# 一：环境，材料准备

参考：

https://www.elastic.co/guide/cn/elasticsearch/guide/current/hardware.html

<https://www.elastic.co/guide/cn/elasticsearch/guide/current/hardware.html>

## 内存推荐：

64 GB 内存的机器是非常理想的，一半给堆内存、一半给非堆内存 指定堆内存方式：export ES\_HEAP\_SIZE=31g，堆内存不要分配超过32 GB

一旦你越过那个神奇的 ~32 GB 的边界，指针就会切回普通对象的指针。 每个对象的指针都变长了，就会使用更多的 CPU 内存带宽，也就是说你实际上失去了更多的内存。事实上，当内存到达 40–50 GB 的时候，有效内存才相当于使用内存对象指针压缩技术时候的 32 GB 内存

启动时候发现：compressed ordinary object pointers [true]说明启动了指针压缩就很好

禁止交互内存：bootstrap.mlockall: true

## CPU推荐：

4核理想

CPU要求不高，但在更快的CPU和更多的核心之间，推荐更多，因为多个内核提供的额外并发远超稍微快点的时钟频率

## 硬盘推荐：

SSD最好，elasticsearch存放数据的磁盘越大越好

提供一个数据做参考：六院47GB 数据表变为索引后51GB

考虑到做2个副本，和定期备份5个，7倍表大小的硬盘容量

## 安装文件：

链接：https://pan.baidu.com/s/1KeocvsaKTfdPsyoqJx8T6w

提取码：pckp

链接：https://pan.baidu.com/s/1xWLrC6Z60Dn-qOulXxie4g

提取码：j1id

复制这段内容后打开百度网盘手机App，操作更方便哦--来自百度网盘超级会员V1的分享

版本：7.9.3 后面有需要再做升级

# 二：单机安装

ELK.zip解压后出现

Elasticsearch-7.9.3

Kibana-7.9.3

Logstash-7.9.3

1. 配置elasticsearch

a：修改elasticsearch\config\elasticsearch.yml

cluster.name: Xiaoping --集群名称

node.name: node-1 --节点名称

node.master: true

node.data: true

path.data: /path/to/data --指定索引数据存储位置

path.logs: /path/to/logs --指定索引数据日志存储位置

path.repo: //172.19.74.26/snapshots --指定快照仓库位置（没有就注释为了快照功能添加的）

# Lock the memory on startup:

bootstrap.memory\_lock: true

network.host: 0.0.0.0

http.port: 9200 --指定启动端口

discovery.seed\_hosts:

- 172.19.74.25 --指定发现节点，多个可以写多个，单节点可以不写

cluster.initial\_master\_nodes:

- node-1 --指定初始化为主节点

#允许跨域访问

http.cors.enabled: true

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

bootstrap.memory\_lock: false

bootstrap.system\_call\_filter: false配置kibana

b：启动服务

bin\elasticsearch.bat 双击

c：变为window servie 服务

bin\elasticsearch-service.bat install

之后window service就出来了，可以配置为自动运行，以便服务器重启服务也自动重启

1. 配置logstash

作用解析数据到es中的，相关配置和使用方法参考：“logstash培训.pptx”

主要也是配置对应的conf文件

1. 配置Kibana

A:指定elasticsearch地址

Kibana\config\kibana.yml

elasticsearch.hosts: ["http://localhost:9200"]

B：启动

Bin\kibana.bat 双击

C：window service运行

Nssm install kibana

浏览器打开：<http://ip:5601>

D：配置ES SearchUI自定义搜索页面

将ES\_SearchUI2.0到上面ELK根目录下

电脑配置node环境：[Node.js 安装配置 | 菜鸟教程 (runoob.com)](https://www.runoob.com/nodejs/nodejs-install-setup.html)

cd ES\_SearchUI2.0

node server.js

配置成功后访问：

[http://ip:82/index.html](http://ip:8082/searchui.html)

注意：这个新版客户端能解决跨域问题直接调用es后台接口，使得定制化功能扩大想象力如export可以导出更多数据导出多少可配置

E：将新搜索地址配置到spotfire中

参考attivio searchui 接入spotfire方式，es searchui方式一样

1. 确保spotfire 中安装有之前attivio searchui的 插件
2. 工具栏中：tools-》administration Manager-》Preference->Evenone->attivio->Searchui server url 中输入新的es searchu地址

至此完成

# 三：集群安装

参考单节点配置

集群配置需要注意点在于elasticsearch服务

### 配置方面需要注意：

主节点elasticsearch 对应的elasticsearch.yml 配置参考单节点配置，需要修改地址：

discovery.seed\_hosts:

- 172.19.74.25 --指定发现节点，多个可以写多个，单节点可以不写

增加你的其他节点

其他节点配置注意项：

cluster.name: Xiaoping --集群名称

node.name: node-2 --节点名称，确保名字唯一性

node.master: true --配置后她可参与选举为主节点，正式环境从节点我推荐false

node.data: true

### 其他注意事项

可能你是一个elasticsearch直接拷贝到从节点的，需要删除配置文件中指定的path.data对应路径，之后再启动从节点，就能加入集群中了