Mikrotik

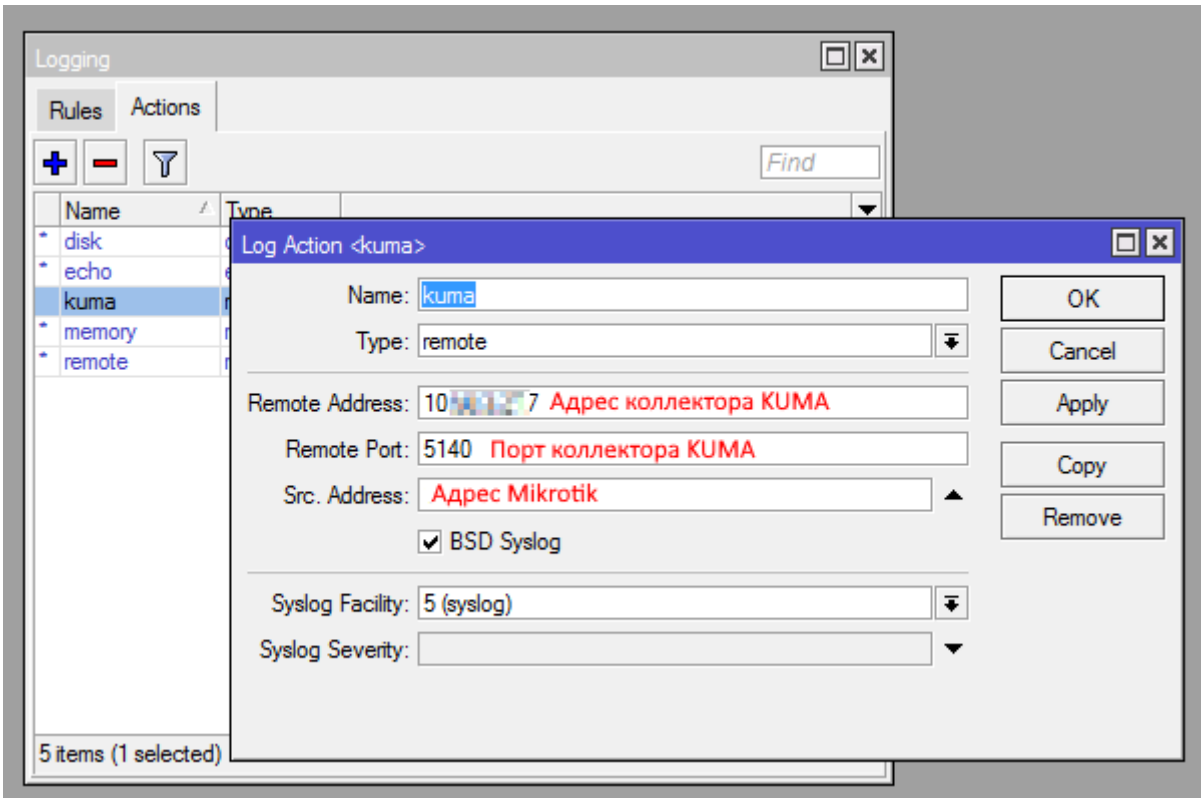
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Инструкция применима для MikroTik с RouterOS 6 и 7+

Настройка Mikrotik

Настройка может выполняется с помощью WinBox (рассматривается этот метод), либо через веб-интерфейс MikroTik RouterOS под учетной записью с правами администратора или через командную строку.

Перейдите в раздел **System - Logging**, во вкладке **Actions** добавляем новый элемент (по умолчанию используется протокол UDP):



Сохраните настройку, нажав **Apply** и **OK**.

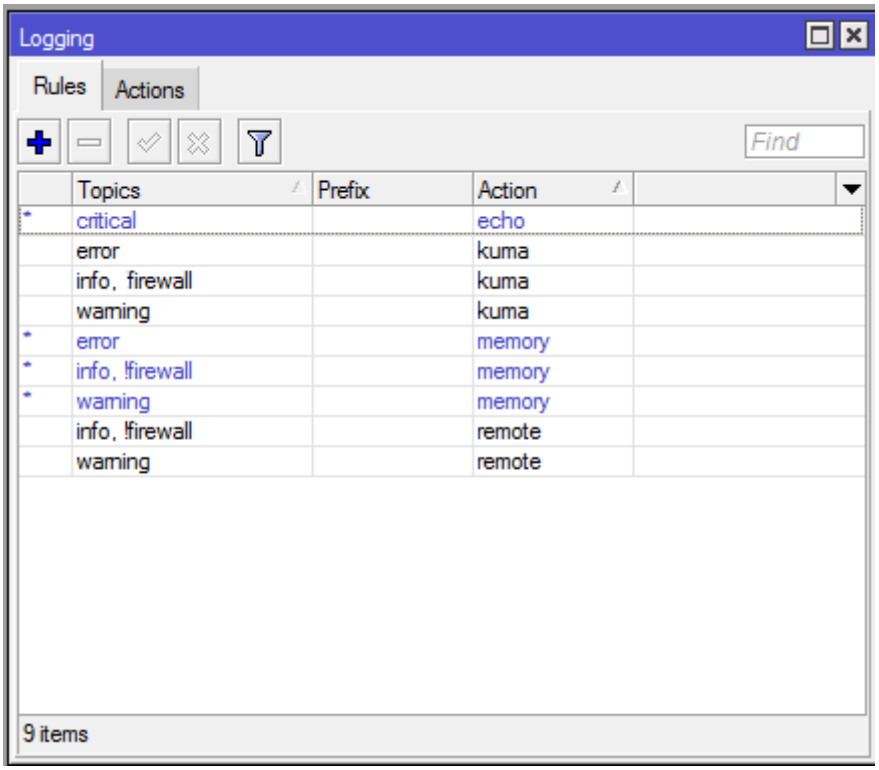
Настройка через командную строку:

```
/system logging action
/system/logging/action> add bsd-syslog=yes name=kuma remote=(KUMA_IP) remote=KUMA_PORT syslog-facility=syslog target=remote
```

Каждое событие в журналах Mikrotik может находиться одновременно в разных Topics, пример ниже:

#	Time	Buffer	Topics
933	Dec/01/2024 12:55:28	memory	ipsec, info
934	Dec/01/2024 13:06:03	memory	ipsec, info
935	Dec/01/2024 13:06:03	memory	ipsec, info
936	Dec/01/2024 15:25:05	memory	l2tp, ppp, info
937	Dec/01/2024 15:25:05	memory	l2tp, ppp, info, account
938	Dec/01/2024 15:25:05	memory	l2tp, ppp, info
939	Dec/01/2024 15:25:19	memory	ipsec, info
940	Dec/01/2024 15:25:20	memory	ipsec, info
941	Dec/01/2024 15:25:22	memory	ipsec, info
942	Dec/01/2024 15:25:22	memory	ipsec, info
943	Dec/01/2024 15:25:35	memory	ipsec, info
944	Dec/01/2024 15:25:36	memory	ipsec, info
945	Dec/01/2024 15:25:39	memory	l2tp, info
946	Dec/01/2024 15:25:39	memory	l2tp, ppp, info, account
947	Dec/01/2024 15:25:39	memory	l2tp, ppp, info
948	Dec/01/2024 15:25:39	memory	l2tp, ppp, info
949	Dec/01/2024 15:26:08	memory	ipsec, info
950	Dec/01/2024 15:26:08	memory	ipsec, info
951	Dec/01/2024 16:51:05	memory	l2tp, info
952	Dec/01/2024 16:52:12	memory	l2tp, info
953	Dec/01/2024 17:36:51	memory	ipsec, info
954	Dec/01/2024 17:36:51	memory	ipsec, info
955	Dec/01/2024 17:36:52	memory	ipsec, info
956	Dec/01/2024 18:18:54	memory	ipsec, info
957	Dec/01/2024 18:18:54	memory	ipsec, error
958	Dec/01/2024 18:18:54	memory	ipsec, error

В правилах логирования необходимо укаказать Topics, не пересекающиеся в других правилах. Иными словами, нужно создать отдельные правила с указанием отдельных Topics и если необходимо указать исключения, для категорий событий, которые не нужно отправлять на коллектора, установите флаг **!** перед Topics. В раскрывающемся списке Action выберите созданное ранее действие kuma, затем нажмите **OK**.



Настройка через командную строку:

```
/system logging
add topics=critical prefix=critical action=kuma
```

> При включении определенных Topics, особенно firewall может возрастать нагрузка на МЭ MikroTik, обращайте внимание на нагрузку системы после влючения логирования, особенно это касается моделей со слабой аппаратной начинкой

Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий MikroTik.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне MikroTik.

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] MikroTik syslog.**

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.

- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Revision #1
Created 4 December 2024 07:52:02 by Boris Rzr
Updated 4 December 2024 08:22:14 by Boris Rzr