

《Splunk实践指南》

图书基本信息

书名：《Splunk实践指南》

13位ISBN编号：9787111487672

出版时间：2015-2

作者：（美） Vincent Bumgarner

页数：336

译者：杨甲东

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Splunk实践指南》

内容概要

Splunk是一个收集、存储、报警、制表和研究机器数据的强有力工具。本书从理解Splunk交互界面的基本元素入手，详细讲解搜索语言的基本知识，对表格、图表、指示板等具体内容进行了细致的描述。通过对高级搜索案例和应用程序的逐步分析，本书向读者展示了构建用户自定义的应用程序的方法，为读者快速学习和掌握Splunk大数据开发与应用提供了系统指导。

《Splunk实践指南》共12章。第1章介绍Splunk交互界面的基本元素和一些重要概念；第2章详细介绍搜索语言的基础，讨论Splunk中的搜索功能，并讲解如何对搜索结果进行一些有用的再加工；第3章展示如何使用字段生成报表，以及如何构建自定义字段；第4章介绍如何通过使用Splunk提供的向导界面构建指示板；第5章深入讨论一些搜索的高级案例，展示搜索语句的若干强大特性；第6章展示更多的Splunk特性以帮助扩展查询语句，并在搜索时丰富数据；第7章深入讨论安装、构建、定制和分享应用程序；第8章介绍高级XML指示板的概念，以及简单XML指示板转换为高级XML指示板的实用方法；第9章讨论摘要索引及其在提高系统性能方面所发挥的作用；第10章深入讲解驱动Splunk的配置文件；第11章深入介绍关于分布式部署的相关内容，以及如何高效地对其进行配置；第12章阐述在输入数据、外部查询、渲染、定制命令和定制行为等方面扩展Splunk的方法。

作者简介

作者简介

Vincent Bumgarner 资深软件设计与开发专家，在多种平台从事软件设计近20年，有丰富的从业经验。他于2007年起开始使用Splunk，并一直关注该产品历年的更新和进展，并帮助许多公司培训了众多Splunk的用户，指导他们驾驭、扩展、管理这一极具灵活性的软件产品。

译者简介

杨甲东 毕业于清华大学，获计算机科学与技术工学博士学位，现任北京搜狐新媒体信息技术有限公司移动应用探索中心高级研发工程师，擅长领域为大规模数据处理、数据挖掘、信息检索、机器学习等。他已发表高水平学术论文10余篇，其中SCI检索论文5篇；获得国家发明专利2项；参与完成国家科技支撑计划项目1项，国家自然科学基金项目2项。

书籍目录

译者序

前言

第1章 Splunk交互界面1

1.1 登录Splunk1

1.2 首页应用程序2

1.3 顶栏4

1.4 搜索应用程序6

1.4.1 数据生成器6

1.4.2 概要视图6

1.4.3 搜索8

1.4.4 动作9

1.4.5 时间轴10

1.4.6 字段选择器11

1.4.7 搜索结果 11

1.5 使用时间选择器15

1.6 使用字段选择器16

1.7 使用管理器17

1.8 总结19

第2章 理解搜索20

2.1 有效地使用搜索词20

2.2 布尔和分组操作符21

2.3 点击修改你的搜索22

2.3.1 事件分割22

2.3.2 字段组件23

2.3.3 时间23

2.4 使用字段进行查询23

2.5 有效地使用通配符24

2.5.1 仅仅尾部通配符是有效的25

2.5.2 通配符最后测试25

2.5.3 在字段中补充通配符25

2.6 关于时间25

2.6.1 Splunk如何解析时间25

2.6.2 Splunk如何存储时间26

2.6.3 Splunk如何显示时间26

2.6.4 确定时区的方法及原因26

2.6.5 搜索时间的不同方式27

2.6.6 在搜索中嵌入式地指定时间29

2.6.7 `_indextime` 与 `_time` 对比29

2.7 加速搜索 29

2.8 分享结果30

2.9 保存结果供再次使用32

2.10 根据搜索创建报警34

2.10.1 定时计划34

2.10.2 动作36

2.11 总结37

第3章 表格、图表和字段38

3.1 关于管道符号38

- 3.2 使用top命令显示常见字段数值39
- 3.3 使用stats命令聚合数值42
- 3.4 使用图表转换数据45
- 3.5 使用时间图显示数值在时间上的变化46
- 3.6 使用字段49
 - 3.6.1 正则表达式49
 - 3.6.2 创建字段的命令51
 - 3.6.3 抽取日志级别52
- 3.7 总结60
- 第4章 简单XML指示板61
 - 4.1 指示板的作用61
 - 4.2 使用向导构建指示板62
 - 4.3 定时生成指示板69
 - 4.4 直接编辑XML69
 - 4.5 用户交互案例应用程序69
 - 4.6 构建表单70
 - 4.6.1 根据指示板创建表单70
 - 4.6.2 从一个表单中产生多个面板74
 - 4.6.3 后处理的搜索结果79
 - 4.6.4 后处理的限制80
 - 4.7 总结84
- 第5章 高级搜索案例85
 - 5.1 使用子查询寻找松散相关的事件85
 - 5.1.1 子查询85
 - 5.1.2 子查询使用的注意事项86
 - 5.1.3 嵌套子查询86
 - 5.2 使用事务命令87
 - 5.2.1 使用事务计算会话时长88
 - 5.2.2 合计事务统计信息90
 - 5.2.3 用事务组合子搜索90
 - 5.3 计算并发量94
 - 5.3.1 使用带并发的任务94
 - 5.3.2 使用并发量估计服务器负载95
 - 5.3.3 使用by字句计算并发量96
 - 5.4 计算每个时间片段的事务100
 - 5.4.1 使用时间chart命令100
 - 5.4.2 计算每分钟内的平均请求量101
 - 5.4.3 计算每分钟、每小时内的平均事件103
 - 5.5 重构top命令105
 - 5.6 总结110
- 第6章 扩展搜索111
 - 6.1 使用标签简化搜索111
 - 6.2 使用事件类型对结果分类113
 - 6.3 通过查找操作丰富数据116
 - 6.3.1 定义查找操作的表格文件117
 - 6.3.2 定义一个查找操作的表格文件118
 - 6.3.3 定义自动查找操作120
 - 6.3.4 在查找操作中排除故障122
 - 6.4 使用宏以重复使用逻辑123

- 6.4.1 创建一个简单的宏123
- 6.4.2 创建带有参数的宏124
- 6.4.3 使用eval命令构建一个宏125
- 6.5 创建工作流动作125
 - 6.5.1 使用事件中的数值运行查询125
 - 6.5.2 链接到外部站点127
 - 6.5.3 构建工作流动作以展示字段上下文128
- 6.6 使用外部命令132
 - 6.6.1 从XML中抽取数值133
 - 6.6.2 使用Google生成结果134
- 6.7 总结135
- 第7章 使用应用程序136
 - 7.1 定义应用程序136
 - 7.2 自带的应用程序137
 - 7.3 安装应用程序137
 - 7.3.1 从Splunk库中安装应用程序138
 - 7.3.2 从文件安装应用程序141
 - 7.4 构建第一个应用程序141
 - 7.5 编辑导航143
 - 7.6 定制应用程序外观146
 - 7.6.1 定制启动图标146
 - 7.6.2 使用定制CSS146
 - 7.6.3 使用定制HTML147
 - 7.7 对象权限151
 - 7.7.1 权限如何影响导航151
 - 7.7.2 权限如何影响其他对象152
 - 7.7.3 纠正权限问题153
 - 7.8 应用程序目录结构154
 - 7.9 将应用程序添加到Splunk库中155
 - 7.9.1 准备你的应用程序155
 - 7.9.2 打包应用程序157
 - 7.9.3 上传应用程序158
 - 7.10 总结158
- 第8章 构建高级指示板159
 - 8.1 使用高级XML的原因159
 - 8.2 不使用高级XML的原因159
 - 8.3 开发过程160
 - 8.4 高级XML结构160
 - 8.5 将简单XML转换为高级XML162
 - 8.6 模块逻辑流166
 - 8.7 理解布局面板168
 - 8.8 再次使用查询170
 - 8.9 使用意图171
 - 8.9.1 字符串替换172
 - 8.9.2 添加查询词 (addterm) 173
 - 8.10 创建定制的细化查询173
 - 8.10.1 根据定制查询语句构建明细查询173
 - 8.10.2 为另一个面板构建细化查询175
 - 8.10.3 对多面板使用HiddenPost- Process模块构建细化查询 177

- 8.11 第三方插件181
 - 8.11.1 Google地图181
 - 8.11.2 边视图工具 (Sideview Utils) 183
- 8.12总结191
- 第9章 摘要索引和CSV文件192
 - 9.1理解摘要索引192
 - 9.2何时使用摘要索引193
 - 9.3何时不使用摘要索引194
 - 9.4利用保存的查询生成摘要索引195
 - 9.5在查询中使用摘要索引事件196
 - 9.6使用sistats、sitop和sitimechart命令198
 - 9.7延迟如何影响摘要查询201
 - 9.8如何以及何时回填摘要数据202
 - 9.8.1使用fill_summary_index.py回填202
 - 9.8.2使用collect命令生成定制的摘要索引203
 - 9.9减少摘要索引的规模206
 - 9.9.1使用eval和rex命令定义分组字段206
 - 9.9.2使用带有通配符的查找操作208
 - 9.9.3使用事件类型对结果分组210
 - 9.10大跨度的时间范围内计算排名靠前的结果212
 - 9.11在摘要索引中存储原始事件215
 - 9.12使用CSV文件存储暂态数据217
 - 9.12.1预填充下拉菜单217
 - 9.12.2计算一天的数据218
 - 9.13总结219
- 第10章 配置Splunk220
 - 10.1Splunk配置文件的位置220
 - 10.2Splunk配置文件的结构221
 - 10.3配置合并逻辑222
 - 10.3.1合并顺序222
 - 10.3.2配置合并逻辑223
 - 10.3.3使用btool229
 - 10.4Splunk中的.conf文件概览230
 - 10.4.1props.conf230
 - 10.4.2inputs.conf236
 - 10.4.3transforms.conf243
 - 10.4.4fields.conf252
 - 10.4.5outputs.conf253
 - 10.4.6indexes.conf253
 - 10.4.7authorize.conf255
 - 10.4.8savedsearches.conf255
 - 10.4.9times.conf256
 - 10.4.10commands.conf256
 - 10.4.11web.conf256
 - 10.5用户交互资源256
 - 10.5.1视图与导航256
 - 10.5.2应用程序服务器资源257
 - 10.5.3元数据257
 - 10.6总结259

- 第11章 高级部署260
 - 11.1 制定安装计划260
 - 11.2 Splunk实例类型261
 - 11.2.1 Splunk转发器261
 - 11.2.2 Splunk索引器262
 - 11.2.3 Splunk搜索263
 - 11.3 常见数据来源263
 - 11.3.1 监视服务器日志263
 - 11.3.2 监视共享驱动器日志264
 - 11.3.3 批量处理日志264
 - 11.3.4 接收系统日志事件265
 - 11.3.5 处理数据库日志268
 - 11.3.6 使用脚本收集数据269
 - 11.4 计算索引器规模269
 - 11.5 制定冗余计划271
 - 11.5.1 索引器负载均衡271
 - 11.5.2 理解典型的系统中断272
 - 11.6 使用多个索引273
 - 11.6.1 索引的目录结构273
 - 11.6.2 创建更多索引的时机274
 - 11.6.3 桶的生命周期275
 - 11.6.4 计算索引规模276
 - 11.6.5 使用卷管理多个索引277
 - 11.7 部署Splunk二进制文件279
 - 11.7.1 根据压缩文件部署280
 - 11.7.2 使用msiexec命令部署280
 - 11.7.3 添加基本配置280
 - 11.7.4 配置Splunk以实现开机时启动281
 - 11.8 使用应用程序组织配置281
 - 11.9 配置分布285
 - 11.9.1 使用你自己的部署系统285
 - 11.9.2 使用Splunk部署服务器286
 - 11.10 为授权使用LDAP291
 - 11.11 使用单点登录 292
 - 11.12 负载均衡与Splunk292
 - 11.12.1 Web292
 - 11.12.2 splunktcp293
 - 11.12.3 部署服务器293
 - 11.13 多搜索头部293
 - 11.14 总结294
- 第12章 扩展Splunk295
 - 12.1 书写脚本化的输入以收集数据295
 - 12.1.1 捕获不带日期的脚本输出295
 - 12.1.2 捕获脚本输出作为单独事件298
 - 12.1.3 编写长时间运行的脚本输入299
 - 12.2 在命令行中使用Splunk300
 - 12.3 通过REST命令查询Splunk301
 - 12.4 编写命令304
 - 12.4.1 何时不编写命令304

- 12.4.2 何时编写命令305
- 12.4.3 配置命令305
- 12.4.4 添加字段306
- 12.4.5操作数据307
- 12.4.6 转换数据308
- 12.4.7产生数据313
- 12.5编写脚本化的查找操作以丰富数据314
- 12.6编写事件渲染器316
 - 12.6.1 使用特殊字段317
 - 12.6.2 基于字段数值的字段表格318
 - 12.6.3 打印XML320
- 12.7 编写脚本化的报警动作以处理结果322
- 12.8 总结324

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com