ОБНОВЛЕНО 16 МАР

Установка DosGate на Ubuntu 22.04: с внешним веб-интерфейсом управления

1. Подготовка операционной системы

1.1 Установка обновлений ОС

Для обновления ОС Ubuntu необходимо выполнить следующие команды:

```
sudo apt update
```

```
sudo apt upgrade
```

1.2 Подключение репозитория Servicepipe

Подключить репозиторий Servicepipe возможно двумя способами: через скрипт или вручную. Для подключения к репозиторию потребуются логин и пароль. Эти учетные данные предоставляются индивидуально для каждого заказчика. Получить их возможно запросив у вендора (Servicepipe или партнёра).

Подключение с помощью скрипта

Выполнить скрипт для автоматической настройки репозитория:

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

При запуске скрипта потребуется ввести логин и пароль. После ввода учетных данных скрипт выполнит все необходимые действия автоматически. В случае некорректной работы скрипта рекомендуется использовать метод ручной настройки репозитория.

Подключение вручную

Добавить ключ:

```
sudo wget --http-user=[ваш логин] --http-password=[ваш пароль] -O -
https://public-repo.svcp.io/keyFile | \
            sudo gpg --dearmor -o /etc/apt/keyrings/servicepipe.gpg
```

Добавить репозиторий:

```
echo "deb [arch=amd64 signed-by=/etc/apt/keyrings/servicepipe.gpg]
https://public-repo.svcp.io/ubuntu/ xenial contrib" >
/etc/apt/sources.list.d/servicepipe.list
```

Добавить авторизационные данные:

```
echo 'machine public-repo.svcp.io login [ЛОГИН] password [ПАРОЛЬ]' >
/etc/apt/auth.conf
```

Проверить доступность репозитория:

```
sudo apt update
```

1.3 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.

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

При настройке интерфейсов *ifupdown* учесть следующее:

- Удалить настройки интерфейсов из профиля *netplan*, отредактировав файл **/etc/netplan/00-installer-config.yaml**.
- 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
```

1.4 Перезагрузка сервера

Перезагрузить сервер, выполнив команду:

```
sudo reboot
```

2. Установка DosGate

Для установки DosGate следует выполнить следующие действия:

- Установить необходимые библиотеки, выполнив команду:

```
sudo apt install libdt1=1.2.4-1 libaevent1=0.2.0-3
```

- Установить DosGate 3.5.0, выполнив команду:

```
sudo apt install dosgate=3.5.0-2
```

2.1 Настройка конфигурации

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.
- Все функции ПО используются за счет взаимодействия с командой: `dgctl`

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.

2.1.1 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: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: SCGI

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

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    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-сокет, используемый на файловой системе сервера. В качестве адреса указывается полный путь к сокету.
- tcp — TCP-сокет. 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-сокет (family = unix).
- Если строка содержит символ `:` , предполагается, что это TCP-сокет (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-сокетов. Если указанная группа отсутствует, используется первичная группа пользователя, под которым выполняется процесс (по умолчанию root).

Mode

Режим доступа для UNIX-сокетов, 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 удается отправить в течение указанного времени, операция будет прервана.

2.1.2 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

Тэг	Значение
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*.

2.1.3 Блок *collectd*

```
collectd:
  hostname: dosgate
  period: 10
```

- `hostname` - имя хоста, который будет использоваться для именования 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.

2.1.4 Примеры конфигурационного файла dosgate.conf

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

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

  - url: /run/dosgate/fapi.socket
    user: nowhere
    group: www-data
    mode: 0660
    acl: any
    type: FCGI
    timeout:
```

```
      send: 10
      idle: 10

  - url: /run/dosgate/crlf.socket
    user: nowhere:www-data
    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
collectd:
  hostname: dosgate
  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
  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
  period: 10
```

2.2 Однократный запуск DosGate

Однократный запуск DosGate выполняется с целью проверки корректности заполнения конфигурационного файла и отсутствия ошибок. Выполнить следующую команду:

```
sudo dosgate -o -l err
```

где:

- `o` — режим однократного запуска (one-shot mode);
- `l err` — параметр, задающий уровень логирования.

Описание уровней логирования:

Уровень	Описание
debug	Отладочная информация. Подробные сведения о действиях процесса, включая системные и библиотечные вызовы.
info	Стандартная информация о работе процесса. Сообщает, например, об открытии файлов без деталей о внутренних вызовах.
warn	Предупреждения о нарушениях нормальной работы процесса без его остановки.
err	Ошибки, приводящие к нарушению нормальной работы объекта.
crit	Критические ситуации, угрожающие стабильности системы.

Детали запуска рекомендуется просмотреть в логах сервиса:

```
sudo systemctl status dosgate
```

2.3 Логирование работы сервисов dosgate и dosgate-uh

Сервисы *dosgate* и *dosgate-uh* осуществляют логирование работы системы в зависимости от выбранного режима. Логирование ведется в *service log* и доступно для просмотра с использованием команд:

```
ssh journalctl -xefu dosgate
```

```
journalctl -xefu dosgate-uh
```

Поддерживаются три режима логирования:

debug – детализированное логирование, фиксируются практически все действия системы, включая обработку каждого сетевого пакета.
error – запись только сообщений об ошибках.
crit – запись только критических ошибок.

Содержание логов зависит от выбранного режима. Для минимизации нагрузки на систему рекомендуется использовать режим **crit** и контролировать состояние сервиса.

2.4 Настройка ротации логов

Открыть файл **/etc/systemd/journald.conf**:

```
sudo nano /etc/systemd/journald.conf
```

Раскомментировать и задать параметры:

```
SystemMaxUse=500M
RuntimeMaxUse=200M
MaxRetentionSec=1day
```

Перезапустить службу:

```
sudo systemctl restart systemd-journald
```

Открыть файл **/etc/logrotate.d/rsyslog**:

```
sudo nano /etc/logrotate.d/rsyslog
```

Рекомендуемая конфигурация:

```
/var/log/syslog
/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
        rotate 2
        size 500M
        missingok
        notifempty
        compress
        delaycompress
        sharedscripts
        postrotate
                /usr/lib/rsyslog/rsyslog-rotate
        endscript
}
```

Открыть файл **/etc/mongod.conf**:

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

Установить уровень логирования *0*:

```
systemLog:
  verbosity: 0       # Уровень логирования (0-5)
```

Перезапустить службу:

```
sudo systemctl restart mongod
```

Открыть файл **/etc/clickhouse-server/config.xml**:

```
sudo nano /etc/clickhouse-server/config.xml
```

Установить уровень логирования *information*

```
<level>information</level>
```

Перезапустить службу:

```
sudo systemctl restart clickhouse-server
```

3. Настройка инструментов визуализации

Процесс включает два этапа:

1 - Установка и конфигурация collectd для сбора аналитики и метрик.

> Collectd — это системный демон, предназначенный для сбора метрик производительности и ресурсов. Collectd может собирать и агрегировать данные в реальном времени, отправляя их в систему мониторинга для дальнейшего анализа и визуализации.

> DosGate предоставляет метрики по всей системе, охватывая различные уровни обработки трафика:

- **Статистика по аренам** – включает направление обработки трафика внутри сетевых интерфейсов и всех профилей, размещенных в арене.
- **Статистика по профилям** – собирается для каждого профиля, расположенного в пределах арен.
- **Статистика по меткам** – формируется для каждой метки статистики, добавленной через действие `-j STATS` до терминального действия (например, `-j DROP`). Метки статистики позволяют детализировать причины сброса или пропуска определенных типов сетевых пакетов.

Передаваемые значения метрик:

`drop` – объем сброшенного трафика.
`accept` (для профилей) / transmit (для арен) – объем пропущенного трафика до конечного получателя.
`pass` – объем трафика, переданного в операционную систему.
`reply` – ответы DosGate на входящие пакеты вместо конечного получателя (например, в рамках TCP-авторизации).
`error` – объем трафика, сброшенного из-за несоответствия IP RFC или другим встроенным проверкам.

Каждая метрика передается в двух форматах:

- BPS (бит в секунду).
- PPS (пакетов в секунду).

2 - Установка и настройка локального Graphite или интеграция внешнего Graphite с collectd.

> После конфигурации collectd настраивается система визуализации. Варианты включают развертывание локального экземпляра Graphite для хранения и отображения метрик или настройку collectd для передачи собранных данных на внешний сервер Graphite.

3.1 Установка collectd

Установить collectd, используя команду:

```
sudo apt install collectd=5.12.0-10ubuntu0.1
```

3.1.1 Настройка collectd

Для настройки следует открыть файл **/etc/collectd/collectd.conf**.

Файл должен содержать только указанную информацию:

```
FQDNLookup true
TypesDB "/usr/share/collectd/types.db"

LoadPlugin logfile
LoadPlugin syslog
```

```
<Plugin logfile>
        LogLevel "info"
        File STDOUT
        Timestamp true
        PrintSeverity false
</Plugin>

<Plugin syslog>
        LogLevel info
</Plugin>

<Include "/etc/collectd/collectd.conf.d">
        Filter "*.conf"
</Include>
```

Далее, открыть файл **/etc/collectd/collectd.conf.d/dosgate.conf**. Поскольку используется внешний интерфейс управления, замените стандартное значение параметра `Host (127.0.0.1)` на IP-адрес внешнего сервера Graphite.

```
LoadPlugin write_graphite
<Plugin write_graphite>
        <Node "localhost">
                Host "127.0.0.1" ## Заменить на IP-адрес внешнего сервера
Graphite
                Port "2003"
                Protocol "tcp"
        </Node>
</Plugin>

LoadPlugin unixsock
<Plugin unixsock>
        SocketFile "/var/run/collectd-unixsock"
        SocketPerms "0660"
        DeleteSocket false
</Plugin>

TypesDB "/etc/collectd/collectd.conf.d/dosgate-types.db"
```

Далее, открыть файл **/etc/collectd/collectd.conf.d/dosgate-types.db**. Файл должен содержать только указанную информацию:

```
dgstats         packets:COUNTER:0:U     bytes:COUNTER:0:U
```

3.1.2 Запуск collectd

Для запуска collectd необходимо выполнить следующие шаги:

Перезапустить службу, используя команду:

```
sudo systemctl restart collectd
```

Проверить, что всё запустилось корректно, используя команду:

```
sudo systemctl status collectd
```

Включить автозапуск службы:

```
sudo systemctl enable collectd
```

3.1.3 Добавление collectd в конфигурационный файл DosGate

> **Внимание!**
> Данный пункт 3.1.3 полностью дублирует 2.1.3. Допустимо его пропустить, если настройка блока collectd уже производилась в пункте 2.1.3.

Открыть конфигурационный файл **/etc/dosgate.conf**. Добавить в него следующую информацию:

```
collectd:
  hostname: dosgate
  period: 10
```

- При установке DosGate в кластере, необходимо убедиться, что его hostname является уникальным для платформы.

3.1.4 Внесение изменений в DosGate после настройки collectd

Перезагрузить службу DoSGate:

```
sudo systemctl restart dosgate
```

Проверить записи метрик, выполнив команду:

```
sudo systemctl status dosgate
```

Лог должен содержать сообщение:

```
[dg_collectd_sender.c:70, GLOB] Collectd send success
```

Необходимо изменить уровень логирования, поскольку текущая конфигурация генерирует избыточные и подробные логи, что приводит к перегрузке диска. Рекомендуется установить уровень логирования на crit, чтобы фиксировать только критически важные события.

Открыть конфигурационный файл `dosgate.service`, используя команду:

```
sudo nano /etc/systemd/system/dosgate.service
```

или

```
sudo nano /usr/lib/systemd/system/dosgate.service
```

Заменить строку `ExecStart=dosgate -f` на `ExecStart=dosgate -f -l crit`.

Примечание
Пути к systemd-юнитам могут отличаться в зависимости от системы и версии программного обеспечения. Перед редактированием или созданием юнита убедитесь, что нужный файл существует и найдено его точное расположение.

Чтобы проверить это, выполните команду: `sudo systemctl status имя-юнита`

Применить изменения:

```
sudo systemctl daemon-reload
```

Запустить службу DosGate:

```
sudo systemctl start dosgate
```

Убедиться, что служба запустилась корректно, выполнив команду:

```
sudo systemctl status dosgate
```

Активировать автозагрузку сервиса DosGate:

```
systemctl enable dosgate
```

3.2 Установка Graphite

3.2.1 Установка Docker

Docker — это платформа, которая помогает запускать приложения в изолированных средах, называемых контейнерами. Эти контейнеры содержат всё необходимое для работы приложения, что делает его проще в установке и запуске на разных компьютерах.

Добавить ключ GPG для Docker:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
```

Изменить права доступа к ключу:

```
sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

Добавить официальный репозиторий Docker в список источников APT:

```
echo \
  "deb [arch="$(dpkg --print-architecture)" signed-
by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu \
  "$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

Обновить список пакетов и установить Docker с помощью следующих команд:

```
sudo apt update
```

```
sudo apt install docker-ce docker-ce-cli containerd.io
```

Добавить пользователя в группу Docker:

```
sudo usermod -aG docker $USER
```

Убедиться, что Docker установлен и работает, запустив следующую команду:

```
docker version
```

Проверить, что служба Docker запущена, с помощью команды:

```
sudo systemctl status docker
```

3.2.2 Установка контейнера Graphite

Создать директории, которые будут использоваться контейнером Graphite для хранения данных, логов, конфигурации и настроек:

```
sudo mkdir -p /data/graphite/{data,logs,conf,statsd_config}
```

3.2.3 Добавление Graphite в systemd

Отредактируйте файл службы graphite-docker.service:

```
sudo nano /etc/systemd/system/graphite-docker.service
```

Вставьте следующее содержимое в файл:

```
[Unit]
Description=Graphite Docker Container
Documentation=https://github.com/graphite-project/docker-graphite-statsd
After=docker.service
Requires=docker.service

[Service]
Type=simple
TimeoutStartSec=0
Restart=on-failure
RestartSec=30s
ExecStartPre=-/usr/bin/docker kill graphite
ExecStartPre=-/usr/bin/docker rm graphite
ExecStartPre=/usr/bin/docker pull graphiteapp/graphite-statsd
ExecStart=/usr/bin/docker run \
            --name graphite \
            --restart=always \
            -p 8080:80 \
            -p 2003-2004:2003-2004 \
            -p 2023-2024:2023-2024 \
            -p 8125:8125/udp \
            -p 8126:8126 \
            -v /data/graphite/data:/opt/graphite/storage \
            -v /data/graphite/conf:/opt/graphite/conf \
            -v /data/graphite/statsd_config:/opt/statsd/config \
            -v /data/graphite/logs:/var/log \
            graphiteapp/graphite-statsd

SyslogIdentifier=graphite
ExecStop=/usr/bin/docker stop graphite

[Install]
WantedBy=multi-user.target
```

3.2.4 Запуск Graphite

Обновить конфигурацию systemd:

```
sudo systemctl daemon-reload
```

Активировать службу для автозапуска:

```
sudo systemctl enable graphite-docker
```

Запуск службы Graphite:

```
sudo systemctl start graphite-docker.service
```

Проверить статус службы, с помощью команды:

```
sudo systemctl status graphite-docker.service
```

3.2.5 Настройка Graphite

Необходимо установить диапазон хранения Graphite в 10 секунд вместо 1 минуты (стандартное значение после установки) для более точной статистики.

Откройте файл `storage-schemas.conf` для редактирования:

```
sudo nano /data/graphite/conf/storage-schemas.conf
```

Добавить следующую конфигурацию в начало файла перед другими записями:

```
[default]
pattern = .*
retentions = 10s:14d,60s:365d
```

Сохраните изменения и закройте файл.

3.2.6 Перезапуск и очистка данных

Остановить службу Graphite перед удалением старых данных:

```
sudo systemctl stop graphite-docker
```

Удалить старые данные из папки dosgate:

```
sudo rm -rf /data/graphite/data/whisper/dosgate
```

Перезапустить службы Graphite:

```
sudo systemctl start graphite-docker
```

3.2.7 Формат хранения данных в Graphite

DosGate имеет следующую вложенность при хранении данных в Graphite:

`hostname.arena|profile.stats.bytes|packets`

hostname - Задается в конфигурационном файле dosgate.conf в блоке collectd.

arena - Задается в конфигурационном файле dosgate.conf, в блоке arenas, атрибут `name`.

profile - Профиль защиты,задаваемый системным администратором при настройке DoSGate.

stats - Это действия, происходящие с трафиком, которые отображают его состояние и обработку. Возможные действия:

`drop` - Трафик сброшен как результат правила `-j DROP`.

`accept` - Трафик принят и отправлен согласно настройкам dosgate.conf, без сброса.

`pass` - Трафик передан операционной системе как результат правила `-j PASS`.

`reply` - DosGate отвечает на пакет вместо конечного получателя. Это применяется при TCP авторизации для проверки IP-спуфинга, когда DosGate отправляет пакет с флагом RST или с некорректным значением последовательности (Sequence) для верификации отправителя.

`error` - Пакет не обработан из-за несоответствия стандартам IP RFC или потому, что DosGate не смог его корректно разобрать (например, пакет поврежден).

`-j STATS name` - сбор статистики по указанной метке. Это настраивается администратором при создании правила и позволяет отслеживать статистику конкретного правила. Например, правило: `-m protocol udp -j STATS udp_packets`, `-j DROP` будет сбрасывать все пакеты UDP и собирать статистику по этим пакетам и их объему.

bytes - Статистика объема данных в байтах. Для перевода в биты умножьте значение на 8.

packets - Статистика количества переданных пакетов.

4. Установка веб-интерфейса

4.1 Архитектурные особенности

Веб-интерфейс SP-Spider предназначен для упрощения и автоматизации управления кластером DosGate, обеспечивая операторам удобный доступ к настройкам системы через визуальный интерфейс. С его помощью можно вводить новые правила, редактировать существующие, применять заранее настроенные пресеты, а также отслеживать состояние кластера и статистику работы в режиме реального времени.

Веб-интерфейс SP-Spider и ноды DosGate могут быть развернуты в различных архитектурных конфигурациях в зависимости от требований заказчика. Интерфейс поддерживает аппаратное резервирование и кластеризацию, обеспечивая работу в режиме active-active для повышения доступности и отказоустойчивости. Подробное описание различных архитектур доступно в разделе Архитектуры инсталляций.

Компоненты системы
Для работы веб-интерфейса используются следующие компоненты:

- **SP-Spider** — это веб-интерфейс, предназначенный для управления и настройки программного обеспечения DosGate.
- **SP-Spider-Broker** - выступает в роли брокера синхронизации для DosGate.
- **Node.js**: Среда выполнения для веб-интерфейса, обеспечивающая его основную функциональность.
- **PostgreSQL**: Реляционная база данных для хранения конфигурационных данных и правил.

- **RabbitMQ**: Брокер сообщений, обеспечивающий синхронизацию и обработку очередей сообщений.

4.2 Инструкция по установке и настройке компонентов

4.2.1 Установка обновления операционной системы

Выполнить команду для обновления списка пакетов:

```
sudo apt-get update
```

Обновить установленные пакеты:

```
sudo apt-get upgrade
```

4.2.2 Установка Node.js

Выполнить команду для установки NodeJS:

```
sudo apt install nodejs=18.18.2-1nodesource1
```

4.2.3 Установка PostgreSQL

Установить PostgreSQL и библиотеку для работы с ней:

```
sudo apt install -y libpq-dev postgresql
```

4.2.4 Настройка PostgreSQL

Для предоставления доступа к серверу PostgreSQL для внешних подключений необходимо открыть файл конфигурации для редактирования:

```
sudo nano /etc/postgresql/14/main/postgresql.conf
```

В разделе **CONNECTIONS AND AUTHENTICATION** следует изменить параметр:

```
listen_addresses = '*'
```

Параметр *listen_addresses* определяет, на каких IP-адресах сервер будет принимать подключения. Значение `'*'` означает, что сервер будет слушать подключения на всех доступных сетевых интерфейсах. По умолчанию в *listen_addresses* установлено значение `'localhost'`, что ограничивает подключения только локальной машиной.

При использовании внешнего веб-интерфейса необходимо разрешить подключения к узлам, на которых развернуты компоненты DosGate. Для управления подключениями к серверу PostgreSQL используется файл конфигурации **pg_hba.conf**.

Открыть файл конфигурации для редактирования:

```
sudo nano /etc/postgresql/14/main/pg_hba.conf
```

В файл необходимо добавить следующие строки, заменив `X.X.X.X/32` на фактические IP-адреса серверов DosGate:

```
host    all             all             127.0.0.1/32            scram-sha-256
host    all             all             X.X.X.X/32              scram-sha-256
host    all             all             Y.Y.Y.Y/32              scram-sha-256
```

Проверить наличие записи командой:

```
cat /etc/postgresql/14/main/pg_hba.conf | grep "host    all             all
127.0.0.1/32            scram-sha-256"
```

Создать базу данных и пользователя:

```
sudo -u postgres psql
```

Выполнить команды в консоли PostgreSQL:

```
CREATE DATABASE dosgate;
```

```
CREATE USER dosgate WITH ENCRYPTED PASSWORD 'password';
```

```
GRANT ALL PRIVILEGES ON DATABASE dosgate TO dosgate;
```

```
\q
```

4.2.5 Установка RabbitMQ

Создать скрипт установки:

```
sudo nano quickrabbitmq.sh
```

Вставить в скрипт следующий код:

```
#!/bin/sh

sudo apt-get install curl gnupg apt-transport-https -y

## Team RabbitMQ's main signing key
curl -1sLf "https://keys.openpgp.org/vks/v1/by-
fingerprint/0A9AF2115F4687BD29803A206B73A36E6026DFCA" | sudo gpg --dearmor |
sudo tee /usr/share/keyrings/com.rabbitmq.team.gpg > /dev/null
## Community mirror of Cloudsmith: modern Erlang repository
curl -1sLf https://ppa1.novemberain.com/gpg.E495BB49CC4BBE5B.key | sudo gpg --
dearmor | sudo tee /usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg >
/dev/null
## Community mirror of Cloudsmith: RabbitMQ repository
curl -1sLf https://ppa1.novemberain.com/gpg.9F4587F226208342.key | sudo gpg --
```

```
dearmor | sudo tee /usr/share/keyrings/rabbitmq.9F4587F226208342.gpg >
/dev/null

## Add apt repositories maintained by Team RabbitMQ
sudo tee /etc/apt/sources.list.d/rabbitmq.list <<EOF
## Provides modern Erlang/OTP releases
##
deb [signed-by=/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-erlang/deb/ubuntu jammy main
deb-src [signed-by=/usr/share/keyrings/rabbitmq.E495BB49CC4BBE5B.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-erlang/deb/ubuntu jammy main

## Provides RabbitMQ
##
deb [signed-by=/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-server/deb/ubuntu jammy main
deb-src [signed-by=/usr/share/keyrings/rabbitmq.9F4587F226208342.gpg]
https://ppa1.novemberain.com/rabbitmq/rabbitmq-server/deb/ubuntu jammy main
EOF

## Update package indices
sudo apt-get update -y

## Install Erlang packages
sudo apt-get install -y erlang-base \
                        erlang-asn1 erlang-crypto erlang-eldap erlang-ftp
erlang-inets \
                        erlang-mnesia erlang-os-mon erlang-parsetools erlang-
public-key \
                        erlang-runtime-tools erlang-snmp erlang-ssl \
                        erlang-syntax-tools erlang-tftp erlang-tools erlang-
xmerl

## Install rabbitmq-server and its dependencies
sudo apt-get install rabbitmq-server -y --fix-missing
```

Сохранить и закрыть файл. Запустить скрипт для установки RabbitMQ:

```
sudo bash quickrabbitmq.sh
```

4.2.6 Настроика RabbitMQ

Создать пользователя RabbitMQ:

```
sudo rabbitmqctl add_user "username" "password"
```

Назначить права доступа пользователю:

```
sudo rabbitmqctl set_permissions -p "/" "username" ".*" ".*" ".*"
```

4.3 Инструкция по подготовке системы DosGate

4.3.1 Увеличить значение TimeoutStartSec (необязательно)

Если конфигурация содержит более 25 профилей, необходимо увеличить тайм-аут для запуска сервиса DosGate. Необходимо открыть файл конфигурации сервиса:

```
sudo nano /lib/systemd/system/dosgate.service
```

Установить значение `TimeoutStartSec=600`:

```
[Unit]
Description=Dosgate anti-ddos controller
After=network.target
ConditionPathExists=/etc/dosgate.conf

[Service]
Type=notify
ExecStart=dosgate -f -l crit
RuntimeDirectory=dosgate
StateDirectory=dosgate
TimeoutStartSec=600

[Install]
WantedBy=multi-user.target
```

Сохранить изменения и закрыть файл.

4.3.2 Настроить конфигурационный файл dosgate.conf

Проверить, что в файле **/etc/dosgate.conf** настроен параметр FAPI.socket для взаимодействия веб-интерфейса:

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

4.3.3 Добавление сервиса проверки прав FAPI.socket

Установить права для FAPI-сокета:

```
chmod 660 /run/dosgate/fapi.socket
```

Перезапустить службу DosGate, выполнив команду:

```
sudo service dosgate restart
```

Создать новый сервис:

```
sudo nano /etc/systemd/system/fix_fapi.service
```

Вставить следующую конфигурацию в созданный файл:

```
[Unit]
Description=Run fix fapi-socket at startup after all systemd services
After=default.target

[Service]
Type=simple
RemainAfterExit=yes
ExecStart=chmod 660 /run/dosgate/fapi.socket
TimeoutStartSec=0
```

```
[Install]
WantedBy=default.target
```

Сохранить файл, активировать и запустить сервис:

```
systemctl enable --now /etc/systemd/system/fix_fapi.service
```

4.3.4 Заведение SSH-пользователя

Для синхронизации и дополнительных проверок, веб-интерфейс соединяется по SSH с каждой системой-dosgate

Убедитесь что на каждой системе-dosgate есть настроенный SSH-пользователь с доступом к `sudo`.

Создать нового пользователя:

```
sudo adduser dosgate-web
```

Добавить пользователя в группу sudo:

```
sudo usermod -aG sudo dosgate-web
```

Убедиться, что авторизация по SSH через пароль разрешена для этого пользователя.

4.3.5 Настроика NGINX

Если Graphite установлен через Docker, важно учитывать некоторые особенности настройки портов и конфигурации.

По умолчанию, Graphite, запущенный через Docker, работает на порту 8080 и не задействует основной сервер nginx. Однако, если на платформе имеются другие конфигурации nginx, которые используют порты 80 или 443, это может привести к конфликтам.

Если Graphite запущен на той же аппаратной платформе, необходимо убедиться, что порты 80 и 443 свободны или не используются другими сервисами. Чтобы проверить текущую конфигурацию Graphite, выполнить следующие шаги:

Открыть файл конфигурации nginx для Graphite, используя команду:

```
sudo nano /etc/nginx/sites-available/graphite
```

Если установлен 80 или 443 порт, изменить на 8080 :

```
listen 8080 default_server;
listen [::]:8080 default_server;
```

Примечание
Если в системе используется Grafana, обновите настройки источника данных.

Обновить систему, используя команды:

```
sudo apt update
```

```
sudo apt upgrade
```

Установить NGINX:

```
sudo apt install nginx=1.26.2-1~jammy-servicepipe-20241111.162950.UTC
```

Удалить стандартную конфигурацию NGINX:

```
sudo rm /etc/nginx/sites-available/default /etc/nginx/sites-enabled/default
```

Создать файл конфигурации для FAPI:

```
sudo nano /etc/nginx/sites-available/fapi.conf
```

Вставить следующую конфигурацию:

```
server {
  listen 80 default_server;
  listen [::]:80 default_server;

  server_name REPLACE_ON_DOMAIN_OR_IP;
  root /var/www/html;
  index index.php;

  location /fapi {
    include fastcgi_params;
    fastcgi_pass  unix:/run/dosgate/fapi.socket;
  }

  location /broker {
    rewrite ^/broker(.*)$ $1 break;
    proxy_pass http://localhost:3335;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_cache_bypass $http_upgrade;
  }
}
```

Примечание
Заменить `server_name REPLACE_ON_DOMAIN_OR_IP` на домен или IP-адрес!

Создать ссылку:

```
sudo ln -s /etc/nginx/sites-available/fapi.conf /etc/nginx/sites-enabled
```

Перезапустить NGINX:

```
sudo systemctl restart nginx
```

4.3.6 Настройка сети

Убедитесь, что веб-интерфейс имеет связанность до каждой системы-dosgate.

4.4 Инструкция по установке веб-интерфейса и брокера синхронизации

Установить пакеты веб-интерфейса и брокера синхронизации:

```
sudo apt install sp-spider sp-spider-broker
```

4.4.1 Настройка веб-интерфейса

В зависимости от условий установки необходимо обновить авторизационные данные, порты базы данных и другие параметры в .env-файле. Сначала выполняется настройка веб-интерфейса, затем — брокера.

Открыть для редактирования файл **/opt/sp-spider/.env**:

```
sudo nano /opt/sp-spider/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
VITE_APP_PORT=3333 # Порт на котором будет работать приложение, потребуется
позднее для входа в веб-интерфейс
NODE_ENV=production
HTTP_TIMEOUT=10000

# Если это основной интерфейс (даже при отсутствии резервирования)
IS_PRIMARY=true

# Секретный ключ, соль для паролей. Нежелательно менять после первого запуска
APP_SECRET=salt_salt_salt

# Данные от пользователя и БД postgresql
DB_HOST="localhost"
```

```
DB_PORT="5432"
DB_USER="dosgate"
DB_DATABASE="dosgate"
DB_PASSWORD="password"

# Активация rabbitmq для синхронизации и брокера
RMQ_ENABLE="true"
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"
RMQ_RECONNECT_INTERVAL="5000"
```

Примечание

Использовать AMQPs при необходимости.

Если требуется поддержка TLS замените

```
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"
```

на

```
 RMQ_URL="amqps://USER:PASSWORD@localhost:5672"
```

4.4.2 Настройка брокера

Открыть для редактирования файл **/opt/sp-spider-broker/.env**:

```
sudo nano /opt/sp-spider-broker/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
APP_PORT=3335 # Порт, на котором запустится сервис

# Ключ из .env интерфейса
APP_SECRET="YOUR_APP_SECRET"

# Данные от базы данных из .env интерфейса
DB_HOST="localhost" (или айпи спайдера)
```

```
DB_PORT="5432"
DB_USER="YOUR_DB_USER"
DB_DATABASE="YOUR_DB_NAME"
DB_PASSWORD="YOUR_DB_PASSWORD"

# Данные RabbitMQ из .env интерфейса
RMQ_URL="amqp://USER:PASSWORD@localhost:5672" (или айпишнег спайдера вместо
локалхост)
RMQ_RECONNECT_INTERVAL="5000"

# Путь к папке с политиками DosGate UH. Обязательно в конце ставить "/"
POLICY_PATH="/var/lib/dosgate-uh/profiles/"

# Путь к конфигурации обработчика оффендеров DosGate UH
OFFENDERS_CONF_PATH="/opt/sp-spider-broker/offenders/offenders.conf"

# Путь к объектам защиты Flowcollector. Обязательно в конце ставить "/"
FC_MO_PATH="/opt/spfc/etc/mo/"

# Путь к симлинкам на объекты защиты Flowcollector. Обязательно в конце ставить
"/"
FC_MO_SYMLINK_PATH="/opt/spfc/etc/mo.enabled/"

# Путь к объектам обучения Treshold Learner. Обязательно в конце ставить "/"
FC_LEARNER_PATH="/opt/spfc/etc/learner/"

# Путь к симлинкам на объекты обучения Treshold Learner. Обязательно в конце
ставить "/"
FC_LEARNER_SYMLINK_PATH="/opt/spfc/etc/learner.enabled/"

# Путь к конфигу dosgate-uh
DGUH_CONF="/etc/dosgate-uh.conf"

# Путь к снэпшотам дампов dosgate-uh
DGUH_SNAPSHOTS="/var/cache/dosgate-uh-snapshots"
```

4.4.3 Создание сервиса

Для веб-интерфейса:

Отредактировать файл **/usr/lib/systemd/system/sp-spider.service**:

```
sudo nano /usr/lib/systemd/system/sp-spider.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider

[Service]
ExecStart=/usr/bin/node /opt/sp-spider/server/main.js
WorkingDirectory=/opt/sp-spider
Restart=always

[Install]
WantedBy=multi-user.target
```

Для брокера:

Отредактировать файл **/usr/lib/systemd/system/sp-spider-broker.service**:

```
sudo nano /usr/lib/systemd/system/sp-spider-broker.service
```

Добавить следующую конфигурацию:

```
[Unit]
Description=SP Spider Broker

[Service]
ExecStart=/opt/sp-spider-broker/sp-spider-broker
WorkingDirectory=/opt/sp-spider-broker
Restart=always

[Install]
WantedBy=multi-user.target
```

Активировать и запустить сервисы:

```
sudo systemctl enable --now sp-spider sp-spider-broker
```

Проверить статус всех компонентов:

```
sudo systemctl status sp-spider
```

```
sudo systemctl status sp-spider-broker
```

```
sudo systemctl status rabbitmq-server
```

```
sudo systemctl status postgresql
```

```
sudo systemctl status nginx
```

4.4.4 Настройка веб-интерфейса с использованием протокола HTTPS

Сгенерировать самоподписанный сертификат, заменив значения CN и DNS на соответствующие окружению.

```
openssl req -x509 -out server.crt -keyout server.key \
  -newkey rsa:2048 -nodes -sha256 \
  -subj '/CN=DosGate Web-Interface' -extensions EXT -config <( \
   printf "[dn]\nCN=DosGate Web-Interface\n[req]\ndistinguished_name =
dn\n[EXT]\nsubjectAltName=DNS:server.local\nkeyUsage=digitalSignature\nextendedKe
```

Сохранить сгенерированные файлы *server.crt* и *server.key* в директорию **/etc/certs/**.

Необходимо отредактировать конфигурацию NGINX.
При размещении DosGate и SP-Spider на одной платформе, необходимо скорректировать файл **/etc/nginx/sites-available/fapi.conf**, указав IP-адрес или доменное имя вместо `REPLACE_ON_DOMAIN_OR_IP`.

```
server {
  listen 80;
```

```
  server_name REPLACE_ON_DOMAIN_OR_IP localhost;

  location /fapi {
    include fastcgi_params;
    fastcgi_pass  unix:/run/dosgate/fapi.socket;
  }

  if ($request_uri !~ "/fapi") {
    return 301 https://$server_name$request_uri;
  }
}

server {
  listen 443 default ssl;

  ssl_certificate /etc/certs/server.crt;
  ssl_certificate_key /etc/certs/server.key;

  root /var/www/html;
  index index.php;

  location /broker {
    rewrite ^/broker(.*)$ $1 break;
    proxy_pass http://localhost:3335;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_cache_bypass $http_upgrade;
  }

  location / {
    proxy_pass http://localhost:3333;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  }
}
```

Для применения изменений необходимо перезапустить NGINX:

```
sudo systemctl restart nginx
```

Настроить UFW для ограничения доступа к порту 3333 только с локального интерфейса:

```
sudo ufw allow from 127.0.0.1
```

```
sudo ufw allow from ::1
```

```
sudo ufw deny 3333
```

```
sudo ufw allow in from any
```

```
sudo ufw enable
```

Запустить веб-интерфейс в браузере, перейдя по адресу https://`REPLACE_ON_DOMAIN_OR_IP`. По умолчанию соединение будет установлено через HTTPS.

При необходимости добавить сертификат в доверенные на устройствах конечных пользователей.

4.4.5 Логирование работы сервисов sp-spider

При использовании веб-интерфейса доступен сервис *sp-spider*, который ведет логи взаимодействия с нодами DosGate.

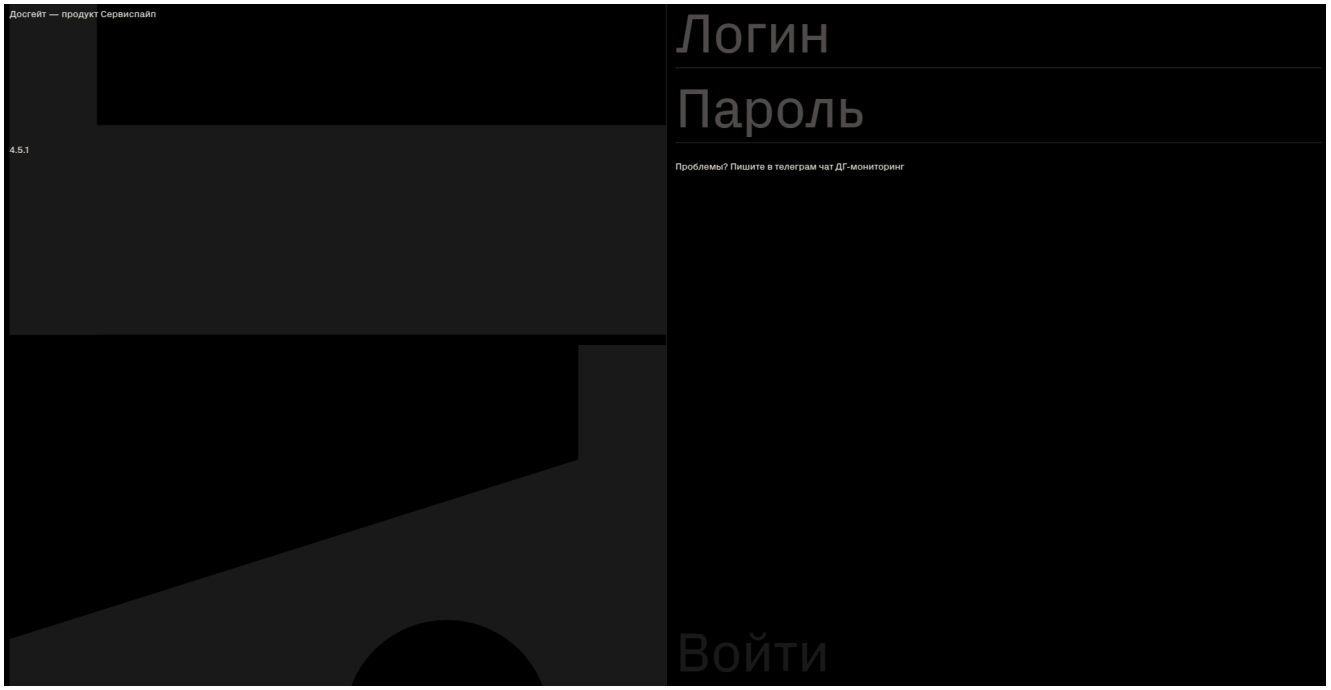
Функции логирования в *sp-spider*:

- Фиксация событий, связанных с подключением к DosGate.
- Отображение ошибок DosGate в реальном времени при успешном соединении.
- Помощь в диагностике. Например, при некорректном формировании правил, которые DosGate не принимает.

5. Первый вход в систему

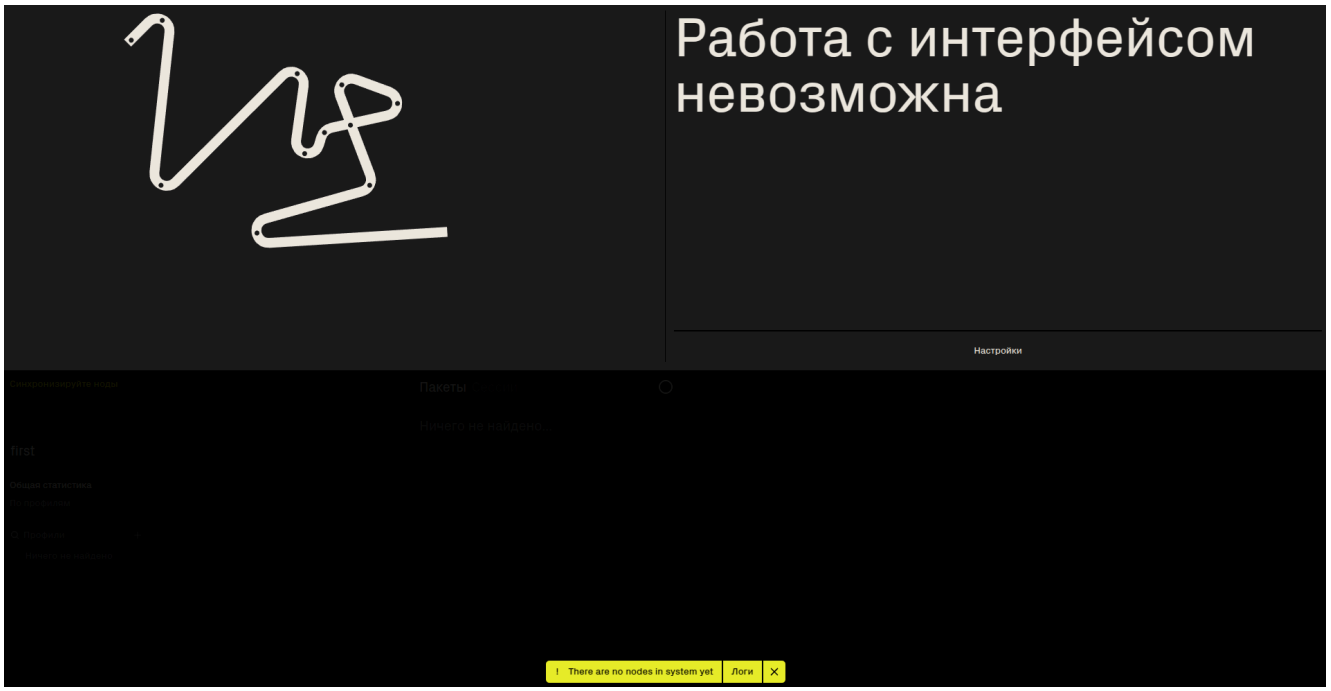
Для входа в Веб-интерфейс DosGate следует ввести в адресной строке браузера IP-адрес и порт по шаблону: `ip:port`. Указать порт, указанный в переменной `VITE_APP_PORT` файла **/opt/sp-spider/.env** в разделе 4.4.1 Настройка веб-интерфейса

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

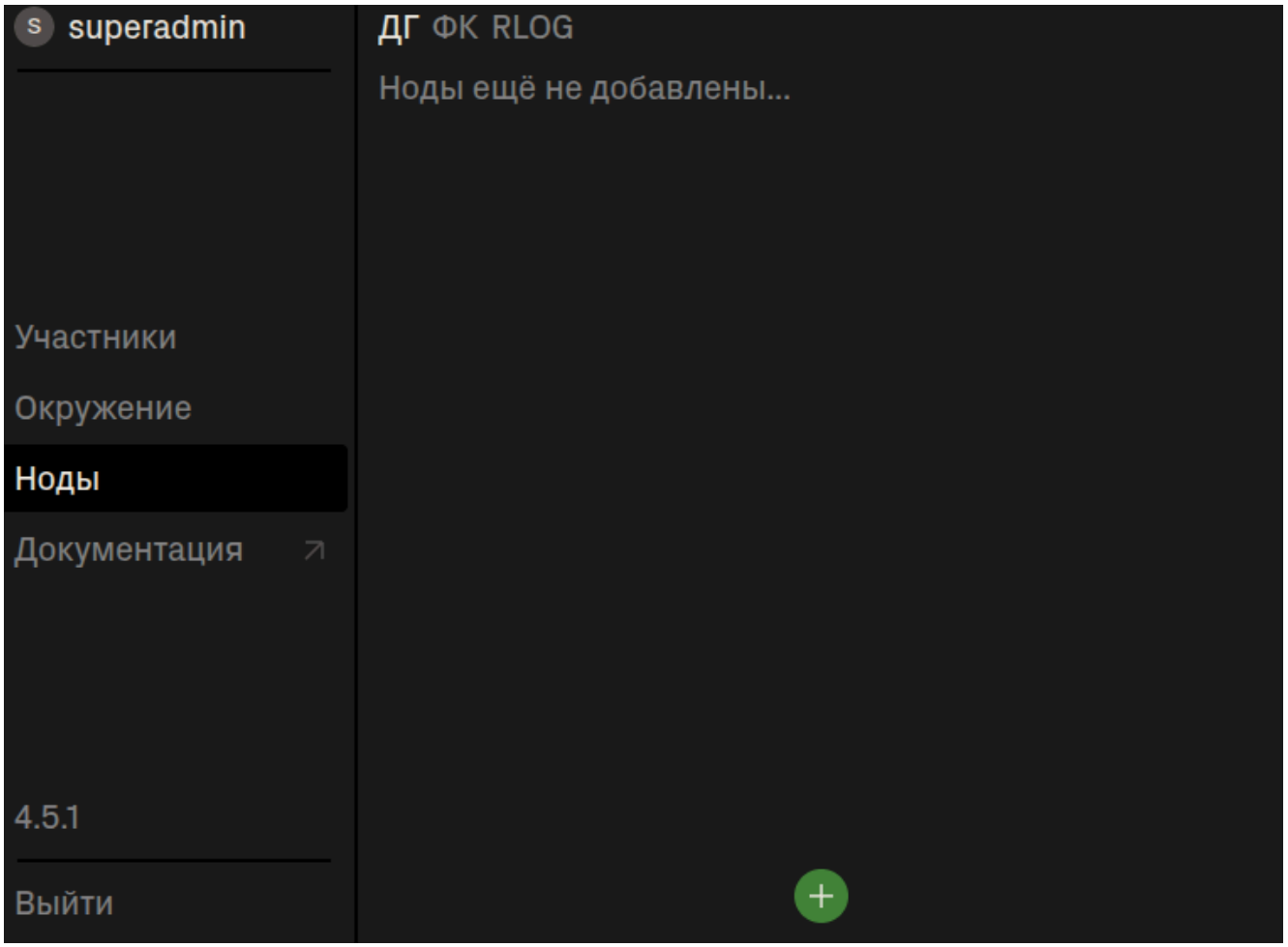


Окно авторизации при входе в систему

После авторизации появится уведомление "Работа с интерфейсом невозможна" (см. рисунок ниже). Это связано с тем, что в данный момент нет настроенной ноды.

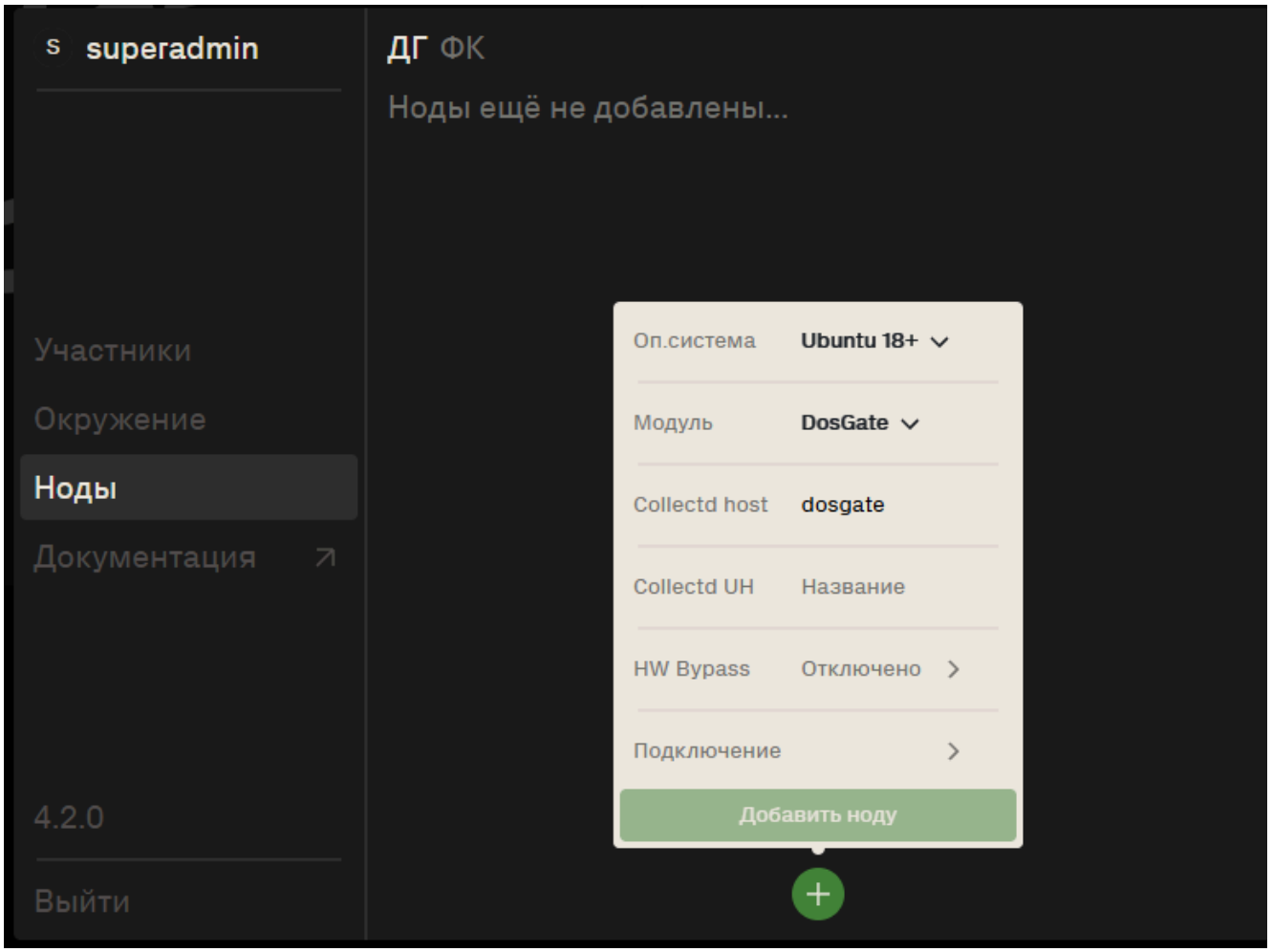


Нажать кнопнку "Настройки". Откроется окно настроек (см. рисунок ниже).

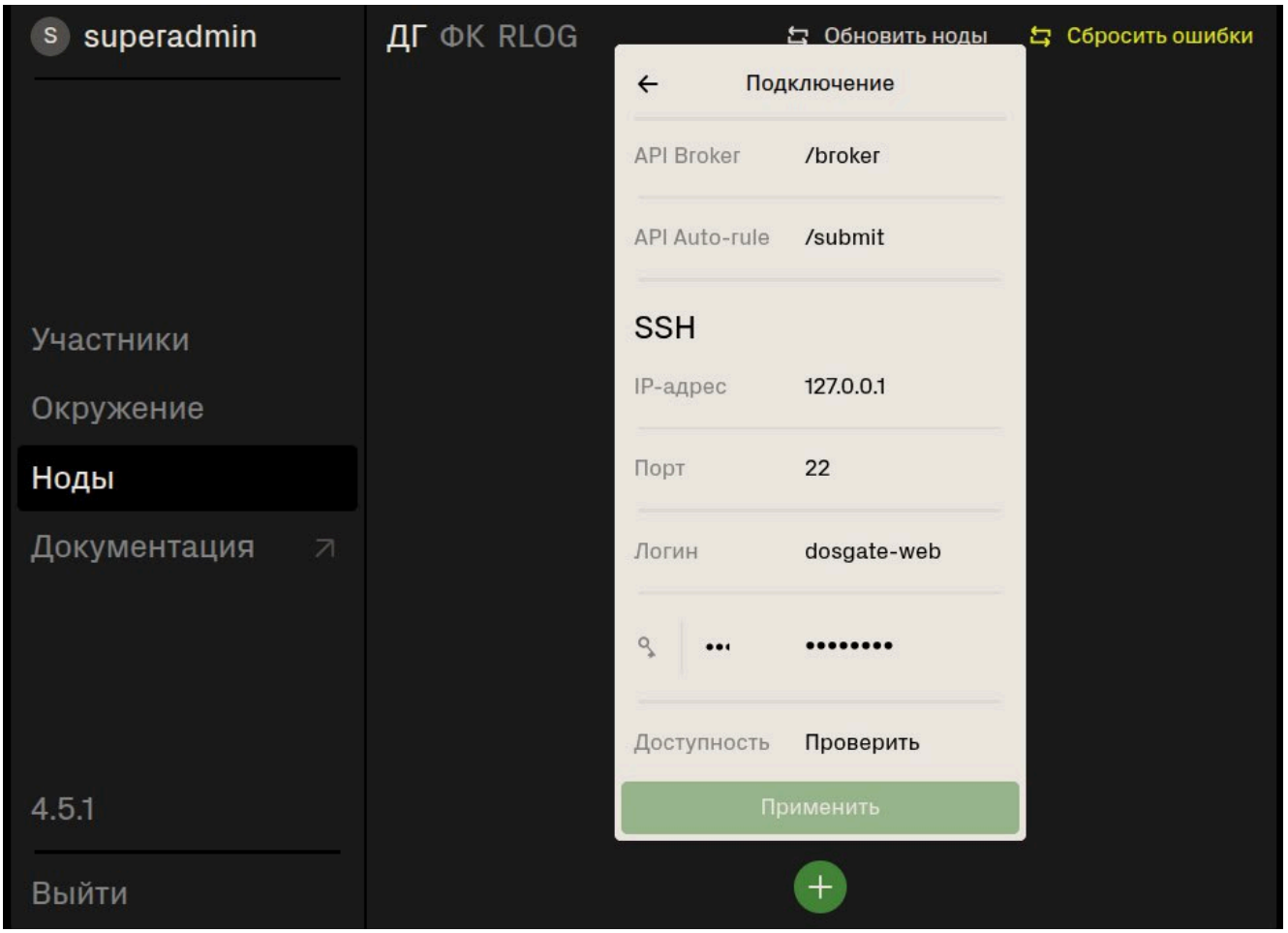


Выбрать меню "Ноды" - нажать на кнопку добавления новой ноды. В открывшимя окне необходимо заполнить "Collectd host". Необходимо использовать hostname, который

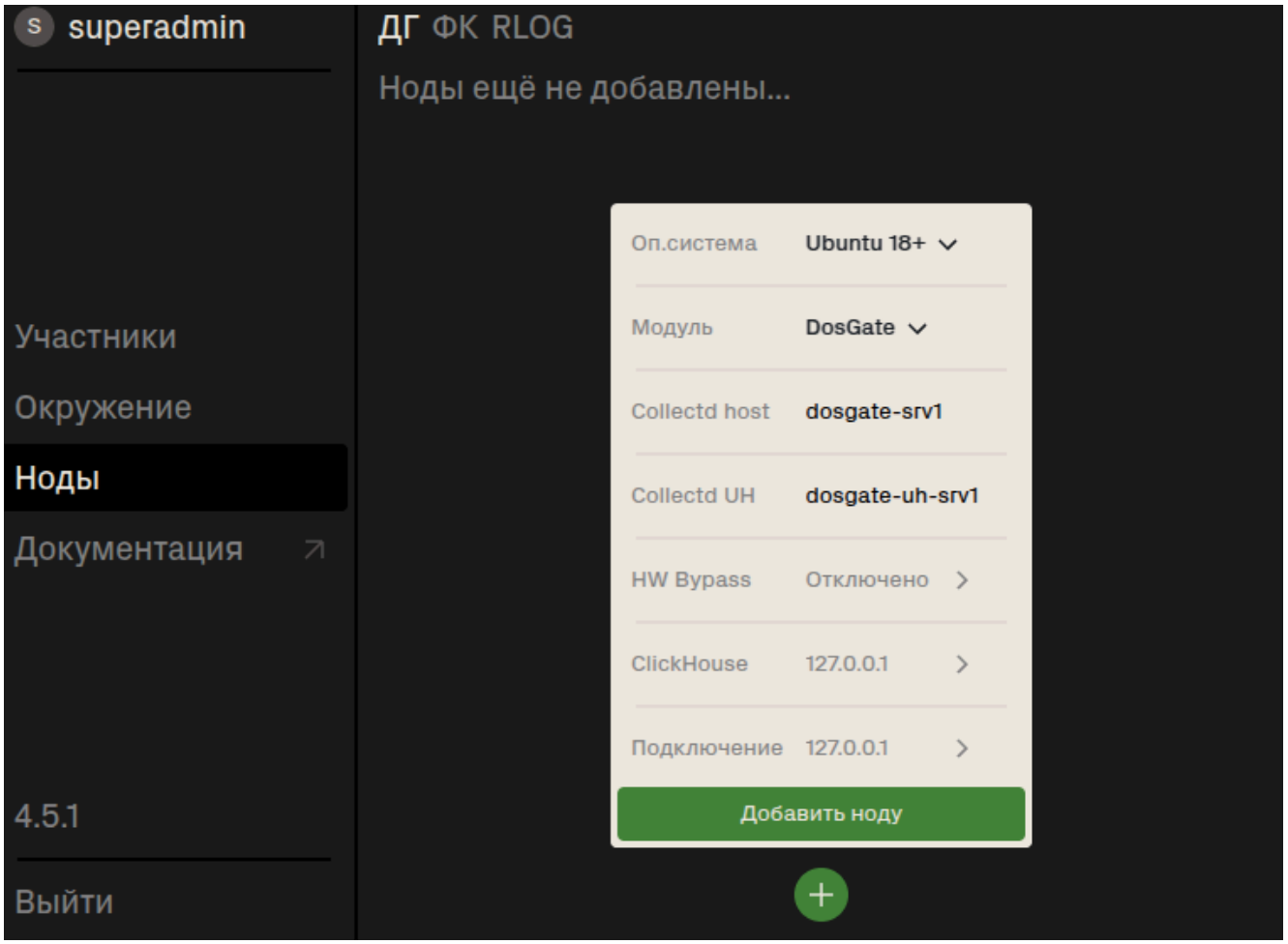
прописан в конфигурационном файле dosgate.conf в блоке *collectd*. Нажать на кнопку "Подключение".



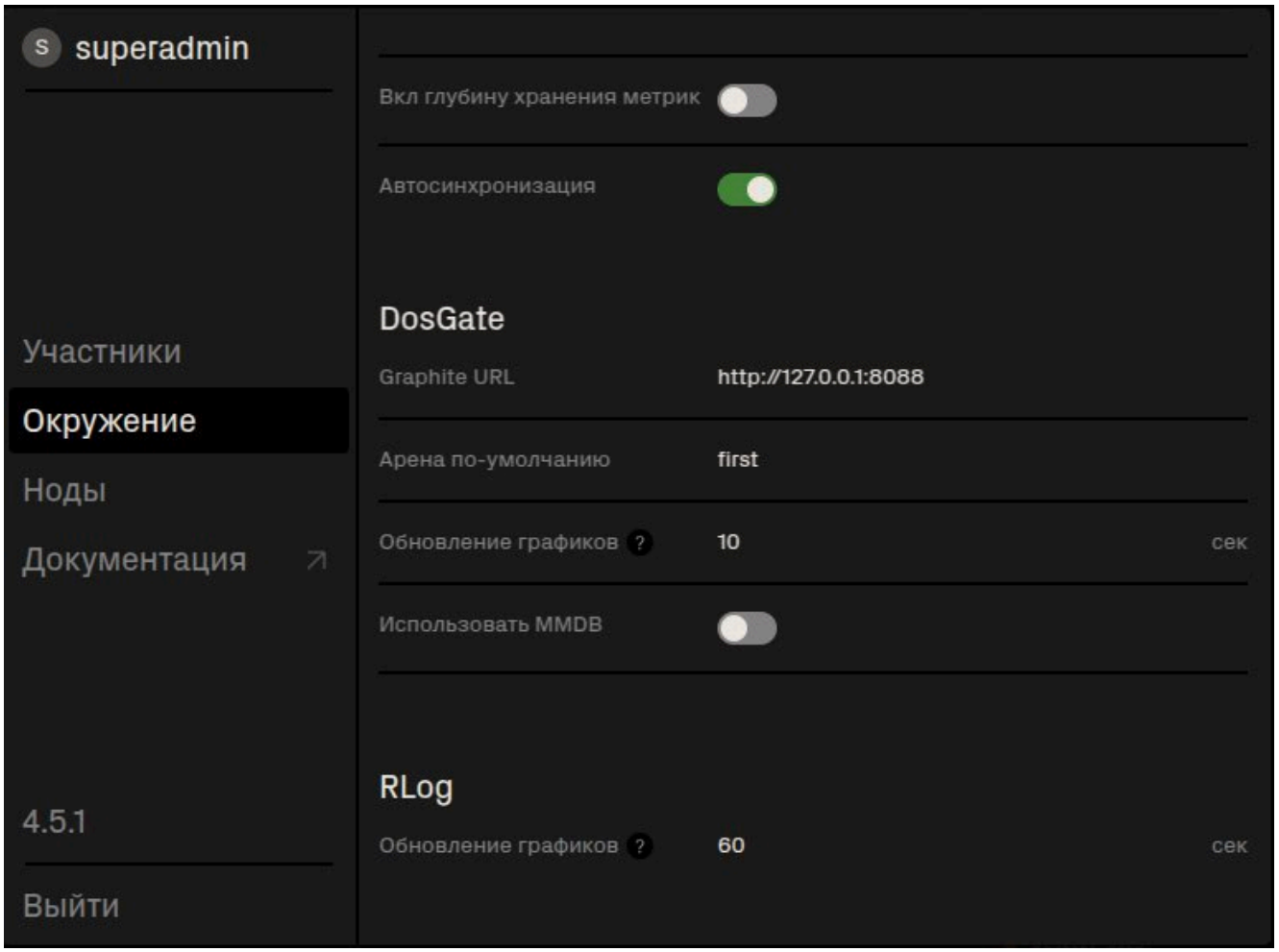
В открывшемся окне указать SSH-данные для подключения к установленной ноде Dosgate (IP-адрес, логин, пароль). Нажать на кнопку "Проверить", чтобы проверить подключение. Если данные введены правильно и нода доступна, статус изменится на "Доступна". После этого нажать кнопку "Применить".



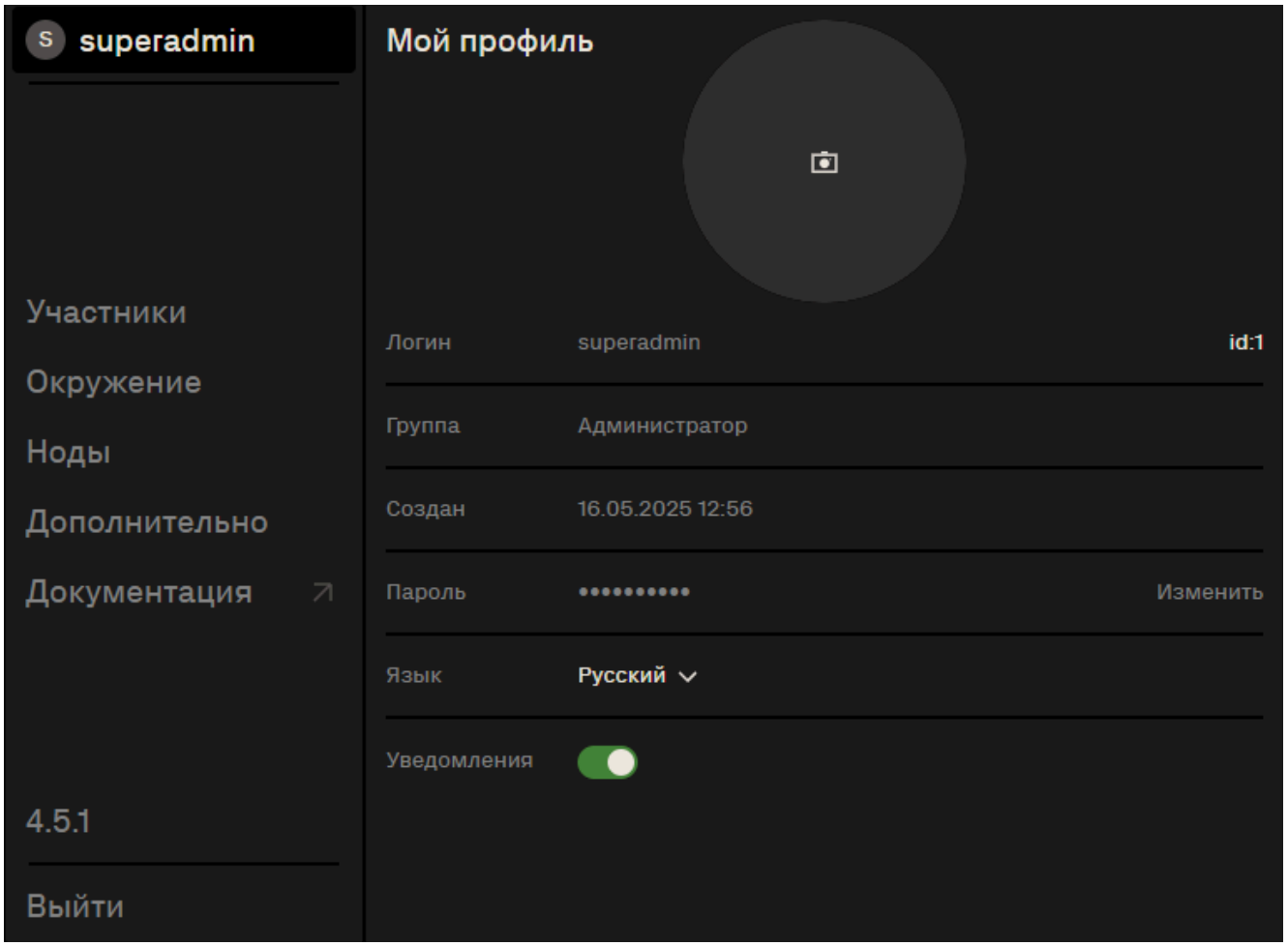
В открывшемся окне нажать "Добавить ноду".



Для отображения графиков и статистики неоьходимо 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.



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



Веб-интерфейс готов к использованию.