北京邮电大学软件学院

2014-2015学年第1学期实验报告

课程名称：数据库系统原理

实验名称：数据库的安全性

实验完成人：

姓名：

学号：

成绩：

指导老师：

日期：2015年6月15日

# 实验目的

在课程理论知识学习的基础上，使用DB2数据库管理系统工具对数据库的备份恢复和安全性操作有直接的体会。

# 实验内容

在了解DB2数据库管理系统中的数据库备份、恢复和数据库安全性机制的基础上，进行有关DB2数据库管理系统的备份和恢复操作。

# 实验环境

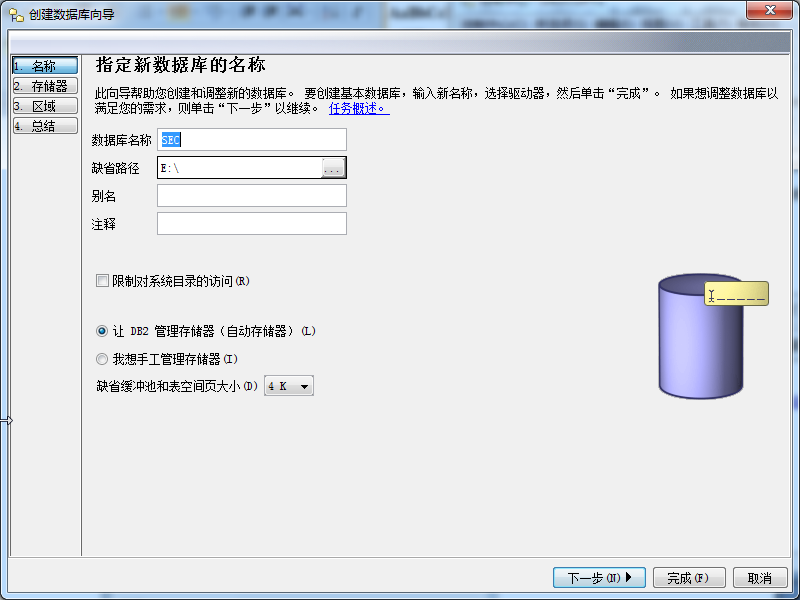
普通PC、Windows系列操作系统、IBM DB2 v8.1 数据库管理系统

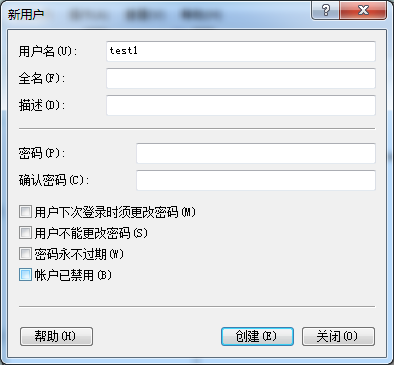
# 实验步骤

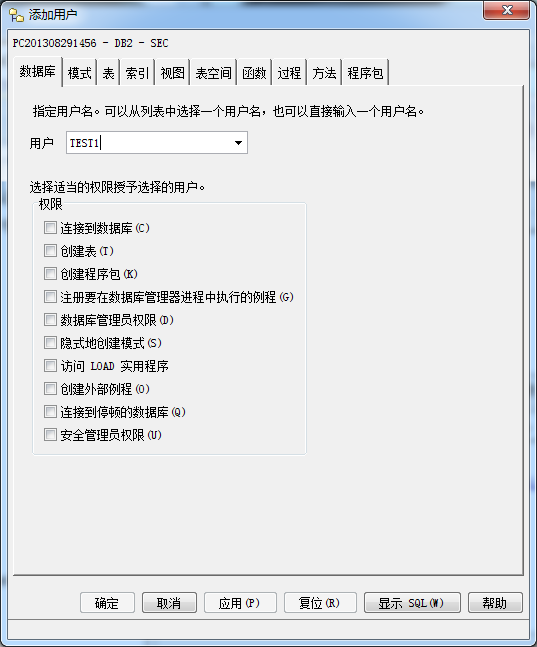
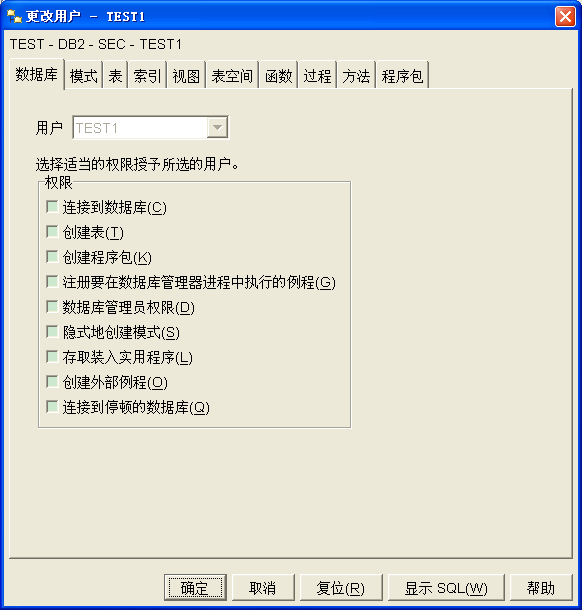
为了完成本实验，应该先进行如下准备操作：

作为 Administrators 组的成员登录到 Windows 计算机，我们将以用户user 登录；

安装了 DB2 9（已完成）；

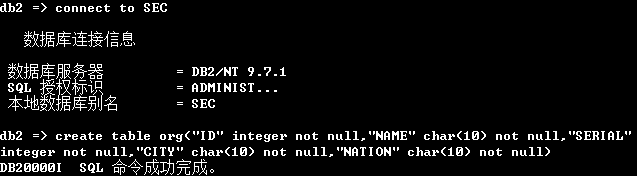
在控制中心创建数据库SEC；

在计算机管理中创建第二个用户test1。注意，test1 用户不是 Administrators 组的成员；在控制中心sec数据库的“用户和组对象”目录中“添加”用户并赋予权限，见下图。



在计算机管理中创建一个新的组db2grp1，将用户test1添加到组中；在控制中心“添加”组并赋予权限，图略。

在数据库SEC中创建表org如下：

CREATE TABLE ORG ( "ID" INTEGER NOT NULL , "NAME" CHAR(10) NOT NULL , "SERIAL" INTEGER NOT NULL , "CITY" CHAR(10) NOT NULL , "NATION" CHAR(10) NOT NULL ) 

下面开始实验步骤：

1. 以拥有 Administrator 权限的用户登录 Windows操作系统
2. 打开两个 DB2 命令窗口。确保将 db2instance 变量设置为 DB2（默认）。

**使用该命令修改变量值：db2 set db2instance=db2inst1**

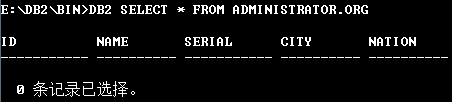
在第一个窗口中执行以下命：db2 connect to sample

在第二个窗口中执行以下命令： db2 connect to sample user test1 using password 

注意，第一个窗口中的命令是由一个拥有 SYSADM 权限的用户发出的。第二个窗口中的命令是由用户 test1 发出的，该用户对示例数据库没有特殊的权限或特权。注意，与示例数据库中的表相关联的模式名是发出 db2sampl 命令的用户的名称。在这些示例中，这个用户是 USER。

1. 在第二个窗口中执行以下命令： db2 select \* from user.org

将等到以下响应： SQL0551N "TEST1" does not have the privilege to perform operation "SELECT" on object "USER.ORG". 

1. 在第一个窗口中执行以下命令： db2 grant select on table user.org to user test1 
2. 重新执行步骤5的命令，命令就会成功。
3. 在第二个窗口中发出一个更复杂的命令： db2 insert into user.org values (100, 'Tutorial', 1, 'Eastern', 'Toronto')

将等到以下响应：SQL0551N "TEST1" does not have the privilege to perform operation "INSERT" on object "USER.ORG"

1. 在第一个窗口中执行以下命令：db2 grant insert on table user.org to group db2grp1 
2. 重新执行步骤8的命令，命令就会成功。

注意 test1 是 db2grp1 组的成员。

1. 在第二个窗口中执行以下命令：db2 drop table user.emp\_photo

将等到以下响应：SQL0551N "TEST1" does not have the privilege to perform operation "DROP TABLE" on object "USER.EMP\_PHOTO".

1. 在第一个窗口中执行以下命令： db2 grant dropin on schema user to all
2. 重新执行步骤11的命令，命令就会成功。
3. 完成了操作还需要撤消刚才授予的特权。

在第一个窗口中发出以下命令：

db2 revoke select on table user.org from user test1

db2 revoke insert on table user.org from group db2grp1

db2 revoke dropin on schema user from all

注意，从组中撤消特权不一定会从这个组的所有成员撤消它。例如，以下命令可以用来从 db2grp1 撤消对 user.org 表的所有特权（CONTROL 除外）： db2 revoke all on table user.org from group db2grp1;但是，test1 用户（他是 db2grp1 的成员）仍然拥有对这个表的选择特权，因为他或她是被直接授予这个特权的。