BUỔI 7: BẢO MẬT CƠ SỞ DỮ LIỆU SQL SERVER

I. CHỦ ĐỀ

- Bảo mật cơ sở dữ liệu
- Cách thực hiện
- Thiết lập bảo mật

II. MỤC ĐÍCH

- Biết cách bảo mật cơ sở dữ liêu người dùng

III. CÔNG CỤ

- Microsoft SQL Server 2014 Express Edition/Management hoặc hơn.

IV. MÔI TRƯỜNG

- Win 10

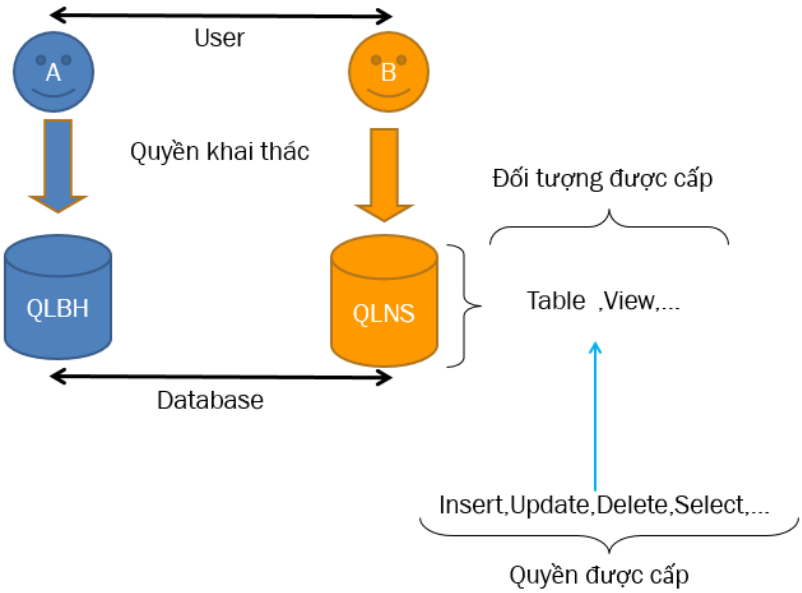
V. CÁCH THỰC HIỆN

1. Bảo mật cơ sở dữ liệu là gì?

Bảo mật cơ sở dữ liệu sql server là giải pháp cho phép các quản trị viên cơ sở dữ liệu thiết lập quyền hạn cho người dùng hoặc nhóm người dùng khai thác cơ sở dữ liệu.

Người dùng hoặc nhóm người dùng sau khi được cấp quyền, có thể đăng nhập vào hệ thống và thực hiện các quyền hạn mà mình được cấp.

Bảo mật cơ sở dữ liệu sql server giúp phân quyền người dùng trên cơ sở dữ liệu. Hình bên dưới là một ví dụ về phân quyền trên cơ sở dữ liệu



2. Thực thi Bảo mật:

Sinh viên tạo Database **QUANLYBANHANG_B7_MSSV** (trong đó MSSV là mã số của sinh viên) với hai file đính kèm là CREATEDATABASE.sql và USEDATABASE.sql.

Cấp quyền cho người dùng tên **test1** được phép xem dữ liệu trên bảng **VATTU** của cơ sở dữ liệu **QuanLyBanHang**

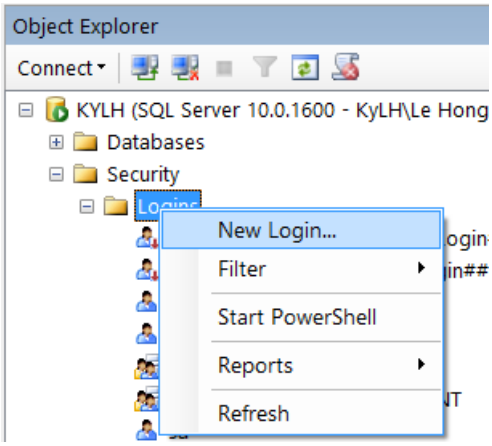
Các bước thực hiện bảo mật cơ sở dữ liệu sql server – Cấp quyền cho người dùng

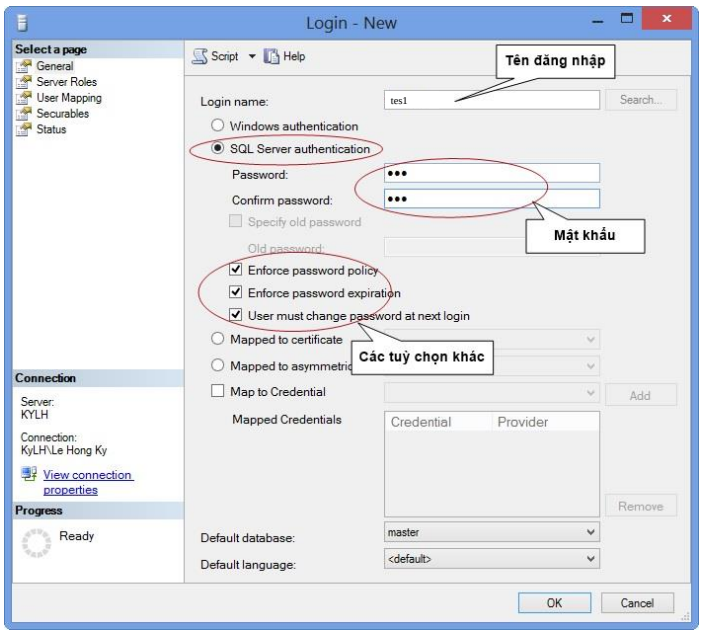
Đăng nhập vào hệ thống với quyền quản trị (Administrator) và thực hiện một trong hai cách sau:

Cách 1: Thực hiện bằng giao diện

Bước 1: Tạo tài khoản sql server (login):

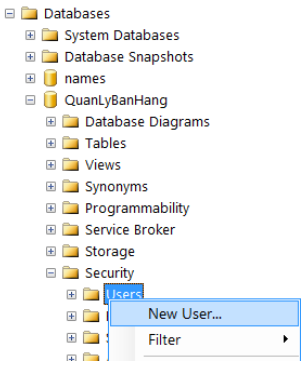
Chọn Security của Server => Click phải chọn New Login => Nhập Login name: test1

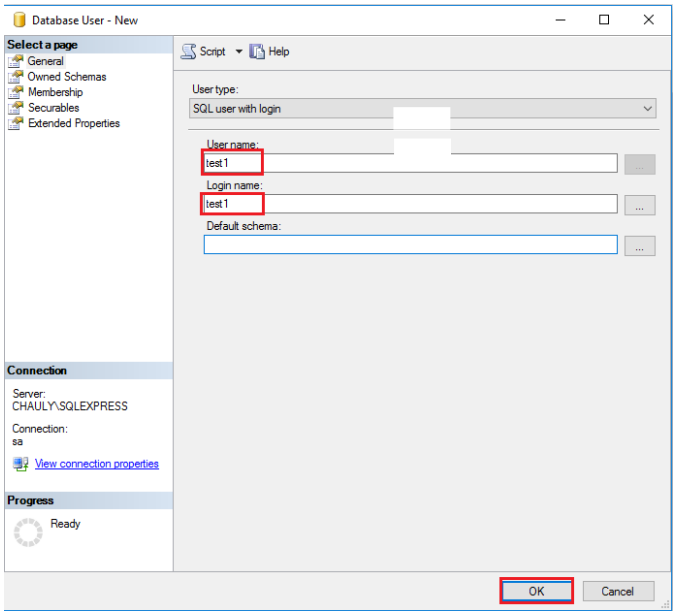




Bước 2: Tạo người sử dụng (user)

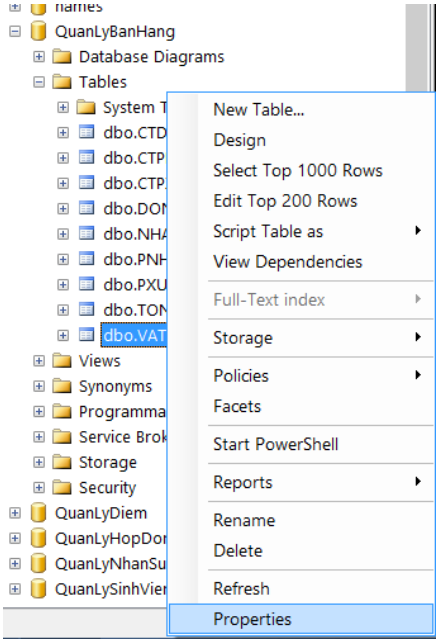
Mở Database QuanLyBanHang => Chọn Security => Click phải Users => New User… => Nhập User name: test1 (có thể tương tự như tên server).



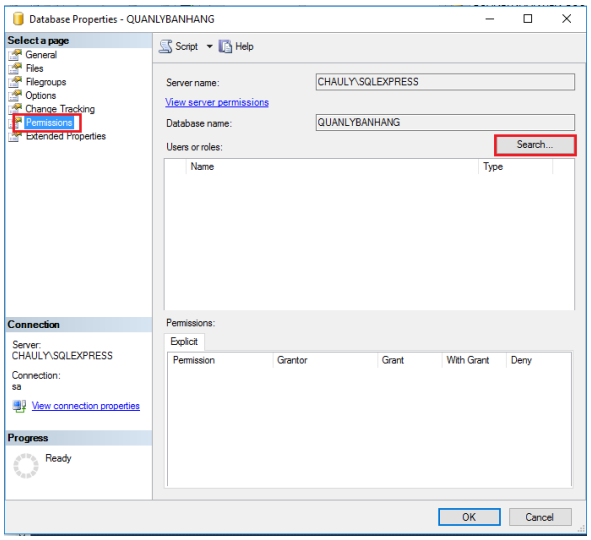


Bước 3: Cấp quyền cho người dùng

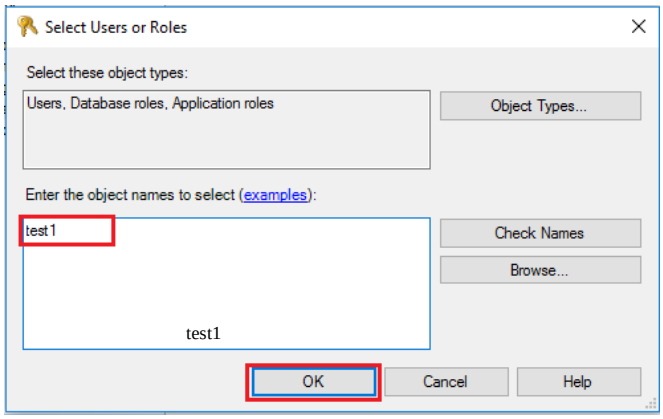
Click phải bảng (table) hoặc cơ sở dữ iệu (Database) -> chọn **Properties**



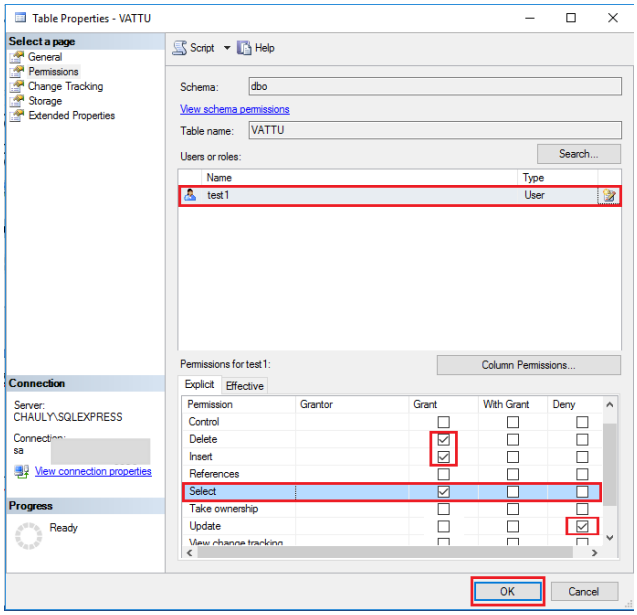
Chọn page Permissions ở khung bên trái, sau đó chọn Search:



Nhập tên User vừa tạo ở trên vào ô "Enter the object name to select" => Chọn OK



Bạn có thể gán quyền cho User test1 các quyền như SELECT, INSERT, UPDATE, DELETE…



Sinh viên kiểm tra lại việc tạo tài khoản, phần quyền User trên bảng VATTU, đăng nhập bằng User test1 sau đó New Query thực hiện 2 câu Query sau để kiểm tra kết quả:

```
SELECT * FROM VATTU  --câu này thành công
```

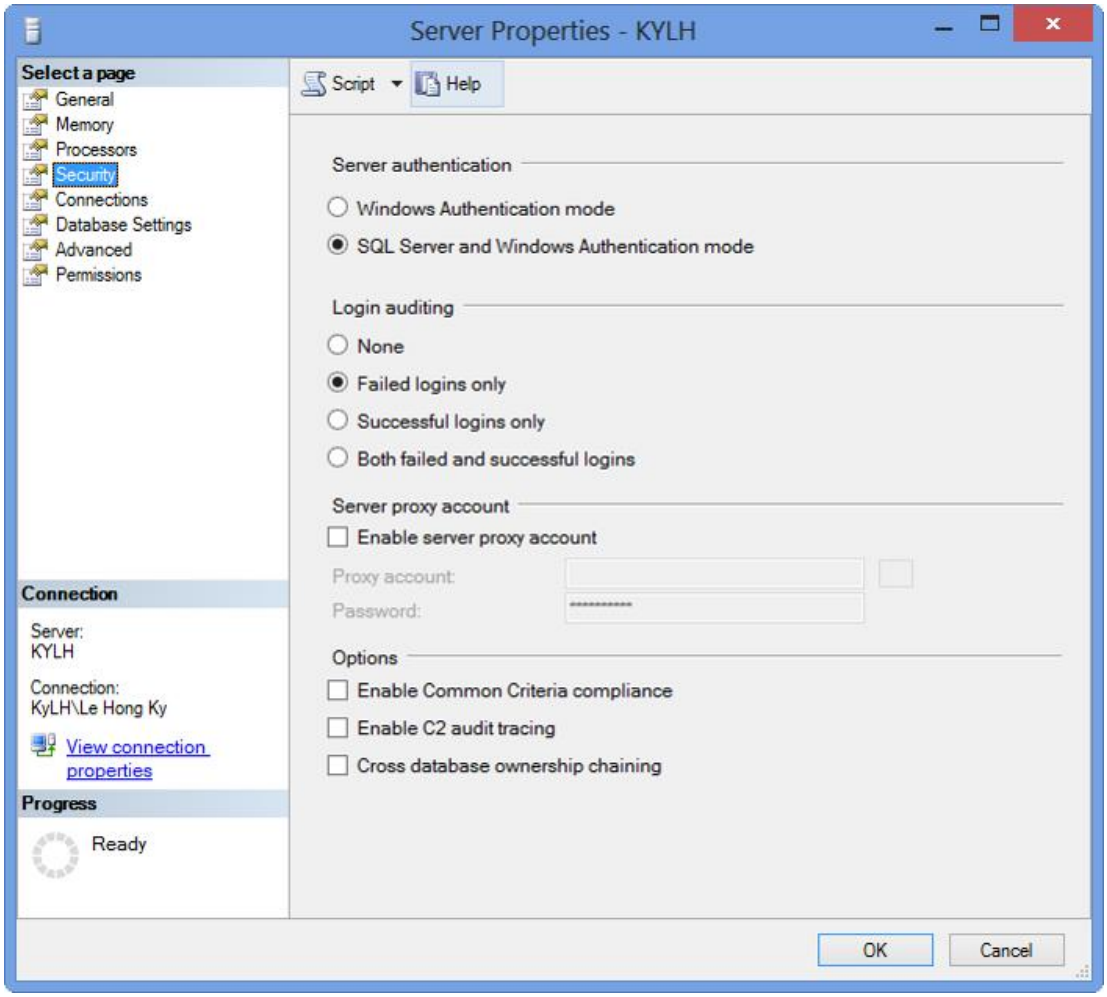
```
UPDATE VATTU SET SOLUONG = 10 WHERE MAHANG = 'M001' ---câu này
không thực hiện được
```

Bảo mật cơ sở dữ liệu sql server – Thiết lập chế độ chứng thực Windows và SQL Server

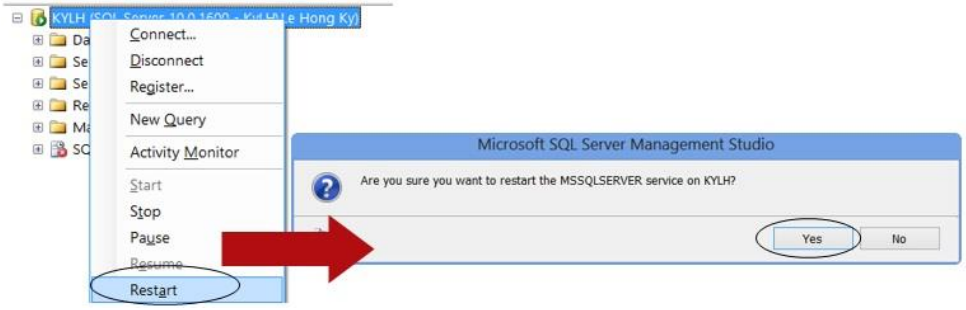
Bước 1: Đăng nhập vào SQL Server bằng chứng thực Windows.

Bước 2: Click phải tên server -> Chọn Properties

Bước 3: Chọn SQL Server and Windows Authentication mode



Bước 4: Khởi động lại SQL Server (đăng nhập lại bằng quyền Admin sa)



Bước 5: Sinh viên có thể đăng nhập vào SQL bằng tài khoản Windows với quyền chứng thực (Authentication) admin sa.

Cách 2: Thực hiện bằng câu lệnh (lưu ý đăng nhập với quyền admin để tạo)

Bước 1: Tạo tài khoản đăng nhập

Cách 1:

Create login tên_login with password = 'nhập_mật_khẩu'

Cách 2:

sp_addlogin 'tên_login','mật_khẩu'

Bước 2: Tạo người dùng

Cách 1:

Create user tên_user for login tên_login

Cách 2:

sp_adduser 'tên_login','tên_user'

Bước 3: Cấp quyền cho người dùng

Grant danh_sách_quyền on tên_bảng to tên_user [with grant option]

*Tuỳ chọn **[with grant option]** được sử dụng để cho phép người dùng được phép cấp lại những quyền của mình cho người dùng khác.*

Ví dụ:

```
Create login test2 with password = '123'

Create user test2 for login test2  ---tạo trên db QLBH

Grant SELECT, INSERT on VATTU to test2 with grant option ---tạo
trên db QLBH
```

Sinh viên đăng nhập bằng test2 để kiểm tra kết quả (lưu ý: nhớ chọn Database QUANLYBANHANG để thực thi).

```
SELECT * FROM VATTU  --câu này thành công
UPDATE VATTU SET SOLUONG = 10 WHERE MAHANG = 'M001' ---câu này
không thực hiện được.
```

Lưu ý: bạn có thể gán quyền CREATE DATABASE, CREATE TABLE trên user như sau:

```
Grant CREATE DATABASE to test2 --nếu test2 được tạo tài khoản và
user trên db master
Grant CREATE TABLE to test2
```

Kiểm tra "with grant option": Tạo thêm tài khoản trên db QLBH để cấp test2 cấp lại quyền.

```
Create login test22 with password = '123'

Create user test22 for login test22  ---tạo trên db QLBH
```

Sau đó sinh viên Login với tài khoản test2 để cấp lại quyền cho test22

```
Grant SELECT on VATTU to test22   ---db QLBH của test2
```

Sinh viên login với tài khoản test22 để kiểm tra, người dùng chỉ SELECT được, INSERT không được:

```
SELECT * FROM VATTU

INSERT INTO VATTU VALUES('M009',N'Ghế','NCC003',1,10,N'Cái',30)
```

Lưu ý khi chúng ta muốn cấp quyền trên các cột, chúng ta phải chỉ định các cột được cấp như cú pháp bên dưới:

Cách 1:

Grant select(danh_sách_cột) on tên_bảng to tên_user

Cách 2:

Grant select on tên_bảng(danh_sách_cột) to tên_user

Ví dụ chỉ cho phép người dùng test3 được phép xem 2 cột mahang và tenhang của bảng VATTU (lưu ý: cần tạo user test3 và chạy câu bên dưới thì câu này mới hiệu lực, vì chạy trên user test2 thì gán quyền trước bao phủ cả quyền Select trên cột này).

Ví dụ:

```
Create login test3 with password = '123'   --db master

Create user test3 for login test3    --db QLBH
```

Grant select(mahang, tenhang) on VATTU to test3

3. Chứng thực bằng Windows Authentication:

Bước 1: Tạo tài khoản đăng nhập hệ điều hành Windows, chúng ta có thể sử dụng câu lệnh sau và thực hiện trong CMD của Windows (lưu ý: nhớ chạy CMD bằng quyền Administrator)

net user accountName accountPassword /add

Sử dụng New Query trong SQL Server Management Studio và thực hiện các bước sau

Bước 2: Tạo login ánh xạ đến tài khoản đăng nhập Windows

create login "hostName\accountName" from windows

Bước 3: Tạo user

create user userName for login "hostName\acountName"

Bước 4: Cấp quyền cho user

grant permission on tableName to userName [with grant option]

Ví dụ:

```
create login "CHAULY\chaulyly" from windows --CHAULY: tên máy
create user test3 for login "CHAULY\chaulyly"--chạy trên db QLBH
grant SELECT on VATTU to test3 with grant option--chạy trên db
QLBH
```

Sinh viên restart lại máy để đăng nhập tài khoản mới, sau đó đăng nhập vào SQL Server bằng Window và kiểm tra kết quả.

4. Cấp quyền cho nhóm

Nhóm trong SQL Server bao gồm 1 hoặc nhiều user, điều này cũng tương tự như trong công ty hoặc tổ chức mỗi phòng ban có 1 hoặc nhiều nhân viên. Thay vì chúng ta cấp quyền cho từng user, người quản trị có thể cấp quyền theo nhóm. Và những user thuộc nhóm quyền nào sẽ có tất cả quyền của nhóm đó. Do đó, khi người quản trị thực hiện thêm bớt quyền sẽ dễ dàng hơn.

Bước 1: Tạo nhóm

Cách 1:

Create Role Tên_Nhóm

Cách 2:

Sp_AddRole 'Tên_Nhóm'

Bước 2: Cấp quyền cho nhóm

Grant danh_sách_quyền On Tên_Bảng To Tên_Nhóm

Bước 3: Thêm user vào nhóm

Sp_AddRoleMember 'Tên_Nhóm', 'Tên_User'

Ví dụ cấp quyền cho nhóm **xemvt** quyền xem dữ liệu cơ sở dữ liệu QuanLyBanHang. Trong nhóm quyền này có một user là **test4:**

```
Create role xemvt --- dùng server admin, bảng QLBH

Grant select on VATTU to xemvt --- dùng server admin, bảng QLBH

Create Login test4 With Password = '123' --- dùng server admin, bảng QLBH

Create User test4 For Login test4 --- dùng server admin, bảng QLBH

Sp_addRoleMember 'xemvt', 'test4'--- dùng server admin, bảng QLBH

SELECT * FROM VATTU  --- dùng user test4, select được
SELECT * FROM LOAIHANG --- dùng user test4, select không được
```

Sinh viên đăng nhập vào tài khoản test4 để kiểm tra quyền đã được cấp cho nhóm xemvt.

VI. BÀI TẬP TẠI LỚP:

- Sinh viên tạo Database **QUANLYNHANVIEN_B7_MSSV** (trong đó MSSV là mã số của sinh viên) với hai file CREATEDATABASE.sql và USEDATABASE.sql đính kèm. Sau đó New Query và thực hiện các yêu cầu sau bằng câu lệnh, đổi tên và nộp bài lên học trực tuyến:

+ Nơi nộp bài:

- **Assignment - Session 7 - Submission**

+ Tên file: StudentID-FullName-Assignment-Session7.sql
Ví dụ: 217000000044-NguyenVanA-Assignment-Session7.sql

+ Hạn nộp: theo lịch học của lớp

+ Đề bài:

Đề bài Lớp 221_71ITIS30203_01 (01, 02, 03):

Câu 1: Tạo tài khoản (trên master)

1.1 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập là *giamdoc* và password là *123456*

1.2 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập là *thutruong* và password là *thutruong*

1.3 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập *nhanvien* với password là *nv123456*

Câu 2: Tạo người dùng (trên database QUANLYNHANVIEN)

2.1 Tạo người dùng có tên *giamdoc* với tài khoản đăng nhập là *giamdoc*

2.2 Tạo người dùng có tên *thutruong* với tài khoản đăng nhập là *thutruong*

2.3 Tạo người dùng tên *nhanvien* với tài khoản đăng nhập là *nhanvien*

Câu 3: Cấp quyền (trên database QUANLYNHANVIEN)

3.1 Cấp quyền cho những người dùng có tên là: *giamdoc, thutruong* quyền thực thi các câu lệnh SELECT, INSERT, UPDATE trên bảng DEAN, PHONGBAN.

3.2 Cho phép những người dùng *nhanvien* quyền xem các cột: **mã nhân viên, họ nhân viên, tên lót nhân viên, tên nhân viên, ngày sinh, địa chỉ, phái, lương** trên bảng NHANVIEN (HONV, TENLOT, TENNV, MANV, NGSINH, DCHI, PHAI, LUONG).

3.3 Cấp quyền cho những người dùng *giamdoc, nhanvien* quyền SELECT, INSERT, UPDATE trên bảng PHANCONG.

3.4 Cho phép người dùng *thutruong* quyền xem dữ liệu trên bảng THANNHAN, đồng thời có thể cấp lại quyền này cho những người dùng khác.

3.5 Cấp quyền tạo cơ sở dữ liệu (Create Database) và tạo bảng (Create Table) cho người dùng có tên là *giamdoc*. (lưu ý: tạo thêm user trên master).

Đề bài Lớp 221_71ITIS30203_02 (01, 02, 03):

Câu 1: Tạo tài khoản (trên master)

1.1 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập là *giamdoc* và password là *123456*

1.2 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập là *truongphong* và password là *truongphong*

1.3 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập *nhanvien* với password là *nv123456*

Câu 2: Tạo người dùng (trên database QUANLYNHANVIEN)

2.1 Tạo người dùng có tên *giamdoc* với tài khoản đăng nhập là *giamdoc*

2.2 Tạo người dùng có tên *truongphong* với tài khoản đăng nhập là *truongphong*

2.3 Tạo người dùng tên *nhanvien* với tài khoản đăng nhập là *nhanvien*

Câu 3: Cấp quyền (trên database QUANLYNHANVIEN)

3.1 Cấp quyền cho những người dùng có tên là: *giamdoc, truongphong* quyền thực thi các câu lệnh SELECT, INSERT, DELETE trên bảng DEAN, PHONGBAN.

3.2 Cho phép những người dùng *nhanvien* quyền xem các cột: **mã nhân viên, họ nhân viên, tên lót nhân viên, tên nhân viên, ngày sinh, địa chỉ, phái, lương** trên bảng NHANVIEN (HONV, TENLOT, TENNV, MANV, NGSINH, DCHI, PHAI, LUONG).

3.3 Cấp quyền cho những người dùng *giamdoc, nhanvien* quyền SELECT, INSERT, UPDATE trên bảng PHANCONG.

3.4 Cho phép người dùng *truongphong* quyền xem dữ liệu trên bảng THANNHAN, đồng thời có thể cấp lại quyền này cho những người dùng khác.

3.5 Cấp quyền tạo cơ sở dữ liệu (Create Database) và tạo bảng (Create Table) cho người dùng có tên là *giamdoc*. (lưu ý: tạo thêm user trên master).

Đề bài Lớp 221_71ITIS30203_03 (01, 02):

Câu 1: Tạo tài khoản (trên master)

1.1 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập là *quanly* và password là *123456*

1.2 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập là *truongphong* và password là *truongphong*

1.3 Tạo tài khoản đăng nhập SQLServer với tên đăng nhập *nhanvien* với password là *nv123456*

Câu 2: Tạo người dùng (trên database QUANLYNHANVIEN)

2.1 Tạo người dùng có tên *quanly* với tài khoản đăng nhập là *quanly*

2.2 Tạo người dùng có tên *truongphong* với tài khoản đăng nhập là *truongphong*

2.3 Tạo người dùng tên *nhanvien* với tài khoản đăng nhập là *nhanvien*

Câu 3: Cấp quyền (trên database QUANLYNHANVIEN)

3.1 Cấp quyền cho những người dùng có tên là: *quanly, truongphong* quyền thực thi các câu lệnh SELECT, INSERT, UPDATE, DELETE trên bảng DEAN, PHONGBAN.

3.2 Cho phép những người dùng *nhanvien* quyền xem các cột: **mã nhân viên, họ nhân viên, tên lót nhân viên, tên nhân viên, ngày sinh, địa chỉ, phái, lương** trên bảng NHANVIEN (HONV, TENLOT, TENNV, MANV, NGSINH, DCHI, PHAI, LUONG).

3.3 Cấp quyền cho những người dùng *quanly, nhanvien* quyền SELECT, INSERT, UPDATE trên bảng PHANCONG.

3.4 Cho phép người dùng *truongphong* quyền xem dữ liệu trên bảng THANNHAN, đồng thời có thể cấp lại quyền này cho những người dùng khác.

3.5 Cấp quyền tạo cơ sở dữ liệu (Create Database) và tạo bảng (Create Table) cho người dùng có tên là *quanly*. (lưu ý: tạo thêm user trên master).

----------o0o----------