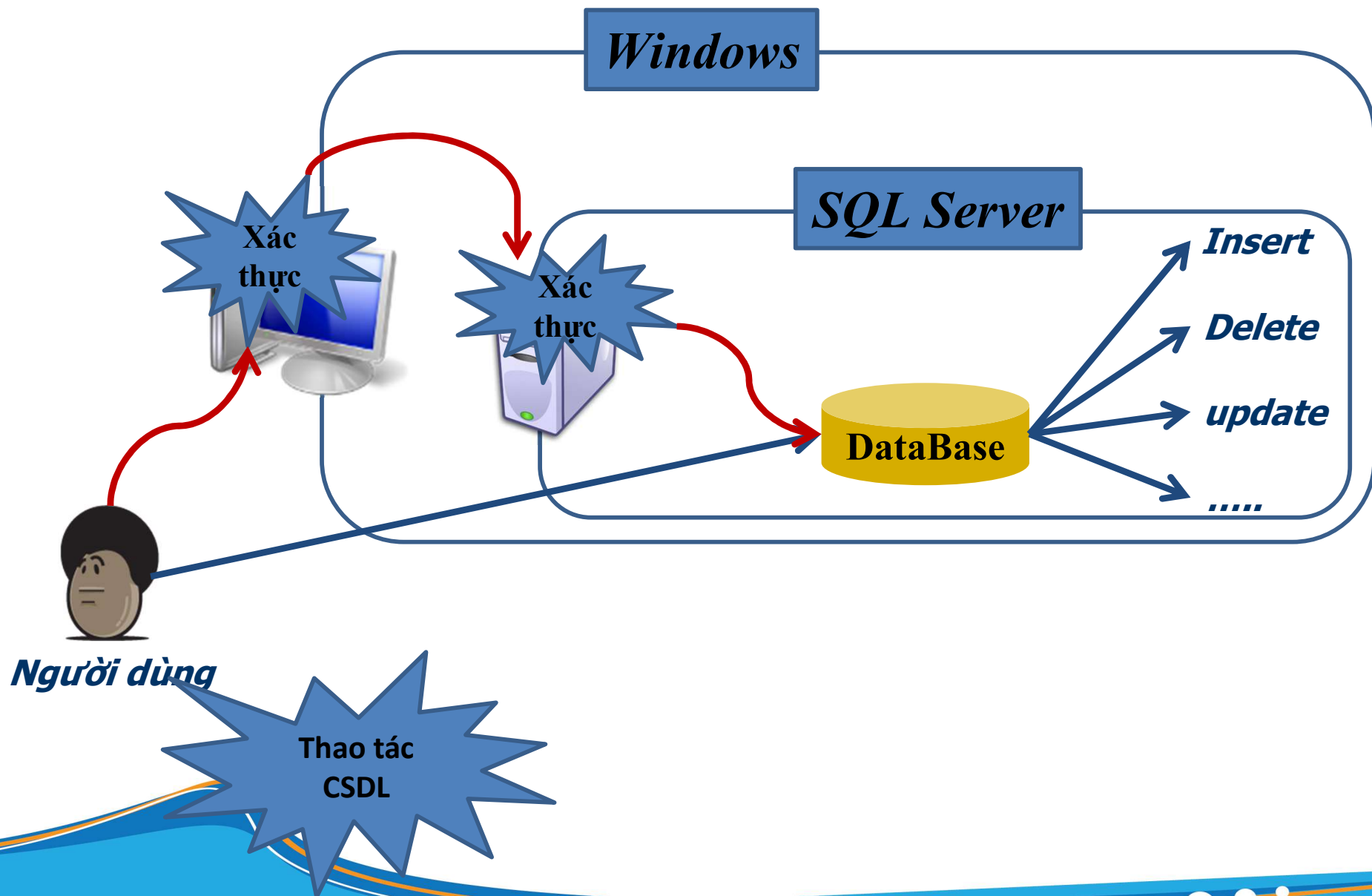


Quản trị quyền người dùng



KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Giới thiệu



Cơ chế quản trị người dùng

- ❖ Cung cấp và quản lý các tài khoản truy cập (login) mà người sử dụng dùng để kết nối với SQL Server
- ❖ Phân quyền: người dùng chỉ được phép thực hiện những thao tác mà họ được “cấp phép”



Khái niệm xác thực

- ❖ Xác nhận xem một tài khoản truy cập (login) có hợp lệ không (có được phép đăng nhập vào windows hoặc SQL server hay không)

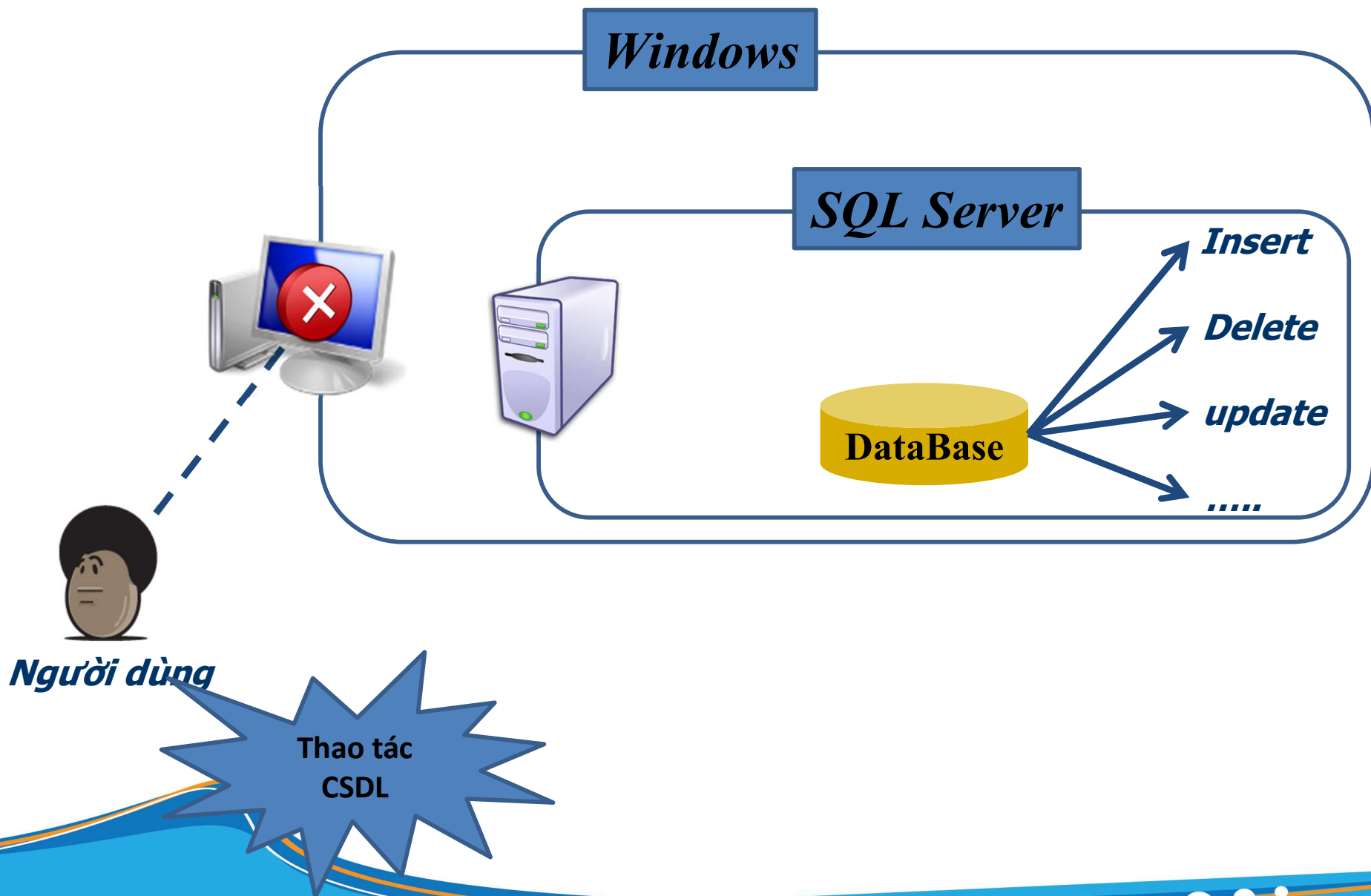


Các cấp độ bảo mật

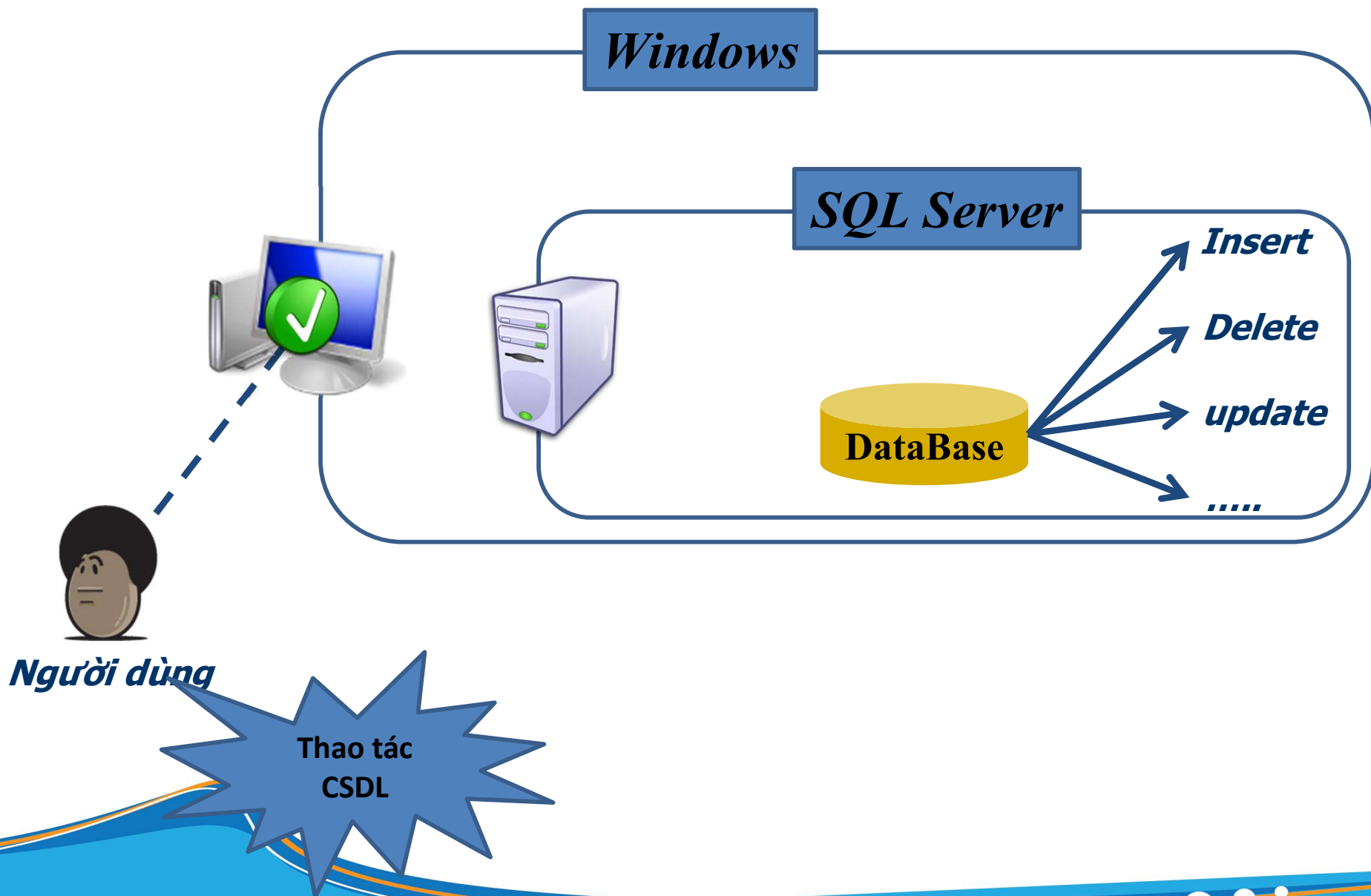
- ❖ Windows Level
- ❖ SQL Server Level
- ❖ Database Level



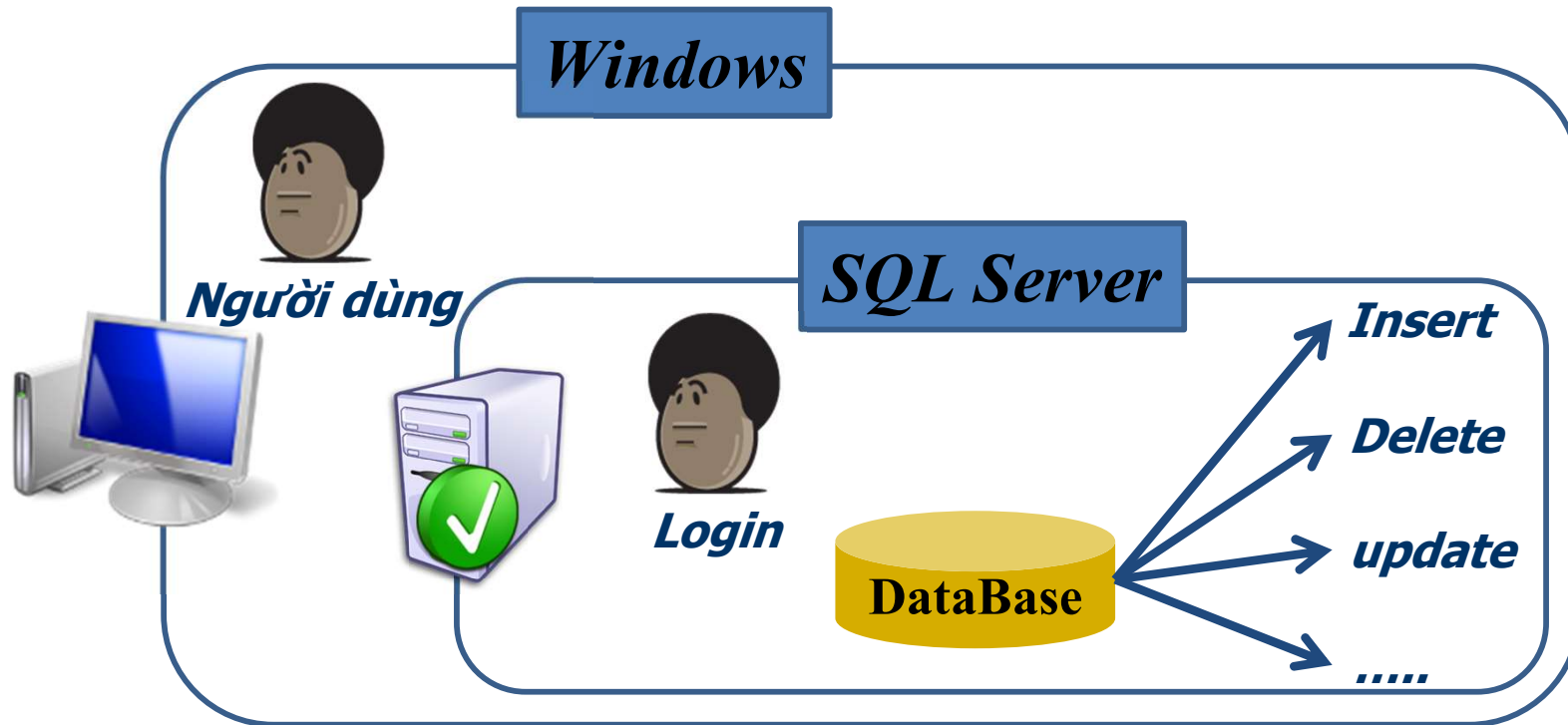
Giới thiệu



Giới thiệu



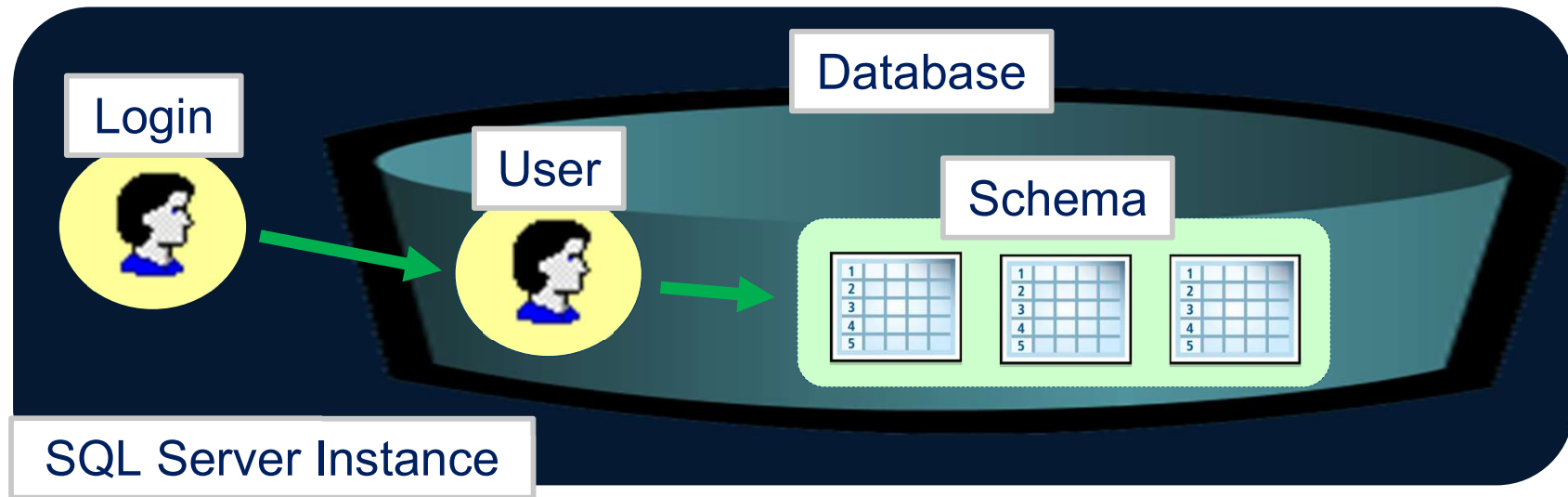
Giới thiệu



Login

- ✓ Windows login
- ✓ SQL login

Login



Các kiểu xác thực của SQL

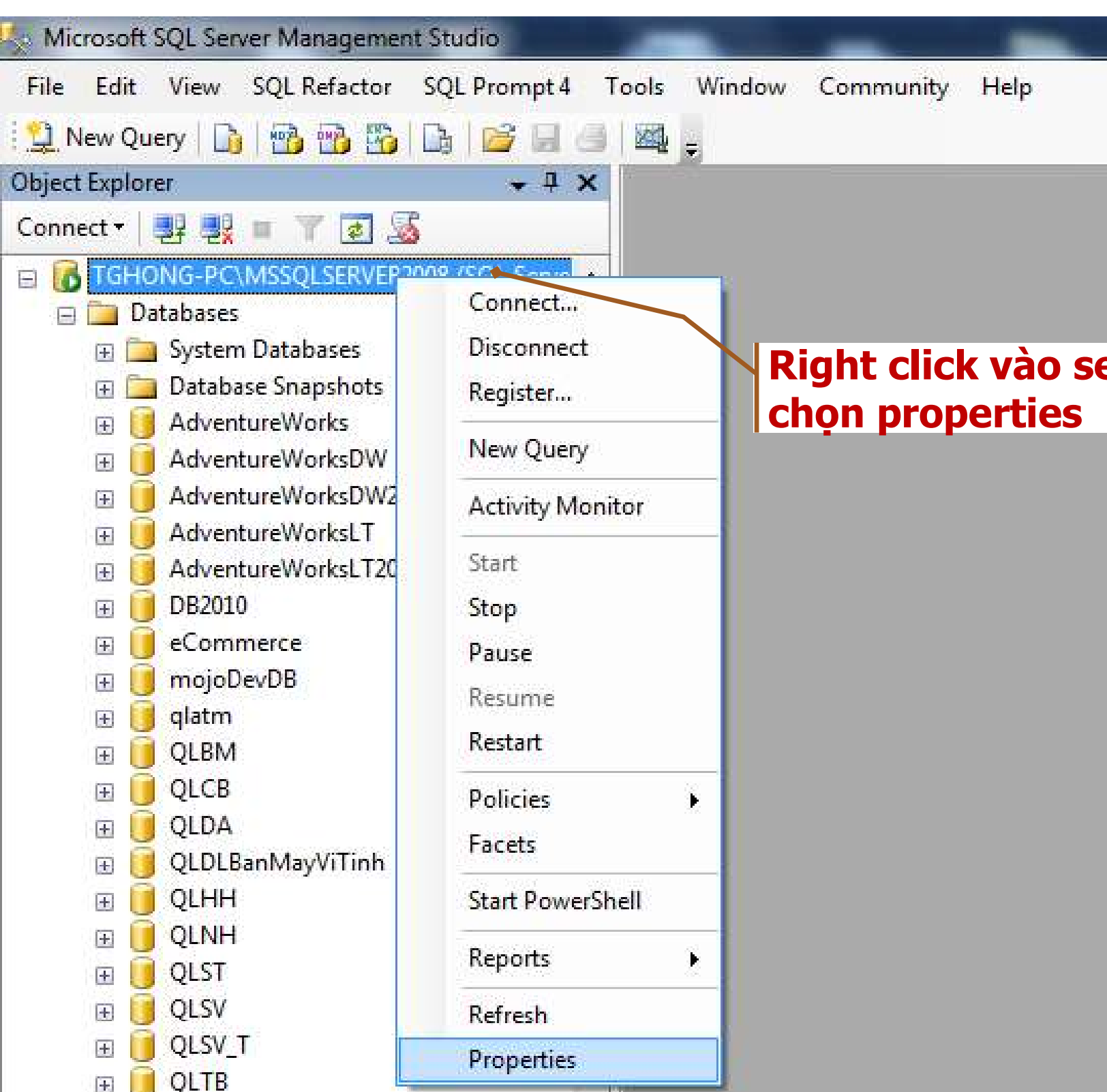
- ❖ Windows Authentication Mode
- ❖ Mixed Mode (Windows Authentication + SQL Server Standard)

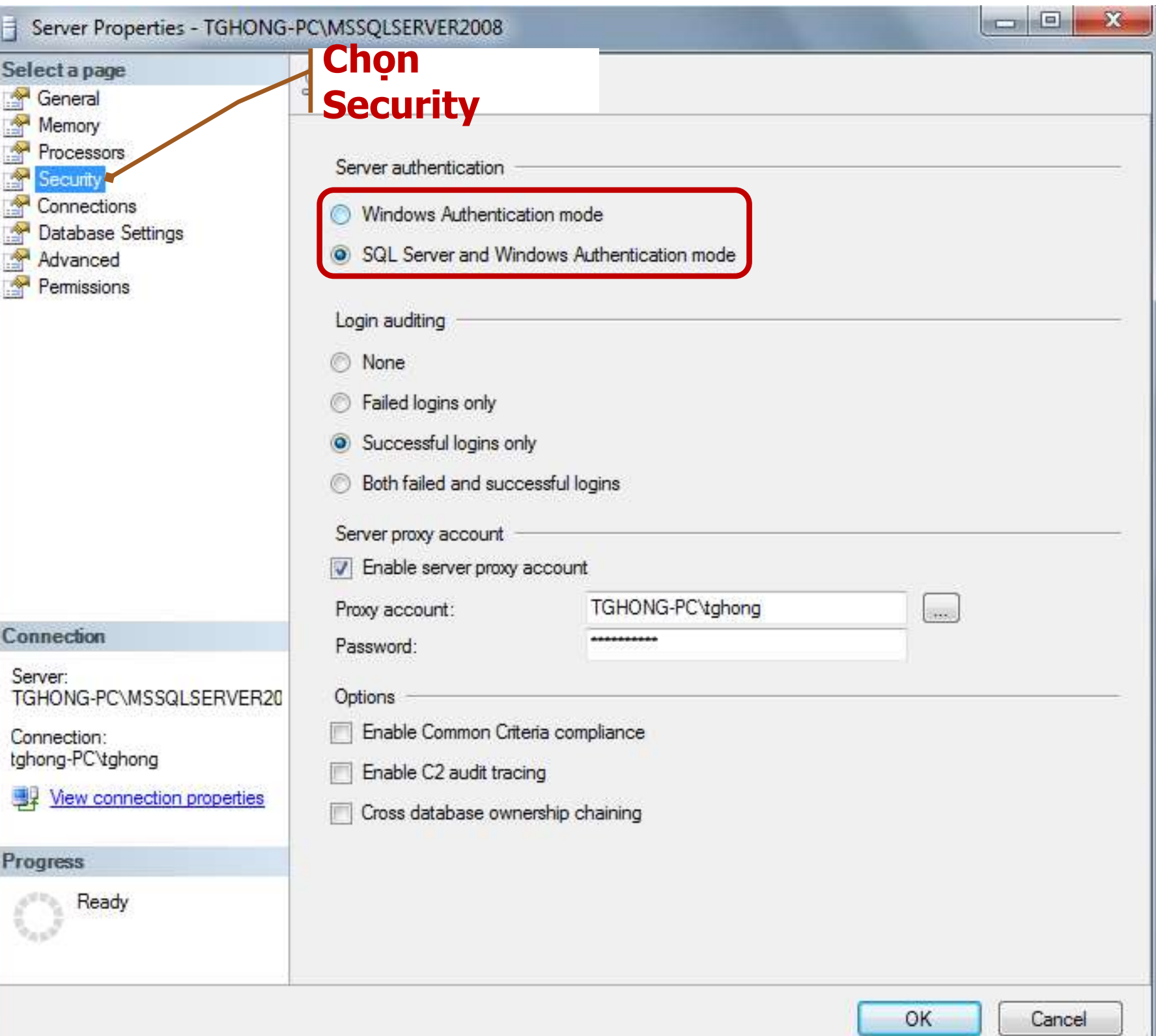


Chọn mode vào MS-SQL

- ❖ Lựa chọn:
 - Chỉ dùng Windows Authentication
 - Mixed mode (sử dụng cả hai chế độ chứng thực)
- ❖ Thực hiện cấu hình này lúc:
 - Cài đặt
 - Thay đổi sau khi đã cài đặt: dùng Enterprise Manager:
 - ✓ Click phải lên tên Server trong cửa sổ duyệt bên trái
 - ✓ Chọn properties







Chọn Security

Server authentication

☐ Windows Authentication mode

☒ SQL Server and Windows Authentication mode

Login auditing

☐ None

☐ Failed logins only

☒ Successful logins only

☐ Both failed and successful logins

Server proxy account

☒ Enable server proxy account

Proxy account: TGHONG-PC\tghong

Password: *****

Options

☐ Enable Common Criteria compliance

☐ Enable C2 audit tracing

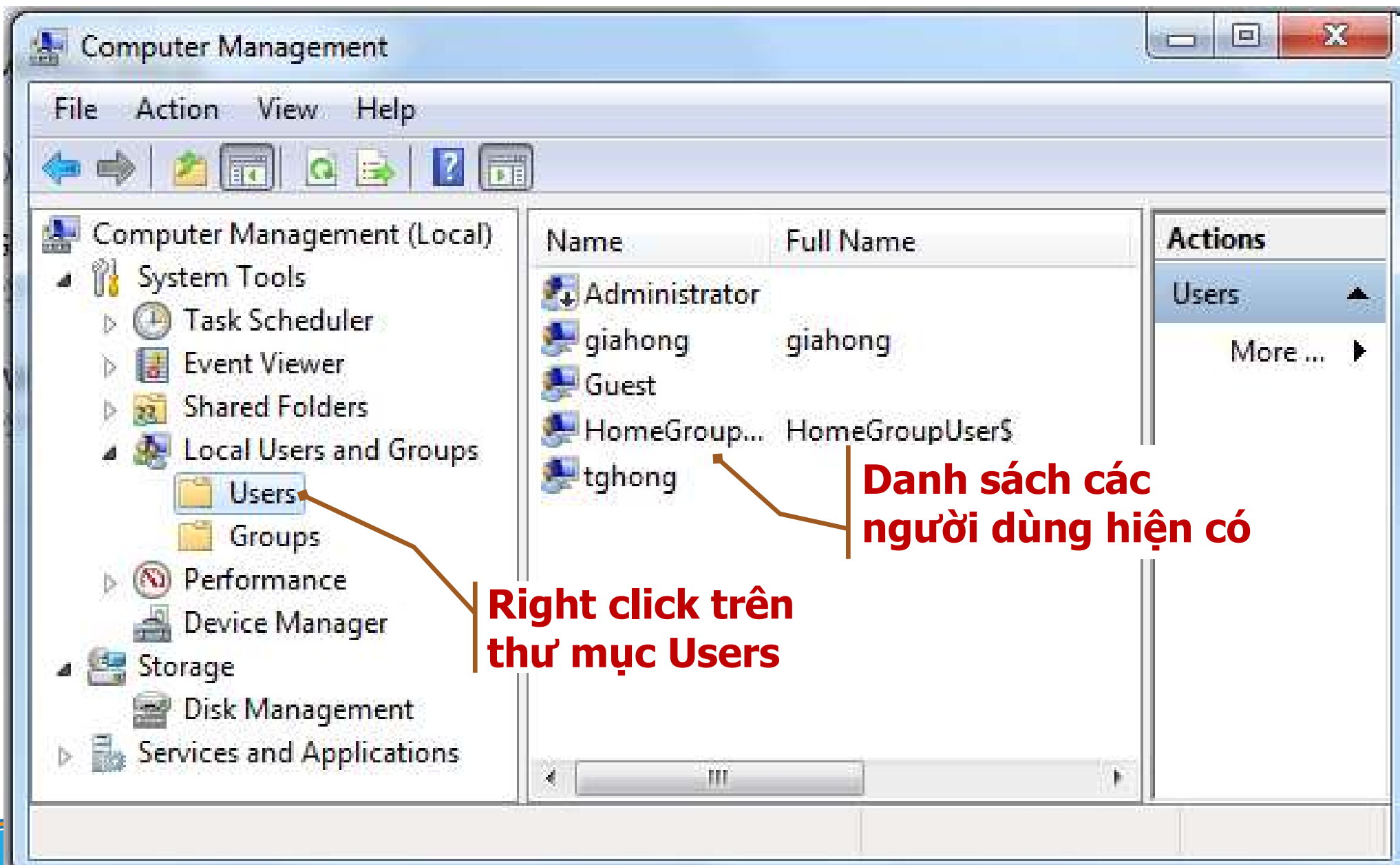
☐ Cross database ownership chaining

OK Cancel

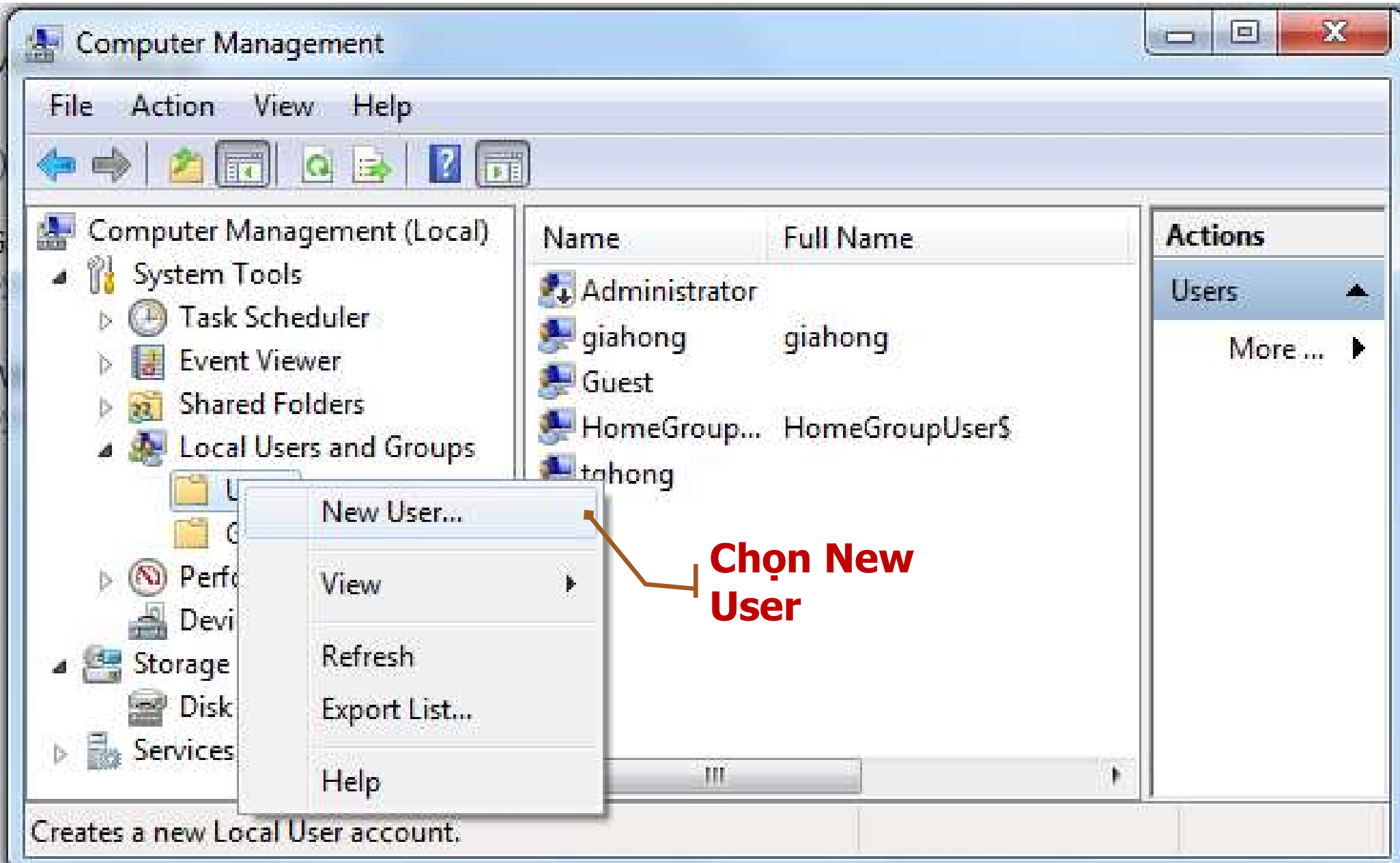
Windows Authentication

- ❖ Cho phép cho các người dùng của Windows được đăng nhập vào SQL Server.
 - Tài khoản người dùng do windows quản lí.
 - Khi người dùng kết nối đến SQL Server sử dụng chế độ Window Authentication, SQL Server chỉ xét xem người dùng này của Windows đã được cấp phép vào SQL Server hay chưa.
 - Admin của hệ điều hành mà SQL Server đang chạy trên đó luôn được phép vào SQL Server với quyền sysadmin.

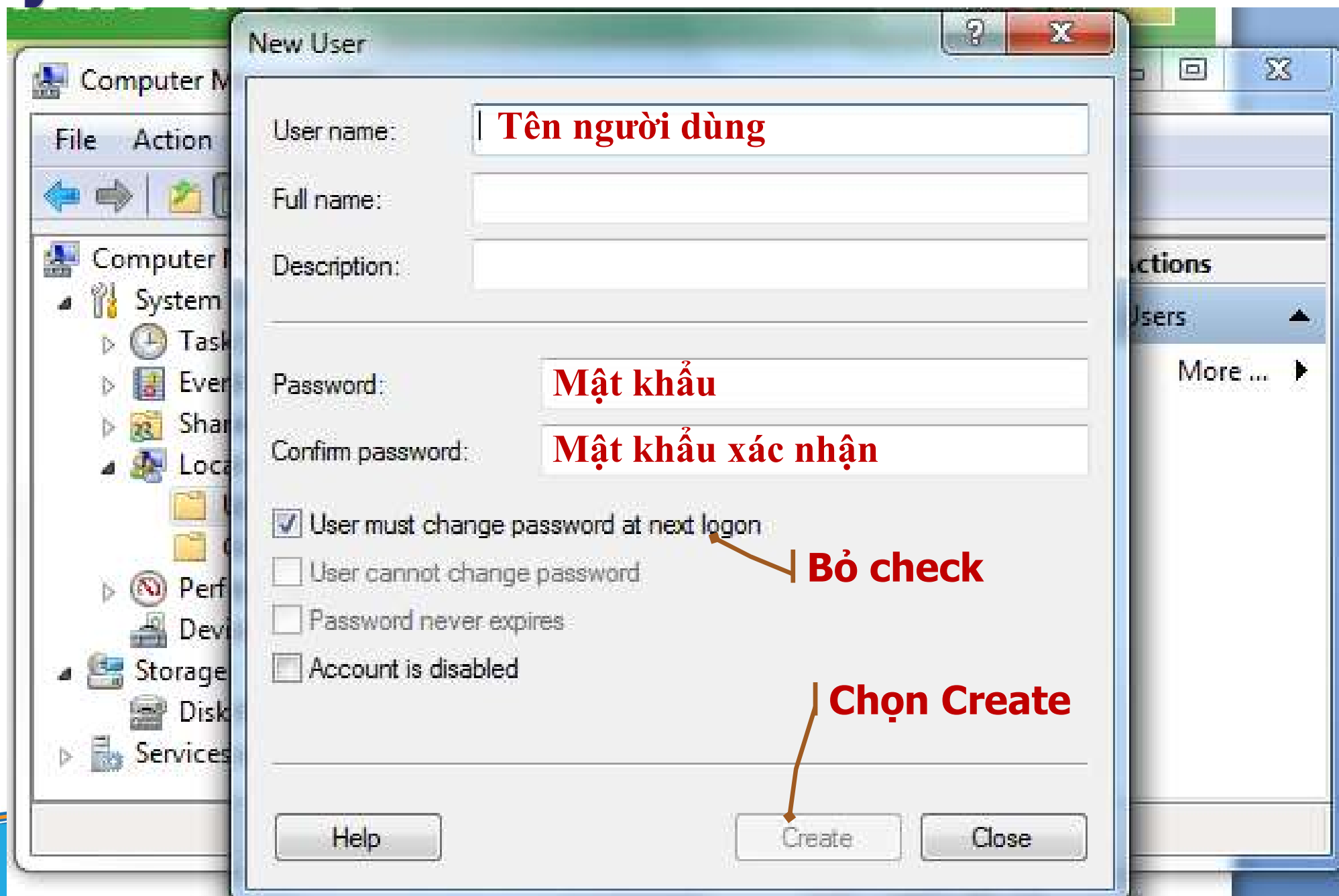
Tạo Win account



Tạo Win account



Tạo Win account

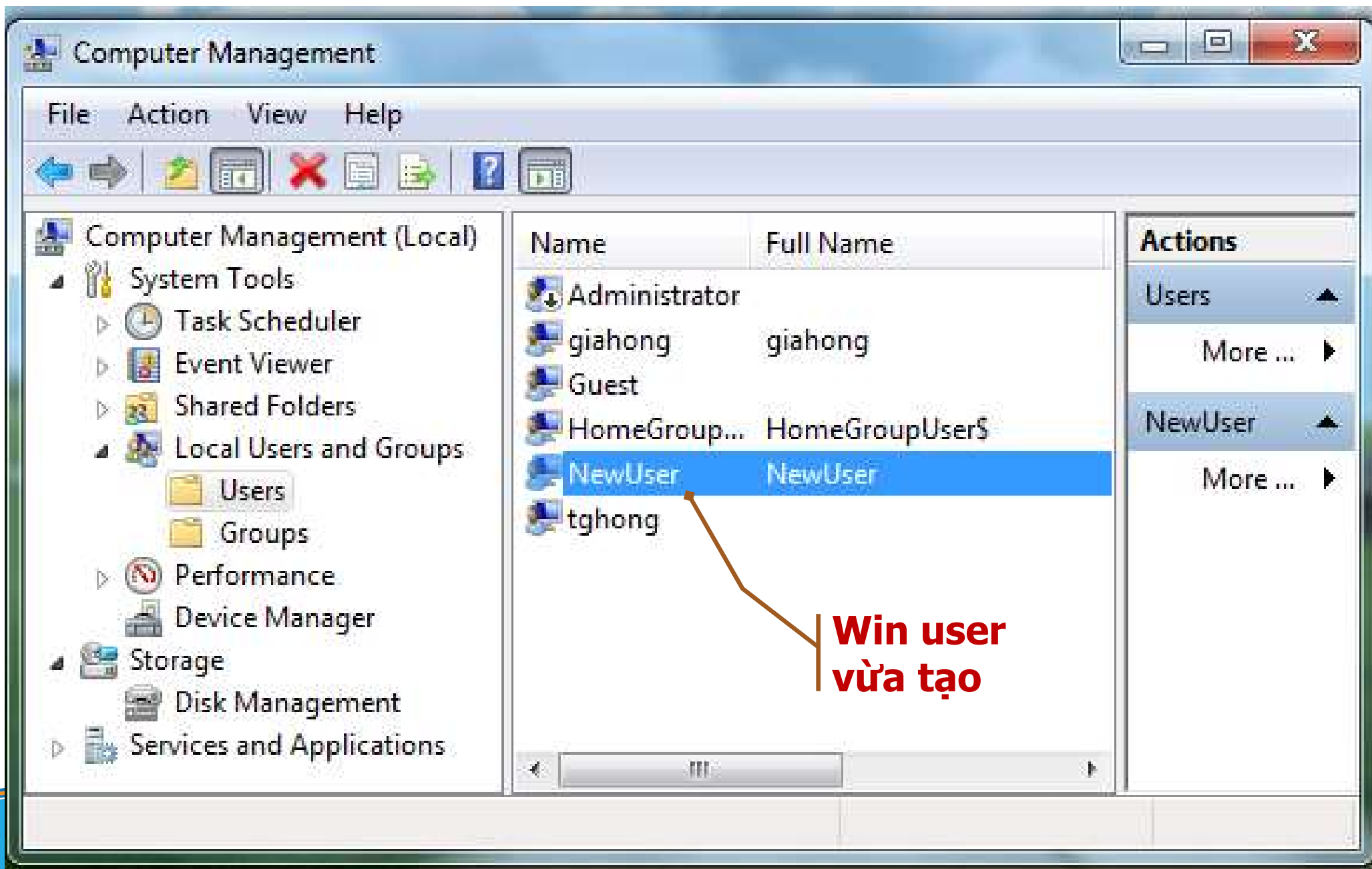


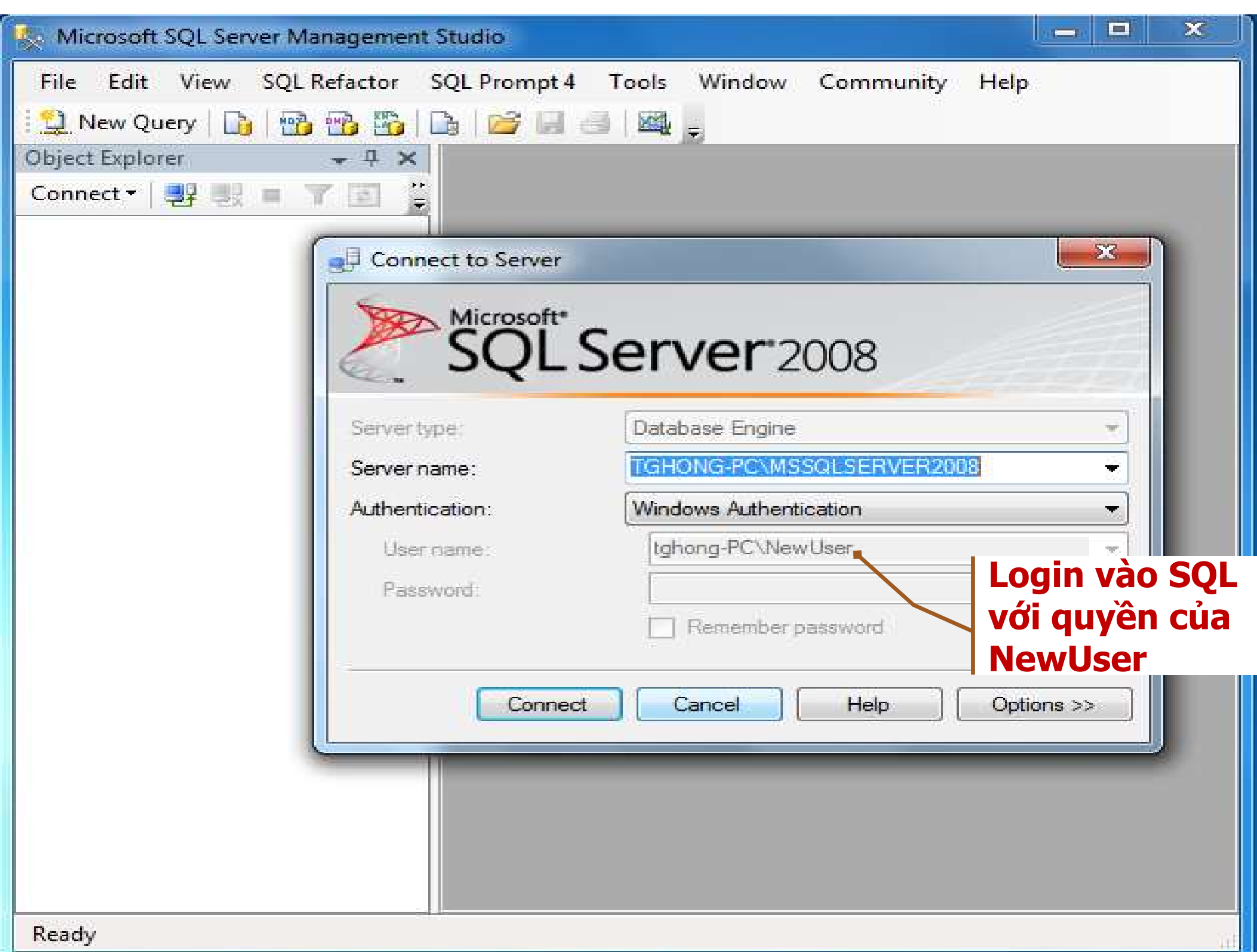
The image shows a Windows XP desktop with a 'New User' dialog box open. The dialog box has the following fields and options:

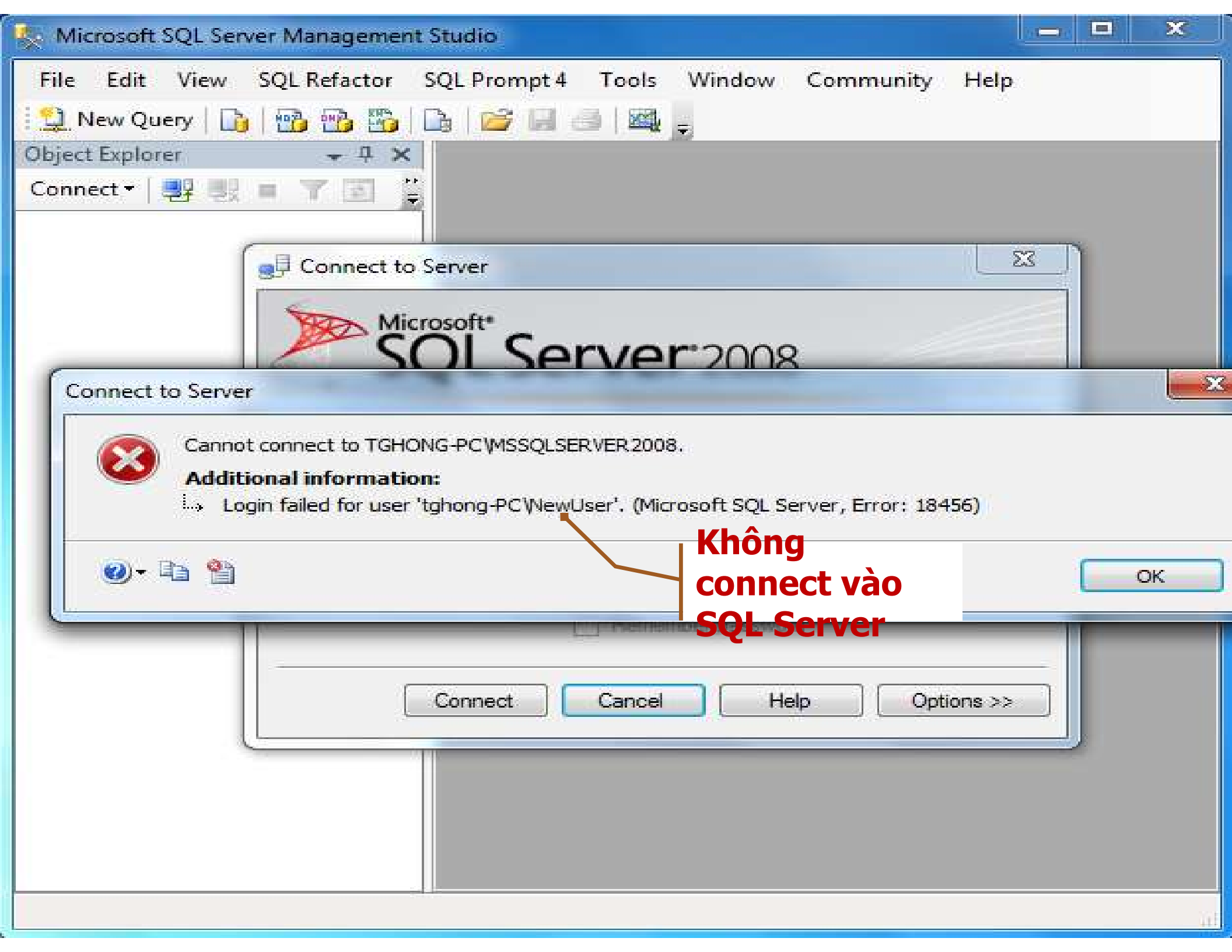
- User name: **Tên người dùng**
- Full name: (empty)
- Description: (empty)
- Password: **Mật khẩu**
- Confirm password: **Mật khẩu xác nhận**
- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled

At the bottom of the dialog box are three buttons: 'Help', 'Create', and 'Close'. An arrow points from the text **Bỏ check** to the 'User must change password at next logon' checkbox. Another arrow points from the text **Chọn Create** to the 'Create' button.

Tạo Win account







Connect to Server



Cannot connect to TGHONG-PC\MSSQLSERVER.2008.

Additional information:

Login failed for user 'tghong-PC\NewUser'. (Microsoft SQL Server, Error: 18456)



OK

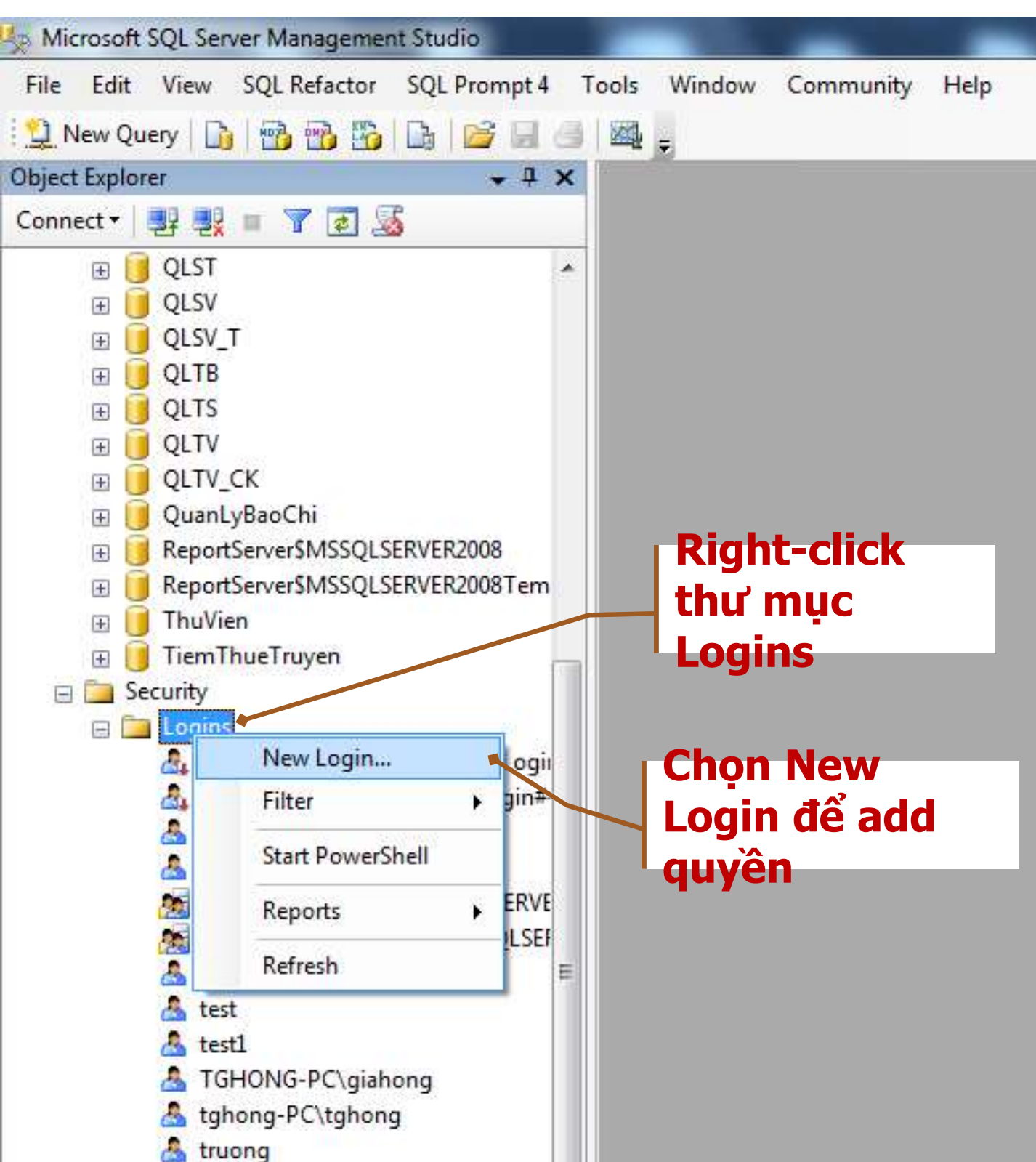
Connect

Cancel

Help

Options >>

Không
connect vào
SQL Server



**Right-click
thư mục
Logins**

**Chọn New
Login để add
quyền**

Login - New

Select a page

General

Server Roles

User Mapping

Securables

Status

Connection

Server:
TGHONG-PC\MSSQLSERVER20

Connection:
tghong-PC\tghong

View connection properties

Progress

Ready

Script

Help

1

Login name:

Tên người dùng

2

Search...

Windows authentication

SQL Server authentication

Password:

Confirm password:

Specify old password

Old password:

Enforce password policy

Enforce password expiration

User must change password at next login

Mapped to certificate

Mapped to asymmetric key

Map to Credential

Add

Mapped Credentials

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

Remove

Default database:

master

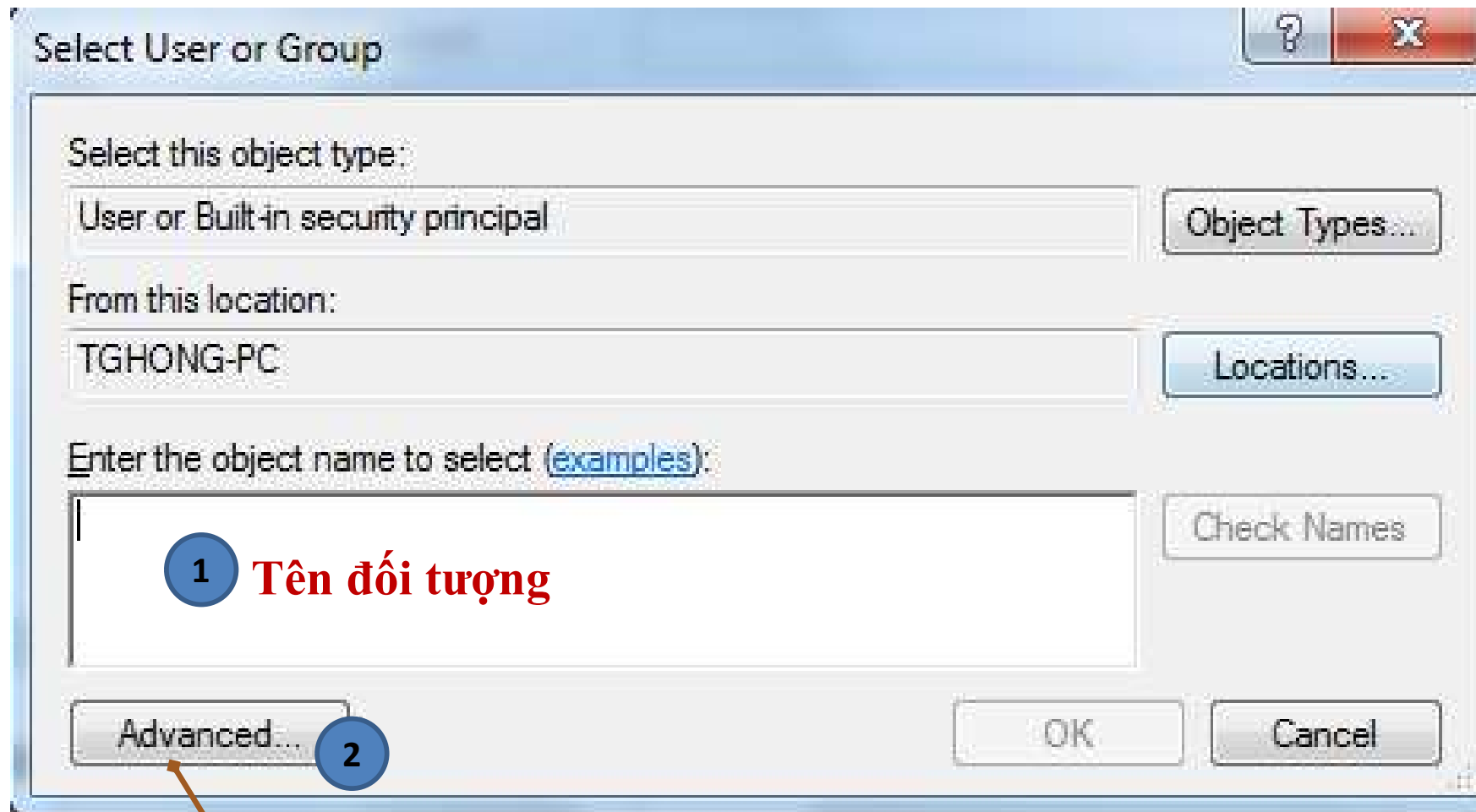
Default language:

<default>

OK

Cancel

Tìm người dùng



1 Tên đối tượng

2
Tìm đối tượng
login

Select User or Group



Select this object type:

User or Built-in security principal

Object Types...

From this location:

TGHONG-PC

Locations...

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

Days since last logon:

Columns...

Find Now

Stop



Tìm đối tượng login

Search results:

OK

Cancel

Name (RDN)	In Folder
------------	-----------

Select User or Group

Select this object type:

User or Built-in security principal

Object Types...

From this location:

TGHONG-PC

Locations...

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

Days since last login:

Columns...

Find Now

Stop



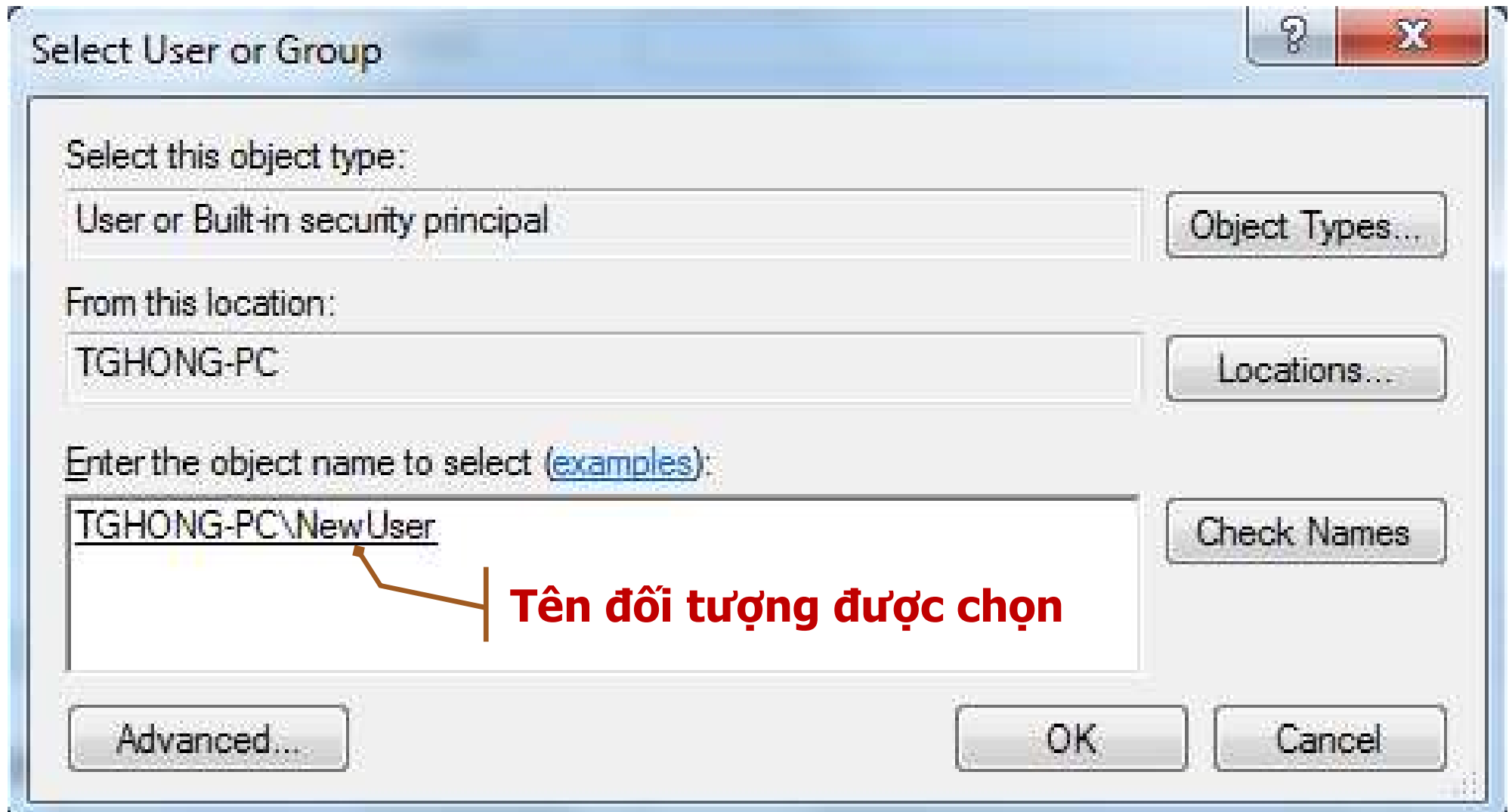
OK

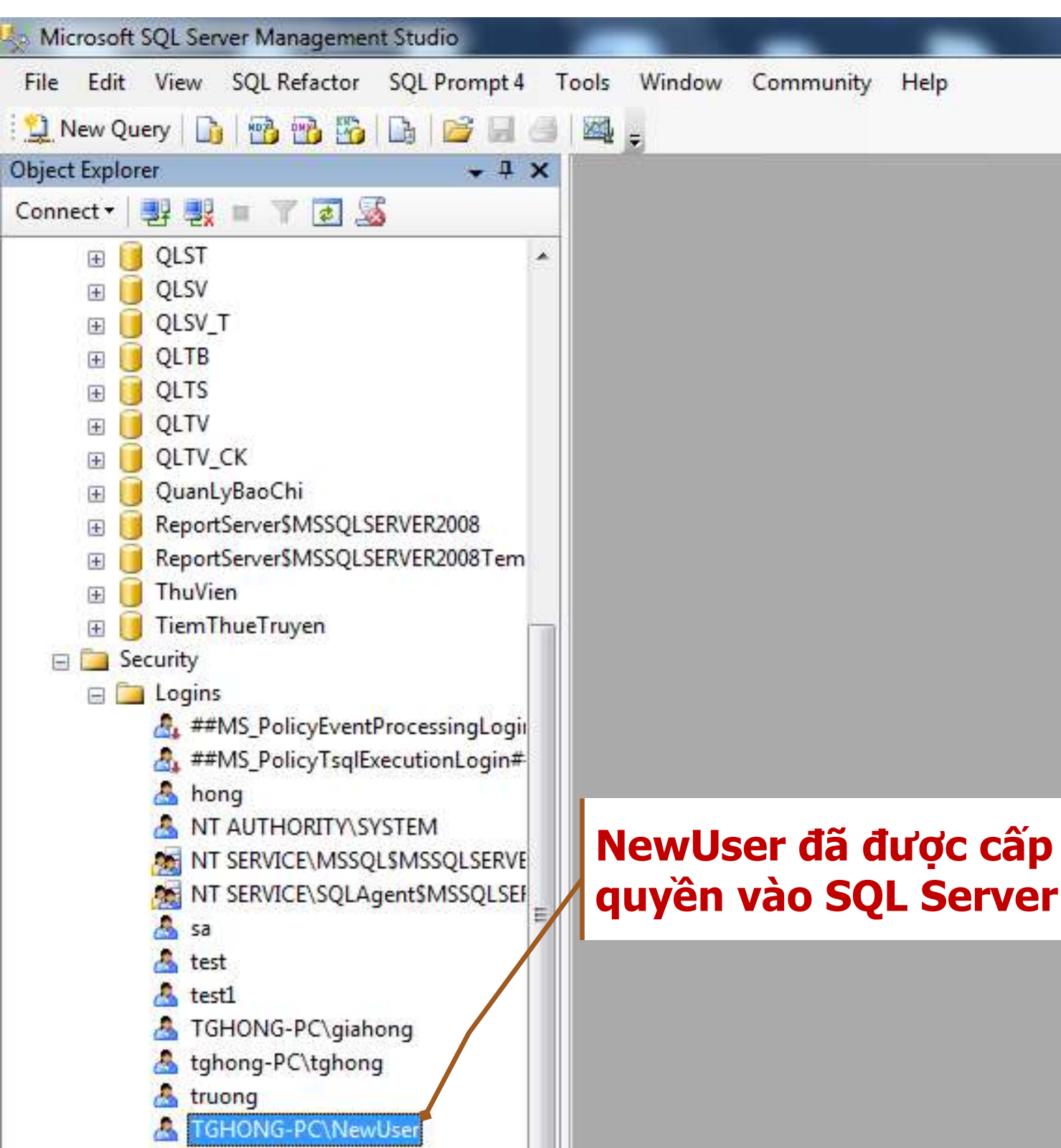
Cancel

Search results:

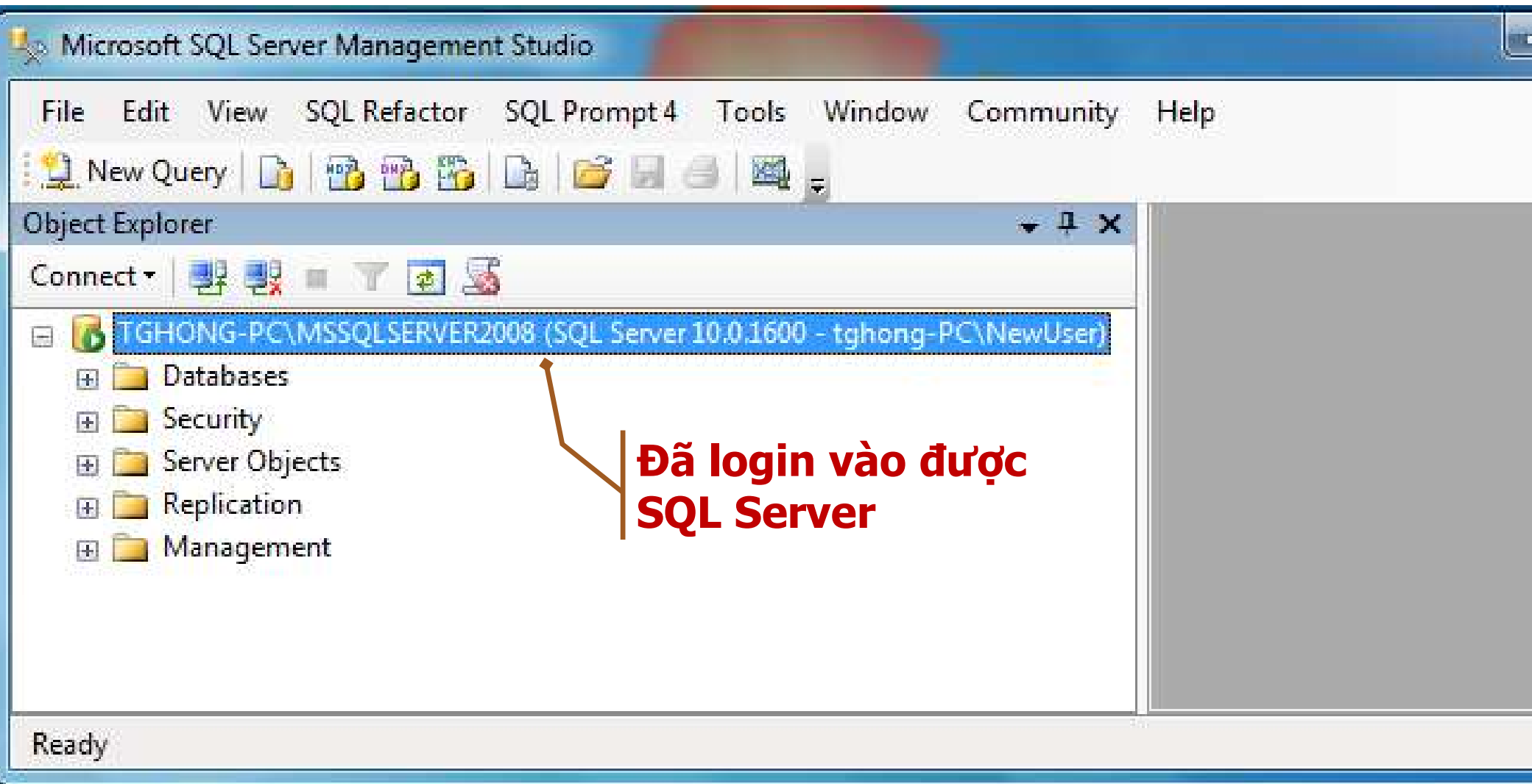
Name (RDN)	In Folder
LOCAL SERV...	
NETWORK	
NETWORK S...	
NewUser	TGHONG-PC
OWNER RIG...	
REMOTE INT...	
SERVICE	
SYSTEM	
TERMINAL S...	

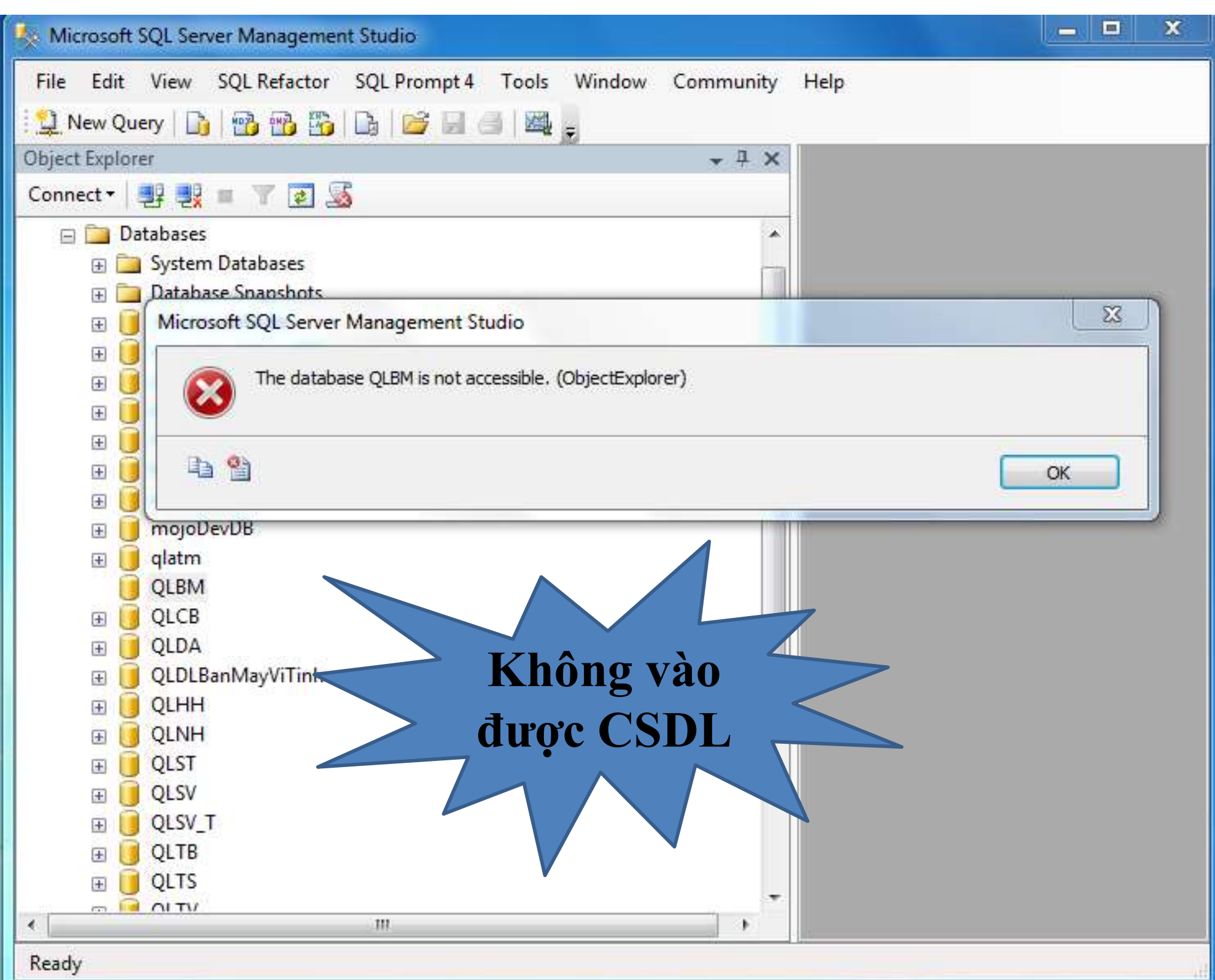
Chọn đối tượng cần add





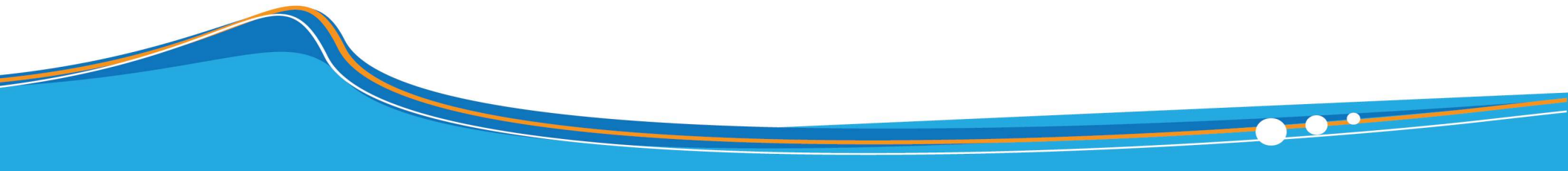
**NewUser đã được cấp
quyền vào SQL Server**

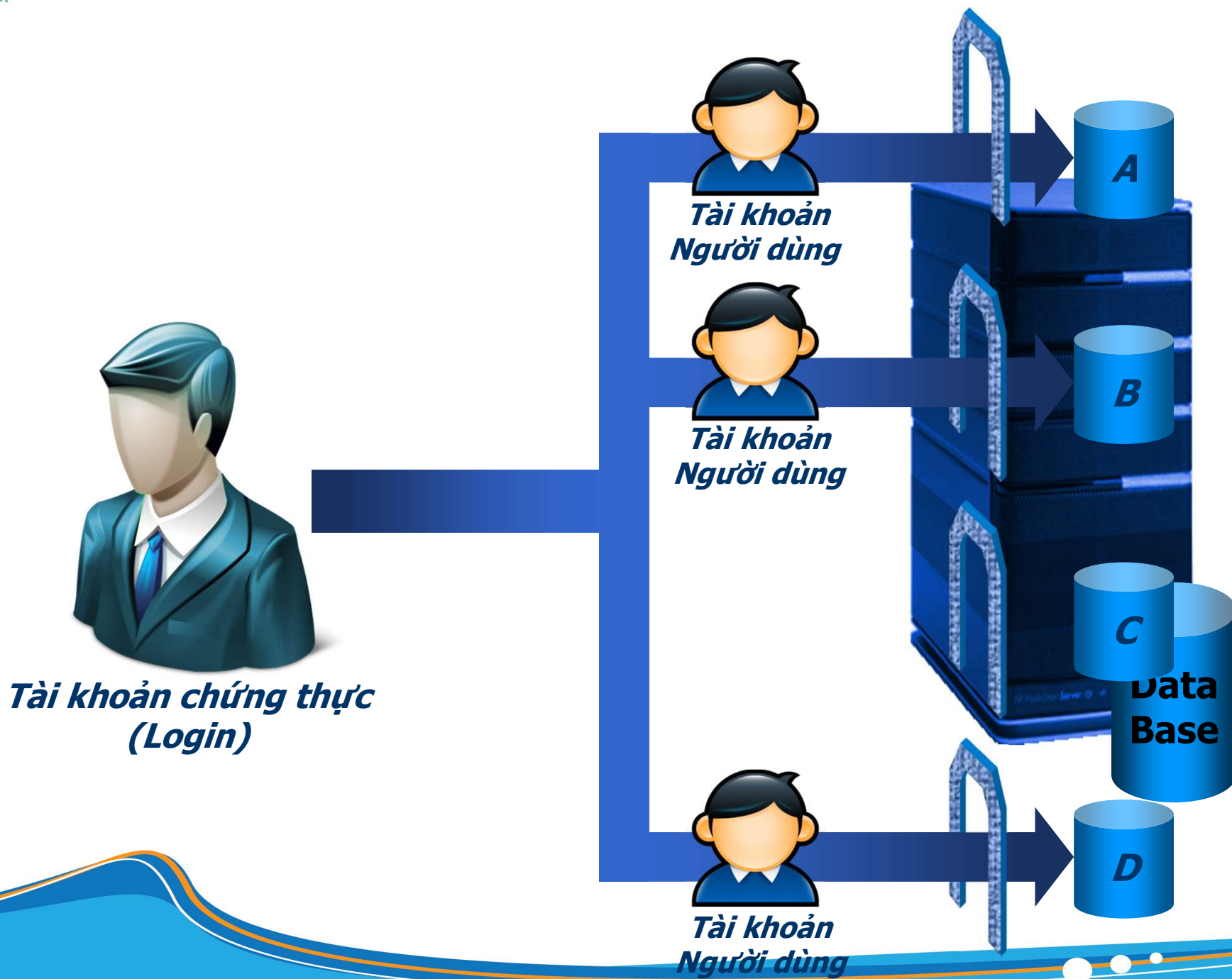


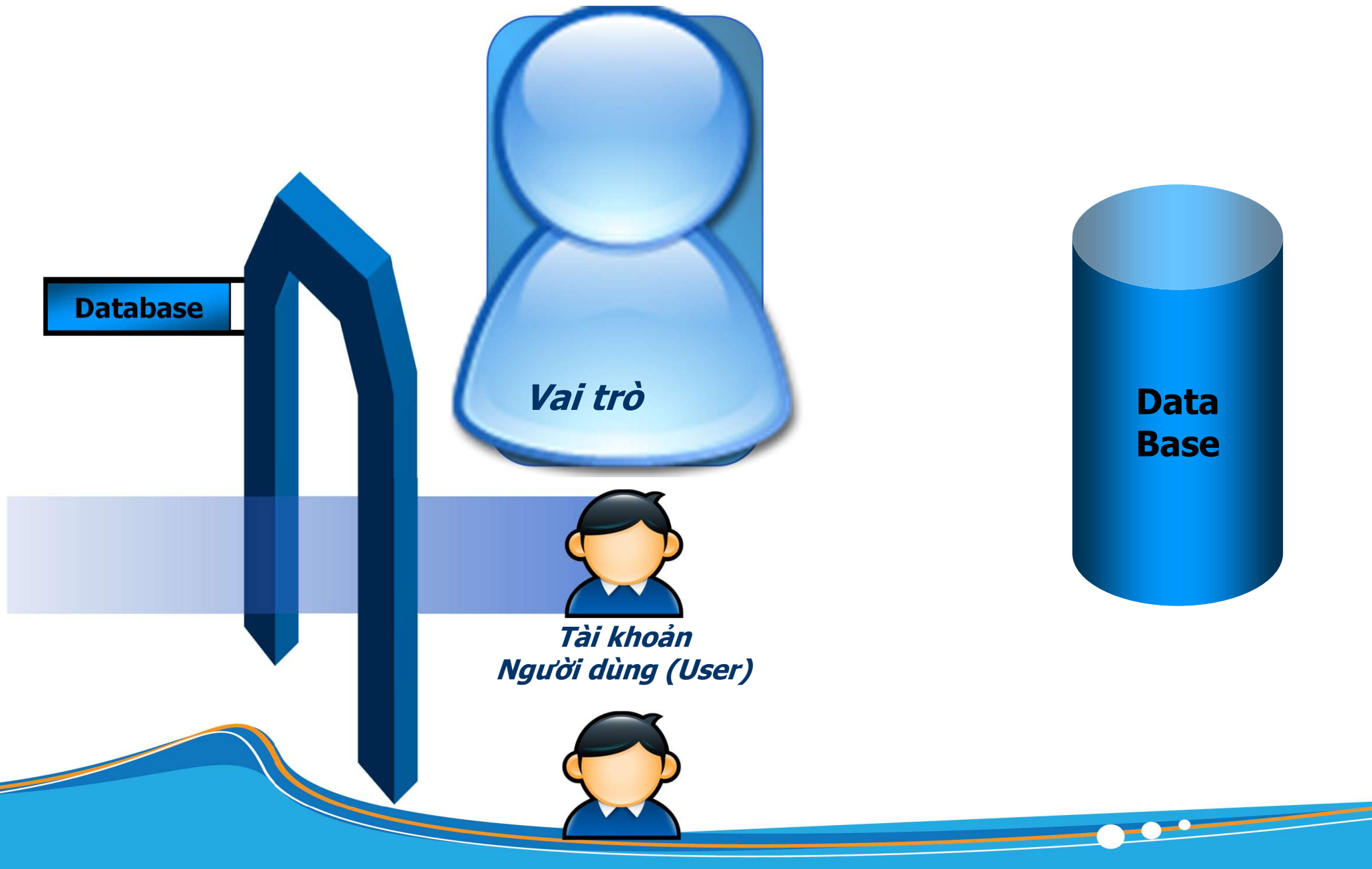


SQL Server xác thực

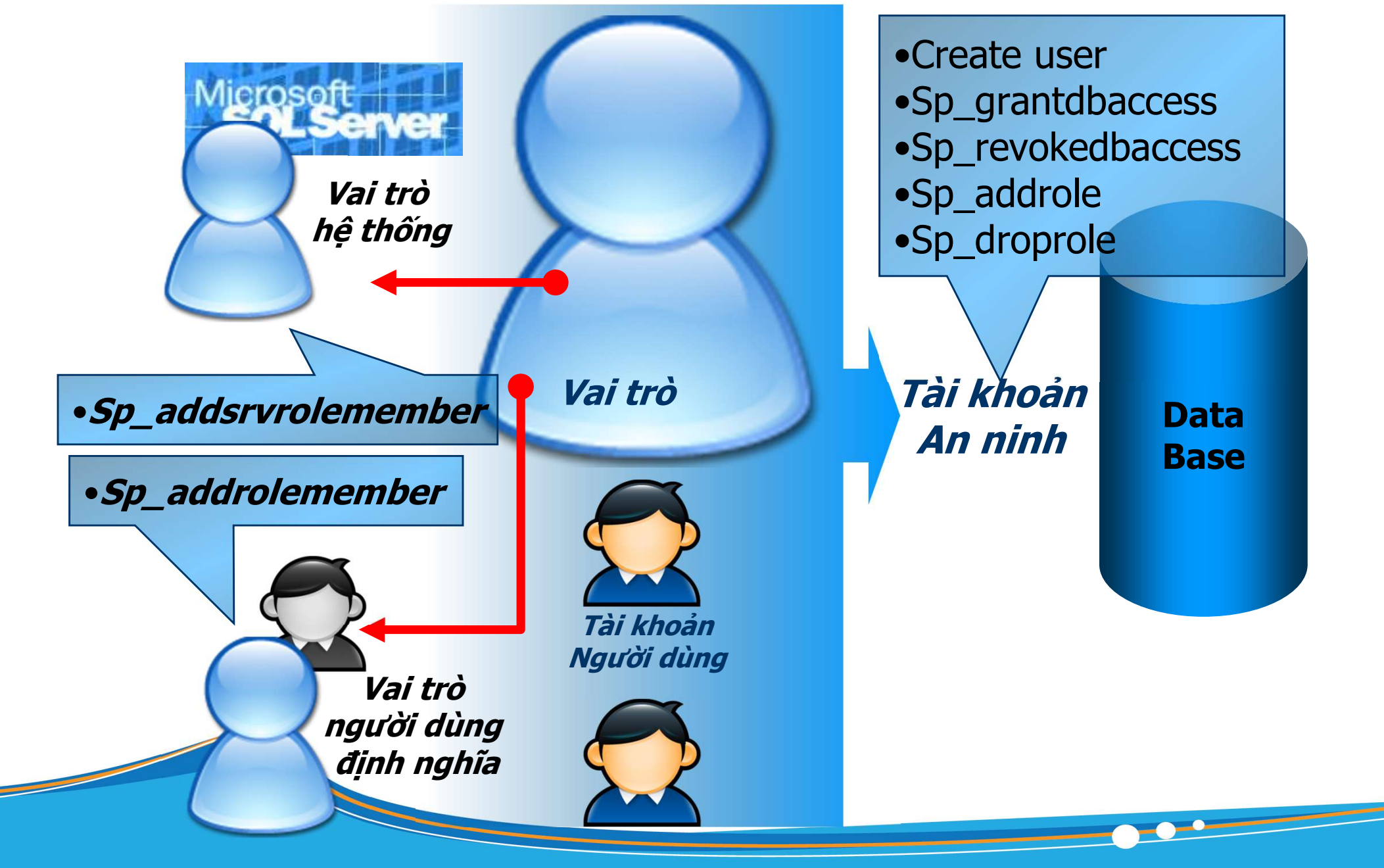
- ❖ SQL Server tự quản lý tên tài khoản (login name) và mật khẩu (password)
- ❖ SQL Server thực hiện việc kiểm tra tài khoản (kiểm tra login name, so khớp password) khi người dùng đăng nhập (mở kết nối) vào SQL Server.



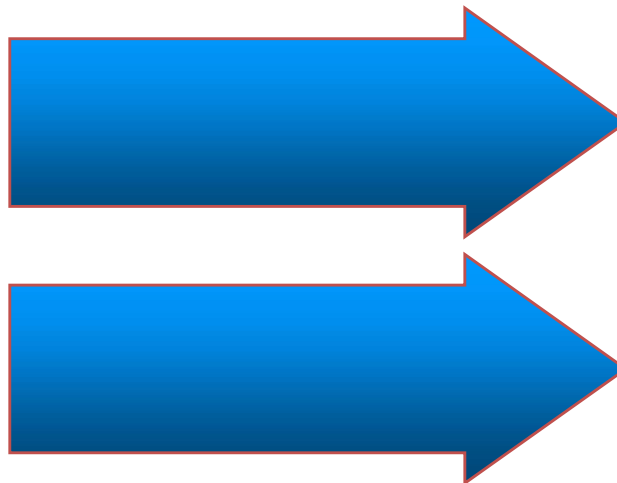




Role



Quyền người dùng



•Bảng DL

•*Thuộc tính*

•*Bộ*

•Ràng buộc

•*Khóa chính*

•*Khóa ngoại*

•*Check*

•*Unique*

•*Default...*



Tài khoản
Người dùng



•Thủ tục TT

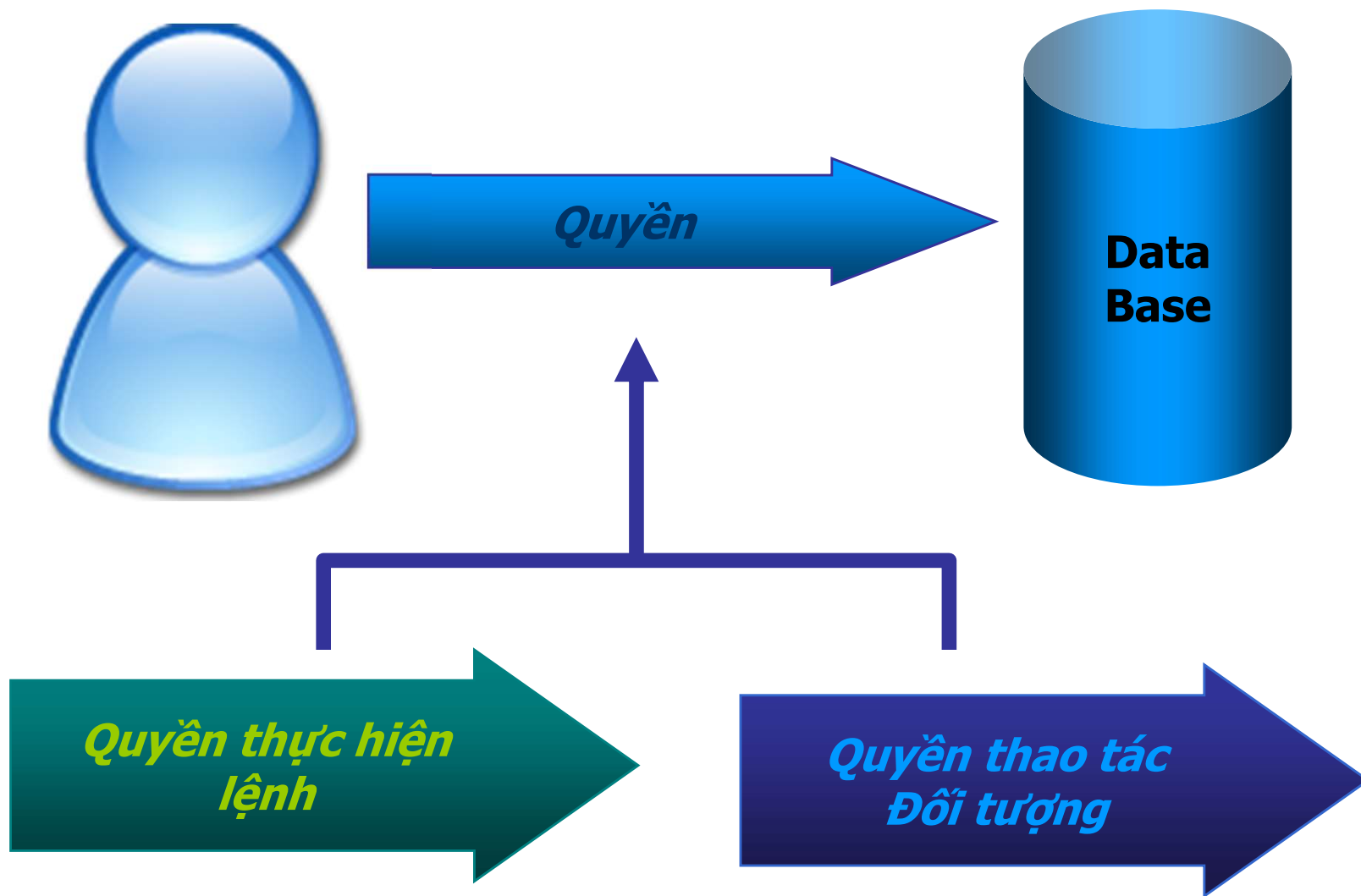
•Hàm người dùng

•Luật

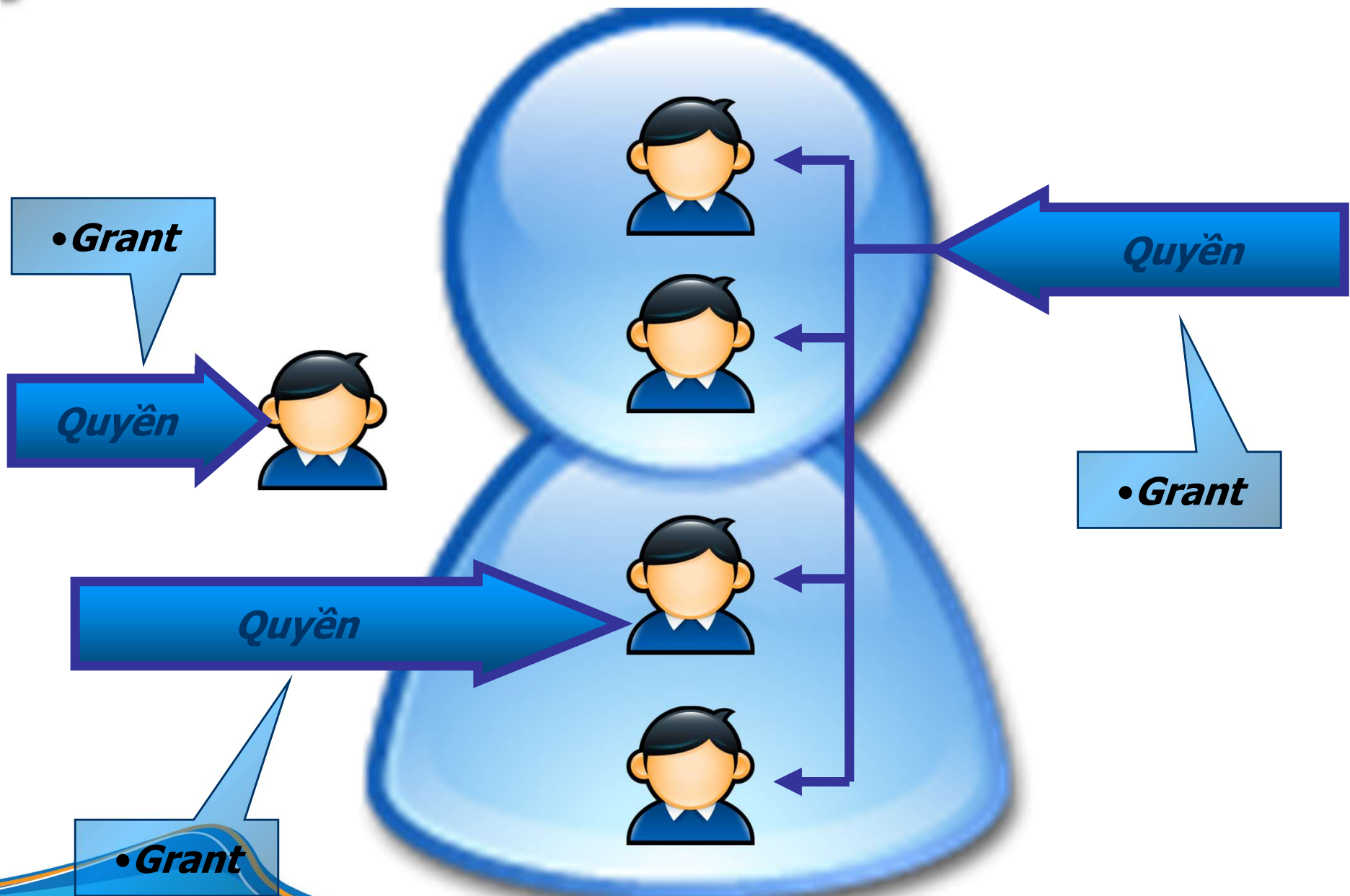
•...



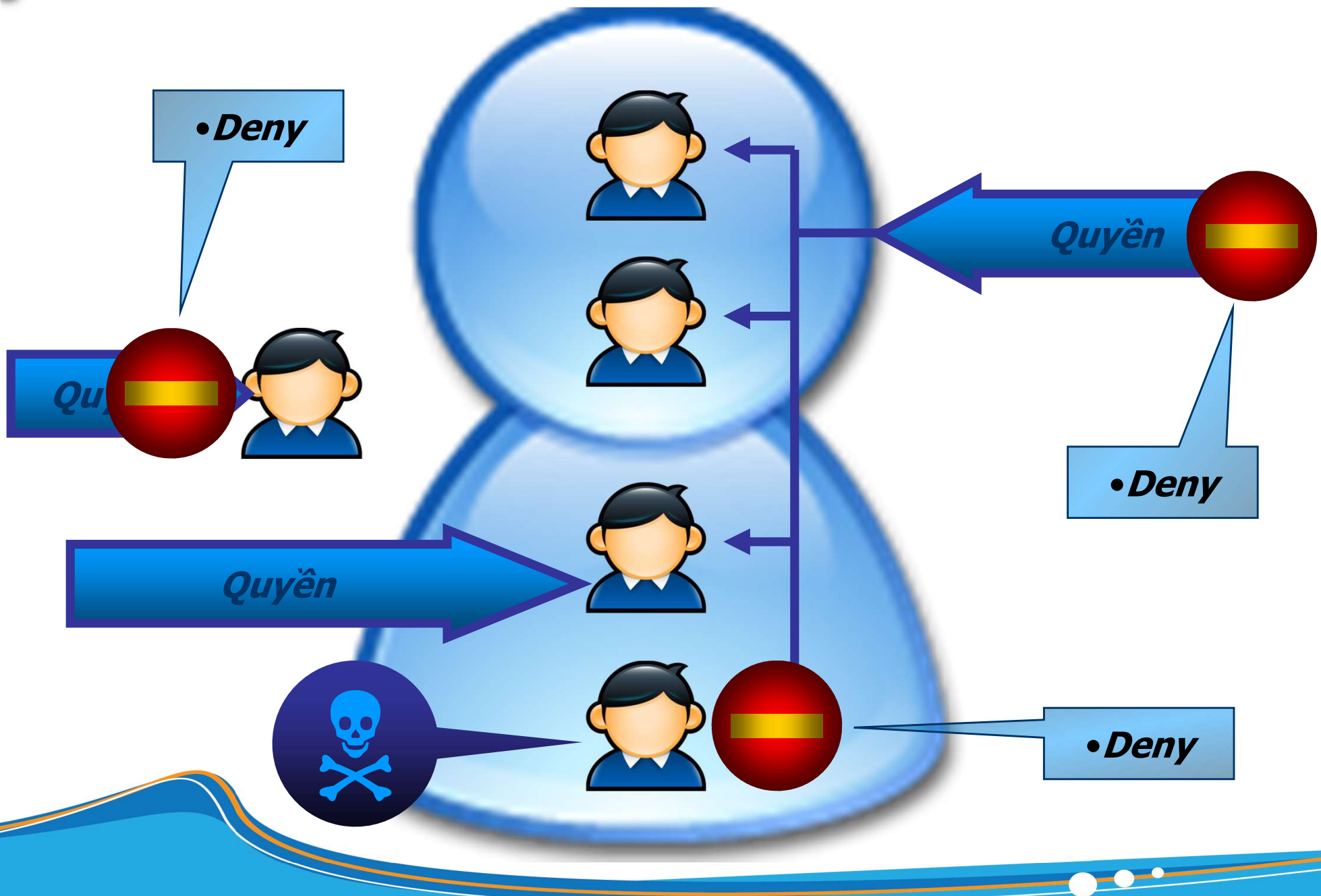
Quyền người dùng



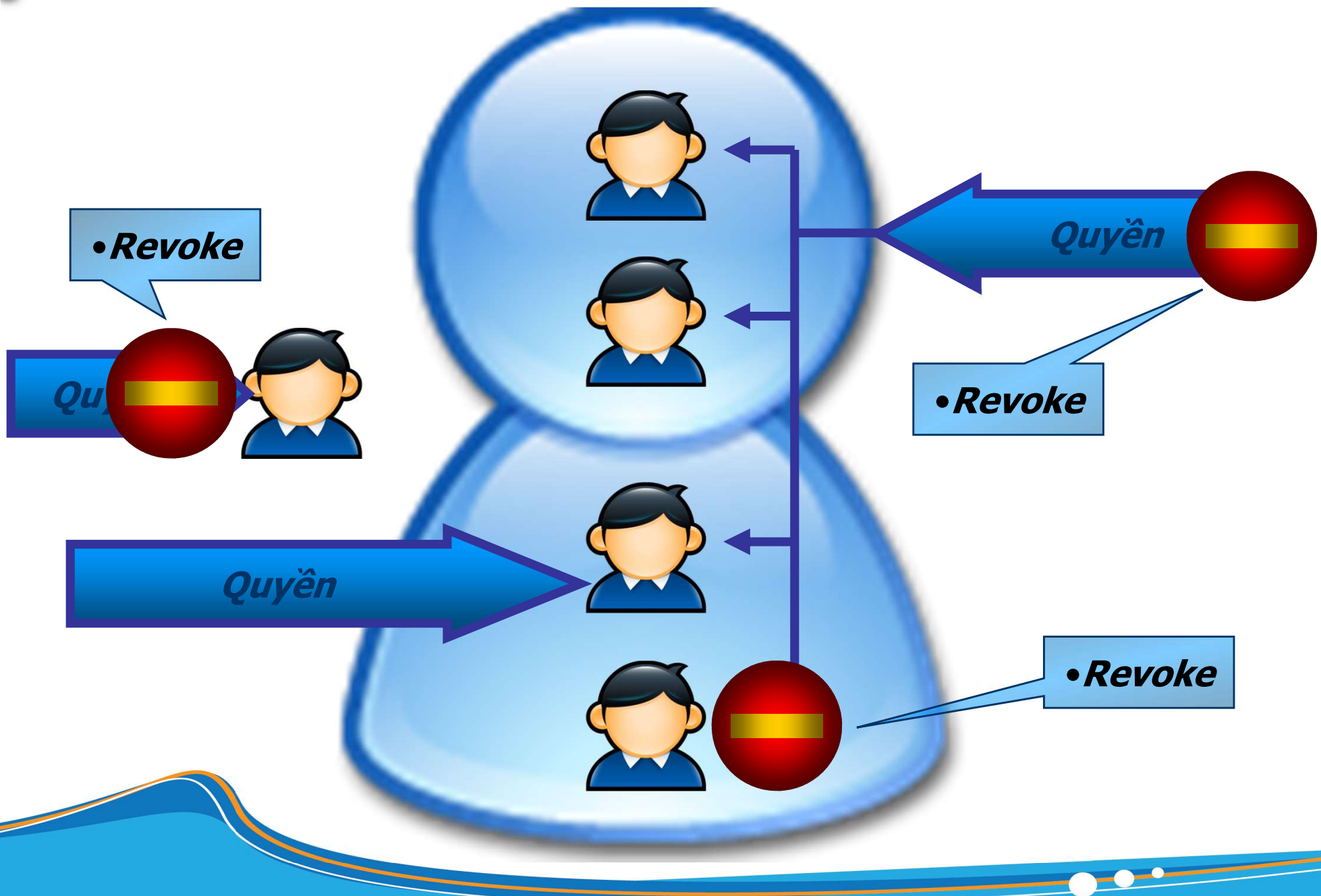
Cấp quyền



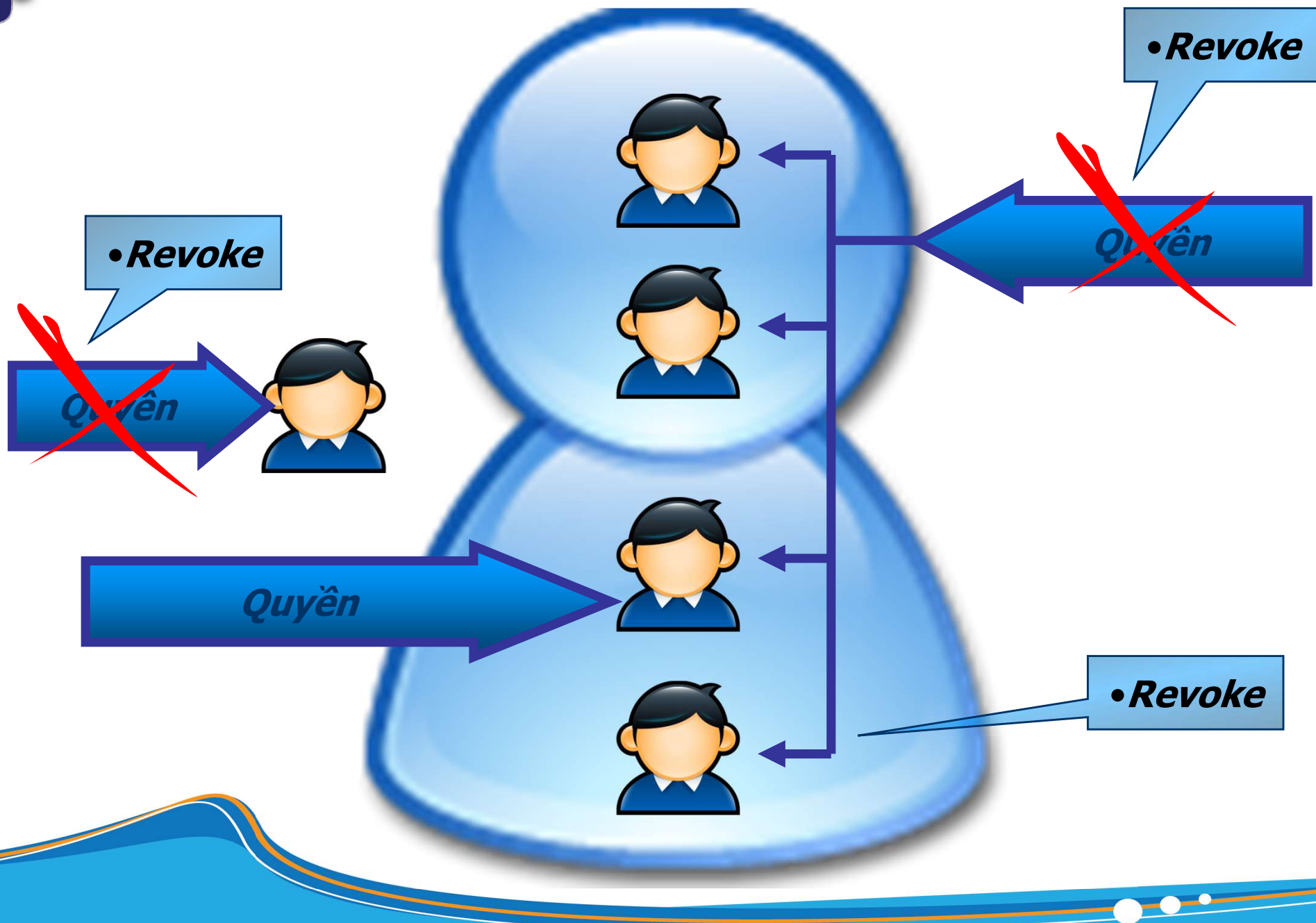
Cấm quyền



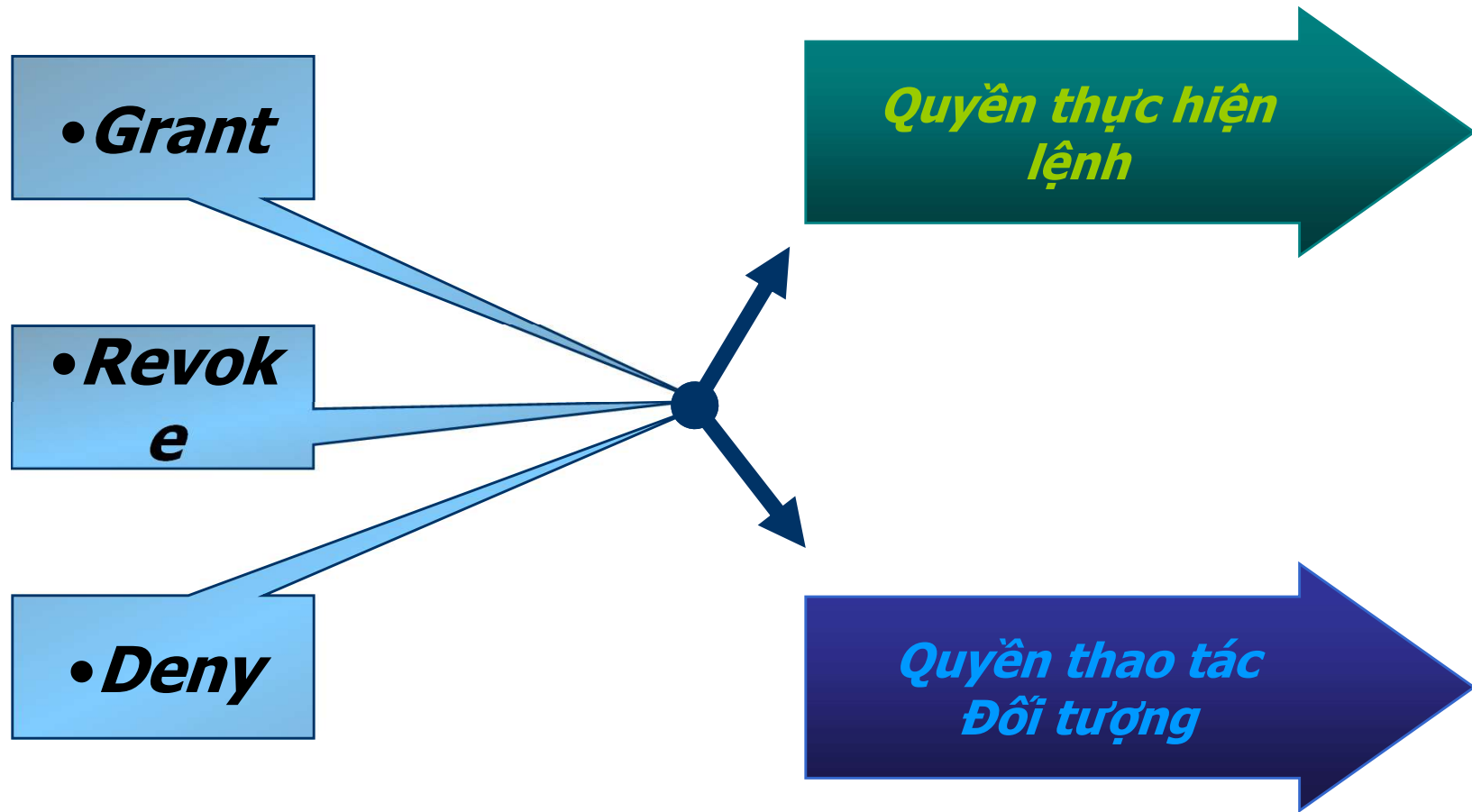
Khôi phục quyền



Hủy quyền



Quyền người dùng



Login

- ❖ Tài khoản mà người sử dụng dùng để kết nối với SQL Server
- ❖ Một login có thể có quyền truy cập vào 0-n database
- ❖ Trong mỗi database, login ứng với một user



SA Login

- ❖ Viết tắt của **system administrator**, là tài khoản do SQL Server cấp phát lúc cài đặt.
- ❖ SA login được phép thao tác trên tất cả các đối tượng của SQL server.



Một số thủ tục trên Login

- ❖ Sp_addlogin — **Thêm login mới**
- ❖ Sp_grantlogin — **Cấp quyền cho login**
- ❖ Sp_droplogin — **Xóa login**
- ❖ Sp_revokelogin — **Hủy quyền đã cấp cho login**
- ❖ Sp_password — **Thay đổi password của login**

Login

- ❖ Login được cấp và quản lý bởi quản trị hệ thống hoặc quản trị an ninh của SQL Server (sysadmin/securityadmin)
- ❖ Lệnh tạo login (SQL Server authentication)

```
sp_addlogin [ @loginame = ] 'login_name'  
[ , [ @passwd = ] 'password' ]  
[ , [ @defdb = ] 'default_database' ]
```

Ví dụ :

```
exec sp_addlogin 'Nam', 'hehe', 'QLSV'
```

Login

❖ Đổi password login

■ Cú pháp:

```
sp_password [[@old =] 'old_pass',]  
{[@new =] 'new_pass'} [,[@loginame =]  
'login']
```

■ Ví dụ:

```
exec sp_password null,'123','login_name'
```

Login

- ❖ Lệnh cấp quyền truy cập (grant login)
 - Cấp phép một hoặc một nhóm người dùng của Windows (Windows user/ group) được kết nối đến SQL Server.
 - Cú pháp:
`sp_grantlogin` [`@loginame` =]
`'windows_account'`
(*windows_account có dạng Domain\User*)
 - Ví dụ:
`exec sp_grantlogin 'Server01\user01'`

Login

- ❖ Hủy quyền của login
 - Lấy lại quyền truy cập đã cấp cho một người dùng/ nhóm người dùng của Windows bằng thủ tục `sp_grantlogin`
 - Cú pháp:
`sp_revokelogin` [*@loginname=*] '*login*'
 - Ví dụ:
`exec sp_revokelogin` '*login_name*'

Login

❖ Xóa login

■ Cú pháp:

`sp_droplogin` [`@loginame =`] *'login_name'*

■ Ví dụ:

`exec` `sp_droplogin` *'login_name'*

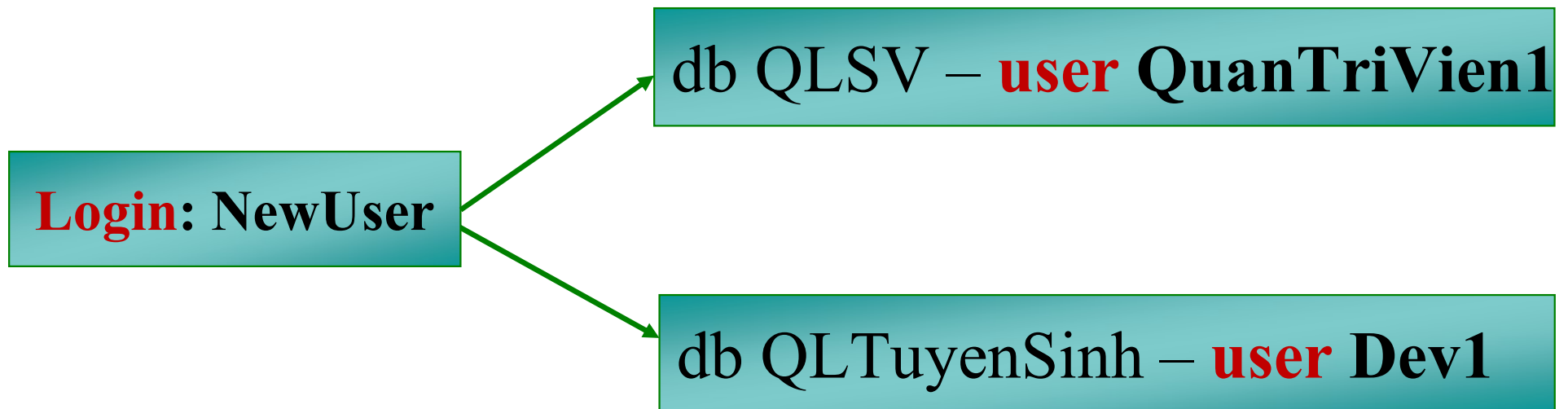


Login

- ❖ Đổi database mặc định của login
 - Áp dụng cho login đã được ánh xạ vào một user trong CSDL đã khai báo mặc định.
 - Cú pháp:
`sp_defaultdb` [`@loginame =`] '*login_name*',
[`@defdb=`] '*database_name*'
 - Ví dụ:
`exec` `sp_defaultdb` '*login_name*', '*QLSV*'

User

- ❖ Một “người dùng” trong một database cụ thể
- ❖ Một user ứng với một login



Database User

❖ Dbo user

- Là owner của tất cả các đối tượng trong CSDL.
- SA login và Win login có server role là sysadmin sẽ được ánh xạ vào dbo.

❖ Guest user

- Là user được định nghĩa trong CSDL.
- Một login được ánh xạ là guest khi thỏa điều kiện sau:
 - ✓ Login connect vào SQL server được nhưng không truy cập vào CSDL được.
 - ✓ CSDL này đã có user guest.

User

- ❖ Tạo user = cấp cho một login quyền truy cập vào database hiện hành
- ❖ Cú pháp:

sp_grantdbaccess [@loginname
=] 'login_name'
[,[@name_in_db =] 'user_name']

- Thủ tục ***sp_grantdbaccess*** chỉ có thể được thực hiện bởi thành viên của vai trò *sysadmin*, *db_owner* và *db_accessadmin*
- Thủ tục ***sp_grantdbaccess*** có thể bị bỏ đi trong tương lai

User

❖ Ví dụ

Exec sp_grantdbaccess 'Nam', 'dev01'

Exec sp_grantdbaccess 'Server01\user01', 'dev02'



User

- ❖ Lệnh tạo user khác (được khuyến khích dùng thay cho *sp_grantdbaccess*)
- ❖ Cú pháp :

```
CREATE USER user_name  
[ { FOR | FROM } { LOGIN login_name }]  
[ WITH DEFAULT_SCHEMA =schema_name ]
```

❖ Ví dụ :

Create User dev01 For Login Nam

Create User dev02 From Login Nam With
Default_Schema = NhanVien

User

❖ Xóa user khỏi database hiện hành

- Cú pháp:

sp_revokedbaccess '*user_name*'

- Ví dụ:

Exec sp_revokedbaccess '*dev02*'



❖ Sau khi tạo user, user có quyền truy cập vào database, nhưng chưa được thao tác gì (đọc, cập nhật, ...) trên các đối tượng trong database.

⇒ *Cần gán những quyền cụ thể cho từng user của database*

❖ Nếu nhiều user được cấp một số quyền giống nhau:

⇒ *Tạo role, gán các quyền cho role, user cần các quyền này sẽ là thành viên của role*



Role

- ❖ **Role = Nhóm các user cùng quyền**
 - Mặc định, các user thành viên của role sẽ được hưởng tất cả những quyền đã cấp cho role.
 - Tuy nhiên, các thành viên này cũng có thể được cấp thêm các quyền riêng, hoặc bị từ chối một số quyền thừa hưởng từ role.





Fixed Server Roles

Role	Mô tả
Sysadmin	Có quyền tương đương sa (Full quyền)
Serveradmin	Có quyền cấu hình và shut down server
Setupadmin	Có quyền add và remove các linked server.
Securityadmin	Có quyền quản lí SQL login (đổi hoặc reset pass, Grant, Revoke và Deny quyền ở mức Server và Database)
Processadmin	Có quyền quản lí và kết thúc các tiến trình trên SQL Server
Dbcreatetor	Có quyền create, drop, alter và restore bất kì CSDL nào trên Server
diskadmin	Có quyền quản lí các file trên đĩa của server và tất cả các CSDL

Fixed Database Roles

Role	Mô tả
Db_owner	Có mọi quyền trên CSDL. Dbo mặc định được gán role này.
Db_accessadmin	Có quyền add hoặc remove các truy cập của Windows logins, Windows groups và SQL Server login
Db_datareader	Có quyền đọc dữ liệu từ các bảng của CSDL
Db_datawriter	Có quyền ghi dữ liệu xuống các bảng của CSDL
Db_securityadmin	Có quyền quản lí các quyền và role trong CSDL



Role

- ❖ Người dùng có thể định nghĩa các vai trò mới cho database hiện hành
- ❖ Cú pháp

```
sp_addrole [ @rolename = ] 'role'  
[ , [ @ownername = ] 'owner' ]
```

*(thủ tục **sp_addrole** chỉ có thể thực hiện bởi thành viên của sysadmin, db_owner, db_securityadmin)*



❖ Ví dụ:

Exec **sp_addrole** 'Developer'

Exec **sp_addrole** 'Developer', 'dbo'

Ghi chú: Khi một login là thành viên của vai trò quản trị hệ thống (sysadmin) vào SQL Server, login này có quyền truy cập vào tất cả các database và có tên user tương ứng trong từng database là “dbo”

❖ Xoá một role đã tạo: **sp_droprole** 'role'

❖ Thêm một login vào các vai trò hệ thống có sẵn:

■ Cú pháp:

```
sp_addsrvrolemember [ @loginame = ] 'login'  
                , [ @rolename = ] 'role'
```

■ Ví dụ:

```
Exec sp_addsrvrolemember 'newuser', 'sysadmin'
```

❖ Ghi chú: *Khi mới cài đặt, SQL Server định nghĩa sẵn login sa, sa và các login là administrator của Windows (Windows Authentication) đều là thành viên của sysadmin.*

Cấp quyền

- ❖ Sử dụng lệnh “Grant...” để cấp quyền cho user / role
- ❖ Có hai dạng:
 - Cấp quyền thực hiện lệnh (create database, create procedure, create table,...)
 - Cấp quyền thao tác trên các đối tượng trong CSDL (đọc/ ghi trên table/view, thực hiện thủ tục,...)



Cấp quyền

❖ Cấp quyền thực hiện lệnh :

■ Cú pháp:

GRANT { **ALL** | *statement* [,...*n*] }
TO *security_account* [,...*n*]

Trong đó:

- Statement = create database| create table| create view| create rule| create procedure| backup database|...
- Security_account = user| role

■ Ví dụ:

GRANT create table, create procedure **to** dev01



Cấp quyền

❖ Cấp quyền thao tác trên đối tượng :

■ Cú pháp

GRANT

{ ALL | *permission* [,...*n*] }
{ [(*column* [,...*n*])] ON { *table* | *view* }
| ON { *table* | *view* } [(*column* [,...*n*])]
| ON { *stored_procedure* }
| ON { *user_defined_function* }
}

TO *security_account* [,...*n*]
[WITH GRANT OPTION]
[AS *role*]

Cấp quyền

❖ Cấp quyền thao tác tr

■ Cú pháp

GRANT

```
{ ALL | permission [ ,...n ] }
{ [ ( column [ ,...n ] ) ] ON { table | view }
| ON { table | view }
| ON { stored_procedure }
| ON { user_defined_function }
}
```

```
TO security_account [ ,...n ]
[ WITH GRANT OPTION ]
[ AS role ]
```

Permission = select| insert| delete|
references|update| execute

WITH GRANT OPTION : cho
phép user được cấp các quyền
thao tác này cho user/ role khác.

As role: lệnh cấp quyền được thực hiện
với tư cách là thành viên của “role”

Cấp quyền

❖ Ví dụ 1:

Grant select, update
on SinhVien (HoTen, DiaChi, NgaySinh)
to Developer

Thành viên của
Developer có quyền
select, update trên
các cột HoTen,
DiaChi và NgaySinh
của bảng SinhVien

Nhưng
không được
cấp quyền
này cho user
khác

Cấp quyền

❖ Ví dụ 2:

Grant select, update
on SinhVien (HoTen, DiaChi, NgaySinh)
to Developer
with grant option

Thành viên của
Developer có quyền
select, update trên
các cột HoTen,
DiaChi và NgaySinh
của bảng SinhVien

Và được phép
cấp quyền này
cho user khác
dưới danh nghĩa
của Developer

Cấm quyền

- ❖ Dùng **Deny** để thu hồi quyền của một user/role
 - Khi một user/role bị thu hồi một quyền, nó sẽ không được thừa hưởng quyền này dù là thành viên của một role có quyền đó
 - Có hai dạng tương tự như Grant:
 - Thu hồi quyền thực hiện lệnh
 - Thu hồi quyền thao tác trên đối tượng

Cấm quyền

❖ Thu hồi quyền thực hiện lệnh

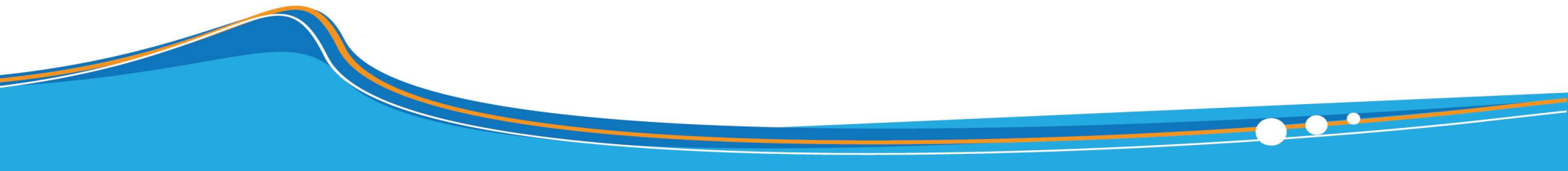
■ Cú pháp:

DENY { ALL | *statement* [,...*n*] }

TO *security_account* [,...*n*]

■ Ví dụ:

Deny create table **to** Dev02



Cấm quyền

❖ Thu hồi quyền thao tác trên đối tượng

■ Cú pháp:

DENY

```
{ ALL | permission [ ,...n ] }  
{ [ ( column [ ,...n ] ) ] ON { table | view }  
  | ON { table | view } [ ( column [ ,...n ] ) ]  
  | ON { stored_procedure }  
  | ON { user_defined_function }  
}
```

TO *security_account* [,...*n*]

[**CASCADE**]

Cấm quyền

❖ Thu hồi quyền thao tác trên đối tượng

■ Ghi chú:

Nếu *security_account* được cấp (grant) trực tiếp quyền này với “**with grant option**”, phải chỉ định **cascade** khi **deny** (từ chối quyền này đối với tất cả user/role đã được *security_account* cấp quyền này)

■ Ví dụ:

Deny select, update

on SinhVien (HoTen, DiaChi, NgaySinh)

to Dev02 **cascade**

Hủy quyền

- ❖ Dùng *revoke* để lấy lại quyền đã cấp
 - Nếu user/ role được cấp (grant) hoặc đang bị thu hồi (deny) một quyền, revoke quyền này sẽ làm mất hiệu lực của lệnh trước đó
- ❖ Có hai dạng tương tự như grant
 - Quyền thực hiện lệnh
 - Quyền thực hiện thao tác trên đối tượng



Cấp lại quyền

❖ Lấy lại / bỏ thu hồi quyền thực hiện lệnh

- Cú pháp:

REVOKE { ALL | *statement* [,...*n*] }

From *security_account* [,...*n*]

- Ví dụ:

Revoke create table **from** Dev02

Cấp lại quyền

❖ Lấy lại / bỏ thu hồi quyền thao tác đối tượng

■ Cú pháp

```
REVOKE { ALL | permission [ ,...n ] }  
    { [ ( column [ ,...n ] ) ] ON { table | view }  
      | ON { table | view } [ ( column [ ,...n ] ) ]  
      | ON { stored_procedure }  
      | ON { user_defined_function }  
    }  
FROM security_account [ ,...n ]  
[ CASCADE ]  
[ AS role ]
```

Cấp lại quyền

- ❖ Lấy lại / bỏ thu hồi quyền thao tác đối tượng

- Ví dụ:

Revoke select, update

on SinhVien (HoTen, DiaChi, NgaySinh)

from Dev02

Revoke update

on SinhVien (HoTen, DiaChi, NgaySinh)

from Developer **cascade**

Bài tập

Hệ thống quản lí sinh viên gồm:

SinhVien (**MaSV**, HoTen, NamSinh, GioiTinh, DiemTB, MaLop)

GiaoVien (**MaGV**, HoTen, NgaySinh, LoaiGV)

MonHoc (**MaMH**, TenMH, SoChi)

KetQua (**MaSV**, **MaMH**, **LanThi**, Diem)

Lop (**MaLop**, NamBD, NamKT, SiSo)

GV_Lop (**MaLop**, **MaMH**, MaGV)



Yêu cầu

1. Tạo login cho GV01, GV02, GV03, SV01, SV02, SV03.
2. Sinh viên chỉ được được cấp quyền xem, cập nhật thông tin cá nhân của mình (tạo view).
3. Tạo 2 nhóm vai trò GiaoVien, QuanLi.
4. GV01 thuộc nhóm quản lí, GV02, GV03 thuộc nhóm giáo viên.
5. Giáo viên được xem thông tin tất cả môn học.
6. Giáo viên được thêm một kết quả và cập nhật điểm của môn học do mình phụ trách.
7. Quản lí được xem, cập nhật, thêm thông tin môn học, sinh viên và được phép cấp các quyền cho user khác.

Yêu cầu

1. Tất cả các sinh viên đều được phép xem thông tin các môn học hiện có ở trường.
2. Giáo viên GV03 không còn giảng dạy ở trường. Hãy hủy các quyền đã cấp cho GV03.
3. Cấm quyền truy cập thông tin của SV03.
4. Thêm GV01 vào nhóm sysadmin.
5. Có thể cập nhật lại mật khẩu của login GV03 thành '111111' được không? Ai được phép thực hiện?
6. Cấp toàn quyền thao tác trên CSDL cho GV01.
7. Cấp quyền thực thi các thủ tục usp_TinhDiem cho GV02.

