Elasticsearch ça roxe. Ave un défaut, la sécurité c'est pas son truc.
A vous de la faire.
Mon problème est le suivant :
1 cluster Elasticsearch composé de 3 noeuds
Tous dans le même réseau
Avec d'autres machines
Comment sécuriser à minima le cluster ES ?

Pour l'accès au plugin head, j'ai opté pour la solution nginx décrite ici.
Par contre pour m'assurer que seul les noeuds elasticsearch discutent entre eux, et qu'ils ne sont accessibles que par le serveur Nginx, je fais appel iptables (!!)

```
apt-get install iptables iptables-persistent

vim /etc/iptables/rules.v4

# Generated by iptables-save v1.4.21 on Wed Jul 29 23:22:59 2015
*filter
# par defaut je DROP ce qui arrive
:INPUT DROP [0:0]
# je route pas !!
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [45:6396]
-A INPUT -i lo -j ACCEPT
# je me coupe pas les pattes
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
# les noeuds se parlent sur le port 9300
-A INPUT -s 192.168.0.11 -p tcp -m tcp --dport 9300 -j ACCEPT
-A INPUT -s 192.168.0.12 -p tcp -m tcp --dport 9300 -j ACCEPT
-A INPUT -s 192.168.0.13 -p tcp -m tcp --dport 9300 -j ACCEPT
# c'est bidirectionnelle
-A INPUT -s 192.168.0.11 -p tcp -m tcp --sport 9300 -j ACCEPT
-A INPUT -s 192.168.0.12 -p tcp -m tcp --sport 9300 -j ACCEPT
-A INPUT -s 192.168.0.13 -p tcp -m tcp --sport 9300 -j ACCEPT
# le discover en multicast
-A INPUT -s 192.168.0.11 -p udp -m pkttype --pkt-type multicast --
sport 54328 --dport 54328 -j ACCEPT
```

```
-A INPUT -s 192.168.0.12 -p udp -m pkttype --pkt-type multicast --
sport 54328 --dport 54328 -j ACCEPT
-A INPUT -s 192.168.0.13 -p udp -m pkttype --pkt-type multicast --
sport 54328 --dport 54328 -j ACCEPT
# nginx lui peut causer sur le port 9200
-A INPUT -s 192.168.0.10 -p tcp -m tcp --dport 9200 -j ACCEPT
# dns dés fois que ....
-A INPUT -s 192.168.0.1 -p udp -m udp --sport 53 -m state --state
ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.0.2 -p udp -m udp --sport 53 -m state --state
ESTABLISHED -j ACCEPT
# a la fin je log et je drop
-A INPUT -j LOG --log-prefix "MYLOG:" --log-level 7
-A INPUT -j DROP
COMMIT
# Completed on Wed Jul 29 23:22:59 2015
```