# ELK环境部署测试

**注：Logstash Elasticsearch Kibana 的下载地址统一为<https://www.elastic.co/downloads/>**

**问题排查可以登录<https://discuss.elastic.co/c>论坛查找相关信息**

## 安装 Logstash

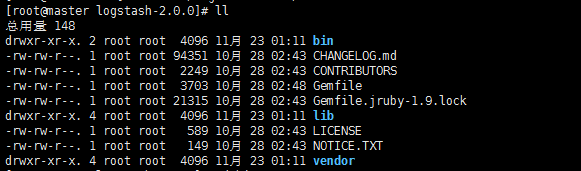
### 1.安装Logstash

下载解压，从上面统一网址找到Logstash下载解压即可，也可以通过wget命令获得：

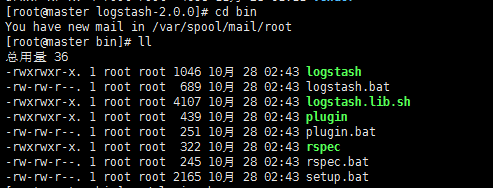
wget <https://download.elastic.co/logstash/logstash/logstash-2.0.0.tar.gz>

### 2.安装插件

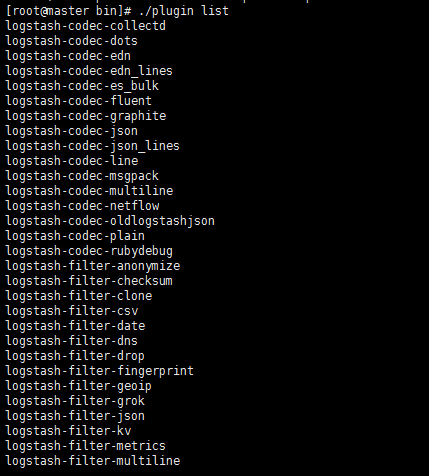
解压后进去看到如下目录：



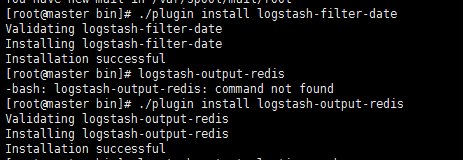
进入bin目录看到：



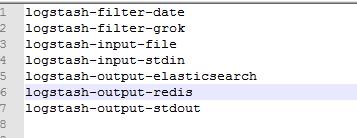
执行./plugin list可以看到目前能安装的插件



通过./plugin install 插件名来安装插件



一些常用的一定要安装的例如：



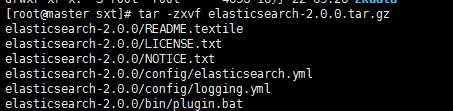
有时候会下载不下来，需要多尝试几次，有时候尝试十几次才行

配置conf文件，启动的时候bin/logstash –f conf文件路径，注意这里的input的文件必须是权限足够的 ，因为Elasticsearch需要普通用户才能启动，所以

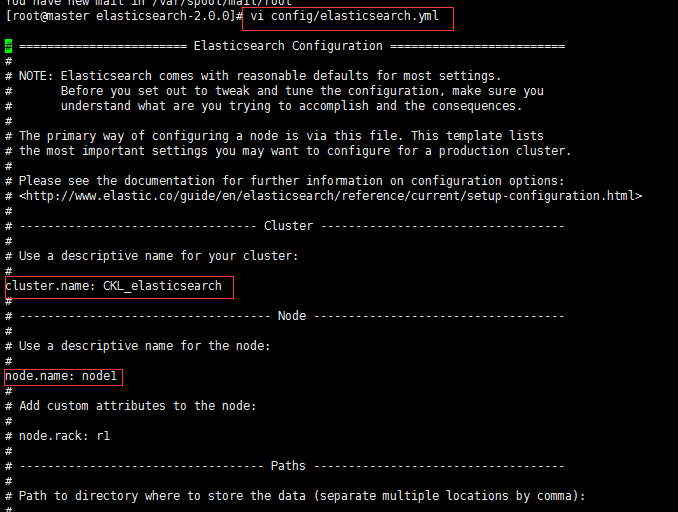
## 安装 Elasticsearch

### 1.安装Elasticsearch集群

下载elasticsearch-2.0.0.tar.gz，执行tar -zxvf elasticsearch-2.0.0.tar.gz解压

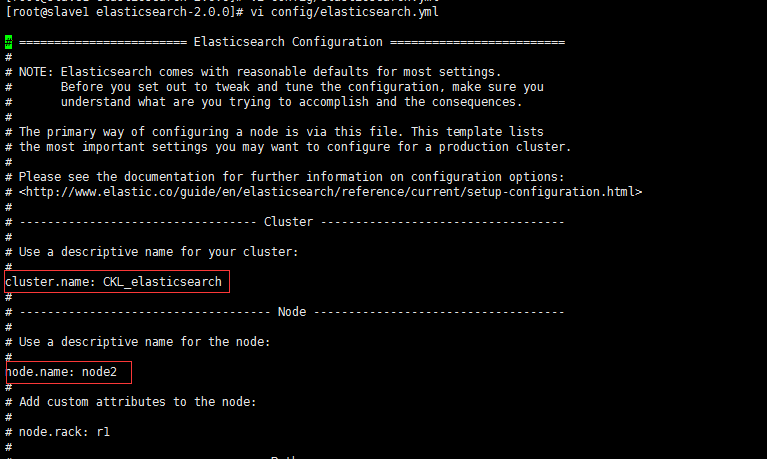


修改配置文件config/elasticsearch.yml



如果要配置集群需要两个节点上的elasticsearch配置的cluster.name相同，都启动可以自动组成集群，这里如果不改cluster.name则默认是cluster.name=elasticsearch，nodename随意取但是集群内的各节点不能相同

本人这里另外一台机器配置如图：

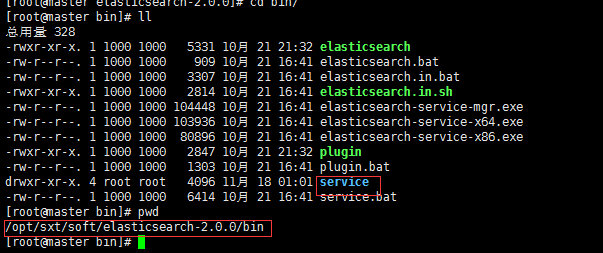


最后同时启动可以组成集群

### ****2.安装elasticsearch-servicewrapper插件****

（1）下载elasticsearch-servicewrapper

                git clone <https://github.com/elasticsearch/elasticsearch-servicewrapper>，然后将目录下的service目录拷贝至ES\_HOME/bin目录下。



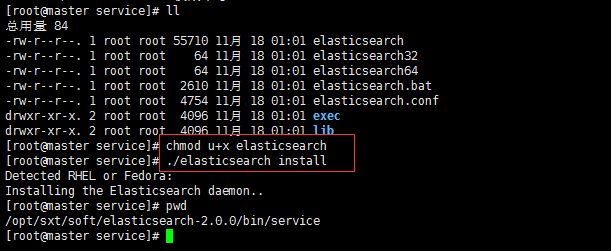
      （2）简单配置jvm的内存

                修改ES\_HOME/bin/service/elasticsearch.conf，set.default.ES\_HEAP\_SIZE=1024，该值根据机器的配置可自定义。

      （3）安装启动服务

                执行命令：ES\_HOME/bin/service/elasticsearch install

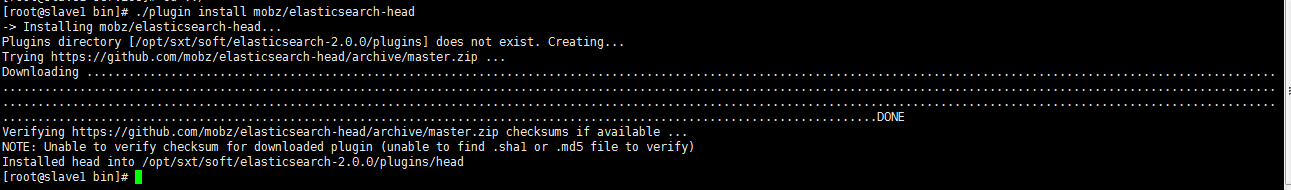
这里需要添加一下执行权限



      （4）启动/停止/重启服务

               执行命令：ES\_HOME/bin/service/elasticsearch start/stop/restart

在bin目录下执行./plugin install mobz/elasticsearch-head来安装head插件



**注意：因为elasticsearch有远程执行脚本的功能所以容易中木马病毒，所以不允许用root用户启动，root用户是起不来的，赋权限，用一般的用户启动**

**要配置network.host和network.publish\_host和network.bind\_host才能别的机器或者网卡访问，否则只能是127.0.0.1或者localhost访问**

**注意配置yml结尾的配置文件都需要冒号后面加空格才行**

**添加防脑裂配置**

**discovery.zen.ping.multicast.enabled: false**

**discovery.zen.ping\_timeout: 120s**

**client.transport.ping\_timeout: 60s**

**discovery.zen.ping.unicast.hosts: ["192.168.57.4","192.168.57.5", "192.168.57.6"]**

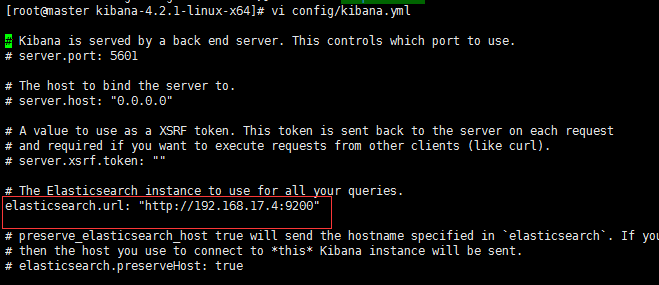
### **3.安装Marvel**

分别在elasticsearch和kibana下安装

|  |  |
| --- | --- |
| **Step 1: Install Marvel into Elasticsearch:** | bin/plugin install license bin/plugin install marvel-agent |
| **Step 2: Install Marvel into Kibana** | bin/kibana plugin --install elasticsearch/marvel/latest |
| **Step 3: Start Elasticsearch and Kibana** | bin/elasticsearch bin/kibana |

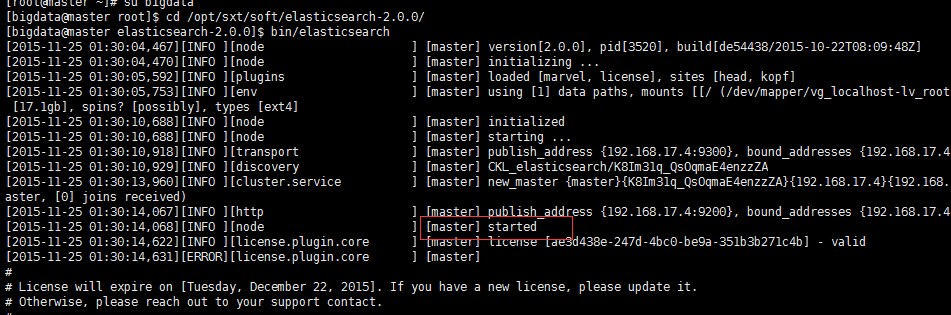
## 安装Kibana

解压安装，修改配置文件vi config/kibana.yml的elasticsearch.url属性即可

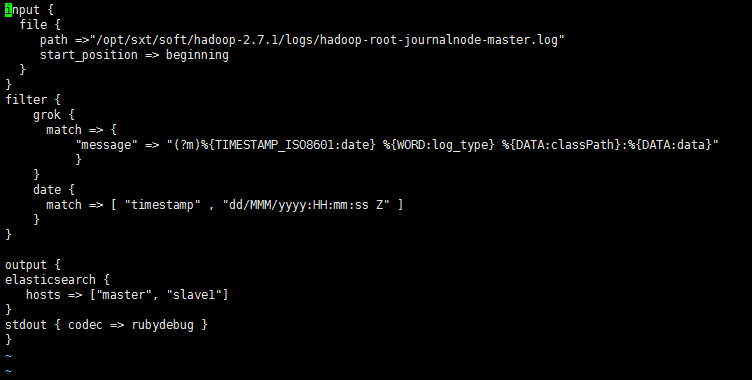


## 测试

用非root用户启动elasticsearch，

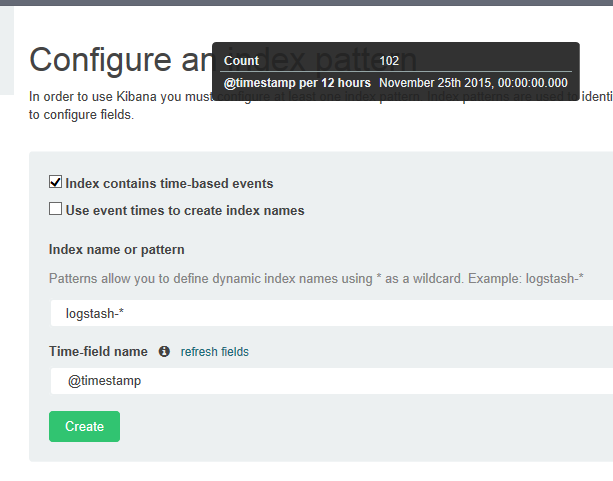


配置logstash的配置文件



启动kibana

访问<http://192.168.17.4:5601/>创建索引



查询结果：

