

数据库系统课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 实验六：数据库的安全性 |
| 实验日期： | 2022/4/21 |
| 实验地点： | 厦门大学德旺图书馆 |
| 提交日期： | 2022/4/21 |
|  | |
| 学号： | 20420192201952 |
| 姓名： | 庾晓萍 |
| 专业年级： | 软工2020级 |
| 学年学期： | 2021-2022学年第二学期 |

1. 实验目的

* 理解数据库系统用户（user）、权限（privilege）和角色（role）的概念和作用
* 熟练掌握用户的管理：创建、查看、删除和权限的授予与回收
* 熟练掌握通过数据字典查看用户权限、表和视图权限的方法
* 熟练掌握使用 Grant 命令给用户、角色授权的方法
* 熟练掌握使用 Revoke 命令回收已授权限的方法
* 熟练掌握角色定义、重命名和删除的方法
* 熟练掌握修改角色中权限的方法
* 理解视图的安全性作用

1. 实验内容和步骤
2. 完成https://bokai.blog.csdn.net/article/details/117912175 的内容。

一、用户及角色

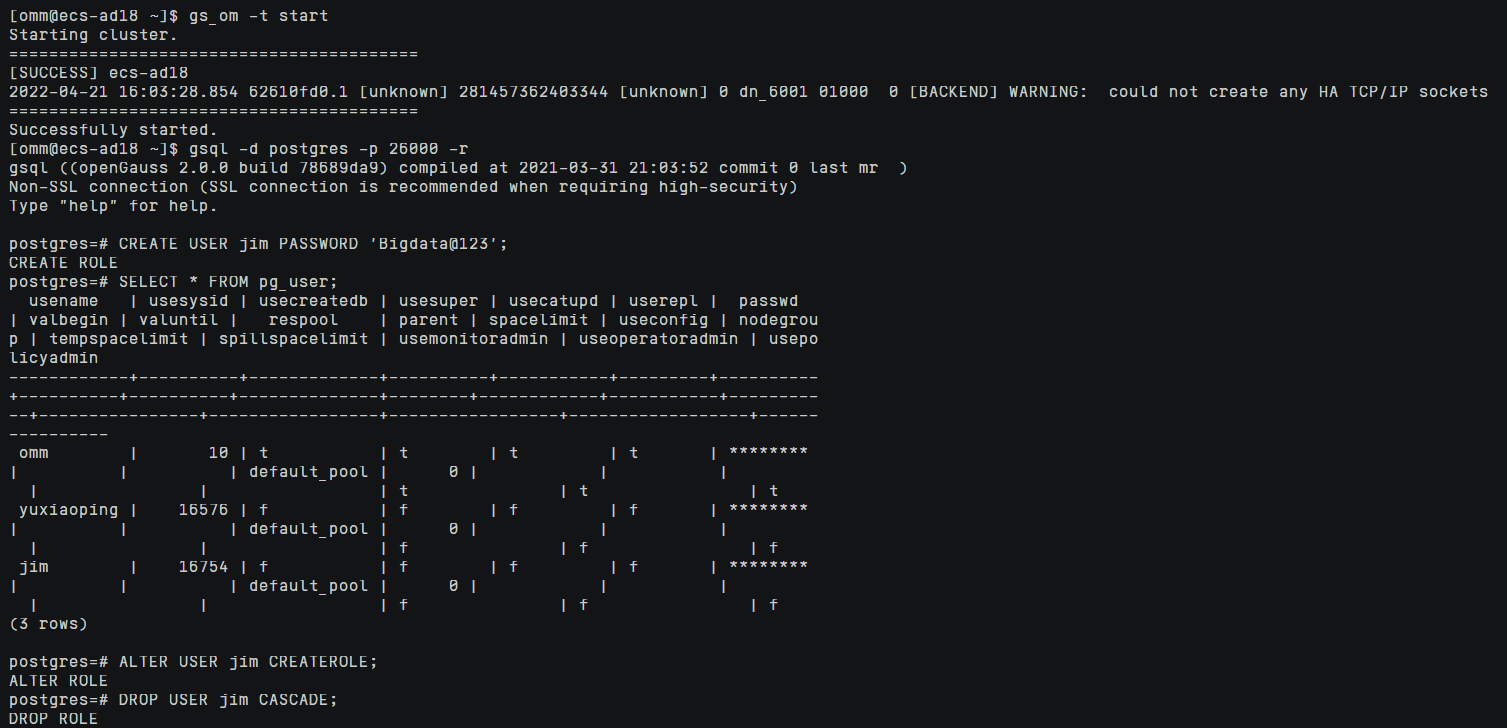
① 用户

· 通过CREATE USER创建的用户，默认具有LOGIN权限；

· 通过CREATE USER创建用户的同时系统会在执行该命令的数据库中，为该用户创建一个同名的SCHEMA；

· 其他数据库中，则不自动创建同名的SCHEMA；用户可使用CREATE SCHEMA命令，分别在其他数据库中，为该用户创建同名SCHEMA。

**步骤：**创建用户jim，登录密码为Bigdata@123。查看用户列表，为用户jim追加有创建角色的CREATE ROLE权限，删除用户。



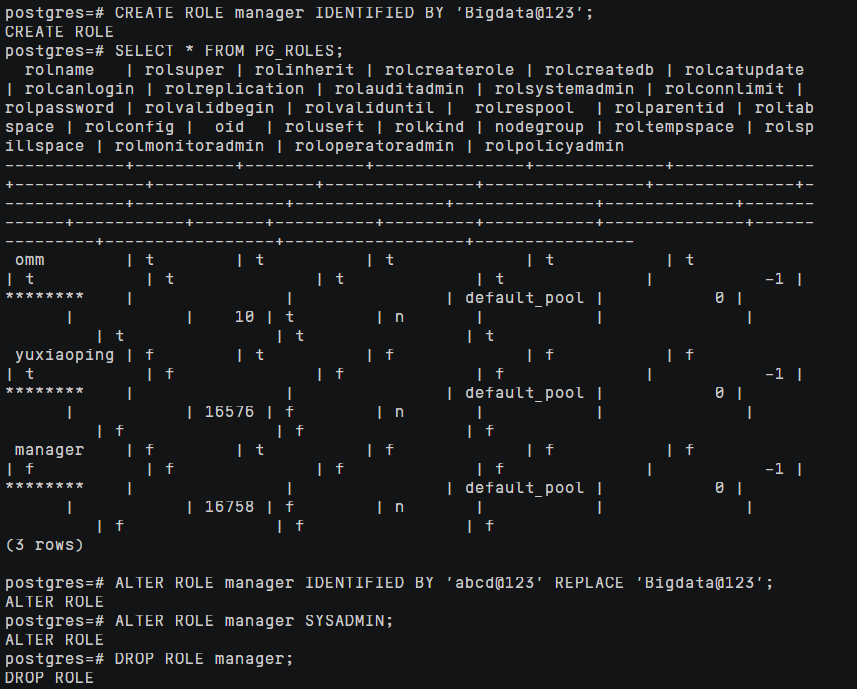
② 角色

·角色是拥有数据库对象和权限的实体。在不同的环境中角色可以认为是一个用户，一个组或者兼顾两者。

·在数据库中添加一个新角色，角色无登录权限。

·创建角色的用户必须具备CREATE ROLE的权限或者是系统管理员。

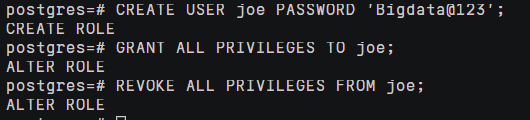
**步骤：**创建一个角色，名为manager，密码为Bigdata@123。查看角色，修改角色manager的密码为abcd@123。修改角色manager为系统管理员，删除角色manager。



二、权限设置及回收

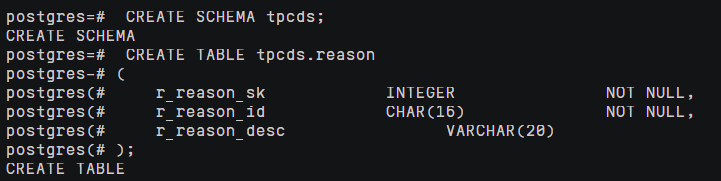
① 将系统权限授权给用户或者角色

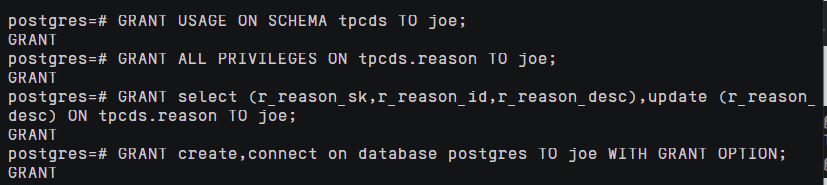
**步骤：**创建名为joe的用户，将sysadmin权限授权给joe，撤销joe用户的sysadmin权限。



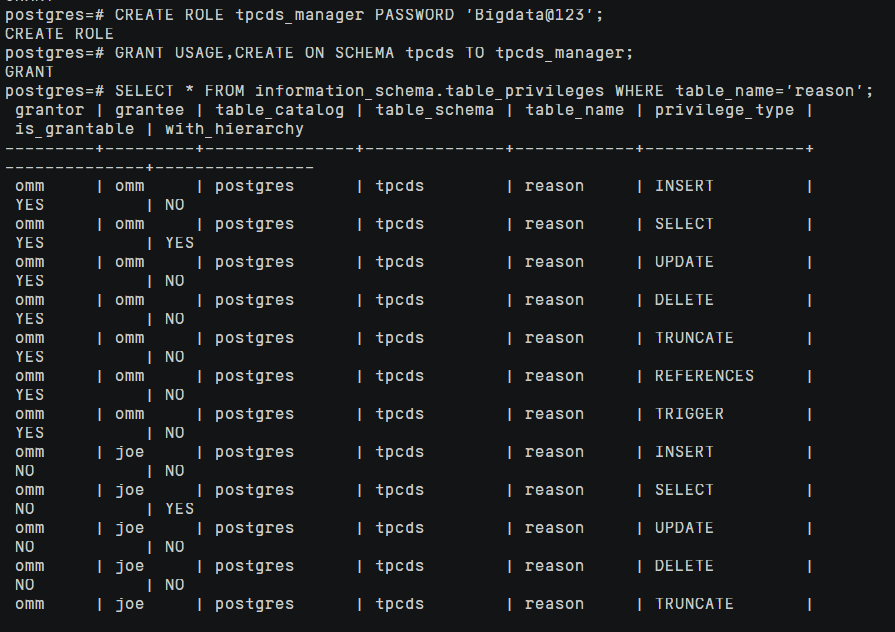
② 将数据库对象授权给角色或用户

**步骤：**创建tpcds模式，tpcds模式下创建一张reason表。

将模式tpcds的使用权限和表tpcds.reason的所有权限授权给用户joe。将tpcds.reason表中r\_reason\_sk、r\_reason\_id、r\_reason\_desc列的查询权限，r\_reason\_desc的更新权限授权给joe。将数据库postgres的连接权限授权给用户joe，并给予其在postgres中创建schema的权限，而且允许joe将此权限授权给其他用户。

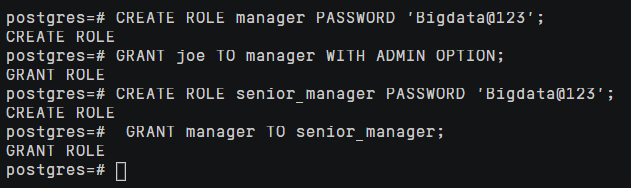


创建角色tpcds\_manager，将模式tpcds的访问权限授权给角色tpcds\_manager，并授予该角色在tpcds下创建对象的权限，不允许该角色中的用户将权限授权给其人。查看表reason权限：



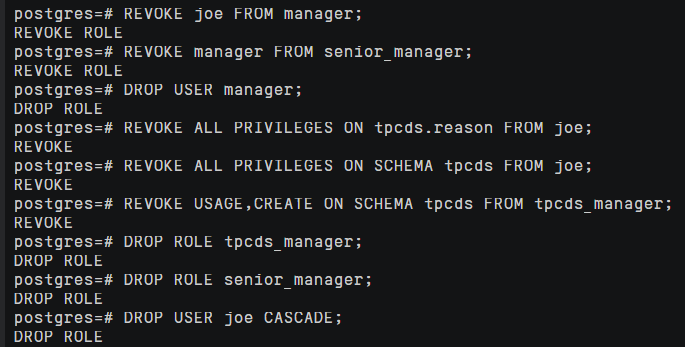
③ 将用户或者角色的权限授权给其他用户或角色

**步骤：**创建角色manager，将joe的权限授权给manager，并允许该角色将权限授权给其他人，创建用户senior\_manager，将用户manager的权限授权给该用户。

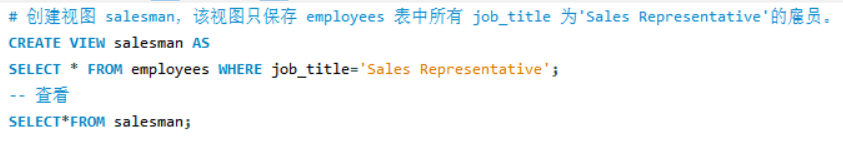


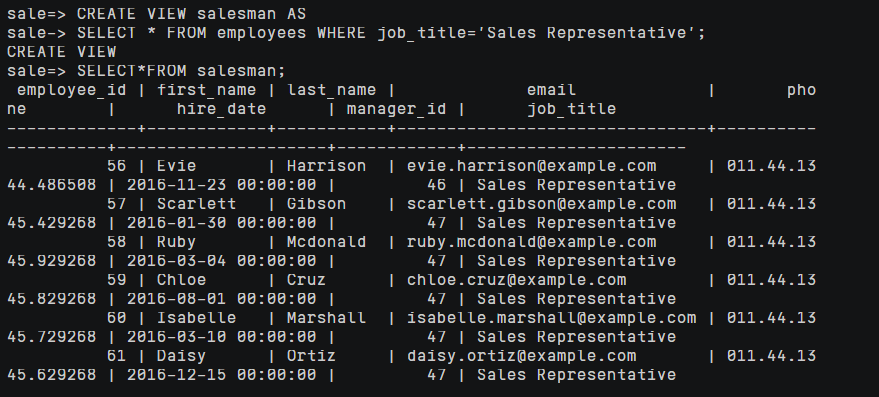
④ 权限回收并清理用户

**步骤：**逐步回收manager权限，删除manager用户，逐步回收joe权限，逐步回收tpcds\_manager权限，删除 tpcds\_manager用户，删除senior\_manager用户，删除joe用户。



1. 创建视图 salesman，该视图只保存 employees 表中所有 job\_title 为'Sales Representative'的雇员。

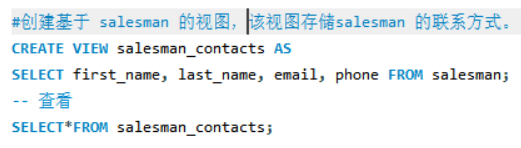


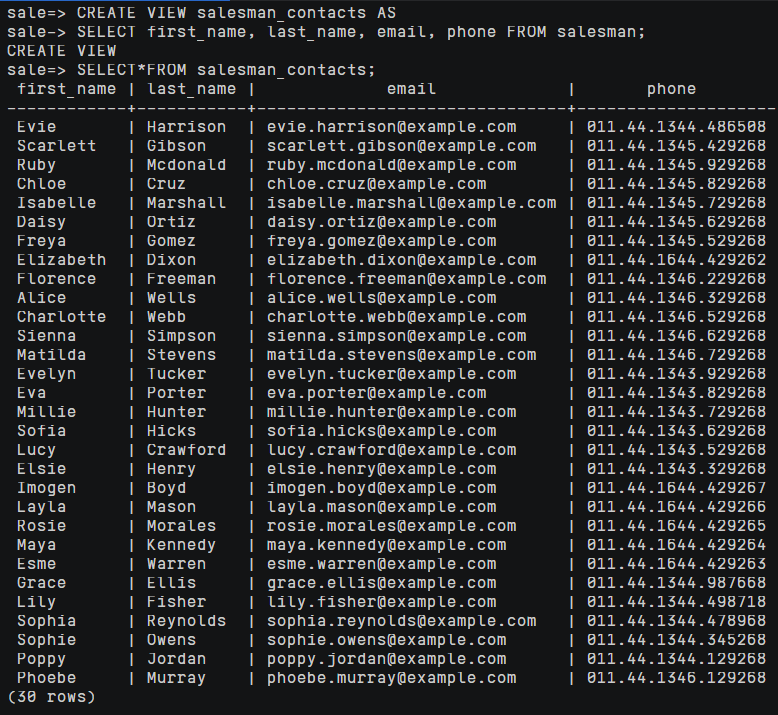


（3）创建基于 salesman 的视图

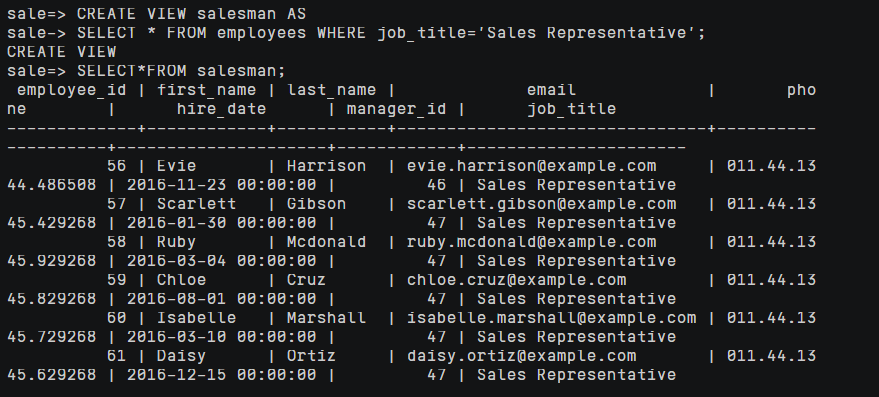
salesman\_contacts(first\_name,last\_name,email,phone)，该视图存储的

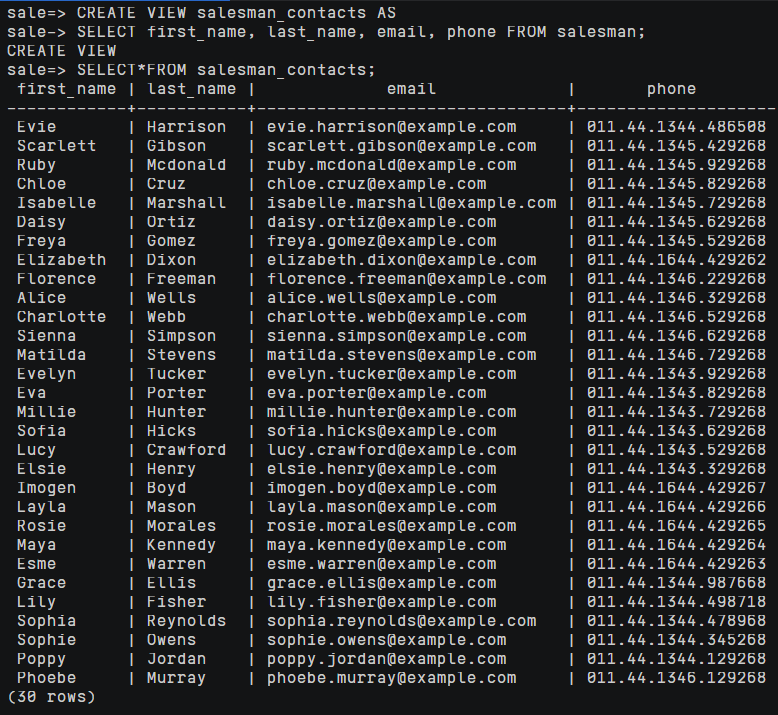
salesman 的联系方式。



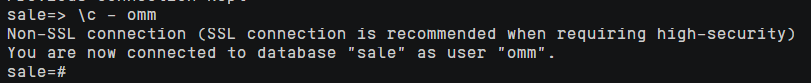


1. 查询视图 salesman 和 salesman\_contacts。





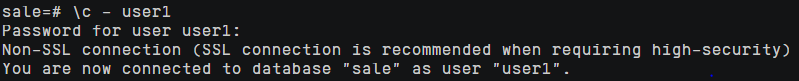
1. 在当前窗口输入命令：\c - omm 切换到 omm 用户。



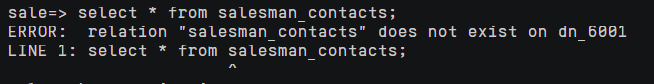
1. 创建新用户 user1。



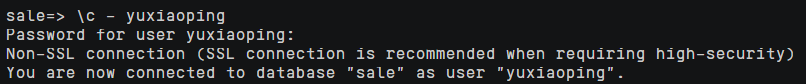
（7）在当前窗口输入命令：\c – user1 切换到 user1 用户。



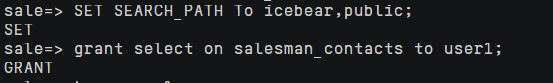
1. 发布查询命令：select \* from salesman\_contacts;观察结果。



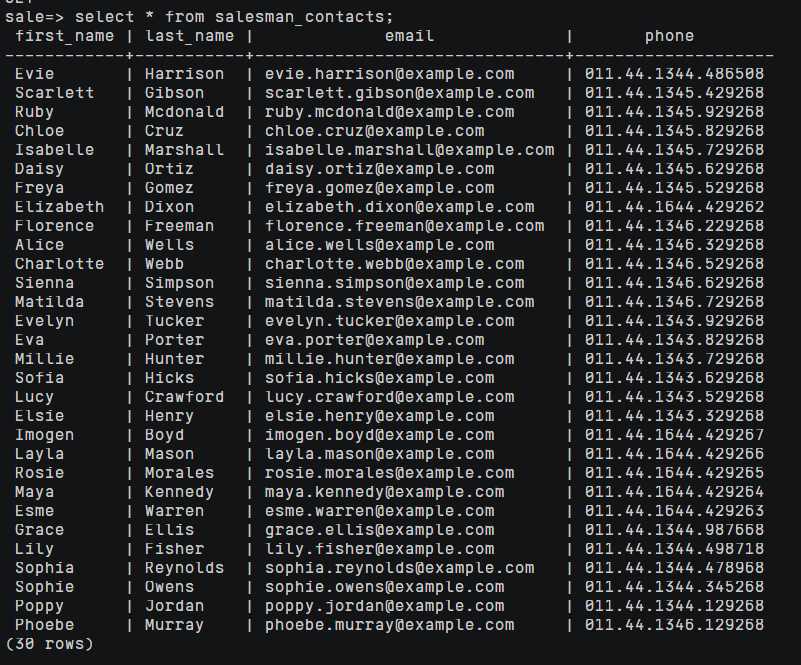
1. 发布命令：\c – yuxiaoping 切换到 whj 用户—此处的 whj 应替换为你们自己创建的用户。密码是yuxiaoping@123



（10）在当前 whj 用户下输入命令：grant select on salesman\_contacts to user1; 实现授权操作。由于opengauss报错，实际上使用了grant all on schema icebear to user1;。



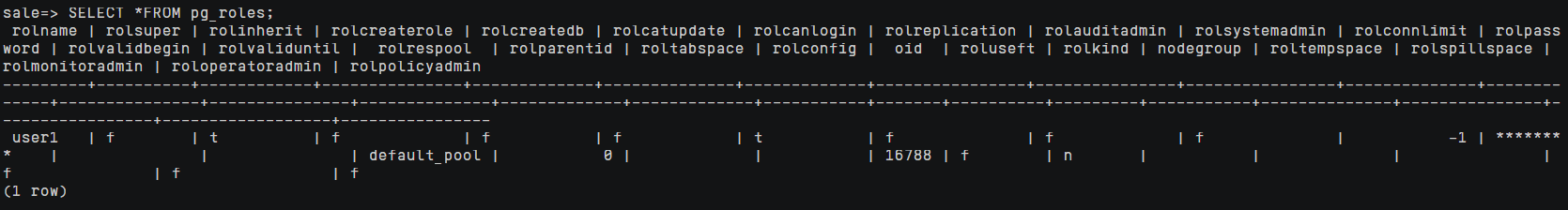
（11）依次重复步骤（7）和（8），比较两次查询的结果。

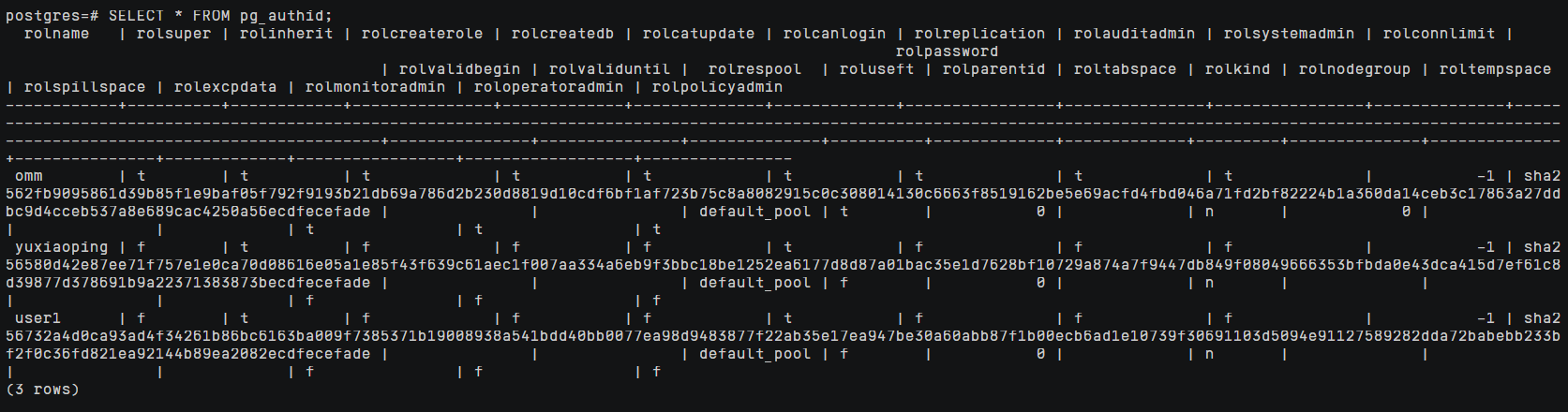


/\*说明：步骤（2）-（11）的主要目的是用于验证视图的作用：被授权用户只能查询在权限范围内的数据，范围外的数据不可访问\*/

（12）查看与角色、权限相关的系统表和系统视图：pg\_roles，pg\_authid。

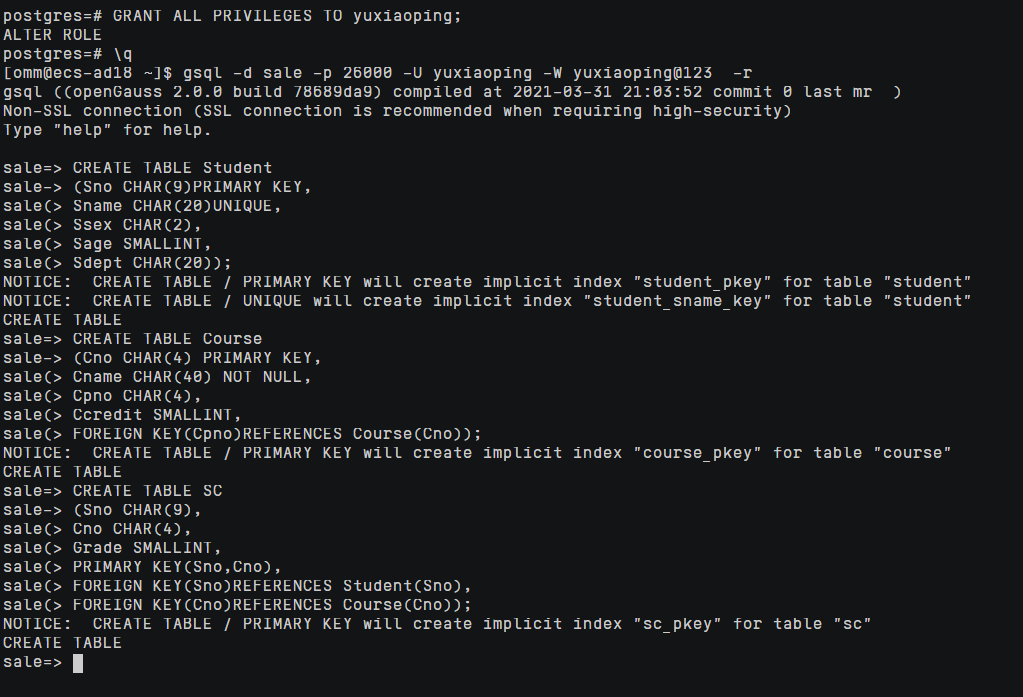
pg\_roles视图提供访问数据库角色有关信息的接口。这个视图只是pg\_authid表的公开可读部分的视图化，同时把口令字段用空白填充。



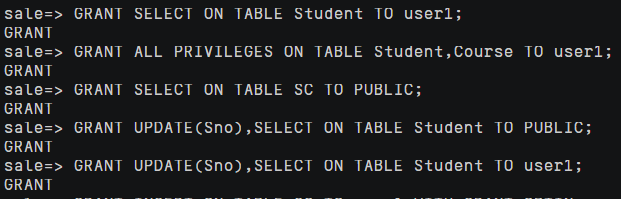


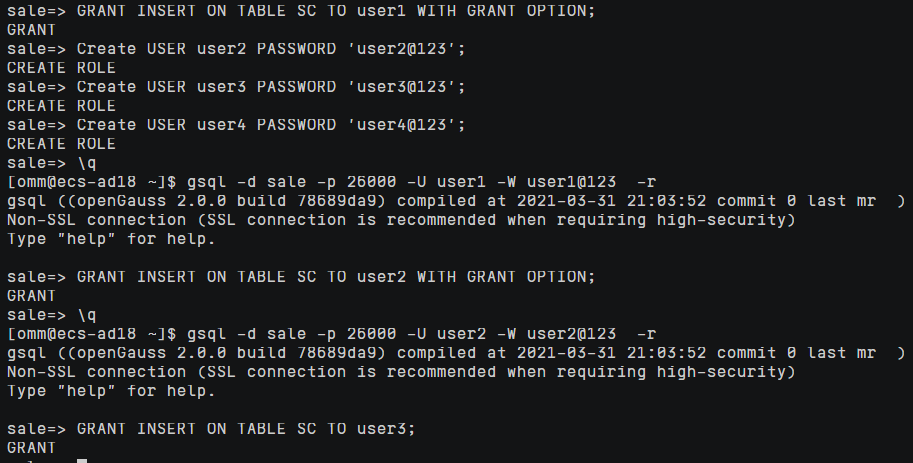
1. 在完成（1）的基础上，重做教材中的[例 4.1-例 4.13]，因为 openGauss 的语法与教材上的不完全一致，可以通过以上实操加深对 openGauss 安全性控制机制的理解。

① 创建表格

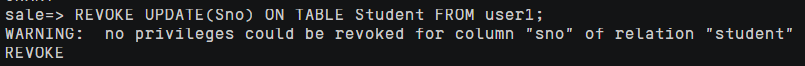


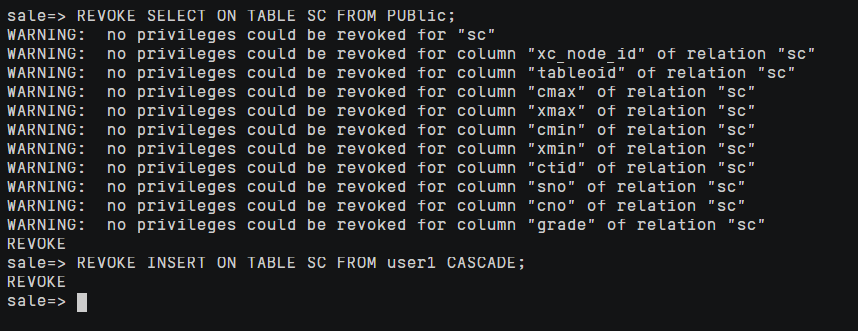
② 创建角色，授权





③ 回收限权





1. 实验总结

3.1 实验思考

·具有什么权限才能创建新用户？

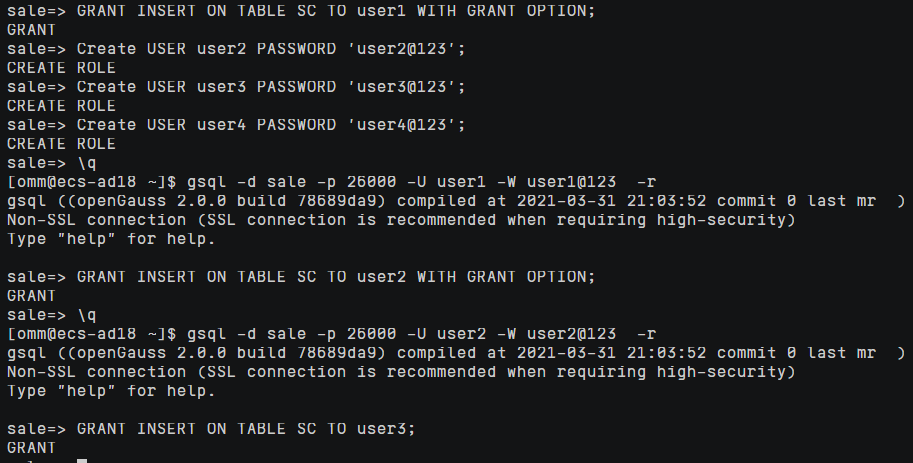
答：用户必须拥有数据库创建的权限或者是数据库的系统管理员权限才能创建数据库。创建用户必须有dba的权限。

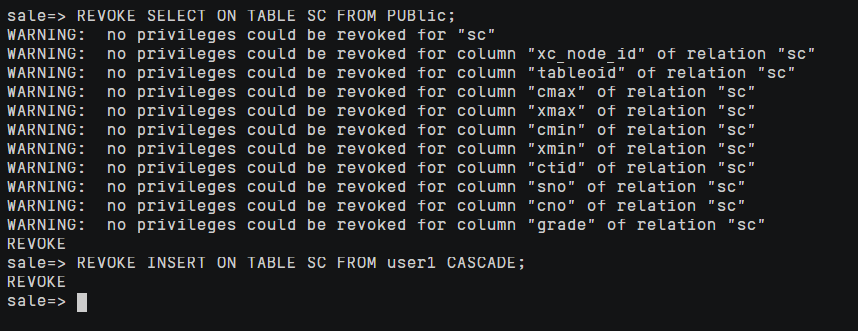
·角色的作用是什么？

答：数据库角色是被命名的一组与数据库操作相关的权限，角色是权限的集合，因此，可以为一组有相同权限的用户创建一个角色，使用角色来管理数据库限权可以简化授权的过程。

·如何实现角色所含权限的修改，请设计样例验证之

答：给角色赋予对象权限，使用GRANT。。要撤销或重新授予角色对权限， 可通过REVOKE实现。如下面的代码：





3.2 对实验的认识

通过实验我对openGauss中的一些语句更熟悉了。如

SET SEARCH\_PATH TO icebear, public;可以将搜索路径设置为icebear、public，首先搜索icebear。如SELECT \* FROM customer\_t1;可以用来查询表customer\_t1的所有数据。gsql -d sale -p 26000 -U yuxiaoping -W yuxiaoping@123 -r或者gsql -d sale -p 26000 -U user1 -W user1@123 -r可以用来将新用户连接到数据库。可以使用gsql -d postgres -p 26000 -r 连接到postgres。gs\_om -t start可以开启数据库。

3.3 遇到的困难及解决方法

要更改当前会话的默认Schema，请使用SET命令。执行如下命令

SET SEARCH\_PATH To icebear,public;将搜索路径设置为myschema、public，首先搜索myschema。



高斯默认有session超时时间，若想要session一直保持，需要修改配置项：ALTER DATABASE sale SET session\_timeout TO 0;

