实验六：数据库的安全性

1. 实验环境

- 华为 ECS+openGauss 数据库服务器平台
- **前提：**openGauss 数据库服务器正常运行
- 已建立带样例数据的 SALES 数据库

2. 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

3. 实验要求

- 完成实验内容并提交实验报告到 FTP 上的相应文件夹“实验六”。
- 实验报告提交截至日期：2022 年 12 月 2 日星期五。

4. 实验内容与步骤

（1）学习并完成 https://bokai.blog.csdn.net/article/details/117912175 的内容。

（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。

（9）发布命令：\c - whj 切换到 whj 用户—此处的 whj 应替换为你们自己创建的用户。

（10）在当前 whj 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。

/*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。

（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。

5. 实验思考

- 具有什么权限才能创建新用户？
- 角色的作用是什么？
- 如何实现角色所含权限的修改，请设计样例验证之。

6. 参考资料

- openGauss 开发者指南.pdf 之语法（16.14.75 CREATE ROLE、16.14.20 ALTER ROLE、16.14.123 DROP ROLE、16.14.91 CREATE USER、16.14.38 ALTER USER、16.14.145 GRANT、16.14.160 REVOKE、3.7 查看系统表）
- 实验一教程的相关命令
- openGauss 松鼠会： openGauss.org
- 墨天轮：https://www.modb.pro/tag/openGauss