BẢO MẬT TRONG SQL

Tài liệu: Trang 102-108

Nội dung

- Các khái niệm
- Tạo người dùng / CREATE
- Cập nhật thông tin người dùng / ALTER
- Xóa người dùng / DROP
- Cấp quyền / GRANT
- Thu hồi quyền / REVOKE

Người dùng cơ sở dữ liệu

Database user

- Là đối tượng sử dụng cơ sở dữ liệu, thực thi các thao tác trên cơ sở dữ liệu như tạo bảng, truy xuất dữ liệu,...
- Xác định thông qua tên người dùng (User ID).
- Nhóm người dùng (User Group): nhiều người dùng có quyền trên hệ thống giống nhau có thể được tổ chức trong một nhóm và được gọi là nhóm người dùng.

Các đối tượng cơ sở dữ liệu

Database objects

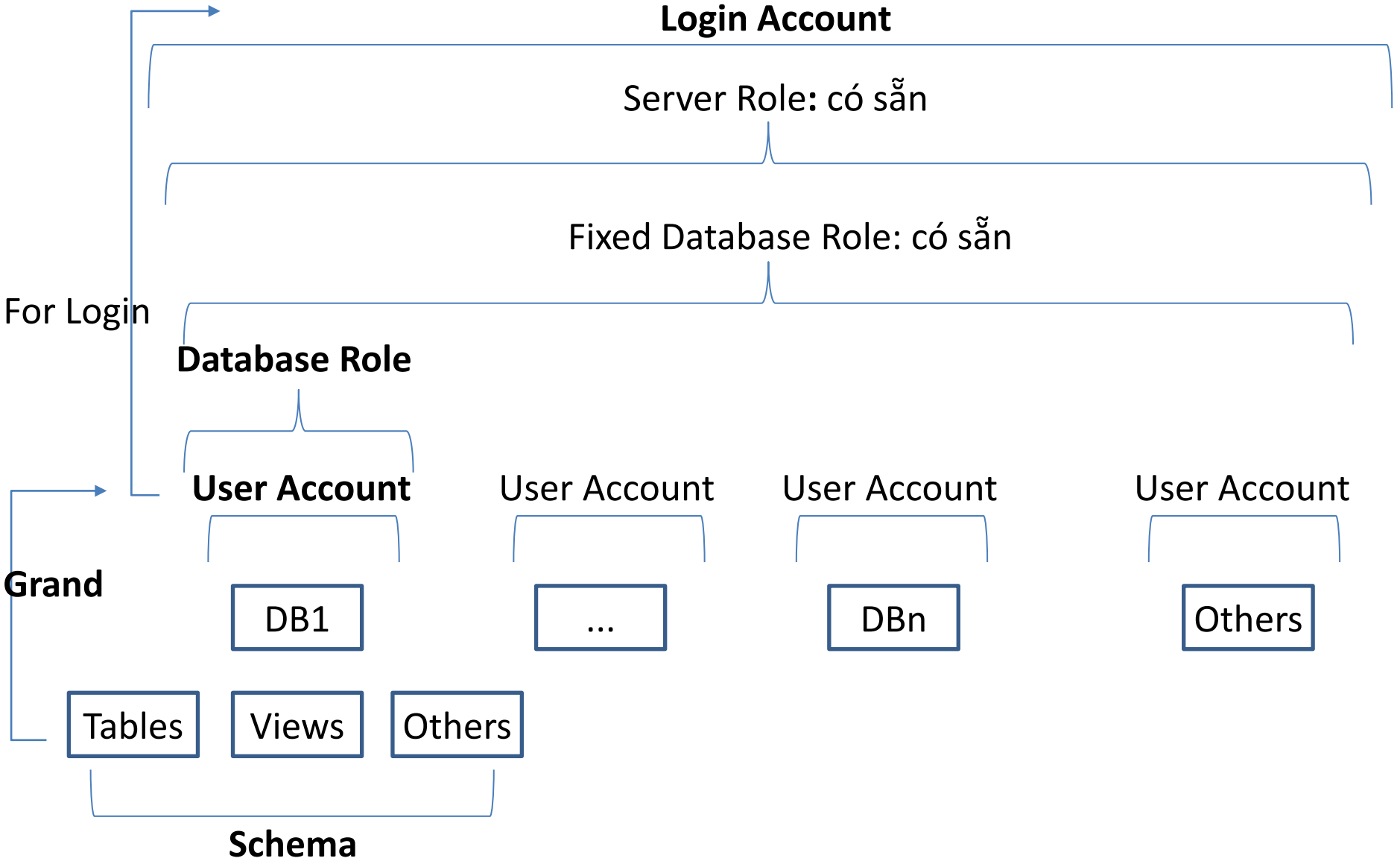
- Tập hợp các đối tượng, các cấu trúc lưu trữ được sử dụng trong cơ sở dữ liệu như bảng, khung nhìn, thủ tục, hàm được gọi là các đối tượng cơ sở dữ liệu.
- Đây là những đối tượng cần được bảo vệ trong chính sách bảo mật của cơ sở dữ liệu.

Đặc quyền (Privileges)

- Là tập những thao tác được cấp phát cho người dùng trên các đối tượng cơ sở dữ liệu.

Ví dụ: Một người dùng có thểtruy xuất dữ liệu trên một bảng bằng câu lệnh SELECT nhưng có thể không thể thực hiện các câu lệnh INSERT, UPDATE hay DELETE trên bảng đó.

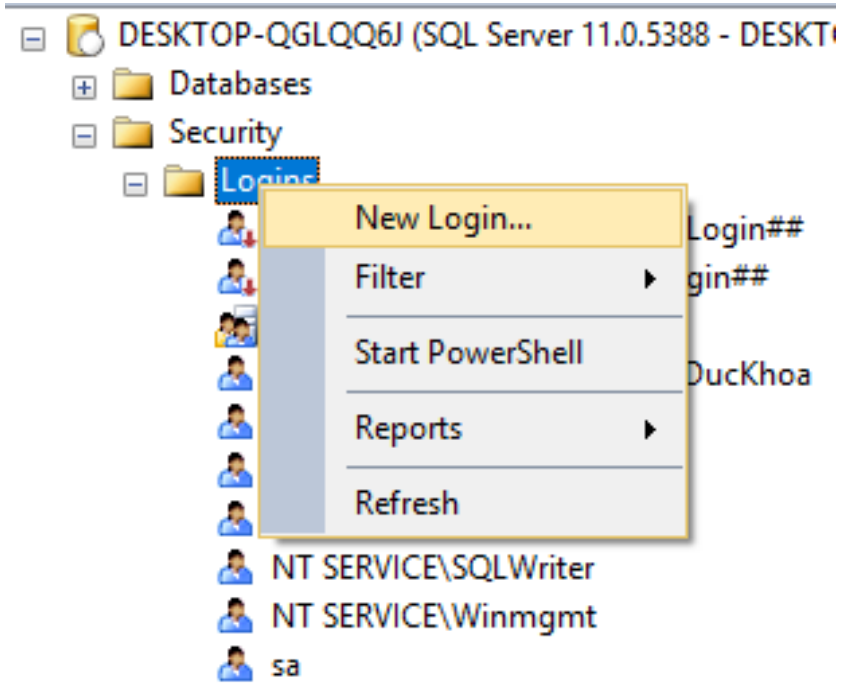
Sơ đồ Phân quyền trong SQL Server

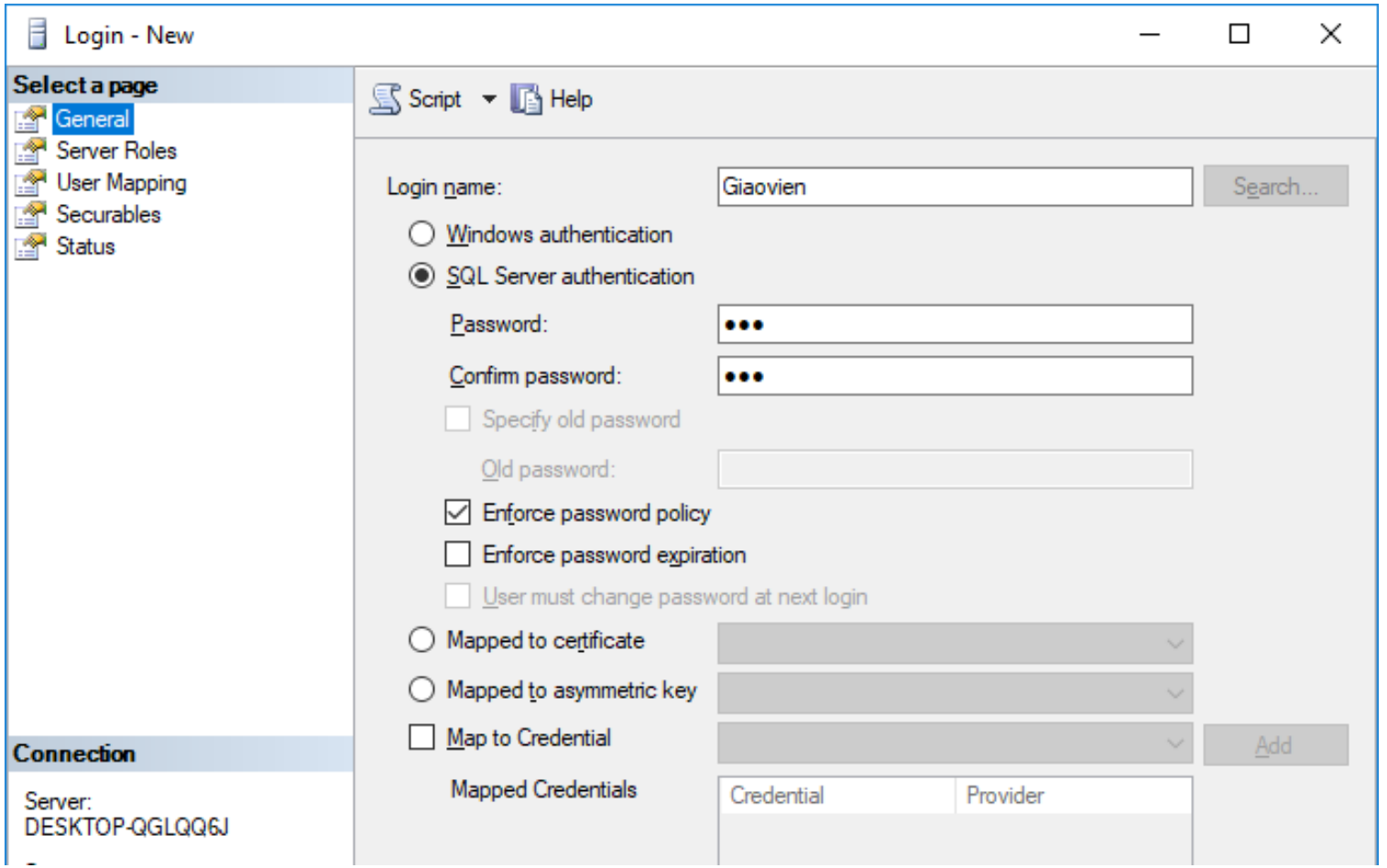


LOGIN ACCOUNT: Truy cập quyền Windows hoặc tài khoản sa

Xem tài khoản có sẵn và tạo tài khoản mới để đăng nhập vào quản trị CSDL:

Cách 1: thực hiện bằng công cụ / Tab General

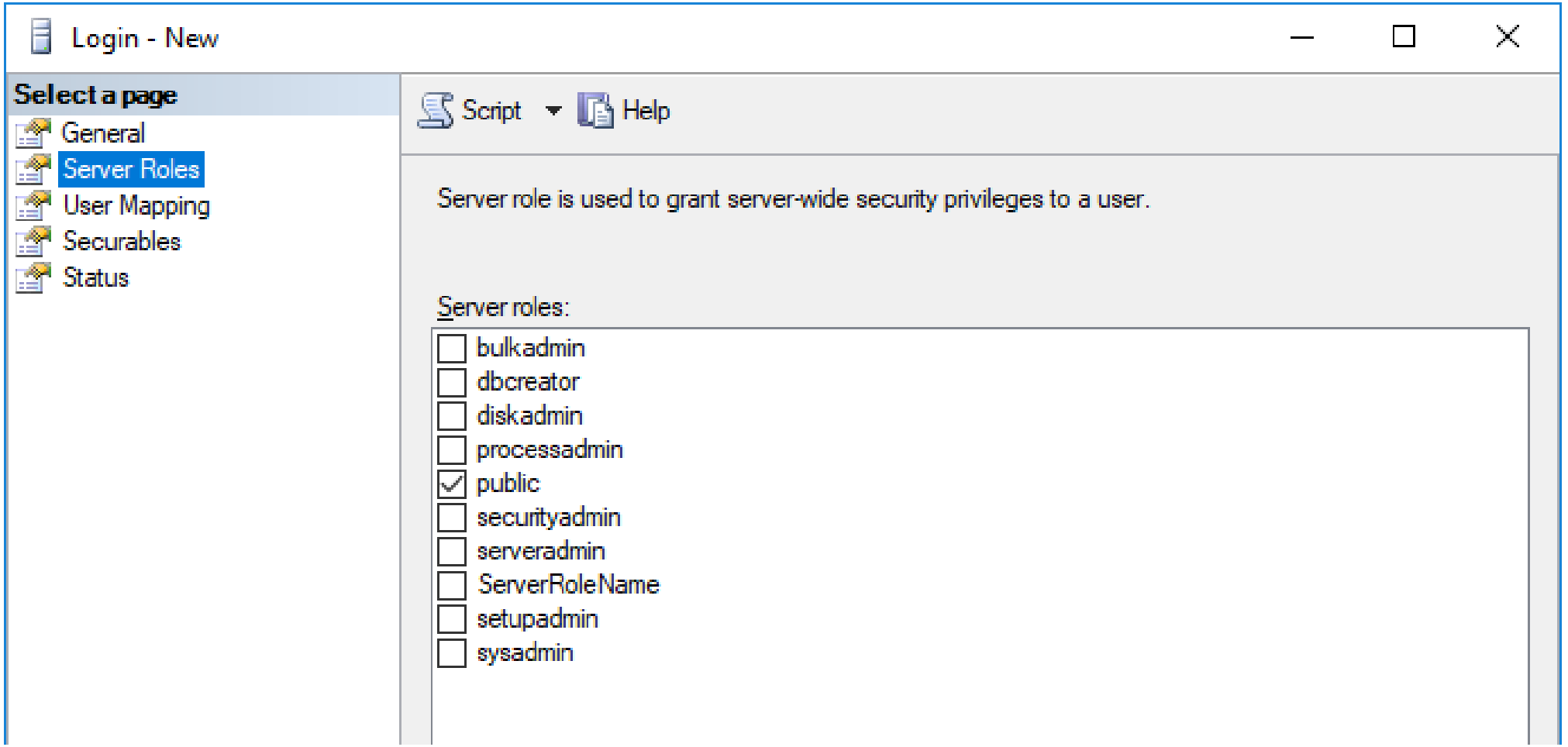




LOGIN ACCOUNT: Truy cập quyền Windows hoặc tài khoản sa

Xem tài khoản có sẵn và tạo tài khoản mới để đăng nhập vào quản trị CSDL:

Cách 1: thực hiện bằng công cụ / Tab Server Role



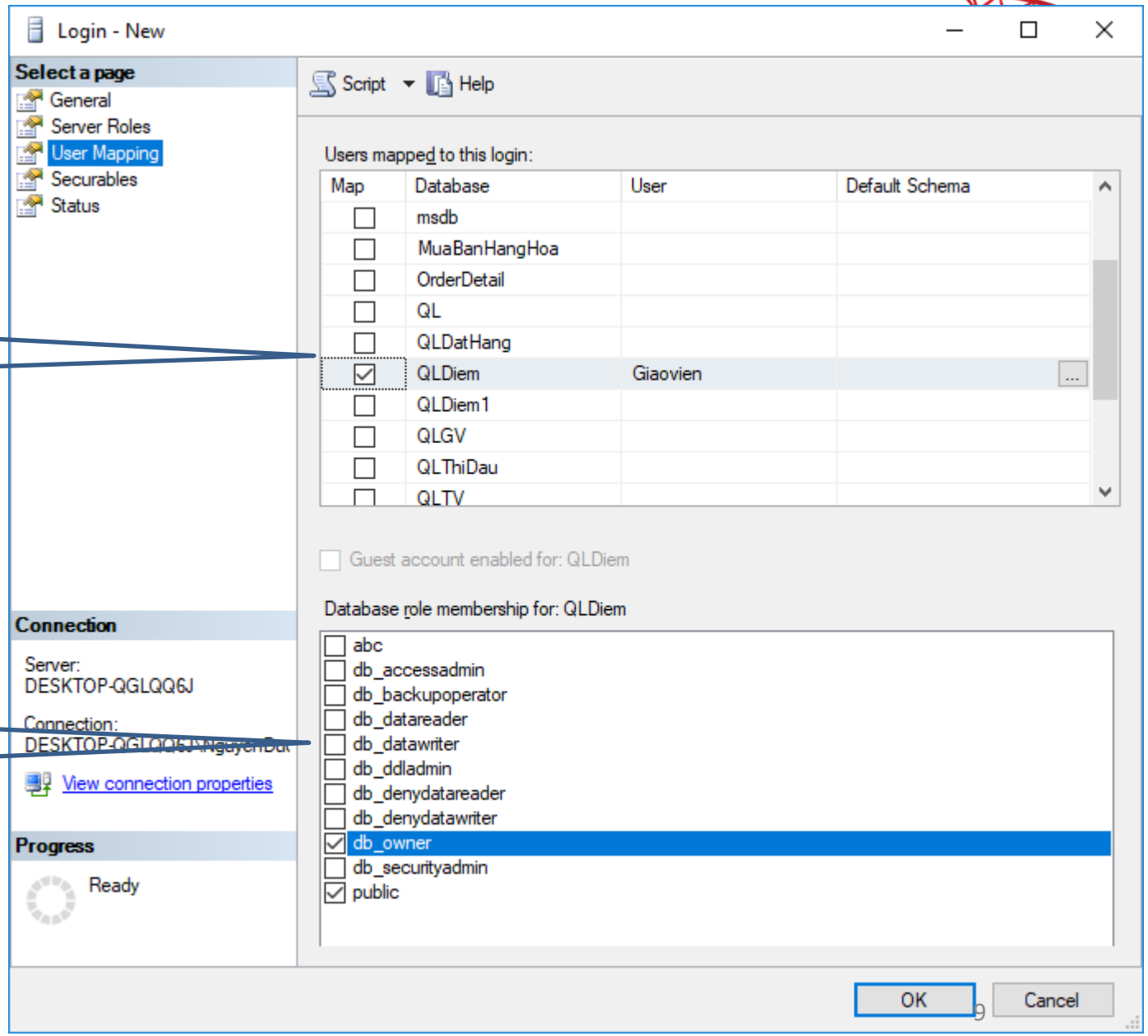
LOGIN ACCOUNT: Truy cập quyền Windows hoặc tài khoản sa

Xem tài khoản có sẵn và tạo tài khoản mới:

Cách 1: thực hiện bằng công cụ / Tab User Mapping

Chọn CSDL để cấp quyền

Cấp quyền Fixed Database Role



LOGIN ACCOUNT: Truy cập quyền Windows hoặc tài khoản sa

Xem tài khoản có sẵn và tạo tài khoản mới:

Cách 2: thực hiện bằng câu lệnh

```
CREATE LOGIN loginName WITH PASSWORD ='pass',
      CHECK_POLICY = ON,
      CHECK_EXPIRATION = OFF ;

ALTER LOGIN loginName WITH PASSWORD ='pass'

DROP LOGIN loginName
```

Ví dụ:

```
CREATE LOGIN Giaovien WITH PASSWORD='123',
    CHECK_POLICY = ON,
    CHECK_EXPIRATION = OFF ;
ALTER LOGIN Giaovien WITH PASSWORD='abc',
CHECK_POLICY = OFF,
CHECK_EXPIRATION = ON;
DROP LOGIN Giaovien
```

SERVER ROLE

Các Server Role có sẵn:

Server Role	**Giải thích**
sysadmin	Có thể làm bất kỳ điều gì trong SQL Server
serveradmin	Có thể tuỳ chỉnh cấu hình máy chủ và tắt máy chủ
setupadmin	Có thể thêm và xóa các máy chủ được liên kết bằng cách sử dụng các câu lệnh Transact-SQL
securityadmin	Có thể **GRANT**, **DENY**, **REVOKE** với cơ sở dữ liệu được cấp quyền truy cập. Có thể tự thay đổi mật khẩu
processadmin	Có thể tắt hoặc tạm dừng bất kỳ tiến trình nào hoạt động trên SQL Server
dbcreator	Có thể tạo, thay đổi, xoá và khôi phục bất kỳ cơ sở dữ liệu nào
diskadmin	Có thể quản lý các file của SQL Server
bulkadmin	Có thể thực thi các câu lệnh BULK INSERT
public	Không thể làm bất kì điều gì tác động tới cơ sở dữ liệu. Chỉ có thể truy cập tới các Object được public bên trong cơ sở dữ liệu

SERVER ROLE (Không tạo được bằng công cụ)

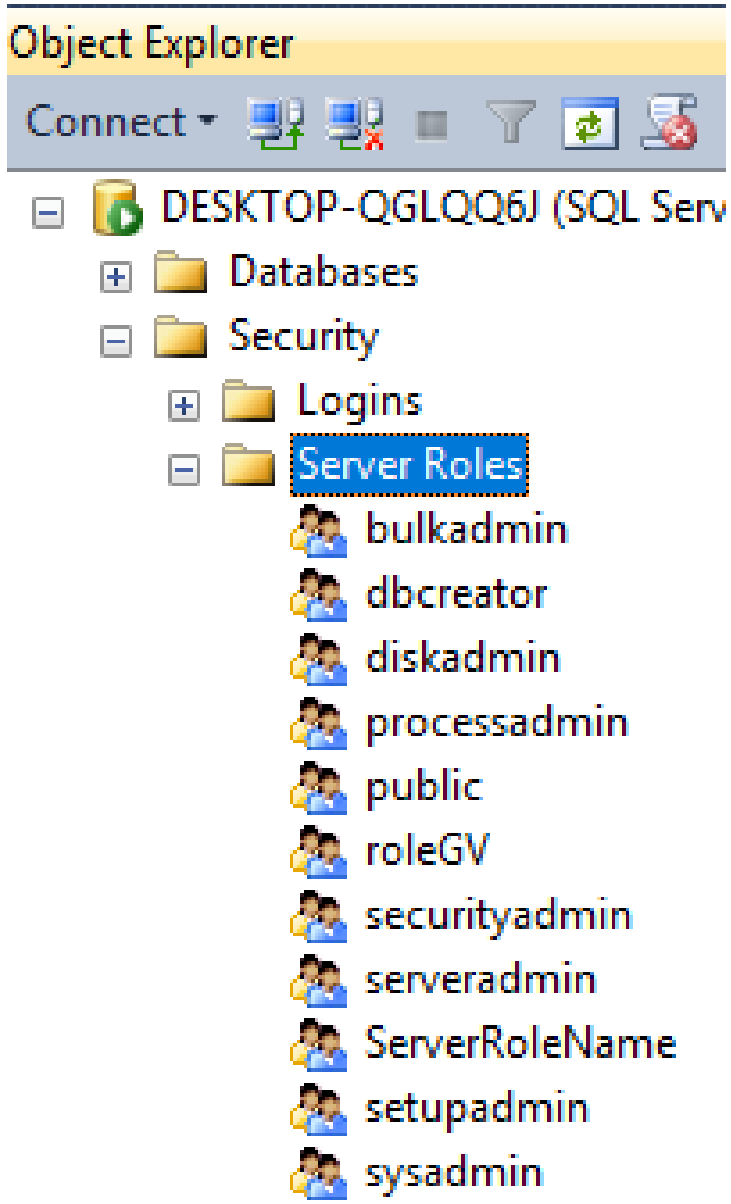
Câu lệnh liên quan Server Role:

```
CREATE SERVER ROLE role_name [ AUTHORIZATION server_principal ]
        Với server_principal chỉ định tài khoản login là owner của role này
        (nếu không có thì tài khoản đang login làm owner)
        Hoặc có thể là một Server Role đã có
 ALTER SERVER ROLE server_role_name
{        [ ADD MEMBER server_principal ] |
        [ DROP MEMBER server_principal ] |
        [ WITH NAME = new_server_role_name ]
}

 DROP SERVER ROLE role_name
```

Ví dụ:

```
CREATE SERVER ROLE roleGV AUTHORIZATION sysadmin
ALTER SERVER ROLE roleGV ADD MEMBER Giaovien
DROP SERVER ROLE roleGV
```

Xem các Server Role



FIXED DATABASE ROLE

Mỗi CSDL mặc nhiên đều có các Role sau:

Database Role	**Giải thích**
db_owner	toàn bộ người dùng có quyền full – access
db_accessadmin	người dùng có quyền quản lý các Windows Group và tài khoản SQL Server đăng nhập
db_datareader	người dùng có thể đọc được toàn bộ dữ liệu
db_datawriter	người dùng có quyền thêm, xóa hoặc chỉnh sửa dữ liệu trong bảng
db_ddladmin	người dùng có thể sử dụng các file dynamic – link library (DLL)
db_securityadmin	người dùng có thể chỉnh sửa vai trò role và quản lý các bậc quản lý, phân quyền khác
db_bckupoperator	người dùng có thể sao lưu cơ sở dữ liệu
db_denydatareader	người dùng không thể xem dữ liệu trong bảng
db_denydatawriter	người dùng không thể xem, thay đổi hoặc xóa dữ liệu trong bảng

DATABASE ROLE

Trong CSDL mặc nhiên có thể:

CREATE ROLE role_name [AUTHORIZATION owner_name]

Với owner_name có thể là database user hoặc role khác

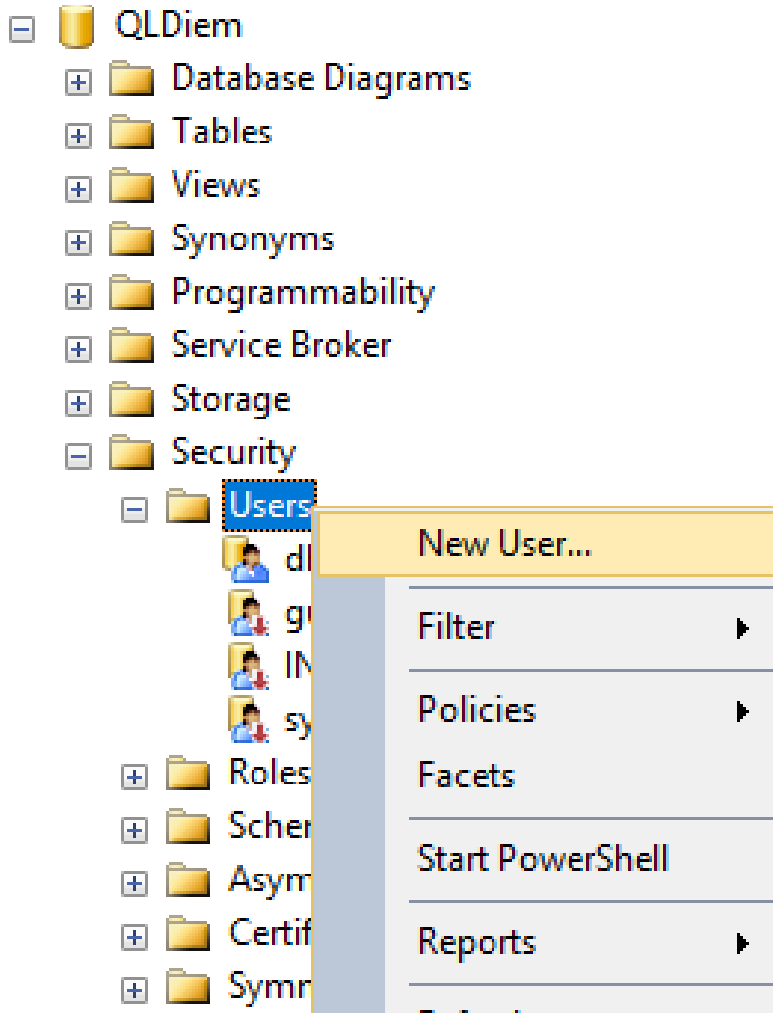
ALTER ROLE role_name
{ ADD MEMBER database_principal |
DROP MEMBER database_principal |
WITH NAME = new_name
}

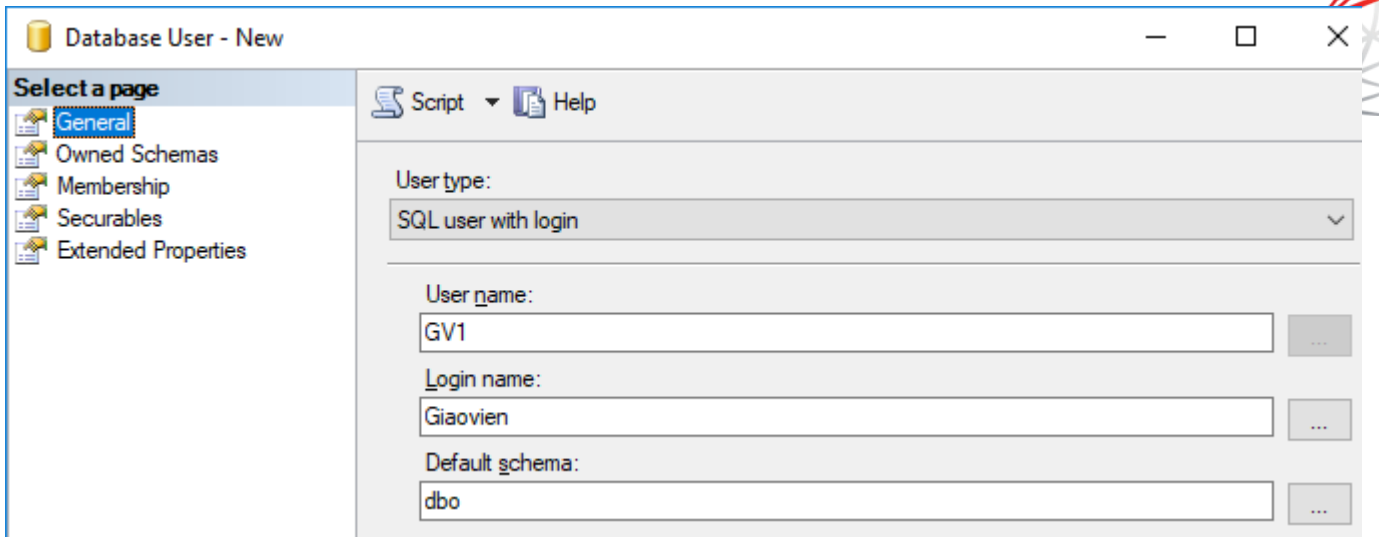
Với database_principal có thể là database user hoặc role tự tạo trong database (không thể là fixed database role hoặc Server role)

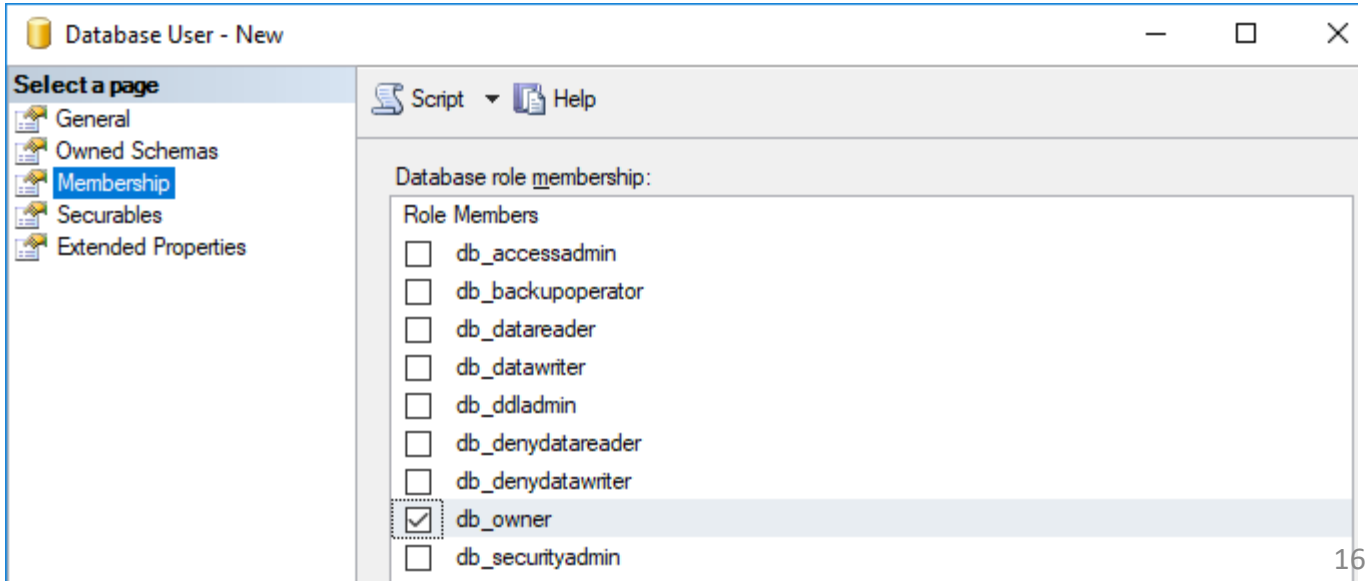
DROP ROLE role_name

USER ACCOUNT (tạo trong từng CSDL, còn gọi là Database User)

Cách 1: tạo bằng công cụ







USER ACCOUNT

Cách 2: Tạo bằng câu lệnh

```
USE [db]
CREATE USER userName FOR LOGIN loginName

ALTER USER olduserName WITH NAME=newuserName

DROP USER userName
```

Ví dụ:

```
USE QLDiem
CREATE USER GV1 FOR LOGIN Giaovien

ALTER USER GV1 WITH NAME=GV2

DROP USER GV2
```

USER ACCOUNT

Ví dụ tổng hợp:

```
        //Tạo tài khoản Login
CREATE LOGIN Giaovien WITH PASSWORD='123',
        CHECK_POLICY = ON,
        CHECK_EXPIRATION = OFF ;

        //Tạo tài khoản Database User và thêm quyền làm chủ Database
USE QLDiem
CREATE USER GV1 FOR LOGIN Giaovien
ALTER ROLE db_owner ADD MEMBER GV1

HOẶC
        //Thêm toàn quyền đối với hệ quản trị cho tài khoản Login
ALTER SERVER ROLE sysadmin ADD MEMBER GIAOVIEN
```

GRANT VÀ REVOKE

Cấp và thu quyền truy cập các đối tượng trong CSDL

GRANT <permission> ON <object> TO <user or group>

REVOKE <permission> ON <object> FROM <user or group>

+ object: TableName, ViewName, …, DATABASE::DatabaseName, ROLE::RoleName, SCHEMA ::SchemaName, …

+ permission

Khi object là Database: BACKUP DATABASE, BACKUP LOG, CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATE RULE, CREATE TABLE, CREATE VIEW.

Khi object là procedure hoặc function: EXECUTE, REFERENCES.

Khi object là table hoặc view: DELETE, INSERT, REFERENCES, SELECT, UPDATE.

+ user: Database User hoặc Login User.

+ group: Server Role, Database Role, Schema.

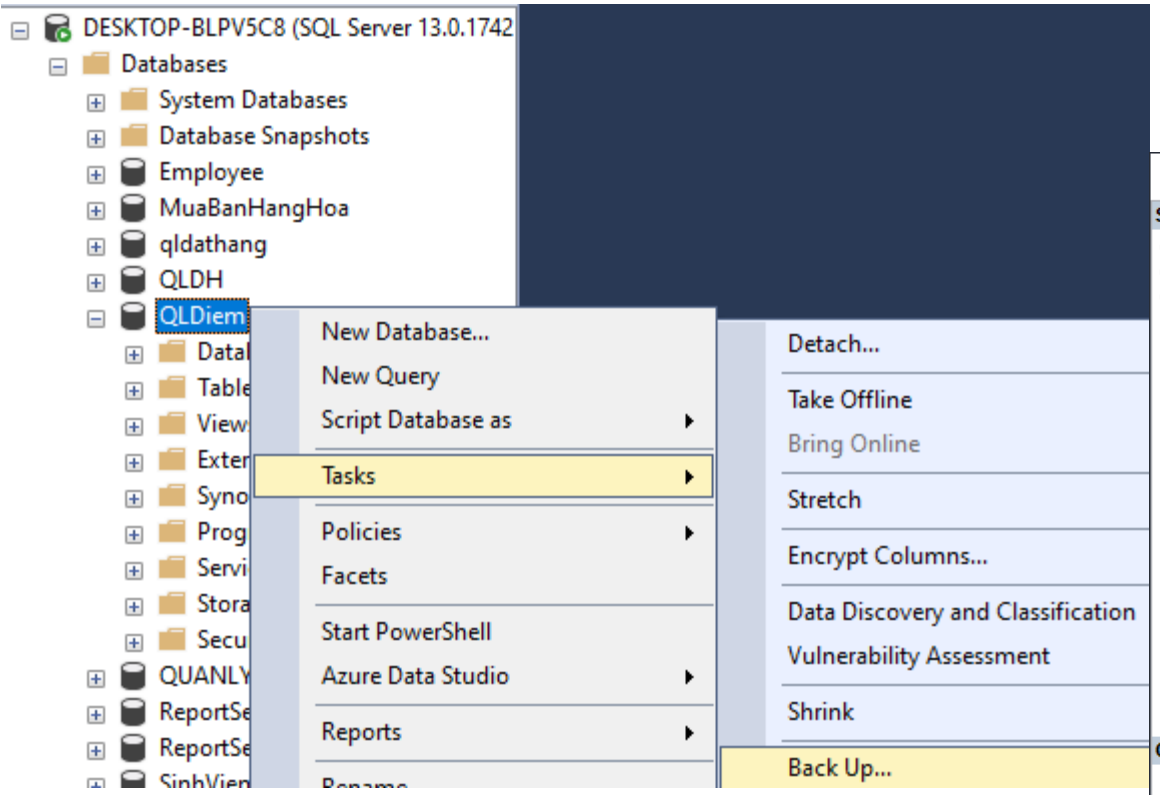
GRANT VÀ REVOKE

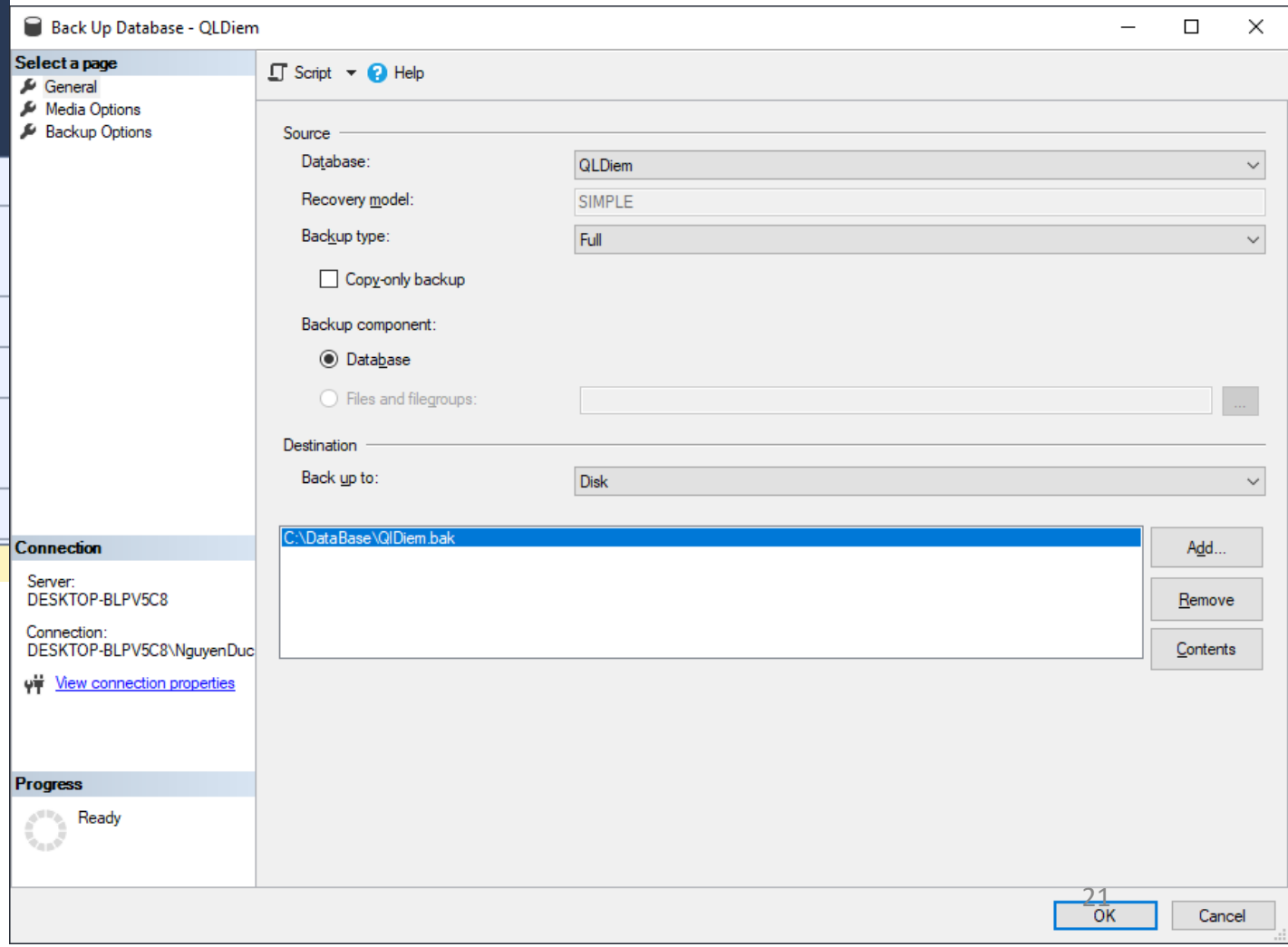
Ví dụ:

```
CREATE LOGIN Giaovien WITH PASSWORD='123',
CHECK_POLICY = ON,
CHECK_EXPIRATION = OFF

USE QLDiem
CREATE USER GV1 FOR LOGIN Giaovien

GRANT SELECT, INSERT, UPDATE, DELETE, REFERENCES ON Khoa TO GV1
REVOKE SELECT, INSERT, UPDATE, DELETE, REFERENCES ON Khoa FROM GV1

GRANT CREATE TABLE ON DATABASE::QLDiem TO GV1
REVOKE CREATE TABLE ON DATABASE::QLDiem FROM GV1

GRANT CREATE TABLE TO GV1
REVOKE CREATE TABLE FROM GV1

GRANT CONTROL ON DATABASE::QLDiem TO GV1
REVOKE CONTROL ON DATABASE::QLDiem FROM GV1
```

BACKUP DATABASE

Cách 1: Dùng công cụ





BACKUP DATABASE

Cách 2: Dùng câu lệnh

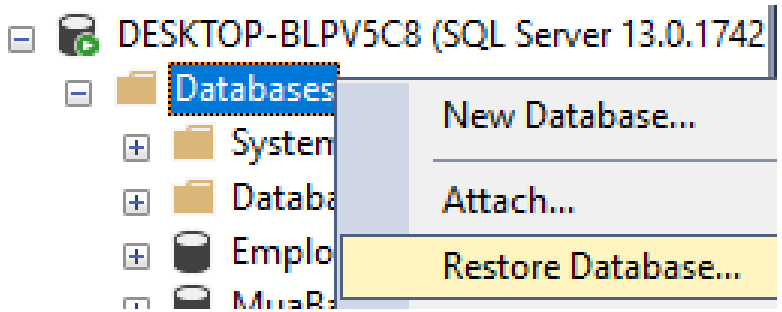
```
BACKUP DATABASE DatabaseName TO Disk='path’
```

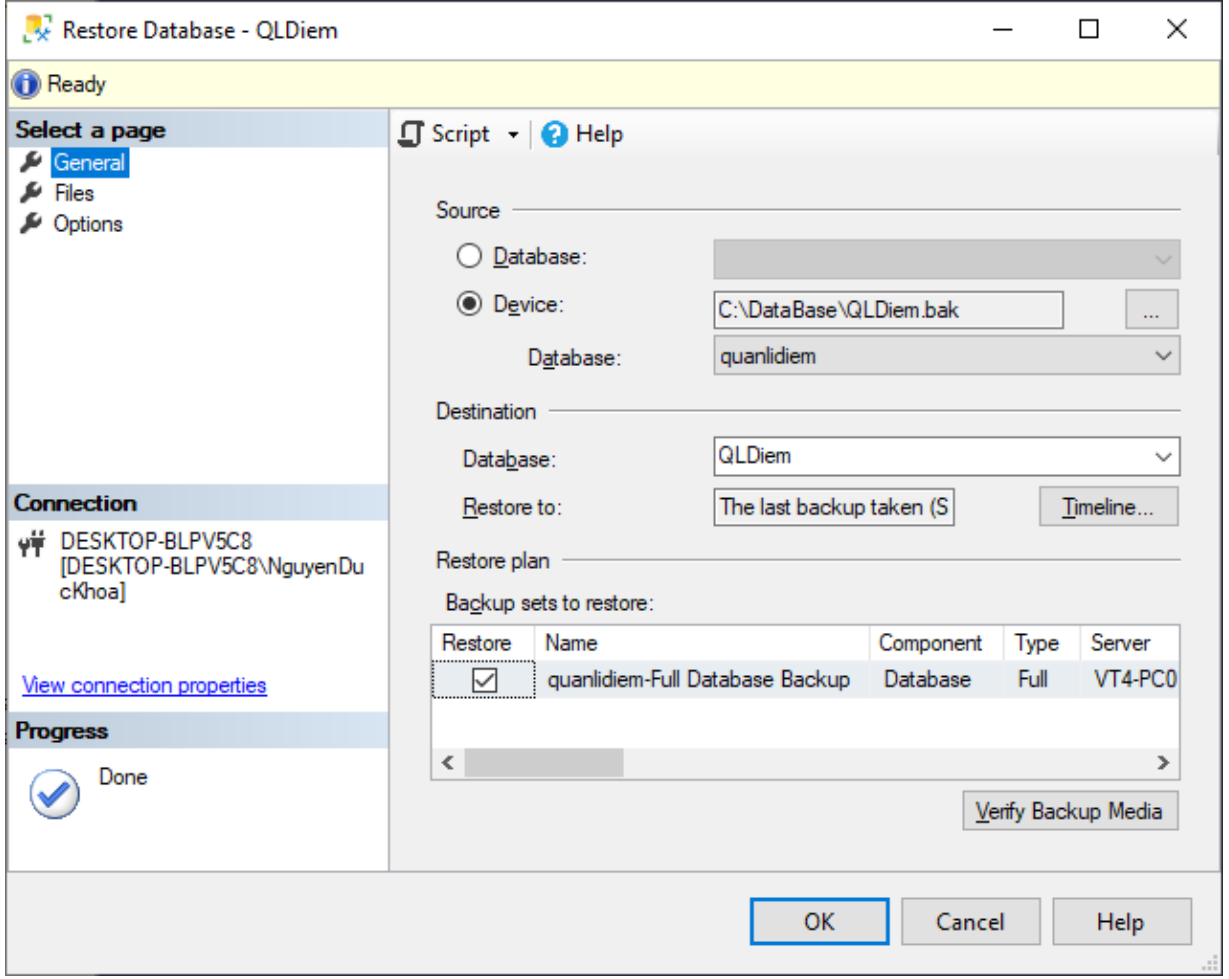
Ví dụ:

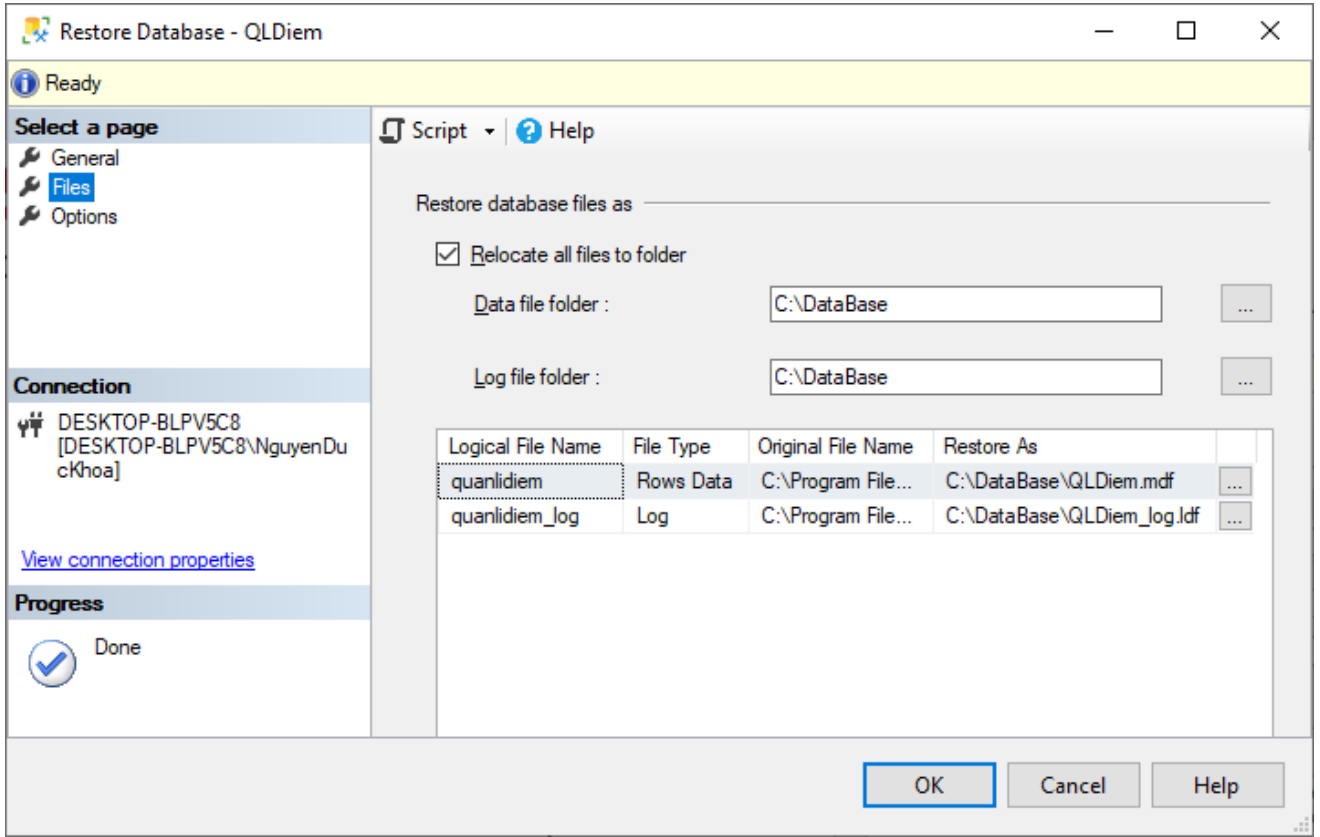
```
BACKUP DATABASE QLDiem TO Disk='C:\Database\QLDiem.bak'
```

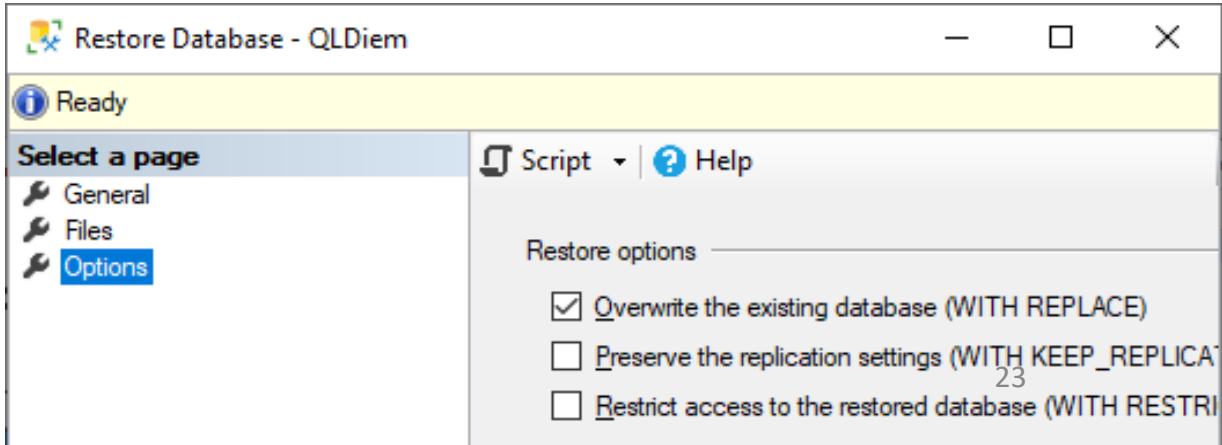
RESTORE DATABASE

Cách 1: Dùng công cụ









RESTORE DATABASE

Cách 2: Dùng câu lệnh

```
RESTORE DATABASE NewDatabaseName FROM Disk='path of .bak' WITH
        MOVE 'LogicalName of mdf' TO 'Path of .mdf',
        MOVE 'LogicalName of log' TO 'Path of .ldf'

 Xem LogicalName (có thể R_click trên Database / Properties / File)
RESTORE FILELISTONLY FROM Disk='Path of .bak'
 Đổi tên LogicalName của Datanbase (Đổi cho cả Data và Log, giống cú pháp)
ALTER DATABASE DatabaseName MODIFY FILE ( NAME=OldLogicalName, NEWNAME=NewLogicalName)
```

Ví dụ:

```
BACKUP DATABASE QLDiem TO Disk='C:\Database\QLDiem.bak'

RESTORE DATABASE QLDiem2 FROM Disk=N'C:\Database\QLDiem.bak' WITH
        MOVE N'Quanlidiem' TO N'C:\Database\QLDiem2.mdf',
        MOVE N'quanlidiem_log' TO N'C:\Database\QLDiem2.ldf'
```

BÀI TẬP

Đối với CSDL quản lý đặt hàng:

1. Tạo các tài khoản Login, User và phân quyền phù hợp cho các tài khoản như sau:
   + Quanly: toàn quyền CSDL.
   + Nhanvien: chỉ được quyền thao tác trên các đơn đặt hàng, loại hàng và mặt hàng.
   + Khachhang: chỉ được xem các đơn đặt hàng.
   + Nhacungcap: chỉ được thao tác trên các mặt hàng.
2. Backup và Restore CSDL khi cần thiết