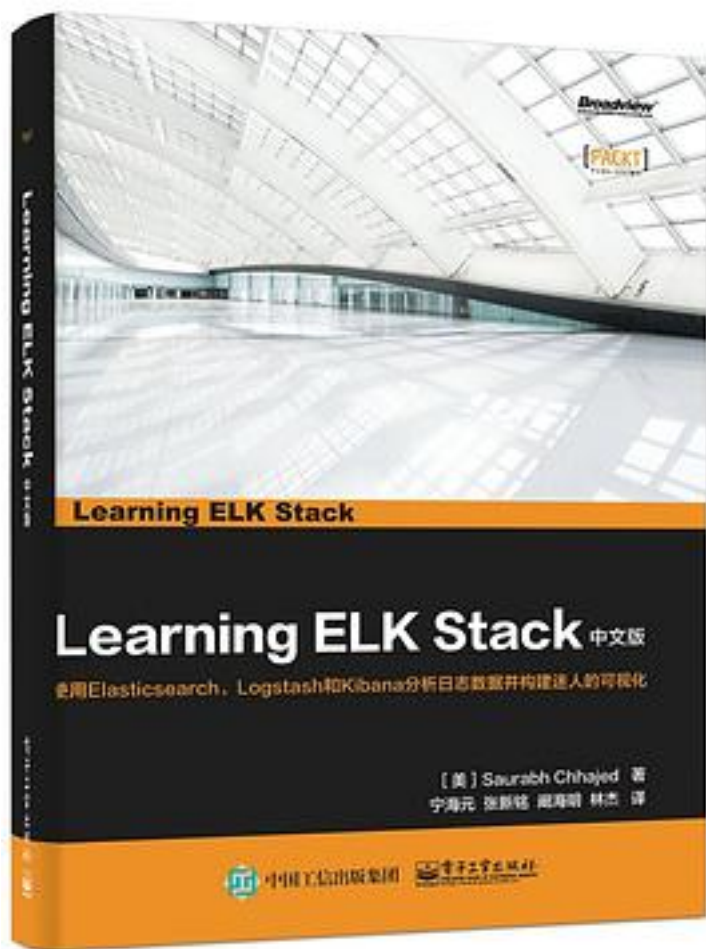


Learning ELK Stack 中文版



[Learning ELK Stack 中文版_下载链接1](#)

著者:【美】Saurabh Chhajer (苏库拉·塞哈特)

出版者:电子工业出版社

出版时间:2016-6

装帧:平装

isbn:9787121288845

ELK 技术栈是一套新兴的日志处理开源系统，ELK 分别代表Elasticsearch、Logstash 和Kibana。Elasticsearch 是基于Lucene

构建的一套分布式搜索引擎，提供了实时搜索和聚合分析的能力，是整个ELK技术栈的核心。Logstash构建了数据采集、解析和输出的框架，通过插件可以支持不同的输入、过滤和输出的场景。Kibana实现了对Elasticsearch的搜索查询和数据可视化。三者组合起来是一套经过很多生产环境验证的日志解决方案。《Learning ELK Stack 中文版》针对ELK技术栈由浅入深地对每个组件做了介绍，并且通过实际的部署和应用案例，真正地讲清楚了如何利用ELK技术栈来实现日志数据的完整管道。

作者介绍:

Saurabh Chhajer

是一名技术专家，在为产品和服务行业构建企业应用领域，有着丰富而专业的经验。他在大数据分析和机器学习领域有很多实际的构建工程应用的经历，并且乐于布道大数据和NoSQL技术。Saurabh利用他丰富的技术经验，帮助美国很多大型的金融和工业企业从零开始构建大型的产品体系和分布式应用。他在个人网站<http://saurzcode.in>分享了很多的个人技术经验。Saurabh过去还帮助审阅了Packt出版社出版的技术书籍，包括Apache Camel Essentials和Java EE 7 Development with NetBeans 8。

目录: 前言 . XIII

1 ELK 技术栈介绍 1

日志分析的必要性 1

问题调试 2

性能分析 2

安全分析 2

预测分析 2

物联网日志 3

日志分析的挑战 3

不一致的日志格式 3

不同的时间格式 4

专业知识的需求 5

ELK 技术栈 5

Elasticsearch 5

Logstash 6

Kibana 6

ELK 数据管道 7

安装ELK 技术栈 8

安装Elasticsearch 8

运行Elasticsearch 9

配置Elasticsearch 10

Elasticsearch 插件 11

安装Logstash 11

运行Logstash 12

Logstash 的文件输入插件 13

Logstash 的Elasticsearch 输出插件 13

配置Logstash 14

安装Logstash forwarder 15

Logstash 插件 15

安装Kibana 17

- 配置Kibana 18
- 运行Kibana 18
- Kibana 的界面 19
- 总结 22
- 2 构建第一条ELK 数据管道 23
 - 输入的数据集 23
 - 输入数据集的数据格式 23
 - 配置Logstash 的输入 25
 - 过滤和处理输入数据 26
 - 将数据存储到Elasticsearch 29
 - 使用Kibana 可视化 32
 - 运行Kibana 32
 - Kibana 可视化组件 34
 - 构建折线图 35
 - 构建柱状图 36
 - 构建度量 37
 - 构建数据表 38
 - 总结 40
- 3 使用Logstash 采集、解析和转换数据 41
 - 配置Logstash 41
 - Logstash 插件 42
 - 列出Logstash 的所有插件 42
 - 插件属性的数据类型 43
 - Logstash 条件语句 44
 - Logstash 插件的类型 46
 - 总结 72
- 4 创建自定义Logstash 插件 73
 - Logstash 插件管理 73
 - 插件生命周期管理 74
 - 安装插件 74
 - 更新插件 75
 - 卸载插件 75
 - Logstash 插件的结构 76
 - 需要的依赖 77
 - 类定义 78
 - 配置插件名字 78
 - 配置选项设置 78
 - 插件方法 79
 - 实现一个Logstash 过滤器插件 81
 - 构建插件 83
 - 总结 86
- 5 为什么需要ELK 中的Elasticsearch 87
 - 为什么是Elasticsearch 87
 - Elasticsearch 的基本概念 88
 - 索引 88
 - 文档 88
 - 字段 89
 - 类型 89
 - 映射 89
 - 分片 89
 - 主分片和副本分片 89
 - 集群 90
 - 节点 90
 - 探索Elasticsearch API 91

- 列出所有可用索引 92
- 列出集群中的所有节点 93
- 检查集群的健康状态 93
- 创建索引 94
- 检索文档 95
- 删除文档 96
- Elasticsearch Query DSL 97
- Elasticsearch 插件 104
- Bigdesk 插件 104
- Elastic-Hammer 插件 105
- Head 插件 105
- 总结 106
- 6 使用Kibana 理解数据 107
- Kibana 4 的功能 107
- 搜索词高亮显示 107
- Elasticsearch 聚合 108
- 衍生字段 108
- 动态仪表盘 108
- Kibana 界面 109
- 搜索页面 109
- 查询和检索数据 111
- 总结 116
- 7 Kibana 可视化和仪表盘 117
- 可视化页面 117
- 创建可视化 118
- 可视化的类型 118
- 度量和桶聚合 119
- 可视化 124
- 仪表盘页面 129
- 创建新的仪表盘 130
- 保存和加载仪表盘131
- 分享仪表盘 131
- 总结 132
- 8 构建完整的ELK 技术栈 133
- 输入数据集 133
- 配置Logstash 输入 134
- 访问日志的Grok 表达式 134
- Kibana 可视化 137
- 运行Kibana 137
- 在搜索页进行搜索 139
- 可视化—图表 141
- 创建折线图 142
- 创建区域图 143
- 创建柱状图 144
- 创建Markdown 145
- 仪表盘页面 146
- 总结 147
- 9 生产环境的ELK 技术栈 149
- 防止数据丢失 149
- 数据保护. 150
- 系统可扩展性 152
- 数据保留 153
- ELK 技术栈实施案例. 153
- LinkedIn 的ELK 技术栈 153

SCA 使用ELK 的案例 156
SCA 如何使用ELK 157
如何帮助分析 157
SCA 使用ELK 做监控 158
Cliffhanger Solutions 使用ELK 的案例 158
Kibana 示例——Packetbeat 仪表盘 160
总结 163
10 扩展ELK 165
Elasticsearch 插件和工具 165
用于索引管理的Curator 165
用于安全的Shield 167
用于监控的Marvel 169
ELK 的路线图 172
Elasticsearch 路线图 172
Logstash 路线图 172
Kibana 路线图 173
总结 174
• • • • • ([收起](#))

[Learning ELK Stack 中文版_下载链接1_](#)

标签

ELK

Elasticsearch

日志分析

计算机科学

计算机

编程

elasticsearch

SaurabhChhajed

评论

谁没面向工资编程过

很通俗易懂，两个小时一口气看完七章，很薄

内容属于入门 helloworld 水平，还不如网上随便搜搜的文章有内容

手册汇编形式的，对于完全不了解ELK的，花上2~3小时浏览一遍还行。

很简单的说明书，而且过时了，ELK这块迭代太快，有空得去看看文档更新一下自己的认知了……

内容过于简单，并且相对现在有些过时了

半小时翻了一下，没错就是半小时，看了一下数目和内容，我仿佛知道这是一本和理解无关的书，只要能实际操作就可以了，以后会不会再翻这本书了？英文好起来的话，估计不会了，关于操作，按道理官网应该有详细介绍了，可惜英语并不好，足见英语之重要性

[Learning ELK Stack 中文版_下载链接1_](#)

书评

该书应该是目前（2016年6月）最新出版的ELK技术的简体中文书，原版书的出版日期2015年11月，原版全书206页，译版为174页（正文）+ 16页（序言、目录、前言等）
对照原版读该译本，发现国内翻译书籍的一些可责之处 ## 封面 原文 Build

mesmerizing visualizations. and anal...

我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了
我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了
我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了 我看过了
我看过了 我看...

[Learning ELK Stack 中文版_下载链接1](#)