

MS ETW (DNS Analytics)

Поддерживается в KUMA с версии 3.2

Расширенное ведение журнала DNS и диагностика доступны по умолчанию с версии Windows Server 2016. Эта функция также доступна в Windows Server 2012 R2 при установке исправления для ведения журнала запросов и аудита изменений, доступного по адресу <https://support.microsoft.com/kb/2956577>

Event Tracing for Windows (ETW) - это механизм логирования различных событий, создаваемых приложениями и драйверами. Фактически является более расширенной версией стандартного журнала событий. Исторически ETW использовался для задач дебага при разработке, сейчас его можно использовать в том числе и для поиска вредоносной активности.

Включение опции логирования ETW оказывает незначительное влияние на производительность (рекомендуется в нагруженных системах). Например, DNS-сервер, работающий на современном оборудовании и получающий 100 000 запросов в секунду (QPS), может испытывать снижение производительности на 5 % при включении аналитических журналов. Очевидного влияния на производительность при скорости запроса 50 000 QPS и ниже не наблюдается. Однако всегда желательно отслеживать производительность DNS-сервера всякий раз, когда включено дополнительное ведение журнала.

??????

ETW состоит из трёх отдельных компонентов:

- Провайдеры (Providers), в некоторых случаях зовутся поставщиками
- Потребители (Consumers)
- Контроллеры (Controllers)

Провайдеры генерируют события, потребители их используют, а контроллеры управляют всей этой деятельностью. Провайдеры - это приложения, которые содержат функционал отправки событий в ETW. Примеры провайдеров: ядро Windows, драйвера устройств, user-mode приложения и другое ПО. Какие необходимо отправлять события решает разработчик в своём коде, упрощенно говоря, если выполняется важная с точки зрения разработчика функция (открывается доступ к SAM), то создается запись в ETW.

Для отправки провайдеры регистрируются в контроллере, контроллер в свою очередь может включить или отключить источник событий. Отключенный источник события не

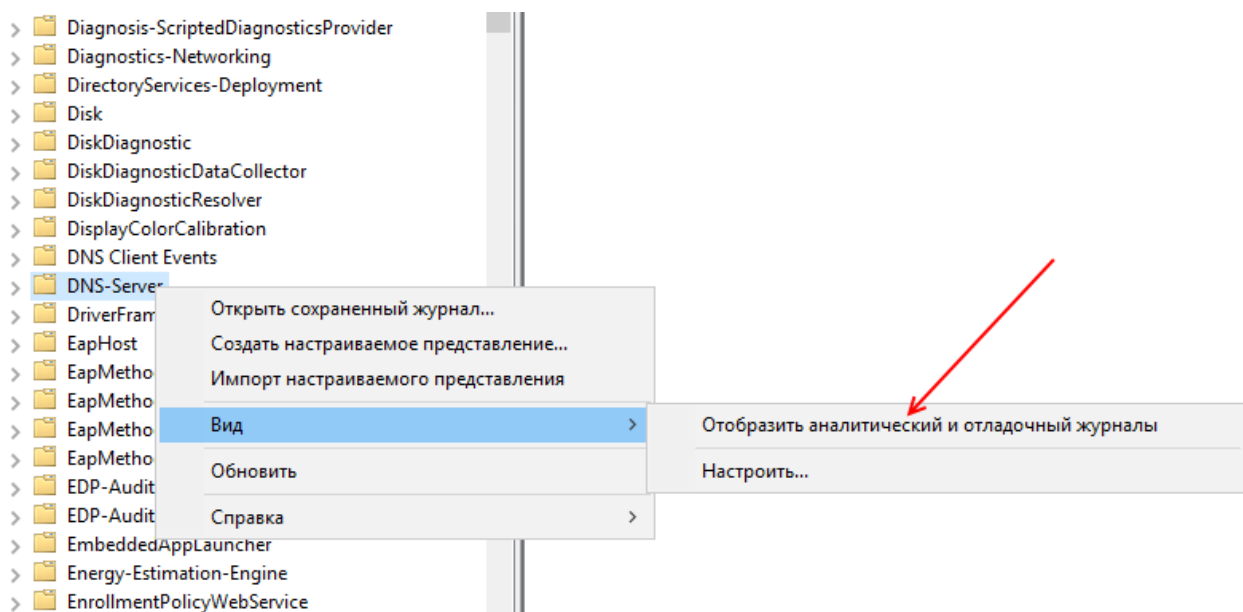
генерирует. Пример контроллеров - это logman или wevtutil. Для связи между провайдером и потребителем контроллер использует так называемые сессии трассировки. Сессия служит в том числе для фильтрации необходимых данных по различным параметрам, потому что потребителю может быть нужна только одна часть информации, а другому потребителю - другая.

Полезные ссылки:

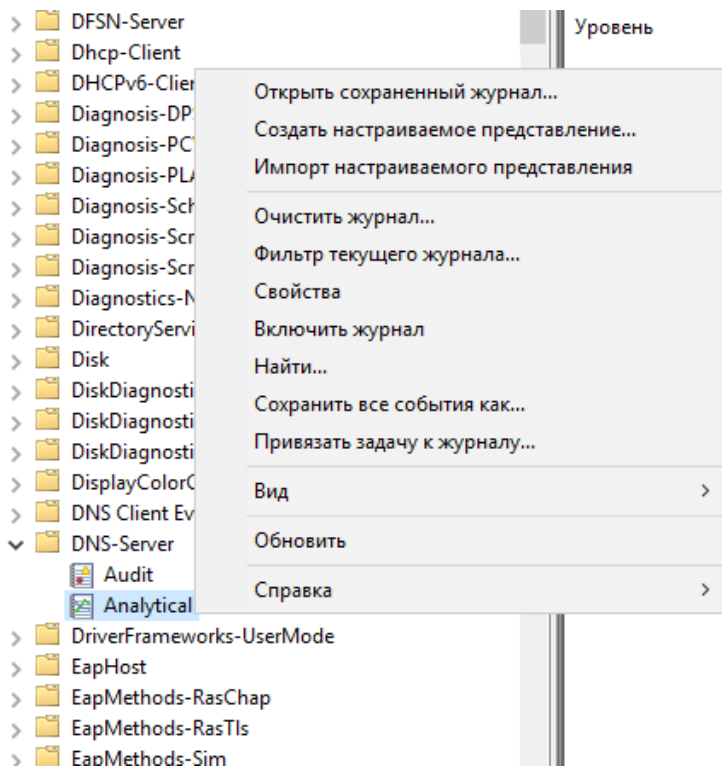
- <https://habr.com/ru/articles/502362/>
- <https://learn.microsoft.com/ru-ru/archive/blogs/teamdhcp/network-forensics-with-windows-dns-analytical-logging>

?????????? ?? ???????? Windows

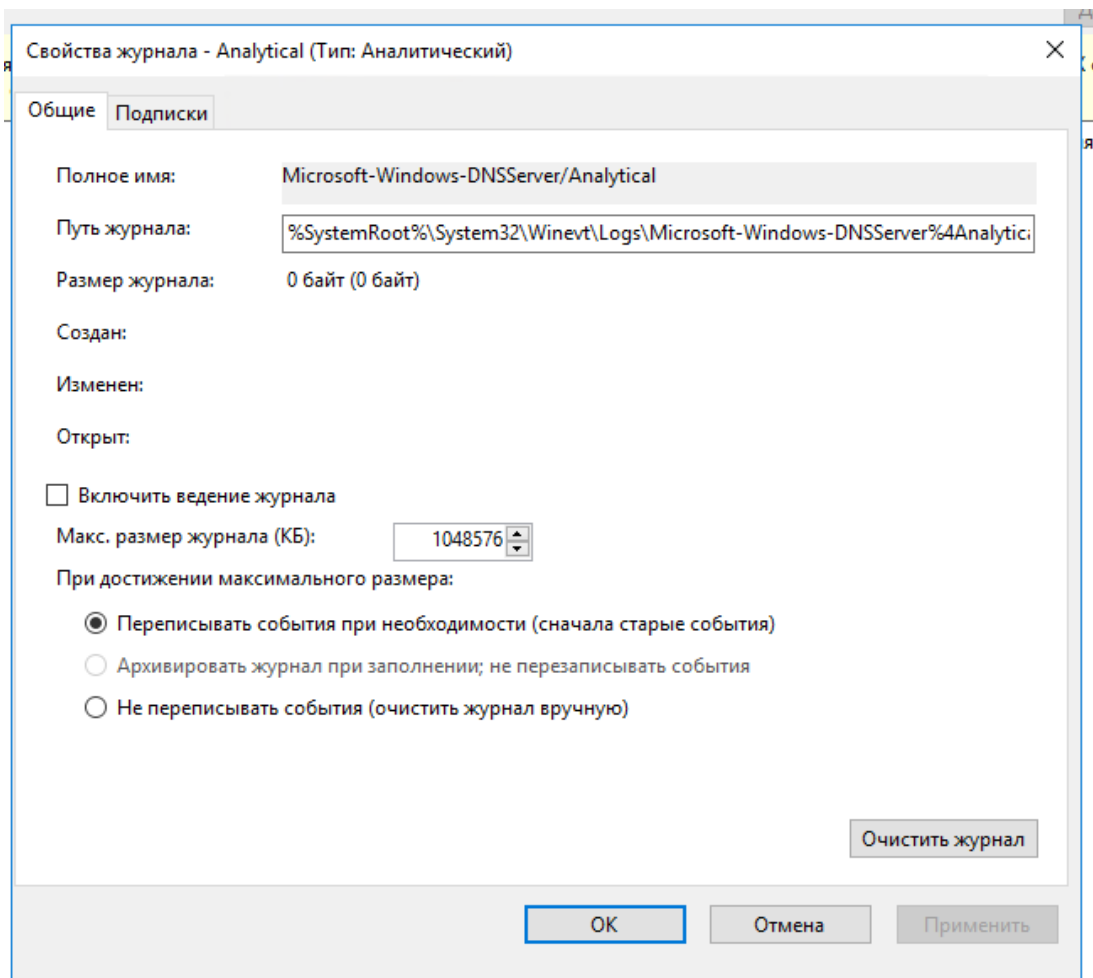
Переходим в **EventViewer** (Выполнить -> eventvwr.msc). Далее переходим в **Журналы приложений и служб\Microsoft\Windows\DNS-Server** (на англ. Applications and Services Logs\Microsoft\Windows\DNS-Server)



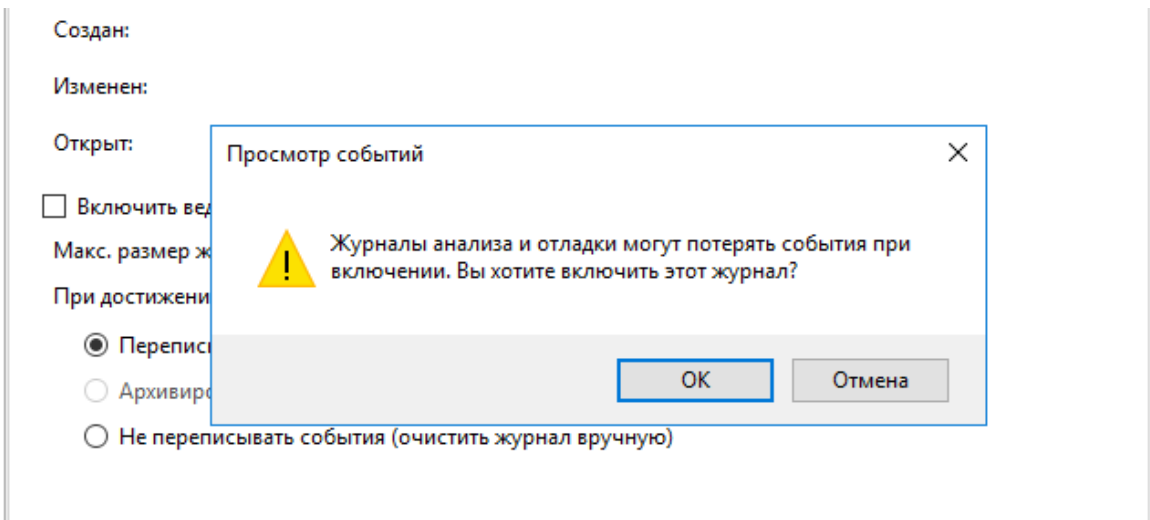
Далее переходим в свойства Аналитического журнала:



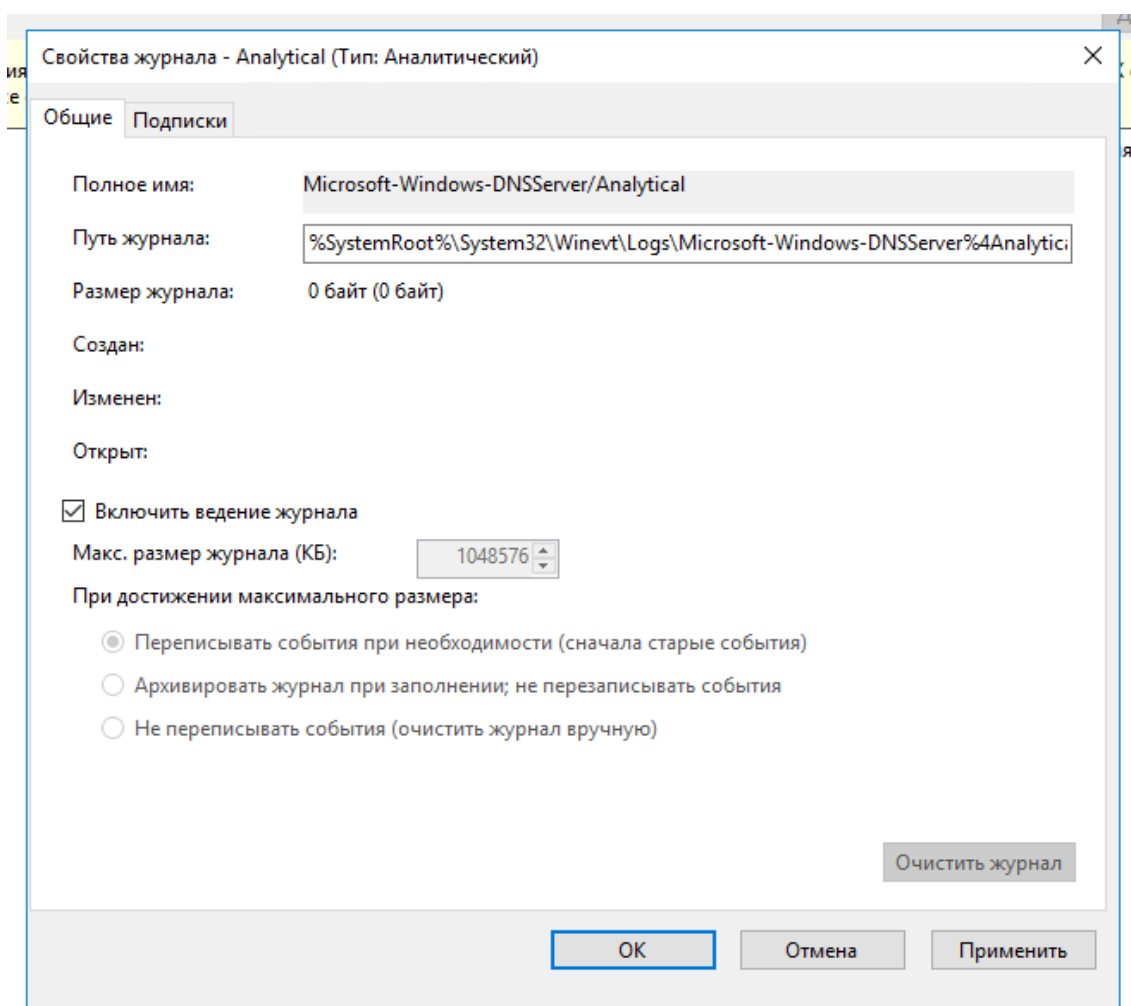
Оставляем максимальный размер журнала по умолчанию в 1 Гб:



Нажимаем на **чекбокс Включить** ведение журнала, затем **ОК**



Должно получиться следующее:



Нажимаем **Применить** и **ОК**.

При появлении следующего окна, не пугаемся, при **включенной ротации аналитического журнала события не отображаются в интерфейсе**, чтобы их увидеть (нам это не понадобится) нужно остановить журнал.

Ошибка запроса



Один или несколько журналов запроса содержат ошибки

Журнал	Ошибка
Microsoft-Windows-...	Запрошенная операция не может быть выпол...

Отображаются частичные результаты событий

OK

- > Desired State Configuration
- > DeviceGuard
- > DeviceManagement-Enterprise-Diagnostics-Provi
- > Devices-Background
- > DeviceSetupManager
- > DeviceSync
- > DFSN-Server
- > Dhcp-Client
- > DHCPv6-Client
- > Diagnosis-DPS
- > Diagnosis-PCW
- > Diagnosis-PLA
- > Diagnosis-Scheduled
- > Diagnosis-Scripted
- > Diagnosis-ScriptedDiagnosticsProvider
- > Diagnostics-Networking
- > DirectoryServices-Deployment
- > Disk
- > DiskDiagnostic
- > DiskDiagnosticDataCollector
- > DiskDiagnosticResolver
- > DisplayColorCalibration
- > DNS Client Events
- > DNS-Server
 - Audit
 - Analytical**
- > DriverFrameworks-UserMode
- > EapHost
- > EapMethods-RasChap
- > EapMethods-RasTls
- > EapMethods-Sim
- > EapMethods-Tls
- > EDP-Audit-Regular
- > EDP-Audit-TCB
- > EmbeddedAppLauncher
- > Event-Subscriptions-Provider

Для облегчения работы с этим аналитическим, отладочным или классическим журналом событий сохраните его в формате EVTХ с помощью команды "Сохранить все события как".

Уровень	Дата и время	Источник	Код события	Категория задачи
---------	--------------	----------	-------------	------------------

Действия

- Открыть сохраненный журнал...
- Создать настраиваемое представление...
- Импорт настраиваемого представления
- Очистить журнал...
- Фильтр текущего журнала...
- Свойства
- Отключить журнал
- Найти...
- Сохранить все события как...
- Привязать задачу к журналу...
- Вид
- Обновить
- Справка

Далее необходимо перейти в **Управление компьютером** и открыть его от Администратора. Переходим **Службные программы - Производительность - Сеансы отслеживания событий запуска (perfmon.msc)**.

Имя	Статус
AppModel	Включ...
Audio	Включ...
AutoLogger-Diagtrack-Listener	Включ...
BluetoothSession	Отклю...
Circular Kernel Context Logger	Отклю...
DefenderApiLogger	Включ...
DefenderAuditLogger	Включ...
DiagLog	Включ...
EventLog-Application	Включ...
EventLog-ForwardedEvents	Включ...
EventLog-Microsoft-Windows-...	Включ...
EventLog-Security	Включ...
EventLog-System	Включ...
LwtNetLog	Отклю...
Mellanox-Kernel	Отклю...
Microsoft-Windows-Setup	Отклю...
NBSMBLOGGER	Отклю...
NtfsLog	Включ...
PEAuthLog	Отклю...
RdrLog	Отклю...
SetupPlatform	Отклю...
SetupPlatformTel	Отклю...
SpoolerLogger	Отклю...
SQMLogger	Отклю...
SUM	Включ...
TCPIPLOGGER	Отклю...
Tpm	Отклю...
UBPM	Включ...
WdiContextLog	Включ...
WFP-IPsec Trace	Отклю...
WiFiSession	Включ...

Создаем группу сборщиков данных:

NtfsLog	Включ...
PEAuthLog	Отклю...
RdrLog	Отклю...
SetupPlatform	Отклю...
SetupPlatformTel	Отклю...
SpoolerLogger	Отклю...
SQMLogger	Отклю...
SUM	Отклю...
TCPIPLOGGER	Отклю...
Tpm	Отклю...
UBPM	Отклю...
WdiContextLog	Отклю...
WFP-IPsec Trace	Отклю...
WiFiSession	Отклю...

Создать > Группа сборщиков данных

Обновить

Экспортировать список...

Вид >

Упорядочить значки >

Выровнять значки

Справка

Задаем имя сборщика, например etwDNS-Analytics:

← Создать новую группу сборщиков данных.

Как создавать новую группу сборщиков данных?

Имя:

etwDNS-Analytics

Создать из шаблона (рекомендуется)

Создать вручную (для опытных)

Далее

Готово

Отмена

Добавляем поставщика **Microsoft-Windows-DNSServer**:

← Создать новую группу сборщиков данных.

Какие службы трассировки событий должны быть включены?

Поставщики:

Microsoft-Windows-DNSServer

Добавить...

Удалить

Свойства:

Свойство	Значение
Ключевые слов...	0x0
Ключевые слов...	0x0
Уровень	0x00
Свойства	0x00000000

Изменить...

Далее

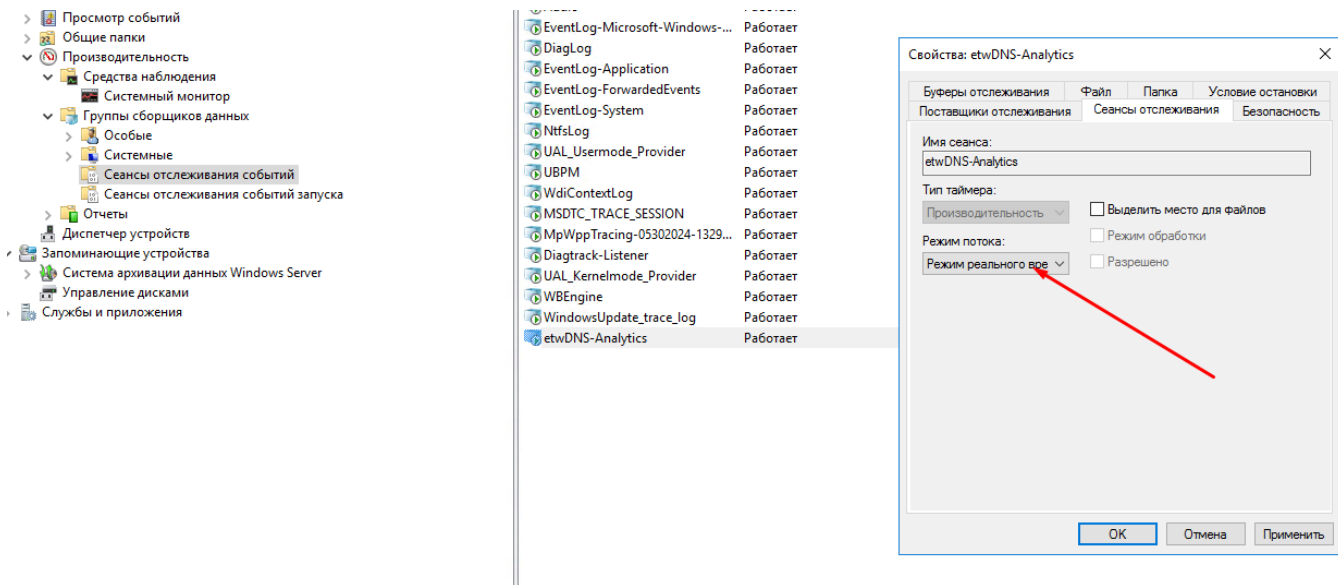
Готово

Отмена

Агент с коннектором ETW работает только с System.Provider.Guid: {EB79061A-A566-4698-9119-3ED2807060E7} - Microsoft-Windows-DNSServer

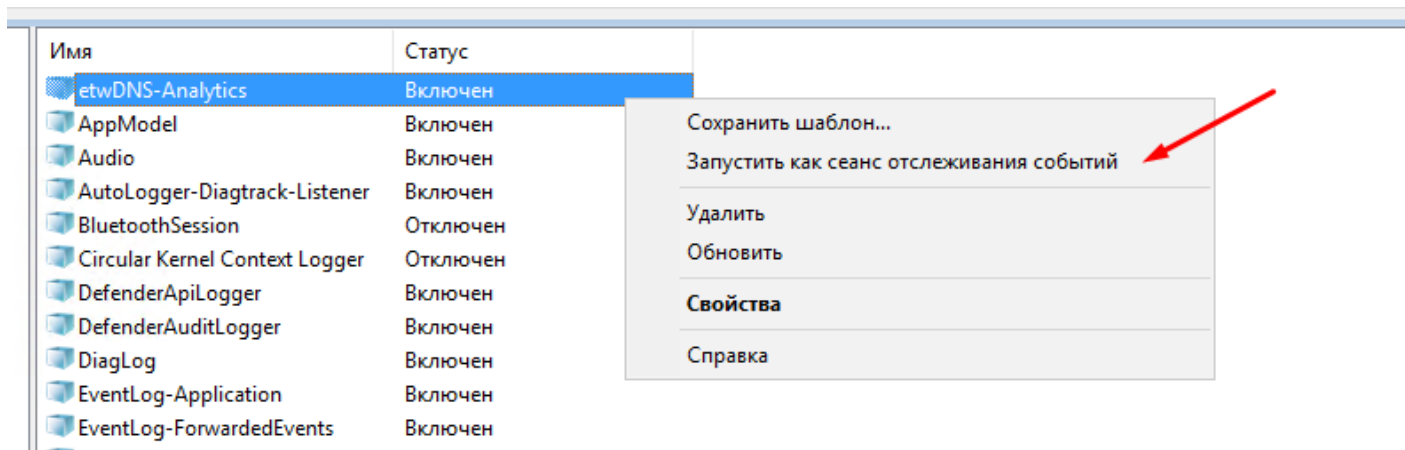
Нажимаем **Далее - Далее - Готово**.

В сеансах отслеживания событий, в свойствах - **Сеансы отслеживания** указываем **Режим реального времени**

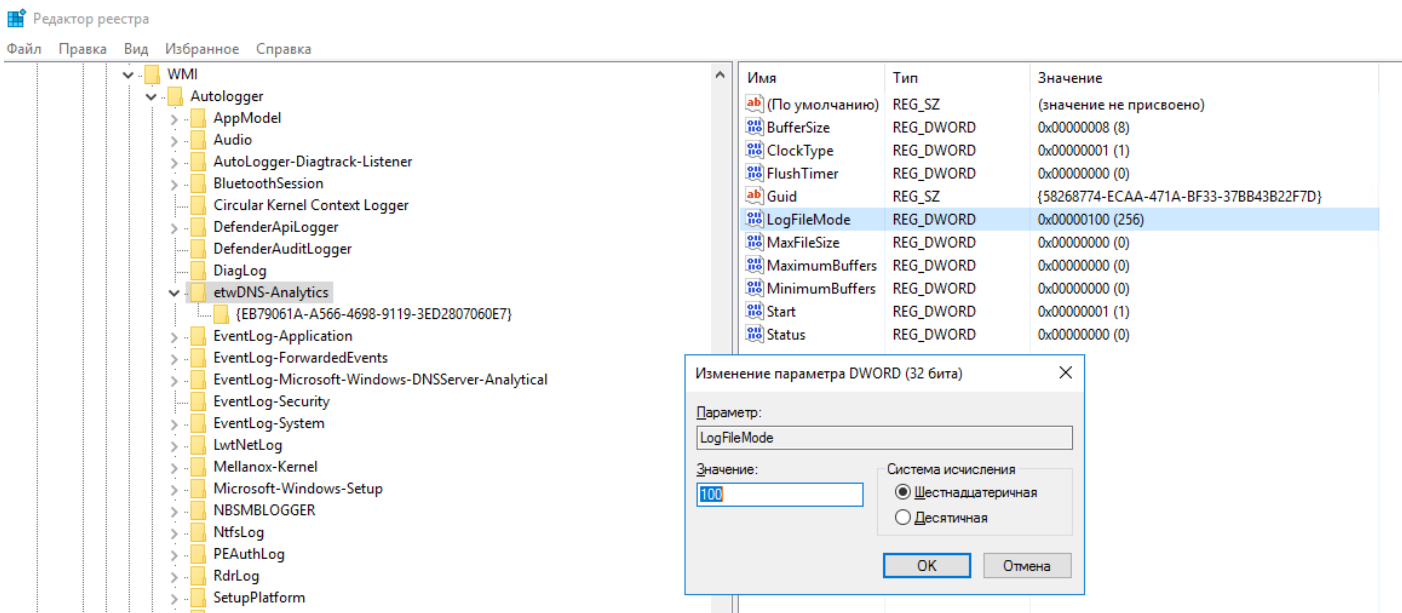


Нажимаем **Применить** и **ОК**.

Запускаем созданного поставщика, как сеанс отслеживания событий:



Для персистентности режима реального времени, в редакторе реестра (regedit.exe) по пути `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger` далее название ранее созданного сеанса в ключе `LogFileMode` установите значение 100.



Чтобы просмотреть, какие типы событий можно отслеживать, выполните следующую команду в командной строке powershell:

```
logman query providers "Microsoft-Windows-DNSServer"
```

Пример вывода:

```
PS C:\Users\Администратор.WIN-I6F9HU7R4L0> logman query providers "Microsoft-Windows-DNSServer"
-----
Поставщик                                GUID
-----
Microsoft-Windows-DNSServer              {EB79061A-A566-4698-9119-3ED2807060E7}
-----
Значение      Ключевое слово      Описание
-----
0x0000000000000001  QUERY_RECEIVED
0x0000000000000002  RESPONSE_SUCCESS
0x0000000000000004  RESPONSE_FAILURE
0x0000000000000008  IGNORED_QUERY
0x0000000000000010  RECURSE_QUERY_OUT
0x0000000000000020  RECURSE_RESPONSE_IN
0x0000000000000040  RECURSE_QUERY_DROP
0x0000000000000080  DYN_UPDATE_RECV
0x0000000000000100  DYN_UPDATE_RESPONSE
0x0000000000000200  IXFR_REQ_OUT
0x0000000000000400  IXFR_REQ_RECV
0x0000000000000800  IXFR_RESP_OUT
0x0000000000001000  IXFR_RESP_RECV
0x0000000000002000  IXFR_RESP_OUT
```

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

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

Для создания коллектора в веб-интерфейсе KUMA перейдите на вкладку **Ресурсы** -> **Коллекторы** и нажмите на кнопку **Добавить коллектор**.

После выполнения вышеуказанных действий откроется мастер настройки. На первом шаге выберите **Имя коллектора** и **Тенант**, к которому будет принадлежать создаваемый коллектор.

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

Название коллектора*	<input type="text" value="ETW-Collector - (tcp/5577)"/>
Тенант*	<input type="text" value="Main"/>
Обработчики	<input type="text" value="0"/>
Отладка	<input type="checkbox"/>
Описание	<div style="border: 1px solid #ccc; height: 40px;"></div>

На втором шаге мастера укажите транспорт. В нашем случае используется TCP (можно также использовать http и режимы с верификацией для защищенной отправки). В поле URL задайте FQDN/порт (выбирается любой из незанятых), на котором коллектор будет ожидать соединение от агента. В качестве разделителя укажите \n.

*можно указать только порт при инсталляции All-in-one.

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор	<input type="text" value="Создать"/>
Тип* ⓘ	<input type="text" value="top"/>
URL* ⓘ	<input type="text" value=":5577"/>
Auditd	<input type="checkbox"/>
Разделитель	<input type="text" value="\n"/>

На третьем шаге мастера укажите нормализатор. В данном случае рекомендуется использовать предустановленный расширенный нормализатор для событий Windows **[OOTB] Microsoft DNS ETW logs json**.

Редактировать

Основной парсинг событий

Подключение источ

Транспорт

Парсинг событий

Фильтрация событ

Агрегация событий

Обогащение событ

Маршрутизация

Проверка параметр

Схема нормализации

Обогащение

Нормализатор	<input type="text" value="[OOTB] Microsoft DNS ETW logs json"/>
Название*	<input type="text" value="[OOTB]-Microsoft-DNS-ETW-logs-json"/>
Метод парсинга* ⓘ	<input type="text" value="regex"/>
Сохранить исходное событие*	<input type="text" value="Не сохранять"/>
Сохранить дополнительные поля*	<input type="text" value="Нет"/>
Примеры событий	<input type="button" value="+ Загрузить из файла"/>

Проверка параметр

Шаги мастера настройки с четвертого по шестой можно пропустить и вернуться к их настройке позднее.

На седьмом шаге мастера задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище**. В случае если предполагается также корреляция по событиям добавьте точку назначения типа **Коррелятор**.

Редактирование коллектора

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация**
- Проверка параметров

Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

+ Добавить 🗑 Удалить			
<input type="checkbox"/>	Название	Тип	URL
<input type="checkbox"/>	[OOTB] Storage	storage	kuma-aio.sales.lab:7230
<input type="checkbox"/>	[OOTB] Correlator	correlator	kuma-aio.sales.lab:7231

На завершающем шаге мастера нажмите на кнопку **Создать и сохранить сервис**. После чего появится строка установки сервиса, которую необходимо скопировать для дальнейшей установки.

Редактирование коллектора



- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров**

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

Сервисы, использующие этот коллектор

Тип	Название
коллектор	ETW Collector (top/5577)

- Сохранить и перезапустить сервисы
- Сохранить и обновить параметры сервисов

Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-aio.sales.lab:7210 --id be451a26-52a2-4ac3-842e-93797d100c9c --api.port 7286 --install
```

Также после выполнения вышеуказанных действий на вкладке **Ресурсы -> Активные сервисы** появится созданный сервис коллектора.

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

Выполните подключение к CLI KUMA (установка коллектора выполняется с правами root).

Для установки сервиса коллектора в командной строке выполните команду, скопированную на прошлом шаге.

```
root@kuma-db:~# /opt/kaspersky/kuma/kuma collector --core https://kuma-db.sales.lab:7210 --id 83458181-b467-49e8-979e-d2fecfb0e952 --api.port 7246 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-83458181-b467-49e8-979e-d2fecfb0e952.service → /lib/systemd/system/kuma-collector-83458181-b467-49e8-979e-d2fecfb0e952.service.
root@kuma-db:~#
```

При необходимости добавьте порт коллектора в исключения фаервола и обновите параметры службы.

```
firewall-cmd --add-port=<порт, выбранный для коллектора>/tcp --permanent
firewall-cmd --reload
```

После успешной установки сервиса его в статус в веб-консоли KUMA изменится на **зеленый**.

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

Для создания агента в веб-интерфейсе KUMA перейдите на вкладку **Ресурсы -> Агенты** и нажмите на кнопку **Добавить агент**.


В открывшейся вкладке **Общие параметры** укажите **Имя агента** и **Тенант**, к которому он будет принадлежать.

Редактирование агента

Общие параметры Подключение №1

Агенты KUMA - это сервисы, которые используются для пересылки необработанных событий с серверов и рабочих станция в точки назначения KUMA. Чтобы создать агент KUMA, выполните шаги мастера установки. Подробнее см. в [онлайн-справке](#).

Название*	<input type="text" value="Agent-ETW"/>
Тенант*	<input type="text" value="Main"/>
Отладка	<input type="checkbox"/>
Описание	<div style="border: 1px solid #ccc; height: 80px;"></div>

 [Скачать конфигурационный ресурс](#)

На вкладке **Подключение 1** в параметрах коннектора задайте имя коннектора, тип `etw` и укажите имя сессии (это имя сборщика созданного на этапе настройки на стороне Windows) в нашем случае это `etwDNS-Analytics`.

Редактирование агента

Общие параметры [Подключение №1](#)

Коннектор

[Основные параметры](#) [Дополнительные параметры](#)

Коннектор	<input type="text" value="Создать"/>
Название*	<input type="text" value="getETW"/>
Тип* ⓘ	<input type="text" value="etw"/>
Имя сессии* ⓘ	<input type="text" value="etwDNS-Analytics"/>
Извлекать информацию о событии	<input checked="" type="checkbox"/>
Извлекать свойства события	<input checked="" type="checkbox"/>

В секции **Точки назначения** укажите имя точки назначения, тип `tcp` (должен совпадать с настройками коллектора). Задайте URL в формате `fqdn:port` (FQDN коллектора и порт, должны совпадать с настройками коллектора).

Точки назначения

[Основные параметры](#) [Дополнительные параметры](#)

Точка назначения	<input type="text" value="Создать"/>
Название*	<input type="text" value="toColl"/>
Состояние	<input checked="" type="checkbox"/>
Тип*	<input type="text" value="tcp"/>
URL* ⓘ	<input type="text" value="kuma-aio.sales.lab:5577"/>
<input type="button" value="+ Добавить"/>	

В дополнительных параметрах укажите размер дискового буфера в 1 Гб.

Точки назначения

Основные параметры Дополнительные параметры

Размер буфера ⓘ	1073741824
Время ожидания ⓘ	0
Размер дискового буфера ⓘ	1073741824
Интервал очистки буфера ⓘ	0
Обработчики	0
Режим TLS	Выключено
Сжатие	Выключено
Политика выбора URL ⓘ	Любой
Разделитель	
Дисковый буфер	<input checked="" type="checkbox"/>

После настройки дополнительных параметров сохраните созданный ресурс агента.

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

В разделе **Ресурсы** -> **Активные сервисы** опубликуйте созданную конфигурацию Agent ETW. Для этого нажмите **Создать сервис** -> выберите созданный сервис агента Agent ETW и нажмите **Создать сервис**. После публикации сервиса скопируйте его идентификатор нажатием на ПКМ данного сервиса для последующей установки агента на Windows сервере.

<input type="checkbox"/>	Статус	Тип	Сервис	Версия	Тенант
<input checked="" type="checkbox"/>	Вкл	Агент	Agent ETW	3.2.0.305	Main
<input checked="" type="checkbox"/>	Вкл	Агент	WEC Agent		Main

Копировать идентификатор
Обновить параметры
Перезапустить

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

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

Для функционирования агента KUMA необходимо создать либо доменную сервисную учетную запись, либо локальную УЗ с помощью которой будет выполняться запуск агента KUMA и обеспечиваться доступ к чтению аналитического журнала.

Для УЗ требуются следующие группы и права:

- **Пользователи журналов производительности (Performance Log Users group)** (чтение журнала, настройка в свойствах пользователя);
- **Вход в качестве службы (Log on service)** (права на запуск сервиса агента, настройка в политиках безопасности).













После запуска сервиса агента можно переключиться на системную локальную учетку (LocalSystem), сделать это можно через Services на Windows. Иногда такое целесообразно при ротации паролей в УЗ.

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

Выполняется на Windows сервере, который обеспечивает прием событий от источников (рабочих станций/серверов). Предварительно FQDN Core KUMA должен быть добавлен в файл hosts на Windows сервере, либо добавлен на DNS-сервере. На Windows сервере рекомендуется создать папку **C:\Users\<имя пользователя>\Desktop\KUMA**.

Далее скопируйте в данную папку исполняемый файл **kuma.exe**.

Файл **kuma.exe** находится в архиве пакетов установки KUMA.

/root/KUMA/kuma-ansible-installer/roles/kuma/files/		
Name	Size	Changed
		13.09.2021 19:52:10
 clickhouse.tar.gz	94 868 KB	13.09.2021 19:52:36
 console.tar.gz	4 339 KB	13.09.2021 19:52:14
 example-content	1 806 KB	13.09.2021 19:52:10
 grafana.tar.gz	33 937 KB	13.09.2021 19:52:32
 kuma	56 291 KB	13.09.2021 19:52:37
 kuma.exe	19 843 KB	13.09.2021 19:52:37
 LEGAL_NOTICES	187 KB	13.09.2021 19:52:10
 LICENSE	41 KB	13.09.2021 19:52:10
 license.key	4 KB	08.10.2021 10:39:28
 mongodb.tar.gz	61 866 KB	13.09.2021 19:52:25
 victoria-metrics.tar.gz	8 713 KB	13.09.2021 19:52:27

Для установки агента KUMA запустите командную строку с правами администратора.

Перейдите в папку **C:\Users\<имя пользователя>\Desktop\KUMA**, примите лицензионное соглашение: `/opt/kaspersky/kuma/kuma.exe license`

Запустите установку агента командой:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --core https://<DOMAIN-NAME-KUMA-CORE-Server>:7210 --id <Windows Agent ID> --user <Имя сервисной доменной УЗ> --install
```

Если агент устанавливается из-под доменной учетной записи пользователь указывается в формате <домен>\<имя учетной записи>, например, demo\user

```
C:\Users\Администратор\Desktop\KUMA>kuma.exe agent --core https://kuma.truecompany.local:7210 --id 7314c259-ed1d-44ec-abd3-8e327e80834a --user truecompany\svc-kuma-wec --install
```

Во время установки сервиса система запросит пароль. Введите пароль сервисной доменной учетной записи.

В результате, на Windows сервере будет установлен сервис KUMA Windows Agent <Windows Agent ID>.

```
User password:
Service KUMAWindowsAgent-7314c259-ed1d-44ec-abd3-8e327e80834a was installed successfully!
C:\Users\Администратор\Desktop\KUMA>
```

Если статус агента в веб-интерфейсе KUMA красный, необходимо удостовериться в доступности портов 7210 и порта коллектора Windows по направлению от агента к KUMA Collector.

Для удаления сервиса агента KUMA по окончании тестирования продукта выполните следующую команду:

```
C:\Users\<имя пользователя>\Desktop\KUMA>kuma.exe agent --id <Windows Agent ID> --uninstall
```

????????? ?????????????? ?????????? Windows ? KUMA

Для проверки, что сбор событий с устройств Windows успешно настроен перейдите в **Ресурсы** -> **Активные сервисы** -> выберите (чекбокс) ранее созданный коллектор для Windows и нажмите **Перейти к событиям**. Либо **ПКМ** - **Перейти к событиям**. В открывшемся окне **События** убедитесь, что присутствуют события с Windows-устройств.

События

```
1 SELECT * FROM `events` WHERE `ServiceID` = 'bbdc1414-3d96-4c1e-8804-09068ce75f9e' ORDER BY `Timestamp` DESC LIMIT 10
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

TenantID	Timestamp	Name	DeviceProduct
Main	26.06.2024 16:53:55:312	QUERY_RECEIVED	DNS Server
Main	26.06.2024 16:53:55:312	INTERNAL_LOOKUP_CNAME	DNS Server
Main	26.06.2024 16:53:55:312	INTERNAL_LOOKUP_CNAME	DNS Server
Main	26.06.2024 16:53:55:312	INTERNAL_LOOKUP_CNAME	DNS Server
Main	26.06.2024 16:53:55:312	RECURSE_QUERY_OUT	DNS Server
Main	26.06.2024 16:53:55:312	QUERY_RECEIVED	DNS Server
Main	26.06.2024 16:53:55:312	RESPONSE_SUCCESS	DNS Server
Main	26.06.2024 16:53:55:312	RECURSE_RESPONSE_IN	DNS Server
Main	26.06.2024 16:53:52:523	INTERNAL_LOOKUP_CNAME	DNS Server
Main	26.06.2024 16:53:52:523	INTERNAL_LOOKUP_CNAME	DNS Server
Main	26.06.2024 16:53:52:522	RECURSE_RESPONSE_IN	DNS Server
Main	26.06.2024 16:53:52:522	INTERNAL_LOOKUP_CNAME	DNS Server

Информация о событии

DeviceCustomNumber2	1
DeviceCustomNumber2Label	QTYPE
DeviceCustomNumber3	1
DeviceCustomNumber3Label	Properties - RD
DeviceCustomString1	10.68.85.92
DeviceCustomString1Label	Properties - source
DeviceCustomString3	.
DeviceCustomString3Label	Additional - info
DeviceCustomString6	0xED9E010000010000000000000377777770462696E6703636F6D0000010001
DeviceCustomString6Label	Packet - data
Service	!BorisTest (top/5577)dd
FileName	etwDNS-Analytics
FlexNumber1	30
FlexNumber1Label	Buffer - size
FlexNumber2	256
FlexNumber2Label	Flags
FlexString1	EB79061A-A566-4698-9119-3ED2807060E7
FlexString1Label	Provider - GUID

Revision #15

Created 2024-05-06 14:52:33 UTC by Boris Rzr

Updated 2025-12-09 11:32:09 UTC by Boris Rzr