

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:

- 1 Введение
- 2 Настройка logstash на прием логов микротик
- 3 Отправка логов mikrotik на удаленный сервер
- 4 Добавление индекса mikrotik в kibana
- 5 Заключение

## 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 vpp 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 вручную 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*:

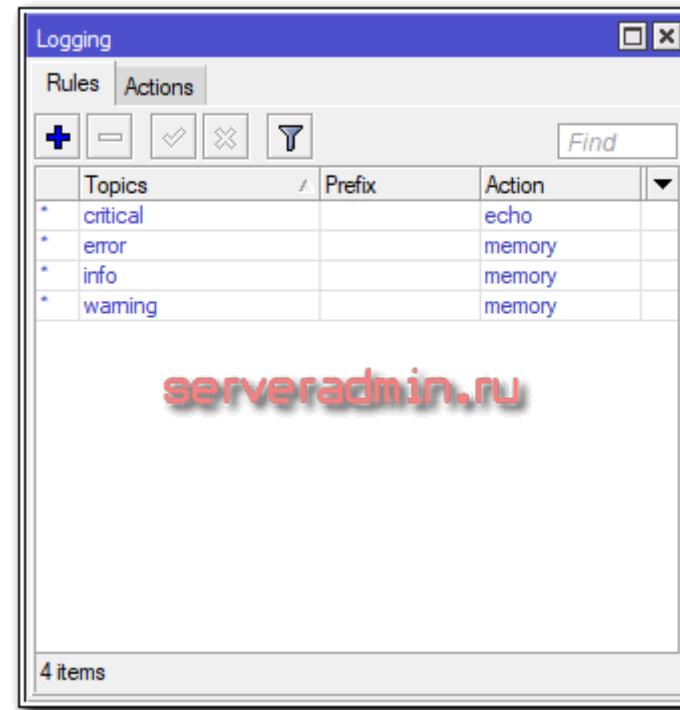
```
else if "mikrotik" in [tags] {
    elasticsearch {
        hosts     => "localhost:9200"
        index    => "mikrotik-%{+YYYY.MM}"
    }
}
```

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.

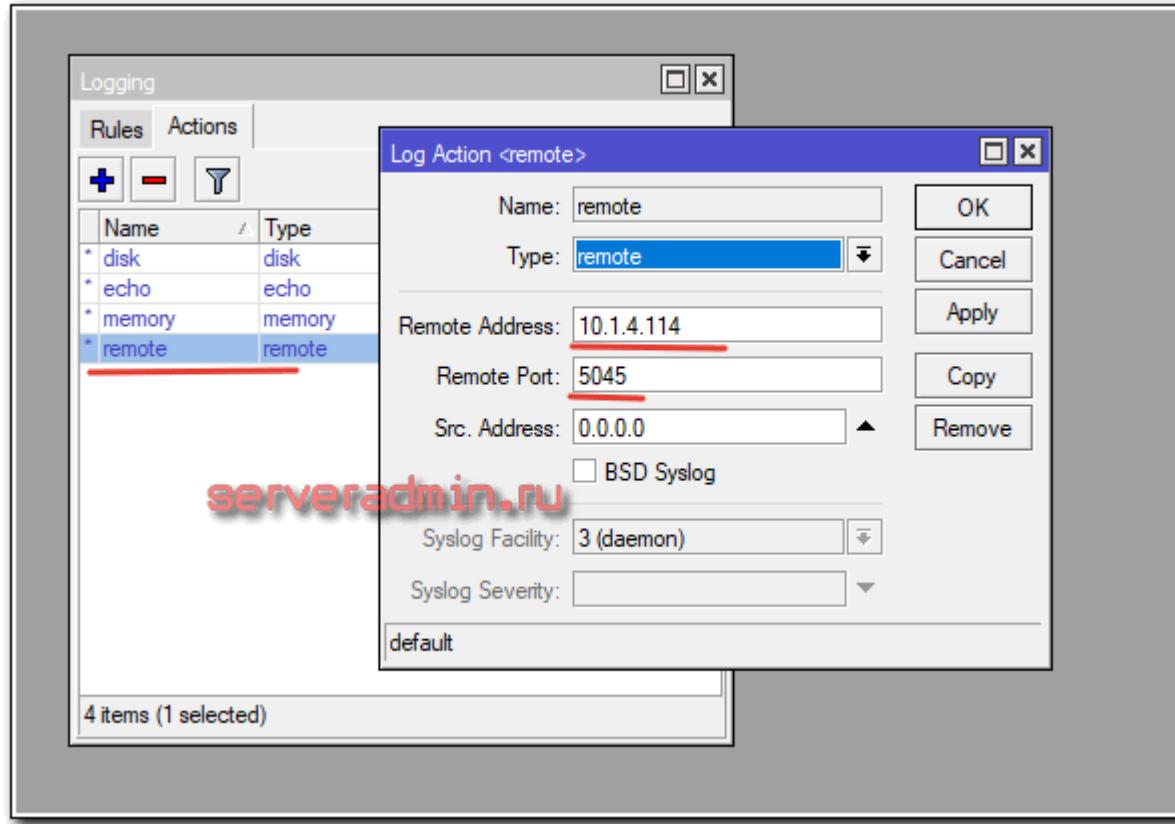
## Отправка логов mikrotik на удаленный сервер

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:

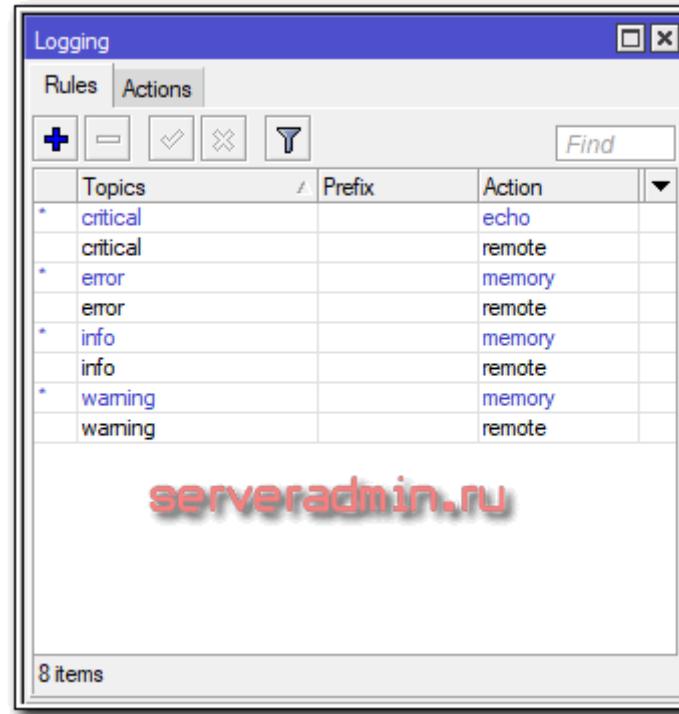




В данном случае:

- 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





Management / Kibana

Index Patterns 2 Saved Objects Reporting Advanced Settings

**+ Create Index Pattern**

**mikrotik-\***

Time Filter field name: @timestamp

This page lists every field in the **mikrotik-\*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API.

Fields (23)	Scripted fields (0)	Source filters (0)			
<input type="text" value="Filter"/> <span style="float: right;">All field types</span>					
Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	string		●		
@version.keyword	string		●	●	
_id	string		●	●	
_index	string		●	●	
_score	number				
_source	_source				
_type	string		●	●	
facility	number		●	●	
facility_label	string		●		

Rows per page: 10 < 1 2 3 >

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



759 hits

Search... (e.g. status:200 AND extension:PHP)

New Save Open Share Reporting Auto-refresh Last 24 hours Options

Discover **mikrotik-\*** November 25th 2018, 18:40:41.616 - November 26th 2018, 18:40:41.616 — Auto

Visualize

Dashboard

Timeline

APM

Dev Tools

Monitoring

Management

Selected fields

t host

t message

Available fields

@timestamp

@version

t \_id

t \_index

# \_score

t \_type

# facility

t facility\_label

# priority

# severity

t severity\_label

**t tags**

Top 5 values in 500 / 500 records

mikrotik	100.0%
.grokparsefailure_sysloginput	100.0%
wifi	99.6%
switch	0.4%

t type

Count

November 25th 2018, 18:40:41.616 - November 26th 2018, 18:40:41.616 — Auto

21:00 00:00 03:00 06:00 09:00 12:00 15:00 18:00

Time host message

November 26th 2018, 18:36:03.168 10.1.3.110 caps,info D8:8F:76:4B:E4:37@cap6 connected, signal strength -58

November 26th 2018, 18:35:26.342 10.1.3.110 caps,info D8:8F:76:4B:E4:37@cap6 disconnected, extensive data loss

November 26th 2018, 18:35:08.046 10.1.3.110 caps,info EC:D0:9F:F6:00:44@cap8 disconnected, received deauth: sending station leaving (3)

November 26th 2018, 18:34:58.809 10.1.4.66 wireless,info AC:AF:89:F0:76:72@wlan1-local: connected, signal strength -79

November 26th 2018, 18:33:26.207 10.1.3.110 caps,info A8:5C:2C:10:B1:07@cap5 disconnected, 4-way handshake timeout

November 26th 2018, 18:33:20.228 10.1.3.110 caps,info A8:5C:2C:10:B1:07@cap5 connected, signal strength -80

November 26th 2018, 18:33:07.740 10.1.3.110 caps,info A8:5C:2C:10:B1:07@cap5 disconnected, 4-way handshake timeout

November 26th 2018, 18:33:01.730 10.1.3.110 caps,info A8:5C:2C:10:B1:07@cap5 connected, signal strength -73

November 26th 2018, 18:32:54.304 10.1.3.110 caps,info A8:5C:2C:10:B1:07@cap5 disconnected, 4-way handshake timeout

November 26th 2018, 18:32:48.305 10.1.3.110 caps,info A8:5C:2C:10:B1:07@cap5 connected, signal strength -68

November 26th 2018, 18:32:41.997 10.1.4.66 wireless,info AC:AF:89:F0:76:72@wlan1-local: disconnected, extensive data loss

November 26th 2018, 18:30:02.394 10.1.3.110 caps,info D8:8F:76:4B:E4:37@cap6 connected, signal strength -60

November 26th 2018, 18:28:33.744 10.1.3.110 caps,info D8:8F:76:4B:E4:37@cap6 disconnected, received disassoc: sending station leaving (8)

November 26th 2018, 18:27:21.539 10.1.4.66 wireless,info C4:0B:CB:85:30:EB@wlan1-local: disconnected, received deauth: class 3 frame received (7)

November 26th 2018, 18:23:36.798 10.1.4.66 wireless,info AC:AF:89:F0:76:72@wlan1-local: connected, signal strength -82

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.

## Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте . Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области. Особенности курсов:

- Знания, ориентированные на практику;
- Реальные ситуации и задачи;
- Лучшее из международных программ.

Помогла статья? Есть возможность отблагодарить автора