数据库实验报告

实 验 人： 伍建霖 学 号： 20337251 日 期： 2022.10.22

院（系）： 计算机学院 专业（班级）： 网络空间安全

联系方式： QQ:773542531

实验题目： 2.1 自主存取控制实验

一. 实验目的

掌握自主存取控制权限的定义和维护方法

二. 实验内容和要求

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为正确。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录数据库以验证权限分配正确性;

方案二：采用 SYSTEM 用户登录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录数据库,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了实验方案一。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。

三. 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。

四. 实验工具

MySQL、SQL Server、Navicat

五. 实验过程

设有一个企业，包括采购、销售和客户管理等三个部门，

采购部门经理 user_pm， 采购员 user_pe;

销售部门经理 user_sm， 销售员 user_se;

客户管理部门经理 user_cm， 职员 user_ce。

该企业一个信息系统覆盖采购、销售和客户管理等三个部门的业务，其数据库为 TPC-H。针对此应用场景，使用自主存取控制机制设计一个具体的权限分配方案。

■ 注：在 MySQL 环境中，以 root 用户登录，运行以下语句（参阅 http://c.biancheng.net/view/7490.html ）。

(1)创建用户

①为采购、销售和客户管理等三个部门的经理创建用户标识，要求具有创建用户或角色的权利。

```
CREATE USER user_pm IDENTIFIED BY '123456';
GRANT CREATE USER on *.* to user_pm;
CREATE USER user_sm IDENTIFIED BY '123456';
GRANT CREATE USER on *.* to user_sm;
CREATE USER user_cm IDENTIFIED BY '123456';
GRANT CREATE USER on *.* to user_cm;
```

②为采购、销售和客户管理等三个部门的职员创建用户标识和用户口令。

```
CREATE USER user_pe IDENTIFIED BY '123456';
```

```
CREATE USER user_se IDENTIFIED BY '123456';

CREATE USER user_ce IDENTIFIED BY '123456';
```

(2)创建角色并分配权限

> ■ 在 MySQL 环境下中要激活角色，即执行以下语句（参阅：https://blog.csdn.net/qq_39746820/article/details/123710158 ）：
>
> ```
> SET GLOBAL activate_all_roles_on_login=ON;
> ```

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。

```
CREATE ROLE PurchaseQueryRole;

GRANT SELECT ON TABLE Part TO PurchaseQueryRole;

GRANT SELECT ON TABLE Supplier TO PurchaseQueryRole;

GRANT SELECT ON TABLE PartSupp TO PurchaseQueryRole;

CREATE ROLE SaleQueryRole;

GRANT SELECT ON TABLE Orders TO SaleQueryRole;

GRANT SELECT ON TABLE LineItem TO SaleQueryRole;

CREATE ROLE CustomerQueryRole;

GRANT SELECT ON TABLE Customer TO CustomerQueryRole;

GRANT SELECT ON TABLE Nation TO CustomerQueryRole;

GRANT SELECT ON TABLE Region TO CustomerQueryRole;
```

②为各个部门分别创建一个职员角色，对本部门信息具有查看、插入权限。

```
CREATE ROLE PurchaseEmployeeRole;

GRANT SELECT, INSERT ON TABLE Part TO PurchaseEmployeeRole;
```

```
GRANT SELECT, INSERT ON TABLE Supplier TO PurchaseEmployeeRole;

GRANT SELECT, INSERT ON TABLE PartSupp TO PurchaseEmployeeRole;

CREATE ROLE SaleEmployeeRole;

GRANT SELECT, INSERT ON TABLE Orders TO SaleEmployeeRole;

GRANT SELECT, INSERT ON TABLE LineItem TO SaleEmployeeRole;

CREATE ROLE CustomerEmployeeRole;

GRANT SELECT, INSERT ON TABLE Customer TO CustomerEmployeeRole;

GRANT SELECT, INSERT ON TABLE Nation TO CustomerEmployeeRole;

GRANT SELECT, INSERT ON TABLE Region TO CustomerEmployeeRole;
```

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，对其他部门的信息具有查询权。经理有权给本部门职员分配权限。

```
CREATE ROLE PurchaseManagerRole;

GRANT CREATE ROLE on *.* to PurchaseManagerRole;

GRANT ALL ON TABLE Part TO PurchaseManagerRole;

GRANT ALL ON TABLE Supplier TO PurchaseManagerRole;

GRANT ALL ON TABLE PartSupp TO PurchaseManagerRole;

GRANT SaleQueryRole TO PurchaseManagerRole;

GRANT CustomerQueryRole TO PurchaseManagerRole;


CREATE ROLE SaleManagerRole;

GRANT CREATE ROLE on *.* to SaleManagerRole;

GRANT ALL ON TABLE Orders TO SaleManagerRole;
```

```
GRANT ALL ON TABLE LineItem TO SaleManagerRole;

GRANT PurchaseQueryRole TO SaleManagerRole;

GRANT CustomerQueryRole TO SaleManagerRole;


CREATE ROLE CustomerManagerRole;

GRANT CREATE ROLE on *.* to CustomerManagerRole;

GRANT ALL ON TABLE Customer TO CustomerManagerRole;

GRANT ALL ON TABLE Nation TO CustomerManagerRole;

GRANT ALL ON TABLE Region TO CustomerManagerRole;

GRANT PurchaseQueryRole TO CustomerManagerRole;

GRANT SaleQueryRole TO CustomerManagerRole;
```

(3)给用户分配权限

①给各部门经理分配权限。

```
GRANT PurchaseManagerRole TO user_pm;

GRANT SaleManagerRole TO user_sm;

GRANT CustomerManagerRole TO user_cm;
```

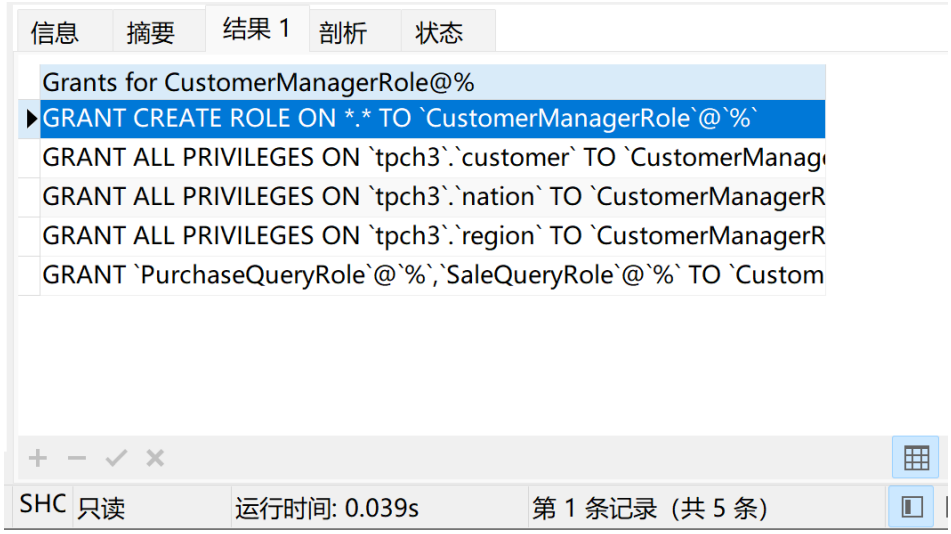
②给各部门职员分配权限。

```
GRANT PurchaseEmployeeRole TO user_pe;

GRANT SaleEmployeeRole TO user_se;

GRANT CustomerEmployeeRole TO user_ce;
```

(4)回收角色或用户权限

①收回客户经理角色的销售信息查看权限。

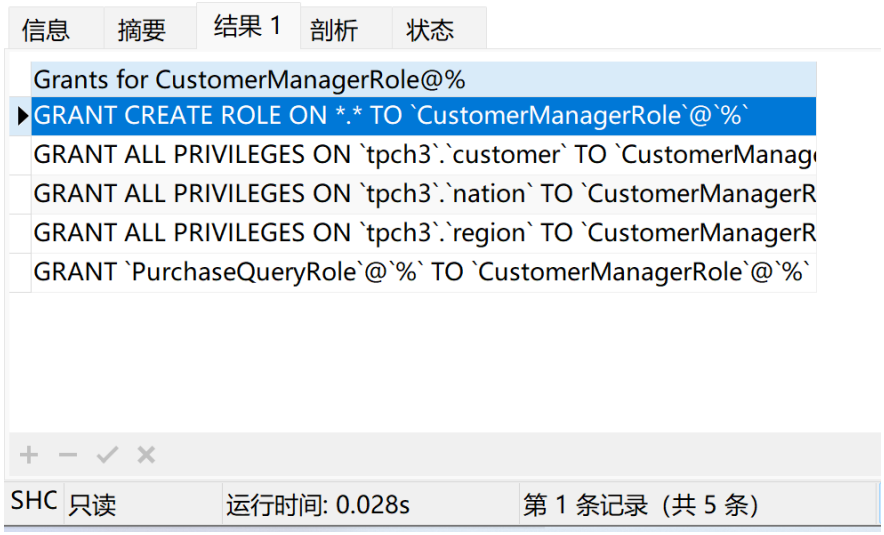
第 1 步执行“SHOW GRANTS FOR CustomerManagerRole;”，可显示：



第 2 步执行：

REVOKE SaleQueryRole FROM CustomerManagerRole;

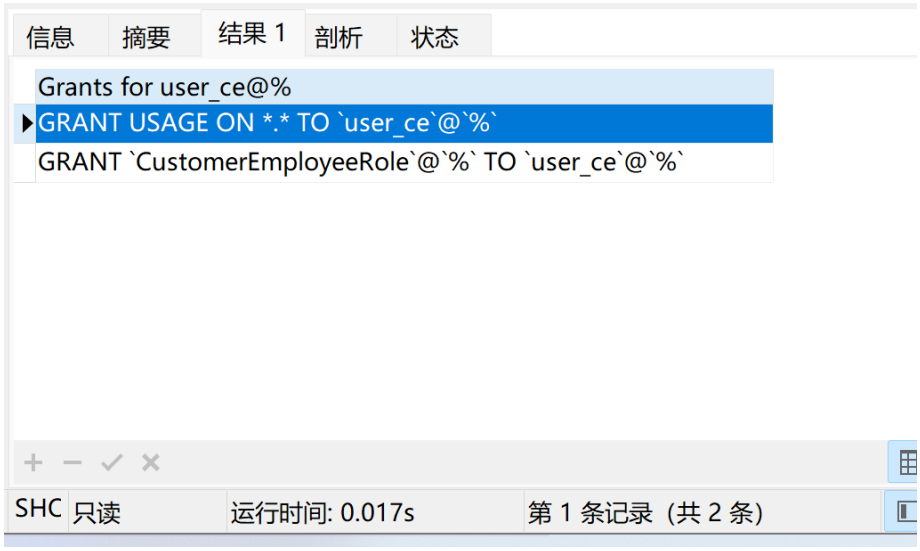
第 3 步再执行“SHOW GRANTS FOR CustomerManagerRole;”，可显示：



结论：超级用户可以回收用户的权限。

②回收 user_ce 的客户部门职员权限

第 1 步执行“SHOW GRANTS FOR user_ce;”，可显示：



第 2 步执行：

```
REVOKE CustomerEmployeeRole FROM user_ce;
```

第 3 步再执行“SHOW GRANTS FOR user_ce;”，可显示：

结论：超级用户可以回收用户的权限。

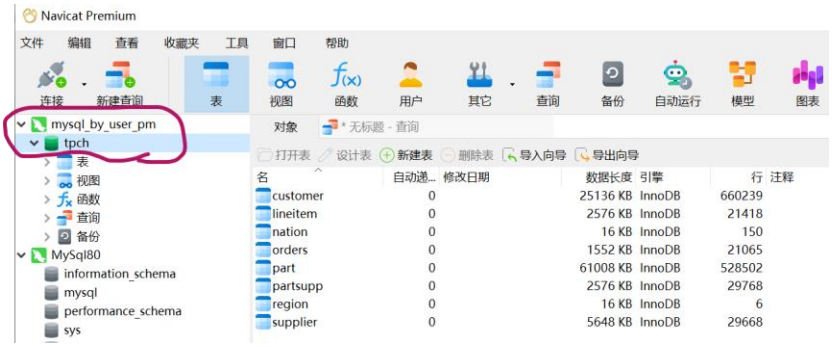
(5)验证权限分配正确性

①以 user_pm 用户名登录数据库，通过执行以下两条命令验证采购部门经理的权限。

```
SELECT * FROM Part;

DELETE FROM orders;
```

第 1 步在 Navicat 中以 user_pm 用户名登录数据库，如图：

“确定”后，可见：



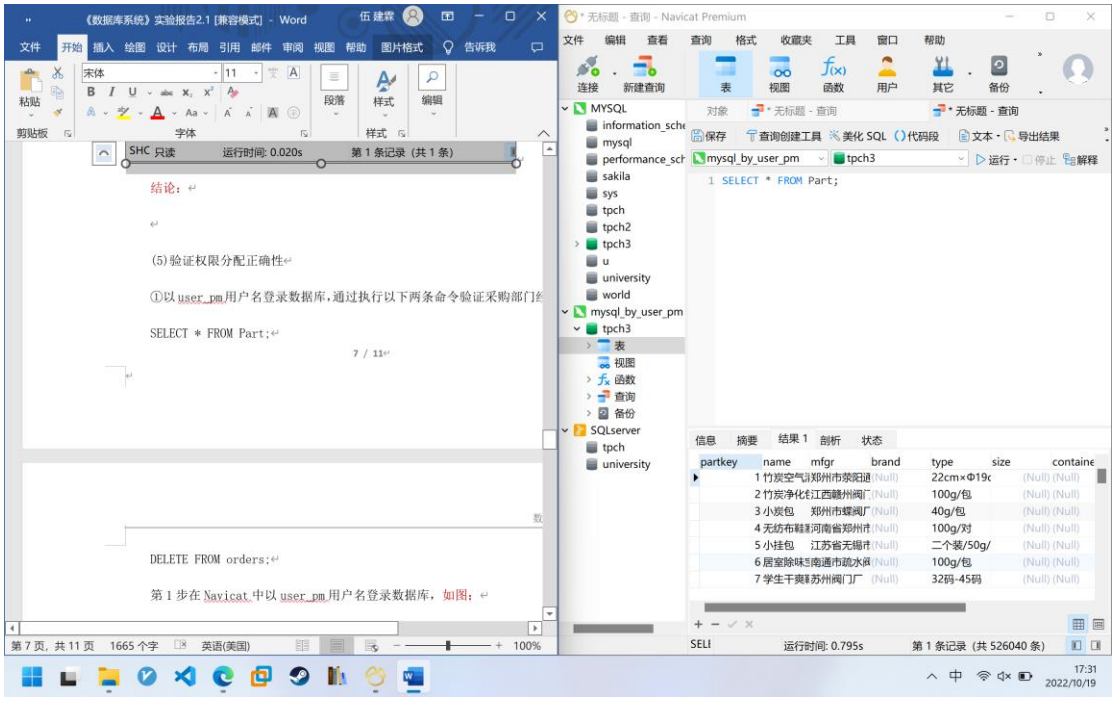
第 2 步“新建查询”，确保当前数据库是连接 mysql_by_user_pm 中的数据库 tpch.

第 3 步执行查询语句，结果如图；

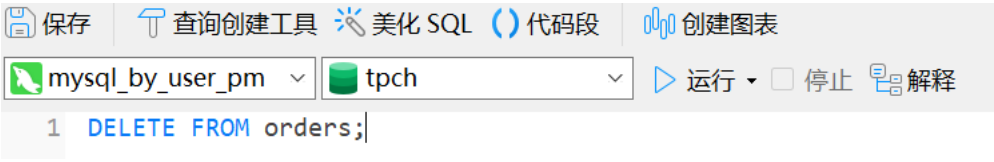
信息 | 摘要 | 结果 1 | 剖析 | 状态

partkey	name	mfgr	brand	type	size	container	retailprice	comment
1	竹炭空气清新篮	郑州市荥阳通	(Null)	22cm×Φ19(	(Null)	(Null)	3	(Null)
2	竹炭净化包	江西赣州阀门	(Null)	100g/包	(Null)	(Null)	3.5	(Null)
3	小炭包	郑州市蝶阀厂	(Null)	40g/包	(Null)	(Null)	4	(Null)
4	无纺布鞋塞	河南省郑州计	(Null)	100g/对	(Null)	(Null)	5	(Null)
5	小挂包	江苏省无锡计	(Null)	二个装/50g/	(Null)	(Null)	5.2	(Null)
6	居室除味宝	南通市疏水阀	(Null)	100g/包	(Null)	(Null)	5.2	(Null)
7	学生干爽鞋垫	苏州阀门厂	(Null)	32码-45码	(Null)	(Null)	5.5	(Null)

结论：经理有查询的权限。



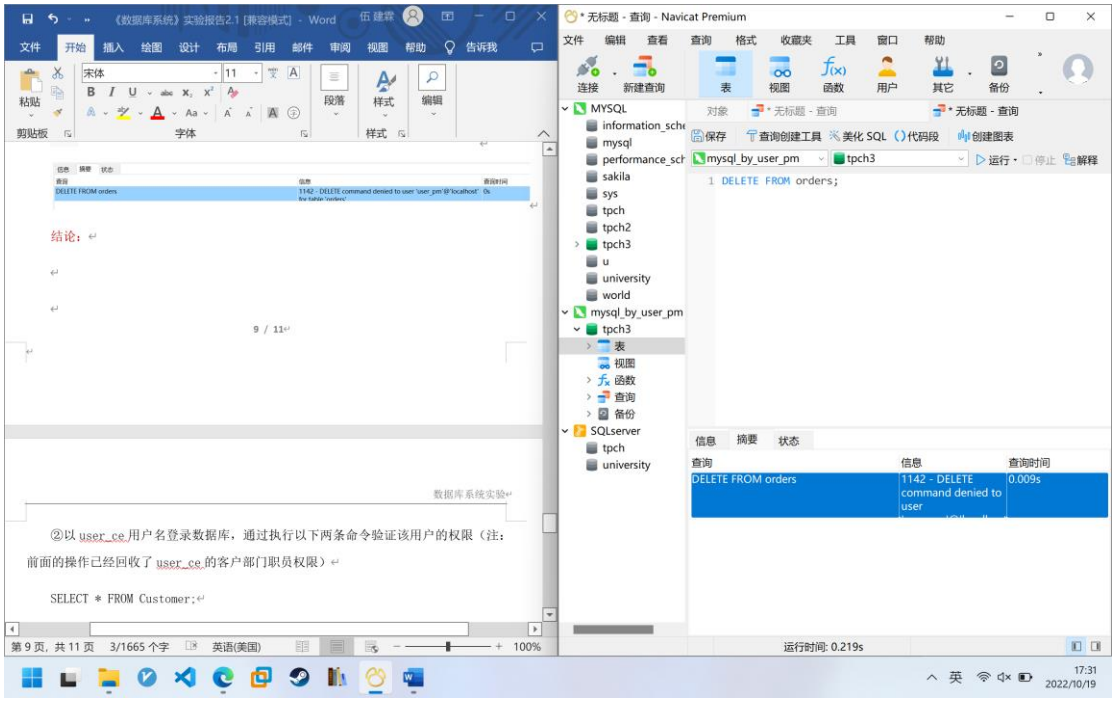
第 4 步执行删除语句，结果如图；



信息 | 摘要 | 状态

查询	信息	查询时间
DELETE FROM orders	1142 - DELETE command denied to user 'user_pm'@'localhost' for table 'orders'	0s

结论：经理没有删除的权限。

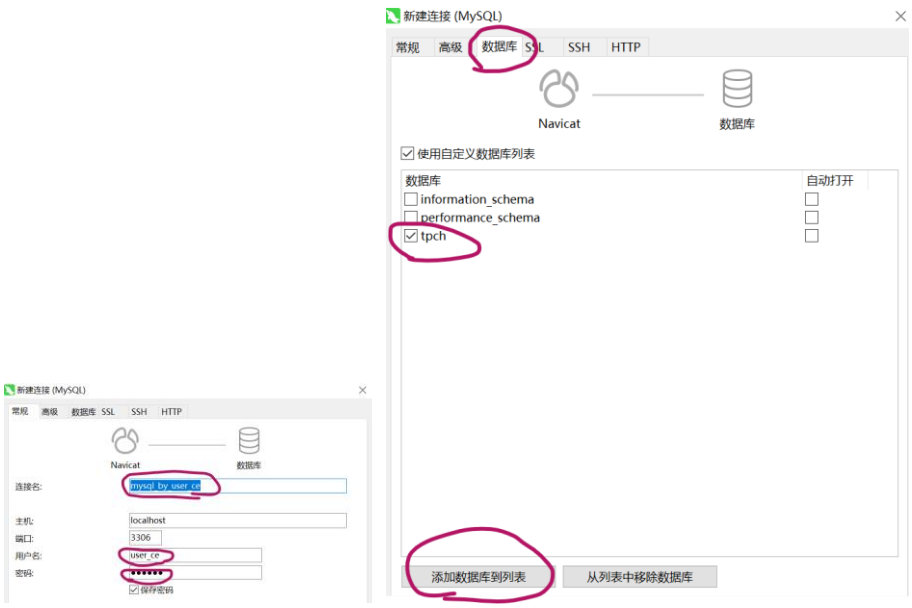


②以 user_ce 用户名登录数据库，通过执行以下两条命令验证该用户的权限（注：前面的操作已经回收了 user_ce 的客户部门职员权限）

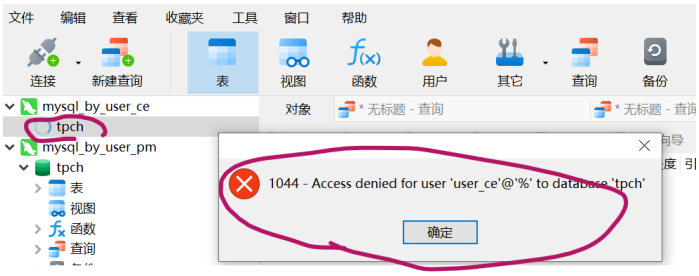
SELECT * FROM Customer;

SELECT * FROM Part;

第 1 步在 Navicat 中以 user_ce 用户名登录数据库，如图：

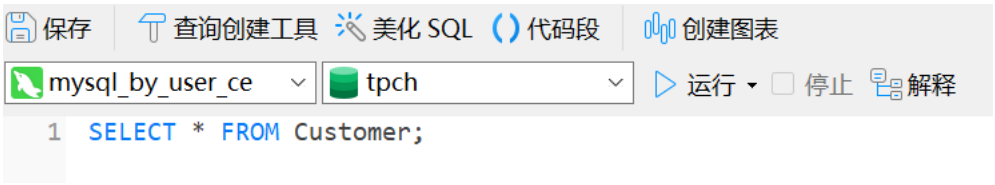


“确定”后，可见(注：出现的提示是指该用户不能访问该数据库中的任何表)：



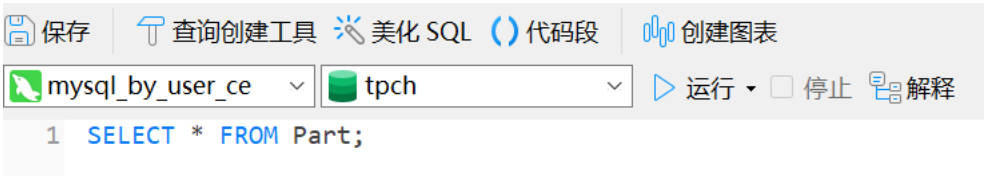
第 2 步“新建查询”，确保当前数据库是连接 mysql_by_user_ce 中的数据库 tpch.

第 3 步执行以下查询语句，结果如图；



结论：ce 职员用户无权查询 customer 表。

第 4 步再执行以下查询语句，结果如图；



结论：ce 职员用户无权查询 part 表。

六. 与实验结果相关的文件

无

七. 实验总结