**HỆ THỐNG TÍNH CÔNG + LƯƠNG CHO NHÂN VIÊN**

**1. Yêu cầu cơ bản**

**R1(1đ).** Mỗi nhóm sưu tầm tất cả loại hóa đơn, chứng từ tại một cơ sở kinh doanh/sản xuất nhỏ. file excel tính công, lương

**R2(1.5đ).** Thiết kế cơ sở dữ liệu ở mức khái niệm, logic và một phần cơ bản của thiết kế vật lý (sẽ hướng dẫn và trao đổi cụ thể trên lớp).

* Thiết kế cơ sở dữ liệu ở mức khái niệm:



* Xây dựng ER cho bảng tổng hợp công (ER-1)

B1: chọn lọc thông tin

| Từ trong HSDL | Từ rõ nghĩa | Viết tắt |
| --- | --- | --- |
| Mã | Mã bảng công | MaBC |
| Mã NV | Mã nhân viên | MaNV |
| Tên NV | Tên nhân viên | TenNV |
| Ngày tổng hợp | Ngày tổng hợp bảng công | NgayTH |
| Ngày công | Ngày công trong tháng | NgayCong |
| Giờ làm | Số giờ nhân viên đã làm trong ngày công | SoGio |
| Tổng công | Tổng công của một tháng | TongCong |

**B2: Xác định thực thể, thuộc tính**

NHANVIEN(**MaNV**, TenNV,SDT)

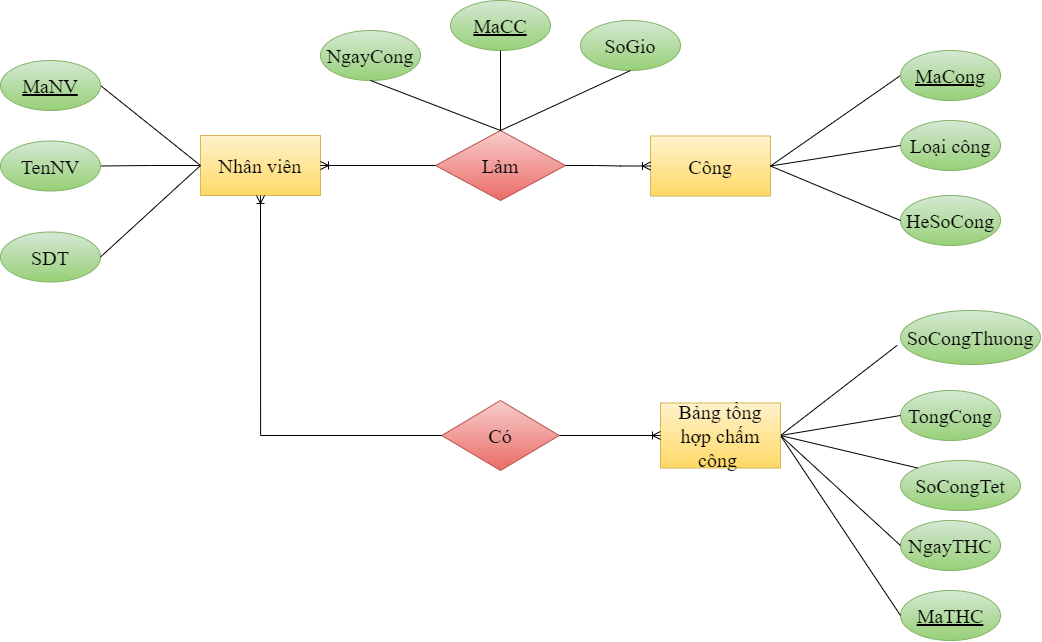
CONG(**MaCong**, LoaiCong, DonViCong)

BANGTHCC(**MaTHC**,NgayTHC,SoCongThuong,SoCongTet,TongCong)

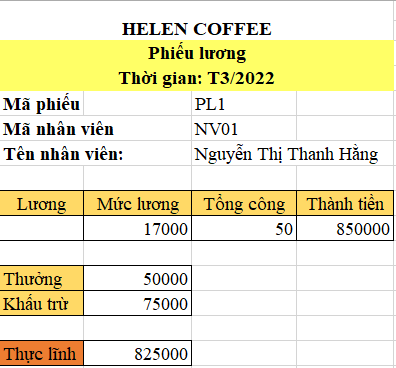
**B3: Xác định quan hệ**

LAM(TongCong, MaBC, NgayTHBC)

**B4: Vẽ**



* Xây dựng ER cho phiếu lương (ER-2)



Bước 1: Chọn lọc thông tin:

| Từ trong HSDL | Từ rõ nghĩa | Viết tắt |
| --- | --- | --- |
| Mã phiếu | Mã số phiếu lương | MaPL |
| Thời gian | Tháng, năm tính lương | ThoiGian |
| Mã nhân viên | Mã số nhân viên | MaNV |
| Tên nhân viên | Họ tên nhân viên | TenNV |
| Lương | Lương | Luong |
| Mức lương | Mức lương trong 1 giờ | MucLuong |
| Tổng công | Tổng số công làm 1 tháng | TongCong |
| Thành tiền | Thành tiền | ThanhTien |
| Thưởng | Số tiền thưởng | Thuong |
| Khấu trừ | Khấu trừ | KhauTru |
| Thực lĩnh | Số tiền thực lĩnh | ThucLinh |

**B2: Xác định thực thể, thuộc tính:**

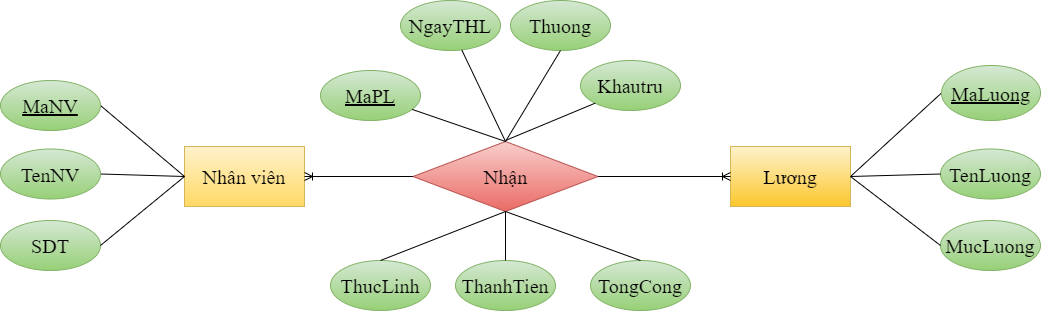
NHANVIEN (**MaNV**, TenNV, SDT)

LUONG (**MaLuong**, TenLuong, MucLuong)

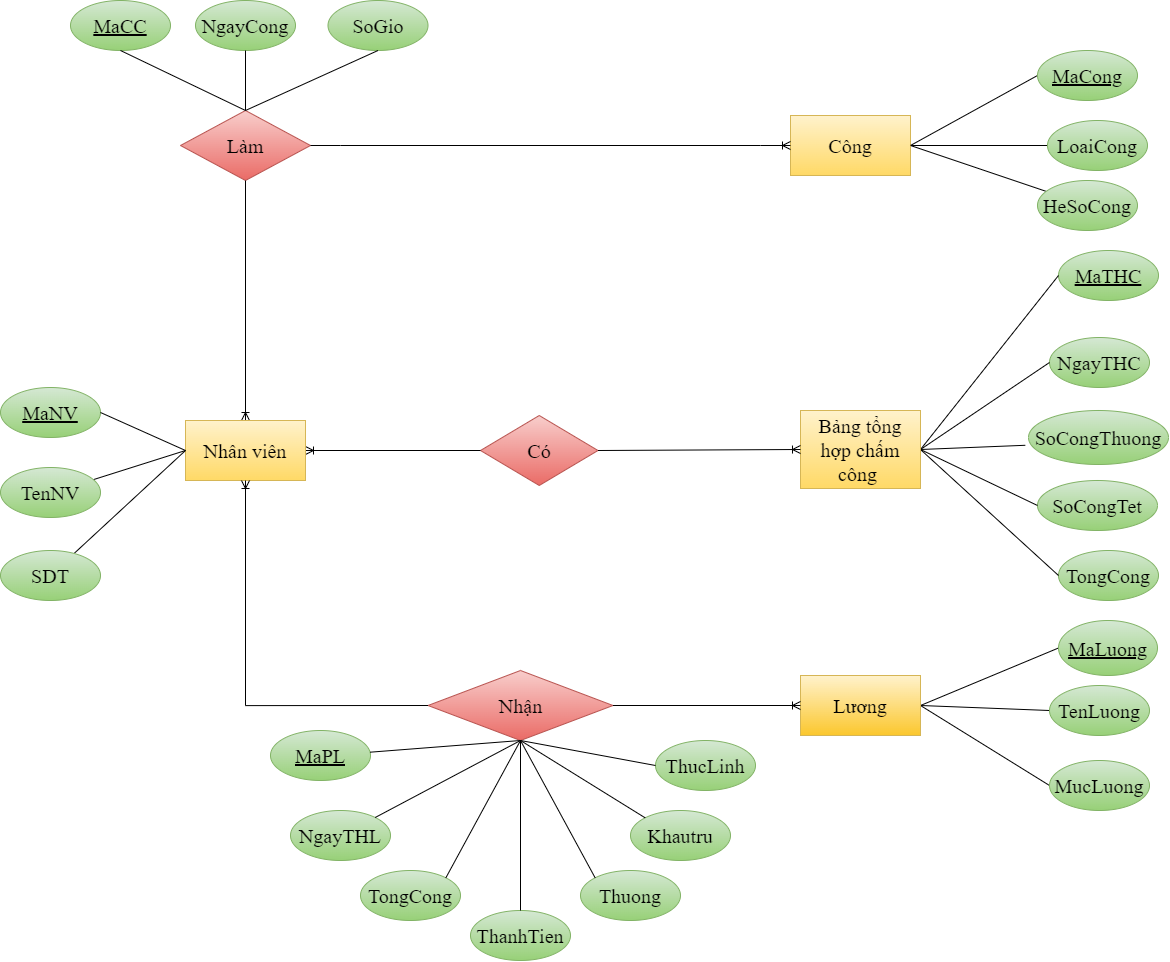
**B3: Xác định quan hệ**

NHAN(MaPL, NgayTHL, TongCong, ThanhTien, Thuong, KhauTru, ThucLinh)

**B4: Vẽ**



TÍCH HỢP ER-1 VỚI ER-2



* Thiết kế cơ sở dữ liệu ở mức Logic:

**B1: Chuyển thực thể, thu được:**

NHANVIEN(MaNV, TenNV, SDT, MaLuong)

CONG(MaCong, LoaiCong, HeSoCong)  
 LUONG(MaLuong, TenLuong, MucLuong)

BANGTHCC(MaTHC, NgayTHC, SoCongThuong, SoCongTet, TongCong)

**B2: Chuyển quan hệ, thu được:**

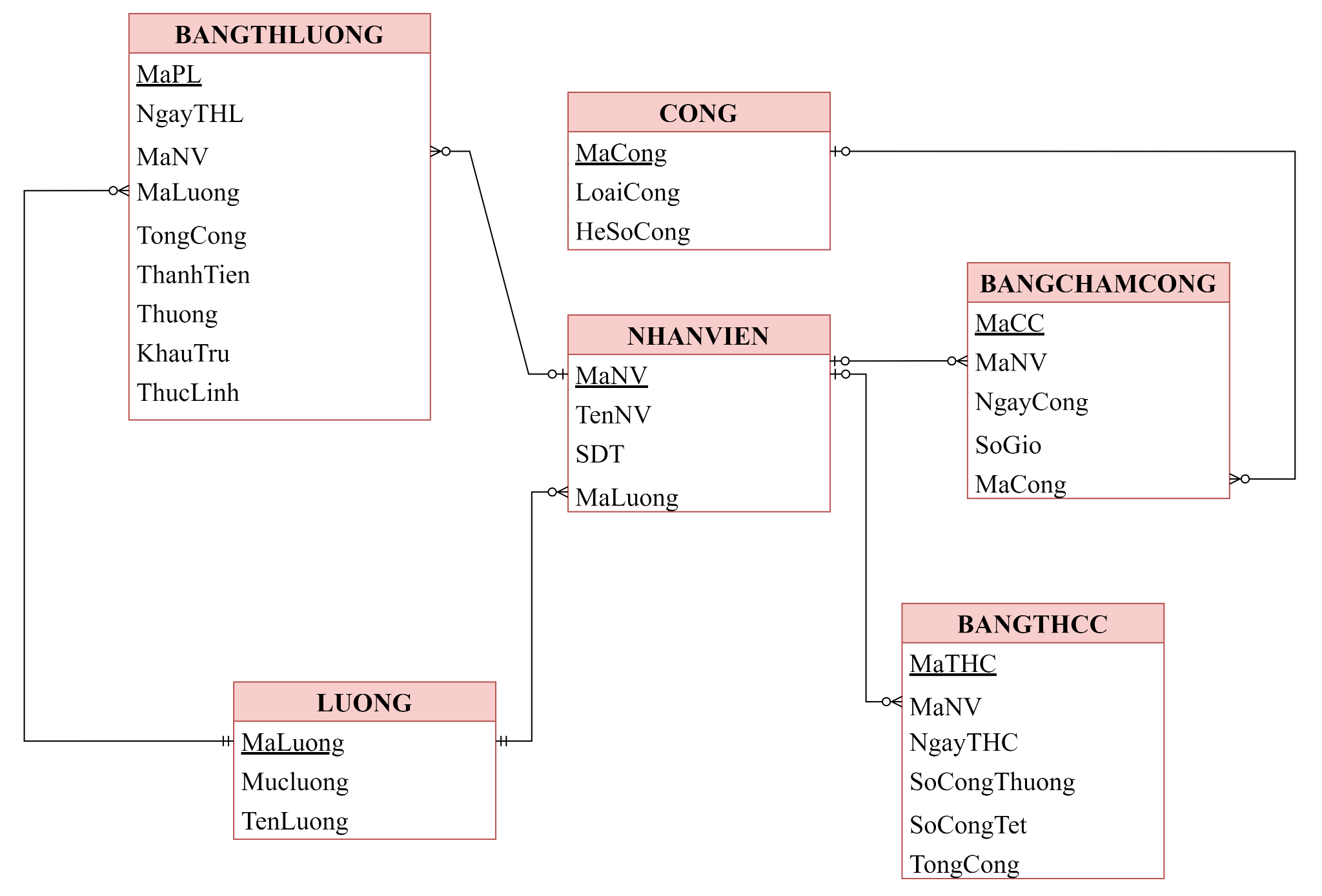
Quan hệ LÀM => BANGCHAMCONG(MaCC, MaNV, NgayCong, SoGio, MaCong)

Quan hệ NHẬN => BANGTHLUONG(MaPL, NgayTHL ,MaNV, MaLuong, TongCong, ThanhTien, Thuong, KhauTru, ThucLinh)

**B3: Chuẩn hóa**

Các quan hệ đã ở dạng 3NF

**B4: Vẽ sơ đồ quan hệ**



* Thiết kế vật lý:

Bảng NHANVIEN

| Thuộc tính | Diễn giải | Kiểu | Độ rộng | Định dạng | Ràng buộc |
| --- | --- | --- | --- | --- | --- |
| MaNV | Mã nhân viên | VARCHAR | 4 | NVxx | Khóa chính |
| TenNV | Họ tên nhân viên | NVARCHAR | 100 | Text | Not Null |
| SDT | Số điện thoại | CHAR | 10 |  | Unique |
| MaLuong | Mã lương | VARCHAR | 3 | Lxx | Khóa ngoại đến bảng LUONG |

Bảng CONG

| Thuộc tính | Diễn giải | Kiểu | Độ rộng | Định dạng | Ràng buộc |
| --- | --- | --- | --- | --- | --- |
| MaCong | Mã công | VARCHAR | 3 | MCx | Khóa chính |
| LoaiCong | Loại công | NVARCHAR | 50 |  |  |
| HeSoCong | Hệ số công | INT |  |  |  |

Bảng LUONG

| Thuộc tính | Diễn giải | Kiểu | Độ rộng | Định dạng | Ràng buộc |
| --- | --- | --- | --- | --- | --- |
| MaLuong | Mã lương | VARCHAR | 3 | Lxx | Khóa chính |
| TenLuong | Tên lương | NVARCHAR | 20 |  |  |
| MucLuong | Mức lương | NUMERIC |  |  |  |

Bảng BANGCHAMCONG

| Thuộc tính | Diễn giải | Kiểu | Độ rộng | Định dạng | Ràng buộc |
| --- | --- | --- | --- | --- | --- |
| MaCC | Mã chấm công | VARCHAR | 10 | CCxxxx\_xxx | Khóa chính |
| MaNV | Mã nhân viên | VARCHAR | 4 | NVxx | Khóa ngoại đến bảng NHANVIEN |
| NgayCong | Ngày công | DATE |  |  |  |
| SoGio | Số giờ làm | INT |  |  |  |
| MaCong | Mã công | VARCHAR | 3 |  | Khóa ngoại đến bảng CONG |

Bảng BANGTHCC

| Thuộc tính | Diễn giải | Kiểu | Độ rộng | Định dạng | Ràng buộc |
| --- | --- | --- | --- | --- | --- |
| MaTHC | Mã tổng hợp công | VARCHAR | 10 | THCxxxx\_xx | Khóa chính |
| NgayTHC | Ngày tổng hợp công | DATE |  |  |  |
| MaNV | Mã nhân viên | VARCHAR | 4 |  | Khóa ngoại đến bảng NHANVIEN |
| SoCongThuong | Số công thường | INT |  |  |  |
| SoCongTet | Số công tết | INT |  |  |  |
| TongCong | Tổng công | INT |  |  |  |

Bang BANGTHLUONG

| MaPL | Mã phiếu lương | VARCHAR | 9 | PLxxxx\_xx | Khóa ngoại đến bảng BANGTHLUONG |
| --- | --- | --- | --- | --- | --- |
| NgayTHL | Ngày tổng hợp lương | DATE |  |  |  |
| MaNV | Mã nhân viên | VARCHAR | 4 |  |  |
| MaLuong | Mã lương | VARCHAR | 3 | Lxx |  |
| TongCong | Tổng công | INT |  |  |  |
| ThanhTien | Thành tiền | NUMERIC |  |  |  |
| Thuong | Thưởng | NUMERIC |  |  |  |
| KhauTru | Khấu trừ | NUMERIC |  |  |  |
| ThucLinh | Thực lĩnh | NUMERIC |  |  |  |

**R3(0.5đ).** Xây dựng cơ sở dữ liệu cho bản thiết kế ở bước R2.

**R4(1đ).** Xác định và tạo các index cho các thuộc tính cần thiết.

(Hãy giải thích vì sao lại đưa ra lựa chọn như vậy)

-- Thêm Clustered Index: mỗi bảng chỉ có 1 Clustered Index và Đã cài mặc định theo Primary Key của bảng

-- Thêm Non-Clustered Index

**Đã có:**

* Bảng NHANVIEN có cột SDT char(10) unique: một non-clustered index đã được tạo mặc định trên cột SDT

**Quyết định:** KHÔNG tạo thêm Non-Clustered Index nào, vì:

* Các bảng dữ liệu nhỏ (CÔNG, LƯƠNG, NHANVIEN) ít bảng ghi nên không cần thiết

Ví dụ: Cột TenNV trong bảng NHANVIEN: số lượng bảng ghi tối đa không quá 50, vì đơn vị kinh doanh nhỏ, số lượng nhân viên không nhiều nên tạo Non-Clustered Index không đem lại lợi ích trong trường hợp này

* Các bảng dữ liệu lớn hơn (BANGCHAMCONG, BANGTHCC, BANGTHLUONG) thường xuyên insert, update thì không nên xài

Ví dụ: Cột NgayCong trong bảng BANGCHAMCONG: thường xuyên thêm mới vào, nếu thêm Non-Clustered Index sẽ dễ ảnh hưởng đến tốc độ thêm mới.

**R5(1đ).** Xây dựng cơ chế bảo mật tương ứng cho CSDL vừa tạo. (Giải thích ngắn gọn lý do lựa chọn giải pháp và triển khai giải pháp cho CSDL của nhóm)

* tạo login cho 2 đối tượng: quản lý, nhân viên
* **quản lý có thể update, insert, delete, select**

create login QUANLY with password = ‘quanly123’

create user quanly for login QUANLY

grant select, insert, update on database::QLNV\_HELEN to quanly;

* **nhân viên có thể select**

create login NHANVIEN with password = ‘nhanvien123’

create user nhanvien for login NHANVIEN

grant select on table: BANGCHAMCONG to nhanvien

* **Bảo mật BANGTHLUONG (mã hóa cột thưởng + thực lĩnh)**
* ***Thêm cột mới vào bảng BANGTHLUONG để lưu dữ liệu mã hóa***

alter table BANGTHLUONG

add EncryptedThuong varbinary(max),

EncryptedThucLinh varbinary(max);

* ***Mã hóa các cột***

update BANGTHLUONG

set EncryptedThuong = encryptbypassphrase('pass mã hóa', convert(varchar(max), Thuong)),

EncryptedThucLinh = encryptbypassphrase('pass mã hóa', covert(varchar(max), ThucLinh));

* ***xóa các cột dữ liệu gốc trong BANGTHLUONG***

alter table BANGTHLUONG

drop column Thuong,

drop column ThucLinh;

* ***truy vấn dữ liệu (giải mã để xem được dữ liệu gốc)***

select

MaPL, NgayTHL, MaNV, MaLuong,

convert(numeric, decryptbypassphrase('pass mã hóa', EncryptedThuong)) as Thuong,

convert(numeric, decryptbypassphrase('pass mã hóa', EncryptedThucLinh)) as ThucLinh

from BANGTHLUONG;

**R6(1đ).** Xây dựng cơ chế backup dữ liệu phù hợp cho CSDL vừa tạo

Cơ chế Backup: backup là làm chậm toàn bộ hệ thống

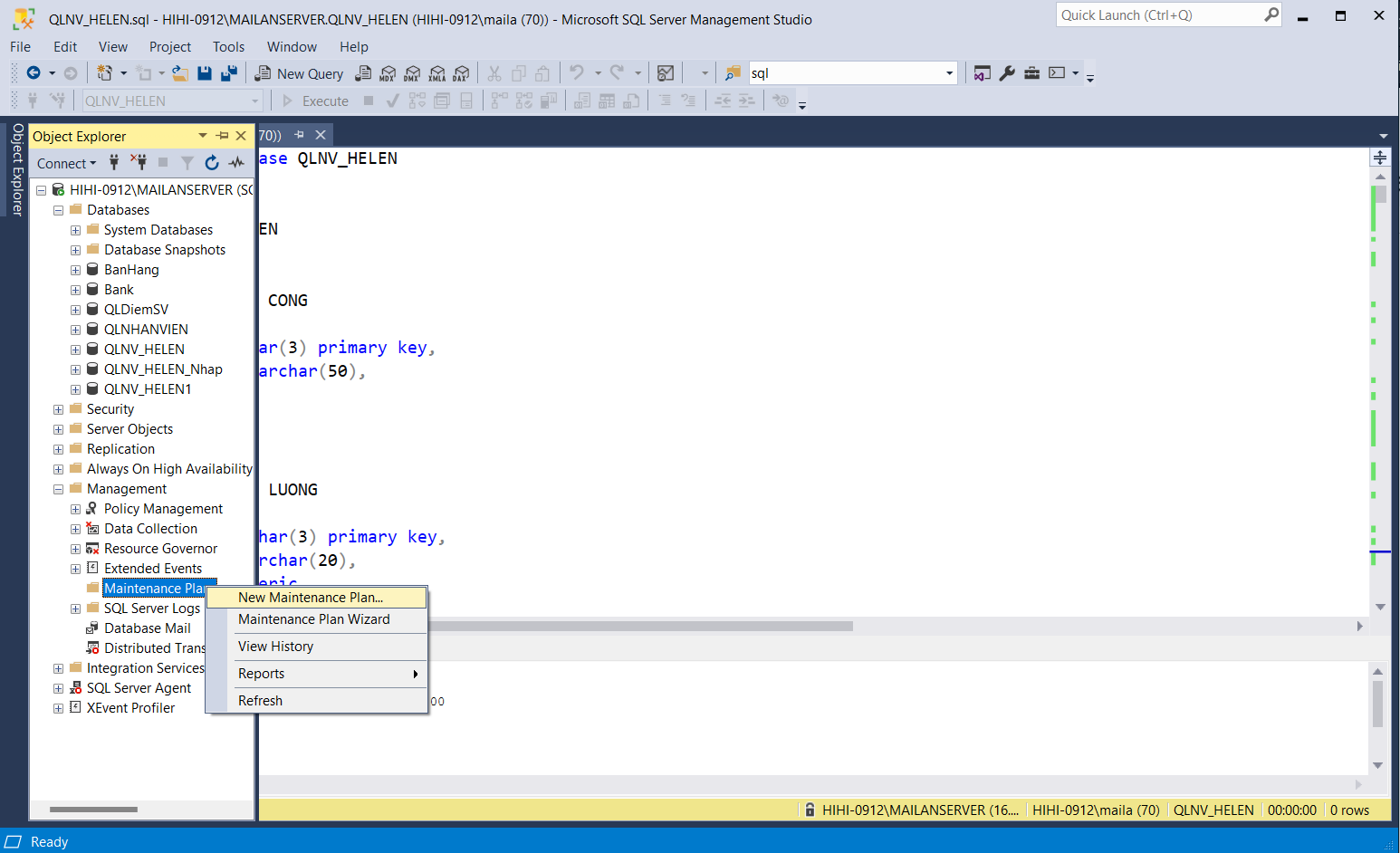
* sử dụng cả 2 loại Back up để sao lưu:
* Full back up: sao lưu toàn bộ dữ liệu lần đầu tiên
* Differential back up: sao lưu những dữ liệu thay đổi kể từ lần full back up gần nhất
* Full back up: ***backup lần đầu tiên của hệ thống (tuần or tháng)***

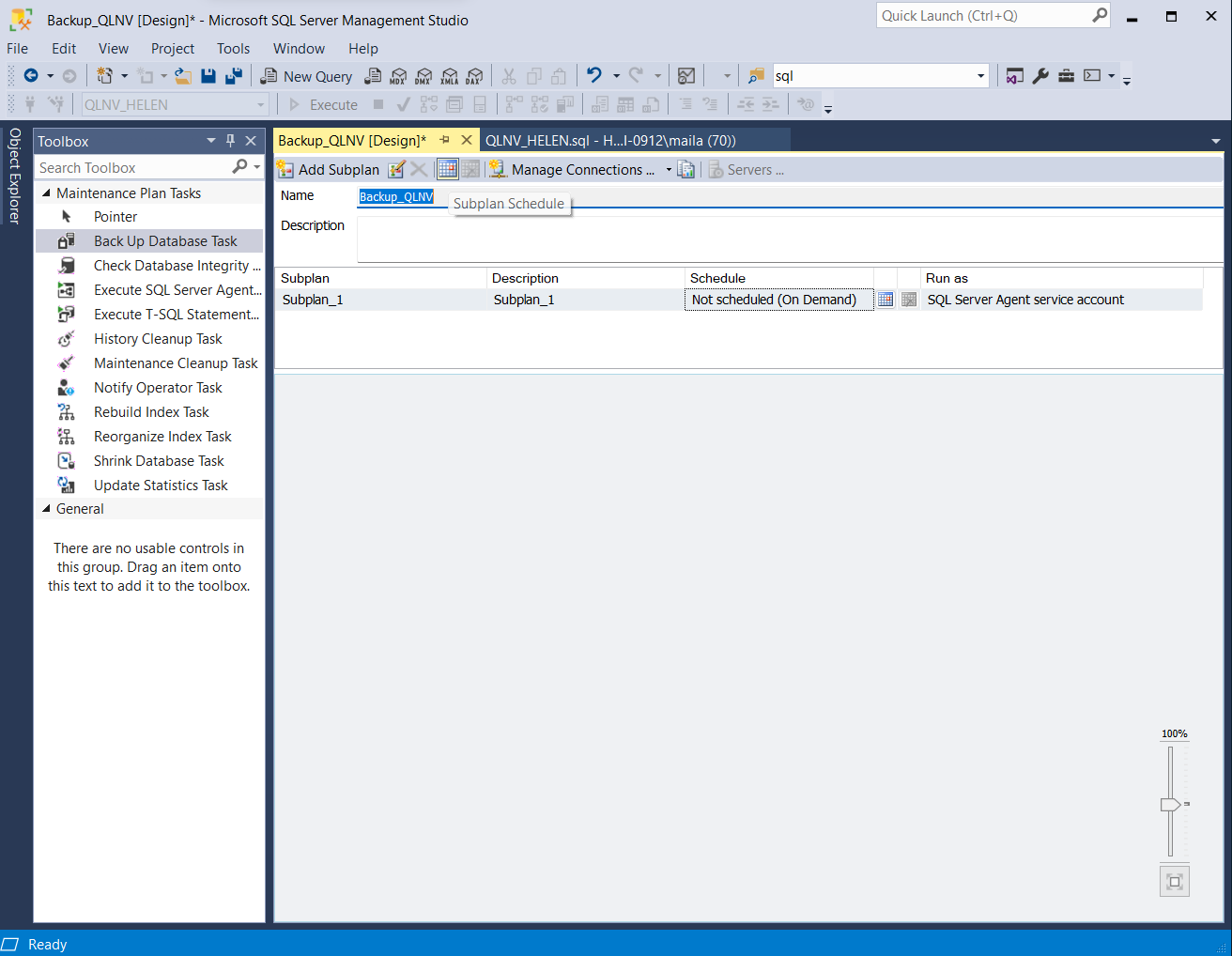
*backup database QLNV\_HELEN to disk = 'D:\QLNV\_HeLen\backup.bak'*

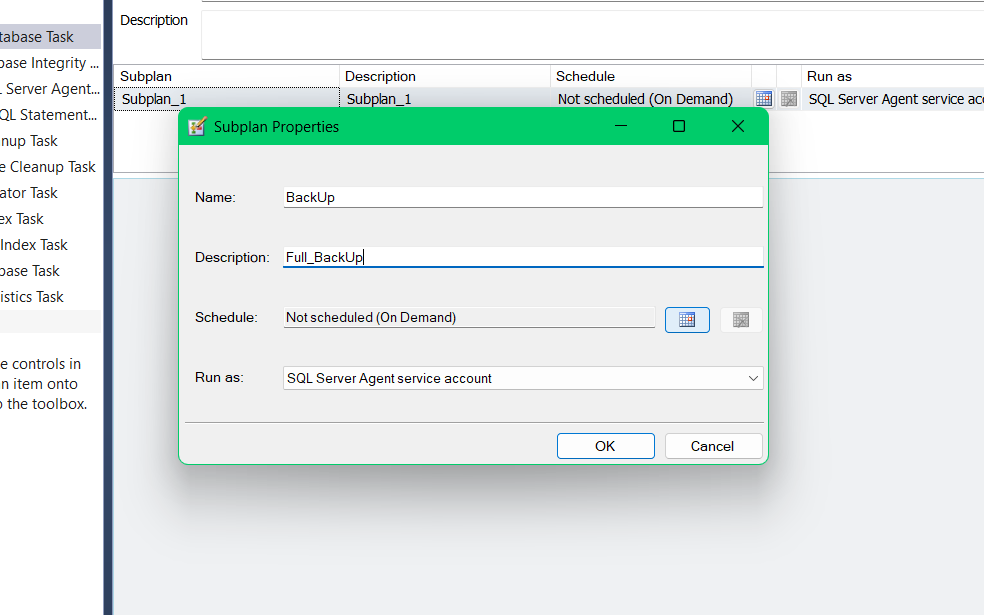
* thực hiện Back up vào 23h cuối mỗi tháng
* Differential backup: ***backup phần khác biệt so với trước***

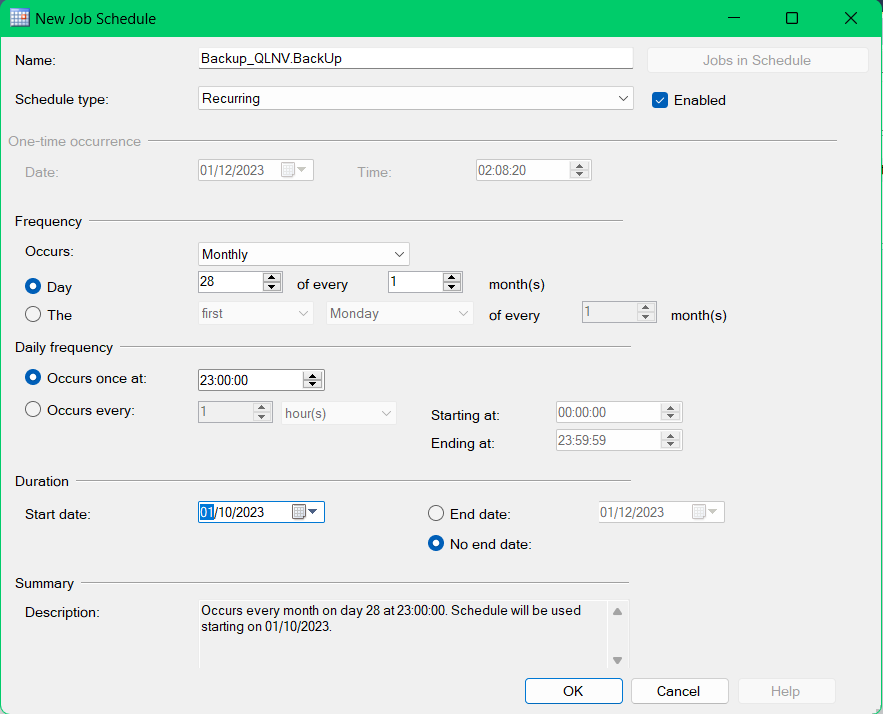
*backup database QLNV\_HELEN to disk = 'D:\QLNV\_HeLen\differential\_bk.bak' with differential*

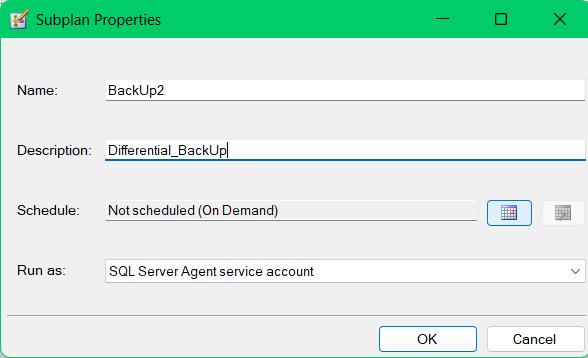
* Thực hiện Differential backup vào 22h mỗi ngày

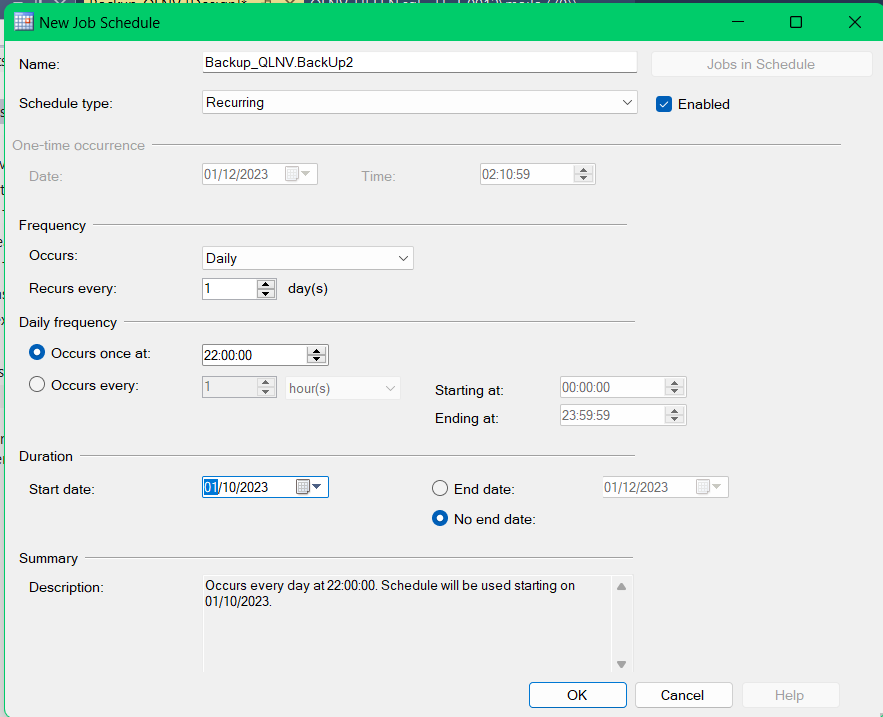


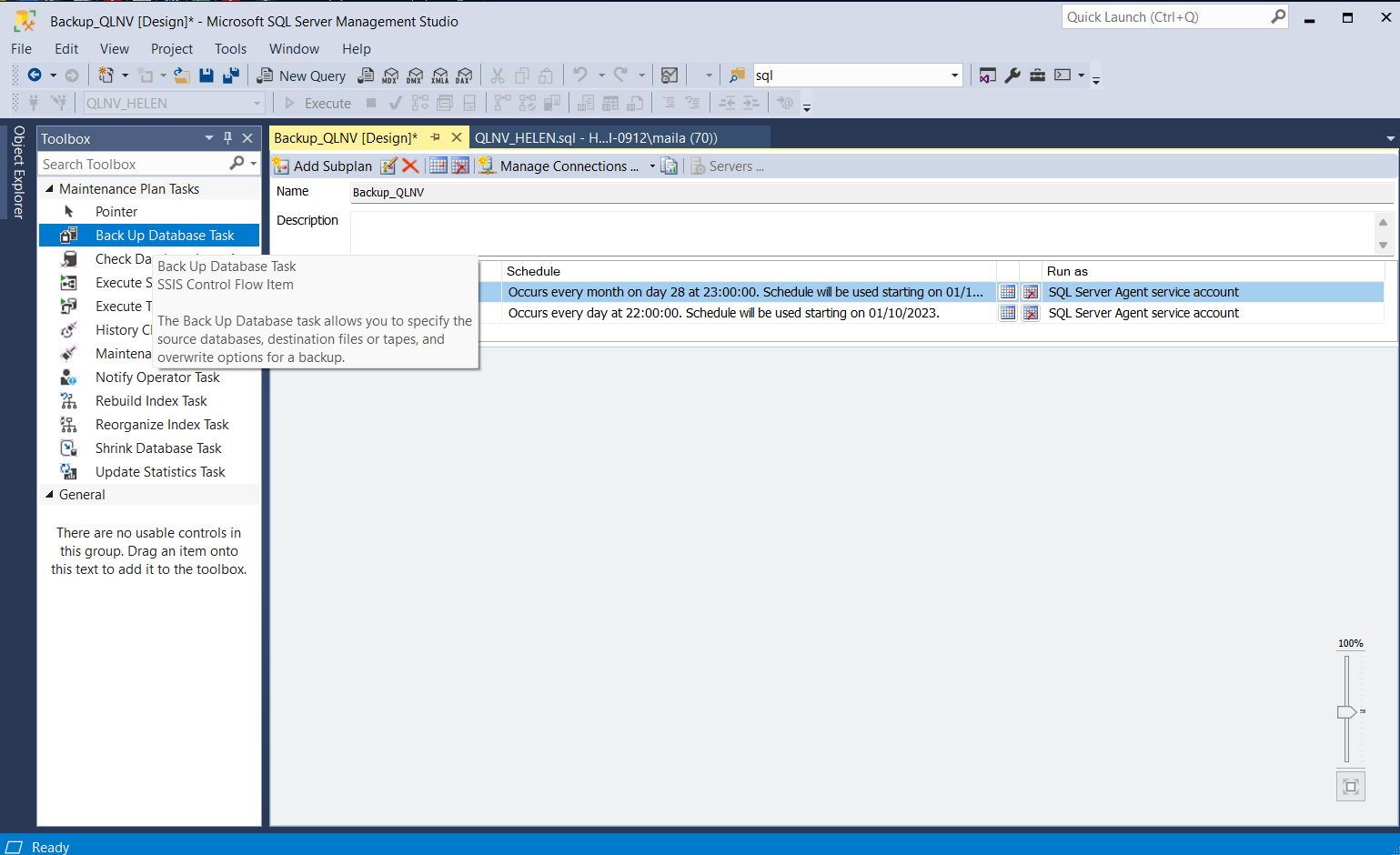


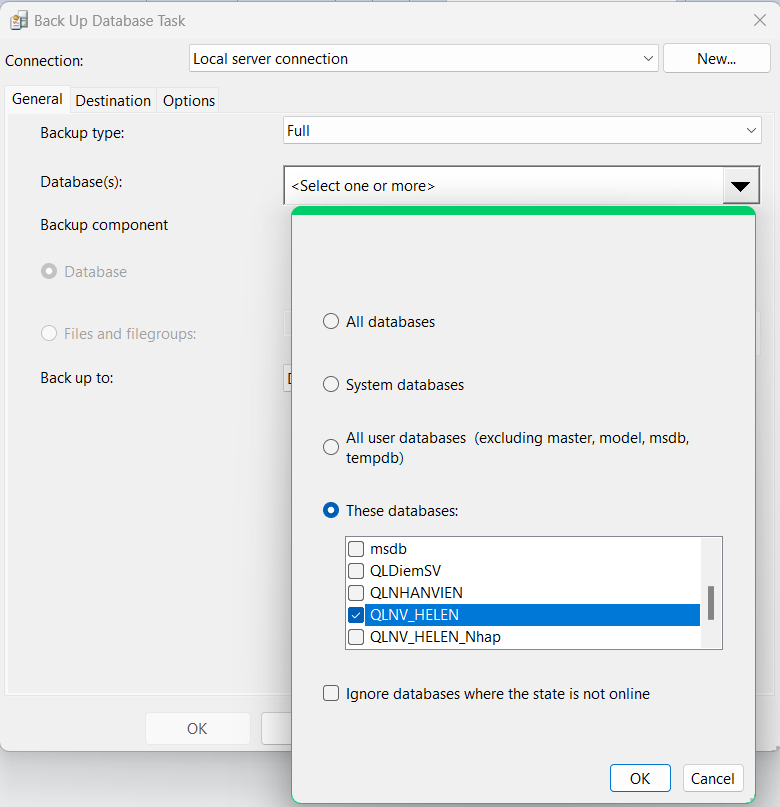


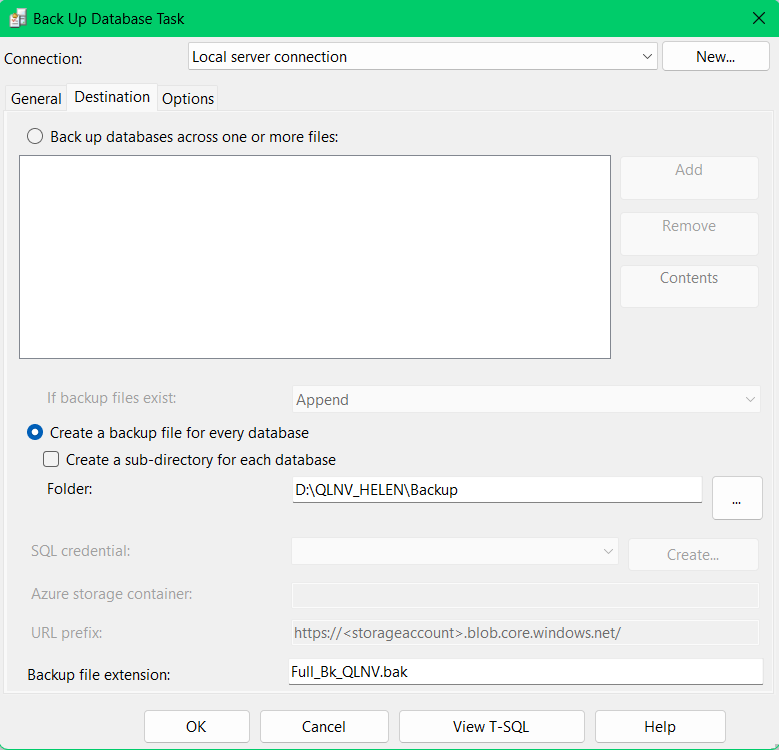


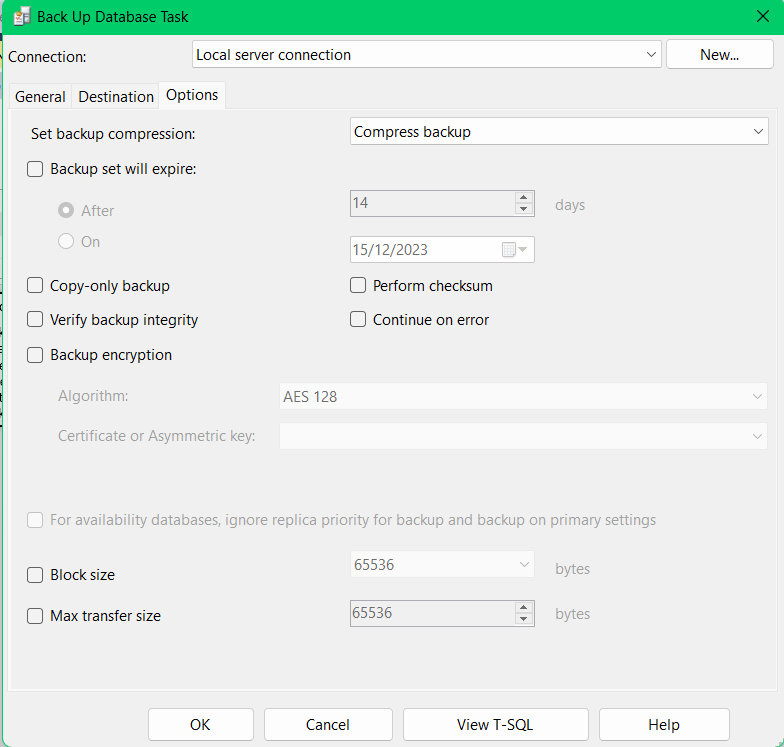


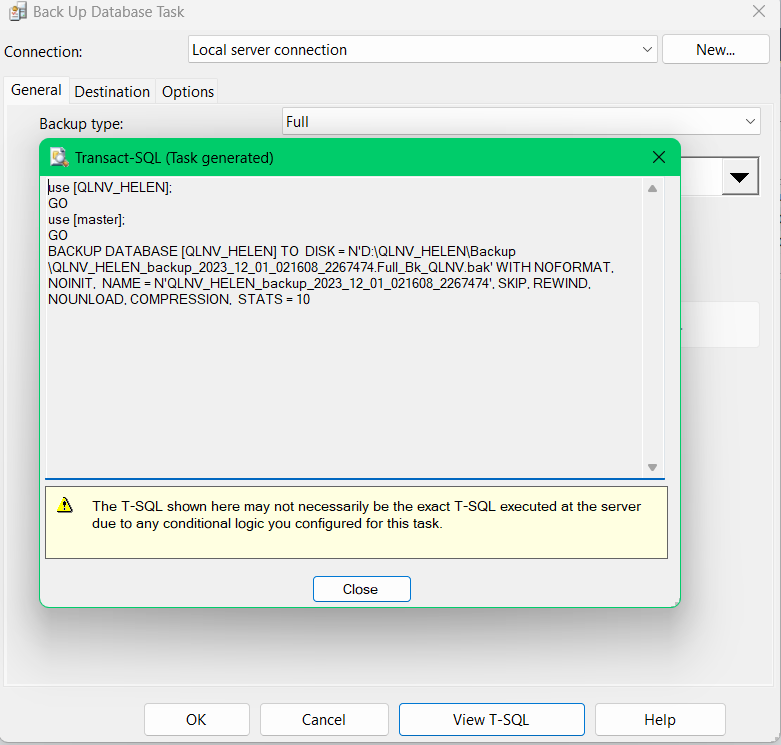
****

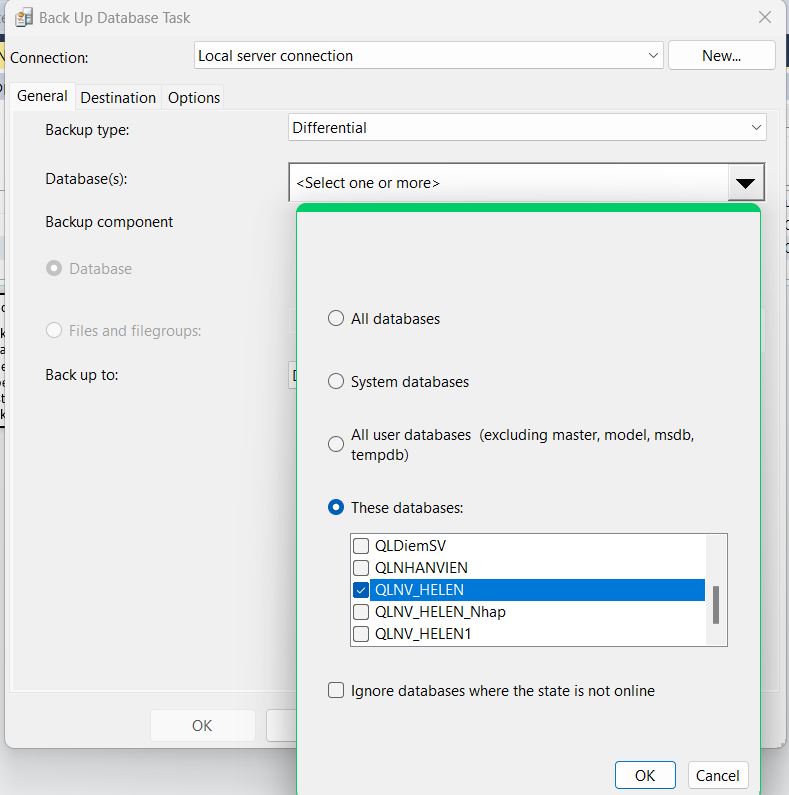
****

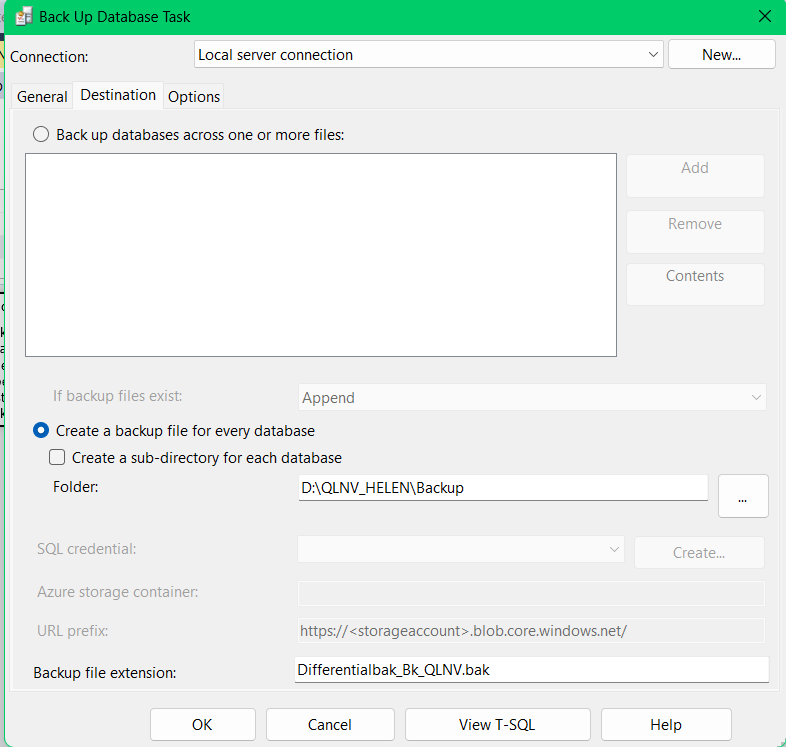
****

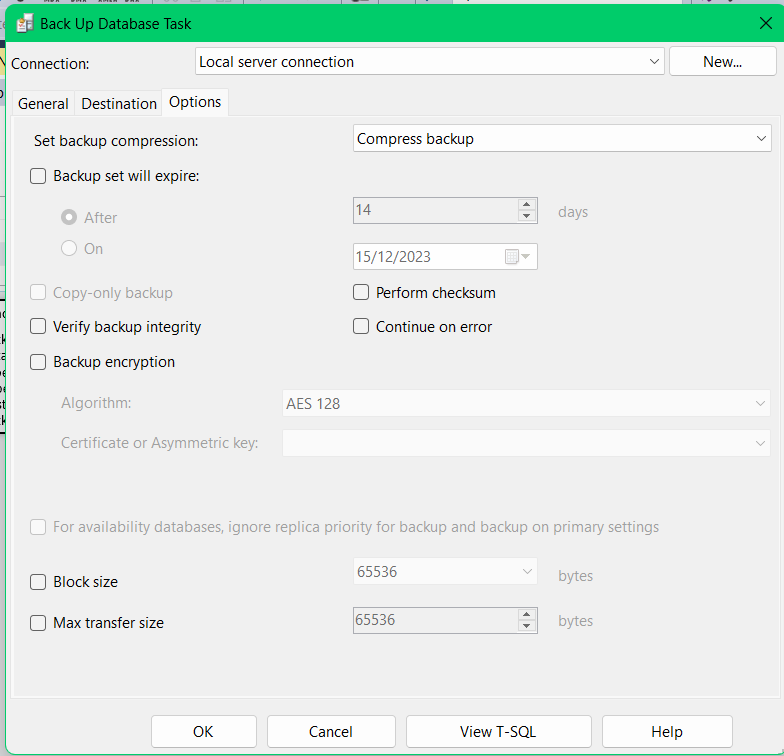
****

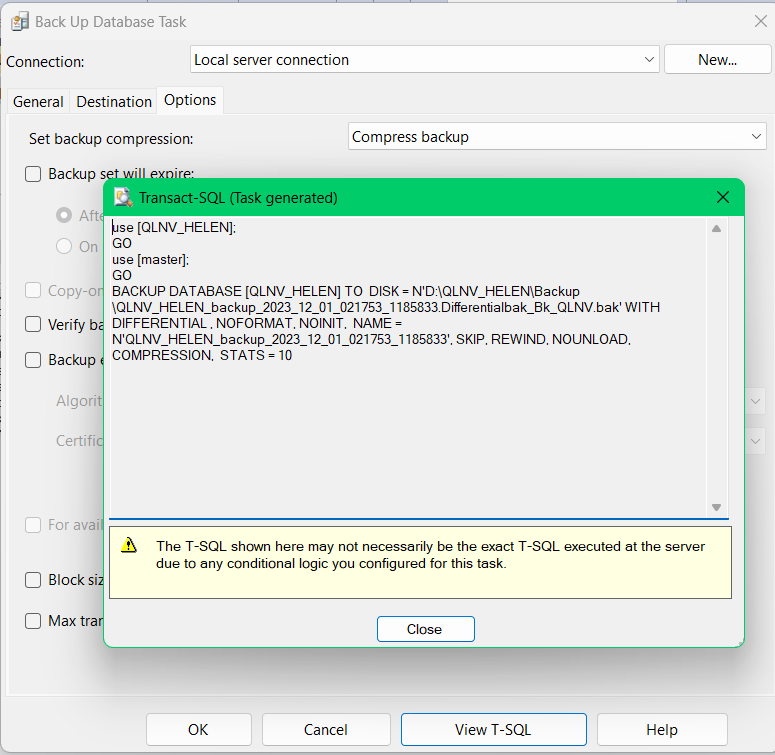
****

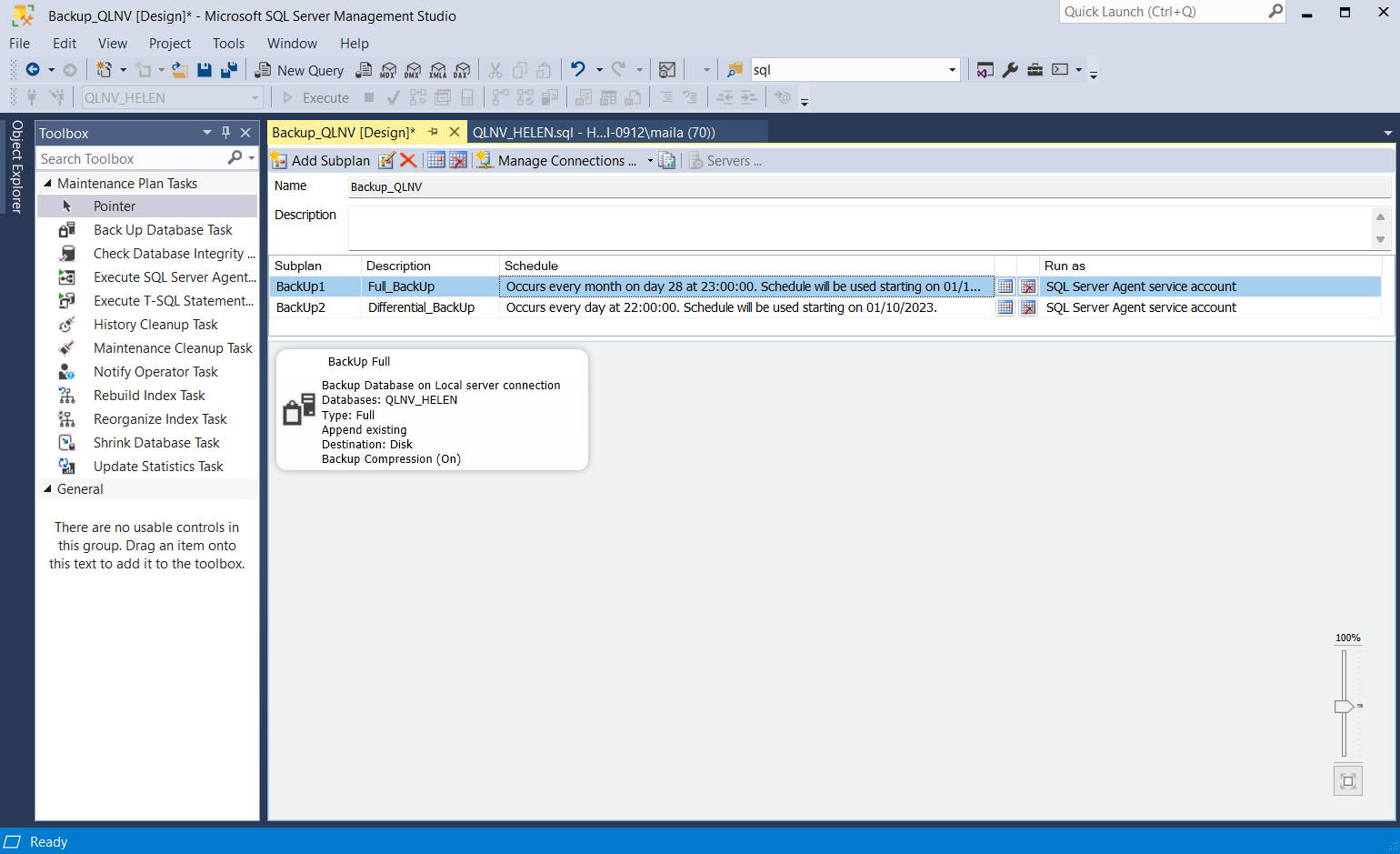
****

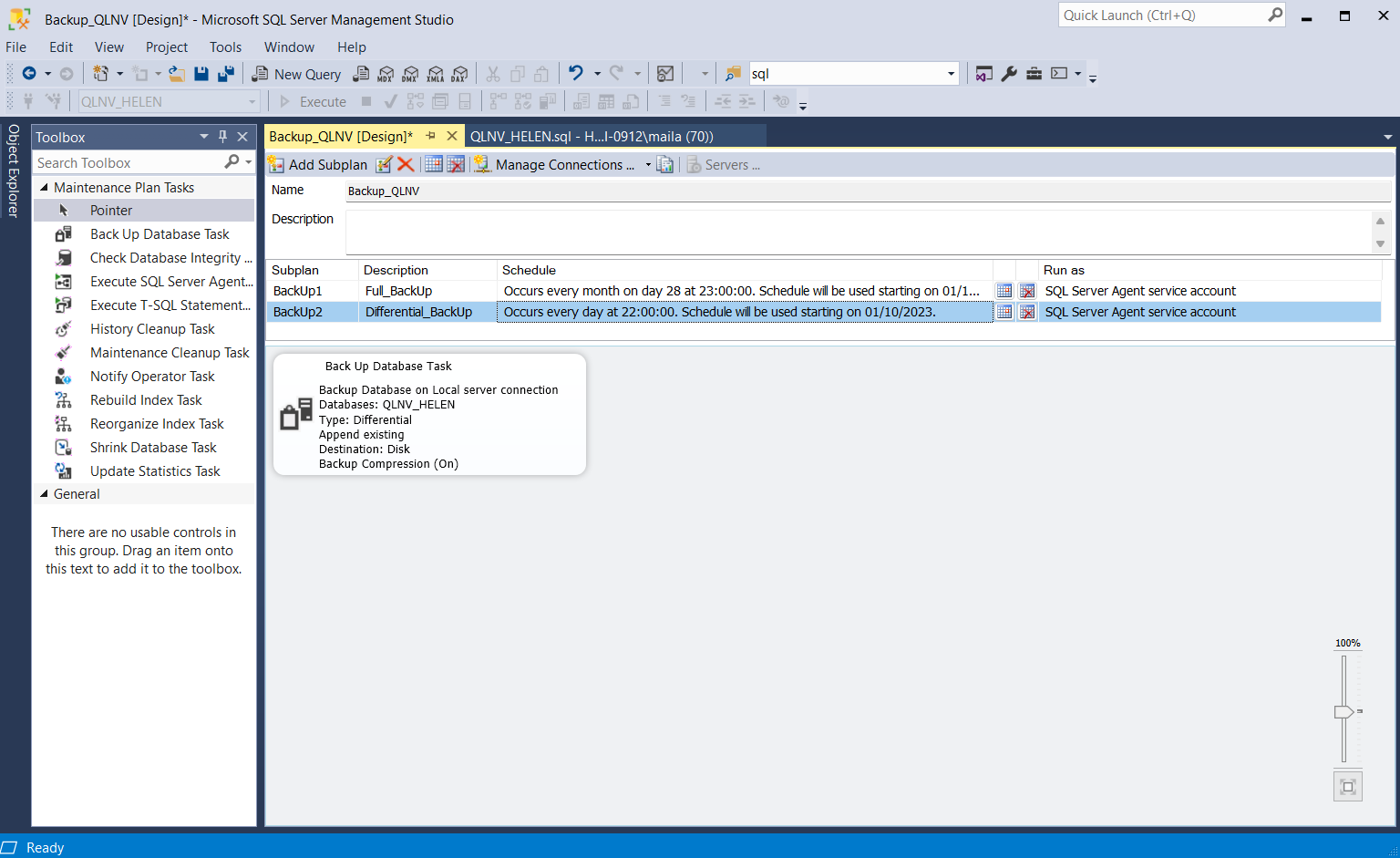
****

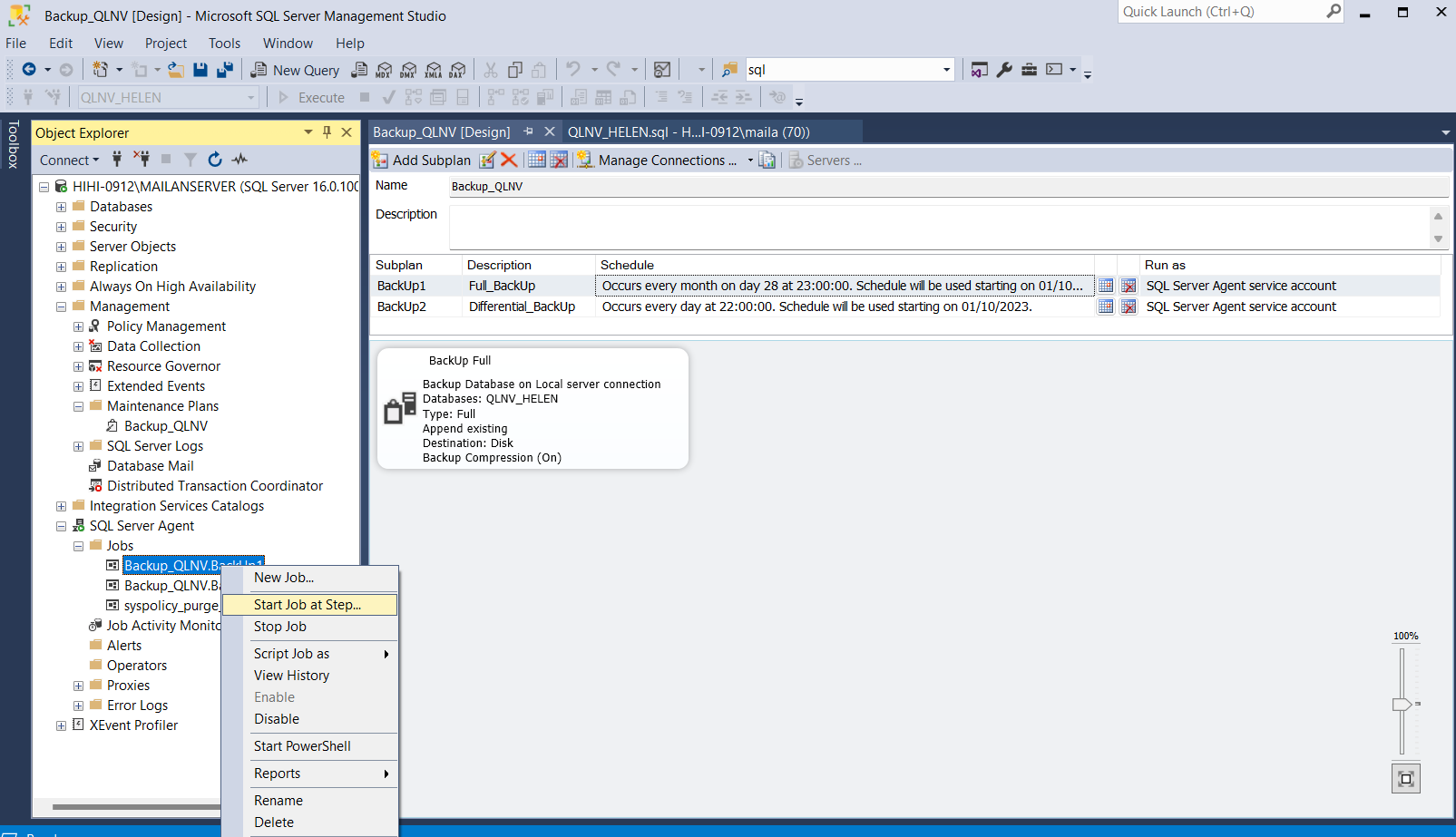
****

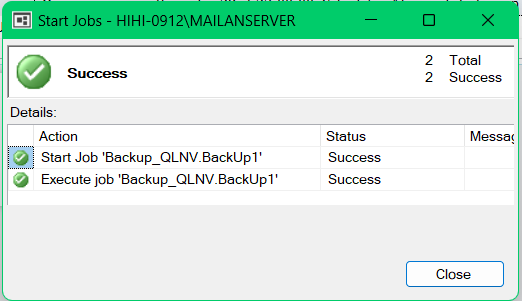
****

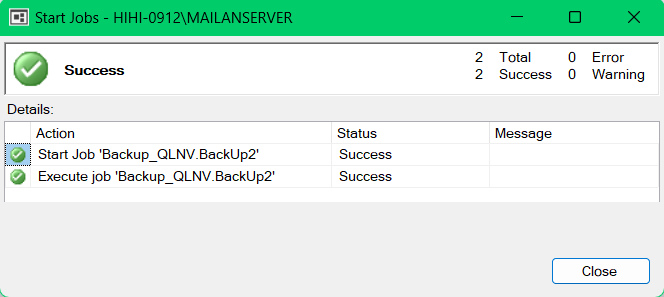
****

****

****

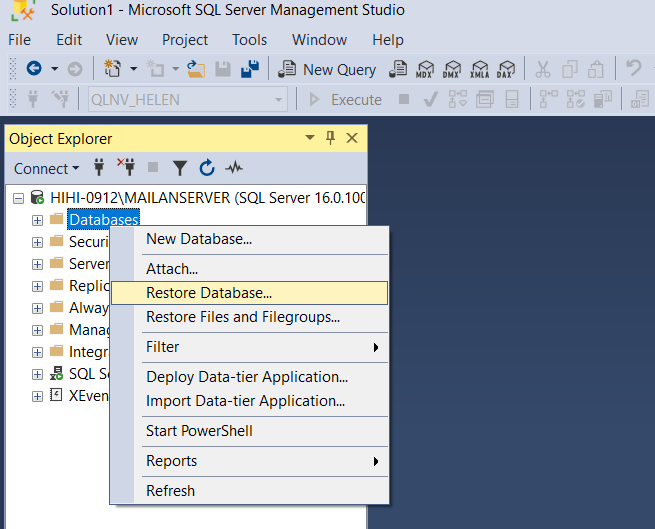
****





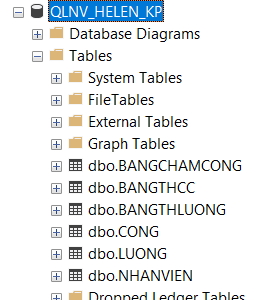


* **Khôi phục:**









**R7(2đ)**. Sử dụng một ngôn ngữ bất kỳ để phát triển một ứng dụng mang tên TESTDB thực hiện chức năng: thêm, sửa, xóa và tìm kiếm cho CSDL vừa tạo. **(C#)**

**2. Yêu cầu nâng cao**

**R8(1đ).** Giả sử lượng dữ liệu rất lớn, không đủ lưu trữ trong một ổ đĩa. Nhóm dự án hãy đưa ra phương án giải quyết TỐT NHẤT cho vấn đề đã đặt ra và thực hiện trên CSDL đã xây dựng. (Nêu lý do lựa chọn giải pháp và thực hiện triển khai giải pháp cho hệ thống)

đưa lên gg cloud

Dùng Microsoft Azure

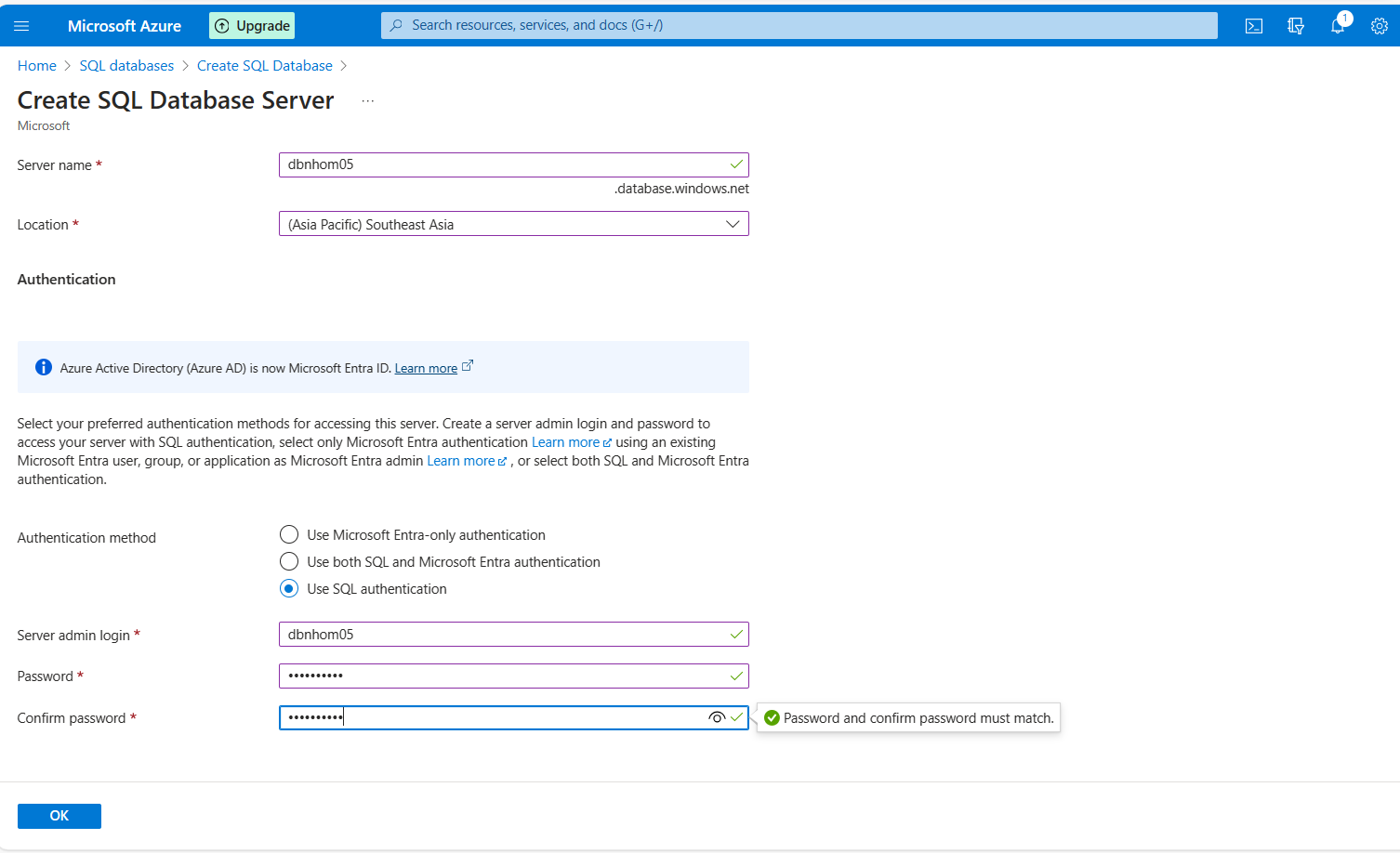
Để khắc phục lượng dữ liệu lớn, không đủ lưu trữ trong một ổ đĩa. Nhóm đưa ra phương án sử dụng Microsoft Azure. Microsoft Azure là nền tảng điện toán đám mây được cung cấp bởi Microsoft. Ứng dụng này cho phép người dùng truy cập và quản lý các dịch vụ, tài nguyên đám mây do Microsoft cung cấp.

Chọn sử dụng Microsoft Azure vì:

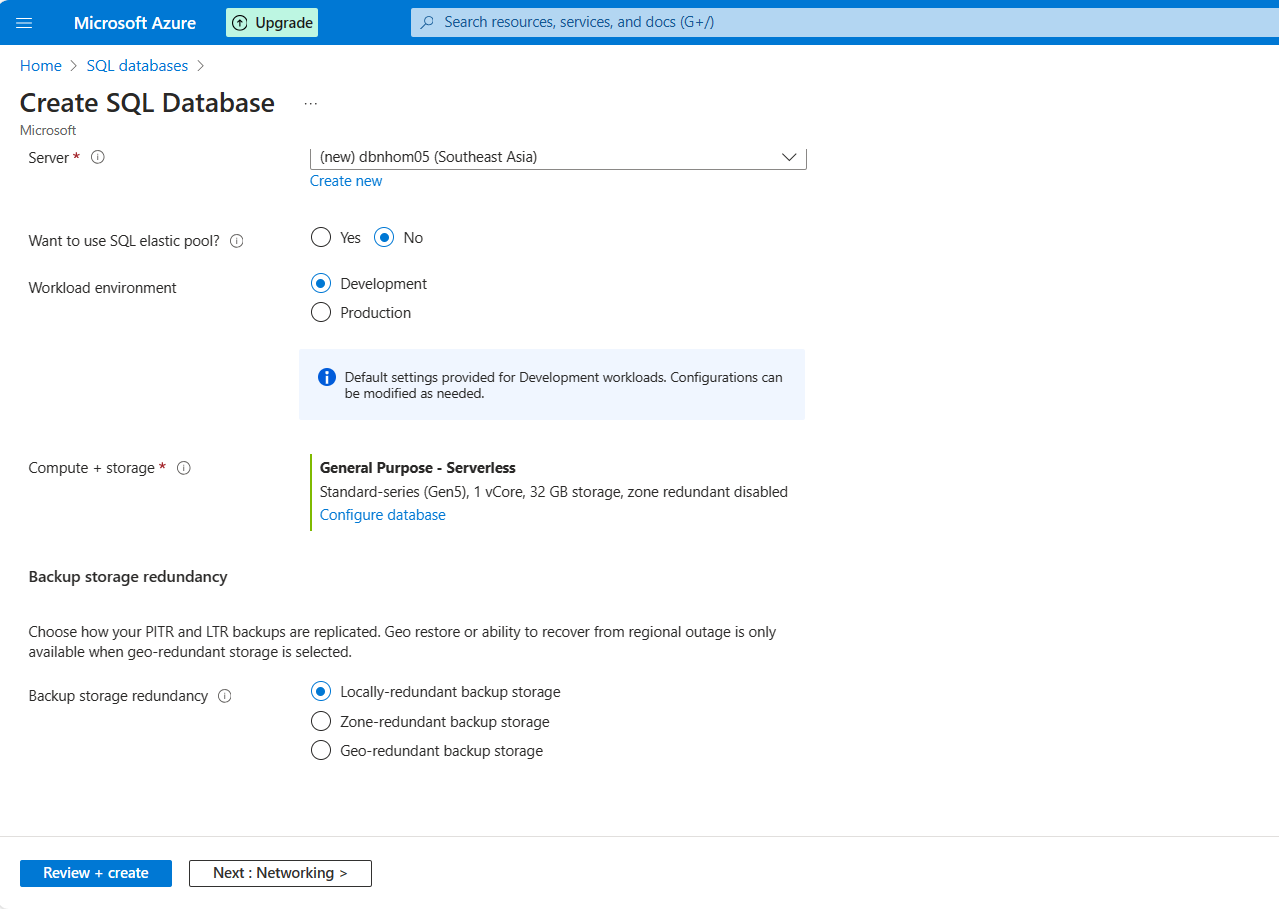
* Giá cả phải chăng cho quy mô quán nhỏ như Helen Coffee
* Microsoft Azure cho phép sao lưu dữ liệu bằng hầu hết mọi ngôn ngữ, trên mọi hệ điều hành.
* Bản sao lưu dữ liệu trên Microsoft Azure được lưu trữ thành ba bản sao dữ liệu ở ba vị trí khác nhau trong trung tâm dữ liệu và ba bản sao khác trong trung tâm dữ liệu Azure từ xa. Vì vậy, không bao giờ phải lo lắng về việc mất dữ liệu.
* Ngoài ra, dịch vụ của Microsoft còn cho phép điều chỉnh quá trình sao lưu tự động theo ý muốn.
* Tạo tài khoản trên ms azure, sau đó nhấn chọn SQL Database → create, sau đó nhập thông tin vào các ô trống, Resource group → create new→ nhập → OK



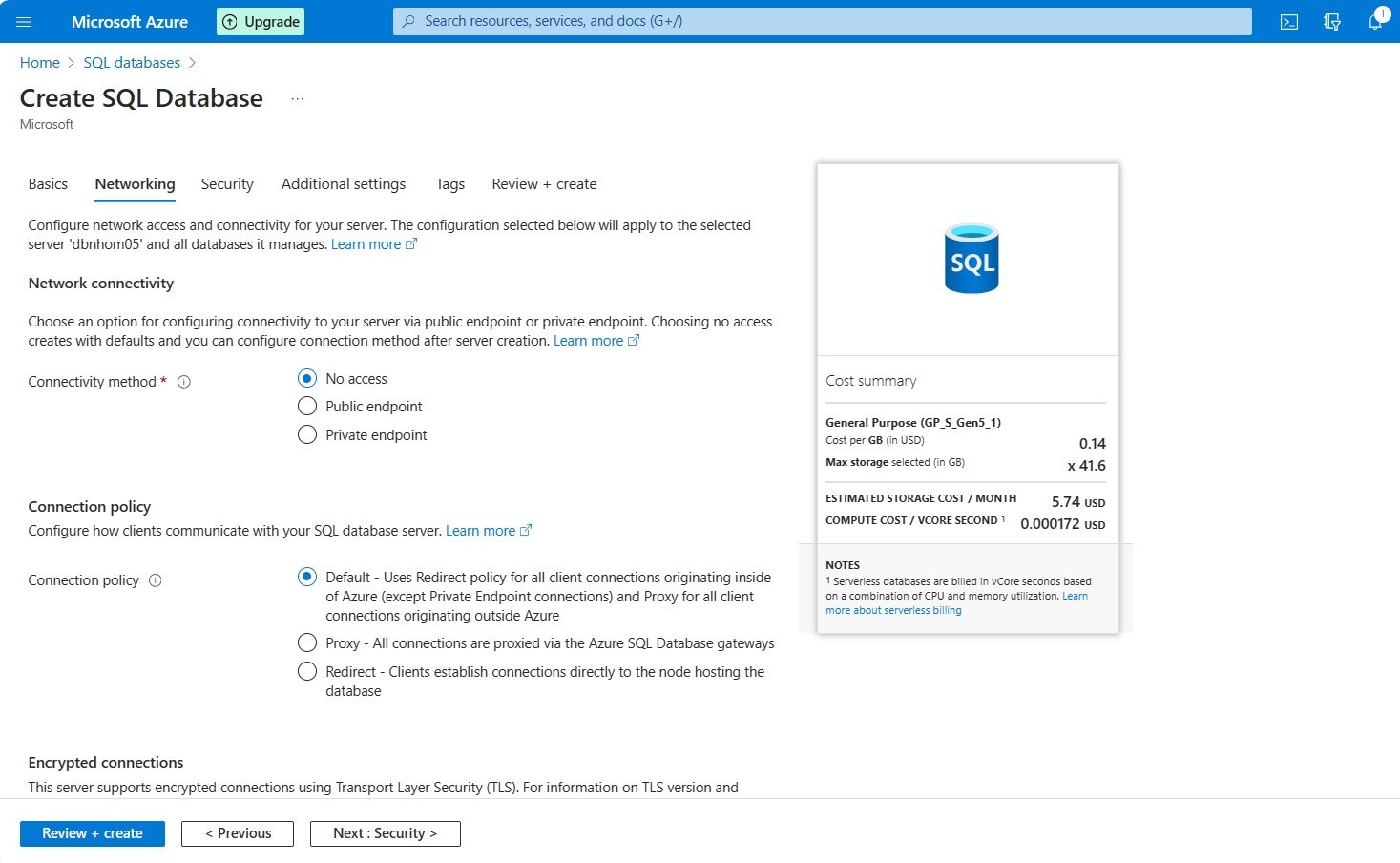
Tạo SQL database trên Microsoft Azure 1



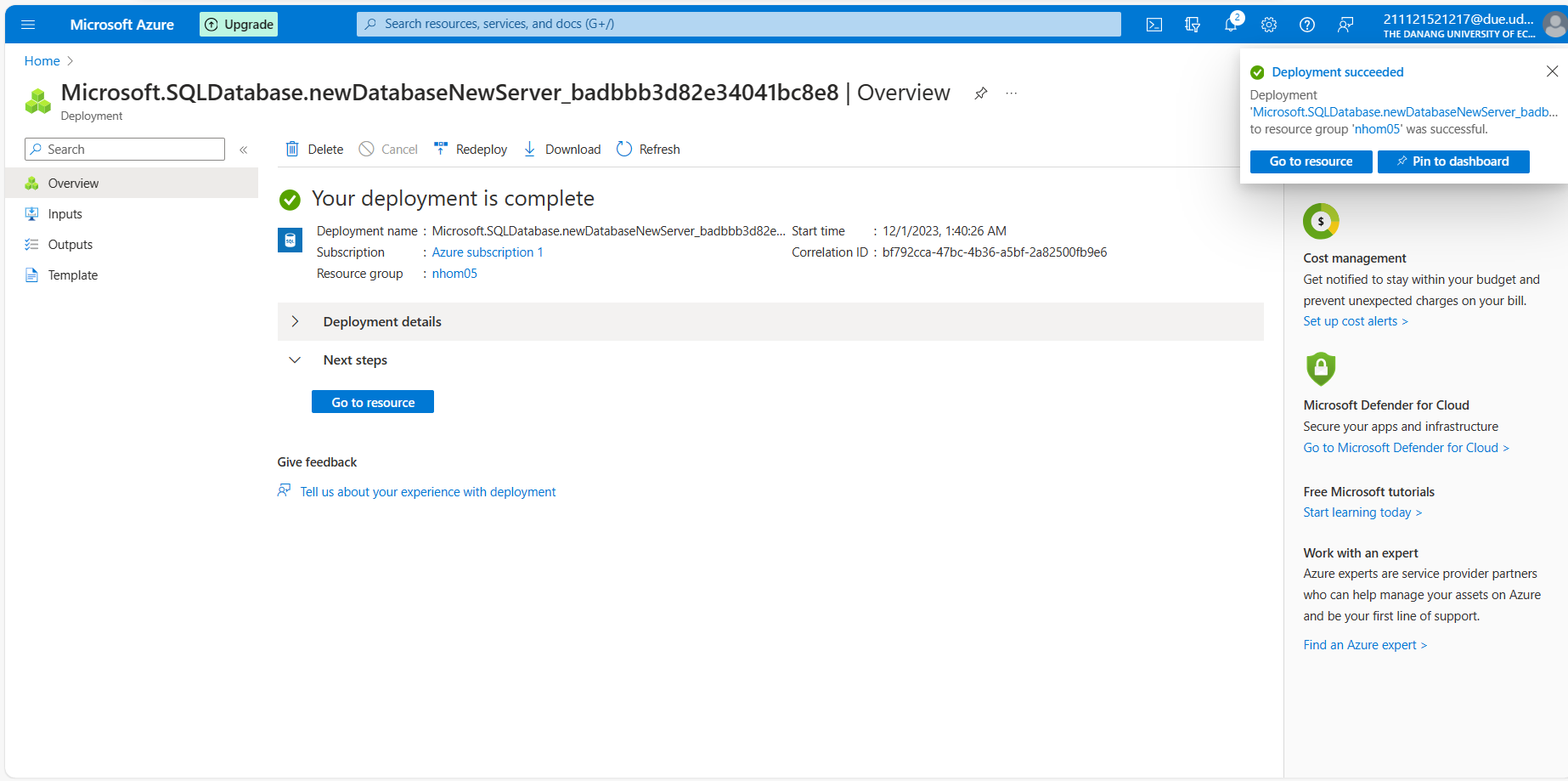
Tạo SQL database trên Microsoft Azure 2



Tạo SQL database trên Microsoft Azure 3

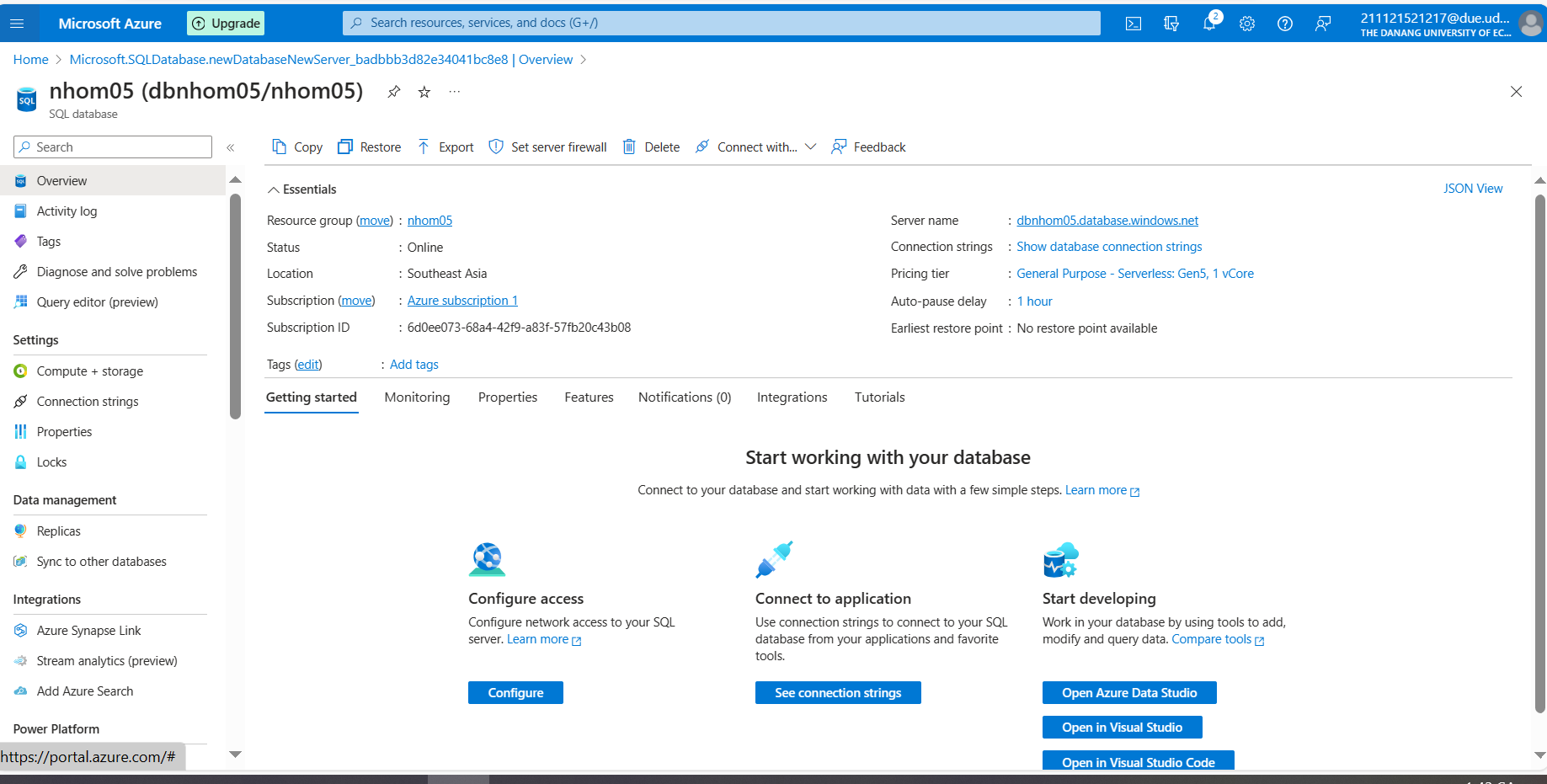


Tạo SQL database trên Microsoft Azure 4

* Sau khi nhấn Review + create, màn hình hiển thị như bên dưới, 

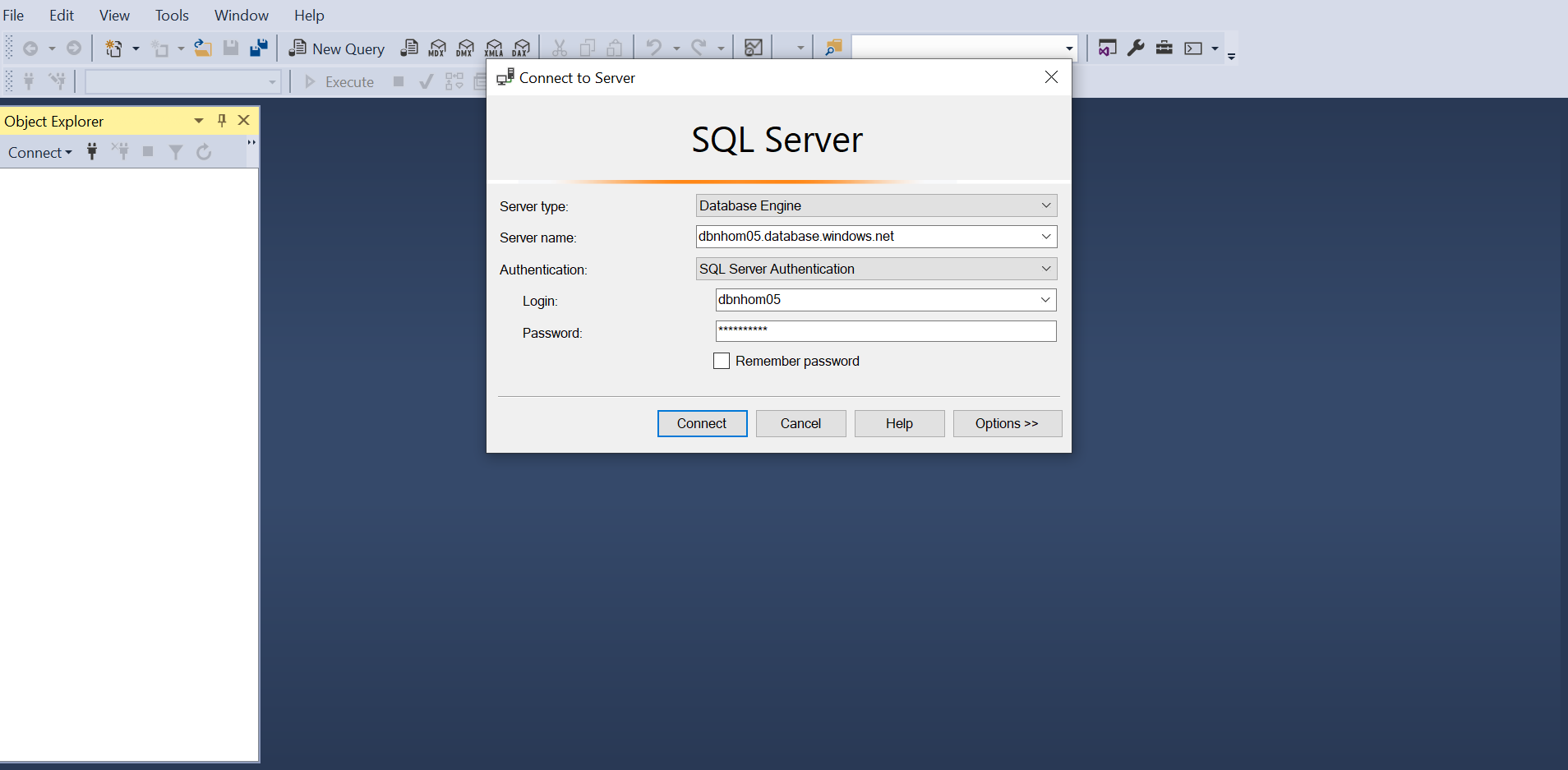
Tạo SQL database trên Microsoft Azure 5

* nhấp vào Go to resource



Màn hình database

* Sao chép link Server name để liên kết với SQL server



Liên kết SQL Server với database vừa tạo trên Azure

****

Cơ sở dữ liệu đã được đưa lên Azure

**R9(1đ).** Để đề phòng phương án hệ thống TESTDB bị tấn công bằng SQL Injection. Nhóm dự án hãy đưa ra phương án tốt nhất và thực thi phương án đó. (Nêu lý do lựa chọn giải pháp và thực hiện triển khai giải pháp cho hệ thống) sửa code trong code backend

Có thể đề phòng tấn công bằng SQL Injection bằng các biện pháp: backup dữ liệu, phân quyền người dùng, sử dụng WAF (Web Application Firewall)

* **Phân quyền người dùng**: Đã tạo login cho cơ sở dữ liệu ở R5, gồm:
* login QUANLY
* login NHANVIEN

người dùng sẽ được phân quyền thành QUANLY hay NHANVIEN khi đăng nhập vào hệ thống. Quản lý có thể xem, thêm, sửa, xóa dữ liệu, còn nhân viên chỉ có quyền xem dữ liệu

* **Backup dữ liệu:** Đã xây dựng cơ chế tự động backup dữ liệu tại R6

Full backup: đặt lịch vào 23h ngày 28 mỗi tháng

Differential backup: đặt lịch vào 22h mỗi ngày

Có thể khôi phục dữ liệu từ file backup khi cần hoặc bị mất dữ liệu gốc.

* **Không hiển thị exception, message lỗi:** Hacker dựa vào message lỗi để tìm ra cấu trúc database. Khi có lỗi, ta chỉ hiện thông báo lỗi chứ đừng hiển thị đầy đủ thông tin về lỗi, tránh hacker lợi dụng.
* **Mật khẩu:**
* Giới hạn độ dài mật khẩu (dùng kiểu dữ liệu VAR)
* Giới hạn loại kí tự đặc biệt (các kí tự: /, ., “”, \*, ‘’, >, <, =,...)
* **Không cộng chuỗi để tạo SQL:** Sử dụng parameter thay vì cộng chuỗi. Nếu dữ liệu truyền vào không hợp pháp, SQL Engine sẽ tự động báo lỗi, ta không cần dùng code để check.
* **Sử dụng** **WAF** (Web Application Firewall)
* WAF là một thiết bị Proxy giúp xử lý các giao thức HTTP nhằm bảo vệ ứng dụng Web hiệu quả. WAF sẽ kiểm tra lưu lượng truy cập và lọc ra những yêu cầu nào có mối đe dọa xâm phạm đến trang Web trước khi đến ứng dụng Web.
* WAF là một phương pháp bảo mật giữa ứng dụng được đặt giữa Web Server và Web Client.
* WAF sẽ thực hiện kiểm tra chi tiết mọi Response và Request đối với tất cả các dạng lưu lượng truy cập Web. Nhờ vậy, WAF sẽ xác định được các mối đe dọa và ngăn chặn chúng xâm nhập vào Server.
* Cơ chế giúp WAF có thể ngăn chặn được tấn công SQL Injection

WAF (Web Application Firewall) có thể được cấu hình để ngăn chặn SQL Injection bằng cách kiểm tra các yêu cầu HTTP đến ứng dụng và chặn các yêu cầu có dấu hiệu của SQL Injection. Dưới đây là một số cách WAF có thể được sử dụng để ngăn chặn SQL Injection:

* ***Kiểm tra Cú Pháp SQL độc hại:***

WAF có thể thực hiện kiểm tra cú pháp SQL để phát hiện các dấu hiệu của SQL Injection trong các yêu cầu đến server. Các biểu hiện phổ biến có thể bao gồm việc kiểm tra các từ khóa SQL như "SELECT", "INSERT", "UPDATE", "DELETE", cũng như các ký tự đặc biệt như dấu nháy đơn ('), dấu nháy kép ("), và dấu chấm phẩy (;).

* ***Kiểm tra Tham Số Đầu Vào:***

WAF có thể kiểm tra các tham số đầu vào của yêu cầu để đảm bảo rằng chúng không chứa cú pháp SQL độc hại. Điều này có thể bao gồm việc kiểm tra chuỗi đầu vào để đảm bảo rằng nó không chứa các ký tự không mong muốn hoặc không hợp lệ.

* ***Xác định Cố Gắng Tấn Công:***

WAF có thể theo dõi các mô hình hoạt động bất thường có thể chỉ ra một cuộc tấn công SQL Injection. Ví dụ, nếu có nhiều yêu cầu có dấu hiệu của SQL Injection đến từ cùng một địa chỉ IP trong một khoảng thời gian ngắn, đó có thể là dấu hiệu của một cuộc tấn công và WAF có thể thực hiện các biện pháp ngăn chặn.

* ***Chặn IP và Mô hình Đối Tượng Đen:***

Nếu một địa chỉ IP cụ thể được xác định là nguồn của cuộc tấn công SQL Injection, WAF có thể chặn hoặc hạn chế tất cả các yêu cầu từ địa chỉ IP đó. Điều này giúp ngăn chặn tấn công từ các nguồn cụ thể.

* ***Cập Nhật Chính Sách Bảo Mật:***

WAF nên có khả năng cập nhật chính sách bảo mật để điều chỉnh quy tắc kiểm tra và chặn dựa trên các mối đe dọa mới và thay đổi trong các biểu hiện của SQL Injection.

* ***Ghi Log và Báo Cáo:***

WAF có thể ghi lại tất cả các yêu cầu được kiểm tra và các hành động chặn được thực hiện. Điều này giúp quản trị viên hệ thống theo dõi và phản ứng nhanh chóng đối với các cuộc tấn công potential.

Tài liệu tham khảo

1. WAF

Tài liệu bài giảng MIS3008

https://microsoft.fptcloud.com/microsoft-azure/

https://www.vnetwork.vn/news/waf-la-gi/

https://www.matbao.net/tin-tuc/waf-la-gi-tuong-lua-ung-dung-web-mang-lai-gi-cho-doanh-nghiep-134240.html