



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

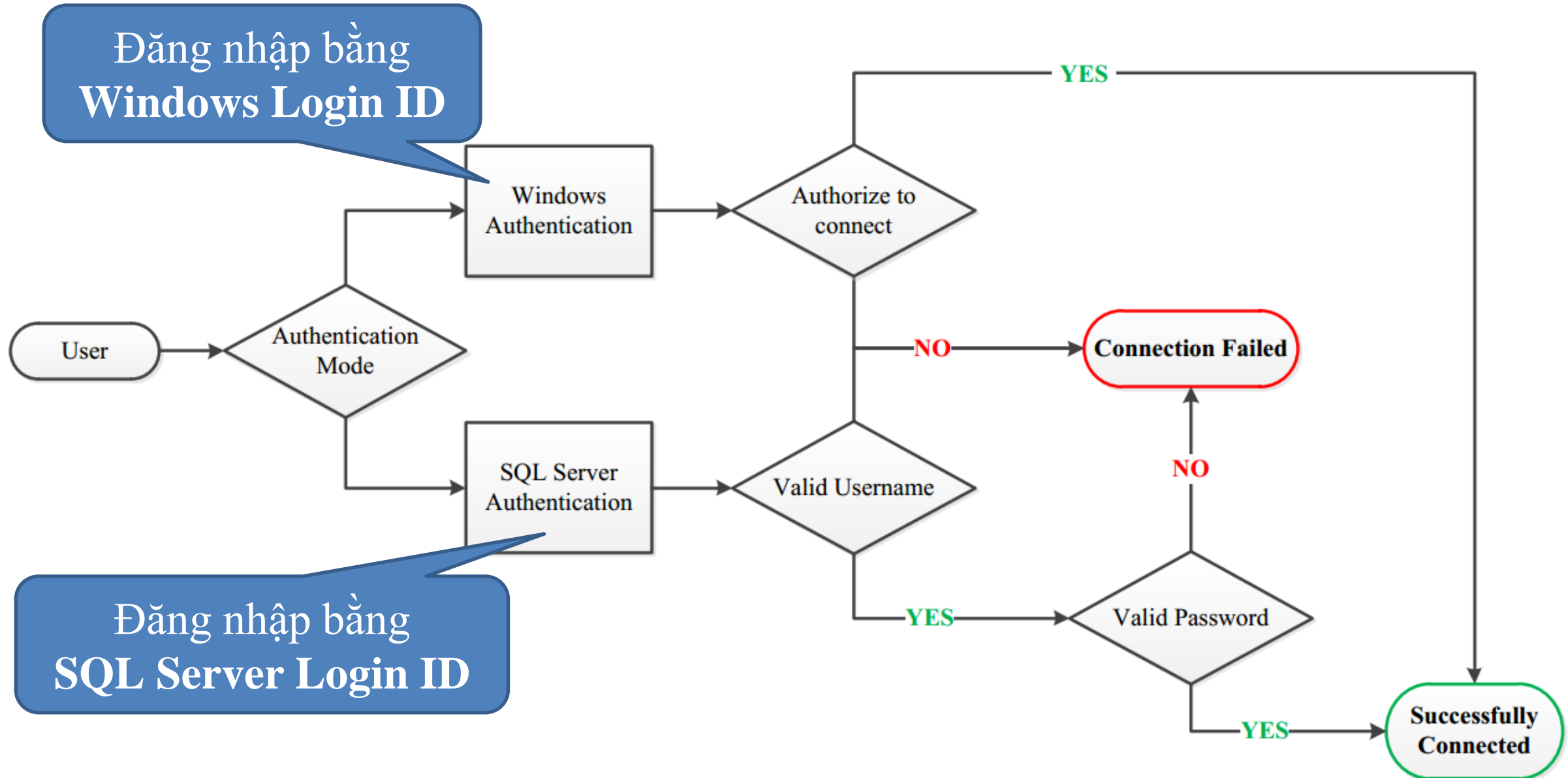




BÀI 5 PHẦN I

QUẢN LÝ THÔNG TIN ĐĂNG NHẬP

QUẢN LÝ SERVER-LEVEL SECURITY



CÀI ĐẶT MODE AUTHENTICATION

The screenshot shows the SQL Server Enterprise Manager interface. On the left, the 'Object Explorer' pane displays a tree view of server components. A context menu is open over the server instance, with the 'Properties' option highlighted at the bottom (marked with a red box and a yellow circle with the number 1). In the center, the 'Server Properties' dialog box is open, showing the 'Security' page (marked with a red box and a yellow circle with the number 2). Under the 'Server authentication' section, the 'SQL Server and Windows Authentication mode' radio button is selected (marked with a red box and a yellow circle with the number 3). A blue speech bubble points to this selected option, containing the text: 'Cho phép đăng nhập bằng Windows Login ID hoặc SQL Server Login ID'.

Object Explorer

Connect ▾

(SQL Server 15.0.2000.5 - WIN10_X64_LAB\TonyTeo)

Databases

Security

Server Objects

Replication

PolyBase

Always On High Avail

Management

Integration Services C

SQL Server Agent

XEvent Profiler

Connect...

Disconnect

Register...

New Query

Activity Monitor

Start

Stop

Pause

Resume

Restart

Policies

Facets

Start PowerShell

Azure Data Studio

Reports

Refresh

Properties

Server Properties - WIN10_X64_LAB

Select a page

General

Memory

Processors

Security

Connections

Database Settings

Advanced

Permissions

Script ▾ ? Help

Server authentication

☐ Windows Authentication mode

☒ SQL Server and Windows Authentication mode

SQL Server and Windows Authentication mode

logins only

successful logins only

failed and successful logins

proxy account

☐ Enable server proxy account

Proxy account:

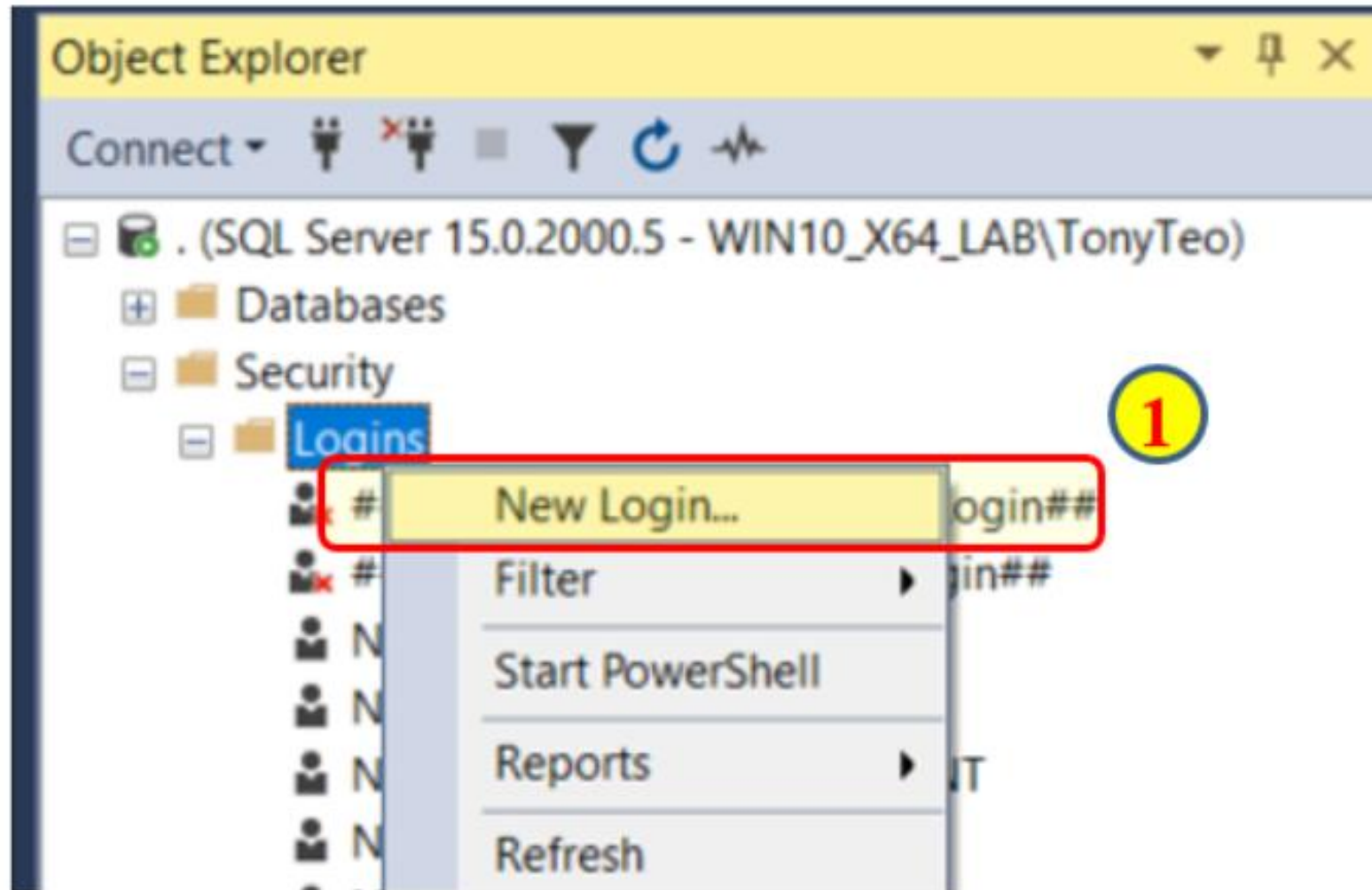
Cho phép đăng nhập bằng
Windows Login ID hoặc
SQL Server Login ID

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.

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

SQL SERVER MANAGEMENT STUDIO (SSMS)



Login - New

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script Help

Login name: DB_01_Admin

Windows authentication

SQL Server authentication

Password:

Confirm password:

Specify old password

Mapped Credentials

Credential	Provider
------------	----------

Server: WIN10_X64_LAB

Connection: WIN10_X64_LAB\TonyTeo

[View connection properties](#)

Progress

Ready

Default database: DemoDB_01

Default language: <default>

Remove

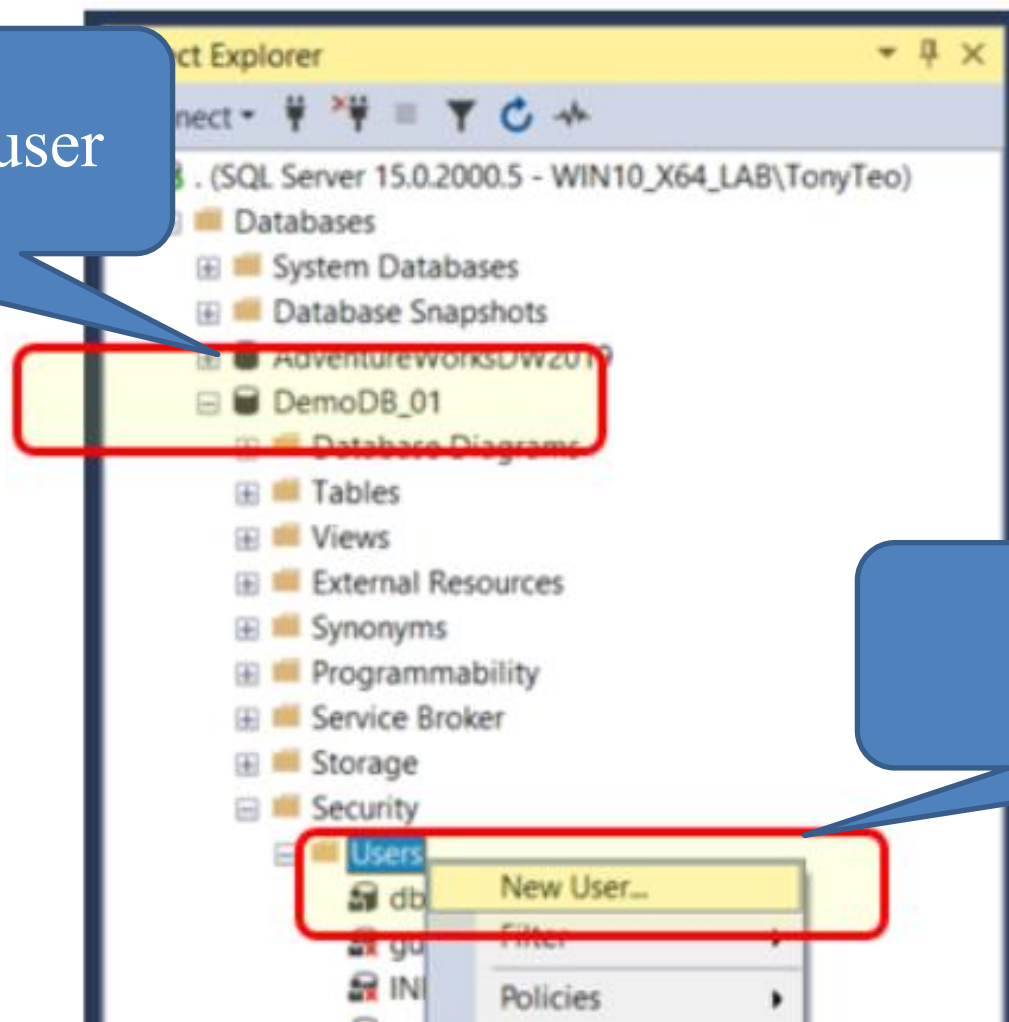
OK Cancel

❑ 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

Chọn Database cần tạo user



Tạo mới User

TẠO MỚI DATABASE USER (TT)

Database User - New

Select a page

- General
- Owned Schemas
- Membership
- Securables
- Extended Properties

Script ▼ ? Help

User type:
SQL user with login

User name:
DB_01_Admin

Login name:
DB_01_Admin

Default schema:

Thông tin Login ID đã tạo trước đó

1

2

3

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

Connect Cancel Help Options >>

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
```

TRANSACTION-SQL (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 ]
```

❑ Cú pháp tạo Database User

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

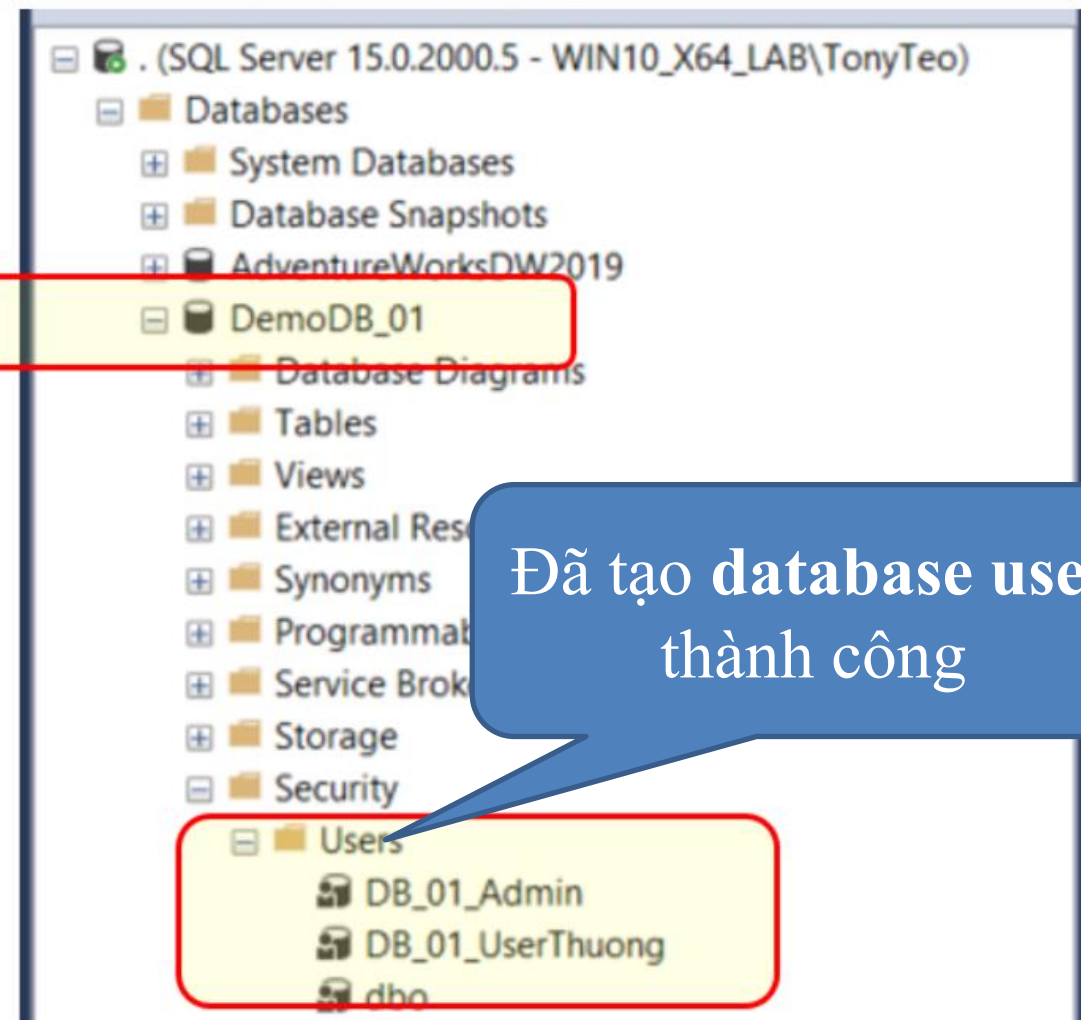
❑ Cú pháp sửa Database User

```
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

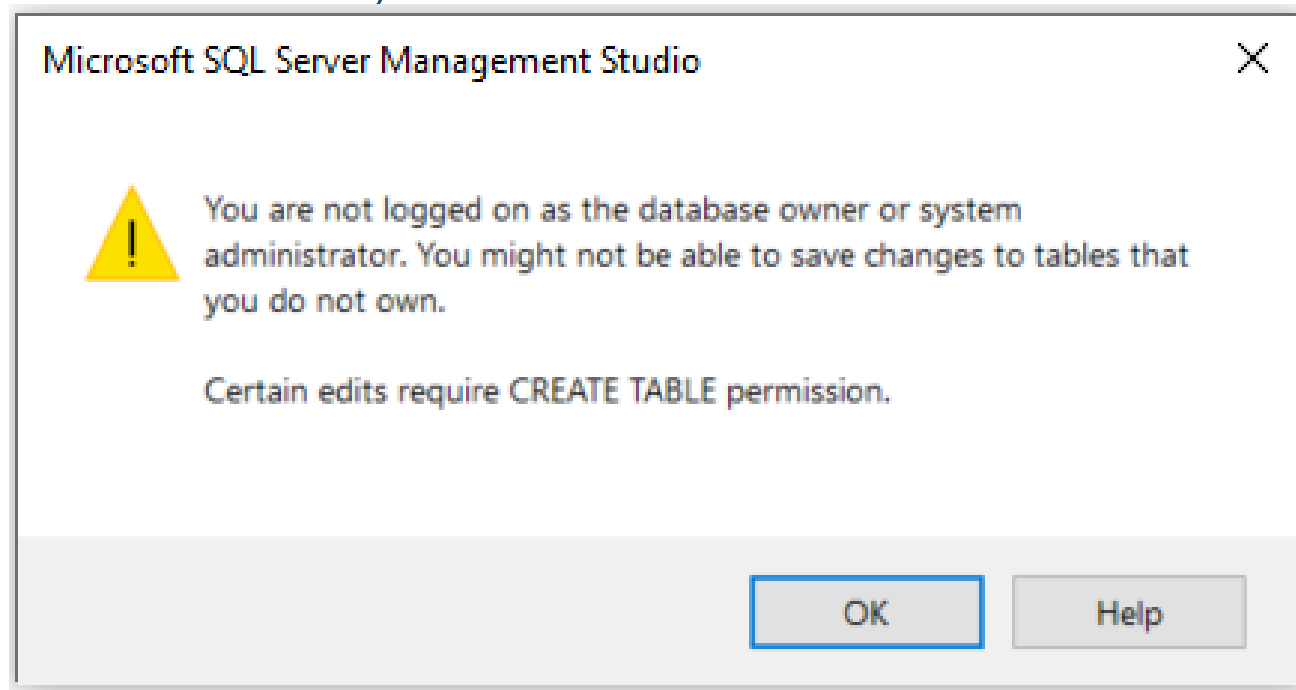




DEMO



- ❑ 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

- ❑ **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.

- ❑ **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 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

GÁN ROLE – VAI TRÒ CHO LOGIN ID

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

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'Object Explorer' pane shows the 'Logins' folder expanded under 'Security'. A red box highlights a list of login IDs, including 'DB_01_Admin', 'DB_01_UserThuong', 'DB_backup', 'NT AUTHORITY\SYSTEM', 'NT Service\MSSQLSERVER', 'NT SERVICE\SQLSERVERAGENT', 'NT SERVICE\SQLTELEMETRY', 'NT SERVICE\SQLWriter', 'NT SERVICE\Winmgmt', 'sa', and 'WIN10_X64_LAB\TonyTeo'. A blue callout bubble points to this list with the text 'Chọn Login ID cần gán Server role'. In the center, the 'Login Properties - sa' dialog box is open, with the 'Server Roles' tab selected and highlighted by a red box. A blue callout bubble points to this tab with the text 'Danh sách Server role'. On the right, the 'Server roles' list is shown, with checkboxes for 'bulkadmin', 'dbcreator', 'diskadmin', 'processadmin', 'public', 'securityadmin', 'serveradmin', 'setupadmin', and 'sysadmin'. The 'public' and 'sysadmin' roles are checked. A red box highlights this list, and a blue callout bubble points to it with the text 'Danh sách Server role'.

Object Explorer

Connect

(SQL Server 15.0.2000.5 - WIN10_X64_LAB\TonyTeo)

Databases

Security

Logins

- ##MS_PolicyEventProcessingLogin##
- ##MS_PolicyTsqlExecutionLogin##
- DB_01_Admin
- DB_01_UserThuong
- DB_backup
- NT AUTHORITY\SYSTEM
- NT Service\MSSQLSERVER
- NT SERVICE\SQLSERVERAGENT
- NT SERVICE\SQLTELEMETRY
- NT SERVICE\SQLWriter
- NT SERVICE\Winmgmt
- sa
- WIN10_X64_LAB\TonyTeo

Server Roles

Login Properties - sa

Select a page

- General
- Server Roles
- User Mapping
- Status

Danh sách Server role

Server roles:

- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☒ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☒ sysadmin

Chọn Login ID cần gán Server role

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)

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'Object Explorer' pane shows the 'DemoDB_01' database selected, with the 'Security' folder expanded to show 'Database Roles'. A list of roles is shown, including 'admin_cddl', 'db_accessadmin', 'db_backupoperator', 'db_datareader', 'db_datawriter', and 'db_ddladmin'. The 'db_backupoperator' role is highlighted. A blue callout bubble points to this role with the text 'Danh sách Database Roles'. In the center, the 'Database Role Properties - db_backupoperator' window is open, showing the 'General' tab. The 'Role name' is 'db_backupoperator' and the 'Owner' is 'dbo'. A list of 'Owned Schemas' is shown, including 'db_accessadmin', 'dbo', 'db_securityadmin', 'sys', 'db_owner', and 'db_backupoperator'. A blue callout bubble points to this list with the text 'Thêm Login ID Database Roles'. At the bottom, the 'Role Members' section shows a list of members, with 'DB_backup' highlighted. A red box highlights this section. The 'Connection' pane at the bottom shows the server 'WIN10_X64_LAB' and the connection 'WIN10_X64_LAB\TonyTeo'.

Danh sách Database Roles

Thêm Login ID Database Roles

❑ 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
```


❑ Kiểm tra user là thành viên của database role

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'Object Explorer' pane shows the server hierarchy. A red box labeled '1' highlights the 'Databases' folder, and another red box labeled '2' highlights the 'DB_backup' database under the 'Users' folder. The right pane shows the 'Database User - DB_backup' properties. A red box labeled '3' highlights the 'Membership' tab in the 'Select a page' section. On the right side of the 'Database role membership' section, a red box labeled '4' highlights the 'db_backupoperator' role, which is checked in the 'Role Members' list.

Object Explorer

Connect ▾

(SQL Server 15.0.2000.5 - WIN10_X64_LAB\TonyTeo)

- Databases
 - System Databases
 - Database Snapshots
 - AdventureWorksDW2019
 - DemoDB_01**
 - Database Diagrams
 - Tables
 - Views
 - External Resources
 - Synonyms
 - Programmability
 - Service Broker
 - Storage
 - Security
 - Users
 - DB 01 Admin
 - DB_backup**
 - dbo

Database User - DB_backup

Select a page

- General
- Owned Schemas
- Membership**
- Securables
- Extended Properties

Script ▾ Help

Database role membership:

Role Members

- ☐ admin_cddl
- ☐ db_accessadmin
- ☒ **db_backupoperator**
- ☐ db_datareader
- ☐ db_datawriter
- ☐ db_ddladmin
- ☐ db_denydatareader
- ☐ db_denydatawriter
- ☐ db_owner
- ☐ db_securityadmin

Connection



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

- ❑ 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 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:** Là lệnh dùng để cấp phát 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
```

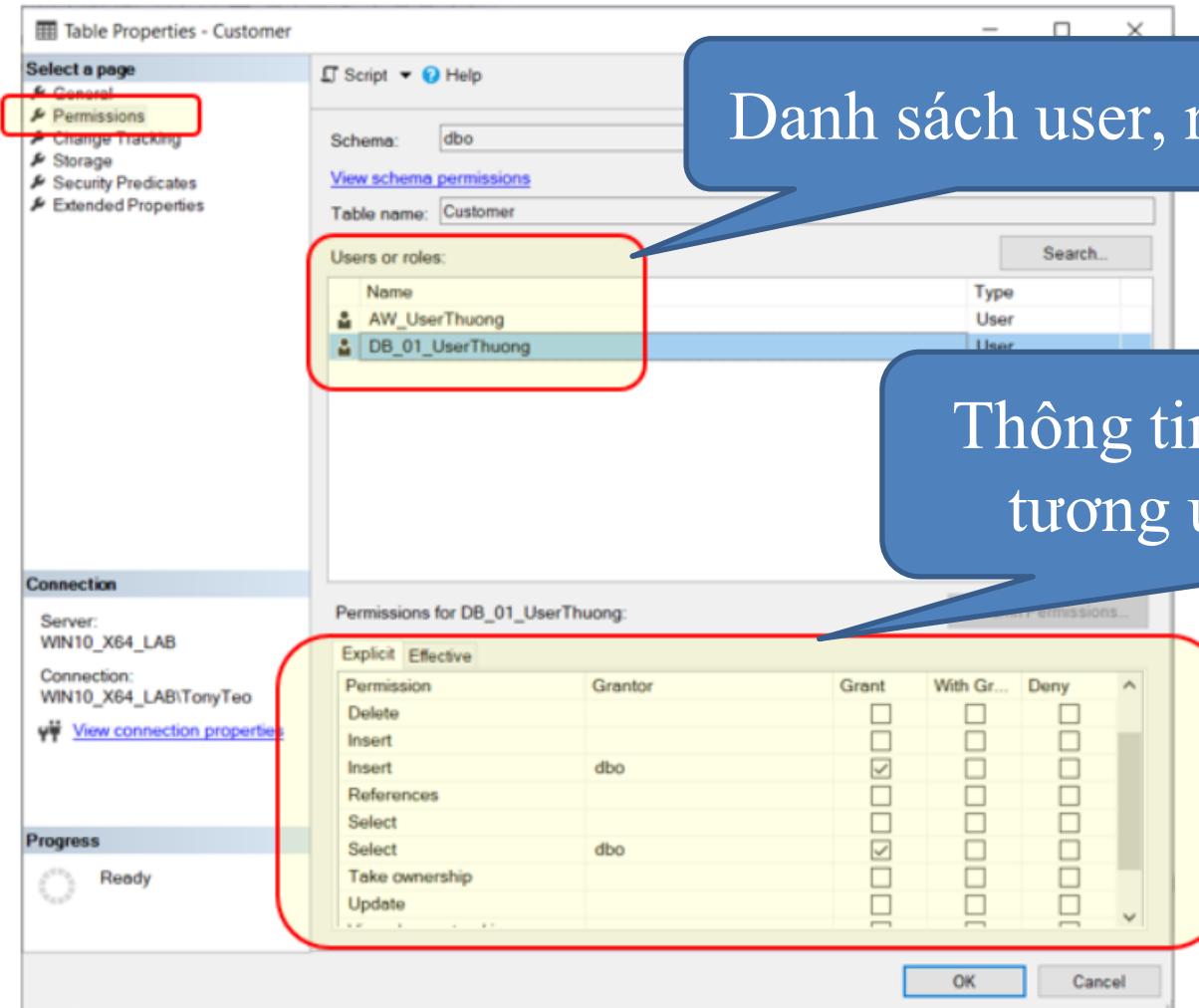
❑ Cú pháp cấm thực thi

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
```

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



Danh sách user, role

Thông tin các quyền cài đặt tương ứng với user/role



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”



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



FPT POLYTECHNIC

Thank you