# 0.介绍

elk（Elasticsearch、LogStash、Kinana）可以用来搭建集中的日志处理系统。

<https://elasticsearch.cn/download/>

# 1.安装

## 1.1.解压方式

### 1.1.1. 解压

tar -xvf elasticsearch-7.7.0-linux-x86\_64.tar.gzip

# 2.运行

## 2.1. 执行运行命令

./bin/elasticsearch

## 2.2. 执行验证命令

curl http://localhost:9200

## 2.3. 配置外网可访问

vi /config/elasticsearch.yml

network.host: ${外网ip} 如172.18.194.140

node.name: node-1 #配置节点在集群中的名称

cluster.initial\_master\_nodes: ["node-1"] #配置集群中的节点（目前单机）

重新运行elasticsearch。

浏览器访问enjoy-elk.com:9200 #enjoy-clk.com域名与network.host配置的ip对应。