FPT Education

FPT POLYTECHNIC

caodang.fpt.edu.vn

HỆ QUẢN TRỊ CSDL

BÀI 5: QUẢN LÝ THÔNG TIN ĐĂNG NHẬP, NGƯỜI DÙNG VÀ PHÂN QUYỀN

MỤC TIÊU

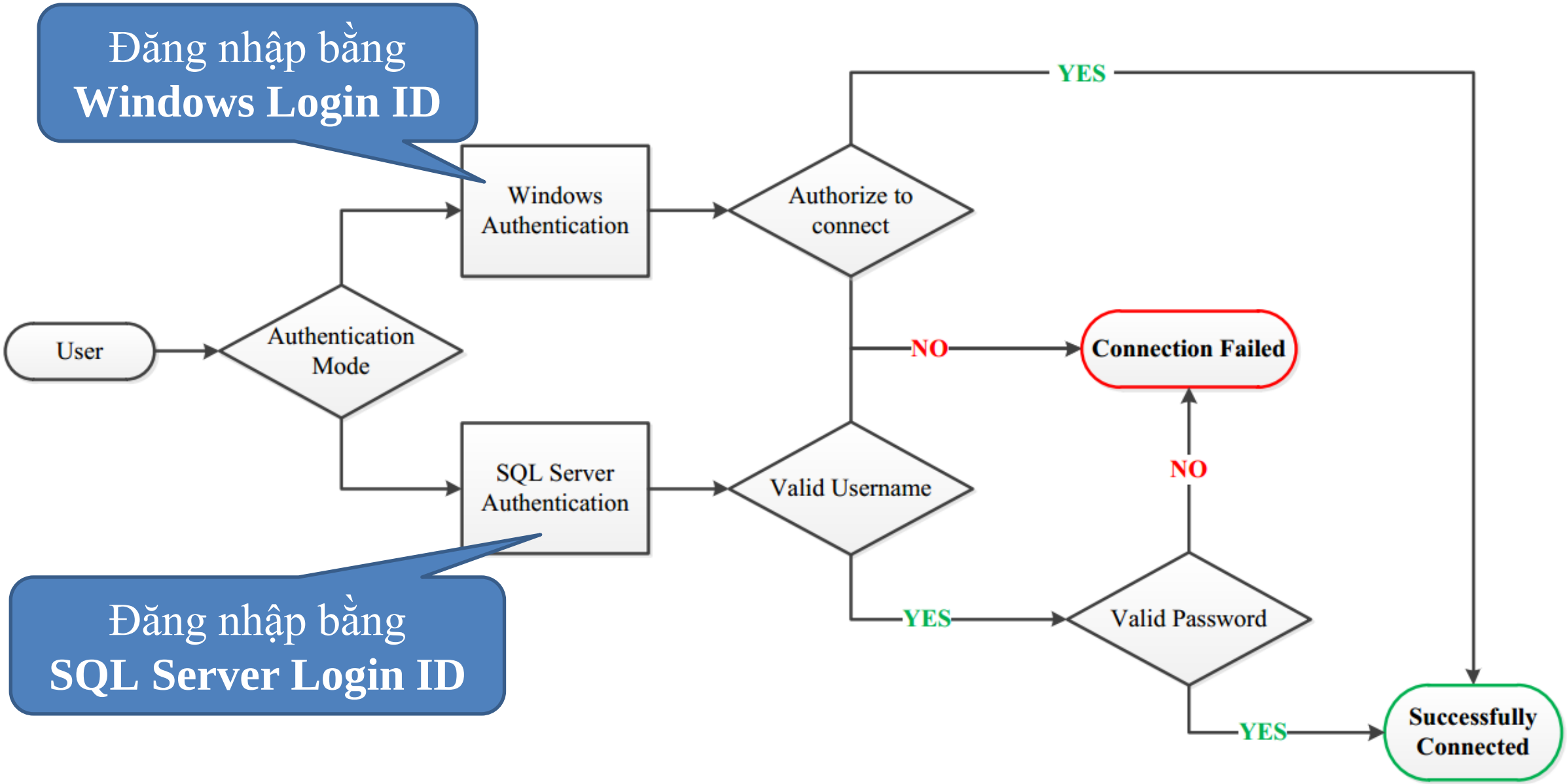
- Quản lý server-level security
- Quản lý Database user và Database Role
- Sử dụng Application Role
- Quản lý Permissions

BÀI 5 PHẦN I

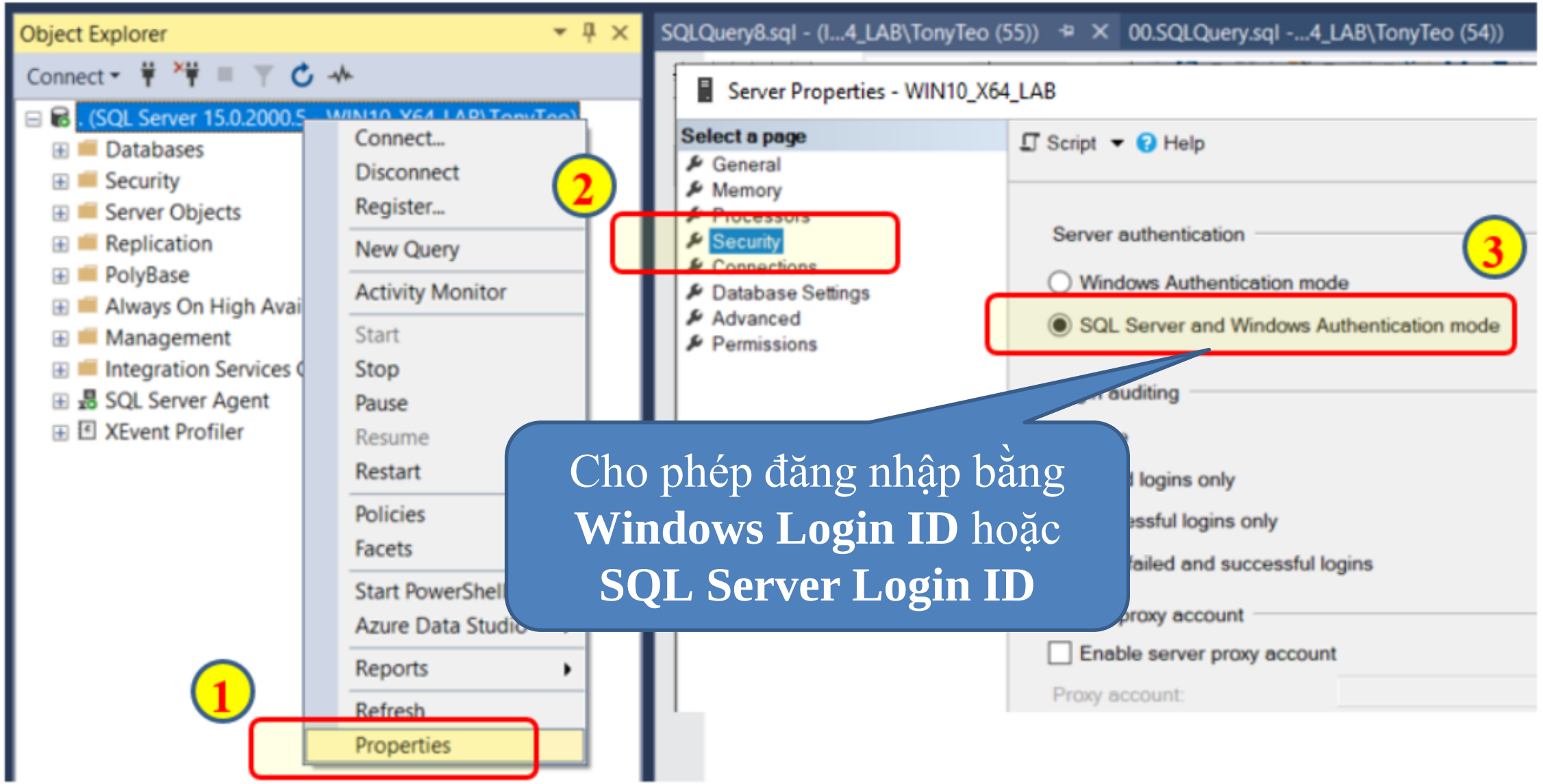
QUẢN LÝ THÔNG TIN ĐĂNG NHẬP

QUẢN LÝ SERVER-LEVEL SECURITY

QUẢN LÝ SERVER-LEVEL SECURITY



CÀI ĐẶT MODE AUTHENTICATION



QUẢN LÝ DATABASE USER

QUẢN LÝ DATABASE USER

- Mỗi CSDL có một danh sách người dùng được xác thực để truy cập đến CSDL đó.

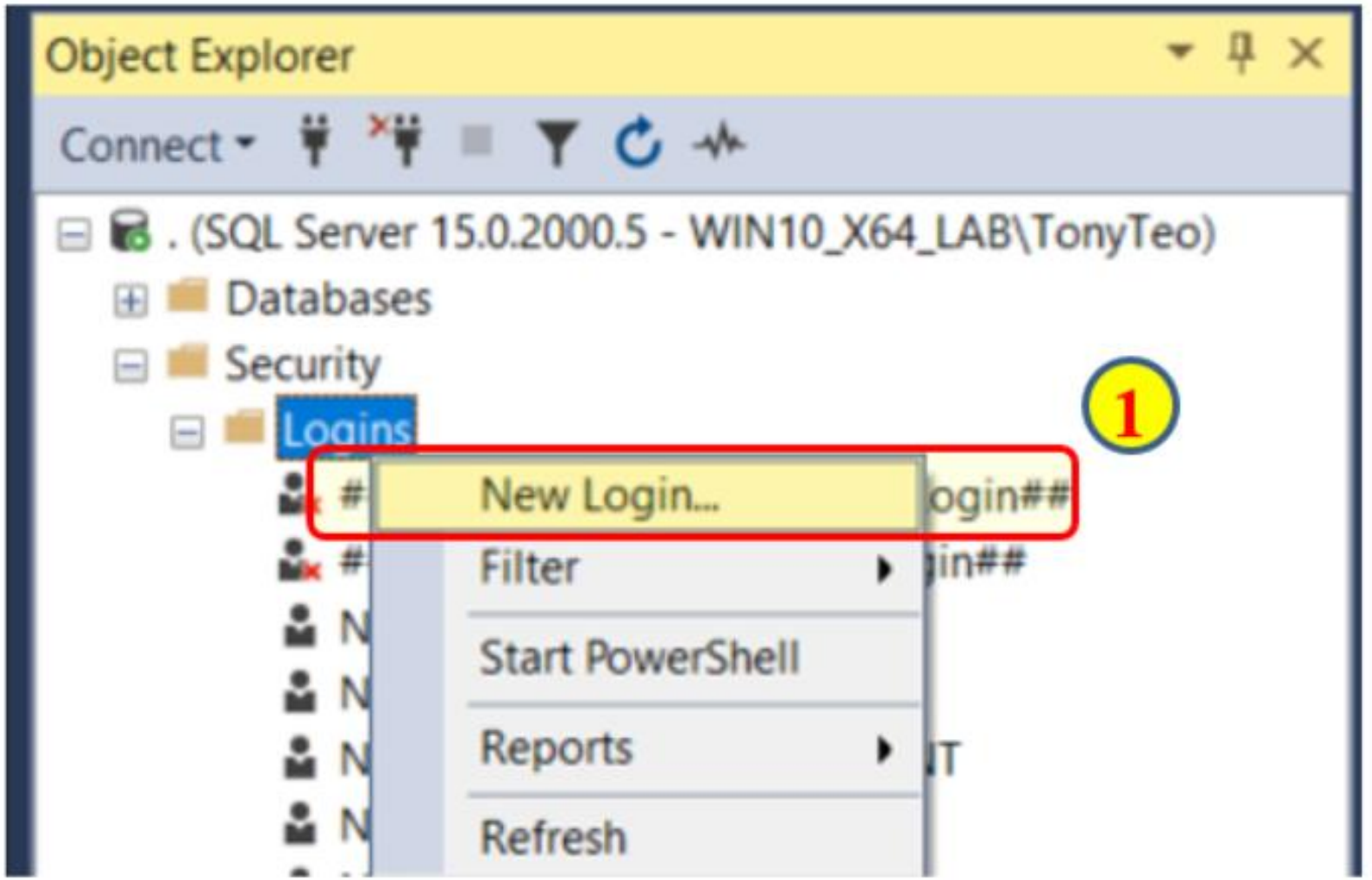
- Khi tạo một database user
  - User chỉ có quyền chọn ngữ cảnh CSDL. Không có quyền thực thi các thao tác trên CSDL và trên các đối tượng của CSDL đó
  - Để có thể thực hiện các thao tác này user phải được cấp quyền đối tượng và quyền CSDL.

TẠO LOGIN ID & TẠO/SỬA XÓA DATABASE USER

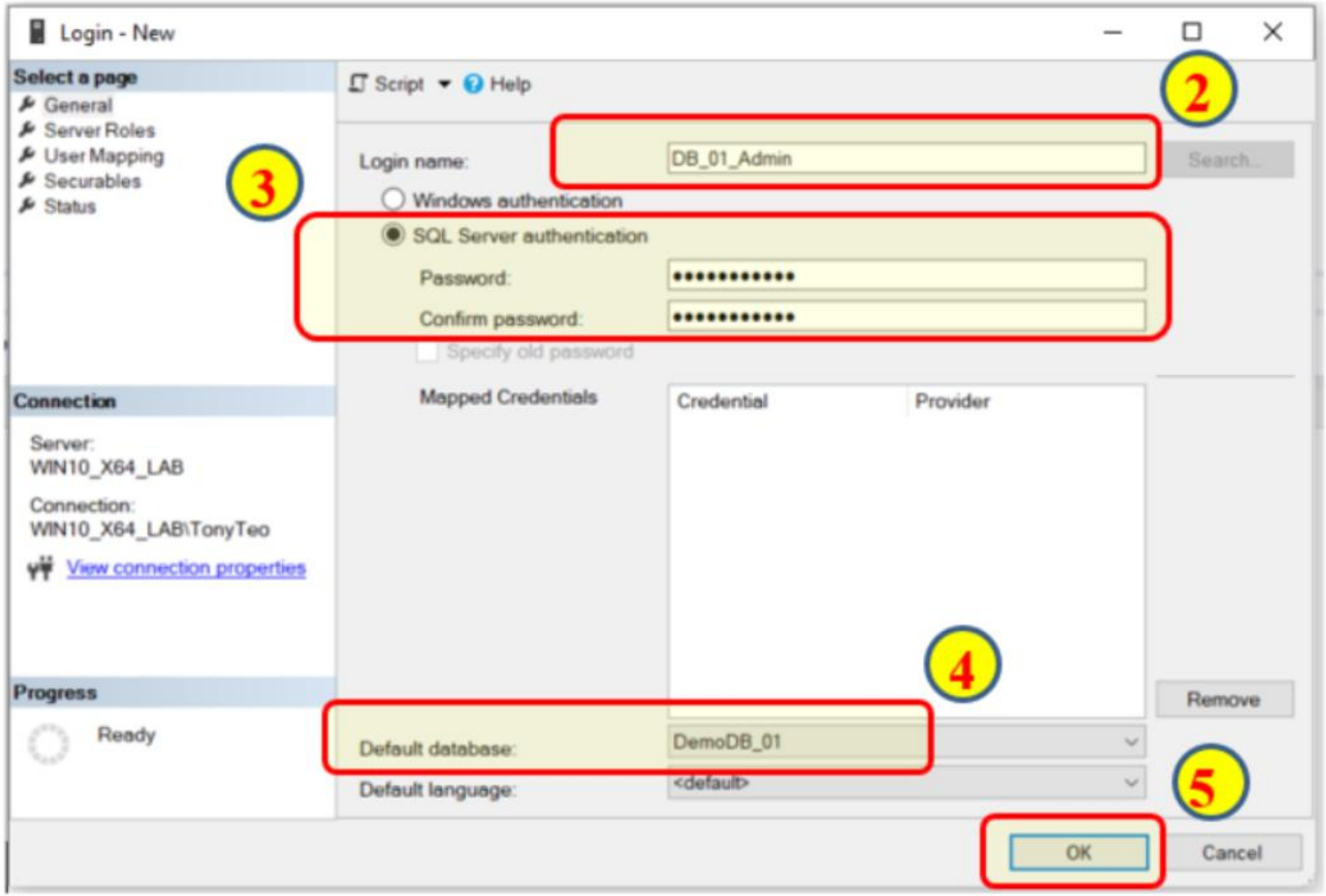
- SQL Server Management Studio (SSMS)
- Transact-SQL (T-SQL)

SQL SERVER MANAGEMENT STUDIO (SSMS)

TẠO LOGIN ID


Object Explorer
Connect
. (SQL Server 15.0.2000.5 - WIN10_X64_LAB\TonyTeo)
Databases
Security
Logins
1
New Login...
Filter
Start PowerShell
Reports
Refresh

TẠO LOGIN ID (TT)

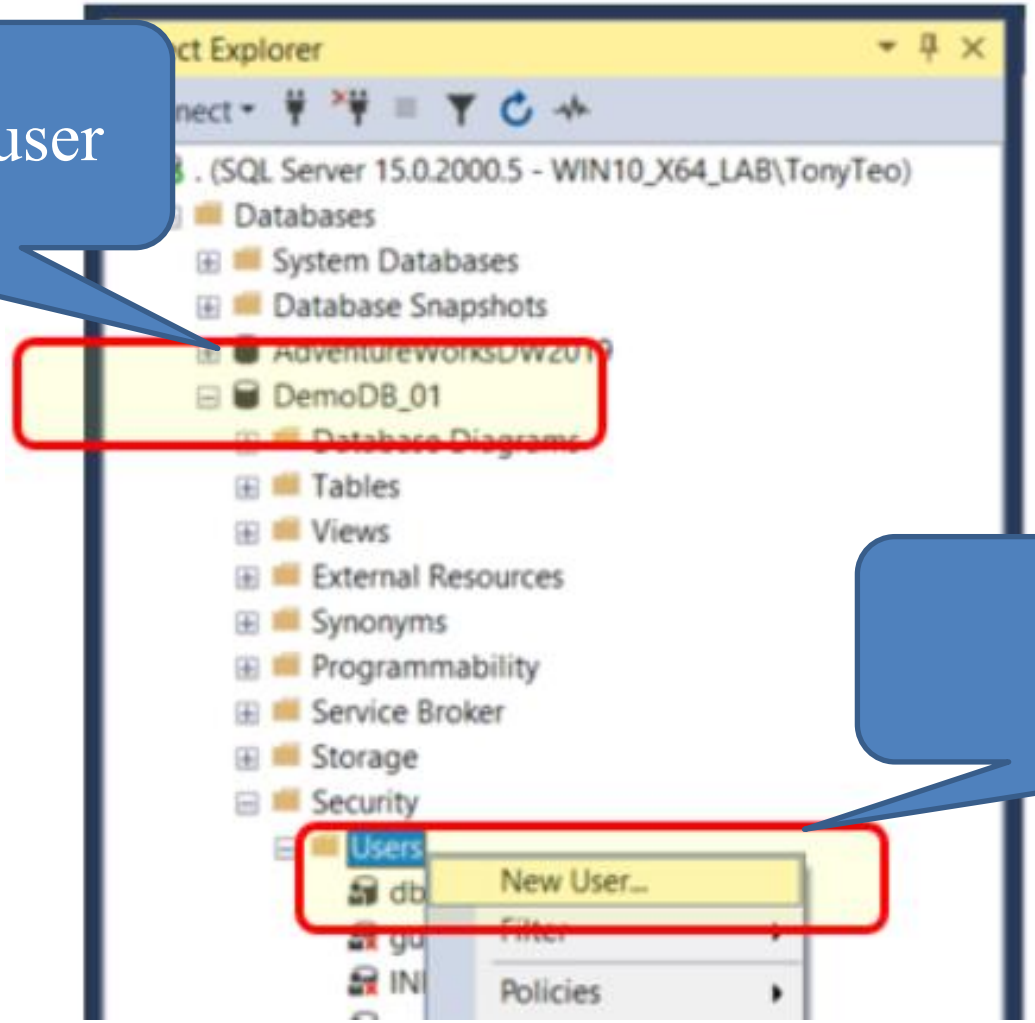


- **Password Complexity:** Độ phức tạp của password
  - Không có nội dung của user
  - Chiều dài ít nhất 8 ký tự
  - Nội dung password bao gồm: Các chữ cái viết thường (a…z), viết hoa (A..Z), số (0…9)
  - KHÔNG CHỨA: dấu chấm than (!), dấu đô la ($), dấu số (#) hoặc phần trăm (%)

- **Password Expiration:** Thời gian hết hạn của password

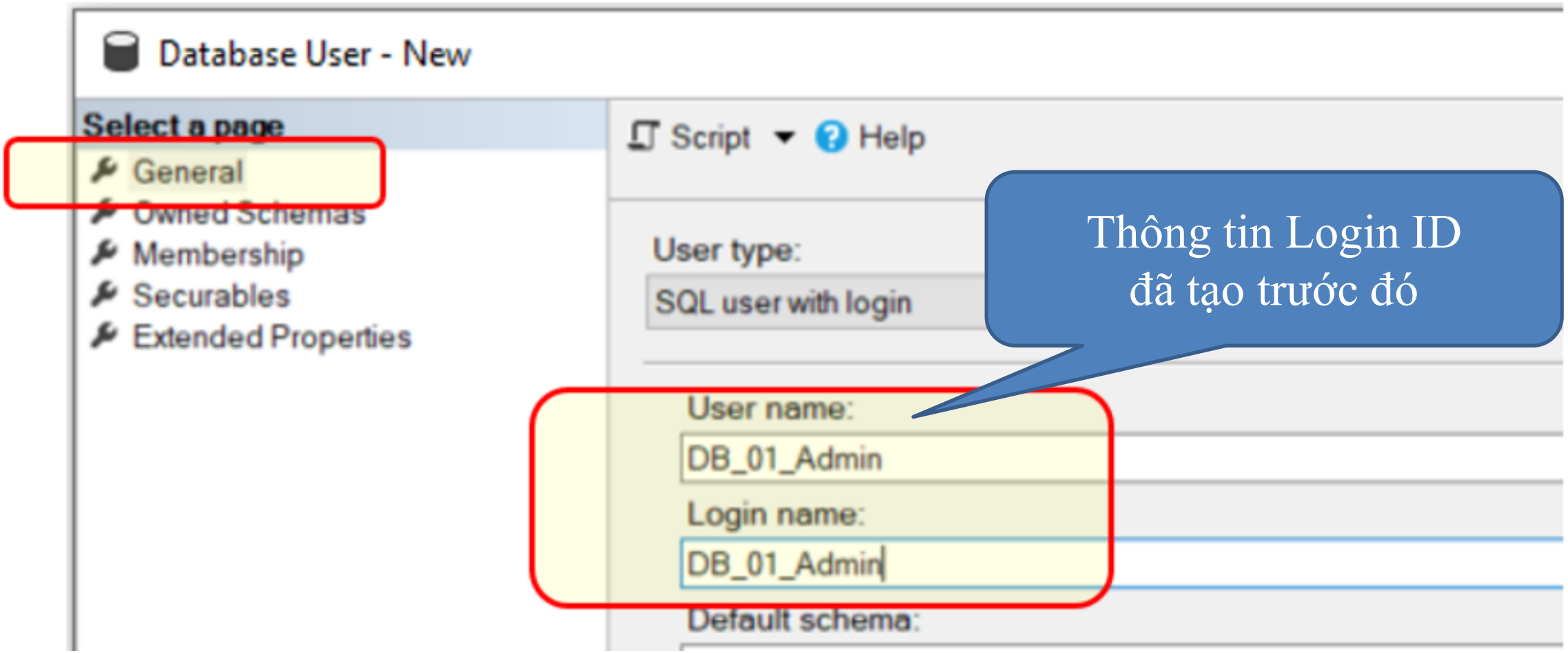
TẠO MỚI DATABASE USER

Chọn Database cần tạo user



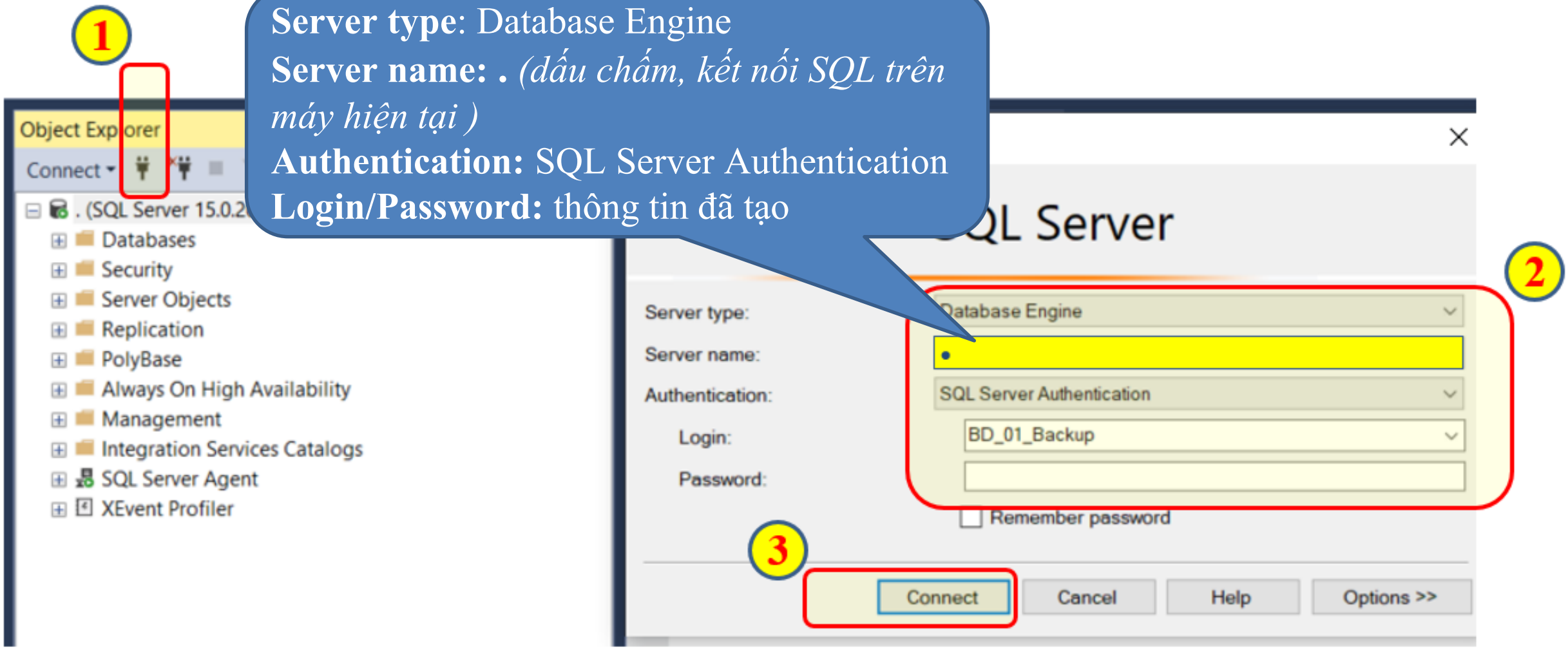
Tạo mới User

TẠO MỚI DATABASE USER (TT)



DÙNG SSMS ĐỂ KẾT NỐI DATABASE TRÊN MÁY HIỆN TẠI

Server type: Database Engine
Server name: . *(dấu chấm, kết nối SQL trên máy hiện tại)*
Authentication: SQL Server Authentication
Login/Password: thông tin đã tạo



Ví dụ - Tạo mới Login ID & Database User bằng T-SQL

```
USE master;
GO

CREATE LOGIN DB_01_UserThuong
    WITH PASSWORD = 'DB_01_UserThuong',
    CHECK_POLICY = OFF, CHECK_EXPIRATION = OFF,
    DEFAULT_DATABASE = DemoDB_01;
GO

CREATE USER DB_01_UserThuong
  FOR LOGIN DB_01_UserThuong
GO
```

TRANSACT-SQL (T-SQL)

TẠO MỚI LOGIN ID BẰNG T-SQL

Cú pháp tạo Login ID

```
CREATE LOGIN  <login_name>
        WITH PASSWORD = password
        [, CHECK_POLICY = {ON | OFF} ]
        [, CHECK_EXPIRATION = {ON | OFF} ]
        [, DEFAULT_DATABASE = database; ]
[ GO ]
```

THAO TÁC DATABASE USER BẰNG T-SQL

Cú pháp tạo Database User

```
CREATE USER  <user_name>
        FOR LOGIN = login_name;
```

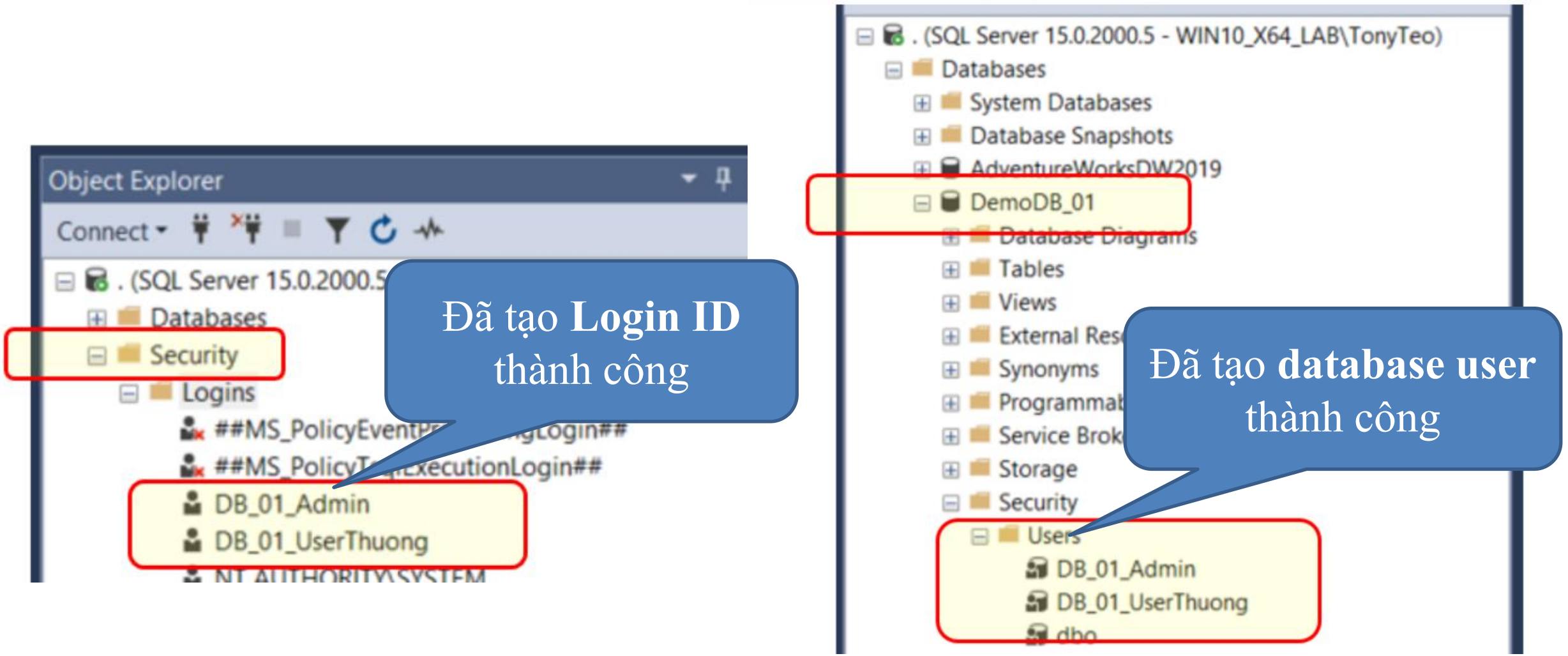
Cú pháp sửa Database User

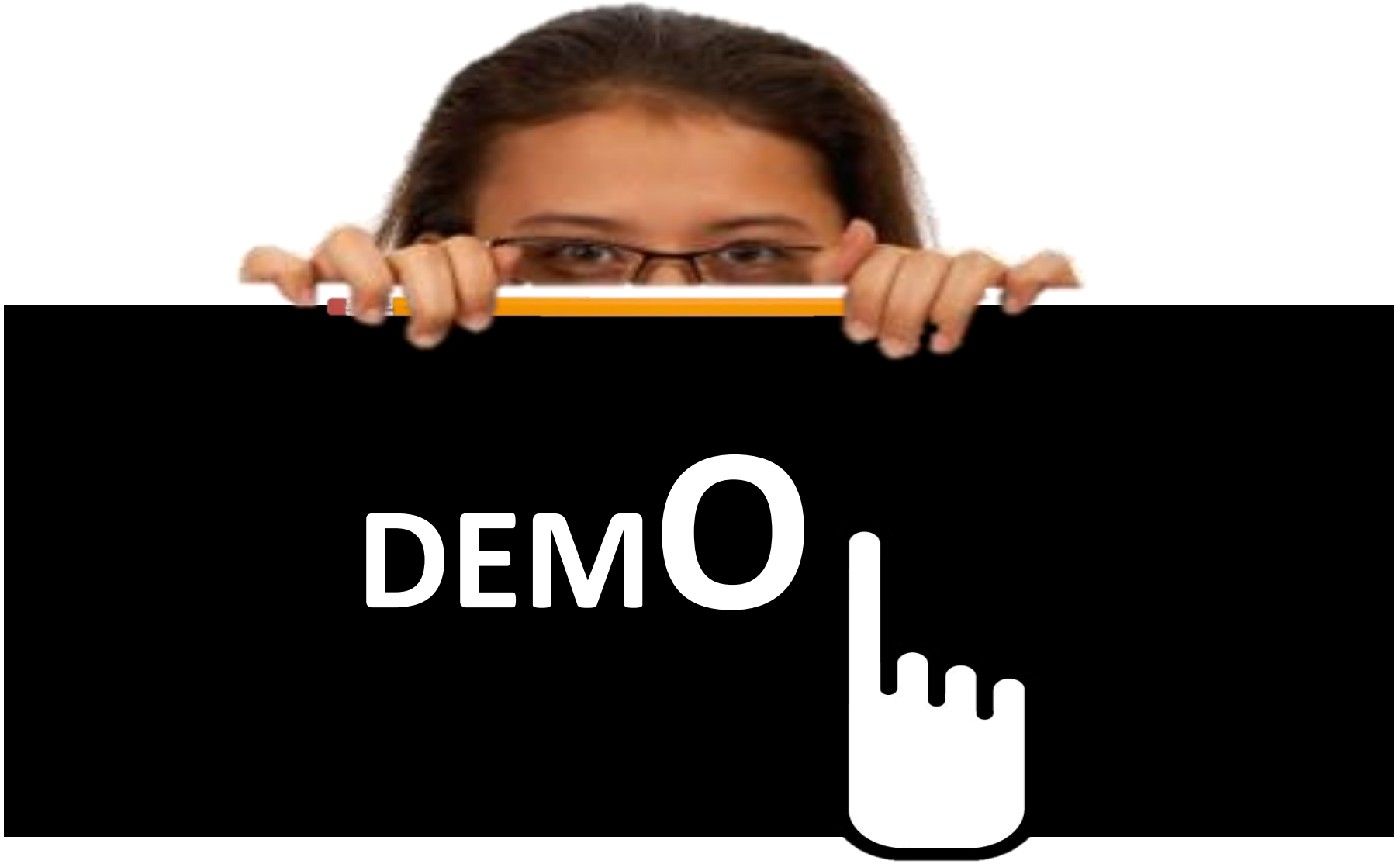
```
ALTER USER  <user_name>
        WITH NAME= new_name;
```

Cú pháp xóa Database User

```
DROP USER  [ IF EXISTS ] <user_name> ;
```

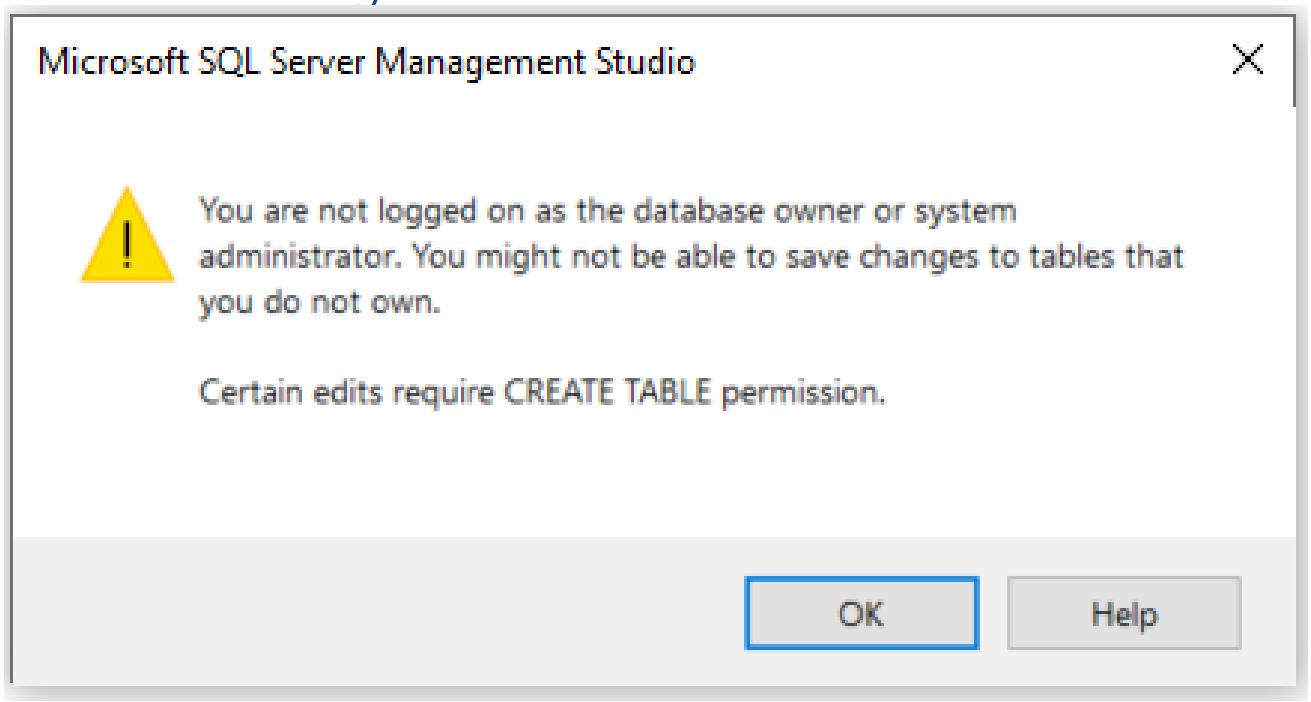
KẾT QUẢ TẠO LOGIN ID & DATABASE USER




DEMO

DEMO

- Tạo mới login và user DB_01_Admin chỉ được phép truy cập CSDL DemoDB_01
- Login với tên vừa tạo và tạo mới bảng dữ liệu và giải thích tại sao có thông báo lỗi này



DATABASE ROLE – VAI TRÒ

DATABASE ROLE – VAI TRÒ

- **Role - Vai trò:** Là một tập các quyền có thể dùng để gán cho một người dùng hoặc một nhóm người dùng.
- **Role - Vai trò mặc định:** SQL Server đã xây dựng sẵn các role mặc định gồm
  - **Server-level roles**: Quản lý các quyền trên Server SQL (như thay đổi cấu hình)
  - **Database-level roles**: Quản lý các quyền trên CSDL như tạo bảng, các câu truy vấn
  - **Application-level roles**: Cho phép các ứng dụng chạy riêng trên quyền của nó.

DATABASE ROLE – VAI TRÒ (TT)

- **Mỗi loại (Server role, CSDL role) SQL cung cấp 2 loại:**
  - **Fixed server roles**: Là các vai trò được xây dựng do SQL Server cung cấp. Các vai trò này có một tập hợp các quyền cố định
    - **Ví dụ:** Vai trò dbcreator có thể thực thi các câu lệnh CREATE/ALTER/DROP DATABASE, RESTORE DATABASE
  - **User-defined roles**: Là các vai trò do người dùng tạo ra để đáp ứng các yêu cầu bảo mật cụ thể.

VAI TRÒ SERVER MẶC ĐỊNH

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

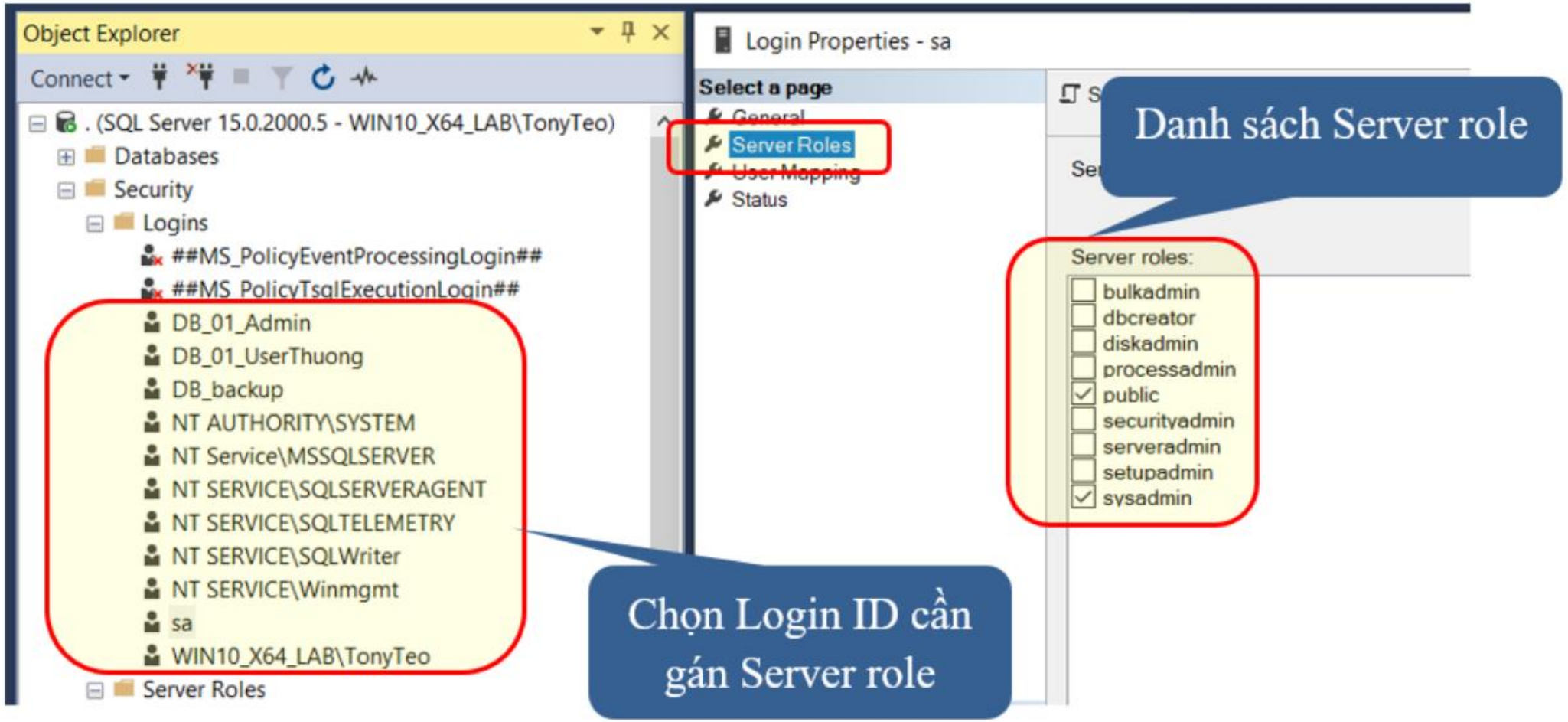
Vai trò	Mô tả
sysadmin	Có thể thực hiện mọi thao tác trên server. Theo mặc định, tất cả thành viên trong nhóm Windows BUILTIN\Administrators đều là thành viên của vai trò này.
securityadmin	Có thể quản lý ID và mật khẩu đăng nhập cho server, đồng thời có thể cấp, từ chối và thu hồi quyền trên cơ sở dữ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

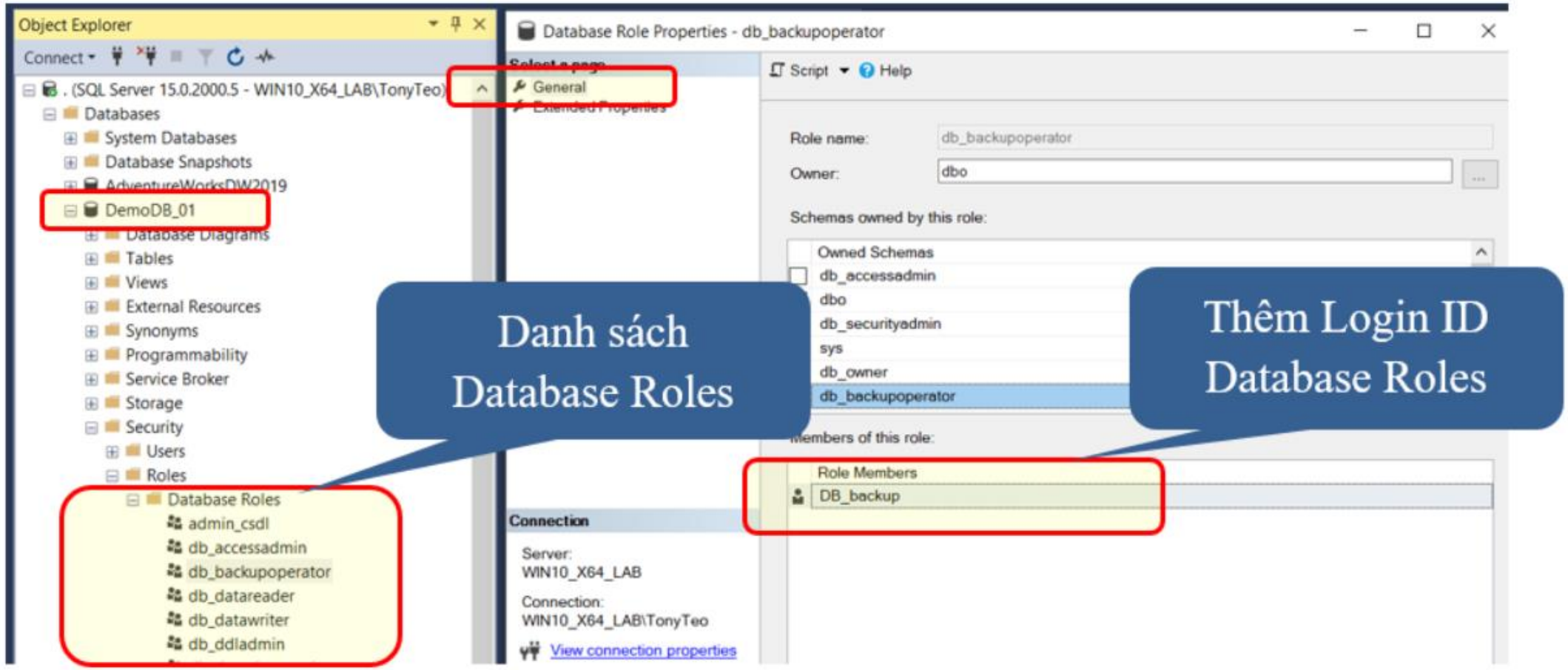
GÁN ROLE – VAI TRÒ CHO LOGIN ID

- Sercurity > Logins > chọn login ID > Property > Server Roles > chọn server role cần gán



THÊM LOGIN ID VÀO DATABASE ROLES

- Databases > chọn CSDL > Sercurity > Roles > Database Roles > chọn database roles cần thêm thành viên -> property > general > add (thêm thành viên)



THAO TÁC ROLES BẰNG T-SQL

Cú pháp tạo Role

```
CREATE ROLE <role_name>;
```

Cú pháp thêm thành viên vào Role

```
ALTER ROLE <role_name>
        ADD MEMBER database_principal;
```

- **database_principal:** là database user hoặc là database role người dùng định nghĩa

Cú pháp xóa Role

```
DROP ROLE  [ IF EXISTS ] < role_name > ;
```

THÊM LOGIN ID VÀO DATABASE ROLES BẰNG T-SQL

- Ví dụ: Tạo mới Login ID tên BD_backup và điều chỉnh cho login ID này chỉ được phép backup CSDL DemoDB_01

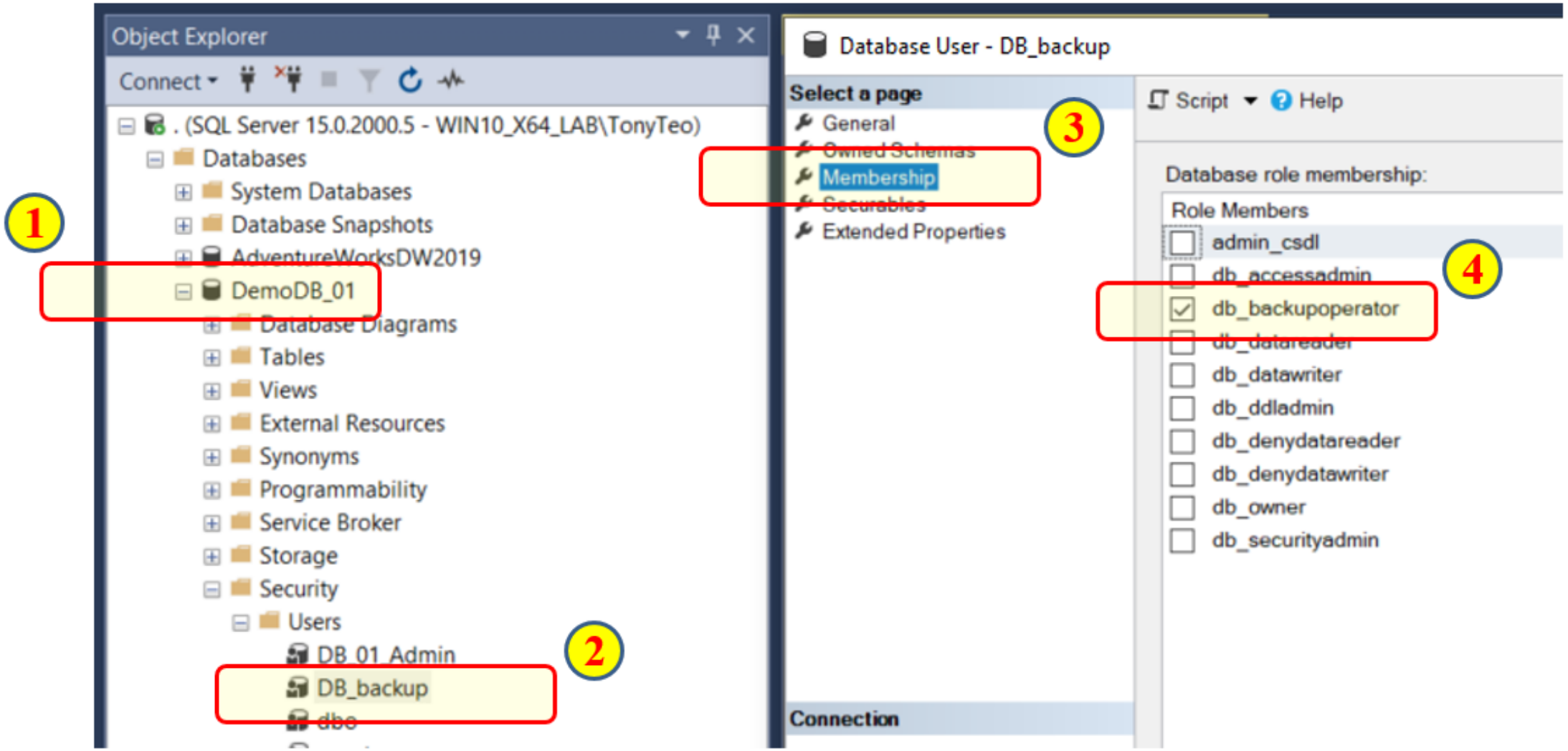
```
USE master
GO
CREATE LOGIN DB_backup
    WITH PASSWORD=N'DB_backup',
    CHECK_EXPIRATION=OFF,
    CHECK_POLICY=OFF
GO
```

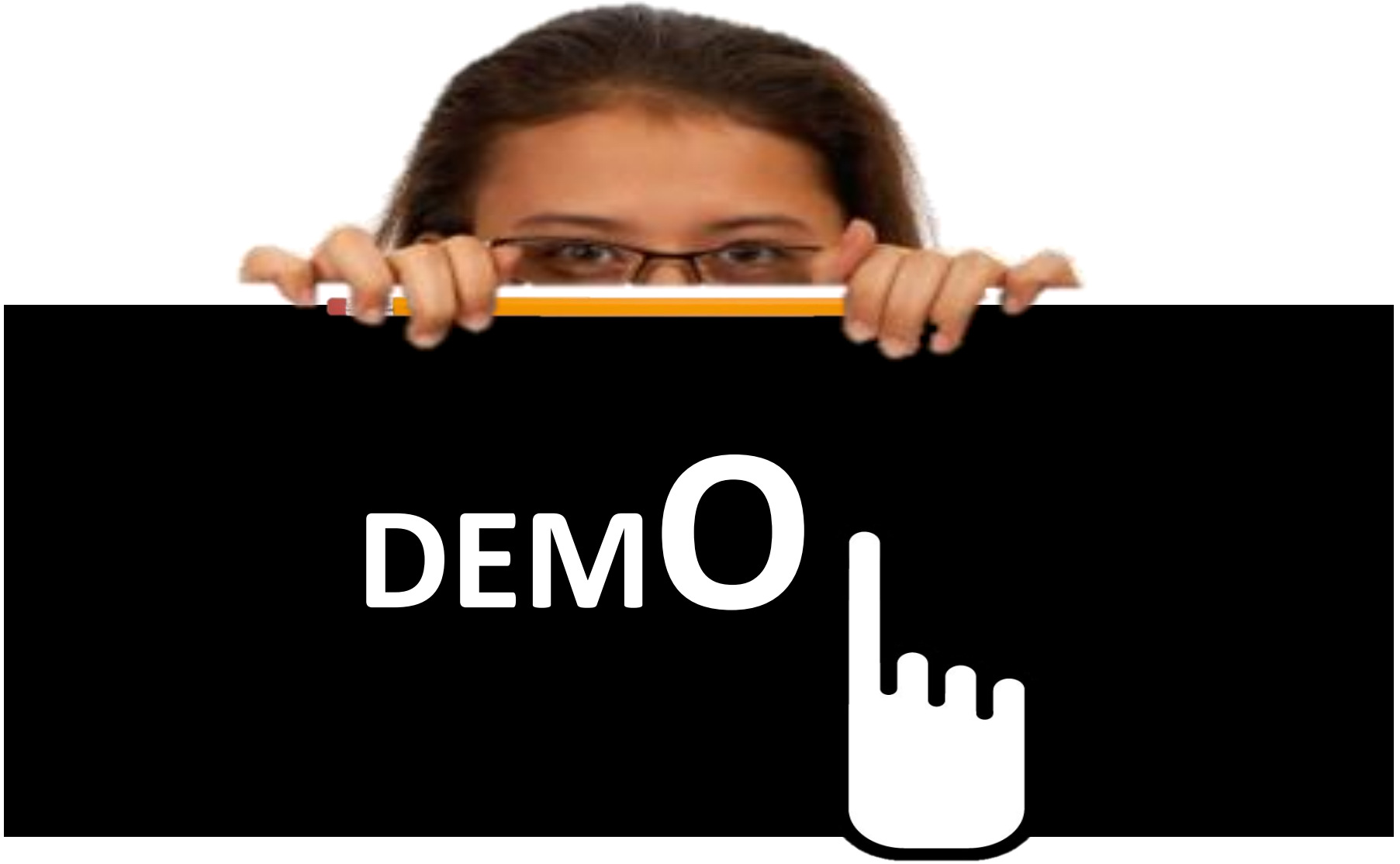
```
USE DemoDB_01
GO
CREATE USER DB_backup
    FOR LOGIN DB_backup
GO
```

```
ALTER ROLE db_backupoperator
    ADD MEMBER DB_backup
GO
```

DATABASE ROLE MEMBERSHIP

❑ Kiểm tra user là thành viên của database role




DEMO

DEMO

- Tạo mới login và user DB_01_Admin chỉ được phép truy cập CSDL DemoDB_01 (nếu user đã tồn tại không cần tạo), thêm user DB_01_Admin vào database role **db_owner** (toàn quyền trên CSDL DemoDB_01)

- Tạo mới login và user DB_backup chỉ được phép truy cập CSDL DemoDB_01 và gán quyền sao user này chỉ được phép thực hiện backup CSDL (không thực hiện được các thao tác khác)

BÀI 5 PHẦN II

PHÂN QUYỀN – PERMISSION

SỬ DỤNG APPLICATION ROLE

SỬ DỤNG APPLICATION ROLE

- Cho phép các ứng dụng thực thi trên cơ sở dữ liệu, giống như một user với các quyền hạn được gán. Ta có thể sử dụng Application roles để cho phép truy cập tới các dữ liệu riêng biệt mà chỉ có một số user mới có quyền kết nối đến thông qua Application.

QUẢN LÝ PERMISSIONS

CÁC QUYỀN CHUẨN - QUẢN LÝ PERMISSIONS

❑ 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

GRANT, REVOKE, DENY - QUẢN LÝ PERMISSIONS

- **GRANT**: Là lệnh dùng để cấp pháp quyền thực thi các thao tác hoặc là quyền truy cập đến đối tượng trên SQL Server.
- **REVOKE**: Thu hồi các quyền mà user đã được cấp phát.
- **DENY**: Cấm không cho thực thi các thao tác hoặc truy cập đến một đối tượng nào đó

❑ Cú pháp cấp quyền cơ bản

```
GRANT permissions
ON securable TO principal;
```

- ❖ Nếu cấp nhiều permission thì mỗi quyền các nhau bằng dấu phẩy ","
- ❖ **Ví dụ:** cho phép user "DB_01_UserThuong" thấy bảng dữ liệu "Customer" và chỉ được phép thực hiện các câu lệnh **select, insert** trên bảng này.

```
USE AdventureWorks2019
GO

GRANT SELECT, INSERT
ON Customer TO DB_01_UserThuong;
GO
```

❑ Cú pháp thu hồi quyền đã cấp

```
REVOKE permissions
ON securable
FROM principal;
```

❖ **Ví dụ:** Thu hồi quyền insert của user "DB_01_UserThuong" trên bảng "DimCustomer"

```
USE AdventureWorks2019
GO
REVOKE INSERT
ON Customer
FROM DB_01_UserThuong;
GO
```

❑ Cú pháp cấm thực thi

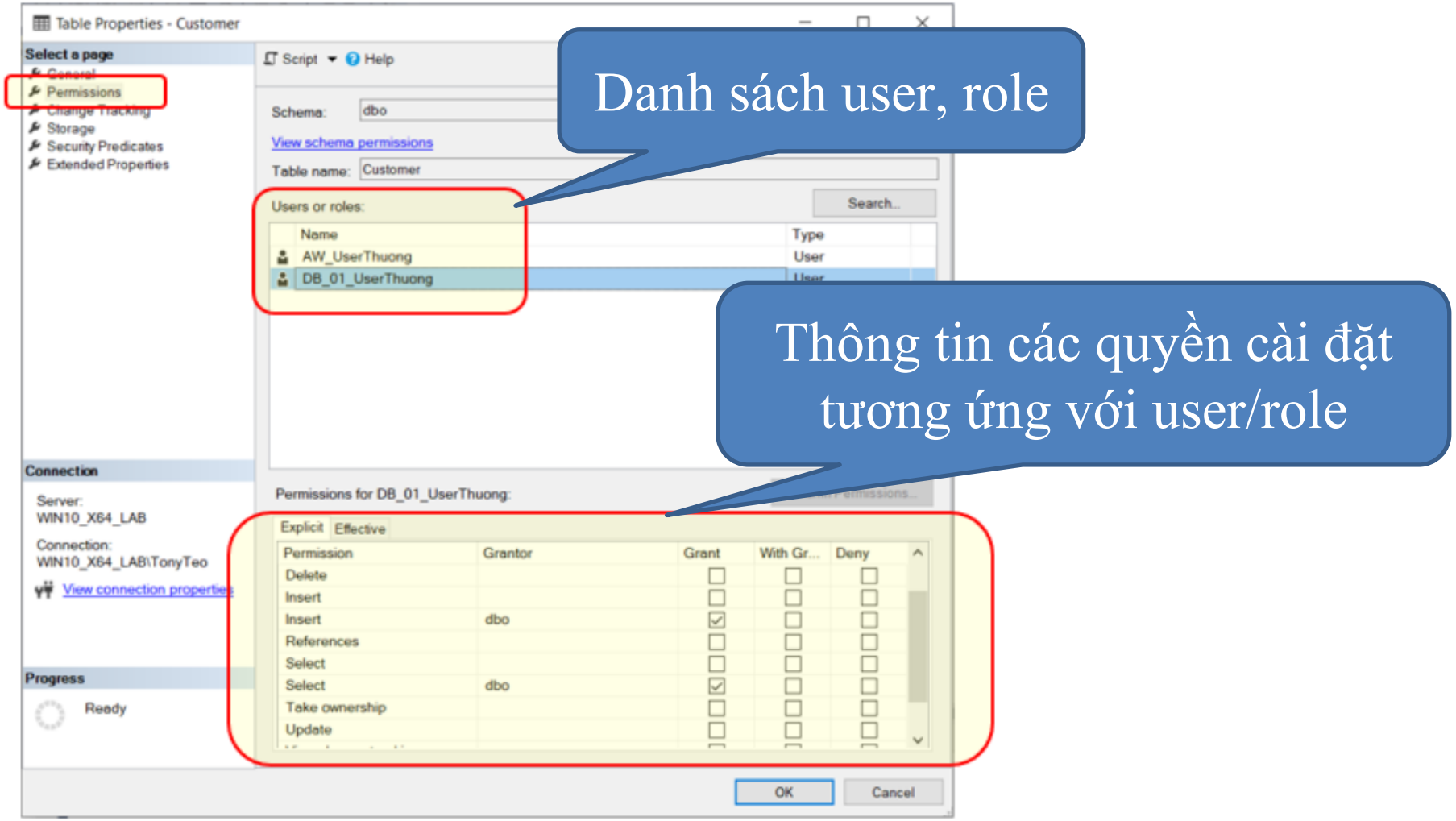
```
DENY permissions
ON securable TO principal;
```

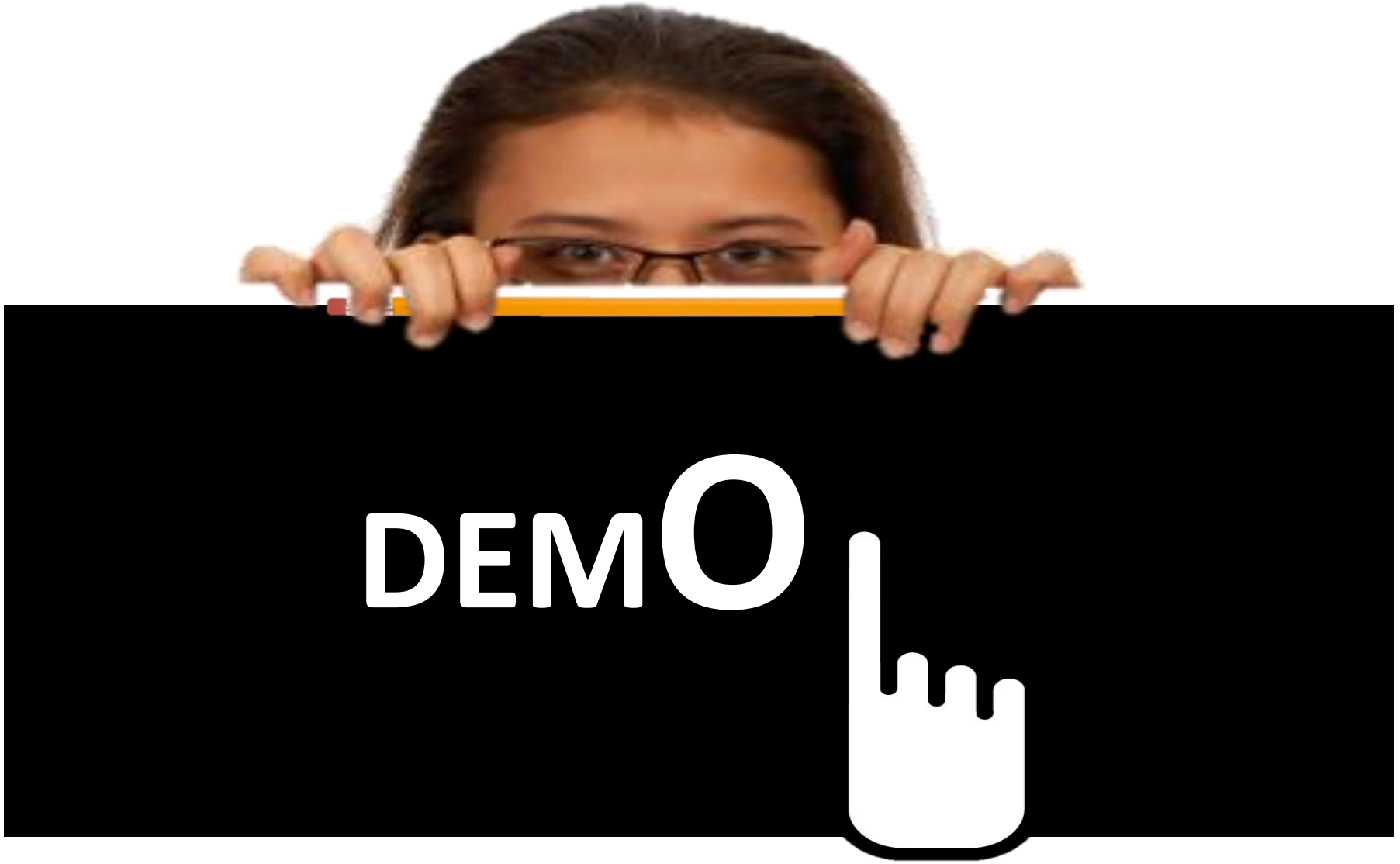
- ❖ **Ví dụ:** Cấm user "DB_01_UserThuong" thực câu lệnh delete trên bảng dữ liệu "Customer"

```
USE AdventureWorks2019
GO
DENY DELETE
ON Customer TO DB_01_UserThuong
GO
```

KIỂM TRA CÁC QUYỀN CÀI ĐẶT

- Chọn bảng dữ liệu cần kiểm tra > property > chọn user cần xem > Explicit




DEMO

- Tạo mới login, user DB_AW_UserThuong chỉ được phép truy cập CSDL AdventureWorks2019

- Cấp quyền cho user "DB_AW_UserThuong" thấy bảng dữ liệu "Customer" và chỉ được phép thực hiện các câu lệnh **select, insert** trên bảng này

- Thu hồi quyền insert của user "DB_AW_UserThuong" trên bảng "Customer"

TÓM TẮT BÀI HỌC

- ☑ Thay đổi mode authentication
- ☑ Quản lý server-level security
- ☑ Quản lý Database user và Database Role
- ☑ Sử dụng Application Role
- ☑ Quản lý Permissions


FPT Education
FPT POLYTECHNIC
Thank you
TIN HỌC VĂN PHÒNG QUỐC TẾ THEO CHUẨN ICDL
Syllabus 5 - Office 2007
LUẬT KINH TẾ
KỸ THUẬT SOẠN THẢO VÀ TRÌNH BÀY VĂN BẢN