RRC

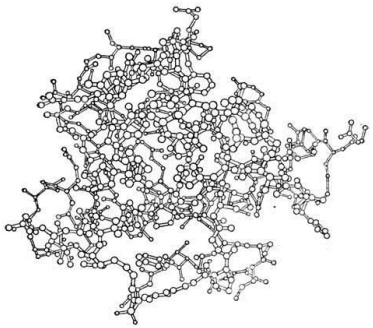
Гибкое решение для анализа данных и мониторинга

Pete Kuzeev, Security Presale Engineer, RRC Moscow

Основные возможности продукта, области применения, детали внедрения и доработки

RRC

Обзор продукта



SPLUNK - это система обработки данных

RRC

Управление приложениями

Поиск и устранение проблем

Получение данных о несовместимости продуктов

Оценка воздействия одного продукта на другой

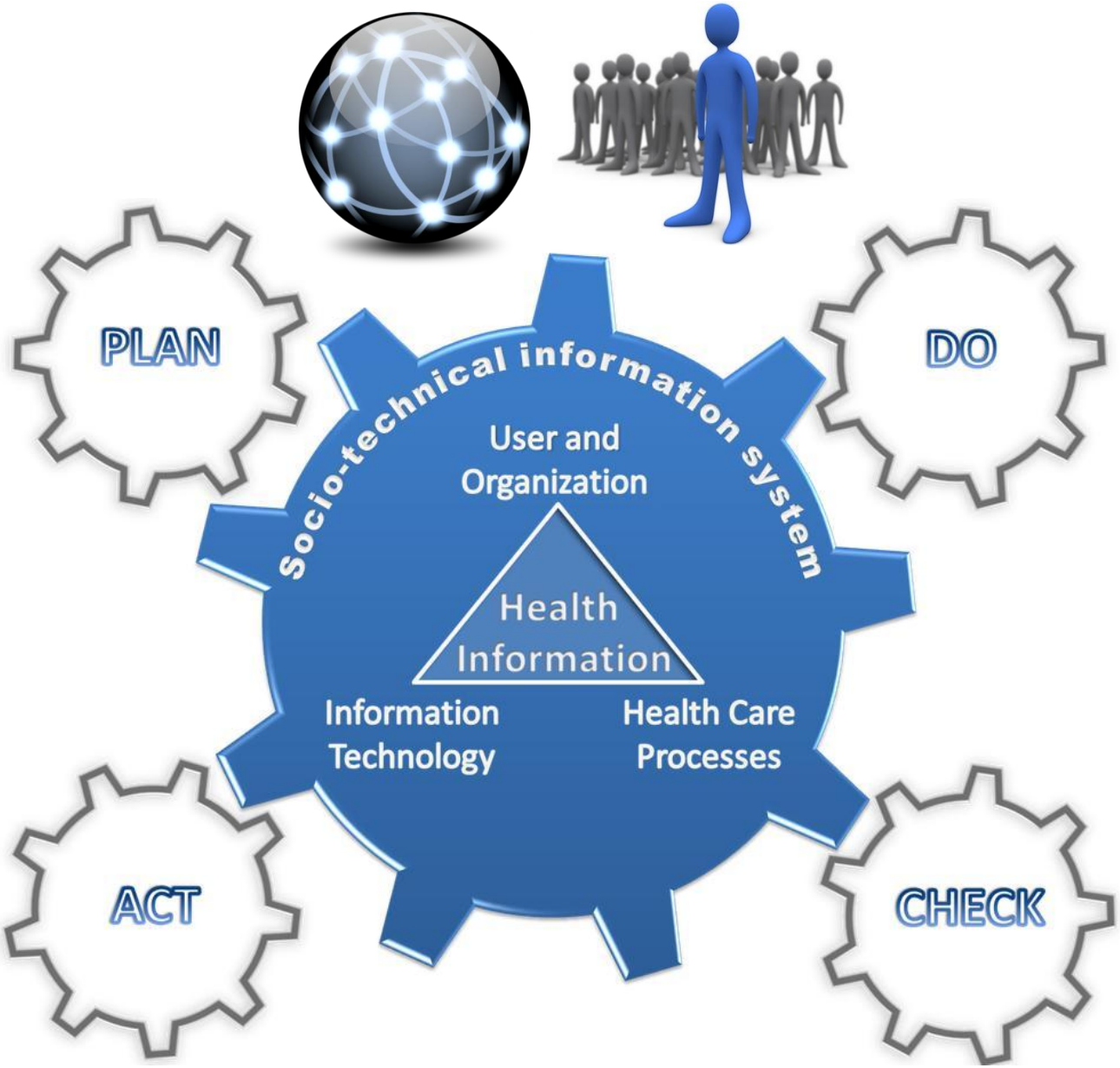
RRC

Управление ИТ инфраструктурой

Масштабируемость от небольшой сети до сети ЦОД

Мониторинг в режиме реального времени

Аналитика для решения скрытых проблем

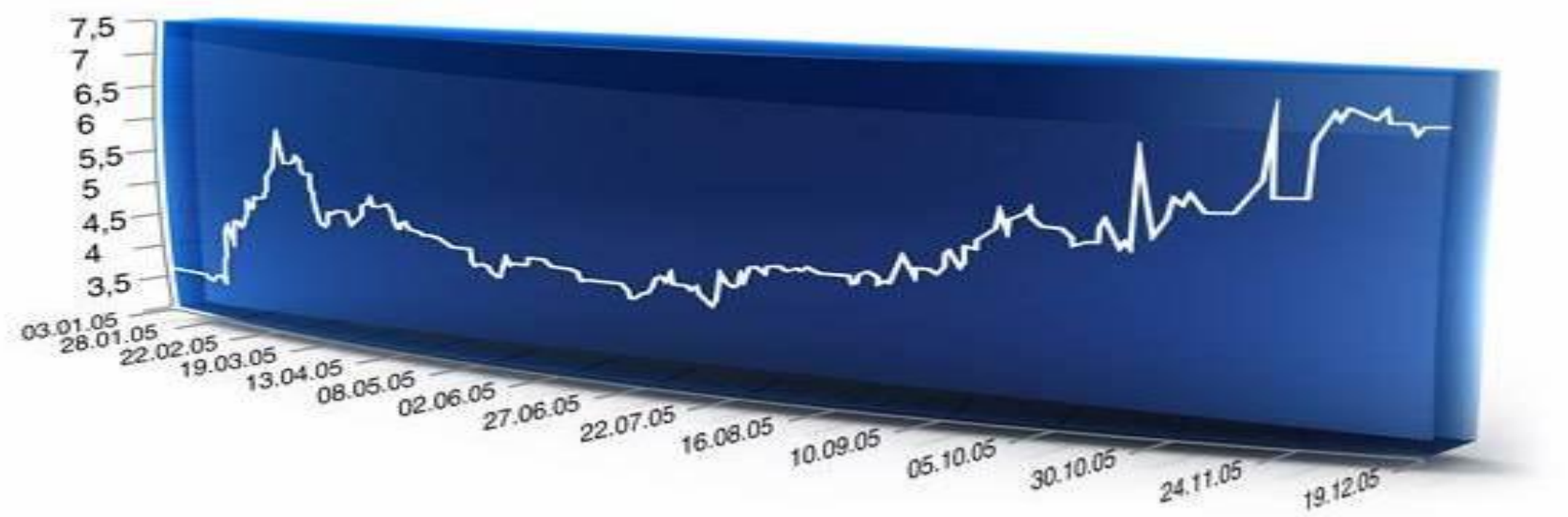


RRC

Безопасность и соответствие стандартам

RRC

Аналитика в бизнес процессах



Автоматизация

Торговые роботы

Аналитика

Анализ трендов

Пронозирование

Прогноз роста

Облачные технологии

next!

Контроль работы облачных сервисов

Анализ использования компонентов

Оптимизация используемых ресурсов

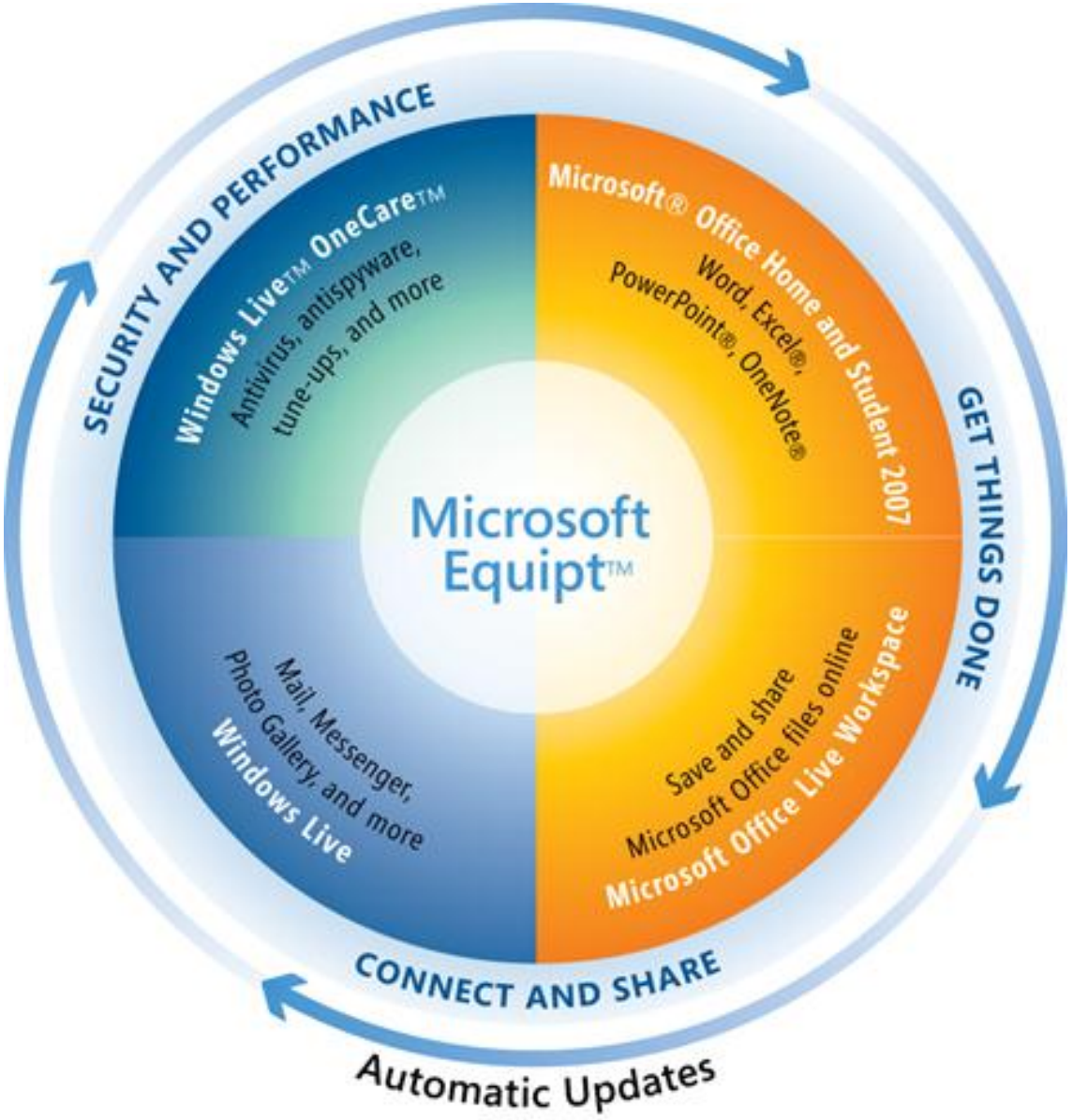
RRC

Решения для ПО Microsoft

Поддержка широкого спектра ПО

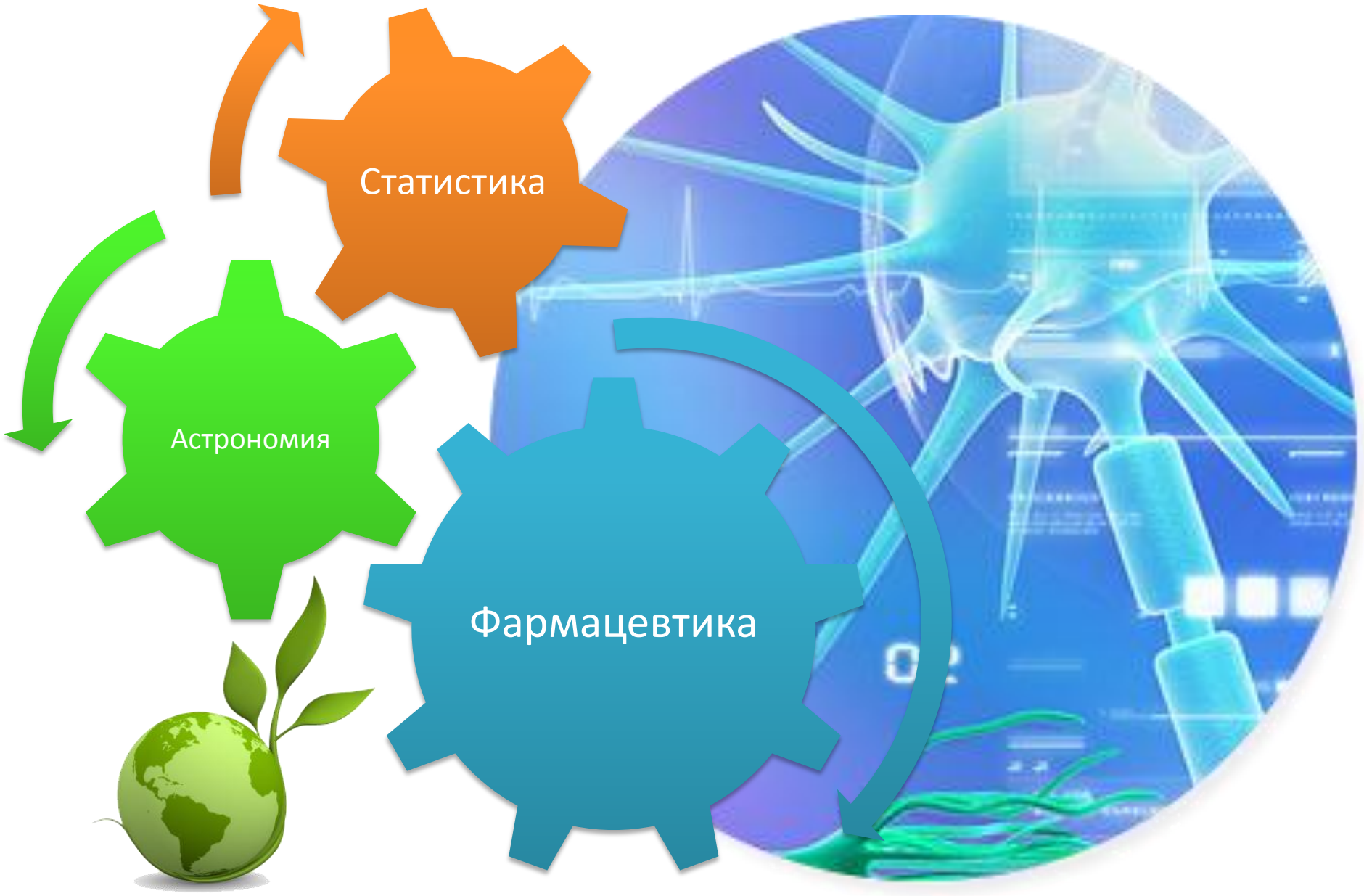
Возможность работы с логами в кириллице

Варианты использование в качестве Help Desk



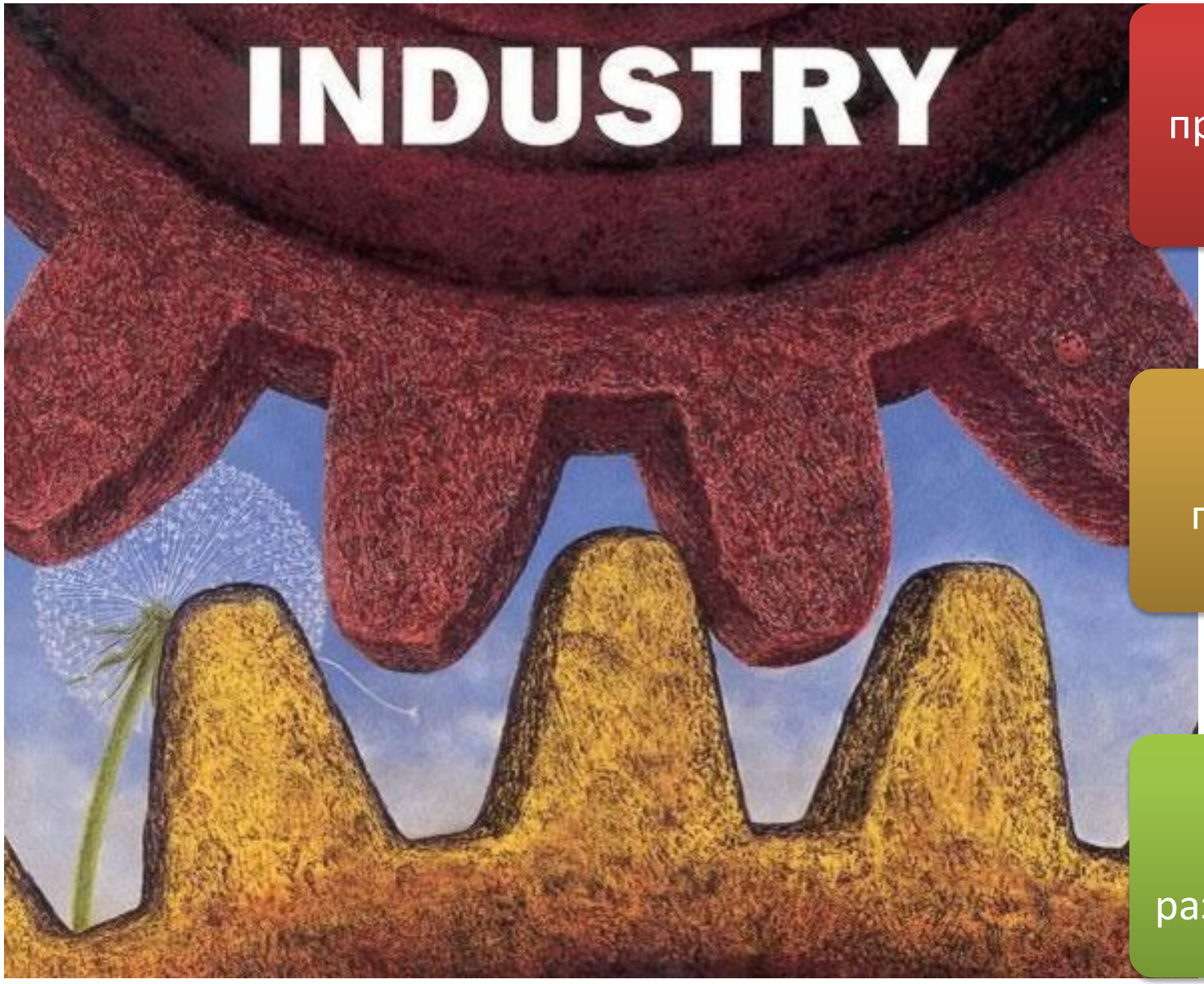
RRC

Данные научных исследований



RRC

Контроль промышленных линий



Контроль промышленных линий

Мониторинг производства

Обработка данных от разных вендоров

RRC

Оптимизация сетевой инфраструктуры

Поиск узких мест

Оптимизация сервисов

Оценка решений

Планирование развития

Общий анализ

RRC

Независимый финансовый аудит

- Деятельность компании
- Работа ритейловых сетей
- Качество автоматизации

RRC

Борьба с мошенничеством в банковской сфере

RRC Анализ работы коммерческих интернет ресурсов

Анализ действий пользователя

Статистика по покупкам

Статистика по переходам

RRC

Примеры данных

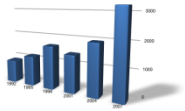
Логи любых устройств или приложений в формате plaintext

Данные полученные по сети – SNMP, Syslog

Данные полученные приложением в любом формате

Информация полученная с помощью Web-login

Информация полученная от коннекторов или агентов



Архивы систем мониторинга – Cisco MARS

Любые любых логов, даже без поля времени и даты

Результаты работы скрипта

RRC

Архитектура приложения

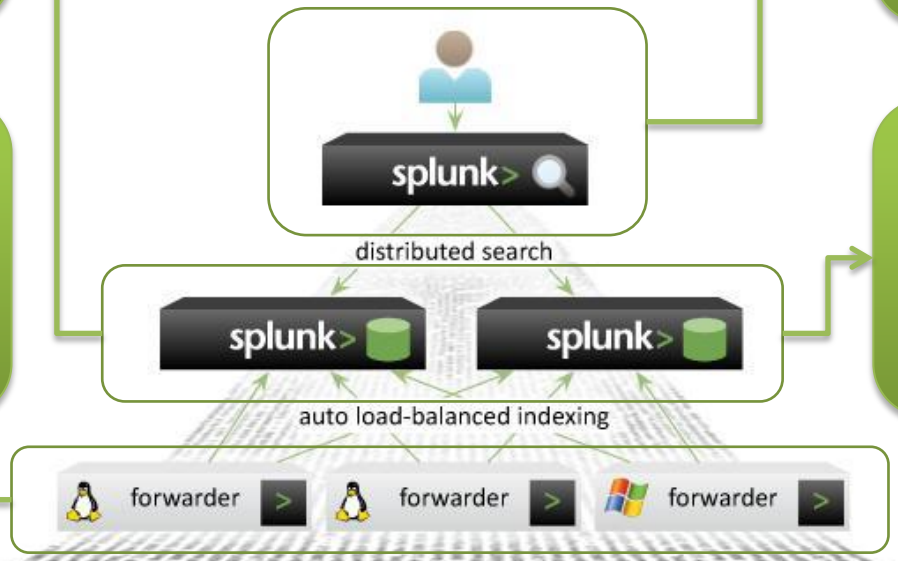
Сервера индексирования, хранения поступивших данных

Кластеризация, работа с токенами

Сервер управления, выполнения запросов, доставки приложений

Коннекторы, форвардеры, агенты

Приложения, скрипты, Syslog, Web-login, SNMP

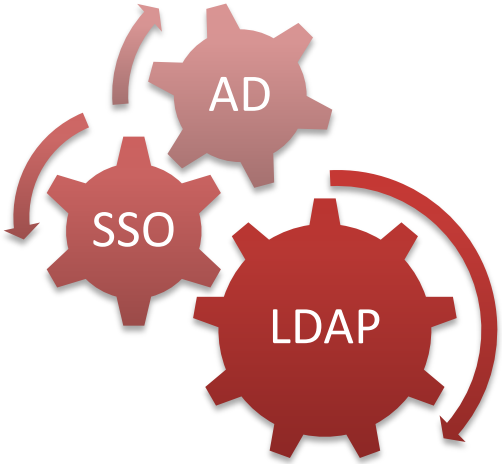


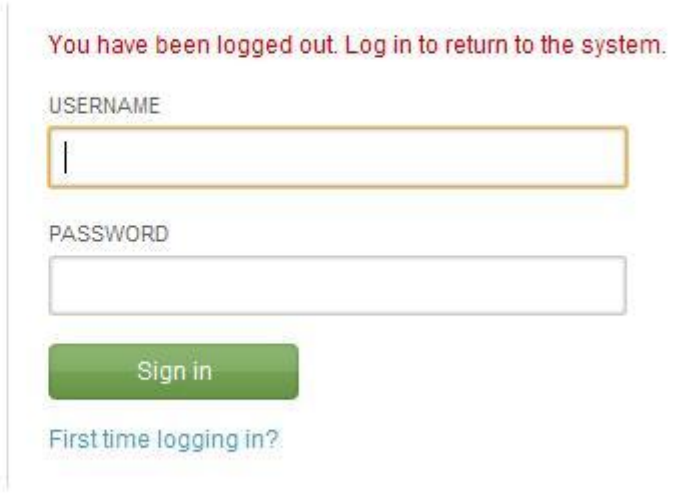
RRC

Установка

Установка → Поддержка любой ОС → Видео по установке → Администратор любого уровня

splunk>

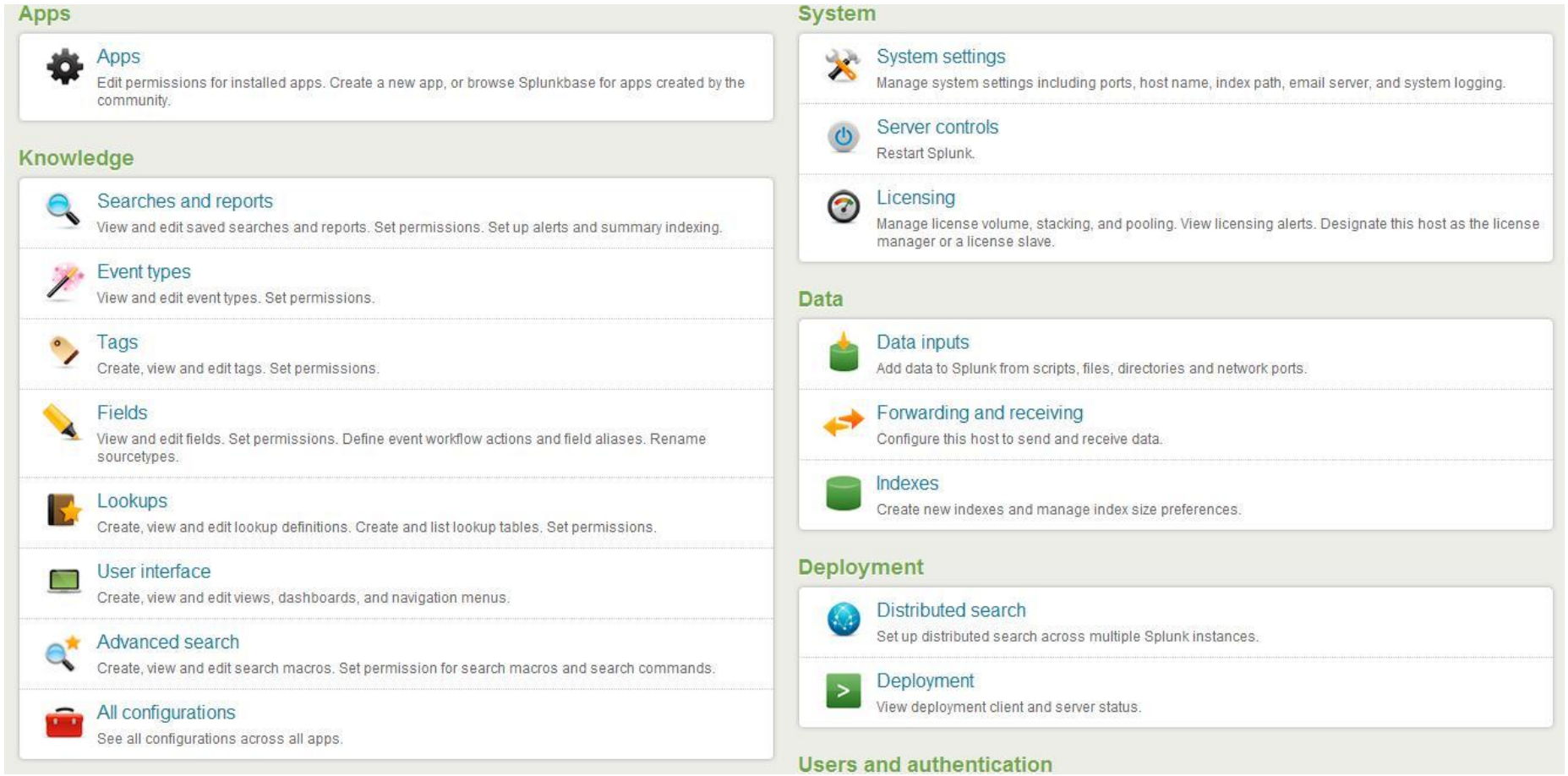




RRC

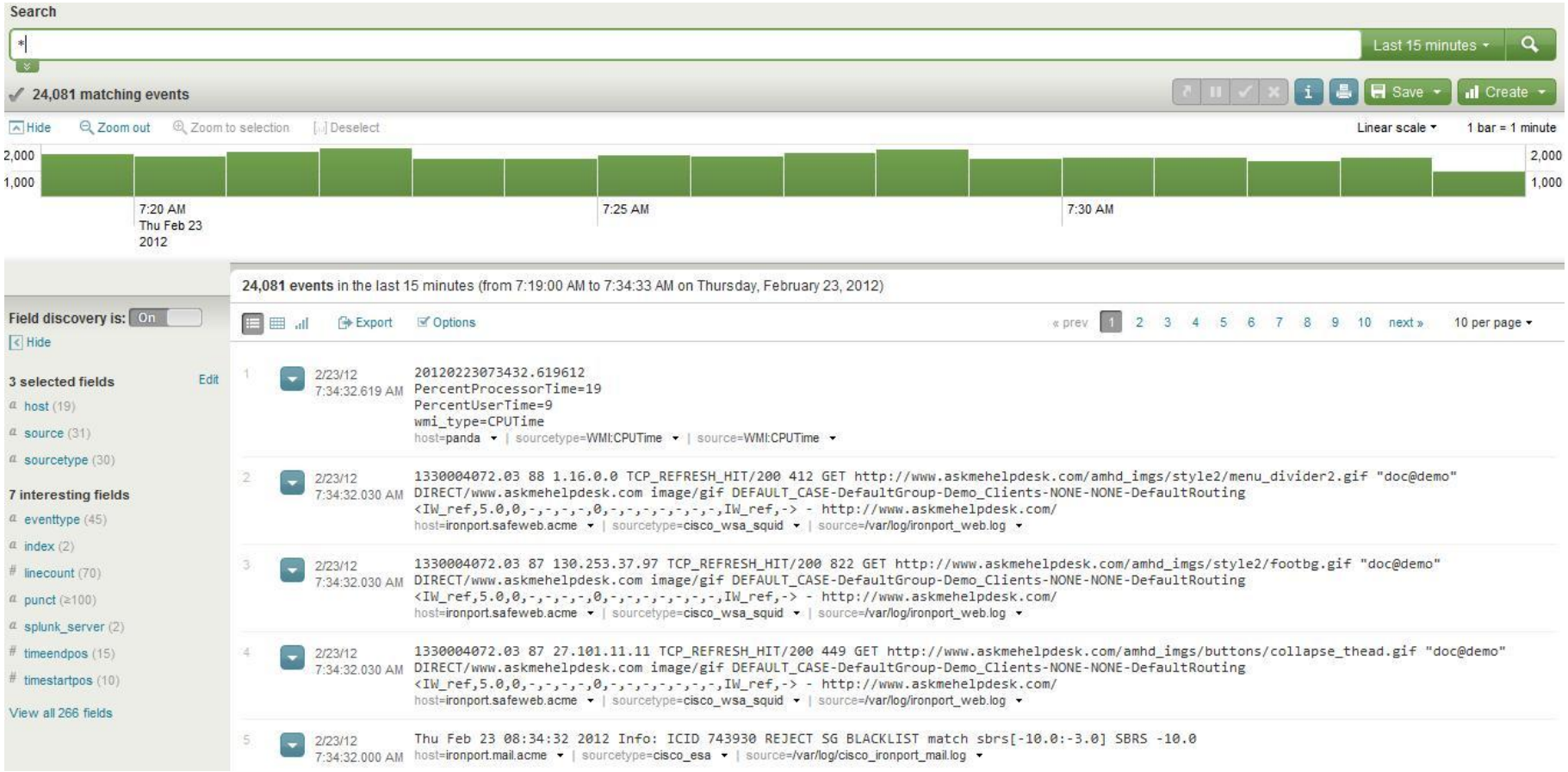
Настройка

Настройка → Просто указать путь к логам → Настроить ожидание данных на порту → Добавить приложение через Web



Поиск

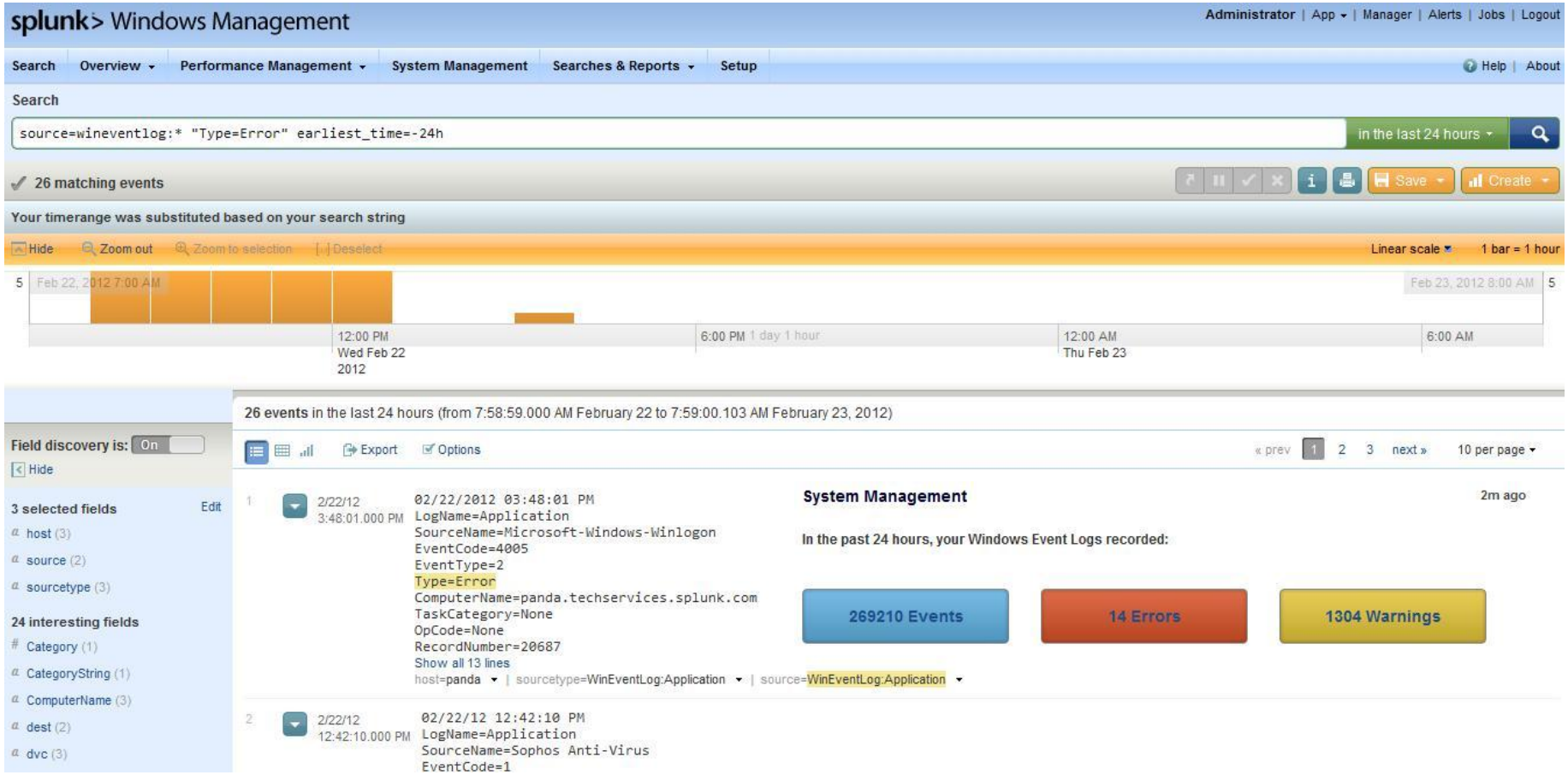
Поиск → Простота выполнения запроса → Корреляция по времени → Сохранение запросов



RRC

Оповещения

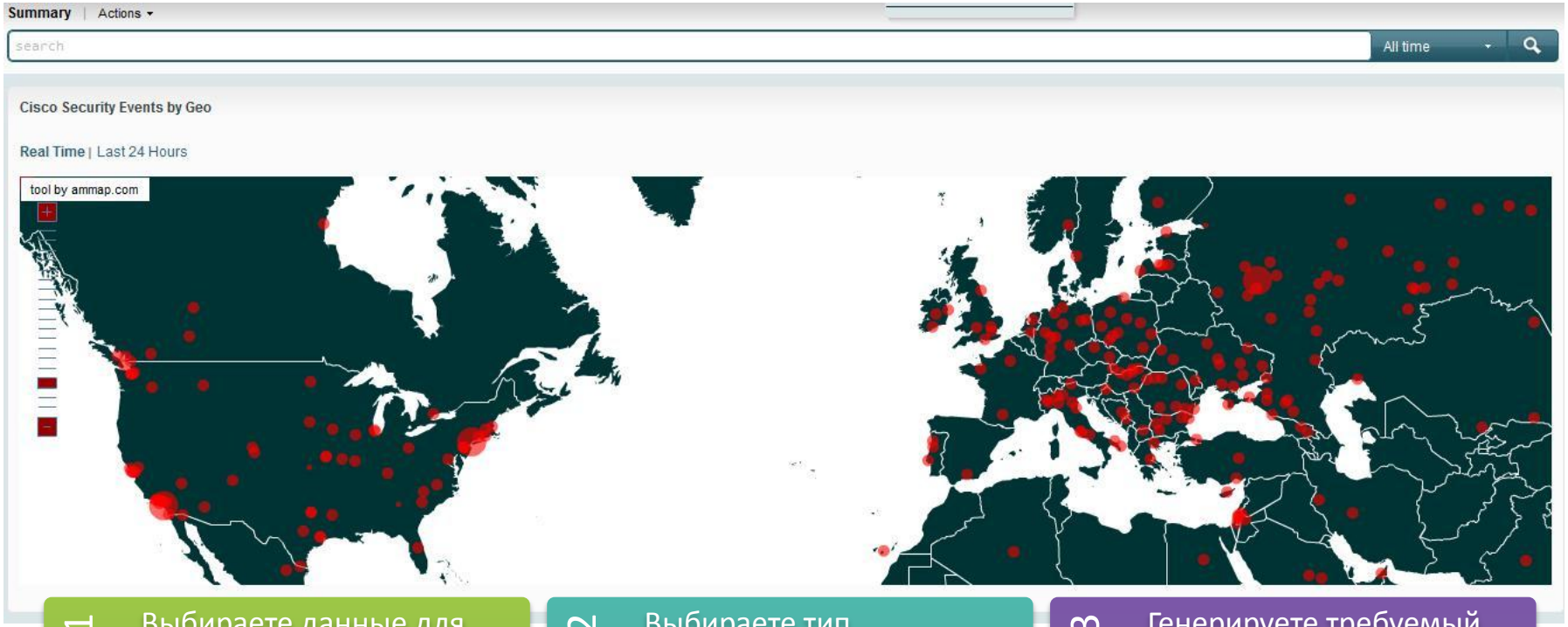
Оповещения → Из сохранённых запросов → Отображение на рабочем столе → Отправка уведомлений



RRC

Отчёты

Отчёты → Рассылка pdf, csv, RSS → Простота генерации → Любое приложение



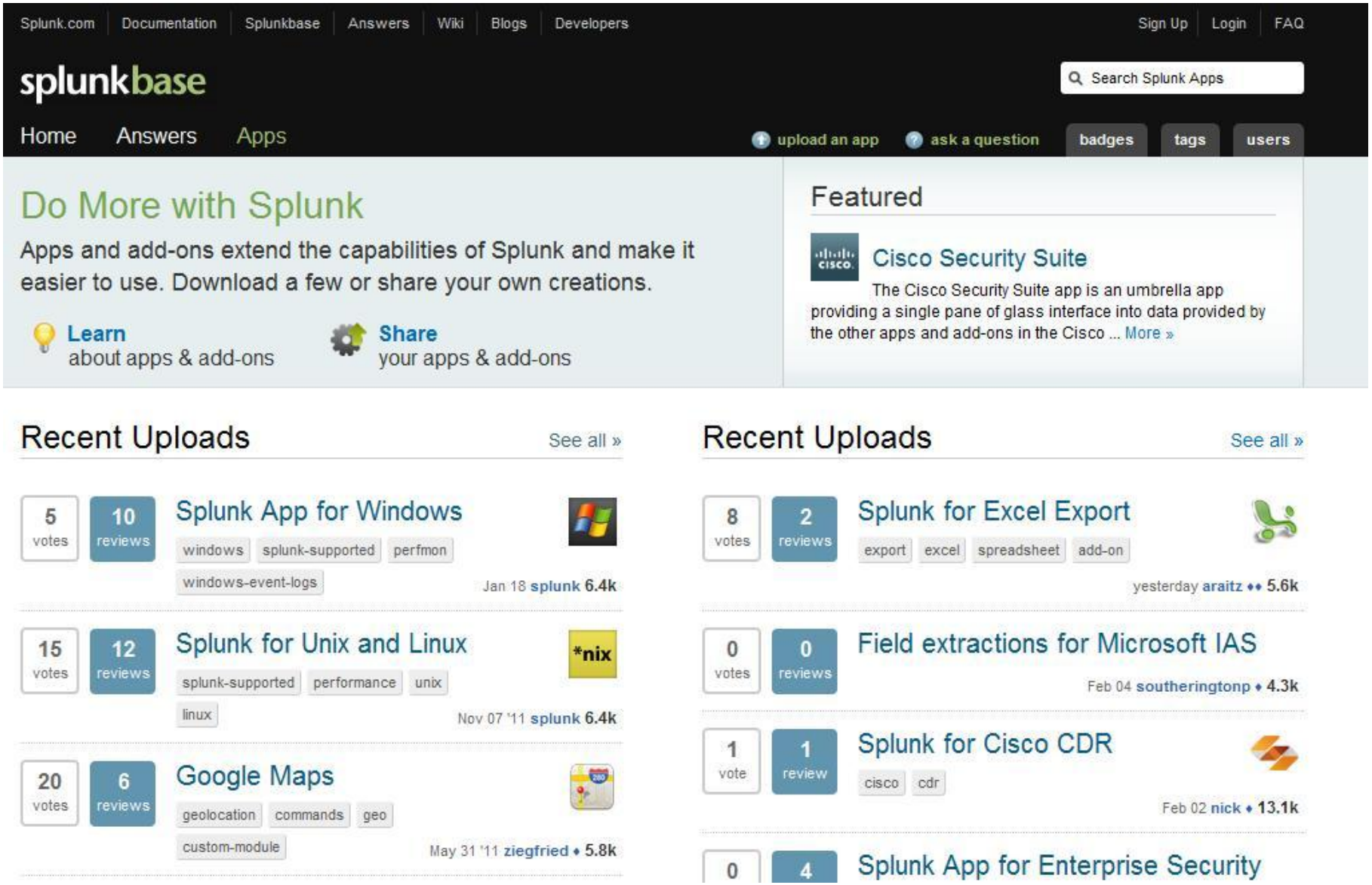
Шаг 1 Выбираете данные для аналитики

Шаг 2 Выбираете тип представления запросов – график, таблица

Шаг 3 Генерируете требуемый вариант отчёта

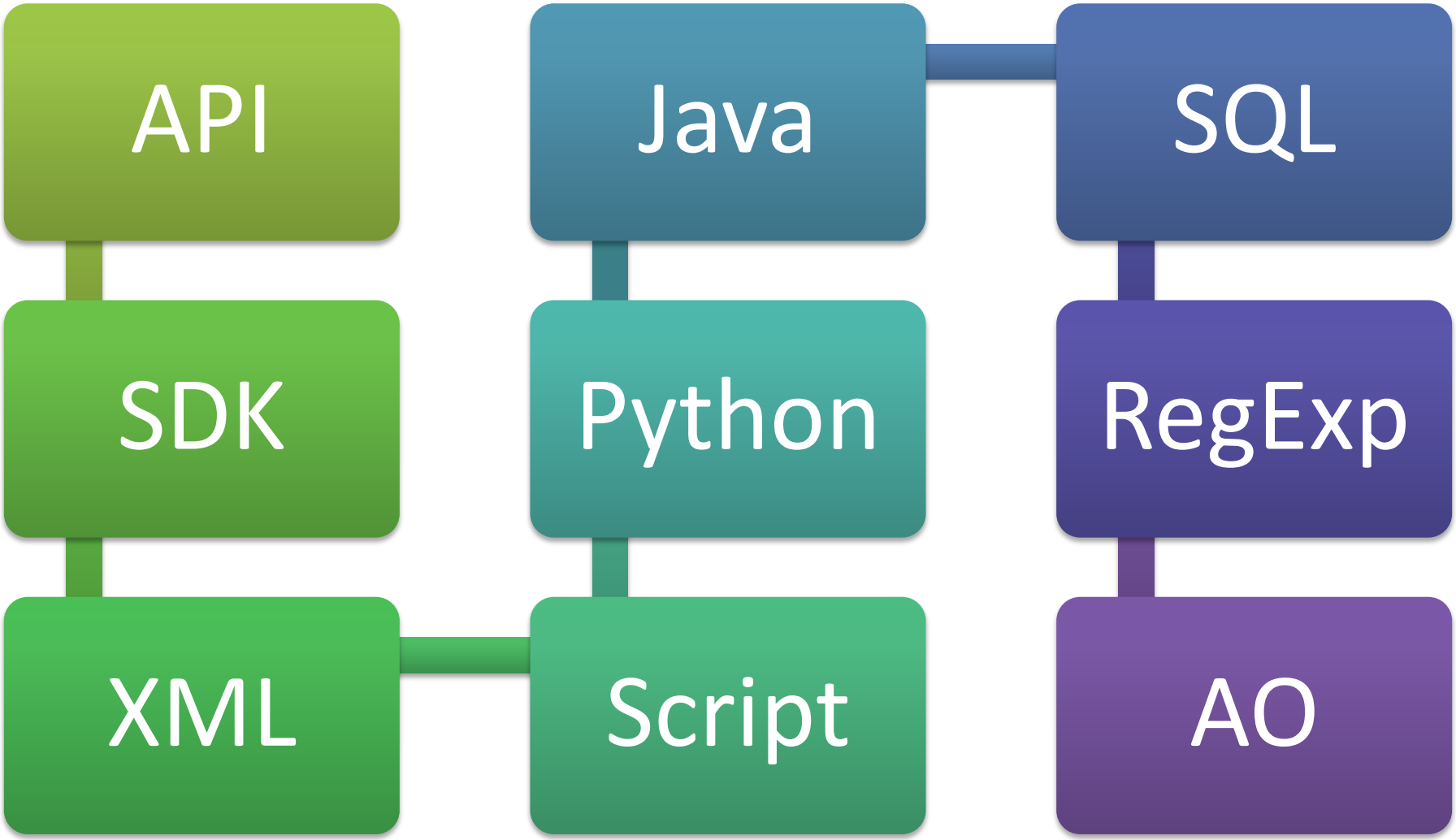
RRC

Использование готовых приложений



RRC

Разработка приложений

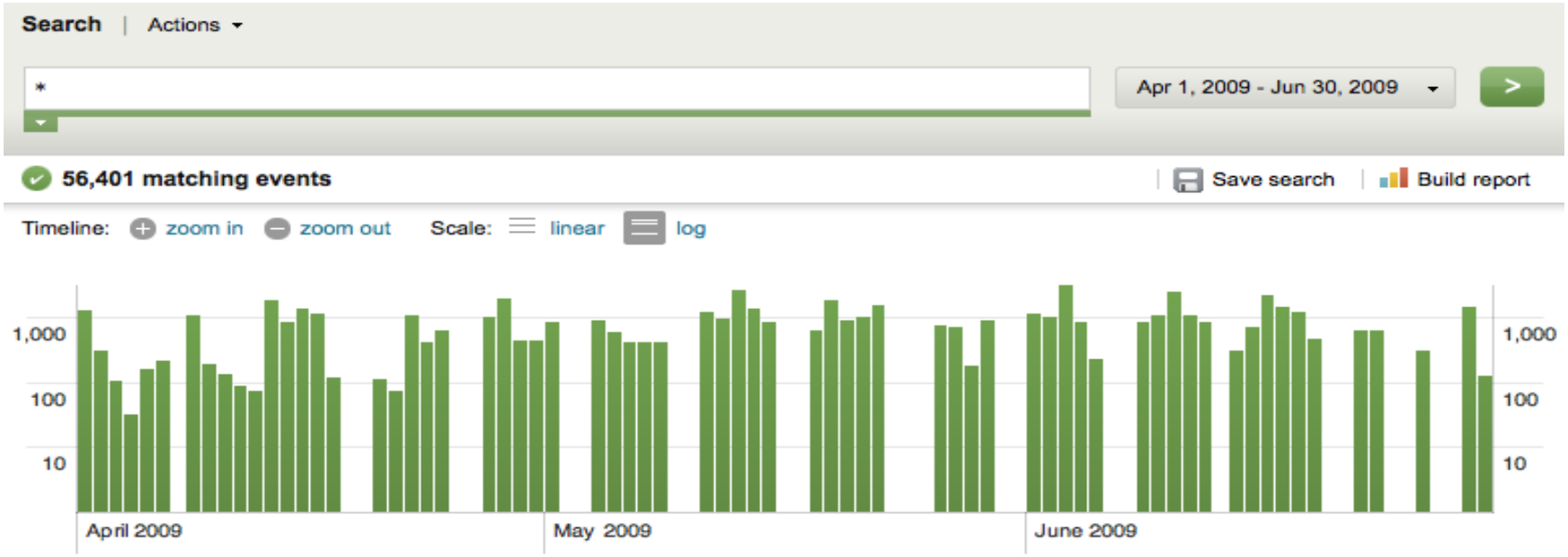


RRC

Дополнительные возможности

- Для удобства анализа и временной корреляции существует timeline, позволяющий связать несколько событий из разных источников для выявления возникшей проблемы и оценки её масштабов

Time Line



- Позволяет пользователям, создавать требуемые выборки данных полей из логов без специальных знаний

Конструктор RegExp

RRC

Документация

Splunk

Документация, база знаний

Splunk Storm

Сервис анализа работы облачных приложений

Splunk App for Enterprise Security

Пакет Информационной Безопасности

Splunk for WebSphere Application Server

Анализ данных WebSphere

Splunk App for Web Intelligence

Приложение для изучения веб-трафика

Splunk MySQL Connector

MySQL коннектор

Splunk App for Microsoft Exchange

Анализатор MS Exchange

Splunk App for Unix and Linux

Набор аналитики для Unix и Linux

Версия сайта на русском языке - http://ru.splunk.com

Лицензирование

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	•	•
Real-time and historical search	•	•
Reporting	•	•
Knowledge mapping	•	•
Dashboards	•	•
Monitoring and alerting		•
Distributed search		•
Data forwarding and receiving	•	•
Role-based access controls		•
Single sign-on		•
Developer APIs	•	•
Community Apps	•	•
Enterprise Apps		•
Standard support	•	
Enterprise support		•

Splunk сжимает поступившие данные до 10ти раз

Учитывается только объём индексов по заданным полям

Пробная лицензия на 500 Мб/день действует 60 дней

Не включает распределённый поиск, мониторинг и оповещения

Ограничена локальным использованием и не поддерживает работу ряда приложений

Вопросы

Графический интерфейс более не привязан к Flash, используется HTML 5

Создание рабочих столов на лету

Увеличение количества одновременных пользователей в 10 раз

Процесс управления большими объёмами данных стал более лёгким

Увеличение скорости поиска в 10 раз

Splunk 4.3

Спасибо за внимание!

pkuzeev@rrc.ru
Skype – zerottl
+7 985 9994824