1. Установка виртуальной машины Java.

Установим программный пакет Java Runtime Environment



Затем установим программный пакет JDK:



1. Установка и настройка Elasticsearch

Установим Elasticsearch при помощи следующих команд:







Внесем следующие изменения в конфигурационный файл:



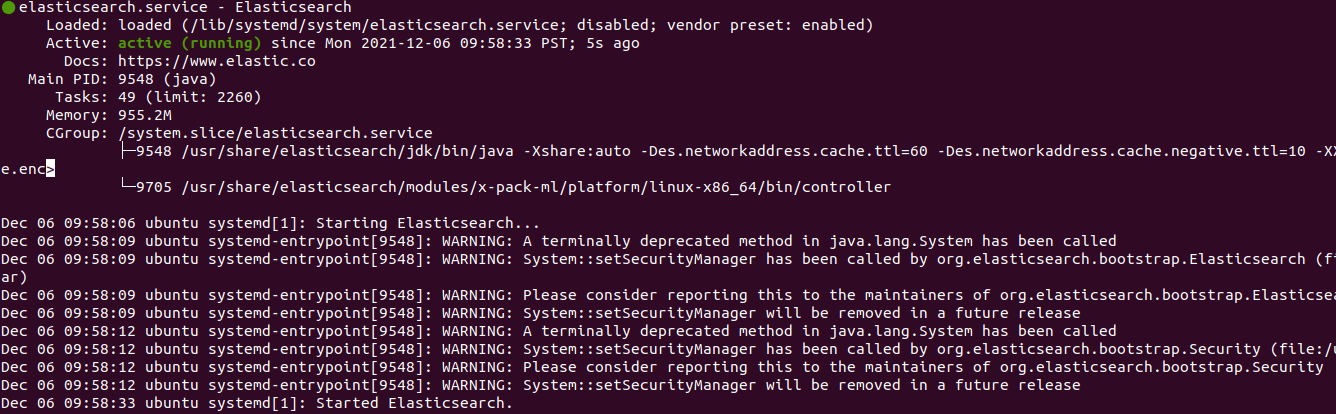


Запустим сервис



И проверим статус запуска сервиса





Далее проверим доступ к сервису, отправив HTTP запрос:



Проверим доступность сервиса с хост машины через браузер:



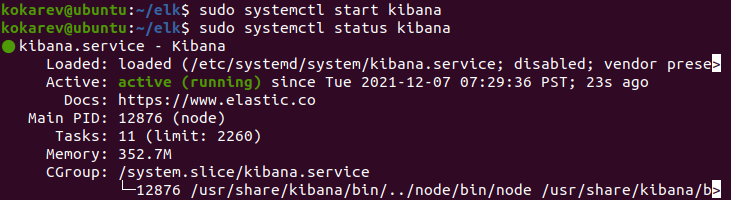
1. Установка и настройка Kibana



Внесем изменения в конфигурационный файл: пропишем порт и ip-адрес сервера, и адрес до elasticsearch и kibana

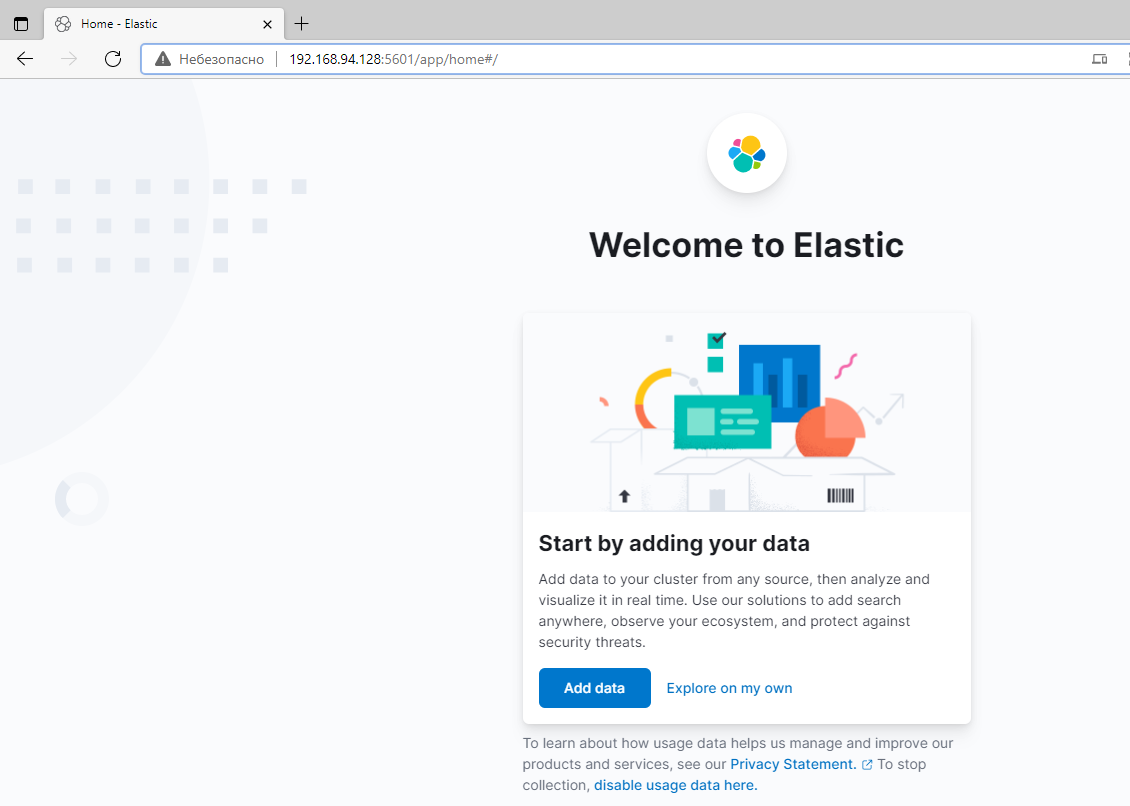


Запустим и проверим статус kibana:



PS: с первого раза все запустилось, но через браузер хотс машины не удалось попасть в kibana. Можно было бы отключить и заново включить elasticsearch, но я пошел по пути reboot-а и все заработало.

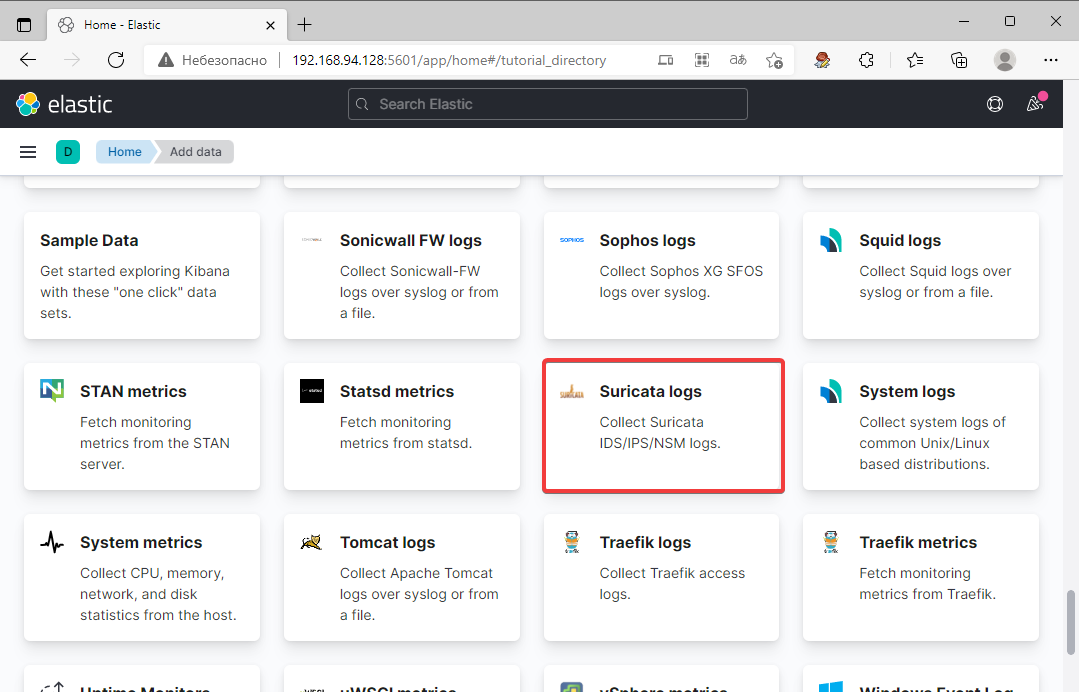
Заходим в kibana через браузер хост машины



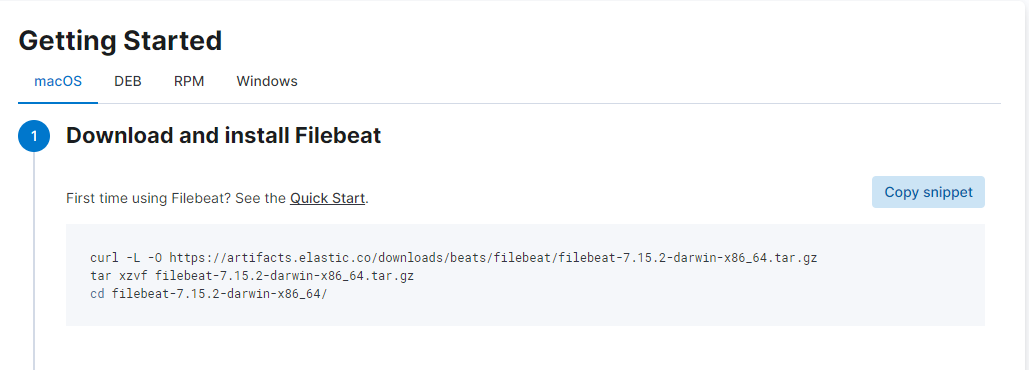
1. Установка и настройка Filebeat

Переходим по ссылке: <http://192.168.94.128:5601/app/home#/tutorial_directory>

И ищем в списке Suricata logs

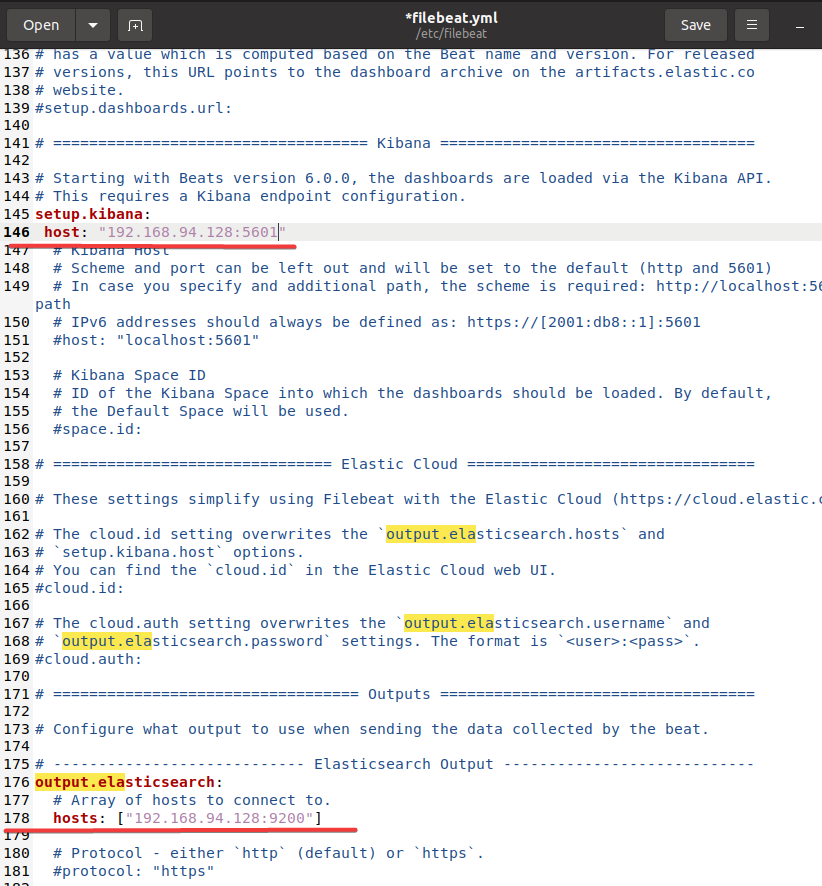


При нажатии будет открыта инструкция, по установки Filebeat и настройки конфигурации

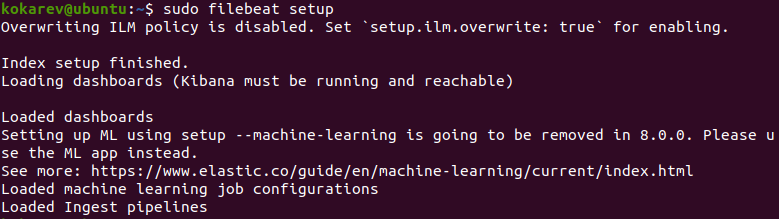


Приступим к установке.

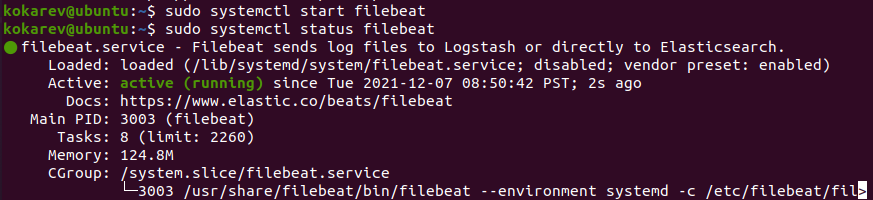




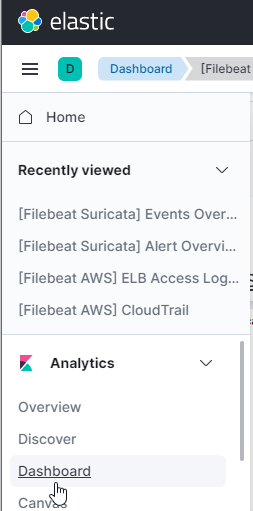


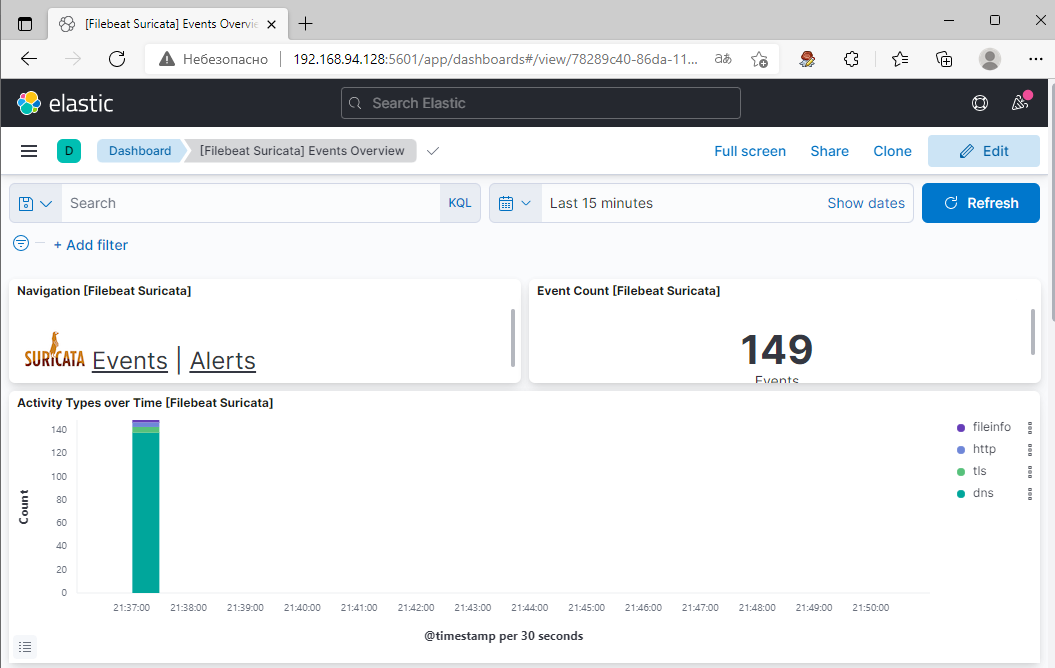


Запустим filebeat и проверим его статус:

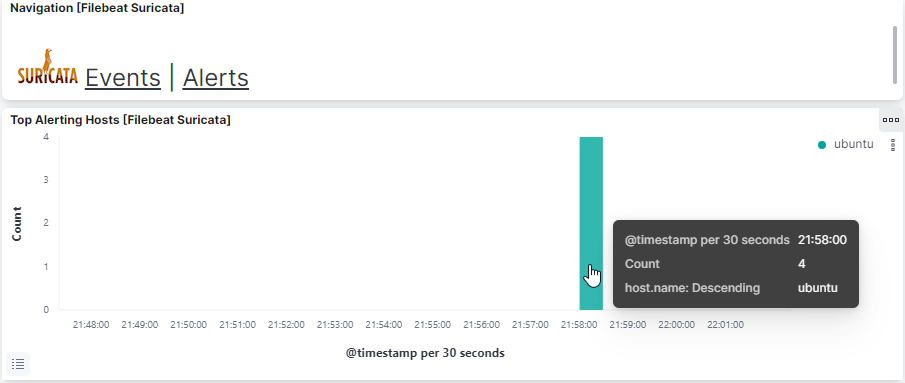


Переходим в kibana, в разделе Dashboard находим Suricata events



Работает:

Проверим работу алертов при нашем правиле пинга:



Запустим сурикату на более продолжительное время, включив при этом правила, которые идут в сборке.