## 硬件选择

### 1，服务器环境

三台机的配置

**Mastar节点机器**

操作系统:linux CentOS 7.0以上

运行内存: 128G以上

硬盘内存:1T以上

**Data节点机器**

操作系统:linux CentOS 7.0 以上

运行内存: 128G 以上

硬盘内存:2T以上

**Data节点机器**

操作系统:linux CentOS 7.0以上

运行内存: 128G 以上

硬盘内存:2T以上

### 2，说明

**命令仅供参考，实际操作请手动输入命令，不要直接复制粘贴！！！**

## 配置选择

### 1，架构选择

elasticsearch 6.2.0+ kibana 6.2.0

elasticsearch 6.2.0 下载地址

https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.0.tar.gz

cerebro 0.7.2 下载地址

https://github.com/lmenezes/cerebro/releases/download/v0.7.2/cerebro-0.7.2.tgz

kibana 6.2.0 下载地址

https://artifacts.elastic.co/downloads/kibana/kibana-6.2.0-linux-x86\_64.tar.gz

**2.2.1 JDK配置版本**

oracle JDK:1.8及以上版本

<http://www.oracle.com/technetwork/java/javase/downloads>

**2.2.2 配置说明**

**JDK**

elasticsearch的环境依赖

### 检查配置

说明: 如果敲入以下命令失败，首先检查命令格式是否正确，然后再检查是否按照顺序敲命令的。

对三台机器IP互相PING,看是否能正常通信

**CentOS 7**

关闭防火墙

systemctl   stop   firewalld.service

## 环境配置

### 1，JDK配置（三台机子都必须装上）

3.1.1 文件准备

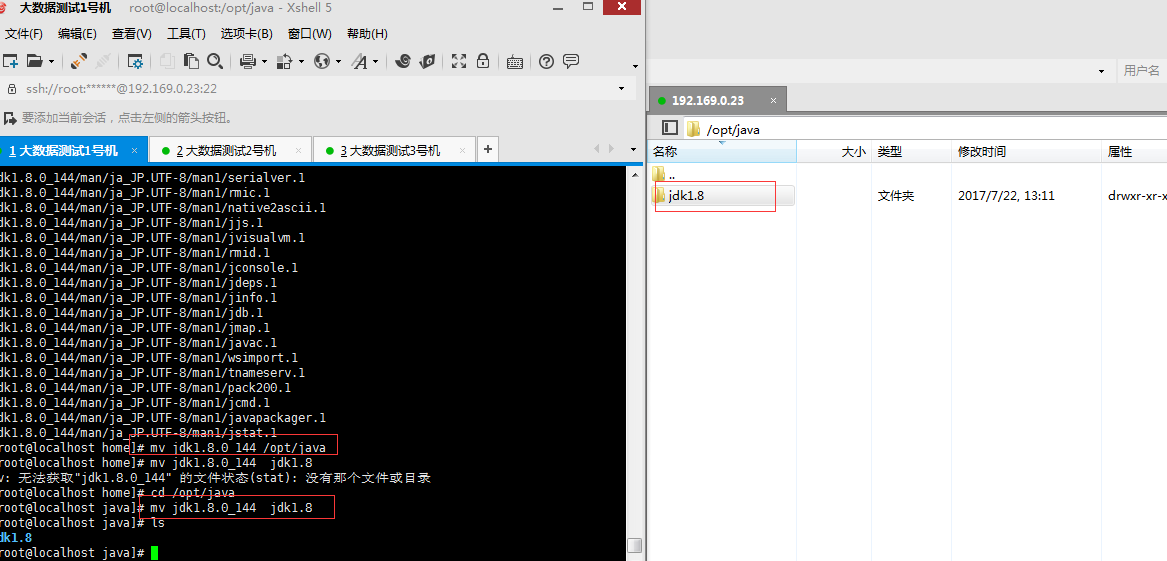
解压下载下来的JDK

tar -xvf jdk-8u144-linux-x64.tar.gz

移动到opt/java文件夹中，没有就新建，然后将文件夹重命名为jdk1.8

mv jdk1.8.0\_144 /opt/java

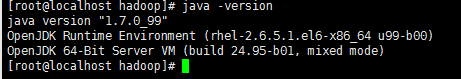
mv jdk1.8.0\_144 jdk1.8



3.1.2环境配置

首先输入 java -version

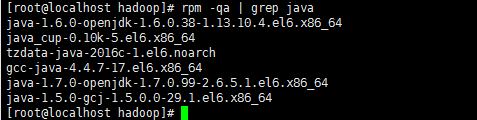
查看是否安装了JDK，如果安装了，但版本不适合的话，就卸载



输入

rpm -qa | grep java

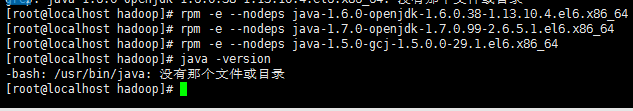
查看信息



然后输入:

rpm -e --nodeps “你要卸载JDK的信息”

如: rpm -e --nodeps java-1.7.0-openjdk-1.7.0.99-2.6.5.1.el6.x86\_64



编辑**/etc/profile** 文件

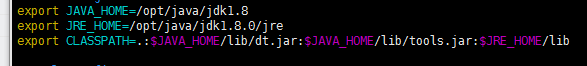
输入:

export JAVA\_HOME=/opt/java/jdk1.8

export JRE\_HOME=/opt/java/jdk1.8/jre

export CLASSPATH=.:$JAVA\_HOME/lib/dt.jar:$JAVA\_HOME/lib/tools.jar:$JRE\_HOME/lib

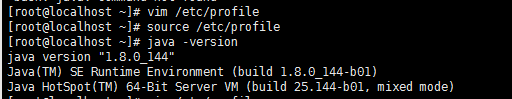
export PATH=.:${JAVA\_HOME}/bin:$PATH



注: JAVA\_HOME的路径是 JDK的路径

使用vim 编辑之后 记得输入 source /etc/profile 是配置生效

配置完后，输入java -version 查看版本信息



### 2，elasticsearch 配置（三台服务器都需要配置）

3.2.1 文件准备

将下载好的elasticsearch-6.2.0.tar.gz文件解压

输入

tar -xvf elasticsearch-6.2.0.tar.gz

然后移动到/opt/elk文件夹 里面，没有该文件夹则创建

输入

mv elasticsearch-6.2.0 /opt/elk

elasticsearch需要在非root的用户下面操作，则

adduser elastic

chown -R elastic:elastic /opt/elk/elasticsearch-6.2.0

接下来创建ES数据文件夹和日志文件夹(注意:需要在数据盘下面创建)

比如数据硬盘挂载在home文件夹，则

chmod o+w /home

此步进入elastic用户环境

su elastic

cd /home

使用ls命令查看是否有elastic文件夹，如果没有的话就执行下面这句命令创建文件夹

mkdir elastic

cd elastic

mkdir data logs

三个服务器操作一样即可

3.2.2环境配置

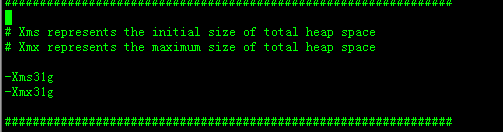
输入:

cd /opt/elk/ elasticsearch-6.2.0

cd config/

1、编辑jvm.options

vi jvm.options



修改为:

-Xms31g

-Xmx31g

保存文件退出，测试环境可以配置1到10G这样即可

2、编辑elasticsearch.yml

先对文件夹下原有的配置文件elasticsearch.yml修改名字以做备份

mv elasticsearch.yml elasticsearch.yml\_back

新建一个全新的elasticsearch.yml

mkdir elasticsearch.yml

vi elasticsearch.yml

这里Master机器节点和data机器节点的配置机子的配置不一样

注意:每台机器的elasticsearch的配置中node.name名字都不一样

**cluster.name**为集群名称，查看日志的时候用到

Master节点服务器的elasticsearch.yml

cluster.name: bigData-cluster

node.name: data01

#数据地址

path.data: /home/elastic/data

#日志地址

path.logs: /home/elastic/logs

network.host: 0.0.0.0

network.publish\_host: 当前机器IP

transport.tcp.port: 9300

http.port: 9200

discovery.zen.ping.unicast.hosts: ["IP1:9300","IP2:9300","IP3:9300"]

node.master: true

node.data: false

discovery.zen.minimum\_master\_nodes: 1

indices.fielddata.cache.size: 12gb

bootstrap.memory\_lock: true

bootstrap.system\_call\_filter: false

Data节点服务器的elasticsearch.yml

cluster.name: bigData-cluster

node.name: data02

#数据地址

path.data: /home/elastic/data

#日志地址

path.logs: /home/elastic/logs

network.host: 0.0.0.0

network.publish\_host: 当前机器IP

transport.tcp.port: 9300

http.port: 9200

discovery.zen.ping.unicast.hosts: ["IP1:9300","IP2:9300","IP3:9300"]

node.master: false

node.data: true

discovery.zen.minimum\_master\_nodes: 1

indices.fielddata.cache.size: 12gb

bootstrap.memory\_lock: true

bootstrap.system\_call\_filter: false

注意:配置中的IP1,IP2,IP3为集群中的每个服务器的实际内网IP，注意查看机器中9300端口和9200端口是否被占用

配置中的indices.fielddata.cache.size在测试的时候可以删掉,也可根据服务器内存配置

### 3、Linux配置

**这里的操作需要回到root用户下操作**

su root

**1、修改sysctl.conf**

vi /etc/sysctl.conf

# 增加

vm.max\_map\_count = 655360

保存退出，输入以下命令执行

sysctl -p

输入 cat /etc/sysctl.conf | grep vm.max\_map\_count



**2、修改90-nproc.conf**

vi /etc/security/limits.d/90-nproc.conf

注:不同的linux服务器90-nproc.conf可能文件名不一样，有的可能是20-nproc.conf，建议先进/etc/security/limits.d/查看文件名再执行vi命令修改

修改如下内容：

\* soft nproc 2048

#修改为

\* soft nproc 4096

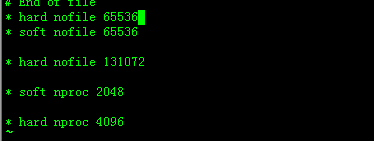
**3、修改limits.conf**

vi /etc/security/limits.conf

添加如下内容:

\* hard nofile 65536

\* soft nofile 65536



### 4，cerebro配置

这个配置也需要在root用户下操作

**说明**

cerebro只需要部署在Master节点的机器即可, ，Data节点服务器不需要部署

3.4.1 文件准备

将下载下来的cerebro 0.7.2.tar.gz进行解压

在linux上输入:

tar -xvf cerebro 0.7.2.tar.gz

然后将解压之后的文件夹移动到opt/elk文件夹下。

在linux上输入移动文件夹命令:

mv cerebro 0.7.2 /opt/elk

### 5，kibana 配置

这个配置也需要在root用户下操作

**说明**

kinaba只需要部署在Master节点的机器即可, Data节点服务器不需要部署

3.5.1 文件准备

将下载下来的kibana-6.2.0-linux-x86\_64.tar.gz的配置文件进行解压

在linux上输入:

tar -xvf kibana-6.2.0-linux-x86\_64.tar.gz

然后移动到/opt/elk 里面

输入

mv kibana-6.2.0-linux-x86\_64 /opt/elk

进入文件夹

cd /opt/elk/kibana-6.2.0-linux-x86\_64

修改配置

vi config/kibana.yml

将配置文件中的

server.host: "localhost"

修改为

server.host: "192.169.2.98"

192.169.2.98这个IP改成你安装kibana这台服务器的内网IP

保存退出

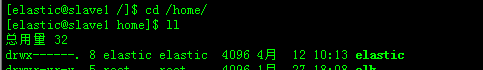
## 运行

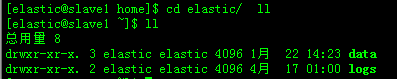
### 1，elasticsearch启动

注: ES必须使用非root用户启动,切换到刚才我们创建好的用户elastic操作

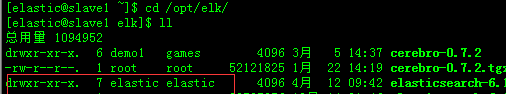
在root的环境下输入,三台机子必须都得这样，查看与elasticsearch相关的文件夹是否已经是elastic用户组

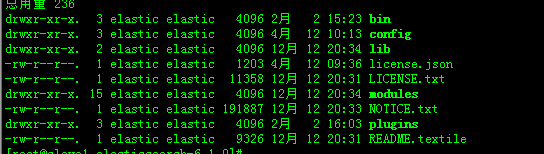
如图





安装文件





如果不是的话请在root用户修改修改文件夹用户组，是的话无需执行以下命令

chown -R elastic:elastic /opt/elk/elasticsearch-6.2.0

chown -R elastic:elastic /home/elastic/

其中/home/elastic 为安装时候创建的数据文件夹

然后切换用户

su elastic

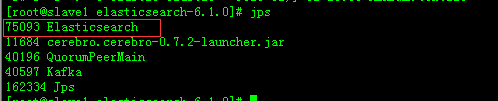
1、先启动Master节点的机器，再依次启动data节点的机器，进入elasticsearch-6.2.0文件夹，启动命令如下

./bin/elasticsearch -d

验证是否成功,输入

jps

查看是否有进程



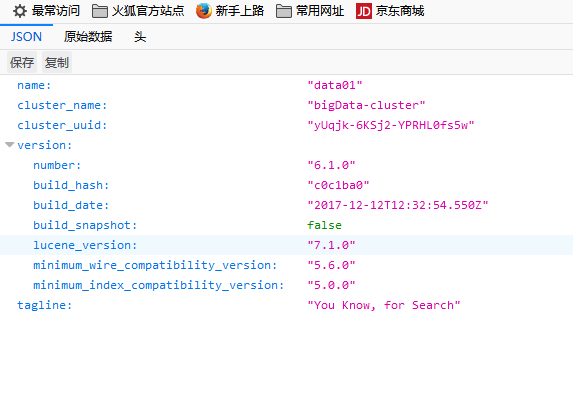
如果启动不起来请到

/home/elastic/logs下面查看日志，日志名为 集群名称.log

然后看第六节测试&问题是否有解决方法

在浏览器输入

[http://IP:9200](http://192.169.0.23:50070)



### 2，cerebro启动

切换回root用户下启动

su root

进去cerebro-0.7.2文件夹

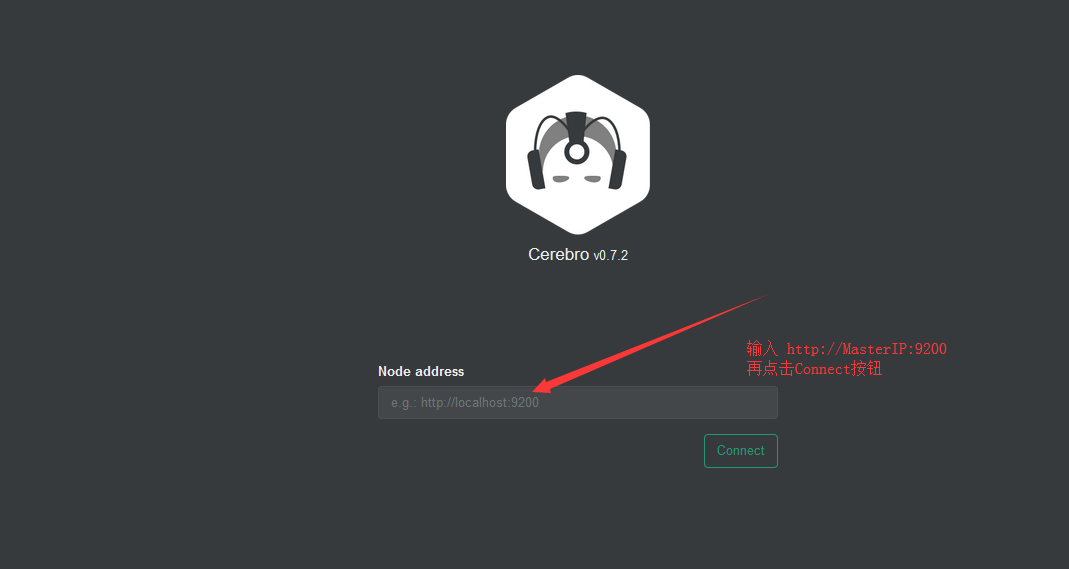
输入:

nohup ./bin/cerebro >/dev/null 2>&1 &

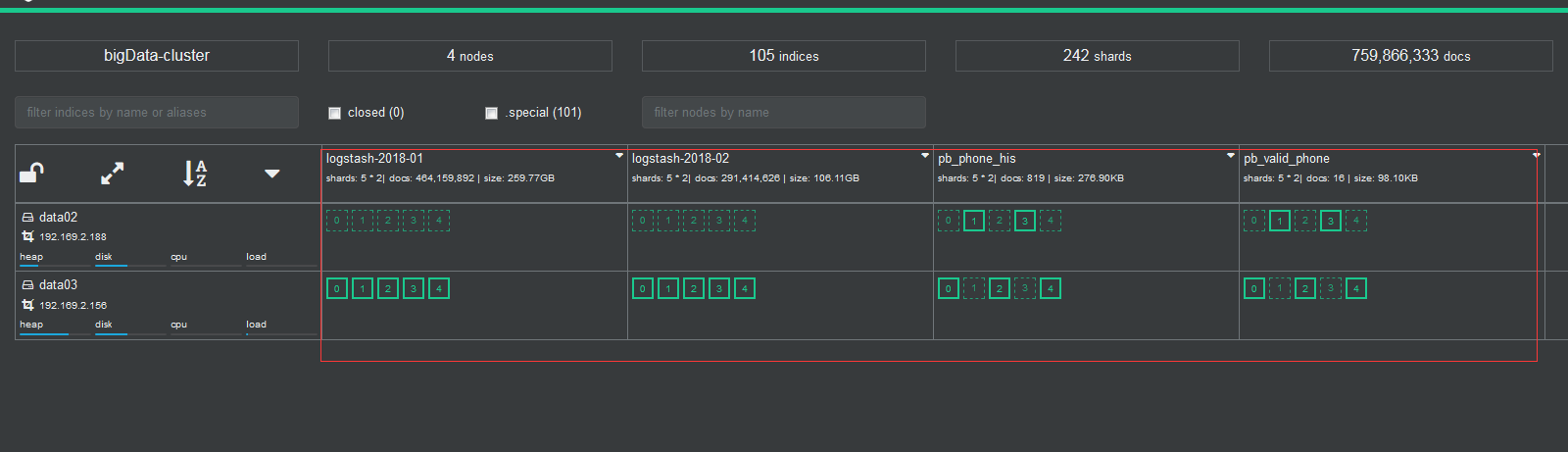
然后启动cerebro

在浏览器输入:

[http://Master的IP:9000](http://192.169.0.23:50070)



**按如图中操作，进入集群管理界面**



**其中红圈部分是数据忽略不计**

### 3，Kinaba 启动

root用户下启动

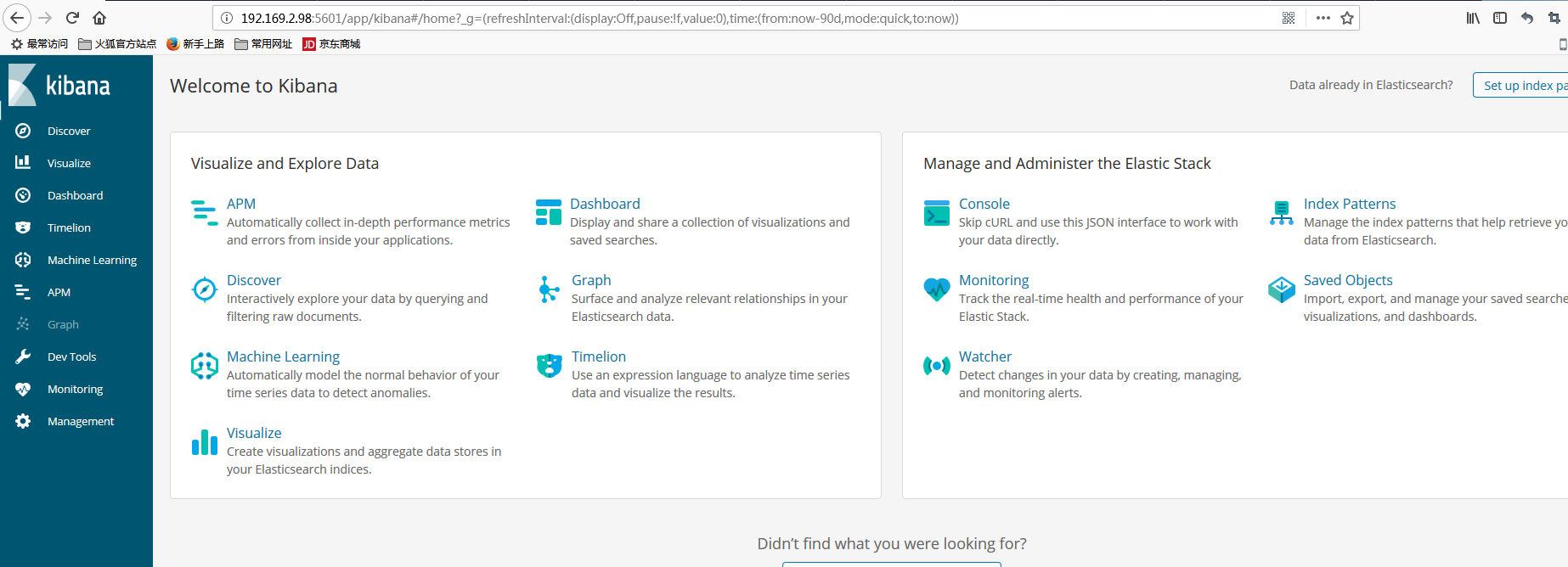
进入kibana-6.1.0-linux-x86\_64文件夹

输入:

nohup ./bin/kibana >/dev/null 2>&1 &

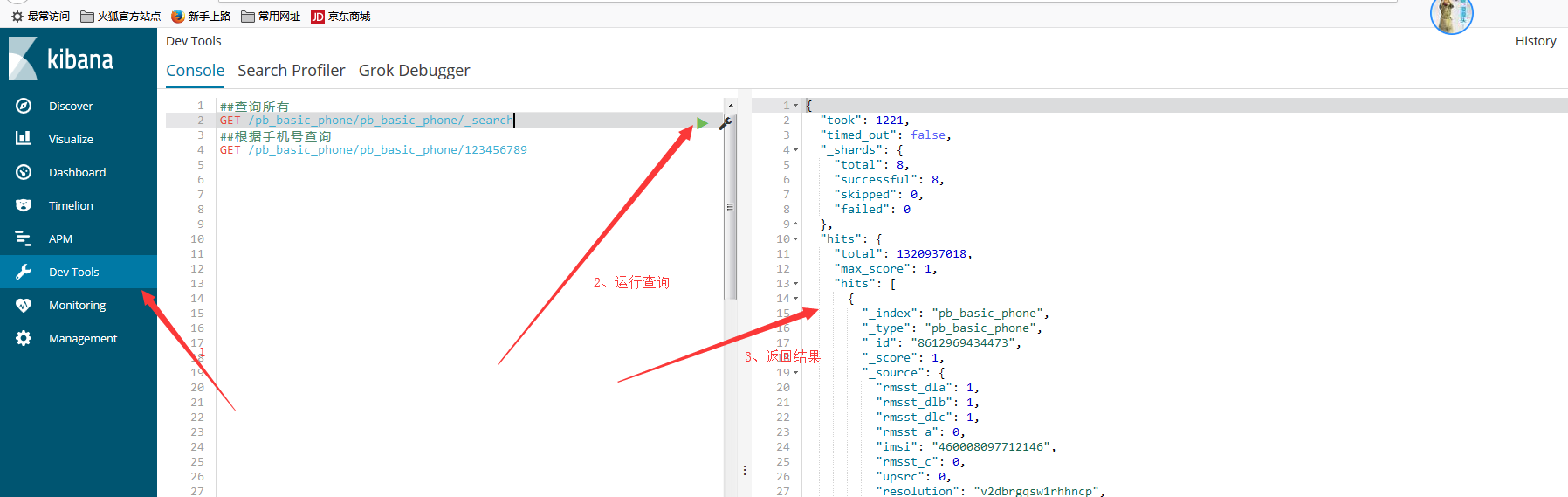
浏览器输入:

[http://Master的IP:5601](http://192.169.0.23:50070)



如图则是运维界面

简单查询操作如下, 相关具体操作可查看文档 www.elastic.co

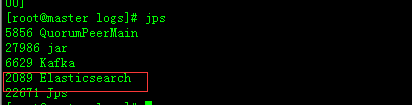


## 停止

### 1，elasticsearch停止

输入

jps获取Elasticsearch进程号



然后执行

kill -9 进程号

如上面图中Elasticsearch进程为2089

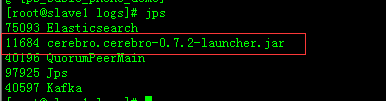
kill -9 2089

注意:如果需要关闭集群需要一个节点一个节点的关闭，如果需要关闭的是Master节点时间长，需要关闭集群下的Data节点。

### 2，cerebro关闭

输入

jps获取cerebro进程号



然后执行

kill -9 进程号

如上面图中cerebro进程为11684

kill -9 11684

### 3，Kinaba 关闭

输入

netstat -tunlp|grep 5601

获取kinaba进程号



然后执行

kill -9 进程号

如上面图中kinaba进程为76587

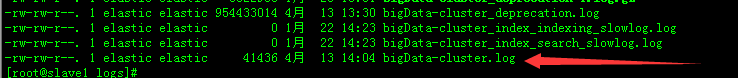
kill -9 76587

## 测试&问题

### 1、如果Elasticsearch启动失败请到/home/elastic/logs 下面查看日志，其中日志名为

集群名称.log

如我这里集群名为bigData-cluster，则查看bigData-cluster.log日志



注: /home/elastic/为你创建的数据文件夹路径

2、注意查看/home/elastic/logs用户归属组是否是elastic，不是的话会报错，改权限



3、如果报以下错，请参考第二个模块第三节Linux配置的1、2、3步

（1）max virtual memory areas vm.max\_map\_count [65530] is too low, increase to at least [262144]

参考第一个配置

(2) max file descriptors [65535] for elasticsearch process likely too low, increase to at least [65536]

参考第三个配置

（3）max number of threads [2048] for user [elastic] is too low, increase to at least [4096]

参考第二个配置

4、如果报以下这个错则去修改elasticsearch.yml文件

ERROR:bootstrap checks failed

修改elasticsearch.yml文件中的参数

bootstrap.memory\_lock: true

改为

bootstrap.memory\_lock: false

注:哪台机器报的错就哪台修改即可