

# 一. 实验目的

- 1. 熟悉SQL的数据控制操作
- 2. 能够使用SQL语句对用户进行授予和收回权限

# 二. 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，查看取消授权的级联反应。

## 实验准备

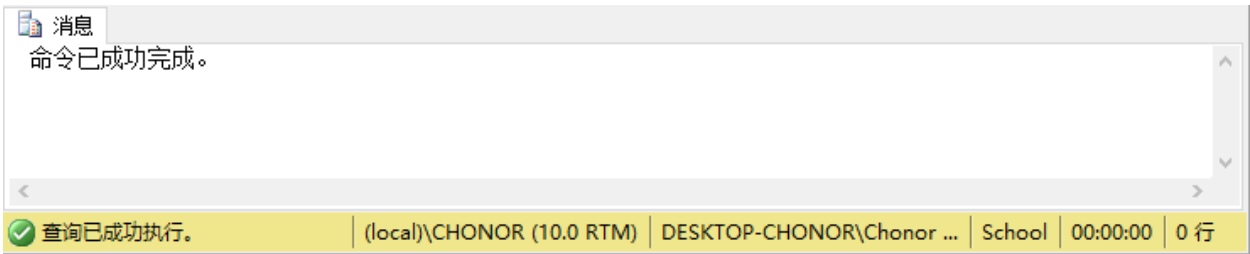
实验前，先在数据库 school中建立三个用户USER1，USER2和USER3，它们在数据库中的角色是 PUBLIC。请按以下要求,分别以管理员身份或这三个用户的身份登录到数据库中,进行操作。

- 展开“安全名”，右击“登录名”，“新建登录名”。选择“SQL Server身份验证”，输入用户名USER1，密码，以及数据库。
- 选择“服务器角色“public”，“用户映射”School。“确定”。同理，重复上述两个步骤建立USER2, USER3。
- 先设置，右键“属性“安全性”，选择“SQL和windows身份验证模式”
- 测试实验账户

# 三. 实验结果

## 1. 授予所有用户对表 STUDENTS的查询权限

```
GRANT SELECT
ON STUDENTS
TO PUBLIC
```



添加后使用USER1-3查询

```
SELECT * FROM STUDENTS
```

结果

消息

	sid	sname	email	grade
1	800001216	gfrgs	hhce4@qhldj.gov	1992
2	800002933	vnbqzsvv	pvhxd4l@zqur.org	2002
3	800005753	waqcj	hlhq0h8@jdba.gov	1992
4	800006682	fiiluommh	ihzd6_k@kzvft.gov	1992

查询已成功执行。

(local)\CHONOR (10.0 RTM) | USER1 (56) | School | 00:00:00 | 100000 行

结果

消息

	sid	sname	email	grade
1	800001216	gfrgs	hhce4@qhldj.gov	1992
2	800002933	vnbqzsvv	pvhxd4l@zqur.org	2002
3	800005753	waqcj	hlhq0h8@jdba.gov	1992
4	800006682	fiiluommh	ihzd6_k@kzvft.gov	1992

查询已成功执行。

(local)\CHONOR (10.0 RTM)

USER2 (57)

School

00:00:00

100000 行

结果

消息

	sid	sname	email	grade
1	800001216	gfrgs	hhce4@qhldj.gov	1992
2	800002933	vnbqzsvv	pvhxd4l@zqur.org	2002
3	800005753	waqcj	hlhq0h8@jdba.gov	1992
4	800006682	fiiluommh	ihzd6_k@kzvft.gov	1992

查询已成功执行。

(local)\CHONOR (10.0 RTM) | USER3 (58) | School | 00:00:00 | 100000 行

## 2. 授予所有用户对表 COURSES 的查询和更新权限

```
GRANT SELECT,UPDATE
ON COURSES
TO PUBLIC
```

消息
命令已成功完成。
查询已成功执行。
(local)\CHONOR (10.0 RTM)   DESKTOP-CHONOR\Chonor ...   School   00:00:00   0 行

添加后使用USER1-3查询

```
UPDATE COURSES
SET hour = hour + 5
WHERE cid = '10001'

SELECT * FROM COURSES
```

cid='10001'的课程初始hour=96，每个用户更新后+5

结果		消息	
	cid	cname	hour
1	10001	database	101
2	10002	operating system	88
3	10003	computer graphics	48
4	10004	java	48

查询已成功执行。 (local)\CHONOR (10.0 RTM) USER1 (56) School 00:00:00 50 行

结果		消息	
	cid	cname	hour
1	10001	database	106
2	10002	operating system	88
3	10003	computer graphics	48
4	10004	java	48

查询已成功执行。 (local)\CHONOR (10.0 RTM) USER2 (57) School 00:00:00 50 行

结果		消息	
	cid	cname	hour
1	10001	database	106
2	10002	operating system	88
3	10003	computer graphics	48
4	10004	java	48

查询已成功执行。 (local)\CHONOR (10.0 RTM) USER2 (57) School 00:00:00 50 行

### 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

此处因为只有更新工资,但是可以查询全部, 所以不用view

```
GRANT SELECT,UPDATE(salary)
ON TEACHERS
TO USER1
WITH GRANT OPTION
```

消息	
命令已成功完成。	

查询已成功执行。 (local)\CHONOR (10.0 RTM) DESKTOP-CHONOR\Chonor ... School 00:00:00 0 行

使用USER1测试一下 tid=200003125 salary初始为3928

```
UPDATE TEACHERS
SET salary = salary + 5
WHERE tid = '200003125'

SELECT * FROM TEACHERS
```

### 4. 授予USER2对表 CHOICES的查询,更新成绩的权限

此处因为只有更新分数,但是可以查询全部, 所以不用view

```
GRANT SELECT,UPDATE(score)
ON CHOICES
TO USER2
```



命令已成功完成。

查询已成功执行。

(local)\CHONOR (10.0 RTM) | DESKTOP-CHONOR\Chonor ... | School | 00:00:00 | 0 行

初始情况如下：



	no	sid	tid	cid	score
1	500000058	823069829	249596497	10037	76
2	500000253	829348273	202560416	10010	87
3	500000984	850955252	234145610	10021	54
4	500001270	847061074	292043491	10025	92

查询已成功执行。

(local)\CHONOR (10.0 RTM) | USER2 (57) | School | 00:00:01 | 299550 行

使用USER2测试一下

```
UPDATE CHOICES
SET score = score + 5
WHERE no = '500000058'

SELECT * FROM CHOICES
```



	no	sid	tid	cid	score
1	500000058	823069829	249596497	10037	81
2	500000253	829348273	202560416	10010	87
3	500000984	850955252	234145610	10021	54
4	500001270	847061074	292043491	10025	92

查询已成功执行。

(local)\CHONOR (10.0 RTM) | USER2 (57) | School | 00:00:01 | 299550 行

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

```
GRANT SELECT
ON TEACHERS
TO USER2
WITH GRANT OPTION
```



命令已成功完成。

查询已成功执行。

(local)\CHONOR (10.0 RTM) | USER1 (56) | School | 00:00:00 | 0 行

使用USER2测试一下

SELECT \* FROM TEACHERS

结果消息

	tid	tname	email	salary
1	200003125	fqmyi	wcjcg@glq.net	3928
2	200005322	udjom	gd5l8@ppmlf.gov	873
3	200009423	jhoulvtr	12cj@pzc.gov	3286
4	200010493	xzgkflko	zcf_m@def.com	3332

查询已成功执行。 (local)\CHONOR (10.0 RTM) USER2 (57) School 00:00:00 15000 行

6. 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?

USER2授予USER3

GRANT SELECT  
ON TEACHERS  
TO USER3  
WITH GRANT OPTION

消息

命令已成功完成。

查询已成功执行。 (local)\CHONOR (10.0 RTM) USER2 (57) School 00:00:00 0 行

USER3授予USER2

GRANT SELECT  
ON TEACHERS  
TO USER2  
WITH GRANT OPTION

消息

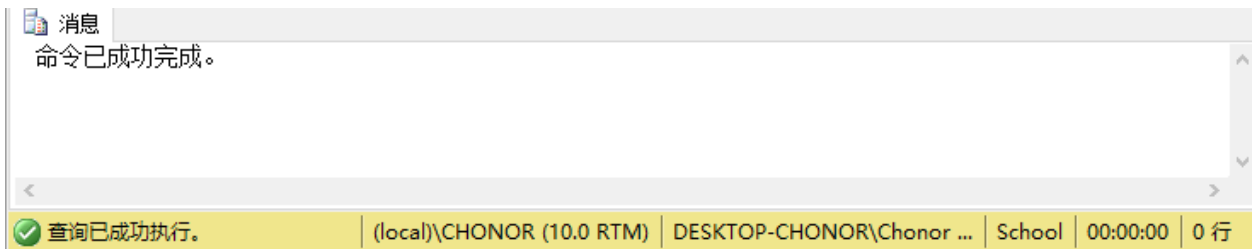
命令已成功完成。

查询已成功执行。 (local)\CHONOR (10.0 RTM) USER3 (58) School 00:00:00 0 行

命令可以成功执行

7. 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?

```
REVOKE SELECT
ON STUDENTS
FROM USER1
```



此时用USER1发现USER1还有对于对STUDENTS的查询权限。因为本实验任务1已经将表STUDENTS的查询权限授予了 PUBLIC,因此数据库中凡是具有 PUBLIC角色的用户都拥有对表 STUDENTS的查询权限。而USER1是PUBLIC角色,此时在使用USER2查询还是可以成功的因为USER2同时也是PUBLIC角色。

我们可以使用

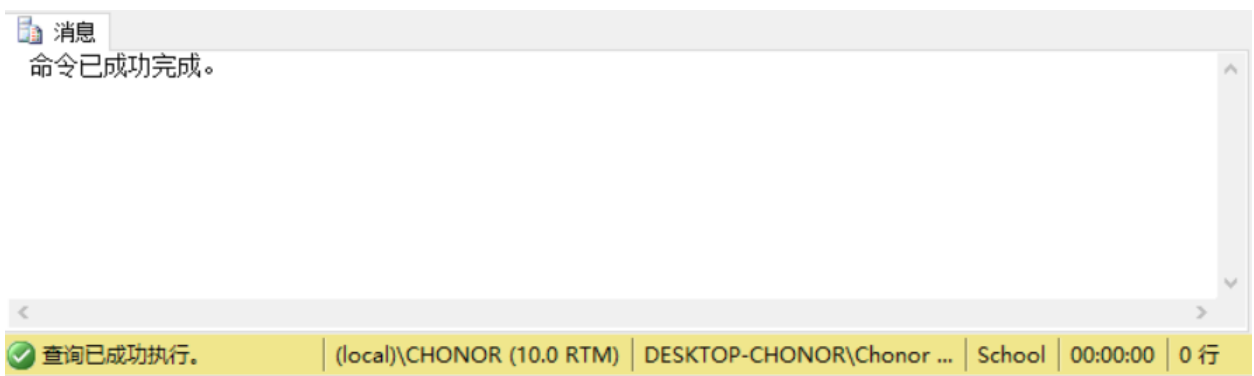
```
REVOKE SELECT
ON STUDENTS
FROM PUBLIC
```

这样就去除了所有PUBLIC用户的权限,此时USER1-3都无法查询。

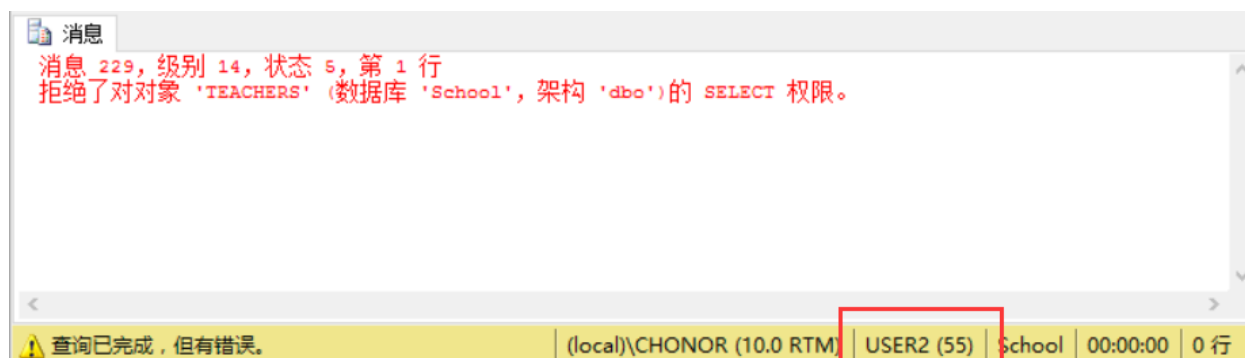
**(改)取消USER1对表 TEACHERS的查询权限,考虑由USER2的身份对表 TEACHERS进行查询,操作能否成功?为什么?**

```
REVOKE SELECT
ON TEACHERS
FROM USER1
CASCADE
```

此处需要加上CASCADE因为对于有传播权利的授权取消需要加上CASCADE,否则会报错:若要撤消或拒绝可授予的特权,请指定 CASCADE 选项。



此时USER2不能查询

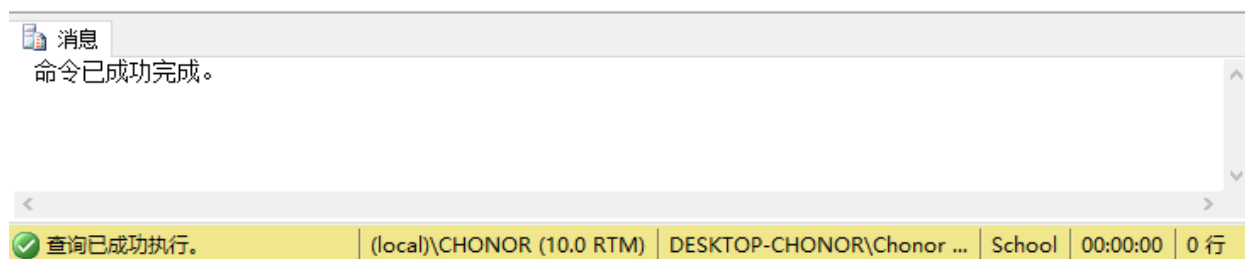


因为管理员取消时是级联删除。

#### 8. 取消USER1和USER2的关于表 COURSES的权限

```
REVOKE SELECT,UPDATE
ON COURSES
FROM USER1,USER2
```

结果如下：



此时还是可以查询。因为本实验任务1已经将表COURSES的查询权限授予了 PUBLIC,因此数据库中凡是具有PUBLIC角色的用户都拥有对表 COURSES的查询权限。而USER1是PUBLIC角色，此时在使用USER2查询还是可以成功的因为USER2同时也是PUBLIC角色。，在任务2中 PUBLIC角色的用户都拥有对表 COURSES的查询和更新权限。

可以使用如下命令直接去除权限达到目标

```
REVOKE SELECT
ON COURSES
FROM PUBLIC
```

## 四. 实验感想

这次实验主要是数据库中的授权操作，授权问题算是很简单的了，因为不用涉及查询什么的，只需要进行权限处理，主要还是理解一下各种权限操作的用法，和一些特殊情况，比如7.8中的取消问题。