学习单元 3

Windows 服务器数据库的安全配置

☆ 单元概要

本单元基于 Windows Server 2008 R2 操作系统环境，讲解 MSSQL 数据库的安全配置，分为三个任务，分别对 MSSQL 数据库系统用户、MSSQL 安全配置和 MSSQL 数据库备份与还原进行讲解。

☆ 单元情境

网络安全工程师小张接到任务，要求对学校 Windows Server 2008 R2 操作系统下搭载的 SQL Server 数据库进行安全加固。经过团队的讨论，认为加固数据库非常重要，应该从数据库用户管理、数据库安全配置和数据库的备份与还原三个部分进行，完成整个的任务。

任务 1　MSSQL 系统用户管理


微课 28

★　任务描述

学校校园内采用 Microsoft SQL Server 2008 作为数据库系统为校园管理系统提供数据服务。网络安全工程师小张接到上级部门的任务，需要对数据库用户进行管理维护，保证数据库的安全。

★　任务分析

数据库用户的安全性，主要体现在允许具有数据库访问权限的用户能够登录到 SQL Server 访问数据，并对数据库对象实施操作，但是要拒绝所有的非授权用户的非法操作。因此，安全性管理与用户管理是密不可分的。需要修改数据库系统的身份验证模式并对数据库服务器、应用系统的数据库或表设置管理员。在数据库权限配置能力内，根据用户的业务需要，配置其用户所需的最小权限，做好用户分级管理。

★　任务实施

1．修改身份验证模式，打开桌面【SQL Server Management Studio】管理工具，如图 3-1 所示。在弹出的【连接到服务器】界面中单击【连接】按钮，如图 3-2 所示。

图 3-1　SQL Server Management Studio 管理工具

图 3-2　链接数据库实例

✿经验分享

SQL Server 数据库有两种登录身份验证模式，一种是 Windows 身份验证；另一种是 SQL Server 账户验证模式。在 SQL Server 账户验证模式中，sa 账户是内置的默认管理员账户，拥有最高的操作权限；sa 账户是大家所熟知的，那么，一些别有用心的人也知道 sa 账户，这就为我们的数据安全留下了安全隐患；

黑客会通过扫描程序在互联网上大量扫描，寻找那些开着远程访问并且使用 sa 账户的数据库服务器，然后用穷举法不断尝试密码。无论密码多么复杂，也很难抵御 24 小时不间断地扫描和破解。

2．选中数据库实例，单击鼠标右键选择【属性】，如图 3-3 所示。

图 3-3　SQL Server Management Studio 管理工具界面

3．在服务器属性左侧窗格中选择【安全性】，在右侧窗格的【服务器身份验证】模式中选中【SQL Server 和 Windows 身份验证模式】。然后单击【确定】按钮，如图 3-4 所示。

4．停用 sa 账户。在【安全性】→【登录名】中选中 sa，单击鼠标右键选择【属性】，如图 3-5 所示。

5．在登录属性【状态】页中，在【是否允许连接到数据库引擎】选项中选择【拒绝】，在【登录】选项中选择【禁用】。然后单击【确定】按钮应用设置，如图 3-6 所示。

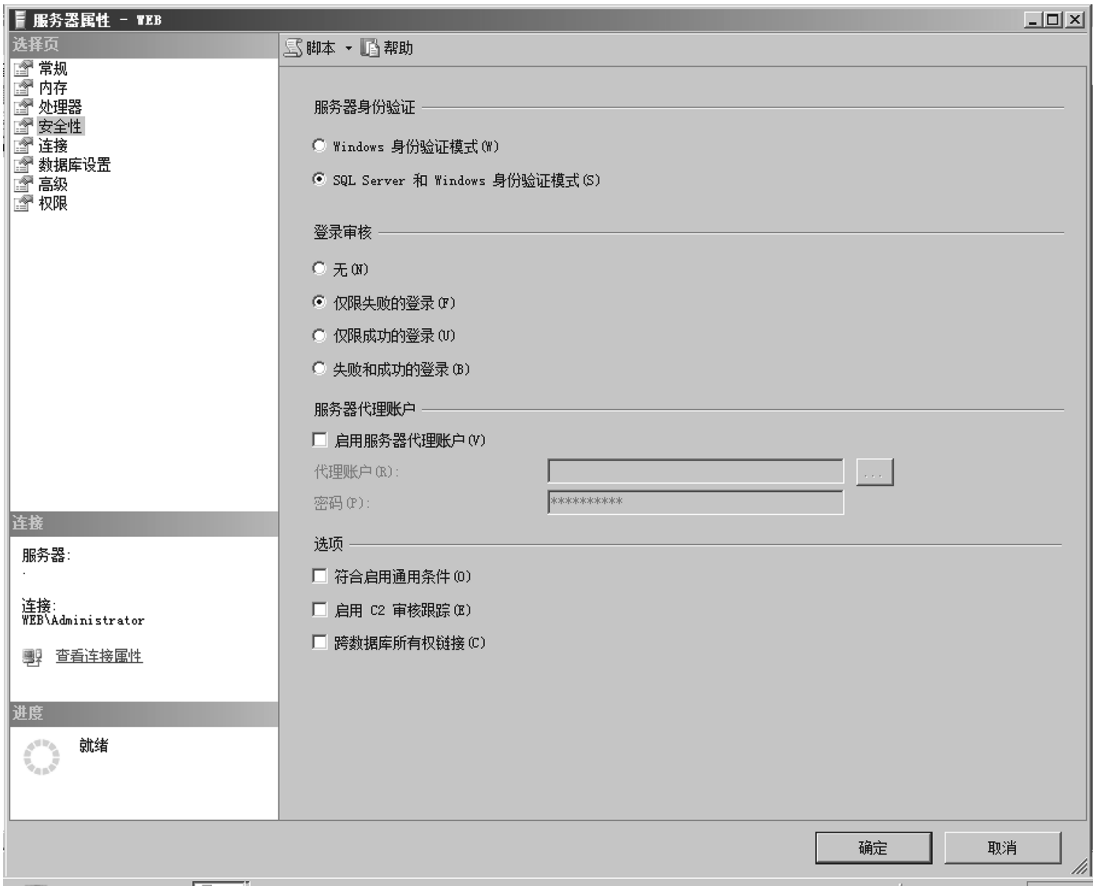

图 3-4　服务器属性安全选项页界面

✿知识链接

Windows 身份验证

Windows 身份验证适用于 Windows 平台的用户，不需要提供密码和 Windows 集成验证，因为 Windows 系统本身就有管理和验证登录用户的能力。用户的管理交给 Windows 系统管理，而数据库管理员专注于数据库库管理，数据库管理员可以利用 Windows 的账户管理的功能，包括安全验证、加密、审核、密码过期、最小密码长度、账户锁定等，不需要在 SQL Server 中另外建立一个登录验证机制。

混合验证

混合验证适用于各种平台操作系统，以及 Internet 用户。使用 SQL Server 用户名和密码登录数据库服务器，即使网络上的客户机没有服务器操作系统的账户也可以登录并使用 SQL Server 数据库，很方便。

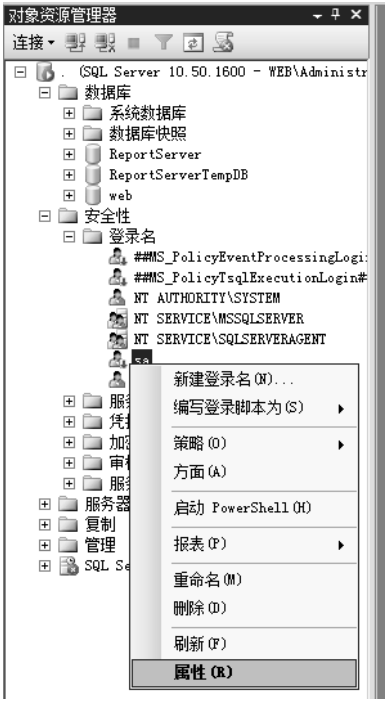

图 3-5　选择 sa 用户

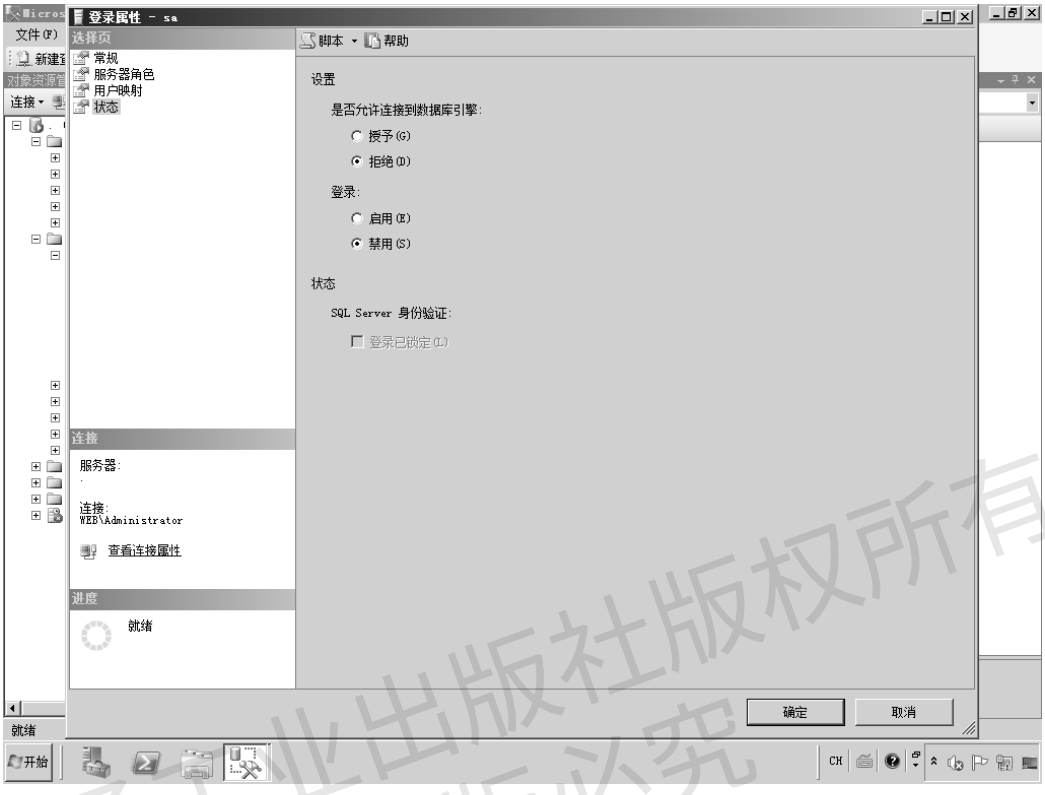

图 3-6　设置 sa 用户状态

6．创建一个服务器管理员账户，选中【登录名】，单击鼠标右键选择【新建登录名】，如图 3-7 所示。

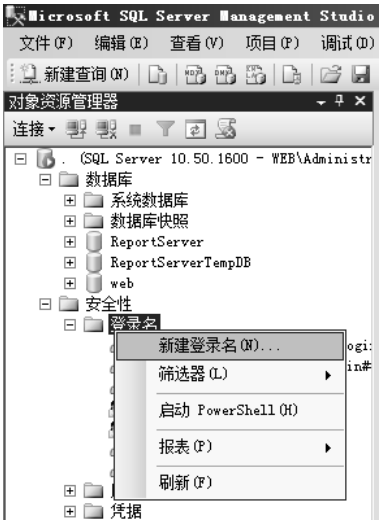

图 3-7　新建登录用户

7．在【常规】右侧窗格中，输入新的用户名和密码后单击【确定】按钮，如图 3-8 所示。

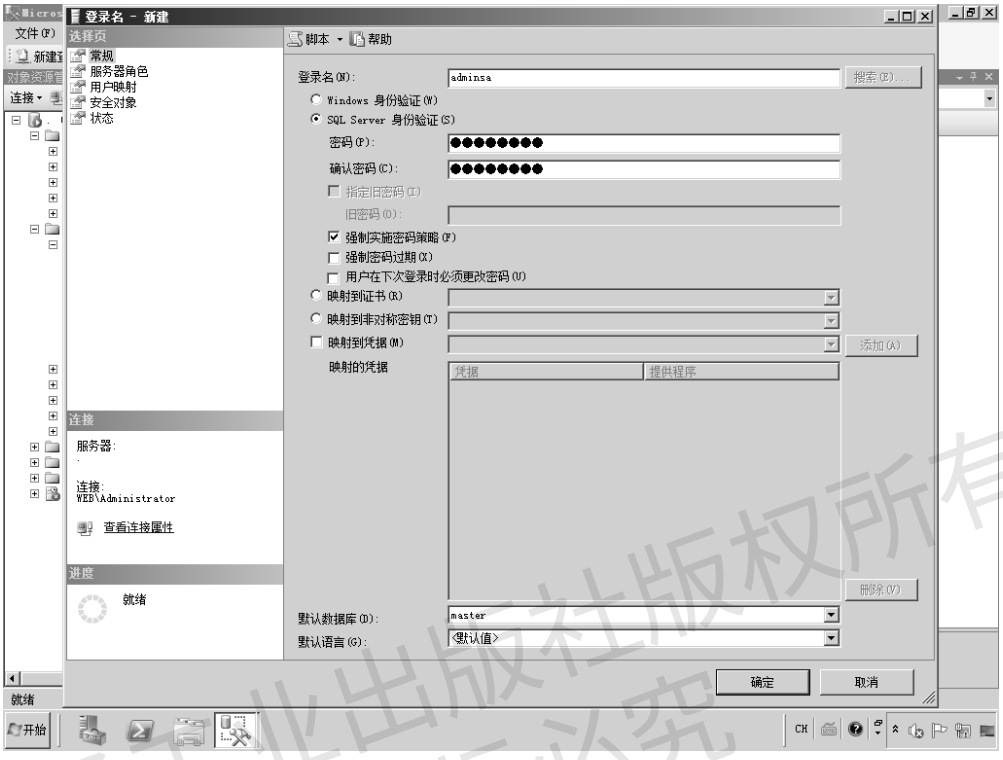

图 3-8　创建用户名和密码

8．在【服务器角色】右侧窗格中，在服务器角色中勾选【public】和【sysadmin】选项。然后单击【确定】按钮创建用户，如图 3-9 所示。

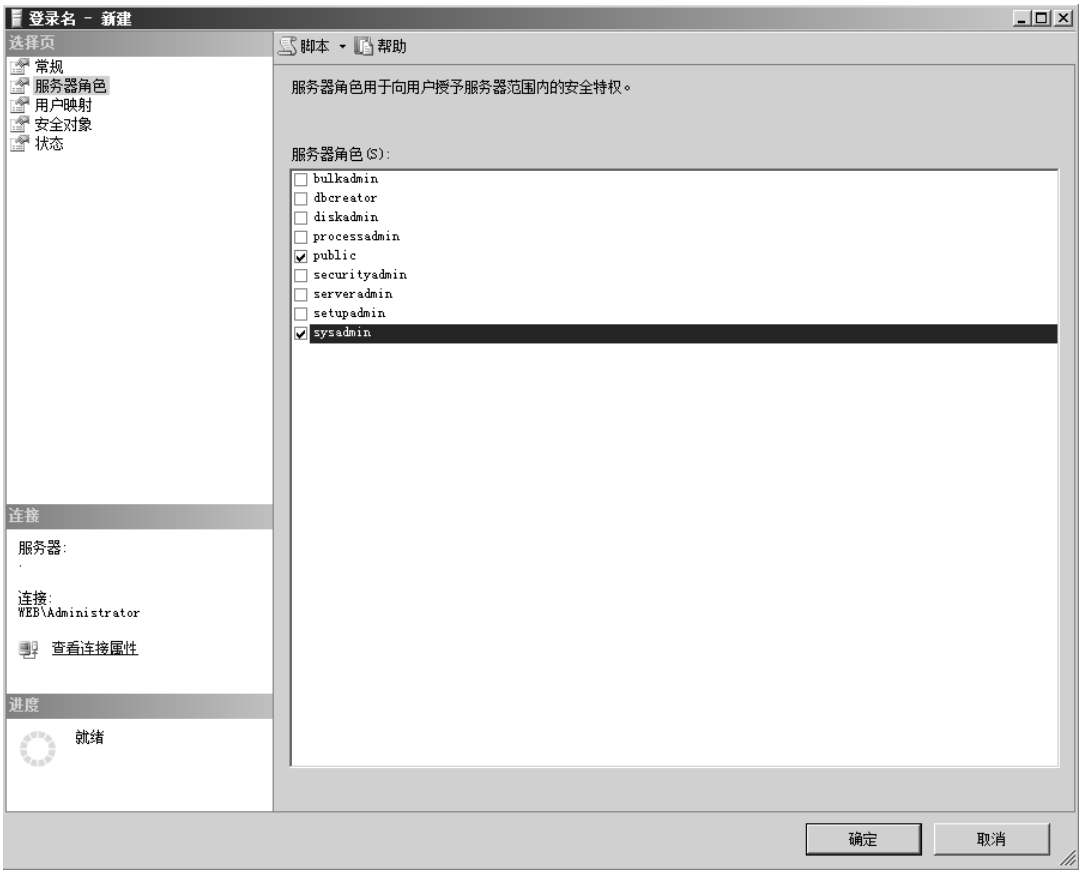

图 3-9　设置用户权限

✿知识链接

服务器角色按照从最低级别角色（bulkadmin）到最高级别角色（sysadmin）的顺序进行描述如下。

1．bulkadmin：这个角色可以运行 BULK INSERT 语句。该语句允许从文本文件中将数据导入到 SQL Server 2008 数据库中，为需要执行大容量插入到数据库的域账号而设计。

2．dbcreator：这个角色可以创建、更改、删除和还原任何数据库。不仅适合助理 DBA 角色，也适合开发人员角色。

3．diskadmin：这个角色用于管理磁盘文件，比如镜像数据库和添加备份设备。适合助理 DBA 角色。

4．processadmin：SQL Server 2008 可以同时多进程处理。这个角色可以结束进程（在 SQL Server 2008 中称为“删除”）。

5．public：有两大特点：第一，初始状态时没有权限；第二，所有数据库用户都是它的成员。

6．securityadmin：这个角色将管理登录名及其属性。可以授权、拒绝和撤销服务器级/数据库级权限。也可以重置登录名和密码。

7．serveradmin：这个角色可以更改服务器范围的配置选项和关闭服务器。

8．setupadmin：为需要管理联接服务器和控制启动的存储过程的用户而设计。

9．sysadmin：这个角色有权在 SQL Server 2008 中执行任何操作。

9．创建一个应用数据的管理用户，在【常规】右侧窗格中，输入新的用户名和密码后单击【确定】按钮，如图 3-10 所示。

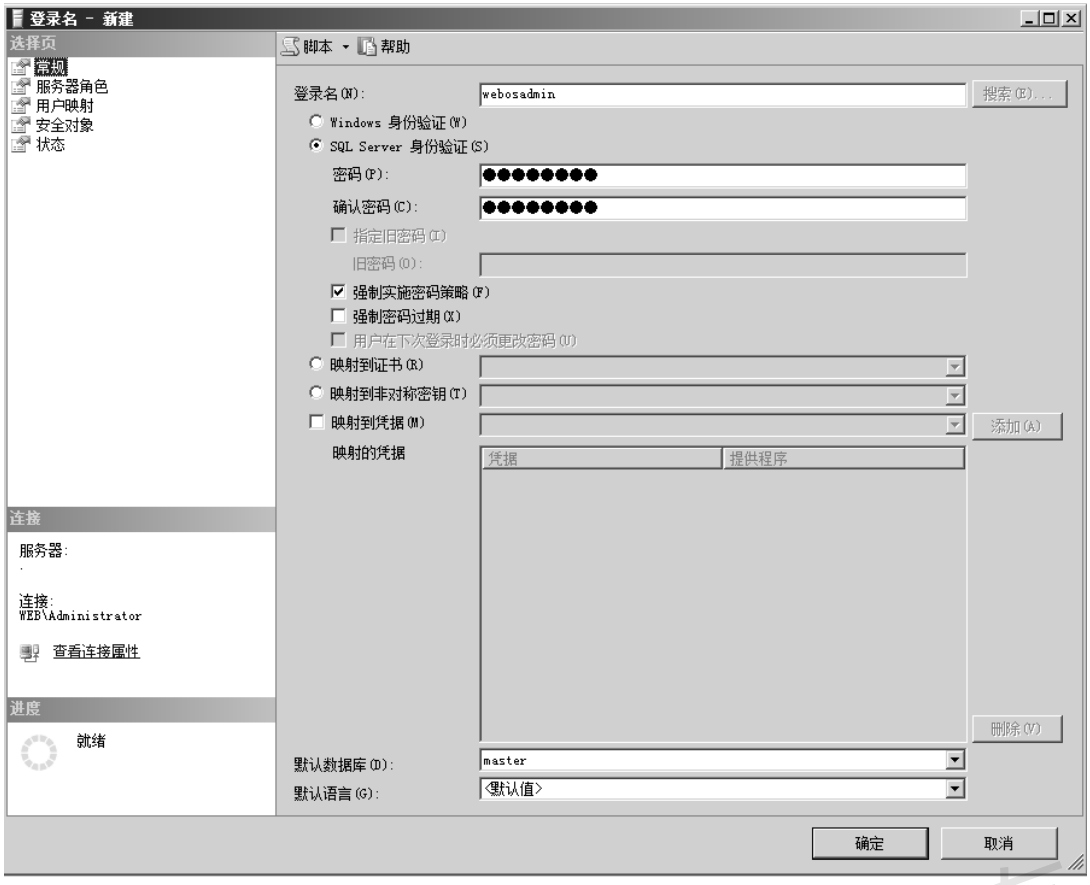

图 3-10　创建用户

10．设置用户权限，选择界面左侧【服务器角色】，在右侧窗格的【服务器角色】中勾选【public】选项后单击【确定】按钮，如图 3-11 所示。

11．单击界面左侧的【用户映射】。在右侧窗格的【映射到此登录名的用户】中勾选需要管理的数据库，在【数据库角色成员身份】中勾选【db_owner】和【db_securityadmin】选项，保持【public】的默认勾选状态然后单击【确定】按钮，如图 3-12 所示。

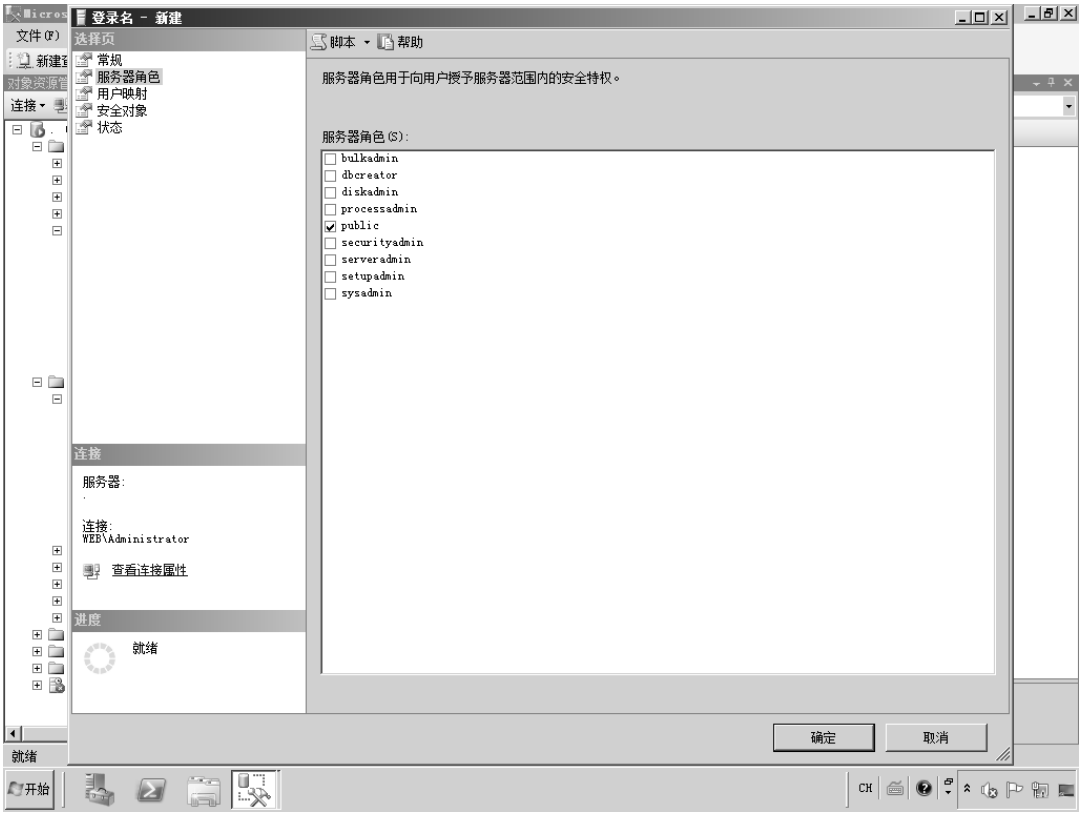

图 3-11　设置用户权限

✿知识链接

数据角色

1．db_accessadmin：可以在数据库中添加和删除数据库用户、组及角色。

2．db_backupoperator：可以备份数据库。

3．db_datareader：可以读取任何表中的数据。

4．db_datawriter：可以添加、更改或删除所有表中的数据。

5．db_ddladmin：可以添加、更改或删除数据库对象（可以执行任何 DDL 语句）。

6．db_denydatareader：不能读取任何表中的数据，但仍然可以通过存储过程来查看。

7．db_denydatawriter：不能更改任何表中的数据，但仍然可以通过存储过程来修改。

8．db_owner：执行任何操作。

9．db_securityadmin：可以更改数据中的权限和角色。

10．public：每个数据库用户都属于 public 角色。未对用户授权之前，该用户将被授予。public 角色的权限。该角色不能被删除。

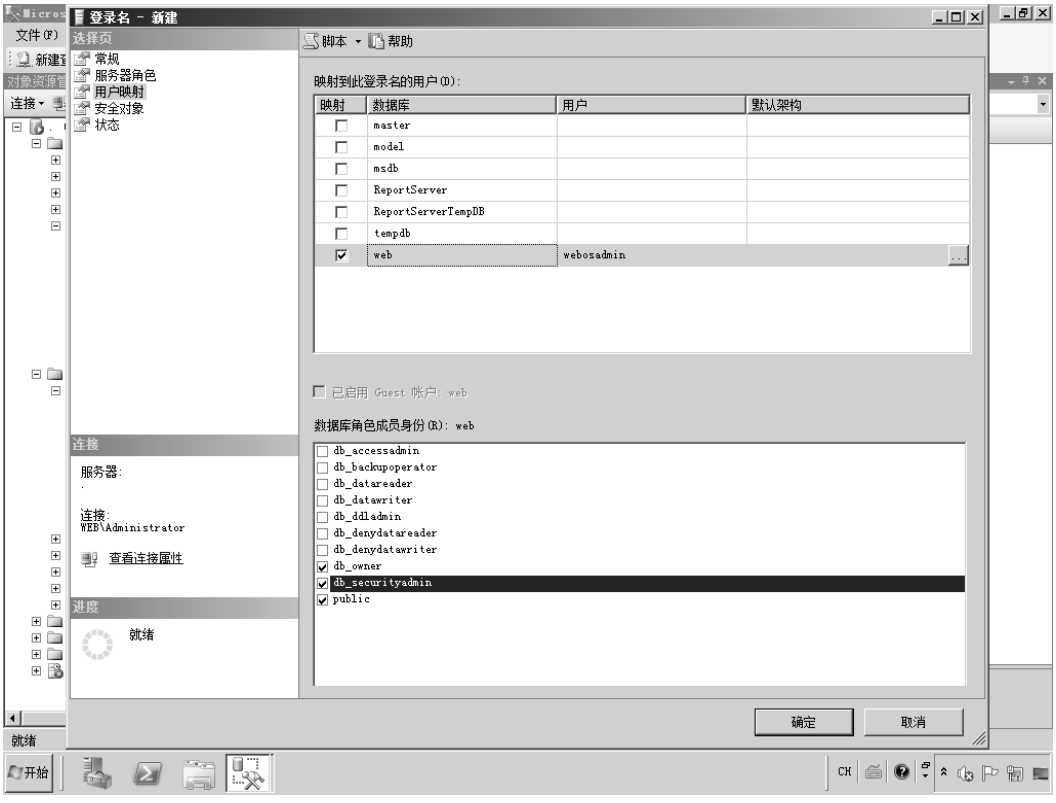

图 3-12　设置数据权限

★　任务验收

通过本任务的实施，学会 MSSQL 数据库系统用户管理。

评价内容	评价标准	完成效果
MSSQL 数据库系统用户管理	在规定时间内，完成 MSSQL 数据库系统用户管理	

★　拓展练习

使用 SQL Server Management Studio 管理数据库用户，禁用 sa 用户，新建用户并赋予权限，提升用户安全性。

任务 2　MSSQL 的安全配置

★　任务描述

学校校园内采用 Microsoft SQL Server 2008 作为数据库系统为校园管理系统提供数据服务。技术人员已经对数据库的用户权限进行了分级管理，现在需要网络安全工程师小张对服务器做进一步的安全加固保证数据库的安全。

微课 29

★ **任务分析**

通过设置通信协议加密、隐藏实例、设置连接协议和监听的 IP 范围，限制不必要的远程客户端访问到数据库资源。设置连接超时功能，修改默认通信端口，禁止高危存储过程处理来增强服务器的安全。

★ **任务实施**

1．设置通信协议加密，单击桌面【开始】菜单，选择【Microsoft SQL Server 2008 R2】→【配置工具】→【SQL Server 配置管理器】，如图 3-13 所示。

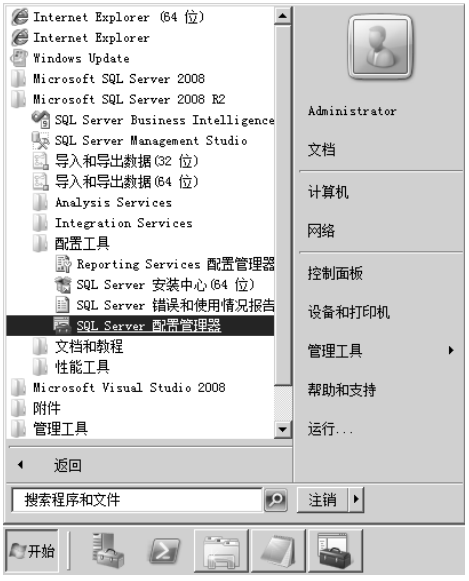

图 3-13　选择【SQL Server 配置管理器】

2．在弹出的【Sql Server Configuration Manager】界面选择【SQL Server 配置管理器（本地）】→【SQL Server 网络配置】→【MSSQLSERVER 的协议】，单击鼠标右键选择【属性】，如图 3-14 所示。

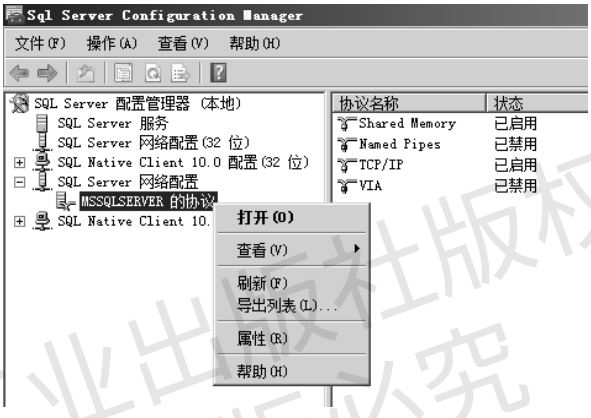

图 3-14　SQL Server 配置管理器界面

3．在【MSSQLSERVER 的协议 属性】界面中单击【标志】选项卡，在【强行加密】和【隐藏实例】中选【是】。然后单击【确定】按钮，如图 3-15 所示。

图 3-15 【SQLSERVER 的协议 属性】界面

4．关闭不必要的连接协议，VIA、Named Pipes 和 Share Memory 方式可能一般不需要使用。单击【MSSQLSERVER 的协议】，在右侧窗格选择相应的协议，单击鼠标右键选择【禁用】，如图 3-16 所示。

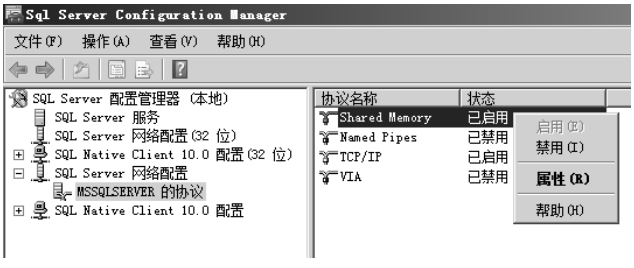

图 3-16 禁用协议

✿知识链接

Shared Memory：最快最简单的协议，使用 Shared Memory 协议的客户端仅可以连接到同一台服务器上的 SQLserver 实例。如果其他协议有误，可以通过 Shared Memory 连接到本地服务器进行故障处理。

TCP/IP：Internet 上广泛使用的通信协议，它包括路由网络协议的标准，提供高级的安全功能。

Named Pipes：为局域网而开发的协议，运行在 TCP、NETBEUI 等基础协议之上，并不是一个基层网络传送协议。客户端连接 Named Pipes（命名管道）的时候，它会首先访问服务器的 IPC$共享，访问 IPC$共享必须通过 Windows 认证协议。如果没有访问 SQL Server 服务器的文件系统的权限，就无法使用命名管道访问 SQL Server。

VIA：虚拟接口适配器 (VIA)协议和 VIA 硬件一同使用。

5．设置 IP 监听：访问数据库的应用程序也装在该服务器上，则只需要监听 127.0.0.1 即可，其他 IP 不需要监听。在应用程序中配置为使用 127.0.0.1 访问数据库。选择【TCP/IP】单击鼠标右键选择【属性】。在弹出的【TCP/IP 属性】界面单击【IP 地址】选项卡。将需要监视的 IP 地址在【活动】选择栏中选择【是】，如图 3-17 所示。

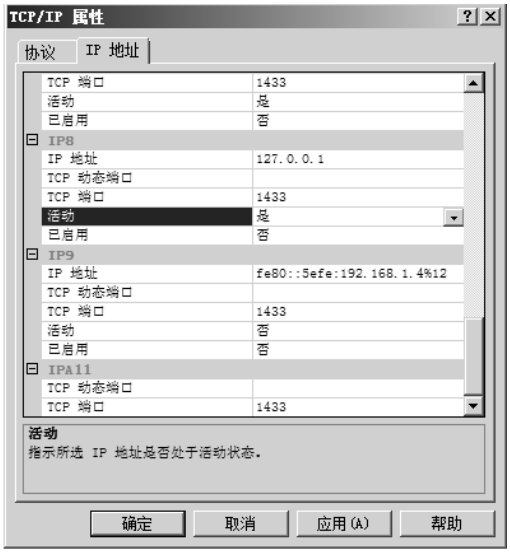

图 3-17　TCP/IP 属性

6．设置连接超时功能，选中数据库实例，单击鼠标右键选择【属性】，如图 3-18 所示。

图 3-18　管理工具界面

7．在服务器属性中，单击界面左侧【高级】选择项，在右侧窗格的【远程登录超时值】文本框内输入【10】然后单击【确定】按钮。设置登录后若无操作 10 秒即断开连接，

如图 3-19 所示。

图 3-19　服务器属性

8．关闭危存储过程处理，提高系统的安全。存储过程为数据库提供了强大的功能，MSSQL 强大的存储功能同时也为攻击者提供了便利，在相应的权限下，攻击者可以利用不同的存储过程执行不同的高级功能，如增加 MSSQL 数据库用户、枚举文件目录等。这些系统存储过程中 xp_cmdshell 功能最强大，通过该存储过程可以在数据库服务器中执行任意系统命令。在【SQL Server Management Studio】管理工具中单击【新建查询】，如图 3-20 所示。

图 3-20　新建查询

9．由于在 SQL Server 2008 中 sp_dropextendedproc 不会删除系统扩展存储过程，输入

代码单击【执行】关闭存储过程。如图 3-21 所示。

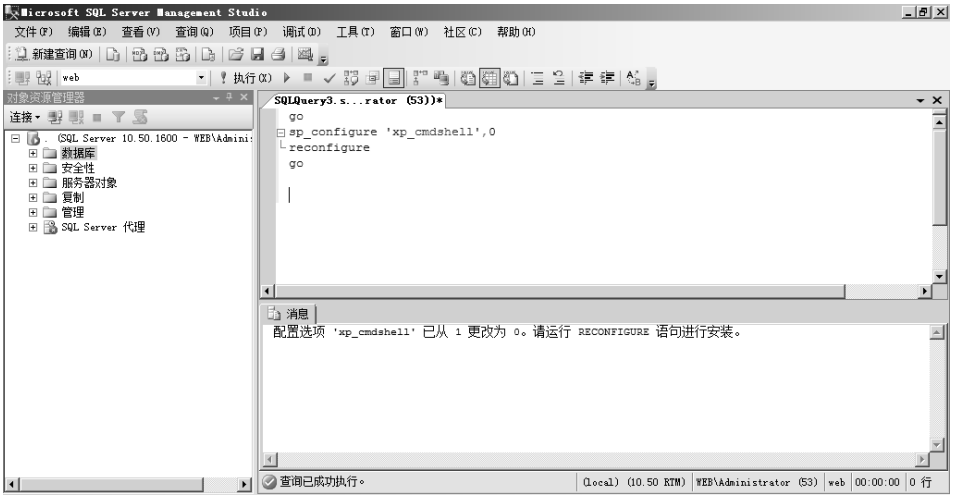

图 3-21　输入代码执行

✿代码

```
go
sp_configure 'xp_cmdshell',0
reconfigure
go
```

★　**任务验收**

通过本任务的实施，学会 MSSQL 的安全配置。

评价内容	评价标准	完成效果
MSSQL 的安全配置	在规定时间内，完成 MSSQL 的安全配置	

★　**拓展练习**

使用 SQL Server Configuration Manager 软件配置 MSSQLSERVER 协议属性，打开强行加密和隐藏实例，同时关闭不必要的连接协议。

任务 3　MSSQL 数据库的备份与还原

★　**任务描述**

学校采用 Microsoft SQL Server 2008 作为数据库系统为校园管理系统提供数据服务。技术人员已对当前系统中引入备份机制，对数据做好相应的保护措施，使得数据库被破坏后损失降到最低。现在需要网络安全工程师小张对数据库系统进行安全加固，保证数据库的安全。

微课 30

★　**任务分析**

对数据库备份使用完整备份和差异备份相结合的方式，设置维护计划任务可以自动进

行备份任务执行。数据库的备份应该在数据业务流量少时（夜间或清晨）进行。备份数据需留存时间应遵循应用业务要求和所在单位的等保规定。

✿知识链接

等保三级系统应用与数据安全部分内容如下。

1．备份和恢复

（1）应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；

（2）应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；

（3）应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

（4）应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

2．数据安全要求

数据安全要求是要求完备的灾难恢复计划和配套资源。

（1）完全备份至少每天一次，不过目前基本都是实时的，除了热备还有场外冷备份，也是至少一天一次，不过可以放松到一周以内，一般都会算符合；

（2）要求异地备份，明确规定距离至少 100 公里；

（3）和网络安全部分重复，要求系统所在网络环境的冗余性，双线双节点的结构；

（4）这里就是要双活或者热站点，都是包含在 DRP 中的资源；此外测评的时候还会考察每年是否有进行灾难恢复的演练，标准中虽然没有明确提出，但是也会作为检查的一项。

★ 任务实施

1．创建备份设备，用于存储数据库备份文件。启动 Microsoft SQL Server Management Studio，展开【服务器对象】，选择【备份设备】，单击鼠标右键选择【新建备份设备】，如图 3-22 所示。

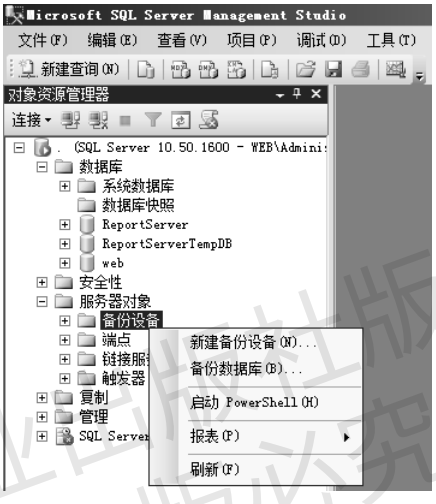

图 3-22　新建备份设备

2．指定设备名称和文件保存位置。在弹出的界面中输入设备名称，输入共享文件夹地址\\58.116.8.22\webbackup\webbackup.bak 作为文件保存位置，最后单击【确定】按钮，如图 3-23 所示。

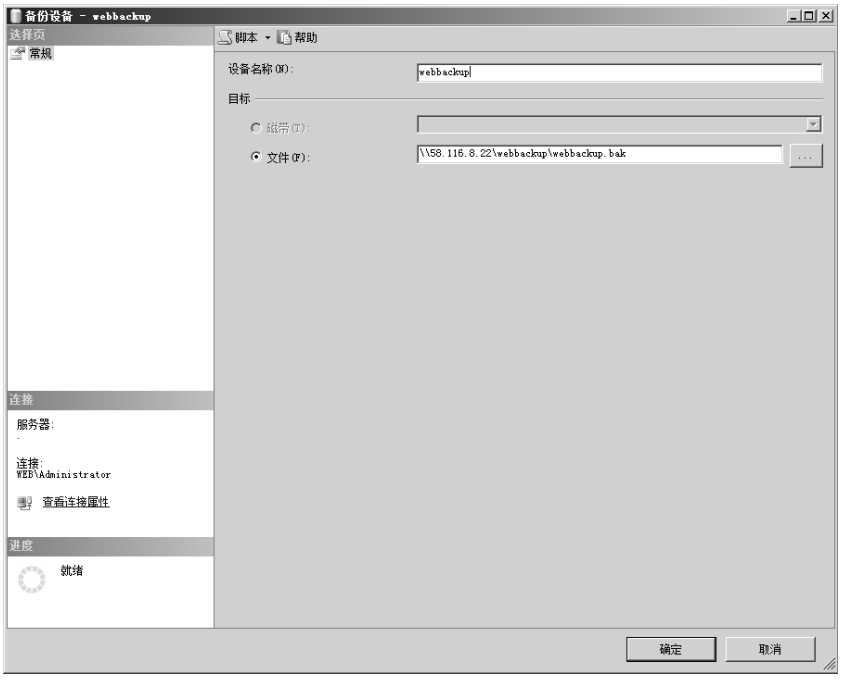

图 3-23　添加备份设备

3．选中需要备份的数据库，单击鼠标右键选择【任务】，弹出下一级菜单单击【备份】，如图 3-24 所示。

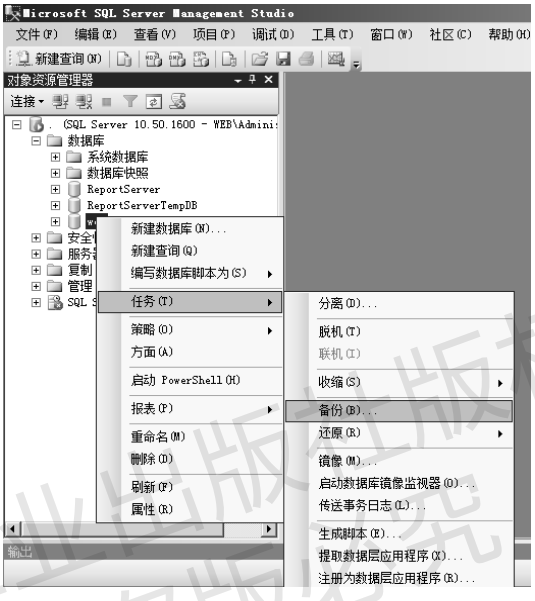

图 3-24　创建备份

4．弹出如图 3-25 所示界面，在【备份类型】下拉选项中选择【完整】，输入备份名称，后设置【备份集过期时间】为【7】天。这个日期用于覆盖备份集时检查用。超过 7 天的数据自动清理，如图 3-25 所示。

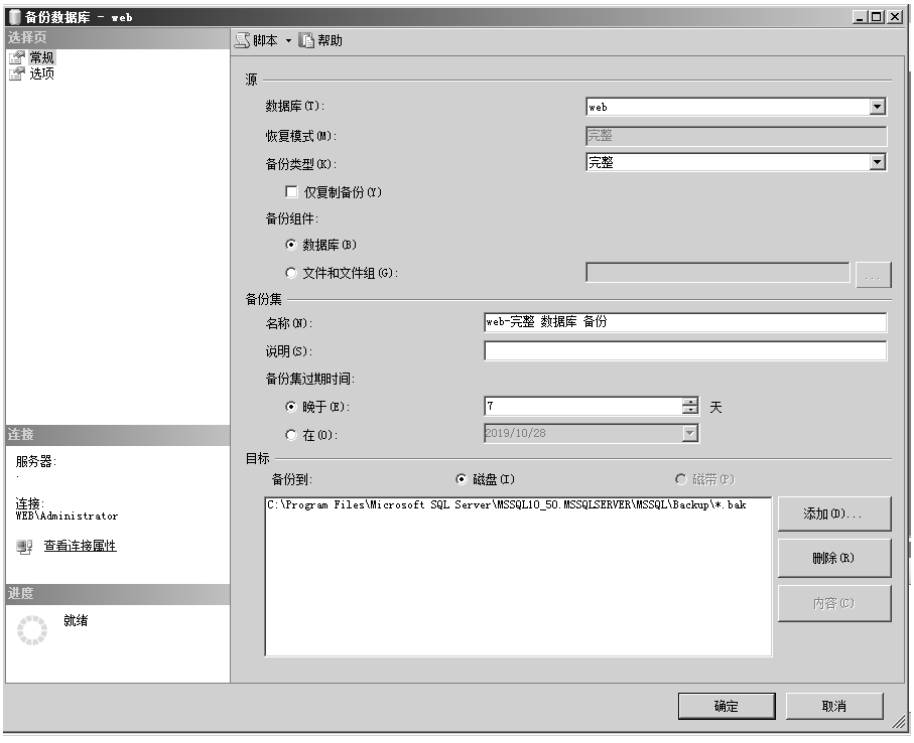

图 3-25　设置备份类型为完整

✿知识链接

SQL Server 备份方式有 4 种：

（1）完整备份，备份整个数据库，包括用户表、系统表、事务日志等，需要较大空间，备份时间长；

（2）差异备份，是完整备份的补充（需要先还原完整备份），比完整备份小、速度快，因此可以经常使用；

（3）事务日志备份，备份事务日志内容，可以使用事务日志备份将数据库还原到故障点，但是必须先还原完整备份，然后依次还原每个事务日志备份；

（4）文件和文件组备份，备份某些文件，可以分多次来备份数据库，避免大型数据库文件备份的时间过长，当数据库文件非常大时采用这个备份很有效。当数据库文件损坏，可以只还原被损坏的文件或文件组，从而加快了还原速度。

5．在【目标】设置中先单击【删除】按钮，删除默认备份位置。后单击【添加】按钮添加新的位置，如图 3-26 所示。

6．在弹出的【选择备份目标】界面中选择【备份设备】在下拉菜单中选择刚创建的设备后单击【确定】按钮，如图 3-27 所示。

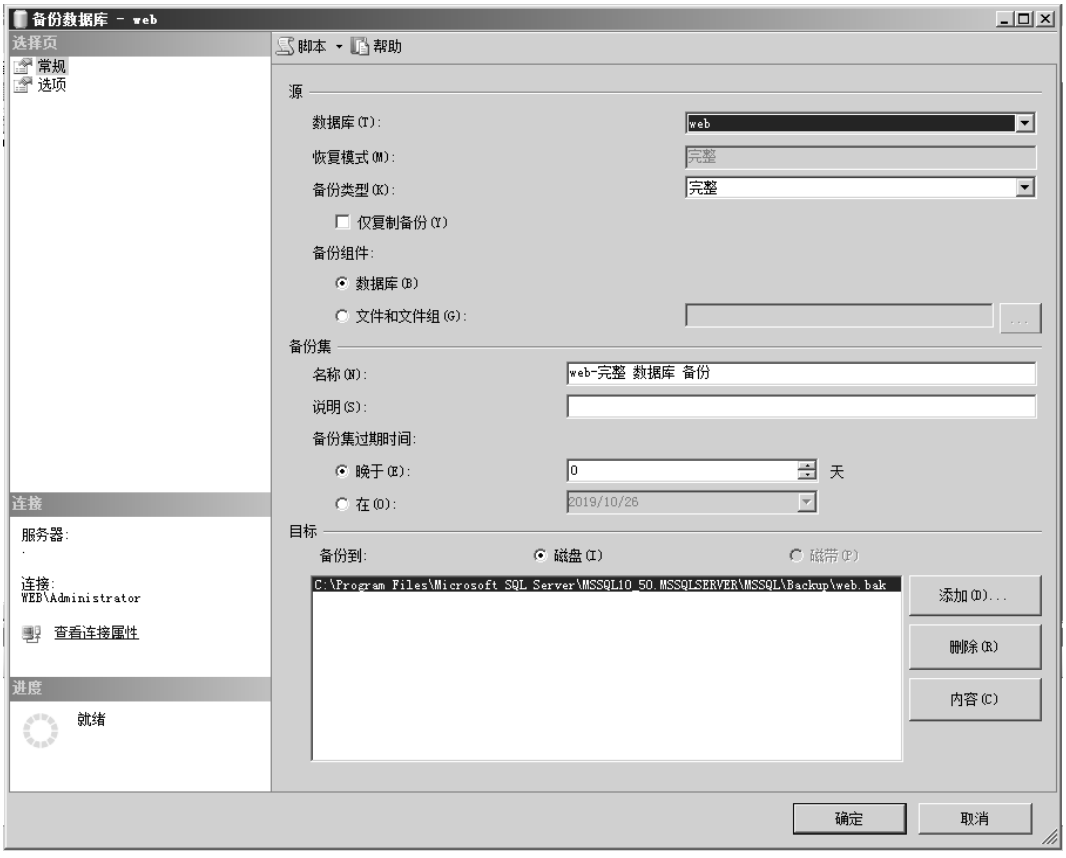

图 3-26　设置目标文件位置

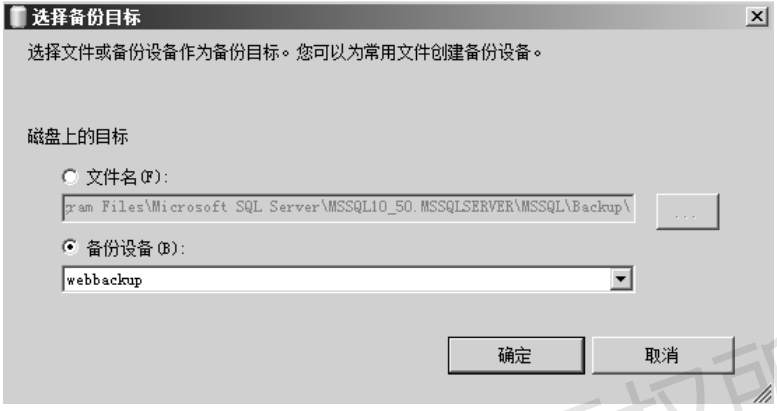

图 3-27　设置备份设备

7．设置完存储位置后，弹出如图 3-28 所示提示框，单击【确定】按钮，进行第一次手动备份。

8．创建一个完整数据库的维护计划，选择【维护计划】单击鼠标右键选择【新建维护计划】，如图 3-29 所示。然后输入计划名称。

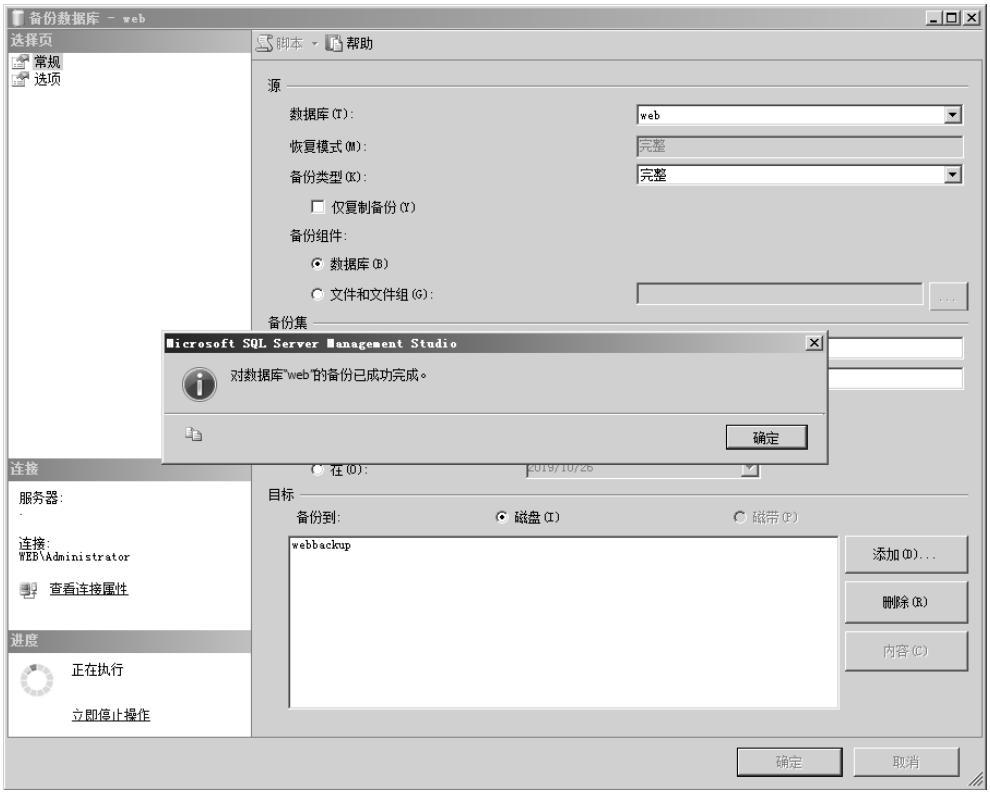

图 3-28　创建备份

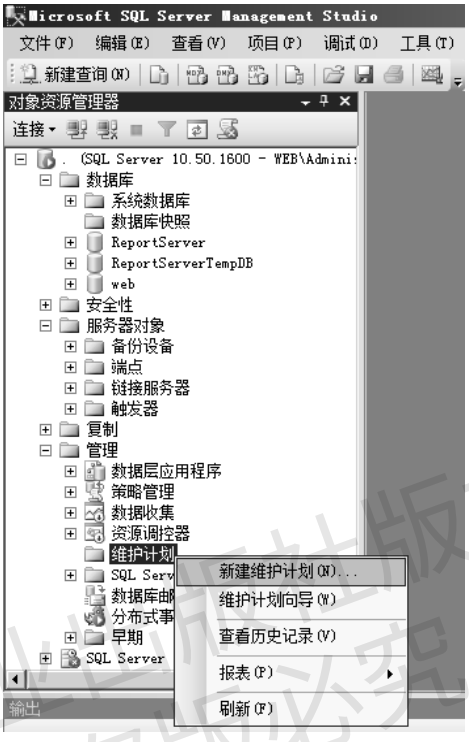

图 3-29　新建维护计划

9．单击左侧窗格【维护计划中的任务】中【“ 备份数据库 ” 任务】，如图 3-30 所示。

图 3-30　创建备份数据库任务

10．在【“ 备份数据库 ” 任务】中单击⊗标记，如图 3-31 所示。

11．在【“ 备份数据库 ” 任务】界面中，【备份类型】选择【完整】。【数据库】下拉菜单中单击【选择一项或多项】后，勾选需要备份的数据库，如图 3-32 所示。

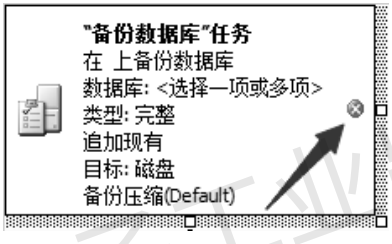

图 3-31　设置备份数据库任务

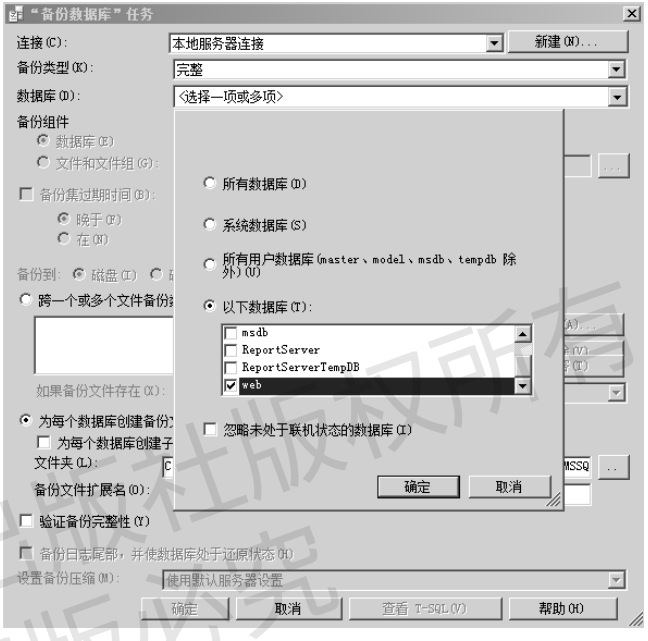

图 3-32　设置备份

12. 勾选【备份集过期时间】设置为【晚于】【7】天，单击【添加】按钮，如图 3-33 所示。在弹出的【选择备份目标】界面中选择刚刚创建的设备并单击【确定】按钮，如图 3-34 所示。

图 3-33　设置备份集过期时间

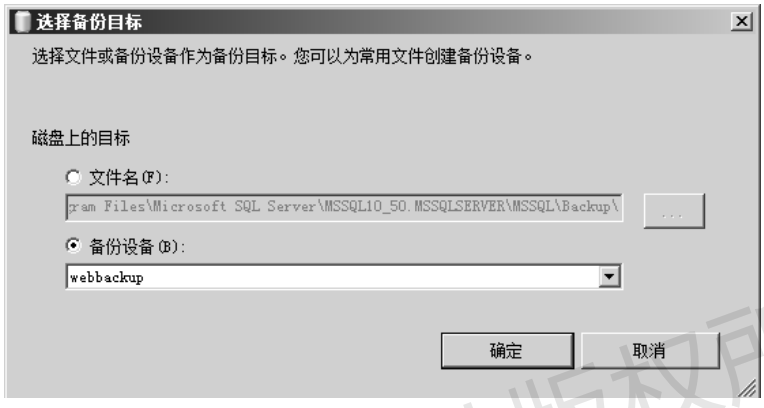

图 3-34　选择备份目标

13. 单击【确定】按钮，完成数据库维护任务，如图 3-35 所示。

14. 单击【作业计划属性】按钮，打开作业计划属性界面，如图 3-36 所示。

15. 设置计划类型，单击下拉菜单选择【重复执行】并勾选【已启用】。在【执行】下拉菜单中选择【每天】，在【每天频率】设置中，设置执行一次，时间为：凌晨零点。然后单击【确定】按钮保存作业计划属性设置，如图 3-37 所示。

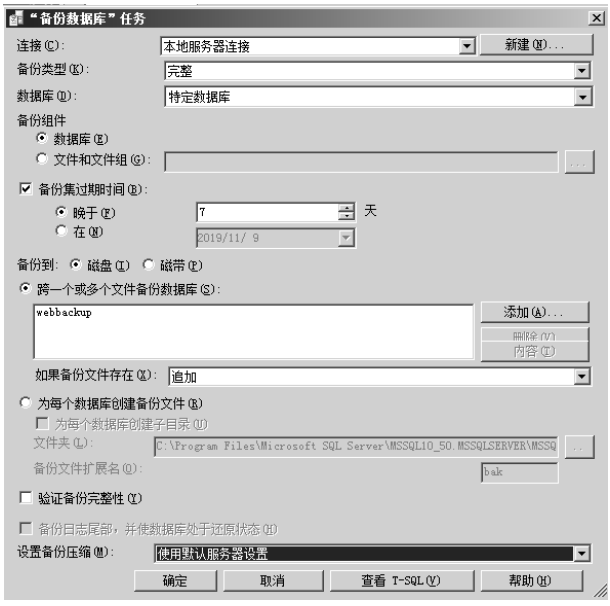

图 3-35　完整数据库维护任务创建完成

图 3-36　打开作业计划属性

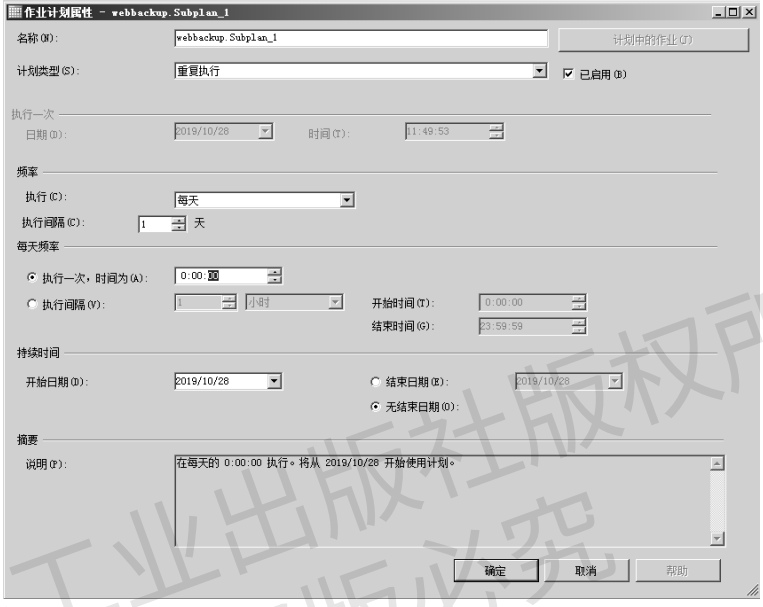

图 3-37　设置计划类型、每天频率

16. 创建一个差异数据库的维护计划。选择【维护计划】单击鼠标右键选择【新建维护计划】。并在右侧窗格中输入计划名称，如图 3-38 所示。

图 3-38　新建维护计划

17. 单击左侧窗格【维护计划中的任务】中【"备份数据库"任务】，在【"备份数据库"任务】中单击红色按钮，如图 3-39 所示。

图 3-39　创建备份数据库任务

18. 在【“备份数据库”任务】界面中【备份类型】选择【差异】，在【数据库】设置中，勾选【备份集过期时间】并设置为【晚于】【7】天，设置完成后界面如图 3-40 所示。再选择【跨一个或多个文件备份数据库】单击【添加】按钮。在如图 3-41 所示界面中选择需要添加的数据库，并单击【确定】按钮。

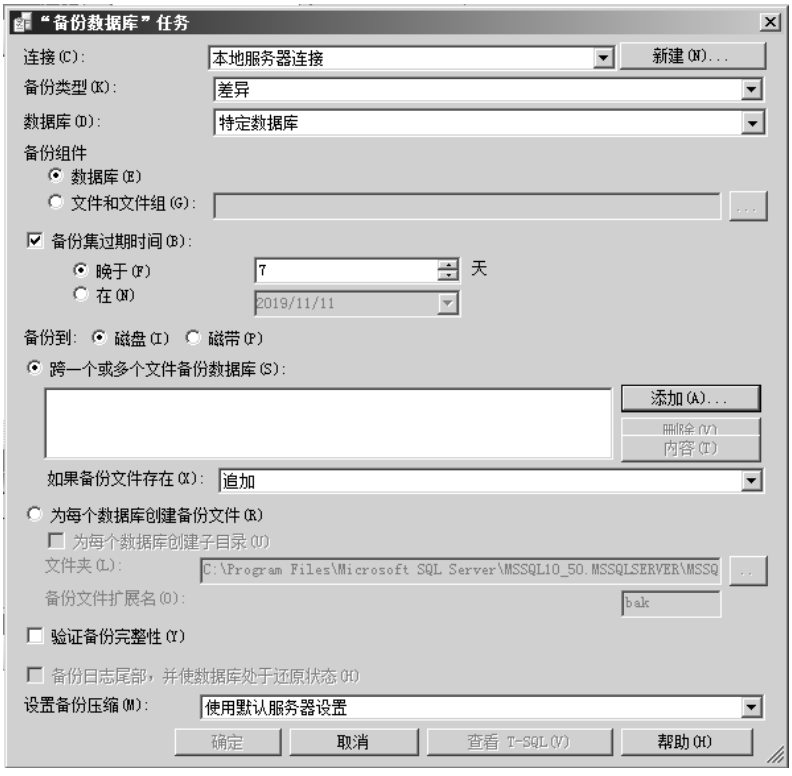

图 3-40　设置备份数据库任务

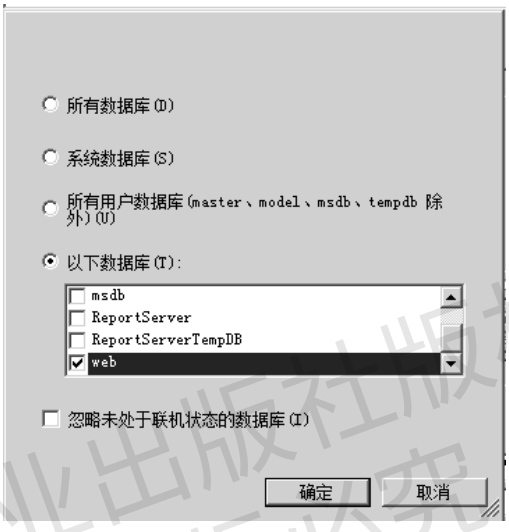

图 3-41　选择备份数据库

19. 选择【文件名】输入保存文件的地址，单击【确定】，如图 3-42 所示。

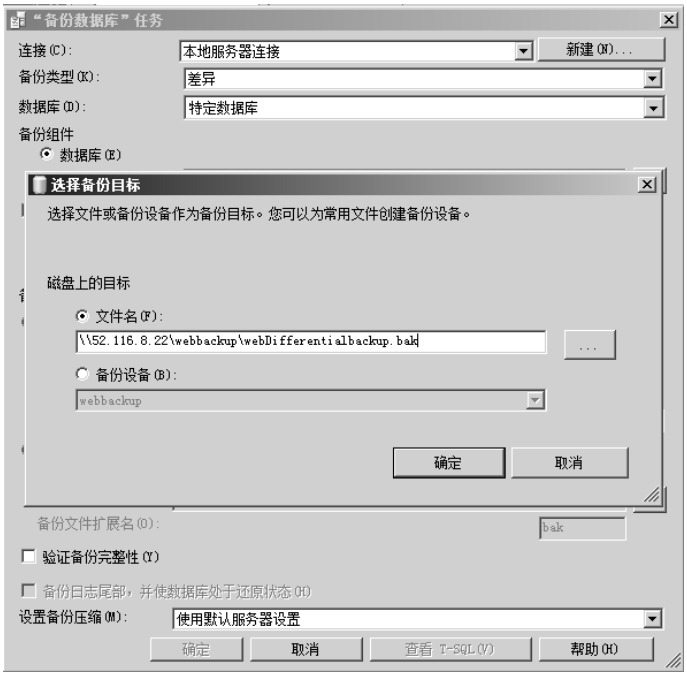

图 3-42　选择备份目标

20. 在【“备份数据库”任务】界面中，单击【确定】按钮，任务设置完成，如图 3-43 所示。

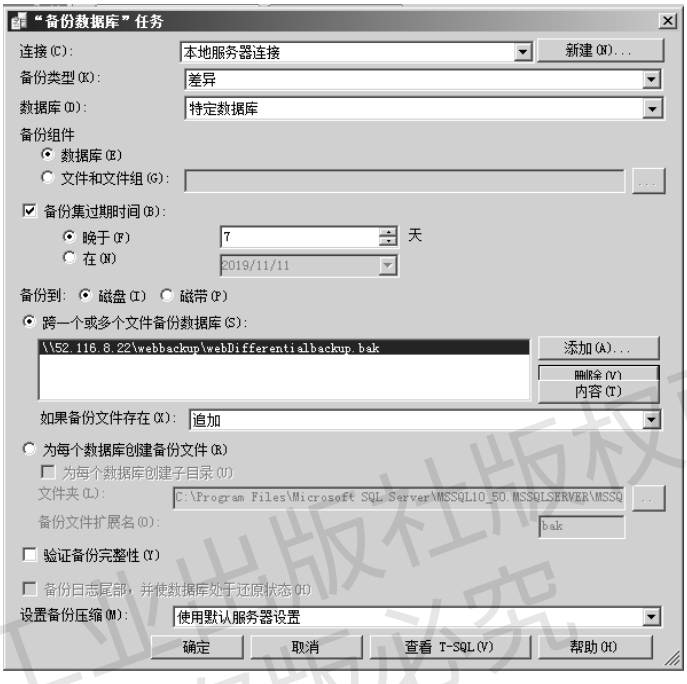

图 3-43　设置数据库备份任务完成

21．单击【作业计划属性】按钮，打开作业计划属性界面，如图 3-44 所示。

图 3-44　打开作业计划属性

22．设置【计划类型】，在下拉菜单中选择【重复执行】并勾选【已启用】。在【执行】下拉菜单中选择【每天】，在【每天频率】设置中，设置【执行一次，时间为 12:00:00】。然后单击【确定】按钮保存作业计划。单击关闭按钮退出维护计划，如图 3-45 所示。

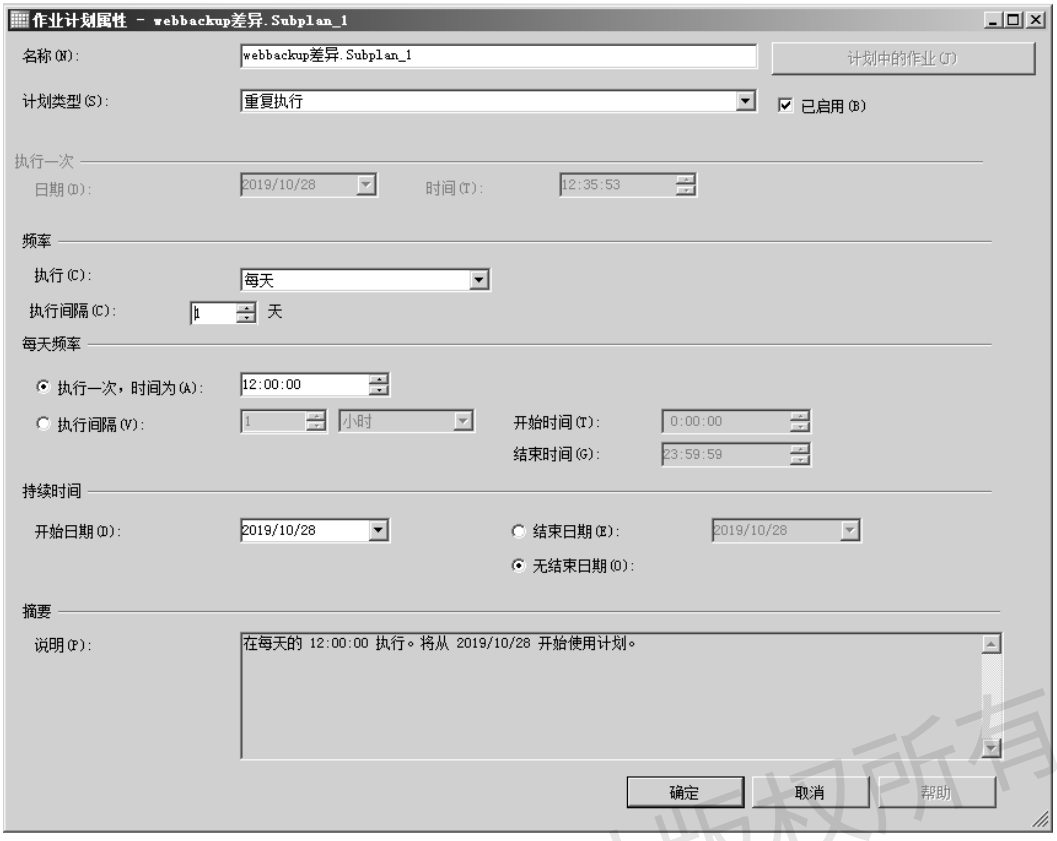

图 3-45　设置作业计划属性

23．当数据丢失需要还原时，通过备份还原数据库，选择要还原的数据，单击鼠标右键选择【任务】→【还原】→【数据库】，如图 3-46 所示。

24．在【常规】选项页中，勾选用于还原的备份集如图 3-47 所示。然后单击进入【选项】选项页。

图 3-46　选择数据库还原

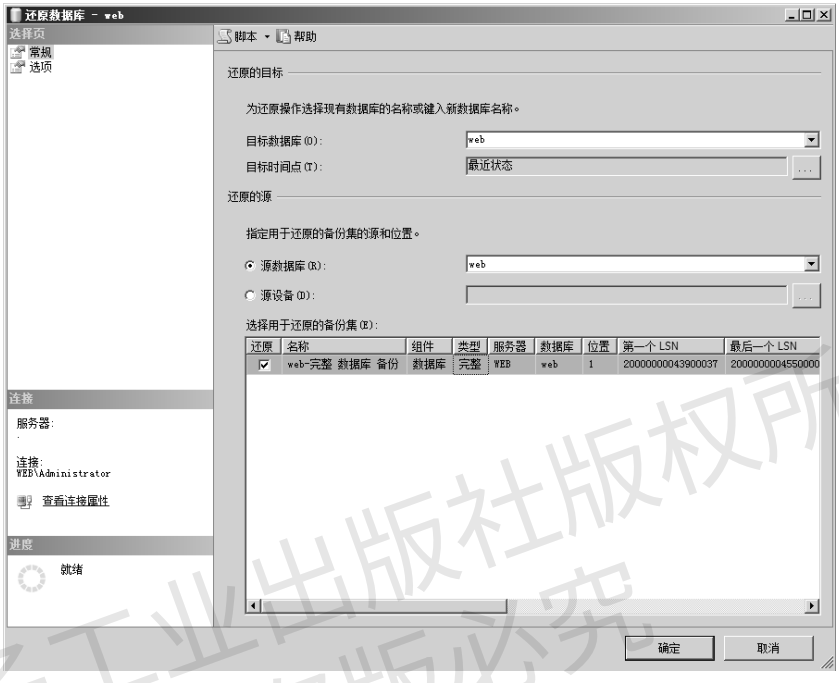

图 3-47　选择还原备份集

25．勾选【覆盖现有数据库】后单击【确定】按钮，进行还原，如图 3-48 所示。

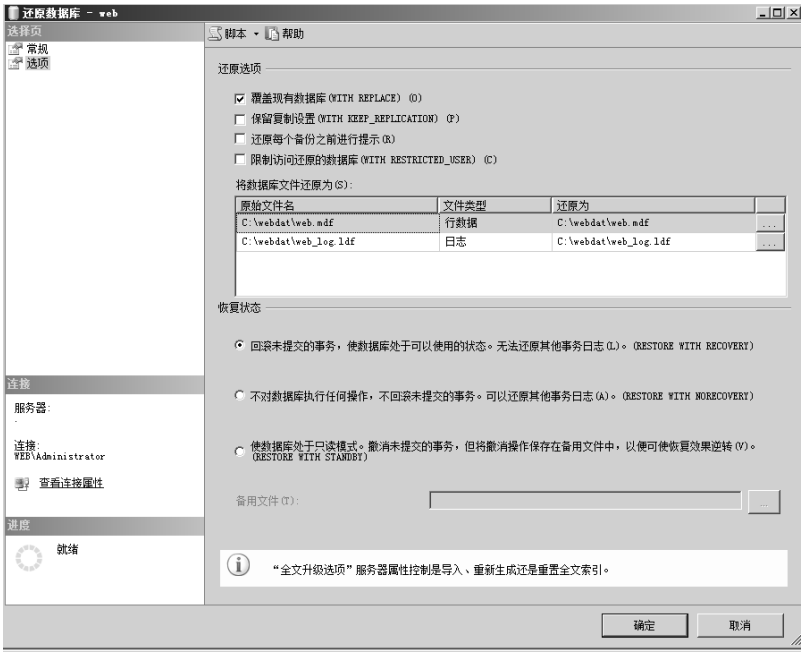

图 3-48　勾选覆盖现有数据库

✿经验分享

异地备份：防止本地磁盘损坏或者整个机房故障，对至关重要的数据，必须采取异地备份的办法。技术人员应定期检查磁盘空间。很多时候由于运维策略的不完善，同时又缺少巡检的过程，备份作业创建后没有及时维护，导致磁盘空间被占满，备份作业失败。

★　任务验收

通过本任务的实施，学会配置 MSSQL 数据库的备份与还原。

评价内容	评价标准	完成效果
MSSQL 数据库的备份与还原	在规定时间内，完成配置 MSSQL 数据库的备份与还原	

★　拓展练习

使用 Microsoft SQL Server Management Studio 软件备份 MSSQL 数据库，提升数据库的整体安全性。

项目习题

一、选择题

1．SQL Server 数据库有（　　）种登录身份验证模式。

A．1　　B．2　　C．3　　D．4

2．SQL Server 的备份方式有（　　）种。

A．4　　B．7　　C．2　　D．3

3．（　　）角色可以运行 BULK INSERT 语句。该语句允许从文本文件中将数据导入到 SQL Server 2008 数据库中，为需要执行大容量插入到数据库的域账号而设计。

A．bulkadmin　　B．dbcreator　　C．diskadmin　　D．SQLuser

4．在服务器中最高级角色是（　　）。

A．public　　B．securityadmin　　C．sysadmin　　D．sa

5．在 SQL Server 账户验证模式中，（　　）账户是内置的默认管理员账户，拥有最高的操作权限。

A．sa　　B．administrator　　C．root　　D．SQLuser

二、简答题

1．简述 Microsoft SQL Server 中两种登陆身份验证模式的区别。

2．简述 Microsoft SQL Server 服务器角色【public】和【sysadmin】功能。

三、操作题

数据库备份

1．创建 teacher 数据库，建立 teable1 和 teable2 表，字段自设，并创建数据。

2．创建维护计划，每周对 teacher 数据库进行一次完整备份，每天凌晨 0 点至 3 点进行差异备份。

单 元 总 结