

УДК 004.056.5  
ББК 32.973  
М60

**Миллер Дж. Д.**

М60 Внедрение Splunk 7 / пер. с англ. А. Н. Киселева. – М.: ДМК Пресс, 2019. – 490 с.: ил.

**ISBN 978-5-97060-698-8**

Среди систем, созданных для агрегации, систематизации и прочей автоматизации работы с логами, Splunk – один из самых мощных. Он позволит следить за тонкостями жизни всех ваших систем, особенно если их много и они достаточно распределенные.

Splunk – ведущая платформа, реализующая эффективные методологии поиска, мониторинга и анализа больших данных с постоянно растущим объемом. Эта книга позволит вам реализовать новые услуги и использовать их для быстрой и эффективной обработки машинных данных.

Вы познакомитесь со всеми возможностями и улучшениями в Splunk 7, включая новые модули Splunk Cloud и Machine Learning Toolkit, научитесь эффективно использовать поисковые запросы и метасимволы, а также работать с полями и расширениями диаграмм.

Издание будет полезно всем, кто занимается информационной безопасностью в организации и выявлением инцидентов ИБ.

УДК 004.056.5  
ББК 32.973

Authorized Russian translation of the English edition of Implementing Splunk 7, Third Edition ISBN 9781788836289 © 2018 Packt Publishing.

This translation is published and sold by permission of Packt Publishing, which owns or controls all rights to publish and sell the same.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-78883-628-9 (англ.)  
ISBN 978-5-97060-698-8 (рус.)

© 2018 Packt Publishing  
© Оформление, издание, перевод, ДМК Пресс, 2019

# Содержание

<b>Участники</b> .....	13
<b>Вступление</b> .....	14
<b>Глава 1. Интерфейс Splunk</b> .....	18
Логирование в Splunk.....	18
Домашнее приложение .....	19
Верхняя полоса меню .....	23
Приложение Search & Reporting .....	27
Генератор данных .....	28
Представление Summary.....	28
Поиск.....	30
Действия .....	31
Шкала времени.....	32
Виджет выбора полей .....	33
Результаты поиска .....	35
Использование виджета выбора времени .....	38
Использование виджета выбора полей.....	39
Раздел с настройками.....	40
Splunk Cloud .....	44
Опробование перед покупкой .....	45
Краткий тур по облаку.....	46
Полоса меню в Splunk Cloud .....	48
Splunk reference App – PAS .....	50
Universal forwarder .....	50
eventgen .....	50
Что дальше .....	50
Итоги .....	51
<b>Глава 2. Основы поиска</b> .....	52
Эффективное использование критериев поиска .....	52
Логические операторы и операторы группировки .....	53
Щелчки мышью могут менять критерии поиска .....	55
Сегментирование событий.....	55
Виджеты полей .....	55
Время .....	57
Использование полей в поиске.....	58
Использование виджета выбора полей .....	58
Эффективное использование метасимволов .....	59
Метасимволы в полях .....	60

## 6 ❖ Содержание

Все о времени.....	60
Как Splunk анализирует время.....	60
Как Splunk хранит время.....	61
Как Splunk отображает время.....	61
Как определяются часовые пояса, и почему это важно.....	61
Разные способы поиска по времени.....	62
Определение времени в строке запроса.....	66
Ускорение поиска.....	67
Передача результатов другим.....	68
Адрес URL.....	68
Сохранение в виде отчета.....	69
Сохранение в виде дашборда.....	71
Сохранение в виде оповещения.....	72
Сохранение в виде типа события.....	73
Настройки задания поиска.....	73
Сохранение поиска для повторного использования.....	74
Создание оповещения на основе поиска.....	77
Enable Actions.....	79
Action Options.....	79
Sharing.....	79
Аннотирование событий.....	81
Иллюстрация.....	82
Итоги.....	83
<b>Глава 3. Таблицы, диаграммы и поля.....</b>	<b>84</b>
О символе вертикальной черты.....	84
Вывод типичных значений полей командой top.....	85
Управление выводом команды top.....	87
Агрегирование значений с помощью команды stats.....	88
Представление данных с помощью команды chart.....	91
Отображение шкалы времени с помощью timechart.....	93
Параметры команды timechart.....	95
Работа с полями.....	96
Пример регулярного выражения.....	97
Команды создания полей.....	99
Извлечение уровня журналирования.....	100
Расширение поддержки диаграмм в версии 7.0.....	110
charting.lineWidth.....	111
charting.data.fieldHideList.....	112
charting.legend.mode.....	113
charting.fieldDashStyles.....	113
charting.axisY.abbreviation.....	114
Итоги.....	114
<b>Глава 4. Модели данных и сводные таблицы.....</b>	<b>115</b>
Что такое модель данных?.....	115
Роль моделей данных в поиске.....	116

Объекты модели данных .....	116
Acceleration в версии 7.0 .....	117
Создание модели данных .....	118
Заполнение полей в диалоге создания новой модели данных .....	119
Добавление полей (атрибутов) .....	122
Подстановочные атрибуты .....	125
Потомки .....	127
Что такое сводная таблица? .....	129
Редактор Pivot Editor .....	131
Работа с элементами сводных таблиц .....	132
Разбиение (на строки или столбцы) .....	133
Форматирование сводной таблицы .....	134
Короткий пример .....	134
Sparklines .....	138
Итоги .....	140

## **Глава 5. Простые дашборды на XML .....**

Назначение дашбордов .....	141
Конструирование дашбордов с помощью мастеров .....	142
Добавление еще одной панели .....	145
Преобразование панели в отчет .....	152
Дополнительные настройки .....	157
И снова о дашборде .....	157
Добавление полей ввода .....	157
Редактирование исходного кода .....	158
Редактирование пользовательского интерфейса .....	158
Непосредственное редактирование XML .....	158
Приложение с примерами пользовательского интерфейса .....	159
Создание форм .....	159
Создание формы из дашборда .....	159
Управление несколькими панелями из одной формы .....	163
Постобработка результатов поиска .....	165
Ограничения постобработки .....	165
Устаревшие функции .....	166
Автоматический запуск дашборда .....	168
Выполнение запросов по расписанию .....	169
Итоги .....	170

## **Глава 6. Примеры продвинутого поиска .....**

Использование подзапросов для поиска дополнительных событий .....	171
Подзапрос .....	171
Ограничения подзапросов .....	173
Вложенные подзапросы .....	174
Использование транзакций .....	175
Определение продолжительности сеанса .....	175
Получение агрегированных статистических показателей .....	177
Подзапросы в транзакциях .....	178

## 8 ❖ Содержание

Команда concurrency .....	182
Использование команд transaction и concurrency .....	182
Использование команды concurrency	
для оценки нагрузки на сервер .....	183
Определение уровня concurrency с использованием предложения by .....	184
Подсчет событий в интервалах времени .....	190
С помощью timechart .....	190
Вычисление среднего числа запросов в минуту .....	191
Вычисление среднего числа событий в минуту за каждый час .....	193
Имитация команды top .....	195
Ускорение .....	201
Большие данные – стратегия получения сводной информации .....	202
Ускорение отчетов .....	202
Доступность ускорения отчетов .....	205
Расширенная поддержка метрик в версии 7.0 .....	205
Определение метрик в Splunk .....	205
Использование метрик в Splunk .....	206
Итоги .....	207

## Глава 7. Расширенный поиск .....

Использование тегов для упрощения поиска .....	208
Классификация результатов по типам событий (eventtypes) .....	212
Использование lookups для обогащения данных .....	216
Определение файла с lookup-таблицей .....	216
Настройка определений lookup .....	218
Определение автоматического Lookup .....	220
Проблемы с lookups .....	223
Применение макросов .....	224
Создание простого макроса .....	224
Создание макроса с аргументами .....	225
Создание сценариев реагирования .....	226
Запуск нового поиска с использованием значения из события .....	226
Ссылки на внешние сайты .....	229
Создание сценария реагирования	
для отображения контекста поля .....	231
Использование внешних команд .....	236
Извлечение значений из XML .....	236
Генерирование результатов с помощью Google .....	238
Итоги .....	239

## Глава 8. Работа с приложениями .....

Определение приложения .....	240
Встроенные приложения .....	241
Установка приложений .....	242
Установка приложений из Splunkbase .....	243
Установка приложений из файлов .....	247
Наше первое приложение .....	247

Настройка навигации.....	251
Настройка внешнего вида приложения.....	253
Настройка значка запуска.....	253
Использование своих стилей оформления CSS.....	254
Использование своей разметки HTML.....	254
Разрешения доступа к объектам.....	258
Как разрешения влияют на навигацию.....	259
Как разрешения влияют на другие объекты.....	259
Исправление проблем с разрешениями.....	260
Структура каталога приложения.....	261
Добавление приложения в Splunkbase.....	263
Упаковка приложения.....	265
Выгрузка приложения.....	265
Самостоятельное управление приложениями.....	266
Итоги.....	267

## **Глава 9. Создание продвинутых дашбордов ..... 268**

Причины использования продвинутого XML.....	268
Причины отказаться от использования продвинутого XML.....	269
Процесс разработки.....	269
Структура продвинутого XML.....	270
Преобразование упрощенного XML в продвинутый.....	272
Логика модулей.....	277
Знакомство с layoutPanel.....	279
Размещение панелей.....	280
Повторное использование запроса.....	281
Использование intentions.....	282
stringreplace.....	282
addterm.....	283
Создание нестандартных детализаций.....	284
Определение детализации в своем запросе.....	284
Создание детализации в отдельной панели.....	286
Применение HiddenPostProcess для создания детализаций с несколькими панелями.....	288
Сторонние расширения.....	291
Google Maps.....	291
Sideview Utils.....	293
Модуль search в Sideview.....	294
Итоги.....	302

## **Глава 10. Summary-индексы и файлы CSV ..... 303**

Общие сведения о summary-индексах.....	303
Создание summary-индекса.....	304
Когда следует использовать summary-индексы.....	305
Когда не следует использовать summary-индексы.....	306
Заполнение summary-индексов через saved search.....	307
Использование summary-индексов в запросах.....	308

Использование sistats, sitop и sitimechart .....	310
Как задержка влияет на запросы, использующие summary-индексы .....	313
Как и когда добавлять исторические данные в summary-индексы .....	315
Использование fill_summary_index.py для заполнения .....	315
Создание нестандартных summary-индексов с помощью collect .....	316
Уменьшение размера summary-индекса.....	319
Определение полей для группировки с помощью eval и rex .....	320
Подстановка с метасимволами .....	322
Группировка результатов по типам событий .....	325
Подсчет наиболее часто встречающихся данных в больших интервалах времени .....	327
Поиск в summary-индексе .....	331
Использование файлов CSV для хранения промежуточных данных.....	332
Предварительное заполнение раскрывающегося списка .....	332
Создание вычислений, выполняющихся в течение дня.....	333
Итоги .....	334

## Глава 11. Настройка Splunk..... 335

Местоположение конфигурационных файлов Splunk .....	335
Структура конфигурационных файлов Splunk .....	336
Логика слияния конфигураций .....	337
Порядок слияния .....	337
Логика слияния конфигураций .....	339
Инструмент btool.....	344
Обзор конфигурационных файлов Splunk.....	345
props.conf .....	345
inputs.conf .....	352
transforms.conf.....	361
fields.conf.....	371
outputs.conf.....	372
indexes.conf.....	372
authorize.conf.....	374
savedsearches.conf.....	375
times.conf .....	375
commands.conf.....	375
web.conf.....	375
Ресурсы пользовательского интерфейса .....	375
Представления и навигация .....	376
Ресурсы сервера приложений .....	376
Метаданные .....	377
Итоги .....	379

## Глава 12. Продвинутая настройка .....

Планирование архитектуры системы .....	380
Типы серверов Splunk.....	381
Форвардеры Splunk .....	381
Индексеры Splunk .....	382
Поиск в Splunk.....	383

Типичные источники данных.....	383
Мониторинг файлов журналов на сервере.....	384
Мониторинг файлов журналов на общих дисках (file share).....	385
Периодическая (Batch) обработка файлов журналов .....	386
Прием событий от syslog .....	387
Извлечение событий из базы данных.....	391
Использование скриптов для сбора данных .....	392
Организация индексирования .....	393
Планирование отказоустойчивости .....	395
Коэффициент репликации .....	396
Балансировка нагрузки на индексеры.....	397
Основные последствия останова индексеров.....	398
Работа с несколькими индексами .....	399
Структура каталогов индекса .....	400
Когда следует создавать дополнительные индексы .....	400
Жизненный цикл корзины (bucket) .....	402
Определение размера индекса.....	404
Использование томов для управления индексами.....	404
Развертывание серверов Splunk .....	406
Развертывание из файла tar .....	407
Развертывание из дистрибутива msixexec .....	407
Добавление базовой конфигурации .....	408
Настройка запуска Splunk на этапе загрузки операционной системы .....	408
Использование приложений для организации конфигурации.....	409
Распределение конфигураций по целям .....	409
Установка конфигурации .....	413
Использование собственной системы развертывания .....	413
Использование Splunk Deployment Server .....	414
Использование LDAP для аутентификации .....	420
Использование единой точки входа.....	420
Балансировщики нагрузки и Splunk .....	421
Веб-серверы.....	421
splunktcp .....	422
Сервер развертывания.....	422
Несколько Search Head .....	422
Итоги .....	423

## Глава 13. Расширение Splunk .....

Разработка скриптов ввода для сбора данных .....	424
Прием данных без дат.....	424
Прием данных, представляющих единственное событие .....	427
Прием данных от скриптов, выполняющихся продолжительное время .....	429
Использование Splunk из командной строки.....	430
Отправка запросов в Splunk через REST-интерфейс.....	431
Реализация своих команд поиска .....	434
Когда не стоит писать свои команды.....	434
Когда стоит писать свои команды .....	435



## 12 ❖ Содержание

Конфигурирование команд .....	436
Добавление полей .....	437
Манипулирование данными .....	438
Преобразование данных.....	439
Генерирование данных.....	444
Реализация скриптов для обогащения данных .....	445
Реализация визуализаторов событий .....	448
Визуализация определенных полей .....	448
Таблица полей на основе их значений .....	450
Форматированный вывод XML .....	453
Реализация скриптов для обработки уведомлений (alert) .....	454
Hunk .....	457
Итоги .....	458
<b>Глава 14. Machine Learning Toolkit .....</b>	<b>459</b>
Что такое машинное обучение?.....	459
Механизмы рекомендаций по содержимому .....	460
Обработка естественного языка .....	460
Оперативные исследования .....	461
Обзор инструментария .....	461
Время, потраченное не зря.....	462
Получение приложения .....	463
Рабочее пространство .....	465
Ассистенты.....	467
Расширенный язык запросов SPL.....	468
Приложение ML-SPL Performance .....	468
Создание модели .....	469
Прогнозирование временных рядов .....	469
Использование Splunk .....	470
Запуск приложения .....	470
Проверка .....	475
Эксплуатация.....	476
Сохранение в виде отчета .....	476
Исследование данных.....	477
Итоги .....	478