ОБНОВЛЕНО 16 МАР

Data Explorer

Data Explorer — модуль системы FlowCollector для анализа данных сетевых потоков. Он сохраняет весь собранный трафик в базе данных и обеспечивает возможности для его анализа и визуализации.

С помощью модуля можно задать фильтры по параметрам трафика (протоколы, порты, IP-адреса, длина пакета и т.д) и получить статистику и графические отчеты. Это позволяет выявлять аномальные или интересующие паттерны трафика, а так же проводить ретроспективный анализ трафика.

Для отображения раздела Data Explorer в веб-интерфейсе требуется включённый параметр save-flow в конфигурации анализатора FlowCollector.

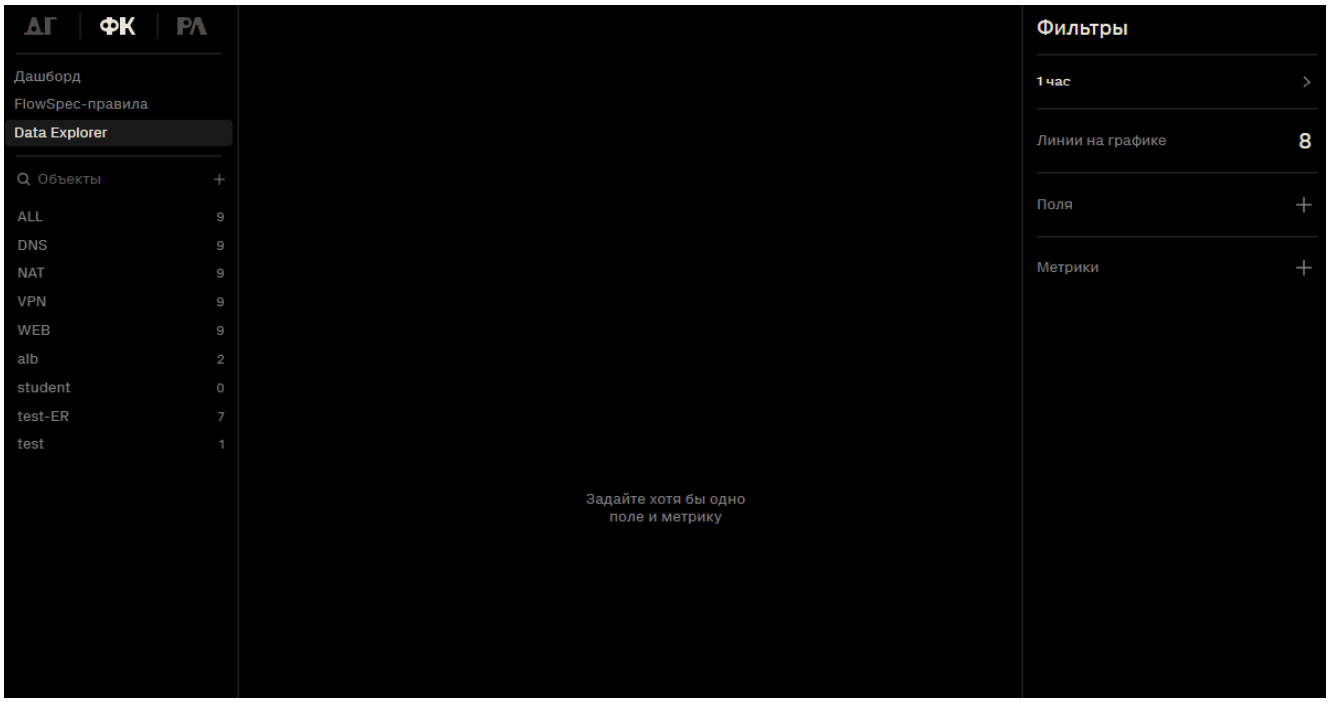
Открыть конфигурационный файл анализатора:

```
sudo nano /opt/spfc/etc/analyzer.yaml
```

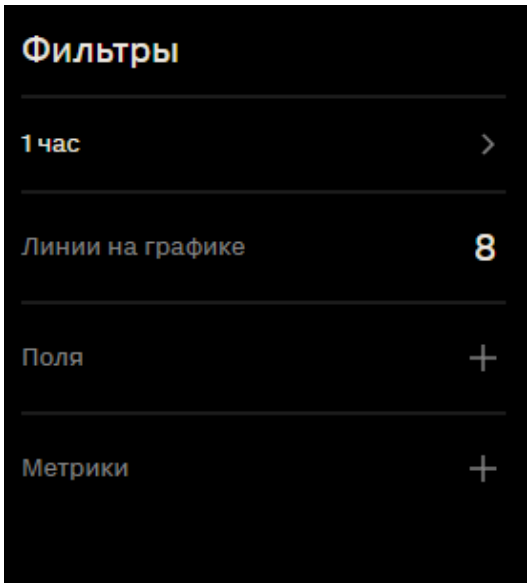
Включить параметр save-flow:

```
save-flow: true
```

Для доступа к модулю выберите **Data Explorer** в боковом меню интерфейса. Затем откроется рабочая область модуля.

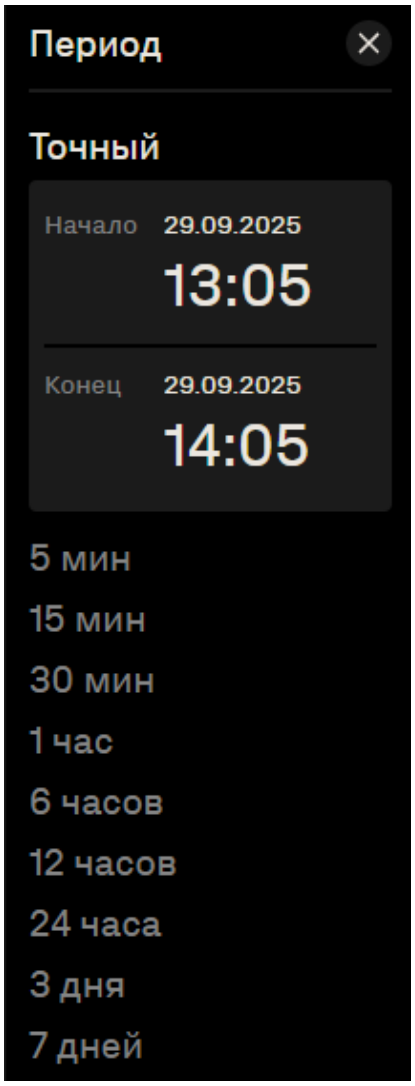


Для построения графиков в **Data Explorer** необходимо предварительно задать параметры фильтра.



Период

Период - это временной интервал, за который выводятся данные. Его можно задать вручную, указав начальное и конечное время, или выбрать из готовых вариантов, например, последние 24 часа или 7 дней.



Линии на графике

Линии на графике — параметр, определяющий число отображаемых линий графика. На график выводятся верхние *N* строк таблицы по текущей сортировке. Каждая строка отображается отдельной линией на графике.

Поля

Поля - это атрибуты данных, по которым производится агрегация и фильтрация. Они определяют, какие именно характеристики данных будут использоваться для анализа или отображения. В системе можно выбрать несколько атрибутов для более детального анализа.

Поле	Описание
Das	Номер автономной системы получателя

Поле	Описание
Dasname	Имя автономной системы получателя
Dport	Порт получателя
Dst	IP-адрес получателя
Geoipdst	Страна получателя
Geoipsrc	Страна отправителя
Len	Длина пакета
Protocol	Протокол
Sas	Номер автономной системы отправителя
Sasname	Имя автономной системы отправителя
Sport	Порт отправителя
Src	IP-адрес отправителя
Tcpflags	TCP флаги
Tos	Тип обслуживания

Метрики

Метрики – это показатели, которые вычисляются на основе значений выбранных полей и отражают количественные характеристики данных в сети. Метрики позволяют анализировать и оценивать различные параметры сетевого трафика такие как количество переданных данных, количество пакетов, географическое распределение трафика и другие показатели.

Метрика	Описание
Bits	Биты
Das	Номер автономной системы получателя
Dport	Порт получателя
Dst	IP-адрес получателя
Geoipdst	Страна получателя
Geoipsrc	Страна отправителя
Packets	Пакеты
Sas	Номер автономной системы отправителя
Sport	Порт отправителя
Src	IP-адрес отправителя

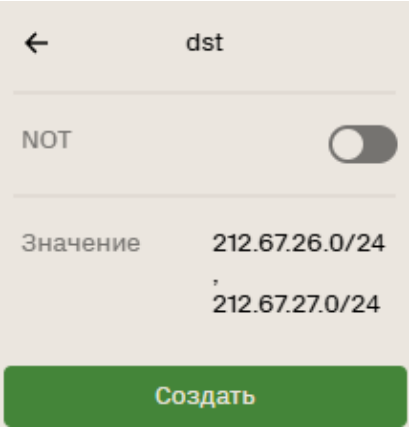
При выборе метрик необходимо указать дополнительный параметр:

Параметр	Описание
Avg	Среднее значение
Max	Максимальное значение
Percentile95	95-й перцентиль
Percentile99	99-й перцентиль
Total	Общее значение

Допустимо выбрать несколько параметров. Параметр **Total** установлен по умолчанию и не может быть отключён.

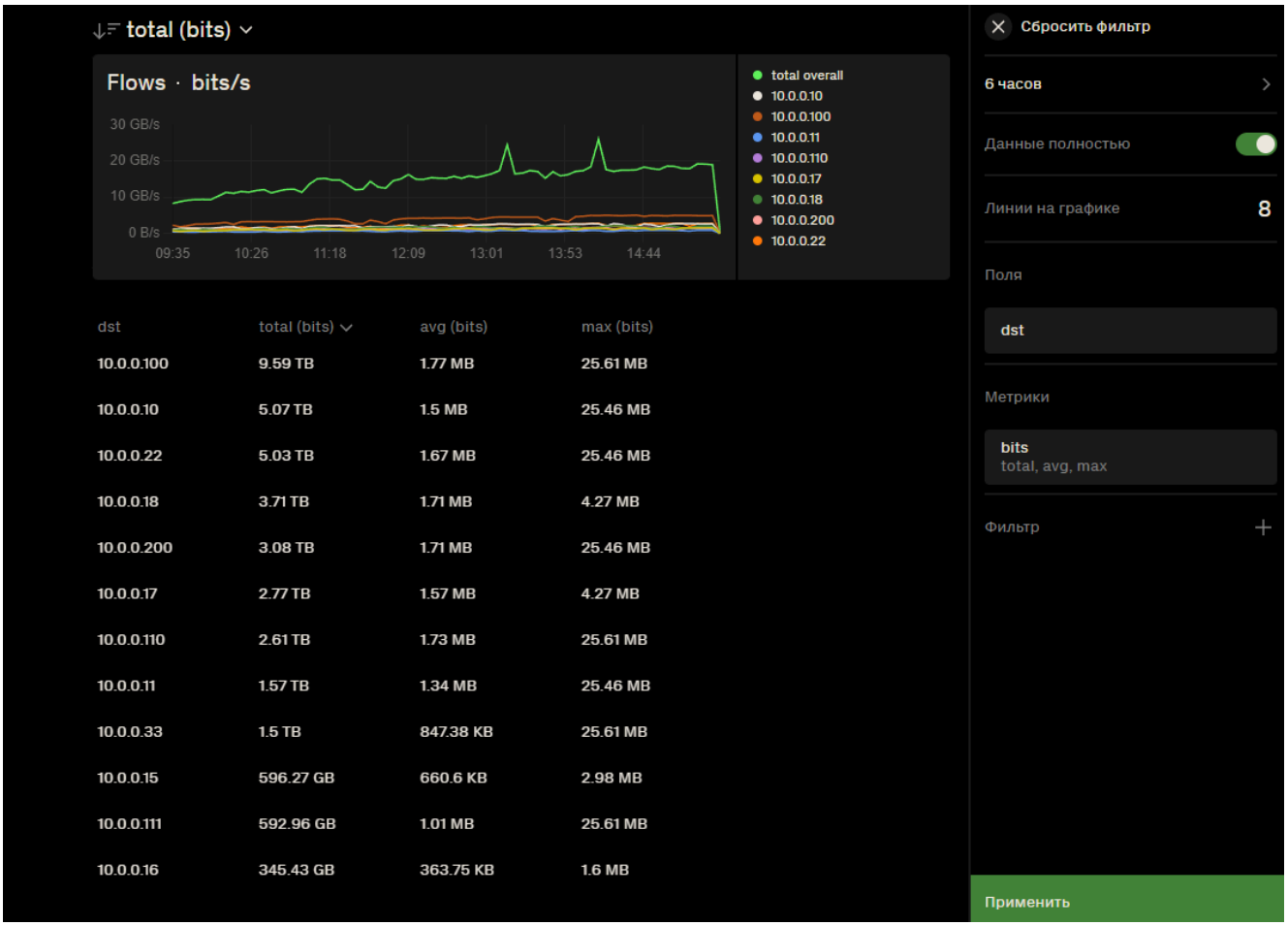
Фильтр

Результаты можно отфильтровать по выбранным атрибутам **Поля**.
При выборе параметра откроется меню, в котором нужно указать значения для фильтрации. Несколько значений можно указать через запятую без пробелов.
Переключатель «NOT» - является логическим операндом «НЕ», при его активации будут отображены все значения, кроме указанного.



После того как все необходимые параметры будут указаны, необходимо нажать зелёную кнопку **Применить**.

В результате на рабочей области появится график и таблица с данными:



На графике представлено количество переданных бит данных в течение шести часов. Под графиком расположена таблица, в которой указаны IP-адрес назначения, общее количество переданных бит, среднее и максимально значение переданных данных.

Если в метрике было выбрано несколько параметров, то возможно переключаться между графиками выбирая нужный параметр.

При сортировке параметров в таблице под графиком также отображается график этого параметра.

По умолчанию на графике отображаются все значения атрибутов. Для отображения конкретного атрибута необходимо выбрать его в правой части интерфейса графика.