Очередной материал на тему централизованной системы сбора логов. Сегодня расскажу, как настроить сбор логов с устройств компании Mikrotik в ELK Stack. Статья ничем не примечательна, так как делается все стандартно и просто. Никакого парсинга и разбора логов я делать не буду. То есть будем просто хранить логи микротиков в одном месте с удобным поиском.

> Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Курс стоящий, все подробности читайте по ссылке.

Содержание:

Введение

Ранее я рассказал, как установить и настроить elk stack, потом как загружать и анализировать логи nginx и samba. Теперь пришел черед логов Mikrotik. Я уже рассказывал, как отправлять логи микротика на удаленный syslog сервер, в качестве которого может выступать в том числе syslog-ng. В данном случае на самом микротике ничего особенного делать не надо. Будем точно так же отправлять данные на удаленный syslog сервер, в качестве которого будет трудиться **logstash**.

Я некоторое время рассуждал на тему парсинга и разбора логов. Но посмотрев на типичную картину стандартных логов mikrotik, понял, что ничего не выйдет. События очень разные и разобрать их одним правилом grok не получится. Если нужен парсинг и добавление метаданных к событиям, необходимо

определенные события выделять и направлять отдельным потоком в logstash, где уже обрабатывать своим фильтром. Например, отдельный фильтр можно настроить на парсинг подключений к vpn или подключение по winbox с анализом имен пользователей.

Я же буду просто собирать все логи скопом и складывать в единый индекс. У записей не будет метаданных, по которым можно строить дашборды и анализировать данные. Но тем не менее, это все равно удобно, так как все логи в одном месте с удобным и быстрым поиском.

Настройка logstash на прием логов микротик

В конфиге */etc/logstash/conf.d/input.conf* добавляем секцию для приема syslog логов. Вместе с логами от beats конфиг будет выглядеть вот так:

```
input {
    beats {
        port => 5044
    }
    syslog {
        port => 5045
        type => syslog
    }
}
```

В конфиге с фильтрами *filter.conf* я разделил с помощью тэгов логи обычных роутеров, свитчей и wifi точек доступа по ip адресам. Получилось примерно так:

```
    else if [host] == "10.1.4.19" or [host] == "10.1.5.1" {
        mutate {
            add_tag => [ "mikrotik", "gateway" ]
        }
    }
    else if [host] == "10.1.4.66" or [host] == "10.1.3.110" or [host] == "10.1.3.111" {
        mutate {
            add_tag => [ "mikrotik", "wifi" ]
        }
```

```
    }
    else if [host] == "10.1.4.14" or [host] == "10.1.5.33" {
        mutate {
            add_tag => [ "mikrotik", "switch" ]
        }
    }
```

Это простой случай, когда устройств мало. Если у вас много устройств, то лучше наверно придумать что-то другое, чтобы не нагружать logstash лишними правилами. Да и в ручную править конфиг неудобно. Как лучше поступать в таком случае — не знаю, не продумывал тему. Наверно имеет смысл разделить потоки по разным портам и на этом основании принимать решение о дальнейшей обработке.

Отправляем полученные логи в elasticsearch, настроив конфиг *output.conf*:

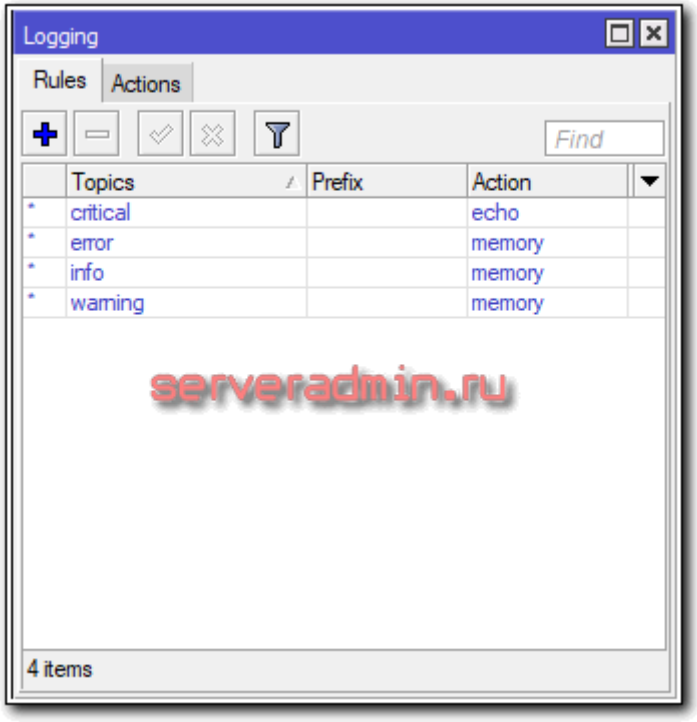
```
    else if "mikrotik" in [tags] {
        elasticsearch {
            hosts     => "localhost:9200"
            index    => "mikrotik-%{+YYYY.MM}"
        }
    }
```

Я просто складываю все логи с тэгом mikrotik в один индекс с разбивкой по месяцам. На типы gateway, switch и wifi не разделяю, хотя можно это сделать. Тэги я добавил просто для удобства просмотра логов. С помощью тэгов можно будет быстро группировать логи по типу устройств.

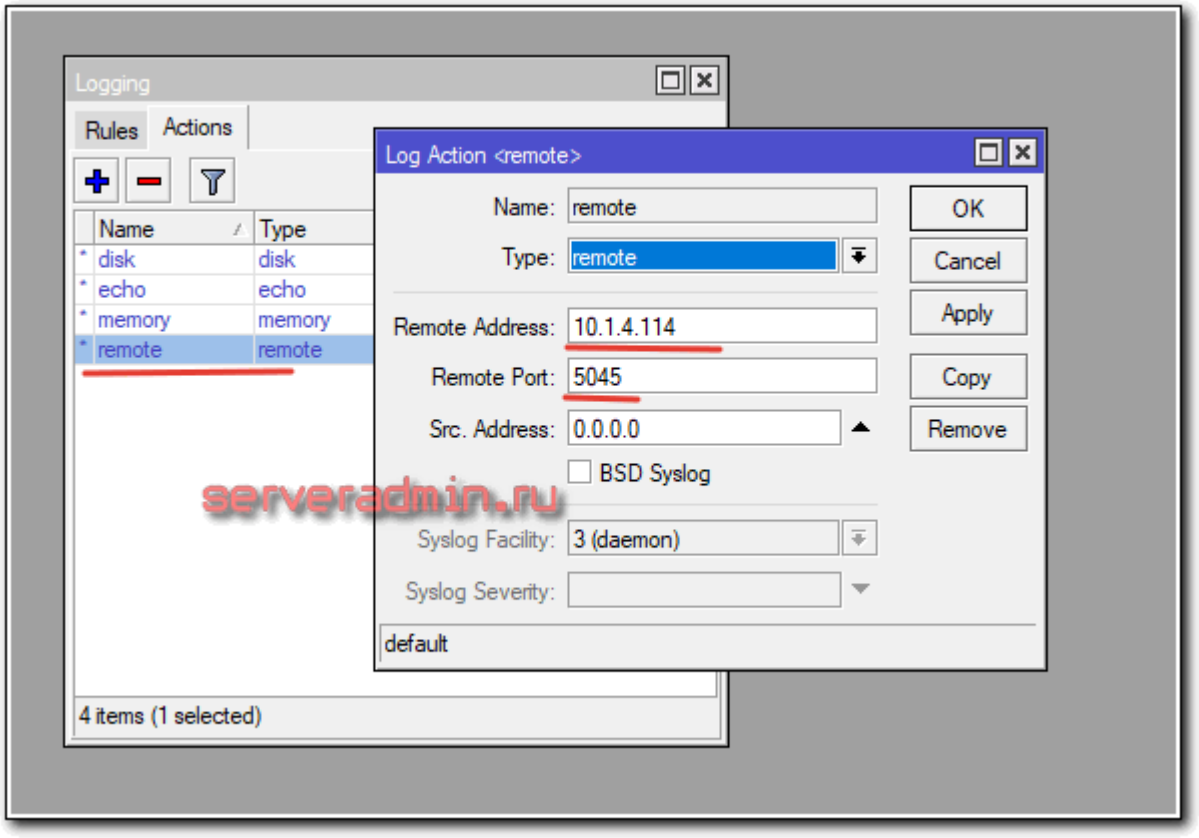
Перезапускаем logstash и идем настраивать микротики на отправку логов на удаленный сервер.

Отправка логов mikrotik на удаленный сервер

Подключаемся к Mikrotik по winbox и идем в раздел **System -> Logging**. Изначально там вот так, если вы ничего не меняли.



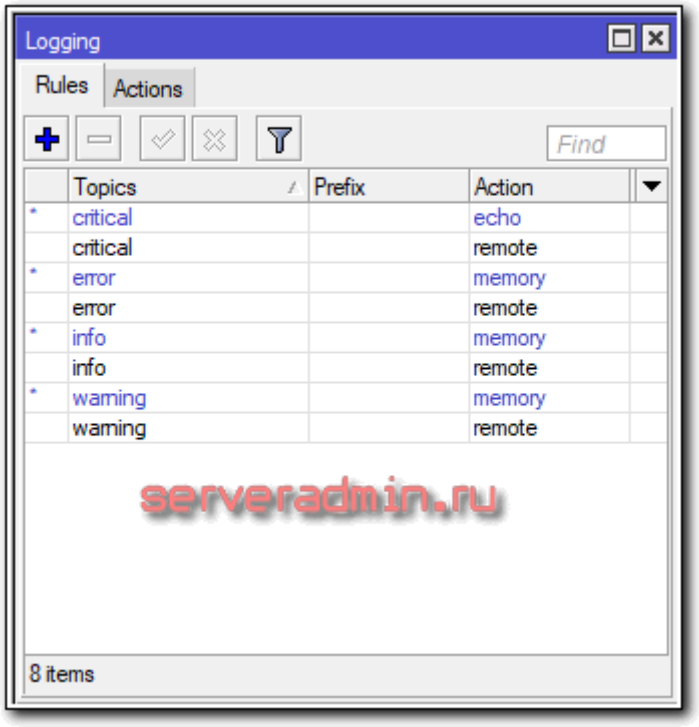
Идем на вкладку Actions, выбираем remote и указываем параметры:



В данном случае:

- 10.1.4.114 — сервер elk, точнее с logstash;
- 5045 — порт, по которому logstash принимает syslog подключения.

После этого идем на вкладку Rules и дублируем стандартные правила, указывая action remote или добавляем новые правила для отправки логов. Должно получиться примерно вот так:



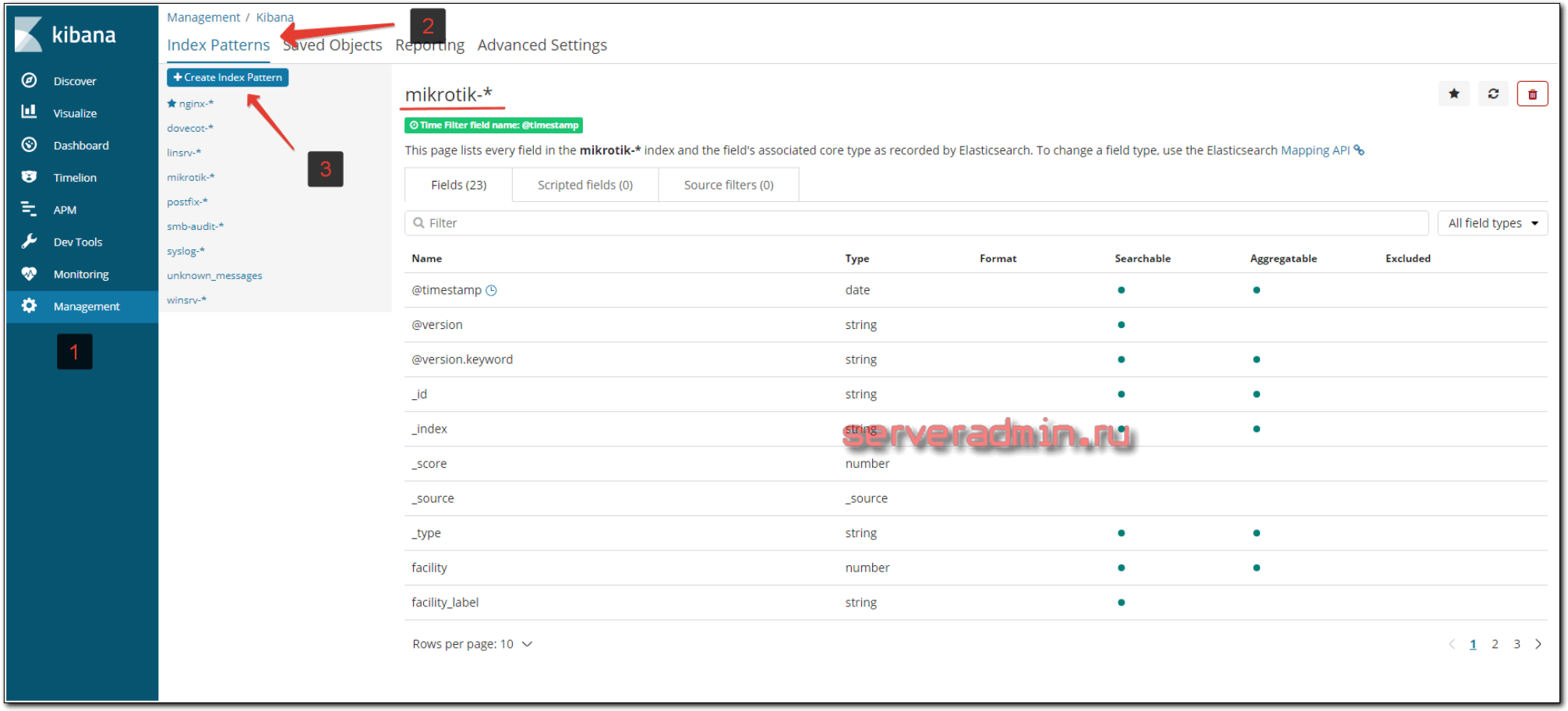
Все, микротик настроен на отправку логов на удаленный сервер. Больше на нем ничего делать не надо. Идем в web интерфейс Kibana.

Добавление индекса mikrotik в kibana

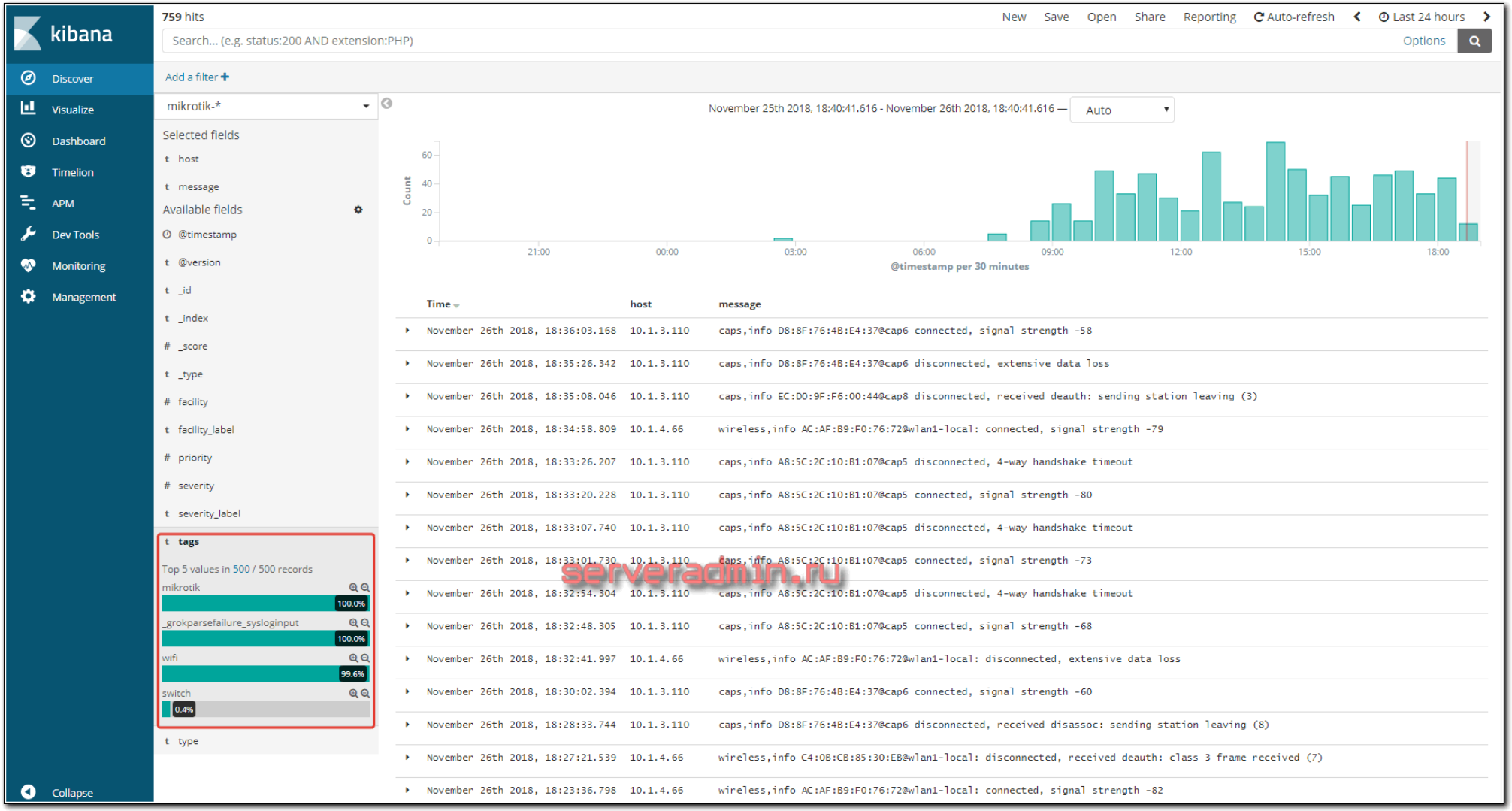
Если в предыдущих разделах вы все сделали правильно, в elasticsearch должны начать поступать данные от микротиков в индекс mikrotik-*. Идем в Kibana в раздел **Management -> Index Patterns** и добавляем новый индекс.

Интересные записи:

Шутки для сисадминов
Мои программы для системного администрирования
Монетизация ИТ блога, сколько можно заработать на информационном сайте



После этого можно в разделе **Discover** просматривать логи. При этом работает группировка по тэгам, которые характеризуют тип устройства.



На этом по настройке хранения логов mikrotik в elk stack все. Надеюсь, было полезно.

Заключение

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

Получилась простая статья по сбору логов. Для тех, кто уже работал с ELK Stack тут ничего нового нет. По сути, никакого анализа и графиков нет, а именно это чаще всего интересует при использовании elk. Я просто не придумал, что может быть полезного в логах микротика, что требует какого-то детального разбора и построения дашбордов. Если у кого-то есть идеи или примеры grok фильтров, прошу поделиться.

Помогла статья? Есть возможность отблагодарить автора