Table of Contents

7 Модуль QoE Stor

Модуль сбора и хранения данных для QoE аналитики

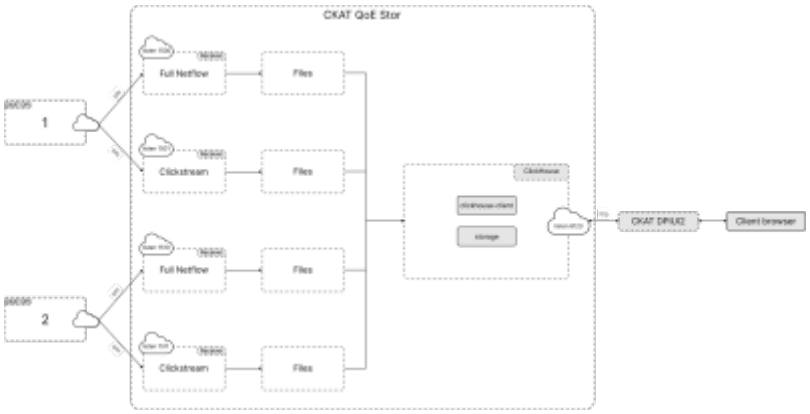
Введение

Модуль предназначен для сбора и хранения данных Нетфлоу и Кликстрим. Данные используются для анализа QoE в DPIUI2.

Архитектура

Данные от СКАТ DPI принимаются на нескольких сокетах (tcp или udp) с помощью утилиты приема IPFIX потоков данных.

Данные хранятся в БД ClickHouse.



Инсталляция и обновление

Рекомендации к оборудованию

Не устанавливайте модуль на сервер с DPI платформой!

Минимальные требования

Для подсистемы можно использовать оборудование или виртуальные машины со сл.характеристиками:

1. Процессор (CPU) 2.5 ГГц - 1 шт
2. Оперативная память (RAM) - от 16 Гб

3. Жесткий диск (SSD крайне желательно) - от 500 Гб
4. Операционная система - CentOS 7+ или CentOS 8+
5. Сетевая плата (NIC) - от 1 Гбит/сек

 Калькулятор с примером оборудования

Процессор

Требуется поддержка набора инструкций SSE 4.2.

Выбирайте процессоры с большим числом ядер. Тактовая частота менее важна. Например, 16 ядер с 2600 МГц лучше, чем 8 ядер 3600 МГц.

 Не отключайте Hyper-threading и Turbo-Boost.

Оперативная память

Памяти должно быть не меньше чем объем запрашиваемых данных.

Чем больше памяти, тем лучше производительность при построении отчетов.

Чем больше памяти, тем меньше нагрузка на диск.

Минимальное требование - 16Гб.

Всегда отключайте файл подкачки.

Жесткий диск

Требуемое место на диске от 16ГБ на каждый день хранения в зависимости от трафика. Подсчитано, что 10 Гбит/с среднесуточного трафика генерирует примерно 25 ГБ данных за один час в QoE Store.

Если ваш бюджет позволяет использовать SSD, используйте SSD (крайне рекомендуется). В противном случае используйте HDD. SATA HDDs 7200 RPM подойдут.

При использовании HDD можно объединить их RAID-10, RAID-5, RAID-6 или RAID-50.

Основной объем данных хранится в каталоге /var/lib/clickhouse.

Временные данные (дампы ipfix) хранятся в каталоге /var/qoestor/backend/dump.

Для лучшей производительности важно (рекомендуется), чтобы эти каталоги находились на отдельном диске или массиве. См. Перенос дампов и данных БД на отдельный диск

Советы по эксплуатации от Яндекс ClickHouse

Советы по эксплуатации от Яндекс ClickHouse вы можете прочитать по ссылке https://clickhouse.yandex/docs/ru/operations/tips/.

Информация о версиях

Версия v.1.7.3 (15.10.2020)

- Возможность хранение данных на HOT и COLD дисках
- Прием и хранение NAT логов. Опция формирования NAT лога из fullflow. Возможность гибкой настройки периода агрегации и списка полей, подлежащих агрегации
- Прием и хранение GTP логов

Версия v.1.6.0 (14.09.2020)

- Опция: подмена поля Логин значением из поля vchannel
- Баг фикс

Версия v.1.4.2 (01.06.2020)

- Баг фикс

Версия v.1.4.0 (04.05.2020)

- Поддержка совместимости с Clickhouse 20.3
- Возможность установки на CentOS 8

Версия v.1.3.8 (09.04.2020)

- Обновлены справочники протоколов
- Добавлено автообновление справочника AC

Версия v.1.3.6 (25.11.2019)

- Обновлены справочники протоколов

Версия v.1.3.5 (06.11.2019)

- Исправлено поведение справочника локальных подсетей (попадали лишние адреса)
- Адаптирована загрузка кликстрима для правильной работы ЛК в dpiui2-2.8.2

Версия v.1.3.4 (25.10.2019)

- Locked в кликстрим

Версия v.1.3.3 (15.10.2019)

- Обновление Кликхаус до последней версии (>= 19.15)
- Улучшен метод загрузки и обработки логов
- Подготовлена база для анализа сырых логов
- Соединение логов Клистрим и Нетфлоу

Версия v.1.1.1 (06.09.2019)

- Обновление Кликхаус до последней версии
- Справочники asnum_exclude_dic, subnets_exclude_dic и соответствующий режим фильтрации по этим справочникам

Версия v.1.0.9 (21.02.2019)

- Устранен баг с неверным распознаванием магистральных коммутаторов
- Обновлен справочник protocols_dic

Версия v.1.0.7 хот фиксы (24.12.2018)

- Предусмотрен реэкспорт ipfix в конфигах ресивера: IPFIX_FULLFLOW_EXPORT и IPFIX_CLICKSTREAM_EXPORT

Версия v.1.0.6 хот фиксы (04.12.2018)

- Исправлены баги в работе справочника subnets_local_dic (типа A call to function range would produce 12884901882 array elements)
- Исправлена конфигурация ресиверов ipfixreceiver2 (FileWriter queue is full. Records dropped.)

Версия v.1.0.5 (03.12.2018)

- Справочники по Категориям хостов
- Переход на ipfixreceiver2

1. Перед обновлением не забудьте обновить скрипт установки (в разделе Инсталляция). Для обновления используйте скрипт установки.
2. После обновления, проверьте, запустились ли ресиверы (netstat -nlpa | grep 1500 и netstat -nlpa | grep 1501). Сокеты должны прослушиваться

ipfixreceiver2
3. Если ресиверы не запустились, выполните скрипт sudo sh /var/qoestor/backend/qoestor-config.sh

Версия v.1.0.4 (02.11.2018)

- Внедрена предагрегация, которая сокращает нетфлоу в 6-7 раз, кликстрим в 3 раза
- Внедрены справочники: абоненты, коммутаторы, автономные системы (AS), crc
- Добавлена опция определения направления трафика и фильтрация абонентов (разделение IP хостов и IP абонентов) по AS и CIDR. Опция актуальна в случае установки СКАТ DPI на зеркале.

Данная версия QoE Stor работает с версией DPIUI2-2.1.5+

Если вы успели поставить версию 1.0.0, перед установкой новой версии необходимо удалить БД (полная несовместимость версий). Для этого выполните команду

```
clickhouse-client --query="drop database qoestor"
```

Версия v.1.0.0 (20.09.2018)

- Создан новый модуль – QoE Stor

Инсталляция

Перед установкой или обновлением проверьте наличие интернета. Запуски скриптов выполняйте из под root или sudo.

Проверьте правильность установки времени и временной зоны на сервере. При необходимости поправьте и перезапустите сервер.

Для установки или обновления в автоматическом режиме, выполните последовательно:

1. Выполните скрипт fastor-rpm_install.sh.

```
sudo yum install wget

sudo wget https://vasexperts.ru/install/fastor-rpm_install.sh
```

```
sudo sh fastor-rpm_install.sh
```

Будет произведена установка rpm-пакетов: ipfixreceiver, clickhouse, fastor. Будет произведена автоматическая настройка согласно конфигурации.

2. Выполните команду

```
clickhouse-client -n < /var/qoestor/backend/etc/db/qoestor.sql
```

Будет обновлена схема БД.

Не забывайте после установки выполнять

```
clickhouse-client -n < /var/qoestor/backend/etc/db/qoestor.sql
```

Это страхует случаи, когда схема не успевает обновиться в результате долгого перезапуска БД.

Обновление

Обновление выполняется теми же скриптами, что и в разделе Инсталляция.

Если вы выполнили команду yum –y update и перестали запускаться ресиверы, обратитесь к разделу решения проблем по ссылке.

Не забывайте после обновления выполнять

```
clickhouse-client -n < /var/qoestor/backend/etc/db/qoestor.sql
```

Это страхует случаи, когда схема не успевает обновиться в результате долгого перезапуска БД.

#Ipfix form DPI 0 IPFIX_FULLFLOW_PORT_TYPE[0]=tcp IPFIX_FULLFLOW_PORT[0]=1500
#IPFIX_FULLFLOW_ROTATE_MINUTES[0]=10 #IPFIX_FULLFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_FULLFLOW_FW_MAX_QUEUE_SIZE[0]=10 #IPFIX_FULLFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_FULLFLOW_EXPORT[0]=10.0.0.2/9920/tcp,10.0.0.3/3440/udp

IPFIX_CLICKSTREAM_PORT_TYPE[0]=tcp IPFIX_CLICKSTREAM_PORT[0]=1501
#IPFIX_CLICKSTREAM_ROTATE_MINUTES[0]=12
#IPFIX_CLICKSTREAM_ROTATE_DELAY_SECONDS[0]=400
#IPFIX_CLICKSTREAM_FW_MAX_QUEUE_SIZE[0]=10
#IPFIX_CLICKSTREAM_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_CLICKSTREAM_EXPORT[0]=10.0.0.2/9921/tcp,10.0.0.3/3441/udp

IPFIX_GTPFLOW_PORT_TYPE[0]=tcp IPFIX_GTPFLOW_PORT[0]=1502
#IPFIX_GTPFLOW_ROTATE_MINUTES[0]=10 #IPFIX_GTPFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_GTPFLOW_FW_MAX_QUEUE_SIZE[0]=10 #IPFIX_GTPFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_GTPFLOW_EXPORT[0]=10.0.0.2/9921/tcp,10.0.0.3/3441/udp

IPFIX_NATFLOW_PORT_TYPE[0]=tcp IPFIX_NATFLOW_PORT[0]=1503
#IPFIX_NATFLOW_ROTATE_MINUTES[0]=10 #IPFIX_NATFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_NATFLOW_FW_MAX_QUEUE_SIZE[0]=10 #IPFIX_NATFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_NATFLOW_EXPORT[0]=10.0.0.2/9921/tcp,10.0.0.3/3441/udp

#Traffic direction definition # 0 - as is # 1 - by AS (for fullflow only) # 2 - by CIDR (for fullflow and clickstream) # 3 - by both: AS and CIDR # 4 - any: AS or CIDR TRAFFIC_DIR_DEF_MODE=0

#Subscriber filter # 0 - no filter # 1 - by AS (for fullflow only) # 2 - by CIDR (for fullflow and clickstream) # 3 - by both: AS and CIDR # 4 - any: AS or CIDR SUBSCRIBER_FILTER_MODE=0

#Subscriber exclude # 0 - no exclude # 1 - by AS (for fullflow only) # 2 - by CIDR (for fullflow and clickstream) # 3 - by both: AS and CIDR # 4 - any: AS or CIDR SUBSCRIBER_EXCLUDE_MODE=0

#Enable host (url) categories dics autoload URLS_CATEGORIES_DIC_AUTOLOAD_ENABLED=1

#Enable asnum dic autoload ASNUM_DIC_AUTOLOAD_ENABLED=1

#Enable auto replacing Login with vchannel on insert # 0 - Disabled # 1 - Enabled # 2 - Enabled if Login is empty ULR_REPLACE_LOGIN_WITH_VCHANNEL=0

Use dictionary when replacing login ULR_USE_DIC_WHEN_REPLACING_LOGIN=0

Enable autoload of vchannel_name_dic ULR_VCHANNEL_NAME_DIC_AUTOLOAD_ENABLED=0

vchannel_name_dic remote url ULR_VCHANNEL_NAME_DIC_URL=

#Import NAT events from fullflow NAT_IMPORT_FROM_FULLFLOW # 0 - Disabled # 1 - Enabled

#Fields to save when aggregating NAT log (bitmask) # 0x1 - Save protocol ID # 0x2 - Save event type, # 0x4 - Save source ipv4, # 0x8 - Save source port, # 0x10 - Save destination ipv4, # 0x20 - Save destination port, # 0x40 - Save post NAT source ipv4, # 0x80 - Save post NAT source_port, # 0x100 - Save session ID, # 0x200 - Save login, # 0x400 - Save DPI ID NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK=0

#Time interval for aggregating NAT logs NAT_AGG_LOG_GROUP_TIME_INTERVAL # 1 - 1 minute # 5 - 5 minutes # 10 - 10 minutes # 15 - 15 minutes # 30 - 30 minutes # 60 - 60 minutes

Конфигурация справочников

Все справчники находятся в папке /var/qoestor/backend/etc/db/ и имеют расширение .txt

Для каждого справочника есть образец sample.txt. Можно использовать в качестве шаблона.

Все столы в справочниках разеделены символом табуляции (\t). Колиество \t должно быть на единицу меньше, чем число столбцов в справочнике. Следите за этим внимательно.

При изменении файлов, данные подгружаются в БД автоматически.

Некоторые полезные команды при работе со справочниками:

- Ускорить обновление данных в справочниках

```
clickhouse-client --database=qoestor --query="system reload
dictionaries"
```

- Проверить, есть ли ошибки в справочниках

```
clickhouse-client --database=qoestor --query="select * from
system.dictionaries"
```

- Проверить, есть ли данные в справочнике, например для subnets_local_dic

```
clickhouse-client --database=qoestor --query="select * from
subnets_local_dic"
```

Справочники asnum_local_dic и subnets_local_dic

В данных справочниках указывается список ваших локальных AS и локальных подсетей. Справочники используется для определения направления трафика (актуально, когда DPI установлен на зеркале) и фильтрации абонентов (чтобы в отчетах по абонентам не фигурировали IP-адреса хостов)

Пример справочника **asnum_local_dic**

```
12345   LOCAL
65535   UNKNOWN
```

Первый столбец - номер AS, второй - название (отображается в отчетах).

Пример справочника **subnets_local_dic**

```
192.168.1.0/24  LOCAL
10.64.66.0/24   LOCAL
172.16.0.0  LOCAL
2a02:2168:aaa:bbbb::2   LOCAL
```

Первый столбец - IP адрес или CIDR, второй – название (не отображается в отчетах, но формат справочника требует).

Не добавляйте слишком большую подсеть. Разбивайте на мелкие. Ограничение - 100000000

Справочники asnum_exclude_dic и subnets_exclude_dic

В данных справочниках указывается список ваших АС и подсетей (либо одиночных IP), которые необходимо исключить из агрегированных логов. Подсети указанные в справочниках будут игнорироваться при записи в агрегированный лог (который используется для построения отчетов). Для управления фильтрацией по этим справочникам используйте параметр SUBSCRIBER_EXCLUDE_MODE . См. раздел Конфигурация.

Пример справочника **asnum_exclude_dic**

```
12345   LOCAL
65535   LOCAL
```

Первый столбец - номер AS, второй - название (не отображается в отчетах, но формат справочника требует).

Пример справочника **subnets_exclude_dic**

```
192.168.1.0/24  LOCAL
10.64.66.0/24   LOCAL
172.16.0.0  LOCAL
2a02:2168:aaa:bbbb::2   LOCAL
```

Первый столбец - IP адрес или CIDR, второй – название (не отображается в отчетах, но формат справочника требует).

Не добавляйте слишком большую подсеть. Разбивайте на мелкие. Ограничение - 100000000

Справочники subscribers_dic, switches_dic, crc_dic

subscribers_dic

Справочник абонентов.

Пример справочника

```
10.64.66.100    login    5    port1    unit_vendor    cabel    contract
services    mac
10.64.66.101    login    2    port1    unit_vendor    cabel    contract
services    mac
10.64.66.102    login    3    port1    unit_vendor    cabel    contract
services    mac
10.64.66.103    login    4    port1    unit_vendor    cabel    contract
services    mac
10.64.66.104    login    5    port1    unit_vendor    cabel    contract
services    mac
```

```
10.64.66.105    login    5    port2    unit_vendor    cabel    contract
services    mac
10.64.66.106    login    5    port3    unit_vendor    cabel    contract
services    mac
```

Столбцы:

1. IP адрес
2. Логин
3. Идентификатор коммутатора (доступа)
4. Порт коммутатора
5. Вендор абонентского оборудования
6. Кабель
7. Договор
8. Сервисы
9. MAC адрес абонентского оборудования (зарезервирован для будущих целей)

switches_dic

Иерархический справочник оборудования (коммутаторов доступа и магистральных коммутаторов)

Пример справочника

```
1  Коммутатор 1    Ethernet    Регион1  Адрес 1    10.140.1.18    oper1    0
0
2  Коммутатор 2    Ethernet    Регион2  Адрес 2    10.140.2.18    oper1    0
0
3  Коммутатор 3    Ethernet    Регион3  Адрес 3    10.140.3.18    oper1    0
1    port1
4  Коммутатор 4    Ethernet    Регион4  Адрес 4    10.140.4.18    oper1    0
3    port1
5  Коммутатор 5    Ethernet    Регион5  Адрес 5    10.140.5.18    oper1    0
4    port1
```

Столбцы:

1. Идентификатор оборудования UInt64
2. Наименование
3. Тип
4. Район
5. Адрес
6. IP адрес коммутатора
7. Оператор
8. Флаг: признак магистрального коммутатора (1 - если да). Не используется, можно везде оставить 0
9. Идентификатор вышестоящего коммутатора UInt64
10. Порт вышестоящего коммутатора
11. Собственник

crc_dic

Справочник ошибок (CRC) на портах коммутаторов

Пример справочника

```
2   port1    450
5   port1    550
5   port2    500
4   port1    780
```

Столбцы

1. Идентификатор коммутатора
2. Порт коммутатора
3. Значение CRC

Справочники urlcats_dic и urlcats_host_dic

Справочники Категорий хостов. Предназначены для определения принадлежности хоста определённой категории.

Справочники подкачиваются автоматически с ресурсов vasexperts.ru.

Для ускорения начальной загрузки выполните

1. ```
   sh /var/qoestor/backend/etc/cron_daily.sh
   ```

2. ```
   clickhouse-client --database=qoestor --query="system reload
   dictionaries"
   ```

Перенос дампов и данных БД на отдельный диск

По умолчанию все данные хранятся в разделе /var.

Допустим, мы подключили отдельный диск к /home.

1. Работаем под root пользователем

   ```
   sudo su
   ```

2. Останавливаем ресиверы и БД

   ```
   systemctl stop qoestor_fullflow_0.service
   systemctl stop qoestor_clickstream_0.service
   sudo /etc/init.d/clickhouse-server stop
   ```

3. Создаем каталоги в разделе /home

```
mkdir /home/qoestor
mkdir /home/qoestor/clickhouse
mkdir /home/qoestor/dump
```

4. Копируем данные на новый диск

```
cp -r /var/lib/clickhouse/* /home/qoestor/clickhouse
cp -r /var/qoestor/backend/dump/* /home/qoestor/dump
```

5. Меняем владельца папки /home/qoestor/clickhouse

```
chown -R clickhouse:clickhouse /home/qoestor/clickhouse
```

6. Удаляем старые каталоги

```
rm -rf /var/lib/clickhouse
rm -rf /var/qoestor/backend/dump/
```

7. Создаем симлинки

```
ln -s /home/qoestor/clickhouse /var/lib/clickhouse
ln -s /home/qoestor/dump /var/qoestor/backend/dump
```

8. Проверяем линки

```
readlink -f /var/lib/clickhouse
readlink -f /var/qoestor/backend/dump
```

9. Запускаем БД

```
sudo /etc/init.d/clickhouse-server restart
```

10. Запускаем ресиверы

```
sudo sh /var/qoestor/backend/qoestor-config.sh
```

Проблемы и решения

Не работает, хотя все установили по инструкции

Если вы все установили и настроили по инструкции, а в разделе DPIUI2 “QoE Аналитика” пусто, то вот перечень шагов, которые стоит выполнить, прежде чем обращаться в тех. поддержку.

1. Проверьте правильность установки времени и таймзоны на серверах с dpiui2 и QoE Stor. Попробуйте в dpiui2 установить большой период. Если дело в таймзоне, данные появятся. Правильно настройте время на серверах dpiui2 и QoE Stor, перезапустите серверы полностью.
2. На сервере с QoE Stor проверить, создана ли БД

```
clickhouse-client --query="show databases" | grep qoestor
```

Если БД не создана, создать ее командой

```
clickhouse-client -n < /var/qoestor/backend/etc/db/qoestor.sql
```

3. На сервере с QoE Stor проверить, есть ли данные в БД

```
clickhouse-client --query="select count(), min(flow_start_time),
max(flow_start_time) from qoestor.fullflow"
```

и

```
clickhouse-client --query="select count(), min(time), max(time) from
qoestor.clickstream"
```

Либо посмотреть, как наполняются партиции через интерфейс по ссылке

```
https://your_gui_host/#QoEAdmin/report=TableSpaceReport
```

4. Проверить, запущены ли ресиверы

```
ps aux | grep ipfix
```

5. На сервере с QoE Stor проверить логи ресиверов в папке

```
/var/qoestor/backend/logs
```

В логах не должно быть ошибок. Должна быть видна ротация дампов и запись их в БД.

6. На сервере с QoE Stor проверить, прослушиваются ли порты 1500 и 1501 командой

```
netstat -nlpa | grep 1500 и netstat -nlpa | grep 1501
```

Перезапустить все ресиверы на всякий случай командой

```
sudo sh /var/qoestor/backend/qoestor-config.sh
```

7. Еще раз проверить настройки экспорта ipfix на dpi
8. На сервере с DPIUI2 проверить настройки подключения GUI к QoE Stor
9. На сервере с QoE Stor проверить, запущена ли СУБД ClickHouse командой

```
ps aux | grep clickhouse
```

Убедитесь, что достаточно оперативной памяти на сервере.

10. На сервере с QoE Stor проверить /var/log/clickhouse-server/clickhouse-server.err.log

Если есть необходимость очистить все данные в БД, то на сервере с QoE Stor надо

1. Удалить БД командой

```
clickhouse-client --query="drop database qoestor"
```

2. Пересоздать БД командой

```
clickhouse-client -n < /var/qoestor/backend/etc/db/qoestor.sql
```

Выполнили yum –y update, не запускаются ресиверы

При выполнении **yum –y update** ломаются некоторые библиотеки. Ресиверы перестают запускаться.

1. Удалите fastor и зависимости

```
 yum remove fastor ipfixreceiver libfixbuf netsa_silk netsa-python
```

2. Установите заново, используя скрипт fastor-rpm_install.sh.gz

Как уменьшить период хранения и очистить данные

Очистка данных производится модулем dpiui2. В файле /var/www/html/dpiui2/backend/.env измените параметры QOESTOR_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR=2 QOESTOR_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS=15 Выполните рестарт php /var/www/html/dpiui2/backend/artisan queue:restart

SQL и выгрузка данных в CSV, JSON, TabSeparated

При необходимости вы можете самостоятельно без дополнительных инструментов сформировать собственные отчеты и выгрузить данные в любом формате CSV, JSON, TabSeparated.

Данные хранятся в 4 основных логах

- qoestor.fullflow – полный netflow лог, период хранения – 24 часа
- qoestor.clicksteam – полный clickstream лог, период хранения – 24 часа
- qoestor.fullflow_agg – предагрегированный neflow лог, период хранения не ограничен
- qoestor.clicksteam_agg – предагрегированный clickstream лог, период хранения не ограничен

Формат команды следущий

```
clickhouse-client --database=qoestor  --query="Ваш sql тут"
```

По умолчанию данные выгружаются в формате TabSeparated.

Пример. Клиент попросил лог соединений с определенным хостом в формате CSV

```
clickhouse-client --database=qoestor --query="select * from fullflow
```

```
prewhere flow_start_date = '2018-10-04' where (source_ipv4 = '10.64.66.100'
or destination_ipv4 = '10.64.66.100') and host = 'google.com' ORDER BY
flow_start_time limit 10 format CSV"
```

Подробную информацию по SQL ClickHouse смотрите по ссылке
https://clickhouse.yandex/docs/ru/query_language/select/