

Автоматическая установка FlowCollector на Astra Linux 1.8

В зависимости от выбранного варианта интеграции требования к аппаратной платформе, процессу установки и уровню производительности могут различаться. Рекомендуется следовать инструкции на всех этапах установки. В случае возникновения вопросов обращайтесь к поставщику программного обеспечения.

1. Аппаратные и программные требования

- **Операционная система:** Astra Linux 1.8 Использование других версий или дистрибутивов не гарантирует корректную работу ПО.
- **Процессор:** Intel Xeon, AMD EPYC, не менее 10 физических ядер.
- **Оперативная память:** не менее 8 ГБ
- **Дисковое пространство:** не менее 100 ГБ
- **Сетевые интерфейсы:**
 - Для режима зеркалирования (DPDK): минимум 2 физических интерфейса:
 - Управляющий интерфейс
 - Интерфейс для обработки трафика (должен [поддерживаться DPDK](#)). Интерфейс резервируется полностью для FlowCollector, его использование для других целей невозможно.
 - Для режима NetFlow: минимум 1 сетевой интерфейс.
- **Рекомендуемые сетевые адаптеры:** Mellanox (mlx5 или mlx6), Intel X520-DA2
- **Права пользователя:** Требуется пользователь с правами *sudo* для запуска установочных скриптов.

1.1. Выбор и подготовка режима интеграции

Режим зеркалирования (Port Mirror, DPDK)

- Рекомендуется для производительных конфигураций и скоростей обработки выше 30 Gbps.

- Требуется выделения отдельного физического интерфейса для обработки трафика (режим DPDK).
- На сетевом оборудовании необходимо настроить зеркалирование трафика (port-mirror) с использованием GRE-туннеля и необходимого коэффициента (например, 1:1000).
- После настройки зеркалирования интерфейс будет полностью использоваться FlowCollector.

Пример настройки зеркалирования трафика

```
# Port mirroring
port-mirroring
mirror-once;
input {
    rate 1000;
    run-length 0;
}

instance {
    flowcollector {
        input {
            rate 250;
            run-length 0;
        }
        family inet {
            output {
                interface gr-0/0/0.15 {
                    next-hop 172.20.5.2;
                }
            }
        }
    }
}

gr-0/0/0.15
description --Tunnel-to-flowcollector;
tunnel {
    source IP;
    destination IP;
}
family inet {
    address 172.20.5.1/30;
}

firewall filter flowcollector-input

term default {
    then {
        port-mirror-instance flowcollector;
        accept;
    }
}
```

```
ae0.2020
description UPSTREAM;
vlan-id 2020;
family inet {
    filter {
        input flowcollector-input;
    }
    sampling {
        input;
    }
    address 10.12.0.2/30;
}
```

Режим потоковых данных

Используется для семплирования трафика. Поддерживает несколько потоковых протоколов:

- **NetFlow v10 (IPFIX)**
- **NetFlow v9**
- **sFlow**
- **IMON**

Для работы потока настройте семплирование пакетов и направьте их на выделенный сетевой интерфейс FlowCollector.

1.2. Подготовка сетевого оборудования

Для режима DPDK:

- Настройте зеркалирование пакетов на уровне сетевого оборудования в сторону выделенного интерфейса.
- Проверьте, что драйвер выбранного сетевого адаптера поддерживается DPDK.

Для режима потоковых данных:

- Настройте отправку семплированных пакетов на соответствующий сетевой интерфейс.

1.3. Подготовка аппаратной платформы

- Установите рекомендованную для запуска ОС: Astra Linux 1.8
**В случае использования других ОС - успешный запуск ПО не гарантирован*
- Используйте рекомендованные CPU: Intel Xeon, AMD EPYC, не менее 10 физических ядер. **В случае использования CPU сторонних производителей - успешный запуск ПО не гарантирован*
- Используйте рекомендованные сетевые карты: Mellanox (mlx5 или mlx6) или Intel (X520-DA2)

2. Установка FlowCollector с помощью скрипта

2.1 Выполнение скрипта установки

Скрипт выполняет подключение репозитория Servicepipe, установку FlowCollector и первоначальное конфигурирование системы.

Для запуска необходимо выполнить команду:

```
curl -o "./setup-fc.sh" "https://public-repo.svcv.io/setup_script/setup-fc.sh" && \
  sudo chmod +x "./setup-fc.sh" && \
  ./setup-fc.sh
```

Перед началом установки выполняется автоматическая проверка системных требований. При обнаружении несоответствия минимально необходимым параметрам отобразится предупреждение:

```
test@ubuntu-test:~$ curl -o "./setup-fc.sh" "https://public-repo.svcv.io/setup_script/setup-fc.sh" && \
  sudo chmod +x "./setup-fc.sh" && \
  ./setup-fc.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 34061  100 34061    0     0  43792      0 --:--:-- --:--:-- --:--:-- 43836
[sudo] password for test:
FlowCollector installation script
=== Проверка версии ОС ===
Ubuntu 22.04. OK
=== Проверка системных требований ===
Количество ядер CPU: 12
Оперативная память: 15 ГБ
=== Проверка наличия утилиты уq ===
уq не найден в /home/test. В случае отсутствия утилиты, внесение изменений в YAML конфигурационные файлы будет пропущено.
Загрузить уq? [Y/n]:
```

2.2 Подключение репозитория

После запуска скрипта выполняется проверка наличия репозитория Servicepipe:

```
100 34061 100 34061 0 0 43792 0 --:--:-- --:--:-- --:--:-- 43836
[sudo] password for test:
FlowCollector installation script
=== Проверка версии ОС ===
Ubuntu 22.04. OK
=== Проверка системных требований ===
Количество ядер CPU: 12
Оперативная память: 15 GB
=== Проверка наличия утилиты uq ===
uq не найден в /home/test. В случае отсутствия утилиты, внесение изменений в YAML конфигурационные файлы будет пропущено.
Загрузить uq? [Y/n]: y
Загружаем uq...
uq успешно загружен в /home/test
=== Проверка наличия подключенного репозитория https://public-repo.svcpr.io/ ===
Репозиторий https://public-repo.svcpr.io/ не подключен.
Выполнить подключение? (Y/n):
```

Для подключения требуется ввести логин и пароль к репозиторию. Учетные данные предоставляются индивидуально для каждого заказчика. Получить их возможно запросив у вендора (Servicepipe или партнёра).

2.3 Выбор конфигурации для установки

После подключения репозитория скрипт предложит выбрать конфигурацию FlowCollector.

Установка включает четыре компонента:

- **FlowCollector** — основной пакет FlowCollector.
- **Spider** — веб-интерфейс.
- **Пакет мониторинга** — компоненты для сбора и отображения данных мониторинга.
- **Grafana** — система визуализации данных мониторинга.

Укажите необходимый вариант и подтвердите установку.

```
## Done

## Servicepipe ubuntu repository installed.

=== Установка пакетов ===
Установить FlowCollector? (y/n): y
Установить spider? (y/n): y
Установить пакет мониторинга? (y/n): y
Установить Grafana? (y/n): y
Будут установлены: flowcollector-only flowcollector-additional spider-only flowcollector-monitoring grafana-enterprise
Hit:1 http://ru.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 https://public-repo.svcpr.io/ubuntu xenial InRelease
Get:4 http://ru.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
0% [Waiting for headers]
```

Внимание:

В процессе установки, в зависимости от выбранной конфигурации, может

потребуется указать учетные данные (логины и пароли) для доступа к базам данных и брокерам сообщений. Эти данные необходимо сохранить, так как они используются при последующем конфигурировании системы.

2.4 Первичная настройка системы

В зависимости от выбранной конфигурации после установки пакетов выполняется первоначальная настройка компонентов.

Сначала выполняется установка ClickHouse. Задайте пароль для пользователя *default*.

```
Config file /etc/clickhouse-server/config.xml already exists, will keep it and extract path info from it.
/etc/clickhouse-server/config.xml has /var/lib/clickhouse/ as data path.
/etc/clickhouse-server/config.xml has /var/log/clickhouse-server/ as log path.
Users config file /etc/clickhouse-server/users.xml already exists, will keep it and extract users info from it.
Creating log directory /var/log/clickhouse-server/.
Data directory /var/lib/clickhouse/ already exists.
Creating pid directory /var/run/clickhouse-server.
chown -R clickhouse:clickhouse '/var/log/clickhouse-server/'
chown -R clickhouse:clickhouse '/var/run/clickhouse-server'
chown clickhouse:clickhouse '/var/lib/clickhouse/'
groupadd -r clickhouse-bridge
useradd -r --shell /bin/false --home-dir /nonexistent -g clickhouse-bridge clickhouse-bridge
chown -R clickhouse-bridge:clickhouse-bridge '/usr/bin/clickhouse-odbc-bridge'
chown -R clickhouse-bridge:clickhouse-bridge '/usr/bin/clickhouse-library-bridge'
Enter password for default user: 
Progress: [ 64%] [#####]
```

После установки, скрипт рассчитывает количество HugePages, выполняет инициализацию ClickHouse и предлагает указать имя пользователя и пароль.

```
=== Рассчитываем hugepages ===
Объем RAM: 15609 MB
NUMA-нод: 1
Рассчитанное количество hugepages: 7804
Файл /opt/spfc/bin/create_hugepages.sh обновлен.

=== Инициализация ClickHouse ===
Synchronizing state of clickhouse-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clickhouse-server
Файл /usr/share/doc/clickhouse-server/graphite/fc-init.sql найден. Выполняем инициализацию ClickHouse...
Введите пользователя ClickHouse (по умолчанию 'default'): 
```

Укажите имя создаваемой базы данных MongoDB, имя пользователя и пароль.

```
=== Инициализация MongoDB ===
Created symlink /etc/systemd/system/multi-user.target.wants/mongod.service → /lib/systemd/system/mongod.service.
Введите имя создаваемой базы данных MongoDB (по умолчанию 'events'): events
Введите имя создаваемого пользователя MongoDB (по умолчанию 'events'): events
Введите пароль создаваемого пользователя MongoDB: password
```

Укажите имя базы данных PostgreSQL, имя пользователя и пароль.

```
=== Инициализация PostgreSQL ===
Failed to enable unit: Unit file postgres.service does not exist.
Введите имя базы данных (по умолчанию spider):
Введите имя пользователя PostgreSQL (по умолчанию spider):
Введите пароль пользователя PostgreSQL: password
```

```
Создаём базу и пользователя PostgreSQL...
CREATE DATABASE
CREATE ROLE
GRANT
Инициализация PostgreSQL завершена.
Postgre host: localhost
Postgre username: spider
Postgre password: password
Postgre db: spider
```

Далее выполняется инициализация NATS.

```
=== Инициализация NATS ===
Created symlink /etc/systemd/system/multi-user.target.wants/nats-server.service → /etc/systemd/system/nats-server.service
Stream analyzer was created

Information for Stream analyzer created 2025-10-20 12:35:15

    Subjects: analyzer.notification
    Replicas: 1
    Storage: File

Options:

    Retention: Interest
    Acknowledgments: true
    Discard Policy: Old
    Duplicate Window: 2m0s
```

После создания и включения необходимых системных сервисов выполняется переход к первоначальной настройке SP-Spider.

```
Created symlink /etc/systemd/system/multi-user.target.wants/analyzer.service → /opt/spfc/lib/systemd/system/analyzer.service
Created symlink /etc/systemd/system/analyzer.service → /opt/spfc/lib/systemd/system/analyzer.service.
Created symlink /etc/systemd/system/multi-user.target.wants/gobgpd.service → /lib/systemd/system/gobgpd.service.

=== Конфигурация carbon-clickhouse, graphite-clickhouse, carbonapi ===
Created symlink /etc/systemd/system/multi-user.target.wants/carbon-clickhouse.service → /lib/systemd/system/carbon-clickhouse.service
Created symlink /etc/systemd/system/multi-user.target.wants/graphite-clickhouse.service → /lib/systemd/system/graphite-clickhouse.service
Created symlink /etc/systemd/system/multi-user.target.wants/carbonapi.service → /etc/systemd/system/carbonapi.service.

1
Файл /etc/carbon-clickhouse/carbon-clickhouse.conf обновлен.
Выполняем перезапуск Carbon-clickhouse
Файл /etc/graphite-clickhouse/graphite-clickhouse.conf обновлен.
Выполняем перезапуск graphite-clickhouse
Created symlink /etc/systemd/system/multi-user.target.wants/sp-spider.service → /lib/systemd/system/sp-spider.service.
Выполнить конфигурацию SP-Spider? (y/n):
```

При настройке SP-Spider используются ранее заданные параметры подключения к PostgreSQL. Затем предлагается создать системного пользователя для веб-интерфейса.

```
=== Создание системного пользователя ===
Введите имя пользователя для веб-интерфейса (по умолчанию dosgate-web):
```

На завершающем этапе выполняется настройка Grafana. Укажите имя базы данных PostgreSQL, имя пользователя и пароль.

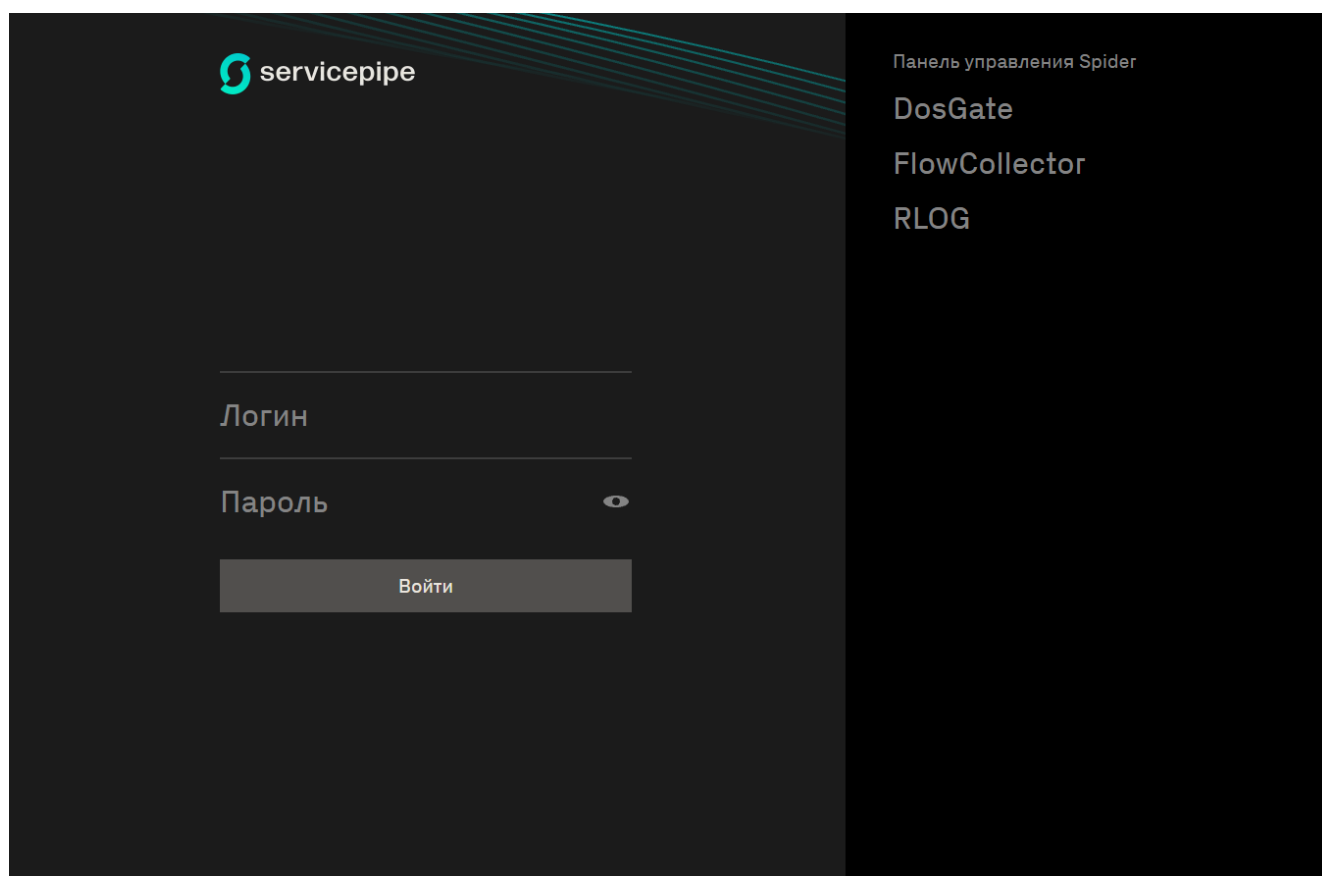
```
Выполнить конфигурацию Grafana? (y/n): y

=== Выполняем конфигурацию Grafana ===
Данные для подключения к PostgreSQL
Введите имя базы данных (по умолчанию grafana):
Введите имя пользователя PostgreSQL (по умолчанию grafana):
Введите пароль пользователя PostgreSQL: password
```

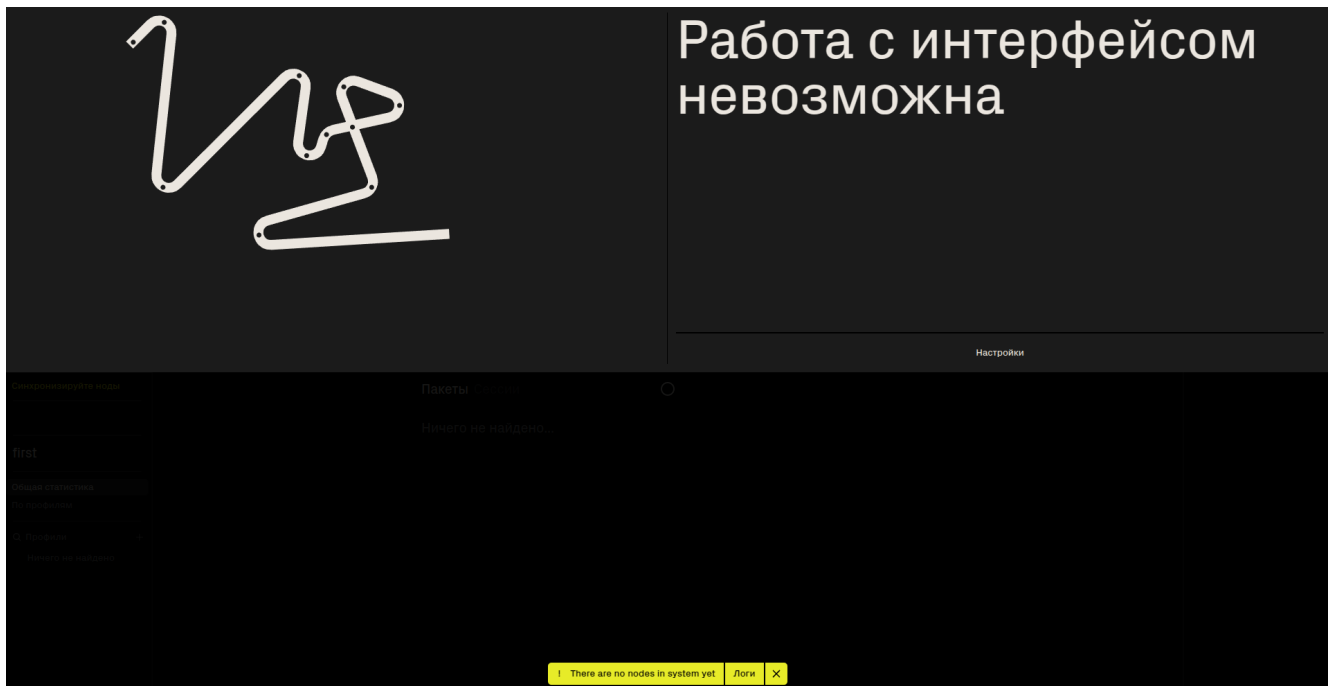
3. Первый вход в систему

Для входа в Веб-интерфейс FlowCollector следует ввести в адресной строке браузера IP-адрес сервера и порт по шаблону: `ip:3333`.

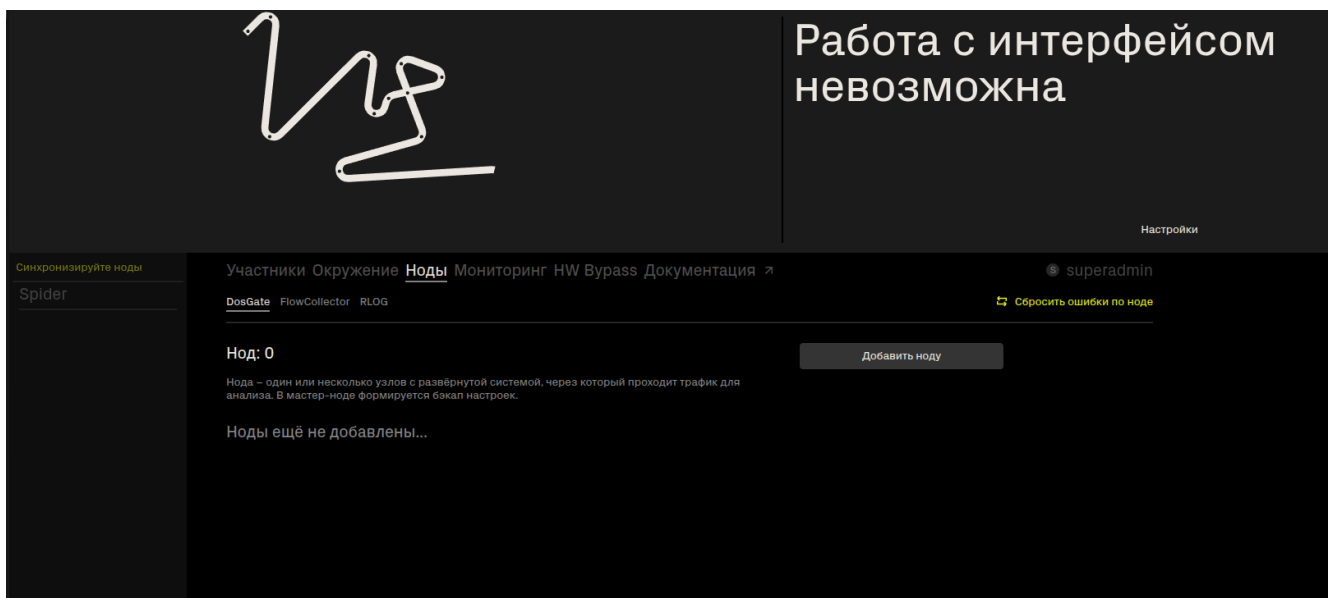
Появится окно авторизации (см. рисунок ниже). В окне авторизации следует указать следующие логин и пароль по умолчанию: ***superadmin/superadmin***



После авторизации появится уведомление **Работа с интерфейсом невозможна**. Это связано с тем, что в данный момент нет настроенной ноды.



Нажать кнопку **Настройки**. Откроется окно настроек.



В меню **Ноды** нажать на **Добавить ноду**. В открывшемся окне указать:

- **Оп.система** — Ubuntu 18+
- **Модуль** — FlowCollector
- **Metrics host** — flowcollector

Добавить ноду

Оп.система

Ubuntu 18+ ▾

Модуль

FlowCollector ▾

Metrics host

flowcollector

MongoDB

>

ClickHouse

>

Подключение

>

Добавить ноду

Перейти в настройки **MongoDB** и указать параметры подключения:

←

MongoDB

Хост

127.0.0.1

Порт

27017

База данных

events

Пользователь

events

Пароль

••••••••

Применить

Нажать на кнопку **Применить**. Перейти в раздел **ClickHouse**.

← ClickHouse

Хост 127.0.0.1

Порт 8123

База данных default

Пользователь default

Пароль

Применить

Нажать на кнопку **Применить**. Перейти в раздел **Подключение**.

← Подключение

API Crash Dump /logcollector

SSH

IP-адрес 127.0.0.1

Порт 22

Логин root

🔑

Доступность Проверить

Применить

В открывшемся окне указать SSH-данные для подключения к ноде FlowCollector (IP-адрес, логин, пароль). Нажмите **Проверить**, чтобы проверить подключение. Если данные указаны верно и нода доступна, её статус изменится на **Доступна**. После успешной проверки нажмите **Применить**. В открывшемся окне нажать **Добавить ноду**.

Для отображения графиков и статистики необходимо указать ссылку на Graphite. Перейдите в раздел **Окружение**. В разделе FlowCollector указать **Graphite URL**.

FlowCollector

Graphite URL	http://127.0.0.1:8088	
Обновление графиков ?	60	сек
Обновление аномалий ?	10	сек
Интервал захвата ?	10	сек

Нажать на профиль в правом верхнем углу экрана и в открывшихся настройках установить новый пароль.

Участники Окружение Ноды Мониторинг HW Bypass Обучение Ещё Документация ↗ **superadmin**



Выйти из аккаунта

Логин superadmin

Роль

Создан

Пароль [Изменить](#)

Язык Русский ▾

Уведомления ☒

API-токен ?

↻ Пересоздать

Обновить страницу. Веб-интерфейс готов к использованию.

4. Настройка конфигурации FlowCollector

Конфигурация разделена на логические блоки для удобства восприятия.

Внимание!

- Перед началом работы рекомендуется изучить комментарии к каждому параметру.
- Для режима DPDK необходимо раскомментировать секцию [dpdk-nic](#).
- Для режима потоковых данных необходимо раскомментировать секцию [Потоки](#).

Открыть файл конфигурации для редактирования:

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

4.1 Параметры логирования

```
log:
  level: debug                                # Уровень логирования: trace, debug, info,
warn/warning, error, fatal
```

Примечание

Уровни логирования *trace* и *debug* могут быть отключены в определённых типах сборки.

4.2 Привязка логических ядер

Секция [lcore-mapping](#) определяет распределение логических ядер между процессами FlowCollector. Если секция не задана, используется автоматическое распределение.

Доступны режимы:

- [auto](#) — автоматическое распределение с указанием количества логических ядер для каждой активности;
- [manual](#) — ручное распределение с указанием количества логических ядер для каждой активности;
- [corebound](#) — привязка активностей к конкретным идентификаторам логических ядер.

Для параметра [dpdk-ix](#) рекомендуется указывать количество ядер, равное степени 2.

<code># lcore-mapping:</code>	
<code># mode: auto</code>	<code># Режим привязки: auto, manual, corebound.</code> <code># Опционально. По умолчанию – auto</code>
 <code># schema:</code>	
<code># auto:</code>	<code># Количество логических ядер для каждой</code>
активности	
<code># detection: 4</code>	<code># Обнаружение аномалий</code>
<code># event-processing: 2</code>	<code># Обработка событий</code>
<code># metrics: 2</code>	<code># Обработка метрик</code>
<code># dpdk-rx: 1</code>	<code># Приём трафика DPDK</code>
<code># dpdk-worker: 4</code>	<code># Обработка трафика DPDK</code>
<code># flow-rx: 1</code>	<code># Приём потоков</code>
<code># flow-worker: 2</code>	<code># Обработка потоков</code>
<code># reports: 2</code>	<code># Формирование отчётов</code>
<code># free: 2</code>	<code># Свободные логические ядра</code>
 <code># manual:</code>	<code># Количество логических ядер для каждой</code>
активности	
<code># detection: 4</code>	<code># Обнаружение аномалий</code>
<code># event-processing: 2</code>	<code># Обработка событий</code>
<code># metrics: 2</code>	<code># Обработка метрик</code>
<code># dpdk-rx: 1</code>	<code># Приём трафика DPDK</code>
<code># dpdk-worker: 4</code>	<code># Обработка трафика DPDK</code>
<code># flow-rx: 1</code>	<code># Приём потоков</code>
<code># flow-worker: 2</code>	<code># Обработка потоков</code>
<code># reports: 2</code>	<code># Формирование отчётов</code>
<code># free: 2</code>	<code># Свободные логические ядра</code>
 <code># corebound:</code>	<code># Привязка активностей к конкретным</code>
идентификаторам	
до N-1	<code># логических ядер. Используются номера от 1</code>
<code># detection: 1-4</code>	<code># Логические ядра для обнаружения аномалий</code>
<code># event-processing: 5,6</code>	<code># Логические ядра для обработки событий</code>
<code># metrics: 7,8</code>	<code># Логические ядра для обработки метрик</code>
<code># dpdk-rx: 9</code>	<code># Логические ядра для приёма трафика DPDK</code>
<code># flow-rx: 14</code>	<code># Логические ядра для приёма потоков</code>
<code># worker: 10,11,12,13,15,16</code>	<code># Логические ядра для обработки данных</code>
<code># reports: 17,18</code>	<code># Логические ядра для формирования отчётов</code>
<code># free: 20-22,23</code>	<code># Свободные логические ядра</code>

4.3 Параметры обнаружения

Параметры обнаружения аномалий задаются в секции `detections`.

<code>detections:</code>	
<code># enable: true</code>	<code># Включение обнаружения. По умолчанию –</code>
<code>true</code>	

<code># average-period: 5000ms</code>	<code>#</code> Период для расчёта текущей скорости. По умолчанию — 5000ms
<code># interval: 5000ms</code>	<code>#</code> Интервал пересчёта текущей скорости. По умолчанию — 5000ms
<code># min-destination-ip: 10</code>	<code>#</code> Минимальное количество IP-адресов назначения под атакой
<code>global.</code>	<code>#</code> в управляемом объекте для правил типа
<code># min-destination-ip-subnet: 10</code>	<code>#</code> Минимальное количество IP-адресов назначения под атакой
<code>умолчанию — 0</code>	<code>#</code> в подсети для правил типа subnet. По умолчанию — 0
<code># confirm-period: 0</code>	<code>#</code> Период подтверждения аномалии. По умолчанию — 0 секунд
<code># action-expiry-timeout: 60</code>	<code>#</code> Время продолжения действия после исчезновения аномалии.
	<code>#</code> По умолчанию — 60 секунд

Для параметров длительности можно использовать единицы `ns`, `us`, `ms`, `s`, `m`, `h`, `d`.

4.4 Параметры метрик

<code>metrics:</code>	
<code>enable: false</code>	<code>#</code> Включение сбора метрик. По умолчанию — false
<code># disable-vector-metrics: false</code>	<code>#</code> Отключение метрик векторов атак для MO, subnet и IP.
	<code>#</code> По умолчанию — false
<code>collectd:</code>	
<code>endpoint: unix:///var/run/collectd-unixsock</code>	<code>#</code> Точка подключения collectd
<code># carbon:</code>	
<code># endpoint: 127.0.0.1:2003</code>	<code>#</code> Точка подключения Carbon
<code>hostname: analyzer-test</code>	<code>#</code> Первый ключ имени метрики
<code>plugin: analyzer</code>	<code>#</code> Второй ключ имени метрики
<code>export-timeout: 5</code>	<code>#</code> Период отправки метрик. По умолчанию — 5 секунд
<code># buffer-size: 50000</code>	<code>#</code> Количество буферов по 4096 байт.
	<code>#</code> По умолчанию — 25000

4.5 Настройки BGP и GoBGP

GoBGP и FlowSpec

```
gobgp:
  enable: false           # Включение GoBGP. По умолчанию – false
  host: localhost         # Хост API GoBGP. По умолчанию – localhost
  port: 50051             # Порт API GoBGP. По умолчанию – 50051
  # thread-number: 1      # Количество потоков API GoBGP. По
  умолчанию – 1
  enable-subnet-splitting: false # Включение разделения CIDR на подсети
  min-subnet-length: 16     # Длина маски для разделения. По умолчанию
  – 16
  enable-flow-spec: false   # Включение FlowSpec
  max-rules-number: 100     # Максимальное количество правил FlowSpec.
  # По умолчанию – 100
  drop-on-restart: true     # Удаление существующих маршрутов и правил
  FlowSpec
  # в GoBGP при перезапуске. По умолчанию –
  true
```

Если значение `min-subnet-length` меньше или равно длине маски CIDR, разделение на подсети не выполняется.

4.6 Аргументы DPDK EAL

```
dpdk-args:                # По умолчанию значение не задано

# --vdev=net_pcap0,rx_iface_in=eth0  # Пример использования сетевого
интерфейса в режиме PCAP:

# --vdev=net_af_packet0,iface=tap0,framecnt=512,qpairs=1 --in-memory --no-pci
# Пример использования сетевого интерфейса с dpdk-testpmd:

# -a <port>                # Пример использования сетевого
интерфейса:
```

4.7 Параметры HTTP API FlowCollector

```
http-api:
  enable: false           # Включение HTTP API. По умолчанию – false
  # endpoint:             # Локальные точки подключения
  #   - unix://path/to/socket
```

```
# - inet://127.0.0.1:8082
# - 127.0.0.1
```

4.8 Параметры FIB

Секция `fib` определяет параметры таблиц маршрутизации для IPv4 и IPv6.

```
# fib:
#   v4:
#     max-routes: 65535          # Максимальное количество маршрутов. По
#                               # умолчанию — 65535
#     table8: 1024              # Количество групп tbl8. По умолчанию —
#                               # 1024
#   v6:
#     max-routes: 65535          # Максимальное количество маршрутов. По
#                               # умолчанию — 65535
#     table8: 1024              # Количество групп tbl8. По умолчанию —
#                               # 1024
```

4.9 Источники трафика

DPDK NIC

```
dppdk-nic:
  enable: true                  # Включение DPDK NIC. true — включено,
                                # false — выключено.
                                # По умолчанию — true

  # rate: 1                     # Коэффициент выборки. Каждый `rate`-й
  пакет отправляется          # в FlowCollector. Реальное количество
                                # пакетов рассчитывается
                                # как количество полученных пакетов × rate.
                                # По умолчанию — 1

  # enable-eth-ports: 0xff      # Маска включённых Ethernet-портов.
                                # Опционально. По умолчанию — max(uint64)

  # port-rx-queue-number: 1     # Количество очередей Rx на сетевой
  интерфейс.                  # Опционально. По умолчанию — 1

  # throttling-rate: 1          # Коэффициент регулирования (1:throttling-
  rate).                       # Опционально. По умолчанию — 1
```

```
# mtu: 9000
значение драйвера,
```

```
# packet-pool:
#   size: 8191
#   cache-size: 128
```

```
# arp:
#   enable: false
выключено.
```

```
#   devices:
умолчанию не задан.
```

```
default-ip, используется значение default-ip.
```

```
devices, ни default-ip, возникает ошибка
```

```
#   -
#       mac: 00:00:00:00:00:00
#       ip:
#       - 127.0.0.1
#       - 192.168.0.0
```

```
#   default-ip: 127.0.0.1
анализатор.
```

```
# sources:
сопоставления с группами
```

```
#   -
#       group: all
автоматически сгенерированный идентификатор группы
```

```
#   disable: false
```

```
#   local:
{} означает любую
#       host: 192.168.0.1
любой
```

```
#   remote:
{} означает любую
#       host: 192.168.0.2
любой
```

```
# MTU Ethernet-портов DPDK.
# Опционально. По умолчанию используется
# обычно 1500
```

```
# Параметры пула пакетов DPDK
# Размер пула. По умолчанию – (64*1024)-1
# Размер кэша. По умолчанию – 128
```

```
# Параметры ARP
# Включение ARP. true – включено, false –
# По умолчанию – false
```

```
# Список устройств для обработки. По
# Если указаны одновременно devices и
```

```
# Если ARP включён, но не заданы ни
```

```
#   -
#       mac: 00:00:00:00:00:00 # MAC-адрес устройства
#       ip:                     # Список IP-адресов устройства
```

```
# IP-адрес машины, на которой работает
# По умолчанию – 127.0.0.1
```

```
# Список источников трафика DPDK для
```

```
#   group: all
# Имя группы. Если не указано, используется
```

```
# Отключение обработки источника.
# Если не указано, используется false
```

```
# Локальная точка. Пустое значение local:
```

```
# IP-адрес. Если не указан, используется
```

```
# Удалённая точка. Пустое значение remote:
```

```
# IP-адрес. Если не указан, используется
```

Если параметры `local` и `remote` не заданы, используется сырое зеркалирование трафика.

Потоки

Секция `flow` определяет параметры приёма потоков IPFIX, NetFlow v9, sFlow и IMon.

```
flow:
  enable: false          # Включение обработки потоков. true –
                          # включено, false – выключено.
                          # По умолчанию – false

  # memory-pool:         # Параметры пула памяти для сообщений о
  # потоках
  #   number: 16383      # Размер пула. По умолчанию – 1024*64-1
  #   cache-size: 128    # Размер кэша. По умолчанию – 128
```

IPFIX

```
flow:
  ipfix:
    enable: false        # Включение IPFIX. true – включено, false –
                          # выключено.
                          # По умолчанию – false

    # rate: 1            # Коэффициент выборки. Каждый `rate`-й
    # пакет отправляется
    # в FlowCollector. Реальное количество
    # пакетов рассчитывается
    # как количество полученных пакетов × rate.
    # По умолчанию – 1

    endpoint:            # Локальные точки подключения для приёма
    # сообщений IPFIX
    #   - udp://127.0.0.1:4739
    #   - tcp://192.168.0.1:4739

    # sources:           # Список источников трафика IPFIX для
    # сопоставления с группами
    #   -
    #   group: all        # Имя группы. Если не указано, используется
    # автоматически
    #   protocol: tcp     # сгенерированный идентификатор группы
    # Протокол. Доступные значения: udp, tcp.
    # Если не указан, используется любой

    # ifIndex: 12        # Индекс входного интерфейса.
    # Если не указан, используется любой
```

интерфейс	#	disable: false	# Отключение обработки источника.
			# Если не указано, используется false
	#	local:	# Локальная точка. Пустое значение local:
{}	означает любую		
	#	host: 192.168.0.1	# IP-адрес. Если не указан, используется
любой			
	#	port: 20000	# Порт. Если не указан, используется любой
	#	remote:	# Удалённая точка. Пустое значение remote:
{}	означает любую		
	#	host: 192.168.0.2	# IP-адрес. Если не указан, используется
любой			
	#	port: 30000	# Порт. Если не указан, используется любой

NetFlow v9

flow:		
netflow9:		
enable: false		# Включение NetFlow v9. true – включено,
false – выключено.		# По умолчанию – false
# rate: 1		# Коэффициент выборки. Каждый `rate`-й
пакет отправляется		# в FlowCollector. Реальное количество
		# как количество полученных пакетов × rate.
пакетов рассчитывается		# По умолчанию – 1
endpoint:		# Локальные точки подключения для приёма
сообщений NetFlow v9		
- 127.0.0.1:2055		
# sources:		# Список источников трафика NetFlow v9 для
сопоставления с группами		
# -		
# group: all		# Имя группы. Если не указано, используется
автоматически		
		# сгенерированный идентификатор группы
# protocol: tcp		# Протокол. Доступные значения: udp, tcp.
		# Если не указан, используется любой
протокол		
# local:		# Локальная точка. Пустое значение local:
{}	означает любую	
	#	host: 192.168.0.1
любой		# IP-адрес. Если не указан, используется
	#	port: 20000
	#	remote:
{}	означает любую	
	#	host: 192.168.0.2
		# IP-адрес. Если не указан, используется

```
# port: 30000 # Порт. Если не указан, используется любой
```

sFlow

```

flow:
  sflow:
    enable: false
    endpoint:
      - 127.0.0.1:6343
      # - 192.168.0.1:6343

    # sources:
    #   group: all
    #   ifIndex: 12

    # disable: false
    # local:
    {}
    # host: 192.168.0.1
    # port: 20000
    # remote:
    {}
    # host: 192.168.0.2
    # port: 30000

```

Включение sFlow. true – включено, false –
По умолчанию – false
Локальные точки подключения для приёма
сообщений sFlow
- 127.0.0.1:6343
- 192.168.0.1:6343
sources:
сопоставления с группами
-
group: all
автоматически
ifIndex: 12
интерфейс
disable: false
local:
{ } означает любую
host: 192.168.0.1
любой
port: 20000
remote:
{ } означает любую
host: 192.168.0.2
любой
port: 30000

Включение sFlow. true – включено, false –
По умолчанию – false
Локальные точки подключения для приёма
сообщений sFlow
- 127.0.0.1:6343
- 192.168.0.1:6343
sources:
Список источников трафика sFlow для
сопоставления с группами
-
group: all
Имя группы. Если не указано, используется
сгенерированный идентификатор группы
ifIndex: 12
Индекс входного интерфейса.
Если не указан, используется любой
Отключение обработки источника.
Если не указано, используется false
local:
Локальная точка. Пустое значение local:
{ } означает любую
host: 192.168.0.1
IP-адрес. Если не указан, используется
любой
port: 20000
Порт. Если не указан, используется любой
remote:
Удалённая точка. Пустое значение remote:
{ } означает любую
host: 192.168.0.2
IP-адрес. Если не указан, используется
любой
port: 30000
Порт. Если не указан, используется любой

IMon

```
flow:  
    imon:  
        enable: false           # Включение IMon. true – включено, false –  
                                ВЫКЛЮЧЕНО.  
  
        endpoint:               # Локальные точки подключения для приёма  
                                сообщений IMon  
            - 127.0.0.1:2055
```

```

# - 192.168.0.1:6343

# sources:
сопоставления с группами
# -
# group: all
автоматически

# ifIndex: 12

интерфейс
# disable: false

# local:
{} означает любую
# host: 192.168.0.1
любой
# port: 20000
# remote:
{} означает любую
# host: 192.168.0.2
любой
# port: 30000

# Список источников трафика IMon для
# Имя группы. Если не указано, используется
# сгенерированный идентификатор группы
# Индекс входного интерфейса.
# Если не указан, используется любой
# Отключение обработки источника.
# Если не указано, используется false
# Локальная точка. Пустое значение local:
# IP-адрес. Если не указан, используется
# Порт. Если не указан, используется любой
# Удалённая точка. Пустое значение remote:
# IP-адрес. Если не указан, используется
# Порт. Если не указан, используется любой

```

4.10 Анонсы и действия

BGP-анонсы

```

announce:
  enable: false
# Включение отправки BGP-анонсов

nexthops:
  - name: transit
    ip: 192.168.10.1
# Имя next-hop
# IP-адрес next-hop

  - name: blackhole
    ip: 192.168.20.1

# communities: 666
# communities:
# - 666:666
# - 777:777

timeout: 20
# Период отправки анонсов для нативного BGP

```

Для BGP communities поддерживаются следующие форматы:

```
<целое_число>: <целое_число>  
<целое_число>  
0x<шестнадцатеричное_число>
```

Глобальное действие

Глобальное действие применяется при обнаружении аномалии, если для соответствующего правила не задано отдельное действие.

```
action:  
  nexthop: transit # IP-адрес next-hop или его имя из  
announce.nexthops  
  
# communities: 666:666  
# communities:  
#   - 666:666  
#   - 777:777
```

Вычитание трафика local и subnet аномалий

```
subtract-local-subnet-traffic: true # По умолчанию – true.
```

Если параметр имеет значение `true`, трафик, вызвавший аномалию уровня `local` или `subnet`, вычитается из скорости соответствующих счетчиков `subnet` и `global` объекта.

4.11 Отправка событий

Notification Service

```
notification-service:  
  enable: false # Включение отправки событий. По умолчанию  
- false  
  
http:  
  enable: false # Включение отправки событий по HTTP  
  host: localhost # Хост удалённого сервиса  
  # port: 8081 # Порт. По умолчанию – 8081  
  # path: / # Путь
```

```
nats:
  enable: false           # Включение отправки событий через NATS
  host: localhost         # Хост NATS
  # port: 4222            # Порт. По умолчанию — 4222
  # path: /
  # subject: analyzer.notification # Subject потока
  # persistence: true     # Сохранение сообщений. По умолчанию — true
```

Аннотации Graphite

```
graphite-annotations:
  enable: false           # Включение отправки событий как аннотаций
Graphite
  host: localhost         # Хост удалённого сервиса
  # port: 80              # Порт. По умолчанию — 80
  # path: /events         # Путь
```

4.12 Параметры IpLookupTable

```
ip-lookup-table:
  mode: overlap           # Режим отслеживания CIDR
```

Значение `overlap` разрешает перекрывающиеся подсети в разных управляемых объектах, `nooverlap` — запрещает.

4.13 Параметры отчётов

```

reports:
  enable: false          # Включение формирования отчётов. По
                          умолчанию – false
  host: localhost        # Хост сервиса для экспорта отчётов
  # port: 9080           # Порт. По умолчанию – 9080
  path: /report          # Путь для экспорта отчётов
  # export-timeout: 20   # Период экспорта. По умолчанию – 20 секунд
  # max-src-addr: 10000  # Максимальное количество адресов источника
  # max-dst-addr: 10000  # Максимальное количество адресов
                          назначения
  # max-src-ports: 1000  # Максимальное количество портов источника
  # max-dst-ports: 1000  # Максимальное количество портов назначения

```

4.14 Хранение данных

PCAP-дампы

```

pcapng-dumper:
  enable: false          # Включение записи дампов. По умолчанию –
false
  # dumps-path: /var/dump/ # Путь для записи дампов
  max-sessions-number: 8  # Максимальное количество одновременных
сессий дампа
  max-packets-number: 10000 # Максимальное количество пакетов в одном
дампе
  keep-alive: 10         # Максимальное время без пакетов для
ручного дампа

```

Параметры FlowWriter

```

save-flow:
  enable: false           # Включение сохранения потоков
  enable-all-mo: true    # Сохранение потоков для всех МО
  enable-save-all: false # Сохранение всего полученного трафика
  table-name: "default.flows" # Имя таблицы для записи потоков.
  db-host: "localhost"    # Хост базы данных
  db-port: 9000           # Порт базы данных
  db-username: "default"  # Пользователь базы данных
  db-password: ""        # Пароль пользователя
  rollup-section: "flows_rollup" # Секция ClickHouse с правилами свёртки. По
умолчанию — flows_rollup
  save-records-number: 10000 # Количество записей потоков в одном блоке
  flush-records-timeout: 60  # Интервал сброса записей

```

4.15 Параметры SNMP

FlowCollector отслеживает интерфейсы следующих типов:

- `ethernet-csmacd(6)` ;
- `prop-virtual(53)` ;
- `tunnel(131)` .

```

snmp:
  enable: false           # Включение SNMP. По умолчанию — false

  agents:
    - peer: example.org:161 # Хост агента и, при необходимости, порт
      version: 1            # Версия SNMP: 1, 2с или 3
      request-timeout: 60s  # Частота запросов. По умолчанию — 60s
      response-timeout: 1s  # Таймаут ожидания ответа. По умолчанию —
1s
    # local-address: 192.168.0.1 # Локальный адрес для привязки.
    # local-port: 11111         # Локальный порт для привязки.
    community: public         # Community для SNMP v1 и v2c
    # security-name: secret    # Security name для SNMP v3
    # security-auth-key: secret-key # Ключ авторизации для для SNMP v3
    # alias: example          # Псевдоним для метрик

```

4.16 Сохранение данных SNMP

```

save-snmpp:
  enable: false           # Включение сохранения данных SNMP
  table-name: "default.snmpp" # Имя таблицы для записи данных SNMP
  db-host: "localhost"    # Хост базы данных

```

```
db-port: 9000 # Порт базы данных
db-username: "default" # Пользователь базы данных
db-password: "" # Пароль пользователя
rollup-section: "snmp_rollup" # Секция ClickHouse с правилами свёртки
```

4.17 База ASN

Секция `asn` определяет файлы базы данных ASN, используемые FlowCollector.

```
# asn:
#   enable: false # Включение базы ASN. По умолчанию – false
#   paths:
#     - "/opt/spfc/etc/asn/RU-GeoIP-ASN-Blocks-IPv6.csv"
#     - "/opt/spfc/etc/asn/RU-GeoIP-ASN-Blocks-IPv4.csv"
```

Если параметр `paths` не задан, используются стандартные пути:

```
/opt/spfc/etc/asn/RU-GeoIP-ASN-Blocks-IPv6.csv
/opt/spfc/etc/asn/RU-GeoIP-ASN-Blocks-IPv4.csv
```

4.18 Параметры лицензии

```
# license:
#   path: "/opt/spfc/etc/analyzer.lic" # Путь к файлу лицензии
```

Если путь не задан, FlowCollector пытается загрузить файл лицензии из `/opt/spfc/etc/analyzer.lic`.

4.19 Глобальные правила обнаружения

Секция `rules` позволяет задавать глобальные правила обнаружения аномалий.

Правило может определять уровни применения, единицы измерения, векторы атак, пороговые значения, приоритет и действие.

```
# rules:
#   -
```

# type: правило.	# Типы объектов, к которым применяется
	# Опционально.
	# По умолчанию – global, subnet, local
# - global	# Весь управляемый объект
# - subnet	# Отдельная подсеть
# - local	# Отдельный IP-адрес
# units: применяется правило.	# Единицы измерения трафика, к которым
	# Опционально.
	# По умолчанию – bytes, packets
# - bytes	
# - packets	
# vectors: правило.	# Векторы атак, к которым применяется
	# Опционально.
	# По умолчанию – все доступные векторы
# - dns-flood	# IPv4/IPv6-пакеты UDP или TCP # с портом назначения 53
# - ip-fragment-flood	# Фрагментированные IPv4/IPv6-пакеты
# - ip-private-flood	# IPv4-пакеты с IP-адресом источника # из диапазонов 10.0.0.0/8, 172.16.0.0/12 # и 192.168.0.0/16
# - icmp-flood	# IPv4/IPv6-пакеты ICMP
# - tcp-flood	# IPv4/IPv6-пакеты TCP
# - tcp-null-flood флагов	# IPv4/IPv6-пакеты TCP без установленных
# - tcp-cwr-flood	# IPv4/IPv6-пакеты TCP с флагом CWR # (Congestion Window Reduced, 0x80)
# - tcp-ecn-flood	# IPv4/IPv6-пакеты TCP с флагом ECE # (ECN-Echo, 0x40)
# - tcp-urg-flood	# IPv4/IPv6-пакеты TCP с флагом URG # (Urgent Pointer field significant, 0x20)
# - tcp-ack-flood	# IPv4/IPv6-пакеты TCP с флагом ACK # (Acknowledgment field significant, 0x10)
# - tcp-psh-flood	# IPv4/IPv6-пакеты TCP с флагом PSH # (Push Function, 0x08)
# - tcp-rst-flood	# IPv4/IPv6-пакеты TCP с флагом RST # (Reset the connection, 0x04)

# - tcp-syn-flood	# IPv4/IPv6-пакеты TCP с флагом SYN # (Synchronize sequence numbers, 0x02)
# - tcp-fin-flood	# IPv4/IPv6-пакеты TCP с флагом FIN # (No more data from sender, 0x01)
# - udp-flood	# IPv4/IPv6-пакеты UDP
# - total-traffic	# Любые IPv4/IPv6-пакеты
# - invalid-protocol-flood протокола 0	# IPv4/IPv6-пакеты с идентификатором
19 # - chargen-amp	# IPv4/IPv6-пакеты UDP с портом источника
53 # - dns-amp	# IPv4/IPv6-пакеты UDP с портом источника
123 # - ntp-amp	# IPv4/IPv6-пакеты UDP с портом источника
161 # - snmp-amp	# IPv4/IPv6-пакеты UDP с портом источника
162 # - snmptrap-amp	# IPv4/IPv6-пакеты UDP с портом источника
389 # - ldap-amp	# IPv4/IPv6-пакеты UDP с портом источника
1434 # - mssql-amp	# IPv4/IPv6-пакеты UDP с портом источника
1435 # - ibm-cics-amp	# IPv4/IPv6-пакеты UDP с портом источника
1900 # - ssdp-amp	# IPv4/IPv6-пакеты UDP с портом источника
3283 # - apple-remote-desktop-amp	# IPv4/IPv6-пакеты UDP с портом источника
3702 # - ws-discovery-amp	# IPv4/IPv6-пакеты UDP с портом источника
11211 # - memcached-amp	# IPv4/IPv6-пакеты UDP с портом источника
# - udp-zero-payload-flood нагрузки 0	# IPv4/IPv6-пакеты UDP с размером полезной

# - udp-big-packets-flood нагрузки	# IPv4/IPv6-пакеты UDP с размером полезной # не менее 1400 байт
# - http-flood 80	# IPv4/IPv6-пакеты TCP с портом назначения
# - https-flood 443	# IPv4/IPv6-пакеты TCP с портом назначения
# - gre-flood	# IPv4/IPv6-пакеты GRE
# - port-any	# IPv4/IPv6-пакеты TCP или UDP, # полученные на любом порту
# - port-custom port	# IPv4/IPv6-пакеты TCP или UDP, # полученные на порту, заданном в секции
# limit-threshold: 100M	# Абсолютное пороговое значение. # Условие срабатывания: last >= limit. # Опционально
# limit-diff: 50KB/s limit.	# Порог абсолютного изменения. # Условие срабатывания: # last > previous и last - previous >= # Опционально
# limit-reldiff: 250% limit.	# Порог относительного изменения. # Условие срабатывания: # last > previous и last / previous >= # Опционально
# priority: 0	# Приоритет правила. # Целое число. Опционально. # По умолчанию — 0
# action:	# Действие для правила. # Опционально. По умолчанию используется # глобальное действие
# nexthop: transit	
# flow-spec-rules-names: правила конфигурации. значение # - "rule1"	# Список правил FlowSpec. # Можно указать имя правила, заданного # в этом файле вне секции rules, или # с таким же именем из основной # Опционально. По умолчанию — пустое

```
#      port:                                # Параметры для векторов port-any и port-
custom                                #
#      protocols: tcp                      # Протоколы для отслеживания: tcp, udp.
                                           # Можно указать несколько значений через
                                           запятую.

#      port-numbers: 0                    # Порты для вектора port-custom.
                                           # Можно указать отдельные порты и диапазоны
                                           # в формате port1,...,portK-
                                           portK+M,...,portN.
```

Для параметров `limit-threshold`, `limit-diff` и `limit-reldiff` можно использовать модификаторы значений.

Если в правиле задан параметр `units`, доступны следующие модификаторы:

Модификатор	Значение	Пример
K	×1000	100K
M	×1 000 000	100M
G	×1 000 000 000	1G
T	×1 000 000 000 000	1T
%	/100	250%

Если `units` не задан, значения применяются к байтам и пакетам.

Единицу измерения также можно указать непосредственно в значении:

Модификатор	Единица измерения	Пример
p, p%	пакеты	100p, 50p%
b, b%	биты	100b, 50b%
B, B%	байты	100B, 50B%
b, Kb, Mb, Gb	бит/с	50Mb/s
B, KB, MB, GB	байт/с	50MB/s
p, Kp, Mp, Gp	пакет/с	100Kp/s

Для значений скорости можно использовать как краткую запись, так и запись с `/s`, например `Mb` или `Mb/s`, `MB` или `MB/s`, `Kp` или `Kp/s`.

