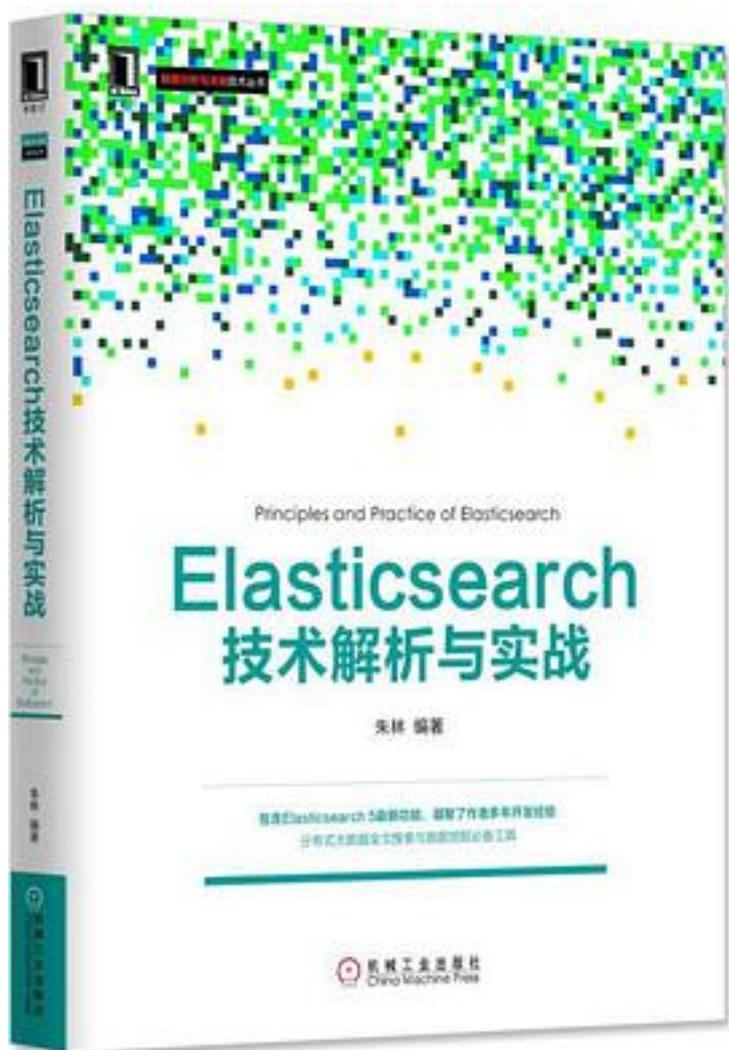


Elasticsearch 技术解析与实战



[Elasticsearch 技术解析与实战_下载链接1](#)

著者:朱林

出版者:机械工业出版社

出版时间:2017-1

装帧:

isbn:9787111553274

作者介绍:

朱林，资深开发人员，有16年开发经验，11年安全产品开发经验，对安全技术、日志分析有较深的研究。于2013年创立南京赛克蓝德网络科技有限公司，公司专注于安全产品的开发，目前主要开发的产品是赛克蓝德日志分析软件。

目录: 前言

第1章 Elasticsearch入门 1

1.1 Elasticsearch是什么 1

1.1.1 Elasticsearch的历史 2

1.1.2 相关产品 3

1.2 全文搜索 3

1.2.1 Lucene介绍 4

1.2.2 Lucene倒排索引 4

1.3 基础知识 6

1.3.1 Elasticsearch术语及概念 6

1.3.2 JSON介绍 10

1.4 安装配置 12

1.4.1 安装Java 12

1.4.2 安装Elasticsearch 12

1.4.3 配置 13

1.4.4 运行 15

1.4.5 停止 17

1.4.6 作为服务 17

1.4.7 版本升级 19

1.5 对外接口 21

1.5.1 API约定 22

1.5.2 REST介绍 25

1.5.3 Head插件安装 26

1.5.4 创建库 27

1.5.5 插入数据 28

1.5.6 修改文档 28

1.5.7 查询文档 29

1.5.8 删除文档 29

1.5.9 删除库 30

1.6 Java接口 30

1.6.1 Java接口说明 30

1.6.2 创建索引文档 33

1.6.3 增加文档 34

1.6.4 修改文档 35

1.6.5 查询文档 35

1.6.6 删除文档 35

1.7 小结 36

第2章 索引 37

2.1 索引管理 37

2.1.1 创建索引 37

2.1.2 删除索引 39

2.1.3 获取索引 39

2.1.4 打开/关闭索引 40

2.2 索引映射管理 41

2.2.1 增加映射 41

2.2.2 获取映射 44

- 2.2.3 获取字段映射 45
- 2.2.4 判断类型是否存在 46
- 2.3 索引别名 46
- 2.4 索引配置 51
 - 2.4.1 更新索引配置 51
 - 2.4.2 获取配置 52
 - 2.4.3 索引分析 52
 - 2.4.4 索引模板 54
 - 2.4.5 复制配置 55
 - 2.4.6 重建索引 56
- 2.5 索引监控 60
 - 2.5.1 索引统计 60
 - 2.5.2 索引分片 62
 - 2.5.3 索引恢复 63
 - 2.5.4 索引分片存储 64
- 2.6 状态管理 64
 - 2.6.1 清除缓存 64
 - 2.6.2 索引刷新 64
 - 2.6.3 冲洗 65
 - 2.6.4 合并索引 65
- 2.7 文档管理 66
 - 2.7.1 增加文档 66
 - 2.7.2 更新删除文档 69
 - 2.7.3 查询文档 73
 - 2.7.4 多文档操作 76
 - 2.7.5 索引词频率 80
 - 2.7.6 查询更新接口 83
- 2.8 小结 87
- 第3章 映射 88
 - 3.1 概念 88
 - 3.2 字段数据类型 90
 - 3.2.1 核心数据类型 91
 - 3.2.2 复杂数据类型 96
 - 3.2.3 地理数据类型 100
 - 3.2.4 专门数据类型 106
 - 3.3 元字段 108
 - 3.3.1 _all字段 109
 - 3.3.2 _field_names字段 109
 - 3.3.3 _id字段 110
 - 3.3.4 _index字段 110
 - 3.3.5 _meta字段 111
 - 3.3.6 _parent字段 111
 - 3.3.7 _routing字段 112
 - 3.3.8 _source字段 114
 - 3.3.9 _type字段 115
 - 3.3.10 _uid字段 115
 - 3.4 映射参数 116
 - 3.4.1 analyzer参数 116
 - 3.4.2 boost参数 118
 - 3.4.3 coerce参数 119
 - 3.4.4 copy_to参数 120
 - 3.4.5 doc_values参数 121
 - 3.4.6 dynamic参数 122
 - 3.4.7 enabled参数 122

- 3.4.8 fielddata参数 123
- 3.4.9 format参数 126
- 3.4.10 geohash参数 128
- 3.4.11 geohash_precision参数 129
- 3.4.12 geohash_prefix参数 130
- 3.4.13 ignore_above参数 131
- 3.4.14 ignore_malformed参数 131
- 3.4.15 include_in_all参数 132
- 3.4.16 index参数 133
- 3.4.17 index_options参数 133
- 3.4.18 lat_lon参数 134
- 3.4.19 fields参数 135
- 3.4.20 norms参数 136
- 3.4.21 null_value参数 137
- 3.4.22 position_increment_gap参数 137
- 3.4.23 precision_step参数 138
- 3.4.24 properties参数 138
- 3.4.25 search_analyzer参数 139
- 3.4.26 similarity参数 140
- 3.4.27 store参数 141
- 3.4.28 term_vector参数 141
- 3.5 动态映射 142
 - 3.5.1 概念 142
 - 3.5.2 _default_ 映射 143
 - 3.5.3 动态字段映射 143
 - 3.5.4 动态模板 145
 - 3.5.5 重写默认模板 148
- 3.6 小结 148
- 第4章 搜索 149
 - 4.1 深入搜索 149
 - 4.1.1 搜索方式 149
 - 4.1.2 重新评分 153
 - 4.1.3 滚动查询请求 155
 - 4.1.4 隐藏内容查询 158
 - 4.1.5 搜索相关函数 161
 - 4.1.6 搜索模板 164
 - 4.2 查询DSL 167
 - 4.2.1 查询和过滤的区别 167
 - 4.2.2 全文搜索 168
 - 4.2.3 字段查询 179
 - 4.2.4 复合查询 183
 - 4.2.5 连接查询 188
 - 4.2.6 地理查询 190
 - 4.2.7 跨度查询 197
 - 4.2.8 高亮显示 200
 - 4.3 简化查询 203
 - 4.4 小结 206
- 第5章 聚合 207
 - 5.1 聚合的分类 207
 - 5.2 度量聚合 209
 - 5.2.1 平均值聚合 209
 - 5.2.2 基数聚合 211
 - 5.2.3 最大值聚合 213
 - 5.2.4 最小值聚合 214

- 5.2.5 和聚合 214
- 5.2.6 值计数聚合 215
- 5.2.7 统计聚合 215
- 5.2.8 百分比聚合 215
- 5.2.9 百分比分级聚合 216
- 5.2.10 最高命中排行聚合 217
- 5.2.11 脚本度量聚合 217
- 5.2.12 地理边界聚合 221
- 5.2.13 地理重心聚合 222
- 5.3 分组聚合 223
 - 5.3.1 子聚合 224
 - 5.3.2 直方图聚合 226
 - 5.3.3 日期直方图聚合 230
 - 5.3.4 时间范围聚合 233
 - 5.3.5 范围聚合 234
 - 5.3.6 过滤聚合 235
 - 5.3.7 多重过滤聚合 236
 - 5.3.8 空值聚合 238
 - 5.3.9 嵌套聚合 239
 - 5.3.10 采样聚合 240
 - 5.3.11 重要索引词聚合 242
 - 5.3.12 索引词聚合 245
 - 5.3.13 总体聚合 251
 - 5.3.14 地理点距离聚合 251
 - 5.3.15 地理散列网格聚合 253
 - 5.3.16 IPv4范围聚合 255
- 5.4 管道聚合 257
 - 5.4.1 平均分组聚合 259
 - 5.4.2 移动平均聚合 261
 - 5.4.3 总和分组聚合 262
 - 5.4.4 总和累计聚合 262
 - 5.4.5 最大分组聚合 264
 - 5.4.6 最小分组聚合 265
 - 5.4.7 统计分组聚合 266
 - 5.4.8 百分位分组聚合 268
 - 5.4.9 差值聚合 269
 - 5.4.10 分组脚本聚合 273
 - 5.4.11 串行差分聚合 275
 - 5.4.12 分组选择器聚合 276
- 5.5 小结 277
- 第6章 集群管理 278
 - 6.1 集群节点监控 278
 - 6.1.1 集群健康值 278
 - 6.1.2 集群状态 279
 - 6.1.3 集群统计 280
 - 6.1.4 集群任务管理 280
 - 6.1.5 待定集群任务 281
 - 6.1.6 节点信息 281
 - 6.1.7 节点统计 282
 - 6.2 集群分片迁移 283
 - 6.3 集群节点配置 284
 - 6.3.1 主节点 285
 - 6.3.2 数据节点 286
 - 6.3.3 客户端节点 286

- 6.3.4 部落节点 287
- 6.4 节点发现 287
 - 6.4.1 主节点选举 288
 - 6.4.2 故障检测 288
- 6.5 集群平衡配置 289
 - 6.5.1 分片分配设置 289
 - 6.5.2 基于磁盘的配置 290
 - 6.5.3 分片智能分配 291
 - 6.5.4 分片配置过滤 292
 - 6.5.5 其他集群配置 293
- 6.6 小结 293
- 第7章 索引分词器 294
 - 7.1 分词器的概念 294
 - 7.2 中文分词器 298
 - 7.3 插件 300
 - 7.3.1 插件管理 301
 - 7.3.2 插件安装 301
 - 7.3.3 插件清单 302
 - 7.4 小结 304
- 第8章 高级配置 305
 - 8.1 网络相关配置 305
 - 8.1.1 本地网关配置 305
 - 8.1.2 HTTP配置 306
 - 8.1.3 网络配置 307
 - 8.1.4 传输配置 308
 - 8.2 脚本配置 310
 - 8.2.1 脚本使用 311
 - 8.2.2 脚本配置 313
 - 8.3 快照和恢复配置 318
 - 8.4 线程池配置 324
 - 8.5 索引配置 326
 - 8.5.1 缓存配置 326
 - 8.5.2 索引碎片分配 329
 - 8.5.3 合并 332
 - 8.5.4 相似模块 332
 - 8.5.5 响应慢日志监控 333
 - 8.5.6 存储 335
 - 8.5.7 事务日志 336
 - 8.6 小结 337
- 第9章 告警、监控和权限管理 338
 - 9.1 告警 338
 - 9.1.1 安装 338
 - 9.1.2 结构 339
 - 9.1.3 示例 352
 - 9.1.4 告警输出配置 354
 - 9.1.5 告警管理 355
 - 9.2 监控 356
 - 9.2.1 安装 356
 - 9.2.2 配置 357
 - 9.3 权限管理 360
 - 9.3.1 工作原理 361
 - 9.3.2 用户认证 361
 - 9.3.3 角色管理 366
 - 9.3.4 综合示例 368

- 9.4 小结 369
- 第10章 ELK应用 370
 - 10.1 Logstash 370
 - 10.1.1 配置 371
 - 10.1.2 插件管理 374
 - 10.2 Kibana配置 377
 - 10.2.1 Discover 379
 - 10.2.2 Visualize 381
 - 10.2.3 Dashboard 383
 - 10.2.4 Settings 386
 - 10.3 综合示例 387
 - 10.4 小结 390
- 附录 Elasticsearch 5.0的特性与改进 391
 - • • • • [\(收起\)](#)

[Elasticsearch 技术解析与实战 下载链接1](#)

标签

elasticsearch

ELK

Java

技术

Elasticsearch

ES

逻辑混乱

流水线叙述

评论

快速读完，没有原理仅仅api使用

官方文档翻译，作为参考书

流水账一样的叙述方式让我感觉很无奈啊 elastic search 入门第一书
感觉选择并不太明智 orz

有一些作者自己的简单总结，有一部分是官方文档的简单翻译，封面和纸质不错。个人
觉得Elasticsearch的书还是Rafal Kuc写得好。

完全看不懂在说什么

就是抄了官网的文字

api的简单使用，很枯燥的描述

看了第1章，忍不住上来吐槽一下：结构混乱，基本概念介绍前后颠倒，错误几处，第1
章作为入门章节，看完就一感觉-混乱。

流水线一样，实在是看的太枯燥了

实在不容易看下去，这本书写的着实不行啊

作者写这本书极不负责任，出版这种书有什么意义？

推荐看官方文档，这个有点老了

烂 实在是看不下去了

可以去看最新的文档,该书版本为2.3.0 ,当前评论时间节点 es已经更新到7.x了

[Elasticsearch 技术解析与实战_下载链接1](#)

书评

非常差劲的一本书，全是硬翻译，译者自己都读不懂吧。给你举个例子，里面有原句：“方便人类的阅读”，脑壳秀逗了吧，难道这本书是给鬼读的吗？一个章节下来，基本不知道你在说什么，我以为自己问题，又重复读了几遍，还是不理解在说什么，只好弃读。你这样为了赚钱而出书，为...

花了大概半年时间翻完。此书作为工具书定位，是合适的，更多的细致的介绍每个内容的含义。但每块涉及又不深。在对于ES解析上，说明较少、比如主节点的选举，意犹未尽。

对于作者提到的结合多年实战写出，并不是非常认可。全书广而不深。如果对于了解原理，不推荐阅读。总体来说...

学途无忧网ElasticSearch5实战课程

课程观看地址：<http://www.xuetuwuyou.com/course/224>

课程出自学途无忧网：<http://www.xuetuwuyou.com> 讲师：西瓜老师

ElasticSearch是一个基于Lucene的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口...

[Elasticsearch 技术解析与实战 下载链接1](#)