**TRƯỜNG ĐẠI HỌC KINH TẾ**

**ĐẠI HỌC ĐÀ NẴNG**

….🖎…🕮…✍….



**BÁO CÁO**

**ĐỀ TÀI: HỆ THỐNG QUẢN LÝ TIỆM PHOTOCOPY QUỐC TRUNG**

**HỌC PHẦN: QUẢN TRỊ CƠ SỞ DỮ LIỆU**

GVHD : Cao Thị Nhâm

Nhóm : 6

Sinh viên thực hiện : Nguyễn Thị Mùi

Nguyễn Thị Thu Hoài

Nguyễn Thị Tiên

Nguyễn Minh Phượng

Nguyễn Thị Duyên

Lê Âu Anh Thư

*Đà Nẵng, 2023*

**MỤC LỤC**

[I. Hóa đơn (R1) 3](#_Toc152341959)

[1. Phiếu đặt hàng 3](#_Toc152341960)

[2. Hóa đơn bán lẻ 1](#_Toc152341961)

[II. Thiết kế và xây dựng cơ sở dữ liệu (R2 + R3) 1](#_Toc152341962)

[1. Xây dựng ER cho đơn mua hàng 1](#_Toc152341963)

[2. Thiết kế cơ sở dữ liệu mức logic 6](#_Toc152341964)

[2.1. Chuyển thực thể, thu được: 6](#_Toc152341965)

[2.2. Chuyển quan hệ, thu được: 7](#_Toc152341966)

[2.3. Chuẩn hóa 7](#_Toc152341967)

[2.4. Vẽ sơ đồ quan hệ 7](#_Toc152341968)

[3. Mức vật lý 8](#_Toc152341969)

[III. Xác định và tạo các index cho các thuộc tính cần thiết (R4) 11](#_Toc152341970)

[IV. Xây dựng cơ chế bảo mật cho cơ sở dữ liệu vừa tạo (R5) 15](#_Toc152341971)

[1. Phương pháp : Xác thực người dùng 15](#_Toc152341972)

[V. Xây dựng cơ chế backup dữ liệu phù hợp cho cơ sở dữ liệu vừa tạo(R6) 20](#_Toc152341973)

[1. Backup 20](#_Toc152341974)

[2. Phục hồi 23](#_Toc152341976)

[VI. Phát triển phần mềm (R7) 27](#_Toc152341977)

[VII. Lưu trữ dữ liệu (R8) 27](#_Toc152341978)

[VIII. Phương án đề phòng hệ thống TESDB bị tấn SQL Injection (R9) 31](#_Toc152341979)

**DANH MỤC HÌNH ẢNH**

[Hình 1.ER-1 4](#_Toc152341904)

[Hình 2.ER-2 5](#_Toc152341905)

[Hình 3.Tích hợp ER-1 và ER-2 6](#_Toc152341906)

[Hình 4.Nhà cung cấp 8](#_Toc152341907)

[Hình 5. Cung cấp 8](#_Toc152341908)

[Hình 6.Cung cấp chi tiết 8](#_Toc152341909)

[Hình 7.Thiết bị 9](#_Toc152341910)

[Hình 8.Khách hàng 9](#_Toc152341911)

[Hình 9.Mua 9](#_Toc152341912)

[Hình 10.Mua chi tiết 10](#_Toc152341913)

[Hình 11. Sản phẩm 10](#_Toc152341914)

[Hình 12.Đặt 10](#_Toc152341915)

[Hình 13.Đặt chi tiết 11](#_Toc152341916)

[Hình 14.Tài liệu 11](#_Toc152341917)

[Hình 15.Tạo index cho bảng SANPHAM 11](#_Toc152341918)

[Hình 16.Ví dụ về truy vấn 12](#_Toc152341919)

[Hình 17.Kết quả index 12](#_Toc152341920)

[Hình 18.Hiệu suất CPU của câu truy vấn khi không dùng index 13](#_Toc152341921)

[Hình 19.Hiệu suất CPU của câu truy vấn khi dùng index 14](#_Toc152341922)

[Hình 20.Chọn login 15](#_Toc152341923)

[Hình 21.Thiết lập thông tin cơ bản về login 16](#_Toc152341924)

[Hình 22.Thiết lập quyền trên server(server roles) 17](#_Toc152341925)

[Hình 23.Thiết lập quyền trên cơ sở dữ liệu 18](#_Toc152341926)

[Hình 24. Thiết lập trạng thái 19](#_Toc152341927)

[Hình 25. Đăng nhập vào hệ thống và sử dụng với vai trò là nhân viên 20](#_Toc152341928)

[Hình 26. Lựa chọn thao tác backup 21](#_Toc152341929)

[Hình 27.Thiết lập các tùy chọn backup 22](#_Toc152341930)

[Hình 28.Lựa chọn nơi sao lưu backup 23](#_Toc152341931)

[Hình 29.Lựa chọn loại phục hồi 24](#_Toc152341932)

[Hình 30.Thiết lập tùy chọn phục hồi 25](#_Toc152341933)

[Hình 31.Lựa chọn các bản backup 26](#_Toc152341934)

[Hình 32.Phục hồi thành công 27](#_Toc152341935)

[Hình 33.Đăng kí 28](#_Toc152341936)

[Hình 34.Tạo product 28](#_Toc152341937)

[Hình 35.Tạo database 29](#_Toc152341938)

[Hình 36.Tạo tài khoản 29](#_Toc152341939)

[Hình 37.Server Name 30](#_Toc152341940)

[Hình 38.Đăng nhập SQL 30](#_Toc152341941)

[Hình 39.Đăng nhập thành công 31](#_Toc152341942)

[Hình 40.Kiểm tra 31](#_Toc152341943)

[Hình 41.Dạng tham số hóa 33](#_Toc152341944)

[Hình 42.Dạng tham số hóa 33](#_Toc152341945)

[Hình 43.Phương thức đăng nhập bằng parameter 34](#_Toc152341946)

[Hình 44.Tài khoản đăng nhập 34](#_Toc152341947)

[Hình 45.Tấn công SQL Injection nhưng không hợp lệ 35](#_Toc152341948)

[Hình 46.Đăng nhập thành công vào hệ thống 35](#_Toc152341949)

**DANH MỤC BẢNG**

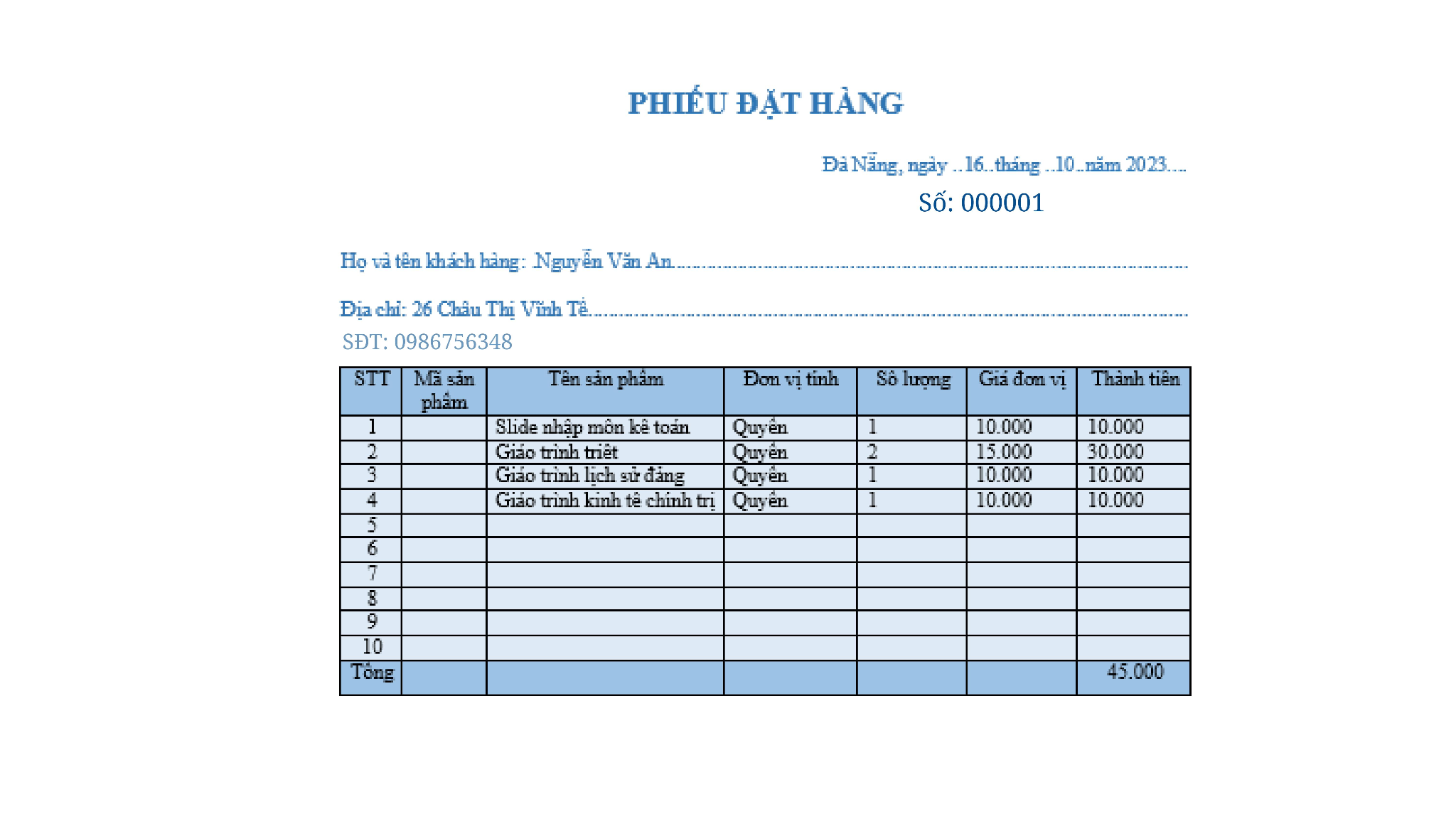
[Bảng 1.Đơn nhập hàng 2](#_Toc152274576)

[Bảng 2.Đơn mua sản phẩm 3](#_Toc152274577)

[Bảng 3.In tài liệu 3](#_Toc152274578)

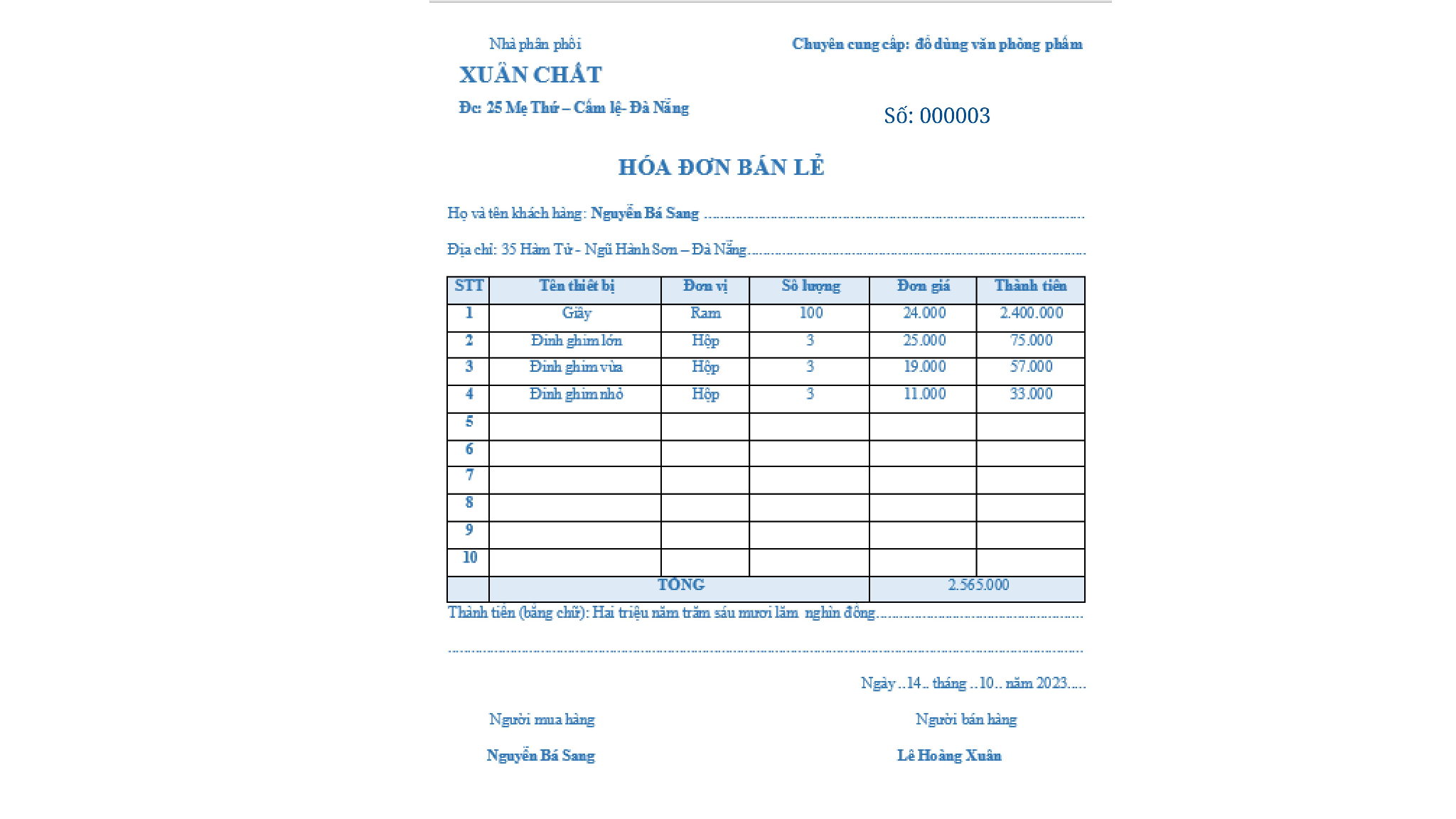
# Hóa đơn (R1)

## Phiếu đặt hàng



## Hóa đơn bán lẻ





# Thiết kế và xây dựng cơ sở dữ liệu (R2 + R3)

## Xây dựng ER cho đơn mua hàng

Bước 1: Chọn lọc thông tin

Bảng 1: Đơn nhập hàng

|  |  |  |
| --- | --- | --- |
| Từ trong HSDL | Từ rõ nghĩa | Từ viết tắt |
| Số | Mã đơn mua hàng | MaDonCC |
| Nhà cung cấp | Tên nhà cung cấp | TenNCC |
| Địa chỉ | Địa chỉ | DiaChi |
| Thiết bị | Tên thiết bị | TenTB |
| Đơn vị | Đơn vị tính | DVT |
| Số lượng | Số lượng | SoLuong |
| Đơn giá | Đơn giá | Dongia |
| Thành tiền | Thành tiền | ThanhTien |
| Tổng | Tổng tiền | TongTien |
| Ngày mua hàng | Ngày mua | NgayMua |
| Số điện thoại | Số điện thoại | SDT |

Bảng 2.Đơn mua sản phẩm

|  |  |  |
| --- | --- | --- |
| Từ trong HSDL | Từ rõ nghĩa | Từ viết tắt |
| Số | Mã đơn mua hàng | MaDonMua |
| Khách hàng | Tên khách hàng | TenKH |
| Địa chỉ | Địa chỉ | DiaChi |
| Mã sản phẩm | Mã sản phẩm | MaSP |
| Tên sản phẩm | Tên sản phẩm | TenSP |
| Đơn vị | Đơn vị tính | DVT |
| Số lượng | Số lượng | SoLuong |
| Đơn giá | Đơn giá | DonGia |
| Thành tiền | Thành tiền | ThanhTien |
| Tổng | Tổng tiền | TongTien |
| Ngày mua hàng | Ngày mua hàng | NgayMua |
| Số điện thoại | Số điện thoại | SDT |

Bảng 3.In tài liệu

|  |  |  |
| --- | --- | --- |
| Từ trong HSDL | Từ rõ nghĩa | Từ viết tắt |
| Mã đơn | Mã đơn tài liệu | MaDonTL |
| Số điện thoại | Số điện thoại | SDT |
| Khách hàng | Tên khách hàng | TenKH |
| Địa chỉ | Địa chỉ | DiaChi |
| Tên tài liệu | Tên tài liệu | TenTL |
| Đơn giá | Đơn giá | DonGia |
| Ngày đặt | Ngày đặt | NgayDat |
| Ngày lấy | Ngày lấy | NgayLay |
| Thành tiền | Thành tiền | ThanhTien |
| Tổng tiền | Tổng tiền | TongTien |
| Số lượng | Số lượng | SoLuong |
| Mã đơn | Mã đơn tài liệu | MaDonTL |

Bước 2: Xác định thực thể, thuộc tính

Bảng 1:

Cung cấp (TenNCC, DiaChi, SDT)

Thiết bị (TenTB, DVT, DonGia)

Bảng 2:

Khách hàng (TenKH, DiaChi, SĐT)

Sản phẩm(TenSP, MaSP, DonGia, DVT)

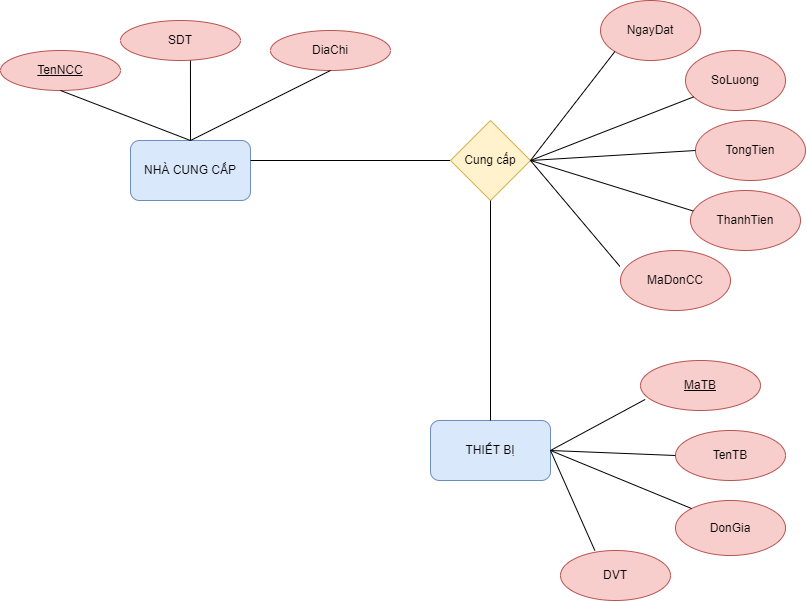
Bảng 3:

Tài liệu (TenTL, DonGia)

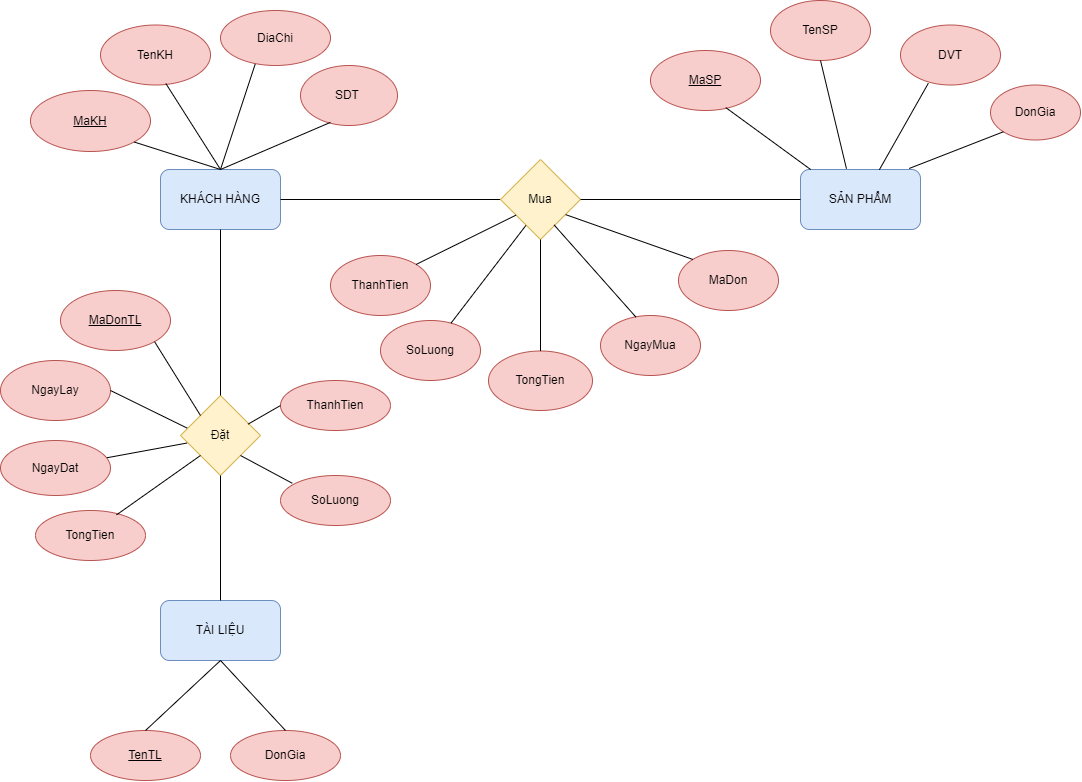
Bước 3: Xác định quan hệ

Đặt: Bao gồm các thuộc tính còn lại trong từ điển

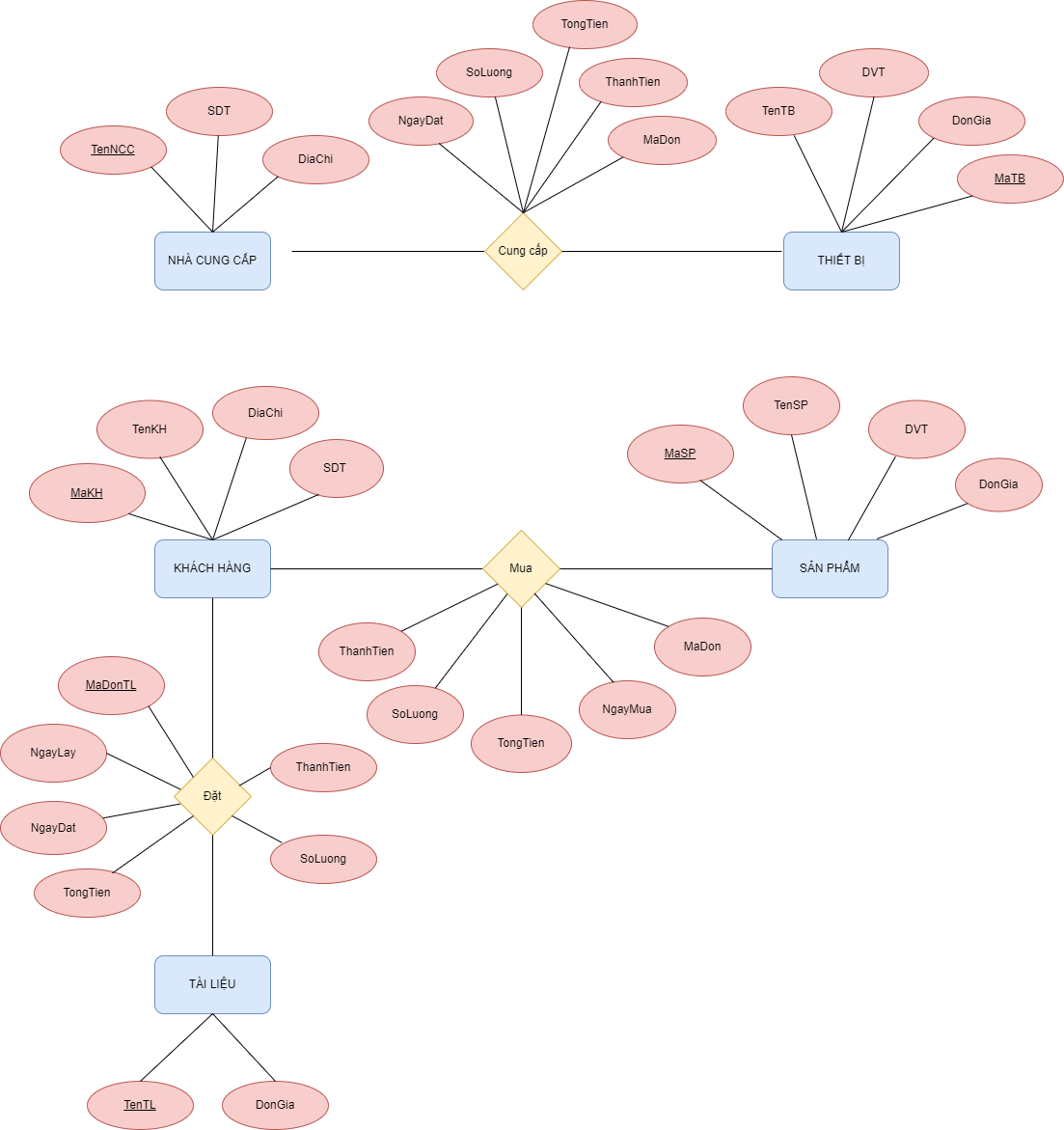
Bước 4: Vẽ



Hình 1.ER-1



Hình 2.ER-2

****

Hình 3.Tích hợp ER-1 và ER-2

## Thiết kế cơ sở dữ liệu mức logic

### Chuyển thực thể, thu được:

Thiết bị (MaTB, TenTB, DVT, DonGia)

Sản phẩm (MaSP, TenSP, DonGia, DVT)

Nhà cung cấp (TenNCC, SDT, DiaChi)

Khách hàng (MaKH, TenKH, SDT, DiaChi)

Tài liệu (TenTL, DonGia)

### Chuyển quan hệ, thu được:

Cung cấp (MaDonCC, SoLuong, TongTien, ThanhTien, NgayDat, TenNCC, MaTB)

Mua (MaDonMua, NgayMua, TongTien, SoLuong, ThanhTien, MaSP, MaKH)

Đặt (MaDonTL, NgayDat, NgayLay, SoLuong, ThanhTien, TongTien, MaKH, TenTL)

### Chuẩn hóa

**Chuẩn hóa quan hệ cung cấp**

Cung cấp(MaDonCC, TenNCC, TongTien, NgayDat)

Cung cấp\_Chi tiết(MaDonCC, MaTB, Soluong, ThanhTien)

**Chuẩn hóa quan hệ mua**

Mua (MaDonMua, MaKH, NgayMua, TongTien)

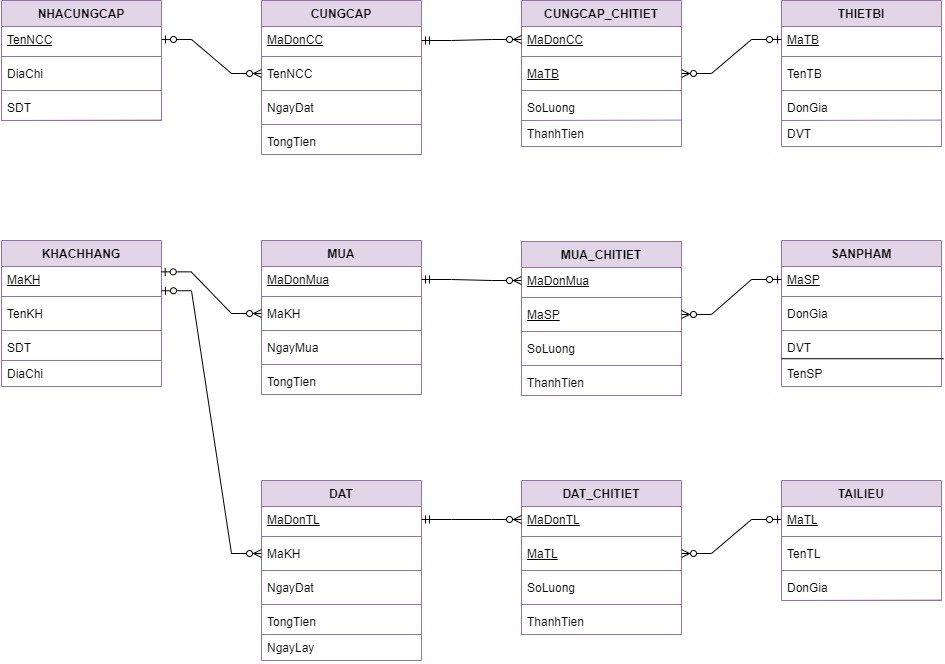
Mua\_Chi tiết(MaDonMua, MaSP, Soluong, ThanhTien)

**Chuẩn hóa quan hệ đặt hàng**

Đặt(MaDonTL, MaKH, NgayDat, NgayLay,TongTien )

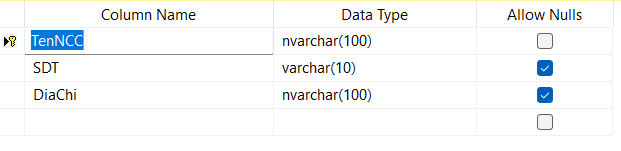
Đặt\_Chi tiêt( MaDonTL, TenTL, SoLuong,ThanhTien)

### Vẽ sơ đồ quan hệ

****

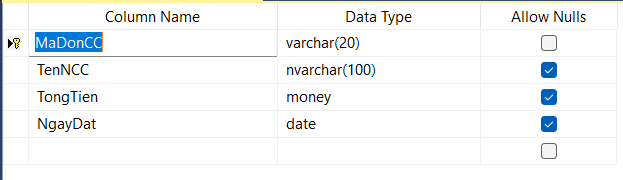
## Mức vật lý

* Nhà cung cấp

****

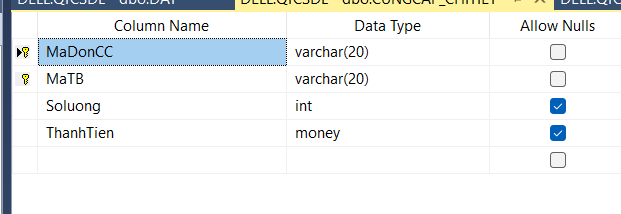
Hình 4.Nhà cung cấp

* Cung cấp

****

Hình 5. Cung cấp

* Cung cấp chi tiết

****

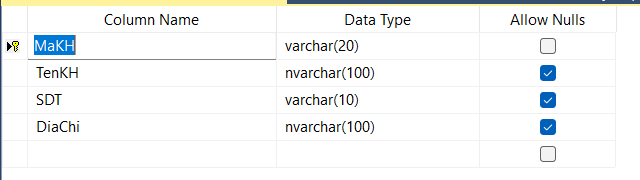
Hình 6.Cung cấp chi tiết

* Thiết bị

****

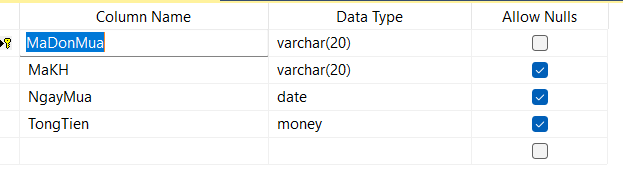
Hình 7.Thiết bị

* Khách hàng

****

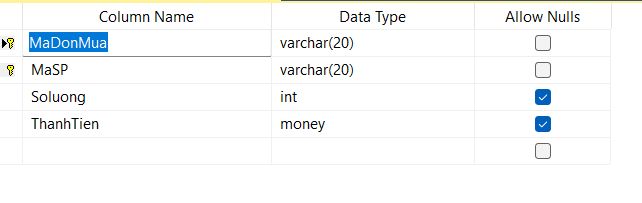
Hình 8.Khách hàng

* Mua

****

Hình 9.Mua

* Mua chi tiết

****

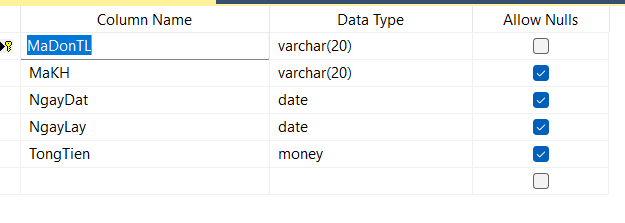
Hình 10.Mua chi tiết

* Sản phẩm

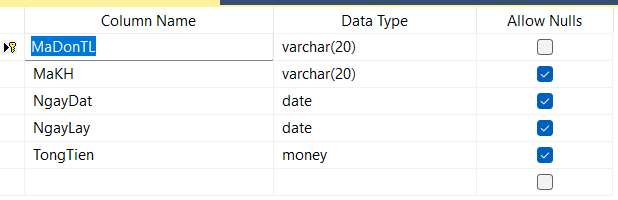
****

Hình 11. Sản phẩm

* Đặt

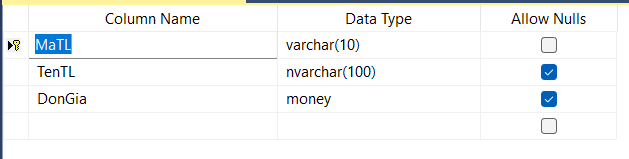
****Hình 12.Đặt

* Đặt chi tiết

****

Hình 13.Đặt chi tiết

* Tài liệu

****

Hình 14.Tài liệu

# Xác định và tạo các index cho các thuộc tính cần thiết (R4)

Tạo index cho bảng SANPHAM



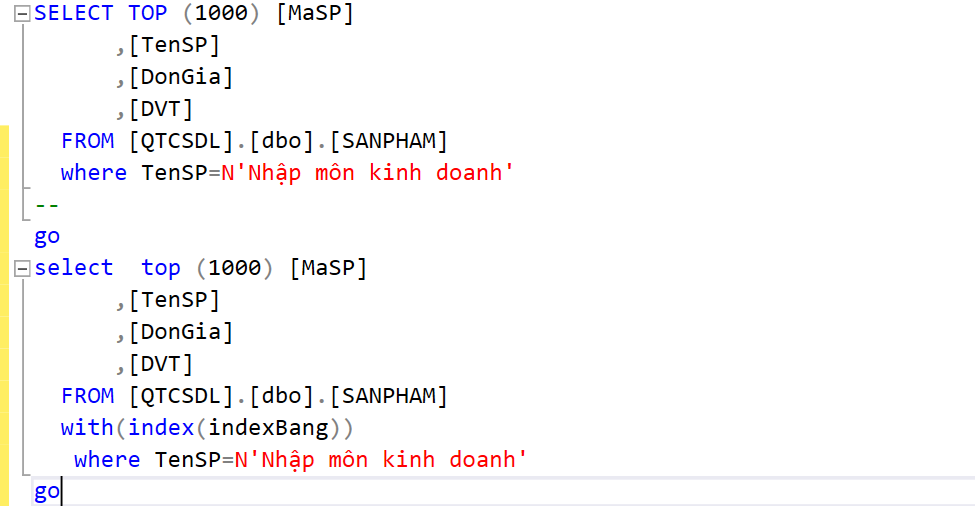
Hình 15.Tạo index cho bảng SANPHAM

Lý do lựa chọn bảng SẢN PHẨM:

* Bảng SANPHAM ít tần suất UPDATE,INSERT.
* Số lượng bản ghi không quá lớn hay nhỏ
* Cột TenSP không thường xuyên sửa đổi

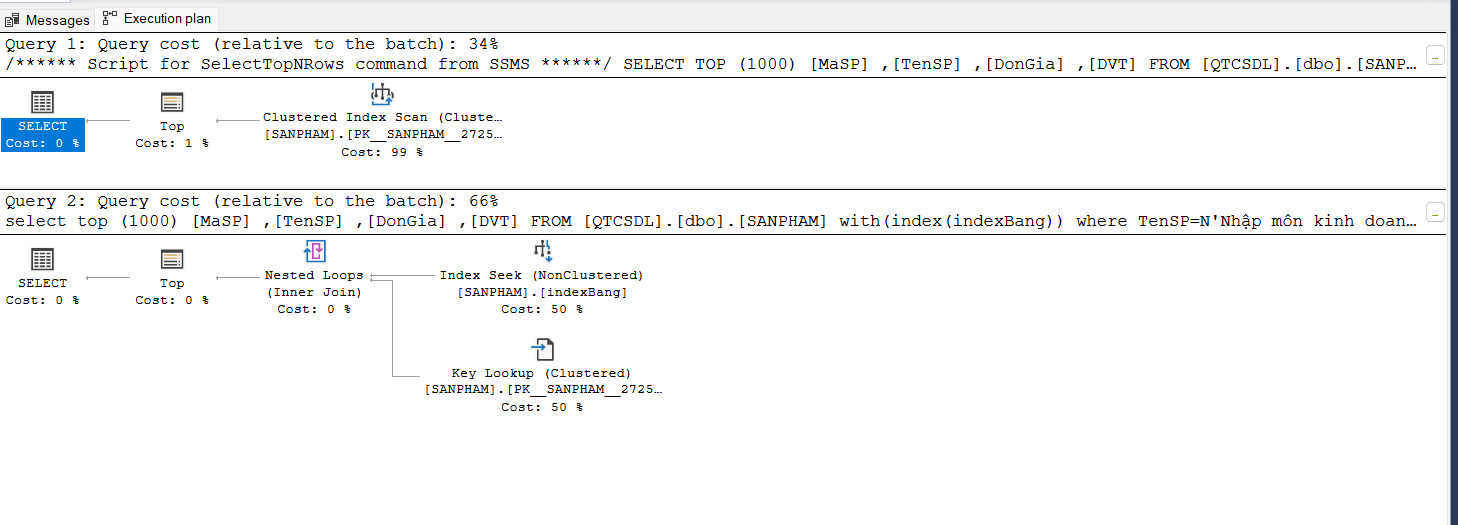
=> Giúp hệ thống truy xuất nhanh hơn

Ví dụ về truy vấn:

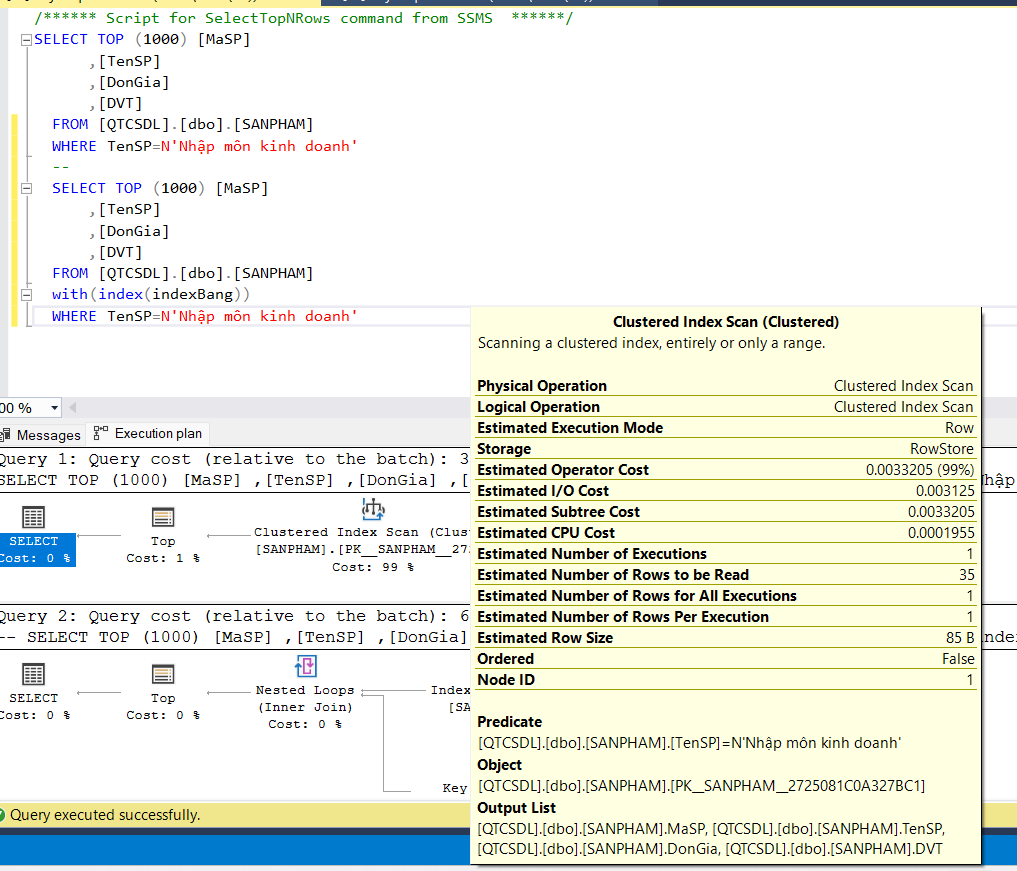


Hình 16.Ví dụ về truy vấn

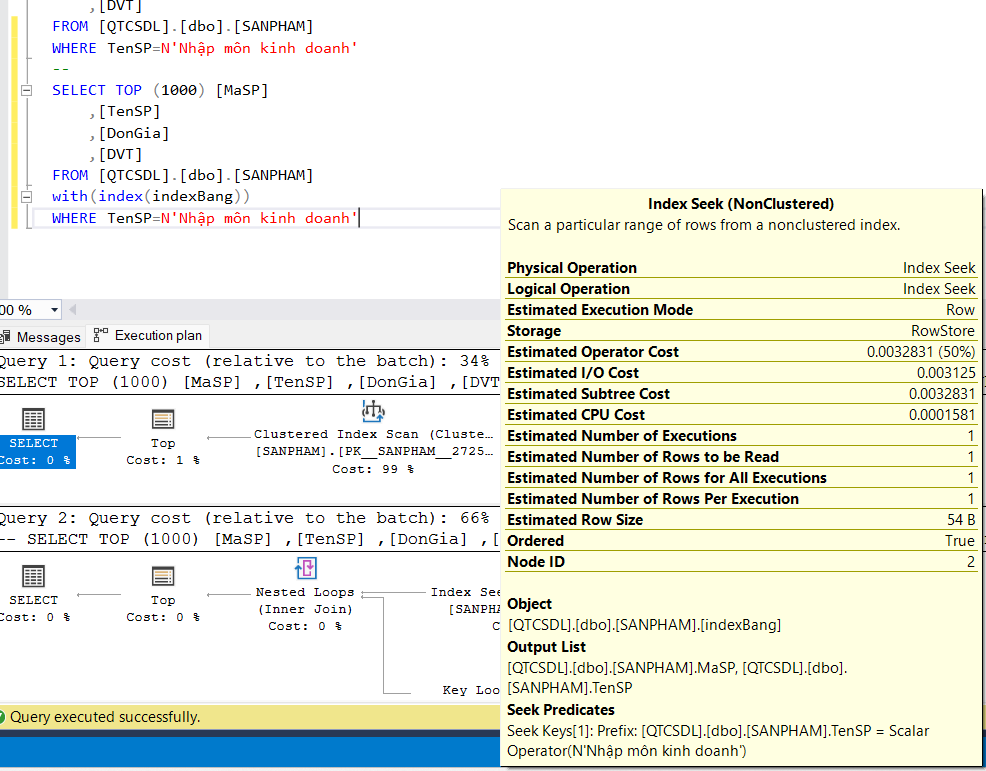
Kết quả sau khi INDEX:

****

Hình 17.Kết quả index



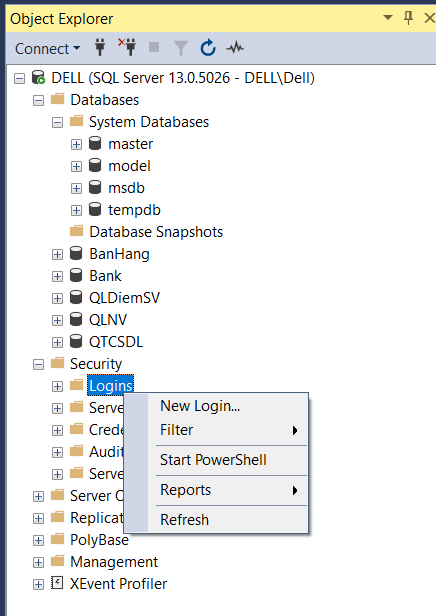
Hình 18.Hiệu suất CPU của câu truy vấn khi không dùng index



Hình 19.Hiệu suất CPU của câu truy vấn khi dùng index

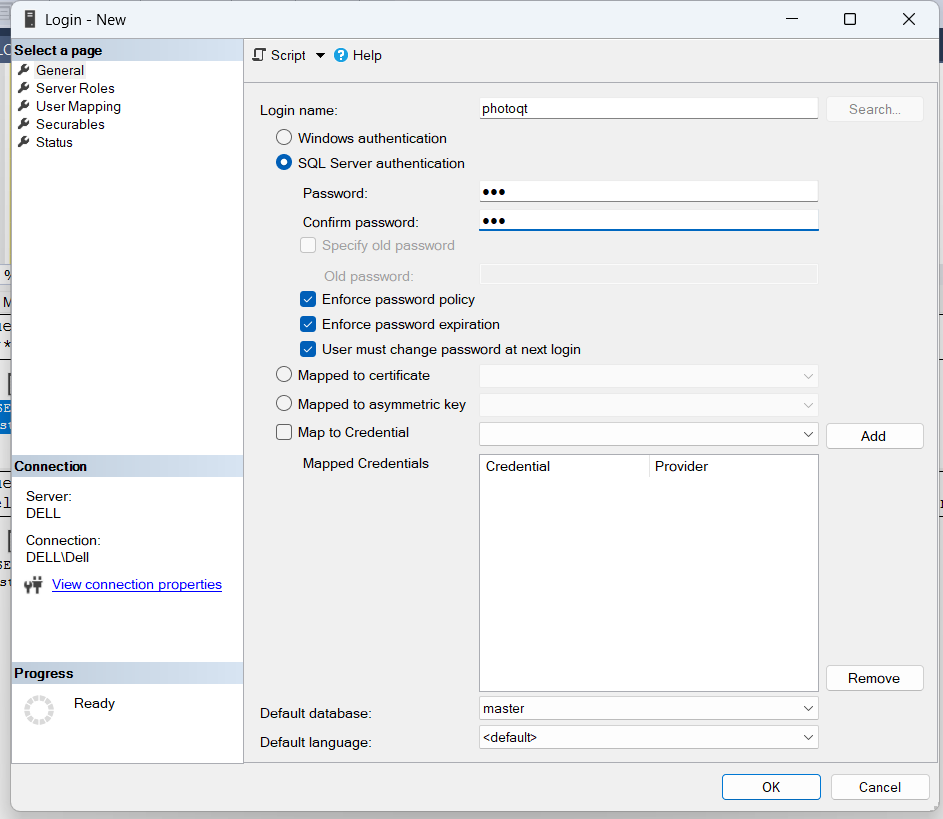
# Xây dựng cơ chế bảo mật cho cơ sở dữ liệu vừa tạo (R5)

## Phương pháp : Xác thực người dùng

****

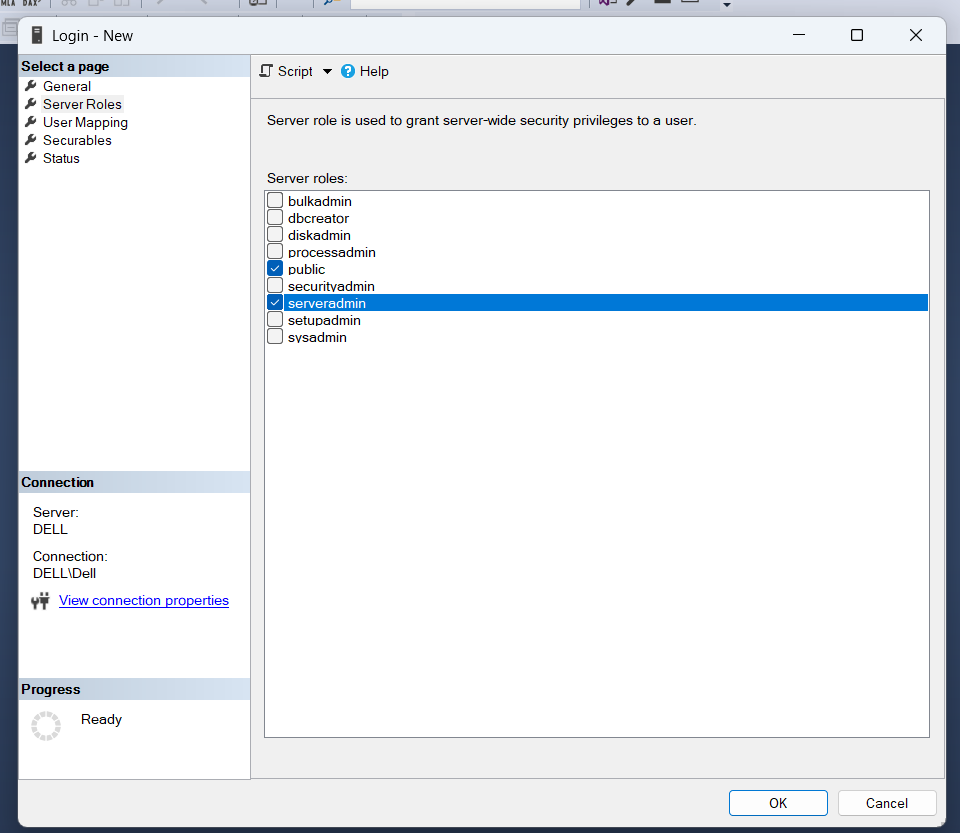
Hình 20.Chọn login

Bước 1: Thiết lập thông tin cơ bản về login bao gồm: tên đăng nhập (login name), phương thức xác thực (Windows, SQL server, Mapped to certificate, mapped to asymmetric key,...). Thường sẽ chọn SQL Server authentication.

****

Hình 21.Thiết lập thông tin cơ bản về login

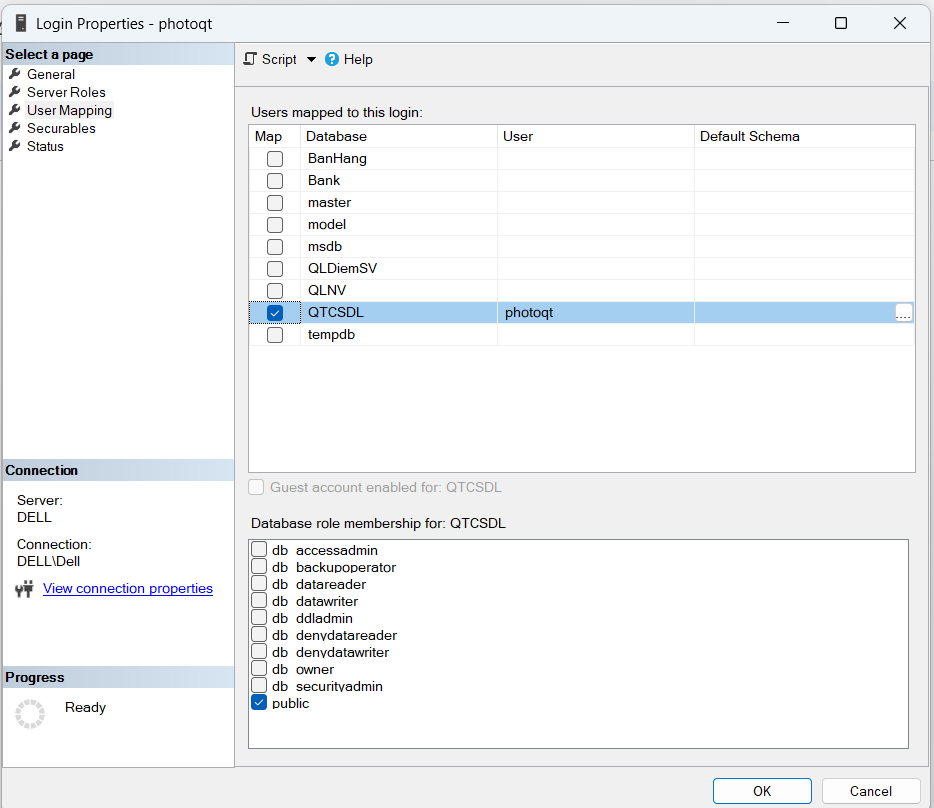
Bước 2: Thiết lập quyền trên server(server roles)

****

Hình 22.Thiết lập quyền trên server(server roles)

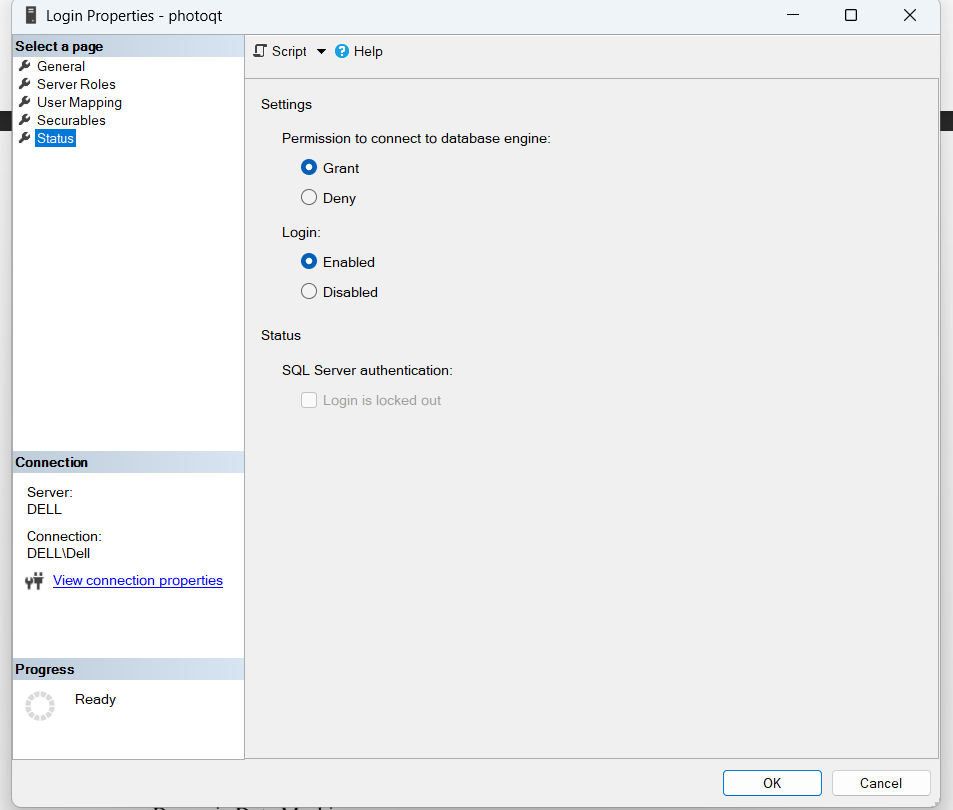
Bước 3: Thiết lập quyền trên cơ sở dữ liệu(user mapping)

Chọn tên QTCSDL để nhân viên của quán dùng sẽ làm việc và quyền của họ trên cơ sở dữ liệu.

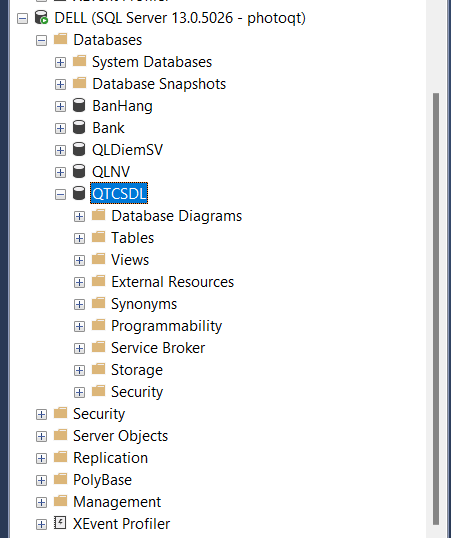
****

Hình 23.Thiết lập quyền trên cơ sở dữ liệu

Bước 4: Thiết lập trạng thái

****

Hình 24. Thiết lập trạng thái

****

Hình 25.: Đăng nhập vào hệ thống và sử dụng với vai trò là nhân viên

# Xây dựng cơ chế backup dữ liệu phù hợp cho cơ sở dữ liệu vừa tạo(R6)

## Backup

## Các thao tác thực hiện backup thực hiện trên SQL Server Management Studio như sau:

Bước 1: Lựa chọn thao tác backup

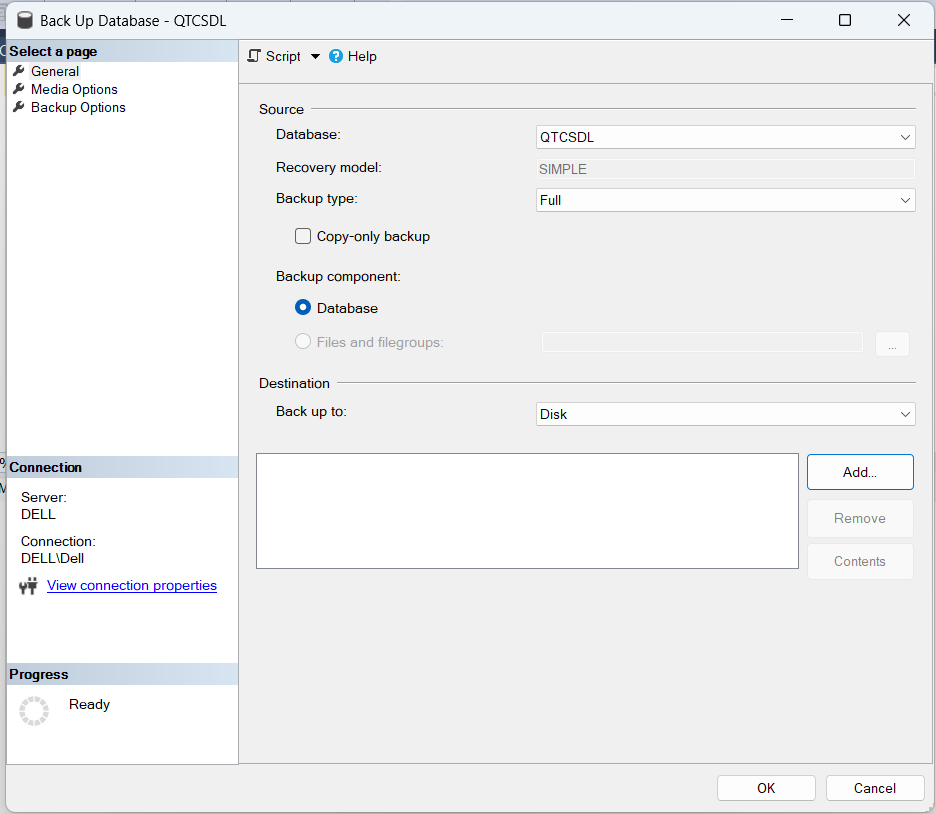
****

Hình 26. Lựa chọn thao tác backup

Bước 2:Thiết lập các tùy chọn backup

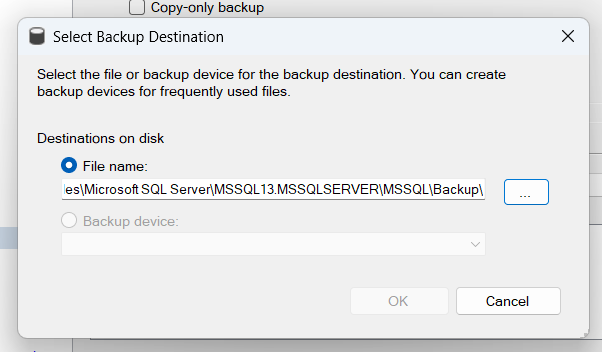
Database: Lựa chọn tên cơ sở dữ liệu backup

Backup type: có thể lựa chọn Full hoặc Differential( chỉ lựa chọn different khi đã thực hiện ít nhất một lần full trước đó).

****

Hình 27.Thiết lập các tùy chọn backup

Bước 3: Lựa chọn nơi sao lưu backup

****

Hình 28.Lựa chọn nơi sao lưu backup

Một số chú ý:

* Database: lựa chọn tên cơ sở dữ liệu backup
* Backup type: có thể lựa chọn Full hoặc Differential (chỉ lựa chọn differential khi đã thực hiện ít nhất một lần full trước đó).
* Backup To: có thể lựa chọn lưu bản backup vào ổ đĩa cứng hoặc lưu lên một máy tính khác trên internet.

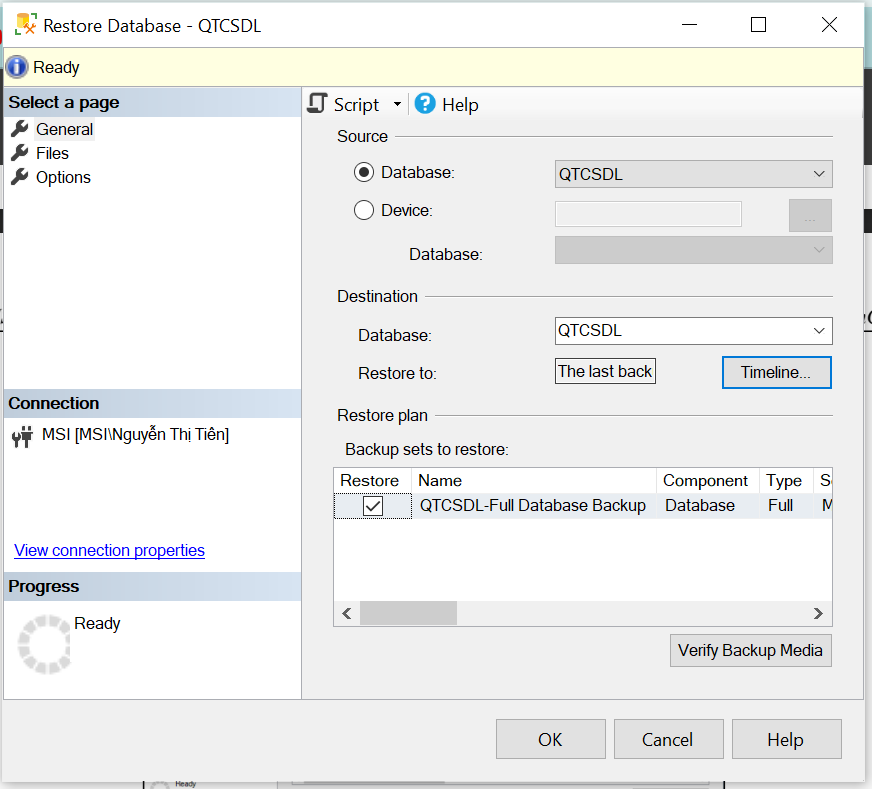
## Phục hồi

Bước 1:Lựa chọn loại phục hồi

****

Hình 29.Lựa chọn loại phục hồi

Bước 2: Thiết lập tùy chọn phục hồi

****

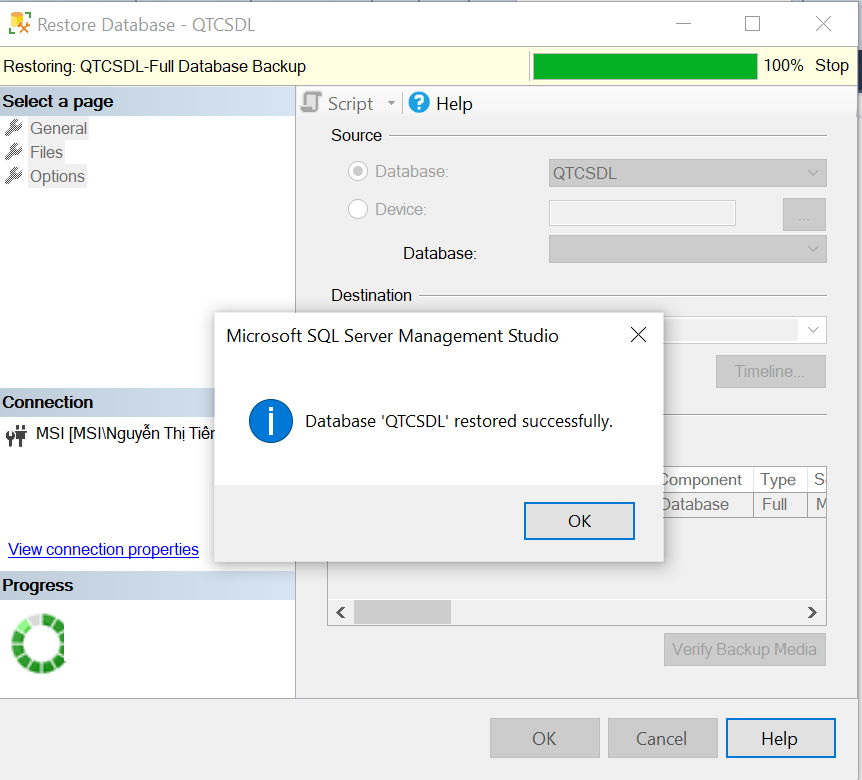
Hình 30.Thiết lập tùy chọn phục hồi

Trong cửa sổ này, người dùng sẽ nhìn thấy các bản backup và có thể lựa chọn phục hồi dữ liệu về một thời điểm nhất định trong khoảng thời gian kể từ khi thực hiện backup (như hình dưới).

****

Hình 31.Lựa chọn các bản backup

Sau khi người dùng bấm chọn phục hồi dữ liệu thì màn hình sẽ hiển thị “Database ‘QTCSDL’ restored successfully.”

****

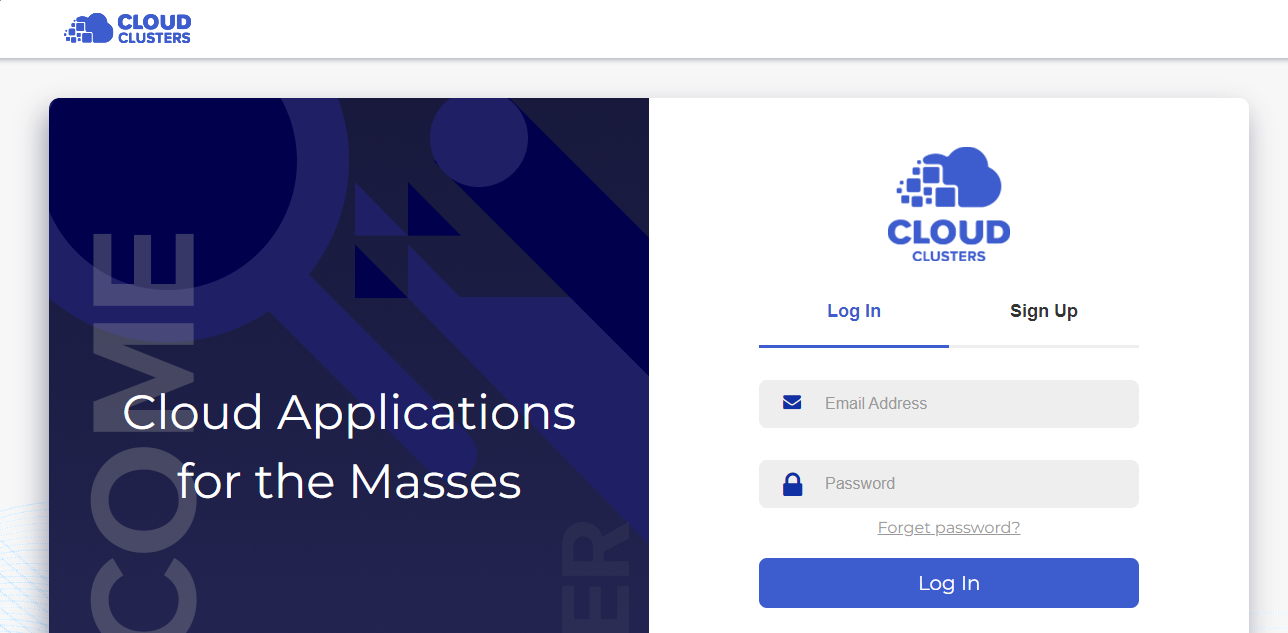
Hình 32.Phục hồi thành công

# Phát triển phần mềm (R7)

<https://bom.so/lnNuED>

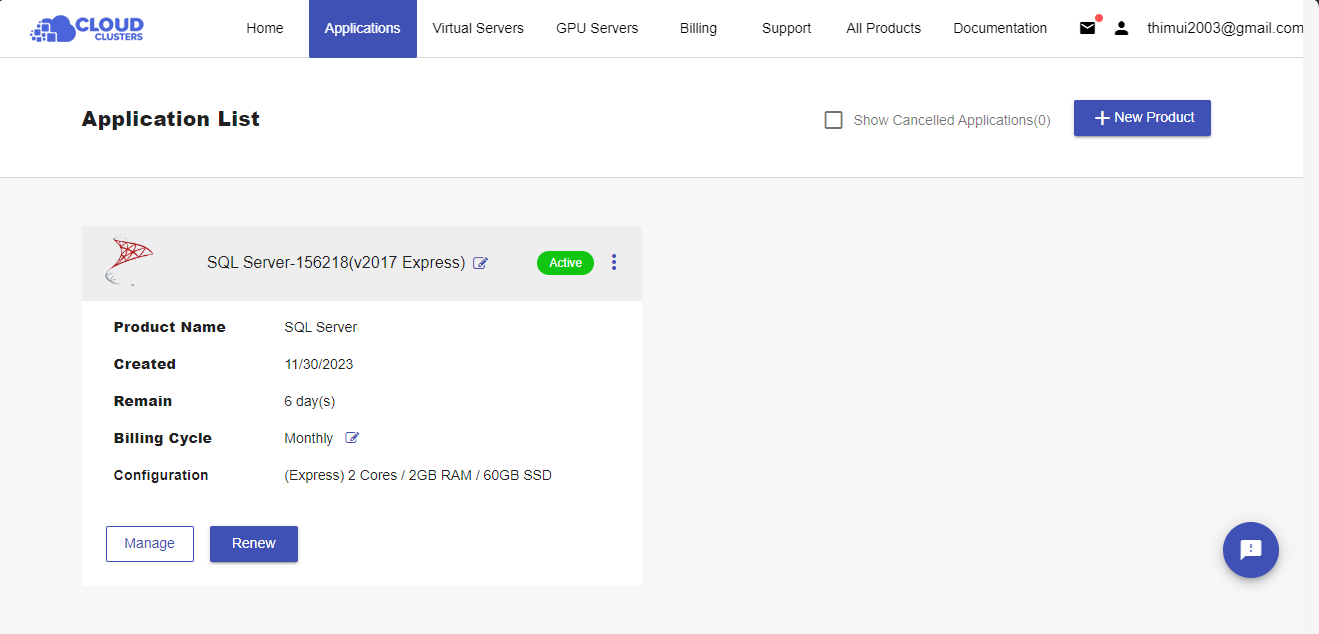
# Lưu trữ dữ liệu (R8)

Bước 1: Đăng ký tài khoản



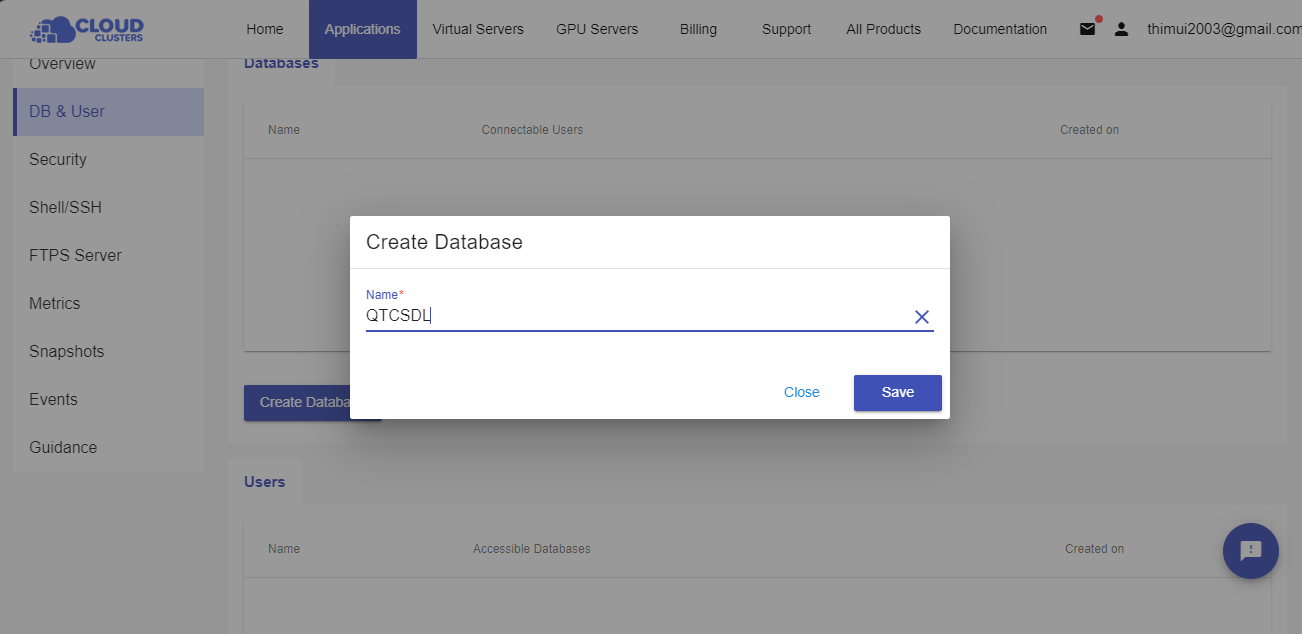
Hình 33.Đăng kí

Bước 2: Tạo product SQL Server và quản lý

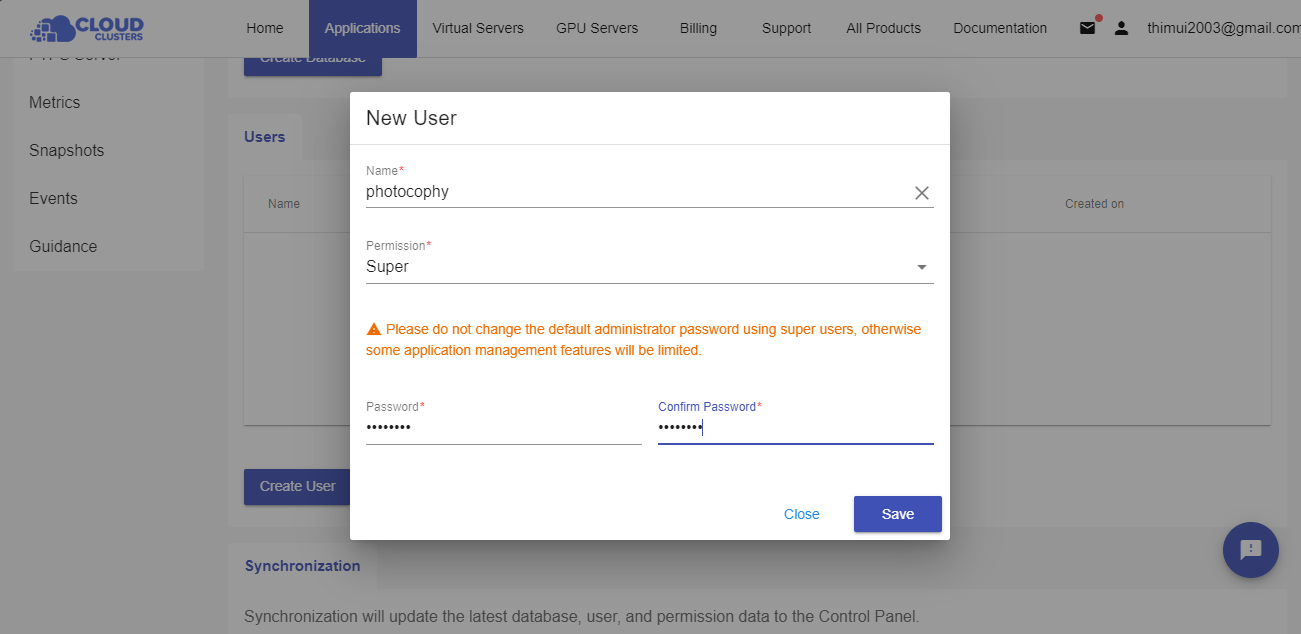


Hình 34.Tạo product

Bước 3: Tạo database và user

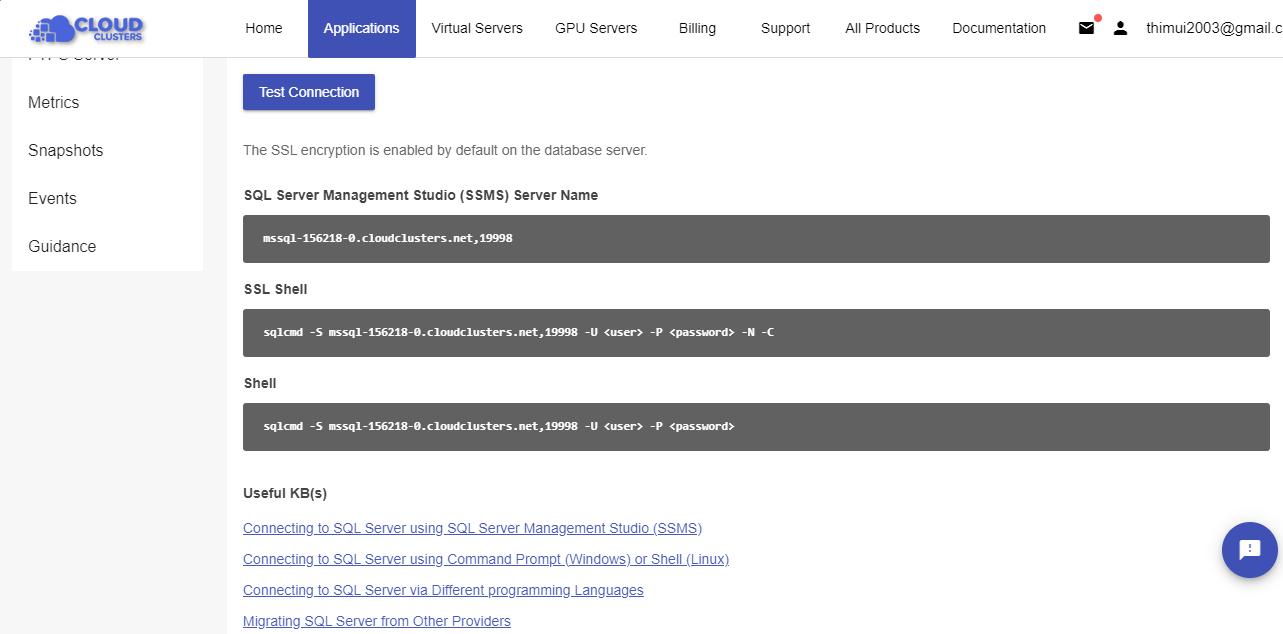


Hình 35.Tạo database



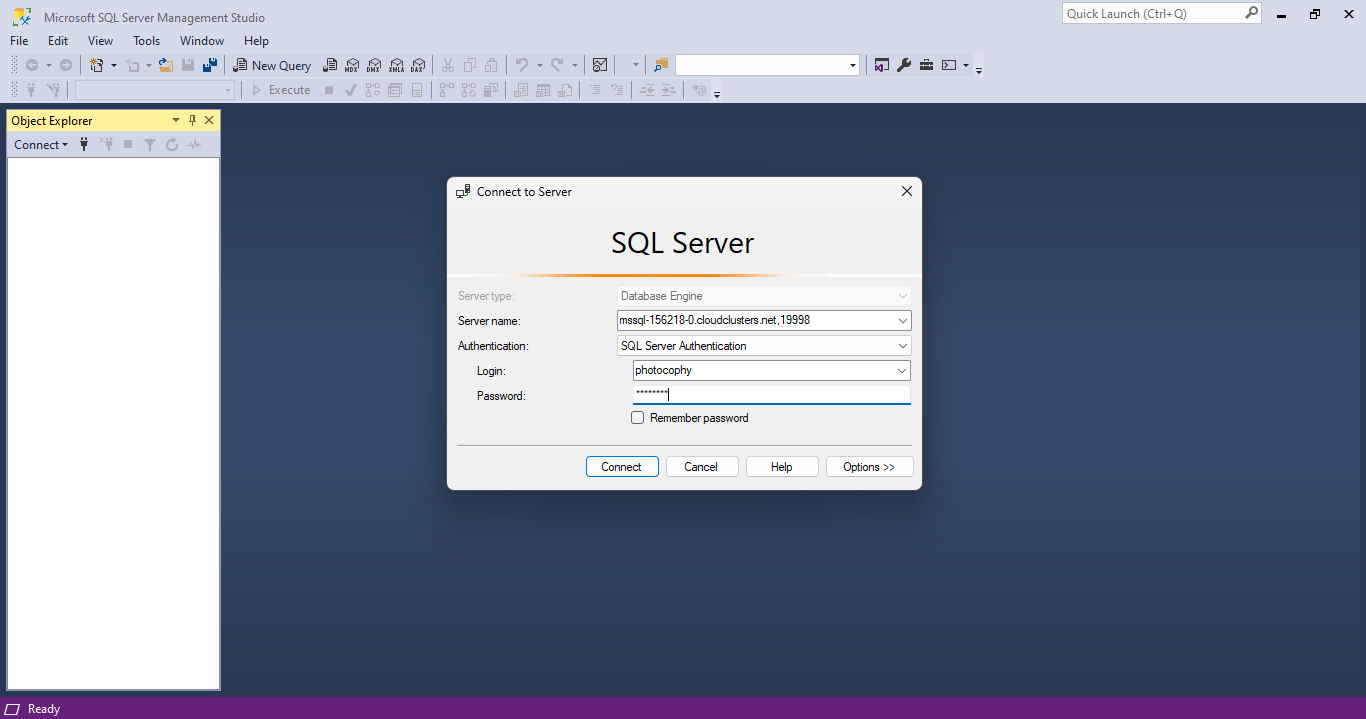
Hình 36.Tạo tài khoản

Bước 4: Copy Server Name

****

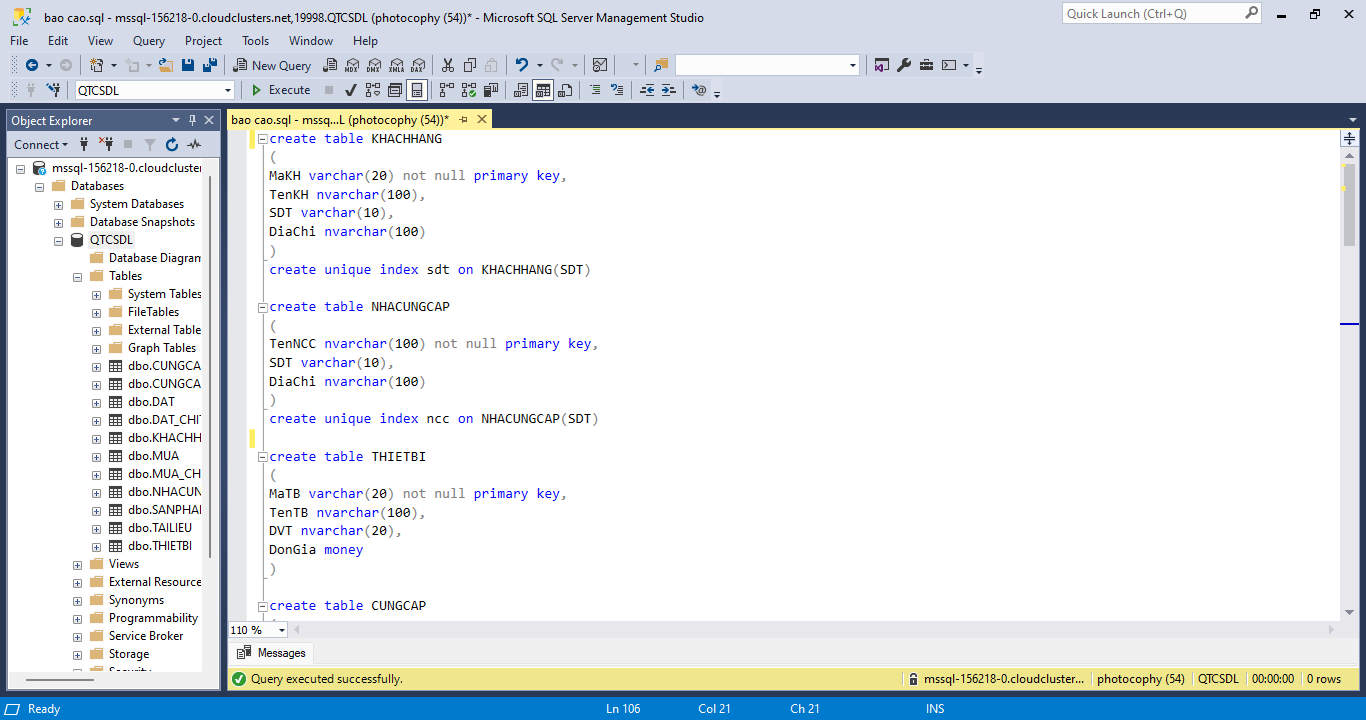
Hình 37.Server Name

Bước 5: Đăng nhập vào Sql Server Managerment Studio với Sever Name, Login và Password đã tạo ở trên.

****

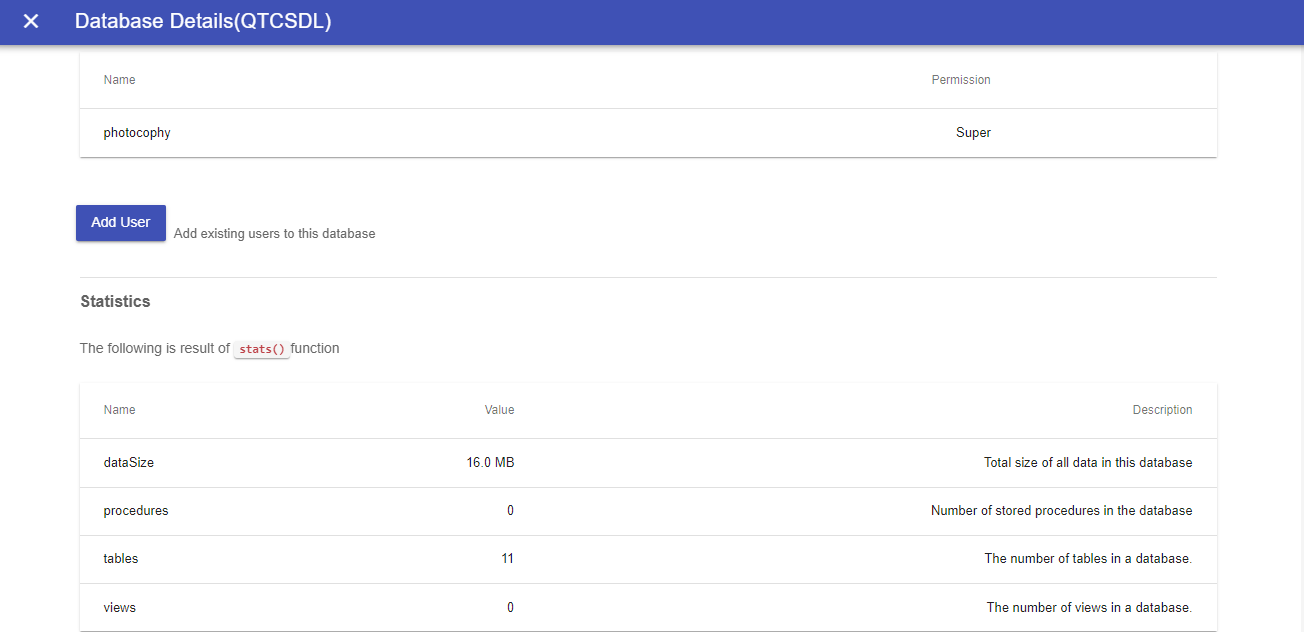
Hình 38.Đăng nhập SQL

Bước 6: Đăng nhập thành công

****

Hình 39.Đăng nhập thành công

Bước 7: Kiểm tra Cloud Clusters đã cập nhật database

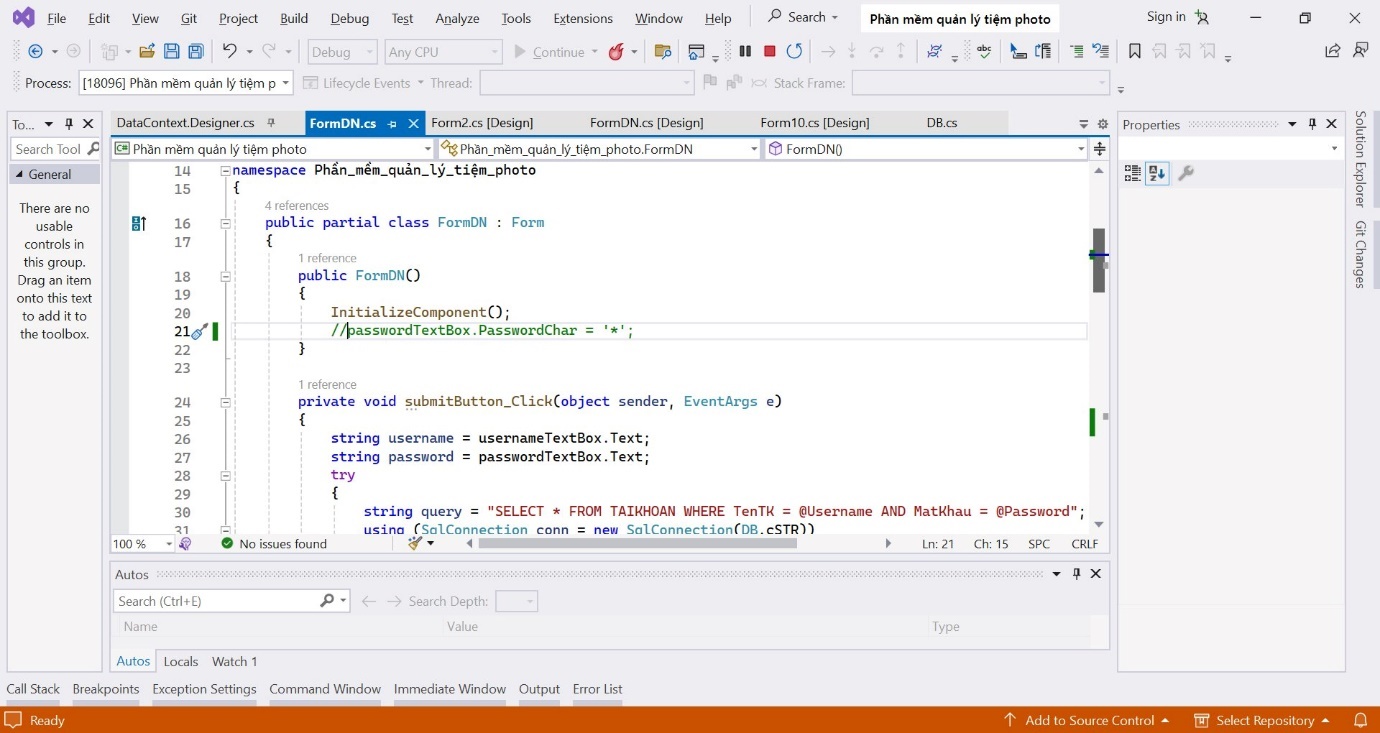
****

Hình 40.Kiểm tra

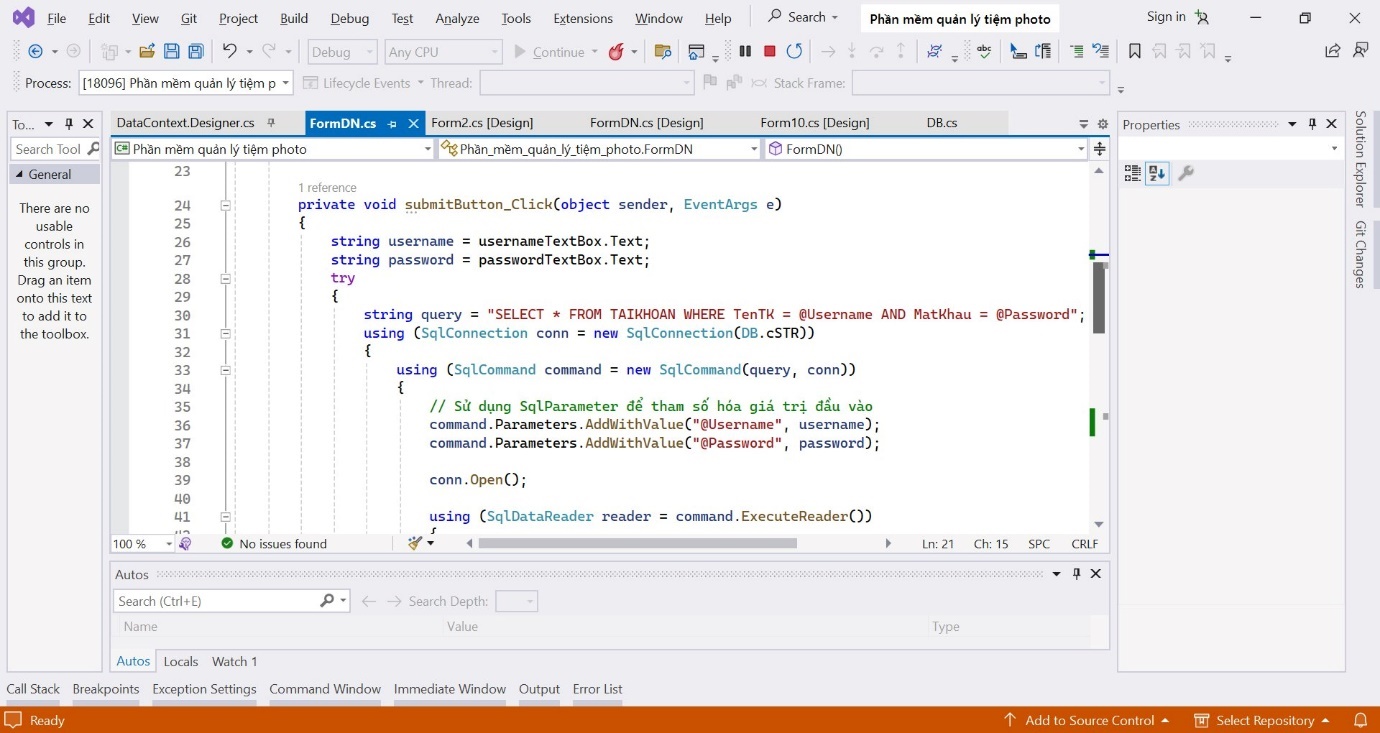
# Phương án đề phòng hệ thống TESDB bị tấn SQL Injection (R9)

* SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng kỹ thuật chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database.
* Phương pháp đối phó SQL Injection, nhóm em chọn sử dụng tham số hóa truy vấn:
* Giải thích lý do lựa chọn:
* Ngăn chặn việc chèn mã SQL độc hại: Khi sử dụng tham số hóa truy vấn, các giá trị được truyền vào câu truy vấn thông qua các tham số, không phải là ghép chuỗi trực tiếp vào câu truy vấn. Điều này ngăn chặn khả năng tấn công bằng cách chèn mã SQL độc hại vào câu truy vấn.
* Tách biệt cấu trúc truy vấn và dữ liệu: Tham số hóa truy vấn tách biệt cấu trúc truy vấn và dữ liệu, giúp tránh việc nhầm lẫn giữa dữ liệu và mã SQL. Khi sử dụng tham số, cấu trúc truy vấn không bị thay đổi, chỉ dữ liệu được thay đổi. Điều này giúp loại bỏ hoặc giảm thiểu khả năng xảy ra lỗi cú pháp SQL và tấn công SQL Injection.
* Ngăn chặn truy vấn động: SQL Injection thường được thực hiện bằng cách chèn các truy vấn SQL động vào câu truy vấn gốc. Sử dụng tham số hóa truy vấn, các truy vấn SQL được xác định trước và không thể thay đổi trong quá trình thực thi câu truy vấn. Điều này ngăn chặn khả năng tấn công bằng cách thực thi các truy vấn động không an toàn.
* Bảo vệ dữ liệu người dùng: Sử dụng tham số hóa truy vấn giúp bảo vệ dữ liệu người dùng khỏi việc lộ thông tin nhạy cảm hay mất điều khiển với cơ sở dữ liệu. Khi sử dụng tham số, dữ liệu người dùng được truyền an toàn và được xử lý một cách đúng đắn trong quá trình truy vấn.
* Hỗ trợ kiểm tra và xử lý đầu vào: Khi sử dụng tham số hóa truy vấn, các tham số có thể được kiểm tra và xử lý đầu vào một cách an toàn. Điều này giúp ngăn chặn việc chèn các giá trị độc hại hoặc không hợp lệ vào truy vấn.
* Phương án đề phòng bằng cách sử dụng tham số hóa truy vấn là một biện pháp hiệu quả để ngăn chặn tấn công SQL Injection. Thay vì tạo truy vấn SQL bằng cách ghép chuỗi các giá trị vào câu truy vấn, ta sẽ sử dụng các tham số để thực hiện truy vấn và truyền giá trị vào các tham số này.

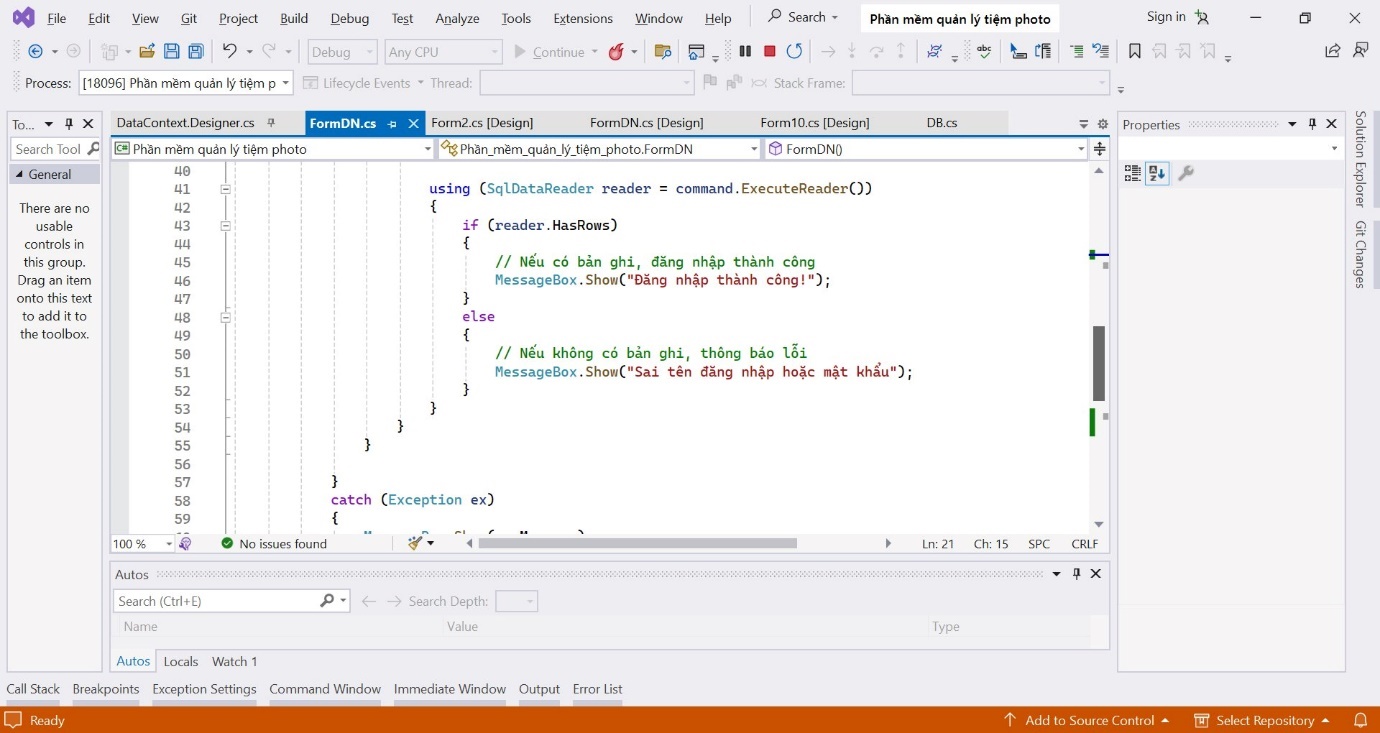
Tham số hóa nó sẽ có dạng:



Hình 41.Dạng tham số hóa



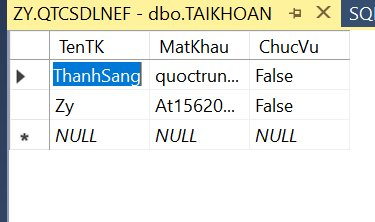
Hình 42.Dạng tham số hóa



Hình 43.Phương thức đăng nhập bằng parameter

Khi thực hiện truy vấn, chúng ta sẽ truyền giá trị cho các tham số @username và @password thay vì chèn trực tiếp vào câu truy vấn. Điều này giúp ngăn chặn việc thực thi các câu lệnh SQL độc hại được chèn vào truy vấn.

Các tài khoản đăng nhập:

****

Hình 44.Tài khoản đăng nhập

Bây giờ hệ thống chỉ chấp nhận những tài khoản có trong cơ sở dữ liệu như trên và sẽ khắc phục được lỗi SQL Injection.



Hình 45.Tấn công SQL Injection nhưng không hợp lệ



Hình 46.Đăng nhập thành công vào hệ thống

**PHỤ LỤC**

1. Script SQL – google doc: <https://bom.so/lnNuED>
2. Phát triển phần mềm: <https://bom.so/iEvphP>