

7.1 Выделение групп и ролей пользователей

(1) объявление возможных ролей

Согласно моему варианту #7 мы имеем следующие роли пользователей склада:

- **superuser (app_user):** главный администратор [уже существует]
- **ro_users:** аналитики, бухгалтерия, стажеры
- **workers:** работа с записью и чтением актов, товаров, вендоров
- **vendors:** работа с проверкой и чтением актов, товаров

Составим таблицу с описанием ролей

Роль	Название	Привелегии	Описание	SSL
app_user	администратор	OWNER	суперпользователь	+
ro_users	аналитики	CONNECT, REPLICATION, USAGE	пользователь, только для чтения	+
workers	работники склада	CONNECT, PARTIAL USAGE	работа с записью актов, товаров, вендоров	+
vendors	вендоры, компании	CONNECT, PARTIAL USAGE	проверка данных в таблицах акты, товары	+

(2) создание групповых ролей

```
CREATE ROLE ro_users WITH NOLOGIN;  
CREATE ROLE workers WITH NOLOGIN;  
CREATE ROLE vendors WITH NOLOGIN;
```

```
-- изменение ролей  
ALTER ROLE ro_users WITH REPLICATION;  
  
-- возможность подключения  
GRANT CONNECT ON DATABASE wirehouse_db TO ro_users;  
GRANT CONNECT ON DATABASE wirehouse_db TO workers;  
GRANT CONNECT ON DATABASE wirehouse_db TO vendors;
```

(3) создание пользователей

```
CREATE ROLE analytic WITH LOGIN PASSWORD '12345678';
CREATE ROLE economist WITH LOGIN PASSWORD 'eco1234';
CREATE ROLE worker WITH LOGIN PASSWORD 'workwork12';
CREATE ROLE some_company WITH LOGIN PASSWORD '1234';
```

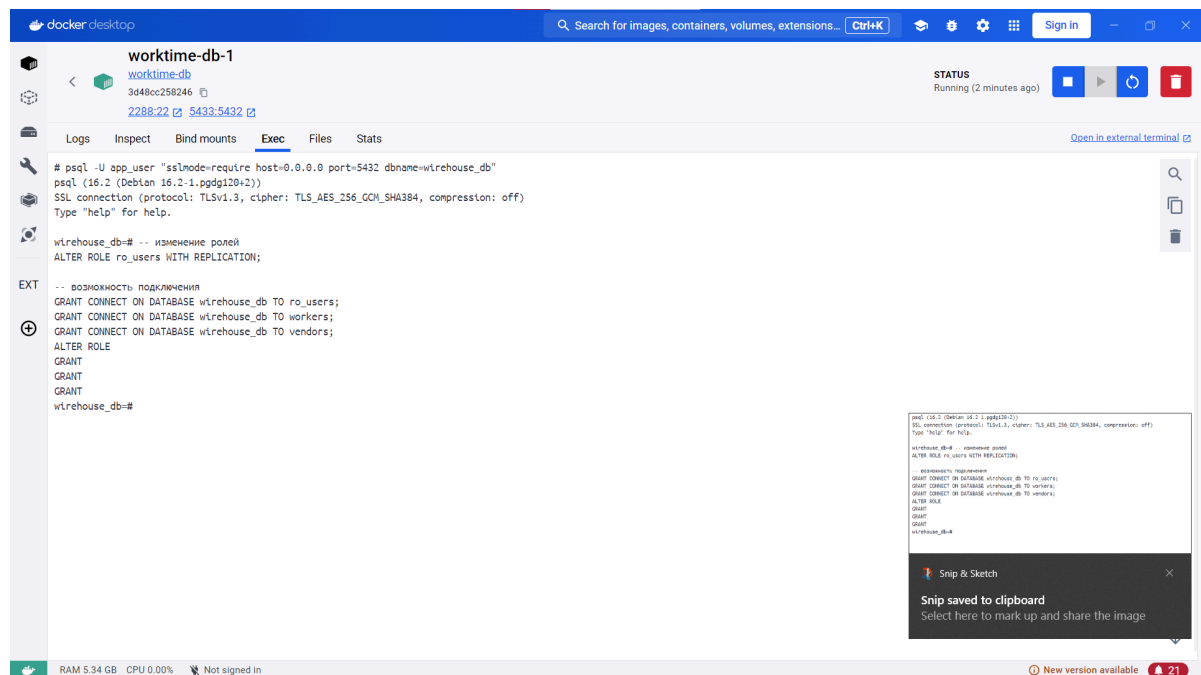
```
-- действие роли компании до конца 2024 года
ALTER ROLE ravi VALID UNTIL '2025-1-1';
```

-- добавление пользователей в группы

```
GRANT ro_users TO analytic;
GRANT ro_users TO economist;
```

```
GRANT workers TO worker;
GRANT vendors TO vendor;
```

(4) Проверка



docker desktop

Search for images, containers, volumes, extensions...

Ctrl+K

Sign in

worktime-db-1

worktime-db

3d48ec258246

2288/22 5433.5432

STATUS

Running (3 minutes ago)

Logs

Inspect

Bind mounts

Exec

Files

Stats

Open in external terminal

SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

wlrehouse_db=# -- изменение ролей
ALTER ROLE ro_users WITH REPLICATION;

-- возможность подключения
GRANT CONNECT ON DATABASE wlrehouse_db TO ro_users;
GRANT CONNECT ON DATABASE wlrehouse_db TO workers;
GRANT CONNECT ON DATABASE wlrehouse_db TO vendors;
ALTER ROLE
GRANT
GRANT
GRANT
wlrehouse_db=# CREATE ROLE analytic WITH LOGIN PASSWORD '12345678';
CREATE ROLE economist WITH LOGIN PASSWORD 'eco1234';
CREATE ROLE worker WITH LOGIN PASSWORD 'workwork12';
CREATE ROLE some_company WITH LOGIN PASSWORD '1234';

-- действие роли компании до конца 2024 года
ALTER ROLE ravi VALID UNTIL '2025-1-1';
CREATE ROLE
CREATE ROLE
CREATE ROLE
CREATE ROLE
ERROR: role "ravi" does not exist
wlrehouse_db=#
ALTER ROLE some_company VALID UNTIL '2025-1-1';
ALTER ROLE
wlrehouse_db=#

RAM 5.33 GB

CPU 1.01%

Not signed in

New version available

21

docker desktop

Search for images, containers, volumes, extensions...

Ctrl+K

Sign in

worktime-db-1

worktime-db

3d48ec258246

2288/22 5433.5432

STATUS

Running (5 minutes ago)

Logs

Inspect

Bind mounts

Exec

Files

Stats

Open in external terminal

GRANT
GRANT
wlrehouse_db=# CREATE ROLE analytic WITH LOGIN PASSWORD '12345678';
CREATE ROLE economist WITH LOGIN PASSWORD 'eco1234';
CREATE ROLE worker WITH LOGIN PASSWORD 'workwork12';
CREATE ROLE some_company WITH LOGIN PASSWORD '1234';

-- действие роли компании до конца 2024 года
ALTER ROLE ravi VALID UNTIL '2025-1-1';
CREATE ROLE
CREATE ROLE
CREATE ROLE
CREATE ROLE
ERROR: role "ravi" does not exist
wlrehouse_db=#
ALTER ROLE some_company VALID UNTIL '2025-1-1';
ALTER ROLE
wlrehouse_db=# -- добавление пользователей в группы
GRANT ro_users TO analytic;
GRANT ro_users TO economist;

GRANT workers TO worker;
GRANT vendors TO vendor;
GRANT ROLE
GRANT ROLE
GRANT ROLE
ERROR: role "vendor" does not exist
wlrehouse_db=# GRANT vendors TO some_company;;
GRANT ROLE
wlrehouse_db=#

RAM 5.33 GB

CPU 0.00%

Not signed in

New version available

21

docker desktop

Search for images, containers, volumes, extensions...

Ctrl+K

Sign in

worktime-db-1

worktime-db

3d48ec258246

2288/22 5433.5432

STATUS

Running (8 minutes ago)

Logs

Inspect

Bind mounts

Exec

Files

Stats

Open in external terminal

-- действие роли компании до конца 2024 года
ALTER ROLE ravi VALID UNTIL '2025-1-1';
CREATE ROLE
CREATE ROLE
CREATE ROLE
CREATE ROLE
ERROR: role "ravi" does not exist
wlrehouse_db=#
ALTER ROLE some_company VALID UNTIL '2025-1-1';
ALTER ROLE
wlrehouse_db=# -- добавление пользователей в группы
GRANT ro_users TO analytic;
GRANT ro_users TO economist;

GRANT workers TO worker;
GRANT vendors TO vendor;
GRANT ROLE
GRANT ROLE
GRANT ROLE
ERROR: role "vendor" does not exist
wlrehouse_db=# GRANT vendors TO some_company;;
GRANT ROLE
wlrehouse_db=# SELECT * FROM pg_catalog.pg_user;
username | usesysid | usecreatedb | usesuper | use repl | usebypassrls | passwd | valuntil | useconfig

app_user | 10 | t | t | t | t | ***** | |
analytic | 32804 | f | f | f | f | ***** | |
economist | 32805 | f | f | f | f | ***** | |
worker | 32806 | f | f | f | f | ***** | |
some_company | 32807 | f | f | f | f | ***** | 2025-01-01 00:00:00+00 |
(5 rows)
wlrehouse_db=#

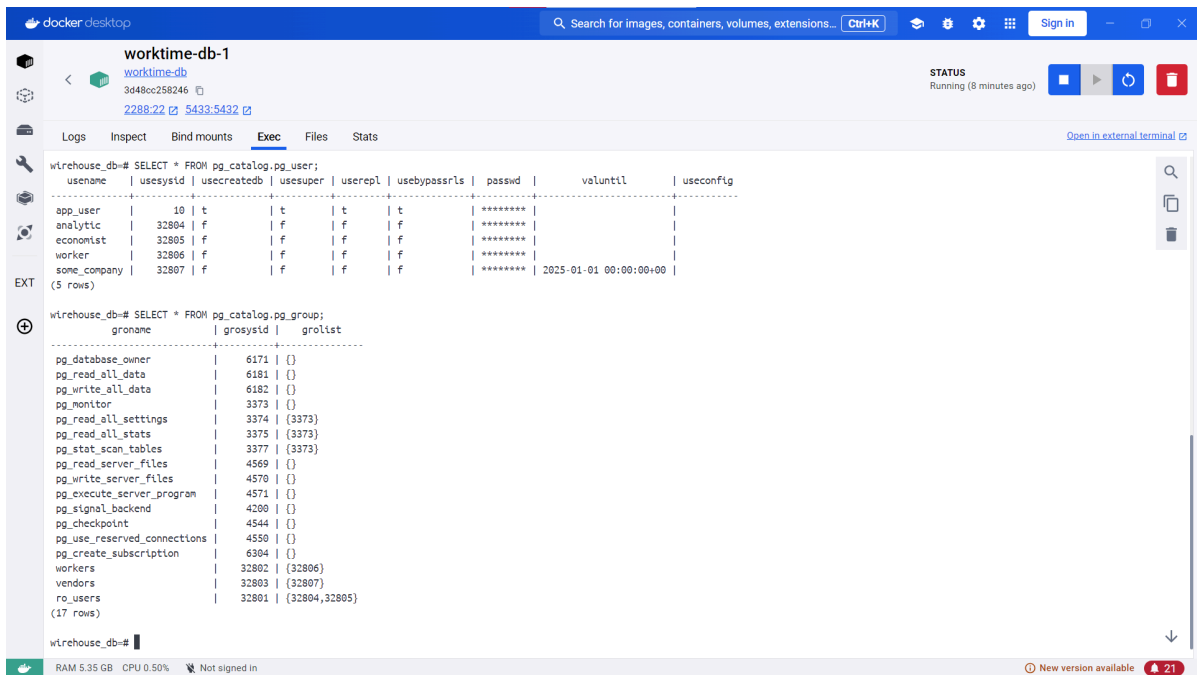
RAM 5.34 GB

CPU 0.13%

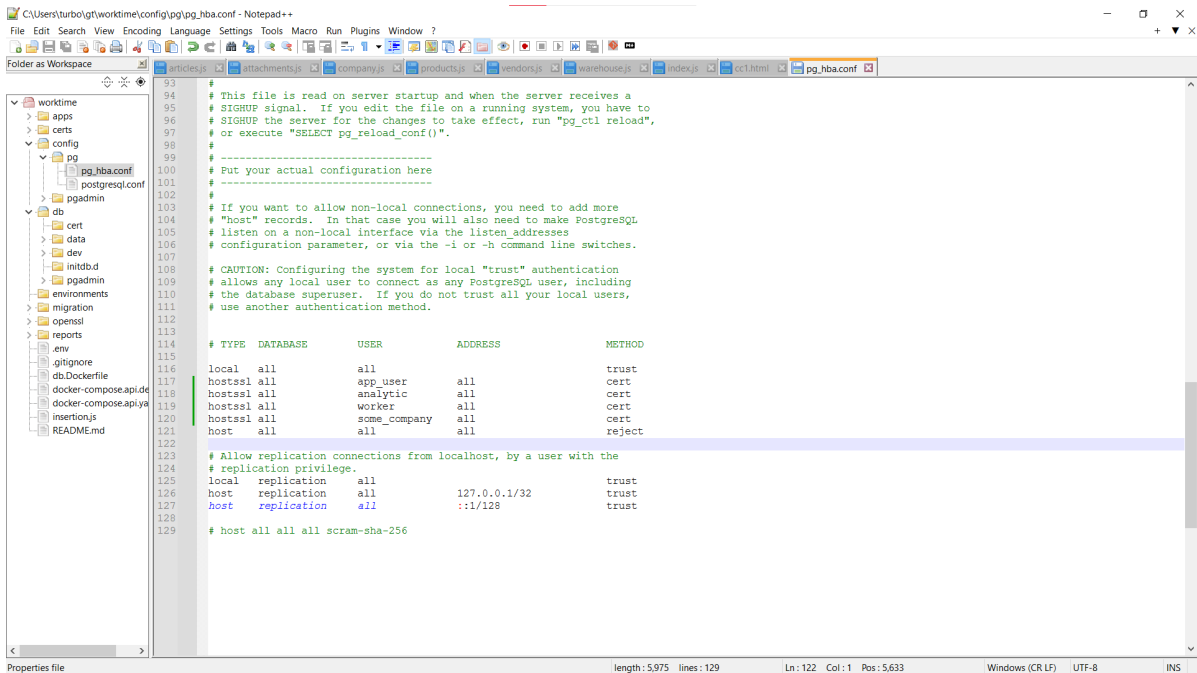
Not signed in

New version available

21



(5) обновление pg_hba.conf



(7) Подключаемся к базе данных от worker

```
#!/bin/bash
# Генерируем сертификаты для worker

KEY_SECRET=12345678
USERNAME=worker

openssl req -new -text -passout pass:$KEY_SECRET -subj /CN=worker -keyout
$USERNAME.pem -out $USERNAME.req
openssl rsa -in $USERNAME.pem -passin pass:$KEY_SECRET -out $USERNAME.key
openssl req -x509 -in $USERNAME.req -text -key $USERNAME.key -out $USERNAME.crt
```

подключение через консоль с проверкой действия сертификата

docker desktop

Search for images, containers, volumes, extensions...

Ctrl+K

Sign in

worktime-db-1

worktime-db

3d48ec258246

2288/22 5433:5432

STATUS

Running (20 minutes ago)

Logs

Inspect

Bind mounts

Exec

Files

Stats

Open in external terminal

psql -U worker "sslmode=require host=0.0.0.0 dbname=wirehouse_db port=5432"

psql (16.2 (Debian 16.2-1.pgdg120+2))

SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)

Type "help" for help.

wirehouse_db=>