

KICS for Linux Nodes 2.0

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

Сбор событий **KICS for Linux Nodes** возможен двумя способами:

- Из БД KSC, если KICS for Linux Nodes управляется централизованно средствами KSC.
- Напрямую средствами самого KICS for Linux Nodes, в случае, когда KSC не используется в инфраструктуре и KICS for Linux Nodes работает в автономном режиме.

Для сбора событий KICS for Linux Nodes из БД PostgreSQL KSC воспользуйтесь следующей [статьей](#).

Настройка коллектора KUMA

Настройка коллектора KUMA для приема и обработки событий **KICS for Linux Nodes** приведена в отдельной [общей статье](#) по созданию сервиса коллектора.

На шаге **Парсинг событий** в качестве нормализатора для событий **KICS for Linux Nodes** выберите нормализатор **[20-07-2026] Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 Syslog-CEF**. Нормализатор доступен в рамках Community Pack.

Настройка KICS for Linux Nodes

По умолчанию KICS for Linux Nodes журналирует события во внутреннюю БД, однако для централизованного хранения и обработки можно настроить отправку событий в SIEM-систему. Для отправки событий может использоваться протокол TCP или UDP.

Чтобы настроить отправку событий **KICS for Linux Nodes** в коллектор KUMA, запустите скрипт **tune_syslog_for_siem.sh** (см. [Приложение 5. Настройка совместной работы с SIEM-системами](#) онлайн-справки KICS for Linux Nodes).

Скрипт **tune_syslog_for_siem.sh** предоставляется по запросу.

```
root@astra-63046:/opt# ./tune_syslog_for_siem.sh udp 192.168.100.99 5170
Found syslog syslog-ng
Tuning syslog-ng
Creating config /etc/syslog-ng/conf.d/siem_exporter.conf
Restarting syslog server
Product already configured
All done.
root@astra-63046:/opt#
```

Проверка поступления событий KICS for Linux Nodes в KUMA

Чтобы убедиться, что сбор событий **KICS for Linux Nodes** успешно настроен, перейдите в **Ресурсы > Активные сервисы > выберите ранее созданный коллектор для KICS for Linux Nodes > ПКМ > Перейти к событиям**.

В открывшемся окне **События** убедитесь, что присутствуют события **KICS for Linux Nodes**.

**Kaspersky**
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 2

Пакеты мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

События

Не обновлять | 5m | now-5m | KUMA-Audit[0078] Storage | 1

1

SELECT * FROM 'events' WHERE ServiceID = '2a766435-7b5b-4726-9a94-b57a8b48d8c' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

Результаты запроса

TSV

TenantID	Timestamp	DeviceVendor	DeviceCustomString2	DeviceHostName	Name	DeviceCustomString1	FlexString1
Main	16.07.2026 18:29:36.828	Kaspersky	KICS	astra-63046	Web_Threat_Protection	ECAR-Test-File	File
Main	16.07.2026 18:29:36.828	Kaspersky	KICS	astra-63046	File_Threat_Protection	ECAR-Test-File	File

Revision #6

Created 2026-07-16 11:55:44 UTC by Dmitry Borisov

Updated 2026-07-20 12:11:04 UTC by Dmitry Borisov