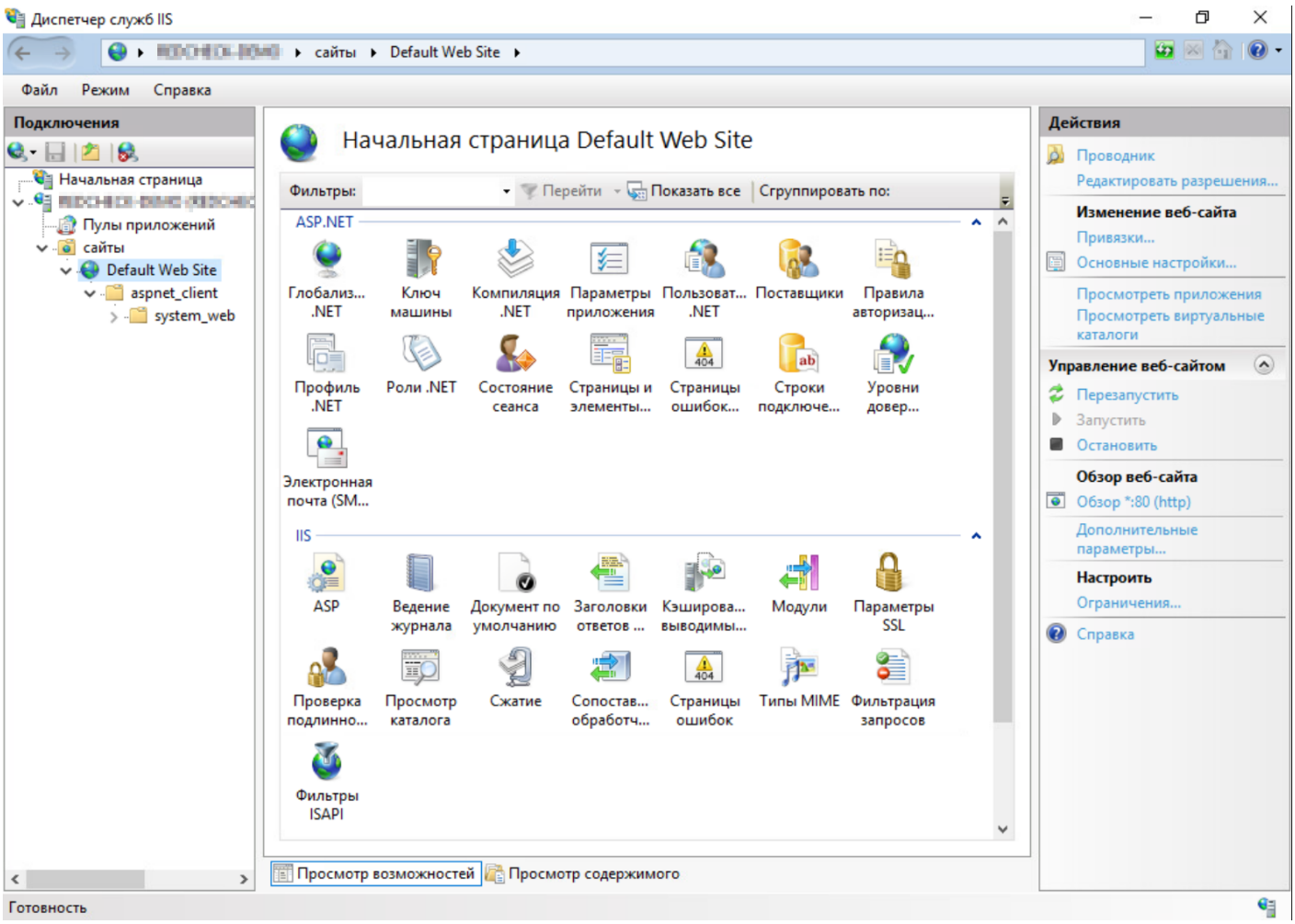
IIS

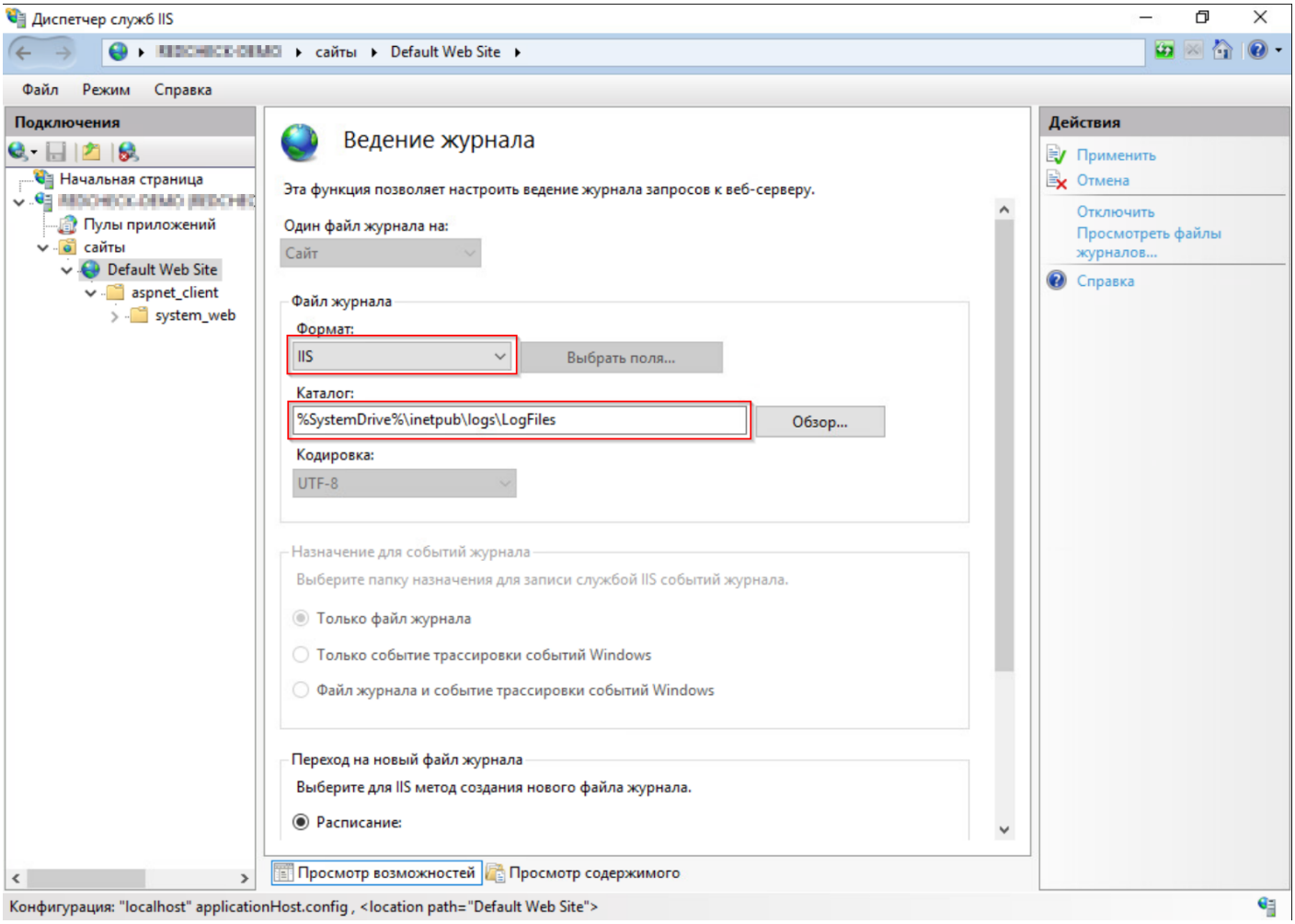
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Настройка IIS сервера

1. Откройте диспетчер служб IIS и перейдите в настройки требуемого сайта

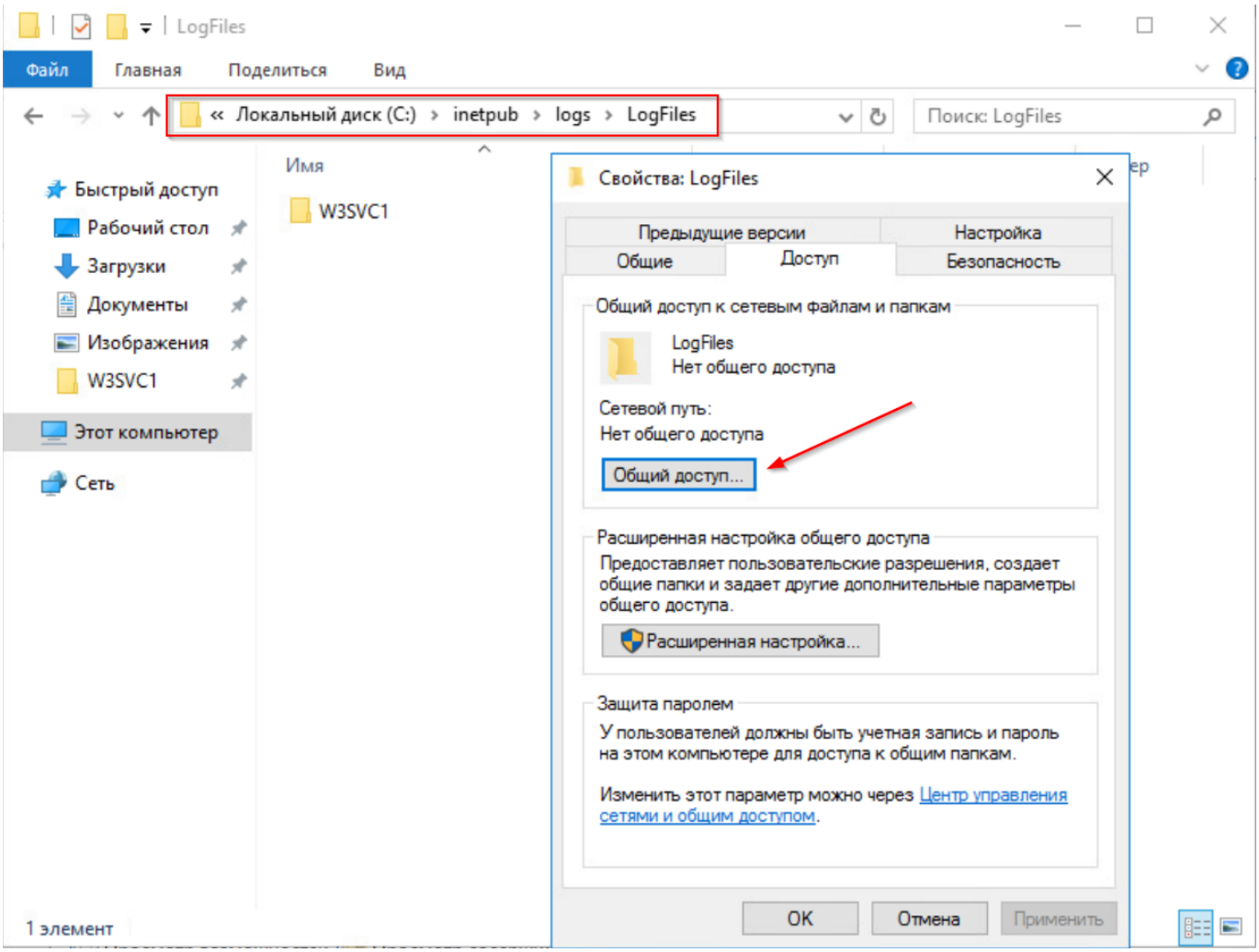


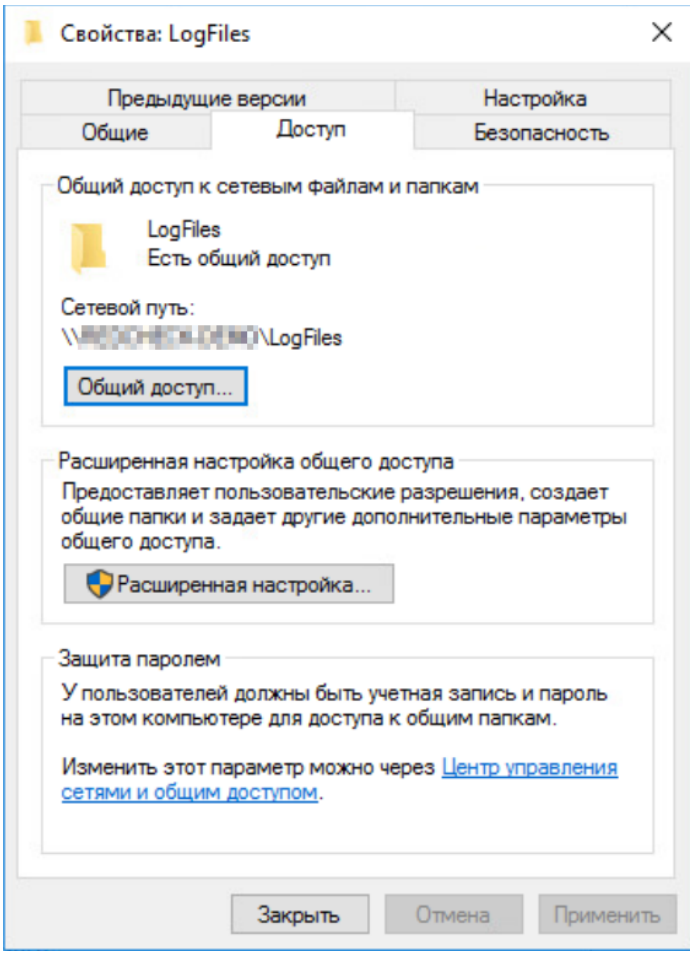
2. В разделе IIS выберите "Ведение журнала". Задайте формат журнала "IIS" и укажите папку для хранения логов. После выполнения настроек в окне "Действия" нажмите применить.



> Формат логов должен быть именно **IIS** для возможности использования коробочного нормализатора
>
> Подробнее про данный формат логов: https://learn.microsoft.com/en-us/windows/win32/http/iis-logging

3. По умолчанию лог IIS будет записан в папку `C:\inetpub\logs\LogFiles`. Для данной папки необходимо включить общий доступ на чтение.


LogFiles
Файл
Главная
Поделиться
Вид
« Локальный диск (C:) › inetpub › logs › LogFiles
Поиск: LogFiles
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
W3SVC1
Этот компьютер
Сеть
Имя
W3SVC1
1 элемент
Свойства: LogFiles
Предыдущие версии
Настройка
Общие
Доступ
Безопасность
Общий доступ к сетевым файлам и папкам
LogFiles
Нет общего доступа
Сетевой путь:
Нет общего доступа
Общий доступ...
Расширенная настройка общего доступа
Предоставляет пользовательские разрешения, создает общие папки и задает другие дополнительные параметры общего доступа.
Расширенная настройка...
Защита паролем
У пользователей должны быть учетная запись и пароль на этом компьютере для доступа к общим папкам.
Изменить этот параметр можно через Центр управления сетями и общим доступом.
OK
Отмена
Применить



Монтирование папки в KUMA

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

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

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

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

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

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

```
mkdir /mnt/iis
```

4. 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:

```
\\iis.demo.lab\dhcp /mnt/iis cifs credentials=/root/.iis-secret,cache=none 0 0
```

5. Далее необходимо примонтировать общую папку командой:

```
mount -a
```

Для проверки успешности монтирования можно выполнить следующую команду:

```
ls /mnt/iis
```

6. Убедитесь, что у пользователя kuma есть права на чтение файлов логов из данной директории, а также возможность просматривать директории по пути к логам.

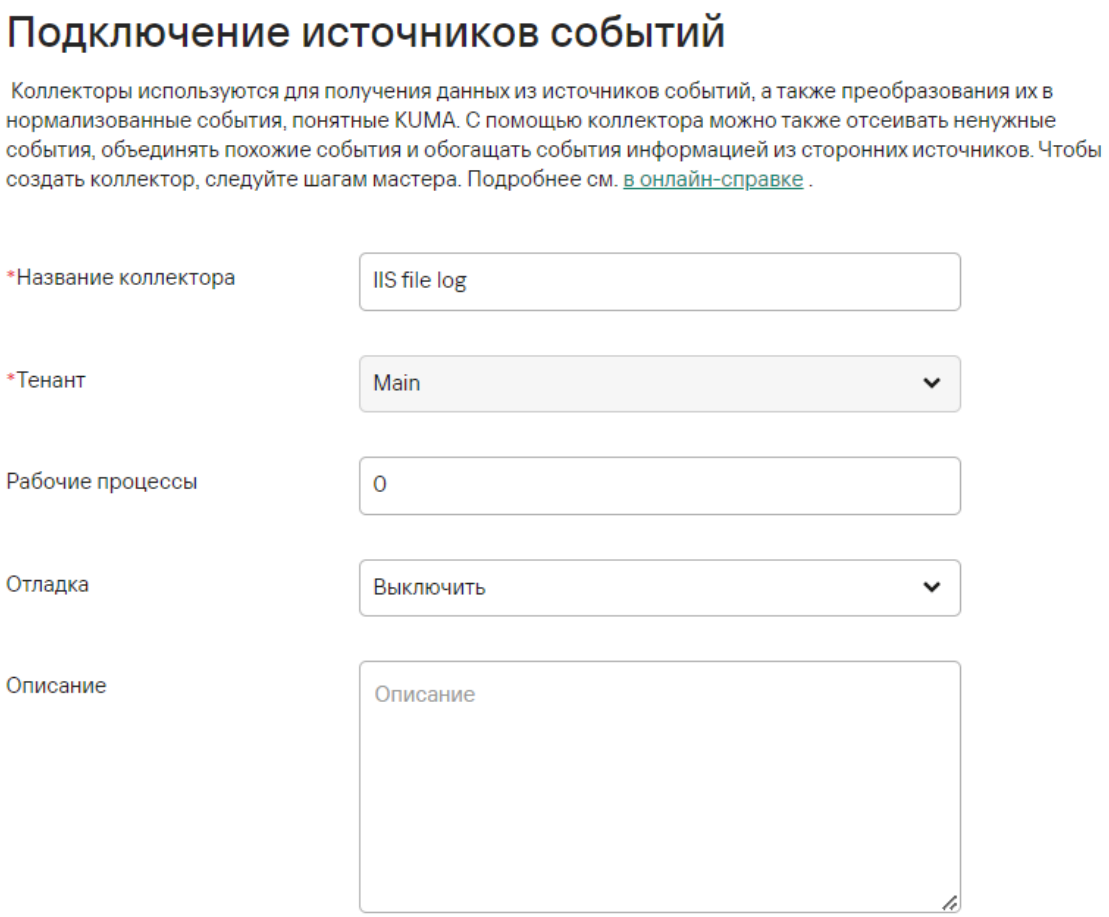
Альтернативно, можно назначить пользователя kuma владельцем примонтированной папки:

```
chown -R kuma:kuma /mnt/iis
```

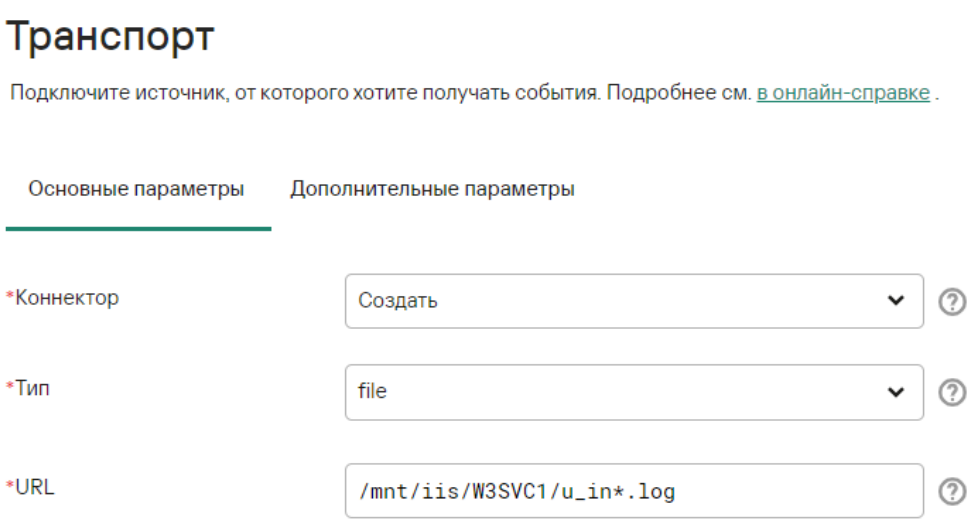
Создание коллектора KUMA

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.

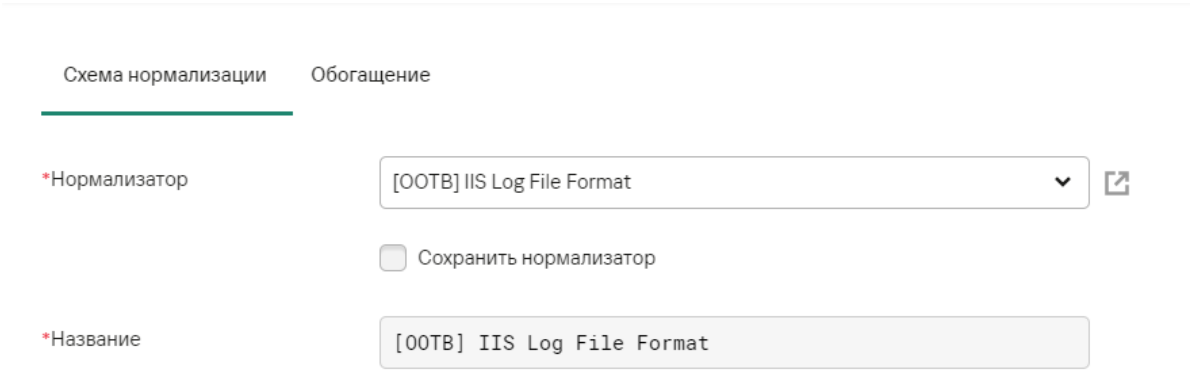
На первом шаге мастера необходимо выбрать **Тенант**, которому будет принадлежать коллектор и также задать **Имя коллектора**.



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

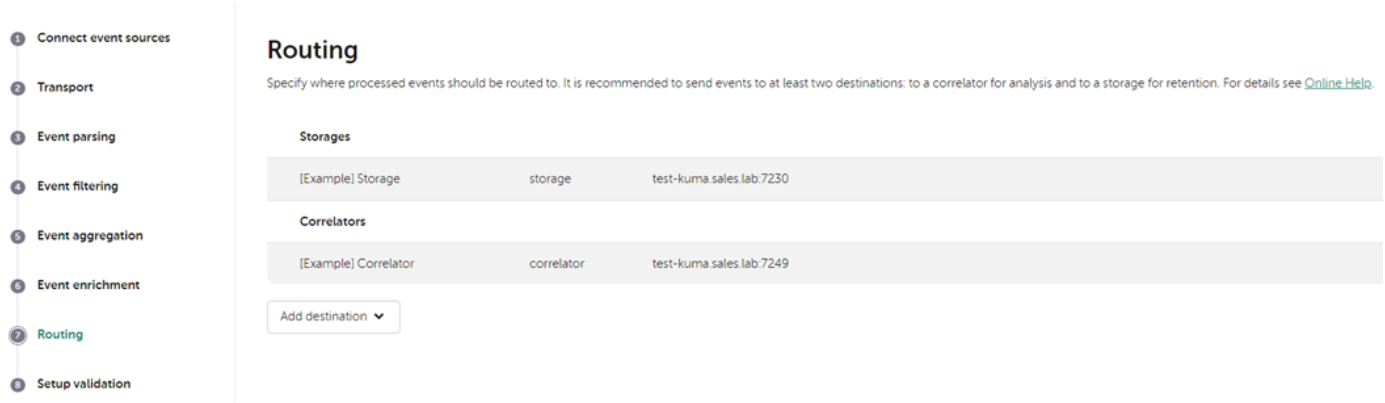


На третьем шаге мастера необходимо выбрать предустановленный нормализатор **[ООТВ] IIS Log File Format**. В случае отсутствия указанного нормализатора, обратитесь к своему менеджеру для его получения.

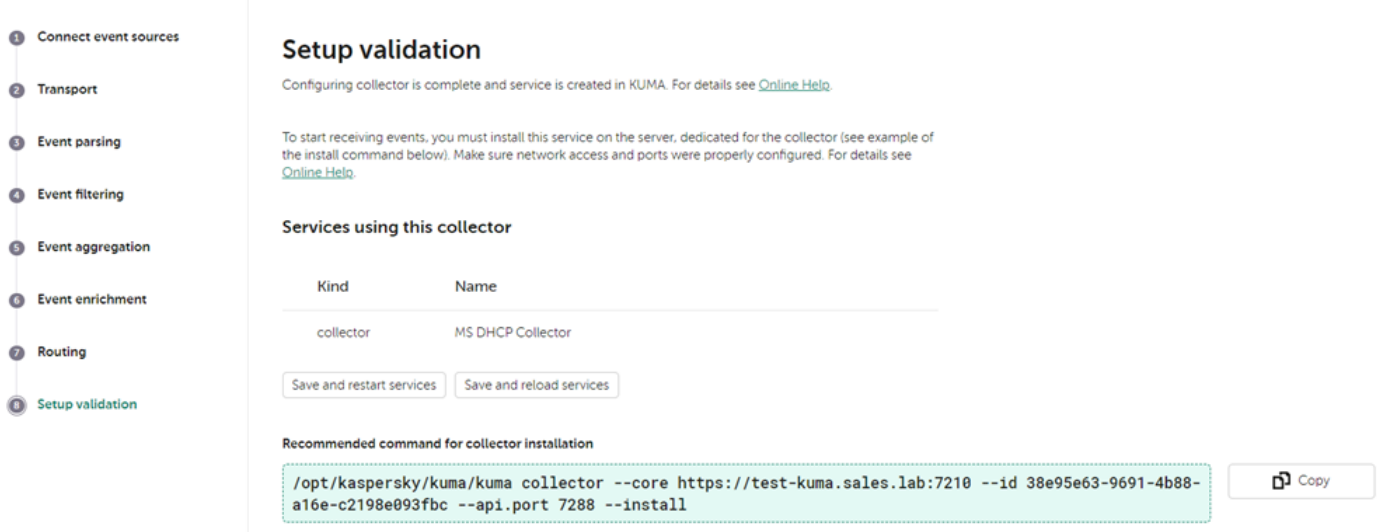


Шаги мастера с четвертого по шестой можно пропустить, либо заполнить позднее по своему усмотрению.

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



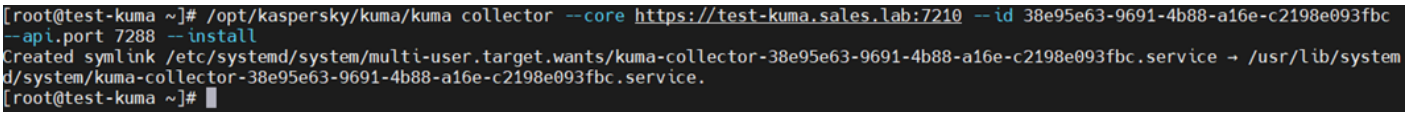
На последнем шаге мастера необходимо нажать на кнопку **Сохранить и создать сервис**, после чего скопировать появившуюся команду для дальнейшей установки сервиса коллектора.



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.



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

Для поиска событий IIS можно использовать следующий запрос

```
SELECT * FROM `events` WHERE DeviceProduct = 'IIS' ORDER BY Timestamp DESC LIMIT 250
```

Revision #3
Created 2023-11-16 08:03:01 UTC by Koala
Updated 2024-07-07 08:50:24 UTC by Koala