



链滴

# ES 服务部署

作者: [qifu](#)

原文链接: <https://ld246.com/article/1606360401088>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

# 服务器设置

编辑 /etc/sysctl.conf

```
vm.max_map_count=262144
vm.swappiness=1
```

配置生效: `sysctl -p`

## 单节点

单节点适用于测试环境，没有做数据持久化。这里的镜像统一采用7.8.0，注意es的版本与kibana的本保持一致。

前提：安装好docker

```
docker create --network host --name elasticsearch -e discovery.type=single-node -v /etc/localtime:/etc/localtime --restart always elasticsearch:7.8.0
```

```
docker start elasticsearch
```

## 多节点

前提：安装好docker,docker-compose

服务器内存：最好16g或者32g,cpu: 4h或者8h

服务器磁盘：不要采用nas,最好是SSD.磁盘大小根据业务量，建议至少1t+，提前做好监控和扩

。

```
创建文件夹： mkdir /ELASTIC
               touch docker-compose.yml
               vi docker-compose.yml
```

```
version: '2.2'
services:
  es01:
    image: docker.elastic.co/elasticsearch/elasticsearch:7.8.0
    container_name: es01
    environment:
      - node.name=es01
      - cluster.name=es-docker-cluster
      - discovery.seed_hosts=es02,es03
      - cluster.initial_master_nodes=es01,es02,es03
      - bootstrap.memory_lock=true
      - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
    ulimits:
      memlock:
        soft: -1
        hard: -1
    volumes:
      - data01:/usr/share/elasticsearch/data
```

```
ports:
  - 9200:9200
networks:
  - elastic
es02:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.8.0
  container_name: es02
  environment:
    - node.name=es02
    - cluster.name=es-docker-cluster
    - discovery.seed_hosts=es01,es03
    - cluster.initial_master_nodes=es01,es02,es03
    - bootstrap.memory_lock=true
    - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
  ulimits:
    memlock:
      soft: -1
      hard: -1
  volumes:
    - data02:/usr/share/elasticsearch/data
  networks:
    - elastic
es03:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.8.0
  container_name: es03
  environment:
    - node.name=es03
    - cluster.name=es-docker-cluster
    - discovery.seed_hosts=es01,es02
    - cluster.initial_master_nodes=es01,es02,es03
    - bootstrap.memory_lock=true
    - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
  ulimits:
    memlock:
      soft: -1
      hard: -1
  volumes:
    - data03:/usr/share/elasticsearch/data
  networks:
    - elastic

volumes:
  data01:
    driver: local
  data02:
    driver: local
  data03:
    driver: local

networks:
  elastic:
    driver: bridge
```

镜像源在国外，所以拉取会比较慢

## 设置容器日志清理脚本

```
#!/bin/sh

echo "当前容器日志大小"
find /var/lib/docker/containers -type f -name "*.log" -exec ls -lh {} \;
echo "5s后开始清空，取消请ctrl+c"
sleep 5
echo "清空容器日志中"
for i in `find /var/lib/docker/containers -type f -name "*.log"`; do cat /dev/null >$i; done
sleep 3
echo "清空后容器日志大小"
find /var/lib/docker/containers -type f -name "*.log" -exec ls -lh {} \;
sleep 3
echo "完成"

chmod +x /data/clearlog.sh

echo '0 3 * * * root /data/clearlog.sh' >> /etc/crontab
```

## 旧数据索引

删除索引就能删除数据

例 选择删除一个索引：  
curl -XDELETE "127.0.0.1:9211/zhongtaifluentd-20200723"

查看集群的健康状态：  
curl 'localhost:9211/\_cat/health?v'

查看所有索引：  
curl 'localhost:9212/\_cat/indices?v'

设置只保留近一周的索引

```
#!/bin/bash
# @Author: richard
# @Date: 2017-08-11 17:27:49
# @Last Modified by: richard
# @Last Modified time: 2017-08-11 18:04:58

time=$(date -d '-7days' +%Y%m%d)
curl -XDELETE http://127.0.0.1:9211/*-${time}

chmod +x /data/deleteins.sh

echo '0 3 * * * root /data/deleteins.sh' >> /etc/crontab
```