**Xây dựng cơ chế bảo mật tương ứng cho CSDL**

1. Authentication (Xác thực):

Cơ chế xác thực trong SQL Server xác định và xác minh danh tính của người dùng khi họ cố gắng truy cập vào cơ sở dữ liệu. SQL Server hỗ trợ 5 phương thức xác thực thì nhóm sẽ lựa chọn SQL Server Authentication:

SQL Server Authentication: Sử dụng tên người dùng và mật khẩu đặt trước để xác thực. Thông tin đăng nhập được lưu trữ trong SQL Server và người dùng cung cấp tên người dùng và mật khẩu khi kết nối với cơ sở dữ liệu.

2. Authorization (Ủy quyền):

Cơ chế ủy quyền trong SQL Server quản lý quyền truy cập và phân quyền cho các đối tượng trong cơ sở dữ liệu. Mỗi người dùng hoặc vai trò được gán các quyền truy cập cụ thể để điều khiển việc thực hiện các hoạt động như đọc, ghi, chỉnh sửa hoặc xóa dữ liệu.

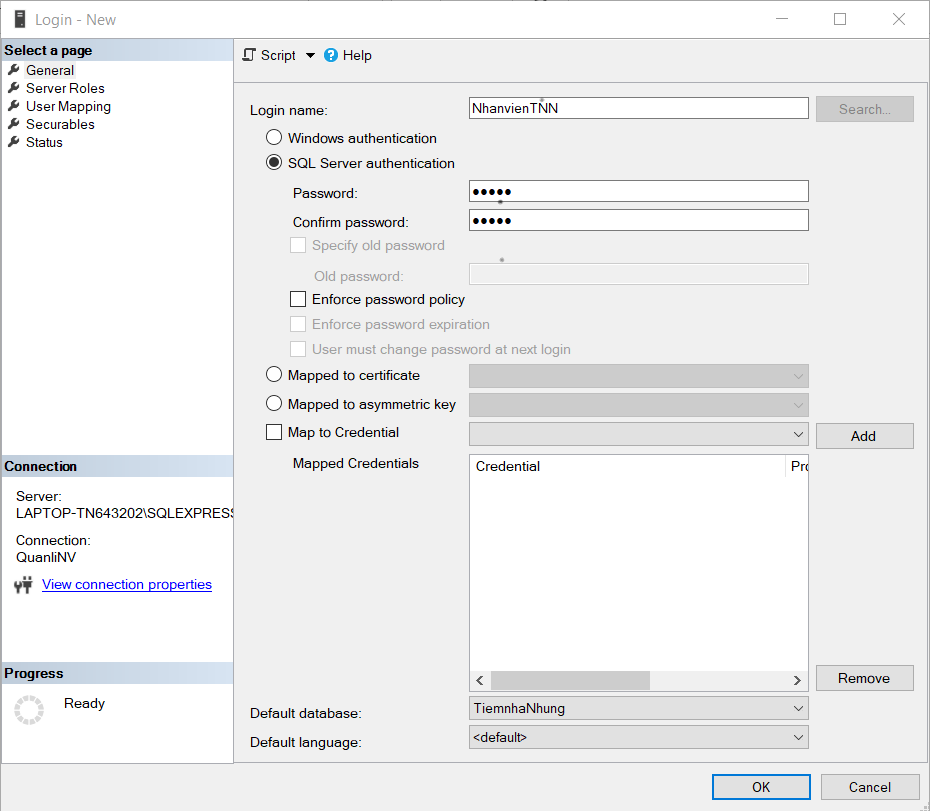
3. Always Encrypted (Mã hóa cột)

Giúp bảo vệ dữ liệu trong cơ sở dữ liệu khi dữ liệu trong bảng được truyền đi hoặc lưu trữ. Tính năng này sử dụng mã hóa mạnh mẽ để mã hóa dữ liệu nhạy cảm như số thẻ tín dụng, số CMND, mật khẩu, v.v.

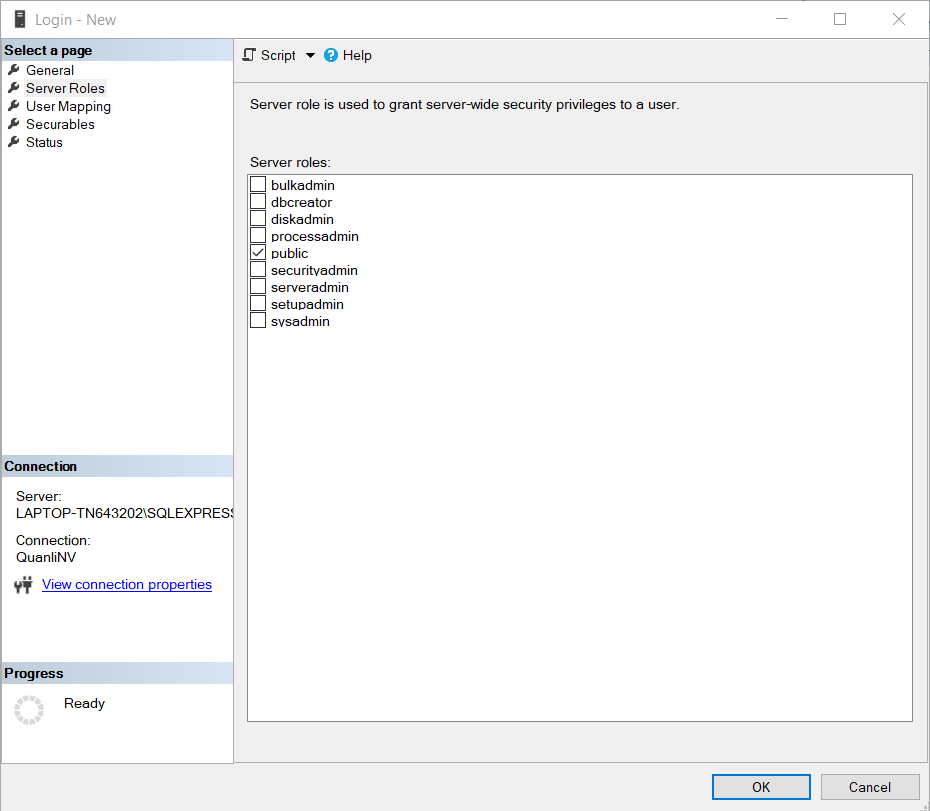
***Lý do lựa chọn bảo mật bằng 3 cơ chế:*** Dùng Authentication để đảm bảo rằng chỉ những người dùng hợp lệ mới có thể truy cập vào hệ thống. Sau đó việc áp dụng Authorization đảm bảo rằng chỉ những người dùng có đủ quyền hạn mới có thể thực hiện các hoạt động cần thiết và truy cập vào dữ liệu nhạy cảm và khi dữ liệu được mã hóa, ngay cả khi có kẻ tấn công truy cập trái phép vào cơ sở dữ liệu hoặc mạng, dữ liệu vẫn được bảo vệ và không thể đọc được. Nhóm lựa chọn bảo mật số điện thoại của khách hàng vì nó là một yếu tố quan trọng trong việc bảo vệ thông tin cá nhân và đảm bảo quyền riêng tư của khách hàng. Bằng cách kết hợp ba cơ chế này, hệ thống bảo mật trở nên mạnh mẽ và linh hoạt hơn.

**Triển khai cơ chế bảo mật cho CSDL**

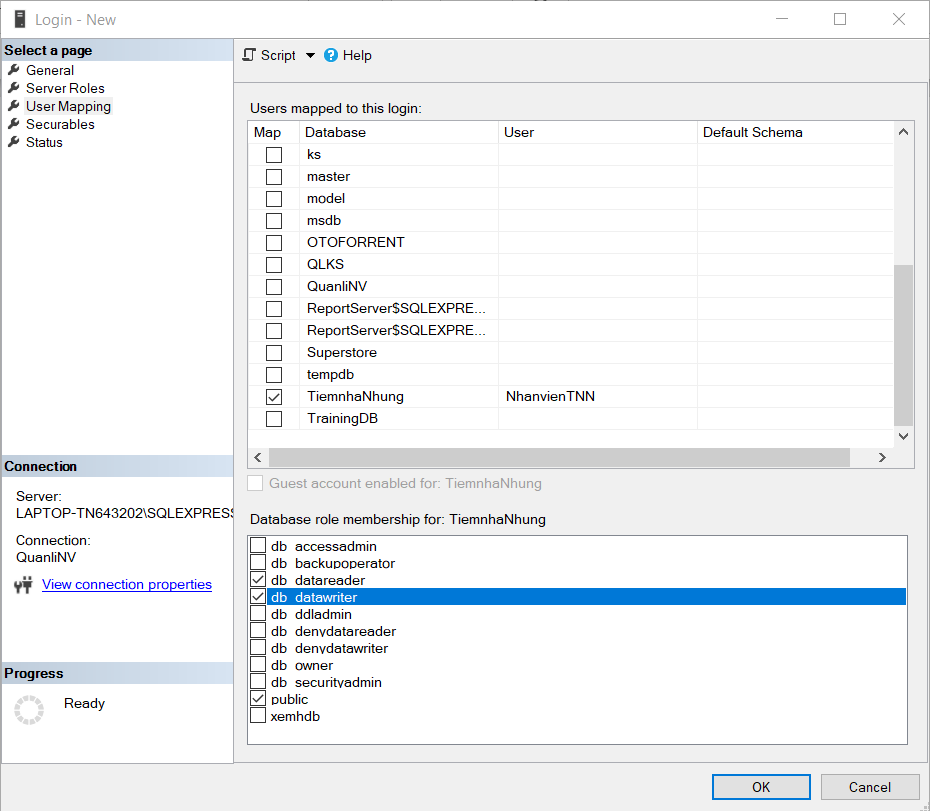
**1. Tạo tài khoản nhân viên**



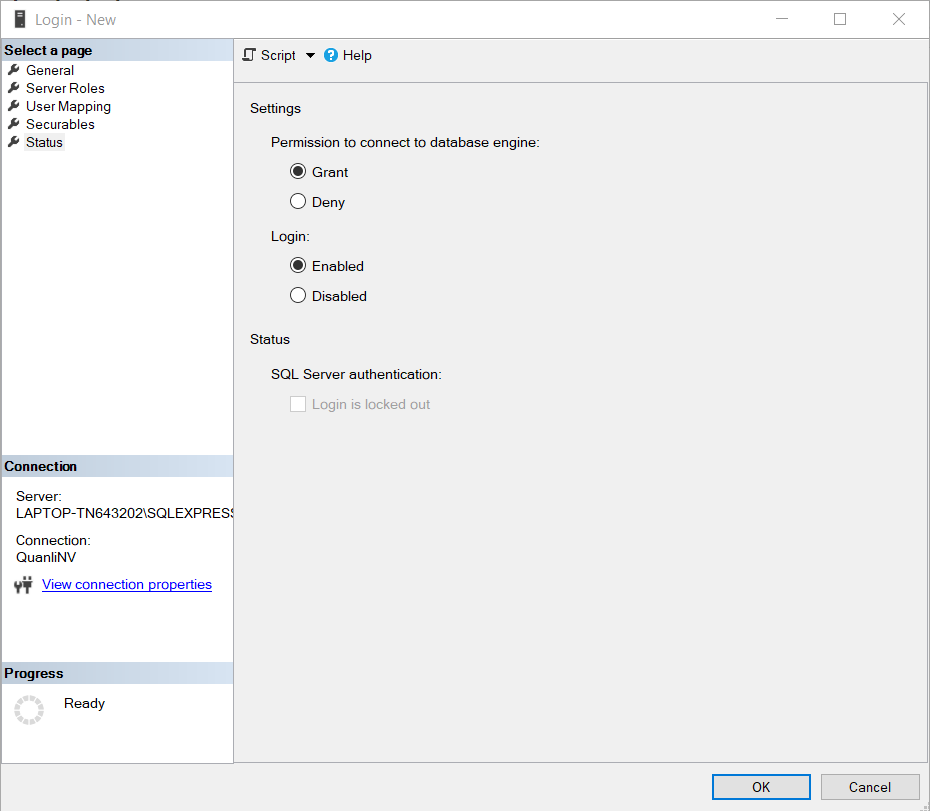
Đặt ít quyền nhất có thể cho mỗi người dùng.



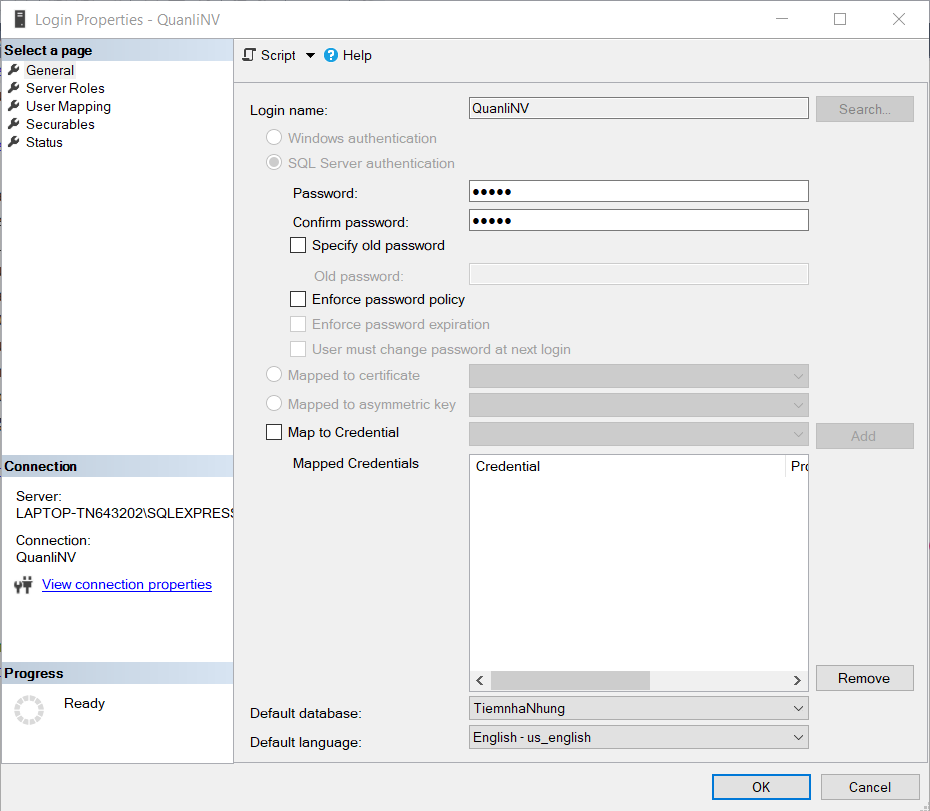
Chọn tên cơ sở dữ liệu mà người dùng sẽ làm việc và quyền của họ trên cơ sở dữ liệu.



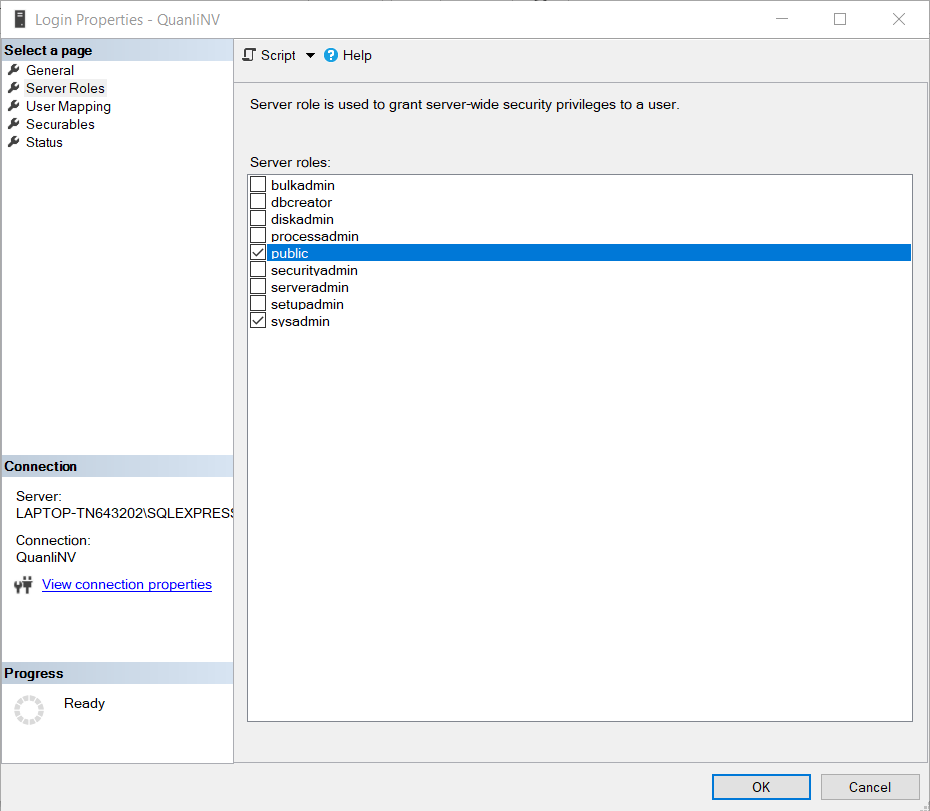
Thiết lập trạng thái



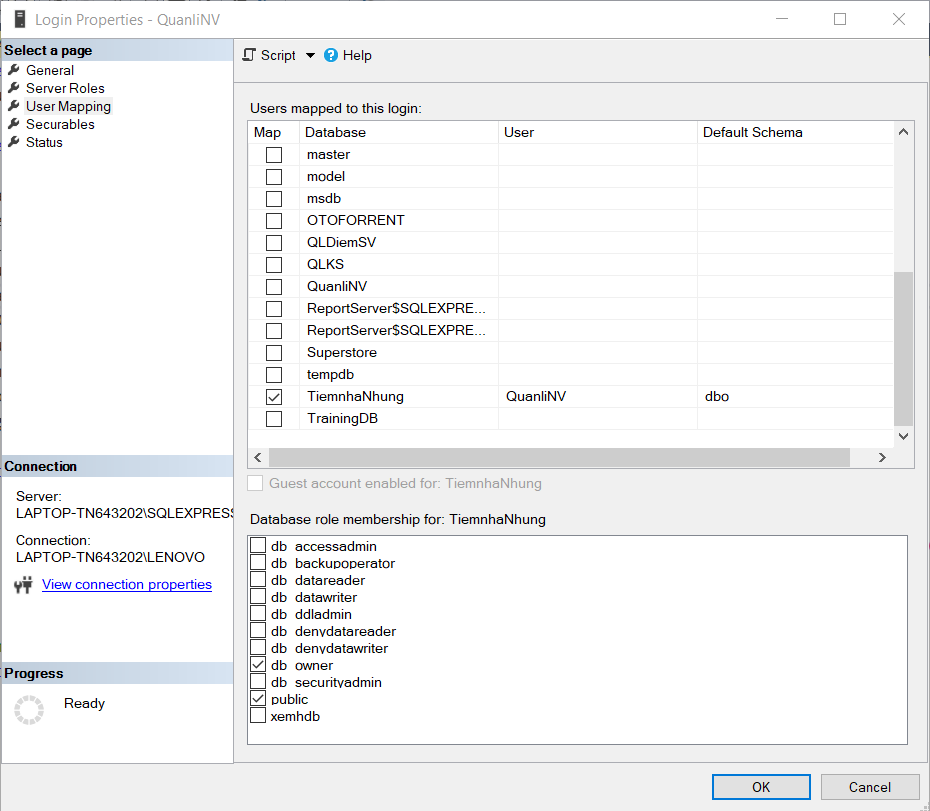
**2. Tạo tài khoản cho Quản lý**



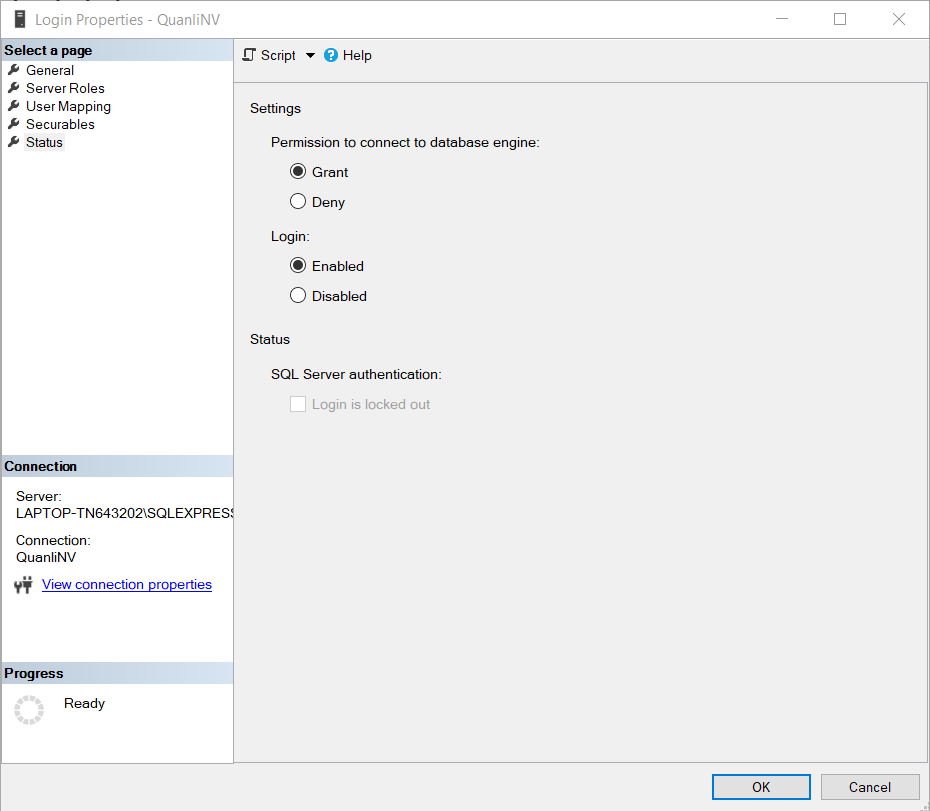
Đối với tài khoản của Quản lý thì chọn Sysadmin để có quyền truy cập và quản lý toàn bộ cơ sở dữ liệu và các thành phần của hệ thống.



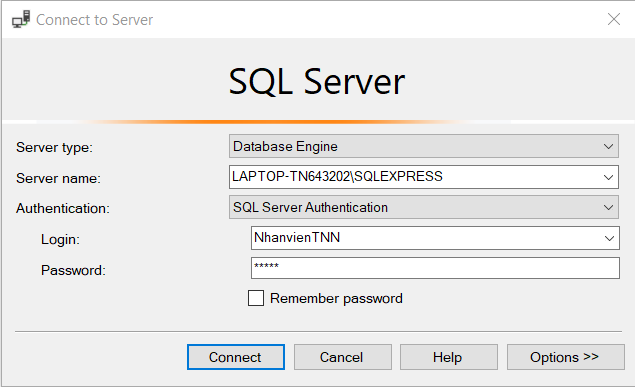
Tài khoản của Quản lý thì sẽ được cấp quyền truy cập vào CSDL của TiemNhaNhung và chọn owner có quyền truy cập, quản lý và thực thi các hoạt động.



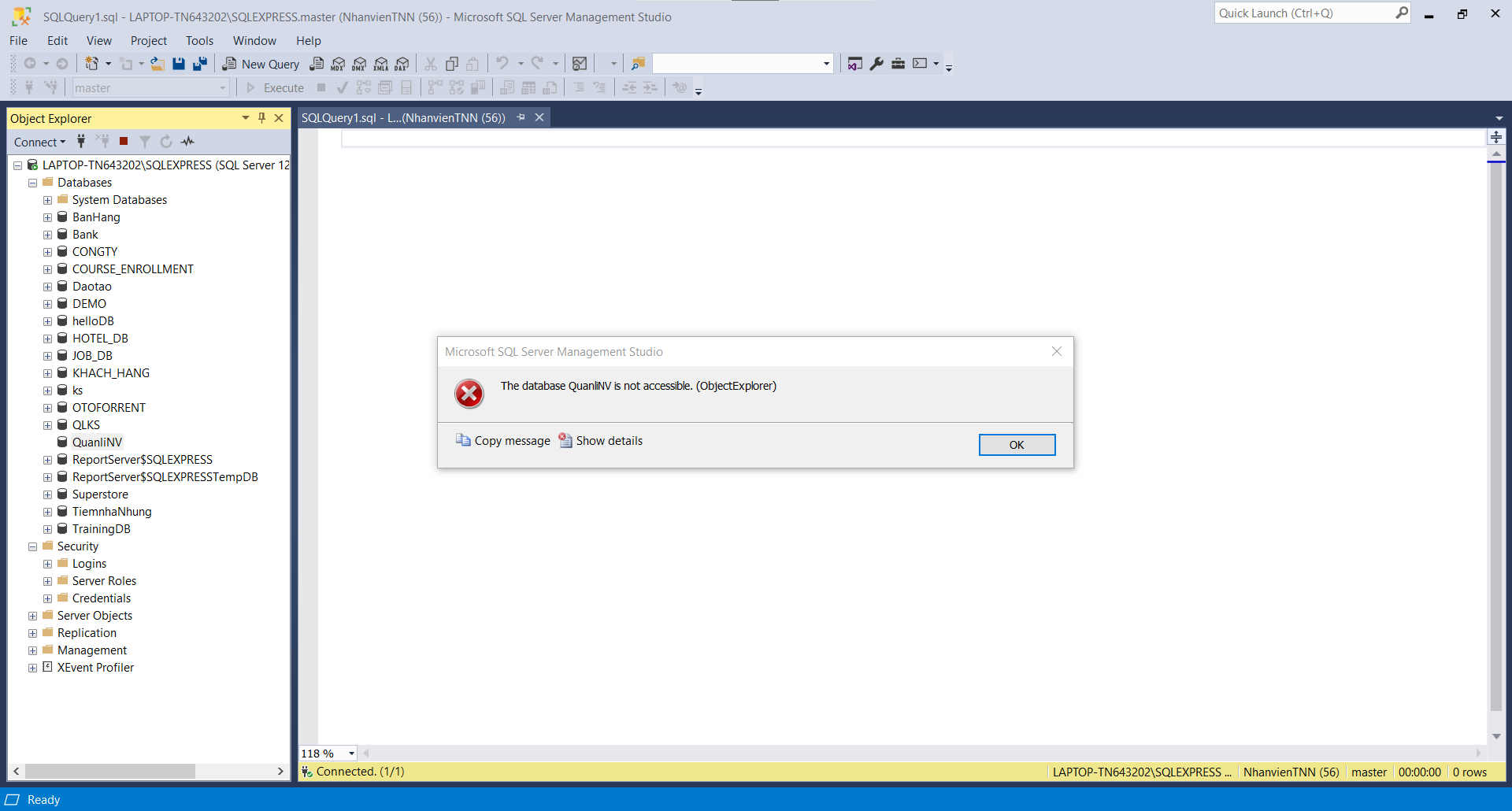
Thiết lập trạng thái



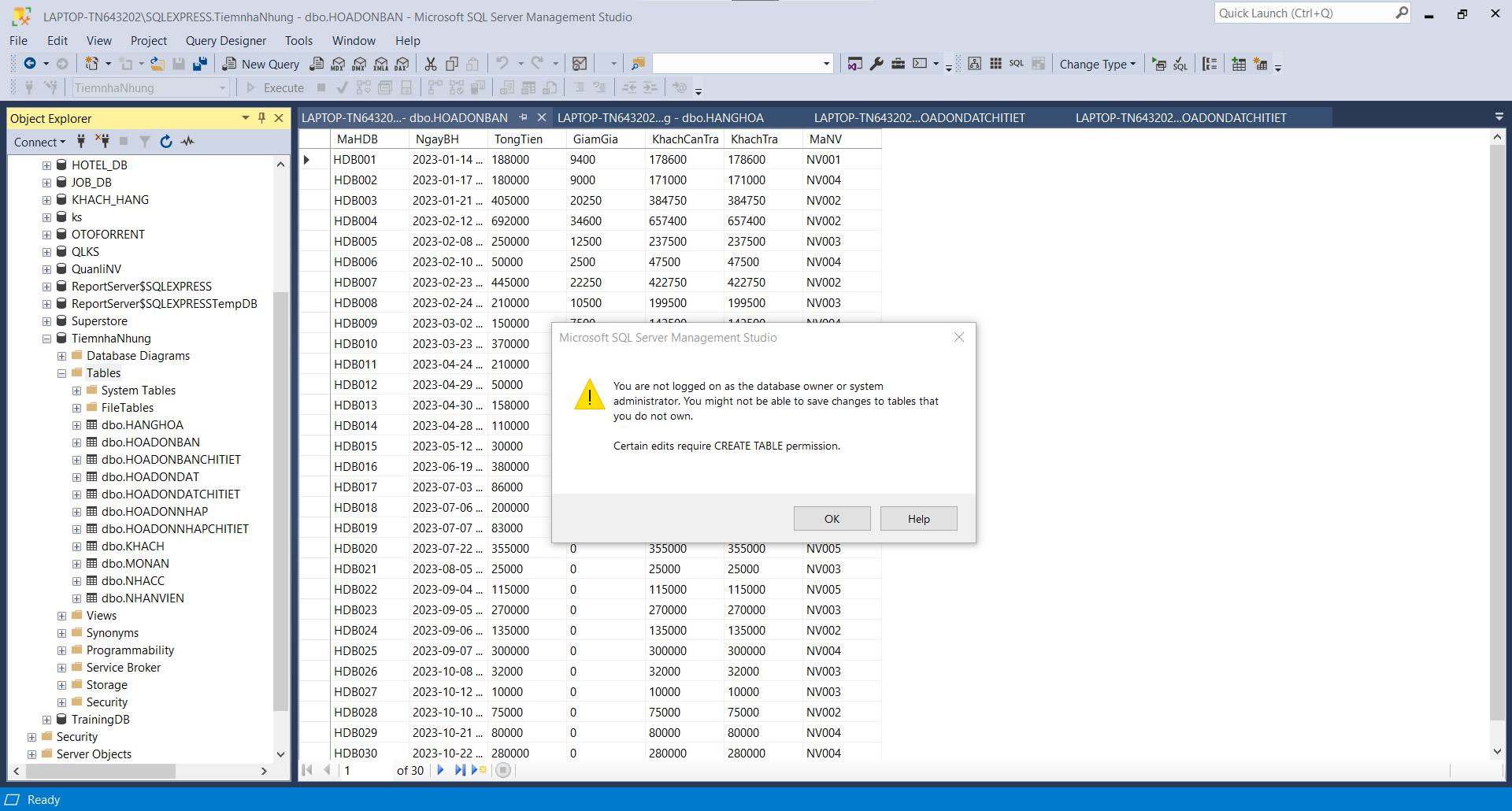
**3. Đăng nhập vào tài khoản Nhân viên**



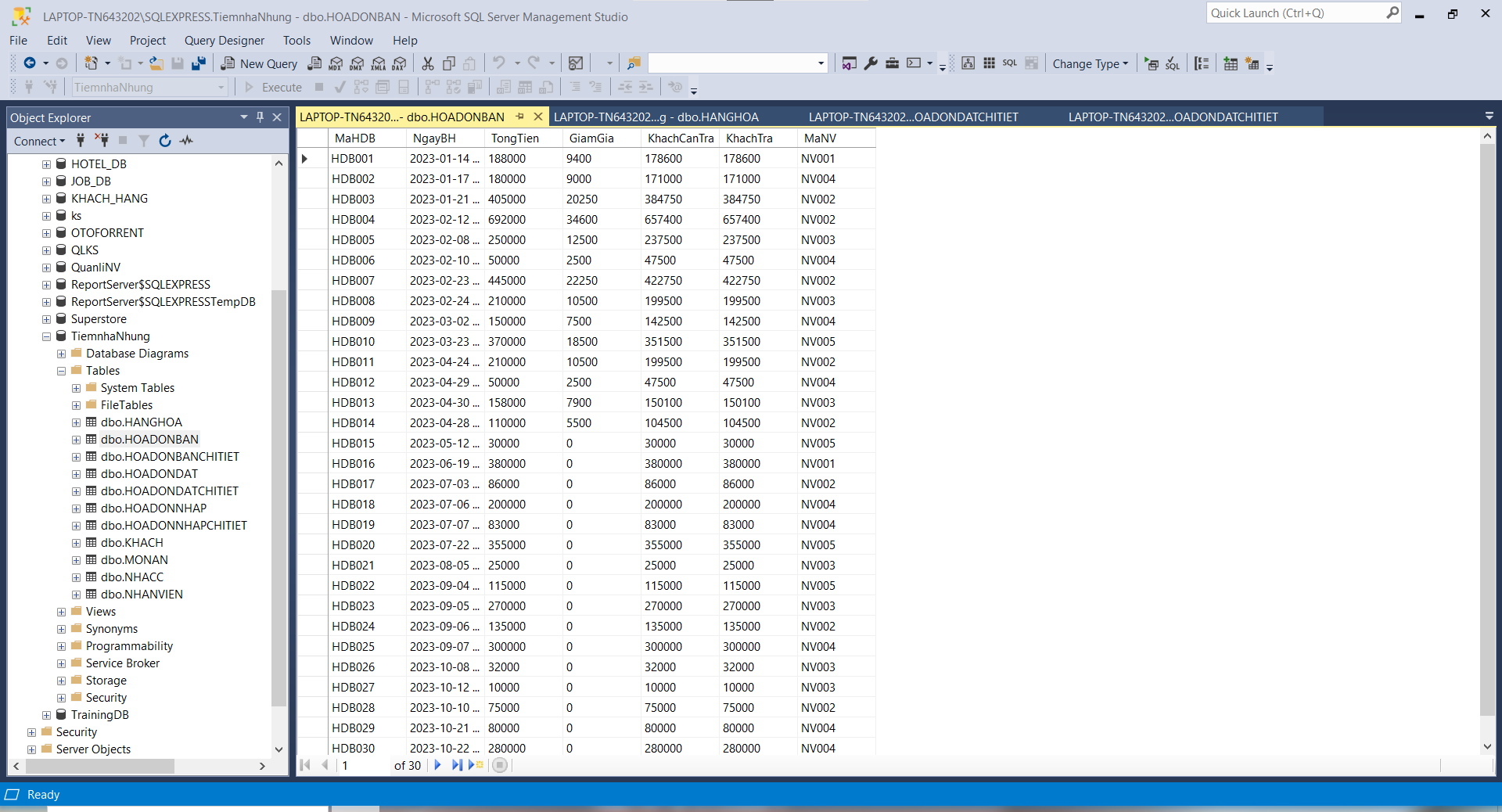
Tài khoản chỉ vào được duy nhất database TiemnhaNhung (được cấp quyền truy cập) và không truy cập được vào database khác

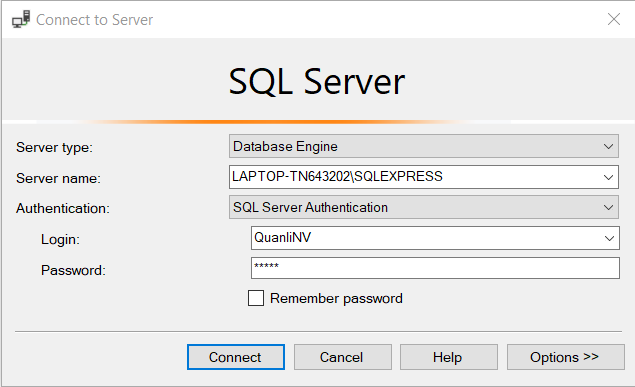


Tài khoản nhân viên không được quyền tạo thêm bảng

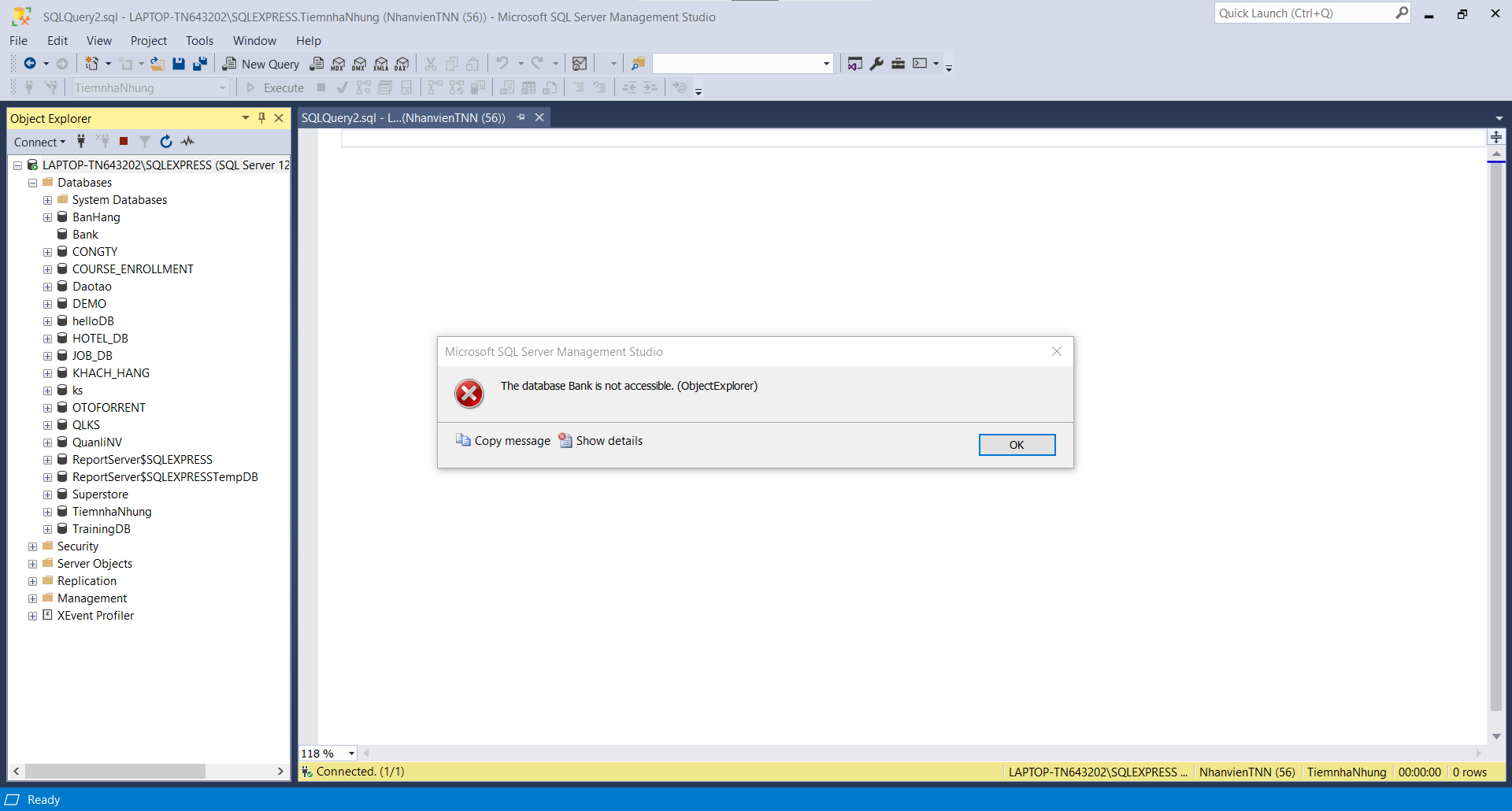


Nhưng thực hiện được quyền xem và sửa, thêm dữ liệu trong bảng

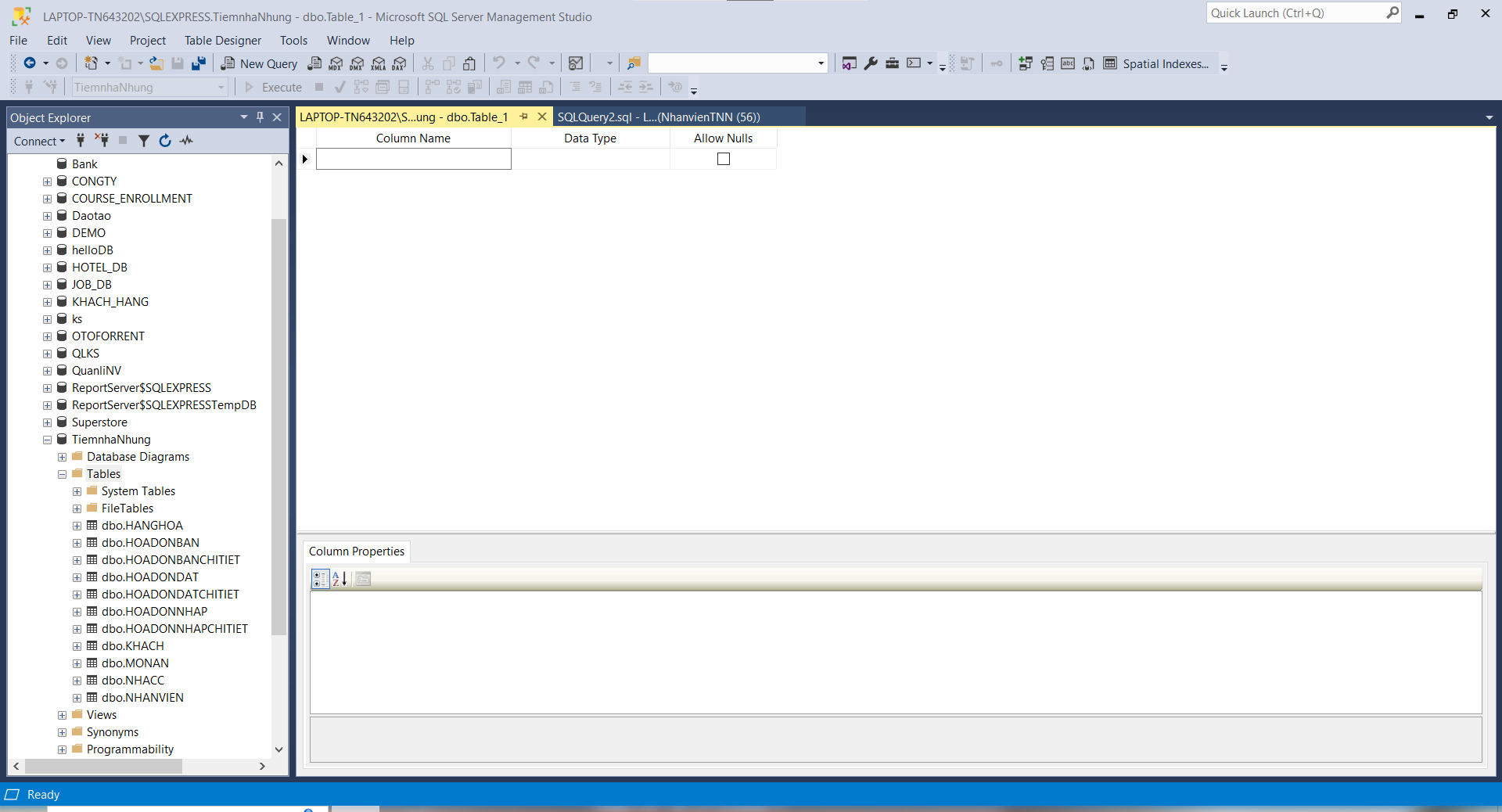
**4. 4. 4.Đăng nhập vào tài khoản Quản lý**

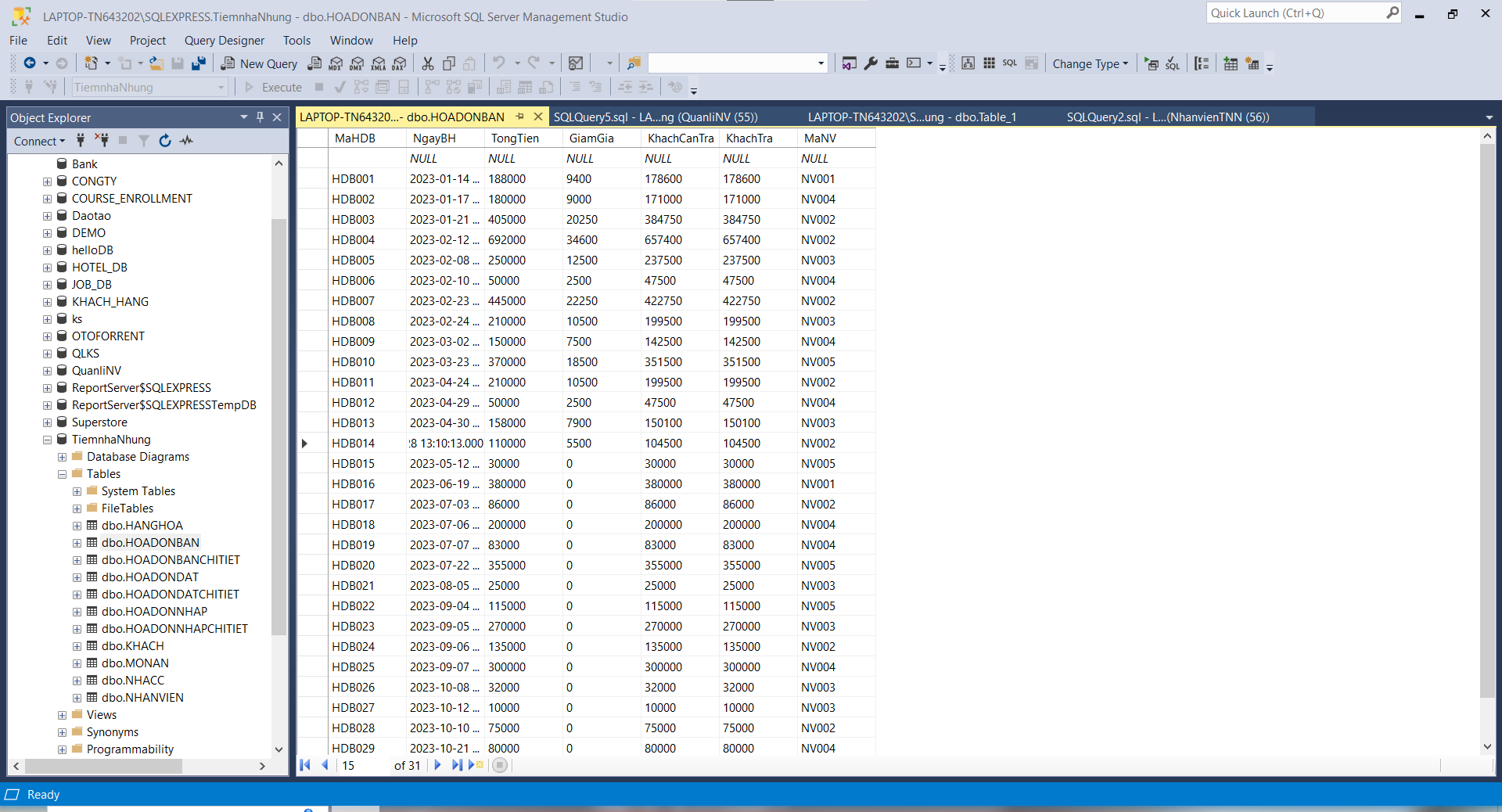


Tài khoản này cũng giống như tài khoản của nhân viên, chỉ có thể truy cập vào database đã được cấp phép là TiemnhaNhung và không vào được những database khác.



Đối với tài khoản của Quản lí thì được toàn quyền thao tác như thêm, sửa, xóa bản ghi, bảng,...





**5. Mã hóa cột SDTKH trong CSDL TiemNhaNhung**

