



Bài 6:
BẢO MẬT TRONG SQL SERVER 2008

- Các nội dung đã học trong bài trước
 - Hàm người dùng định nghĩa
 - View

1. Bảo mật CSDL

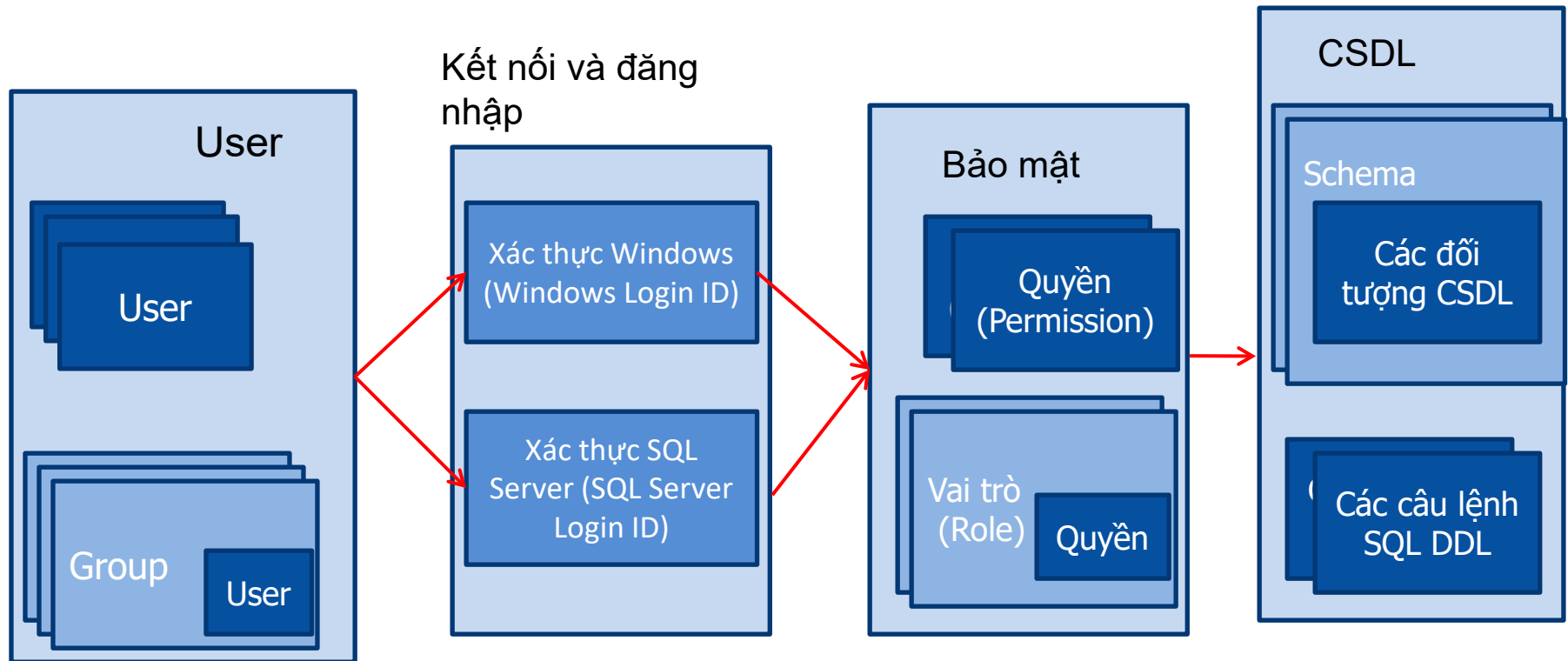
2. Login ID

3. Người dùng CSDL

4. Quyền & Vai trò

BẢO MẬT CƠ SỞ DỮ LIỆU

- 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 hoạch, 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 (học trong bài này)
 - Lập các chiến lược sao lưu CSDL để phục hồi khi gặp sự cố (học trong bài sau)
 - Tạo lịch sao lưu CSDL tự động (học trong bài sau)
 -



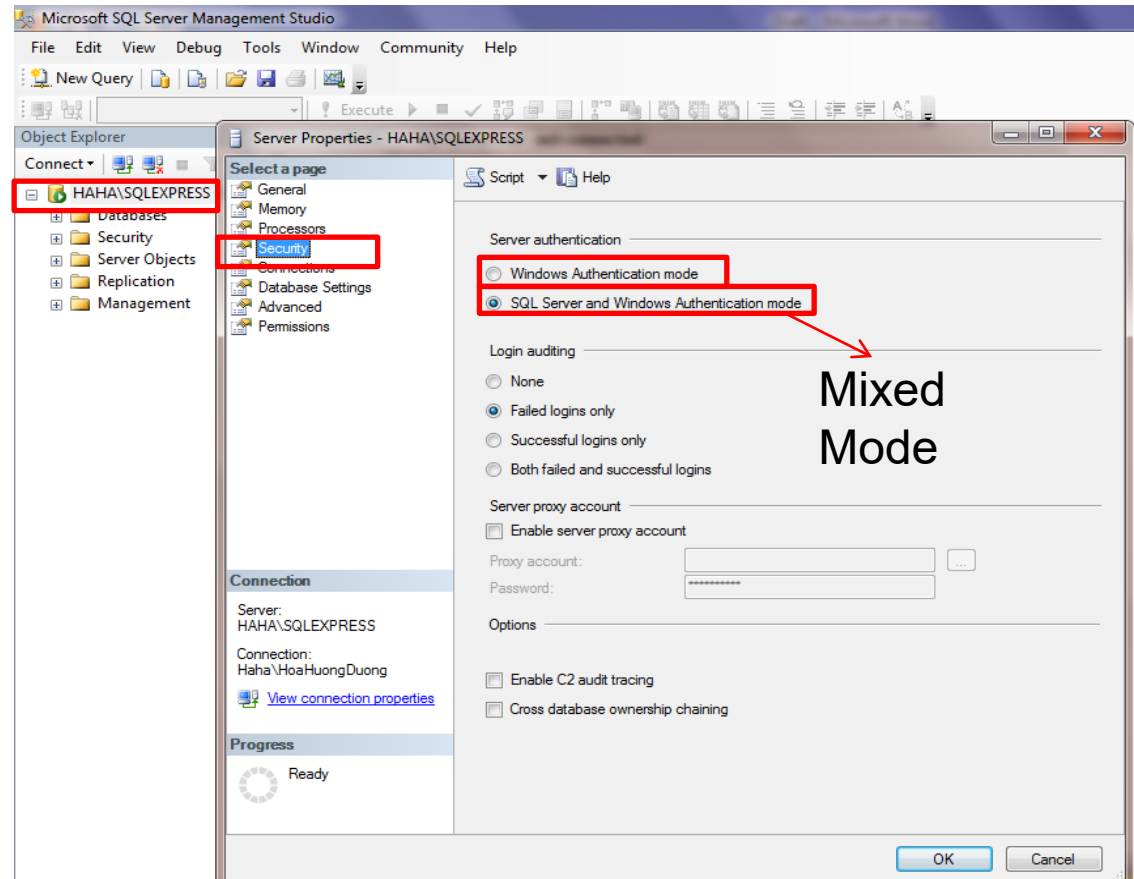
Xử lý truy cập tới CSDL trên SQL Server

- 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
- 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

■ Nhấp chuột phải vào Server chọn Properties

■ Hai chế độ:

- Windows Authentication mode
- Mixed Mode: Chọn chế độ này, người dùng có thể đăng nhập sử dụng Windows Login ID hoặc SQL Server Login ID



- **T-SQL**

- Được dùng để quản trị Login ID, người dùng CSDL, quyền, vai trò

- **Management Studio**

- Sử dụng Management Studio để thực hiện tất cả các cấu hình bảo mật

LOGIN ID

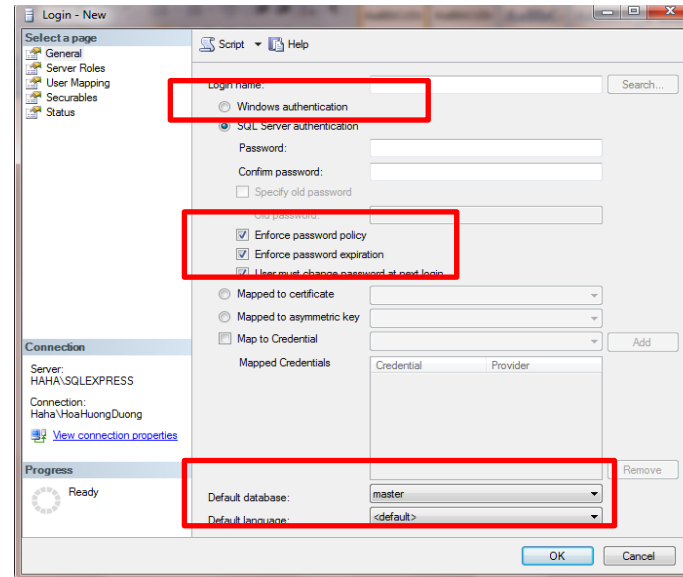
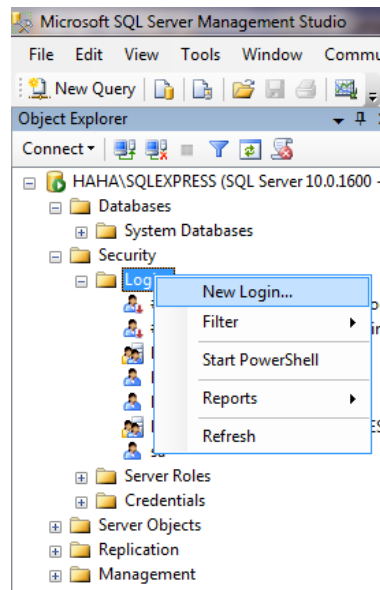
- Người dùng kết nối tới CSDL SQL Server sử dụng Login ID
- Hai loại Login ID
 - Windows Login ID
 - SQL Server Login ID

■ Tạo Windows Login ID

- Chọn checkbox Windows authentication

■ Tạo SQL Login ID

- Chọn checkbox SQL Server authentication



■ Sinh viên tìm hiểu thêm về các tùy chọn trong SGK

■ Tạo Windows Login ID

```
CREATE LOGIN <tên đăng nhập> FROM WINDOWS  
[WITH [DEFAULT_DATABASE = <Tên cơ sở dữ liệu>]  
[, DEFAULT_LANGUAGE = <Ngôn ngữ>]]
```

■ Tạo SQL Login ID

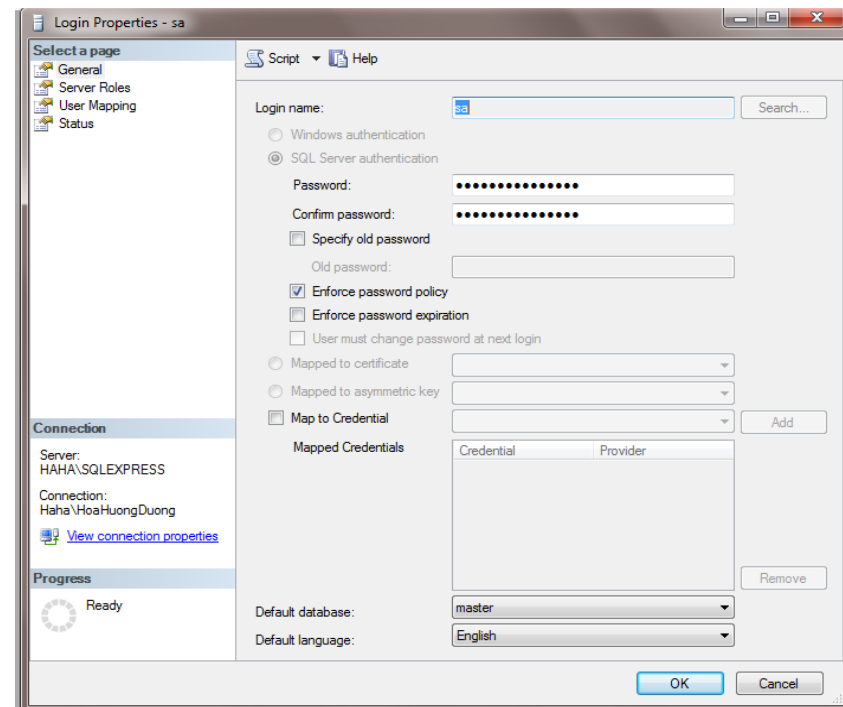
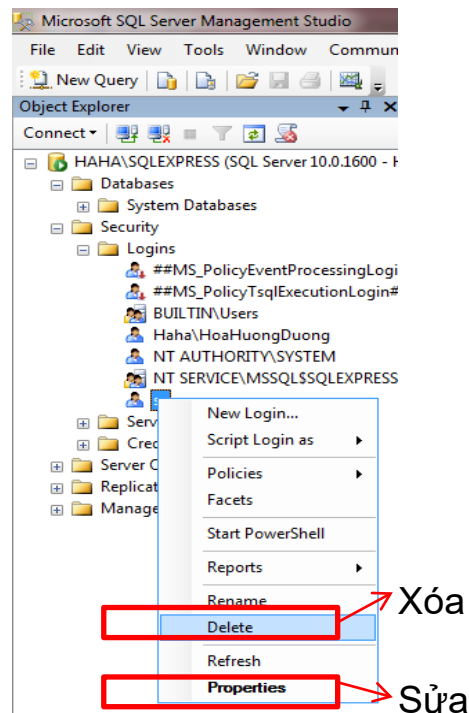
```
CREATE LOGIN <Tên đăng nhập>  
WITH PASSWORD = 'password' [MUST_CHANGE]  
[, DEFAULT_DATABASE = <Tên cơ sở dữ liệu>]  
[, DEFAULT_LANGUAGE = <Ngôn ngữ>]  
[, CHECK_EXPIRATION = {ON|OFF}  
[, CHECK_POLICY = {ON|OFF}]
```

■ Ví dụ tạo SQL Login ID

```
CREATE LOGIN JohnDoe WITH PASSWORD = 'pt8806FG$B',  
DEFAULT_DATABASE = AP
```

- Không để trống trường Password hoặc sử dụng các giá trị "Password", "Admin", "Administrator", "sa", hay "sysadmin"
- Không sử dụng tên máy, hoặc tên người dùng hiện thời
- Có nhiều hơn 8 ký tự
- Phải chứa ít nhất ba trong số các loại ký tự sau: Chữ cái viết hoa, chữ cái viết thường, ký tự số, ký tự đặc biệt (#, %, &, ...)

Sửa Login ID



- Sinh viên tham khảo thêm cách sử dụng câu lệnh T-SQL để sửa/xóa Login ID trong sách giáo khoa

NGƯỜI DÙNG CƠ SỞ DỮ LIỆU

- Mỗi CSDL có một danh sách người dùng được xác thực để truy cập đến CSDL đó
- Khi tạo một database user
 - User chỉ có quyền chọn ngữ cảnh CSDL, không có quyền thực thi các thao tác trên CSDL và trên các đối tượng của CSDL đó
 - Để có thể thực hiện các thao tác này user phải được cấp quyền đối tượng và quyền CSDL

■ Cú pháp tạo Database User

```
CREATE USER <Tên user>  
    [{FOR|FROM} LOGIN <Tên đăng nhập>]  
    [WITH DEFAULT_SCHEMA = <Tên schema>]
```

■ Cú pháp sửa Database User

```
ALTER USER <Tên user> WITH  
    [NAME = <Tên user mới>]  
    [, DEFAULT_SCHEMA = <Tên schema>]
```

■ Cú pháp xóa Database User

```
DROP USER <Tên user>
```

- Chú ý: Câu lệnh CREATE user tạo một user mới trong CSDL hiện thời. Do đó bạn phải chọn ngữ cảnh CSDL trước khi thực thi câu lệnh

- Tạo Database User với tên User và Login ID trùng nhau

```
CREATE USER JohnDoe
```

- Tạo Database User cho một Windows User Account

```
CREATE USER SusanRoberts FOR LOGIN [Accounting\SusanRoberts]
```

- Đổi tên User

```
ALTER USER SusanRoberts WITH NAME = SusanStanley
```

QUYỀN & VAI TRÒ

■ 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 là một tập các quyền**
 - Có thể dùng để gán cho một người dùng hoặc một nhóm người dùng.
- **SQL Server đã xây dựng sẵn các Vai trò mặc định gồm**
 - Vai trò Server mặc định
 - Vai trò CSDL mặc định
- **Bạn có thể tự định nghĩa thêm các Vai trò mới**
- **Mỗi Vai trò được gán một tập quyền**
 - Ví dụ Vai trò dbcreator có thể thực thi các câu lệnh CREATE/ALTER/DROP DATABASE, RESTORE DATABASE

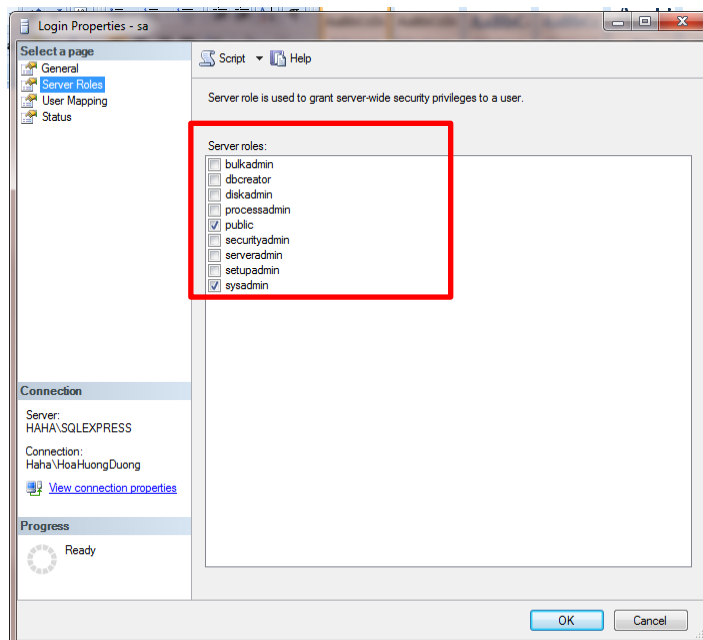
- Vai trò Server mặc định bao gồm những người dùng quản trị Server

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.

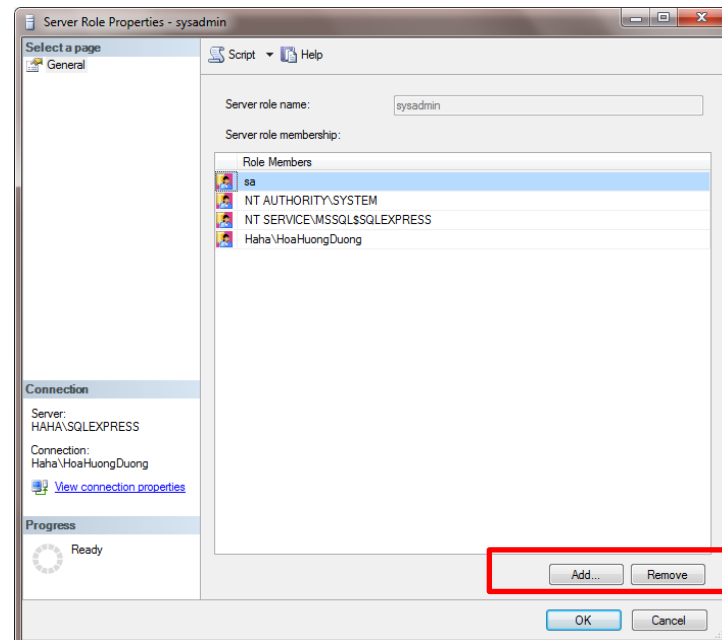
Vai trò	Mô tả
Db_owner	Có tất cả các quyền đối với CSDL
Db_accessadmin	Có quyền thêm hoặc xóa một LoginID của CSDL
Db_securityadmin	Có thể quản trị quyền đối tượng, quyền CSDL, Vai trò, các thành viên của Vai trò
Db_datawriter	Có thể thêm, xóa, cập nhật dữ liệu trên toàn bộ các bảng trong CSDL
Db_datareader	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

Hai cách gán vai trò Server cho một Login ID

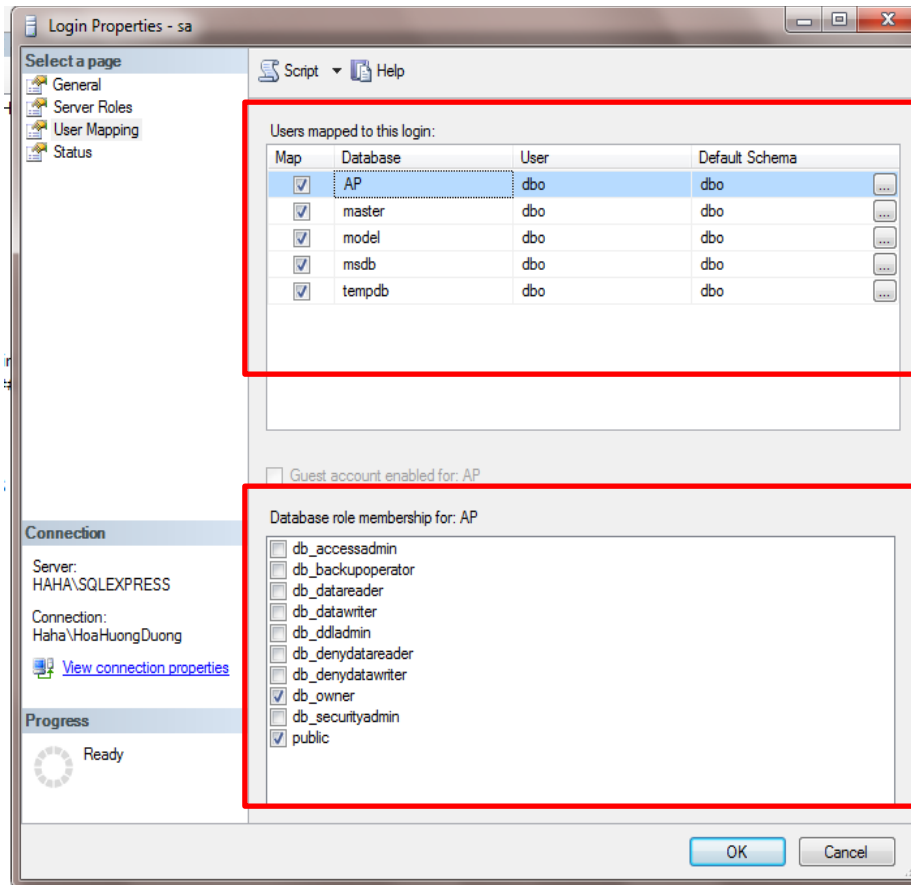
- Sử dụng trang **Server Role Properties** để chọn và gán vai trò Server cho một Login ID



- Sử dụng **Server Role Properties** để thêm Login ID vào danh sách thành viên của vai trò Server



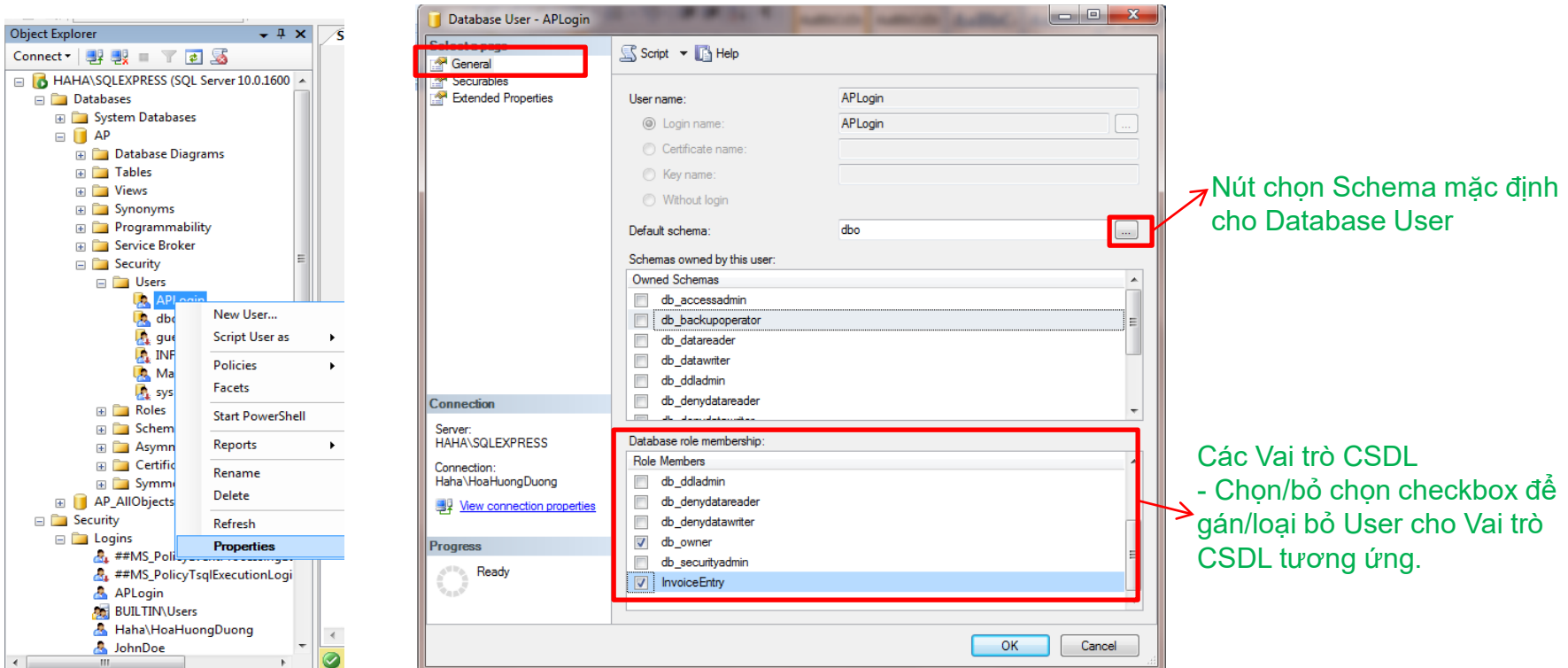
Gán vai trò CSDL cho Login ID



Danh sách tất cả CSDL trên Server
- Chọn/bỏ chọn các checkbox để cấp quyền truy cập CSDL cho LoginID

Danh sách tất cả các Vai trò CSDL của dòng CSDL đang được chọn
- Chọn/bỏ chọn checkbox để thêm Login ID vào các Vai trò

Gán Vai trò CSDL cho một Database User

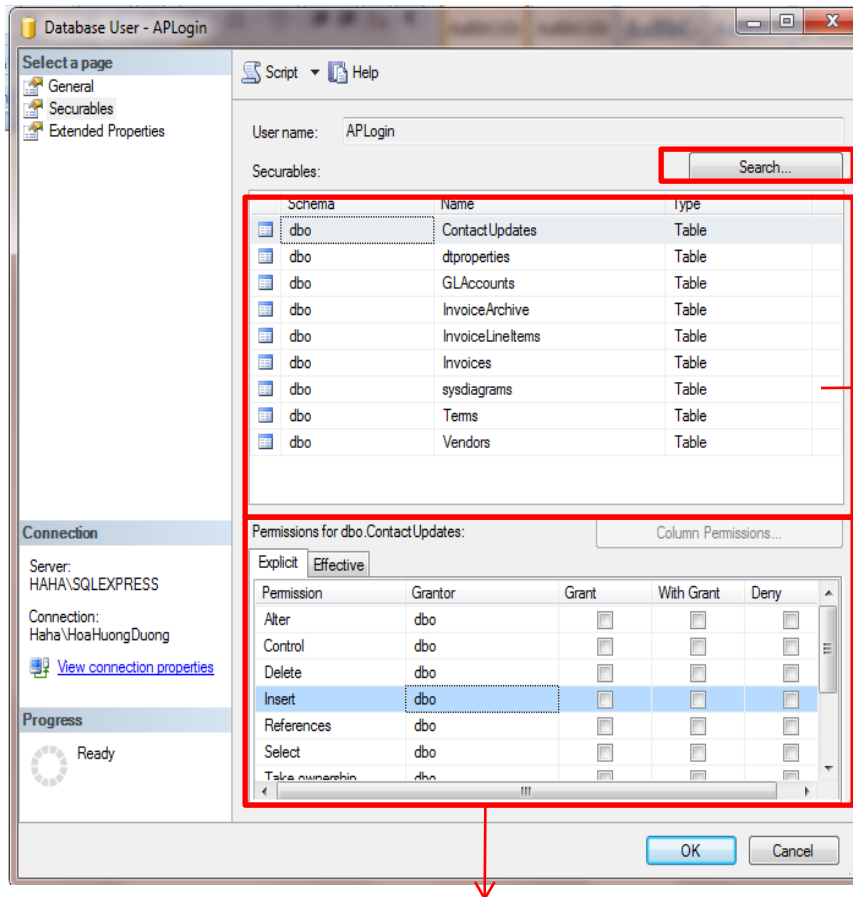


The screenshot shows the 'Database User - APLogin' properties dialog in SQL Server Enterprise Manager. The 'General' tab is selected. The 'User name' is 'APLogin'. The 'Login name' is 'APLogin'. The 'Default schema' is 'dbo'. The 'Database role membership' section shows a list of roles with checkboxes. The 'db_owner' and 'db_securityadmin' roles are checked. The 'db_datareader' and 'db_datawriter' roles are unchecked. The 'db_accessadmin' and 'db_backupoperator' roles are also unchecked. The 'db_denydatareader' and 'db_denydatawriter' roles are unchecked.

Nút chọn Schema mặc định cho Database User

Các Vai trò CSDL - Chọn/bỏ chọn checkbox để gán/loại bỏ User cho Vai trò CSDL tương ứng.

Gán quyền truy cập các đối tượng CSDL cho một Login ID



Click vào đây để thêm các thực thể có thể bảo mật vào danh sách bên dưới

Danh sách các thực thể có thể bảo mật

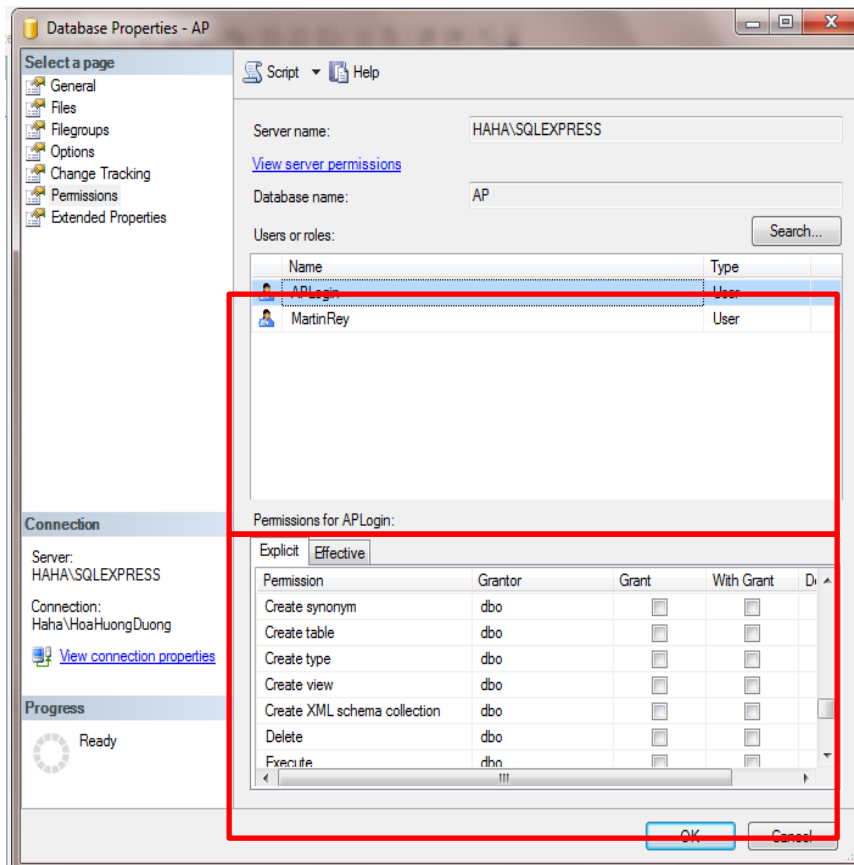
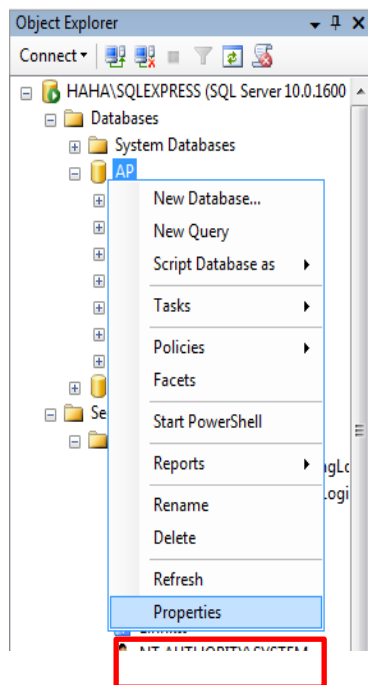
Danh sách các quyền mà User được cấp để làm việc với thực thể có thể bảo mật được chọn trong danh sách ở trên

Chọn/bỏ chọn checkbox Grant: Cấp/thu hồi quyền

Chọn/bỏ chọn checkbox With Grant: Cho phép/không cho phép user cấp quyền cho user khác

Chọn checkbox Deny: Từ chối quyền người dùng trên thực thể có thể bảo mật được chọn

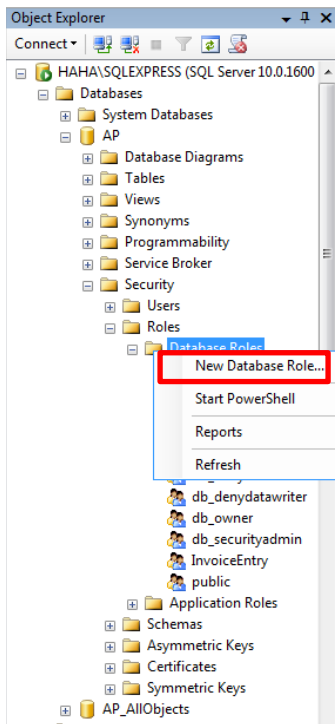
Làm việc với Quyền CSDL



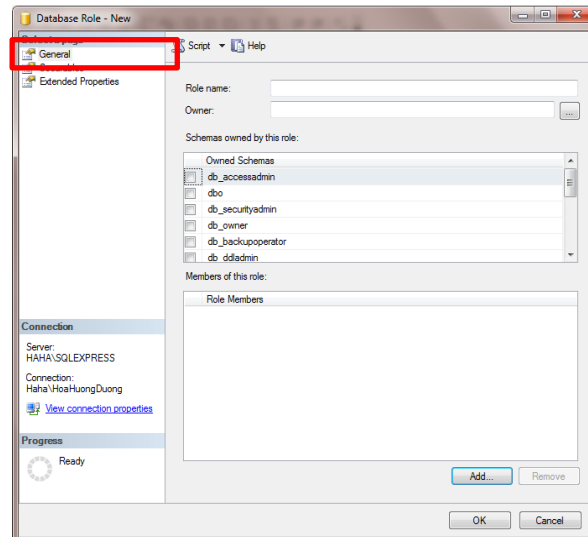
Danh sách user/Vai trò được quyền truy cập CSDL

Danh sách các quyền mà user/Vai trò được chọn được phép thực hiện trên CSDL

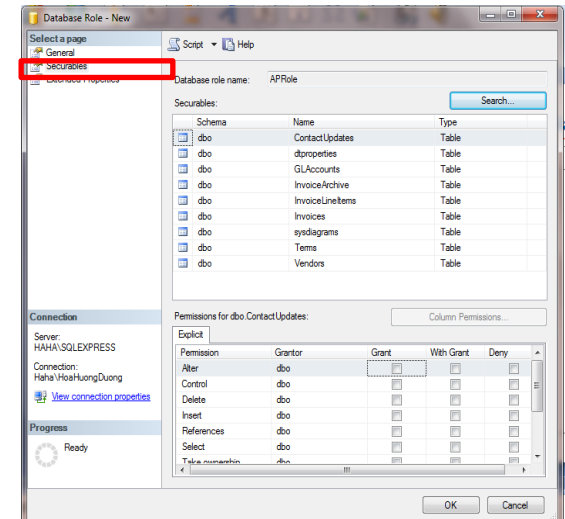
■ Tạo Vai trò tự định nghĩa



Chỉ định schema và các thành viên của Vai trò



Cấp quyền cho Vai trò trên các thực thể có thể bảo mật



■ Cú pháp câu lệnh tạo Vai trò

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

■ Cú pháp câu lệnh xóa Vai trò

```
DROP ROLE role_name
```

■ Ví dụ câu lệnh tạo Vai trò

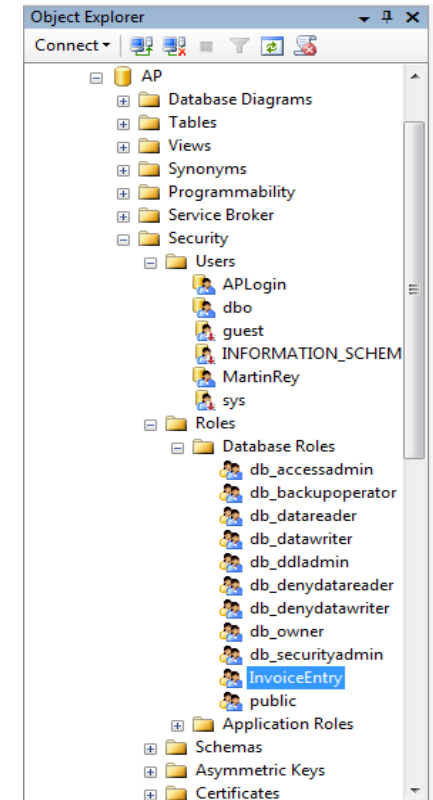
```
CREATE ROLE InvoiceEntry
```

■ Ví dụ câu lệnh cấp quyền cho Vai trò

```
GRANT INSERT, UPDATE
ON Invoices
TO InvoiceEntry
GRANT INSERT, UPDATE
ON InvoiceLineItems
TO InvoiceEntry
```

■ Chú ý:

- Câu lệnh CREATE ROLE sẽ tạo một Vai trò cho cơ sở dữ liệu hiện thời
- Tên Vai trò chứa tối đa 128 ký tự bao gồm các chữ cái, biểu tượng, số và không chứa ký tự \



■ Bảo mật CSDL

- Người dùng kết nối tới SQL Server sử dụng Login ID
- Hai cách SQL Server sử dụng để xác thực người dùng
 - Windows Authentication
 - SQL Server Authentication
- SQL Server dựa vào Quyền, và vai trò cấp cho người dùng để xác định các đối tượng, câu lệnh SQL người dùng được phép tác động trên CSDL
- Quyền: SELECT, UPDATE, DELETE...
- Vai trò: là một tập các quyền để gán cho một người dùng hoặc một nhóm người dùng.

XIN CẢM ƠN!