### Elastic\_Stack操作手册

**前言：**

1.蓝色字体表示命令行命令，正式执行时不要复制前面的#号，#号只是提示应该使用root权限操作

2.绿色字体表示注释，有时注释太多就不用绿色表示了

3.注意：本文档的所有操作请先在测环境进行实践，请不要直接在真实的服务器中操作！

**版权声明**：

本文档以开源的形式发布，所有条款如下：

 （1）无担保：作者不保证文档内容的准确无误，亦不承担由于使用此文档所导致的任何后果

 （2）自由使用：任何人可以出于任何目的而自由地 阅读/链接/打印/转载/引用/分发/再创作 此文档，无需任何附加条件

若您 阅读/链接/打印/转载/引用/分发/再创作 本文档，则说明接受以上2个条款。

作者：李茂福

更新日期：2024-01-15

**★第1章、安装Elastic Stack**

ELK是三个开源项目的首字母缩写：Elasticsearch、Logstash 和 Kibana

在ELK这个生态圈的发展过程中，加入了一个新成员Beats，然后就更名为Elastic Stack

各组件功能说明

|  |  |
| --- | --- |
| Elasticsearch | 是一个搜索和分析引擎 |
| Logstash | 是服务器端数据处理管道，能够同时从多个来源采集数据，转换数据，然后将数据发送到诸如 Elasticsearch 等“存储库”中 |
| Kibana | 可以让用户在 Elasticsearch 中使用图形和图表对数据进行可视化 |
| Beats | 是负责单一用途数据采集并推送给Logstash或Elasticsearch的轻量级产品采集一切数据：日志文件，网络流量，服务指标，win事件日志，健康检查。收集到的数据发给Elastiscsearch或Logstash |

**★Elasticsearch部署**

Elasticsearch是用Java开发的基于Lucene（一个搜索引擎）的搜索服务器，提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口。

ELK下载地址： https://www.elastic.co/downloads

ElasticSearch下载： https://www.elastic.co/downloads/elasticsearch

**★下载安装包到服务器上并解压**

# tar -xf elasticsearch-8.11.3-linux-x86\_64.tar.gz -C /usr/local/

elaticsearch默认不能用root用户启动，所以会报java.lang.RuntimeException: can not run elasticsearch as root异常。

为elaticsearch创建用户并赋予相应权限：

# useradd es

# chown -R es:es /usr/local/elasticsearch-8.11.3

# CA证书 /usr/local/elasticsearch-8.11.3/config/certs/http\_ca.crt

# su es -c "/usr/local/elasticsearch-8.11.3/bin/elasticsearch" & #以es用户身份运行elasticsearch程序

**★重置elastic密码**

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-reset-password -u elastic

This tool will reset the password of the [elastic] user to an autogenerated value.

The password will be printed in the console.

Please confirm that you would like to continue [y/N]y #输入y

Password for the [elastic] user successfully reset.

New value: MsMZCFmb34aiamjv4SGz

# curl -k https://10.99.1.233:9200/ -u elastic:MsMZCFmb34aiamjv4SGz #查看es集群状态信息



# curl -k -u elastic:MsMZCFmb34aiamjv4SGz https://10.99.1.233:9200/\_cat/nodes?v #查看集群节点

ip heap.percent ram.percent cpu load\_1m load\_5m load\_15m node.role master name

127.0.0.1 21 94 5 0.04 0.26 0.18 cdfhilmrstw \* elk.cof-lee.com

# curl -k -u elastic:MsMZCFmb34aiamjv4SGz https://10.99.1.233:9200/\_cat/allocation?v #验证集群磁盘分配情况

shards disk.indices disk.used disk.avail disk.total disk.percent host ip node

 1 18.2kb 4.2gb 12.6gb 16.9gb 25 127.0.0.1 127.0.0.1 elk.cof-lee.com

# curl -k -u elastic:MsMZCFmb34aiamjv4SGz https://10.99.1.233:9200/\_cat/health?v #验证集群健康状况



# curl -k -u elastic:MsMZCFmb34aiamjv4SGz https://10.99.1.233:9200/\_cat/indices?v #查看集群的索引数

health status index uuid pri rep docs.count docs.deleted store.size pri.store.size dataset.size

# cat > /usr/local/elasticsearch-8.11.3/config/elasticsearch.yml <<EOF

#默认配置：

xpack.security.enabled: true

xpack.security.enrollment.enabled: true

xpack.security.http.ssl:

 enabled: true

 keystore.path: certs/http.p12

xpack.security.transport.ssl:

 enabled: true

 verification\_mode: certificate

 keystore.path: certs/transport.p12

 truststore.path: certs/transport.p12

cluster.initial\_master\_nodes: ["elk.cof-lee.com"]

http.host: 0.0.0.0

#允许跨域访问：

http.cors.enabled: true

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

#其他配置：

cluster.name: es-cluster1

node.name: elk.cof-lee.com

http.port: 9200

node.roles: [data,master]

action.destructive\_requires\_name: false

#启用系统索引自动创建

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

EOF

# cat >> /etc/hosts <<EOF

10.99.1.233 elk.cof-lee.com es-cluster1

EOF

# firewall-cmd --add-port=9200/tcp

# firewall-cmd --runtime-to-permanent

**重启elasticsearch**

★创建elasticsearch用户：

默认已创建好3个用户：elastic logstash\_system kibana\_system

执行下面对应命令，重置密码（密码自动生成）

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-reset-password -u 用户名

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-reset-password -u logstash\_system

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-reset-password -u kibana\_system # =oki6w=D\_Nk+29wWcQqg

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-users useradd cof #创建一个名为cof的es用户

Enter new password:

Retype new password:

赋角色权限

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-users roles -a superuser cof #超级管理员角色

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-users roles -a kibana\_system cof #kibana的用户角色

# /usr/local/elasticsearch-8.11.3/bin/elasticsearch-users roles -a logstash\_system cof #logstash的用户角色

★浏览器访问elasticsearch

https://10.99.1.233:9200/



用户名：elastic

密码：MsMZCFmb34aiamjv4SGz

显示以下信息表示可正常访问



**★kibana部署**

kibana下载地址： https://www.elastic.co/downloads/kibana

**★下载安装包到服务器上并解压**

# tar -xf kibana-8.11.3-linux-x86\_64.tar.gz -C /usr/local/

# cat > /usr/local/kibana-8.11.3/config/kibana.yml <<EOF

server.port: 5601 #配置监听端口号，默认5601

server.host: "0.0.0.0" #配置IP，建议设置0.0.0.0，方便访问

elasticsearch.hosts: ["https://10.99.1.233:9200"]

i18n.locale: "zh-CN" #默认是英文，这个是中文设置

elasticsearch.username: "kibana\_system"

elasticsearch.password: "=oki6w=D\_Nk+29wWcQqg"

#server.ssl.enabled: true

elasticsearch.ssl.verificationMode: none # 有四种模式，分别是full，strict，certificate和none

#certificate模式进行认证，即只认证CA证书，不认证主机名信息

EOF

# useradd kibana

# chown -R kibana:kibana /usr/local/kibana-8.11.3

# cd /usr/local/kibana-8.11.3/

# su kibana -c "/usr/local/kibana-8.11.3/bin/kibana" & #启动kibana服务进程

FATAL Error: [config validation of [elasticsearch].username]: value of "elastic" is forbidden. This is a superuser account that cannot write to system indices that Kibana needs to function. Use a service account token instead.

# firewall-cmd --add-port=5601/tcp

# firewall-cmd --runtime-to-permanent

★浏览器访问kibana

http://10.99.1.233:5601/







**★fliebeat部署**

下载地址： https://www.elastic.co/downloads/beats/filebeat

**★下载安装包到服务器上并解压**

# tar -xf filebeat-8.11.3-linux-x86\_64.tar.gz -C /usr/local/

# cd /usr/local/filebeat-8.11.3-linux-x86\_64/

#查看elasticsearch的ca证书指纹（也叫序列号）

# openssl x509 -text -noout -in /usr/local/elasticsearch-8.11.3/config/certs/http\_ca.crt

Certificate:

 Data:

 Version: 3 (0x2)

 Serial Number:

 a8:61:04:3c:52:41:d1:b8:b2:17:fc:26:1f:e0:fa:4a:79:91:aa:5a

 Signature Algorithm: sha256WithRSAEncryption

 Issuer: CN = Elasticsearch security auto-configuration HTTP CA

# cat > /usr/local/filebeat-8.11.3-linux-x86\_64/filebeat.yml <<EOF

output.elasticsearch:

 hosts: ["https://elk.cof-lee.com:9200"]

 username: "elastic"

 password: "MsMZCFmb34aiamjv4SGz"

 # If using Elasticsearch's default certificate，去除冒号

 ssl.ca\_trusted\_fingerprint: "a861043c5241d1b8b217fc261fe0fa4a7991aa5a"

setup.kibana:

 host: "http://elk.cof-lee.com:5601"

EOF

# /usr/local/filebeat-8.11.3-linux-x86\_64/filebeat setup

# /usr/local/filebeat-8.11.3-linux-x86\_64/filebeat -e -c /usr/local/filebeat-8.11.3-linux-x86\_64/filebeat.yml