1. **logstash:**

**配置文件**

input {

file {

type => "log"

path => "/logs/\*.log" #注意此为logstash机器的路径

start\_position => "beginning"

}

}

output {

stdout {

codec => rubydebug { }

}

elasticsearch {

hosts => "127.0.0.1" #注意此为es的机器地址。如果es的端口不是9200，则需要填入指定的端口

index => "log-%{+YYYY.MM.dd}"

}

}

1. 收集不到日志：此种情况请检查path是否配对，是否写入了新的log。
2. 连不上es：90%是es地址配错，还有就是es的机器开了防火墙。
3. **Es**

**配置文件：**

cluster.name: my-es#注意一个集群里面的机器一定要保持一致

node.name: node-01 #集群需要改名字 同一个集群里面的名字不能相同

node.master: true#尽量配置机器差作为主节点 注意只有两个节点的话第二个请配置为false

node.data: true

network.host: 192.168.0.15

http.port: 9200

transport.tcp.port: 9300

#单播(unicast)协议，指定要发现的节点信息了，可以不指定端口[默认9300]

discovery.zen.ping.unicast.hosts: ["192.168.0.15","192.168.0.15:8300"]

#默认是1看到的具有master节点资格的最小数量，然后才能在集群中做操作。官方的推荐值是(N/2)+1，如果只有2个节点设为1

discovery.zen.minimum\_master\_nodes: 1

discovery.zen.ping.timeout:3s #ping的超时时间，如果网络差则延长

discovery.zen.ping.timeout:180s #设置集群中自动发现其他节点时ping连接的超时时间

http.cors.enabled: true

http.cors.allow-origin: "\*"

bootstrap.system\_call\_filter: false

问题一：外网访问不了：防火墙，端口开放。

问题二：es集群连不上，或者启动报错。请注意如果是直接复制的es文件夹则一定要先去删除es文件夹下面的data目录下所有的文件。否则启动必报错。

1. **Es-head插件安装：**

wget  <https://github.com/mobz/elasticsearch-head/archive/master.zip> 下载head插件

1. 解压：unzip  elasticsearch-head-master.zip
2. 进入到elasticsearch-head-master目录：注意head不能放在es的目录下，否则es启动会报错。
3. 安装nodejs：需要root权限

a.在线方式安装：

curl -sL https://rpm.nodesource.com/setup\_8.x | bash -

yum install -y nodejs

b.离线方式安装：官方文档，下载最新版即可,推荐使用这种方式安装，因为现在已经有很多同学采用在线安装的形式有可能会报错。估计是linux系统版本问题导致

<https://www.runoob.com/nodejs/nodejs-install-setup.html>

c.运行 node –v可以看到版本则安装成功。

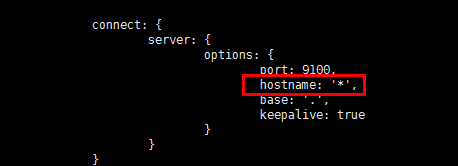
1. 这一步一定要保证在head的目录下：

npm install -g grunt-cli

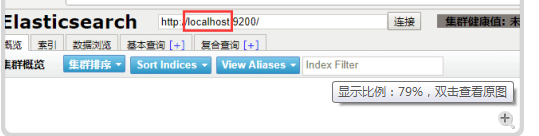
执行完后 会产生node\_modules文件夹

npm install

（5）进入elasticsearch-head-master 文件夹下，执行命令vi Gruntfile.js文件：增加hostname属性，设置为\*。



（6）启动：grunt server，在head的目录下执行。./grunt是在bin下执行，但是现已经证明有些系统这样启动会报错，因此不推荐。注意在访问es-head时出现连接不上，注意只要把截图里面的localhost改成es机器的ip就可以了，集群模式的随便哪一台都没有问题。



1. **Kibana**

在Es和logstash都安装成功后，一定要先往logstash里面写入日志，直到es的索引创建成功再来启动kibana。此时会进入配置界面，如下所示：其中红框的内容是es的索引名字正则表达式，和logstash里面（index => "log-%{+YYYY.MM.dd}"

）的需要一致（也就是正则能匹配的到）。我这里用log-\*就可以匹配

