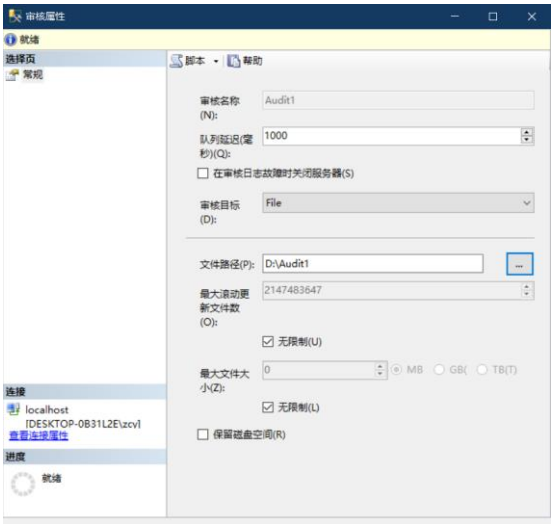
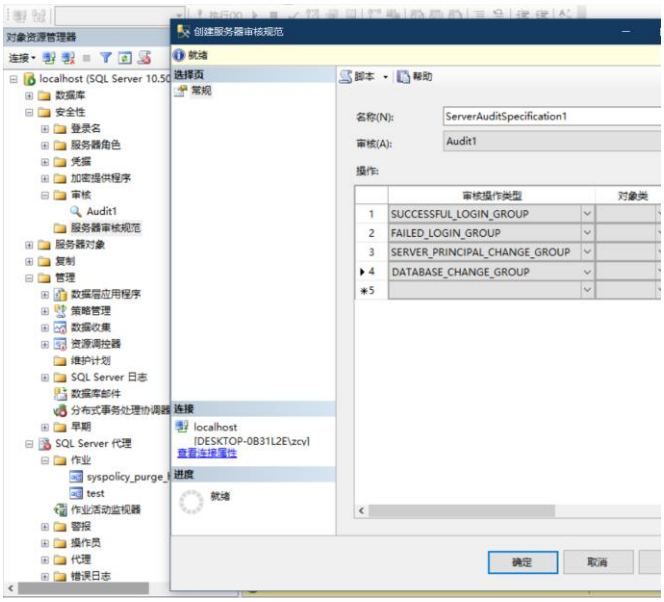
上机实验报告

课程名：_____ 指导教师：_____

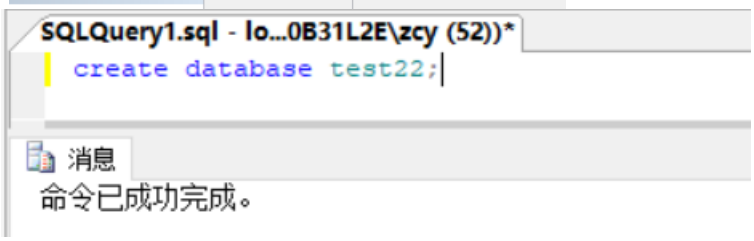
姓名		班级		实验得分	
		学号			
实验时间		实验地点			
实验主题	数据库审计				
实验目的	（1）通过实验，深入理解数据库审计主要功能、特点和机制。 （2）结合实际业务应用需求，在 SQL Server 数据库系统中，设计实现对数据库的操作审计，按需将发生在数据库中的各项行为进行记录，从而可进行相关的行为分析与追溯。 （3）深入理解数据审计对数据库安全所具有的重要作用。				
实验内容	1、环境准备 创建审核对象 Audit1，将审核操作对象保存在指定文件夹 SQLAudit 中。 2、服务器级审计 （1）为 Audit1 创建服务器级审核规范 ServerAuditSpecification1，对以下事件进行审计：①使用系统存储过程创建或删除登录名②登录名登录成功③登录名登录失败④创建、更改或删除任何数据库 （2）然后启用审核规范 ServerAuditSpecification1。 （3）执行（1）题中的①~④操作，然后查看审核对象 Audit1 中相应的审计记录。语法格式如下：select*fromsys.fn_get_audit_file('文件夹 SQLAudit 的路径',NULL,NULL) （4）修改审核规范 ServerAuditSpecification1，不再对④事件进行审计，但增加对“用户名更改登录密码”事件的审计（修改前先禁用该审核规范，修改完成后再启动），并验证是否修改成功（通过查看审核记录）。 3、数据库级审计 （1）为 Audit1 创建数据库级审核规范 DatabaseAuditSpecification2，对 STUDY 数据库中以下事件进行审计：①对 STUDY 数据库备份或还原操作②在 STUDY 数据库创建或删除用户操作③对 STUDY 数据库某一表中数据的增、删、改、查操作④对 STUDY 数据库某一存储过程的执行操作				

	（2）然后启用审核规范 ServerAuditSpecification2。 （3）对 Study 数据库执行(1)题中的①~④操作,然后查看审核对象 Audit1 中关于 Study 数据库的审计记录。语法格式如下： select*fromsys.fn_get_audit_file('文件夹 SQLAudit 的路径',NULL,NULL)WHEREdatabase_name='Study' （4）修改审核规范 ServerAuditSpecification2,仅对③类事件进行审计，但另外增加对“对 STUDY 数据库中特定角色架构中所有对象的 DML(创建、修改、删除)操作”事件的审计（修改前先禁用该审核规范，修改完成后再启动），并验证是否修改成功（通过查看审核记录）。
实验结果/实验结论	1. 环境准备  2. 服务器级别审计 


启用服务器审核规范
成功
1 总计
1 成功
0 错误
0 警告
详细信息(D):
操作
状态
消息
启用服务器审核规范 "ServerAuditS...
成功
关闭(C)

测试

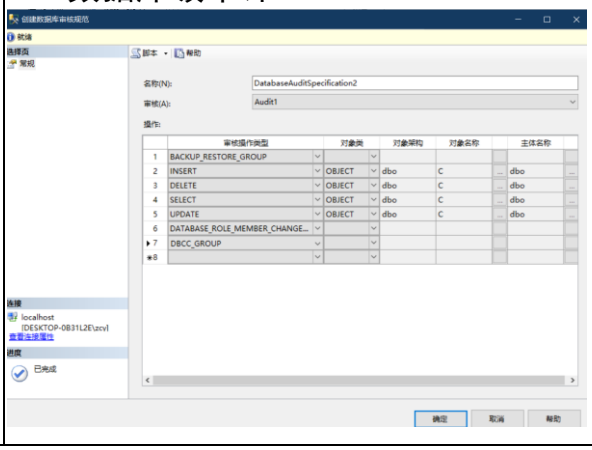

SQLQuery1.sql - lo...0B31L2E\zcy (52))*
create database test1;
EXEC sp_addlogin 'test1', 'test1', 'SM'
连接到服务器
Microsoft SQL Server 2008 R2
服务器类型(T):
数据库引擎
服务器名称(S):
localhost
身份验证(A):
SQL Server 身份验证
登录名(L):
test1
连接到数据库引擎
Microsoft SQL Server 2008 R2
数据库引擎
无法连接到 localhost。
其他信息:
用户 'test' 登录失败。 (Microsoft SQL Server，错误: 18456)
日志文件查看器 - localhost
选项(O) >>



可见更改以失效，为记录创建 database，记录了更改密码

✓	2021/5/3 10:35:45	10:35:45.0633333	DESKTOP-OB31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0	False	59	261	0	0	0
✓	2021/5/3 10:35:42	10:35:42.1141877	DESKTOP-OB31L2E	RESET PASSWORD	SQL LOGIN	1	True	0	False	59	261	1	275	0

3. 数据库级审计

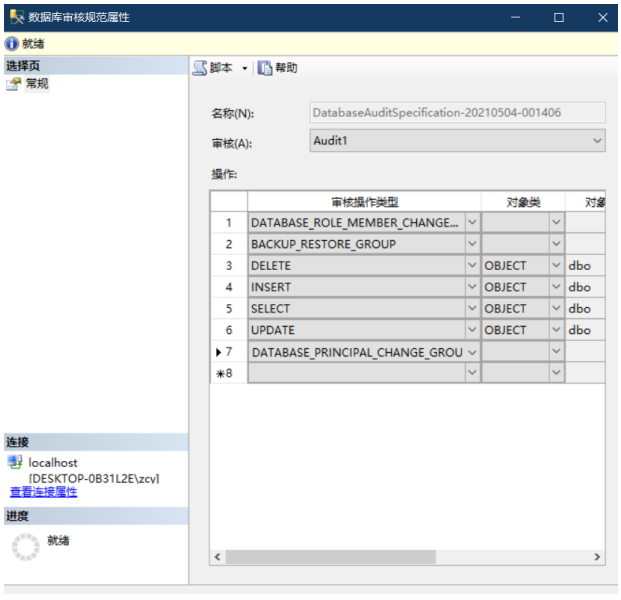


测试

```
use master
select * from C
backup database SM to disk = 'C:\Users\zcy\Desktop\tmp\1.db'
```

2021/5/3 16:25:07	16:25:07.1698798	DESKTOP-0B31L2E	DROP	SQL LOGIN	1	True	0
2021/5/3 16:24:59	16:24:59.2700000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:24:59	16:24:59.1600000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:24:32	16:24:32.8733333	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:24:32	16:24:32.8733333	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:24:28	16:24:28.0700000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:24:00	16:24:00.7666666	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:24:00	16:24:00.6533333	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:34	16:23:34.1200000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:34	16:23:34.1200000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:29	16:23:29.7966666	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:28	16:23:28.6133333	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:24	16:23:24.7666666	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:24	16:23:24.7600000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:24	16:23:24.7500000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:23:14	16:23:14.8496789	DESKTOP-0B31L2E	BACKUP	DATABASE	1	True	0
2021/5/3 16:22:26	16:22:26.8742373	DESKTOP-0B31L2E	SELECT	TABLE	1	True	1

删除与新增



删除之前创建的 U2

2021/5/3 16:29:55	16:29:55.7026930	DESKTOP-0B31L2E	DROP	SQL USER	1	True	0
2021/5/3 16:29:54	16:29:54.4233333	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:29:54	16:29:54.3000000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:29:49	16:29:49.7700000	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0
2021/5/3 16:29:45	16:29:45.6133333	DESKTOP-0B31L2E	LOGIN SUCCEEDED	LOGIN	1	True	0

实验心得	通过此处实验，我了解了何为数据库审计。数据库审计是以安全事件为中心，以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。它通过对用户访问数据库行为的记录、分析和汇报，来帮助用户事后生成合规报告、事故追根溯源，同时通过大数据搜索技术提供高效查询审计报告，定位事件原因，以便日后查询、分析、过滤，实现加强内外部数据库网络行为的监控与审计，提高数据资产安全。通过数据库审计，能增加应急响应能力。