



TRƯỜNG ĐẠI HỌC THỦ DẦU MỘT  
KHOA CÔNG NGHỆ THÔNG TIN



## HỆ QUẢN TRỊ CSDL

### Chương 6

# BẢO MẬT & PHÂN QUYỀN


Phone: 0274. 3834930

Website: [www.et.tdmu.edu.vn](http://www.et.tdmu.edu.vn)




## Nội dung






## 6.1. Tổng quan


- Quản trị quyền người dùng




**SQL  
SERVER**



**Login**  
(Tài khoản chứng thực)




**Login**  
của HĐH




**Login** của SQL  
Server

- Sp\_addlogin
- Sp\_grantlogin
- Sp\_droplogin
- Sp\_password




## 6.1. Tổng quan


- Quản trị quyền người dùng (tt)




**SQL  
SERVER**




**User**  
(TK người dùng)




**A**




**User**  
(TK người dùng)




**C**




**User**  
(TK người dùng)



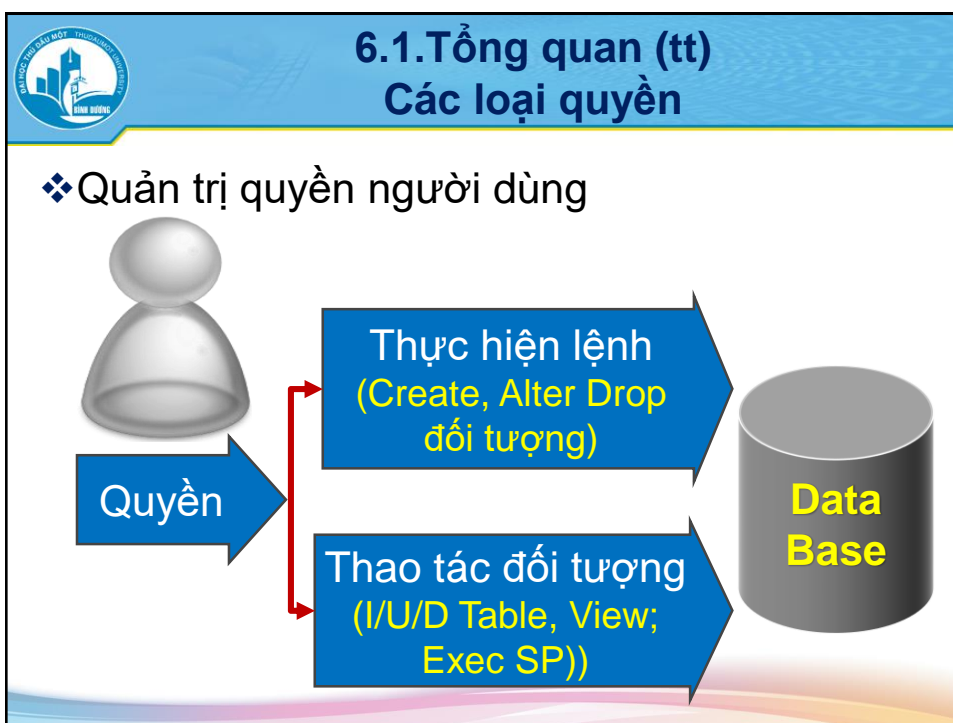
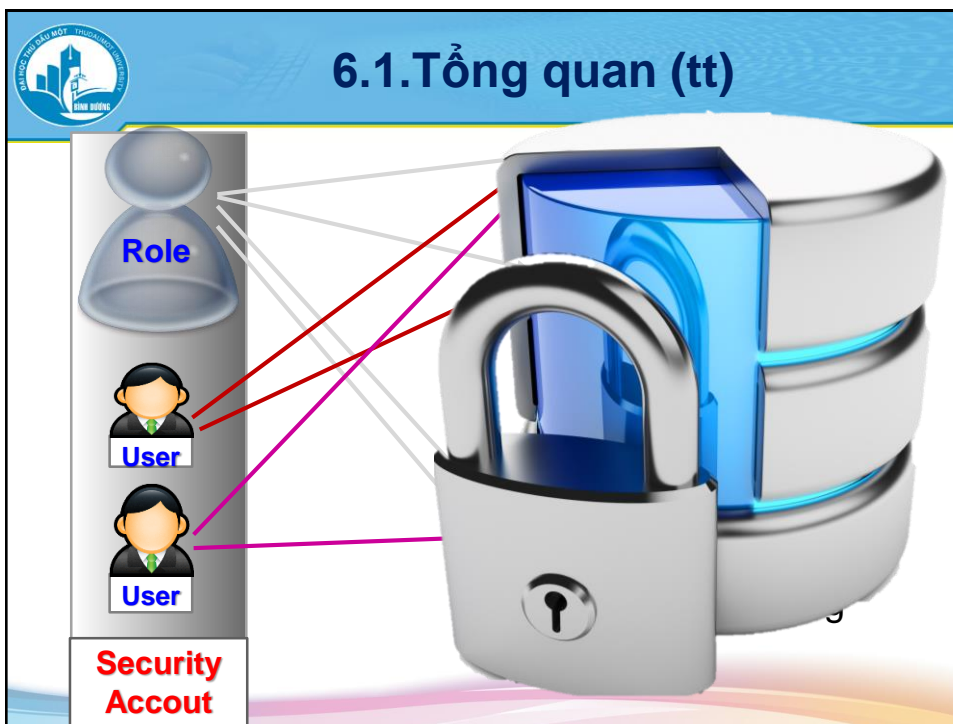
**D**

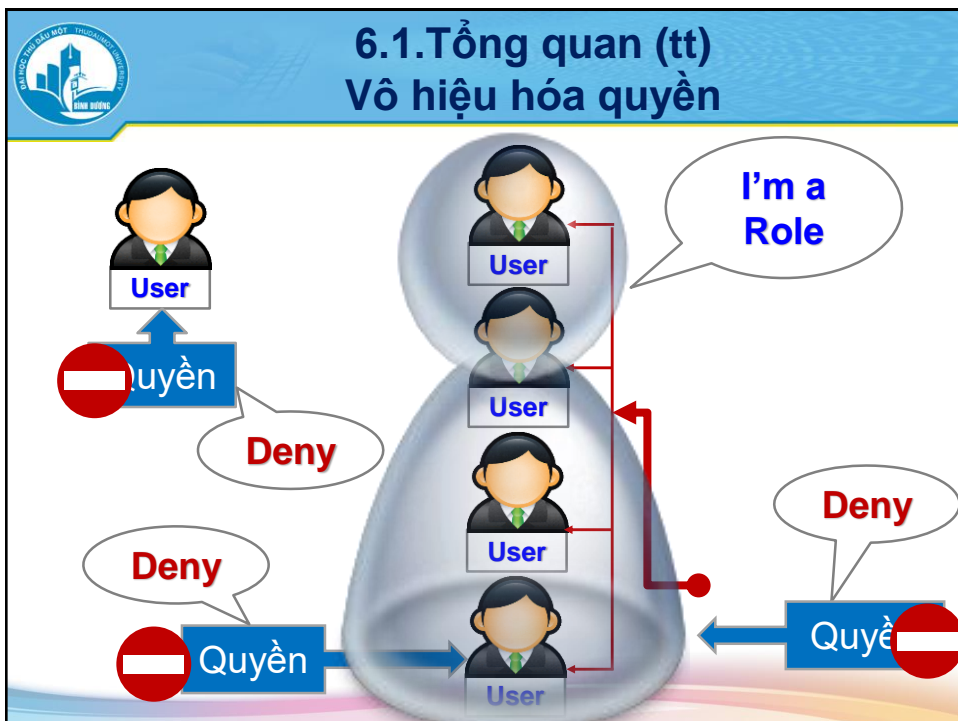
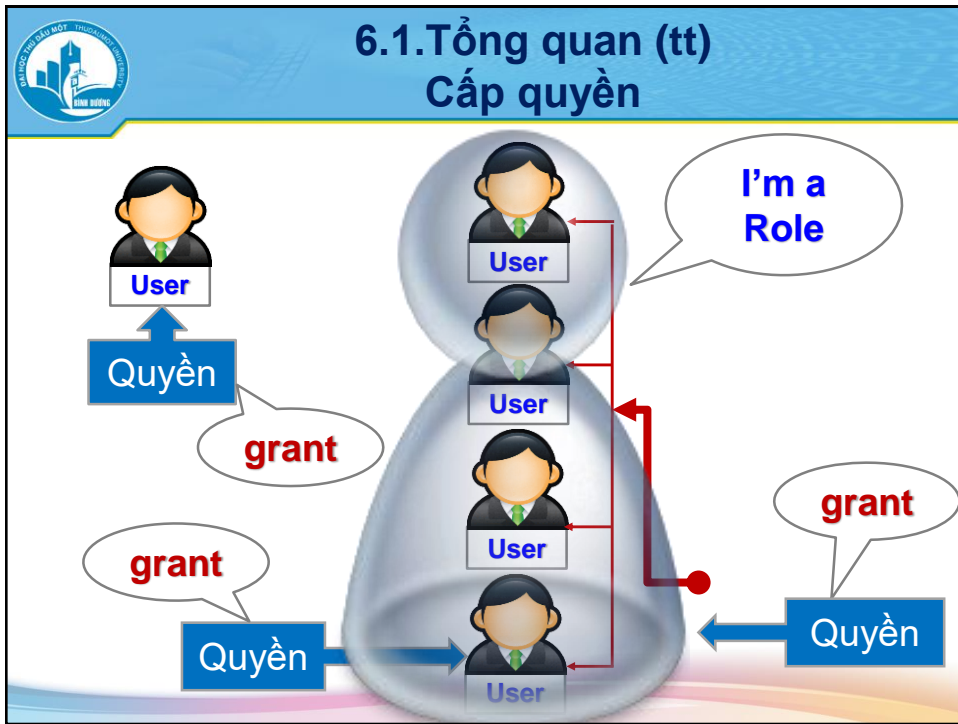


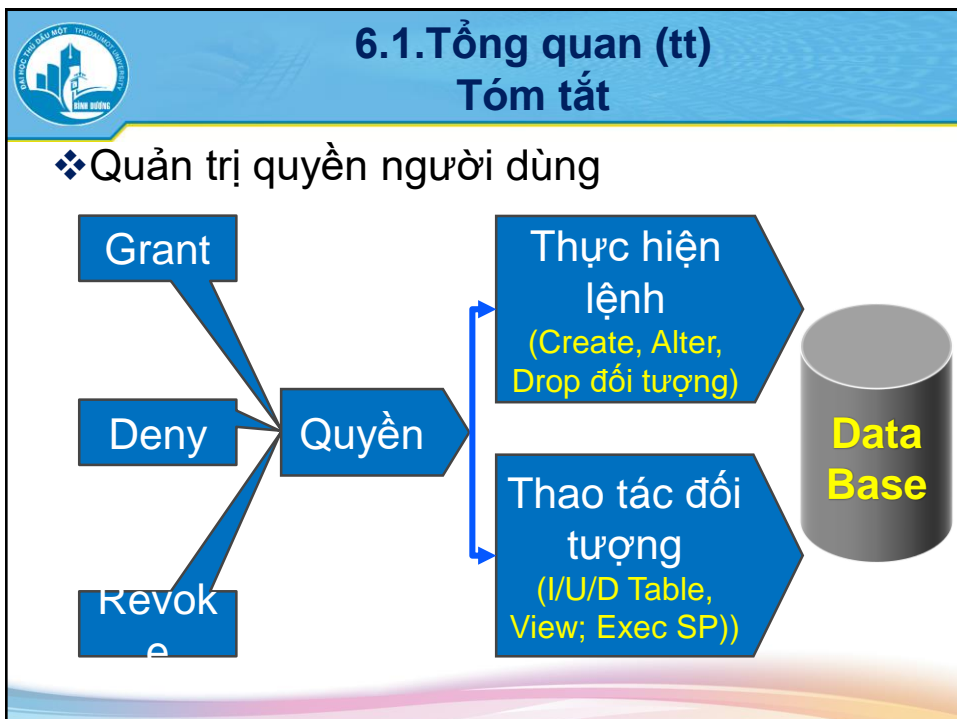
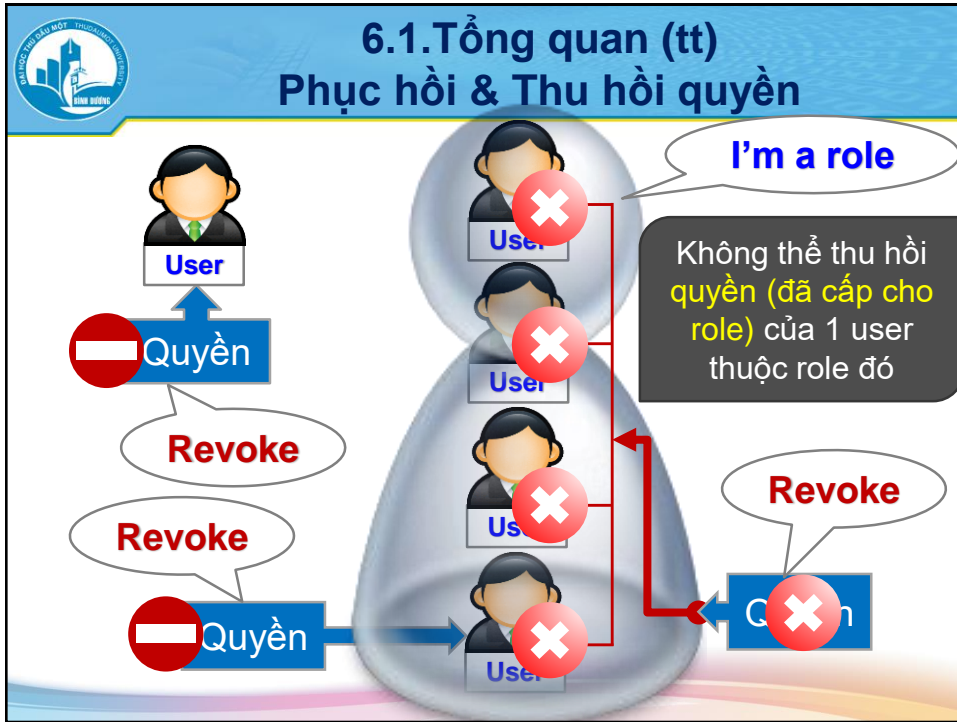
**Login**















## 6.2. Chi tiết phân quyền

### ❖ Cơ chế quản trị quyền người dùng:

- Cung cấp và quản lý các tài khoản truy cập (login) cho người dùng kết nối đến SQL Server
- Phân quyền: người dùng chỉ được phép thực hiện những thao tác mà họ được cấp phép.



## 6.2. Chi tiết phân quyền (tt)

### ❖ Khái niệm chứng thực:

- Xác nhận một tài khoản truy cập (login) có hợp lệ hay không (được phép kết nối đến 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)



## 6.2. Chi tiết phân quyền (tt)

### ❖ 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 (login name, password) khi người dùng đăng nhập (yêu cầu kết nối) vào SQL Server

### ❖ Chức thực của Windows :

- Sử dụng chung tài khoản với Windows.
- Khi kết nối không cần nhập thông tin login (login name, password)



## 6.2. Chi tiết phân quyền (tt)

### ❖ Thiết lập cơ chế chứng thực

Dùng cơ chế chứng thực của Windows

Chọn 1 trong 2 cơ chế chứng thực: Của windows hoặc của SQL Server





## 6.2. Chi tiết phân quyền (tt)

### ❖ 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 1 user

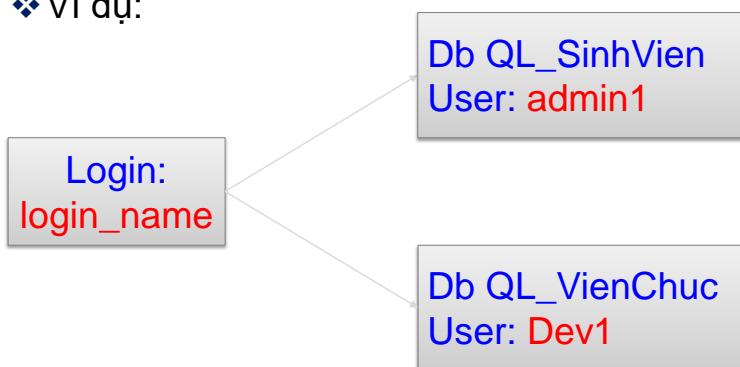
### ❖ User:

- Là một “người dùng” trong 1 database cụ thể
- Một user ứng với 1 login



## 6.2. Chi tiết phân quyền (tt)

### ❖ Ví dụ:





## 6.2. Chi tiết phân quyền (tt)

❖ Login được cung cấp và quản lý bởi quản trị viên hệ thống hoặc quản trị viên an ninh của SQL Server (sysadmin/ securityadmin)

❖ Lệnh tạo login (SQL Server Authentication)

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

• Ví dụ:

```
Exec sp_addlogin 'Thanh', 'testpass', 'QL_SinhVien'
```



## 6.2. Chi tiết phân quyền (tt)

```
CREATE LOGIN loginName { WITH <option_list1> | FROM <sources> }
<option_list1> ::=
    PASSWORD = { 'password' | hashed_password HASHED } [ MUST_CHANGE ]
    [ , <option_list2> [ ,... ] ]
<option_list2> ::=
    SID = sid
    | DEFAULT_DATABASE = database
    | DEFAULT_LANGUAGE = language
    | CHECK_EXPIRATION = { ON | OFF }
    | CHECK_POLICY = { ON | OFF }
    | CREDENTIAL = credential_name
<sources> ::=
    WINDOWS [ WITH <windows_options> [ ,... ] ]
    | CERTIFICATE certname
    | ASYMMETRIC KEY asym_key_name
<windows_options> ::=
    DEFAULT_DATABASE = database
    | DEFAULT_LANGUAGE = language
```



## 6.2. Chi tiết phân quyền (tt)

### ❖ Lệnh cấp quyền truy cập (grant login / Windows Authentication)

- Cấp phép một hoặc một nhóm người dùng của Windows (Windows user/ group) được kết nối đến SQL Server
- **User admin của windows** thì chắc chắn có quyền login vào SQL Server nên không cần cấp quyền.

```
sp_grantlogin [@loginname=]
```

```
'windows_account'
```

– Trong đó windows\_account: Domain\User

- Ví dụ:


```
Exec sp_grantlogin 'Server01\user01'
```



## 6.2. Chi tiết phân quyền (tt)

### ❖ Một số thủ tục liên quan đến login:

- **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\_revokellogin**: lấy lại quyền đã cấp cho một người dùng/ nhóm người dùng của Windows bằng thủ tục sp\_grantlogin



## 6.2. Chi tiết phân quyền (tt)


### Một số thủ tục liên quan đến login

- ❖ Đổi password login
  - Cú pháp:
 

```
Sp_password [[@old=] 'old_pass',] {@new=} 'new_pass'},[@loginname=] 'login_name'
```

    - Ví dụ:
 

```
Exec sp_password null, '123' , 'abc'
```



## 6.2. Chi tiết phân quyền (tt)

### Một số thủ tục liên quan đến login

- ❖ Hủy quyền của login
  - Thu hồi 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_name'
```

    - Ví dụ:
 

```
Exec sp_revokelogin 'user01'
```



## 6.2. Chi tiết phân quyền (tt)

### Một số thủ tục liên quan đến login

#### ❖ Xóa login

- Xóa bỏ login đã tạo bằng thủ tục

`sp_addlogin`

- Cú pháp:

```
Sp_droplogin [@loginame=] 'login_name'
```

- Ví dụ:

```
Exec sp_droplogin 'Thanh'
```



## 6.2. Chi tiết phân quyền (tt)

### Một số thủ tục liên quan đến login

#### ❖ Đổi database mặc định của login

- Áp dụng cho login đã được ánh xạ vào một user trong CSLD mà có khai báo mặc định.

- Cú pháp:

```
Sp_defaultdb [@loginame=] 'login_name',  
[@defdb=] 'database_name'
```

- Ví dụ:

```
Exec sp_defaultdb 'Thanh', 'QL_DatHang'
```



## 6.2. Chi tiết phân quyền (tt)

### User

#### ❖ Tạo user (Cách 1)

- Cấp cho một login quyền truy cập vào database **hiện hành**.
- Chỉ có thể được thực thực hiện bởi thành viên của vai trò sysadmin, db\_owner và db\_accessadmin.
- Những phiên bản sau này. Thay bằng Create user.
- Cú pháp:

```
Sp_grantdbaccess [@loginname=] 'login_name'
[,[@name_in_db=] 'user_name' [OUTPUT]]
```

- Ví dụ:

```
Exec sp_grantdbaccess 'Thanh', 'dev01'
```

```
Exec sp_grantdbaccess 'Server01\user01', 'dev02'
```



## 6.2. Chi tiết phân quyền (tt)

### User

#### ❖ Tạo user (Cách 2)

- 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
```





## 6.2. Chi tiết phân quyền (tt)

### User

#### ❖ Xóa user khỏi database hiện hành

##### ➤ Cú pháp:

`Sp_revokedbaccess 'user_name'`

##### • Ví dụ:

Exec `sp_revokedbaccess 'dev01'`



## 6.2. Chi tiết phân quyền (tt)

### 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



## 6.2. Chi tiết phân quyền (tt)

### User

- ❖ Sau khi tạo user:
  - User có quyền truy cập vào database
  - Chưa được thao tác trên các đối tượng của database
  - ➔ Cần gán quyền cụ thể cho từng user của database
- ❖ Nếu nhiều user cần được cấp cho một số quyền giống nhau:
  - Tạo role
  - Gán quyền cho role
  - User cần các quyền này sẽ được đưa vào là thành viên của role



## 6.2. Chi tiết phân quyền (tt)

### Role

- ❖ Định nghĩa:
  - Người dùng có thể định nghĩa cá vai trò mới cho database hiện hành bằng thủ tục sp\_addrole
  - Chỉ có thể được thực hiện bởi thành viên của sysadmin, db\_owner, db\_securityadmin.
- ❖ Cú pháp:
 

```
Sp_addrole [@rolename=] 'role_name'
[, [@ownername=] 'owner']
```

  - Ví dụ:
 

```
Exec sp_addrole 'Developer'
Exec sp_addrole 'Developer', 'dbo'
```



## 6.2. Chi tiết phân quyền (tt)

### Role

- ❖ Thêm một thành viên vào một vai trò trong database hiện hành:

- ❖ Cú pháp:

`Sp_addrolemember [@rolename=] 'role_name',  
[@membername=] 'security_account'`

- (Security\_account = user\_name | role)

- Ví dụ:

-- Đưa user dev01 vào role Developer

Exec `sp_addrolemember` 'Developer' , 'dev01'



## 6.2. Chi tiết phân quyền (tt)

### Role

- ❖ Lưu ý:

- 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"

- ❖ Xóa một role đã tạo

Cú pháp:

`Sp_droprole [@rolename=] 'role_name'`

- Ví dụ:

Exec `sp_droprole` 'Developer'



## 6.2. Chi tiết phân quyền (tt)

### System Role

- ❖ Là những vai trò do SQL Server định nghĩa sẵn
- ❖ Sa và các login là administrator của Windows (Windows Authentication) đều là các thành viên của sysadmin
- ❖ Ta có thể thêm một login vào các vai trò hệ thống có sẵn (system role)
- ❖ Cú pháp:

```
Sp_addsrvrolemember [@loginame=] 'login_name' ,
[@rolename=] 'role_name'
```

- Ví dụ:

```
Exec sp_addsrvrolemember 'Thanh' , 'sysadmin'
```



## 6.2. Chi tiết phân quyền (tt)

### Các Server Role

Role	Mô tả
<b>Sysadmin</b>	Có quyền tương đương sa (Full)
<b>Serveradmin</b>	Có quyền cấu hình và shutdown server
<b>Setupadmin</b>	Có quyền add và remove các linked server
<b>Securityadmin</b>	Có quyền quản lý SQL login (đổi hoặc reset pass, Grant, Revoke và Deny quyền ở mức Server và Database
<b>Processadmin</b>	Có quyền quản lý và kết thúc các tiến trình trên SQL Server
<b>dbcreator</b>	Có quyền create, drop, alter và restore bất kỳ Database nào trên Server
<b>Diskadmin</b>	Có quyền quản lý các file trên đĩa của server và tất cả các Database



## 6.2. Chi tiết phân quyền (tt)

### Các Database Role

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



## 6.2. Chi tiết phân quyền (tt)

### Cấp quyền

- ❖ Sử dụng lệnh “Grant...” để cấp quyền cho user /role
- ❖ Có hai dạng:
  - Cấp quyền thực hiện lệnh (Create, Alter, Drop)
  - Cấp quyền thao tác trên đối tượng trong database (I/U/D/ Exec)



## 6.2. Chi tiết phân quyền (tt)

### Cấp quyền thực hiện

#### ❖ Cú pháp:

Grant { All | statement [,..n] }

To security\_account [,..n]

Trong đó:

- **Statement** = create database | create table | create view | create procedure | backup database | ...
- **Security\_account** = user | role

#### Ví dụ:

Grant create table, create procedure to dev01



## 6.2. Chi tiết phân quyền (tt)

### Cấp quyền thao tác trên đối tượng

#### ❖ Cú pháp:

Grant

{ All | permission [,..n] }

{ [column [,..n]] ON { table | view }

| ON { table | view } [(column [,..n])]

| ON { store\_procedure }

| ON { user\_defined\_function }

}

To security\_account [,..n]

[With Grant Option]

[As role]

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

Cho phép user được cấp các quyền thao tác này cho user / role khác

Lệnh cấp quyền được thực hiện với tư cách là thành viên của "role"





## 6.2. Chi tiết phân quyền (tt)

### Cấp quyền thao tác trên đối tượng

- Ví dụ: Cấp quyền select, update trên các cột Hoten, DiaChi, NgaySinh của bảng SinhVien cho thành viên của role Developer

Grant select, update  
On SinhVien(HoTen, DiaChi, NgaySinh)  
To Developer

Grant select, update  
On SinhVien(HoTen, DiaChi, NgaySinh)  
To Developer  
With grant option



## 6.2. Chi tiết phân quyền (tt)

### Vô hiệu hóa quyền

- ❖ Khi một user/ role bị cấm sử dụng 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
  - Vô hiệu hóa quyền thực hiện lệnh
  - Vô hiệu hóa quyền thao tác trên đối tượng



## 6.2. Chi tiết phân quyền (tt)

### Vô hiệu hóa quyền thực hiện

#### ❖ Cú pháp

```
Deny {All | statement [...n]}
To security_account [...n]
```

- Ví dụ:

```
Deny create table
To Dev02
```



## 6.2. Chi tiết phân quyền (tt)

### Vô hiệu hóa quyền thao tác trên đối tượng

#### ❖ Cú pháp:

```
Deny
{All | permission [...n]}
{[column [...n]] ON {table | view}
 | ON {table | view} [(column [...n])]
 | ON {store_procedure}
 | ON {user_defined_function}
}
To security_account [...n]
[Cascade]
```



## 6.2. Chi tiết phân quyền (tt)

### Vô hiệu hóa quyền thao tác trên đối tượng

- Ghi chú: Nếu security\_account được cấp trực tiếp quyền này với “with grant option”, thì Cascade sẽ giúp vô hiệu hóa quyền này trên toàn bộ user/ role đã được security\_account cấp quyền này
- Ví dụ:

Deny select, update

On SinhVien (HoTen, DiaChi, NgaySinh)

To Dev02

Cascade



## 6.2. Chi tiết phân quyền (tt)

### Thu hồi/hiệu lực hóa quyền thao tác trên đối tượng

#### ❖ Cú pháp:

Revoke {All | statement [...n]}

From security\_account [...n]

#### — Ví dụ:

Revoke create table From Dev02

Nếu quyền này được cấp cho role mà Dev02 là member và đang dùng được revoke không có tác dụng.

Nếu quyền này đang bị Deny thì Dev02 được sử dụng trở lại

Nếu quyền này được cấp trực tiếp và Dev02 đang dùng được thì Dev02 sẽ bị thu hồi quyền này



## 6.2. Chi tiết phân quyền (tt)

### Thu hồi/hiệu lực hóa quyền thao tác trên đối tượng

#### ❖ Cú pháp:

```

Revoke
{All | permission [...n]}
{[column [...n]] ON {table | view}
  | ON {table | view} [(column [...n])]
  | ON {store_procedure}
  | ON {user_defined_function}
}
From security_account [...n]
[Cascade]
[As role]
  
```



## 6.2. Chi tiết phân quyền (tt)

### Thu hồi/hiệu lực hóa quyền thao tác trên 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 áp dụng

- Trong hệ thống quản lý trường học gồm các thông tin cần quản lý sau:
  - ✓ Quản lý sinh viên; Quản lý Giảng Viên; Quản lý cơ sở vật chất
- Yêu cầu:
  - ✓ Sinh viên có quyền vào xem thông tin về học phần (HocPhan) của QLSV
  - ✓ Giảng viên có quyền truy cập vào xem thông tin học phần (HocPhan); Xem, Cập nhật điểm thi (KetQua) của QLSV
  - ✓ QL giáo vụ có thao tác đối tượng trên QLSV và QLGV
  - ✓ Hiệu Trưởng có quyền xem tất cả các thông tin cần quản lý



## Tài liệu tham khảo

- Slide HQTCSDL, Tuấn Nguyễn Hoài Đức - ĐH KHTN Tp.HCM.
- Wikipedia
- SQL Server 2008, Trung tâm CNTT Nhất Nghệ
- Bài giảng tóm tắt Hệ quản trị CSDL, Trường ĐH Đà Lạt.
- Bài giảng Hệ quản trị CSDL SQL Server, Nguyễn Văn Lợi



## Hết chương 6



Phone: 0660. 3834930

Website: [www.fit.tdmu.edu.vn](http://www.fit.tdmu.edu.vn)