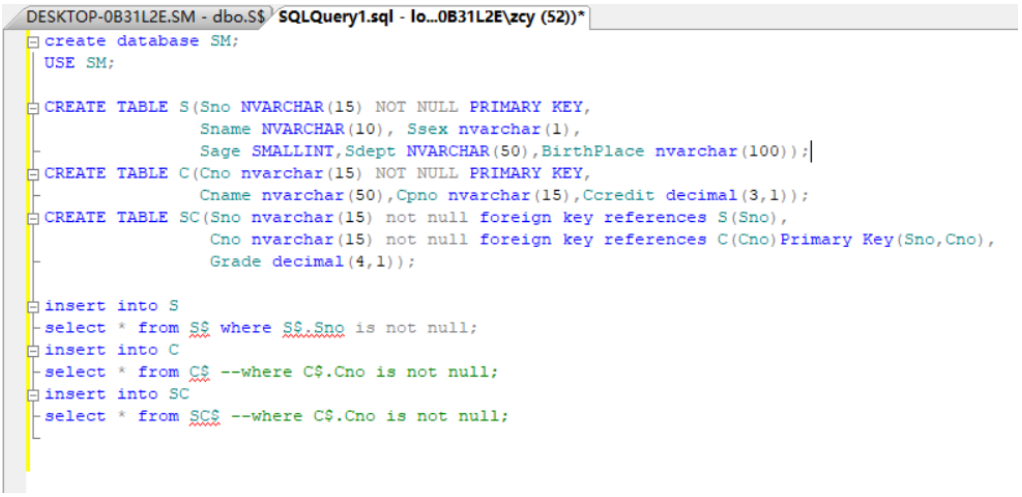
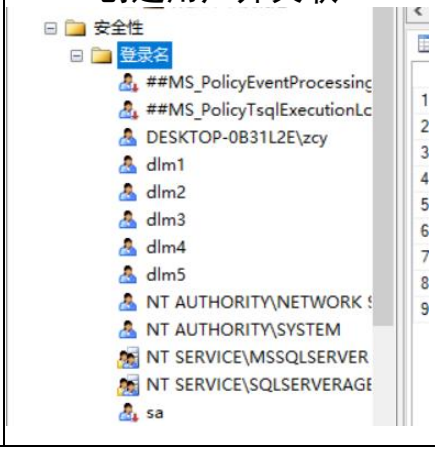
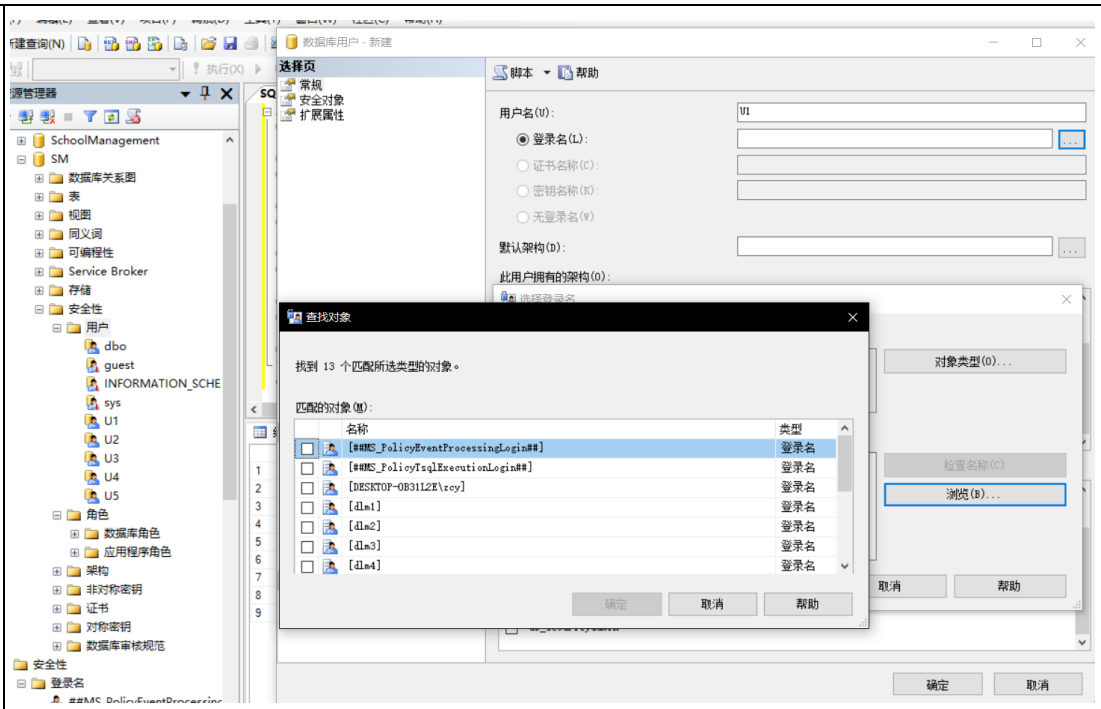
上机实验报告

课程名：_____ 指导教师：_____

姓名		班级		实验得分	
		学号			
实验时间		实验地点			
实验主题	SQL 的安全授权功能				
实验目的	（1）理解 SQLServer 的安全权限管理方法。 （2）深入理解 SQLServer 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。				
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。并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。）。 （3）通过登录名与数据库用户，实现对数据的访问。 （4）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。
实验结果/实验结论	创建表 创建数据库和表以及插入从 excel 导入的数据  TSQL 创建登录用户并关联数据库用户  SSMS 创建用户并关联 



授权、回收权限并进行权限验证

（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。

授予权限之前：

```
select *from S
```

```
消息
消息 229，级别 14，状态 5，第 1 行
拒绝了对对象 'S' (数据库 'SM'，架构 'dbo')的 SELECT 权限。
消息
消息 229，级别 14，状态 5，第 1 行
拒绝了对对象 'C' (数据库 'SM'，架构 'dbo')的 SELECT 权限。
消息
消息 229，级别 14，状态 5，第 3 行
拒绝了对对象 'SC' (数据库 'SM'，架构 'dbo')的 SELECT 权限。
消息
消息 229，级别 14，状态 5，第 4 行
拒绝了对对象 'SC' (数据库 'SM'，架构 'dbo')的 INSERT 权限。
消息
消息 229，级别 14，状态 5，第 5 行
拒绝了对对象 'SC' (数据库 'SM'，架构 'dbo')的 SELECT 权限。
消息 229，级别 14，状态 5，第 5 行
拒绝了对对象 'SC' (数据库 'SM'，架构 'dbo')的 UPDATE 权限。
```

把查询 S 表权限授给用户 U1。

```
GRANT SELECT ON SC TO U1 --WITH GRANT OPTION
```

消息

命令已成功完成。

```
SELECT * FROM S;
```

结果 消息

Sno	Sname	Ssex	Sage	Sdept	BirthPlace
2016302251	杨波	男	23	网安	北京
2017300870	高胜远	男	22	网安	上海

把对 S 表和 C 表的全部权限授予用户 U2 和 U3。

```
grant all privileges
on S
to u2,u3;
grant all privileges
on C
to u2,u3;
```

消息

命令已成功完成。

```
SELECT * FROM S;
SELECT *FROM C
```

结果 消息

Cno	Cname	Cpno	Ccredit
C01001	高等数学（上）	NULL	6.0
C01002	高等数学（下）	C01001	6.0
C01003	线性代数	C01001	2.5

把对表 SC 的查询权限授予所有用户。

```
grant select
on sc
to public;
```

消息

命令已成功完成。

```
SELECT * FROM SC
```

结果 消息

Sno	Cno	Grade
2018302186	C01001	99.0
2018302186	C01002	69.0
2018302186	C01003	101.0
2018302186	C01004	77.0
2018302186	C01005	59.0

把查询 S 表和修改学生姓名的权限授给用户 U4。

```
grant select,update(sname)
on S
to U4;
```

消息

命令已成功完成。

```
UPDATE S set sname='tyx' where sno='2018302198'
SELECT * FROM S
```

结果 消息

Sno	Sname	Ssex	Sage	Sdept	BirthPlace
2018302198	tyx	男	19	网安	北京

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。

```
grant insert
on SC
to U5
with grant option;
```

消息

命令已成功完成。

U5 赋权 U4

```
grant insert
on SC
to U4
```

消息

命令已成功完成。

把用户 U4 修改学生学号的权限收回。

无法完成，前面赋予的是更改学号权限

语句如下：

```
revoke update(sno)
on S
from U4;
```

消息

消息 15151，级别 16，状态 1，第 13 行
无法对 对象 's' 执行 查找，因为它不存在，或者您没有所需的权限。

收回所有用户对表 SC 的查询权限。

```
revoke select
on sc
from public;
```

消息

命令已成功完成。

```
select * from sc
```

消息

```
消息 229，级别 14，状态 5，第 18 行
拒绝了对对象 'SC'（数据库 'SM'，架构 'dbo'）的 SELECT 权限。
```

把用户 U5 对 SC 表的 INSERT 权限收回。

```
revoke insert
on sc
from U5;
```

消息

命令已成功完成。

消息

```
消息 229，级别 14，状态 5，第 4 行
拒绝了对对象 'SC'（数据库 'SM'，架构 'dbo'）的 INSERT 权限。
```

熟练掌握以下存储过程并通过实验予以应用

sp_addlogin

```
EXEC sp_addlogin 'test', 'test', 'SM'
```

消息

命令已成功完成。

```
exec sp_helplogins
```

结果 消息

LoginName	SID	DefDBName	DefLangName	AUser	ARemote
dlm3	0x5452182CD01A7E48A5A930CB9FE1626D	SM	简体中文	yes	no
dlm4	0x00C7F9BC751275448 2CEEB8B96B4B4C3	SM	简体中文	yes	no
dlm5	0x5C3AE2678558B814C9BEC0BBD02A968	SM	简体中文	yes	no
NT AUTHORITY\NETWORK SERVICE	0x0101000000000005140000000	master	简体中文	yes	no
NT AUTHORITY\SYSTEM	0x0101000000000005120000000	master	简体中文	NO	no
NT SERVICE\MSSQLSERVER	0x0106000000000005500000000E20F4FE7B15874E48E19026...	master	简体中文	NO	no
NT SERVICE\SQLSERVERAGENT	0x0106000000000005500000000DCA88F14B79FD47A992A3D...	master	简体中文	NO	no
sa	0x01	master	简体中文	yes	no
test	0x0B63909CFD09224BB9F53EE32EDBCA64	SM	简体中文	NO	no

创建登录用户，可以指定用户名，密码，默认数据库，语言，SID

sp_droplogin

```
exec sp_droplogin 'test'
exec sp_helplogins
```

结果 消息

LoginName	SID	DefDBName	Defl
dlm2	0xAA709C8306266C47876B65A92B4E7E5B	SM	简体
dlm3	0x5452182CD01A7E48A5A930CB9FE1626D	SM	简体
dlm4	0x00C7F9BC7512754482CEE8B896B4B4C3	SM	简体
dlm5	0x5C3AE267855B814C9BEC0BBD02A968	SM	简体
NT AUTHORITY\NETWORK SERVICE	0x010100000000000514000000	master	简体
NT AUTHORITY\SYSTEM	0x010100000000000512000000	master	简体
NT SERVICE\MSSQLSERVER	0x0106000000000005500000000E20F4FE7B15874E48E19026...	master	简体
NT SERVICE\SQLSERVERAGENT	0x0106000000000005500000000DCA88F14B79FD47A992A3D...	master	简体
sa	0x01	master	简体

sp_addrole

```
exec sp_addrole 'testl'
```

添加新的数据库成员

```
exec sp_adduser 'test','SM'
exec sp_helplogins
```

消息

命令已成功完成。

sp_grantlogin 加入新的 WindowsNT 组

```
exec sp_defaultdb 'test','SM'
```

消息

命令已成功完成。

更换默认数据库

sp_addsrvrolemember

```
exec sp_addsrvrolemember 'test', 'sysadmin'
```

消息

命令已成功完成。

对于第二个参数的值有取值要求

sp_dropsrvrolemember 从固定服务器角色中删除角色

```
exec sp_srvrolepermission
exec SP_HELPSRVROLE
exec SP_HELPSRVROLEMEMBER
exec SP_HELPdbfixedrole
exec SP_HELPROLE
exec SP_HELPUSER
exec sp_helplogins
exec xp_logininfo
```

结果 消息

ServerRole	Permission
bulkadmin	Add member to bulkadmin
bulkadmin	BULK INSERT
dbcreator	Add member to dbcreator
dbcreator	ALTER DATABASE
dbcreator	CREATE DATABASE

sp_srvrolepermission：浏览固定服务器角色的权限。

SP_HELPSRVROLE：查看服务器角色。

SP_HELPSRVROLEMEMBER：查看服务器角色成员。

SP_HELPdbfixedrole：浏览固定的数据库角色。

SP_HELPROLEMEMBER：查看数据库角色成员。

SP_HELPROLE：查看数据库角色。

SP_HELPUSER：查看数据库用户信息。

*sp_helplogins：查看每个数据库中的登录及相关用户的信息

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

sp_password：添加或更改登录密码。

```
exec sp_password  '12345678','12345678','dlm5'
```

消息

命令已成功完成。

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

xp_logininfo 常用于孤立账户情况。

孤立帐户，就是某个数据库的帐户只有用户名而没有登录名，这样的用户在用户库的 sysusers 系统表中存在，而在 master 数据库的 syslogins 中

	却没有对应的记录。 孤立帐户的产生一般是一下两种： 1 .将备份的数据库在其它机器上还原； 2 .重装系统或 SQL SERVER 之后只还原了用户库
实验心得	对于存储过程有了更加深刻认识理解，了解 Sql Server2008 安全性与用户角色和权限的分配和回收管理。通过新建用户和合理分配用户权限可以增加系统的安全性。