

数据库系统课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 数据库安全性 |
| 实验日期： | 2022.11.25 |
| 实验地点： | 四号楼 |
| 提交日期： | 2022.11.28 |
|  | |
| 学号： | 22920202202877 |
| 姓名： | 陈鑫蕾 |
| 专业年级： | 数媒2020级 |
| 学年学期： | 2022-2023学年第一学期 |

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

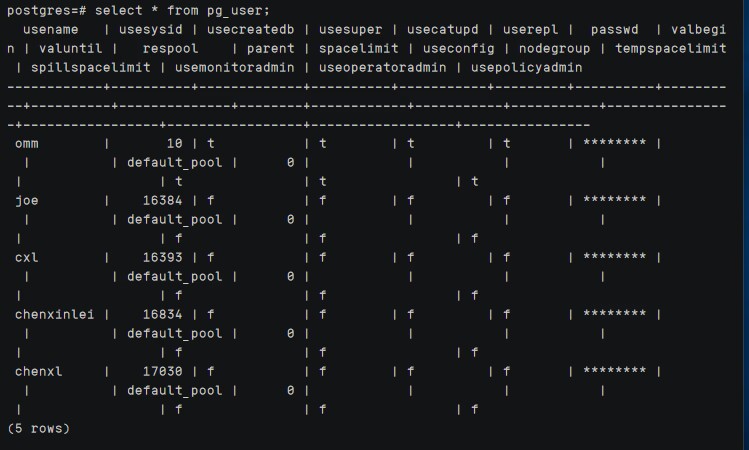
1. 实验内容和步骤

1.完成 https://bokai.blog.csdn.net/article/details/117912175 的内容。

(1)创建用户chenxl

)3V{3`${L`G~$7YNHL)[2KF

（2）查看用户列表



（3）为用户chenxl追加有创建角色的CREATE ROLE权限

9Z4H82Q9VS5HZL8)VJ~7RE5

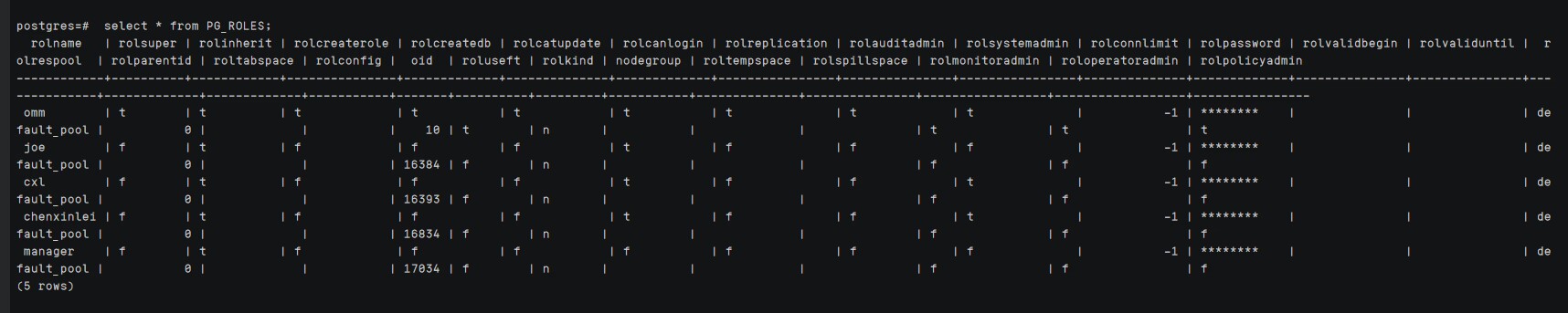
（4）删除用户

MULUL1F6}D}}J3}Q1W4]@ZX

（5）创建一个角色名为manager，密码为Bigdata123

%9LM]YAAZKX0(FF6~F{~_MI

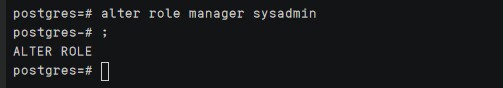
（6）查看角色



（7）修改角色manager密码为abcd@123

FD@3HPX$E%8VX6T}~CXK(CJ

（8）修改角色manager为系统管理员



（9）删除角色manager

D68H953OP@SL@[(N[2TG`DF

（10）创建名为jow的用户

U~WSQYG2VP`9Y2B40G{9062

（11）将sysadmin权限授权为jow

OQ)D}FM73J51EC3SIZ)5DF2

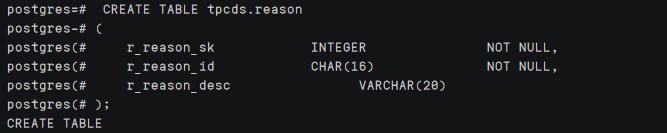
（12）撤销jow用户的syadmin权限

W3KIG$EJ09Y9G[]B6[A`[G1

1. 创建tpcds模式

1PD71H~$)6LFXP1}MB2@`{G

（14）tpcds模式下创建一张reason表



（15）将模式tpcds的使用权限和表tpcds.reason的所有权限授权给用户jow

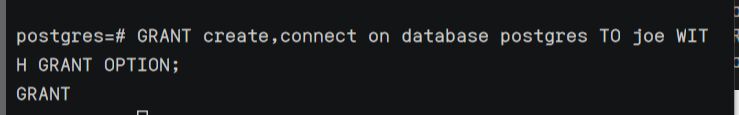
EP`$166@10@)CNM94Z(U9D2

B5P%K%{8P({`_(]U@EV]T68

（16）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jow

UA9PQV_J1QLHLT]J1N{NA_1

（17）将数据库postgres的连接权限授权给用户jow，并给予其在postgres中创建schema的权限，而且允许jow将此权限授权给其他用户



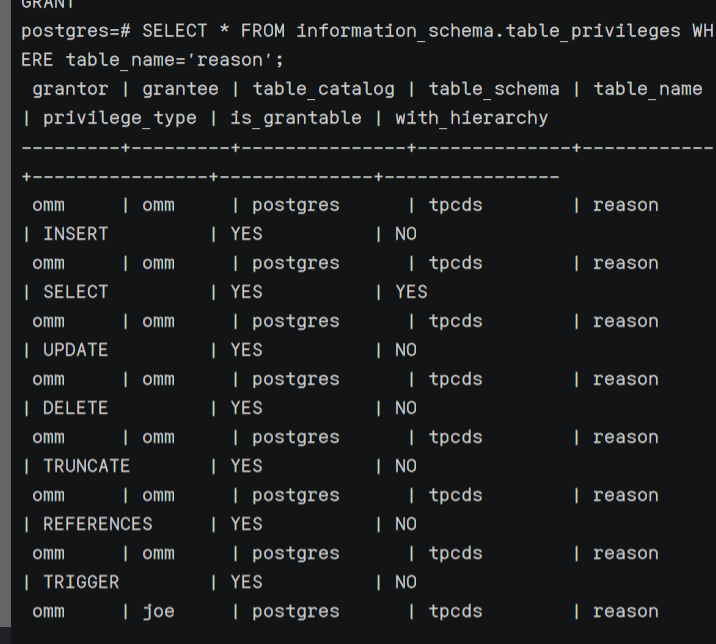
（18）创建角色tpcds\_manager

(QQ5GVJSV{}_SSV$NUH)}IK

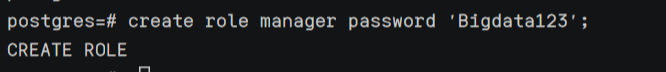
1. 将模式tpcds的访问权限授权给角色tpcds\_manager，并授予该角色在tpcds下创建对象的权限，不允许该角色中的用户将权限授权给其人

0DKEZQ07UTJ}UMWI0PKLZ_0

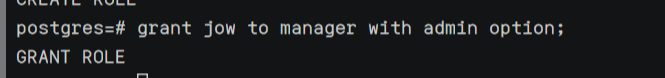
1. 查看表reason权限



（21）创建角色manager



（22）将joe的权限授权给manager，并允许该角色将权限授权给其他人



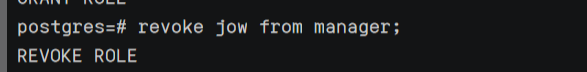
（23）创建用户senior\_manager

W]AP$W5KECV@EY9`C9Y($LL

（24）将用户manager的权限授权给该用户

R[_}30PI(II{2JPQ[2G@UME

（25）回收manager权限

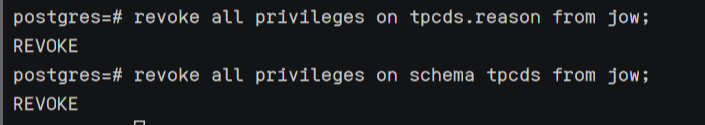


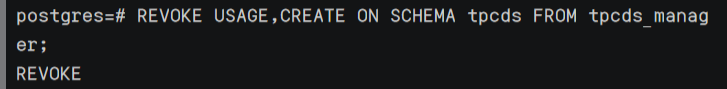
N]`U1C$Y`6N$RK8}_X7L501

（26）删除用户manager

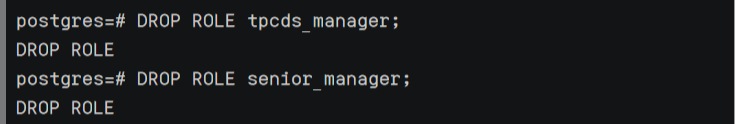
0}OB8R$W%(S0AS23A4AK0)7

（27）回收tpcds\_manager权限



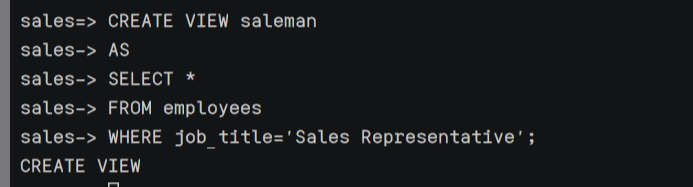


（28）删除 tpcds\_manager用户，删除senior\_manager用户，删除jow用户



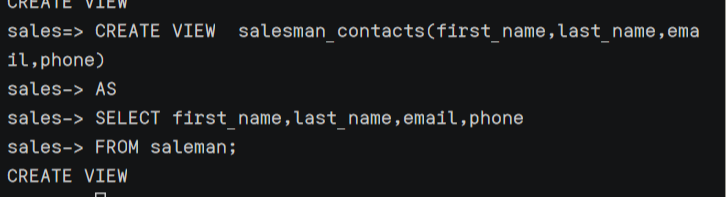
]CW0LOCTEHEM1UM1`}_65S1

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

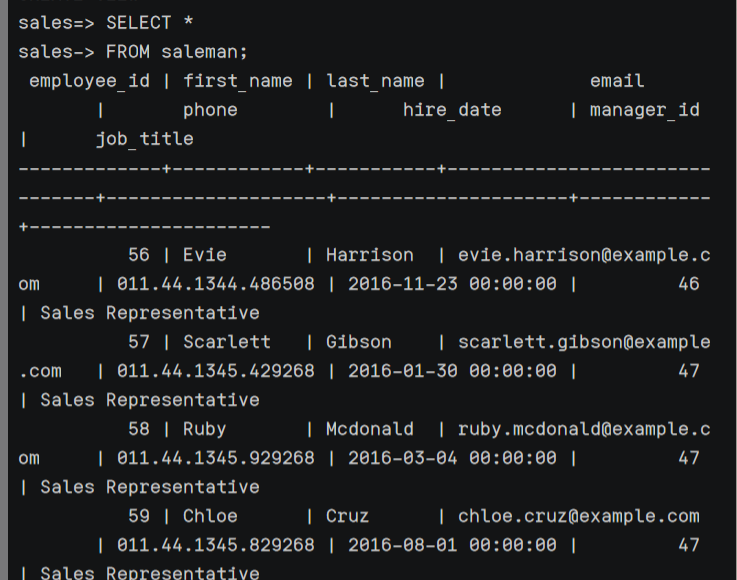


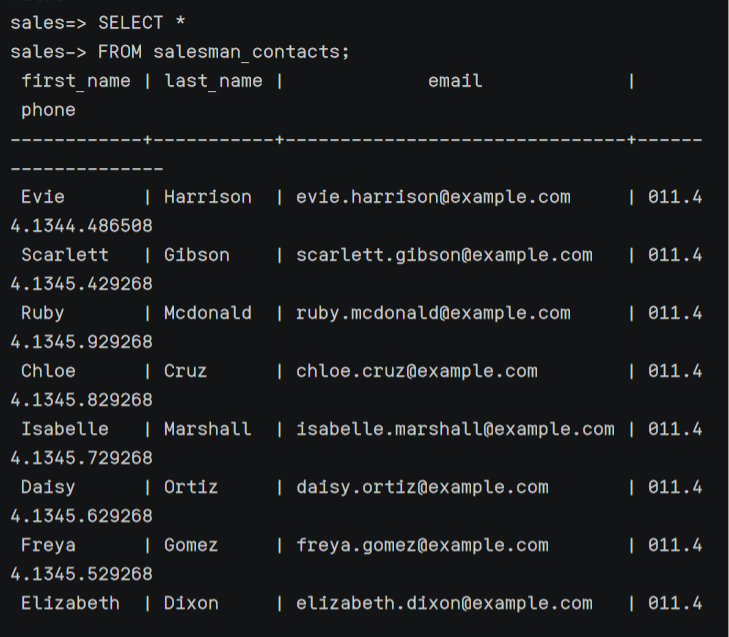
3.创建基于 salesman 的视图 salesman\_contacts(first\_name,last\_name,email,phone)，该视图存储的

salesman 的联系方式。

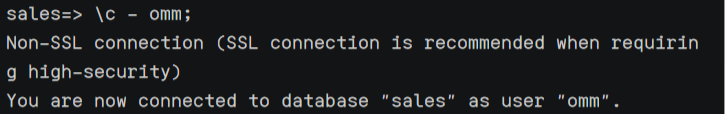


4.查询视图 salesman 和 salesman\_contacts。

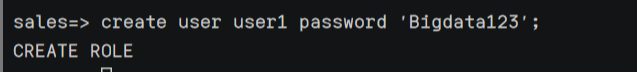




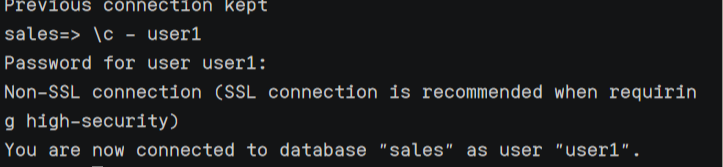
5.在当前窗口输入命令：\c - omm 切换到 omm 用户。



6.创建新用户 user1。



7.在当前窗口输入命令：\c –user1 切换到 user1 用户。



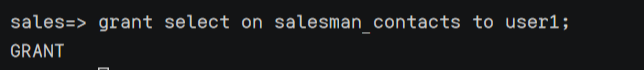
8.发布查询命令：select \* from salesman\_contacts;观察结果。

V%K9EIE}EIC38VYQ21574Y5

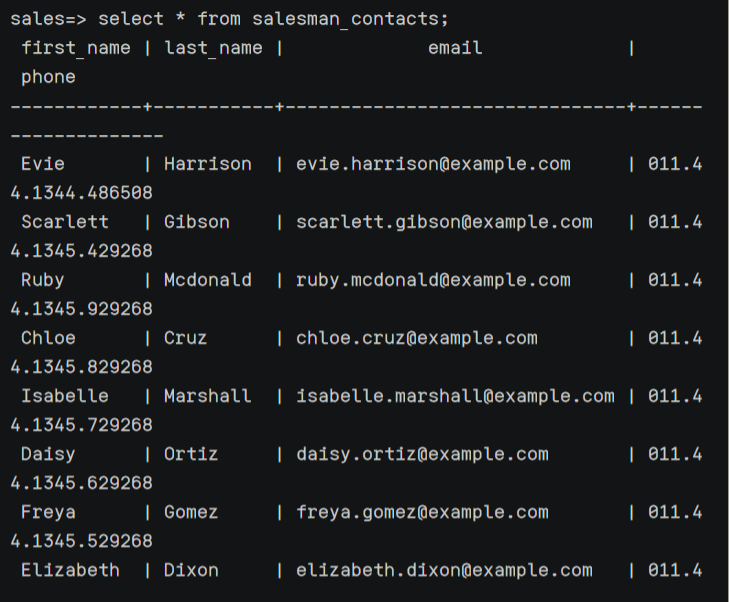
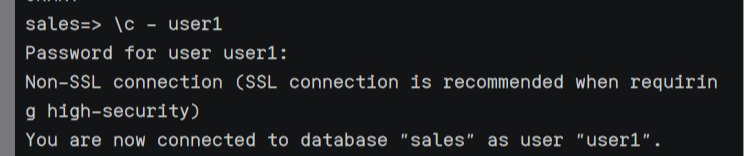
报错：无权限

9.发布命令：\c – chenxinlei 切换到 chenxinlei 用户

10.在当前 chenxinlei用户下输入命令：grant select on alesman\_contacts to user1; 实现授权操作。

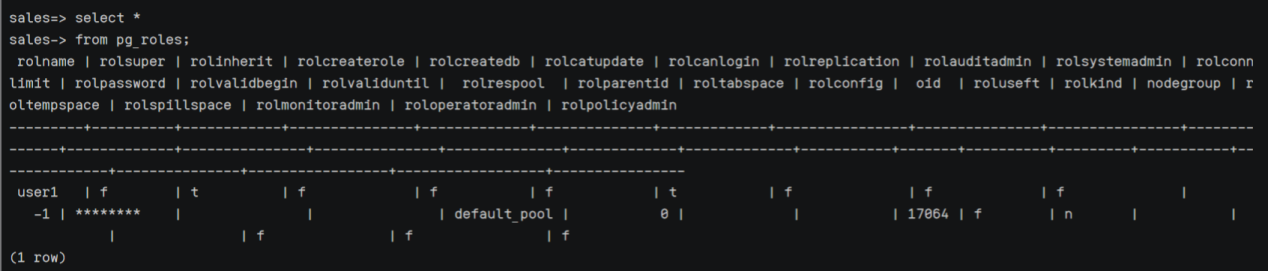


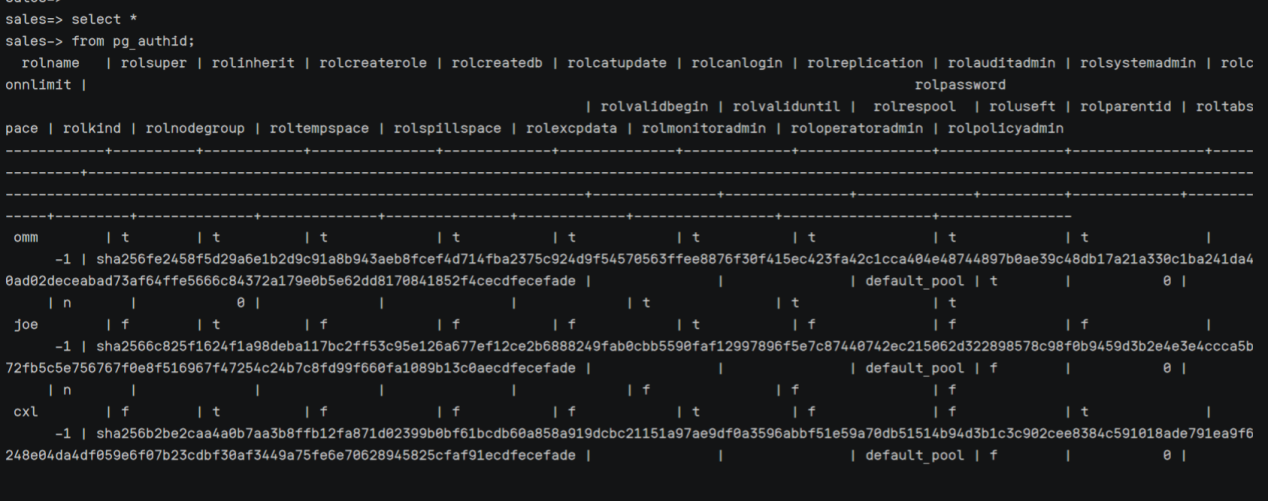
11.依次重复步骤（7）和（8），比较两次查询的结果。



此时可以查询salesman\_contacts,因为已经给予user1查询权限

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





13.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.将student表的查询权限授给u1



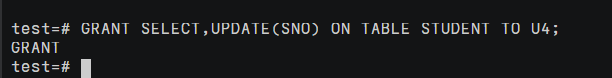
2.对student和course的所有权限授予u2和u3



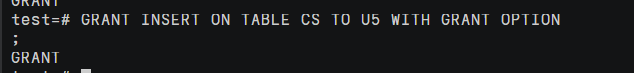
3.对sc表的查询权限授予所有用户



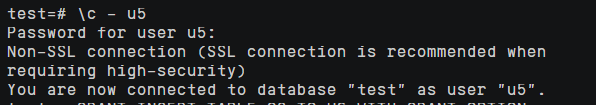
4.将查询student和修改学号的权限授予u4

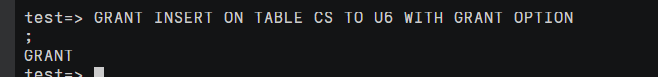


5.把对cs表插入的权限授予u5，并且可以再次授权

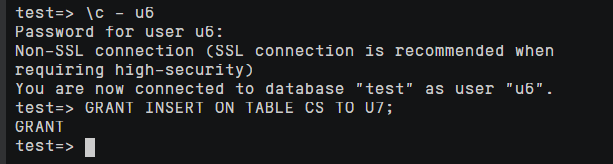


6.切换到u5，授权给u6

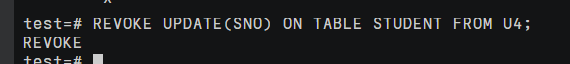




7.切换到u6，授权给u7



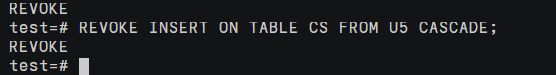
8.把用户u4的权限收回



9.收回对cs的查询权限

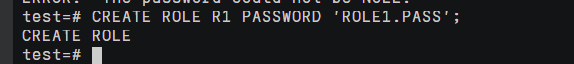


10.把u5的权限收回

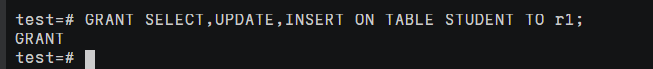


11.创建角色来授权用户

11.1新建角色



11.2授权角色



11.3授权



11.4回收



12.修改权限



13.修改权限



思考：

只有拥有DBA权限的用户才能创建新用户

角色是拥有数据库对象和权限的实体，在不同的环境中可以认为是一个或一组用户

Grant和revoke可以实现角色权限的修改

1. 实验总结

3.1 完成的工作

创建视图

创建用户，角色，对他们赋予不同的权限，收回他们的权限

3.2 对实验的认识

掌握了视图的创建；

新建用户、新建角色；

对用户和角色赋予不同的权限；

把用户的权限赋予角色；

角色的权限赋予用户；

理解视图的安全性作用；

3.3 遇到的困难及解决方法

无