

# PHÂN QUYỀN VÀ QUẢN TRỊ NGƯỜI DÙNG

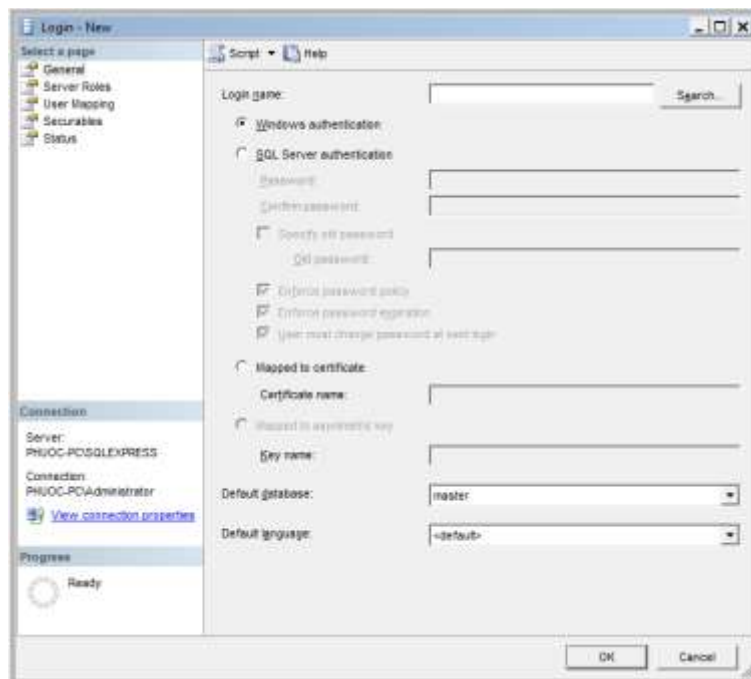
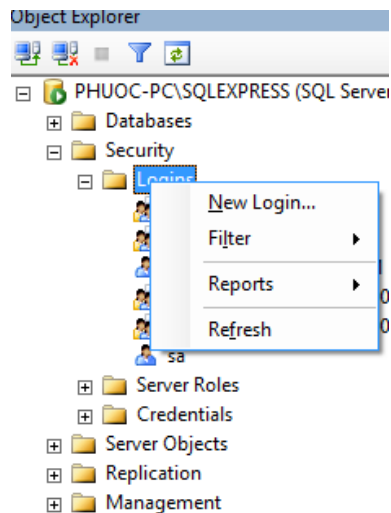
## Phần I. Lý thuyết

### 1. Tạo tài khoản đăng nhập

Tài khoản đăng nhập là một tài khoản mà người dùng (user) sử dụng để đăng nhập vào hệ thống SQL Server.

Để tạo tài khoản đăng nhập ta thực hiện các bước sau:

- Mở rộng danh mục Security trong server hiện hành > nhấp chuột phải vào Logins > chọn New login.



- Nhập tên tài khoản đăng nhập (login name), loại xác thực (windows authentication hay Sql Server authentication).
- Chọn thẻ Server Roles (nhóm quyền Server), trên thẻ này có thể chỉ ra nhóm quyền server cho đăng nhập.

- Chọn thẻ User mapping để chọn CSDL có thể truy cập.

Ngoài ra chúng ta có thể tạo tài khoản đăng nhập bằng thủ tục hệ thống có cú pháp như sau:

### Cú pháp:

```
sp_addlogin <tên tài khoản>[,<mật khẩu>] [,<CSDL mặc định>]
```

Trong đó:

- Tên tài khoản: Là tên của tài khoản được dùng để đăng nhập vào hệ thống.
- Mật khẩu: Là mật khẩu đăng nhập vào hệ thống, nếu không cung cấp mật khẩu thì mặc định là NULL.
- CSDL mặc định: Là CSDL sẽ được truy cập vào khi đăng nhập bằng tên tài khoản và mật khẩu đã chỉ định. Nếu không cung cấp CSDL mặc định thì CSDL Master sẽ được chọn làm CSDL mặc định.

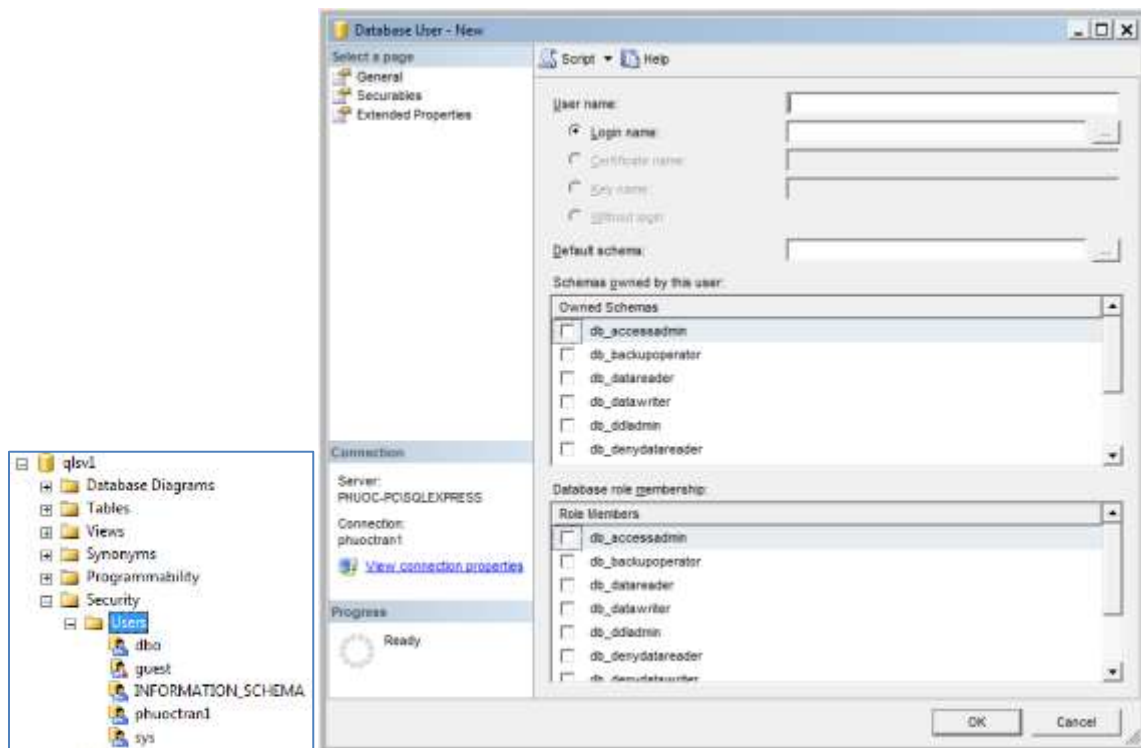
Ví dụ: Tạo tài khoản đăng nhập với tên là TAI\_KHOAN1, mật khẩu là 123456, CSDL mặc định là QLSV.

```
sp_addlogin 'Phuoctran1', '123456', 'qlsv1'
```

## 2. Tạo người dùng SQL Server.

Để tạo người dùng SQL-Server trước hết phải tạo tài khoản đăng nhập cho người dùng đó bởi vì tên người dùng sẽ tham khảo đến tên đăng nhập. Không giống như tên đăng nhập được tạo từ danh mục Security của Enterprise Manager, tên người dùng được tạo từ trong danh mục CSDL cụ thể. Lưu ý là trong quá trình tạo tài khoản đăng nhập nếu chúng ta chỉ ra CSDL nào mà tài khoản đăng nhập có thể truy cập tại thẻ User mapping thì chúng ta không cần tạo người dùng cho tài khoản đó nữa bởi vì khi đó hệ thống sẽ tạo ra một người dùng có tên giống với tên của tài khoản đăng nhập. Chúng ta có thể dùng trình ứng dụng Enterprise Manager để tạo người dùng như sau:

- Mở rộng danh mục CSDL hiện hành > Security > nhấn chuột phải vào Users > New users.



- Chọn quyền cho người dùng

Ngoài ra chúng ta có thể sử dụng thủ tục hệ thống để tạo mới một người dùng với cú pháp như sau:

**Cú pháp:**

```
sp_adduser <tên đăng nhập>,<tên người dùng>
```

Trong đó:

- Tên đăng nhập: Là tên tài khoản đăng nhập đã được tạo trước đó.
- Tên người dùng: Là tên người dùng cần tạo. Nếu không chỉ ra tên người dùng thì mặc định sẽ cùng tên với tên đăng nhập.

Ví dụ: Tạo người dùng có tên là USER1 trên cơ sở dữ liệu QLSV với tên tài khoản đăng nhập là TAI\_KHOAN1

```
USE QLSV
```

```
GO
```

```
sp_adduser 'Phuoctran1' , 'user1'
```

### **3. Quản lý quyền CSDL.**

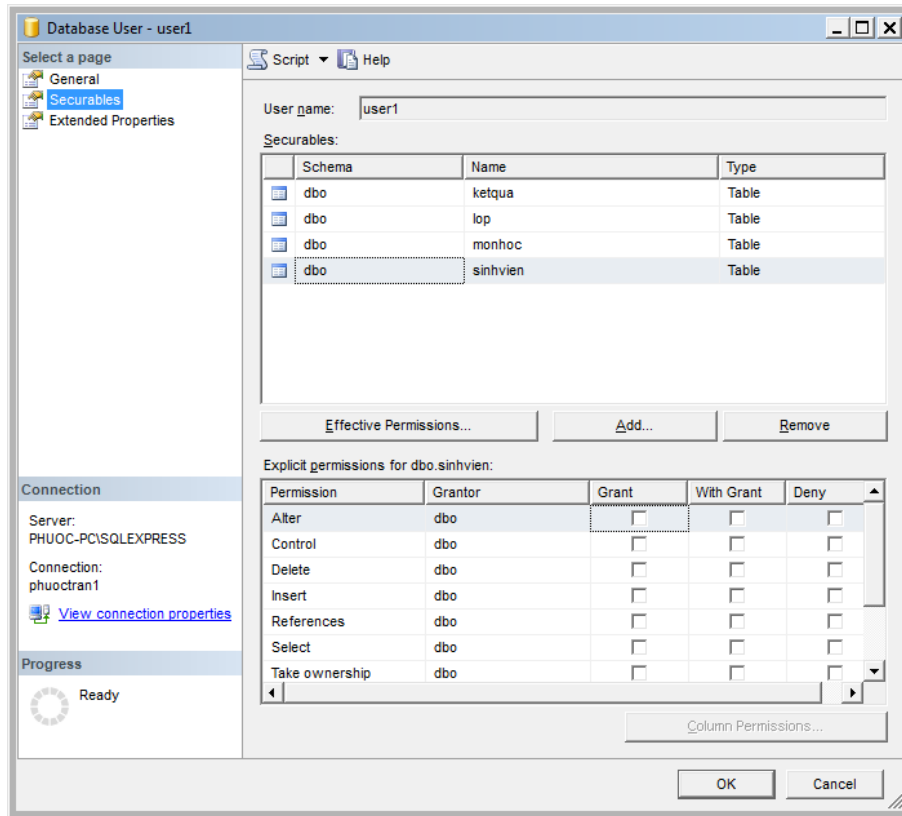
Quyền trên CSDL được dùng để kiểm soát sự truy cập của người dùng đến các đối tượng CSDL nhằm mục đích tránh sự sửa đổi dữ liệu của một số người dùng không được phép, đảm bảo cho CSDL hoạt động ổn định và hiệu quả. Có 2 loại quyền: Quyền thao tác trên các đối tượng CSDL và quyền định nghĩa các đối tượng CSDL.

#### **3.1. Quyền thao tác trên đối tượng CSDL.**

Quyền trên đối tượng CSDL là các quyền được cấp phát để người sử dụng có thể truy cập các đối tượng CSDL thường là trên đối tượng bảng (table), bảng ảo (View) hay thủ tục (stored procedure) bằng các lệnh SELECT, INSERT, UPDATE, EXECUTE.

Chúng ta có thể dùng Enterprise Manager hay lệnh T-SQL để cấp quyền, sau đây là các bước thực hiện:

- Mở rộng danh mục CSDL hiện hành > chọn đối tượng Users sẽ liệt kê ra danh sách các user đã tạo trên khung bên phải > nhấp chuột phải vào user cần cấp quyền > chọn Properties.
- Trong màn hình tiếp theo sau khi chọn Securables chúng ta gán quyền cho người dùng. (như hình bên dưới)



Chúng ta có thể cấp quyền cho người dùng bằng lệnh T-SQL như sau:

### Cú pháp:

GRANT <các lệnh cập nhật hay thực thi thủ tục> | <ALL>

ON <tên đối tượng>

TO <tên user>

Trong đó:

- Các lệnh cập nhật là các lệnh SELECT, INSERT, UPDATE, DELETE, lệnh thực thi thủ tục là EXEC.
- Từ khoá ALL là cấp tất cả các quyền trên đối tượng liệt kê trong từ khoá ON.
- Tên đối tượng: Là tên đối tượng cần cấp quyền cho người dùng tác động lên có thể là table, view hay procedure.
- Tên user: Là tên người dùng cần cấp quyền.

Ví dụ: Cấp các quyền SELECT, INSERT, UPDATE trên bảng LOP của CSDL có tên là QLSV cho người dùng USER1

```
USE QLSV
```

```
GO
```

```
GRANT SELECT, INSERT, UPDATE
```

```
ON LOP
```

```
TO USER1
```

Ví dụ: Cấp tất cả các quyền trên bảng SINHVIENT cho USER1

```
USE QLSV
GO
GRANT ALL
ON SINHVIEN
TO USER1
```

Ví dụ: Cấp quyền thực thi thủ tục có tên là DS\_SV cho người sử dụng USER1.

```
USE QLSV
GO
GRANT EXEC
ON DS_SV
TO USER1
```

Để có thể lấy lại quyền đã cấp chúng ta sử dụng lệnh REVOKE có cấu trúc như sau:

**Cú pháp:**

```
REVOKE <các lệnh cập nhật hay thực thi thủ tục> | <ALL>
ON <tên đối tượng>
FROM <tên user>
```

Ví dụ: Lấy lại quyền INSERT, UPDATE trên bảng LOP đã cấp cho USER1 trước đó.

```
USE QLSV
GO
REVOKE INSERT, UPDATE
ON LOP
FROM USER1
```

Ví dụ: Lấy lại tất cả các quyền đã cấp cho USER1 trên bảng SINHVIEN

```
USE QLSV
GO
REVOKE ALL
ON SINHVIEN
FROM USER1
```

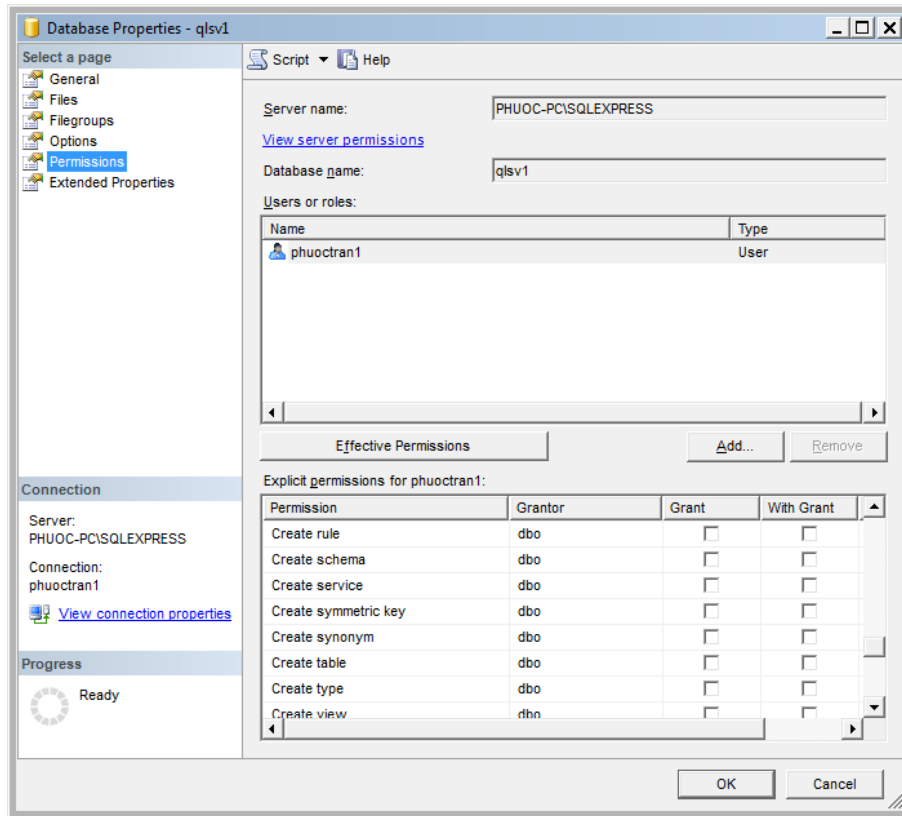
### **3.2. Quyền định nghĩa đối tượng CSDL.**

Quyền định nghĩa các đối tượng CSDL cho phép người dùng tạo ra các đối tượng CSDL: create, alter table, ...

Để tạo quyền định nghĩa các đối tượng CSDL chúng ta thực hiện các bước sau:

Bước 1: Trong Server hiện hành mở rộng danh mục Databases > nhấp chuột phải vào CSDL muốn cấp quyền > chọn Properties.

Bước 2: Trong màn hình Properties chọn thẻ Permissions, sau đó cấp quyền bằng cách chọn vào các ô kiểm tương ứng. Sau khi cấp quyền xong, chọn OK để hoàn tất.



Ngoài ra chúng ta cũng có thể dùng lệnh T-SQL để cấp quyền định nghĩa đối tượng với cú pháp như sau:

#### Cú pháp:

```
GRANT <các quyền định nghĩa đối tượng> | <ALL>
TO <tên user>
```

Trong đó:

- Các quyền định nghĩa đối tượng: Là các quyền định nghĩa đối tượng CSDL như đã trình bày ở phần trên.
- ALL: Cấp tất cả các quyền cho người dùng.
- Tên user: Là tên người dùng cần cấp quyền.

Ví dụ: Cấp quyền Create Table, Create SP cho người dùng có tên là USER1

```
GRANT Create Table, Create Proc
TO USER1
```

Ví dụ: Cấp tất cả quyền thực thi cho USER1.

```
GRANT ALL
TO USER1
```

Bên cạnh việc cấp quyền thì chúng ta có thể lấy lại quyền đã cấp bằng lệnh REVOKE có cấu trúc như sau:

#### Cú pháp:

```
REVOKE <các quyền định nghĩa đối tượng> | <ALL>
```

FROM <tên user>

Ví dụ: Lấy lại quyền Create Table, Create Proc đã cấp cho USER1

REVOKE Create Table, Create Proc

FROM USER1

Hay lấy lại tất cả các quyền đã cấp cho USER1

REVOKE ALL

FROM USER1

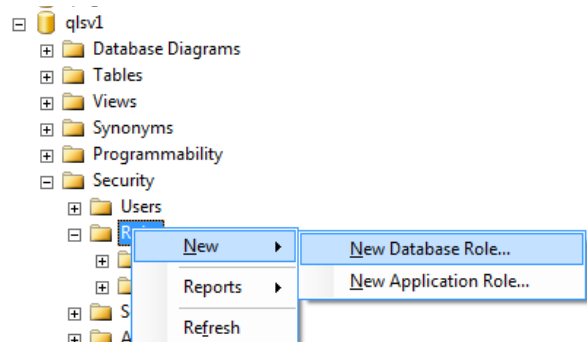
#### 4. Quản lý nhóm quyền CSDL.

Trong một CSDL có nhiều người sử dụng, và mỗi người sử dụng đều được cấp một số quyền nhất định. Chúng ta sẽ gặp khó khăn trong việc quản lý quyền và người sử dụng nếu như CSDL có số lượng người dùng nhiều và các quyền cấp phát đa dạng. Do đó để đơn giản hoá việc quản lý nhiều quyền cấp cho nhiều người dùng, Microsoft SQL Server đưa ra nhóm quyền CSDL. Các nhóm quyền được thiết kế cho phép các nhóm những người dùng nhận các quyền CSDL giống nhau mà không phải cấp những quyền này một cách riêng biệt. Thay vì cấp từng quyền cho từng người dùng, chúng ta tạo ra nhóm quyền đại diện cho các quyền được sử dụng bởi một nhóm người dùng và sau đó cấp nó cho nhóm người dùng.

Để sử dụng được nhóm quyền, đầu tiên chúng ta phải tạo ra nhóm quyền, sau đó gán các quyền cho nhóm quyền và gán người dùng cho nhóm quyền.

Để tạo nhóm quyền, chúng ta thực hiện các bước sau:

- Chọn database > Security > Roles > Chọn New Database Roles > chọn các quyền cho Role này.



Chúng ta cũng có thể tạo và quản lý nhóm quyền bằng lệnh T-SQL như sau:

#### Tạo nhóm quyền:

##### Cú pháp:

sp\_addrole <tên nhóm quyền>

Trong đó:

- Tên nhóm quyền: Là tên của nhóm quyền cần tạo và phải duy nhất trong một CSDL.

Ví dụ: Tạo nhóm quyền có tên là Xem\_dulieu.

USE QLSV

GO

sp\_addrole 'Xem\_dulieu'

### **Thêm quyền vào nhóm quyền:**

#### **Cú pháp:**

GRANT <các lệnh cập nhật hay thực thi thủ tục> | <ALL>

ON <tên đối tượng>

TO <tên nhóm quyền>

Ví dụ: Gán các quyền SELECT, INSERT, UPDATE trên bảng SINHVIEN cho nhóm quyền Xem\_dulieu.

GRANT SELECT, INSERT, UPDATE

ON SINHVIEN

TO Xem\_dulieu

### **Thêm người dùng vào nhóm quyền:**

#### **Cú pháp:**

sp\_addrolemember <tên nhóm quyền>, <tên người>

Ví dụ: Thêm người dùng USER1 vào nhóm quyền Xem\_dulieu.

sp\_addrolemember 'Xem\_dulieu' , 'USER1'



## **Phần 2: Bài tập**

1. Tạo cơ sở dữ liệu quản lý sinh viên gồm các bảng:
  - a. Lop (malop, tenlop)
  - b. Sinhvien (masv, hoten, ngaysinh, malop)
  - c. Monhoc (Mamh, tenmh, tinchi)
  - d. Ketqua (Masv, mamh, diem)
2. Tạo tài khoản đăng nhập login1 cho CSDL này.
3. Cấp phát quyền tạo, xoá, và thay đổi table cho tài khoản này.
4. Cấp phát quyền select cho CSDL này.

## **Phần 3: kiểm tra kết thúc.**