« Une autre vision de la messagerie »

Auteur : Pascal SALAUN

En date du 13/08/2017

Table des matières

Préambule....3

1. Définition des objectifs....4

1.1 L'architecture cible....4
1.2 bmSearch....5

2. Installation de bmSearch....6

2.1 Les dépendances....6
2.2 Installation du paquet....6
2.3 La configuration de bmSearch....6
2.4 Injection du template....7
2.5 Démarrage de bmSearch....7

3. KIBANA....9

3.1 Ajouter l'index « bmsearch »....9
3.2 Ajouter les « objets » propres à bmSearch....10
3.3 Dernière petite configuration....12

4. Le dashboard bmSearch....13

4.1 Afficher le dashboard principal....13
4.2 Le dashboard des messages....15
4.3 Le dashboard des types de pièces jointes....16

5. Quelques bricoles concernant KIBANA....17

5.1 Le type des champs (fields) n'est pas reconnu....17

Préambule

Je ne suis pas un expert ELK, que ce soit (re)dit.

Certains connaissent « bm-stats » un outil/portail de stats messagerie adossé à la solution Bluemind (https://www.bluemind.net)

J’ai conçu bmSearch pour limiter l’adhérence au serveur Bluemind. Il a juste besoin d’accéder au fichier « mail.log » de postfix, et d’en gérer la rotation si nécessaire.

L’autre point à l’origine de ce développement est l ‘absence de temps réel de « bm-stats ». En effet, ce dernier traite les données seulement après rotation du journal, après 0:00.

bmSearch, quant à lui, se connecte sur le journal et traite les datas au fil de l’eau. Seule la mise à jour des infos liées au dépôt des messages par Cyrus est programmée toutes les 5 minutes.

Enfin, je suis désolé pour les heureux sysadmin RHEL/CentOS, mais les commandes d’installation sont celles de DEBIAN (guéguerre oblige ;-)). Une version « install from source » sera bientôt disponible, promis.

Et bien je crois qu’on est parti pour une installation.

1. Définition des objectifs

Avant d'attaquer le vif du sujet, on déjà définir :

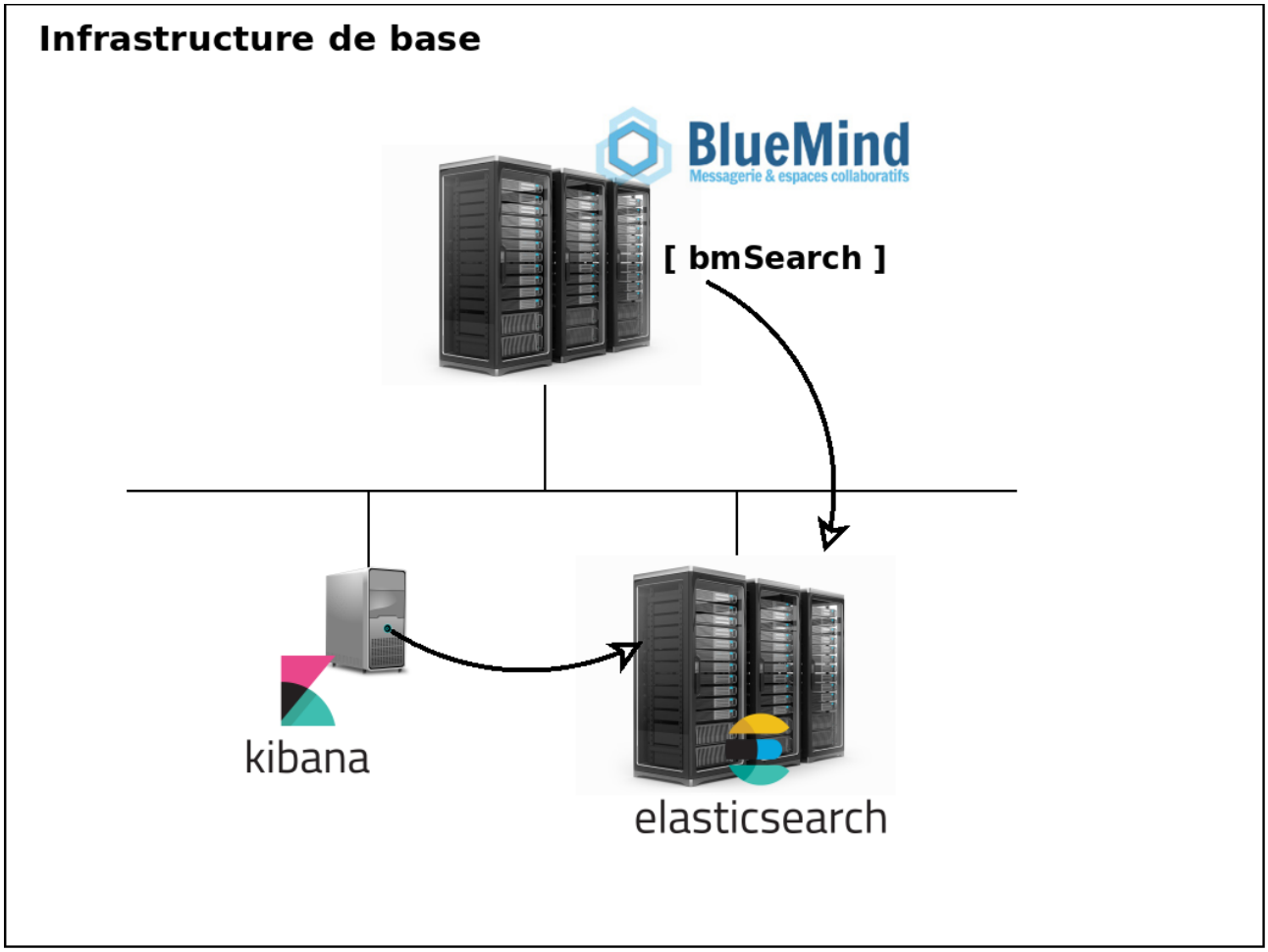
- ce que l'on veut (installer bmSearch)
- ce dont on a besoin (l'architecture cible)

1.1 L'architecture cible

Dans ce document, on va traiter le cas le plus simple , et le seul possible à cette heure (**le passage par logstash n'est pas en pris en compte**)

Pour cela, nous avons besoin :

- d'un serveur de messagerie (Bluemind)
- d'un serveur Elasticsearch
- d'un serveur Kibana



Et je vais considérer que vous avez déjà tout cela sous la main (sinon ça risque de prendre un peu de temps).

Je ne reviendrai pas non plus sur la configuration de chaque composant. J'ai pondu une doc sur la stack ELK. Faut bien qu'elle serve à quelque chose ! ;-)

1.2 bmSearch

La solution bmSearch est composé de 2 éléments :

- un paquet que l'on installera sur le serveur de messagerie
- les définitions des objects à injecter dans Kibana

Ces 2 éléments sont téléchargeables :

- soit depuis le site « http://bm-stats.org/ », item « bmSearch »
- soit depuis le market place de Bluemind (https://marketplace.bluemind.net/)

Je vous laisse le choix du site de téléchargement.

2. Installation de bmSearch

Les actions listées ci-après sont à mener sur le serveur de messagerie

2.1 Les dépendances

BmSearch est écrit en Python 2.7, et a besoin pour fonctionner de 2 « addons » :

- python-magic
- python-requests

Sous Debian & Co, la commande est :

apt-get install python-magic python-requests

2.2 Installation du paquet

Pour l'instant, il n'y a rien de compliqué. Il suffit de passer la commande :

dpkg -i bmSearch-z.y.z_all.deb

Pour résumer, le packager va :

- installer le contenu dans les dossiers de base (/etc /usr /var)
- configurer la gestion de la rotation du journal mail.log (cf /etc/logrotate.d/rsyslog)
- configurer l'activation des traces par Postfix (cf /etc/postfix/main.cf)
- préparer un fichier de configuration (cf /etc/bmSearch/config.py)

2.3 La configuration de bmSearch

Il s'agit du fichier « /etc/bmSearch/config.py ».

Vous ne devriez normalement n'avoir besoin de modifier que :

- **HOSTNAME** : le nom de la machine tel que vous voulez qu'il apparaisse dans Elasticsearch

- **APIURL** : l'url complète vers le serveur Elasticsearch

Faites attention, le fichier « config.py » est en Python. Il est donc très sensible à l'indentation.

2.4 Injection du template

Elasticsearch est une base de données, et à ce titre, s'appuie sur des schémas (template) de données.

Nous allons donc injecter celui de bmSearch, au moyen de la commande « curl ». Si elle n'est pas présente, alors soit vous l'installer sur le serveur de messagerie soit sur une autre machine.

On va considérer que l'on est bien dans le dossier où se trouve le fichier « bmSearch.template.json », dans « /etc/bmSearch », la commande est alors :

curl -XPUT 'http://<votreServeurElasticsearch>:9200/_template/bmsearch-*?pretty' -d@ bmSearch.template.json

Comme par exemple :

curl -XPUT 'http://192.168.1.100:9200/_template/bmsearch-*?pretty' -d@bmSearch.template.json

Si tout s'est bien passé, alors le serveur Elasticsearch vous répondra :

```
{
  "acknowledged" : true
}
```

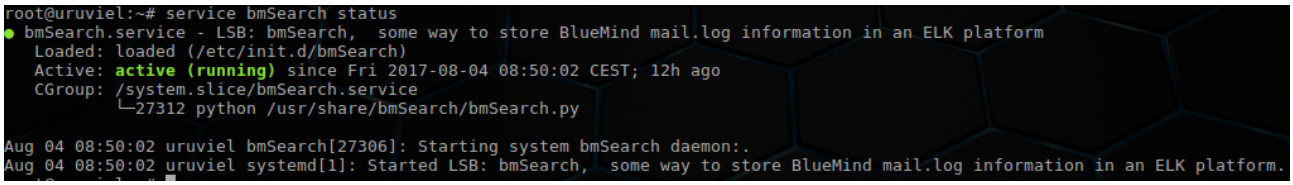
Sinon, il faudra chercher qui s'est encore emmêlé les pinceaux, vous ? Moi ?

2.5 Démarrage de bmSearch

bmSearch est démarrable comme n'importe quel autre soft, via la commande « service » :

- service bmSearch start
- service bmSearch stop
- service bmSearch restart
- service bmSearch status

Si le démarrage s'est bien passé, « **service bmSearch status** » doit vous retourner quelque chose comme :



Si ce n’est pas le cas, alors lancez bmSearch en mode manuel :

/usr/share/bmSearch/bmSearch.py

et tenter de corriger l’erreur qui est affichée (la dernière ligne de la stack trace)
sinon appelez à l’aide. Je squatte le forum de Bluemind (https://forum.bluemind.net/)

Si vous voulez lancer bmSearch dès le démarrage, la commande est :

update-rc.d elasticsearch defaults

Si vous voulez le supprimer du démarrage, alors la commande est :

update-rc.d elasticsearch remove

3. KIBANA

Voilà, a priori, l'installation sur le serveur de messagerie s'est bien passé. Il nous reste maintenant qu'à intervenir sur KIBANA.

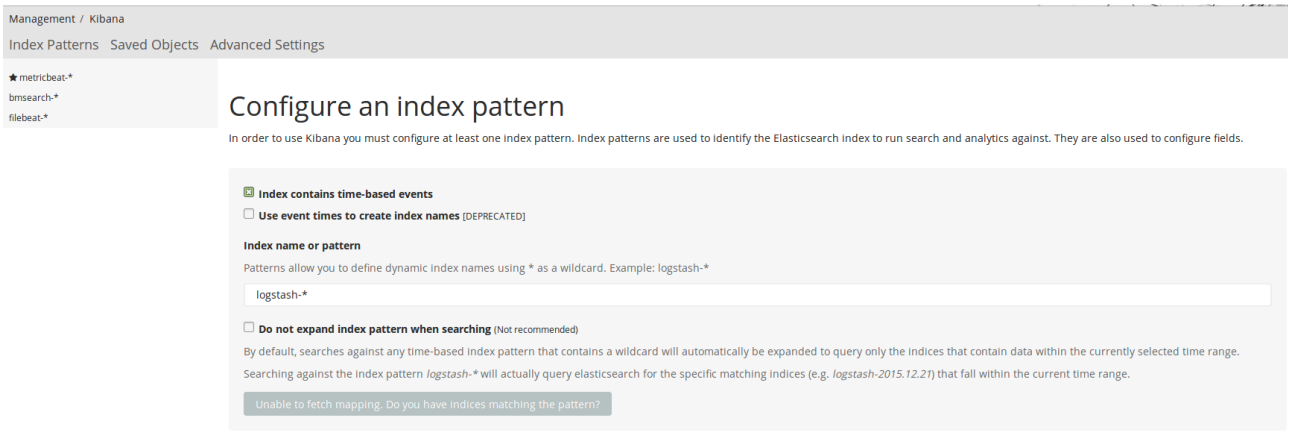
En fait, c'est simple, le boulot consiste à :

- ajouter l'index « bmsearch » à ceux déjà présents (metricbeat ? filebeat?)
- injecter les objets (search, dashboard, view)
- configurer le format du champ (field) « size »

3.1 Ajouter l'index « bmsearch »

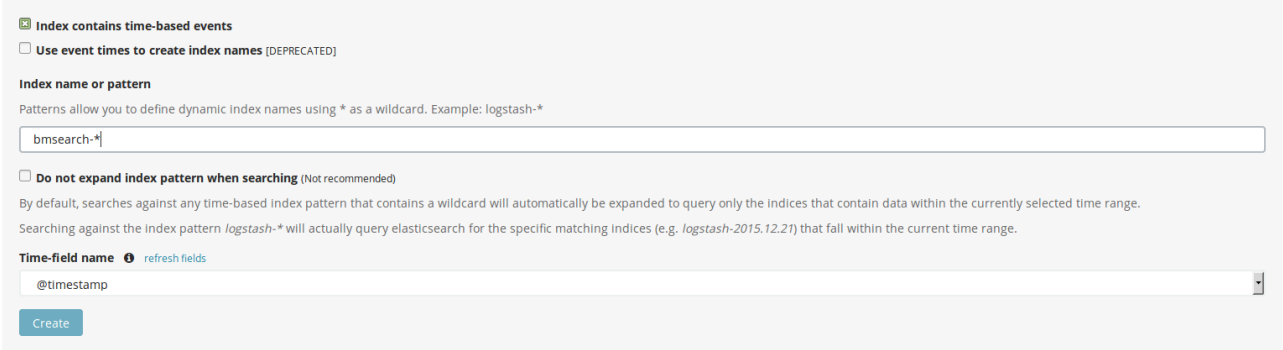
Il faut attendre un peu avant de pouvoir le faire. Hé oui, il faut que quelques datas soient stockées dans Elasticsearch.

Donc, on va dans « Management », puis dans « Index Patterns » , puis « + Add new », pour afficher :



Remplacez ensuite « logstash-* » par « bmsearch-* »

Kibana va tenter de récupérer le schéma et vous présenter un champ 'Time-field'



Vous acceptez celui qui est proposé et cliquez sur « create »

3.2 Ajouter les « objets » propres à bmSearch

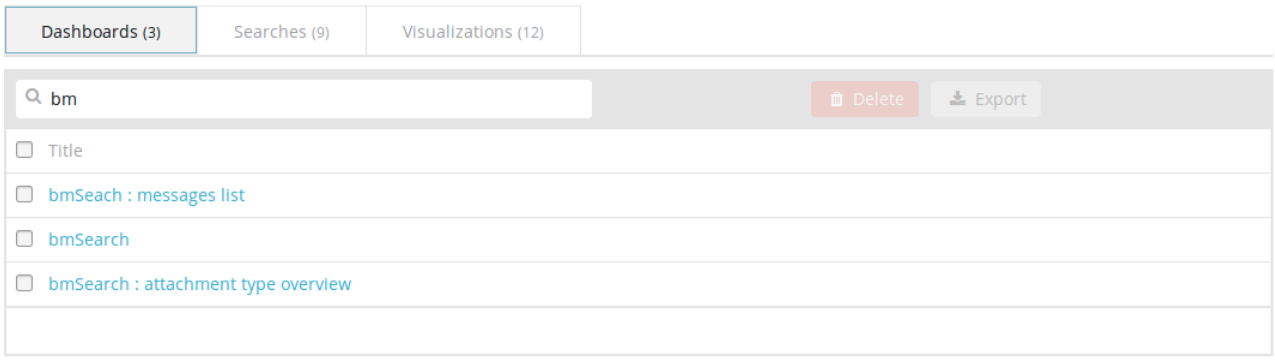
Ces objets sont en fait les configurations :

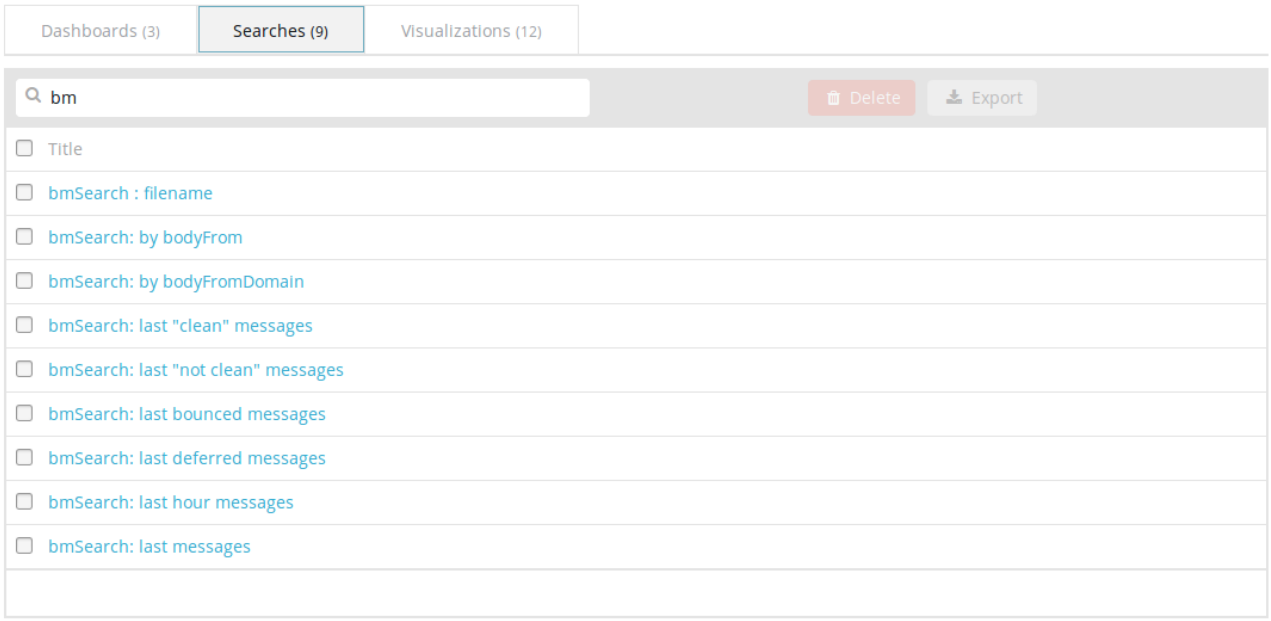
- du dashboard
- des « view » (mise en forme des requêtes)
- des « search » (requêtes de base)

Le plus simple est d'aller, toujours dans « Management », dans « Saved objects», en haut à droite, il y a un bouton « import » que l'on va cliquer.

Un formulaire nous demande d'uploader un fichier, le fichier « kibana_bmSearchAllObjects.json » présent dans l'archive « bmSearch_Stuff4Kibana-x.y.z.tar.gz »

En renseignant le filtre avec « bm », vous devriez avoir quelque chose comme :





Dashboards (3) | Searches (9) | Visualizations (12)

bm

Delete | Export

Title
bmSearch : clean messages
bmSearch : not clean messages
bmSearch : Servers List Overview
bmSearch : Top 20 Sender Domain
bmSearch : Top 20 Senders
bmSearch : view by archive type
bmSearch : view by Deferred and Bounced messages
bmSearch : view by image type
bmSearch : view by multimedia type
bmSearch : view by Nb of deferred messages
bmSearch : view by nb of recip
bmSearch : view by office applications type

3.3 Dernière petite configuration

Il s'agit d'afficher correctement la taille d'un message (champ size).

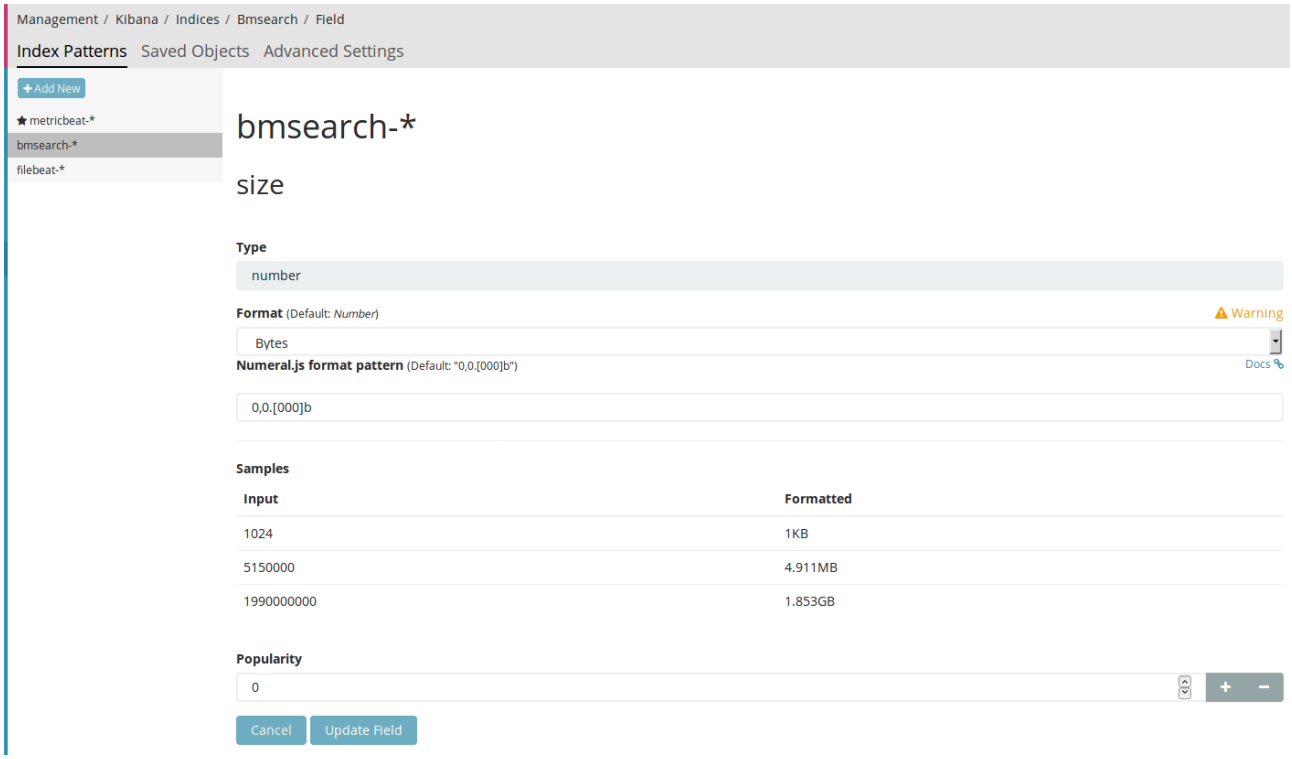
Toujours dans « Management », on retourne dans « Index patterns » .

Puis on sélectionne « bmsearch-* ».

A ce moment, nous avons la totalité des champs (field) du « schéma » de bmSearch.

On va indiquer que le field « size » s'exprime en byte.

On clique sur l'icône à droite pour éditer le champ « size » , pour obtenir ceci :



On sélectionne le bon format, et on valide (update).

Et voilà, c'est fini !

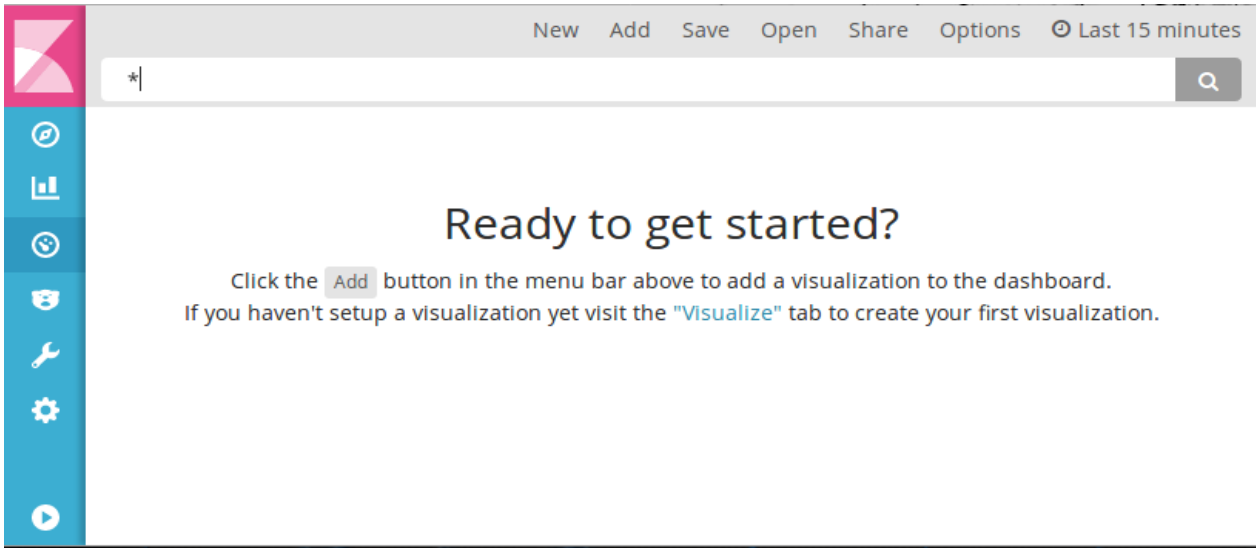
Une p'tite mousse ?

On a plus qu'à afficher le magnifique dashboard « bmSearch »

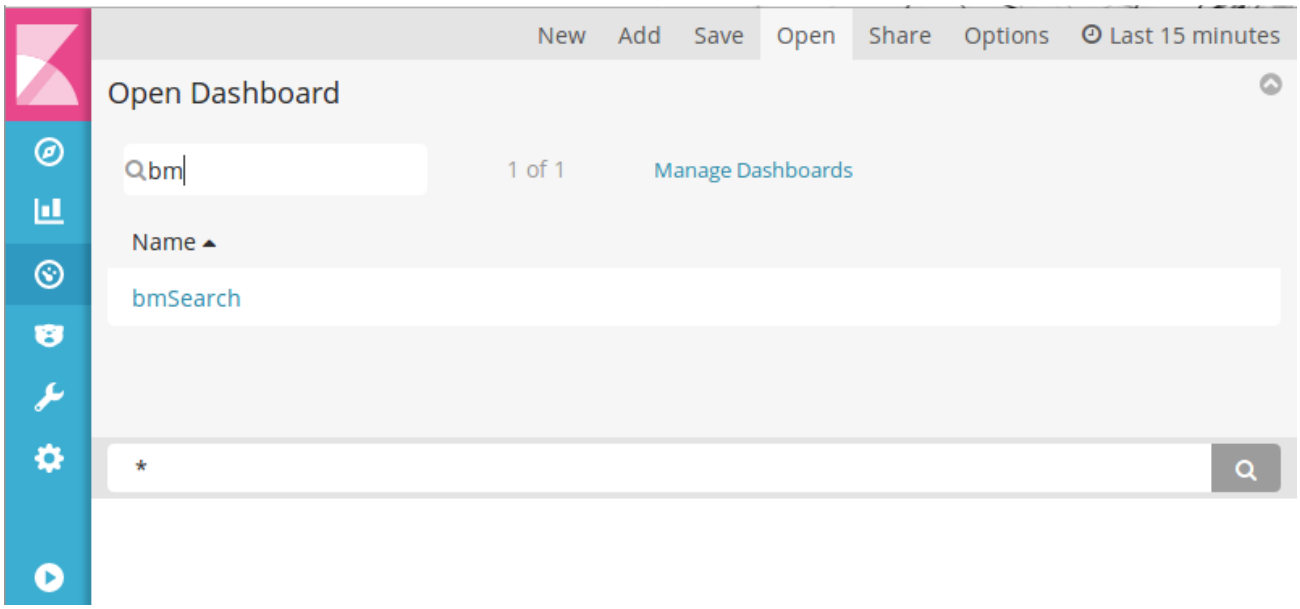
4. Le dashboard bmSearch

4.1 Afficher le dashboard principal

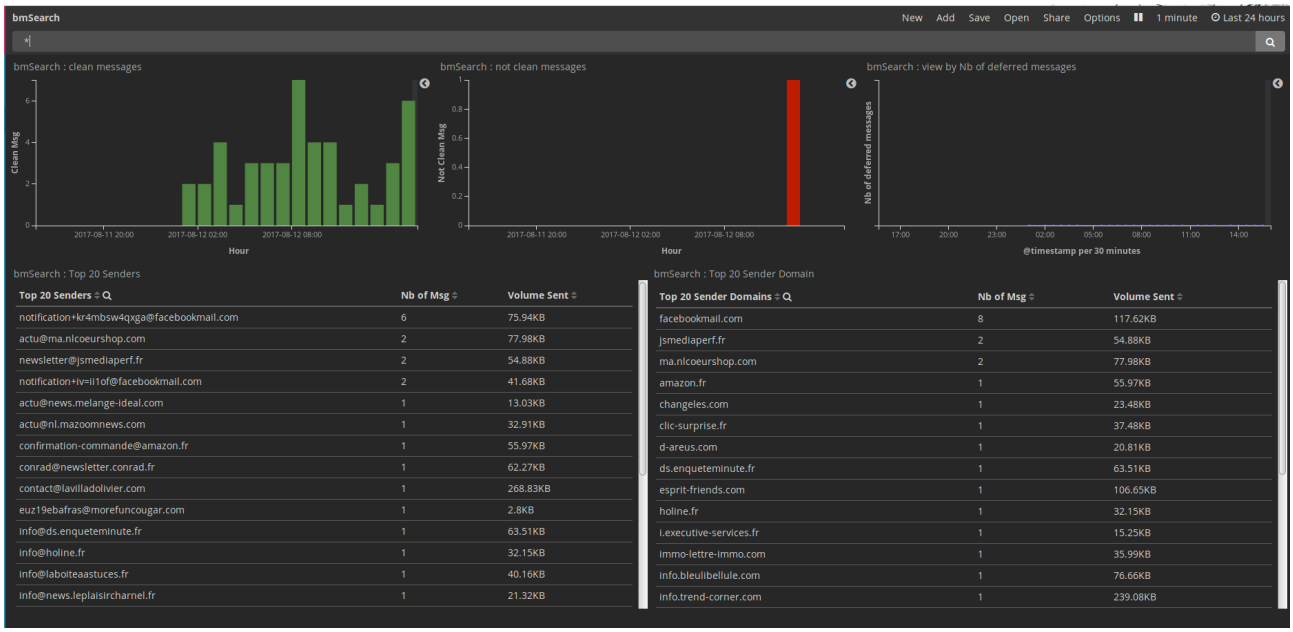
Il est accessible depuis « Dashboards », puis « Open ».



On filtre sur « bm », et on clique sur « bmSearch »



Ce qui donne un truc comme :

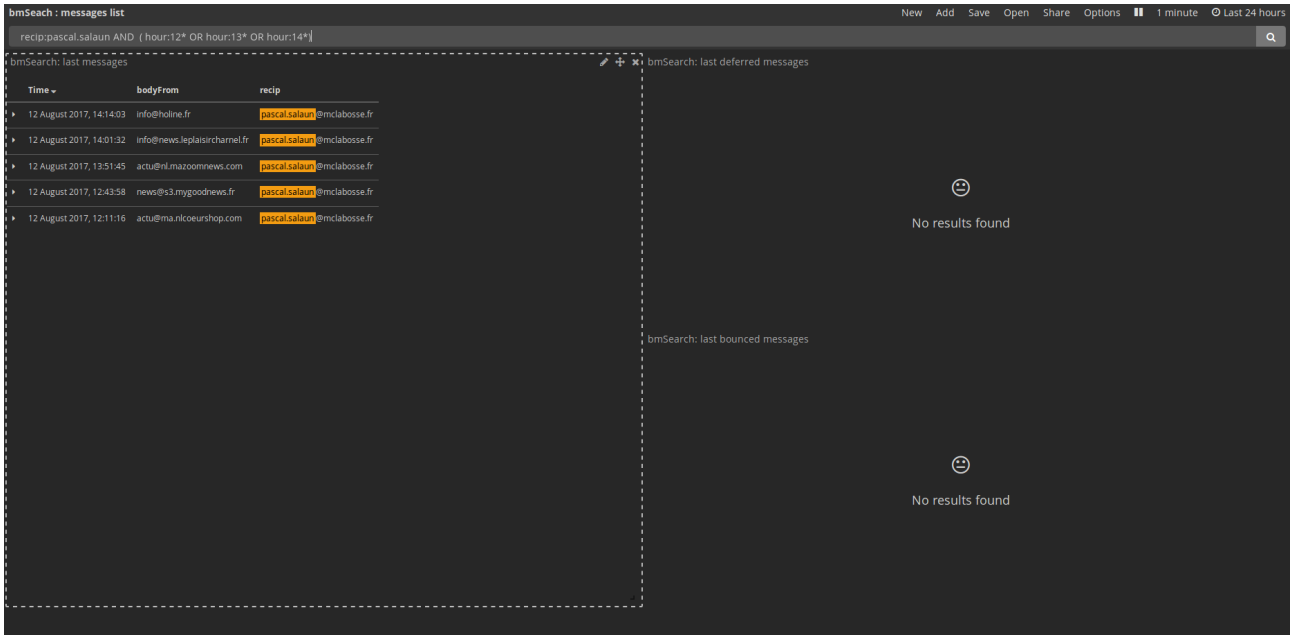


Par défaut, il affiche :

- 1 graphique relatif aux messages validés par l’antivirus, s’il y en a un, comme étant « clean »
- 1 graphique relatif aux messages « relevés » par l’antivirus
- 1 graphique relatif aux messages mis en attente (deferred)
- 1 top 20 des plus « émetteurs », le tri est possible sur le nombre ou le volume des messages
- 1 top 20 des domaines les plus émetteurs, avec aussi le tri sur le nombre ou le volume

4.2 Le dashboard des messages

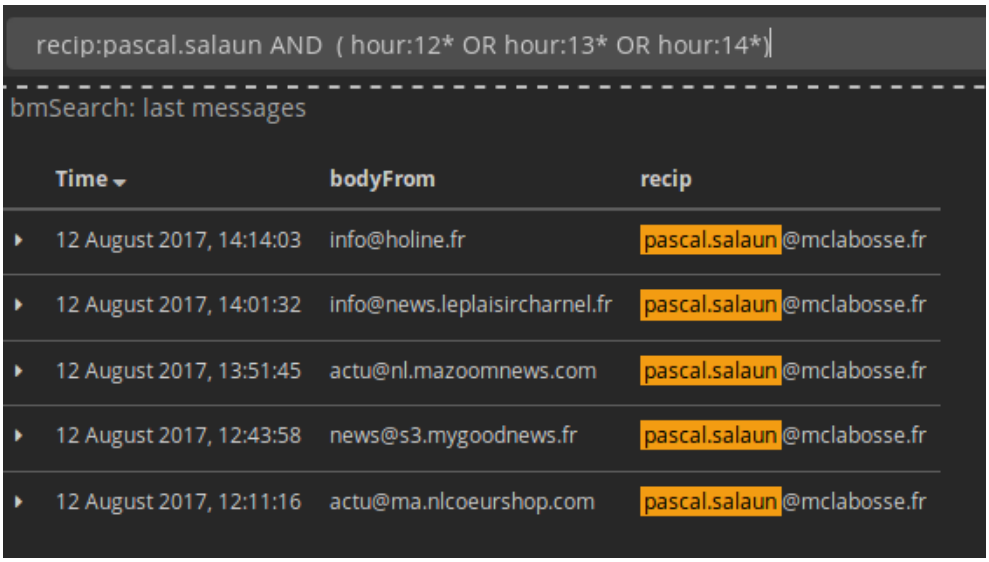
Comme pour le « main », je vous propose un dashboard centré sur les messages. Il s'appelle « bmSearch : messages list », et affiche :



à savoir :

- la liste de tous les messages
- la liste des messages deferred (en attente)
- la liste des messages bounced (détruit)

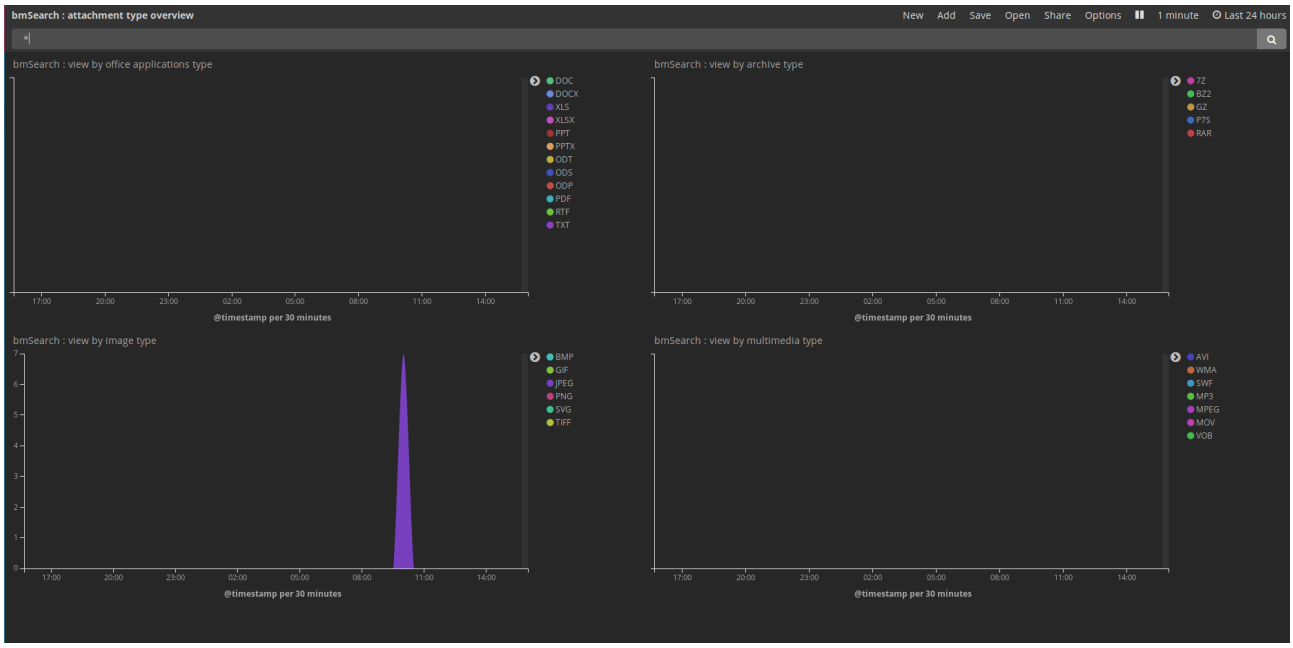
La particularité de cette capture est l'usage, à titre d'exemple, du format de requêtes.



4.3 Le dashboard des types de pièces jointes

Toujours dans la volonté de en fournir plus, vous avez la possibilité de visualiser les types de pièces jointes via « bmSearch : attachment type overview »

Ce qui donne :



Oui, je sais, on ne voit pas grand-chose. Je fais attention à ce que j'envoie ;-)

5. Quelques bricoles concernant KIBANA

5.1 Le type des champs (fields) n’est pas reconnu

Ca c’est parce que soit vous avez modifié le schéma (et c’est pas bien), soit il s’agit de champ qui n’ont que très récemment été alimentés.

Pour y remédier, il suffit de se rendre dans « Management », puis dans « Index Patterns », puis cliquez sur « bmsearch-* »

Vous avez la possibilité de rafraichir la liste des champs en cliquant sur l’icône du mileu, hein, pas celui de droite.

Il va vous dire que cette action va réinitialiser un champ (popularity counters), mais bon, quand on doit, on doit.