数据库上机 （五） 数据库安全性访问控制

一、实验目的

1. 掌握SQL Server访问控制方法。

2. 熟悉自主访问控制机制。

3. 熟练使用授权和回收语句。

二、实验内容和要求

利用前面建立的学生数据库和其中的Student、Course、SC表，并利用SSMS工具完成下列操作。

1. 用SSMS工具建立SQL Server身份验证模式的登录名：log1、log2和log3。

方法一：图形界面方式。

方法二：SQL语句

CREATE LOGIN <登录名> WITH PASSWORD='<密码>'

CREATE LOGIN log1 WITH PASSWORD='123456'

CREATE LOGIN log2 WITH PASSWORD='123456'

CREATE LOGIN log3 WITH PASSWORD='123456'

1. 用log1建立一个新的数据库引擎查询，在“可用数据库”下拉列表框中是否能选中学生数据库？为什么？

**答：不能选中。因为log1添加为学生数据库中的用户**

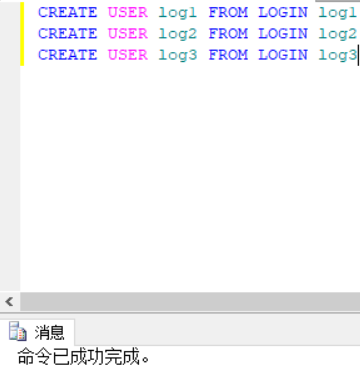
3.    用系统管理员身份建立一个新的数据库引擎查询，将log1、log2和log3映射为学生数据库中的用户，用户名同登录名。

（1）创建用户log1，log2，log3。

方法一：图形界面方式。

方法二：SQL语句

CREATE USER <用户名> FROM LOGIN <登录名>



（2）创建架构（schema）log1，log2，log3，架构所有者分别是用户log1，log2，log3

（3）修改log1，log2，log3用户的默认架构

1. 在log1建立的数据库引擎查询中，现在在“可用数据库”下列列表框中是否能选中学生数据库？为什么？

**答：可以，因为log1已经是学生数据库的用户**

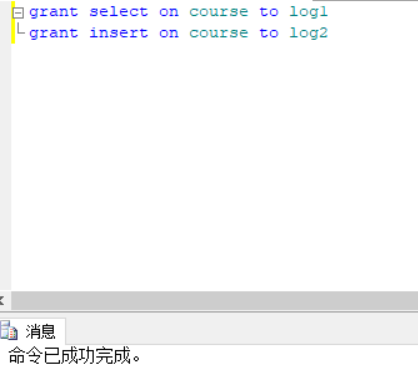
5.      在log1建立的数据库引擎查询中，选中学生数据库，执行下述语句，能否成功？为什

么？

SELECT \* FROM Course

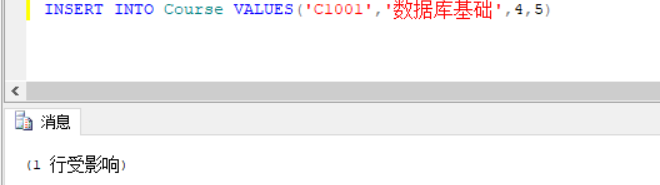
**答：不能，因为没有授予log1 查询course的权限**

6.      在系统管理员的数据库引擎查询中，执行合适的授权语句，授予log1具有对Course表的查询权限，授予log2具有对Course表的插入权限。



7.      用log2登陆，建立一个新的数据库引擎查询，执行下述语句，能否成功？为什么？

INSERT INTO Course VALUES('C1001'，'数据库基础'，4，5)



可以，因为已经授予log2插入course表的权限

再执行下述语句，能否成功？为什么？

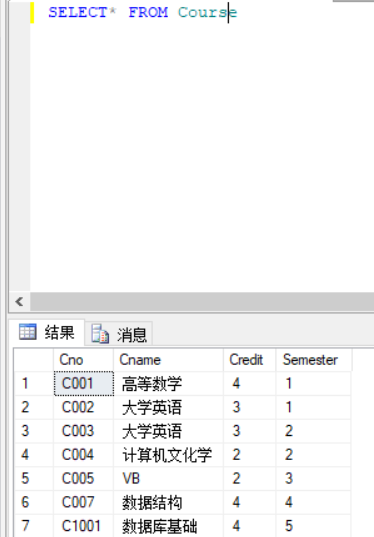
SELECT \* FROM Course

**答：不能成功，因为没有没有授予log2查询course表的权限**

8.      在log1建立的数据库引擎查询中，再次执行下述语句：

    SELECT\* FROM Course

这次能否成功？



**答：可以，因为已经授予log1查询course表的权限**

如果执行下述语句：

INSERT INTO Course VALUES('C103','软件工程',4, 5)

能否成功？为什么？

**答：不能，因为没有没有授予log1插入course表的权限**

9.     登陆 log3，建立一个新的数据库引擎查询，执行下述语句，能否成功？为什么？

    CREATE TABLE NewTable(

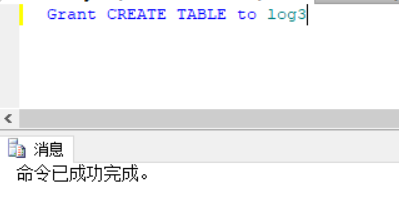
      C1 int,

      C2 char(4))

**答:不能，因为没有创建表的权限**

10.   授予log3在学生数据库中具有创建表的权限。

Grant CREATE TABLE to log3



11.  登陆log3用户，建立一个新的数据库引擎查询中，再次执行第9题的语句，能否成功？为什么？



**答：可以成功，因为已经授予了log3创建表的权限**

注意：数据库的下级对象应该是架构（schema），如果想获得创建表对象的权限，必须要获得使用架构的权限，因此我们在第3题的第（2），（3）步中创建了相应架构（log3并没有默认架构dbo的使用权限），并获得了使用权限，这样才可以创建表对象。

如果执行下述语句：

   SELECT \* from NewTable

能否成功？表的架构名是什么？为什么？

**答：可以成功，log3，因为前面已经将默认架构名改为log3**

SQL Server给用户提供了预定义的服务器角色和数据库角色，这些角色不能添加、修改和删除。用户可以根据需要，创建自己的数据库角色，一边对具有相同操作的用户进行统一管理。

12.新建登陆名log4，映射为学生数据库用户log4，为该用户选定角色为db\_Owner，登陆log4，看看是否能够访问数据库，执行以下操作

（1）Select \* from student

（2）INSERT INTO Course VALUES('C1016'，'VB基础'，4，5)

（3）CREATE TABLE NewTable2(

      C1 int,

      C2 char(4))

能否进行，为什么？

**答：可以，因为log4位db\_Owner,数据库拥有者角色，具有学生数据库的所有权限**

13.新建角色R1，赋予查询student表、更新Sc表grade列权限，将角色R1授予用户log1，log2，接着执行

grant select on student to R1

grant update on sc(grade) to R1

（1）Select \* from student ok

（2）Update sc

Set grade=grade\*0.9

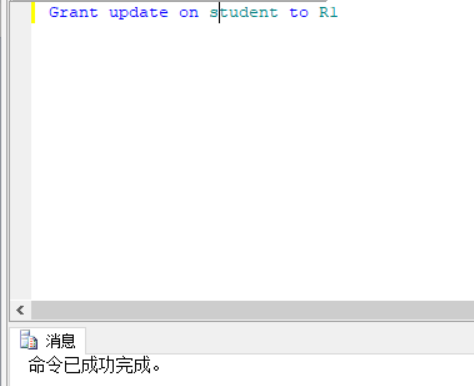
验证log1，log2用户的相应权限。

语句1可以成功执行，语句2不能。因为更新需要先查询，没有查询权限更新不了。故授予了查询权限之后才能够进行更新操作。

（3）如果想收回用户log1，log2查询student表的权限，增加对student表的更新权限，请问可以怎么操作？

revoke select on student from R1

Grant update on student to R1



试一试图形界面方式和sql语句两种方式。

注意：在Ms sql server中，向角色中添加用户的语句为

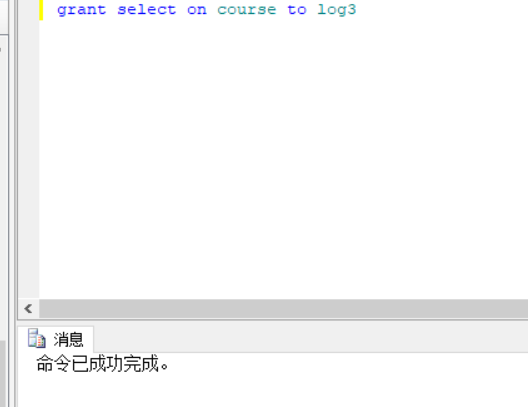
sp\_addrolemember ‘角色’,’用户’

从角色中删除用户的语句为：sp\_droprolemember ‘角色’,’用户’

14. 用户log1的权限如果想转授权给log3，应该怎么操作？动手实践验证你的想法。

grant select on course to log1 with grant option

在授权给log1的时候在后面添加with grant option，让其有权将权限授予其他用户



上述诸题，如果操作能够成功，请给出相应SQL语句以及结果截屏，如果不能成功，请说明原因。

在第一次实验结果的基础上进行本次数据查询操作，提交查询结果。

实验报告应包括：实验标题、实验目的，实验内容，实验结果，实验小结

其中实验结果应包含本次实验要用到的SQL语句，能够执行的操作对结果进行截图，不能的进行也请对系统的拒绝结果窗口进行截图，并分析不能进行的原因。

实验小结主要提交在实验中遇到的问题及解决方法。

以姓名+学号为文件名存盘，提交给学委

修改登陆信息，用户信息

--禁用登陆帐户

alter login [登录名] disable

--启用登陆帐户

alter login [登录名] enable

--登陆帐户改名

alter login [登录名] with name=dba\_tom

--登陆帐户改密码：

alter login [登录名]with password='aabb@ccdd'

--数据库用户改名：

alter user [用户名] with name=dba\_tom

--更改数据库用户 defult\_schema：

alter user [用户名] with default\_schema=sales

--删除数据库用户：

drop user [用户名]

--删除 SQL Server登陆帐户：

drop login [登录名]

https://blog.csdn.net/a123132123/article/details/102344611