

# 授权控制



# 讲授内容

- 1 授权GRANT
- 2 收权REVOKE



## 自主访问控制

- 自主访问控制就是用户自主控制对数据库对象的操作权限。

### ❖ 操作权限

- 创建CREATE
- 修改ALTER
- 删除DROP
- 查询SELECT
- 插入INSERT
- 修改UPDATE
- 删除DELETE

### ❖ 数据库用户

- 系统管理员用户(SA)
- 数据库管理员 (DBA)
- 数据库对象用户
- 数据库访问用户

### ❖ 数据库对象

- 数据库
- 基本表
- 视图
- 索引



## 授权GRANT

GRANT授权语句的一般格式:

**GRANT** <权限列表>

SELECT,INSERT,  
UPDATE,DELETE

**ON** <数据库对象>

基本表,视图

**TO** <用户表>

[ WITH GRANT OPTION ]

授权的用户可以将权限  
继续转授给其他用户





## 授权GRANT

- 把查询SC表和修改学生成绩的权限授给用户U4，并允许其将权限转授出去。

**GRANT** SELECT, UPDATE (GRADE)  
**ON** SC  
**TO** U4  
**WITH GRANT OPTION;**

列权限

主体 (P): U4

授权者 (G): dbo

表名 (M): dbo.SC

权限名称 (M): 更新

列权限 (C):

列名	授予	具有授...	拒绝
CNO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GRADE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

确定 取消 帮助

dbo.SC 的权限 (P):

显式 有效

权限	授权者	授予	具有授...	拒绝
更改		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
更新		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
更新	dbo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
接管所有权		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
控制		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
删除		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
选择		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
选择	dbo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
引用		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

列权限 (C)...

确定 取消



## 收权REVOKE

REVOKE收权语句的一般格式:

**REVOKE** [GRANT OPTION FOR] <权限表>  
**ON** <数据库对象>  
**FROM** <用户表>  
[CASCADE | RESTRICT]

只有授权权限被收回

把该用户授权给其他用户的权限同时级联收回

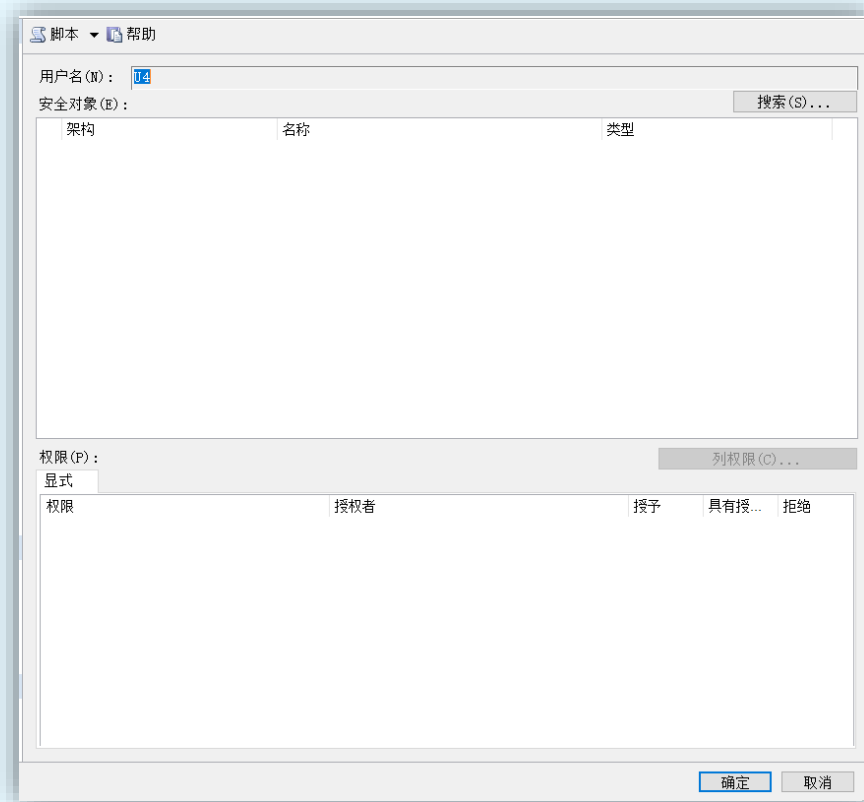
当用户没有给其他用户授权时，才能收回权限



## 收权REVOKE

- 把用户U4查询和修改学生学号的权限收回，并级联收回所授出的权限。

```
REVOKE SELECT, UPDATE (GRADE)  
ON SC  
FROM U4  
CASCADE;
```

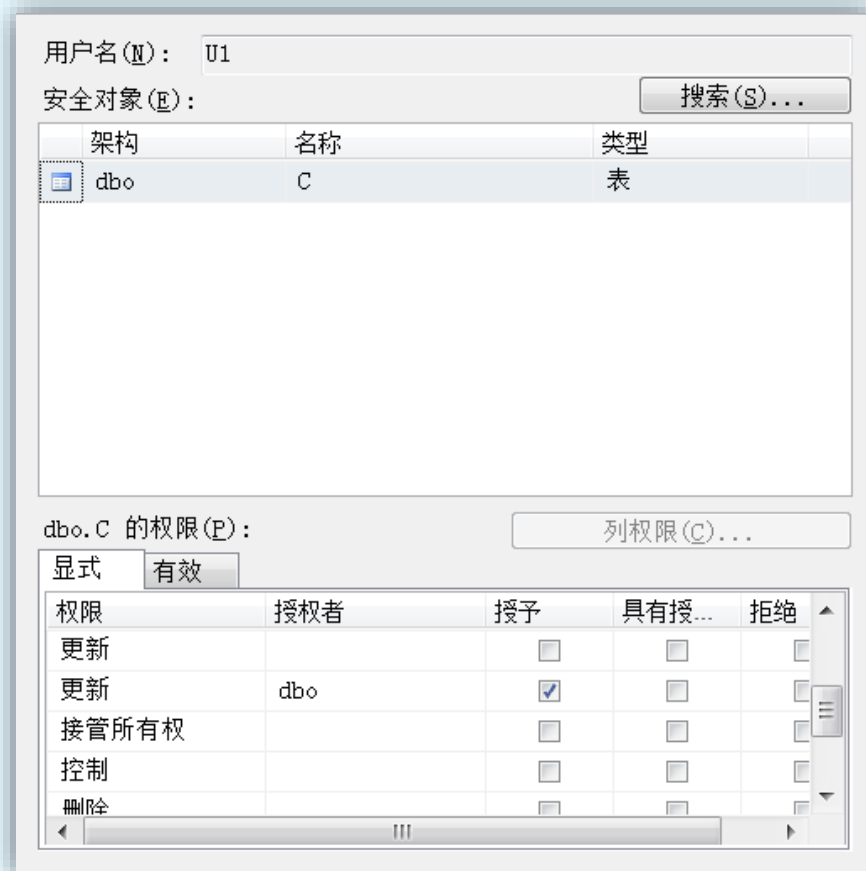




## 自主访问控制示例

► (1) 授予用户U1对表C的更新权限。

**GRANT UPDATE ON C TO U1;**







## 自主访问控制示例

- (2) 授予用户U1对表S的查询权限，并具有给其他用户授权的权限。

**GRANT SELECT ON S TO U1  
WITH GRANT OPTION;**

用户名(N): U1

安全对象(O):  搜索(S)...

架构	名称	类型
dbo	C	表
dbo	S	表

dbo. S 的权限(P):  列权限(C)...

显式 有效

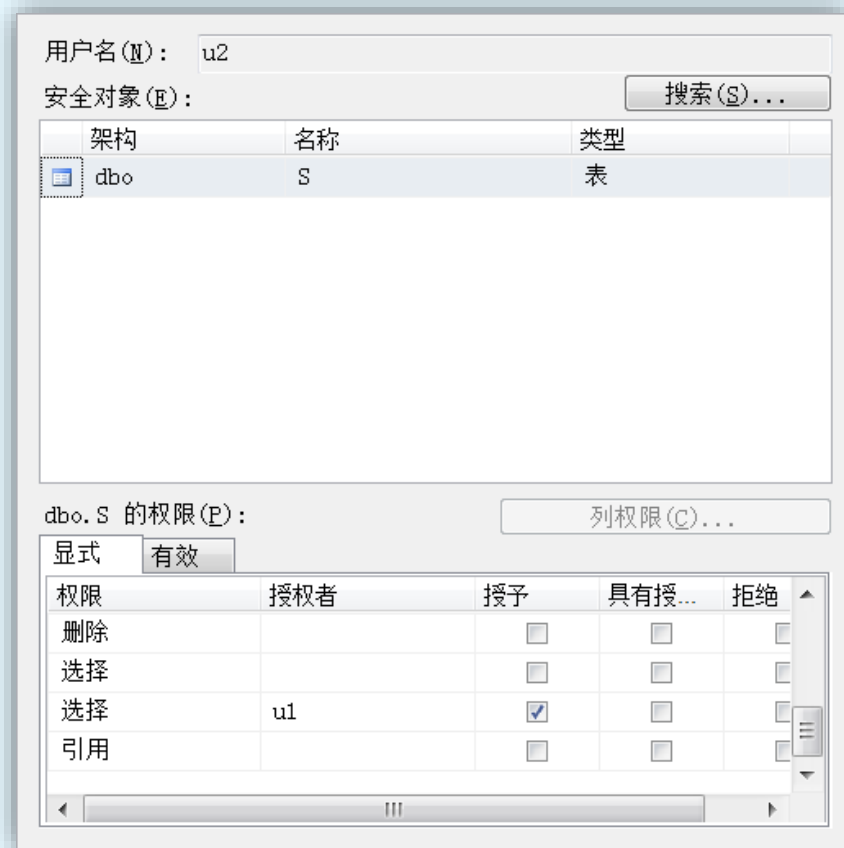
权限	授权者	授予	具有授...	拒绝
控制		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
删除		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
选择		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
选择	dbo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
引用		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## 自主访问控制示例

► (3)以U1登录，把对学生表S的查询权限授予用户U2。

**GRANT SELECT ON S TO U2;**

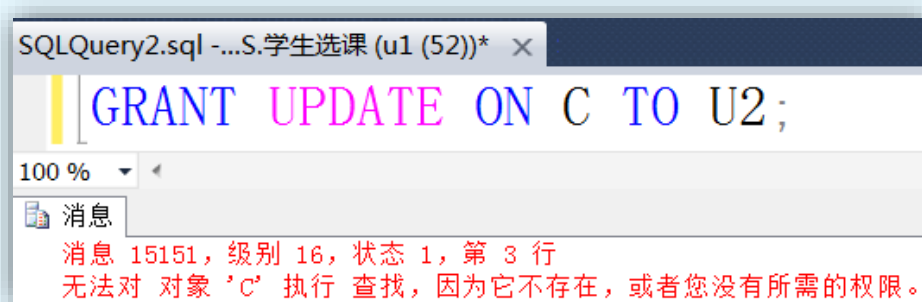




## 自主访问控制示例

- (4) U1再把对课程表C的更新权限授予用户U2。

**GRANT UPDATE ON C TO U2;**

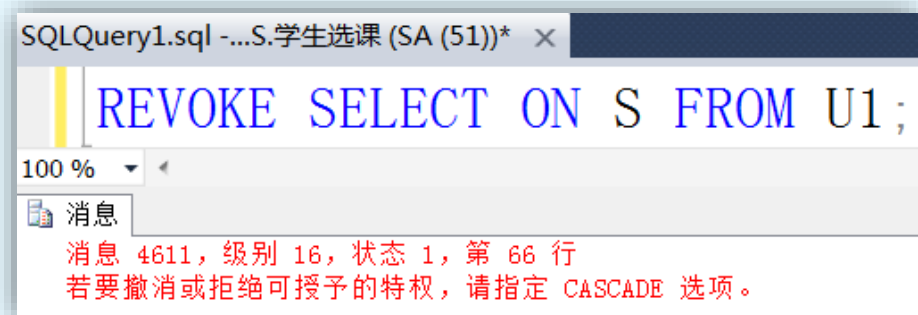




## 自主访问控制示例

- (5) 数据库管理员要收回用户U1对学生表S的查询权限。

**REVOKE SELECT ON S FROM U1;**





## 自主访问控制示例

- (6) 数据库管理员级联收回用户U1对学生表S的查询权限。

**REVOKE SELECT ON S FROM U1**

**CASCADE;**

用户名(U): U1  
安全对象(O):  搜索(S)...

架构	名称	类型
dbo	C	表

dbo.C 的权限(P):  列权限(C)...

权限	授权者	授予	具有授...	拒绝
更新		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
更新	dbo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
接管所有权		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
控制		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
删除		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

用户名(U): u2  
安全对象(O):  搜索(S)...

架构	名称	类型
----	----	----

权限(P):  列权限(C)...

权限	授权者	授予	具有授...	拒绝
----	-----	----	--------	----



## 自主访问控制示例

- ▶ (7)在用户U1具有对学生表S的SELECT权限时，再授予其对视图M\_S的SELECT和UPDATE权限。

**GRANT SELECT, UPDATE**

**ON M\_S**

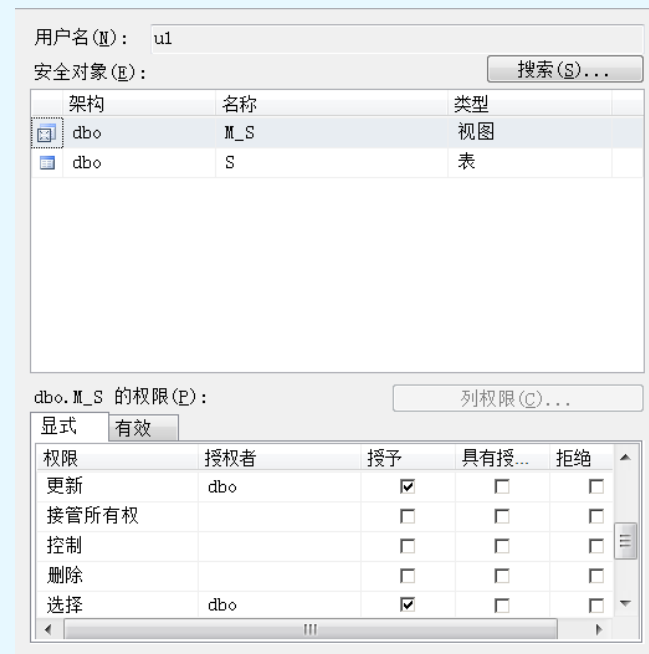
**TO U1;**

**CREATE VIEW M\_S (M\_SNO,M\_SN,M\_SB)**

**AS SELECT SNO, SN, SB**

**FROM S**

**WHERE SD = '数学' ;**







## 自主访问控制示例

- ▶ (8) 用户U1修改视图中属性SNO值为“S16”的学生姓名为“王廷”。

```
UPDATE M_S  
SET M_SN= '王廷'  
WHERE M_SNO='S16';
```

SQLQuery3.sql -...S.学生选课 (u1 (56))\* x

```
UPDATE M_S  
SET M_SN='王廷'  
WHERE M_SNO='S16';
```

100 %

消息

(1 行受影响)

SQLQuery3.sql -...S.学生选课 (u1 (56))\* x

```
SELECT * FROM S  
WHERE SNO='S16';
```

100 %

结果 消息

	SNO	SN	SEX	SB	SD
1	s16	王廷	男	2000-10-01	数学



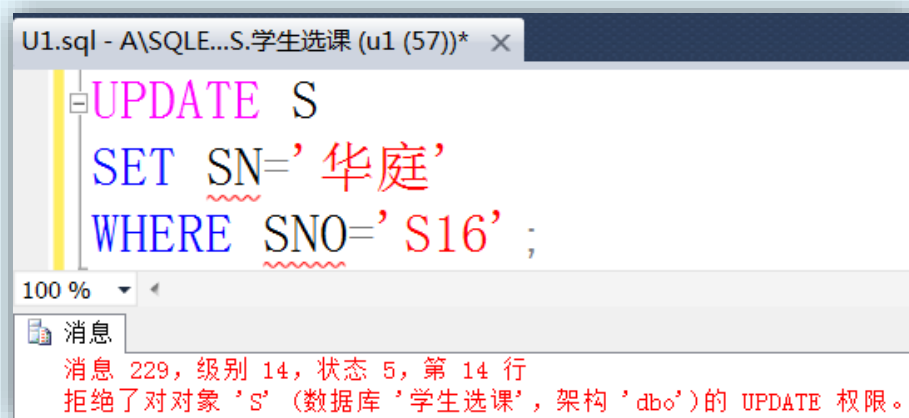
## 自主访问控制示例

- ▶ (9)用户U1再来修改学生表S中属性SNO值为“S16”的学生姓名为“华庭”。

**UPDATE S**

**SET SN= '华庭'**

**WHERE SNO='S16';**





## 自主访问控制示例

- 用户所具有的关系上的权限与其拥有的关系上的视图的权限是不同的。
- 用户只能在其具有的权限下对数据库进行操作。
- DBMS可通过为用户定义视图，并为用户授予访问视图的相关权限，在满足用户操作需求的情况下，提高了数据库中数据的安全性。



## 自主访问控制示例

- 利用**GRANT**和**REVOKE**语句，用户可以“自主”地决定将数据的存取权限授予其他用户，“自主”地决定是否也将“授权”的权限授予其他用户。



## 小结

- 基于角色的访问控制通过给角色授权来简化为用户授权的过程。
- 自主访问控制 (Discretionary Access Control) 通过GRANT和REVOKE语句实现权限的管理。访问控制方式灵活，但容易失控。
- 高安全级别的DBMS要求支持强制访问控制 (Mandatory Access Control) 。