## 1.1实验目的、内容与要求

* + 1. 实验目的

通过本实验，掌握SQL Server安全管理中的登录、数据库服务器角色、用户、数据库角色、特定对象权限等基本概念与安全机制，掌握数据库服务器角色授权、数据库角色授权和特定对象授权的方法与各种方法的差异。

学会使用SQL Server实现我们的对SQL Server数据库的权限分配和安全管理的具体操作

* + 1. 实验内容

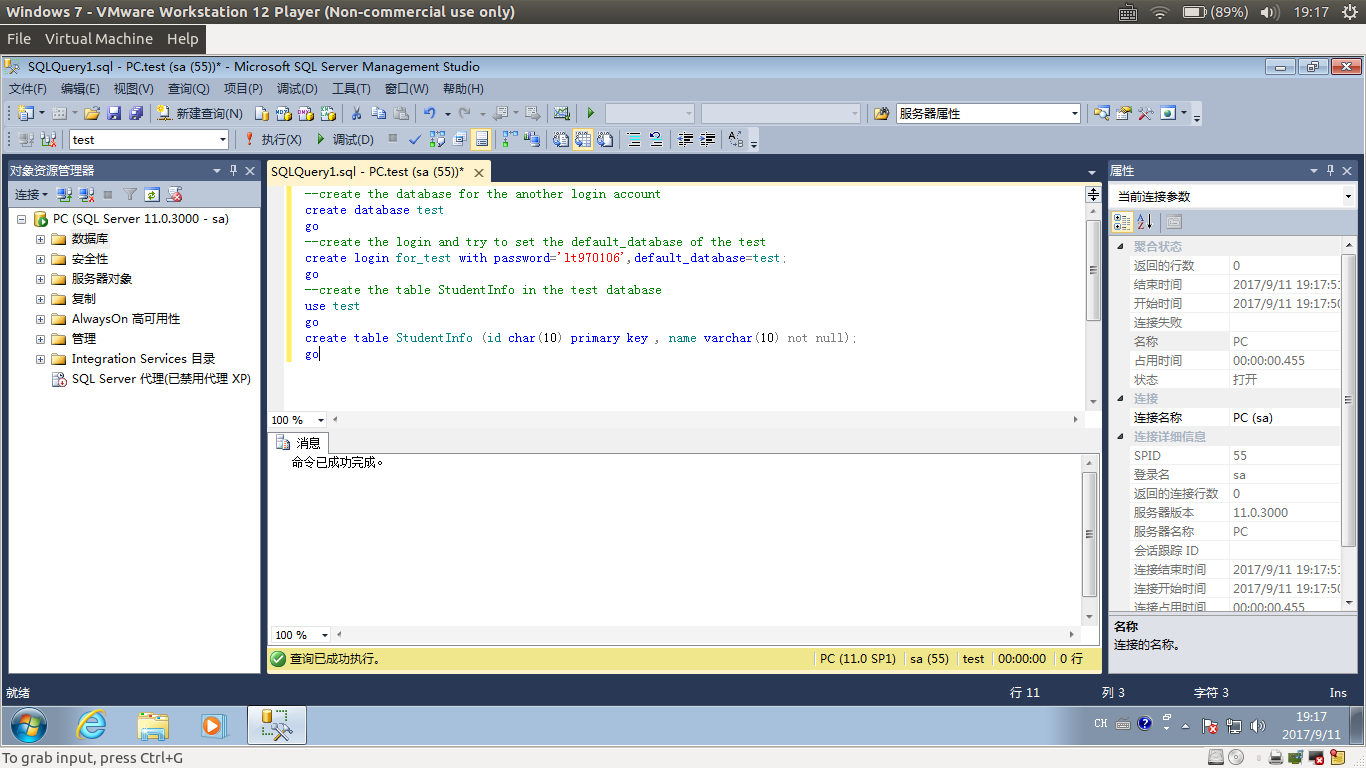
实验一 SQL Server的基本安全管理

使用管理员登录连接到数据库服务器创建一个SQL Server登录并使用它完成如下的操作：

具体的实验内容：

CREATE TABLE StudentInfo (id char(10) primary key,

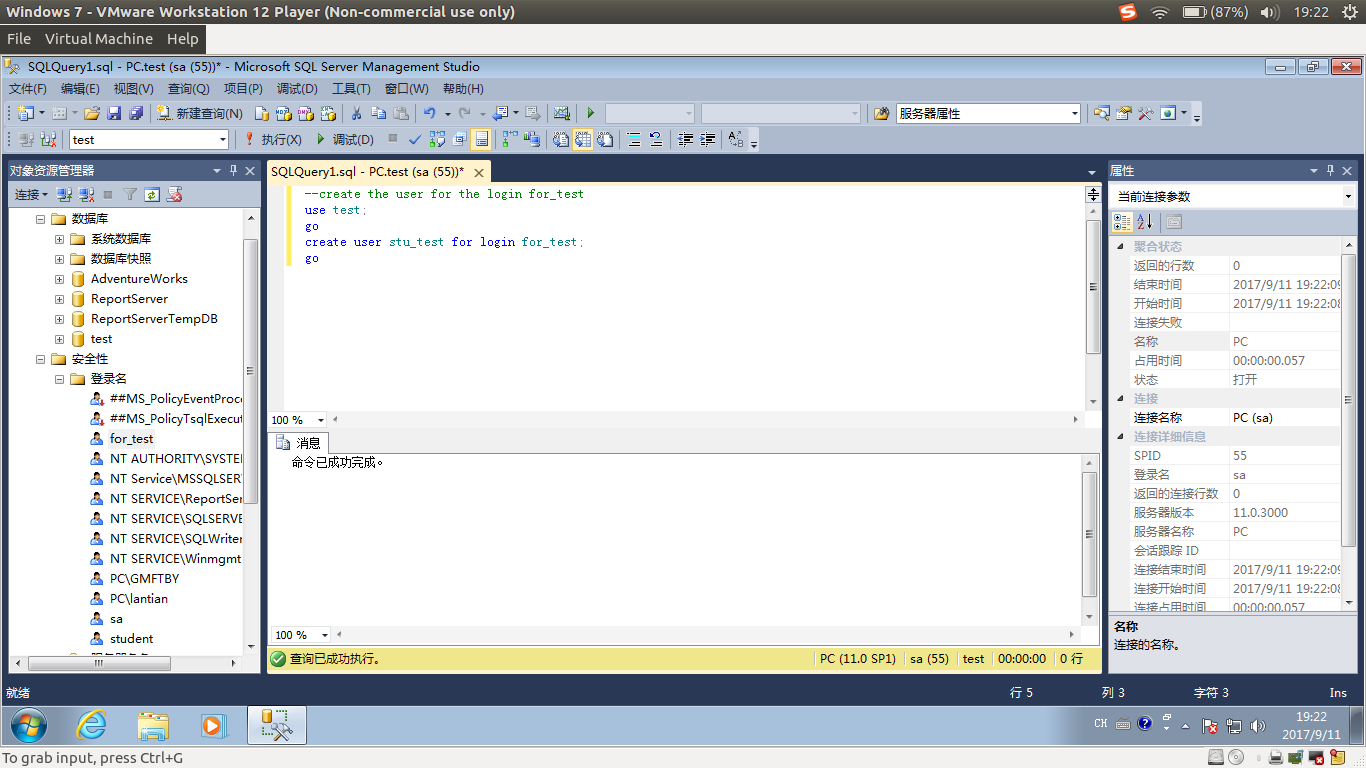
name varchar(10) not null);

(1)创建一个登录并将创建的数据库设置为该登录的默认数据库。 

如上我们创建了数据库test,并且创建了一个登录for\_test,并且其的默认数据库设定

成我们刚刚建立的数据库test，利用sa用户在数据库test下创建表dbo.StudentInfo

(2)设置登录在默认数据库中的用户映射。

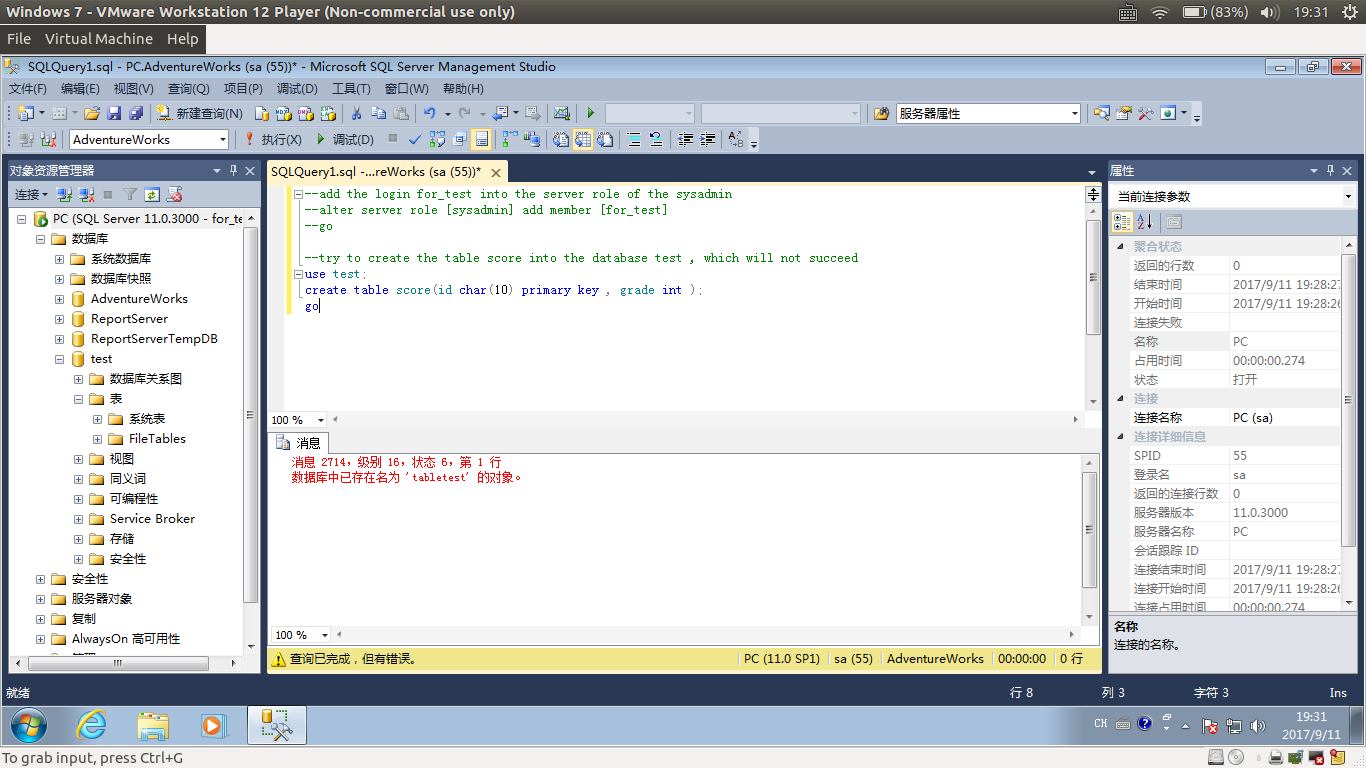


如上图所示，我们在数据库test中利用sa账户的权限为我们的登录for\_test创建一

个针对的用户映射stu\_user，这样子我们就可以对for\_test用户进行登录和使用了

(3)尝试将登录加入到两个不同的数据库服务器角色中对默认数据库进行操作（如创建表Score，查询表StudentInfo等）。注意每次只使用一个数据库服务器角色来验证授权。

１.1修改前的必要检查

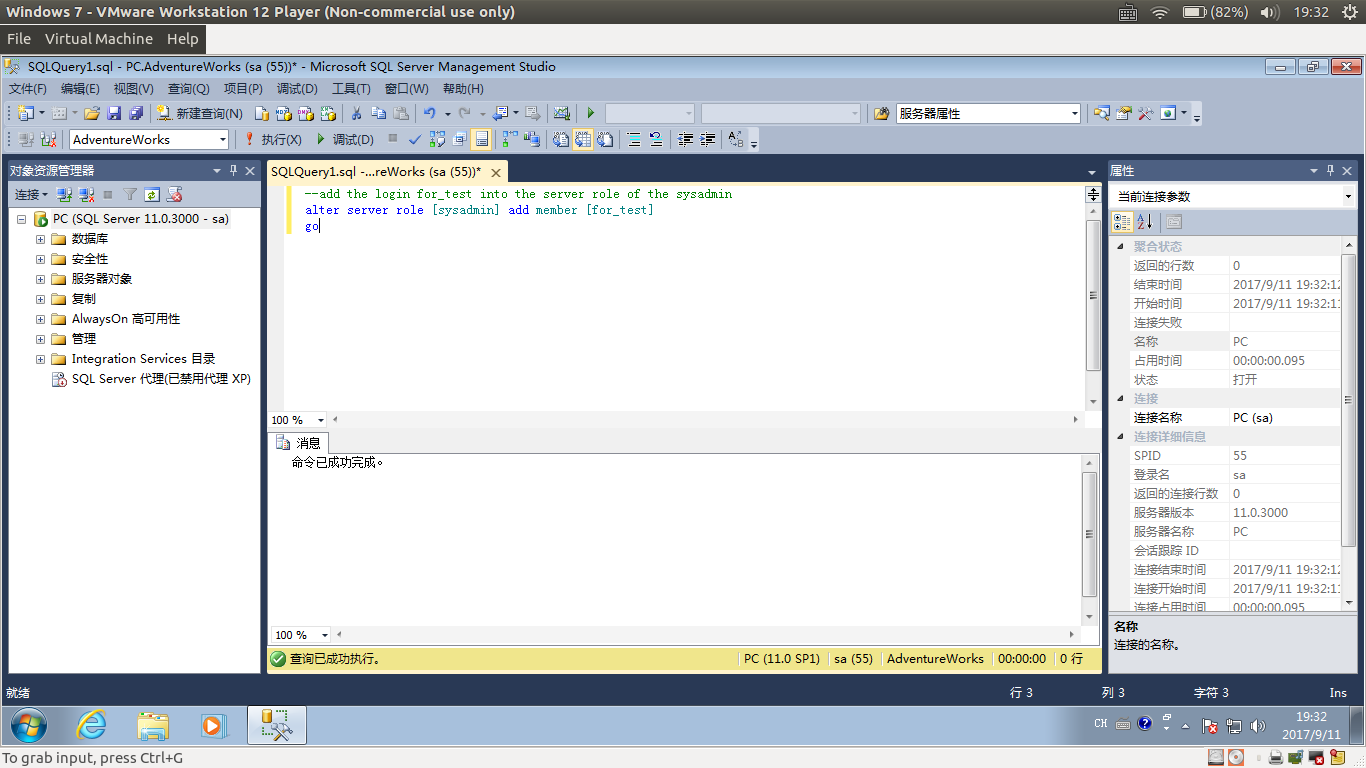


我们可以清楚的发现，在左侧的对象资源管理器中，我们的for\_test账户虽然针对的

是数据库test，但是我们任然查看不了我们在test数据库中已经创建的表

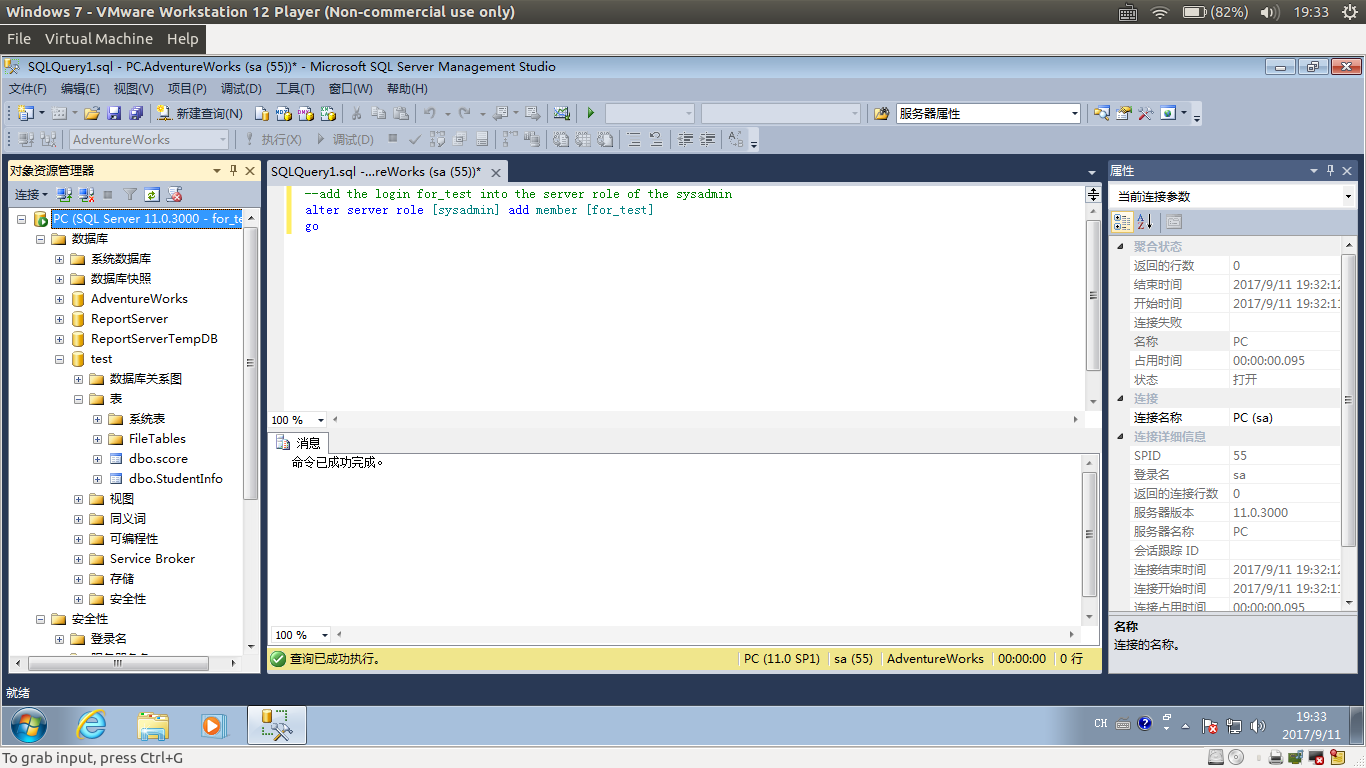
dbo.StudentInfo,原因在于没有相应的数据库的权限，下面即将加入权限

2.1 为for\_test账户加入数据库服务器角色权限，拥有了对所有的数据库和所有的数据对象的操作权限，自然可以查看到我们的所有的数据对象(包括dbo.StudentInfo)



在下方已经显示我们的语句执行成功，当前的用户for\_test用户拥有了和sa一样权限

3.1 检验结果



显然，我们左边的对象资源管理器中已经可以查看到所有的在test数据库下的所有的

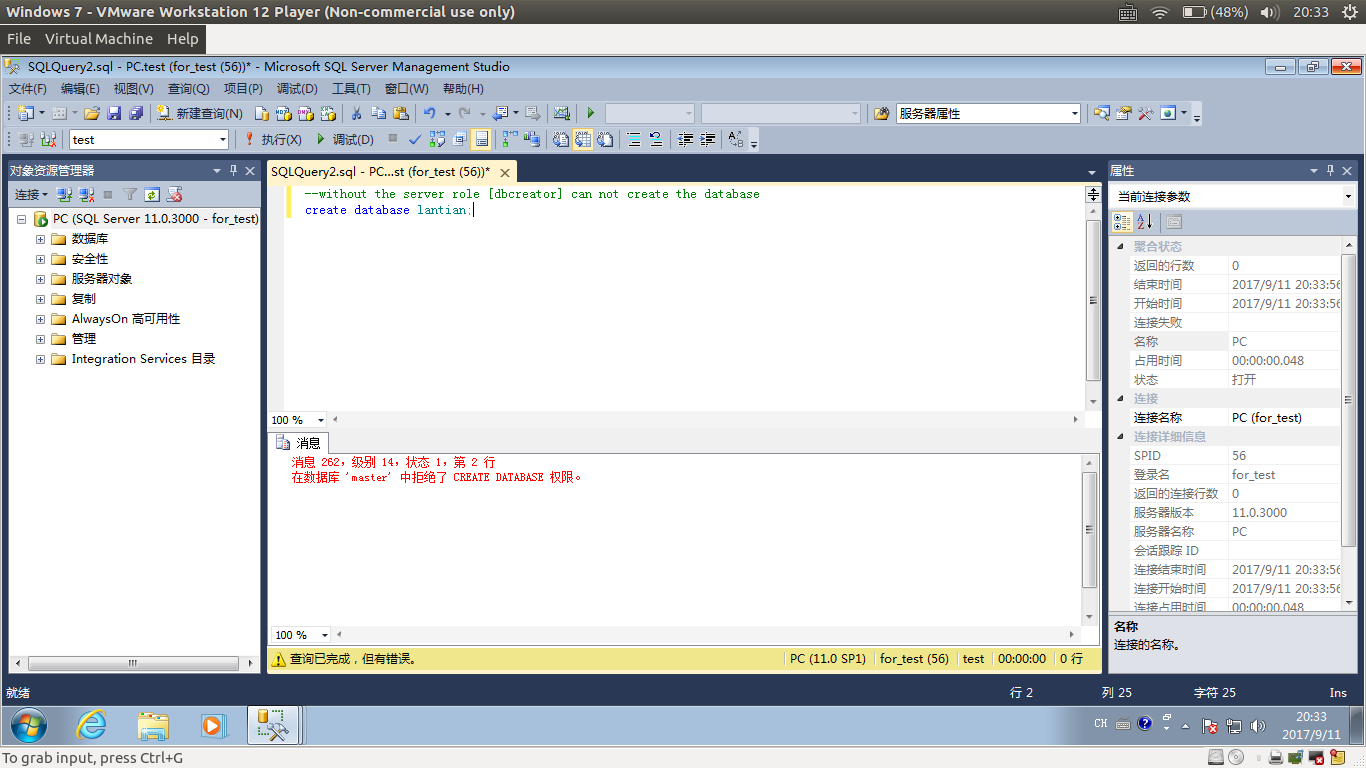
数据对象，包括之前用sa创建的表dbo.StudentInfo,表明我们的当前的账户for\_test

已经具有了对应的sysadmin服务器角色的权限

在进行下一个实验之前，我们之间已经进行了语句删除了刚才的for\_test登录的

sysadmin服务器角色的权限，保证下面的实验的正确性

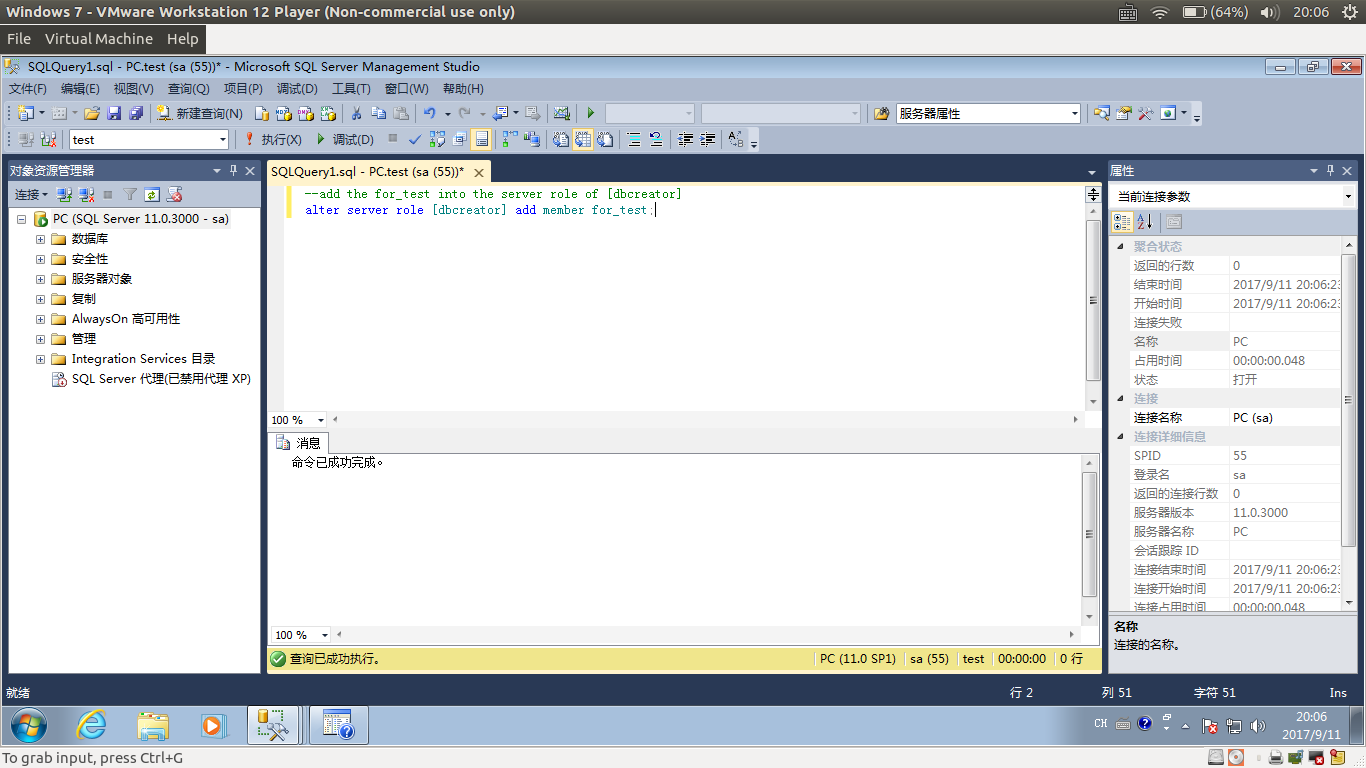
1.2 对dbcreator服务器角色的修改前检查



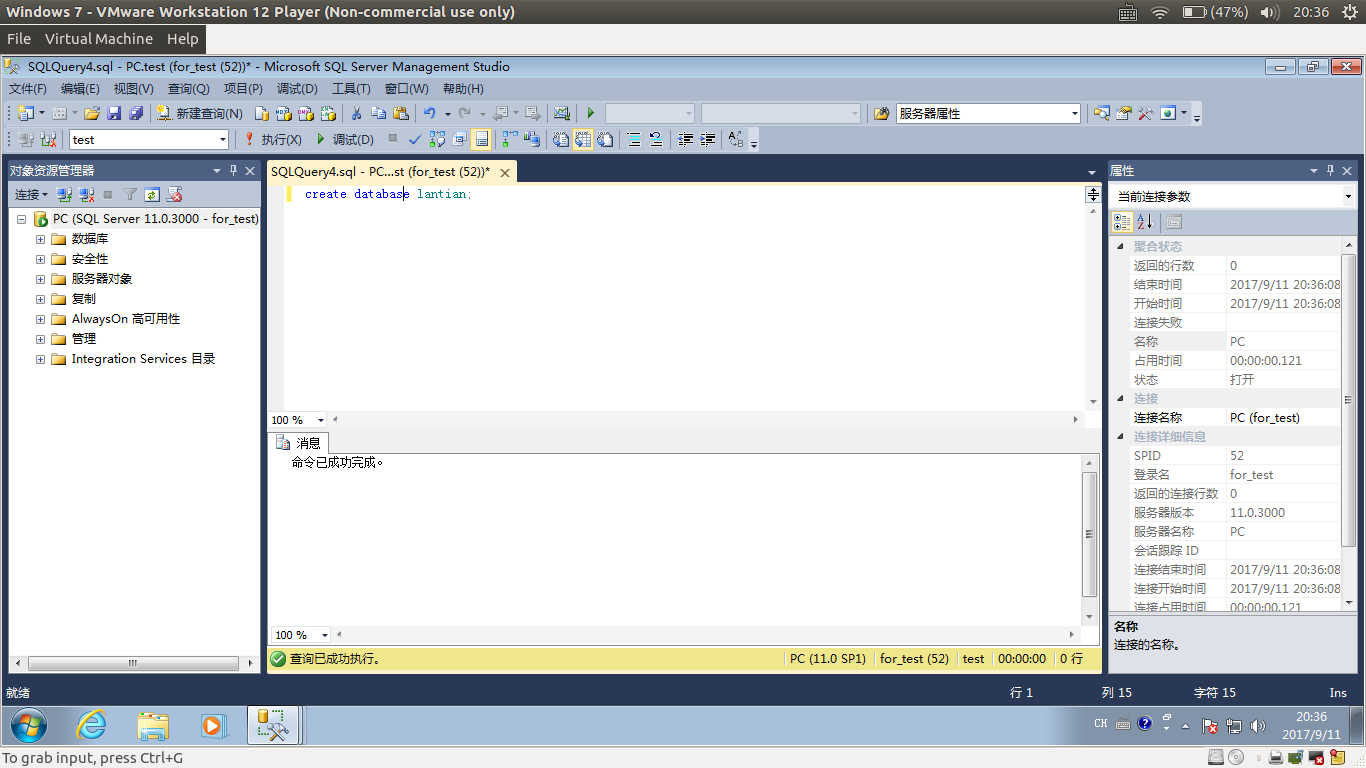
我们会发现，在没有为登录for\_test增加dbcreator服务器角色权限之前，我们是没

有办法创建数据库lantian的

2.2 利用sa用户为for\_test登录增加dbcreator服务器权限，dbcreator服务器角色可以让用户执行CREATE DATABASE等语句，创建和修改数据库，现在的登录for\_test已经具备了创建数据库的权限



3.2 检查结果



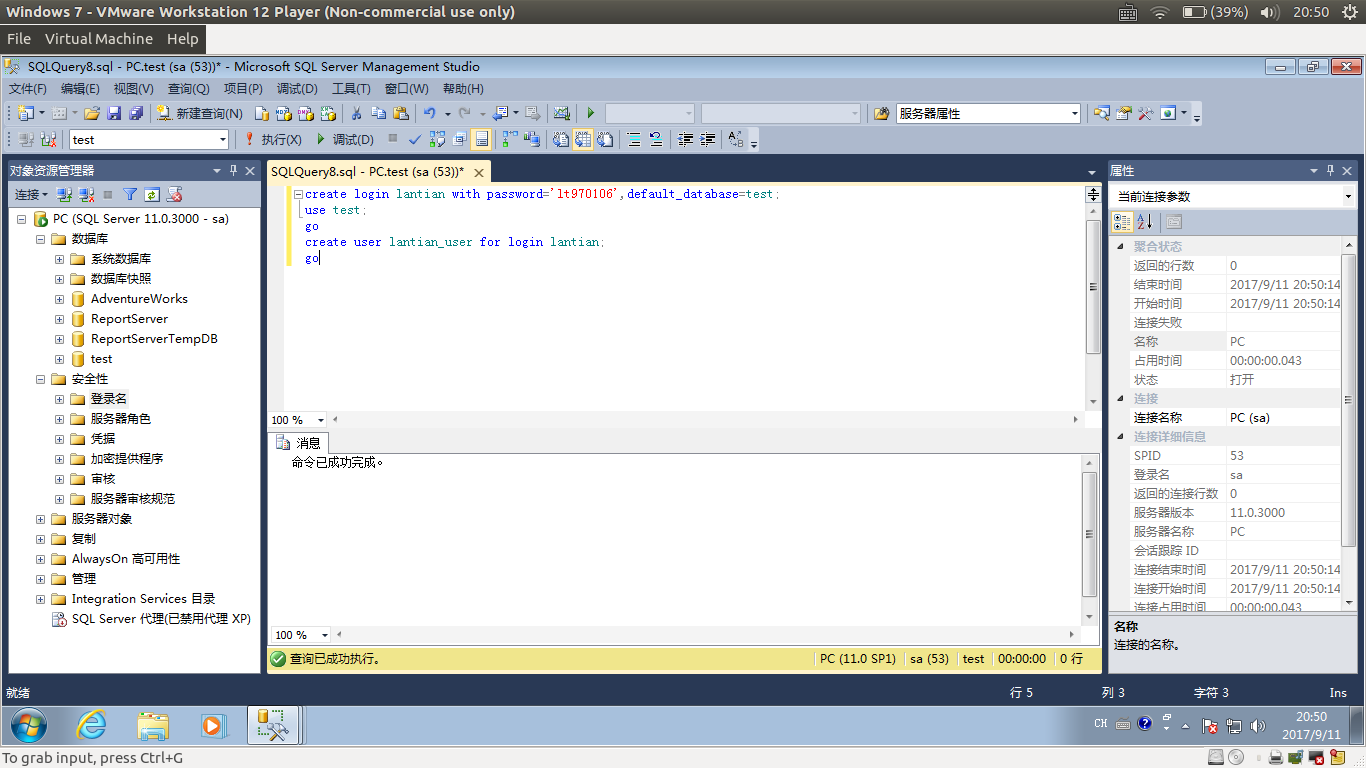
如图所示，上面的语句create database lantian 执行成功，说明我们的for\_test

登录已经可以执行创建数据库的操作了，说明我们的dbcreator的服务器权限已经成

功的授权给了我们的用户for\_test

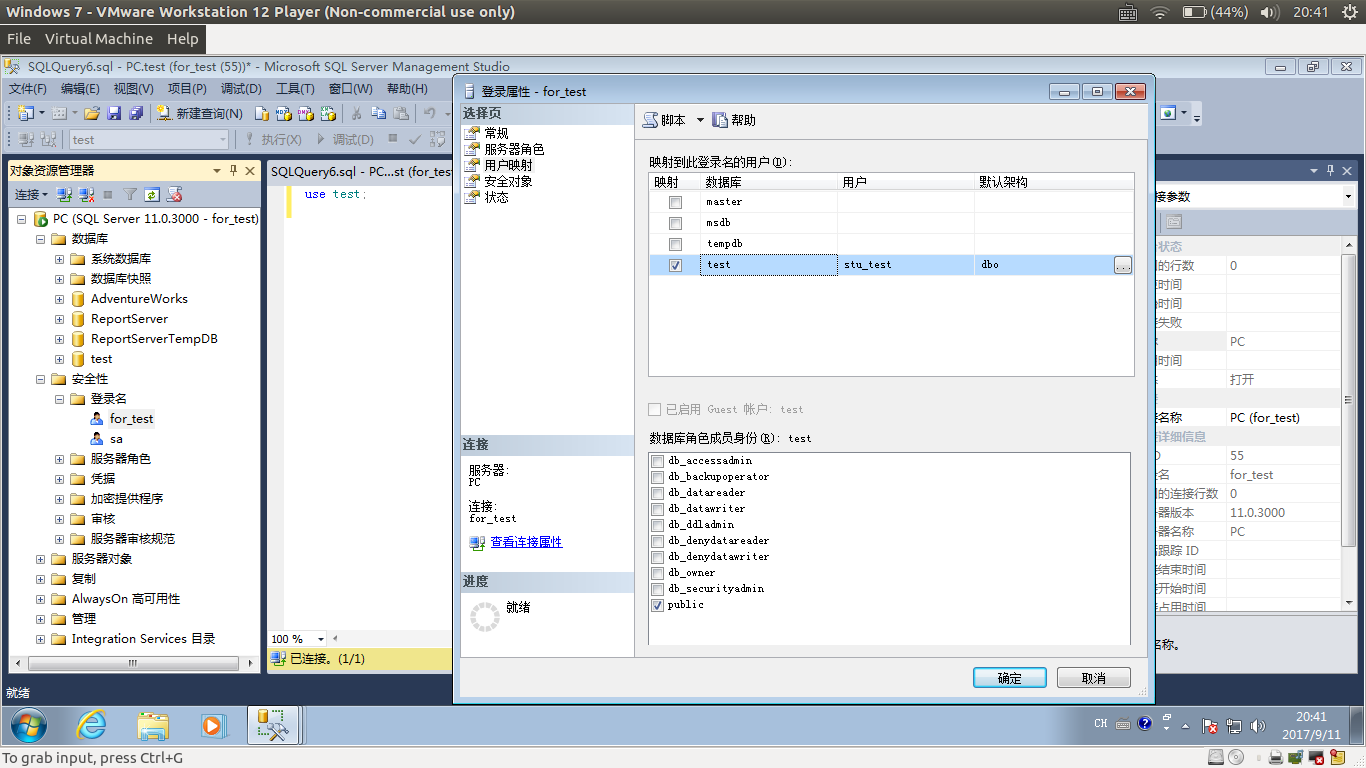
(4)尝试使用两个不同的数据库角色进行相应的授权操作。

1.1 首先，我们为了之后的测试方便加入新的登录lantian,并利用sa为其增加用户映射lantian\_user，新登录lantian对数据库没有的db\_datawriter权限，无法对数据执行写操作

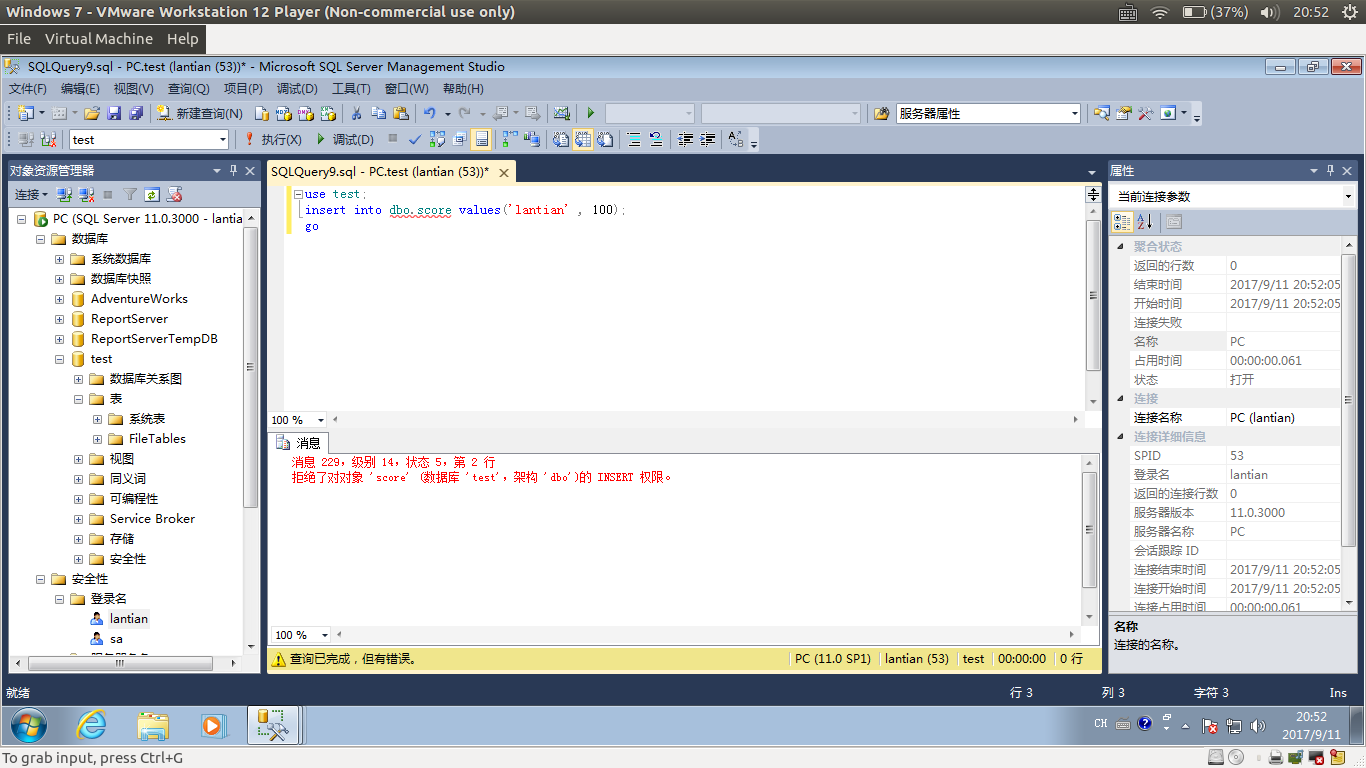


如下图所示，我们的登录lantian没有对数据库的db\_datawriter数据库角色，所以

我们是没有办法对数据库进行insert等写入操作的

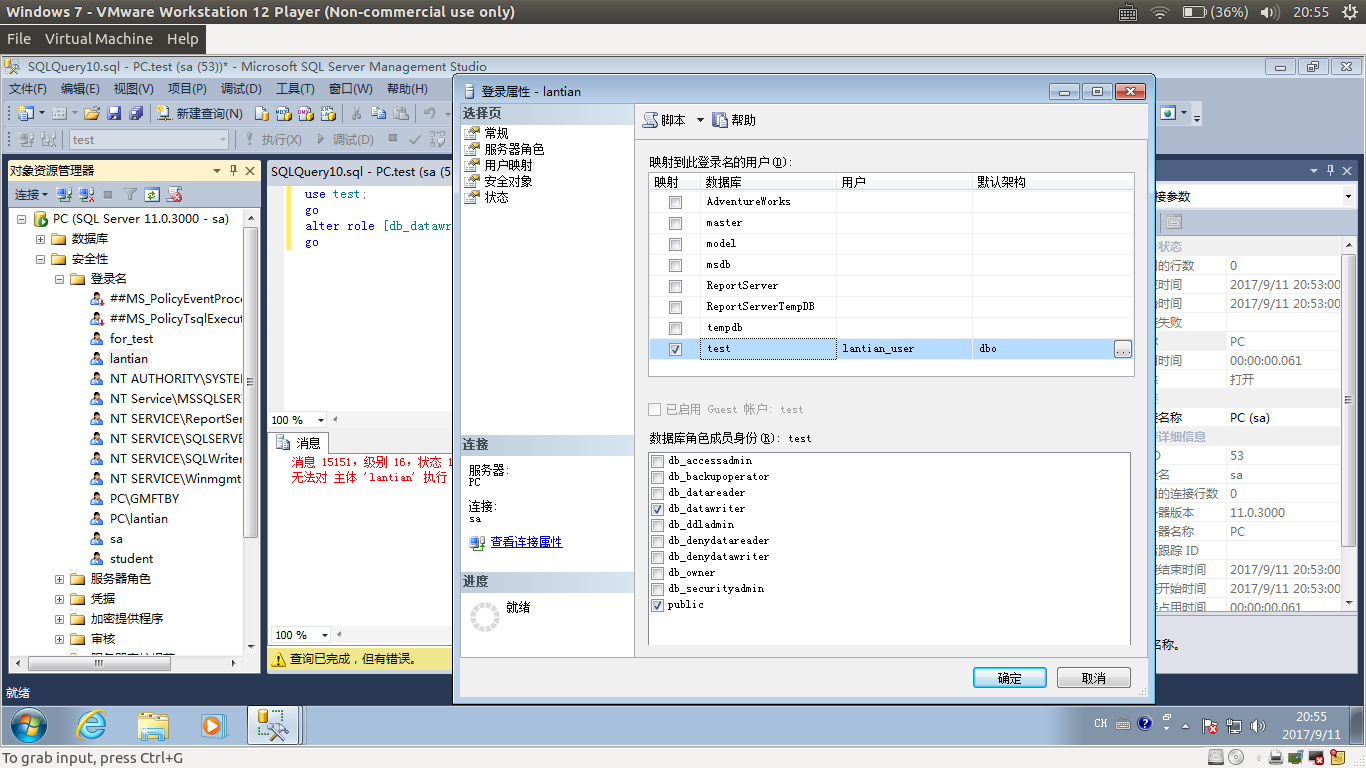


缺少数据库快角色权限db\_datawriter,写入操作失败

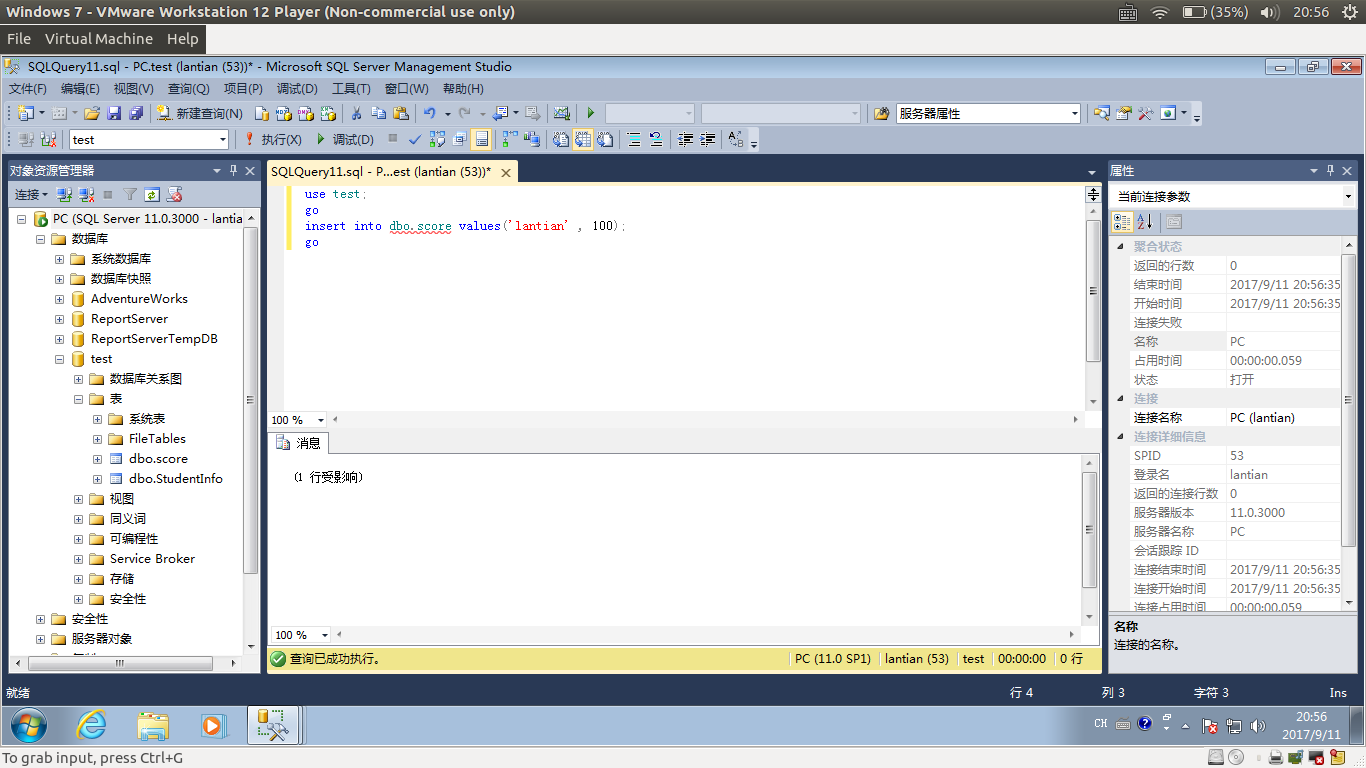


2.1 利用sa用户为登录lantian增加对数据库test的db\_datawriter的写权限

增加了db\_datawriter权限之后，我们可以对SQL Server的数据库test执行包括insert,delete,update在内的写入操作



3.1 写入成功



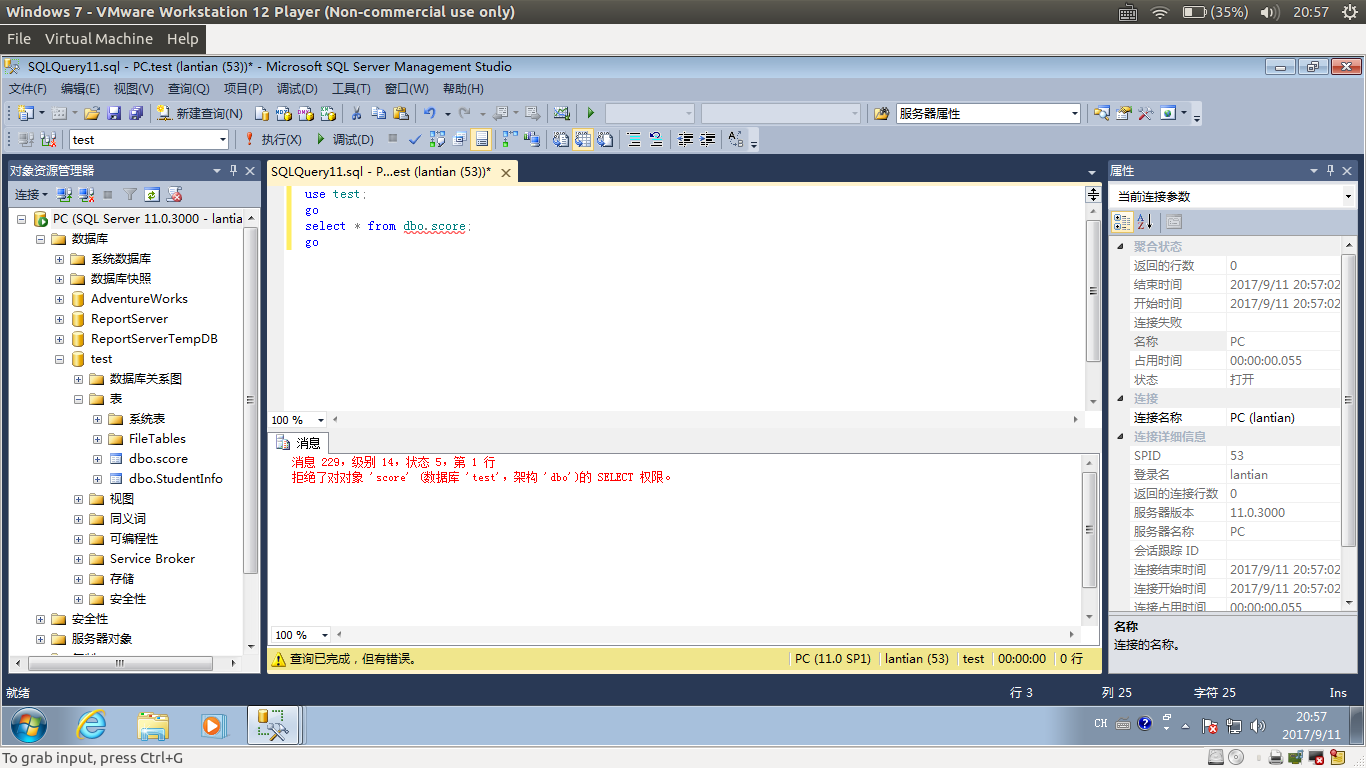
加入了db\_datawriter之后我们可以对数据库进行插入操作，如上图所示，我们的写

入操作insert成功的影响了数据库的test的dbo.score表的内容

对读权限的查看结果

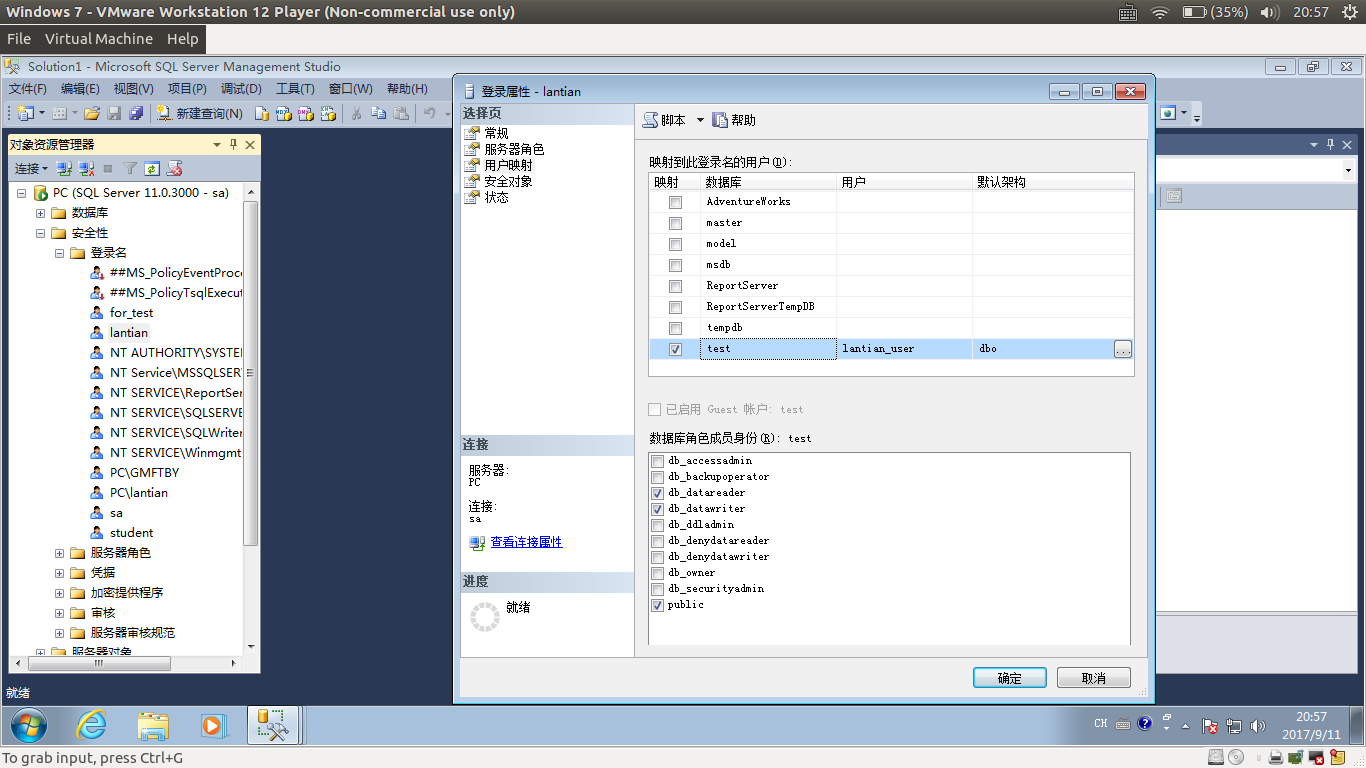
1.2 新登录对数据库test没有读权限

我们在数据库的test的读权限db\_datareader确实导致我们的select代码的执行失败

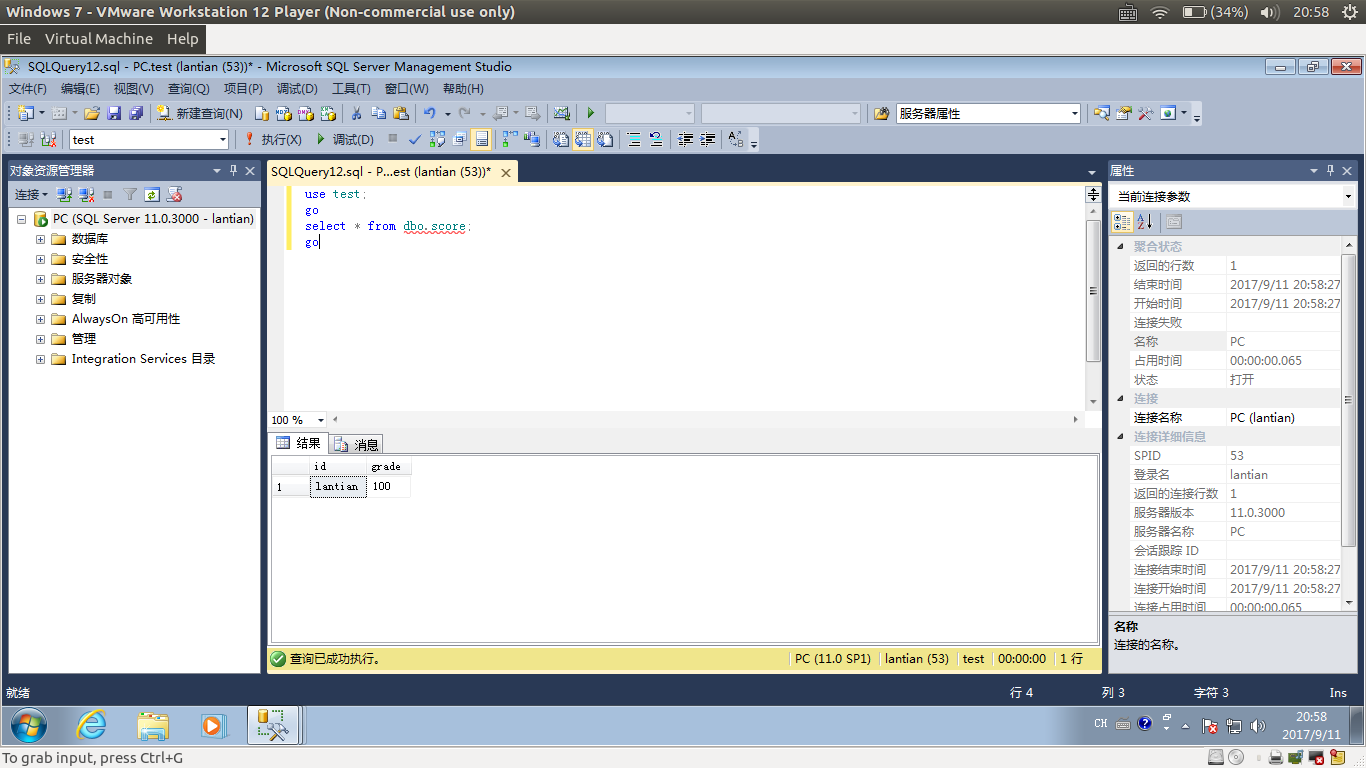


2.2利用sa用户添加读权限

如下图所示，我们增加了我们的test数据库的db\_datareader的权限



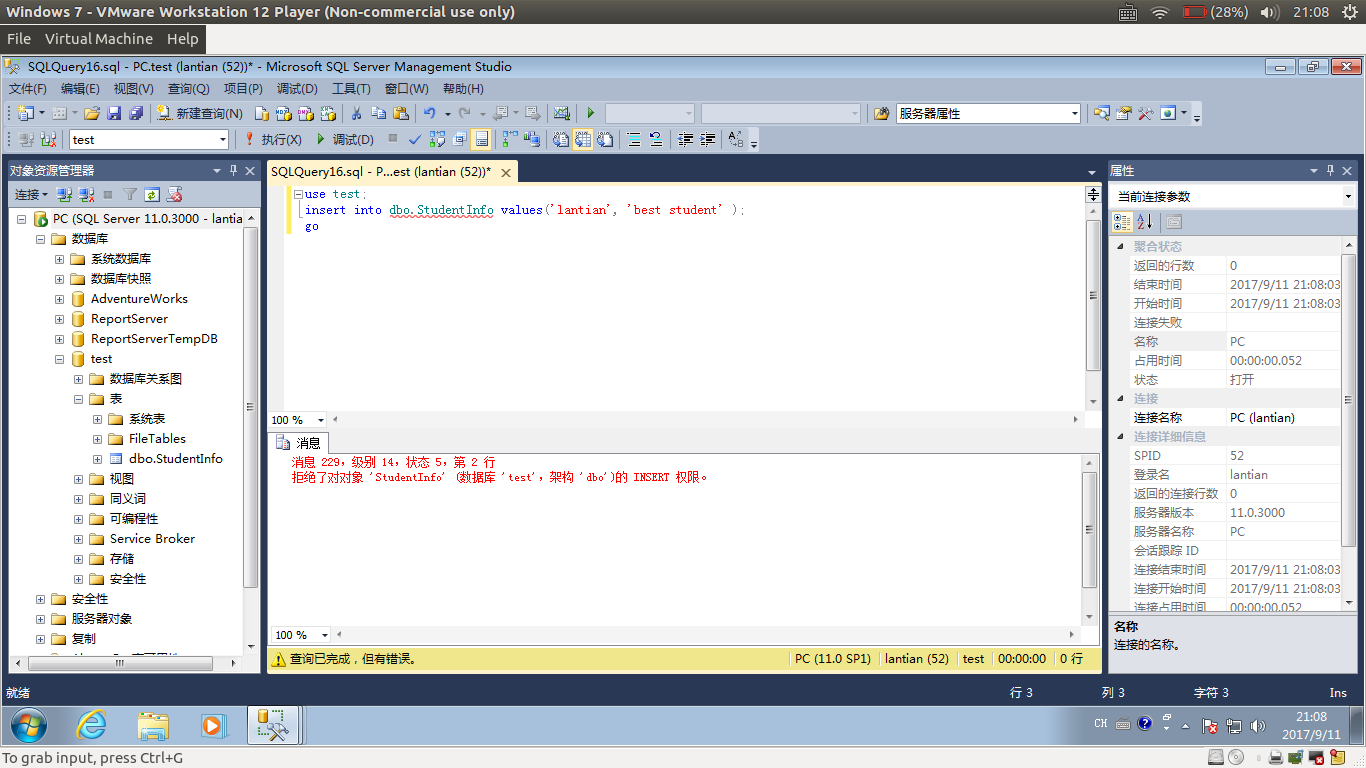
2.3 最后对我们的查询结果进行实验，执行语句查询我们的数据库test中的表StudentInfo中的数据，结果显示可以查询，语句执行成功



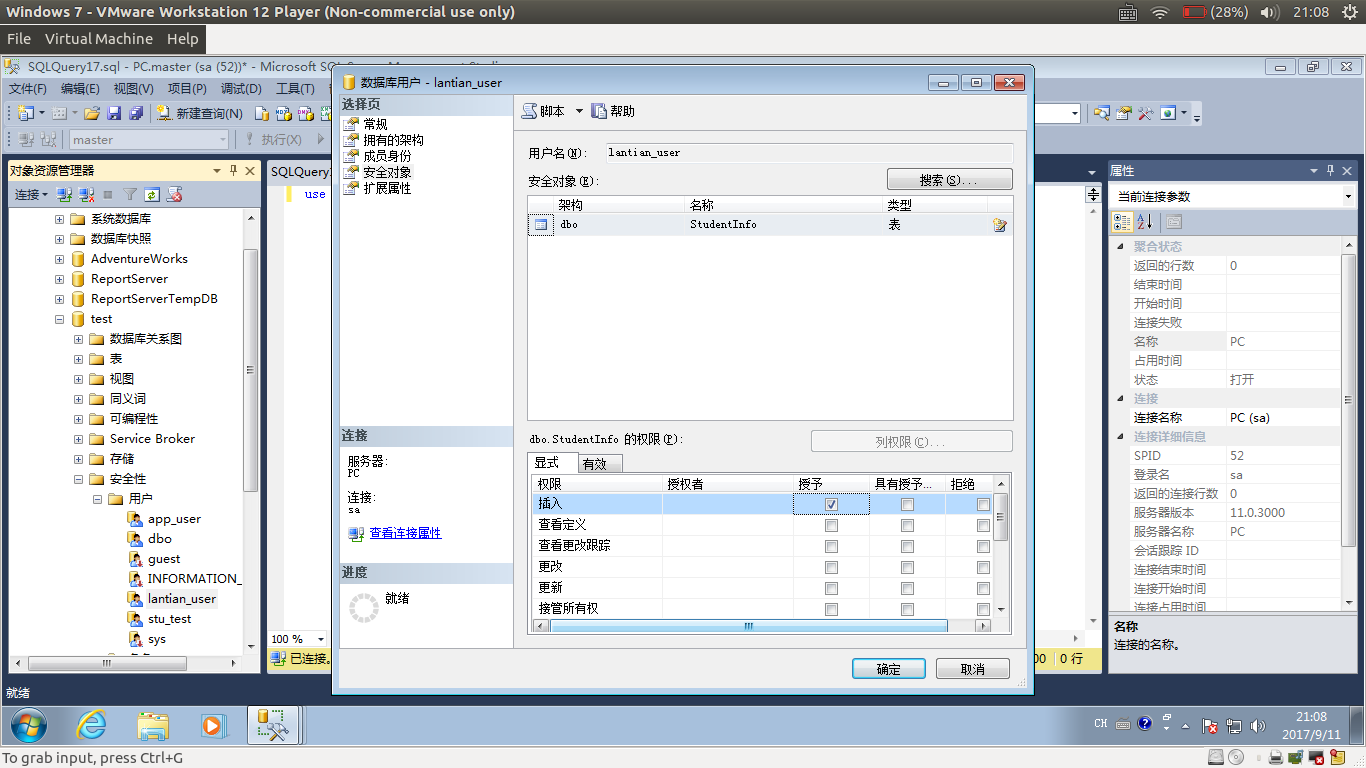
为了下面的实验的正确性，我已经提前讲为lantian登录的数据库的权限都进行可删除，以便下面的具体的操作

(5)只使用特定对象授权，完成相应的操作以验证授权的成功和没有授权时发生的错误。

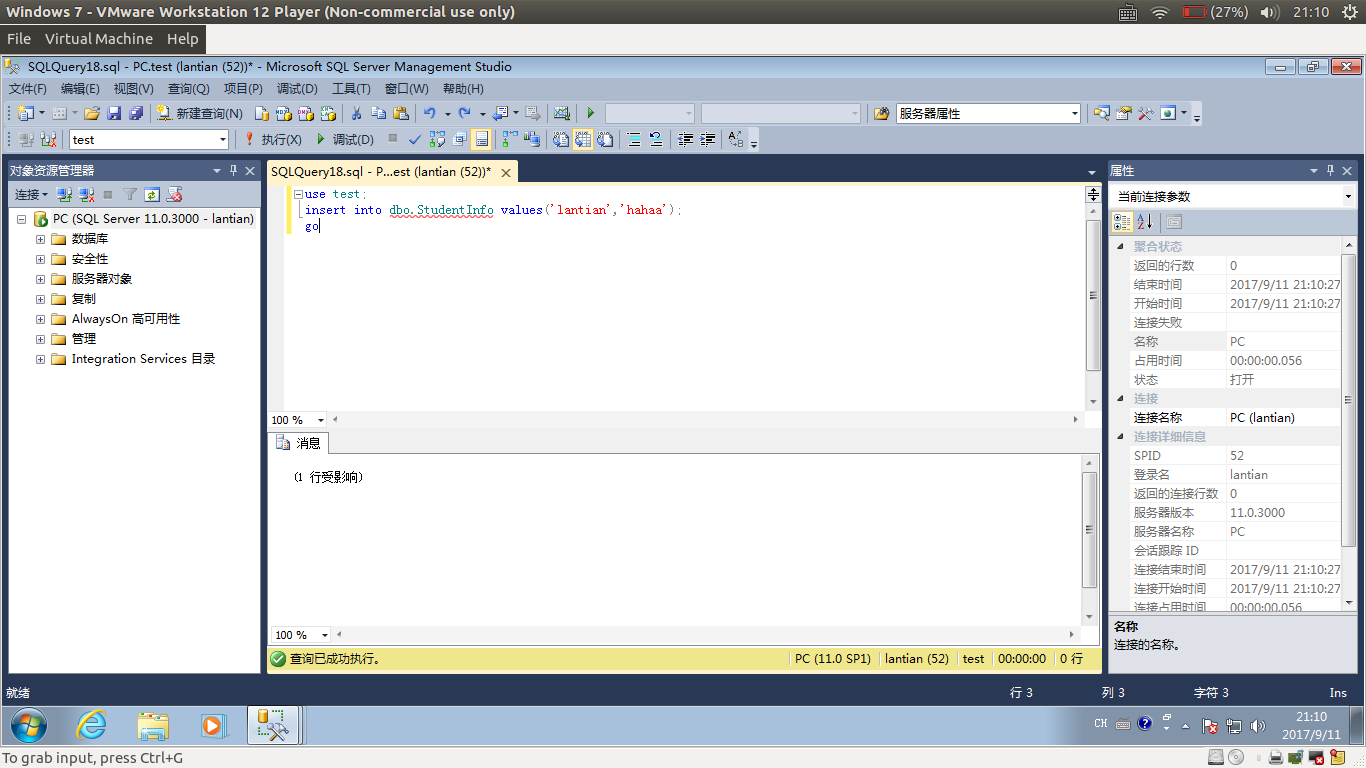
1.1 因为没有了针对数据库test的中的特定的数据对象dbo.StudentInfo表的写权限，所以我们的针对StudentInfo表的insert操作是会失败的



2.1在对象资源管理器中，我们打开数据库的安全选项，对特定对象插入我们的对特定对象StudentInfo表的写权限(插入),如下图所示

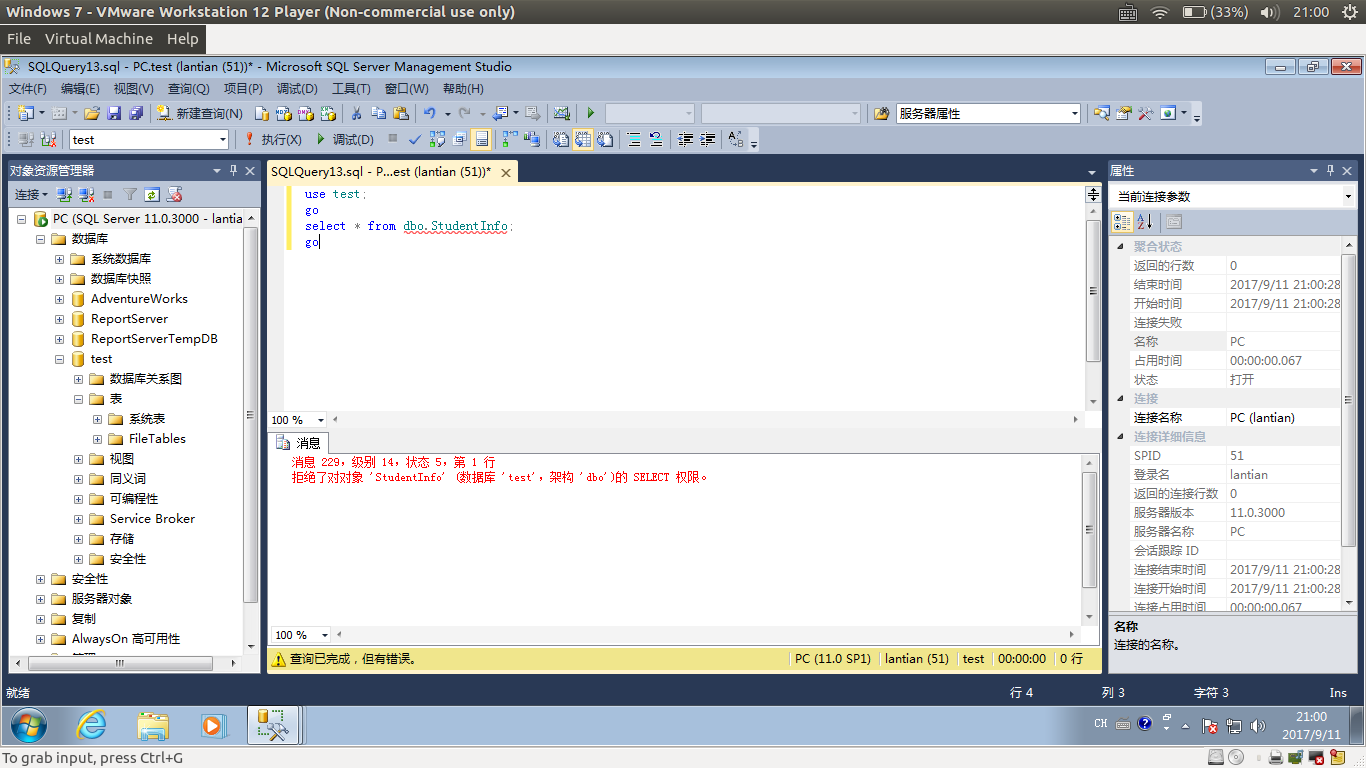


3.1 查看写入的最终结果



可以明确的看出来，在我们执行完了对lantian登陆的test数据库的特定数据对象的 写操作的权限，我们的写操作成功，运行结果显示1行受影响

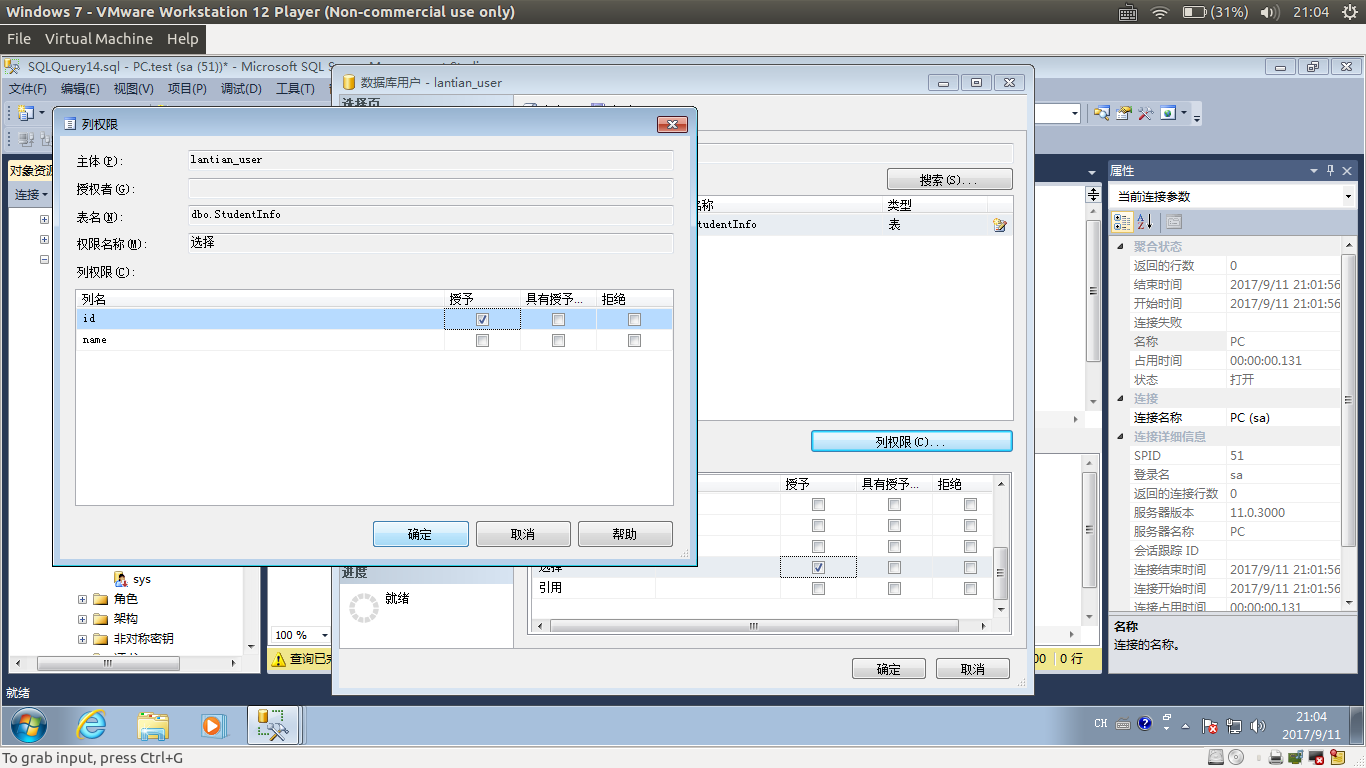
1.2 同理，我们对test数据库中的特别的数据对象dbo.StudentInfo缺少对应的读的权限，所以不论是对特定列还是对整个数据表StudentInfo的读操作都将会是失败的



如上图所示，我们的select操作因为权限的限制导致运行失败，提示我们缺少对应的

test数据库的StudentInfo表的读权限

2.2 在对象资源管理器中，我们对dbo.StudentInfo数据表的特定列id列增加读权限，这样我们就可以对具体的数据StudentInfo的id列进行读操作



3.2 结果显示我们的读操作成功，虽然数据库test中的dbo.StudentInfo数据表中没有数据，但是我们的语句运行结果是成功的，显示出来我们的读操作是空表

