ELK 搭建

任务名称：通过搭建elk平台 收集ngin服务访问日志

搭建平台：CentOS (Aliyun Linux release 2.1903 LTS)

任务提交者：邹辉

1.搭建环境

程序依赖环境：jdk ,docker(elasticsearch-head组件使用)

数据库:自带elasticsearch

组件： elasticsearch

logstash

kibana

elasticsearch-head组件

2.安装说明

本次搭建使用两台阿里云 云服务器ECS （ node1 node2 ）

两台服务器配置为

CPU 4核 内存8G 硬盘40G

node1 网络 172.26.40.15(私网） 121.89.193.140(公网) tcp 的 5601 9100 9200 都映射到外网相同端口

node2 网络 172.26.40.16(私网）

两台服务器上安装的软件

node1 安装 的软件有

elasticsearch （ 与node2 组成集群）

kibana

elasticsearch-head组件

node2 安装的软件有

elasticsearch

nginx （ 编译安装）

logstash

3.安装步骤

elasticsearch安装 （ node1 node2 需要操作）

1.安装java环境

orcale官网下载jdk

```
#解压到/usr/local
tar xvf jdk-8u241-linux-x64.tar.gz  -C /usr/local
#软连接
ln -s  /usr/local/jdk1.8.0_241  /usr/local/jdk
#配置环境变量
cat /etc/profile.d/java.sh
export JAVA_HOME=/usr/local/jdk
export PATH=$JAVA_HOME/bin:$JAVA_HOME/jre/bin:$PATH
export
CLASSPATH=.$CLASSPATH:$JAVA_HOME/lib:$JAVA_HOME/jre/lib:$JAVA_HOME/lib/tools.jar
# 使其生效
source /etc/profile.d/java.sh
#检查java环境
java -version
```

2.下载 `elasticsearch` rpm 包安装

```
#下载rpm包
wget
https://mirrors.tuna.tsinghua.edu.cn/elasticstack/5.x/yum/5.6.16/elasticsearch-
5.6.16.rpm
#安装
rpm -ivh  elasticsearch-5.6.16.rpm
#java创造软连接
ln -sv /usr/local/jdk/bin/java /usr/bin/
```

3.配置文件

```
node.name: node1  #node2 上改为node2
path.data: /elk/data    #数据目录
path.logs: /elk/logs    #日志目录
bootstrap.memory_lock: true
network.host: 172.26.40.15
http.port: 9200
discovery.zen.ping.unicast.hosts: ["172.26.40.15", "172.26.40.16"]
discovery.zen.minimum_master_nodes: 1
action.destructive_requires_name: true
# elasticsearch-head组件使用
http.cors.enabled: true
http.cors.allow-origin: "*"
```

4.创建数据日志文件目录并修改权限

```
mkdir /elk/{data,logs} -pv
chown  elasticsearch.elasticsearch /elk -R
```

5.启动服务

```
systemctl  restart elasticsearch
systemctl  enable  elasticsearch
```

6.查看集群状态

```
curl -sXGET  http://172.26.40.15:9200/_cluster/health?pretty=true
# status = green 表示正常
```

安装elasticsearch -head插件（node1）

采用docker安装插件

```
 yum install docker -y #安装docker
 systemctl enable docker && systemctl start docker
 docker run -d  -p 9100:9100 mobz/elasticsearch-head:5
```

logstash 环境准备及安装（node2）

1.jdk已经安装可以直接安装 logstash

```
# node1上下载然后 scp 传到node2上
wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-5.x/5.6.16/logstash-5.6.16.rpm
# 安装
rpm -ivh logstash-5.6.16.rpm
```

2.添加配置文件/etc/logstash/conf.d/nginx.conf 内容为

```
input {
  file {
    path => "/apps/nginx/logs/access.log"     start_position => "end"
    codec => json
    }
   }
output {
  elasticsearch {
    hosts => ["172.26.40.16:9200"]
    index => "logstash-nginx-accesslog-%{+YYYY.MM.dd}"
      }
     }
    }
```

3.编译安装的nginx 的配置主目录为 `/apps/nginx`

配置文件为 `/apps/nginx/conf/nginx.conf`

日志文件为 `/apps/nginx/logs/access.log`

配置文件的日志段改为

```
log_format access_json '{"@timestamp":"$time_iso8601",'
    '"host":"$server_addr",'
    '"clientip":"$remote_addr",'
    '"size":$body_bytes_sent,'
    '"responsetime":$request_time,'
    '"upstreamtime":"$upstream_response_time",'
    '"upstreamhost":"$upstream_addr",'
    '"http_host":"$host",'
    '"url":"$uri",'
    '"domain":"$host",'
    '"xff":"$http_x_forwarded_for",'
    '"referer":"$http_referer",'
    '"status":"$status"}';
    access_log  /apps/nginx/logs/access.log  access_json;
```

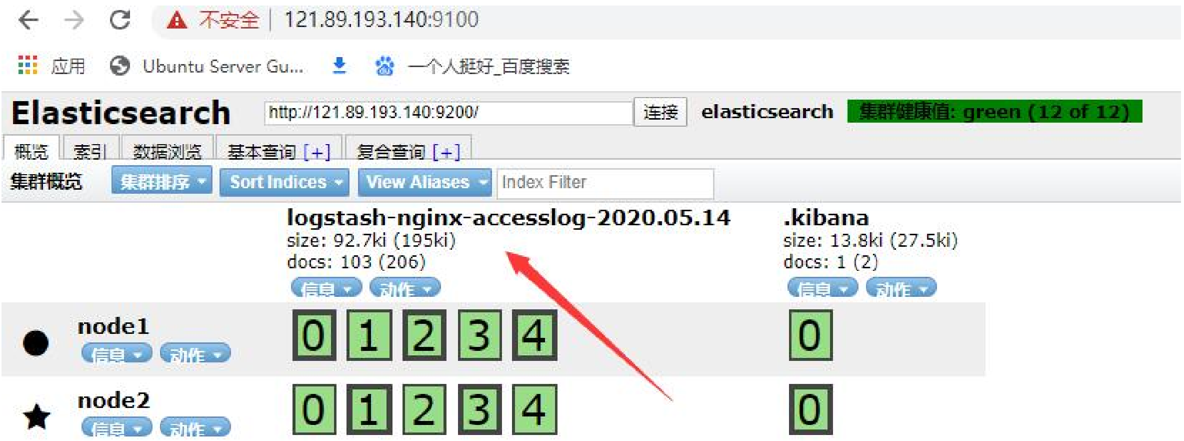
4 检查启动nginx

```
/apps/nginx/sbin/nginx -t # 测试语法
/apps/nginx/sbin/nginx    # 启动nginx
```

5.在 node1 或者node2上 访问nginx 多次

```
curl  172.26.40.16
```

6.在 本地浏览器上 http://121.89.193.140:9100 可查看收集到的日志



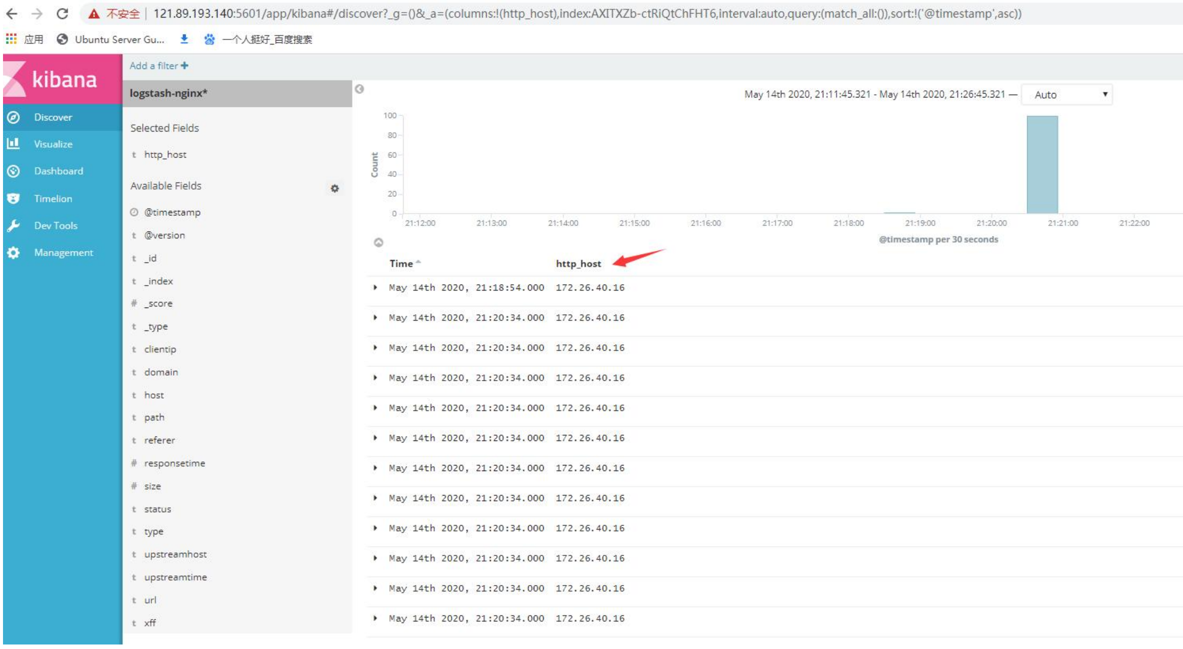
logstash-nginx-accesslog-2020.05.14
size: 92.7ki (195ki)
docs: 103 (206)

.kibana
size: 13.8ki (27.5ki)
docs: 1 (2)

	logstash-nginx-accesslog-2020.05.14	.kibana
● node1	0 1 2 3 4	0
★ node2	0 1 2 3 4	0

7.在本地浏览器上 http://121.89.193.140:5601 可图像化查看日志

![(C:\Users\pomelo\Desktop\2.jpg)



```
Time                          http_host
May 14th 2020, 21:18:54.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
May 14th 2020, 21:20:34.000  172.26.40.16
```