

BẢO MẬT CƠ SỞ DỮ LIỆU

Lab05 - Transparent Data Encryption - TDE

Sinh viên:

Khúc Khánh Đăng – 20120262

Giảng viên hướng dẫn :

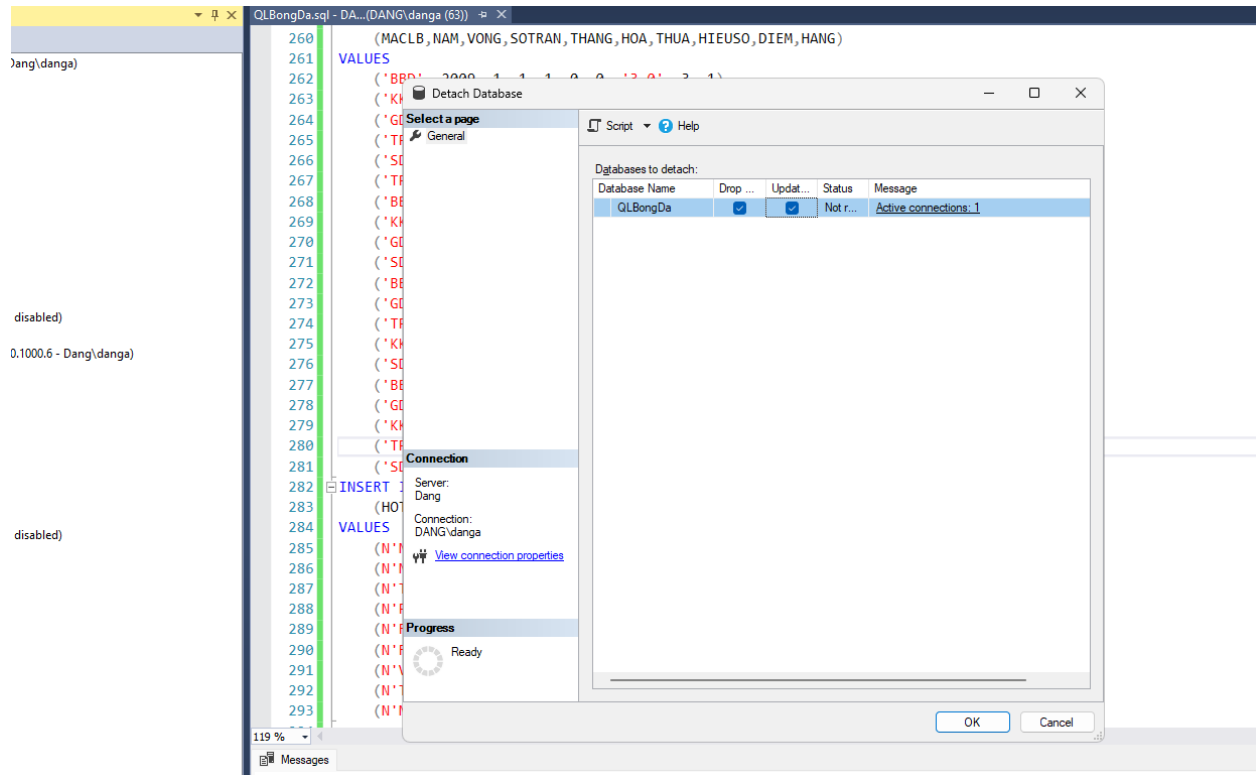
PSG.TS Nguyễn Đình Thúc

TS. Trần Bảo Ngọc

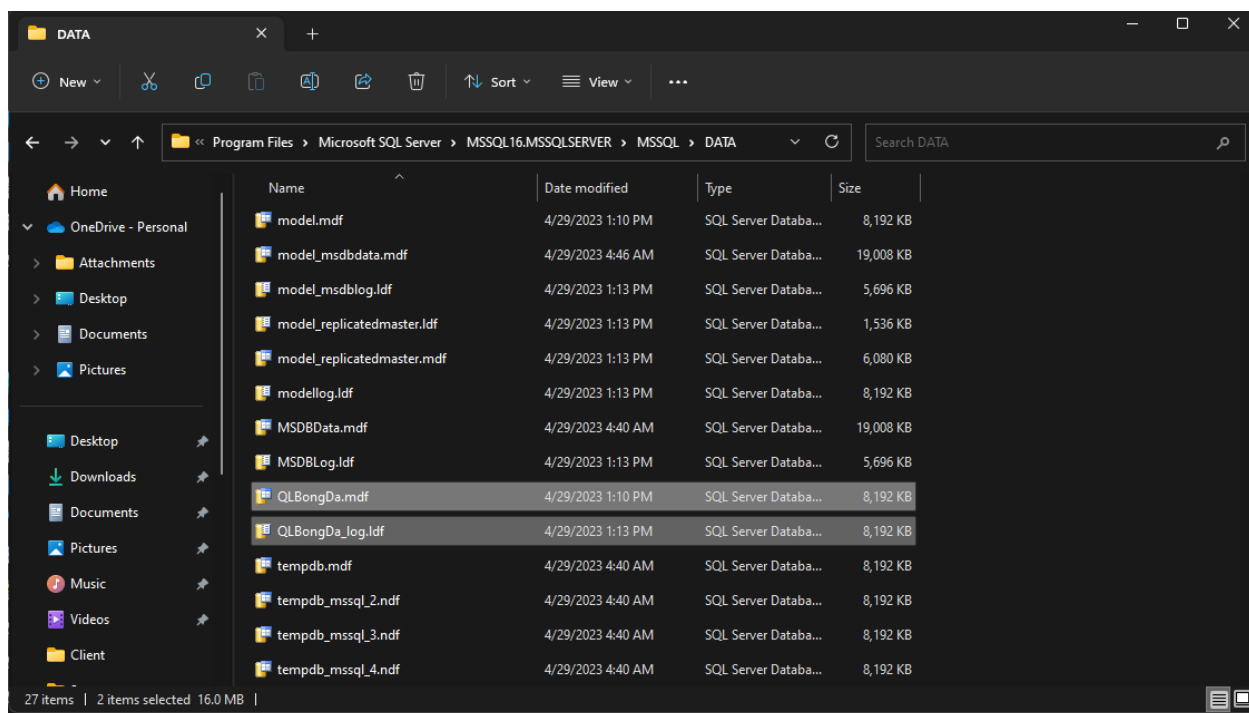
ThS. Nguyễn Thị Hương



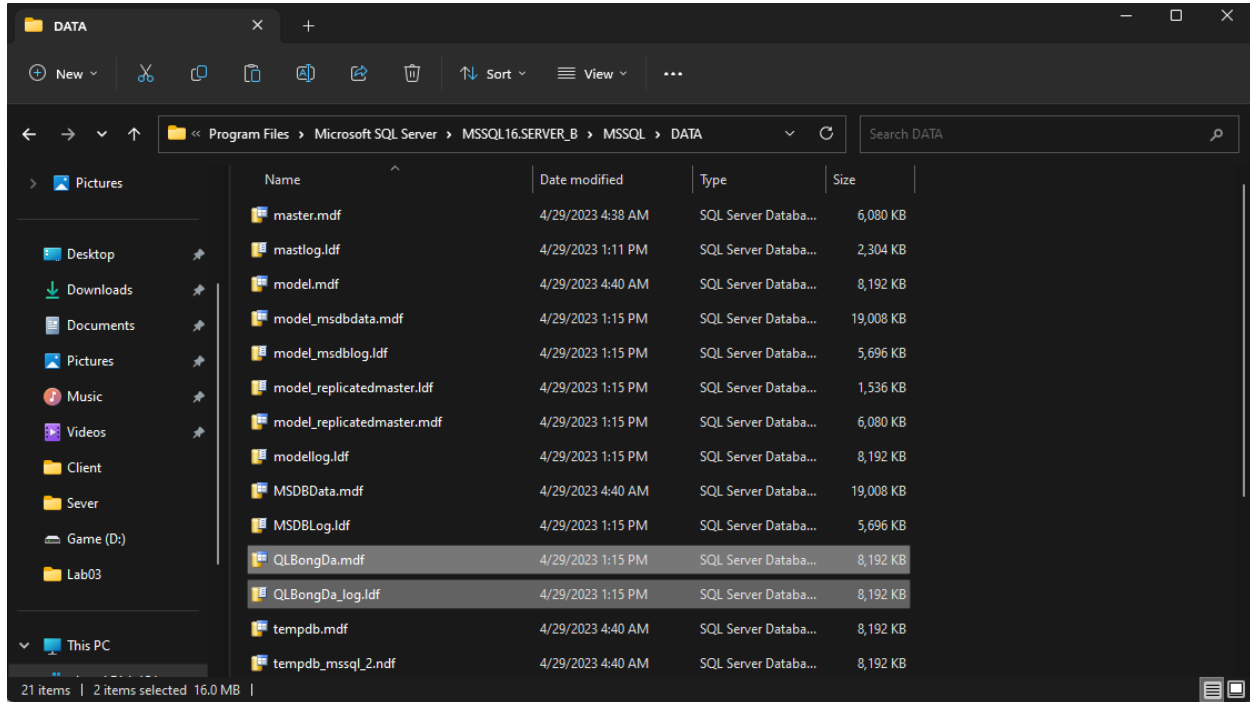
Khoa Công nghệ Thông tin
Đại học Khoa học Tự nhiên TP HCM



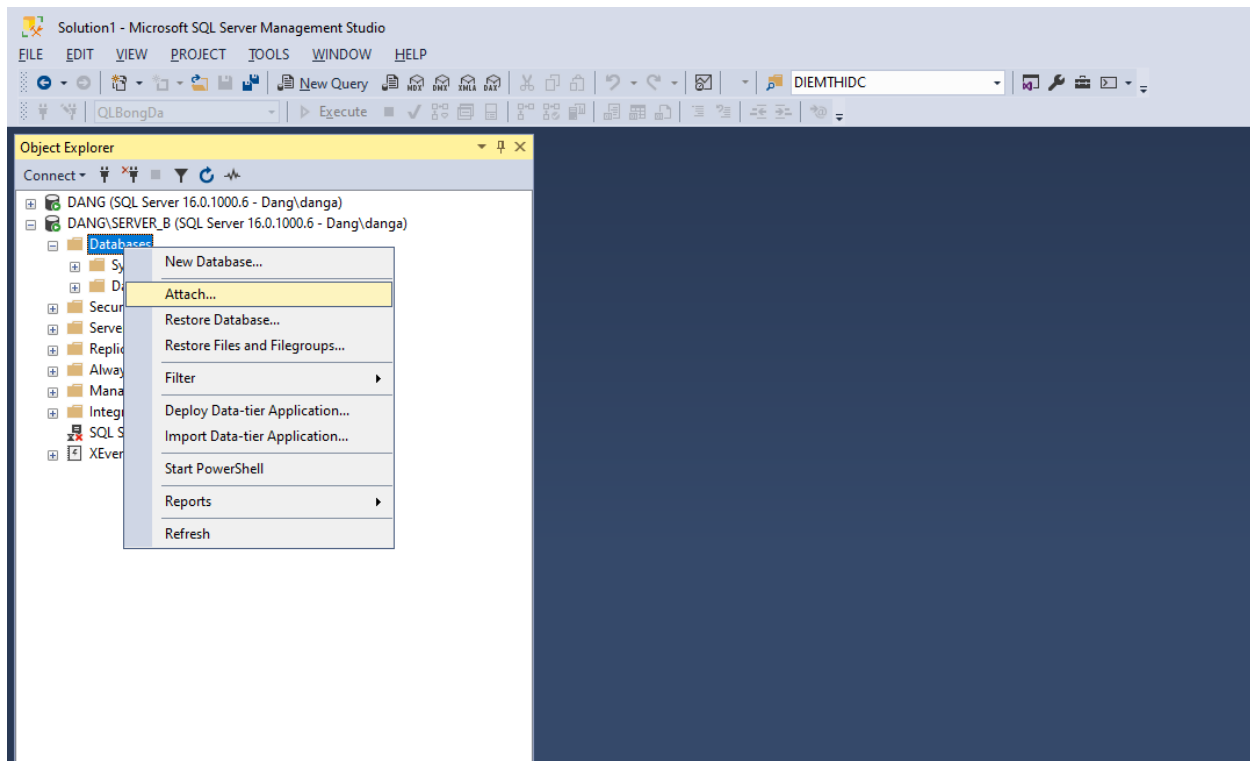
— Copy các file .mdf và .ldf từ folder của Server A sang Server B

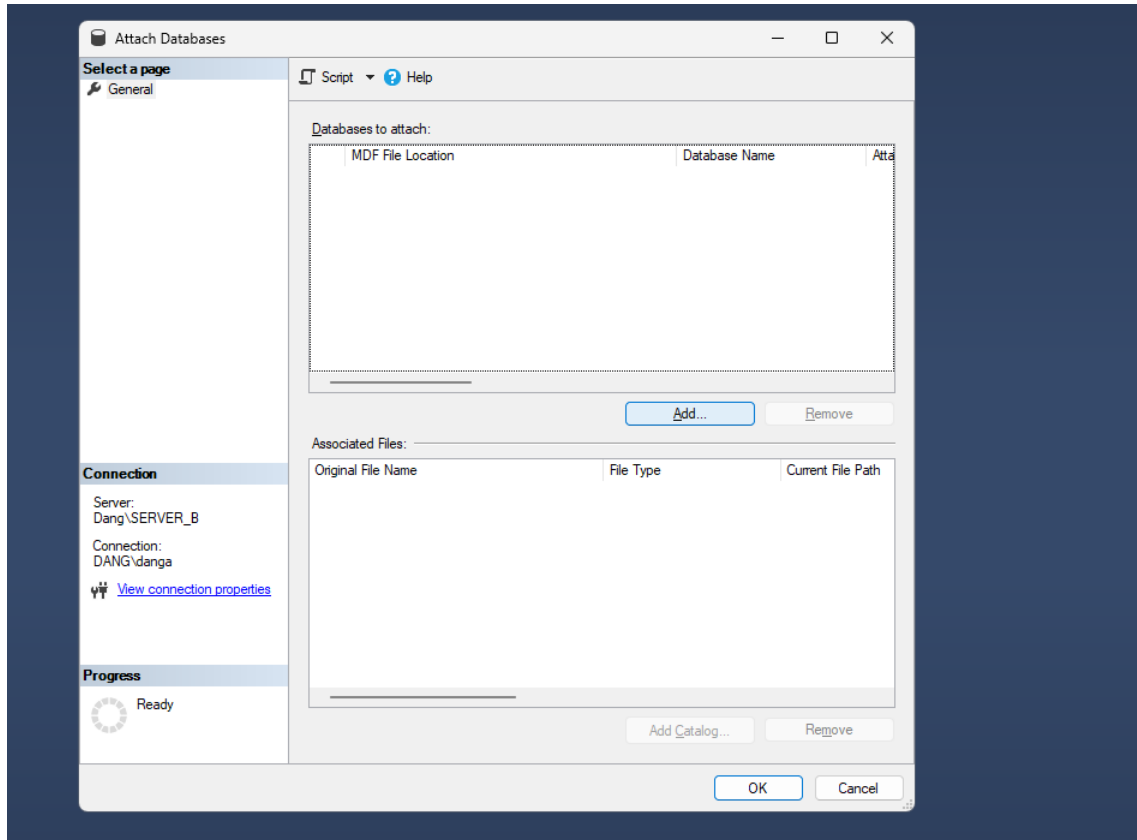


— Folder Server B

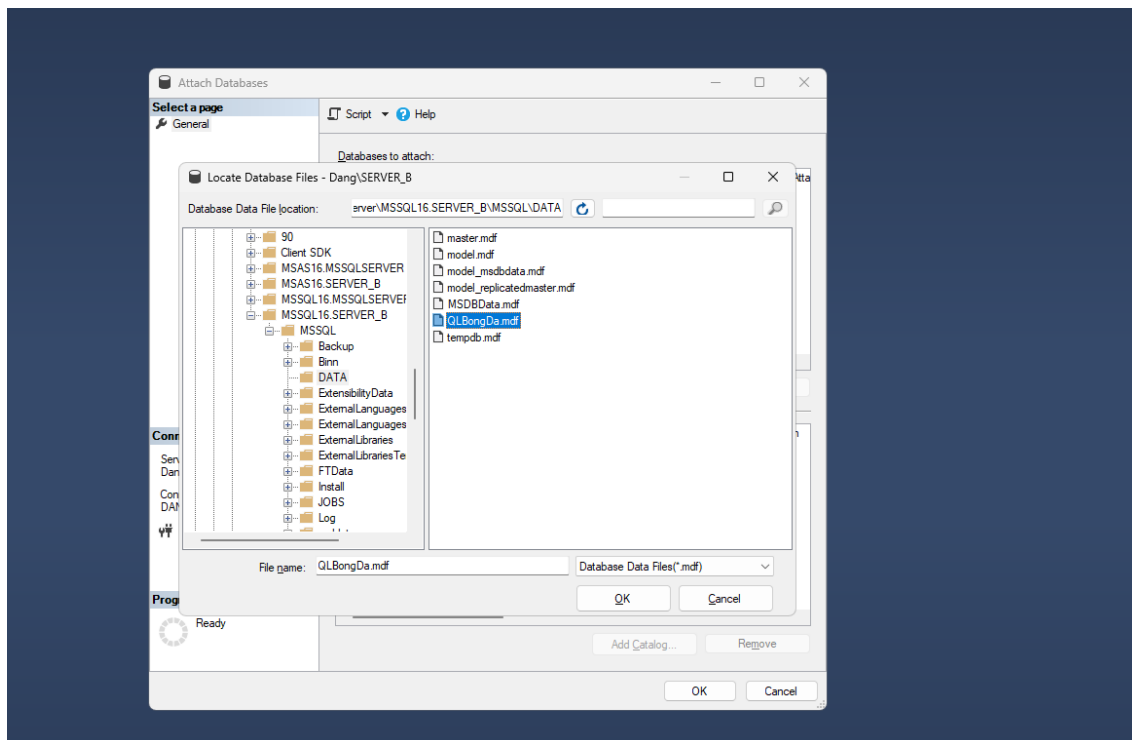


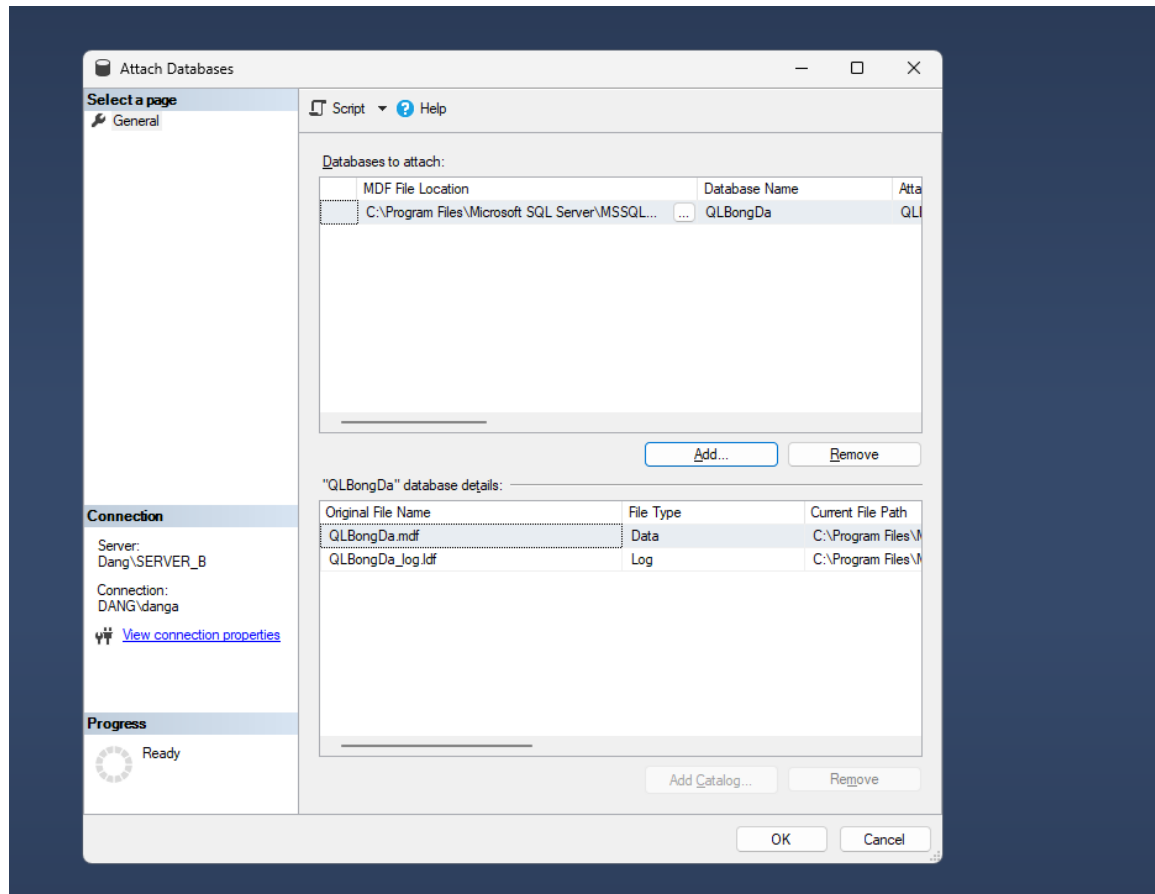
— Thực hiện Attach tại Server B



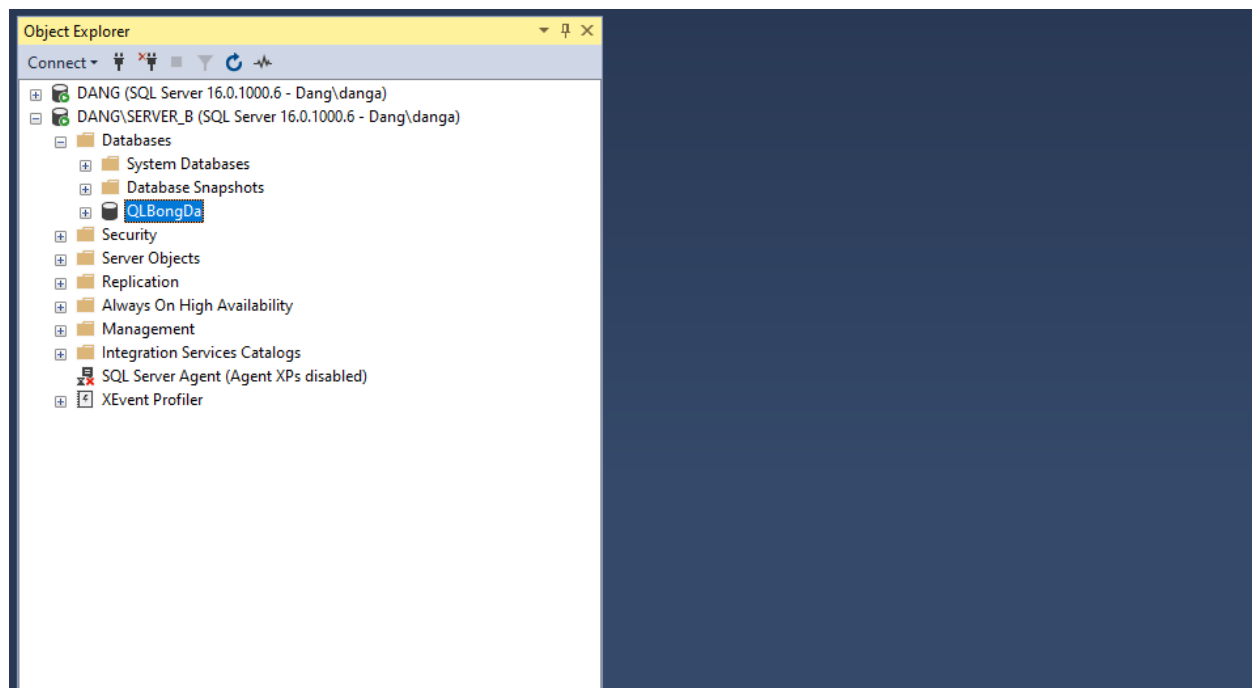


— Chọn file để Attach



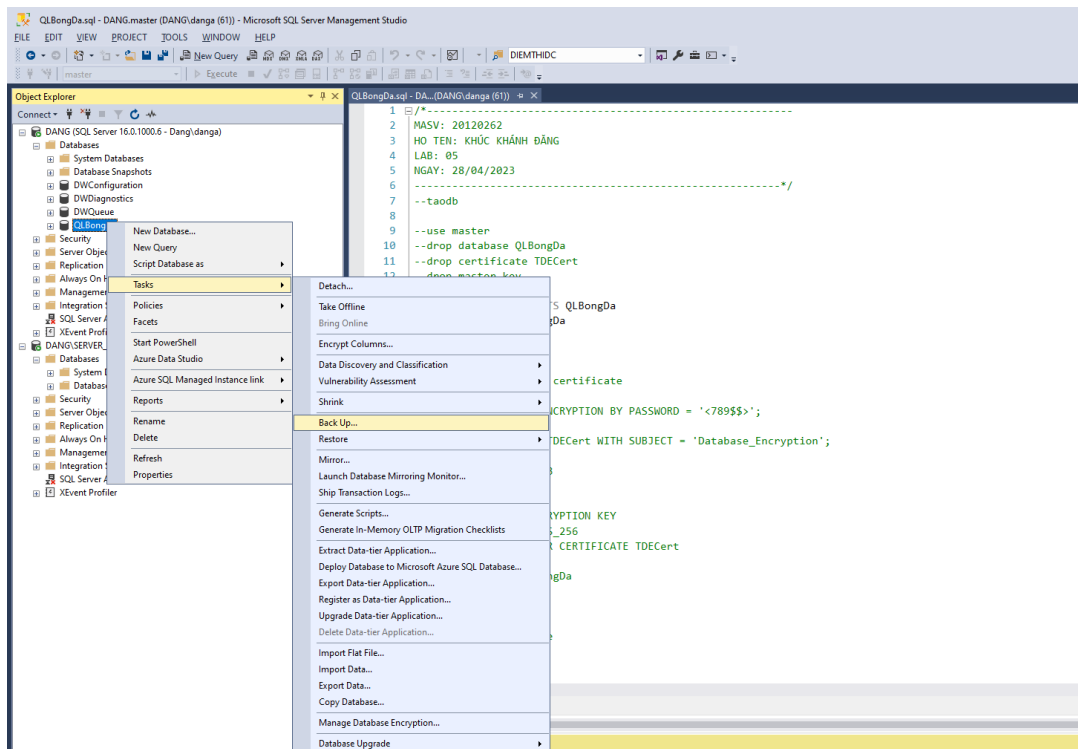


— Attach thành công

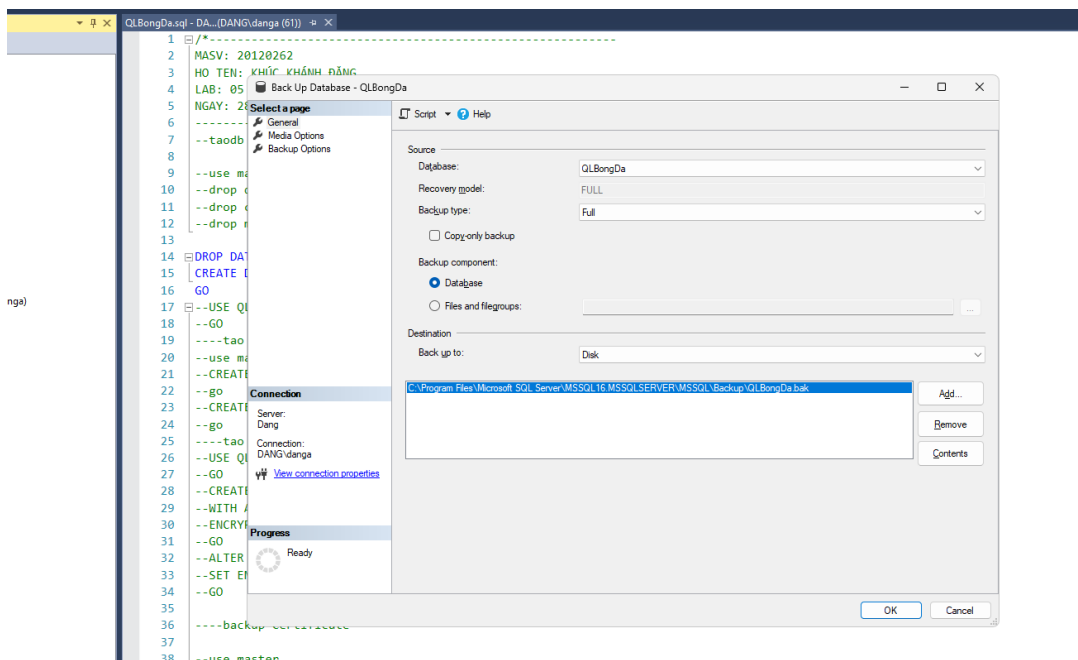


2. Backup – Restore

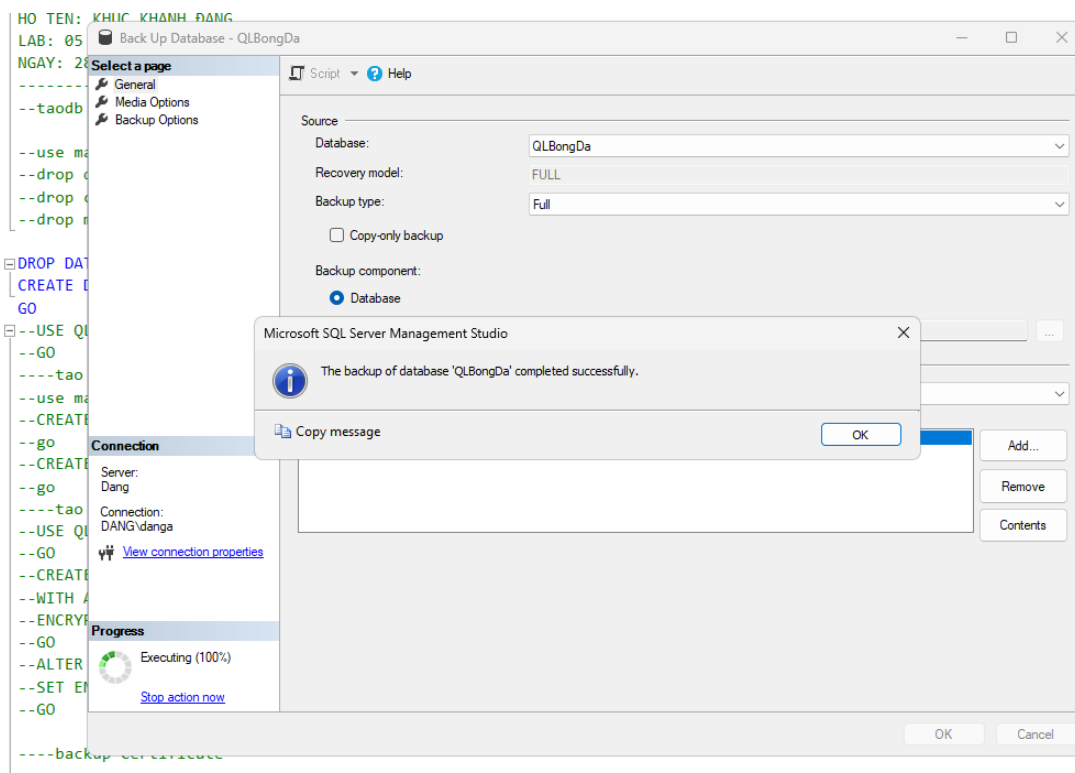
— Tại Server A chọn Back Up Database (QLBongDa)



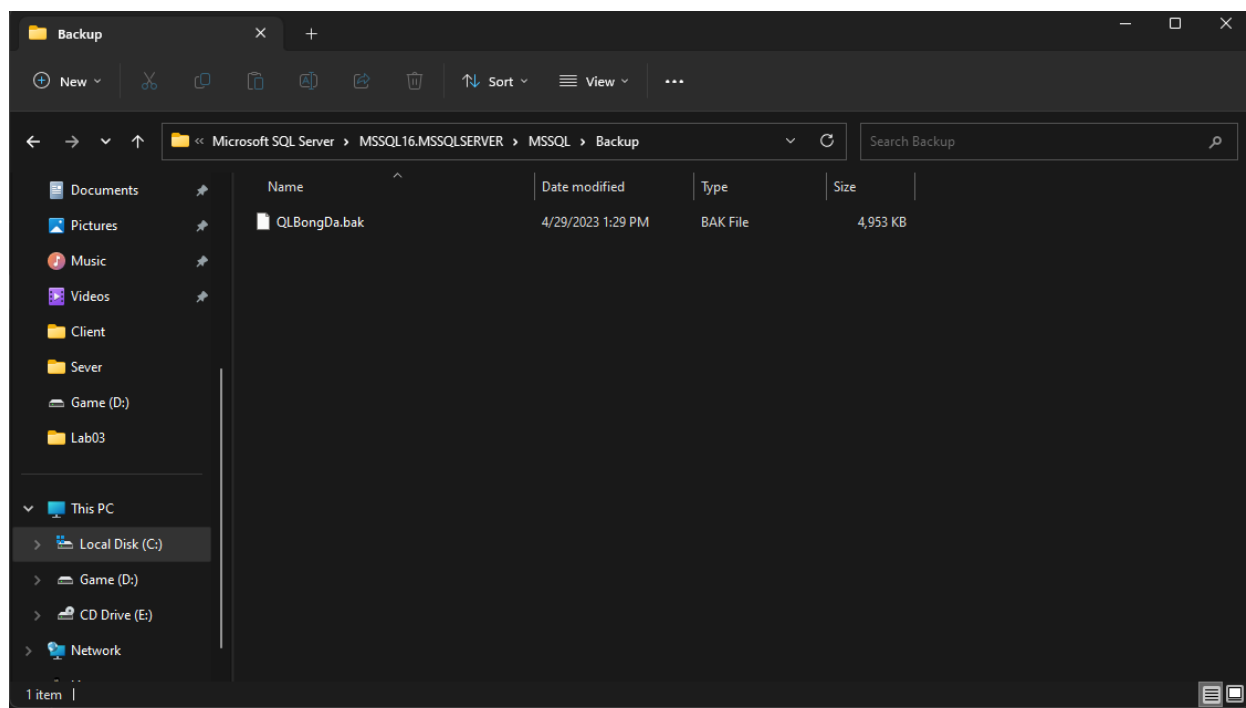
— Backup type là Full

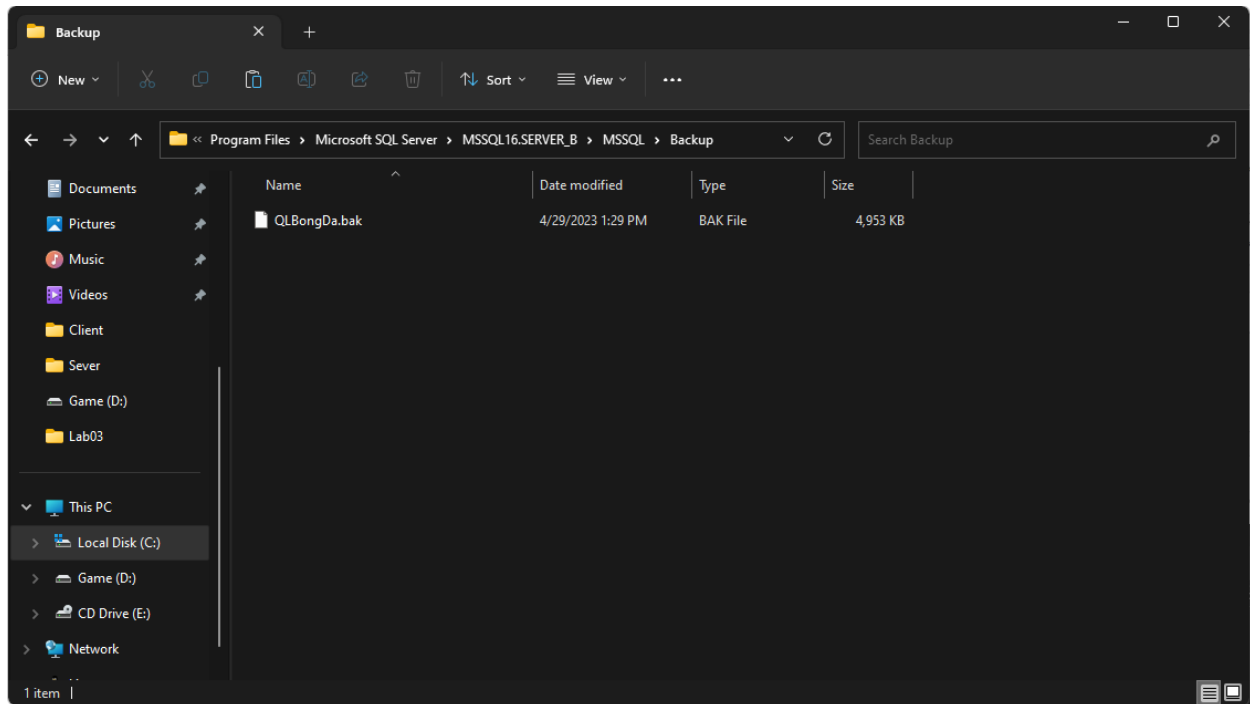


— Tạo file Backup thành công

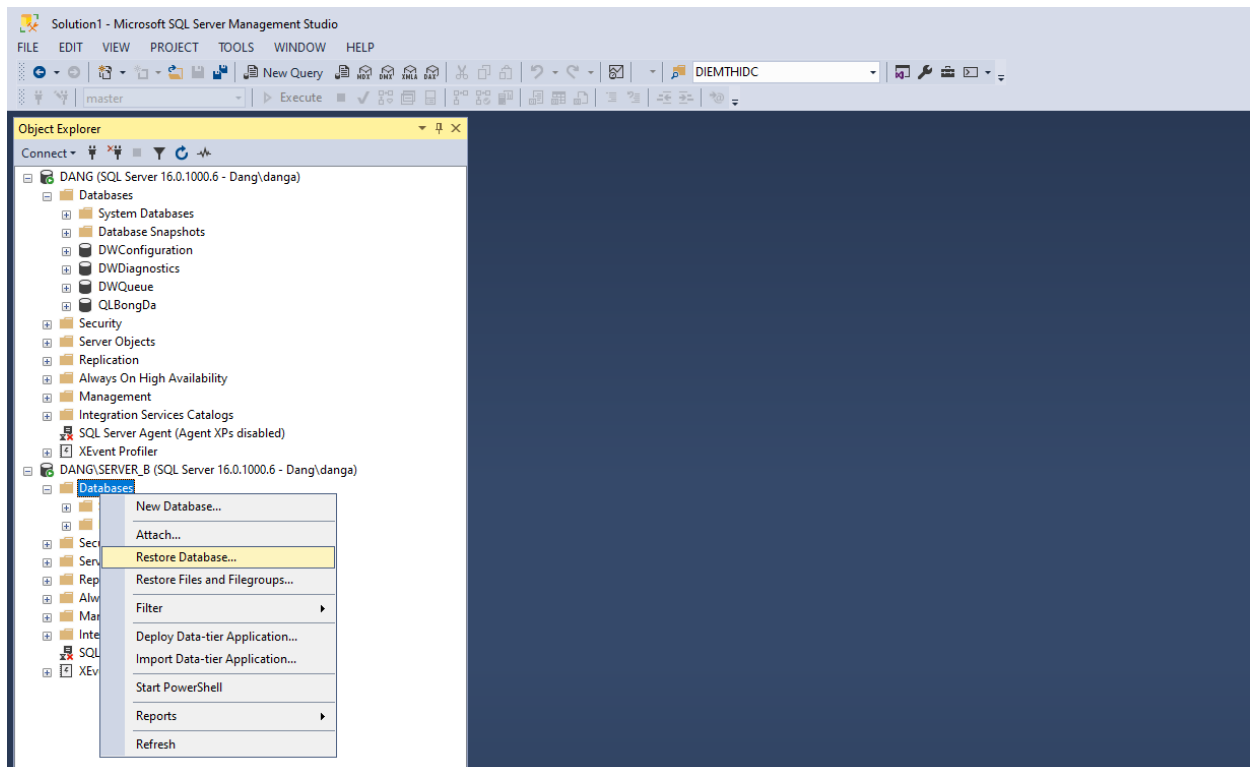


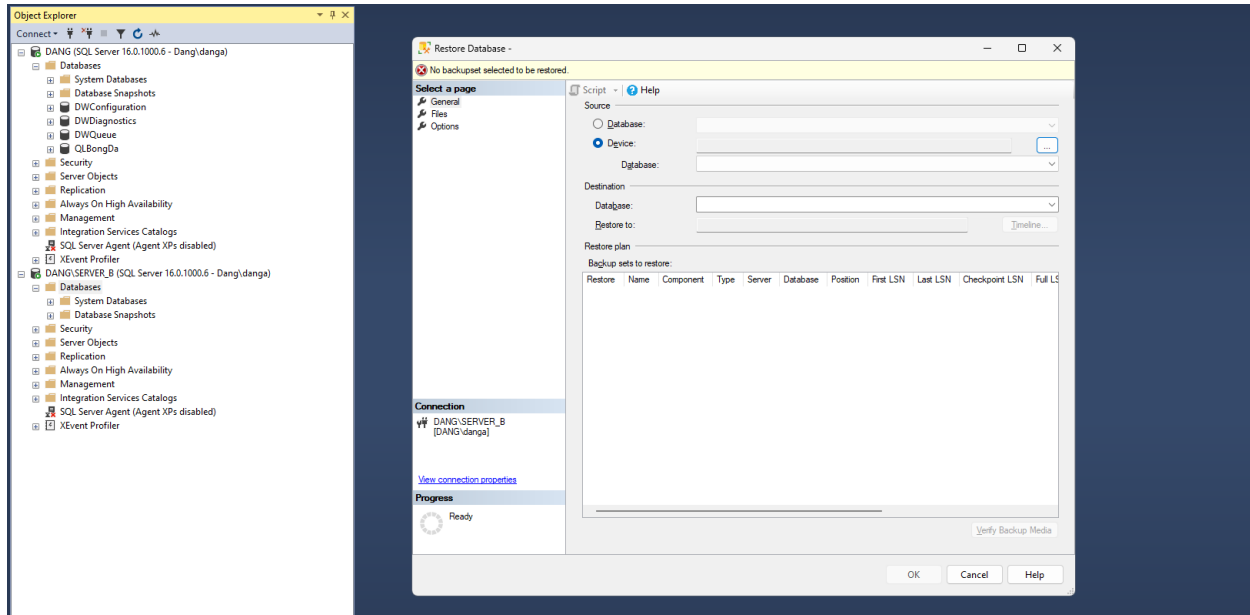
— Copy file Backup từ folder Server A sang folder Server B



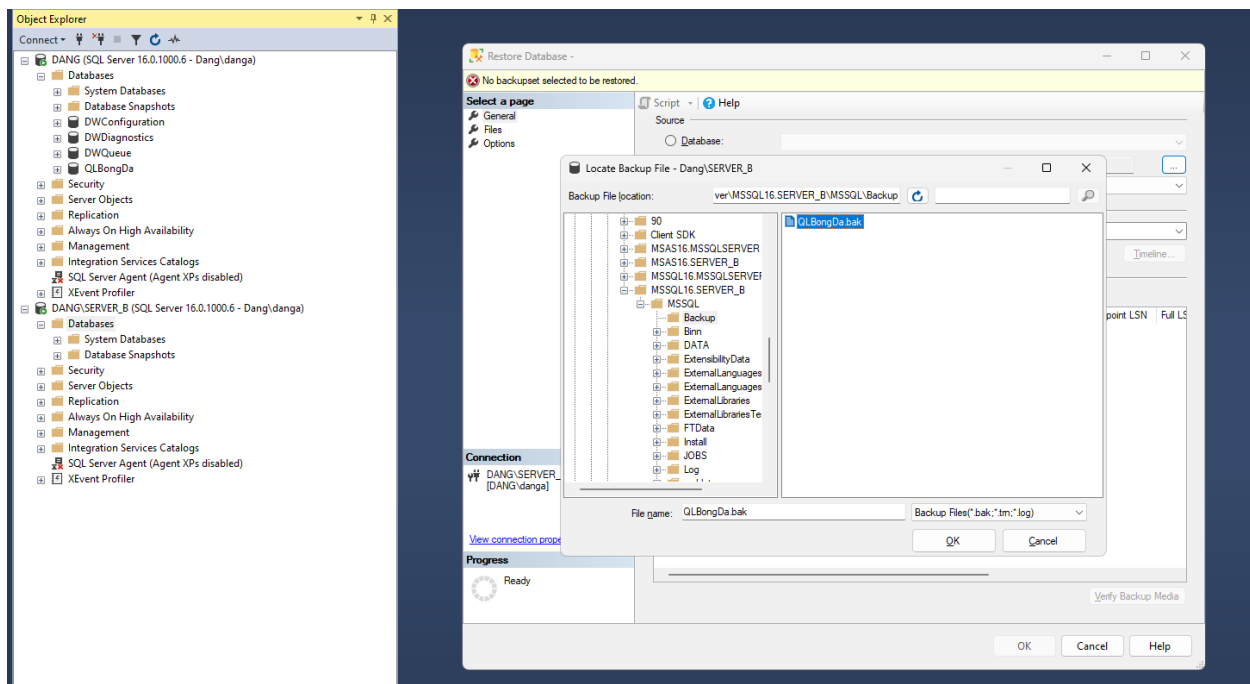


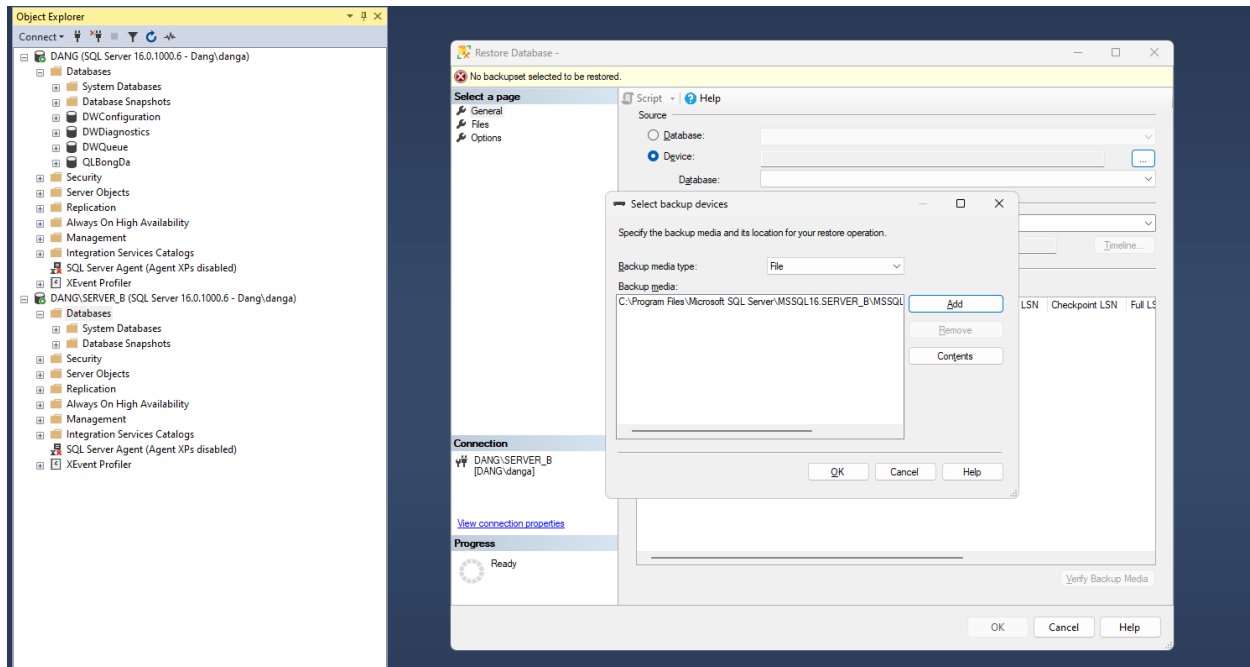
— Thực hiện restore ở Server B



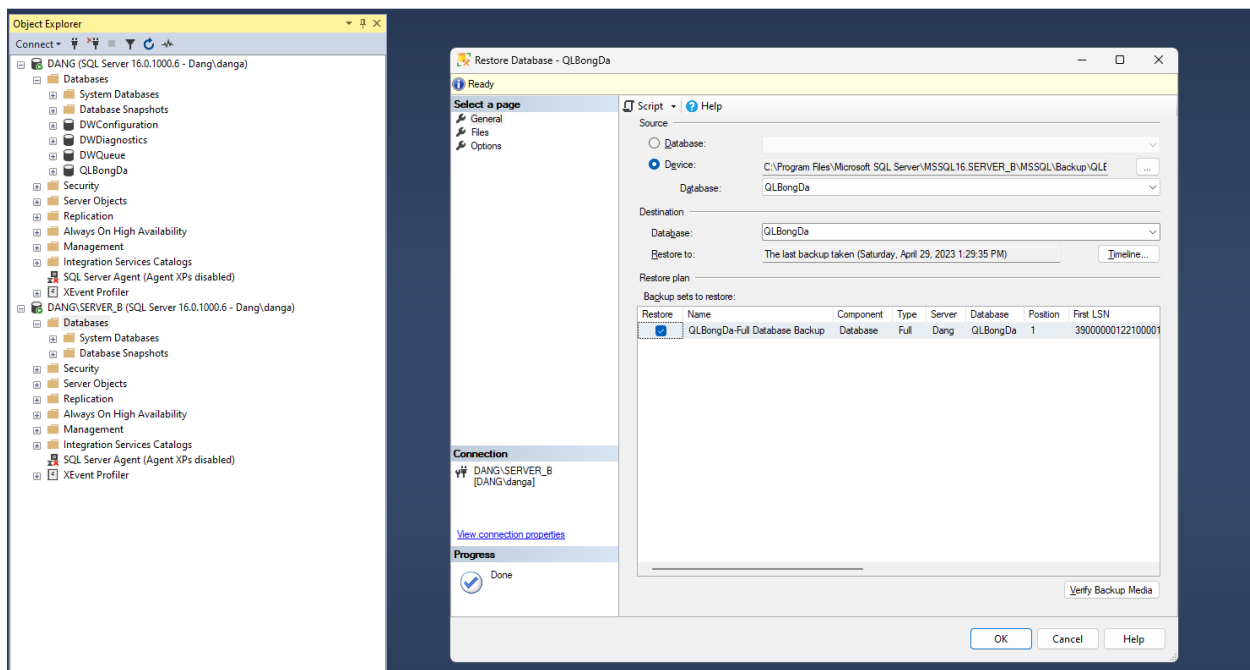


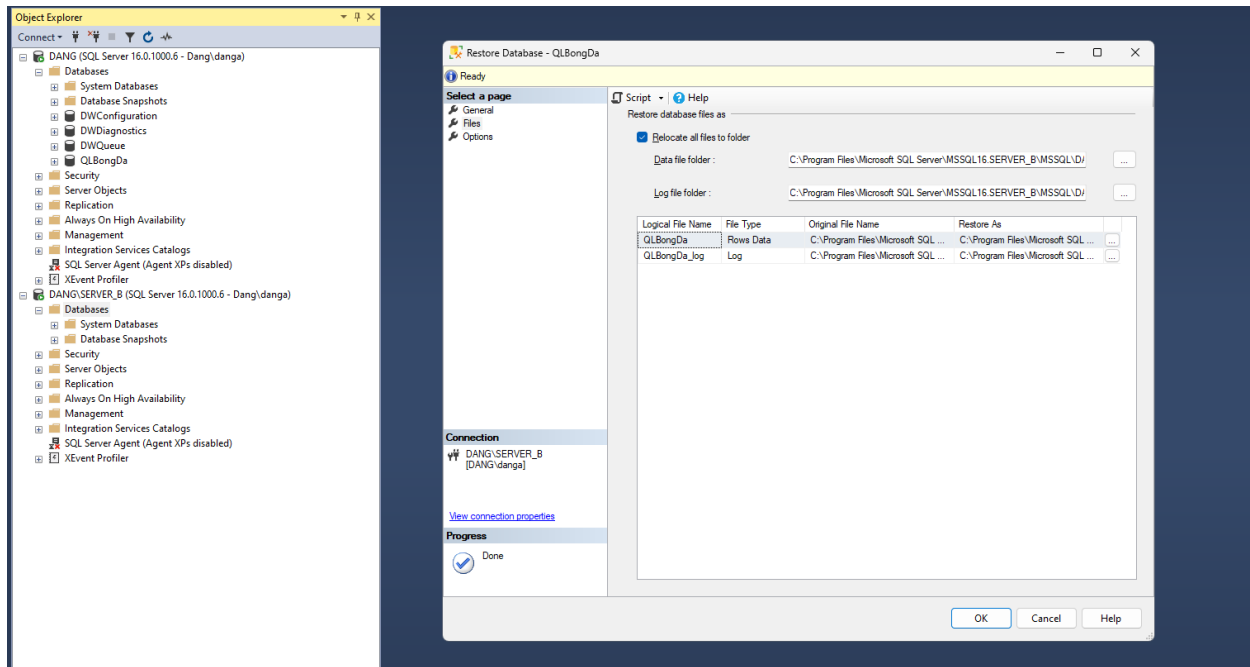
— Chọn file Backup



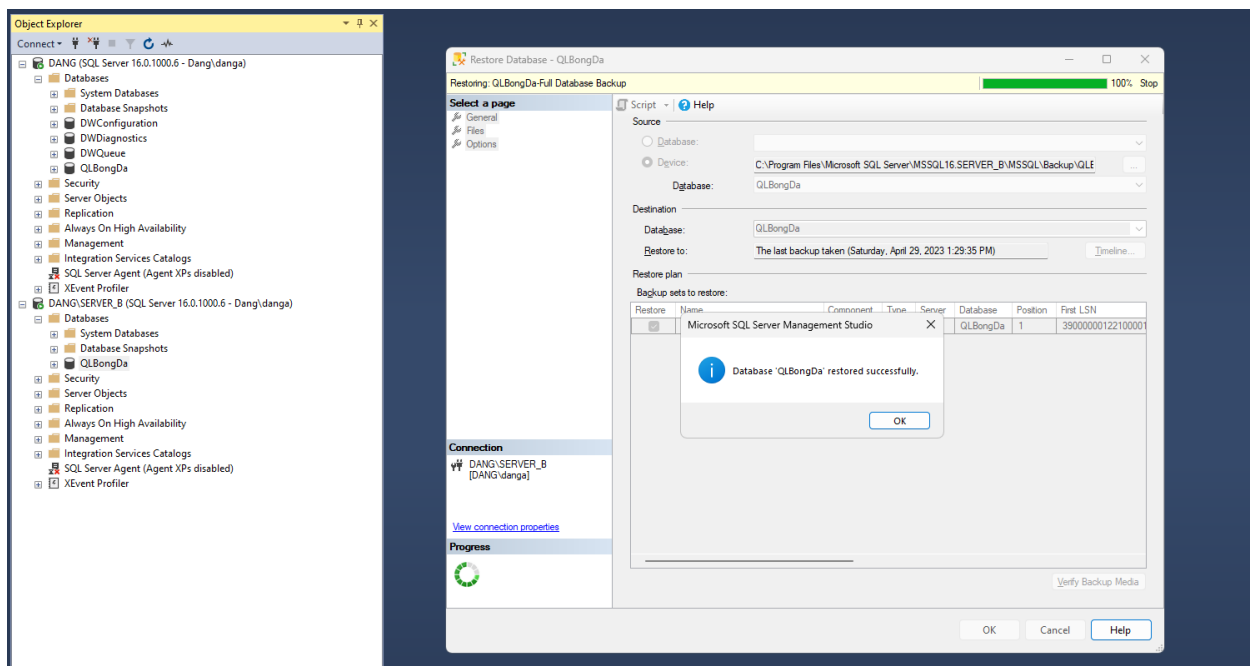


— Đã nhận diện được file Backup, cần thiết lập Relocate all files to folder

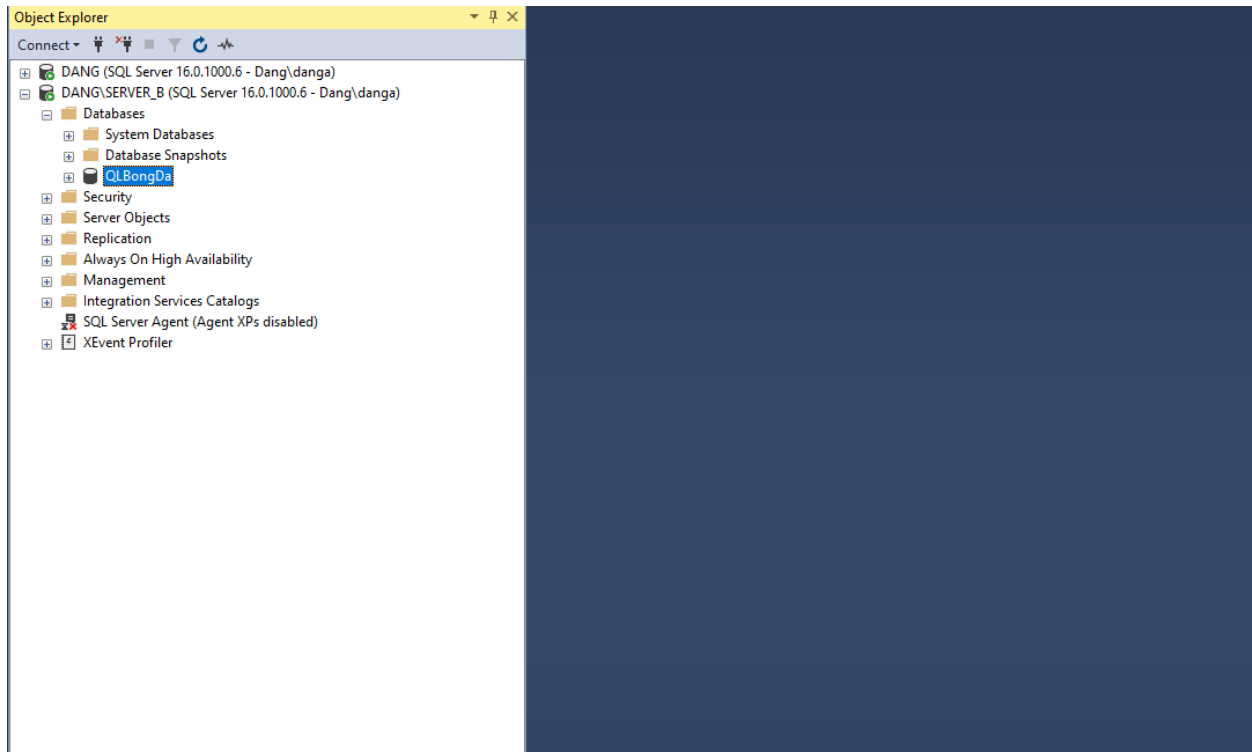




— Restore thành công



— Kết quả của việc Restore



II. Mã hóa TDE cho Database

1. Tạo Master Key và Certificate

```
----TAO MASTER KEY
USE MASTER
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<20120262LAB05>';
GO
-- TẠO CERTIFICATE
USE MASTER
CREATE CERTIFICATE TDESERVERACert WITH SUBJECT = 'Certificate to protect TDE key';
GO
```

2. Tạo Key Mã Hóa DB và Bật Mã Hóa

```

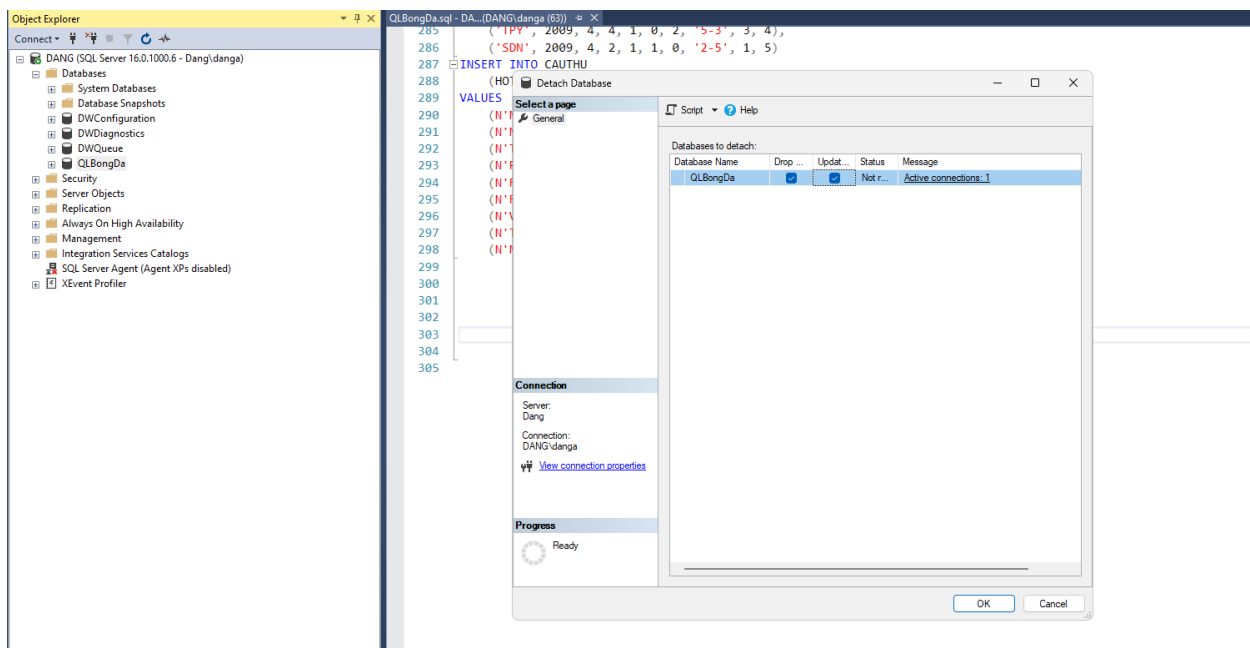
----TAO KEY MA HOA DATABASE
USE QLBongDa;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE TDESERVERACert
GO
--BẬT MÃ HÓA DATABASE
ALTER DATABASE QLBongDa
SET ENCRYPTION ON;
GO

```

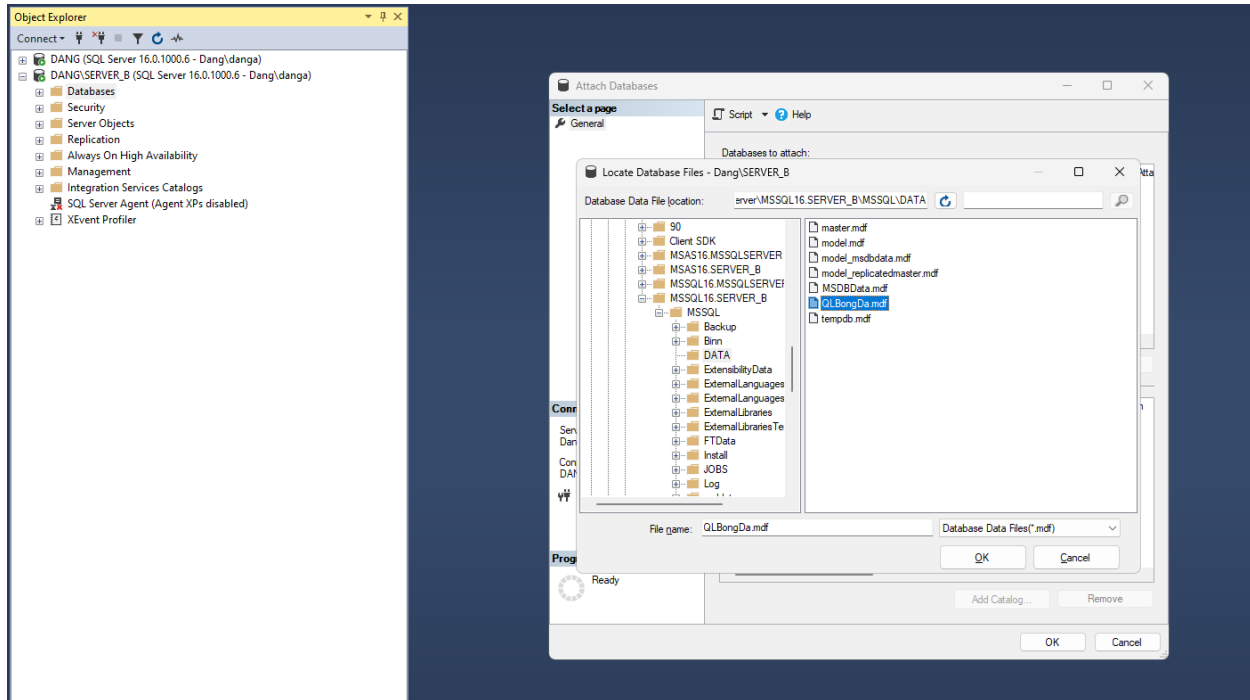
III. Attach – Detach & Backup – Restore với Database có TDE

1. Attach – Detach

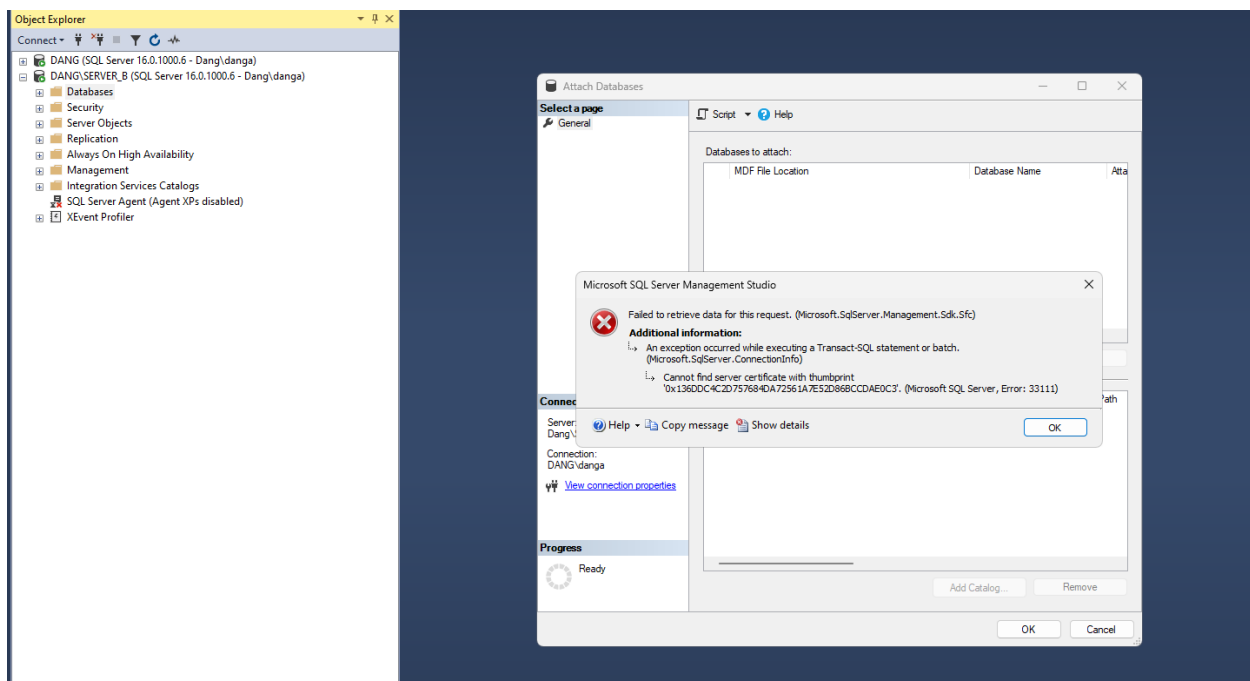
— Ở Server A thực hiện Detach, sau đó copy các file .mdf và .ldf ở folder Server A sang folder của Server B



— Tại Server B tiến hành chọn file Attach

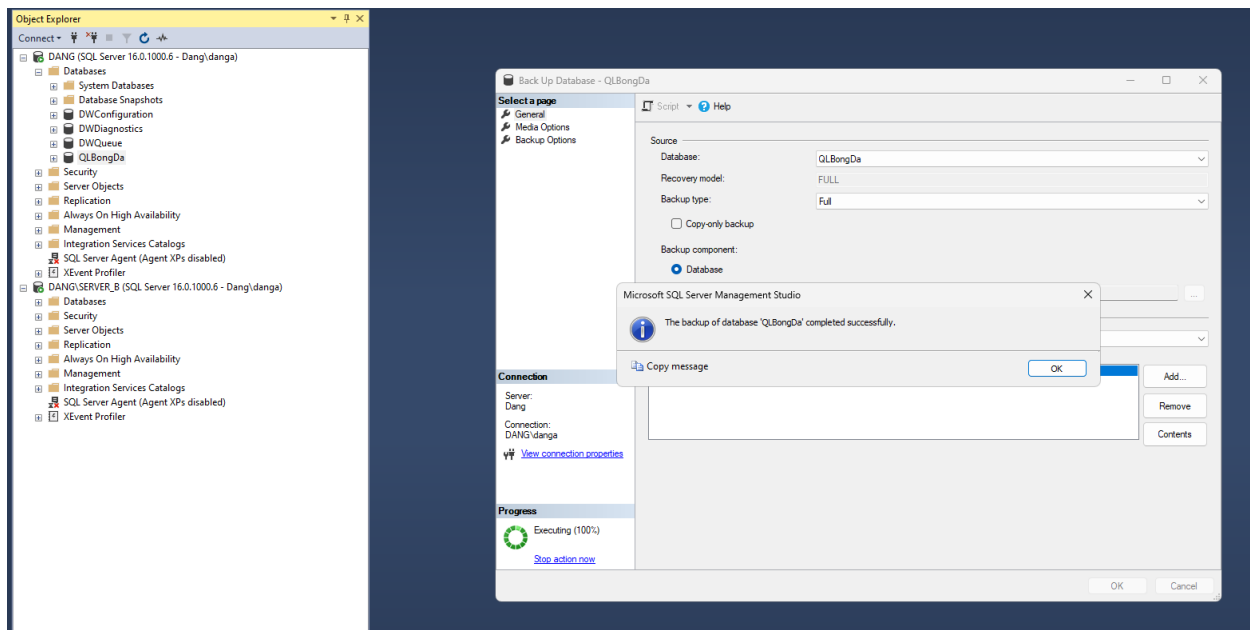
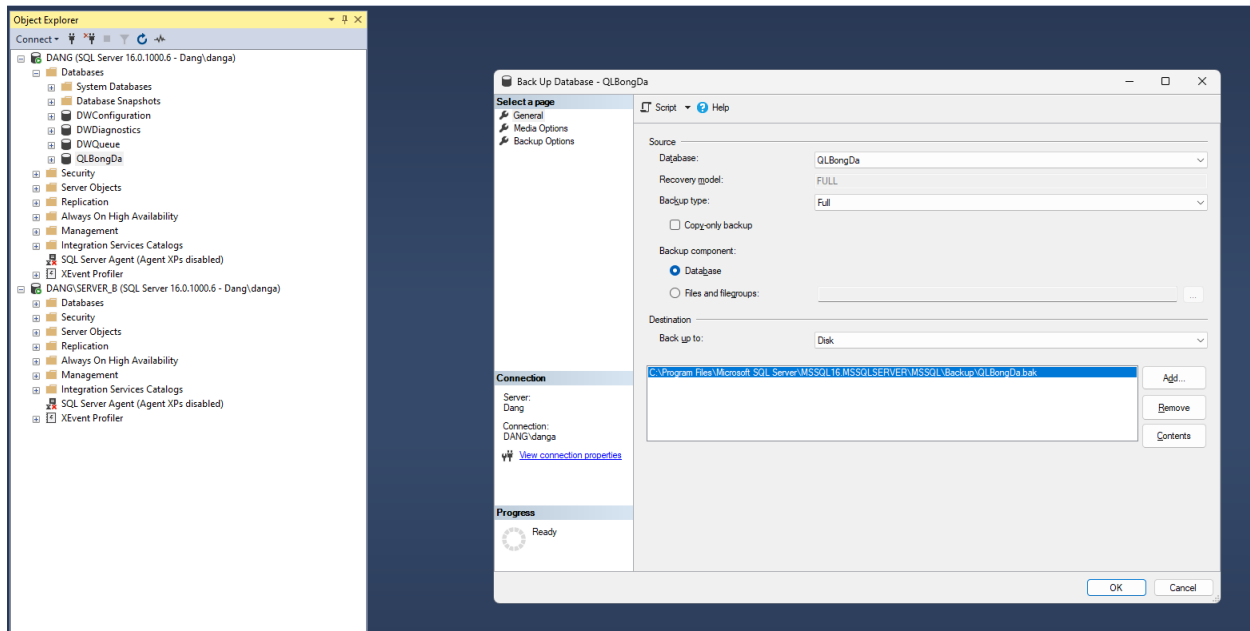


— Attach thất bại Certificate và Key mã hóa Database từ Server A

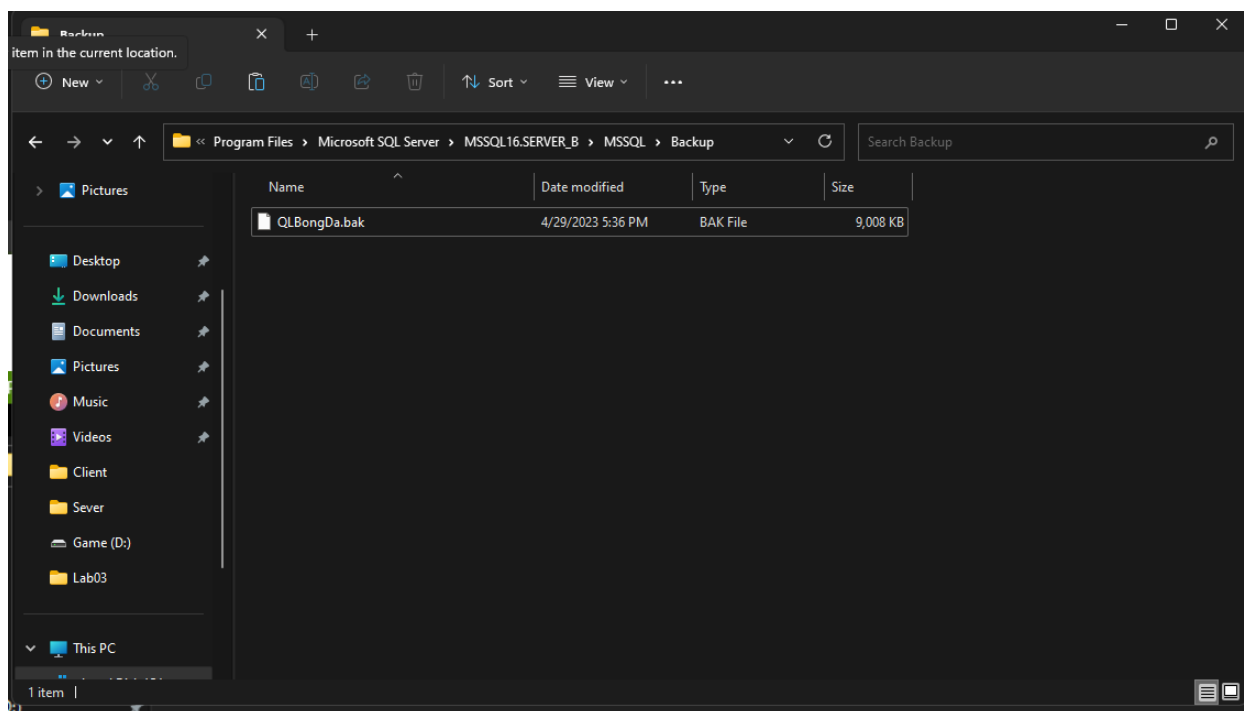
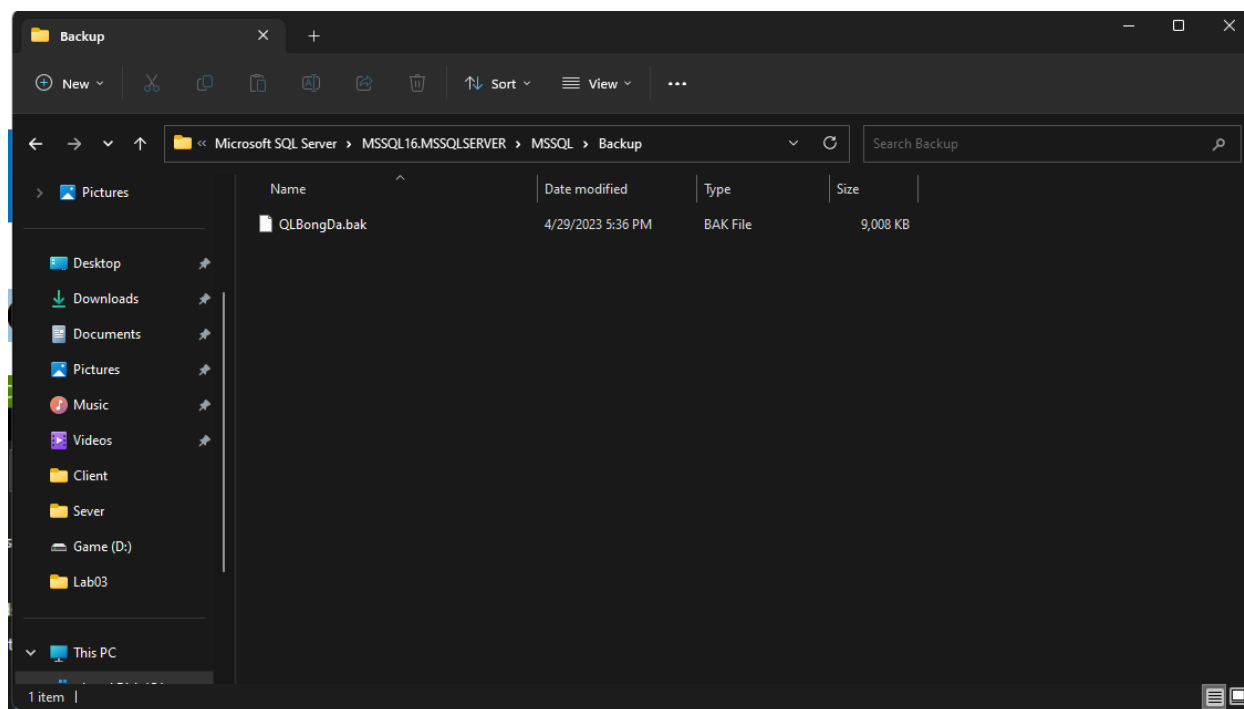


2. Backup – Restore

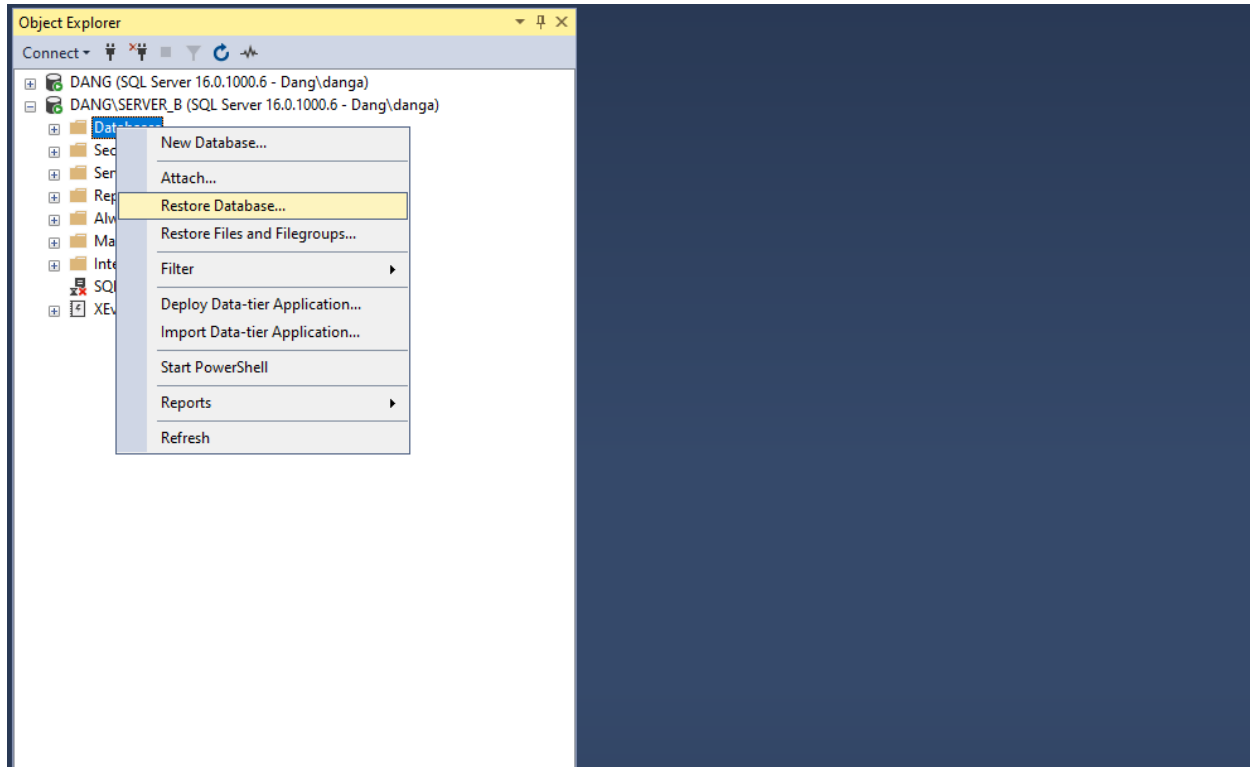
— Tại Server chính tiến hành tạo file Backup



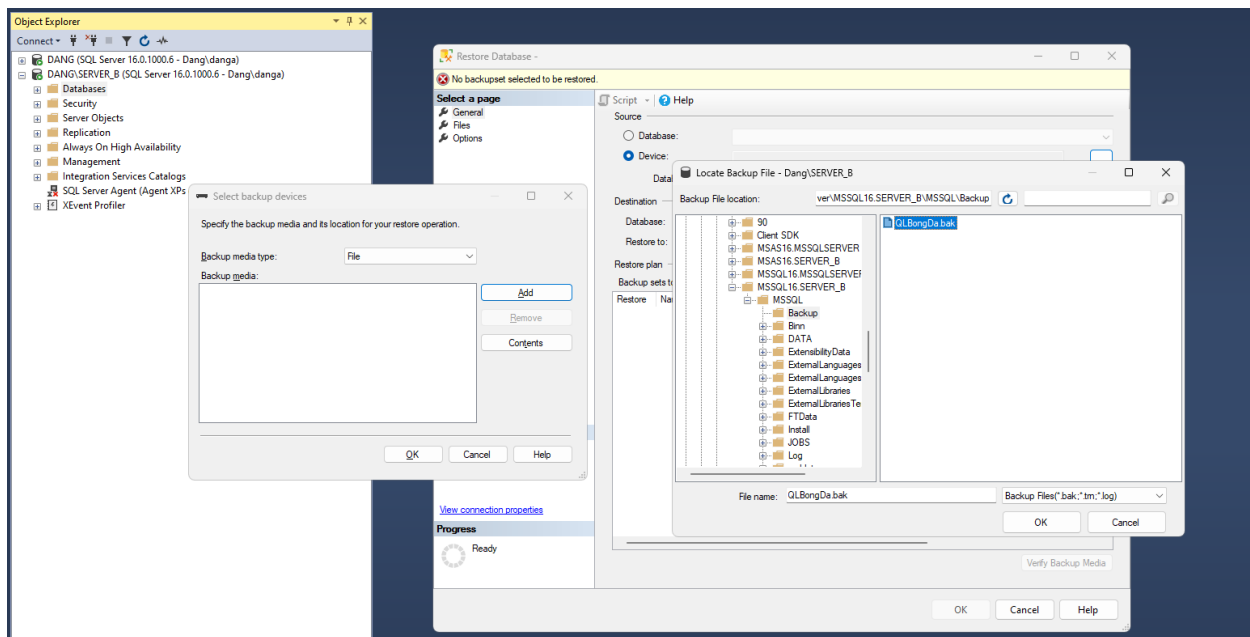
— Copy file Backup từ folder Server A qua folder Server B

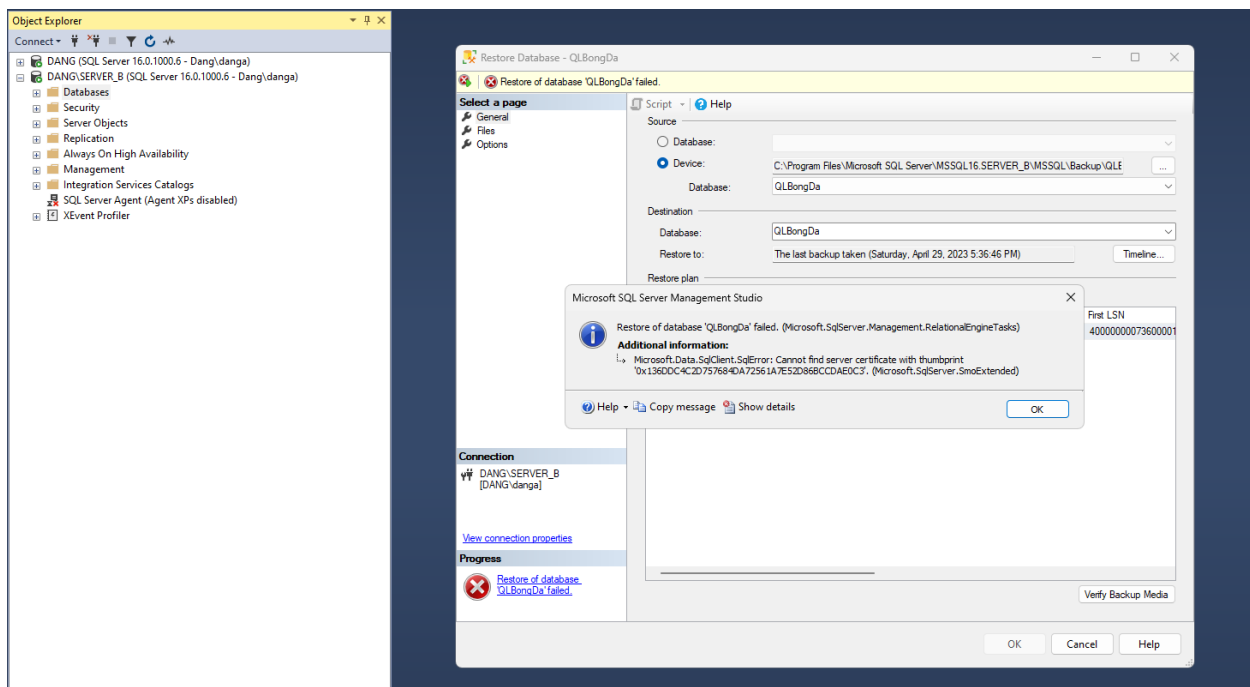
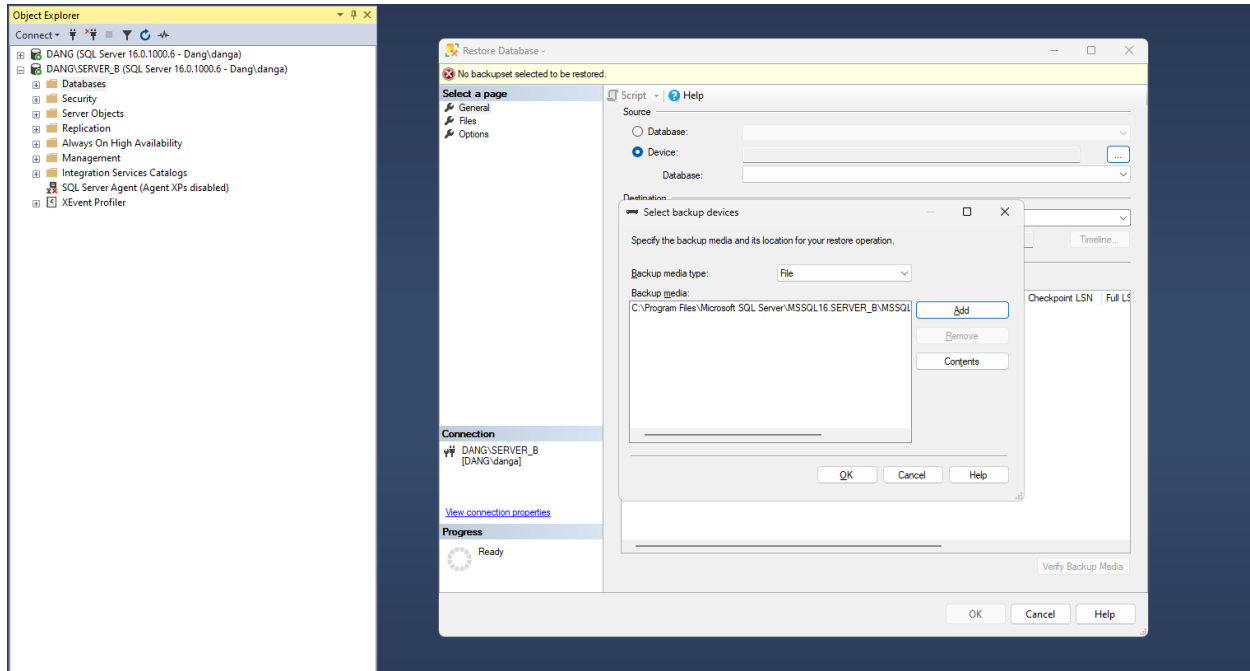


— Tiến hành Restore tại Server B



— Chọn file Backup





IV. Giải pháp

— Ta cần phải backup lại Certificate dùng để mã hóa dữ liệu ở Server A và khôi phục lại Certificate đó để giải mã dữ liệu ở Server B kia. Sau khi Restore thành công Certificate thì Database QLBongDa có thể được Attach và Restore lại như bình thường

- Backup lại Certificate ở server ban đầu

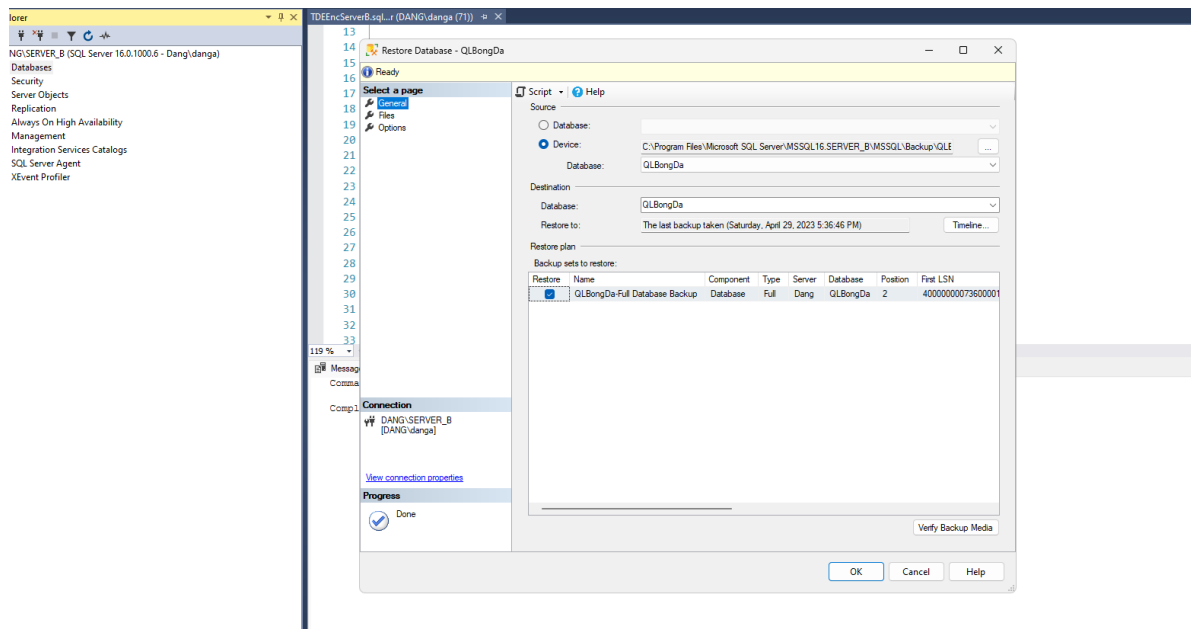
----BACKUP CERTIFICATE

USE MASTER

GO

```
BACKUP CERTIFICATE TDESERVERACert to file = 'D:\LAB05_Certificate_Backup.cer'
with private key(
file = 'D:\LAB05_PK_Backup.pvk',
ENCRYPTION BY PASSWORD = '123abc')
```

- Khôi phục lại Certificate ở server ban đầu từ file back up, file private key và phải mật khẩu dùng để mã hóa Certificate đó



```
--CAC CAU LENH DE THUC HIEN MA HOA
USE MASTER;
go
drop certificate TDESERVERBCert
drop master key

USE MASTER;
GO
CREATE MASTER KEY ENCRYPTION
BY PASSWORD = '20120262LAB05';
GO

CREATE CERTIFICATE TDESERVERBCert
FROM FILE = N'D:\LAB05_Certificate_Backup.cer'
WITH PRIVATE KEY (
    FILE = N'D:\LAB05_PK_Backup.pvk',
    DECRYPTION BY PASSWORD = '123abc'
);
GO
```

