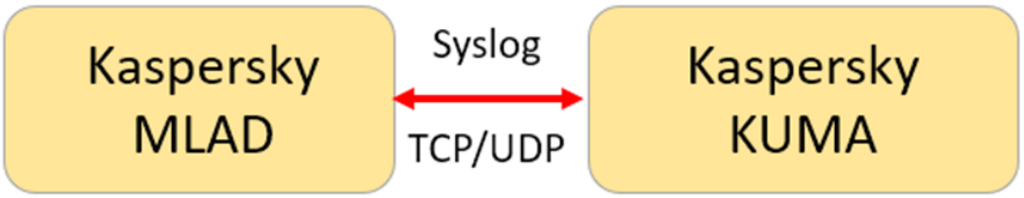
# ?????????? Kaspersky MLAD ? KUMA ?? Syslog

## 1. ???????? ??????

?????? ???????? ????????? ??????? ????????? Kaspersky MLAD ??? ?????????? ? KUMA ?? ????????? Syslog.

???? ?????? ?????????? – ?????????? ???????? ??????? ???????????? ?? Kaspersky MLAD ? SIEM ??????? ??? ?????????? ??? ????????????? ???????????? ? ????????????? ???????.

???? ????????? ?????????? ????? ??????????, ???????????? ? ?????????? ? ?????? ????????? ??????????.

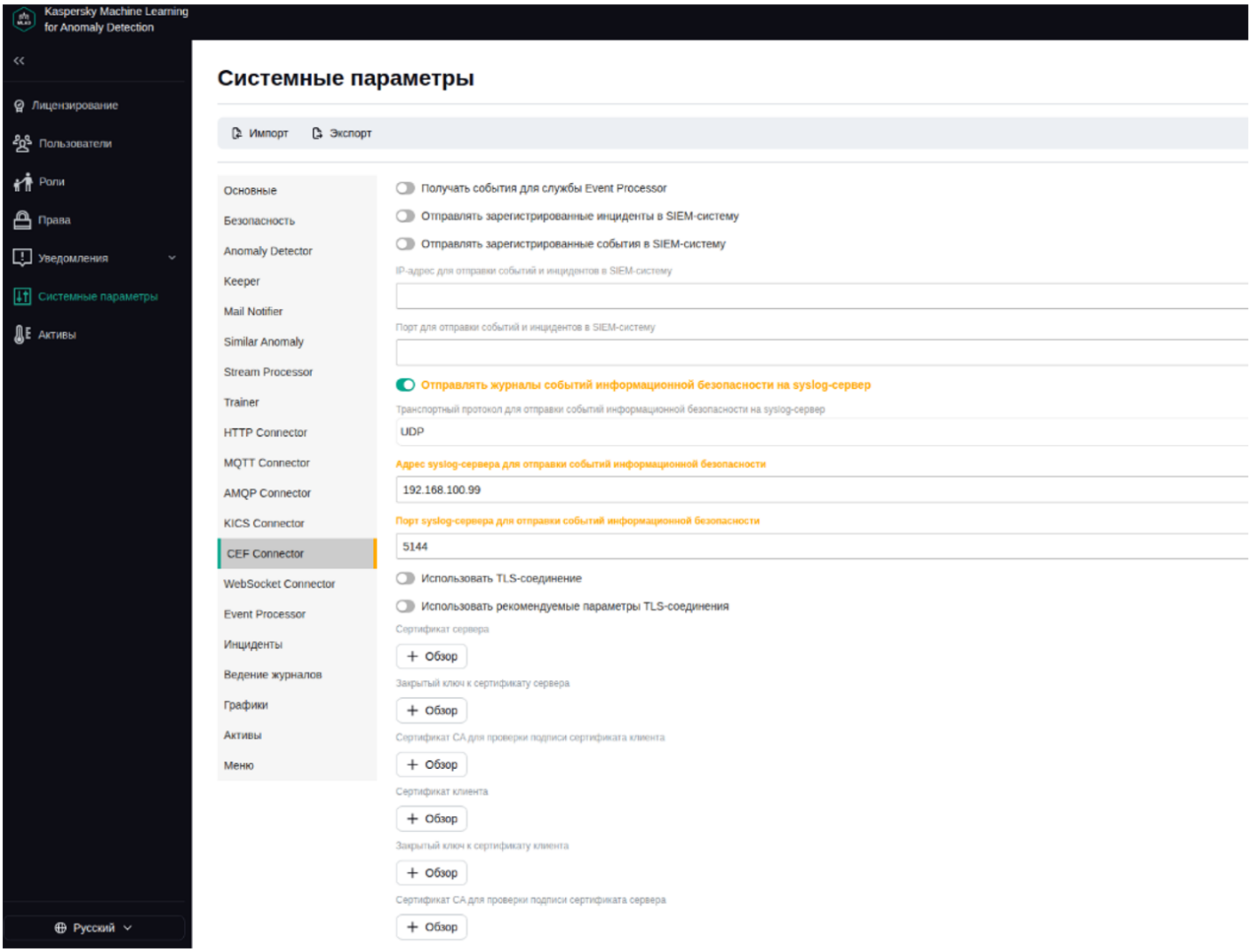



## 2. ?????????? ??????

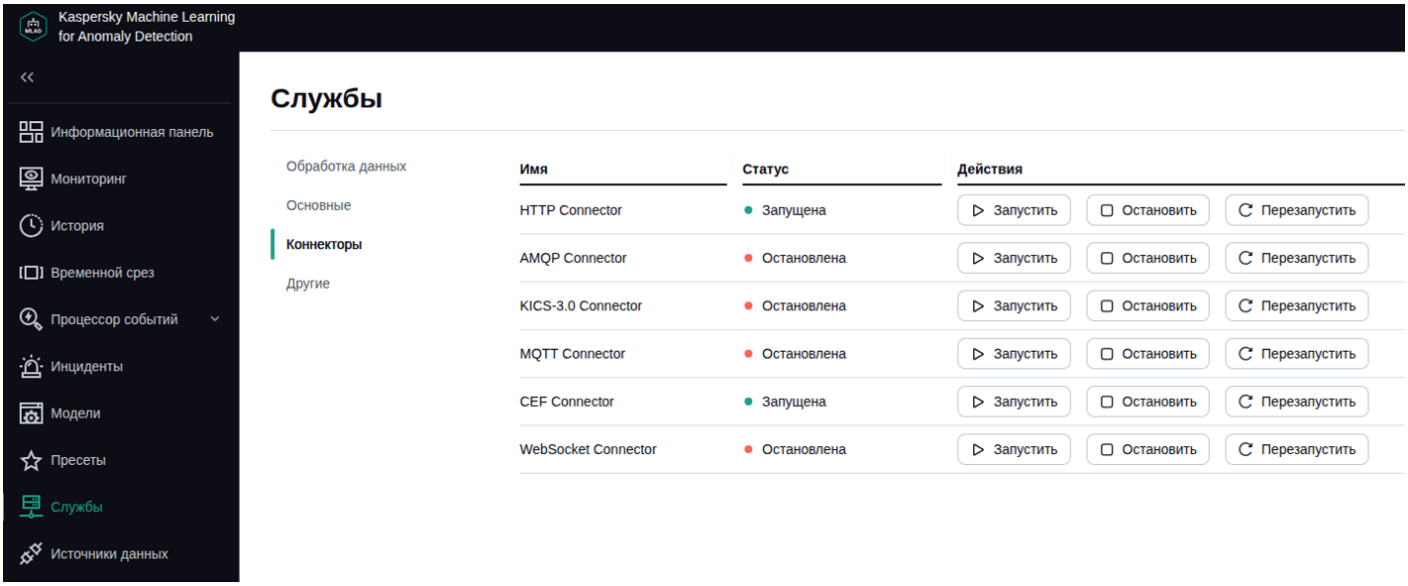
?????? ????? ?????????? ????????? CEF-????????? ? ??????? Kaspersky MLAD ?? ???????? ??????? ???????????? ? SIEM-???????.

??? ????? ????????? ? **???? ?????????????**, ????? ? **????????? ?????????**, ????? ? ????????? **CEF-??????????**.

????? ??? ?????????? ???????????? ????????????? **?????????? ??????? ??????? ????????????? ???????????? ?? Syslog-??????**, ??????? ??? ?????????? (TCP ??? UDP), ??????? ????? ? ???? Syslog -???????. ???? ?? ?????????? ???????????? ?????????? TLS-??????????, ?? ??? ?????????? ????? ????????? ??????????/???????? ???? ??????? ? CA-?????????? ??? ?????????? ????????? ???????.

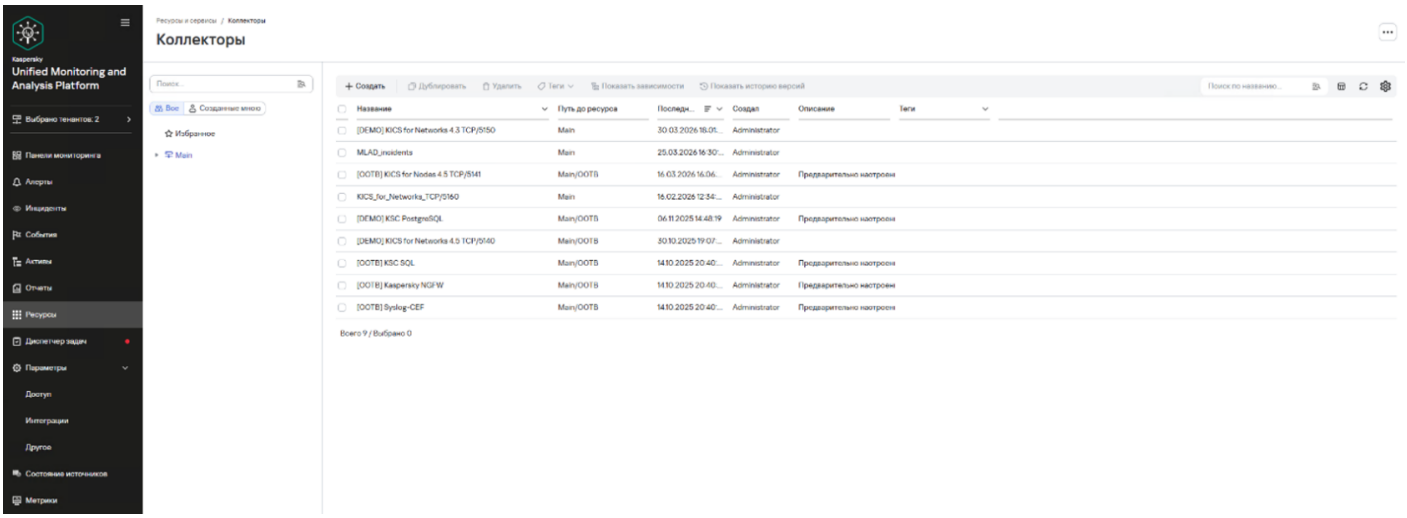



????? ????? ????????? ? ???????? ????, ????? ? ??????, ????? ? ?????? **??????????**. ????????? ?????? **CEF connector**, ??? ????????????? ??, ???? ?? ??????? ????????? ? ?????????.

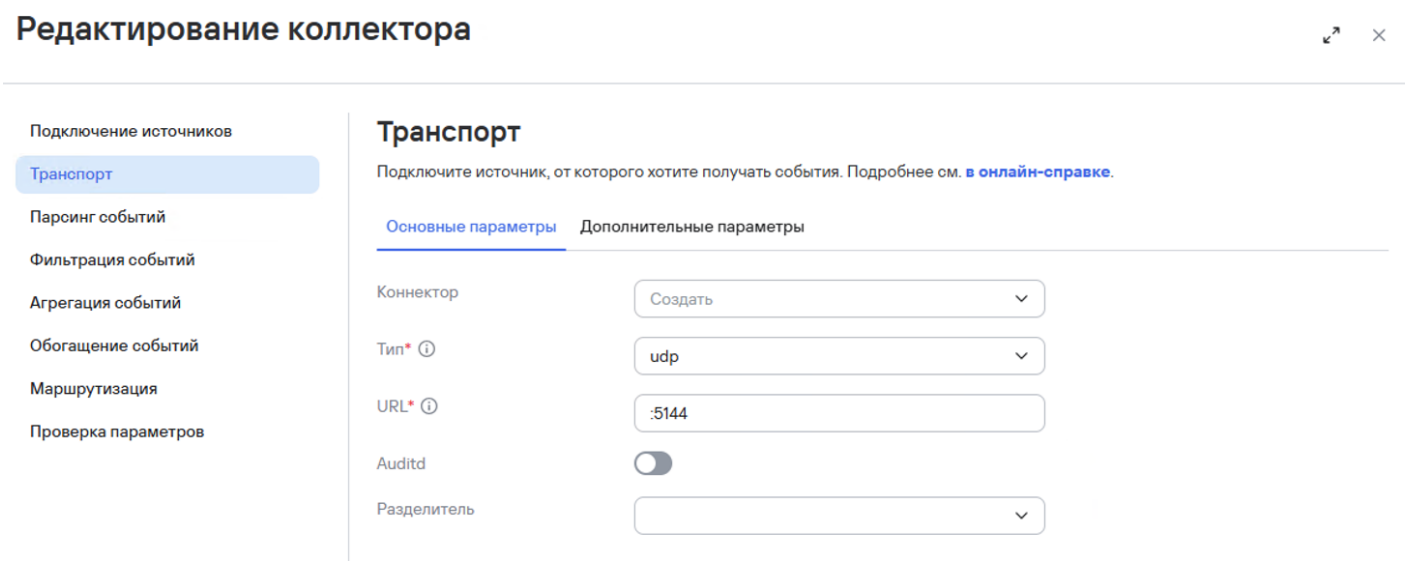



?? ???? ????????? ?? ??????? MLAD ?????????.

? KUMA ????????? ? ?????? **???????**, ????? **??????????**.



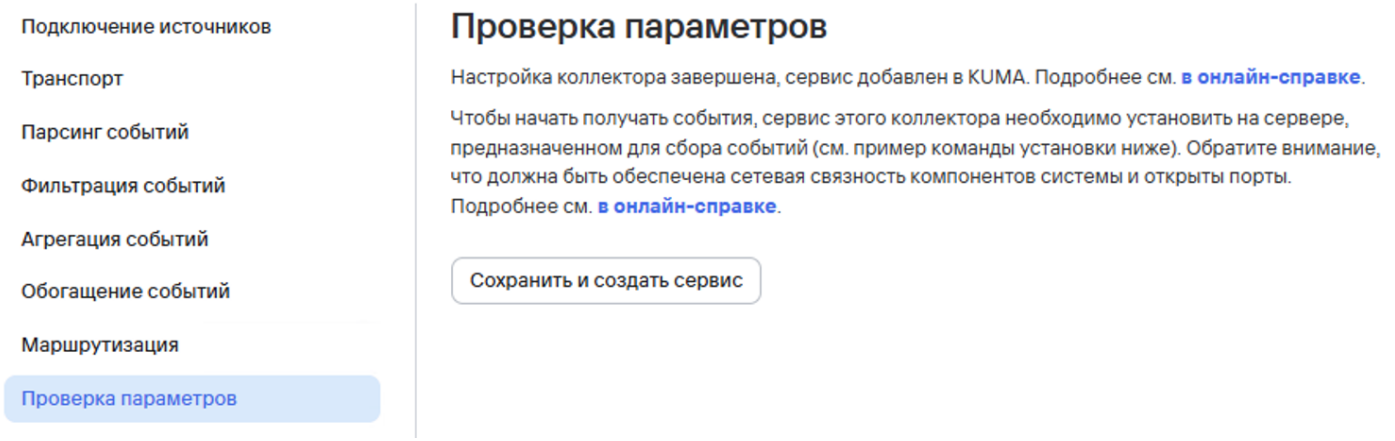

? ?????? ???????? KUMA ?????? ?????????????? ??????????? ????????? **[OOTB] Syslog CEF**. ???????? ????? ?? ?????? ??????? ?????????? ? ????????? ? ??? ?????????. ???????? ????????? ??????????? ???????? ?? ??????? **?????????**.



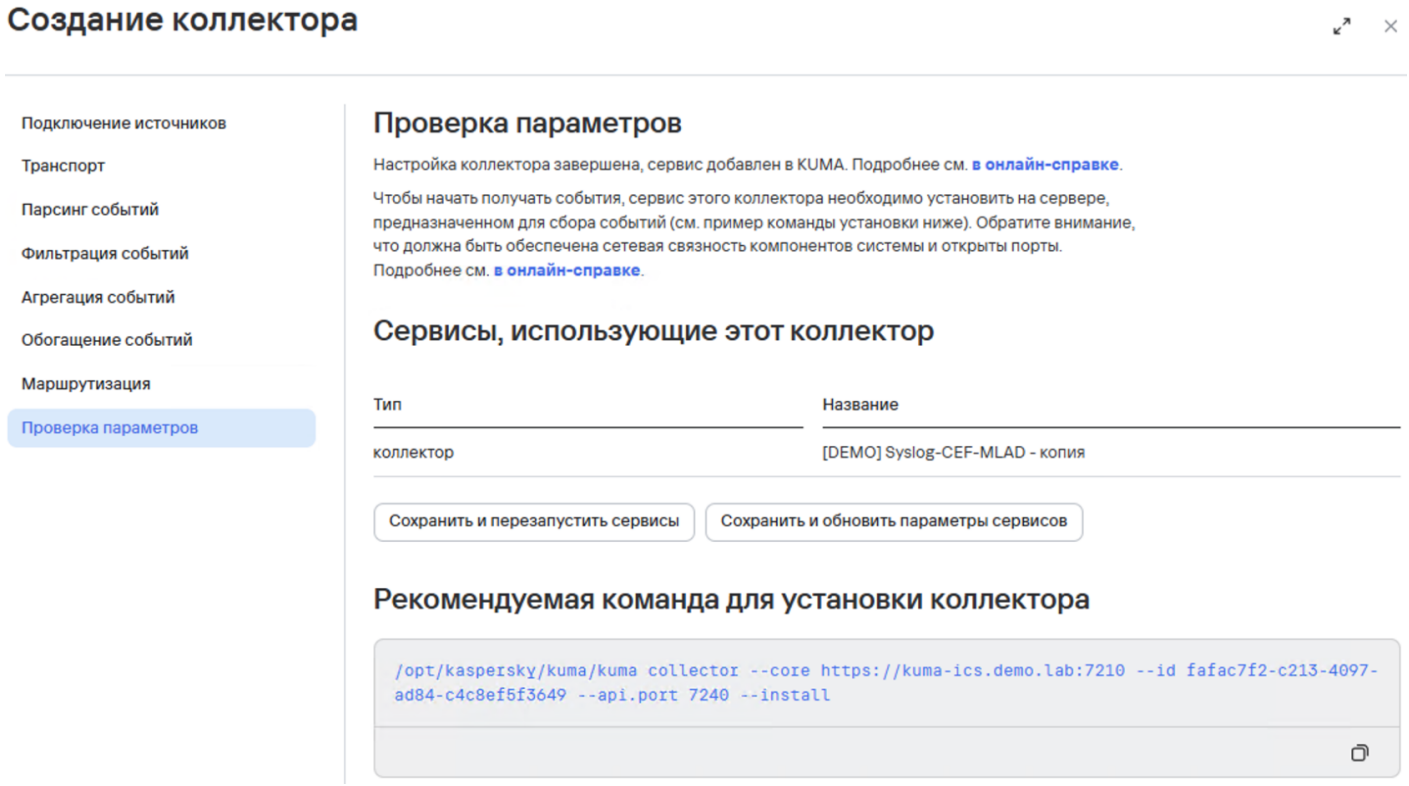

??????? ??? ?????????, ????????? ? ????, ?? ??????? KUMA ????? ????????? ??????????? ?? Syslog. ?????????, ??? ????????? ??????????? ? MLAD ????????? ? ??????????? ? ?????? ???????.

????????? ????????? ??????? ?? ?????? ?? ????? ????????? Syslog. ?? ??????? **??????? ???????** ?? ?????? ?????????, ??? ????? ????????? ??????? Syslog, ?????????? ?? MLAD. ??? ????? ??? ????????????? ?????????? ??????? ???????????????? ??????. ??????? ???????? ? ????????? ??????? ?????? ? ???????????? ?? KUMA, ? ? ?????? ????????? ?? ????????????,

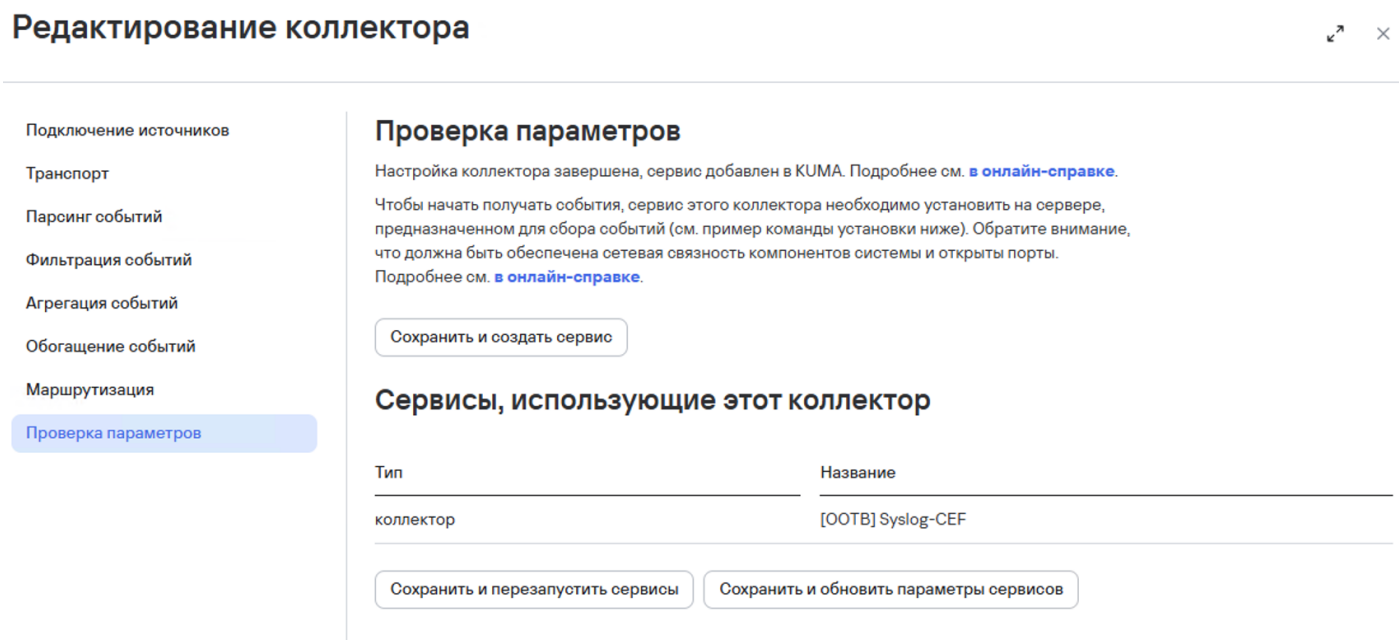
????? ?????????? ????????? ??? ??????? ????? ?????????? ????? ??????? ???????????????? ??????.


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.
Сохранить и создать сервис

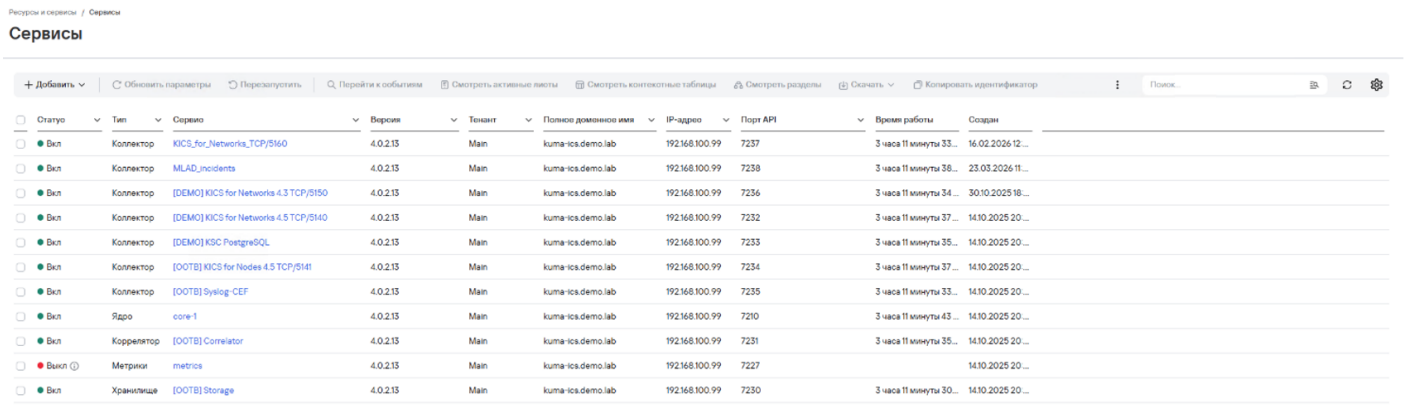
??? ????? ?????????? ????????? ???????????? ??????? (????? sudo) ?? ?????? ? KUMA.


Создание 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
[DEMO] Syslog-CEF-MLAD - копия
Сохранить и перезапустить сервисы
Сохранить и обновить параметры сервисов
Рекомендуемая команда для установки коллектора
/opt/kaspersky/kuma/kuma collector --core https://kuma-ics.demo.lab:7210 --id fafac7f2-c213-4097-ad84-c4c8ef5f3649 --api.port 7240 --install

???? ?????? ??? ??????????, ?? ????? ?????????? ????????? ????????? ?? ???????
**???????? ??????????** ? ??????? ?????? **????????? ? ???????????? ???????**.

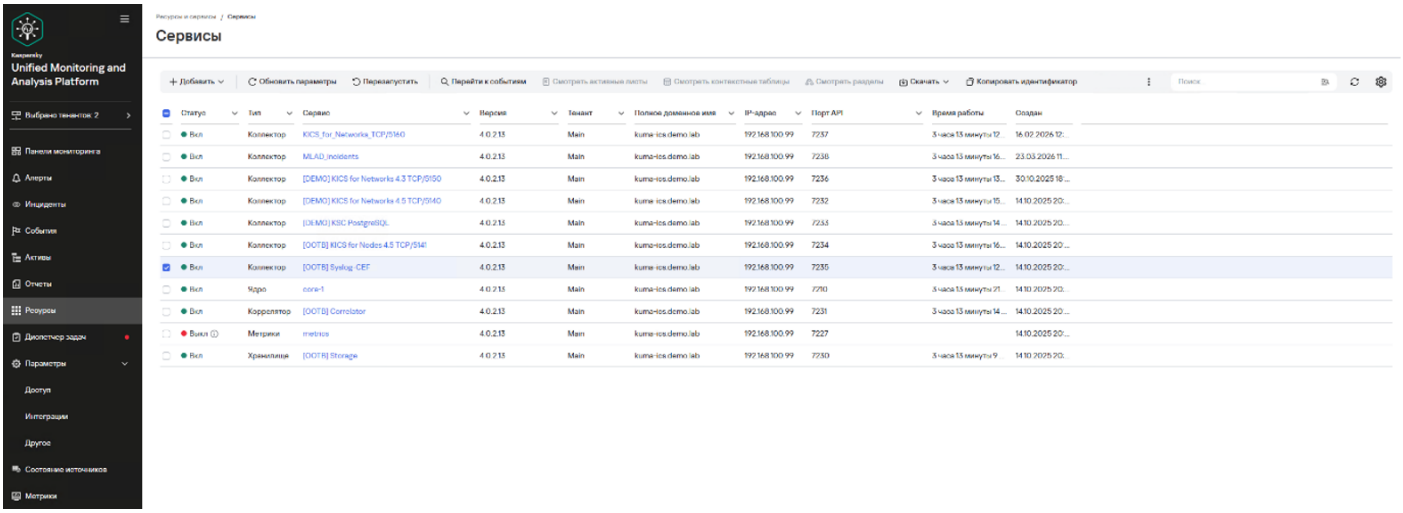



????????? ? ?????? **???????? ???????** ? ?????????, ??? ??? ?????? ?????????? Syslog ???????.

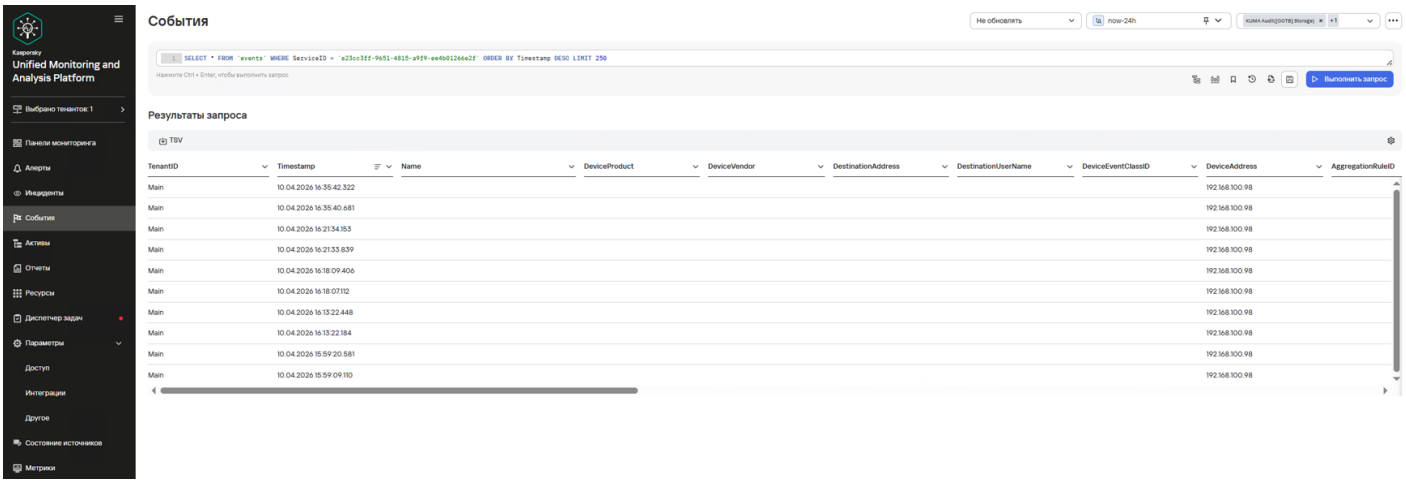



????????? ? MLAD ? ??????????? ?????-?????? ????????? ????????, ????????, ??????? ? ????? ??????? ? ???????.

????? ???????? ???? ???????? ?????? ? KUMA ? ??????? ?????? **??????? ? ????????.**




C???????? ????????? SQL-??????. ?? ??????? ? ?????? ??????? ???????????? ?? MLAD.




---

Revision #2
Created 10 April 2026 13:57:30 by Эльдар Юсуфов
Updated 10 April 2026 14:08:16 by Эльдар Юсуфов