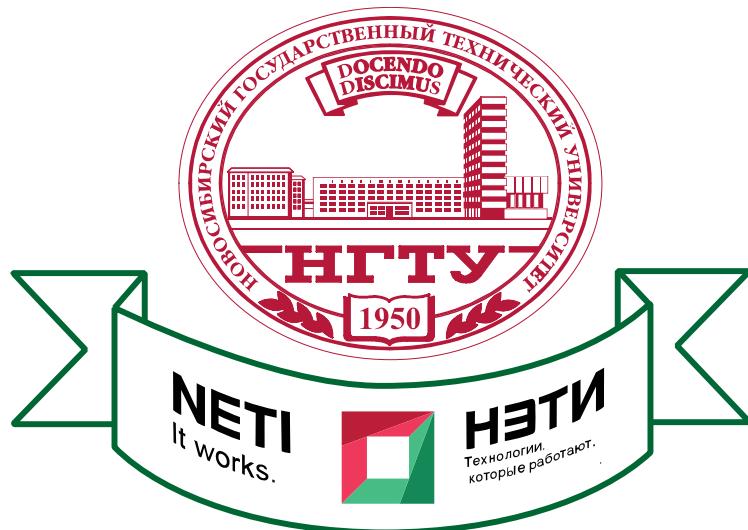


Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования

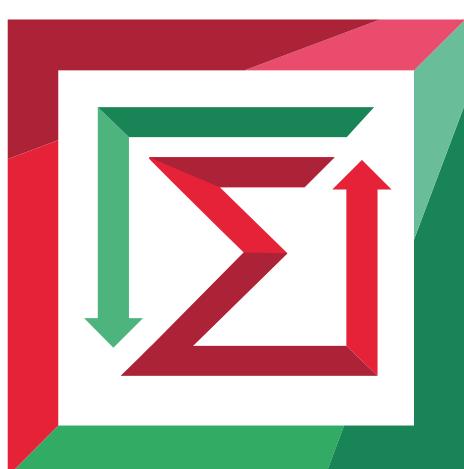
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



Кафедра теоретической и прикладной информатики

Лабораторная работа № 5

по дисциплине «Администрирование информационных систем»



Факультет: ПМИ
Группа: ПМИ-02
Бригада: 8
Студенты: Сидоров Даниил,
Дюков Богдан
Преподаватель: Аврунев О.Е.

Новосибирск

2026

Ход работы

1. Создали двух пользователей с проверкой пароля, без прав суперпользователя:

```
[dba@centos-stream-8 ~]$ createuser -h 127.0.0.1 -p 5432 -P user1
Enter password for new role:
Enter it again:
Password:
[dba@centos-stream-8 ~]$ createuser -h 127.0.0.1 -p 5432 -P user2
Enter password for new role:
Enter it again:
Password:
[dba@centos-stream-8 ~]$
```

Если мы попытаемся подключиться к базе данных как к пользователю PostgreSQL (5 пункт), который не является UNIX-пользователем, мы получим ошибку. Поэтому сразу создали этих пользователей в Linux:

```
[root@centos-stream-8 ~]# useradd user1
[root@centos-stream-8 ~]# passwd user1
Changing password for user user1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

[root@centos-stream-8 ~]# useradd user2
[root@centos-stream-8 ~]# passwd user2
Changing password for user user2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@centos-stream-8 ~]#
```

2. Привели список пользователей кластера:

```
[dba@centos-stream-8 ~]$ sudo -u postgres psql -c "\du"
[sudo] password for dba:
                                         List of roles
   Role name |                         Attributes                         | Member of
-----+-----+
    dba      | Superuser, Create role, Create DB                      | {}
  postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
    user1    |                                                       | {}
    user2    |                                                       | {}
```

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

Содержимое файла непосредственно: sudo cat /var/lib/pgpro/std-15/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-stream-8 ~]$
```

Как результат запроса:

```
demo=# SELECT * FROM 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 | fffff: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 | fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff | md5 | | |  
(6 rows)
```

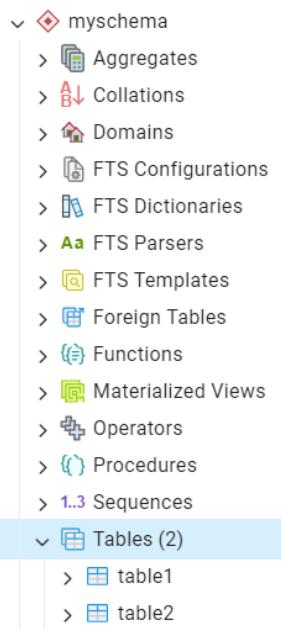
4. Пользователю №1 дали права на создание схемы:

```
demo=# grant create on database demo to user1;  
GRANT
```

5. Подключились под этим пользователем, создали схему и в ней две таблицы:

```
[user1@centos-stream-8 ~]$ psql -d demo  
psql (15.5)  
Type "help" for help.  
  
demo=> CREATE SCHEMA myschema;  
CREATE SCHEMA  
demo=> CREATE TABLE myschema.table1(id serial PRIMARY KEY, name VARCHAR(50));  
CREATE TABLE  
demo=> CREATE TABLE myschema.table2(id serial PRIMARY KEY, name VARCHAR(50));  
CREATE TABLE  
demo=>
```

Содержимое созданной схемы в pgadmin:



6. Под пользователем dba создали роль, которой дали права на выборку из таблиц п.5:

```
[dba@centos-stream-8 ~]$ createuser -h 127.0.0.1 -p 5432 -P user3
Enter password for new role:
Enter it again:
Password:
[dba@centos-stream-8 ~]$
```

Аналогично предыдущим пользователям, создали этого пользователя в Linux:

```
[root@centos-stream-8 dba]# useradd user3
[root@centos-stream-8 dba]# passwd user3
Changing password for user user3.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@centos-stream-8 dba]#
```

Включили пользователя №2 в созданную роль (сразу оценили результат, приведя список пользователей кластера):

```
demo=# grant select on myschema.table1, myschema.table2 to user3;
GRANT
demo=# grant user3 to user2;
GRANT ROLE
demo=# \du
          List of roles
Role name | Attributes | Member of
-----+-----+-----+
dba      | Superuser, Create role, Create DB | {}
postgres | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
user1    |           | {}
user2    |           | {user3}
user3    |           | {}

demo=#
```

Обеспечили невозможность входа под этой ролью:

```
demo=# alter role user3 with nologin;
ALTER ROLE
```

Попытались подключиться под этой ролью и получили ожидаемую ошибку:

```
[user3@centos-stream-8 ~]$ psql -d demo
psql: error: connection to server on socket "/tmp/.s.PGSQL.5432" failed: FATAL:  role "user3" is not permitted to log in
[user3@centos-stream-8 ~]$
```

7. Подключились под пользователем №2, проверили доступность таблиц из п.5:

```
[user2@centos-stream-8 ~]$ psql -d demo
psql (15.5)
Type "help" for help.

demo=> select * from myschema.table1;
ERROR:  permission denied for schema myschema
LINE 1: select * from myschema.table1;
^
```

(доступа нет)

8. Проверили доступ по порту 5432 к экземпляру postgres другой бригады:

```
[dba@centos-stream-8 ~]$ telnet 172.17.7.71 5432
Trying 172.17.7.71...
telnet: connect to address 172.17.7.71: No route to host
[dba@centos-stream-8 ~]$
```

(маршрут к хосту не найден)

Другая бригада, выполняя аналогичную проверку, получит ту же самую ошибку.

Исправим это. Сначала настроим наш файрвол:

```
[dba@centos-stream-8 ~]$ sudo firewall-cmd --zone=public --permanent --add-port=5432/tcp
[sudo] password for dba:
success
[dba@centos-stream-8 ~]$ sudo firewall-cmd --reload
success
[dba@centos-stream-8 ~]$
```

Другая бригада снова проверяет доступность по порту 5432 к экземпляру postgres нашей бригады:

```
[dba@centos-stream-8 ~]$ telnet 172.17.6.58 5432
Trying 172.17.6.58...
telnet: connect to address 172.17.6.58: Connection refused
[dba@centos-stream-8 ~]$
```

Получили ошибку, которая означает то, что наш PostgreSQL настроен на прослушивание только localhost. Исправим это. Перейдем в файл конфигурации postgresql.conf и изменим параметр listen_addresses на '*', что позволит PostgreSQL принимать соединения с любого IP-адреса:

Перезапустили службу, после чего другая бригада снова проверяет доступность:

```
[root@centos-stream-8 ~]# systemctl restart postgresql-15.service
[root@centos-stream-8 ~]# telnet 172.17.6.58 5432
Trying 172.17.6.58...
Connected to 172.17.6.58.
Escape character is '^]'.
```

Получили корректный результат. После того, как другая бригада проделает аналогичные махинации, нам будет также предоставлен доступ к их экземпляру.

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

Этим пользователем будет user1. Добавляем соответствующую строку в файл pg_hba.conf:

```
# TYPE DATABASE USER ADDRESS METHOD
# "local" is for Unix domain socket connections only
local  all      all
# IPv4 local connections:
host   all      all      127.0.0.1/32
# IPv6 local connections:
host   all      all      ::1/128
# Allow replication connections from localhost, by a user with the
# replication privilege.
local  replication all
host   replication all      127.0.0.1/32
host   replication all      ::1/128
host   demo     user1    172.17.7.71/32

```

10. Проверили корректность, прочитав его содержимое через системное представление:

```
demo=# select * from 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 |
  95 | host | {demo} | {user1} | 172.17.7.71 | 255.255.255.255 | trust |
(7 rows)
```

11. Проверили подключение к экземпляру под обеими пользователями:

Подключение пользователем user1:

```
[dba@centos-stream-8 ~]$ psql -h 172.17.6.58 -U user1 -d demo
psql (15.5)
Type "help" for help.

demo=> 
```

(успешно, за счет корректировки файла pg_hba.conf)

Подключение пользователем user2:

```
[dba@centos-stream-8 ~]$ psql -h 172.17.6.58 -U user2 -d demo
psql: error: connection to server at "172.17.6.58", port 5432 failed: FATAL:
no pg_hba.conf entry for host "172.17.7.71", user "user2", database "demo",
no encryption
[dba@centos-stream-8 ~]$ 
```

(ожидали ошибку)

12. При подключенном пользователе из другой бригады вывели информацию о текущих сессиях:

Подключились пользователем user1 из другой бригады. Выведенная информация о текущих сессиях:

```
[dba@centos-stream-8 ~]$ 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      -
tcp        0      0 172.17.6.58:5432       172.17.7.71:49152   ESTABLISHED -
tcp6       0      0 ::1:5432            ::*:*              LISTEN      -
unix  2      [ ACC ]         STREAM     LISTENING     1408660  -
[dba@centos-stream-8 ~]$ 
```

(наблюдаем подключение другой бригады)