# 安装elasticsearch

1. 上传压缩包解压到/usr/local/elasticsearch-6.2.4；
2. 创建用户组：groupadd elasticsearch；
3. 创建用户加入用户组：useradd elasticsearch -g elasticsearch；

4. 设置ElasticSerach文件夹为用户elasticsearch所有：chown -R elasticsearch.elasticsearch /usr/local/zcx/elasticsearch-6.2.4；

5.vim /etc/sysctl.conf

文件中追加一行

vm.max\_map\_count = 655360

1. sudo sysctl -p
2. vim /etc/security/limits.conf

添加如下内容:   
elasticsearch soft memlock unlimited   
elasticsearch hard memlock unlimited

1. 安装完成配置文件

主节点：

cluster.name: es\_dev

node.name: node-1

#如果是master节点设置成true 如果是

node.master: true

#如果是data节点设置成true

node.data: true

network.host: 127.0.0.1

http.port: 9200

transport.tcp.port: 9300

discovery.zen.ping.unicast.hosts: ["127.0.0.1:9300", "127.0.0.1:9301","127.0.0.1:9302"]

discovery.zen.minimum\_master\_nodes: 1

bootstrap.memory\_lock: true

bootstrap.system\_call\_filter: false

http.cors.enabled: true

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

数据节点：

cluster.name: es\_dev

node.name: node-2

#如果是master节点设置成true 如果是

node.master: false

#如果是data节点设置成true

node.data: true

network.host: 127.0.0.1

http.port: 9201

transport.tcp.port: 9301

discovery.zen.ping.unicast.hosts: ["127.0.0.1:9300","127.0.0.1:9301","127.0.0.1:9302"]

discovery.zen.minimum\_master\_nodes: 1

bootstrap.memory\_lock: true

bootstrap.system\_call\_filter: false

http.cors.enabled: true

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

安装完成

su elasticsearch

cd usr/local/elasticsearch-6.2.4-2\bin

nohup ./elasticsearch &

# Logstash安装

1. 上传压缩包解压到/usr/local/logstash-6.2.4；
2. cd /usr/local/logstash-6.2.4/bin

logstash-plugin install logstash-filter-multiline

1. 配置文件：

cd /usr/local/logstash-6.2.4/bin

vim logstash.conf

添加以下配置：

input {

file {

path => "D:/temp/logs/card-manager.log"

add\_field => {"system"=>"card-manager"}

add\_field => {"ip"=>"10.150.200.193"}

#codec=> multiline {

# pattern => "^\[CCM"

# negate => true

# what => "previous"

# }

}

}

#logstash-plugin install logstash-filter-multiline需要安装插件

filter{

multiline {

#根据不同系统添加不同的正则匹配

pattern => "^\[CCM"

negate => true

what => "previous"

}

}

output {

elasticsearch {

hosts => ["127.0.0.1:9200","127.0.0.1:9201"]

index => "logstash-card-manager-%{+YYYY-MM-dd}"

#用户必须是elastic用户[其他用户无权限]

user => "elastic"

password => "MoDctDHCM1cWHFLNKcU6"

}

}

logstash.yml

增加配置项：

xpack.monitoring.elasticsearch.username: logstash\_system

xpack.monitoring.elasticsearch.password: rsWRrzsMM3OQQpYOmOOD

保存

vim run.sh

nohup ./logstash -f logstash.conf &

保存

chmod -R 777 run.sh

# KIBANA安装

1. 上传压缩包解压到

/usr/local/kibana-6.2.4-linux-x86\_64；

1. 配置文件

cd /usr/local/kibana-6.2.4-linux-x86\_64/config

vim kibana.yml

添加以下配置文件：

server.port: 5601

server.host: "127.0.0.1"

elasticsearch.url: "http://127.0.0.1:9200"

#x-pack安全插件

elasticsearch.username: "elastic"

elasticsearch.password: "MoDctDHCM1cWHFLNKcU6"

1. 启动

cd /usr/local/kibana-6.2.4-linux-x86\_64/bin

nohup ./kibana &

exit;

登录使用elastic用户登录[其他用户看不到推送的log]

X-PACK安装

./bin/elasticsearch-plugin install x-pack

./bin/kibana-plugin install x-pack

logstash-plugin install x-pack

生成用户名密码

\bin\x-pack>setup-passwords auto

本地密码：

Changed password for user kibana

PASSWORD kibana = kVdAZ5A3dHgFiRwx03f4

Changed password for user logstash\_system

PASSWORD logstash\_system = rsWRrzsMM3OQQpYOmOOD

Changed password for user elastic

PASSWORD elastic = MoDctDHCM1cWHFLNKcU6

删除索引命令：

curl -XDELETE 'http://host.IP.address:9200/logstash-\*'

# 四、KAFKA安装

/bin/kafka-server-start.sh –daemon config/server.properties

kafka-server-start.bat –daemon ../../config/server.properties