

*Trường Đại học Khoa học Tự nhiên*

*Khoa Công nghệ Thông tin*

*Bộ môn Hệ thống Thông tin*

## *Quản trị Cơ sở Dữ liệu*

# *Chương V :* **AN NINH VÀ AN TOÀN DL**

**GV : TUẤN NGUYỄN HOÀI ĐỨC**

**E-mail : [tnhduc@fit.hcmus.edu.vn](mailto:tnhduc@fit.hcmus.edu.vn)**

# Nội dung trình bày

- ◆ Tìm hiểu thêm về Trigger
- ◆ Khung nhìn
- ◆ Quản trị quyền người dùng
  - ***Tổng quan***
  - ***Chi tiết***
- ◆ Sao lưu và phục hồi dữ liệu



# Tìm hiểu thêm về trigger

- ◆ Xem lại cú pháp khai báo trigger :

*Create trigger* **tên\_trigger**

*On* {**tên\_bảng/tên\_view**}

{*For/ After/ Instead of* }

{ [*delete*] [,] [*insert*] [,] [*update*] }

*As*

{ **các lệnh**

*go*

Trigger được gọi thực hiện **thay cho** thao tác delete/ insert/ update tương ứng

- Các dòng mới được thêm **chỉ** chứa trong bảng inserted
- Các dòng bị chỉ định xoá nằm đồng thời trong bảng deleted và bảng dữ liệu (dữ liệu không bị xoá).



# Tìm hiểu thêm về trigger

## ❖ Lưu ý:

- **Lệnh tạo trigger phải là lệnh đầu tiên trong một query batch**
- **Trên một bảng có thể định nghĩa nhiều trigger *for/after* cho mỗi thao tác...**
- **...nhưng chỉ có thể định nghĩa một trigger *instead of* cho mỗi thao tác**



# Tìm hiểu thêm về trigger

## ❖ Lưu ý:

- Không thể định nghĩa trigger instead of update/ delete trên bảng có cài đặt khoá ngoại dạng update cascade/ delete cascade
- Trong thân trigger, có thể sử dụng hàm ***Update(tên\_cột)*** để kiểm tra xem việc cập nhật/ insert được thực hiện trên cột nào.
  - $\text{Update(tên\_cột)} = \text{true}$  : *có thực hiện cập nhật trên cột tên\_cột*



# Nội dung trình bày

- ◆ Tìm hiểu thêm về Trigger
- ◆ Khung nhìn
- ◆ Quản trị quyền người dùng
  - ***Tổng quan***
  - ***Chi tiết***
- ◆ Sao lưu và phục hồi dữ liệu



# Khung nhìn

- ❖ **Khái niệm :** View (khung nhìn) là một bảng ảo được định nghĩa bởi một lệnh select
  - ***Đối với người dùng: view giống như một bảng thật***
  - ***Dữ liệu của view là dữ liệu trong một hoặc nhiều bảng thật (view không chứa dữ liệu thật sự)***
  - ***Sự thay đổi dữ liệu tương ứng trong các bảng thật luôn được phản ánh lên view***



# Khung nhìn

## ❖ Mục đích sử dụng:

- ***Thể hiện dữ liệu ở dạng phù hợp với từng nhóm nghiệp vụ/ nhóm NSD.***
- ***Bảo mật dữ liệu(security).***



# Khung nhìn

❖ Cú pháp:

*Create view* **view\_name**

**[(column\_name [ ,...n ])]**

**[With Schemabinding]**

**As**

**select\_statement**



# Khung nhìn

## ❖ Cú pháp:

*Create view view\_name  
[(column\_name) ...]  
[With Schema Binding]  
As*

select

### Gắn kết view với lược đồ, khi đó:

- Không thể xóa bảng hay view khác có liên quan đến định nghĩa của view có schemabinding
- Không thể thay đổi cấu trúc bảng/ view nếu việc thay đổi này ảnh hưởng đến định nghĩa view có schemabinding
- Câu select định nghĩa view phải chỉ định rõ thuộc tính (không được **select \***)
- Các tên bảng, view trong câu select phải được viết dưới dạng **owner.Tênbảng/Tênview**
- Nếu view schemabinding định nghĩa trên một view khác, view đó cũng phải ở dạng **schemabinding**.



# Khung nhìn

◈ Ví dụ :

*Create view*

*ThiSinh\_Nganh*

*(SBD, HoTen, MaNganh, TenNganh)*

*as*

*select*

*ts.SBD, ts.HoTen, ts.Nganh, n.TenNganh*

*from ThiSinh ts, Nganh n*

*where ts.Nganh = n.MaNganh*



# Khung nhìn

## ♦ Lưu ý :

- **Lệnh select trong định nghĩa view không được chứa:**
  - *Order by*, nếu có phải kèm với *TOP*
  - *Compute/ compute...by*
  - *Select into*
- **Không thể gắn kết rule hay default vào view**
- **Không thể khai báo trigger for/after trên view (chỉ có thể khai báo trigger instead of)**
- **Một view có thể được định nghĩa trên một view khác, nhưng không quá 32 cấp**



# Khung nhìn

- ❖ Truy xuất dữ liệu từ view (select)
  - ***Như truy xuất trên bảng***
- ❖ Cập nhật dữ liệu (insert/ delete/ update)
  - ***Dùng các lệnh insert / delete / update tương tự như thao tác trên bảng.***
  - ***Dữ liệu sẽ được cập nhật trong các bảng dữ liệu thật sự bên dưới view***



# Khung nhìn

◆ View chỉ có thể được cập nhật (insert/ update/ delete) nếu:

• ***lệnh select định nghĩa view không chứa:***

- Các hàm tổng hợp (count, sum, avg, max,...)
- Group by, Top, select distinct
- Union (trừ partitioned view)
- Cột dẫn suất (tính toán từ các cột dữ liệu thật sự) (trong một số trường hợp có thể xóa được)



# Khung nhìn

- *Trong mệnh đề from của lệnh select phải tham chiếu đến ít nhất một bảng ( hoặc view với dữ liệu được lấy từ bảng), và phải select ít nhất một cột từ dữ liệu.*
- *Lệnh cập nhật phải viết sao cho chỉ làm thay đổi dữ liệu thật sự trong một bảng (lệnh xóa chỉ thực hiện được nếu view chỉ tham chiếu đến đúng một bảng)*
- *Không thỏa các điều kiện trên, nhưng có trigger instead of for insert/ update/ delete tương ứng*



# Khung nhìn

❖ Ví dụ: Các view định nghĩa như sau không thể cập nhật được:

- **Create view V\_SoNV**

**As Select MaPhong, Count (\*) as SoNV**

**From NhanVien**

**Group by MaPhong**

- **Create View V\_NhanVien**

**As select MaNV, HoNV + ' ' + TenNV as HoTen**

**From NhanVien**

- **Create View V1**

**As select getdate() as NgayHienHanh**

Có thể  
xóa



## Khung nhìn

- ❖ Có thể dùng trigger instead of để cập nhật view
- ❖ Ví dụ: Viết trigger instead of để cho phép insert trên view V\_NhanVien



# Khung nhìn

```
create trigger tr_Ins_View_NV  
on V_NhanVien  
instead of insert  
as
```

```
insert into NhanVien (MaNV, HoNV, TenNV)  
select MaNV, left(TenNV, charindex(' ',TenNV)),  
right(TenNV,len(TenNV) - CharIndex(' ',TenNV))  
from inserted
```

```
go
```



## Khung nhìn có chỉ mục (Indexed View)

- ❖ Dùng khi dữ liệu của view lớn, truy xuất thường xuyên
- ❖ Cài đặt một cluster index trên view → view trở thành index view
  - *Dữ liệu và index của view được lưu trữ lại như một bảng*
  - *Có thể định nghĩa thêm các chỉ mục nonclustered trên indexed view*
  - *View phải được khai báo với schemabinding*



# Khung nhìn

## ❖ Thay đổi cấu trúc view:

*Thay từ khóa **create** trong các lệnh tạo view bằng từ khóa **alter***

## ❖ Xóa view

*Drop view **tên\_view\_cần\_xóa** [...n]*

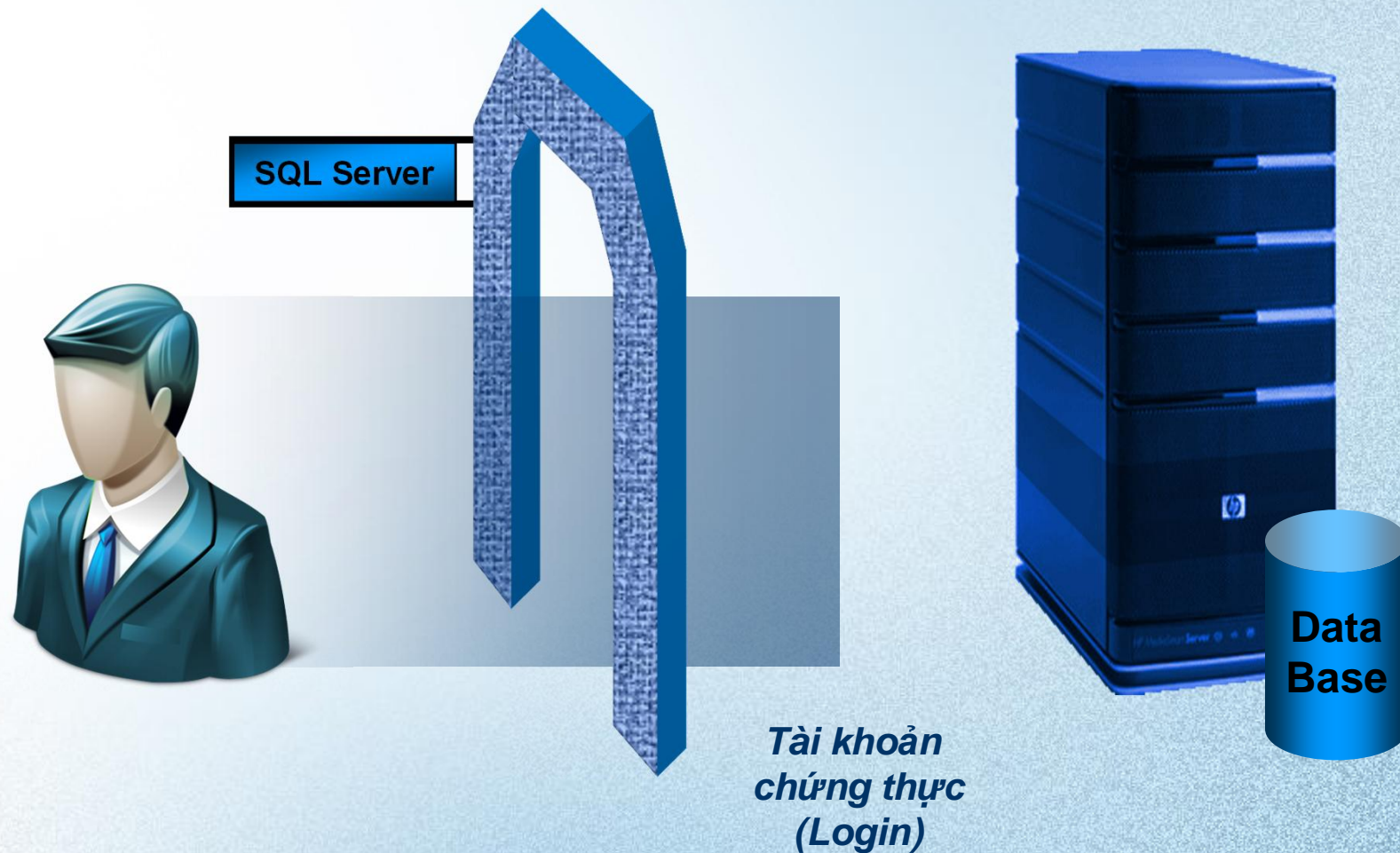


# Nội dung trình bày

- ◆ Tìm hiểu thêm về Trigger
- ◆ Khung nhìn
- ◆ Quản trị quyền người dùng
  - **Tổng quan**
  - **Chi tiết**
- ◆ Sao lưu và phục hồi dữ liệu

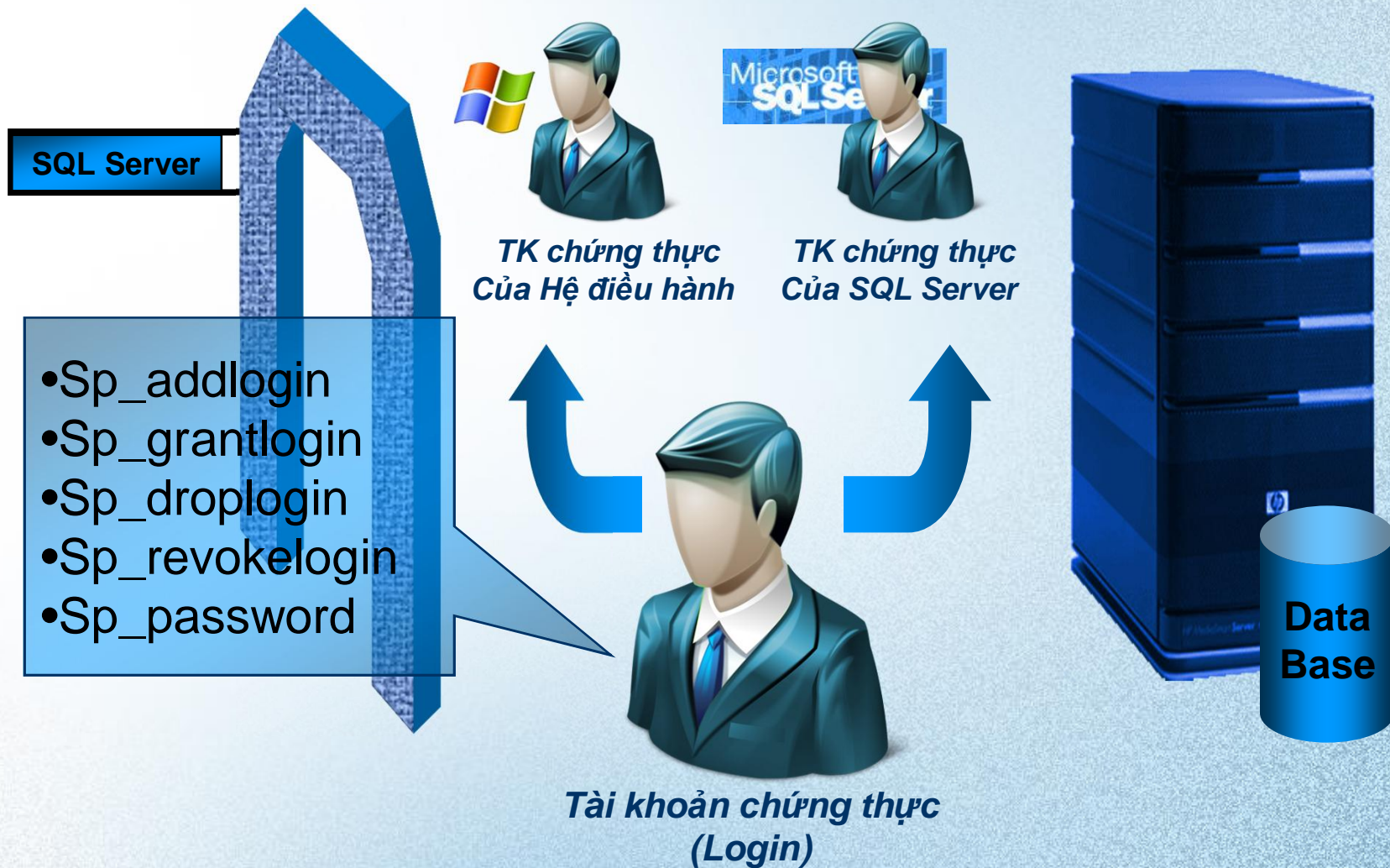


# Tổng quan



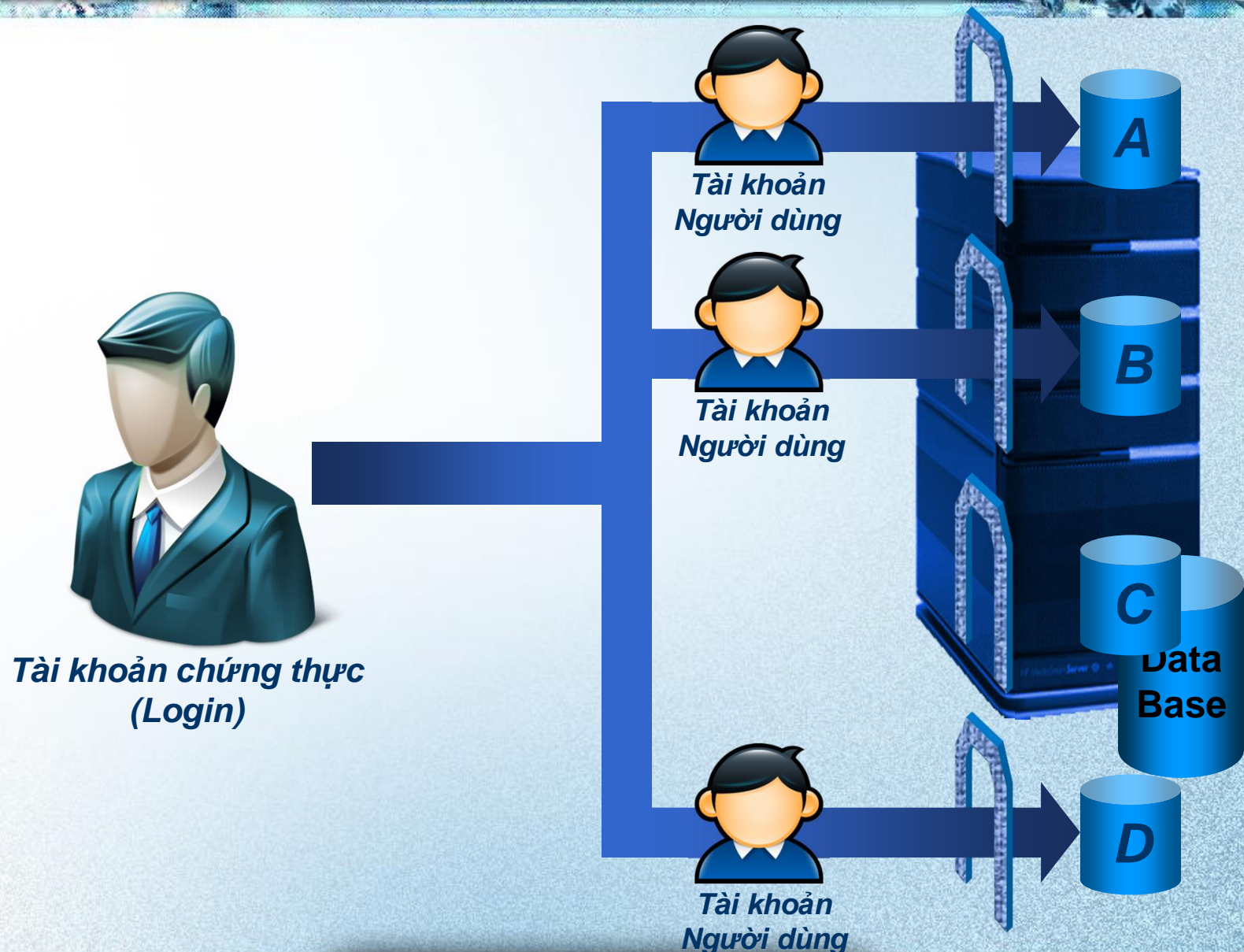


# Tổng quan



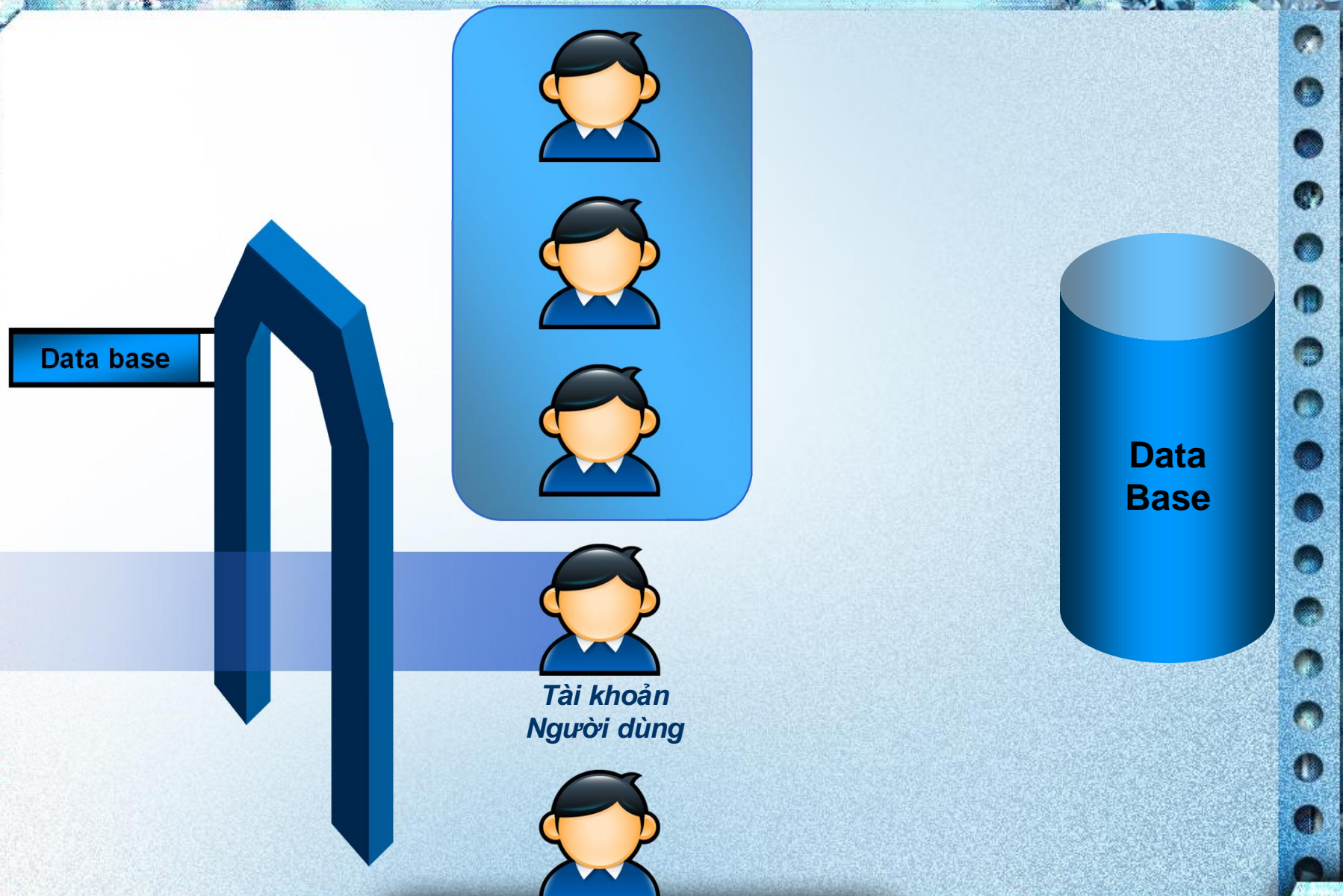


# Tổng quan



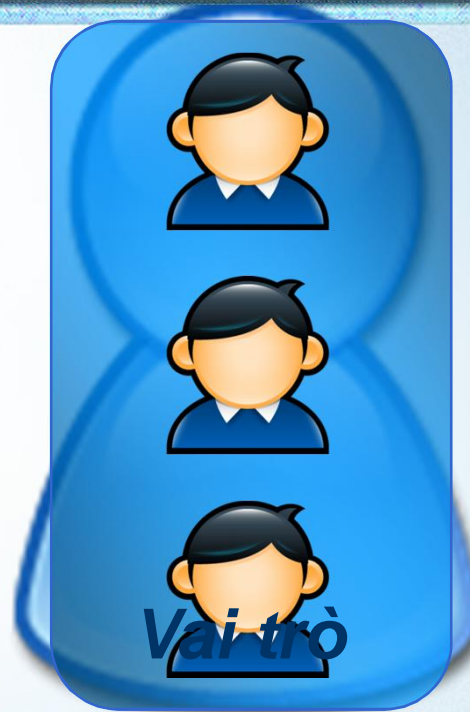


# Tổng quan





# Tổng quan

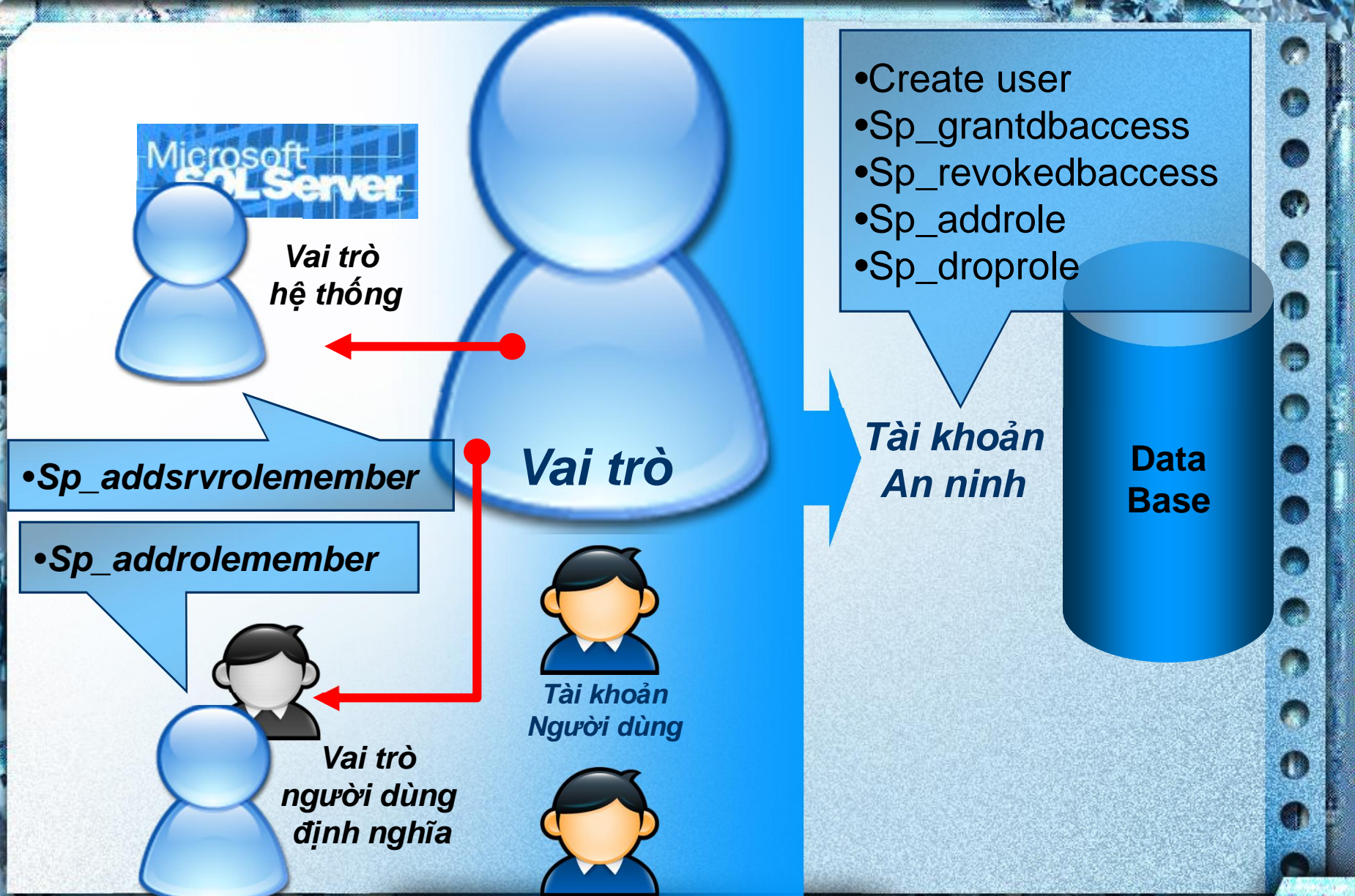


Tài khoản  
Người dùng





# Tổng quan





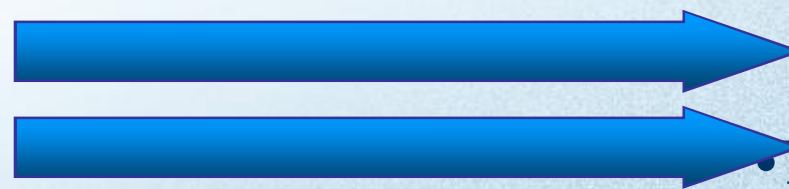
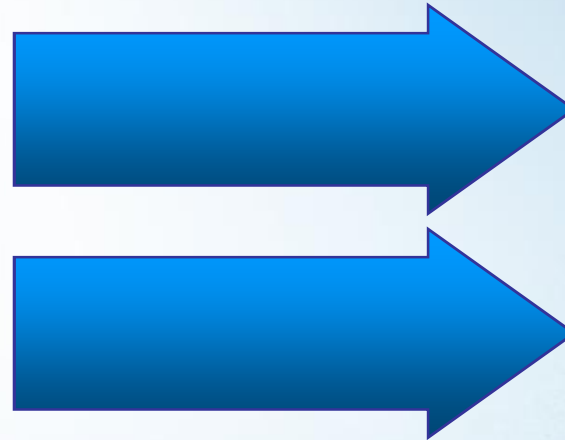
# Tổng quan



- Bảng DL
  - Thuộc tính
  - Bộ
- Ràng buộc
  - Khóa chính
  - Khóa ngoại
  - Check Data Base
  - Unique
  - Default...
- Thủ tục TT
- Hàm người dùng
- Luật



# Tổng quan



## •Bảng DL

•*Thuộc tính*

•*Bộ*

## •Ràng buộc

•*Khóa chính*

•*Khóa ngoại*

•*Check*

•*Unique*

•*Default...*

## •Thủ tục TT

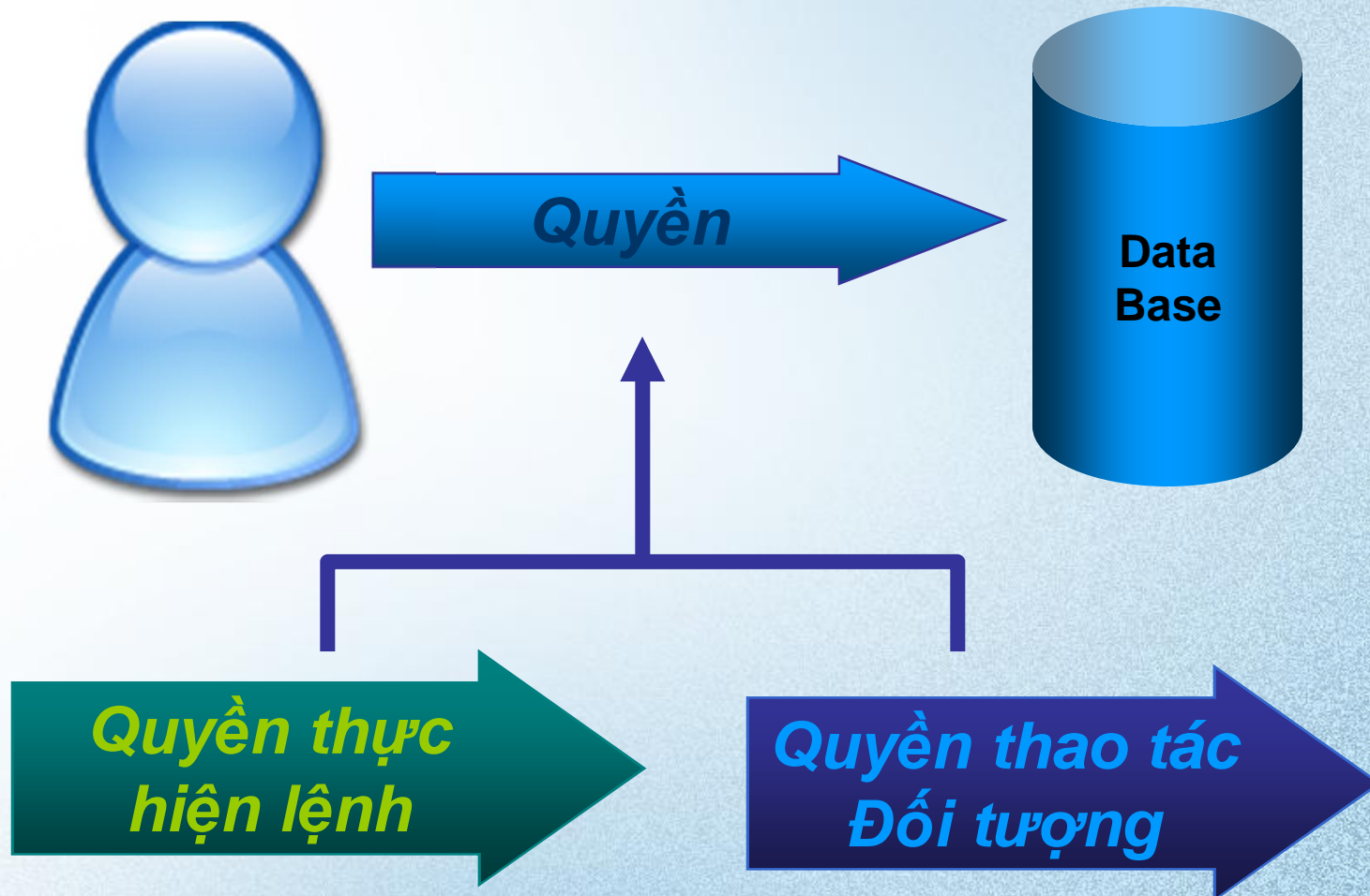
•*Hàm người dùng*

•*Luật*

•*...*

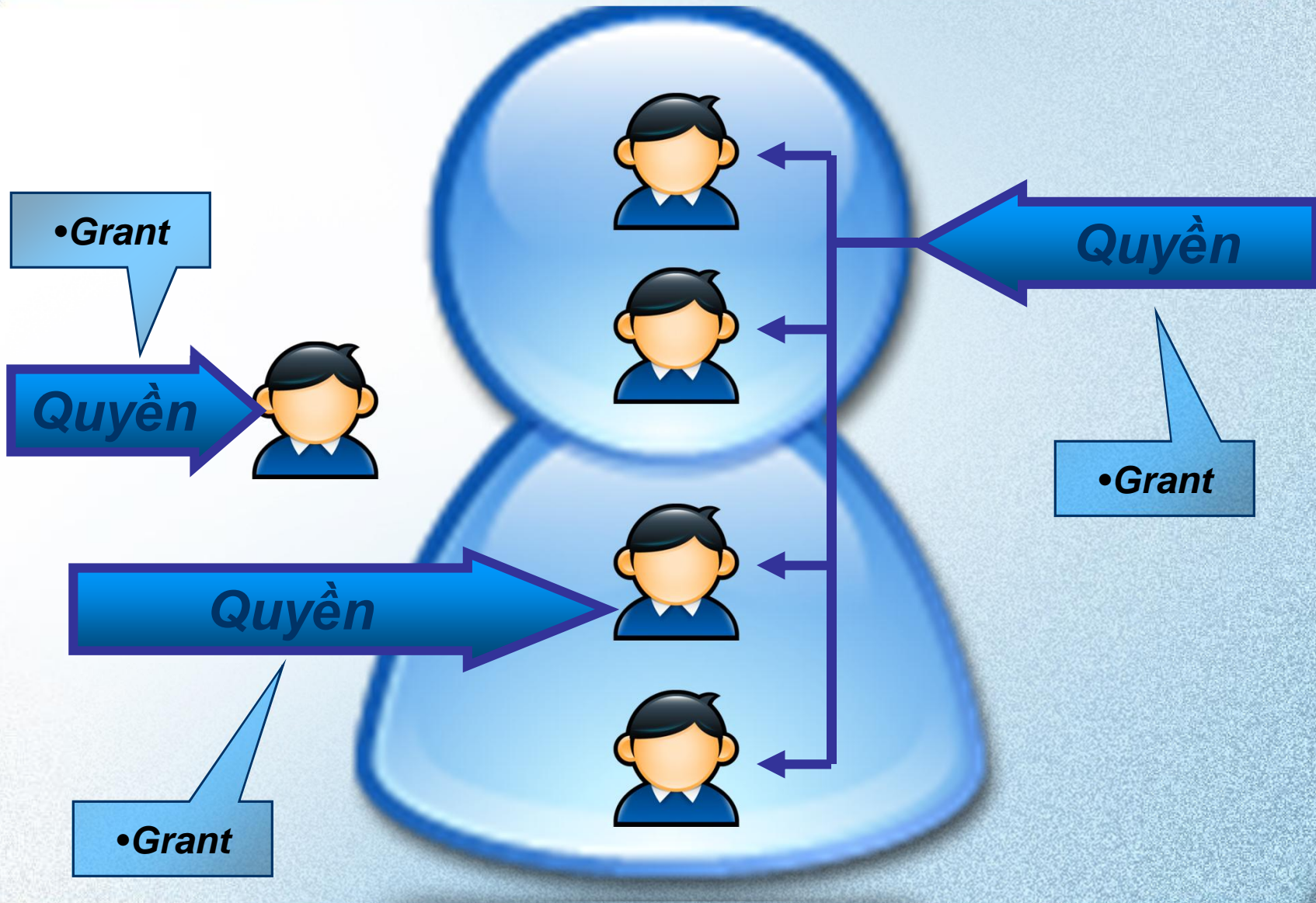


# Tổng quan



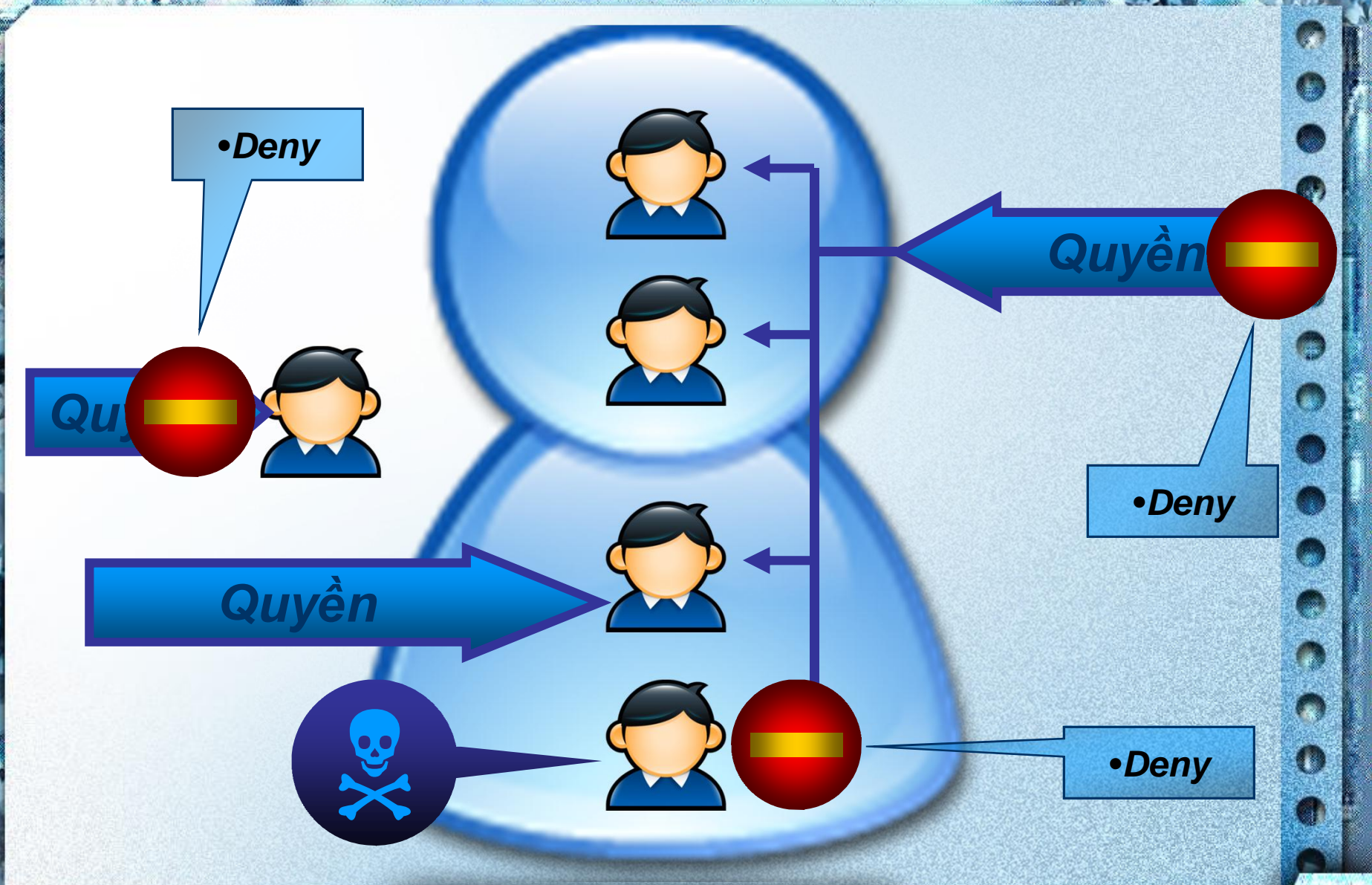


# Tổng quan



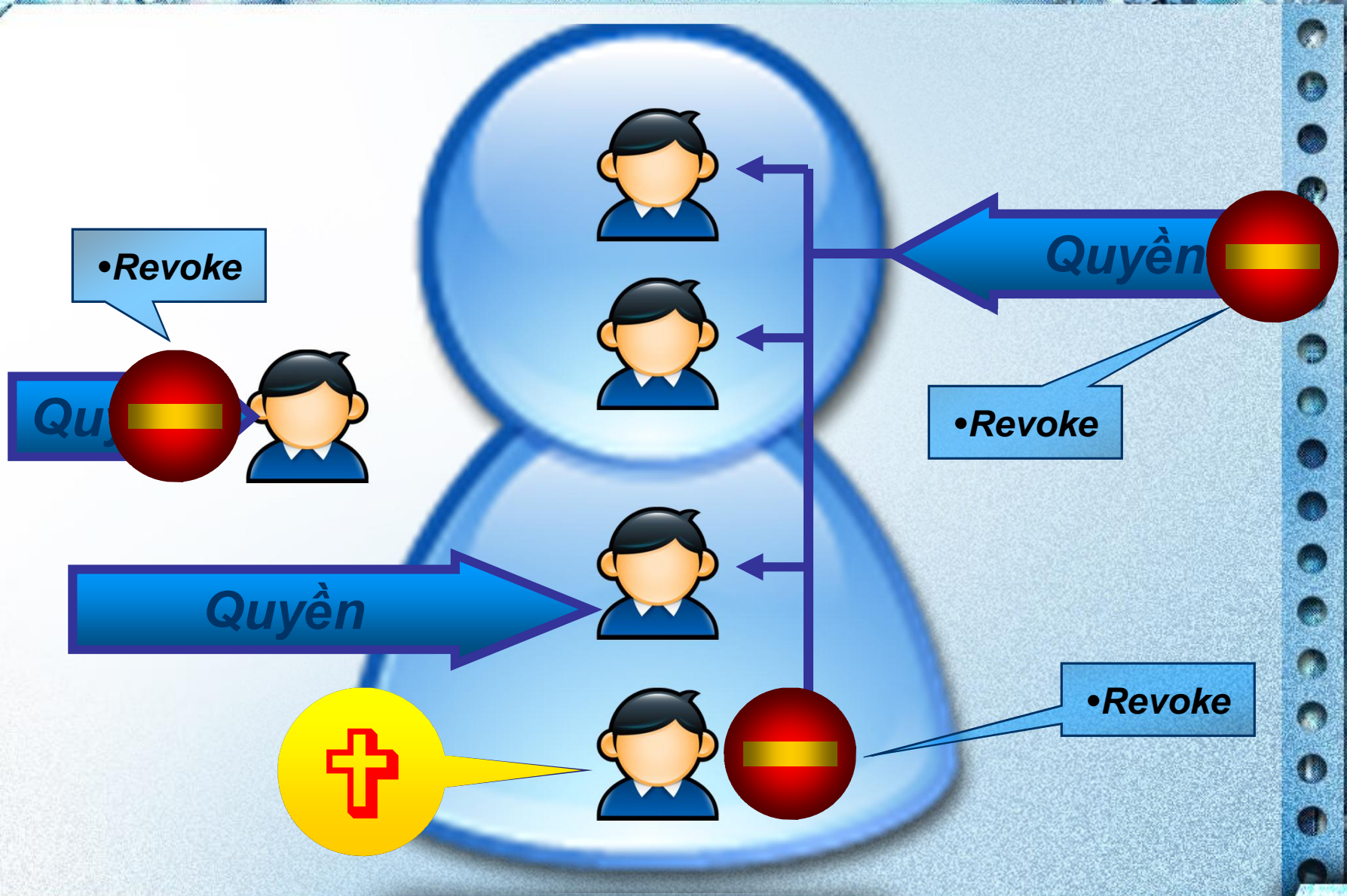


# Tổng quan



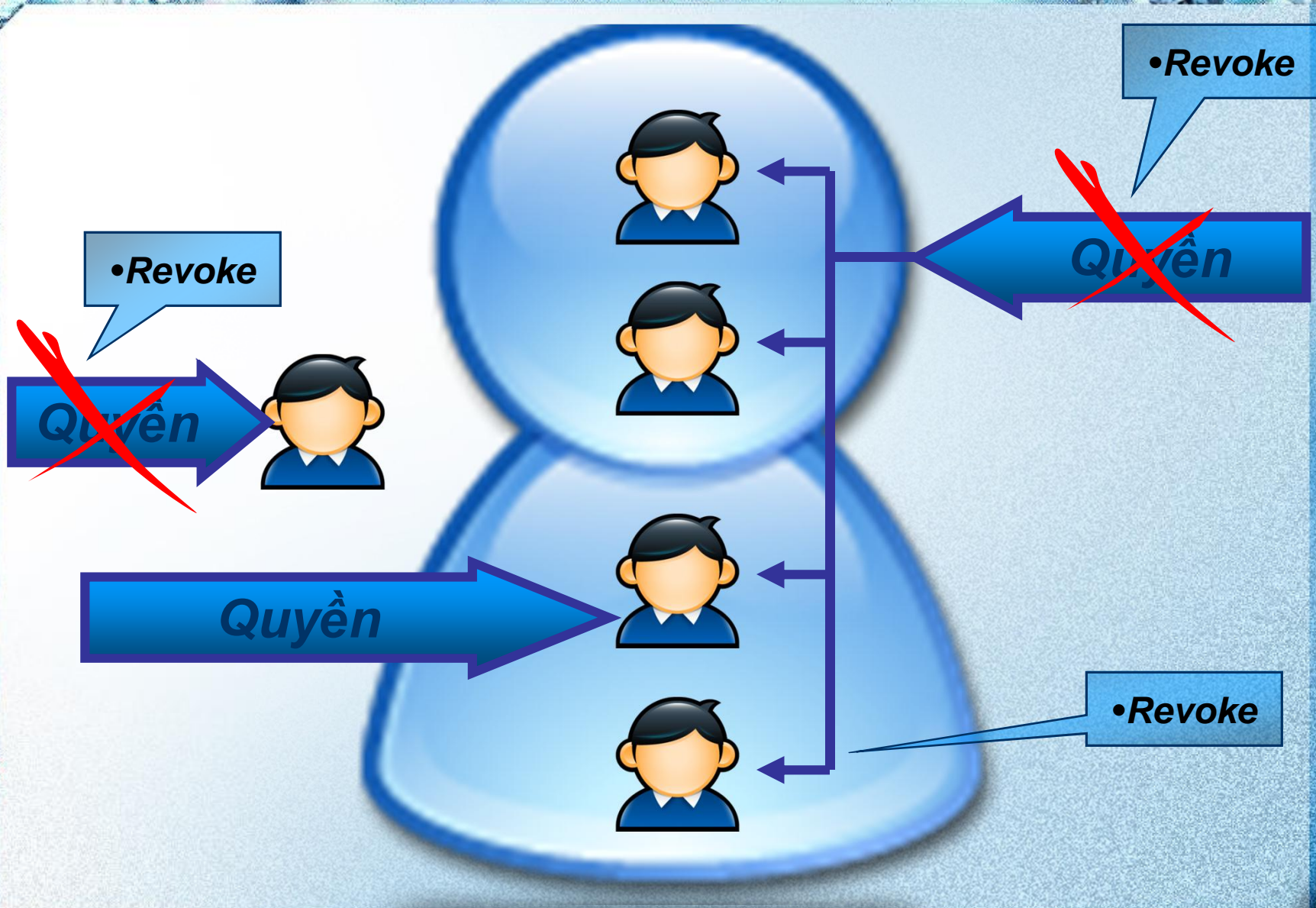


# Tổng quan



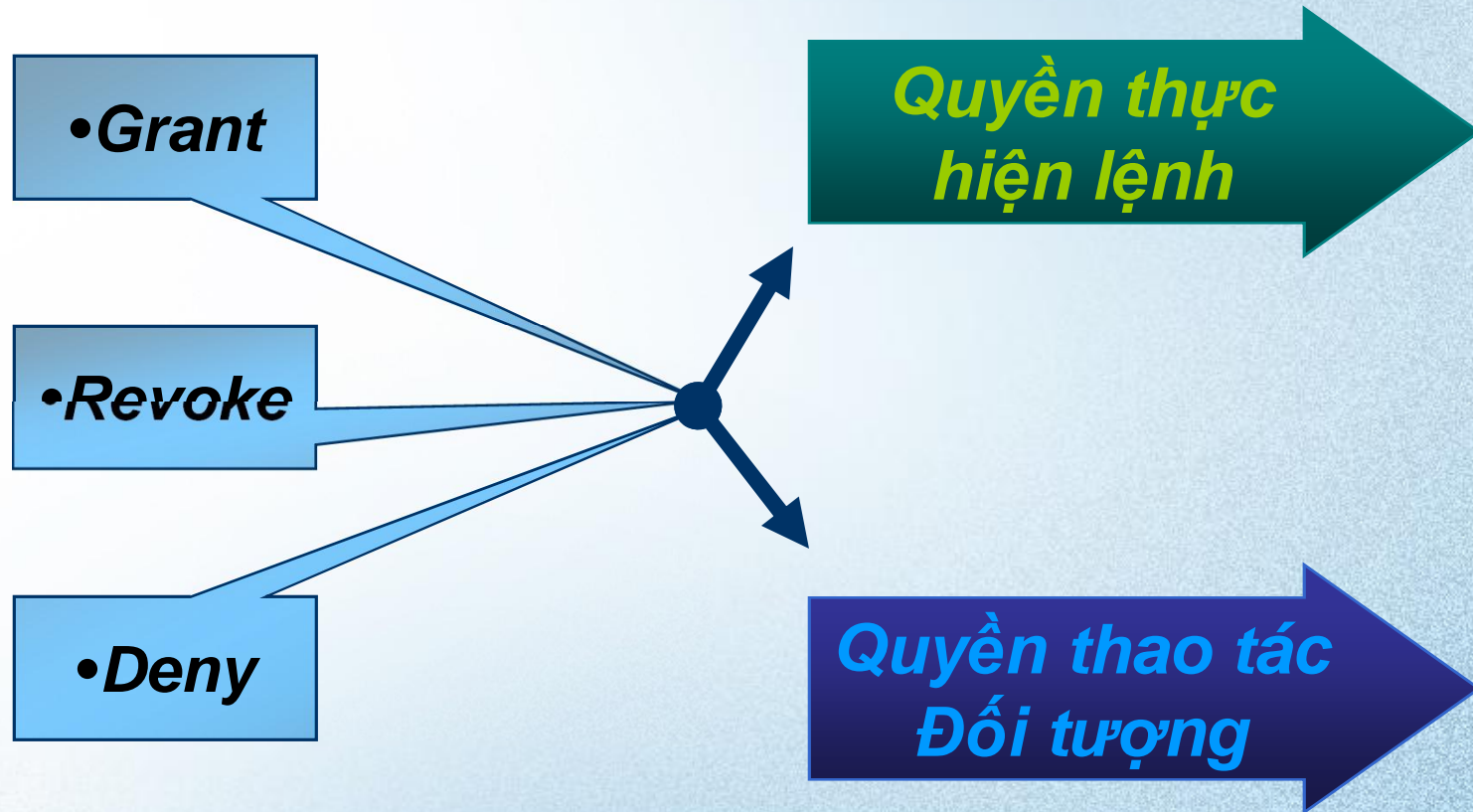


# Tổng quan





# Tổng quan





# Nội dung trình bày

- ◆ Tìm hiểu thêm về Trigger
- ◆ Khung nhìn
- ◆ Quản trị quyền người dùng
  - ***Tổng quan***
  - ***Chi tiết***
- ◆ Sao lưu và phục hồi dữ liệu



# Quản lý quyền người dùng

## ❖ 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”*



# Quản lý quyền người dùng

## ◆ Khái niệm chứng thực:

- *Xác nhận xem một tài khoản truy cập (login) có hợp lệ không (có được phép kết nối với SQL server hay không)*

## ◆ Các chế độ chứng thực:

- *Chứng thực của SQL Server (SQL Server Authentication)*
- *Chứng thực của Windows (Windows Authentication) (integrated security/ trusted connection)*



# Quản lý quyền người dùng

## ❖ Chứng thực của SQL Server:

- *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.*



# Quản lý quyền người dùng

- ◆ Chứng thực của Windows : Cấp phép cho các người dùng của Windows được kết nối đến SQL Server.
  - *Windows quản lý các tài khoản của người dùng và thực hiện việc chứng thực khi người dùng đăng nhập vào Windows*
  - *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.*



# Quản lý quyền người dùng

## ❖ Lựa chọn:

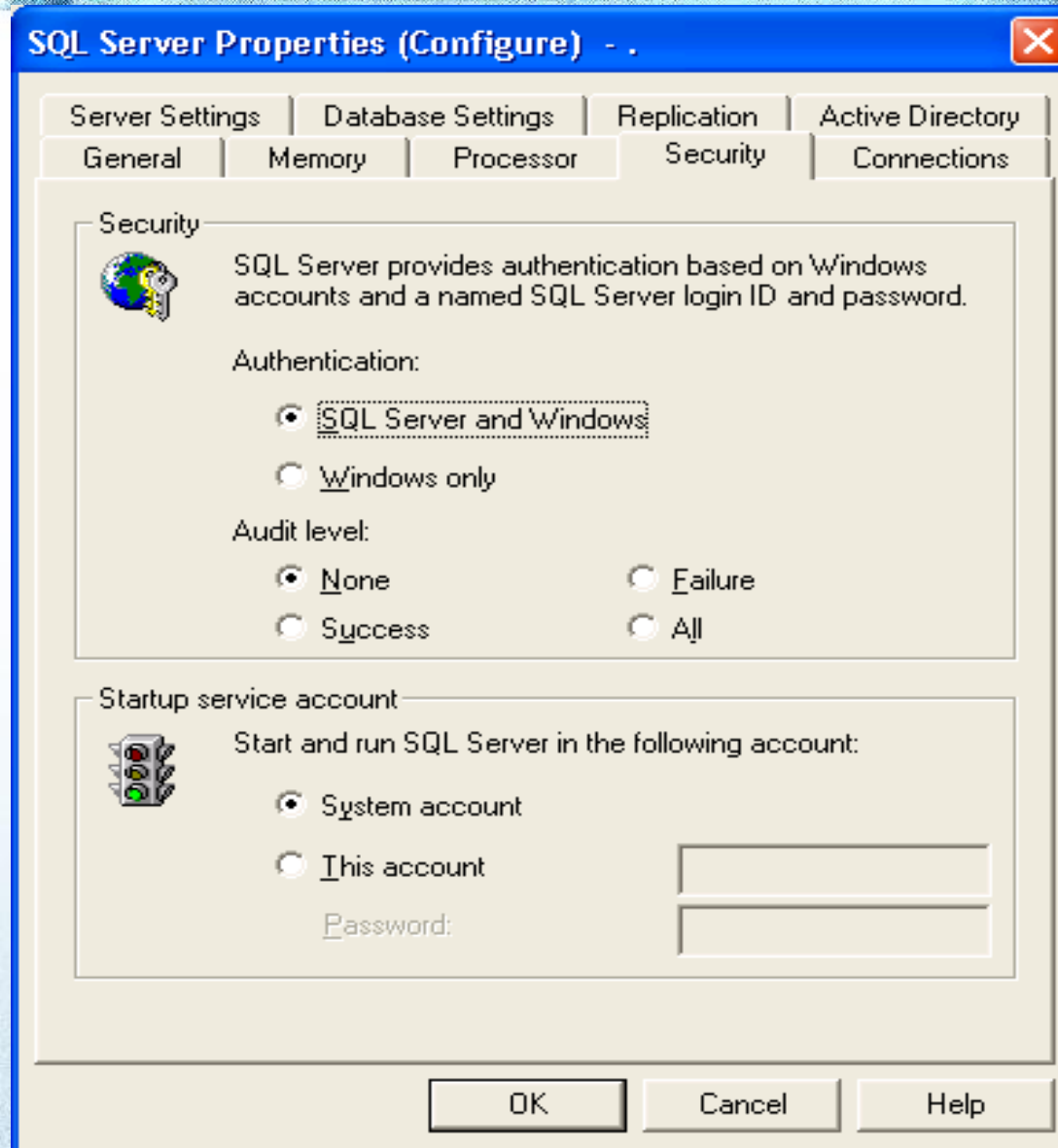
- ***Chỉ dùng Windows Authentication***
- ***Mixed mode (sử dụng cả hai chế độ chứng thực)***

## ❖ 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



# Quản lý quyền người dùng





# Quản lý 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.

## ◆ User:

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



# Quản lý 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*

## ◆ User:

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



# Quản lý quyền người dùng

**Login: tnhdud**

db QLSV – user QuanTriVien1

db QLTuyenSinh – user Dev1



# Quản lý quyền người dùng

- ◆ 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'
```



# Quản lý quyền người dùng

- ◆ **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'`**



# Quản lý quyền người dùng

## ❖ Một số thủ tục liên quan

- *sp\_password: đổi password của login*
- *sp\_defaultdb: đổi database mặc định của login*
- *sp\_droplogin: xóa login đã cấp bằng thủ tục sp\_addlogin*
- *sp\_revokelogin: lấy lại quyền truy cập đã cấp cho một người dùng/ nhóm người dùng của Windows bằng thủ tục sp\_grantlogin*



# Quản lý quyền người dùng

## ❖ Một số thủ tục liên quan

- **Đổi password login**

- **Cú pháp:**

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

- **Ví dụ:**

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



# Quản lý quyền người dùng

## ❖ Một số thủ tục liên quan

- *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 [@loginame=] 'login'`
- *Ví dụ:*
  - `exec sp_revokelogin 'login_name'`



# Quản lý quyền người dùng

- ◆ Xóa login
- ◆ Cú pháp :
  - ***sp\_droplogin [@loginame =] 'login\_name***
- ◆ Ví dụ:
  - ***exec sp\_droplogin 'login\_name'***



# Quản lý quyền người dùng

- ◆ **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'`



# Quản lý quyền người dùng

◆ Tạo user = cấp cho một login quyền truy cập vào database hiện hành

◆ Cú pháp:

*sp\_grantdbaccess*

*[@loginame =] 'login\_name'*

*[,[@name\_in\_db =] 'user\_name'[OUTPUT]]*

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 các phiên bản mới.



# Quản lý quyền người dùng

## ❖ Ví dụ

- ***exec sp\_grantdbaccess 'Nam', 'dev01'***
- ***exec sp\_grantdbaccess  
'Server01\user01', 'dev02'***



# Quản lý quyền người dùng

- ◆ 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*



# Quản lý quyền người dùng

## ❖ Xóa user khỏi database hiện hành

### • **Cú pháp**

*sp\_revokedbaccess* 'user\_name'

### • **Ví dụ:**

*exec sp\_revokedbaccess* 'dev02'



# Quản lý quyền người dùng

## ◆ 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.



# Quản lý quyền người dùng

- ❖ 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 cần được cấp cho một số quyền giống nhau:
  - Tạo role, gán các quyền cho role, user cần các quyền này sẽ là thành viên của role



# Quản lý quyền người dùng

◆ Role = Nhóm các user

- *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*



# Quản lý quyền người dùng

- ◆ 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`)



# Quản lý quyền người dùng

◆ 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'*



# Quản lý quyền người dùng

- ◆ Thêm một login vào các vai trò hệ thống có sẵn:
  - ✱ **Cú pháp:**  
`sp_addsrvrolemember [ @loginame = ] 'login'`  
`, [ @rolename = ] 'role'`
  - ✱ **Ví dụ:**  
`exec sp_addsrvrolemember 'tnhduc', '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.*



# Quản lý quyền người dùng

- ◆ Thêm một thành viên vào một vai trò trong database hiện hành (định nghĩa sẵn hoặc do người dùng khai báo):

- **Cú pháp:**

```
sp_addrolemember [ @rolename = ] 'role' ,  
[ @membername = ] 'security_account '  
(security_account = user_name/role)
```

- **Ví dụ:**

```
exec sp_addrolemember 'Developer', 'dev01'
```



# Quản lý quyền người dùng

## ◆ Các Server role

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 lý SQL login (đổi hoặc reset pass, <b>Grant, Revoke</b> và <b>Deny</b> quyền ở mức Server và Database)
Processadmin	Có quyền quản lý và kết thúc các tiến trình trên SQL Server
Dbcreatetor	Có quyền <b>create, drop, alter</b> và restore bất kì CSDL nào trên Server
diskadmin	Có quyền quản lý các file trên đĩa của server và tất cả các CSDL



# Quản lý quyền người dùng

## ◆ Các Database role

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 lý các quyền và role trong CSDL



# Quản lý quyền người dùng

- ◆ 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,...)**



# Quản lý quyền người dùng

## ❖ 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
```



# Quản lý quyền người dùng

## ◆ 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 ]
```



# Quản lý quyền người dùng

## ◆ 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 ]
```

*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*”



# Quản lý quyền người dùng

## ❖ 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



# Quản lý quyền người dùng

## ❖ 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



# Quản lý quyền người dùng

- ◆ Dừng 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*
  - *Cú pháp: Có hai dạng tương tự như Grant:*
    - Thu hồi quyền thực hiện lệnh
    - Thu hồi quyền thao tác trên đối tượng



# Quản lý quyền người dùng

## ❖ Thu hồi quyền thực hiện lệnh

### • **Cú pháp:**

**DENY** { **ALL** | *statement* [ ,...*n* ] }  
**TO** *security\_account* [ ,...*n* ]

### • **Ví dụ**

**Deny create table to Dev02**



# Quản lý quyền người dùng

## ◆ 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]
```



# Quản lý quyền người dùng

## ❖ 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**



# Quản lý quyền người dùng

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



# Quản lý quyền người dùng

## ❖ 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**



# Quản lý quyền người dùng

## ◆ 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 ]
```



# Quản lý quyền người dùng

## ❖ 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**



# Nội dung trình bày

- ◆ Tìm hiểu thêm về Trigger
- ◆ Khung nhìn
- ◆ Quản trị quyền người dùng
  - ***Tổng quan***
  - ***Chi tiết***
- ◆ Sao lưu và phục hồi dữ liệu