

Создание сервисов KUMA для SMP

Создание сервисов KUMA

В разделе описано создание хранилища (Storage), коррелятора (Correlator) и коллектора (Collector) KUMA.

Убедитесь, что хост, на который выполняется установка сервиса резолвит FQDN Ядра KUMA, заданный при установке SMP.

Убедитесь, что кластер SMP резолвит FQDN хоста, на который планируется установка сервиса (FQDN хоста должен разрешаться через DNS-сервер, который использует SMP).

В случае наличия локального МЭ на хосте с сервисами KUMA не забудьте добавить разрешающие правила для портов сервисов: API-порты, указанные в таблицы Активных сервисов и порты приема событий Коллекторами, заданные в настройках Транспорта соответствующих коллекторов. Примеры команд доступны [здесь](#).

Подготовка целевого устройства для установки сервисов

Если устройства уже подготовлены к установке сервисов KUMA (при установке SMP был указан файл инвентаря KUMA в разделе inventory) пропустите этот раздел и переходите к следующему.

Если в процессе установки SMP не был указан файл инвентаря KUMA в разделе inventory и устройства не были подготовлены для установки сервисов - их можно подготовить после установки SMP по инструкции ниже.

1. Выполните **все** шаги инструкции по развертыванию начиная с проверки [Аппаратных требований](#) и заканчивая [созданием файла инвентаря для сервисов KUMA](#).

Шаги после создания инвентаря для сервисов KUMA выполнять не нужно!

2. Перейдите на хост администратора, с которого ранее выполнялась установка SMP в директорию с утилитой KDT.

3. Выполните команду:

```
./kdt invoke kuma --action addHosts --param host_inventory='<путь_к_файлу_инвентаря>'
```

4. Дождитесь окончания установки, после чего переходите к следующим разделам для установки сервисов.

Создание хранилища (Storage)

Перейдите в **Мониторинг** → **Ресурсы и сервисы** → **Хранилища** → **Создать** и используйте пошаговый мастер настройки:

- В разделе **Основные параметры** укажите произвольное имя хранилища и требуемый тенант.
- Задайте **Варианты условий хранения** и **Срок хранения событий аудита** (в днях).
- В **Узлах кластера ClickHouse** укажите FQDN хранилища, а также идентификаторы шарда, реплики и кипера.
- В конце нажмите **Создать**.

Перейдите в **Мониторинг** → **Ресурсы и сервисы** → **Хранилища**, нажмите ПКМ по только что добавленному хранилищу и выберите опцию **Копировать идентификатор** - этот параметр потребуется для установки сервиса.

Затем установите сервис **Storage** из SSH-консоли следующей командой

```
/opt/kaspersky/kuma/kuma storage --core https://<kuma_core_FQDN>:7210 --id <service_id> --api.port 7230 --install
```

Здесь `<kuma_core_FQDN>` - доменное имя Ядра KUMA, заданное при установке SMP. По умолчанию - kuma.<smp_domain>.

А `<service_id>` - идентификатор сервиса, скопированный ранее.

Создание точки назначения типа Хранилище

После установки хранилища, необходимо создать точку назначения, которая будет использоваться остальными сервисами для передачи событий в Хранилище. Для создания точки назначения выполните следующее:

Перейдите в **Мониторинг → Ресурсы и сервисы → Точки назначения → Создать**.

Выберите **Тип** точки назначения **storage**.

Нажмите на поле **URL** - в выпадающем списке появятся доступные адреса Хранилища, выберите адрес только что созданного хранилища.

Название точки назначения заполнится автоматически.

Создание коррелятора (Correlator)

Перейдите в **Мониторинг → Ресурсы и сервисы → Корреляторы → Создать** и используйте пошаговый мастер настройки:

- В разделе **Общие** укажите произвольное имя коррелятора и требуемый тенант.
- В разделе **Корреляция** привяжите все необходимые правила корреляции.
- В разделе **Маршрутизация** нажмите **Добавить** и выберите ранее созданную точку назначения Хранилища.
- В разделе **Проверка параметров** выберите **Сохранить и создать сервис**.

В результате KUMA отобразит команду для установки коррелятора в ОС. Скопируйте её, нажмите кнопку **Сохранить** и вставьте команду в SSH-консоль.

Создание точки назначения типа Коррелятор

После установки коррелятора, необходимо создать точку назначения, которая будет использоваться коллекторами для передачи событий в Коррелятор для сопоставления с правилами корреляции на потоке и последующим созданием Алертов и Инцидентов. Для создания точки назначения выполните следующее:

Перейдите в **Мониторинг → Ресурсы и сервисы → Точки назначения → Создать**.

Выберите **Тип** точки назначения **correlator**.

Нажмите на поле **URL** - в выпадающем списке появятся доступные адреса Корреляторов, выберите адрес только что созданного коррелятора.

Название точки назначения заполнится автоматически.

Создание коллектора (Collector)

Более подробные инструкции по созданию Коллектора и подключению различных источников можно найти в соответствующем [разделе](#).

Перейдите в **Мониторинг → Ресурсы и сервисы → Коллекторы → Создать** и используйте пошаговый мастер настройки:

- В разделе **Подключение источников** укажите произвольное **Имя** коллектора и требуемый **Тенант**.
- В разделе **Транспорт** укажите **Тип** (протокол) и **URL** (:порт или FQDN:порт), по которым коллектор будет принимать данные от источника.
- В разделе **Парсинг событий** выберите метод нормализации. Фильтрация, агрегация и обогащение событий - необязательные настройки.
- В разделе Маршрутизация добавьте ранее созданные точки назначения Коррелятор и Хранилища.
- В разделе **Проверка параметров** выберите **Сохранить и создать сервис**.

В результате KUMA отобразит команду для установки коллектора в ОС. Скопируйте её, нажмите кнопку **Сохранить** и вставьте команду в SSH-консоль.

Проверка поступления событий

Перейдите в **Мониторинг → Ресурсы и сервисы → Активные сервисы** и выберите ранее созданный коллектор галочкой.

В верхнем меню выберите **Перейти к событиям**.

Дождитесь загрузки окна **Поиск угроз** и нажмите кнопку **Выполнить запрос**

В таблице ниже должны отобразиться события.

Дополнительные материалы

[Создание и установка сервисов KUMA \(подробно\)](#)

Revision #1

Created 2026-08-19 07:29:22 UTC by Koala

Updated 2026-08-19 08:28:04 UTC by Koala