

第 16 章

用户账户及角色权限的管理



本章内容提要

安全性对于任何一个数据库管理系统来说都非常重要。为此，SQL Server 为用户提供了安全机制，通过对用户账户以及角色的管理，可以提高数据的安全性。本章介绍用户账户及角色权限的管理，主要内容包括与数据库安全相关的对象、登录账号的管理、用户的管理、角色的管理以及权限的管理等。

16.1 与数据库安全相关的对象

在 SQL Server 中，与数据库安全相关的对象主要有用户、角色、权限等，只有了解了这些对象的作用，才能灵活地设置和使用这些对象，从而提高数据库的安全性。



微视频

16.1.1 数据库用户

数据库用户就是指能够使用数据库的用户，在 SQL Server 中，可以为不同的数据库设置不同的用户，从而提高数据库访问的安全性。

在 SQL Server 数据库中有两个比较特殊的用户，一个就是 DBO 用户，它是数据库的创建者，每个数据库只有一个数据库所有者，DBO 有数据库中的所有特权，可以提供给其他用户访问权限；另一个是 guest 用户，该用户最大的特点就是可以被禁用。

16.1.2 用户权限

通过给用户设置权限，使每个数据库用户有不同的访问权限，如：让用户只能查询数据库中的信息而不能更新数据库的信息。在 SQL Server 数据库中，用户权限主要分为系统权限与对象权限两类。系统权限是指在数据库基本执行某些操作的权限，或针对某一类对象进行操作的权限；对象权限主要是针对数据库对象执行某些操作的权限，如对表的增删（删除数据）查改等。

16.1.3 认识角色

角色相当于 Windows 操作系统中的用户组，可以集中管理数据库或服务器的权限。假如直接给每一个用户赋予权限，这将是一个巨大又麻烦的工作，同时也不方便 DBA 进行管理，于是就引用了角色这个概念。使用角色具有以下优点：

(1) 权限管理更方便。将角色赋予多个用户，实现不同用户相同的授权。如果要修改这些用户的权限，只需修改角色即可。

(2) 角色的权限可以激活和关闭。使得 DBA 可以方便地选择是否赋予用户某个角色。

(3) 提高性能，使用角色减少了数据字典中授权记录的数量，通过关闭角色使得在语句执行过程中减少了权限的确认。

用户和角色是不同的，用户是数据库的使用者，角色是权限的授予对象，给用户授予角色，相当于给用户授予一组权限。数据库中的角色可以授予多个用户，一个用户也可以被授予多个角色。

16.1.4 登录账户

登录账户是用来访问 SQL Server 数据库系统使用的，它不同于数据库用户，是用来访问某个特定数据库的。一个登录账户可以访问多个数据库，而一个用户只能访问特定的数据库，并且不能直接访问 SQL Server 系统，只有给用户设置登录账户映射才能访问 SQL Server 系统，因此，合理地控制用户使用登录账号，也是确保数据库安全性的一个手段。

16.2 登录账号管理



微视频

管理登录名包括创建登录名、设置密码查看登录策略、查看登录名信息、修改和删除登录名。通过使用不同的登录名可以配置不同的访问级别。

16.2.1 创建登录账户

在创建登录账户时，一定要注意账号不能重名。下面介绍创建登录账户的方法。

1. 使用 T-SQL 语句创建登录账户

创建登录账户的 T-SQL 语法格式如下。

```
CREATE LOGIN loginName WITH PASSWORD='password'
[DEFAULT DATABASE=dbname]
```

主要参数介绍如下。

- loginName: 指定创建的登录名。
- password: 设置的登录账户密码，密码要尽量复杂一些。
- dbname: 指定账户登录的默认数据库名。如果不指定默认数据库名，则会将 master 数据库作为默认数据库。

实例 1：创建 SQL Server 登录名账户，语句如下。

```
CREATE LOGIN DBAdmin WITH PASSWORD= 'dbpwd', DEFAULT_DATABASE=test
```

输入完成，单击“执行”按钮，执行完成之后会创建一个名称为 DBAdmin 的 SQL Server 账户，密码为 dbpwd，默认数据库为 test，如图 16-1 所示。

知识扩展：除使用 CREATE LOGIN 语句创建登录账户外，我们还可以使用系统存储过程 sp_addlogin 来创建登录账户，具体的语法格式如下。

```
sp_addlogin username,userpwd default database;
```

其中，username 为登录名，userpwd 为密码，default database 为用户指定的默认数据库。如果使用 sp_addlogin 创建名称为 DBAdmin 的登录账户，具体语句如下。

```
sp_addlogin 'DBAdmin', 'dbpwd';
```

通过这个语句就可以与 CREATE LOGIN 语句一样登录账户了，如图 16-2 所示。

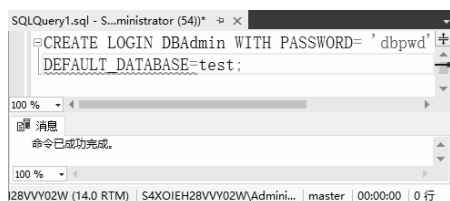


图 16-1 创建 SQL Server 登录名账户

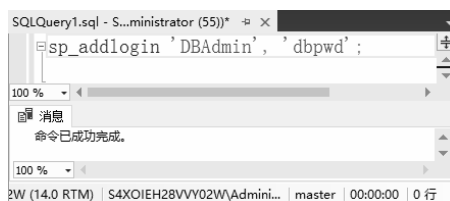


图 16-2 使用系统存储过程创建登录账户

2. 以图形向导方式创建 Windows 登录账户

Windows 身份验证模式是默认的验证方式，可以直接使用 Windows 的账户登录。创建过程可以分为如下几步：

(1) 单击“开始”按钮，在弹出的快捷菜单中选择“控制面板”命令，打开“控制面板”窗口，选择“管理工具”选项，如图 16-3 所示。

(2) 打开“管理工具”窗口，双击“计算机管理”选项，如图 16-4 所示。

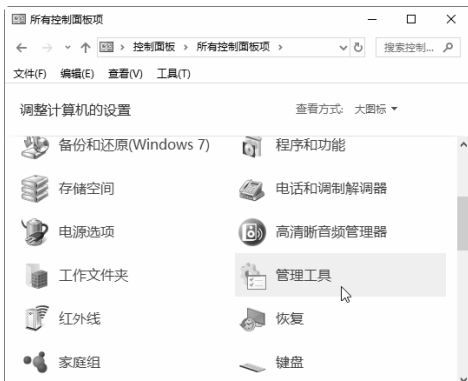


图 16-3 “控制面板”窗口

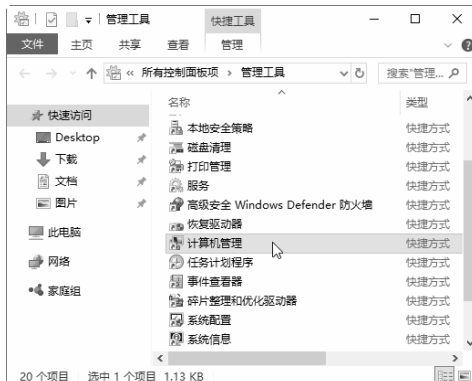


图 16-4 “管理工具”窗口

(3) 打开“计算机管理”窗口，选择“系统工具”→“本地用户和组”选项，选择“用户”节点，右击，在弹出的快捷菜单中选择“新用户”命令，如图 16-5 所示。

(4) 弹出“新用户”对话框，输入用户名为 DataBaseAdmin，描述为“数据库登录账户名”，设置登录密码之后，选中“密码永不过期”复选框，单击“创建”按钮，完成新用户的创建，如图 16-6 所示。

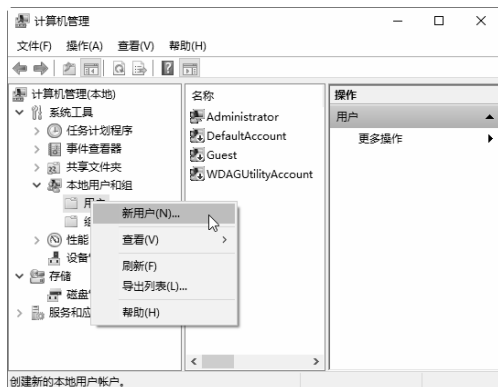


图 16-5 “计算机管理”窗口



图 16-6 “新用户”对话框

(5) 新用户创建完成之后，下面就可以创建映射到这些账户的 Windows 登录。登录到 SQL Server 2017 之后，在“对象资源管理器”窗口中打开“安全性”→“登录名”节点，选择“登录名”节点，右击，在弹出的快捷菜单中选择“新建登录名”命令，如图 16-7 所示。

(6) 打开“登录名-新建”窗口，单击“搜索”按钮，如图 16-8 所示。

(7) 弹出“选择用户或组”对话框，单击对话框中的“高级”和“立即查找”按钮，从用户列表中选择刚才创建的名称为 DataBaseAdmin 的用户，如图 16-9 所示。

(8) 选择用户完毕，单击“确定”按钮，返回“选择用户或组”对话框，这里列出了刚才选择的用户，如图 16-10 所示。



图 16-7 选择“新建登录名”命令

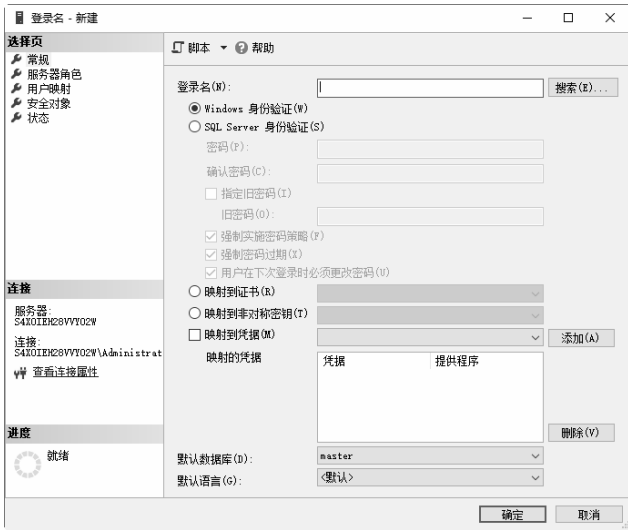


图 16-8 “登录名-新建”窗口



图 16-9 “选择用户或组”对话框 1



图 16-10 “选择用户或组”对话框 2

(9) 单击“确定”按钮，返回“登录名-新建”窗口，在该窗口中选中“Windows 身份验证”单选按钮，同时在下方的“默认数据库”下拉列表框中选择 master 数据库，如图 16-11 所示。

(10) 单击“确定”按钮，完成 Windows 身份验证账户的创建。为了验证创建结果，创建完成之后，重新启动计算机，使用新创建的操作系统用户 DataBaseAdmin 登录本地计算机，就可以使用 Windows 身份验证方式连接服务器了。

3. 以图形向导方式创建 SQL Server 登录账户

Windows 登录账户使用非常方便，只要能获得 Windows 操作系统的登录权限，就可以与 SQL Server 建立连接，如果正在为其创建登录的用户无法建立连接，则必须为其创建 SQL Server 登录账户。创建 SQL Server 登录账户可以分为如下几步：

(1) 登录到 SQL Server 2017 数据库，在“对象资源管理器”窗口中打开“安全性”→“登录名”

节点，选择“登录名”节点，右击，在弹出的快捷菜单中选择“新建登录名”命令，打开“登录名-新建”窗口，选中“SQL Server 身份验证”单选按钮，然后输入用户名和密码，取消选中的“强制实施密码策略”复选框，选择新账户的默认数据库，如图 16-12 所示。

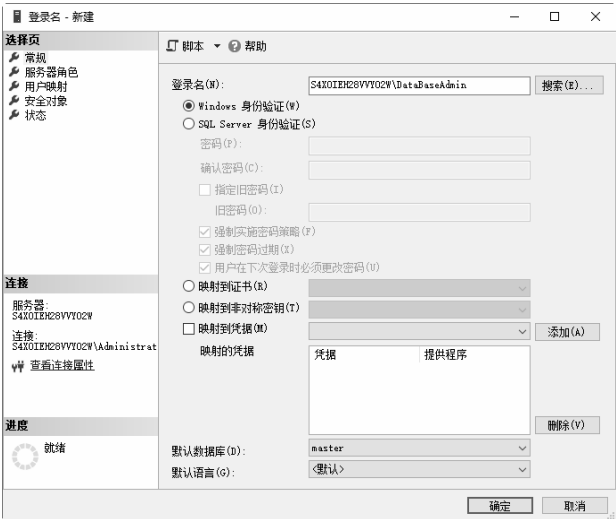


图 16-11 新建 Windows 登录

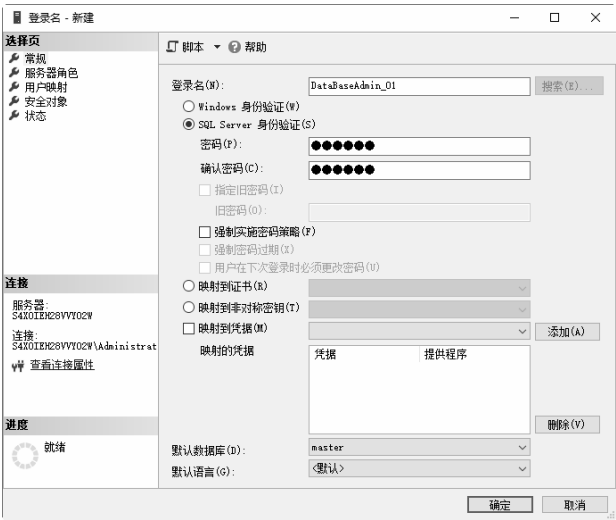


图 16-12 创建 SQL Server 登录账户

(2) 选择左侧的“用户映射”选项卡，启用默认数据库 master，系统会自动创建与登录名同名的数据库用户，并进行映射，这里可以选择该登录账户的数据库角色，为登录账户设置权限，默认选择 public 表示拥有最小权限，如图 16-13 所示。

(3) 单击“确定”按钮，完成 SQL Server 登录账户的创建。

4. 使用新账户登录 SQL Server

创建完成之后，可以断开服务器连接，重新打开 SQL Server Management Studio，使用登录名 DataBaseAdmin_01 进行连接，具体的操作步骤如下：

(1) 使用 Windows 登录账户登录到服务器之后，选择服务器节点，右击，在弹出的快捷菜单中选择“重新启动”命令，如图 16-14 所示。

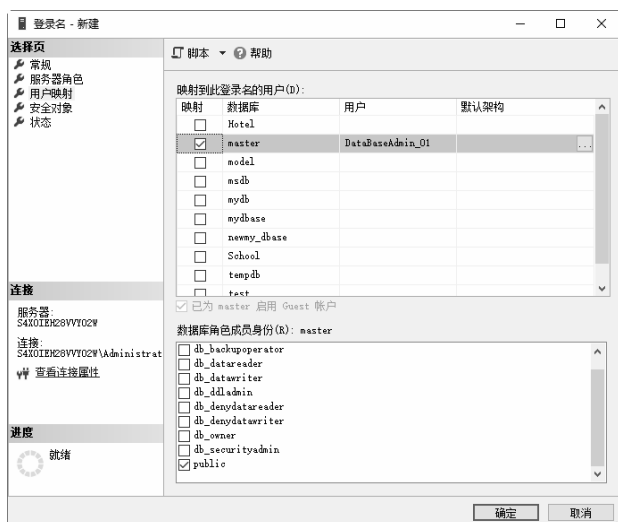


图 16-13 选择“用户映射”选项卡



图 16-14 选择“重新启动”命令

- (2) 在弹出的重启确认对话框中单击“是”按钮，如图 16-15 所示。
- (3) 系统开始自动重启，并显示重启的进度条，如图 16-16 所示。

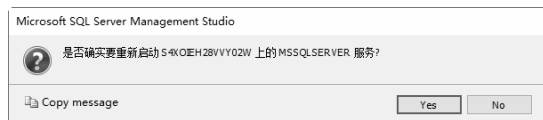


图 16-15 重启服务器提示对话框



图 16-16 显示重启进度

注意：上述重启步骤并不是必须的。如果在安装 SQL Server 2017 时指定登录模式为“混合模式”，则不需要重新启动服务器，直接使用新创建的 SQL Server 账户登录即可；否则需要修改服务器的登录方式，然后重新启动服务器。

- (4) 单击“对象资源管理器”左上角的“连接”按钮，在下拉列表框中选择“数据库引擎”命令，弹出“连接到服务器”对话框，从“身份验证”下拉列表框中选择“SQL Server 身份验证”选项，在“登录名”文本框中输入用户名 DataBaseAdmin_01，在“密码”文本框中输入对应的密码，如图 16-17 所示。
- (5) 单击“连接”按钮，登录服务器，登录成功之后可以查看相应的数据库对象，如图 16-18 所示。

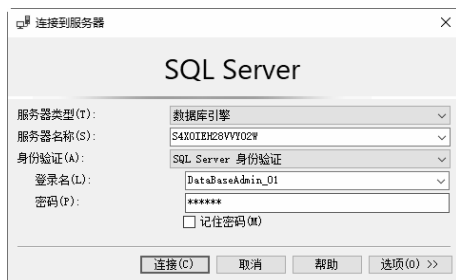


图 16-17 “连接到服务器”对话框



图 16-18 使用 SQL Server 账户登录

注意：使用新建的 SQL Server 账户登录之后，虽然能看到其他数据库，但是只能访问指定的 master 数据库，如果访问其他数据库，因为无权访问，系统将提示错误信息。另外，因为系统并没有给该登录账户配置任何权限，所以当前登录只能进入 master 数据库，不能执行其他操作。

16.2.2 修改登录账户

登录账户创建完成之后，可以根据需要修改登录账户的名称、密码、密码策略、默认数据库以及禁用或启用该登录账户等。

1. 使用 T-SQL 语句修改登录账户

修改登录账户信息使用 ALTER LOGIN 语句，具体的语法格式如下。

```
ALTER LOGIN loginName
[ENABLE | DISABLE]
WITH
{DEFAULT_DATABASE =database|NAME=new_loginName|PASSWORD='password'}
```

主要参数介绍如下。

- login_Name: 要修改的登录账户名称。
- ENABLE | DISABLE: 启用或禁用此登录。
- database: 默认数据库名。
- new_loginName: 修改后的账户名称。
- password: 密码。

实例 2: 使用 ALTER LOGIN 语句将登录名 DBAdmin 修改为 NewAdmin，输入如下语句。

```
ALTER LOGIN DBAdmin WITH NAME=NewAdmin;
```

输入完成，单击“执行”按钮即可完成登录账户名称的修改，如图 16-19 所示。

提示：除了使用 ALTER 语句修改登录账户外，还可以使用系统存储过程来完成，在修改登录账户密码时，可以使用系统存储过程 sp_password 来完成，在修改登录账号的默认数据库时，可以使用系统存储过程 sp_defaultdb 来完成。

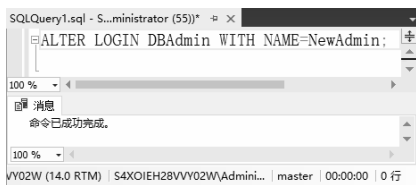


图 16-19 修改登录账户的名称

2. 以图形向导方式修改登录账户

用户可以通过图形化的管理工具修改登录账户，操作步骤如下。

- (1) 登录到 SQL Server 2017 数据库，在“对象资源管理器”窗口中打开“安全性”→“登录名”节点，该节点下列出了当前服务器中所有登录账户。
- (2) 选择要修改的用户，例如这里刚修改过的 DataBaseAdmin，右击，在弹出的快捷菜单中选择“重命名”命令，在显示的虚文本框中输入新的名称即可，如图 16-20 所示。
- (3) 如果要修改账户的其他属性信息，如默认数据库、权限等，可以在弹出的快捷菜单中选择“属性”命令，然后在弹出的“登录属性”窗口中进行修改，如图 16-21 所示。



图 16-20 选择“重命名”命令

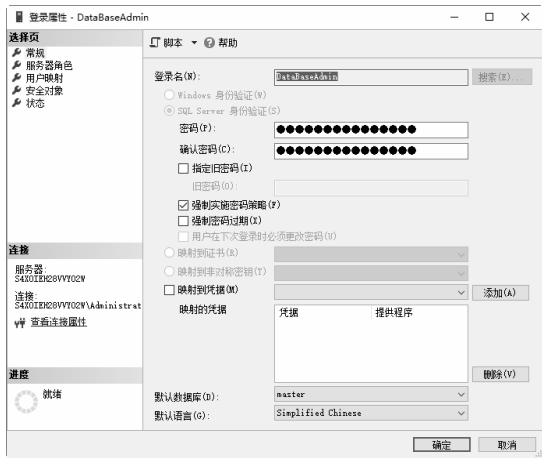


图 16-21 “登录属性”窗口

16.2.3 删除登录账户

对于不需要的登录账户，要及时进行删除，这样可以提高数据库的安全性。

1. 使用 T-SQL 语句删除登录账户

用户可以使用 DROP LOGIN 语句删除登录账户。DROP LOGIN 语句的语法格式如下。

```
DROP LOGIN login_name;
```

主要参数介绍如下。

- login_name: 登录账户的登录名。

实例 3: 使用 DROP LOGIN 语句删除名称为 NewAdmin 的登录账户，输入如下语句。

```
DROP LOGIN NewAdmin;
```

输入完成，单击“执行”按钮，完成删除操作，如图 16-22 所示。

提示: 删除登录账户还可以使用系统存储过程 sp_droplogin 来完成。

2. 以图形向导方式删除登录账户

用户可以在对象资源管理器中删除登录账户，操作步骤如下：

(1) 登录到 SQL Server 2017 数据库，在“对象资源管理器”窗口中打开“安全性”→“登录名”节点，该节点下列出了当前服务器中所有登录账户，如图 16-23 所示。

(2) 选择要删除的用户，例如这里选择 DataBaseAdmin，右击，在弹出的快捷菜单中选择“删除”命令，弹出“删除对象”窗口，如图 16-24 所示。

(3) 单击“确定”按钮，完成登录账户的删除操作。

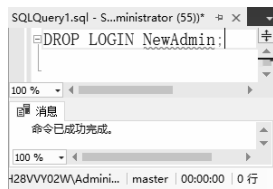


图 16-22 删除登录账户

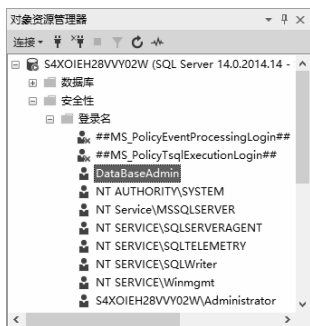


图 16-23 登录账户列表

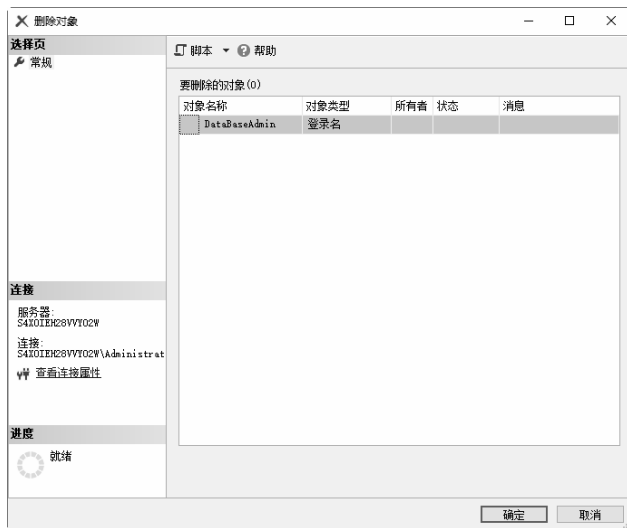


图 16-24 “删除对象”窗口



微视频

16.3 用户管理

使用登录账户只能让用户登录到 SQL Server 中，而不能让用户访问服务器中的数据库。如果想要访问特定的数据库，就必须有用户。对于用户的管理，我们可以通过 T-SQL 语句来完成，也可以以图形向导方式来完成。

16.3.1 创建用户

创建用户是用户管理中的第 1 步，注意，数据库中的用户不能重名，而且用户名不能以数字开头。

1. 使用 T-SQL 语句创建用户

创建用户的语法格式如下。

```
CREATE USER user_name [{FOR|FROM}
    { LOGIN login_name
    }
    | WITHOUT LOGIN
    ]
```

主要参数介绍如下。

- **user_name**: 用户名，指定登录数据库的用户名。
- **login_name**: 指定要创建数据库用户的 SQL Server 登录名。
- **WITHOUT LOGIN**: 指定不应该将用户映射到现有登录名。

注意: 如果在创建用户时没有指定登录名，那么就要将用户名创建成与登录名同名才可以，否则就会出现错误。

实例 4: 创建用户 testuser。

为方便创建用户，首先将用户 testuser 创建成登录名，然后再使用 CREATE USER 语句创建用户，语句如下。

```
CREATE LOGIN testuser WITH PASSWORD='000000';
CREATE USER testuser;
```

单击“执行”按钮，即可完成用户 testuser 的创建操作，如图 16-25 所示。

实例 5: 在指定数据库上创建用户，名称为 testuser_01，语句如下。

```
USE test
CREATE USER testuser_01 FOR LOGIN testuser;
```

单击“执行”按钮，即可完成用户 testuser_01 的创建操作，如图 16-26 所示。

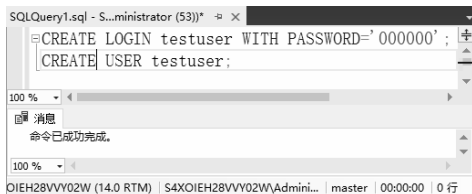


图 16-25 创建 testuser 用户

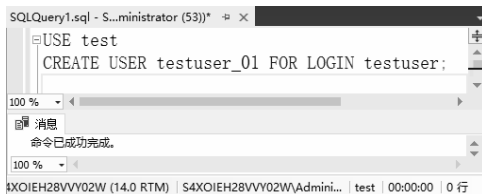


图 16-26 在指定数据库上创建用户

2. 以图形向导方式创建用户

在 SQL Server Management Studio 中，用户可以以图形向导方式创建用户，具体创建过程可分为如下几步：

- (1) 登录到 SQL Server 2017 数据库中，在“对象资源管理器”窗口中打开“数据库”→test→“安全性”节点，然后选择“用户”节点，右击，在弹出的快捷菜单中选择“新建用户”命令，如图 16-27 所示。
- (2) 弹出“数据库用户-新建”窗口，在这里需要为新建的用户选择一个登录名，如图 16-28 所示。
- (3) 单击登录名后面的“...”按钮，弹出“选择登录名”对话框，如图 16-29 所示。
- (4) 单击“浏览”按钮，打开“查找对象”对话框，在其中选择需要的登录名，这里选择 testuser，如图 16-30 所示。
- (5) 单击“确定”按钮，返回到“数据库用户-新建”对话框，在“用户名”文本框中输入创建的用户名信息，如图 16-31 所示。
- (6) 单击“确定”按钮，即可完成用户的创建，打开数据库下“安全性”节点，然后再打开“用户”节点，即可在用户列表中看到创建的用户，如图 16-32 所示。

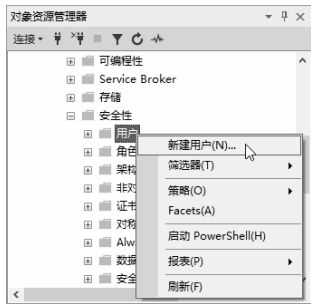


图 16-27 选择“新建用户”命令

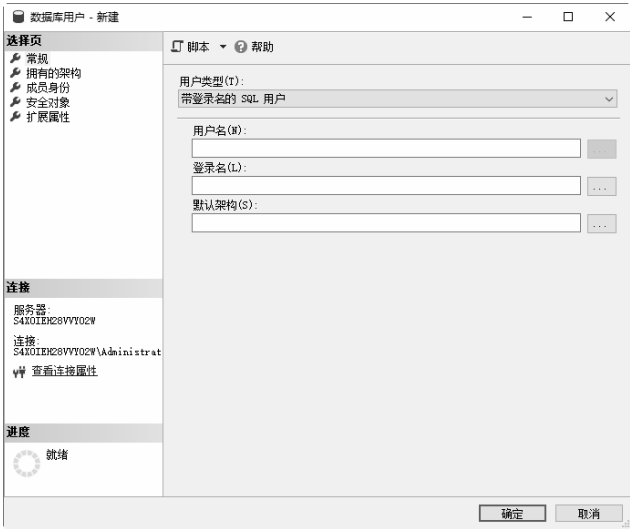


图 16-28 “数据库用户-新建”对话框

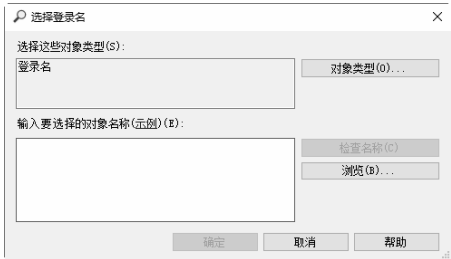


图 16-29 “选择登录名”对话框



图 16-30 “查找对象”对话框

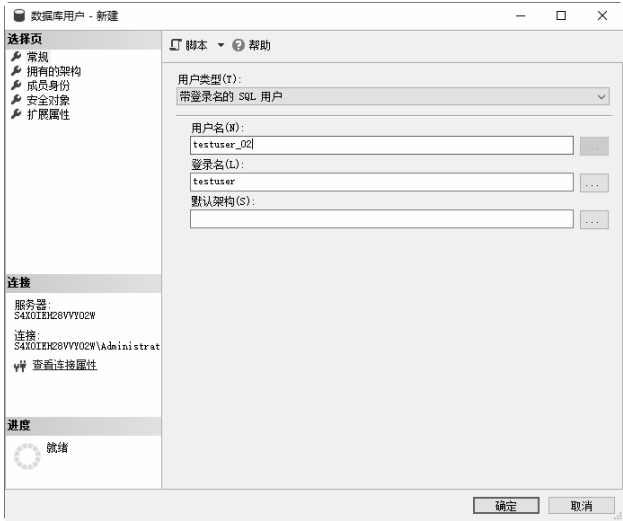


图 16-31 输入用户名信息

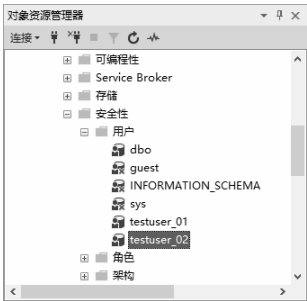


图 16-32 完成用户的创建

16.3.2 修改用户

用户创建完成后，我们还可以根据需要对用户进行修改，下面介绍修改用户信息的方法。

1. 使用 SQL 语句修改用户

使用 ALTER USER 语句可以修改用户信息，具体的语法格式如下。

```
ALTER USER user_name WITH
{
    NAME=new_username|LOGIN=loginname
}
```

主要参数介绍如下。

- user_name: 用户名，指定要修改的用户名。
- new_username: 修改后的用户名。
- loginname: 修改后的登录名。

实例 6: 修改用户 testuser 的名称为 newtestuser，语句如下。

```
USE master
ALTER USER testuser WITH
NAME=newtestuser;
```

单击“执行”按钮，即可完成用户 testuser 名称的修改操作，如图 16-33 所示。

2. 以图形向导方式修改用户

在 SQL Server Management Studio 中，用户可以以图形向导方式修改用户，不过，这个方式不能修改用户的登录名，修改用户可分为如下几步：

(1) 登录到 SQL Server 2017 数据库中，在“对象资源管理器”窗口中打开“数据库”→test→“安全性”→“用户”节点，选择需要修改的用户，右击，在弹出的快捷菜单中选择“属性”命令，如图 16-34 所示。

(2) 打开“数据库用户-testuser_01”对话框，选择“常规”选项卡，在打开的界面中可以修改用户的默认架构，但是不能修改用户名与登录名，如图 16-35 所示。

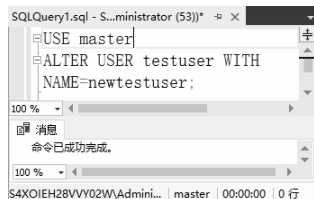


图 16-33 修改用户的名称



图 16-34 选择“属性”命令

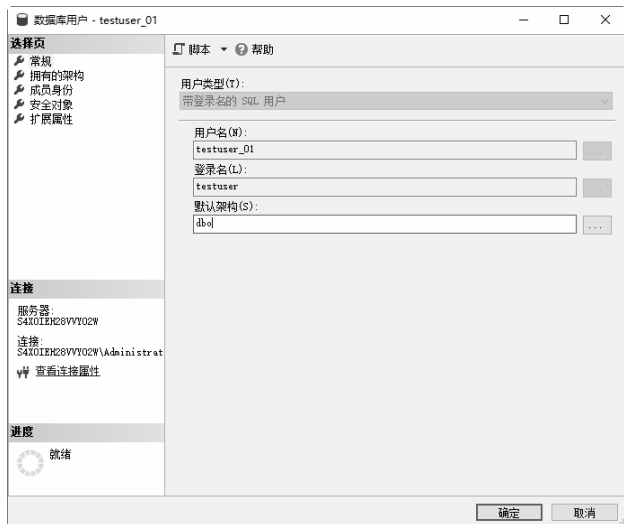


图 16-35 “数据库用户”对话框

(3) 选择“拥有的架构”选项卡，在右侧可以查看此用户拥有的架构，并对其进行选择操作，如图 16-36 所示。

(4) 选择“成员身份”选项卡，在右侧可以查看此用户拥有的数据库角色成员身份，并对其进行选择操作，如图 16-37 所示。

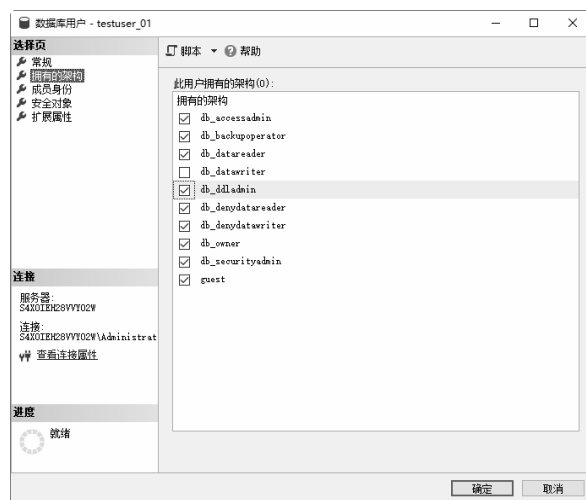


图 16-36 选择“拥有的架构”选项卡

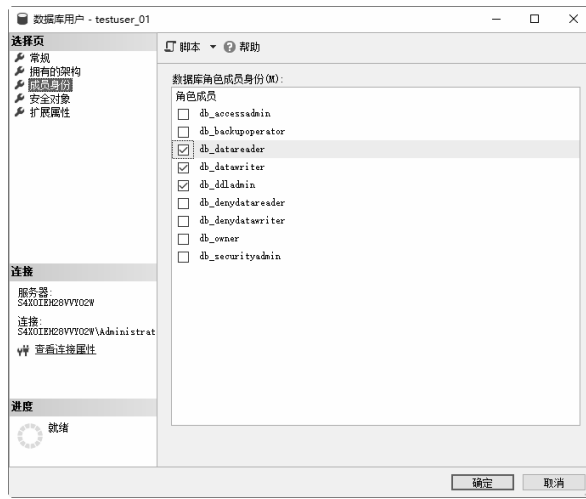


图 16-37 选择“成员身份”选项卡

16.3.3 删除用户

对于不需要的用户，我们可以将其删除，下面介绍删除用户的方法。

1. 使用 T-SQL 语句删除用户

使用 DROP USER 语句可以删除用户信息，具体的语法格式如下。

```
DROP USER user_name;
```

user_name 为要删除的用户名称。

注意：在删除用户名之前，先要将用户所在的数据库使用 USE 语句打开。

实例 7：删除用户 newtestuser，语句如下。

```
USE master
DROP USER newtestuser;
```

单击“执行”按钮，即可完成用户 newtestuser 的删除操作，如图 16-38 所示。

2. 以图形向导方式删除用户

在 SQL Server Management Studio 中，用户可以以图形向导方式删除用户，删除用户可分为如下几步：

(1) 登录到 SQL Server 2017 数据库中，在“对象资源管理器”窗口中打开“数据库”→test→“安全

性”→“用户”节点，选择需要删除的用户，右击，在弹出的快捷菜单中选择“删除”命令，如图 16-39 所示。

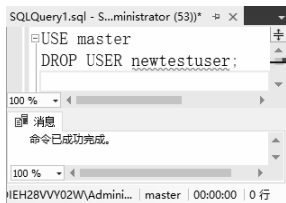


图 16-38 删除用户

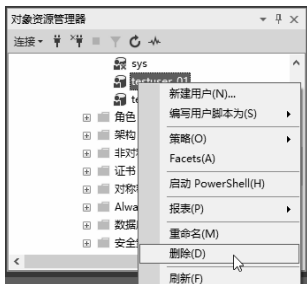


图 16-39 选择“删除”命令

(2) 打开“删除对象”对话框，单击“确定”按钮，即可删除选择的用户，如图 16-40 所示。

知识扩展：如果不清楚要删除的用户名，可以通过系统存储过程 SP_HELPUSER 来查看，语句如下。

```
SP_HELPUSER;
```

单击“执行”按钮，即可在“结果”窗格中显示当前数据库的用户信息，如图 16-41 所示。

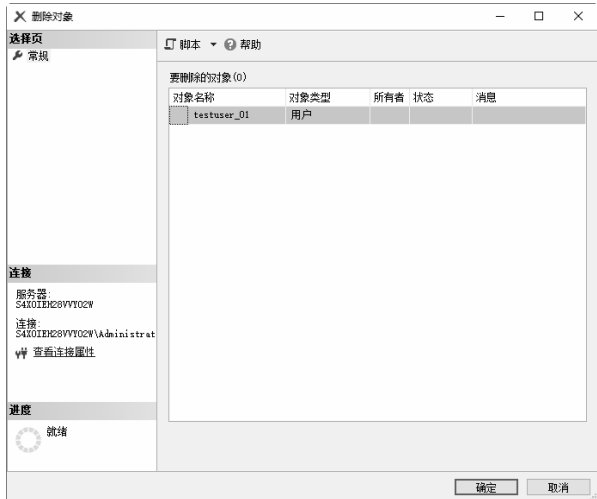


图 16-40 “删除对象”对话框

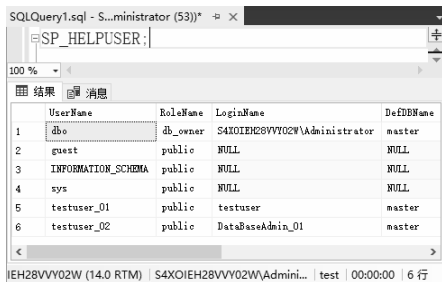


图 16-41 当前数据库用户信息

16.4 角色管理

数据库中的角色相当于 Windows 操作系统中的用户组，可以集中管理数据库或服务器的权限，本节就来介绍角色的管理。

16.4.1 认识角色

按照角色的作用范围，可以将数据库中的角色分为 4 类，分别为：固定服务器角色、数据库角色、应用程序角色和自定义数据库角色。

1. 固定服务器角色

SQL Server 2017 为用户提供了 9 个固定服务器角色，在“对象资源管理器”窗口中打开“安全性”→“服务器角色”节点，即可看到所有的固定服务器角色，如图 16-42 所示。



微视频

下面详细介绍各个服务器角色功能。

- (1) **bulkadmin**: 固定服务器角色的成员可以运行 **BULK INSERT** 语句。
- (2) **dbcreator**: 固定服务器角色的成员可以创建、更改、删除和还原任何数据库。
- (3) **diskadmin**: 固定服务器角色用于管理磁盘文件。
- (4) **processadmin**: 固定服务器角色的成员可以终止在 SQL Server 实例中运行的进程。
- (5) **public**: 每个 SQL Server 登录名都属于 **public** 服务器角色。如果未向某个服务器主体授予或拒绝对某个安全对象的特定权限，该用户将继承授予该对象的 **public** 角色的权限。
- (6) **securityadmin**: 固定服务器角色的成员可以管理登录名及其属性。它们可以拥有 **GRANT**、**DENY** 和 **REVOKE** 服务器级别的权限，也可以拥有 **GRANT**、**DENY** 和 **REVOKE** 数据库级别的权限。此外，它们还可以重置 SQL Server 登录名的密码。
- (7) **serveradmin**: 固定服务器角色的成员可以更改服务器范围的配置选项和关闭服务器。
- (8) **setupadmin**: 固定服务器角色的成员可以添加和删除连接服务器。
- (9) **sysadmin**: 固定服务器角色的成员可以在服务器上执行任何活动。默认情况下，Windows **BUILTIN\Administrators** 组（本地管理员组）的所有成员都是 **sysadmin** 固定服务器角色的成员。

2. 数据库角色

数据库角色是针对某个具体数据库的权限分配，数据库用户可以作为数据库角色的成员，继承数据库角色的权限，数据库管理人员也可以通过管理角色的权限来管理数据库用户的权限。

SQL Server 2017 中系统默认添加了 10 个固定的数据库角色，在“对象资源管理器”窗口中打开“数据库”→**test**→“安全性”→“角色”→“数据库角色”节点，即可看到所有的数据库角色，如图 16-43 所示。

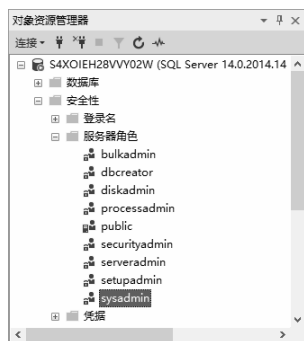


图 16-42 固定服务器角色列表

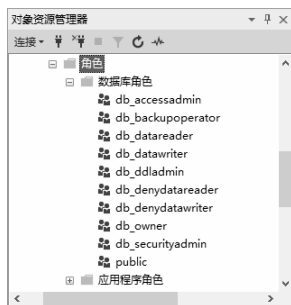


图 16-43 数据库角色列表

下面详细介绍各个数据库角色的功能。

- (1) **db_accessadmin**: 数据库角色的成员可以为 Windows 登录名、Windows 组和 SQL Server 登录名添加或删除数据库访问权限。
- (2) **db_backupoperator**: 数据库角色的成员可以备份数据库。
- (3) **db_datareader**: 数据库角色的成员可以从所有用户表中读取所有数据。
- (4) **db_datawriter**: 数据库角色的成员可以在所有用户表中添加、删除或更改数据。
- (5) **db_ddladmin**: 数据库角色的成员可以在数据库中运行任何数据定义语言（DDL）命令。
- (6) **db_denydatareader**: 数据库角色的成员不能读取数据库内用户表中的任何数据。
- (7) **db_denydatawriter**: 数据库角色的成员不能添加、修改或删除数据库内用户表中的任何数据。
- (8) **db_owner**: 数据库角色的成员可以执行数据库的所有配置和维护活动，还可以删除数据库。
- (9) **db_securityadmin**: 数据库角色的成员可以修改角色成员身份和管理权限。向此角色中添加主体可能会导致意外的权限升级。
- (10) **public**: 每个数据库用户都属于 **public** 数据库角色。如果未向某个用户授予或拒绝对安全对象的特定权限时，该用户将继承授予该对象的 **public** 角色的权限。

3. 应用程序角色

应用程序角色能够用其自身、类似用户的权限来运行，它是一个数据库主体。应用程序主体只允许通过特定应用程序连接的用户访问特定数据。与服务器角色和数据库角色不同，SQL Server 2017 中应用程序角色在默认情况下不包含任何成员，并且应用程序角色必须激活之后才能发挥作用。当激活某个应用程序角色之后，连接将失去用户权限，转而获得应用程序权限。

4. 自定义数据库角色

在实际的数据库管理过程中，某些用户可能只能对数据库进行插入、更新和删除的操作，但是固定数据库角色中不能提供这样一个角色，这就需要用户自己来定义数据库角色，这些角色就是自定义数据库角色。

16.4.2 创建角色

我们可以使用 T-SQL 语句和以图形向导方式来创建角色。

1. 使用 T-SQL 语句创建角色

自定义角色使用 CREATE ROLE 语句来完成，具体的语法格式如下。

```
CREATE ROLE role_name [AUTHORIZATION OWNER_name];
```

主要参数介绍如下。

- **role_name**: 角色名称。该角色名称不能与数据库固定角色名称重名。
- **OWNER_name**: 用户名称。角色所作用的用户名称，如果省略了该名称，角色就被创建到当前数据库的用户上。

注意：通过 CREATE ROLE 语句创建的角色并没有设置权限，只是创建了一个角色名称而已，在下面的小节中会介绍如何给角色分配权限。

实例 8：创建角色 role_01，该角色作用于 test 数据库中的 testuser_01 用户上，语句如下。

```
CREATE ROLE role_01 AUTHORIZATION testuser_01;
```

单击“执行”按钮，即可完成角色 role_01 的创建，如图 16-44 所示。

知识扩展：如果想要查看数据库是否存在这个角色，可以通过系统存储过程 SP_HELPROLE 来查看。具体的查询效果如图 16-45 所示，其中第 2 个角色就是我们创建的自定义角色。

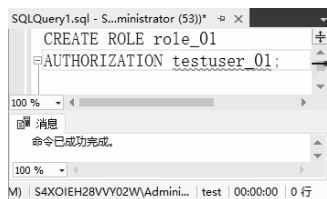


图 16-44 创建角色

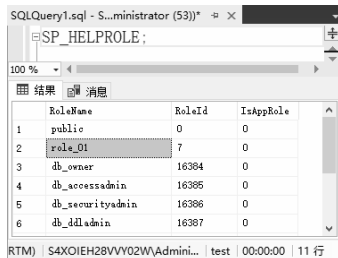


图 16-45 查询角色

2. 以图形向导方式创建角色

在 SQL Server Management Studio 中，用户可以以图形向导方式创建用户，具体创建过程可分为如下几步：

1) 添加用户

(1) 登录到 SQL Server 2017 数据库，在“对象资源管理器”窗口中打开“数据库”→test→“安全性”→“角色”节点，选择“数据库角色”节点，右击，在弹出的快捷菜单中选择“新建数据库角色”命令，如图 16-46 所示。

(2) 打开“数据库角色-新建”窗口。设置角色名称为 role_02，所有者选择 dbo，单击“添加”按钮，如图 16-47 所示。



图 16-46 选择“新建数据库角色”命令

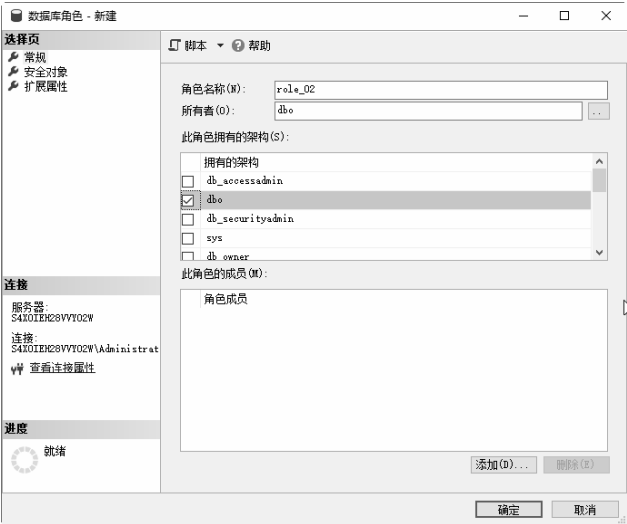


图 16-47 “数据库角色-新建”窗口 1

(3) 打开“选择数据库用户或角色”对话框，单击“浏览”按钮，找到并添加对象 public，单击“确定”按钮，如图 16-48 所示。

(4) 添加用户完成，返回“数据库角色-新建”窗口，如图 16-49 所示。

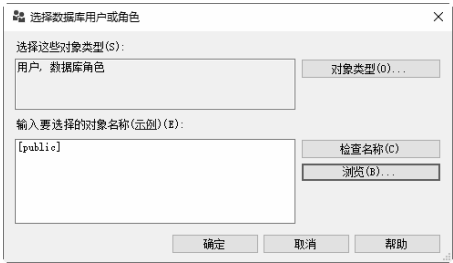


图 16-48 “选择数据库用户或角色”对话框

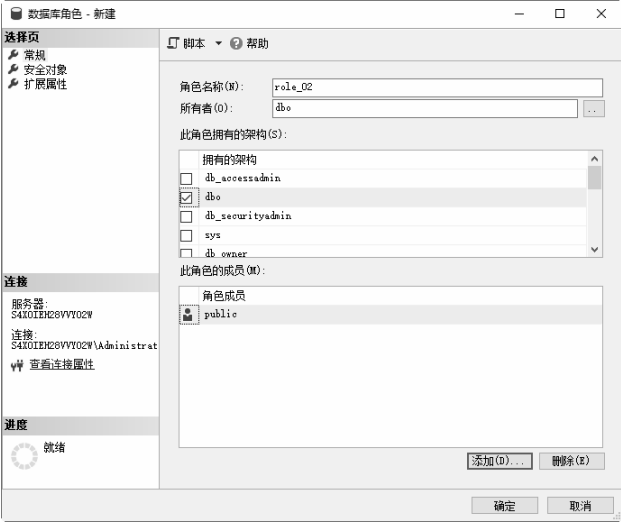


图 16-49 “数据库角色-新建”窗口 2

2) 添加角色

(1) 选择“数据库角色-新建”窗口左侧的“安全对象”选项卡，在“安全对象”选项卡中单击“搜索”按钮，如图 16-50 所示。

(2) 打开“添加对象”对话框，选中“特定对象”单选按钮，如图 16-51 所示。

(3) 单击“确定”按钮，打开“选择对象”对话框，单击“对象类型”按钮，如图 16-52 所示。

(4) 打开“选择对象类型”对话框，选中“表”复选框，如图 16-53 所示。

(5) 完成选择后，单击“确定”按钮返回，然后再单击“选择对象”窗口中的“浏览”按钮，如图 16-54 所示。



图 16-50 选择“安全对象”选项卡

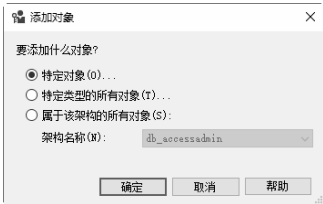


图 16-51 “添加对象”对话框



图 16-52 “选择对象”对话框 1

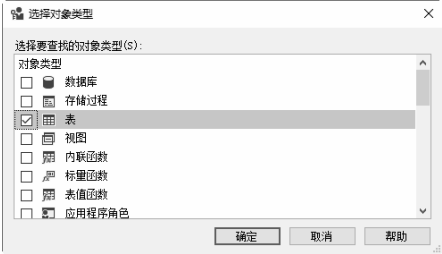


图 16-53 “选择对象类型”对话框

(6) 打开“查找对象”对话框，选中匹配的对象列表中的“人员信息表”前面的复选框，如图 16-55 所示。

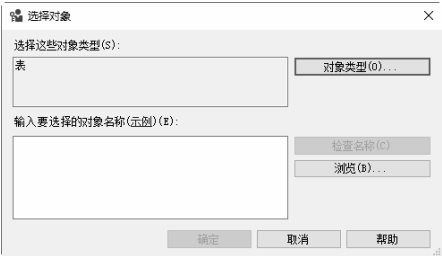


图 16-54 “选择对象”对话框 2

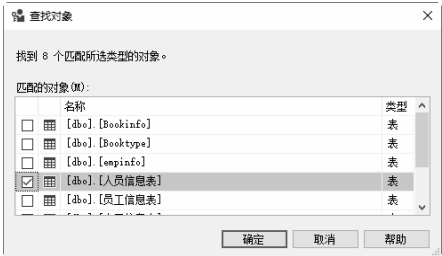


图 16-55 选择人员信息表数据表

(7) 单击“确定”按钮，返回“选择对象”对话框，如图 16-56 所示。

(8) 单击“确定”按钮，返回“数据库角色-新建”窗口，如图 16-57 所示。

(9) 单击“确定”按钮，完成角色的创建。

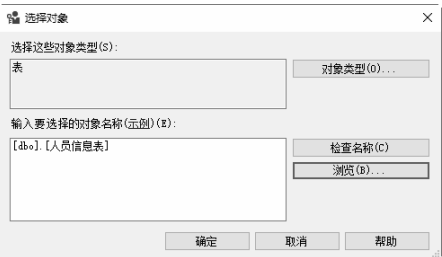


图 16-56 “选择对象”对话框 3

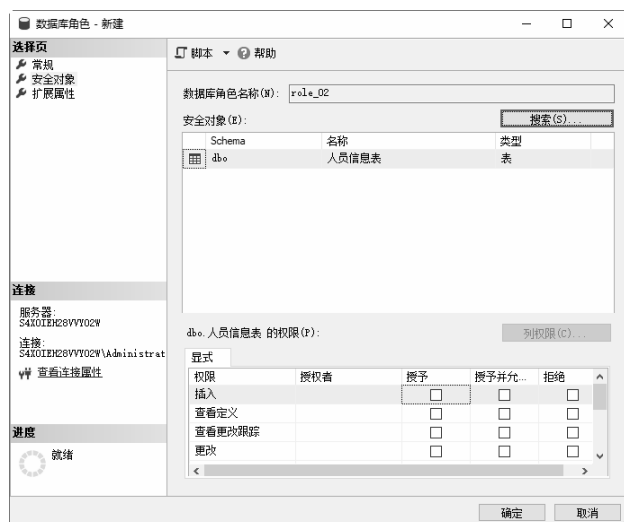


图 16-57 “数据库角色-新建”窗口 3

16.4.3 修改角色

修改角色比较简单，不过只能对角色的名称进行修改，其他的内容是不能够被修改的。

1. 使用 T-SQL 语句修改角色

修改角色使用 ALTER ROLE 语句，具体的语法格式如下。

```
ALTER ROLE role_name WITH NAME=new_role_name;
```

主要参数介绍如下。

- role_name: 角色名称，指定要修改的角色名称。
- new_role_name: 修改后的角色名称。

实例 9：修改角色 role_01 的名称为 new_role_01，语句如下。

```
USE test
ALTER ROLE role_01 WITH
NAME=new_role_01;
```

单击“执行”按钮，即可完成角色 role_01 名称的修改操作，如图 16-58 所示。

2. 以图形向导方式修改角色

在 SQL Server Management Studio 中，用户可以以图形向导方式修改角色，修改角色可分为如下几步：

(1) 登录到 SQL Server 2017 数据库中，在“对象资源管理器”窗口中打开“数据库”→test→“安全性”→“角色”节点，选择需要修改的角色，右击，在弹出的快捷菜单中选择“属性”命令，如图 16-59 所示。

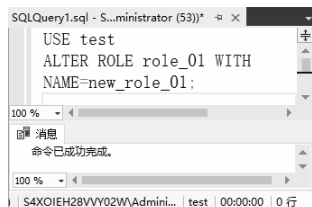


图 16-58 修改角色



图 16-59 选择“属性”命令

(2) 打开“数据库角色属性-new_role_01”窗口，在其中可以修改角色的相关信息，最后单击“确定”按钮，即可完成修改操作，如图 16-60 所示。

16.4.4 删除角色

对于不需要的角色，我们可以将其删除，下面介绍删除角色的方法。

1. 使用 T-SQL 语句删除角色

使用 DROP ROLE 语句可以删除角色信息，具体的语法格式如下。

```
DROP ROLE role_name;
```

role_name 为要删除的角色名称。

注意：在删除角色之前，先要将角色所在的数据库使用 USE 语句打开。

实例 10：删除角色 new_role_01，语句如下。

```
USE test
DROP ROLE new_role_01;
```

单击“执行”按钮，即可完成角色 new_role_01 的删除操作，如图 16-61 所示。

2. 以图形向导方式删除角色

在 SQL Server Management Studio 中，用户可以以图形向导方式删除角色，删除角色可分为如下几步：

(1) 登录到 SQL Server 2017 数据库中，在“对象资源管理器”窗口中打开“数据库”→test→“安全性”→“角色”节点，选择需要删除的角色，右击，在弹出的快捷菜单中选择“删除”命令，如图 16-62 所示。

(2) 打开“删除对象”对话框，单击“确定”按钮，即可删除选择的角色，如图 16-63 所示。

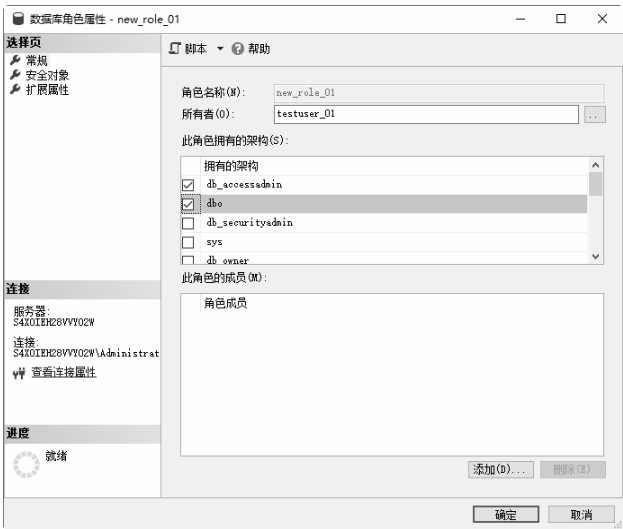


图 16-60 “数据库角色属性-new_role_01”窗口

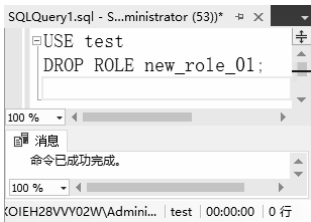


图 16-61 删除角色



图 16-62 选择“删除”命令

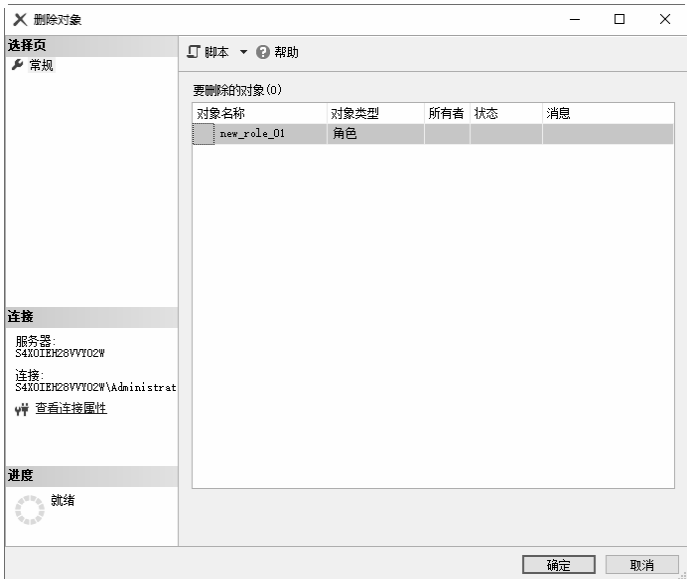


图 16-63 “删除对象”对话框



微视频

16.5 权限管理

在 SQL Server 2017 中，根据是否是系统预定义，可以把权限划分为预定义权限和自定义权限；按照权限与特定对象的关系，可以把权限划分为针对所有对象的权限和针对特殊对象的权限。

16.5.1 认识权限

在 SQL Server 中，根据不同的情况，可以把权限更为细致地分类，包括预定义权限和自定义权限、所有对象权限和特殊对象权限。

- 预定义权限：SQL Server 2017 安装完成之后即可以拥有预定义权限，不必通过授予即可取得。固定服务器角色和固定数据库角色就属于预定义权限。
- 自定义权限：是指需要经过授权或者继承才可以得到的权限，大多数安全主体都需要经过授权才能获得指定对象的使用权限。
- 所有对象权限：可以针对 SQL Server 2017 中所有的数据库对象，CONTROL 权限可用于所有对象。
- 特殊对象权限：是指某些只能在指定对象上执行的权限，例如 SELECT 可用于表或者视图，但是不可用于存储过程；而 EXEC 权限只能用于存储过程，而不能用于表或者视图。

针对表和视图，数据库用户在操作这些对象之前必须拥有相应的操作权限，可以授予数据库用户的针对表和视图的权限有 INSERT、UPDATE、DELETE、SELECT 和 REFERENCES 5 种。

用户只有获得了针对某种对象指定的权限后，才能对该类对象执行相应的操作，在 SQL Server 2017 中，不同的对象有不同的权限，权限管理包括下面的内容：授予权限、拒绝权限和撤销权限。

16.5.2 授予权限

为了允许用户执行某些操作，需要授予相应的权限，使用 GRANT 语句进行授权活动，授予权限命令的基本语法格式如下。

```
GRANT permission
    [ ON table_name|view_name]
    TO user_name|role_name
    WITH GRANT OPTION
```

主要参数介绍如下。

- permission: 权限的名称，例如 SELECT、UPDATE、EXEC 等。
- table_name|view_name: 表名或视图名。
- user_name|role_name: 用户名或角色名。
- WITH GRANT OPTION: 表明权限授予者可以向其他用户授予权限。

实例 11: 向 role_02 角色授予对 test 数据库中水果信息表的 SELECT、INSERT、UPDATE 和 DELETE 权限，输入如下语句。

```
USE test;
GRANT SELECT, INSERT, UPDATE, DELETE
ON 水果信息表
TO role_02
GO
```

单击“执行”按钮，即可完成授予权限的操作，如图 16-64 所示。

16.5.3 拒绝权限

拒绝权限可以在授予用户指定的操作权限之后，根据需要暂时停止用户对指定数据库对象的访问或操作，拒绝对象权限的基本语法格式如下。

```
DENY permission
```

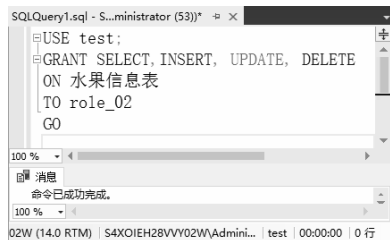


图 16-64 授予权限

```
[ ON table_name|view_name]
TO user_name|role_name
WITH GRANT OPTION
```

主要参数介绍如下。

- permission: 权限的名称, 例如 SELECT、UPDATE、EXEC 等。
- table_name|view_name: 表名或视图名。
- user_name|role_name: 用户名或角色名。
- WITH GRANT OPTION: 表明权限授予者可以向其他用户授予权限。

实例 12: 拒绝 guest 用户对 test 数据库中水果信息表的 INSERT 和 DELETE 权限, 输入如下语句。

```
USE test;
GO
DENY INSERT, DELETE
ON 水果信息表
TO guest
GO
```

单击“执行”按钮, 即可完成拒绝权限的操作, 如图 16-65 所示。

知识扩展: 使用系统存储过程 sp_helprotect 可以查看用户 guest 用户当前所具有的权限, 如图 16-66 所示。



图 16-65 拒绝权限



图 16-66 查看用户具有的权限

16.5.4 撤销权限

撤销权限可以删除某个用户已经授予的权限。撤销权限使用 REVOKE 语句, 具体的语法格式如下。

```
REVOKE permission
[ ON table_name|view_name]
TO user_name|role_name
WITH GRANT OPTION
```

主要参数介绍如下。

- permission: 权限的名称, 例如 SELECT、UPDATE、EXEC 等。
- table_name|view_name: 表名或视图名。
- user_name|role_name: 用户名或角色名。
- WITH GRANT OPTION: 表明权限授予者可以向其他用户授予权限。

实例 13: 撤销 role_02 角色对 test 数据库中水果信息表的 DELETE 权限, 输入如下语句。

```
USE test;
REVOKE DELETE
ON 水果信息表
TO role_02
GO
```

单击“执行”按钮, 即可完成撤销权限的操作, 如图 16-67 所示。

注意: 在数据库中, 权限是不能够独立创建的, 全部都是在其用户或角色上进行操作的, 因此, 在 SQL Server Management Studio 中, 创

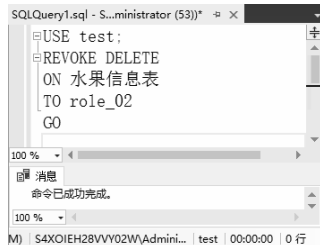


图 16-67 撤销权限

建用户或角色时,其权限也就设置完成了。这里就不再介绍以图形向导方式管理权限的操作了。

16.6 课后习题与练习

一、填空题

1. 创建登录账户使用的 SQL 语句是_____。

答案: CREATE LOGIN loginName

2. 在 SQL Server 中,授权的 SQL 语句是_____,拒绝权限的 SQL 语句是_____,撤销权限的语句是_____。

答案: GRANT, DENY, REVOKE

3. 在 SQL Server 中,角色可分为两类,分别是系统角色和_____。

答案: 自定义角色

4. SQL Server 的登录账户可以分为_____和 SQL Server 账户两种。

答案: Windows 登录账户

5. 通过系统存储过程_____可以查看固定数据库角色列表。

答案: SP_HELPROLE

二、选择题

1. 下面哪个语句是用来创建用户的_____。

A. CREATE USER B. CREATE TABLE C. CREATE USERS D. 以上都不是

答案: A

2. 下面关于角色的描述正确的是_____。

A. 在 SQL Server 数据库中,角色与用户是同一个意思
B. 在 SQL Server 数据库中,角色可以理解成权限的一个集合,可以通过角色给用户授予权限
C. 在 SQL Server 数据库中,角色就是权限
D. 以上都不对

答案: B

3. 下面不属于 SQL Server 登录名管理语句的是_____。

A. CREATE LOGIN B. EXEC SP_GRANTLOGIN
C. EXEC SP_ADDLOGIN D. DELETE LOGIN

答案: D

4. 下面_____角色不允许用户读取数据库内所有表中的数据。

A. db_datareader B. db_datawriter C. db_denydatareader D. db_denydatawriter

答案: C

5. 将数据库中创建数据表的权限授予数据库用户 testUser,使用下面_____语句。

A. GRANT testUser ON CREATE TABLE
B. GRANT CREATE TABLE TO testUser
C. REVOKE CREATE TABLE FROM testUser
D. DENY CREATE TABLE FROM testUser

答案: B

三、简答题

1. 登录账户与用户有什么区别?
2. 在数据库中,使用角色的好处有哪些?
3. 简述角色与权限的关系。

16.7 新手疑难问题解答

疑问 1: 创建数据库用户后, 给该用户授予操作权限, 怎样来验证用户是否具有这些权限?

解答: 创建数据库用户之后, 可以以数据库用户的身份重新与 SQL Server 建立连接, 这时对 SQL Server 执行操作的就是已创建的用户, 可以验证该用户的权限。

疑问 2: 在删除登录账户时, 有时会提示无法删除映射的数据库用户, 这是为什么?

解答: 在删除登录名之前, 最好将其映射到数据库的用户名删除, 若没有删除用户名, 则系统会给出一个提示信息。

16.8 实战训练

在 SQL Server Management Studio 中, 对图书管理数据库 Library 的安全性进行设置。

- (1) 创建图书管理数据库的管理员 admin, 可以对该数据库执行所有的操作。
- (2) 创建读者用户 user, 只能对 Reader 表中 Readername、Birthday、Sex、Address 和 Tel 字段进行操作。
- (3) 创建图书借阅操作员用户 operator, 可以对借阅记录 Record 表进行查看、修改、删除操作。
- (4) 创建一个角色 Role, 只能对 Record 表进行操作。
- (5) 创建一个图书借阅操作员用户 op, 将该用户添入角色 Role 中。