实验六：安全性-自主存取控制

1. 实验环境

- 华为云数据库 RDS
- 前提：已购买华为云数据库 RDS 数据库实例+数据库中的所有表都有数据

2. 实验目的

- 掌握自主存取控制权限的定义和维护方法

3. 实验要求和内容

3.1 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正确。
- 实验报告提交到 ftp://121.192.180.66 的上传作业文件夹：实验六 安全性
- 实验报告名：学号-姓名-实验六
- 实验报告上交截至日期：2021 年 5 月 29 日 0 点之前。

3.2 内容：

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 David，采购员 Jeffery；销售部门经理 Tom，销售员 Jane；客户管理部门经理 Kathy，职员 Mike。该企业的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，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。

(1) 创建用户

- 创建三个用户 David，Tom，Kathy，注意观察与页面操作的结果对应的 SQL 语句

(2) 创建角色并分配权限

2.1 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 Part TO PurchaseQueryRole;

GRANT SELECT ON Supplier TO PurchaseQueryRole;

GRANT SELECT ON PartSupp TO PurchaseQueryRole;

CREATE ROLE SaleQueryRole;

GRANT SELECT ON Order 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;
```

2.2 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 Part TO PurchaseEmployeeRole;

GRANT SELECT, INSERT ON Supplier TO PurchaseEmployeeRole;

GRANT SELECT, INSERT ON PartSupp TO PurchaseEmployeeRole;

CREATE ROLE SaleEmployeeRole;

GRANT SELECT,INSERT ON Order 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;
```

2.3 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限。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;

GRANT SaleQueryRole TO PurchaseManagerRole;

GRANT CustomerQueryRole TO PurchaseManagerRole;

CREATE ROLE SaleManagerRole;

GRANT ALL ON Order TO SaleManagerRole;

GRANT ALL ON LineItem TO SaleManagerRole;

GRANT PurchaseQueryRole TO SaleManagerRole;

GRANT CustomerQueryRole TO SaleManagerRole;

CREATE ROLE CustomerManagerRole;

GRANT ALL ON Customer TO CustomerManagerRole;

GRANT ALL ON Nation TO CustomerManagerRole;

GRANT ALL ON Region TO CustomerManagerRole;

GRANT PurchaseQueryRole TO CustomerManagerRole;

GRANT SaleQueryRole TO CustomerManagerRole;
```

(3) 给用户分配权限

3.1 给各部门经理分配权限。

```
GRANT SaleManagerRole TO Tom WITH ADMIN OPTION;

GRANT CustomerManagerRole TO Tom WITH ADMIN OPTION;
```

3.2 给各部门职员分配用户权限

```
GRANT PurchaseEmployeeRole TO Jeffery;

GRANT SaleEmployeeRole TO Jane;

GRANT CustomerEmployeeRole TO Mike;
```

(4) 验证权限分配的正确性

4.1 以 David 用户名登录数据库，验证采购部门经理的权限。

```
SELECT * FROM Part;

DELETE * FROM Order;
```

4.2 以 Mike 用户名登录数据库，验证 Mike 的客户部门职员权限

```
SELECT * FROM Customer;

SELECT * FROM Part;
```

(5) 回收角色或用户权限

5.1 收回客户经理角色的销售信息查看权限。

```
REVOKE SaleQueryRole FROM CustomerManagerRole;
```

5.2 收回 Mike 的客户部门职员权限。

```
REVOKE CustomerEmployeeRole FROM Mike;
```

4. 实验总结

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

附：MYSQL 的语法参考列表

https://blog.csdn.net/qq_32444825/article/details/105317944

https://www.cnblogs.com/kcxg/p/11363008.html

https://dev.mysql.com/doc/refman/8.0/en/roles.html#roles-checking

https://blog.csdn.net/qq_40323844/article/details/89922035