

# **Инструкция по установке Servicepipe FlowCollector**

Листов: 42

2026 г.

|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 1 |

## Оглавление

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| 1 Область применения .....                                                   | 3  |
| 2 Назначение программного обеспечения.....                                   | 4  |
| 3 Требования к системе .....                                                 | 5  |
| 3.1 Требования к операционной системе .....                                  | 5  |
| 3.2 Аппаратные требования .....                                              | 5  |
| 3.3 Требования к сетевым интерфейсам.....                                    | 5  |
| 3.4 Требования к правам доступа.....                                         | 5  |
| 4 Подготовка к установке.....                                                | 7  |
| 4.1 Выбор режима интеграции .....                                            | 7  |
| 4.1.1 Режим зеркалирования трафика .....                                     | 7  |
| 4.1.2 Режим приёма потоковых данных .....                                    | 7  |
| 4.2 Обновление системы .....                                                 | 8  |
| 5 Установка компонентов FlowCollector .....                                  | 8  |
| 5.1 Состав метапакетов FlowCollector .....                                   | 8  |
| 5.2 Установка компонентов .....                                              | 9  |
| 5.3 Настройка крупных страниц памяти.....                                    | 9  |
| 5.4 Настройка базы данных.....                                               | 11 |
| 5.5 Настройка сервиса загрузки метрик .....                                  | 13 |
| 5.6 Настройка сервиса чтения метрик .....                                    | 14 |
| 5.7 Настройка сервиса обработки запросов к метрикам.....                     | 14 |
| 5.8 Настройка базы данных событий .....                                      | 15 |
| 5.9 Настройка сервиса обмена сообщениями .....                               | 16 |
| 5.10 Настройка конфигурации FlowCollector.....                               | 17 |
| 5.10.1 Параметры логирования.....                                            | 17 |
| 5.10.2 Основные параметры.....                                               | 18 |
| 5.10.2.1 Привязка логических ядер .....                                      | 18 |
| 5.10.2.2 Параметры обнаружения.....                                          | 19 |
| 5.10.2.3 Параметры метрик .....                                              | 19 |
| 5.10.3 Дополнительные аргументы запуска режима прямой обработки трафика..... | 20 |

|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 2 |

|                                 |                                                                        |    |
|---------------------------------|------------------------------------------------------------------------|----|
| 5.10.4                          | Параметры HTTP API.....                                                | 21 |
| 5.10.5                          | Настройка сетевых интерфейсов.....                                     | 21 |
| 5.10.5.1                        | Конфигурация режима прямой обработки сетевого трафика .....            | 22 |
| 5.10.5.2                        | Конфигурация режима приёма потоковых данных.....                       | 24 |
| 5.10.6                          | Политики обнаружения и реагирования .....                              | 25 |
| 5.10.6.1                        | Параметры счетчиков пакетов.....                                       | 25 |
| 5.10.6.2                        | Анонсы и действия .....                                                | 26 |
| 5.10.6.3                        | Глобальные параметры обнаружения.....                                  | 28 |
| 5.10.6.4                        | Оповещения и интеграция с внешними сервисами.....                      | 28 |
| 5.10.6.5                        | Отправка уведомлений.....                                              | 29 |
| 5.10.6.6                        | Параметры таблицы поиска IP-адресов.....                               | 30 |
| 5.10.7                          | Параметры отчётов .....                                                | 30 |
| 5.10.8                          | Хранение данных .....                                                  | 31 |
| 5.10.8.1                        | Дампы сетевого трафика .....                                           | 31 |
| 5.10.8.2                        | Параметры сохранения данных о сетевых потоках .....                    | 32 |
| 5.10.9                          | Параметры SNMP .....                                                   | 33 |
| 5.11                            | Настройка тестового объекта .....                                      | 34 |
| 5.12                            | Настройка сетевого интерфейса для режима прямой обработки трафика..... | 36 |
| 5.13                            | Запуск сервисов.....                                                   | 37 |
| Составили.....                  |                                                                        | 40 |
| Согласовано .....               |                                                                        | 41 |
| Лист регистрации изменений..... |                                                                        | 42 |

|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 3 |

## 1 Область применения

Настоящая инструкция устанавливает порядок установки и первичной настройки программного обеспечения FlowCollector.

Документ предназначен для системных администраторов и специалистов, осуществляющих развертывание FlowCollector в инфраструктуре заказчика.

|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 4 |

## 2 Назначение программного обеспечения

Программное обеспечение FlowCollector предназначено для сбора, агрегирования и анализа потокового сетевого трафика с целью выявления DDoS-атак и иных сетевых аномалий.

При выявлении аномалии программное обеспечение может инициировать меры реагирования, включая формирование BGP-анонсов для перенаправления трафика в защитный контур.

|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 5 |

## **3 Требования к системе**

### **3.1 Требования к операционной системе**

Операционная система — Ubuntu Server.

### **3.2 Аппаратные требования**

Процессор — не менее 10 физических ядер. Оперативная память — не менее 8 ГБ. Дисковое пространство — не менее 100 ГБ.

### **3.3 Требования к сетевым интерфейсам**

Для эксплуатации в режиме прямой обработки сетевого трафика сервер должен быть оснащён не менее чем двумя физическими сетевыми интерфейсами:

- интерфейсом управления
- интерфейсом обработки сетевого трафика.

Для эксплуатации в режиме приёма данных о сетевых потоках сервер должен быть оснащён не менее чем одним сетевым интерфейсом. Сетевые адаптеры, используемые для обработки трафика, должны обеспечивать производительность, достаточную для приёма, обработки и передачи трафика в соответствии с расчётной нагрузкой. Также должна быть обеспечена поддержка используемого режима обработки сетевого трафика на уровне драйверов и операционной системы.

### **3.4 Требования к правам доступа**

|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 6 |

Для выполнения установки требуется пользователь с административными привилегиями.

|               |                                       |
|---------------|---------------------------------------|
| Наименование: | Инструкция по установке FlowCollector |
|---------------|---------------------------------------|

## **4 Подготовка к установке**

### **4.1 Выбор режима интеграции**

#### **4.1.1 Режим зеркалирования трафика**

Режим предназначен для эксплуатации в условиях высокой пропускной способности и обработки трафика со скоростью более 30 Гбит/с.

Требуется:

- выделение физического интерфейса;
- настройка зеркалирования трафика на сетевом оборудовании;
- настройка коэффициента выборки при использовании GRE-туннелирования.

#### **4.1.2 Режим приёма потоковых данных**

Режим предназначен для обработки данных, сформированных в результате выборки сетевого трафика. Поддерживается приём данных по следующим протоколам:

- NetFlow v10 (IPFIX);
- NetFlow v9;
- sFlow;
- IMON.



|                |                                       |        |
|----------------|---------------------------------------|--------|
| Наименование:  | Инструкция по установке FlowCollector |        |
| Код документа: |                                       | Стр. 8 |

## 4.2 Обновление системы

Для работы приложения требуется актуальная версия операционной системы. Перед установкой необходимо проверить наличие обновлений и установить их.

# 5 Установка компонентов FlowCollector

## 5.1 Состав метапакетов FlowCollector

Установка FlowCollector включает три метапакета:

Таблица 1 — Состав метапакетов FlowCollector

| Метапакет                                                | Состав                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| flowcollector<br>Основные компоненты                     | analyzer<br>dpdk                                                                                                                                                                                                                                                                              |
| flowcollector-additional<br>Дополнительные<br>компоненты | curl<br>mongodb-org<br>clickhouse-server<br>clickhouse-client<br>libpq-dev<br>libatomic1<br>zlib1g-dev<br>libpcap-dev<br>libnuma-dev<br>libssl-dev<br>libbpf-dev<br>libfdt-dev<br>libisal-dev<br>libibverbs-dev<br>ibverbs-providers<br>libprotobuf-dev<br>libgrpc++-dev<br>protobuf-compiler |



|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 10 |

где

Н - количество крупных страниц памяти;

Р - объем RAM, выделяемый для FlowCollector, ГБ;

Р - размер страницы памяти (фиксированное значение 2048 kB);

S - количество NUMA-узлов.

Коэффициент 1024 используется для перевода гигабайт в мегабайты.

Количество NUMA-узлов определяется командой:

```
ls -d /sys/devices/system/node/node* | wc -l
```

Пример расчёта для системы с двумя NUMA-узлами. Общий объём оперативной памяти — 160 ГБ. Объём памяти, выделяемый для FlowCollector, — 80 ГБ. Количество NUMA-узлов — 2.

$$N = (80 \times 1024) / (2 \times 2) = 20480$$

Открыть текстовый редактор для создания скрипта:

```
sudo nano /opt/spfc/bin/create_hugepages.sh
```

Вставить следующий код в открытый файл:

```
#!/bin/bash
```

```
mkdir -p /dev/hugepages
```

```
mountpoint -q /dev/hugepages || mount -t hugetlbfs nodev /dev/hugepages
```

```
#node 0 (CPU 0)
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 11 |

```
echo 20480 | sudo tee /sys/devices/system/node/node0/hugepages/hugepages-2048kB/nr_hugepages
```

```
#node 1 (CPU 1)
```

```
echo 20480 | sudo tee /sys/devices/system/node/node1/hugepages/hugepages-2048kB/nr_hugepages
```

Пример расчёта для системы с одним NUMA-узлом. Общий объём оперативной памяти — 16 ГБ. Объём памяти, выделяемый для FlowCollector, — 12 ГБ. Количество NUMA-узлов — 1.

$$N = (12 \times 1024) / (2 \times 1) = 6144$$

Открыть текстовый редактор для создания скрипта:

```
sudo nano /opt/spfc/bin/create_hugepages.sh
```

Скопировать и вставить следующий код в открытый файл:

```
#!/bin/bash
```

```
mkdir -p /dev/hugepages
```

```
mountpoint -q /dev/hugepages || mount -t hugetlbfs nodev /dev/hugepages
```

```
#node 0 (CPU 0)
```

```
echo 6144 | sudo tee /sys/devices/system/node/node0/hugepages/hugepages-2048kB/nr_hugepages
```

## 5.4 Настройка базы данных

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 12 |

Аналитическая база данных используется для хранения метрик, данных о сетевых потоках и справочной информации, а также для выполнения аналитических запросов. В составе FlowCollector она обеспечивает доступ к информации, необходимой для анализа сетевого трафика и работы связанных функциональных модулей.

1. Запустить службу базы данных и проверить её состояние на наличие ошибок:

```
sudo systemctl start clickhouse-server && systemctl status clickhouse-server
```

2. Для корректной работы FlowCollector требуется создать следующие таблицы:

- graphite — метрики;
- graphite\_index — индексы метрик;
- graphite\_tagged — теги graphite;
- flows — таблица для хранения данных о сетевых потоках;
- asn\_dict — справочник ASN;
- cidr\_location\_dict — справочник CIDR;
- geo\_name\_dict — справочник географических названий;
- flows\_fast\_dataset — основная таблица для обработки данных о сетевых потоках;
- flows\_fast\_dataset\_mv — материализованное представление fast\_dataset;
- flows\_full\_dataset — полная таблица для хранения данных о сетевых потоках;
- flows\_full\_dataset\_mv — материализованное представление full\_dataset.

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 13 |

Если при установке базы данных был задан пароль для пользователя, выполнить соответствующую команду с параметром `--password`. Если пароль не задавался, выполнять команду без этого параметра.

Без пароля:

```
clickhouse-client --multiline --multiquery < /usr/share/doc/clickhouse-server/graphite/fc-init.sql
```

С паролем:

```
clickhouse-client --multiline --multiquery --password=[пароль clickhouse] <
/usr/share/doc/clickhouse-server/graphite/fc-init.sql
```

3. Проверить создание необходимых таблиц. Ожидаемое количество таблиц — 11.

Без пароля:

```
clickhouse-client --query="SHOW TABLES" | wc -l
```

С паролем:

```
clickhouse-client --query="SHOW TABLES" --password=[пароль clickhouse] | wc -l
```

## 5.5 Настройка сервиса загрузки метрик

Данный раздел выполняется только в случае, если для подключения к аналитической базе данных задан пароль.

Необходимо отредактировать конфигурационный файл сервиса загрузки метрик:

```
sudo nano /etc/carbon-clickhouse/carbon-clickhouse.conf
```

В секциях `[upload.graphite]` и `[upload.graphite_index]` указать параметры подключения в формате:

```
default:[пароль]@localhost:8123
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 14 |

Использование стандартного значения localhost:8123 без указания учётных данных в данном случае не допускается.

Включить автозапуск сервиса и проверить его состояние:

```
sudo systemctl enable --now carbon-clickhouse && systemctl status carbon-clickhouse
```

## 5.6 Настройка сервиса чтения метрик

Данный раздел выполняется только в случае, если для подключения к аналитической базе данных задан пароль.

Необходимо отредактировать конфигурационный файл сервиса чтения метрик:

```
sudo nano /etc/graphite-clickhouse/graphite-clickhouse.conf
```

В секции [clickhouse] указать параметры подключения в формате:

```
default:[пароль]@localhost:8123
```

Использование стандартного значения localhost:8123 без указания учётных данных в данном случае не допускается.

Включить автозапуск сервиса и проверить его состояние:

```
sudo systemctl enable --now graphite-clickhouse && systemctl status graphite-clickhouse
```

## 5.7 Настройка сервиса обработки запросов к метрикам

Сервис обработки запросов к метрикам используется для получения, обработки и агрегации временных рядов из хранилища метрик. Сервис обеспечивает доступ к метрикам через совместимый программный интерфейс и поддерживает функции агрегации, необходимые для аналитической обработки.

Включить автозапуск службы и проверить её состояние:

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 15 |

```
sudo systemctl enable --now carbonapi && systemctl status carbonapi
```

## 5.8 Настройка базы данных событий

База данных событий используется для хранения событий и другой структурированной информации, необходимой для работы компонентов FlowCollector.

1. Запустить службу базы данных, включить автозапуск и проверить текущее состояние:

```
sudo systemctl enable --now mongod && systemctl status mongod
```

2. Создать коллекцию reports в базе данных test:

```
mongosh test --eval 'db.createCollection("reports")'
```

3. Создать индексы для коллекции reports:

```
mongosh test --eval 'db.reports.createIndex({ mo: 1, unixStartTime: 1, unixLastTime: 1 })'
```

4. Создать пользователя для работы приложений. Имя пользователя и пароль указываются в соответствии с политикой безопасности организации:

```
mongosh
```

```
db.createUser(
```

```
{
```

```
  user: "events",
```

```
  pwd: "events",
```

```
  roles: [ { role: "readWrite", db: "test" } ]
```

```
}
```

```
)
```



|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 16 |

exit

#### 5. Отредактировать конфигурационный файл базы данных:

```
sudo nano /etc/mongod.conf
```

#### 6. Добавить или раскомментировать секцию security и включить авторизацию:

security:

authorization: enabled

Для автоматизации изменения можно использовать команду:

```
sudo sed -i 's/^#\?security:/security:\n authorization: enabled/' /etc/mongod.conf
```

#### 7. Перезапустить службу базы данных для применения изменений:

```
sudo systemctl restart mongod
```

После включения авторизации для всех подключений к базе данных потребуется указание имени пользователя и пароля.

### 5.9 Настройка сервиса обмена сообщениями

Сервис обмена сообщениями используется для взаимодействия компонентов FlowCollector и доставки событий между ними.

#### 1. Включить автозапуск и запустить службу обмена сообщениями:

```
sudo systemctl enable --now nats-server
```

#### 2. Создать поток сообщений с использованием конфигурационного файла:

```
nats stream add --config /opt/nats/stream.conf
```

#### 3. Создать обработчик сообщений с параметрами по умолчанию:

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 17 |

nats consumer add \

--pull \

--deliver all \

--ack explicit \

--wait 30s \

--replay instant \

--max-pending 1000 \

--max-waiting 512 \

--inactive-threshold 0 \

analyzer first

## 5.10 Настройка конфигурации FlowCollector

Перед началом работы рекомендуется изучить комментарии к каждому параметру.

В зависимости от выбранного режима интеграции необходимо включить соответствующую секцию конфигурации. Для режима прямой обработки сетевого трафика используется секция `dpdk-nic`. Для режима приёма потоковых данных используется секция `ipfix`.

Открыть файл конфигурации для редактирования:

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

### 5.10.1 Параметры логирования

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 18 |

Поддерживаются следующие уровни логирования: trace, debug, info, warn(warning), error, fatal. Параметр level определяет уровень детализации сообщений журнала:

log:

level: debug

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

## 5.10.2 Основные параметры

### 5.10.2.1 Привязка логических ядер

Секция lcore-mapping задаёт параметры распределения потоков обработки по логическим ядрам процессора.

Если секция lcore-mapping закомментирована, распределение выполняется автоматически. Для оптимизации нагрузки допускается раскомментировать секцию и задать параметры распределения вручную.

Пример конфигурации:

```
# lcore-mapping:
```

```
# mode: auto # auto | manual
```

```
# schema: # определяет количество логических ядер, назначенных для каждой активности
```

```
# auto:
```

```
# detection: 4
```

```
# event-processing: 2
```

```
# metrics: 2
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 19 |

```
#   dpdk-rx: 1

#   dpdk-worker: 4

#   ipfix-rx: 1

#   ipfix-worker: 2

#   reports: 2

#   free: 2

#   manual:

#   detection: 4

#   event-processing: 2

#   metrics: 2

#   dpdk-rx: 1

#   dpdk-worker: 4

#   ipfix-rx: 1

#   ipfix-worker: 2

#   reports: 2

#   free: 2
```

### 5.10.2.2 Параметры обнаружения

Секция detection задаёт параметры механизма обнаружения аномалий.

detection:

```
enable: true
```

### 5.10.2.3 Параметры метрик

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 20 |

Секция `metrics` задаёт параметры сбора и отправки метрик. Метрики формируются с использованием структуры имени `[hostname].[plugin].*`, где `hostname` и `plugin` задаются соответствующими параметрами конфигурации.

`metrics:`

`enable: true`

`carbon:`

`endpoint: 127.0.0.1:2003`

`hostname: flowcollector`

`plugin: analyzer`

`interval: 5`

`export-timeout: 5`

- `enable` — состояние механизма сбора метрик.
- `endpoint` — адрес сервиса приёма метрик.
- `hostname` — первый ключ при формировании имени метрики.
- `plugin` — второй ключ при формировании имени метрики.
- `interval` — период сбора метрик, с.
- `export-timeout` — период отправки метрик, с.

### 5.10.3 Дополнительные аргументы запуска режима прямой обработки трафика

Параметр `dpdk-args` задаёт дополнительные аргументы запуска режима прямой обработки сетевого трафика. По умолчанию значение не задано.

`# dpdk-args:`

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 21 |

Параметр используется при необходимости передать дополнительные низкоуровневые параметры запуска, связанные с выбором сетевого интерфейса, режимом работы драйвера или особенностями аппаратной конфигурации сервера

Пример задания параметра:

```
# dpdk-args: -a <port>
```

#### 5.10.4 Параметры HTTP API

Блок `http-api` задаёт параметры работы программного интерфейса FlowCollector.

`http-api:`

`enable: true`

`endpoint: inet://127.0.0.1:10505`

- `enable` — состояние HTTP API (`true` — включено, `false` — отключено).
- `endpoint` — точка привязки, по которой FlowCollector принимает входящие соединения.

Поддерживаются следующие форматы адреса:

- `unix://path/to/socket`

- `inet://127.0.0.1:8082`

- `127.0.0.1`

#### 5.10.5 Настройка сетевых интерфейсов

FlowCollector поддерживает несколько режимов получения данных о сетевом трафике. В конфигурационном файле должна быть активна только

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 22 |

секция, соответствующая выбранному режиму работы. Остальные секции должны оставаться закомментированными.

#### 5.10.5.1 Конфигурация режима прямой обработки сетевого трафика

Секция `dpdk-nic` задаёт параметры режима прямой обработки сетевого трафика. Пример конфигурации:

`dpdk-nic:`

`enable: false`

`# enable-eth-ports: 0xff`

`# port-rx-queue-number: 1`

`# throttling-rate: 1`

`# packet-pool:`

`# size: 8191`

`# cache-size: 128`

`# arp:`

`# enable: false`

`# devices:`

`# mac: 00:00:00:00:00:00`

`# ip:`

`# - 127.0.0.1`

`# - 192.168.0.0`

`# default-ip: 127.0.0.1`

`sources:`

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 23 |

group: all

# local:

# host: 192.168.0.1

local: {}

# remote:

# host: 192.168.0.2

remote: {}

- enable — состояние режима прямой обработки сетевого трафика
- enable-eth-ports — маска включённых Ethernet-портов.
- port-rx-queue-number — количество очередей Rx на интерфейс.
- throttling-rate — коэффициент регулирования нагрузки.
- packet-pool.size — размер пула пакетов.
- packet-pool.cache-size — размер кэша пула пакетов.
- arp.enable — включает обработку ARP.
- arp.devices — перечень устройств для обработки ARP.
- arp.default-ip — IP-адрес по умолчанию для анализатора.
- sources — источники трафика для сопоставления с группами.
- sources.group — имя группы источников.
- local — параметры локальной точки. Пустое значение {} соответствует любому адресу.
- remote — параметры удалённой точки. Пустое значение {} соответствует любому адресу.

При отсутствии параметров local и remote применяется полное зеркалирование трафика.



|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 24 |

### 5.10.5.2 Конфигурация режима приёма потоковых данных

Секция `ipfix` задаёт параметры режима приёма данных о сетевых потоках. Пример конфигурации:

`ipfix:`

`enable:`

`endpoint:`

`- 127.0.0.1:4739`

`# - 192.168.0.1:4739`

`# exclusive-sockets-mode: false`

`# memory-pool:`

`# number: 16383`

`# cache-size: 64`

`sources:`

`-`

`group: all`

`# local:`

`# host: 192.168.0.1`

`# port: 20000`

`local: {}`

`# remote:`

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 25 |

# host: 192.168.0.2

# port: 30000

remote:

- enable — состояние режима приёма потоковых данных (true — включено, false — отключено).
- endpoint — перечень адресов и портов, на которых FlowCollector принимает данные о сетевых потоках.
- exclusive-sockets-mode — режим работы сокетов. Поддерживаются:
  - кооперативный (по умолчанию),
  - эксклюзивный.
- memory-pool.number — размер пула памяти для обработки сообщений о сетевых потоках.
- memory-pool.cache-size — размер кэша пула памяти.
- sources — перечень источников данных о сетевых потоках.
- sources.group — имя группы источников.
- sources.local — параметры локальной точки. Пустое значение {} соответствует любому адресу и порту.
- sources.remote — параметры удалённой точки. Пустое значение {} соответствует любому адресу и порту.

## 5.10.6 Политики обнаружения и реагирования

### 5.10.6.1 Параметры счетчиков пакетов

packet-counters:

rate: 1

average-period: 5000

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 26 |

interval: 5000

- rate — коэффициент выборки пакетов. Передаётся каждый N-й пакет; итоговое количество пакетов вычисляется как полученное значение, умноженное на rate.
- average-period — период усреднения скорости, мс.
- interval — интервал времени, за который рассчитывается средняя скорость трафика, мс.

### 5.10.6.2 Анонсы и действия

# Параметры для отправки BGP анонсов

announce:

enable: false

nexthops:

- name: transit

ip: 192.168.10.1

- name: blackhole

ip: 192.168.20.1

# communities: 666

# communities:

# - 666:666                   # - <целое\_число\_основание\_10>:<целое\_число\_основание\_10>

# - 777:777                   # - <целое\_число\_основание\_10>

# - 0x<целое\_число\_основание\_16>

timeout: 20

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 27 |

# Конец announce

- enable — состояние отправки BGP-анонсов.
- nexthops — перечень next-hop значений, используемых при формировании BGP Update.
- nexthops.name — имя next-hop, которое может использоваться в параметрах действия.
- nexthops.ip — IP-адрес next-hop.
- nexthops.communities — BGP communities для next-hop. Допускается одно значение или список значений.
- timeout — интервал отправки анонсов, с. Применяется только для нативного BGP.

Действие выполняется для обнаруженной аномалии, если правило не содержит собственного действия. На данный момент доступен только BGP анонс как действие

action:

nexthop: transit

# communities: 666:666

# communities:                   # Доступные форматы:

# - 666:666                       # - <целое\_число\_основание\_10>:<целое\_число\_основание\_10>

# - 777:777                       # - <целое\_число\_основание\_10>

                                  # - 0x<целое\_число\_основание\_16>

# Конец action

- nexthop — next-hop для действия. Допускается IP-адрес или имя из announce.nexthops.name.

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 28 |

- communities — BGP communities для действия. Если параметр задан, он переопределяет значение announce.nexthops.communities для выбранного next-hop.

### 5.10.6.3 Глобальные параметры обнаружения

Параметры confirm-period и action-expiry-timeout задают общие условия подтверждения аномалий и выполнения связанных действий. Пример конфигурации:

confirm-period: 0

action-expiry-timeout: 60

- confirm-period — период подтверждения аномалии, с. После первичного обнаружения аномалия подтверждается, если сохраняется в течение указанного времени.
- action-expiry-timeout — время продолжения действия после исчезновения аномалии, с.

### 5.10.6.4 Оповещения и интеграция с внешними сервисами

Секция action-events задаёт параметры отправки событий, формируемых при обнаружении аномалий. Пример конфигурации:

action-events:

enable: true

graphite: false

host: 127.0.0.1

port: 8081

path: /

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 29 |

- enable — состояние механизма отправки событий.
- graphite — режим доставки событий: при значении false используется компонент sp-events.
- host — адрес компонента sp-events.
- port — порт компонента sp-events.
- path — путь подключения к сервису.

#### 5.10.6.5 Отправка уведомлений

Секция notification-service задаёт параметры сервиса уведомлений.

Пример конфигурации:

notification-service:

enable: true

nats:

enable: true

host: localhost

port: 4222

path: /

subject: analyzer.notification

persistance: true

- enable — состояние сервиса уведомлений.
- nats.enable — состояние интеграции с сервисом обмена сообщениями.
- nats.host — адрес сервиса обмена сообщениями.
- nats.port — порт сервиса обмена сообщениями.
- nats.path — путь подключения.

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 30 |

- nats.subject — subject для публикации уведомлений.
- nats.persistance — режим сохранения сообщений.

#### 5.10.6.6 Параметры таблицы поиска IP-адресов

Секция ip-lookup-table задаёт режим обработки пересечений CIDR-подсетей между объектами мониторинга. Пример конфигурации:

ip-lookup-table:

mode: overlap

- mode — режим обработки CIDR-перекрытий:
- overlap — допускаются пересекающиеся подсети в разных управляемых объектах.
- nooverlap — пересекающиеся подсети запрещены.

#### 5.10.7 Параметры отчётов

Секция reports задаёт параметры формирования и экспорта отчётов. Пример конфигурации:

reports:

enable: true

host: localhost

port: 9080

path: /report

export-timeout: 10

max-src-addr: 10000

max-dst-addr: 10000

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 31 |

max-src-ports: 1000

max-dst-ports: 1000

- enable — состояние механизма формирования и экспорта отчётов.
- host — адрес сервиса экспорта отчётов.
- port — порт сервиса экспорта отчётов.
- path — путь для отправки отчётов.
- export-timeout — таймаут экспорта, с.
- max-src-addrс — максимальное количество исходных IP-адресов в отчёте.
- max-dst-addrс — максимальное количество целевых IP-адресов в отчёте.
- max-src-ports — максимальное количество исходных портов в отчёте.
- max-dst-ports — максимальное количество целевых портов в отчёте.

## 5.10.8 Хранение данных

### 5.10.8.1 Дампы сетевого трафика

Секция `pcapng-dumper` задаёт параметры формирования дампов сетевого трафика. Пример конфигурации:

`pcapng-dumper:`

`enable: false`

`# dumps-path: /var/dump/`

`max-sessions-number: 8`

`max-packets-number: 10000`

`keep-alive: 10`

- enable — состояние механизма формирования дампов сетевого трафика.



|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 32 |

- `dumps-path` — каталог для записи дампов.
- `max-sessions-number` — максимальное количество одновременно активных сессий дампа.
- `max-packets-number` — максимальное количество пакетов в одном дампе.
- `keep-alive` — максимальное время ожидания пакетов в сессии ручного дампа, с.

#### 5.10.8.2 Параметры сохранения данных о сетевых потоках

Секция `save-flow` задаёт параметры сохранения данных о сетевых потоках в аналитическую базу данных. Пример конфигурации:

`save-flow:`

`enable: false`

`enable-all-mo: true`

`enable-save-all: false`

`table-name: "default.flows"`

`db-host: "localhost"`

`db-username: "default"`

`db-password: "[пароль clickhouse]"`

`dp-port: 9000`

`rollup-section: "flows_rollup"`

`save-records-number: 10000`

`flush-records-timeout: 60`

- `enable` — состояние механизма сохранения потоков.

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 33 |

- enable-all-mo — включает сохранение потоков для всех управляемых объектов.
- enable-save-all — включает сохранение всего поступающего трафика.
- table-name — имя таблицы для записи потоков.
- db-host — адрес сервера базы данных.
- db-username — имя пользователя базы данных.
- db-password — пароль пользователя базы данных.
- db-port — порт подключения к базе данных.
- rollup-section — имя секции конфигурации с правилами агрегации данных о сетевых потоках.
- save-records-number — количество записей в одном блоке сохранения.
- flush-records-timeout — интервал принудительного сброса блока записей, с.

### 5.10.9 Параметры SNMP

FlowCollector выполняет опрос сетевых интерфейсов следующих типов: ethernet-csmacd(6), prop-virtual(53), tunnel(131).

Секция snmp задаёт параметры опроса сетевого оборудования по протоколу SNMP. Пример конфигурации:

snmp:

enable: false

agents:

- peer: example.org:161

version: 1

request-timeout: 60s

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 34 |

response-timeout: 1s

# local-address: 192.168.0.1

# local-port: 11111

community: public

# security-name: secret

# security-auth-key: secret-key

# alias: example

- enable — состояние механизма опроса SNMP.
- agents — перечень SNMP-агентов.
- agents.peer — адрес агента в формате host[:port].
- agents.version — версия SNMP: 1, 2с или 3.
- agents.request-timeout — интервал между запросами, с.
- agents.response-timeout — время ожидания ответа, с.
- agents.local-address — локальный адрес привязки.
- agents.local-port — локальный порт привязки.
- community — строка community для SNMP версий 1 и 2с.
- security-name — имя безопасности для SNMP версии 3.
- security-auth-key — ключ аутентификации SNMP версии 3.
- alias — имя, используемое при формировании метрик.

## 5.11 Настройка тестового объекта

1. Для создания директории выполнить следующие команды:

```
sudo mkdir /opt/spfc/etc/mo/test_logic_folder
```

```
sudo mkdir /opt/spfc/etc/mo.enabled/test_logic_folder
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 35 |

## 2. Открыть и отредактировать файл конфигурации:

```
sudo nano /opt/spfc/etc/mo/test_logic_folder/test_object.yaml
```

## 3. Добавить в конфигурационный файл следующие тестовые настройки:

```
name: test_object # Имя объекта, case-sensitive
```

```
cids:           # Анализируемые сети
```

```
- 0.0.0.0/1
```

```
- 128.0.0.0/1
```

```
rules:          # Блок правил
```

```
-
```

```
type:
```

```
- local         # Счетчик на /32
```

```
vectors:
```

```
- total-traffic
```

```
limit-threshold: 250Mb/s # 250 мбит/с
```

```
-
```

```
type:
```

```
- global        # Счетчик на весь объект
```

```
vectors:
```

```
- total-traffic
```

```
limit-threshold: 2500Mb/s # 2.5 гбит/с
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 36 |

4. Создать символическую ссылку в директории активированных объектов:

```
sudo ln -s /opt/spfc/etc/mo/test_logic_folder/test_object.yaml
/opt/spfc/etc/mo.enabled/test_logic_folder/test_object.yaml
```

## 5.12 Настройка сетевого интерфейса для режима прямой обработки трафика

Раздел применяется только при эксплуатации FlowCollector в режиме прямой обработки сетевого трафика.

При использовании сетевых адаптеров, поддерживающих работу без передачи порта под управление специализированного драйвера, дополнительная привязка интерфейса не требуется.

1. Определить идентификатор сетевого интерфейса порта, задействованного для получения зеркального трафика:

```
sudo /usr/local/bin/dpdk-devbind.py -s
```

Из вывода команды необходимо определить идентификатор порта. Например:

```
0000:13:00.0 'VMXNET3 Ethernet Controller 07b0' drv=vfio-pci unused=vmxnet3
```

В данном примере идентификатор порта — 13:00.0.

2. Открыть конфигурационный файл:

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

3. Указать идентификатор порта в параметре дополнительных аргументов запуска:

```
dpdk-args: -a 13:00.0
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 37 |

4. Указать параметры сетевого интерфейса, используемого для прямой обработки сетевого трафика:

dpdk-nic:

enable: true

arp:

enable: true

#devices:

# - mac: "00:50:56:a8:51:79"

# ip:

# - 10.0.101.10

# Если задействована одна сетевая карта, то достаточно будет указать её IP (без маски)

default-ip: 10.0.101.2

5. Записать идентификатор порта, используемого для прямой обработки сетевого трафика:

echo "13:00.0" | sudo tee /opt/spfc/etc/nic\_port

### 5.13 Запуск сервисов

1. Назначить права на выполнение служебных скриптов и включить системные сервисы:

sudo chmod +x /opt/spfc/bin/bind\_driver.sh /opt/spfc/bin/create\_hugepages.sh

sudo systemctl enable --now \

/opt/spfc/lib/systemd/system/bind\_driver.service \

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 38 |

/opt/spfc/lib/systemd/system/create\_hugepages.service \

/opt/spfc/lib/systemd/system/analyzer.service

## 2. Проверить состояние сервиса подготовки сетевого интерфейса:

```
sudo systemctl status bind_driver
```

При эксплуатации в режиме приёма потоковых данных возможно сообщение:

Warning: Configuration file /opt/spfc/etc/nic\_port not found. Interface binding was skipped

Это ожидаемое поведение.

## 3. Проверить состояние сервиса выделения памяти для обработки трафика:

```
sudo systemctl status create_hugepages
```

При корректной работе в выводе команды должно отображаться сообщение: Finished Create hugepages

## 4. Проверить статус сервиса analyzer:

```
sudo systemctl status analyzer
```

## 5. Убедиться, что после запуска трафика происходит запись метрик в аналитическую базу данных:

Без указания пароля:

```
clickhouse-client --query "SELECT * FROM graphite WHERE Path LIKE '%analyzer%' LIMIT 10"
```

С указанием пароля:

```
clickhouse-client --password=[пароль clickhouse] --query "SELECT * FROM graphite WHERE Path LIKE '%analyzer%' LIMIT 10"
```

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 39 |

При возникновении ошибок рекомендуется проверить журнал сервиса:

```
sudo journalctl -fu analyzer
```



|                |                                       |  |         |
|----------------|---------------------------------------|--|---------|
| Наименование:  | Инструкция по установке FlowCollector |  |         |
| Код документа: |                                       |  | Стр. 40 |

**Составили**

| Наименование<br>организации,<br>предприятия | Должность<br>исполнителя | Фамилия, имя,<br>отчество | Подпись | Дата |
|---------------------------------------------|--------------------------|---------------------------|---------|------|
|                                             |                          |                           |         |      |

|                |                                       |         |  |
|----------------|---------------------------------------|---------|--|
| Наименование:  | Инструкция по установке FlowCollector |         |  |
| Код документа: |                                       | Стр. 41 |  |

**Согласовано**

| Наименование<br>организации,<br>предприятия | Должность<br>исполнителя | Фамилия, имя,<br>отчество | Подпись | Дата |
|---------------------------------------------|--------------------------|---------------------------|---------|------|
|                                             |                          |                           |         |      |
|                                             |                          |                           |         |      |
|                                             |                          |                           |         |      |
|                                             |                          |                           |         |      |

|                |                                       |         |
|----------------|---------------------------------------|---------|
| Наименование:  | Инструкция по установке FlowCollector |         |
| Код документа: |                                       | Стр. 42 |

**Лист регистрации изменений**

| № версии док-та | Дата изменения | Автор изменений | Изменения |
|-----------------|----------------|-----------------|-----------|
|                 |                |                 |           |