第 5 章　数据库系统安全技术

➢ **本章课前准备**

学习本章内容之前，需要准备如下知识：

- 了解数据库系统安全的重要意义；
- 查找数据库系统受到侵害的案例；
- 了解数据库系统安全的相关技术。

➢ **本章教学目标**

本章的教学目标是：

- 了解数据库系统安全的重要意义；
- 掌握数据库系统安全设置的常规方法；
- 掌握数据库备份及还原相关技术。

➢ **本章教学要点**

本章的教学要点包括：

- 数据库系统安全设置技术；
- 数据库系统常见攻击原理及操作；
- 数据库系统加固策略。

➢ **本章教学建议**

本章内容采用案例引导模式进行教学。

5.1　数据库系统安全概述

数据库安全问题是信息系统安全问题的一个子问题，数据库技术是构建信息系统的核心技术。在当今开放式的互联网时代，许多关键的业务系统运行在数据库平台上，数据库系统中的数据为众多用户所共享，如果数据库安全无法保证，其上的应用系统也会被非法访问或破坏。近年来，基于 Web 的应用程序和信息系统迅速增加，使得数据库的数据受到黑客的攻击和篡改的风险进一步增加，造成的损失也越来越大，数据库系统的安全正变得越来越重要。

5.1.1　数据库安全定义

数据库安全的核心是数据的安全。数据安全是指防止数据信息被故意或偶然的非授

权泄露、更改、破坏或使用数据信息被非法的系统控制，以确保数据的完整性、保密性、可用性、可控性和可审查型。

数据库安全是指数据库的任何部分都不允许受到恶意侵害或未经授权的存取或修改。数据库管理系统安全性保护是通过各种防范措施，以防止用户越权使用数据库。数据库系统中一般采用用户标识和鉴别、存取控制、视图以及密码存储等技术进行安全控制。

5.1.2　数据库管理系统的安全机制

数据库管理系统负责管理大量的业务数据，保证其业务数据的安全是最重要的任务。一般大型数据库管理系统都会提供强大的安全机制来保证数据的安全。我们以 SQL Server 2008 为例来认识数据库管理系统的安全机制。

SQL Server 2008 的安全性管理分为三个等级：操作系统级、SQL Server 级和数据库级。

1. 操作系统级的安全性

用户使用客户机通过网络实现对 SQL Server 服务器访问时，首先要获得操作系统的使用权。SQL 可以直接访问网络端口，对 Windows 安全体系外的服务器及其数据库的访问。由于 SQL 采用了集成 Windows 网络安全性机制，使得 OS 安全性提高。

2. SQL Server 级的安全性

这个级别的安全性主要通过登录账户进行控制，要想访问一个数据库服务器，必须拥有一个登录账户。登录账户可以是 Windows 账户或组，也可以是 SQL Server 的登录账户。用户登录时提供的登录账号和口令决定了用户能否获得 SQL Server 的访问权及其登录后拥有的具体访问权限。

3. 数据库级的安全性

用户通过 SQL Server 级的服务器安全性的检验后，要访问数据库对象，还要进行数据库级的安全检验。这个级别的安全性主要通过用户账户进行控制，要想访问一个数据库，必须拥有该数据库的一个用户账户身份。用户账户是通过登录账户进行映射的，可以属于固定的数据库角色或自定义数据库角色。

5.2　SQL Server 常规安全设置

5.2.1　创建登录账户

SQL Server 提供了两种确认用户账户：Windows 登录账号和 SQL Server 登录账号。Windows 登录账号是由 Windows 服务器来对登录的账号进行身份验证，支持 Windows 操作系统的密码策略，账号和密码保存在 Windows 操作系统的账户数据库中。SQL Server 登录账号是 SQL Server 自身负责验证身份的登录账号。当使用 SQL Server

登录账号和口令连接 SQL Server 服务器时，由 SQL Server 验证该用户是否存在，且其口令是否与记录的口令匹配，如图 5.1 所示。

图 5.1 SQL Server 2005 身份验证界面

1. Windows 登录账号的创建

任务：为 SQL Server 2005 创建名为 DBSecurity 的 Windows 登录账户。

(1) 在 Windows 中创建一个名为 DBSecurity 的用户，如图 5.2 所示。

图 5.2 创建一个 Windows 用户

(2) 使用有 sysadmin 角色权限的用户登录“SQL Server 管理控制台”，简称 SSMS。

(3) 在“对象资源管理器”中依次展开“安全性”节点。右击“登录名”在弹出的快捷菜单中单击“新建登录名”，弹出“登录名—新建”对话框，如图 5.3 和图 5.4 所示。

(3) 选择“Windows 身份验证”，单击“搜索”按钮，打开“选择用户或组”对话框，如图 5.5 所示。

(4) 在“输入要选择的对象名称”文本框中输入 DBSecurity，单击“检查名称”按钮检查名称无误后，单击“确定”返回，如图 5.6 所示。

(5) 返回“登录名—新建”对话框，单击“确定”按钮完成登录名的创建。展开登录名节点，可查看新创建的 DBSecurity 账号，如图 5.7 所示。

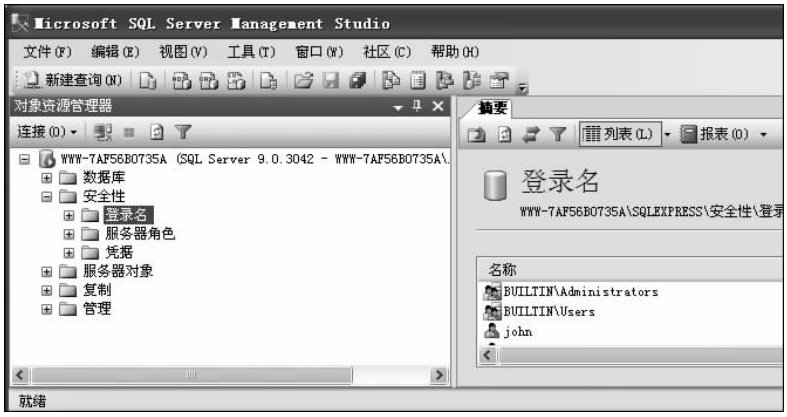

图 5.3　登录名节点

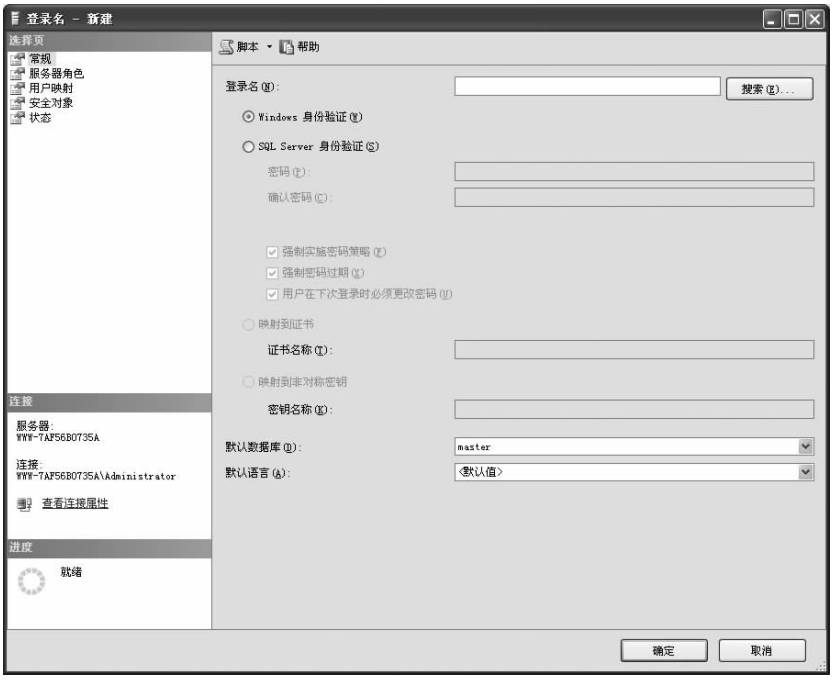

图 5.4　新建登录名对话框

图 5.5　选择 Windows 用户对话框

图 5.6 输入 Windows 用户名

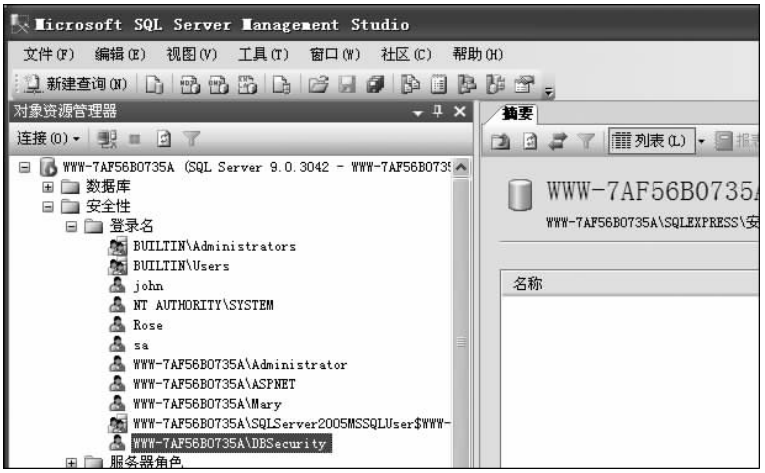

图 5.7 新创建的 Windows 登录账号

2. SQL Server 登录账号的创建

任务：为 SQL Server 2005 创建名为 Security 的 SQL Server 登录账户。

(1) 在“对象资源管理器”中依次展开“安全性”节点。右击“登录名”在弹出的快捷菜单中单击“新建登录名”，弹出“登录名—新建”对话框。

(2) 在“登录名—新建”对话框中选择“SQL Server 身份验证”选项，在“登录名”文本框中输入 Security，在“密码”和“确认密码”文本框中输入口令和确认口令，如图 5.8 所示。

(3) 单击“确定”按钮完成登录名的创建。

3. 关于 sa

SQL Server 服务器安装成功后会自动创建一个特殊的登录账户，名为 sa。sa 是 SQL Server 账户，在混合模式情况下，sa 账户自动启用。sa 拥有最高管理权限，可执行服务器范围内的所有操作，用户不能更改它的属性，也不能删除它。

5.2.2 创建数据库用户

一个服务器登录账号要访问数据库，必须在这个数据库内有数据库用户与其对应。

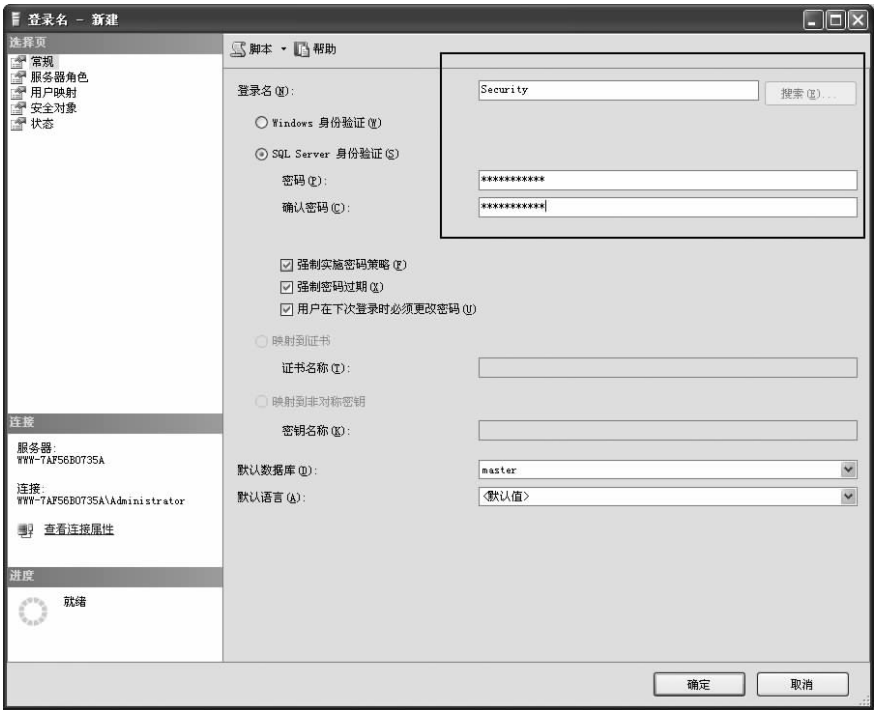

图 5.8　新建 SQL Server 账户界面

每个数据库用户都和服务器登录账户之间存在着一种映射关系。

任务：为 Security 账户在 Exercise 数据库中创建对应的数据库用户 Security。

(1) 使用具有足够操作权限的用户登录 SSMS。

(2) 在“对象资源管理器”中依次展开“数据库”→Exercise→“安全性”→“用户”节点，如图 5.9 所示。

图 5.9　数据库用户节点

(3) 在图 5.10 中的“用户”节点上右击，在弹出的快捷菜单中选择“新建用户”，打开“数据库用户—新建”对话框，如图 5.10 所示。

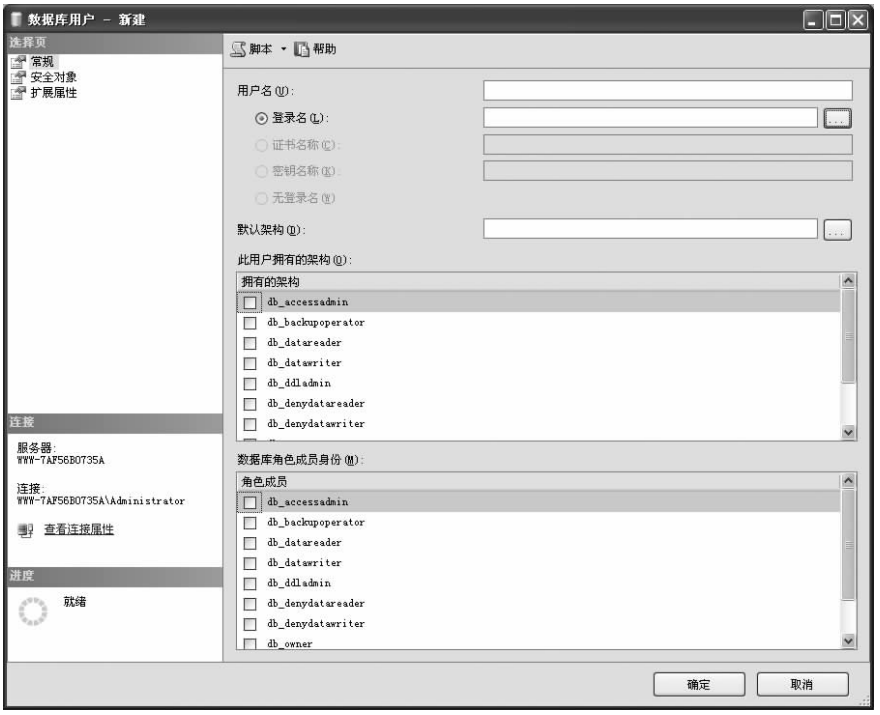

图 5.10 “数据库用户—新建”对话框

(4) 在打开的“数据库用户—新建”对话框中,在“用户名”文本框中输入要创建的数据库用户名 Security(用户名可以与登录名相同),在登录名文本框中输入与该用户名对应的登录账号,也可以通过单击“浏览”按钮来打开“选择登录名”对话框来选择。

(5) 设置好选项后,单击“确定”按钮,完成数据库用户 Security 的创建。

5.2.3 角色管理

角色是一种权限机制,可以方便管理员对用户权限的集中管理,大大减少管理员的工作量。SQL Server 管理者可以将用户设置为某一角色,这样只要对角色进行权限设置便可以实现对所有用户权限的设置。SQL Server 提供服务器角色和数据库角色。

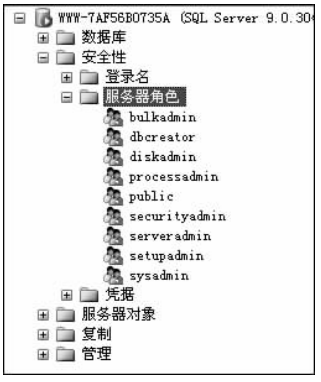

图 5.11 服务器角色

1. 将登录名映射到服务器角色

任务:使用 SSMS 将 Security 映射到服务器角色 sysadmin 中。

(1) 使用具有 sysadmin 角色权限的账户登录到 SSMS,在对象资源管理器中,依次展开“安全性”和“服务器角色”,如图 5.11 所示。

(2) 在 sysadmin 服务器角色上右击,在弹出的快捷菜单中选择“属性”,弹出“服务器角色属性”对话框,如图 5.12

所示。

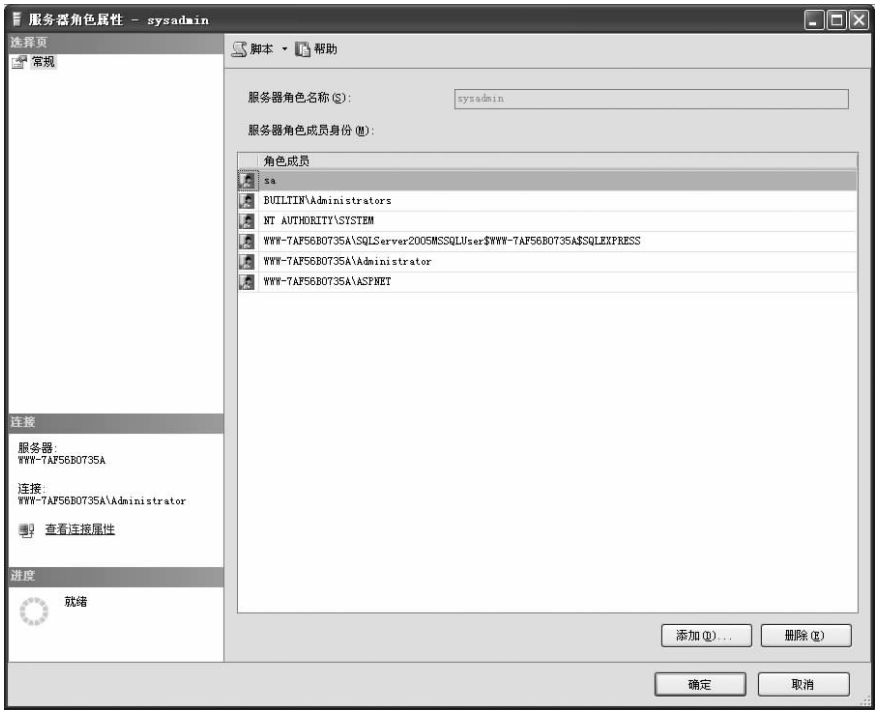

图 5.12　“服务器角色属性”对话框

(3) 在图 5.12 中显示的“服务器角色属性”对话框中单击“添加”按钮,将弹出“选择登录名”对话框,如图 5.13 所示。

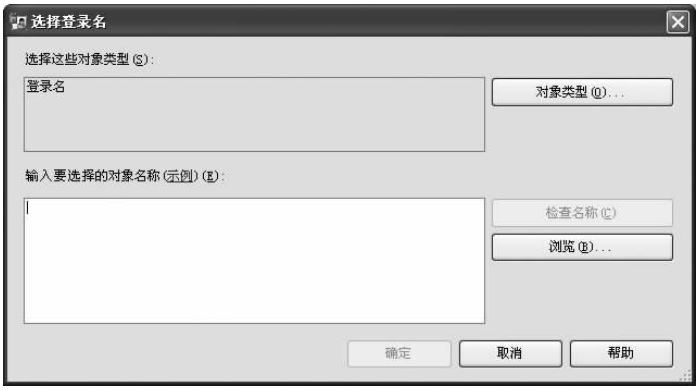

图 5.13　“选择登录名”对话框

(4) 单击“浏览”按钮,会弹出“查找对象”对话框,如图 5.14 所示。选中 Security 登录名前的复选框,单击“按钮”,完成角色映射。

2. 为用户名分配数据库角色

数据库角色是为某一用户或某一组用户授予不同级别的管理或访问数据库以及数据

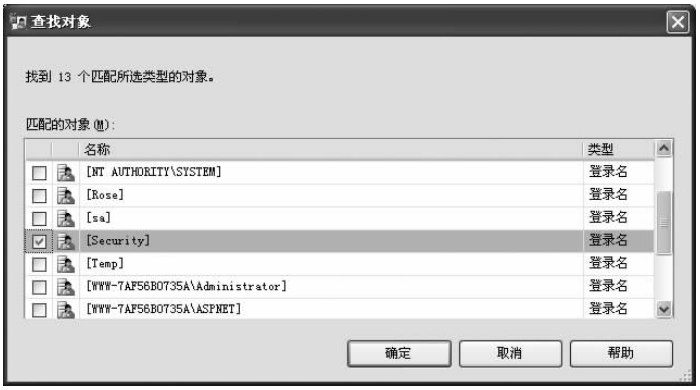

图 5.14 “查找对象”对话框

库对象的权限,这些权限是数据库专有的,并且还可以给一个用户授予属于同一数据库的多个角色。SQL Server 提供了两种数据库角色:固定数据库角色和用户自定义数据库角色。

任务:将数据库用户 Security 添加到 Exercise 数据库的 db_owner 角色中。

(1) 在“对象资源管理器”中依次展开“数据库”→Exercise→“安全性”→“角色”节点→“数据库角色”节点,如图 5.15 所示。

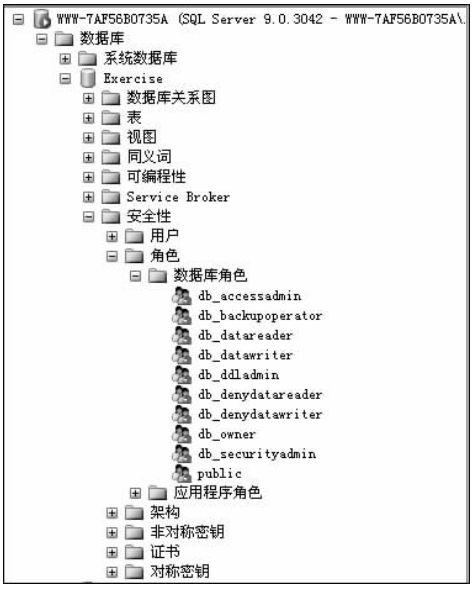

图 5.15 数据库用户角色

(2) 右击 db_owner 角色,在弹出的快捷菜单中选择“属性”选项,打开“数据库角色属性—db_owner”对话框。

(3) 在“数据库角色属性—db_owner”对话框中,单击“添加”按钮,打开“选择数据用户或角色”对话框如图 5.16 所示,单击“浏览”按钮,打开“查找对象”对话框。

图 5.16　“选择数据库用户或角色”对话框

(4) 选择“[Security]”数据库用户,单击“确定”按钮角色指定,如图 5.17 所示。

图 5.17　“ 查找对象”对话框

5.3　数据安全保障——备份及恢复

5.3.1　数据备份简介

数据备份(Data Backup)与恢复是 SQL Server 非常重要的保护功能,是防止意外故障的必备措施。数据备份是指为防止系统出现操作失误或系统故障导致数据丢失,而将全系统或部分数据从应用主机中复制(转存)到其他存储介质上的功能。其目的是为了系统数据崩溃时能够快速地恢复数据,使系统迅速恢复运行。

1. 备份类型

SQL Server 备份一般可分为四种类型:数据库备份、差异备份、事务日志备份及文件和文件组备份。