实验九：安全访问授权

一、实验目的

（1）理解 SQL Server 的安全权限管理方法。

（2）深入理解 SQL Server 的登录名、各种固定服务器角色、数据库用户、各种固定数据库角色、架构等概念及用途。

（3）深入理解对象权限、语句权限和隐式权限的概念。

（4）熟练创建登录名、数据库用户，并能熟练应用 SQL 语句进行安全授权管理。

二、实验前期准备

（1）利用 SQL 语言，创建数据库 SchoolManagement，关系表分别如下。

a、学生关系表 S：

学号 Sno	姓名 Sname	性别 Ssex	年龄 Sage	所在系 Sdept	出生地 BirthPlace
主键	非空	非空	非空	非空	允许空

b、课程关系表 C：

课程号 Cno	课程名 Cname	先行课 Cpno	学分 Ccredit
主键	非空	外键，允许空	非空，整数

c、选修关系表 SC：

学号 Sno	课程号 Cno	成绩 Grade
主键		非空，两位小数

（2）利用 SQL 语言，向建立的数据库中插入记录。要求：

a、学生关系表 S 中插入各学生自己所在班的全体学生的信息。

b、课程关系表 C 插入至少 10 门课程信息（每个学生输入的课程不能相同）。

c、选修关系表 SC 至少要 20 名同学有选课信息，且至少要有 5 名同学选修了所有课程，有 10 名同学选修了 3 门以上课程。

三、实验内容

1、创建登录名、数据库用户，实现对数据库的访问

（1）创建登录名 dlm1，dlm2，dlm3，dlm4，dlm5 并赋予固定服务器角色。

（2）针对 SchoolManagement 数据库，创建数据库用户 U1，U2，U3，U4，U5。

（3）分别将所创建的各数据库用户关联到各登录名（一个登录名可以作为不同用户映射到不同的数据库，但在每个数据库中只能作为一个用户进行映射。）。

（4）通过登录名与数据库用户，实现对数据的访问。

（5）要求分别使用 SSMS 和 T_SQL 语句，对以上（1）~（4）加以实现。

2、授权、回收权限

（1）把查询 S 表权限授给用户 U1。

（2）把对 S 表和 C 表的全部权限授予用户 U2 和 U3。

（3）把对表 SC 的查询权限授予所有用户。

（4）把查询 S 表和修改学生姓名的权限授给用户 U4。

（5）把对表 SC 的 INSERT 权限授予 U5 用户，并允许他再将此权限授予其他用户。

（6）把用户 U4 修改学生学号的权限收回。

（7）收回所有用户对表 SC 的查询权限。

（8）把用户 U5 对 SC 表的 INSERT 权限收回。

3、权限验证

（1）以上所有的授权，均须通过相应的 SQL 语句予以验证。

（2）权限验证要求：比如针对用户 U1 查询学生表 S：

a、授权前用户时候可以查询？

b、如果不可以查询，授权后是否可以查询？

c、如果可以查询，回收权限后是不是不能再查询？

4、熟练掌握以下存储过程并通过实验予以应用（带“*”表示重要）

（1）*sp_addlogin：创建登录名。

（2）*sp_droplogin：删除登录名。

（3）sp_addrole：创建角色。

（4）*sp_adduser：创建用户。

（5）sp_grantlogin：添加 Windows NT 用户或组。

（6）sp_defaultdb：更改登录的默认数据库

（7）*sp_addsrvrolemember：将登录名添加到固定服务器角色。

（8）sp_dropsrvrolemember：从固定服务器角色中删除登录名。

（9）sp_srvrolepermission：浏览固定服务器角色的权限。

（10）SP_HELPSRVROLE：查看服务器角色。

（11）SP_HELPSRVROLEMEMBER：查看服务器角色成员。

（12）SP_HELPdbfixedrole：浏览固定的数据库角色。

（13）SP_HELPROLEMEMBER：查看数据库角色成员。

（14）SP_HELPROLE：查看数据库角色。

（15）SP_HELPUSER：查看数据库用户信息。

（16）*sp_helplogins：查看每个数据库中的登录及相关用户的信息

（17）sp_password：添加或更改登录密码。

（18）sp_revokelogin：删除用 sp_grantlogin 或 sp_denylogin 创建的用户。

（19）xp_logininfo ：查看帐户、帐户类型、帐户的特权级别、帐户的映射登录名和帐户访问的权 限路径

（20）sp_change_users_login：①：exec sp_change_users_login 'REPORT' 列出当前数据库的孤立用户（某个数据库的帐户只有用户名而没有登录名）；②：exec sp_change_users_login 'AUTO_FIX','用户名' 可以自动将用户名所对应的同名登录添加到 syslogins 中；③：exec sp_change_users_login 'UPDATE_ONE','用户名','登录名' 将用户名映射为指定的登录名。

四、实验要求：

（1）请同学们事先做好准备；

（2）独立编写代码，调试通过，完成实验。

五、附录：固定服务器角色与固定数据库角色

固定的服务器角色

角色	描述
①sysadmin	可执行任何操作
②dbcreator	创建和修改数据库
③diskadmin	管理磁盘文件
④serveradmin	配置服务器级的设置
⑤securityadmin	管理和审核服务器登录
⑥processadmin	管理 SQL Server 进程
⑦bulkadmin	执行 BULK INSERT 语句
⑧setupadmin	配置和复制已链接的服务器
⑨public	

固定的数据库角色

角色	描述
①db_owner	数据库所有者，可执行数据库的所有管理操作。
②db_accessadmin	数据库访问权限管理者，具有添加、删除数据库使用者、数据库角色和组的权限。
③db_securityadmin	数据库安全管理员，可管理数据库中的权限，如设置数据库表的增、删、修改和查询等存取权限。
④db_ddladmin	数据库DDL管理员，可增加、修改或删除数据库中的对象
⑤db_backupoperator	数据库备份操作员，具有执行数据库备份的权限。
⑥db_datareader	数据库数据读取者
⑦db_datawriter	数据库数据写入者，具有对表进行增、删修改的权限。
⑧db_denydatareader	数据库拒绝数据读取者，不能读取数据库中任何表内容。
⑨db_denydatawriter	数据库拒绝数据写入者，不能对任何表进行增、删修改操作。
⑩public	是一个特殊的数据库角色，每个数据库用户都是 public 角色的成员。