# 【ELK：开源搜索与分析技术栈】

## 主要内容

1. Elasticsearch简介
2. Linux安装Elasticsearch
3. 常用Elasticsearch管理操作
4. 常用元数据简介
5. 分词器和标准化处理
6. Elasticsearch中的mapping问题
7. Search搜索详解
8. Spring Data Elasticsearch
9. Logstash

## 学习目标

|  |  |
| --- | --- |
| 知识点 | 要求 |
| Elasticsearch简介 | 掌握 |
| Linx安装Elasticsearch | 掌握 |
| 常用Elasticsearch管理操作 | 掌握 |
| 常用元数据简介 | 掌握 |
| 分词器和标准化处理 | 掌握 |
| Elasticsearch中的mapping问题 | 掌握 |
| Search搜索详解 | 掌握 |
| Spring Data Elasticsearch | 掌握 |
| Logstash | 掌握 |

## ELK

Elasticsearch官网中提供了很多技术，其中一些技术是可以配合使用的，里面比较出名的就是ELK技术栈。

ELK是Elasticsearch、Logstash、Kibana三个软件首字母。

Elasticsearch： 全文检索工具。

Kibana：页面管理工具。可以通过Kibana的管理界面操作Elasticsearch

Logstash：日志收集的工具，通过此工具可以实现日志内容收集及格式转换。

## Elasticsearch简介

Elasticsearch是一个基于Lucene的搜索服务器。它提供了一个分布式的全文搜索引擎，其对外服务是基于RESTful web接口发布的。Elasticsearch是用Java开发的应用，并作为Apache许可条款下的开放源码发布，是当前流行的企业级搜索引擎。设计用于云计算中，能够达到近实时搜索，稳定，可靠，快速，安装使用方便。

### 功能分类

Elasticsearch具备两个主要功能：

搜索。功能和Solr类似。代替目前（海量数据）的MySQL模糊查询。

分析。结合LogStash使用。

### 相关概念

#### cluster

集群。Elasticsearch集群由一或多个节点组成，其中有一个主节点，这个主节点是可以通过选举产生的，主从节点是对于集群内部来说的。Elasticsearch的一个概念就是去中心化，字面上理解就是无中心节点，这是对于集群外部来说的，因为从外部看Elasticsearch集群，在逻辑上是个整体，你与集群中的任何一个节点通信和与整个Elasticsearch集群通信是等价的。也就是说，主节点的存在不会产生单点安全隐患、并发访问瓶颈等问题。

#### Index

索引。相当于关系型数据库中的表。其中存储若干相似结构的Document数据。如：客户索引，订单索引，商品索引等。Elasticsearch中的索引不像数据库表格一样有强制的数据结构约束，在理论上，可以存储任意结构的数据。但了为更好的为业务提供搜索数据支撑，还是要设计合适的索引体系来存储不同的数据。

#### shards

primary shard：代表索引的主分片，Elasticsearch可以把一个完整的索引分成多个primary shard，这样的好处是可以把一个大的索引拆分成多个分片，分布存储在不同的Elasticsearch节点上，从而形成分布式存储，并为搜索访问提供分布式服务，提高并发处理能。primary shard的数量只能在索引创建时指定，并且索引创建后不能再更改primary shard数量。

#### replicas

replica shard：代表索引主分片的副本，Elasticsearch可以设置多个replica shard。replica shard的作用：一是提高系统的容错性，当某个节点某个primary shard损坏或丢失时可以从副本中恢复。二是提高Elasticsearch的查询效率，Elasticsearch会自动对搜索请求进行负载均衡，将并发的搜索请求发送给合适的节点，增强并发处理能力。

#### Type

类型。每个索引中都必须有唯一的一个Type，Type是Index中的一个逻辑分类。Elasticsearch中的数据Document是存储在索引下的Type中的。

注意：Elasticsearch5.x及更低版本中，一个Index中可以有多个Type。Elasticsearch6.x版本之后，type概念被弱化，一个index中只能有唯一的一个type。且在7.x版本之后，删除type定义。

#### Document

文档。Elasticsearch中的最小数据单元。一个Document就是一条数据，一般使用JSON数据结构表示。每个Index下的Type中都可以存储多个Document。一个Document中可定义多个field，field就是数据字段。如：学生数据（{"name":"张三", "age":20, "gender":"男"}）。

#### 元数据

在Elasticsearch中所有以“\_”开头的属性都成为元数据，都有着自己特定的含义。

例如:\_index:表示索引

#### 倒排索引（Elasticsearch搜索原理，面试题）反向索引

对数据进行分析，抽取出数据中的词条，以词条作为key，对应数据的存储位置作为value，实现索引的存储。这种索引称为倒排索引。倒排索引是Document写入Elasticsearch时分析维护的。

如：

|  |  |  |
| --- | --- | --- |
| 数据 | | |
| 商品主键 | 商品名 | 商品描述 |
| 1 | 荣耀10 | 更贵的手机 |
| 2 | 荣耀8 | 相对便宜的手机 |
| 3 | IPHONE X | 要卖肾买的手机 |

|  |  |
| --- | --- |
| 分析结果、倒排索引 | |
| 词条 | 数据 |
| 手机 | 1，2，3 |
| 便宜 | 2 |
| 卖肾 | 3 |
| 相对 | 2 |
| 荣耀 | 1，2 |
| IPHONE | 3 |

### Elasticsearch常见使用场景

维基百科：全文检索，高亮显示，搜索推荐

The Guardian（国外的一个新闻网站），此平台可以对用户的行为（点击、浏览、收藏、评论）、社区网络数据（对新闻的评论等）进行数据分析，为新闻的发布者提供相关的公众反馈。

Stack Overflow（国外的程序异常讨论论坛）

Github（开源代码管理），在千亿级别的代码行中搜索信息

电子商务平台等。

## Linux安装Elasticsearch

使用的Elasticsearch的版本是7.6.2。Elasticsearch7.x要求Linux内核必须是4+版本以上。

在linux操作系统中，查看内核版本的命令是： uname -a

课堂使用的Linux是CentOS8。内核使用的是4.18。

### 基于Docker安装

#### 安装Elasticsearch

##### 拉取Elasticsearch镜像

如果docker还没有开启。需要先开始docker软件

|  |
| --- |
| systemctl start docker |

拉取Elasticsearch镜像

|  |
| --- |
| docker pull elasticsearch:7.6.2 |

##### 创建并启动容器

--name 名字为elasticsearch

-d 后台启动

-p 端口号。9200restful访问端口，9300为java代码访问端口

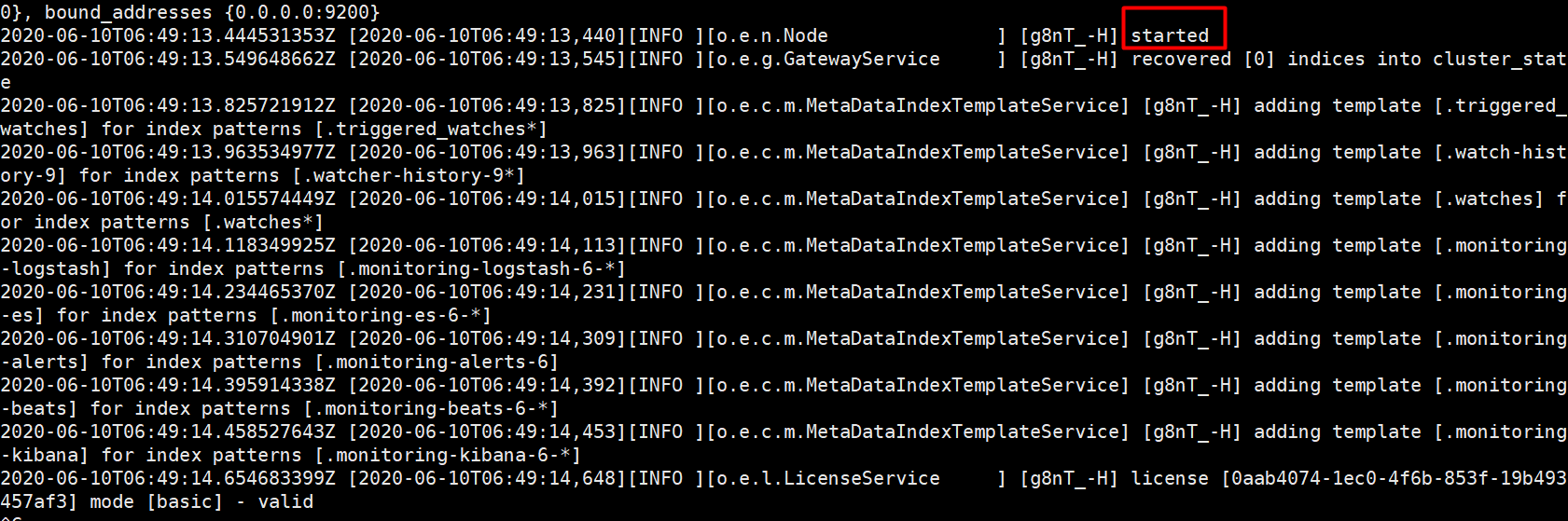
discovery.type=single-node 集群模式：单机版

|  |
| --- |
| docker run --name elasticsearch -d -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" elasticsearch:7.6.2 |

##### 查看日志

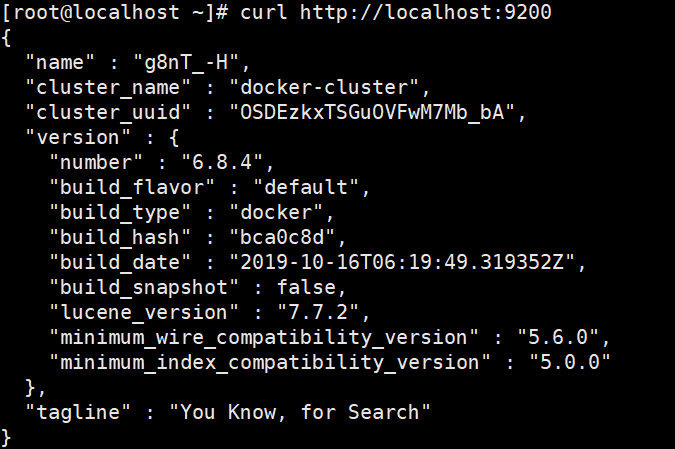
|  |
| --- |
| docker logs -f elasticsearch |

如果日志中出现started状态，说明启动成功



##### 测试结果

|  |
| --- |
| curl http://localhost:9200 |



#### 基于Docker的Kibana

Kibana的版本必须和ES的版本对应。

##### 拉取镜像

|  |
| --- |
| docker pull kibana:7.6.2 |

##### 新建并启动容器

192.168.8.137 Docker所在服务器的IP

--link elasticsearch:elasticsearch 中第一个elasticsearch是容器名，第二个elasticsearch是容器别名。设置link后才能让容器互通。

|  |
| --- |
| docker run -d --name kibana --link elasticsearch:elasticsearch -p 5601:5601 kibana:7.6.2 |

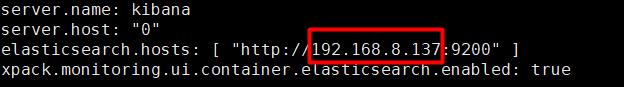
##### 修改Kibana参数

# docker exec -it kibana /bin/bash

# cd config

# vi kibana.yml

选中部分修改成Docker的IP

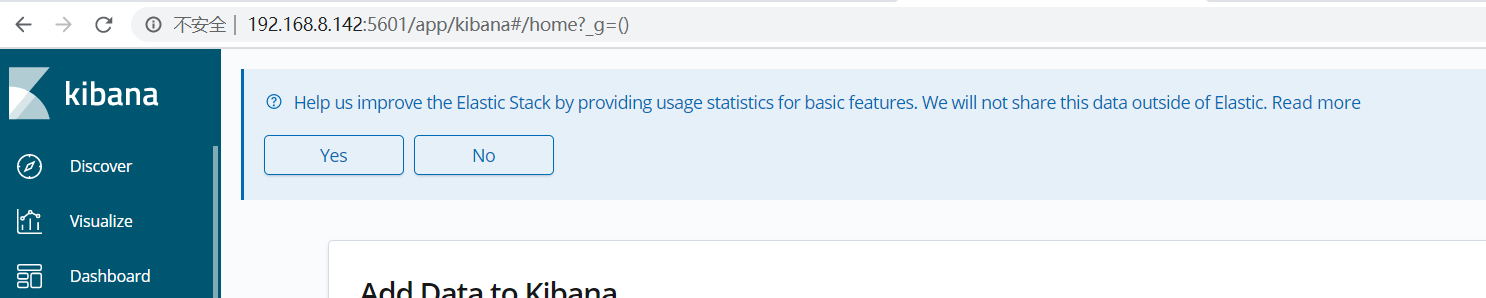


重启docker容器

# docker restart kibana

##### 访问

在浏览器输入 [http://192.168.8.137:5601](http://192.168.8.142:5601)



## 常用Elasticsearch管理操作

### 查看健康状态

?v表示带有标题头

GET \_cat/health?v

|  |
| --- |
| Epoch（编号） timestamp（时间戳） cluster（集群名称） status（健康状态） node.total（节点总数） node.data（数据节点数） shards（分片数）  1531290005 14:20:05 Elasticsearch green 1 1 2  Pri（主分片数量） relo（备份节点） init（正在初始化的） unassign（未分配的） pending\_tasks（正在等待执行的任务）  2 0 0 0 0  max\_task\_wait\_time（挂起任务的等待时间） active\_shards\_percent（活动的分片的占有百分比）  - 100.0% |

status：green、yellow、red

green：每个索引的primary shard和replica shard都是active的

yellow：每个索引的primary shard都是active的，但部分的replica shard不是active的

red：不是所有的索引的primary shard都是active状态的。

### 查看节点信息

GET /\_cat/nodes?v

|  |
| --- |
| ip heap.percent ram.percent cpu load\_1m load\_5m load\_15m node.role master name  172.17.0.4 10 90 1 0.00 0.00 0.00 dilm \* bb883a561e42 |

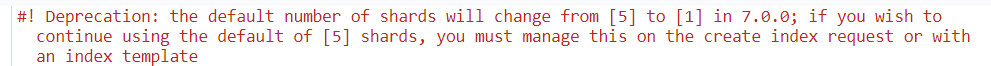
### 创建索引

命令语法：PUT 索引名{索引配置参数}

index名称必须是小写的，且不能以下划线'\_'，'-'，'+'开头。

在Elasticsearch6.x及更早版本中，默认的创建索引的时候，会分配5个primary shard，并为每个primary shard分配一个replica shard。ElasticSearch7.x版本中，默认创建索引时，分配1个primary shard，每个primary shard分配一个replica shard。在Elasticsearch中，默认的限制是：如果磁盘空间不足15%的时候，不分配replica shard。如果磁盘空间不足5%的时候，不再分配任何的primary shard。Elasticsearch中对shard的分布是有要求的。Elasticsearch尽可能保证primary shard平均分布在多个节点上。Replica shard会保证不和他备份的那个primary shard分配在同一个节点上。

创建默认索引。默认索引在7版本之前是5个，到7.x之后改成1个。一个主分片一个副本分片。



PUT test\_index1

GET \_cat/indices 查看所有索引

GET \_cat/shards 查看所有分片

#### 创建索引时指定分片

注意： 编写时大括号要和put命令等不在一行。重点不能把{放在索引名后，kibana会把{当成索引名的一部分。

PUT test\_index2

{

"settings":{

"number\_of\_shards" : 2,

"number\_of\_replicas" : 1

}

}

解释说明：

number\_of\_shards:主分片数量

number\_of\_relicas:每个主分片的副本分片数量。

### 修改索引

命令语法：PUT 索引名/\_settings{索引配置参数}

注意：索引一旦创建，primary shard数量不可变化，可以改变replica shard数量。

PUT test\_index2/\_settings

{

"number\_of\_replicas" : 2

}

### 删除索引

命令语法：DELETE 索引名1[, 索引名2 ...]

DELETE test\_index1

### 查看索引详情

GET /索引名称

GET /first\_index

### 查看索引信息

GET \_cat/indices?v

|  |
| --- |
| health status index uuid pri rep docs.count  yellow open test\_index 2PJFQBtzTwOUhcy-QjfYmQ 5 1 0  docs.deleted store.size pri.store.size  0 460b 460b |

### 检查分片信息

查看索引的shard信息。

GET \_cat/shards?v

|  |
| --- |
| index shard prirep state docs store ip node  test\_index2 1 p STARTED 0 261b 192.168.89.142 mN\_pylT  test\_index2 1 r UNASSIGNED  test\_index2 1 r UNASSIGNED  test\_index2 0 p STARTED 0 261b 192.168.89.142 mN\_pylT  test\_index2 0 r UNASSIGNED  test\_index2 0 r UNASSIGNED |

### 新增Document

在索引中增加文档。在index中增加document。

Elasticsearch有自动识别机制。如果增加的document对应的index不存在，自动创建index；如果index存在，type不存在，则自动创建type。如果index和type都存在，则使用现有的index和type。

#### PUT语法

此操作为手工指定id的Document新增方式。

语法：

PUT 索引名/\_doc/唯一ID{字段名:字段值} #如果不存在新增，如果存在全量替换

PUT 索引名/\_create/ID # 强制新增。如果不存在新增，如果存在报错。

如：

|  |
| --- |
| put index\_test/\_doc/1  {  "name":"李四",  "address":"北京亦庄"  }  put index\_test/\_create/2  {  "field1":"属性1",  "field2":"属性2"  } |

结果：

|  |
| --- |
| {  "\_index": "test\_index", 新增的document在什么index中，  "\_type": "test\_type", 新增的document在index中的哪一个type中。  "\_id": "1", 指定的id是多少  "\_version": 1, document的版本是多少，版本从1开始递增，每次写操作都会+1  "result": "created", 本次操作的结果，created创建，updated修改，deleted删除  "\_shards": { 分片信息  "total": 2, 分片数量只提示primary shard  "successful": 1, 数据document一定只存放在index中的某一个primary shard中  "failed": 0  },  "\_seq\_no": 0, 执行的序列号  "\_primary\_term": 1 词条比对。  } |

如果使用PUT语法对同id的Document执行多次操作。是一种覆盖操作（全量替换）。如果需要Elasticsearch辅助检查PUT的Document是否已存在，可以使用强制新增语法。使用强制新增语法时，如果Document的id在Elasticsearch中已存在，则会报错。（version conflict, document already exists）

#### POST语法

POST允许主键自动生成方式。

此操作为Elasticsearch自动生成id的新增Document方式。

语法：

POST 索引名/ID # 虽然在此处指定ID值，但是ID依然自动生成。

POST 索引名/\_doc

如：

|  |
| --- |
| post index\_test/1  {  "name":"张三",  "age":12  }  post index\_test/\_doc  {  "name":"王五",  "age":13  } |

### 查询Document

#### GET ID单数据查询

语法：GET 索引名/\_doc/唯一ID

如：

GET test\_index/\_doc/1

结果：

|  |
| --- |
| {  "\_index": "test\_index",  "\_type": "test\_type",  "\_id": "1",  "\_version": 1,  "found": true,  "\_source": { 找到的document数据内容。  "name": "test\_doc\_01",  "remark": "first test elastic search",  "order\_no":1  }  } |

#### GET \_mget批量查询

批量查询可以提高查询效率。推荐使用（相对于单数据查询来说）。

语法如下：

|  |
| --- |
| get index\_test/\_mget  {  "docs":[  {  "\_id":1  },  {  "\_id":2  }  ]  } |

#### 查询全部

查询全部语法

GET 索引名/\_search

### 修改Document

#### 替换Document（全量替换）

和新增的PUT语法是一致。

PUT 索引名/\_doc/唯一ID{字段名:字段值}

本操作相当于覆盖操作。全量替换的过程中，Elasticsearch不会真的修改Document中的数据，而是标记Elasticsearch中原有的Document为deleted状态，再创建一个新的Document来存储数据，当Elasticsearch中的数据量过大时，Elasticsearch后台回收deleted状态的Document。

如：

|  |
| --- |
| put index\_test/\_doc/1  {  "name":"测试"  } |

结果：

|  |
| --- |
| {  "\_index": "test\_index",  "\_type": "test\_type",  "\_id": "1",  "\_version": 2,  "result": "updated",  "\_shards": {  "total": 2,  "successful": 1,  "failed": 0  },  "\_seq\_no": 1,  "\_primary\_term": 1  } |

#### 更新Document（partial update）

语法：POST 索引名/\_update/唯一ID{doc:{字段名:字段值}}

只更新某Document中的部分字段。这种更新方式也是标记原有数据为deleted状态，创建一个新的Document数据，将新的字段和未更新的原有字段组成这个新的Document，并创建。对比全量替换而言，只是操作上的方便，在底层执行上几乎没有区别。

如：

|  |
| --- |
| post index\_test/\_update/1  {  "doc":{  "address":"测试地址123",  "name":"111"  }  } |

结果：

|  |
| --- |
| {  "\_index": "test\_index",  "\_type": "test\_type",  "\_id": "1",  "\_version": 5,  "result": "updated",  "\_shards": {  "total": 2,  "successful": 1,  "failed": 0  },  "\_seq\_no": 2,  "\_primary\_term": 1  } |

### 删除Document

Elasticsearch中执行删除操作时，Elasticsearch先标记Document为deleted状态，而不是直接物理删除。当Elasticsearch存储空间不足或工作空闲时，才会执行物理删除操作。标记为deleted状态的数据不会被查询搜索到。

语法：DELETE 索引名/\_doc/唯一ID

如：

|  |
| --- |
| DELETE test\_index/\_doc/1 |

结果：

|  |
| --- |
| {  "\_index": "test\_index",  "\_type": "test\_type",  "\_id": "1",  "\_version": 6,  "result": "deleted",  "\_shards": {  "total": 2,  "successful": 1,  "failed": 0  },  "\_seq\_no": 5,  "\_primary\_term": 1  } |

### bulk批量增删改（重点记忆）

使用bulk语法执行批量增删改。语法格式如下：

注意：\_bulk的两个{}都不要出现换行等操作，两个{}使用回车符进行识别。

POST \_bulk

{ "action\_type" : { "metadata\_name" : "metadata\_value" } }

{ document datas | action datas }

语法中的action\_type可选值为：

create : 强制创建，相当于PUT 索引名/类型名/唯一ID/\_create。主键必须有。

index: 普通的POST操作，相当于创建Document或全量替换

update: 更新操作（partial update）,相当于 POST 索引名/类型名/唯一ID/\_update

delete: 删除操作

案例如下：

|  |
| --- |
| 新增数据：  POST \_bulk  { "create" : { "\_index" : "test\_index" , "\_id" : "1" } }  { "field\_name" : "field value" } |
| PUT操作新增或全量替换  POST \_bulk  { "index" : { "\_index" : "test\_index", "\_id" : "2" } }  { "field\_name" : "field value 2" } |
| POST更新数据  POST \_bulk  { "update" : { "\_index" : "test\_index", "\_id" : 2, "\_retry\_on\_conflict" : 3 } }  { "doc" : { "field\_name" : "partial update field value" } } |
| DELETE删除数据  POST \_bulk  { "delete" : { "\_index" : "test\_index", "\_id" : "2" } } |
| 批量写操作  post \_bulk  {"index":{"\_index":"index\_test","\_id":1}}  {"name":"批量新增name","address":"批量新增address"}  {"index":{"\_index":"index\_test","\_id":2}}  {"name":"批量新增name2","address":"批量新增address2"}  {"delete":{"\_index":"index\_test","\_id":1}}  {"update":{"\_index":"index\_test","\_id":2}}  {"doc":{"address":"批量新增address3"}} |

注意：bulk语法中要求一个完整的json串不能有换行。不同的json串必须使用换行分隔。多个操作中，如果有错误情况，不会影响到其他的操作，只会在批量操作返回结果中标记失败。bulk语法批量操作时，bulk request会一次性加载到内存中，如果请求数据量太大，性能反而下降（内存压力过高），需要反复尝试一个最佳的bulk request size。一般从1000~5000条数据开始尝试，逐渐增加。如果查看bulk request size的话，一般是5~15MB之间为好。

bulk语法要求json格式是为了对内存的方便管理，和尽可能降低内存的压力。如果json格式没有特殊的限制，Elasticsearch在解释bulk请求时，需要对任意格式的json进行解释处理，需要对bulk请求数据做json对象会json array对象的转化，那么内存的占用量至少翻倍，当请求量过大的时候，对内存的压力会直线上升，且需要jvm gc进程对垃圾数据做频繁回收，影响Elasticsearch效率。

生产环境中，bulk api常用。都是使用java代码实现循环操作。一般一次bulk请求，执行一种操作。如：批量新增10000条数据等。

## 分词器（analyzer）和标准化处理（normalization）

### Elasticsearch默认提供的常见分词器

要切分的语句：Set the shape to semi-transparent by calling set\_trans(5)

standard analyzer - 是Elasticsearch中的默认分词器。标准分词器，处理英语语法的分词器。切分后的key\_words：set, the, shape, to, semi, transparent, by, calling, set\_trans, 5。这种分词器也是Elasticsearch中默认的分词器。切分过程中不会忽略停止词（如：the、a、an等）。会进行单词的大小写转换、过滤连接符（-）或括号等常见符号。

GET \_analyze

{

"text": "Set the shape to semi-transparent by calling set\_trans(5)",

"analyzer": "standard"

}

simple analyzer - 简单分词器。切分后的key\_words：set, the, shape, to, semi, transparent, by, calling, set, trans。就是将数据切分成一个个的单词。使用较少，经常会破坏英语语法。

GET \_analyze

{

"text": "Set the shape to semi-transparent by calling set\_trans(5)",

"analyzer": "simple"

}

whitespace analyzer - 空白符分词器。切分后的key\_words：Set, the, shape, to, semi-transparent, by, calling, set\_trans(5)。就是根据空白符号切分数据。如：空格、制表符等。使用较少，经常会破坏英语语法。

GET \_analyze

{

"text": "Set the shape to semi-transparent by calling set\_trans(5)",

"analyzer": "whitespace"

}

language analyzer - 语言分词器，如英语分词器（english）等。切分后的key\_words：set, shape, semi, transpar, call, set\_tran, 5。根据英语语法分词，会忽略停止词、转换大小写、单复数转换、时态转换等，应用分词器分词功能类似standard analyzer。

GET \_analyze

{

"text": "Set the shape to semi-transparent by calling set\_trans(5)",

"analyzer": "english"

}

注意：Elasticsearch中提供的常用分词器都是英语相关的分词器，对中文的分词都是一字一词。

### 基于Docker安装中文分词器

#### 进入容器

|  |
| --- |
| docker exec -it es /bin/bash |

#### 安装IK

由于是从github上下载资源，所以耗时较长。

|  |
| --- |
| ./bin/elasticsearch-plugin install https://github.com/medcl/elasticsearch-analysis-ik/releases/download/v7.6.2/elasticsearch-analysis-ik-7.6.2.zip |

#### 重启容器

|  |
| --- |
| docker restart es |

#### 测试IK分词器

IK分词器提供了两种analyzer，分别是ik\_max\_word和ik\_smart。

ik\_max\_word: 会将文本做最细粒度的拆分，比如会将“中华人民共和国国歌”拆分为“中华人民共和国,中华人民,中华,华人,人民共和国,人民,人,民,共和国,共和,国,国歌”，会穷尽各种可能的组合；

ik\_smart: 会做最粗粒度的拆分，比如会将“中华人民共和国国歌”拆分为“中华人民共和国,国歌”。

|  |
| --- |
| GET \_analyze  {  "text" : "中华人民共和国国歌",  "analyzer": "ik\_max\_word"  }  GET \_analyze  {  "text" : "中华人民共和国国歌",  "analyzer": "ik\_smart"  } |

### 本地安装IK步骤

复制分词器压缩包到容器中。

docker cp elasticsearch-analysis-ik-7.6.2.zip es:/usr/share/elasticsearch/plugins

进入容器

docker exec -it es bash

进入plugins目录

cd /usr/share/elasticsearch/plugins

创建目录

mkdir ik

移动压缩包到目录中

mv elasticsearch-analysis-ik-7.6.2.zip ik/

解压缩

unzip elasticsearch-analysis-ik-7.6.2.zip

删除压缩包

rm -rf \*.zip

重启容器

docker restart es

### 配置词条

由于在容器内部直接vi时词条为乱码，所以需要在windows或linux中操作。

在压缩包中config目录中main.dic中配置需要配置的文字内容。

每个中文词语独占一行。

最简单方法：

在linux中/usr/local/es中直接操作main.dic，在此处操作成功后，容器内容跟随变化。

进入到容器内部后，直接进入/usr/shard/elasticsearch/plugins/ik/config 中

执行：

# cp /bjsxt/config/main.dic main.dic

# exit

# docker restart es

## Elasticsearch中的mapping问题

强调：

1. 类型必须记住。
2. text和keyword区别。
3. mapping一旦生效不允许修改。所以创建索引时直接指定mapping关系。

Mapping在Elasticsearch中是非常重要的一个概念。决定了一个index中的field使用什么数据格式存储，使用什么分词器解析，是否有子字段等。

为什么要学习Mapping？

如果没有mapping所有text类型属性默认都使用standard分词器。所以如果希望使用IK分词就必须配置自定义mapping。

### mapping核心数据类型

Elasticsearch中的数据类型有很多，在这里只介绍常用的数据类型。

**只有text类型才能被分词。其他类型不允许**。

文本（字符串）：text

整数：byte、short、integer、long

浮点型：float、double

布尔类型：boolean

日期类型：date

数组类型：array {a:[]}

对象类型：object {a:{}}

不分词的字符串（关键字）： keyword

### dynamic mapping对字段的类型分配

true or false -> boolean

123 -> long

123.123 -> float

"2018-01-01" "2018-01-01T00:00:00.000" -> date

"hello world" -> text

[] -> array

{} -> object

在上述的自动mapping字段类型分配的时候，只有text类型的字段需要分词器。默认分词器是standard分词器。

### 查看索引mapping

可以通过命令查看已有index的mapping具体信息，语法如下：

GET 索引名/\_mapping

如：

|  |
| --- |
| GET test\_index/\_mapping |

结果：

|  |
| --- |
| {  "test\_index": { # 索引名  "mappings": { # 映射列表  "test\_type": { # 类型名  "properties": { # 字段列表  "age": { # 字段名  "type": "long" # 字段类型  },  "gender": {  "type": "text",  "fields": { # 子字段列表  "keyword": { # 子字段名  "type": "keyword", # 子字段类型，keyword不进行分词处理的文本类型  "ignore\_above": 256 # 子字段存储数据长度  }  }  },  "name": {  "type": "text",  "fields": {  "keyword": {  "type": "keyword",  "ignore\_above": 256  }  }  }  }  }  }  }  } |

### custom mapping

可以通过命令，在创建index和type的时候来定制mapping映射，也就是指定字段的类型和字段数据使用的分词器。

手工定制mapping时，只能新增mapping设置，不能对已有的mapping进行修改。

如：有索引a，其中有类型b，增加字段f1的mapping定义。后续可以增加字段f2的mapping定义，但是不能修改f1字段的mapping定义。

通常都是手工创建index，并进行各种定义。如：settings,mapping等。

#### 创建索引时指定mapping

语法：

PUT 索引名称

{

"mappings":{

"properties":{

"字段名":{

"type":类型,

["analyzer":字段的分词器,]

["index":是否创建索引树,]

["fields":{

"子字段名称":{

"type":类型,

"ignore\_above":长度限制

}

}]

}

}

}

}

如：

|  |
| --- |
| put index\_demo  {  "mappings":{  "properties":{  "id":{  "type":"long",  "index":true  },  "title":{  "type":"text",  "index":true,  "analyzer":"ik\_max\_word"  },  "name":{  "type":"keyword"  }  }  }  } |

"index" - 是否可以作为搜索索引。可选值：true | false

"analyzer" - 指定分词器。

"type" - 指定字段类型

#### 为已有索引添加**新的字段mapping**

语法：

PUT 索引名/\_mapping

{

"properties":{

"新字段名":{

"type":类型,

"analyer":字段的分词器,

"fields":{

"子字段名":{

"type":类型,

"ignore\_above":长度

}

}

}

}

}

如：

|  |
| --- |
| put index\_demo/\_mapping  {  "properties":{  "address":{  "type":"text",  "analyzer":"ik\_max\_word"  }    }  } |

#### 测试不同的字段的分词器

语法：

GET 索引名称/\_analyze

{

"field":"索引中的text类型的字段名",

"text":"要分词处理的文本数据"

}

使用索引中的字段对应的分词器，对文本数据做分词处理。

如：

|  |
| --- |
| GET test\_index/\_analyze  {  "field": "new\_field",  "text": "中华人民共和国国歌"  }  GET /test\_index/\_analyze  {  "field": "content",  "text": "中华人民共和国国歌"  } |

## Search 搜索详解

### 搜索学习测试数据

|  |
| --- |
| PUT test\_search  {  "mappings": {  "properties": {  "dname" : {  "type" : "text",  "analyzer": "standard"  },  "ename" : {  "type" : "text",  "analyzer": "ik\_max\_word"  },  "eage" : {  "type": "long"  },  "hiredate" : {  "type": "date"  },  "gender" : {  "type" : "keyword"  }  }  }  }  POST test\_search/\_bulk  { "index": {}}  { "dname" : "Sales Department", "ename" : "张三", "eage":20, "hiredate" : "2019-01-01", "gender" : "男性" }  { "index": {}}  { "dname" : "Sales Department", "ename" : "李四", "eage":21, "hiredate" : "2019-02-01", "gender" : "男性" }  { "index": {}}  { "dname" : "Development Department", "ename" : "王五", "eage":23, "hiredate" : "2019-01-03", "gender" : "男性" }  { "index": {}}  { "dname" : "Development Department", "ename" : "赵六", "eage":26, "hiredate" : "2018-01-01", "gender" : "男性" }  { "index": {}}  { "dname" : "Development Department", "ename" : "韩梅梅", "eage":24, "hiredate" : "2019-03-01", "gender" : "女性" }  { "index": {}}  { "dname" : "Development Department", "ename" : "钱虹", "eage":29, "hiredate" : "2018-03-01", "gender" : "女性" } |

### query string search

search的参数都是类似http请求头中的字符串参数提供搜索条件的。

GET [/index\_name/]\_search[?parameter\_name=parameter\_value&...]

#### 全搜索

timeout参数：是超时时长定义。代表每个节点上的每个shard执行搜索时最多耗时多久。不会影响响应的正常返回。只会影响返回响应中的数据数量。

如：索引a中，有10亿数据。存储在5个shard中，假设每个shard中2亿数据，执行全数据搜索的时候，需要耗时1000毫秒。定义timeout为10毫秒，代表的是shard执行10毫秒，搜索出多少数据，直接返回。

在商业项目中，是禁止全数据搜索的。必须指定搜索的索引，类型和关键字。如果没有指定索引或类型，则代表开发目的不明确，需要重新做用例分析。如果没有关键字，称为索引内全搜索，也叫魔鬼搜索。

语法：

|  |
| --- |
| GET [索引名/类型名/]\_search?timeout=10ms |

结果：

|  |
| --- |
| {  "took": 144, #请求耗时多少毫秒  "timed\_out": false, #是否超时。默认情况下没有超时机制，也就是客户端等待Elasticsearch搜索结束（无论执行多久），提供超时机制的话，Elasticsearch则在指定时长内处理搜索，在指定时长结束的时候，将搜索的结果直接返回（无论是否搜索结束）。指定超时的方式是传递参数，参数单位是：毫秒-ms。秒-s。分钟-m。  "\_shards": {  "total": 1, #请求发送到多少个shard上  "successful": 1,#成功返回搜索结果的shard  "skipped": 0, #停止服务的shard  "failed": 0 #失败的shard  },  "hits": {  "total": 1, #返回了多少结果  "max\_score": 1, #搜索结果中，最大的相关度分数，相关度越大分数越高，\_score越大，排位越靠前。  "hits": [ #搜索到的结果集合，默认查询前10条数据。  {  "\_index": "test\_index", #数据所在索引  "\_type": "test\_type", #数据所在类型  "\_id": "1", #数据的id  "\_score": 1, #数据的搜索相关度分数  "\_source": { # 数据的具体内容。  "field": "value"  }  }  ]  }  } |

#### multi index搜索

所谓的multi-index就是从多个index中搜索数据。相对使用较少，只有在复合数据搜索的时候，可能出现。一般来说，如果真使用复合数据搜索，都会使用\_all。

如：搜索引擎中的无条件搜索。（现在的应用中都被屏蔽了。使用的是默认搜索条件，执行数据搜索。 如： 电商中的搜索框默认值， 搜索引擎中的类别）

无条件搜索，在搜索应用中称为“魔鬼搜索”，代表的是，搜索引擎会执行全数据检索，效率极低，且对资源有非常高的压力。

语法：

|  |
| --- |
| GET \_search  GET 索引名1,索引名2/\_search # 搜索多个index中的数据  GET 索引名/类型名/\_search # 所属一个index中type的数据  GET prefix\_\*/\_search # 通配符搜索  GET \*\_suffix/\_search  GET 索引名1,索引名2/类型名/\_search # 搜索多个index中type的数据  GET \_all/\_search # \_all代表所有的索引 |

|  |
| --- |
| GET 索引名/\_search?q=搜索条件 代表在所有的字段中搜索  GET 索引名/\_search?**q=**字段名:搜索条件  示例：get test\_search/test\_type/\_search?q=eage:26  对搜索条件为中文支持不友好。 |

#### 分页搜索

默认情况下，Elasticsearch搜索返回结果是10条数据。从第0条开始查询。

size和from是es中具有特定含义的属性名。

语法：

|  |
| --- |
| GET 索引名/\_search?size=10 # size查询数据的行数  GET 索引名/\_search?from=0&size=10 # from 从第几行开始查询，行号从0开始。 |

#### +/-搜索

语法：

|  |
| --- |
| GET 索引名/\_search?q=字段名:条件  GET 索引名/\_search?q=+字段名:条件  GET 索引名/\_search?q=-字段名:条件 |

+ ：和不定义符号含义一样，就是搜索指定的字段中包含key words的数据

- ： 与+符号含义相反，就是搜索指定的字段中不包含key words的数据

示例：

搜索dname中包含Sales单词的内容。dname使用standard分词器，会把内容进行拆分为单词。搜索Sales可以匹配到单词，但是搜索Sal是无法匹配到单词。

get test\_search/test\_type/\_search?q=+dname:Sales

#### **排序**

语法：GET 索引名/\_search?sort=字段名:排序规则

排序规则： asc(升序,默认) | desc(降序)

注意：text类型字段不可排序，因为倒排索引无法排序。

|  |
| --- |
| GET test\_search/\_search?sort=eage:asc  GET test\_search/\_search?sort=eage:desc |

### query DSL

DSL - Domain Specified Language ， 特殊领域的语言。

请求参数是请求体传递的。在Elasticsearch中，请求体的字符集默认为UTF-8。

语法格式：

GET 索引名/\_search

{

"command":{ "parameter\_name" : "parameter\_value"}

}

#### 查询所有数据

|  |
| --- |
| GET 索引名/\_search  {  "query" : { "match\_all" : {} }  } |

#### match search(项目搜索功能使用此命令)

全文检索。要求查询条件拆分后的任意词条与具体数据匹配就算搜索结果。

|  |
| --- |
| GET 索引名/\_search  {  "query": {  "match": {  "字段名": "搜索条件"  }  }  } |

#### phrase search

短语检索。要求查询条件必须和具体数据完全匹配才算搜索结果。其特征是：

1. 对搜索条件进行拆词
2. 把拆词当作一个整体，整体去索引（索引是存储内容被拆词后的结果）中匹配，必须严格匹配（存储内容拆词后是:北京，大兴，朝阳，条件拆词是：北京,朝阳。这种情况是不能被查询的，因为北京和朝阳之前还有大兴。）才能查询到

|  |
| --- |
| GET 索引名/\_search  {  "query": {  "match\_phrase": {  "字段名": "搜索条件"  }  }  } |

#### range

范围比较搜索

|  |
| --- |
| GET 索引名/类型名/\_search  {  "query" : {  "range" : {  "字段名" : {  "gt" : 搜索条件1,  "lte" : 搜索条件2  }  }  }  } |

#### 多条件复合搜索

在一个请求体中，有多个搜索条件，就是复合搜索。如：搜索数据，条件为部门名称是Sales Department，员工年龄在20到26之间，部门员工姓名叫张三。上述条件中，部门名称为可选条件，员工年龄必须满足要求，部门员工姓名为可选要求。这种多条件搜索就是复合搜索。

|  |
| --- |
| GET 索引名/类型名/\_search  {  "query": {  "bool": {  "must": [ #数组中的多个条件必须同时满足  {  "range": {  "字段名": {  "lt": 条件  }  }  }  ],  "must\_not":[ #数组中的多个条件必须都不满足  {  "match": {  "字段名": "条件"  }  },  {  "range": {  "字段名": {  "gte": "搜索条件"  }  }  }  ]  "should": [# 数组中的多个条件有任意一个满足即可。  {  "match": {  "字段名": "条件"  }  },  {  "range": {  "字段名": {  "gte": "搜索条件"  }  }  }  ]  }  }  } |

#### 排序

在Elasticsearch的搜索中，默认是使用相关度分数实现排序的。可以通过搜索语法实现定制化排序。

|  |
| --- |
| GET 索引名/类型名/\_search  {  "query": {  [搜索条件]  },  "sort": [  {  "字段名1": {  "order": "asc"  }  },  {  "字段名2": {  "order": "desc"  }  }  ]  } |

注意：在Elasticsearch中，如果使用text类型的字段作为排序依据，会有问题。Elasticsearch需要对text类型字段数据做分词处理。如果使用text类型字段做排序，Elasticsearch给出的排序结果未必友好，毕竟分词后，先使用哪一个单词做排序都是不合理的。所以Elasticsearch中默认情况下不允许使用text类型的字段做排序，如果需要使用字符串做结果排序，则可使用keyword类型字段作为排序依据，因为keyword字段不做分词处理。

#### 分页

DSL分页也是使用from和size实现的。

|  |
| --- |
| GET 索引名称/\_search  {  "query":{  "match\_all":{}  },  "from": 起始下标,  "size": 查询记录数  } |

#### highlight display

在搜索中，经常需要对搜索关键字做高亮显示，这个时候就可以使用highlight语法。

语法：

|  |
| --- |
| GET 索引名/\_search  {  "query": {  "match": {  "字段名": "条件"  }  },  "highlight": {  "fields": {  "要高亮显示的字段名": {  "fragment\_size": 5, #每个分段长度，默认20  "number\_of\_fragments": 1 #返回多少个分段，默认3  }  },  "pre\_tags": ["前缀"],  "post\_tags": ["后缀"]  }  } |
| // 演示案例  GET test\_search/\_search  {  "query": {  "bool": {  "should": [  {  "match": {  "dname": "Development department"  }  },  {  "match": {  "gender": "男性"  }  }  ]  }  },  "highlight": {  "fields": {  "dname": {  "fragment\_size": 20,  "number\_of\_fragments": 1  },  "gender": {  "fragment\_size": 20,  "number\_of\_fragments": 1  }  },  "pre\_tags":["<span style='color:red'>"],  "post\_tags":["</span>"]  },  "from": 2,  "size": 2  } |

fragment\_size：代表字段数据**如果过长**，则分段，每个片段数据长度为多少。长度不是字符数量，是Elasticsearch内部的数据长度计算方式。默认不对字段做分段。

number\_of\_fragments：代表搜索返回的高亮片段数量，默认情况下会将拆分后的所有片段都返回。

pre\_tags：高亮前缀

post\_tags：高亮后缀

很多搜索结果显示页面中都不会显示完整的数据，这样在数据过长的时候会导致页面效果不佳，都会按照某一个固定长度来显示搜索结果，所以fragment\_size和number\_of\_fragments参数还是很常用的。