

MS DNS

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

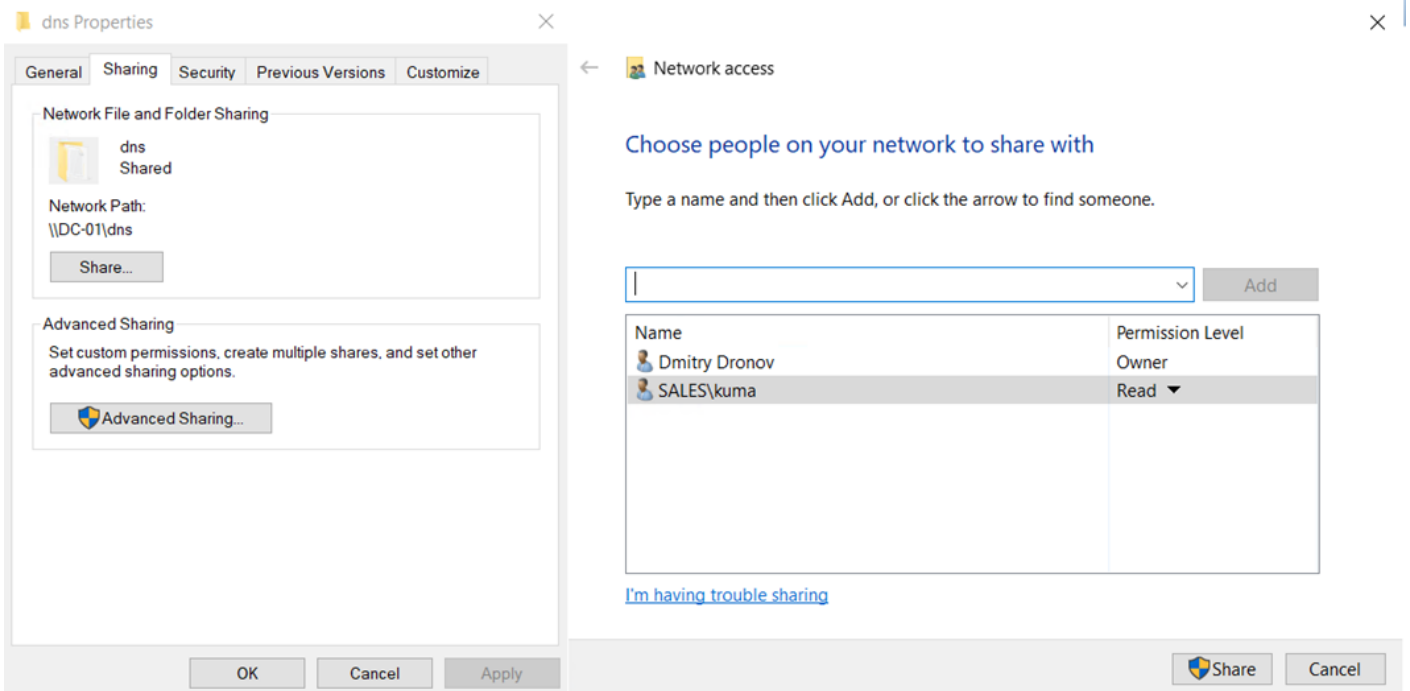
Для KUMA 3.2 добавился новый способ сбора DNS логов в формате ETW. Подробнее в статье: <https://kb.kuma-community.ru/books/podklyucenie-istocnikov/page/ms-etw-dns-analytics-kuma-32>

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

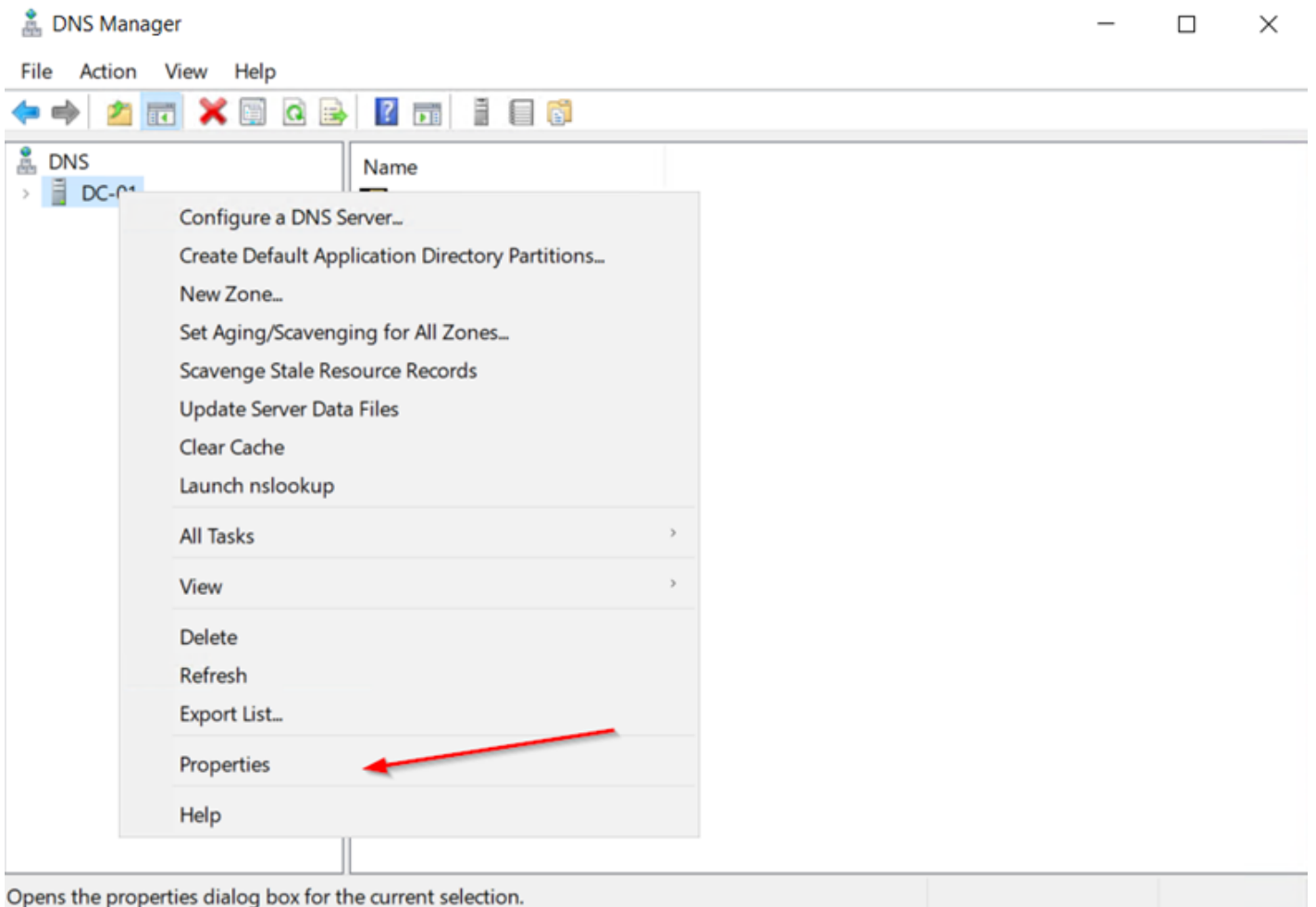
Передача событий из MS DNS в KUMA осуществляется путем чтения лог файла DNS. По умолчанию запись событий в файл на DNS сервере выключена.

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 записываться логи DNS сервера. Размер лог файла рекомендуется 50 Мб.

Interfaces Forwarders Advanced Root Hints

Debug Logging Event Logging Monitoring Security

To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

Log packets for debugging

Packet direction: Transport protocol:

Outgoing } select at least one UDP } select at least one

Incoming } TCP } select at least one

Packet contents: Packet type:

Queries/Transfers } select at least one Request } select at least one

Updates } Response } select at least one

Notifications

Other options:

Log unmatched incoming response packets

Details

Filter packets by IP address Filter...

Log file

File path and name:

Maximum size (bytes):

OK Cancel Apply Help

???????????????? ???? ? 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

```
[root@test-kuma ~]# ls -l /mnt/dns
total 66304
-rwxr-xr-x 1 root root 67821587 Sep 19 12:19 dns.log
```

????????? ?????????????? 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	<input type="text" value="MS DNS Collector"/>
*Tenant	<input type="text" value="Main"/>
Workers	<input type="text" value="Worker count"/>
Debug	<input type="text" value="Disable"/>
Description	<input type="text" value="Description"/>

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

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

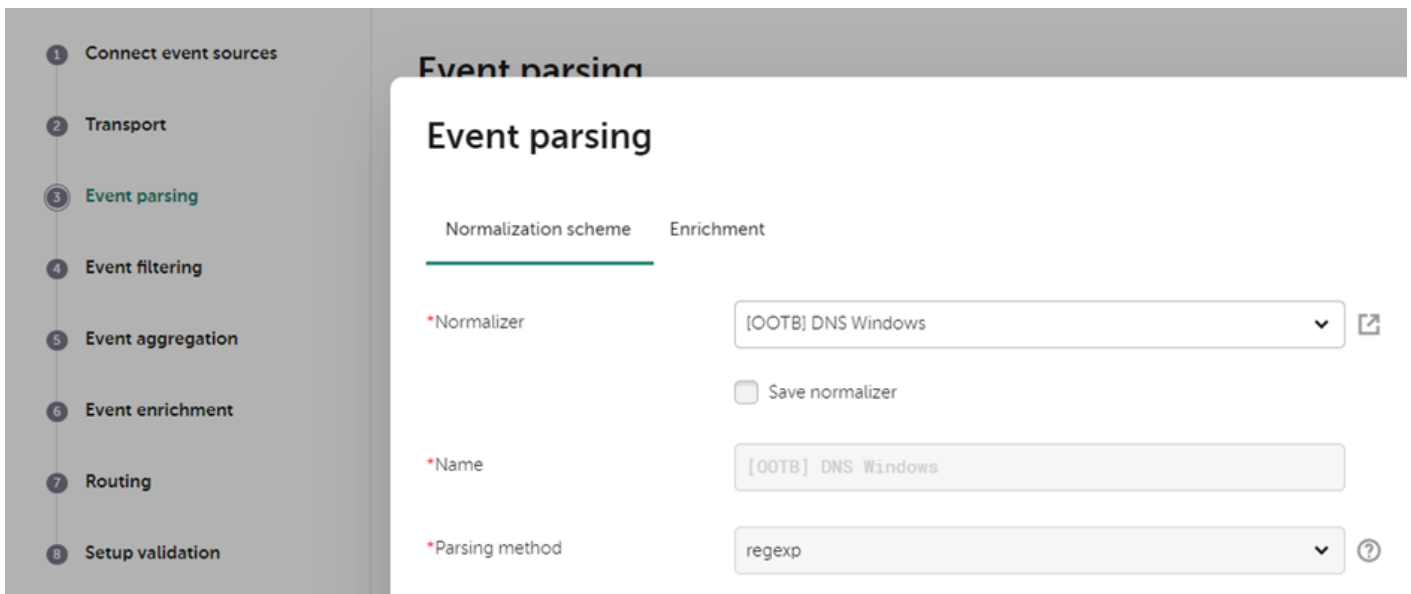
Transport

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

Basic settings Advanced settings

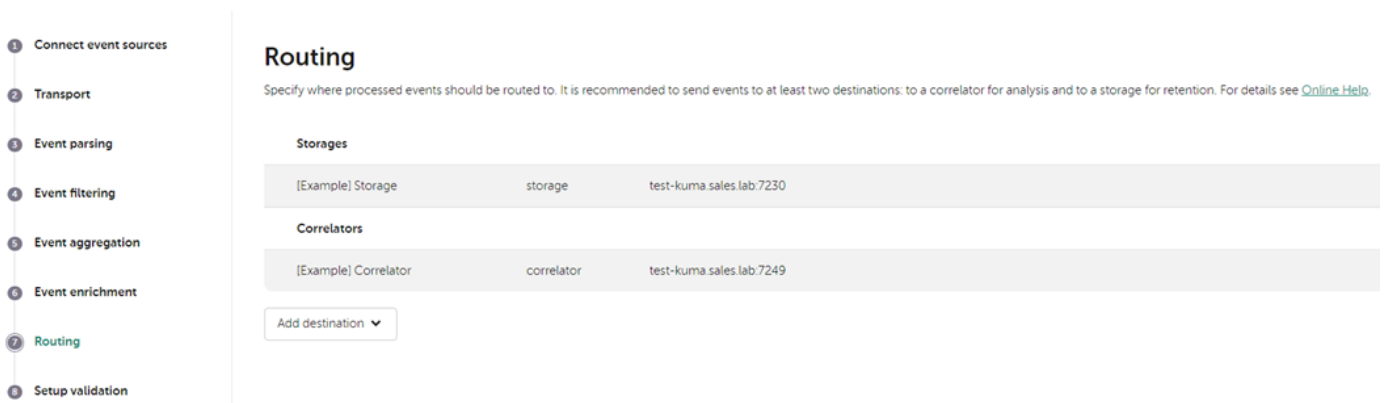
*Connector	<input type="text" value="Create new"/>	?
*Kind	<input type="text" value="file"/>	?
*URL	<input type="text" value="/mnt/dns/dns.log"/>	?

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.

- 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 DNS Collector

Recommended command for collector installation

```
/opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 4882d631-eae4-4c85-ba64-1efecf9ce744 --api.port 7286 --install
```

Copy

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

[Resources and services](#) > **Services**

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

????????? ?????????????? 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 4882d631-eae4-4c85-ba64-1efecf9ce744 --api.port 7286 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-4882d631-eae4-4c85-ba64-1efecf9ce744.service → /usr/lib/systemd/system/kuma-collector-4882d631-eae4-4c85-ba64-1efecf9ce744.service.
[root@test-kuma ~]# █
```

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

[Resources and services](#) > **Services**

<input type="checkbox"/>	Status	Kind ↑	Service	Version	Tenant	FQDN	IP Address	API port	Uptime
<input type="checkbox"/>	●	Collector	MS DNS Collector	2.0.0.306	Main	test-kuma.sales.lab	10.68.85.125	7286	16 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 DNS сервера.

Events						Event details	
<pre>SELECT * FROM 'events' WHERE ServiceID = '4882d631-eae4-4c85-ba64-1efecf9ce744' LIMIT 250</pre>							
TenantID	Timestamp	DeviceCustomStri...	DeviceCustomStri...	DeviceCustomStri...	DeviceCustomStri...	TenantName	Main
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	Timestamp	2022-09-19 12:37:01:780
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	EndTime	2022-09-19 12:36:54:780
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceAction	R
Main	2022-09-19 12:37:01	Q	8081	DR	NOERROR	DeviceReceiptTime	2022-09-19 12:37:01:780
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceTimeZone	+03:00
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	SourceAddress	10.68.85.95
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	DestinationHostName	elasticsearch1
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DestinationProcessName	DNS
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	DeviceCustomString1	Q
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceCustomString1Label	Opcodes
Main	2022-09-19 12:37:01	Q	8081	DR	NOERROR	DeviceCustomString2	8281
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceCustomString2Label	Flags_hex
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	DeviceCustomString3	DR
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceCustomString3Label	Flags_char
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	DeviceCustomString4	SERVFAIL
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceCustomString4Label	ResponseCode
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	DeviceCustomString5	A
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	DeviceCustomString5Label	QuestionType
Main	2022-09-19 12:37:01	Q	0001	D	NOERROR	Service	MS DNS Collector
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	TransportProtocol	UDP
Main	2022-09-19 12:37:01	Q	8281	DR	SERVFAIL	Type	Base

Revision #12

Created 2023-08-10 12:17:51 UTC by Boris RZR

Updated 2025-01-24 10:28:31 UTC by Koala