实验7 数据库的安全性

一、实验目的

- 1. 掌握 Windows 登录名和 SQL Server 登录名的建立与删除方法;
- 2. 掌握创建和管理数据库用户的方法;
- 3. 掌握数据库用户权限的授予、撤销等方法;
- 4. 了解数据库角色的分类、作用及使用方法。

二、实验环境

1. 硬件

每位学生配备计算机一台。

2. 软件

Windows Server 2003 操作系统,安装 SQL Server 2008 企业版软件。

3. 网络

局域网环境

- 4. 工具
- 无

三、实验理论与预备知识

- 1. SQL Server 的身份验证模式;
- 2. SQL Server2008 的安全性机制;
- 3. 创建和管理数据库用户的方法;
- 4. 命令方式授予、撤销权限的语法格式。

四、实验任务

- 1. 管理数据库用户;
- 2. 服务器角色应用;
- 3. 数据库权限管理。

五、实验内容及步骤

- (一) 数据库用户的管理
- 1. 创建 Windows 登录名

(1) 以管理员身份登录到 Windows,选择【开始】→【控制面板】→【管理工具】→【计算
 机管理】,进入【计算机管理窗口】,如图 7.1 所示;

			新用户	
★ 计算机管理 文件(E) 操作(A) 查看(V) 報 ◆ ● ● ●	助(出) 名称 》 系统工具 译存储 》 服务和应用程序	×	用户名 (U): 全名 (2): 描述 (U): 一 密码 (2): 确认密码 (C): 用户下次登录 同用户不能更改 密码永不过期 一 帐户已禁用 (2	thang thang thang ●●●●●●●● ●●●●●●●● 御辺須更改密码 (W) 変密码 (S) 周(W) B)
			帮助创	创建(2) 关闭(2)

图 7.1 计算机管理窗口

图 7.2 创建新用户

(2) 在该窗口中选择【系统工具】→【本地用户和组】→【用户】,右击后,在弹出的快捷菜 单中选择【新用户】,打开【新用户】窗口,新建用户"zhang",密码为"password",并取消"用户 下次登录时需更改密码"选项,单击【创建】按钮创建该用户,如图 7.2 所示;

(3) 以管理员身份登录到 SQL Server Management Studio,在对象资源管理器中选择【安全性】 →【登录名】,右击后,在弹出的快捷菜单中选择【新建登录名】,如图 7.3 所示。在【新建登录名】 窗口中单击【搜索】按钮,在弹出的【选择用户或组】窗口中单击【高级】→【立即查找】,将【搜 索结果】中的用户名"zhang"添加为登录名。选择【Windows 身份验证模式】,单击【确定】按钮 完成创建,如图 7.4、7.5 所示。

½ Microsoft SQL Server Management Studio	选择用户或组	8 ×
文件の 単構成 登録の 構成の 正月 (2000 社区(2 単物化) ・ 新建造物(2000 中) 10 10 10 10 10 10 10 10 10 10 10 10 10	 法择此对象类型(S): 用户或内置安全主体 查找位置(E): LEXOVO-PC 输入要选择的对象名称(例如)(E): 	对象类型 (0)) (位置 (L))
A Information A Infor		检查名称①
▲ 50 ● ■ 路务器角色 ● ■ 党集 で ■ 加密提供程序	高级 (4) 确定	取消



图 7.4 选择用户或组

选择用户或组	? ×			
选择此对象类型(2): 用户或内置安全主体	对象类型 (0)	3 登录名 - 新建		F Addice Address Address
查扶位置(2): LENOVO-FC 一般性查询 名称(4): 起脑为 ~ 描述(2): 起脑为 ~ 描述(2): 起脑为 ~ 算用的帐户(2) 不过期密码(2): 自上次登录后的天数(2): ~	(位置 U) 列 C) う即宣执 O) 停止 C)	送择页	 ○ 純本 ▼ ○ 帮助 ※ 新助 ※ Windows 身份验证(1) ③ SQL Server 身份验证(2) ※ 密码(2): · 補法密码(2): · 描述由密码(1): · 旧密码(2): 	zhao S) ••••••
按索结果 ①: 名称 (GDB) 所在文件夹 Addministr LENOVO-PC ANDFWONG Authentic Authentic CREATOR G CREATOR G CREATOR G CREATOR D	· 确定 取消 · E	连接	 ○ 建制灰箱密封续器 ● 温利密码过期(2) ● 用户在下太登录时处 ● 映射到非对称密钥(2) ● 映射到非对称密钥(2) ● 映射到洋湖(2) ● 映射到凭据(2) ● 映射到汽流器 	D) (须更改密码 (U) (二) (注::::::::::::::::::::::::::::::::::::
Guest LENOVO-PC	-			

图 7.5 选择用户或组

图 7.6 新建登录名

2. 创建 SQL Server 登录名

在对象资源管理器中单击【安全性】→【登录名】,右击后,在弹出的快捷菜单中选择【新建登录名】,在【新建登录名】窗口中输入需创建的登录名"zhao",并选择【SQL Server 身份验证模式】,设置密码为"123456",取消"用户下次登录时需更改密码"选项,单击【确定】按钮完成 SQL Server 登录名创建,如图 7.6 所示。

3. 创建数据库用户

在对象资源管理器中单击【数据库】→【Stu】→【安全性】→【用户】,右击后,在弹出的快 捷菜单中选择【新建用户】菜单项,在【数据库用户】窗口中输入需要新建的数据库用户的用户名 "zhao",输入登录名"zhao",【默认架构】为"dbo",单击【确定】按钮,完成创建,如图 7.7 所 示。

数据库用户·新建	2	Autors Autors Autors Autors	
选择页	🔜 脚本 🝷 🌄 帮助		
☆ 常規 愛 安全対象 愛 扩展属性	用户名 (1):	zhao	
and the second	◎ 發景名(L):	zhao	
	() (汗水を除た):		
	0 200 E		
	 一 五部444 (4) (1) (2) (3) (4) (5) (5) (6) (7) (7) (7) (8) (9) (9) (1) (
	數认架构 (L):	db-o	
	此用户拥有的限构 (0):		
	拥有的架构		*
	db_accessadain		_
	db_backup-perator		1
	db.datewriter		
	db_ddladmin		
	🔲 db_denydatar eader		
连接	db_danydatasriter		-
服务器: (Local)	数据库角色成员身份 图:		
连摘:	角色成员		*
lenovo-FC\lenovo	db_accessadain		_
····································	db_backupoperator		
	db_datareader		E
进度	di dilakin		
一 数绪	db_denordatar eader		
New Y	db_denydataeriter		
	d owner		-

ABIG IF IF • DE BID # R BRS BADE Frag De Frag De Frag Babe # RSB BADE Frag De Frag De Frag Babe BRS BADE Frag De Frag Babe # RSB BADE Frag De Frag Babe BRS BADE Babe # RSB BADE Frag De Frag Babe BRS BADE Babe # RSB BADE Frag De Frag Babe BRS BADE Babe # RSB BADE Frag De Frag Babe BRSB BADE Babe # RSB BADE Frag De Frag Babe BRSB BADE Babe # RSB BADE Frag De Frag Babe BRSB BADE Babe # RSB BADE Babe BRSB BADE Babe # RSB BADE Babe BRSB BADE Babe	Britis E . lenovo - C denovo		
MR MR <t< th=""><th>連择页 </th><th>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</th><th></th></t<>	連择页 	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	
BR Bala O: Brancie Brancie <td>用户映射 安全对象</td> <td>服务嘉角色用于向用户授予服务基范围内的安全特权。</td> <td></td>	用户映射 安全对象	服务嘉角色用于向用户授予服务基范围内的安全特权。	
		服务器角色 (2):	
Same Same		distanti di stato di	
tan Sam Sam Sam Sam Sam Sam Sam Sam		precessadnin V public	
Xinguakia ✓ vryuskia ✓ vryuskia ✓ vryuskia ✓ ✓ vryuskia ✓		securi tyadain.	
Sime 2 synchrin Sime Sime Sime Sime Sime Sime		netupadain.	
		V synadnin	
tim Bing Jam Kilam g Sassagat sa			
 要認 要認 調査 要求 の 数項 			
在 日の円 二 注意: 一 第 二 二 二 二 二 二 二 二 二 二 二 二 二			
6월			
5753 jimerr FC1 Game 57 55.15521 mm 60 505 mm	连接		
38 55 55 55 55 55 55 55 55 55 55 55 55 55	勝方器: (Local)		
80 261921	進接: lenovo-FC\lenovo		
8# 0 8/2	劉 宣后注拍置性		
O 800	进度		
	O ##		
減定 取消		福宝	取消

图 7.8 设置服务器角色

(二) 服务器角色应用

1. 添加固定服务器角色成员

以系统管理员身份登录 SQL Server,单击【安全性】→【登录名】→【zhao】,右击后,在弹出 的快捷菜单中选择【属性】,在弹出的【登录名属性】窗口中选择【服务器角色】选项卡,选择要添 加到的服务器角色,单击【确定】按钮完成添加,如图 7.8 所示。

2. 添加固定数据库角色成员

以系统管理员身份登录 SQL Server,单击【数据库】→【Stu】→【安全性】→【角色】→【数 据库角色】→【db_owner】,右击后,在弹出的快捷菜单中选择【属性】,打开【数据库角色属性】 窗口,如图 7.9 所示。单击【添加】按钮,打开【选择数据库用户或角色】窗口,单击【浏览】按 钮,在打开的【查找对象】窗口中为该固定数据库角色添加成员,如图7.10所示。

选择页	三〇四本 - 〇茶助						
常展展性							
	角色名称(图)	db_owner					
	所有者(0):	de		and a second			
	此角色拥有的架构	g):					
	拥有的架构			-	🥭 查找对:	象	
	da_accessade	in					-
	E &o						
	db_security	dnin			状型は3	个匹配的法类开始动力会	
	ab_owner	rator			120329 5	I EERONAA EERONISK	1
	db_ddladain						
	此角色的成员 图)				匹置的汉	據(11):	
	角色成员					名称	
	dia dia					[mest]	
连接						C con 2	
服务器						[public]	
(Lister)					🛛 🔽 🥭	[zhao]	
這指: lenovo-FC'lenovo					5		
·····································							
St. Martinett							
通度							
一 就線							
0			() (1) (1) (1) (1) (1) (1) (1) (1) (1) ((B); (D)			
			28/02	取消			

图 7.10	添加固	定数据	库角	色成	员
--------	-----	-----	----	----	---

确定 取消

X

类型

用户

用户

数据库角色

帮助

3. 创建自定义数据库角色

以系统管理员身份登录 SQL Server,在对象资源管理器中单击【数据库】→【Stu】→【安全性】 →【角色】→【数据库角色】, 右击后, 在弹出的快捷菜单中选择【新建数据库角色】, 在弹出的【数 据库角色-新建】窗口中输入要创建的角色名"Role",所有者设为"dbo",单击【确定】按钮,完 成创建,如图 7.11 所示。

图 7.9 数据库角色属性

			J 数据库属性 - PXSCJ	0 00 X 11	7 Autoca Autoca	NUMBER AN	BI NECC	- C -X-
			选择页	◎○ 即本 ▼ ○○ 款助				
● 数価率角色 - 新建 務務政 ● 電報 ● 学校30余 ● 学校30余 ● 学校30余	● 単本 ◆ ● 新助 角色生体 ①: 所有者 ②: 此角色原約5時約(⑤): 原約5時約 角。4.cccrtabia の。	balt Bar Bar Transformer Bar	学家院 学文科書 学文科書 学校開始 学校開始 学校開始 学校開始 学校開始 学校開始 学校開始 学校 学校 学校 学校 学校 学校 学校 学校 学校 学校 学校 学校 学校	○○日本 ● □ 1000 原告書名本(1): 原告書名書(2): 原告書名本(2): 月二月二月二日(1): 氏年 ① 100: ① 100: ① 100: ○ 100:<	LHNY9-FC FESCJ			趙东① 3
	db_securityadai	a	连接	zhao 的初課(D):				
	db_owner		服务器;	显式 有效				
	db_backupoperat	or.	(Local)	权限	授权者	授予	具有授予权限	拒绝 ^
	dh ddladain		连接:	音份日志	dbo		1	
		Ψ	Lenovo-FU/Lenovo	音份數据库	dbo			
	此角色的成员(M):		· 查看连接屬性	描入	dbo			
				查看定义	dbo		E.	
	論色成局		进度	查看数据库状态	dbo			
	710000		ALISE	创建 XML 架构集合	dbo		1	
			() ^{就结}	创建表	dbo	V		8
连接			10 a g 4	包建程序集	dbo			
an to 98.								
助方面: (Local) 连接:							確定	取消

图 7.11 创建自定义数据库角色

图 7.12 数据库级别授权

(三) 数据库权限管理

1. 授予数据库权限

通过界面方式和 SQL 命令两种方式实现数据库权限的授予。

(1) 授予数据库用户 Stu 数据库上的 CREATE TABLE 权限。

以系统管理员的身份登录到 SQL Server,在对象资源管理器中右击数据库"Stu",在弹出的快捷菜单中选择【属性】,打开【数据库属性】窗口,选择【权限】选项页,选择数据库用户"zhao",在下方的权限列表中,单击【创建表】对应【授予】列中的复选框,单击【确定】按钮,完成数据库级别上的权限授予,如图 7.12 所示。

(2) 授予数据库用户在 Stu 数据库中 student 表上的 SELECT、INSERT、DELETE 权限。

以系统管理员的身份登录到 SQL Server,在对象资源管理器中单击【数据库】→【Stu】→【表】 →【dbo.student】,右击后,在弹出的快捷菜单中选择【属性】,打开【表属性】窗口,选择【权限】 选择页,单击【搜索】按钮,打开【选择数据库用户或角色】窗口,单击【浏览】按钮,选择要授 权的用户或角色,然后在权限列表中选择要授予的权限。

2. 撤销数据库权限

- (1) 以命令方式撤销已授予用户的 CREATE TABLE 权限;
- (2) 以命令方式撤销对用户授予的在 student 表上的 SELECT 权限。

六、实验分析

- 使用用户 "zhang" 登录 Windows, 启动 SQL Server Management Studio, 以 Windows 身份 验证模式连接, 与以系统管理员身份登录有何不同?
- 2. 如何在对象资源管理器中删除数据库角色成员 Role? 请试一试。
- 3. 通过命令方式,如何撤销授予多个用户的多个语句权限?请举例说明。

七、课外自主实验

以系统管理员身份登录到 SQL Server 服务器,以 Stu 数据库为例,在 SQL Server2008 界面中实现下列操作。

- 1. 在数据库 Stu 中创建用户 stu1、stu2 和 stu3,登录帐号分别为 stu1、stu2 和 stu3;
- 2. 给数据库用户 stu1 赋予对 sc 表进行 INSERT、UPDATE、DELETE 操作权限;
- 给数据库用户 stu2 和 stu3 赋予对 student 表、course 表所有操作权限及查询 sc 的操作权限, 并允许再授权给其他用户;
- 4. 收回数据库用户 stu2 对 student 表和 course 表的 DELETE 操作的权限;
- 5. 创建数据库角色 Role1,并授予其在 student 表上拥有 SELECT 权限;
- 6. 添加用户 stu1 为 Role1 的成员;
- 八、实验扩展资源
 - 1. 图书

(1)郑阿奇.SQL Server 实用教程(第3版)(SQL Server 2008 版)[M].电子工业出版社,2009.

(2) 闪四清.SQL Server 2008 基础教程 [M]. 清华大学出版社,2010.

2. 期刊论文

无

3. 在线学习平台

无

- 4. 其他资源
 - (1) http://msdn.microsoft.com/zh-cn/sqlserver
 - (2) http://bbs.csdn.net/