



Elasticsearch

权威指南

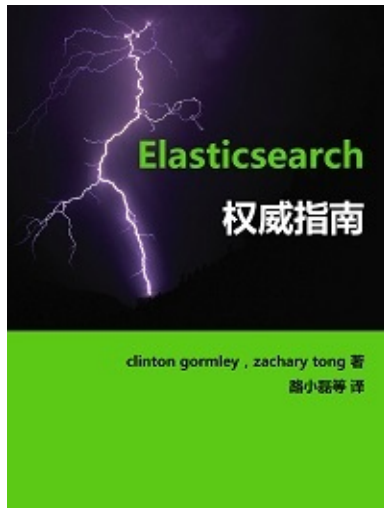
clinton gormley , zachary tong 著

路小磊等 译

Table of Contents

1. [Introduction](#)
2. [入门](#)
 - i. [是什么](#)
 - ii. [安装](#)
 - iii. [API](#)
 - iv. [文档](#)
 - v. [索引](#)
 - vi. [搜索](#)
 - vii. [聚合](#)
 - viii. [小结](#)
 - ix. [分布式](#)
 - x. [结语](#)
3. [分布式集群](#)
 - i. [空集群](#)
 - ii. [集群健康](#)
 - iii. [添加索引](#)
 - iv. [故障转移](#)
 - v. [横向扩展](#)
 - vi. [更多扩展](#)
 - vii. [应对故障](#)
4. [数据](#)
 - i. [文档](#)
 - ii. [索引](#)
 - iii. [获取](#)
 - iv. [存在](#)
 - v. [更新](#)
 - vi. [创建](#)
 - vii. [删除](#)
 - viii. [版本控制](#)
 - ix. [局部更新](#)
 - x. [Mget](#)
 - xi. [批量](#)
 - xii. [结语](#)
5. [分布式增删改查](#)
 - i. [路由](#)
 - ii. [分片交互](#)
 - iii. [新建、索引和删除](#)
 - iv. [检索](#)
 - v. [局部更新](#)
 - vi. [批量请求](#)
 - vii. [批量格式](#)
6. [搜索](#)
 - i. [空搜索](#)
 - ii. [多索引和多类型](#)
 - iii. [分页](#)
 - iv. [查询字符串](#)
7. [映射和分析](#)
 - i. [数据类型差异](#)
 - ii. [确切值对决全文](#)
 - iii. [倒排索引](#)
 - iv. [分析](#)
 - v. [映射](#)

- vi. [复合类型](#)
- 8. [结构化查询](#)
 - i. [请求体查询](#)
 - ii. [结构化查询](#)
 - iii. [查询与过滤](#)
 - iv. [重要的查询子句](#)
 - v. [过滤查询](#)
 - vi. [验证查询](#)
 - vii. [结语](#)
- 9. [排序](#)
 - i. [排序](#)
 - ii. [字符串排序](#)
 - iii. [相关性](#)
 - iv. [字段数据](#)
- 10. [分布式搜索](#)
 - i. [查询阶段](#)
 - ii. [匹配阶段](#)
 - iii. [搜索选项](#)
 - iv. [扫描和滚动](#)
- 11. [索引管理](#)
 - i. [创建删除](#)
 - ii. [设置](#)
 - iii. [配置分析器](#)
 - iv. [自定义分析器](#)
 - v. [映射](#)
 - vi. [根对象](#)
 - vii. [元数据中的source字段](#)
 - viii. [元数据中的all字段](#)
 - ix. [元数据中的ID字段](#)
 - x. [动态映射](#)
 - xi. [自定义动态映射](#)
 - xii. [默认映射](#)
 - xiii. [重建索引](#)
 - xiv. [别名](#)
- 12. [深入分片](#)
 - i. [使文本可以被搜索](#)
 - ii. [动态索引](#)
 - iii. [近实时搜索](#)
 - iv. [持久化变更](#)
 - v. [合并段](#)
- 13. [结构化搜索](#)
 - i. [查询准确值](#)
 - ii. [组合过滤](#)
 - iii. [查询多个准确值](#)
 - iv. [包含，而不是相等](#)
 - v. [范围](#)
 - vi. [处理 Null 值](#)
 - vii. [缓存](#)
 - viii. [过滤顺序](#)



Elasticsearch 权威指南（中文版）

阅读地址：[Elasticsearch权威指南（中文版）](#)

原书地址：[Elasticsearch the definitive guide](#)

原作者：clinton gormley, zachary tong

译者：[Looly](#)

参与翻译：

- [@iridiumcao](#)
- [@cvvnx1](#)
- [@conan007ai](#)
- [@sailxjx](#)
- [@wxlfight](#)
- [@xieyunzi](#)
- [@xdream86](#)
- [@conan007ai](#)
- [@williamzhao](#)

感谢参与翻译的小伙伴们~~

邮箱：looly@gmail.com

微博：[@路小磊](#)

项目地址：

<https://github.com/looly/elasticsearch-definitive-guide-cn>

<http://git.oschina.net/looly/elasticsearch-definitive-guide-cn>

阅读地址：

<http://es.xiaoleilu.com/>

说明

之前接触Elasticsearch只是最简单的使用，想要深入了解内部功能，借助翻译同时系统学习。由于英语比较菜，第一次翻译文档，如有不妥，欢迎提issue:

[github](#)

[git@osc](#)

翻译关键字约定

- index -> 索引
- type -> 类型
- token -> 表征
- filter -> 过滤器
- analyser -> 分析器

Pull Request流程

开始我对Pull Request流程不熟悉，后来参考了[@numbbbbb](#)的《The Swift Programming Language》协作流程，在此感谢。

1. 首先fork我的项目
2. 把fork过去的项目也就是你的项目clone到你的本地
3. 运行 `git remote add looly git@github.com:looly/elasticsearch-definitive-guide-cn.git` 把我的库添加为远端库
4. 运行 `git pull looly master` 拉取并合并到本地
5. 翻译内容
6. commit后push到自己的库（`git push origin master`）
7. 登陆Github在你首页可以看到一个 `pull request` 按钮，点击它，填写一些说明信息，然后提交即可。

1~3是初始化操作，执行一次即可。在翻译前必须执行第4步同步我的库（这样避免冲突），然后执行5~7既可。

注意

1. 文档还未翻译完成，使用gitbook格式，已经翻译完成的章节会陆续提交到gitbook。
2. 为了便于翻译，未翻译部分拷贝自官方英文文档。

入门

Elasticsearch是一个实时分布式搜索和分析引擎。它让你以前所未有的速度处理大数据成为可能。

它用于全文搜索、结构化搜索、分析以及将这三者混合使用：

- 维基百科使用Elasticsearch提供全文搜索并高亮关键字，以及输入实时搜索(**search-as-you-type**)和搜索纠错(**did-you-mean**)等搜索建议功能。
- 英国卫报使用Elasticsearch结合用户日志和社交网络数据提供给他们的编辑以实时的反馈，以便及时了解公众对新发表的文章的回应。
- StackOverflow结合全文搜索与地理位置查询，以及**more-like-this**功能来找到相关的问题和答案。
- Github使用Elasticsearch检索1300亿行的代码。

但是Elasticsearch不仅用于大型企业，它还让像DataDog以及Klout这样的创业公司将最初的想法变成可扩展的解决方案。Elasticsearch可以在你的笔记本上运行，也可以在数以百计的服务器上处理PB级别的数据。

Elasticsearch所涉及到的每一项技术都不是创新或者革命性的，全文搜索，分析系统以及分布式数据库这些早就已经存在了。它的革命性在于将这些独立且有用的技术整合成一个一体化的、实时的应用。它对新用户的门槛很低，当然它也会跟上你技能和需求增长的步伐。

如果你打算看这本书，说明你已经有数据了，但光有数据是不够的，除非你能对这些数据做些什么事情。

很不幸，现在大部分数据库在提取可用知识方面显得异常无能。的确，它们能够通过时间戳或者精确匹配做过滤，但是它们能够进行全文搜索，处理同义词和根据相关性给文档打分吗？它们能根据同一份数据生成分析和聚合的结果吗？最重要的是，它们在没有大量工作进程（线程）的情况下能做到对数据的实时处理吗？

这就是Elasticsearch存在的理由：Elasticsearch鼓励你浏览并利用你的数据，而不是让它烂在数据库里，因为在数据库里实在太难查询了。

Elasticsearch是你新认识的最好的朋友。

为了搜索，你懂的

Elasticsearch是一个基于[Apache Lucene\(TM\)](#)的开源搜索引擎。无论在开源还是专有领域，Lucene可以被认为是迄今为止最先进、性能最好的、功能最全的搜索引擎库。

但是，Lucene只是一个库。想要使用它，你必须使用Java来作为开发语言并将其直接集成到你的应用中，更糟糕的是，Lucene非常复杂，你需要深入了解检索的相关知识来理解它是如何工作的。

Elasticsearch也使用Java开发并使用Lucene作为其核心来实现所有索引和搜索的功能，但是它的目的是通过简单的 `RESTful API` 来隐藏Lucene的复杂性，从而让全文搜索变得简单。

不过，Elasticsearch不仅仅是Lucene和全文搜索，我们还能这样去描述它：

- 分布式的实时文件存储，每个字段都被索引并可被搜索
- 分布式的实时分析搜索引擎
- 可以扩展到上百台服务器，处理PB级结构化或非结构化数据

而且，所有的这些功能被集成到一个服务里面，你的应用可以通过简单的 `RESTful API`、各种语言的客户端甚至命令行与之交互。

上手Elasticsearch非常容易。它提供了许多合理的缺省值，并对初学者隐藏了复杂的搜索引擎理论。它开箱即用（安装即可使用），只需很少的学习既可在生产环境中使用。

Elasticsearch在[Apache 2 license](#)下许可使用，可以免费下载、使用和修改。

随着你对Elasticsearch的理解加深，你可以根据不同的问题领域定制Elasticsearch的高级特性，这一切都是可配置的，并且配置非常灵活。

模糊的历史

多年前，一个叫做Shay Banon的刚结婚不久的失业开发者，由于妻子要去伦敦学习厨师，他便跟着也去了。在他找工作的过程中，为了给妻子构建一个食谱的搜索引擎，他开始构建一个早起版本的Lucene。

直接基于Lucene工作会比较困难，所以Shay开始抽象Lucene代码以便Java程序员可以在应用中添加搜索功能。他发布了他的第一个开源项目，叫做“Compass”。

后来Shay找到一份工作，这份工作处在高性能和内存数据网格的分布式环境中，因此高性能的、实时的、分布式的搜索引擎也是理所当然需要的。然后他决定重写Compass库使其成为一个独立的服务叫做Elasticsearch。

第一个公开版本出现在2010年2月，在那之后Elasticsearch已经成为Github上最受欢迎的项目之一，代码贡献者超过300人。一家主营Elasticsearch的公司就此成立，他们一边提供商业支持一边开发新功能，不过Elasticsearch将永远开源且对所有人可用。

Shay的妻子依旧等待着她的食谱搜索.....

安装Elasticsearch

理解Elasticsearch最好的方式是去运行它，让我们开始吧！

安装Elasticsearch唯一的要求是安装官方新版的Java，地址：www.java.com

你可以从 elasticsearch.org/download 下载最新版本的Elasticsearch。

```
curl -L -O http://download.elasticsearch.org/PATH/TO/VERSION.zip <1>
unzip elasticsearch-$VERSION.zip
cd elasticsearch-$VERSION
```

1. 从 elasticsearch.org/download 获得最新可用的版本号并填入URL中

提示：

在生产环境安装时，除了以上方法，你还可以使用Debian或者RPM安装包，地址在这里：[downloads page](#)，或者也可以使用官方提供的 [Puppet module](#) 或者 [Chef cookbook](#)。

安装Marvel

[Marvel](#)是Elasticsearch的管理和监控工具，在开发环境下免费使用。它包含了一个叫做 [Sense](#) 的交互式控制台，使用户方便的通过浏览器直接与Elasticsearch进行交互。

Elasticsearch线上文档中的很多示例代码都附带一个 [View in Sense](#) 的链接。点击进去，就会在 [Sense](#) 控制台打开相应的实例。安装Marvel不是必须的，但是它可以通过在你本地Elasticsearch集群中运行示例代码而增加与此书的互动性。

Marvel是一个插件，可在Elasticsearch目录中运行以下命令来下载和安装：

```
./bin/plugin -i elasticsearch/marvel/latest
```

你可能想要禁用监控，你可以通过以下命令关闭Marvel：

```
echo 'marvel.agent.enabled: false' >> ./config/elasticsearch.yml
```

运行Elasticsearch

Elasticsearch已经准备就绪，执行以下命令可在前台启动：

```
./bin/elasticsearch
```

如果想在后台以守护进程模式运行，添加 `-d` 参数。

打开另一个终端进行测试：

```
curl 'http://localhost:9200/?pretty'
```

你能看到以下返回信息：


```
{
  "status": 200,
  "name": "Shrunkn Bones",
  "version": {
    "number": "1.4.0",
    "lucene_version": "4.10"
  },
  "tagline": "You Know, for Search"
}
```

这说明你的Elasticsearch集群已经启动并且正常运行，接下来我们可以开始各种实验了。

集群和节点

节点(**node**)是一个运行着的Elasticsearch实例。集群(**cluster**)是一组具有相同 `cluster.name` 的节点集合，他们协同工作，共享数据并提供故障转移和扩展功能，当然一个节点也可以组成一个集群。

你最好找一个合适的名字来替代 `cluster.name` 的默认值，比如你自己的名字，这样可以防止一个新启动的节点加入到相同网络中的另一个同名的集群中。

你可以通过修改 `config/` 目录下的 `elasticsearch.yml` 文件，然后重启Elasticsearch来做到这一点。当Elasticsearch在前台运行，可以使用 `Ctrl-C` 快捷键终止，或者你可以调用 `shutdown` API来关闭：

```
curl -XPOST 'http://localhost:9200/_shutdown'
```

查看Marvel和Sense

如果你安装了Marvel（作为管理和监控的工具），就可以在浏览器里通过以下地址访问它：

http://localhost:9200/_plugin/marvel/

你可以在Marvel中通过点击 `dashboards`，在下拉菜单中访问**Sense**开发者控制台，或者直接访问以下地址：

http://localhost:9200/_plugin/marvel/sense/

与Elasticsearch交互

如何与Elasticsearch交互取决于你是否使用Java。

Java API

Elasticsearch为Java用户提供了两种内置客户端：

节点客户端(node client)：

节点客户端以无数据节点(none data node)身份加入集群，换言之，它自己不存储任何数据，但是它知道数据在集群中的具体位置，并且能够直接转发请求到对应的节点上。

传输客户端(Transport client)：

这个更轻量的传输客户端能够发送请求到远程集群。它自己不加入集群，只是简单转发请求给集群中的节点。

两个Java客户端都通过9300端口与集群交互，使用Elasticsearch传输协议(Elasticsearch Transport Protocol)。集群中的节点之间也通过9300端口进行通信。如果此端口未开放，你的节点将不能组成集群。

TIP

Java客户端所在的Elasticsearch版本必须与集群中其他节点一致，否则，它们可能互相无法识别。

关于Java API的更多信息请查看相关章节：[Java API](#)

基于HTTP协议，以JSON为数据交互格式的RESTful API

其他所有程序语言都可以使用RESTful API，通过9200端口的与Elasticsearch进行通信，你可以使用你喜欢的WEB客户端，事实上，如你所见，你甚至可以通过 `curl` 命令与Elasticsearch通信。

NOTE

Elasticsearch官方提供了多种程序语言的客户端——Groovy, Javascript, .NET, PHP, Perl, Python, 以及 Ruby——还有很多由社区提供的客户端和插件，所有这些可以在[文档](#)中找到。

向Elasticsearch发出的请求的组成部分与其它普通的HTTP请求是一样的：

```
curl -X<VERB> '<PROTOCOL>://<HOST>/<PATH>?<QUERY_STRING>' -d '<BODY>'
```

- VERB HTTP方法：`GET`，`POST`，`PUT`，`HEAD`，`DELETE`
- PROTOCOL `http`或者`https`协议（只有在Elasticsearch前面有`https`代理的时候可用）
- HOST Elasticsearch集群中的任何一个节点的主机名，如果是在本地的节点，那么就叫`localhost`
- PORT Elasticsearch HTTP服务所在的端口，默认为`9200`
- QUERY_STRING 一些可选的查询请求参数，例如 `?pretty` 参数将使请求返回更加美观易读的JSON数据
- BODY 一个JSON格式的请求主体（如果请求需要的话）

举例说明，为了计算集群中的文档数量，我们可以这样做：

```
curl -XGET 'http://localhost:9200/_count?pretty' -d '{
  "query": {
    "match_all": {}
  }
}'
```

```
'
```

Elasticsearch返回一个类似 200 OK 的HTTP状态码和JSON格式的响应主体（除了 HEAD 请求）。上面的请求会得到如下的JSON格式的响应主体：

```
{
  "count" : 0,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "failed" : 0
  }
}
```

我们看不到HTTP头是因为我们没有让 curl 显示它们，如果要显示，使用 curl 命令后跟 -i 参数:

```
curl -i -XGET 'localhost:9200/'
```

对于本书的其余部分，我们将简写 curl 请求中重复的部分，例如主机名和端口，还有 curl 命令本身。

一个完整的请求形如：

```
curl -XGET 'localhost:9200/_count?pretty' -d '
{
  "query": {
    "match_all": {}
  }
}'
```

我们将简写成这样：

```
GET /_count
{
  "query": {
    "match_all": {}
  }
}
```

事实上，在Sense控制台中也使用了与上面相同的格式。

面向文档

应用中的对象很少只是简单的键值列表，更多时候它拥有复杂的数据结构，比如包含日期、地理位置、另一个对象或者数组。

总有一天你会想到把这些对象存储到数据库中。将这些数据保存到由行和列组成的关系数据库中，就好像是把一个丰富，信息表现力强的对象拆散了放入一个非常大的表格中：你不得不拆散对象以适应表模式（通常一列表示一个字段），然后又不得不在查询的时候重建它们。

Elasticsearch是面向文档(**document oriented**)的，这意味着它可以存储整个对象或文档(**document**)。然而它不仅仅是存储，还会索引(**index**)每个文档的内容使之可以被搜索。在Elasticsearch中，你可以对文档（而非成行成列的数据）进行索引、搜索、排序、过滤。这种理解数据的方式与以往完全不同，这也是Elasticsearch能够执行复杂的全文搜索的原因之一。

JSON

Elasticsearch使用**Javascript**对象符号(**JavaScript Object Notation**)，也就是**JSON**，作为文档序列化格式。JSON现在已经被大多语言所支持，而且已经成为NoSQL领域的标准格式。它简洁、简单且容易阅读。

以下使用JSON文档来表示一个用户对象：

```
{
  "email":      "john@smith.com",
  "first_name": "John",
  "last_name":  "Smith",
  "info": {
    "bio":      "Eco-warrior and defender of the weak",
    "age":      25,
    "interests": [ "dolphins", "whales" ]
  },
  "join_date": "2014/05/01"
}
```

尽管原始的 `user` 对象很复杂，但它的结构和对象的含义已经被完整的体现在JSON中了，在Elasticsearch中将对象转化为JSON并做索引要比在表结构中做相同的事情简单的多。

NOTE

尽管几乎所有的语言都有相应的模块用于将任意数据结构转换为JSON，但每种语言处理细节不同。具体请查看“`serialization`” Or “`marshalling`”两个用于处理JSON的模块。[Elasticsearch官方客户端](#)会自动为你序列化和反序列化JSON。

开始第一步

我们现在开始进行一个简单教程，它涵盖了一些基本的概念介绍，比如索引(**indexing**)、搜索(**search**)以及聚合(**aggregations**)。通过这个教程，我们可以让你对Elasticsearch能做的事以及其易用程度有一个大致的感觉。

我们接下来将陆续介绍一些术语和基本的概念，但就算你没有马上完全理解也没有关系。我们将在本书的各个章节中更加深入的探讨这些内容。

所以，坐下来，开始以旋风般的速度来感受Elasticsearch的能力吧！

让我们建立一个员工目录

假设我们刚好在**Megacorp**工作，这时人力资源部门出于某种目的需要让我们创建一个员工目录，这个目录用于促进人文关怀和用于实时协同工作，所以它有以下不同的需求：

- 数据能够包含多个值的标签、数字和纯文本。
- 检索任何员工的所有信息。
- 支持结构化搜索，例如查找30岁以上的员工。
- 支持简单的全文搜索和更复杂的短语(**phrase**)搜索
- 高亮搜索结果中的关键字
- 能够利用图表管理分析这些数据

索引员工文档

我们首先要做的是存储员工数据，每个文档代表一个员工。在Elasticsearch中存储数据的行为就叫做索引(**indexing**)，不过在索引之前，我们需要明确数据应该存储在哪里。

在Elasticsearch中，文档归属于一种类型(**type**)，而这些类型存在于索引(**index**)中，我们可以画一些简单的对比图来类比传统关系型数据库：

```
Relational DB -> Databases -> Tables -> Rows -> Columns
Elasticsearch -> Indices   -> Types  -> Documents -> Fields
```

Elasticsearch集群可以包含多个索引(**indices**)（数据库），每一个索引可以包含多个类型(**types**)（表），每一个类型包含多个文档(**documents**)（行），然后每个文档包含多个字段(**Fields**)（列）。

「索引」含义的区分

你可能已经注意到索引(**index**)这个词在Elasticsearch中有着不同的含义，所以有必要在此做一下区分：

- 索引（名词）
如上文所述，一个索引(**index**)就像是传统关系数据库中的数据库，它是相关文档存储的地方，index的复数是**indices** 或**indexes**。
- 索引（动词）
「索引一个文档」表示把一个文档存储到索引（名词）里，以便它可以被检索或者查询。这很像SQL中的 `INSERT` 关键字，差别是，如果文档已经存在，新的文档将覆盖旧的文档。
- 倒排索引
传统数据库为特定列增加一个索引，例如B-Tree索引来加速检索。Elasticsearch和Lucene使用一种叫做倒排索引(**inverted index**)的数据结构来达到相同目的。

默认情况下，文档中的所有字段都会被索引（拥有一个倒排索引），只有这样他们才是可被搜索的。

我们将会[在倒排索引](#)章节中更详细的讨论。

所以为了创建员工目录，我们将进行如下操作：

- 为每个员工的文档(**document**)建立索引，每个文档包含了相应员工的所有信息。
- 每个文档的类型为 `employee`。
- `employee` 类型归属于索引 `megacorp`。
- `megacorp` 索引存储在Elasticsearch集群中。

实际上这些都是很容易的（尽管看起来有许多步骤）。我们能通过一个命令执行完成的操作：

```
PUT /megacorp/employee/1
{
  "first_name" : "John",
  "last_name" : "Smith",
  "age" : 25,
  "about" : "I love to go rock climbing",
  "interests": [ "sports", "music" ]
}
```

我们看到path: `/megacorp/employee/1` 包含三部分信息：

名字	说明
megacorp	索引名
employee	类型名
1	这个员工的ID

请求实体（JSON文档），包含了这个员工的所有信息。他的名字叫“John Smith”，25岁，喜欢攀岩。

很简单吧！它不需要你做额外的管理操作，比如创建索引或者定义每个字段的数据类型。我们能够直接索引文档，Elasticsearch已经内置所有的缺省设置，所有管理操作都是透明的。

接下来，让我们在目录中加入更多员工信息：

```
PUT /megacorp/employee/2
{
  "first_name" : "Jane",
  "last_name" : "Smith",
  "age" : 32,
  "about" : "I like to collect rock albums",
  "interests": [ "music" ]
}

PUT /megacorp/employee/3
{
  "first_name" : "Douglas",
  "last_name" : "Fir",
  "age" : 35,
  "about": "I like to build cabinets",
  "interests": [ "forestry" ]
}
```

检索文档

现在Elasticsearch中已经存储了一些数据，我们可以根据业务需求开始工作了。第一个需求是能够检索单个员工的信息。

这对于Elasticsearch来说非常简单。我们只要执行HTTP GET请求并指出文档的“地址”——索引、类型和ID既可。根据这三部分信息，我们就可以返回原始JSON文档：

```
GET /megacorp/employee/1
```

响应的内容中包含一些文档的元信息，John Smith的原始JSON文档包含在 `_source` 字段中。

```
{
  "_index" : "megacorp",
  "_type" : "employee",
  "_id" : "1",
  "_version" : 1,
  "found" : true,
  "_source" : {
    "first_name" : "John",
    "last_name" : "Smith",
    "age" : 25,
    "about" : "I love to go rock climbing",
    "interests": [ "sports", "music" ]
  }
}
```

我们通过HTTP方法 `GET` 来检索文档，同样的，我们可以使用 `DELETE` 方法删除文档，使用 `HEAD` 方法检查某文档是否存在。如果想更新已存在的文档，我们只需再 `PUT` 一次。

简单搜索

`GET` 请求非常简单——你能轻松获取你想要的文档。让我们来进一步尝试一些东西，比如简单的搜索！

我们尝试一个最简单的搜索全部员工的请求：

```
GET /megacorp/employee/_search
```

你可以看到我们依然使用 `megacorp` 索引和 `employee` 类型，但是我们在结尾使用关键字 `_search` 来取代原来的文档ID。响应内容的 `hits` 数组中包含了我们所有的三个文档。默认情况下搜索会返回前10个结果。

```
{
  "took": 6,
  "timed_out": false,
  "_shards": { ... },
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "megacorp",
        "_type": "employee",
        "_id": "3",
        "_score": 1,
        "_source": {
          "first_name": "Douglas",
          "last_name": "Fir",
          "age": 35,
          "about": "I like to build cabinets",
          "interests": [ "forestry" ]
        }
      },

```

```

{
  "_index":      "megacorp",
  "_type":      "employee",
  "_id":        "1",
  "_score":      1,
  "_source": {
    "first_name": "John",
    "last_name":  "Smith",
    "age":        25,
    "about":      "I love to go rock climbing",
    "interests": [ "sports", "music" ]
  }
},
{
  "_index":      "megacorp",
  "_type":      "employee",
  "_id":        "2",
  "_score":      1,
  "_source": {
    "first_name": "Jane",
    "last_name":  "Smith",
    "age":        32,
    "about":      "I like to collect rock albums",
    "interests": [ "music" ]
  }
}
]
}

```

注意：

响应内容不仅会告诉我们哪些文档被匹配到，而且这些文档内容完整的被包含在其中——我们在给用户展示搜索结果时需要用到的所有信息都有了。

接下来，让我们搜索姓氏中包含“**Smith**”的员工。要做到这一点，我们将在命令行中使用轻量级的搜索方法。这种方法常被称为查询字符串(**query string**)搜索，因为我们像传递URL参数一样去传递查询语句：

```
GET /megacorp/employee/_search?q=last_name:Smith
```

我们在请求中依旧使用 `_search` 关键字，然后将查询语句传递给参数 `q=`。这样就可以得到所有姓氏为Smith的结果：

```

{
  ...
  "hits": {
    "total":      2,
    "max_score":  0.30685282,
    "hits": [
      {
        ...
        "_source": {
          "first_name": "John",
          "last_name":  "Smith",
          "age":        25,
          "about":      "I love to go rock climbing",
          "interests": [ "sports", "music" ]
        }
      },
      {
        ...
        "_source": {
          "first_name": "Jane",
          "last_name":  "Smith",
          "age":        32,
          "about":      "I like to collect rock albums",
          "interests": [ "music" ]
        }
      }
    ]
  }
}

```


使用DSL语句查询

查询字符串搜索是便于通过命令行完成点对点(**ad hoc**)的搜索,但是它也有局限性(参阅简单搜索章节)。Elasticsearch提供更加丰富且灵活的查询语言叫做**DSL查询(Query DSL)**,它允许你构建更加复杂、强大的搜索。

DSL(Domain Specific Language领域特定语言)指定JSON做为请求体。我们可以这样表示之前关于“Smith”的查询:

```
GET /megacorp/employee/_search
{
  "query" : {
    "match" : {
      "last_name" : "Smith"
    }
  }
}
```

这会返回与之前查询相同的结果。你可以看到有些东西做了改变,我们不再使用查询字符串(**query string**)做为参数,而是使用请求体代替。这个请求体使用JSON表示,其中使用了 `match` 语句(查询类型之一,其余我们将在接下来的章节学习到)。

更复杂的搜索

我们让搜索变的复杂一些。我们依旧想要找到姓氏为“Smith”的员工,但是我们只想得到年龄大于30岁的员工。我们的语句将做一些改变用来添加过滤器(**filter**),它允许我们有效的执行一个结构化搜索:

```
GET /megacorp/employee/_search
{
  "query" : {
    "filtered" : {
      "filter" : {
        "range" : {
          "age" : { "gt" : 30 } <1>
        }
      },
      "query" : {
        "match" : {
          "last_name" : "smith" <2>
        }
      }
    }
  }
}
```

- <1> 这部分查询是 `range` 过滤器(**filter**),它用于查找所有年龄大于30岁的数据(译者注: `age` 字段大于30的数据),—— `gt` 代表“greater than”。
- <2> 这部分查询与之前的 `match` 语句(**query**)一致。

现在不要担心语法太多,我们将会在后面的章节详细的讨论。只要知道我们添加了一个过滤器(**filter**)用于执行区间搜索,然后重复利用了之前的 `match` 语句。现在我们只显示一个32岁且名字是“Jane Smith”的员工了:

```
{
  ...
  "hits": {
    "total": 1,
    "max_score": 0.30685282,
    "hits": [
      {
        ...
        "_source": {
          "first_name": "Jane",
          "last_name": "Smith",
          "age": 32,
          "about": "I like to collect rock albums",
          "interests": [ "music" ]
        }
      }
    ]
  }
}
```

```
}
  }
}
}
```

全文搜索

到目前为止搜索都很简单：简单的名字，通过年龄筛选。让我们尝试一种更高级的搜索，全文搜索——一种传统数据库很难实现的功能。

我们将会搜索所有喜欢“**rock climbing**”的员工：

```
GET /megacorp/employee/_search
{
  "query" : {
    "match" : {
      "about" : "rock climbing"
    }
  }
}
```

你可以看到我们使用与之前一致的 `match` 查询搜索 `about` 字段中的“**rock climbing**”，我们会得到两个匹配文档：

```
{
  ...
  "hits": {
    "total":      2,
    "max_score":  0.16273327,
    "hits": [
      {
        ...
        "_score":      0.16273327, <1>
        "_source": {
          "first_name": "John",
          "last_name":  "Smith",
          "age":        25,
          "about":      "I love to go rock climbing",
          "interests": [ "sports", "music" ]
        }
      },
      {
        ...
        "_score":      0.016878016, <1>
        "_source": {
          "first_name": "Jane",
          "last_name":  "Smith",
          "age":        32,
          "about":      "I like to collect rock albums",
          "interests": [ "music" ]
        }
      }
    ]
  }
}
```

- `<1>` 相关评分。

一般Elasticsearch根据相关评分排序，相关评分是根据文档与语句的匹配度来得出，第一个最高分很明确：John Smith 的 `about` 字段明确的写到“**rock climbing**”。

但是为什么Jane Smith也会出现在结果里？原因是“**rock**”在她的 `about` 字段中提及了。因为只有“**rock**”被提及而“**climbing**”没有，所以她的 `_score` 要低于John。

这个例子很好的解释了Elasticsearch如何进行全文字段搜索且首先返回相关性最大的结果。相关性(**relevance**)概念在Elasticsearch中非常重要，而这也是它与传统关系型数据库中记录只有匹配和不匹配概念最大的不同。

短语搜索

能找到字段中单独的单词固然最好，但是有时候你想要匹配确切的单词序列或者短语(**phrases**)。例如我们想要查询 `about` 包含完整短语“**rock climbing**”的员工。

为了实现以上效果，我们将查询 `match` 变更为 `match_phrase`：

```
GET /megacorp/employee/_search
{
  "query" : {
    "match_phrase" : {
      "about" : "rock climbing"
    }
  }
}
```

毫无悬念返回John Smith的文档：

```
{
  ...
  "hits": {
    "total":      1,
    "max_score":  0.23013961,
    "hits": [
      {
        ...
        "_score":      0.23013961,
        "_source": {
          "first_name": "John",
          "last_name":  "Smith",
          "age":        25,
          "about":       "I love to go rock climbing",
          "interests": [ "sports", "music" ]
        }
      }
    ]
  }
}
```

高亮我们的搜索

很多应用喜欢从每个搜索结果中高亮(**highlight**)匹配到的关键字，以便用户可以知道为什么文档这样匹配查询。Elasticsearch中高亮片段是非常容易的。

让我们在之前的语句上增加 `highlight` 参数：

```
GET /megacorp/employee/_search
{
  "query" : {
    "match_phrase" : {
      "about" : "rock climbing"
    }
  },
  "highlight" : {
    "fields" : {
      "about" : {}
    }
  }
}
```

当我们运行这个语句，会命中与之前相同的结果，但是会得到一个新的叫做 `highlight` 的部分，这里包括了 `about` 字段中匹配的文本片段，并且用 `` 包围匹配到的单词。

```

{
  ...
  "hits": {
    "total":      1,
    "max_score":  0.23013961,
    "hits": [
      {
        ...
        "_score":      0.23013961,
        "_source": {
          "first_name": "John",
          "last_name":  "Smith",
          "age":        25,
          "about":      "I love to go rock climbing",
          "interests": [ "sports", "music" ]
        },
        "highlight": {
          "about": [
            "I love to go <em>rock</em> <em>climbing</em>" <1>
          ]
        }
      ]
    ]
  }
}

```

<1> The highlighted fragment from the original text.

- <1> 原有文本中高亮的片段

你可以在高亮章节阅读更多关于搜索高亮的部分。

分析

最后，我们还有一个需求需要完成：允许管理者在职员目录中分析。Elasticsearch把这项功能叫做聚合(**aggregations**)，它允许你在数据基础上生成复杂的统计。它很像SQL中的 GROUP BY 但是功能更强大。

举个例子，让我们找到最受职员欢迎的兴趣：

```
GET /megacorp/employee/_search
{
  "aggs": {
    "all_interests": {
      "terms": { "field": "interests" }
    }
  }
}
```

忽略语法只看结果：

```
{
  ...
  "hits": { ... },
  "aggregations": {
    "all_interests": {
      "buckets": [
        {
          "key": "music",
          "doc_count": 2
        },
        {
          "key": "forestry",
          "doc_count": 1
        },
        {
          "key": "sports",
          "doc_count": 1
        }
      ]
    }
  }
}
```

我们可以看到两个职员对音乐有兴趣，一个喜欢森林，一个喜欢运动。这些聚合的数据并没有被预先计算好，它们从匹配查询语句的文档中动态生成。如果我们想知道姓**"Smith"**的人什么兴趣最受欢迎，我们只需要增加合数的语句既可：

```
GET /megacorp/employee/_search
{
  "query": {
    "match": {
      "last_name": "smith"
    }
  },
  "aggs": {
    "all_interests": {
      "terms": {
        "field": "interests"
      }
    }
  }
}
```

`all_interests` 已经变成只包含匹配语句的文档了：

```
...
"all_interests": {
  "buckets": [
```

```

    {
      "key": "music",
      "doc_count": 2
    },
    {
      "key": "sports",
      "doc_count": 1
    }
  ]
}

```

聚合也允许分级汇总。例如，让我们统计每种兴趣下职员平均年龄：

```

GET /megacorp/employee/_search
{
  "aggs" : {
    "all_interests" : {
      "terms" : { "field" : "interests" },
      "aggs" : {
        "avg_age" : {
          "avg" : { "field" : "age" }
        }
      }
    }
  }
}

```

虽然这次返回的聚合结果更加复杂，但是依旧容易理解：

```

...
"all_interests": {
  "buckets": [
    {
      "key": "music",
      "doc_count": 2,
      "avg_age": {
        "value": 28.5
      }
    },
    {
      "key": "forestry",
      "doc_count": 1,
      "avg_age": {
        "value": 35
      }
    },
    {
      "key": "sports",
      "doc_count": 1,
      "avg_age": {
        "value": 25
      }
    }
  ]
}

```

输出基本上是我们之前运行聚合的一个丰富化版本。我们依旧有兴趣以及它们数量的列表，但是现在每个兴趣额外拥有 `avg_age` 用来显示拥有此兴趣职员平均年龄。

即使你依旧不能理解语法，但是可以很轻松的看到如此复杂的聚合和分组能够使用这些特性完成。处理数据的能力取决于你能提取什么样的数据！

教程小结

希望这个小的指南对于Elasticsearch的功能是一个好的范例。当然这只是一些皮毛，为了保持简短，还有很多特性未提及——像推荐、定位、渗透、模糊以及部分匹配等。但这也强调了构建高级搜索功能是多么容易。无需配置，只需要添加数据然后开始搜索既可！

可能有些语法让你有困惑的地方，或者在微调方面有些疑问。那么，本书的其余部分将深入这些问题的细节，让你全面了解Elasticsearch的工作过程。

分布式的特性

在章节的开始我们提到Elasticsearch可以扩展到上百（甚至上千）的服务器来处理PB级的数据。我们的教程只是给出了一些样例来告诉你Elasticsearch如何使用，并未提及相关机制。Elasticsearch为分布式而生，而且被设计为隐藏分布式环境中的复杂性。

分布式的Elasticsearch在很大程度上都是透明的，在教程中你不需要知道任何关于分布式系统、分片、集群发现或者其他分布式概念的知识。你可能在笔记本上运行着教程的例子，但是如果你在拥有100个节点的集群里运行，一切操作都是一样的。

Elasticsearch致力于隐藏分布式系统的复杂性，一些操作都是在底层自动完成的：

- 将你的文档分区到不同的容器或者分片(**shards**)中，它们可以存在于一个或多个节点中。
- 在集群的不同节点平衡分片，合理分布索引和搜索负载。
- 复制每个节点提供数据冗余，防止硬件故障造成的数据丢失。
- 在集群中的任意节点路由到你感兴趣的数据所在节点。
- 当你的集群需要扩展或者节点恢复再分配时做到无缝整合新节点。

当你阅读本书时，你可以遇到关于Elasticsearch分布式特性的补充章节。这些章节将教给你如何扩展集群和故障转移（《分布式集群》），如何处理文档存储（《分布式文档》），如何执行分布式搜索（《分布式搜索》），分片是什么以及如何工作（《深入分片》）。

这些章节不是必读的——不懂它们也是可以使用Elasticsearch的。但是这些能帮助你更深入和完整的了解Elasticsearch。轻松略读它们然后在你需要更完整的理解时回头翻阅。

结语

现在你可以细细品味Elasticsearch可以做什么，而且多么简单的上手。Elasticsearch致力于降低学习成本和减少配置。学习Elasticsearch最好的方式是使用它：开始索引和检索吧！

当然，关于Elasticsearch你懂的越多，生产力就越高。你也可以依据你程序的特定领域节点，它就可以给你更适合的数据。

本书其余部分将帮助你从新手晋级到专家。每一个章节都会阐述一个要点，但是依旧会包含专家级别的提示。如果你只是刚起步，这些提示现在可能并不适合你。Elasticsearch有合理的缺省值而且可以在没有用户干预的情况下做正确的事情。当需要提升性能时你可以随时回顾这些章节。

体验集群

补充章节

正如之前提及的，这是关于Elasticsearch分布式操作的一些补充章节的第一部分。这个章节我们解释一些通用的术语，例如集群(**cluster**)、节点(**node**)和分片(**shard**)，Elasticsearch的扩展机制，以及它如何处理硬件故障。

尽管这章不是必读的——你可以长时间使用Elasticsearch而不必担心分片、复制和故障转移——但是它会帮助你理解Elasticsearch内部的工作流程，你可以先跳过这章，以后再来查阅。

Elasticsearch用于构建高可用和可扩展的系统。扩展的方式可以是购买更好的服务器(纵向扩展(**vertical scale or scaling up**))或者购买更多的服务器(横向扩展(**horizontal scale or scaling out**))。

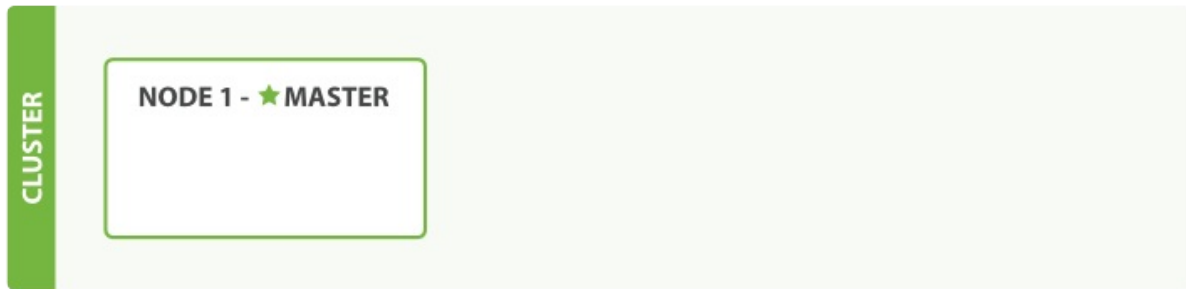
Elasticsearch能从更强大的硬件中获得更好的性能，但是纵向扩展也有一定的局限性。真正的扩展应该是横向的，它通过增加节点来传播负载和增加可靠性。

对于大多数数据库而言，横向扩展意味着你的程序将做非常大的改动来利用这些新添加的设备。对比来说，Elasticsearch天生是分布式的：它知道如何管理节点来提供高扩展和高可用。这意味着你的程序不需要关心这些。

在这章我们将探索如何创建你的集群(**cluster**)、节点(**node**)和分片(**shards**)来按照你的需求扩展，并保证在硬件故障后数据依旧安全。

空集群

如果我们启动一个单独的节点，没有数据和索引，这个集群我们称作“只有一个空节点的集群”。



一个节点(**node**)就是一个Elasticsearch实例，而一个集群(**cluster**)由一个或多个节点组成，它们具有相同的 `cluster.name`，它们协同工作，分享数据和负载。当有新的节点加入或者删除节点，集群就会感知到并平衡数据。

集群中一个节点会被选举为主节点(**master**)，它用来管理集群中的一些变更，例如新建或删除索引、增加或移除节点等。主节点不需要参与文档级别的更改或搜索，这意味着只有一个主节点不会随着流量的增长而成为集群的瓶颈。任何节点可以成为主节点。我们例子中的集群只有一个节点，所以它会充当主节点的角色。

做为用户，我们能够与集群中的任何节点(**any node in the cluster**)通信，包括主节点。任何一个节点互相知道文档存在于哪个节点上，它们可以转发请求到我们需要数据所在的节点上。我们通信的节点负责收集各节点返回的数据，最后一起返回给客户端。这一切都由Elasticsearch透明的管理。

集群健康

在Elasticsearch集群中可以监控统计很多信息，但是只有一个是最重要的：集群健康(cluster health)。它用 green、yellow 或 red 表示 status ；

```
GET /_cluster/health
```

在一个没有索引的空集群中，它将返回一些信息类似如下：

```
{
  "cluster_name":      "elasticsearch",
  "status":            "green", <1>
  "timed_out":         false,
  "number_of_nodes":   1,
  "number_of_data_nodes": 1,
  "active_primary_shards": 0,
  "active_shards":     0,
  "relocating_shards": 0,
  "initializing_shards": 0,
  "unassigned_shards": 0
}
```

- <1> status 是我们最感兴趣的字段。

status 字段提供一个整体的标识来指示集群的功能是否可用。三种颜色表示：

颜色	意义
green	所有主要和复制的分片都可用
yellow	所有主分片可用，但不是所有复制分片都可用
red	不是所有的主分片都可用

在接下来的章节，我们将说明什么是主要分片(primary shard)和复制分片(replica shard)，并说明这些颜色在实际环境中的意义。

添加索引

为了将数据添加到Elasticsearch，我们需要索引(index)——一个存储关联数据的地方。实际上，索引只是一个用来指向一个或多个分片(shards)的“逻辑命名空间(logical namespace)”。

一个分片(shard)是一个最小级别“工作单元(worker unit)”，它只是保存索引中所有数据的一小片。在接下来的《深入分片》一章，我们将详细说明分片的工作原理，但是现在只要知道分片是一个单一的Lucene实例既可，并且它本身就是一个完整的搜索引擎。我们的文档存储和被索引在分片中，但是我们的程序不知道如何直接与它们通信。取而代之的是，他们直接与索引通信。

分片用于Elasticsearch在你的集群中分配数据。想象把分片当作数据的容器。文档存储在分片中，然后分片分配给你集群中的节点上。当你的集群扩容或缩小，Elasticsearch将会自动在你的节点间迁移分片，以使集群保持平衡。

分片可以是主分片(primary shard)或者复制分片(replica shard)。你索引中的每个文档属于一个单独的主分片，所以主分片的数量决定了你最多能存储多少数据。

理论上主分片对存储多少数据没有限制，限制取决于你实际的使用情况。碎片的最大容量完全取决于你的使用状况：硬件存储的大小、文档的大小和复杂度、如何索引和查询你的文档，以及你期望的响应时间。

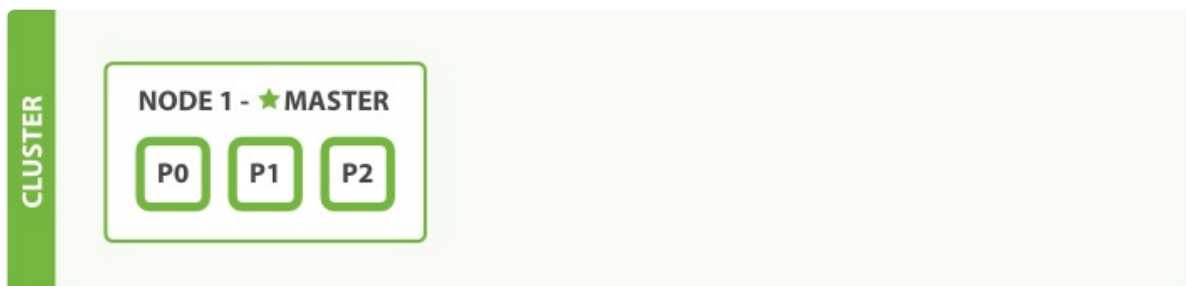
复制分片只是主分片的一个副本，它用于提供数据的冗余副本，在硬件故障之后提供数据保护，同时服务于像搜索和检索等只读请求。

主分片的数量会在其索引创建完成后修正，但是复制分片的数量会随时变化。

让我们在集群中一个空节点上创建一个叫做 blogs 的索引。一个索引默认指派5个主分片，但是为了演示的目的，我们只指派3个主分片和一个复制分片（每个主分片有一个复制分片对应）：

```
PUT /blogs
{
  "settings" : {
    "number_of_shards" : 3,
    "number_of_replicas" : 1
  }
}
```

附带索引的单一节点集群：



我们的集群现在看起来像单节点集群(cluster-one-node)——三个主分片都被分配到 Node 1。如果我们现在想检查集群健康(cluster-health)，我们将见到以下信息：

```
{
  "cluster_name":      "elasticsearch",
  "status":            "yellow", <1>
  "timed_out":         false,
  "number_of_nodes":   1,
  "number_of_data_nodes": 1,
  "active_primary_shards": 3,
  "active_shards":     3,
```

```
"relocating_shards": 0,  
"initializing_shards": 0,  
"unassigned_shards": 3 <2>  
}
```

- <1> 集群的 `status` 现在是 `yellow` .
- <2> 我们的三个复制分片还没有被分配到节点上。

集群的健康状况 `yellow` 意味着所有的主分片(**primary shards**)启动并且运行了——集群已经可以成功的接受任意请求——但是复制分片(**replica shards**)还没有全部可用。事实上所有的三个复制分片现在是 `unassigned` (未分配) 状态——它们还未被分配给节点。在同一个节点上保存相同的数据副本是没有必要的, 如果这个节点故障了, 那所有的数据副本也会丢失。

现在我们的集群已经功能完备, 但是依旧存在因硬件故障而导致的数据丢失的风险。

增加故障转移

在单一节点上运行意味着有单点故障的风险——没有数据冗余备份。幸运的是我们可以启动另一个节点来保护我们的数据不被丢失。

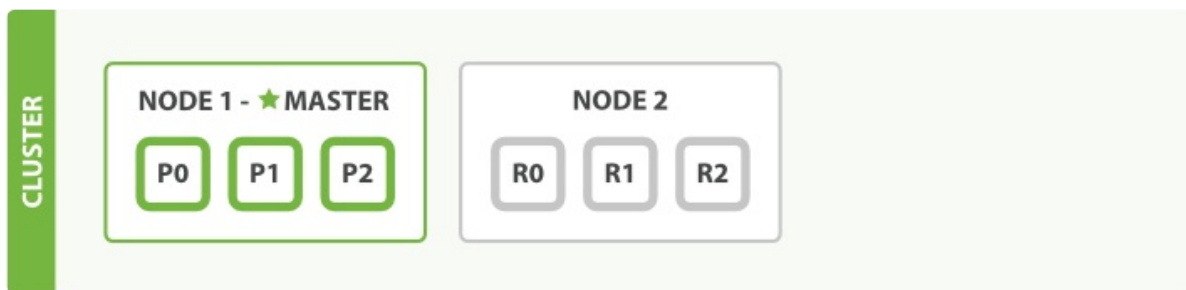
启动第二个节点

为了测试在增加第二个节点后发生了什么，你可以使用与第一个节点相同的方式启动第二个节点（《运行 Elasticsearch》一章），而且在同一个目录——多个节点可以分享同一个目录。

只要第二个节点与第一个节点有相同的 `cluster.name`（请看 `./config/elasticsearch.yml` 文件），它就能自动发现并加入第一个节点的集群。如果没有，检查日志找出哪里出了问题。这可能是网络广播被禁用，或者防火墙阻止了节点通信。

如果我们启动了第二个节点，这个集群应该叫做双节点集群(**cluster-two-nodes**)

双节点集群——所有的主分片和复制分片都被分配:



第二个节点加入集群时，三个复制碎片(**replica shards**)已经被分配了——与三个主分片一一对应。那意味着在丢失一个节点的情况下依旧可以保证数据的完整性。

一些新的被索引的文档将首先被存储在主分片中，然后平行复制到关联的复制节点上。这可以确保我们的数据在主节点和复制节点上都可以被检索。

`cluster-health` 现在的状态是 `green`，这意味着所有的6个分片（三个主分片和三个复制分片）都已可用：

```
{
  "cluster_name":      "elasticsearch",
  "status":            "green", <1>
  "timed_out":         false,
  "number_of_nodes":   2,
  "number_of_data_nodes": 2,
  "active_primary_shards": 3,
  "active_shards":     6,
  "relocating_shards": 0,
  "initializing_shards": 0,
  "unassigned_shards": 0
}
```

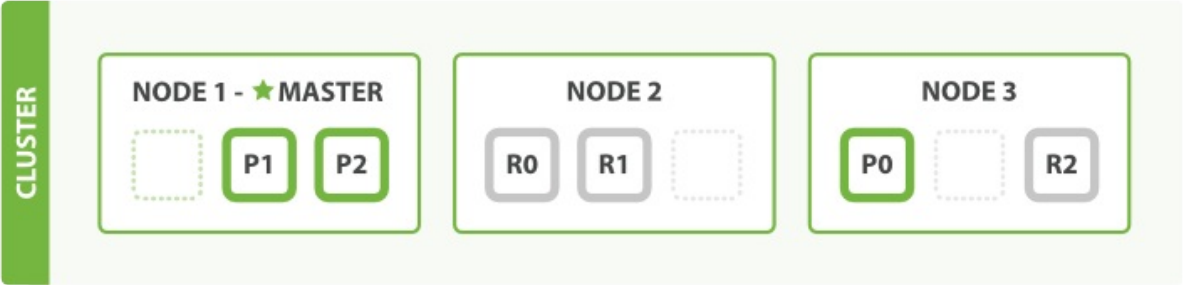
- <1> 集群的 `status` 是 `green` .

我们的集群不仅是全功能的，而且是高可用的。

横向扩展

随着应用需求的增长，我们该如何扩展？如果我们启动第三个节点，我们的集群会自我感知，这时便成为了三节点集群 (cluster-three-nodes)

分片已经被重新分配以平衡负载：



从 Node 1 和 Node 2 来的分片已经被移动到新的 Node 3 上，这样每个节点就有两个分片，以代替之前的三个。这意味着每个节点的硬件资源（CPU、RAM、I/O）被较少的分片共享，这样每个分片就会有更好的表现。

分片本身就是一个完整成熟的搜索引擎，它可以使用单一节点的所有资源。使用这6个分片（3个主分片和三个复制分片）我们可以扩展最多到6个节点，每个节点上有一个分片，这样就可以100%使用这个节点的资源了。

更多扩展

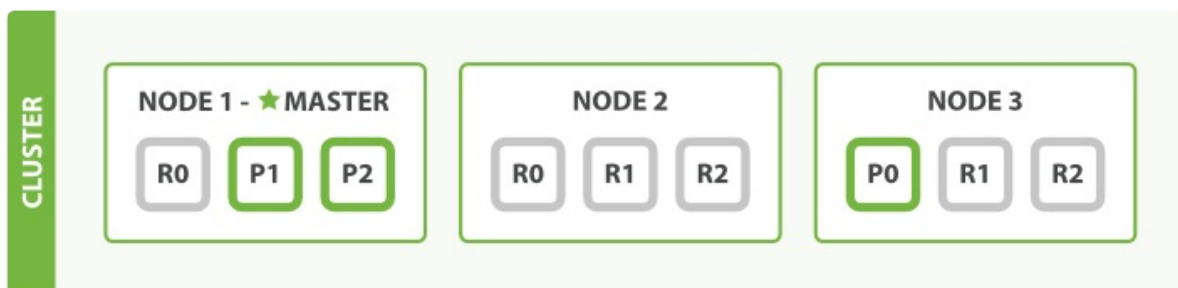
但是要怎么做才可以扩展我们的搜索使之大于6个节点？

主分片的数量在创建索引时已经给定。实际上，这个数字定义了能存储到索引里数据的最大数量（实际的数量取决于你的数据、硬件和使用情况）。当然，读请求——搜索和文档检索——能够通过主分片或者复制分片处理，所以数据的冗余越多，我们能处理的搜索吞吐量就越大。

复制分片的数量可以在运行中的集群中动态地变更，这允许我们可以根据需求扩大或者缩小规模。让我们增加复制分片的数量，从原来的 1 变成 2：

```
PUT /blogs/_settings
{
  "number_of_replicas" : 2
}
```

增加 number_of_replicas 到2：



从图中可以看出，blogs 索引现在有9个分片：三个主分片和6个复制分片。这意味着我们能够扩展到9个节点，再次的变成每个节点一个分片。这样使我们的搜索性能相比标准的三节点集群扩展三倍。

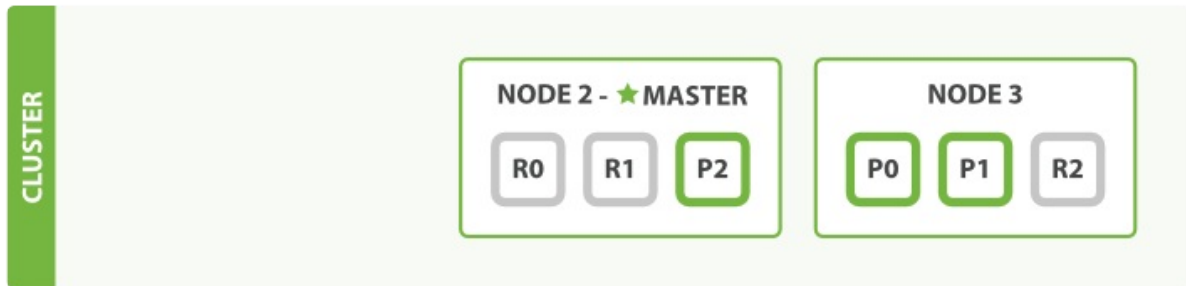
注意：

当然，只是有更多的复制分片在同样数量的节点上并不能提高我们的性能，因为每个分片都要访问更小比重的节点资源（译者注：大部分请求都聚集到了分片少的节点，导致一个节点吞吐量太大，反而降低性能）。你需要增加硬件来提高吞吐量。

不过这些额外的复制节点意味着我们有更多的冗余：通过以上对接点的设置，我们更够承受两个节点故障而不丢失数据。

应对故障

我们已经说过Elasticsearch可以应对节点失效，所以让我们继续尝试。如果我们杀掉第一个节点的进程（以下简称杀掉节点），看起来像如此：



我们杀掉的节点是一个主节点。必须有一个主节点来让集群的功能可用，所以发生的第一件事就是各节点选举了一个新的主节点：Node 2。

主分片 1 和 2 在我们杀掉 Node 1 时已经丢失，我们的索引在丢失主节点时不能正常工作。如果此时我们检查集群健康，我们将看到状态 red：不是所有主节点都可用！

幸运的是丢失的两个主分片的完整拷贝在其他节点上还存在，所以新主节点的第一件事是提升这些在 Node 2 和 Node 3 上的分片的副本为主分片，集群健康回到 yellow 状态。这个提升是瞬间完成的，就好像按了一下开关。

为什么集群健康状态是 yellow 而不是 green？我们三个主分片，但是我们指定了每个主分片对应两个复制分片，当前却只有一个被定义。这阻止我们达到 green 状态，不过不用太担心这个：当我们杀掉 Node 2，我们的程序依旧可以在没有丢失数据的情况下运行，因为 Node 3 还有每个分片的拷贝。

如果我们重启 Node 1，集群将能够分配丢失的复制分片，结果状态与三主节点双复制一致。如果 Node 1 依旧有旧节点的拷贝，它将会尝试再利用它们，它只会复制在故障期间数据变更的部分。

现在你应该对分片如何使Elasticsearch可以水平扩展并保证数据安全有了一个清晰的认识。接下来我们将会讨论分片生命周期的更多细节。

数据吞吐

无论程序怎么写，意图是一样的：组织数据为我们的目标所服务。但数据并不只是由随机比特和字节组成，我们在数据节点间建立关联来表示现实世界中的实体或者“某些东西”。属于同一个人的名字和Email地址会有更多的意义。

在现实世界中，并不是所有相同类型的实体看起来都是一样的。一个人可能有一个家庭电话号码，另一个人可能只有一个手机号码，有些人可能两者都有。一个人可能有三个Email地址，其他人可能没有。西班牙人可能有两个姓氏，但是英国人（英语系国家的人）可能只有一个。

面向对象编程语言之所以受欢迎，一个原因是对象帮助我们表示和处理现实生活中包含潜在复杂结构的实体。到目前为止这非常好。

当我们想存储这些实体时问题便来了。传统上，我们以行和列的形式把数据存储的关系型数据库中，相当于使用电子表格。这种固定的存储方式导致对象的灵活性不复存在了。

但是如何能以对象的形式存储对象呢？相对于围绕表格去为我们的程序去建模，我们可以专注于使用数据，把对象本来的灵活性找回来。

对象(**object**)是特定语言（language-specific）和内存式（in-memory）的数据结构。为了在网络间发送，或者存储它，我们需要一些标准的格式来表示它。**JSON (JavaScript Object Notation)**是一种可读的以文本来表示对象的方式。它已经成为NoSQL世界中数据交换的一种事实标准。当对象被序列化为JSON，它就成为**JSON文档(JSON document)**了。

Elasticsearch是一个分布式的文档(**document**)存储引擎。它实时的可以存储并检索复杂的数据结构——序列化的JSON文档。换言之，一旦文档被存储在Elasticsearch中，它在集群的任一节点上就可以被检索。

当然，我们不仅需要存储数据，还要快速的批量查询。虽然已经有很多NoSQL的解决方案允许我们以文档的形式存储对象，但它们依旧需要考虑如何查询我们的数据，以及哪些字段需要被索引以便让数据检索更加快速。

在Elasticsearch中，每一个字段的数据都是默认被索引的。也就是说，每个字段专门有一个反向索引用于快速检索。而且，与其它数据库不同，它可以在同一个查询中利用所有的这些反向索引，以惊人的速度返回结果。

在这一章我们将探讨如何使用API来创建、检索、更新和删除文档。目前，我们并不关心数据如何在文档中以及如何查询它们。所有我们关心的是文档如何安全在Elasticsearch中存储，以及如何让它们返回。

什么是文档？

程序中大多数的实体或对象能够被序列化为包含键值对的JSON对象，键(key)是字段(field)或属性(property)的名字，值(value)可以是字符串、数字、布尔类型、另一个对象、值数组或者其他特殊类型，比如表示日期的字符串或者表示地理位置的对象。

```
{
  "name":      "John Smith",
  "age":       42,
  "confirmed": true,
  "join_date": "2014-06-01",
  "home": {
    "lat":     51.5,
    "lon":     0.1
  },
  "accounts": [
    {
      "type": "facebook",
      "id":   "johnsmith"
    },
    {
      "type": "twitter",
      "id":   "johnsmith"
    }
  ]
}
```

通常，我们使用可互换的对象(object)和文档(document)。然而，还是有区别的。对象(Object)仅是一个JSON对象——类似于哈希、hashmap、字典或者关联数组。对象(Object)则可以包含其他对象(Object)。

在Elasticsearch中，文档(document)这个术语有着特殊含义。它指的是拥有唯一ID的最顶层或者根对象(root object)序列化成JSON。

文档元数据

一个文档不只有数据。它还包含了元数据(metadata)——关于文档的信息。三个必须的元数据节点是：

节点	说明
<code>_index</code>	文档存储的地方
<code>_type</code>	文档代表的对象的类
<code>_id</code>	文档的唯一标识

`_index`

索引(index)类似于关系型数据库里的“数据库”——它是我们存储和索引关联数据的地方。

提示：

事实上，我们的数据被存储和索引在分片(shards)中，索引只是一个把一个或多个分片分组在一起的逻辑空间。然而，这只是一些内部细节——我们的程序完全不用关心分片。对于我们的程序而言，文档存储在索引(index)中。剩下的细节由Elasticsearch关心既可。

我们将会在《索引管理》章节中探讨如何创建并管理索引，但现在，我们将让Elasticsearch为我们创建索引。我们唯一需要做的仅仅是选择一个索引名。这个名字必须是全部小写，不能以下划线开头，不能包含逗号。让我们使用 `website` 做为索引名。

`_type`

在应用中，我们使用对象表示一些“事物”，例如一个用户、一篇博客、一个评论，或者一封邮件。每个对象都属于一个类(class)，这个类定义了属性或与对象关联的数据。 `user` 类的对象可能包含姓名、性别、年龄和Email地址。

在关系型数据库中，我们经常将相同类的对象存储在一个表里，因为它们有着相同的结构。同理，在Elasticsearch中，我们使用相同类型(type)的文档表示相同的“事物”，因为他们的数据结构也是相同的。

每个类型(type)都有自己的映射(mapping)或者结构定义，就像传统数据库表中的列一样。所有类型下的文档被存储在同一个索引下，但是类型的映射(mapping)会告诉Elasticsearch不同的文档如何被索引。我们将会 在《映射》章节探讨如何定义和管理映射，但是现在我们将依赖Elasticsearch去自动处理数据结构。

`_type` 的名字可以是大写或小写，不能包含下划线或逗号。我们将使用 `blog` 做为类型名。

`_id`

`id` 仅仅是一个字符串，它与 `_index` 和 `_type` 组合时，就可以在Elasticsearch中唯一标识一个文档。当创建一个文档，你可以自定义 `_id`，也可以让Elasticsearch帮你自动生成。

其它元数据

还有一些其它的元数据，我们将在《映射》章节探讨。使用上面提到的元素，我们已经可以在Elasticsearch中存储文档并通过ID检索——换言之，把Elasticsearch做为文档存储器使用了。

索引一个文档

文档通过 `index` API 被索引——使数据可以被存储和搜索。但是首先我们需要决定文档所在。正如我们讨论的，文档通过其 `_index`、`_type`、`_id` 唯一确定。我们可以自己提供一个 `_id`，或者也使用 `index` API 为我们生成一个。

使用自己的ID

如果你的文档有自然的标识符（例如 `user_account` 字段或者其他值表示文档），你就可以提供自己的 `_id`，使用这种形式的 `index` API：

```
PUT /{index}/{type}/{id}
{
  "field": "value",
  ...
}
```

例如我们的索引叫做“website”，类型叫做“blog”，我们选择的ID是“123”，那么这个索引请求就像这样：

```
PUT /website/blog/123
{
  "title": "My first blog entry",
  "text": "Just trying this out...",
  "date": "2014/01/01"
}
```

Elasticsearch的响应：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "123",
  "_version": 1,
  "created": true
}
```

响应指出请求的索引已经被成功创建，这个索引中包含 `_index`、`_type` 和 `_id` 元数据，以及一个新元素：`_version`。

Elasticsearch中每个文档都有版本号，每当文档变化（包括删除）都会使 `_version` 增加。在《版本控制》章节中我们将探讨如何使用 `_version` 号确保你程序的一部分不会覆盖掉另一部分所做的更改。

自增ID

如果我们的数据没有自然ID，我们可以让Elasticsearch自动为我们生成。请求结构发生了变化：`PUT` 方法——“在这个URL中存储文档”变成了 `POST` 方法——“在这个文档下存储文档”。（译者注：原来是把文档存储到某个ID对应的空间，现在是把这个文档添加到某个 `_type` 下）。

URL现在只包含 `_index` 和 `_type` 两个字段：

```
POST /website/blog/
{
  "title": "My second blog entry",
  "text": "Still trying this out...",
  "date": "2014/01/01"
}
```

响应内容与刚才类似，只有 `_id` 字段变成了自动生成的值：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "wM00SFhDQXGZAWDf0-drSA",
  "_version": 1,
  "created": true
}
```

自动生成的ID有22个字符长，URL-safe, Base64-encoded string universally unique identifiers, 或者叫 [UUIDs](#)。

检索文档

想要从Elasticsearch中获取文档，我们使用同样的 `_index`、`_type`、`_id`，但是HTTP方法改为 `GET`：

```
GET /website/blog/123?pretty
```

响应包含了现在熟悉的元数据节点，增加了 `_source` 字段，它包含了在创建索引时我们发送给Elasticsearch的原始文档。

```
{
  "_index" : "website",
  "_type" : "blog",
  "_id" : "123",
  "_version" : 1,
  "found" : true,
  "_source" : {
    "title": "My first blog entry",
    "text": "Just trying this out...",
    "date": "2014/01/01"
  }
}
```

pretty

在任意的查询字符串中增加 `pretty` 参数，类似于上面的例子。会让Elasticsearch美化输出(**pretty-print**)JSON响应以便更加容易阅读。`_source` 字段不会被美化，它的样子与我们输入的一致。

`GET`请求返回的响应内容包括 `{"found": true}`。这意味着文档已经找到。如果我们请求一个不存在的文档，依旧会得到一个JSON，不过 `found` 值变成了 `false`。

此外，HTTP响应状态码也会变成 `'404 Not Found'` 代替 `'200 OK'`。我们可以在 `curl` 后加 `-i` 参数得到响应头：

```
curl -i -XGET http://localhost:9200/website/blog/124?pretty
```

现在响应类似于这样：

```
HTTP/1.1 404 Not Found
Content-Type: application/json; charset=UTF-8
Content-Length: 83

{
  "_index" : "website",
  "_type" : "blog",
  "_id" : "124",
  "found" : false
}
```

检索文档的一部分

通常，`GET` 请求将返回文档的全部，存储在 `_source` 参数中。但是可能你感兴趣的字段只是 `title`。请求个别字段可以使用 `_source` 参数。多个字段可以使用逗号分隔：

```
GET /website/blog/123?_source=title,text
```

`_source` 字段现在只包含我们请求的字段，而且过滤了 `date` 字段：


```
{
  "_index" :   "website",
  "_type" :    "blog",
  "_id" :      "123",
  "_version" : 1,
  "exists" :   true,
  "_source" : {
    "title": "My first blog entry" ,
    "text": "Just trying this out..."
  }
}
```

或者你只想得到 `_source` 字段而不要其他的元数据，你可以这样请求：

```
GET /website/blog/123/_source
```

它仅仅返回:

```
{
  "title": "My first blog entry",
  "text": "Just trying this out...",
  "date": "2014/01/01"
}
```

检查文档是否存在

如果你想做的只是检查文档是否存在——你对内容完全不感兴趣——使用 `HEAD` 方法来代替 `GET`。 `HEAD` 请求不会返回响应体，只有HTTP头：

```
curl -i -XHEAD http://localhost:9200/website/blog/123
```

Elasticsearch将会返回 `200 OK` 状态如果你的文档存在：

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=UTF-8
Content-Length: 0
```

如果不存在返回 `404 Not Found`：

```
curl -i -XHEAD http://localhost:9200/website/blog/124
```

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=UTF-8
Content-Length: 0
```

当然，这只代表你在查询的那一刻文档不存在，但并不表示几毫秒后依旧不存在。另一个进程在这期间可能创建新文档。

更新整个文档

文档在Elasticsearch中是不可变的——我们不能修改他们。如果需要更新已存在的文档，我们可以使用《索引文档》章节提到的 `index` API 重建索引(*reindex*) 或者替换掉它。

```
PUT /website/blog/123
{
  "title": "My first blog entry",
  "text": "I am starting to get the hang of this...",
  "date": "2014/01/02"
}
```

在响应中，我们可以看到Elasticsearch把 `_version` 增加了。

```
{
  "_index" : "website",
  "_type" : "blog",
  "_id" : "123",
  "_version" : 2,
  "created": false <1>
}
```

- `<1>` `created` 标识为 `false` 因为同索引、同类型下已经存在同ID的文档。

在内部，Elasticsearch已经标记旧文档为删除并添加了一个完整的新文档。旧版本文档不会立即消失，但你也不能去访问它。Elasticsearch会在你继续索引更多数据时清理被删除的文档。

在本章的后面，我们将会 在《局部更新》中探讨 `update` API。这个API 似乎 允许你修改文档的局部，但事实上Elasticsearch遵循与之前所说完全相同的过程，这个过程如下：

1. 从旧文档中检索JSON
2. 修改它
3. 删除旧文档
4. 索引新文档

唯一的不同是 `update` API完成这一过程只需要一个客户端请求既可，不再需要 `get` 和 `index` 请求了。

创建一个新文档

当索引一个文档，我们如何确定是完全创建了一个新的还是覆盖了一个已经存在的呢？

请记住 `_index`、`_type`、`_id` 三者唯一确定一个文档。所以要想保证文档是新加入的，最简单的方式是使用 `POST` 方法让 Elasticsearch 自动生成唯一 `_id`：

```
POST /website/blog/  
{ ... }
```

然而，如果想使用自定义的 `_id`，我们必须告诉 Elasticsearch 应该在 `_index`、`_type`、`_id` 三者都不同时才接受请求。为了做到这点有两种方法，它们其实做的是同一件事情。你可以选择适合自己的方式：

第一种方法使用 `op_type` 查询参数：

```
PUT /website/blog/123?op_type=create  
{ ... }
```

或者第二种方法是在 URL 后加 `/_create` 做为端点：

```
PUT /website/blog/123/_create  
{ ... }
```

如果请求成功的创建了一个新文档，Elasticsearch 将返回正常的元数据且响应状态码是 `201 Created`。

另一方面，如果包含相同的 `_index`、`_type` 和 `_id` 的文档已经存在，Elasticsearch 将返回 `409 Conflict` 响应状态码，错误信息类似如下：

```
{  
  "error" : "DocumentAlreadyExistsException[[website][4] [blog][123]:  
            document already exists]",  
  "status" : 409  
}
```

删除文档

删除文档的语法模式与之前基本一致，只不过要使用 `DELETE` 方法：

```
DELETE /website/blog/123
```

如果文档被找到，Elasticsearch将返回 `200 OK` 状态码和以下响应体。注意 `_version` 数字已经增加了。

```
{
  "found" :    true,
  "_index" :   "website",
  "_type" :    "blog",
  "_id" :      "123",
  "_version" : 3
}
```

如果文档未找到，我们将得到一个 `404 Not Found` 状态码，响应体是这样的：

```
{
  "found" :    false,
  "_index" :   "website",
  "_type" :    "blog",
  "_id" :      "123",
  "_version" : 4
}
```

尽管文档不存在——`"found"` 的值是 `false` ——`_version` 依旧增加了。这是内部记录的一部分，它确保在多节点间不同操作可以有正确的顺序。

正如在《更新文档》一章中提到的，删除一个文档也不会立即从磁盘上移除，它只是被标记成已删除。Elasticsearch 将会在你之后添加更多索引的时候才会在后台进行删除内容的清理。

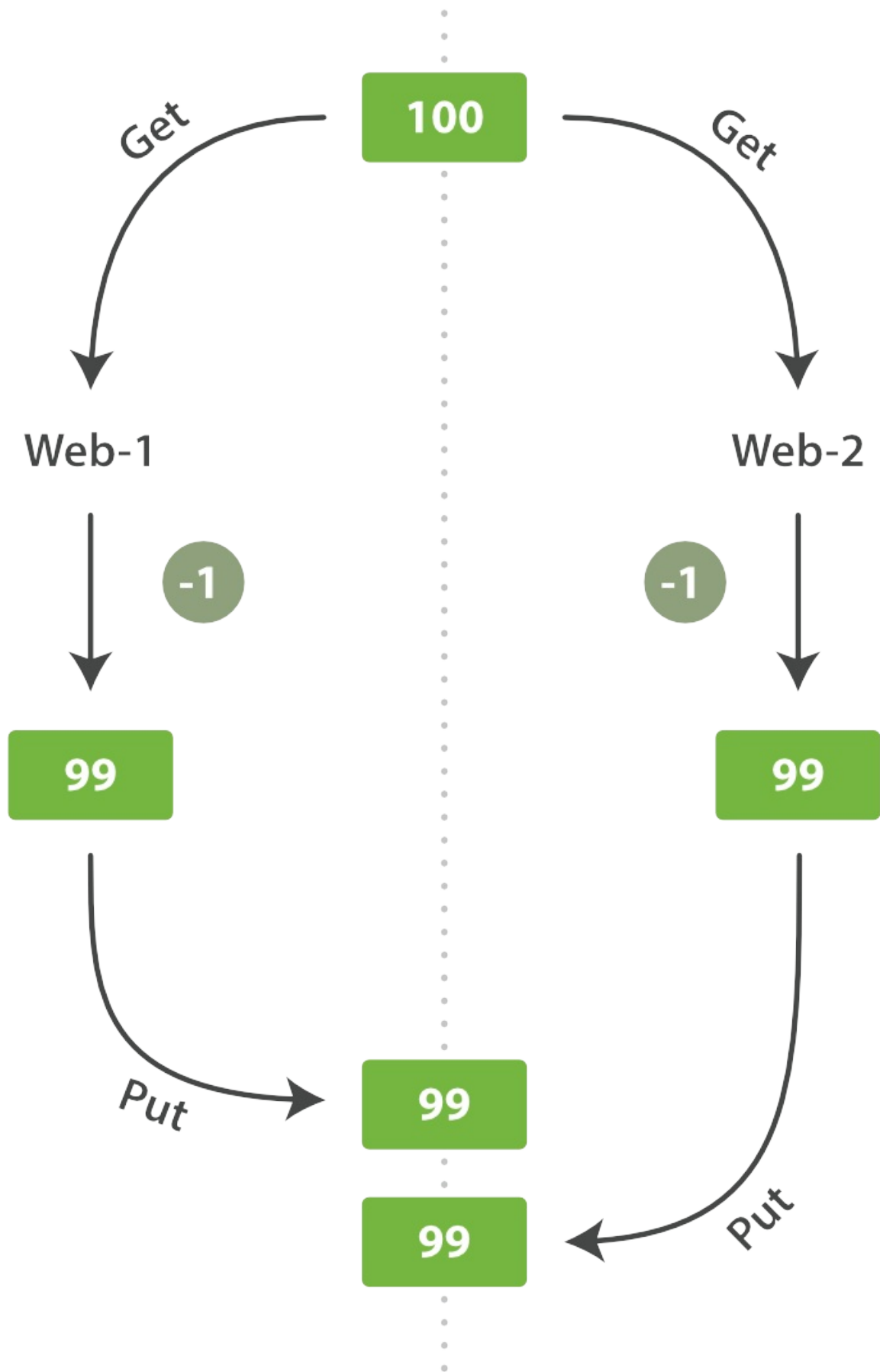
处理冲突

当使用 `index` API更新文档的时候，我们读取原始文档，做修改，然后将整个文档(**whole document**)一次性重新索引。最近的索引请求会生效——Elasticsearch中只存储最后被索引的任何文档。如果其他人同时也修改了这个文档，他们的修改将会丢失。

很多时候，这并不是一个问题。或许我们主要的数据存储在关系型数据库中，然后拷贝数据到Elasticsearch中只是为了可以用于搜索。或许两个人同时修改文档的机会很少。亦或者偶尔的修改丢失对于我们的工作来说并无大碍。

但有时丢失修改是一个很严重的问题。想象一下我们使用Elasticsearch存储大量在线商店的库存信息。每当销售一个商品，Elasticsearch中的库存就要减一。

一天，老板决定做一个促销。瞬间，我们每秒就销售了几个商品。想象两个同时运行的web进程，两者同时处理一件商品的订单：



web_1 让 stock_count 失效是因为 web_2 没有察觉到 stock_count 的拷贝已经过期 (译者注: web_1 取数据, 减一后更新)

了 `stock_count` 。可惜在 `web_1` 更新 `stock_count` 前它就拿到了数据，这个数据已经是过期的了，当 `web_2` 再回来更新 `stock_count` 时这个数字就是错的。这样就会造成看似卖了一件东西，其实是卖了两件，这个应该属于幻读。）。结果是我们认为自己确实还有更多的商品，最终顾客会因为销售给他们没有的东西而失望。

变化越是频繁，或读取和更新的时间越长，越容易丢失我们的更改。

在数据库中，有两种通用的方法确保在并发更新时修改不丢失：

悲观并发控制（Pessimistic concurrency control）

这在关系型数据库中被广泛的使用，假设冲突的更改经常发生，为了解决冲突我们把访问区块化。典型的例子是在读一行数据前锁定这行，然后确保只有加锁的那个线程可以修改这行数据。

乐观并发控制（Optimistic concurrency control）：

被Elasticsearch使用，假设冲突不经常发生，也不区块化访问，然而，如果在读写过程中数据发生了变化，更新操作将失败。这时候又程序决定在失败后如何解决冲突。实际情况中，可以重新尝试更新，刷新数据（重新读取）或者直接反馈给用户。

乐观并发控制

Elasticsearch是分布式的。当文档被创建、更新或删除，文档的新版本会被复制到集群的其它节点。Elasticsearch即是同步的又是异步的，意思是这些复制请求都是平行发送的，并无序(out of sequence)的到达目的地。这就需要一种方法确保老版本的文档永远不会覆盖新的版本。

上文我们提到 `index` 、 `get` 、 `delete` 请求时，我们指出每个文档都有一个 `_version` 号码，这个号码在文档被改变时加一。Elasticsearch使用这个 `_version` 保证所有修改都被正确排序。当一个旧版本出现在新版本之后，它会被简单的忽略。

我们利用 `_version` 的这一优点确保数据不会因为修改冲突而丢失。我们可以指定文档的 `version` 来做想要的更改。如果那个版本号不是现在的，我们的请求就失败了。

Let's create a new blog post: 让我们创建一个新的博文：

```
PUT /website/blog/1/_create
{
  "title": "My first blog entry",
  "text": "Just trying this out..."
}
```

响应体告诉我们这是一个新建的文档，它的 `_version` 是 `1`。现在假设我们要编辑这个文档：把数据加载到web表单中，修改，然后保存成新版本。

首先我们检索文档：

```
GET /website/blog/1
```

响应体包含相同的 `_version` 是 `1`

```
{
  "_index" : "website",
  "_type" : "blog",
  "_id" : "1",
  "_version" : 1,
  "found" : true,
  "_source" : {
    "title": "My first blog entry",
    "text": "Just trying this out..."
  }
}
```



```
}
```

现在，当我们通过重新索引文档保存修改时，我们这样指定了 `version` 参数：

```
PUT /website/blog/1?version=1 <1>
{
  "title": "My first blog entry",
  "text": "Starting to get the hang of this..."
}
```

- `<1>` 我们只希望文档的 `_version` 是 1 时更新才生效。

This request succeeds, and the response body tells us that the `_version` has been incremented to 2：

请求成功，响应体告诉我们 `_version` 已经增加到 2：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "1",
  "_version": 2
  "created": false
}
```

然而，如果我们重新运行相同的索引请求，依旧指定 `version=1`，Elasticsearch将返回 `409 Conflict` 状态的HTTP响应。响应体类似这样：

```
{
  "error" : "VersionConflictEngineException[[website][2] [blog][1]:
            version conflict, current [2], provided [1]]",
  "status" : 409
}
```

这告诉我们当前 `_version` 是 2，但是我们指定想要更新的版本是 1。

我们需要做什么取决于程序的需求。我们可以告知用户其他人修改了文档，你应该在保存前再看一下。而对于上文提到的商品 `stock_count`，我们需要重新检索最新文档然后申请新的更改操作。

所有更新和删除文档的请求都接受 `version` 参数，它可以允许在你的代码中增加乐观锁控制。

使用外部版本控制系统

一种常见的结构是使用一些其他的数据库作为主数据库，然后使用Elasticsearch搜索数据，这意味着所有主数据库发生变化，就要将其拷贝到Elasticsearch中。如果有多个进程负责这些数据的同步，就会遇到上面提到的并发问题。

如果主数据库有版本字段——或一些类似于 `timestamp` 等可以用于版本控制的字段——是你就可以在Elasticsearch的查询字符串后面添加 `version_type=external` 来使用这些版本号。版本号必须是整数，大于零小于 `9.2e+18` ——Java中的正的 `long`。

外部版本号与之前说的内部版本号在处理的时候有些不同。它不再检查 `_version` 是否与请求中指定的一致，而是检查是否小于指定的版本。如果请求成功，外部版本号就会被存储到 `_version` 中。

外部版本号不仅在索引和删除请求中指定，也可以在创建(**create**)新文档中指定。

例如，创建一个包含外部版本号 5 的新博客，我们可以这样做：

```
PUT /website/blog/2?version=5&version_type=external
```

```
{
  "title": "My first external blog entry",
  "text": "Starting to get the hang of this..."
}
```

在响应中，我们可以看到当前的 `_version` 号码是 5：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "2",
  "_version": 5,
  "created": true
}
```

现在我们更新这个文档，指定一个新 `version` 号码为 10：

```
PUT /website/blog/2?version=10&version_type=external
{
  "title": "My first external blog entry",
  "text": "This is a piece of cake..."
}
```

请求成功的设置了当前 `_version` 为 10：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "2",
  "_version": 10,
  "created": false
}
```

如果你重新运行这个请求，就会返回一个像之前一样的冲突错误，因为指定的外部版本号不大于当前在Elasticsearch中的版本。

文档局部更新

在《更新文档》一章，我们说了一种通过检索，修改，然后重建整文档的索引方法来更新文档。这是对的。然而，使用 `update` API，我们可以使用一个请求来实现局部更新，例如增加数量的操作。

我们也说过文档是不可变的——它们不能被更改，只能被替换。`update` API必须遵循相同的规则。表面看来，我们似乎是局部更新了文档的位置，内部却是像我们之前说的一样简单的使用 `update` API处理相同的检索-修改-重建索引流程，我们也减少了其他进程可能导致冲突的修改。

最简单的 `update` 请求表单接受一个局部文档参数 `doc`，它会合并到现有文档中——对象合并在一起，存在的标量字段被覆盖，新字段被添加。举个例子，我们可以使用以下请求为博客添加一个 `tags` 字段和一个 `views` 字段：

```
POST /website/blog/1/_update
{
  "doc" : {
    "tags" : [ "testing" ],
    "views": 0
  }
}
```

如果请求成功，我们将看到类似 `index` 请求的响应结果：

```
{
  "_index" : "website",
  "_id" : "1",
  "_type" : "blog",
  "_version" : 3
}
```

检索文档文档显示被更新的 `_source` 字段：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "1",
  "_version": 3,
  "found": true,
  "_source": {
    "title": "My first blog entry",
    "text": "Starting to get the hang of this...",
    "tags": [ "testing" ], <1>
    "views": 0 <1>
  }
}
```

- <1> 我们新添加的字段已经被添加到 `_source` 字段中。

使用脚本局部更新

使用Groovy脚本

这时候当API不能满足要求时，Elasticsearch允许你使用脚本实现自己的逻辑。脚本支持非常多的API，例如搜索、排序、聚合和文档更新。脚本可以通过请求的一部分、检索特殊的 `.scripts` 索引或者从磁盘加载方式执行。

默认的脚本语言是**Groovy**，一个快速且功能丰富的脚本语言，语法类似于Javascript。它在一个沙盒(**sandbox**)中运行，以防止恶意用户毁坏Elasticsearch或攻击服务器。

你可以在《脚本参考文档》中获得更多信息。

脚本能够使用 `update` API 改变 `_source` 字段的内容，它在脚本内部以 `ctx._source` 表示。例如，我们可以使用脚本增加博客的 `views` 数量：

```
POST /website/blog/1/_update
{
  "script" : "ctx._source.views+=1"
}
```

我们还可以使用脚本增加一个新标签到 `tags` 数组中。在这个例子中，我们定义了一个新标签做为参数而不是硬编码在脚本里。这允许Elasticsearch未来可以重复利用脚本，而不是在想要增加新标签时必须每次编译新脚本：

```
POST /website/blog/1/_update
{
  "script" : "ctx._source.tags+=new_tag",
  "params" : {
    "new_tag" : "search"
  }
}
```

获取最后两个有效请求的文档：

```
{
  "_index": "website",
  "_type": "blog",
  "_id": "1",
  "_version": 5,
  "found": true,
  "_source": {
    "title": "My first blog entry",
    "text": "Starting to get the hang of this...",
    "tags": ["testing", "search"], <1>
    "views": 1 <2>
  }
}
```

- <1> `search` 标签已经被添加到 `tags` 数组。
- <2> `views` 字段已经被增加。

通过设置 `ctx.op` 为 `delete` 我们可以根据内容删除文档：

```
POST /website/blog/1/_update
{
  "script" : "ctx.op = ctx._source.views == count ? 'delete' : 'none'",
  "params" : {
    "count": 1
  }
}
```

更新可能不存在的文档

想象我们要在Elasticsearch中存储浏览量计数器。每当有用户访问页面，我们增加这个页面的浏览量。但如果这是个新页面，我们并不确定这个计数器存在与否。当我们试图更新一个不存在的文档，更新将失败。

在这种情况下，我们可以使用 `upsert` 参数定义文档来使其不存在时被创建。

```
POST /website/pageviews/1/_update
{
  "script" : "ctx._source.views+=1",
  "upsert": {
    "views": 1
  }
}
```

第一次执行这个请求，`upsert` 值被索引为一个新文档，初始化 `views` 字段为 `1`。接下来文档已经存在，所以 `script` 被更新代替，增加 `views` 数量。

更新和冲突

在这一节介绍中，我们说了如何在检索(**retrieve**)和重建索引(**reindex**)间使用更小的窗口，如何更小的机会发生冲突性的变更的话题。但它并不能完全排除这种可能性。

在这一节的介绍中，我们介绍了如何在检索(**retrieve**)和重建索引(**reindex**)中保持更小的窗口，如何减少冲突性变更发生的概率，不过这些无法被完全避免，像一个其他进程在 `update` 进行重建索引时修改了文档这种情况依旧可能发生。

为了避免丢失数据，`update` API在检索(**retrieve**)阶段检索文档的当前 `_version`，然后在重建索引(**reindex**)阶段通过 `index` 请求提交。如果其他进程在检索(**retrieve**)和重建索引(**reindex**)阶段修改了文档，`_version` 将不能被匹配，然后更新失败。

对于多用户的局部更新，文档被修改了并不要紧。例如，两个进程都要增加页面浏览量，增加的顺序我们并不关心——如果冲突发生，我们唯一要做的仅仅是重新尝试更新既可。

这些可以通过 `retry_on_conflict` 参数设置重试次数来自动完成，这样 `update` 操作将会在发生错误前重试——这个值默认为 `0`。

```
POST /website/pageviews/1/_update?retry_on_conflict=5 <1>
{
  "script" : "ctx._source.views+=1",
  "upsert": {
    "views": 0
  }
}
```

- `<1>` 在错误发生前重试更新5次

这适用于像增加计数这种顺序无关的操作，但是还有一种顺序非常重要的情况。例如 `index` API，使用“保留最后更新(**last-write-wins**)”的 `update` API，但它依旧接受一个 `version` 参数以允许你使用乐观并发控制(**optimistic concurrency control**)来指定你要更细文档的版本。

检索多个文档

像Elasticsearch一样，检索多个文档依旧非常快。合并多个请求可以避免每个请求单独的网络开销。如果你需要从Elasticsearch中检索多个文档，相对于一个一个的检索，更快的方式是在一个请求中使用**multi-get**或者 `mget` API。

`mget` API参数是一个 `docs` 数组，数组的每个节点定义一个文档的 `_index`、`_type`、`_id` 元数据。如果你只想检索一个或几个确定的字段，也可以定义一个 `_source` 参数：

```
GET /_mget
{
  "docs" : [
    {
      "_index" : "website",
      "_type" : "blog",
      "_id" : 2
    },
    {
      "_index" : "website",
      "_type" : "pageviews",
      "_id" : 1,
      "_source": "views"
    }
  ]
}
```

响应体也包含一个 `docs` 数组，每个文档还包含一个响应，它们按照请求定义的顺序排列。每个这样的响应与单独使用 `get request`响应体相同：

```
{
  "docs" : [
    {
      "_index" : "website",
      "_id" : "2",
      "_type" : "blog",
      "found" : true,
      "_source" : {
        "text" : "This is a piece of cake...",
        "title" : "My first external blog entry"
      },
      "_version" : 10
    },
    {
      "_index" : "website",
      "_id" : "1",
      "_type" : "pageviews",
      "found" : true,
      "_version" : 2,
      "_source" : {
        "views" : 2
      }
    }
  ]
}
```

如果你想检索的文档在同一个 `_index` 中（甚至在同一个 `_type` 中），你就可以在URL中定义一个默认的 `/_index` 或者 `/_index/_type`。

你依旧可以在单独的请求中使用这些值：

```
GET /website/blog/_mget
{
  "docs" : [
    { "_id" : 2 },
    { "_type" : "pageviews", "_id" : 1 }
  ]
}
```

事实上，如果所有文档具有相同 `_index` 和 `_type`，你可以通过简单的 `ids` 数组来代替完整的 `docs` 数组：

```
GET /website/blog/_mget
{
  "ids" : [ "2", "1" ]
}
```

注意到我们请求的第二个文档并不存在。我们定义了类型为 `blog`，但是ID为 `1` 的文档类型为 `pageviews`。这个不存在的文档会在响应体中被告知。

```
{
  "docs" : [
    {
      "_index" : "website",
      "_type" : "blog",
      "_id" : "2",
      "_version" : 10,
      "found" : true,
      "_source" : {
        "title": "My first external blog entry",
        "text": "This is a piece of cake..."
      }
    },
    {
      "_index" : "website",
      "_type" : "blog",
      "_id" : "1",
      "found" : false <1>
    }
  ]
}
```

- `<1>` 这个文档不存在

事实上第二个文档不存在并不影响第一个文档的检索。每个文档的检索和报告都是独立的。

注意：

尽管前面提到有一个文档没有被找到，但HTTP请求状态码还是 `200`。事实上，就算所有文档都找不到，请求也还是返回 `200`，原因是 `mget` 请求本身成功了。如果想知道每个文档是否都成功了，你需要检查 `found` 标志。

更省时的批量操作

就像 `mget` 允许我们一次性检索多个文档一样，`bulk` API允许我们使用单一请求来实现多个文档的 `create`、`index`、`update` 或 `delete`。这对索引类似于日志活动这样的数据流非常有用，它们可以以成百上千的数据为一个批次按序进行索引。

`bulk` 请求体如下，它有一点不同寻常：

```
{ action: { metadata }}\n{ request body      }\n{ action: { metadata }}\n{ request body      }\n...
```

这种格式类似于用 `"\n"` 符号连接起来的一行一行的JSON文档流(**stream**)。两个重要的点需要注意：

- 每行必须以 `"\n"` 符号结尾，包括最后一行。这些都是作为每行有效的分离而做的标记。
- 每一行的数据不能包含未被转义的换行符，它们会干扰分析——这意味着JSON不能被美化打印。

提示:

在《批量格式》一章我们介绍了为什么 `bulk` API使用这种格式。

action/metadata这一行定义了文档行为(**what action**)发生在哪个文档(**which document**)之上。

行为(**action**)必须是以下几种：

行为	解释
<code>create</code>	当文档不存在时创建之。详见《创建文档》
<code>index</code>	创建新文档或替换已有文档。见《索引文档》和《更新文档》
<code>update</code>	局部更新文档。见《局部更新》
<code>delete</code>	删除一个文档。见《删除文档》

在索引、创建、更新或删除时必须指定文档的 `_index`、`_type`、`_id` 这些元数据(**metadata**)。

例如删除请求看起来像这样：

```
{ "delete": { "_index": "website", "_type": "blog", "_id": "123" }}
```

请求体(**request body**)由文档的 `_source` 组成——文档所包含的一些字段以及其值。它被 `index` 和 `create` 操作所必须，这是有道理的：你必须提供文档用来索引。

这些还被 `update` 操作所必需，而且请求体的组成应该与 `update` API（`doc`，`upsert`，`script` 等等）一致。删除操作不需要请求体(**request body**)。

```
{ "create": { "_index": "website", "_type": "blog", "_id": "123" }}\n{ "title":    "My first blog post" }
```

如果定义 `_id`，ID将会被自动创建：

```
{ "index": { "_index": "website", "_type": "blog" }}
```



```
{ "title": "My second blog post" }
```

为了将这些放在一起，bulk 请求表单是这样的：

```
POST /_bulk
{ "delete": { "_index": "website", "_type": "blog", "_id": "123" }} <1>
{ "create": { "_index": "website", "_type": "blog", "_id": "123" }}
{ "title": "My first blog post" }
{ "index": { "_index": "website", "_type": "blog" }}
{ "title": "My second blog post" }
{ "update": { "_index": "website", "_type": "blog", "_id": "123", "_retry_on_conflict" : 3} }
{ "doc" : { "title" : "My updated blog post" } } <2>
```

- <1> 注意 delete 行为(action)没有请求体，它紧接着另一个行为(action)
- <2> 记得最后一个换行符

Elasticsearch响应包含一个 items 数组，它罗列了每一个请求的结果，结果的顺序与我们请求的顺序相同：

```
{
  "took": 4,
  "errors": false, <1>
  "items": [
    { "delete": {
      "_index": "website",
      "_type": "blog",
      "_id": "123",
      "_version": 2,
      "status": 200,
      "found": true
    }},
    { "create": {
      "_index": "website",
      "_type": "blog",
      "_id": "123",
      "_version": 3,
      "status": 201
    }},
    { "create": {
      "_index": "website",
      "_type": "blog",
      "_id": "EiwfApScQiiy7TIKfXRCTw",
      "_version": 1,
      "status": 201
    }},
    { "update": {
      "_index": "website",
      "_type": "blog",
      "_id": "123",
      "_version": 4,
      "status": 200
    }}
  ]
}
```

- <1> 所有子请求都成功完成。

每个子请求都被独立的执行，所以一个子请求的错误并不影响其它请求。如果任何一个请求失败，顶层的 error 标记将被设置为 true，然后错误的细节将在相应的请求中被报告：

```
POST /_bulk
{ "create": { "_index": "website", "_type": "blog", "_id": "123" }}
{ "title": "Cannot create - it already exists" }
{ "index": { "_index": "website", "_type": "blog", "_id": "123" }}
{ "title": "But we can update it" }
```

响应中我们将看到 create 文档 123 失败了，因为文档已经存在，但是后来的在 123 上执行的 index 请求成功了：

```
{
  "took": 3,
  "errors": true, <1>
  "items": [
    { "create": {
      "_index": "website",
      "_type": "blog",
      "_id": "123",
      "status": 409, <2>
      "error": "DocumentAlreadyExistsException <3>
        [[website][4] [blog][123]:
        document already exists]"
    }},
    { "index": {
      "_index": "website",
      "_type": "blog",
      "_id": "123",
      "_version": 5,
      "status": 200 <4>
    }
  ]
}
```

- <1> 一个或多个请求失败。
- <2> 这个请求的HTTP状态码被报告为 409 CONFLICT。
- <3> 错误消息说明了什么请求错误。
- <4> 第二个请求成功了，状态码是 200 OK。

这些说明 bulk 请求不是原子操作——它们不能实现事务。每个请求操作时分开的，所以每个请求的成功与否不干扰其它操作。

不要重复

你可能在同一个 index 下的同一个 type 里批量索引日志数据。为每个文档指定相同的元数据是多余的。就像 mget API，bulk 请求也可以在URL中使用 /_index 或 /_index/_type：

```
POST /website/_bulk
{ "index": { "_type": "log" } }
{ "event": "User logged in" }
```

你依旧可以覆盖元数据行的 _index 和 _type，在没有覆盖时它会使用URL中的值作为默认值：

```
POST /website/log/_bulk
{ "index": {} }
{ "event": "User logged in" }
{ "index": { "_type": "blog" } }
{ "title": "Overriding the default type" }
```

多大才算太大？

整个批量请求需要被加载到接受我们请求节点的内存里，所以请求越大，给其它请求可用的内存就越小。有一个最佳的 bulk 请求大小。超过这个大小，性能不再提升而且可能降低。

最佳大小，当然并不是一个固定的数字。它完全取决于你的硬件、你文档的大小和复杂度以及索引和搜索的负载。幸运的是，这个最佳点(sweetspot)还是容易找到的：

试着批量索引标准的文档，随着大小的增长，当性能开始降低，说明你每个批次的大小太大了。开始的数量可以在 1000-5000个文档之间，如果你的文档非常大，可以使用较小的批次。

通常着眼于你请求批次的物理大小是非常有用的。一千个1kB的文档和一千个1MB的文档大不相同。一个好的批次最好保持在5-15MB大小间。

结语

现在你知道如何把Elasticsearch当作一个分布式的文件存储了。你可以存储、更新、检索和删除它们，而且你知道如何安全的进行这一切。这确实非常非常有用，尽管我们还没有看到更多令人激动的特性，例如如何在文档内搜索。但让我们首先讨论下如何在分布式环境中安全的管理你的文档相关的内部流程。

分布式文档存储

在上一章，我们看到了将数据放入索引然后检索它们的所有方法。不过我们有意忽略了许多关于数据是如何在集群中分布和获取的相关技术细节。这种使用和细节分离是刻意为之的——你不需要知道数据在Elasticsearch如何分布它就会很好的工作。

这一章我们深入这些内部细节来帮助你更好的理解数据是如何在分布式系统中存储的。

注意：

下面的信息只是出于兴趣阅读，你不必为了使用Elasticsearch而弄懂和记住所有的细节。讨论的这些选项只提供给高级用户。

阅读这一部分只是让你了解下系统如何工作，并让你知道这些信息以备以后参考，所以不要被细节吓到。

路由文档到分片

当你索引一个文档，它被存储在单独一个主分片上。Elasticsearch是如何知道文档属于哪个分片的呢？当你创建一个新文档，它是如何知道是应该存储在分片1还是分片2上的呢？

进程不能是随机的，因为我们将来要检索文档。事实上，它根据一个简单的算法决定：

```
shard = hash(routing) % number_of_primary_shards
```

`routing` 值是一个任意字符串，它默认是 `_id` 但也可以自定义。这个 `routing` 字符串通过哈希函数生成一个数字，然后除以主切片的数量得到一个余数(**remainder**)，余数的范围永远是 0 到 `number_of_primary_shards - 1`，这个数字就是特定文档所在的分片。

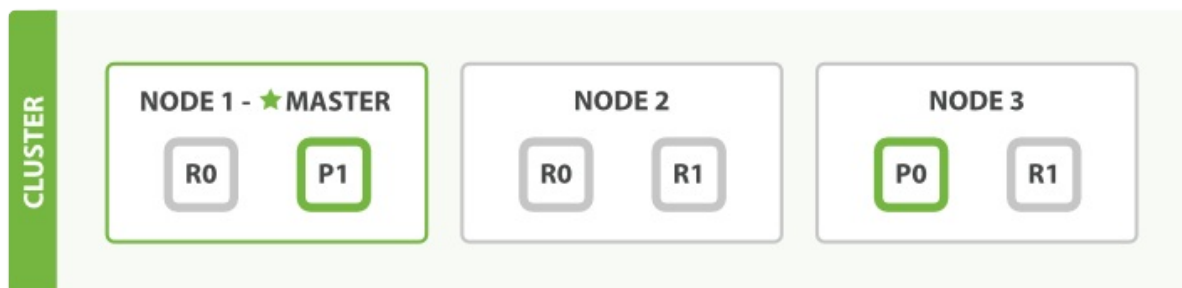
这也解释了为什么主分片的数量只能在创建索引时定义且不能修改：如果主分片的数量在未来改变了，所有先前的路由值就失效了，文档也就永远找不到了。

有时用户认为固定数量的主分片会让之后的扩展变得很困难。现实中，有些技术会在你需要的时候让扩展变得容易。我们将在《扩展》章节讨论。

所有的文档API（`get`、`index`、`delete`、`bulk`、`update`、`mget`）都接收一个 `routing` 参数，它用来自定义文档到分片的映射。自定义路由值可以确保所有相关文档——例如属于同一个人的文档——被保存在同一分片上。我们将在《扩展》章节说明你为什么需要这么做。

主分片和复制分片如何交互

为了阐述意图，我们假设有三个节点的集群。它包含一个叫做 `bblogs` 的索引并拥有两个主分片。每个主分片有两个复制分片。相同的分片不会放在同一个节点上，所以我们的集群是这样的：



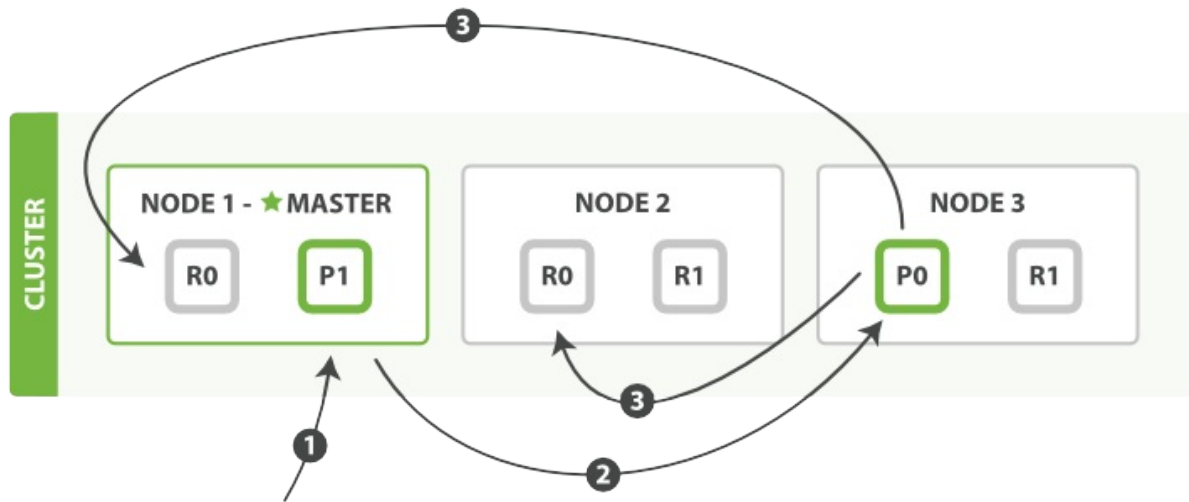
我们能够发送请求给集群中任意一个节点。每个节点都有能力处理任意请求。每个节点都知道任意文档所在的节点，所以也可以将请求转发到需要的节点。下面的例子中，我们将发送所有请求给 `Node 1`，这个节点我们将会称之为请求节点 (**requesting node**)

提示：

当我们发送请求，最好的做法是循环通过所有节点请求，这样可以平衡负载。

新建、索引和删除文档

新建、索引和删除请求都是写(write)操作，它们必须在主分片上成功完成才能复制到相关的复制分片上。



下面我们罗列在主分片和复制分片上成功新建、索引或删除一个文档必要的顺序步骤：

1. 客户端给 Node 1 发送新建、索引或删除请求。
2. 节点使用文档的 `_id` 确定文档属于分片 0。它转发请求到 Node 3，分片 0 位于这个节点上。
3. Node 3 在主分片上执行请求，如果成功，它转发请求到相应的位于 Node 1 和 Node 2 的复制节点上。当所有的复制节点报告成功，Node 3 报告成功到请求的节点，请求的节点再报告给客户端。

客户端接收到成功响应的时候，文档的修改已经被应用于主分片和所有的复制分片。你的修改生效了。

有很多可选的请求参数允许你更改这一过程。你可能想牺牲一些安全来提高性能。这一选项很少使用因为Elasticsearch已经足够快，不过为了内容的完整我们将做一些阐述。

replication

复制默认的值是 `sync`。这将导致主分片得到复制分片的成功响应后才返回。

如果你设置 `replication` 为 `async`，请求在主分片上被执行后就会返回给客户端。它依旧会转发请求给复制节点，但你将不知道复制节点成功与否。

上面的这个选项不建议使用。默认的 `sync` 复制允许Elasticsearch强制反馈传输。`async` 复制可能会因为在不等待其它分片就绪的情况下发送过多的请求而使Elasticsearch过载。

consistency

默认主分片在尝试写入时需要规定数量(**quorum**)或过半的分片（可以是主节点或复制节点）可用。这是防止数据被写入到错的网络分区。规定的数量计算公式如下：

```
int( (primary + number_of_replicas) / 2 ) + 1
```

`consistency` 允许的值为 `one`（只有一个主分片），`all`（所有主分片和复制分片）或者默认的 `quorum` 或过半分片。

注意 `number_of_replicas` 是在索引中的的设置，用来定义复制分片的数量，而不是现在活动的复制节点的数量。如果你定义了索引有3个复制节点，那规定数量是：


```
int( (primary + 3 replicas) / 2 ) + 1 = 3
```

但如果你只有2个节点，那你的活动分片不够规定数量，也就不能索引或删除任何文档。

timeout

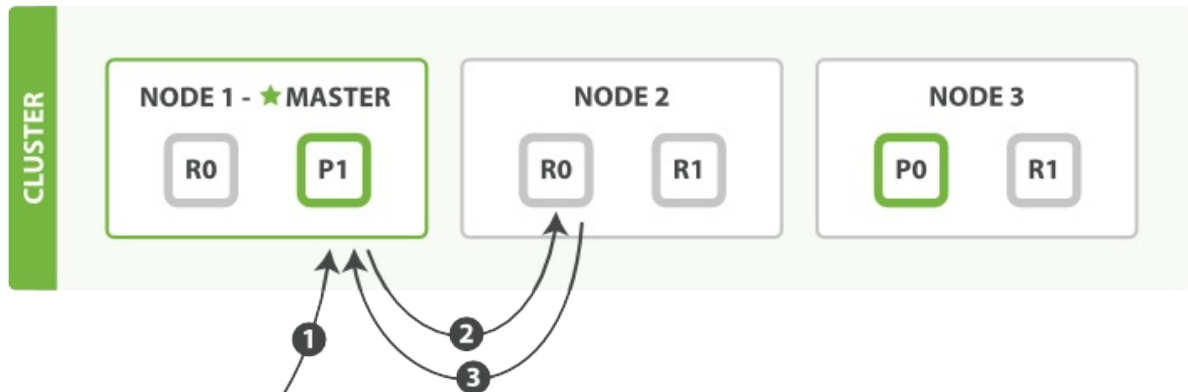
当分片副本不足时会怎样？Elasticsearch会等待更多的分片出现。默认等待一分钟。如果需要，你可以设置 `timeout` 参数让它终止的更早：`100` 表示100毫秒，`30s` 表示30秒。

注意：

新索引默认有 1 个复制分片，这意味着为了满足 quorum 的要求需要两个活动的分片。当然，这个默认设置将阻止我们在单一节点集群中进行操作。为了避开这个问题，规定数量只有在 `number_of_replicas` 大于一时才生效。

检索文档

文档能够从主分片或任意一个复制分片被检索。



下面我们罗列在主分片或复制分片上检索一个文档必要的顺序步骤：

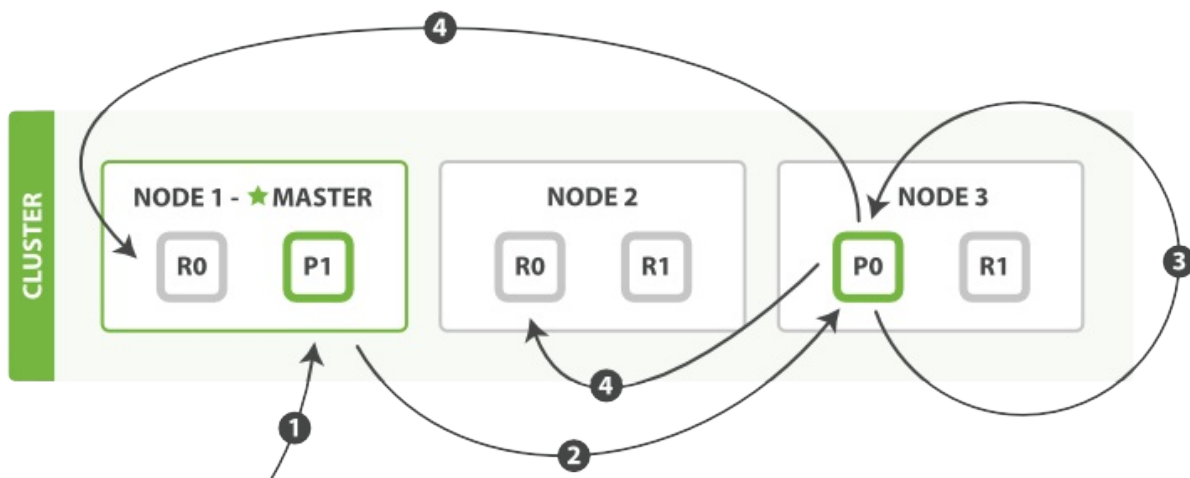
1. 客户端给 Node 1 发送get请求。
2. 节点使用文档的 `_id` 确定文档属于分片 0。分片 0 对应的复制分片在三个节点上都有。此时，它转发请求到 Node 2。
3. Node 2 返回endangered给 Node 1 然后返回给客户端。

对于读请求，为了平衡负载，请求节点会为每个请求选择不同的分片——它会循环所有分片副本。

可能的情况是，一个被索引的文档已经存在于主分片上却还没来得及同步到复制分片上。这时复制分片会报告文档未找到，主分片会成功返回文档。一旦索引请求成功返回给用户，文档则在主分片和复制分片都是可用的。

局部更新文档

`update` API 结合了之前提到的读和写的模式。



下面我们罗列执行局部更新必要的顺序步骤：

1. 客户端给 Node 1 发送更新请求。
2. 它转发请求到主分片所在节点 Node 3。
3. Node 3 从主分片检索出文档，修改 `_source` 字段的JSON，然后在主分片上重建索引。如果有其他进程修改了文档，它以 `retry_on_conflict` 设置的次数重复步骤3，都未成功则放弃。
4. 如果 Node 3 成功更新文档，它同时转发文档的新版本到 Node 1 和 Node 2 上的复制节点以重建索引。当所有复制节点报告成功，Node 3 返回成功给请求节点，然后返回给客户端。

`update` API 还接受《新建、索引和删除》章节提到的 `routing`、`replication`、`consistency` 和 `timeout` 参数。

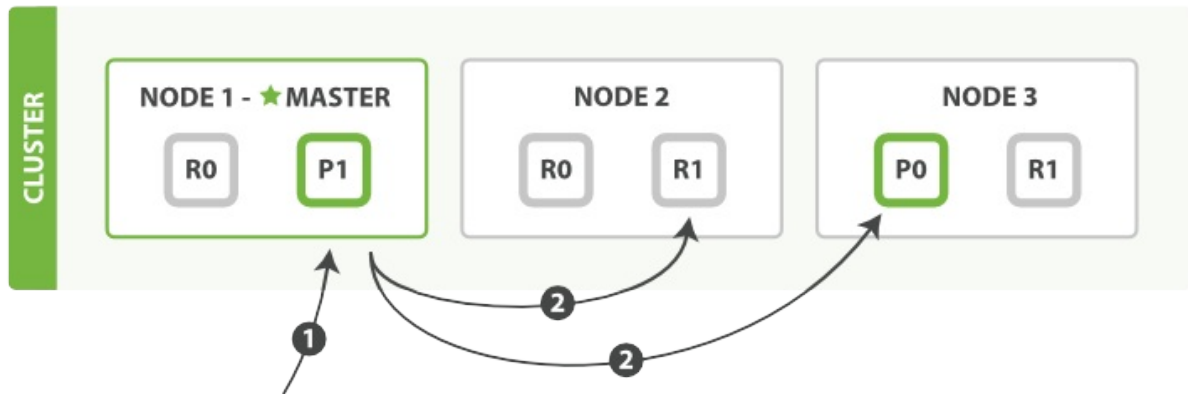
基于文档的复制

当主分片转发更改给复制分片时，并不是转发更新请求，而是转发整个文档的新版本。记住这些修改转发到复制节点是异步的，它们并不能保证到达的顺序与发送相同。如果Elasticsearch转发的仅仅是修改请求，修改的顺序可能是错误的，那得到的就是个损坏的文档。

多文档模式

`mget` 和 `bulk` API与单独的文档类似。差别是请求节点知道每个文档所在的分片。它把多文档请求拆成每个分片的对文档请求，然后转发每个参与的节点。

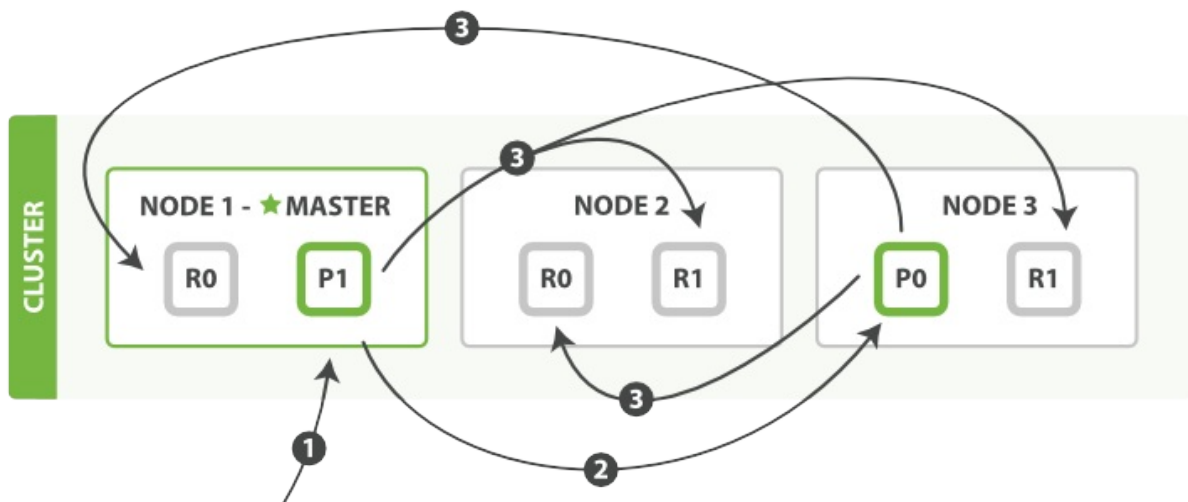
一旦接收到每个节点的应答，然后整理这些响应组合为一个单独的响应，最后返回给客户端。



下面我们将罗列通过一个 `mget` 请求检索多个文档的顺序步骤：

1. 客户端向 Node 1 发送 `mget` 请求。
2. Node 1 为每个分片构建一个多条数据检索请求，然后转发到这些请求所需的主分片或复制分片上。当所有回复被接收，Node 1 构建响应并返回给客户端。

`routing` 参数可以被 `docs` 中的每个文档设置。



下面我们将罗列使用一个 `bulk` 执行多个 `create`、`index`、`delete` 和 `update` 请求的顺序步骤：

1. 客户端向 Node 1 发送 `bulk` 请求。
2. Node 1 为每个分片构建批量请求，然后转发到这些请求所需的主分片上。
3. 主分片一个接一个的按序执行操作。当一个操作执行完，主分片转发新文档（或者删除部分）给对应的复制节点，然后执行下一个操作。复制节点为报告所有操作完成，节点报告给请求节点，请求节点整理响应并返回给客户端。

`bulk` API还可以在最上层使用 `replication` 和 `consistency` 参数，`routing` 参数则在每个请求的元数据中使用。

为什么是奇怪的格式？

当我们在《批量》一章中学习了批量请求后，你可能会问：“为什么 `bulk` API需要带换行符的奇怪格式，而不是像 `mget` API一样使用JSON数组？”

为了回答这个问题，我们需要简单的介绍一下背景：

批量中每个引用的文档属于不同的主分片，每个分片可能被分布于集群中的某个节点上。这意味着批量中的每个操作 **(action)** 需要被转发到对应的分片和节点上。

如果每个单独的请求被包装到JSON数组中，那意味着我们需要：

- 解析JSON为数组（包括文档数据，可能非常大）
- 检查每个请求决定应该到哪个分片上
- 为每个分片创建一个请求的数组
- 序列化这些数组为内部传输格式
- 发送请求到每个分片

这可行，但需要大量的RAM来承载本质上相同的数据，还要创建更多的数据结构使得JVM花更多的时间执行垃圾回收。

取而代之的，Elasticsearch则是从网络缓冲区中一行一行的直接读取数据。它使用换行符识别和解析 **action/metadata** 行，以决定哪些分片来处理这个请求。

这些行请求直接转发到对应的分片上。这些没有冗余复制，没有多余的数据结构。整个请求过程使用最小的内存在进行。

搜索——基本的工具

到目前为止，我们已经学会了如何使用elasticsearch作为一个简单的NoSQL风格的分布式文件存储器——我们可以将一个JSON文档扔给Elasticsearch，也可以根据ID检索它们。但Elasticsearch真正强大之处在于可以从混乱的数据中找出有意义的信息——从大数据到全面的信息。

这也是为什么我们使用结构化的JSON文档，而不是无结构的二进制数据。Elasticsearch不只会存储(store)文档，也会索引(indexes)文档内容来使之可以被搜索。

每个文档里的字段都会被索引并被查询。而且不仅如此。在简单查询时，Elasticsearch可以使用所有的索引，以非常快的速度返回结果。这让你永远不必考虑传统数据库的一些东西。

A search can be: 搜索(search)可以：

- 在类似于 gender 或者 age 这样的字段上使用结构化查询， join_date 这样的字段上使用排序，就像SQL的结构化查询一样。
- 全文检索，可以使用所有字段来匹配关键字，然后按照关联性(relevance)排序返回结果。
- 或者结合以上两条。

很多搜索都是开箱即用的，为了充分挖掘Elasticsearch的潜力，你需要理解以下三个概念：

概念	解释
映射(Mapping)	数据在每个字段中的解释说明
分析(Analysis)	全文是如何处理的可以被搜索的
领域特定语言查询(Query DSL)	Elasticsearch使用的灵活的、强大的查询语言

以上提到的每个点都是一个巨大的话题，我们将在《深入搜索》一章阐述它们。本章节我们将介绍这三点的一些基本概念——仅仅帮助你大致了解搜索是如何工作的。

我们将使用最简单的形式开始介绍 search API。

测试数据

本章节测试用的数据可以在这里被找到<https://gist.github.com/clintongormley/8579281>

你可以把这些命令复制到终端中执行以便可以实践本章的例子。

空搜索

最基本的搜索API表单是空搜索(**empty search**)，它没有指定任何的查询条件，只返回集群索引中的所有文档：

```
GET /_search
```

响应内容（为了编辑简洁）类似于这样：

```
{
  "hits" : {
    "total" :      14,
    "hits" : [
      {
        "_index":   "us",
        "_type":    "tweet",
        "_id":      "7",
        "_score":    1,
        "_source": {
          "date":    "2014-09-17",
          "name":    "John Smith",
          "tweet":   "The Query DSL is really powerful and flexible",
          "user_id": 2
        }
      },
      ... 9 RESULTS REMOVED ...
    ],
    "max_score" :    1
  },
  "took" :          4,
  "_shards" : {
    "failed" :       0,
    "successful" :   10,
    "total" :        10
  },
  "timed_out" :     false
}
```

hits

响应中最重要的部分是 `hits`，它包含了 `total` 字段来表示匹配到的文档总数，`hits` 数组还包含了匹配到的前10条数据。

`hits` 数组中的每个结果都包含 `_index`、`_type` 和文档的 `_id` 字段，被加入到 `_source` 字段中这意味着在搜索结果中我们将可以直接使用全部文档。这不像其他搜索引擎只返回文档ID，需要你单独去获取文档。

每个节点都有一个 `_score` 字段，这是相关性得分(**relevance score**)，它衡量了文档与查询的匹配程度。默认的，返回的结果中关联性最大的文档排在首位；这意味着，它是按照 `_score` 降序排列的。这种情况下，我们没有指定任何查询，所以所有文档的相关性是一样的，因此所有结果的 `_score` 都是取得一个中间值 `1`

`max_score` 指的是所有文档匹配查询中 `_score` 的最大值。

took

`took` 告诉我们整个搜索请求花费的毫秒数。

shards

`_shards` 节点告诉我们参与查询的分片数（`total` 字段），有多少是成功的（`successful` 字段），有多少的是失败的（`failed` 字段）。通常我们不希望分片失败，不过这个有可能发生。如果我们遭受一些重大的故障导致主分片和复制分片都故障，那这个分片的数据将无法响应给搜索请求。这种情况下，Elasticsearch将报告分片 `failed`，但仍将继续返回剩余分片

上的结果。

==== `timeout`

timeout

`time_out` 值告诉我们查询超时与否。一般的，搜索请求不会超时。如果响应速度比完整的结果更重要，你可以定义 `timeout` 参数为 `10` 或者 `10ms`（10毫秒），或者 `1s`（1秒）

```
GET /_search?timeout=10ms
```

Elasticsearch将返回在请求超时前收集到的结果。

超时不是一个断路器（circuit breaker）（译者注：关于断路器的理解请看警告）。

警告

需要注意的是 `timeout` 不会停止执行查询，它仅仅告诉你目前顺利返回结果的节点然后关闭连接。在后台，其他分片可能依旧执行查询，尽管结果已经被发送。

使用超时是因为对于你的业务需求（译者注：SLA，Service-Level Agreement服务等级协议，在此我翻译为业务需求）来说非常重要，而不是因为你想中断执行长时间运行的查询。

多索引和多类别

你注意到空搜索的结果中不同类型的文档—— `user` 和 `tweet` ——来自于不同的索引—— `us` 和 `gb` 。

通过限制搜索的不同索引或类型，我们可以在集群中跨所有文档搜索。Elasticsearch转发搜索请求到集群中平行的主分片或每个分片的复制分片上，收集结果后选择顶部十个返回给我们。

通常，当然，你可能想搜索一个或几个自定的索引或类型，我们能通过定义URL中的索引或类型达到这个目的，像这样：

```
/_search
```

在所有索引的所有类型中搜索

```
/gb/_search
```

在索引 `gb` 的所有类型中搜索

```
/gb,us/_search
```

在索引 `gb` 和 `us` 的所有类型中搜索

```
/g*,u*/_search
```

在以 `g` 或 `u` 开头的索引的所有类型中搜索

```
/gb/user/_search
```

在索引 `gb` 的类型 `user` 中搜索

```
/gb,us/user,tweet/_search
```

在索引 `gb` 和 `us` 的类型为 `user` 和 `tweet` 中搜索

```
/_all/user,tweet/_search
```

在所有索引的 `user` 和 `tweet` 中搜索 `search types user and tweet in all indices`

当你搜索包含单一索引时，Elasticsearch转发搜索请求到这个索引的主分片或每个分片的复制分片上，然后聚集每个分片的结果。搜索包含多个索引也是同样的方式——只不过或有更多的分片被关联。

重要

搜索一个索引有5个主分片和5个索引各有一个分片事实上是一样的。

接下来，你将看到这些简单的情况如何灵活的扩展以适应你需求的变更。

分页

《空搜索》一节告诉我们在集群中有14个文档匹配我们的（空）搜索语句。单数只有10个文档在 `hits` 数组中。我们如何看到其他文档？

和SQL使用 `LIMIT` 关键字返回只有一页的结果一样，Elasticsearch接受 `from` 和 `size` 参数：

`size`：果数，默认 10

`from`：跳过开始的结果数，默认 0

如果你想每页显示5个结果，页码从1到3，那请求如下：

```
GET /_search?size=5
GET /_search?size=5&from=5
GET /_search?size=5&from=10
```

应该当心分页太深或者一次请求太多的结果。结果在返回前会被排序。但是记住一个搜索请求常常涉及多个分片。每个分片生成自己排好序的结果，它们接着需要集中起来排序以确保整体排序正确。

在集群系统中深度分页

为了理解为什么深度分页是有问题的，让我们假设在一个有5个主分片的索引中搜索。当我们请求结果的第一页（结果1到10）时，每个分片产生自己最顶端10个结果然后返回它们给请求节点(**requesting node**)，它再排序这所有的50个结果以选出顶端的10个结果。

现在假设我们请求第1000页——结果10001到10010。工作方式都相同，不同的是每个分片都必须产生顶端的10010个结果。然后请求节点排序这50050个结果并丢弃50040个！

你可以看到在分布式系统中，排序结果的花费随着分页的深入而成倍增长。这也是为什么网络搜索引擎中任何语句不能返回多于1000个结果的原因。

TIP

在《重建索引》章节我们将阐述如何能高效的检索大量文档

简易搜索

`search` API有两种表单：一种是“简易版”的查询字符串(**query string**)将所有参数通过查询字符串定义，另一种版本使用JSON完整的表示请求体(**request body**)，这种富搜索语言叫做结构化查询语句 (DSL)

查询字符串搜索对于在命令行下运行点对点(**ad hoc**)查询特别有用。例如这个语句查询所有类型为 `tweet` 并在 `tweet` 字段中包含 `elasticsearch` 字符的文档：

```
GET /_all/tweet/_search?q=tweet:elasticsearch
```

下一个语句查找 `name` 字段中包含 "john" 和 `tweet` 字段包含 "mary" 的结果。实际的查询只需要：

```
+name:john +tweet:mary
```

但是百分比编码(**percent encoding**) (译者注：就是url编码) 需要将查询字符串参数变得更加神秘：

```
GET /_search?q=%2Bname%3Ajohn+%2Btweet%3Amary
```

"+" 前缀表示语句匹配条件必须被满足。类似的 "-" 前缀表示条件必须不被满足。所有条件如果没有 + 或 - 表示是可选的——匹配越多，相关的文档就越多。

`_all` 字段

返回包含 "mary" 字符的所有文档的简单搜索：

```
GET /_search?q=mary
```

在前一个例子中，我们搜索 `tweet` 或 `name` 字段中包含某个字符的结果。然而，这个语句返回的结果在三个不同的字段中包含 "mary"：

- 用户的名字是“Mary”
- “Mary”发的六个推文
- 针对“@mary”的一个推文

Elasticsearch是如何设法找到三个不同字段的结果的？

当你索引一个文档，Elasticsearch把所有字符串字段值连接起来放在一个大字符串中，它被索引为一个特殊的字段 `_all`。例如，当索引这个文档：

```
{
  "tweet": "However did I manage before Elasticsearch?",
  "date": "2014-09-14",
  "name": "Mary Jones",
  "user_id": 1
}
```

这好比我们增加了一个叫做 `_all` 的额外字段值：

```
"However did I manage before Elasticsearch? 2014-09-14 Mary Jones 1"
```

查询字符串在其他字段被定以前使用 `_all` 字段搜索。

TIP

`_all` 字段对于开始一个新应用时是一个有用的特性。之后，如果你定义字段来代替 `_all` 字段，你的搜索结果将更加可控。当 `_all` 字段不再使用，你可以停用它，这个会在《全字段》章节阐述。

更复杂的语句

下一个搜索推特的语句：

`_all` field

- `name` 字段包含 "mary" 或 "john"
- `date` 晚于 2014-09-10
- `_all` 字段包含 "aggregations" 或 "geo"

```
+name:(mary john) +date:>2014-09-10 +(aggregations geo)
```

编码后的查询字符串变得不太容易阅读：

```
?q=%2Bname%3A(mary+john)+%2Bdate%3A%3E2014-09-10+%2B(aggregations+geo)
```

就像你上面看到的例子，简单(**lite**)查询字符串搜索惊人的强大。它的查询语法，会在《查询字符串语法》章节阐述。参考文档允许我们简洁明快的表示复杂的查询。这对于命令行下一次性查询或者开发模式下非常有用。

然而，你可以看到简洁带来了隐晦和调试困难。而且它很脆弱——查询字符串中一个细小的语法错误，像 `-`、`:`、`/` 或 `"` 错位就会导致返回错误而不是结果。

最后，查询字符串搜索允许任意用户在索引中任何一个字段上运行潜在的慢查询语句，可能暴露私有信息甚至使你的集群瘫痪。

TIP

因为这些原因，我们不建议直接暴露查询字符串搜索给用户，除非这些用户对于你的数据和集群可信。

取而代之的，生产环境我们一般依赖全功能的请求体搜索API，它能完成前面所有的事情，甚至更多。在了解它们之前，我们首先需要看看数据是如何在Elasticsearch中被索引的。

映射(**mapping**)机制用于进行字段类型确认，将每个字段匹配为一种确定的数据类型(`string` , `number` , `booleans` , `date` 等)。

分析(**analysis**)机制用于进行全文文本(**Full Text**)的分词，以建立供搜索用的反向索引。

映射及分析

当在索引中处理数据时，我们注意到一些奇怪的事。有些东西似乎被破坏了：

在索引中有12个tweets，只有一个包含日期 2014-09-15，但是我们看看下面查询中的 total hits。

```
GET /_search?q=2014           # 12 个结果
GET /_search?q=2014-09-15     # 还是 12 个结果！
GET /_search?q=date:2014-09-15 # 1 一个结果
GET /_search?q=date:2014      # 0 个结果！
```

为什么全日期的查询返回所有的tweets，而针对 date 字段进行年度查询却什么都不返回？为什么我们的结果因查询 _all 字段(译者注：默认所有字段中进行查询)或 date 字段而变得不同？

想必是因为我们的数据在 _all 字段的索引方式和在 date 字段的索引方式不同而导致。

让我们看看Elasticsearch在对 gb 索引中的 tweet 类型进行mapping(也称之为模式定义[注：此词有待重新定义(schema definition)])后是如何解读我们的文档结构：

```
GET /gb/_mapping/tweet
```

返回：

```
{
  "gb": {
    "mappings": {
      "tweet": {
        "properties": {
          "date": {
            "type": "date",
            "format": "dateOptionalTime"
          },
          "name": {
            "type": "string"
          },
          "tweet": {
            "type": "string"
          },
          "user_id": {
            "type": "long"
          }
        }
      }
    }
  }
}
```

Elasticsearch为对字段类型进行猜测，动态生成了字段和类型的映射关系。返回的信息显示了 date 字段被识别为 date 类型。_all 因为是默认字段所以没有在此显示，不过我们知道它是 string 类型。

date 类型的字段和 string 类型的字段的索引方式是不同的，因此导致查询结果的不同，这并不会让我们觉得惊讶。

你会期望每一种核心数据类型(strings, numbers, booleans及dates)以不同的方式进行索引，而这点也是现实：在Elasticsearch中他们是被区别对待的。

但是更大的区别在于确切值(exact values)(比如 string 类型)及全文文本(full text)之间。

这两者的区别才真的很重要 - 这是区分搜索引擎和其他数据库的根本差异。

确切值(Exact values) vs. 全文文本(Full text)

Elasticsearch中的数据可以大致分为两种类型：

确切值 及 全文文本。

确切值是确定的，正如它的名字一样。比如一个date或用户ID，也可以包含更多的字符串比如username或email地址。

确切值 "Foo" 和 "foo" 就并不相同。确切值 2014 和 2014-09-15 也不相同。

全文文本，从另一个角度来说文本化的数据(常常以人类的语言书写)，比如一片推文(Twitter的文章)或邮件正文。

全文文本常常被称为 非结构化数据，其实是一种用词不当的称谓，实际上自然语言是高度结构化的。

问题是自然语言的语法规则是如此的复杂，计算机难以正确解析。例如这个句子：

```
May is fun but June bores me.
```

到底是说的月份还是人呢？

确切值是很容易查询的，因为结果是二进制的 -- 要么匹配，要么不匹配。下面的查询很容易以SQL表达：

```
WHERE name      = "John Smith"
      AND user_id = 2
      AND date    > "2014-09-15"
```

而对于全文数据的查询来说，却有些微妙。我们不会去询问 这篇文档是否匹配查询要求？。但是，我们会询问 这篇文档和查询的匹配程度如何？。换句话说，对于查询条件，这篇文档的相关性有多高？

我们很少确切的匹配整个全文文本。我们想在全文中查询包含查询文本的部分。不仅如此，我们还期望搜索引擎能理解我们的意图：

- 一个针对 "uk" 的查询将返回涉及 "United Kingdom" 的文档
- 一个针对 "jump" 的查询同时能够匹配 "jumped"，"jumps"，"jumping" 甚至 "leap"
- "johnny walker" 也能匹配 "Johnnie Walker"，"johnnie depp" 及 "Johnny Depp"
- "fox news hunting" 能返回有关hunting on Fox News的故事，而 "fox hunting news" 也能返回关于fox hunting的新闻故事。

为了方便在全文文本字段中进行这些类型的查询，Elasticsearch首先对文本分析(analyzes)，然后使用结果建立一个倒排索引。我们将在以下两个章节讨论倒排索引及分析过程。

倒排索引

Elasticsearch使用一种叫做倒排索引(**inverted index**)的结构来做快速的全文搜索。倒排索引由在文档中出现的唯一的单词列表，以及对于每个单词在文档中的位置组成。

例如，我们有两个文档，每个文档 `content` 字段包含：

- 1. The quick brown fox jumped over the lazy dog
- 2. Quick brown foxes leap over lazy dogs in summer

为了创建倒排索引，我们首先切分每个文档的 `content` 字段为单独的单词（我们把它叫做词(**terms**)或者表征(**tokens**)）（译者注：关于 `terms` 和 `tokens` 的翻译比较生硬，只需知道语句分词后的个体叫做这两个。），把所有的唯一词放入列表并排序，结果是这个样子的：

Term	Doc_1	Doc_2
Quick		X
The	X	
brown	X	X
dog	X	
dogs		X
fox	X	
foxes		X
in		X
jumped	X	
lazy	X	X
leap		X
over	X	X
quick	X	
summer		X
the	X	

现在，如果我们想搜索 `"quick brown"`，我们只需要找到每个词在哪个文档中出现既可：

Term	Doc_1	Doc_2
brown	X	X
quick	X	
-----	-----	-----
Total	2	1

两个文档都匹配，但是第一个比第二个有更多的匹配项。如果我们加入简单的相似度算法(**similarity algorithm**)，计算匹配单词的数目，这样我们就可以说第一个文档比第二个匹配度更高——对于我们的查询具有更多相关性。

但是在我们的倒排索引中还有些问题：

- 1. `"Quick"` 和 `"quick"` 被认为是不同的单词，但是用户可能认为它们是相同的。
- 2. `"fox"` 和 `"foxes"` 很相似，就像 `"dog"` 和 `"dogs"` ——它们都是同根词。
- 3. `"jumped"` 和 `"leap"` 不是同根词，但意思相似——它们是同义词。

上面的索引中，搜索 "+Quick +fox" 不会匹配任何文档（记住，前缀 + 表示单词必须匹配到）。只有 "Quick" 和 "fox" 都在同一文档中才可以匹配查询，但是第一个文档包含 "quick fox" 且第二个文档包含 "Quick foxes"。（译者注：这段真罗嗦，说白了就是单复数和同义词没法匹配）

用户可以合理的希望两个文档都能匹配查询，我们也可以做的更好。

如果我们将词为统一为标准格式，这样就可以找到不是确切匹配查询，但是足以相似从而可以关联的文档。例如：

- 1. "Quick" 可以转为小写成为 "quick"。
- 2. "foxes" 可以被转为根形式 ""fox。同理 "dogs" 可以被转为 "dog"。
- 3. "jumped" 和 "leap" 同义就可以只索引为单个词 "jump"

现在的索引：

Term	Doc_1	Doc_2
brown	X	X
dog	X	X
fox	X	X
in		X
jump	X	X
lazy	X	X
over	X	X
quick	X	X
summer		X
the	X	X

但我们还未成功。我们的搜索 "+Quick +fox" 依旧失败，因为 "Quick" 的确切值已经不在索引里，不过，如果我们使用相同的标准化规则处理查询字符串的 content 字段，查询将变成 "+quick +fox"，这样就可以匹配到两个文档。

IMPORTANT

这很重要。你只可以找到确实存在于索引中的词，所以索引文本和查询字符串都要标准化为相同的形式。

这个表征化和标准化的过程叫做分词(analysis)，这个在下节中我们讨论。

分析和分析器

分析(**analysis**)是这样一个过程：

- 首先，表征化一个文本块为适用于倒排索引单独的词(**term**)
- 然后标准化这些词为标准形式，提高它们的“可搜索性”或“查全率”

这个工作是分析器(**analyzer**)完成的。一个分析器(**analyzer**)只是一个包装用于将三个功能放到一个包里：

字符过滤器

首先字符串经过字符过滤器(**character filter**)，它们的工作是在表征化（译者注：这个词叫做断词更合适）前处理字符串。字符过滤器能够去除HTML标记，或者转换 "&" 为 "and"。

分词器

下一步，分词器(**tokenizer**)被表征化（断词）为独立的词。一个简单的分词器(**tokenizer**)可以根据空格或逗号将单词分开（译者注：这个在中文中不适用）。

表征过滤

最后，每个词都通过所有表征过滤(**token filters**)，它可以修改词（例如将 "Quick" 转为小写），去掉词（例如停用词像 "a"、"and"、"the" 等等），或者增加词（例如同义词像 "jump" 和 "leap"）

Elasticsearch提供很多开箱即用的字符过滤器，分词器和表征过滤器。这些可以组合来创建自定义的分析器以应对不同的需求。我们将在《自定义分析器》章节详细讨论。

内建的分析器

不过，Elasticsearch还附带了一些预装的分析器，你可以直接使用它们。下面我们列出了最重要的几个分析器，来演示这个字符串分词后的表现差异：

```
"Set the shape to semi-transparent by calling set_trans(5)"
```

标准分析器

标准分析器是Elasticsearch默认使用的分析器。对于文本分析，它对于任何语言都是最佳选择（译者注：就是没啥特殊需求，对于任何一个国家的语言，这个分析器就够用了）。它根据Unicode Consortium的定义的单词边界(**word boundaries**)来切分文本，然后去掉大部分标点符号。最后，把所有词转为小写。产生的结果为：

```
set, the, shape, to, semi, transparent, by, calling, set_trans, 5
```

简单分析器

简单分析器将非单个字母的文本切分，然后把每个词转为小写。产生的结果为：

```
set, the, shape, to, semi, transparent, by, calling, set, trans
```

空格分析器

空格分析器依据空格切分文本。它不转换小写。产生结果为：

```
Set, the, shape, to, semi-transparent, by, calling, set_trans(5)
```

语言分析器

特定语言分析器适用于很多语言。它们能够考虑到特定语言的特性。例如，`english` 分析器自带一套英语停用词库——像 `and` 或 `the` 这些与语义无关的通用词。这些词被移除后，因为语法规则的存在，英语单词的主体含义依旧能被理解（译者注：`stem English words` 这句不知道该如何翻译，查了字典，我理解的大概意思应该是将英语语句比作一株植物，去掉无用的枝叶，主干依旧存在，停用词好比枝叶，存在与否并不影响对这句话的理解。）。

`english` 分析器将会产生以下结果：

```
set, shape, semi, transpar, call, set_tran, 5
```

注意 `"transparent"`、`"calling"` 和 `"set_trans"` 是如何转为词干的。

当分析器被使用

当我们索引(**index**)一个文档，全文字段会被分析为单独的词来创建倒排索引。不过，当我们在全文字段搜索(**search**)时，我们要让查询字符串经过同样的分析流程处理，以确保这些词在索引中存在。

全文查询我们将在稍后讨论，理解每个字段是如何定义的，这样才可以让它们做正确的事：

- 当你查询全文(**full text**)字段，查询将使用相同的分析器来分析查询字符串，以产生正确的词列表。
- 当你查询一个确切值(**exact value**)字段，查询将不分析查询字符串，但是你可以自己指定。

现在你可以明白为什么《映射和分析》的开头会产生那种结果：

- `date` 字段包含一个确切值：单独的一个词 `"2014-09-15"`。
- `_all` 字段是一个全文字段，所以分析过程将日期转为三个词：`"2014"`、`"09"` 和 `"15"`。

当我们在 `_all` 字段查询 `2014`，它一个匹配到12条推文，因为这些推文都包含词 `2014`：

```
GET /_search?q=2014 # 12 results
```

当我们在 `_all` 字段中查询 `2014-09-15`，首先分析查询字符串，产生匹配任一词 `2014`、`09` 或 `15` 的查询语句，它依旧匹配12个推文，因为它们都包含词 `2014`。

```
GET /_search?q=2014-09-15 # 12 results !
```

当我们在 `date` 字段中查询 `2014-09-15`，它查询一个确切的日期，然后只找到一条推文：

```
GET /_search?q=date:2014-09-15 # 1 result
```

当我们在 `date` 字段中查询 `2014`，没有找到文档，因为没有文档包含那个确切的日期：

```
GET /_search?q=date:2014 # 0 results !
```

测试分析器

尤其当你是Elasticsearch新手时，对于如何分词以及存储到索引中理解起来比较困难。为了更好的理解如何进行，你可以使

用 `analyze` API来查看文本是如何被分析的。在查询字符串参数中指定要使用的分析器，被分析的文本做为请求体：

```
GET /_analyze?analyzer=standard
Text to analyze
```

结果中每个节点在代表一个词：

```
{
  "tokens": [
    {
      "token": "text",
      "start_offset": 0,
      "end_offset": 4,
      "type": "<ALPHANUM>",
      "position": 1
    },
    {
      "token": "to",
      "start_offset": 5,
      "end_offset": 7,
      "type": "<ALPHANUM>",
      "position": 2
    },
    {
      "token": "analyze",
      "start_offset": 8,
      "end_offset": 15,
      "type": "<ALPHANUM>",
      "position": 3
    }
  ]
}
```

`token` 是一个实际被存储在索引中的词。`position` 指明词在原文本中是第几个出现的。`start_offset` 和 `end_offset` 表示词在原文本中占据的位置。

`analyze` API 对于理解Elasticsearch索引的内在细节是个非常有用的工具，随着内容的推进，我们将继续讨论它。

指定分析器

当Elasticsearch在你的文档中探测到一个新的字符串字段，它将自动设置它为全文 `string` 字段并用 `standard` 分析器分析。

你不可能总是想要这样做。也许你想使用一个更适合这个数据的语言分析器。或者，你只想把字符串字段当作一个普通的字段——不做任何分析，只存储确切值，就像字符串类型的用户ID或者内部状态字段或者标签。

为了达到这种效果，我们必须通过映射(mapping)人工设置这些字段。

映射

正如《数据吞吐》一节所说，索引中每个文档都有一个类型(**type**)。每个类型拥有自己的映射(**mapping**)或者模式定义(**schema definition**)。一个映射定义了字段类型，每个字段的数据类型，以及字段被Elasticsearch处理的方式。映射还用于设置关联到类型上的元数据。

在《映射》章节我们将探讨映射的细节。这节我们只是带你入门。

核心简单字段类型

Elasticsearch支持以下简单字段类型：

类型	表示的数据类型
String	string
Whole number	byte , short , integer , long
Floating point	float , double
Boolean	boolean
Date	date

当你索引一个包含新字段的文档——一个之前没有的字段——Elasticsearch将使用动态映射猜测字段类型，这类型来自于JSON的基本数据类型，使用以下规则：

JSON type	Field type
Boolean: true OR false	"boolean"
Whole number: 123	"long"
Floating point: 123.45	"double"
String, valid date: "2014-09-15"	"date"
String: "foo bar"	"string"

注意

这意味着，如果你索引一个带引号的数字——"123"，它将被映射为 "string" 类型，而不是 "long" 类型。然而，如果字段已经被映射为 "long" 类型，Elasticsearch将尝试转换字符串为long，并在转换失败时会抛出异常。

查看映射

我们可以使用 `_mapping` 后缀来查看Elasticsearch中的映射。在本章开始我们已经找到索引 `gb` 类型 `tweet` 中的映射：

```
GET /gb/_mapping/tweet
```

这展示给了我们字段的映射（叫做属性(**properties**)），这些映射是Elasticsearch在创建索引时动态生成的：

```
{
  "gb": {
    "mappings": {
      "tweet": {
        "properties": {
          "date": {
            "type": "date",
            "format": "dateOptionalTime"
          },

```

```
        "name": {
            "type": "string"
        },
        "tweet": {
            "type": "string"
        },
        "user_id": {
            "type": "long"
        }
    }
}
}
```

小提示

错误的映射，例如把 `age` 字段映射为 `string` 类型而不是 `integer` 类型，会造成查询结果混乱。

要检查映射类型，而不是假设它是正确的！

自定义字段映射

映射中最重要的字段参数是 `type`。除了 `string` 类型的字段，你可能很少需要映射其他的 `type`：

```
{
  "number_of_clicks": {
    "type": "integer"
  }
}
```

`string` 类型的字段，默认的，考虑到包含全文本，它们的值在索引前要经过分析器分析，并且在全文搜索此字段前要把查询语句做分析处理。

对于 `string` 字段，两个最重要的映射参数是 `index` 和 `analyzer`。

index

`index` 参数控制字符串以何种方式被索引。它包含以下三个值中的一个：

值	解释
<code>analyzed</code>	首先分析这个字符串，然后索引。换言之，以全文形式索引此字段。
<code>not_analyzed</code>	索引这个字段，使之可以被搜索，但是索引内容和指定值一样。不分析此字段。
<code>no</code>	不索引这个字段。这个字段不能为搜索到。

`string` 类型字段默认值是 `analyzed`。如果我们想映射字段为确切值，我们需要设置它为 `not_analyzed`：

```
{
  "tag": {
    "type": "string",
    "index": "not_analyzed"
  }
}
```

其他简单类型——`long`、`double`、`date` 等等——也接受 `index` 参数，但相应的值只能是 `no` 和 `not_analyzed`，它们的值不能被分析。

分析

对于 `analyzed` 类型的字符串字段，使用 `analyzer` 参数来指定哪一种分析器将在搜索和索引的时候使用。默认的，Elasticsearch使用 `standard` 分析器，但是你可以通过指定一个内建的分析器来更改它，例如 `whitespace`、`simple` 或 `english`。

```
{
  "tweet": {
    "type": "string",
    "analyzer": "english"
  }
}
```

在《自定义分析器》章节我们将告诉你如何定义和使用自定义的分析器。

更新映射

你可以在第一次创建索引的时候指定映射的类型。此外，你也可以晚些时候为新类型添加映射（或者为已有的类型更新映射）。

重要

你可以向已有映射中增加字段，但你不能修改它。如果一个字段在映射中已经存在，这可能意味着那个字段的数据已经被索引。如果你改变了字段映射，那已经被索引的数据将错误并且不能被正确的搜索到。

我们可以更新一个映射来增加一个新字段，但是不能把已有字段的类型那个从 `analyzed` 改到 `not_analyzed`。

为了演示两个指定的映射方法，让我们首先删除索引 `gb`：

```
DELETE /gb
```

然后创建一个新索引，指定 `tweet` 字段的分析器为 `english`：

```
PUT /gb <1>
{
  "mappings": {
    "tweet" : {
      "properties" : {
        "tweet" : {
          "type" : "string",
          "analyzer": "english"
        },
        "date" : {
          "type" : "date"
        },
        "name" : {
          "type" : "string"
        },
        "user_id" : {
          "type" : "long"
        }
      }
    }
  }
}
```

<1> 这将创建包含 `mappings` 的索引，映射在请求体中指定。

再后来，我们决定在 `tweet` 的映射中增加一个新的 `not_analyzed` 类型的文本字段，叫做 `tag`，使用 `_mapping` 后缀：

```
PUT /gb/_mapping/tweet
{
  "properties" : {
    "tag" : {
```

```
    "type" :    "string",
    "index":    "not_analyzed"
  }
}
```

注意到我们不再需要列出所有的已经存在的字段，因为我们没法修改他们。我们的新字段已经被合并至存在的那个映射中。

测试映射

你可以通过名字使用 `analyze` API测试字符串字段的映射。对比这两个请求的输出：

```
GET /gb/_analyze?field=tweet
Black-cats <1>

GET /gb/_analyze?field=tag
Black-cats <1>
```

<1> 我们想要分析的文本被放在请求体中。

`tweet` 字段产生两个词，`"black"` 和 `"cat"`，`tag` 字段产生单独的一个词 `"Black-cats"`。换言之，我们的映射工作正常。

复合核心字段类型

除了之前提到的简单的标量类型，JSON还有 `null` 值，数组和对象，所有这些Elasticsearch都支持：

多值字段

我们想让 `tag` 字段包含多个字段，这非常有可能发生。我们可以索引一个标签数组来代替单一字符串：

```
{ "tag": [ "search", "nosql" ] }
```

对于数组不需要特殊的映射。任何一个字段可以包含零个、一个或多个值，同样对于全文字段将被分析并产生多个词。

言外之意，这意味着数组中所有值必须为同一类型。你不能把日期和字符串混合。如果你创建一个新字段，这个字段索引了一个数组，Elasticsearch将使用第一个值的类型来确定这个新字段的类型。

当你从Elasticsearch中取回一个文档，任何一个数组的顺序和你索引它们的顺序一致。你取回的 `_source` 字段的顺序同样与索引它们的顺序相同。

然而，数组是做为多值字段被索引的，它们没有顺序。在搜索阶段你不能指定“第一个值”或者“最后一个值”。倒不如把数组当作一个值集合(gag of values)

==== Empty fields

空字段

当然数组可以是空的。这等价于有零个值。事实上，Lucene没法存放 `null` 值，所以一个 `null` 值的字段被认为是空字段。

这四个字段将被识别为空字段而不被索引：

```
"empty_string":      "",
"null_value":        null,
"empty_array":        [],
"array_with_null_value": [ null ]
```

多层对象

我们需要讨论的最后一个自然JSON数据类型是对象(object)——在其它语言中叫做hashed、hashmaps、dictionaries 或者 associative arrays.

内部对象(inner objects)经常用于嵌入一个实体或对象里的另一个地方。例如，做在 `tweet` 文档中 `user_name` 和 `user_id` 的替代，我们可以这样写：

```
{
  "tweet": "Elasticsearch is very flexible",
  "user": {
    "id": "@johnsmith",
    "gender": "male",
    "age": 26,
    "name": {
      "full": "John Smith",
      "first": "John",
      "last": "Smith"
    }
  }
}
```

内部对象的映射

Elasticsearch 会动态的检测新对象的字段，并且映射它们为 `object` 类型，将每个字段加到 `properties` 字段下

```
{
  "gb": {
    "tweet": { <1>
      "properties": {
        "tweet": { "type": "string" },
        "user": { <2>
          "type": "object",
          "properties": {
            "id": { "type": "string" },
            "gender": { "type": "string" },
            "age": { "type": "long" },
            "name": { <2>
              "type": "object",
              "properties": {
                "full": { "type": "string" },
                "first": { "type": "string" },
                "last": { "type": "string" }
              }
            }
          }
        }
      }
    }
  }
}
```

<1> 根对象.

<2> 内部对象.

The mapping for the `user` and `name` fields have a similar structure to the mapping for the `tweet` type itself. In fact, the `type` mapping is just a special type of `object` mapping, which we refer to as the *root object*. It is just the same as any other object, except that it has some special top-level fields for document metadata, like `_source`, the `_all` field etc.

对 `user` 和 `name` 字段的映射与 `tweet` 类型自己很相似。事实上，`type` 映射只是 `object` 映射的一种特殊类型，我们将 `object` 称为根对象。它与其他对象一模一样，除非它有一些特殊的顶层字段，比如 `_source`，`_all` 等等。

内部对象是怎样被索引的

Lucene doesn't understand inner objects. A Lucene document consists of a flat list of key-value pairs. In order for Elasticsearch to index inner objects usefully, it converts our document into something like this:

```
{
  "tweet": [elasticsearch, flexible, very],
  "user.id": [@johnsmith],
  "user.gender": [male],
  "user.age": [26],
  "user.name.full": [john, smith],
  "user.name.first": [john],
  "user.name.last": [smith]
}
```

Inner fields can be referred to by name, eg `"first"`. To distinguish between two fields that have the same name we can use the full *path*, eg `"user.name.first"` or even the *type* name plus the path: `"tweet.user.name.first"`.

NOTE: In the simple flattened document above, there is no field called `user` and no field called `user.name`. Lucene only indexes scalar or simple values, not complex datastructures.

[[object-arrays]] === Arrays of inner objects

Finally, consider how an array containing inner objects would be indexed. Let's say we have a `followers` array which looks

like this:

[source,js]

```
{ "followers": [ { "age": 35, "name": "Mary White"}, { "age": 26, "name": "Alex Jones"}, { "age": 19, "name": "Lisa Smith"} ] }
```

This document will be flattened as we described above, but the result will look like this:

[source,js]

```
{ "followers.age": [19, 26, 35], "followers.name": [alex, jones, lisa, smith, mary, white] }
```

The correlation between `{age: 35}` and `{name: Mary White}` has been lost as each multi-value field is just a bag of values, not an ordered array. This is sufficient for us to ask:

- *Is there a follower who is 26 years old?*

but we can't get an accurate answer to:

- *Is there a follower who is 26 years old **and who is called Alex Jones?***

Correlated inner objects, which are able to answer queries like these, are called *nested* objects, and we will discuss them later on in <>.

请求体查询

简单查询语句(lite)是一种有效的命令行`adhoc`查询。但是，如果你想要善用搜索，你必须使用请求体查询(request body search) API。之所以这么称呼，是因为大多数的参数以JSON格式所容纳而非查询字符串。

请求体查询(下文简称查询)，并不仅仅用来处理查询，而且还可以高亮返回结果中的片段，并且给出帮助你的用户找寻最好结果的相关数据建议。

空查询

我们以最简单的 `search` API开始，空查询将会返回索引中所有的文档。

```
GET /_search
{} <1>
```

- `<1>` 这是一个空查询数据。

同字符串查询一样，你可以查询一个，多个或 `_all` 索引(indices)或类型(types)：

```
GET /index_2014*/type1,type2/_search
{}
```

你可以使用 `from` 及 `size` 参数进行分页：

```
GET /_search
{
  "from": 30,
  "size": 10
}
```

携带内容的 GET 请求？

任何一种语言(特别是js)的HTTP库都不允许 GET 请求中携带交互数据。事实上，有些用户很惊讶 GET 请求中居然会允许携带交互数据。

真实情况是，<http://tools.ietf.org/html/rfc7231#page-24>[RFC 7231]，一份规定HTTP语义及内容的RFC中并未规定 GET 请求中允许携带交互数据！所以，有些HTTP服务允许这种行为，而另一些(特别是缓存代理)，则不允许这种行为。

Elasticsearch的作者们倾向于使用 GET 提交查询请求，因为他们觉得这个词相比 POST 来说，能更好的描述这种行为。然而，因为携带交互数据的 GET 请求并不被广泛支持，所以 `search` API同样支持 POST 请求，类似于这样：

```
POST /_search
{
  "from": 30,
  "size": 10
}
```

这个原理同样应用于其他携带交互数据的 GET API请求中。

我们将在后续的章节中讨论聚合查询，但是现在我们把关注点仅放在查询语义上。

相对于神秘的查询字符串方法，请求体查询允许我们使用结构化查询Query DSL(Query Domain Specific Language)

结构化查询 Query DSL

结构化查询是一种灵活的，多表现形式的查询语言。Elasticsearch在一个简单的JSON接口中用结构化查询来展现Lucene绝大多数能力。你应当在你的产品中采用这种方式进行查询。它使得你的查询更加灵活，精准，易于阅读并且易于debug。

使用结构化查询，你需要传递 `query` 参数：

```
GET /_search
{
  "query": YOUR_QUERY_HERE
}
```

空查询 - `{}` - 在功能上等同于使用 `match_all` 查询子句，正如其名字一样，匹配所有的文档：

```
GET /_search
{
  "query": {
    "match_all": {}
  }
}
```

查询子句

一个查询子句一般使用这种结构：

```
{
  QUERY_NAME: {
    ARGUMENT: VALUE,
    ARGUMENT: VALUE, ...
  }
}
```

或指向一个指定的字段：

```
{
  QUERY_NAME: {
    FIELD_NAME: {
      ARGUMENT: VALUE,
      ARGUMENT: VALUE, ...
    }
  }
}
```

例如，你可以使用 `match` 查询子句用来找寻在 `tweet` 字段中找寻包含 `elasticsearch` 的成员：

```
{
  "match": {
    "tweet": "elasticsearch"
  }
}
```

完整的查询请求会是这样：

```
GET /_search
{
  "query": {
    "match": {
```

```
    "tweet": "elasticsearch"
  }
}
```

合并多子句

查询子句就像是搭积木一样，可以合并简单的子句为一个复杂的查询语句，比如：

- 简单子句(*leaf clauses*)(比如 `match` 子句)用以在将查询字符串与一个字段(或多字段)进行比较
- 复合子句(*compound*)用以合并其他的子句。例如，`bool` 子句允许你合并其他的合法子句，无论是 `must`，`must_not` 还是 `should`：

```
{
  "bool": {
    "must": { "match": { "tweet": "elasticsearch" }},
    "must_not": { "match": { "name": "mary" }},
    "should": { "match": { "tweet": "full text" }}
  }
}
```

复合子句能合并 任意其他查询子句，包括其他的复合子句。 这就意味着复合子句可以相互嵌套，从而实现非常复杂的逻辑。

以下实例查询在inbox中或未标记spam的邮件中找出包含 "business opportunity" 的星标(starred)邮件：

```
{
  "bool": {
    "must": { "match": { "email": "business opportunity" }},
    "should": [
      { "match": { "starred": true }},
      { "bool": {
        "must": { "folder": "inbox" },
        "must_not": { "spam": true }}
      ]
    },
    "minimum_should_match": 1
  }
}
```

不用担心这个例子的细节，我们将在后面详细解释它。重点是复合子句可以合并多种子句为一个单一的查询，无论是简单子句还是其他的复合子句。

查询与过滤

前面我们讲到的是关于结构化查询语句，事实上我们可以使用两种结构化语句：结构化查询（Query DSL）和结构化过滤（Filter DSL）。查询与过滤语句非常相似，但是它们由于使用目的不同而稍有差异。

一条过滤语句会询问每个文档的字段值是否包含着特定值：

- 是否 `created` 的日期范围在 `2013` 到 `2014` ？
- 是否 `status` 字段中包含单词 "published" ？
- 是否 `lat_lon` 字段中的地理位置与目标点相距不超过10km ？

一条查询语句与过滤语句相似，但问法不同：

查询语句会询问每个文档的字段值与特定值的匹配程度如何？

查询语句的典型用法是为了找到文档：

- 查找与 `full text search` 这个词语最佳匹配的文档
- 查找包含单词 `run`，但是也包含 `runs`，`running`，`jog` 或 `sprint` 的文档
- 同时包含着 `quick`，`brown` 和 `fox` --- 单词间离得越近，该文档的相关性越高
- 标识着 `lucene`，`search` 或 `java` --- 标识词越多，该文档的相关性越高

一条查询语句会计算每个文档与查询语句的相关性，会给出一个相关性评分 `_score`，并且按照相关性对匹配到的文档进行排序。这种评分方式非常适用于一个没有完全配置结果的全文本搜索。

性能差异

使用过滤语句得到的结果集 -- 一个简单的文档列表，快速匹配运算并存入内存是十分方便的，每个文档仅需要1个字节。这些缓存的过滤结果集与后续请求的结合使用是非常高效的。

查询语句不仅要查找相匹配的文档，还需要计算每个文档的相关性，所以一般来说查询语句要比过滤语句更耗时，并且查询结果也不可缓存。

幸亏有了倒排索引，一个只匹配少量文档的简单查询语句在百万级文档中的查询效率会与一条经过缓存的过滤语句旗鼓相当，甚至略占上风。但是一般情况下，一条经过缓存的过滤查询要远胜一条查询语句的执行效率。

过滤语句的目的就是缩小匹配的文档结果集，所以需要仔细检查过滤条件。

什么情况下使用

原则上来说，使用查询语句做全文本搜索或其他需要进行相关性评分的时候，剩下的全部用过滤语句

最重要的查询过滤语句

Elasticsearch 提供了丰富的查询过滤语句，而有一些是我们较常用到的。我们将会在后续的《深入搜索》中展开讨论，现在我们快速的介绍一下 这些最常用到的查询过滤语句。

term 过滤

term 主要用于精确匹配哪些值，比如数字，日期，布尔值或 not_analyzed 的字符串(未经分析的文本数据类型)：

```
{ "term": { "age": 26 } }
{ "term": { "date": "2014-09-01" } }
{ "term": { "public": true } }
{ "term": { "tag": "full_text" } }
```

terms 过滤

terms 跟 term 有点类似，但 terms 允许指定多个匹配条件。如果某个字段指定了多个值，那么文档需要一起去做匹配：

```
{
  "terms": {
    "tag": [ "search", "full_text", "nosql" ]
  }
}
```

range 过滤

range 过滤允许我们按照指定范围查找一批数据：

```
{
  "range": {
    "age": {
      "gte": 20,
      "lt": 30
    }
  }
}
```

范围操作符包含：

gt :: 大于

gte :: 大于等于

lt :: 小于

lte :: 小于等于

exists 和 missing 过滤

exists 和 missing 过滤可以用于查找文档中是否包含指定字段或没有某个字段，类似于SQL语句中的 IS_NULL 条件

```
{
  "exists": {
```

```
    "field": "title"
  }
}
```

这两个过滤只是针对已经查出一批数据来，但是想区分出某个字段是否存在的时候使用。

bool 过滤

`bool` 过滤可以用来合并多个过滤条件查询结果的布尔逻辑，它包含一下操作符：

`must` :: 多个查询条件的完全匹配,相当于 `and` 。

`must_not` :: 多个查询条件的相反匹配，相当于 `not` 。

`should` :: 至少有一个查询条件匹配, 相当于 `or` 。

这些参数可以分别继承一个过滤条件或者一个过滤条件的数组：

```
{
  "bool": {
    "must": { "term": { "folder": "inbox" } },
    "must_not": { "term": { "tag": "spam" } },
    "should": [
      { "term": { "starred": true } },
      { "term": { "unread": true } }
    ]
  }
}
```

match_all 查询

使用 `match_all` 可以查询到所有文档，是没有查询条件下的默认语句。

```
{
  "match_all": {}
}
```

此查询常用于合并过滤条件。比如说你需要检索所有的邮箱,所有的文档相关性都是相同的，所以得到的 `_score` 为1

match 查询

`match` 查询是一个标准查询，不管你需要全文本查询还是精确查询基本上都要用到它。

如果你使用 `match` 查询一个全文本字段，它会在真正查询之前用分析器先分析 `match` 一下查询字符：

```
{
  "match": {
    "tweet": "About Search"
  }
}
```

如果用 `match` 下指定了一个确切值，在遇到数字，日期，布尔值或者 `not_analyzed` 的字符串时，它将为你搜索你给定的值：

```
{ "match": { "age": 26 } }
{ "match": { "date": "2014-09-01" } }
{ "match": { "public": true } }
{ "match": { "tag": "full_text" } }
```

提示：做精确匹配搜索时，你最好用过滤语句，因为过滤语句可以缓存数据。

不像我们在《简单搜索》中介绍的字符查询，`match` 查询不可以用类似`"+usid:2 +tweet:search"`这样的语句。它只能就指定某个确切字段某个确切的值进行搜索，而你要做的就是为它指定正确的字段名以避免语法错误。

multi_match 查询

`multi_match` 查询允许你做 `match` 查询的基础上同时搜索多个字段：

```
{
  "multi_match": {
    "query": "full text search",
    "fields": [ "title", "body" ]
  }
}
```

bool 查询

`bool` 查询与 `bool` 过滤相似，用于合并多个查询子句。不同的是，`bool` 过滤可以直接给出是否匹配成功，而 `bool` 查询要计算每一个查询子句的 `_score`（相关性分值）。

`must` :: 查询指定文档一定要被包含。

`must_not` :: 查询指定文档一定不要被包含。

`should` :: 查询指定文档，有则可以为文档相关性加分。

以下查询将会找到 `title` 字段中包含 "how to make millions"，并且 "tag" 字段没有被标为 `spam`。如果有标识为 "starred" 或者发布日期为2014年之前，那么这些匹配的文档将比同类网站等级高：

```
{
  "bool": {
    "must": { "match": { "title": "how to make millions" }},
    "must_not": { "match": { "tag": "spam" }},
    "should": [
      { "match": { "tag": "starred" }},
      { "range": { "date": { "gte": "2014-01-01" }}}
    ]
  }
}
```

提示：如果 `bool` 查询下没有 `must` 子句，那至少应该有一个 `should` 子句。但是如果有 `must` 子句，那么没有 `should` 子句也可以进行查询。

查询与过滤条件的合并

查询语句和过滤语句可以放在各自的上下文中。在 Elasticsearch API 中我们会看到许多带有 `query` 或 `filter` 的语句。这些语句既可以包含单条 `query` 语句，也可以包含一条 `filter` 子句。换句话说，这些语句需要首先创建一个 `query` 或 `filter` 的上下文关系。

复合查询语句可以加入其他查询子句，复合过滤语句也可以加入其他过滤子句。通常情况下，一条查询语句需要过滤语句的辅助，全文本搜索除外。

所以说，查询语句可以包含过滤子句，反之亦然。以便于我们切换 `query` 或 `filter` 的上下文。这就要求我们在读懂需求的同时构造正确有效的语句。

带过滤的查询语句

过滤一条查询语句

比如说我们有这样一条查询语句：

```
{
  "match": {
    "email": "business opportunity"
  }
}
```

然后我们想要让这条语句加入 `term` 过滤，在收信箱中匹配邮件：

```
{
  "term": {
    "folder": "inbox"
  }
}
```

`search` API中只能包含 `query` 语句，所以我们需要用 `filtered` 来同时包含 `"query"` 和 `"filter"` 子句：

```
{
  "filtered": {
    "query": { "match": { "email": "business opportunity" }},
    "filter": { "term": { "folder": "inbox" }}
  }
}
```

我们在外层再加入 `query` 的上下文关系：

```
GET /_search
{
  "query": {
    "filtered": {
      "query": { "match": { "email": "business opportunity" }},
      "filter": { "term": { "folder": "inbox" }}
    }
  }
}
```

单条过滤语句

在 `query` 上下文中，如果你只需要一条过滤语句，比如在匹配全部邮件的时候，你可以省略 `query` 子句：

```
GET /_search
{
  "query": {
    "filtered": {
      "filter": { "term": { "folder": "inbox" }}
    }
  }
}
```

如果一条查询语句没有指定查询范围，那么它默认使用 `match_all` 查询，所以上面语句的完整形式如下：

```
GET /_search
{
  "query": {
    "filtered": {
      "query": { "match_all": {}},
      "filter": { "term": { "folder": "inbox" }}
    }
  }
}
```

查询语句中的过滤

有时候，你需要在 `filter` 的上下文中使用一个 `query` 子句。下面的语句就是一条带有查询功能的过滤语句，这条语句可以过滤掉看起来像垃圾邮件的文档：

```
GET /_search
{
  "query": {
    "filtered": {
      "filter": {
        "bool": {
          "must": { "term": { "folder": "inbox" }},
          "must_not": {
            "query": { <1>
              "match": { "email": "urgent business proposal" }
            }
          }
        }
      }
    }
  }
}
```

<1> 过滤语句中可以使用 `query` 查询的方式代替 `bool` 过滤子句。

提示：我们很少用到的过滤语句中包含查询，保留这种用法只是为了语法的完整性。只有在过滤中用到全文本匹配的时候才会使用这种结构。

验证查询

查询语句可以变得非常复杂，特别是与不同的分析器和字段映射相结合后，就会有些难度。

`validate` API 可以验证一条查询语句是否合法。

```
GET /gb/tweet/_validate/query
{
  "query": {
    "tweet" : {
      "match" : "really powerful"
    }
  }
}
```

以上请求的返回值告诉我们这条语句是非法的：

```
{
  "valid" :      false,
  "_shards" : {
    "total" :    1,
    "successful" : 1,
    "failed" :    0
  }
}
```

理解错误信息

想知道语句非法的具体错误信息，需要加上 `explain` 参数：

```
GET /gb/tweet/_validate/query?explain <1>
{
  "query": {
    "tweet" : {
      "match" : "really powerful"
    }
  }
}
```

<1> `explain` 参数可以提供语句错误的更多详情。

很显然，我们把 `query` 语句的 `match` 与字段名位置弄反了：

```
{
  "valid" :      false,
  "_shards" : { ... },
  "explanations" : [ {
    "index" :    "gb",
    "valid" :    false,
    "error" :    "org.elasticsearch.index.query.QueryParseException:
                  [gb] No query registered for [tweet]"
  } ]
}
```

理解查询语句

如果是合法语句的话，使用 `explain` 参数可以返回一个带有查询语句的可阅读描述，可以帮助了解查询语句在ES中是如何执行的：

```
GET /_validate/query?explain
{
  "query": {
    "match" : {
      "tweet" : "really powerful"
    }
  }
}
```

`explanation` 会为每一个索引返回一段描述，因为每个索引会有不同的映射关系和分析器：

```
{
  "valid" :      true,
  "_shards" :   { ... },
  "explanations" : [ {
    "index" :    "us",
    "valid" :    true,
    "explanation" : "tweet:really tweet:powerful"
  }, {
    "index" :    "gb",
    "valid" :    true,
    "explanation" : "tweet:really tweet:power"
  } ]
}
```

从返回的 `explanation` 你会看到 `match` 是如何为查询字符串 `"really powerful"` 进行查询的，首先，它被拆分成两个独立的词分别在 `tweet` 字段中进行查询。

而且，在索引 `us` 中这两个词为 `"really"` 和 `"powerful"`，在索引 `gb` 中被拆分成 `"really"` 和 `"power"`。这是因为我们在索引 `gb` 中使用了 `english` 分析器。

结语

这一章详细介绍了如何在项目中使用常见的查询语句。

也就是说，想要完全掌握搜索和结构化查询，还需要在工作中花费大量的时间来理解ES的工作方式。

更高级的部分，我们将会在《深入搜索》中详细讲解，但是在讲解之前，你还需要理解查询结果是如何进行排序的，

下一章我们将学习如何根据相关性对查询结果进行排序以及指定排序过程。

相关性排序

默认情况下，结果集会按照相关性进行排序 -- 相关性越高，排名越靠前。这一章我们会讲述相关性是什么以及它是如何计算的。在此之前，我们先看一下 `sort` 参数的使用方法。

排序方式

为了使结果可以按照相关性进行排序，我们需要一个相关性的值。在ElasticSearch的查询结果中，相关性分值会用 `_score` 字段来给出一个浮点型的数值，所以默认情况下，结果集以 `_score` 进行倒序排列。

有时，即便如此，你还是没有一个有意义的相关性分值。比如，以下语句返回所有tweets中 `user_id` 是否包含值 `1`：

```
GET /_search
{
  "query" : {
    "filtered" : {
      "filter" : {
        "term" : {
          "user_id" : 1
        }
      }
    }
  }
}
```

过滤语句与 `_score` 没有关系，但是有隐含的查询条件 `match_all` 为所有的文档的 `_score` 设值为 `1`。也就相当于所有的文档相关性是相同的。

字段值排序

下面例子中，对结果集按照时间排序，这也是最常见的情形，将最新的文档排列靠前。我们使用 `sort` 参数进行排序：

```
GET /_search
{
  "query" : {
    "filtered" : {
      "filter" : { "term" : { "user_id" : 1 } }
    }
  },
  "sort": { "date": { "order": "desc" } }
}
```

你会发现这里有两个不同点：

```
"hits" : {
  "total" :      6,
  "max_score" : null, <1>
  "hits" : [ {
    "_index" :    "us",
    "_type" :     "tweet",
    "_id" :       "14",
    "_score" :     null, <1>
    "_source" :    {
      "date":      "2014-09-24",
      ...
    },
    "sort" :       [ 1411516800000 ] <2>
  },
  ...
}
```

<1> `_score` 字段没有经过计算，因为它没有用作排序。

<2> `date` 字段被转为毫秒当作排序依据。

首先，在每个结果中增加了一个 `sort` 字段，它所包含的值是用来排序的。在这个例子当中 `date` 字段在内部被转为毫秒，即长整型数字 `1411516800000` 等同于日期字符串 `2014-09-24 00:00:00 UTC`。

其次就是 `_score` 和 `max_score` 字段都为 `null`。计算 `_score` 是比较消耗性能的，而且通常主要用作排序 -- 我们不是用相关性进行排序的时候，就不需要统计其相关性。如果你想强制计算其相关性，可以设置 `track_scores` 为 `true`。

默认排序

作为缩写，你可以只指定要排序的字段名称：

```
"sort": "number_of_children"
```

字段值默认以顺序排列，而 `_score` 默认以倒序排列。

多级排序

如果我们想要合并一个查询语句，并且展示所有匹配的结果集使用第一排序是 `date`，第二排序是 `_score`：

```
GET /_search
{
  "query" : {
    "filtered" : {
      "query": { "match": { "tweet": "manage text search" }},
      "filter" : { "term" : { "user_id" : 2 }}
    }
  },
  "sort": [
    { "date": { "order": "desc" }},
    { "_score": { "order": "desc" }}
  ]
}
```

排序是很重要的。结果集会先用第一排序字段来排序，当用用作第一字段排序的值相同的时候，然后再用第二字段对第一排序值相同的文档进行排序，以此类推。

多级排序不需要包含 `_score` -- 你可以使用几个不同的字段，如位置距离或者自定义数值。

字符串参数排序

字符查询也支持自定义排序，在查询字符串使用 `sort` 参数就可以：

```
GET /_search?sort=date:desc&sort=_score&q=search
```

为多值字段排序

在为一个字段的多个值进行排序的时候，其实这些值本来是没有固定的排序的-- 一个拥有多值的字段就是一个集合，你准备

以哪一个作为排序依据呢？

对于数字和日期，你可以从多个值中取出一个来进行排序，你可以使用 `min`，`max`，`avg` 或 `sum` 这些模式。比如说你可以在 `dates` 字段中用最早的日期来进行排序：

```
"sort": {
  "dates": {
    "order": "asc",
    "mode": "min"
  }
}
```

多值字段字符串排序

`analyzed` 字符串字段同时也是多值字段，在这些字段上排序往往得不到你想要的值。比如你分析一个字符 `"fine old art"`，它最终会得到三个值。例如我们想要按照第一个词首字母排序，如果第一个单词相同的话，再用第二个词的首字母排序，以此类推，可惜 `ElasticSearch` 在进行排序时是得不到这些信息的。

当然你可以使用 `min` 和 `max` 模式来排（默认使用的是 `min` 模式）但它是依据 `art` 或者 `old` 排序，而不是我们所期望的那样。

为了使一个string字段可以进行排序，它必须只包含一个词：即完整的 `not_analyzed` 字符串。当然我们需要对字段进行全文本搜索的时候还必须使用 `analyzed`。

在 `_source` 下相同的字符串上排序两次会造成不必要的资源浪费。而我们想要的是一个字段中同时包含这两种索引方式。现在我们介绍一个在所有核心字段类型上通用的参数 `fields`，这样我们就可以改变它的mapping：

```
"tweet": {
  "type": "string",
  "analyzer": "english"
}
```

改变后的多值字段mapping如下：

```
"tweet": { <1>
  "type": "string",
  "analyzer": "english",
  "fields": {
    "raw": { <2>
      "type": "string",
      "index": "not_analyzed"
    }
  }
}
```

<1> `tweet` 字段用于全文本的 `analyzed` 索引方式不变。

<2> 新增的 `tweet.raw` 子字段索引方式是 `not_analyzed`。

现在，在给数据重建索引后，我们既可以使用 `tweet` 字段进行全文本搜索，也可以用 `tweet.raw` 字段进行排序：

```
GET /_search
{
  "query": {
    "match": {
      "tweet": "elasticsearch"
    }
  },
  "sort": "tweet.raw"
}
```

警告：对 `analyzed` 字段进行强制排序会消耗大量内存。详情请查阅《字段类型简介》相关内容。

相关性简介

我们曾经讲过，默认情况下，返回结果是按相关性倒序排列的。但是什么是相关性？相关性如何计算？

每个文档都有相关性评分，用一个相对的浮点数字段 `_score` 来表示 -- `_score` 的评分越高，相关性越高。

查询语句会为每个文档添加一个 `_score` 字段。评分的计算方式取决于不同的查询类型 -- 不同的查询语句用于不同的目的：`fuzzy` 查询会计算与关键词的拼写相似程度，`terms` 查询会计算找到的内容与关键词组成部分匹配的百分比，但是一般意义上我们说的全文本搜索是指计算内容与关键词的类似程度。

ElasticSearch的相似度算法被定义为 TF/IDF，即检索词频率/反向文档频率，包括一下内容：

检索词频率::

检索词在该字段出现的频率？出现频率越高，相关性也越高。字段中出现过5次要比只出现过1次的相关性高。

反向文档频率::

每个检索词在索引中出现的频率？频率越高，相关性越低。检索词出现在多数文档中会比出现在少数文档中的权重更低，即检验一个检索词在文档中的普遍重要性。

字段长度准则::

字段的长度是多少？长度越长，相关性越低。检索词出现在一个短的 `title` 要比同样的词出现在一个长的 `content` 字段。

单个查询可以使用TF/IDF评分标准或其他方式，比如短语查询中检索词的距离或模糊查询里的检索词相似度。

相关性并不只是全文本检索的专利。也适用于 `yes|no` 的子句，匹配的子句越多，相关性评分越高。

如果多条查询子句被合并为一条复合查询语句，比如 `bool` 查询，则每个查询子句计算得出的评分会被合并到总的相关性评分中。

理解评分标准

当调试一条复杂的查询语句时，想要理解相关性评分 `_score` 是比较困难的。ElasticSearch 在每个查询语句中都有一个 `explain` 参数，将 `explain` 设为 `true` 就可以得到更详细的信息。

```
GET /_search?explain <1>
{
  "query" : { "match" : { "tweet" : "honeymoon" } }
}
```

<1> `explain` 参数可以让返回结果添加一个 `_score` 评分的得来依据。

增加一个 `explain` 参数会为每个匹配到的文档产生一大堆额外内容，但是花时间去理解它是很有意义的。如果现在看不明白也没关系 -- 等你需要的时候再来回顾这一节就行。下面我们来一点点的了解这块知识点。

首先，我们看一下普通查询返回的元数据：

```
{
  "_index" :      "us",
  "_type" :      "tweet",
  "_id" :        "12",
  "_score" :      0.076713204,
  "_source" :     { ... trimmed ... },
```

```
}
```

这里加入了该文档来自于哪个节点哪个分片上的信息，这对我们是比较有帮助的，因为词频率和 文档频率是在每个分片中计算出来的，而不是每个索引中：

```
"_shard" :      1,
"_node" :      "mzIVYCsqSwCG_M_ZffSs9Q",
```

然后返回值中的 `_explanation` 会包含在每一个入口，告诉你采用了哪种计算方式，并让你知道计算的结果以及其他详情：

```
"_explanation": { <1>
  "description": "weight(tweet:honeymoon in 0)
                  [PerFieldSimilarity], result of:",
  "value":      0.076713204,
  "details": [
    {
      "description": "fieldWeight in 0, product of:",
      "value":      0.076713204,
      "details": [
        { <2>
          "description": "tf(freq=1.0), with freq of:",
          "value":      1,
          "details": [
            {
              "description": "termFreq=1.0",
              "value":      1
            }
          ]
        },
        { <3>
          "description": "idf(docFreq=1, maxDocs=1)",
          "value":      0.30685282
        },
        { <4>
          "description": "fieldNorm(doc=0)",
          "value":      0.25,
        }
      ]
    }
  ]
}
```

<1> honeymoon 相关性评分计算的总结

<2> 检索词频率

<3> 反向文档频率

<4> 字段长度准则

重要：输出 `explain` 结果代价是十分昂贵的，它只能用作调试工具 --千万不要用于生产环境。

第一部分是关于计算的总结。告诉了我们 "honeymoon" 在 `tweet` 字段中的检索词频率/反向文档频率或 TF/IDF，（这里的文档 `0` 是一个内部的ID，跟我们没有关系，可以忽略。）

然后解释了计算的权重是如何计算出来的：

检索词频率::

检索词 ``honeymoon`` 在 ``tweet`` 字段中的出现次数。

反向文档频率::

检索词 `honeymoon` 在 `tweet` 字段在当前文档出现次数与索引中其他文档的出现总数的比率。

字段长度准则::

文档中 `tweet` 字段内容的长度 -- 内容越长, How long s the d field in this document -- the longer the field, the smaller this number.

复杂的查询语句解释也非常复杂, 但是包含的内容与上面例子大致相同。通过这段描述我们可以了解搜索结果是如何产生的。

提示: JSON形式的explain描述是难以阅读的 但是转成 YAML 会好很多, 只需要在参数中加上 `format=yaml`

Explain Api

文档是如何被匹配到的

当 `explain` 选项加到某一文档上时, 它会告诉你为何这个文档会被匹配, 以及一个文档为何没有被匹配。

请求路径为 `/index/type/id/_explain`, 如下所示:

```
GET /us/tweet/12/_explain
{
  "query" : {
    "filtered" : {
      "filter" : { "term" : { "user_id" : 2 }},
      "query" : { "match" : { "tweet" : "honeymoon" }}
    }
  }
}
```

除了上面我们看到的完整描述外, 我们还可以看到这样的描述:

```
"failure to match filter: cache(user_id:[2 TO 2])"
```

也就是说我们的 `user_id` 过滤子句使该文档不能匹配到。

数据字段

本章的目的在于介绍关于ElasticSearch内部的一些运行情况。在这里我们先不介绍新的知识点，数据字段是我们要经常查阅的内容之一，但我们使用的时候不必太在意。

当你对一个字段进行排序时，ElasticSearch 需要进入每个匹配到的文档得到相关的值。倒排索引在用于搜索时是非常卓越的，但却不是理想的排序结构。

- 当搜索的时候，我们需要用检索词去遍历所有的文档。
- 当排序的时候，我们需要遍历文档中所有的值，我们需要做颠倒序排列操作。

为了提高排序效率，ElasticSearch 会将所有字段的值加载到内存中，这就叫做"数据字段"。

重要：ElasticSearch将所有字段数据加载到内存中并不是匹配到的那部分数据。而是索引下所有文档中的值，包括所有类型。

将所有字段数据加载到内存中是因为从硬盘反向倒排索引是非常缓慢的。尽管你这次请求需要的是某些文档中的部分数据，但你下个请求却需要另外的数据，所以将所有字段数据一次性加载到内存中是十分必要的。

ElasticSearch中的字段数据常被应用到以下场景：

- 对一个字段进行排序
- 对一个字段进行聚合
- 某些过滤，比如地理位置过滤
- 某些与字段相关的脚本计算

毫无疑问，这会消耗掉很多内存，尤其是大量的字符串数据 -- string字段可能包含很多不同的值，比如邮件内容。值得庆幸的是，内存不足是可以通过横向扩展解决的，我们可以增加更多的节点到集群。

现在，你只需要知道字段数据是什么，和什么时候内存不足就可以了。稍后我们会讲述字段数据到底消耗了多少内存，如何限制ElasticSearch可以使用的内存，以及如何预加载字段数据以提高用户体验。

[[distributed-search]] == Distributed Search Execution

Before moving on, we are going to take a detour and talk about how search is executed in a distributed environment. (((("distributed search execution")))) It is a bit more complicated than the basic *create-read-update-delete* (CRUD) requests(((("CRUD (create-read-update-delete) operations")))) that we discussed in <>.

.Content Warning

The information presented in this chapter is for your interest. You are not required to understand and remember all the detail in order to use Elasticsearch.

Read this chapter to gain a taste for how things work, and to know where the information is in case you need to refer to it in the future, but don't be overwhelmed by the detail.

A CRUD operation deals with a single document that has a unique combination of `_index`, `_type`, and `<>` (which defaults to the document's `_id`). This means that we know exactly which shard in the cluster holds that document.

Search requires a more complicated execution model because we don't know which documents will match the query: they could be on any shard in the cluster. A search request has to consult a copy of every shard in the index or indices we're interested in to see if they have any matching documents.

But finding all matching documents is only half the story. Results from multiple shards must be combined into a single sorted list before the `search` API can return a ``page" of results. For this reason, search is executed in a two-phase process called *query then fetch*.

=== Query Phase

During the initial *query phase*, the query is broadcast to a shard copy (a primary or replica shard) of every shard in the index. Each shard executes the search locally and builds a *priority queue* of matching documents.

.Priority Queue

A *priority queue* is just a sorted list that holds the *top-n* matching documents. The size of the priority queue depends on the pagination parameters `from` and `size`. For example, the following search request would require a priority queue big enough to hold 100 documents:

[source,js]

```
GET /_search { "from": 90, "size": 10
```

```
}
```

The query phase process is depicted in <>.

 .Query phase of distributed search image::images/elas_0901.png["Query phase of distributed search"]

The query phase consists of the following three steps:

1. The client sends a `search` request to `Node 3`, which creates an empty priority queue of size `from + size`.
2. `Node 3` forwards the search request to a primary or replica copy of every shard in the index. Each shard executes the query locally and adds the results into a local sorted priority queue of size `from + size`.
3. Each shard returns the doc IDs and sort values of all the docs in its priority queue to the coordinating node, `Node 3`, which merges these values into its own priority queue to produce a globally sorted list of results.

When a search request is sent to a node, that node becomes the coordinating node. It is the job of this node to broadcast the search request to all involved shards, and to gather their responses into a globally sorted result set that it can return to the client.

The first step is to broadcast the request to a shard copy of every node in the index. Just like <>, search requests can be handled by a primary shard or by any of its replicas. This is how more replicas (when combined with more hardware) can increase search throughput. A coordinating node will round-robin through all shard copies on subsequent requests in order to spread the load.

Each shard executes the query locally and builds a sorted priority queue of length `from + size`—in other words, enough results to satisfy the global search request all by itself. It returns a lightweight list of results to the coordinating node, which contains just the doc IDs and any values required for sorting, such as the `_score`.

The coordinating node merges these shard-level results into its own sorted priority queue, which represents the globally sorted result set. Here the query phase ends.

[NOTE]

An index can consist of one or more primary shards, so a search request against a single index needs to be able to combine the results from multiple shards. A search against *multiple* or *all* indices works in exactly the same

way--there are just more shards involved.

=== Fetch Phase

The query phase identifies which documents satisfy((((("distributed search execution", "fetch phase")))((("fetch phase of distributed search")))) the search request, but we still need to retrieve the documents themselves. This is the job of the fetch phase, shown in <>.

[[img-distrib-fetch]] .Fetch phase of distributed search image::images/elas_0902.png["Fetch Phase of distributed search"]

The distributed phase consists of the following steps:

1. The coordinating node identifies which documents need to be fetched and issues a multi `GET` request to the relevant shards.
2. Each shard loads the documents and *enriches* them, if required, and then returns the documents to the coordinating node.
3. Once all documents have been fetched, the coordinating node returns the results to the client.

The coordinating node first decides which documents *actually* need to be fetched. For instance, if our query specified `{ "from": 90, "size": 10 }`, the first 90 results would be discarded and only the next 10 results would need to be retrieved. These documents may come from one, some, or all of the shards involved in the original search request.

The coordinating node builds a <> for each shard that holds a pertinent document and sends the request to the same shard copy that handled the query phase.

The shard loads the document bodies--the `_source` field--and, if requested, enriches the results with metadata and <>. Once the coordinating node receives all results, it assembles them into a single response that it returns to the client.

.Deep Pagination

The query-then-fetch process supports pagination with the `from` and `size` parameters, but *within limits*. (((("size parameter")))((("from parameter")))((("pagination", "supported by query-then-fetch process")))((("deep paging, problems with")))) Remember that each shard must build a priority queue of length `from + size`, all of which need to be passed back to the coordinating node. And the coordinating node needs to sort through `number_of_shards * (from + size)` documents in order to find the correct `size` documents.

Depending on the size of your documents, the number of shards, and the hardware you are using, paging 10,000 to 50,000 results (1,000 to 5,000 pages) deep should be perfectly doable. But with big-enough `from` values, the sorting process can become very heavy indeed, using vast amounts of CPU, memory, and bandwidth. For this reason, we strongly advise against deep paging.

In practice, ``deep pagers'' are seldom human anyway. A human will stop paging after two or three pages and will change the search criteria. The culprits are usually bots or web spiders that tirelessly keep fetching page after page until your servers crumble at the knees.

If you *do* need to fetch large numbers of docs from your cluster, you can do so efficiently by disabling sorting with the `scan` search type, which we discuss <>.

=== Search Options

A few ({"search options"}) optional query-string parameters can influence the search process.

==== preference

The `preference` parameter allows({"preference parameter"})({"search options", "preference"}) you to control which shards or nodes are used to handle the search request. It accepts values such as `_primary`, `_primary_first`, `_local`, `_only_node:xyz`, `_prefer_node:xyz`, and `_shards:2,3`, which are explained in detail on the <http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/search-request-preference.html> [search preference] documentation page.

However, the most generally useful value is some arbitrary string, to avoid the *bouncing results* problem.({"bouncing results problem"})

[[bouncing-results]] .Bouncing Results

Imagine that you are sorting your results by a `timestamp` field, and two documents have the same timestamp. Because search requests are round-robin between all available shard copies, these two documents may be returned in one order when the request is served by the primary, and in another order when served by the replica.

This is known as the *bouncing results* problem: every time the user refreshes the page, the results appear in a different order. The problem can be avoided by always using the same shards for the same user, which can be done by setting the `preference` parameter to an arbitrary string like the user's session ID.

==== timeout

By default, the coordinating node waits({"search options", "timeout"}) to receive a response from all shards. If one node is having trouble, it could slow down the response to all search requests.

The `timeout` parameter tells({"timeout parameter"}) the coordinating node how long it should wait before giving up and just returning the results that it already has. It can be better to return some results than none at all.

The response to a search request will indicate whether the search timed out and how many shards responded successfully:

[source,js]

```
...
"timed_out":    true, <1>
"_shards": {
  "total":      5,
  "successful": 4,
  "failed":     1 <2>
},
...
```

<1> The search request timed out.

<2> One shard out of five failed to respond in time.

If all copies of a shard fail for other reasons--perhaps because of a hardware failure--this will also be reflected in the `_shards` section of the response.

[[search-routing]] ==== routing

In <>, we explained how a custom `routing` parameter((("search options", "routing"))((("routing parameter")))) could be provided at index time to ensure that all related documents, such as the documents belonging to a single user, are stored on a single shard. At search time, instead of searching on all the shards of an index, you can specify one or more `routing` values to limit the search to just those shards:

[source,js]

GET /_search?routing=user_1,user2

This technique comes in handy when designing very large search systems, and we discuss it in detail in <>.

[[search-type]] ===== search_type

While `query_then_fetch` is the default((("query_then_fetch search type"))((("search options", "search_type")))((("search_type")))) search type, other search types can be specified for particular purposes, for example:

[source,js]

GET /_search?search_type=count

`count ::`

The `count` search type has only a `query` phase.((("count search type")) It can be used when you don't need search results, just a document count or <> on documents matching the query.

`query_and_fetch ::`

The `query_and_fetch` search type ((("query_and_fetch search type"))combines the query and fetch phases into a single step. This is an internal optimization that is used when a search request targets a single shard only, such as when a <> value has been specified. While you can choose to use this search type manually, it is almost never useful to do so.

`dfs_query_then_fetch` and `dfs_query_and_fetch ::`

The `dfs` search types((("dfs search types")) have a prequery phase that fetches the term frequencies from all involved shards in order to calculate global term frequencies. We discuss this further in <>.

`scan ::`

The `scan` search type is((("scan search type")) used in conjunction with the `scroll` API ((("scroll API"))to retrieve large numbers of results efficiently. It does this by disabling sorting. We discuss *scan-and-scroll* in the next section.

[[scan-scroll]] === scan and scroll

The `scan` search type and the `scroll` API(("scroll API", "scan and scroll")) are used together to retrieve large numbers of documents from Elasticsearch efficiently, without paying the penalty of deep pagination.

`scroll` ::

+

A *scrolled search* allows us to(("scrolled search")) do an initial search and to keep pulling batches of results from Elasticsearch until there are no more results left. It's a bit like a *cursor* in (("cursors")) a traditional database.

A scrolled search takes a snapshot in time. It doesn't see any changes that are made to the index after the initial search request has been made. It does this by keeping the old data files around, so that it can preserve its ``view" on what the index looked like at the time it started.

--

`scan` ::

The costly part of deep pagination is the global sorting of results, but if we disable sorting, then we can return all documents quite cheaply. To do this, we use the `scan` search type.(("scan search type")) Scan instructs Elasticsearch to do no sorting, but to just return the next batch of results from every shard that still has results to return.

To use *scan-and-scroll*, we execute a search(("scan-and-scroll")) request setting `search_type` to(("search_type", "scan and scroll")) `scan`, and passing a `scroll` parameter telling Elasticsearch how long it should keep the scroll open:

[source,js]

GET /old_index/_search?search_type=scan&scroll=1m <1> { "query": { "match_all": {}}, "size": 1000

}

<1> Keep the scroll open for 1 minute.

The response to this request doesn't include any hits, but does include a `_scroll_id`, which is a long Base-64 encoded(("scroll_id")) string. Now we can pass the `_scroll_id` to the `_search/scroll` endpoint to retrieve the first batch of results:

[source,js]

GET /_search/scroll?scroll=1m <1>
c2NhbjJs1OzExODpRNv9aY1VyUVM4U0NMd2pjWlJ3YWlBOzExOTpRNv9aY1VyUVM4U0 <2>
NMd2pjWlJ3YWlBOzExNjpRNv9aY1VyUVM4U0NMd2pjWlJ3YWlBOzExNzpRNv9aY1Vy
UVM4U0NMd2pjWlJ3YWlBOzEyMDpRNv9aY1VyUVM4U0NMd2pjWlJ3YWlBOzE7dG90YW

xfaGl0czoxOw==

<1> Keep the scroll open for another minute.

<2> The `_scroll_id` can be passed in the body, in the URL, or as a query parameter.

Note that we again specify `?scroll=1m`. The scroll expiry time is refreshed every time we run a scroll request, so it needs to give us only enough time to process the current batch of results, not all of the documents that match the query.

The response to this scroll request includes the first batch of results. Although we specified a `size` of 1,000, we get back many more documents.(((("size parameter", "in scanning"))) When scanning, the `size` is applied to each shard, so you will get back a maximum of `size * number_of_primary_shards` documents in each batch.

NOTE: The scroll request also returns a *new* `_scroll_id` . Every time we make the next scroll request, we must pass the `_scroll_id` returned by the *previous* scroll request.

When no more hits are returned, we have processed all matching documents.

TIP: Some of the [http://www.elasticsearch.org/guide\[official](http://www.elasticsearch.org/guide[official) Elasticsearch clients] provide *scan-and-scroll* helpers that provide an easy wrapper around this functionality.(((("clients", "providing scan-and-scroll helpers")))

创建索引

迄今为止，我们简单的通过添加一个文档的方式创建了一个索引。这个索引使用默认设置，新的属性通过动态映射添加到分类中。现在我们需要对这个过程有更多的控制：我们需要确保索引被创建在适当数量的分片上，在索引数据之前设置好分析器和类型映射。

为了达到目标，我们需要手动创建索引，在请求中加入所有设置和类型映射，如下所示：

```
PUT /my_index
{
  "settings": { ... any settings ... },
  "mappings": {
    "type_one": { ... any mappings ... },
    "type_two": { ... any mappings ... },
    ...
  }
}
```

事实上，你可以通过在 `config/elasticsearch.yml` 中添加下面的配置来防止自动创建索引。

```
action.auto_create_index: false
```

NOTE

今后，我们将介绍怎样用【索引模板】来自动预先配置索引。这在索引日志数据时尤其有效：你将日志数据索引在一个以日期结尾的索引上，第二天，一个新的配置好的索引会自动创建好。

删除索引

使用以下的请求来删除索引：

```
DELETE /my_index
```

你也可以用下面的方式删除多个索引

```
DELETE /index_one,index_two
DELETE /index_*
```

你甚至可以删除所有索引

```
DELETE /_all
```

索引设置

你可以通过很多种方式来自定义索引行为，你可以阅读[Index Modules reference documentation](#)，但是：

提示: Elasticsearch 提供了优化好的默认配置。除非你明白这些配置的行为和为什么要这么做，请不要修改这些配置。

下面是两个最重要的设置：

`number_of_shards`

定义一个索引的主分片个数，默认值是 `5`。这个配置在索引创建后不能修改。

`number_of_replicas`

每个主分片的复制分片个数，默认是 `1`。这个配置可以随时在活跃的索引上修改。

例如，我们可以创建只有一个主分片，没有复制分片的小索引。

```
PUT /my_temp_index
{
  "settings": {
    "number_of_shards" : 1,
    "number_of_replicas" : 0
  }
}
```

然后，我们可以用 `update-index-settings` API 动态修改复制分片个数：

```
PUT /my_temp_index/_settings
{
  "number_of_replicas": 1
}
```

配置分析器

第三个重要的索引设置是 `analysis` 部分，用来配置已存在的分析器或创建自定义分析器来定制化你的索引。

在【分析器介绍】中，我们介绍了一些内置的分析器，用于将全字符串转换为适合搜索的倒排索引。

`standard` 分析器是用于全文字段的默认分析器，对于大部分西方语系来说是一个不错的选择。它考虑了以下几点：

- `standard` 分词器，在词层级上分割输入的文本。
- `standard` 表征过滤器，被设计用来整理分词器触发的所有表征（但是目前什么都没做）。
- `lowercase` 表征过滤器，将所有表征转换为小写。
- `stop` 表征过滤器，删除所有可能会造成搜索歧义的停用词，如 `a`，`the`，`and`，`is`。

默认情况下，停用词过滤器是被禁用的。如需启用它，你可以通过创建一个基于 `standard` 分析器的自定义分析器，并且设置 `stopwords` 参数。可以提供一个停用词列表，或者使用一个特定语言的预定停用词列表。

在下面的例子中，我们创建了一个新的分析器，叫做 `es_std`，并使用预定义的西班牙语停用词：

```
PUT /spanish_docs
{
  "settings": {
    "analysis": {
      "analyzer": {
        "es_std": {
          "type": "standard",
          "stopwords": "_spanish_"
        }
      }
    }
  }
}
```

`es_std` 分析器不是全局的，它仅仅存在于我们定义的 `spanish_docs` 索引中。为了用 `analyze` API 来测试它，我们需要使用特定的索引名。

```
GET /spanish_docs/_analyze?analyzer=es_std
El veloz zorro marrón
```

下面简化的结果中显示停用词 `El` 被正确的删除了：

```
{
  "tokens" : [
    { "token" : "veloz", "position" : 2 },
    { "token" : "zorro", "position" : 3 },
    { "token" : "marrón", "position" : 4 }
  ]
}
```

自定义分析器

虽然 Elasticsearch 内置了一系列的分析器，但是真正的强大之处在于定制你自己的分析器。你可以通过在配置文件中组合字符过滤器，分词器和表征过滤器，来满足特定数据的需求。

在【分析器介绍】中，我们提到分析器是三个顺序执行的组件的结合（字符过滤器，分词器，表征过滤器）。

字符过滤器

字符过滤器是让字符串在被分词前变得更加“整洁”。例如，如果我们的文本是 HTML 格式，它可能会包含一些我们不想被索引的 HTML 标签，诸如 `<p>` 或 `<div>`。

我们可以使用 `html_strip` 字符过滤器来删除所有的 HTML 标签，并且将 HTML 实体转换成对应的 Unicode 字符，比如将 `Á` 转成 `Á`。

一个分析器可能包含零到多个字符过滤器。

分词器

一个分析器必须包含一个分词器。分词器将字符串分割成单独的词（terms）或表征（tokens）。`standard` 分析器使用 `standard` 分词器将字符串分割成单独的字词，删除大部分标点符号，但是现存的其他分词器会有不同的行为特征。

例如，`keyword` 分词器输出和它接收到的相同的字符串，不做任何分词处理。`[whitespace 分词器]`只通过空格来分割文本。`[pattern 分词器]`可以通过正则表达式来分割文本。

表征过滤器

分词结果的表征流会根据各自的情况，传递给特定的表征过滤器。

表征过滤器可能修改，添加或删除表征。我们已经提过 `lowercase` 和 `stop` 表征过滤器，但是 Elasticsearch 中有更多的选择。`stemmer` 表征过滤器将单词转化为他们的根形态（root form）。`ascii_folding` 表征过滤器会删除变音符号，比如从 `très` 转为 `tres`。`ngram` 和 `edge_ngram` 可以让表征更适合特殊匹配情况或自动完成。

在【深入搜索】中，我们将举例介绍如何使用这些分词器和过滤器。但是首先，我们需要阐述一下如何创建一个自定义分析器

创建自定义分析器

与索引设置一样，我们预先配置好 `es_std` 分析器，我们可以再 `analysis` 字段下配置字符过滤器，分词器和表征过滤器：

```
PUT /my_index
{
  "settings": {
    "analysis": {
      "char_filter": { ... custom character filters ... },
      "tokenizer": { ... custom tokenizers ... },
      "filter": { ... custom token filters ... },
      "analyzer": { ... custom analyzers ... }
    }
  }
}
```

作为例子，我们来配置一个这样的分析器：

1. 用 `html_strip` 字符过滤器去除所有的 HTML 标签
2. 将 `&` 替换成 `and`，使用一个自定义的 `mapping` 字符过滤器

```
"char_filter": {
  "&_to_and": {
    "type": "mapping",
    "mappings": [ "&=> and " ]
  }
}
```

1. 使用 `standard` 分词器分割单词
2. 使用 `lowercase` 表征过滤器将词转为小写
3. 用 `stop` 表征过滤器去除一些自定义停用词。

```
"filter": {
  "my_stopwords": {
    "type": "stop",
    "stopwords": [ "the", "a" ]
  }
}
```

根据以上描述来将预定义好的分词器和过滤器组合成我们的分析器：

```
"analyzer": {
  "my_analyzer": {
    "type": "custom",
    "char_filter": [ "html_strip", "&_to_and" ],
    "tokenizer": "standard",
    "filter": [ "lowercase", "my_stopwords" ]
  }
}
```

用下面的方式可以将以上请求合并成一条：

```
PUT /my_index
{
  "settings": {
    "analysis": {
      "char_filter": {
        "&_to_and": {
          "type": "mapping",
          "mappings": [ "&=> and " ]
        }
      },
      "filter": {
        "my_stopwords": {
          "type": "stop",
          "stopwords": [ "the", "a" ]
        }
      },
      "analyzer": {
        "my_analyzer": {
          "type": "custom",
          "char_filter": [ "html_strip", "&_to_and" ],
          "tokenizer": "standard",
          "filter": [ "lowercase", "my_stopwords" ]
        }
      }
    }
  }
}
```

创建索引后，用 `analyze` API 来测试新的分析器：

```
GET /my_index/_analyze?analyzer=my_analyzer
The quick & brown fox
```

下面的结果证明我们的分析器能正常工作了：

```
{
```



```
"tokens" : [
  { "token" : "quick", "position" : 2 },
  { "token" : "and", "position" : 3 },
  { "token" : "brown", "position" : 4 },
  { "token" : "fox", "position" : 5 }
]
```

除非我们告诉 Elasticsearch 在哪里使用，否则分析器不会起作用。我们可以通过下面的映射将它应用在一个 `string` 类型的字段上：

```
PUT /my_index/_mapping/my_type
{
  "properties": {
    "title": {
      "type": "string",
      "analyzer": "my_analyzer"
    }
  }
}
```

类型和映射

类型在 Elasticsearch 中表示一组相似的文档。类型由一个名称（比如 `user` 或 `blogpost`）和一个类似数据库表结构的映射组成，描述了文档中可能包含的每个字段的属性，数据类型（比如 `string`，`integer` 或 `date`），和是否这些字段需要被 Lucene 索引或储存。

在【文档】一章中，我们说过类型类似关系型数据库中的表格，一开始你可以这样做类比，但是现在值得更深入阐释一下什么是类型，且在 Lucene 中是怎么实现的。

Lucene 如何处理文档

Lucene 中，一个文档由一组简单的键值对组成，一个字段至少需要有一个值，但是任何字段都可以有多个值。类似的，一个单独的字符串可能在分析过程中被转换成多个值。Lucene 不关心这些值是字符串，数字或日期，所有的值都被当成不透明字节

当我们在 Lucene 中索引一个文档时，每个字段的值都被加到相关字段的倒排索引中。你也可以选择将原始数据储存起来以备今后取回。

类型是怎么实现的

Elasticsearch 类型是在这个简单基础上实现的。一个索引可能包含多个类型，每个类型有各自的映射和文档，保存在同一个索引中。

因为 Lucene 没有文档类型的概念，每个文档的类型名被储存在一个叫 `_type` 的元数据字段上。当我们搜索一种特殊类型的文档时，Elasticsearch 简单的通过 `_type` 字段来过滤出这些文档。

Lucene 同样没有映射的概念。映射是 Elasticsearch 将复杂 JSON 文档映射成 Lucene 需要的扁平化数据的方式。

例如，`user` 类型中 `name` 字段的映射声明这个字段是一个 `string` 类型，在被加入倒排索引之前，它的数据需要通过 `whitespace` 分析器来分析。

```
"name": {
  "type": "string",
  "analyzer": "whitespace"
}
```

预防类型陷阱

事实上不同类型的文档可以被加到同一个索引里带来了一些预想不到的困难。

想象一下我们的索引中有两种类型：`blog_en` 表示英语版的博客，`blog_es` 表示西班牙语版的博客。两种类型都有 `title` 字段，但是其中一种类型使用 `english` 分析器，另一种使用 `spanish` 分析器。

使用下面的查询就会遇到问题：

```
GET /_search
{
  "query": {
    "match": {
      "title": "The quick brown fox"
    }
  }
}
```

我们在两种类型中搜索 `title` 字段，首先需要分析查询语句，但是应该使用哪种分析器呢，`spanish` 还是 `english`？Elasticsearch 会采用第一个被找到的 `title` 字段使用的分析器，这对于这个字段的文档来说是正确的，但对另一个来说却是错误的。

我们可以通过给字段取不同的名字来避免这种错误——比如，用 `title_en` 和 `title_es`。或者在查询中明确包含各自的类型名。

```
GET /_search
{
  "query": {
    "multi_match": { <1>
      "query": "The quick brown fox",
      "fields": [ "blog_en.title", "blog_es.title" ]
    }
  }
}
```

<1> `multi_match` 查询在多个字段上执行 `match` 查询并一起返回结果。

新的查询中 `english` 分析器用于 `blog_en.title` 字段，`spanish` 分析器用于 `blog_es.title` 字段，然后通过综合得分组合两种字段的结果。

这种办法对具有相同数据类型的字段有帮助，但是想象一下如果你将下面两个文档加入同一个索引，会发生什么：

- 类型: `user`

```
{ "login": "john_smith" }
```

- 类型: `event`

```
{ "login": "2014-06-01" }
```

Lucene 不在乎一个字段是字符串而另一个字段是日期，它会一视同仁的索引这两个字段。

然而，假如我们试图排序 `event.login` 字段，Elasticsearch 需要将 `login` 字段的值加载到内存中。像我们在【字段数据介绍】中提到的，它将任意文档的值加入索引而不管它们的类型。

它会尝试加载这些值为字符串或日期，取决于它遇到的第一个 `login` 字段。这可能会导致预想不到的结果或者以失败告终。

提示：为了保证你不会遇到这些冲突，建议在同一个索引的每一个类型中，确保用同样的方式映射同名的字段

根对象

映射的最高一层被称为 **根对象**，它可能包含下面几项：

- 一个 *properties* 节点，列出了文档中可能包含的每个字段的映射
- 多个元数据字段，每一个都以下划线开头，例如 `_type`，`_id` 和 `_source`
- 设置项，控制如何动态处理新的字段，例如 `analyzer`，`dynamic_date_formats` 和 `dynamic_templates`。
- 其他设置，可以同时应用在根对象和其他 `object` 类型的字段上，例如 `enabled`，`dynamic` 和 `include_in_all`

属性

我们已经在【核心字段】和【复合核心字段】章节中介绍过文档字段和属性的三个最重要的设置：

`type`：字段的数据类型，例如 `string` 和 `date`

`index`：字段是否应当被当成全文来搜索（`analyzed`），或被当成一个准确的值（`not_analyzed`），还是完全不可被搜索（`no`）

`analyzer`：确定在索引和或搜索时全文字段使用的 **分析器**。

我们将在下面的章节中介绍其他字段，例如 `ip`，`geo_point` 和 `geo_shape`

元数据：_source 字段

默认情况下，Elasticsearch 用 JSON 字符串来表示文档主体保存在 `_source` 字段中。像其他保存的字段一样，`_source` 字段也会在写入硬盘前压缩。

这几乎始终是需要的功能，因为：

- 搜索结果中能得到完整的文档 —— 不需要额外去别的数据源中查询文档
- 如果缺少 `_source` 字段，部分 `更新` 请求不会起作用
- 当你的映射有变化，而且你需要重新索引数据时，你可以直接在 Elasticsearch 中操作而不需要重新从别的数据源中取回数据。
- 你可以从 `_source` 中通过 `get` 或 `search` 请求取回部分字段，而不是整个文档。
- 这样更容易排查错误，因为你可以准确的看到每个文档中包含的内容，而不是只能从一堆 ID 中猜测他们的内容。

即便如此，存储 `_source` 字段还是要占用硬盘空间的。假如上面的理由对你来说不重要，你可以用下面的映射禁用 `_source` 字段：

```
PUT /my_index
{
  "mappings": {
    "my_type": {
      "_source": {
        "enabled": false
      }
    }
  }
}
```

在搜索请求中你可以通过限定 `_source` 字段来请求指定字段：

```
GET /_search
{
  "query": { "match_all": {} },
  "_source": [ "title", "created" ]
}
```

这些字段会从 `_source` 中提取出来，而不是返回整个 `_source` 字段。

储存字段

除了索引字段的值，你也可以选择 `储存` 字段的原始值以备日后取回。使用 Lucene 做后端的用户用储存字段来选择搜索结果的返回值，事实上，`_source` 字段就是一个储存字段。

在 Elasticsearch 中，单独设置储存字段不是一个好做法。完整的文档已经被保存在 `_source` 字段中。通常最好的办法会是使用 `_source` 参数来过滤你需要的字段。

元数据：_all 字段

在【简单搜索】中，我们介绍了 `_all` 字段：一个所有其他字段值的特殊字符串字段。`query_string` 在没有指定字段时默认用 `_all` 字段查询。

`_all` 字段在新应用的探索阶段比较管用，当你还不清楚最终文档的结构时，可以将任何查询用于这个字段，就有机会得到你想要的文档：

```
GET /_search
{
  "match": {
    "_all": "john smith marketing"
  }
}
```

随着你应用的发展，搜索需求会变得更加精准。你会越来越少的使用 `_all` 字段。`_all` 是一种简单粗暴的搜索方式。通过查询独立的字段，你能更灵活，强大和精准的控制搜索结果，提高相关性。

提示

【相关性算法】考虑的一个最重要的原则是字段的长度：字段越短，就越重要。在较短的 `title` 字段中的短语会比较长的 `content` 字段中的短语显得更重要。而字段间的这种差异在 `_all` 字段中就不会出现

如果你决定不再使用 `_all` 字段，你可以通过下面的映射禁用它：

```
PUT /my_index/_mapping/my_type
{
  "my_type": {
    "_all": { "enabled": false }
  }
}
```

通过 `include_in_all` 选项可以控制字段是否要被包含在 `_all` 字段中，默认值是 `true`。在一个对象上设置 `include_in_all` 可以修改这个对象所有字段的默认行为。

你可能想要保留 `_all` 字段来查询所有特定的全文字段，例如 `title`，`overview`，`summary` 和 `tags`。相对于完全禁用 `_all` 字段，你可以先默认禁用 `include_in_all` 选项，而选定字段上启用 `include_in_all`。

```
PUT /my_index/my_type/_mapping
{
  "my_type": {
    "include_in_all": false,
    "properties": {
      "title": {
        "type": "string",
        "include_in_all": true
      },
      ...
    }
  }
}
```

谨记 `_all` 字段仅仅是一个经过分析的 `string` 字段。它使用默认的分析器来分析它的值，而不管这值本来所在的字段指定的分析器。而且像所有 `string` 类型字段一样，你可以配置 `_all` 字段使用的分析器：

```
PUT /my_index/my_type/_mapping
{
  "my_type": {
    "_all": { "analyzer": "whitespace" }
  }
}
```


文档 ID

文档唯一标识由四个元数据字段组成：

`_id`：文档的字符串 ID

`_type`：文档的类型名

`_index`：文档所在的索引

`_uid`： `_type` 和 `_id` 连接成的 `type#id`

默认情况下，`_uid` 是被保存（可取回）和索引（可搜索）的。`_type` 字段被索引但是没有保存，`_id` 和 `_index` 字段则既没有索引也没有储存，它们并不是真实存在的。

尽管如此，你仍然可以像真实字段一样查询 `_id` 字段。Elasticsearch 使用 `_uid` 字段来追溯 `_id`。虽然你可以修改这些字段的 `index` 和 `store` 设置，但是基本上不需要这么做。

`_id` 字段有一个你可能用得上的设置：`path` 设置告诉 Elasticsearch 它需要从文档本身的哪个字段中生成 `_id`

```
PUT /my_index
{
  "mappings": {
    "my_type": {
      "_id": {
        "path": "doc_id" <1>
      },
      "properties": {
        "doc_id": {
          "type": "string",
          "index": "not_analyzed"
        }
      }
    }
  }
}
```

<1> 从 `doc_id` 字段生成 `_id`

然后，当你索引一个文档时：

```
POST /my_index/my_type
{
  "doc_id": "123"
}
```

`_id` 值由文档主体的 `doc_id` 字段生成。

```
{
  "_index": "my_index",
  "_type": "my_type",
  "_id": "123", <1>
  "_version": 1,
  "created": true
}
```

<1> `_id` 正确的生成了。

警告：虽然这样很方便，但是注意它对 `bulk` 请求（见【bulk 格式】）有个轻微的性能影响。处理请求的节点将不能仅靠解析元数据行来决定将请求分配给哪一个分片，而需要解析整个文档主体。

动态映射

当 Elasticsearch 遭遇一个位置的字段时，它通过【动态映射】来确定字段的数据类型且自动将该字段加到类型映射中。

有时这是理想的行为，有时却不是。或许你不知道今后会有哪些字段加到文档中，但是我希望它们能自动被索引。或许你仅仅想忽略它们。特别是当你使用 Elasticsearch 作为主数据源时，你希望未知字段能抛出一个异常来警示你。

幸运的是，你可以通过 `dynamic` 设置来控制这些行为，它接受下面几个选项：

`true` ：自动添加字段（默认）

`false` ：忽略字段

`strict` ：当遇到未知字段时抛出异常

`dynamic` 设置可以用在根对象或任何 `object` 对象上。你可以将 `dynamic` 默认设置为 `strict`，而在特定内部对象上启用它：

```
PUT /my_index
{
  "mappings": {
    "my_type": {
      "dynamic": "strict", <1>
      "properties": {
        "title": { "type": "string"},
        "stash": {
          "type": "object",
          "dynamic": true <2>
        }
      }
    }
  }
}
```

<1> 当遇到未知字段时，`my_type` 对象将会抛出异常

<2> `stash` 对象会自动创建字段

通过这个映射，你可以添加一个新的可搜索字段到 `stash` 对象中：

```
PUT /my_index/my_type/1
{
  "title": "This doc adds a new field",
  "stash": { "new_field": "Success!" }
}
```

但是在顶层做同样的操作则会失败：

```
PUT /my_index/my_type/1
{
  "title": "This throws a StrictDynamicMappingException",
  "new_field": "Fail!"
}
```

备注：将 `dynamic` 设置成 `false` 完全不会修改 `_source` 字段的内容。`_source` 将仍旧保持你索引时的完整 JSON 文档。然而，没有被添加到映射的未知字段将不可被搜索。

自定义动态索引

如果你想在运行时的增加新的字段，你可能会开启动态索引。虽然有时动态映射的 `规则` 显得不那么智能，幸运的是我们可以通过设置来自定义这些规则。

日期检测

当 Elasticsearch 遇到一个新的字符串字段时，它会检测这个字段是否包含一个可识别的日期，比如 `2014-01-01`。如果它看起来像一个日期，这个字段会被作为 `date` 类型添加，否则，它会被作为 `string` 类型添加。

有些时候这个规则可能导致一些问题。想象你有一个文档长这样：

```
{ "note": "2014-01-01" }
```

假设这是第一次见到 `note` 字段，它会被添加为 `date` 字段，但是如果下一个文档像这样：

```
{ "note": "Logged out" }
```

这显然不是一个日期，但为时已晚。这个字段已经被添加为日期类型，这个 `不合法的日期` 将引发异常。

日期检测可以通过在根对象上设置 `date_detection` 为 `false` 来关闭：

```
PUT /my_index
{
  "mappings": {
    "my_type": {
      "date_detection": false
    }
  }
}
```

使用这个映射，字符串将始终是 `string` 类型。假如你需要一个 `date` 字段，你得手动添加它。

提示：

Elasticsearch 判断字符串为日期的规则可以通过 [dynamic_date_formats](#) 配置来修改。

动态模板

使用 `dynamic_templates`，你可以完全控制新字段的映射，你设置可以通过字段名或数据类型应用一个完全不同的映射。

每个模板都有一个名字用于描述这个模板的用途，一个 `mapping` 字段用于指明这个映射怎么使用，和至少一个参数（例如 `match`）来定义这个模板适用于哪个字段。

模板按照顺序来检测，第一个匹配的模板会被启用。例如，我们给 `string` 类型字段定义两个模板：

- `es`：字段名以 `_es` 结尾需要使用 `spanish` 分析器。
- `en`：所有其他字段使用 `english` 分析器。

我们将 `es` 模板放在第一位，因为它比匹配所有字符串的 `en` 模板更特殊一点

```
PUT /my_index
{
  "mappings": {
    "my_type": {
      "dynamic_templates": [
```

```

        { "es": {
          "match":      "*_es", <1>
          "match_mapping_type": "string",
          "mapping": {
            "type":      "string",
            "analyzer":   "spanish"
          }
        }},
        { "en": {
          "match":      "*", <2>
          "match_mapping_type": "string",
          "mapping": {
            "type":      "string",
            "analyzer":   "english"
          }
        }
      }
    ]
  }
}

```

<1> 匹配字段名以 `_es` 结尾的字段。

<2> 匹配所有字符串类型字段。

`match_mapping_type` 允许你限制模板只能使用在特定的类型上，就像由标准动态映射规则检测的一样，（例如 `strong` 和 `long`）

`match` 参数只匹配字段名， `path_match` 参数则匹配字段在一个对象中的完整路径，所以 `address.*.name` 规则将匹配一个这样的字段：

```

{
  "address": {
    "city": {
      "name": "New York"
    }
  }
}

```

`unmatch` 和 `path_unmatch` 规则将用于排除未被匹配的字段。

更多选项见[根对象参考文档](#)

默认映射

通常，一个索引中的所有类型具有共享的字段和设置。用 `_default_` 映射来指定公用设置会更加方便，而不是每次创建新的类型时重复操作。`_default_` 映射像新类型的模板。所有在 `_default_` 映射之后的类型将包含所有的默认设置，除非在自己的类型映射中明确覆盖这些配置。

例如，我们可以使用 `_default_` 映射对所有类型禁用 `_all` 字段，而只在 `blog` 字段上开启它：

```
PUT /my_index
{
  "mappings": {
    "_default_": {
      "_all": { "enabled": false }
    },
    "blog": {
      "_all": { "enabled": true }
    }
  }
}
```

`_default_` 映射也是定义索引级别的动态模板的好地方。

重新索引数据

虽然你可以给索引添加新的类型，或给类型添加新的字段，但是你不能添加新的分析器或修改已有字段。假如你这样做，已被索引的数据会变得不正确而你的搜索也不会正常工作。

修改在已存在的数据最简单的方法是重新索引：创建一个新配置好的索引，然后将所有的文档从旧的索引复制到新的上。

`_source` 字段的一个最大的好处是你已经在 Elasticsearch 中有了完整的文档，你不再需要从数据库中重建你的索引，这通常会比较慢。

为了更高效的索引旧索引中的文档，使用【scan-scroll】来批量读取旧索引的文档，然后将通过【bulk API】来将它们推送给新的索引。

批量重新索引：

你可以在同一时间执行多个重新索引的任务，但是你显然不愿意它们的结果有重叠。所以，可以将重建大索引的任务通过日期或时间戳字段拆分成较小的任务：

```
GET /old_index/_search?search_type=scan&scroll=1m
{
  "query": {
    "range": {
      "date": {
        "gte": "2014-01-01",
        "lt": "2014-02-01"
      }
    }
  },
  "size": 1000
}
```

假如你继续在旧索引上做修改，你可能想确保新增的文档被加到了新的索引中。这可以通过重新运行重建索引程序来完成，但是记得只要过滤出上次执行后新增的文档就行了。

索引别名和零停机时间

前面提到的重新索引过程中的问题是必须更新你的应用，来使用另一个索引名。索引别名正是用来解决这个问题的！

索引别名就像一个快捷方式或软连接，可以指向一个或多个索引，也可以给任何需要索引名的 API 使用。别名带给我们极大的灵活性，允许我们做到：

- 在一个运行的集群上无缝的从一个索引切换到另一个
- 给多个索引分类（例如，`last_three_months`）
- 给索引的一个子集创建 `视图`

我们以后会讨论更多别名的使用场景。现在我们将介绍用它们怎么在零停机时间内从旧的索引切换到新的索引。

这里有两种管理别名的途径：`_alias` 用于单个操作，`_aliases` 用于原子化多个操作。

在这一章中，我们假设你的应用采用一个叫 `my_index` 的索引。而事实上，`my_index` 是一个指向当前真实索引的别名。真实的索引名将包含一个版本号：`my_index_v1`，`my_index_v2` 等等。

开始，我们创建一个索引 `my_index_v1`，然后将别名 `my_index` 指向它：

```
PUT /my_index_v1 <1>
PUT /my_index_v1/_alias/my_index <2>
```

<1> 创建索引 `my_index_v1`。

<2> 将别名 `my_index` 指向 `my_index_v1`。

你可以检测这个别名指向哪个索引：

```
GET /*/_alias/my_index
```

或哪些别名指向这个索引：

```
GET /my_index_v1/_alias/*
```

两者都将返回下列值：

```
{
  "my_index_v1" : {
    "aliases" : {
      "my_index" : { }
    }
  }
}
```

然后，我们决定修改索引中一个字段的映射。当然我们不能修改现存的映射，索引我们需要重新索引数据。首先，我们创建有新的映射的索引 `my_index_v2`。

```
PUT /my_index_v2
{
  "mappings": {
    "my_type": {
      "properties": {
        "tags": {
          "type": "string",
          "index": "not_analyzed"
        }
      }
    }
  }
}
```

```
    }  
  }  
}
```

然后我们从将数据从 `my_index_v1` 迁移到 `my_index_v2`，下面的过程在【重新索引】中描述过了。一旦我们认为数据已经被正确的索引了，我们就将别名指向新的索引。

别名可以指向多个索引，所以我们需要在新索引中添加别名的同时从旧索引中删除它。这个操作需要原子化，所以我们需要用 `_aliases` 操作：

```
POST /_aliases  
{  
  "actions": [  
    { "remove": { "index": "my_index_v1", "alias": "my_index" }},  
    { "add": { "index": "my_index_v2", "alias": "my_index" }}  
  ]  
}
```

这样，你的应用就从旧索引迁移到了新的，而没有停机时间。

提示：

即使你认为现在的索引设计已经是完美的了，当你的应用在生产环境使用时，还是有可能在今后有一些改变的。

所以请做好准备：在应用中使用别名而不是索引。然后你就可以在任何时候重建索引。别名的开销很小，应当广泛使用。

In <>, we introduced the *shard*, and described(("shards")) it as a low-level *worker unit*. But what exactly *is* a shard and how does it work? In this chapter, we answer these questions:

- Why is search *near* real-time?
- Why are document CRUD (create-read-update-delete) operations *real-time*?
- How does Elasticsearch ensure that the changes you make are durable, that they won't be lost if there is a power failure?
- Why does deleting documents not free up space immediately?
- What do the `refresh`, `flush`, and `optimize` APIs do, and when should you use them?

The easiest way to understand how a shard functions today is to start with a history lesson. We will look at the problems that needed to be solved in order to provide a distributed durable data store with near real-time search and analytics.

.Content Warning

The information presented in this chapter is for your interest. You are not required to understand and remember all the detail in order to use Elasticsearch. Read this chapter to gain a taste for how things work, and to know where the information is in case you need to refer to it in the future, but don't be overwhelmed by the detail.

[[making-text-searchable]] === Making Text Searchable

The first challenge that had to be solved was how to(("text", "making it searchable")) make text searchable. Traditional databases store a single value per field, but this is insufficient for full-text search. Every word in a text field needs to be searchable, which means that the database needs to be able to index multiple values--words, in this case--in a single field.

The data structure that best supports the *multiple-values-per-field* requirement is the *inverted index*, which(("inverted index")) we introduced in <>. The inverted index contains a sorted list of all of the unique values, or *terms*, that occur in any document and, for each term, a list of all the documents that contain it.

Term	Doc 1	Doc 2	Doc 3	...

brown	X		X	...
fox	X	X	X	...
quick	X	X		...
the	X		X	...

[NOTE]

When discussing inverted indices, we talk about indexing *documents* because, historically, an inverted index was used to index whole unstructured text documents. A *document* in Elasticsearch is a structured JSON document with fields and values. In reality, every indexed field in a JSON document has its

own inverted index.

The inverted index may hold a lot more information than the list of documents that contain a particular term. It may store a count of the number of documents that contain each term, the number of times a term appears in a particular document, the order of terms in each document, the length of each document, the average length of all documents, and more. These statistics allow Elasticsearch to determine which terms are more important than others, and which documents are more important than others, as described in <>.

The important thing to realize is that the inverted index needs to know about *all* documents in the collection in order for it to function as intended.

In the early days of full-text search, one big inverted index was built for the entire document collection and written to disk. As soon as the new index was ready, it replaced the old index, and recent changes became searchable.

[role="pagebreak-before"] ==== Immutability

The inverted index that is written to disk is *immutable*: it doesn't change.(("inverted index", "immutability")) Ever. This immutability has important benefits:

- There is no need for locking. If you never have to update the index, you never have to worry about multiple processes trying to make changes at the same time.
- Once the index has been read into the kernel's filesystem cache, it stays there, because it never changes. As long as there is enough space in the filesystem cache, most reads will come from memory instead of having to hit disk. This provides a big performance boost.
- Any other caches (like the filter cache) remain valid for the life of the index. They don't need to be rebuilt every time the data changes, because the data doesn't change.
- Writing a single large inverted index allows the data to be compressed, reducing costly disk I/O and the amount of RAM needed to cache the index.

Of course, an immutable index has its downsides too, primarily the fact that it is immutable! You can't change it. If you want

to make new documents searchable, you have to rebuild the entire index. This places a significant limitation either on the amount of data that an index can contain, or the frequency with which the index can be updated.

[[dynamic-indices]] === Dynamically Updatable Indices

The next problem that needed to be (((("indices", "dynamically updatable"))))solved was how to make an inverted index updatable without losing the benefits of immutability? The answer turned out to be: use more than one index.

Instead of rewriting the whole inverted index, add new supplementary indices to reflect more-recent changes. Each inverted index can be queried in turn--starting with the oldest--and the results combined.

Lucene, the Java libraries on which Elasticsearch is based, introduced the concept of *per-segment search*. (((("per-segment search"))))(((("segments"))))(((("indices", "in Lucene")))) A *segment* is an inverted index in its own right, but now the word *index* in Lucene came to mean a *collection of segments* plus a *commit point*—a file(((("commit point")))) that lists all known segments, as depicted in <>. New documents are first added to an in-memory indexing buffer, as shown in <>, before being written to an on-disk segment, as in <>

[[img-index-segments]] .A Lucene index with a commit point and three segments image::images/elas_1101.png["A Lucene index with a commit point and three segments"]

.Index Versus Shard

To add to the confusion, a *Lucene index* is what we call a *shard* in Elasticsearch, while an *index* in Elasticsearch(((("indices", "in Elasticsearch"))))(((("shards", "indices versus")))) is a collection of shards. When Elasticsearch searches an index, it sends the query out to a copy of every shard (Lucene index) that belongs to the index, and then reduces the per-shards results to a global result set, as described in <>.

A per-segment search works as follows:

1. New documents are collected in an in-memory indexing buffer. See <>.
2. Every so often, the buffer is *committed*:

A new segment--a supplementary inverted index--is written to disk. A new *commit point* is written to disk, which includes the name of the new segment. ** The disk is *fsync'ed*—all writes waiting in the filesystem cache are flushed to disk, to ensure that they have been physically written.

1. The new segment is opened, making the documents it contains visible to search.
2. The in-memory buffer is cleared, and is ready to accept new documents.

[[img-memory-buffer]] .A Lucene index with new documents in the in-memory buffer, ready to commit image::images/elas_1102.png["A Lucene index with new documents in the in-memory buffer, ready to commit"]

[[img-post-commit]] .After a commit, a new segment is added to the commit point and the buffer is cleared image::images/elas_1103.png["After a commit, a new segment is added to the index and the buffer is cleared"]

When a query is issued, all known segments are queried in turn. Term statistics are aggregated across all segments to ensure that the relevance of each term and each document is calculated accurately. In this way, new documents can be added to the index relatively cheaply.

[[deletes-and-updates]] ==== Deletes and Updates

Segments are immutable, so documents cannot be removed from older segments, nor can older segments be updated to reflect a newer version of a document. Instead, every (((("deleted documents"))))commit point includes a `.del` file that lists which documents in which segments have been deleted.

When a document is `'deleted,'` it is actually just `_marked_` as deleted in the `.del` file. A document that has been marked as deleted can still match a query, but it is removed from the results list before the final query results are returned.

Document updates work in a similar way: when a document is updated, the old version of the document is marked as

deleted, and the new version of the document is indexed in a new segment. Perhaps both versions of the document will match a query, but the older deleted version is removed before the query results are returned.

In <>, we show how deleted documents are purged from the filesystem.

[[near-real-time]] === Near Real-Time Search

With the development of per-segment search, the delay between indexing a document and making it visible to search dropped dramatically. New documents could be made searchable within minutes, but that still isn't fast enough.

The bottleneck is the disk. Committing a new segment to disk requires an <http://en.wikipedia.org/wiki/Fsync> to ensure that the segment is physically written to disk and that data will not be lost if there is a power failure. But an `fsync` is costly; it cannot be performed every time a document is indexed without a big performance hit.

What was needed was a more lightweight way to make new documents visible to search, which meant removing `fsync` from the equation.

Sitting between Elasticsearch and the disk is the filesystem cache. As before, documents in the in-memory indexing buffer (<>) are written to a new segment (<>). But the new segment is written to the filesystem cache first--which is cheap--and only later is it flushed to disk--which is expensive. But once a file is in the cache, it can be opened and read, just like any other file.

[[img-pre-refresh]] .A Lucene index with new documents in the in-memory buffer image::images/elas_1104.png["A Lucene index with new documents in the in-memory buffer"]

Lucene allows new segments to be written and opened--making the documents they contain visible to search--without performing a full commit. This is a much lighter process than a commit, and can be done frequently without ruining performance.

[[img-post-refresh]] .The buffer contents have been written to a segment, which is searchable, but is not yet committed image::images/elas_1105.png["The buffer contents have been written to a segment, which is searchable, but is not yet committed"]

[[refresh-api]] ==== refresh API

In Elasticsearch, this lightweight process of writing and opening a new segment is called a *refresh*. By default, every shard is refreshed automatically once every second. This is why we say that Elasticsearch has *near* real-time search: document changes are not visible to search immediately, but will become visible within 1 second.

This can be confusing for new users: they index a document and try to search for it, and it just isn't there. The way around this is to perform a manual refresh, with the `refresh` API:

[source,json]

POST /_refresh <1>

POST /blogs/_refresh <2>

<1> Refresh all indices.

<2> Refresh just the `blogs` index.

[TIP]

While a refresh is much lighter than a commit, it still has a performance cost. A manual refresh can be useful when writing tests, but don't do a manual refresh every time you index a document in production; it will hurt your performance. Instead, your application needs to be aware of the near

real-time nature of Elasticsearch and make allowances for it.

Not all use cases require a refresh every second. Perhaps you are using Elasticsearch to index millions of log files, and you would prefer to optimize for index speed rather than near real-time search. You can reduce the frequency of refreshes on a per-index basis by (((("refresh_interval setting"))))setting the `refresh_interval` :

[source,json]

```
PUT /my_logs { "settings": { "refresh_interval": "30s" <1> } }
```

```
}
```

<1> Refresh the `my_logs` index every 30 seconds.

The `refresh_interval` can be updated dynamically on an existing index. You can turn off automatic refreshes while you are building a big new index, and then turn them back on when you start using the index in production:

[source,json]

```
POST /my_logs/_settings { "refresh_interval": -1 } <1>
```

```
POST /my_logs/_settings
```

```
{ "refresh_interval": "1s" } <2>
```

<1> Disable automatic refreshes.

<2> Refresh automatically every second.

CAUTION: The `refresh_interval` expects a *duration* such as `1s` (1 second) or `2m` (2 minutes). An absolute number like `1` means *1 millisecond*--a sure way to bring your cluster to its knees.

[[translog]] === Making Changes Persistent

Without an `fsync` to flush data in the filesystem cache to disk, we cannot be sure that the data will still ("persistent changes, making")("changes, persisting")be there after a power failure, or even after exiting the application normally. For Elasticsearch to be reliable, it needs to ensure that changes are persisted to disk.

In <>, we said that a full commit flushes segments to disk and writes a commit point, which lists all known segments. ("commit point") Elasticsearch uses this commit point during startup or when reopening an index to decide which segments belong to the current shard.

While we refresh once every second to achieve near real-time search, we still need to do full commits regularly to make sure that we can recover from failure. But what about the document changes that happen between commits? We don't want to lose those either.

Elasticsearch added a *translog*, or transaction log,("translog (transaction log)") which records every operation in Elasticsearch as it happens. With the translog, the process now looks like this:

1. When a document is indexed, it is added to the in-memory buffer *and* appended to the translog, as shown in <>. +
[[img-xlog-pre-refresh]] .New documents are added to the in-memory buffer and appended to the transaction log
image::images/elas_1106.png["New documents are added to the in-memory buffer and appended to the transaction log"]
2. The refresh leaves the shard in the state depicted in <>. Once every second, the shard is refreshed:

+

The docs in the in-memory buffer are written to a new segment, without an `fsync`. The segment is opened to make it visible to search.

** The in-memory buffer is cleared.

[[img-xlog-post-refresh]] .After a refresh, the buffer is cleared but the transaction log is not

image::images/elas_1107.png["After a refresh, the buffer is cleared but the transaction log is not"]

1. This process continues with more documents being added to the in-memory buffer and appended to the transaction log (see <>). + [[img-xlog-pre-flush]] .The transaction log keeps accumulating documents
image::images/elas_1108.png["The transaction log keeps accumulating documents"]
1. Every so often--such as when the translog is getting too big--the index is flushed; a new translog is created, and a full commit is performed (see <>):

+


Any docs in the in-memory buffer are written to a new segment. The buffer is cleared. **A commit point is written to disk.** The filesystem cache is flushed with an `fsync`. ** The old translog is deleted.

--

The translog provides a persistent record of all operations that have not yet been flushed to disk. When starting up, Elasticsearch will use the last commit point to recover known segments from disk, and will then replay all operations in the translog to add the changes that happened after the last commit.

The translog is also used to provide real-time CRUD. When you try to retrieve, update, or delete a document by ID, it first

checks the translog for any recent changes before trying to retrieve the document from the relevant segment. This means that it always has access to the latest known version of the document, in real-time.

. After a flush, the segments are fully committed and the transaction log is cleared

==== flush API

The action of performing a commit and truncating the translog is known in Elasticsearch as a *flush*. Shards are flushed automatically every 30 minutes, or when the translog becomes too big. See the <http://bit.ly/1E3HKbD> for settings that can be used to control these thresholds:

The <http://bit.ly/1ICgxiU> API can be used to perform a manual flush:

[source,json]

POST /blogs/_flush <1>

POST /_flush?wait_for_ongoing <2>

<1> Flush the `blogs` index.

<2> Flush all indices and wait until all flushes have completed before returning.

You seldom need to issue a manual `flush` yourself; usually, automatic flushing is all that is required.

That said, it is beneficial to `<>` your indices before restarting a node or closing an index. When Elasticsearch tries to recover or reopen an index, it has to replay all of the operations in the translog, so the shorter the log, the faster the recovery.

.How Safe Is the Translog?

The purpose of the translog is to ensure that operations are not lost. This begs the question: how safe is the translog (transaction log), "safety of") is the translog?

Writes to a file will not survive a reboot until the file has been `+fsync+`ed to disk. By default, the translog is `+fsync+`ed every 5 seconds. Potentially, we could lose 5 seconds worth of data--if the translog were the only mechanism that we had for dealing with failure.

Fortunately, the translog is only part of a much bigger system. Remember that an indexing request is considered successful only after it has completed on both the primary shard and all replica shards. Even if the node holding the primary shard were to suffer catastrophic failure, it would be unlikely to affect the nodes holding the replica shards at the same time.

While we could force the translog to `fsync` more frequently (at the cost of indexing performance), it is unlikely to provide more reliability.

[[merge-process]] === Segment Merging

With the automatic refresh process creating a new segment(("segments", "merging")) every second, it doesn't take long for the number of segments to explode. Having too many segments is a problem. Each segment consumes file handles, memory, and CPU cycles. More important, every search request has to check every segment in turn; the more segments there are, the slower the search will be.

Elasticsearch solves this problem by merging segments in the background(("merging segments")) Small segments are merged into bigger segments, which, in turn, are merged into even bigger segments.

This is the moment when those old deleted documents(("deleted documents", "purging of")) are purged from the filesystem. Deleted documents (or old versions of updated documents) are not copied over to the new bigger segment.

There is nothing you need to do to enable merging. It happens automatically while you are indexing and searching. The process works like as depicted in <>:

1. While indexing, the refresh process creates new segments and opens them for search.
2. The merge process selects a few segments of similar size and merges them into a new bigger segment in the background. This does not interrupt indexing and searching. + [[img-merge]] .Two committed segments and one uncommitted segment in the process of being merged into a bigger segment image::images/elas_1110.png["Two committed segments and one uncommitted segment in the process of being merged into a bigger segment"]
3. <> illustrates activity as the merge completes:

+

The new segment is flushed to disk. A new commit point is written that includes the new segment and

excludes the old, smaller segments.

The new segment is opened for search. The old segments are deleted.

[[img-post-merge]] .Once merging has finished, the old segments are deleted

image::images/elas_1111.png["Once merging has finished, the old segments are deleted"]

The merging of big segments can use a lot of I/O and CPU, which can hurt search performance if left unchecked. By default, Elasticsearch throttles the merge process so that search still has enough resources available to perform well.

TIP: See <> for advice about tuning merging for your use case.

[[optimize-api]] ==== optimize API

The `optimize` API is best(("merging segments", "optimize API and"))(("optimize API"))(("segments", "merging", "optimize API"))described as the *forced merge* API. It forces a shard to be merged down to the number of segments specified in the `max_num_segments` parameter. The intention is to reduce the number of segments (usually to one) in order to speed up search performance.

WARNING: The `optimize` API should *not* be used on a dynamic index--an index that is being actively updated. The background merge process does a very good job, and optimizing will hinder the process. Don't interfere!

In certain specific circumstances, the `optimize` API can be beneficial. The typical use case is for logging, where logs are stored in an index per day, week, or month. Older indices are essentially read-only; they are unlikely to change.

In this case, it can be useful to optimize the shards of an old index down to a single segment each; it will use fewer resources and searches will be quicker:

[source,json]

**POST /logstash-2014-10/_optimize?max_num_segments=1
<1>**

<1> Merges each shard in the index down to a single segment

[WARNING]

Be aware that merges triggered by the `optimize` API are not throttled at all. They can consume all of the I/O on your nodes, leaving nothing for search and potentially making your cluster unresponsive. If you plan on optimizing an index, you should use shard allocation (see <>) to first move the index to a node where it is safe to

run.

结构化搜索

结构化搜索 是指查询包含内部结构的数据。日期，时间，和数字都是结构化的：它们有明确的格式给你执行逻辑操作。一般包括比较数字或日期的范围，或确定两个值哪个大。

文本也可以被结构化。一包蜡笔有不同的颜色：红色，绿色，蓝色。一篇博客可能被打上 分布式 和 搜索 的标签。电子商务产品有商品统一代码（UPCs）或其他有着严格格式的标识。

通过结构化搜索，你的查询结果始终是 是或非；是否应该属于集合。结构化搜索不关心文档的相关性或分数，它只是简单的包含或排除文档。

这必须是有意义的逻辑，一个数字不能比同一个范围中的其他数字 更多。它只能包含在一个范围中 —— 或不在其中。类似的，对于结构化文本，一个值必须相等或不等。这里没有 更匹配 的概念。

查找准确值

对于准确值，你需要使用过滤器。过滤器的重要性在于它们非常的快。它们不计算相关性（避开所有计分阶段）而且很容易被缓存。我们今后再来讨论过滤器的性能优势【过滤器缓存】，现在，请先记住尽可能多的使用过滤器。

用于数字的 `term` 过滤器

我们下面将介绍 `term` 过滤器，首先因为你可能经常会用到它，这个过滤器旨在处理数字，布尔值，日期，和文本。

我们来看一下例子，一些产品最初用数字来索引，包含两个字段 `price` 和 `productID`：

```
POST /my_store/products/_bulk
{ "index": { "_id": 1 } }
{ "price" : 10, "productID" : "XHDK-A-1293-#fJ3" }
{ "index": { "_id": 2 } }
{ "price" : 20, "productID" : "KDKE-B-9947-#kL5" }
{ "index": { "_id": 3 } }
{ "price" : 30, "productID" : "JODL-X-1937-#pV7" }
{ "index": { "_id": 4 } }
{ "price" : 30, "productID" : "QQPX-R-3956-#aD8" }
```

我们的目标是找出特定价格的产品。假如你有关系型数据库背景，可能用 SQL 来表现这次查询比较熟悉，它看起来像这样：

```
SELECT document
FROM products
WHERE price = 20
```

在 Elasticsearch DSL 中，我们使用 `term` 过滤器来实现同样的事。`term` 过滤器会查找我们设定的准确值。`term` 过滤器本身很简单，它接受一个字段名和我们希望查找的值：

```
{
  "term" : {
    "price" : 20
  }
}
```

`term` 过滤器本身并不能起作用。像在【查询 DSL】中介绍的一样，搜索 API 需要得到一个查询语句，而不是一个过滤器。为了使用 `term` 过滤器，我们需要将它包含在一个过滤查询语句中：

```
GET /my_store/products/_search
{
  "query" : {
    "filtered" : { <1>
      "query" : {
        "match_all" : {} <2>
      },
      "filter" : {
        "term" : { <3>
          "price" : 20
        }
      }
    }
  }
}
```

<1> `filtered` 查询同时接受接受 `query` 与 `filter`。

<2> `match_all` 用来匹配所有文档，这是默认行为，所以在以后的例子中我们将省略掉 `query` 部分。

<3> 这是我们上面见过的 `term` 过滤器。注意它在 `filter` 分句中的位置。

执行之后，你将得到预期的搜索结果：只能文档 2 被返回了（因为只有 2 的价格是 20）：

```
"hits" : [
  {
    "_index" : "my_store",
    "_type" : "products",
    "_id" : "2",
    "_score" : 1.0, <1>
    "_source" : {
      "price" : 20,
      "productID" : "KDKE-B-9947-#kL5"
    }
  }
]
```

<1> 过滤器不会执行计分和计算相关性。分值由 `match_all` 查询产生，所有文档一视同仁，所有每个结果的分值都是 1

用于文本的 `term` 过滤器

像我们在开头提到的，`term` 过滤器可以像匹配数字一样轻松的匹配字符串。让我们通过特定 UPC 标识码来找出产品，而不是通过价格。如果用 SQL 来实现，我们可能会使用下面的查询：

```
SELECT product
FROM products
WHERE productID = "XHDK-A-1293-#fJ3"
```

转到查询 DSL，我们用 `term` 过滤器来构造一个类似的查询：

```
GET /my_store/products/_search
{
  "query" : {
    "filtered" : {
      "filter" : {
        "term" : {
          "productID" : "XHDK-A-1293-#fJ3"
        }
      }
    }
  }
}
```

有点出乎意料：我们没有得到任何结果值！为什么呢？问题不在于 `term` 查询；而在于数据被索引的方式。如果我们使用 `analyze` API，我们可以看到 UPC 被分解成短小的表征：

```
GET /my_store/_analyze?field=productID
XHDK-A-1293-#fJ3
```

```
{
  "tokens" : [ {
    "token" : "xhdk",
    "start_offset" : 0,
    "end_offset" : 4,
    "type" : "<ALPHANUM>",
    "position" : 1
  }, {
    "token" : "a",
    "start_offset" : 5,
    "end_offset" : 6,
    "type" : "<ALPHANUM>",
    "position" : 2
  }, {
    "token" : "1293",
    "start_offset" : 7,
    "end_offset" : 11,
```

```

    "type" :      "<NUM>",
    "position" :   3
  }, {
    "token" :      "fj3",
    "start_offset" : 13,
    "end_offset" : 16,
    "type" :      "<ALPHANUM>",
    "position" :   4
  } ]
}

```

这里有一些要点：

- 我们得到了四个分开的表征，而不是一个完整的表征来表示 UPC。
- 所有的字符都被转为了小写。
- 我们失去了连字符和 # 符号。

所以当我们用 `XHDK-A-1293-#fJ3` 来查找时，得不到任何结果，因为这个表征不在我们的倒排索引中。相反，那里有上面列出的四个表征。

显然，在处理唯一标识码，或其他枚举值时，这不是我们想要的结果。

为了避免这种情况发生，我们需要通过设置这个字段为 `not_analyzed` 来告诉 Elasticsearch 它包含一个准确值。我们曾在【自定义字段映射】中见过它。为了实现目标，我们要先删除旧索引（因为它包含了错误的映射），并创建一个正确映射的索引：

```

DELETE /my_store <1>

PUT /my_store <2>
{
  "mappings" : {
    "products" : {
      "properties" : {
        "productID" : {
          "type" : "string",
          "index" : "not_analyzed" <3>
        }
      }
    }
  }
}

```

<1> 必须首先删除索引，因为我们不能修改已经存在的映射。

<2> 删除后，我们可以用自定义的映射来创建它。

<3> 这里我们明确表示不希望 `productID` 被分析。

现在我们可以继续重新索引文档：

```

POST /my_store/products/_bulk
{ "index": { "_id": 1 }}
{ "price" : 10, "productID" : "XHDK-A-1293-#fJ3" }
{ "index": { "_id": 2 }}
{ "price" : 20, "productID" : "KDKE-B-9947-#kL5" }
{ "index": { "_id": 3 }}
{ "price" : 30, "productID" : "JODL-X-1937-#pV7" }
{ "index": { "_id": 4 }}
{ "price" : 30, "productID" : "QQPX-R-3956-#aD8" }

```

现在我们的 `term` 过滤器将按预期工作。让我们在新索引的数据上再试一次（注意，查询和过滤都没有修改，只是数据被重新映射了）。

```
GET /my_store/products/_search
{
  "query" : {
    "filtered" : {
      "filter" : {
        "term" : {
          "productID" : "XHDK-A-1293-#fJ3"
        }
      }
    }
  }
}
```

`productID` 字段没有经过分析，`term` 过滤器也没有执行分析，所以这条查询找到了准确匹配的值，如期返回了文档 1。

内部过滤操作

Elasticsearch 在内部会通过一些操作来执行一次过滤：

1. 查找匹配文档。

`term` 过滤器在倒排索引中查找词 `XHDK-A-1293-#fJ3`，然后返回包含那个词的文档列表。在这个例子中，只有文档 1 有我们想要的词。

2. 创建字节集

然后过滤器将创建一个字节集——一个由 1 和 0 组成的数组——描述哪些文档包含这个词。匹配的文档得到 1 字节，在我们的例子中，字节集将是 `[1,0,0,0]`

3. 缓存字节集

最后，字节集被储存在内存中，以使我们能用它来跳过步骤 1 和 2。这大大的提升了性能，让过滤变得非常的快。

当执行 `filtered` 查询时，`filter` 会比 `query` 早执行。结果字节集会被传给 `query` 来跳过已经被排除的文档。这种过滤器提升性能的方式，查询更少的文档意味着更快的速度。

[[combining-filters]] === Combining Filters

The previous two examples showed a single filter in use.(((("structured search", "combining filters")))((("filters", "combining")))) In practice, you will probably need to filter on multiple values or fields. For example, how would you express this SQL in Elasticsearch?

[source,sql]

```
SELECT product FROM products WHERE (price = 20 OR productID = "XHDK-A-1293-#fJ3")
```

AND (price != 30)

In these situations, you will need the `bool` filter.(((("filters", "combining", "in bool filter")))((("bool filter")))) This is a *compound filter* that accepts other filters as arguments, combining them in various Boolean combinations.

[[bool-filter]] ==== Bool Filter

The `bool` filter is composed of three sections:

[source,js]

```
{ "bool" : { "must" : [], "should" : [], "must_not" : [], }
```

```
}
```

`must` ::

All of these clauses *must* match. The equivalent of `AND` .

`must_not` :: All of these clauses *must not* match. The equivalent of `NOT` .

`should` ::

At least one of these clauses must match. The equivalent of `OR` .

And that's it!(((("should clause", "in bool filters")))((("must_not clause", "in bool filters")))((("must clause", "in bool filters")))) When you need multiple filters, simply place them into the different sections of the `bool` filter.

[NOTE]

Each section of the `bool` filter is optional (for example, you can have a `must` clause and nothing else), and each section can contain a single filter or an

array of filters.

To replicate the preceding SQL example, we will take the two `term` filters that we used(((("term filter", "placing inside bool filter")))((("bool filter", "with two term filters in should clause and must_not clause")))) previously and place them inside the `should` clause of a `bool` filter, and add another clause to deal with the `NOT` condition:

[source,js]

```
GET /my_store/products/_search { "query" : { "filtered" : { <1> "filter" : { "bool" : { "should" : [ { "term" : { "price" : 20 }}, <2> { "term" : { "productID" : "XHDK-A-1293-#fJ3" } } <2> ], "must_not" : { "term" : { "price" : 30 } <3> } } } }
```



```
}
```

```
// SENSE: 080_Structured_Search/10_Bool_filter.json
```

<1> Note that we still need to use a `filtered` query to wrap everything.

<2> These two `term` filters are *children* of the `bool` filter, and since they are placed inside the `should` clause, at least one of them needs to match.

<3> If a product has a price of `30`, it is automatically excluded because it matches a `must_not` clause.

Our search results return two hits, each document satisfying a different clause in the `bool` filter:

[source,json]

```
"hits": [ { "_id": "1", "_score": 1.0, "_source": { "price": 10, "productID": "XHDK-A-1293-#fJ3" } }, { "_id": "2", "_score": 1.0, "_source": { "price": 20, "productID": "KDKE-B-9947-#kL5" } } ]
```

```
]
```

<1> Matches the `term` filter for `productID = "XHDK-A-1293-#fJ3"`

<2> Matches the `term` filter for `price = 20`

==== Nesting Boolean Filters

Even though `bool` is a compound filter and accepts children filters, it is important to understand that `bool` is just a filter itself.(((("filters", "combining", "nesting bool filters")))((("bool filter", "nesting in another bool filter")))) This means you can nest `bool` filters inside other `bool` filters, giving you the ability to make arbitrarily complex Boolean logic.

Given this SQL statement:

[source,sql]

```
SELECT document FROM products WHERE productID = "KDKE-B-9947-#kL5" OR ( productID = "JODL-X-1937-#pV7"
```

```
AND price = 30 )
```

We can translate it into a pair of nested `bool` filters:

[source,js]

```
GET /my_store/products/_search { "query": { "filtered": { "filter": { "bool": { "should": [ { "term": { "productID": "KDKE-B-9947-#kL5" } }, <1> { "bool": { <1> "must": [ { "term": { "productID": "JODL-X-1937-#pV7" } }, <2> { "term": { "price": 30 } } } ] } } } } }
```

```
}
```

```
// SENSE: 080_Structured_Search/10_Bool_filter.json
```

<1> Because the `term` and the `bool` are sibling clauses inside the first Boolean `should`, at least one of these filters must

match for a document to be a hit.

<2> These two `term` clauses are siblings in a `must` clause, so they both have to match for a document to be returned as a hit.

The results show us two documents, one matching each of the `should` clauses:

[source,json]

```
"hits": [ { "_id": "2", "_score": 1.0, "_source": { "price": 20, "productID": "KDKE-B-9947-#kL5" <1> } }, { "_id": "3",  
"_score": 1.0, "_source": { "price": 30, <2> "productID": "JODL-X-1937-#pV7" <2> } }
```

]

<1> This `productID` matches the `term` in the first `bool` .

<2> These two fields match the `term` filters in the nested `bool` .

This was a simple example, but it demonstrates how Boolean filters can be used as building blocks to construct complex logical conditions.

=== Finding Multiple Exact Values

The `term` filter is useful for finding a single value, but often you'll want to search for multiple values.(((("exact values", "finding multiple")))((("structured search", "finding multiple exact values")))) What if you want to find documents that have a price of \$20 or \$30?

Rather than using multiple `term` filters, you can instead use a single `terms` filter (note the s at the end). The `terms` filter(((("terms filter")))) is simply the plural version of the singular `term` filter.

It looks nearly identical to a vanilla `term` too. Instead of specifying a single price, we are now specifying an array of values:

[source,js]

```
{ "terms" : { "price" : [20, 30] }
```

```
}
```

And like the `term` filter, we will place it inside a `filtered` query to (((("filtered query", "terms filter in")))) use it:

[source,js]

```
GET /my_store/products/_search { "query" : { "filtered" : { "filter" : { "terms" : { <1> "price" : [20, 30] } } } }
```

```
}
```

// SENSE: 080_Structured_Search/15_Terms_filter.json

<1> The `terms` filter as seen previously, but placed inside the `filtered` query

The query will return the second, third, and fourth documents:

[source,json]

```
"hits" : [ { "_id" : "2", "_score" : 1.0, "_source" : { "price" : 20, "productID" : "KDKE-B-9947-#kL5" } }, { "_id" : "3", "_score" : 1.0, "_source" : { "price" : 30, "productID" : "JODL-X-1937-#pV7" } }, { "_id" : "4", "_score" : 1.0, "_source" : { "price" : 30, "productID" : "QQPX-R-3956-#aD8" } }
```

```
]
```

==== Contains, but Does Not Equal

It is important to understand that `term` and `terms` are *contains* operations, not *equals*.(((("structured search", "contains, but does not equal")))((("terms filter", "contains, but does not equal")))((("term filter", "contains, but does not equal")))) What does that mean?

If you have a term filter for `{ "term" : { "tags" : "search" } }`, it will match *both* of the following documents:

[source,js]

```
{ "tags" : ["search"] }
```

{ "tags" : ["search", "open_source"] } <1>

<1> This document is returned, even though it has terms other than `search`.

Recall how the `term` filter works: it checks the inverted index for all documents that contain a term, and then constructs a bitset. In our simple example, we have the following inverted index:

```
[width="50%",frame="topbot"] |===== | Token | DocIDs | open_source | 2 | search | 1, 2  
|=====
```

When a `term` filter is executed for the token `search`, it goes straight to the corresponding entry in the inverted index and extracts the associated doc IDs. As you can see, both document 1 and document 2 contain the token in the inverted index. Therefore, they are both returned as a result.

[NOTE]

The nature of an inverted index also means that entire field equality is rather difficult to calculate. How would you determine whether a particular document contains *only* your request term? You would have to find the term in the inverted index, extract the document IDs, and then scan *every row in the inverted index*, looking for those IDs to see whether a doc has any other terms.

As you might imagine, that would be tremendously inefficient and expensive. For that reason, `term` and `terms` are *must contain* operations, not

must equal exactly.

==== Equals Exactly If you do want that behavior--entire field equality--the best way to accomplish it involves indexing a secondary field. (((("structured search", "equals exactly")))) In this field, you index the number of values that your field contains. Using our two previous documents, we now include a field that maintains the number of tags:

[source,js]

```
{ "tags" : ["search"], "tag_count" : 1 }
```

{ "tags" : ["search", "open_source"], "tag_count" : 2 }

// SENSE: 080_Structured_Search/20_Exact.json

Once you have the count information indexed, you can construct a `bool` filter that enforces the appropriate number of terms:

[source,js]

```
GET /my_index/my_type/_search { "query": { "filtered": { "filter": { "bool": { "must": [ { "term": { "tags": "search" } }, <1> {  
"term": { "tag_count": 1 } } <2> ] } } } }
```

```
}
```

```
// SENSE: 080_Structured_Search/20_Exact.json
```

<1> Find all documents that have the term `search` .

<2> But make sure the document has only one tag.

This query will now match only the document that has a single tag that is `search` , rather than any document that contains `search` .

=== Ranges

When dealing with numbers in this chapter, we have so far searched for only exact numbers. (((("structured search", "ranges"))) In practice, filtering on ranges is often more useful. For example, you might want to find all products with a price greater than \$20 and less than \$40.

In SQL terms, a range can be expressed as follows:

[source,sql]

```
SELECT document FROM products
```

WHERE price BETWEEN 20 AND 40

Elasticsearch has a `range` filter, (((("range filters", "using on numbers")))which, unsurprisingly, allows you to filter ranges:

[source,js]

```
"range" : { "price" : { "gt" : 20, "lt" : 40 }
```

```
}
```

The `range` filter supports both inclusive and exclusive ranges, through combinations of the following options:

- `gt` : `>` greater than
- `lt` : `<` less than
- `gte` : `>=` greater than or equal to
- `lte` : `<=` less than or equal to

.Here is an example range filter:

[source,js]

```
GET /my_store/products/_search { "query" : { "filtered" : { "filter" : { "range" : { "price" : { "gte" : 20, "lt" : 40 } } } } }
```

```
}
```

```
// SENSE: 080_Structured_Search/25_Range_filter.json
```

If you need (((("unbounded ranges")))an unbounded range (for example, just `>20`), omit one of the boundaries:

[source,js]

```
"range" : { "price" : { "gt" : 20 }
```

```
}
```

```
// SENSE: 080_Structured_Search/25_Range_filter.json
```

==== Ranges on Dates

The `range` filter can be used on date (`((("date ranges")))((("range filters", "using on dates")))`)fields too:

[source,js]

```
"range" : { "timestamp" : { "gt" : "2014-01-01 00:00:00", "lt" : "2014-01-07 00:00:00" }  
}
```

When used on date fields, the `range` filter (`((("date math operations")))`)supports *date math* operations. For example, if we want to find all documents that have a timestamp sometime in the last hour:

[source,js]

```
"range" : { "timestamp" : { "gt" : "now-1h" }  
}
```

This filter will now constantly find all documents with a timestamp greater than the current time minus 1 hour, making the filter a *sliding window* across your documents.

Date math can also be applied to actual dates, rather than a placeholder like `now`. Just add a double pipe (`||`) after the date and follow it with a date math expression:

[source,js]

```
"range" : { "timestamp" : { "gt" : "2014-01-01 00:00:00", "lt" : "2014-01-01 00:00:00||+1M" <1> }  
}
```

`<1>` Less than January 1, 2014 plus one month

Date math is *calendar aware*, so it knows the number of days in each month, days in a year, and so forth. More details about working with dates can be found in the <http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/mapping-date-format.html>[date format reference documentation].

==== Ranges on Strings

The `range` filter can also operate on string fields.`((("range filters", "using on strings")))((("strings", "using range filter on")))((("lexicographical order, string ranges")))` String ranges are calculated *lexicographically* or alphabetically. For example, these values are sorted in lexicographic order:

- 5, 50, 6, B, C, a, ab, abb, abc, b

[NOTE]

Terms in the inverted index are sorted in lexicographical order, which is why

string ranges use this order.

If we want a range from `a` up to but not including `b`, we can use the same `range` filter syntax:

[source,js]

```
"range" : { "title" : { "gte" : "a", "lt" : "b" }
```

```
}
```

.Be Careful of Cardinality

Numeric and date fields are indexed in such a way that ranges are efficient to calculate.(((("cardinality", "string ranges and"))) This is not the case for string fields, however. To perform a range on a string field, Elasticsearch is effectively performing a `term` filter for every term that falls in the range. This is much slower than a date or numeric range.

String ranges are fine on a field with *low cardinality*—a small number of unique terms. But the more unique terms you have, the slower the string range will be.

=== Dealing with Null Values

Think back to our earlier example, where documents have a field named `tags`. This is a multivalued field. ("structured search", "dealing with null values") ("null values") A document may have one tag, many tags, or potentially no tags at all. If a field has no values, how is it stored in an inverted index?

That's a trick question, because the answer is, it isn't stored at all. Let's look at that inverted index from the previous section:

```
[width="50%",frame="topbot"] |===== | Token | DocIDs | open_source | 2 | search | 1, 2 |=====
```

How would you store a field that doesn't exist in that data structure? You can't! An inverted index is simply a list of tokens and the documents that contain them. If a field doesn't exist, it doesn't hold any tokens, which means it won't be represented in an inverted index data structure.

Ultimately, this(("strings", "empty"))(("arrays", "empty")) means that a `null`, `[]` (an empty array), and `[null]` are all equivalent. They simply don't exist in the inverted index!

Obviously, the world is not simple, and data is often missing fields, or contains explicit nulls or empty arrays. To deal with these situations, Elasticsearch has a few tools to work with null or missing values.

==== exists Filter

The first tool in your arsenal is the `exists` filter. ("null values", "working with, using exists filter") ("exists filter") This filter will return documents that have any value in the specified field. Let's use the tagging example and index some example documents:

[source,js]

```
POST /my_index/posts/_bulk { "index": { "_id": "1" } } { "tags" : ["search"] } <1> { "index": { "_id": "2" } } { "tags" : ["search", "open_source"] } <2> { "index": { "_id": "3" } } { "other_field" : "some data" } <3> { "index": { "_id": "4" } } { "tags" : null } <4> { "index": { "_id": "5" } } { "tags" : ["search", null] } <5>
```

```
// SENSE: 080_Structured_Search/30_Exists_missing.json
```

```
<1> The tags field has one value.
```

```
<2> The tags field has two values.
```

```
<3> The tags field is missing altogether.
```

```
<4> The tags field is set to null .
```

```
<5> The tags field has one value and a null .
```

The resulting inverted index for our `tags` field will look like this:

```
[width="50%",frame="topbot"] |===== | Token | DocIDs | open_source | 2 | search | 1, 2, 5 |=====
```

Our objective is to find all documents where a tag is set. We don't care what the tag is, so long as it exists within the document. In SQL parlance, we would use an `IS NOT NULL` query:

[source,sql]

```
SELECT tags FROM posts
```

WHERE tags IS NOT NULL

In Elasticsearch, we use the `exists` filter:

[source,js]

```
GET /my_index/posts/_search { "query" : { "filtered" : { "filter" : { "exists" : { "field" : "tags" } } } } }
```

```
// SENSE: 080_Structured_Search/30_Exists_missing.json
```

Our query returns three documents:

[source,json]

```
"hits" : [ { "_id" : "1", "_score" : 1.0, "_source" : { "tags" : ["search"] } }, { "_id" : "5", "_score" : 1.0, "_source" : { "tags" : ["search", null] } <1> }, { "_id" : "2", "_score" : 1.0, "_source" : { "tags" : ["search", "open source"] } } ]
```

<1> Document 5 is returned even though it contains a `null` value. The field exists because a real-value tag was indexed, so the `null` had no impact on the filter.

The results are easy to understand. Any document that has terms in the `tags` field was returned as a hit. The only two documents that were excluded were documents 3 and 4.

==== missing Filter

The `missing` filter is essentially(("null values", "working with, using missing filter"))(("missing filter")) the inverse of `exists` : it returns documents where there is *no* value for a particular field, much like this SQL:

[source,sql]

```
SELECT tags FROM posts
```

WHERE tags IS NULL

Let's swap the `exists` filter for a `missing` filter from our previous example:

[source,js]

```
GET /my_index/posts/_search { "query" : { "filtered" : { "filter": { "missing" : { "field" : "tags" } } } } }
```

```
// SENSE: 080_Structured_Search/30_Exists_missing.json
```

And, as you would expect, we get back the two docs that have no real values in the `tags` field--documents 3 and 4:

[source,json]

```
"hits": [ { "_id": "3", "_score": 1.0, "_source": { "other_field": "some data" } }, { "_id": "4", "_score": 1.0, "_source": { "tags": null } } ]
```

]

.When null Means null

Sometimes you need to be able to distinguish between a field that doesn't have a value, and a field that has been explicitly set to `null`. With the default behavior that we saw previously, this is impossible; the data is lost. Luckily, there is an option that we can set that replaces explicit `null` values with a *placeholder* value of our choosing.

When specifying the mapping for a string, numeric, Boolean, or date field, you can also set a `null_value` that will be used whenever an explicit `null` value is encountered. (((("null_value setting")))) A field without a value will still be excluded from the inverted index.

When choosing a suitable `null_value`, ensure the following:

- It matches the field's type. You can't use a string `null_value` in a field of type `date`.
- It is different from the normal values that the field may contain, to avoid confusing real values with `null` values.

==== exists/missing on Objects

The `exists` and `missing` filters (((("objects", "using exists/missing filters on")))((("exists filter", "using on objects")))((("missing filter", "using on objects"))))also work on inner objects, not just core types. With the following document

[source,js]

```
{ "name": { "first": "John", "last": "Smith" }
```

```
}
```

you can check for the existence of `name.first` and `name.last` but also just `name`. However, in <>, we said that an object like the preceding one is flattened internally into a simple field-value structure, much like this:

[source,js]

```
{ "name.first": "John", "name.last": "Smith"
```

```
}
```

So how can we use an `exists` or `missing` filter on the `name` field, which doesn't really exist in the inverted index?

The reason that it works is that a filter like

[source,js]

```
{ "exists" : { "field" : "name" }
```

```
}
```

is really executed as

[source,js]

```
{ "bool": { "should": [ { "exists": { "field": { "name.first" }}} , { "exists": { "field": { "name.last" }}} ] }
```

```
}
```

That also means that if `first` and `last` were both empty, the `name` namespace would not exist.

[[filter-caching]] === All About Caching

Earlier in this chapter (<<_internal_filter_operation>>), we briefly discussed how filters are calculated.(((("structured search", "caching of filter results")))((("caching", "bitsets representing documents matching filters")))((("bitsets, caching of")))((("filters", "bitsets representing documents matching, caching of"))) At their heart is a bitset representing which documents match the filter. Elasticsearch aggressively caches these bitsets for later use. Once cached, these bitsets can be reused *wherever* the same filter is used, without having to reevaluate the entire filter again.

These cached bitsets are ``smart``: they are updated incrementally. As you index new documents, only those new documents need to be added to the existing bitsets, rather than having to recompute the entire cached filter over and over. Filters are real-time like the rest of the system; you don't need to worry about cache expiry.

==== Independent Filter Caching

Each filter is calculated and cached independently, regardless of where it is used.(((("filters", "independent caching of"))) If two different queries use the same filter, the same filter bitset will be reused. Likewise, if a single query uses the same filter in multiple places, only one bitset is calculated and then reused.

Let's look at this example query, which looks for emails that are either of the following:

- In the inbox and have not been read
- *Not* in the inbox but have been marked as important

[source,js]

```
"bool": { "should": [ { "bool": { "must": [ { "term": { "folder": "inbox" } }, <1> { "term": { "read": false } } ] }, { "bool": { "must_not": [ { "term": { "folder": "inbox" } <1> }, "must": { "term": { "important": true } } ] } } ] } }
```

<1> These two filters are identical and will use the same bitset.

Even though one of the inbox clauses is a `must` clause and the other is a `must_not` clause, the two clauses themselves are identical. This means that the bitset is calculated once for the first clause that is executed, and then the cached bitset is used for the other clause. By the time this query is run a second time, the inbox filter is already cached and so both clauses will use the cached bitset.

This ties in nicely with the composability of the query DSL. It is easy to move filters around, or reuse the same filter in multiple places within the same query. This isn't just convenient to the developer--it has direct performance benefits.

==== Controlling Caching

Most *leaf filters*—those dealing directly with fields like the `term` filter—are cached, while(((("leaf filters, caching of"))) ((("caching", "of leaf filters, controlling")))((("filters", "controlling caching of"))) compound filters, like the `bool` filter, are not.

[NOTE]

Leaf filters have to consult the inverted index on disk, so it makes sense to cache them. Compound filters, on the other hand, use fast bit logic to combine the bitsets resulting from their inner clauses, so it is efficient to

recalculate them every time.

Certain leaf filters, however, are not cached by default, because it doesn't make sense to do so:

Script filters::

The results(((("script filters, no caching of results")))) from

[http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/filter-caching.html#_controlling_caching\[script` filters\]](http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/filter-caching.html#_controlling_caching[script` filters])

cannot be cached because the meaning of the script is opaque to Elasticsearch.

Geo-filters::

The geolocation filters, which(((("geolocation filters, no caching of results")))) we cover in more detail in <>, are usually used to filter results based on the geolocation of a specific user. Since each user has a unique geolocation, it is unlikely that geo-filters will be reused, so it makes no sense to cache them.

Date ranges::

Date ranges that (((("date ranges", "using now function, no caching of")))((("now function", "date ranges using"))))use the `now` function (for example `"now-1h"`), result in values accurate to the millisecond. Every time the filter is run, `now` returns a new time. Older filters will never be reused, so caching is disabled by default. However, when using `now` with rounding (for example, `now/d` rounds to the nearest day), caching is enabled by default.

Sometimes the default caching strategy is not correct. Perhaps you have a complicated `bool` expression that is reused several times in the same query. Or you have a filter on a `date` field that will never be reused. The default caching strategy (((("_cache flag", sortas="cache flag")))((("filters", "overriding default caching strategy on"))))can be overridden on almost any filter by setting the `_cache` flag:

[source,js]

```
{ "range" : { "timestamp" : { "gt" : "2014-01-02 16:15:14" <1> }, "_cache": false <2> }
```

```
}
```

<1> It is unlikely that we will reuse this exact timestamp.

<2> Disable caching of this filter.

Later chapters provide examples of when it can make sense to override the default caching strategy.

=== Filter Order

The order of filters in a `bool` clause is important for performance.(((("structured search", "filter order")))((("filters", "order of")))) More-specific filters should be placed before less-specific filters in order to exclude as many documents as possible, as early as possible.

If Clause A could match 10 million documents, and Clause B could match only 100 documents, then Clause B should be placed before Clause A.

Cached filters are very fast, so they should be placed before filters that are not cacheable.(((("caching", "cached filters, order of")))) Imagine that we have an index that contains one month's worth of log events. However, we're mostly interested only in log events from the previous hour:

[source,js]

```
GET /logs/2014-01/_search { "query" : { "filtered" : { "filter" : { "range" : { "timestamp" : { "gt" : "now-1h" } } } } } }
```

This filter is not cached because it uses the `now` function,(((("now function", "filters using, caching and")))) the value of which changes every millisecond. That means that we have to examine one month's worth of log events every time we run this query!

We could make this much more efficient by combining it with a cached filter: we can exclude most of the month's data by adding a filter that uses a fixed point in time, such as midnight last night:

[source,js]

```
"bool": { "must": [ { "range" : { "timestamp" : { "gt" : "now-1h/d" <1> } } }, { "range" : { "timestamp" : { "gt" : "now-1h" <2> } } } ] }
```

<1> This filter is cached because it uses `now` rounded to midnight.

<2> This filter is not cached because it uses `now` *without* rounding.

The `now-1h/d` clause rounds to the previous midnight and so excludes all documents created before today. The resulting bitset is cached because `now` is used with rounding, which means that it is executed only once a day, when the value for *midnight-last-night* changes. The `now-1h` clause isn't cached because `now` produces a time accurate to the nearest millisecond. However, thanks to the first filter, this second filter need only check documents that have been created since midnight.

The order of these clauses is important. This approach works only because the *since-midnight* clause comes before the *last-hour* clause. If they were the other way around, then the *last-hour* clause would need to examine all documents in the index, instead of just documents created since midnight.