MS DNS

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

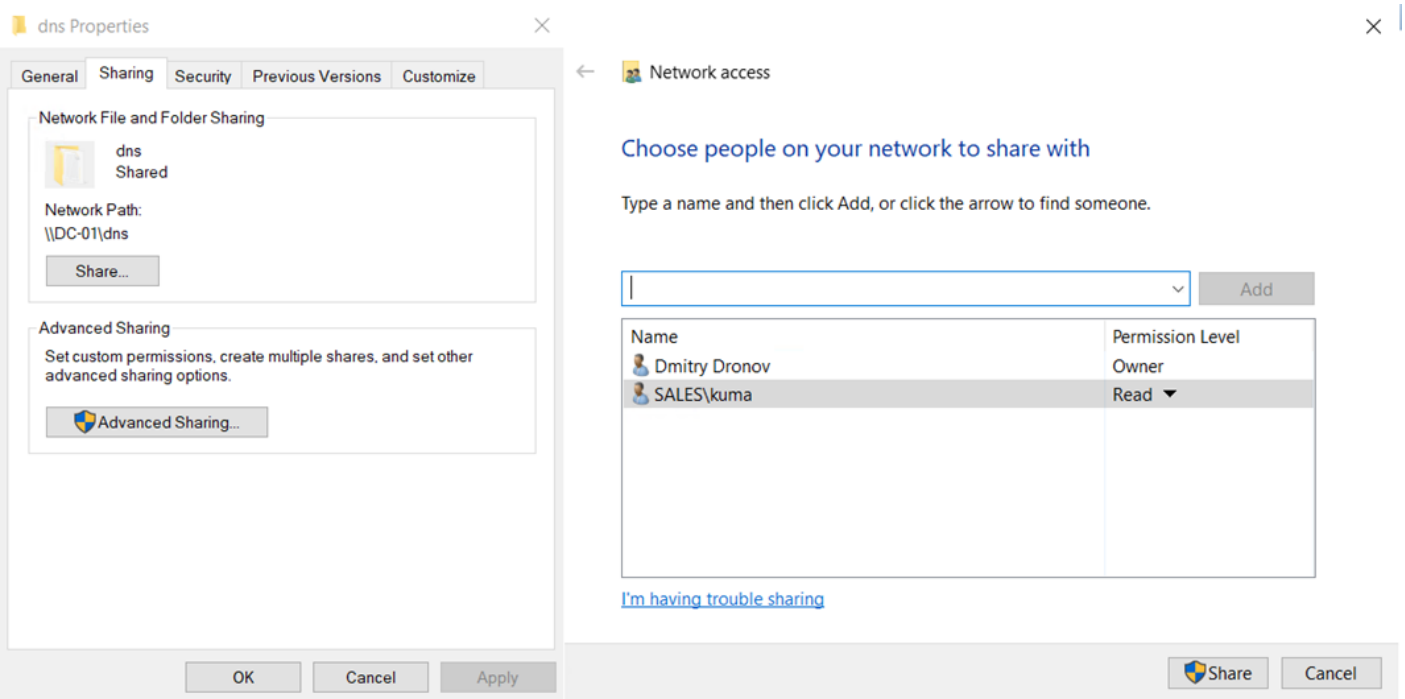
> Для KUMA 3.2 добавился новый способ сбора DNS логов в формате ETW. Подробнее в статье: https://kb.kuma-community.ru/books/podkliucenie-istocnikov/page/ms-etw-dns-analytics-kuma-32

????????? DNS ???????

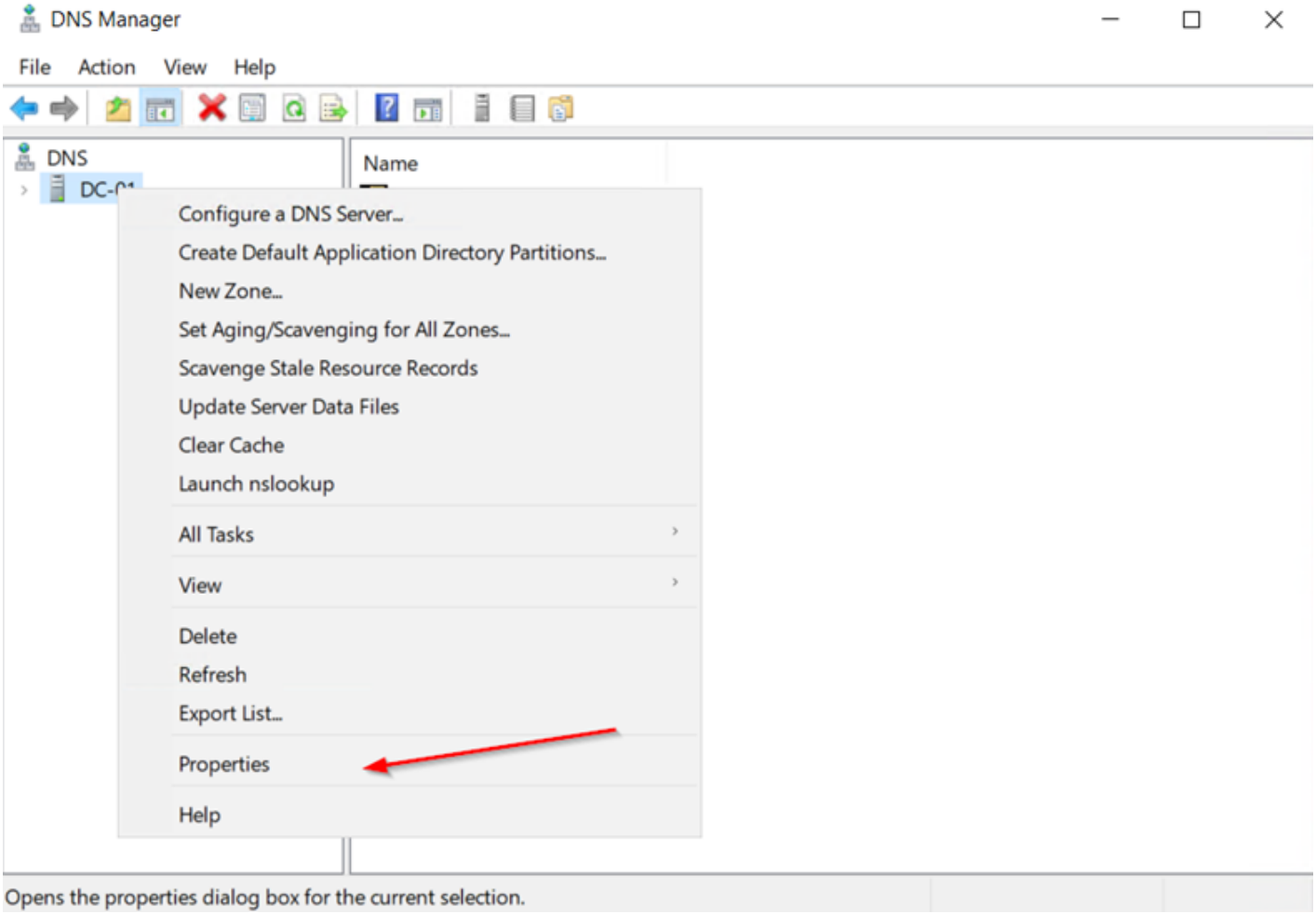
Передача событий из MS DNS в KUMA осуществляется путем чтения лог файла DNS. По умолчанию запись событий в файл на DNS сервере выключена.

Чтобы включить логирование событий DNS в файл необходимо для начала создать папку, в которую будут записываться файлы событий DNS. Например, `C:\dns`.

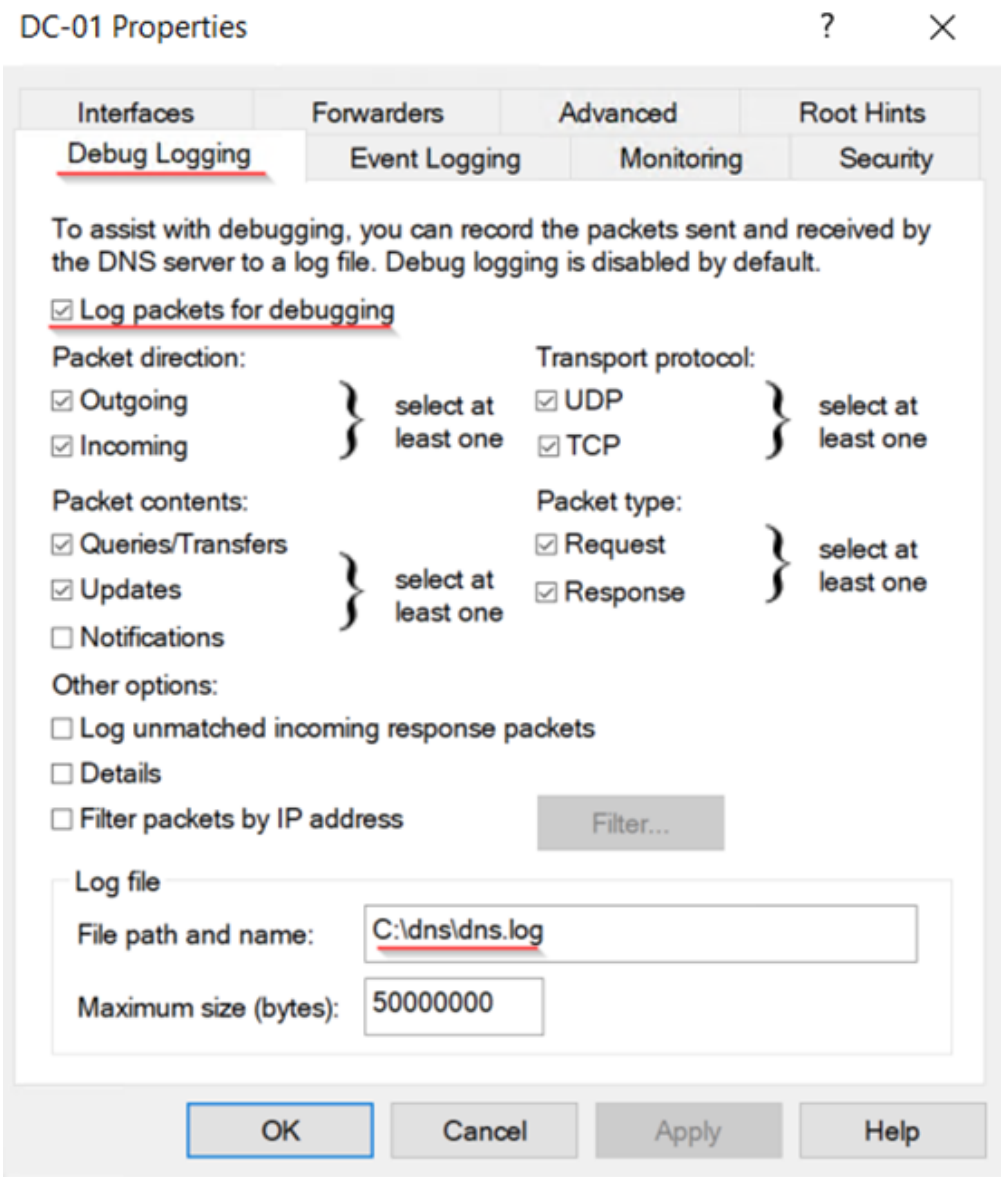
После создания папки необходимо разрешить общий доступ на чтение к этой папке. Рекомендуется создать отдельного пользователя для этой операции.



Далее необходимо запустить оснастку **DNS Manager**, выбрать нужный DNS сервер и перейти в свойства.



В свойствах сервера необходимо перейти на вкладку **Debug Logging**, включить расширенное логирование и задать путь к файлу, в который будут записывать слоги DNS сервера. Размер лог файла рекомендуется 50 Мб.



????????????? ????? ? KUMA

Для чтения файла логов коллектором KUMA необходимо примонтировать папку содержащую логи DNS 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/.dns-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/dns
```

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

```
\\<путь к общей папке сервера> <путь монтирования> cifs credentials=<файл с учетными данными>,cache=none 0 0
```

Пример:

```
\\dc-01.sales.lab\dns /mnt/dns cifs credentials=/root/.dns-secret,cache=none 0 0
```

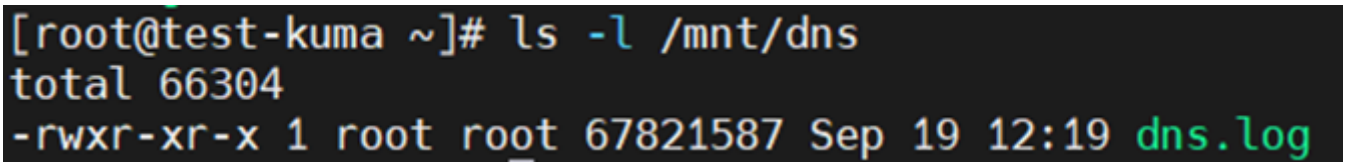
Далее необходимо примонтировать общую папку командой:

```
mount -a
```

Для проверки успешности монтирования можно выполнить следующую команду:

```
ls /mnt/dns
```

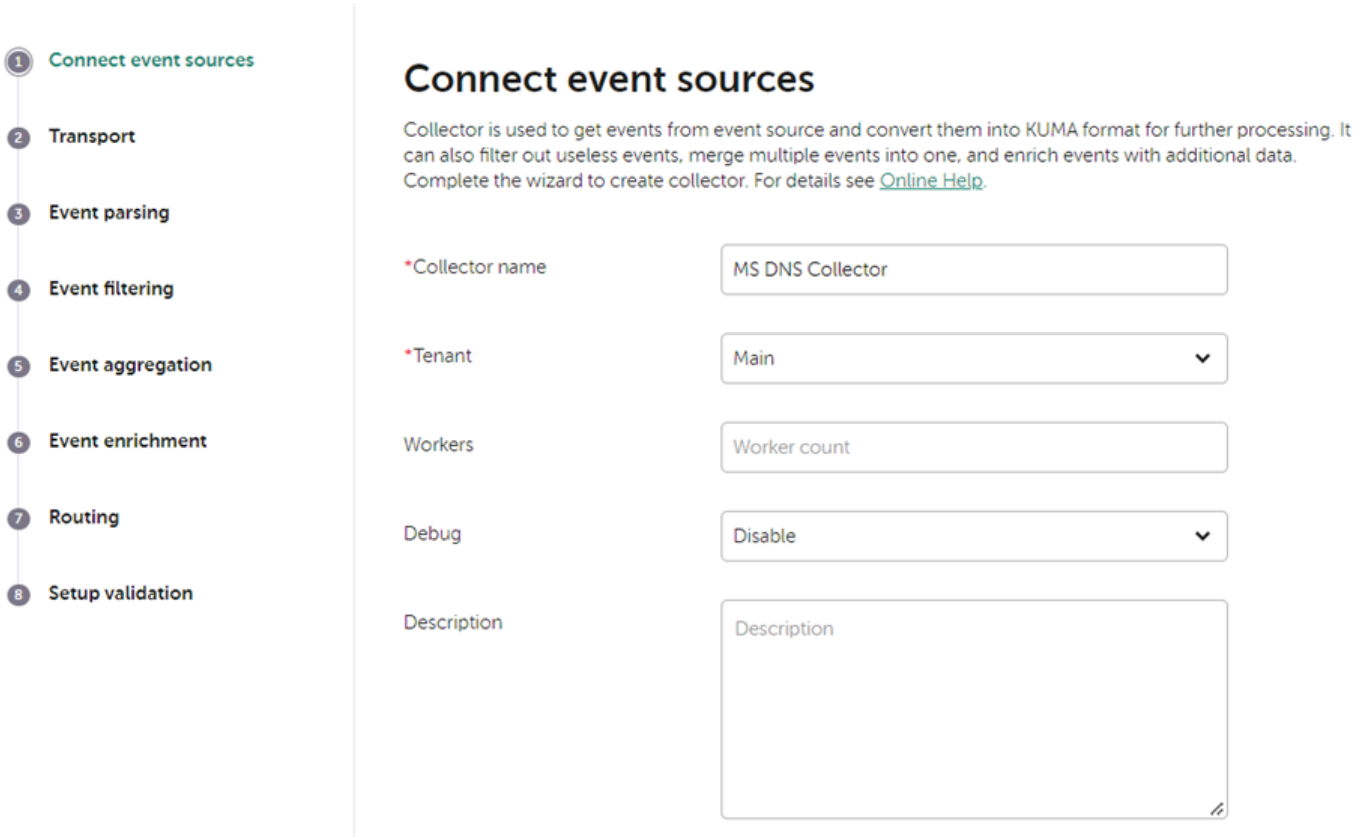
В выводе консоли должен присутствовать файл логов DNS сервера с правами на чтение для всех пользователей



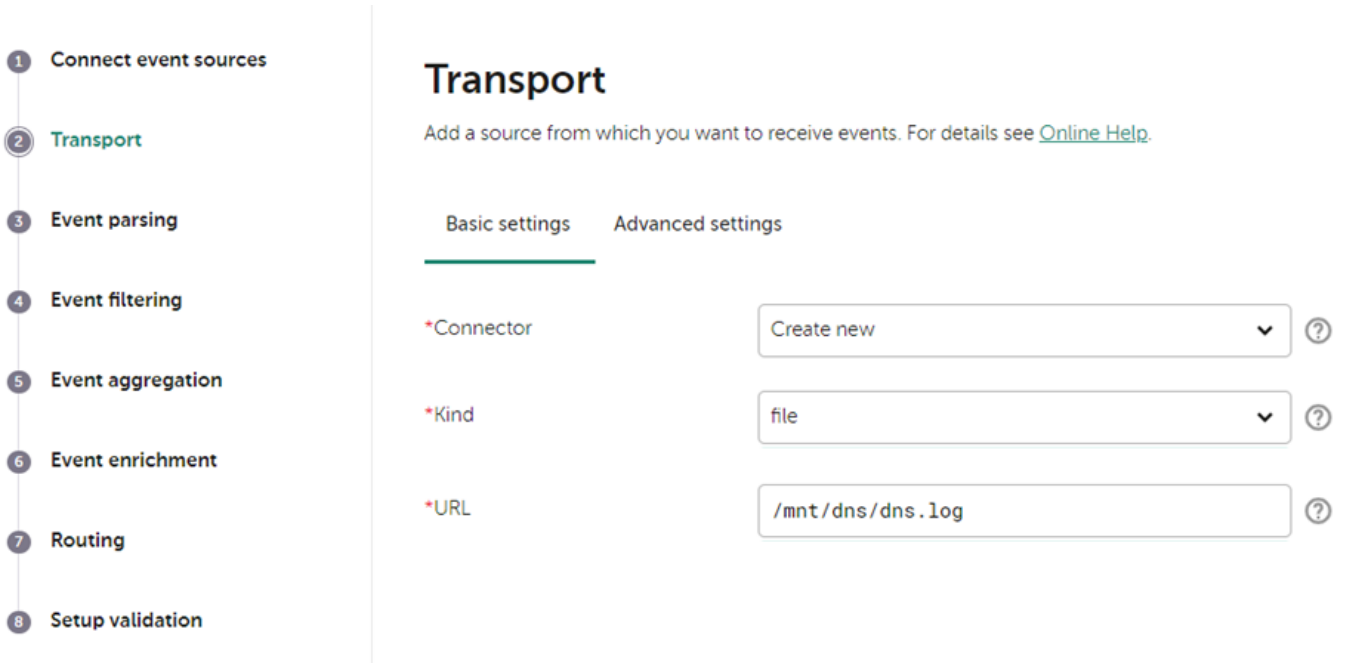
???????? ??????????? KUMA

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.

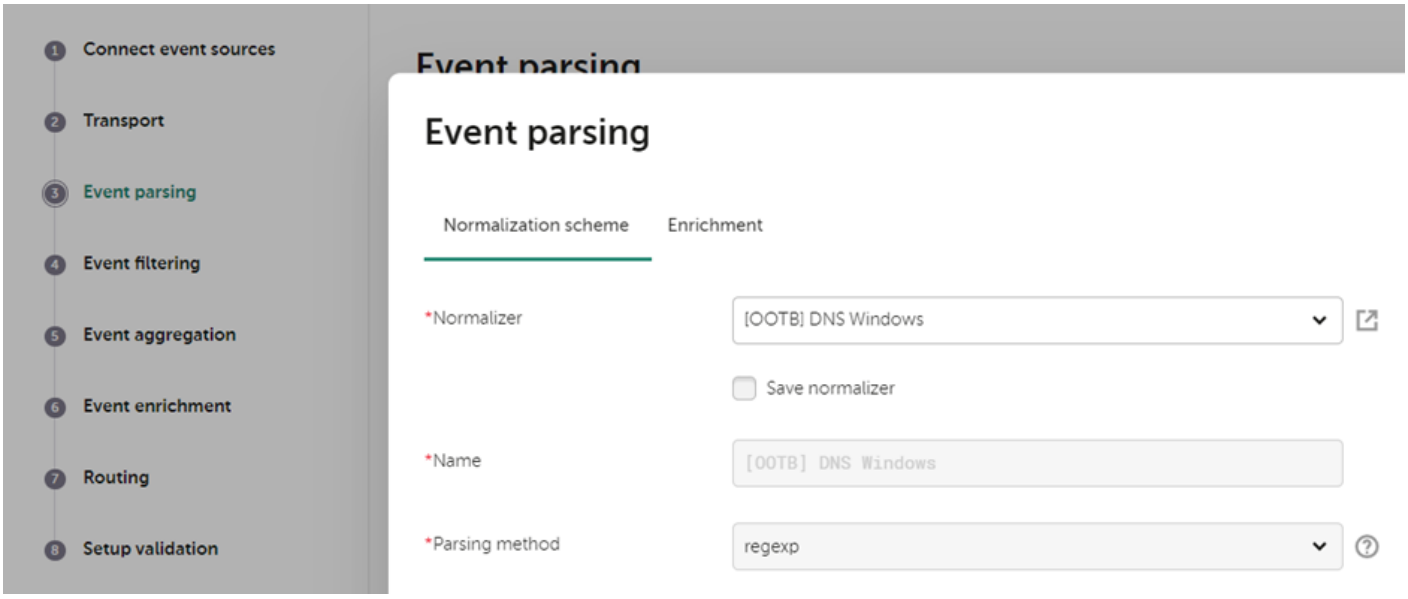
На первом шаге мастера необходимо выбрать **Тенант**, которому будет принадлежать коллектор и также задать **Имя** коллектора.



На втором шаге мастера необходимо выбрать тип подключения file и указать **папку** сервера коллектора, куда примонтирована папка с логами DNS сервера.

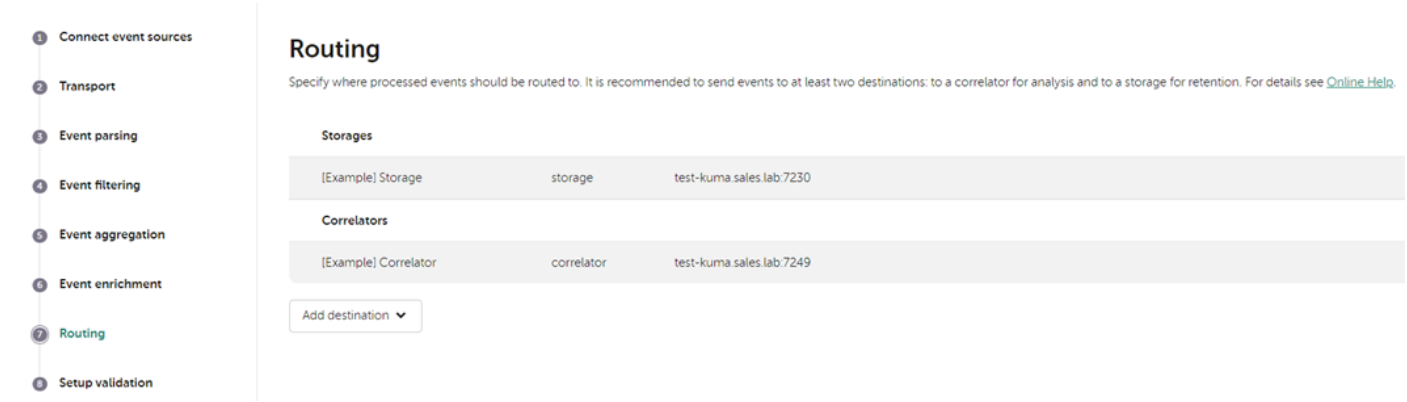


На третьем шаге мастера необходимо выбрать предустановленный нормализатор **[OOTB] DNS Windows**. В случае отсутствия указанного нормализатора, обратитесь к своему менеджеру для его получения.

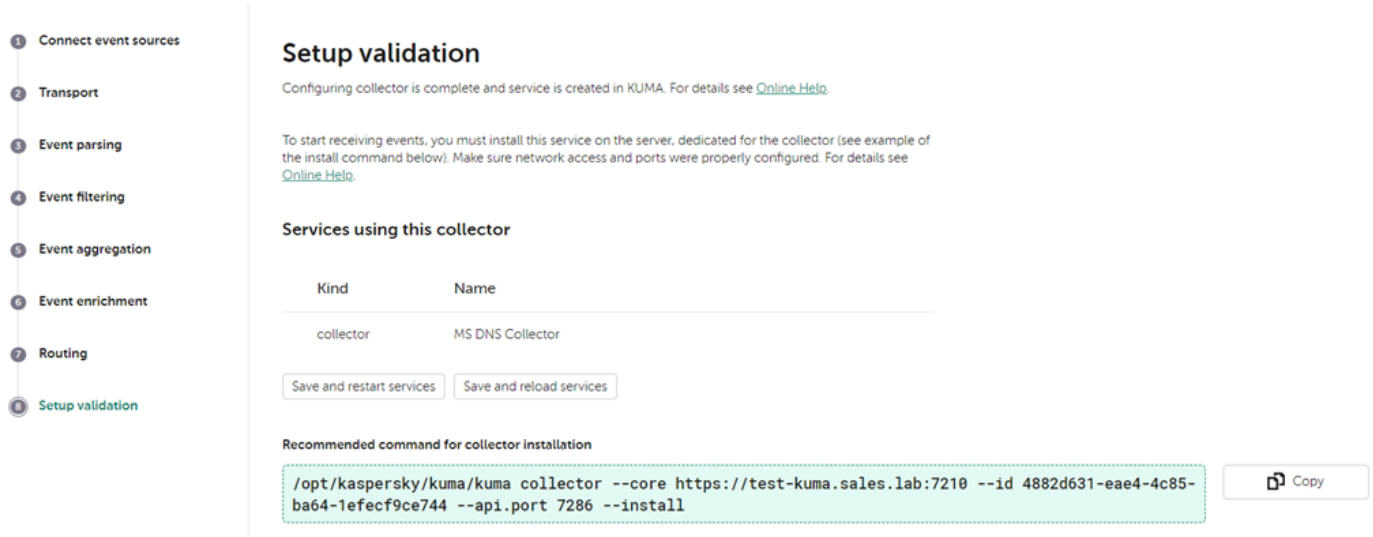


Шаги мастера с четвертого по шестой можно пропустить, либо заполнить позднее по своему усмотрению.

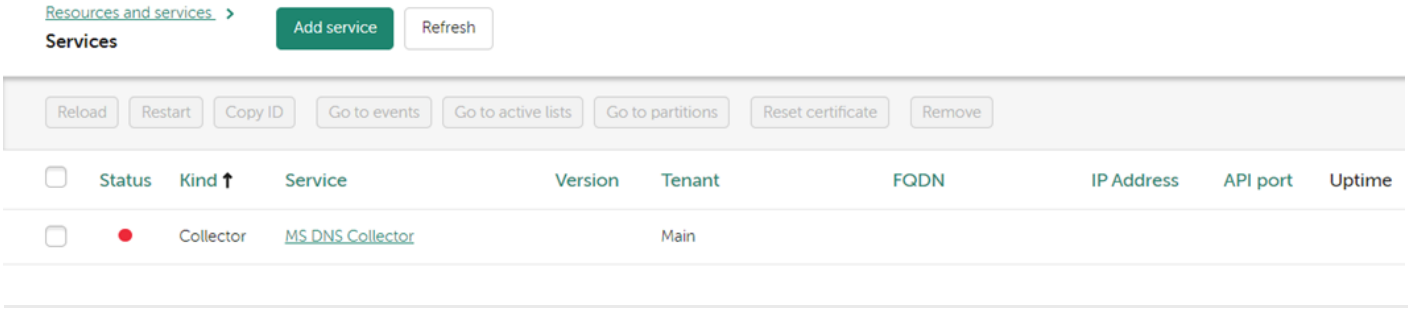
На седьмом шаге мастера необходимо указать точки назначения типа **Хранилище**, если требуется сохранение событий в БД и типа **Коррелятор**, если требуется корреляция событий.



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



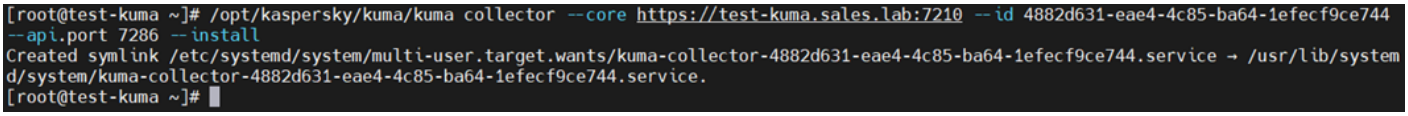
В результате на вкладке **Ресурсы – Активные сервисы** появится созданный сервис коллектора.



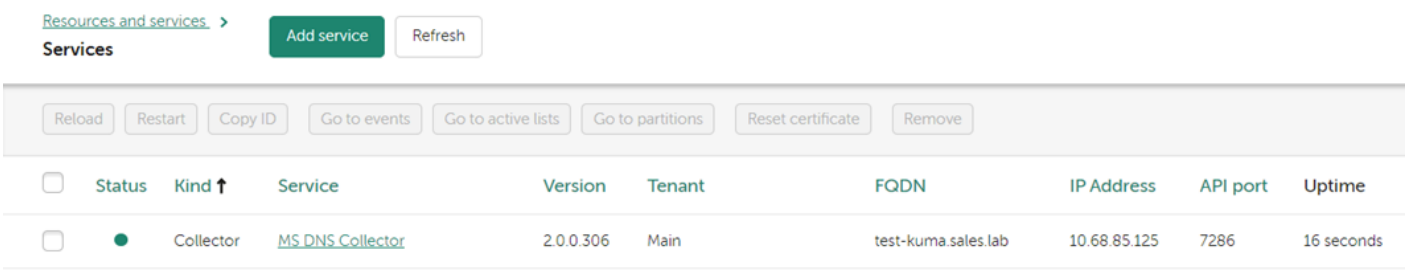
????????? ??????????? KUMA

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

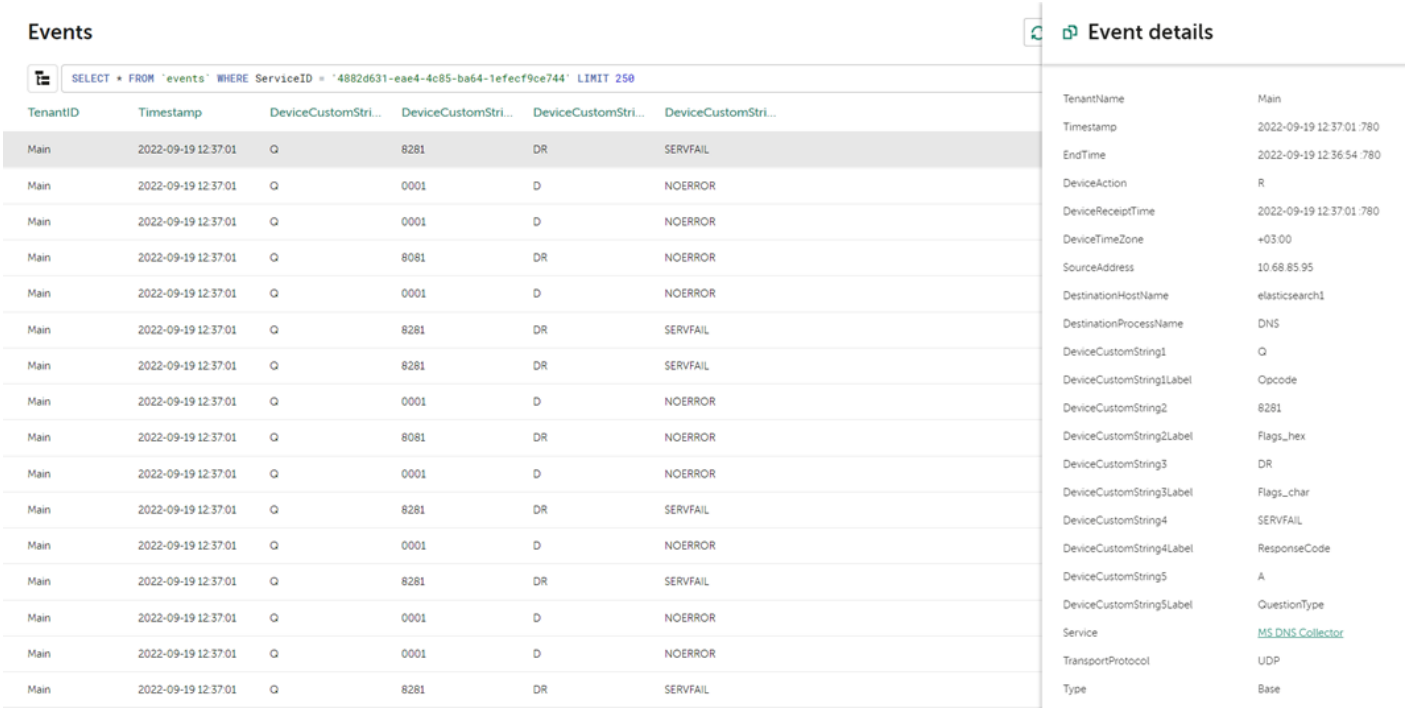
Для установки сервиса коллектора необходимо выполнить скопированную команду.



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 DNS сервера.



Revision #12
Created 10 August 2023 12:17:51 by Boris Rzr
Updated 24 January 2025 10:28:31 by Koala