

**EasticSearch原生部署手册**

版本号V1.0



**2025-05-27**

广州云趣信息科技有限公司

广东省广州市天河区建工路4号

【 历次版本修订记录，版本修订描述重要说明】

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 提交日期 | 版本号 | 版本修订内容描述 | 修改人 | 备注 |
| 20250527 | V1.0 | 首次发布 | 雷思思 |  |

目录

[1. 声明 4](#_Toc12896)

[1.1. 关于版权 4](#_Toc9284)

[1.2. 阅读约定 5](#_Toc670)

[2. 手册说明 6](#_Toc27499)

[3. ElasticSearch单机部署 6](#_Toc1445)

[3.1. 安装包获取 6](#_Toc22660)

[3.2. 安装方法 6](#_Toc23792)

[3.3. 单机配置 7](#_Toc29567)

[3.4. 启动ES 9](#_Toc13197)

[3.5. 查看日志 9](#_Toc23205)

[3.6. 常用操作 10](#_Toc6214)

[4. ElasticSearch集群部署 11](#_Toc19608)

[4.1. 安装包获取 11](#_Toc5681)

[4.2. 安装方法 11](#_Toc15145)

[4.3. 集群配置 12](#_Toc26277)

[4.4. 启动ES 14](#_Toc30199)

[4.5. 常用操作 14](#_Toc12256)

# 声明

## 关于版权

广州云趣信息科技有限公司版权所有，受中国及其他国家商业法律及版权法保护，保留一切权利。未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

我们尽力保证本文档的完整性和准确性，但不排除文档中有错误存在。广州云趣信息科技有限公司有权在不通知您的情况下更改此文档。

、“YQ”、“yunqu”均为广州云趣信息科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。如需要获取最新手册，请登录http://www.yunqu-info.com。

## 阅读约定

|  |  |
| --- | --- |
| **格式** | **意义** |
| **加粗字体** | 手册中，所有加粗的正文字体均表示关键字段。 |
| **红色字体** | 手册中，所有红色显示字体，均表示需要重点、需要特别关注的字段。 |
| **< >** | 手册中，所有带“< >”均表示按钮名，如“单击<确定> 按钮”。 |
| **[ ]** | 带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。 |
| **/** | 多级菜单及并行选项用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。 |

# 手册说明

ARM指令集下麒麟系统/X86架构，ElasticSearch的原生部署文档

# ElasticSearch单机部署

## 安装包获取

登录SVN版本服务器下载：取对应系统版本

http://version.yunqu-info.com/!/#version/view/head/4#--产品项目/4.5#--智能化产品安装包/第三方工具/ElasticSearch

## 安装方法

1. 优化好操作系统后，再增加下面步骤

echo 'vm.max\_map\_count = 262144' >> /etc/sysctl.conf

reboot

1. 创建elasticsearch专用账号，因为不能root启动

groupadd elastic

useradd -g elastic elastic

passwd elastic 输入两次密码

1. 解压程序包，假设es根目录为/home/yq/es/elasticsearch-7.9.3/

cd /home/yq/es 放入elasticsearch-7.9.3-linux-x86\_64.tar.gz

tar -zxvf elasticsearch-7.9.3-linux-x86\_64.tar.gz

1. 创建存放数据目录

mkdir /home/yq/es/elasticsearch-7.9.3/data

1. 改变es目录拥有者账号

chown -R elastic:elastic /home/yq/es/elasticsearch-7.9.3

su elastic 至此后续，都用 elastic 用户来操作

## 单机配置

3.3.1编辑elasticsearch.yml

vim /home/yq/es/elasticsearch-7.9.3/config/elasticsearch.yml

找到下面的行进行修改或添加

# 集群名称，默认

cluster.name: my-application

# 节点名称，可任意设置

node.name: node-1

node.attr.rack: r1

# ES数据所在路径

path.data: /home/yq/es/elasticsearch-7.9.3/data

# ES日志所在路径

path.logs: /home/yq/es/elasticsearch-7.9.3/logs

# 绑定主机地址，默认localhost

network.host: 172.16.80.147

# HTTP 服务端口，默认为9200

http.port: 9200

#配置为本机ip

discovery.seed\_hosts: ["172.16.80.147"]

# 配置为节点名称候选列表

确定长期使用单节点可以移除该参数，再新增discovery.type: single-node

cluster.initial\_master\_nodes: ["node-1" ]

# 单节点集群发现模式，自动选举自己为主节点，若后续改用集群，需移除该参数

# discovery.type: single-node

#否启用跨域资源共享(CORS)

http.cors.enabled: true

#允许的CORS来源

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

#是否锁定JVM内存(防止交换)

bootstrap.memory\_lock: false

# 启用安全功能，启用后需要输入密码才能访问ES（如不启用安全功能，则将下面行都注释；**以下配置为没有证书，生成自签名证书的方式**）

xpack.security.enabled: true

xpack.security.transport.ssl.enabled: true

xpack.security.transport.ssl.keystore.type: PKCS12

xpack.security.transport.ssl.verification\_mode: certificate

xpack.security.transport.ssl.keystore.path: elastic-certificates.p12

xpack.security.transport.ssl.truststore.path: elastic-certificates.p12

3.3.2按需修改jvm.options内存设置

# vim /home/yq/es/elasticsearch-7.9.3/config/jvm.options

根据实际情况修改占用内存，默认都是1G，单机1G内存，启动会占用700m+， 内存设置超出物理内存，也会无法启动，启动报错

-Xms2g

-Xmx2g

两个参数设置成一样，为内存大小，建议设置4g

3.3.3设置 elastic 用户启动密码

如在elasticsearch.yml中启用了安全功能，则需要执行以下步骤（否则跳过）

1、设置 elastic 用户启动密码（再次执行可覆盖密码）：

/home/yq/es/elasticsearch-7.9.3/bin/elasticsearch-keystore add bootstrap.password

2、执行后系统会提示你输入密码：

Enter value for bootstrap.password:

输入想设置的密码（可与创建的es账号使用同一密码），比如：

Yunqu168

**生成自签名证书（如果没有证书）**

3、进入 Elasticsearch 安装目录的 bin 文件夹

cd /home/yq/es/elasticsearch-7.9.3/bin/

4、生成 CA 和节点证书

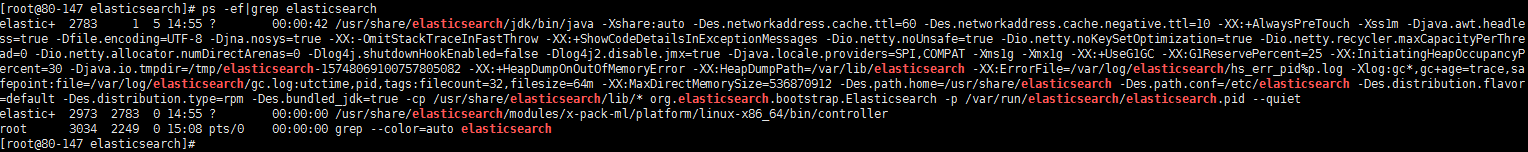
./elasticsearch-certutil cert -out config/elastic-certificates.p12 -pass ""

## 启动ES

/home/yq/es/elasticsearch-7.9.3/bin/elasticsearch -d

启动后可查看elasticsearch进程是否存在

ps -ef|grep elasticsearch



通过以下命令测试连接：

curl -k -u elastic http://ip:9200/\_cluster/health?pretty



## 查看日志

tail -200 /var/log/elasticsearch/my-application.log

若无异常报错输出，浏览器访问验证服务

http://172.16.80.147:9200/

输入用户名跟密码进行登录



因没有接入kibana 可视化，当前登录后只会返回ES节点相关信息



## 常用操作

查看接口监听

netstat -tlunp |grep 9200

查看集群健康状态

curl -k -u elastic http://172.16.80.147:9200/\_cluster/health?pretty

查看索引列表

curl -k -u elastic http://172.16.80.147:9200/\_cat/indices?v

# ElasticSearch集群部署

## 安装包获取

登录SVN版本服务器下载：取对应系统版本

http://version.yunqu-info.com/!/#version/view/head/4#--产品项目/4.5#--智能化产品安装包/第三方工具/ElasticSearch

## 安装方法

1、ElasticSearch引擎最新集群本地方式，部署步骤(3台机器)

部署前要先规划好服务器，例如：

192.168.100.111:9200 node-1 r1

192.168.100.112:9200 node-2 r2

192.168.100.113:9200 node-3 r3

2、部署之前，还是照常使用一体化安装包，优化好操作系统后，再增加下面步骤

echo 'vm.max\_map\_count = 262144' >> /etc/sysctl.conf

reboot

3、创建elasticsearch专用账号，因为不能root启动

groupadd elastic

useradd -g elastic elastic

passwd elastic 输入两次密码

4、解压程序包(三台机器都操作)

cd /home/yq/es

放入elasticsearch-7.9.3-linux-x86\_64.tar.gz

tar -zxvf elasticsearch-7.9.3-linux-x86\_64.tar.gz

5、创建存放数据目录

mkdir /home/yq/es/elasticsearch-7.9.3/data

6、改变es目录拥有者账号

chown -R elastic:elastic /home/yq/es/elasticsearch-7.9.3

su elastic 至此后续，都用 elastic 用户来操作

## 集群配置

4.3.1编辑elasticsearch.yml（三台机器都操作）

vim /home/yq/es/elasticsearch-7.9.3/config/elasticsearch.yml

找到下面的行进行修改或添加

# 集群名称，默认

cluster.name: my-application

# 节点名称，可任意设置

node.name: node-1 （每台的值都不能一样：node-1 node-2 node-3）

node.attr.rack: r1 （每台的值都不能一样：r1 r2 r3）

# ES数据所在路径

path.data: /home/yq/es/elasticsearch-7.9.3/data

# ES日志所在路径

path.logs: /home/yq/es/elasticsearch-7.9.3/logs

# 绑定主机地址，默认localhost

network.host: 192.168.100.111 （这个值每台都不能一样，配置为本机ip）

# HTTP 服务端口，默认为9200

http.port: 9200

#配置为三台机器的ip，这个值三台机器的配置都要保持一致

discovery.seed\_hosts: ["192.168.100.111","192.168.100.112","192.168.100.113"]

# 配置为节点名称候选列表，这个值三台机器的配置都要保持一致

cluster.initial\_master\_nodes: ["node-1","node-2","node-3"]

# 集群恢复前需要加入的节点数

gateway.recover\_after\_data\_nodes: 3

# 开启安全功能以及证书配置，参考提供的elasticsearch.yml文件，最后9行

4.3.2按需修改jvm.options内存设置

# vim /home/yq/es/elasticsearch-7.9.3/config/jvm.options

根据实际情况修改占用内存，默认都是1G，单机1G内存，启动会占用700m+， 内存设置超出物理内存，也会无法启动，启动报错

-Xms2g

-Xmx2g

两个参数设置成一样，为内存大小，建议设置4g

4.3.3配置elasticsearch集群的安全性（在第一台上操作就行）

1. 创建SSL证书目录：

mkdir /home/yq/es/elasticsearch-7.9.3/config/certs/

1. 创建SSL证书

/home/yq/es/elasticsearch-7.9.3/bin/elasticsearch-certutil ca

第一次输入：/home/yq/es/elasticsearch-7.9.3/config/certs/elastic-stack-ca.p12

第二次输入：直接按回车键

/home/yq/es/elasticsearch-7.9.3/bin/elasticsearch-certutil cert --ca /home/yq/es/elasticsearch-7.9.3/config/certs/elastic-stack-ca.p12

第一次输入：直接按回车键

第二次输入：/home/yq/es/elasticsearch-7.9.3/config/certs/elastic-certificates.p12

第三次输入：直接按回车键

1. 同步SSL证书到另外2台服务器

scp -rp /home/yq/es/elasticsearch-7.9.3/config/certs [root@192.168.100.112:/home/yq/es/elasticsearch-7.9.3/config/](mailto:root@192.168.100.112:/home/yq/es/elasticsearch-7.9.3/config/)

1. (三台机器都操作)给SSL证书赋权

chown -R elastic:elastic /home/yq/es/elasticsearch-7.9.3/config/certs

## 启动ES

1、(三台机器都操作)正式启动elasticsearch集群

/home/yq/es/elasticsearch-7.9.3/bin/elasticsearch -d

2、启动后可查看elasticsearch进程是否存在

ps -ef|grep elasticsearch

3、修改elasticsearch集群相关用户的密码(在第一台上操作就行)

/home/yq/es/elasticsearch-7.9.3/bin/elasticsearch-setup-passwords interactive 输入y，按回车，然后提示密码时输入想要设置的密码

## 常用操作

1、(随便一台操作)测试elasticsearch集群是否正常(IP地址换成想要测试的那台，密码换成你设置的那个)

1、查看集群信息

curl -XGET -u elastic:yunqu168 '192.168.100.111:9200/\_cat/health?v'

2、查询所有索引

curl -XGET -u elastic:yunqu168 '192.168.100.112:9200/\_cat/indices?v'

3、查询所有用户

curl -XGET -u elastic:yunqu168 '192.168.100.113:9200/\_security/user?pretty' |grep 'username'