实验二 安全性语言实验

16337341 朱志儒

实验 2.1 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。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。

实验步骤

1) 创建用户

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

```
CREATE LOGIN David WITH PASSWORD = '123456', DEFAULT_DATABASE = TPCH
CREATE USER David FOR LOGIN David WITH DEFAULT_SCHEMA = dbo
GRANT CREATE ROLE TO David;
```

```
CREATE LOGIN Tom WITH PASSWORD = '123456', DEFAULT_DATABASE = TPCH
CREATE USER Tom FOR LOGIN Tom WITH DEFAULT_SCHEMA = dbo
GRANT CREATE ROLE TO Tom;

CREATE LOGIN Kathy WITH PASSWORD = '123456', DEFAULT_DATABASE = TPCH
CREATE USER Kathy FOR LOGIN Kathy WITH DEFAULT_SCHEMA = dbo
GRANT CREATE ROLE TO Kathy;
```

· 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 LOGIN Jeffery WITH PASSWORD = '123456', DEFAULT_DATABASE =
TPCH
CREATE USER Jeffery FOR LOGIN Jeffery WITH DEFAULT_SCHEMA = dbo;

CREATE LOGIN Jane WITH PASSWORD = '123456', DEFAULT_DATABASE = TPCH
CREATE USER Jane FOR LOGIN Jane WITH DEFAULT_SCHEMA = dbo;

CREATE LOGIN Mike WITH PASSWORD = '123456', DEFAULT_DATABASE = TPCH
CREATE USER Mike FOR LOGIN Mike WITH DEFAULT_SCHEMA = dbo;
```

2) 创建角色并分配权限

· 为各个部门分别创建一个查询角色，并分配查询权限。

```
CREATE ROLE PurchaseQueryRole;
GRANT SELECT ON Part TO PurchaseQueryRole;
GRANT SELECT ON Supplier TO PurchaseQueryRole;
GRANT SELECT ON Partsupp TO PurchaseQueryRole;

CREATE ROLE SaleQueryRole;
GRANT SELECT ON Orders TO SaleQueryRole;
GRANT SELECT ON Lineitem TO SaleQueryRole;

CREATE ROLE CustomerQueryRole;
GRANT SELECT ON Customer TO CustomerQueryRole;
GRANT SELECT ON Nation TO CustomerQueryRole;
GRANT SELECT ON Region TO CustomerQueryRole;
```

- 为各个部门分别创建一个职员角色，对本部门的信息具有查看、插入权限。

```
CREATE ROLE PurchaseEmployeeRole;
GRANT SELECT,INSERT ON Part TO PurchaseEmployeeRole;
GRANT SELECT,INSERT ON Supplier TO PurchaseEmployeeRole;
GRANT SELECT,INSERT ON PartSupp TO PurchaseEmployeeRole;

CREATE ROLE SaleEmployeeRole;
GRANT SELECT,INSERT ON Orders TO SaleEmployeeRole;
GRANT SELECT,INSERT ON Lineitem TO SaleEmployeeRole;

CREATE ROLE CustomerEmployeeRole;
GRANT SELECT,INSERT ON Customer TO CustomerEmployeeRole;
GRANT SELECT,INSERT ON Nation TO CustomerEmployeeRole;
GRANT SELECT,INSERT ON Region TO CustomerEmployeeRole;
```

- 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 ALL ON Part TO PurchaseManagerRole;
GRANT ALL ON Supplier TO PurchaseManagerRole;
GRANT ALL ON PartSupp TO PurchaseManagerRole;
exec sp_addrolemember 'SaleQueryRole','PurchaseManagerRole';
exec sp_addrolemember 'CustomerQueryRole','PurchaseManagerRole';

CREATE ROLE SaleManagerRole;
GRANT ALL ON Orders TO SaleManagerRole;
GRANT ALL ON Lineitem TO SaleManagerRole;
exec sp_addrolemember 'PurchaseQueryRole','SaleManagerRole';
exec sp_addrolemember 'CustomerQueryRole','SaleManagerRole';

CREATE ROLE CustomerManagerRole;
GRANT ALL ON Customer TO CustomerManagerRole;
GRANT ALL ON Nation TO CustomerManagerRole;
GRANT ALL ON Region TO CustomerManagerRole;
exec sp_addrolemember 'PurchaseQueryRole','CustomerManagerRole';
```

```
exec sp_addrolemember 'SaleQueryRole','CustomerManagerRole';
```

3) 给用户分配权限

- 给各部门经理分配权限

```
exec sp_addrolemember 'PurchaseManagerRole','David';
exec sp_addrolemember 'SaleManagerRole','Tom';
exec sp_addrolemember 'CustomerManagerRole','Kathy';
```

- 给各部门职员分配权限

```
exec sp_addrolemember 'PurchaseEmployeeRole','Jeffery';
exec sp_addrolemember 'SaleEmployeeRole','Jane';
exec sp_addrolemember 'CustomerEmployeeRole','Mike';
```

4) 回收角色或用户权限

- 回收客户经理角色的销售信息查看权限

```
exec sp_droprolemember 'SaleQueryRole','CustomerManagerRole';
```

- 回收 MIKE 的客户部门职员权限

```
exec sp_droprolemember 'CustomerEmployeeRole','Mike';
```

5) 验证权限分配正确性

- 以 David 用户名登录数据库，验证采购部门经理的权限

```
SELECT * FROM Part;
SELECT * FROM Orders;
```

结果：

可以查询 Part 中的内容：

	partkey	name	mfgr	brand	type	size	container	retaiprice	comment	name_length
1	1	竹炭空气清新篮	郑州市荥阳通用阀门厂	NULL	22cm×Φ19cm/只	NULL	NULL	3	NULL	7
2	2	竹炭净化包	江西赣州阀门厂	NULL	100g/包	NULL	NULL	3.5	NULL	5
3	3	小炭包	郑州市蝶阀厂	NULL	40g/包	NULL	NULL	4	NULL	3
4	4	无纺布鞋塞	河南省郑州市上街蝶阀厂	NULL	100g/对	NULL	NULL	5	NULL	5
5	5	小挂包	江苏省无锡市阀门厂	NULL	二个装/50g/包	NULL	NULL	5.2	NULL	3
6	6	居室除味宝	南通市疏水阀厂	NULL	100g/包	NULL	NULL	5.2	NULL	5
7	7	学生干爽鞋垫	苏州阀门厂	NULL	32码-45码	NULL	NULL	5.5	NULL	6
8	8	冰箱除味包	淮阴市清江化工阀门总厂	NULL	150g/盒	NULL	NULL	6	NULL	5
9	9	竹炭保暖鞋垫	山东省青岛高中压阀门厂	NULL	35码-47码	NULL	NULL	6	NULL	6
10	10	儿童网眼鞋垫	上海沪祥阀门厂	NULL	1-6号	NULL	NULL	6	NULL	6

但不可查询 Orders 中的内容：

```
消息 229，级别 14，状态 5，第 88 行
拒绝了对对象 'Orders' (数据库 'TPCH'，架构 'dbo')的 SELECT 权限。
```

· 回收 MIKE 的客户部门职员权限

```
SELECT * FROM Customer;
SELECT * FROM Part;
```

结果：

```
消息 229，级别 14，状态 5，第 90 行
拒绝了对对象 'Customer' (数据库 'TPCH'，架构 'dbo')的 SELECT 权限。
消息 229，级别 14，状态 5，第 92 行
拒绝了对对象 'Part' (数据库 'TPCH'，架构 'dbo')的 SELECT 权限。
```

实验总结

在进行权限分配后，针对不同用户所具有的权限设计并执行若干 SQL 语言，验证权限分配是否有效。

本次实验中的创建用户过程遇到些许麻烦，书上的代码在 SQL SERVER 2017 上并不支持，在查阅相关文档后我才直到该如何创建符合条件的用户。在创建部门的经理角色时，我也遇到不少问题，与书上的 GRANT SalesQueryRole TO PurchaseManagerRole 不同的是 SQL SERVER 使用的是 exec sp_addrolemember 'SaleQueryRole','PurchaseManagerRole'，进行给用户分配权限和回收角色或用户权限的操作 SQL SERVER 和书上的代码也是完全不同。

通过本次实验，我了解了如何在 SQL SERVER 上定义角色、分配权限和回收权限。