Возникло желание собирать логи с роутера Mikrotik. Была нужна информация о подключенных по **pptp** абонентах и **логи firewall** для настройки. По-умолчанию, Mikrotik пишет все логи в лог журнал, который можно просмотреть через winbox. Стандартно, там хранятся последние 100 строк лога.

Содержание:

Настраиваем удаленный сервер rsyslog

У меня в хозяйстве имелся сервер Debian. Решил хранить логи с микротиков именно на нем. В составе Debian уже имеется сервис сбора логов с удаленных источников **rsyslog**. Необходимо только включить в нем необходимый функционал. Правим файл **/etc/rsyslog.conf**:

Раскомментируем строки

```
# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

чтобы получать логи по UDP, либо

```
# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

чтобы получать логи по TCP

И в секцию RULES добавим несколько строк для удобного хранения файлов логов от разных удаленных источников:

```
# Зададим шаблон создания имен файлов (на основании IP адреса клиента)
$template FILENAME,"/var/log/!remote/%fromhost-ip%/syslog.log"
```

```
# Укажем сохранять сообщения от любого источника (*) с любым приоритетом (*) в файл, заданный шаблоном
# Например, клиенты (10.0.0.2,10.0.0.3...) будут раскладываться в соответствующие каталоги /var/log/10.0.0.2/syslog.log
 *.* ?FILENAME
```

Перезапускаем rsyslog для применения настроек:

```
/etc/init.d/rsyslog restart
```

Теперь наш сервер готов принимать логи с удаленных источников. Хранить он их будет в папке /var/log/!remote Для каждого источника будет создана папка с именем IP адреса этого источника.

Настраиваем пересылку логов в Mikrotik

Теперь настраиваем в роутере хранение логов на удаленном сервере. Для этого заходим в раздел **System -> Logging**, выбираем закладку **Actions**, два раза щелкаем по строчке remote. Открывается окно настроек. В нем вводим адрес удаленного сервера сбора логов. Порт на свое усмотрение либо оставляем по-умолчанию, либо меняем на свой. Больше ничего добавлять не надо.

Дальше в разделе **Rules** создаем необходимое правило хранения:

Все готово. Теперь все наши логи будут храниться на удаленном сервере. Необходимо не забыть настроить ротацию логов, дабы в один прекрасный день они не заняли все свободное место.

Если вы используете ELK Stack для централизованного сбора логов, то у меня есть статья по отправке логов mikrotik в elk stack.

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 Курсы по ИТ. Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области.

Помогла статья? Есть возможность отблагодарить автора

Рекомендую полезные материалы по схожей тематике:

- Инструкция о том, как быстро выполнить настройку mikrotik.
- Использование протокола Layer7 для блокировки сайтов средствами Микротик.
- Настройка простых правил фаервола для защиты локальной сети.
- Создание единой wifi сети из множества точек доступа mikrotik с помощью **capsman**.
- 2 провайдера и 2 wan интерфейса для создания отказоустойчивой связи с интернет.