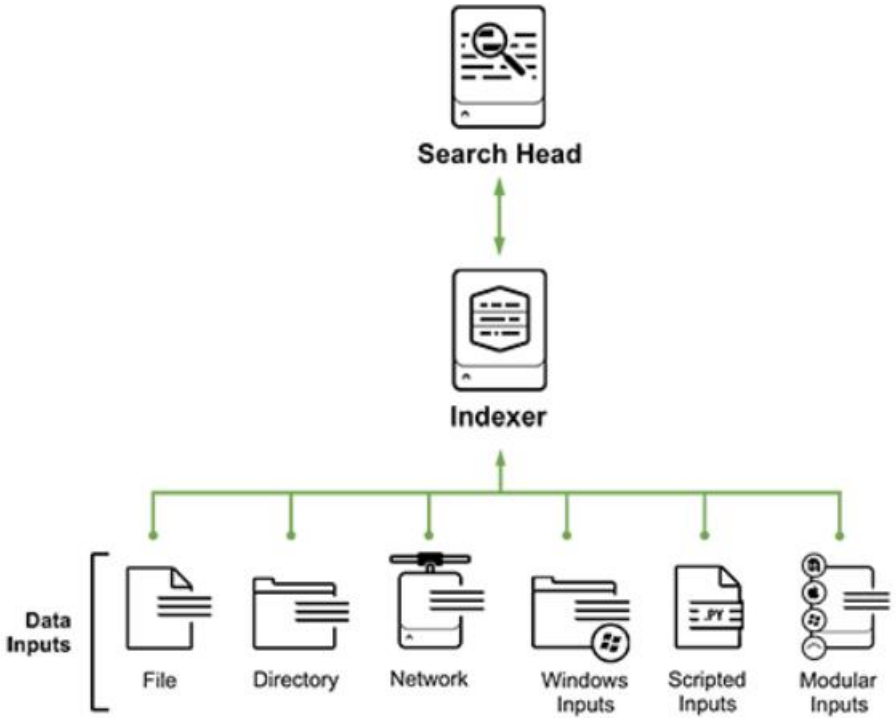
C311. Splunk — SPL запросы и визуализация логов

Загрузка данных в систему



В системе можно выделить 5 основных источников сбора логов (это не полный список):

Files and Directories: Splunk может разово забирать или мониторить конкретный файл или директорию с файлами, причем самостоятельно следит за изменением

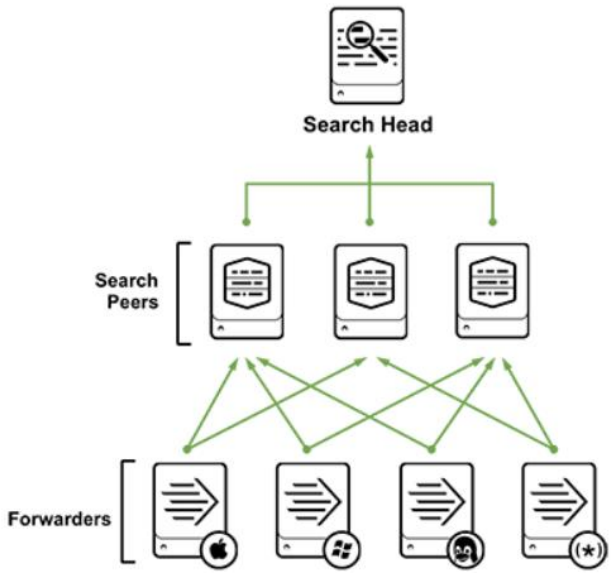
Network events: данные, поступающие с сетевых портов (syslog например)

Windows sources: журналы событий (event log) Windows, события AD

Scripted Inputs: данные собираемые посредством скриптов

Modular Inputs: забор данных из специфических платформ, систем и приложений

В данной работе, для наглядности мы будем использовать наиболее простой метод. Мы просто загрузим тестовый файл в Splunk с локального компьютера. Понятно, что в истории с Enterprise использованием так никто не делает, и как раз используются варианты описанные выше вместе с агентами (forwarder), стоящими на целевых системах, и тогда инфраструктура выглядит следующим образом:

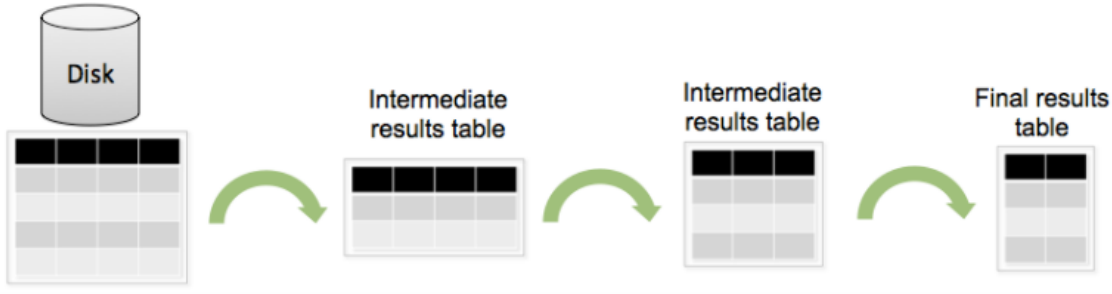


Но в нашем учебном примере, нам будет достаточно одного скаченного на локальный компьютер бесплатного Splunk Enterprise Free.
Теперь когда Вы скачали данные и установили Splunk их надо загрузить в него. На самом деле это достаточно просто (инструкция), потому что данные заранее подготовлены. **Важно**! Не нужно разархивировать архив.

SPL запросы

Ключевые особенности языка SPL:

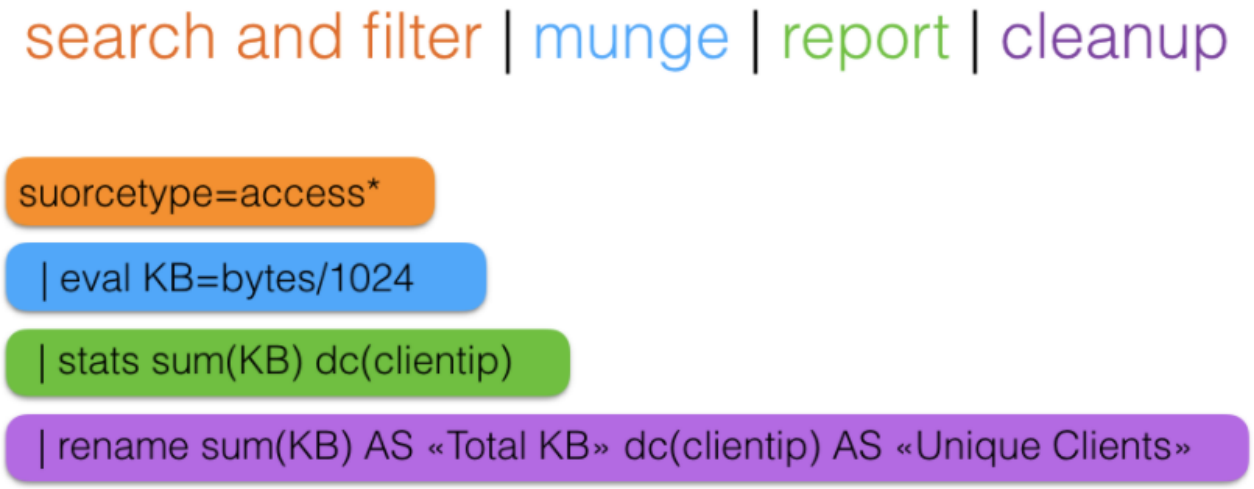
- 140+ поисковых команд
- Синтаксис похож на Unix pipeline и SQL и оптимизирован на **данные с временной отметкой**
- SPL позволяет искать, фильтровать, модифицировать, обогащать, совмещать и удалять
- SPL включает функционал **машинного обучения** и **поиска аномалий**



Структура SPL:

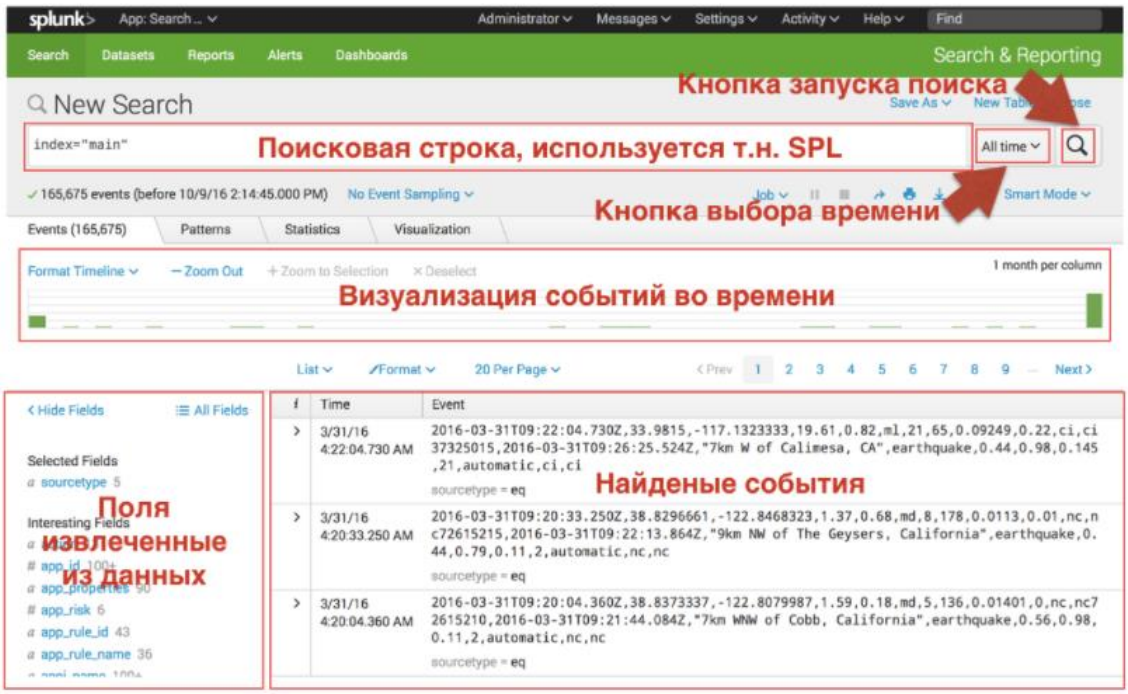
Стандартно SPL запрос можно разделить на несколько этапов: фильтрация и выбор нужных данных,

затем создание новых полей на основе уже существующих, затем агрегирование данных и вычисление статистик, и в конце переименование полей, сортировка другими словами облагораживание вывода.



После того как Вы загрузили данные в систему вы можете осуществлять поиски по ним (ниже примеры запросов, с результатами выполнения):

Поисковый интерфейс имеет следующий вид:

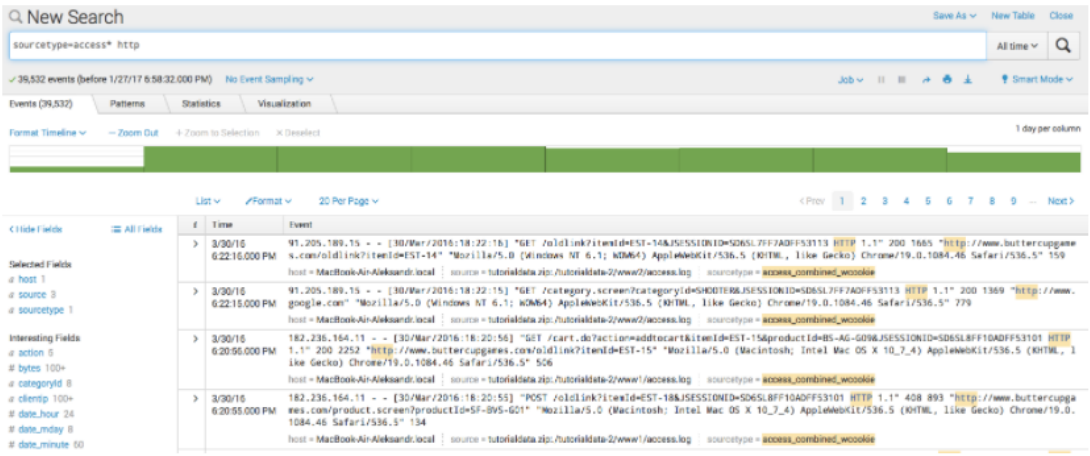


Поиск и фильтрация:

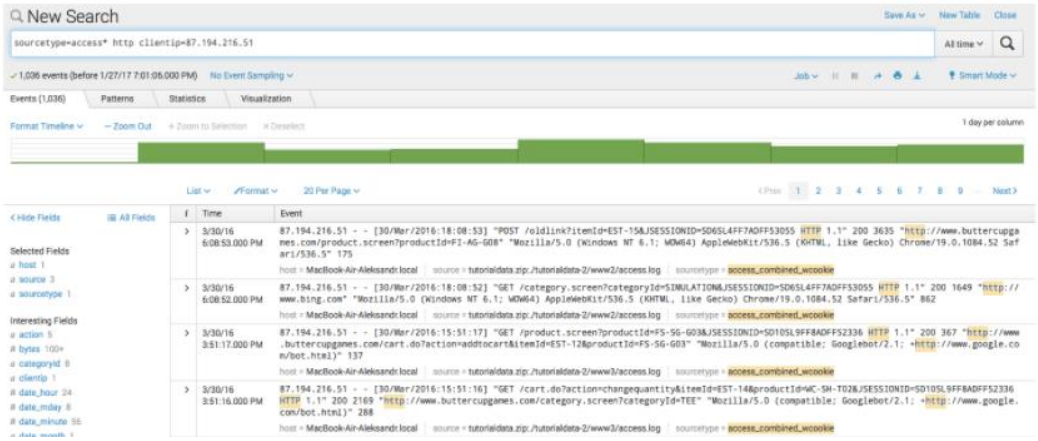
В Splunk можно «как в гугле» искать события по ключевому слову, или набору ключевых слов разделенных стандартными логическими операторами, примеры ниже. Также вы можете в любой момент актуализировать свой поиск, выбрав нужный вам временной интервал как в меню справа, так и центральной зеленой гистограмме, которая показывает количество событий в определенный период

времени.

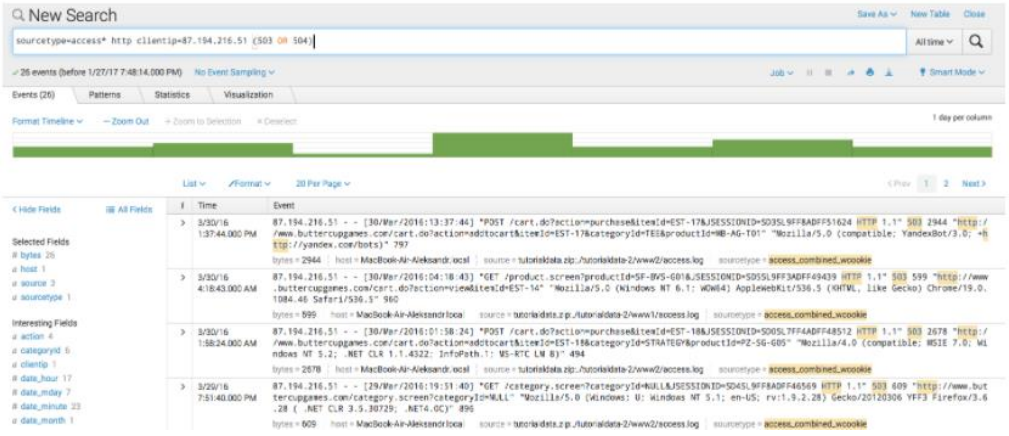
Поиск по ключевому слову: sourcetype=access* http



Фильтрация: sourcetype=access* http clientip=87.194.216.51



Комбинация: sourcetype=access* http clientip=87.194.216.51 (503 OR 504)



[Splunk. Введение в анализ машинных данных. Примеры SPL запросов и визуализация логов]