1.先安装es

1.解压es

2.修改elasticsearch.yml

到config下备份elasticsearch.yml 并修改原始的elasticsearch.yml内容为:

```
#es配置的集群名称默认为:"cluster_name" : "elasticsearch",
cluster.name: my.elk       #集群名称，如果有多个集群，那么每个集群名就得是唯一的
node.name: node-192.168.0.8              #节点名称
node.master: true          #该节点是否是master，true表示是的，false表示否，默认是true
node.data: true                    #该节点是否存储数据，默认true表示是的
http.port: 9200                    #http访问端口，默认是9200，通过这个端口，调用方可以索引查询请求
transport.tcp.port: 9300  #节点之间通信的端口，默认为9300
network.host: 0.0.0.0              #访问地址 配置外网访问
#discovery.zen.ping.unicast.hosts: ["127.0.0.1:9300", "127.0.0.1:8300"]
#node.max_local_storage_nodes: 2              #设置一台机子能运行的节点数目，一般采用默认的1即可，因为我们一般也只在一台机子上部署一个节点
```

启动命令:

```
./bin/elasticSearch  –d  #启动，-d表示后台启动
#日志文件在
logs/下面
tail -f logs/txx-elk.log
```

3.安装head插件

在bin目录下：

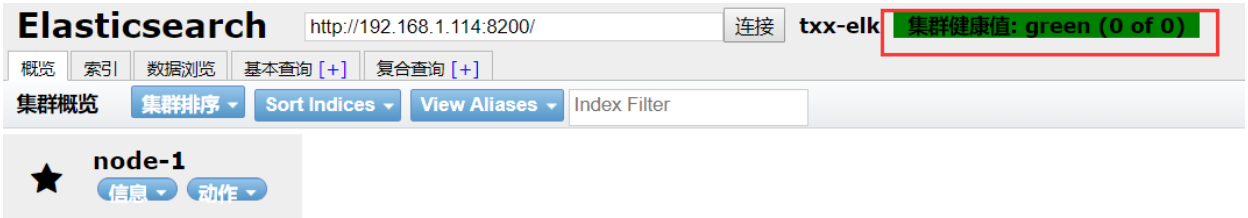
```
[root@localhost bin]# ./plugin install mobz/elasticsearch-head
```

插件在安装目录下的plugins/下

验证是否已经成功：http://x.x.x.x:9200

访问图形界面：http://192.168.0.8:9200/_plugin/head/

浏览器打开es可以查看到



es上方黄色和绿色

绿色

绿色正常

黄色

黄色是因为只有一台机器达不到集群高可用的要求

分片3 副本3

分片3 副本1

2.安装logstash

1.解压

logstash需要自己在安装目录下创建一个config的文件夹

2.编辑config下的配置文件

做好input ，filter，output三大块， 其中input是吸取logs文件下的所有log后缀的日志文件，filter是一个过滤函数，配置则可进行个性化过滤，output配置了导入到hosts为127.0.0.1:9200的elasticsearch中，每天一个索引

config下创建一个抓取文件的配置文件 如果除了.log结尾的文件外还需要.out结尾.json结尾的文件 那么配置多个启动文件,指定启动目录来获取多个启动配置文件读取日志.

```
input {          //收集标志
    file {
        type => "log" //自定义 可以写其他的
        path => ["/export/home/tomcat/domains/*/*/logs/*.log"] //收集日志的地
```

```
方,注意不能远程收取
            start_position => "end"          //如果log文件已经很大了 不要配start，第二次会有记录
                    ignore_older => 0          //忽略最后修改时间是大于多少s的
                    codec=> multiline {                //重点注意 解决日志换行问题。
                    pattern => "^%{TIMESTAMP_ISO8601}"
                    negate => true
                    what => "previous"
                }
        }
        beats {
           port => 5044  //logstash的端口
        }
}
output {
        if [type] == "log" {
                elasticsearch {
                    hosts => ["http://127.0.0.1:9200"]
                    index => "log-%{+YYYY.MM}"              //表示的是索引库 按日期分
                    user => user          //如果配置了nginx密码的则需要填写
                    password => pwd
                }
        }
}
```

说明：start_position是监听的位置，默认是end，即一个文件如果没有记录它的读取信息，则从文件的末尾开始读取，也就是说，仅仅读取新添加的内容。对于一些更新的日志类型的监听，通常直接使用end就可以了；相反，beginning就会从一个文件的头开始读取。但是如果记录过文件的读取信息，则不会从最开始读取。重启读取信息不会丢失。

3.启动logstash

bin目录下启动logstash了，配置文件设置为conf/logstash.conf

启动命令：

```
./logstash -f ../config/logstash.conf
```

后台启动：

```
nohup ./bin/logstash -f config/log.conf > log.log &
```

（4）配置多个文件：./logstash -f ../config 指定启动目录，然后启动目录下配置多个*.conf文件。里面指定不同的logpath。

3.安装kibana

解压后在kibana.yml文件中指定一下你需要读取的elasticSearch地址和可供外网访问的bind地址就可以了。

下面为配置文件：

```
elasticsearch.url: http://localhost:9200  #kibana中这个是注释的
server.host: 0.0.0.0
```

启动命令：

```
./kibana
```

后台启动：

```
nohup ./bin/kibana &
```

ES集成IK分词器