Выбор варианта сбора событий Windows

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

Сбор событий Windows может выполняться одним из трех способов:

- С помощью агента KUMA (WEC);
- С помощью агента KUMA (WMI);
- С помощью Kaspersky Endpoint Security.

Выбор способа зависит от конкретных условий и требований инфраструктуры, таких как масштаб сети, доступные ресурсы, политики безопасности и уровень экспертизы.

Использование агента KUMA (WEC) рекомендуется в следующих случаях:

- Имеются свободные ресурсы для развертывания WEC-сервера или нескольких WEC-серверов (в зависимости от количества собираемых событий).
- Необходима гибкая настройка собираемых типов событий (Event ID) и возможность их фильтрации.
- Имеется экспертиза в настройке и управлении технологией Windows Event Forwarding (WEF).
- Требуется централизованное управление сбором событий и хранение событий.

Использование агента KUMA (WMI) рекомендуется в следующих случаях:

- Отсутствует возможность использовать технологию WEF для централизованного сбора событий.
- Отсутствуют свободные ресурсы для развертывания WEC-сервера или нескольких WEC-серверов (в зависимости от количества собираемых событий).
- Необходимо выполнить сбор событий с небольшого количества хостов (не более 500 хостов на один агент KUMA).
- Имеется возможность открыть порты (135, 445, 49152-65535) на всех рабочих станциях/серверах, с которых планируется собирать события.

Использование Kaspersky Endpoint Security рекомендуется в следующих случаях:

- Наличие Kaspersky Endpoint Security 12.6 и выше на рабочих станция/серверах (можно использовать комбинированный подход с одним из вариантов выше в случае неполного покрытия инфраструктуры KES'ами).
- Отсутствие возможности выделения ресурсов для развертывания WEC-сервера и агента KUMA.
- Необходима гибкая настройка собираемых типов событий (Event ID) и возможность их фильтрации.
- Требуется централизованное управление сбором событий.

> Каждый из трех вариантов требует настройки политики аудита на рабочих станциях/серверах локально или средствами GPO.

Revision #1
Created 2026-07-14 10:53:48 UTC by Dmitry Borisov
Updated 2026-07-14 11:08:37 UTC by Dmitry Borisov