# 官网

https://www.elastic.co/cn/

# 下载地址

https://www.elastic.co/cn/downloads/elasticsearch

# 版本

最新版本：8.6.2

# 基本概念

Elasticsearch 是一个分布式、RESTful 风格的搜索和数据分析引擎，能够解决不断涌现出的各种用例。作为 Elastic Stack 的核心，它集中存储您的数据，帮助您发现意料之中以及意料之外的情况。

ElasticSearch 是基于 Lucene 的搜索服务器。它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。Elasticsearch 是用 Java 开发的，并作为 Apache 许可条款下的开放源码，是当前流行的企业级搜索引擎。

## 集群（cluster）

一个Elasticsearch集群由一个或多个ES节点组成，并提供集群内所有节点的联合索引和搜索能力（所有节点共同存储数据）。一个集群被命名为唯一的名字（默认为elasticsearch），集群名称非常重要，因为节点需要通过集群的名称加入集群。请确保在不同的环境使用不同的集群名称，否则会导致节点添加到错误的集群中。

## 节点（node）

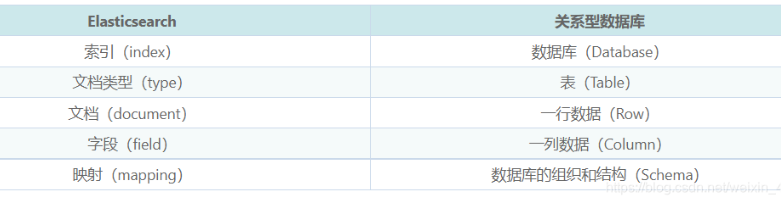
一个节点是集群中的一个服务器，用来存储数据并参与集群的索引和搜索。和集群类似，节点由一个名称来标识，默认情况下，该名称是在节点启动时分配给节点的随机通用唯一标识符（UUID）。您也可以自定义任意节点的名称，节点名称对于管理工作很重要，因为通过节点名称可以确定网络中的哪些服务器对应于Elasticsearch集群中的哪些节点。

一个节点可以被添加到指定名称的集群中。默认情况下，每个节点会被设置加入到名称为elasticsearch的集群中，这意味着，如果在您在网络中启动了某些节点（假设这些节点可以发现彼此），它们会自动形成并加入名称为elasticsearch的集群中。

一个集群可以拥有任意多的节点。此外，如果在您的网络中没有运行任何Elasticsearch节点，此时启动一个节点会创建一个名称为elasticsearch的单节点集群。

## 索引（index）

一个索引是一个拥有一些相似特征的文档的集合（相当于关系型数据库中的一个数据库）。例如，您可以拥有一个客户数据的索引，一个商品目录的索引，以及一个订单数据的索引。一个索引通常使用一个名称（所有字母必须小写）来标识，当针对这个索引的文档执行索引、搜索、更新和删除操作的时候，这个名称被用来指向索引。 Elasticsearch与关系型数据库的对应关系：



## 类型（type）

一个类型通常是一个索引的一个逻辑分类或分区，允许在一个索引下存储不同类型的文档（相当于关系型数据库中的一张表），例如用户类型、博客类型等。目前已经不支持在一个索引下创建多个类型，并且类型概念已经在后续版本中删除，详情请参见es官方文档。

## 文档（document）

一个文档是可以被索引的基本信息单元（相当于关系型数据库中的一行数据）。例如，您可以为一个客户创建一个文档，或者为一个商品创建一个文档。文档可以用JSON格式来表示。在一个索引中，您可以存储任意多的文档，且文档必须被索引.

## 字段（field）

组成文档的最小单位。相当于关系型数据库中的一列数据。

## 分片

## 映射（mapping）

用来定义一个文档以及其所包含的字段如何被存储和索引，例如在mapping中定义字段的名称和类型，以及所使用的分词器。相当于关系型数据库中的Schema。 分片（shards） 代表索引分片，Elasticsearch可以把一个完整的索引分成多个分片，这样的好处是可以把一个大的索引拆分成多个，分布到不同的节点上，构成分布式搜索。分片的数量只能在索引创建前指定，并且索引创建后不能更改。

一个分片可以是主分片或副本分片。Elasticsearch 7.0以下版本默认为一个索引创建5个主分片，并分别为每个主分片创建1个副本分片，7.0及以上版本默认创建1个主分片和1个副本分片。两者区别如下：



## recovery

代表数据恢复或数据重新分布，Elasticsearch在有节点加入或退出时会根据机器的负载对索引分片进行重新分配，挂掉的节点重新启动时也会进行数据恢复。

## gateway

代表Elasticsearch索引快照的存储方式，Elasticsearch默认优先将索引存放到内存中，当内存满时再将这些索引持久化存储至本地硬盘。gateway对索引快照进行存储，当这个Elasticsearch集群关闭再重新启动时就会从gateway中读取索引备份数据。Elasticsearch支持多种类型的gateway，有本地文件系统（默认）、分布式文件系统、Hadoop的HDFS和阿里云的OSS云存储服务。

## discovery.zen

代表Elasticsearch的自动发现节点机制，Elasticsearch是一个基于p2p的系统，它先通过广播寻找存在的节点，再通过多播协议进行节点之间的通信，同时也支持点对点的交互。

## Transport

Transport代表Elasticsearch内部节点或集群与客户端的交互方式，默认使用TCP协议进行交互。同时，通过插件的方式集成，也支持使用HTTP协议（JSON格式）、thrift、servlet、memcached、zeroMQ等传输协议进行交互。

# 特点

1、分布式的实时文件存储，每个字段都被索引且可用于搜索。

2、分布式的实时分析搜索引擎，海量数据下近实时秒级响应。

3、简单的 restful api，天生的兼容多语言开发。

4、易扩展，处理 PB 级结构化或非结构化数据。

# 应用场景

## 1、全文搜索

Elasticsearch提供了全文搜索的功能，适用于电商商品搜索、App搜索、企业内部信息搜索、IT系统搜索等。例如当您运营一个提供客户检索商品的在线电子商城的时候，可以使用Elasticsearch来存储整个商品的目录和库存，并且为客户提供检索和自动推荐的功能。

## 2、日志分析

复杂的业务场景通常会产生繁杂多样的日志，如Apache Log、System Log、MySQL Log等，往往很难从繁杂的日志中获取价值，却要承担其存储的成本。Elasticsearch能够借助Beats、Logstash等快速对接各种常见的数据源，并通过集成的Kibana高效地完成日志的可视化分析，让日志产生价值。

## 3、运维监控

当您在ECS或者物理机中部署了Docker容器、MySQL或MongoDB等数据库，或者您有复杂的IOT场景等，可使用Elasticsearch结合Beats、Logstash或ElasticFlow将所有日志实时集中并构建索引，然后通过集成的Kibana灵活地运用数据构建可视化运维看板，并在看板上展示主机名称、IP地址、部署情况、显示颜色等信息。

## 4、安全分析

当您需要通过日志解决公司内部繁杂的安全审计工作，可通过Elasticsearch分析、检索海量历史日志，高效地完成安全审计工作。同时您可以借助Elasticsearch的数据响应性能，快速感知系统中实时发生的事件，及时帮助您规避风险。

# 安装 Easticsearch 需要依赖什么组件吗

ES 早期版本需要JDK，在 7.X 版本后已经集成了 JDK，已无需第三方依赖。

# windows安装教程

## 1、下载es

## 2、安装elasticsearch

安装elasticsearch之前，需要安装好jdk并配置好环境变量。要注意的是，最近版本的elasticsearch所需的jdk版本至少在1.8以上。下载好压缩包后，直接解压后即可使用，无需其他配置。

## 3、启动elasticsearch

打开bin目录，双击elasticsearch.bat即可启动，出现如下：



即表明成功启动，要保证该窗口一直运行。如果一切正常，默认会在9200端口运行，打开浏览器输入默认的地址http://localhost:9200/ 即可得到说明信息：

图形用户界面, 文本, 应用程序

描述已自动生成

## 4、出现错误的解决方法

### 1、received plaintext http traffic on an https channel, closing connection Netty4HttpChannel [2022-02-16T21:08:50,085][WARN ][o.e.x.s.t.n.SecurityNetty4HttpServerTransport] [DESKTOP-VCT39JM] received plaintext http traffic on an https channel, closing connection Netty4HttpChannel{localAddress=/[0:0:0:0:0:0:0:1]:9200, remoteAddress=/[0:0:0:0:0:0:0:1]:1172}

解决方法：是因为开启了 ssl 认证。在 ES/config/elasticsearch.yml 文件中把 xpack.security.http.ssl:enabled 设置成 false 即可。

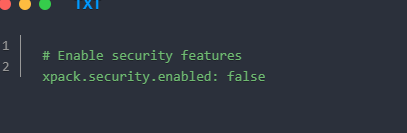


### 2、elasticsearch 账号密码

windows 下直接启动 ElasticSearch ，见到 started 为成功启动，访问 htttp://localhost:9200 需要输入密码，是因为开启了密码验证模式。找了一轮没看到有账号密码，干脆就设置免密登录就好。

解决方法：

找到 elasticsearch.yml 文件， 把 xpack.security.enabled 属性设置为 false 即可。



### 3、设置内存大小

ES 的内存是自己调节的。在 config/jvm.options 文件中直接设置就好(追加):

文本

中度可信度描述已自动生成

### 4、windows Could not rename log file ‘logs/gc.log’ to ‘logs/gc.log.14’ (Permission denied).

ES 在 windows 中只允许打开一个应用程序，当你再想去创建一个 ES 应用程序的时候，就会显示 Permission denied，即使是使用 cmd 管理员运行 elasticsearch.bat 文件也是一样的错误。

解决方法：注意查看是否已经在别的地方已经打开 ES 服务，实在不行则进行电脑重启。

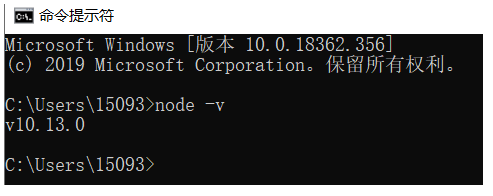
## 5、安装ElasticSearch-head插件

### （1）安装node环境

网址：<https://nodejs.org/en/download/>

下载Windows版msi的,下载完直接安装，一直确定。

安装完后cmd查看版本node -v



### （2）grunt

grunt是一个很方便的构建工具，可以进行打包压缩、测试、执行等等的工作，5.x里之后的head插件就是通过grunt启动的。因此需要安装grunt

npm install -g grunt-cli

查看版本号 grunt -version



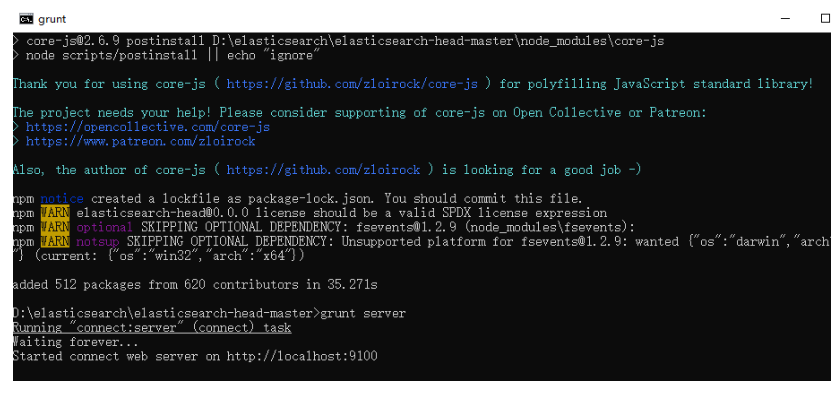
（3）下载head插件

1、网址:https://github.com/mobz/elasticsearch-head下载安装包

2、解压

3、进入head文件夹下，执行命令：npm install (此处是为安装进行安装pathomjs)

4、安装完成之后npm run start或grunt server,启动head插件



5、修改es使用的参数.编辑D:\elasticsearch\elasticsearch-7.3.2-windows-x86\_64\elasticsearch-7.3.2\config\elasticsearch.yml文件

图形用户界面, 应用程序, 表格

描述已自动生成

文本

描述已自动生成

文本

描述已自动生成

6、修改完配置将es重启,浏览器访问 [http://localhost:9100](http://localhost:9100/)

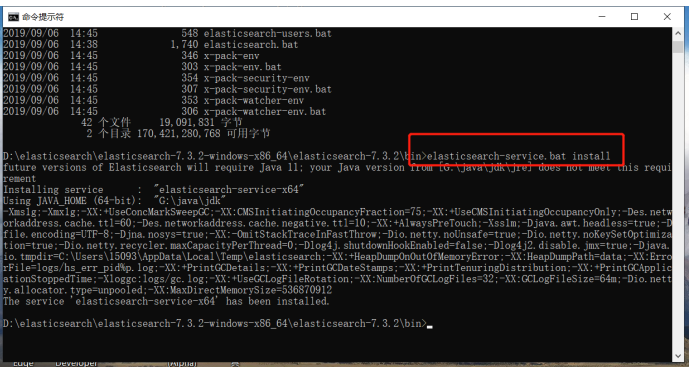
图形用户界面, 文本, 应用程序

描述已自动生成

## ElasticSearch安装为Windows服务

1、elasticsearch的bin目录下有一个elasticsearch-service.bat

2、md 进入bin目录下执行: elasticsearch-service.bat install



3、查看电脑服务es已经存在了

图形用户界面, 文本, 应用程序

描述已自动生成

文本, 信件

描述已自动生成

# 解释一下Easticsearch Cluster

Elasticsearch 集群是一组连接在一起的一个或多个 Elasticsearch 节点实例。Elasticsearch 集群的功能在于在集群中的所有节点之间分配任务，进行搜索和建立索引。

# 解释一下Elasticsearch Node

节点是 Elasticsearch 的实例。实际业务中，我们会说: ES 集群包含 3 个节点7 个节点。这里节点实际就是:一个独立的 Elasticsearch 进程，一般将一个节点部署到-台独立的服务器或者虚拟机、容器中。

不同节点根据角色不同，可以划分为 :

主节点：

帮助配置和管理在整个集群中添加和删除节点

数据节点：

存储数据并执行诸如 CRUD (创建/读取/更新/删除)作，对数据进行搜索和聚合的操作。

1、客户端节点(或者说: 协调节点)将集群请求转发到主节点，将与数据相关的请求转发到数据节点。

2、摄取节点

用于在索引之前对文档进行预处理。