# 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;

1. **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';

1. **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';

1. **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';

1. **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：



但不可查询Orders中的内容：

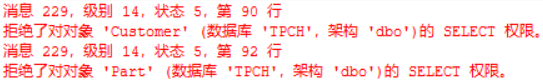


* 回收MIKE的客户部门职员权限

    SELECT \* FROM Customer;

    SELECT \* FROM Part;

结果：



### 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。