Mastering Splunk

精通Splunk

机器数据处理与分析

[美] James Miller（詹姆斯·米勒） / 著
[中] 宫鑫 谢金秀 郑智超 / 译

使用 Splunk 进行高级分析，有效优化机器大数据

[PACKT] PUBLISHING

中国工信出版集团 電子工業出版社 PUBLISHING HOUSE OF ELECTRONICS INDUSTRY http://www.phei.com.cn

精通 Splunk

机器数据处理与分析

[美] James Miller（詹姆斯·米勒）/著
[中] 宫鑫　谢金秀　郑智超/译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书内容丰富，实战性强，讲解细致，理论与操作相结合，详细介绍了 Splunk 的各项功能，包括如何索引和搜索数据，如何制作可视化图表，如何创建仪表板和应用程序，如何创建警报和数据模型等内容，任何想通过 Splunk Enterprise 平台进行智能运维的读者都可以阅读本书。

本书力求引用信息的准确性，但并非毫无瑕疵。对本书所带来的问题或者可能由本书直接或间接引起的问题，无论是作者，亦或 Packt 出版社、零售商及分销商均不承担任何责任。

本书中所提到的公司和产品商标信息均由 Packt 出版社提供，并以大写的形式标出，但 Packt 出版社不能保证信息的准确性。

版权贸易合同登记号　图字：01-2015-6974

图书在版编目（CIP）数据

精通 Splunk：机器数据处理与分析 /（美）米勒（Miller,J.）著；宫鑫，谢金秀，郑智超译. 北京：电子工业出版社，2016.1

书名原文：Mastering Splunk

ISBN 978-7-121-27676-7

Ⅰ. ①精… Ⅱ. ①米… ②宫… ③谢… ④郑… Ⅲ. ①数据处理软件 Ⅳ. ①TP274

中国版本图书馆 CIP 数据核字（2015）第 284560 号

策划编辑：董亚峰
责任编辑：董亚峰
特约编辑：田学清　赵海红
印　　刷：三河市华成印务有限公司
装　　订：三河市华成印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编 100036
开　　本：720×1000　1/16　　印张：19.5　　字数：375 千字
版　　次：2016 年 1 月第 1 版
印　　次：2016 年 1 月第 1 次印刷
定　　价：68.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

本书不再讲述 Splunk 介绍性的话题，而是从企业建构的角度来介绍一些更深入的概念（结合实例）。本书非常具有实用性，介绍了一个思考型领导者的思维模式，这是所有 Splunk 专家都应具备的。

本书以简单易懂的方式呈现了 Splunk 所有关键的特性，使你能够轻松了解每个特性的功能和工作实例。另外，从企业的角度介绍了进行 Splunk 知识开发的关键概念。

本书涵盖内容

第 1 章　介绍 Splunk 的定义及其在企业建构路线图中的应用。在讨论哪些是该技术的标准或常规用途的同时，会介绍该技术的发展过程。最后，介绍一些 Splunk 的创新用法。

第 2 章　将结合重要的案例讲解高级搜索和技巧。

第 3 章　介绍更深入的 Splunk 表格、图表和字段使用方法，并给出一些实际的案例。

第 4 章　介绍 Splunk 查询与其工作流程。

第 5 章　首先介绍 Splunk 的默认仪表板，进而扩展说明 Splunk 商用高效仪表板的高级特性。

第 6 章　介绍索引的概念、运行方式及其之所以重要的原因。本章将一步一步地分析索引的基本概念及高级概念。

第 7 章　首先介绍 Splunk 应用程序基础知识，之后介绍 Splunk 应用程序和附件方面更深入的内容，如导航、搜索和共享。同时还会给出几个查找附加应用程序源的例子。

第 8 章　从计算机层面介绍 Splunk 技术的监测和预警功能，并将 Splunk 与其他监测工具进行对比。

第 9 章　从企业角度（或企业组织）定义和描述 Splunk 交易。

第 10 章　从企业的视角介绍 Splunk。详细介绍开发的最佳案例、命名、测试及发展前景。

附录 A　快速入门附录中，为读者提供成为 Splunk 大师的各种丰富的资源，从工程师认证系列课程到公司的网站和支持门户，以及其间的任何内容。阅读本部分同时也会让读者了解获取最新 Splunk 版本副本的过程，以及如何进行默认设置安装。最后，本部分会讨论创建有益于个人研究和练习环境的一些想法。

阅读本书的准备工作

如果你没有时间参加正式的培训，或没有时间阅读帮助文件，但仍然想掌握 Splunk 的使用方法，那么本书便是你最佳的选择。你只需要一个有 Windows 系统的笔记本、掌握 Windows 基本的使用技巧及你想研究的数据。

本书适合的阅读人群

本书会介绍许多深刻的见解及详细的、不常见的 Splunk 解决方案案例，因此无论你是否了解 Splunk 的基础知识，本书都能使你成为 Splunk 大师。

体例

在本书中，你会发现许多不同类型的文本，目的是区分不同类型的信息。下面给出了几个不同类型的例子及其所表示的意义。

文本中的编码语言、数据库表名、文件夹名称、文件名、文件扩展、路径名称、虚拟网址、用户输入及 Twitter 名称显示如下：“第一步是编辑 transforms.conf 配置文件，添加新的查找应用函数。”

一个代码块设置如下：

```
[subsearch]
maxout = 250
maxtime = 120
```

```
ttl = 400
```

当我们想将你的注意力吸引到代码块的某个特定部分时，便会将相关的语句或词汇设置成粗体：

```
lookup BUtoBUName BU as "Business Unit" OUTPUT BUName as "Business Unit Name"
| Table Month, "Business Unit", "Business Unit Name", RFCST
```

指令行输入或输出的写法如下：

```
splunk restart
```

新词和**重要的词语**用粗体显示，你在屏幕、菜单或对话框中看到的词语会出现在如下文本中：“点击**设置**，然后**检索**。”

> 警告或要点会在这样的框中显示。

> 提示或诀窍会这样显示。

读者反馈

我们永远欢迎读者反馈。让我们了解您对本书的看法——不管您喜欢哪里或者不喜欢哪里都请告诉我们。读者反馈对我们继续开发能让您充分受益的书籍至关重要。

要想给我们发送反馈，只需发送邮件到 feedback@packtpub.com，并在邮件主题标注书名即可。

如果你擅长某个项目，并有兴趣编写或参与撰写一本书，请从 www.packtpub.com/ authors 查阅我们的作者指南。

客户支持

你已购买了 Packt 图书，我们为你准备了物超所值的福利。

下载本书的彩色图像

同时，我们提供给你一份 PDF 文件，该文件包含本书所使用的屏幕截图或图表的彩色图像。彩色图像会帮助你更好地了解输出内容的变化。你可以从 https://www.packtpub.com/sites/default/files/downloads/3830EN_ColoredImages.pdf 下载该文件。

勘误

尽管我们千方百计确保书中内容的准确性，但错误还是不可避免。如果您在我们的某本书中发现错误，不管是文本错误还是代码错误，向我们报告该错误都会让我们非常感激。您这样做能让其他读者免受挫折，以及帮助我们在随后的版本中加以改进。如果您发现任何错误，请访问 http://www.packtpub.com/submit-errata 向我们报告，选择您阅读的书，点击**勘误表提交表格**链接，并输入勘误详情。您提交的勘误表一旦被核实，其将被接受，勘误表会上传到我们的网站，或添加到现有勘误表列表中，勘误列表就在该书名下的勘误表部分。前往 http://www.packtpub.com/support 选择您的书名，可以浏览现有的勘误表。

盗版

所有媒体都存在互联网盗版的问题。对 Packt 来说，我们严格保护版权和许可。如果您在网上遇到我公司作品的任何形式的盗版，请马上给我们提供地址或网站名称，以便我们采取补救措施。

请访问 copyright@packtpub.com 联系我们，并给出可疑盗版材料的链接。

我们会感激您协助捍卫作者的知识产权，只有这样我们才能为您提供优质内容。

疑问

如果您有关于本书的任何问题，都可以联系 questions@packtpub.com，我们会尽力解答。

译者序

面对快速变化的业务和日趋复杂的网络应用环境，不少 IT 管理者追赶变化时却举步维艰。Splunk 在这个技术的困境中应运而生，以灵活、敏捷的数据管理能力为企业带来一场 IT 管理的创新革命！Splunk 可以收集、索引、关联和监控数据，把看似枯燥的机器数据转化为价值非凡的运维智能。通过 Splunk 生成的直观、生动的可视化图表，用户可以获得更加深刻的见解，更好地做出决策。

本书内容丰富，实战性强，讲解细致，理论与操作相结合，详细介绍了 Splunk 的各项功能，包括如何索引和搜索数据，如何制作可视化图表，如何创建仪表板和应用程序，如何创建警报和数据模型等内容，任何想通过 Splunk Enterprise 平台进行智能运维的读者都可以阅读本书。

本书的翻译工作由射手学院的译者团队完成，除封面译者外，刘婷婷还承担了本书的部分翻译与审校工作。

本书的专业审校由信通网赢的郑智超完成。信通网赢是全球领先的企业通信与 400 电话服务商，郑智超先生及同事的参与，保证了本书的专业品质。

虽然译者始终谨慎动笔，仔细求证，但难免还会存在疏漏，恳请广大读者批评指正。

目　录