**Лабораторная работа 7.** **SIEM**

**Цель работы:** получение теоритических и практических навыков работы с SIEM.

**Ход работы:**

**Задания к лабораторной работе**

• Загрузите Splunk Enterprise

• После загрузки дистрибутива, его необходимо установить. Установка deb пакета выполняется командой <dpkg -i splunk\_package\_name.deb>.

• Для запуска Splunk выполните </opt/splunk/bin/splunk start>

• Запустите web-интерфейс, при запуске splunk будет указано, как полдключиться к нему (Что-то похожее на https://sit-VirtualBox:8000 ), чтобы начать использовать систему.

• Учётные данные по умолчанию – admin – changeme. При первом входе Вам будет предложено их изменить.

• В левой части окна будут перечислены приложения, установленные в Splunk и доступные для работы. Приложение это своего рода среда или интерфейс, в котором пользователь работает с событиями, которые собирает Splunk. По умолчанию доступно приложение Search and Reporting. У Splunk есть несколько основных типов расширения функциональности – приложения (Apps) и дополнения (Add-on).

• В центральной части экрана будет пустое окно, на котором предполагается размещение главного дашборда. В правой верхней части расположено меню для управления системой Splunk, в том числе всеми источниками данных.

• Подключим источник событий. Добавим журнал событий Linux, для мониторинга. В правой верхней части экрана выбирайте меню Settings и переходите в Data Inputs

• Перейдите в меню Settings – Data Input - Files & directories. Тип Files & directories позволяет получать события из локальных файлов и директорий.

• Нажмите на кнопку «New», введите путь к файлу auth.log (var/log/.auth.log) и выберите continuously monitor.

• Нажмите «Next». Выберите тип данных (sourcetype – operating system) из списка, а именно «linux\_audit». В открывшемся окне можно ничего не менять. Если всё прошло успешно, то после нажатия на «Start searching» вы увидите перечень событий из журнала аудита.

• Перейдите в меню Settings – Data Input - Files & directories. Добавьте домашнюю директорию, в ней создайте и удалите несколько файлов, Просмотрите журнал событий в Splunk.

• Добавьте еще несколько файлов, директорий и логов, через меню Settings – Data Input - Files & directories.

• Перейдите в приложение «Search and Reporting». Вы попадете на вкладку Search.

• Найдите события, которые относятся к файлу var/log/.auth.log , для этого введите «source=var/log/.auth.log». Здесь так же можно выбрать записи который относятся к Sourcetype (sourcetupe=operating system) – это имя типа данных, куда предполагается относить все данные определённого типа, или Host (host=splunk) – это идентификатор источника, от которого приходят события в какой-либо sourcetype (обычно доменное имя или ip-адрес). Можно фильтровать данные, введя в строку поиска определенные параметры, вы получите записи, только с этими параметрами. Можно делать составные запросы. Один запрос может состоять из множества подзапросов разделенных между собой pipe (|), и справа налево каждый следующий запрос оперирует данными полученными в результате выполнения предыдущего.

• Сбор логов – это далеко не всё, что необходимо для безопасности. Для SIEM нужно, чтобы система не только собирала логи, но и находила события, связанные с нарушениями безопасности. При слежении за логами, можно автоматически обнаруживать любые угрозы безопасности. Splunk можно использовать вместе с IDS.

• Запустите Snort с ведением логов <sudo snort -A console -i eth0 -c snort.conf -l /var/log/snort/>. Произведите различные типы сканирования nmap, и проверку правил Snort. И добавьте логи Snort в Splunk. Вы так же можете загрузить приложение Snort для Splunk https://splunkbase.splunk.com/app/340/ . Вместо Snort можно так же использовать OSSEC, для OSSEC тоже есть приложение в Splunk.

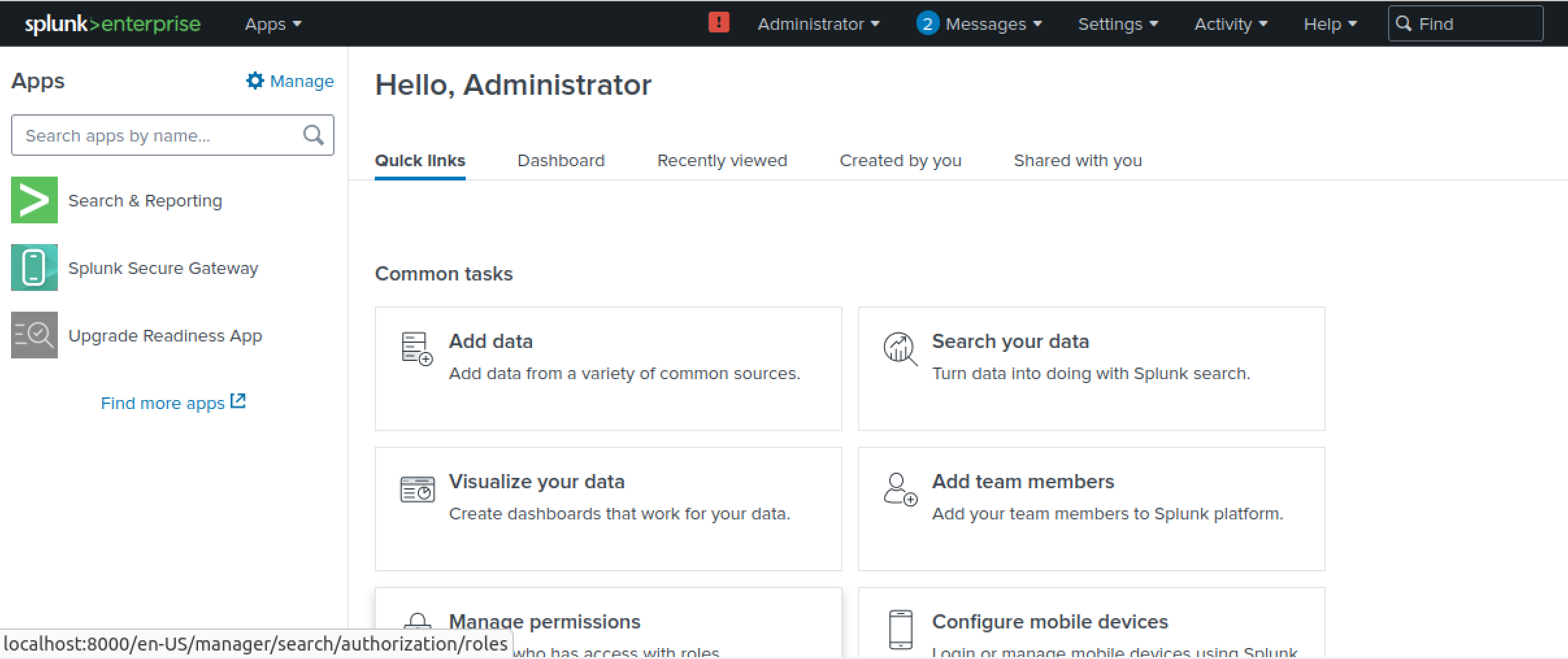


Рисунок 1 – Главное меню splunk

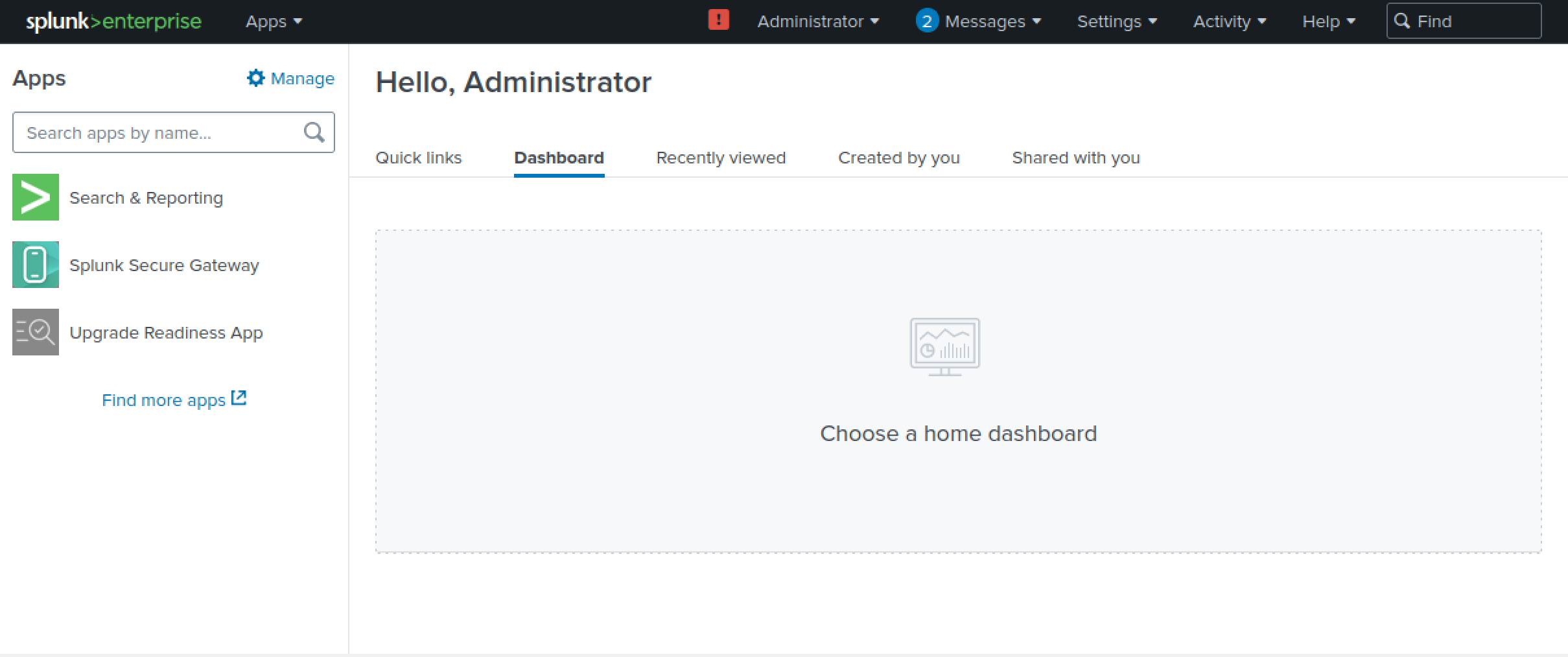


Рисунок 2 – splunk

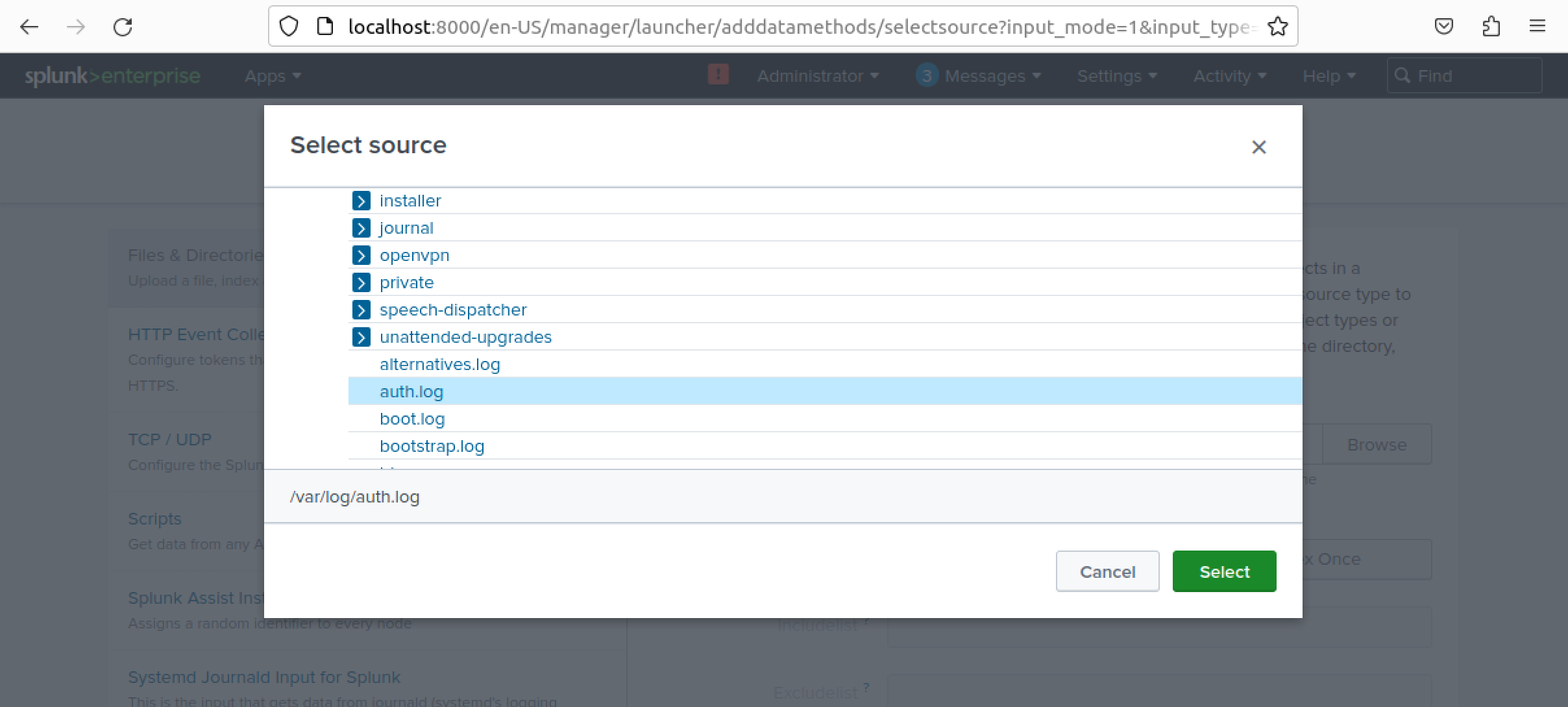


Рисунок 3 – Выбор файла авторизации

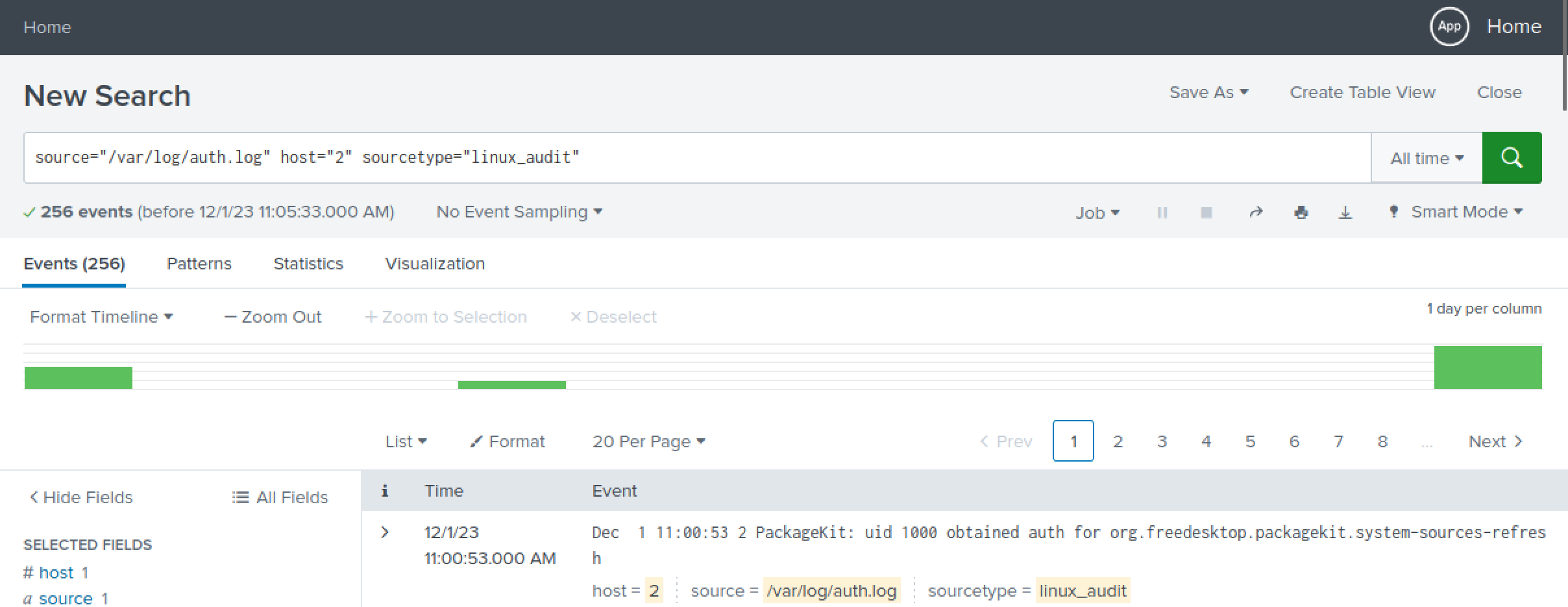


Рисунок 4 – Добавление файла авторизации в список отслеживаемых файлов

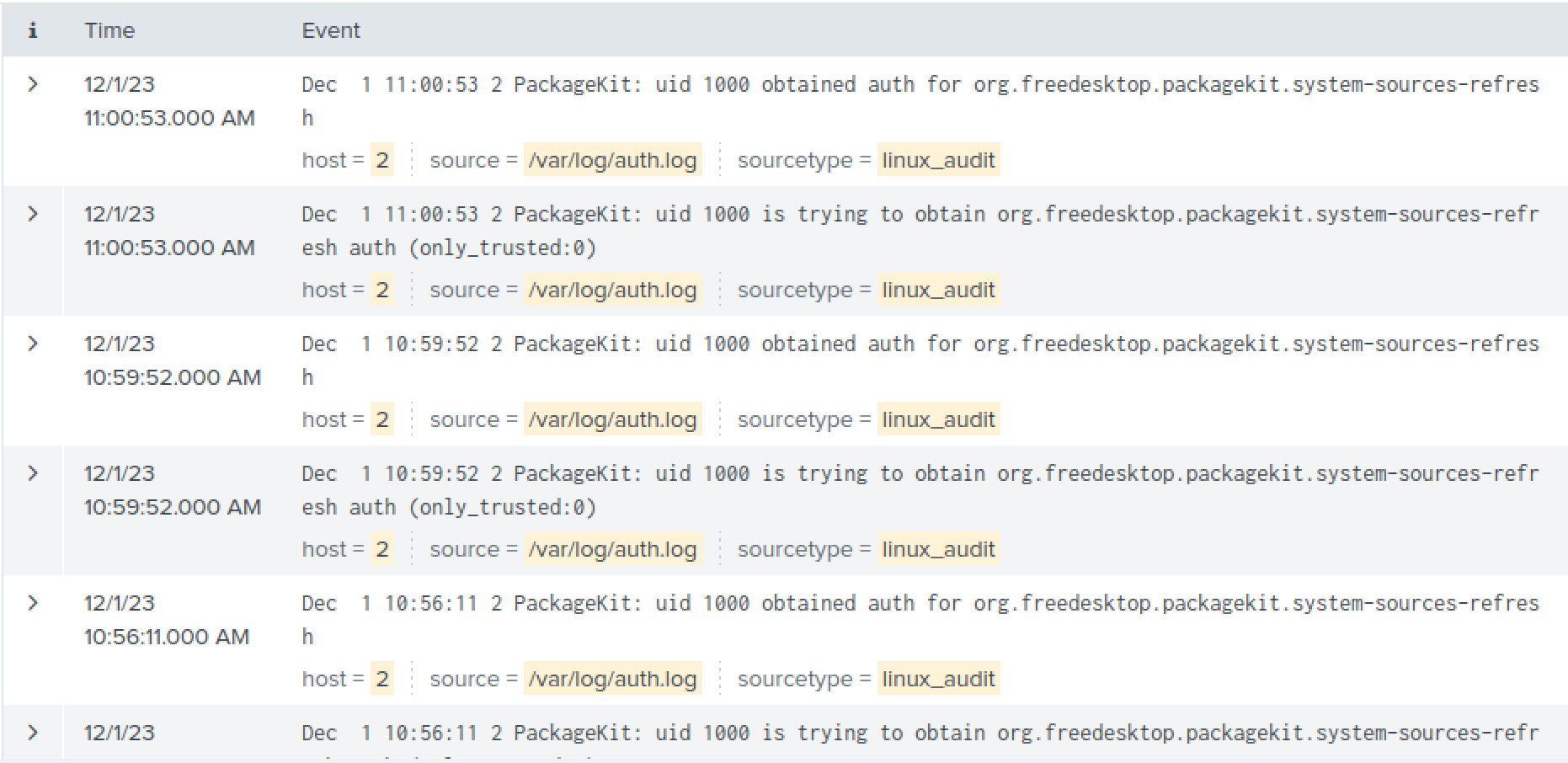


Рисунок 5 – Log об изменениях

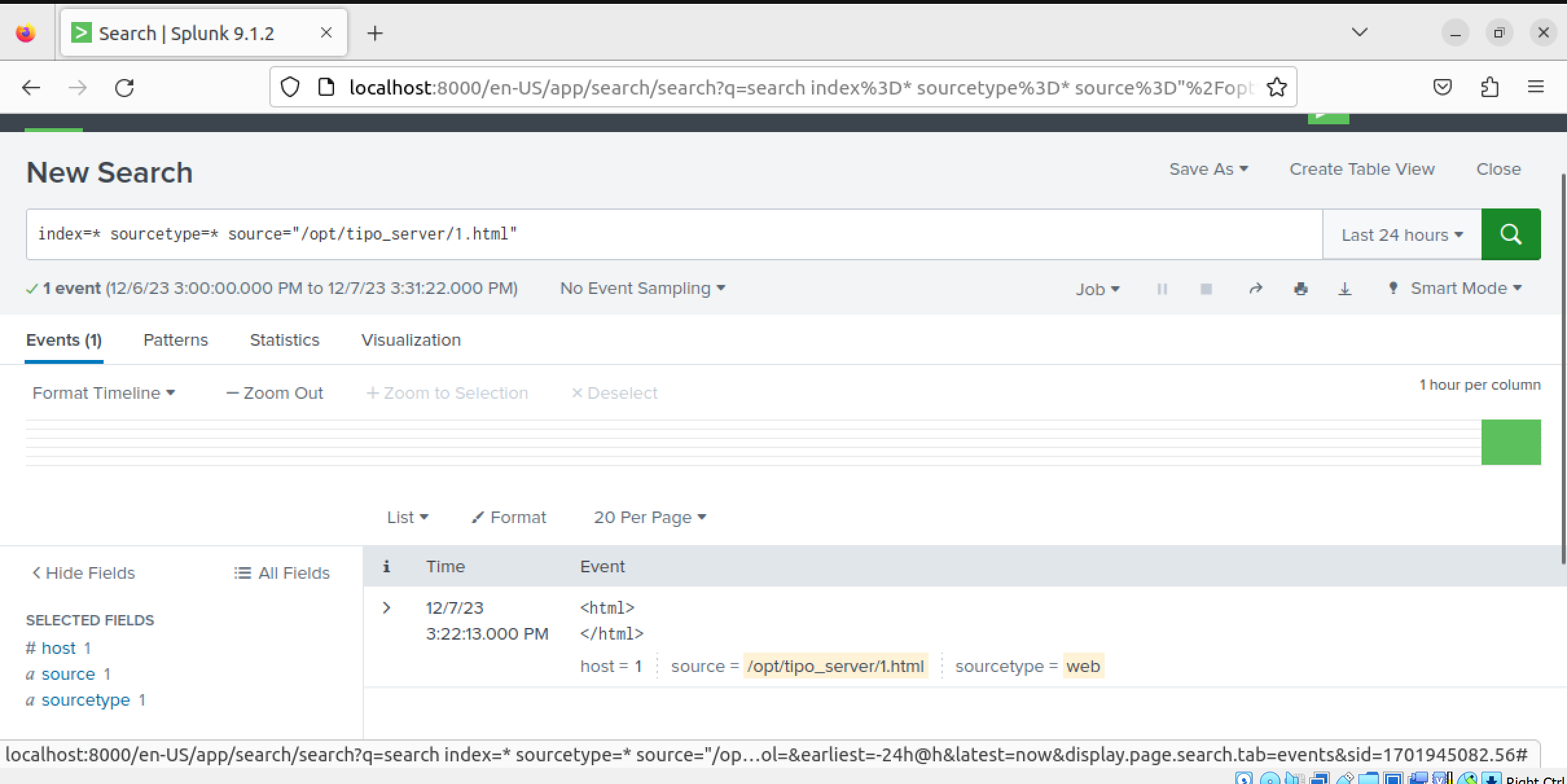


Рисунок 6 – Log об изменениях

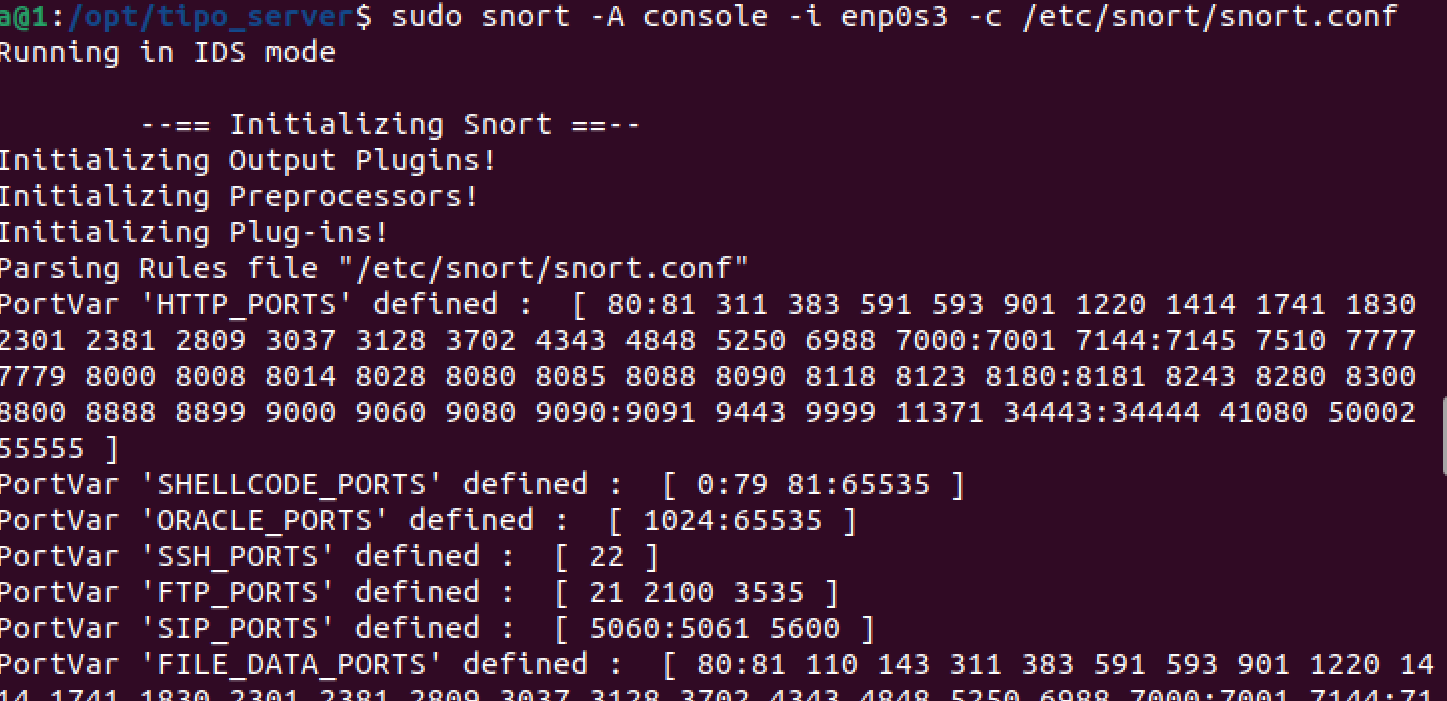


Рисунок 7 – Запуск Snort

**Вывод:** получил теоретические и практические навыки работы с SIEM.