1. **Nội dung R5:**
2. **Quản lý người dùng:**

Người sử dụng admin, công việc: quản trị hệ thống cơ sở dữ liệu.

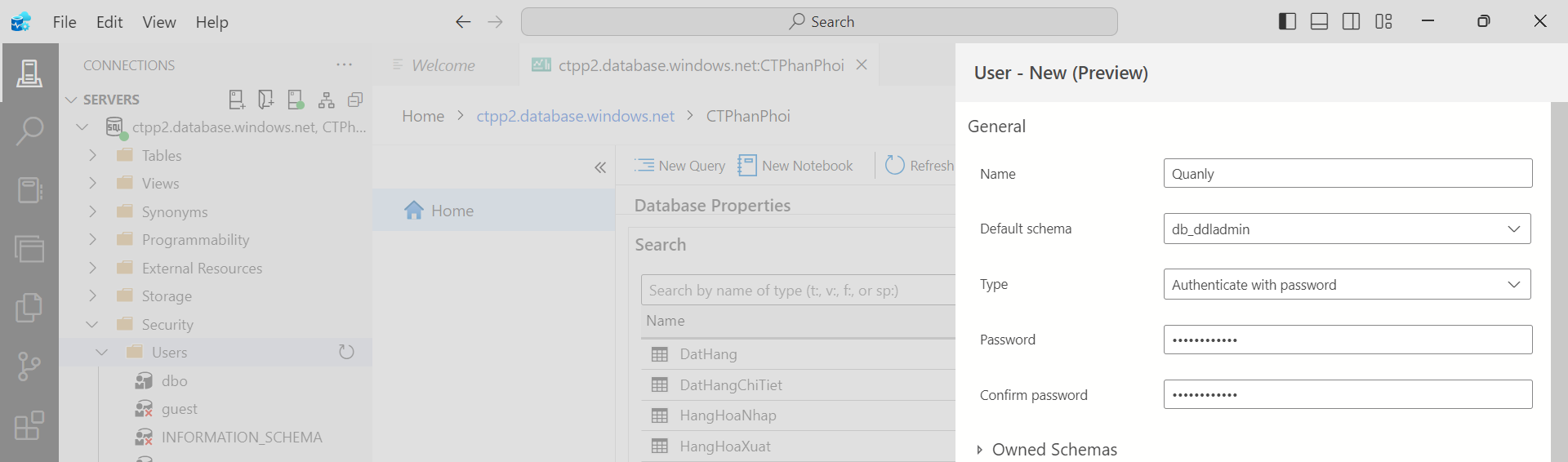
Bảng phân quyền:

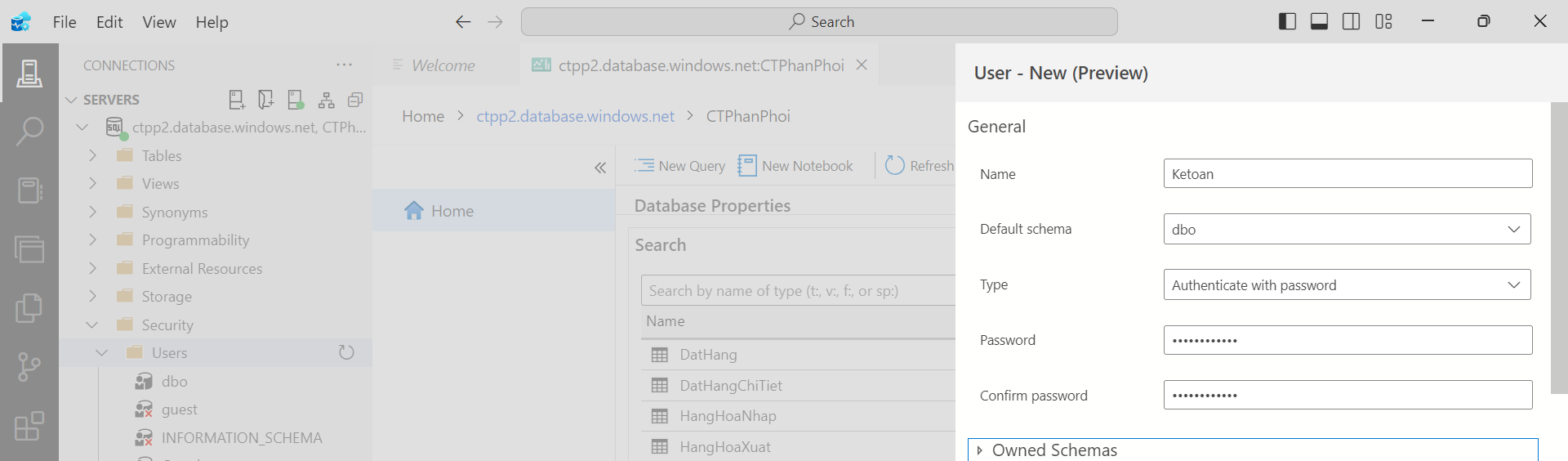
| Role | Account | Quyền DB | Quyền bảng |
| --- | --- | --- | --- |
| Quản lý | Quanly | Db\_ddladmin | Full bảng |
| NV Kế toán | Ketoan | Db\_datareader,  Db\_datawriter. | dbo.ThanhToan, dbo.ThanhToanChiTiet,  dbo.NhaCungCap  :Update,Insert,Select  Các bảng còn lại chỉ xem. |
| NV Kho | Thukho | Db\_datareader,  Db\_datawriter. | dbo.XuatKho,dbo.XuatKhoChiTiet,dbo.NhapKho,dbo.NhapKKhoChiTiet,dbo.Kho,dbo.HangHoaNhap  : Update,Insert,Select. |
| NV Bán hàng | Banhang | Db\_datareader,  Db\_datawriter. | dbo.DatHang,dbo.DatHangChiTiet,dbo.HangHoaXuat,dbo.KhachHang  : Update,Select,Insert. |

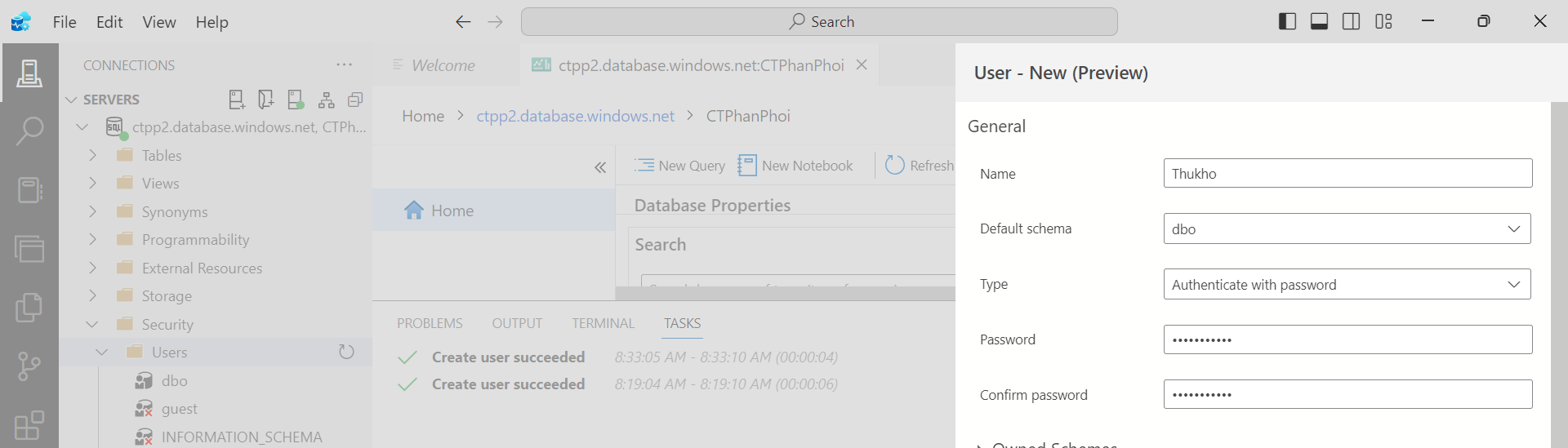
1. Tạo tài khoản User:

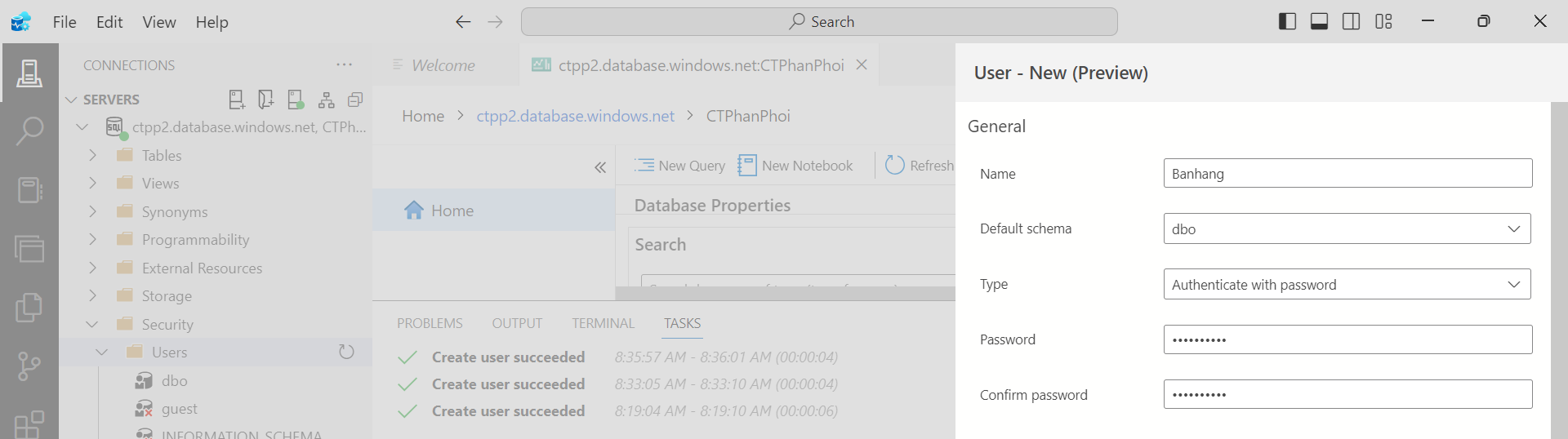
Tạo 4 tài khoản: Quản lý, Kế toán, Bán Hàng, Thủ kho. Với Username và password như sau:

|  | Username | Password |
| --- | --- | --- |
| 1 | Quanly | Q@un4Ly2024! |
| 2 | Ketoan | K#3toAn!2024 |
| 3 | Thukho | Thuk0!2024$ |
| 4 | Banhang | B@nh@ng12\* |



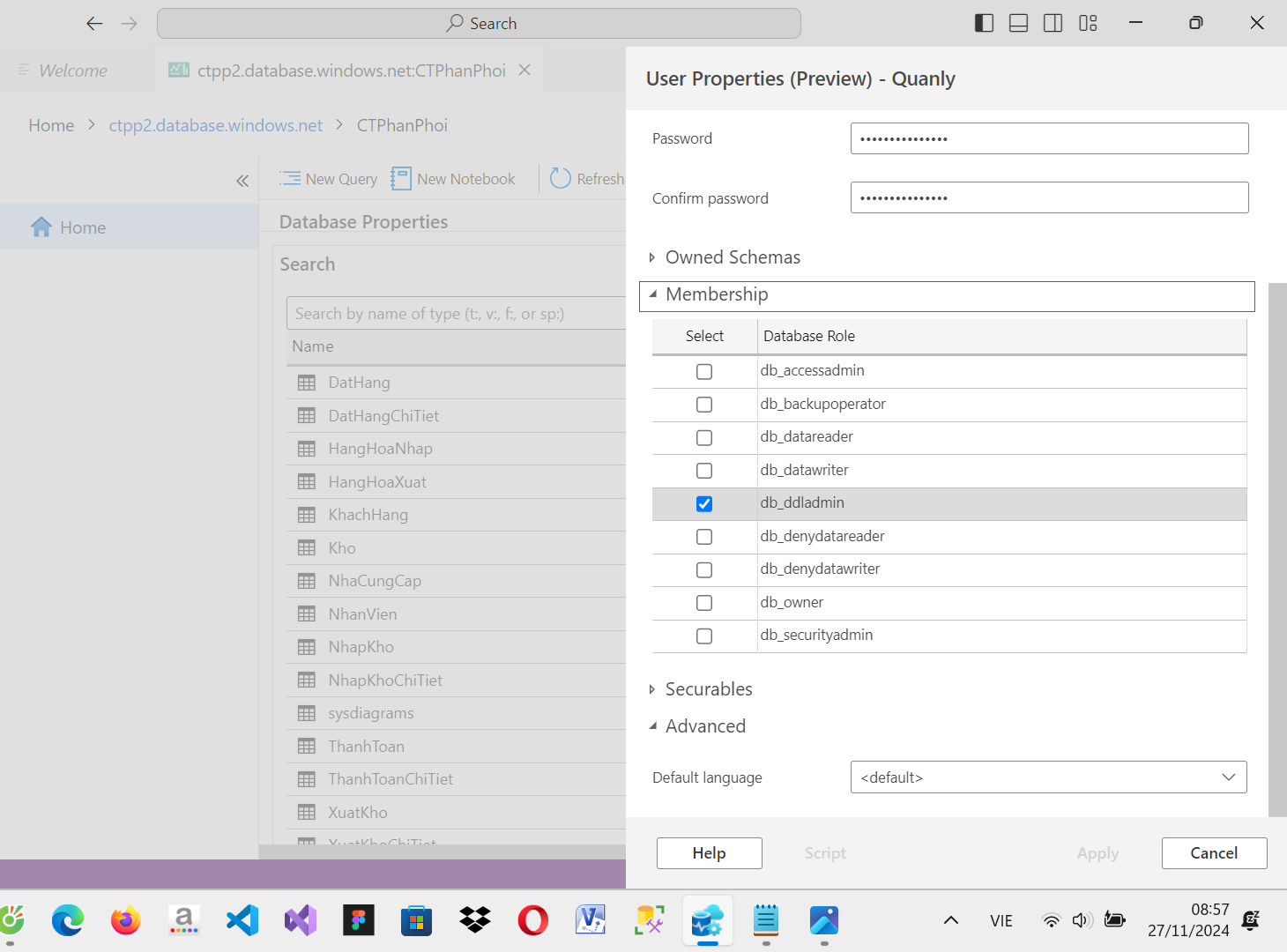




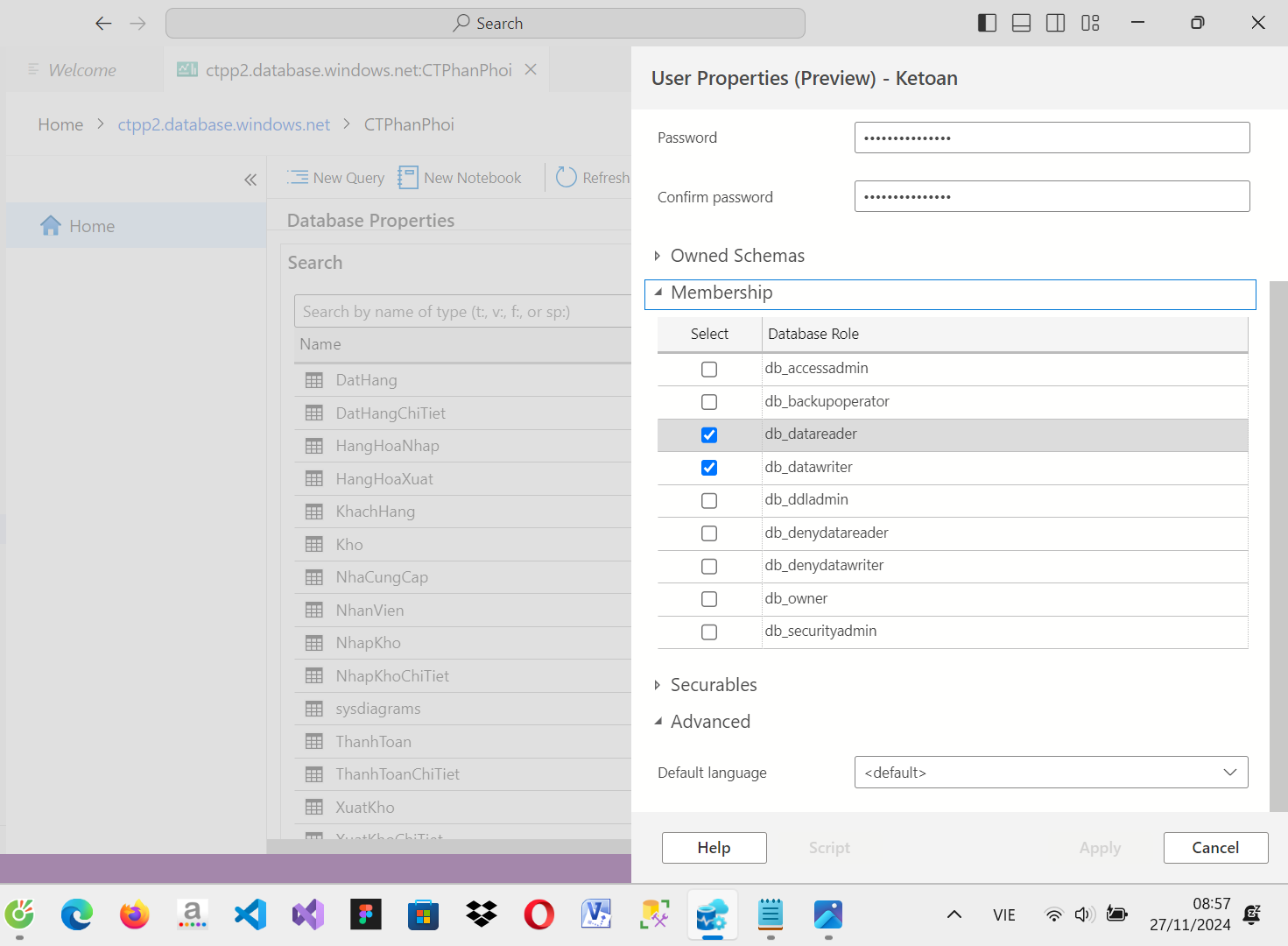


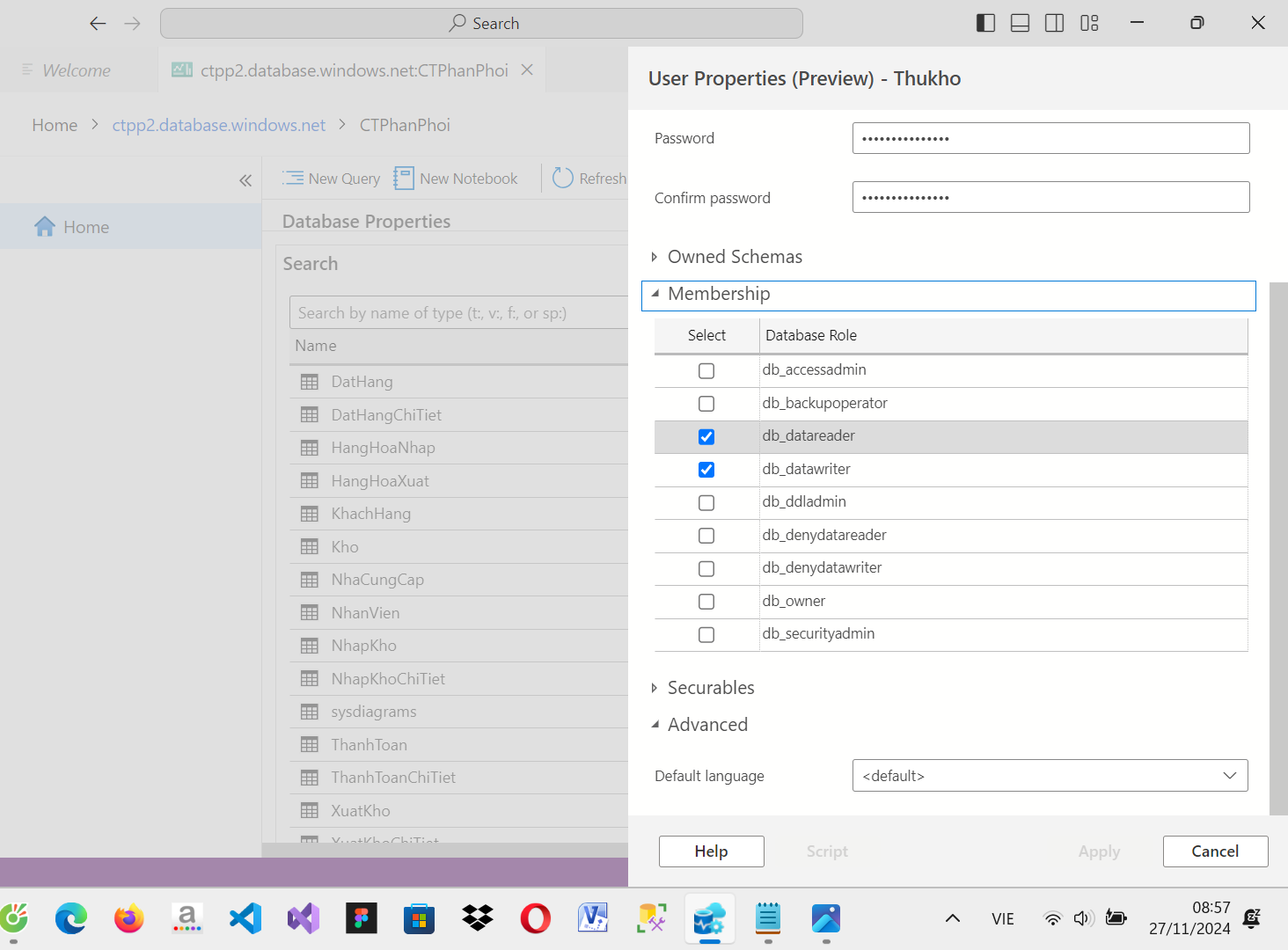
1. Thiết lập quyền trên database ( CTPhanPhoi):

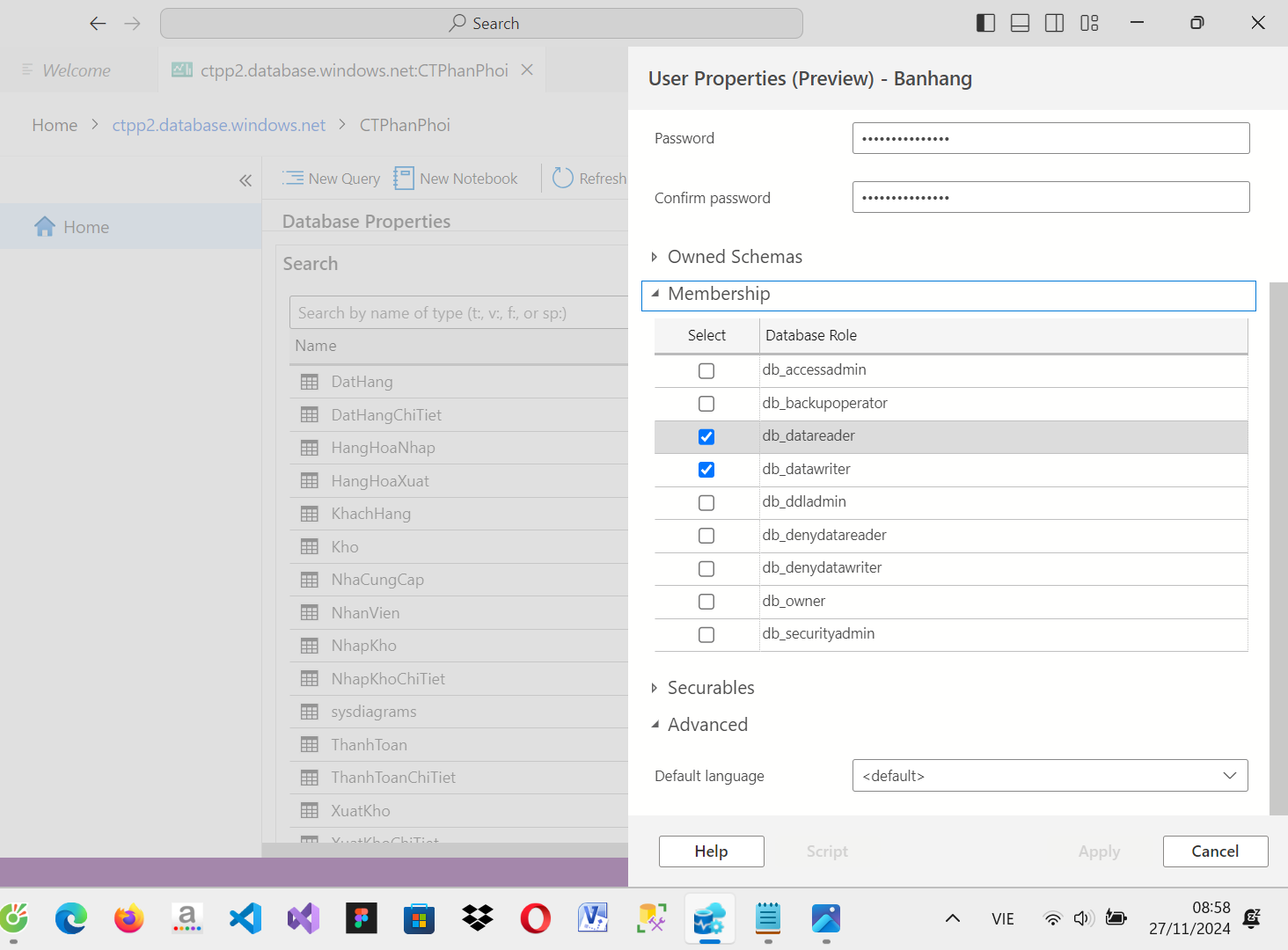
Với quản lý có quyền hạn là db\_ddladmin. Mục đích: Quản lý toàn bộ database với quyền hạn của tài khoản admin.



Với User: Ketoan,Thukho,BanHang cùng chung 1 nhóm quyền là đọc và ghi vào do đó quyền được cấp là db\_datawriter,db\_datareader. Mục đích: Ghi nhận việc đã làm và xem được công việc đó, không ảnh hưởng đến các quyền hạn khác.

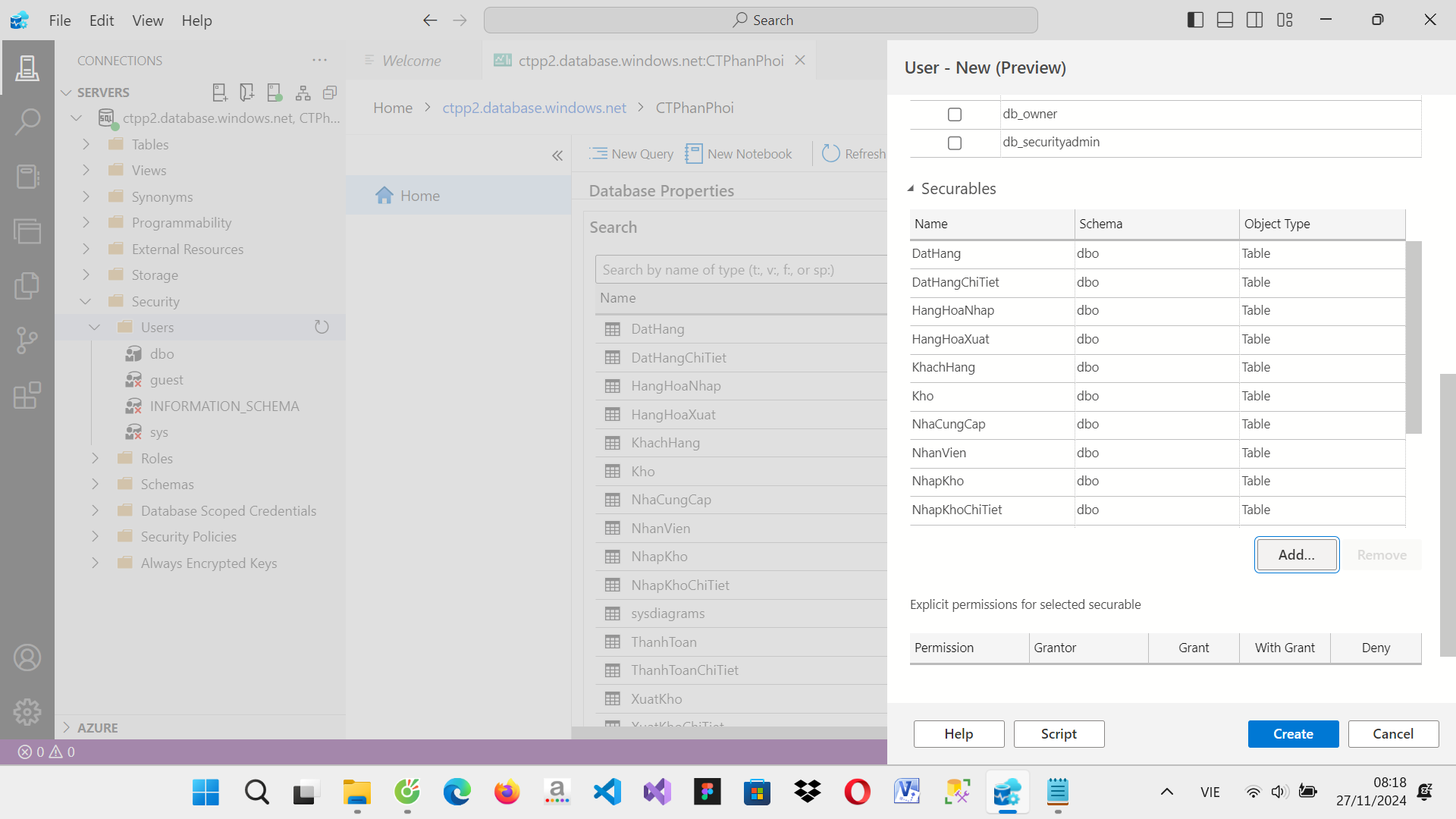


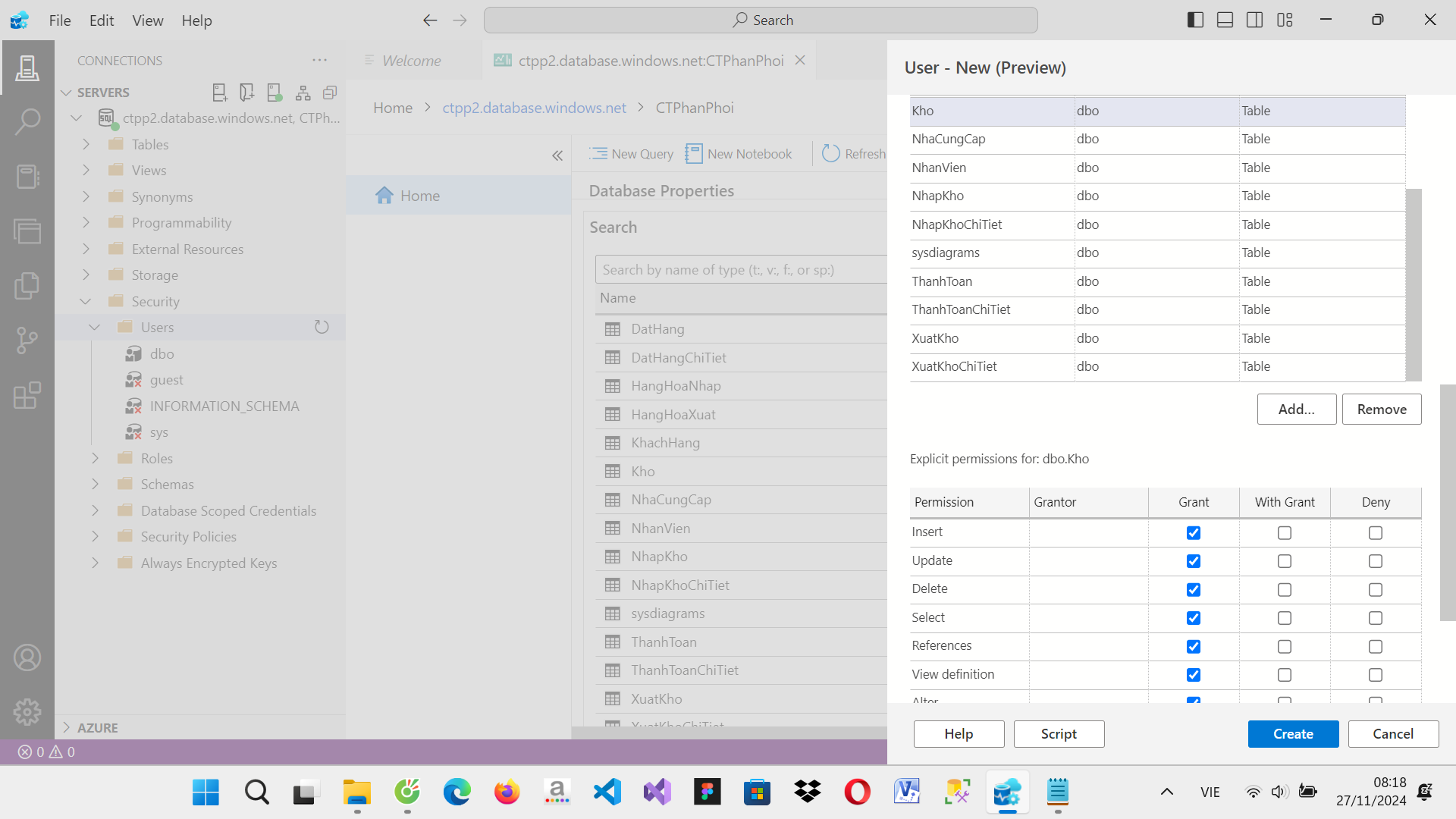




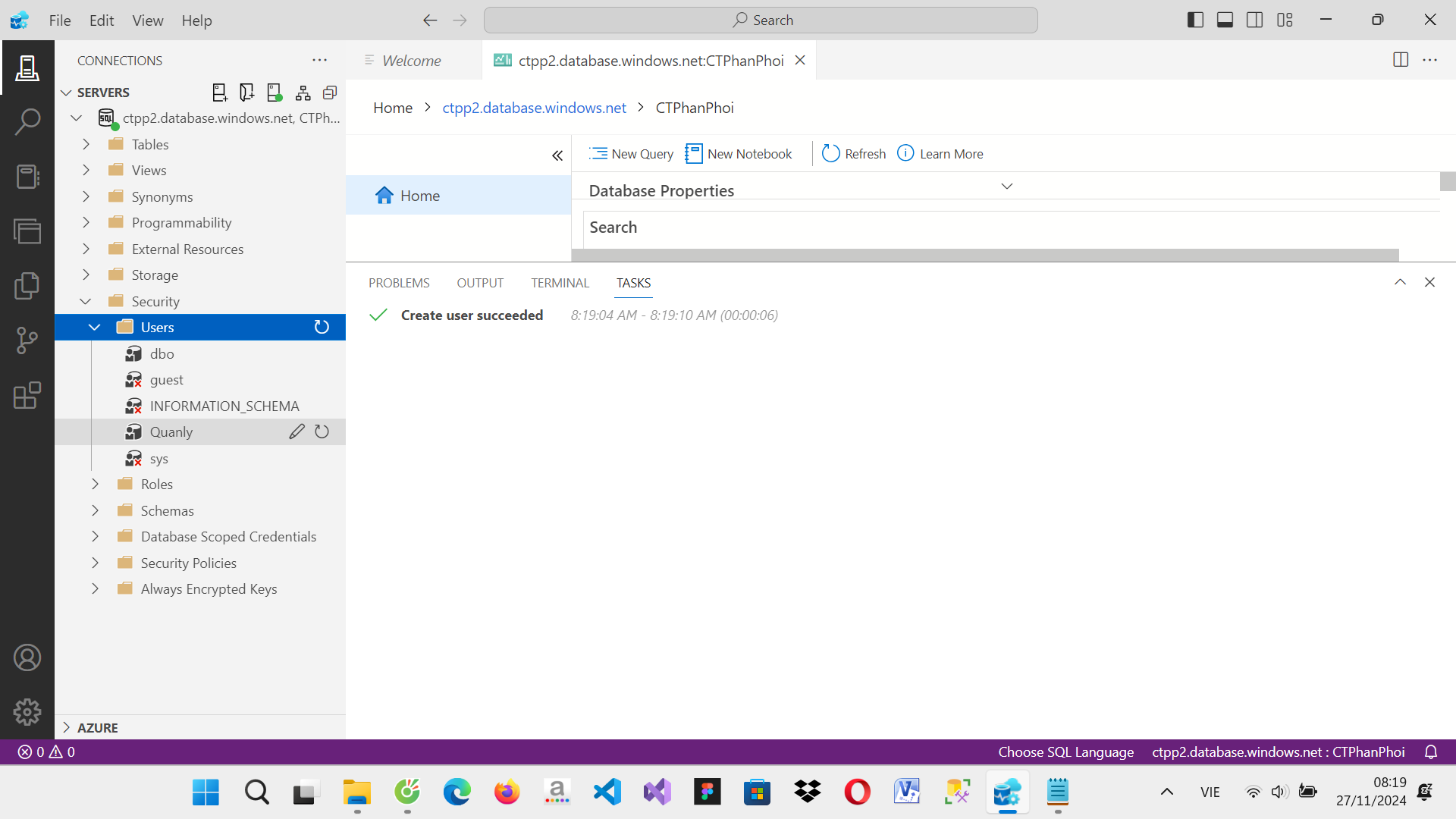
1. Thiết lập quyền trên bảng nhất định của database đã chọn: ( database: CTPhanPhoi):

* User Quanly với mục đích được xác lập để quản lý toàn bộ database do đó có quyền trên toàn bộ các bảng với đầy đủ các nhóm quyền.

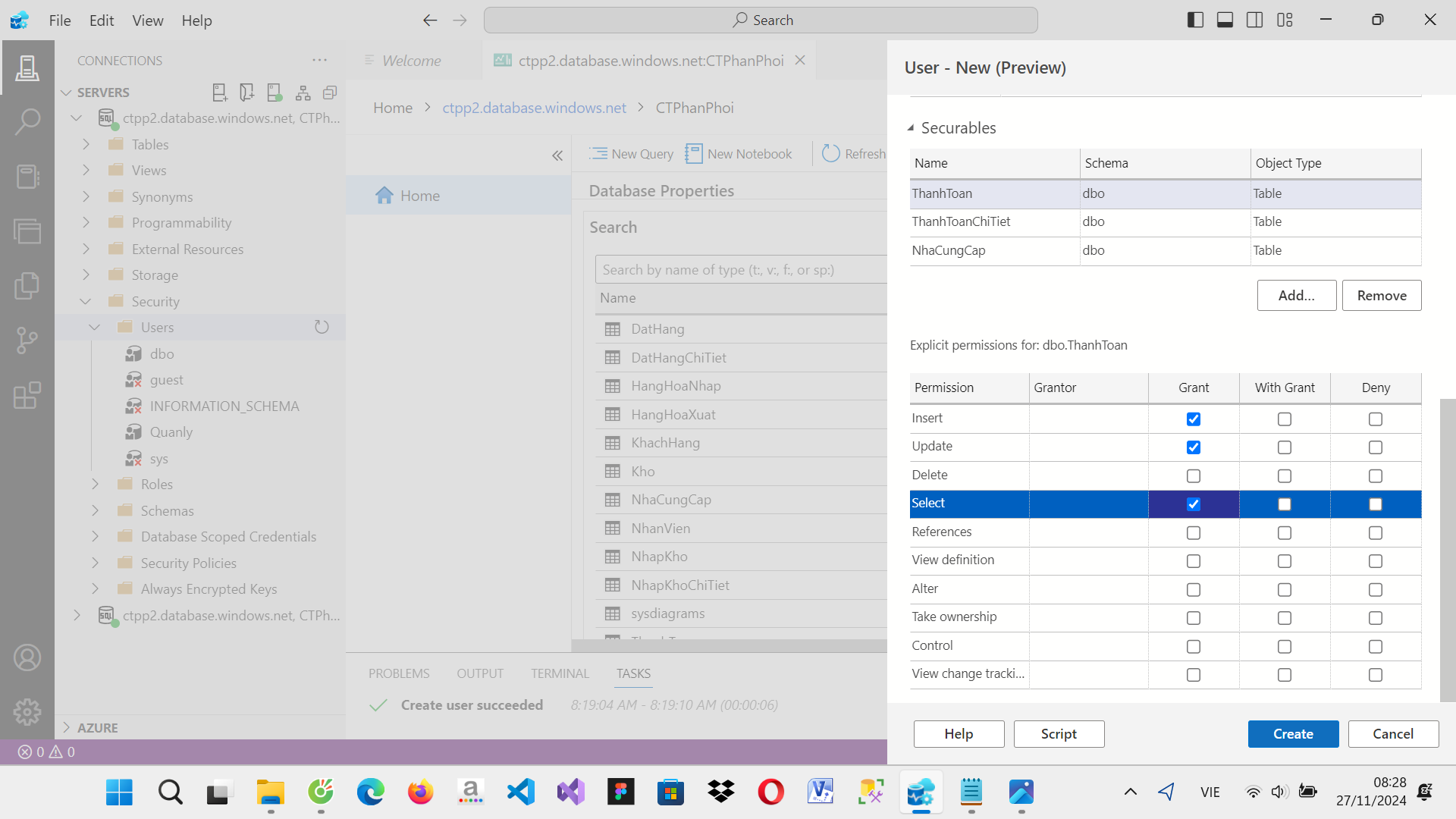
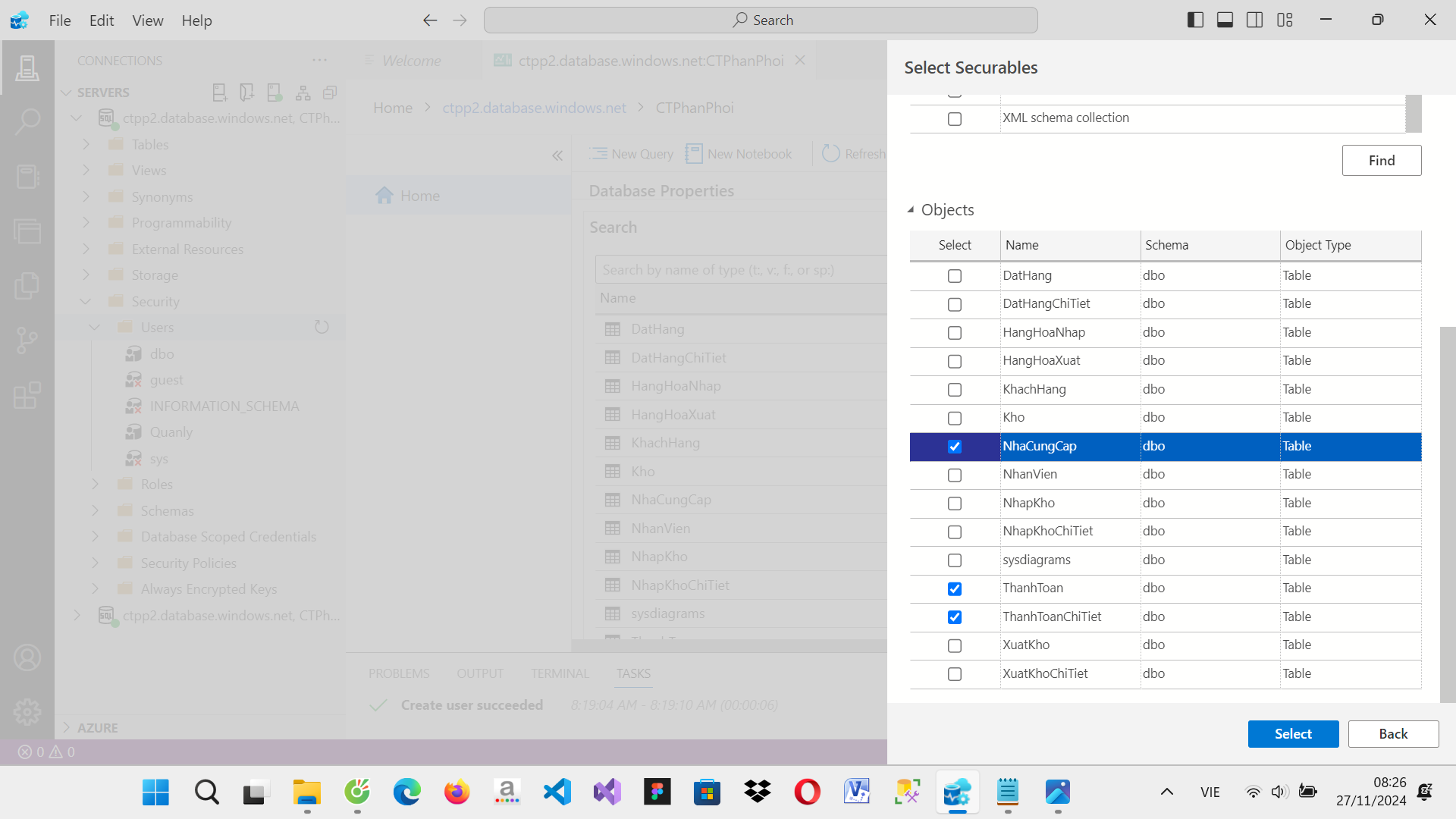




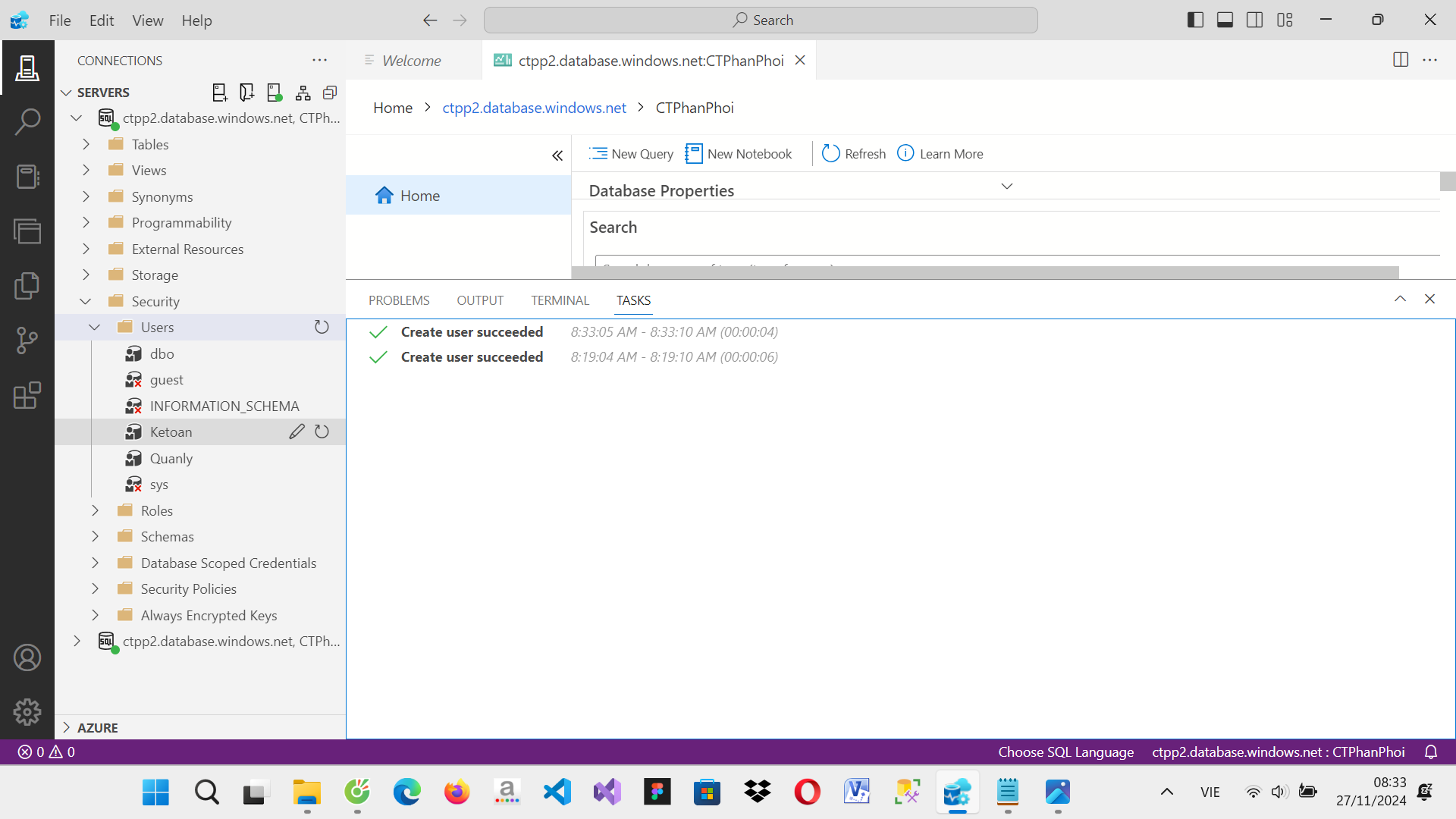
Sau khi ta phân quyền xong cho 1 bảng, tiến hàng phân quyền cho các bảng còn lại tương tự cho đến khi hết.



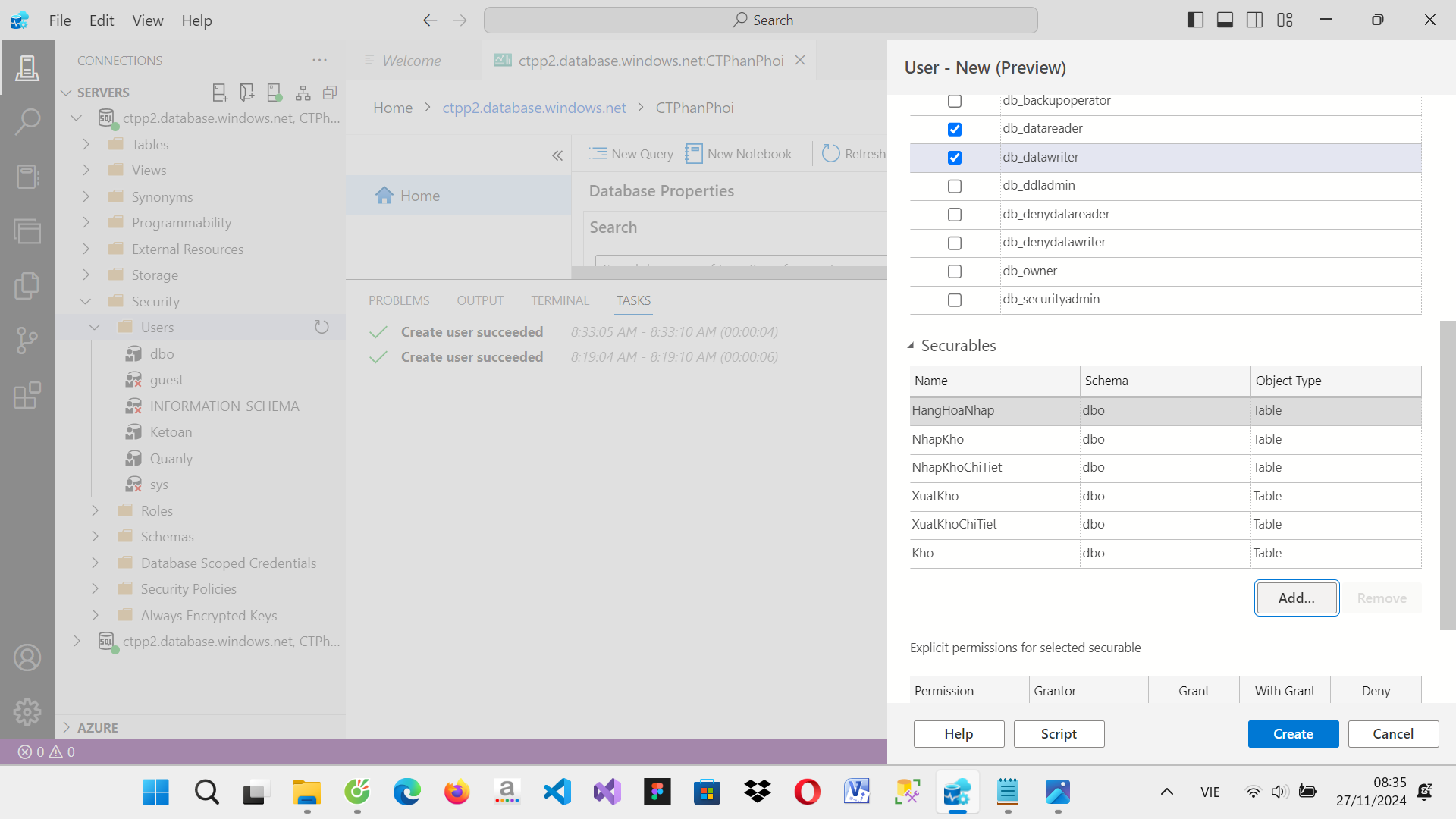
* User Ketoan với công việc là quản lý thanh toán và dòng tiền nên được chọn các bảng như trên bảng mô tả. Mục đích phân quyền: Được cập nhật, sửa đổi và xem trên bảng nhất định của công việc kế toán.

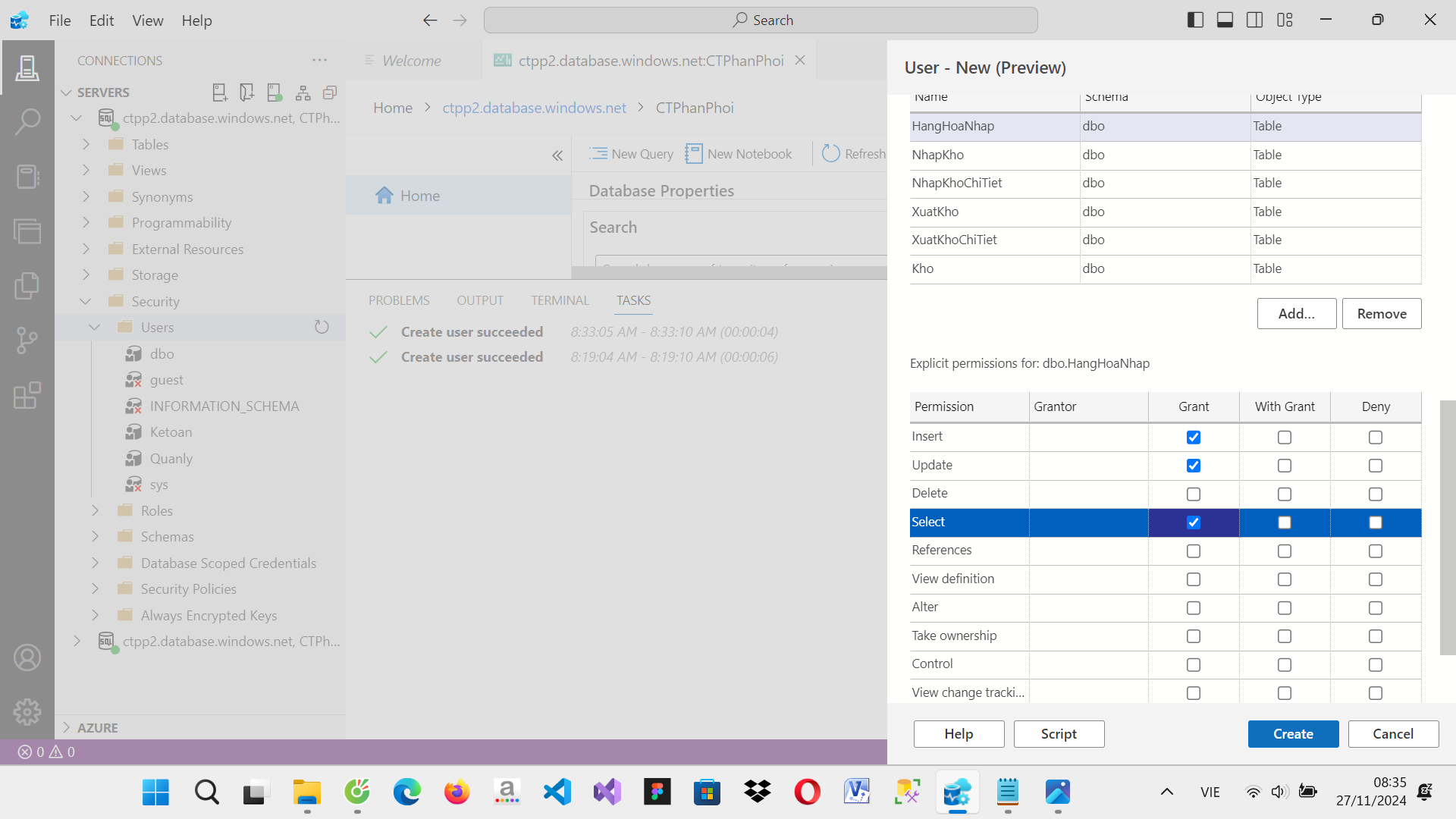


Sau khi ta phân quyền xong cho 1 bảng, tiến hàng phân quyền cho các bảng còn lại tương tự cho đến khi hết.

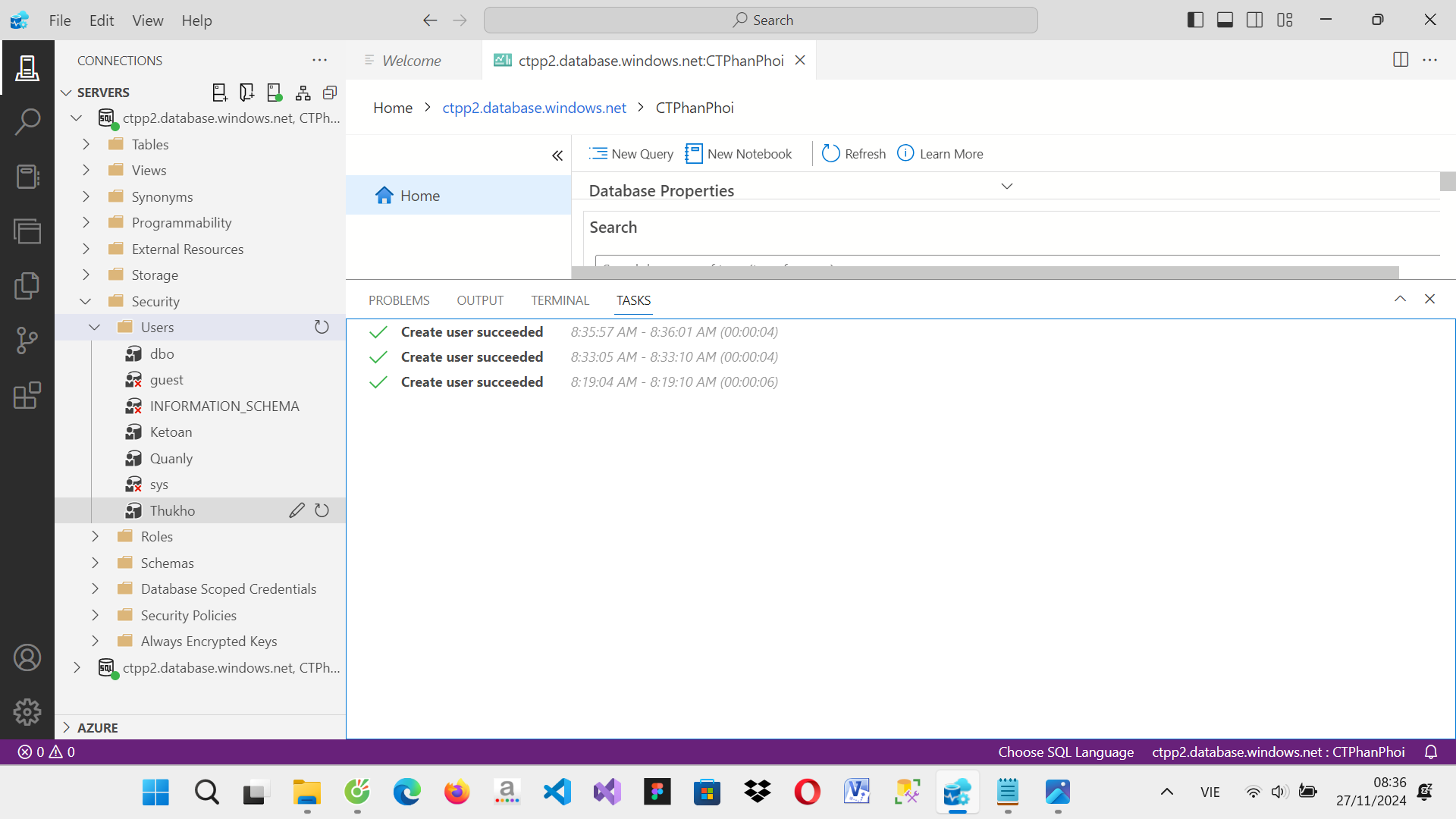


* User Thukho với công việc quản lý kho hàng và nguồn hàng ra vào. Do đó được phân quyền với các bảng như trên bảng mô tả. Mục đích phân quyền: Được cập nhật, sửa đổi và xem trên bảng nhất định của công việc thủ kho.

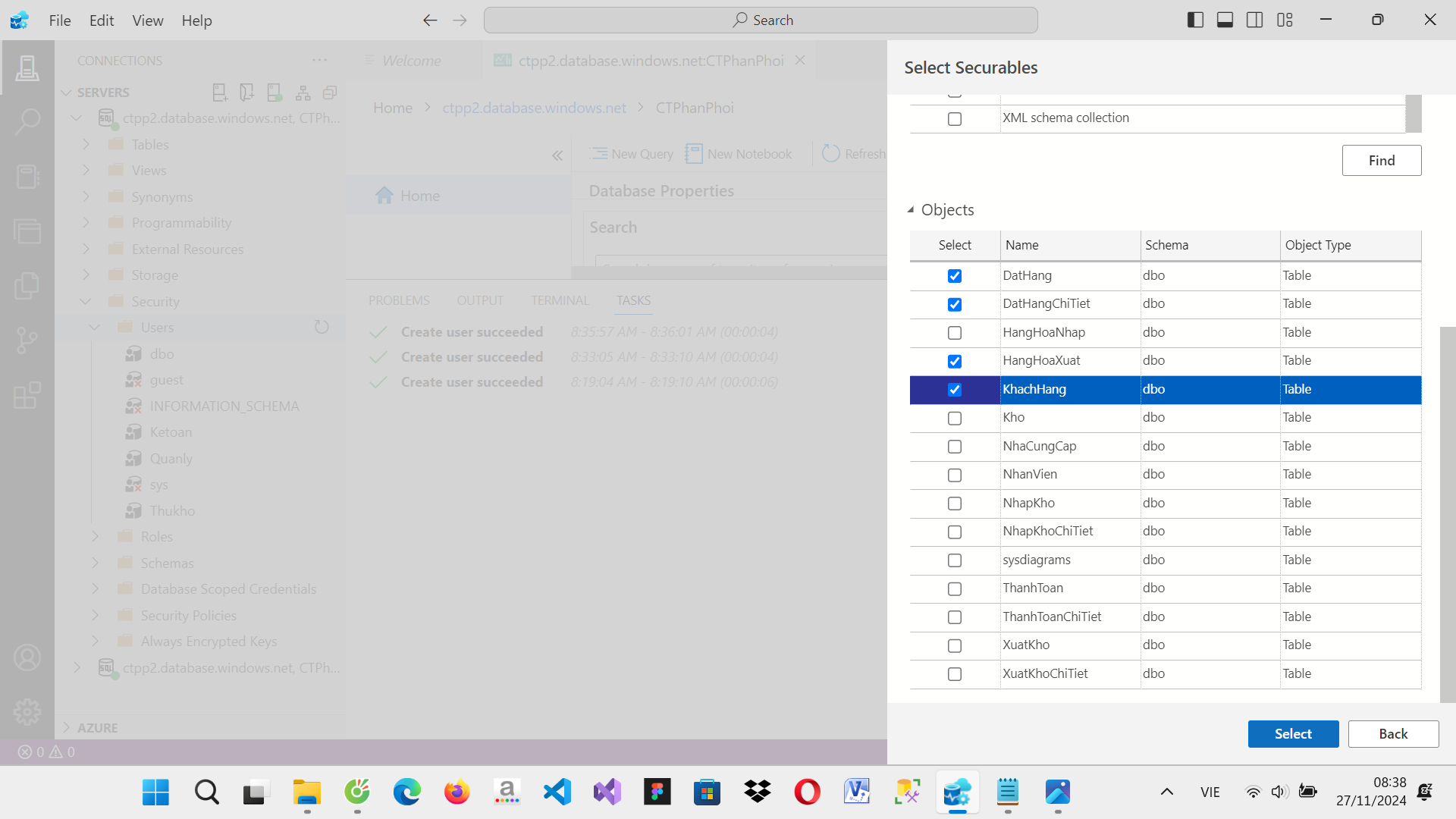


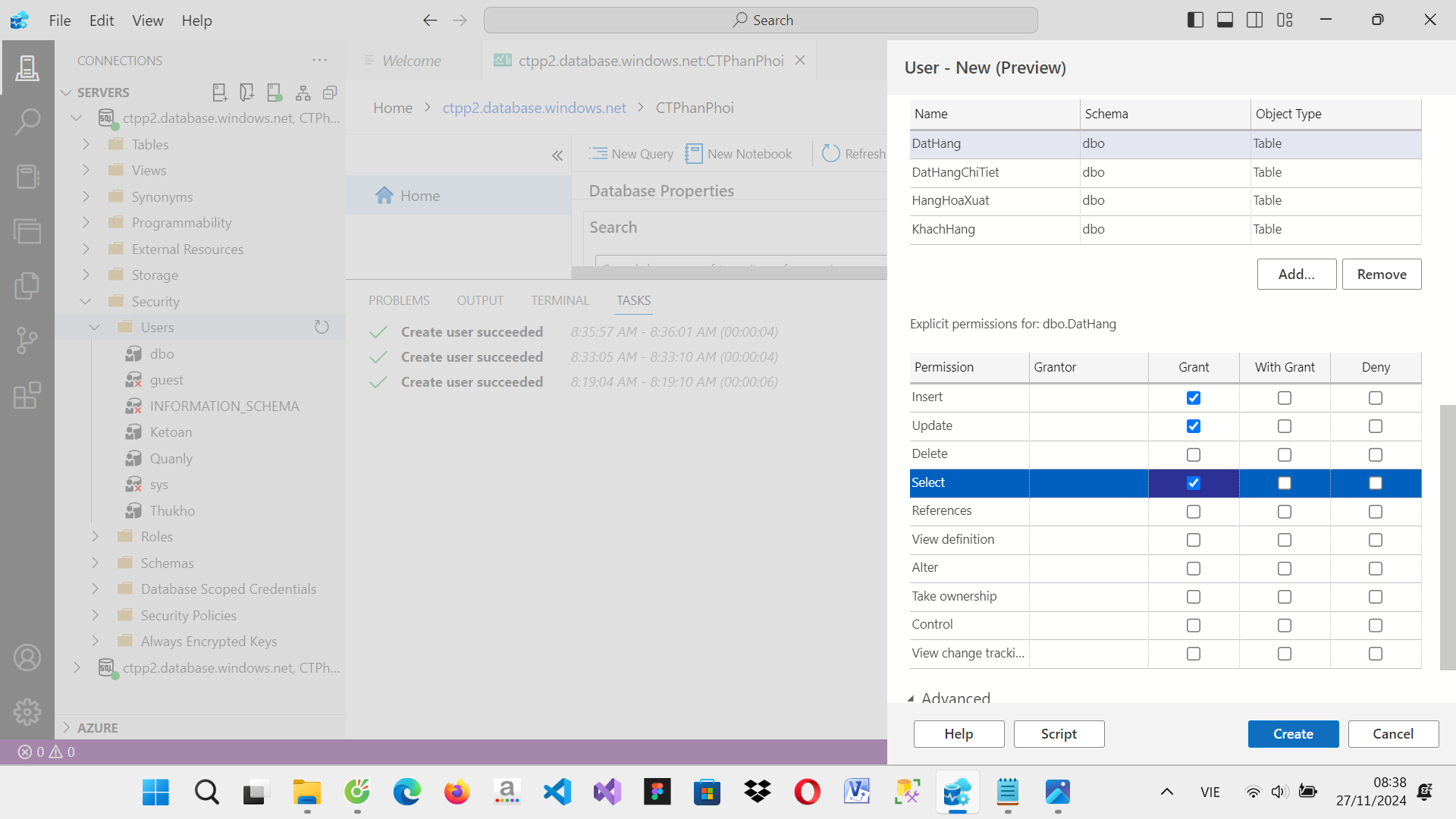


Sau khi ta phân quyền xong cho 1 bảng, tiến hàng phân quyền cho các bảng còn lại tương tự cho đến khi hết.

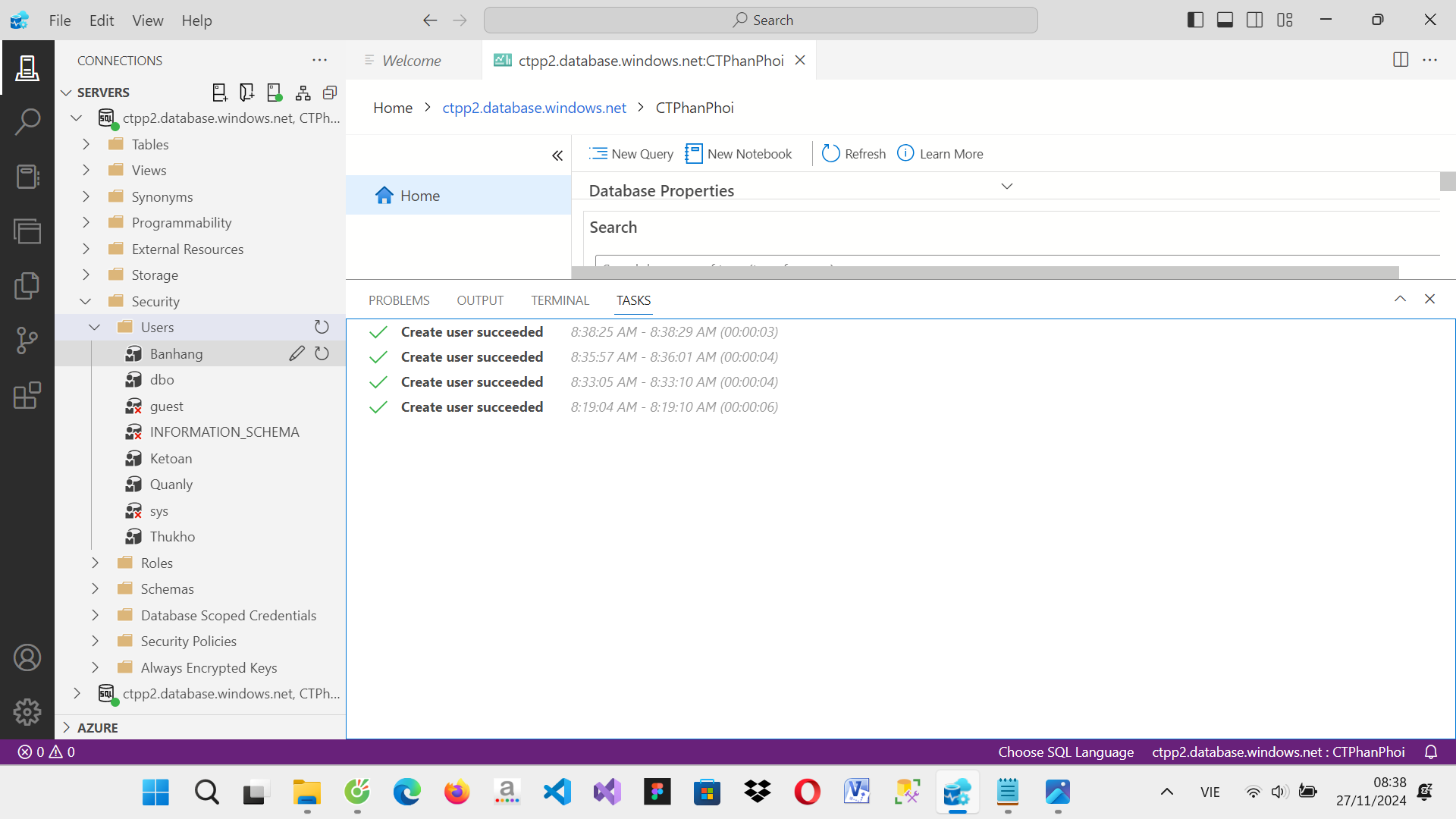


* Với User Banhang với công việc là bán hàng cho khách hàng. Do đó được phân quyền trên 1 số bảng liên quan đến bán hàng như trên bảng mô tả. Mục đích phân quyền: Chỉ được cập nhật, sửa đổi và xem xét trên bảng nhất định trong công việc của nhân viên bán hàng.





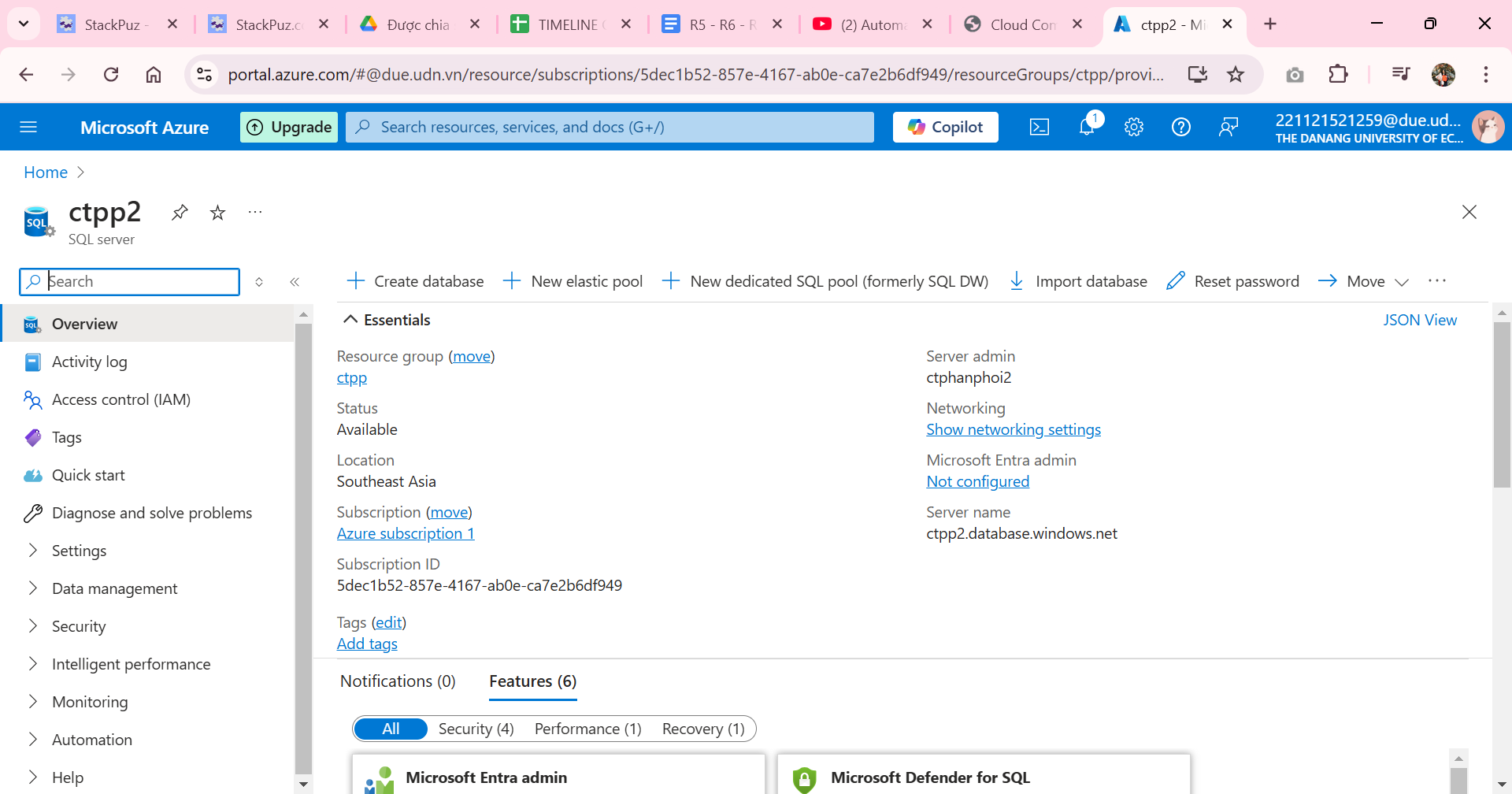
Sau khi ta phân quyền xong cho 1 bảng, tiến hàng phân quyền cho các bảng còn lại tương tự cho đến khi hết.



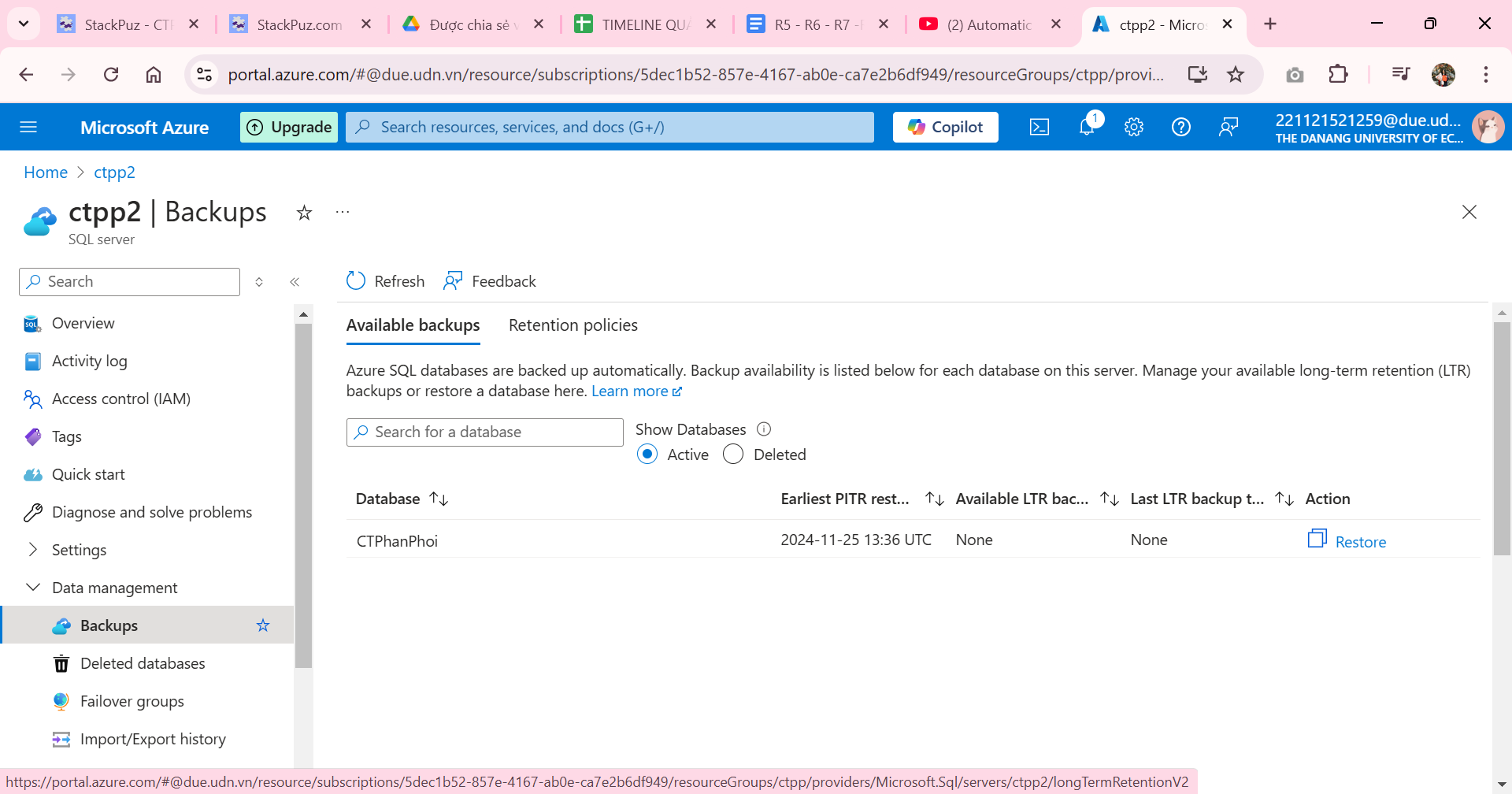
**II. Mã hóa cột:**

1. **Nội dung R6:**

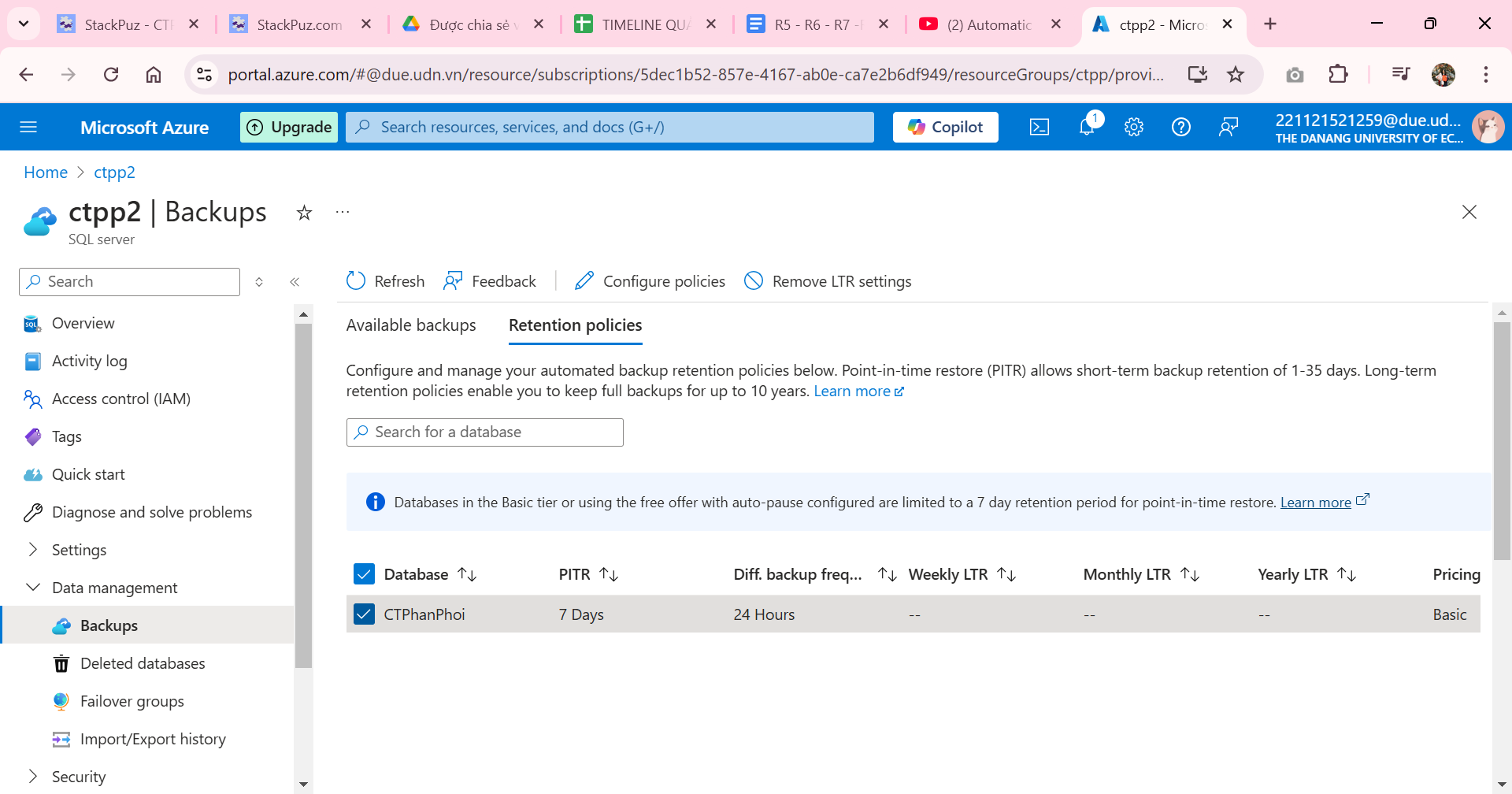
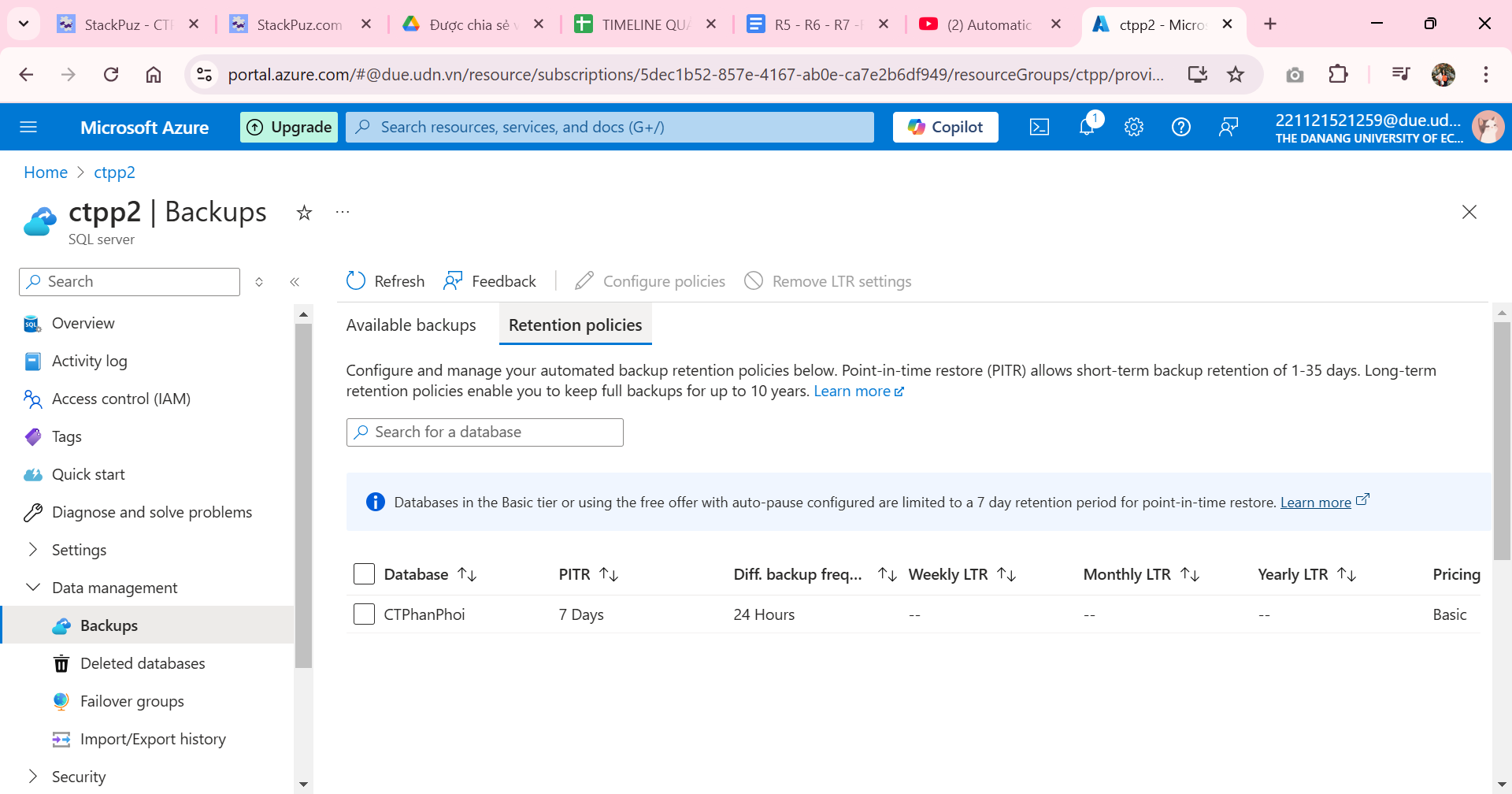
**B1:** đăng nhập vào tài khoản **Microsoft Azure** và kết nối với database trong **SQL server**. Sau khi kết nối được dữ liệu, truy cập vào database đó trên **MS Azure**.

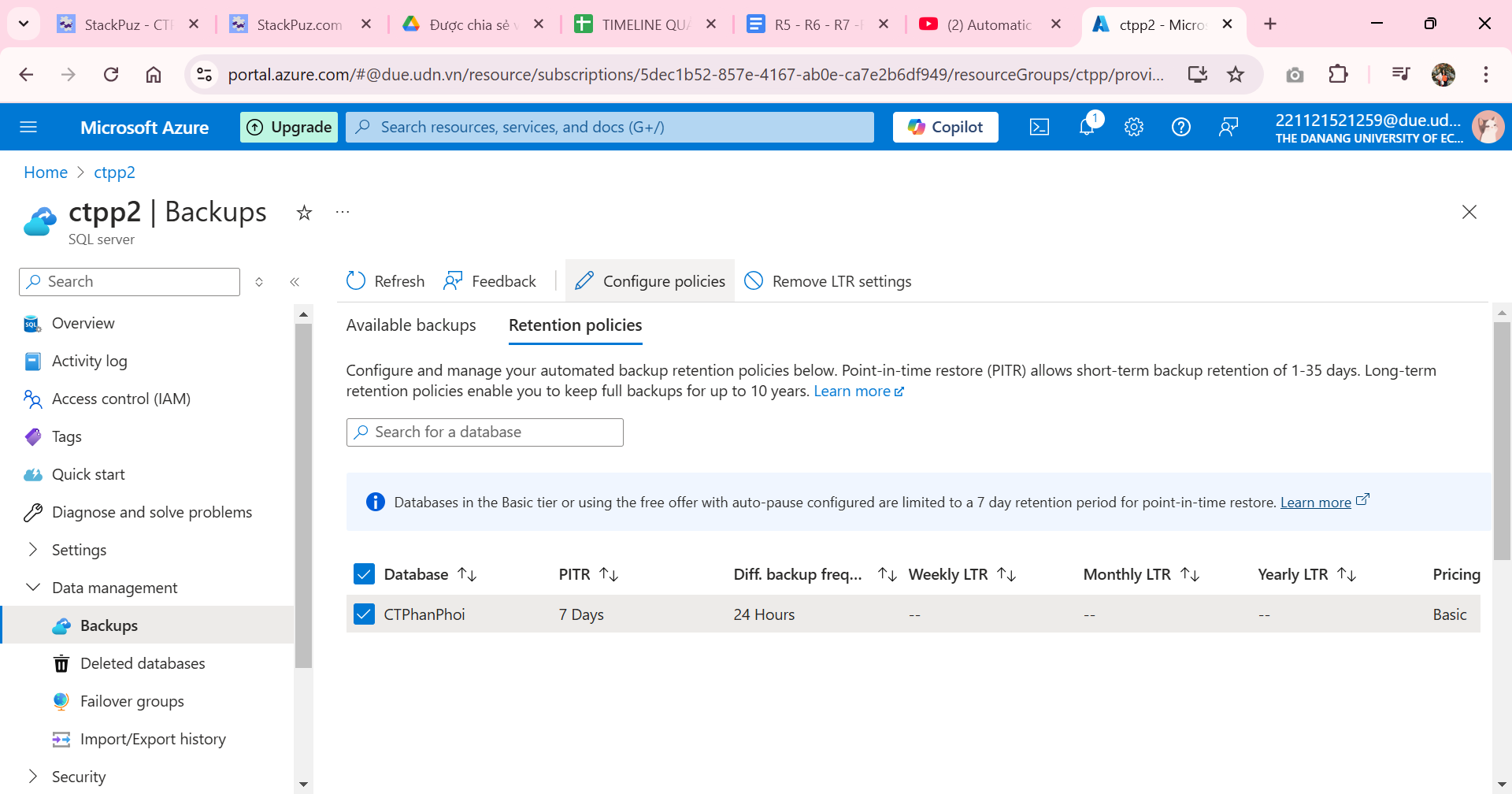
****

**B2:** Chọn **Data Management**, chọn **BackupBackups**

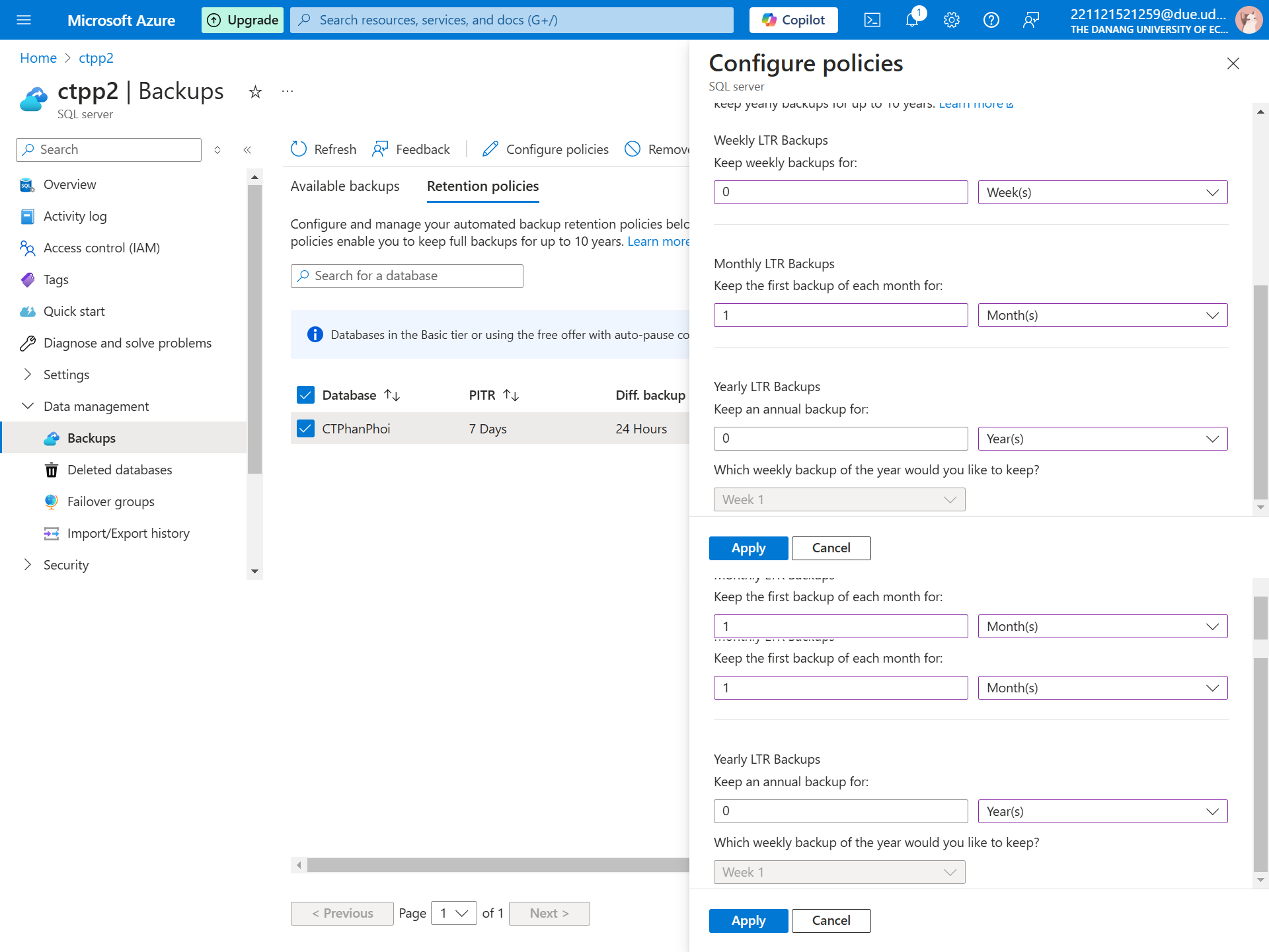
****

**B3:** Chọn **Retention policies** và chọn vào database muốn sao lưu

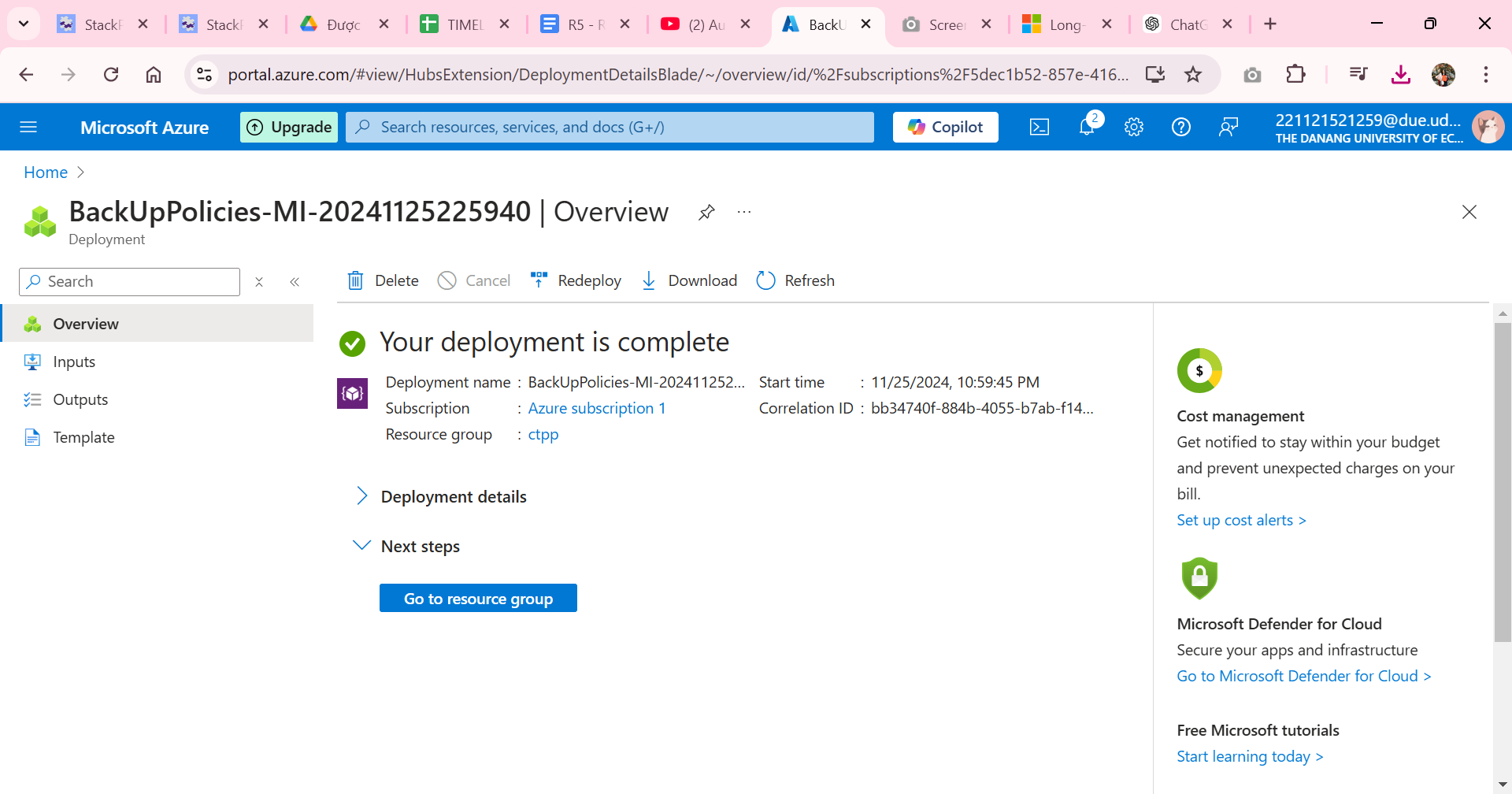
****

****

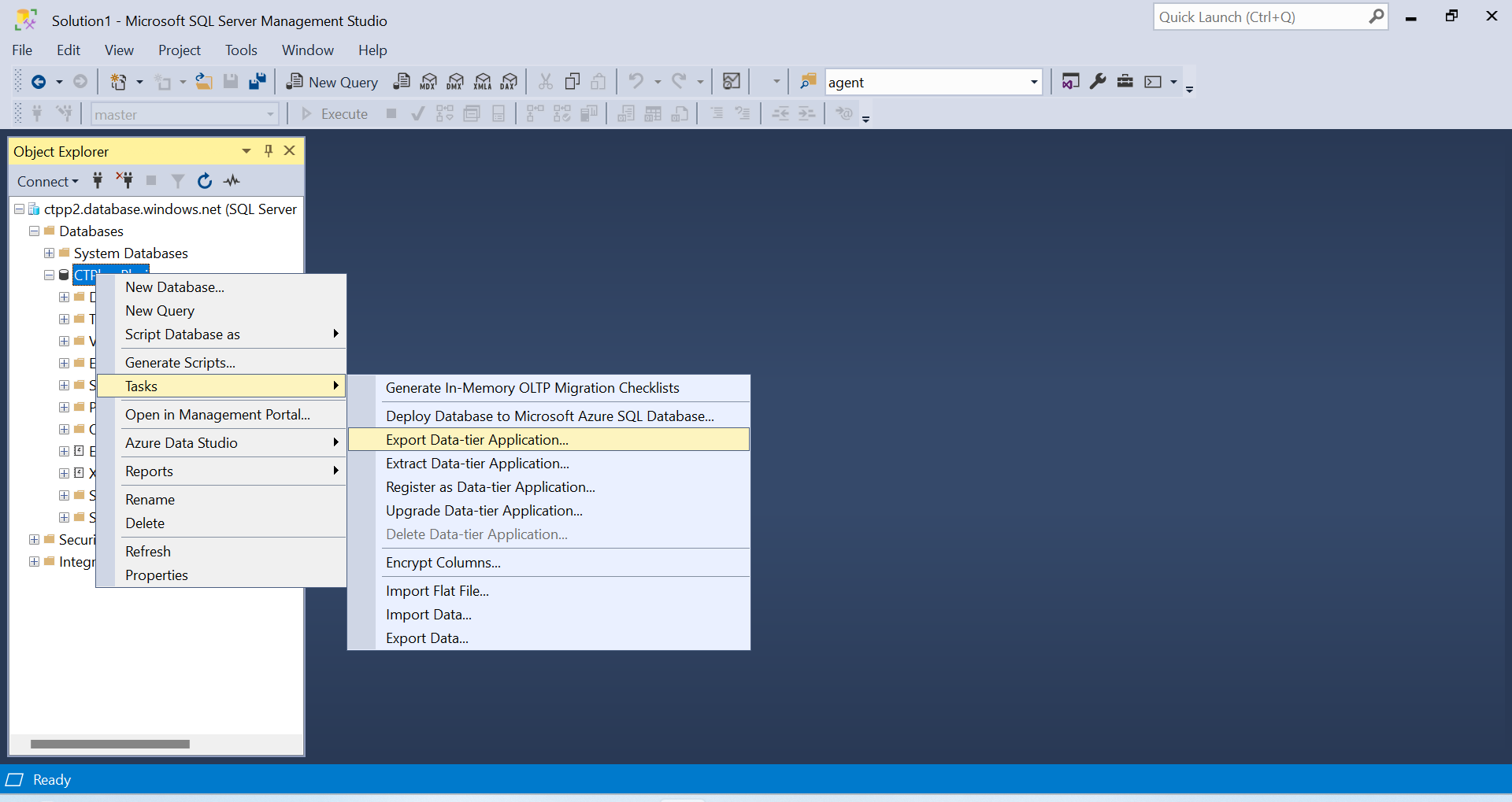
**B4:** lựa chọn thời gian sao lưu

****

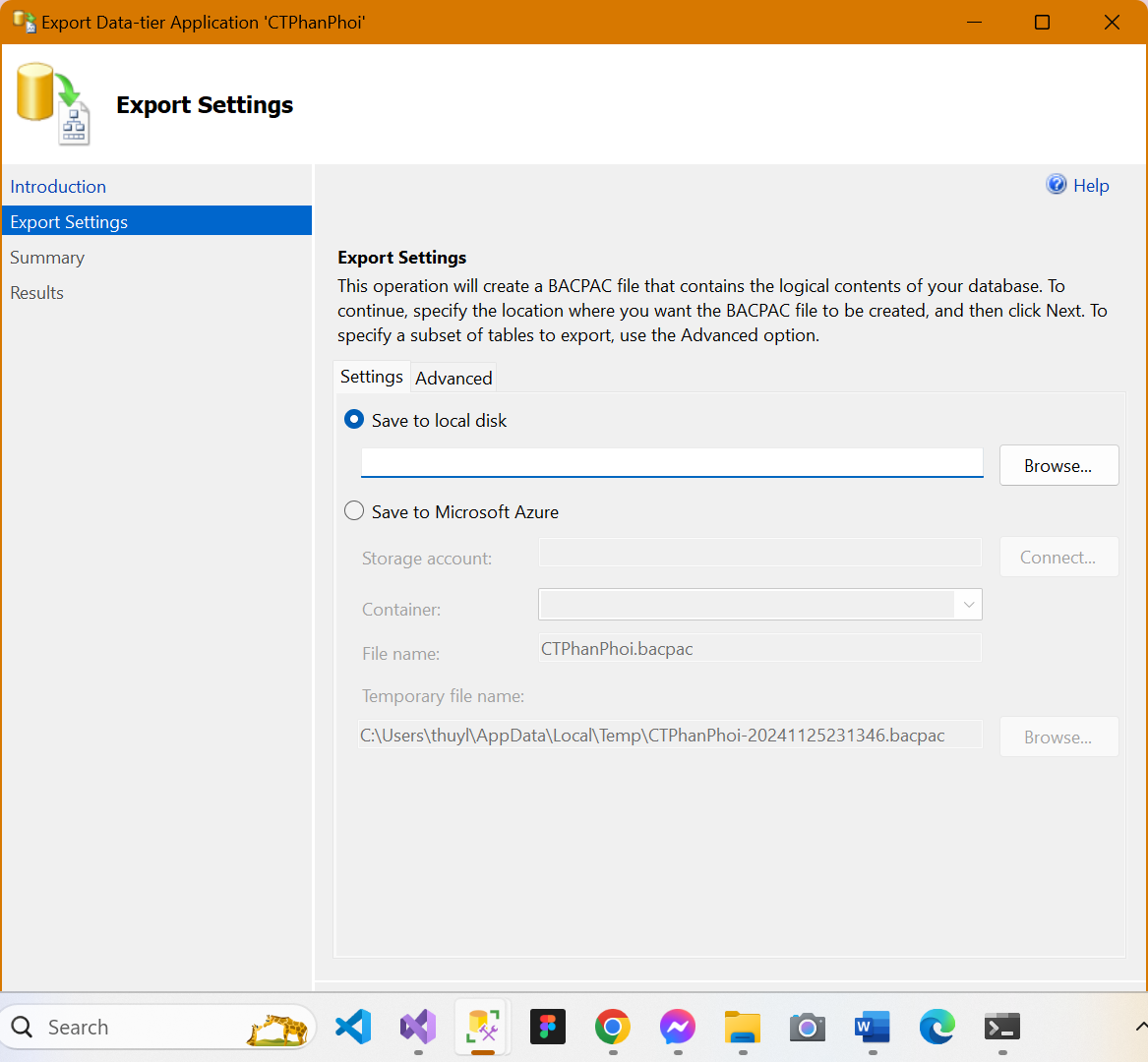
**B5:** sau khi lựa chọn thời gian sao lưu xong, chọn vào **Apply**. Sau đó màn hình sẽ hiển thị thông báo **Your deployment is complete**

****

**B6:** mở SQL server lên, ấn chuột phải vào database muốn sao lưu, chọn **Tasks**, chọn **Export Data tier Application…**

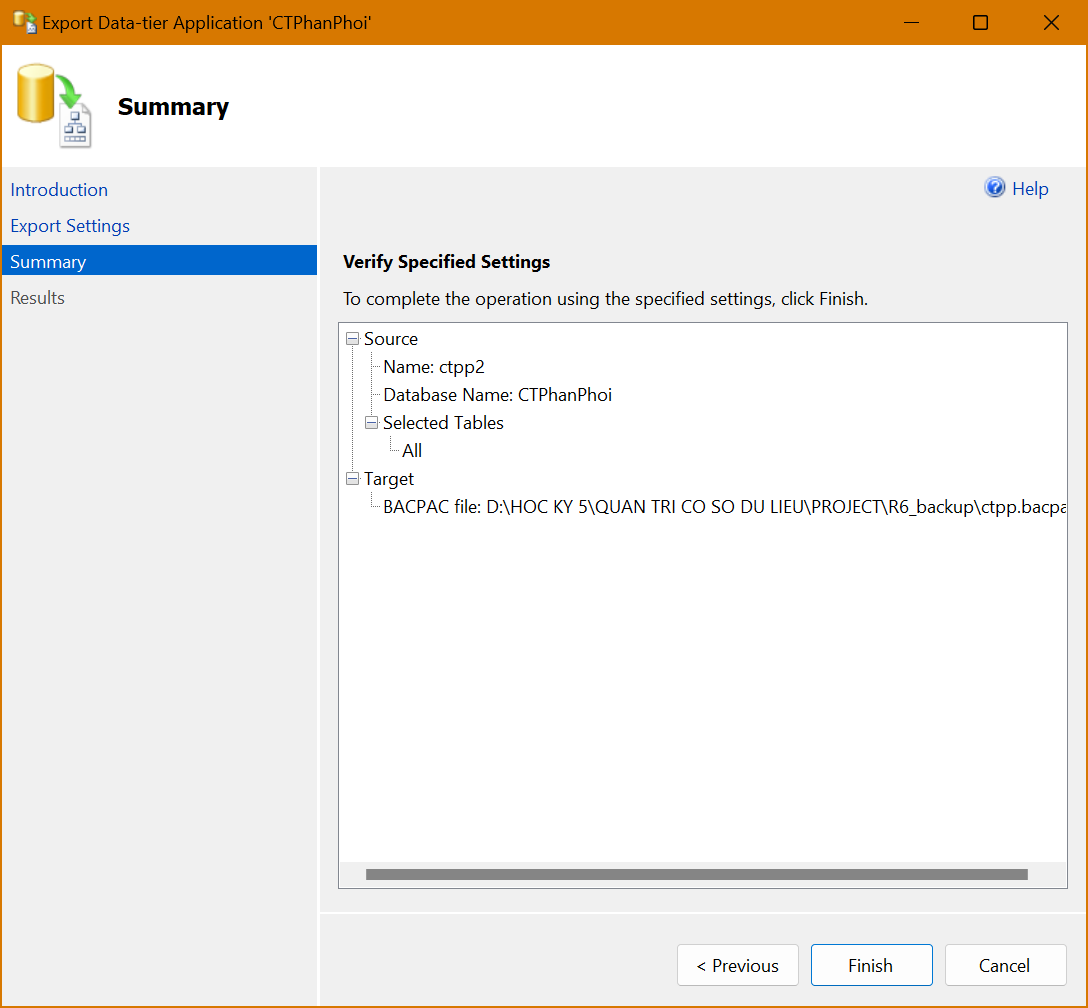
****

**B7:** Chọn nơi muốn lưu trữ file backpack và đặt tên file

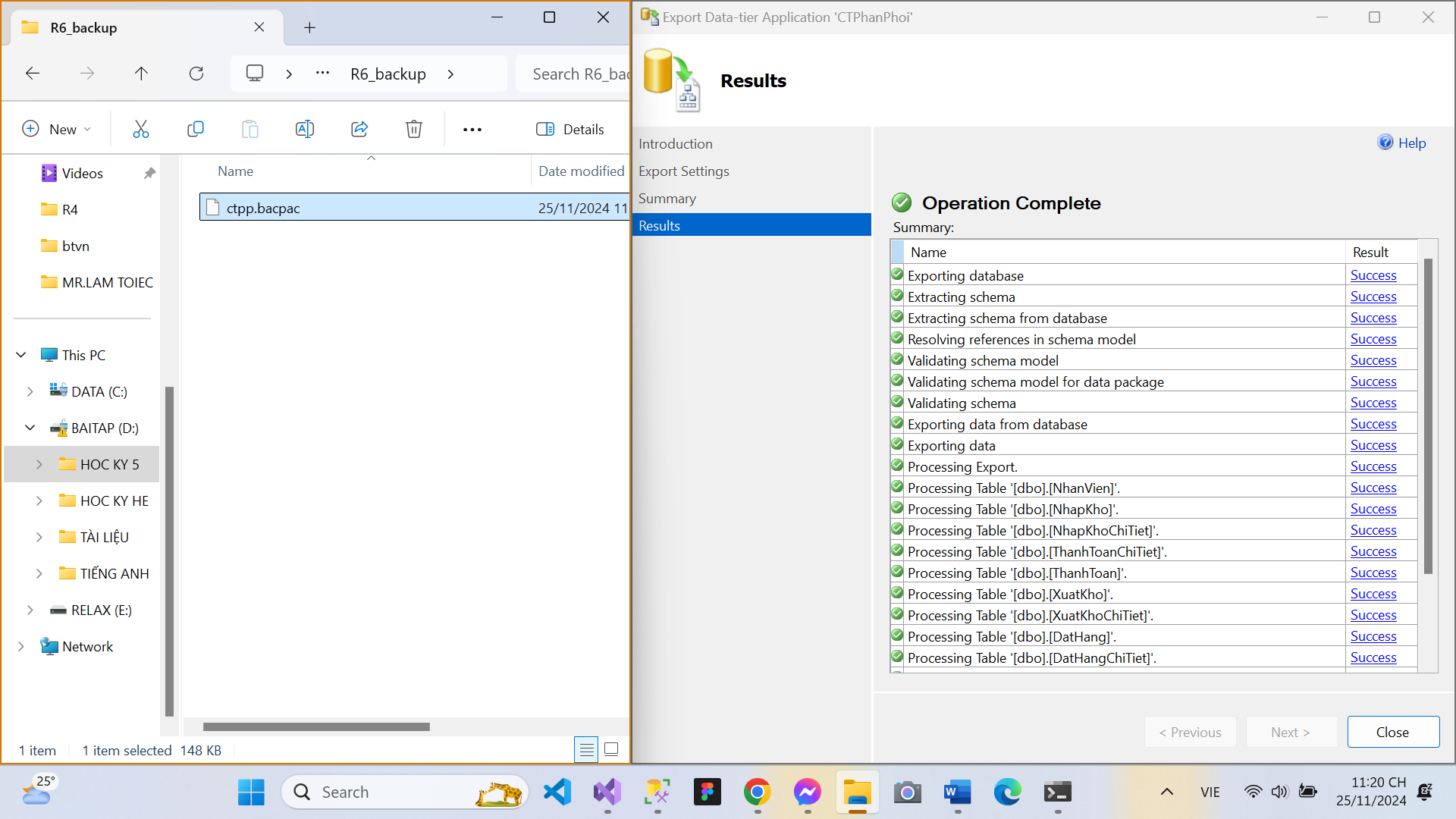
****

****

**B8:** Chọn **Finish** để bắt đầu sao lưu dữ liệu

****

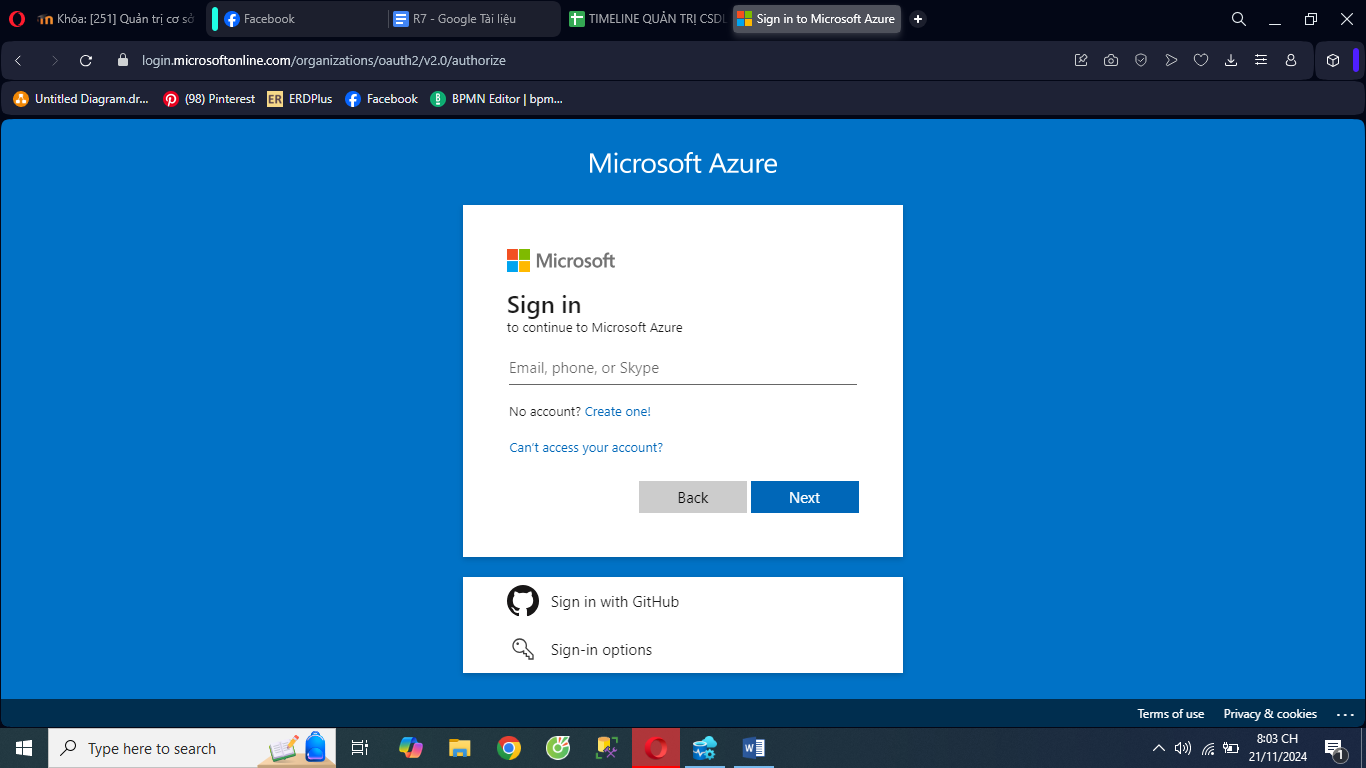
**B9:** Nếu dữ liệu được sao lưu thành công, màn hình sẽ hiển thị thông báo **Operation Complete** và xuất hiện file .bacpac ở thư mục đã được chỉ định trước đó.

****

1. **Nội dung R7:**

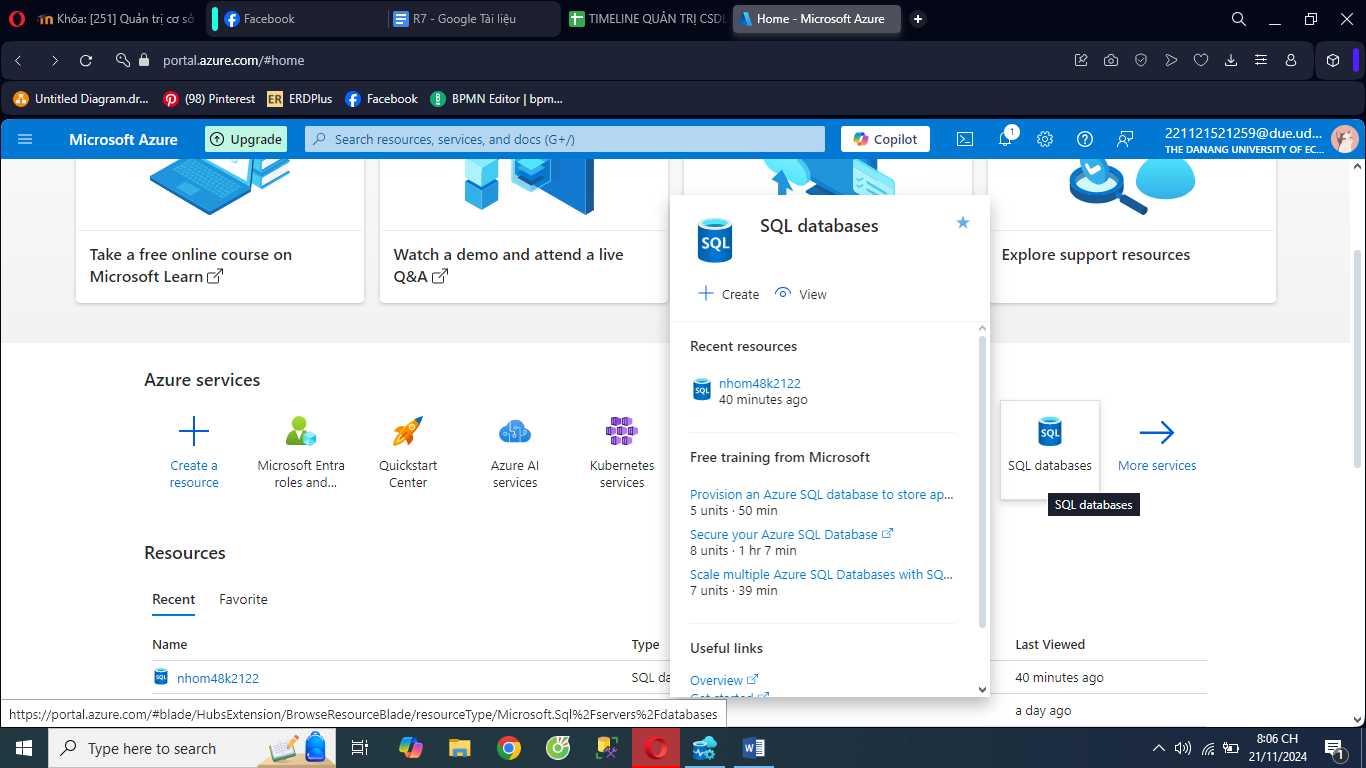
R7. Phương án giải quyết tốt nhất cho việc lượng dữ liệu rất lớn: Sử dụng Cloud

1. Đăng nhập vào Microsoft Azure

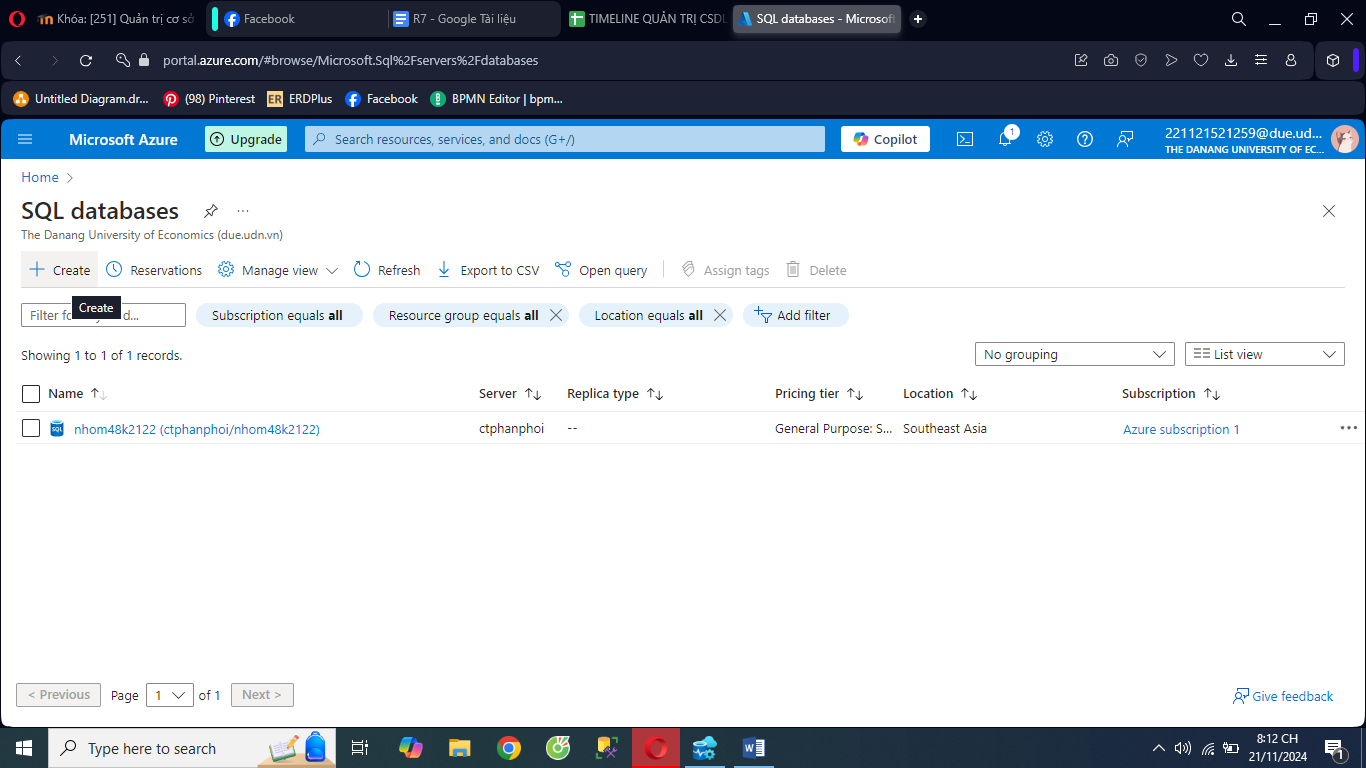


1. Tạo một cơ sở dữ liệu trên Microsoft Azure

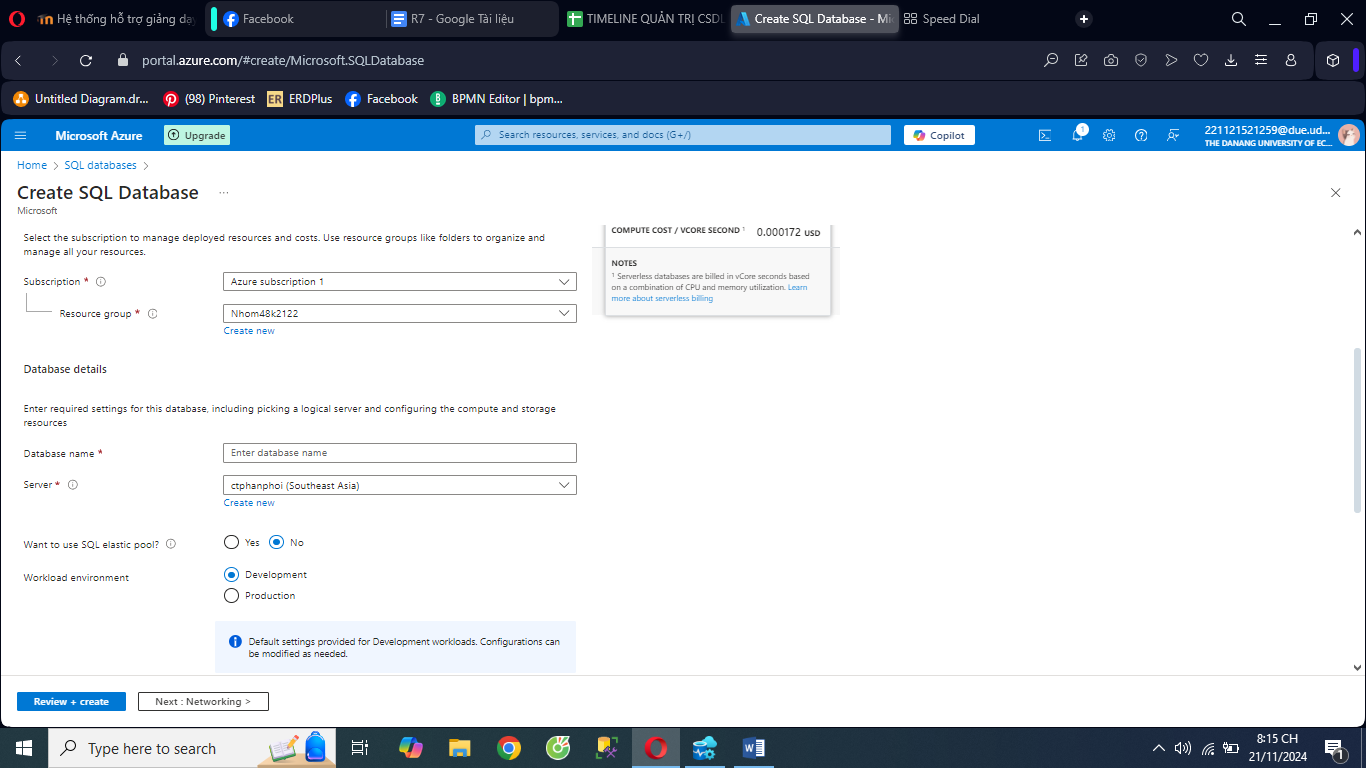
B1: Chọn SQL databases



B2: Chọn Create

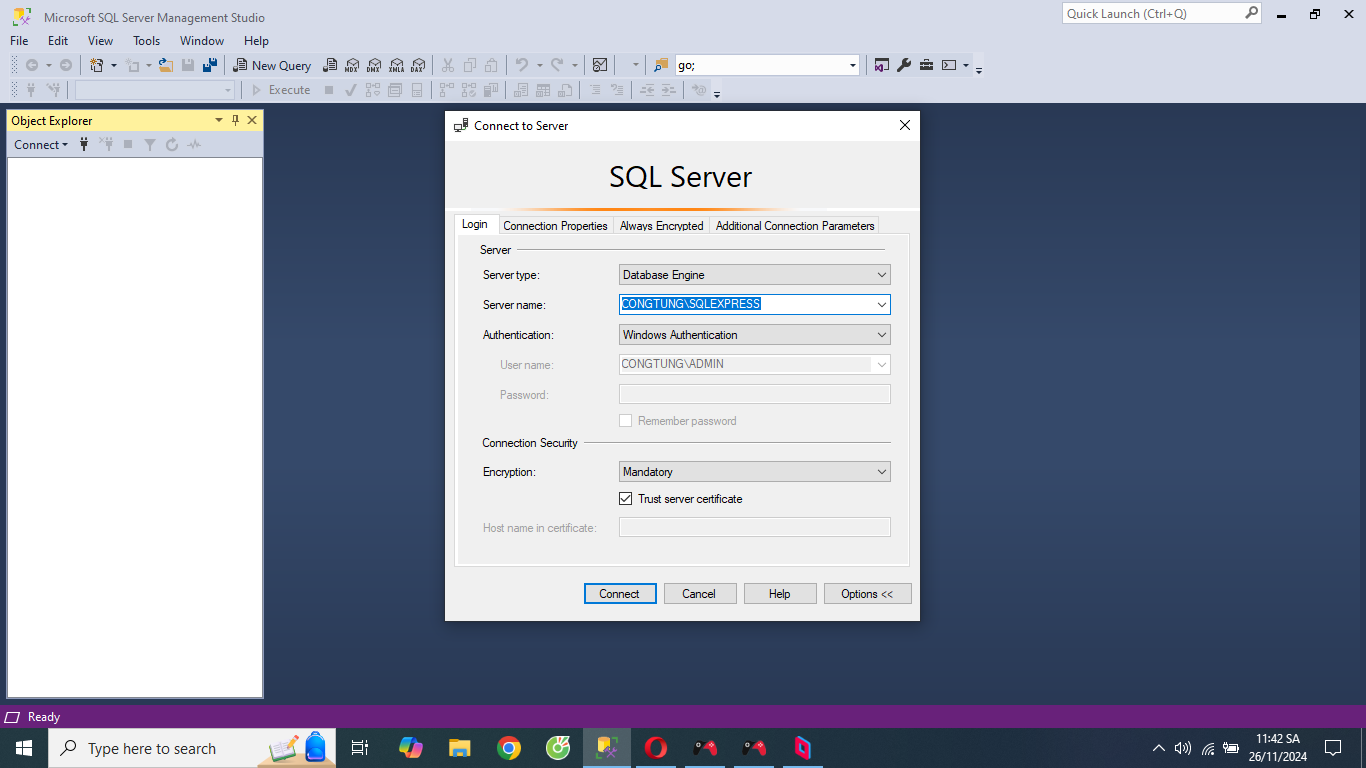


B3: Nhập các thông tin

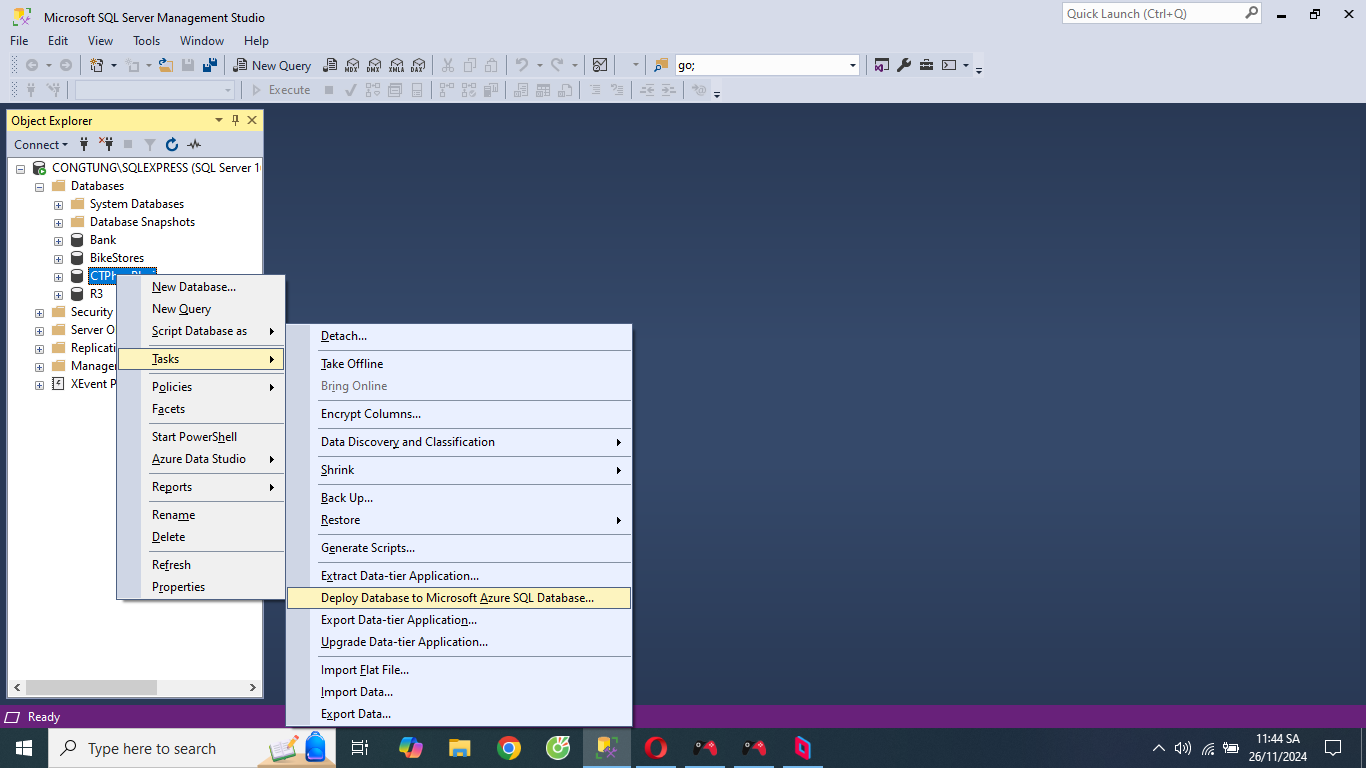


B4: Sau khi nhập xong chọn Review + Create

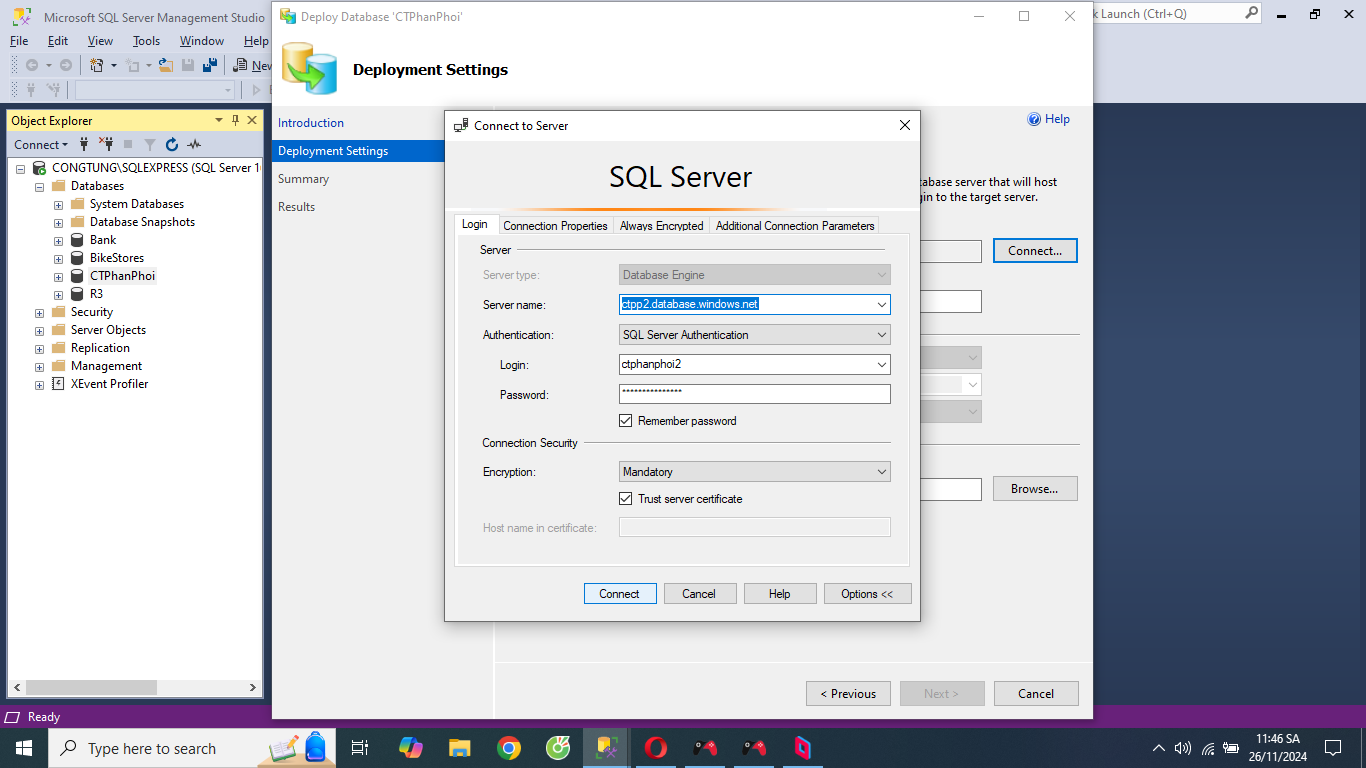
1. Vào SMSS



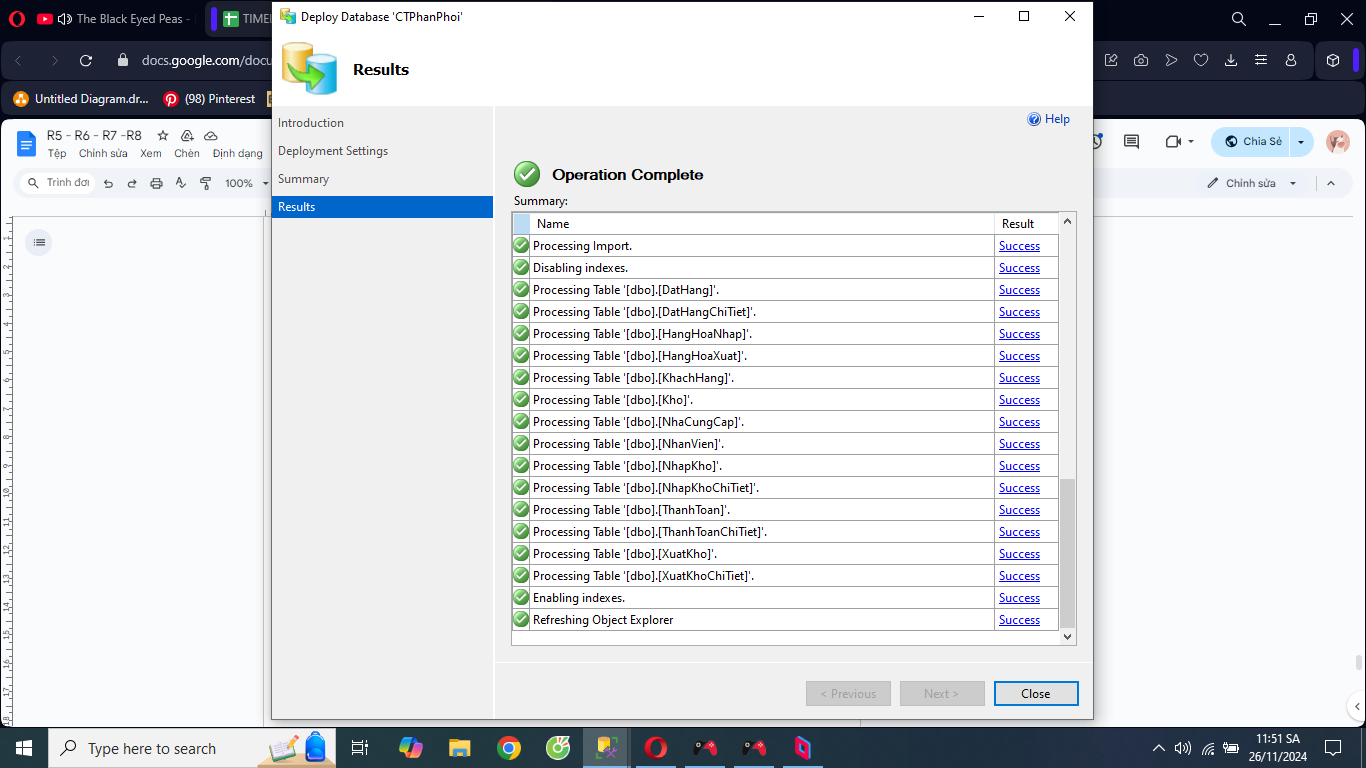
1. Chọn Database, vào task => chọn Deploy Database to Microsoft Azure SQL Database



1. Nhập thông tin Server và chọn Connect



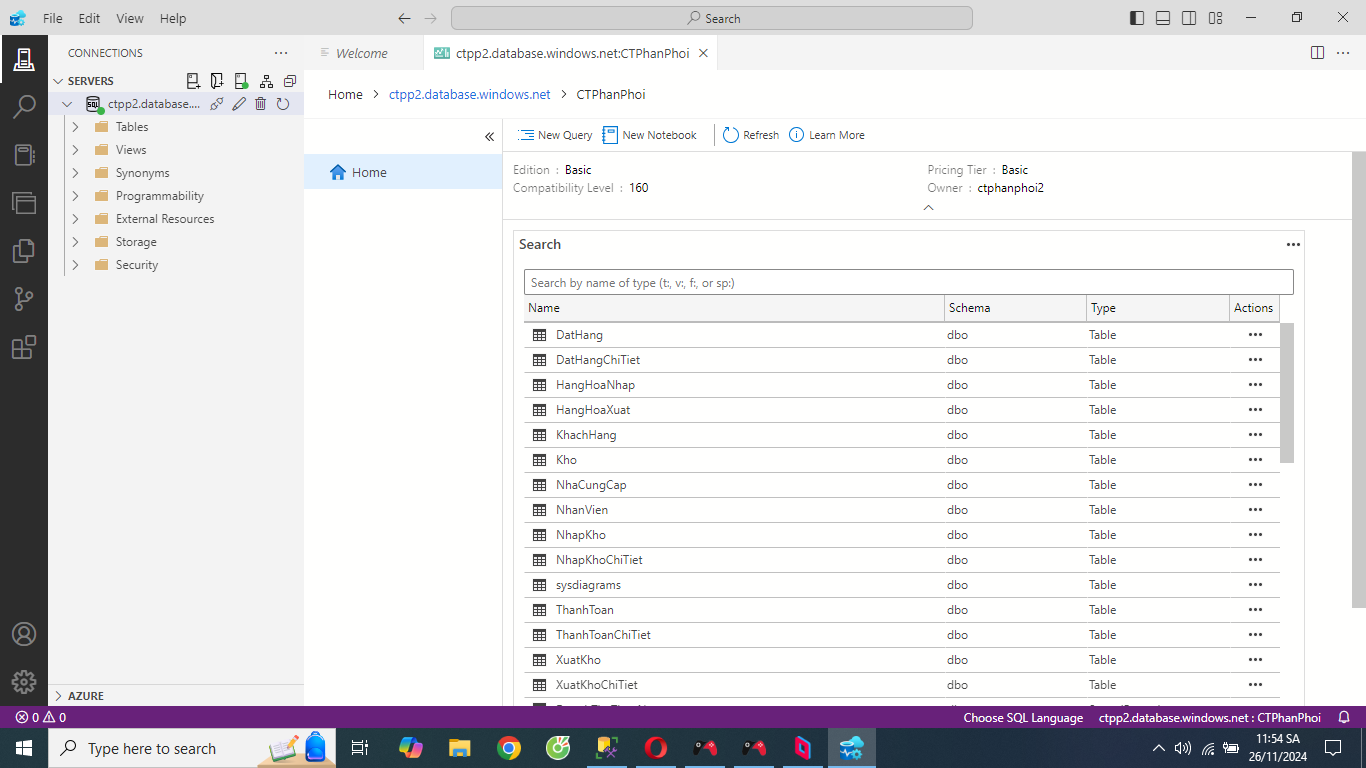
1. Đẩy dữ database thành công lên Azure Data Studio



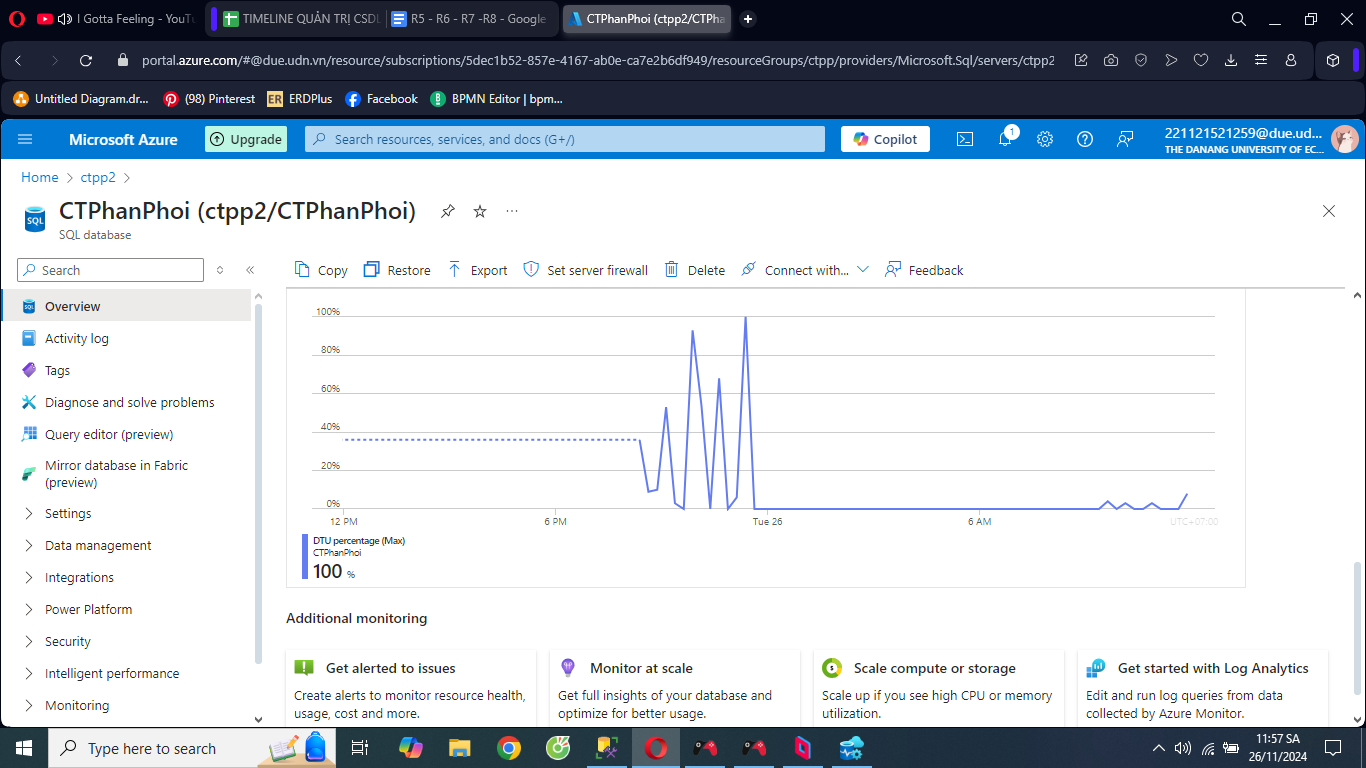
1. Mở Azure Data Studio, nhập thông tin Server rồi Connect



1. Thông tin Database được đẩy lên



1. Biểu đồ hoạt động của Database



1. **Nội dung R8:**

| **Tên cách phòng chống** | **Nội dung thực hiện** | **Kết quả thực hiện** |
| --- | --- | --- |
| 1. **Sử dụng Stored Procedures.** | Một Stored Procedure được tạo ra trước, do đó các giá trị đầu vào không làm thay đổi cấu trúc của câu lệnh SQL trong thủ tục. Điều này có nghĩa là nếu kẻ tấn công cố gắng chèn mã SQL độc hại vào đầu vào cho thủ tục, nó sẽ chỉ được coi là dữ liệu, không phải là mã SQL để thực thi. | [**R8.sql**](https://drive.google.com/file/d/1yuQrVU5zv5gxyfwJtDa4oXMCCCla5SMd/view?usp=sharing) |
| 1. **Tham số hóa truy vấn dữ liệu.** | Khi sử dụng tham số, giá trị đầu vào được xử lý như một dữ liệu và không ảnh hưởng đến quá trình phân tích cú pháp của câu lệnh. Điều này giúp ngăn chặn việc chèn mã SQL độc hại.  Tham số hóa truy vấn hiểu theo nghĩa Sql là việc gọi lại các biến, tham số đã có từ đó đảm bảo an toàn trong sql. |
| 1. **Xác thực và Kiểm soát đầu vào** | Bằng cách kiểm tra và giới hạn kích thước đầu vào, kiểu dữ liệu và định dạng, ngăn chặn việc chèn các ký tự đáng ngờ như dấu nháy đơn ('), dấu chấm phẩy (;), và các ký tự đặc biệt khác có thể được sử dụng trong các cuộc tấn công SQL Injection. |

**Tham khảo code R8:**

use CTPhanPhoi

**--R8: Thực hiện tạo bảng User và thiết lập kiểm tra đăng nhập với các phương pháp xác thực đầu vào dữ liệu, tham số hóa truy vấn sql và tạo thủ tục.**

**--B1: Tạo bảng lưu Users**

Create table Users(

id int IDENTITY(1,1) primary key,

username varchar(200) COLLATE SQL\_Latin1\_General\_CP1\_CS\_AS,

passwords varchar(200) COLLATE SQL\_Latin1\_General\_CP1\_CS\_AS

)

**--Tạo thủ tục inset dữ liệu**

Create proc InsertUsers( @i\_username VARCHAR(200),

@i\_password VARCHAR(200))

As

Begin

declare @ktra int

set @ktra = (Select Count(\*) from Users where username = @i\_username)

if @ktra > 0

begin

print 'Chen that bai'

return

end

Insert into Users(username,passwords)

values (@i\_username,@i\_password)

print 'Da chen'

end

--

Exec InsertUsers 'Thukho','Thuk0!2024$'

select \* from Users

**--B2: Tạo thủ tục, xác thực dữ liệu đầu vào và tham số hóa truy vấn dữ liệu.**

Create proc CheckLogins

@i\_username varchar(200),

@i\_password varchar(200),

@tbao varchar(200) output

As

Begin

***-- 1. Kiểm tra tên đăng nhập và mật khẩu không để trống.***

If @i\_username IS NULL OR @i\_username = ''

Begin

Set @tbao = N'Tên đăng nhập hoặc mật khẩu sai';

return;

end

If @i\_password IS NULL OR @i\_password = ''

Begin

set @tbao = N'Tên đăng nhập hoặc mật khẩu sai';

return;

end

***-- 2. Kiểm tra tên đăng nhập chỉ chứa chữ cái và số***

If PATINDEX('%[^a-zA-Z0-9\_]%', @i\_username) > 0

Begin

set @tbao = N'Tên đăng nhập hoặc mật khẩu sai.';

return;

end

***-- 3. Kiểm tra tên đăng nhập và mật khẩu***

Declare @ktra int;

Select @ktra = COUNT(\*)

from Users

where username = @i\_username AND passwords = @i\_password; -- Kiểm tra mật khẩu

If @ktra < 1

begin

SET @tbao = N'Tên đăng nhập hoặc mật khẩu sai.';

return;

end

-- Đăng nhập thành công

set @tbao = N'Đăng nhập thành công.';

end

***-- Gọi thủ tục lưu trữ***

Declare @tbao varchar(200)

Exec CheckLogins 'Thukho', 'Thuk0!2024$',@tbao =@tbao output

Print @tbao