ELK安装

注意：1.Elasticsearch、Kibana、Logstash版本要一致

2.不要在root用户下安装

## 一、Elasticsearch安装：

### 1.下载安装包

进入官网:<https://www.elastic.co/>下载最新安装包

### 2.上传至服务器

### 3.解压安装包

tar -zxvf elasticsearch-6.x.tat.gz

### 4.修改配置文件

进入安装目录下/config文件夹下，修改elasticsearch.yml文件

YML文件是YAML编写的文件格式

它的基本语法规则如下。

|  |
| --- |
| 1.大小写敏感  2.使用缩进表示层级关系  3.缩进时不允许使用Tab键，只允许使用空格。  4.缩进的空格数目不重要，只要相同层级的元素左侧对齐即可  5. # 表示注释，从这个字符一直到行尾，都会被解析器忽略 |

修改的主要内容：注意空格

|  |
| --- |
| #配置es的集群名称，默认是elasticsearch，es会自动发现在同一网段下的  es，如果在同一网段下有多个集群，就可以用这个属性来区分不同的集群。  cluster.name: my-es  #节点名称  node.name： node1  #设置索引数据的存储路径  path.data： 安装路径/data  #设置日志的存储路径  path.logs: 安装路径/logs  #设置当前的ip地址，通过指定相同网段的其他节点会加入该集群中  network.host： 10.18.0.19  #设置对外服务的http端口  http.port: 9200  #设置集群中master节点的初始列表，可以通过这些节点来自动发现新加入  集群的节点  discovery.zen.ping.unicast.hosts: ["node1"] |

### 5.解决启动时报错

1）在root用户下启动报错

因为安全问题elasticsearch 不让用root用户直接运行，所以要创建新用户或者用其他用户。

|  |
| --- |
| 具体操作如下：  useradd es -m  passwd <input es>  mkdir -p elasticsearch-6.3.2/data  mkdir -p elasticsearch-6.3.2/logs  chown -R es:es elasticsearch-6.3.2  chown -R es:es elasticsearch-6.3.2/data  chown -R es:es elasticsearch-6.3.2/logs |

然后使用es用户启动

切换es用户命令：su es

启动集群命令：bin/elasticsearch

1. 在es用户下启动时报错

原因：Centos6不支持SecComp，而ES默认bootstrap.system\_call\_filter为true进行检测，所以导致检测失败，失败后直接导致ES不能启动。

详见 ：<https://github.com/elastic/elasticsearch/issues/22899>

解决方案：在elasticsearch.yml中新增配置bootstrap.system\_call\_filter，设为false。

bootstrap.system\_call\_filter: false

3）在es用户下启动继续报错

第一个问题的原因：

|  |
| --- |
| 原因：无法创建本地文件问题,用户最大可创建文件数太小  解决方案：切换到root用户，编辑limits.conf配置文件， 添加类似如下内容：  vi /etc/security/limits.conf  添加如下内容: 注意\*不要去掉了  \* soft nofile 65536  \* hard nofile 131072  备注：\* 代表Linux所有用户名称（比如 hadoop）  需要保存、退出、重新登录才可生效。 |

第二个错误的原因：

|  |
| --- |
| 原因：无法创建本地线程问题,用户最大可创建线程数太小  解决方案：切换到root用户，进入limits.d目录下，修改90-nproc.conf 配置文件。  vi /etc/security/limits.d/90-nproc.conf  找到如下内容：  \* soft nproc 1024  #修改为  \* soft nproc 4096 |

第三个错误的原因：

|  |
| --- |
| 原因：最大虚拟内存太小  每次启动机器都手动执行下。  root用户执行命令：  执行命令：sysctl -w vm.max\_map\_count=262144  查看修改结果命令：sysctl -a|grep vm.max\_map\_count  看是否已经修改  永久性修改策略：  echo "vm.max\_map\_count=262144" >> /etc/sysctl.conf |

**6.访问ES**

http://10.18.0.19:9200？pretty

#参数pretty是为了美化输出

|  |
| --- |
| JSON  namenode-1  cluster\_namemy-es  cluster\_uuidZdqxuk1jS-K2-ktpMNcZlw  version  number6.3.2  build\_flavordefault  build\_typetar  build\_hash053779d  build\_date2018-07-20T05:20:23.451332Z  build\_snapshotfalse  lucene\_version7.3.1  minimum\_wire\_compatibility\_version5.6.0  minimum\_index\_compatibility\_version5.0.0  taglineYou Know, for Search |

安装成功

## 二、Kibana安装：

### 1.下载安装包

进入官网:<https://www.elastic.co/>下载最新安装包

### 2.上传到服务器

### 3.解压

**tar -zxvf kibana-6.x-xxxx.tar.gz**

### 4.修改配置文件

进入到kibana安装目录下的config文件夹中，修改kibana.yml 文件

|  |
| --- |
| server.host: "10.18.0.19"  elasticsearch.url: "http://10.0.18.19:9200" |

(1)、授权

   chown -R es:es 安装目录/kibana

(2)、启动kibana

 bin/kibana

后台运行：

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

ps -ef|grep node   查看kibana进程

(3)、访问kibana界面

http://node1:5601

## 三、Logstash安装部署

### 1、下载安装包

访问elasticSearch官网地址 <https://www.elastic.co/>

下载指定版本的安装包：kibana-6.x-linux-x86\_64.tar.gz

### 2、上传安装包到指定目录

### 3、解压安装包

tar -zxvf logstash-6.x.tar.gz