Содержание

Участники

Об авторе

Джеймс Д. Миллер (James D. Miller) – эксперт, сертифицированный в IBM, творческий новатор, директор, руководитель проектов и архитектор систем и приложений с более чем 35-летним опытом применения, проектирования и разработки. Помогает клиентам внедрять новые и иногда революционные технологии и платформы, интеграцию с IBM Watson Analytics, Cognos BI, TM1, веб-архитектуры, системный анализ, проектирование и тестирование графических интерфейсов и моделирование баз данных. Занимался проектированием и разработкой OLAP, клиент-серверных и веб-приложений, а также приложений для больших вычислительных систем.

Хочу поблагодарить Нанетт (Nanette), Шелби (Shelby) и Пейдж (Paige), которые не перестают удивлять меня своей поддержкой и любовью.

О рецензентах

Кайл Смит (Kyle Smith) – истинный энтузиаст из Пенсильвании, активно использующий Splunk с 2010 года. Много раз выступал на конференции Splunk User Conference, активный участник сообщества Splunk Answers Community, IRC-канала #splunk и каналов Splunk Slack. Опубликовал несколько приложений для Splunk и расширений для Splunkbase, главного приложения сообщества Splunk, а также дополнений к платформе публикации. В настоящее время работает консультантом/разработчиком в компании Aplura, LLC. Написал книгу «Splunk Developer's Guide», также выпущенную издательством Packt.

Хочу сказать спасибо моей супруге, которая терпеливо мирилась с моей занятостью, когда я работал над этой книгой. Без нее все это было бы бессмысленным.

Йогеш Рахея (Yogesh Raheja) – сертифицированный эксперт в области DevOps и облачных технологий с десятилетним опытом. Имеет опыт в таких областях, как администрирование операционных систем, управление исходным кодом, сборка и выпуск инструментов, использование средств непрерывной интеграции/развертывания/доставки, настройка контейнеров, использование инструментов управления конфигурациями, мониторинг, применение инструментов журналирования и организация общедоступных и частных облачных окружений. С радостью делится своим опытом с другими на различных форумах, конференциях, вебинарах, блогах и в LinkedIn (https://in.linkedin.com/in/yogesh-raheja-b7503714). Написал книги «Automation with Puppet 5» и «Automation with Ansible».

Вступление

Splunk – ведущая платформа, предлагающая эффективные методы поиска, мониторинга и анализа растущих объемов данных. Эта книга поможет вам внедрить новые службы и использовать их для быстрой и эффективной обработки машинных данных.

Мы познакомим вас со всеми новыми особенностями, улучшениями и предложениями в Splunk 7. Рассмотрим новые модули Splunk – Splunk Cloud и Machine Learning Toolkit – упрощающие применение данных. Кроме того, вы узнаете, как эффективно использовать поиск с логическими операторами и операторами группировки. Вы не только узнаете об оптимизации скорости поиска, но и познакомитесь с приемами эффективного использования шаблонных символов. Далее вы увидите, как использовать статистические и агрегированные значения, строить диаграммы данных и временные диаграммы для отображения изменения значений с течением времени; вы также научитесь работать с полями и Chart Enhancements и узнаете, как создать модель данных с Faster Data Model Acceleration. После этого мы перейдем к знакомству с XML-панелями, работе с приложениями, созданию продвинутых панелей, настройке и расширению Splunk и многим другим возможностям. Наконец, мы научим вас пользоваться инструментами машинного обучения Machine Learning Toolkit и дадим несколько советов и рекомендаций, которые помогут вам быстро и эффективно внедрить Splunk.

К концу этой книги вы будете иметь полное представление о программном обеспечении Splunk и уметь интегрировать Splunk в свои задачи и проекты.

Кому адресована эта книга

Эта книга предназначена для аналитиков данных, бизнес-аналитиков и ИТ-администраторов, желающих поднять на новый уровень умение работы с большими данными, операционный анализ, управление журналами и мониторинг систем в своей организации. Обладание некоторыми знаниями Splunk поможет вам получить максимум выгоды от этой книги.

О чем рассказывается в книге

Глава 1 «*Интерфейс Splunk*» познакомит вас с основными элементами интерфейса Splunk.

Глава 2 «*Основы поиска*» знакомит с техническими деталями работы механизма поиска, чтобы вы могли эффективнее выполнять поиск и создавать отчеты.

Глава 3 «*Таблицы, диаграммы и поля*» расскажет, как использовать поля не только для поиска; здесь вы будете учиться строить таблицы и графики. А затем узнаете, как создавать свои поля.

Глава 4 «*Модели данных и сводные таблицы (Pivot)*» охватывает модели данных и сводные таблицы, редактор сводных таблиц, элементы и фильтры сводных таблиц и встраиваемые графики.

Глава 5 «*Дашборды на упрощенном XML*» демонстрирует дашборды на упрощенном XML; их назначение; создание с помощью мастера, планирование создания и редактирование разметки XML непосредственно; конструирование форм.

Глава 6 «*Примеры продвинутого поиска*» демонстрирует интересные примеры улучшения поиска. Здесь мы раскроем некоторые по-настоящему мощные возможности языка поиска и рассмотрим несколько трюков, которые я накопил за годы работы.

Глава 7 «*Расширенный поиск*» демонстрирует еще более мощные возможности Splunk для расширения языка поиска и пополнения данных во время поиска.

Глава 8 «*Работа с приложениями*» описывает структуру приложений для Splunk, а также рассказывает о последней версии механизма Self-Service App Management (первоначально появившегося в Splunk 6.6), обновленной в версии 7.0.

Глава 9 «*Создание продвинутых дашбордов*» охватывает методы вложения модулей, атрибут `layoutPanel`, intention и альтернативу intentions – SideView Utils.

Глава 10 «*Summary-индексы и файлы CSV*» исследует использование summary-индексов и команд для работы с ними.

Глава 11 «*Настройка Splunk*» знакомит с приемами настройки и описывает наиболее широко используемые аспекты конфигурации Splunk.

Глава 12 «*Продвинутая настройка*» погружается в особенности развертывания в распределенной среде и показывает, как эффективно настроить такое развертывание.

Глава 13 «*Расширение Splunk*» демонстрирует множество способов расширения Splunk новыми средствами ввода, управления и вывода событий.

Глава 14 «*Инструменты машинного обучения*» знакомит с основами инструментов Machine Learning Toolkit в Splunk и показывает, как с их помощью создать модель машинного обучения.

Что необходимо, чтобы извлечь максимум пользы из книги

Прежде чем начать читать эту книгу, вам нужно загрузить Splunk с сайта https://www.splunk.com/ru_ru/download.html.

Официальное руководство по установке можно найти по адресу: http://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements.

Код в этой книге использует генератор данных, который можно применять для проверки демонстрируемых здесь запросов. Однако, поскольку данные генерируются случайным образом, не все запросы будут работать, как ожидается, и вам может потребоваться внести в них соответствующие изменения.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com или www.дмк.рф в разделе **Читателям – Файлы к книгам**.

После загрузки файла архива распакуйте его, используя последнюю версию:

- WinRAR/7-Zip в Windows;
- Zipeg/iZip/UnRarX в Mac;
- 7-Zip/PeaZip в Linux.

Пакет с исходным кодом примеров доступен также в репозитории GitHub по адресу: https://github.com/PacktPublishing/Implementing-Splunk-7-Third-Edition. Все обновления кода, по мере дальнейшей работы над ними, мы будем производить только в репозитории GitHub.

Соглашения

В этой книге используется несколько разных стилей оформления текста с целью обеспечить визуальное отличие информации разных типов.

Программный код в тексте, имена таблиц баз данных, имена папок, имена файлов, расширения файлов, пути в файловой системе, фиктивные адреса URL, ввод пользователя и ссылки в Twitter оформляются, как показано в следующем предложении: «События должны иметь поле `_time`».

Блоки программного кода оформляются так:

```
sourcetype="impl_splunk_gen" ip="*"
| rex "ip=(?P<subnet>\d+\.\d+\.\d+)\.\d+"
| table ip subnet
```

Новые термины и важные определения, а также надписи на экране будут выделяться в обычном тексте **жирным шрифтом**. Например, пункты меню или надписи в диалоговых окнах будут оформляться так: «Определить поле можно несколькими способами. Сначала рассмотрим интерфейс **Extract Fields**».

Так будут оформляться предупреждения и важные примечания.

Так будут оформляться советы или рекомендации.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв прямо на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com, при этом напишите название книги в теме письма.

Если есть тема, в которой вы квалифицированы, и вы заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры, для того чтобы удостовериться в качестве наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг — возможно, ошибку в тексте или в коде, — мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от расстройств и поможете нам улучшить последующие версии данной книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Packt очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконно выполненной копией любой нашей книги, пожалуйста, сообщите нам адрес копии или веб-сайта, чтобы мы могли принять меры.

Пожалуйста, свяжитесь с нами по адресу электронной почты dmkpress@gmail.com со ссылкой на подозрительные материалы.

Мы высоко ценим любую помощь по защите наших авторов, помогающую нам предоставлять вам качественные материалы.

Глава 1

Интерфейс Splunk

Это уже третье издание книги! Популярность Splunk продолжает расти, и появление каждой новой версии продукта с энтузиазмом встречается пользователями. Содержимое всех глав в этом издании было пересмотрено и приведено в соответствие с версией Splunk 7.0. Появились новые разделы, охватывающие новые особенности, добавленные в версии 7.0. Также появились две новые главы, одна из них охватывает набор инструментов машинного обучения (Machine Learning Toolkit, MLT), а другая предлагает рекомендации, эффективность которых подтверждена практикой. Поэтому даже если у вас уже есть более раннее издание этой книги (спасибо вам за его покупку!), вам определенно стоит приобрести данное издание.

Приступим!

Эта глава познакомит вас с наиболее часто используемыми элементами интерфейса Splunk и затронет некоторые понятия, которые более подробно будут рассматриваться в последующих главах. Возможно, у вас появится желание сразу перейти к их изучению, но имейте в виду, что общее знакомство с интерфейсом в этой главе может предохранить вас от неудач в будущем. В этой главе мы рассмотрим следующие темы:

- журналирование и выбор приложений;
- подробное описание элементов интерфейса поиска;
- краткий обзор интерфейса администратора.

Логирование в Splunk

Графический интерфейс Splunk (Splunk поддерживает также интерфейс командной строки (CLI) и REST API) доступен через веб-интерфейс, то есть вам не потребуется устанавливать никакого клиентского программного обеспечения. Новейшие браузеры с быстрыми движками JavaScript, такие как Chrome, Firefox и Safari, прекрасно отображают этот интерфейс. Начиная с версии Splunk 6.2.0 (и версия 7.0 не исключение) не требуется устанавливать в браузеры никаких расширений.

По умолчанию Splunk использует порт `8000` (который можно изменить). Адрес будет выглядеть примерно так: `http://mysplunkserver:8000` или `http://mysplunkserver.mycompany.com:8000`:

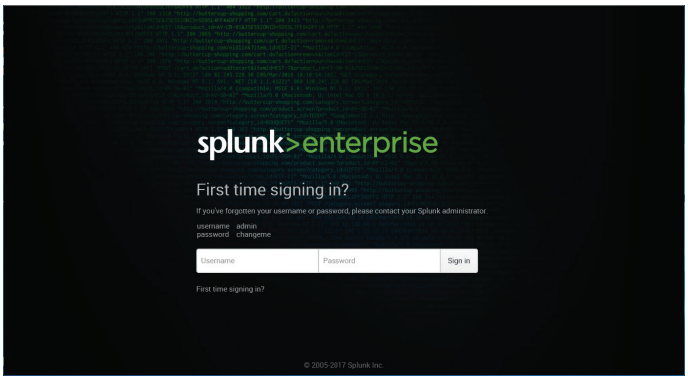

Рис. 1.1 ❖ Интерфейс Splunk

Если вы установили систему Splunk на локальный компьютер, она будет доступна по любому из следующих адресов: `http://localhost:8000`, `http://127.0.0.1:8000`, `http://имя_компьютера:8000` или `http://имя_компьютера.local:8000`.

После ввода адреса в окне браузера вы увидите самую первую страницу – страницу входа. По умолчанию создается учетная запись с именем пользователя *admin* и паролем *changeme*. Сразу после входа вам будет предложено изменить пароль пользователя `admin`. *Обязательно* измените его, чтобы предотвратить несанкционированный доступ к вашей системе.

По умолчанию учетные записи создаются и хранятся внутри Splunk. Однако есть возможность настроить аутентификацию с использованием другой системы, например **Lightweight Directory Access Protocol** (**LDAP**). По умолчанию аутентификация выполняется локально. Если у вас есть настроенная система LDAP, тогда аутентификация будет выполняться в таком порядке: `LDAP/Local`.

Домашнее приложение

После входа автоматически запускается приложение **Launcher** (некоторые называют его **домашним** – **Home**). Это панель для запуска других приложений и руководств.

Обратите внимание, что после первого входа в систему Splunk отобразит всплывающее окно **Help us improve Splunk software** (Помогите нам улучшить Splunk), в котором предлагается дать право системе Splunk собирать информацию об особенностях ее использования. Вам решать, как ответить на эту просьбу.

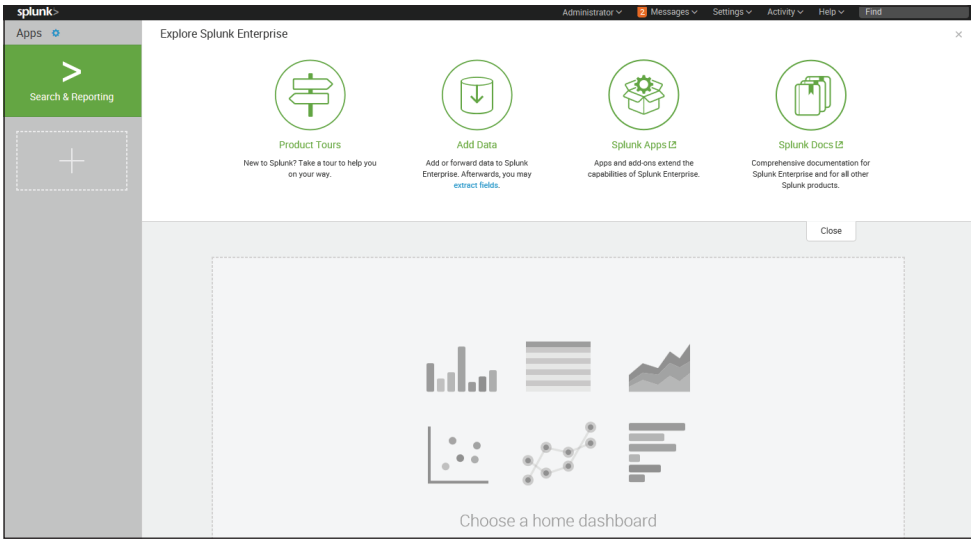

Рис. 1.2 ❖ Приложение **Launcher**

В предыдущих версиях Splunk на вкладке **Welcome** (Добро пожаловать) присутствовали два важных ярлыка: **Add data** (Добавить данные) и **Launch search** (Запустить поиск). В версии 6.2.0 домашнее приложение было разделено на отдельные области, или панели: **Explore Splunk Enterprise** (**Add Data** (Добавить данные), **Splunk Apps** (Приложения Splunk), **Splunk Docs** (Документация Splunk) и **Splunk Answers** (Ответы Splunk)), **Apps** (страница управления приложениями), **Search & Reporting** (ссылка на приложение поиска) и область, куда вы сможете поместить свою панель по умолчанию.

В версии 7.0 главная страница изменилась не очень сильно, хотя вы можете заметить некоторые изменения в графическом оформлении. Но в целом компоновка страницы осталась прежней, с теми же панелями и ссылками на те же функции.

Подробнее о приложениях и панелях мы поговорим в последующих главах.

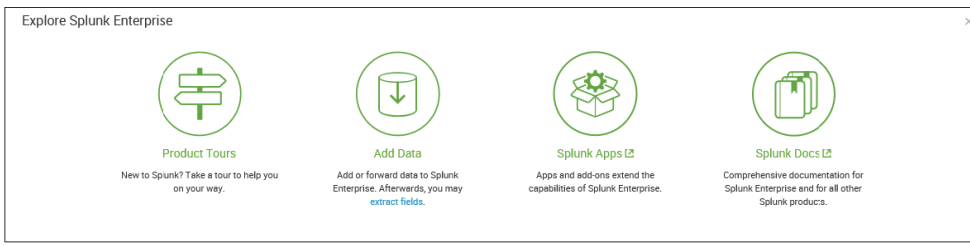

Рис. 1.3 ❖ Панель **Explore Splunk Enterprise**

На панели **Explore Splunk Enterprise** присутствуют следующие ссылки (см. рис. 1.3):

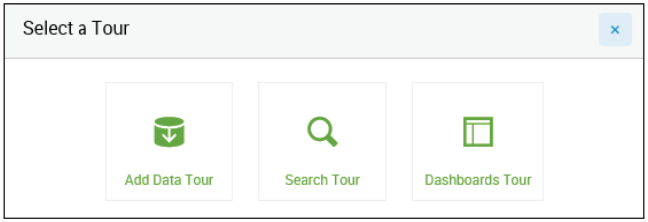

Рис. 1.4 ❖ Выбор обзора

- **Product Tours** (Обзор продуктов, новинка версии 7.0): после щелчка по этой ссылке вам будет предложено на выбор три обзора (рис. 1.4) – **Add Data Tour** (Обзор добавления данных), **Search Tour** (Обзор поиска) и **Dashboards Tour** (Обзор дашбордов[1]);

Обратите внимание: когда вы впервые щелкнете на любой из ссылок, перечисленных далее, вам будет предложено сделать паузу и познакомиться с обзором соответствующей функции. Конечно, вы всегда сможете вернуться назад к ссылке **Product Tours** (Обзор продуктов), чтобы познакомиться с тем или иным обзором.

- **Add Data** (Добавить данные): ссылка для добавления данных на страницу Splunk. Этот интерфейс послужит отличной начальной точкой для получения локальных данных, поступающих в Splunk (чтобы сделать их доступными для пользователей Splunk). Интерфейс **Preview data** (Предварительный просмотр данных) избавляет от необходимости выполнять сложные настройки. Мы не будем рассматривать эти интерфейсы здесь, но исследуем файлы конфигурации, которые эти мастера производят, в главе 11 «*Настройка Splunk*»;
- **Splunk Apps** (Приложения Splunk): поможет найти дополнительные приложения в онлайн-магазине Splunk Apps Marketplace (https://splunkbase.splunk.com/) и установить их. Это очень удобный ресурс, где пользователи и разработчики Splunk могут размещать свои приложения для Splunk, в основном бесплатные, но среди них есть платные премиум-версии. Обратите внимание, что для загрузки приложений необходимо иметь идентификатор пользователя splunk.com;

[1] От англ. *dashboard*. В Splunk – это документ с лаконично представленными статистическими данными, отчетами и нередко с инфографикой. В Splunk используются два похожих термина «dashbord» и «panel», поэтому, чтобы избежать путаницы, я буду использовать транслитерацию «дашборд» для перевода термина «dashbord» и «панель» для перевода «panel». – *Прим. перев.*

- **Splunk Docs** (Документация Splunk): по этой ссылке доступен огромный объем документации для Splunk, в частности, перейдя по ссылке https://answers.splunk.com, вы сможете присоединиться к сообществу Splunk на Splunkbase (https://splunkbase.splunk.com/) и решить вопросы, возникающие у вас при работе с системой Splunk. Кроме того, здесь же вы увидите ссылку http://docs.splunk.com/Documentation/Splunk на самую свежую документацию для любых (почти) версий Splunk;
- в разделе **Apps** (Приложения, слева на рис. 1.2) отображаются приложения с элементами графического интерфейса в вашем экземпляре Splunk. Термин «приложение» в Splunk имеет свое значение. Приложение не обязательно должно иметь графический интерфейс; это просто коллекция конфигураций, заключенная в структуру каталогов, имеющая особый смысл для Splunk. Мы обсудим приложения более подробно в главе 8 «*Работа с приложениями*»;
- **Search & Reporting** (Поиск и отчеты, слева на рис. 1.2): ссылка на Splunk-приложение **Search & Reporting** (Поиск и отчеты);

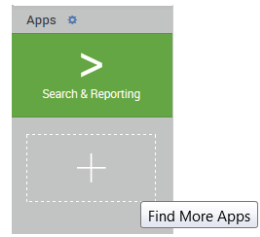

Рис. 1.5 ❖ Ссылка для добавления дополнительных приложений

- под ссылкой **Search & Reporting** (Поиск и отчеты) вы увидите прямоугольную область, ограниченную пунктирной рамкой, при наведении указателя мыши на которую появляется всплывающая подсказка **Find More Apps** (Найти еще приложения), как показано на рис. 1.5. Щелчок на ссылке откроет страницу **Browse more apps** (Обзор дополнительных приложений), что и ссылка **Splunk Apps** (Приложения Splunk), описанная выше;
- **Choose a home dashboard** (Выбор домашнего дашборда, см. рис. 1.6) предлагает понятный способ выбора существующего дашборда (на упрощенном XML) для отображения на начальной (домашней) странице. Благодаря этому вы всегда будете видеть знакомый начальный экран после входа в Splunk. На рис. 1.7 показан диалог **Choose Default Dashboard** (Выбор дашборда по умолчанию).

Рис. 1.6 ❖ Ссылка для выбора домашней панели

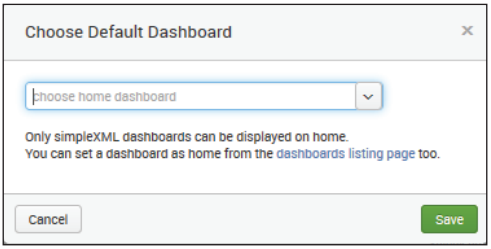

Рис. 1.7 ❖ Диалог выбора дашборда по умолчанию

После выбора дашборда в раскрывающемся списке он станет частью вашей домашней страницы и будет отображаться при каждом входе в Splunk, пока вы его не замените. Вместе с системой Splunk по умолчанию не устанавливается никаких дашбордов, кроме приложения **Search & Reporting** (Поиск и отчеты). Поэтому выбрать дашборд по умолчанию вы сможете только после его создания.

Верхняя полоса меню

Полоса меню, располагающаяся *вдоль верхнего края* окна, содержит информацию о вашем текущем местоположении в системе, а также ссылки на настройки, другие приложения и на раздел администрирования.

В левом верхнем углу отображается текущее приложение, например на рис. 1.8 показана часть верхней полосы с текущим местоположением после перехода в приложение **Search & Reporting** (Поиск и отчеты).

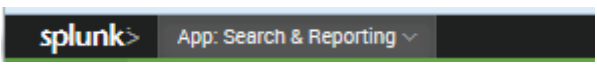

Рис. 1.8 ❖ Текущее местоположение в полосе меню

Щелчок на этой области перенесет вас на страницу по умолчанию указанного приложения. В большинстве приложений просто изменяется текст рядом с логотипом, но есть возможность полностью реорганизовать блок с использованием логотипов и альтернативного текста изменением стилей CSS-приложения. Подробнее об этом мы поговорим в главе 8 «*Работа с приложениями*».

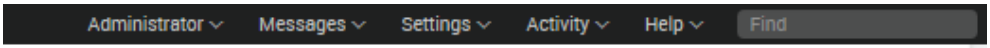

Рис. 1.9 ❖ Пункты меню

Справа в верхней полосе находится меню (рис. 1.9) со ссылками на почти всегда доступные действия.

- Первым следует имя текущего пользователя. В данном случае (рис. 1.9) это пользователь **Administrator**. В предыдущих версиях Splunk щелчок на имени пользователя позволял выбрать пункт меню **Edit Account** (Изменить учетную запись) и перейти на страницу **Your account** (Ваша учетная запись), или пункт **Logout** (Выйти). В версии 7.0 произошли небольшие изменения. Первый пункт теперь доступен под именем **Account Settings** (Настройки учетной записи) и открывает страницу с настройками, напоминающую аналогичную страницу из предыдущих версий (предшествовавших версии 7.0). Пункт **Logout** (Выйти) остался прежним и завершает текущий сеанс, вынуждая пользователя вновь ввести учетные данные.

  На рис. 1.10 показано, как выглядит страница с настройками учетной записи.

  В этой форме перечислены глобальные настройки, которые пользователь может изменить. Другие настройки определяют разрешения на объекты и параметры в ролях. (Обратите внимание, что настройки можно также изменять с использованием интерфейса командной строки или путем редактирования конфигурационных файлов Splunk.) В число настроек, доступных для изменения, входят:
  - **Full name** (Полное имя) и **Email address** (Адрес электронной почты) – предусмотрены для удобства администратора;
  - поля в разделе **Set password** (Установка пароля) позволяют изменить пароль. Это актуально, только если система Splunk настроена на использование внутреннего механизма аутентификации. Например, если система настроена на использование Windows Active Directory через LDAP (что на практике встречается очень часто), пользователи должны менять свои пароли в Windows;
  - **Global/Time zone** (Глобальные/Часовой пояс) определяет часовой пояс для зарегистрированного пользователя;

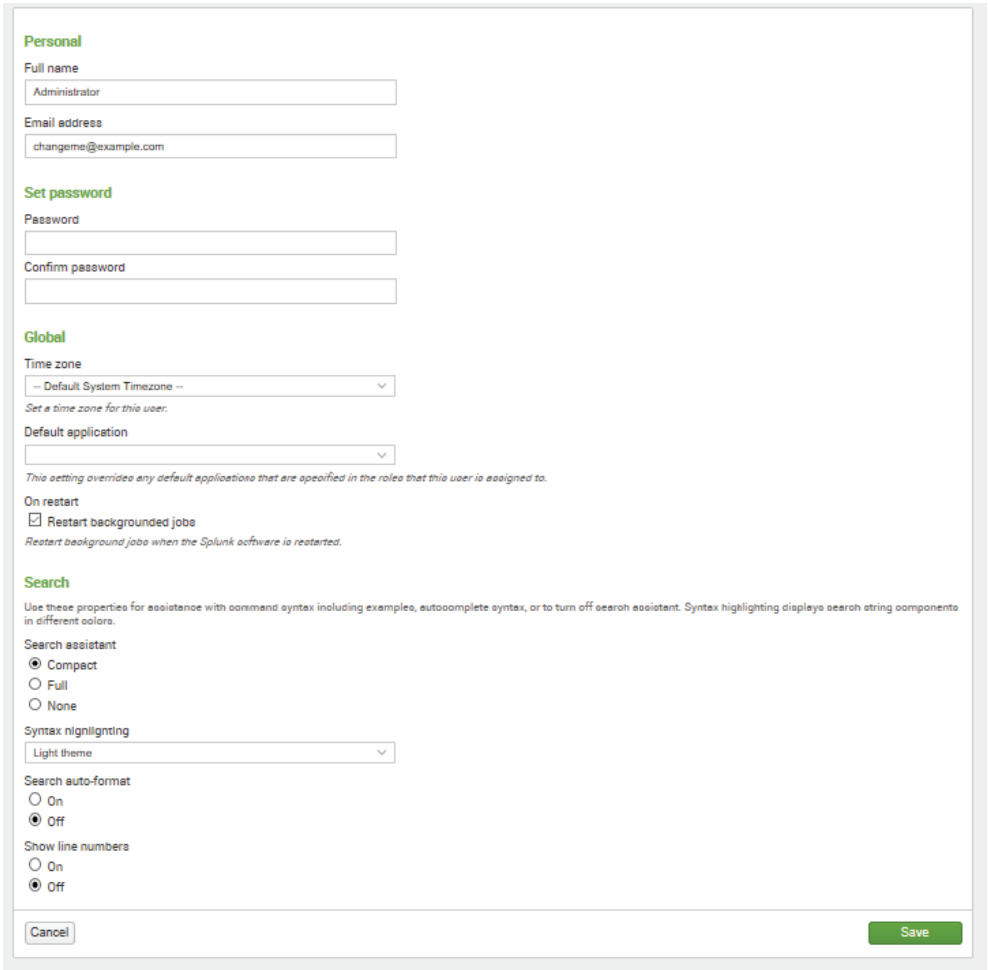

Рис. 1.10 ❖ Страница с настройками учетной записи

Настройка часового пояса используется только для отображения данных. Это очень важно для правильного представления данных при индексировании событий. Подробнее об этом мы поговорим в главе 2 «*Основы поиска*».

- **Default application** (Приложение по умолчанию) определяет приложение, которое будет запущено первым сразу после входа. На роль такого приложения большинство пользователей выбирает приложение поиска;
- **Restart backgrounded jobs** (Перезапускать фоновые задания) определяет необходимость повторного запуска незавершенных запросов при

перезапуске Splunk;

- **Search assistant** (Ассистент поиска), **Syntax highlighting** (Подсветка синтаксиса), **Search auto-format** (Автоматическое форматирование результатов поиска) и **Show line numbers** (Показывать номера строк): эти параметры используются для оказания помощи с синтаксисом команд, включая вывод примеров, автодополнение и включение/выключение ассистента поиска. Подсветка синтаксиса выделяет цветами разные компоненты строки поиска.

- Меню **Messages** (Сообщения) позволяет увидеть все системные сообщения об ошибках, ожидающие обработки. С появлением нового сообщения об ошибке, требующего вашего внимания, рядом с меню **Messages** (Сообщения) появится уведомление с числом ошибок. Вы можете щелкнуть на значке с крестиком, чтобы удалить сообщение.
- Ссылка **Settings** (Настройки) перенесет пользователя на страницу с разделами **Knowledge** (Объекты знаний), **Distributed environment** (Распределенное окружение), **System and Licensing** (Система и лицензирование), **Data** (Данные) и **Users and Authentication** (Пользователи и аутентификация), в которых перечислены ссылки на конкретные страницы с настройками (см. рис. 1.11). Здесь отображаются только ссылки на настройки, которые вы имеете право просматривать или изменять.

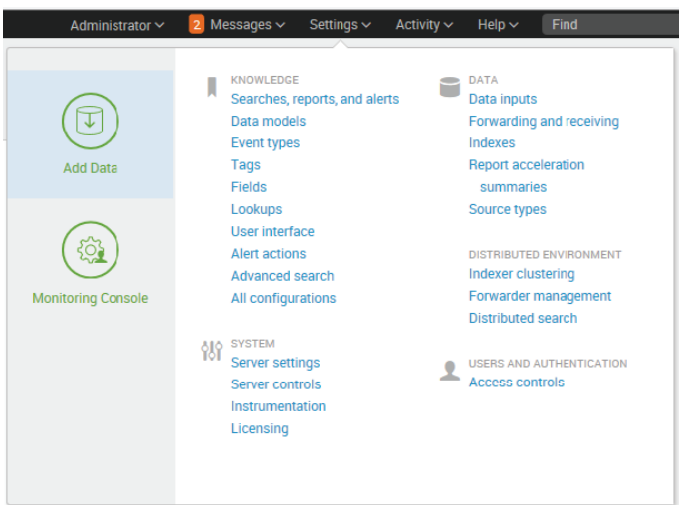

Рис. 1.11 ❖ Страница с разделами настроек

- Меню **Activity** (Деятельность) содержит пункты **Jobs** (Задания), **Triggered Alerts** (Оповещения), как показано на рис. 1.12. В предыдущих

версиях имелся также пункт **System Activity** (Системная деятельность). После выбора пункта **Jobs** (Задания) откроется окно диспетчера заданий поиска, где можно просматривать запущенные запросы поиска и управлять ими. Выбор пункта **Triggered Alerts** (Оповещения) позволяет просмотреть запланированные оповещения.

Пункт **System Activity** (Системная деятельность), открывавший дашборды с информацией о деятельности пользователей и состоянии системы, в версии 7.0 был убран из меню **Activity** (Деятельность). Теперь вся эта информация доступна в приложении поиска!

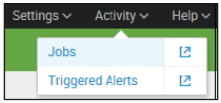

Рис. 1.12 ❖ Меню **Activity** (Деятельность)

- В меню **Help** (Справка) перечисляются ссылки на видеоруководства, **Splunk Answers** (Ответы Splunk), портал **Contact Support** (Контакты поддержки) и онлайн-документацию, как показано на рис. 1.13.

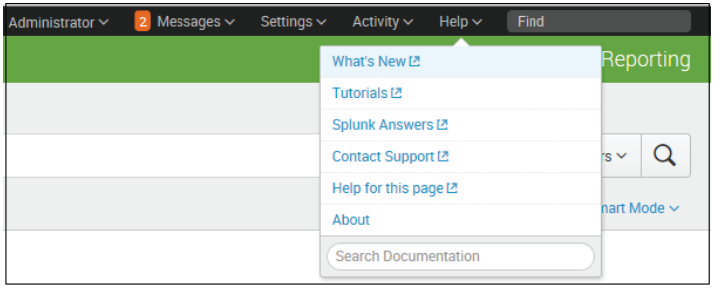

Рис. 1.13 ❖ Меню **Help** (Справка)

- Поле **Find** (Найти) можно использовать для поиска объектов в вашем экземпляре Splunk Enterprise, в том числе отчеты, дашборды, оповещения и т. д. Поиск ошибок можно выполнить в приложении **Search & Reporting** (Поиск и отчеты), щелкнув на ссылке **Open error** (Открыть ошибки).

Приложение Search & Reporting

Приложение **Search & Reporting** (Поиск и отчеты), или просто приложение поиска, – это место, где запускается большинство действий, производимых системой Splunk. Это приложение отображается как дашборд, откуда вы будете начинать поиск.

Генератор данных

Если у вас есть желание повторить у себя примеры, которые приводятся в следующих нескольких главах, установите демонстрационное приложение `ImplementingSplunkDataGenerator`, выполнив следующие шаги.

1. Загрузите архив `ImplementingSplunkDataGenerator.tar.gz`, входящий в состав пакета с примерами кода, доступного на сайте www.dmkpress.com или www.дмк.рф в разделе **Читателям – Файлы к книгам**.
2. Выберите пункт **Manage apps...** (Управление приложениями...) в меню **Apps** (Приложения).
3. Щелкните на кнопке **Install app from the file** (Установить приложение из файла).
4. Щелкните на ссылке **Choose File** (Выбрать файл), выберите файл и щелкните на кнопке **Upload** (Выгрузить).

Приложение генератора данных производит порядка 16 мегабайт выходных данных в день. Его можно остановить, выбрав пункт **Manage apps...** (Управление приложениями...) в меню **Apps** (Приложения), и тем самым прекратить генерирование данных.

Представление Summary

Внутри приложения **Search & Reporting** (Поиск и отчеты) перед пользователем отображается представление **Summary** (Сводка) с информацией о данных, поиск в которых осуществляется по умолчанию. Это важное отличие; в системах Splunk, действующих достаточно продолжительное время, не все пользователи будут выполнять поиск во всех данных. Но если вы впервые используете **Search & Reporting** (Поиск и отчеты), то увидите картину, как на рис. 1.14.

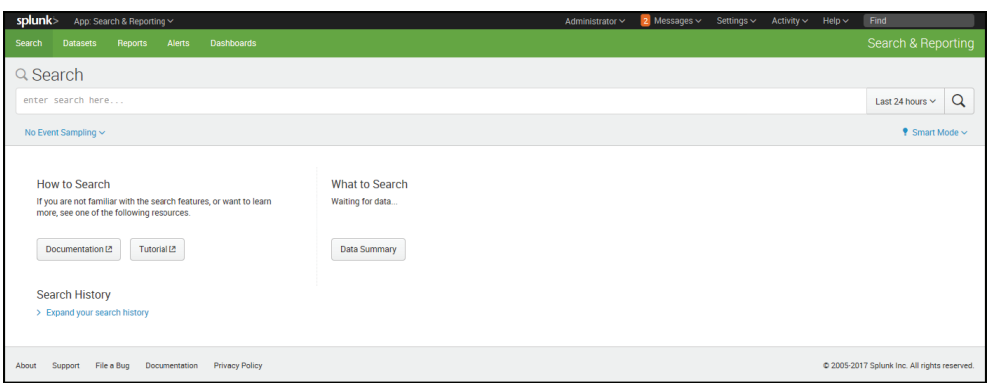

Рис. 1.14 ❖ Страница приложения **Search & Reporting**

Как показано на скриншоте (рис. 1.14), у пользователя есть доступ к документации, имеющей отношение к разделам **What to Search** (Что искать) и **How**

to Search (Как искать). После того как у вас появятся *первые индексированные данные* (эту тему мы обсудим позже), Splunk представит в разделе **What to Search** (Что искать) некоторую статистику о доступных данных.

Не забывайте, что здесь отображаются только индексы, которые текущий пользователь ищет по умолчанию; есть также другие события, которые индексируются системой Splunk, включая события, касающиеся самой системы Splunk. Мы обсудим индексы в главе 9 «*Создание продвинутых дашбордов*».

На рис. 1.15 показано, как примерно будет выглядеть раздел **What to Search** (Что искать).

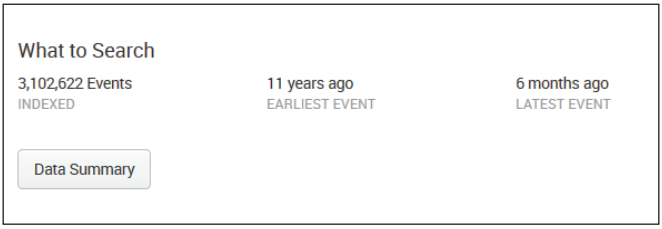

Рис. 1.15 ❖ Содержимое раздела **What to Search**

В предыдущих версиях Splunk *панели*, такие как **All indexed data** (Все индексированные данные), включали статистику по пользовательским индексированным данным. Другие панели разбивали данные на три основные группы по метаданным – **Source** (Источник), **Sourcetype** (Тип источника) и **Hosts** (Хосты). В текущей версии 7.0.0 эта информация становится доступна после щелчка на кнопке **Data Summary** (Сводные данные), в диалоге, изображенном на рис. 1.16.

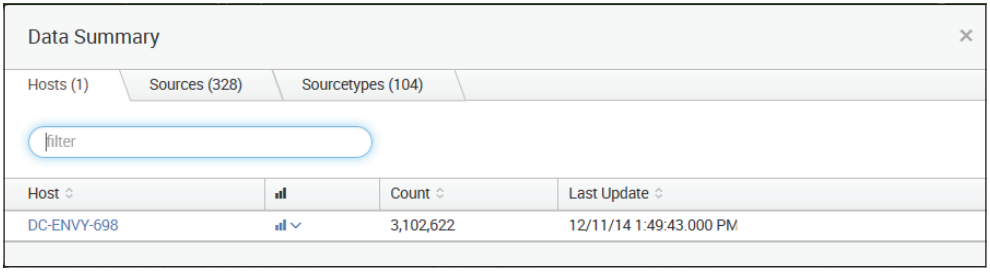

Рис. 1.16 ❖ Сводная информация о данных

В этом окне информация разбита на три вкладки – **Hosts** (Хосты), **Sources** (Источники) и **Sourcetypes** (Типы источников).

- Хост определяется именем хоста, где возникло событие. В большинстве случаев в поле `host` (хост) записывается имя компьютера, откуда полу-

чены данные. Иногда имя хоста неизвестно, и тогда значение для этого поля можно настроить произвольно.

- Под источником в Splunk понимается уникальный путь или имя. В больших системах может иметься по нескольку тысяч компьютеров, посылающих данные, но все данные с одинаковыми путями будут считаться как принадлежащие одному источнику. Если источником данных является не файл, это поле может иметь произвольное значение. Например, имя сценария или номер сетевого порта.
- Тип источника – это произвольное значение для классификации события. В системе может иметься большое количество разных источников среди множества хостов, имеющих один и тот же тип источника. Например, на источники `/var/log/access.2012-03-01.log` и `/var/log/access.2012-03-02.log` на хостах `fred` и `wilma` можно ссылаться по типу источника как на журналы или под любым другим названием типа источника.

А теперь продолжим и рассмотрим виджеты, находящиеся непосредственно под названием приложения. Первый виджет – полоса навигации, изображенная на рис. 1.17.

Рис. 1.17 ❖ Полоса навигации

Как правило, элементы с треугольником, направленным вершиной вниз, в Splunk являются раскрывающимися списками, или меню, а элементы без такого треугольника – обычными ссылками.

Подробнее о настройке полосы навигации мы поговорим в главе 8 «*Работа с приложениями*».

Ниже находится поле **Search** (Поиск), как показано на рис. 1.18. Именно здесь начинает твориться волшебство. Подробнее об этом поле рассказывается ниже.

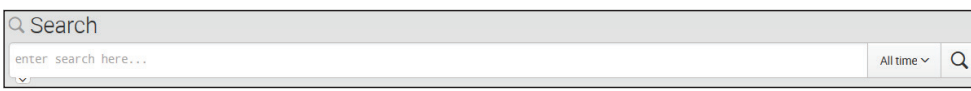

Рис. 1.18 ❖ Поле поиска

Поиск

Вот мы и добрались до поиска. Именно здесь сосредоточена вся мощь Splunk.

В качестве первого примера попробуем выполнить поиск (без учета регистра символов) по слову `error`. Щелкните в поле поиска, введите слово `error` и затем нажмите клавишу **Enter** или щелкните на значке с изображением лупы справа от поля, как показано на рис. 1.19.

Рис. 1.19 ❖ Поле поиска **Search**

После запуска процедуры поиска откроется страница с результатами (которая мало изменилась в версии 7.0), как показано на рис. 1.20.

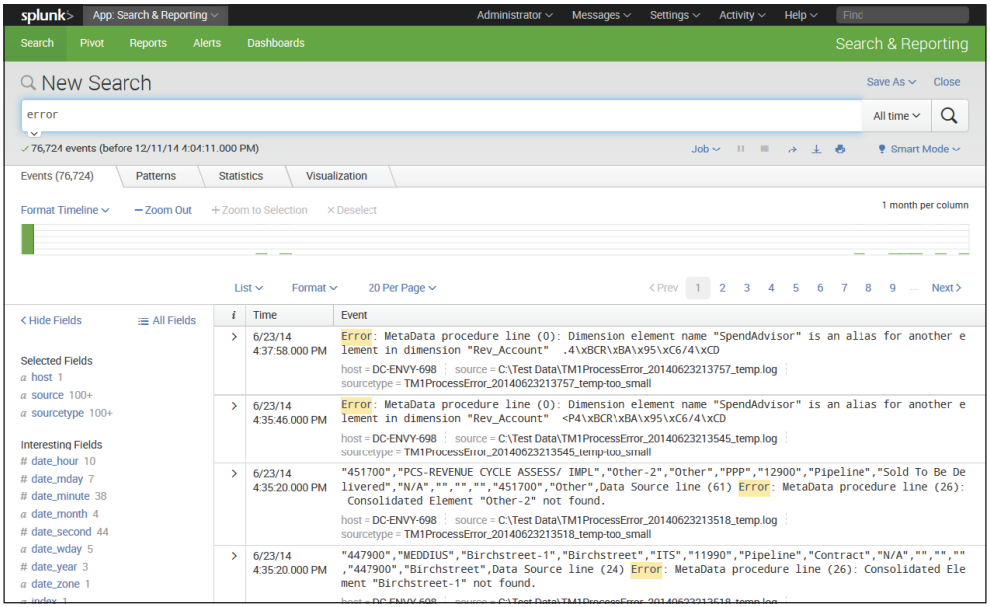

Рис. 1.20 ❖ Страница с результатами поиска

Обратите внимание, что мы запустили поиск по данным за все время (по умолчанию); чтобы изменить интервал времени для поиска, можно использовать виджет выбора времени.

Однако из-за того, что мы экспериментируем на случайно сгенерированных данных, не все запросы будут действовать, как ожидается, и вам может потребоваться изменить их.

Описание этапов загрузки наборов данных вы найдете в предыдущем разделе «Генератор данных».

Как изменить интервал времени для поиска, вы узнаете в разделе «Использование виджета выбора времени».

Действия

Рассмотрим элементы на этой странице. Под поисковой строкой **Search** (Поиск) выводятся счетчик событий, значки действий и меню (рис. 1.21).

Рис. 1.21 ❖ Информация под полем **Search** (Поиск)

Вот какие сведения выводятся под поисковой строкой (слева направо).

- **Количество событий**, найденных в процессе поиска. Технически это число может не соответствовать количеству результатов, прочитанных с диска, в зависимости от параметров поиска. Кроме того, если в запросе используются команды, это число может отличаться от числа событий в списке ниже.
- **Меню Job** (Задание): открывает окно инспектора заданий поиска, в котором приводится очень подробная информация о запросе.
- **Кнопка «Пауза»**: приостанавливает текущий поиск событий, но не удаляет результаты. Это может пригодиться, когда нужно просмотреть уже полученные результаты, чтобы определить – стоит ли продолжать поиск, который может занять продолжительное время.
- **Кнопка «Стоп»**: останавливает выполнение запроса, но сохраняет на странице уже полученные результаты. Это может пригодиться, когда получен достаточный объем информации и можно переходить к их исследованию.
- **Кнопка «Поделиться»**: растягивает временной интервал поиска до семи суток и открывает доступ к результатам для чтения всем пользователям.
- **Кнопка «Печать»**: форматирует страницу для печати и запускает функцию печати в браузере.
- **Кнопка «Экспорт»**: экспортирует результаты, предлагая указать количество экспортируемых результатов и формат – CSV, простой текст, XML или JSON (JavaScript Object Notation – форма записи объектов JavaScript).
- **Меню Smart mode (Интеллектуальный режим)**: управляет режимом поиска. Вы можете использовать это меню для ускорения поиска, ограничивая объем возвращаемых данных и количество полей, которые Splunk будет извлекать из данных (**Fast mode** (Быстрый режим)). Также можно выбрать **Verbose mode** (Подробный режим), чтобы получить максимальный объем информации о событиях. В режиме **Smart mode** (Интеллектуальный режим), который используется по умолчанию, поведение поиска определяется его типом.

Шкала времени

Теперь перейдем к шкале времени, отображаемой под полосой с кнопками действий (рис. 1.22).

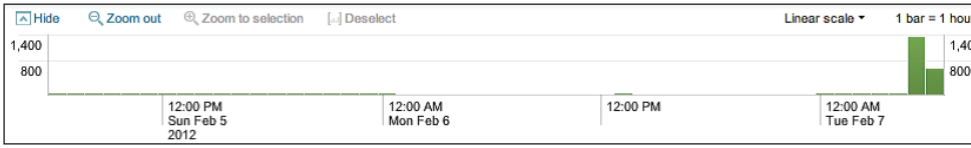

Рис. 1.22 ❖ Шкала времени

Шкала времени не только позволяет быстро оценить распределение событий в заданном интервале, но и является ценным инструментом, помогающим выбрать подходящий интервал. Если навести указатель мыши на шкалу времени, появится всплывающая подсказка с количеством событий в данном промежутке. Щелчок на шкале выбирает события за конкретный отрезок времени.

Если нажать левую кнопку мыши и потянуть указатель, выделится несколько отрезков времени, как показано на рис. 1.23.

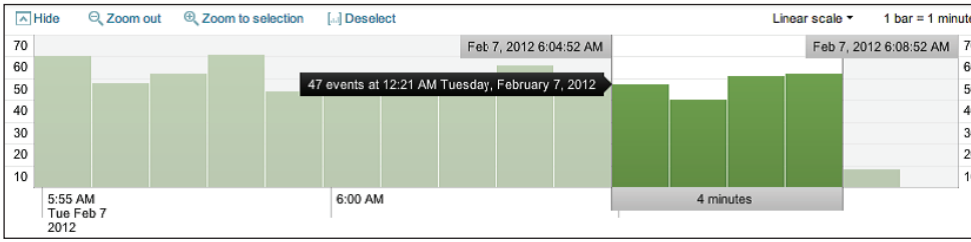

Рис. 1.23 ❖ Выделение нескольких отрезков времени

Выделив интервал, можно щелкнуть на ссылке **Zoom to selection** (Увеличить масштаб выделения), чтобы изменить интервал и повторить поиск для данного интервала. Повторяя этот процесс, можно добраться до конкретных событий.

Deselect (Убрать выделение) снова возвращает отображение всех событий в интервале времени, установленном в виджете выбора времени.

Zoom out (Уменьшить масштаб) увеличивает интервал времени, отображаемый в окне.

Виджет выбора полей

Слева от результатов поиска находится *виджет выбора полей* (рис. 1.24). Это отличный инструмент для выявления закономерностей и фильтрации результатов поиска.

Рис. 1.24 ❖ Виджет выбора полей

Поля

Виджет выбора полей содержит два списка:

- **Selected Fields** (Выбранные поля) перечисляет поля, значения которых в данный момент отображаются в результатах поиска;
- **Interesting Fields** (Интересные поля) перечисляет поля, которые Splunk извлек для вас.

Над списками полей имеются две ссылки: **Hide Fields** (Скрыть поля) и **All Fields** (Все поля):

- **Hide Fields** (Скрыть поля) скрывает область со списком полей;
- **All Fields** (Все поля): открывает окно **Selected Fields** (Выбранные поля) со списком полей для выбора (рис. 1.25).