TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THÔNG TIN TP.HCM

CHƯƠNG 6
QUẢN LÝ NGƯỜI DÙNG & BẢO VỆ HỆ THỐNG

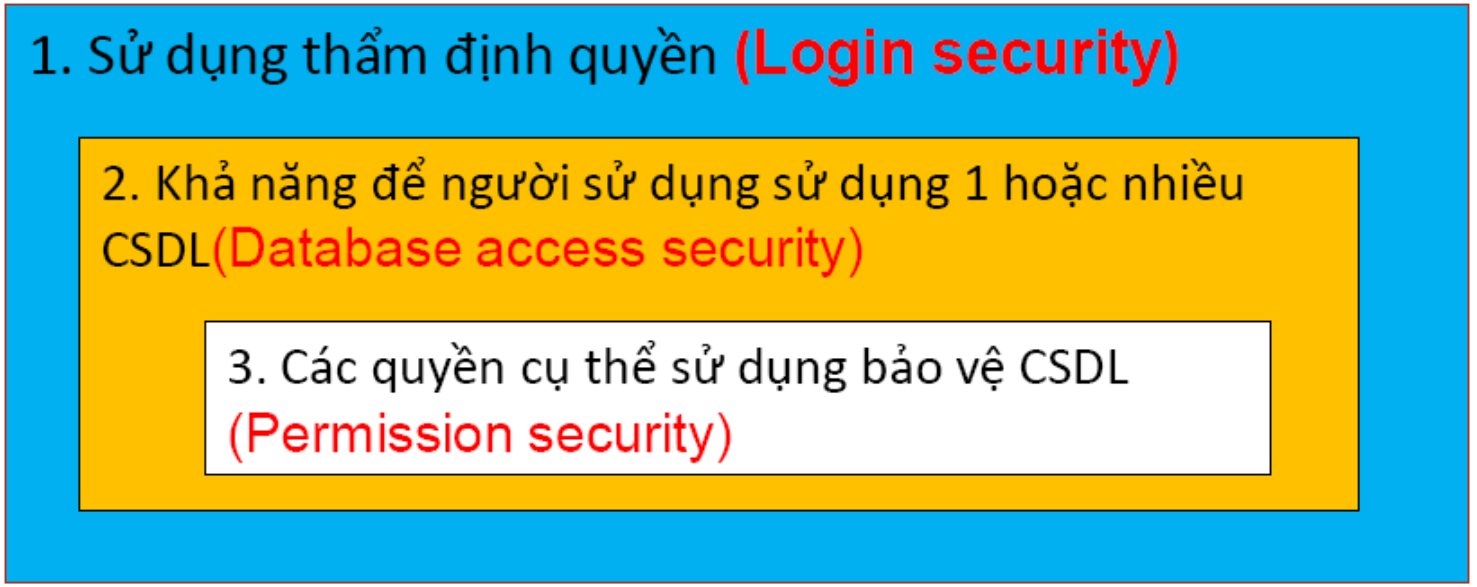
GV: Dương Quang Huy

NỘI DUNG

1. Giới thiệu.
2. Chế độ bảo mật.
3. Phân quyền người dùng.
4. Vai trò của Server và Database.
5. Quản trị người dùng.

Giới thiệu

- Bảo mật: là cho phép người quản trị CSDL tự ra quyết định cho phép, hay không cho phép người dùng truy cập và thao tác trên CSDL sao cho có hiệu quả bảo mật dữ liệu tốt nhất.
- Bảo mật trong SQL Server có thể sử dụng mô hình 3 tầng:



Chế độ bảo mật

- SQL Server có 2 chế độ bảo mật:

1. Windows Authentication Mode (Windows Authentication)
2. Mixed Mode (Windows Authentication and SQL Server Authentication)

Chế độ bảo mật

1. Windows Authentication:

- Là chế độ bảo mật mà những User truy nhập SQL Server phải là những User của Windows.

- Khi Server đặt ở chế độ bảo mật này, những User phải là những User được Windows quản lý mới được truy cập.

Chế độ bảo mật

2. SQL Server Authentication:

- Khi thiết lập ở chế độ bảo mật này, những User được quyền khai thác phải là những User do quản trị SQL_Server tạo ra.
- Những user của Windows không được khai thác.

Phân quyền người dùng

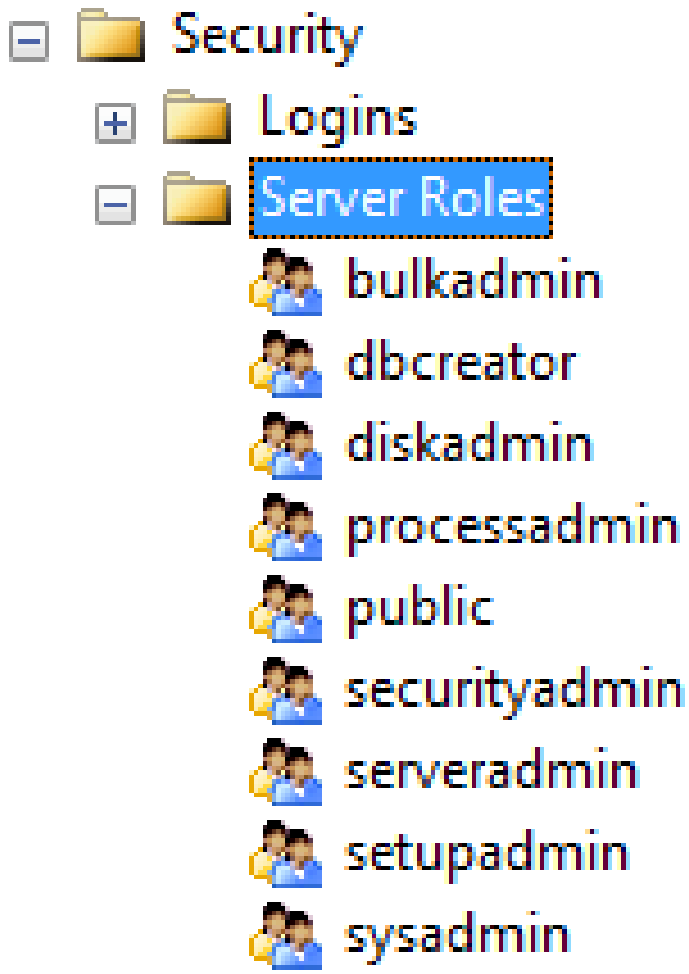
- Quyền người dùng được định nghĩa như mức độ người dùng có thể hay không thể thực thi trên CSDL, quyền được chia thành 4 loại như sau:
  - Quyền truy cập vào SQL Server
  - Quyền truy cập vào CSDL
  - Quyền thực hiện trên các đối tượng của CSDL.
  - Quyền xử lý dữ liệu.

Vai trò của Server và Database

- Role là một công cụ cho phép cấp quyền cho một nhóm user thay vì thực hiện trên từng user.
- Các quyền được grant, deny hay revoke trên role đều có hiệu lực với các thành viên của role.
- Nêu không còn muốn duy trì quyền hạn cho một user chỉ cần loại user khỏi danh sách các thành viên của role.
- Thường các role được định nghĩa dựa vào nhóm công việc của một nhóm các user.

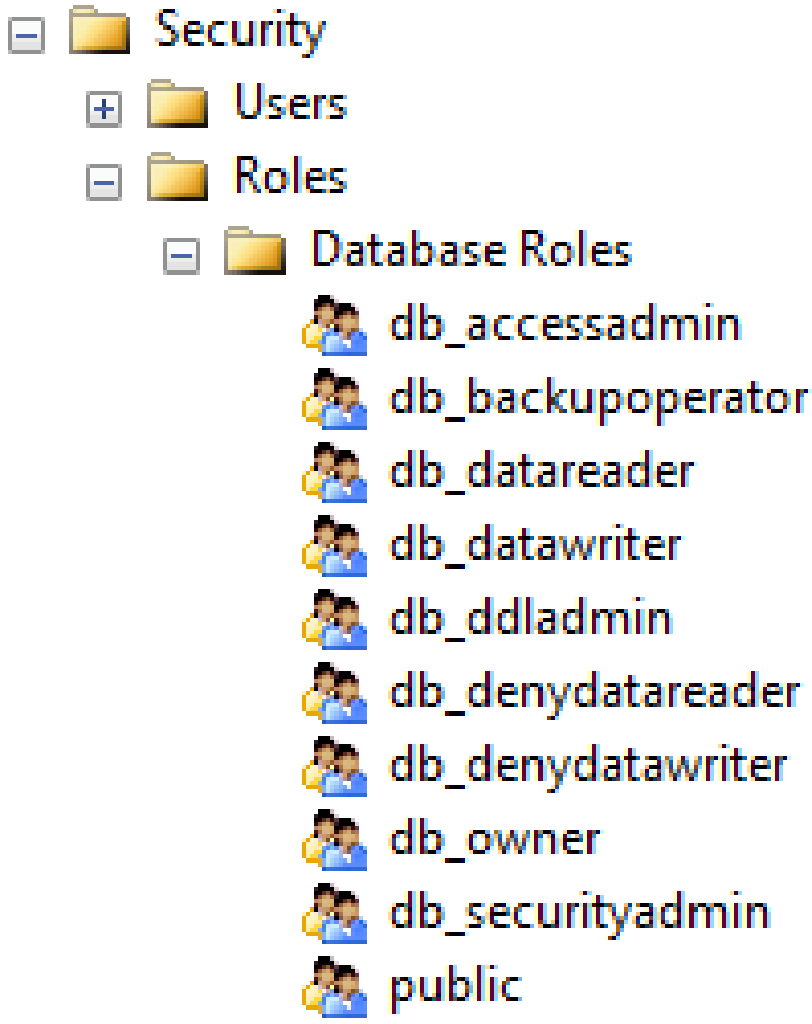
Vai trò của Server và Database

- Role mức Server do hệ thống tạo ra không thay đổi được.



Vai trò của Server và Database

- Role Database do CSDL quản lý, khi tạo CSDL hệ thống tự đặt một số Role ngầm định:



Vai trò của Server và Database

Tên Role	Diễn giải
Db_datawriter	Cho phép sửa chữa dữ liệu trong tất cả các bảng người dùng định nghĩa trong CSDL
Db_datareader	Cho phép người dùng hiển thị dữ liệu từ các bảng người dùng định nghĩa trong CSDL
Db_denydatawriter	Ngăn chặn người dùng sửa chữa dữ liệu trong bảng người dùng định nghĩa trong CSDL
Db_denydatareader	Ngăn chặn người dùng hiển thị dữ liệu trong bảng người dùng định nghĩa trong CSDL
Public	Vai trò public này hầu như không có quyền hạn ngoại trừ vài quyền rất cơ bản cho phép người dùng tạo kết nối tới CSDL

Vai trò của Server và Database

Tên Role	Diễn giải
Db_owner	Đây là vai trò cao nhất. Người dùng có toàn quyền kiểm soát CSDL. Người dùng sa là thành viên của vai trò này.
Db_securityadmin	Cho phép người dùng quản lý tất cả các vai trò và các thành viên của chúng. Vai trò này cũng cho phép gán các quyền hạn cho các vai trò.
Db_ accessadmin	Vai trò này dùng cung cấp các quyền người dùng để thêm hoặc gỡ bỏ các người dùng trong CSDL
Db_addadmin	Cho phép người dùng thao tác tất cả các đối tượng trong CSDL. Ví dụ: có thể tạo lập, sửa chữa hoặc xoá các đối tượng trong CSDL.
Db_backupoperator	Cho phép người dùng thực hiện thao tác sao chép dự phòng

Vai trò của Server và Database

- Tạo role trong CSDL hiện hành.
  - Sp_addrole 'role'
- Đưa một user vào role.
  - Sp_addrolemember 'role', 'user'
- Xóa nhóm.
  - Sp_droprole 'role'
- Xóa một thành viên trong nhóm.
  - Sp_droprolemember 'role', 'user'

Nhà quản trị hệ thống (System administrator)

- Nhà quản trị hệ thống có login là **sa**.
- Có toàn quyền truy xuất đến tất cả đối tượng trong SQL Server.
- Không thể xóa login **sa.**

Người chủ CSDL (database owner)

- Login dbo được gọi là database owner.
- **dbo** là thành viên của nhóm db_owner.
- Không thể xóa khỏi nhóm này.

Quản trị người dùng

- Người dùng trong SQL Server được chia thành 2 mức:
  - Người truy nhập vào SQL Server gọi là Login.
  - Người khai thác CSDL gọi là User.

Tạo đăng nhập(login)

- Tạo login bằng phát biểu SQL

```
Create Login Login_name with password=<password>
```

- Ví dụ:

```
Create login Teo with password = '123'
```

- Liệt kê danh sách login

```
Select  name, createdate
From    syslogins
```

Tạo đăng nhập(login)

- Tạo login bằng sp_addlogin:

```
EXEC sp_addlogin [@login= <'login'>]
                 [,@password= <'password'>]
                 [,@defdb= <'database'>]
```

- Ví dụ:

```
Use QL_BanHang
EXEC sp_addlogin 'Ty', '123'
```

Thay đổi password

- Cú pháp:

```
EXEC sp_password [@old= <'old password'>]
                 [,@new= <'new password'>]
                 [,@loginname= <'login'>]
```

- Ví dụ:

```
EXEC sp_password '123', 'abc', 'Ty'
```

Cấp quyền truy cập vào CSDL

- Cú pháp:

```
EXEC sp_grantdbaccess [@loginname = <'login'>]
                      [,@name_in_db=<'tên user'>]
```

- Ví dụ:

```
Use QL_BanHang
EXEC sp_grantdbaccess 'Ty', 'u1'
```

Xóa quyền truy cập vào CSDL

- Cú pháp:

```
EXEC sp_revokedbaccess [@name_in_db=<'tên user'>]
```

- Ví dụ:

```
Use QL_BanHang
EXEC sp_revokedbaccess 'u1'
```

Quyền thực hiện trên CSDL

- Cấp quyền tạo đối tượng.

```
Grant <all | các quyền > To [tên user]
```

  - Ví dụ: Cấp quyền tạo view

```
Use QL_BanHang
Grant Create Table, Create View To u1
```

- Cấm quyền tạo đối tượng.

```
Deny <all | các quyền > to [tên user]
```

  - Ví dụ:

```
DENY create table To u1
```

Quyền thực hiện trên CSDL

- **Các quyền:**
  - Create Database
  - Create Table
  - Create View
  - Create Proc
  - Create Rule
  - Create Default
  - Backup Database
  - Backup Log

Quyền xử lý dữ liệu

- Cấp quyền xử lý dữ liệu.

```
Grant <ALL| các quyền On <Table hay View> To <tên_user>
```

  - Ví dụ:

```
Grant Insert, Update, Delete On MatHang To u1
```

- Cấm quyền xử lý dữ liệu.

```
Deny <all | các quyền > on <bảng, view,…>to [tên_user]
```

  - Ví dụ:

```
Deny insert on MatHang to u1
```

Quyền xử lý dữ liệu

- **Các quyền:**
  - Select
  - Update
  - Insert
  - Delete
  - References
  - Execute

Quyền xử lý dữ liệu

- Grant/Revoke/Deny còn cho phép cấp quyền trên từng Field của table.

  - Ví dụ: Cho user u1 chỉ được quyền hiệu chỉnh dữ liệu trên các field trong bảng NhanVien

```
Grant Update(TenNV,Phai,DiaChi,NgaySinh)
ON NhanVien To u1
```

Ví dụ

- Tạo 3 login L1, L2, L3 có chung 1 password là '123' làm việc trên CSDL QL_BanHang.

```
Use master
Exec sp_addlogin 'L1', '123','QL_BanHang'
Exec sp_addlogin 'L2', '123','QL_BanHang'
Exec sp_addlogin 'L3', '123','QL_BanHang'
```

Ví dụ(tt)

- Tạo nhóm 'R' và cho L1, L2 thuộc nhóm này.

```
Use QL_BanHang
Exec sp_grantdbaccess @loginame='L1'
Exec sp_grantdbaccess @loginame='L2'
Exec sp_grantdbaccess @loginame='L3'
Exec sp_addrole 'R'
Exec sp_addrolemember 'R', 'L1'
Exec sp_addrolemember 'R', 'L2'
```

FAQ