Содержание

Поиск статистики по IP-адресу абонента

Для работы данной функциональности необходимы следующие **компоненты**:

1. Модуль QoE Stor
2. Интерфейс управления CKAT DPI

Для работы данной функциональности необходимы следующие **лицензии**:

1. CKAT: CG-NAT — Трансляция сетевых адресов и выгрузка статистики в формате IPFIX
2. QoE: Сбор статистики NAT Flow, сжатие, пользовательские фильтры.

В зависимости от типа абонента определяется набор данных для хранения:

- Для публичного IP адреса достаточно выгрузки Full NetFlow в QoE Stor. Настройка экспорта в формате IPFIX
- Для приватного IP адреса необходимо дополнительно собирать NAT Flow - информацию о трансляциях. Конфигурация NAT Flow

Типы данных

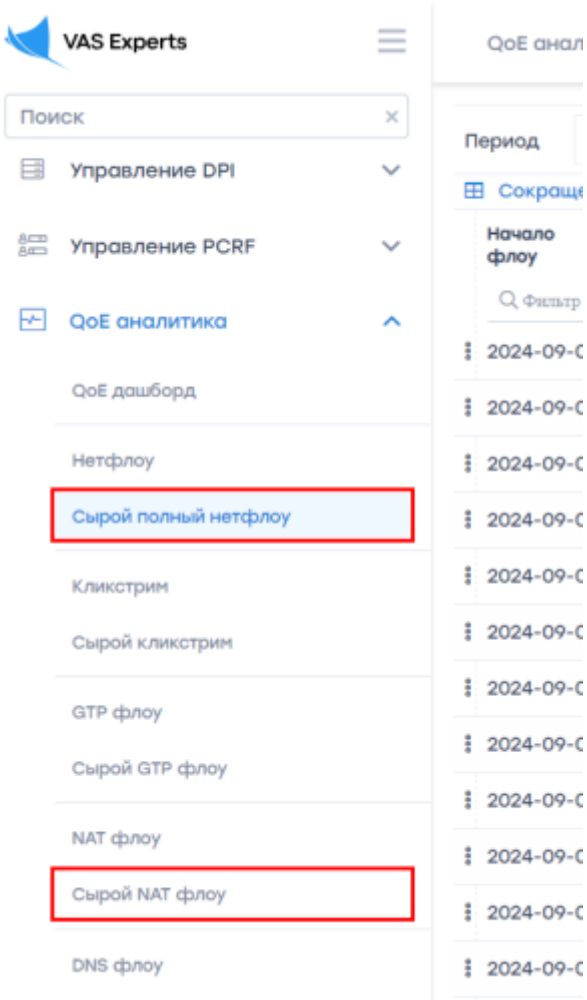
- **Сырые (неагрегированные) логи** — это полный набор полей IPFIX, они содержат все детали: время, IP-адреса, порты и многое другое. Эти логи позволяют получить информацию с точностью до секунды.
- **Агрегированные логи** — это обобщённые данные, которые используются для отчетов, таких как ТОП абонентов или хостов. Агрегация группирует события по времени (например, каждые 15 минут) и убирает лишние детали, например, порты. В результате получаются данные для анализа за временные интервалы, без точного времени.

Для точного анализа нужны сырые логи, а для отчётов — агрегированные.

Поиск информации осуществляется по агрегированным данным. Первоначально CKAT выгружает сырые данные в QoE Stor, по умолчанию агрегация выполняется каждые 15 минут. Подробнее про изменение периода агрегации и переагрегации.

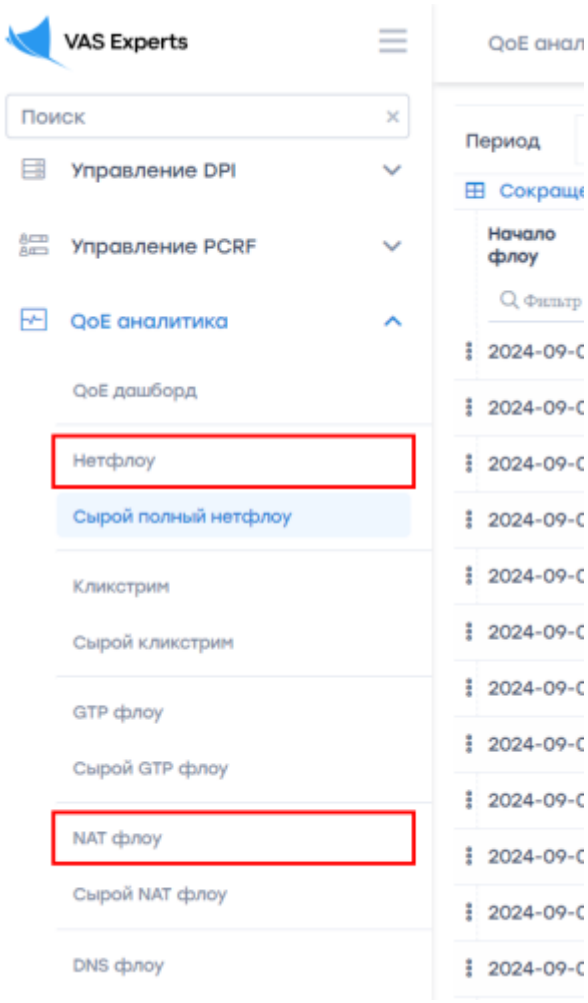
Сырые неагрегированные данные находятся в следующих разделах QoE Аналитики в GUI:

1. *Сырой полный нетфлоу* (по умолчанию данные хранятся **2 часа**)
2. *Сырой NAT флоу* (по умолчанию данные хранятся **2 часа**), требуется лицензия QoE



Агрегированная статистика находится в следующих разделах QoE Аналитики в GUI:

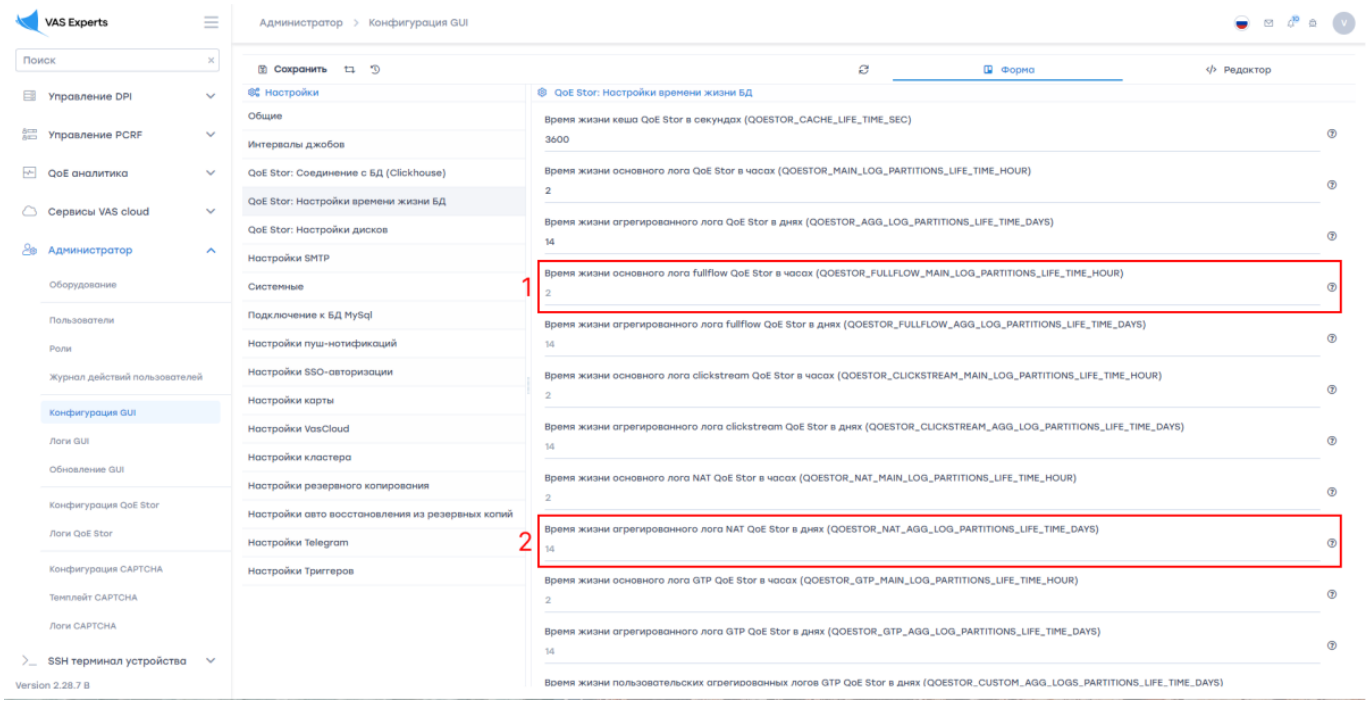
1. *Нетфлоу* (по умолчанию данные хранятся **14 дней**)
2. *NAT флоу* (по умолчанию данные хранятся **14 дней**), требуется лицензия QoE



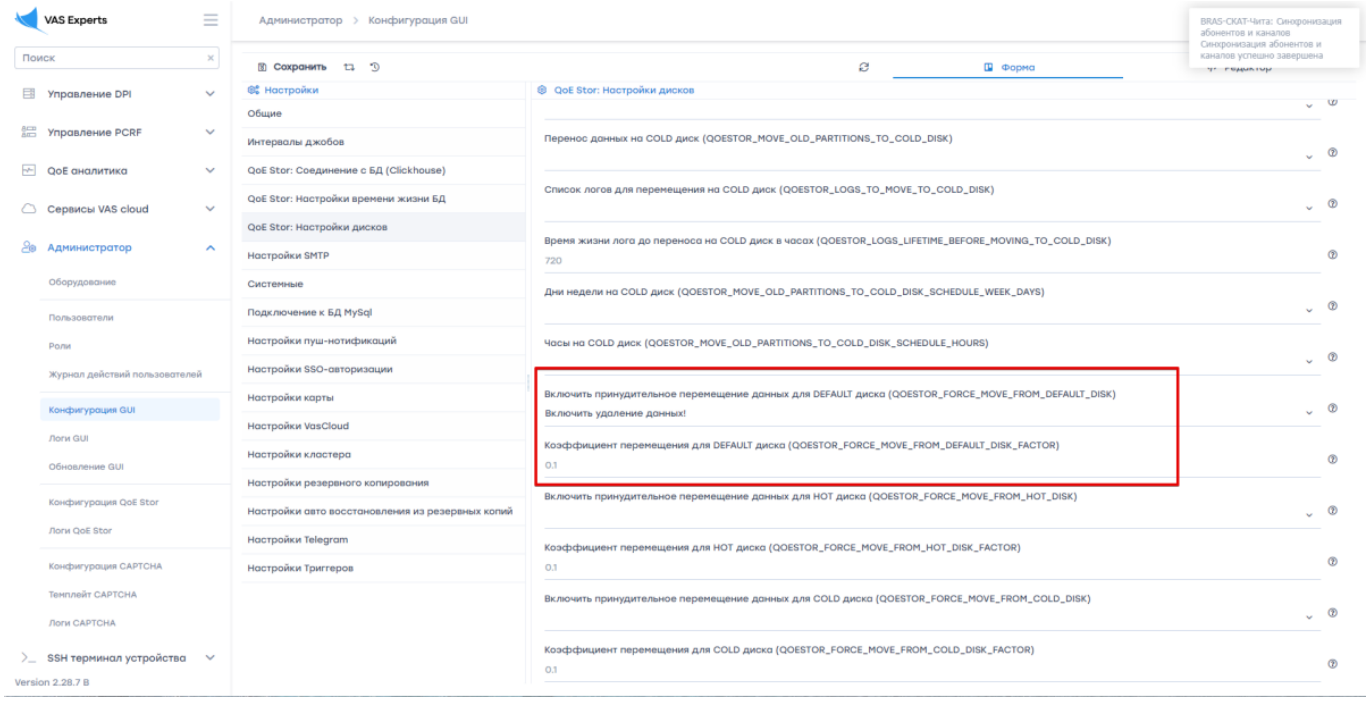
Настройка периода хранения данных

В GUI в разделе Администратор → Конфигурация GUI → Настройки → QoE Stor: Настройки времени жизни БД:

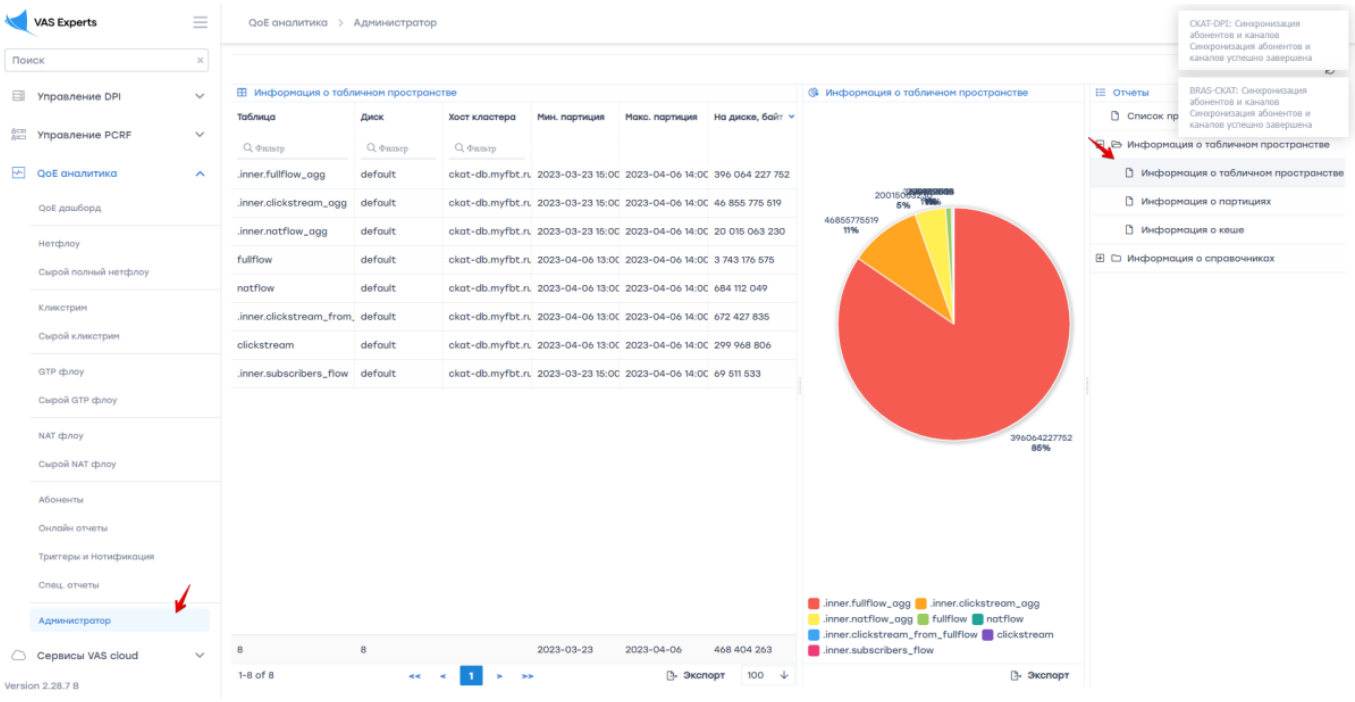
- Для Сырого полного нетфлоу пункт *Время жизни основного лога fullflow QoE Stor в часах* **(1)**.
- Для NAT флоу пункт *Время жизни агрегированного лога NAT QoE Stor в днях* **(2)**.



При увеличении времени хранения данных рекомендуется включить удаление старых данных при заполнении диска: Администратор → Конфигурация GUI → Настройки → QoE Stor: Настройки дисков → Пункт *Включить принудительное перемещение данных ...* – выбрать *Включить удаление данных!* → Пункт *Коэффициент перемещения для DEFAULT диска ...* – задать значение *0.1*.



Узнать, сколько места на диске занимают логи можно в разделе QoE аналитика → Администратор → Отчеты → Информация о табличном пространстве.



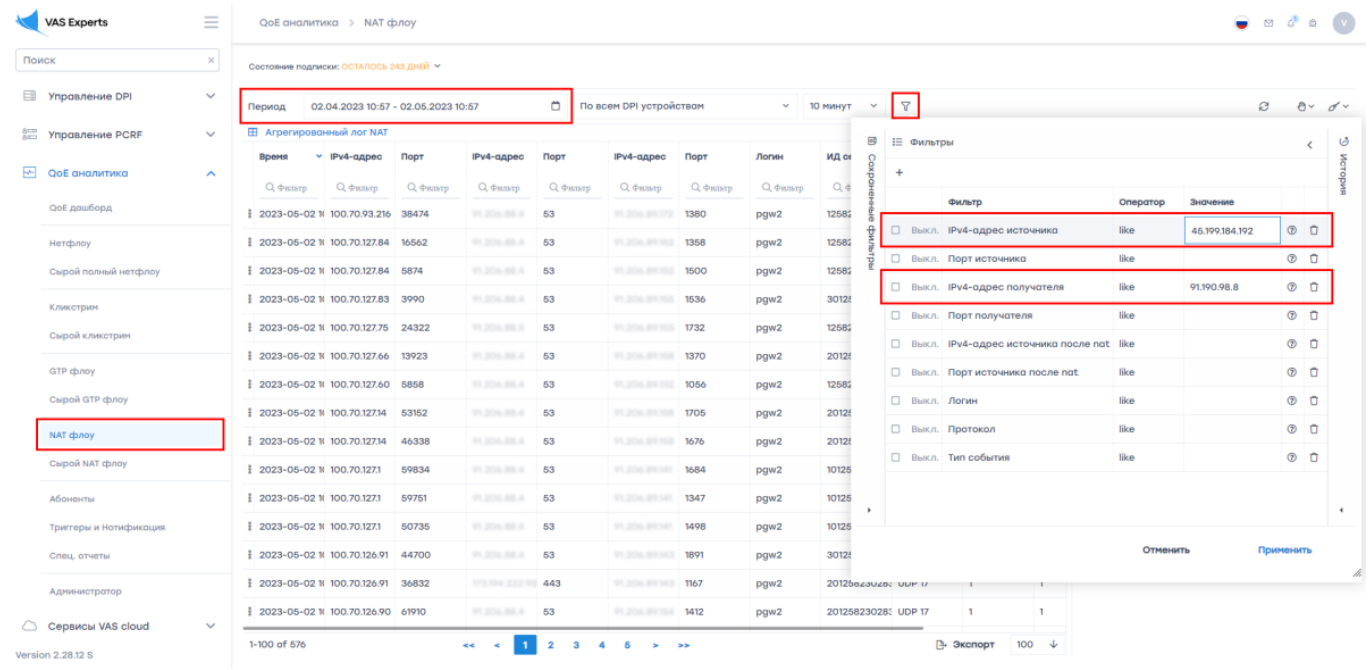
Поиск активности абонента в GUI CKAT

Для приватного IP адреса. Раздел NAT флоу. Требуется лицензия QoE

Запрос лицензии вы можете сделать из GUI после перехода в раздел путем заполнения формы или обратиться на sd@vas.expert

Возможность просматривать данные об активности абонентов появится после формирования NAT-лога — инструкция Конфигурация NAT Flow.
В GUI необходимо перейти в раздел QoE аналитика → NAT флоу.
В разделе NAT флоу нужно:

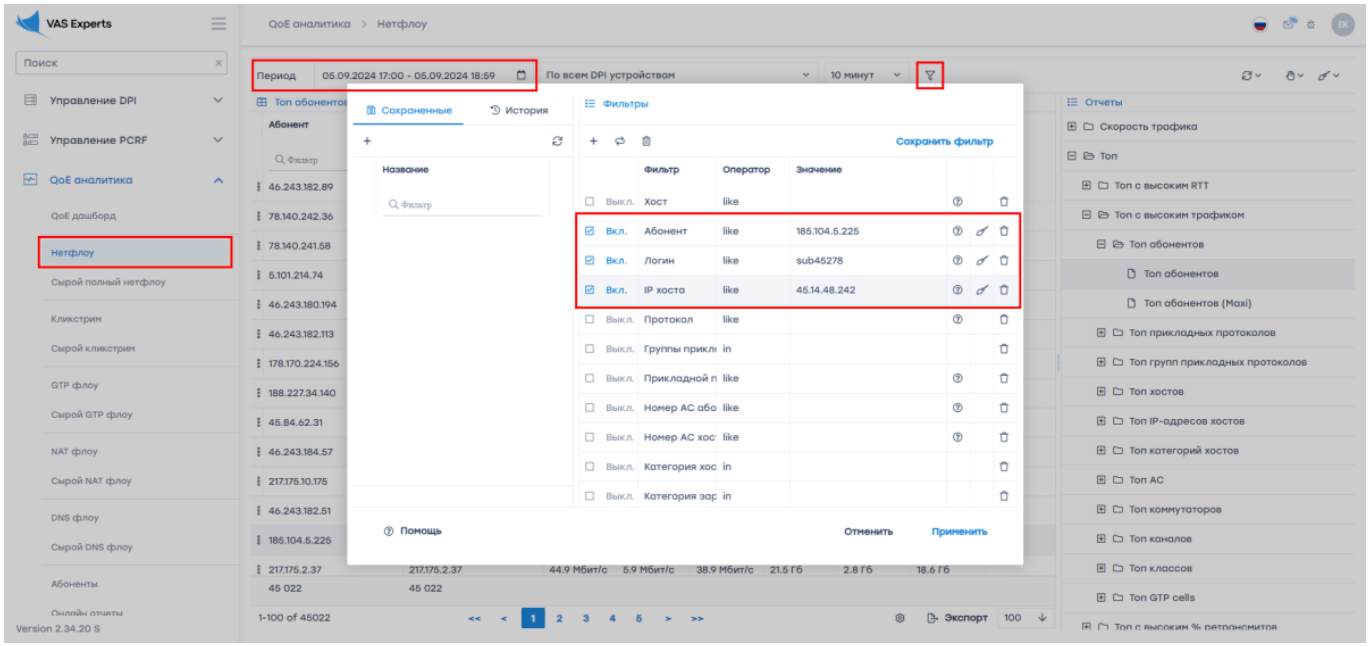
1. Выбрать период
2. Включить фильтры “IPv4-адрес источника” и “IPv4-адрес получателя” (отметить галочкой)
3. Задать значения включенным фильтрам, применить изменения



Для Публичного IP адреса из Агрегированных данных. Раздел Нетфлоу

В GUI необходимо перейти в раздел QoE аналитика → Нетфлоу.
В разделе Нетфлоу нужно:

1. Выбрать период **(по умолчанию хранится всего 14 дней!)**
2. Включить фильтры "Абонент", "Логин" и "IP хоста" (отметить галочкой)
3. Задать значения включенным фильтрам, применить изменения



Для Публичного IP адреса. Раздел Сырой полный нетфлоу

В GUI необходимо перейти в раздел QoE аналитика → Сырой полный нетфлоу.
В разделе Сырой полный нетфлоу нужно:

1. Выбрать период **(по умолчанию хранится всего 2 часа!)**
2. Включить фильтры “IPv4-адрес источника” и “IPv4-адрес получателя” (отметить галочкой)
3. Задать значения включенным фильтрам, применить изменения