实验五、安全机制

一、实验目的

1．掌握数据库安全管理机制中的常规方法，理解用户、模式、角色、权限的概念、定义及使用;

2．掌握视图、存储过程、触发器的概念、定义及如何发挥特殊的安全控制作用。

二、实验学时

2学时

三、实验内容

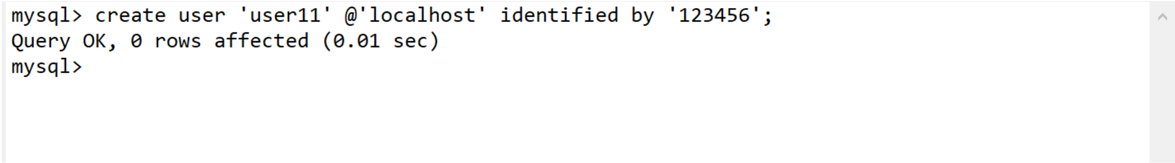
1．理解用户、模式、角色、权限的概念，在MySQL中感知用户、模式、角色和权限。

2．完成以下操作:

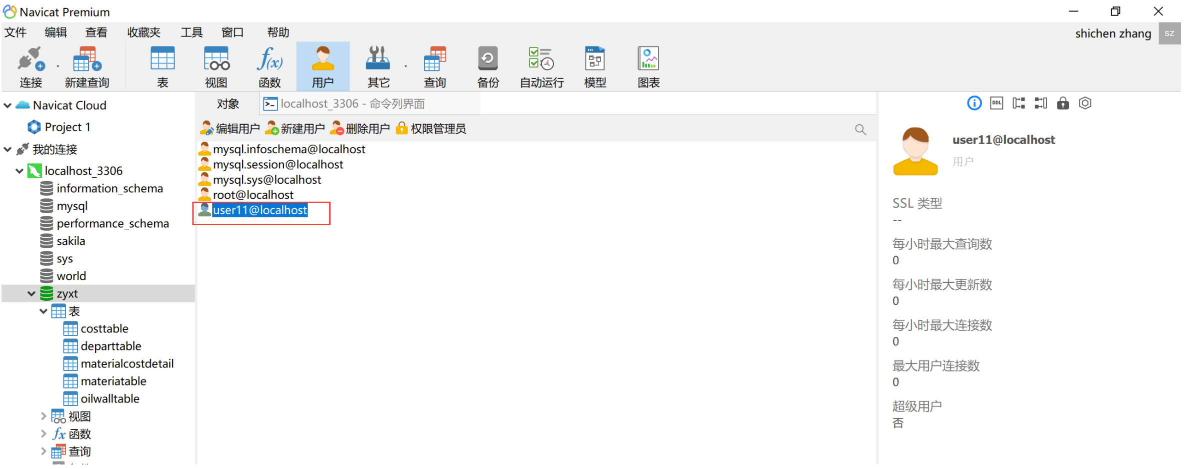
(1) 建立采油一矿的成本的视图，把该视图的查询权限授予给采油一矿的用户user11，以user11的身份查询该视图，观察执行情况；再以其他用户的身份查询该视图，观察执行情况。
创建用户user11:

```
create user 'user11' @'localhost' identified by '123456';
```

结果:



```
mysql> create user 'user11' @'localhost' identified by '123456';
Query OK, 0 rows affected (0.01 sec)
mysql>
```



mysql.infoschema@localhost
mysql.session@localhost
mysql.sys@localhost
root@localhost
user11@localhost

user11@localhost
用户

SSL 类型
--

每小时最大查询数
0

每小时最大更新数
0

每小时最大连接数
0

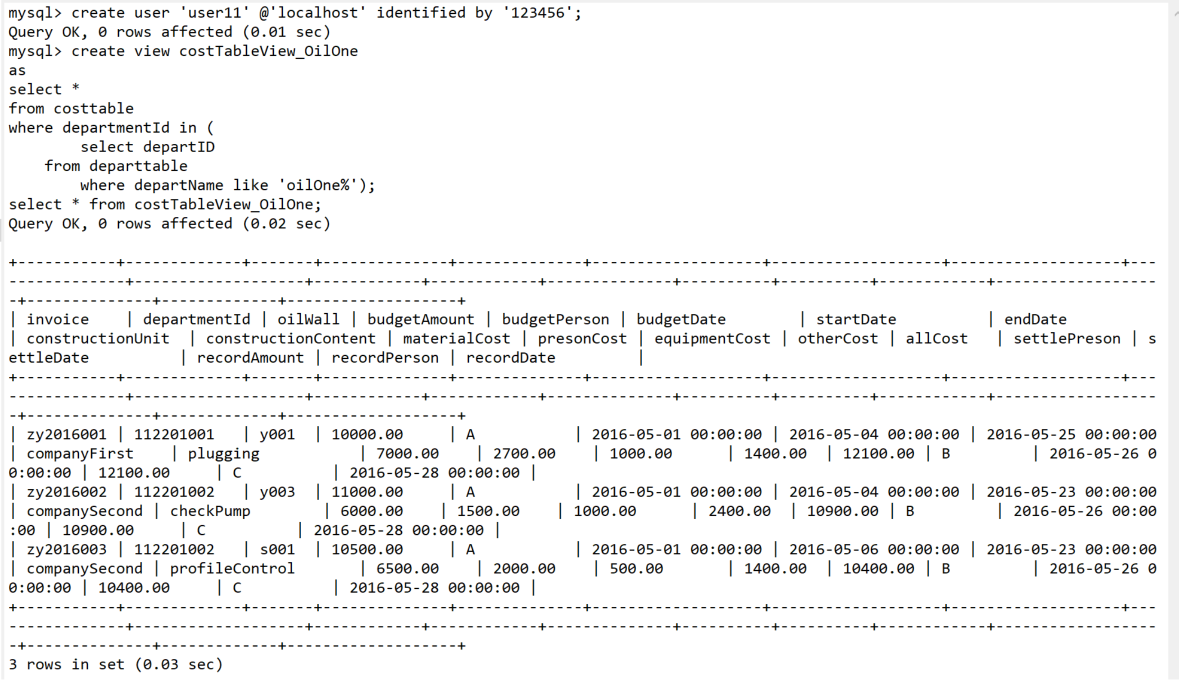
最大用户连接数
0

超级用户
否

创建视图:

```
create view costTableView_OilOne
as
select *
from costtable
where departmentId in (
    select departID
    from departtable
    where departName like 'oilOne%');
select * from costTableView_OilOne;
```

结果:



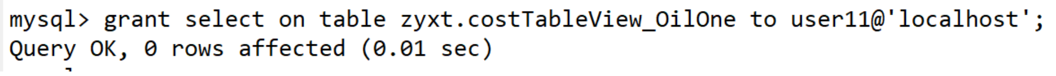
```
mysql> create user 'user11' @'localhost' identified by '123456';
Query OK, 0 rows affected (0.01 sec)
mysql> create view costTableView_OilOne
as
select *
from costtable
where departmentId in (
        select departID
    from departtable
        where departName like 'oilOne%');
select * from costTableView_OilOne;
Query OK, 0 rows affected (0.02 sec)

+-----------+--------------+---------+--------------+--------------+---------------------+---------------------+---------------------+---
---------------+---------------------+--------------+------------+---------------+-----------+----------+--------------+--------------------
-+--------------+--------------+---------------------+
| invoice   | departmentId | oilWall | budgetAmount | budgetPerson | budgetDate          | startDate           | endDate
| constructionUnit | constructionContent | materialCost | presonCost | equipmentCost | otherCost | allCost  | settlePreson | s
ettleDate          | recordAmount | recordPerson | recordDate          |
+-----------+--------------+---------+--------------+--------------+---------------------+---------------------+---------------------+---
---------------+---------------------+--------------+------------+---------------+-----------+----------+--------------+--------------------
-+--------------+--------------+---------------------+
| zy2016001 | 112201001    | y001    | 10000.00     | A            | 2016-05-01 00:00:00 | 2016-05-04 00:00:00 | 2016-05-25 00:00:00
| companyFirst     | plugging            | 7000.00      | 2700.00    | 1000.00       | 1400.00   | 12100.00 | B            | 2016-05-26 0
0:00:00 | 12100.00     | C            | 2016-05-28 00:00:00 |
| zy2016002 | 112201002    | y003    | 11000.00     | A            | 2016-05-01 00:00:00 | 2016-05-04 00:00:00 | 2016-05-23 00:00:00
| companySecond | checkPump           | 6000.00      | 1500.00    | 1000.00       | 2400.00   | 10900.00 | B            | 2016-05-26 00:00
:00 | 10900.00     | C            | 2016-05-28 00:00:00 |
| zy2016003 | 112201002    | s001    | 10500.00     | A            | 2016-05-01 00:00:00 | 2016-05-06 00:00:00 | 2016-05-23 00:00:00
| companySecond | profileControl      | 6500.00      | 2000.00    | 500.00        | 1400.00   | 10400.00 | B            | 2016-05-26 0
0:00:00 | 10400.00     | C            | 2016-05-28 00:00:00 |
+-----------+--------------+---------+--------------+--------------+---------------------+---------------------+---------------------+---
---------------+---------------------+--------------+------------+---------------+-----------+----------+--------------+--------------------
-+--------------+--------------+---------------------+
3 rows in set (0.03 sec)
```

授权:

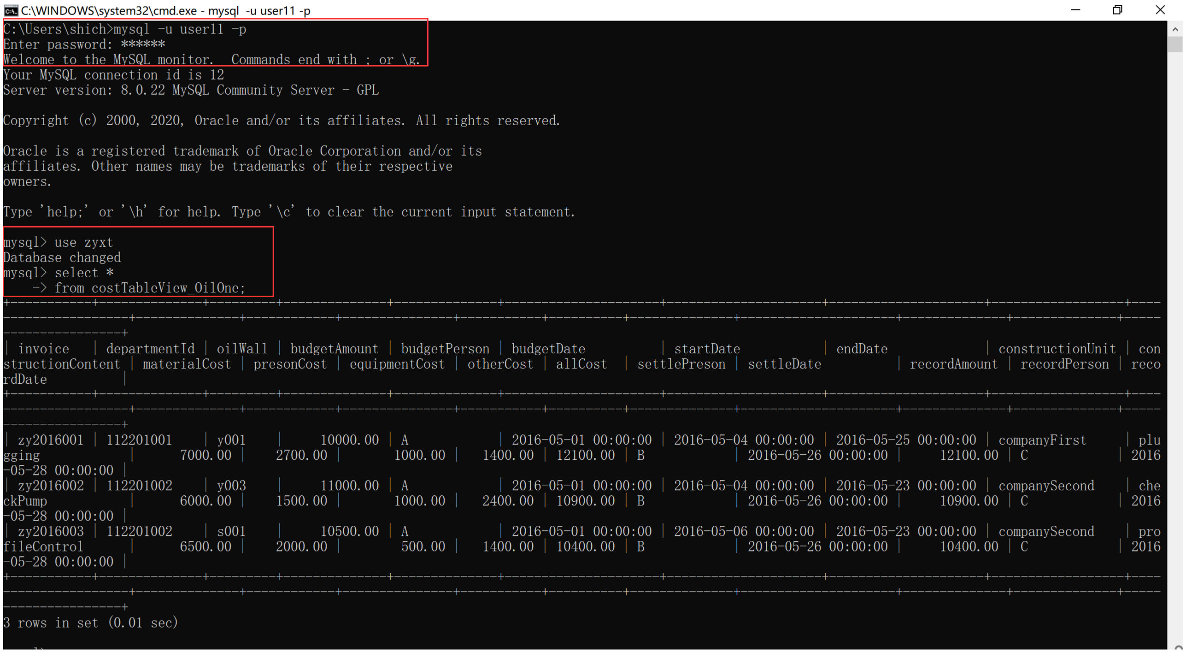
```
grant select on table zyxt.costTableView_OilOne to user11@'localhost';
```

结果;



```
mysql> grant select on table zyxt.costTableView_OilOne to user11@'localhost';
Query OK, 0 rows affected (0.01 sec)
```

使用user11查看:



C:\WINDOWS\system32\cmd.exe - mysql -u user11 -p

```
C:\Users\shich>mysql -u user11 -p
Enter password: ******
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use zyxt
Database changed
mysql> select *
    -> from costTableView_OilOne;
+-----------+--------------+---------+--------------+--------------+---------------------+---------------------+---------------------+------------------+----
-----------------+--------------+------------+---------------+-----------+----------+--------------+---------------------+--------------+--------------+-----
----------------+
| invoice   | departmentId | oilWall | budgetAmount | budgetPerson | budgetDate          | startDate           | endDate             | constructionUnit | con
structionContent | materialCost | presonCost | equipmentCost | otherCost | allCost  | settlePreson | settleDate          | recordAmount | recordPerson | reco
rdDate          |
+-----------+--------------+---------+--------------+--------------+---------------------+---------------------+---------------------+------------------+----
-----------------+--------------+------------+---------------+-----------+----------+--------------+---------------------+--------------+--------------+-----
----------------+
| zy2016001 | 112201001    | y001    |     10000.00 | A            | 2016-05-01 00:00:00 | 2016-05-04 00:00:00 | 2016-05-25 00:00:00 | companyFirst     | plu
gging            |      7000.00 |    2700.00 |       1000.00 |   1400.00 | 12100.00 | B            | 2016-05-26 00:00:00 |     12100.00 | C            | 2016
-05-28 00:00:00 |
| zy2016002 | 112201002    | y003    |     11000.00 | A            | 2016-05-01 00:00:00 | 2016-05-04 00:00:00 | 2016-05-23 00:00:00 | companySecond    | che
ckPump           |      6000.00 |    1500.00 |       1000.00 |   2400.00 | 10900.00 | B            | 2016-05-26 00:00:00 |     10900.00 | C            | 2016
-05-28 00:00:00 |
| zy2016003 | 112201002    | s001    |     10500.00 | A            | 2016-05-01 00:00:00 | 2016-05-06 00:00:00 | 2016-05-23 00:00:00 | companySecond    | pro
fileControl      |      6500.00 |    2000.00 |        500.00 |   1400.00 | 10400.00 | B            | 2016-05-26 00:00:00 |     10400.00 | C            | 2016
-05-28 00:00:00 |
+-----------+--------------+---------+--------------+--------------+---------------------+---------------------+---------------------+------------------+----
-----------------+--------------+------------+---------------+-----------+----------+--------------+---------------------+--------------+--------------+-----
----------------+
3 rows in set (0.01 sec)
```

(2) 创建一个用户user12，以user12的身份执行实验四中所定义的存储过程，观察记录是否成功执行；然后把该存储过程的执行权限授予给user12，再次以user12的身份执行该存储过程，观察记录是否成功执行。

```
create user 'user12' @'localhost' identified by '123456';
select host,user from mysql.user;
```

结果：

```
mysql> grant select on table zyxt.costTableView_OilOne to user11@'localhost';
Query OK, 0 rows affected (0.01 sec)
mysql> create user 'user12' @'localhost' identified by '123456';
select host,user from mysql.user;
Query OK, 0 rows affected (0.01 sec)
+-----------+------------------+
| host      | user             |
+-----------+------------------+
| localhost | mysql.infoschema |
| localhost | mysql.session    |
| localhost | mysql.sys        |
| localhost | root             |
| localhost | user11           |
| localhost | user12           |
+-----------+------------------+
6 rows in set (0.08 sec)
```

定义一个存储结构：

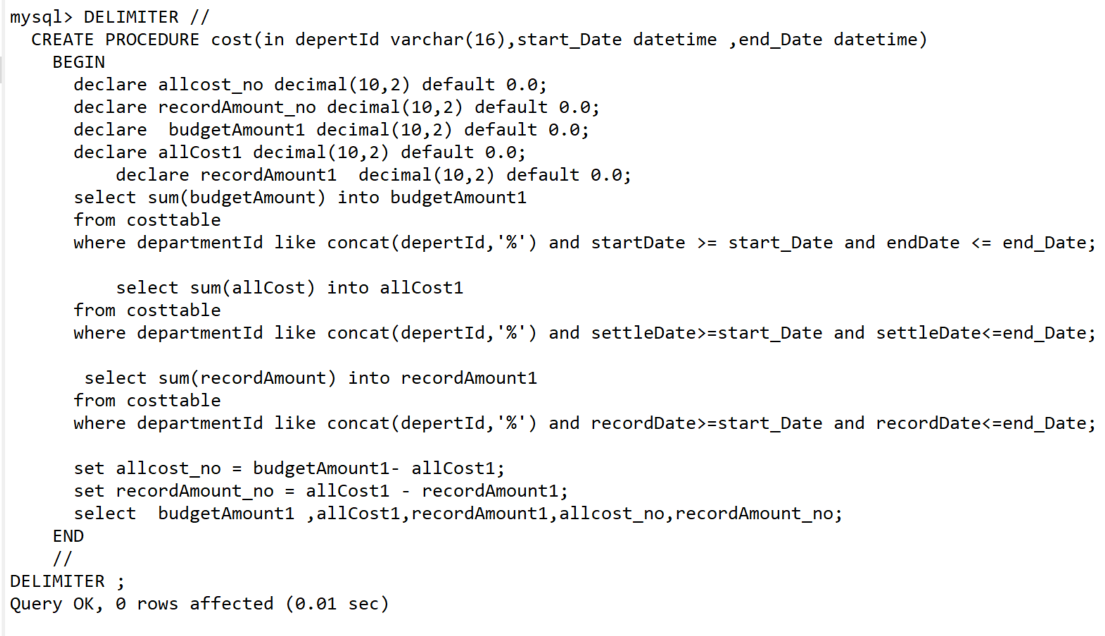
```
DELIMITER //
  CREATE PROCEDURE cost(in depertId varchar(16),start_Date datetime ,end_Date
datetime)
      BEGIN
        declare allcost_no decimal(10,2) default 0.0;
        declare recordAmount_no decimal(10,2) default 0.0;
        declare  budgetAmount1 decimal(10,2) default 0.0;
        declare allCost1 decimal(10,2) default 0.0;
        declare recordAmount1  decimal(10,2) default 0.0;
        select sum(budgetAmount) into budgetAmount1
        from costtable
        where departmentId like concat(depertId,'%') and startDate >= start_Date
and endDate <= end_Date;

        select sum(allCost) into allCost1
        from costtable
        where departmentId like concat(depertId,'%') and settleDate>=start_Date
and settleDate<=end_Date;

       select sum(recordAmount) into recordAmount1
        from costtable
        where departmentId like concat(depertId,'%') and recordDate>=start_Date
and recordDate<=end_Date;

        set allcost_no = budgetAmount1- allCost1;
        set recordAmount_no = allCost1 - recordAmount1;
        select  budgetAmount1 ,allCost1,recordAmount1,allcost_no,recordAmount_no;
      END
      //
DELIMITER ;
```

结果：



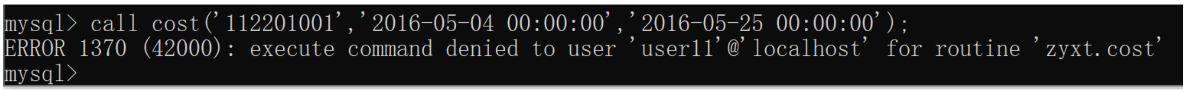
```
mysql> DELIMITER //
  CREATE PROCEDURE cost(in depertId varchar(16),start_Date datetime ,end_Date datetime)
    BEGIN
      declare allcost_no decimal(10,2) default 0.0;
      declare recordAmount_no decimal(10,2) default 0.0;
      declare  budgetAmount1 decimal(10,2) default 0.0;
      declare allCost1 decimal(10,2) default 0.0;
          declare recordAmount1  decimal(10,2) default 0.0;
      select sum(budgetAmount) into budgetAmount1
      from costtable
      where departmentId like concat(depertId,'%') and startDate >= start_Date and endDate <= end_Date;

          select sum(allCost) into allCost1
      from costtable
      where departmentId like concat(depertId,'%') and settleDate>=start_Date and settleDate<=end_Date;

       select sum(recordAmount) into recordAmount1
      from costtable
      where departmentId like concat(depertId,'%') and recordDate>=start_Date and recordDate<=end_Date;

      set allcost_no = budgetAmount1- allCost1;
      set recordAmount_no = allCost1 - recordAmount1;
      select  budgetAmount1 ,allCost1,recordAmount1,allcost_no,recordAmount_no;
    END
    //
DELIMITER ;
Query OK, 0 rows affected (0.01 sec)
```

使用user12 调用：

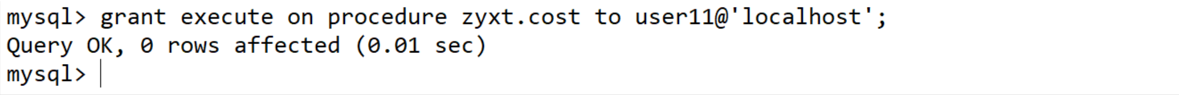


```
mysql> call cost(’112201001’,’2016-05-04 00:00:00’,’2016-05-25 00:00:00’);
ERROR 1370 (42000): execute command denied to user ’user11’@’localhost’ for routine ’zyxt.cost’
mysql>
```

授予权限：

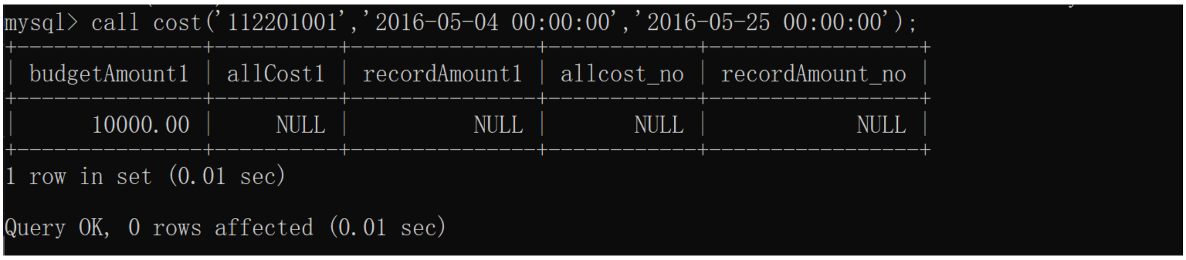
```
grant execute on procedure zyxt.cost to user11@'localhost';
```

结果：



```
mysql> grant execute on procedure zyxt.cost to user11@'localhost';
Query OK, 0 rows affected (0.01 sec)
mysql>
```

再次调用：



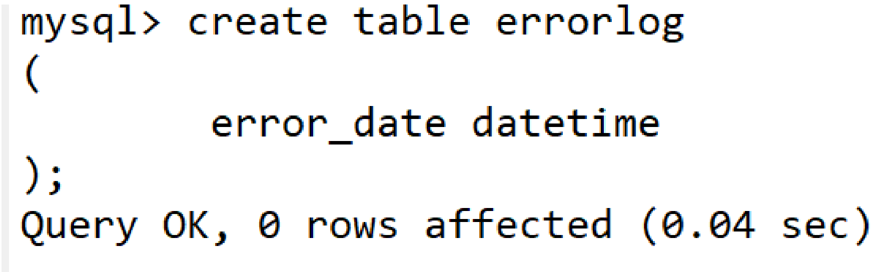
```
mysql> call cost('112201001','2016-05-04 00:00:00','2016-05-25 00:00:00');
+----------------+----------+---------------+-------------+-----------------+
| budgetAmount1  | allCost1 | recordAmount1 | allcost_no  | recordAmount_no |
+----------------+----------+---------------+-------------+-----------------+
|       10000.00 |     NULL |          NULL |        NULL |            NULL |
+----------------+----------+---------------+-------------+-----------------+
1 row in set (0.01 sec)

Query OK, 0 rows affected (0.01 sec)
```

(3) 定义触发器，实现只能在工作时间内更新“成本表”的数据，然后通过选择不同的时间进行适当的更新操作来验证。

定义错误日志表（mysql8.0不支持返回）：

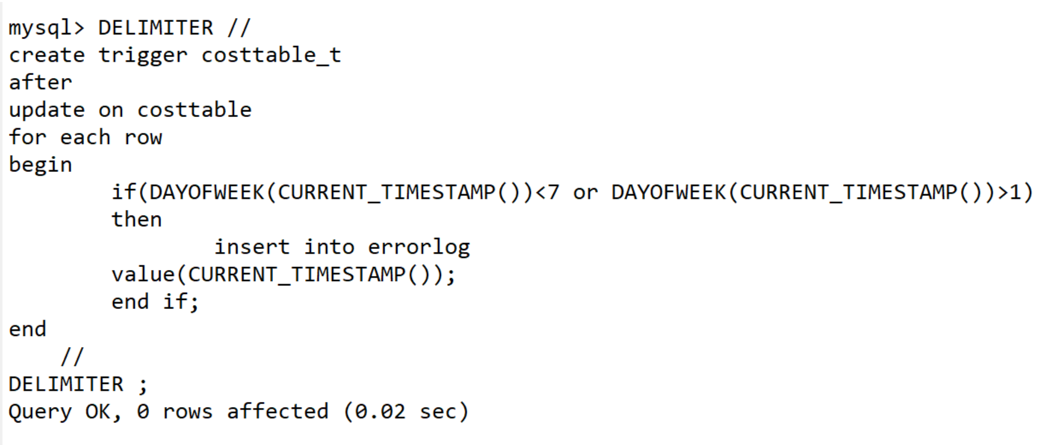
```
create table errorlog
(
    error_date datetime
);
```



```
mysql> create table errorlog
(
        error_date datetime
);
Query OK, 0 rows affected (0.04 sec)
```

定义触发器：

```
DELIMITER //
create trigger costtable_t
after
update on costtable
for each row
begin
    if(DAYOFWEEK(CURRENT_TIMESTAMP())<7 or DAYOFWEEK(CURRENT_TIMESTAMP())>1)
    then
        insert into errorlog
        value(CURRENT_TIMESTAMP());
    end if;
end
    //
DELIMITER ;
```

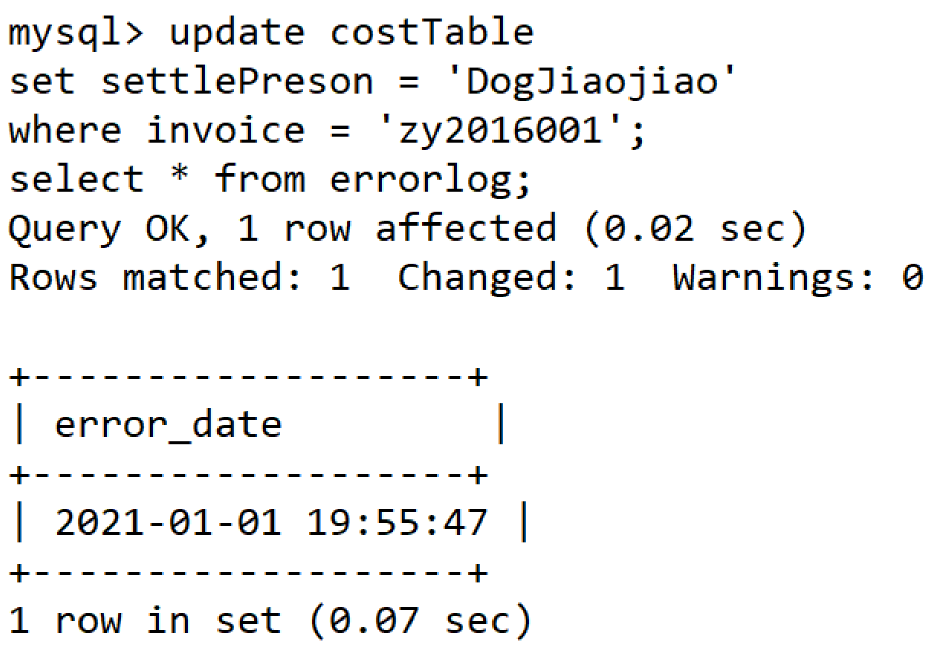


```
mysql> DELIMITER //
create trigger costtable_t
after
update on costtable
for each row
begin
        if(DAYOFWEEK(CURRENT_TIMESTAMP())<7 or DAYOFWEEK(CURRENT_TIMESTAMP())>1)
        then
                insert into errorlog
        value(CURRENT_TIMESTAMP());
        end if;
end
    //
DELIMITER ;
Query OK, 0 rows affected (0.02 sec)
```

测试：

①时间：1.1——周五

```
update costTable
set settlePreson = 'DogJiaojiao'
where invoice = 'zy2016001';
select * from errorlog;
```



```
mysql> update costTable
set settlePreson = 'DogJiaojiao'
where invoice = 'zy2016001';
select * from errorlog;
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0

+---------------------+
| error_date          |
+---------------------+
| 2021-01-01 19:55:47 |
+---------------------+
1 row in set (0.07 sec)
```

四、实验报告

提交实验内容中用SQL语句完成的题目的SQL语句文档及相应的执行结果。