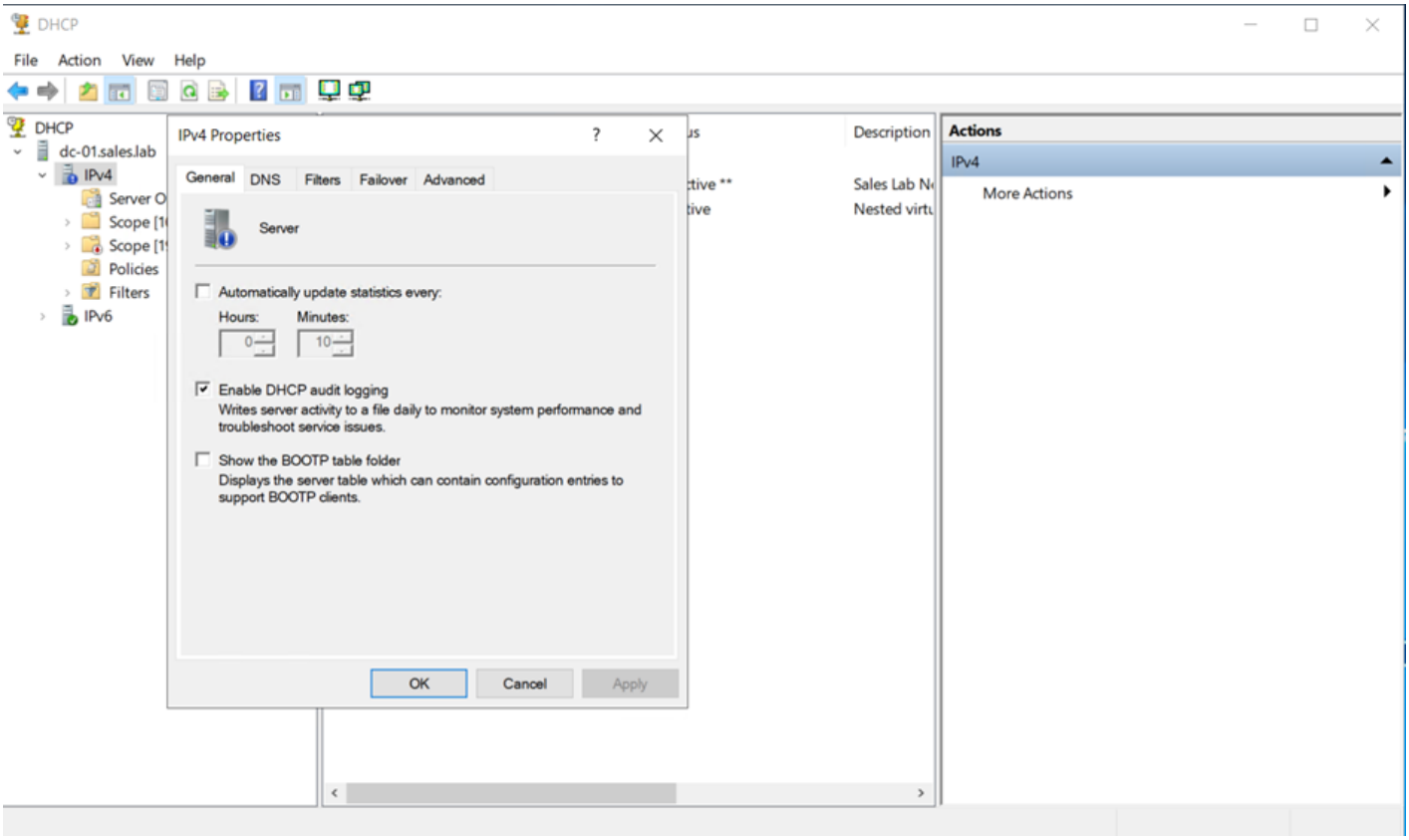
MS DHCP

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

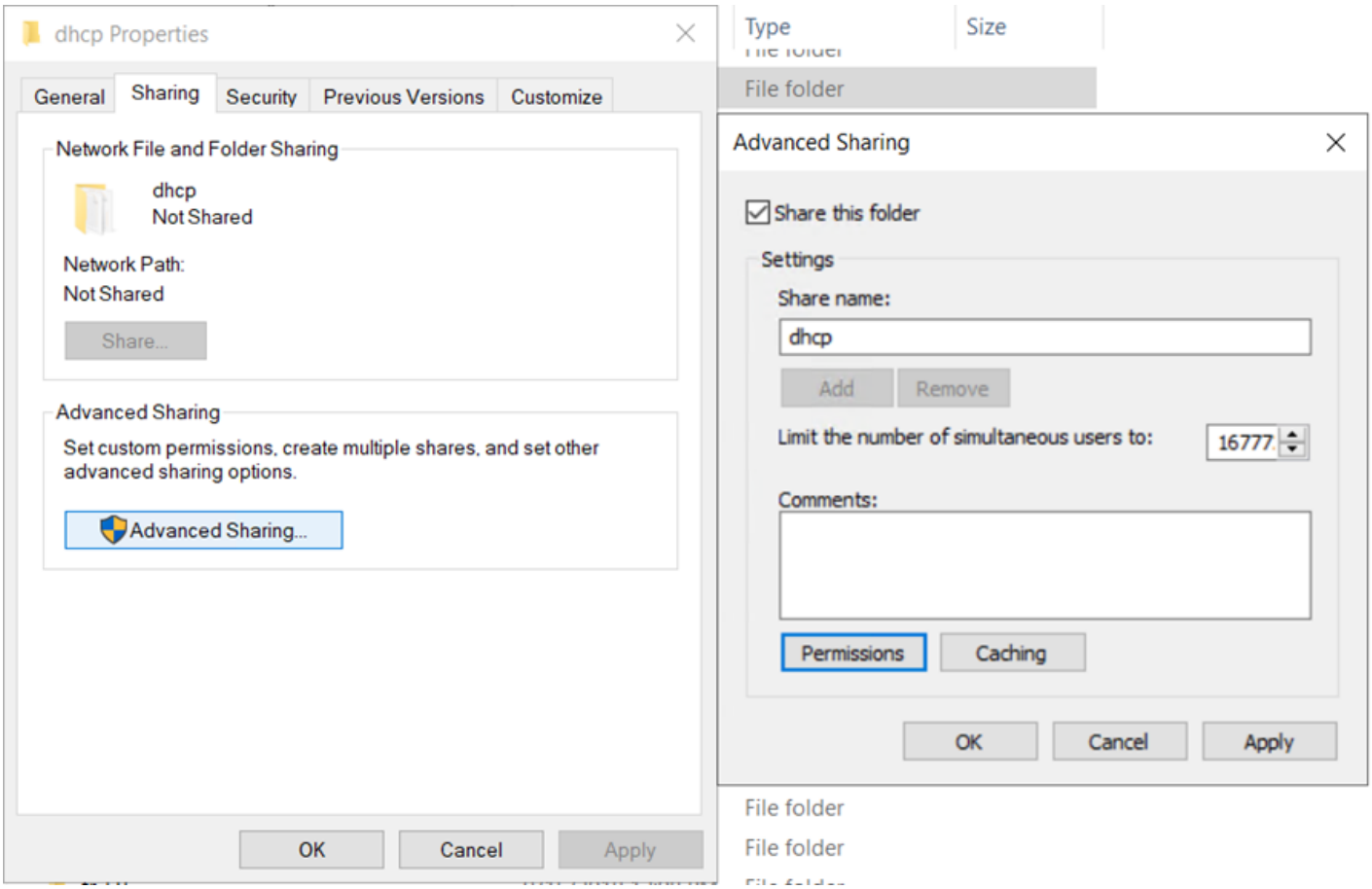
Настройка DHCP сервера

Передача событий из MS DHCP в KUMA осуществляется путем чтения лог файлов DHCP.

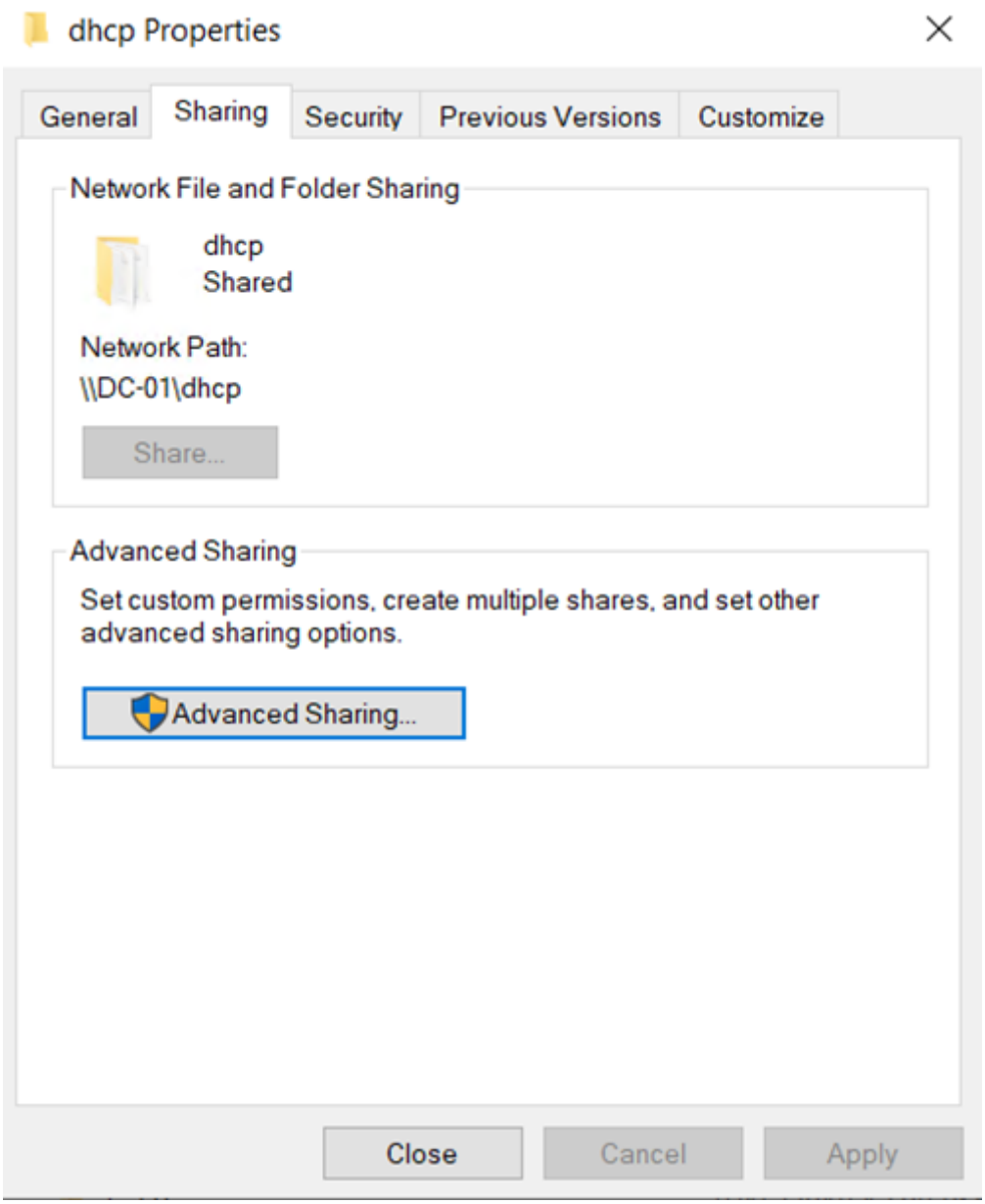
Откройте оснастку DHCP и убедитесь, что для DHCP сервера включено логирование.



События DHCP сервера пишутся в папку `C:\Windows\system32\dhcp\`. Для данной папки необходимо включить общий доступ на чтение.



После предоставления общего доступа у папки должен быть статус **Shared**.



Монтирование папки в KUMA

Для чтения файла логов коллектором KUMA необходимо примонтировать папку содержащую логи DHCP сервера на сервер коллектора KUMA.

Для начала необходимо установить утилиту **cifs**, если она еще не установлена.

```
yum install -y cifs-utils
```

Далее необходимо создать файл с учетными данными пользователя для доступа к общей папке **/root/.dhcp-secret** со следующим содержимым:

```
username=<имя пользователя с правами на чтение папки>
password=<пароль пользователя>
domain=<домен, в случае доменного пользователя>
```

Далее нужно создать папку на сервере коллектора KUMA, куда будет примонтирована папка с логами DNS сервера.

```
mkdir /mnt/dhcp
```

Далее в конец файла `/etc/fstab` необходимо добавить строку

```
\\<путь к общей папке сервера> <путь монтирования> cifs credentials=<файл с учетными данными>
0 0
```

Пример:

```
\\dc-01.sales.lab\dhcp /mnt/dhcp cifs credentials=/root/.dhcp-secret 0 0
```

Далее необходимо примонтировать общую папку командой:

```
mount -a
```

Для проверки успешности монтирования можно выполнить следующую команду:

```
ls /mnt/dhcp
```

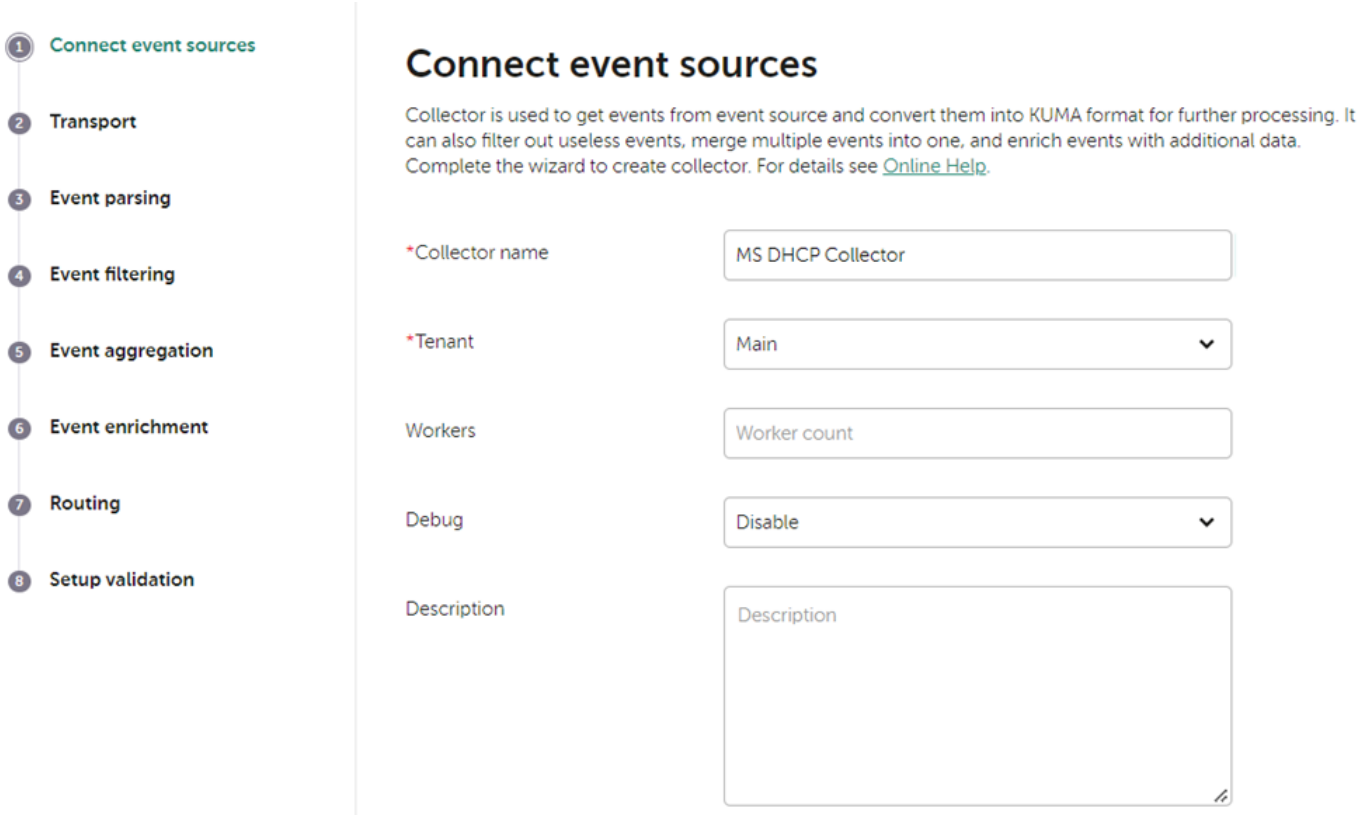
В выводе консоли должны присутствовать файлы логов DHCP сервера с правами на чтение для всех пользователей

```
[root@test-kuma ~]# ls -l /mnt/dhcp
total 32424
drwxr-xr-x 2 root root       0 Sep 19 12:42 backup
-rwxr-xr-x 1 root root   16384 Sep 19 12:42 dhcp.jfm
-rwxr-xr-x 1 root root 1048576 Sep 19 12:42 dhcp.mdb
-rwxr-xr-x 1 root root       0 Sep 19 12:42 dhcp.pat
-rwxr-xr-x 1 root root  287335 Sep 16 23:59 DhcpSrvLog-Fri.log
-rwxr-xr-x 1 root root  354767 Sep 19 12:54 DhcpSrvLog-Mon.log
-rwxr-xr-x 1 root root  644746 Sep 18 00:00 DhcpSrvLog-Sat.log
-rwxr-xr-x 1 root root  645334 Sep 19 00:00 DhcpSrvLog-Sun.log
-rwxr-xr-x 1 root root   11510 Sep 15 23:40 DhcpSrvLog-Thu.log
-rwxr-xr-x 1 root root  536088 Sep 13 23:39 DhcpSrvLog-Tue.log
-rwxr-xr-x 1 root root   10444 Sep 14 23:40 DhcpSrvLog-Wed.log
```

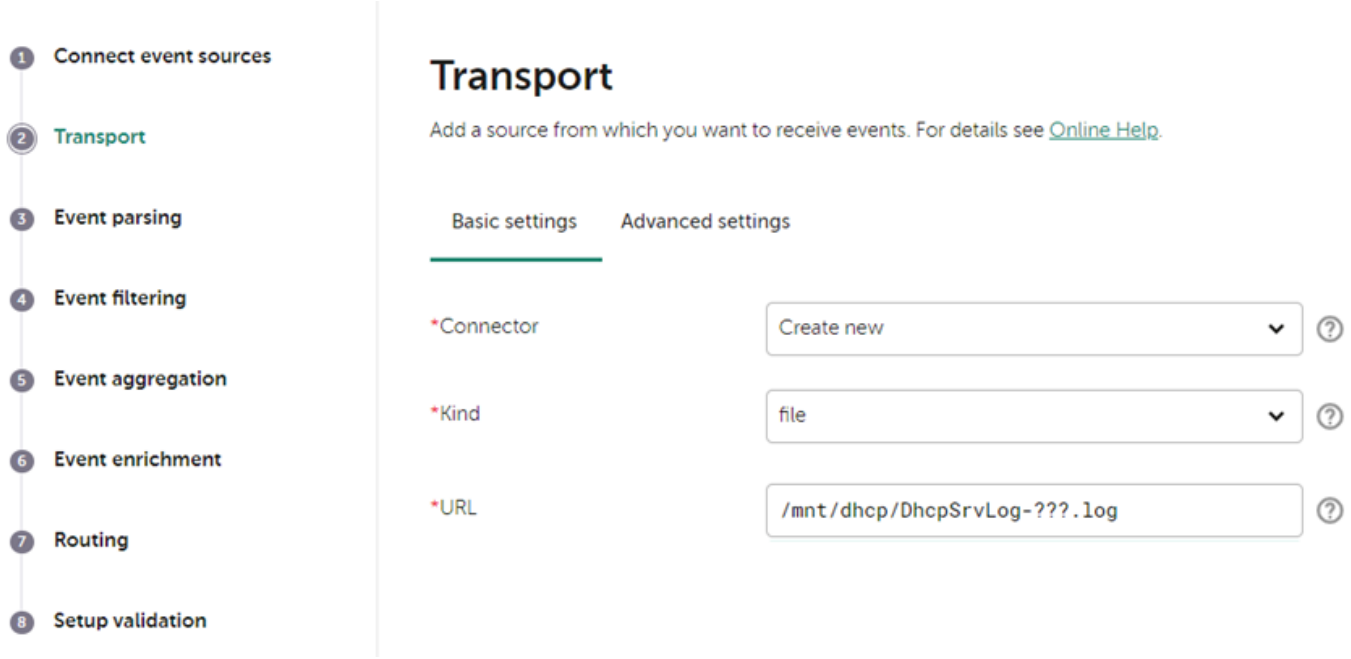
Создание коллектора KUMA

Для создания коллектора KUMA необходимо в веб-консоли KUMA перейти на вкладку **Ресурсы – Коллекторы** и нажать на кнопку **Добавить коллектор**. Также можно на вкладке **Ресурсы** выбрать пункт **Подключить источник**. В обоих случая откроется мастер подключения источников событий.

На первом шаге мастера необходимо выбрать **Тенант**, которому будет принадлежать коллектор и также задать **Имя коллектора**.



На втором шаге мастера необходимо выбрать тип подключения **file** и указать **маску пути** для файлов логов DHCP сервера.



Поддерживаемые маски:

- `*` – соответствует любой последовательности символов;
- `[' [ '^' ] { диапазон символов } ']` – класс символов (не должен быть пустым);
- `?` – соответствует любому одиночному символу.

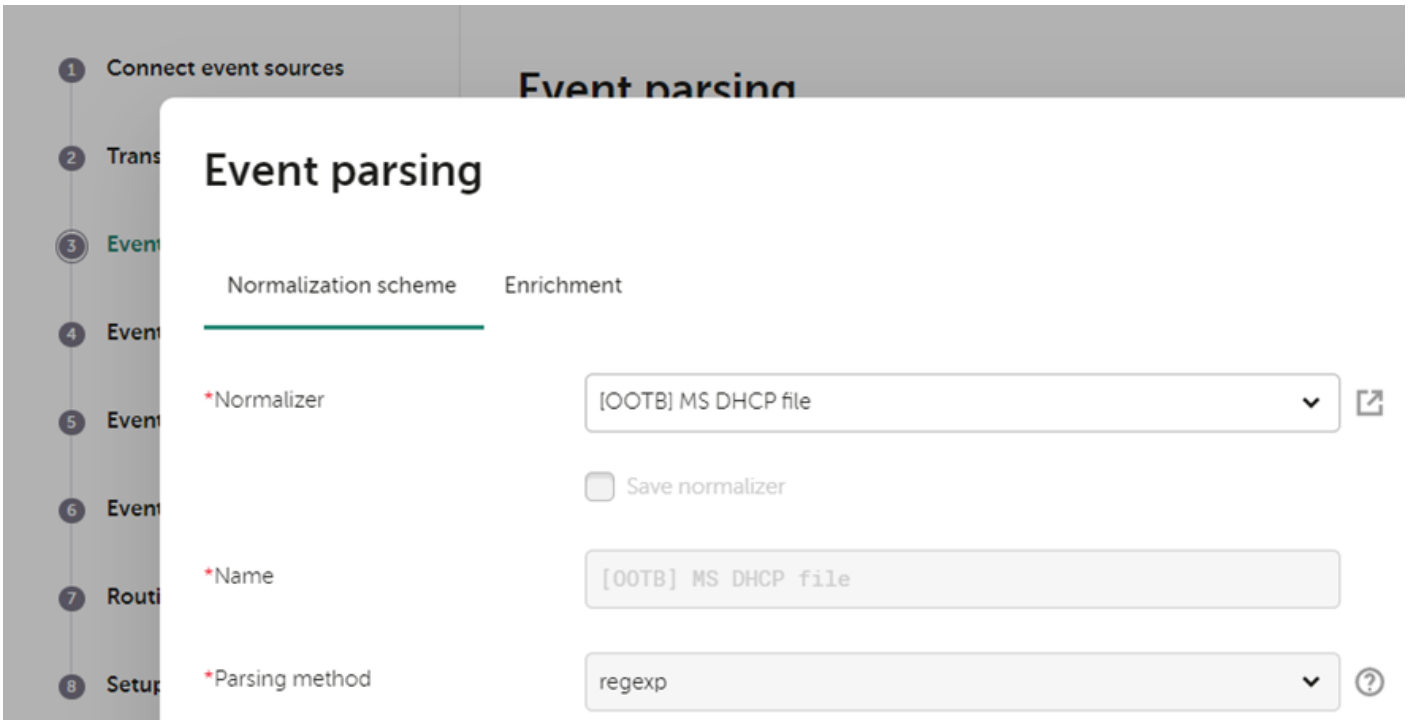
Диапазоны символов:

- `[0-9]` – числа;
- `[a-zA-Z]` – буквы латинского алфавита.

Примеры:

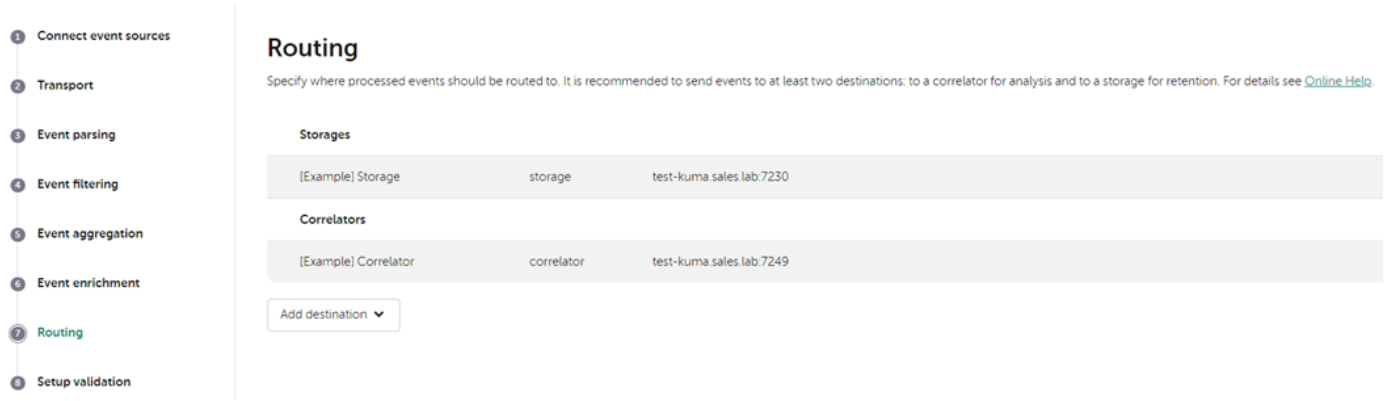
- `/var/log/*som?[1-9].log`
- `/mnt/dns_logs/*/dns.log`
- `/mnt/proxy/access*.log`

На третьем шаге мастера необходимо выбрать предустановленный нормализатор **[OOTB] MS DHCP file**. В случае отсутствия указанного нормализатора, обратитесь к своему менеджеру для его получения.

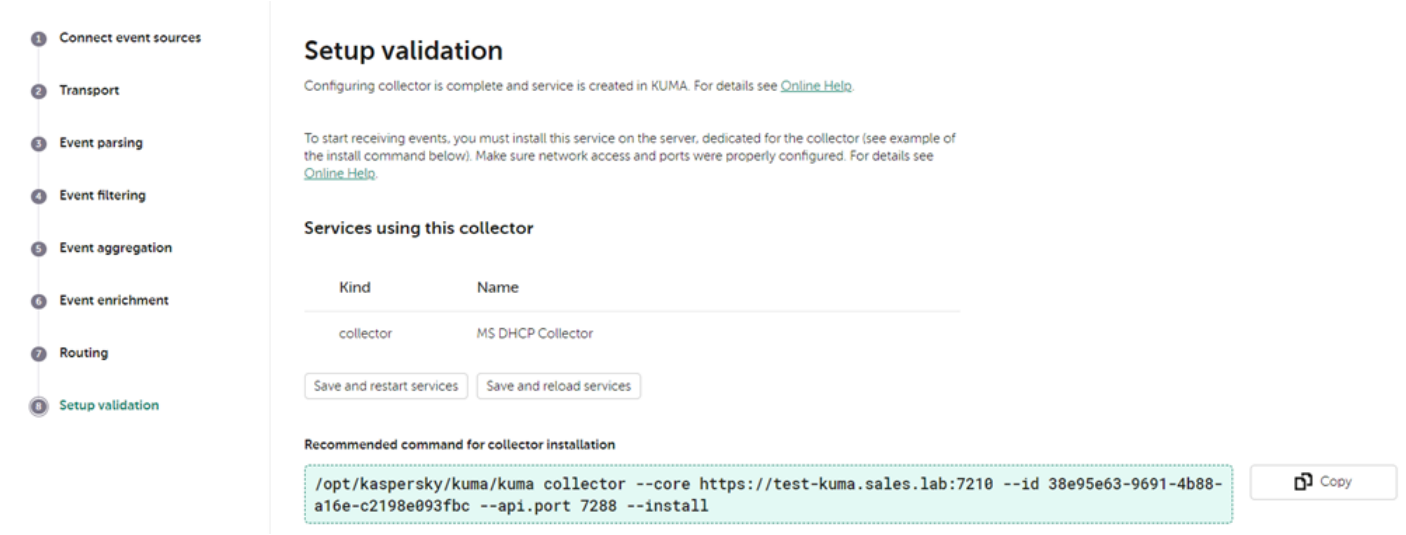


Шаги мастера с четвертого по шестой можно пропустить, либо заполнить позднее по своему усмотрению.

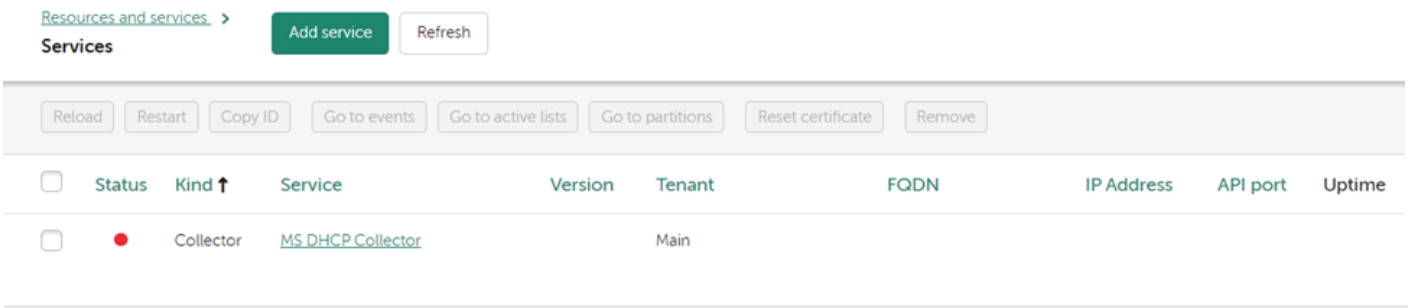
На седьмом шаге мастера необходимо указать точки назначения типа **Хранилище**, если требуется сохранение событий в БД и типа **Коррелятор**, если требуется корреляция событий.



На последнем шаге мастера необходимо нажать на кнопку **Сохранить и создать сервис**, после чего скопировать появившуюся команду для дальнейшей установки сервиса коллектора.



В результате на вкладке **Ресурсы – Активные сервисы** появится созданный сервис коллектора.



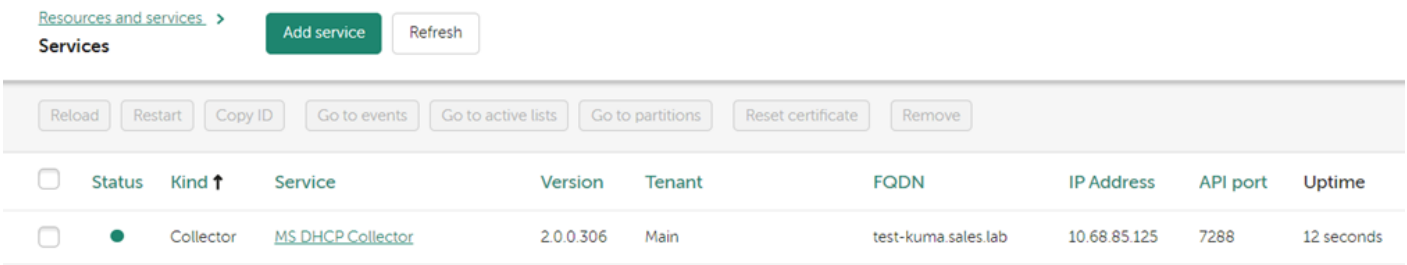
Установка коллектора KUMA

Для установки сервиса коллектора необходимо подключиться к консоли сервера коллектора KUMA.

Для установки сервиса коллектора необходимо выполнить скопированную команду.

```
[root@test-kuma ~]# /opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 38e95e63-9691-4b88-a16e-c2198e093fbc
--api.port 7288 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-38e95e63-9691-4b88-a16e-c2198e093fbc.service → /usr/lib/system
d/system/kuma-collector-38e95e63-9691-4b88-a16e-c2198e093fbc.service.
[root@test-kuma ~]#
```

В результате статус коллектора в веб-интерфейсе KUMA изменится на **зеленый**.



Для проверки поступления событий выберите соответствующий коллектор (галочка слева) и нажмите на кнопку **Перейти к событиям**. В открывшемся окне события при нажатии на значок лупы должны появиться события DHCP сервера.

Revision #8
Created 2023-08-11 06:59:13 UTC by Boris Rzr
Updated 2025-01-24 10:28:54 UTC by Koala