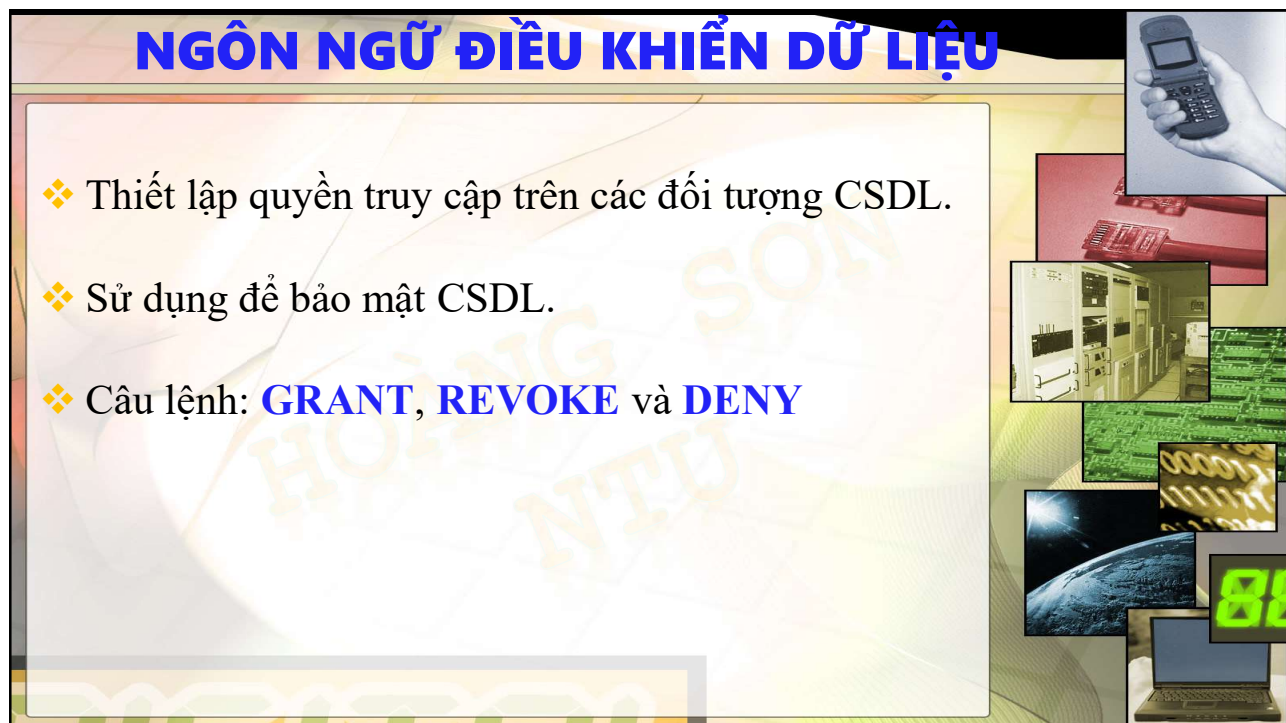


176

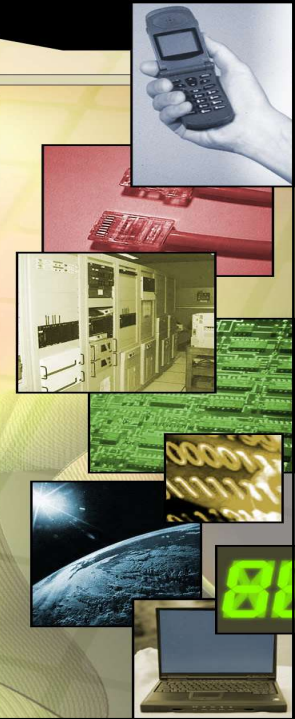


177

## BẢO MẬT TRONG SQL SERVER

### 3 lớp

- ❖ **Login security:** đăng nhập vào SQL Server
- ❖ **Database access security:** user có thể truy cập vào một CSDL cụ thể trên server.
- ❖ **Permission security:** user có thể thực hiện thao tác gì trên CSDL



178

## BẢO MẬT TRONG SQL SERVER

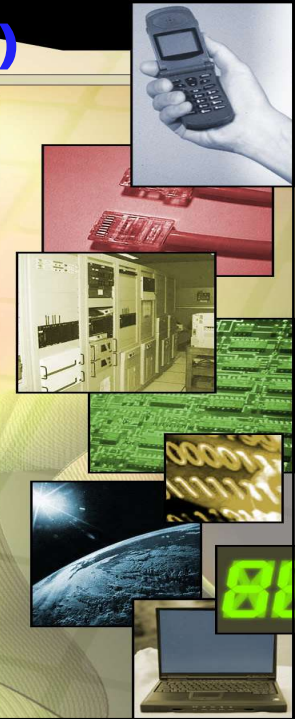
- ❖ SQL Server sử dụng **Permission** và **Role** để bảo mật CSDL
  - *Permission:* Quy định các hành động mà người dùng thực hiện trên các đối tượng CSDL.
  - *Role:* tập các quyền được gán cho người dùng.
- ❖ SQL server dựa vào Permission và Role để xác định các đối tượng, hành động mà người dùng được phép thực hiện trên CSDL



179

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

- ❖ Lệnh CREATE LOGIN được dùng để tạo tài khoản đăng nhập (Login) kết nối tới SQL Server. Tài khoản đăng nhập sau đó sẽ được ánh xạ vào tài khoản người dùng.
- ❖ 2 loại tài khoản đăng nhập chính:
  - Tài khoản đăng nhập sử dụng xác thực SQL Server Authentication.
  - Tài khoản đăng nhập sử dụng xác thực Windows Authentication.



180

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

- ❖ Tạo tài khoản đăng nhập sử dụng xác thực SQL Server Authentication

```
CREATE LOGIN tên_login
WITH PASSWORD = 'mật_khẩu'
[ MUST_CHANGE, CHECK_EXPIRATION=ON ]
[ , DEFAULT_DATABASE = tên_CSDL ]
[ , DEFAULT_LANGUAGE = tên_ngôn_ngữ ]
;
```



181

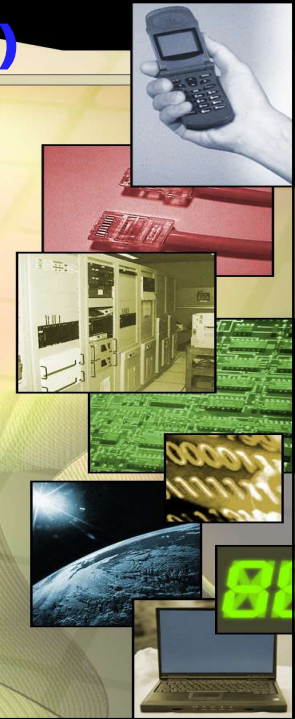


## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

**Lưu ý:** Để khai báo CSDL mặc định (DEFAULT\_DATABASE) khác với **master** cần phải chuyển owner của CSDL cho **tên\_login** bằng câu lệnh

**ALTER AUTHORIZATION**

**ON DATABASE::tên\_CSDL TO tên\_login ;**



182

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

❖ Tạo tài khoản đăng nhập sử dụng xác thực Windows Authentication

Trong Windows, trong **CMD** (Admin) hoặc **Windows PowerShell** (Admin):

- Xem tài khoản Windows

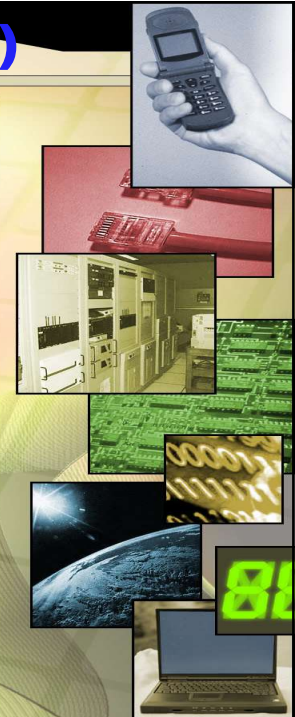
**net user**

- Tạo tài khoản Windows

**net user tên\_tk mật\_khẩu /add**

- Xem hostname

**hostname**



183

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

- ❖ Tạo tài khoản đăng nhập sử dụng xác thực Windows Authentication

Sử dụng *SQL Server Management Studio*

**CREATE LOGIN "hostname\tên\_login"**

**FROM WINDOWS**

**[ WITH DEFAULT\_DATABASE = tên\_CSDL ]**

**[ , DEFAULT\_LANGUAGE = tên\_ngôn\_ngữ ]**

**;**

184

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

- ❖ Sửa đổi tài khoản đăng nhập

**ALTER LOGIN tên\_login [ ENABLE | DISABLE ]**

**[ [ WITH [ PASSWORD = 'mật\_khẩu\_mới'**

**[ OLD\_PASSWORD = 'mật\_khẩu\_cũ' ]**

**[ MUST\_CHANGE ] [ UNLOCK ]**

**]**

**[ , DEFAULT\_DATABASE = tên\_CSDL ]**

**[ , DEFAULT\_LANGUAGE = tên\_ngôn\_ngữ ]**

**[ , NAME = tên\_login\_mới ]**

**[ , CHECK\_EXPIRATION = ON | OFF ]**

**];**

185

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

- ❖ Xóa tài khoản đăng nhập

```
DROP LOGIN tên_login ;
```




186

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

- ❖ Chuyển đổi tài khoản đăng nhập

```
EXECUTE | EXEC AS LOGIN = 'tên_login'  
[ WITH NO REVERT ] ;
```



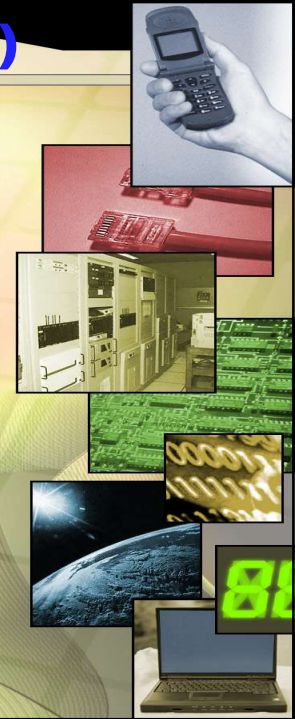
187



## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

Ví dụ: Liệt kê danh sách tài khoản đăng nhập

```
SELECT name AS Login_Name,
       type_desc AS Account_Type
FROM sys.server_principals
WHERE TYPE IN ('U', 'S', 'G')
and name not like '%###%'
ORDER BY name, type_desc;
```



188

## TÀI KHOẢN ĐĂNG NHẬP (LOGIN)

Ví dụ: Hiển thị tài khoản đăng nhập hiện tại

```
SELECT
  SUSER_NAME() AS ProcessLoginName,
  SUSER_NAME(1) AS AdminLoginName,
  SUSER_SNAME(SUSER_SID()) AS SystemLoginName;
```



189

## NGƯỜI DÙNG (USER)

- ❖ SQL Server cho phép truy nhập vào hệ thống thông qua các login nhưng chưa truy nhập được vào các CSDL chứa trong đó.
- ❖ Mỗi CSDL duy trì một danh sách các user, các user ánh xạ (mapped) với một login ở mức server. Khi đăng nhập vào SQL Server thông qua login thì sẽ có quyền truy nhập vào CSDL thông qua user với các quyền hạn xác định.



190

## NGƯỜI DÙNG (USER)

- ❖ Tạo người dùng


**CREATE USER** *tên\_user*

[ <**FOR** | **FROM**> **LOGIN** *tên\_login* | **WITHOUT LOGIN** ]

[ **WITH** [ **PASSWORD** = '*mật\_khẩu*' ]

[ , **DEFAULT\_SCHEMA** = *tên\_schema* ]

;

 **Lưu ý:** Nếu sử dụng Windows Authentication thì *tên\_user* và *tên\_login* sẽ là "hostname\tên\_login"



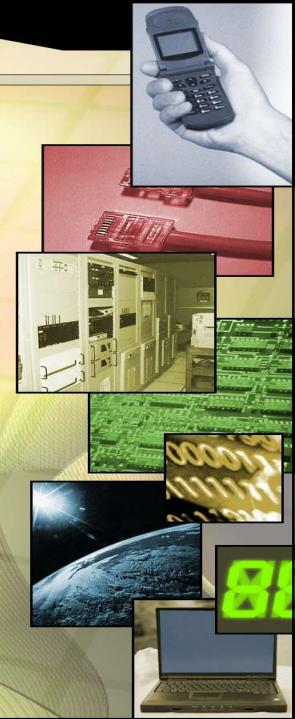
191



## NGƯỜI DÙNG (USER)

Ví dụ: Liệt kê danh sách người dùng

```
select * from sys.database_principals
where type not in ('A', 'G', 'R', 'X')
and sid is not null
and name != 'guest';
```

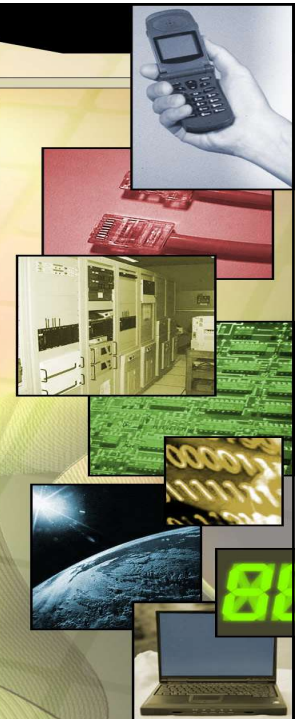


192

## NGƯỜI DÙNG (USER)

Ví dụ: Hiển thị tên người dùng hiện tại

```
select CURRENT_USER;
hoặc
select USER_NAME();
```

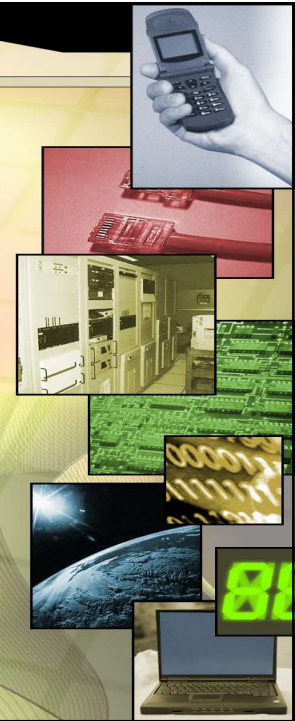


193

## NGƯỜI DÙNG (USER)

Ví dụ:

```
create login HS
    with password = '8fdkj13$nlnv';
use QLSV2019;
create user user1 for login HS
    with default_schema = marketing;
```



194

## NGƯỜI DÙNG (USER)

Ví dụ:

```
create user [HS\MyLogin]
for login [HS\MyLogin];
```



195

## NGƯỜI DÙNG (USER)

Ví dụ:

```
use QLSV2019 ;  
create user CustomApp without login ;  
grant impersonate on user::CustomApp  
to [HS\MyLogin] ;
```

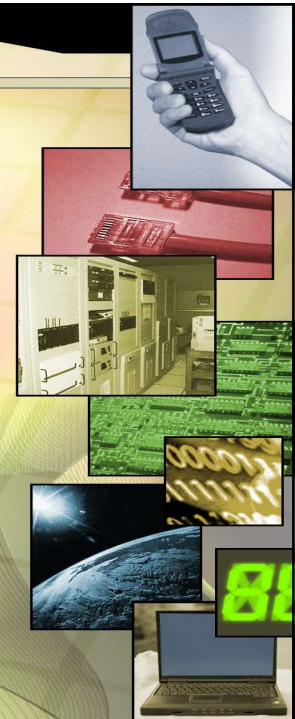


196

## NGƯỜI DÙNG (USER)

Ví dụ:

```
use QLSV2019 ;  
create user user1  
with password = 'RN92piTCh%$'  
    , default_schema = [dbo];
```



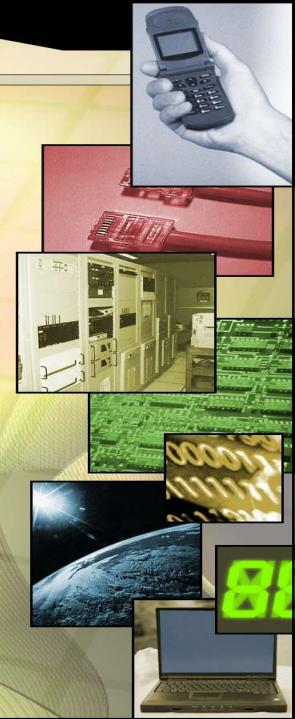
197



## NGƯỜI DÙNG (USER)

### ❖ Sửa đổi user

```
ALTER USER tên_user
WITH [ NAME = tên_user_mới ]
[ , DEFAULT_SCHEMA = tên_schema | NULL ]
[ , LOGIN = tên_login ]
[ , PASSWORD = 'mật_khẩu'
  [ OLD_PASSWORD = 'mật_khẩu_cũ' ]
];
```

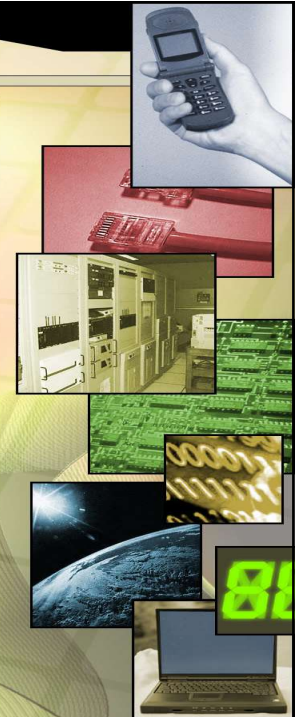


198

## NGƯỜI DÙNG (USER)

### ❖ Thiết lập / chuyển đổi user

```
EXECUTE | EXEC AS USER = 'tên_user' ;
```



199

## NGƯỜI DÙNG (USER)

### ❖ Xóa user

**DROP USER [ IF EXISTS ] 'tên\_user'**

200

## GRANT

### ❖ Lệnh GRANT được sử dụng để cấp thêm đặc quyền mới cho người dùng cơ sở dữ liệu.

**GRANT** < privileges >

**ON** < object >

**TO** < users | roles | PUBLIC >

**[ WITH GRANT OPTION ]**

201

## GRANT

- ❖ **PRIVILEGES:** quyền thực hiện những thao tác được cấp phát cho người dùng trên các đối tượng CSDL.  
*Ví dụ:* CREATE DATABASE, SELECT, INSERT, UPDATE, DELETE, EXECUTE, CREATE VIEW và **ALL**
- ❖ **OBJECT:** *một* đối tượng chịu tác động của các quyền.  
*Ví dụ:* DATABASE, FUNCTION, STORED PROCEDURE, TABLE, VIEW.
- ❖ **USERS:** các người dùng hoặc nhóm người dùng của CSDL.
- ❖ **WITH GRANT OPTION:** cho phép USERS cấp các quyền trong PRIVILEGES cho người dùng khác.

202

## GRANT

*Ví dụ:* Hiển thị các quyền hiện hành

- *Quyền trên SERVER*

```
select *
from fn_my_permissions(NULL, 'SERVER');
```

- *Quyền trên DATABASE*

```
select *
from fn_my_permissions(NULL, 'DATABASE');
```

203



## GRANT

Ví dụ: Cấp phát cho người dùng có tên user1 quyền thực thi các câu lệnh SELECT, INSERT và UPDATE trên bảng NHANVIEN

```
grant SELECT, INSERT, UPDATE
on NHANVIEN
to user1;
```

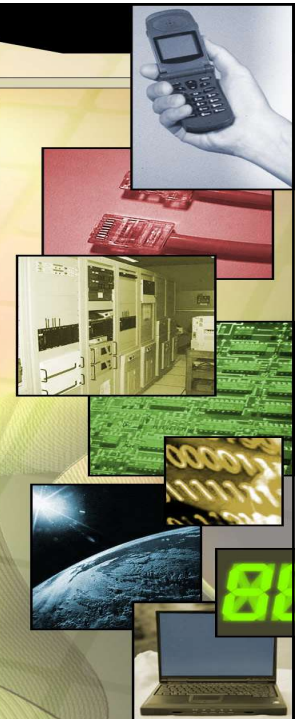


204

## GRANT

Ví dụ: Cho phép người dùng user1 quyền xem họ, tên, ngày sinh và giới tính của các nhân viên.

```
grant SELECT (honv, tennv, ngaysinh, gioitinh)
on NHANVIEN
to user1;
hoặc
grant SELECT
on object::NHANVIEN(honv, tennv, ngaysinh,
gioitinh)
to user1;
```



205

## GRANT

Ví dụ: Cấp phát cho người dùng user1 quyền tạo bảng và khung nhìn

```
grant CREATE TABLE, CREATE VIEW  
to user1;
```

206

## GRANT

Ví dụ: Cho phép người dùng user1 quyền xem, thêm, sửa dữ liệu trên schema user1Schema

```
grant SELECT, INSERT, UPDATE  
on schema::user1Schema  
to user1;
```

207

## GRANT

Ví dụ: Cấp phát cho người dùng user1 quyền CONTROL cho cơ sở dữ liệu QLSV2019

```
use QLSV2019;
grant control on database::QLSV2019
TO user1;
```

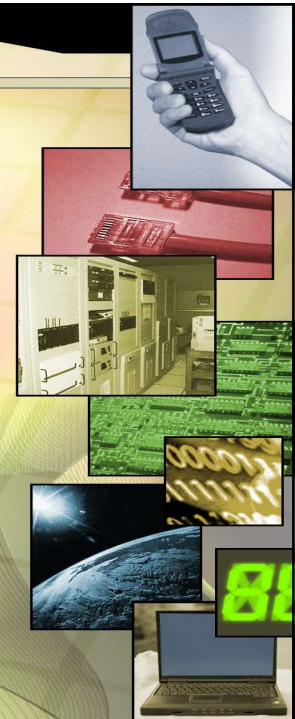


208

## REVOKE

- ❖ Lệnh REVOKE được dùng để loại bỏ các quyền truy xuất CSDL mà trước đó được gán thông qua lệnh GRANT.

```
REVOKE [ GRANT OPTION FOR ] < privileges >
ON < object >
FROM | TO < users | PUBLIC >
[ CASCADE ]
```



209



## REVOKE

- ❖ **PRIVILEGES:** các đặc quyền muốn loại bỏ từ người dùng. Lệnh này cũng sẽ loại bỏ việc chuyển giao hoặc từ chối (DENY) của người dùng đối với quyền bị loại bỏ (REVOKE)
- ❖ **GRANT OPTION FOR:** loại bỏ khả năng chuyển giao quyền và các quyền được gán cho người dùng khác nhưng đặc quyền được gán trước đó của user sẽ không bị loại bỏ.
- ❖ **CASCADE:** loại bỏ đặc quyền của các người dùng được cấp bởi user có tùy chọn WITH GRANT OPTION

210

## REVOKE

Ví dụ: Thu hồi quyền thực thi lệnh INSERT trên bảng NHANVIEN đối với người dùng user1.

```
revoke INSERT
on NHANVIEN
from user1;
```

211

## REVOKE

Ví dụ: Thu hồi quyền đã cấp phát trên cột NGAYSINH (chỉ cho phép xem dữ liệu trên cột HODEM và TEN) trên bảng NHANVIEN đối với người dùng user1.

```
revoke SELECT
on NHANVIEN(NGAYSINH)
from user1;
```

212

## REVOKE

Ví dụ: Người dùng A cấp phát quyền xem dữ liệu trên bảng R cho C:

```
grant SELECT on R to C
```

Người dùng B cấp phát quyền xem và bổ sung dữ liệu trên bảng R cho C:

```
grant SELECT, INSERT on R to C
```

Người dùng B thu hồi các quyền đã cấp trên bảng R của C: `revoke SELECT, INSERT on R from C`

*Người dùng C sẽ không còn quyền bổ sung dữ liệu trên bảng R nhưng vẫn có thể xem được dữ liệu của bảng này (quyền do A cấp cho C và vẫn còn hiệu lực).*

213



## REVOKE

Ví dụ: Cấp phát quyền xem dữ liệu cho người dùng A trên bảng R

**grant** SELECT **on** R **to** A **with grant option**

Người dùng A cấp phát cho người dùng B quyền xem dữ liệu trên R (vì A trước đó có *WITH GRANT OPTION*)

**grant** SELECT **on** R **to** B

Thu hồi quyền đã cấp phát cho người dùng A

**revoke** SELECT **on** R **from** A **CASCADE**

Câu lệnh trên sẽ đồng thời thu hồi quyền mà A đã cấp cho B (vì có *CASCADE*) và như vậy cả A và B đều không thể xem được dữ liệu trên bảng R.

214

## REVOKE

Ví dụ: Với ví dụ trước, nếu thay câu lệnh

**revoke** SELECT

**on** R **from** A **CASCADE**

bằng câu lệnh

**revoke** GRANT OPTION FOR SELECT

**on** R **from** A **CASCADE**

thì B sẽ không còn quyền xem dữ liệu trên bảng R đồng thời A không thể chuyển tiếp quyền cấp phát cho những người dùng khác (*tuy nhiên A vẫn còn quyền xem dữ liệu trên bảng R*).


215



## DENY

- ❖ Lệnh DENY được sử dụng để ngăn chặn việc người dùng có thể được cấp đặc quyền trong CSDL


**DENY** < privileges >  
**ON** < object >  
**TO** < users | PUBLIC >  
**[ CASCADE ]**



216

## ROLE

- ❖ Role là tập hợp các đặc quyền hoặc quyền truy cập.
- ❖ Được sử dụng trong việc cấp hoặc thu hồi quyền cho nhiều người dùng.
- ❖ Phân loại:
  - *Server Role*
  - *Database Role*
  - *Application Role*



217

## SERVER ROLE

- ❖ Nhóm các quyền ở mức server mà login khi được cấp sẽ có thể thực hiện một số thao tác xác định ở mức server.
- ❖ Server Roles cố định trong SQL Server
 

▪ <b>sysadmin</b>	▪ processadmin
▪ bulkadmin	▪ securityadmin
▪ dbcreator	▪ serveradmin
▪ diskadmin	▪ setupadmin



218

## SERVER ROLE

- ❖ Tạo Server Role mới  
**use master;**  
**CREATE SERVER ROLE** **tên\_server\_role**  
**[ AUTHORIZATION tên\_login\_cấp\_quyền ] ;**
- ❖ Gán thêm quyền cho role  
**GRANT** **các\_quyền\_server** **TO** **tên\_server\_role**  
**[ WITH GRANT OPTION ] ;**
- ❖ Gán role cho login | role khác  
**ALTER SERVER ROLE** **tên\_server\_role**  
**ADD MEMBER** **tên\_login** | **tên\_role\_con ;**



219



## SERVER ROLE

- ❖ Loại bỏ role của login | role khác

```
ALTER SERVER ROLE tên_server_role
DROP MEMBER tên_login | tên_role_con ;
```

- ❖ Đổi tên role

```
ALTER SERVER ROLE tên_server_role
WITH NAME = tên_server_role_mới ;
```

- ❖ Xóa role

```
DROP SERVER ROLE tên_server_role;
```

220

## SERVER ROLE

Ví dụ: Tạo role cấp quyền kết nối, tạo, xem CSDL cho đăng nhập xyz

```
use master;
create server role myRole;
alter server role [myRole] add member [xyz];
grant alter trace to [myRole];
grant connect sql to [myRole];
grant create any database to [myRole];
grant view any database to [myRole];
grant view any definition to [myRole];
grant view server state to [myRole];
GO
```

221



## SERVER ROLE

*Ví dụ:* Cấp quyền xử lý CSDL theo role **dbcreator** của SQL Server (CREATE, ALTER, DROP và RESTORE) cho đăng nhập xyz

```
use master;
create server role myRole;
alter server role [myRole]
    add member [xyz];
alter server role [dbcreator]
    add member [myRole];
GO
```

222

## DATABASE ROLE

- ❖ Tập hợp các quyền truy xuất CSDL thành từng nhóm và được đại diện bởi một tên dùng để cấp phát quyền truy cập CSDL cho các users.
- ❖ Database Roles có định trong SQL Server
 

▪ <b>db_owner</b>	▪ db_datawriter
▪ db_securityadmin	▪ db_datareader
▪ db_accessadmin	▪ db_denydatawriter
▪ db_backupoperator	▪ db_denydatareader
▪ db_ddladmin	

223

## DATABASE ROLE

- ❖ Tạo Database Role mới

```
CREATE ROLE tên_database_role
[ AUTHORIZATION tên_user_cấp_quyền ] ;
```

- ❖ Gán thêm quyền cho role

```
GRANT các_quyền_database TO tên_database_role
[ WITH GRANT OPTION ] ;
```

- ❖ Gán role cho user | role khác

```
ALTER ROLE tên_database_role
ADD MEMBER tên_user | tên_role_con ;
```

224

## DATABASE ROLE

- ❖ Loại bỏ role của user | role khác

```
ALTER ROLE tên_database_role
DROP MEMBER tên_user | tên_role_con ;
```

- ❖ Đổi tên role

```
ALTER ROLE tên_database_role
WITH NAME = tên_database_role_mới ;
```

- ❖ Xóa role

```
DROP ROLE tên_database_role;
```

225



## APPLICATION ROLE

- ❖ Cho phép các ứng dụng thực thi trên CSDL, tương tự như một user với các quyền hạn được gán. Ta có thể sử dụng APPLICATION ROLE 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.
- ❖ Cú pháp tạo APPLICATION ROLE  
**CREATE APPLICATION ROLE** *tên\_app\_role*  
**WITH PASSWORD** = '*mật\_khẩu*'  
**[ , DEFAULT\_SCHEMA = tên\_schema ] ;**



226

## APPLICATION ROLE

- ❖ Gán quyền cho APPLICATION ROLE  
**GRANT ... TO** *tên\_app\_role* ;
- ❖ Sửa đổi APPLICATION ROLE  
**ALTER APPLICATION ROLE** *tên\_app\_role*  
**WITH [ NAME = tên\_app\_role\_mới ]**  
**[ , PASSWORD = 'mật\_khẩu' ]**  
**[ , DEFAULT\_SCHEMA = tên\_schema ] ;**
- ❖ Xóa APPLICATION ROLE  
**DROP APPLICATION ROLE** *tên\_app\_role* ;



227



## APPLICATION ROLE

- ❖ Kích hoạt APPLICATION ROLE trong CSDL hiện hành

**EXECUTE** | **EXEC** *sp\_setapprole*

[ @rolename = ] '**tên\_app\_role**' ,

[ @password = ] '**mật\_khẩu**' ;

- ❖ Thủ tục sp\_setapprole chỉ có thể được gọi trực tiếp bằng lệnh EXECUTE (EXEC). Nó không thể được thực thi bên trong 1 thủ tục khác hay từ 1 transaction của người dùng

