

数据库系统实验

实验二：安全性语言实验

16 级计科教务 2 班

16337327

郑映雪

实验题目

自主存取控制实验

实验目的

掌握自主存取控制权限的定义和维护方法。

实验重点和难点

实验重点：定义角色，分配权限和回收权限。

实验难点：实验方案二实现权限的再分配和回收。

实验内容

定义用户、角色，分配权限给用户、角色，回收权限，以相应的用户名登录数据库验证权限分配是否正确。选择一个应用场景，使用自主存取控制机制设计权限分配。可以采用两种方案。方案一：采用 SYSTEM 超级用户登录数据库，完成所有权限分配工作，然后用相应用户名登陆数据库以验证权限分配正确性；方案二：采用 SYSTEM 用户登陆数据库创建三个部门经理用户，并分配相应的权限，然后分别用三个经理用户名登陆数据库，创建相应部门的 USER, ROLE，并分配相应权限。下面的实验报告示例，采用实验

方案一。验证权限分配之前，请备份好数据库；针对不同用户所具有的权限，分别设计相应的 SQL 语句加以验证。

实验操作和结果

（由于书上全是 kingbase 的语句，所以我查阅 SQL SERVER 的相同操作的语句）

创建用户

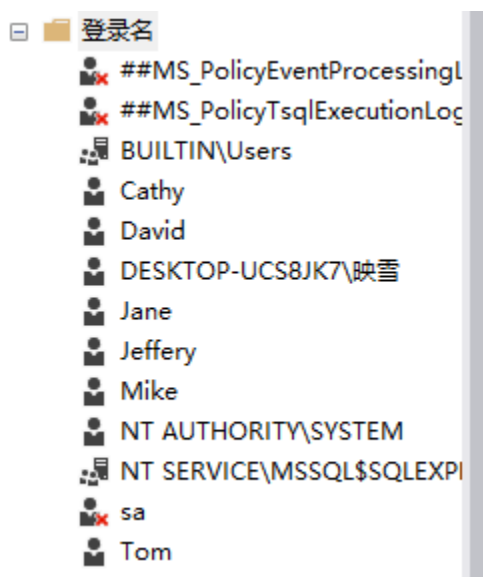
①为 David、Tom、Kathy 创建用户标识，要求具有创建用户或角色的权利。

②为 Jeffery、Jane、Mike 创建用户。

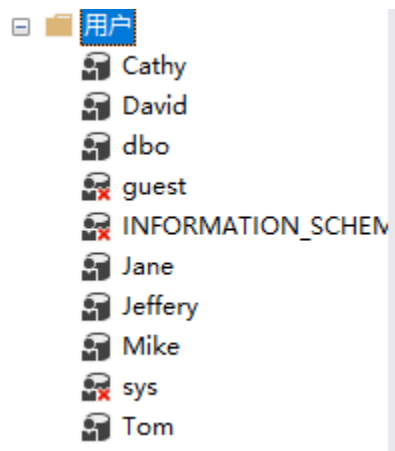
```
EXEC sp_addlogin 'David','123456','TPCH';
EXEC sp_addlogin 'Cathy','123456','TPCH';
EXEC sp_addlogin 'Tom','123456','TPCH';
EXEC sp_adduser 'Tom','Tom'
EXEC sp_adduser 'David','David'
EXEC sp_adduser 'Cathy','Cathy'
EXEC sp_addlogin 'Mike','123456','TPCH';
EXEC sp_addlogin 'Jeffery','123456','TPCH';
EXEC sp_addlogin 'Jane','123456','TPCH';
EXEC sp_adduser 'Mike','Mike';
EXEC sp_adduser 'Jeffery','Jeffery';
EXEC sp_adduser 'Jane','Jane';
```

创建成功：

登录名：



用户:



创建角色并分配权限

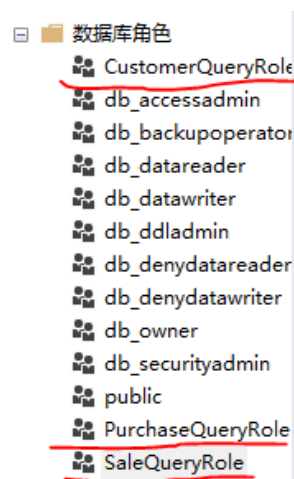
①为各个部门分别创建一个查询角色，并分配相应的查询权限。

```
EXEC sp_addrole 'PurchaseQueryRole';
GRANT SELECT ON Part TO PurchaseQueryRole;
GRANT SELECT ON Supplier TO PurchaseQueryRole;
GRANT SELECT ON PartSupp TO PurchaseQueryRole;

EXEC sp_addrole 'SaleQueryRole';
GRANT SELECT ON Orders TO SaleQueryRole;
GRANT SELECT ON Lineitem TO SaleQueryRole;

EXEC sp_addrole 'CustomerQueryRole';
GRANT SELECT ON Customer TO CustomerQueryRole;
GRANT SELECT ON Nation TO CustomerQueryRole;
GRANT SELECT ON Region TO CustomerQueryRole;
```

角色创建成功，结果如下:



数据库角色名称(N): CustomerQueryRole

安全对象(E):

Schema	名称	类型
dbo	Customer	表
dbo	Nation	表
dbo	Region	表

数据库角色名称(N): PurchaseQueryRole

安全对象(E):

Schema	名称	类型
dbo	Part	表
dbo	PartSupp	表
dbo	Supplier	表

数据库角色名称(N): SaleQueryRole

安全对象(E):

Schema	名称	类型
dbo	Lineitem	表
dbo	Orders	表

②为各部门创建职员角色，对本部门信息具有查看、插入权限。

```
EXEC sp_addrole 'PurchaseEmployeeRole';
GRANT SELECT,INSERT ON Part TO PurchaseEmployeeRole;
GRANT SELECT,INSERT ON Supplier TO PurchaseEmployeeRole;
GRANT SELECT,INSERT ON PartSupp TO PurchaseEmployeeRole;

EXEC sp_addrole 'SaleEmployeeRole';
GRANT SELECT,INSERT ON Orders TO SaleEmployeeRole;
GRANT SELECT,INSERT ON Lineitem TO SaleEmployeeRole;

EXEC sp_addrole 'CustomerEmployeeRole';
GRANT SELECT,INSERT ON Customer TO CustomerEmployeeRole;
GRANT SELECT,INSERT ON Nation TO CustomerEmployeeRole;
GRANT SELECT,INSERT ON Region TO CustomerEmployeeRole;
```

结果如下：

数据库角色名称(N): CustomerEmployeeRole

安全对象(E): 搜索(S)...

	Schema	名称	类型
	dbo	Customer	表
	dbo	Nation	表
	dbo	Region	表

数据库角色名称(N): PurchaseEmployeeRole

安全对象(E): 搜索(S)...

	Schema	名称	类型
	dbo	Part	表
	dbo	PartSupp	表
	dbo	Supplier	表

数据库角色名称(N): SaleEmployeeRole

安全对象(E): 搜索(S)...

	Schema	名称	类型
	dbo	Lineitem	表
	dbo	Orders	表

③为各部门创建一个经理角色，相应角色对本部门的信息具有完全控制权限，对其它部门的信息具有查询权。经理有权给本部门职员分配权限。

```
EXEC sp_addrolemember 'PurchaseManagerRole','David';
EXEC sp_addrolemember 'SaleManagerRole','Tom';
EXEC sp_addrolemember 'CustomerManagerRole','Cathy';
EXEC sp_addrolemember 'PurchaseEmployeeRole','Jeffery';
EXEC sp_addrolemember 'SaleEmployeeRole','Jane';
EXEC sp_addrolemember 'CustomerEmployeeRole','Mike';
```

权限分配结果如下：

数据库用户 - Cathy

选择页

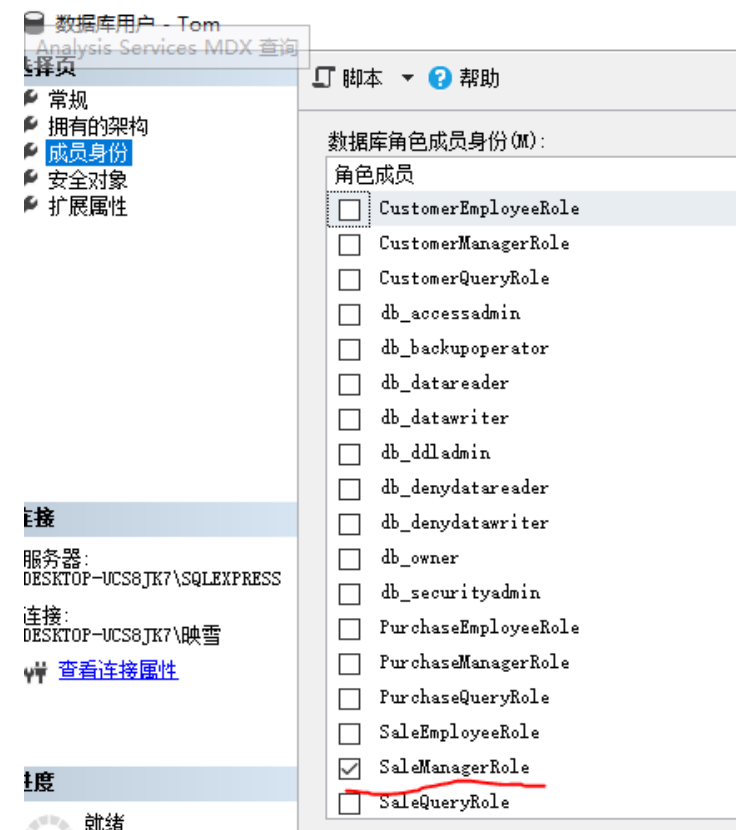
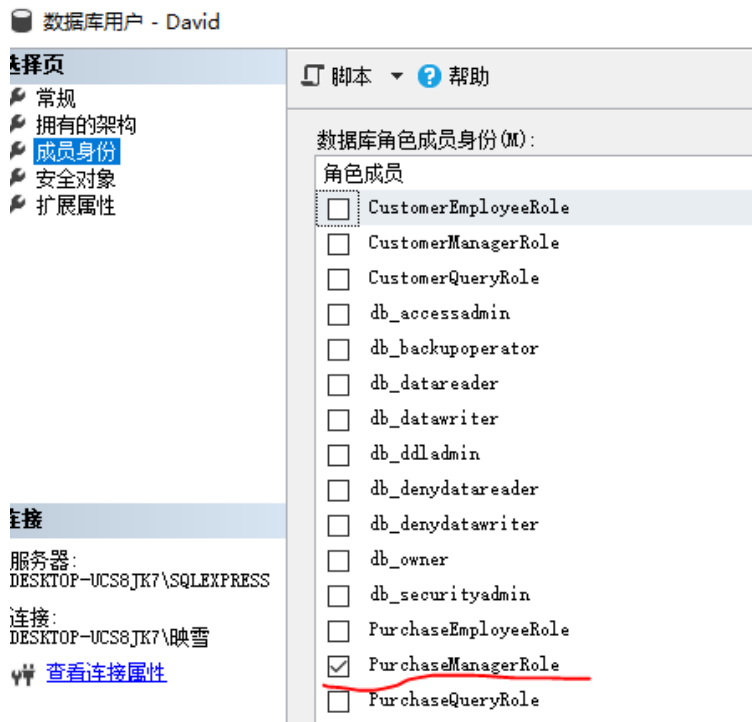
- 常规
- 拥有的架构
- 成员身份**
- 安全对象
- 扩展属性

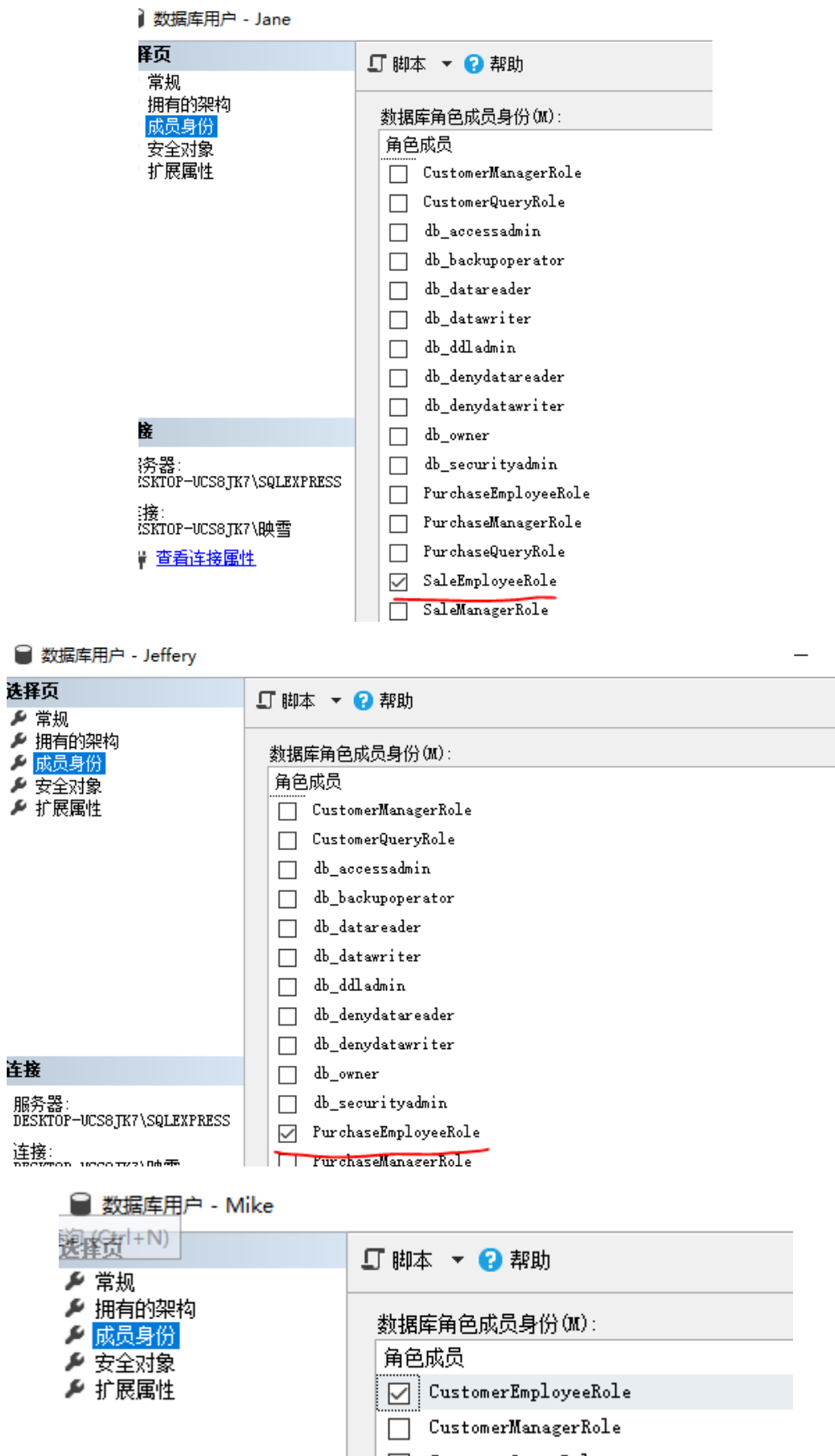
脚本 ? 帮助

数据库角色成员身份(M):

角色成员

- ☐ CustomerEmployeeRole
- ☒ CustomerManagerRole





测试分配权限的效果

①登录 David，输入查询语句。

```
SELECT * FROM Part;
```

查询结果如下，可以看到通过 David 的登录是可以成功查询的。

	partkey	name	mfg
1	1	竹炭空气清新篮	郑州市荣阳
2	2	竹炭净化包	江西赣州福
3	3	小炭包	郑州市蝶湖
4	4	无纺布鞋塞	河南省郑小
5	5	小挂包	江苏省无锡
6	6	居室除味宝	南通市疏小
7	7	学生干爽鞋垫	苏州阀门厂
8	8	冰箱除味包	淮阴市清江

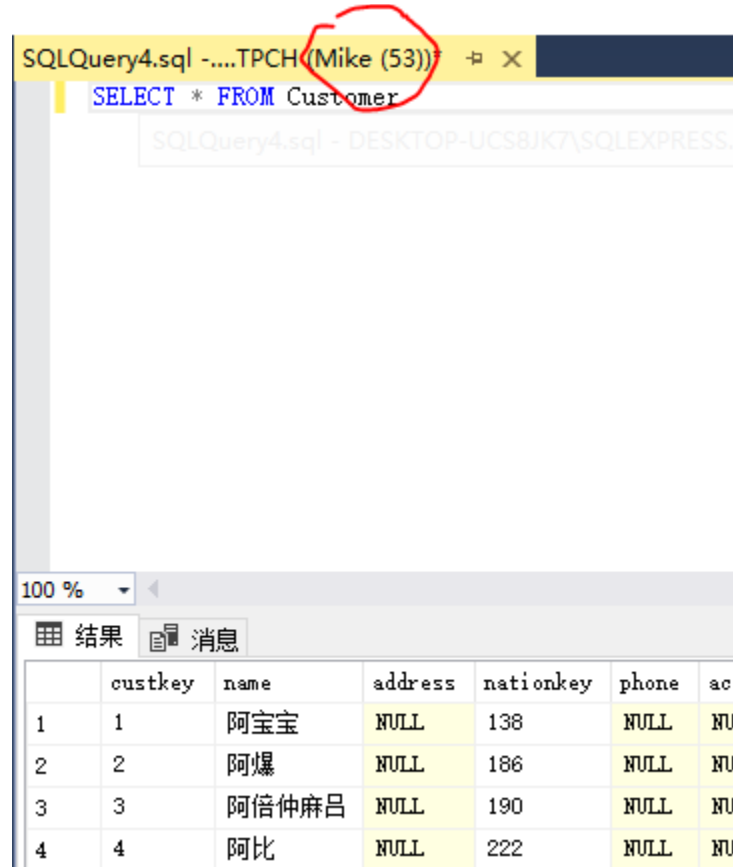
②输入删除语句。

```
DELETE FROM Orders WHERE orderkey=1;
```

结果如下，没有权限。因为当初授权的时候只授予了插入和查找权限，没有授予删除。

消息 229, 级别 14, 状态 5, 第 1 行
拒绝了对对象 'Orders' (数据库 'TPCH', 架构 'dbo') 的 DELETE 权限。

③登录 Mike，输入查询本部门表的语句，查询成功：



SQLQuery4.sql -TPCH (Mike (53))

```
SELECT * FROM Customer
```

SQLQuery4.sql - DESKTOP-UCS8JK7\SQLEXPRESS.

100 %

结果 消息

	custkey	name	address	nationkey	phone	ac
1	1	阿宝宝	NULL	138	NULL	NU
2	2	阿爆	NULL	186	NULL	NU
3	3	阿倍仲麻吕	NULL	190	NULL	NU
4	4	阿比	NULL	222	NULL	NU

但是查询别的部门的表时显示：

SQLQuery4.sql -TPCH (Mike (53))*

```
SELECT * FROM Orders
```

SQLQuery4.sql - DESKTOP-UCS8JK7\SQLEXPRESS:TPCH (Mike (53))*

100 %

消息

消息 229, 级别 14, 状态 5, 第 1 行
拒绝了对对象 'Orders' (数据库 'TPCH', 架构 'dbo')的 SELECT 权限。

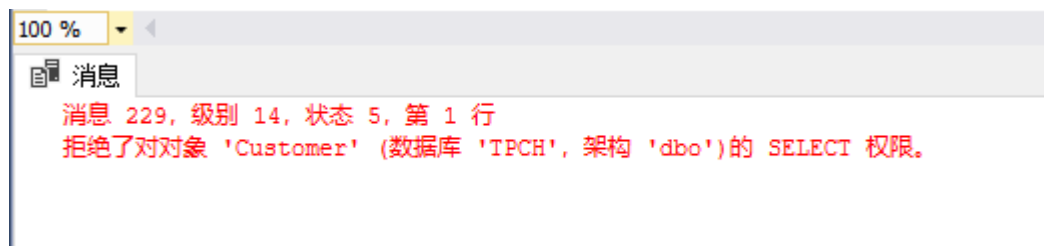
说明 Mike 的权限也授权成功了，只能查询本部门的几个表。

收回权限

收回对 Mike 对 Customer 的查询权限：

```
REVOKE SELECT ON Customer FROM Mike;
```

再登录 Mike 进行上一步中的查询：



由图可见验证成功。

实验总结

这个实验真的是一波三折……由于语句和理论书、实验书大都不一样，所以在查阅资料上花费了挺大一番功夫。听说使用 MySQL 的同学遇到了更大的麻烦，这样对比一下我当初选择使用 SQL Server 起码有与书上要求差不多的操作。

首先，书上明确说了这一节的语句为 KINGBASE 中的语句，不管是使用 sql server 还是 mysql 的同学都不能照搬书上的语句做实验了（其实这样也挺好的，可以在查资料的过程中对自己使用的 DBMS 的语句有一个熟悉的过程）。

在进行实验的过程中，主要出现了以下的一些困难：

①登录名和用户名的问题。在实验书上，只设置了用户名。而 SQL Server 用户名和登录名是独立分开的。需要用 EXEC sp_addlogin 进行设置，为了方便加上不混淆，我将用户名与登录名设置一致。

②语句差异。这个实验中的语句“不兼容性”更强了……不仅在语句上的表达不同，有些操作本身在 SQL Server 里也是不支持的（例如早已经不再被 SQL Server 推荐使用的 delete all），所以我将实验里的一些语句替换了，只力求实现本身要实现的效果。

③SQL Server 本身的操作不够娴熟。在更换登录用户的时候，由于我本地数据库我没有设置兼容性登录，所以一直登录不上 SQL 账户，我还一直以为是我代码写得有问题。后来在逐步排错之后才发现是我数据库本身没有设置好。

除了以上三个方面的问题，本次实验本身的难度还是不高的。在授权、收回权限的前后进行权限的测试是验证授权、收权是否成功的重要一步。通过这次实验，我对权限管理有了一个更深的认识，巩固了理论课上的内容。