Централизованный сбор логов Mikrotik на сервер The Dude

Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

- Главная
- Централизованный сбор логов Mikrotik на сервер The Dude

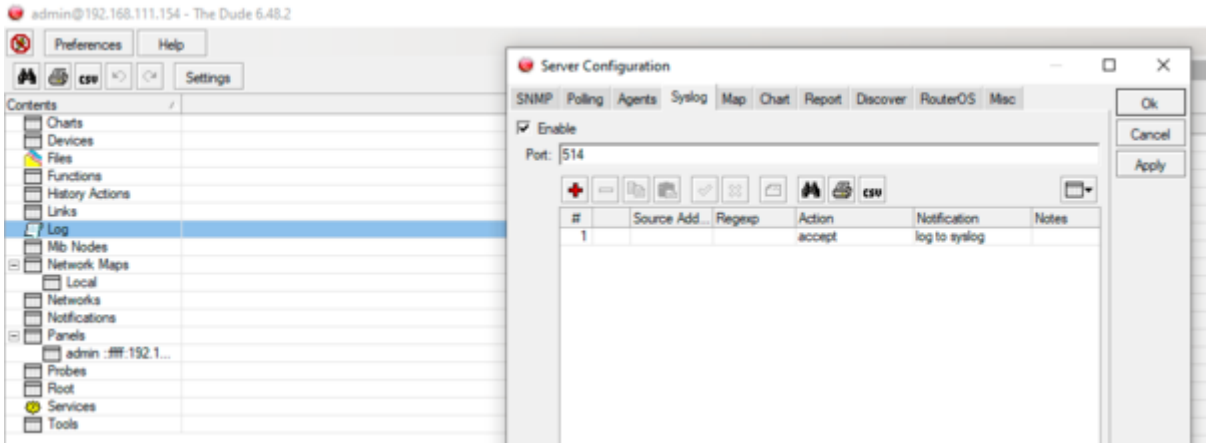
Сбор и изучение логов - важная часть работы системного администратора, помогающая разобраться в любой, даже самой сложной и запутанной ситуации. Точно также и если вы обратитесь за помощью, то первым делом от вас попросят предоставить логи. Когда устройств и сервисов в вашей сети немного, то каждый из них может собирать логи самостоятельно, но по мере увеличения количества устройств хочется иметь единую точку сбора информации. И ей вполне может стать сервер The Dude, который хоть и не дотягивает до полноценного сервера сбора логов, но все-таки может оказаться полезен.

В первую очередь коснемся особенностей ведения логов на устройствах Mikrotik. В целях экономии ресурсов флеш-памяти лог пишется в оперативную память и ограничен 1000 последних записей. При выключении или перезагрузке устройства логи теряются. В целом, если пользоваться логами грамотно и направлять туда только действительно важные события, то 1000 строк вполне достаточно, а в случае диагностики всегда можно включить подробные логи для нужных служб.

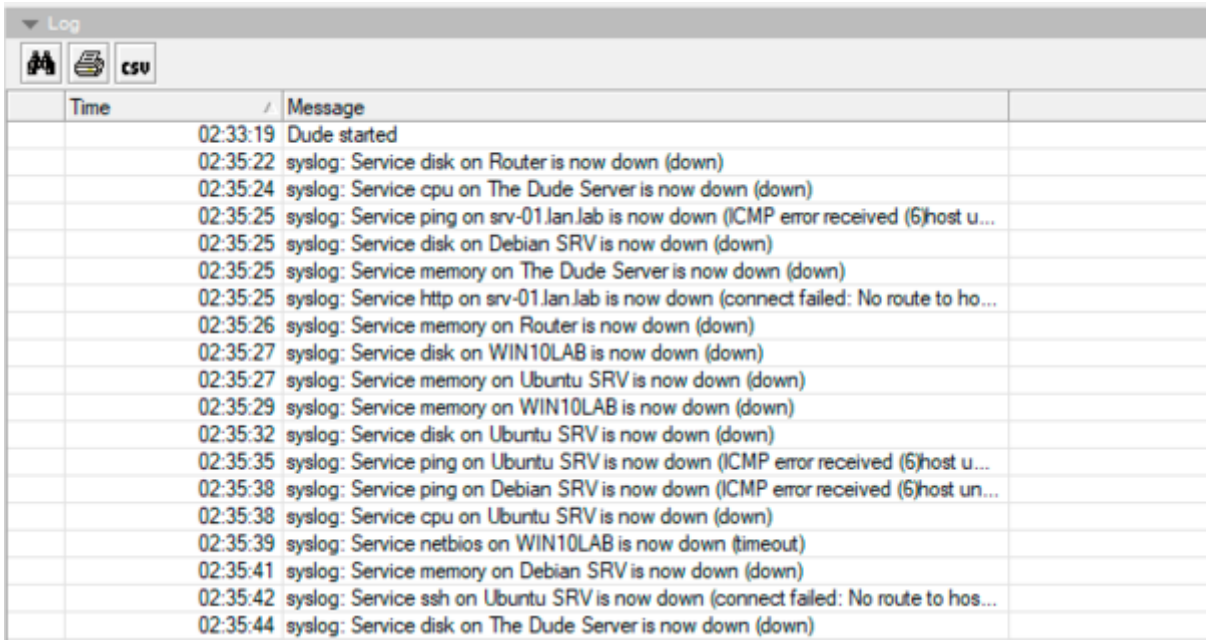
The Dude предоставляет функции сервера логов, но в крайне ограниченном виде, какие-либо инструменты поиска и анализа отсутствуют, а сам сервер фактически является только централизованной точкой сбора логов, со всеми присущими Mikrotik особенностями. Собираемые The Dude логи также хранятся в оперативной памяти и ограничены 10 000 записей, при перезагрузке роутера с The Dude они теряются. Также нет никаких настроек, позволяющих изменить такое поведение, даже если вы используете CHR и не стеснены в ресурсах, как по памяти, так и по дисковому пространству.

Но несмотря на очень и очень ограниченные возможности пренебрегать сервером логов в The Dude не стоит, при грамотном подходе он способен принести вполне ощутимую пользу, да и вообще ситуация, когда есть хоть какой-то сервер логов всегда лучше ситуации, когда никакого сервера логов нет.

По умолчанию лог-сервер в The Dude включен, чтобы убедиться в этом перейдем в **Settings - Syslog** где увидим установленный флаг **Enable** и порт на котором работает служба - **514**, ниже расположено правило, указывающее принимать логи из любого источника и записывать их в **syslog**.

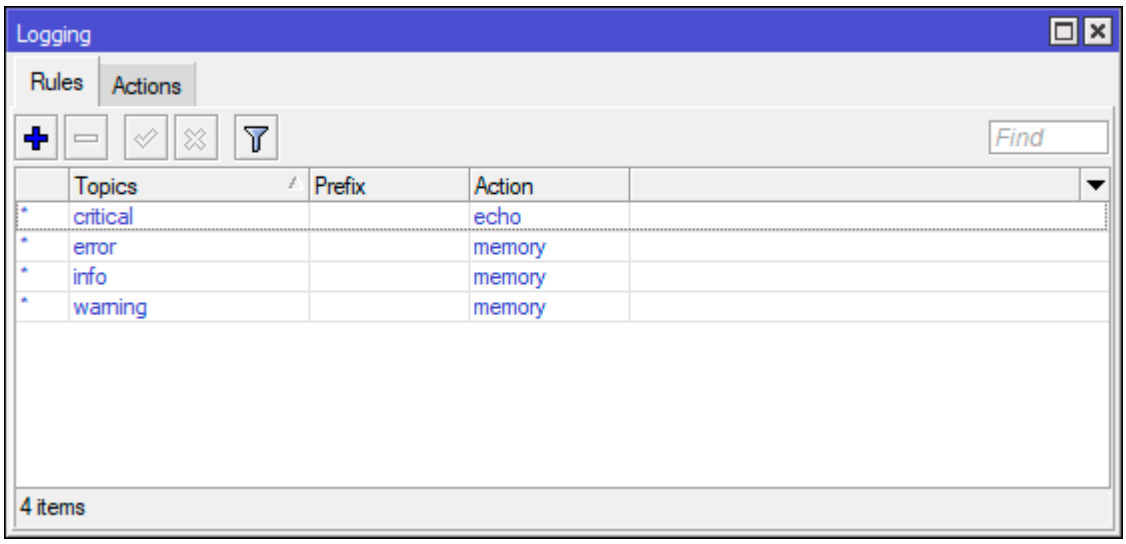


Сам сервер логов по-спартански лаконичен: из возможностей присутствует только поиск и возможность распечатать лог или выгрузить его в CSV. Даже нет возможности наложить фильтр, как это можно сделать в интерфейсе RouterOS.

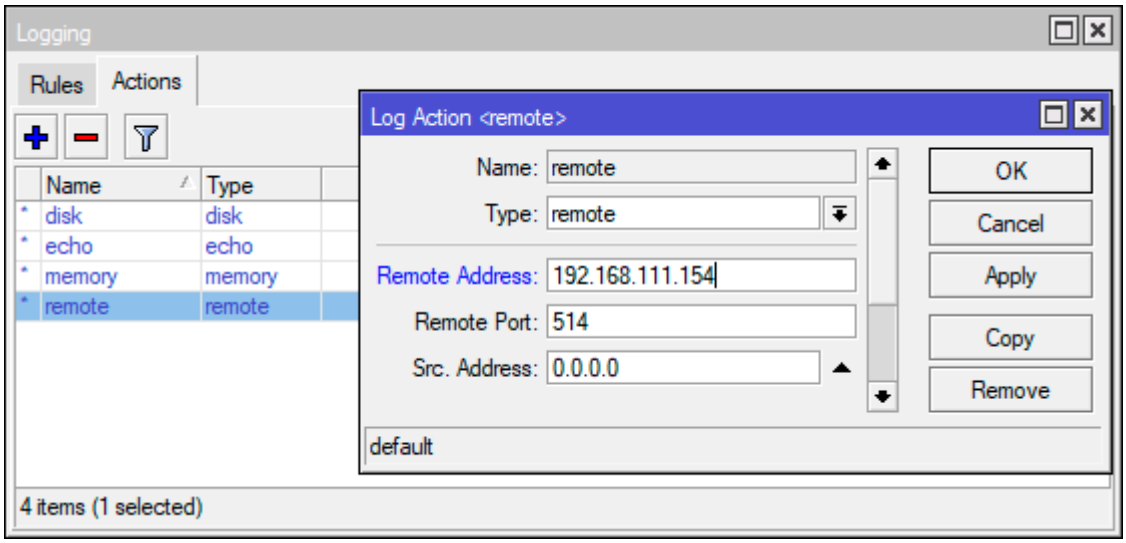


Естественно все это не добавляет привлекательности данному инструменту, но некоторые плюсы становятся видны уже здесь и сейчас. Даже в таком виде сервер логов позволяет удобно отлаживать межсетевое взаимодействие. Вы будете в одном месте видеть в реальном времени и логи клиента, и логи сервера, что гораздо удобнее, чем парсить и сопоставлять два лога.

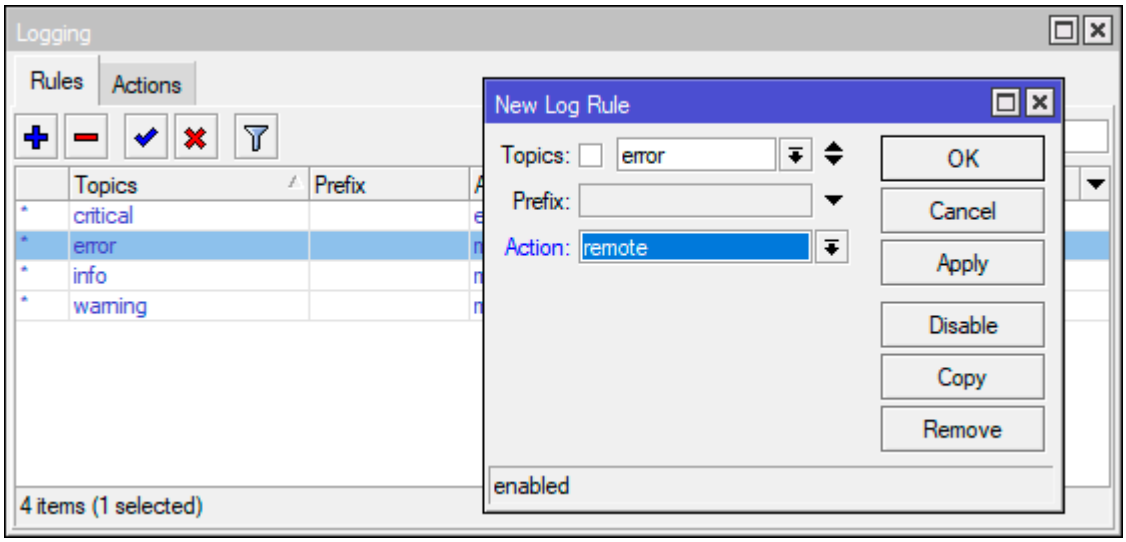
Чтобы перенаправить логи на удаленный сервер в Mikrotik перейдем в **System - Logging**. На закладке **Rules** представлены правила для логирования различных событий, т.е. какой уровень логов куда следует направить. Как видим критические события выводятся прямо в терминал, а остальные пишутся в память.



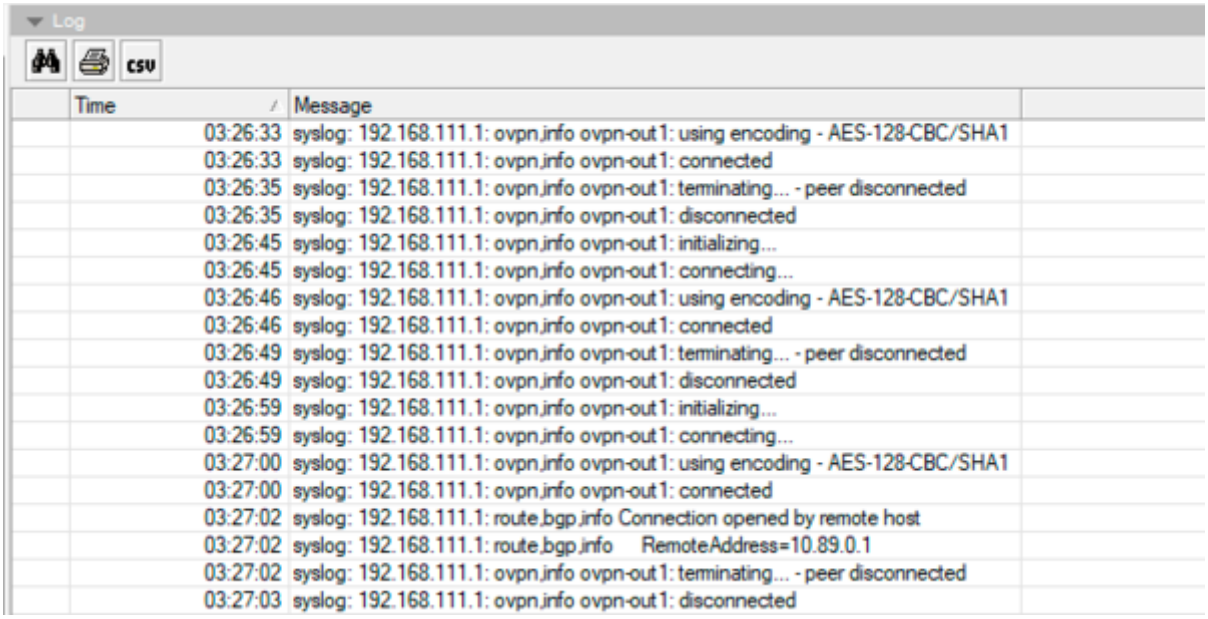
На закладке **Action** перечислены возможные действия, нас интересует **remote**, откроем его и укажем в поле **Remote Address** адрес нашего The Dude сервера.



Теперь мы можем перенаправить лог любого уровня на удаленный сервер, просто изменив **Action** для него, но в этом случае мы окажемся без локального лога, что тоже неправильно. Поэтому мы вернемся на закладку **Rules** и скопируем нужное правило, указав поле **Action** для него **remote**.

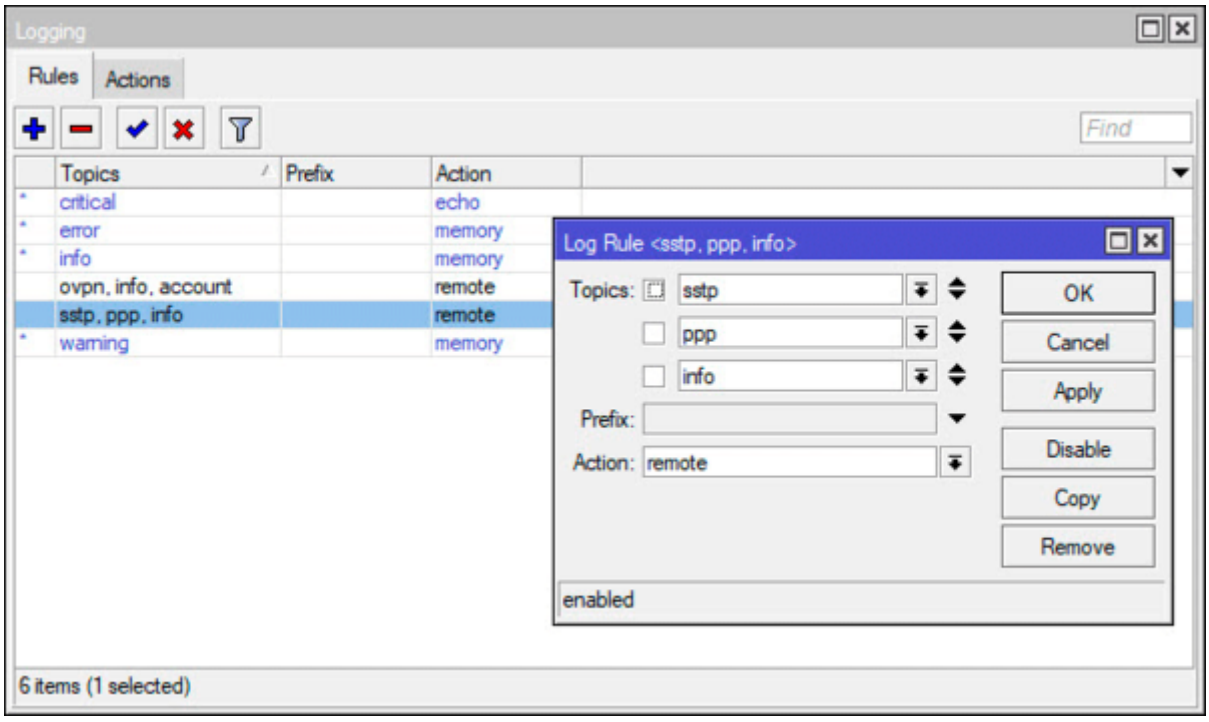


Возвращаемся в The Dude и видим, что на наш сервер пошли логи от удаленного устройства:

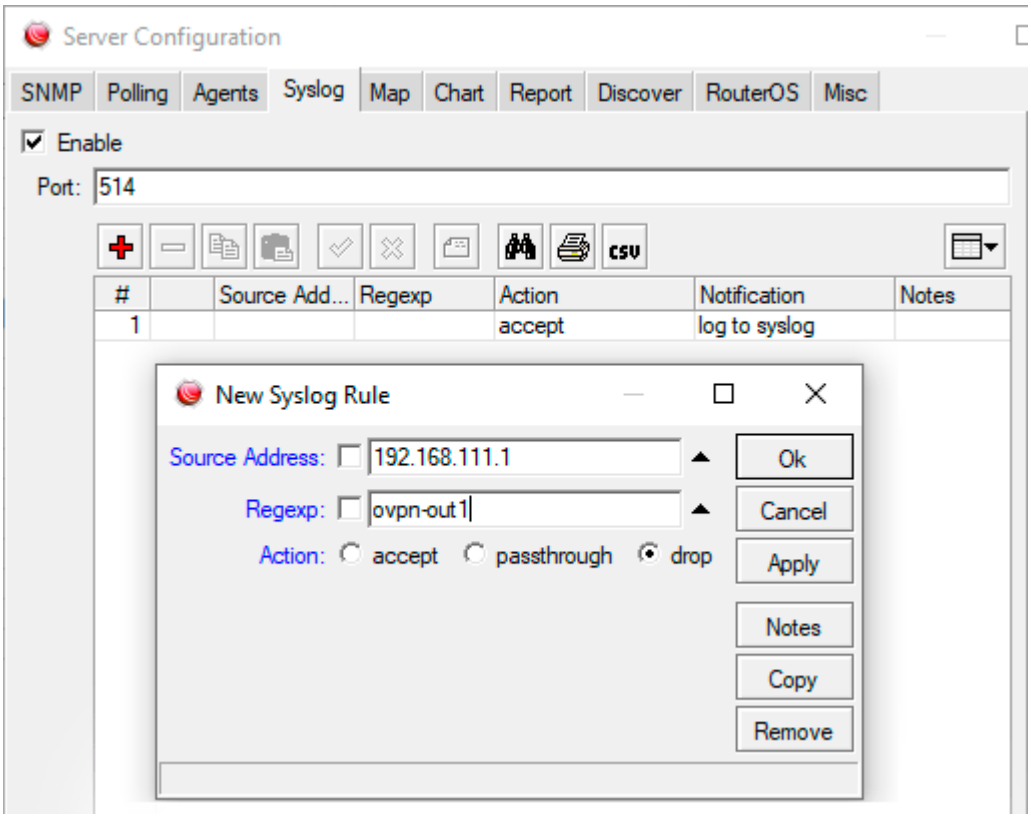


По умолчанию они все пишутся в **syslog**, в принципе это можно изменить, только практической пользы от этого немного, все, что изменится - это строка **Message**, что, учитывая отсутствие каких либо инструментов аналитики, практически ничего не даст.

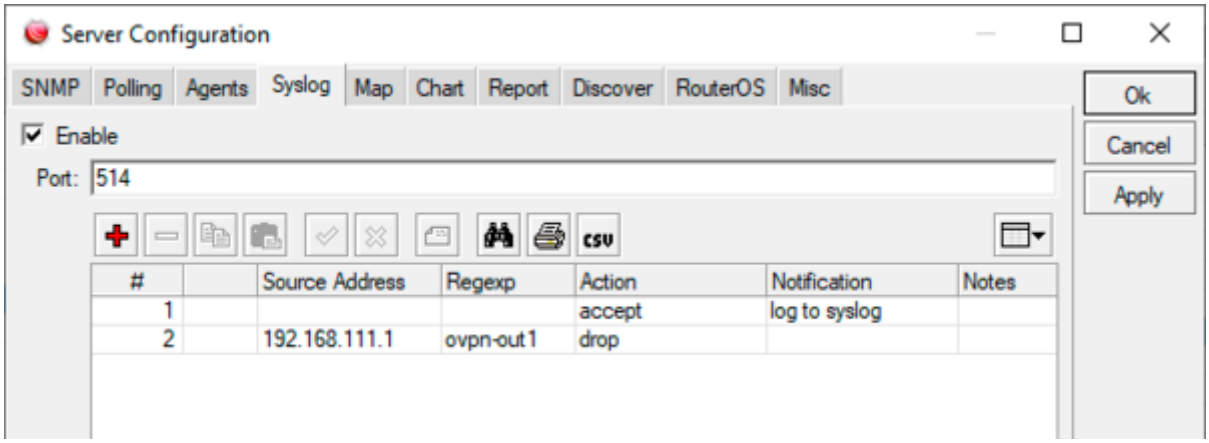
Исходя из того, что возможности хранения логов в The Dude ограничены 10 000 строк напрашивается вывод, что не следует отправлять на удаленный сервер все подряд, а только те логи, которые представляют практический интерес. Допустим мы хотим передавать на удаленный сервер события, связанные с подключением и отключением SSTP-клиентов. Находим в логе нужное событие и смотрим что указано в поле **Topics**, затем на основании полученных данных создаем новое правило:



Но фильтровать логи можно не только на стороне отправляющего устройства, но и со стороны The Dude. Если мы взглянем на приведенный выше лог, то увидим, что он заполнен событиями о неудачном подключении к некому OpenVPN-серверу, но это тестовый сервер и в настоящий момент он выключен, поэтому избавимся от этих событий в логе. Снова перейдем в **Settings - Syslog** и создадим нажатием на кнопку "плюс" новое правило. В поле **Source Address** укажем адрес источника, в поле **Regexp** - выражение по которому будем осуществлять фильтрацию, в нашем случае это часть строки, но вы можете использовать всю мощь регулярных выражений. И наконец действие с отобранными строками - **drop**.

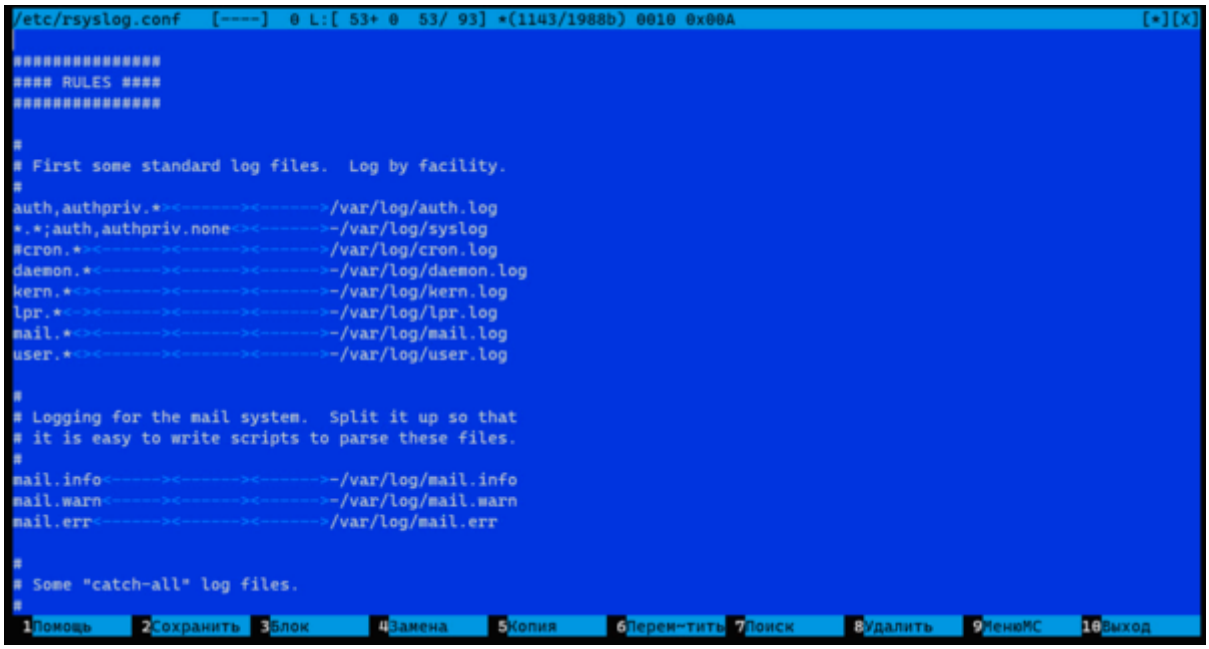


Создали правило, сохранили и... никакого эффекта... Почему? А потому что правила применяются в порядке их перечисления в списке и более общее правило перекрывает созданное нами более частное.



Способа изменить порядок правил в The Dude нет, но можно скопировать вышестоящее правило, после чего оно попадет в самый низ списка, а затем удалить его. После этого, когда правила выстроятся в правильном порядке, фильтр начнет работать. Неудобно? Да. Поэтому основную фильтрацию следует производить на конечных устройствах, которые отправляют логи.

Что еще можно делать при помощи сервера логов The Dude? Можно собирать логи с Linux узлов. Для этого откройте файл **/etc/rsyslog.conf** и перейдите в секцию Rules. Ее содержимое достаточно понятно и в комментариях не нуждается.



Допустим, мы хотим передавать на удаленный сервер содержимое **syslog**, для этого скопируем строку:

```
*.*;auth,authpriv.none      -/var/log/syslog
```

И приведем ее к виду:

```
*.*;auth,authpriv.none      @192.168.111.154:514
```

Где после символа @ укажем адрес нашего сервера логов и порт.

При этом не забываем, что возможности сервера логов The Dude имеют существенные ограничения и следует стараться максимально фильтровать логи, собирая только действительно нужную и полезную информацию.