

国家“十三五”重点出版规划项目
上海高校优秀教材奖获得者主编

上海市高校精品课程
特色教材(立体化新形态)

数据库原理及应用

——基于SQL Server 2016

主编 贾铁军 徐方勤

副主编 邓红霞 戴春妮 王佃来 曹锐

参编 陶维天 张野 降爱莲

 机械工业出版社
CHINA MACHINE PRESS

第8章 数据库基础



第8章 目录

国家十三五重点规划项目
上海市高校精品课程

第8章 目录

- 8.1 数据库安全概念及特点
- 8.2 数据库安全技术和机制
- 8.3 身份验证和访问控制
- 8.4 数据备份及恢复
- 8.5 并发控制和封锁技术
- 8.6 实验八 数据备份及恢复操作
- 8.7 本章小结
- 8.8 练习与实践八(注:网上作业)



上海高校精品课程 www.jiatj.sdju.edu.cn/

教学目标

- 理解数据库安全概念及特点
- 理解数据库安全风险分析
- **掌握**数据库安全关键技术 **重点**
- **掌握**数据库的安全策略和机制
- **掌握**角色、权限管理及完整性控制 **重点**
- **掌握**数据库备份及恢复 **重点**
- 理解并发控制和封锁技术

友情
提示



同步实验(上机)



8.1 数据库安全概念及特点

上海市高校精品课程
国家十三五规划项目

案例8-1

信息技术为社会的进步和发展带来了便利，也带来了许多的安全隐患。数据库安全事件层出不穷：

某系统开发工程师通过互联网入侵移动中心数据库，盗取充值卡；

某医院数据库系统遭到非法入侵，导致上万名患者隐私信息被盗取； ...

8.1.1 数据库安全相关概念

1. 数据库安全

数据库安全（DataBase Security）是指采取各种安全措施对数据库及其相关文件和数据进行保护。



8.1 数据库安全概念及特点

上海市高校精品课程
国家十三五规划项目

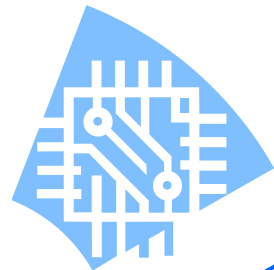
2. 数据库系统安全

数据库系统安全，以各种防范措施防止非授权使用数据库，主要通过DBMS实现的。

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。

数据库系统安全主要利用在**系统级控制**数据库的存取和使用的机制，包含：

- (1) 系统的安全设置及管理，包括法律法规、政策制度、实体安全等；
- (2) 数据库的访问控制和权限管理；
- (3) 用户的资源限制，包括访问、使用、存取、维护与管理等；
- (4) 系统运行安全及用户可执行的系统操作；
- (5) 数据库审计有效性；
- (6) 用户对象可用的磁盘空间及数量。



8.1 数据库安全概念及特点

上海市高校精品课程
国家十三五规划项目

3. 数据安全

数据库安全的核心和关键是其数据安全。

数据安全是指以保护措施确保数据的完整性、保密性、可用性、可控性和可审查性。

主要通过**实施对象级控制**数据库的访问、存取、加密、使用、应急处理和审计等机制，包括用户可存取指定的模式对象及在对象上允许作具体操作类型等。



8.1 数据库安全概念及特点

上海市高校精品课程
国家十三五规划项目

8.1.2 数据库安全风险分析

主要表现在以下三个层面：

管理层面：主要表现为人员的职责、流程有待完善，内部员工的日常操作有待规范，第三方维护人员的操作监控失效等等，致使安全事件发生时，无法追溯并定位真实的操作者。

技术层面：现有的数据库内部操作不明，无法通过外部的任何安全工具(比如：防火墙、IDS、IPS等)来阻止内部用户的恶意操作、滥用资源和泄露企业机密信息等行为。

审计层面：现有的依赖于数据库日志文件的审计方法，存在诸多的弊端，比如：数据库审计功能的开启会影响数据库本身的性能、数据库日志文件本身存在被篡改的风险，难于体现审计信息的真实性。



8.1 数据库安全概念及特点

上海市高校精品课程
国家十三五规划项目

常见数据库的安全缺陷和隐患要素，主要包括：

- (1) 数据库应用程序的研发、管理和维护等人为因素的疏忽；
- (2) 用户对数据库安全的忽视，安全设置和管理失当；
- (3) 部分数据库机制威胁网络低层安全；
- (4) 系统安全特性自身存在的缺陷；
- (5) 数据库账号、密码容易泄漏和破译；
- (6) 操作系统后门及漏洞隐患；
- (7) 网络协议、病毒及运行环境等其它威胁。

📖 讨论思考

常见数据库的安全缺陷和隐患要素，主要包括哪些？



8.2数据库安全技术和机制

上海市高校精品课程
国家十三五规划项目

案例8-2

数据库的一大特点是数据可以共享，但数据共享必然带来数据库的安全性问题，而数据库系统中的数据共享不能是无条件的共享。

比如：新产品实验数据、市场营销策略、销售计划、医疗档案、银行储蓄数据等。

所以说，数据库中数据的共享是在DBMS统一的严格的控制之下的共享，即只允许有合法使用权限的用户访问允许他存取的数据，因此，数据库系统的安全保护措施是否有效是数据库系统主要的性能指标之一。

8.2.1 数据库安全关键技术

常用的数据库安全关键技术包括三大类：

注意

- (1) **预防保护类**。主要包括身份认证、访问管理、加密、防恶意代码、防御和加固。
- (2) **检测跟踪类**。主体对客体的访问行为需要进行监控和事件审计，防止在访问过程中可能产生的安全事故的各种举措，包括监控和审核跟踪。
- (3) **响应恢复类**。网络或数据一旦发生安全事件，应确保在最短的时间内对其事件进行应急响应和备份恢复，尽快将其影响降至最低。

8.2.1 数据库安全关键技术

常用8种数据库安全关键技术：

注意

- 1) 身份认证 (Identity and Authentication)
- 2) 访问管理 (Access Management)
- 3) 加密 (Cryptography)
- 4) 防恶意代码 (Anti-Mali code)
- 5) 加固 (Hardening)
- 6) 监控 (Monitoring)
- 7) 审核跟踪 (Audit Trail)
- 8) 备份恢复 (Backup and Recovery)



8.2.2 数据库的安全策略和机制

1. SQL Server的安全策略

- (1) 管理规章制度方面的安全性
- (2) 数据库服务器物理方面的安全性
- (3) 数据库服务器逻辑方面的安全性



2. SQL Server的安全管理机制

SQL Server的安全机制对数据库系统的安全极为重要，包括：访问控制与身份认证、存取控制、审计、数据加密、视图机制、特殊数据库的安全规则等。

8.2数据库安全技术和机制

上海市高校精品课程
国家十三五规划项目

SQL Server 2016的安全性管理可分为3个等级：

- (1) 操作系统级的安全性
- (2) **SQL Server**级的安全性
- (3) 数据库级的安全性



注意：

一个用户如果要对某一数据库进行操作，必须满足以下3个条件：

- (1) 登录SQL Server服务器时必须通过操作系统级身份验证；
- (2) 必须是该数据库的用户，或者是某一数据库角色的成员；
- (3) 必须有对数据库对象执行该操作的权限。

讨论思考

常用的数据库安全关键技术包括哪些？



8.3 身份验证和访问控制

上海市高校精品课程
国家十三五规划项目

案例8-3

数据的安全性管理是数据库服务器应实现的重要功能之一。SQL Server 2016数据库采用了非常复杂的安全访问控制措施，其安全管理体现在如下几个方面：

- 1) **对用户登录进行身份验证**。当用户登录到数据库系统时，系统验证该用户账户和口令，包括确认用户账户是否有效以及能否访问数据库系统。
- 2) **对用户进行的操作进行权限控制**。当用户登录到数据库后，只能对数据库中的数据在允许的权限内进行操作。



8.3 身份验证和访问控制

上海市高校精品课程
国家十三五规划项目

8.3.1 身份验证及权限管理

1. 身份验证

身份验证模式是指系统确认用户的方式，身份验证使用登录账号，并只验证该用户连接**SQL Server**实例的能力。

SQL Server 2016中支持两种身份验证模式：

Windows身份验证模式、**SQL Server**身份验证模式。

⚠注意

(1) Windows验证模式

用户登录**Windows**时进行身份验证，登录**SQL Server**时就不再进行身份验证了。

(2) SQL Server验证模式

在**SQL Server**验证模式下，**SQL Server**服务器对要登录的用户进行身份验证。系统管理员必须设定登录验证模式的类型为混合验证模式。

8.3.1 身份验证及权限管理

2. 权限管理概念

权限是进行操作和访问数据的通行证。**SQL**管理者可通过权限保护分层实体集。其实体被称为安全对象，是**SQL**的各种受安全保护控制资源。主体（**Principal**）和安全对象之间是通过权限相关联的，在**SQL**中，主体可以请求系统资源的个体和组合过程。

权限用于管理控制用户对数据库对象的访问，以及指定用户对数据库可执行的操作，用户可以设置服务器和数据库的权限。

主要涉及**3种权限**：服务器权限、数据库对象权限和数据库权限。

8.3 身份验证和访问控制

上海市高校精品课程
国家十三五规划项目

(1) **服务器权限**。允许**DBA**执行管理任务。这些权限定义在固定服务器角色 (**Fixed Server Roles**) 中。这些角色可以分配给登录用户，但不能修改。一般只将服务器权限授给**DBA**，而不需要修改或授权给别的用户登录。服务器的相关权限和配置将在后面介绍。

(2) **数据库对象权限**。数据库对象是授予用户以允许其访问数据库中对象的一类权限，对象权限对于使用**SQL**语句访问表或视图是必须的。

(3) **数据库权限**。用于控制对象访问和语句执行。对象权限使用户可访问存在于数据库中的对象，除此权限外，还可给用户分配数据库权限。

8.3 身份验证和访问控制

上海市高校精品课程
国家十三五规划项目

8.3.2 数据库安全访问控制

SQL Server 2016的安全访问控制包含通过SQL Server身份验证模式进入SQL Server实例，通过SQL Server安全性机制控制对SQL Server 2016数据库及其对象的操作。

1. 登录名管理

登录名管理包括创建登录名、设置密码策略、查看登录名信息、修改和删除登录名。

登录名管理的方法，主要有两种：

(1) 创建登录名

创建登录名操作主要包括：创建基于Windows登录名、创建SQL Server登录名、查看登录名信息。

🔗 参看案例8-4 创建登录名操作

(2) 修改和删除登录名

数据库管理员DBA定期检查SQL Server用户，执行修改或删除登录名。

8.3.2 数据库安全访问控制

2. 监控错误日志

- 用户应时常查看**SQL Server**错误日志。在查看错误日志的内容时，主要应注意在正常情况下不应出现的错误消息。
- 当浏览错误日志时，要特别注意以下的关键字：错误、故障、表崩溃、**16级错误**和严重错误等。
- 查看日志方法有**2种**：利用**SSMS**查看日志，利用文本编辑器查看日志。

3. 记录配置信息

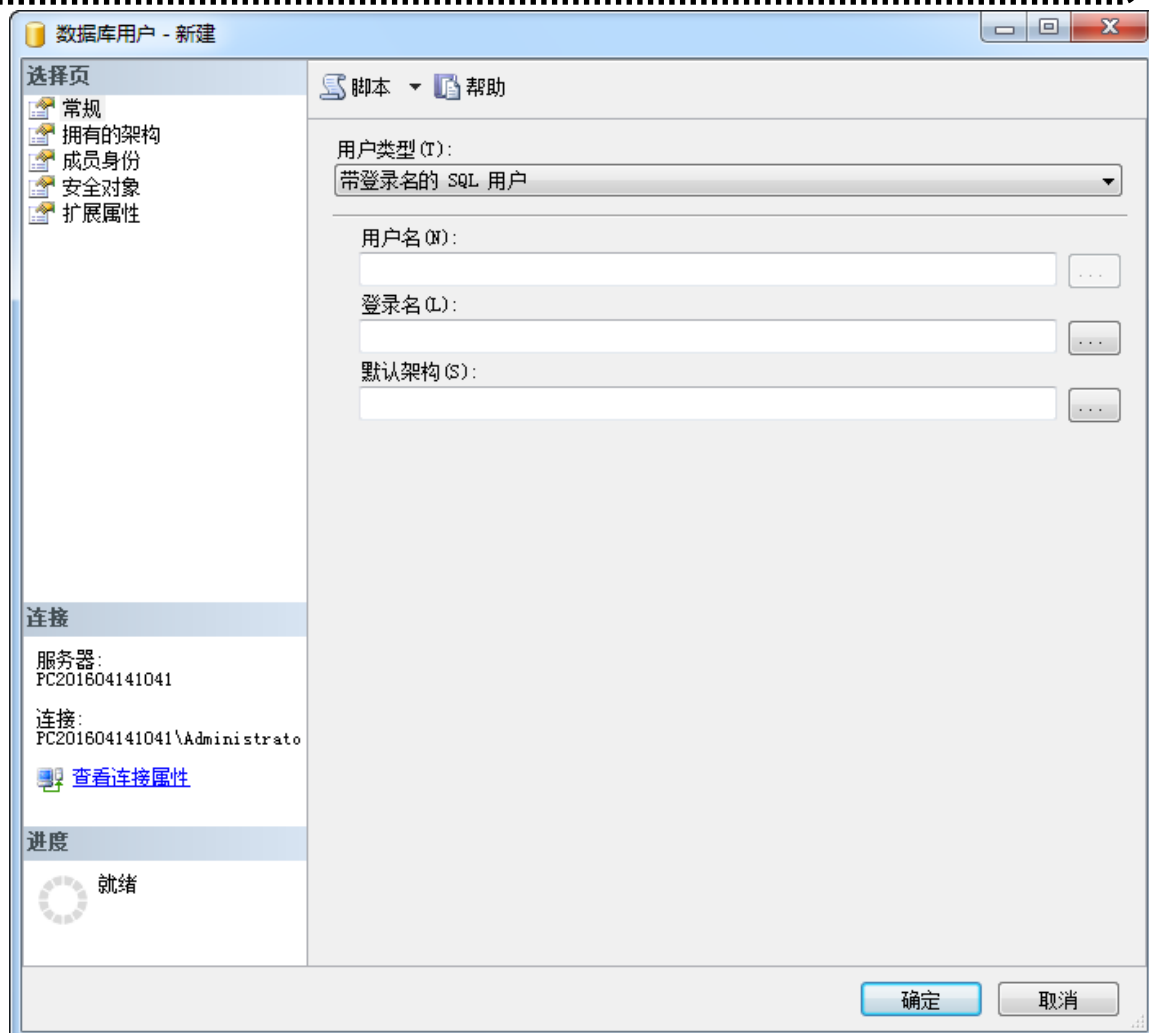
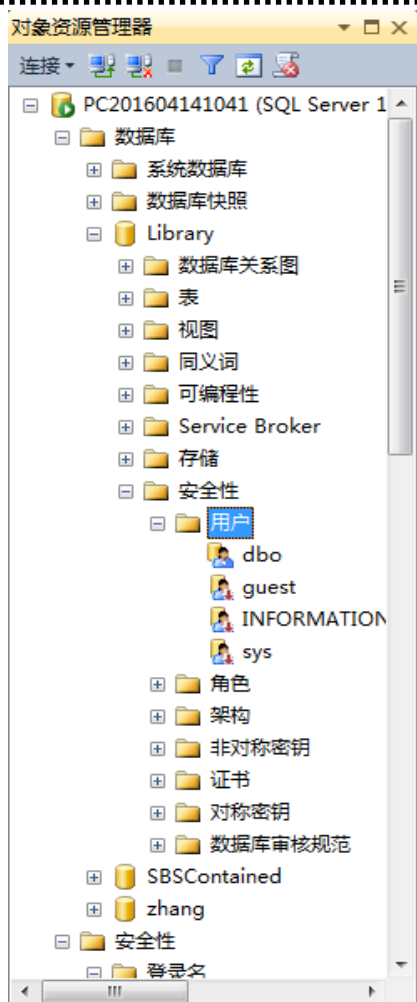
在日常的维护计划中应该安排对配置信息的维护，特别是当配置信息修改时。使用系统过程**Sp_configure**可以生成服务器的配置信息列表。当无法启动**SQL Server**时可借助服务器的配置信息，并恢复服务器的运行。

8.3 身份验证和访问控制

上海市高校精品课程
国家十三五规划项目

8.3.3 用户与角色管理

1. 【案例8-5】使用SSMS创建用户



8.3 身份验证和访问控制

8.3.3 用户与角色管理

2. 角色管理

(1) 角色的概念

- **角色 (Role)** 是具有指定权限的用户 (组)，用于管理数据库访问权限。根据角色自身的设置不同，一个角色可以看作是一个数据库用户或一组用户。角色可以拥有数据库对象 (如表) 并可将这些对象上的权限赋予其它角色，以控制所拥有的具体访问对象的权限。
- **角色分为两类：服务器角色和数据库角色。**此外，SQL Server 2016 中还有一种角色被称为**应用程序角色**。



8.3 身份验证和访问控制

上海市高校精品课程
国家十三五规划项目

8.3.3 用户与角色管理

2. 角色管理

(2) 服务器角色

- 服务器角色也称为“固定服务器角色”，是系统内置的，因为用户不能创建新的服务器级角色。服务器级角色的权限作用域为服务器范围。

🔔 参看案例8-6 用SSMS为用户分配固定服务器角色

- 用户可以向服务器角色中添加SQL Server登录名、Windows账户和Windows组。固定服务器角色的每个成员都可以向其所属角色添加其它登录名。通过给用户分配固定服务器角色，可使用户具有执行管理任务的角色权限。

🔔 参看课本表8-1 固定服务器角色及其服务器级权限描述

(3) 数据库角色 🔔 参看课本表8-2 固定数据库角色

- SQL Server 2016中有两种类型的数据库级角色：数据库中预定义的“固定数据库角色”和可以创建的“用户定义数据库角色”。

🔔 参看案例8-7利用SSMS创建新的数据库角色
利用SQL命令创建新的数据库角色

8.3 身份验证和访问控制

8.3.3 用户与角色管理

2. 角色管理

(4) 应用程序角色



- 应用程序角色是特殊的数据库角色，用于允许用户通过特定应用程序获取特定数据。应用程序角色不包含任何成员，而且在使用它们之前要在当前连接中将它们激活。

讨论思考

用户权限的种类有哪些？各自的作用？



8.4 数据备份及恢复

案例8-9

虽然数据库管理系统采取了各种措施来保证数据库的安全性和完整性，但还是需要防止可能出现的**意外故障**如：存储媒体损坏、用户操作错误、硬件故障或自然灾害等。这些故障会造成运行事务的异常中断，影响数据的正确性，甚至会破坏数据库，使数据库中的数据破坏或丢失。数据的备份与恢复是数据库文件管理中最常见的操作，是最简单的数据恢复方式。

8.4.1 数据备份

- 设计备份策略的指导思想：以最小的代价恢复数据。备份与恢复是相互联系的，备份策略与恢复应结合起来考虑。

1. 备份内容

- **SQL Server**数据库需备份的内容分为**数据文件**（包括主要数据文件和次要数据文件）、**日志文件**两部分。
- 根据每次备份的目标不同，可以将备份分为**数据备份**和**日志备份**。

8.4 数据备份及恢复

8.4.1 数据备份

2. 备份介质

- **备份介质**是指将数据库备份到目标载体，即备份到何处。
- **SQL Server 2016**中，允许使用两种类型的备份介质：
 - (1) 硬盘（备份本地文件、备份网络文件）
 - (2) 磁带（仅可用于备份本地文件）



3. 备份时机

- 对于**系统数据库**和**用户数据库**，备份的时机是不同的。
 - (1) 系统数据库。当系统数据库**Master**、**Msdb**和**Model**中的任何一个被修改以后，都要将其备份。
 - (2) 用户数据库。当创建数据库或加载数据库时，应备份数据库；当为数据库创建索引时，应备份数据库，以便恢复时能够大大节省时间。

8.4 数据备份及恢复

上海市高校精品课程
国家十三五规划项目

8.4.1 数据备份

4. 备份方法

数据库备份常用的两类方法：**完全备份**和**差异备份**。完全备份每次都备份到整个数据库或事务日志，差异备份只备份自上次备份以来发生变化的数据库数据。差异备份也称为增量备份。

数据备份的类型：

- | | | |
|------------|--------------|----------|
| (1) 完整备份 | (2) 完整差异备份 | (3) 部分备份 |
| (4) 部分差异备份 | (5) 文件和文件组备份 | |
| (6) 文件差异备份 | (7) 事务日志备份 | |



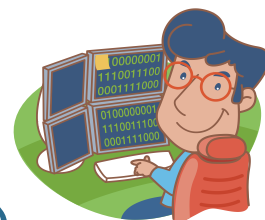
8.4 数据备份及恢复

8.4.1 数据备份

5. 谁做备份

在**SQL Server 2016**中，具有下列角色的成员可以做备份工作：

- (1) 固定服务器角色**Sysadmin**（系统管理员）
- (2) 固定数据库角色**Db_owner**（数据库所有者）
- (3) 固定数据库角色**Db_backupoperator**（允许进行数据库备份的用户）



除上述角色外，还可以通过授权允许其它角色进行数据库备份。

8.4 数据备份及恢复

8.4.1 数据备份

6. 限制操作

在执行数据库备份的过程中，允许用户对数据库继续操作，但不允许用户在备份时执行下列操作：


- 创建或删除数据库文件
- 创建索引
- 不记日志的命令。

 **注意：**若在系统正执行上述操作中的任何一种时试图进行备份，则备份进程不能执行。

8.4 数据备份及恢复

8.4.2 数据恢复

数据恢复（Data Restore）是指将备份到存储介质上的数据再恢复(还原)到计算机系统的过程。与数据备份是一个逆过程，可能需要涉及整个数据库系统的恢复。

 **注意：**数据恢复是与数据备份相对应的系统维护和管理操作。系统进行恢复操作时，先执行一些系统安全性检查，包括检查所要恢复的数据库是否存在、数据库是否变化以及数据库文件是否兼容等，然后根据所采用的数据库备份类型采取相应的恢复措施。

8.4 数据备份及恢复

8.4.2 数据恢复

1. 准备工作

数据库恢复的准备工作包括系统安全性检查和备份介质验证。在进行恢复时，系统先执行安全性检查、重建数据库及其相关文件等操作，保证数据库安全的恢复，这是数据库恢复必要的准备，可以防止错误的恢复操作。

 **注意：**当系统发现出现了以下情况时，恢复操作将不进行：

- (1) 指定要恢复的数据库已存在，但在备份文件中记录的数据库与其不同；
- (2) 服务器上数据库文件集与备份中的数据库文件集不一致；
- (3) 未提供恢复数据库所需的所有文件或文件组。

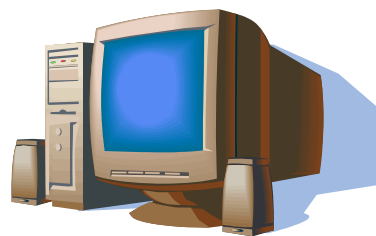
8.4 数据备份及恢复

8.4.2 数据恢复

2. 数据库的故障和恢复策略

数据库运行过程中可能会出现各种各样的故障，这些故障可分为**3类：事务故障、系统故障和介质故障**。根据故障类型的不同，应该采取不同的恢复策略。

- (1) 事务故障及其恢复
- (2) 系统故障及其恢复
- (3) 介质故障及其恢复



8.4 数据备份及恢复

上海市高校精品课程
国家十三五规划项目

8.4.2 数据恢复

■ 故障发生后对数据库的影响有两种可能性：

- 1) 数据库没有被破坏，但数据可能处于不一致状态。这是由事务故障和系统故障引起的，这种情况在恢复时，不需要重装数据库副本，直接根据日志文件，撤销故障发生时未完成的事务，并重做已完成的事务，使数据库恢复到正确的状态。这类故障的恢复是系统在重新启动时自动完成的，不需要用户干预。
- 2) 数据库本身被破坏。由介质故障引起，在此情况恢复时，将最近一次备份的数据装入，并借助日志文件，对数据库进行更新，从而重建数据库。这类故障的恢复不能自动完成，需要DBA的介入，先由DBA利用DBMS重装最近备份的数据库副本和相应的日志文件的副本，再执行系统提供的恢复命令。

8.4 数据备份及恢复

上海市高校精品课程
国家十三五规划项目

8.4.2 数据恢复

3. 数据恢复类型

数据恢复操作通常有**3**种类型：全盘恢复、个别文件恢复和重定向恢复。

(1) **全盘恢复**。是将备份到介质上的指定系统信息全部备份到其原来的地方。

(2) **个别文件恢复**。是将个别已备份的最新版文件恢复到原来的地方。

(3) **重定向恢复**。是将备份的文件或数据，恢复到另一个不同的位置或系统上去，而不是做备份操作时其所在的位置。

8.4 数据备份及恢复

上海市高校精品课程
国家十三五规划项目

8.4.2 数据恢复

4. 恢复模式

恢复模式是一个数据库属性，用于控制数据库备份和还原操作的基本行为。如恢复模式控制了将事务记录在日志中的方式、事务日志是否需要备份以及可用的还原操作。

（1）恢复模式的优点：可以简化恢复计划，并简化备份和恢复过程，明确系统操作要求之间的权衡，明确可用性和恢复要求之间的权衡。

（2）恢复模式的分类

在SQL中，有3种恢复模式：简单恢复模式、完整恢复模式和大容量日志恢复模式。

SQL server 2016默认恢复模式为“完整恢复模式”。

8.4 数据备份及恢复

8.4.2 数据恢复

5. 执行恢复数据库操作

- (1) 使用**SSMS**恢复数据库
- (2) 使用备份设备恢复
- (3) 使用**T-SQL**语句恢复数据库



📖 讨论思考

- 1、数据备份常用方法及数据备份的范围主要有哪些？
- 2、数据库的故障及其恢复策略？



8.5 并发控制和封锁技术

上海市高校精品课程
国家十三五规划项目

案例8-10

现代信息系统几乎不存在单用户操作，基本上都是多用户操作，多个用户共享数据库，多个用户可能在同一时刻去访问或修改同一部分数据，这样就引出了一个问题——**并发**。这样可能导致数据库中的数据不一致，这时就需要用到**事务**。

8.5 并发控制和封锁技术

- 并发成为问题主要是基于**资源争用**，资源争用会引起一系列的问题，主要体现在**事务的阻塞**上面。另外一个重要的问题就是**数据的不一致性**。
- **事务**就是一个操作单元，这个操作可能是一行Update语句，也可能是异常复杂的一系列增删改查操作。
- **事务具有4个基本特性（ACID）**：原子性（Atomicity）、一致性（Consistency）、隔离性（Isolation）、持久性（Durability）
- SQL Server默认保证其中3个特性：原子性、一致性和持久性。

8.5 并发控制和封锁技术

上海市高校精品课程
国家十三五规划项目

8.5.1 并发操作产生的问题

- **数据库资源**可为多个应用程序所**共享**。
- 各用户在存取数据时，可能是**串行执行**。串行执行时，其它用户程序必须等到前一用户程序结束才能进行存取，若一个用户程序涉及大量数据的输入/输出交换，则系统的大部分时间将处于闲置状态。
- 为了充分利用数据资源，进行**并行存取**，就会发生多用户并发同时存取同一数据的情况，即数据库的**并行操作（并发操作）**。



8.5 并发控制和封锁技术

8.5.2 并发控制概述

1. 并发控制概念

- 数据库的并发控制是对多用户程序并行存取的控制机制，目的是避免数据的丢失修改、无效数据的读出与不可重复读数据现象的发生，从而保持数据的一致性。
- 事务是数据库并发控制的基本单位。是用户定义的一个操作序列。对事务的操作实行“要么都做，要么都不做”原则，将事务作为一个不可分割的工作单位。
- 通过事务 **SQL Server** 可将逻辑相关的一组操作绑定在一起，以便服务器保持数据的完整性。

8.5 并发控制和封锁技术

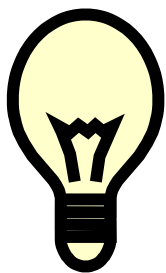
上海市高校精品课程
国家十三五规划项目

2. 并发控制需要处理的问题

事务的并发操作带来的数据不一致问题主要包括：

(1) 丢失更新。

- 当两个或多个事务选择同一行（数据记录），然后基于最初选定的值更新该行时，会发生丢失更新问题。




例如：最初有一份原始的电子文档，文档人员W和L同时修改此文档，当修改完成之后保存时，最后修改完成的文档必将替换第一个修改完成的文档，那么就造成了数据丢失更新的后果。如果在文档人员W修改并保存之后，文档人员L再进行修改则可以避免此问题。

8.5 并发控制和封锁技术

2. 并发控制需要处理的问题

(2) 读“脏”数据（脏读）。

- 指一个事务正在访问数据，而其它事务正在更新该数据，但尚未提交，此时就会发生脏读问题，即第一个事务所读取的数据是“脏”（不正确）数据，它可能会引起错误。




例如：文档人员L复制了文档人员W正在修改的文档，并将文档人员W的文档发布，此后，文档人员W认为文档中存在着一一些问题需要重新修改，此时文档人员L所发布的文档就将与重新修改的文档内容不一致，如果在文档人员W将文档修改完成并确认无误的情况下，文档人员L再复制文档则可以避免此问题。

8.5 并发控制和封锁技术

2. 并发控制需要处理的问题

(3) 不可重复读。

当一个事务多次访问同一行且每次读取不同的数据时，会发生此问题。不可重复读与脏读有相似之处，因为该事务也是正在读取其它事务正在更改的数据。当一个事务访问数据时，另外的事务也访问该数据并对其进行修改，因此就发生了由于第二个事务对数据的修改而导致第一个事务两次读到的数据不一样的情况，这就是不可重复读。




例如：文档人员L两次读取文档人员W的文档，但在文档人员L读取时，文档人员W又重新修改了该文档中的内容，在文档人员L第二次读取文档人员W的文档时，文档中的内容已被修改，此时就发生了不可重复读的情况。如果文档人员L在文档人员W全部修改完成后读取文档，则可以避免该问题。

8.5 并发控制和封锁技术

2. 并发控制需要处理的问题

(4) **幻读**。当一个事务对某行执行插入或删除操作，而该行属于某个事务正在读取的行的范围时，会发生幻读问题。



例如：文档人员L更改了文档人员W所提交的文档，但当文档人员L将更改后的文档合并到主、副本时，却发现文档人员W已将新数据添加到该文档中。如果文档人员L在更改文档之前，不会有人将新数据添加到该文档中，则可以避免该问题。

8.5 并发控制和封锁技术

上海市高校精品课程
国家十三五规划项目

8.5.3 常用的封锁技术

1. 封锁技术

- 并发控制的主要技术是**封锁（locking）**。它是实现数据库并发控制的主要手段。封锁可以防止用户读取正在由其它用户更改的数据，并可以防止多个用户同时更改相同数据。
- 如果不使用封锁，则数据库中的数据可能在逻辑上不正确，并且对于数据的查询可能会产生意想不到的结果。
- 具体来讲，封锁可以防止丢失更新、脏读、不可重复读、幻读等并发操作带来的数据不一致性问题。



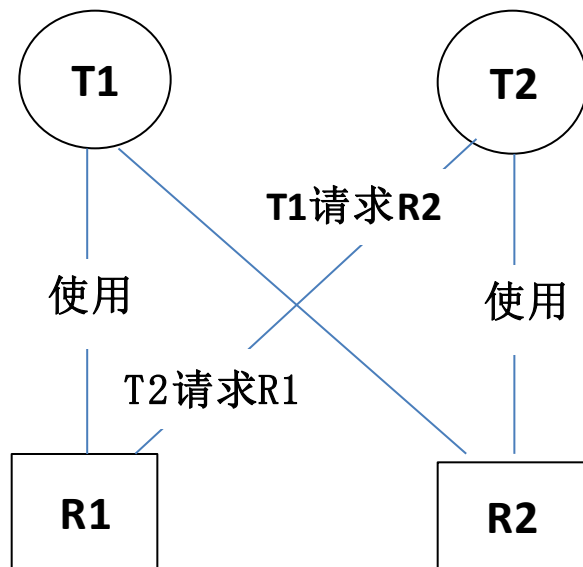
8.5 并发控制和封锁技术

上海市高校精品课程
国家十三五规划项目

8.5.3 常用的封锁技术

1. 封锁技术

- 当两个事务分别封锁某个资源，而又分别等待对方释放其封锁的资源时，就会发生死锁（Deadlock）。



8.5 并发控制和封锁技术

上海市高校精品课程
国家十三五规划项目

8.5.3 常用的封锁技术

1. 封锁技术

- **活锁 (livelock)** 指的是任务或者执行者没有被阻塞，由于某些条件没有满足，导致一直重复尝试，失败，尝试，失败。
- **活锁和死锁的区别**：处于活锁的实体是在不断的改变状态，所谓的“活”，而处于死锁的实体表现为等待；活锁有可能自行解开，死锁则不能。

“活锁”举例：如果事务T1封锁了数据R，事务T2又请求封锁R，于是T2等待。T3也请求封锁R，当T1释放了R上的封锁后，系统首先批准了T3的请求，T2仍然等待。然后T4又请求封锁R，当T3释放了R上的封锁之后，系统又批准了T4的请求……T2可能永远等待。

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

2. 锁定粒度

- **SQL Server**中，可被封锁的资源从小到大分别是行、页、扩展盘区、表和数据库，被封锁的资源单位称为**锁定粒度**。
- 上述**5**种资源单位其锁定粒度是由小到大排列的。
- 锁定粒度不同，资源的开销将不同，并且锁定粒度与数据库访问并发度是一对矛盾，锁定粒度大，系统开销小，但并发度会降低；锁定粒度小，系统开销大，但并发度可提高。

🔔 参看课本表8-3 锁的粒度及其说明

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

- **SQL Server**使用不同的锁模式锁定资源，这些锁模式确定了并发事务访问资源的方式。
- 共有7种封锁模式：分别是共享（**Shared, S**）、排它（**Exclusive, X**）、更新（**Update, U**）、意象（**Intent**）、架构（**Schema**）、键范围（**Key-range**）、大容量更新（**Bulk Update, BU**）



8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

- (1) **共享（S锁、读锁）**：共享锁允许并发事务读取一个资源。当一个资源上存在共享锁时，任何其它事务都不能修改数据。
 - 默认情况下，SQL Server会自动在需要读取的数据上加上S锁，表、页和单独的行（表或者索引上）都可以持有S锁。通常情况下，SQL Server会在读取完数据后马上释放S锁，不需要等待事务结束。

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

- **（2）排它（X锁、写锁）**：排它锁可以防止并发事务对资源进行访问。其它事务不能读取或修改排它锁锁定的数据。
 - 当SQL Server通过Insert、Update、Delete等操作修改数据时，会对相应的数据加X锁。任何时候（事务范围内），一个特定的数据资源上只能有一个X锁。被修改的数据在事务提交或者回滚前，对于其它事务都是不可用的。

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

(3) **更新锁**。更新锁可以防止通常形式的死锁。一般更新模式由一个事务组成，此事务读取记录，获取资源（页或行）的共享锁，然后修改行，此操作要求锁转换为排它锁。

- 如果两个事务获得了资源上的共享锁，然后试图同时更新数据，则其中的一个事务将尝试把锁转换为排它锁。共享模式到排它锁的转换必须等待一段时间，因为一个事务的排它锁与其它事务的共享锁不兼容，这就是锁等待。第二个事务试图获取排它锁以进行更新。由于两个事务都要转换为排它锁，并且每个事务都等待另一个事务释放共享锁，因此会发生死锁，这就是潜在的死锁问题。
- 为避免这种情况的发生，可使用更新锁。一次只允许有一个事务可获得资源的更新锁，如果该事务要修改锁定的资源，则更新锁将转换为排它锁，否则为共享锁。

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

(4) **意向锁**。意向锁表示**SQL Server**需要在层次结构中的某些底层资源（如表中的页或行）上获取共享锁或排它锁。

- 例如，放置在表级的共享意向锁表示事务打算在表中的页或行上放置共享锁。在表级设置意向锁可防止另一事务随后在包含那一页的表上获取排它锁。
- 意向锁可以提高性能，因为**SQL Server**仅在表级检查意向锁来确定事务是否可以安全地获取该表上的锁，而无须检查表中的每行或每页的锁以确定事务是否可以锁定整个表。

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

(5) **架构锁**。执行表的数据定义语言操作（如增加列或删除表）时使用架构修改锁。

- 当编译查询时，使用架构稳定性锁。架构稳定性锁不阻塞任何事务锁，包括排它锁。因此在编译查询时，其它事务（包括表上有排它锁的事务）都能继续运行，但不能在表上执行**DDL**操作。

(6) **键范围锁**。键范围锁用于序列化的事务隔离级别，可以保护由**T-SQL**语句读取的记录集合中隐含的行范围。

- 键范围锁可以防止幻读，还可以防止对事务访问的记录集进行幻想插入或删除。

8.5 并发控制和封锁技术

8.5.3 常用的封锁技术

3. 封锁模式

(7) **大容量更新锁**。当将数据大容量复制到表，且指定了**Tablock**提示或者使用**Sp_tableoption**设置了**Table lock on bulk**表选项时，将使用大容量更新锁。

- 大容量更新锁允许进程将数据并发地大容量复制到同一表，同时可防止其它不进行大容量复制数据的进程访问该表。



8.5 并发控制和封锁技术

8.5.4 并发操作的调度

- 计算机系统以随机的方式对并行操作调度，而不同的调度可能会产生不同的结果。若一个事务运行中不同时运行其它事务，则可认为该事务的运行结果为正常或预期的，因此将所有事务串行起来的调度策略是正确的调度策略。
- 几个事务的并行执行是正确的，当且仅当其结果与按某一次序串行地执行的结果相同。此并行调度策略称为可串行化（**Serializable**）的调度。可串行性（**Serializability**）是并行事务正确性的唯一准则。

🔔 参看课本表8-4 对两个事务的不同调度策略

8.5 并发控制和封锁技术

上海市高校精品课程
国家十三五规划项目

讨论思考

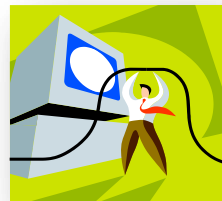
并发控制需要处理的问题有哪些？



8.6 实验八 数据备份及恢复操作

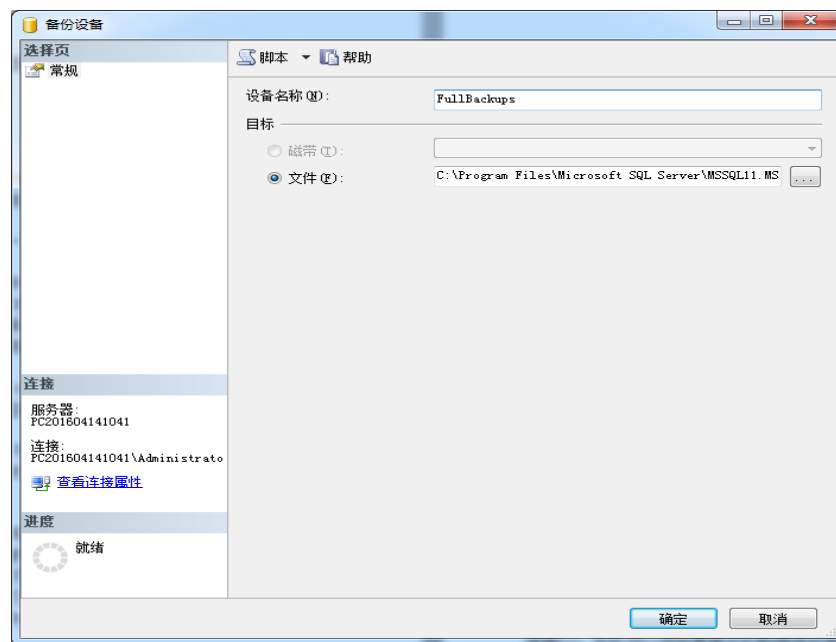
8.6.1 实验目的

- (1) 掌握数据备份的基本方法。
- (2) 掌握数据还原（恢复）的基本方法



8.6.2 实验内容及步骤

- (1) 利用SQL Server Management Studio (SSMS) 管理备份设备。在备份一个数据库之前，需要先创建一个备份设备，比如磁带、硬盘等，然后再去复制有备份的数据库、事务日志、文件/文件组。请自己新建一个备份设备，查看备份设备，删除备份设备。
- 使用SSMS来创建备份设备：



8.6 实验八 数据备份及恢复操作

上海市高校精品课程
国家十三五规划项目

- （2）备份数据库。打开SSMS，右击需要备份的数据库，选择“任务”→“备份”命令，出现备份数据库窗口。在此可以选择要备份的数据库和备份类型。

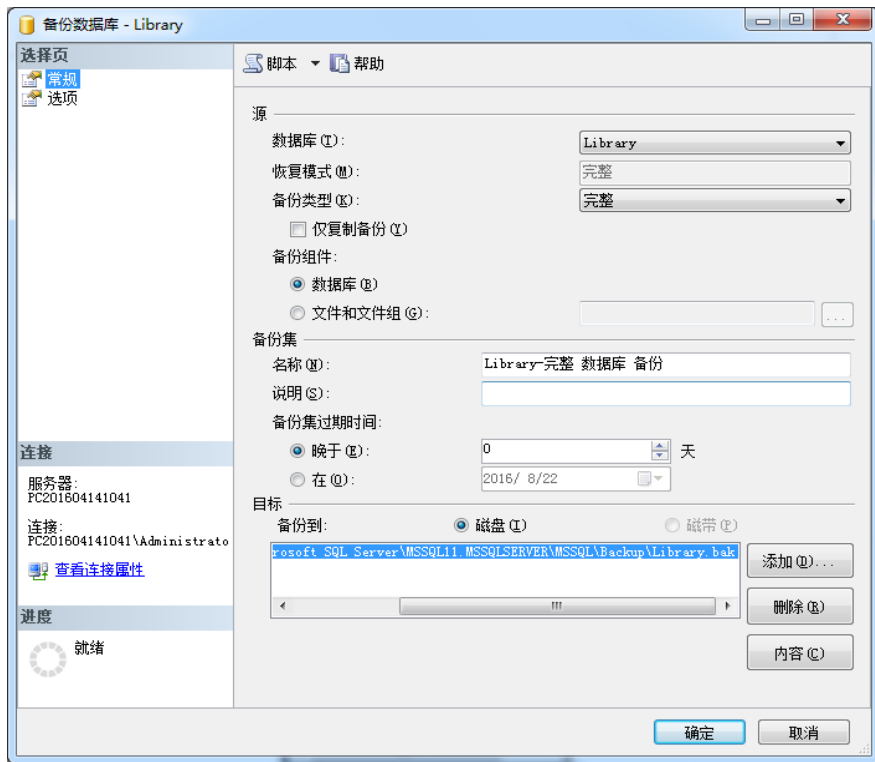


图8-7 使用SSMS执行完整数据库备份

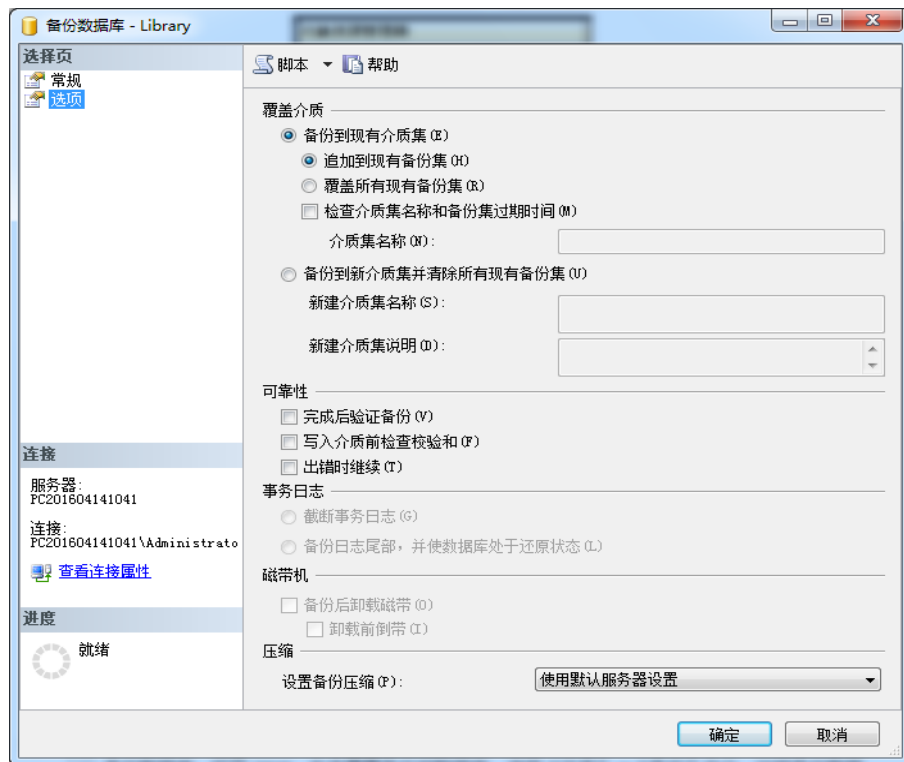


图8-8 使用SSMS执行完整数据库备份选项卡

8.6 实验八 数据备份及恢复操作

上海市高校精品课程
国家十三五规划项目

- (3) 数据库的差异备份。差异数据库备份只记录自上次数据库备份后发生更改的数据。差异数据库备份比数据库备份小而且备份速度快，因此可以经常地备份，经常备份将减少丢失数据的危险。
- 使用差异数据库备份将数据库还原到差异数据库备份完成时那一点。若要恢复到精确的故障点，必须使用事务日志备份。

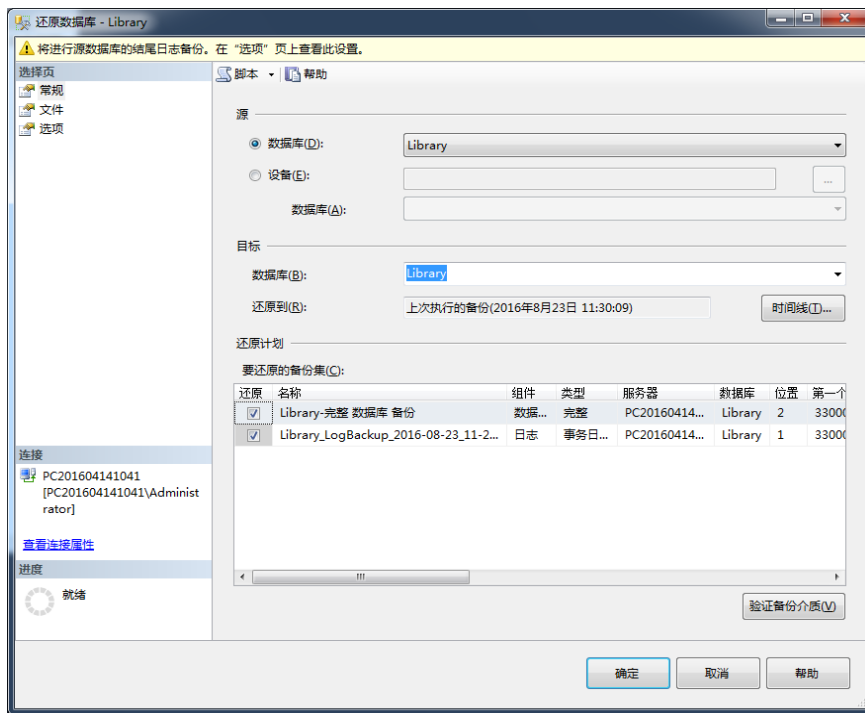


图8-9 使用SSMS执行差异备份

8.7 本章小结

上海市高校精品课程
国家十三五规划项目

- 通过对数据库安全的叙述，讲解了SQL server 2016在安全方面的特性。概述了数据库安全、数据库系统安全、数据安全的有关概念。数据库安全的核心和关键是数据安全。
- 在此基础上做了数据库安全风险分析，指出了常见数据库的安全缺陷和隐患要素。介绍了数据库安全关键技术，SQL Server的安全策略和安全管理机制，在数据的访问权限及控制方面，涉及数据库的身份验证及权限管理，以及数据库安全访问控制方法。并结合SQL Server 2016实际应用，概述了具体的登录控制、用户与角色管理和权限管理等应用操作。
- 数据的备份与恢复是数据库文件管理中最常见的操作，数据备份应考虑备份内容、备份介质、备份时机、备份方法及类型。数据恢复是与数据备份相对应的系统维护和管理操作，通过叙述数据库运行故障，介绍了相对应的数据恢复类型。介绍了利用SQL Server 2016管理器SSMS或SQL备份/恢复语句在本地主机上进行数据库备份和恢复操作。
- 最后介绍了并发控制与封锁等管理技术和方法。

国家“十三五”重点出版规划项目
上海高校优秀教材奖获得者主编

上海市高校精品课程
特色教材

诚挚谢意！



数据库原理及应用

——基于SQL Server 2016