# 电子科技大学信息与软件工程学院

**标 准 实 验 报 告**

**（实验）课程名称网络安全技术（国际班）**

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名： 赵则橦 学 号：2017221305013 指导教师：钟婷**

**实验地点：三教400 实验时间：2019/11/14**

**一、实验室名称：** 网络安全专业课程实验室

**二、实验项目名称：**实验一 SQLServer安全配置实验

**三、实验学时：** 2

**四、实验原理：**

数据库管理系统内置了安全配置，安全审计，数据库备份与恢复的相关功能。

**五、实验目的：**

1. 掌握SQLServer安全配置的关键技术。
2. 掌握SQLServer安全审计的关键技术。
3. 掌握SQLServer数据库备份与恢复的关键技术。

**六、实验内容：**

1. SQLServer安全配置
2. SQLServer安全审计
3. SQLServer数据库备份与恢复

**七、实验器材（设备、元器件）：**

PC微机一台、SimpleISES信息安全实验教学系统

**八、实验步骤：**

1. SQLServer安全配置

打开Windows实验台，运行Windows 2003系统；运行SQL Server 2000的“查询分析器”和“企业管理器”。

1. **使用安全的密码策略**
2. 查看不符合密码要求的账号

很多数据库帐号的密码过于简单，同系统密码过于简单是一个道理。对于sa更应该注意，同时不要让sa帐号的密码写于应用程序或者脚本中。健壮的密码是安全的第一步。同时养成定期修改密码的好习惯。数据库管理员应该定期查看是否有不符合密码要求的帐号。在如下图“查询分析器”窗口使用下面的SQL语句：

Use master

Select name,PassWord from syslogins where passWord is null

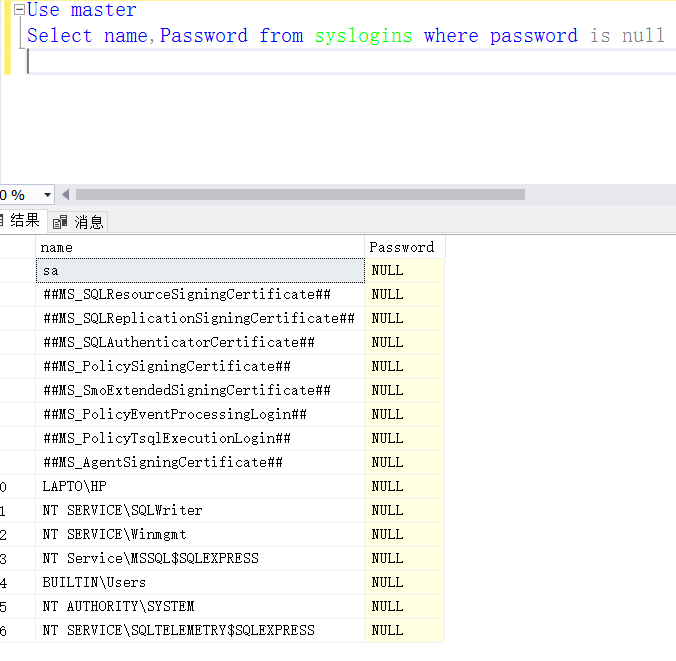


图2.2.1‑1

1. 设置SA 用户的密码

打开企业管理器，展开服务器组，然后展开服务器，如下图所示。

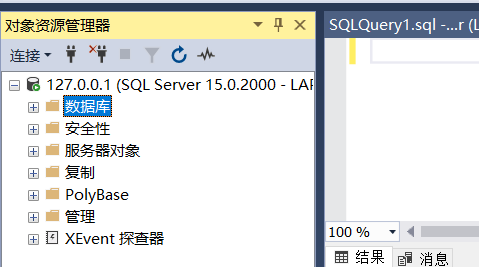


图2.2.1‑2

展开安全性，然后点击登录，如下图所示。

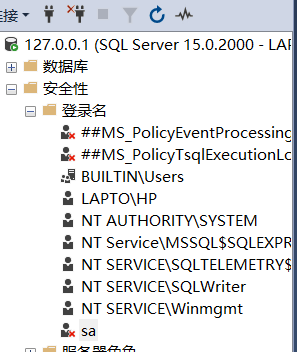


图2.2.1‑3

在细节窗格中，右键点击SA，然后点击属性，如下图所示。

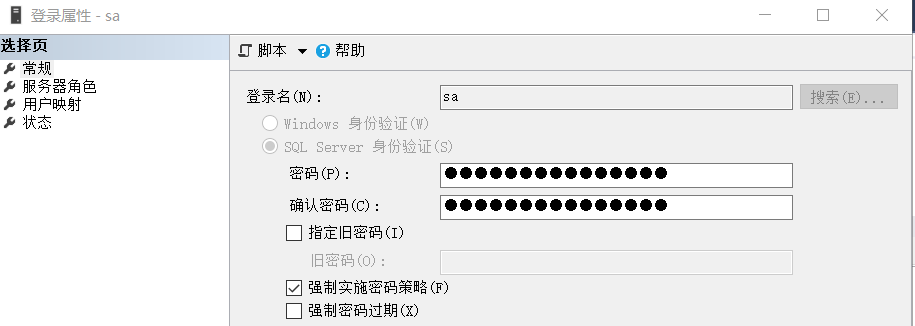


图2.2.1‑4

在密码方框中，输入新的密码1q2w3e4r5t6y，如图所示。

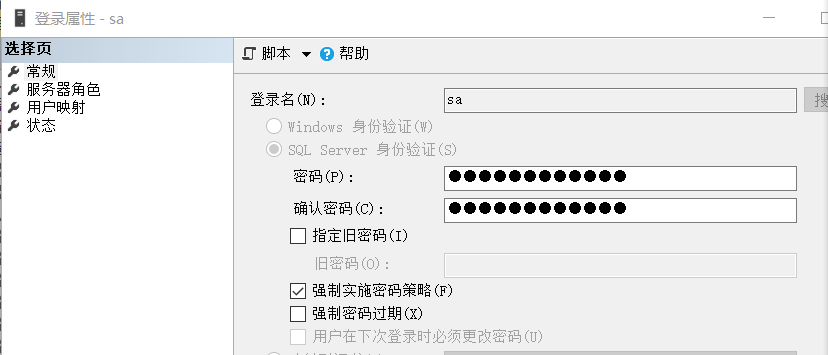


图2.2.1‑5修改sa的密码

1. **使用安全的帐号策略**

由于SQL Server不能更改sa用户名称，也不能删除这个超级用户，所以，我们必须对这个帐号进行最强的保护，当然，包括使用一个非常强壮的密码，最好不要在数据库应用中使用sa帐号，只有当没有其它方法登录到 SQL Server 实例(例如，当其它系统管理员不可用或忘记了密码)时才使用 sa。建议数据库管理员新建立一个拥有与sa一样权限的超级用户来管理数据库。安全的帐号策略还包括不要让管理员权限的帐号泛滥。

SQL Server的认证模式有Windows身份认证和混合身份认证两种。如果数据库管理员不希望操作系统管理员通过操作系统登录来接触数据库的话，可以在帐号管理中把系统帐号“BUILTIN\Administrators”删除，如下图所示。不过这样做的结果是一旦sa帐号忘记密码的话，就没有办法来恢复了。

很多主机使用数据库应用只是用来做查询、修改等简单功能的，请根据实际需要分配帐号，并赋予仅仅能够满足应用要求和需要的权限。比如，只要查询功能的，那么就使用一个简单的public帐号能够select就可以了。

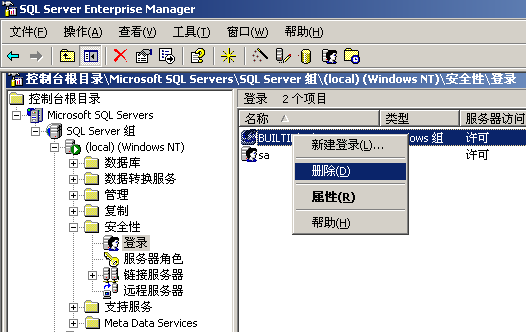


图2.2.1‑6

1. **查看数据库日志**

 定期查看SQL Server日志检查是否有可疑的登录事件发生，如下图所示，

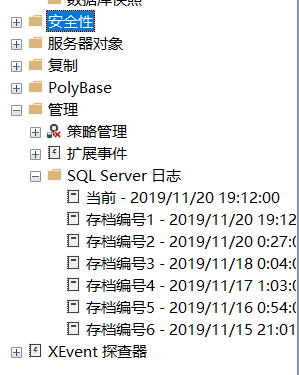


图2.2.1‑7

1. **管理SQL Server 内置存储过程xp\_cmdshell 控制系统**
2. 建立连接

打开sql 查询分析器，输入要访问的数据库地址(如实验台IP地址)，然后点击确定。如下图所示；利用SA弱口令登录SQLServer 服务。



图2.2.1‑8

1. 执行查询并查看结果

在新开的窗口中输入：xp\_cmdshell “dir c:”；并按 F5 执行查询。如下图所示。

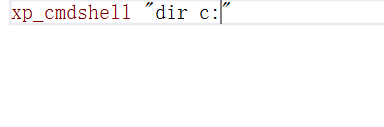


图2.2.1‑9执行查询

查看返回结果，如下图所示。

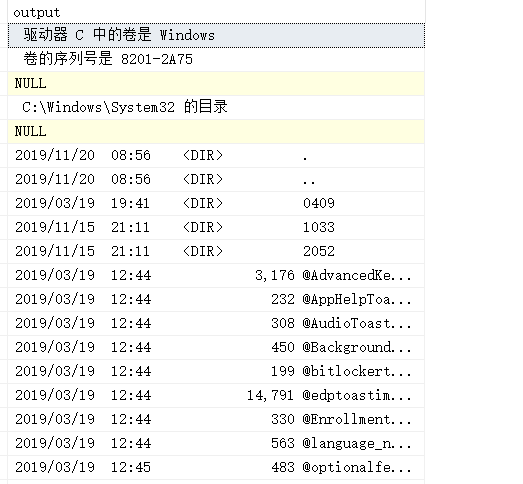


图2.2.1‑10返回结果

1. 试图建立新用户

输入：“xp\_cmdshell "net user Atest 654321 /add"”后将添加一个 mytest用户，密码为123456，如下图所示。

首先将windows使用的账户修改为本地账户，然后重启sql服务

参考：<https://www.cnblogs.com/jinanxiaolaohu/p/10715690.html>

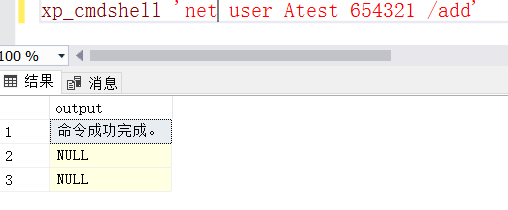


图2.2.1‑11建立新用户

输入“xp\_cmdshell"net user mytest"”查看用户列表，如下图所示。

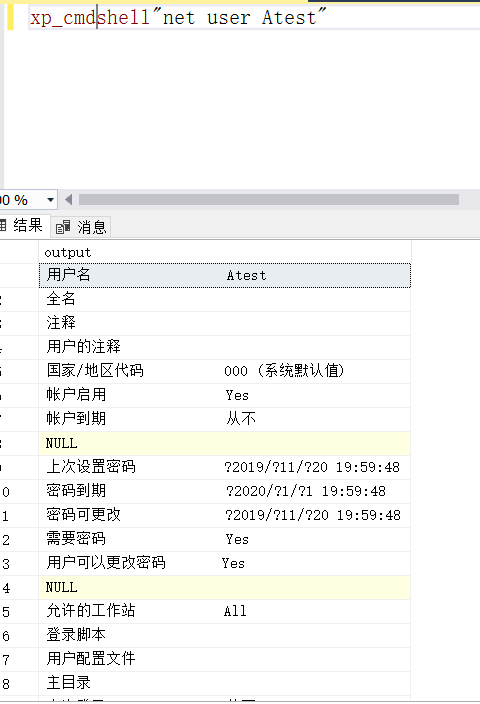


图2.2.1‑12用户列表

输入“xp\_cmdshell “net user Atest /delete””删除新添加的用户mytest，如下图所示：



图2.2.1‑13

1. 将新用户加入管理员组

输入“xp\_cmdshell "net localgroup administrators Atest/add"”，然后按 F5 执行查询，如下图所示。

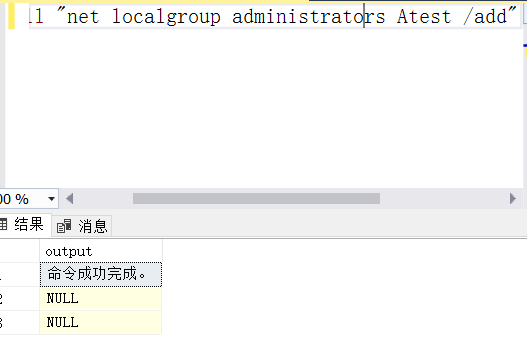


图2.2.1‑14将新用户加入管理员组

输入“xp\_cmdshell "net user mytest"”，检查修改结果，如下图所示。

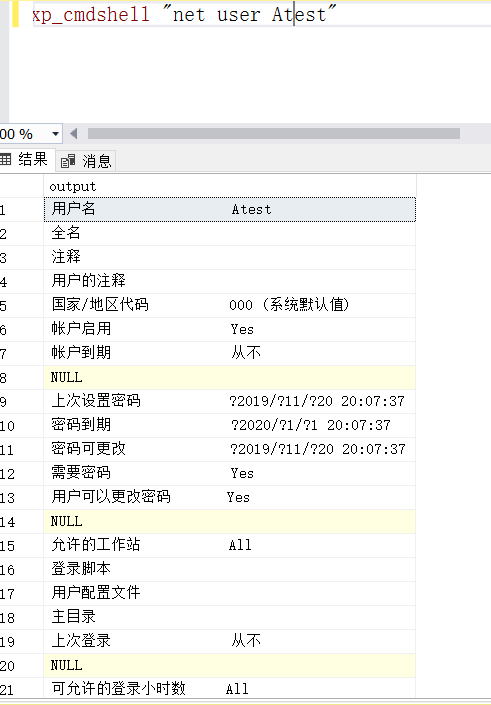
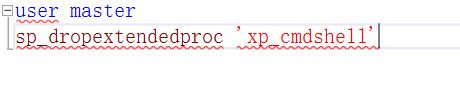


图2.2.1‑15将新用户加入管理员组

1. 删除xp\_cmdshell

数据库用户通过存储过程xp\_cmdshell，能调用到Windows系统的内置命令，对系统安全是极大的威胁。向数据库提交如下图所示的sql 语句，将xp\_cmdshell存储过程从系统中删除。



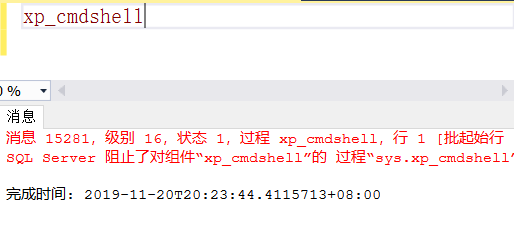


图2.2.1‑16从系统中删除xp\_cmdshell存储过程

验证是否删除成功，通过xp\_cmdshell 存储过程调用系统命令，看看是否删除成功。

恢复删除操作exec sp\_addextendedproc xp\_cmdshell ,@dllname =‘xplog70.dll'。

1. SQLServer安全审计

打开Windows实验台，运行Windows 2003系统；运行SQL Server 2000的“查询分析器”和“企业管理器”。

1. **在“事件查看器”中查看服务器的运行情况**

SQL Server 2000服务器的启动、关闭和暂停动作，都会产生一个事件记录，这个记录将会记在Windows的“事件查看器”中。

1. 选择计算机的“开始|设置|控制面板|管理工具|事件查看器|应用程序”，如下图所示。

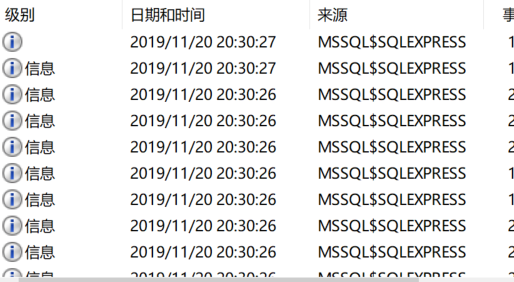


图2.2.1‑28

1. 双击其中一个事件，将弹出如下图所示的“事件属性”对话框，在这里可以看到事件的详细内容。



图2.2.1‑29

1. 在“事件查看器”里有可能记录了各种不同应用程序的事件记录，如果只想查看和SQL Server有关的事件记录的话，可以右击“应用程序”，在弹出的快捷菜单里选择“查看|筛选”。如下图所示的“应用程序属性”对话框。在这里可以筛选事件类型、事件来源、类别、事件时间等。

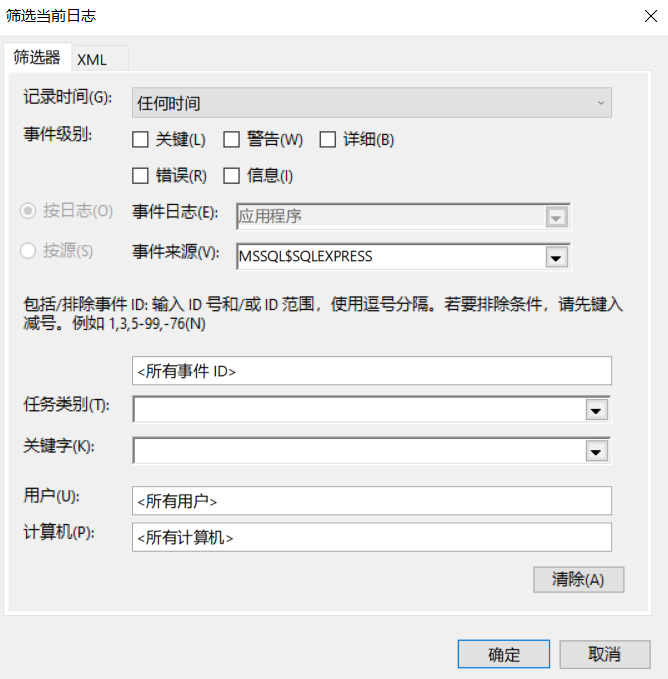


图2.2.1‑30

1. **通过日志查看器查看SQL Server日志**
2. 通过企业管理器窗口，查看日志，如下图所示。

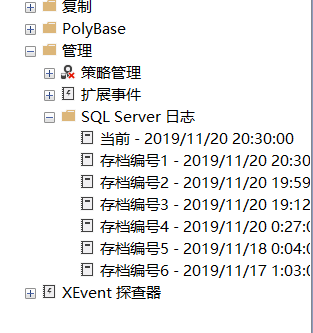


图2.2.1‑31

双击某一个日志存档，如下图所示，可以查看日志的具体内容。

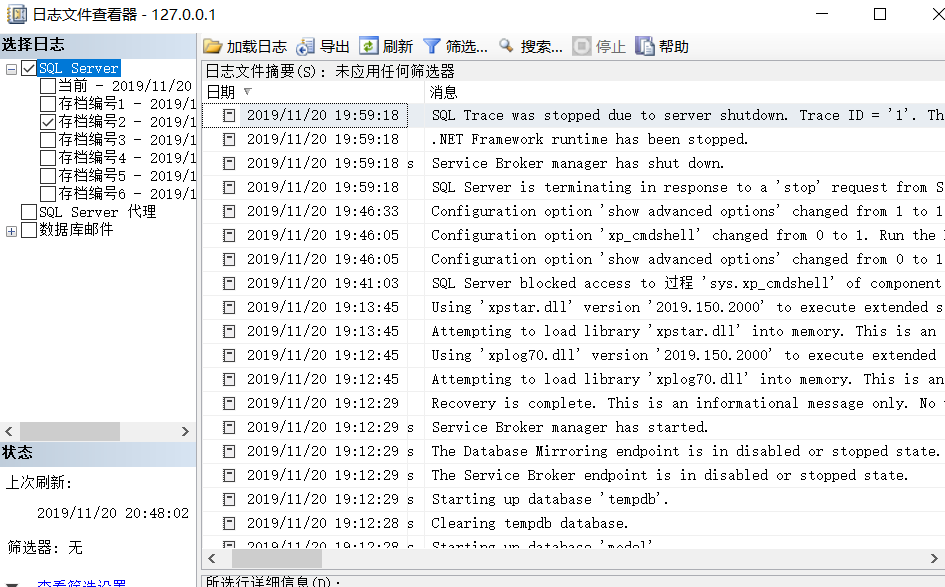
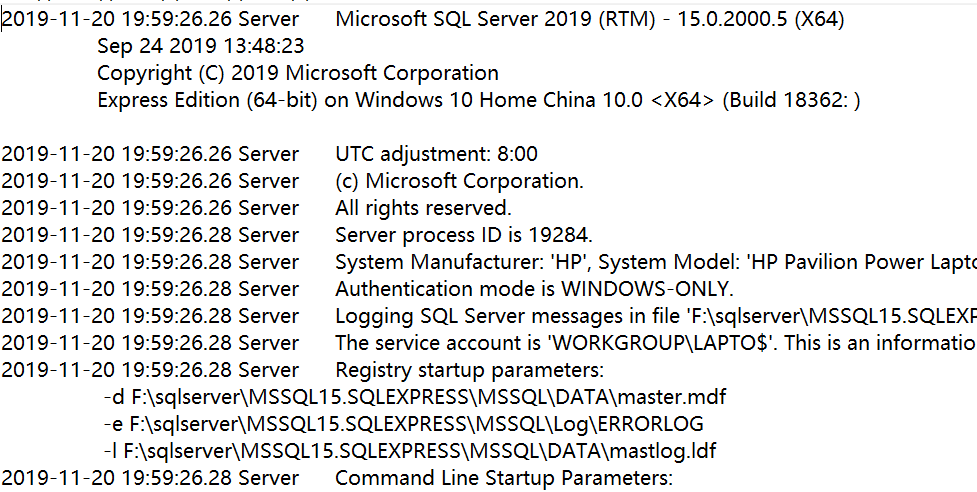


图2.2.1‑32

1. 在LOG文件夹中查看SQL Server错误日志

SQL Server 还会将错误日志存在其安装路径下的“……\Program Files\Microsoft SQL Server\MSSQL\LOG”目录中，文件名“ERRORLOG”和“ERRORLOG.X ”，其中“X”是数字。用记事本可以打开来查看。



1. **查看SQL SERVER的事务日志**
2. 通过dbcc sqlperf(logspace)命令，在查询分析器中，可以获取实例中每个数据库日志文件大小及使用情况，如下图所示。

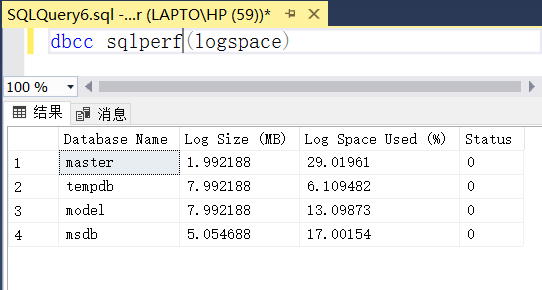


图2.2.1‑33

1. 查看具体数据库的事务日志

在SQL SERVER中，可以用下面的命令查看日志：

DBCC log ( { dbid|dbname} , [, type={ 0|1|2|3|4} ] )

参数：

Dbid or dbname - 任一数据库的ID或名字

type - 输出结果的类型:

0 - 最少信息(operation, context, transaction id)

1 - 更多信息(plus flags, tags, row length)

2 - 非常详细的信息(plus object name, index name,page id, slot id)

3 - 每种操作的全部信息

4 - 每种操作的全部信息加上该事务的16进制信息

默认 type = 0。

要查看MSATER数据库的事务日志可以使用DBCC log (master,type=4)命令，如下图所示。

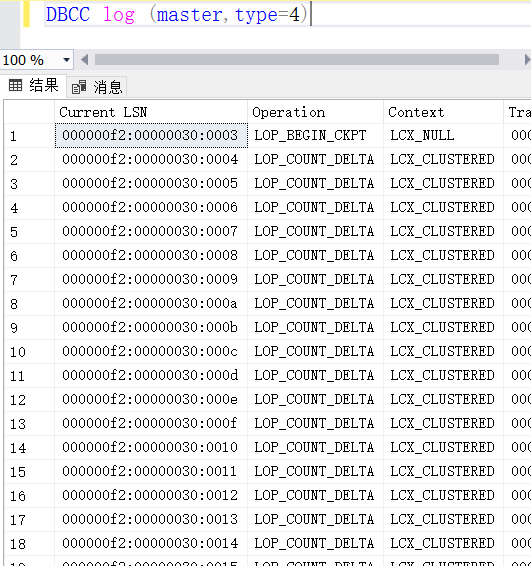
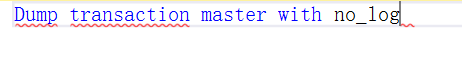


图2.2.1‑34

1. **SQL Server压缩日志及数据库文件大小**
2. 清空日志

Dump transaction 数据库名 with no\_log



1. 截断事务日志

Backup log 数据库名 with no\_log



1. 收缩数据库文件(如果不压缩，数据库的文件不会减小)

进入“企业管理器”，右键单击要压缩的库，选择“所有任务\收缩数据库”。

如下图所示。

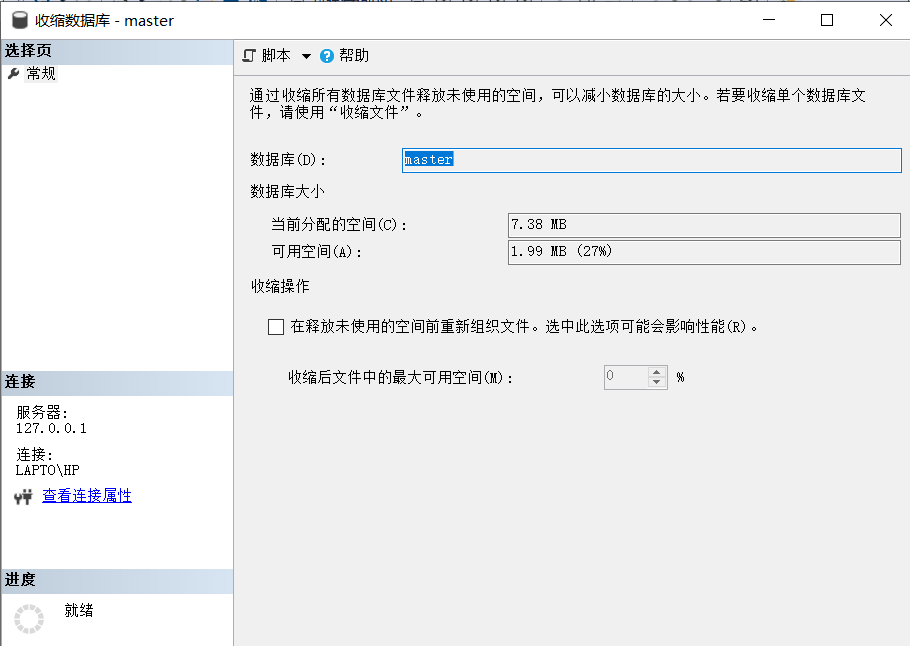


图2.2.1‑35

点击上图中的“收缩文件”选项下的“文件”按钮，如下图所示；在“收缩操作”选项中，“收缩文件至”里选择收缩至XXM，这里会给出一个允许收缩到的最小M数，直接输入这个数，确定；



图2.2.1‑36

1. 最大化的缩小日志文件(如果是sql 7.0，这步只能在查询分析器中进行)

分离数据库：

企业管理器 / 服务器 / 数据库 / 右键 / 分离数据库

在我的电脑中删除LOG文件

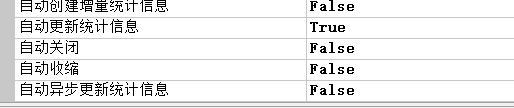
附加数据库：

企业管理器 / 服务器 / 数据库 / 右键 / 附加数据库

此法将生成新的LOG，大小只有500K

1. 自动收缩

选择“企业管理器|服务器”，右键“数据库”，选择“属性|选项”，选择“自动收缩”。



1. 设置日志大小

选择“企业管理器|服务器”，右键“数据库”，选择“属性|事务日志”；将文件增长限制为xM(x是你允许的最大数据文件大小) 。

1. **SQL Server的C2审核功能的命令**

命令如下：EXEC sp\_configure 'c2 audit mode', '1' reconfiguer。

启用C2审核模式并重新启动之后，SQ L Server自动在\MSSQL\Data目录下面创建跟踪文件。可以使用SQL Server Profiler查看这些监视服务器活动的跟踪文件。

SQL Server以128KB大小的块为单位把数据写入跟踪文件。因此，当SQL Server非正常停止时，最多可能丢失128 KB的日志数据。可以想象，包含审核信息的日志文件将以很快的速度增大。例如，某次实验只访问了三个表，跟踪文件已经超过了1MB。当跟踪文件超过200MB时，C2审核将关闭旧文件并创建新文件。每次SQL Server启动的时候，它会创建一个新的跟踪文件。如果磁盘空间不足，SQL Server将停止运行，直至我们为审核日志释放出足够的磁盘空间并重新启动SQL Server实例。在SQL Server启动的时候，可以使用-f参数禁用审核。

1. SQLServer数据库备份与恢复

打开Windows实验台，运行Windows 2003系统；运行SQL Server 2000的“查询分析器”和“企业管理器”。

1. **SQL Server 数据库备份**
2. 打开企业管理器，展开服务器组，然后展开服务器，如下图所示。

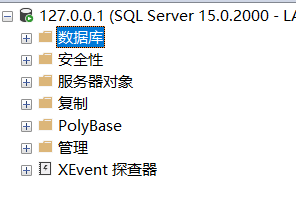


图2.2.1‑17展开服务器

1. 展开数据库，选中所要备份的数据库，单击鼠标右键，依次选择“所有任务”，“备份数据库”，如下图所示。

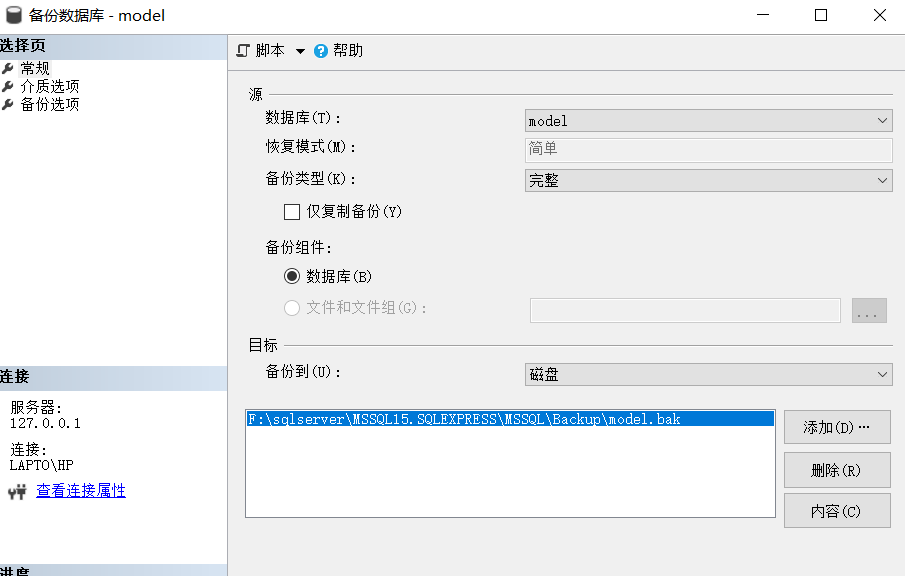


图2.2.1‑18备份数据库

1. 在弹出的对话框中，依次修改：“名称”、“备份方式”、“目的”、“重写方式”，最后点“确定”，如下图所示。

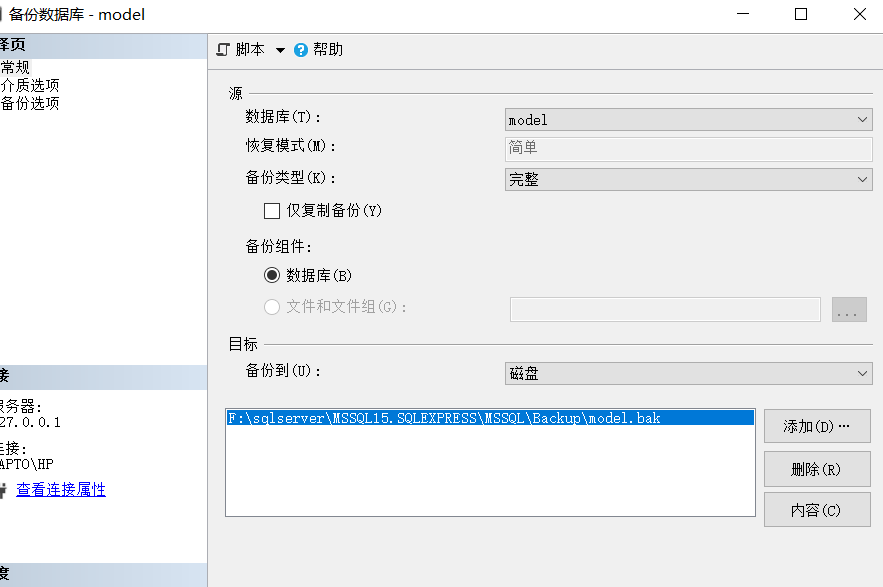


图2.2.1‑19备份数据库

1. 开始备份。
2. 最后备份完成。如下图所示。



图2.2.1‑21备份数据库

1. **SQL Server 数据库还原**
2. 打开企业管理器，展开服务器组，然后展开服务器，如下图所示。

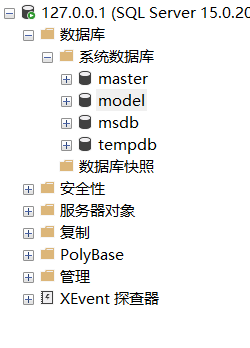


图2.2.1‑22展开服务器

1. 展开数据库，选中所要还原的数据库，单击鼠标右键，依次选择“所有任务”，“还原数据库”，如下图所示。

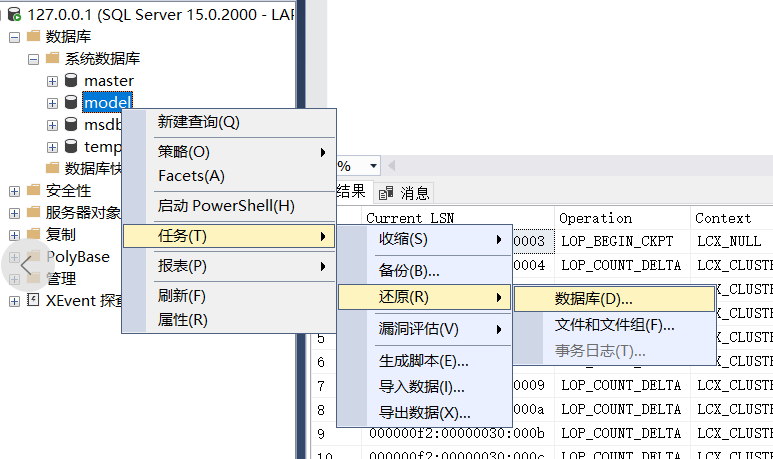


图2.2.1‑23还原数据库

1. 在弹出的对话框中，依次修改：“还原后的数据名”、“要还原的备份文件”，如下图所示。

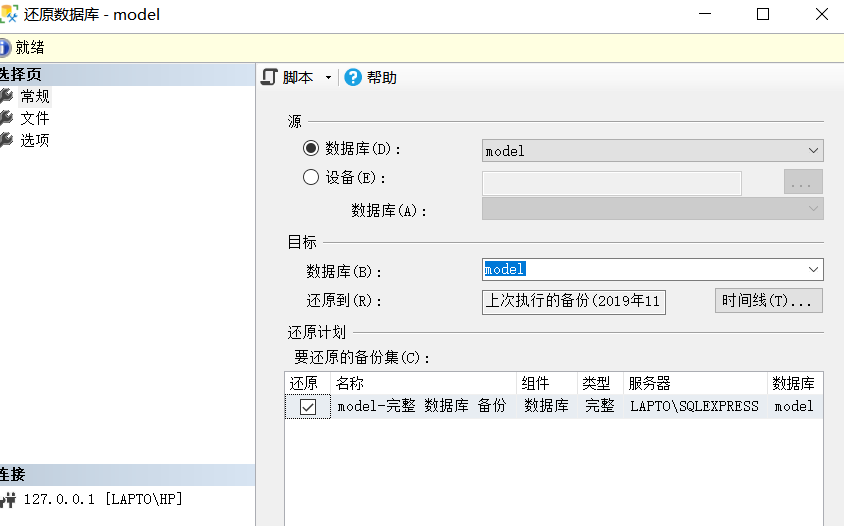


图2.2.1‑24还原数据库

1. 然后选择“选项”标签卡，选中“在现有数据库上强制还原”多选项，如下图所示。

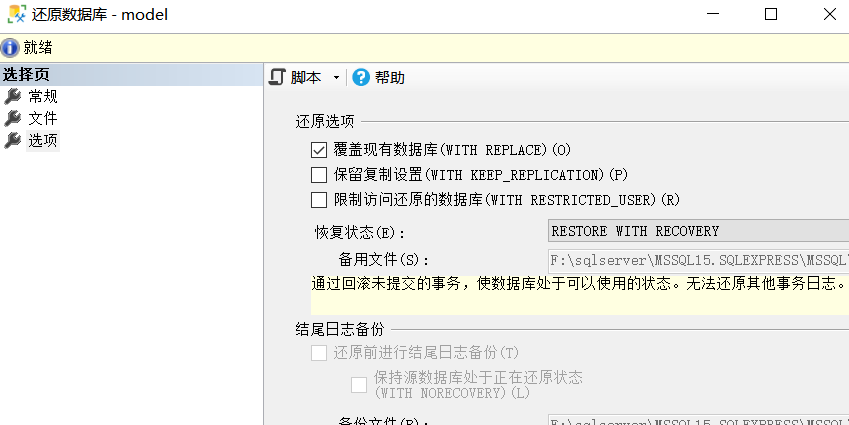


图2.2.1‑25还原数据库

1. 点击“确定”按钮开始还原，如下图所示。

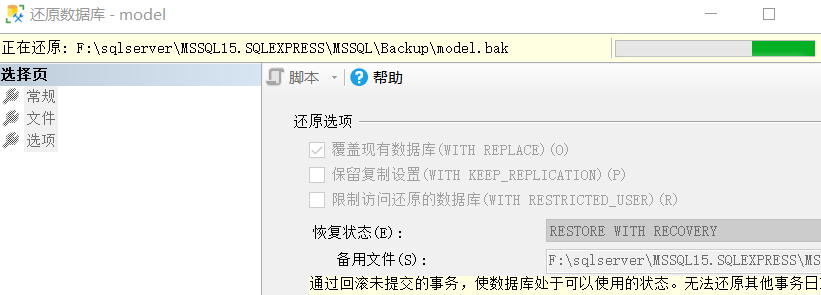


图2.2.1‑26还原数据库

1. 最后还原完成，如下图所示。



图2.2.1‑27还原数据库

**九、实验数据及结果分析：**

可以成功的实现SQLServer数据库的安全配置，实现安全审计功能以及数据库的备份与恢复。

**十、实验结论：**

SQLServer数据库内置了强大的安全配置，安全审计与数据库备份与恢复功能。

**十一、总结及心得体会：**

通过本实验对SQLServer数据库的安全配置有了进一步的了解。

**十二、对本实验过程及方法、手段的改进建议：**

无。

**报告评分： XX**

**指导教师签字：XXXX**