**Môn học: Quản trị hệ cơ sở dữ liệu**

**Bài thực hành:**

**Bảo mật (phần 1/2)**

**Nội dung (Lý thuyết ở chương 5):**

**Tham khảo: Chapter 6 – Sách Beginning SQL Server 2008 Administration**

**BÁO CÁO NỘI DUNG THỰC HÀNH**

Họ tên sinh viên:

Mã số sinh viên:

Lớp:

Số máy tính:

Ngày, buổi thực hành: 11/11/2024

Các câu hỏi, bài thực hành: Sinh viên có thể trả lời bằng cách gõ văn bản hay chụp màn hình dán vào ngay tại sau mỗi câu hỏi

Sơ đồ kết nối và bảo mật của SQL server:



***Trên máy host Windows 10, SQL 2019 developer, thực hiện các bài thực hành sau:***

1. Dùng chức năng của hệ điều hành Windows để tạo người dùng của hệ điều hành mới (Windows local user mới) tên TenMayTinh\WindowsUser1 (ví dụ C50\ WindowsUser1). Trong SQL Server, dùng login có quyền cao (như sa hay TenMayTinh\Admin) để tạo Log in mới từ Windows local user vừa tạo. Sign out Windows và sign in lại dùng Windows local user mới để đăng nhập hệ điều hành và đăng nhập SQL Server. Hình minh họa:

Graphical user interface, application

Description automatically generated

+ b1: this pc -> tao user ms

+ b2: vaof sqlserver tao login bang user do -> siginout dang nhap bang user moi tao

**Từ câu 2, nếu làm trên phòng máy thì nên cài một instance mới để thực hành**

1. Tạo 2 login của SQL Server tên SQLLogin1, SQLLogin2 (chưa phân quyền, để toàn bộ thông số mặc định, chụp login properties sau khi tạo)

* Tạo 2 login mới trong sa or admin
* Phân quyền (tại user admin or sa ) trực tiếp or gián tiếp () -> chọn login mún phân quyền -> property -> ServerRole or securables-> Chọn quyền muốn phân
* ở dây quyền là : Create any database -> giant , view any database -> deny, riêng nếu chọn serverRole thì k có quyền từ chối vẫn phải vô từ chỗi trực tiếp

1. Gán quyền cho SQLLogin1 để có thể tạo cơ sở dữ liệu nhưng không thể xem thấy được tất cả các cơ sở dữ liệu do login khác tạo ra, chụp cửa sổ phân quyền, chụp tạo thành công 1 cơ sở dữ liệu ABC, chụp các CSDL mà login SQLLogin1 nhìn thấy
2. Gán quyền cho SQLLogin2 để có thể tạo login mới, xem, sửa các login đã tạo. Chụp đăng nhập bằng SQLLogin2 và tạo thành công 1 login mới LogAFromLG2, sau đó sửa thành login LogBFromLG2.

* Làm như trên chọn quyền -> alter any login

1. Tạo SQLLogin3 và gán cho login SQLLogin3 thành database user tên SQLLogin3\_DBuser1 của cơ sở dữ liệu AdventureWorks (Chụp login property của SQLLogin3, tab User Mapping; chụp property của SQLLogin3\_DBuser1)

* Tạo user xong vô property-> userMap -> chọn db muốn gán quyền

1. Gán quyền cho SQLLogin3\_DBuser1 chỉ được xem và thêm dữ liệu nhưng không cho xóa dữ liệu bảng department (Chụp màn hình phân quyền), và kiểm tra quyền.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Vào admin chọn db được user gán quyền -> property-> chọn securable -> search -> all object type -> chọn bảng-> chọn bảng muốn gán quyền -> ở phân permission chọn quyền muốn gán.

1. Tạo mới một server role tên **QLLogin\_TaoDB\_KhongXemThayTenDB** có các quyền:  
   - quản lý các login (thuộc server role **SecurityAdmin**)  
   - tạo, xóa, sửa, phục hồi CSDL (thuộc server role **dbCreator**)  
   - không nhìn thấy tên các CSDL do login khác tạo (bị deny hành động **View any database**)  
     
   Tạo SQLLogin4 và gán cho login SQLLogin4 làm thành viên của server role mới **QLLogin\_TaoDB\_KhongXemThayTenDB.** Đăng nhập bằng login SQLLogin4 để thử các quyền của role.

* Vào sa tạo login4
* Sa -> security -> serverRole -> tạo new
  + Nếu mún roles trong roles thì -> membership chọn -> role mình muốn nương nhờ
  + Chọn quyền trực tiếp ở general -> chọn server -> tên server của mình -> chọn các quyền muốn cho phép
* Gán quyền cho login4

1. Tạo mới một database role Trong CSDL Northwind tên **XemThemKhongSuaXoaNhanVien** có quyền:  
   - cho xem, thêm nhưng không cho sửa, xóa dữ liệu bảng dbo. Employees  
     
   Tạo SQLLogin5, gán login SQLLogin5 làm database user tên **SQLLogin5\_DBUser** của CSDL Northwind. Gán **SQLLogin5\_DBUser** làm thành viên của server role mới **XemThemKhongSuaXoaNhanVien.** Đăng nhập bằng login SQLLogin5 để thử các quyền của database role.

* Tạo DB roles
  + muốn gán quyền cho user (Northwind) -> sercurity -> Roles -> dbRoles -> news -> nhập tên -> sercurable -> chọn bảng muốn phân quyền
* Khi tạo user xong -> property -> Usermap -> chọn db muốn phân quyền -> chọn quyền bên dưới
* Or Gán quyền cho user -> ... -> Sercurity -> User -> chọn user muốn gán quyền -> gán quyền mới tạo
* Test quyền

1. Tạo mới một application role Trong CSDL Northwind tên **XemThemKhongSuaXoaKhachHang** có password là “P@ssw0rd”, schema mặc định là “dbo”, không có làm chủ (own) schema nào, có quyền:  
   - cho xem, thêm nhưng không cho sửa, xóa dữ liệu bảng dbo. Customers  
     
   Tạo một ứng dụng mới trong Visual Studio để kết nối CSDL Northwind, dùng application role vừa tạo.

***Trên máy ảo Windows 2003 Server, SQL 2005 developer, thực hiện các bài thực hành sau:***

1. Tạo 1 domain account mới tên MSSV của SV làm bài, tạo login từ account của domain này, và đăng nhập thành công vào Domain và SQL Server (chưa phân quyền, chụp màn hình chỉnh domain policies, chụp khi đăng nhập thành công bằng login MSSV)
2. Gán cho login MSSV thành database user tên DBuser2 của cơ sở dữ liệu AdventureWorks (Chụp login property của MSSV, tab User Mapping; chụp property của DBuser2)
3. Gán quyền cho database user DBuser2 để chỉ có quyền duy nhất: SELECT trên 2 cột EmployeeID và BirthDate của bảng Employee (Chụp màn hình phân quyền, chụp chạy thành công câu lệnh SELECT trên 2 cột trên, chụp SELECT không thành công trên cả bảng Employee)
4. Tạo 1 login của SQL Server tên SQLLogin3, gán thành user DBuser3 của cơ sở dữ liệu AdventureWorks, gán DBuser3 là thành viên Database role db\_datareader. Đăng nhập bằng SQLLogin3, hỏi:
   1. Chụp danh sách các table của CSDL AdventureWorks trong cửa sổ Object explorer. Select một bảng bất kỳ, chụp kết quả và giải thích tại sao.
   2. Chọn Deny quyền View definition trên table HumanResouces.Department của DBuser3. Chụp lại danh sách các table của CSDL AdventureWorks trong cửa sổ Object explorer. So sánh khác biệt với câu a. Chạy lệnh ‘SELECT \* FROM HumanResouces.Department’, chụp kết quả và giải thích.
   3. Lấy lại quyền View definition, nhưng deny quyền Select trên table HumanResouces.Department của DBuser3. Chụp lại danh sách các table của CSDL AdventureWorks trong cửa sổ Object explorer và giả thích. Chạy lệnh ‘SELECT \* FROM HumanResouces.Department’, chụp kết quả và giải thích.
5. Tạo 1 login của SQL Server tên SQLLogin4, gán thành user DBuser4 của cơ sở dữ liệu AdventureWorks. Tìm phương án gán quyền để DBuser4 có thể sao lưu CSDL AdventureWorks, nhưng không thấy nội dung bên trong (View definition) của CSDL AdventureWorks. Liệt kê và chụp các bước thực hiện.

Bài về nhà:

1. **Tạo code gán quyền quản trị**: Sử dụng Object Explorer và Query Editor để tạo script gán quyền cho login (chừng nào thực thi script thì mới gán quyền). Xem và gán quyền trên server cho các login ở mục Permision của cửa sổ Property của Instance (chú ý sau khi chọn quyền thì tạo script chứ không nhấn nút OK để gán quyền ngay mà phải nhấn nút Cancel để đóng cửa sổ), các yêu cầu báo cáo:
   * Tạo script gán quyền (GRANT) “thay đổi các login” cho 1 login, lưu script vào “GanQuyenThayDoiLogin.sql”. Sau khi gán quyền bằng cách chạy script, ta thử xem việc gán quyền có tác dụng chưa. Báo cáo chụp từng bước để tạo login, tạo script sau (tên login có thể không giống), và bước thử sử dụng quyền đã gán:

use [master]

GO

GRANT ALTER ANY LOGIN TO [sqlLogin1]

GO

* + Tạo script gán quyền là thành viên của 1 server role “dbcreater” cho 1 login, lưu script vào “GanQuyenThuocServerRoleDBcreater.sql”. Sau khi gán quyền bằng cách chạy script, ta thử xem việc gán quyền có tác dụng chưa. Báo cáo chụp từng bước để tạo login, tạo script sau (tên login có thể không giống), và bước thử sử dụng quyền đã gán:

EXEC master..sp\_addsrvrolemember @loginame = N'sqlLogin2', @rolename = N'dbcreator'

GO

1. **Tạo code gán quyền trên dữ liệu**: Sử dụng Object Explorer và Query Editor để tạo script gán quyền cho database user (chừng nào thực thi script thì mới gán quyền). Xem và gán quyền trên dữ liệu cho database user ở mục Securables của cửa sổ Property của 1 database user (chú ý sau khi chọn quyền thì tạo script chứ không nhấn nút OK để gán quyền ngay, mà phải nhấn nút Cancel để đóng cửa sổ), các yêu cầu báo cáo:
   * Tạo script gán quyền (GRANT) Select cho 1 database user, lưu script vào “GanQuyenSelectDuLieu.sql”. Sau khi gán quyền bằng cách chạy script, ta thử xem việc gán quyền có tác dụng chưa. Báo cáo chụp từng bước để tạo database user của CSDL AdventureWorks, tạo script (tên database user có thể không giống), và bước thử sử dụng quyền đã gán:

use [AdventureWorks]

GO

GRANT SELECT ON [HumanResources].[Department] TO [DBUSer1]

GO

* + Tạo script gán quyền là thành viên của 1 database role “db\_datawriter” cho 1 database user, lưu script vào “GanQuyenThuocRoleDataWriter.sql”. Sau khi gán quyền bằng cách chạy script, ta thử xem việc gán quyền có tác dụng chưa. Báo cáo chụp từng bước để tạo database user của CSDL AdventureWorks, tạo script (tên database user có thể không giống), và bước thử sử dụng quyền đã gán:

USE [AdventureWorks]

GO

EXEC sp\_addrolemember N'db\_datawriter', N'DBUSer2'

GO