

Создание и установка сервисов

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

Хранилище

Хранилище состоит из двух частей: одна часть создается в веб-интерфейсе KUMA, а вторая устанавливается на сервере или серверах, предназначенных для хранения событий. Серверная часть хранилища KUMA представляет собой собранные в кластер узлы ClickHouse.

Статья онлайн-справки «Структура кластера ClickHouse»:

<https://support.kaspersky.ru/kuma/4.0/221938>

Создание хранилища выполняется в несколько этапов:

- Создание ресурса хранилища в веб-интерфейсе KUMA.
- Создание сервиса хранилища в веб-интерфейсе KUMA.
- Установка узлов хранилища на сервере или серверах.

Создание ресурса Хранилища

Если установка сервиса **хранилища** планируется с помощью «коробочного» ресурса **[OOTB] Storage** перейдите в Раздел [Установка сервиса хранилища](#).

Чтобы создать ресурс хранилища:

- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Хранилища** нажмите **Добавить хранилище**.
- В окне **Создание хранилища**:
 - На вкладке **Основные параметры** в поле **Название хранилища** введите уникальное имя создаваемого сервиса.

- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.
- В поле **Варианты условий хранения** выберите для хранилища условие хранения событий в кластере ClickHouse, при выполнении которого события будут переноситься на диски холодного хранения или удаляться, если холодное хранение не настроено или настроено неверно. Условие будет применено к пространству по умолчанию и к событиям из удаленных пространств.

По умолчанию ClickHouse перемещает события на диски холодного хранения или удаляет их, если заполнено более 97% хранилища. В KUMA при создании хранилища также используется дополнительное условие хранения 365 дней. Вы можете настроить пользовательские условия хранения для более устойчивой работы хранилища.

Дни: Если вы хотите ограничить срок хранения событий, в раскрывающемся списке выберите Дни и в поле укажите максимальный срок хранения событий в днях в кластере горячего хранилища ClickHouse.

По истечении указанного срока события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Минимальное значение – 1. Значение по умолчанию – 365.

ГБ: Если вы хотите ограничить максимальный размер хранилища, в раскрывающемся списке выберите ГБ и в поле укажите максимальный размер хранилища в гигабайтах. Когда размер хранилища достигнет указанного значения, события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Минимальное значение и значение по умолчанию – 1 ГБ.

Проценты: Если вы хотите ограничить размер хранилища относительно объема диска, который доступен хранилищу, в раскрывающемся списке выберите **Проценты** и укажите максимальный размер хранилища в процентах от доступного объема диска. Когда размер хранилища достигнет указанной доли от доступного ему размера диска, события будут автоматически перенесены на диски холодного хранения или удалены из кластера ClickHouse, начиная с партиций за самую старую дату. Допустимые значения – от 1 до 95. Значение по умолчанию – 80.

Статья онлайн-справки «Холодное хранение событий»:

<https://support.kaspersky.ru/kuma/4.0/243503>

- В поле **Срок хранения событий аудита** укажите, в течение какого количества дней вы хотите хранить события аудита. Минимальное значение и значение по умолчанию: 365.

- Укажите параметры узла кластера ClickHouse (ниже пример для архитектуры All-in-One):
 - FQDN (доменное имя сервера, например, kuma.demo.lab)
 - Идентификатор шарда – 1
 - Идентификатор реплики – 1
 - Идентификатор кипера – 1
- Нажмите **Создать**.

Создание хранилища

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

Хранилище KUMA используется для хранения нормализованных событий, чтобы у вас был быстрый доступ к событиям с возможностью извлечь аналитические данные. Скорость и бесперебойность доступа обеспечивается за счет использования технологии ClickHouse. Это означает, что хранилище - это кластер ClickHouse, связанный с сервисом хранилища KUMA. Чтобы создать хранилище KUMA, выполните шаги мастера установки. Подробнее см. в [онлайн-справке](#).

Название хранилища*	[OOTB] Storage 1
Тенант*	Main 2
Теги	
Описание	
Варианты условий хранения* ⓘ	14 3 80 4 Дни Проценты
Срок хранения событий аудита* ⓘ	365 5
Переопределение параметров ClickHouse ⓘ	

Узлы кластера ClickHouse

FQDN*	kuma.demo.lab 6
Идентификатор шарда* ⓘ	1 7
Идентификатор реплики* ⓘ	1 8
Идентификатор кипера* ⓘ	1 9

10

Ресурс хранилища создан и доступен в разделе **Ресурсы → Хранилища**.

Установка сервиса хранилища

Для установки сервиса хранилища:

- Перейдите в **Ресурсы → Активные сервисы** и нажмите **Добавить**.
- В появившемся окне выберите импортированный/созданный ресурс хранилища и нажмите **Создать сервис**.

Выберите сервис

storage 1

Название	Название тена...	Тип
[OOTB] Storage 2	Main	storage

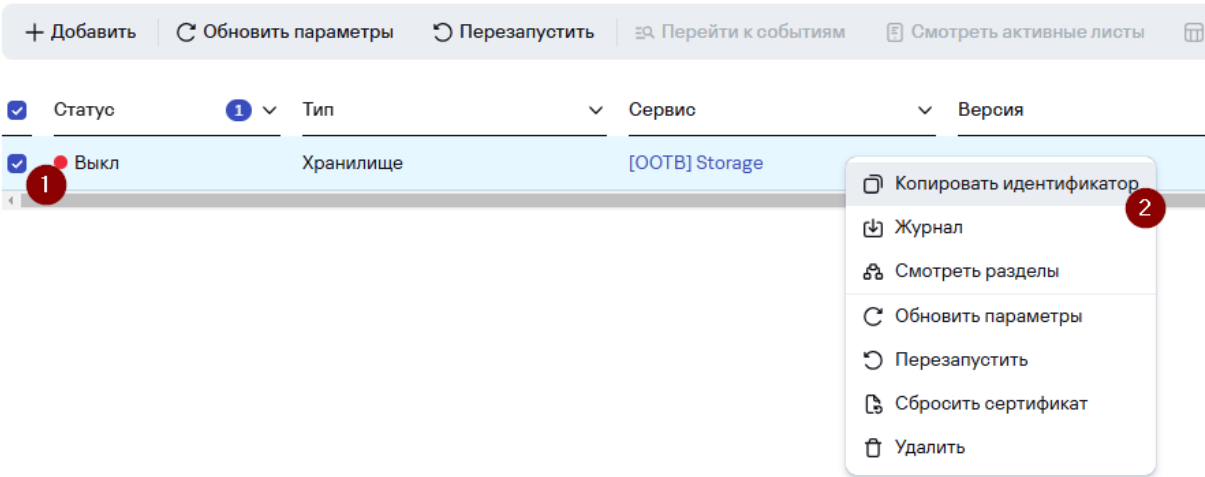
3

Создать сервис

Отмена

- Нажмите **ПКМ** на строку с сервисом Storage и выберите **Копировать идентификатор**.

Сервисы

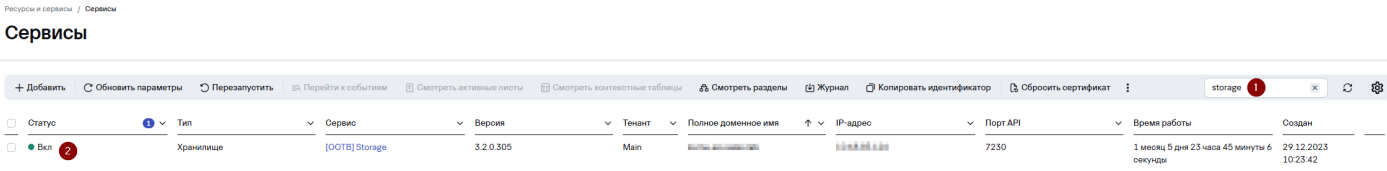


- Выполните подключение к CLI сервера, на котором выполнялось развертывание KUMA.
- Для установки сервиса хранилища в командной строке выполните следующую команду под учетной записью root:

```
/opt/kaspersky/kuma/kuma storage https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA> --api.port 7230 --install
```

Пример: `/opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --id XXXXX --api.port 7230 --install`

- В веб-интерфейсе KUMA перейдите в **Ресурсы** → **Активные сервисы** и убедитесь, что сервис хранилища (Storage) находится в статусе **Вкл** с зеленой индикацией.



Установка сервиса хранилища успешно завершена.

На одном сервере может быть установлен только один сервис хранилища.

Создание ресурса Точка назначения, тип Storage

Точки назначения задают сетевые параметры для передачи нормализованных событий. Точки назначения используются в коллекторах и корреляторах для описания того, куда передавать обработанные события. Как правило, в роли точек назначения выступают коррелятор и хранилище.

Данный шаг является опциональным. В случае если были импортированы демонстрационные ресурсы из файла ootb-content, достаточно указать актуальный URL и порт в параметрах ресурса **Точка назначения [OOTB] Storage**. Для этого:

- Перейдите в **Ресурсы** → **Точки назначения**.
- Выберите ресурс **[OOTB] Storage**.
- В поле URL укажите актуальный FQDN и порт сервиса хранилища.
- Нажмите **Сохранить**.

Редактирование точки назначения

Основные параметры

Дополнительные параметры

Название*

[OOTB] Storage

Тенант*

Main

Состояние



Тип*

storage

URL* ⓘ

kuma.demo.lab:7230

1

+ Добавить

Описание

Описание

Сохранить

Отмена

Для создания ресурса **Точка назначения тип Storage**:

- Перейдите в раздел **Ресурсы** → **Точки** назначения и нажмите **Добавить**.
- В появившемся окне **Создание точки назначения** укажите:
 - **Название** – например, **[OOTB] Storage**
 - **Тенант** – Main (по умолчанию)
 - **Состояние** – во включенном состоянии
 - **Тип** – storage
 - **URL** – <FQDN сервера KUMA>:<API-порт, используемый сервисом Storage. По умолчанию 7230>
 - **Описание** (опционально)

Создание точки назначения

Основные параметры

Дополнительные параметры

Название*	[OOTB] Storage 1
Тенант*	Main 2
Состояние	☒ 3
Тип*	storage 4
URL* ⓘ	kuma.demo.lab:7230 5
	+ Добавить
Описание	Описание 6

- Нажмите **Создать**.

Точка назначения успешно создана.

Коррелятор

Коррелятор состоит из двух частей: одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на сервере, предназначенном для обработки событий.

Создание коррелятора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы объединяются в набор ресурсов для коррелятора, а по завершении мастера на основе этого набора ресурсов автоматически

создается и сам сервис.

Создание сервиса Коррелятора

Если установка сервиса коррелятора планируется с помощью «коробочного» ресурса **[OOTB] Correlator** перейдите в раздел [Установка сервиса Коррелятора](#).

Чтобы создать сервис коррелятора:

- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** и нажмите **Создать коррелятор**.
- В появившемся окне мастера настройки **Создание коррелятора** на первом шаге (**Общие**) укажите **Название коррелятора** и **Тенант**, к которому будет принадлежать создаваемый коррелятор (по умолчанию **Main**).

Создание коррелятора

Общие **1**

Глобальные переменные

Корреляция

Обогащение

Реагирование

Маршрутизация

Проверка параметров

Общие

Коррелятор используется для анализа поступающих в него событий с целью выявления угроз: в случае подозрительной активности создаются алерты и рассылаются оповещения. Кроме того, коррелятор можно настроить на дополнение информации, содержащейся в событиях. Чтобы создать коррелятор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

Название*

[OOTB] Correlator **2**

Тенант*

Main **3**

Обработчики

0

Отладка

☐

Описание

- Шаги со **2 (Глобальные переменные)** по **5 (Реагирование)** можно пропустить и при необходимости настроить позднее.
- Перейдите на шаг **Маршрутизация** и нажмите **Добавить**. В появившемся окне **Создание точки назначения**:
 - В поле **Точка назначения** выберите ранее созданную точку назначения типа **Storage** (параметры точки назначения подставляются автоматически).
 - Нажмите **Сохранить**.

Создание точки назначения

Основные параметры

Дополнительные параметры

Точка назначения

Создать

1



Название*

Создать

Состояние



Тип*

[OOTB] Storage

Main/.../OOTB

2

- На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.
- В окне появится **Рекомендуемая команда для установки коррелятора**, скопируйте команду и далее выполните установку сервиса коррелятора согласно разделу [Установка сервиса Коррелятора](#).

Установка сервиса коррелятора

Если установка сервиса коррелятора планируется с помощью «коробочного» ресурса **[OOTB] Correlator**:

- Перейдите в **Ресурсы** → **Активные сервисы** и нажмите **Добавить**.
- В появившемся окне выберите импортированный ресурс коррелятора и нажмите **Создать сервис**.
- Далее нажмите на название созданного сервиса коррелятора.
- В появившемся окне **Редактирование коррелятора** перейдите на шаг **Проверка параметров** и скопируйте **Рекомендуемую команду для установки коррелятора**.

Для установки сервиса коррелятора:

- Выполните подключение к CLI сервера, на котором выполнялось развертывание KUMA.
- Для установки сервиса коррелятора в командной строке выполните ранее скопированную команду под учетной записью **root**.
- В веб-интерфейсе KUMA перейдите в **Ресурсы** → **Активные сервисы** и убедитесь, что сервис **коррелятора (Correlator)** находится в статусе **Вкл** с зеленой индикацией.

Установка сервиса Коррелятора успешно завершена.

Создание ресурса Точка назначения, типа Correlator

Данный шаг является опциональным. В случае если были импортированы демонстрационные ресурсы из файла ootb-content, достаточно указать актуальный URL и порт в параметрах ресурса **Точка назначения [OOTB] Correlator**. Для этого:

- Перейдите в **Ресурсы** → **Точки назначения**.
- Выберите ресурс **[OOTB] Correlator**.
- В поле URL укажите актуальный FQDN и порт сервиса коррелятора.
- Нажмите **Сохранить**.

Редактирование точки назначения

Для создания ресурса Точка назначения тип Correlator:

- Перейдите в раздел **Ресурсы** → **Точки назначения** и нажмите **Добавить**.
- В появившемся окне **Создание точки назначения** укажите:
 - **Название** – например, [OOTB] Correlator.
 - **Тенант** – Main (по умолчанию)
 - **Состояние** – во включенном состоянии
 - **Тип** – correlator
 - **URL** – <FQDN сервера KUMA>:<API-порт, используемый сервисом Correlator. По умолчанию 7231>
 - **Описание** (опционально)

Создание точки назначения

Основные параметры

Дополнительные параметры

Название*	[OOTB] Correlator 1
Тенант*	Main 2
Состояние	☒ 3
Тип*	correlator 4
URL* ①	kuma.demo.lab:7231 5
	+ Добавить
Описание	Описание 6

- Нажмите **Создать**.

Точка назначения успешно создана.

Статья онлайн-справки «Создание коррелятора»:
<https://support.kaspersky.ru/kuma/4.0/217787>

Коллектор

См. статью [Создание коллектора KUMA](#)

Revision #4

Created 2026-08-18 13:18:08 UTC by Dmitry Borisov

Updated 2026-08-18 14:49:42 UTC by Dmitry Borisov