# 环境

Java 1.8.0\_131 及以上

三个应用都用6.3.1版本

# Java 安装

## 查看是否安装java

yum list installed |grep java

## 卸载不要的版本

yum -y remove java-1.8.0-openjdk\*

## 查看可安装版本

yum -y list java\*

## 安装

yum install java-1.8.0-openjdk java-1.8.0-openjdk-devel 安装JDK,如果没有java-1.8.0-openjdk-devel就没有javac命令

### 实际执行

yum install -y java-1.8.0-openjdk.x86\_64

## 配置环境变量

通过yum默认安装的路径为  **/usr/lib/jvm**

export JAVA\_HOME=/usr/lib/jvm/jre-1.8.0-openjdk-1.8.0.171-8.b10.el7\_5.x86\_64(临时的)

针对用户的

vi /root/.bashrc

末尾添加

export JAVA\_HOME=/usr/lib/jvm/jre-1.8.0-openjdk-1.8.0.171-8.b10.el7\_5.x86\_64

全局写法所有人可用

vi /etc/profile

JAVA\_HOME=/usr/lib/jvm/jre-1.8.0-openjdk-1.8.0.171-8.b10.el7\_5.x86\_64

PATH=$PATH:$JAVA\_HOME/bin

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

export JAVA\_HOME  CLASSPATH  PATH

## 生效

source /etc/profile

## 检查

echo $JAVA\_HOME

echo $CLASSPATH

# Elasticsearch 安装

tar -xzf elasticsearch-6.3.1.tar.gz

cd elasticsearch-6.3.1/

## 关闭自动索引

[action.auto\_create\_index](https://www.elastic.co/guide/en/elasticsearch/reference/current/docs-index_.html" \l "index-creation" \o "Automatic Index Creationedit) in elasticsearch.yml 关闭自动索引

action.auto\_create\_index: .security,.monitoring\*,.watches,.triggered\_watches,.watcher-history\*,.ml\*

## 命令行启动

./bin/elasticsearch

## 关闭stdout

Ctrl-C.

## **检查是否运行**

config/elasticsearch.yml net

http://192.168.1.4:9200

## 静默模式运行

-q or --quiet(就不会打印)

## 后台运行

./elasticsearch -d

## Daemon方式运行

./bin/elasticsearch -d -p pid

$ES\_HOME/logs/

## 关闭

ps -ef | grep elastic

netstat -tunlp |grep 9200

kill -9 进程号

kill `cat pid`

## 配置

$ES\_HOME/config/elasticsearch.yml

## 命令行启动配置

./bin/elasticsearch -d -Ecluster.name=my\_cluster -Enode.name=node\_1

## 子节点配置

vim /etc/elasticsearch

cluster.name: aubin-cluster # 集群名称

node.name: els1 # 节点名称，仅仅是描述名称，用于在日志中区分

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

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

network.host: 192.168.0.1 # 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: ["172.18.68.11", "172.18.68.12","172.18.68.13"] # 集群个节点IP地址，也可以使用els、els.shuaiguoxia.com等名称，需要各节点能够解析

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

vim /etc/elasticsearch/jvm.options-Xms1g # JVM最大、最小使用内存-Xmx1g

systemctl enable elasticsearch.service

systemctl start elasticsearch

### 测试

Elasticsearch直接听过了http接口，所以直接使用curl命令就可以查看到一些集群相关的信息。

可以使用curl命令来获取集群的相关的信息，

\_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

curl -XGET 'http://192.168.1.2:9200/\_cat/nodes?pretty'

172.18.68.12 18 68 0 0.07 0.06 0.05 mdi - els2

172.18.68.13 25 67 0 0.01 0.02 0.05 mdi \* els3

# \*号表示为当前节点为主节点的意思

172.18.68.11 7 95 0 0.02 0.04 0.05 mdi - els1

如果你要想查看更多有关于集群信息、当前节点统计信息等等，可以使用一下命令来获取到所有可以查看的信息。

curl -XGET 'http://192.168.1.2:9200/\_cat?pretty'

## 问题

### 1、can not run elasticsearch as root

#### 创建elsearch用户组及elsearch用户

groupadd elsearch

useradd elsearch -g elsearch -p elasticsearch

#### 更改elasticsearch文件夹及内部文件的所属用户及组为elsearch:elsearch

chown -R elsearch:elsearch elasticsearch-6.3.1

#### 切换到elsearch用户再启动

su elsearch

cd elasticsearch/bin

./elasticsearch

### 错误: 找不到或无法加载主类 org.elasticsearch.tools.launchers.JavaVersionChecker

mv elasticsearch-6.3.1 /usr/share/elasticsearch

### java.lang.IllegalStateException: failed to obtain node locks, tried [[/usr/share/elasticsearch/data/elasticsearch]] with lock id [0]; maybe these locations are not writable or multiple nodes were started without increasing [node.max\_local\_storage\_nodes]

rm -rf data/nodes/0/node.lock

外网访问

vim config/elasticsearch.yml

增加：network.host: 0.0.0.0

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

elasticsearch用户拥有的可创建文件描述的权限太低，至少需要65536；

解决办法：

#切换到root用户修改

vim /etc/security/limits.conf

# 在最后面追加下面内容

\*\*\* hard nofile 65536

\*\*\* soft nofile 65536

\*\*\*  是启动ES的用户

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

解决办法：   
1、切换到root用户修改配置sysctl.conf

vi /etc/sysctl.conf

添加下面配置：

vm.max\_map\_count=655360

并执行命令：

sysctl -p

# Logstash 安装

tar -xzf logstash-6.3.1.tar.gz

cd logstash-6.3.1

## 基本运行

./bin/logstash &

bin/logstash -e 'input { stdin { } } output { stdout {} }'

## 安装Filebeat

docker pull docker.elastic.co/beats/filebeat:6.3.1

### yml方式安装

### 下载公钥

sudo rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

### 创建源

/etc/yum.repos.d/ elastic.repo

[elastic-6.x]

name=Elastic repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

### 安装

sudo yum install -y filebeat

### 配置自动启动

sudo chkconfig --add filebeat

## 配置Filebeat

/etc/filebeat/filebeat.yml

Docker 在/usr/share/filebeat/filebeat.yml

filebeat.yml中定义日志路径

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/\*.log

也剋以这么匹配

/var/log/\*/\*.log

//设置kibana主机地址

setup.kibana:

host: "192.168.1.4:5601"

//开启kibana的仪表盘

setup.dashboards.enabled: true

### 输出到elasticsearch

output.elasticsearch:

hosts: ["192.168.1.4:9200"]

//使用kibana仪表盘提供的例子

setup.kibana:

host: "192.168.1.4:5601"

### X-Pack

<https://www.elastic.co/guide/en/beats/filebeat/6.3/securing-filebeat.html>

（安全配置）

//角色定义json格式

{

"run\_as": [ ... ], IMG_256

"cluster": [ ... ], IMG_257

"indices": [ ... ] IMG_258

}

## 配置filebeat 使用 logstash

//这是输出到logstash的 （2选1 与output.elasticsearch:

）

output.logstash:

hosts: ["127.0.0.1:5044"]

## 在elasticsearch中定义索引模板

(定义setings 和mappings 如何分析)

链接上elasticsearch后自动载入模板，如果已经存在不会主动覆写

可以关闭自动加载，或加载自己的模板或修改模板的名字

输出到logstash的要手动加载

载入指定的模板

setup.template.name: "your\_template\_name"

setup.template.fields: "path/to/fields.yml"

配置是否覆盖已经存在的模板

setup.template.overwrite: true

关闭自动载入

setup.template.enabled: false

## 配置kibana仪表盘

可以命令行, 也可以在filebeat.yml配置

启动kibana后 shell执行

filebeat setup --dashboards

docker方式

docker run docker.elastic.co/beats/filebeat:6.3.1 setup --dashboards

## Logstash输出配置仪表盘

**Rpm:**

filebeat setup -e \

-E output.logstash.enabled=false \

-E output.elasticsearch.hosts=['localhost:9200'] \

-E output.elasticsearch.username=filebeat\_internal \

-E output.elasticsearch.password=YOUR\_PASSWORD \

-E setup.kibana.host=localhost:5601

**docker:**

docker run docker.elastic.co/beats/filebeat:6.3.1 setup -e \

-E output.logstash.enabled=false \

-E output.elasticsearch.hosts=['localhost:9200'] \

-E output.elasticsearch.username=filebeat\_internal \

-E output.elasticsearch.password=YOUR\_PASSWORD \

-E setup.kibana.host=localhost:5601

## 启动filebeat

**rpm:**

sudo service filebeat start

**docker:**

docker run docker.elastic.co/beats/filebeat:6.3.1

# Kibana 安装

tar -xzf kibana-6.3.1-linux-x86\_64.tar.gz

cd kibana-6.3.1-linux-x86\_64/

wget https://artifacts.elastic.co/downloads/kibana/kibana-6.3.1-darwin-x86\_64.tar.gz

tar -xzf kibana-6.3.1-darwin-x86\_64.tar.gz

cd kibana-6.3.1-darwin-x86\_64/

## 运行

./bin/kibana & (后台运行)

ctrl + c 关闭标准输出

## 配置

$KIBANA\_HOME/config/kibana.yml

server.port: 5601

server.host: "192.168.1.4"

elasticsearch.url: "http://192.168.1.4:9200"

## 查看状态

<http://192.168.1.4:9200/status>

## 使用

### 定义索引模式

Management->Index Patterns