2 - Visualisation des indicateurs avec Kibana

Afin de visualiser le contenu de votre entrepôt elasticsearch, vous pouvez installer Kibana.

> Kibana ne prévoit pas d'authentification interne à l'application (à moins d'utiliser X-Pack, payant). Vous devez assurer par ailleurs la vérification de l'accès à l'outil. Nous vous proposons une architecture à la page Sécuriser l'accès à kibana

Installation

Installation générique

```
cd /opt/
wget https://download.elasticsearch.org/kibana/kibana/kibana-4.6.3-linux-x86_64.tar.gz
tar -zxvf kibana-4.6.3-linux-x86_64.tar.gz
ln -s kibana-4.6.3-linux-x86_64 kibana
rm kibana-4.6.3-linux-x86_64.tar.gz
```

Activation du service

sur Debian

Télécharger le fichier de démarrage de kibana4 kibana4_init et l'enregistrer sous /etc/init.d/kibana

Centos7

Télécharger le fichier de démarrage de kibana4 kibana4.service et l'enregistrer sous /usr/lib/systemd/system/kibana4.service

Pour que kibana soit lancé au démarrage :

systemctl

```
systemctl enable kibana4.service
```

ACL

Kibana a besoin d'effectuer une requête vers le port 9200 du serveur lorsqu'on veut visualiser les données. Il faut donc penser à ouvrir l'accès au port 9200 dans les ACL pour les personnes autorisées à voir le tableau de bord de Kibana.

La version de Kibana 4 est standalone et tourne sur le port 5601.

Autoriser les requêtes depuis les navigateurs

Depuis Elasticsearch 1.4, il faut ajouter dans la configuration un paramètre autorisant les requêtes depuis un navigateur se trouvant sur une autre machine. Pour cela, il faut modifier le fichier /etc/elasticsearch/elasticsearch.yml et ajouter :

```
#Autorise les requêtes depuis un navigateur situé sur une autre machine
#L'expression régulière ci-dessous indique les URL qui peuvent être requêtées
http.cors.allow-origin: /http://agimus.univ.fr(:9200)?/
http.cors.enabled: true
```

La valeur du paramètre http.cors.allow-origin est traitée comme une expression régulière. Elle indique l'url de base qui peut être requêtée depuis un navigateur (ici c'est http://agimus.univ.fr avec éventuellement le port 9200 spécifié)

Dashboard d'exemple

Vous trouverez des dashboards et des visualisations d'exemple sur l'espace github du projet

Suivant les attributs que vous avez utilisés pour enrichir vos logs, il se peut que certaines visualisations n'affichent pas de données. N'hésitez pas à les modifier via l'interface graphique après les avoir importées.

A titre d'exemple, le tableau de bord d'authentification CAS contient une visualisation qui utilise l'attribut [network][type] qui est facultatif dans la configuration logstash correspondante logstash-casrequest.conf