

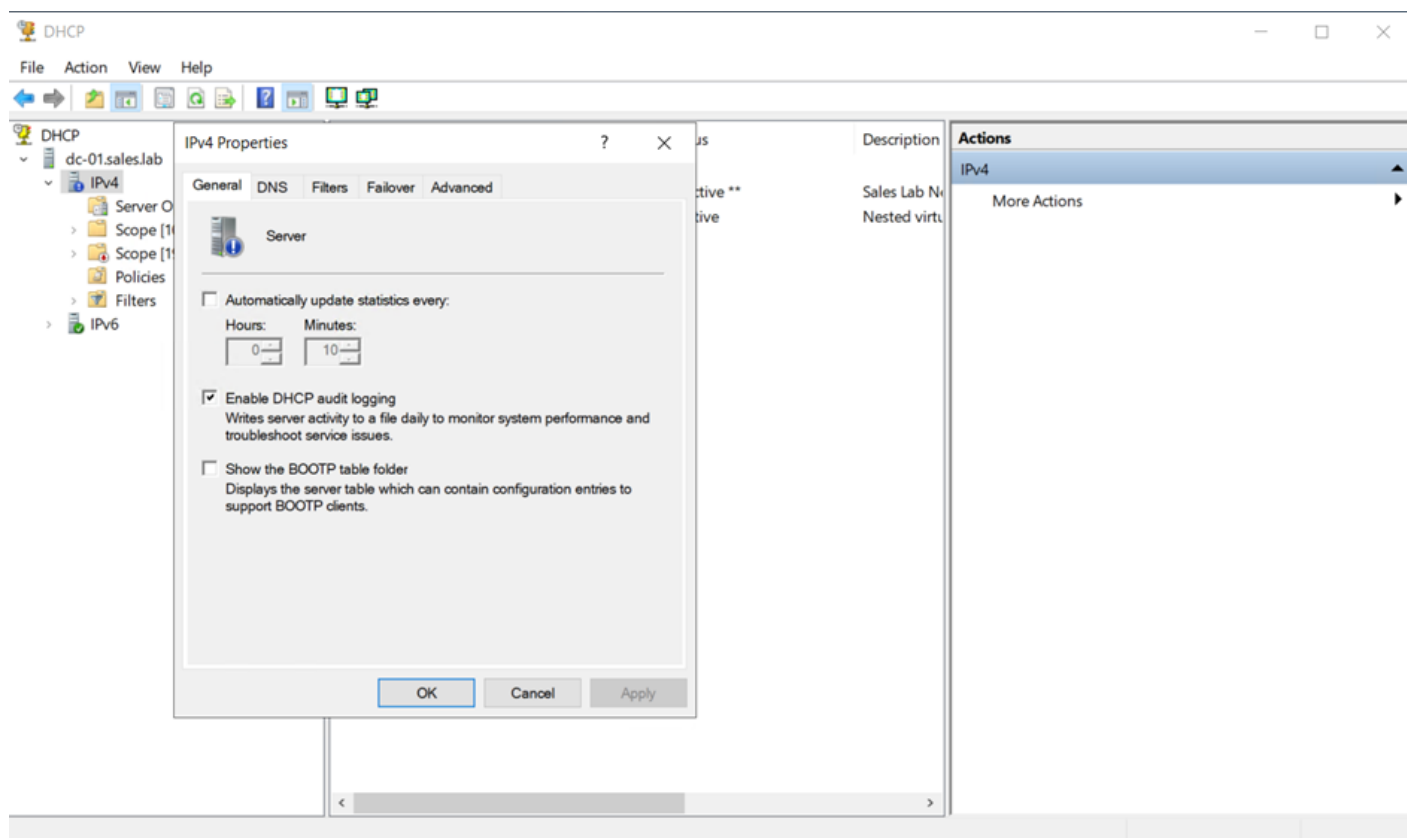
MS DHCP

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

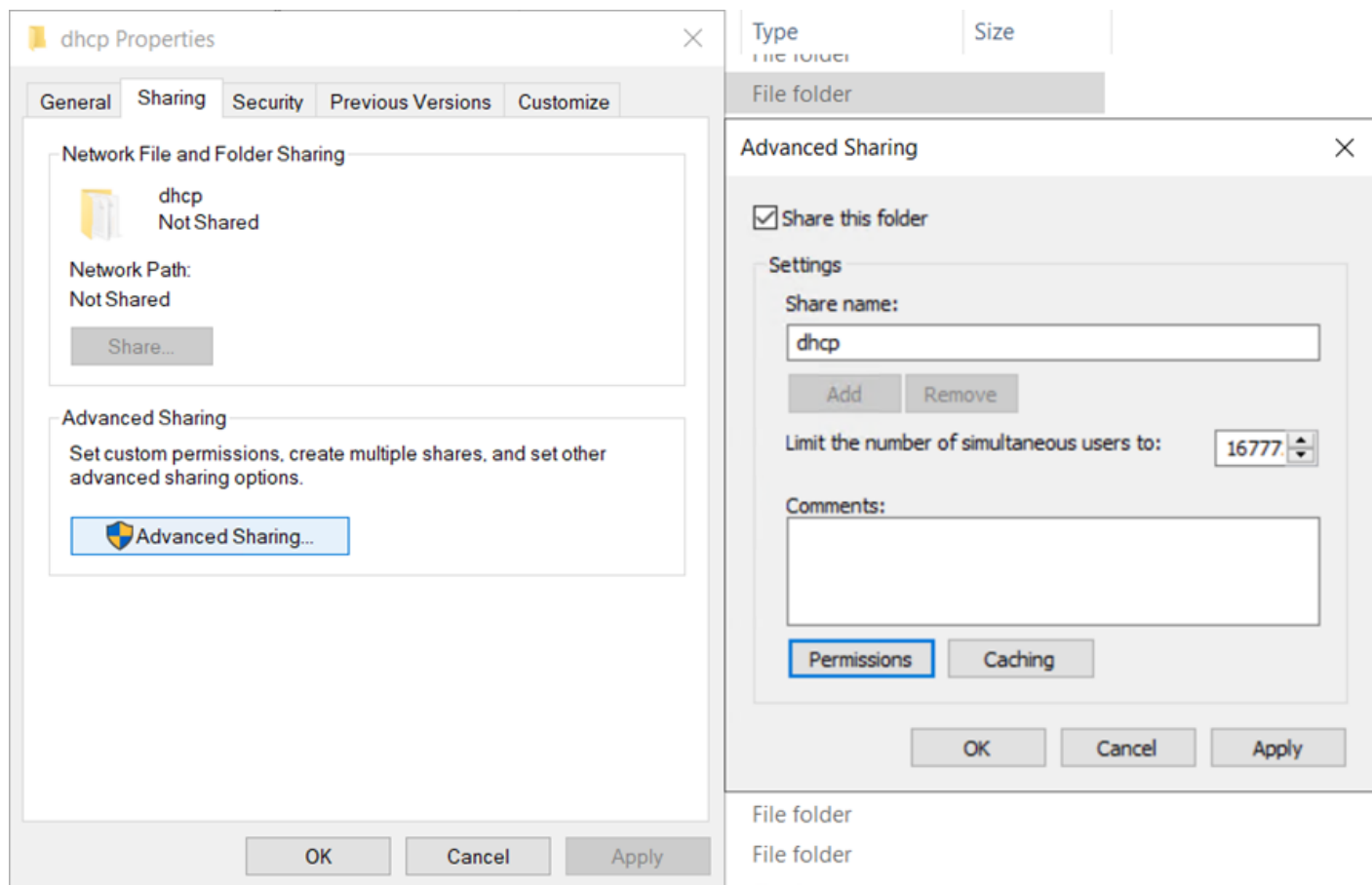
Настройка DHCP сервера

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

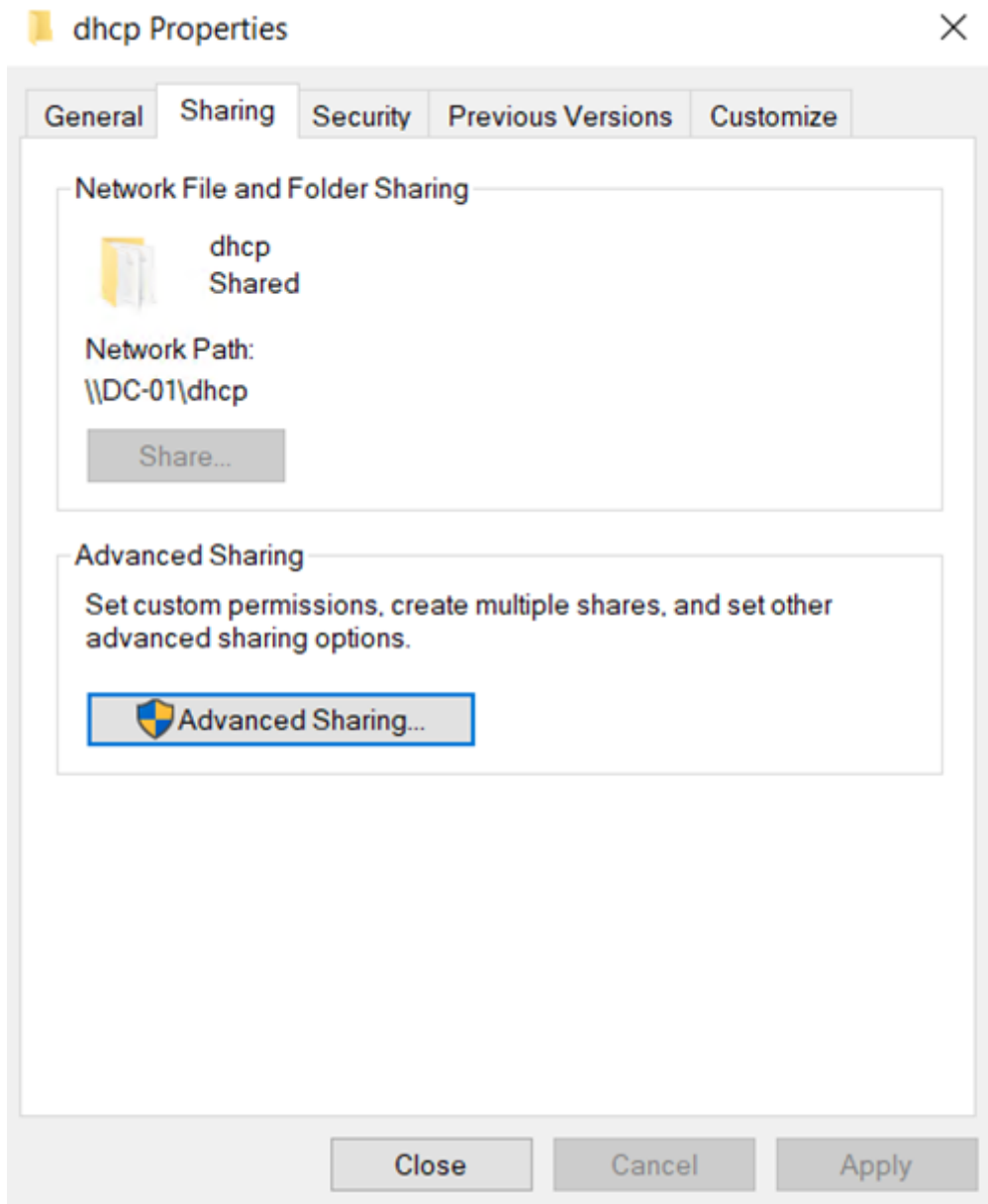
Откройте оснастку DHCP и убедитесь, что для DHCP сервера включено логирование.



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 случаях откроется мастер подключения источников событий.

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

1

Connect event sources

2

Transport

3

Event parsing

4

Event filtering

5

Event aggregation

6

Event enrichment

7

Routing

8

Setup validation

Connect event sources

Collector is used to get events from event source and convert them into KUMA format for further processing. It can also filter out useless events, merge multiple events into one, and enrich events with additional data. Complete the wizard to create collector. For details see [Online Help](#).

*Collector name

MS DHCP Collector

*Tenant

Main

▼

Workers

Worker count

Debug

Disable

▼

Description

Description

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

- 1 Connect event sources
- 2 **Transport**
- 3 Event parsing
- 4 Event filtering
- 5 Event aggregation
- 6 Event enrichment
- 7 Routing
- 8 Setup validation

Transport

Add a source from which you want to receive events. For details see [Online Help](#).

Basic settings Advanced settings

*Connector	Create new	?
*Kind	file	?
*URL	/mnt/dhcp/DhcpSrvLog-???.log	?

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.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Event parsing

Normalization schemeEnrichment

*Normalizer

[OOTB] MS DHCP file

Save normalizer

*Name

[OOTB] MS DHCP file

*Parsing method

regex

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.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Routing

Specify where processed events should be routed to. It is recommended to send events to at least two destinations: to a correlator for analysis and to a storage for retention. For details see [Online Help](#).

Storages

[Example] Storage	storage	test-kuma.sales.lab.7230
-------------------	---------	--------------------------

Correlators

[Example] Correlator	correlator	test-kuma.sales.lab.7249
----------------------	------------	--------------------------

Add destination

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

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Setup validation

Configuring collector is complete and service is created in KUMA. For details see [Online Help](#).

To start receiving events, you must install this service on the server, dedicated for the collector (see example of the install command below). Make sure network access and ports were properly configured. For details see [Online Help](#).

Services using this collector

Kind	Name
collector	MS DHCP Collector

Save and restart services

Save and reload services

Recommended command for collector installation

```
/opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 38e95e63-9691-4b88-a16e-c2198e093fbc --api.port 7288 --install
```

Copy

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

[Resources and services](#) >

Add service

Refresh

Reload

Restart

Copy ID

Go to events

Go to active lists

Go to partitions

Reset certificate

Remove

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	●	Collector	MS DHCP Collector		Main				

Установка коллектора KUMA

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

Перед выполнением установки рекомендуется выполнить команду, скопированную на предыдущем шаге, **без ключа --install**.

```
[root@test-kuma ~]# /opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 38e95e63-9691-4b88-a16e-c2198e093fbc --api.port 7288
[ dictionaries ] 2022/09/19 08:14:19 /opt/tfs-agent/_work/1/s/sdk/dictionaries/simple_storage.go:48: '[00TB] MS DHCP Event IDs Description' loaded
[ destination '[Example] Storage' ] 2022/09/19 08:14:24 /opt/tfs-agent/_work/1/s/sdk/destinations/base.go:65: started
[ destination '[Example] Correlator' ] 2022/09/19 08:14:24 /opt/tfs-agent/_work/1/s/sdk/destinations/base.go:65: started
[ connector '35404193-20f7-4034-8539-8fcca07b0c31' ] 2022/09/19 08:14:24 /opt/tfs-agent/_work/1/s/sdk/connectors/base.go:36: started
[ collector 38e95e63-9691-4b88-a16e-c2198e093fbc ] 2022/09/19 08:14:24 /opt/tfs-agent/_work/1/s/collector/processor.go:85: started
```

В случае отсутствия ошибок и изменения статуса коллектора в веб-интерфейсе KUMA на **зеленый**, необходимо темринировать выполнение команды и перейти к установке.

Для установки сервиса коллектора необходимо выполнить скопированную команду с **ключом --install**.


```
[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/systemd/system/kuma-collector-38e95e63-9691-4b88-a16e-c2198e093fbc.service.
[root@test-kuma ~]#
```

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

[Resources and services](#) >
Services Add service Refresh

Reload Restart Copy ID Go to events Go to active lists Go to partitions Reset certificate Remove

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	●	Collector	MS DHCP Collector	2.0.0.306	Main	test-kuma.sales.lab	10.68.85.125	7288	12 seconds

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.