Bảo mật trong SQL Server

Nội dung

- Bảo mật cơ sở dữ liệu
  - Khái niệm cơ bản
  - Xác thực đăng nhập
  - Úy quyền người dùng CSDL
  - Quyền truy nhập của người sử dụng
  - Ví dụ minh họa
  - Thảo luận

Bảo mật dữ liệu

- **Bảo mật cơ sở dữ liệu** là sự bảo vệ dữ liệu trong CSDL, chống lại những truy nhập, sửa đổi hay phá hủy bất hợp pháp.
- Người sử dụng hợp pháp là những người sử dụng được cấp phép, được ủy quyền. Ngược lại là những người sử dụng bất hợp pháp.
- Để đảm bảo tính an toàn cho cơ sở dữ liệu, cần có một cơ chế để quản lý người dùng hợp lý.
- Những nhóm người dùng khác nhau trong hệ CSDL có quyền sử dụng khác nhau đối với các dữ liệu trong CSDL.

Các quyền truy nhập của người sử dụng

- Quyền **đọc dữ liệu**: được phép đọc một phần hay toàn bộ dữ liệu trong CSDL
- Quyền **cập nhật dữ liệu**: được phép sửa đổi một số giá trị nhưng không được xóa dữ liệu trong CSDL
- Quyền **xóa dữ liệu**: được phép xóa dữ liệu trong CSDL
- Quyền **bổ sung dữ liệu**: được phép thêm dữ liệu mới vào trong CSDL nhưng không được phép thay đổi dữ liệu
- Quyền **tạo chỉ dẫn** trên các quan hệ trong CSDL
- Quyền **thay đổi sơ đồ cơ sở dữ liệu**: thêm hay xóa các thuộc tính của các quan hệ trong CSDL
- Quyền **loại bỏ quan hệ** trong CSDL

…

Trách nhiệm của người quản trị hệ thống

- Để có thể phân biệt được người sử dụng trong hệ CSDL, người quản trị hệ thống phải có trách nhiệm:
  - Xác định các quyền cụ thể mà mỗi người sử dụng hay một nhóm người sử dụng được phép thực hiện, xác định vai trò và trách nhiệm của mỗi người sử dụng. Điều này được gọi chung là **Phân quyền người sử dụng**
  - Cung cấp một phương tiện cho người sử dụng để hệ thống có thể nhận biết được người sử dụng đó hay còn gọi là **Xác minh người sử dụng**

Xác thực người sử dụng

- Để xác thực được người sử dụng, người ta có thể dùng các kỹ thuật sau:
  - Kỹ thuật dùng tài khoản và mật khẩu
  - Kỹ thuật sử dụng các hàm kiểm tra cho người sử dụng: Đối sánh kết quả của y = F(x) giữa hệ thống và người dùng.
  - Kỹ thuật dùng thẻ điện tử, thẻ thông minh.
  - Kỹ thuật sử dụng nhận dạng tiếng nói, hình ảnh, QR code, vân tay, v..v.
  - …

Kiểm tra quyền truy nhập của người sử dụng

- Mỗi người sử dụng sẽ có một bộ hồ sơ do người quản trị thiết lập và được hệ thống quản lý, trong hồ sơ đó sẽ có chi tiết về các thao tác người sử dụng được phép thực hiện:
  - **Phân quyền người sử dụng**: Người quản trị hệ thống phải có trách nhiệm xác định khung nhìn để kiểm soát xem mỗi người sử dụng chỉ được truy nhập phần dữ liệu nào trong CSDL và có được các quyền nào trong số các quyền đọc, thêm, xóa , sửa đổi.
  - **Xác định và kiểm soát sự lưu chuyển dữ liệu**: Hệ thống phải bảo trì danh sách các quyền một cách chặt chẽ vì người sử dụng có thể được quyền lan truyền các quyền cho người sử dụng khác.

Login, User và quyền truy cập CSDL

- Login
- User
- Quyền
- Vai trò (Role)

Create Login

- 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 (nên trước khi tạo người dùng trong SQL Server bạn phải tạo tài khoản đăng nhập trước).
- Cách 1: create login tên_login with password = 'nhập_mật_khẩu'
- Cách 2: sp_addlogin 'tên_login','mật_khẩu

  Sắp bị loại khỏi SQL server

Create User

- CREATE USER tạo user để thực hiện các thao tác trên một cơ sở dữ liệu trong SQL Server. Một sẽ được ánh xạ đến Login, định danh được dùng để kết nối với một instance SQL Server cụ thể.
- Cách 1: create user tên_user for login tên_login
- Cách 2: sp_adduser 'tên_login','tên_user'
  Sắp bị loại khỏi SQL server

Login với User

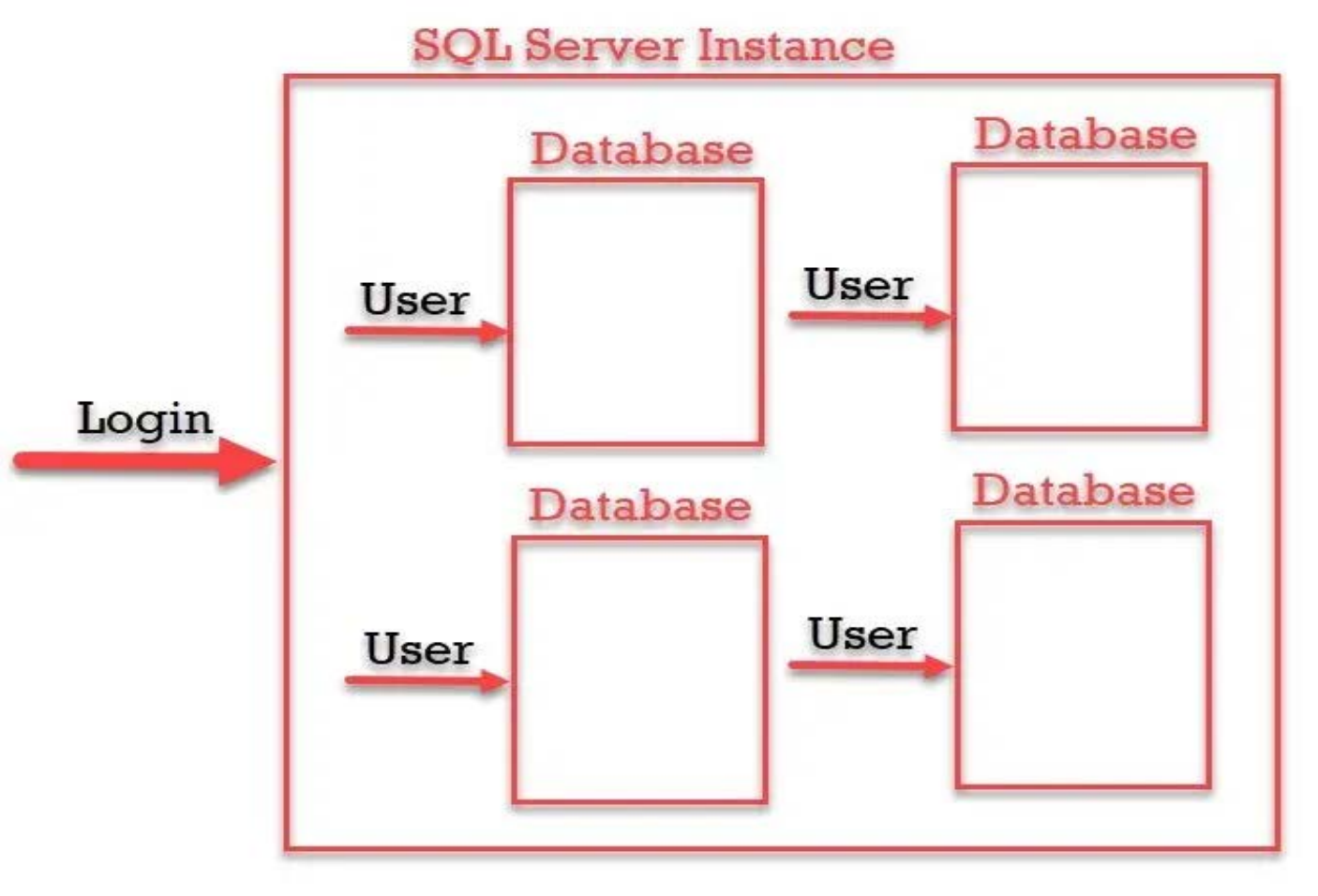
- SQL Login là Authentication (xác thực)

Quyết định BẠN có quyền để truy cập tới server hay là không

- SQL Server User là Authorization (ủy quyền)

Quyết định những thao tác nào mà BẠN có thể thực hiện (Thao tác) trên 1 cơ sở dữ liệu

Login với User



Phân quyền cho User

- GRANT <D/s thao tác> ON <Đối tượng> TO <D/s User> [WITH GRANT OPTION]
  - <D/s thao tác>: có thể bao gồm 1 hay nhiều thao tác được liệt kê dưới đây:
  - Insert: chèn dữ liệu vào trong CSDL có sẵn nhưng không được thay đổi bất kỳ mục dữ liệu nào trong CSDL
  - Update: sửa đổi dữ liệu nhưng không được xóa dữ liệu
  - Delete: xóa dữ liệu trong CSDL
  - Select : tìm kiếm
  - Alter: Thay đổi cấu trúc của quan hệ
  - All

Phân quyền cho user

Quyền	Mô tả
SELECT	Khả năng thực hiện lệnh SELECT trên bảng
INSERT	Khả năng thực hiện lệnh INSERT trên bảng
UPDATE	Khả năng thực hiện lệnh UPDATE trên bảng
DELETE	Khả năng thực hiện lệnh DELETE trên bảng
REFERENCES	Khả năng tạo ràng buộc tham chiếu tới bảng
ALTER	Khả năng thực hiện lệnh ALTER TABLE trên bảng để thay đổi định nghĩa bảng.
ALL	ALL không trao tất cả quyền trên bảng mà trao các quyền theo chuẩn ANSI-92, gồm SELECT, INSERT, UPDATE, DELETE và REFERENCES.

Phân quyền cho user (tiếp)

- <Đối tượng>: bảng/khung nhìn/ thủ tục/ …
- <D/s người dùng>: Một người hay một nhóm hay một danh sách người sử dụng. Từ khóa public được dùng thay thế cho mọi người sử dụng
- [With Grant Option] Nếu dùng từ khóa này trong câu lệnh phân quyền thì người dùng xuất hiện trong <D/s người dùng> có quyền được lan truyền các quyền vừa được tuyên bố cho những người dùng khác

Ví dụ phân quyền cho user

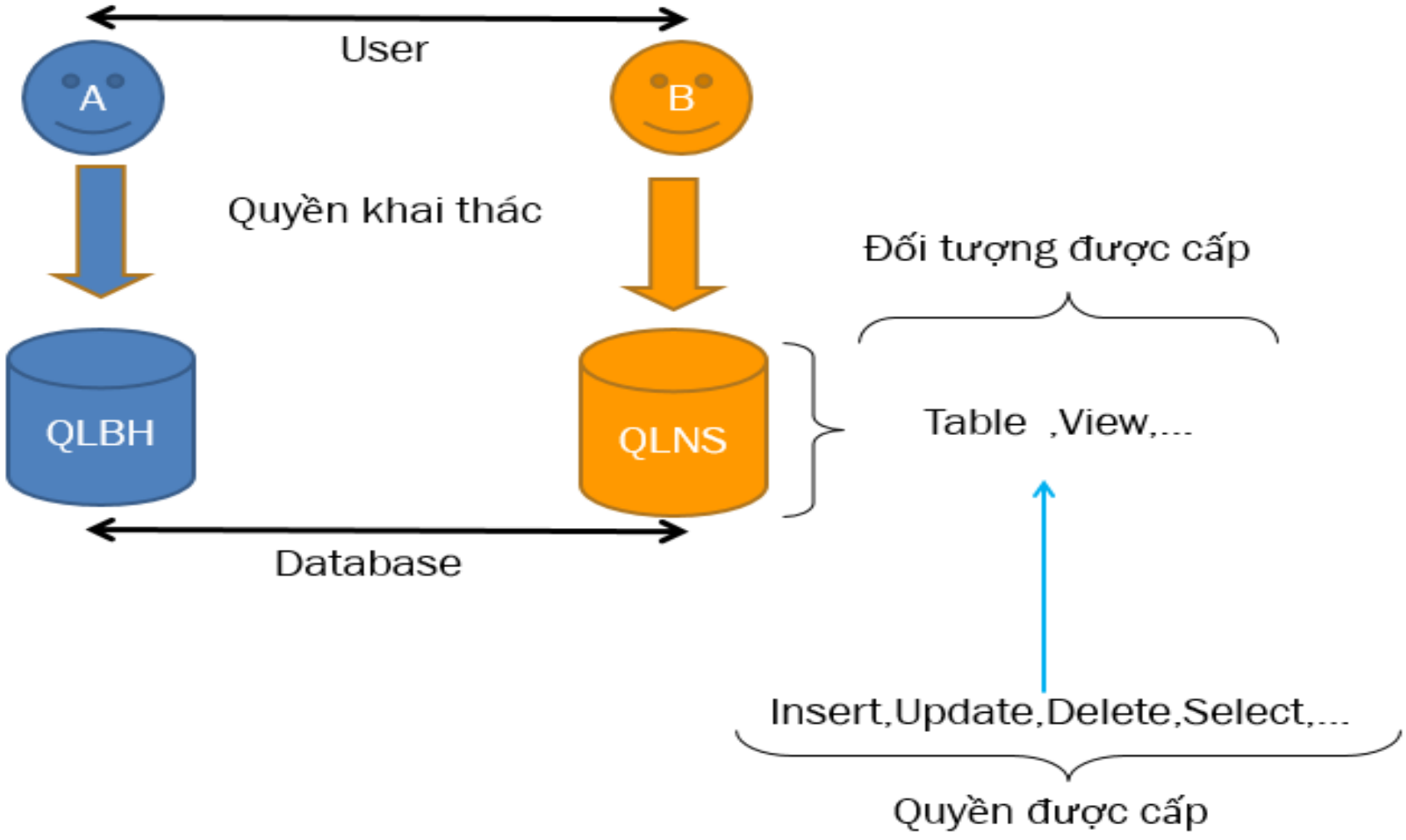
- Trao quyền tìm kiếm/đọc cho người dùng k59pap tới bảng KHOA

  GRANT select ON khoa TO k59pap;

- Trao quyền chèn, xóa cho cho người dùng k59pap tới bảng KHOA

  GRANT insert, delete ON khoa TO k59pap;

Ví dụ phân quyền cho user



Thu hồi quyền của user

- REVOKE <D/s thao tác> ON <Đối tượng> FROM <D/s người dùng> [RESTRICT/CASCADE]
  - <D/s thao tác>, <Đối tượng>, <D/s người dùng> giống như đối với câu lệnh GRANT.
  - Phần [RESTRICT/CASCADE] là chỉ ra cơ chế thu hồi với các quyền đã được người dùng trong <D/s người dùng> lan truyền

Thu hồi quyền của user (tiếp)

- Nếu Restrict thì có nghĩa là chỉ hủy bỏ quyền của những người có trong danh sách, quyền đã được lan truyền cho người khác không bị thu hồi.
- Nếu dùng Cascade thì hủy bỏ quyền của người trong <D/s người dùng>, đồng thời kéo theo hủy bỏ quyền mà người dùng đó đã luân chuyển cho những người khác.

- Ví dụ:

  REVOKE delete ON khoa FROM k59pap CASCADE

Xóa user, login

- DROP LOGIN …
- DROP USER …

Thực hành

https://giasutinhoc.vn/database/quan-tri-csdl-voi-sql-server/bao-mat-co-so-du-lieu-sql-server-bai-3/

Thực hành

B1. Tạo 1 login

B2. Tạo 1 database

B3. Trong database thì tao 3 tables

Bảng 1. Hoso(msv, hoten, quequan)

Bảng 2. Hocphan(mhp, tenhp, sotc)

Bảng 3. Ketqua(msv, mhp, diem)

B4. Nhập 5 dòng cho bảng 1; 2 dòng cho bảng 2. 4 dòng cho bảng 3

B5. Tạo 1 user tương ứng với login đã tạo ở Bước 1 với CSDL đã tạo ở Bước 2

Thực hành

B6. Chọn menu file /Connect Object Explorer

Để login với tài_khoản_login đã tạo ở B1

B7. Tại cửa sổ đăng nhập mới (của tài khoản logi mới) chọn CSDL đã tạo ở B2, nháy chuột phải chọn NEW QUERY. Sau đó viết lệnh SELECT * FROM hoso --- Thì có lỗi chưa có quyền

B8. Chọn cửa sổ đăng nhập của tài khoản TOÀN QUYỀN (sa/), thực hiện lệnh GRANT select ON hoso TO đã tạo ở bước 5 và thành công thì thực hiện lại lệnh ở B7

Thực hành

Bài tập vận dụng cao: Lập trình để User vừa tạo ở Bước 5 chỉ được XEM họ tên, điểm học phần của các sinh viên

Bài tập nâng cao: Đề xuất giải pháp. Tạo login, user và phân quyền cho một sinh viên chỉ được XEM họ tên, điểm học phần của chính mình

Lỗi không connect

https://www.youtube.com/watch?v=aU8RhjdkCoE