

实验报告8

实验目的

实验内容

1. 使用 GRANT 语句对用户授权
2. 使用 WITH GRANT OPTION 子句
3. 循环授权的检测
4. 使用 REVOKE 子句收回授权

课内实验

1. 授予所有用户对表COURSES的查询权限。
2. 授予USER1对表STUDENTS插入和更新的权限，但不授予删除权限，并且授予USER1传播这两个权限...
3. 允许USER2在表CHOICE中插入元组，更新的SCORE列，可以选取除了SID以外的所有列。
4. USER1授予USER2对表STUDENTS插入和更新的权限，并且授予USER2传播插入操作的权利。
5. 收回对USER1对表COURSES查询权限的授权。
6. 由上面2. 和4. 的授权，再由USER2对USER3授予表STUDENTS插入和更新的权限，并且授予USER3 ...

自我实践

1. 授予所有用户对表STUDENTS的查询权限。
2. 授予所有用户对表COURSES的查询和更新权限。
3. 授予USER1对表TEACHERS的查询，更新工资的权限，且允许USER1可以传播这些权限。
4. 授予USER2对表CHOICES的查询，更新成绩的权限。
5. 授予USER2对表TEACHERS的除了工资之外的所有信息的查询。
6. 由USER1授予USER2对表TEACHERS的查询权限和传播的此项权限的权利。
7. 由USER2授予USER3对表TEACHERS的查询权限，和传播的此项权限的权利。再由USER3授予 USER...
8. 取消USER1对表STUDENTS的查询权限，考虑由USER2的身份对表STUDENTS进行查询，操作能否 ...
9. 取消USER1和USER2的关于表COURSES的权限。注意：以上各题目，若无特别指明，均指由表的所有...

实验问题

实验目的

熟悉数据库用户管理和权限管理，能够使用SQL语句来向用户授予和收回权限。

实验内容

1. 使用GRANT语句对用户授权，对单个用户和多个用户授权，或使用保留字PUBLIC对所有用户授权。对不同的操作对象包括数据库、视图、基本表等进行不同权限的授权。
2. 使用WITH GRANT OPTION子句授予用户传播该权限的权利。
3. 在授权时发生循环授权，考察DBS能否发现这个错误。如果不能，结合取消权限操作，查看DBS对循环授权的控制。
4. 使用REVOKE子句收回授权，取消授权的级联反应。

常用的sql句式

1. 使用 GRANT 语句对用户授权

对单个用户授权：

```
1 GRANT SELECT ON TABLE my_table TO 'username';
```

对多个用户授权：

```
1 GRANT SELECT ON TABLE my_table TO 'user1', 'user2';
```

使用 PUBLIC 对所有用户授权：

```
1 GRANT SELECT ON TABLE my_table TO PUBLIC;
```

这里，`SELECT` 是权限类型，`my_table` 是操作对象，可以是数据库、视图或基本表。

2. 使用 WITH GRANT OPTION 子句

```
1 GRANT SELECT ON TABLE my_table TO 'username' WITH GRANT OPTION;
```

这条命令授予 `username` 对 `my_table` 的 `SELECT` 权限，并允许 `username` 将此权限授予其他用户。

3. 循环授权的检测

循环授权发生在用户 A 授予用户 B 权限，并且用户 B 也授予用户 A 相同权限的情况下。PostgreSQL 通常不允许直接的循环授权，因为它在执行授权时会检查权限的授予链。如果尝试创建循环授权，PostgreSQL 会抛出错误。

4. 使用 REVOKE 子句收回授权

取消授权：

```
1 REVOKE SELECT ON TABLE my_table FROM 'username';
```

课内实验

要求：

在数据库school中建立三个用户USER1,USER2和USER3,它们在数据库中的角色是PUBLIC。请按以下要求，分别以管理员身份或这三个用户的身份登录到数据库中，进行操作。

```
1 CREATE USER user1 WITH PASSWORD 'password';
2 CREATE USER user2 WITH PASSWORD 'password';
3 CREATE USER user3 WITH PASSWORD 'password';
```

1. 授予所有用户对表COURSES的查询权限。

```
1 GRANT SELECT ON courses TO PUBLIC;
```

数据输出 消息 通知

GRANT

耗时63 毫秒 成功返回查询。

2. 授予USER1对表STUDENTS插入和更新的权限，但不授予删除权限，并且授予USER1传播这两个权限的权利。

SQL

```
1 grant update ,insert on students to USER1 with grant option
```

数据输出 消息 通知

GRANT

耗时57 毫秒 成功返回查询。

3. 允许USER2在表CHOICE中插入元组，更新的SCORE列，可以选取除了SID以外的所有列。

SQL

```
1 grant insert on choices to user2
2 grant update(score) on choice to user2
3 grant select (cid,tid,score,no) on choices to user2
```

数据输出 消息 通知

GRANT

耗时61 毫秒 成功返回查询。

4. USER1授予USER2对表STUDENTS插入和更新的权限，并且授予USER2传播插入操作的权利。

首先，以user1的身份登入服务器

连接到服务器

请输入用户'user1'的密码以连接服务器PostgreSQL 17


.....


☒ 保存密码


SQL


```
1 GRANT insert ON students TO USER2 WITH GRANT OPTION;
2 GRANT update ON students TO USER2 ;
3
```


test_3/user1@PostgreSQL 17
































无限制

查询 查询历史

```
1 -- 授予USER2对表STUDENTS的插入权限，并允许传播此权限
2 GRANT INSERT ON students TO USER2 WITH GRANT OPTION;
3
```

数据输出 消息 通知

GRANT

耗时53 毫秒 成功返回查询。

查询当前用户的权限

```

3  SELECT |
4      privilege_type,
5      is_grantable
6  FROM
7      information_schema.role_table_grants
8  WHERE
9      table_name = 'students'
10     AND (grantee = current_user OR grantor = current_user);

```

数据输出 消息 通知

	privilege_type character varying	is_grantable character varying (3)
1	INSERT	YES
2	UPDATE	YES

5. 收回对USER1对表COURSES查询权限的授权。

```

1  REVOKE SELECT ON COURSES FROM USER1;

```

SQL

```

1  REVOKE SELECT ON COURSES FROM USER1;

```

数据输出 消息 通知

REVOKE

耗时69 毫秒 成功返回查询。

6. 由上面2. 和4. 的授权，再由USER2对USER3授予表STUDENTS插入和更新的权限，并且授予USER3

传播插入操作的权利。这时候，如果由USER3对USER1授予表STUDENTS的插入和更新权限是否能

得到成功?如果能够成功，那么如果由USER2取消USER3的权限，对USER1会有什么影响?如果再由

DBA取消USER1的权限，对USER2有什么影响?

```

1 grant insert on students to user4 WITH GRANT OPTION
2
3 grant update on students to user4

```

由于update没有传播权限，所以查询出的权限为no

数据输出 消息 通知

	privilege_type character varying	is_grantable character varying (3)
1	INSERT	YES
2	UPDATE	NO

不能成功

数据输出 消息 通知

错误： 不能将grant选项授予您自己的授予者

错误： 不能将grant选项授予您自己的授予者

SQL 状态：0LP01

由于user2的权限依赖于user1所以无法直接使用，可用关键词cascade级联删除

```

19 revoke insert on students from user1
20

```

数据输出 消息 通知

错误： 存在依赖权限

HINT： 使用CASCADE回收这些权限

错误： 存在依赖权限

SQL 状态：2BP01

自我实践

1. 授予所有用户对表STUDENTS的查询权限。

```
1 GRANT SELECT ON students TO PUBLIC;
```

数据输出 消息 通知

GRANT

耗时87 毫秒 成功返回查询。

2. 授予所有用户对表COURSES的查询和更新权限。

```
1 GRANT SELECT,update ON courses TO PUBLIC;
```

数据输出 消息 通知

GRANT

耗时87 毫秒 成功返回查询。

3. 授予USER1对表TEACHERS的查询，更新工资的权限，且允许USER1可以传播这些权限。

```
1 grant select ,update(salary) on teachers to user1 WITH GRANT OPTION
```

数据输出 消息 通知

GRANT

耗时87 毫秒 成功返回查询。

4. 授予USER2对表CHOICES的查询，更新成绩的权限。

▼ SQL |

```
1 grant select ,update(score) on choices to user2
```

数据输出 消息 通知

GRANT

耗时87 毫秒 成功返回查询。

5. 授予USER2对表TEACHERS的除了工资之外的所有信息的查询。

▼ SQL |

```
1 grant select (tid,tname,email) on teachers to user2
```

数据输出 消息 通知

GRANT

耗时87 毫秒 成功返回查询。

6. 由USER1授予USER2对表TEACHERS的查询权限和传播的此项权限的权利。

▼

```
1 grant select on teachers to user
2 WITH GRANT OPTION
```

需要先登录加入user1进行授权

GRANT

耗时87 毫秒 成功返回查询。

7. 由USER2授予USER3对表TEACHERS的查询权限，和传播的此项权限的权利。再由USER3授予USER2上述权限，这样的SQL语句能否成功得到执行？

SQL

```

1  grant select on teachers to user4 WITH GRANT OPTION
2  grant select on teachers to user2 WITH GRANT OPTION

```

不能执行成功，因为循环授权。

循环授权报错

错误： 不能将grant选项授予您自己的授予者

错误： 不能将grant选项授予您自己的授予者

SQL 状态：0LP01

8. 取消USER1对表STUDENTS的查询权限，考虑由USER2的身份对表STUDENTS进行查询，操作能否成功?为什么？

SQL

```

1  REVOKE SELECT ON students FROM USER1;
2  select * from students

```

可以成功，因为user2的权力不是由user1授权的

	sid [PK] character (9)	sname character varying (30)	email character varying (30)	grade integer
1	800002933	vnbqz%svv	pvhxd4l@zqur.org	2002
2	800008565	ehlycg	nach10@uic.com	1999
3	800009026	rcxaihj	4ul4kqb@hko.edu	2002
4	800013889	nahhluoe	w6org6@maq.com	2000
5	800015244	egwwnf	pgf6@ivtri.org	1999
6	800017444	cxjinq	w047ow@nwqk.gov	1998
7	800017736	wupposq	vf1o@jiqnn.edu	1998
8	800020890	orcgzh	gfd9w9x@ipe.net	1998
9	800023487	tkbzqduq	9jlhkm@jtwg.gov	1999
10	800028044	ztozk	r369l9m@lmykh.gov	2001
11	800029781	kkivmiw	vb8bt76@jkha.edu	2000
12	800031326	frroly	c1waigg@gxo.gov	1999

9. 取消USER1和USER2的关于表COURSES的权限。注意：以上各题目，若无特别指明，均指由表的所有者授权或取消授权。

	SQL
1	REVOKE all ON COURSES FROM USER1;
2	REVOKE all ON COURSES FROM USER2;

实验问题

1. 使用GRANT语句对用户授权

通过使用GRANT语句，可以对数据库中的不同对象进行精细的权限控制。对单个用户授权时，可以精确控制每个用户的权限范围，而对多个用户授权则可以简化管理过程。使用PUBLIC可以方便地对所有用户授予相同的权限，但在安全性上可能不如单独对用户授权来得细致。如果对PUBLIC授权过于宽松，可能会降低系统的安全性。

2. 使用WITH GRANT OPTION子句

- WITH GRANT OPTION子句允许用户将他们拥有的权限授予其他用户，这在需要权限传递的场景中非常有用。例如，一个高级用户可以将权限授予其他用户，以便他们也能对其他用户进行授权。如果不当使用WITH GRANT OPTION，可能会导致权限扩散，使得权限管理变得复杂，难以追踪权限的最终来源和范围。

