Продолжаю цикл статей по настройке централизованной системы сбора логов ELK Stack. Сегодня расскажу, как собирать логи с Windows Server различных версий в elasticsearch. Данные предложенным способом можно будет собирать не только с серверных систем, но и со всех остальных, где используется журнал windows.

Содержание:

- 1 Введение
- 2 Сбор windows логов
- 3 Dashboard в Kibana для Windows Server
- 4 Сбор и анализ логов Windows Fileserver
- 5 Заключение

Введение

В своей статье я буду считать, что вы установили и настроили elk stack по моему материалу. Если это не так, то сами подредактируйте представленные конфиги под свои реалии. По большому счету, все самое основное по сбору логов windows серверов уже дано в указанной статье. Как минимум, там рассказано, как начать собирать логи с помощью **winlogbeat**. Дальше нам нужно их обработать и нарисовать функциональный дашборд для быстрого анализа поступающей информации.

Для того, чтобы оценить представленные мной графики и дашборды, рекомендую собирать логи сразу с нескольких серверов. Так можно будет оценить представленную информацию на практике. С одним сервером не так наглядно получится.

С визуализацией данных из windows журналов проблем нет никаких. Winlogbeat из коробки умеет парсить логи и добавлять все необходимые метаданные. Со стороны logstash не нужны никакие фильтры. Принимаем все данные как есть с winlogbeat.

Сбор windows логов

Приступим к настройке. Устанавливаем последнюю версию winlogbeat на сервер, с которого мы будем отправлять логи в elk stack. Вот конфиг с тестового сервера, по которому пишу статью:

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: Security
  - name: System

tags: ["winsrv"]

output.logstash:
  hosts: ["10.1.4.114:5044"]

logging.level: info
logging.to_files: true
logging.files:
  path: C:/Program Files/Winlogbeat/logs
  name: winlogbeat
  keepfiles: 7
```

Теперь настраивает logstash на прием этих логов. Добавляем в конфиг:

```
    else if "winsrv" in [tags] {
        elasticsearch {
            hosts     => "localhost:9200"
            index    => "winsrv-%{+YYYY.MM}"
        }
    }
```

Я формирую месячные индексы с логами windows серверов. Если у вас очень много логов или хотите более гибкое управление занимаемым объемом, то

делайте индексы дневные, указав winsrv-%{+YYYY.MM**.dd**}.

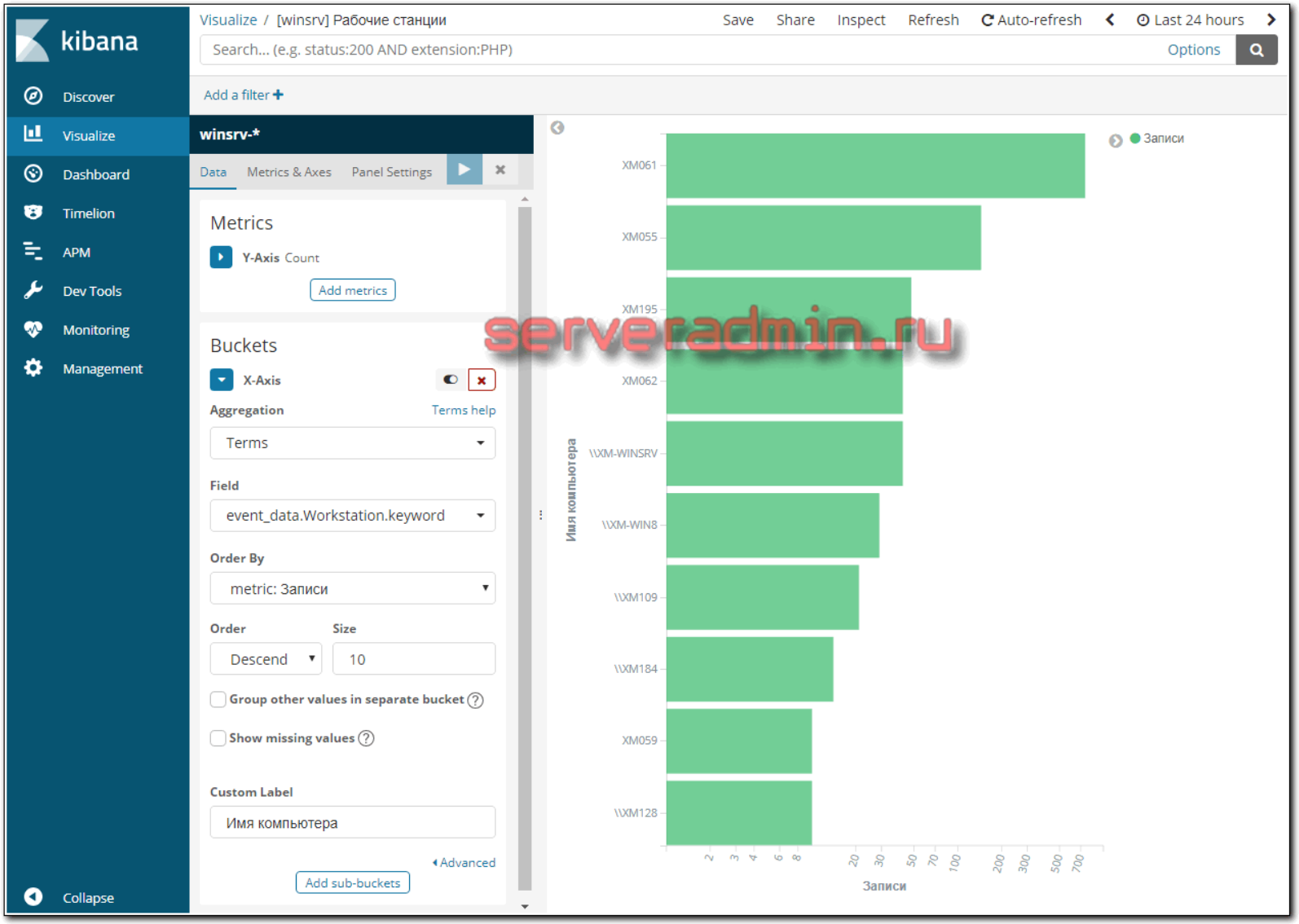
Перезапускайте службы на серверах и ждите поступления данных в elasticsearch.

Dashboard в Kibana для Windows Server

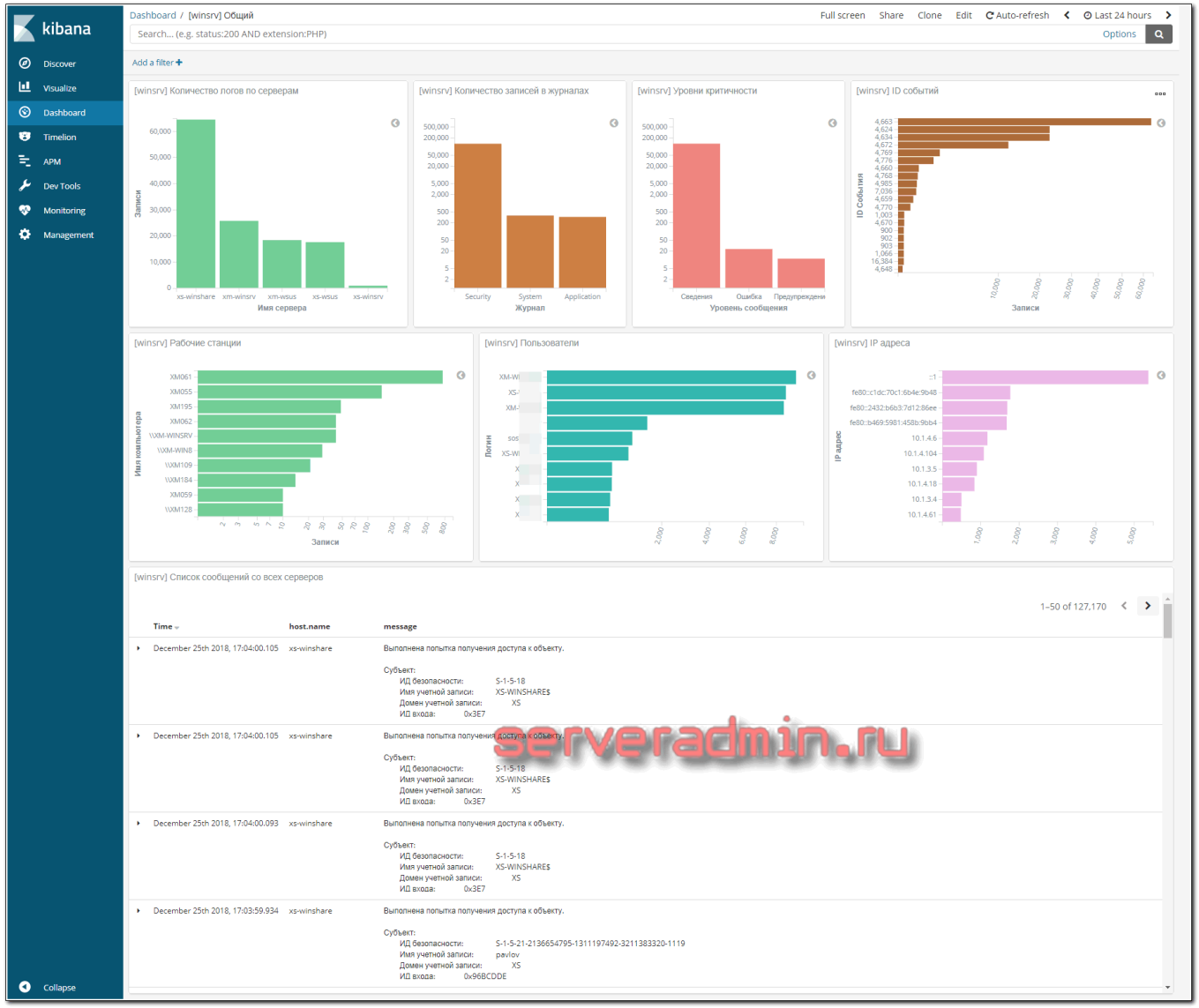
После того, как данные из логов windows серверов начали поступать в elk stack, можно приступить к их визуализации. Я предлагаю такую информацию для Dashboard в kibana:

- Количество логов с разбивкой по серверам
- Количество записей в каждом журнале
- Разбивка по уровням критичности (поле level)
- Разбивка по ID событий в логах (поле event_id)
- Список имен компьютеров, фигурирующих в логах (поле event_data.Workstation)
- Список пользователей в логах (поле event_data.TargetUserName)
- Разбивка по IP адресам (поле event_data.IpAddress)

Визуализации создаются достаточно просто, плюс они все похожи друг на друга. Вот пример одной из них — разбивка по рабочим станциям:



А вот какой Dashbord у меня получился в итоге:

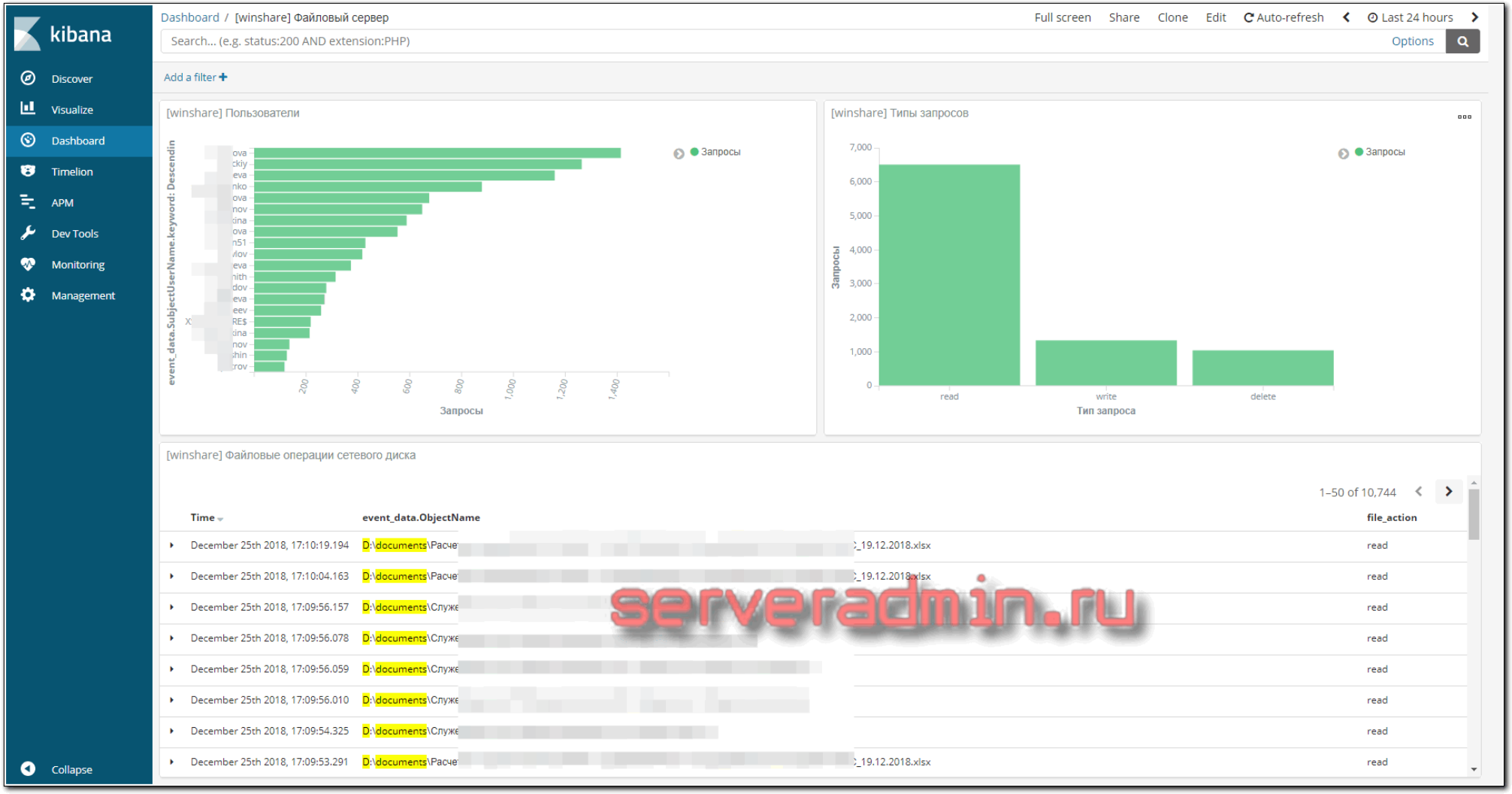


В самом низу идет список логов с сырым текстом события. Отдельно представляю дашборд для файлового сервера windows.

Сбор и анализ логов Windows Fileserver

Для файлового сервера настраиваем сбор логов в ELK Stack точно так же, как я показал выше. Для визуализации данных я настроил отдельный дашборд в Kibana со следующей информацией:

- Имена пользователей, которые обращаются к файлам (поле event_data.SubjectUserName)
- Типы запросов, которые выполняются (поле file_action)
- Список доступа к файлам (формируется из сохраненного фильтра поиска)



Возможно, кому-то будет актуально выводить на дашборд еще и информацию об именах файлов, к которым идет доступ. Информация об этом хранится в

поле event_data.ObjectName. Лично я не увидел в этом необходимости.

Заключение

> Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Материал написан исключительно на основании своего видения и небольшого опыта использования elk stack. Нигде не видел статей и мыслей на данную тему, так что буду рад предложениям, замечаниям. Ко всему прочему, я практически не администрирую windows сервера. Пишите обо всем в комментариях.

Помогла статья? Есть возможность отблагодарить автора