数据库系统开发实验报告

SQL Server 安全机制

1. 实验目的

通过本实验，掌握 SQL Server 安全机制，包括 SQL Server 安全、数据库用户与权限，掌握身份验证、登录、数据库用户、服务器角色、数据库角色、权限与授权方法等相关概念及其相互关系。

2. 实验内容

（1） 创建一个数据库。在新创建的数据库下创建一个学生基本信息表，插入若干记录。

使用管理员登录连接到服务器，新建数据库 E2_3,并在该数据库下创建学生基本信息表 Student，插入 5 条记录，实现命令代码如下：

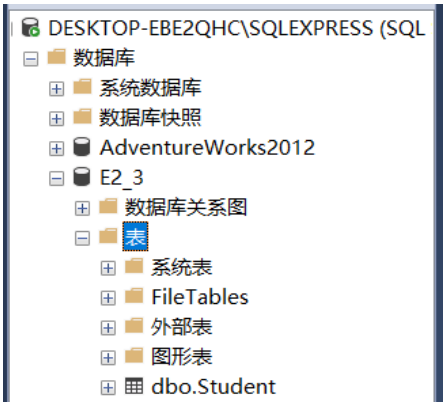
```
use master
go
create database E2_3 on primary
(
    name='E2_3',
    filename = 'D:\MyLocalDB\E2_3.mdf',
    size = 5mb,
    maxsize = 50mb,
    filegrowth = 1mb
)
log on
(
    name='E2_3_log',
    filename='D:\MyLocalDB\E2_3_log.ldf',
    size=2mb,
    maxsize=20mb,
    filegrowth=1mb
)
go
use E2_3
go
create table Student(
    sno char(10) primary key,
    sname nvarchar(10) not null,
    ssex nchar(2) check(ssex in('男','女')) not null
)
go
```

```
insert into Student(sno,sname,ssex) values('1001','张三','男');
insert into Student(sno,sname,ssex) values('1002','李四','女');
insert into Student(sno,sname,ssex) values('1003','王五','男');
insert into Student(sno,sname,ssex) values('1004','赵六','女');
insert into Student(sno,sname,ssex) values('1005','孙七','男');
go
```

命令代码运行结果为:

```
(1 行受影响)

(1 行受影响)

(1 行受影响)

(1 行受影响)

(1 行受影响)

完成时间: 2020-09-21T11:39:47.8286989+08:00
```

资源管理器显示相应数据库与表

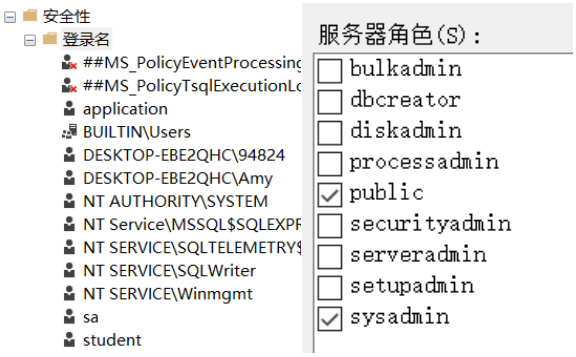


(2) 创建一个 Windows 身份验证的登录 1，将默认数据库设置为 Master 数据库。将登录 1 设置为数据库系统管理员。

创建 Windows 身份验证的登录名 DESKTOP-EBE2QHC\Amy，设置默认数据库为 master，并设置服务器角色 sysadmin，实现命令代码如下

```
USE [master]
GO
CREATE LOGIN [DESKTOP-EBE2QHC\Amy] FROM WINDOWS WITH DEFAULT_DATABASE=[master]
GO
ALTER SERVER ROLE [sysadmin] ADD MEMBER [DESKTOP-EBE2QHC\Amy]
GO
```

服务器实例中出现登录名 DESKTOP-EBE2QHC\Amy，其服务器角色为:

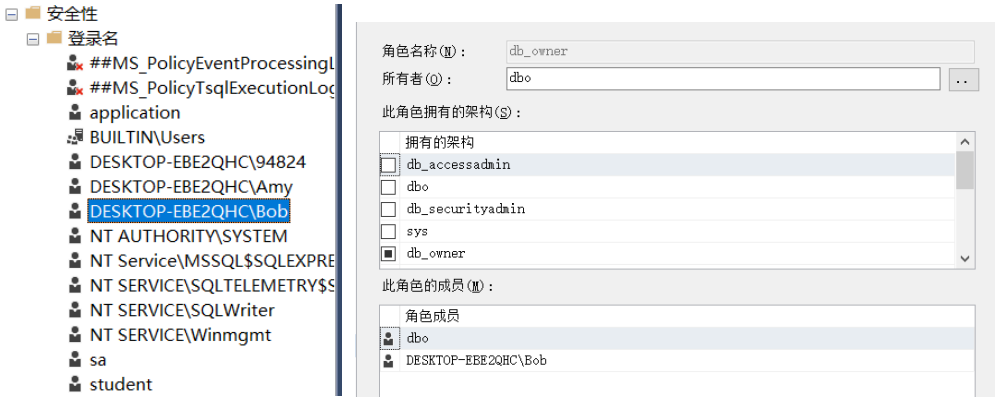


(3) 创建一个 Windows 身份验证的登录 2，将默认数据库设置为新创建的数据库。授权登录 2 为新创建的数据库的管理员。

创建 Windows 身份验证的登录名 DESKTOP-EBE2QHC\Bob，设置默认数据库为 E2_3，并设置其对数据库 E2_3 映射的用户 DESKTOP-EBE2QHC\Bob 添加到 db_owner 数据库成员列表中，实现命令代码如下

```
USE [master]
GO
CREATE LOGIN [DESKTOP-EBE2QHC\Bob] FROM WINDOWS WITH DEFAULT_DATABASE=[E2_3]
GO
USE [E2_3]
GO
CREATE USER [DESKTOP-EBE2QHC\Bob] FOR LOGIN [DESKTOP-EBE2QHC\Bob]
GO
USE [E2_3]
GO
ALTER ROLE [db_owner] ADD MEMBER [DESKTOP-EBE2QHC\Bob]
GO
```

服务器实例中出现登录名 DESKTOP-EBE2QHC\Bob，E2_3 数据库 db_owner 角色成员列表如下，DESKTOP-EBE2QHC\Bob 成为该数据库管理员：

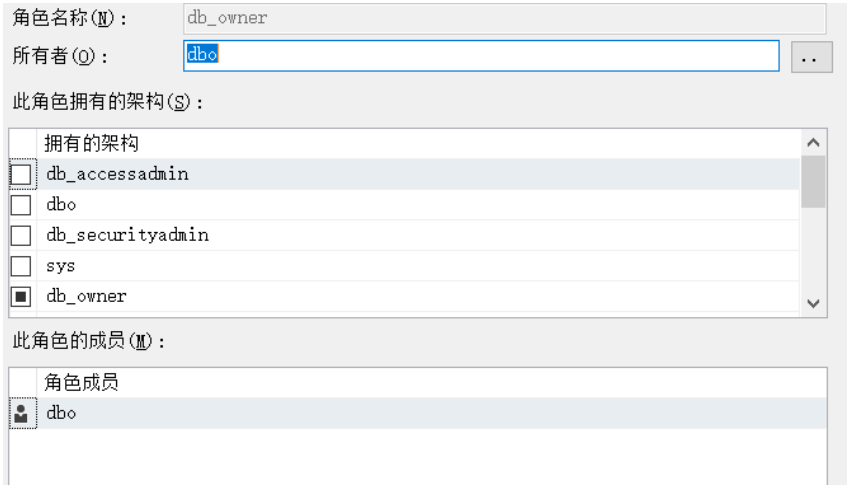


（4） 撤消登录 2 的新创建的数据库的管理员权限。

修改登录名 DESKTOP-EBE2QHC\Bob 的属性，对其映射到 E2_3 数据库的用户 DESKTOP-EBE2QHC\Bob 移除其 db_owner 角色，实现命令代码如下：

```
USE [E2_3]
GO
ALTER ROLE [db_owner] DROP MEMBER [DESKTOP-EBE2QHC\Bob]
GO
```

E2_3 数据库 db_owner 角色成员列表如下，DESKTOP-EBE2QHC\Bob 对该数据库管理员权限移除：



（5） 授权登录 2 查询和更新学生基本信息表中部分字段的权限。验证查询、有权限更新、无权限更新、无权限插入和删除。

使用系统管理员登录名 sa 修改登录名 DESKTOP-EBE2QHC\Bob 映射到 E2_3 数据库的用户 DESKTOP-EBE2QHC\Bob 对安全对象表 dbo.Student 的权限，授予选择查询权限和更新 sname 列的权限，实现命令代码如下：

```
use [E2_3]
GO
GRANT SELECT ON [dbo].[Student] TO [DESKTOP-EBE2QHC\Bob]
GO
use [E2_3]
GO
GRANT UPDATE ON [dbo].[Student] ([sname]) TO [DESKTOP-EBE2QHC\Bob]
GO
```

依照设置，此时 E2_3 数据库用户 DESKTOP-EBE2QHC\Bob 对数据库 E2_3 中表 Student 具有选择查询权限、列 sname 更新权限，接下来开始权限验证。

验证选择查询权限，代码如下：

```
USE E2_3
GO
select * from Student
GO
```

查询成功，结果如下：

结果 消息

	sno	sname	ssex
1	1001	张三	男
2	1002	李四	女
3	1003	王五	男
4	1004	赵六	女
5	1005	孙七	男

因为登录 DESKTOP-EBE2QHC\Bob 在数据库 E2_3 中映射到用户 DESKTOP-EBE2QHC\Bob，而用户具有对数据库 E2_3 表 Student 选择权限，所以能够查询该表。

验证有权限更新，代码如下：

```
USE E2_3
GO
update Student set sname='周八' where sno='1001'
Go
select * from Student
GO
```

更新成功，结果如下：

结果 消息

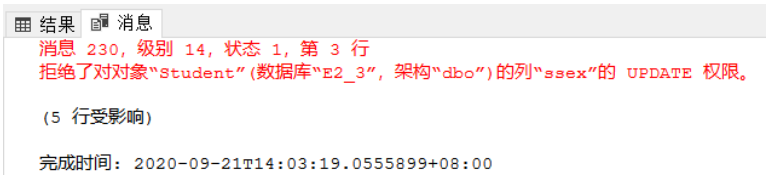
	sno	sname	ssex
1	1001	周八	男
2	1002	李四	女
3	1003	王五	男
4	1004	赵六	女
5	1005	孙七	男

因为登录 DESKTOP-EBE2QHC\Bob 在数据库 E2_3 中映射到用户 DESKTOP-EBE2QHC\Bob，而用户具有对数据库 E2_3 表 Student 中 sname 列更新权限，所以能够更新该表。

验证无权限更新，代码如下：

```
USE E2_3
GO
update Student set ssex='女' where sno='1001'
Go
select * from Student
GO
```

更新失败，返回消息如下：

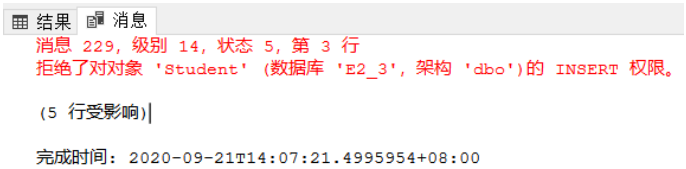


因为登录 DESKTOP-EBE2QHC\Bob 在数据库 E2_3 中映射到用户 DESKTOP-EBE2QHC\Bob，而用户不具有对数据库 E2_3 表 Student 中 ssex 列更新权限，所以不能更新该表。

验证无权限插入，代码如下：

```
USE E2_3
GO
insert into Student(sno,sname,ssex) values ('1006','吴九','女')
Go
select * from Student
GO
```

插入失败，返回消息如下：

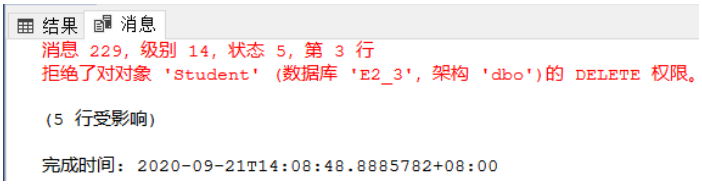


因为登录 DESKTOP-EBE2QHC\Bob 在数据库 E2_3 中映射到用户 DESKTOP-EBE2QHC\Bob，而用户不具有对数据库 E2_3 表 Student 插入权限，所以不能对该表插入记录。

验证无权限删除，代码如下：

```
USE E2_3
GO
delete from Student where sno='1001'
Go
select * from Student
GO
```

删除失败，返回消息如下：

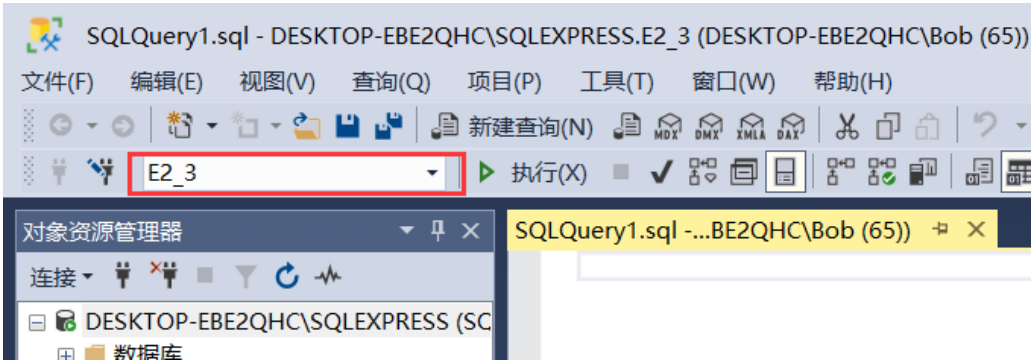


因为登录 DESKTOP-EBE2QHC\Bob 在数据库 E2_3 中映射到用户 DESKTOP-EBE2QHC\Bob，而用户不具有对数据库 E2_3 表 Student 删除权限，所以不能对该表删除记录。

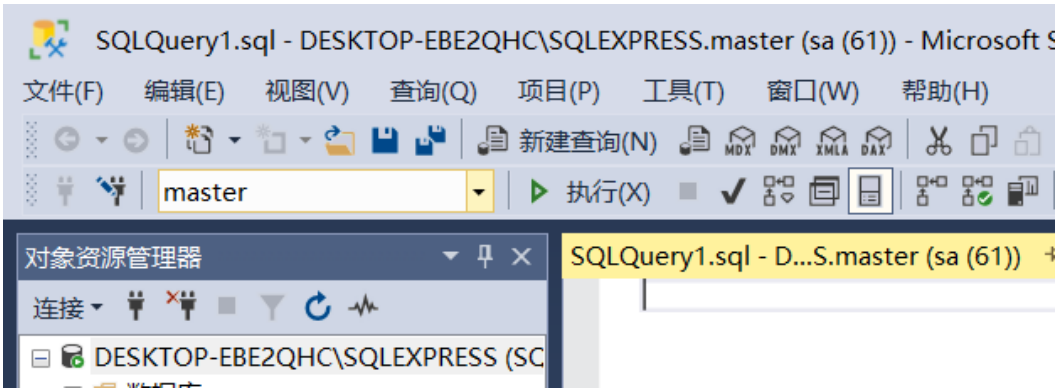
3. 问题回答

（1） 简述什么是默认数据库并用实验结果说明不同的默认数据库在登录到数据库服务器后有什么不同。

默认数据库由登录名定义设置，即登录名连接后操作的数据库。在登录名连接到 SQL 服务器后，若不显式使用 USE 语句，则其定义的默认数据库将成为当前数据库，即查询语句等执行的对象。
比如登录 DESKTOP-EBE2QHC\Bob 的默认数据库设为 E2_3，在连接服务器后，如下图所示



红线框选部分即为当前数据库名，连接服务器后当前数据库即为登录名设置的默认数据库 E2_3。
而登录名 sa 设置的默认数据库为 master，故连接服务器后当前数据库为 master



(2) 说明实验内容（2)、(3)、(5）中所用的授权方法的差异，简述每种方法的优缺点。

（2）中所用方法是修改登录名的服务器角色集，将登录名添加到服务器 sysadmin 角色中，授予该登录名数据库系统管理员的权限。
（3）中所用方法是将登录名映射到某一数据库的用户添加到该数据库的 db_owner 数据库成员列表中，该用户便继承了 db_owner 的所有权限，登录名又继承了该用户的所有权限，则该登录名授权为了该数据库的管理员。
（5）中所用方法是对登录名映射到某一数据库的用户对特定对象授权，登录名继承了该用户的所有权限，则该登录名具有了对该数据库某些特定对象的部分权限。

（2）的优点是操作简单，但被授权的登录名获取了对整个 SQL 系统任意操作的权限，可能造成很大的安全问题。
（3）的优点是操作相对简单，但被授权的登录名获取了对数据库任意操作的权限，可能造成安全问题，只适合对少部分登录名做此类授权。
（5）的优点是授权相对严格，授予的权限细化，适合给不同类的用户做授予不同权限，数据库安全相对有保障，但操作相对复杂。