МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

НГТУ
НЭТИ | **Факультет прикладной математики и информатики**

Кафедра теоретической и прикладной информатики

Лабораторная работа № 5

по дисциплине «Администрирование информационных систем»

Бригада 2 ХАЙДАЕВ К.Е.

Группа ПМИ-82 ЗЯБЛИЦЕВА У.П.

Вариант 2

Преподаватели АВРУНЕВ О.Е.

Новосибирск, 2022

1 Создать двух пользователей с проверкой пароля, без прав суперпользователя.

createuser -h 127.0.0.1 -p 5432 -P user1

createuser -h 127.0.0.1 -p 5432 -P user2

```
[dba@centos-7 ~]$ createuser -h 127.0.0.1 -p 5432 -P user1
Enter password for new role:
Enter it again:
Password:
[dba@centos-7 ~]$ createuser -h 127.0.0.1 -p 5432 -P user2
Enter password for new role:
Enter it again:
Password:
```

2 Привести список пользователей кластера

```
Password:
[dba@centos-7 ~]$ psql demo
psql (14.1)
Type "help" for help.

demo=# \du
                                   List of roles
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 backup    | Replication                                                | {}
 dba       | Superuser, Create role, Create DB                          | {}
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
 user1     |                                                            | {}
 user2     |                                                            | {}
```

3 Привести содержимое файла pg_hba.conf непосредственно, и как результат запроса к системному представлению.

sudo cat /var/lib/pgpro/std-14/data/pg_hba.conf

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
[dba@centos-7 ~]$
```

table pg_hba_file_rules;

```
demo=# table pg_hba_file_rules;
 line_number | type  |   database    | user_name |  address  |                netmask                 | auth_method | options | error
-------------+-------+---------------+-----------+-----------+----------------------------------------+-------------+---------+-------
          85 | local | {all}         | {all}     |           |                                        | peer        |         |
          87 | host  | {all}         | {all}     | 127.0.0.1 | 255.255.255.255                        | md5         |         |
          89 | host  | {all}         | {all}     | ::1       | ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff | md5         |         |
          92 | local | {replication} | {all}     |           |                                        | peer        |         |
          93 | host  | {replication} | {all}     | 127.0.0.1 | 255.255.255.255                        | md5         |         |
          94 | host  | {replication} | {all}     | ::1       | ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff | md5         |         |
(6 rows)
```

4 Пользователю №1 дать права на создание схемы.

GRANT CREATE ON DATABASE demo TO user1;

```
demo=# GRANT CREATE ON DATABASE demo TO user1;
GRANT
```

5 Подключиться под этим пользователем, создать схему, создать две таблицы в ней.

```
demo=# \c - user1
connection to server on socket "/tmp/.s.PGSQL.5432" failed: FATAL:  Peer authentication failed for user "user1"
Previous connection kept
```

Данная ошибка возникла из-за того, что имя созданного для БД пользователя не совпадает с пользователем для ОС. Для решения данной проблемы необходимо отредактировать файл pg_hba.conf, заменив метод peer на trust в первой строке, затем необходимо перезапустить службу.

Метод аутентификации peer работает, получая имя пользователя операционной системы клиента из ядра и используя его в качестве разрешённого имени пользователя базы данных (с возможностью сопоставления имён пользователя). Этот метод поддерживается только для локальных подключений.

Когда указан способ аутентификации trust, PostgreSQL предполагает, что любой подключающийся к серверу авторизован для доступа к базе данных вне зависимости от указанного имени пользователя базы данных (даже если это имя суперпользователя). Конечно, ограничения, прописанные в столбцах база и пользователь, продолжают работать. Этот метод должен применяться только в том случае, когда на уровне операционной системы обеспечена адекватная защита от подключений к серверу.

Изменим файл pg_hba.conf.

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     trust
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```

systemctl restart postgrespro-std-14

\c – user1

CREATE SCHEMA schema_user1;
CREATE TABLE schema_user1.table1 (id character(8) NOT NULL UNIQUE,
name character(20),
color character(20));

CREATE TABLE schema_user1.table2 (id character(8) NOT NULL UNIQUE,
name character(20),
count character(20));

```
demo=# \c - user1
You are now connected to database "demo" as user "user1".
demo=> CREATE TABLE schema_user1.table1 (id character(8) NOT NULL UNIQUE,
 name character(20),
 color character(20));
CREATE TABLE
demo=> CREATE TABLE schema_user1.table2 (id character(8) NOT NULL UNIQUE,
 name character(20),
 count character(20));
CREATE TABLE
```

6 Под пользователем dba создать роль, которой дать права на выборку из таблиц п.5. Включить пользователя №2 в эту роль. Обеспечить невозможность входа под этой ролью.

createuser -h 127.0.0.1 -p 5432 -P role_for_user2

GRANT SELECT ON schema_user1.table1, schema_user1.table2 TO role_for_user2;

GRANT role_for_user2 TO user2;

```
demo=# GRANT SELECT ON schema_user1.table1, schema_user1.table2 TO role_for_user2;
GRANT
demo=# GRANT role_for_user2 TO user2;
GRANT ROLE
demo=# \du
                                   List of roles
   Role name    |                         Attributes                         |    Member of
----------------+----------------------------------------------------------------+------------------
 backup         | Replication                                                    | {}
 dba            | Superuser, Create role, Create DB                              | {}
 postgres       | Superuser, Create role, Create DB, Replication, Bypass RLS     | {}
 role_for_user2 |                                                                | {}
 user1          |                                                                | {}
 user2          |                                                                | {role_for_user2}
```

Обеспечить невозможность входа под этой ролью.

Revoke connect on database demo from role_for_user2;

```
demo=# revoke connect on database demo from role_for_user2;
REVOKE
```

7 Подключиться под пользователем №2, проверить доступность таблиц из п.5.

```
demo=# \c - user2
You are now connected to database "demo" as user "user2".
demo=> select * from schema_user1.table1, schema_user1.table2;
ERROR:  permission denied for schema schema_user1
LINE 1: select * from schema_user1.table1, schema_user1.table2;
```

User2 унаследовал запрет от role_for_user2, поэтому схема не доступна.

Выполняется в паре с другой бригадой

8 Проверить доступ по порту 5432 к экземпляру postgres другой бригады. При необходимости настроить файрволл

sudo firewall-cmd --zone=public --permanent --add-port=5432/tcp

sudo firewall-cmd –reload

```
[dba@centos-7 ~]$ sudo firewall-cmd --zone=public --permanent --add-port=5432/tcp
[sudo] password for dba:
success
[dba@centos-7 ~]$ sudo firewall-cmd --reload
success
```

В postgresql.conf разрешим принимать соединения из сети.

В файле/var/lib/pgpro/std-14/data/postgresql.conf заменим значение переменной listen_addresses на * вместо localhost, затем перезапустим службу.

sudo vi /var/lib/pgpro/std-14/data/postgresql.conf

```
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                # comma-separated list of addresses;
                                # defaults to 'localhost'; use '*' for all
```

Наш ip

```
[dba@centos-7 ~]$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.4.77  netmask 255.255.0.0  broadcast 172.17.255.255
```

telnet 172.17.6.1 5432

```
[dba@centos-7 ~]$ telnet 172.17.6.1 5432
Trying 172.17.6.1...
Connected to 172.17.6.1.
Escape character is '^]'.
^CConnection closed by foreign host.
```

9 Скорректировать файл pg_hba.conf так, чтобы один из пользователей другой бригады мог выполнять соединение.

sudo vi /var/lib/pgpro/std-14/data/pg_hba.conf

host demo dba ip/16 trust

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     trust
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
host    demo            dba             172.17.6.1/16           trust
```

systemctl restart postgrespro-std-14

10 Проверить корректность, прочитав его содержимое через системное представление.

table pg_hba_file_rules;

```
demo=# table pg_hba_file_rules;
 line_number | type  |   database    | user_name |  address   |                 netmask                 | auth_method | options | error
-------------+-------+---------------+-----------+------------+-----------------------------------------+-------------+---------+-------
          85 | local | {all}         | {all}     |            |                                         | trust       |         |
          87 | host  | {all}         | {all}     | 127.0.0.1  | 255.255.255.255                         | md5         |         |
          89 | host  | {all}         | {all}     | ::1        | ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff | md5         |         |
          92 | local | {replication} | {all}     |            |                                         | peer        |         |
          93 | host  | {replication} | {all}     | 127.0.0.1  | 255.255.255.255                         | md5         |         |
          94 | host  | {replication} | {all}     | ::1        | ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff | md5         |         |
          95 | host  | {demo}        | {dba}     | 172.17.6.1 | 255.255.0.0                             | trust       |         |
(7 rows)
```

11 Проверить подключение к экземпляру под обоими пользователями

sudo -Hiu postgres psql -h 172.17.4.77 -p 5432 demo -U dba

select inet_server_addr();

```
[dba@centos-7 ~]$ sudo -Hiu postgres psql -h 172.17.4.77 -p 5432 demo -U dba
psql (14.1)
Type "help" for help.

demo=# select inet_server_addr();
 inet_server_addr
------------------
 172.17.4.77
(1 row)
```

sudo -Hiu postgres psql -h 172.17.6.1 -p 5432 demo -U dba

```
[dba@centos-7 ~]$ sudo -Hiu postgres psql -h 172.17.6.1 -p 5432 demo -U dba
psql (14.1)
Type "help" for help.

demo=# select inet_server_addr();
 inet_server_addr
------------------
 172.17.6.1
(1 row)
```

12 При подключенном пользователе из другой бригады вывести информацию о текущих сеансах.

netstat -pano | grep -e 5432

172.17.6.10

```
[dba@centos-7 ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.6.10  netmask 255.255.0.0  broadcast 172.17.255.255
```

```
[dba@centos-7 ~]$ netstat -pano | grep -e 5432
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      -                   off (0.00/0/0)
tcp        0      0 127.0.0.1:5432          127.0.0.1:49282         ESTABLISHED -                   keepalive (3715.44/0/0)
tcp        0      0 172.17.4.77:5432        172.17.6.10:59034       ESTABLISHED -                   keepalive (7188.84/0/0)
tcp        0      0 172.17.4.77:5432        172.17.6.10:59032       TIME_WAIT   -                   timewait (17.65/0/0)
tcp        0      0 127.0.0.1:49282         127.0.0.1:5432          ESTABLISHED 1016/python         keepalive (3715.44/0/0)
tcp6       0      0 :::5432                 :::*                    LISTEN      -                   off (0.00/0/0)
unix  2      [ ACC ]     STREAM     LISTENING     648400   -                    /tmp/.s.PGSQL.5432
```