CÁC TÁC VỤ QUẢN TRỊ HỆ THỐNG

Vai trò của người quản trị CSDL

- Quản trị viên CSDL là người chịu trách nhiệm về hiệu năng, tính toàn vẹn dữ liệu và bảo mật cho CSDL. Đồng thời người quản trị có vai trò lập kế hoạc, phát triển, khắc phục sự cố xảy ra với CSDL.
- Các tác vụ quản trị thường thực hiện:
  - Bảo mật, tạo tài khoản người dùng và phân quyền
  - Lập các chiến lược sao lưu CSDL để phục hồi khi gặp sự cố
  - Tạo lịch sao lưu CSDL tự động
  - …

Nội dung

- Phân quyền và bảo mật
- Sao lưu và phục hồi
- Chuyển đổi giữa các loại CSDL
- Kiến trúc nhân bản

Phân quyền và bảo mật

Bảo mật CSDL

- **Mục đích của bảo mật**: nhằm bảo vệ CSDL khỏi những truy xuất trái phép
- SQL server sử dụng quyền và vai trò để bảo mật CSDL:
  - Quyền (Permission)
    - Quy định các hành động (action) người dùng có thể thực hiện trên CSDL hoặc các đối tượng CSDL cụ thể
  - Vai trò (Role)
    - Là tập quyền được gán cho người dùng

Bảo mật CSDL (tiếp)

- Mỗi người dùng hoặc nhóm người dùng được gán các quyền và vai trò nhất định để truy cập tới CSDL
- SQL Server dựa vào quyền và vai trò cấp cho người dùng/nhóm người dùng để xác định các đối tượng, câu lệnh SQL … người dùng được phép tác động trên CSDL

Các mức bảo mật của SQL Server

- Bảo mật trong SQL Server gồm 3 lớp
  - Mức xác thực đăng nhập (Authentication/Login Security): là mức ngoài cùng, kiểm soát xem ai có thể đăng nhập vào server
  - Database access security: kiểm soát xem user nào có thể truy cập vào một Database cụ thể trên server
  - Permission security: kiểm soát một user có thể thực hiện được thao tác gì trên Database

Mức Login Security

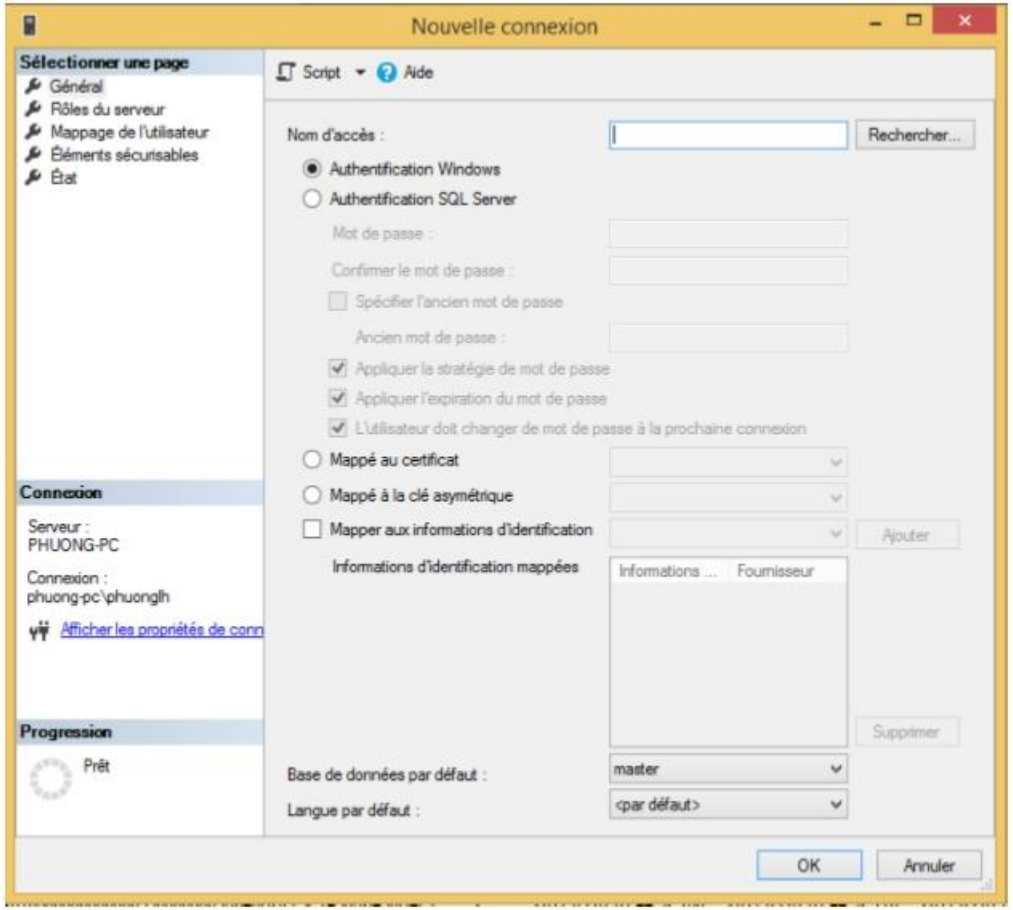
- Login là đối tượng được quyền truy cập vào SQL Server (khác với User là người khai thác CSDL).
- Các Login chỉ mới kết nối vào SQL Server chứ chưa hẳn có quyền truy cập vào CSDL.
- Thông tin đăng nhập được lưu trong bảng syslogins của CSDL master
- Có 2 loại đăng nhập:
  - Window authentification
  - SQL Server authentification

Mức Login Security (tiếp)

- **Window authentification**:
  - Login vào SQL Server với tư cách một Window account
  - Không cần nhập username, password
- **SQL Server authentification**:
  - Login vào SQL Server với tư cách người dùng của SQL Server, do quản trị SQL Server tạo ra
  - Cần nhập username, password
  - Trình cài đặt SQL Server tự động tạo ra một user có name là sa và password là NULL.

Tạo Login bằng SQL Server Management Studio

- Mở rộng cây bên trái, chọn Security, nhấn chuột phải vào Logins, chọn New Login:
  - Tạo Window login:
    - chọn Authentification Window
    - Có thể chọn trong danh sách Account của Windows
  - Tạo SQL Server login:
    - Chọn Authentification SQL Server
    - Cần nhập tên mới, mật khẩu



Tạo Login bằng T-SQL

- Tạo Window login:
  - Dùng lệnh:

    sp_grantlogin tên_đăng_nhập
- Tạo SQL Server login:
  - Dùng lệnh:

    sp_addlogin ‘tên_đăng_nhập’, ‘mật_khẩu’

Chế độ bảo mật

- SQL Server có 2 chế độ bảo mật:
  - Windows Authentication mode: là chế độ bảo mật mà những người dùng truy cập SQL Server phải là những user của Window, kết nối với SQL Server bằng Windows Authentication. Việc kiểm tra an toàn các kết nối được ủy nhiệm cho Windows
  - Mixed Mode: Kết nối với SQL Server bằng Windows Authentication hoặc SQL Server Authentication
- Để chuyển đổi chế độ chứng thực:

Database access security

- Các login mới chỉ có quyền truy nhập vào server chứ chưa hẳn đã có quyền truy nhập vào CSDL chứa trong đó.
- Mỗi Database có một danh sách các user được phép truy cập vào cơ sở dữ liệu, các user này luôn luôn đính (mapped) với một login ở mức Server.
- Khi đăng nhập vào SQL Server thông qua login, ta sẽ có quyền truy nhập vào CSDL theo quyền hạn mà user tương ứng với login được cung cấp

Database access security (tiếp)

- Xem danh sách các user của mỗi CSDL trong mục Security/Users của CSDL tương ứng
- Mỗi login có thể là user của nhiều CSDL với những quyền hạn khác nhau
- Mặc định, user name trùng tên với login account
- Ví dụ: login có tên là userSQL. CSDL 1 có user userSQL (có quyền đọc) gắn với login userSQL. CSDL 2 có user userSQL (có quyền đọc/ghi) gắn với login userSQL.
  - Khi truy cập vào SQL Server với login userSQL, bạn sẽ có quyền đọc trên CSDL 1 và quyền đọc/ghi trên CSDL 2

Tạo Database user

- Tạo một user trong CSDL
  - Dùng SQL Server Management Studio: vào CSDL muốn tạo user, chọn Security/Users, nhấn chuột phải chọnNew User
  - Dùng lệnh

```
sp_grantdbaccess ‘login name’, ‘user name’
```

  - Ví dụ: gán quyền khai thác cho user của Windows và lấy theo tên mới

```
USE QLSV

exec sp_grantdbaccess ‘phuonglh’, ‘Phuong’
```

Xóa Database user

- Xóa một user trong CSDL
  - Dùng SQL Server Management Studio: vào CSDL cần xóa user, chọn Security\Users, nhấn chuột phải chọn Delete User
  - Dùng lệnh

    sp_revokedbaccess ‘user name’
  - Ví dụ:

    USE QLCH

    exec sp_revokedbaccess ‘Phuong’

PERMISSION SECURITY

- SQL Server sử dụng quyền và vai trò để kiểm soát user có thể được làm gì trên CSDL
  - Vai trò (Roles):
    - là tập quyền được gán cho người dùng
  - Quyền (Object/Statement Permission):
    - quy định các quyền user có thể thao tác trên các đối tượng và các lệnh cụ thể

Các quyền chuẩn của các đối tượng SQL Server

Quyền	Các thao tác được phép thực hiện	Đối tượng áp dụng
SELECT	Truy xuất dữ liệu	Bảng, View, Hàm giá trị bảng
UPDATE	Cập nhật dữ liệu	Bảng, View, Hàm giá trị bảng
INSERT	Thêm dữ liệu mới	Bảng, View, Hàm giá trị bảng
DELETE	Xóa dữ liệu	Bảng, View, Hàm giá trị bảng
EXECUTE	Thực thi một Stored Procedure hay một hàm	Stored procedure, Hàm vô hướng và hàm kết hợp
REFERENCES	Tạo các đối tượng tham chiếu tới đối tượng này	Bảng, View, Hàm
ALL	Có tất cả các quyền đối với đối tượng	Bảng, View, Hàm , Stored Procedure

Vai trò

- Khái niệm ROLE tương tự như khái niệm GROUP
- Role là công cụ để cung cấp quyền cho một nhóm các user thay vì phải thực hiện trên từng user
- Cách thức cấp quyền cho user thông qua Role:
  - Gán quyền cho mỗi Role
  - Xếp user vào Role
- Nếu không muốn duy trì quyền hạn cho một user=>loại user ra khỏi role

Vai trò (tiếp)

- Có 2 loại vai trò:
  - Server Role: được sử dụng để cho phép hoặc hạn chế user thực hiện các thao tác (operation) trên server
  - Database Role: được sử dụng để cung cấp các mức khác nhau để truy cập CSDL. Có 2 loại
    - Fixed Database Roles: những role có sẵn trong hệ thống
    - User defined Roles: do người dùng tạo ra. Để có quyền tạo ra role, bạn phải là thành viên db_secutityadmin, hoặc db_owner hoặc sysadmin.

Vai trò server mặc định

- Vai trò Server mặc định bao gồm những người dùng quản trị Server:

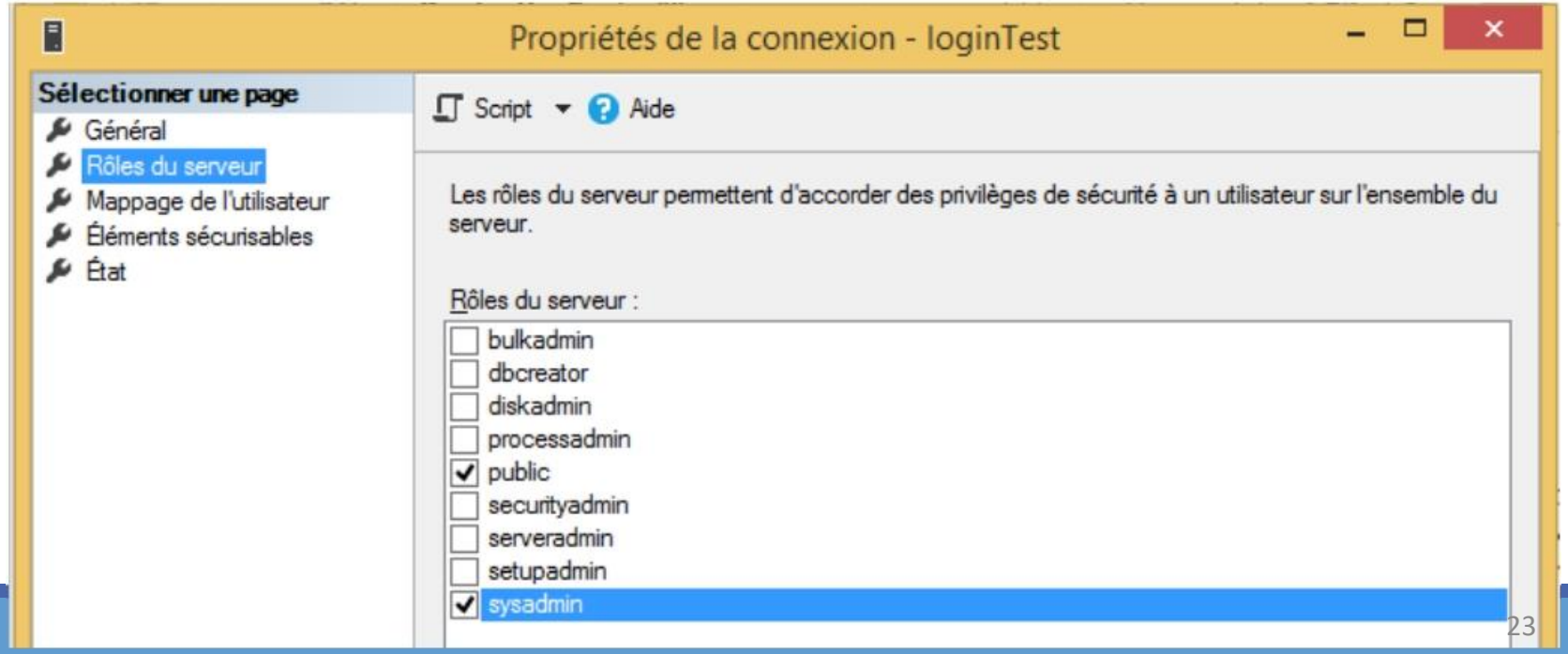
Vai trò	Mô tả
sysadmin	Có thể thực hiện mọi thao tác trên server. Theo mặc định, tất cả thành viên trong nhóm Windows BUILTIN\Administrators đều là thành viên của vai trò này.
securityadmin	Có thể quản lý ID và mật khẩu đăng nhập cho server, đồng thời có thể cấp, từ chối và thu hồi quyền trên cơ sở dữ liệu.
dbcreator	Có thể tạo, thay đổi, xóa và khôi phục cơ sở dữ liệu.

Vai trò CSDL mặc định

Vai trò	Mô tả
Db_owner	Có tất cả các quyền đối với CSDL
Db_accessadmin	Có quyền thêm hoặc xóa một LoginID của CSDL
Db_securityadmin	Có thê quản trị quyền đối tượng, quyền CSDL, Vai trò, các thành viên của Vai trò
Db_datawriter	Có thể thêm, xóa, cập nhật dữ liệu trên toàn bộ các bảng trong CSDL
Db_datareader	Có thể truy xuất dữ liệu từ tất cả các bảng trong CSDL
Db_denydatawriter	Không thể thêm, xóa, cập nhật dữ liệu trên toàn bộ các bảng trong CSDL
Db_denydatareader	Không thể truy xuất dữ liệu từ tất cả các bảng trong CSDL
Db_backupoperator	Có thể thực hiện sao lưu CSDL và chạy các kiểm tra tính nhất quán trên CSDL

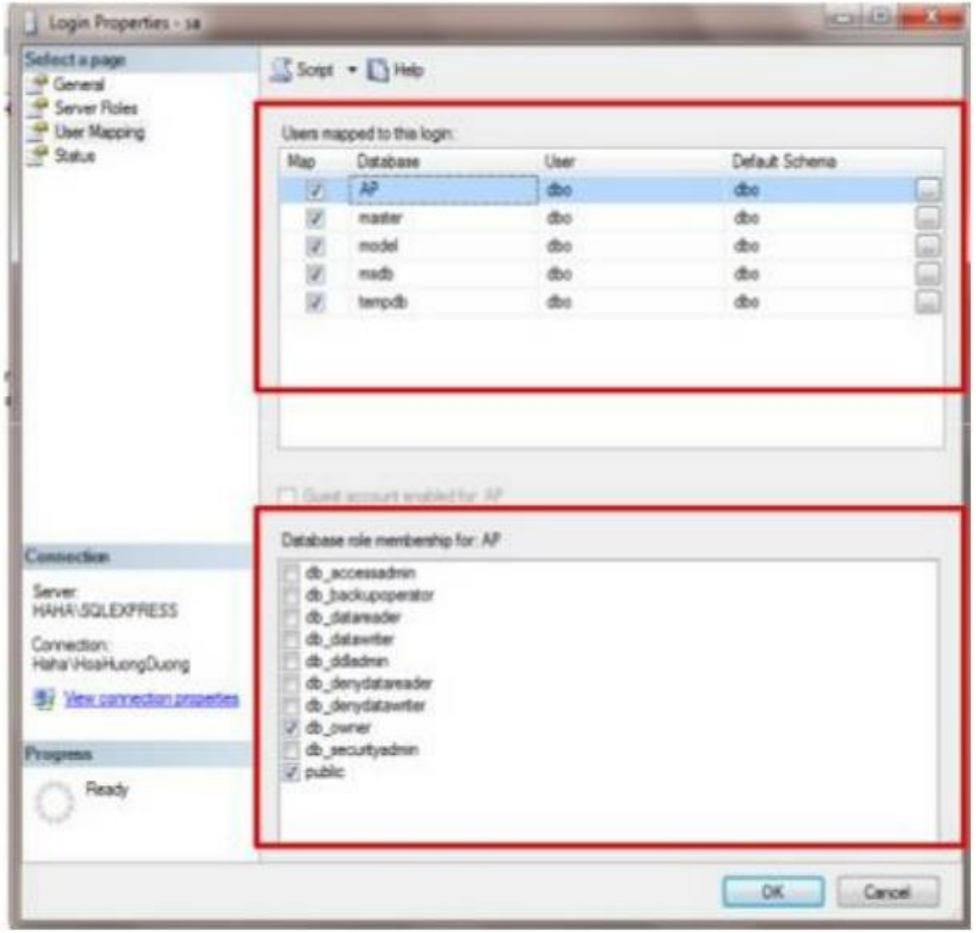
Gán vai trò Server cho một Login ID

- Nhấn chuột phải vào Login tương ứng, chọn Properties, sau đó chọn các **server role** để gán vai trò server cho một Login ID



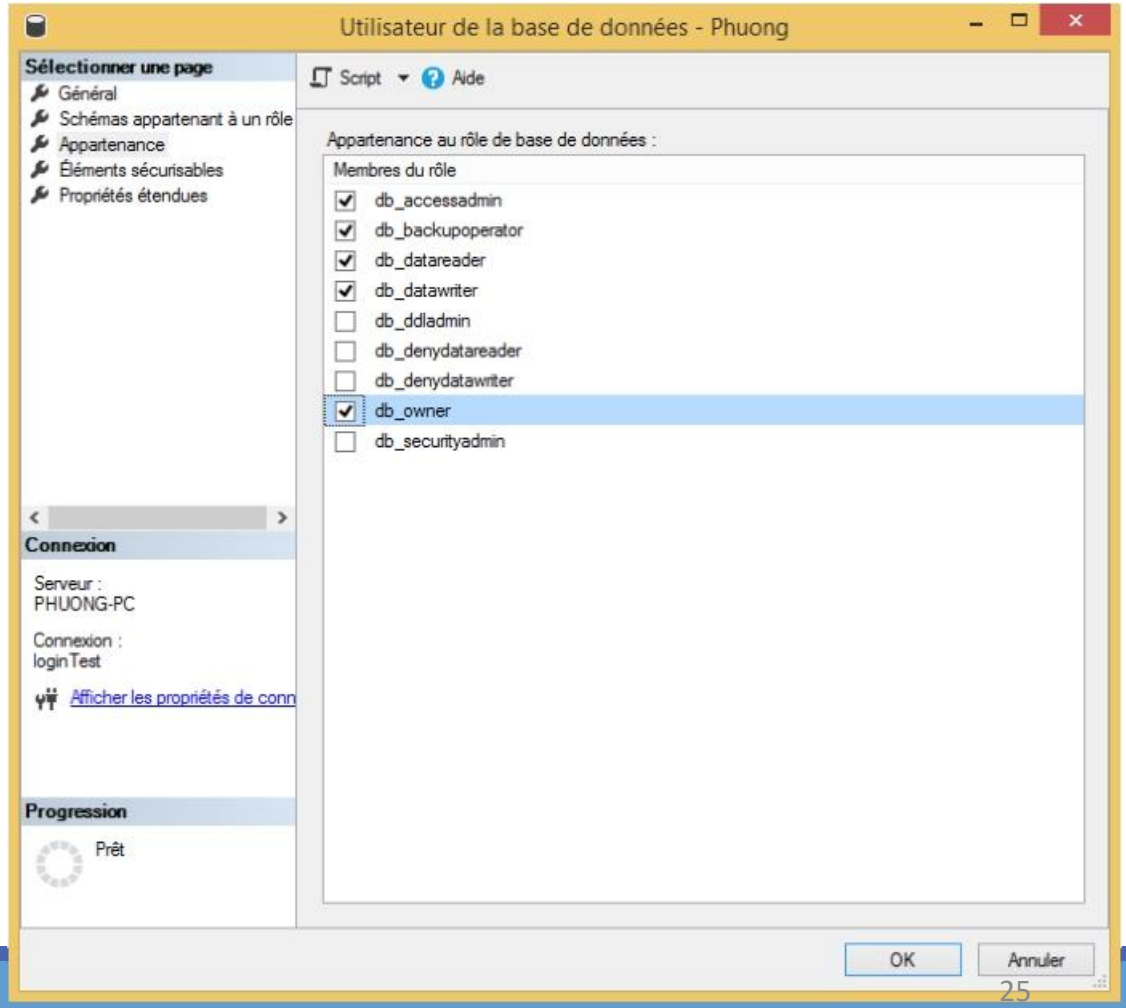
Gán vai trò CSDL cho một Login ID

- Nhấn chuột phải vào Login tương ứng, chọn Properties, sau đó chọn các User mapping để gán vai trò CSDL cho một Login ID
  - Chọn danh sách các CSDL
  - Chọn các quyền tương ứng



Gán vai trò CSDL cho một Database user

- Nhấn chuột phải vào User tương ứng, chọn Properties, sau đó chọn các vai trò CSDL tương ứng với user



Vai trò tự định nghĩa (User defined role)

- Các bước dùng T-SQL để tạo ra user defined role
  - Bước 1: Định nghĩa một role (Tạo một role mới)
  - Bước 2: Gán quyền về statement và object cho role
  - Bước 3: Gán các user là thành viên của role

Vai trò tự định nghĩa (User defined role) (tiếp)

- Định nghĩa một role

  sp_addrole ‘rolename’, ‘role_owner’

  - Ví dụ:

  sp_addrole ‘teacher’

- Cấp quyền cho role teacher

```
GRANT SELECT ON SINHVIEN to teacher
```

Vai trò tự định nghĩa (User defined role) (tiếp)

- Thêm user vào role

  sp_addrolemember ‘role_name’, ‘user_name’

  - Ví dụ:

    sp_addrolememer ‘teacher’, ‘phuonglh’

- Xóa một role:

  sp_droprole ‘role_name’

  - Ví dụ:

    sp_droprole ‘teacher’

PERMISSION SECURITY: OBJECT AND STATEMENT PERMISSION

- Kiểm soát một user/role có thể thực hiện hành động gì trên một object cụ thể trên CSDL
- Object nhỏ nhất là column
- Các object: column, row, table, data type, constraint, default, rule, index, view, stored procedure, trigger
- **Statement Permission**: điều khiển xem user được phép hay ko được phép **tạo, xóa** các object (CREATE, DROP)
- **Object Permission**: điều khiển user nào được phép thao tác dữ liệu (INSERT, DELETE, UPDATE) trên object

PERMISSION SECURITY: OBJECT AND STATEMENT SECURITY

- GRANT (Lệnh cấp quyền): Nếu bạn cấp quyền cho user, user lại là thành viên của role thì user sẽ có quyền do bạn cấp + quyền của role

```
GRANT { { ALL | permission [ ,...n ] } [ (
   column_name [ ,...n ] ) ]
ON
   { table | view | stored_procedure |
   extended_procedure | user_defined_function }}
   TO user_name [ ,...n ]
```

PERMISSION SECURITY: OBJECT AND STATEMENT SECURITY

- **DENY (Lệnh từ chối)**: ngăn không cho user sử dụng quyền và không cho phép user có cơ hội thừa hưởng quyền đó với tư cách là thành viên của role
- **Ví dụ**: Bạn deny quyền SELECT của một user, trong khi user thuộc về một role có quyền SELECT thì user không thể dùng quyền SELECT

```
DENY { { ALL | permission [ ,...n ] } [ ( column_name
    [ ,...n ] ) ]
ON
    { table | view | stored_procedure |
    extended_procedure | user_defined_function }}
    TO user_name [ ,...n ]
```

27

PERMISSION SECURITY: OBJECT AND STATEMENT SECURITY

- REVOKE: thu hồi lại quyền đã cấp cho user
- Cú pháp:

  REVOKE{ALL | permissions [,…,n]}

  FROM user_name [,…,n]
- Ví dụ:

  REVOKE CREATE TABLE, CREATE DEFAULT

  FROM Phuong, Chau