

Zecurion DLP

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

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

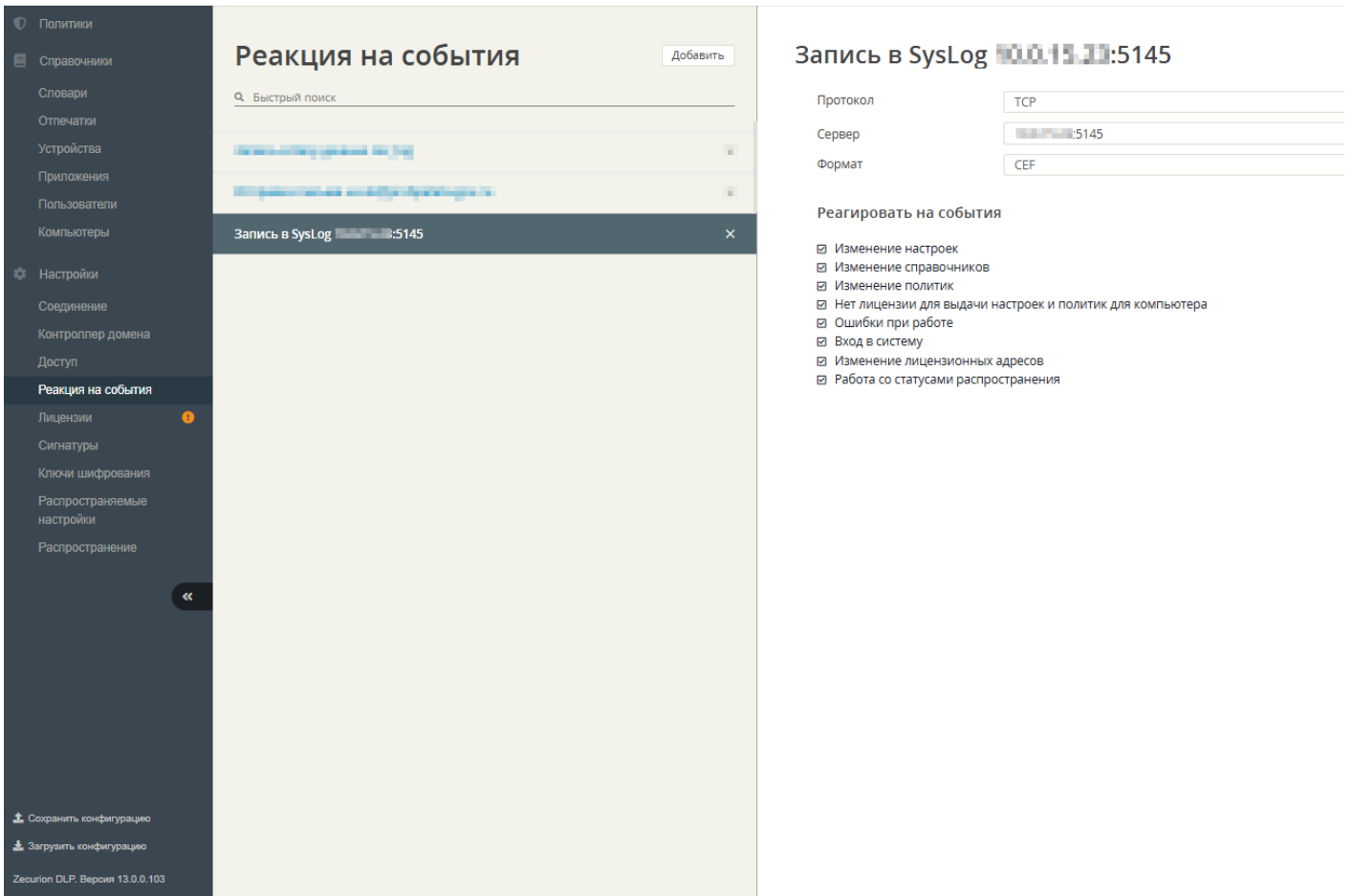
Настройка коллектора KUMA для приема и обработки событий **Zecurion DLP** приведена в отдельной [общей статье](#) по созданию сервиса коллектора.

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

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



????????? ?????????????????? ?????????? Zecurion DLP ? 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.**



Kaspersky

Unified Monitoring and Analysis Platform

- Выбрано tenants: 2
- Панели мониторинга
- Алерты
- Инциденты
- События 1**
- Активы
- Отчеты
- Ресурсы
- Оубег Trace
- Диспетчер задач
- Параметры
- Доступ

События

Не обновлять | 5m | now-5m | KUMAAudit([OOTB] Storage) +12

```

1 SELECT * FROM `events` WHERE ServiceID = '2b7f1ae8-177a-4142-8dc3-1e2eabfcec0a' ORDER BY Timestamp DESC LIMIT 250
  
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

Результаты запроса

TSV

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

Revision #2

Created 2026-07-01 20:06:43 UTC by Dmitry Borisov

Updated 2026-07-01 20:49:57 UTC by Dmitry Borisov