# CHƯƠNG 5. CƠ CHẾ ĚẢM BẢO AN TOÀN TRONG

SQL SERVER

Ěể đảm bảo sự an toàn cho hệ thống thì ta phải cung cấp login name, password của mình cho hệ thống biết khi làm việc với SQL Server. Sau khi login, ta sẽ điều khiển được cơ sở dữ liệu theo kiểu mà người quản trị hệ thống cấp cho.

Các mức bảo mật:

1. Server : Login name
2. Database : User Name
3. Table : Grant / Revoke:

USER BINH chỉ được quyền xem điểm, toàn quyền trên SINHVIEN không được quyền thao tác trên LOP, MONHOC

1. Field : Grant / Revoke : SINHVIEN : user HOANG chỉ được quyền hiệu chỉnh field HO, TEN, không được xem NGAYSINH

## CÁC CƠ CHẾ AN TOÀN:

* 1. **Login vào Server của HĚH** (WINNT) : Khi login vào HĚH, ta phải cung cấp cho máy biết user name của mình và password.
  2. **Login vào SQL Server**: Tương tự như NT Server, SQL Server cǜng đòi hỏi khi ta login vào hệ thống thì phải có 1 danh hiệu cụ thể. Ta có thể đặt cấu hình của SQL Server để nó lấy thông tin login của NT Server hay đòi user phải vào login name. Một login của SQL Server là 1 đối tượng chứa **login name, password**, và các thuộc tính khác cho phép truy xuất cơ sở dữ liệu của SQL Server. Các login name phải khác nhau cho mỗi server.

Ta cần phải phân biệt rõ 1 số khái niệm giữa NT Server và SQL Server :

|  |  |  |  |
| --- | --- | --- | --- |
| **Thuật ngữ trong NT Server** | **Thuật ngữ trong**  **SQL Server** | **Mục đích** | **Ghi chú** |
| User (còn gọi là  user account) | Login | Ěối tượng chứa danh hiệu, password và các thuộc tính của user | * Login của SQL Server đại diện cho 1 người sử dụng đĕng nhập vào SQL Server * Một user của SQL Server đại diện cho 1 user của 1 cơ sở dữ liệu. |
| User Name | Login name | Danh hiệu | * UserName : tối đa 20 ký tự. * LoginName: tối đa 128 ký tự, chứa mọi ký tự, ngọai trừ ‘\’ |
| Group | Role | Ěối tượng chứa danh hiệu và các thuộc tính đại diện cho 1 nhóm các user |  |

* 1. **Nhóm trong SQL Server ( Role):** Role trong SQL Server là 1 đối tượng có các đối tượng user, hoặc role khác là thành viên
* Một user theo mặc định sẽ có tất cả các quyền mà nhóm nó thuộc về có. Nếu 1 user thuộc nhiều nhóm, user đó sẽ có tất cả các quyền mà các nhóm đó có.
* Nếu 1 user thuộc 1 nhóm A và nhóm A đó thuộc về 1 hay nhiều nhóm khác, thì user sẽ có các quyền của các nhóm khác mà user không thuộc về trực tiếp.

Như vậy, nhóm cung cấp 1 phương tiện đơn giản để quản lý sự an toàn, vì ta có thể tạo ra các nhóm để phản ánh các công việc cần làm, sau đó cho các user làm thành viên của nhóm. Có 3 loại role trong SQL Server:

* Role trên server (được định nghƿa sẵn bởi hệ thống)
* Role trên cơ sở dữ liệu (được định nghƿa sẵn bởi hệ thống)
* Nhóm user sử dụng cơ sở dữ liệu.
  + 1. Role trên server: có 9 nhóm. Ta không thể thay đổi, xóa role trên server. Nhà quản trị hệ thống có quyền thêm, xóa login, các thành viên của 1 server role. Một login có tất cả các quyền của các server role mà nó thuộc về.

|  |  |
| --- | --- |
| **Role Name** | **Khả nĕng** |
| dbcreator | Tạo và thay đổi cơ sở dữ liệu, phục hồi cơ sở dữ liệu. |
| diskadmin | Quản lý các file trên dƿa |
| processadmin | Quản lý các tiến trình đang hoạt động trong SQL Server |
| securityadmin | Quản lý việc logon cho server, thay đổi mật khẩu |
| serveradmin | Thiết lập cấu hình cho server |
| setupadmin | Có thể cài đặt việc nhân bản dữ liệu và quản lý các thủ tục mở rộng |
| **Sysadmin** | Thực hiện mọi thao tác trên server. |

* + 1. Role trên cơ sở dữ liệu (được định nghƿa bởi hệ thống): đối với cơ sở dữ liệu, SQL Server cung cấp 10 nhóm.

|  |  |
| --- | --- |
| **Role Name** | **Khả nĕng** |
| db\_accessadmin | Thêm hay xóa các user khỏi cơ sở dữ liệu. |
| db\_backupoperator | Có thể backup cơ sở dữ liệu. |
| db\_datareader | Ěọc tất cả dữ liệu từ các bảng trong cơ sở dữ liệu. |
| db\_datawriter | Thêm, hiệu chỉnh, xóa dữ liệu trong các bảng của cơ sở dữ liệu. |
| db\_ddladmin | Tạo, thay đổi, xóa các đối tượng trong cơ sở dữ liệu. |
| db\_denydatareader | Không thể đọc dữ liệu trong cơ sở dữ liệu. |
| db\_denydatawriter | Không thể hiệu chỉnh dữ liệu trong cơ sở dữ liệu. |
| **db\_owner** | Ěược thực hiện tất cả các thao tác trên cơ sở dữ liệu. |
| db\_securityadmin | Cho phép quản lý nhóm, và các thành viên của nhóm trong cơ sở dữ liệu; cấp và thu hồi quyền lên các đối tượng trong cơ sở dữ liệu. |
| public | Cho phép thực hiện các thao tác với các quyền đã được cho. |

* + 1. Nhóm user sử dụng cơ sở dữ liệu: Người tạo ra cơ sở dữ liệu có thể tạo ra các nhóm thao tác trên cơ sở dữ liệu, và gán các quyền cho các nhóm này. Mỗi user được đưa vào cơ sở dữ liệu đều tự động là thành viên của loại nhóm này, và người tạo cơ sở dữ liệu có thể đưa username vào bất kǶ nhóm nào trong cơ sở dữ liệu.

Ghi chú: *Cách tạo 1 nhóm sử dụng cơ sở dữ liệu xem ở phần sau trong chương này*.

## Nhà quản trị hệ thống (System Administrator):

* SQL Server có 1 nhà quản trị hệ thống mặc định với login name là **sa**. sa login là 1 thành viên của nhóm sysadmin, và có toàn quyền truy xuất tất cả đối tượng của SQL Server. Ta có thể cho 1 login vào nhóm sysadmin nhưng ta không thể xóa sa login.

## Database Owner (người chủ cơ sở dữ liệu):

Trong SQL Server, user tên **dbo** được gọi là database owner. User dbo luôn luôn là 1 thành viên của nhóm db\_owner và ta không thể xóa nó khỏi nhóm này.

## CÀI ĚẶT CÁC USER CỦA DATABASE:

Ta có các bước sau để thiết lập các đối tượng an toàn cho cơ sở dữ liệu của mình, và cài đặt các user sẽ truy xuất cơ sở dữ liệu. Sau khi các đối tượng đã được thiết lập, ta có thể cấp các quyền truy xuất cụ thể đến cơ sở dữ liệu để mọi người có thể làm việc với cơ sở dữ liệu theo cơ chế an toàn mà ta đã cho.

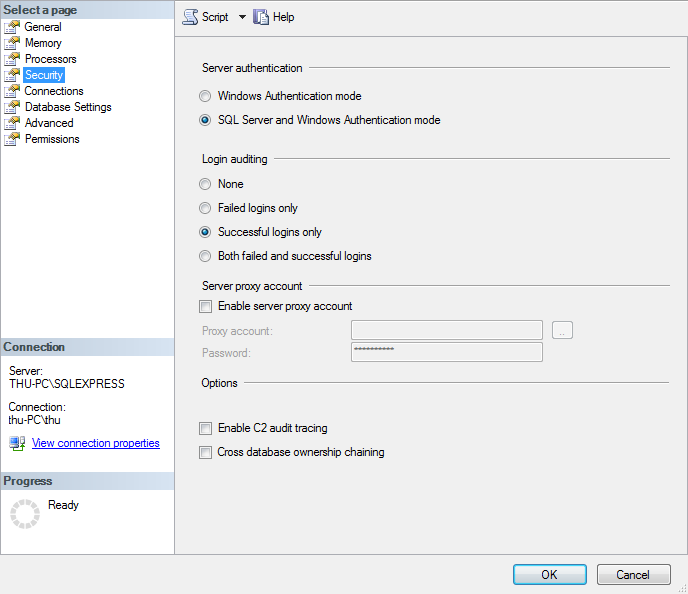
* 1. **Thiết lập kiểu an toàn cho SQL Server**: có 2 mode: dùng login WINNT để vào SQL Server hay phải có login name riêng.

Cách làm:

* Khởi động SQL Server Management Studio, connect vào SQL Server với tên login name

là **sa.**

* Right click trên tên server, chọn Properties / Security. Và chọn kiểu an toàn thích hợp

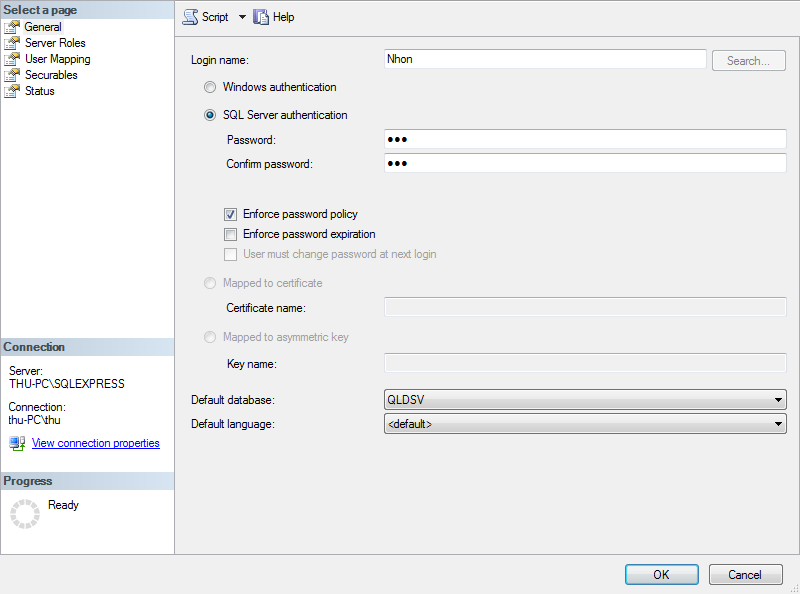


## Tạo login SQL Server cho user:

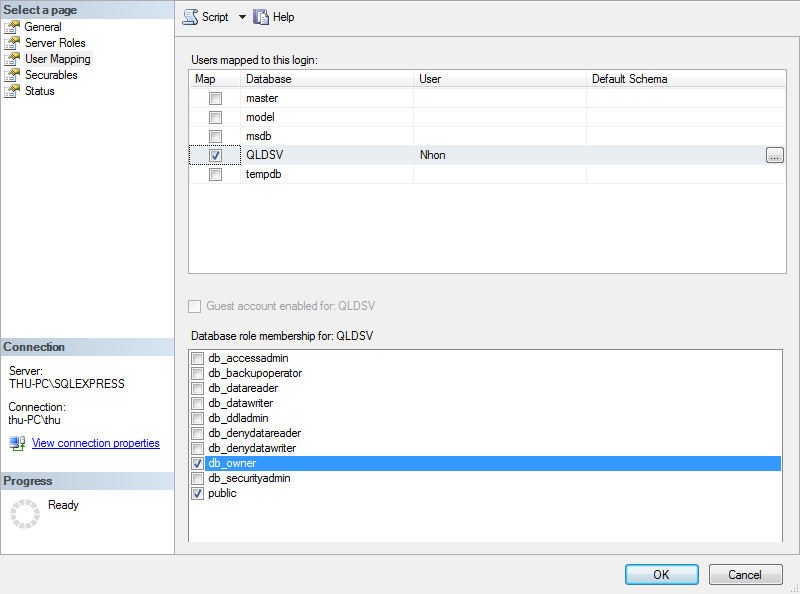
* Khởi động SQL Server Management Studio, connect vào SQL Server với tên login name

là **sa** hoặc tên login cho phép quản lý việc logon vào hệ thống.

* Mở rộng node Security, right click trên folder Logins / New Login (Nhon)



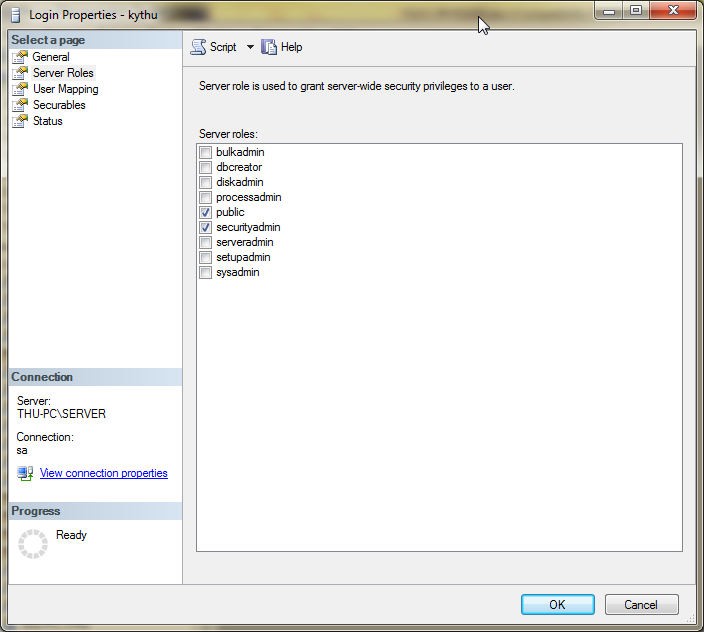
* 1. **Tạo User**: Tạo user Nhon và cho user Nhon thuộc nhóm db\_owner. Ta có 2 cách tạo user mới :
* Tạo user khi tạo login : trên cửa sổ login, chọn User Mapping, chọn check trên cơ sở dữ liệu (QLDSV) , ta sẽ thấy mặc định tên user cǜng là tên login (ta có thể sửa tên user)



- Tạo user: Right click trên đối tượng **User/ New Database User :**

Lưu ý:Nếu ta muốn login là 1 thành viên của nhóm SQL Server, ta đưa nó vào nhóm bằng

cách click tab Server Role.

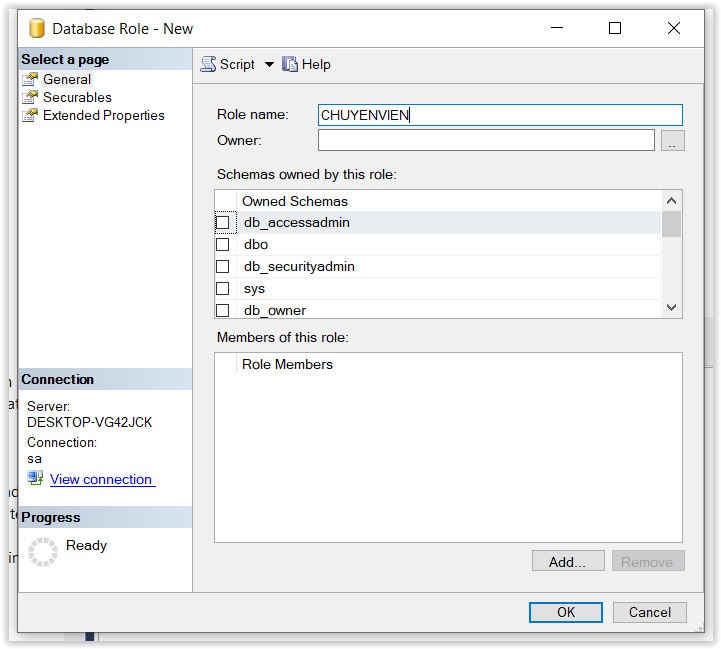


## Cài đặt các nhóm user sử dụng cơ sở dữ liệu:

Nếu ta không dùng nhóm NT Server để thiết lập các nhóm logic, ta nên tạo 1 nhóm user sử dụng cơ sở dữ liệu tại bước này.

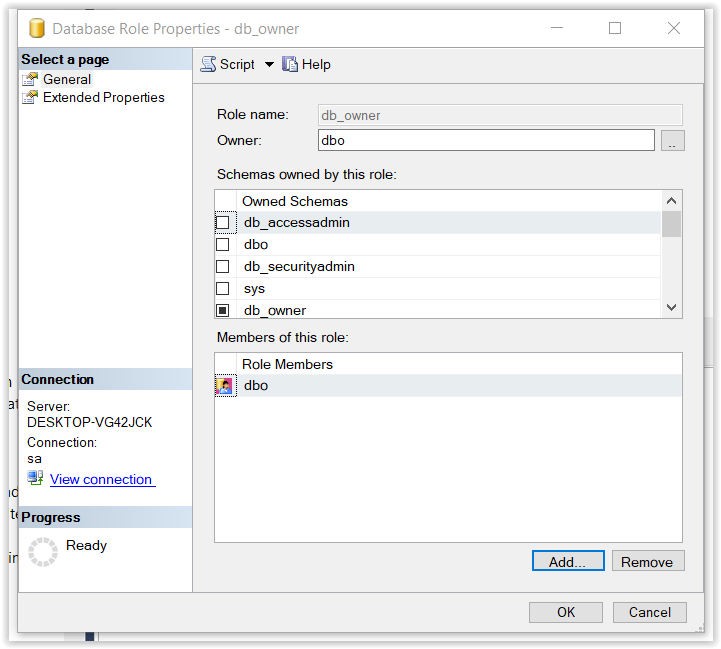
Cách làm:

* Khởi động SQL Server Enterprise Manager, mở rộng folder database.
  + Right click Roles/ New Database Role để tạo 1 nhóm user.
  + Gõ tên nhóm vào Name (CHUYENVIEN), chọn OK



-

Ěưa nhóm CHUYENVIEN vào nhóm db\_owner : Right click db\_owner/Properties:



Ěưa 1 role hoặc 1 user

vào nhóm

\* **Tóm lại**: SQL Server Management Studio đã cung cấp cho ta phương tiện thuận lợi để tạo

login name, nhóm và user name. Khi thực hiện ta nên cân nhắc các điều sau:

* Nếu ta tạo cơ sở dữ liệu mới với login name mới cho người sử dụng cơ sở dữ liệu, thì tạo cơ sở dữ liệu trước. Kế tiếp, tạo nhóm user-defined. Cuối cùng, mới tạo login name.
* Ta phải tạo 1 login name trước user name
* Ta có thể đặt login name trùng tên với tên user liên kết với nó; điều này sẽ tránh nhầm lẫn.
* Login name, username, tên role không nên quá 20 ký tự.

## III. CÁC STORED PROCEDURE LÀM VIỆC VỚI LOGIN:

1. **Tạo Login:**

return = **sp\_addLogin** ‘ten login’ , ‘password’ , ‘co so du lieu’ Nếu tên login tạo bị trùng thì sp\_addLogin trả về 1

## Thay đổi password của 1 login:

sp\_password ‘password cǜ’, ‘password mới’, ‘login’ Ví dụ: Thay đổi password cho login **Victoria** : ok.

EXEC sp\_password NULL, 'ok', 'Victoria'

1. **Cấp quyền truy xuất dữ liệu cho login:** return=sp\_grantdbaccess ’ten login’[, ‘TEN USER’] Nếu tên user tạo bị trùng thì sp\_ grantdbaccess trả về 1

## Ěưa một login vào server role :

|  |  |  |
| --- | --- | --- |
| sp\_add | **srv** | rolemember ‘logi |

n’, ‘role’

## Xóa login:

sp\_droplogin ‘login’

1. **Tạo nhóm**: tạo nhóm trong cơ sở dữ liệu hiện hành sp\_addrole ‘role’

## Ěưa một user vào role:

sp\_addrolemember ‘role’, ‘user’

## Xóa nhóm:

sp\_droprole ‘role’

## Xóa một thành viên trong nhóm:

sp\_droprolemember ‘role’, ‘user’

Ví dụ:

* Tạo 3 login Nhon, Thao, Trang có chung 1 password l ‘password’ làm việc trên cơ sở dữ liệu QLVT
* Tạo nhóm PKD cho 2 user Nhon, Thao thuộc nhóm này. EXEC sp\_addlogin ‘Nhon’, ‘password’, ‘QLVT’

EXEC sp\_addlogin ‘Thao’, ‘password’, ‘QLVT’

EXEC sp\_addlogin ‘Trang’, ‘password’, ‘QLVT’

EXEC sp\_grantdbaccess ‘Nhon’

EXEC sp\_grantdbaccess @loginame = ‘Thao’ EXEC sp\_grantdbaccess @loginame = ‘Trang’ EXEC sp\_addrole ‘PKD’

EXEC sp\_addrolemember ‘PKD’, ‘Nhon’

EXEC sp\_addrolemember ‘PKD’, ‘Thao’

**Bài tập**:

* 1. Dùng SQL Server Management Studio để thực hiện việc tạo 2 nhóm PKD, PKT và cho 3 user Nhon, Thao , Trang thuộc nhóm PKD; cho user Trang thuộc PKT.

1. Bạn hãy cho biết thông tin login của SQL Server được lưu trong table nào? Nếu ta login vào Server với login và password đã tạo từ 1 phần mềm lập trình cơ sở dữ liệu như Visual Basic hoặc Visual C thì có được hay không?
2. Bạn hãy cho biết thông tin user, role và thông tin user là 1 thành viên của role được lưu vào trong table hệ thống nào?
3. Viết 1 SP **Ds\_nhom** trả về danh sách các nhóm mà 1 username là 1 thành viên. Kết xuất có dạng : mã nhóm, tên nhóm
4. Viết 1 SP **DS\_user** trả về danh sách các user là thành viên của 1 nhóm @X. Kết xuất có dạng : username.
5. Viết stored procedure tên sp\_TaoTaiKhoan với các tham số (@LGNAME ,

@PASS, @USERNAME , @ROLE) để tạo tài khoản và user tương ứng. Nếu @role = ’Admin’ thì tài khoản này được quyền tạo tài khoản mới, được sao lưu và phục hồi cơ sở dữ liệu.

1. Viết stored procedure tên sp\_ThongTinDangNhap @tenlogin để trả về username , rolename của @tenlogin