

BÀI THỰC HÀNH SỐ 7:

Bảo đảm dữ liệu trong SQL Server

1. Phân quyền và bảo mật trong SQL Server

1. Tạo và quản lý người dùng

a) Các chế độ xác thực

Để truy cập vào SQL Server ta dùng hai chế độ xác thực:

- *Xác thực thông qua hệ điều hành:* Với kiểu xác thực này, SQL Server dựa vào Windows NT/2000 để cấp bảo mật đăng nhập. Khi người dùng đăng nhập vào Windows NT/2000, sổ định danh tài khoản người dùng được kiểm tra sự hợp lệ. SQL Server tích hợp quá trình bảo mật đăng nhập của nó với quá trình bảo mật đăng nhập của Windows để cung cấp những dịch vụ này. Khi người dùng xác thực bằng hệ điều hành thì không cần thêm chế độ xác thực nào nữa để truy cập SQL Server.
- *Chế độ xác thực hỗn hợp:* Với chế độ xác thực hỗn hợp người dùng có thể truy cập vào SQL Server bằng xác thực thực Windows hoặc bằng xác thực SQL Server. Khi chế độ xác thực kết hợp được dùng, kết nối được tạo từ hệ thống không bảo mật, SQL Server xác thực đăng nhập bằng cách kiểm tra tài khoản đăng nhập có được thiết lập để truy cập hay không. SQL Server thực hiện xác thực tài khoản này bằng cách so sánh tên tài khoản và mật khẩu do người dùng cung cấp để thực hiện kết nối với thông tin tài khoản được lưu trong CSDL. Nếu tài khoản đăng nhập chưa được thiết lập hoặc người dùng nhập sai thì SQL Server từ chối kết nối.

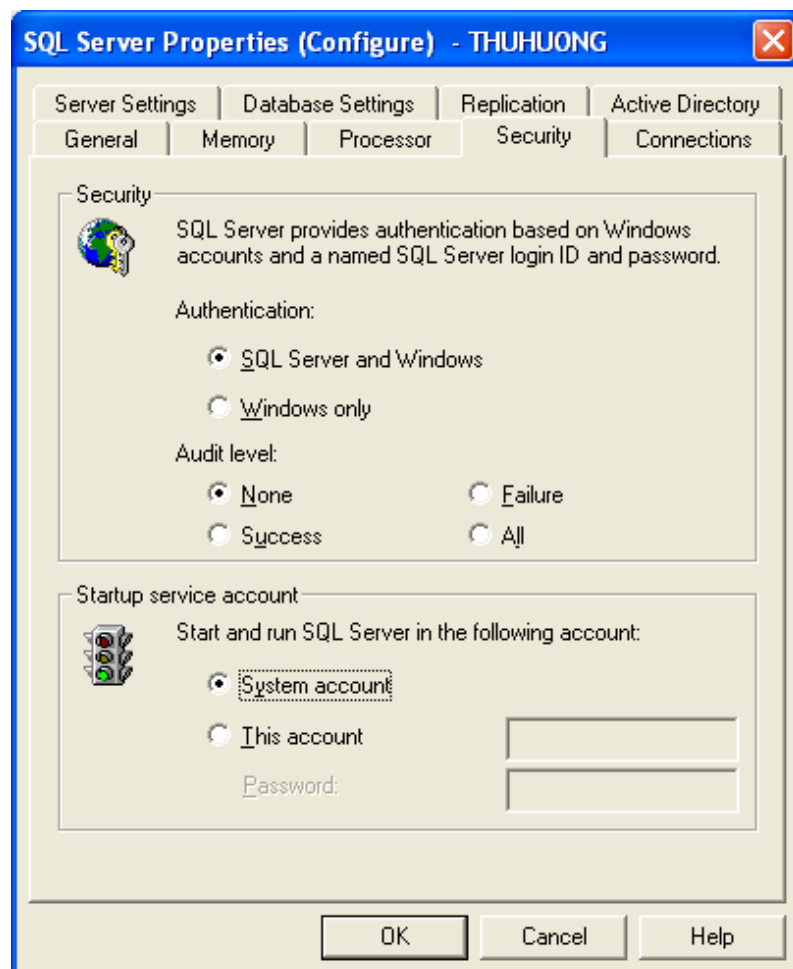
Thiết lập chế độ xác thực:

** Đối với SQL Server 2000:*

- + Trong cửa sổ Enterprise Manager, Right click lên tên server quản lý CSDL mà muốn thiết lập chế độ xác thực và chọn Properties. Xuất hiện cửa sổ Properties như hình 3.58.
-

Chọn tab Security.

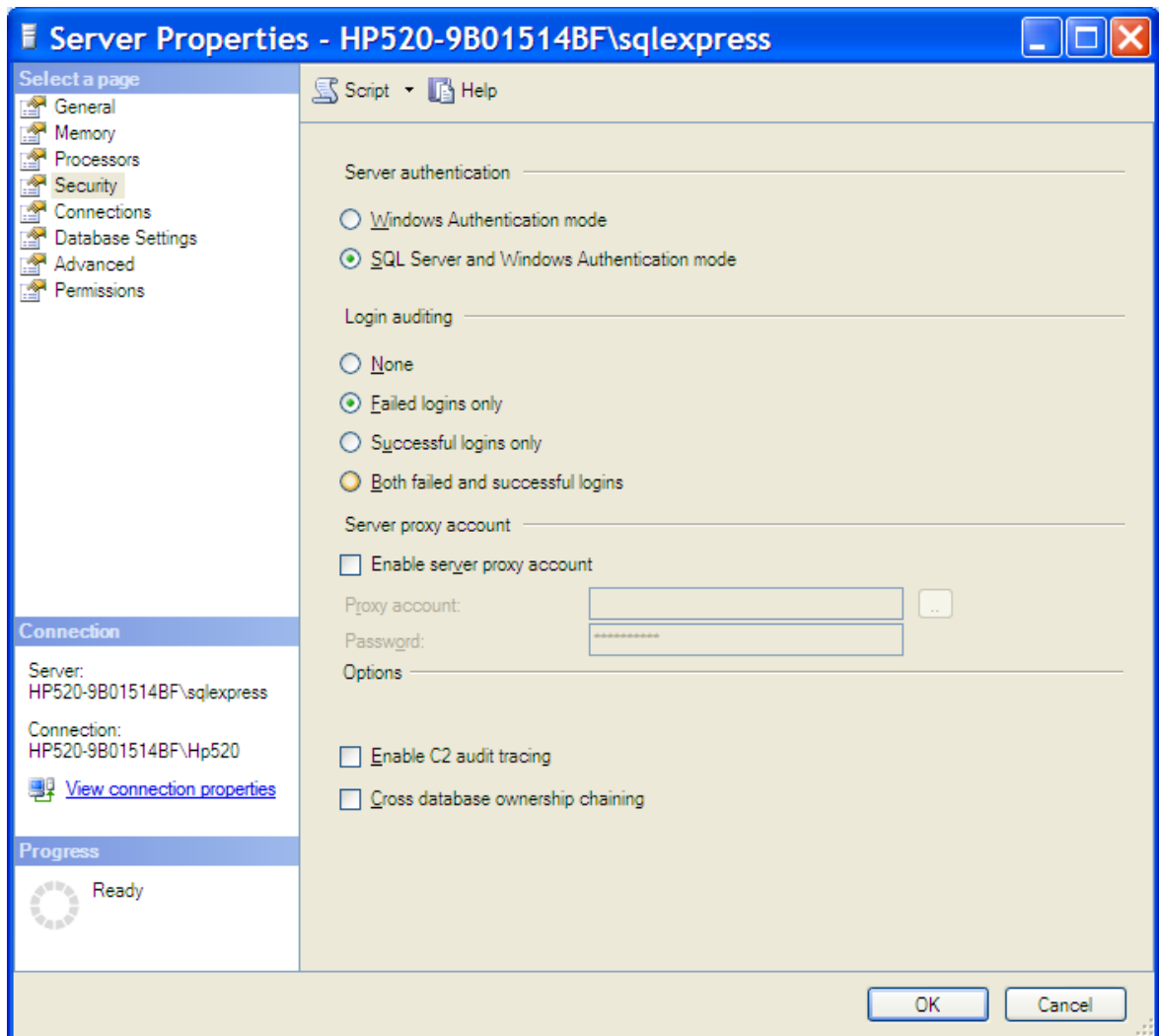
- + Vùng Security ta chọn chế độ xác thực: SQL Server and Windows hoặc Windows Only. Và các mức dò xét hành vi đăng nhập, tùy thuộc vào yêu cầu ảo mật. Có 4 mức cho sẵn đó là:
 - *None*: Không thực hiện dò xét hành vi,
 - *Success*: Ghi nhận tất cả các đăng nhập thành công,
 - *Failure*: Ghi nhận những đăng nhập không thành công,
 - *All*: ghi nhận tất cả các lần đăng nhập.
- + Trong vùng Startup service account: Chỉ ra tài khoản Windows được dùng khi SQL Server khởi động.
 - + System account: các tài khoản hệ thống cục bộ được xây dựng sẵn.
 - + This account: Chỉ ra một tài khoản cụ thể.



Hình 1. Cửa sổ Properties

* Đối với SQL Server 2005:

- + Trong cửa sổ SQL Server Management Studio, right click vào thẻ hiện của SQL Server muốn thiết lập chế độ xác thực và chọn Properties xuất hiện cửa sổ Server Properties (Hình 2), chọn trang Security.



Hình 2. Cửa sổ *Server Properties*

- + Mục Server Authentication: Chọn chế độ xác thực Window (Windows Authentication mode) hoặc chế độ xác thực hỗn hợp (SQL Server and Windows Authentication mode)
- + Login Auditing: Kiểu ghi nhận thông tin login (None, Failed logins only, Successful login only, ...)

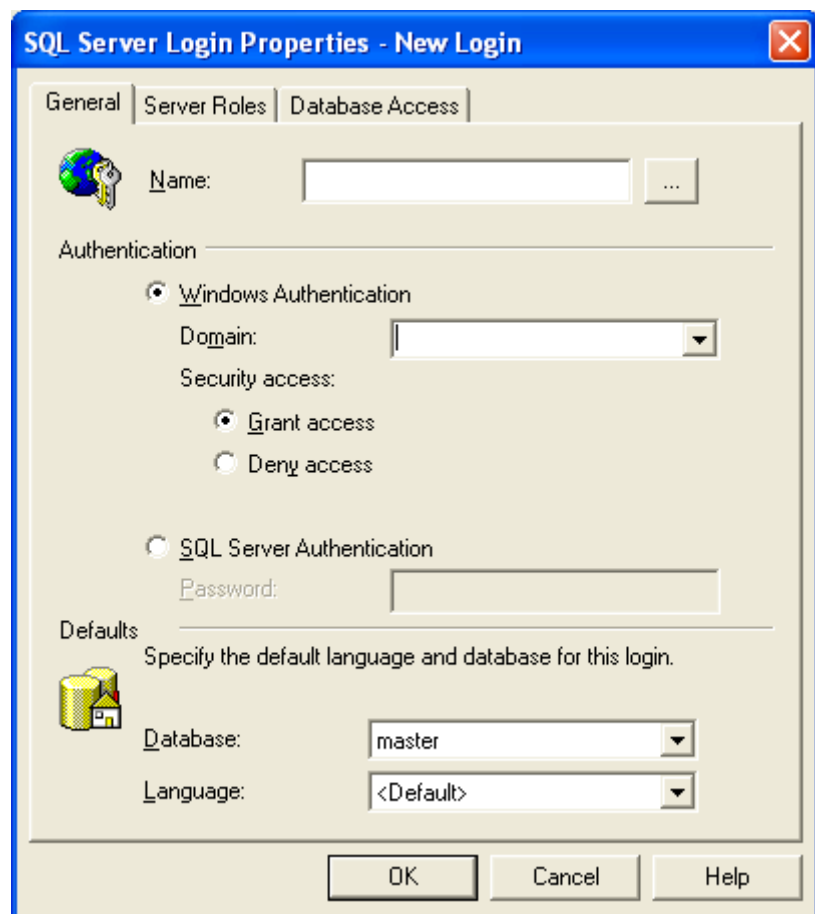
b) Người dùng và đăng nhập

Tài khoản dùng để kết nối tới SQL Server được gọi là tài khoản đăng nhập SQL Server. Cùng với tài khoản đăng nhập SQL Server, mỗi CSDL có một tài khoản người dùng ảo được gán với nó. Những tài khoản ảo này cung cấp một bí danh tới tài khoản đăng nhập SQL Server được gọi là tài khoản người dùng CSDL.

*** Tạo tài khoản đăng nhập SQL Server:**

¾ Dùng Enterprise manager:

- + Trong cửa sổ Enterprise Manager, mở rộng server muốn tạo tài khoản đăng nhập và mở rộng mục Security. Right click lên Logins và chọn New Login để xuất hiện cửa sổ SQL Server Login Properties (hình 3).



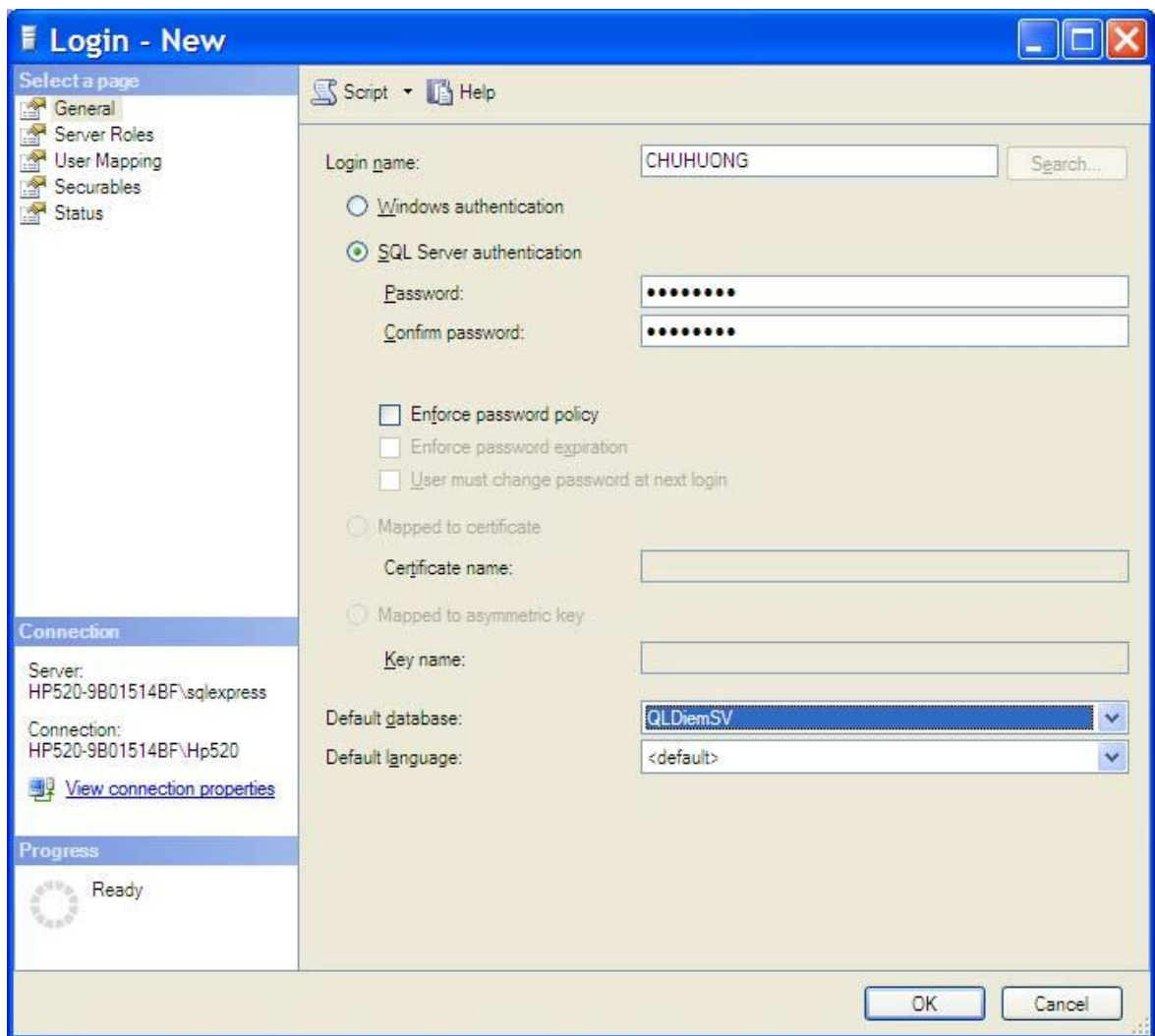
Hình 3 Cửa sổ New Login

- + Trên tab General:

- + Name: Nhập tên tài khoản đăng nhập. nếu chọn chế độ xác thực bằng Window thì tên tài khoản đăng nhập phải là tài khoản đã tồn tại trong Windows.
- + Authentication: Chọn chế độ xác thực của Windows là Windows Authentication hay chế độ xác hỗn hợp SQL Server Authentication.
- + Default: Chọn CSDL và ngôn ngữ mặc định sẽ được dùng.
- + Tab Server Roles: Ở đây ta chọn nhóm quyền server cho đăng nhập mới bằng cách chọn các nhóm quyền trong danh sách. Click vào nút Properties để xem và sửa đổi nhóm quyền đã chọn. Nếu là tài khoản đăng nhập thường thì không cần cấp quyền server.
- + Tab Database Access: Cho phép chọn CSDL mà người dùng được phép truy cập.

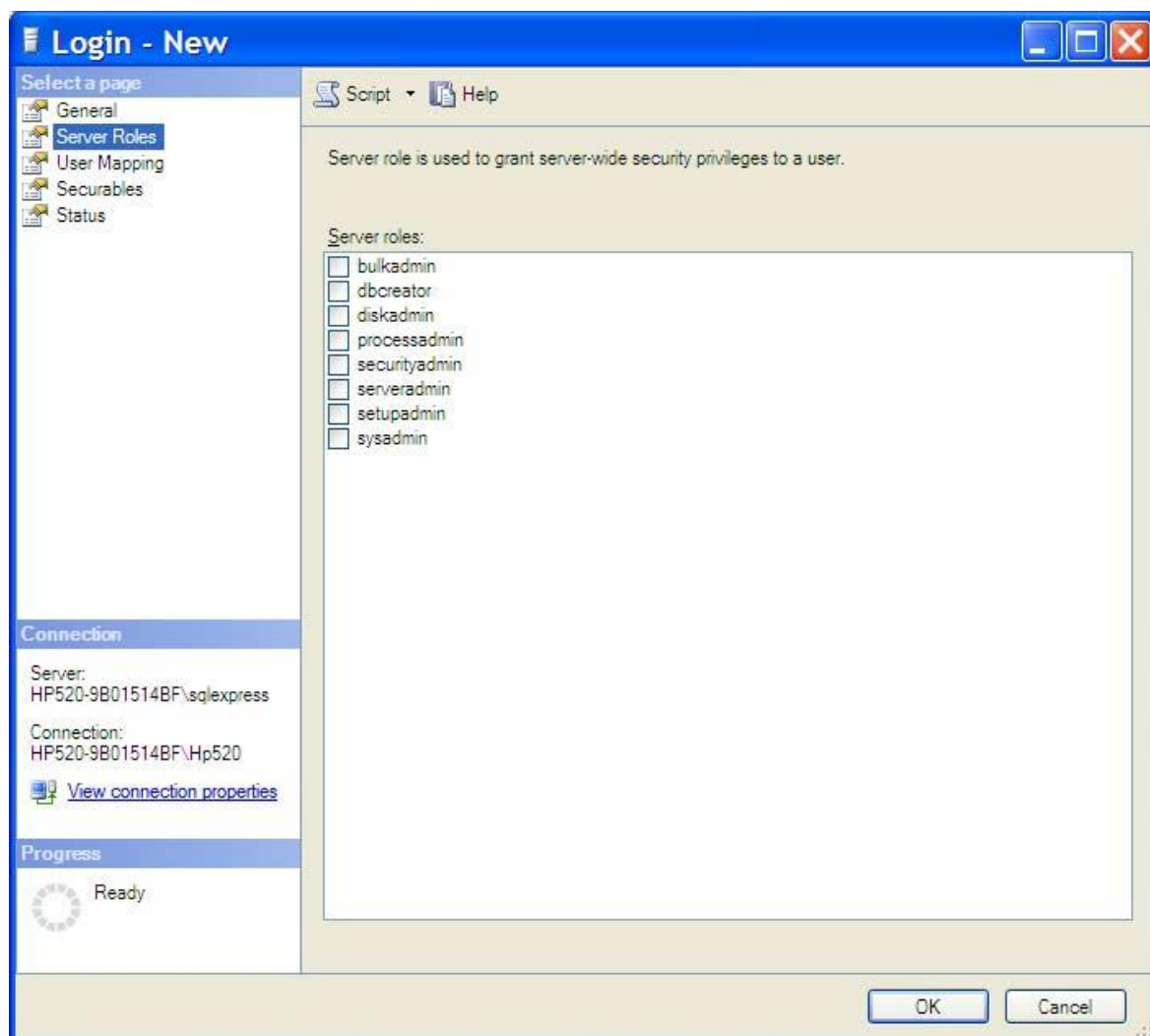
$\frac{3}{4}$ Dùng SQL Server Management Studio:

- + Trong cửa sổ SQL Server Management Studio, mở rộng thể hiện server muốn tạo tài khoản đăng nhập và mở rộng mục Security. Right click lên Logins và chọn New Login để xuất hiện cửa sổ Login – New (hình 3.61).
 - + Trang General có các lựa chọn:
 - Login Name: Nhập tên tài khoản đăng nhập. Nếu chọn chế độ xác thực bằng Window thì tên tài khoản đăng nhập phải là tài khoản đã tồn tại trong Windows.
 - Default database: Chọn CSDL mặc định được sử dụng.
 - Default language: Chọn ngôn ngữ mặc định.
-

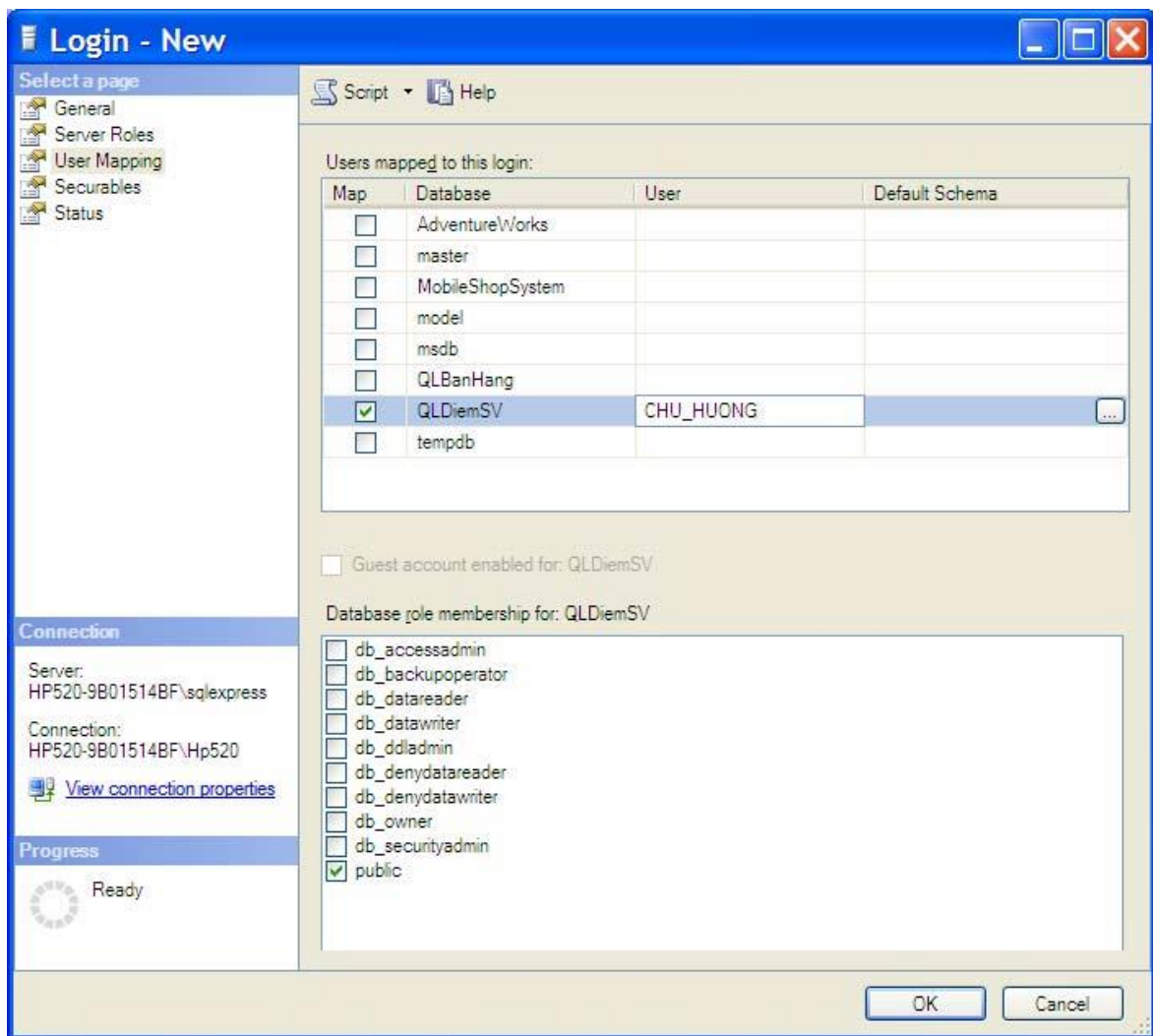


Hình 4. Cửa sổ Login - New

- + Trang Server Roles có các lựa chọn: Chọn nhóm quyền server cho đăng nhập mới bằng cách chọn các nhóm quyền trong danh sách (Hình 5).
- + Trang User Mapping (Hình 6): Cho phép chọn CSDL mà người dùng được phép truy cập.



Hình 5. Cửa sổ Login - New



Hình 6. Cửa sổ Login - New

$\frac{3}{4}$ Dùng T-SQL:

- Ta có thể tạo tài khoản đăng nhập bằng thủ tục `sp_addlogin` hoặc `sp_grandlogin`.
 - + Thủ tục `sp_addlogin` chỉ có thể thêm người dùng được xác thực bằng SQL Server.
 - + Thủ tục `sp_grandlogin` có thể thêm người dùng được xác thực bằng Windows.

Ví dụ 3.11. Tạo tài khoản đăng nhập *Huongct* với Password là 'abcd' và CSDL mặc định là 'QLDiemSV'

```
EXEC sp_addlogin 'Huongct1', 'abcd', 'QLDiemSV'
```

Ví dụ 3.12. Tạo tài khoản đăng nhập *Huongct* với chế độ xác thực Windows.

```
EXEC sp_grantlogin 'THUHUONG\Huongct'
```

- Ngoài ra, đối với SQL Server 2005 ta có thể sử dụng cú pháp T-SQL sau:

+ Tạo Login

```
CREATE LOGIN login_name { WITH PASSWORD =  
'password' [, <option_list>[ ,... ] ] | FROM  
WINDOWS [ WITH <windows_options> [ ,... ] ] }
```

```
<option_list> ::=  
    DEFAULT_DATABASE = database  
    | DEFAULT_LANGUAGE = language  
    | CHECK_EXPIRATION = { ON | OFF }  
    | CHECK_POLICY = { ON | OFF }  
    [ CREDENTIAL = credential_name ]
```

```
<windows_options> ::=  
    DEFAULT_DATABASE = database  
    | DEFAULT_LANGUAGE = language
```

+ Sửa Login

```
ALTER LOGIN login_name  
{  
    <status_option>  
    | WITH <set_option> [ ,... ]  
}
```

```
<status_option> ::=  
    ENABLE | DISABLE
```

```
<set_option> ::=  
    PASSWORD = 'password'  
    [  
        OLD_PASSWORD = 'oldpassword'  
    ]  
    | DEFAULT_DATABASE = database  
    | DEFAULT_LANGUAGE = language  
    | NAME = login_name  
    | CHECK_POLICY = { ON | OFF }  
    | CHECK_EXPIRATION = { ON | OFF }
```

+ Xóa Login

`DROP LOGIN login_name`

Ví dụ 3.13. Tạo các login

- Tạo Login HUONGCT dùng chế độ xác thực SQL

```
USE master
CREATE LOGIN HUONGCT WITH PASSWORD = '123456';
GO
```

- Tạo Login [HP520-9B01514BF\Hp520] từ domain account Windows.

```
CREATE LOGIN [HP520-9B01514BF\Hp520] FROM WINDOWS;
GO
```

- Sửa Login HUONGCT

```
USE master
ALTER LOGIN HUONGCT WITH PASSWORD =
'12102006', DEFAULT_DATABASE = QLDiemSV;
```

- Xóa Login HUONGCT

```
USE master
DROP LOGIN HUONGCT
```

¾ Dùng Wizard trong SQL Server 2000:

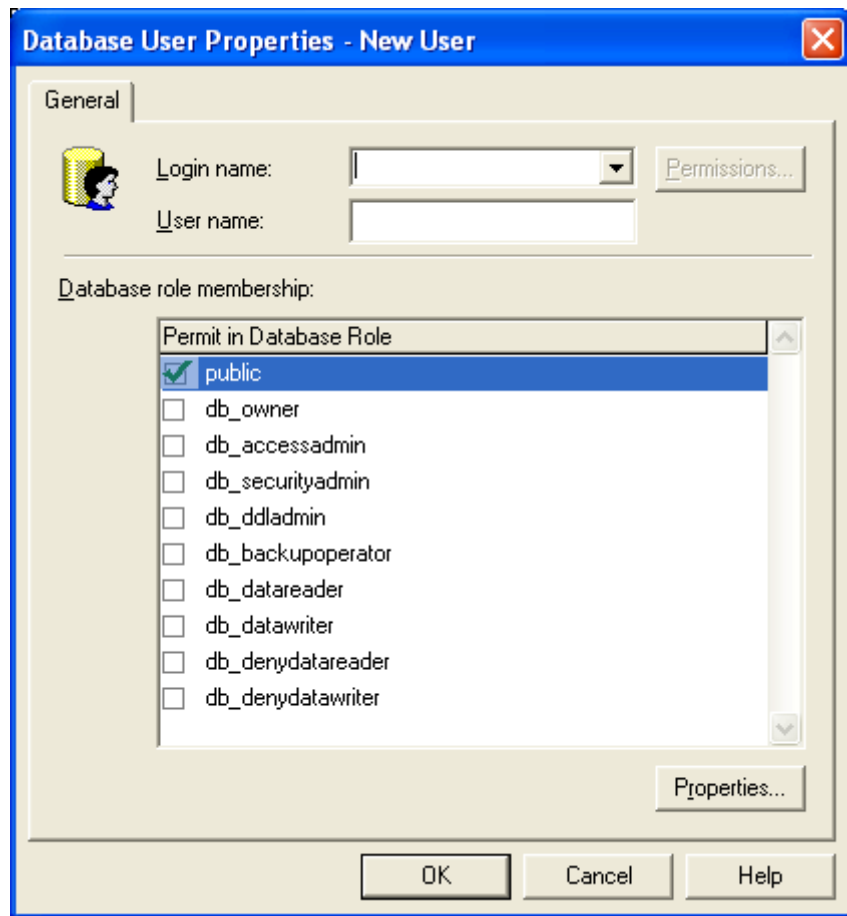
Vào Tools\Wizard xuất hiện cửa sổ hình 3.5. Chọn mục Database và chọn Create Login Wizard. Sau đó thực hiện theo sự chỉ dẫn của trình Wizard.

*** Tạo người dùng SQL Server:**

Để tạo người dùng SQL Server, trước hết ta phải tạo đăng nhập SQL Server cho người dùng đó vì tên người dùng tham chiếu đến tên đăng nhập.

¾ Dùng Enterprise manager:

- + Trong cửa sổ Enterprise Manager, mở rộng mục Database. Right click CSDL muốn tạo người dùng và chọn New\Database User xuất hiện cửa sổ New User (hình 7).



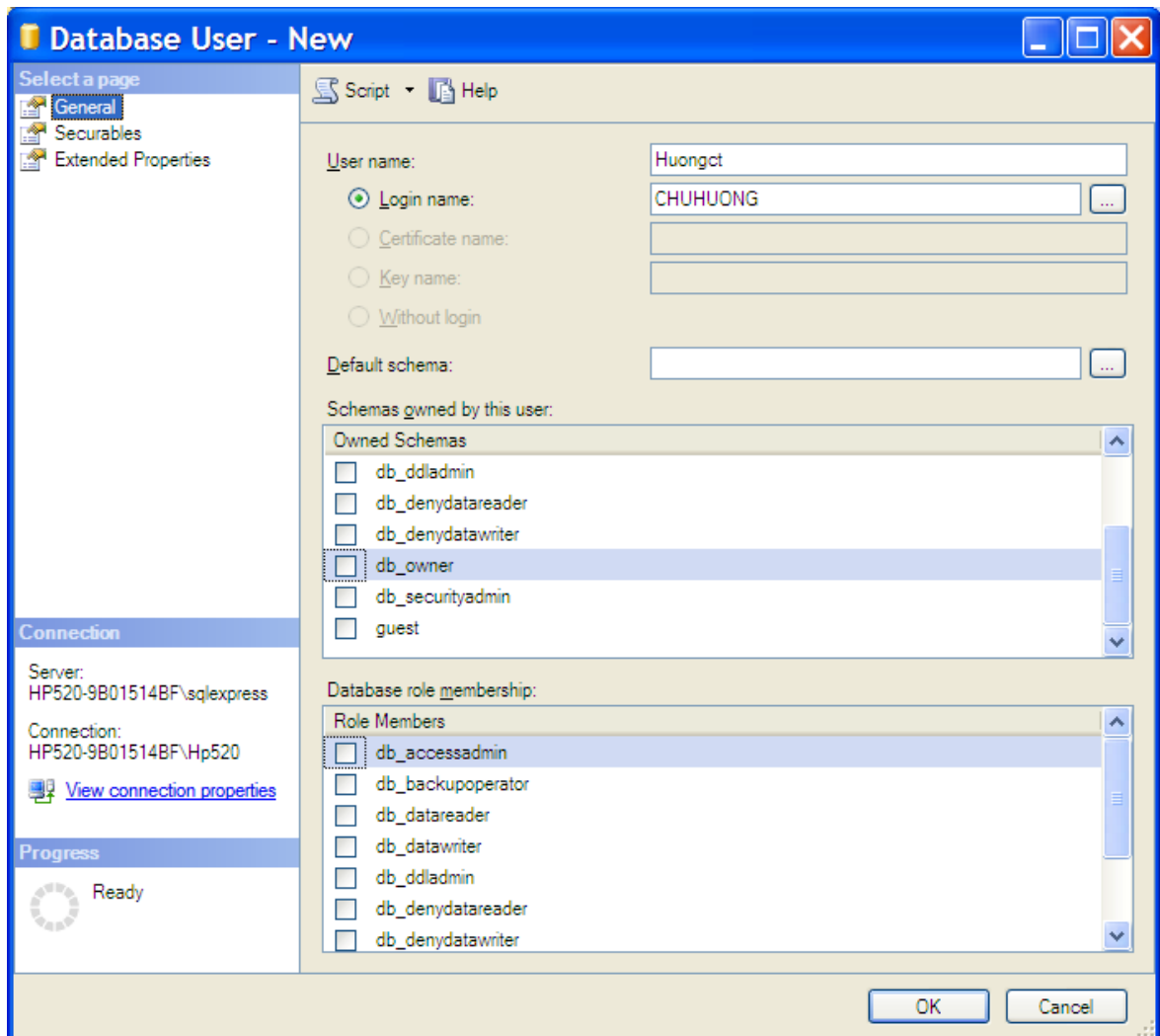
Hình 7. Cửa sổ New User

- + Nhập tên đăng nhập hợp lệ trong danh sách các tên đăng nhập của hộp combo Login Name và nhập tên người dùng mới vào hộp User Name (Mặc định SQL Server tự điền tên User Name trùng tên Login Name, ta có thể thay đổi tên này)
- + Chọn nhóm quyền CSDL mà người dùng mới này là thành viên, sau đó chọn OK.

^{3/4} Dùng SQL Server Management Studio:

- + Trong cửa sổ SQL Server Management Studio, mở rộng thể hiện server và mục Database. Mở rộng mục Security của cơ sở dữ liệu muốn tạo người dùng, Right click lên Users và chọn New User để xuất hiện cửa sổ Database User – New (hình 3.65).
- + Trang General có các lựa chọn:

- User name: Nhập tên người dùng
- Login name: Nhập tên hoặc chọn Login mà người dùng này ánh xạ đến.



Hình 8. Cửa sổ Database User - New

$\frac{3}{4}$ Dùng T-SQL:

- Ta có thể tạo người dùng mới bằng thủ tục sp_adduser.
- Đối với SQL Server 2005 ta có thể dùng cú pháp sau:

+ Tạo User

```
CREATE USER user_name
{ { FOR | FROM } LOGIN login_name |
  WITHOUT LOGIN }
[ WITH DEFAULT_SCHEMA = schema_name ]
```

+ Sửa User

```
ALTER USER user_name
    WITH <set_item> [ ,...n ]
<set_item> ::=
    NAME = new_user_name
    | DEFAULT_SCHEMA = schema_name
```

+ Xóa User

```
DROP USER user_name
```

Ví dụ 3.14. Tạo các người dùng mới là *Huong* với tên đăng nhập *Huongct* trên CSDL QLDiemSV

```
USE QLDiemSV
Go
sp_adduser 'Huongct', 'Huong'
```

Ví dụ 3.15. Tạo các người dùng mới trùng với tên đăng nhập *Huongct* trên CSDL QLDiemSV sử dụng xác thực của Windows

```
USE QLDiemSV
Go
sp_adduser 'THUHUONG\Huongct'
```

Ví dụ 3.16. Tạo các User

```
CREATE USER Huongct WITHOUT LOGIN
CREATE USER ChuHuong FOR LOGIN CHUHUONG
```

2. Quản lý nhóm quyền CSDL

Các nhóm quyền CSDL được thiết kế cho phép các nhóm những người dùng nhận các quyền CSDL giống nhau mà không cần phải cấp quyền một cách riêng biệt cho từng người dùng.

a) Các nhóm quyền Server cố định

Một số nhóm quyền ở cấp server đã được định nghĩa trước tại thời điểm cài đặt SQL Server. Những nhóm quyền cố định này được dùng để cấp quyền cho người quản trị CSDL. Các nhóm quyền server cố định được liệt kê trong danh sách sau:

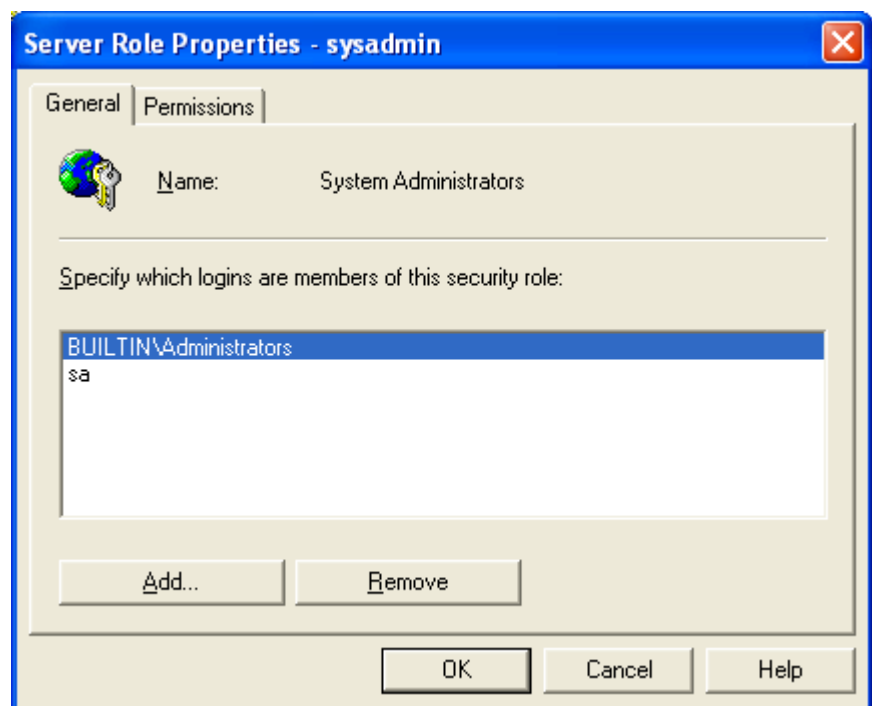
- + bulkadmin: Có thể thực thi lệnh BULK INSERT để thêm lượng lớn dữ liệu vào bảng.
-

- + dbcreator: Có thể tạo và sửa đổi CSDL.
- + diskadmin: Có thể quản lý các tập tin trên đĩa.
- + processadmin: Có thể quản lý các quá trình của SQL Server.
- + securityadmin: Có thể quản lý đăng nhập và tạo các quyền CSDL.
- + serveradmin: Có thể thiết lập bất kỳ tùy chọn server nào và có thể đóng CSDL.
- + setupadmin: Có thể quản lý các server liên kết và có thể đóng CSDL.
- + sysadmin: Có thể thực hiện bất kỳ hoạt động server nào.

Thêm người dùng vào các nhóm quyền server cố định.

³/₄ **Dùng Enterprise Manager**

- + Trong cửa sổ Enterprise Manager, mở rộng server và mở rộng mục Security. Sau đó chọn server roles và right click lên nhóm quyền server muốn thêm người dùng, chẳng hạn chọn System Administrators xuất hiện cửa sổ hình 9

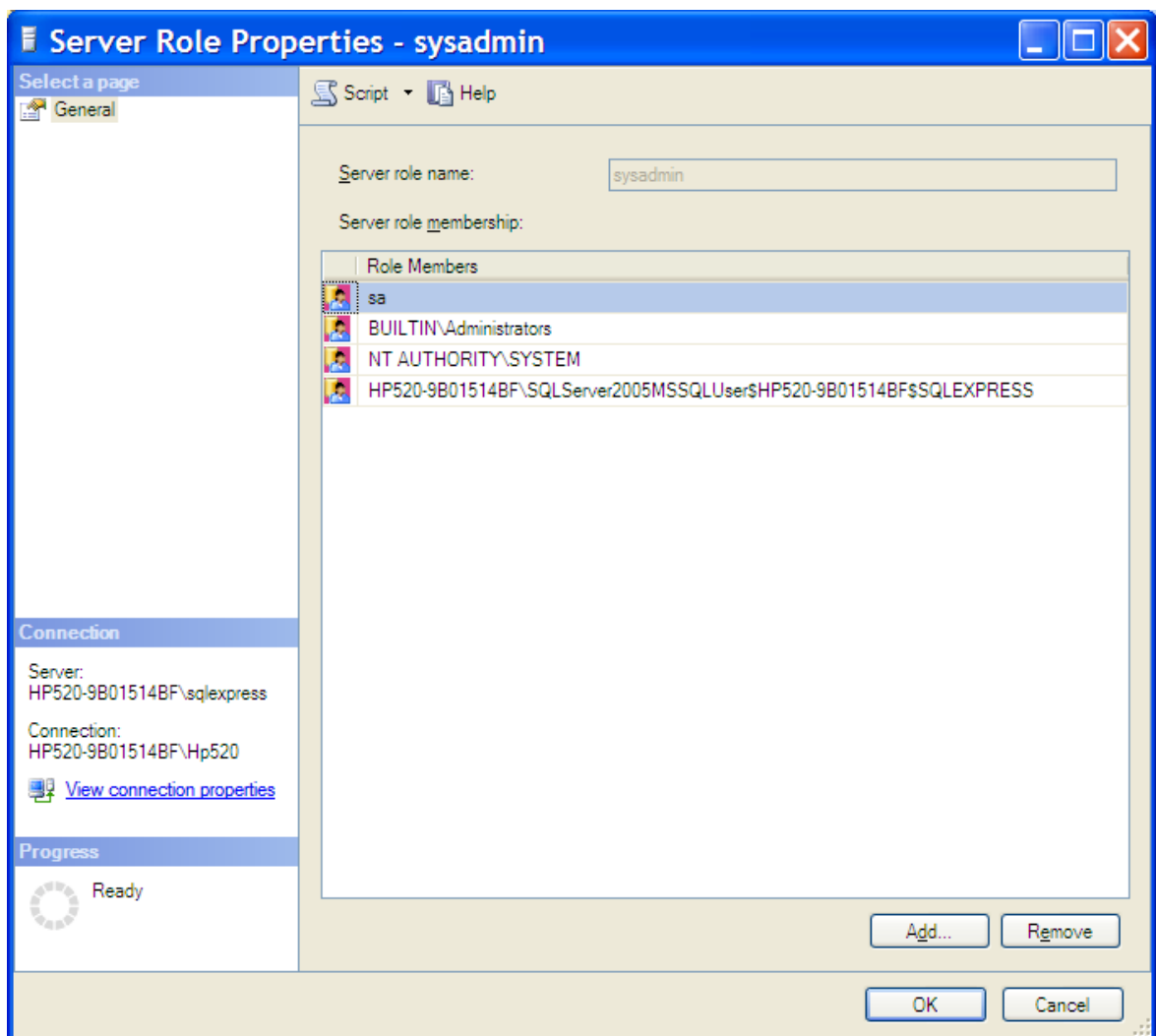


Hình 9. Cửa sổ *Server Role Properties*

- + Click nút Add để thêm người dùng vào trong nhóm.

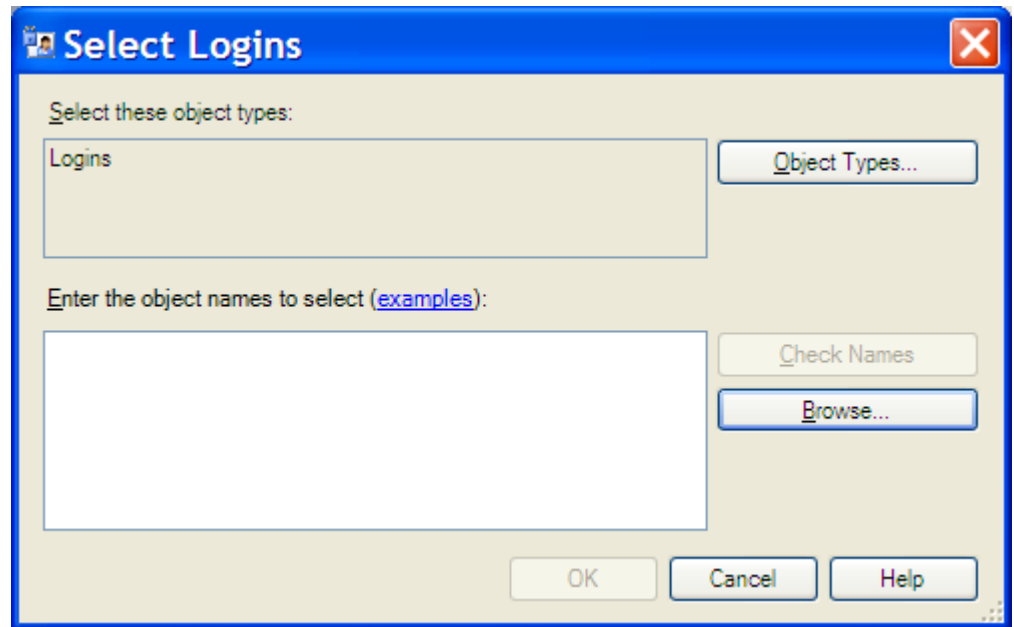
3/4 Dùng SQL Server Management Studio

- + Trong cửa sổ SQL Server Management Studio, mở rộng mục Security ở cấp Server. Sau đó chọn Server roles và right click lên nhóm quyền server muốn thêm người dùng, chẳng hạn chọn System Administrators xuất hiện cửa sổ hình 10

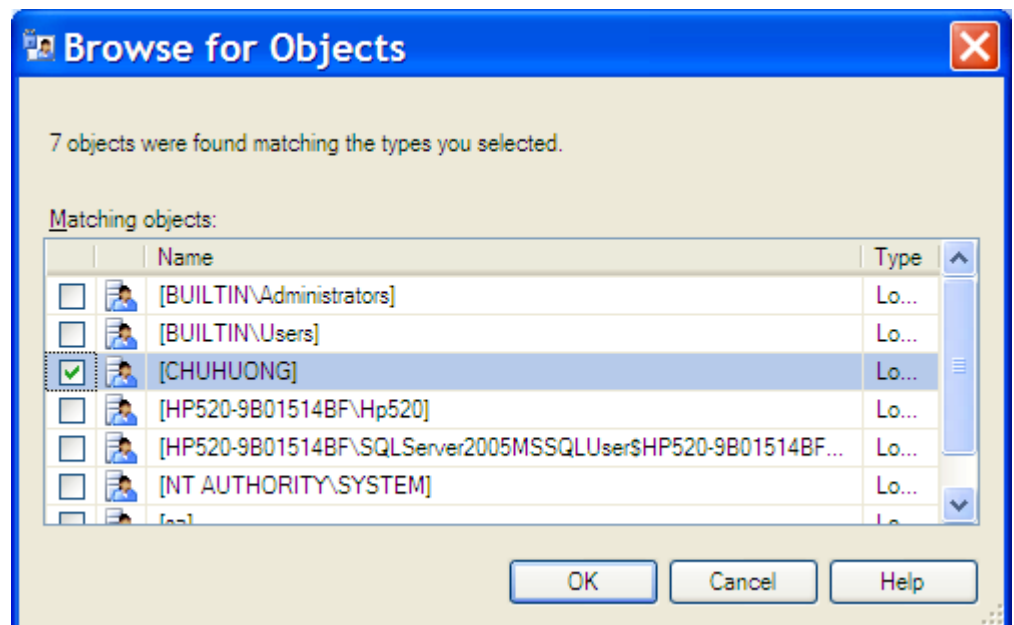


Hình 10. Cửa sổ Server Role Properties

- + Click vào nút Add để thêm người dùng vào nhóm. Hộp thoại Select Login xuất hiện (Hình 11).
- + Click vào nút Browse để chọn đăng nhập ta muốn thêm vào nhóm. Xuất hiện hộp thoại Browse for Objects (Hình 12)



Hình 11. Cửa sổ Select Login



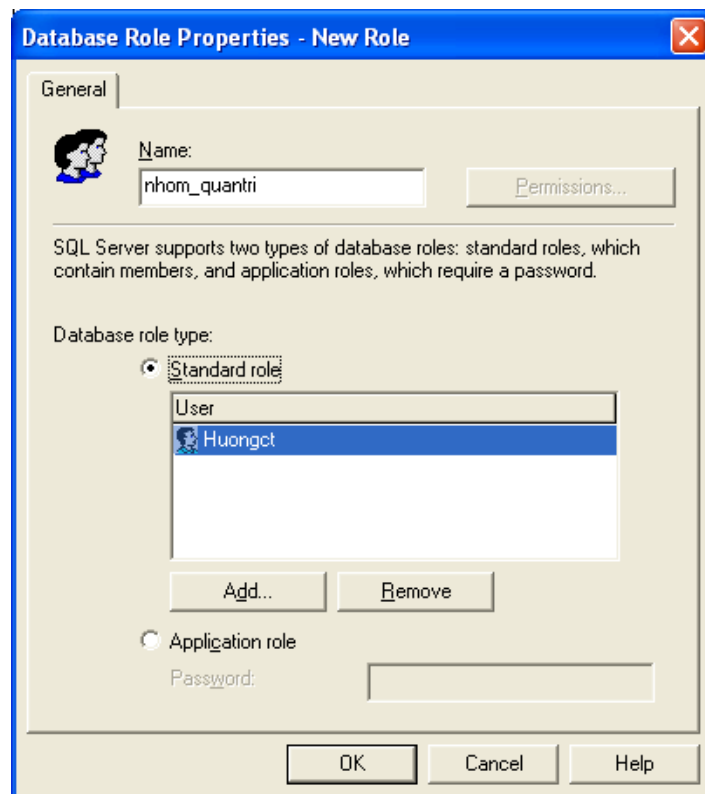
Hình 12. Cửa sổ Browse for Objects

- + Chọn các Login và click OK để đóng cửa sổ Browse for Objects.
- + Click OK để đóng cửa sổ Select Logins.
- + Click OK để đóng cửa sổ Server Role Properties để thêm người dùng đã chọn vào nhóm.

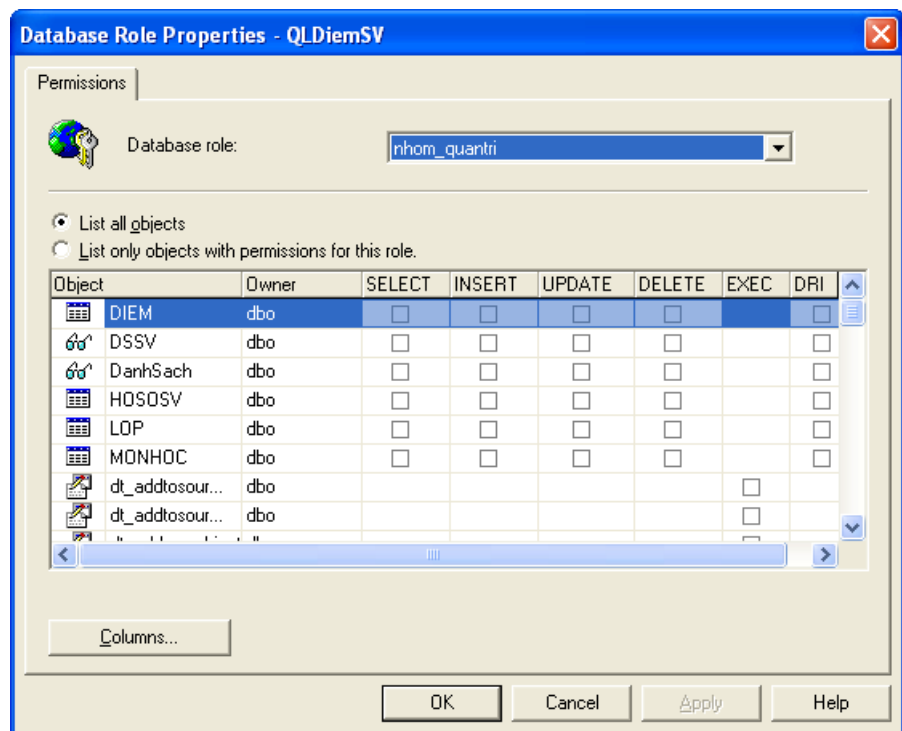
b) Tạo và sửa đổi nhóm quyền

³/₄ Dùng Enterprise manager:

- + Trong cửa sổ Enterprise Manager, mở rộng mục Database. Right click CSDL muốn tạo nhóm người dùng và chọn New\Database Role xuất hiện cửa sổ (hình 3.70).
- + Trong cửa sổ này ta nhập tên mô tả nhóm và Add các tài khoản người dùng thuộc nhóm bằng cách click vào nút Add và chọn các người dùng trong danh sách. Sau đó click nút OK để tạo nhóm.
- + Trở về Enterprise Manage, chọn mục Roles ta sẽ thấy nhóm quyền mới vừa tạo ở danh mục bên phải.
- + Ta gán quyền cho nhóm bằng cách right click lên nhóm quyền và chọn Properties. Xuất hiện cửa sổ Database Role Properties và chọn Permissions xuất hiện cửa sổ hình 3.71.



Hình 13. Cửa sổ New Role



Hình 14. Cửa sổ Database Role Properties

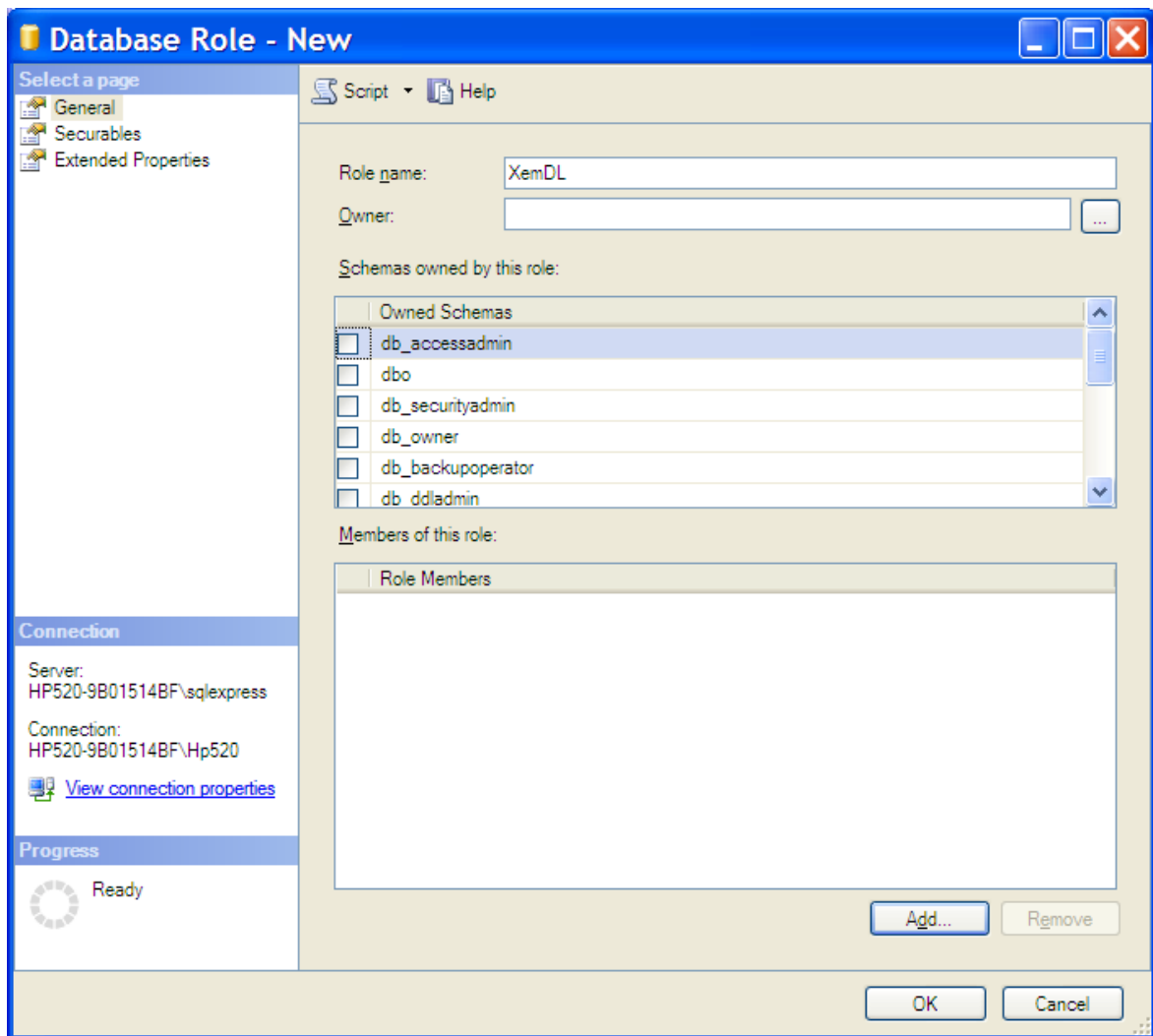
- + Ta thực hiện gán các quyền cho các nhóm quyền này trên các đối tượng của CSDL và click OK.

3/4 Dùng SQL Server Management Studio: SQL Server 2005 cung cấp hai loại nhóm quyền do người dùng định nghĩa

- + Database Roles: Đây là nhóm quyền chuẩn, dùng cho các tác vụ gán quyền tới cơ sở dữ liệu.
- + Application Roles: Dùng cho các quyền liên quan đến ứng dụng.

Xây dựng nhóm quyền Database Role ta tiến hành thực hiện theo các bước sau:

- + Trong SQL Server Management Studio, mở rộng mục Security cấp CSDL của CSDL ta muốn tạo nhóm quyền.
- + Mở rộng mục Roles, right click lên mục Database Roles và chọn New Database Role xuất hiện cửa sổ Database Role – New (Hình 15)



Hình 15. Cửa sổ Database Role - New

- Role name: Nhập tên nhóm
- Owner: Chọn danh sách các người dùng.
- Members of this role: Click vào nút Add để thêm các người dùng vào nhóm.

$\frac{3}{4}$ **Dùng T-SQL:**

+ Ta thực hiện thông qua 2 bước.

1. *Tạo nhóm quyền:* Ta có thể tạo nhóm quyền bằng thủ tục sp_addrole. Đối SQL Server 2005 ta có thể dùng cú pháp sau:

```
CREATE ROLE role_name [AUTHORIZATION owner_name ]
```

Trong đó:

- *role_name*: Là tên của nhóm sẽ được tạo.
- *AUTHORIZATION owner_name* : Là người dùng CSDL hoặc các nhóm mà sở hữu nhóm mới này. Nếu không có người dùng nào chỉ định thì nhóm sẽ được sở hữu bởi người dùng thực hiện câu lệnh CREATE ROLE này.

Ví dụ 3.21. Tạo nhóm quyền ‘xem_dl’ trên CSDL QLDiemSV.

```
Use QLDiemSV
Go
Sp_addrole 'xem_dl'
```

2. *Thêm quyền vào nhóm*: Ta có thể thêm quyền vào nhóm bằng việc sử dụng lệnh GRANT và thu hồi quyền của nhóm sử dụng lệnh REVOKE.

Ví dụ 3.22. Ta thêm quyền SELECT bảng HOSOSV vào nhóm ‘xem_dl’ trên CSDL QLDiemSV.

```
Use QLDiemSV
Go
GRANT SELECT
ON HOSOSV
TO xem_dl
```

3. *Thêm người dùng vào nhóm quyền*: Để thêm người dùng vào nhóm quyền ta sử dụng thủ tục sp_addrolemember

Ví dụ 3.23. Thêm người dùng Guest vào nhóm quyền ‘xem_dl’ trên CSDL QLDiemSV.

```
Use QLDiemSV
Go
Sp_addrolemember 'xem_dl', 'Guest'
Go
```

3. *Quản lý quyền CSDL*

Xác thực người dùng là quá trình đảm bảo chỉ có những người dùng hợp lệ mới được phép làm việc với cơ sở dữ liệu. Sau khi người dùng truy cập được vào CSDL thì họ có các quyền cụ thể với các đối tượng trong CSDL.

Các quyền trên các đối tượng là:

- + Đối tượng database: BACKUP DATABASE, BACKUP LOG, CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATERULE, CREATE TABLE, và CREATE VIEW.
- + Đối tượng scalar function: EXECUTE và REFERENCES.
- + Đối tượng table-valued function: DELETE, INSERT, REFERENCES, SELECT, và UPDATE.
- + Đối tượng stored procedure: DELETE, EXECUTE, INSERT, SELECT, và UPDATE.
- + Đối tượng table: DELETE, INSERT, REFERENCES, SELECT, và UPDATE.
- + Đối tượng view: DELETE, INSERT, REFERENCES, SELECT, and UPDATE.

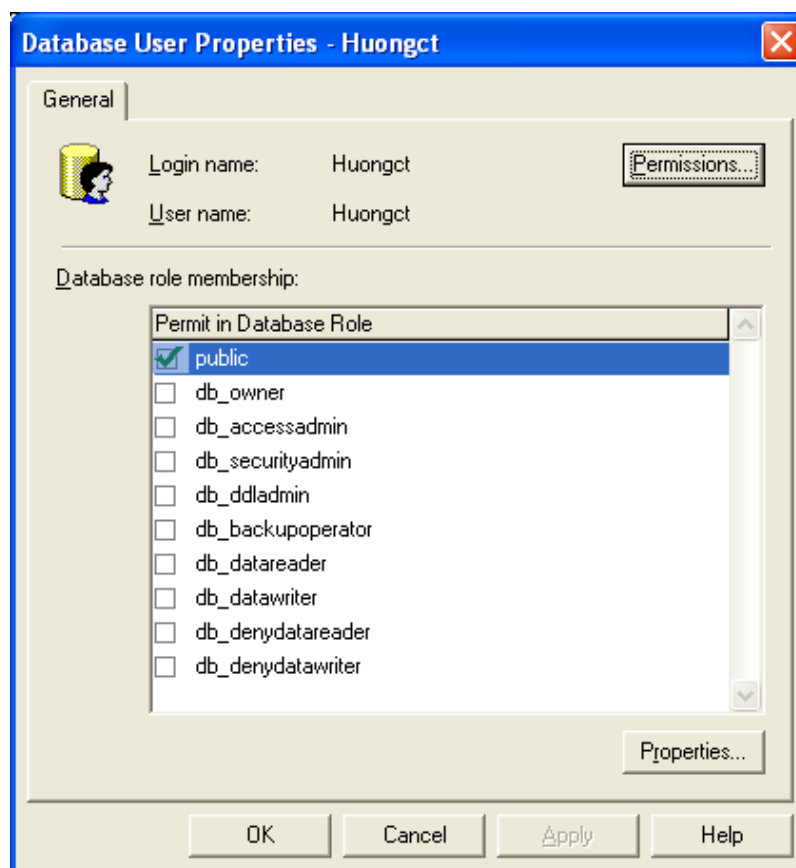
Cấp quyền trên các đối tượng CSDL ta tiến hành thực hiện như sau:

³/₄ Dùng Enterprise manager để cấp quyền trên các đối tượng:

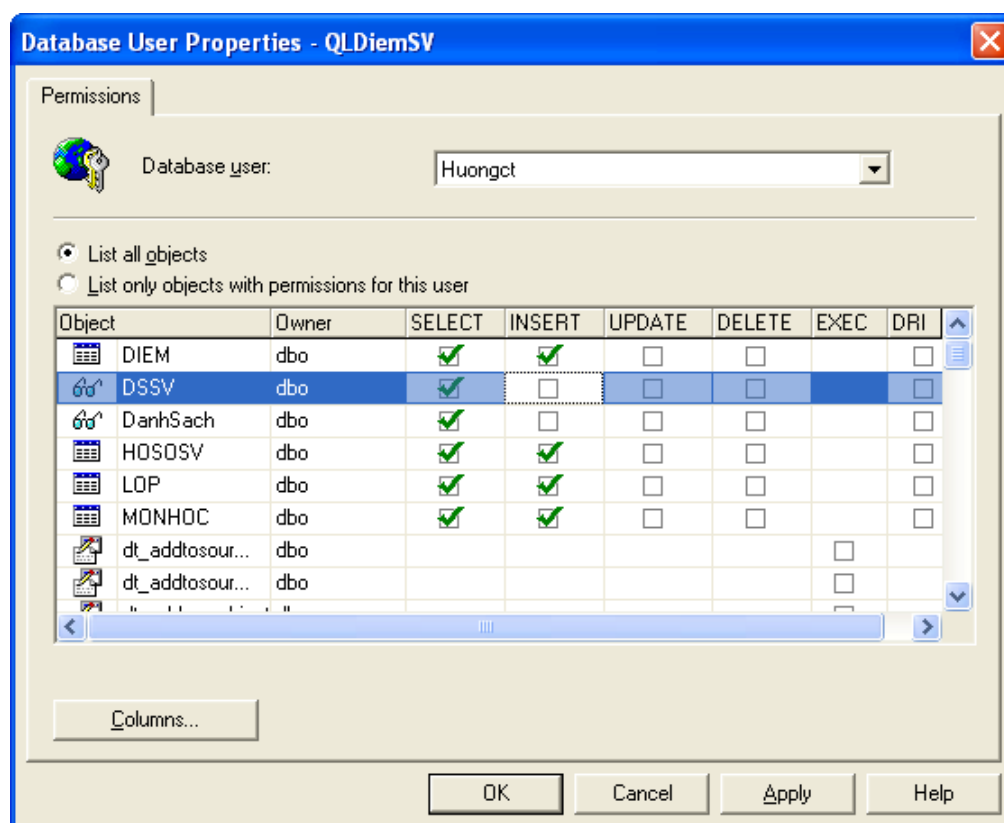
Có hai cách quản lý quyền trên các đối tượng.

Cách 1: Gán quyền cho tất cả các đối tượng cho một người dùng hoặc một nhóm người dùng.

- + Trong cửa sổ Enterprise Manager, mở rộng mục Database. Chọn CSDL muốn cấp quyền và mở rộng mục Users. Sau đó right click lên tên người dùng muốn cấp quyền và chọn Properties, xuất hiện cửa sổ như hình 16.
 - + Click vào nút Permissions để hiển thị cửa sổ Database Users Properties như hình 17. Ta gán các quyền cho người dùng này trên các đối tượng bằng cách chọn hộp kiểm tương ứng. Các tùy chọn *List all Objects* dùng để liệt kê tất cả các đối tượng còn chọn *List only objects with permissions for this user* thì chỉ liệt kê các đối tượng mà người dùng này có quyền truy cập.
-



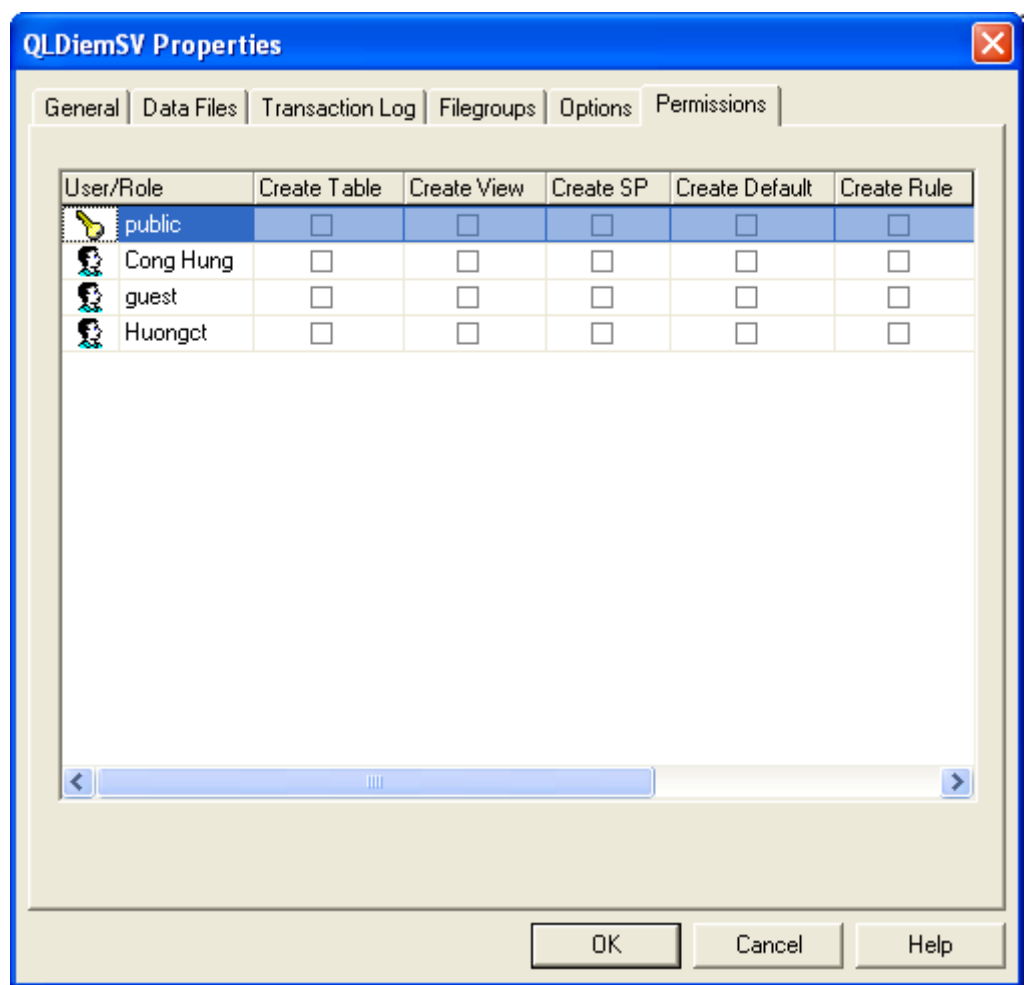
Hình 16. Cửa sổ Database Users Properties



Hình 17. Cửa sổ Database Users Properties

Cách 2: Gán các quyền trên một đối tượng cho tất cả các người dùng hoặc các nhóm người dùng.

- + Trong cửa sổ Enterprise Manager, mở rộng mục Database. Sau đó right click lên CSDL muốn cấp quyền, ví dụ QLDiemSV và chọn Properties, xuất hiện cửa sổ như hình 18. Chọn tab Permissions.
- + Thực hiện cấp quyền thực thi cho các người dùng bằng cách tích vào ô tương ứng với các quyền đó.

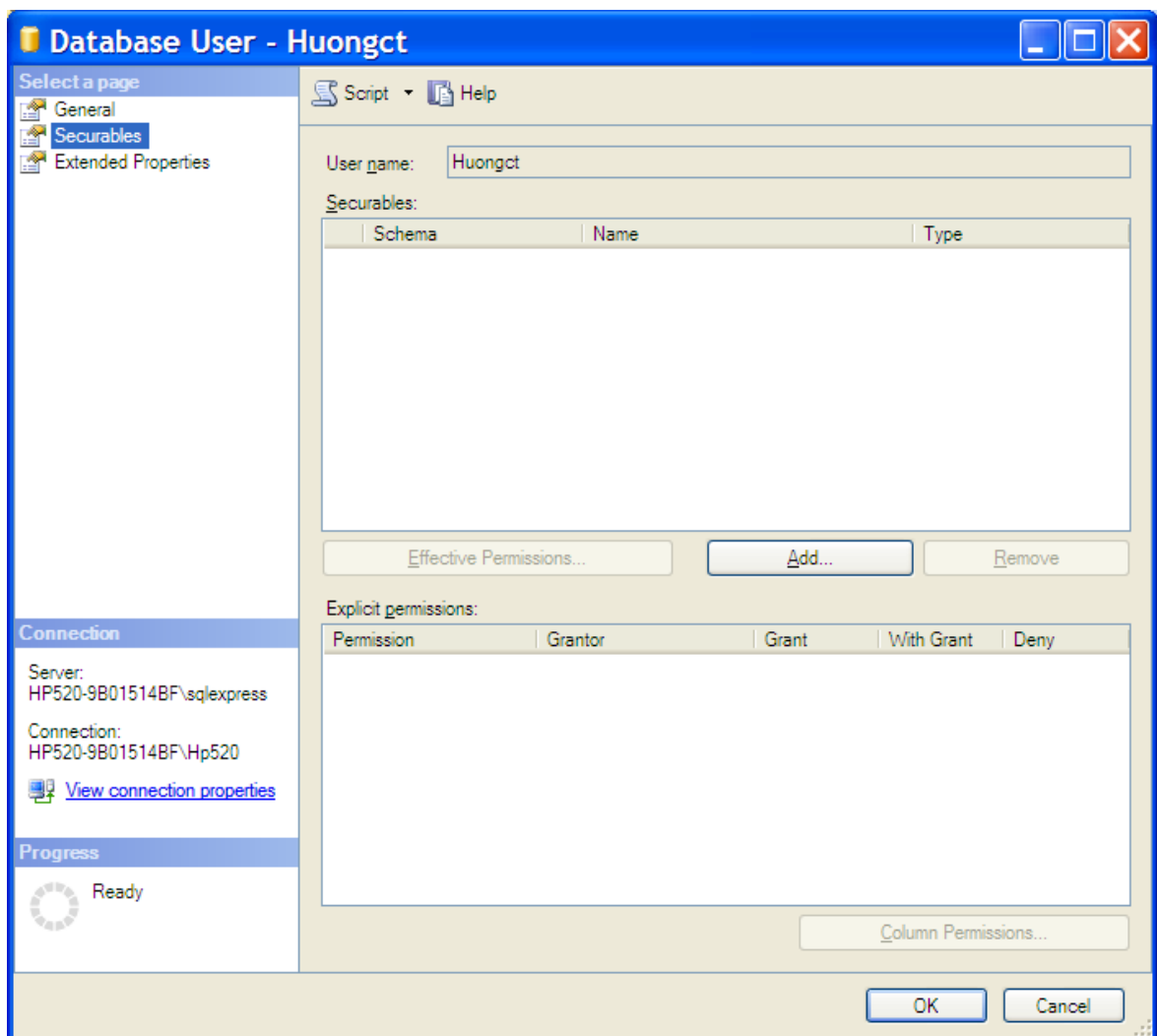


Hình 18. Cửa sổ QLDiemSV Properties

3/4 Dùng SQL Server Management Studio để cấp quyền trên các đối tượng: Có hai cách quản lý quyền trên các đối tượng.

Cách 1: Gán quyền cho tất cả các đối tượng cho một người dùng hoặc một nhóm người dùng.

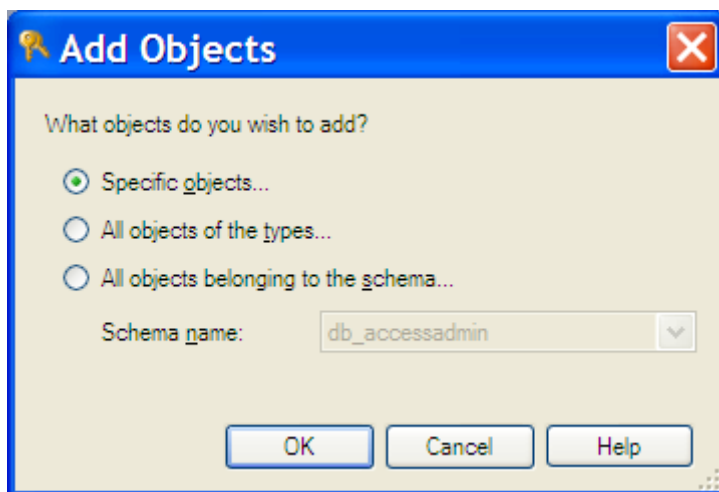
- + Trong cửa sổ Object Explorer của SQL Server Management Studio, mở rộng mục Database. Chọn CSDL muốn cấp quyền và mở rộng mục Users hoặc Roles\Database Roles.
- + Right click lên người dùng hoặc nhóm người dùng muốn và chọn Properties. Hộp thoại Properties xuất hiện chọn trang Securables (Hình 19)



Hình 19. Cửa sổ Database User

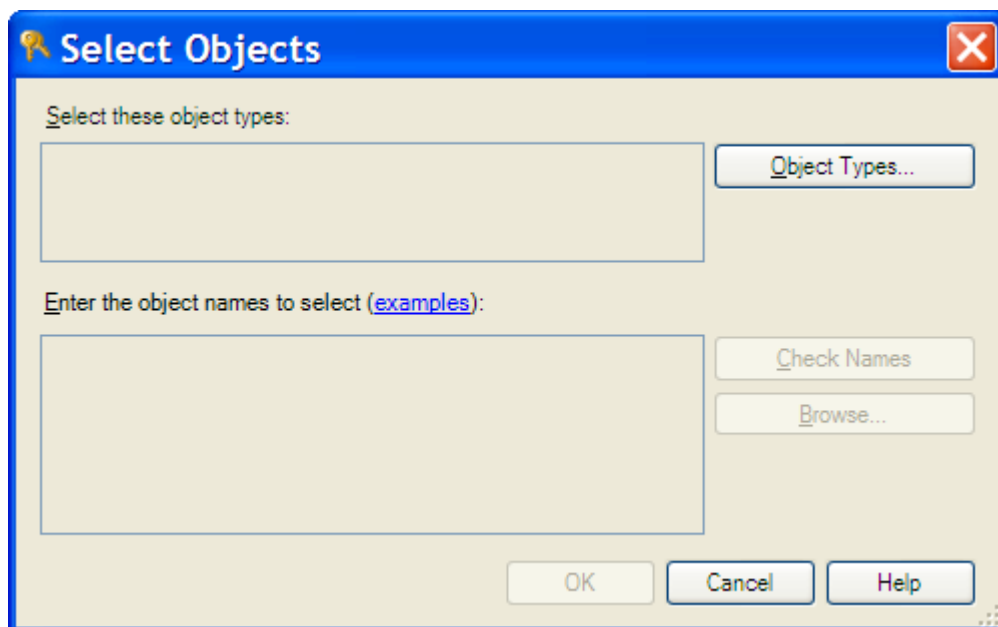
- + Click nút Add để thêm các đối tượng muốn bảo mật. Hộp thoại Add Objects xuất hiện (Hình 20), ta chỉ các đối tượng muốn bảo mật.
 - Specific objects: Chỉ định các đối tượng cụ thể.

- All objects of the types: Tất cả các đối tượng của các kiểu cụ thể.
- All objects belong to schema: Các đối tượng thuộc giản đồ.



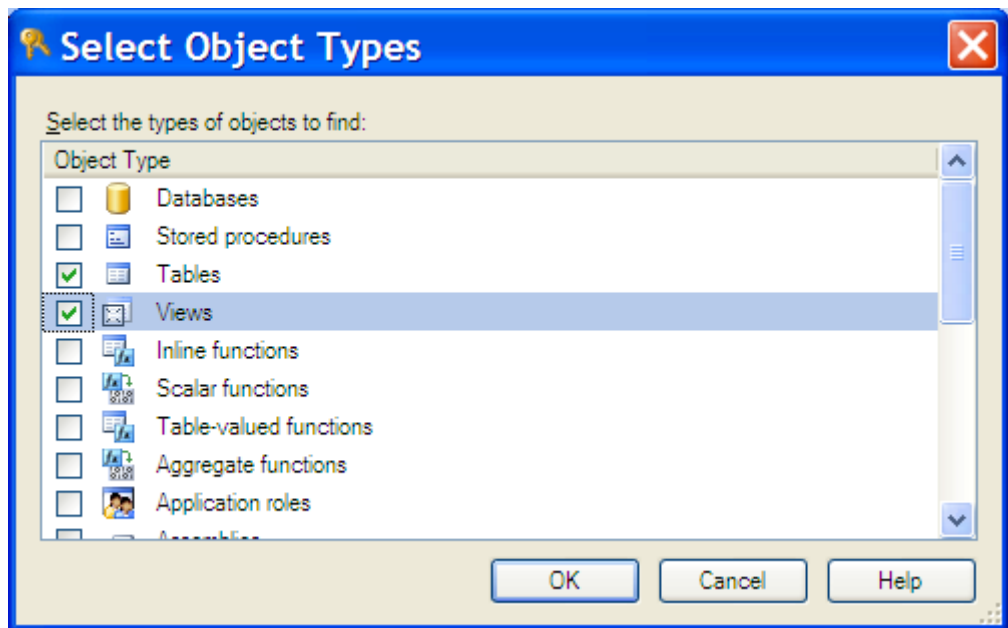
Hình 20. Cửa sổ Add Objects

- + Nếu chọn tùy chọn Specific objects, click OK hộp thoại Select Object xuất hiện (Hình 21).



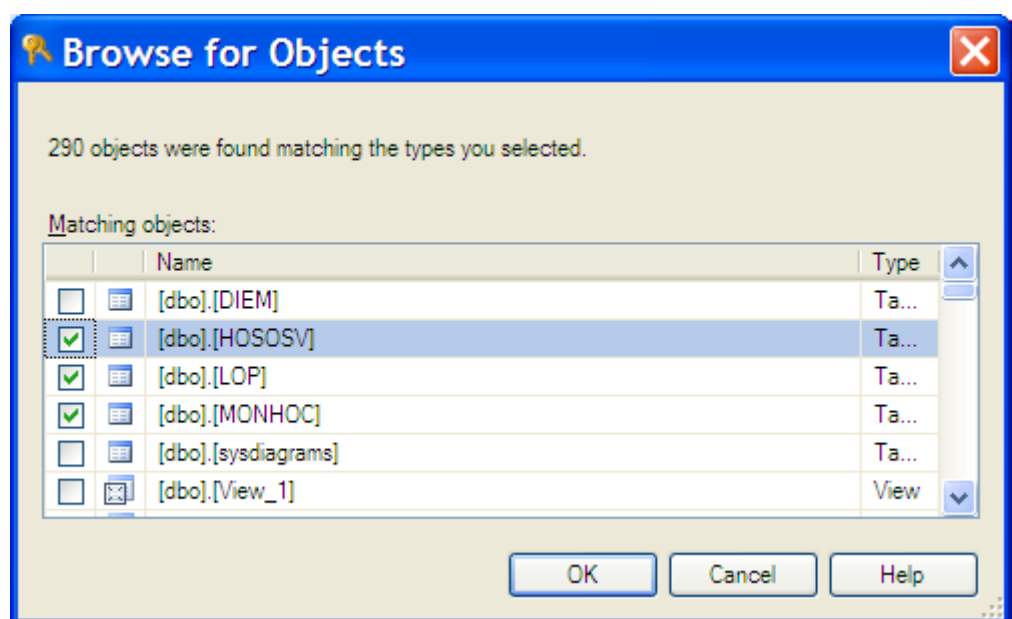
Hình 21. Cửa sổ Select Objects

- + Click vào nút Object Types, hộp thoại Select Object Types xuất hiện như hình 22. Ta chọn các kiểu đối tượng mà muốn bảo mật cho người dùng đó và click OK.

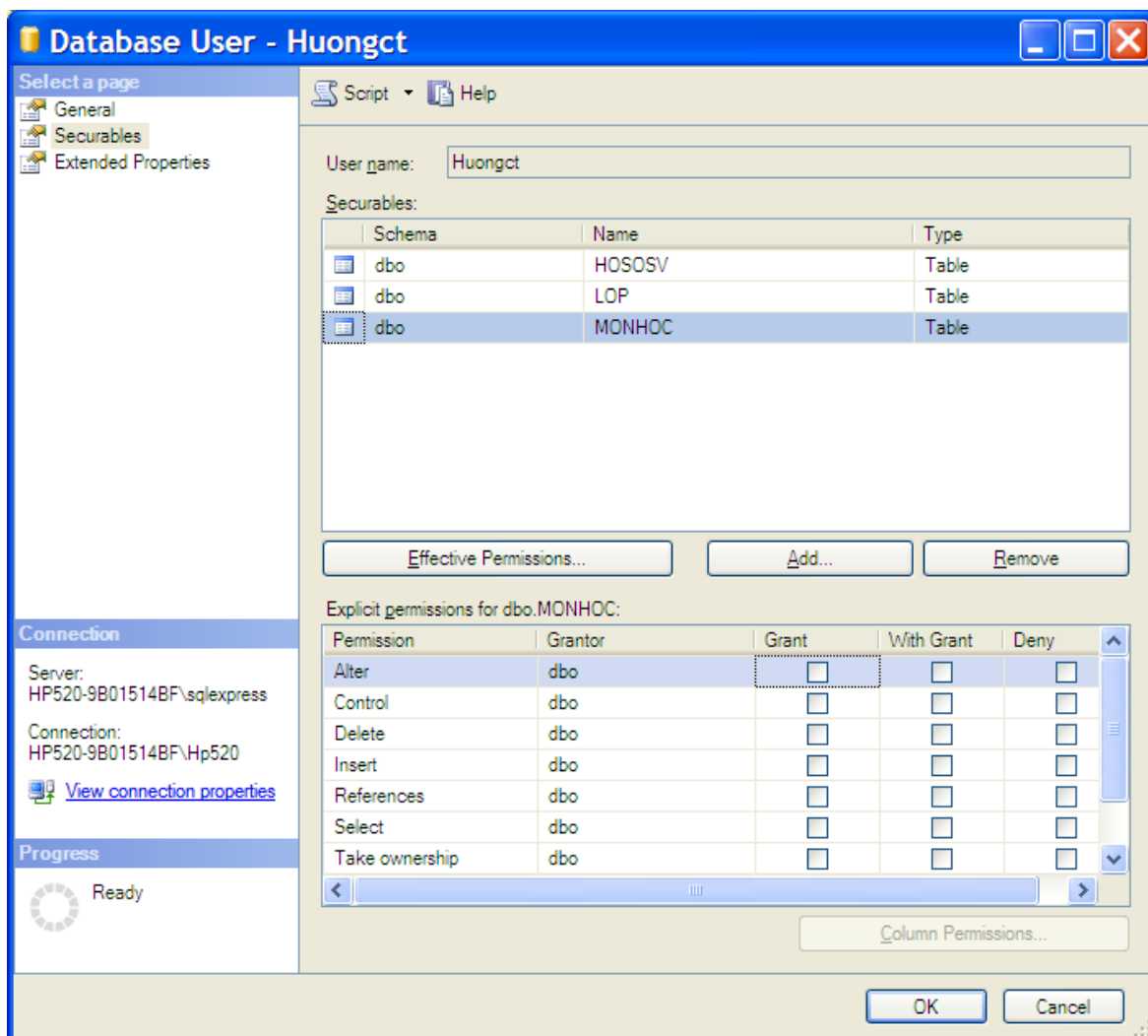


Hình 22. Cửa sổ Select Object Type

- + Click vào nút Browse trên hộp thoại Select Objects (Hình 22) xuất hiện cửa sổ Browse for Objects hình 23. Ta chọn các đối tượng mà muốn bảo mật cho người dùng đó và click OK.
- + Click OK trên cửa sổ Select Objects để quay trở lại trang Securable của hộp thoại Database User như hình 24. Ta chọn từng đối tượng và cấp quyền cho người dùng này.



Hình 23. Cửa sổ Browse for Objects



Hình 24. Cửa sổ Database User

¾ **Dùng T-SQL để cấp quyền:** Ta dùng lệnh các lệnh

- + **GRANT:** để cấp quyền cho người dùng;
- + **DENY:** dùng để ngăn cản quyền của người dùng nào đó. Ngăn cản các người dùng từ việc kế thừa các quyền trong nhóm.
- + **REVOKE:** để thu hồi lại quyền đã cấp.

Có cú pháp như sau:

```
GRANT { ALL }
| permission [( column [ ,...n ] ) ] [ ,...n ]
[ ON securable ] TO principal [ ,...n ]
[ WITH GRANT OPTION ]
```

```

DENY { ALL }
    | permission [( column [ ,...n ] ) ] [ ,...n ]
    [ ON securable ] TO principal [ ,...n ]
    [ CASCADE]

REVOKE [ GRANT OPTION FOR ]
    {
        [ ALL ]
        | permission[( column [ ,...n ] ) ] [ ,...n ]
    }
    [ ON securable ]
    { TO | FROM } principal [ ,...n ]
    [ CASCADE]

```

Trong đó:

- + ALL: Cấp tất cả các quyền ;
- + permission: Tên các quyền cụ thể được cấp;
- + column: Tên các cột của bảng mà các quyền đó được cấp;
- + securable: Chỉ định đối tượng đang cấp quyền trên đó.
- + Principal: Chỉ định người được cấp quyền.
- + WITH GRANT OPTION: Chỉ định người được cấp quyền có thể cấp quyền này cho người khác.
- + CASCADE: Chỉ định ngăn cản (đối với DENY) hoặc thu hồi (đối với REVOKE) theo dây truyền đối với các người dùng được cấp quyền với từ khóa WITH GRANT OPTION.

Ví dụ 3.15. Trao các quyền INSERT, SELECT, UPDATE cho *Huongct* trên CSDL QLDiemSV.

```

Use QLDiemSV
Go
GRANT INSERT, SELECT, UPDATE
ON HOSOSV
TO Huongct

```

Ví dụ 3.16. Trao tất cả các quyền cho *Huongct* trên CSDL QLDiemSV.

```

Use QLDiemSV
Go

```

```
GRANT ALL
ON LOP
TO Huongct
```

Ví dụ 3.17. Lấy các quyền INSERT, UPDATE của *Huongct* trên CSDL QLDiemSV.

```
Use QLDiemSV
Go
REVOKE INSERT, UPDATE
ON HOSOSV
TO Huongct
```

Ví dụ 3.18. Lấy tất cả các quyền của *Huongct* trên bảng LOP của CSDL QLDiemSV.

```
Use QLDiemSV
Go
REVOKE ALL
ON LOP
TO Huongct
```

Ví dụ 3.19. Cấp các quyền CREATE TABLE, CREATE VIEW cho *Huongct* trên CSDL QLDiemSV.

```
Use QLDiemSV
Go
GRANT CREATE TABLE, CREATE VIEW
TO Huongct
```

Ví dụ 3.20. Thu hồi tất cả các quyền của *Huongct* trên CSDL QLDiemSV.

```
Use QLDiemSV
Go
REVOKE ALL
TO Huongct
```

2. Sao lưu - phục hồi CSDL

1. Sao lưu CSDL

Sao lưu là hoạt động dữ liệu được sao chép từ CSDL và lưu ở một nơi khác. Có nhiều phương pháp sao lưu CSDL khác nhau, đó là:

- **Sao lưu đầy đủ (Full Database):** Là sao lưu toàn bộ CSDL, tất cả các nhóm tập tin và tập tin CSDL là một phần của CSDL đều
-

được sao lưu. Đây là kỹ thuật phổ biến dùng cho các CSDL có kích thước vừa và nhỏ.

- **Sao lưu những thay đổi (Differential Database):** Cho phép chỉ sao lưu những dữ liệu thay đổi kể từ lần sao lưu gần nhất. Kỹ thuật này nhanh hơn và ít tốn không gian lưu trữ hơn so với sao lưu đầy đủ. Nhưng dùng phương pháp này khó khăn hơn và tốn nhiều thời gian gian hơn để khôi phục dữ liệu.
- **Sao lưu tập tin log giao dịch (Transaction Log):** Cho phép sao lưu transaction log, sao lưu này rất quan trọng cho phục hồi CSDL.
- **Sao lưu nhóm tập tin (Full File Group):** bao gồm sao lưu tất cả các tập tin dữ liệu kết hợp với tập tin đơn trong CSDL. Dùng phương pháp này để sao lưu các nhóm tập tin riêng biệt tùy thuộc vào cách hệ thống được cấu hình
- **Sao lưu tập tin dữ liệu (Full File):** Cho phép sao lưu một tập tin đơn trong nhóm tập tin. Phương pháp này kết hợp với khả năng của SQL Server để khôi phục một tập tin dữ liệu đơn riêng biệt.

Thực hiện sao lưu dữ liệu: Ta có thể thực hiện bằng các phương pháp như dùng:

Đối với SQL Server 2000: Enterprise manager, T-SQL, Create Database Backup Wizard.

Đối với SQL Server 2005: Phương pháp sử dụng SQL Server Management Studio, T-SQL

Physical and Logical Devices

SQL Server Database Engine nhận dạng các thiết bị back up (backup devices) hoặc là tên thiết bị vật lý (physical device) hoặc tên logic (logical device) :

- Thiết bị sao lưu vật lý là tên được sử dụng bởi hệ điều hành cho việc nhận dạng thiết bị back up. Ví dụ: C:\Backups\Accounting\Full.bak.

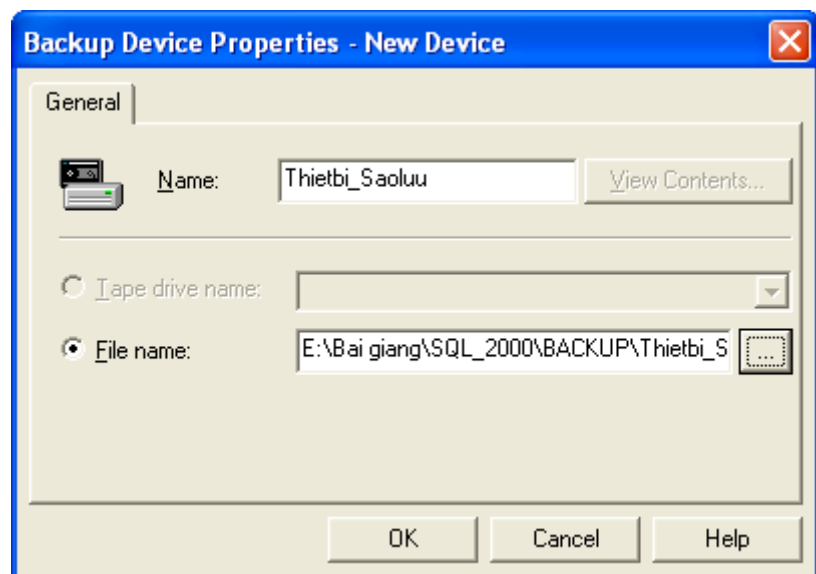
- Thiết bị sao lưu logic là bí danh do người dùng định nghĩa, được sử dụng để nhận dạng một thiết bị sao lưu vật lý. Tên thiết bị logic được lưu trữ thường trực trên các bảng hệ thống trong SQL Server. Tiện lợi của việc sử dụng thiết bị sao lưu logic là tên của nó đơn giản hơn so với tên thiết bị vật lý. Ví dụ, ta sử dụng tên logic là Accounting_Backup nhưng tên vật lý có thể là E:\Backups\Accounting\Full.bak.

Hoạt động sao lưu có thể hướng tới thiết bị vật lý hoặc thiết bị logic. Thiết bị vật lý là đĩa cứng, băng từ, v.v... còn thiết bị logic chỉ tồn tại trong SQL Server và chỉ được dùng cho SQL Server thực hiện sao lưu. Để sao lưu tới thiết bị logic, ta phải tạo thiết bị đó trước.

$\frac{3}{4}$ Dùng Enterprise manager:

- **Tạo thiết bị sao lưu logic:**

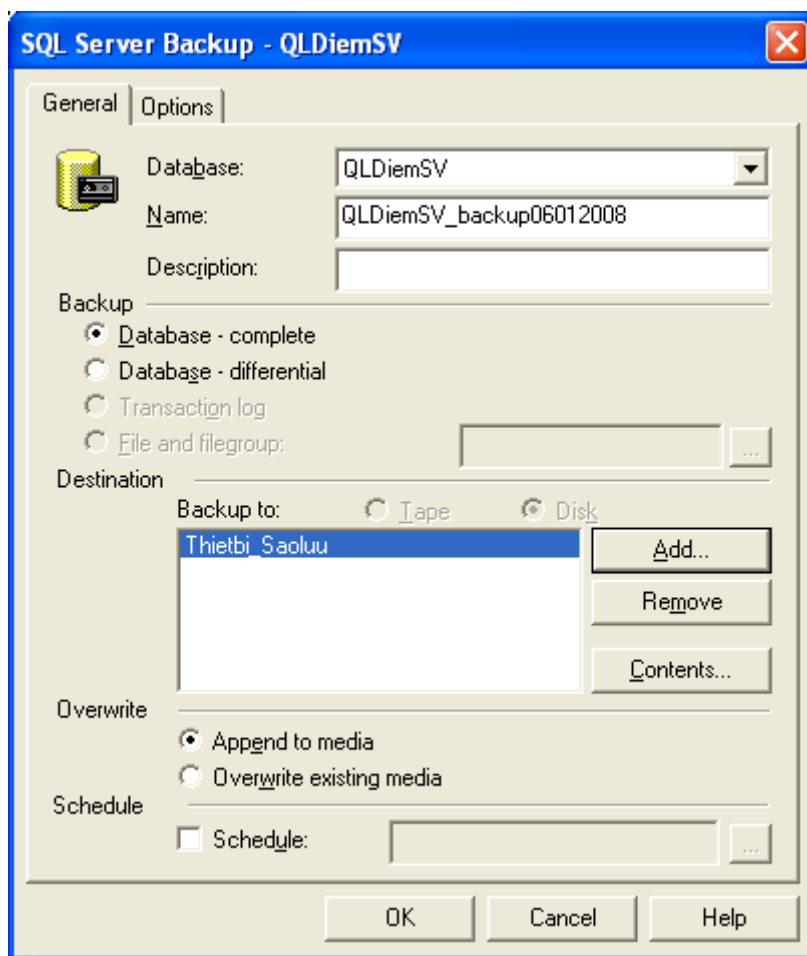
- + Trong cửa sổ Enterprise Manager, mở rộng server muốn thực hiện sao lưu và mở rộng mục Management.
- + Right click lên danh mục Backup và chọn New Backup Device xuất hiện cửa sổ *Backup Device Properties* (Hình 25). Ta nhập tên cho thiết bị sao lưu vào hộp Name và đường dẫn lưu file vào hộp thoại File Name. Sau đó click OK để lưu lại.



Hình 25. Cửa sổ *Backup Device Properties*

- **Thực hiện sao lưu:**

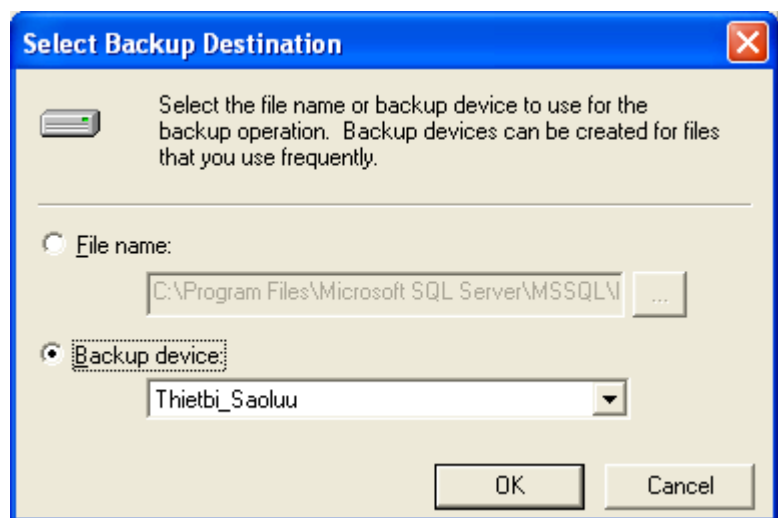
- + Trong cửa sổ Enterprise Manager, mở rộng server muốn thực hiện sao lưu và mở rộng mục Management.
- + Right click lên danh mục Backup và chọn New Backup a Database xuất hiện cửa sổ SQL Server Backup (Hình 26).



Hình 26. Cửa sổ SQL Server Backup

- + Trong danh sách Database chọn CSDL muốn thực hiện sao lưu, chẳng hạn chọn QLDiemSV. Tên sao lưu được điền tự động vào hộp Name, ta có thể thay đổi tên này. Nhập mô tả vào hộp Description.
 - + Trong vùng BACKUP chỉ ra kiểu sao lưu. Có các tùy chọn có sẵn như là:
-

- *Database Complete*: Thực hiện sao lưu đầy đủ CSDL.
 - *Database Differential*: Thực hiện sao lưu phần thay đổi.
 - *Transaction log*: Thực hiện sao lưu tập tin log giao dịch.
 - *File and filegroup*: Thực hiện sao lưu tập tin và nhóm tập tin.
- + Trong vùng Destination: Click vào nút Add xuất hiện cửa sổ *Select Backup Destination* hình 27.
- *File Name*: Chọn vào tùy chọn này để thực hiện sao lưu thành một tập tin lưu trực tiếp xuống hệ điều hành (dùng thiết bị vật lý)
 - *Backup device*: Chọn thiết bị sao lưu logic. Chọn Thietbi_Saoluu vừa tạo ở mục trên và chọn OK.



Hình 27. Cửa sổ *Select Backup Destination*

- + Trong vùng Overwrite: Có 2 tùy chọn
- *Append to media*: Ghi nối tiếp vào thiết bị
 - *Overwrite existing media*: để ghi đè lên thiết bị đang tồn tại.
- + Trong vùng Shedule: Dùng khi muốn thiết lập biểu sao lưu tự động.
-

+ Click OK để thực hiện sao lưu.

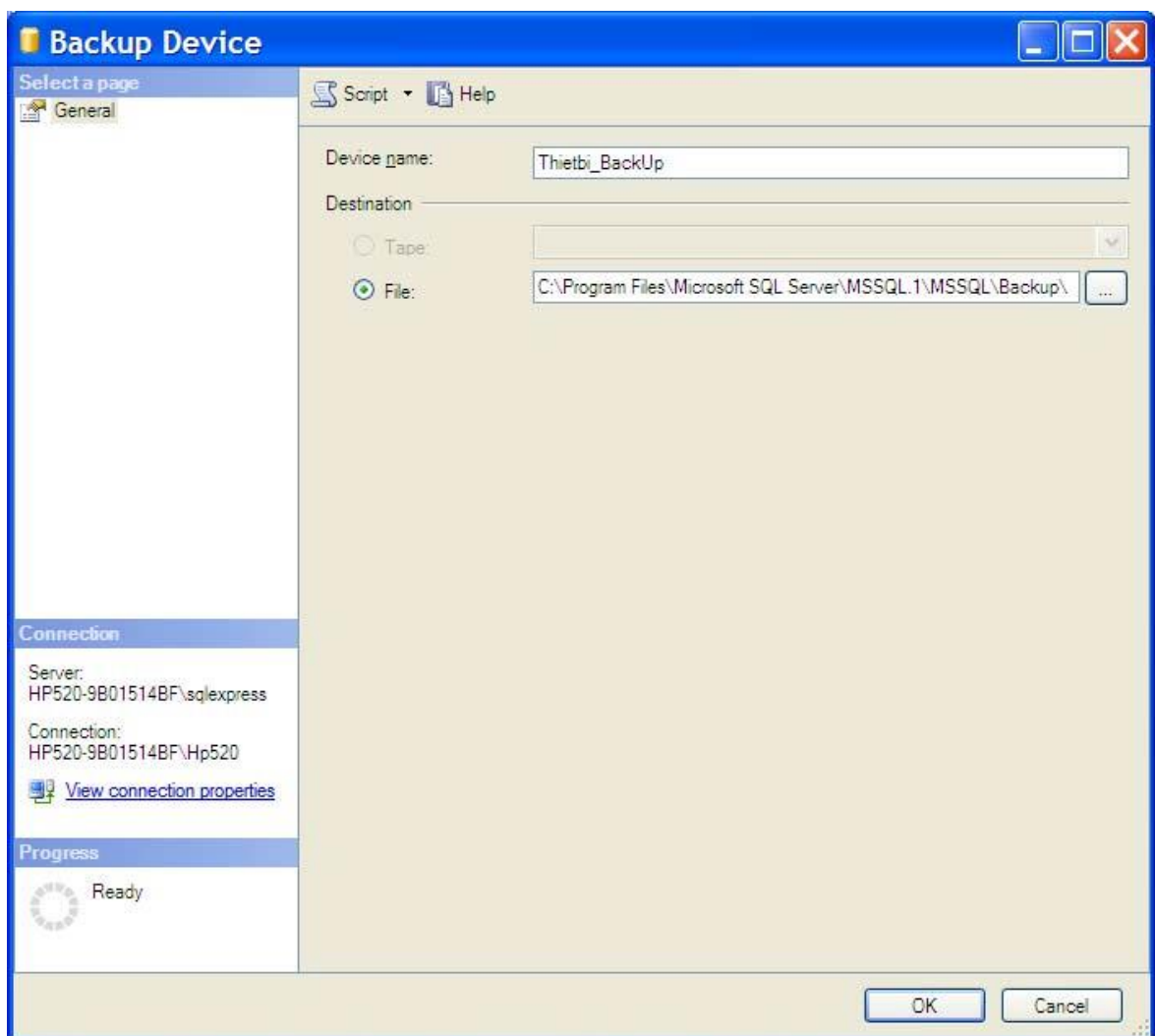
¾ Dùng SQL Server Management Studio:

- **Tạo thiết bị sao lưu logic:**

- + Trong cửa sổ Object Explorer, click vào tên server để mở rộng cây server.
- + Mở rộng mục Server Objects, và right-click Backup Devices và chọn New Backup Device. Xuất hiện hộp thoại Backup Device (Hình 28). Trong hộp thoại mục:

- f Device name: Nhập tên thiết bị logic.

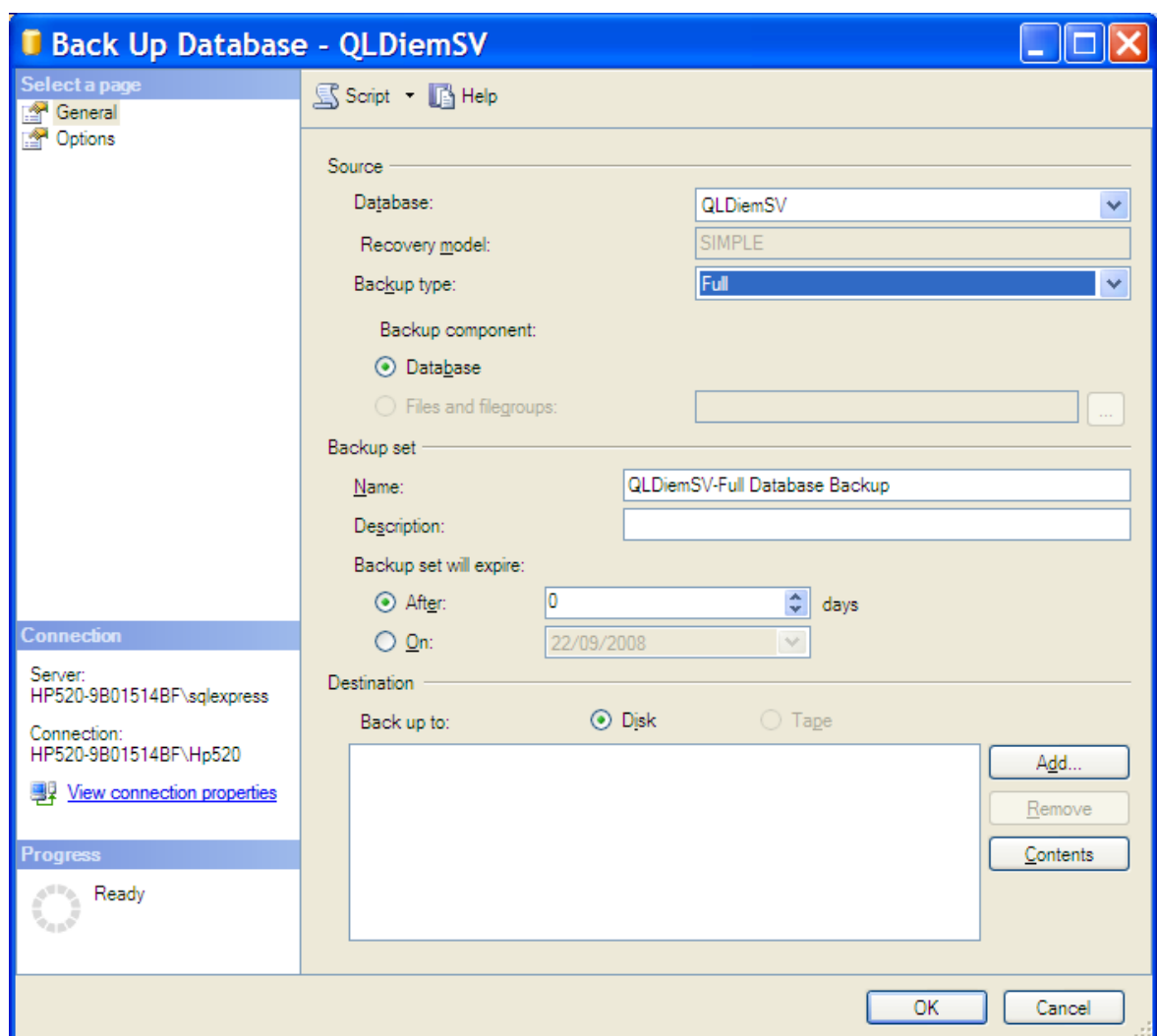
- f Destination, click File và chỉ định đường dẫn đầy đủ của file.



Hình 28. Cửa sổ Backup Device

- **Thực hiện sao lưu:**

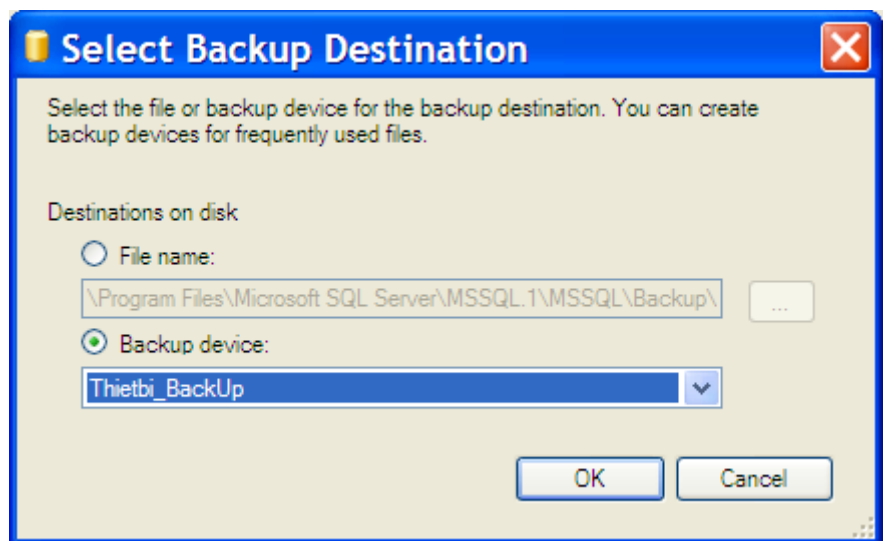
- + Trong cửa sổ Object Explorer, click vào tên server để mở rộng cây server.
- + Mở rộng mục Databases, và right-click lên cơ sở dữ liệu muốn tạo file Backup và chọn Tasks\Back Up. Xuất hiện hộp thoại Back Up Database (Hình 29).



Hình 29. Cửa sổ Back Up Database

- + Trong hộp thoại ta thực hiện các lựa chọn:
 - f Vùng Source: Database: Chọn Database muốn tạo file Back Up; Backup type: Chọn kiểu Back Up.

- f Vùng Backup set: Thiết lập tên, mô tả,... file BackUp.
- f Vùng Destination: Mục Backup to chọn Disk và click vào nút Add để chọn thiết bị sao lưu. Xuất hiện cửa sổ Select Backup Destination (Hình 30) ta sẽ chọn kiểu thiết bị sao lưu vật lý (chọn File name) hoặc logic (Backup device) và click OK.



Hình 30. Cửa sổ Select Backup Destination

- + Ta click vào nút OK trên cửa sổ Back Up Database để thực hiện quá trình sao lưu.

2. Phục hồi dữ liệu

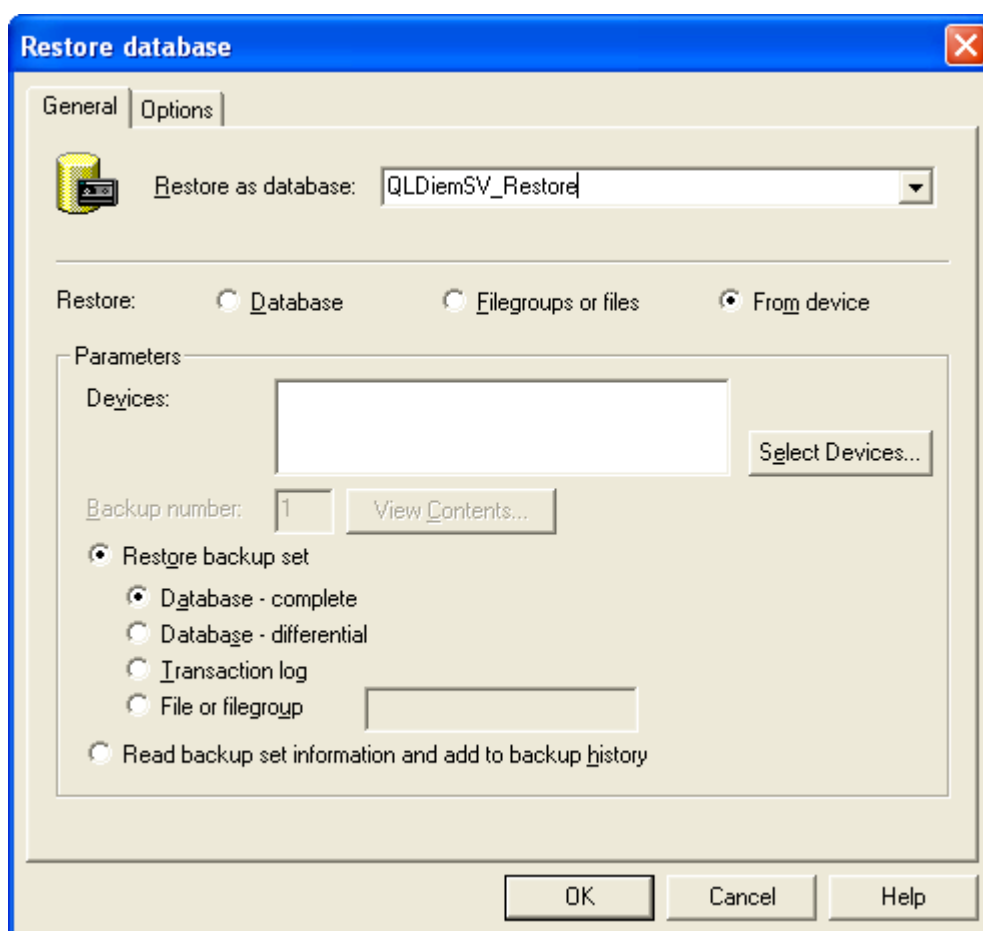
Phục hồi dữ liệu có thể coi là một quá trình ngược với quá trình sao lưu, dữ liệu sao chép được sao chép trở lại CSDL. Loại sao lưu dữ liệu sẽ ảnh hưởng đến cách khôi phục dữ liệu. Ta thực hiện các bước sau để khôi phục dữ liệu.

$\frac{3}{4}$ Dùng Enterprise manager:

- Trong cửa sổ Enterprise Manager, right click lên mục Database. Chọn *All Task/Restore Database*. Khi đó xuất hiện hộp thoại Restore Database hình 31.

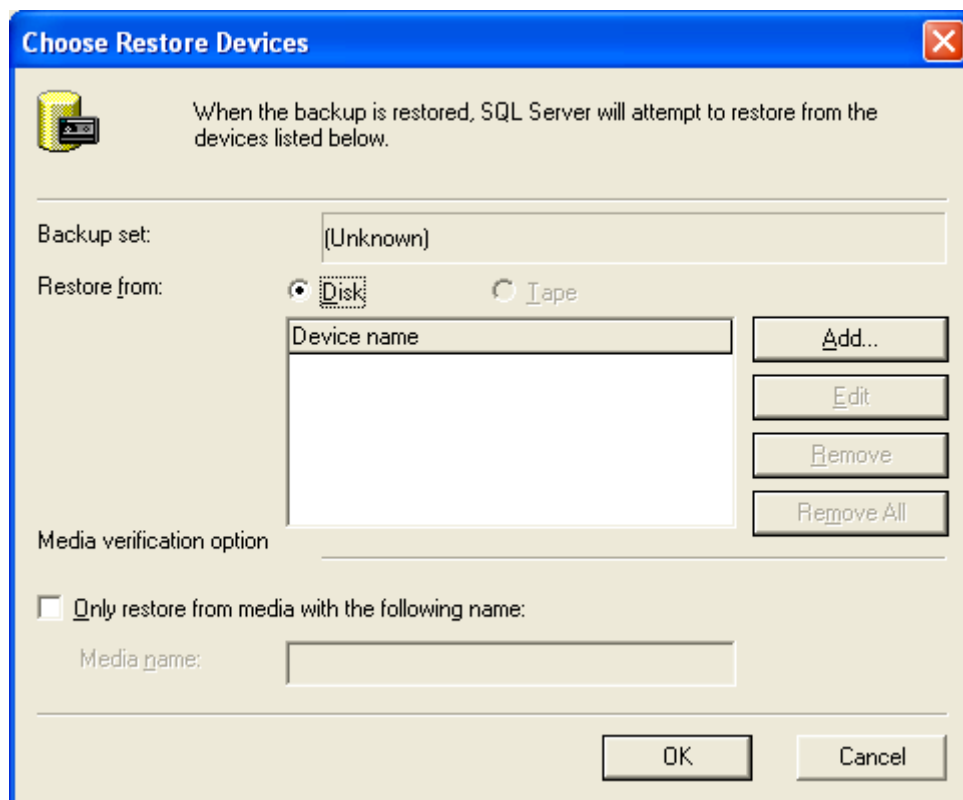
- Chọn tab General, mục Restore As Database cho phép chỉ ra CSDL sẽ được phục hồi từ dữ liệu sao lưu. Ví dụ ta chọn CSDL QLDiemSV thì việc khôi phục dữ liệu sao lưu sẽ thay thế toàn bộ dữ liệu hiện thời trong QLDiemSV. Khi đó ta phải chọn hộp check box Force Restore Over Existing Database trong tab Options.

SQL Server không đòi hỏi phải khôi phục CSDL trực tiếp mà cho phép ta khôi phục dữ liệu với một cái tên khác. Ví dụ, người dùng xóa nhầm bảng dữ liệu. Như vậy, nếu ta khôi phục toàn bộ dữ liệu thì dữ liệu cũ sẽ thay thế toàn bộ dữ liệu đang có trên các bảng khác. Thay vào đó ta khôi phục với một cái tên khác sau đó trích bảng đã bị xóa và thêm vào CSDL đã bị mất. Ví dụ ta thay với tên QLDiemSV_Restore.



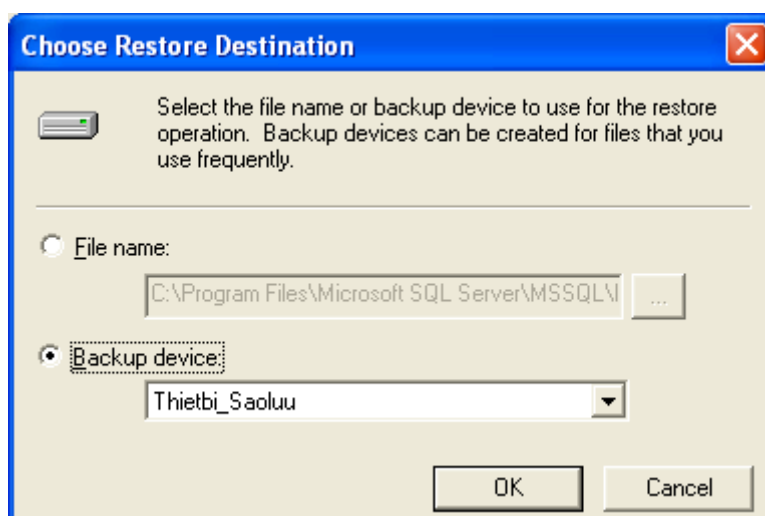
Hình 31. Cửa sổ Restore Database.

- Trong vùng Restore chọn From Device. Trong vùng Parameters chọn Restore backup set và chọn Database complete.
- Click vào nút Select Device xuất hiện hộp thoại Choose Restore Device như hình 32.



Hình 32. Cửa sổ Choose Restore Device.

- Và chọn nút Add xuất hiện hộp thoại Choose Restore Destination (Hình 33).



Hình 33. Cửa sổ Choose Restore Destination.

- Trong đó có hai lựa chọn:
 - + File name: Chọn tập tin sao lưu trên thiết bị vật lý.
 - + Backup Device: Chọn tên thiết bị logic.
- Sau đó chọn OK để trở về cửa sổ hình 32. Trong cửa sổ 32 click OK để trở về cửa sổ 31.
- Chọn tab Options:
 - + Force Restore Over Existing Database: Chọn nếu ta thực hiện khôi phục trực tiếp CSDL với dữ liệu cũ sẽ đè lên dữ liệu mới.
 - + Move to physical file name: Ta có thể sửa đổi lại thành tên khác với tên tập tin ban đầu. Ví dụ tập tin QLDiemSV_Restore.mdf chuyển thành QLDiemSV_Restore_Data.mdf
 - Click OK để bắt đầu thực hiện phục hồi dữ liệu.

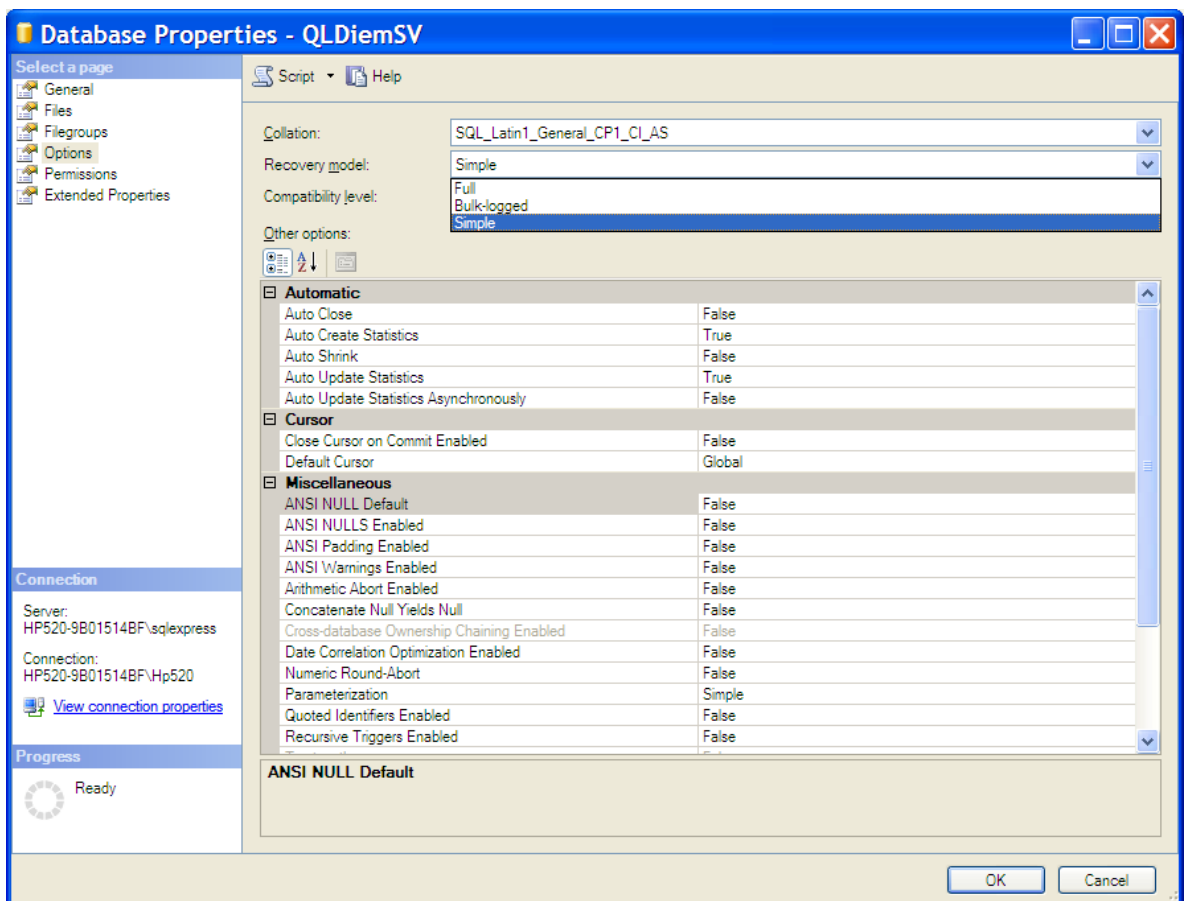
$\frac{3}{4}$ **Dùng SQL Server Management Studio:**

- ***Các mô hình khôi phục dữ liệu:***
 - + Full Recovery Model: Đây là mô hình cho phép phục hồi dữ liệu với ít rủi ro nhất. Nếu một database ở trong mô hình này thì tất cả các hoạt động không chỉ insert, update, delete mà kể cả insert bằng Bulk Insert, hay bcp đều được log vào transaction log file. Khi có sự cố thì ta có thể phục hồi lại dữ liệu ngược trở lại tới một thời điểm trong quá khứ. Khi data file bị hư nếu ta có thể backup được transaction log file thì ta có thể phục hồi database đến thời điểm transaction gần nhất được committed.
 - + Bulk-Logged Recovery Model: Ở mô hình này các hoạt động mang tính hàng loạt như Bulk Insert, bcp, Create Index, WriteText, UpdateText chỉ được log minimum vào transaction log file đủ để cho biết là các hoạt động này có diễn ra mà không log toàn bộ chi tiết như trong Full Recovery Mode. Các hoạt động khác như Insert, Update, Delete vẫn được log đầy đủ để dùng cho việc phục hồi sau này.
-

- + Simple Recovery Model: Ở mô hình này thì Transaction Log File được truncate thường xuyên. Với mô hình này bạn chỉ có thể phục hồi tới thời điểm backup gần nhất mà không thể phục hồi tới một thời điểm trong quá khứ.

Để thay đổi mô hình Recovery, ta tiến hành thực hiện như sau:

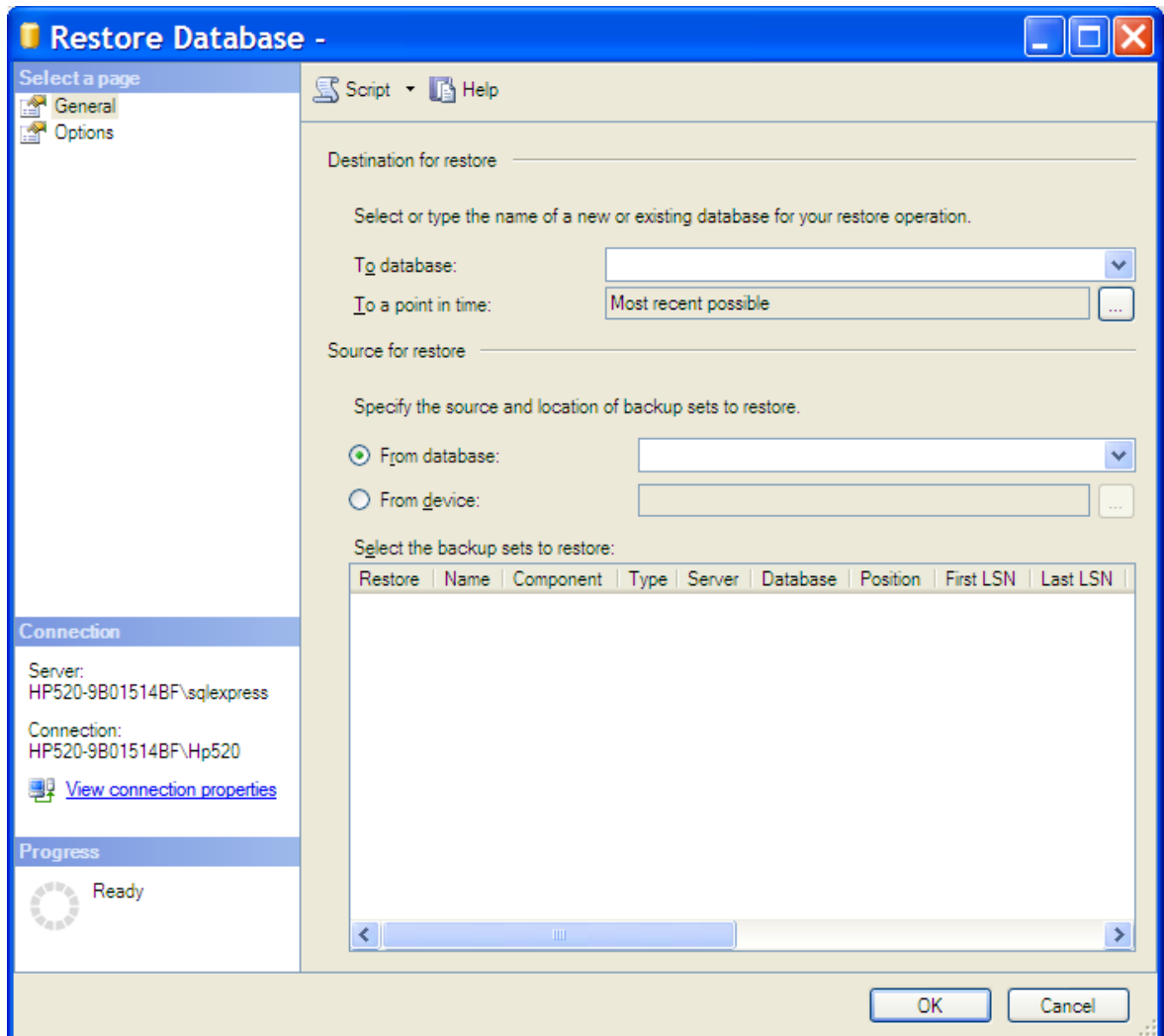
- + Trong cửa sổ Object Explorer, click vào tên server để mở rộng cây server.
- + Mở rộng mục Databases, và right-click lên cơ sở dữ liệu muốn thay đổi mô hình Recovery và chọn Properties. Xuất hiện hộp thoại Database Properties, chọn trang Options (Hình 34).
- + Mục Recovery model: Ta chọn mô hình khôi phục dữ liệu.



Hình 34. Cửa sổ Database Properties

- **Phục hồi dữ liệu:**

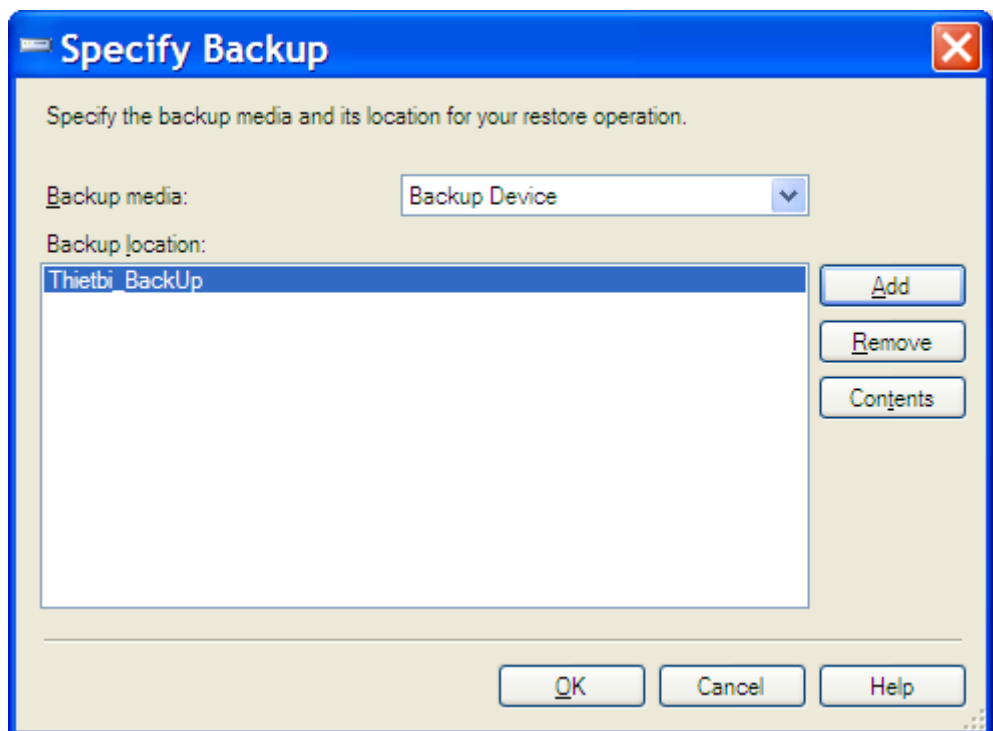
- Trong cửa sổ Object Explorer, click vào tên server để mở rộng cây server.
- Right click lên mục Databases, và chọn Restore Database xuất hiện cửa sổ Restore Database (Hình 35). Có các lựa chọn.



Hình 35. Cửa sổ Restore Database

- + *To database:* Điền tên Database sẽ được phục hồi. Tên này có thể là một tên Database mới hoặc chọn trong danh sách các Database có trong Server.

- + *To a point in time*: Restore database đến thời điểm sẵn có backup gần đây nhất hoặc đến một thời điểm được chỉ định.
- + *From database*: Chọn database để restore từ danh sách. Danh sách này chỉ chứa các database đã được backed up theo nhật ký của msdb backup.
- + *From device*: Chọn nguồn từ tập các file backup. Click vào nút browse để xuất hiện cửa sổ Specify Backup (Hình 36). Trong hộp thoại này ta chọn kiểu thiết bị (Backup media) là thiết bị vật lý hay thiết bị logic. Click nút Add để lấy các file Backup dùng để phục hồi dữ liệu.
- Trong cửa sổ Restore Database, sau khi thiết lập các tham số click OK để thực hiện quá trình phục hồi dữ liệu.



Hình 36. Cửa sổ Restore Database

