elk安装

==========使用tar.gz包安装elk==========

elasticsearch安装==========

1. 下载安装及配置

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.1.3.tar.gz

tar -zxvf elasticsearch-6.1.3.tar.gz

编辑config/elasticsearch.yml

cluster.name: my-application

node.name: node-1

path.data: /servers/data/elasticsearsh

path.logs: /servers/log/elasticsearch

network.host: 192.168.0.209

http.port: 9200

2. linux创建用户(root用户启动elasticsearch会报错)

useradd elk

passwd elk

chown -R elk:elk /servers

3. root用户编辑`vi /etc/security/limits.conf`

添加如下内容：

```
* soft nofile 65536
* hard nofile 131072
* soft nproc 2048
* hard nproc 4096
```

4. root用户编辑`vi /etc/sysctl.conf`

添加下面配置：

```
vm.max_map_count=655360
```

并执行命令：

```
sysctl -p
```

5. 启动

elasticsearch/bin/elasticsearch -d

kibana安装==========

1. 下载安装及配置

wget https://artifacts.elastic.co/downloads/kibana/kibana-6.1.3-linux-x86_64.tar.gz

tar -zxvf kibana-6.1.3-linux-x86_64.tar.gz

编辑config/kibana.yml

server.port: 5601

server.host: "192.168.0.209"

elasticsearch.url: "http://192.168.0.209:9200"

2. 启动

bin/kibana

logstash安装==========

1. 下载安装及配置

wget https://artifacts.elastic.co/downloads/logstash/logstash-6.1.3.tar.gz

tar -zxvf logstash-6.1.3.tar.gz

编辑 config/logstash.yml
http.host: "192.168.0.209"
http.port: 9600

2. 最简单配置
vi elk.conf
```
input {
  kafka {
    bootstrap_servers => ["192.168.0.209:9092"]
    topics => ["elkTopic"]
    decorate_events => true
    codec => "json"
  }
}

output {
  elasticsearch {
    hosts => ["192.168.0.209:9200"]
    index => "elk"
  }
  stdout {
    codec => rubydebug
  }
}
```

3. 启动
bin/logstash -f elk.conf # -f指定加载配置文件

==========使用tar.gz包安装elk结束==========

kill -9 `ps -ef | grep elastic | awk '{print $2}'`

---

elasticsearch配置说明
```
cluster.name:  elasticsearch
#这是集群名字，我们 起名为 elasticsearch
#es启动后会将具有相同集群名字的节点放到一个集群下。

node.name: "es-node1"
#节点名字。

discovery.zen.minimum_master_nodes: 2
#指定集群中的节点中有几个有master资格的节点。
#对于大集群可以写3个以上。

discovery.zen.ping.timeout: 40s
```

#默认是3s，这是设置集群中自动发现其它节点时ping连接超时时间，
#为避免因为网络差而导致启动报错，我设成了40s。

discovery.zen.ping.multicast.enabled: false
#设置是否打开多播发现节点，默认是true。

network.bind_host: 192.168.137.100
#设置绑定的ip地址，这是我的master虚拟机的IP。

network.publish_host: 192.168.137.100
#设置其它节点和该节点交互的ip地址。

network.host: 192.168.137.100
#同时设置bind_host和publish_host上面两个参数。

discovery.zen.ping.unicast.hosts: ["192.168.137.100", "192.168.137.101","192.168.137.100：9301"]
#discovery.zen.ping.unicast.hosts:["节点1的 ip","节点2 的ip","节点3的ip"]
#指明集群中其它可能为master的节点ip,
#以防es启动后发现不了集群中的其他节点。
#第一对引号里是node1，默认端口是9300,
#第二个是 node2 ，在另外一台机器上,
#第三个引号里是node3，因为它和node1在一台机器上，所以指定了9301端口。