MS Windows XP & 2003 SNMP

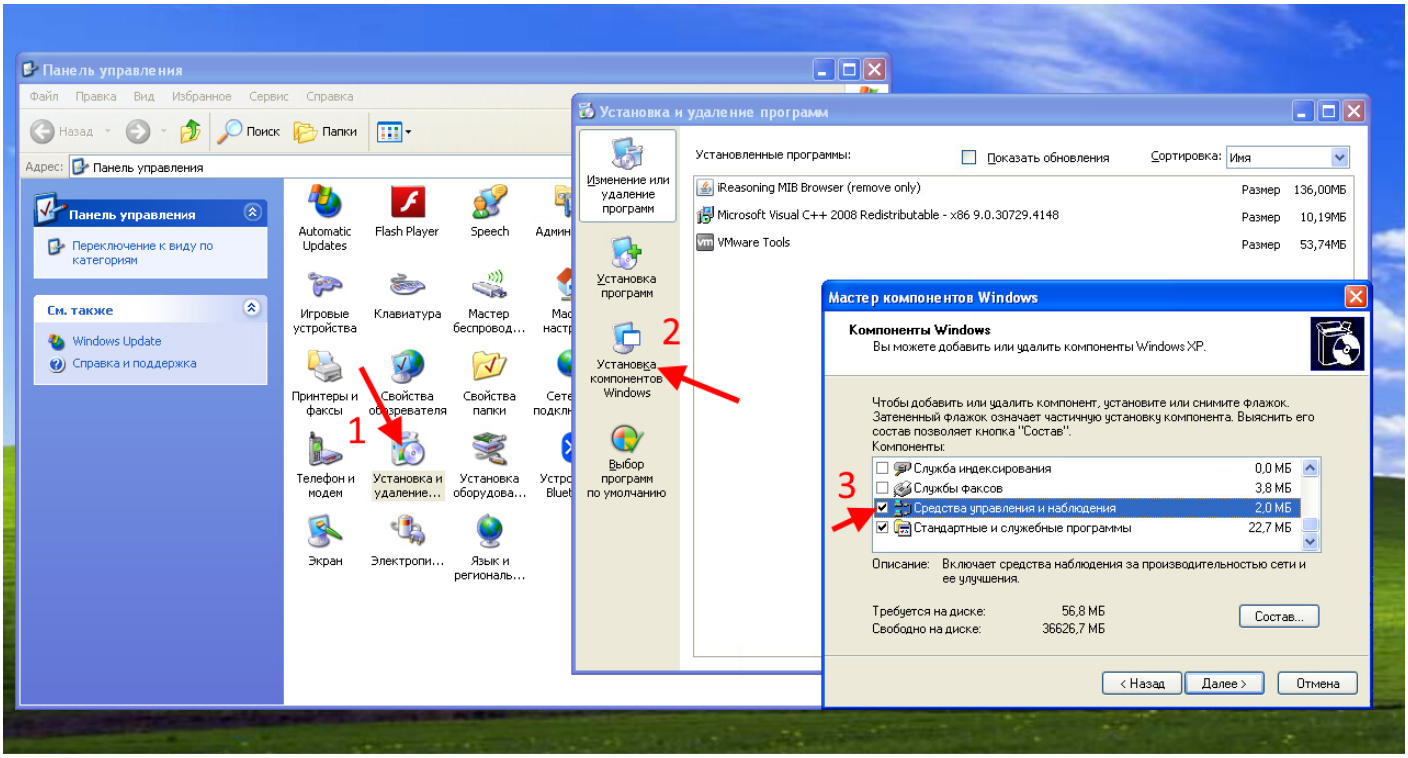
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/help/KUMA/3.0.3/ru-RU/239864.htm

Настройка на стороне Windows.

Настройка сервиса SNMP

В статье рассматривается настройка на ОС Windows XP. Перейдите в **Панель управления - Установка и удаление программ - Установка компонентов Windows.** Установите Средства управления и наблюдения и провайдер WMI SNMP (если есть).

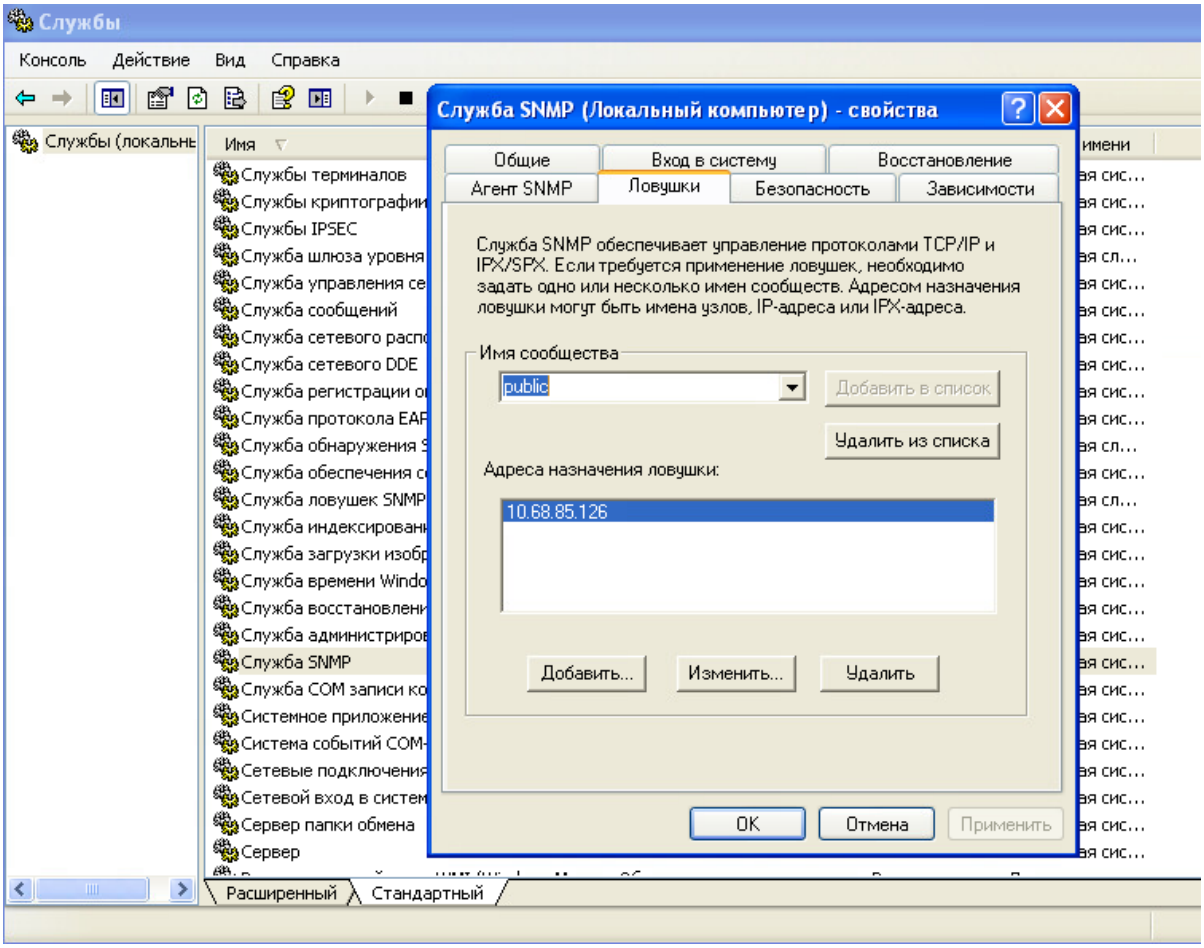


Дождитесь завершения установки и перезагрузите компьютер.

Убедитесь, что службы SNMP запущена (**Панель управления - Администрирование - Службы**): Служба SNMP (SNMP Service) и Служба ловушек SNMP (SNMP Trap). Если какие-то из перечисленных ниже служб не запущены - Запустите

Настройка сервиса SNMP

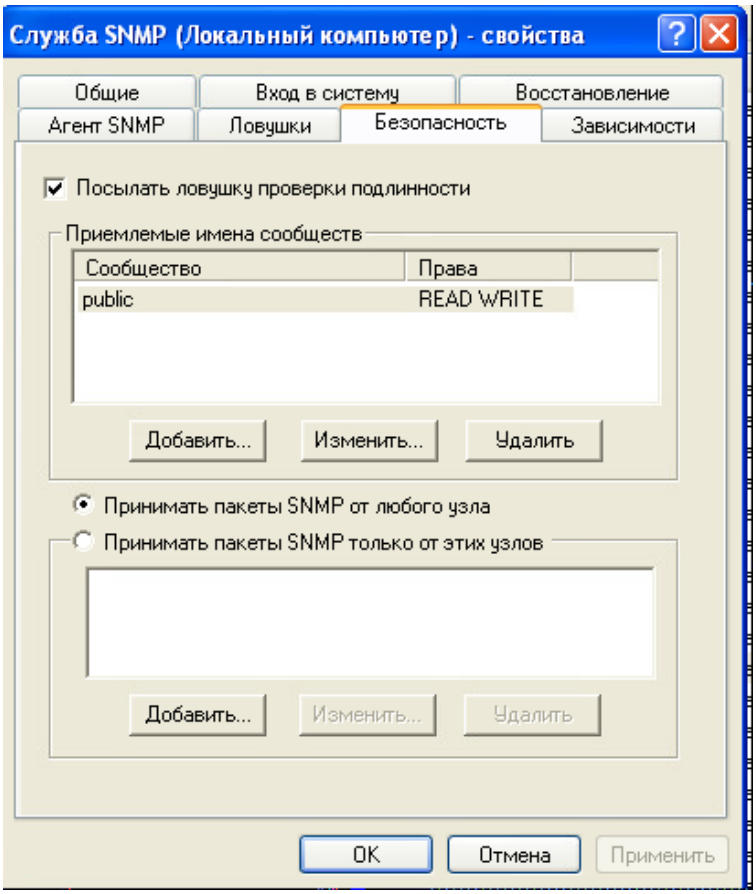
Перейдите в **Панель управления - Администрирование - Службы - Служба SNMP (Свойства) - Вкладка Ловушки**



Добавьте имя сообщества: **public**
Адрес назначения ловушек: **<IP_адрес_коллектора>**

На вкладке Безопасность:

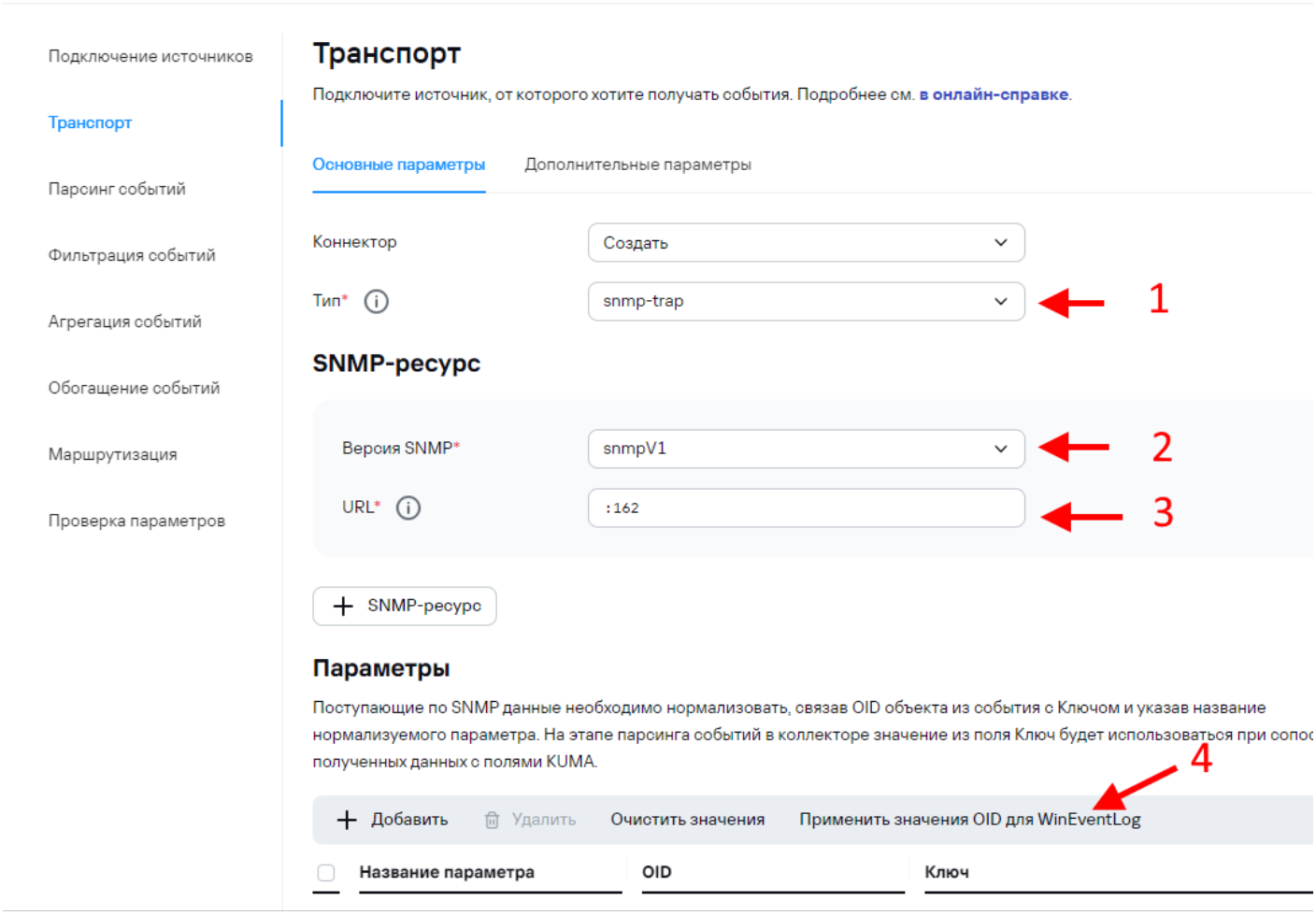
- Установите флажок: Посылать ловушку проверки подлинности (Send authentication trap)
- В таблице Приемлемые имена сообществ (Accepted community names) добавьте сообщество: public, с правами READ WRITE
- Установите флажок: Принимать пакеты SNMP от любого узла (Accept SNMP packets from any hosts)



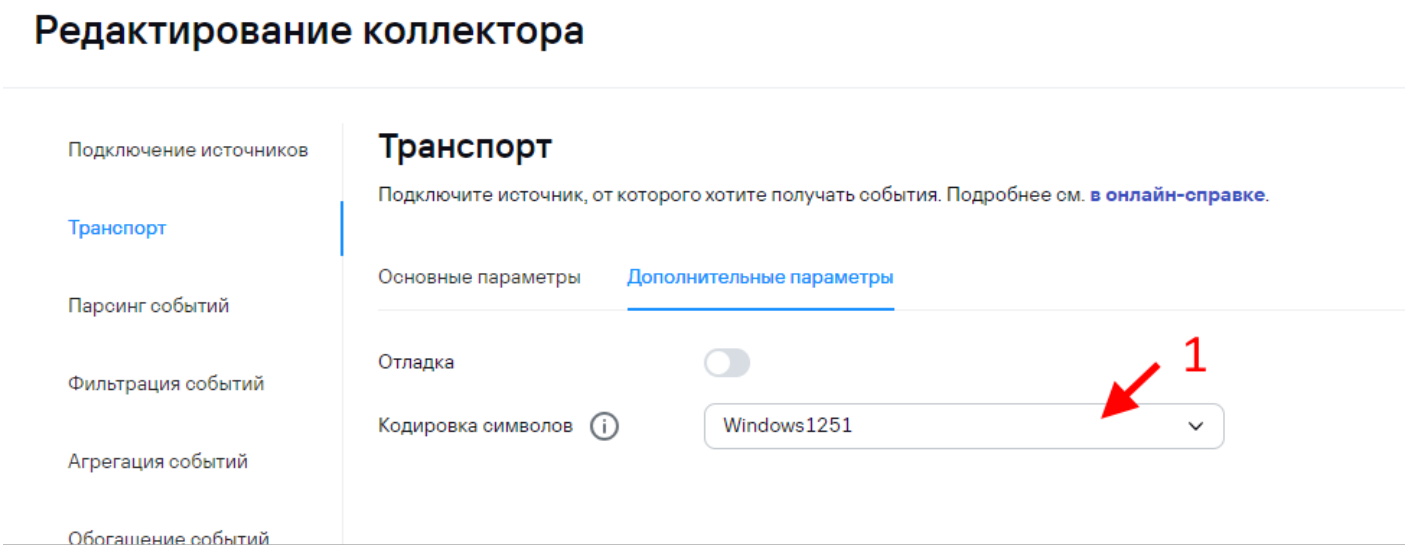
Затем Применить и OK.

Настройки на стороне KUMA

Создайте коллектор со следующим транспортом:

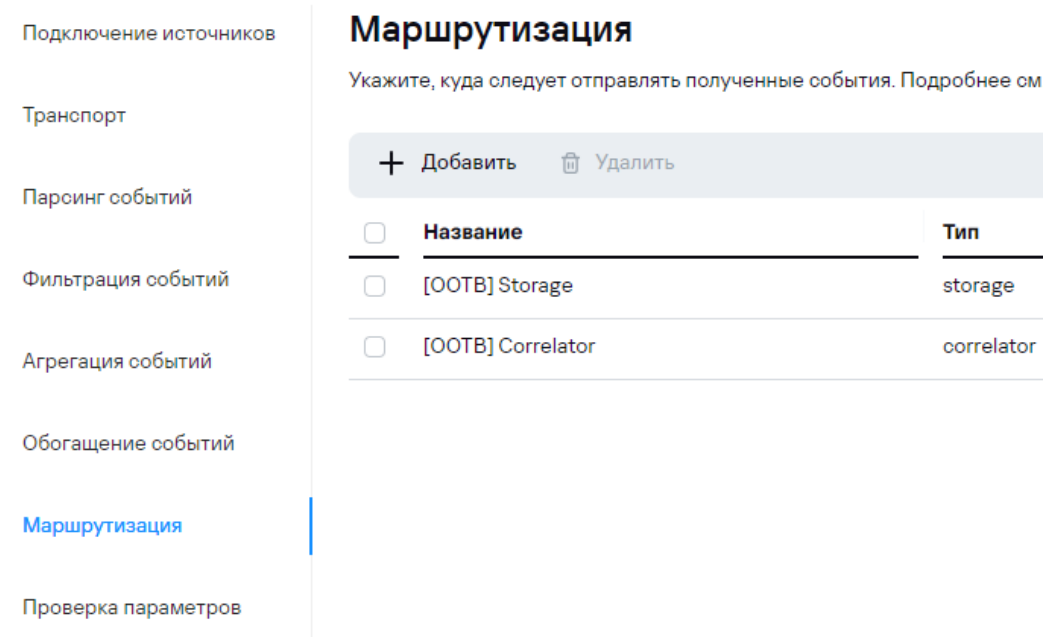


В дополнительных параметрах в случае Русской локали в ОС кажите явно кодировку:



> В качестве парсера рекомендуем использовать комьюнити нормализатор (предварительно импортируйте его в KUMA, пароль импорта: `q123123Q!`): **ссылка**

Задайте маршрут куда отправлять обработанные события коллектором:

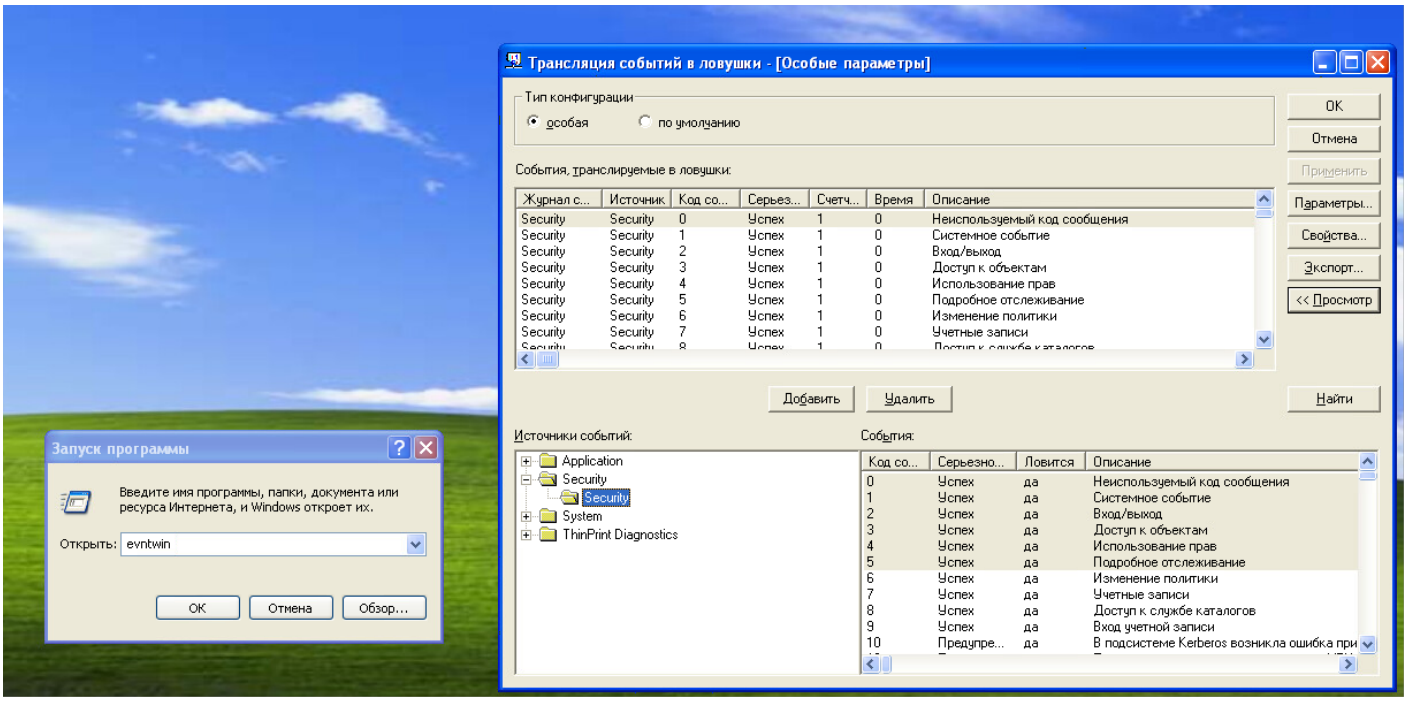


Нажмите сохранить и создать сервис, скопируйте строку установки и выполните ее в консоли SSH.

> SNMP использует порт **161 UDP** для общих сообщений, для ловушек используется порт **162 UDP**. Для прослушки порта SNMP обновите параметры службы в Linux (предварительно скопируйте ID коллектора), инструкция как настроить прослушку ниже 1024 порта в Linux: **ссылка**

Настройка аудита на стороне Windows

Нажмите **Пуск - Выполнить** - Введите: **evntwin**

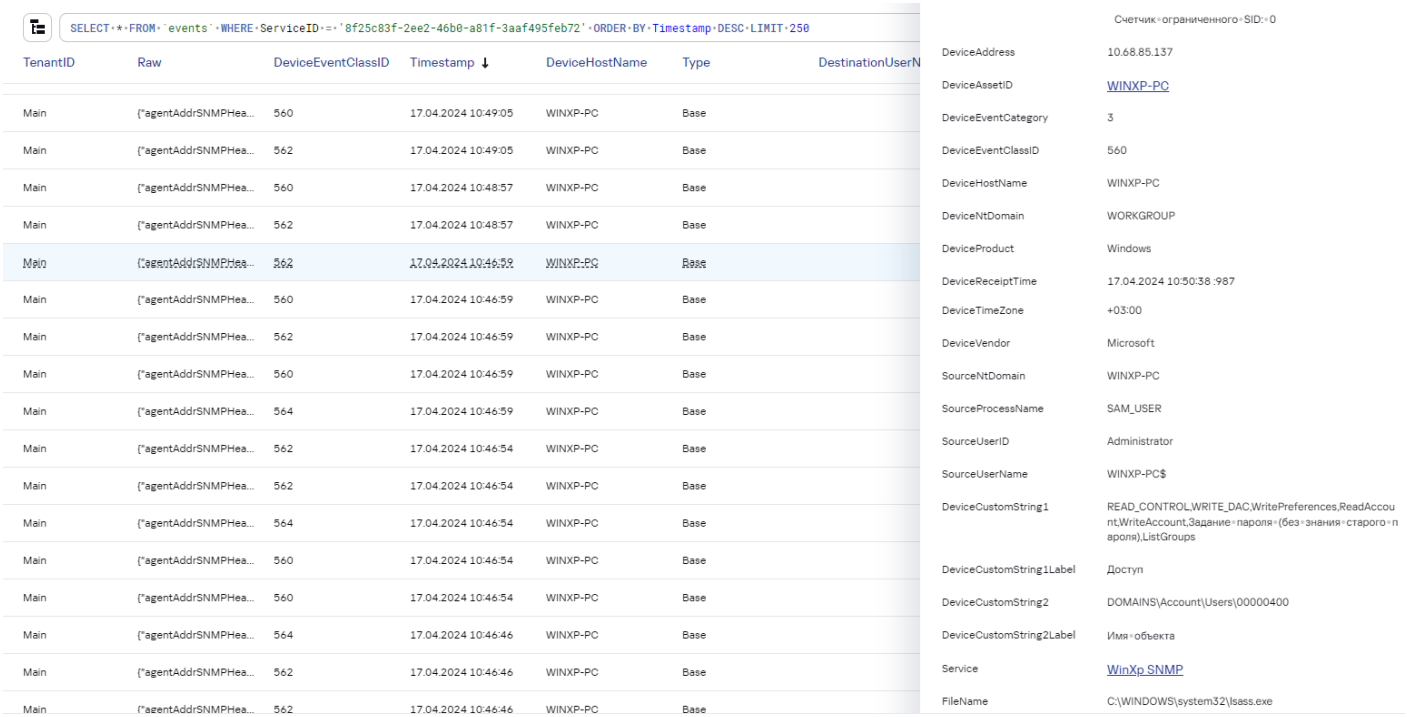


- В переключателе Тип конфигурации (Configuration type) выберите особая (Custom), а затем нажмите на кнопку Правка (Edit)
- В блоке параметров Источники событий (Event sources) найдите и добавьте с помощью кнопки Добавить (Add) события, которые вы хотите отправить в коллектор KUMA с установленным коннектором SNMP Trap (рекомендуется отправлять все из папки Security)
- Нажмите на кнопку Settings, в открывшемся окне установите флажок Не применять глушитель (Don't apply throttle) и нажмите OK
- Нажмите Применить (Apply) и OK

Генерация тестовых событий на Windows

Создайте и удалите тестового пользователя в системе для генерации событий в **Панель управления - Администрирование - Управление компьютером - Локальные пользователи - Папка пользователи**.

При корректных настройках в кума должно отобразиться событие:



Revision #4
Created 17 April 2024 07:43:33 by Boris Rzr
Updated 18 December 2024 10:16:19 by Koala