Проекты VK WorkSpace

Установка PGBouncer

© VK WorkSpace, 2026 г. Все права защищены

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Шаг 1: Установка PGBouncer 3
Шаг 2: Настройка PGBouncer 3
Шаг 3: Добавление пользователей 5
Шаг 4: Задание LimitNOFILE в файле pgbouncer.service 5

PGBouncer — программа, управляющая пулом соединений PostgreSQL. Любое конечное приложение может подключиться к PGBouncer, как если бы это был непосредственно сервер PostgreSQL. PGBouncer создаст подключение к реальному серверу, либо задействует одно из ранее установленных подключений.

Назначение PGBouncer — минимизировать издержки, связанные с установлением новых подключений к PostgreSQL. Вы также можете ознакомиться с руководством в официальной документации PGBouncer.

Установка состоит из нескольких этапов:

1. Установка PGBouncer
2. Настройка PGBouncer
3. Добавление пользователей
4. Задание LimitNOFILE в файле pgbouncer.service

Шаг 1: Установка PGBouncer

Установите PGBouncer на узел с PostgreSQL, используя следующую команду:

```
sudo apt-get install pgbouncer -y
```

Шаг 2: Настройка PGBouncer

1. Переместите конфигурационный файл по умолчанию:

```
sudo mv /etc/pgbouncer/pgbouncer.ini{,.original}
```

2. Создайте и откройте для редактирования новый конфигурационный файл:

```
sudo nano /etc/pgbouncer/pgbouncer.ini
```

3. Добавьте пример конфигураций в файл:

```
[databases]
postgres = host=127.0.0.1 port=5432 dbname=vkdb
* = host=127.0.0.1 port=5432

[pgbouncer]
logfile = /var/log/postgresql/pgbouncer.log
pidfile = /var/run/postgresql/pgbouncer.pid
listen_addr = *
listen_port = 6432
unix_socket_dir = /var/run/postgresql
auth_type = md5
auth_file = /etc/pgbouncer/userlist.txt
admin_users = postgres
ignore_startup_parameters = extra_float_digits,geqo
pool_mode = session
server_reset_query = DISCARD ALL
max_client_conn = 10000
default_pool_size = 800
reserve_pool_size = 150
reserve_pool_timeout = 1
max_db_connections = 1000
pkt_buf = 8192
listen_backlog = 4096
log_connections = 0
log_disconnections = 0
```

где:

- `listen_addr` — список адресов через запятую, где прослушивать соединения TCP. Если вы установите *, будут прослушивать все адреса;

- `listen_port` — порт для прослушивания, по умолчанию установлено 6432;
- `pool_mode` — режим работы;
- `auth_type` — режим аутентификации пользователей;
- `max_client_conn` — максимально допустимое количество клиентских подключений;
- `default_pool_size` — размер пула открытых подключений к базам данных;
- `reserve_pool_size` — размер резервного пула открытых подключений к базам данных;
- `max_db_connections` — максимально допустимое количество открытых подключений к базам данных
- `[databases]` — определяет имена баз данных, к которым могут подключаться клиенты PgBouncer. Указывает, куда будут маршрутизироваться эти подключения.

Настройка включения TLS/SSL в PGBouncer

Для включения поддержки TLS/SSL в PGBouncer дабавьте в файл конфигурации /etc/pgbouncer/pgbouncer.ini следующие параметры:

client_tls_sslmode — задайте режим работы TLS, выставив require; client_tls_ca_file — укажите путь до файла корневого CA; client_tls_cert_file — укажите путь до файла сертификата сервера; client_tls_key_file — укажите путь до файла закрытого ключа.

```
[databases]
postgres = host=127.0.0.1 port=5432 dbname=vkdb
* = host=127.0.0.1 port=5432

[pgbouncer]
logfile = /var/log/postgresql/pgbouncer.log
pidfile = /var/run/postgresql/pgbouncer.pid
listen_addr = *
listen_port = 6432
unix_socket_dir = /var/run/postgresql
auth_type = md5
auth_file = /etc/pgbouncer/userlist.txt
admin_users = postgres
ignore_startup_parameters = extra_float_digits,geqo
pool_mode = session
server_reset_query = DISCARD ALL
max_client_conn = 10000
default_pool_size = 800
reserve_pool_size = 150
reserve_pool_timeout = 1
max_db_connections = 1000
pkt_buf = 8192
listen_backlog = 4096
log_connections = 0
log_disconnections = 0
client_tls_sslmode = require
client_tls_ca_file = /etc/ssl/certs/rootCA.pem
client_tls_key_file = /etc/ssl/private/selfsigned.key
client_tls_cert_file = /etc/ssl/certs/selfsigned.crt
```

Подробнее о настройке TLS/SSL в PGBouncer читайте в официальной документации PGBouncer.

Шаг 3: Добавление пользователей

Добавьте в файл `/etc/pgbouncer/userlist.txt` имена пользователей и пароли, с которыми PGBouncer подключается к базе. Для этого:

1. Создайте файл `userlist.txt`, выполнив команду:

```
sudo nano /etc/pgbouncer/userlist.txt
```

2. Добавьте в файл `userlist.txt` пользователя и пароль для подключения к PostgreSQL. Пользователь vkuser был ранее создан при развёртывании PostgreSQL.

```
"vk" "SecretPassword"
```

Шаг 4: Задание LimitNOFILE в файле pgbouncer.service

Добавьте в файл сервиса PGBouncer в секцию Service параметр `LimitNOFILE`.

1. Откройте файл `/lib/systemd/system/pgbouncer.service`, выполнив команду:

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

2. Задайте лимит на открытие файлов `LimitNOFILE` равным `15000`.

   Пример добавления LimitNOFILE в pgbouncer.service

```
[Unit]
Description=connection pooler for PostgreSQL
Documentation=man:pgbouncer(1)
Documentation=https://www.pgbouncer.org/
After=network.target
#Requires=pgbouncer.socket

[Service]
Type=notify
User=postgres
ExecStart=/usr/sbin/pgbouncer /etc/pgbouncer/pgbouncer.ini
ExecReload=/bin/kill -HUP $MAINPID
KillSignal=SIGINT
LimitNOFILE=15000

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

3. Перезапустите PGBouncer, выполнив команду:

```
sudo systemctl daemon-reload
sudo systemctl restart pgbouncer
```

Технический писатель: Белова Ирина

12 мая 2026 г.