

Автоматическая установка DG на Ubuntu 22.04: локальная инсталляция

1. Подготовка операционной системы

1.1 Настройка сетевых интерфейсов

Внести необходимые изменения в сетевые интерфейсы в соответствии с текущей сетевой архитектурой компании. При Outline-инсталляции обязательно настроить VLAN'ы.

Для Inline-инсталляции необходимо использовать минимум два физических порта для передачи данных и один порт для управления (mgmt).

Для Outline-инсталляции требуется минимум один физический порт для передачи данных и один порт для управления.

При настройке интерфейсов *ifupdown* учесть следующее:

- Удалить конфигурации линейных интерфейсов из профиля *netplan*, отредактировав файл **/etc/netplan/00-installer-config.yaml**. Конфигурации, относящиеся к mgmt-интерфейсам, допускается оставить без изменений.
- Добавить DNS-сервер в настройку *systemd-resolved*, отредактировав файл **/etc/systemd/resolved.conf**.

В случае недоступности NTP-серверов в связи с политиками безопасности возможно добавить собственный NTP-сервер отредактировав файл **/etc/systemd/timesyncd.conf**.

Примечание

При использовании сетевых карт Intel с драйвером ixgbe рекомендуется ограничить кол-во потоков до 24:

```
ethtool -L eth1 combined 24
```

- <https://www.spinics.net/lists/netdev/msg439438.html>

При использовании сетевых карт Mellanox, в настройках аппаратных интерфейсов, на которых будет работать DosGate, рекомендуется указать настройку `tune_xdp = 1`. Необходимо открыть для редактирования файл `/etc/network/interfaces`.

Вставить следующую строку:

```
tune_xdp = 1
```

1.2 Перезагрузка сервера

Перезагрузить сервер, выполнив команду:

```
sudo reboot
```

2. Установка DosGate с помощью скрипта

2.1 Выполнение скрипта установки DosGate

Скрипт выполняет подключение репозитория Serviceripe, установку DosGate в выбранной конфигурации и первоначальное конфигурирование системы.

Для запуска необходимо выполнить команду:

```
curl -o "./setup-dg.sh" "https://public-repo.svc.p.io/setup_script/setup-dg.sh" && \
```

```
sudo chmod +x "./setup-dg.sh" && \
./setup-dg.sh
```

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

```
=== Проверка системных требований ===
Количество ядер CPU: 12
Оперативная память: 4 ГБ
Внимание: объем оперативной памяти (4 ГБ) меньше минимального (8 ГБ)
Продолжить установку? (y/n): 
```

2.2 Подключение репозитория

После запуска скрипта выполняется проверка наличия репозитория Servicepipe:

```
=== Проверка наличия подключенного репозитория https://public-repo.svcp.io/ ===
Репозиторий https://public-repo.svcp.io/ не подключен.
Выполнить подключение? (y/n): y
```

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

2.3 Выбор конфигурации DosGate для установки

После подключения репозитория скрипт предложит выбрать конфигурацию DosGate.

Установка DosGate включает четыре метапакета:

Метапакет	Компоненты
dosgate Основные компоненты DosGate	<ul style="list-style-type: none">• collectd• nginx• sp-spider-broker• libdt1• libaevent1• dosgate
dosgate-uh Сессионная защита	<ul style="list-style-type: none">• libxskexp• dosgate-uh
spider Компоненты веб-интерфейса	<ul style="list-style-type: none">• nodejs (= 18.18.2-1nodesource1)• libpq-dev• postgresql (= 14+238)

Метапакет	Компоненты
	<ul style="list-style-type: none"> • rabbitmq-server (= 3.13.6-1) • sp-spider-broker • sp-spider
dosgate-monitoring Компоненты мониторинга	<ul style="list-style-type: none"> • clickhouse-server (= 23.10.5.20-servicepipe-20250331.151941.UTC) • clickhouse-client (= 23.10.5.20) • carbon-clickhouse • graphite-clickhouse • carbonapi

Укажите необходимый вариант и подтвердите установку.

```
=== Установка пакетов ===
Установить dosgate? (y/n): y
Установить dosgate-uh? (y/n): y
Установить spider? (y/n): y
Установить пакет мониторинга? (y/n): y
```

Внимание:

В процессе установки, в зависимости от выбранной конфигурации, может потребоваться 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 выполняется начальная настройка установленных компонентов.

Так, при установке пакета Spider и пакета Monitoring скрипт предложит инициализировать ClickHouse с созданием базы данных, задать параметры в конфигурационных файлах .env для SP-Spider и SP-Spider-Broker.

```
=== Первоначальная конфигурация ===
Synchronizing state of nginx.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
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
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.
Выполнить первоначальную инициализацию Clickhouse? (y/n): y
Выполняем перезапуск Clickhouse
Выполняем первоначальную инициализацию Clickhouse...
Файл /usr/share/doc/clickhouse-server/graphite/dg-init.sql найден. Выполняем инициализацию ClickHouse...
Введите пользователя ClickHouse (по умолчанию 'default'): default
Введите пароль ClickHouse (оставьте пустым, если нет пароля):
Инициализация ClickHouse завершена.
Файл /etc/carbon-clickhouse/carbon-clickhouse.conf обновлен с логином и паролем ClickHouse.
Выполняем перезапуск Carbon-clickhouse
Файл /etc/graphite-clickhouse/graphite-clickhouse.conf обновлен с логином и паролем ClickHouse.
Выполняем перезапуск graphite-clickhouse
Первоначальная инициализация Clickhouse завершена.
Created symlink /etc/systemd/system/multi-user.target.wants/sp-spider.service → /lib/systemd/system/sp-spider.service.
Выполнить первоначальную конфигурацию SP-Spider? (y/n): y
Выполняем первоначальную конфигурацию SP-Spider...
```

Затем, выполняется создание базы данных и пользователя PostgreSQL, а также настройка учётной записи RabbitMQ с назначением пароля и прав доступа.

```
=== Конфигурация базы данных PostgreSQL ===
Введите имя базы данных (по умолчанию dosgate):
Введите имя пользователя PostgreSQL (по умолчанию dosgate):
Введите пароль пользователя PostgreSQL:
Создаём базу и пользователя PostgreSQL...
CREATE DATABASE
CREATE ROLE
GRANT
=== Конфигурация RabbitMQ ===
Введите логин для RabbitMQ (по умолчанию username):
Введите пароль для RabbitMQ:
Создаём пользователя RabbitMQ и назначаем права...
Adding user "username" ...
Done. Don't forget to grant the user permissions to some virtual hosts! See 'rabbitmqctl help set_permissions' to learn more.
Setting permissions for user "username" in vhost "/" ...
```

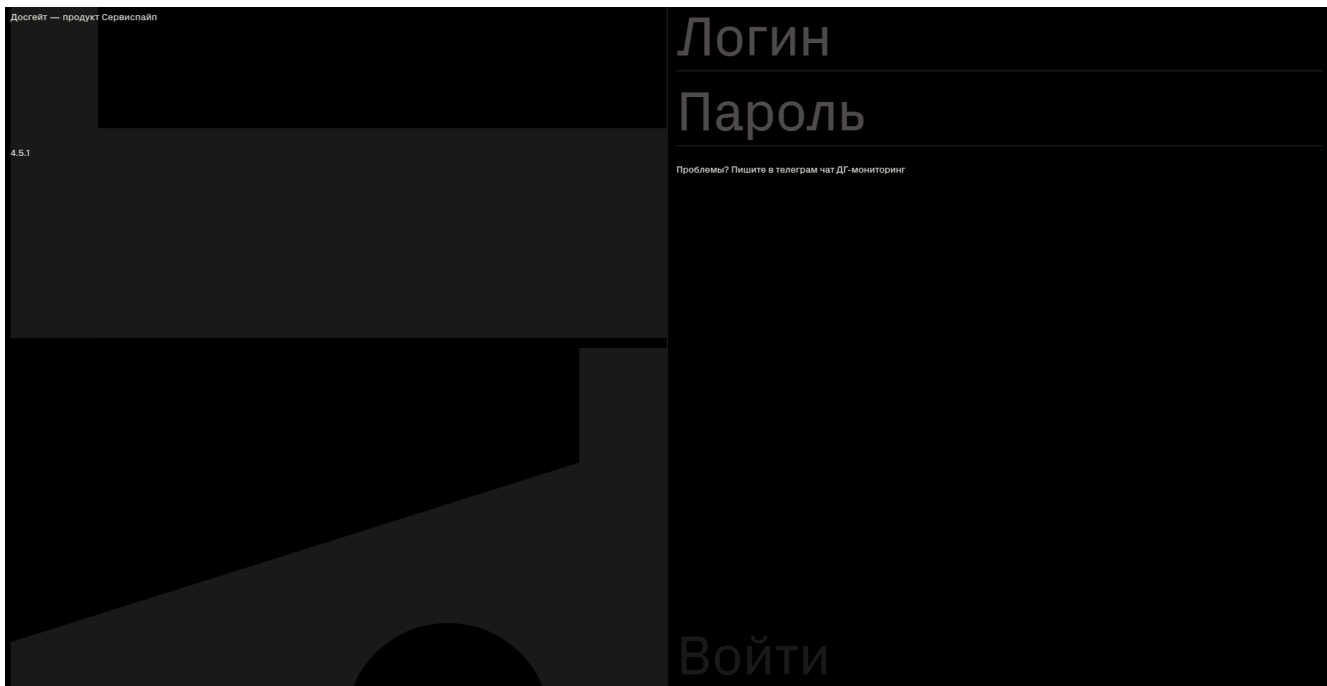
Затем выполняется создание системного пользователя для веб-интерфейса.

```
=== Создание системного пользователя ===
Введите имя пользователя для веб-интерфейса (по умолчанию dosgate-web): dosgate-web
Adding user `dosgate-web' ...
Adding new group `dosgate-web' (1001) ...
Adding new user `dosgate-web' (1001) with group `dosgate-web' ...
Creating home directory `/home/dosgate-web' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
```

3. Первый вход в систему

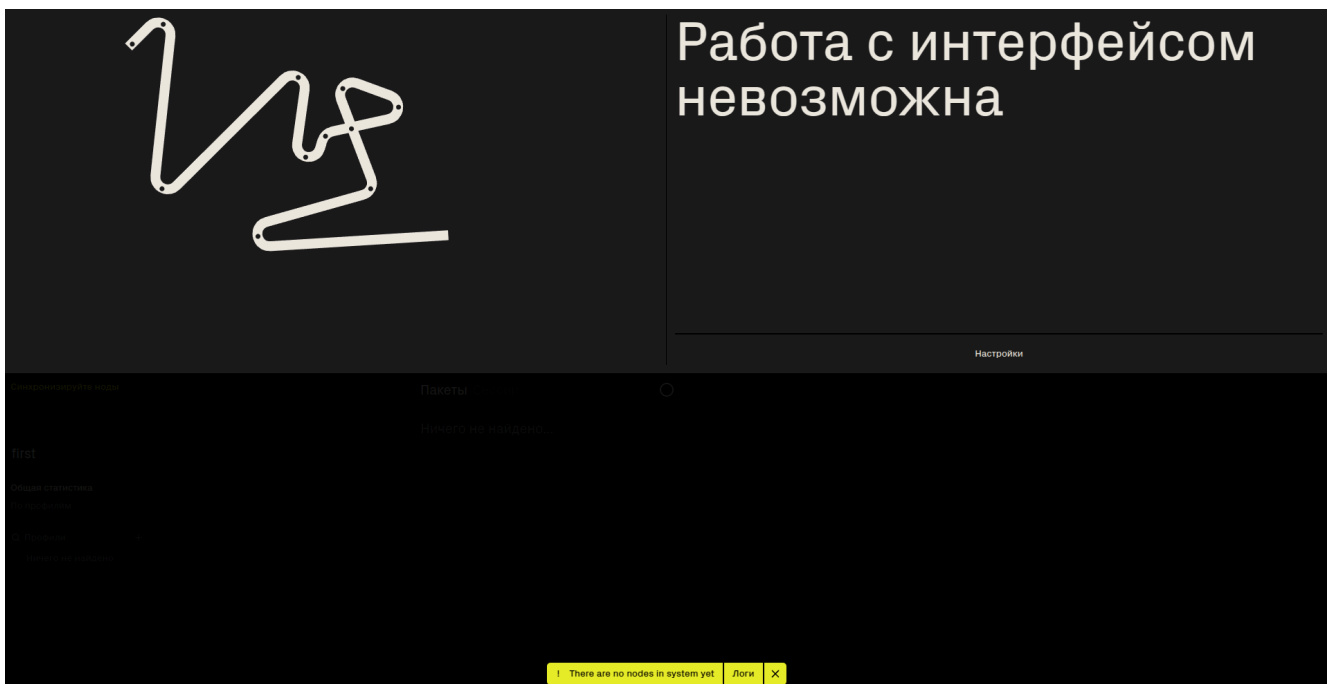
Для входа в Веб-интерфейс DosGate следует ввести в адресной строке браузера IP-адрес сервера и порт по шаблону: `ip:3333` .

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

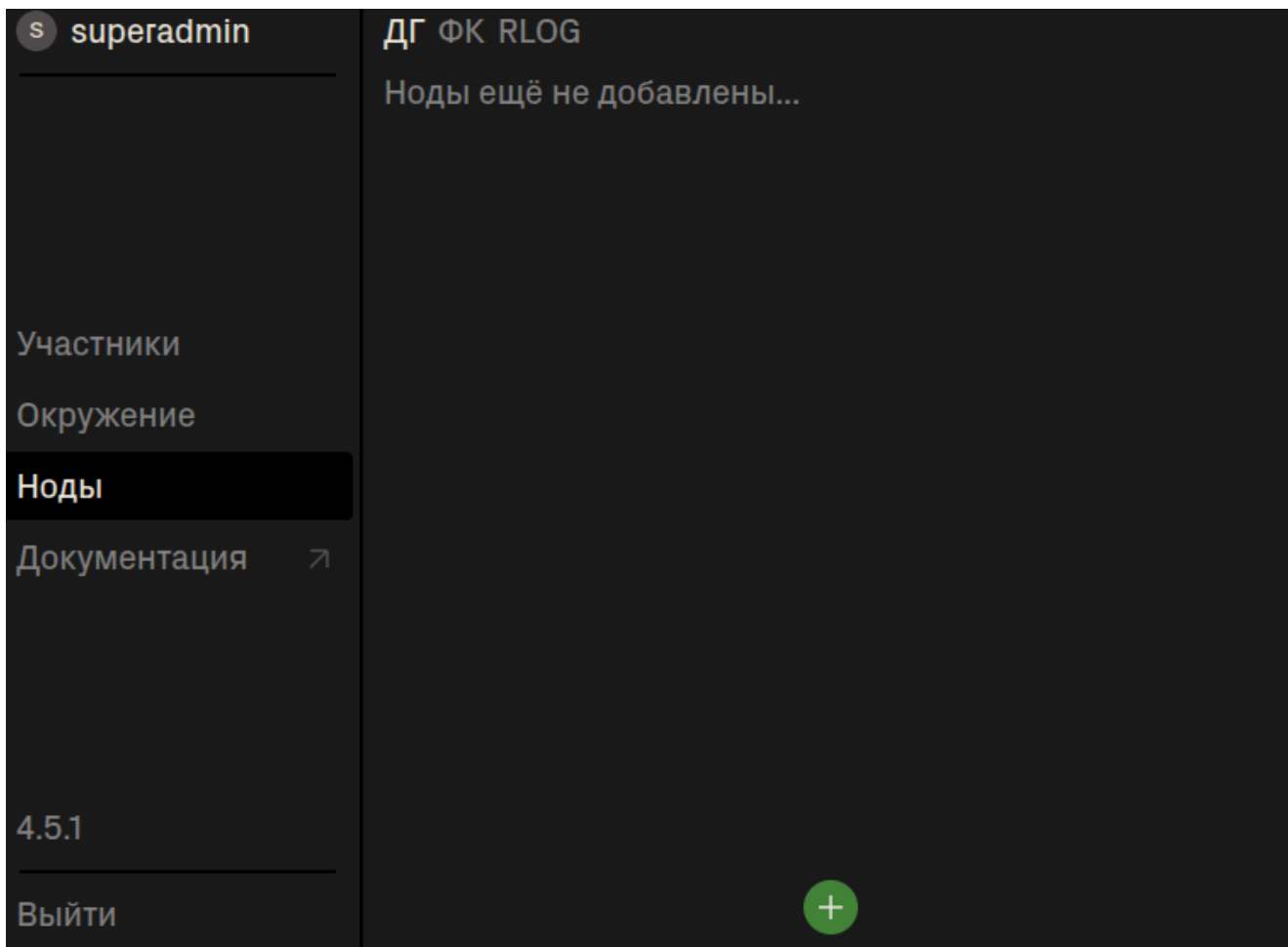


Окно авторизации при входе в систему

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 зелёную иконку с плюсом. В открывшемся окне указать:

- **Collectd host** — значение должно соответствовать параметру `hostname`, указанному в конфигурационном файле `dosgate.conf` в блоке `collectd`. По умолчанию используется `dosgate-srv1`.
- **Collectd UH** — укажите имя узла, по умолчанию — `dosgate-uh-srv1`.

Оп.система	Ubuntu 18+ ▾
Модуль	DosGate ▾
Collectd host	dosgate-srv1
Collectd UH	dosgate-uh-srv1
HW Bypass	Отключено >
ClickHouse	>
Подключение	>

Добавить ноду

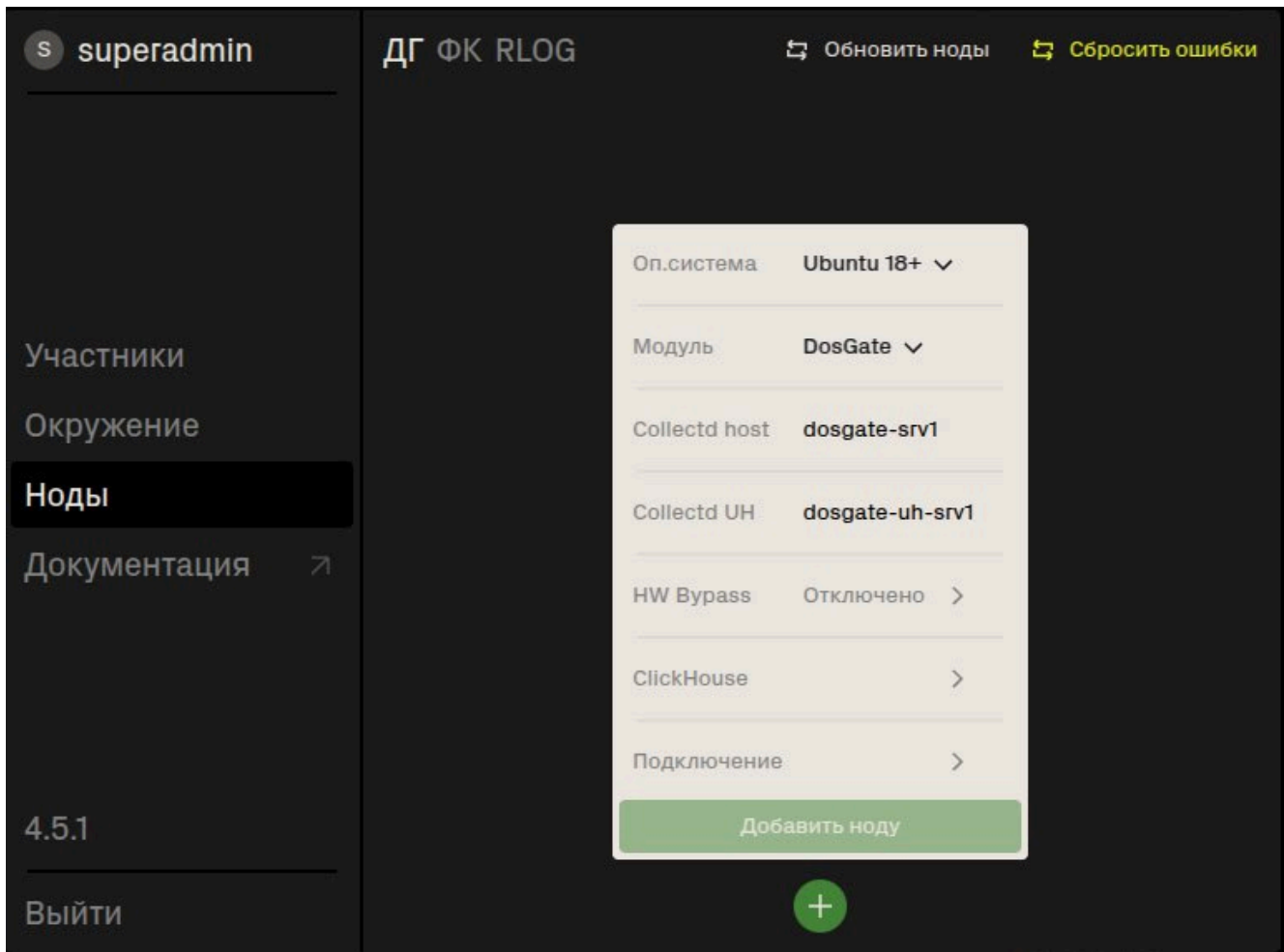
Перейти в настройки **ClickHouse** и указать параметры подключения. Пример настроек для подключения к ClickHouse, установленному на локальной ноде:

← ClickHouse

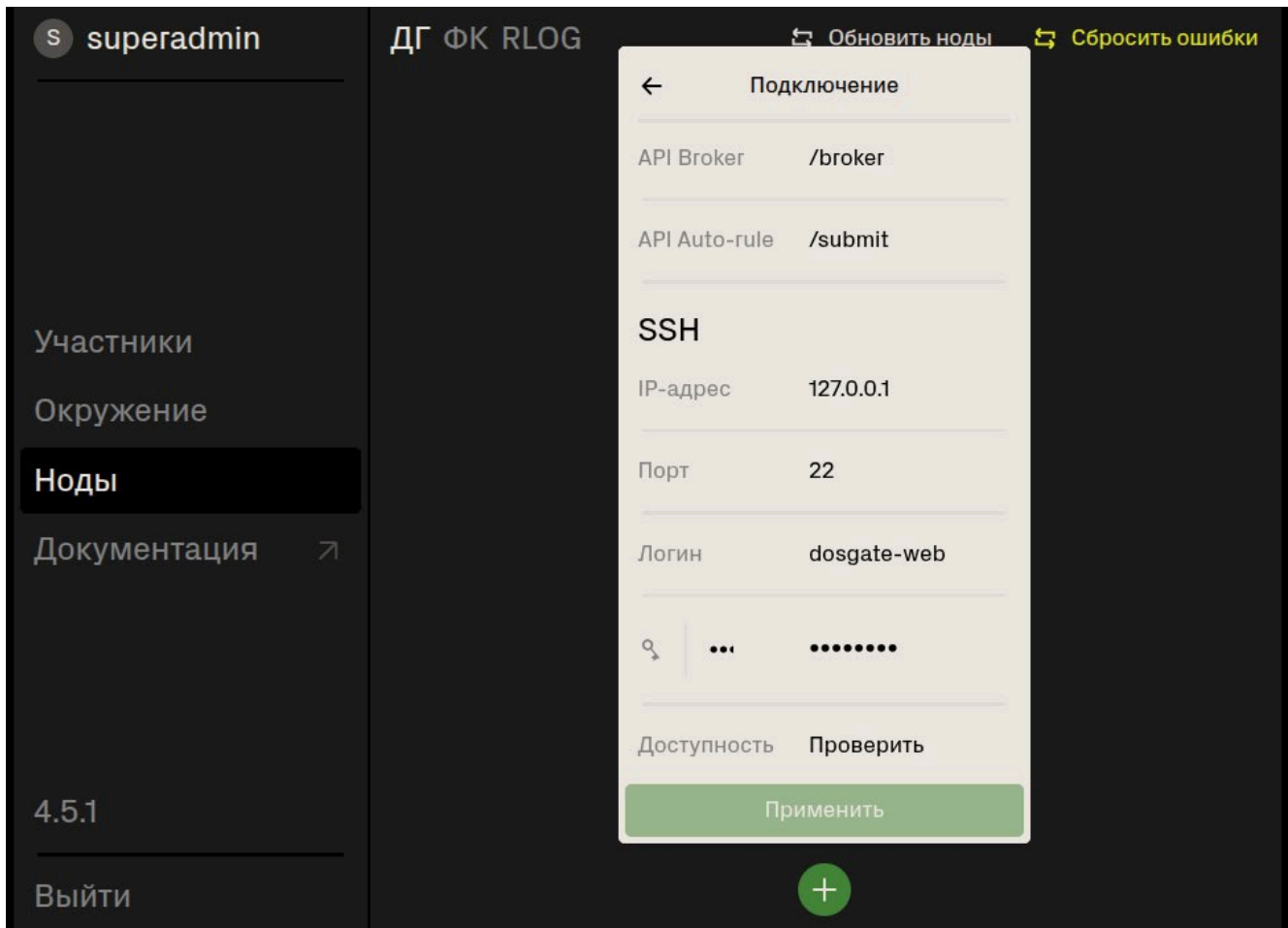
Хост	127.0.0.1
Порт	8123
База данных	default
Пользователь	default
Пароль	••••••••

Применить

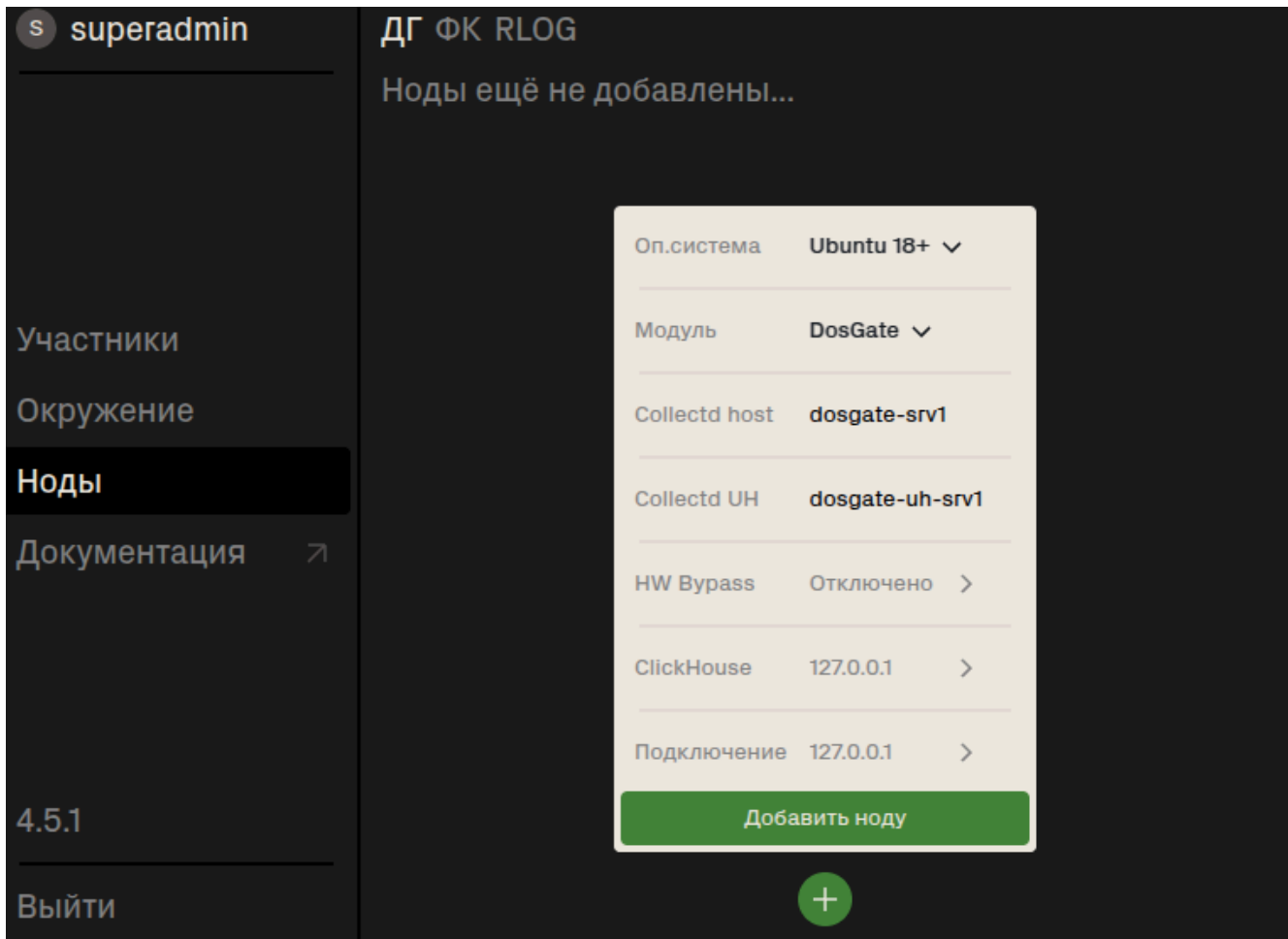
Нажать на кнопку **Применить**. Перейти в раздел **Подключение**.



В открывшемся окне указать SSH-данные для подключения к установленной ноде Dosgate (IP-адрес, логин, пароль). Нажать на кнопку **Проверить**, чтобы проверить подключение. Если данные введены правильно и нода доступна, статус изменится на **Доступна**. После этого нажать кнопку **Применить**. Пример заполненных настроек приведён ниже:



В открывшемся окне нажать **Добавить ноду**.



Для отображения графиков и статистики необходимо указать ссылку на Graphite. Перейдите в раздел **Окружение**. В разделе DosGate указать "Graphite URL" и "Арена по умолчанию". Название арены должно соответствовать значению, указанному в конфигурационном файле dosgate.conf для всех нод кластера.

Пример настроек:

s superadmin

Участники

Окружение

Ноды

Документация ↗

4.5.1

Выйти

Вкл глубину хранения метрик

Автосинхронизация

DosGate

Graphite URL `http://127.0.0.1:8088`

Арена по-умолчанию `first`

Обновление графиков ? `10` сек

Использовать MMDB

RLog

Обновление графиков ? `60` сек

Нажать на свой профиль в левом верхнем углу экрана, чтобы открыть настройки профиля. Установить новый пароль.

S
superadmin

Мой профиль

Участники

Окружение

Ноды

Дополнительно

Документация ➤

4.5.1

Выйти

Логин	superadmin	id:1
Группа	Администратор	
Создан	16.05.2025 12:56	
Пароль	••••••••	Изменить
Язык	Русский ▼	
Уведомления	<input checked="" type="checkbox"/>	

Выполнить обновление страницы. Веб-интерфейс готов к использованию.

ΔГ

first

Общая статистика

По профилям

Q. Профили +

Ничего не найдено

Пакеты Сессии ○

Период

Точный +

5 мин

15 мин

30 мин

1 час

6 часов

12 часов

24 часа

3 дня

7 дней

dosgate-srv1-first · bits/s

- dgstats-drop
- dgstats-error
- dgstats-pass
- dgstats-pass_uh
- dgstats-reply
- dgstats-transmit

dosgate-srv1-first · packets/s

- dgstats-drop
- dgstats-error
- dgstats-pass
- dgstats-pass_uh
- dgstats-reply
- dgstats-transmit

dosgate-srv1-output · bits/s

- dgstats-drop
- dgstats-error
- dgstats-pass
- dgstats-pass_uh
- dgstats-reply
- dgstats-transmit

4. Настройка конфигурации DosGate

Все параметры работы Dosgate задаются в едином конфигурационном файле `dosgate.conf`. Конфигурационный файл находится по пути `/etc/dosgate.conf`. Его настройка обязательна перед первым запуском программного обеспечения. Для доступа к командам управления производится аутентификация по SSH.

Конфигурационный файл написан в формате YAML и содержит следующие блоки:

- `socket_conf`
- `arena_conf`
- `collectd`

Подробнее о каждом блоке описано в следующих разделах.

При конфигурировании файла `dosgate.conf` следует использовать только пробелы; табуляция недопустима.

Для валидации корректности синтаксиса YAML, допустимо использовать сайт <https://www.yamllint.com>.

4.1 Блок *socket_conf*

Блок *socket_conf* сразу после установки имеет значения по умолчанию. Он настроен для использования и работы с CLI.

Пример конфигурации:

```
sockets:
  - url: /run/dosgate/api.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: SCGI

  - url: /run/dosgate/fapi.socket
    user: nginx
    group: nginx
    mode: 0660
    acl: any
    type: FCGI
    timeout:
      send: 10
      idle: 10
```

```
- url: /run/dosgate/crlf.socket
  user: nginx:nginx
  mode: 0660
  acl: any
  type: CRLF
  timeout:
    idle: 10
    send: 10

- url: /run/dosgate/cli.socket
  user: root:dosgate
  mode: 0660
  acl: any
  type: CLI
  timeout:
    idle: 10
    send: 10
```

Описание блока

URL

URL для сокетов имеет формат `family://address`, где:

family — тип сокета, который может принимать следующие значения:

- `unix` — UNIX-сокеты, используемый на файловой системе сервера. В качестве адреса указывается полный путь к сокету.
- `tcp` — TCP-сокеты. Адрес указывается в формате `host:port` или `:port`. Если указан только порт (`:port`), сокет будет прослушивать все доступные адреса (`0.0.0.0` или `::`).

Определение типа сокета по строке адреса

Если `family` не указано в URL, тип сокета определяется автоматически по формату строки адреса:

- Если строка начинается с `/`, предполагается, что это UNIX-сокеты (`family = unix`).
- Если строка содержит символ `:`, предполагается, что это TCP-сокеты (`family = tcp`).

User

Имя пользователя для UNIX-сокетов. Если указанный пользователь отсутствует, сокет будет использовать учетную запись пользователя, от имени которого выполняется процесс (по умолчанию `root`).

Group

Группа для UNIX-сокеты. Если указанная группа отсутствует, используется первичная группа пользователя, под которым выполняется процесс (по умолчанию root).

Mode

Режим доступа для UNIX-сокеты, задается в формате, аналогичном команде `chmod`.

ACL

Список контроля доступа (Access Control List). Перечисляются через запятую разрешенные target (например: `profile`, `router`, `arena`, `mark`, `pset`), значение `any` - разрешает доступ ко всем частям системы.

Type

Тип протокола/диалекта для сокета:

- FCGI - FastCGI протокол, полный диалект
- SCGI - SCGI протокол, полный диалект
- CRLF - raw протокол, полный диалект
- CLI - raw протокол, диалект CLI

RAW - протокол, при котором запрос заканчивается либо последовательностью CRLF, либо закрытием сокета в сторону сервера. Ответ также завершается CRLF или окончательным закрытием сокета.

Особенность для CLI:

Для отправки запросов через CLI должен быть настроен хотя бы один сокет с типом CLI, с family UNIX и адресом `/run/dosgate/cli.socket`

Timeout

Общий лимит времени, в течение которого сокет ожидает завершения операции. Указывается в секундах. При отсутствии установленного таймаута сокет продолжает ожидание завершения операций или остается в состоянии бездействия без ограничения по времени.

- `idle` - время, в течение которого сокет может оставаться бездействующим (неактивным) перед тем, как будет разорвано соединение или предприняты другие действия.
- `send` - время, отведенное на отправку данных через сокет. Если данные не удастся отправить в течение указанного времени, операция будет прервана.

4.2 Блок *arena_conf*

Основной блок конфигурации DosGate. Данный блок не имеет значений по умолчанию и требует обязательной настройки.

Пример конфигурации:

```
arenas:  
- name: first  
  id: 1  
  nets:  
    - rx:  
      name: ens1f0  
      mode: vlan  
      vid: 50  
      tx:  
        name: ens1f0  
        mac: 00:cc:34:47:a8:44  
        mode: swap  
        vid: 51  
    - rx:  
      name: ens1f0  
      mode: vlan  
      vid: 62  
      tx:  
        name: ens1f0  
        mac: 00:cc:34:4a:88:30  
        mode: swap  
        vid: 63  
    - rx:  
      name: ens3f0  
      mode: vlan  
      vid: 54  
      tx:  
        name: ens3f0  
        mac: 00:cc:34:4a:88:30  
        mode: swap  
        vid: 55  
    - rx:  
      name: ens3f0  
      mode: vlan  
      vid: 58  
      tx:  
        name: ens3f0  
        mac: 00:cc:34:47:a8:44  
        mode: swap  
        vid: 59
```

Описание блока:

Arenas - Набор сетевых интерфейсов и настроек обработки и возврата трафика.

Name - Уникальное имя арены.

Id - Уникальный Id арены (обязателен с 3.2.2-5).

Name (nets) - Имя сетевого интерфейса, как показывает ip link. Обязательное поле.

MAC - MAC-адрес. Может быть записан в одном из следующих форматов:

`XX:XX:XX:XX:XX:XX` или `XX-XX-XX-XX-XX-XX` или `XXXX.XXXX.XXXX`

Где `X` - шестнадцатеричная цифра.

VID - VLAN id. Число от 0 до 4095, где 0 означает отсутствие тега.

Protocol - Протокол VLAN. Либо hex-число в формате 0x0000, либо мнемоническое значение:

Тэг	Значение
802.1q, 8021q, q	0x8100
802.1ad, 8021ad, ad	0x88A8
802.1ah, 8021ah, ah	0x88E7
q-in-q, qq, qinq	0x9100
q-in-q1, qq2, qinq2	0x9200
q-in-q3, qq3, qinq3	0x9300

RX block - Описывает способ обработки входящего трафика. Должен присутствовать всегда.

```
- rx:  
  name: ens5  
  inline: true  
  mode: transparent  
  tx-policy: lACP
```

Если в блоке указан MAC-адрес, то обрабатывается только трафик с этим destination address.

`inline` - Интерфейс работает в inline-режиме, то есть он невидим для других хостов в сети. ARP-запросы, широковещательные запросы, STP/GVRP/etc не передаются в ОС.

Если опция не указана, то интерфейс пересылает этот трафик в ОС.

mode - Режим обработки входящего трафика:

- **vlan** - обрабатывается только трафик в указанном VLAN, остальной пропускается в ОС. Если VID = 0 или не указан, обрабатывается только нетегированный трафик.
- **transparent** - обрабатывается трафик во всех VLAN + нетегированный. Используется по умолчанию.

swap - Указывает, нужно ли менять MAC-адреса во фрейме при отправке.

Если указано **false** или **0**, то адреса не меняются. Если указано **true**, **1** или значение не указано, то адреса меняются.

tx-policy - управляет обработкой следующих классов трафика:

- **lacp** — медленный протокол LACP.
- **llm** — IEEE802.1 Link-local multicast, предназначенная для 01:80:C2:00:00:x.
- **multicast** - Любой L2 multicast, кроме link-local.
- **unknown** - unhandled ethertypes.

Например, если параметр LACP отсутствует, то LACP будет передан в ОС DosGate, а не в TX-интерфейс.

TX block - Описывает политику обработки трафика, который должен быть переслан в соответствии с окончанием обработки правилами или срабатывании действия ACCEPT. Если не указан, то копируется из блока RX, а отсутствующие в нём параметры принимают значения по умолчанию.

```
- tx:
  name: ens4
  mac: fa:16:3e:56:32:6a
  swap: false
```

Если в блоке указан MAC-адрес, то трафик пересылается на него. В противном случае он отправляется на тот адрес, с которого был получен

Mode - Режим обработки исходящего трафика:

- **swap** - меняется последний в стеке тег VLAN, или добавляется если трафик нетегированный. Если VID отсутствует, то пакет не меняется, если равен 0, то верхний тег снимается при наличии. Используется по умолчанию.

- `push` - новый тег добавляется безусловно, даже если последний был точно таким же. Если VID = 0 или отсутствует, то ничего не добавляется.

`cos` - Класс сервиса в тегированных пакетах. Число от 0 до 7.

Reply block - Описывает политику обработки трафика, который должен быть переслан в соответствии с правилами, которые генерируют собственный трафик в ответ на входящий пакет.

```
tx:
  name: ens5
  swap: false
reply:
  name: ens4
  swap: true
```

- Если `reply` не указан, то автоматически копируется из *TX block*. Формат полностью соответствует формату *TX block*.

4.3 Блок *collectd*

```
collectd:
  hostname: dosgate-srv1
  period: 10
```

- `hostname` - имя хоста, который будет использоваться для именованя метрик. Если вы устанавливаете DosGate в кластере, название должно быть уникально для каждой платформы. Именно под этим именем будут отображаться графики по серверам в общей статистике. Также с этим именем записываются метрики относительно сервера.
- `period` - частота записи метрик в collectd.

4.4 Примеры конфигурационного файла *dosgate.conf*

Ниже приведены примеры конфигурационных файлов **dosgate.conf**:

Пример outline инсталляции с VLAN swap и возвратом трафика в том-же интерфейсе

```
sockets:
  - url: /run/dosgate/api.socket
```

user: nginx
group: nginx
mode: 0660
acl: any
type: SCGI

- url: /run/dosgate/fapi.socket
user: nginx
group: nginx
mode: 0660
acl: any
type: FCGI
timeout:
 send: 10
 idle: 10

- url: /run/dosgate/crlf.socket
user: nginx:nginx
mode: 0660
acl: any
type: CRLF
timeout:
 idle: 10
 send: 10

- url: /run/dosgate/cli.socket
user: root:dosgate
mode: 0660
acl: any
type: CLI
timeout:
 idle: 10
 send: 10

arenas:

- name: first
id: 1
nets:
 - rx:
 name: ens1f0
 mode: vlan
 vid: 50
 tx:
 name: ens1f0
 mac: 00:cc:34:47:a8:44
 mode: swap
 vid: 51
 - rx:
 name: ens1f0
 mode: vlan
 vid: 62
 tx:
 name: ens1f0

```
mac: 00:aa:12:45:87:99
mode: swap
vid: 63
```

```
collectd:
  hostname: dosgate-srv1
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DosGate

```
sockets:
- url: /run/dosgate/api.socket
  user: nginx
  group: nginx
  mode: 0660
  acl: any
  type: SCGI

- url: /run/dosgate/fapi.socket
  user: nginx
  group: nginx
  mode: 0660
  acl: any
  type: FCGI
  timeout:
    send: 120
    idle: 120

- url: /run/dosgate/crlf.socket
  user: nginx
  group: nginx
  mode: 0660
  acl: any
  type: CRLF
  timeout:
    idle: 10
    send: 10

- url: /run/dosgate/cli.socket
  user: nginx
  group: nginx
  mode: 0660
  acl: any
  type: CLI
  timeout:
    idle: 10
    send: 10

arenas:
```

```
- name: first
  id: 1
  nets:
    - rx:
        name: enp4s0f0np0
        inline: true
        mode: transparent
      tx:
        name: enp4s0f1np1
        swap: false
      reply:
        name: enp4s0f0np0
        swap: true
- name: output
  id: 2
  nets:
    - rx:
        name: enp4s0f1np1
        inline: true
        mode: transparent
      tx:
        name: enp4s0f0np0
        swap: false

collectd:
  hostname: dosgate-srv1
  period: 10
```

Пример inline инсталляции с возвратом трафика в другом интерфейсе, и обратным трафиком через DoSGate с LACP

```
sockets:
- url: /run/dosgate/api.socket
  user: nginx
  group: nginx
  mode: 0660
  acl: any
  type: SCGI

- url: /run/dosgate/fapi.socket
  user: nginx
  group: nginx
  mode: 0660
  acl: any
  type: FCGI
  timeout:
    send: 120
    idle: 120

- url: /run/dosgate/crlf.socket
```

```
user: nginx
group: nginx
mode: 0660
acl: any
type: CRLF
timeout:
  idle: 10
  send: 10
```

```
- url: /run/dosgate/cli.socket
user: nginx
group: nginx
mode: 0660
acl: any
type: CLI
timeout:
  idle: 10
  send: 10
```

arenas:

```
- name: first
  id: 1
  nets:
    - rx:
        name: enp136s0f0
        mode: transparent
        inline: true
        tx-policy: lACP
      tx:
        name: enp136s0f1
        swap: false
      reply:
        name: enp136s0f0
        swap: true
    - rx:
        name: enp138s0f0
        mode: transparent
        inline: true
        tx-policy: lACP
      tx:
        name: enp138s0f1
        swap: false
      reply:
        name: enp138s0f0
        swap: true
- name: output
  id: 2
  nets:
    - rx:
        name: enp136s0f1
        mode: transparent
        inline: true
        tx-policy: lACP
```

```
tx:
  name: enp136s0f0
  swap: false
- rx:
  name: enp138s0f1
  mode: transparent
  inline: true
  tx-policy: lACP
tx:
  name: enp138s0f0
  swap: false

collectd:
  hostname: dosgate-srv1
  period: 10
```

5. Настройка конфигурации сессионной защиты

Все параметры работы сессионной защиты задаются в едином конфигурационном файле `dosgate-uh.conf`.

Для редактирования конфигурационного файла выполнить команду:

```
sudo nano /etc/dosgate-uh.conf
```

5.1 Глобальная конфигурация

Глобальные параметры определяют политику обработки сетевого трафика:

```
global:
  traffic-policy:
    good: accept # Разрешение корректного трафика
    bad: drop # Отклонение подозрительного трафика
    violate: drop # Отклонение нарушающего трафика
```

5.2 Конфигурация сетевых устройств

Для эффективного управления очередями приема и передачи пакетов необходимо настроить параметры сетевых интерфейсов:

```
net:
  ens224:
    rx:
      queues:
        count: 8 # Количество очередей приема
        len: 512 # Длина каждой очереди
  ens256:
    tx:
      queues:
        count: 8 # Количество очередей приема
        len: 512 # Длина каждой очереди
```

5.3 Настройки захвата трафика

Функция захвата трафика позволяет записывать сетевые пакеты в файлы для последующего анализа:

```
capture:
  path: /var/cache/dosgate-uh/capture # Директория для сохранения
  filename: cap_${DEV}_${ID}_${NUM}.pcap # Шаблон имен файлов
  age: 3600 # Максимальное время хранения файла
  (в секундах)
  count: 10 # Максимальное количество файлов
  size: 10M # Максимальный размер файла
```

5.4 Конфигурация сбора и экспорта статистики

Статистика помогает отслеживать состояние системы в реальном времени и экспортировать данные в систему мониторинга:

```
stats:
  period: 10 # Период сбора статистики (в секундах)
  push:
    type: collectd # Метод передачи данных
    plugin: unixsock # Используемый плагин
    target: /var/run/collectd-unixsock # Целевой сокет
    stats: all # Объем передаваемых данных
    hostname: dosgate-uh-srv1 # Идентификатор хоста
    queue-len: 0 # Длина очереди отправки
    period:
      collect: 5 # Интервал сбора данных (в секундах)
```

```
send: 10
секундах)
```

```
# Интервал отправки данных (в
```

5.5 Настройка отслеживания подключений

Параметры контроля соединений позволяют задавать ограничения и определять политику обработки трафика:

```
conntrack:
  limit: 10000000 # Максимальное количество отслеживаемых соединений
  reclaim:
    soft: 80 # Порог мягкого освобождения соединений (в % от лимита)
    hard: 95 # Порог жесткого освобождения соединений (в % от
лимита)
```

5.6 Путь к каталогу с реестром профиля приложения

По умолчанию: `/var/lib/dosgate-uh/profiles`

```
application:
  registry: /var/lib/dosgate-uh/profiles
  monitor-fs: true
```

5.7 Настройка экспорта фреймов

Обеспечение работы функции экспорта фреймов, которая выполняется в рамках действия dosgate action `-j EXPORT` :

```
frame-export:
  enabled: true # Включение функции экспорта фреймов
  export-objects: all # Экспорт всех объектов
```

5.8 Пример конфигурационного файла `dosgate-uh.conf`

Ниже приведен пример конфигурационного файла `dosgate-uh.conf`:

```
global:
  threads: 8
  thread-policy: pooled
  cpus:
    irq: 0-7
    thread: 0-7
  traffic-policy:
    good: accept
    bad: drop
    violate: drop
  trace: exp

net:
  eth0:
    rx:
      queues:
        count: 8
        len: 512
    tx:
      queues:
        count: 8
        len: 512
  eth1:
    rx:
      queues:
        count: 8
        len: 512
    tx:
      queues:
        count: 8
        len: 512

capture:
  path: /var/cache/dosgate-uh/capture
  filename: cap_${DEV}_${ID}_${NUM}.pcap
  age: 10
  count: 1
  size: 100M

stats:
  period: 10
  push:
    type: collectd
    plugin: unixsock
    target: /var/run/collectd-unixsock
    stats: all
    hostname: dosgate-uh-srv1
    queue-len: 0
  period:
    collect: 5
    send: 10

conntrack:
```

```
limit: 100000
```

```
reclaim:
```

```
  soft: 80
```

```
  hard: 95
```

```
application:
```

```
  registry: /var/lib/dosgate-uh/profiles
```

```
  monitor-fs: true
```