KICS for Linux Nodes 2.0

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **HE** ???????? ??????????? ????????????? ???????.

???? ??????? **KICS for Linux Nodes** ???????? ????? ?????????:

- ?? ?? KSC, ???? KICS for Linux Nodes ??????????? ?????????????? ?????????? KSC.
- ???????? ?????????? ?????? KICS for Linux Nodes, ? ??????, ????? KSC ?? ???????????? ? ????????????? ? KICS for Linux Nodes ???????? ? ?????????? ??????.

??? ????? ??????? KICS for Linux Nodes ?? ?? PostgreSQL KSC ????????????? ????????? ???????.

Настройка коллектора KUMA

????????? ?????????? KUMA ??? ?????? ? ????????? ??????? **KICS for Linux Nodes** ????????? ? ????????? ????? ?????? ?? ???????? ??????? ??????????.

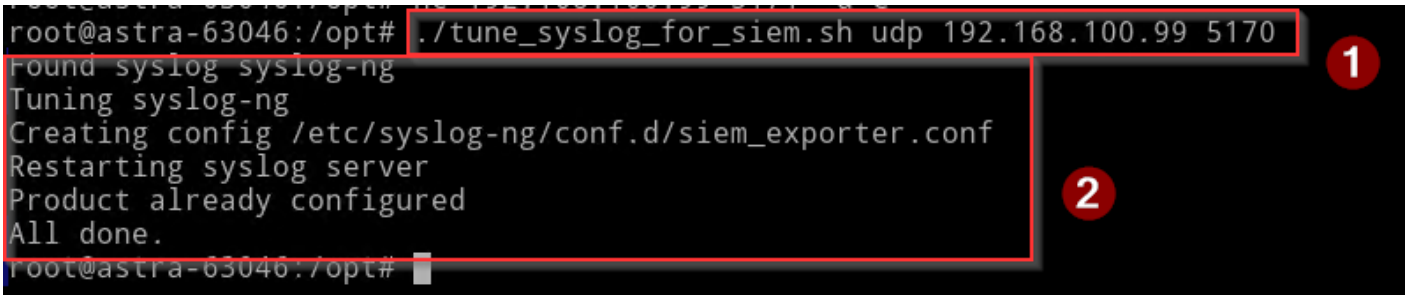
?? ???? **Парсинг событий** ? ???????? ????????????? ??? ??????? **KICS for Linux Nodes** ???????? ???????????? **[20-07-2026] Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 Syslog-CEF**. ???????????? ???????? ? ?????? Community Pack.

Настройка KICS for Linux Nodes

?? ????????? KICS for Linux Nodes ??????????? ??????? ?? ?????????? ??, ?????? ??? ???????????????? ???????? ? ????????? ????? ????????? ???????? ??????? ? SIEM-???????. ??? ???????? ??????? ????? ????????????? ???????? TCP ??? UDP.

????? ????????? ???????? ??????? **KICS for Linux Nodes** ? ????????? KUMA, ????????? ?????? **tune_syslog_for_siem.sh** (??. ?????????? 5. ????????? ?????????? ?????? ? SIEM-????????? ??????-??????? KICS for Linux Nodes).

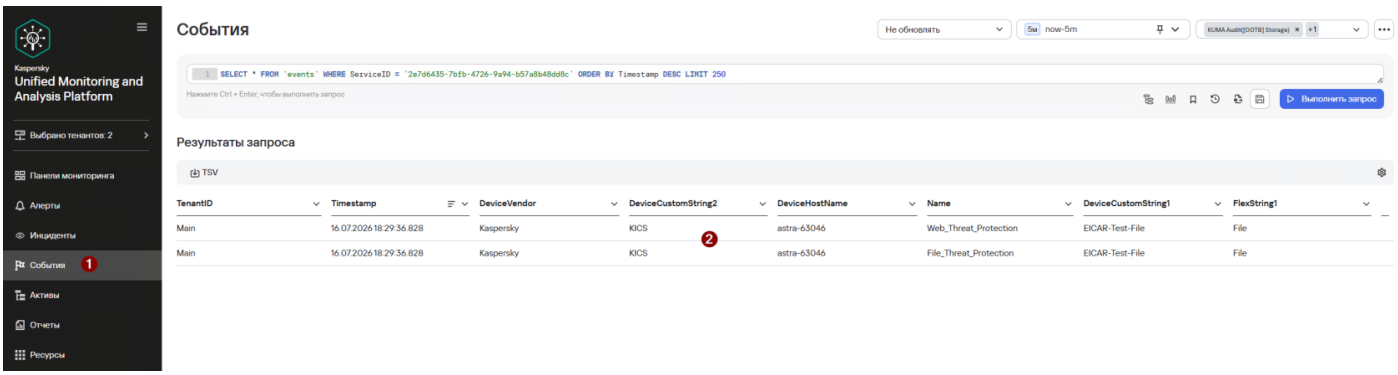
?????? **tune_syslog_for_siem.sh** ????????????? ?? ???????.



Проверка поступления событий KICS for Linux Nodes в KUMA

????? ?????????, ??? ???? ??????? **KICS for Linux Nodes** ??????? ????????, ????????? ? **Ресурсы** > **Активные сервисы** > ???????? ????? ????????? ????????? ??? **KICS for Linux Nodes** > ??? > **Перейти к событиям.**

? ??????????? ???? **События** ?????????, ??? ???????????? ??????? **KICS for Linux Nodes**.



Revision #6
Created 2026-07-16 11:55:44 UTC by Dmitry Borisov
Updated 2026-07-20 12:11:04 UTC by Dmitry Borisov