

**国家电网公司**

**ELK 实时日志分析平台**

**环境搭建手册**

2019年3月

文 档 说 明

|  |  |  |  |
| --- | --- | --- | --- |
| 文档名称 | 《ELK实时日志分析平台环境搭建手册》 | | |
| 文档编号 |  | 版本号 | 1.0 |
| 文档类型 | ○原型稿 ●初稿 ○征求意见稿 ○最终稿 | | |
| 编 制 |  | 日 期 | 2019/03/8 |
| 审 核 |  | 日 期 |  |
| 备 注 |  | | |

修 订 记 录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 修订人 | 修订内容摘要 | 产生版本 | 修订日期 | 审核人 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **ELK配置**
   1. **组件介绍**

###### Elasticsearch:

  是一个基于Lucene的搜索服务器。提供搜集、分析、存储数据三大功能。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口。Elasticsearch是用Java开发的，并作为Apache许可条款下的开放源码发布，是当前流行的企业级搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便。

###### Logstash:

  主要是用来日志的搜集、分析、过滤日志的工具。用于管理日志和事件的工具，你可以用它去收集日志、转换日志、解析日志并将他们作为数据提供给其它模块调用，例如搜索、存储等。

###### Kibana:

  是一个优秀的前端日志展示框架，它可以非常详细的将日志转化为各种图表，为用户提供强大的数据可视化支持。

###### Filebeat: 隶属于Beats。目前Beats包含四种工具：

1.Packetbeat（搜集网络流量数据）

2.Metricbeat（搜集系统、进程和文件系统级别的 CPU 和内存使用情况等数据。通过从操作系统和服务收集指标，帮助您监控服务器及其托管的服务。）

3.Filebeat（搜集文件数据）

4.Winlogbeat（搜集 Windows 事件日志数据）

###### Kafka：

1.发布和订阅记录流，类似于消息队列或企业消息传递系统。

2.以容错持久的方式存储记录流。

3.处理记录发生的流。

* 1. **环境需求**

（1）VMware

（2）Centos 6.5

（3）JDK 1.8

（4）nginx

**jdk官方下载地址** http://www.oracle.com/technetwork/java/javase/downloads/index.html

* 1. **JDK安装** 
     1. **卸载旧版本JDK**

查看是否安装过java

rpm -qa | grep java

rpm -e --nodeps #要卸载的包 (包通过上面的指令可以获取到)

* + 1. **选择安装目录**

选择安装JDK的位置/opt/install，如果存在这个目录无需创建，一般新到的机器是没有这个目录的，这个我们创建这个目录。 指令 需要输入密码

管理员：mkdir /opt/install

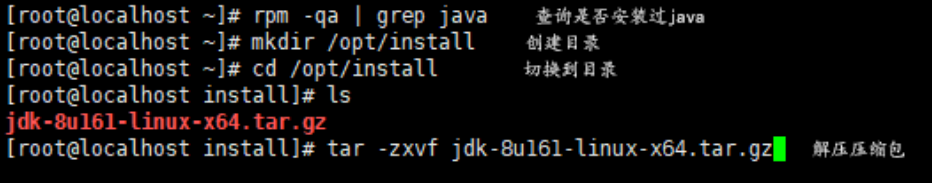
非管理员：sudo mkdir /opt/install

* + 1. **上传和解压**

将jdk-8u131-linux-x64.tar.gz上传到服务器的/opt/install，使用SecureFXPortable(或者filelilla)将文件上传到服务器解压：

cd /opt/install #进入install目录

tar -zxvf jdk-8u131-linux-x64.tar.gz #解压到当前目录



* + 1. **环境变量配置**

vi /etc/profile #打开配置文件

**在文档的最后面添加如下内容，记住不要带空格：**

export JAVA\_HOME=/opt/install/jdk1.8.0\_131

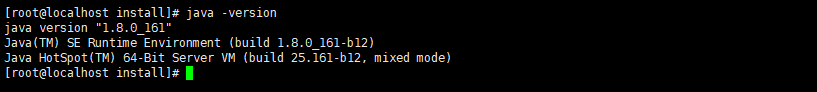
export JRE\_HOME=$JAVA\_HOME/jre

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

export PATH=$PATH:$JAVA\_HOME/bin

source /etc/profile #让配置生效

java –version #验证是否安装成功



**2.Elasticsearch**

## 2.1安装Elasticsearch

将elasticsearch-6.5.3.tar.gz上传到服务器的/opt/install，使用SecureFXPortable(或者filelilla)将文件上传到服务器解压：

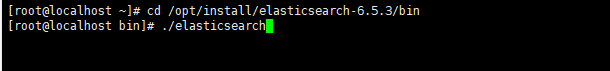
cd /opt/install #进入install目录

tar -zxvf elasticsearch-6.5.3.tar.gz #解压到当前目录

## 2.2运行Elasticsearch

切换至elasticsearch-6.5.3目录下的bin目录，使用

./ elasticsearch 运行



**2.3处理异常**

### 2.3.1[WARN][o.e.b.ElasticsearchUncaughtExceptionHandler] uncaught exception in thread [main]org.elasticsearch.bootstrap.StartupException: java.lang.RuntimeException: can not run elasticsearch as root

原因是elasticsearch默认是不支持用root用户来启动的。

解决方案一：Des.insecure.allow.root=true

修改/usr/local/elasticsearch-2.4.0/bin/elasticsearch，

添加 ES\_JAVA\_OPTS="-Des.insecure.allow.root=true"

或执行时添加： sh /usr/local/elasticsearch-2.4.0/bin/elasticsearch -d -Des.insecure.allow.root=true

注意：正式环境用root运行可能会有安全风险，不建议用root来跑。

解决方案二：添加专门的用户

useradd elastic

chown -R elastic:elastic elasticsearch-2.4.0

su elastic

sh /usr/local/elasticsearch-2.4.0/bin/elasticsearch -d

### 2.3.2ERROR Could not register mbeans java.security.AccessControlException: access denied ("javax.management.MBeanTrustPermission" "register")

sudo chown -R noroot:noroot elasticsearch 改变 elasticsearch 文件夹所有者到当前用户

这是因为 elasticsearch 需要读写配置文件，我们需要给予 config 文件夹权限，需要新建了 elsearch 用户，elsearch 用户不具备读写权限，因此还是会报错，解决方法是切换到管理员账户，赋予权限即可：

sudo –root 切换至管理员权限

chmod -R 775 config 赋予权限

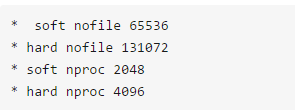
### ****2.3.3 ERROR: [4] bootstrap checks failed[1]: max file descriptors [4096] for elasticsearch process is too low, increase to at least [65536]****

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：

vim /etc/security/limits.conf

添加如下内容:



### ****2.3.4 [2]: max number of threads [1024] for user [tzs] is too low, increase to at least [2048]****

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。

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

找到如下内容：

soft nproc 1024

修改为

soft nproc 2048

### ****2.3.5[3]: max virtual memory areas vm.max\_map\_count [65530] is too low, increase to at least [262144]****

原因：最大虚拟内存太小

root用户执行命令：

sysctl -w vm.max\_map\_count=262144

或者修改 /etc/sysctl.conf 文件，添加 “vm.max\_map\_count”设置 设置后，可以使用 $ sysctl –p

### ****2.3.6 java.lang.IllegalArgumentException:property [elasticsearch.version] is missing for plugin [head]****

在es 的配置文件中加：

http.cors.enabled: true

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

## 2.4 集群部署

### 2.4.1配置节点

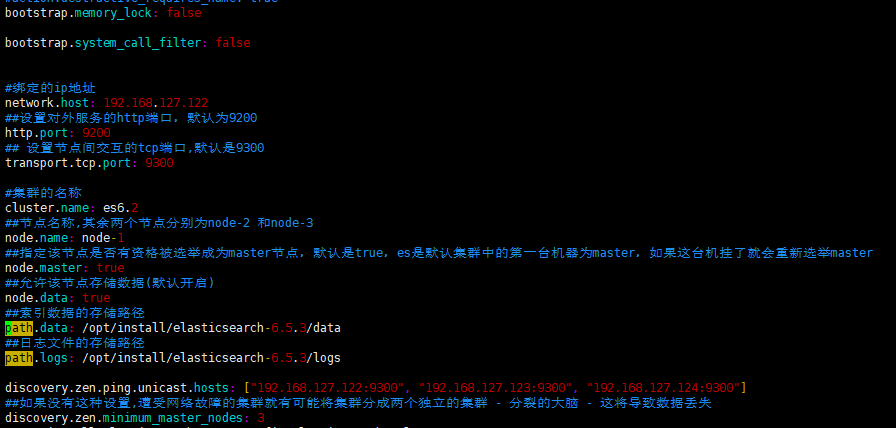
采用三台CentOS7.3部署Elasticsearch集群，需要不同的节点名和IP

|  |  |  |
| --- | --- | --- |
| **系统** | **节点名** | **IP地址** |
| CentOs6.5 | node-1 | 192.168.127.122 |
| CentOs6.5 | node-2 | 192.168.127.123 |
| CentOs6.5 | node-3 | 192.168.127.124 |

### 2.4.2 修改配置文件

使用命令 vim /opt/install/ elasticsearch-6.5.3/config/elasticsearch.yml

下面增加以下内容

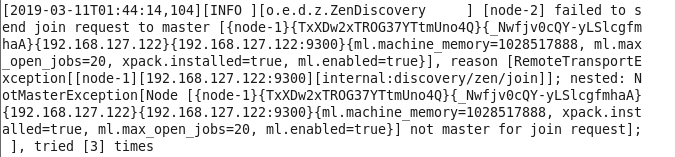


### 2.4.3 集群配置

将该文件复制到不同虚拟机下，设置对应的ip和节点名称（不推荐）

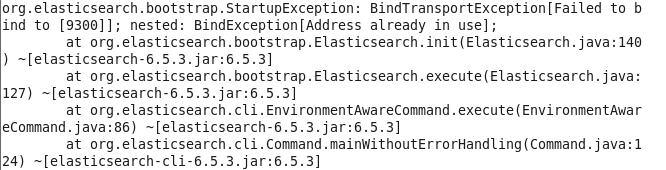
按照单机配置依次安装（推荐）

### 2.4.4 集群异常



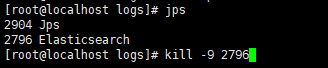
解决方法：删除data目录下的nodes文件

rm –rf nodes



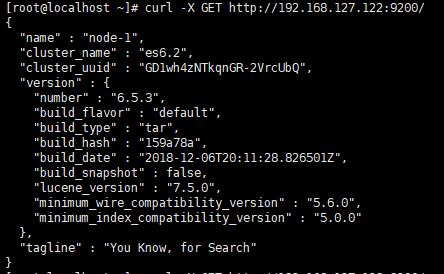
原因：端口占用

解决方法：

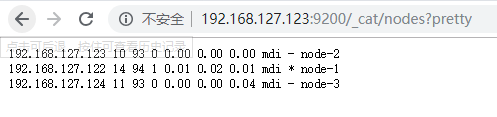


## 2.5 测试

curl -X GET <http://192.168.127.122:9200/> （输入自己的IP）



浏览器输入：<http://192.168.127.122:9200/_cat/nodes?pretty>



# 3. Logstash

## 3.1安装Logstash

注意：ELK下整套环境必须统一版本！！！

将安装压缩包复制至/opt/install目录下解压缩，然后进入bin目录下 新增配置文件logstash**.**conf，文件内容：

input**{**

file**{**

path **=>** **[**"/var/log/\*.log"**]**

**}**

**}**

output**{**

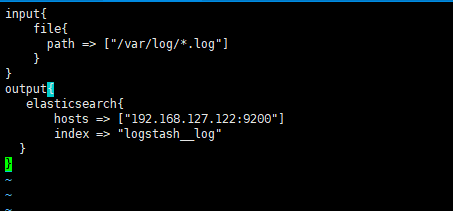
elasticsearch**{**

hosts **=>** **[**"192.168.127.122:9200"**]**

index **=>** "logstash\_\_log"

**}**

**}**



## 3.2运行Logstash

## 在bin目录下运行 ./logstash -f logstash.conf

# 4.Kibana

## 4.1 安装Kibana

安装解压方式同Logstash，然后修改配置文件

kibana-6.5.3/config/kibana.yml

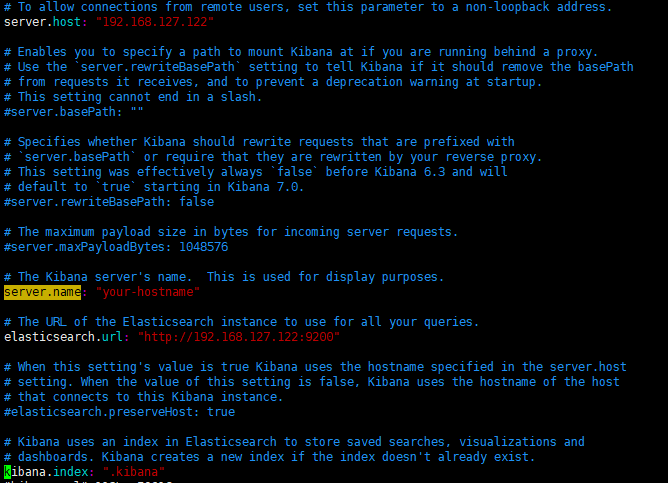
添加：

server.host: "192.168.127.122"

server.name: "your-hostname"

elasticsearch.url: <http://192.168.127.122:9200>

kibana.index: ".kibana"



## 4.2 运行Kibana

在 /usr/local/kibana-5.5.2/bin 目录下运行： ./kibana

## 4.3 连接测试

Web界面访问: [http://192.168.127.122:5601](http://link.zhihu.com/?target=http%3A//ip%3A5601/) ，如果此时需要输入用户名和密码登录,默认分别是 elastic 和 changeme



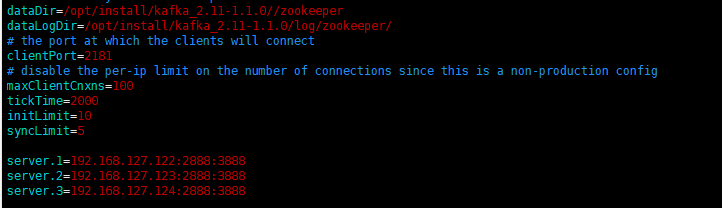
# 5.kafka

## 5.1安装

安装解压方式同Logstash，然后修改配置文件

## 5.2 配置zookeeper

### 5.2.1先通过配置文件，建立zookeeper集群，修改config下的zookeeper.properties文件：



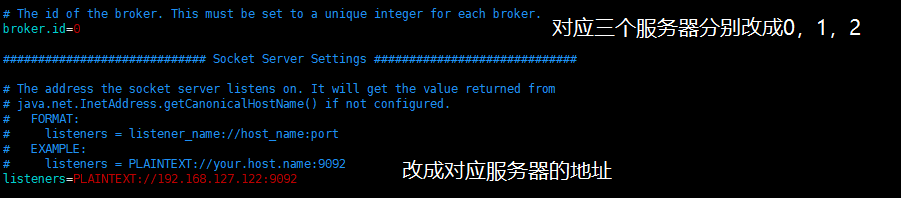
注意：dataDir路径与dataLogDir路径需要手动创建，配置文件不会自动生成

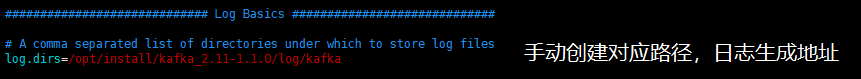
### 5.2.2 进入 /opt/install/kafka\_2.11-1.1.0/zookeeper 创建mkdir文件，在三个服务器下分别写入1，2，3.

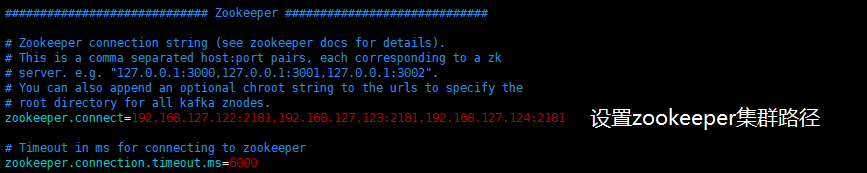
### ------myid是zk集群用来发现彼此的标识，必须创建，且不能相同；

## 5.3 搭建kafka集群

修改server.properties配置文件







## 5.4 启动kafka

启动kafka需要先启动zookeeper，kafka目录下输入

./bin/zookeeper-server-start.sh config/zookeeper.properties &

将三台服务器的zookeeper全部启动。

然后kafka目录下输入

./bin/kafka-server-start.sh config/server.properties &

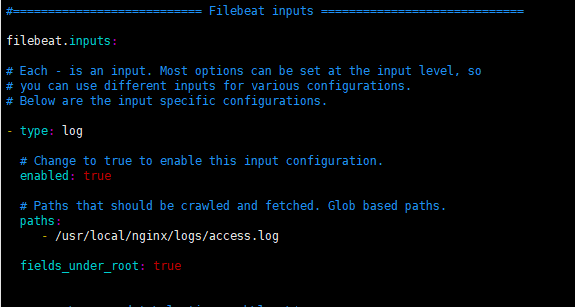
三台服务器全部启动无报错即成功

# 6.filebeat

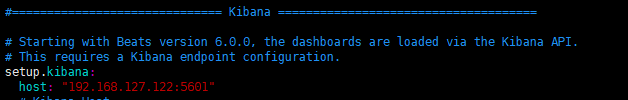
## 6.1 安装

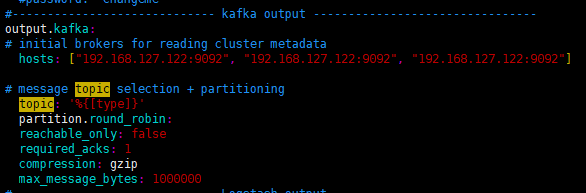
安装解压方式同Logstash，然后修改配置文件

## 6.2 修改配置文件



Paths路径为nginx日志存储路径





输出为kafka集群

## 6.3 运行

## 在filebeat的安装目录下 执行

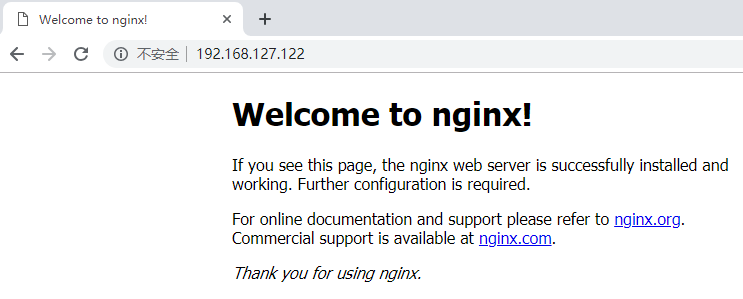
## ./filebeat -e -c filebeat.yml -d "publish"

## 6.4 测试

开启nginx，登录对应IP，端口号默认为80

192.168.127.122:80

出现页面



控制台会接收到nginx的日志并且打印出来

