Installations requises sur le serveur Agimus-NG

- Installations Logstash - Elasticsearch
  - Elasticsearch
  - Logstash
- Paramétrage Elasticsearch important
- Ajouts intéressants
- Python

Installations Logstash - Elasticsearch

Suivez les instructions correspondant à votre distribution :

Elasticsearch

https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html

/etc/elasticsearch/jvm.options

```
# Les deux valeurs doivent être identiques et correspondrent au maximum à la moitié de la RAM de la machine
-Xms8g
-Xmx8g
```

Pour éviter que les nœuds elasticsearch ne swappent, il faut les paramétrer pour leur indiquer de ne pas utiliser le swap :

/etc/sysctl.d/99-swappiness.conf

```
vm.swappiness = 1
```

POUR TESTER

Lancez la commande suivante sur votre serveur. Elle doit vous retourner une ligne d'information (nom, @IP, ...) concernant votre serveur elasticsearch.

```
[agimus@agimus logstash]$ curl -XGET http://localhost:9200/_cat/nodes
```

Logstash

https://www.elastic.co/guide/en/logstash/current/installing-logstash.html

Nous utilisons des plugins spécifiques dans les fichiers de configurations par défaut qu'il vous faudra installer grâce aux commandes suivantes (chemin à adapter)

```
/opt/logstash/bin/logstash-plugin install logstash-input-LDAPSearch
/opt/logstash/bin/logstash-plugin install logstash-filter-translate
/opt/logstash/bin/logstash-plugin install logstash-filter-cidr
/opt/logstash/bin/logstash-plugin install logstash-filter-elasticsearch
```

POUR TESTER

Les appels à logstash se feront alors **/opt/logstash/bin/logstash**.

Pour tester la bonne installation de logstash et LDAPSearch, téléchargez le fichier test-logstash.conf, paramétrez la partie LDAP en début de fichier et lancez la commande suivante dans le répertoire contenant le fichier modifié :

```
[agimus@agimus logstash]$ /opt/logstash/bin/logstash -f test-logstash.conf
```

Vous devez voir apparaître la liste des personnes dont l'uid commence par "dupon". Si ce n'est pas le cas, vérifiez les ouvertures réseau entre votre serveur Agimus-NG et votre LDAP et analyser les erreurs retournées par logstash.

Paramétrage Elasticsearch important

Avant de démarrer et commencer à utiliser votre serveur elasticsearch, il est important de vérifier le paramétrage suivant dans le fichier de configuration d'elasticsearch.

Le fichier de configuration elasticsearch s'appelle **elasticsearch.yml** et se trouve soit dans ./config/elasticsearch.yml du répertoire des sources soit dans /etc/elasticsearch/elasticsearch.yml pour une installation par paquet.

- Modifier le paramètre **cluster.name** : par défaut il utilise elasticsearch. Si vous lancez un autre serveur elasticsearch non paramétré sur le même réseau, il va commencer à recopier toutes les données car ils considéreront qu'ils font partie du même cluster.

```
# Nom du cluster utilisé pour Agimus. Toutes les machines utilisées (si vous utilisez le mécanisme de distribution) doivent avoir le même.
cluster.name: Agimus
```

- Modifier le paramètre **node.name** : permet de savoir plus précisément quelle machine pose problème le cas échéant. Le nœud est un serveur elasticsearch. Vous pouvez lui donner le nom réel du serveur pour plus de clarté.

```
# Nom du noeud (une des machines du cluster). Permet de différencier chaque machine du cluster.
node.name: "Agimus1"
```

- Modifier **network.host** pour écouter en local et sur l'IP externe

```
# Pour écouter sur 127.0.0.1 et sur l'IP externe
network.host: [_global_, _local_]
```

- Prévoir beaucoup de RAM sur la ou les machines du cluster. Le heap space (variable d'environnement ES_HEAP_SIZE) du processus ne devrait pas dépasser 50% de la RAM.
- Ajouter le paramètre **indices.fielddata.cache.size** : 40% .
  Ceci permet de limiter l'espace de heap alloué à fielddata et d'éviter que les requêtes ne soient bloquées par un circuit breaker (cf http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/_limiting_memory_usage.html)

```
indices.fielddata.cache.size:  40%
```

- Avant de commencer l'indexation, ajoutez ces templates qui permettent de paramétrer les champs par défaut et un meilleur fonctionnement pour l'usage qui est fait d'elasticsearch.
  - [Facultatif] Ingest pipeline qui va être exécutée par défaut pour toute insertion dans un index agimus.
    Permet de créer 3 nouveaux champs : Jour de la semaine, heure du jour, type de périphérique lisible. Ces champs seront utilisés dans les rendus kibana.

Ingest pipeline - création automatique de champ

```
$ curl -XPUT "http://localhost:9200/_ingest/pipeline/agimus" -d '
{
  "description": "ajout des champs heure et jour de la semaine pour l'événement et valeur lisible
de is_mobile",
  "processors": [
    {
      "set": {
        "field": "ts",
        "value": "{{@timestamp}}"
      }
    },
    {
      "script": {
        "lang": "painless",
        "source": """
          ZonedDateTime dateEvt = ZonedDateTime.parse(ctx.ts);
          ZonedDateTime dateEvtChezNous = dateEvt.withZoneSameInstant(ZoneId.of('Europe/Paris'));
          ctx.heure = dateEvtChezNous.getHour();
          ctx.jour_semaine = dateEvtChezNous.getDayOfWeek().getValue() +"-"+dateEvtChezNous.
getDayOfWeek().getDisplayName(TextStyle.SHORT, Locale.FRANCE);
        """
      }
    },
    {
      "remove": {
        "field": "ts"
      }
    },
    {
      "script": {
        "lang": "painless",
        "source": """
          if (ctx?.is_mobile =="0") {
          ctx.is_mobile_hr = "Ordinateur";
        } else if (ctx?.is_mobile =="1") {
          ctx.is_mobile_hr = "Smartphone/Tablette";
        } else {
          ctx.is_mobile_hr = "Non détectable";
        }
        """
      }
    }
  ]
}
```

- Template principal. Si vous n'utilisez pas la pipeline ci-dessus, retirez la ligne "default_pipeline" : "agimus",
  Les champs texte sont par défaut de type keyword car nous n'utiliserons généralement pas de recherche approximative mais chaque valeur aura un sens uniquement si elle est prise en compte dans sa totalité
  Les types des autres champs sont prédéfinis pour éviter des erreurs à l'ingestion des données et pour permettre une bonne utilisation dans kibana

template "agimus"

```
$ curl -XPUT "http://localhost:9200/_template/agimus" -d '
{
    "order" : 0,
    "index_patterns" : [
      "ag-*"
    ],
    "settings" : {
      "index" : {
        "default_pipeline" : "agimus",
        "refresh_interval" : "1s",
        "number_of_shards" : "1",
        "number_of_replicas" : "0"
      }
    },
    "mappings" : {
      "dynamic_templates" : [
        {
          "string_fields" : {
            "mapping" : {
              "type" : "keyword"
            },
            "match_mapping_type" : "string",
            "match" : "*"
          }
        }
      ],
      "properties" : {
        "@timestamp" : {
          "type" : "date"
        },
        "estinscrit" : {
          "type" : "boolean"
        },
        "@version" : {
          "type" : "keyword"
        },
        "insc-annee" : {
          "type" : integer"
        }
      }
    },
    "aliases" : { }
  }'
```

- Template de l'index contenant le dump ldap et de ldap-stat permettant le suivi du ldap. Il vous faudra peut-être le modifier si vous y intégrer des valeurs spécifiques

template "ldap"

```
$ curl -XPUT "http://localhost:9200/_template/ldap" -d '
{
    "order" : 0,
    "index_patterns" : [
      "ldap*"
    ],
    "settings" : {
      "index" : {
        "number_of_shards" : "3",
        "number_of_replicas" : "0",
        "refresh_interval" : "60s"
      }
    },
    "mappings" : {
      "dynamic_templates" : [
        {
          "string_fields" : {
            "mapping" : {
              "type" : "keyword"
            },
            "match_mapping_type" : "string",
            "match" : "*"
          }
        }
      ],
      "properties" : {
        "@timestamp" : {
          "type" : "date"
        },
        "estinscrit" : {
          "type" : "boolean"
        },
        "@version" : {
          "type" : "keyword"
        },
        "insc-annee" : {
          "type" : "integer"
        }
      }
    },
    "aliases" : { }
  }'
```

- Exemples de templates spécifiques s'appliquant à un type de log en particulier

Template s'appliquant aux cours moodle

```
$ curl -XPUT "http://localhost:9200/_template/moodlecours" -d '
{
    "order" : 2,
    "index_patterns" : [
      "ag-moodlecours-*"
    ],
    "settings" : { },
    "mappings" : {
      "dynamic_templates" : [
        {
          "type_activites_as_int" : {
            "path_match" : "mdl_type_activites.*",
            "mapping" : {
              "type" : "integer"
            }
          }
        }
      ],
      "properties" : {
        "mdl_id_comp" : {
          "type" : "integer"
        },
        "mdl_activites" : {
          "type" : "nested",
          "properties" : {
            "id_activite" : {
              "type" : "integer"
            }
          }
        },
        "mdl_courseid" : {
          "type" : "integer"
        },
        "mdl_id_cat" : {
          "type" : "integer"
        },
        "mdl_id_coll" : {
          "type" : "integer"
        },
        "mdl_actif" : {
          "type" : "boolean"
        }
      }
    },
    "aliases" : { }
  }'
```

Template s'appliquant aux logs moodle

```
$ curl -XPUT "http://localhost:9200/_template/moodledb" -d '
{
    "order" : 2,
    "index_patterns" : [
      "ag-moodledb-*"
    ],
    "settings" : { },
    "mappings" : {
      "properties" : {
        "mdl_courseid" : {
          "type" : "integer"
        },
        "mdl_id" : {
          "type" : "integer"
        },
        "mdl_contextinstanceid" : {
          "type" : "integer"
        },
        "mdl_objectid" : {
          "type" : "integer"
        },
        "mdl_contextid" : {
          "type" : "integer"
        },
        "mdl_actif" : {
          "type" : "boolean"
        }
      }
    },
    "aliases" : { }
  }'
```

Template s'appliquant aux logs ezpaarse

```
$ curl -XPUT "http://localhost:9200/_template/ezagimus" -d '
{
    "order" : 2,
    "index_patterns" : [
      "ag-ezagimus-*"
    ],
    "settings" : { },
    "mappings" : {
      "properties" : {
        "size" : {
          "type" : "integer"
        },
        "on_campus" : {
          "type" : "boolean"
        },
        "status" : {
          "type" : "integer"
        }
      }
    },
    "aliases" : { }
  }'
```

Template s'appliquant aux logs trace

```
$ curl -XPUT "http://localhost:9200/_template/trace" -d '
{
    "order" : 0,
    "index_patterns" : [
      "trace*"
    ],
    "settings" : {
      "index" : {
        "number_of_shards" : "3",
        "number_of_replicas" : "0",
        "refresh_interval" : "60s"
      }
    },
    "mappings" : {
      "dynamic_templates" : [
        {
          "string_fields" : {
            "mapping" : {
              "type" : "keyword"
            },
            "match_mapping_type" : "string",
            "match" : "*"
          }
        }
      ],
      "properties" : {
        "@timestamp" : {
          "type" : "date"
        },
        "@version" : {
          "type" : "keyword"
        }
      }
    },
    "aliases" : { }
  }'
```

Template s'appliquant aux logs rocketchat

```
$ curl -XPUT "http://localhost:9200/_template/rocketchat" -d '
{
    "order" : 2,
    "index_patterns" : [
      "ag-rocketchat-*"
    ],
    "settings" : { },
    "mappings" : {
      "properties" : {
        "rc_totalChannels" : {
          "type" : "long"
        },
        "rc_totalUsers" : {
          "type" : "long"
        },
        "rc_totalRooms" : {
          "type" : "long"
        },
        "rc_totalMessages" : {
          "type" : "long"
        },
        "rc_totalConnectedUsers" : {
          "type" : "long"
        },
        "rc_totalDirectMessages" : {
          "type" : "long"
        },
        "rc_totalPrivateGroupMessages" : {
          "type" : "long"
        },
        "rc_totalChannelMessages" : {
          "type" : "long"
        },
        "rc_totalLivechatMessages" : {
          "type" : "long"
        },
        "rc_totalLivechat" : {
          "type" : "long"
        },
        "rc_totalPrivateGroups" : {
          "type" : "long"
        },
        "rc_totalDirect" : {
          "type" : "long"
        }
      }
    },
    "aliases" : { }
  }'
```

POUR TESTER

Pour vous assurer que les commandes ont été prises en compte, vérifier que vous avez les entrées "agimus", "ldap", "trace" et templates spécifiques ajoutés en lançant la commande suivante :

```
curl -XGET "http://localhost:9200/_template/?pretty"
```

Ajouts intéressants

- Pour en savoir plus sur elasticsearch : http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/

- Vous pouvez installer l'application Cerebro (https://github.com/lmenezes/cerebro) qui est le remplaçant du plugin kopf utilisé sur la version 2.
  Elle vous permettra de suivre l'état de votre cluster d'avoir des informations sur les index, alias et autres composants du cluster.
  Une fois installée, l'application est disponible sur le port 9000
- Il existe deux outils maintenant disponibles par défaut dans l'onglet "Dev Tools" de kibana. Prenez le temps de les tester ils pourront vous aider :
  - Console : pour tester vos requêtes ES ou vérifier le contenu de vos index
  - Grok debugger : pour vous aider à créer vos découpages grok dans logstash

> Si vous avez paramétré la variable d'environnement http_proxy et que votre serveur elasticsearch se trouve sur la même machine que logstash, il faut utiliser le script suivant pour appeler logstash.
>
> En effet, la variable no_proxy, suivant son contenu, n'est pas toujours correctement interprétée par ruby. Le script désactive donc temporairement http_proxy, le temps de l'appel à logstash.

Python

Python 3 est utilisé pour faire une synthèse quotidienne de la répartition dans le LDAP par type de population.

Pour cela le script (donné ci-dessous), nécessite un plugin elasticsearch afin d'interroger le LDAP. Pour installer ce plugin lancer la commande suivante :

```
pip install elasticsearch
```

Si vous rencontrez des problèmes avec pip, vous pouvez télécharger la version que vous souhaitez et installer directement :

```
#Récupération du paquet du module
wget https://pypi.python.org/packages/source/e/elasticsearch/elasticsearch-7.8.1.tar.gz
#Récupération de sa dépendance
wget https://pypi.python.org/packages/source/u/urllib3/urllib3-1.22.tar.gz

# On décompresse les fichiers
tar -zxf urllib3-1.22.tar.gz
tar -zxf elasticsearch-7.8.1.tar.gz

#On installe d'abord la dépendance
cd urllib3-1.22
python setup.py install
#Puis le module elasticsearch
cd ../elasticsearch-7.8.1
python setup.py install
```

> **POUR TESTER**
>
> Pour tester la bonne installation du module elasticsearch pour python, télécharger le script de test test-elasticsearch.py et exécutez le sur votre serveur. Vérifiez qu'il n'y a pas d'erreur en sortie.

```
[agimus@agimus scripts]$ cp config-sample.py config.py
# Paramétrer les informations spécifiques à votre installation
[agimus@agimus scripts]$ vim config.py
[agimus@agimus scripts]$ python test-elasticsearch.py
L'index test-index est cree
Il y a 1 document(s) dans l'index test-index :
Créé le 2020-08-03T12:03:55.976158 par testeur : Elasticsearch fonctionne dans python
L'index de test "test-index" est supprimé.

Le test s'est déroulé correctement. Le plugin elasticsearch pour python est installé correctement

[agimus@agimus scripts]$
```

approve ÉTAPE SUIVANTE : Paramétrer Agimus-NG