# ELK安装配置使用教程

teamviewer

1173466706 密码：106511

服务器地址： root !QAZ2wsx

套一：

elasticsearch:

http://192.168.210.24:9200/\_cat/nodes

集群：192.168.210.24,25,26

kibana :

http://192.168.210.23:5601

logstash :192.168.210.23

filebeat： 192.168.210.22

套二：

Elasticsearch： 192.168.210.21,27,28

Filebeat：192.168.210.29

Logstash：192.168.210.29

Kibana：192.168.210.29

## rpm包安装教程：

### **一、环境准备**：

Centos7，jdk8

地址：

Elasticsearch ：192.168.210.21,192.168.210.27,192.168.210.28

Filebeat,logstach,kibana: 192.168.210.29

#### 1）、依赖包

准备rpm包：

<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.6.0.rpm>

<https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.0-x86_64.rpm>

<https://artifacts.elastic.co/downloads/logstash/logstash-6.6.0.rpm>

<https://artifacts.elastic.co/downloads/kibana/kibana-6.6.0-x86_64.rpm>

或

wget –c <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.0-x86_64.rpm>

安装：

rpm -ivh elasticsearch-6.6.0.rpm

rpm -ivh logstash-6.6.0.rpm

rpm -ivh filebeat-6.6.0-x86\_64.rpm

rpm -ivh kibana-6.6.0-x86\_64.rpm

#### 2）、安装信息

配置文件默认目录： /etc/elasticsearch,logstash,filebeat,kibana

安装目录：/usr/share/

日志目录： /var/log/

数据存放目录 /var/lib/

#### **3）、设置开机启动**：

sudo systemctl enable elasticsearch.service|logstash.service|filebeat.service|kibana.service

sudo systemctl daemon-reload #重启systemctl

启动命令： systemctl start|stop|status|restart elasticsearch|logstash|filebeat|kibana

#### 4）、关闭防火墙

sudo systemctl status firewalld。

sudo systemctl stop firewalld

systemctl disable firewalld.service#开机关闭防火墙

#开启相关端口 -是或

firewall-cmd --permanent --zone=public --add-port=9200-9300/tcp

### 二、Elasticsearch配置

/etc/elasticsearch/elasticsearch.yml # els的配置文件

/etc/elasticsearch/jvm.options # JVM相关的配置，内存大小等等

/etc/elasticsearch/log4j2.properties # 日志系统定义

/var/lib/elasticsearch # 数据的默认存放位置

#### 1）、elasticsearch.yml

/etc/elasticsearch/

1)、elasticsearch.yml

cluster.name: els-cluster #集群名称-集群节点名称一致

node.name: node-1 #节点名称 -不限制

path.data: /var/lib/elasticsearch #数据默认存放路径

path.logs: /var/log/elasticsearch # 日志的默认存放路径

network.host: 192.168.210.21 #当前节点的ip地址

http.port: 9200 # 对外提供服务的端口，9300为集群服务的端口

discovery.zen.ping.unicast.hosts: ["192.168.210.21", "192.168.210.27","192.168.210.28"] #集群节点

discovery.zen.minimum\_master\_nodes: 2 # 为了避免脑裂，集群节点数最少为 半数+1

#### 2）、jvm.options

-Xmx1g与-Xms1gJVM的最大最小内存。默认1g

如果太小会导致Elasticsearch刚刚启动就立刻停止，太大会拖慢系统本身

3）、启动：

sudo systemctl start elasticsearch

#### 4）、测试

集群测试：

curl -XGET 'http://192.168.210.21:9200/\_cat/nodes?pretty'

* \_cat代表查看信息
* nodes为查看节点信息，默认会显示为一行，所以就用刀了?preety让信息更有好的显示
* ?preety让输出信息更友好的显示

\*代表主节点

<http://192.168.210.21:9200/_cat/nodes> #查看节点情况

<http://192.168.210.21:9200/_cat/health?v> #查看集群健康情况

<http://192.168.210.21:9200/_cat/indices?v> #查看elasticsearch 数据

删除节点数据

curl -XDELETE <http://192.168.210.21:9200/filebeat-6.6.0-2019.02.19>（数据名）

#### 5）、遇到的问题

1、master\_not\_discovered\_exception ：防火墙没关·

2、Curl ‘http://192.168.210.21:9200’

拒绝连接： 关闭防火墙，或开发端口

### 三、logstash 配置

#### 1）、logstash.yml

/etc/logstash/logstash.yml

logstash.yml配置

node.name: node-log #设置节点名称，一般写主机名

path.data: /usr/local/logstash/plugin-data #创建logstash 和插件使用的持久化目录

config.reload.automatic: true #开启配置文件自动加载

config.reload.interval: 10 #定义配置文件重载时间周期

http.host: "192.168.210.23" #定义访问主机名，一般为域名或IP

#### 2）、conf.d(目录)

拷贝logstash-sample.conf 到conf.d 目录 修改 elasticsearch地址

#输入 filebeat

input {

beats {

port => 5044

}

}

#输出 elasticsearch

output {

elasticsearch {

hosts => ["http://192.168.210.21:9200","http://192.168.210.27:9200","http://192.168.210.28:9200"]

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

#user => "elastic"

#password => "changeme"

}

}

注：配置logstash 从Filebeat 输入、过滤、输出至elasticsearch

#### 3）、启动

systemctl start logstash

（默认在 /etc/init.d/ 不存在）

查看日志

cat /var/log/logstash/logstash-plain.log

端口是否正常 监听

netstat -lntp |grep 9600

netstat -lntp |grep 5044

### 四、filebeat配置

#### 1）、filebeat.yml配置

--修改配置文件

/etc/filebeat/conf/filebeat.yml

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/\*.log ###获取在/var/log/\*.log路径下的所有文件作为输入

如果你打算用Kibana仪表盘，可以这样配置Kibana端点：

setup.kibana:

host: "localhost:5601"

output.logstash:

hosts: ["192.168.210.29:5044"]

logging.level: info

#### 2）、启动

service filebeat start/systemctl start filebeat

### 五、安装kibana：

#### 1）、kibana.yml配置

配置/etc/kibana/kibana.yml

#配置本机ip

server.host: "192.168.210.29"

#配置es集群url

elasticsearch.hosts: ["http://192.168.210.21:9200","http://192.168.210.27:9200","http://192.168.210.28:9200"]

#### 2）、启动

sudo systemctl start kibana

浏览器访问

http://192.168.210.29:5601

报错：

Kibana server is not ready yet

解决：集群不健康 修改kibana.yml

kibana.index: ".newkibana"

xpack.security.enabled: false

默认是kibana.index: ".kibana"会报错

重启 systemctl restart kibana

### 附：

--查看elasticsearch数据

curl http://192.168.210.21:9200/\_cat/indices?v

--删除elasticsearch 数据

curl -XDELETE <http://192.168.210.24:9200/filebeat-6.6.0-2019.02.19>

curl -XGET 'http://192.168.210.21:9200/\_cluster/health/balance\_sheet?pretty

<http://192.168.210.21:9200/_cat/health?v>

## 解压版安装

### 环境准备

Elasticsearch:192.168.210.24,25,26

Logstash:192.168.210.23

Filebeat :192.168.210.22

Kibana:192.168.210.23

#### 1）、解压包

<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.6.0.tar.gz>

<https://artifacts.elastic.co/downloads/logstash/logstash-6.6.0.tar.gz>

<https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.5.0-linux-x86_64.tar.gz>

<https://artifacts.elastic.co/downloads/kibana/kibana-6.6.0-linux-x86_64.tar.gz>

或

wget –c <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.6.0.tar.gz>

#### 2）、解压

cd /usr/local

tar -zxvf elasticsearch-6.6.0.tar.gz -C /usr/local

mv elasticsearch-6.6.0 elasticsearch

其他类似

#### 2）、安装信息

安装目录：/usr/local/

日志目录： /var/log/

数据存放目录 /var/lib/

#### 3）、关闭防火墙

sudo systemctl status firewalld。

sudo systemctl stop firewalld

systemctl disable firewalld.service#开机关闭防火墙

#开启相关端口 -是或

firewall-cmd --permanent --zone=public --add-port=9200-9300/tcp

### 二、Elasticsearch配置

/usr/local/elasticsearch/elasticsearch.yml # els的配置文件

/usr/local/elasticsearch/jvm.options # JVM相关的配置，内存大小等等

/usr/local/elasticsearch/log4j2.properties # 日志系统定义

/var/lib/elasticsearch # 数据的默认存放位置

创建用户

adduser els

passwd els

chown -R els elasticsearch #给/usr/local/elasticsearch/ 授权

#日志数据文件 /var/log/\* 授权

cd /var

chown -R els els

#### 1）、elasticsearch.yml

/etc/elasticsearch/

1)、elasticsearch.yml

cluster.name: els-cluster #集群名称-集群节点名称一致

node.name: node-1 #节点名称 -不限制

path.data: /var/lib/elasticsearch #数据默认存放路径

path.logs: /var/log/elasticsearch # 日志的默认存放路径

network.host: 192.168.210.24 #当前节点的ip地址

http.port: 9200 # 对外提供服务的端口，9300为集群服务的端口

discovery.zen.ping.unicast.hosts: ["192.168.210.24", "192.168.210.25","192.168.210.26"] #集群节点

discovery.zen.minimum\_master\_nodes: 2 # 为了避免脑裂，集群节点数最少为 半数+1

#### 2）、jvm.options

-Xmx1g与-Xms1gJVM的最大最小内存。默认1g

如果太小会导致Elasticsearch刚刚启动就立刻停止，太大会拖慢系统本身

#### 3）、修改/etc/security/limits.conf

#els 是用户名

els hard nofile 65536

els soft nofile 65536

注：elasticsearch用户拥有的客串建文件描述的权限太低，至少需要65536个

#重新登录 els账户,查看是否生效

su els

#查看配置是否生效

ulimit -Hn

#### 4）、/etc/sysctl.conf

#添加如下配置

vm.max\_map\_count=262144

#让配置生效

sysctl -p

#查看配置的数目

sysctl -a|grep vm.max\_map\_count

注：运行elasticsearch需要vm.max\_map\_count至少需要262144内存，默认 [65530]

6）、启动：

切换到 els用户

/usr/local/elasticsearch/bin/elasticsearch –d #后台启动

注：也可以配置命令启动 见附表

#### 7）、测试

集群测试：

curl -XGET 'http://192.168.210.24:9200/\_cat/nodes?pretty'

* \_cat代表查看信息
* nodes为查看节点信息，默认会显示为一行，所以就用刀了?preety让信息更有好的显示
* ?preety让输出信息更友好的显示

\*代表主节点

<http://192.168.210.24:9200/_cat/nodes> #查看节点情况

<http://192.168.210.24:9200/_cat/health?v> #查看集群健康情况

<http://192.168.210.24:9200/_cat/indices?v> #查看elasticsearch 数据

删除节点数据

curl -XDELETE <http://192.168.210.24:9200/filebeat-6.6.0-2019.02.19>（数据名）

#### 5）、遇到的问题

1、master\_not\_discovered\_exception ：防火墙没关·

2、Curl ‘http://192.168.210.21:9200’

拒绝连接： 关闭防火墙，或开发端口

3、ERROR: [2] bootstrap checks failed

[1]: max file descriptors [4096] for elasticsearch process is too low, increase to at least [65536]

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

第三、第四部解决

### 三、logstash 配置

#### 1）、logstash.yml

/usr/local/logstash/logstash.yml

logstash.yml配置

node.name: node-log #设置节点名称，一般写主机名

path.data: /usr/local/logstash/plugin-data #创建logstash 和插件使用的持久化目录

config.reload.automatic: true #开启配置文件自动加载

config.reload.interval: 10 #定义配置文件重载时间周期

http.host: "192.168.210.23" #定义访问主机名，一般为域名或IP

#### 2）、配置logstash 从Filebeat 输入、过滤、输出至elasticsearch

拷贝logstash-sample.conf 到from\_beat.conf 重命名 修改 elasticsearch地址

#输入 filebeat

input {

beats {

port => 5044

}

}

#输出 elasticsearch

output {

elasticsearch {

hosts => ["http://192.168.210.24:9200","http://192.168.210.25:9200","http://192.168.210.26:9200"]

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

#user => "elastic"

#password => "changeme"

}

}

注：配置logstash 从Filebeat 输入、过滤、输出至elasticsearch

安装插件：

安装logstash-input-jdbc 和logstash-input-beats-master 插件

/usr/local/logstash/bin/logstash-plugin install  logstash-input-jdbc

wget [https://github.com/logstash-plugins/logstash-input-beats/archive/master.zip -O /opt/master.zip](https://github.com/logstash-plugins/logstash-input-beats/archive/master.zip%20-O /opt/master.zip)

unzip -d /usr/local/logstash /opt/master.zip

#### 3）、启动

/usr/local/logstash/bin/logstash -f /usr/local/logstash/config/from\_beat.conf

端口是否正常 监听

netstat -lntp |grep 9600

netstat -lntp |grep 5044

### 四、filebeat配置

#### 1）、filebeat.yml配置

--修改配置文件

/usr/local/filebeat/conf/filebeat.yml

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/\*.log ###获取在/var/log/\*.log路径下的所有文件作为输入

如果你打算用Kibana仪表盘，可以这样配置Kibana端点：

setup.kibana:

host: "localhost:5601"

output.logstash:

hosts: ["192.168.210.29:5044"]

logging.level: info

#### 2）、启动

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

### 五、安装kibana：

#### 1）、kibana.yml配置

配置/etc/kibana/kibana.yml

#配置本机ip

server.host: "192.168.210.29"

#配置es集群url

elasticsearch.hosts: ["http://192.168.210.21:9200","http://192.168.210.27:9200","http://192.168.210.28:9200"]

#### 2）、启动

./kibana &

浏览器访问

http://192.168.210.29:5601

查出端口：

fuser -n tcp 5601

或

netstat -tunlp|grep 5601

杀死进程

### 附：

#### Elastic设置开机自启动

在/etc/init.d目录下新建文件elasticsearch

#!/bin/sh

#chkconfig: 2345 80 05

#description: elasticsearch

#export JAVA\_HOME=/usr/java/jdk1.8.0\_112

#export JAVA\_BIN=/usr/java/jdk1.8.0\_112/bin

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

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

#export JAVA\_HOME JAVA\_BIN PATH CLASSPATH

case "$1" in

start)

su els<<!

cd /usr/local/elasticsearch

./bin/elasticsearch -d

!

echo "elasticsearch startup"

;;

stop)

es\_pid=`ps aux|grep elasticsearch | grep -v 'grep elasticsearch' | awk '{print $2}'`

kill -9 $es\_pid

echo "elasticsearch stopped"

;;

restart)

es\_pid=`ps aux|grep elasticsearch | grep -v 'grep elasticsearch' | awk '{print $2}'`

kill -9 $es\_pid

echo "elasticsearch stopped"

su els<<!

cd /usr/local/elasticsearch

./bin/elasticsearch -d

!

echo "elasticsearch startup"

;;

\*)

echo "start|stop|restart"

;;

esac

exit $?

保存退出：

执行

chmod +x elasticsearch

添加开机启动

chkconfig -add elasticsearch

service elasticsearch start/stop/restart

#### elasticsearch查询

--查看elasticsearch数据

curl http://192.168.210.21:9200/\_cat/indices?v

--删除elasticsearch 数据

curl -XDELETE <http://192.168.210.24:9200/filebeat-6.6.0-2019.02.19>

curl -XGET 'http://192.168.210.21:9200/\_cluster/health/balance\_sheet?pretty

<http://192.168.210.21:9200/_cat/health?v>

## 应用案例：

Filebeat过滤数据+logstash 解析数据+elsaticsearch存储数据+kibana显示数据

### **一、Filebeat过滤：**

修改 filebeat 配置文件

include\_lines: ['\d{1}:\d{2}:\d{2}'] 过滤满足条件的行

register：显示



### 二、 logstash 过滤

修改/etc/logstash/conf.d/from\_beat.conf 添加Filter过滤



### 三、elasticsearch存储



### 四、kibana 显示

