## 实验四 安全性控制

**一、实验目的**

1. 熟练使用DBMS提供的功能组件来实现为数据库中添加用户和角色，以及对用户和角色进行权限管理。

2. 掌握不同的登录帐户及数据库用户对数据库对象的访问权限

**二、实验内容**

1.登录管理。

2.角色管理。

3.权限管理。

**三、实验学时**

4学时

**四、实验准备**

1.实验用微机以安装好DBMS。

2.已创建好包含实验数据的实验数据库。

3.了解SQL中GRANT、REVOKE语句的格式。

4.了解实验内容并书写实现权限管理的SQL语句。

**五、实验方法与步骤**

**第一阶段：**

1.启动DBMS服务器，视情况决定是否附加实验用数据库。

2.登录管理

（1）新建登录名。

(2)查看登录属性。

（3）删除登录名。

（4）开启sa账号。

3.用户管理

（1）新建数据库用户

（2）查看数据库用户属性

（3）删除数据库用户

4.角色管理

（1）服务器角色

设置服务器角色

查看登录的所属服务器角色

（2）数据库角色

①固定数据库角色

查看固定数据库角色db\_datawriter的属性，并将数据库用户u2添加到该角色中。

②用户定义数据库角色

创建用户定义数据库角色db\_user

5.权限管理

（1）使用SSMS管理权限

①管理SC表的权限。

属性-权限-添加-搜索-选择指定的用户或角色-设置权限

（2）使用T-SQL管理权限

①查看数据库用户属性

②删除数据库用户

授予用户U1对“学生-课程库” 中S表的查询和删除操作

**第二阶段：**

1．以Windows身份验证(管理员)登录，分别创建eshop和school数据库，其中eshop数据库中有三张表(members,products,orders)，school数据库有三张表(Student,Course,SC)，创建上述两个数据库及相应表的SQL语句，见共享文件的eshop.txt和school.txt。

2. 创建U1~U7共7个登录用户。

思考：以U1用户登录，观察该用户能访问哪些数据库，是否可以访问上述创建的eshop和school数据库？

3．若想用U1登录用户，访问school数据库该如何处理？

4. 把查询Student表的权限授给用户U1,然后以U1身份登录数据库，并验证U1是否可以查询Student表，能否修改、删除表中的数据?

授权、查询、修改、删除的SQL语句如何写？

5. 把对Student表和Course表的全部操作权限授予用户U2和U3,然后以U2身份登录数据库，并验证U2是否具有相应的权限；

授权、查询、修改、删除的SQL语句如何写？

6. 把对表SC的查询权限授予所有用户；

SQL语句如何写？

7. 把查询Student表和修改学生学号的权限授给用户U4, 然后以U4身份登录数据库，并验证U4是否具有相应的权限；

SQL语句如何写？

8. 把对表SC的INSERT权限授予U5用户，并允许将此权限再授予用户U6；

SQL语句如何写？

9. 回收用户U4修改学生姓名的权限；

SQL语句如何写？

10. 收回所有用户对表SC的查询权限；

SQL语句如何写？

11. 使用SQL语句创建角色ROLE1；

12. 为角色授权，使得角色ROLE1拥有对Student表的SELECT、UPDATE、INSERT权限；

SQL语句如何写？

13. 将用户U1,U3和U7添加到角色ROLE1中；

SQL语句如何写？

14. 对角色ROLE1的权限进行修改，增加对Student表的DELETE权限，并回收对Student表的INSERT权限；

SQL语句如何写？

15. 删除角色ROLE1；

SQL语句如何写？

**第三阶段：**

1.创建登录名并配置角色及用户

（1）使用sa登录SQLServer2008；

（2）创建数据库sa\_test，其中创建数据表dbo.saTable；

（3）创建登录名L1，具有dbcreator权限，影射用户名U1，映射数据库sa\_test，数据库角色为public；

（4）创建登录名L2，具有dbcreator权限，影射用户名U2，映射数据库sa\_test，数据库角色为public。

2.使用新登录名登录服务器并验证权限

（1）使用L1登录SQLServer2008，验证是否可以浏览表dbo.saTable；

（2）创建数据库L1\_test，用户名默认为dbo，模式默认为dbo；

（3）在L1\_test中创建数据表dbo.L1Table；

（4）使用L2登录SQLServer2008，验证是否可以浏览表dbo.saTable；

（5）创建数据库L2\_test，用户名默认为dbo，模式默认为dbo；

（6）在L2\_test中创建数据表dbo.L2Table。

3.sa用户对新建用户授权

（1）使用sa登录SQLServer2008；

（2）授权U1在dbo.saTable上的select权限；

（3）授权U2在dbo.saTable上的insert权限。

4.新建用户之间授权

（1）使用L1登录SQLServer2008，验证是否可以浏览表dbo.saTable中的数据，是否可以插入数据；

（2）授权U2在dbo.L1Table上的select权限和insert权限；

（3）授权U2在L1\_test中创建表的权限；

5.验证用户权限并对指定属性授权

（1）使用L2登录SQLServer2008，验证是否可以浏览表dbo.saTable中的数据，是否可以插入数据；

（2）验证是否可以浏览表dbo.L1Table中数据，是否可以插入数据；

（3）授权U1在dbo.L2Table上的select权限和修改指定列的权限。

6.收回权限并验证

（1）使用L1登录SQLServer2008，验证是否可以浏览dbo.L2Table中数据，是否可以修改指定的列；

（2）收回U2在dbo.L1Table上的insert权限；

7. 创建角色并授权

（1）使用L1登录SQLServer2008，在L1\_test中创建数据表dbo.L1Table2；

（2）创建数据库角色R1；

（3）将在dbo.L1Table表上的查询和插入权限授予角色R1，将dbo.L1Table2表上的查询权限和修改指定列权限授予角色R1；

（4）将用户添加到角色R1中；

（5）使用L2登录SQLServer2008，验证对L1\_test中数据表的操作权限。

8. 收回角色的权限

（1）使用L1登录SQLServer2008，收回角色R1在dbo.L1Table表上的插入权限；

（2）使用L2登录SQLServer2008，验证对L1\_test中数据表的操作权限。

**六、注意事项**

**七、思考题**