : "2015-04-27T08:06:06Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
```

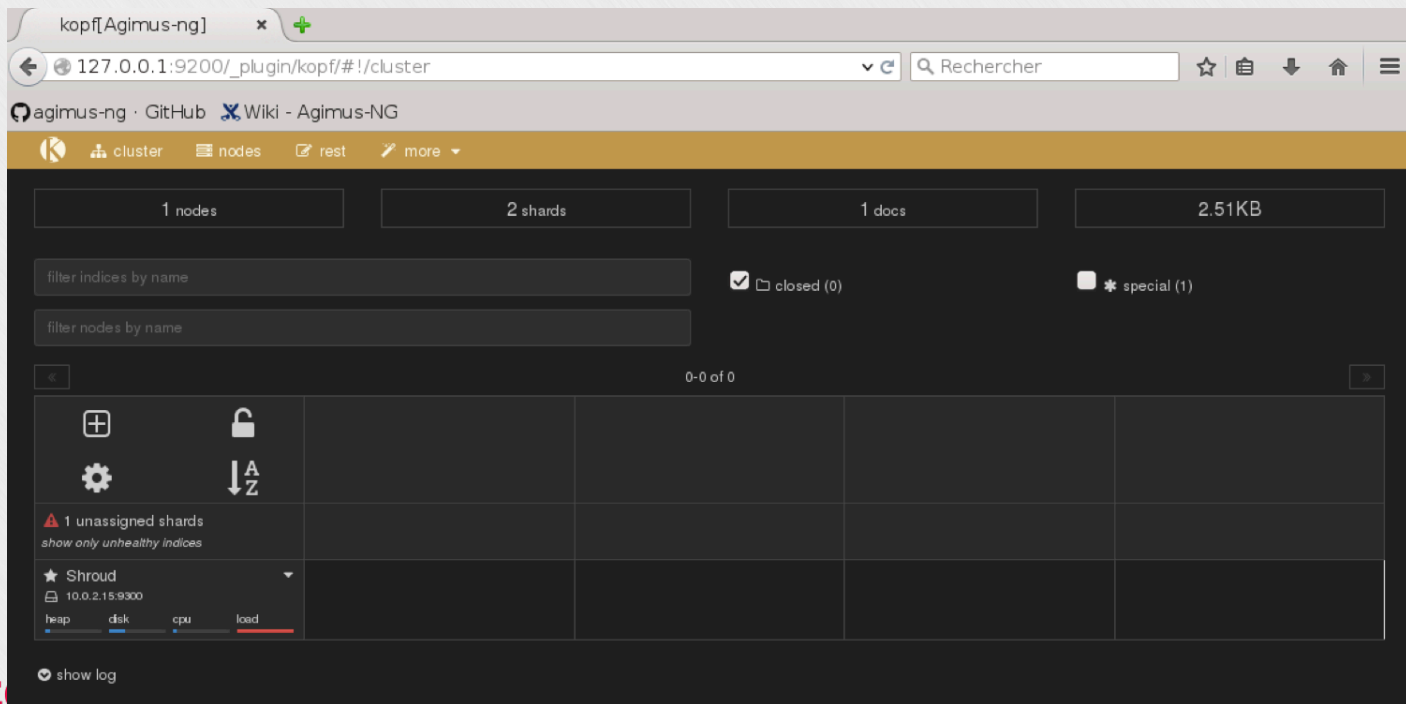
Installation des briques nécessaires

► Vérification sur navigateur : Elasticsearch/kopf

Kopf est un plugin d'ES installé sur la VM :

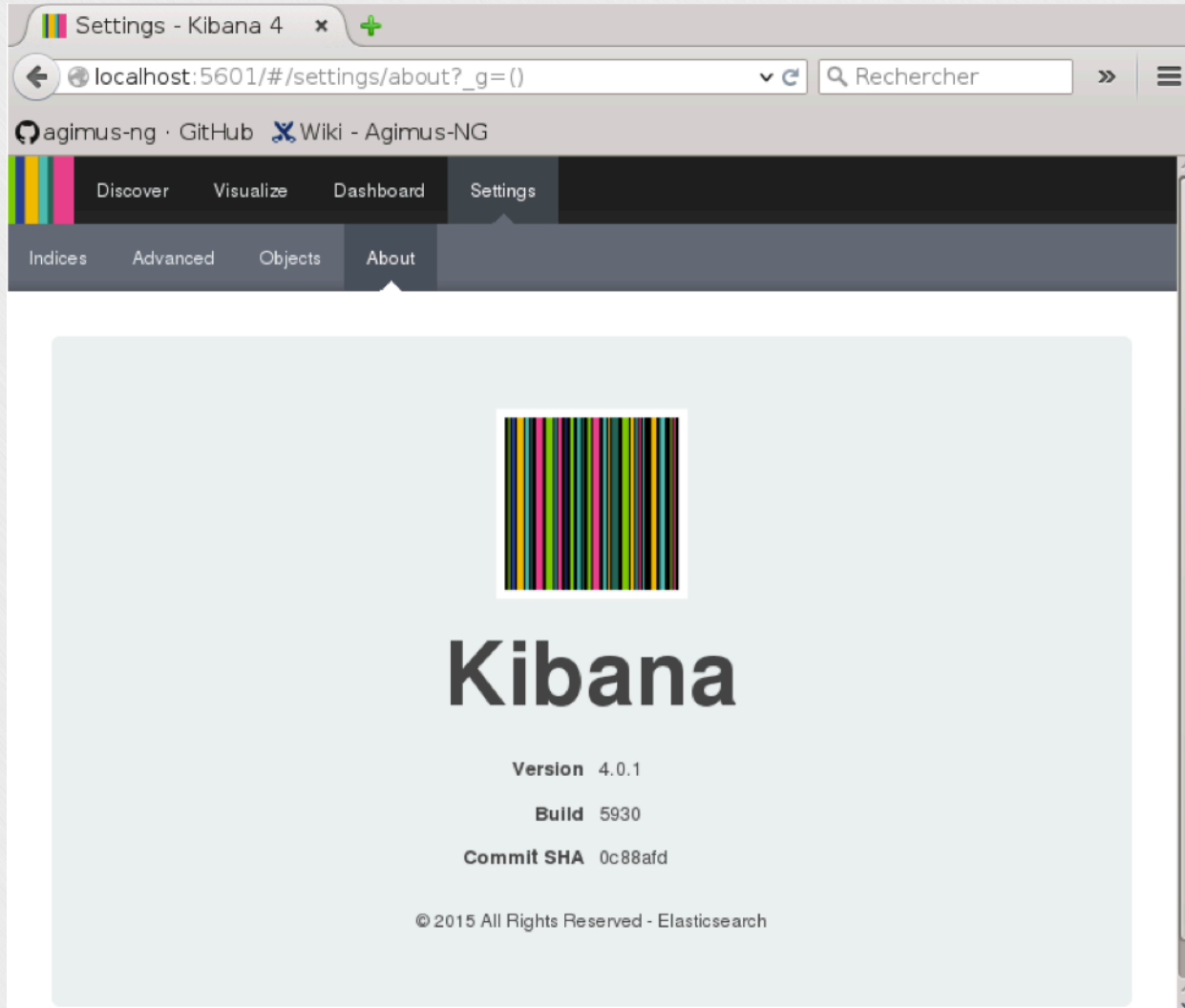
<https://github.com/lmenezes/elasticsearch-kopf>

Il existe d'autres plugins pour utiliser ou gérer ES, par exemple Marvel et son onglet Sense qui facilite le requêtage dans ES (auto-complétion etc.)



Installation des briques nécessaires

► Vérification sur navigateur : Kibana



The screenshot shows a web browser window with the address bar displaying `localhost:5601/#/settings/about?_g=()`. The page title is "Settings - Kibana 4". The browser's search bar contains the text "Rechercher". The navigation menu includes "Discover", "Visualize", "Dashboard", and "Settings". The "Settings" menu is expanded, showing "Indices", "Advanced", "Objects", and "About". The "About" page features the Kibana logo (a square of vertical bars) and the following information:

- Version** 4.0.1
- Build** 5930
- Commit SHA** 0c88afd

At the bottom of the page, it says "© 2015 All Rights Reserved - Elasticsearch".

Installation des briques nécessaires

► Tests

► Présentation de Logstash : ETL

```
[agimus@agimus agimus-ng]$ /lib64/logstash/bin/  
logstash
```

No command given

Usage: logstash <command> [command args]

Run a command with the `--help` flag to see the arguments.

For example: `logstash agent -help`

Available commands:

`agent` - runs the logstash agent

`version` - emits version info about this logstash



Installation des briques nécessaires

► Tests

► Présentation de Logstash : ETL

```
[agimus@agimus agimus-ng]$ /lib64/logstash/bin/logstash -e
'input {stdin{}} output {stdout{}}'
Logstash startup completed
Hello world
2015-10-10T09:08:13.338Z agimus.sandbox Hello world
^C
2015-10-10T09:08:17.237Z agimus.sandbox
SIGINT received. Shutting down the pipeline. {:level=>:warn}
Received shutdown signal, but pipeline is still waiting for
in-flight events
to be processed. Sending another ^C will force quit Logstash,
but this may cause
data loss. {:level=>:warn}

Logstash shutdown completed
```

Installation des briques nécessaires

► Tests

► Présentation de Logstash : ETL

```
[agimus@agimus agimus-ng]$ /lib64/logstash/bin/logstash -e  
'input {stdin{}} output {stdout{codec=>rubydebug}}'
```

```
Logstash startup completed
```

```
hello world
```

```
{
```

```
  "message" => "hello world",
```

```
  "@version" => "1",
```

```
  "@timestamp" => "2015-10-10T09:12:31.405Z",
```

```
  "host" => "agimus.sandbox"
```

```
}
```

```
^CSIGINT received. Shutting down the pipeline.
```

```
{:level=>:warn}
```

```
Logstash shutdown completed
```

Installation des briques nécessaires

► Déploiement

► Présentation Deploy_univ.py

```
[agimus@agimus agimus-ng]$ cd /opt/agimus-ng/github/scripts/  
[agimus@agimus scripts]$ python deploy_univ.py  
eduPersonPrimaryAffiliation supannAffectation supannOrganisme  
The modified files are available in the build directory: /  
opt/agimus-ng/github/build
```

Attention, toutes les modifications se font dans build !



Installation des briques nécessaires

► Déploiement

► Présentation Deploy_univ.py

► Test du LDAP

Paramétrer LDAPSearch dans **logstash/test-logstash.conf**

```
LDAPSearch {  
  host => "localhost"  
  dn => "cn=admin,dc=univ,dc=fr"  
  password => "esup"  
  filter => "(&(objectclass=person)(uid=pers*))"  
  base => "ou=people,dc=univ,dc=fr"  
  attrs => ['uid', 'eduPersonPrimaryAffiliation',  
  'supannAffectation', 'supannOrganisme']  
}
```



Installation des briques nécessaires

► Tests - résultats

► Logstash

```
[agimus@agimus logstash]$ cd /opt/agimus-ng/github/build/logstash
[agimus@agimus logstash]$ vim test-logstash.conf
[agimus@agimus logstash]$ /lib64/logstash/bin/logstash -f test-
logstash.conf
Logstash startup completed
{
    "@version" => "1",
    "@timestamp" => "2015-10-10T09:20:03.014Z",
    "host" => "localhost",
    "supannAffectation" => [
      [0] "scd"
    ],
    ...
}
```

Installation des briques nécessaires

► Tests

► Logstash

► Elasticsearch

```
[agimus@agimus logstash]$ curl -XGET "localhost:9200/_cat/nodes"  
agimus.sandbox 10.0.2.15 4 62 0.05 d * Awesome Android
```



Installation des briques nécessaires

► Tests

- Logstash
- Elasticsearch
- module elasticsearch de python

```
[agimus@agimus logstash]$ cd /opt/agimus-ng/github/  
[agimus@agimus github]$ python scripts/test-elasticsearch.py  
L'index test-index est cree  
Il y a 1 document dans l'index test-index :  
2015-10-10T11:29:48.801632 testeur: Elasticsearch fonctionne  
dans python  
On le supprime
```



Installation des briques nécessaires

► Paramétrage elasticsearch

► Ajout des templates ldap et logs_agimus

```
[agimus@agimus github]$ cd /opt/agimus-ng/  
[agimus@agimus agimus-ng]$ chmod u+x ajout_templates.sh  
[agimus@agimus agimus-ng]$ ./ajout_templates.sh  
{"acknowledged":true}{"acknowledged":true}
```



Installation des briques nécessaires

► Paramétrage elasticsearch

► Ajout des templates ldap et logs_agimus

► Vérification

```
[agimus@agimus agimus-ng]$ curl -XGET "http://localhost:9200/_template/?pretty"
{
  "logs_agimus" : {
    "order" : 1,
    "template" : "logstash-*",
    "settings" : {
      "index.number_of_replicas" : "0",
      "index.number_of_shards" : "1"
    },
    ...
  }
}
```



Principe de fonctionnement

► Test du traitement des logs avec logstash : LDAP

1. Configurez le fichier logstash-ldap.conf

Attention, le cluster est « Agimus-ng »

```
LDAPSearch {  
  host => "localhost"  
  dn => "cn=admin,dc=univ,dc=fr"  
  password => "esup"  
  filter => "(&(objectclass=person)(uid=pers*))"  
  base => "ou=people,dc=univ,dc=fr"  
  attrs => ['uid', 'eduPersonPrimaryAffiliation',  
  'supannAffectation', 'supannOrganisme']  
}
```

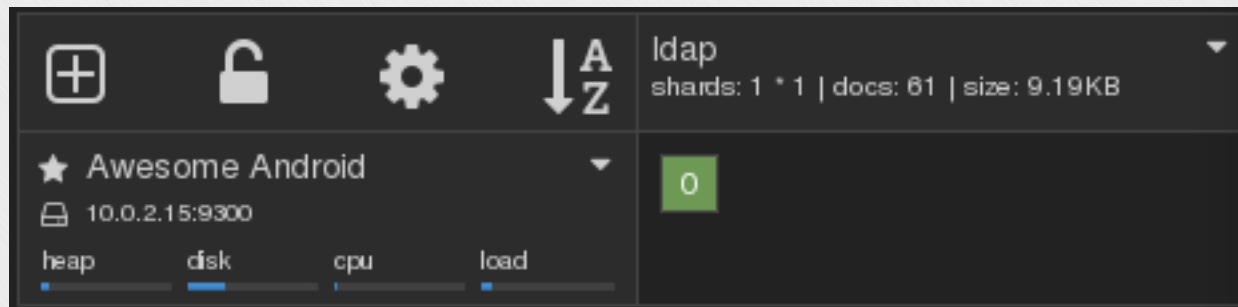


Principe de fonctionnement

► Test du traitement des logs avec logstash : LDAP

2. Lancer le traitement pour charger ES avec les data du ldap

```
[agimus@agimus logstash]$ cd /opt/agimus-ng/github/build/logstash
[agimus@agimus logstash]$ vim logstash-ldap.conf
[agimus@agimus logstash]$ /lib64/logstash/bin/logstash -f logstash-ldap.conf
```



Principe de fonctionnement

► Test du traitement des logs avec logstash : Trace

1. On récupère une ligne de log trace
2. On modifie le logstash-trace.conf pour tester

```
[agimus@agimus logstash]$ vim logstash-trace.conf
[agimus@agimus logstash]$ tail -n 1 /opt/agimus-ng/demo/logs/2015/09/25/trace.log
TRACE-81053-i4zu39i0RinRzAgrEHKLRNbocefwy3jV4WSf7ygLFbNE7BWEr3-cas1:pers1
[agimus@agimus logstash]$ /lib64/logstash/bin/logstash -f logstash-trace.conf
Logstash startup completed
TRACE-81053-i4zu39i0RinRzAgrEHKLRNbocefwy3jV4WSf7ygLFbNE7BWEr3-cas1:pers1
{
  "message" => "TRACE-81053-
i4zu39i0RinRzAgrEHKLRNbocefwy3jV4WSf7ygLFbNE7BWEr3-cas1:pers1",
  "@version" => "1",
  "@timestamp" => "2015-10-10T10:11:17.445Z",
  ...
}
^CSIGINT received. Shutting down the pipeline. {:level=>:warn}

Logstash shutdown completed
```

Principe de fonctionnement

► Test du traitement des logs avec logstash : Trace

3. Réinitialiser le fichier logstash-trace.conf

Attention, le cluster est « Agimus-ng »

4. Lancer le traitement pour charger ES avec les data du fichier

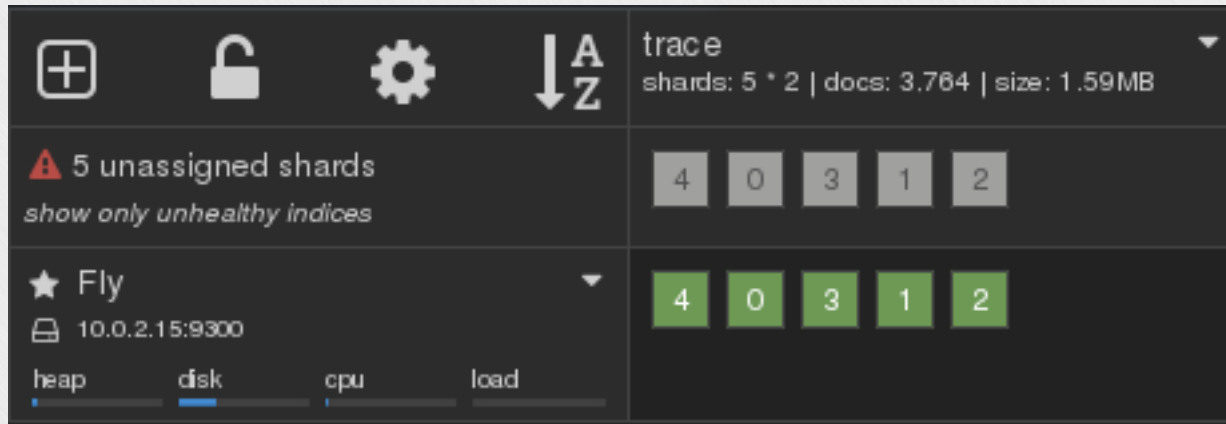
```
[agimus@agimus logstash]$ cat /opt/agimus-ng/demo/logs/2015/09/25/trace.log | /lib64/logstash/bin/logstash -f logstash-trace.conf
```



Principe de fonctionnement

► Test du traitement des logs avec logstash : Trace

5. Résultat :



Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

1. On récupère une ligne de log avec cookie

```
[agimus@agimus logstash]$ tail -n 1 /opt/agimus-ng/demo/logs/2015/09/25/moodle-access.log
```

```
90.7.17.56 - 3 687/51872 51287 - [25/Sep/2015:08:07:53 +0200] "GET moodle.univ-lille1.fr/course/view.php?id=157 HTTP/1.1" 200 "http://moodle.univ-lille1.fr/my/" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0" _pk_id.2.a9d0=761c1921eeb0f26f.1442837436.6.1443160721.1443160453.; _pk_ref.2.a9d0=%5B%22%22%2C%22%22%2C1443160453%2C%22https%3A%2F%2Fwww.google.fr%22%5D; AGIMUS=TRACE-70604-ZzdxHctoH3kL1bQK4G0hJF2V0zPUEXGryHVfnluUuJtuBySVfP-sso-cas.univ-lille1.fr; MoodleSessionmdlilleun=mql8u9c6jo818bsdl8b8hdghq2; _pk_ses.2.a9d0=*
```

2. On modifie le fichier logstash-moodle.conf (#geoip et #drop)



Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

3. On test :

```
[agimus@agimus logstash]$  
/lib64/logstash/bin/logstash -f logstash-moodle.conf
```



Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

3. On test :

1. Premier test failure : grok parse ! Changer le pattern...

```
grok {
  #match => [ "message", "%{IPORHOST:clientip} %{USER:ident} %
{USER:auth} %{NUMBER} \[%{HTTPDATE:requestdate}\] \"%{WORD:method} %
{DATA:request} HTTP/%{NUMBER:httpversion}\" %{NUMBER:response} (?:%
{NUMBER:bytes}|-) \"%{DATA:referrer}\" \"%{DATA:agent}\" (?
<agimus>[0-9A-Za-z-]*)" ]
  match => { "message" => "%{IPORHOST:clientip} (?:%
{IPORHOST:httpshost}|-) (?:%{NUMBER:timesec}|-) (?:%
{NUMBER:bytesinc}|-)/(?:%{NUMBER:bytesout}|-) (?:%
{NUMBER:bytessent}|-) (?:%{USER:auth}|-) \[%{HTTPDATE:requestdate}\]
\"(?:%{WORD:method} %{NOTSPACE:request}(?: HTTP/%
{NUMBER:httpversion})|-)\\" %{NUMBER:response} %{QS:referrer} %
{QS:agent} (?:.*AGIMUS=%{NOTSPACE:agimus}.*|.*)" }
}
```

Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

3. On test :

1. Premier test failure : grok parse ! Changer le pattern...

Doc :

<https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html>

Test pattern : <http://grokdebug.herokuapp.com/>

2. Deuxième test : Failed parsing date from field

→ #locale

Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

3. On test :

3. Troisième| test OK ...

```
{
  "@version" => "1",
  "@timestamp" => "2015-09-25T06:07:53.000Z",
  "clientip" => "90.7.17.56",
  "timesec" => "3",
  "bytesinc" => "687",
  "bytesout" => "51872",
  "bytessent" => "51287",
  "request" => "moodle.univ-lille1.fr/course/view.php?id=157",
  "referrer" => "\"http://moodle.univ-lille1.fr/my/\"",
  "agimus" => "TRACE-70604-ZzdxHctoH3kL1bQK4G0hJF2V0zPUEXGryHVfnluUuJtuBySVfP-sso-cas.univ-lille1.fr",
  "os" => "Windows 8.1",
  "os_name" => "Windows 8.1",
  "device" => "other",
  "geopip" => {
    "location" => [
      1.6046000000000005,
      50.720699999999994
    ]
  },
  "uid" => "735d55f0552bf1f9ab3ae25f618e07b76e3ca58d",
  "browser" => "firefox"
}
```

SI TOUT OK ALORS ON
REINITIALISE LE FICHER ET
ON LANCE LE TRAITEMENT

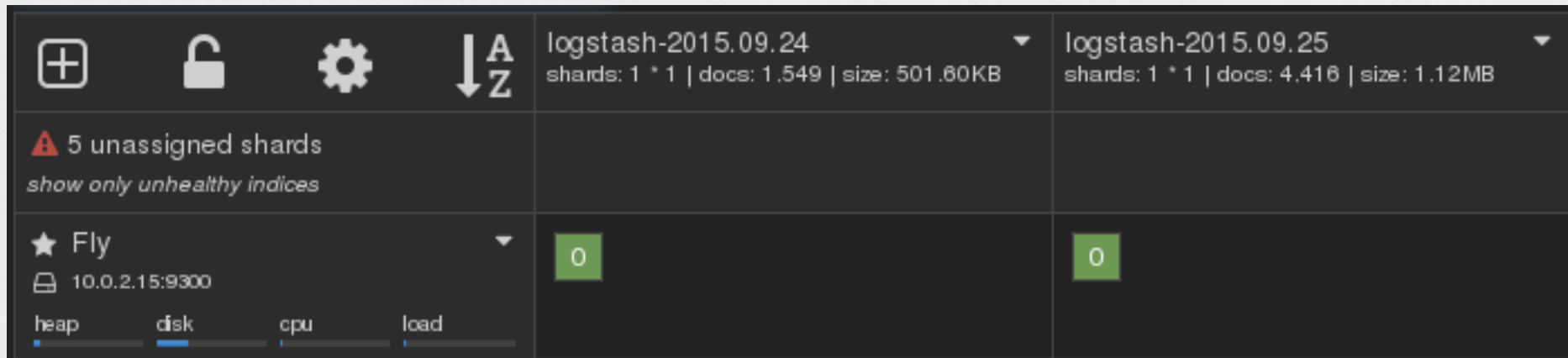
Attention, le cluster est « Agimus-ng »

Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

```
[agimus@agimus logstash]$ vim logstash-moodle.conf
[agimus@agimus logstash]$
cat /opt/agimus-ng/demo/logs/2015/09/25/moodle-access.log | /
lib64/logstash/bin/logstash -f logstash-moodle.conf
```

Résultat:

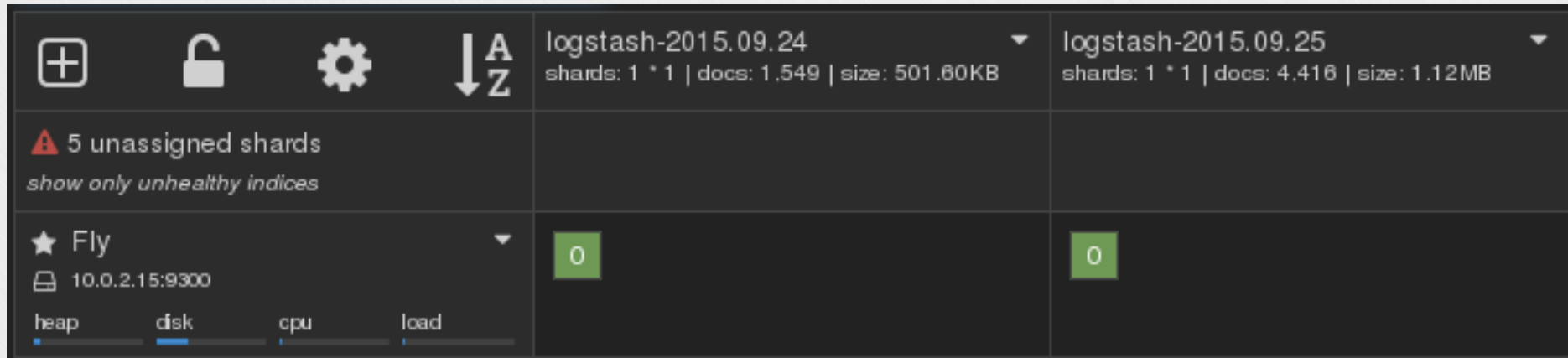


Principe de fonctionnement

► Test du traitement des logs avec logstash : Esup etc.

Recommencez les mêmes étapes pour traiter les logs esup4

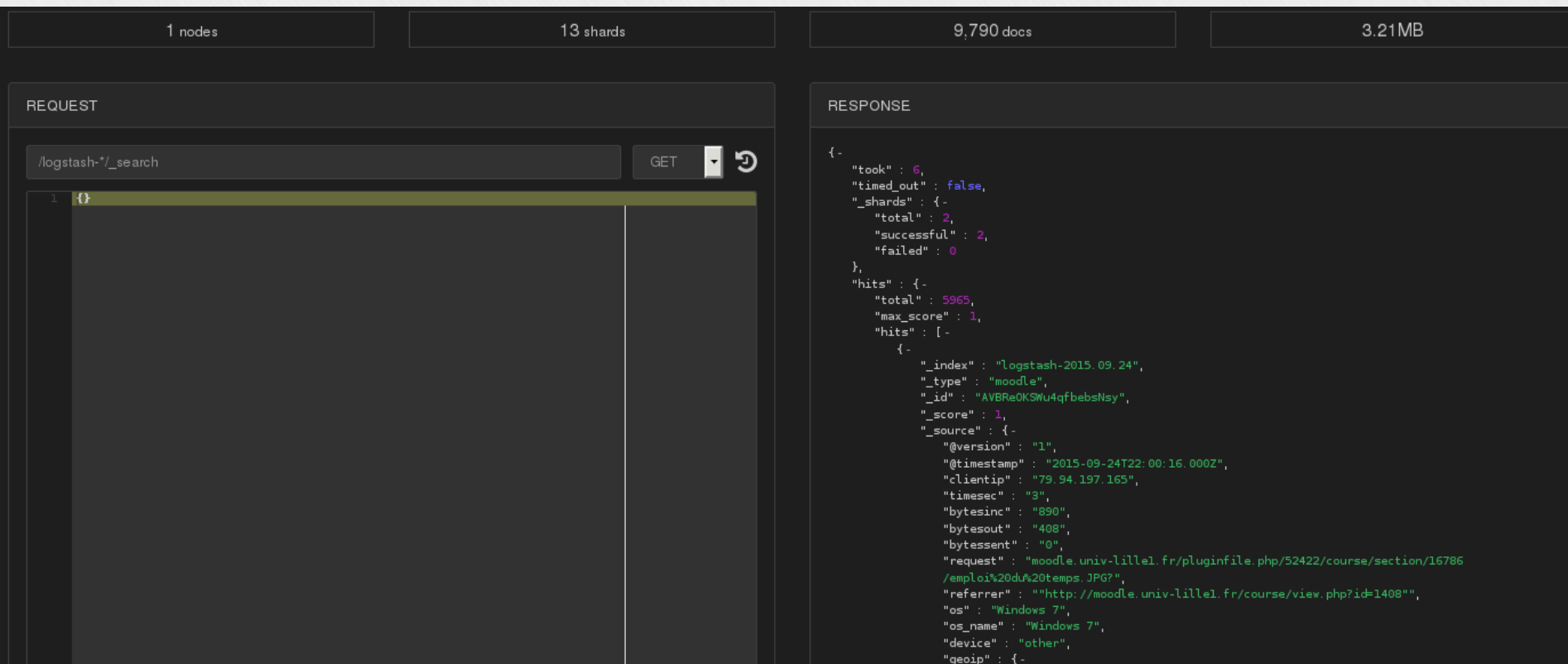
```
[agimus@agimus logstash]$ vim logstash-esup4.conf
[agimus@agimus logstash]$
cat /opt/agimus-ng/demo/logs/2015/09/25/access-ent.log | /
lib64/logstash/bin/logstash -f logstash-esup4.conf
```



Principe de fonctionnement

► Test du traitement des logs avec logstash : Moodle

Résultat dans ES:



The screenshot displays the Elasticsearch Kibana interface. At the top, four summary boxes show: 1 nodes, 13 shards, 9,790 docs, and 3.21MB. The main area is split into 'REQUEST' and 'RESPONSE' sections.

REQUEST

```
/logstash-*/_search
```

RESPONSE

```
{-
  "took" : 6,
  "timed_out" : false,
  "_shards" : {-
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "hits" : {-
    "total" : 5965,
    "max_score" : 1,
    "hits" : [-
      {-
        "_index" : "logstash-2015.09.24",
        "_type" : "moodle",
        "_id" : "AVBRReOKSwu4qfbebSnsy",
        "_score" : 1,
        "_source" : {-
          "@version" : "1",
          "@timestamp" : "2015-09-24T22:00:16.000Z",
          "clientip" : "79.94.197.165",
          "timesec" : "3",
          "bytesinc" : "890",
          "bytesout" : "408",
          "bytesent" : "0",
          "request" : "moodle.univ-lille1.fr/pluginfile.php/52422/course/section/16786/emploi%20du%20temps.JPG?",
          "referrer" : "http://moodle.univ-lille1.fr/course/view.php?id=1408",
          "os" : "Windows 7",
          "os_name" : "Windows 7",
          "device" : "other",
          "geoip" : {-
```


Principe de fonctionnement

▶ Script quotidien:

▶ Mise en place :

```
[agimus@agimus logstash]$ cp /opt/agimus-ng/github/scripts/daily_batch.sh /opt/agimus-ng/github/build/scripts/.
```

▶ Les différentes sections :

```
[agimus@agimus scripts]$ cd /opt/agimus-ng/github/build/scripts  
[agimus@agimus scripts]$ cat daily_batch.sh
```

▶ Mise en place en crontab

Ex :

```
10 0 * * * /opt/agimus-ng/build/scripts/daily_batch.sh | logger
```



Configuration et prise en main d'Elasticsearch

▶ Initiation à Elasticsearch

▶ Présentation vidéo à cette adresse:

[https://www.esup-portail.org/wiki/pages/viewpage.action?
pageId=439255076#ESUP-Daysn](https://www.esup-portail.org/wiki/pages/viewpage.action?pageId=439255076#ESUP-Daysn)

[°19&AperioEurope-15:15-15:35TechnoExpress:IntroductionàElasticSearch\[FR\]](https://www.esup-portail.org/wiki/pages/viewpage.action?pageId=439255076#ESUP-Daysn%2019&AperioEurope-15:15-15:35TechnoExpress:IntroductionàElasticSearch[FR])

▶ Basé sur Apache Lucène

▶ Moteur de recherche distribué

▶ Indexation complète

► Initiation à Elasticsearch

► Vocabulaire

Cluster : Ensemble de nœuds répondant aux mêmes requêtes

Nœud : Machine physique hébergeant une instance Elasticsearch.

Dans un cluster, le nœud master gère l'assignation des tâches à l'ensemble des nœuds.

Index : Espace logique permettant d'organiser les données

Shard : Instance Lucène stockant réellement les données

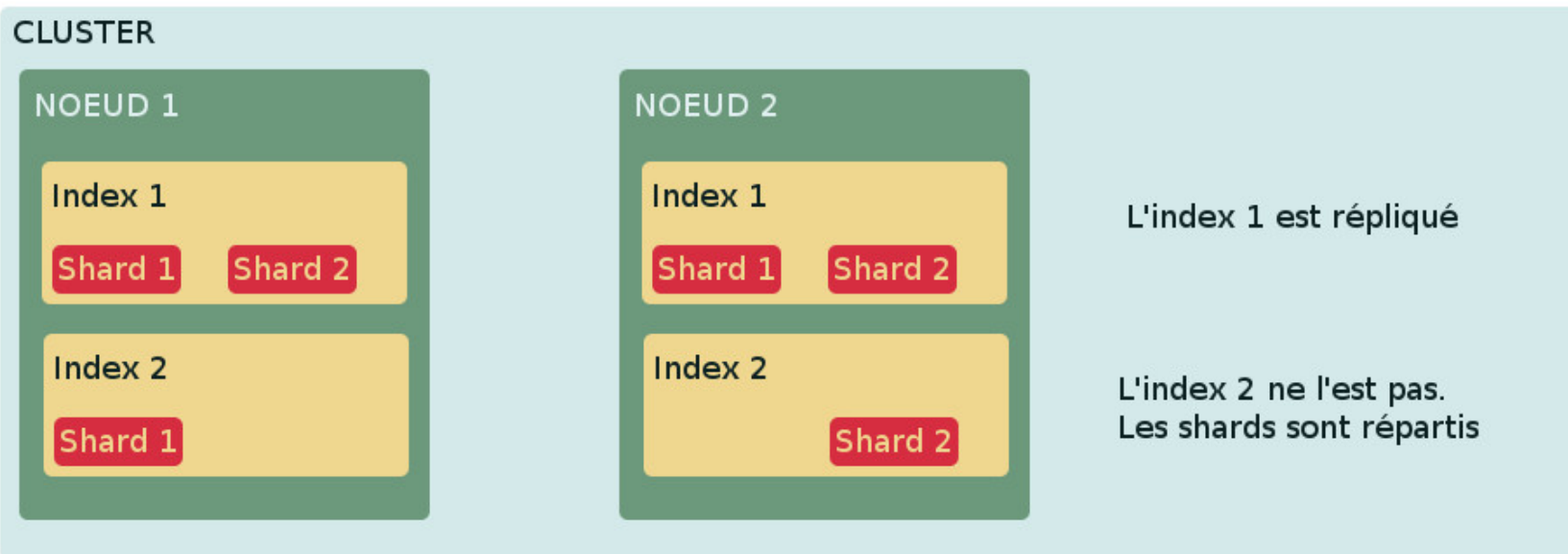
Replicat : Copie d'un index

Alias : Index virtuel pointant vers 1 ou plusieurs index réels

Configuration et prise en main d'Elasticsearch

► Initiation à Elasticsearch

► Vocabulaire



► Initiation à Elasticsearch

► Alimenter un index

```
curl -XPUT 'http://localhost:9200/index_essai/type_essai/1' -d' {  
  "champ1" : "Agimus",  
  "champ2" : "Agimus est en place",  
  "numero" : 325,  
  "champs_multiples" : [  
    "objet 1",  
    "valeur 1"  
  ]  
}'
```

► Initiation à Elasticsearch

► Requête un index

```
curl -XGET 'http://localhost:9200/index_essai/type_essai/1'  
curl -XGET 'http://localhost:9200/index_essai/_search' -d'  
{  
  "query": {  
    "match": {  
      "champ2": "Agimus"  
    }  
  }  
}'
```

► Initiation à Elasticsearch

► Différence Query/Filter

FILTER : Permet de limiter les enregistrements traités (tout ou rien)

QUERY : Permet de calculer le score des enregistrements afin de retourner les plus probants

Les différents types de Query permettent d'ajuster le score et donc les éléments retournés

Configuration et prise en main d'Elasticsearch

► Initiation à Elasticsearch

► Agrégations

Décomptes des résultats par critères sans préjuger des valeurs présentes

```
GET ldap/_search
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "Affiliation": {
      "terms": {
        "field": "eduPersonPrimaryAffiliation.raw",
        "size": 100
      }
    }
  }
}

...,
"aggregations": {
  "Affiliation": {
    "doc_count_error_upper_bound": 0,
    "sum_other_doc_count": 0,
    "buckets": [
      {
        "key": "student",
        "doc_count": 76235
      },
      {
        "key": "teacher",
        "doc_count": 5214
      },
      ...
    ]
  }
}
```

Configuration et prise en main d'Elasticsearch

► Initiation à Elasticsearch : Manipulation

|-> nous allons utiliser le plugin kopf installé sur la VM

Simple requête : `/_search`

Est équivalent à : `/_search`

```
{
  "query": {
    "match_all": {}
  }
}
```

On peut restreindre la recherche sur un index : `/ldap/_search`

```
{
  "query": {
    "match_all": {}
  }
}
```

► Initiation à Elasticsearch : Manipulation suite

requête filtrante : `/ldap/_search?q=eduPersonPrimaryAffiliation:student`

Est équivalente à : `/ldap/_search`

```
{
  "query": {
    "match": {
      "eduPersonPrimaryAffiliation": "student"
    }
  }
}
```

→ Recherche exacte

► Initiation à Elasticsearch : Manipulation suite

Recherche par chaine : /logstash-*/_search

```
{
  "query": {
    "query_string": {
      "query": "_type:moodle AND eduPersonPrimaryAffiliation:student"
    }
  }
}
```

► Initiation à Elasticsearch : Manipulation suite

Recherche par chaine avec agrégation : /logstash-*/_search

```
{
  "query": {
    "query_string": {
      "query": "_type:moodle AND eduPersonPrimaryAffiliation:student"
    }
  },
  "aggs": {
    "affectation": {
      "terms": {
        "field": "supannAffectation.raw",
        "size": 20
      }
    }
  }
}
```

► Initiation à Elasticsearch : Manipulation suite

Recherche par chaine avec agrégation et date : /logstash-*/_search

```
{
  "query": {
    "filtered": {
      "query": {
        "query_string": {
          "query": "_type:moodle AND eduPersonPrimaryAffiliation:student"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
            "gte": "2015-09-25",
            "lte": "2015-09-25"
          }
        }
      }
    }
  }
}
```

. . .

Configuration et prise en main d'Elasticsearch

► Initiation à Elasticsearch : Manipulation suite

Recherche par chaine avec agrégation et date : /logstash-*/_search

```
...
    }
  }
},
"aggs": {
  "affectation": {
    "terms": {
      "field": "supannAffectation.raw",
      "size": 200
    }
  }
}
}
```

Configuration et prise en main d'Elasticsearch

► Initiation à Elasticsearch : Manipulation suite

Utilisez le format brut : raw – exemple agrégation sur champ analysé

```
{
  "query": {
    "filtered": {
      "query": {
        "query_string": {
          "query": "_type:moodle AND eduPersonPrimaryAffiliation:student"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
            "gte": "2015-09-25",
            "lte": "2015-09-25"
          }
        }
      }
    }
  },
  "size": 0,
  "aggs": {
    "affectation": {
      "terms": {
        "field": "request",
        "size": 200
      }
    }
  }
}
```

```
"aggregations" : {
  "affectation" : {
    "doc_count_error_upper_bound" : 2,
    "sum_other_doc_count" : 990,
    "buckets" : [
      {
        "key" : "fr",
        "doc_count" : 1604
      },
      {
        "key" : "lille1",
        "doc_count" : 1604
      },
      {
        "key" : "moodle.univ",
        "doc_count" : 1604
      },
      {
        "key" : "index.php",
        "doc_count" : 553
      },
      ...
    ]
  }
}
```


Configuration et prise en main d'Elasticsearch

► Initiation à Elasticsearch : Manipulation suite

Utilisez le format brut : raw – exemple agrégation sur champ brut

```
{
  "query": {
    "filtered": {
      "query": {
        "query_string": {
          "query": "_type:moodle AND eduPersonPrimaryAffiliation:student"
        }
      },
      "filter": {
        "range": {
          "@timestamp": {
            "gte": "2015-09-25",
            "lte": "2015-09-25"
          }
        }
      }
    },
    "size": 0,
    "aggs": {
      "affectation": {
        "terms": {
          "field": "request.raw",
          "size": 200
        }
      }
    }
  }
}
```

```
"aggregations" : {
  "affectation" : {
    "doc_count_error_upper_bound" : 1,
    "sum_other_doc_count" : 366,
    "buckets" : [
      {
        "key" : "moodle.univ-lille1.fr/login/index.php",
        "doc_count" : 147
      },
      {
        "key" : "moodle.univ-lille1.fr/?",
        "doc_count" : 111
      },
      {
        "key" : "moodle.univ-lille1.fr/my/?",
        "doc_count" : 66
      },
      {
        "key" : "moodle.univ-lille1.fr/index.php?",
        "doc_count" : 56
      },
      ...
    ]
  }
}
```



Création de graphiques et tableaux de bord

Création de graphiques et tableaux de bord

▶ Documentation :

<https://www.esup-portail.org/wiki/display/AGIMUSNG/2+-+Visualisation+des+indicateurs+avec+Kibana>

▶ Prise en main de kibana

- ▶ Configuration -> ajout index
- ▶ Configuration -> création de visualisation
- ▶ Configuration -> création de dashboard

▶ Import des graphiques existants

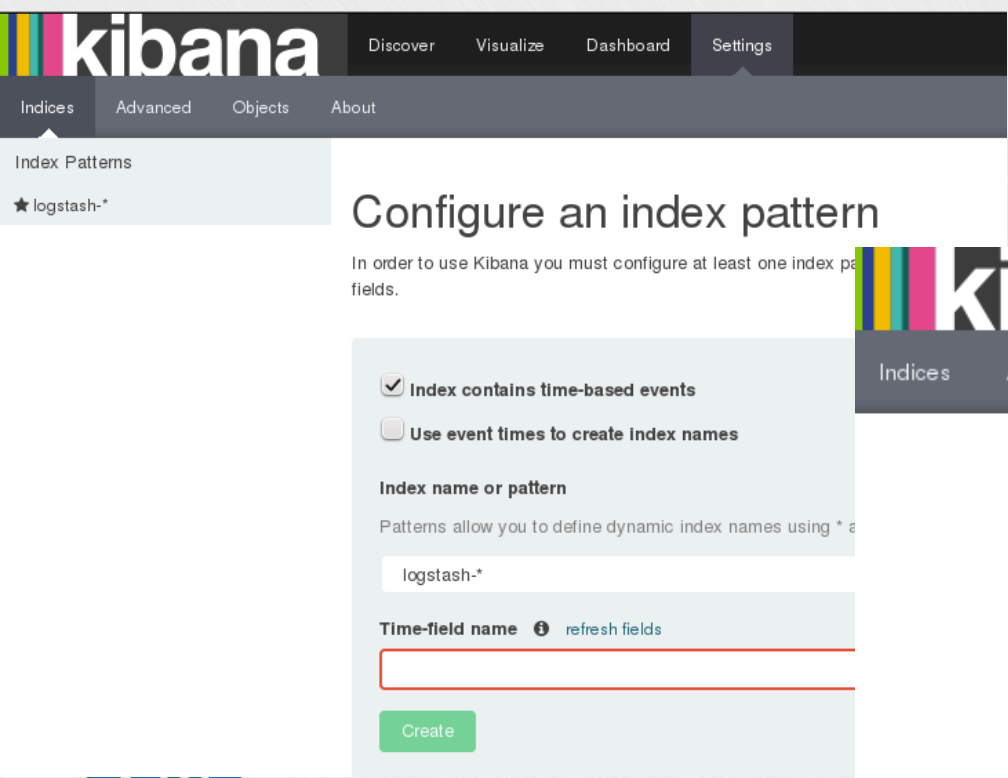
▶ Frontal



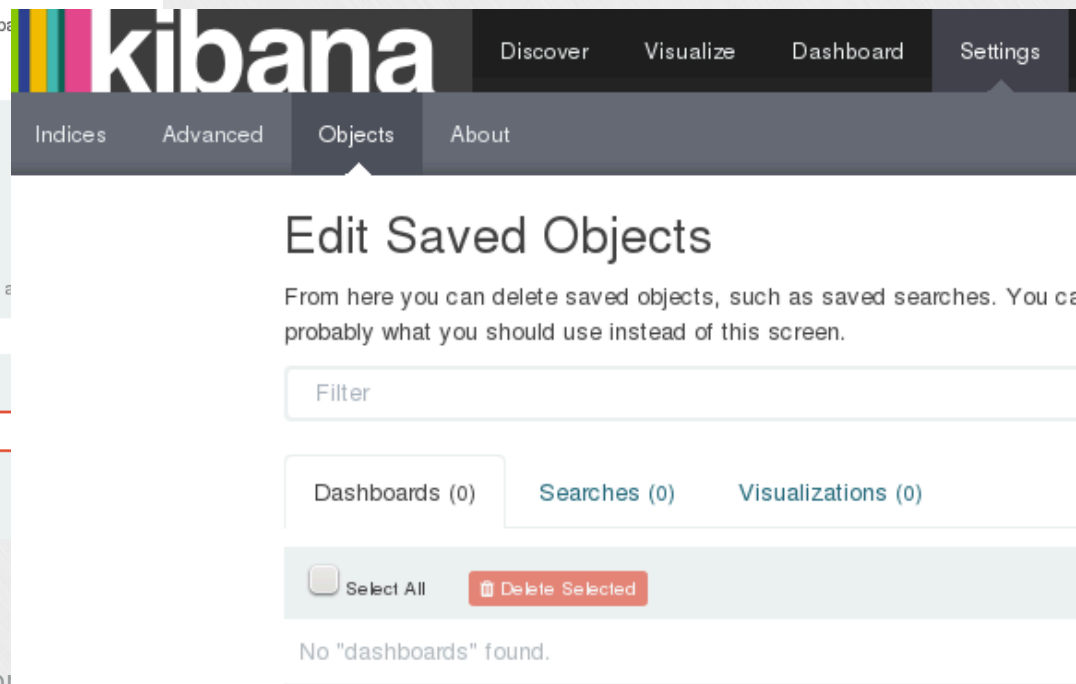
Création de graphiques et tableaux de bord

► Prise en main de kibana

► Configuration -> index



The screenshot shows the Kibana interface for configuring an index pattern. The top navigation bar includes 'Discover', 'Visualize', 'Dashboard', and 'Settings'. Below it, a sub-menu shows 'Indices', 'Advanced', 'Objects', and 'About'. The main heading is 'Configure an index pattern'. A sub-heading reads: 'In order to use Kibana you must configure at least one index pattern with at least one field.' The configuration options include: a checked checkbox for 'Index contains time-based events', an unchecked checkbox for 'Use event times to create index names', a text input field for 'Index name or pattern' containing 'logstash-*', and a 'Time-field name' field with a 'refresh fields' link. A green 'Create' button is at the bottom.



The screenshot shows the 'Edit Saved Objects' page in Kibana. The top navigation bar is the same as the previous screenshot. The main heading is 'Edit Saved Objects'. Below the heading, a message states: 'From here you can delete saved objects, such as saved searches. You can probably what you should use instead of this screen.' There is a search input field labeled 'Filter'. Below that, three categories are listed: 'Dashboards (0)', 'Searches (0)', and 'Visualizations (0)'. At the bottom, there are two buttons: 'Select All' and 'Delete Selected'. A message at the very bottom says 'No "dashboards" found.'

Création de graphiques et tableaux de bord

- ▶ **Prise en main de kibana**
 - ▶ Configuration -> visualisation

logstash-

metrics

▼ Slice Size

Aggregation

Unique count

Field

uid.raw

Advanced

buckets

▼ Split Slices

Aggregation

Terms

Field

eduPersonPrimaryAffiliation.raw

Order

Size

Top 5

Order By

metric: Unique count of uid.raw

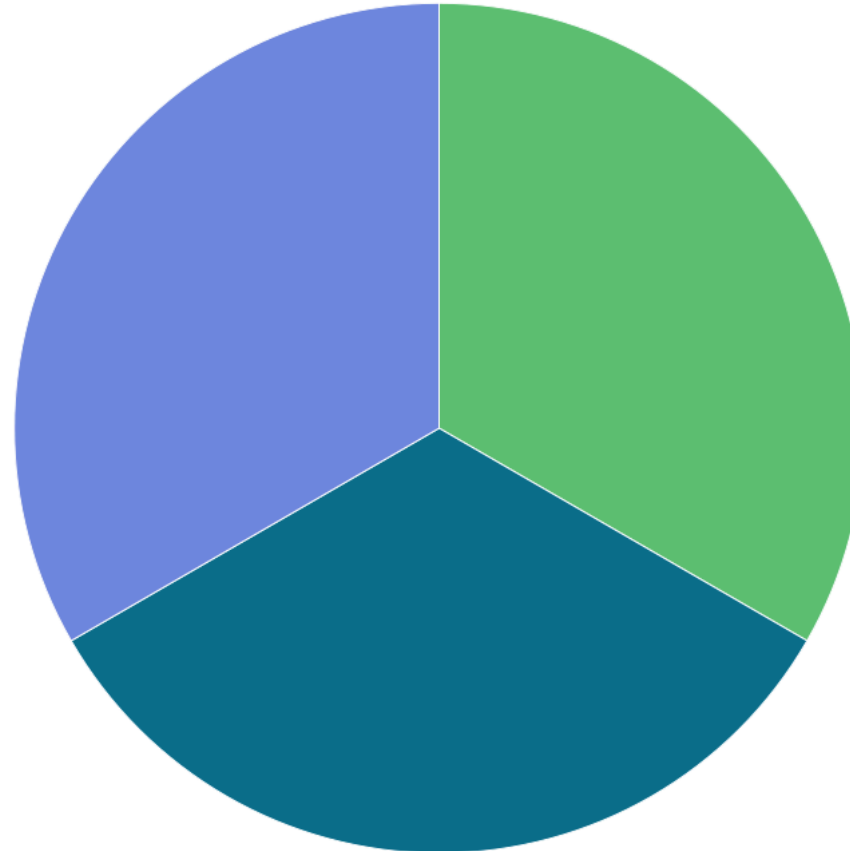
Advanced

Add Sub Aggregation

view options

Apply

Discard

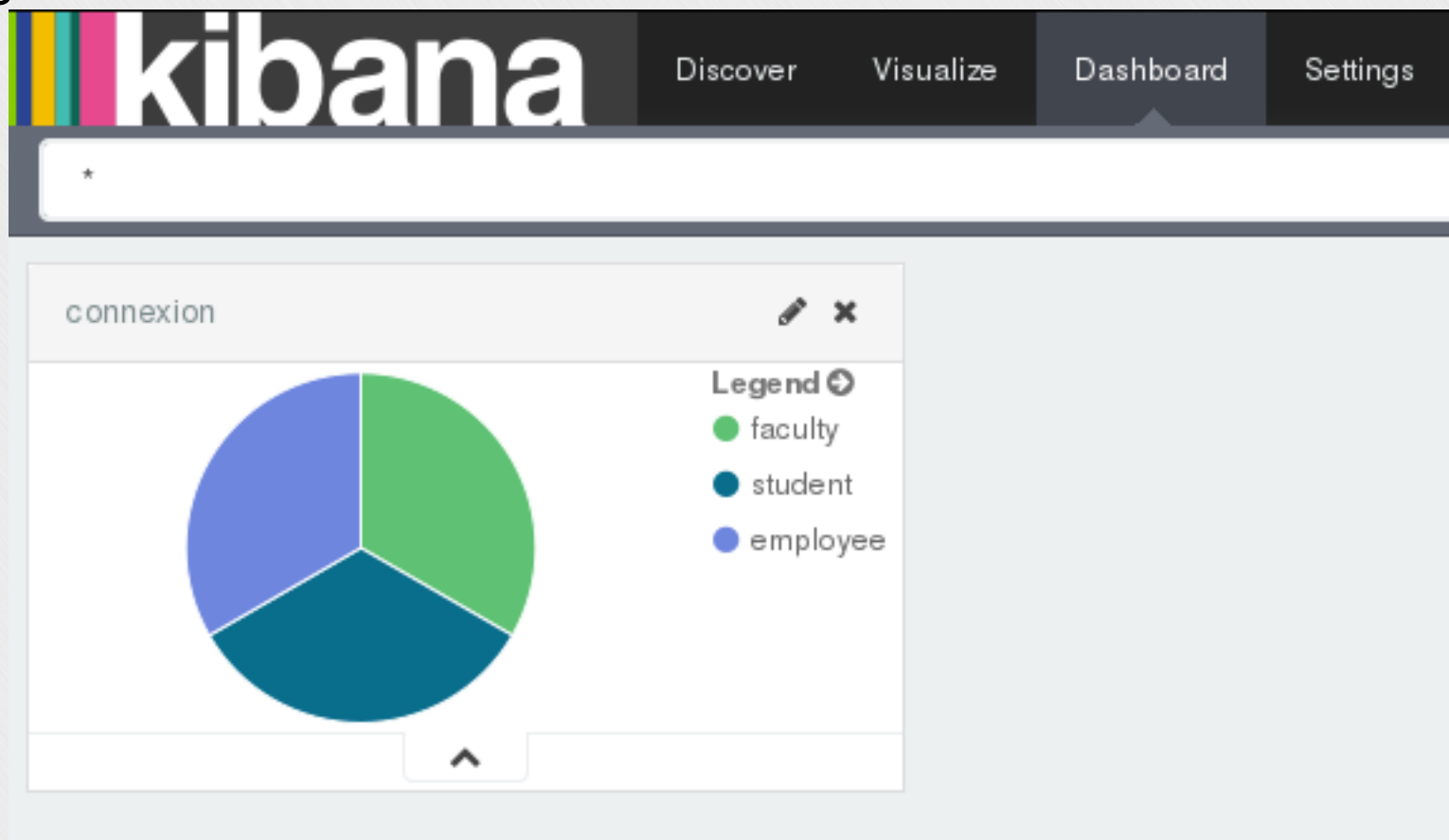


Legend

- faculty
- student
- employee

Création de graphiques et tableaux de bord

- ▶ Prise en main de kibana
 - ▶ Configuration -> dashboard



Création de graphiques et tableaux de bord

- ▶ Documentation
- ▶ Prise en main de kibana
- ▶ Import des graphiques existants

<https://github.com/EsupPortail/agimus-ng/tree/master/kibana#import-des-visualisations>

Les fichiers de configurations contenus dans le sous-dossier visualization doivent être importés dans elasticsearch grâce à la ligne de commande ci-dessous. Nous supposons ici que vous exécutez la commande sur le serveur elasticsearch et que vous utilisez le nom d'index par défaut de kibana4 (.kibana)

```
curl -XPUT "http://localhost:9200/.kibana/visualization/FICHER_A_IMPORTER" -d @visualization/FICHER_A_IMPORTER.json
```

- ▶ Frontal



Création de graphiques et tableaux de bord

- ▶ Documentation
- ▶ Prise en main de kibana
- ▶ Import des graphiques existants
- ▶ Frontal

<https://github.com/EsupPortail/agimus-ng/tree/master/experimentation/front-agimus-ng>

The screenshot displays the Agimus NG dashboard interface. On the left is a navigation sidebar with a 'Logo' button and menu items: 'Administration', 'Vos tableaux de bords:', 'Annuaire' (highlighted), 'Moodle', and 'Portail Esup'. The main content area is titled 'Agimus NG Tableau de bord "Annuaire"'. It features three data visualizations:

- ANNUAIRE : Nombre de personnes pour les 20 affectations principales à ce jour**: A bar chart showing the maximum count for the top 20 LDAP affiliations. The y-axis is 'Max count' (0 to 6,000) and the x-axis lists LDAP entries like 'n0000', 'h0000', etc. The highest count is for 'n0000' at approximately 6,000.
- ANNUAIRE : Répartition des affiliations dans le LDAP**: A pie chart showing the distribution of affiliations. The 'student' category (green) is the largest, followed by 'employee' (teal), 'faculty' (blue), 'affiliate' (purple), 'researcher' (pink), 'retired' (brown), 'registered_reader' (orange), and 'emeritus' (yellow).
- ANNUAIRE : Suivi par affiliation**: A line chart showing the average count per day for each affiliation from 2015-09-15 to 2015-09-29. The y-axis is 'Average count' (0 to 30,000). The 'student' line (green) shows significant fluctuations, peaking near 30,000, while other categories remain below 5,000.

At the top right of the dashboard, there is a date range selector set to '2015-09-09 - 2015-10-09' and a 'Déconnexion' button.

Discussion autour de la démarche d'indicateur



Discussion autour de la démarche d'indicateur

Création de graphiques et tableaux de bord

▶ Nos idées

- ▶ Utilisation des salles machines
- ▶ Corrélation usages des services – réussite
- ▶ A-B testing : choix du service le plus utilisé après mises en place de deux services
- ▶ Analyse plus fine du service Moodle envisagée
- ▶ D'autres services intéressants. Dans quelle optique ?



Création de graphiques et tableaux de bord

- ▶ Nos idées
- ▶ Vos suggestions

