Другие типы источников

- Кибер Бэкап (Cyber Backup)
- Zecurion DLP
- Dr.Web Enterprise Security Suite
- Битрикс24 (Bitrix24) CRM
- ALD Pro отправка логов

Кибер Бэкап (Cyber Backup)

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

Настройка коллектора KUMA

Настройка коллектора KUMA для приема и обработки событий **Кибер Бэкап** приведена в отдельной общей статье по созданию сервиса коллектора.

> На шаге **Парсинг событий** в качестве нормализатора для событий **Кибер Бэкап** выберите нормализатор **[OOTB] Cyberprotect Cyber Backup syslog**.

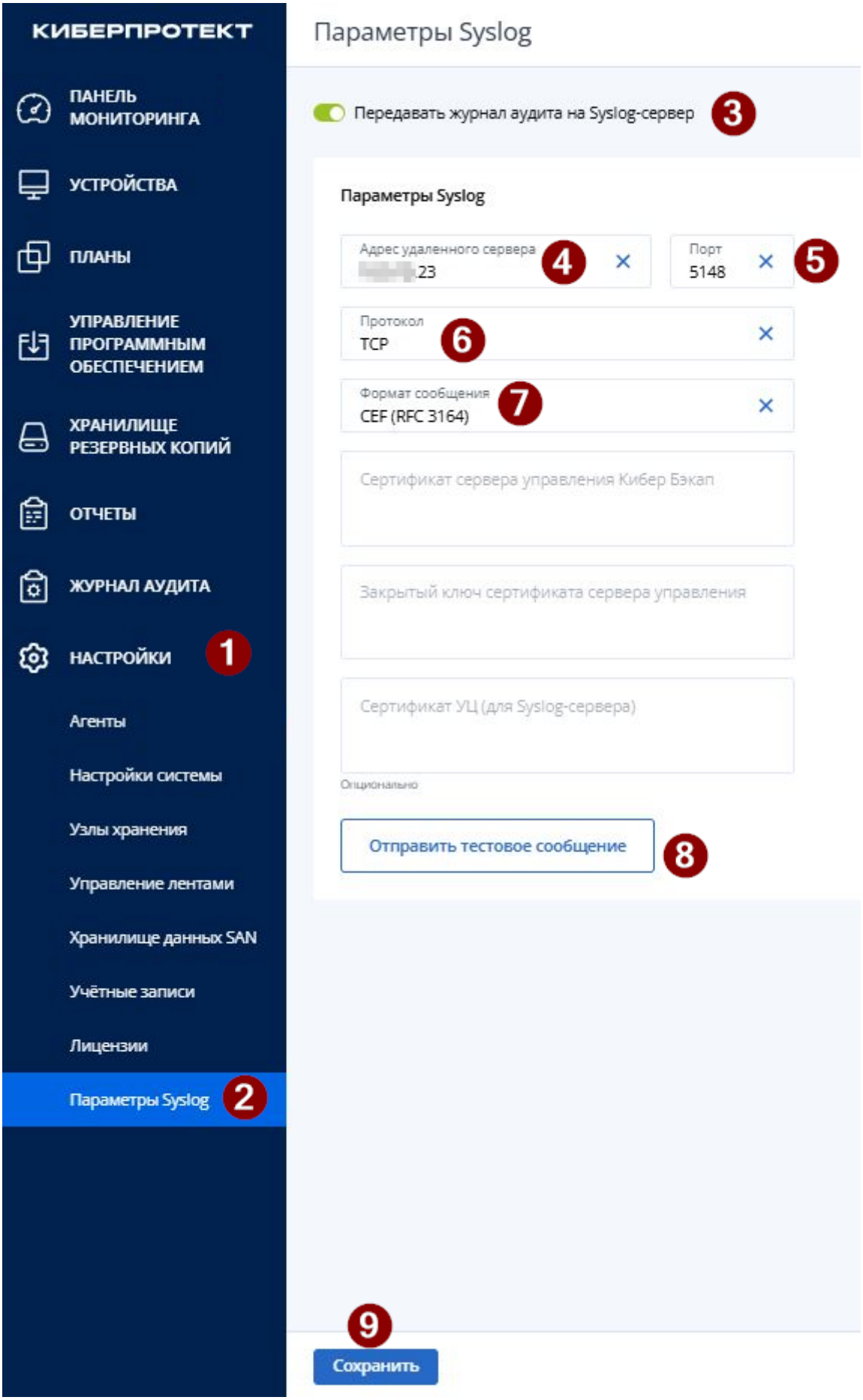
Настройка Кибер Бэкап

По умолчанию журнал аудита хранится в базе данных продукта Кибер Бэкап, однако для централизованного хранения и обработки можно настроить отправку записей журнала аудита в SIEM-систему. Для событий может использоваться протокол TCP, UDP или TLS.

Чтобы настроить отправку событий **Кибер Бэкап** в коллектор KUMA:

- В веб-интерфейсе **Кибер Бэкап** перейдите в **Настройки → Параметры Syslog.**
- В окне **Параметры Syslog** активируйте параметр **Передавать журнал аудита на Syslog-сервер** и укажите:
  - В поле **Адрес удаленного сервера** IP-адрес/DNS-имя сервера коллектора KUMA.
  - **Порт** для подключения (используйте значение, заданное на шаге **Транспорт** при создании коллектора).
  - Используемый **протокол** (используйте значение, заданное на шаге **Транспорт** при создании коллектора).
  - **Формат сообщения**, в котором будут отправляться события. Выберите **CEF (RFC 3164)**.
- Нажмите **Отправить тестовое сообщения** для проверки интеграции.

- Нажмите **Сохранить**.

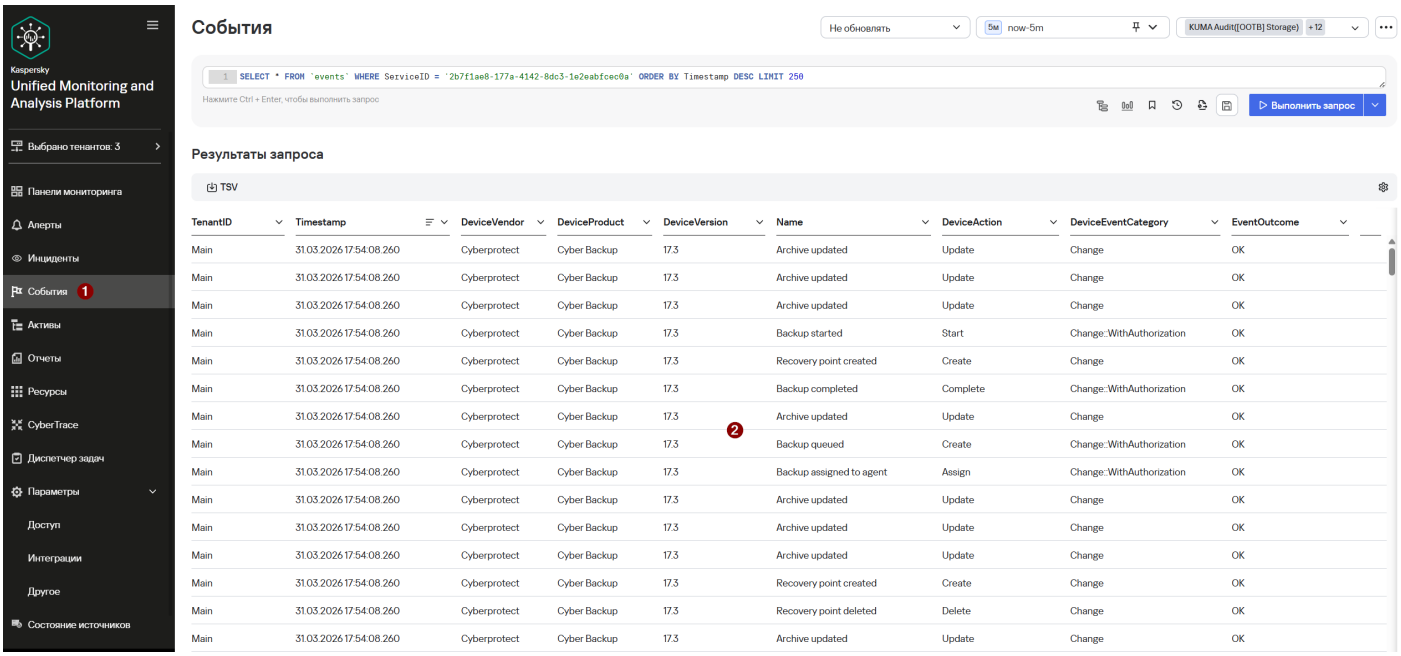


> Опционально в Кибер Бэкап поддерживается настройка защищенного соединения с использованием протокола TLS.

Проверка поступления событий Кибер Бэкап в KUMA

Для проверки, что сбор событий **Кибер Бэкап** успешно настроен перейдите в **Ресурсы** > **Активные сервисы** > выберите ранее созданный коллектор для **Кибер Бэкап** > ПКМ > **Перейти к событиям.**

В открывшемся окне **События** убедитесь, что присутствуют события **Кибер Бэкап**.



Полезные ссылки

[Документация Кибер Бэкап]

Zecurion DLP

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

Настройка коллектора KUMA

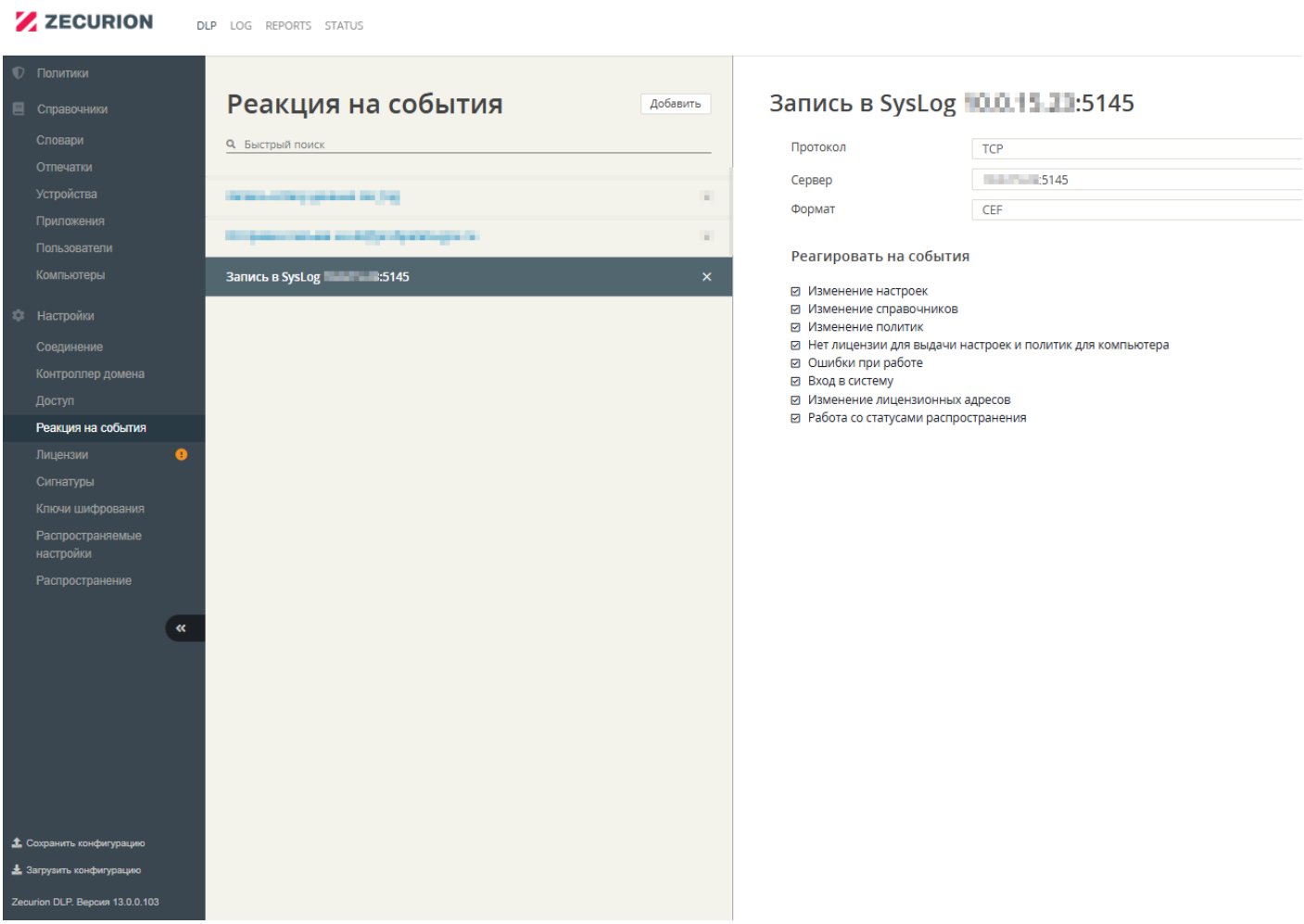
Настройка коллектора KUMA для приема и обработки событий **Zecurion DLP** приведена в отдельной общей статье по созданию сервиса коллектора.

> На шаге **Парсинг событий** в качестве нормализатора для событий **Zecurion DLP** выберите нормализатор **[OOTB] Zecurion DLP syslog CEF**

Настройка Zecurion DLP

Чтобы настроить отправку событий **Zecurion DLP** в коллектор KUMA:

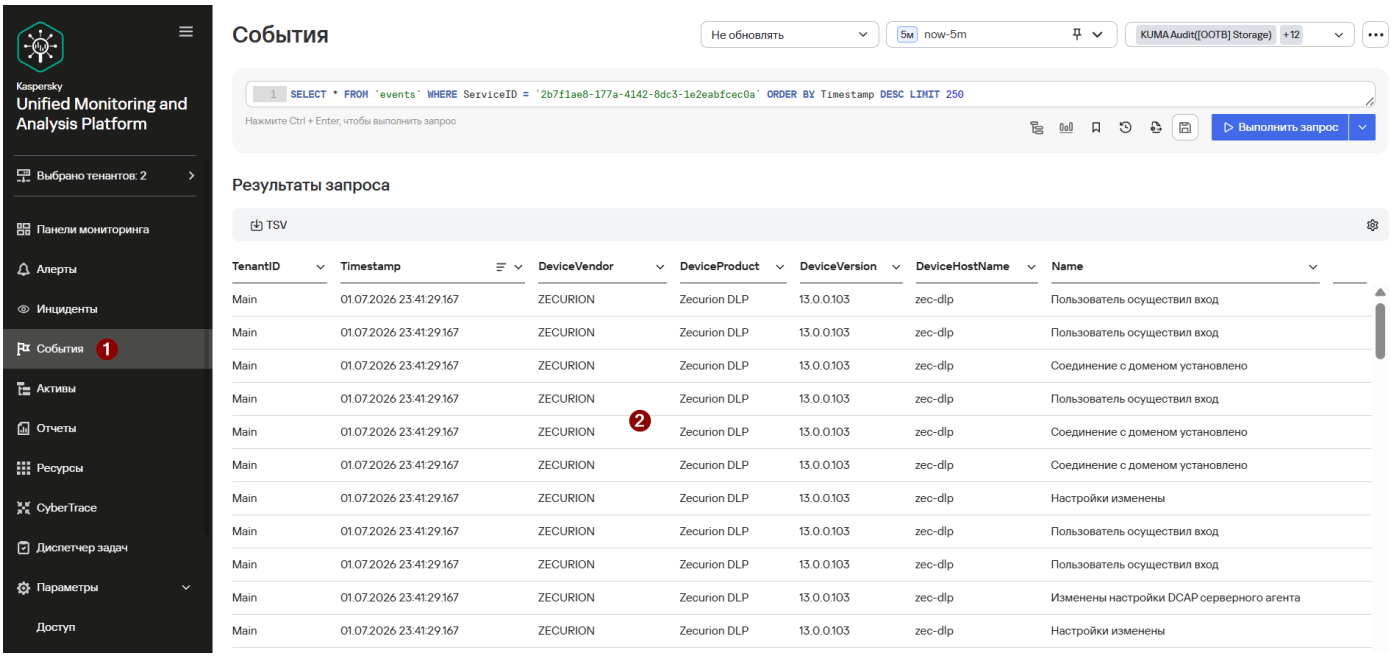
- В веб-интерфейсе **Zecurion DLP** перейдите в **Настройки → Реакция на события.**
- В окне **Реакция на события** нажмите **Добавить**. В появившемся окне **Запись в Syslog** укажите:
  - В поле **Протокол** используемый протокол (используйте значение, заданное на шаге **Транспорт** при создании коллектора).
  - В поле **Сервер** IP-адрес/DNS-имя сервера коллектора KUMA и порт для подключения (используйте значение, заданное на шаге **Транспорт** при создании коллектора).
  - **Формат**, в котором будут отправляться события. Выберите **CEF.**
  - В секции **Реагировать на события** типы событий для отправки в KUMA.



Проверка поступления событий Zecurion DLP в KUMA

Для проверки, что сбор событий **Zecurion DLP** успешно настроен перейдите в **Ресурсы** > **Активные сервисы** > выберите ранее созданный коллектор для **Zecurion DLP** > ПКМ > **Перейти к событиям.**

В открывшемся окне **События** убедитесь, что присутствуют события **Zecurion DLP**.



TenantID	Timestamp	DeviceVendor	DeviceProduct	DeviceVersion	DeviceHostName	Name
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Пользователь осуществил вход
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Пользователь осуществил вход
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Соединение с доменом установлено
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Пользователь осуществил вход
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Соединение с доменом установлено
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Соединение с доменом установлено
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Настройки изменены
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Пользователь осуществил вход
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Пользователь осуществил вход
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Изменены настройки DCAP серверного агента
Main	01.07.2026 23:41:29.167	ZECURION	Zecurion DLP	13.0.0.103	zec-dlp	Настройки изменены

Dr.Web Enterprise Security Suite

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

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://cdn-download.drweb.com/pub/drweb/esuite/13.0.1/documentation/html/ru/admin_manual/index.html?notifications_configure.htm

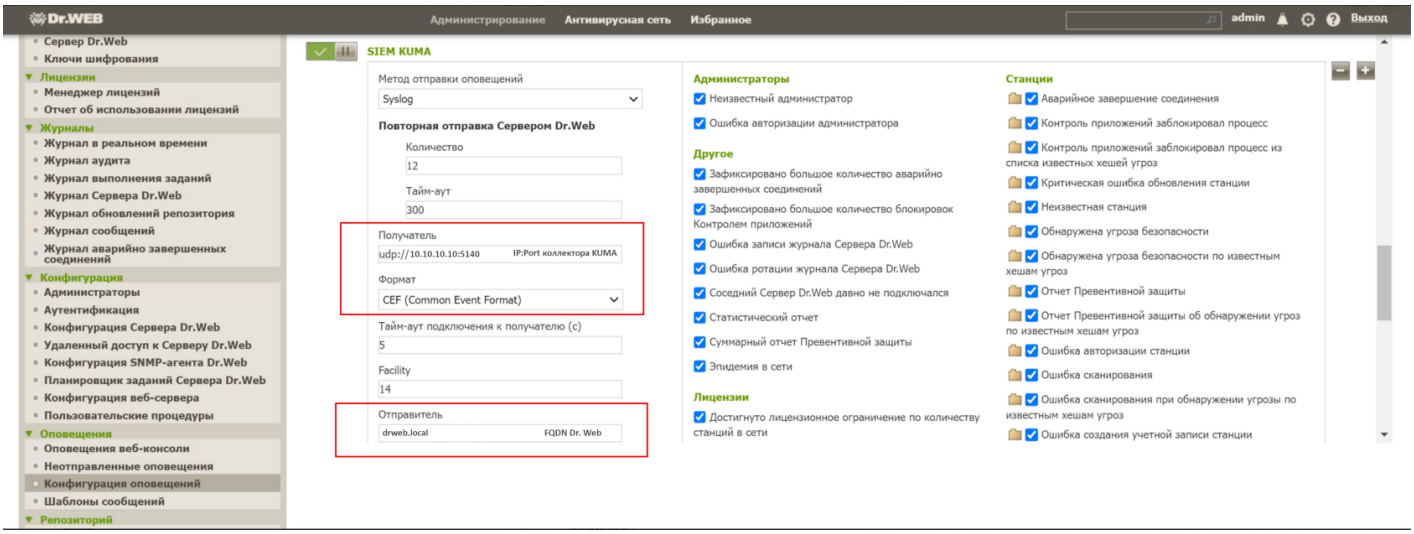
Настройка на стороне Dr.WEB Enterprise Security Suite

Настройка производится под встроенным УЗ admin в его разделе **Администрирование → Конфигурация оповещений**

У него два блока настроек оповещений:

- первый настроен под email;
- второй (SIEM KUMA) под Syslog.

Для настройки в этой версии сервера Dr.Web лучше прямо под встроенным УЗ admin в консоль заходить. У других админов этот блок может быть не всегда виден, либо не работать кнопка тестового события, либо ещё что-то.



Настройка коллектора KUMA по аналогии с этой главой (предварительно выберите тип коннектора **UDP**) - **ссылка**

Рекомендуемый парсер (без агрегации/склейки событий) для правил корреляции Community - **[2024-09-23] Dr. Web CEF** (из Community-Pack)

Битрикс24 (Bitrix24) CRM

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

Настройка Битрикс24 CRM

В данной статье рассматривается вариант, когда в качестве базы данных Битрикс24 CRM используется MySQL. Все настройки выполняются **в консоли** сервера БД с помощью утилиты **mysql**. Вы можете использовать наиболее привычный для Вас способ.

> Протестировано на версии Битрикс24 CRM 24.0.400

Создание пользователя БД и предоставление прав

- В консоли сервера выполните подключение к БД MySQL с правами администратора (по умолчанию **root**).

```
mysql -u root -p
```

> Если пароль для пользователя **root** не установлен, попробуйте подключиться без `-p`

- Создайте нового пользователя, который сможет подключаться к серверу MySQL только с IP-адреса сервера KUMA (коллектора KUMA в случае распределенной инсталляции).

```
CREATE USER 'kuma'@'10.10.10.10' IDENTIFIED BY '<задайте пароль>';
```

- Предоставьте пользователю права доступа. В данном случае предоставляется право выполнять операцию `SELECT` (только чтение) к таблице `b_event_log` в базе данных `sitemanager`.

```
GRANT SELECT ON sitemanager.b_event_log TO 'kuma'@'10.10.10.10';
```

- MySQL автоматически обновит привилегии для нового пользователя.
- Чтобы убедиться, что права были предоставлены корректно, выполните следующую команду для отображения прав созданного пользователя:

```
SHOW GRANTS FOR 'kuma'@'10.10.10.10';
```

> По умолчанию сервер MySQL настроен на работу только с локальным подключением через `localhost.` При необходимости разрешите удаленные запросы и входящие соединения на порт TCP/3306 (используется по умолчанию) на локальном МЭ.

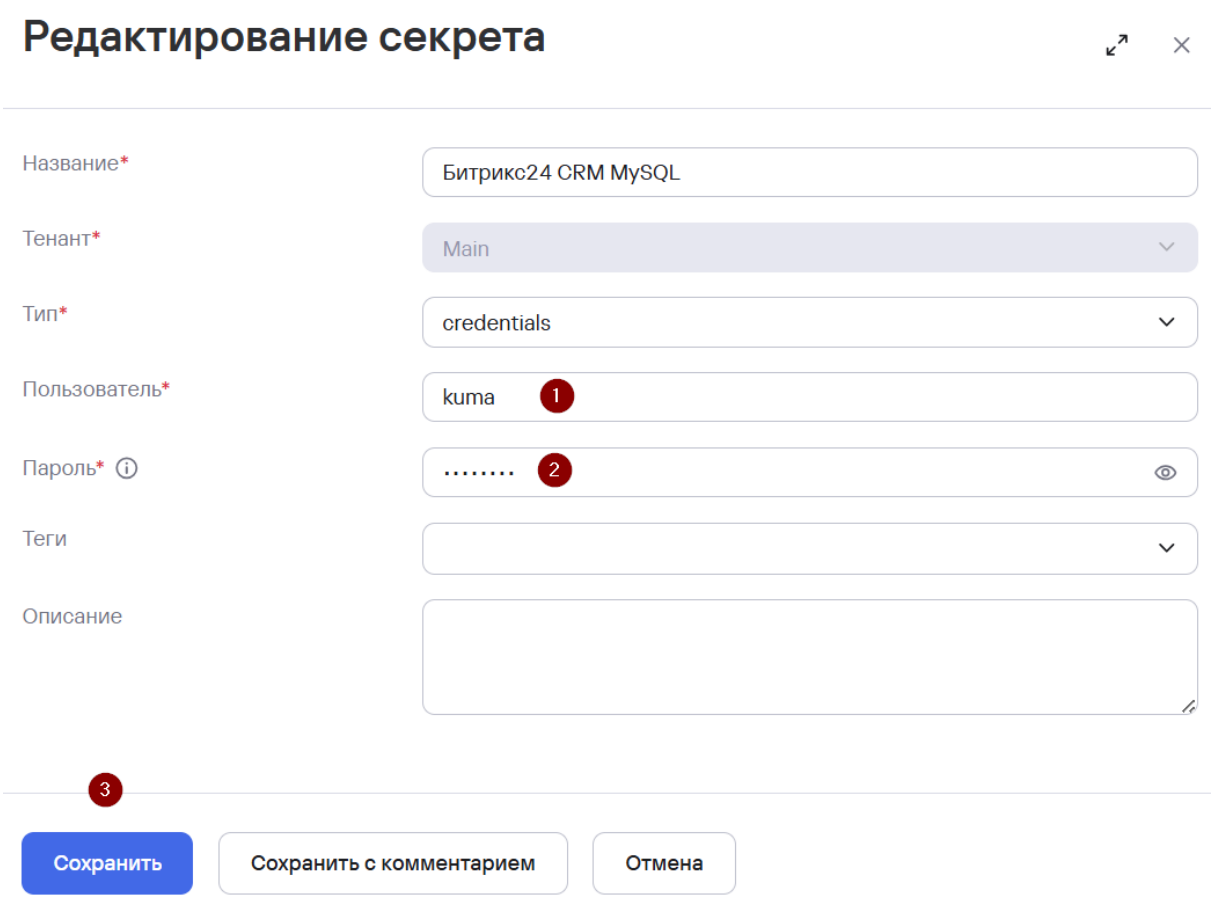
Настройка KUMA

Импорт набора ресурсов Битрикс24 CRM MySQL

- Выполните импорт набора ресурсов KUMA для Битрикс24 CRM MySQL (пароль `q123123Q!q123123Q!`).

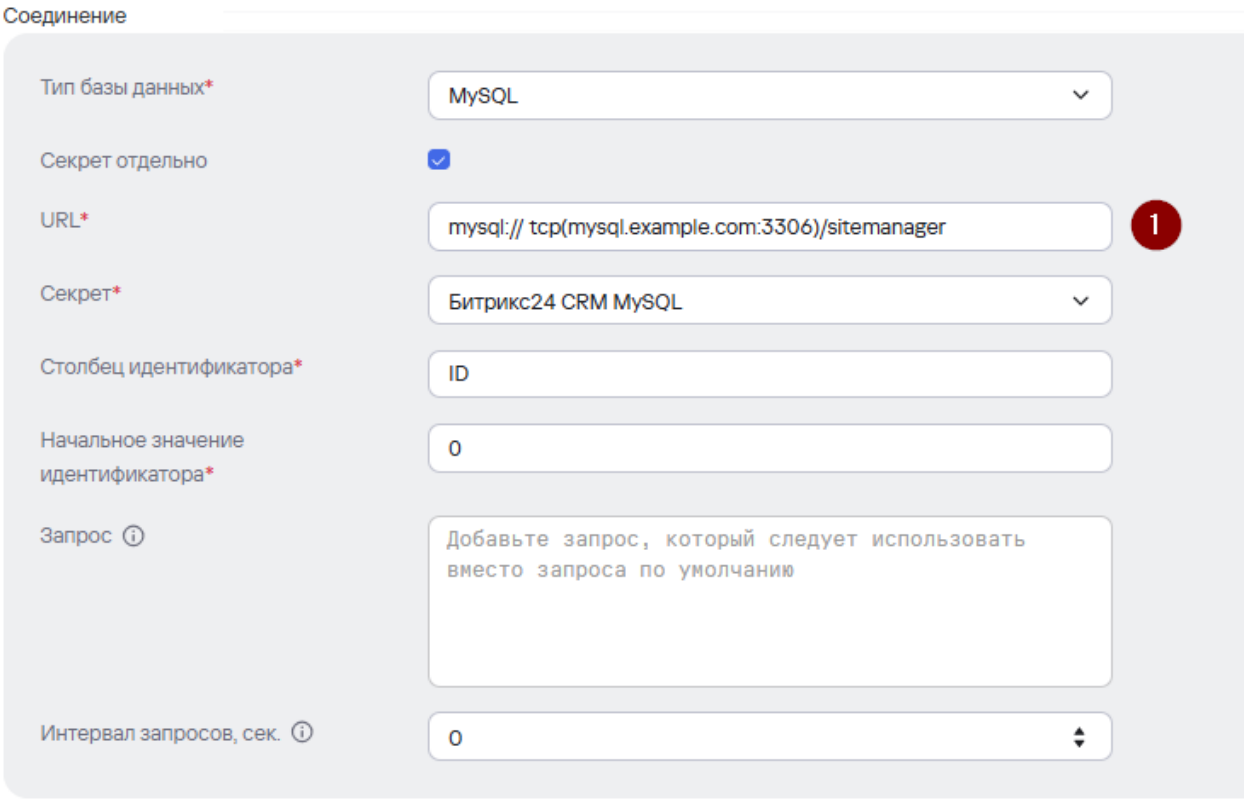
Настройка секрета

- В веб-интерфейсе KUMA внесите изменения в ресурс Секрета **Битрикс24 CRM MySQL,** импортированный на предыдущем шаге, указав актуальные учетные данные для подключения к БД MySQL:
  - Перейдите в **Ресурсы** > **Секреты**.
  - Выберите секрет **Битрикс24 CRM MySQL** и укажите **Пользователя** и **Пароль.**



Настройка коннектора

- В веб-интерфейсе KUMA внесите изменения в ресурс Коннектора **Битрикс24 CRM MySQL,** импортированный на предыдущем шаге, указав актуальный URL-адрес сервера MySQL:
  - Перейдите в раздел **Ресурсы** > **Коннекторы.**
  - Выберите коннектор **Битрикс24 CRM MySQL** и укажите актуальный URL-адрес сервера MySQL.



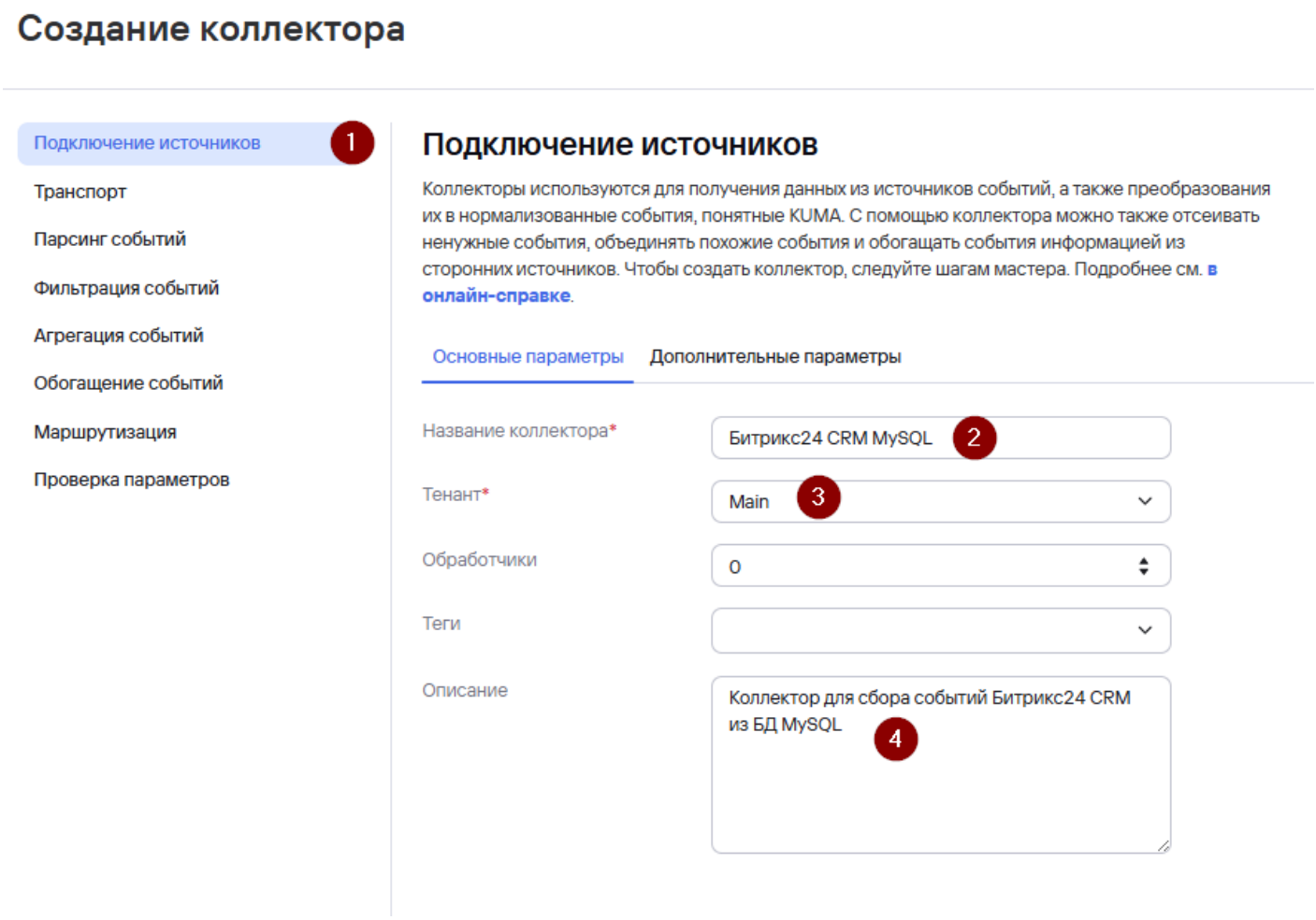
> В поле URL можно указать FQDN или IP-адрес сервера MySQL:
> mysql://user:password@tcp(mysql.example.com:3306)/sitemanager
> mysql://user:password@tcp(10.10.10.11:3306)/sitemanager

> В качестве идентификатора используется столбец ID. При необходимости Вы можете использовать столбец TIMESTAMP_X (если требуется собирать события, начиная с определенной даты) . Для этого измените значение в параметре **Столбец идентификатора** и внесите изменения в применяемый SQL-запрос.

Создание коллектора

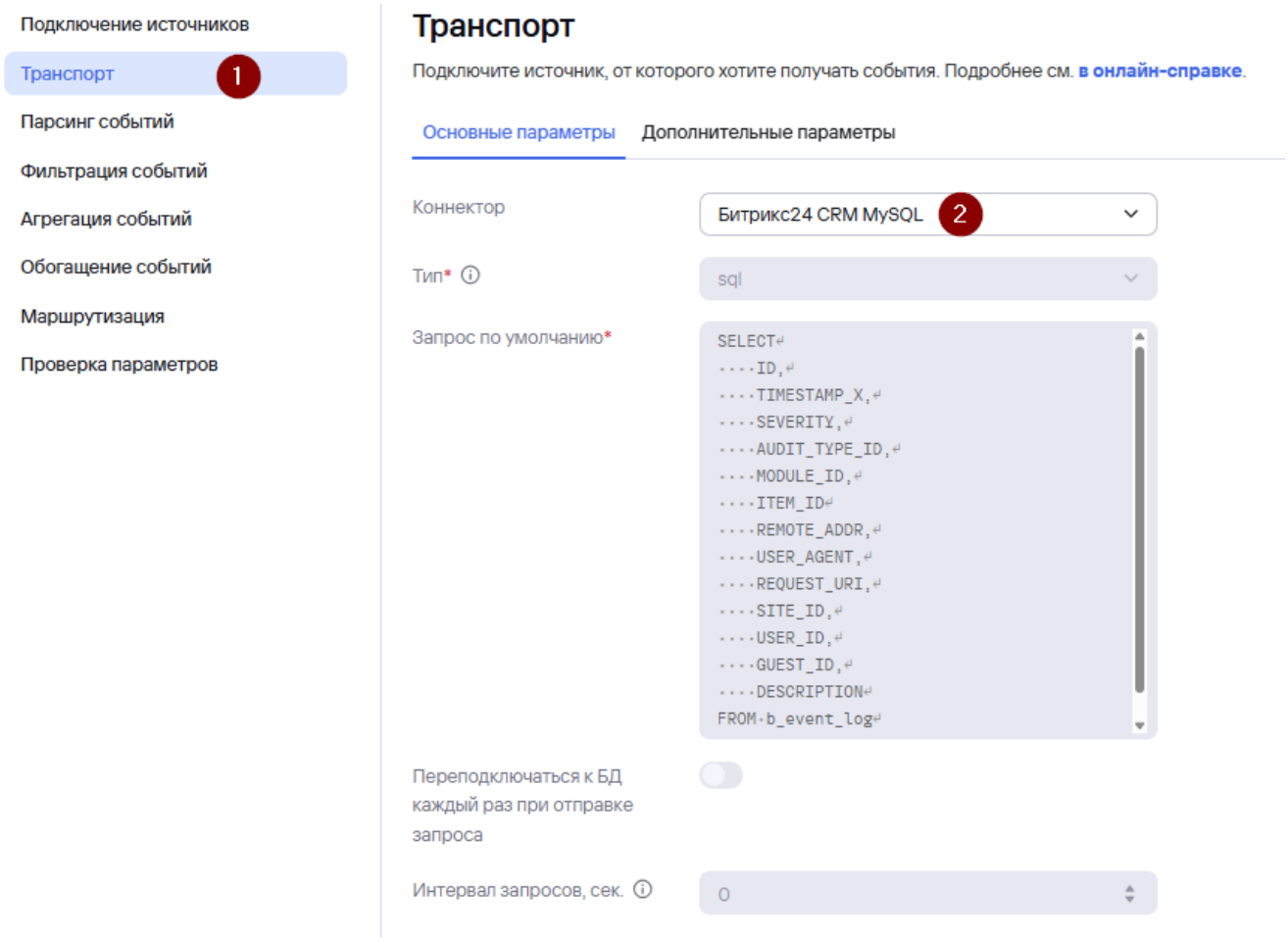
Для сбора событий Битрикс24 CRM необходимо создать сервис коллектора в KUMA. Для этого в веб-интерфейсе KUMA перейдите в раздел **Ресурсы** и нажмите на кнопку **Подключить источник.** В появившемся окне мастера настройки **Создание коллектора:**

- На первом шаге (**Подключение источников**) выберите **Имя коллектора** и **Тенант**, к которому будет относиться создаваемый коллектор.



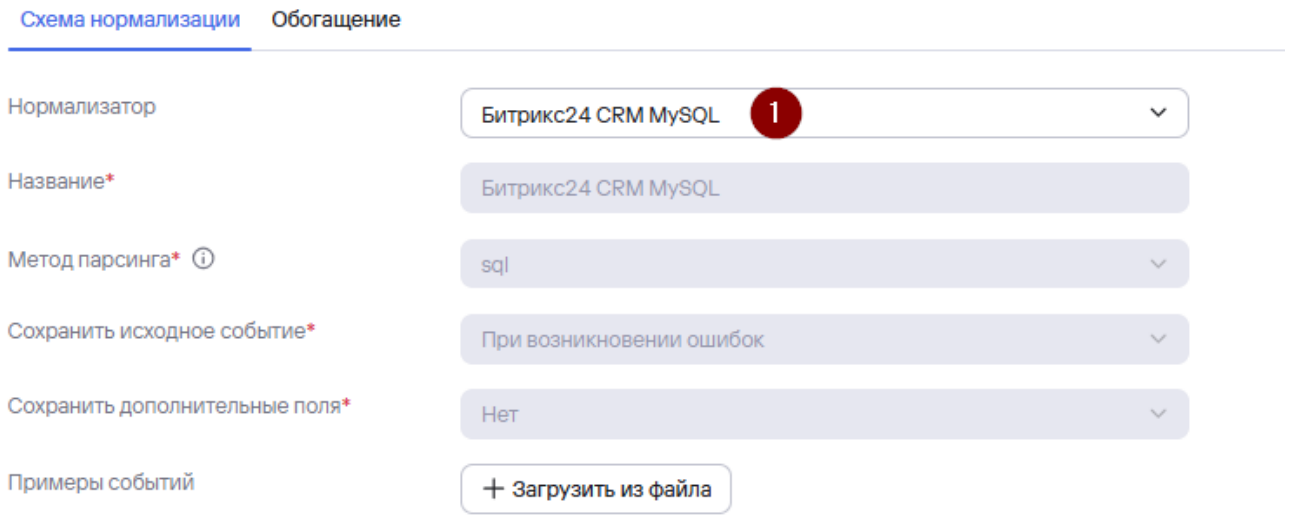
- На втором шаге мастера (**Транспорт**) укажите ранее созданный коннектор для подключения к БД MySQL.

Создание коллектора



- На третьем шаге мастера укажите импортированный ранее нормализатор **Битрикс24 CRM MySQL.**

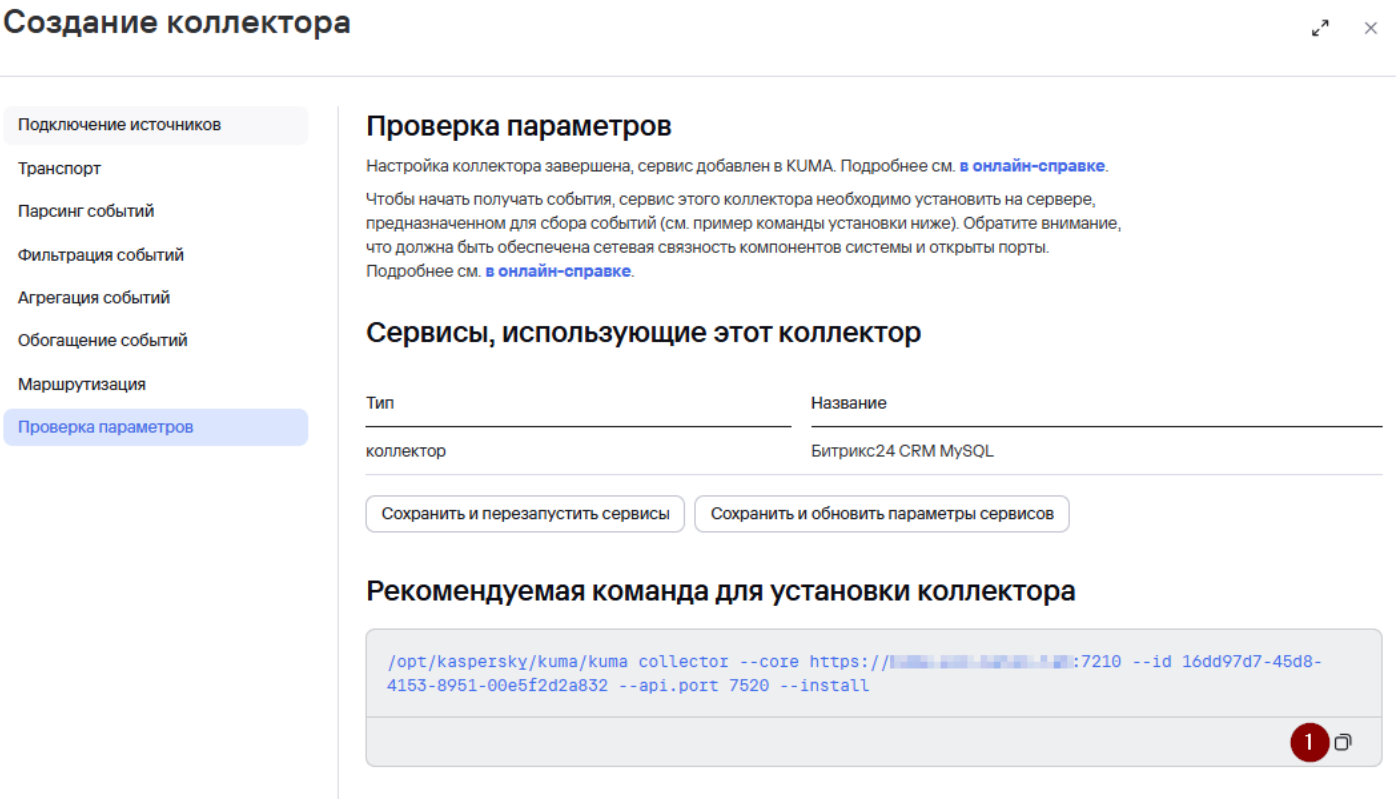
Основной парсинг событий



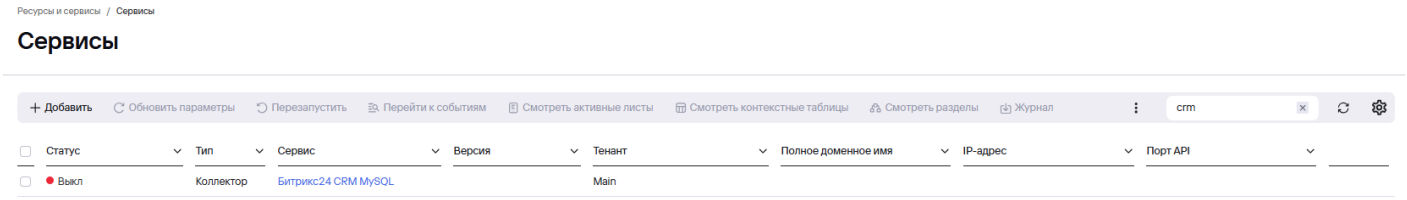
- Шаги мастера настройки с четвертого по шестой (**Фильтрация событий**, **Агрегация событий** и **Обогащение событий**) можно пропустить и вернуться к их настройке позднее.
- На седьмом шаге **Маршрутизация** задайте точки назначения. Для хранения событий добавьте точку назначения типа **Хранилище (Storage)**. В случае если предполагается также анализ потока событий правилами корреляции добавьте точку назначения типа **Коррелятор (Correlator)**.

Создание коллектора

- На завершающем шаге мастера **Проверка параметров** нажмите на кнопку **Сохранить и создать сервис**. После чего появится команда установки сервиса, которую необходимо скопировать для дальнейшей установки.



- Нажмите **Сохранить**.
- После выполнения вышеуказанных действий в разделе **Ресурсы** > **Активные сервисы** появится созданный сервис коллектора.



Установка коллектора KUMA

- Выполните подключение к CLI сервера KUMA (коллектора KUMA при распределенной инсталляции).
- Для установки сервиса коллектора в командной строке выполните команду под учетной записью root, скопированную на прошлом шаге.
- После успешной установки сервиса его статус в веб-интерфейсе KUMA изменится на **Вкл** с **зеленой индикацией**.

Проверка поступления событий

- Для проверки, что сбор событий Битрикс24 CRM из БД MySQL успешно настроен перейдите в **Ресурсы** > **Активные сервисы** > выберите ранее созданный коллектор Битрикс24 CRM MySQL > нажмите ПКМ > **Перейти к событиям.**
- В открывшемся окне **События** убедитесь, что присутствуют события Битрикс24 CRM .

ALD Pro отправка логов

Ссылка на документацию вендора: https://wiki.astralinux.ru/kb/nastrojka-syslog-ng-dlya-peredachi-logov-v-siem-sistemu-348162837.html

Файл pdf: Настройка_syslog_ng_для_передачи_логов_в_SIEM_систему_v1_20250218.pdf