

ĐẠI HỌC QUỐC GIA TPHCM
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN

BỘ MÔN MẠNG MÁY TÍNH VÀ VIỄN THÔNG HƯỚNG AN TOÀN THÔNG TIN

Báo cáo Lab 5

Đề tài: Mã hóa dữ liệu trong suốt Transparent Data Encryption – TDE

Môn học: Bảo mật Cơ sở dữ liệu

Sinh viên thực hiện:

Lưu Thành Đạt (22127063)

Mai Xuân Thường (22127409)

Giáo viên hướng dẫn:

Ths. Nguyễn Thị Hường

Ngày 11 tháng 4 năm 2025



Mục lục

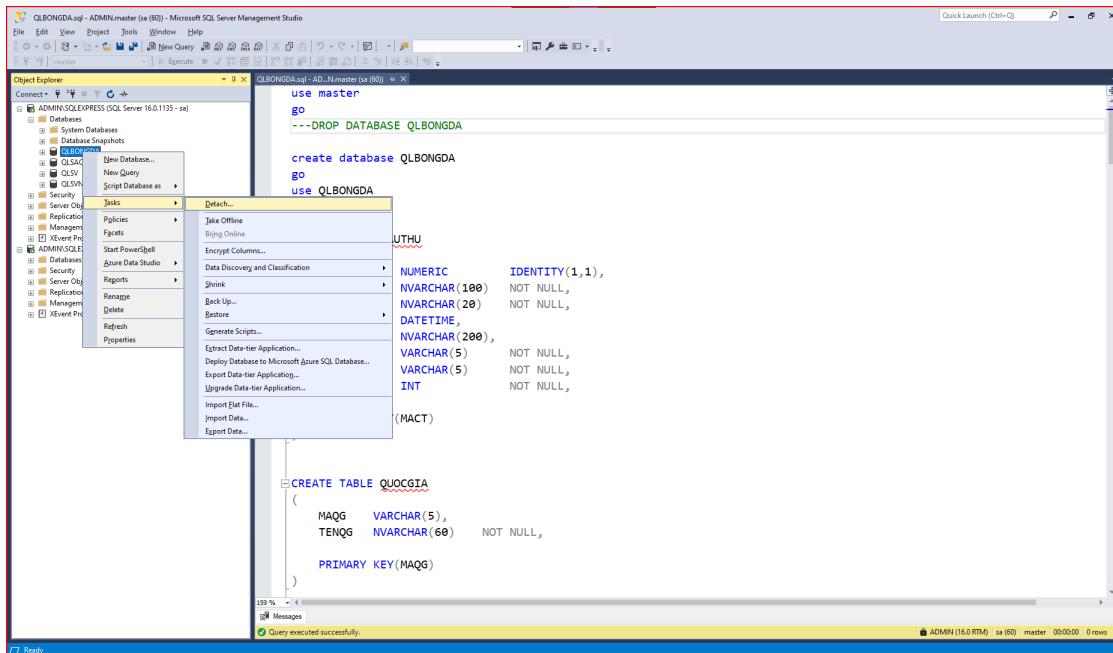
1 Phân công	1
2 Detach & Attach CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia V-League” trong Lab02 từ server A sang server B _ Nhận xét kết quả Attach file	1
3 Backup & Restore CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia V-League” trong Lab02 từ server A sang server B _ Nhận xét kết quả Attach file	8
4 Viết script mã hóa CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia V-League” trong Lab02 sử dụng TDE.	13
5 Thực hiện Detach và Attach CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia VLeague” trong Lab02 đã mã hóa TDE từ server A sang server B.	15
6 Nếu kết quả câu d là thất bại, mô tả các bước thực hiện để xử lý lỗi trên	17
7 Thực hiện Backup và Restore CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia VLeague” trong Lab02 đã mã hóa TDE từ server A sang server B.	21
8 Nếu kết quả câu f là thất bại, mô tả các bước thực hiện để xử lý lỗi trên	22

1 Phân công

MSSV	Họ tên	Công việc	Mức độ hoàn thành
22127063	Lưu Thành Đạt	Câu a), c), d) và e) Viết báo cáo	100%
22127409	Mai Xuân Thường	Câu b), f) và g) Viết báo cáo	100%

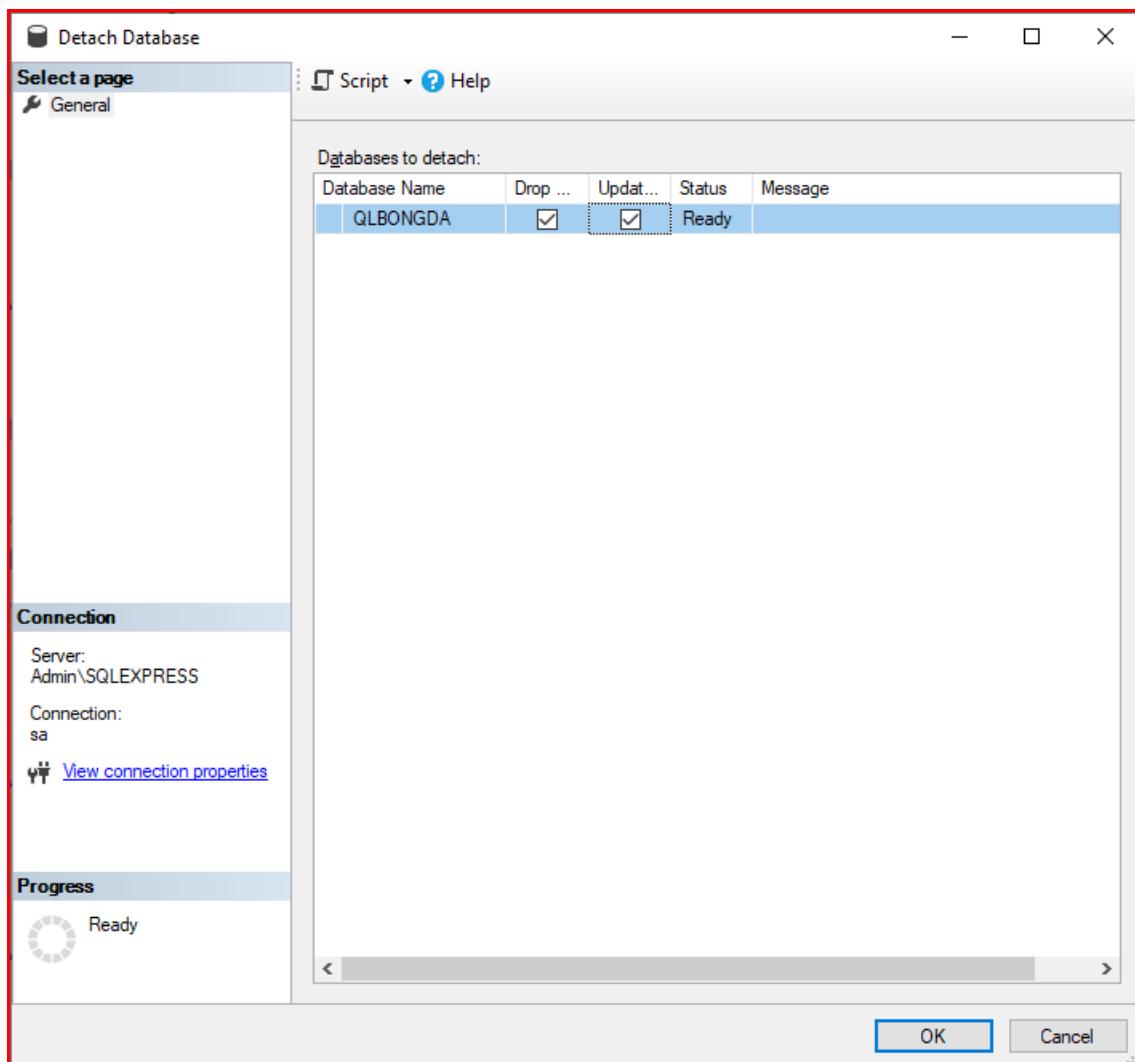
Bảng 1: Bảng phân công công việc

2 Detach & Attach CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia V-League” trong Lab02 từ server A sang server B _ Nhận xét kết quả Attach file



Hình 1: Chọn detach database QLBongDa

Báo cáo Lab 5



Hình 2: Detach database QLBongDa

Báo cáo Lab 5

```

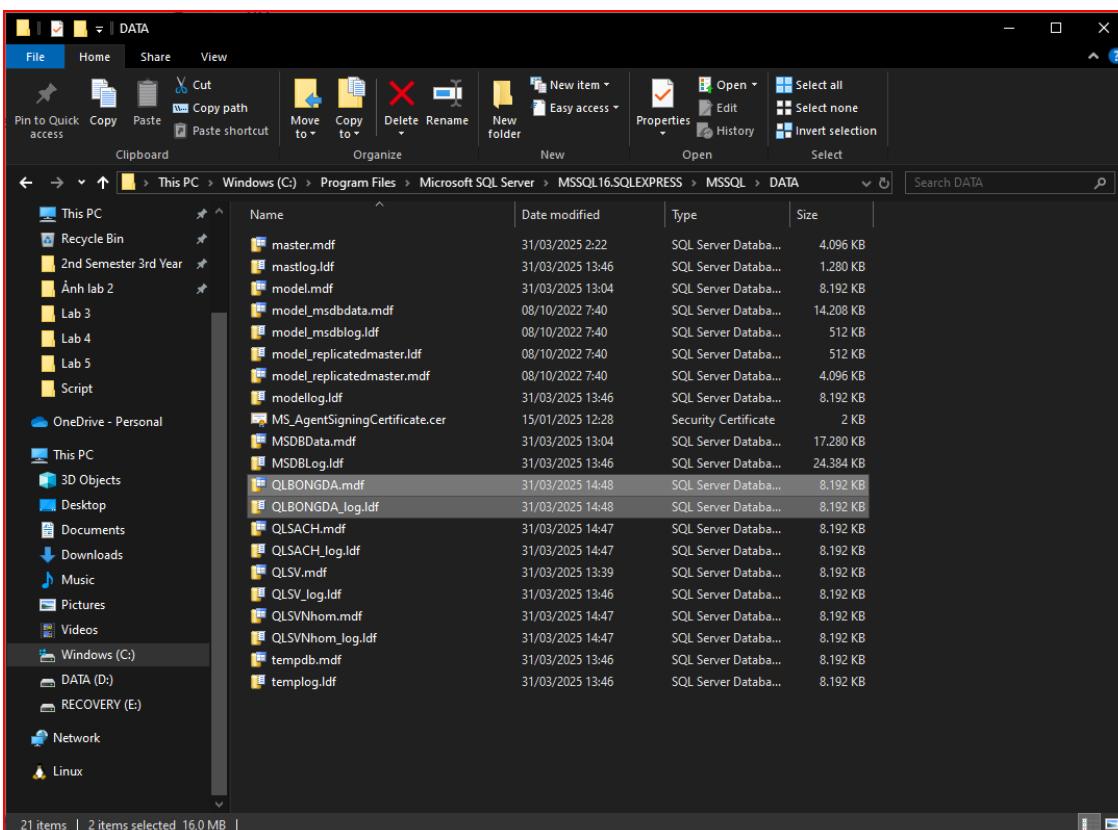
File Edit View Project Tools Window Help
File Edit View Project Tools Window Help
Object Explorer Connect > New Query > Execute > Back Forward > Home > Refresh > Stop > Close > Back Launch (Ctrl+Q) >
QLBONGDA.sql - ADMIN.master (sa (60)) - Microsoft SQL Server Management Studio
ADMIN\SQLEXPRESS (SQL Server 16.0.1135 - sa)
Databases System Databases QLSV QLSVnhom
Replication Management XEvent Profiler
ADMIN\SQLEXPRESS2 (SQL Server 16.0.1000 - sa)
Databases Security Replication Management XEvent Profiler
use master
go
---DROP DATABASE QLBONGDA
create database QLBONGDA
go
use QLBONGDA
go

CREATE TABLE CAUTHU
(
    MACT      NUMERIC      IDENTITY(1,1),
    HOTEN    NVARCHAR(100) NOT NULL,
    VITRI     NVARCHAR(20)  NOT NULL,
    NGAYSINH  DATETIME,
    DIACHI    NVARCHAR(200),
    MACLB    VARCHAR(5)   NOT NULL,
    MAQG     VARCHAR(5)   NOT NULL,
    SO        INT          NOT NULL,
    PRIMARY KEY(MACT)
)

CREATE TABLE QUOCGIA
(
    MAQG    VARCHAR(5),
    TENQG   NVARCHAR(60) NOT NULL,
    PRIMARY KEY(MAQG)
)
159 % < Messages > Query executed successfully.
ADMIN (16.0 RTM) | sa (60) | master | 00:00:00 | 0 rows
Ready

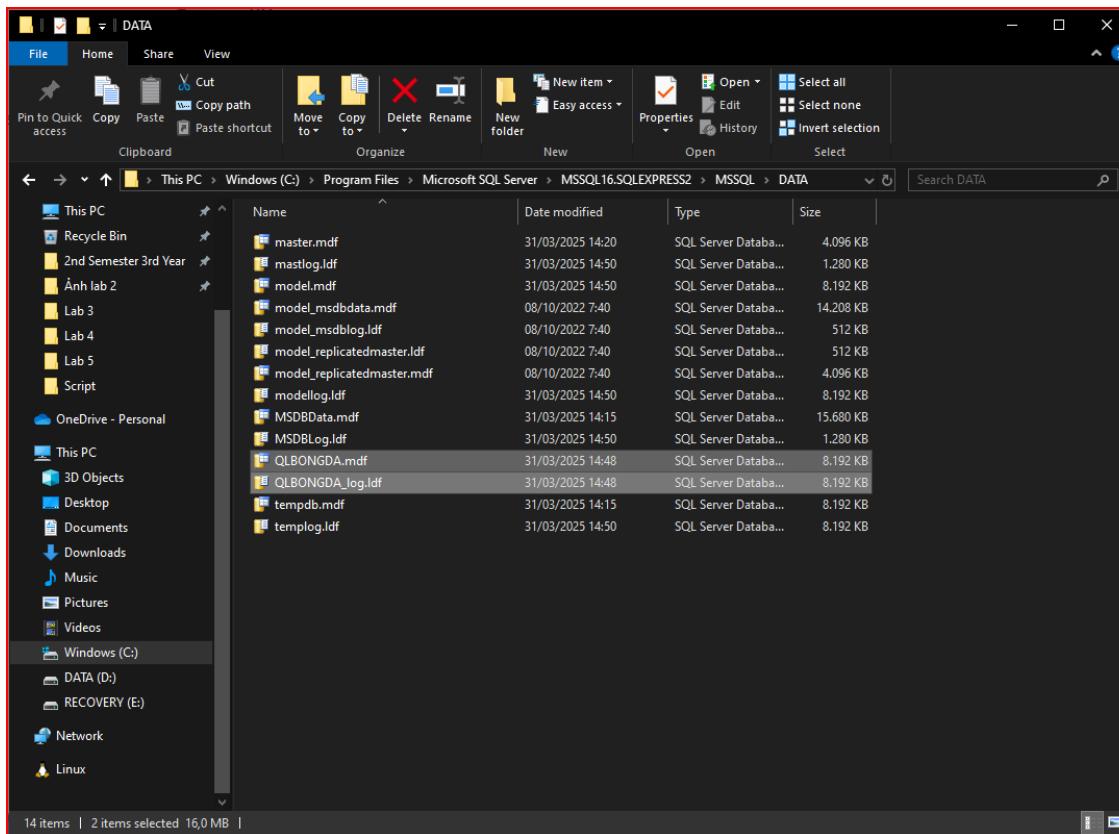
```

Hình 3: Kết quả sau khi detach

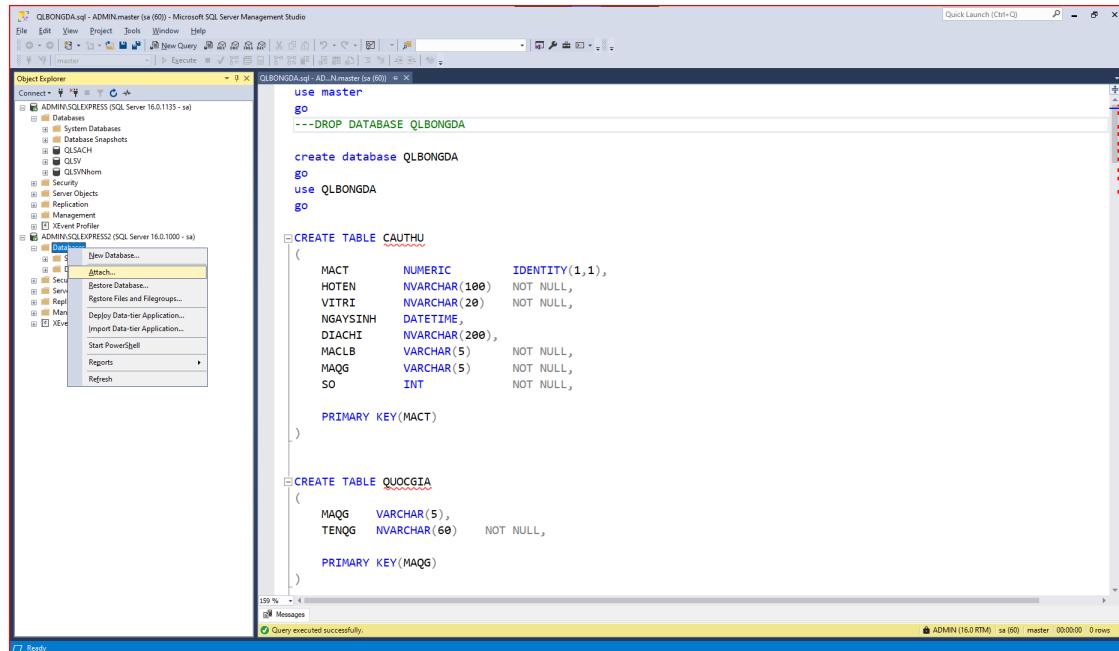


Hình 4: Copy 2 file .mdf và .ldf từ server A sang server B

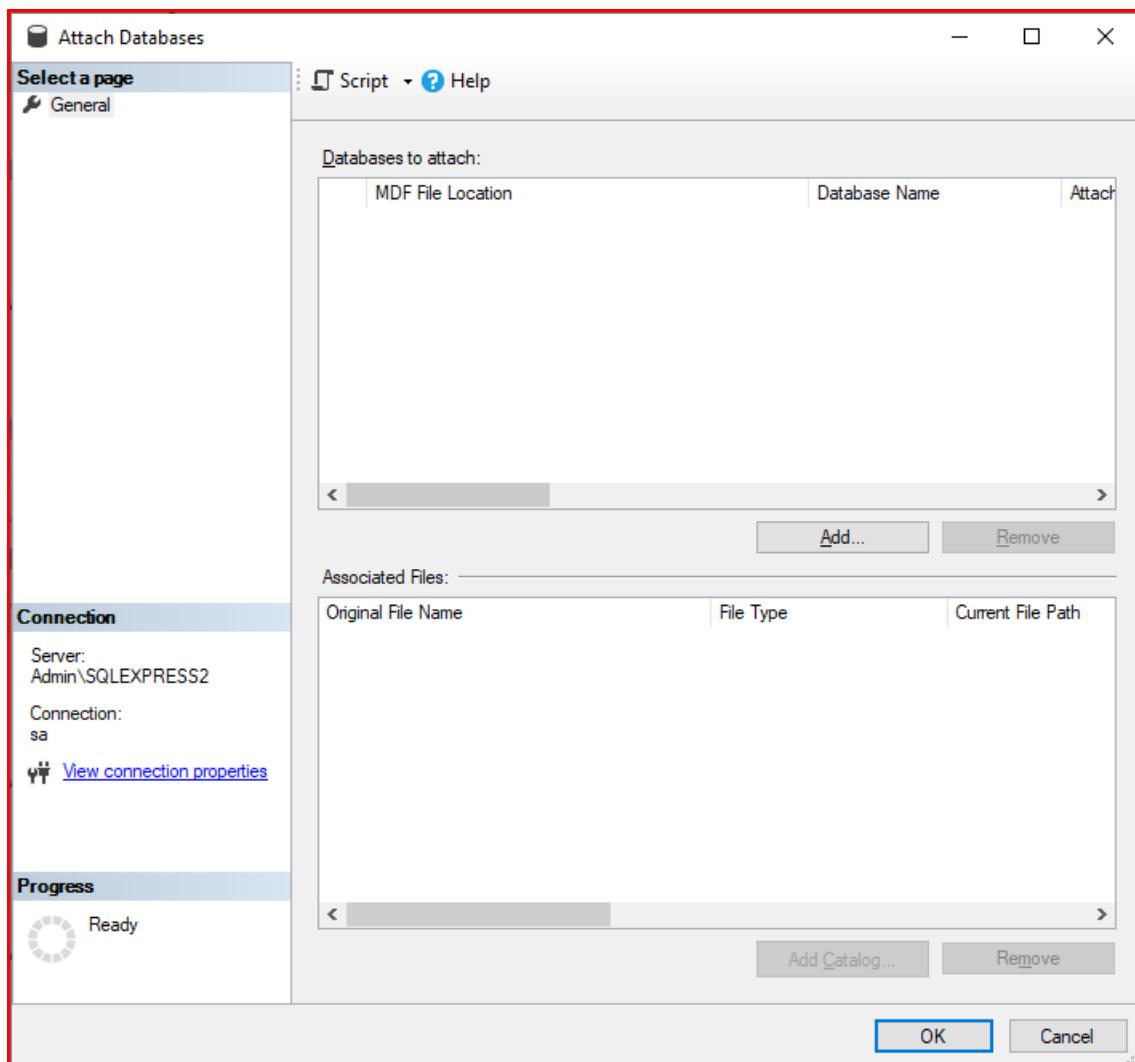
Báo cáo Lab 5



Hình 5: Copy 2 file .mdf và .ldf từ server A sang server B

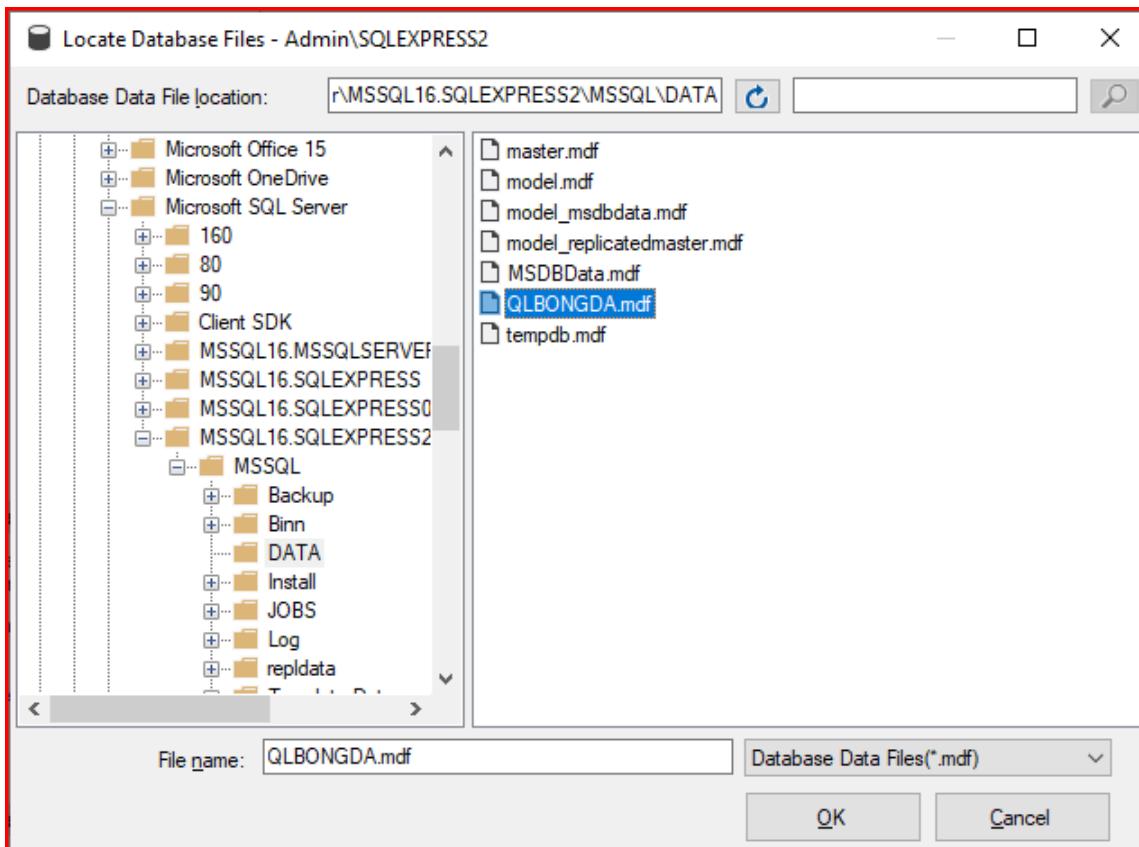


Hình 6: Chọn attach thêm database



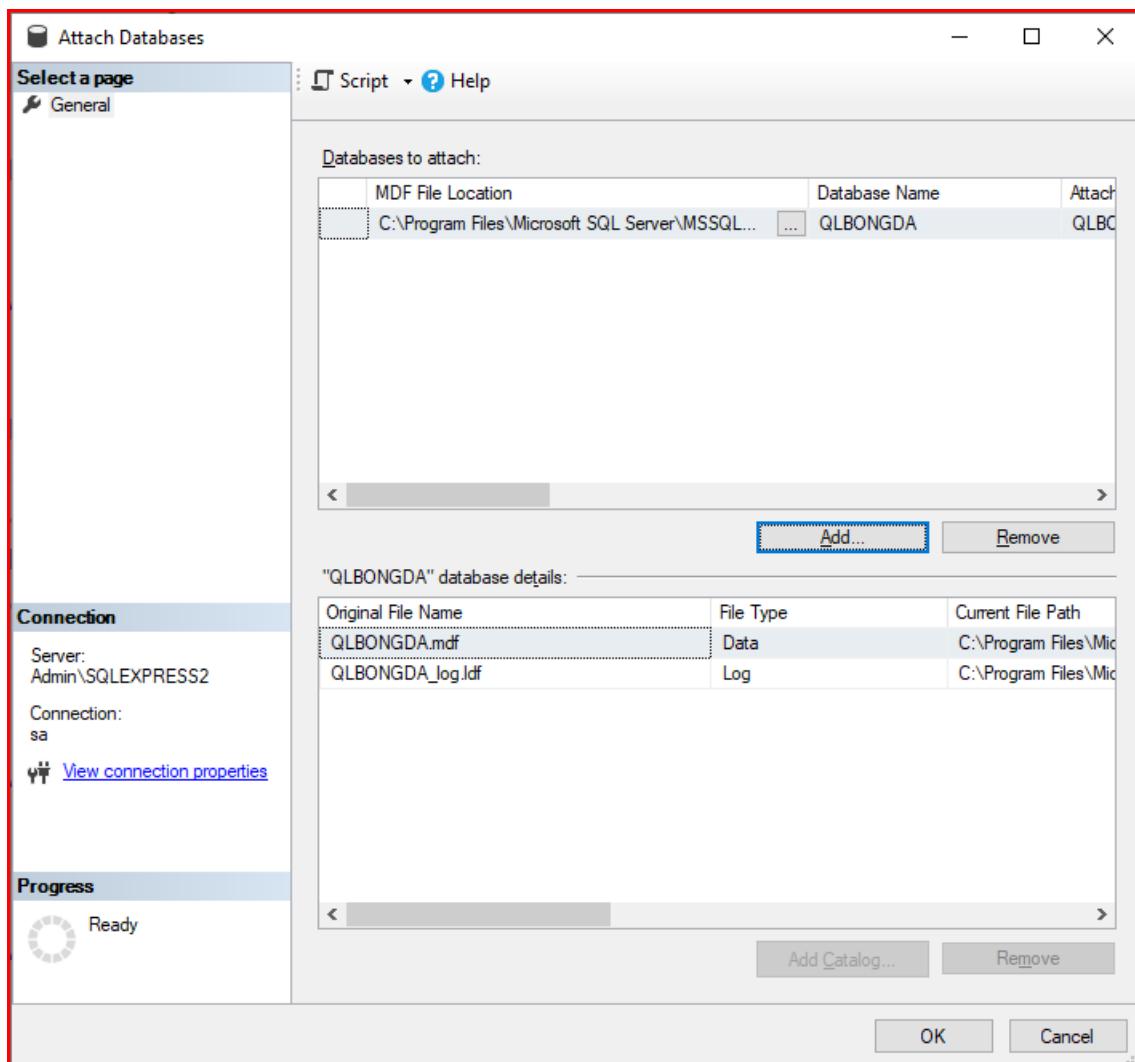
Hình 7: Giao diện attach database

Báo cáo Lab 5



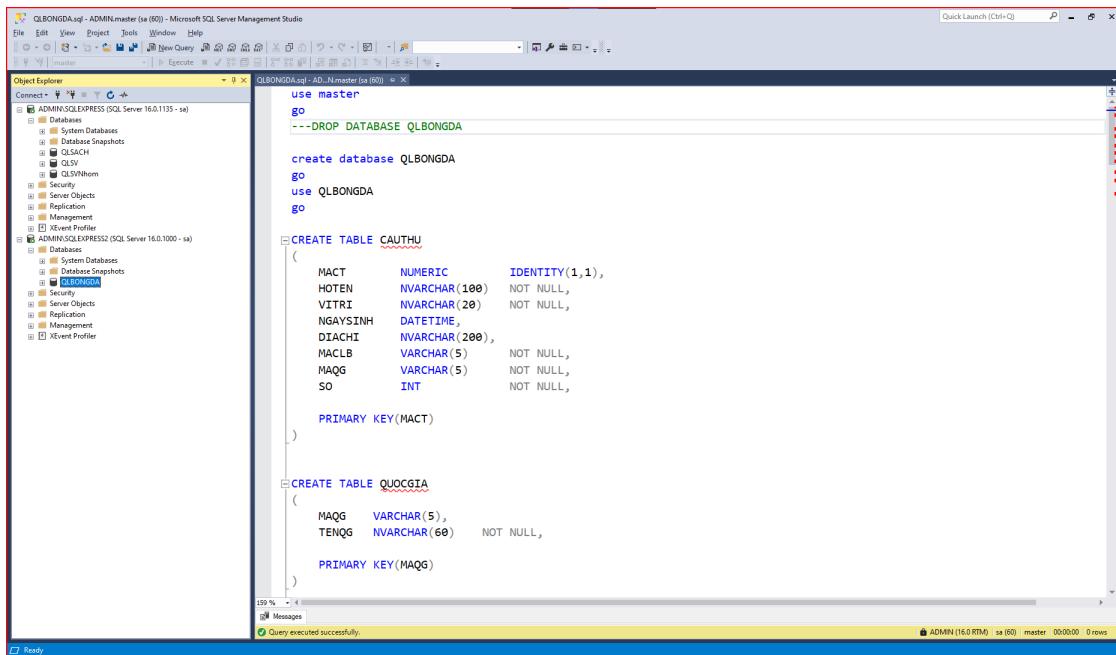
Hình 8: Chọn file .mdf của database QLBongDa

Báo cáo Lab 5



Hình 9: Attach database QLBongDa

Báo cáo Lab 5



```

use master
go
---DROP DATABASE QLBONGDA
create database QLBONGDA
go
use QLBONGDA
go

CREATE TABLE CAUTHU
(
    MACT      NUMERIC      IDENTITY(1,1),
    HOTEN    NVARCHAR(100) NOT NULL,
    VITRI     NVARCHAR(20)  NOT NULL,
    NGAYSINH  DATETIME,
    DIACHI    NVARCHAR(200),
    MACLB    VARCHAR(5)   NOT NULL,
    MAQG     VARCHAR(5)   NOT NULL,
    SO        INT          NOT NULL,
    PRIMARY KEY(MACT)
)

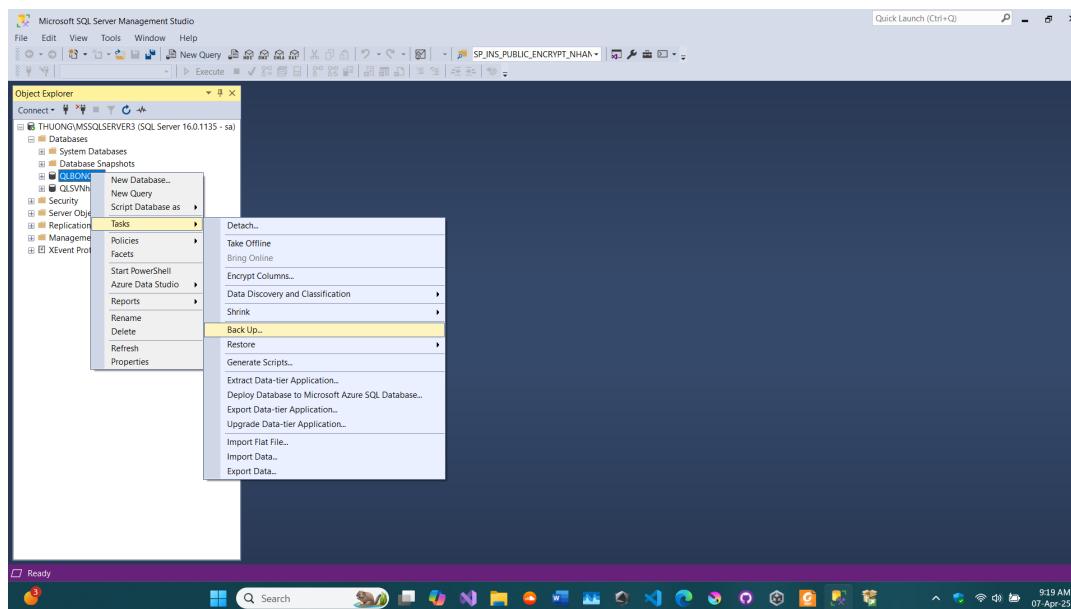
CREATE TABLE QUOCGIA
(
    MAQG     VARCHAR(5),
    TENQG    NVARCHAR(60) NOT NULL,
    PRIMARY KEY(MAQG)
)

```

Query executed successfully.

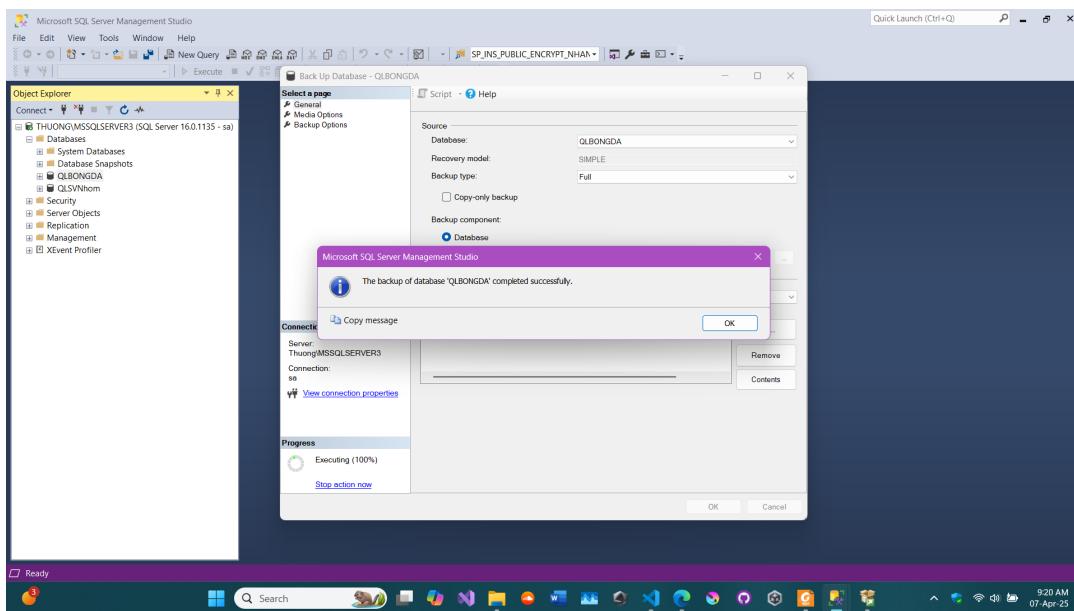
Hình 10: Kết quả sau khi attach

3 Backup & Restore CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia V-League” trong Lab02 từ server A sang server B _ Nhận xét kết quả Attach file

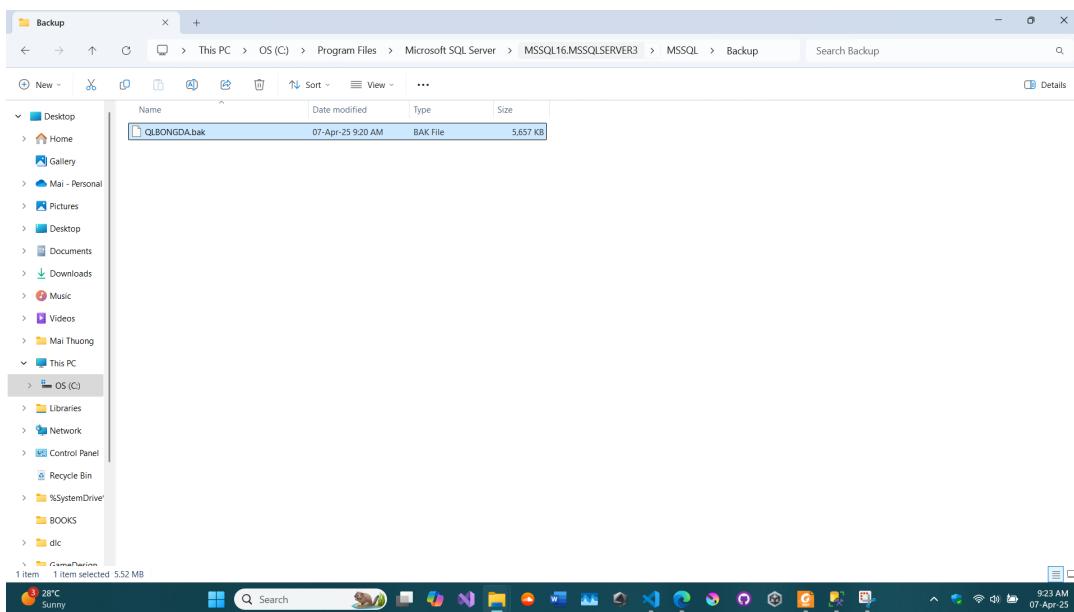


Hình 11: Chọn backup database bên server A

Báo cáo Lab 5

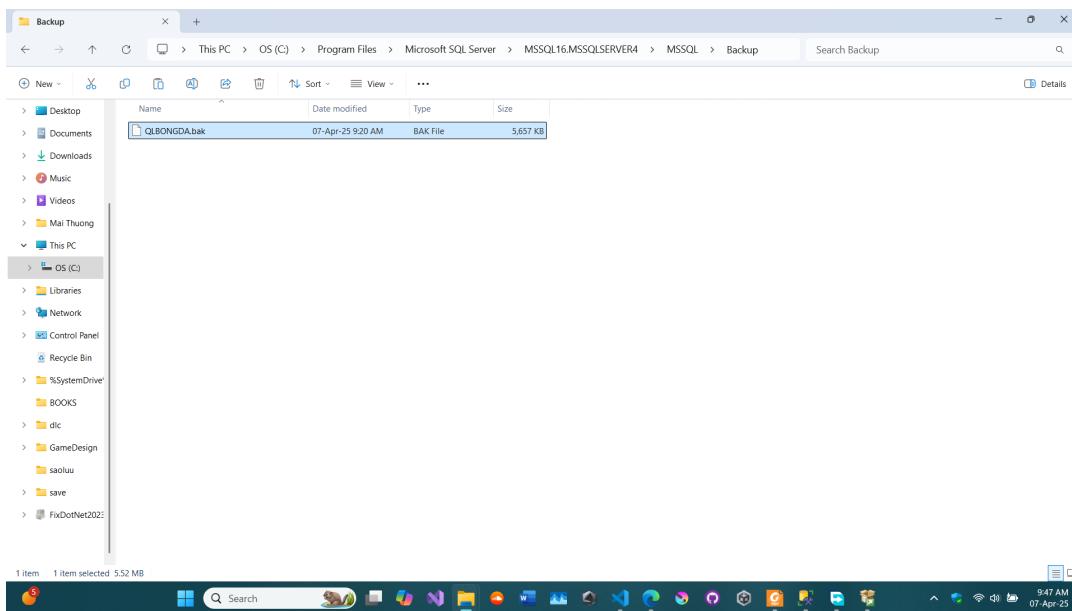


Hình 12: Backup database thành công

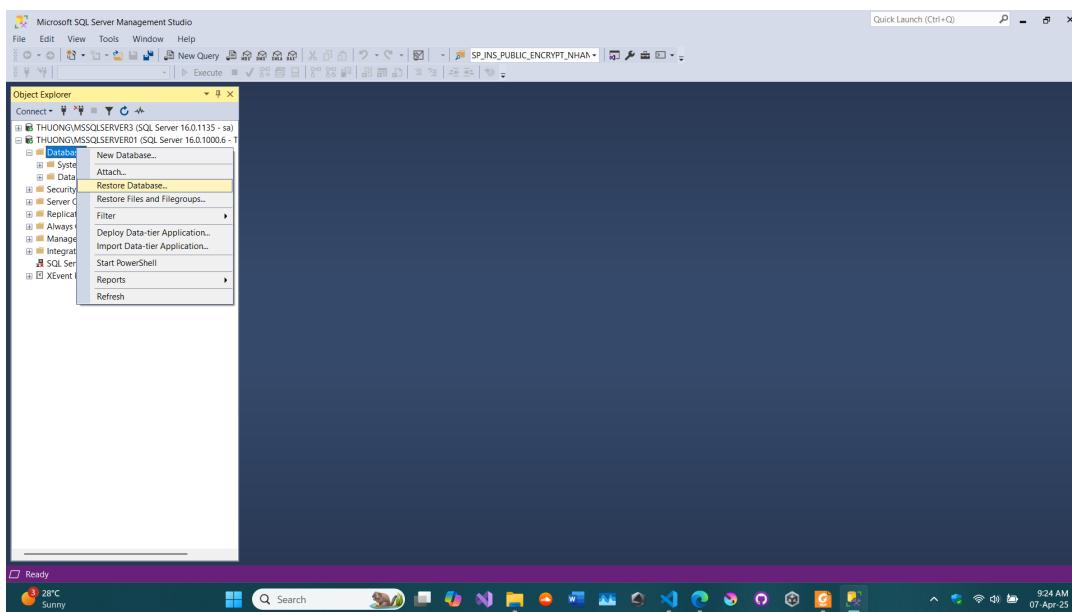


Hình 13: File backup của database

Báo cáo Lab 5

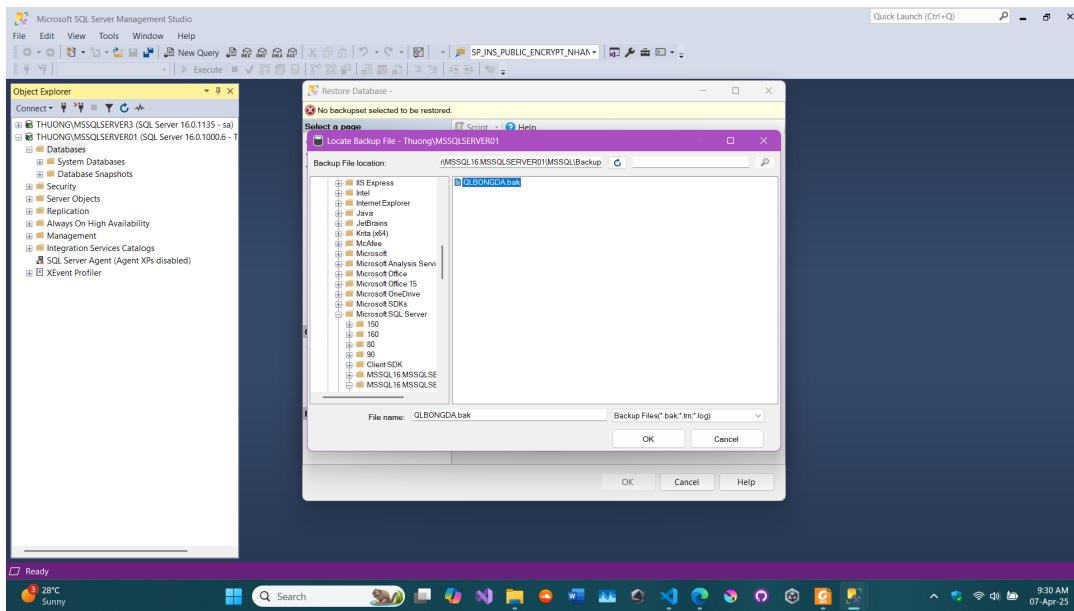


Hình 14: Copy file backup từ server A sang server B

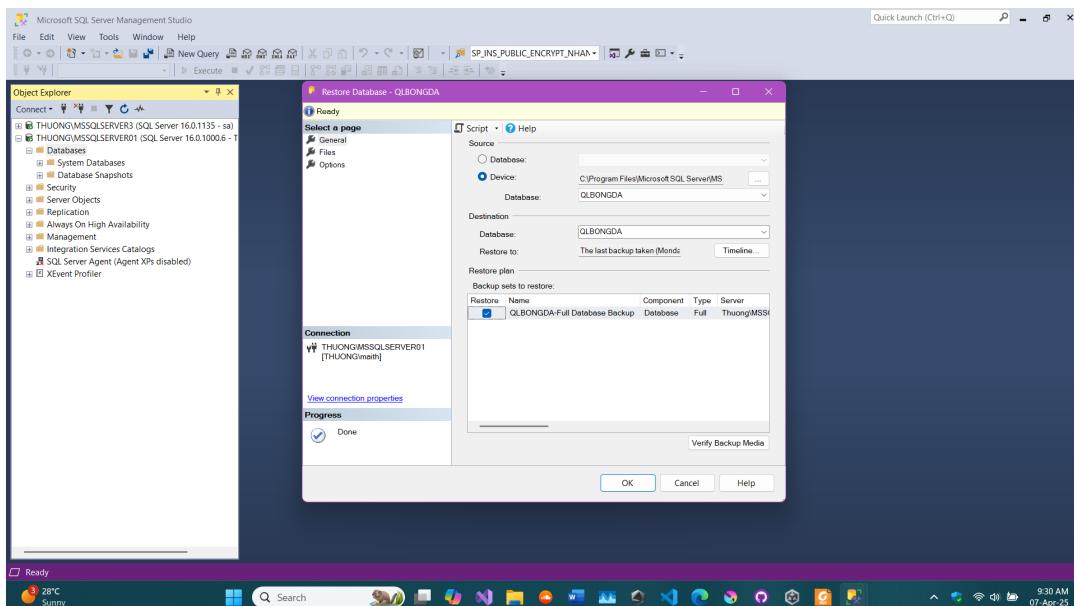


Hình 15: Chọn restore database bên server B

Báo cáo Lab 5

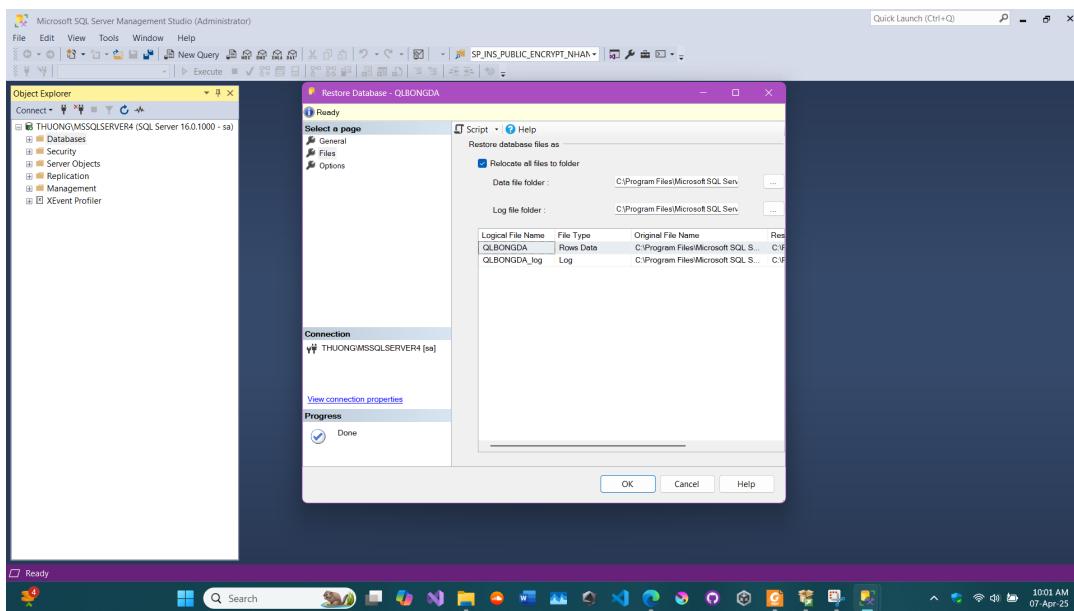


Hình 16: Chọn file backup database QLBongDa để restore

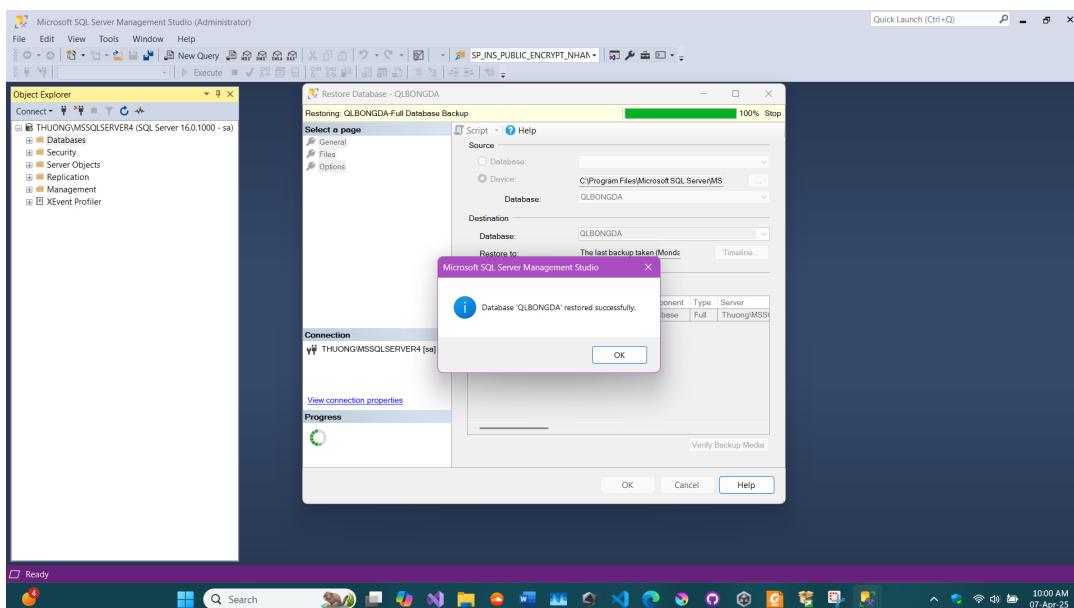


Hình 17: Restore lại database

Báo cáo Lab 5

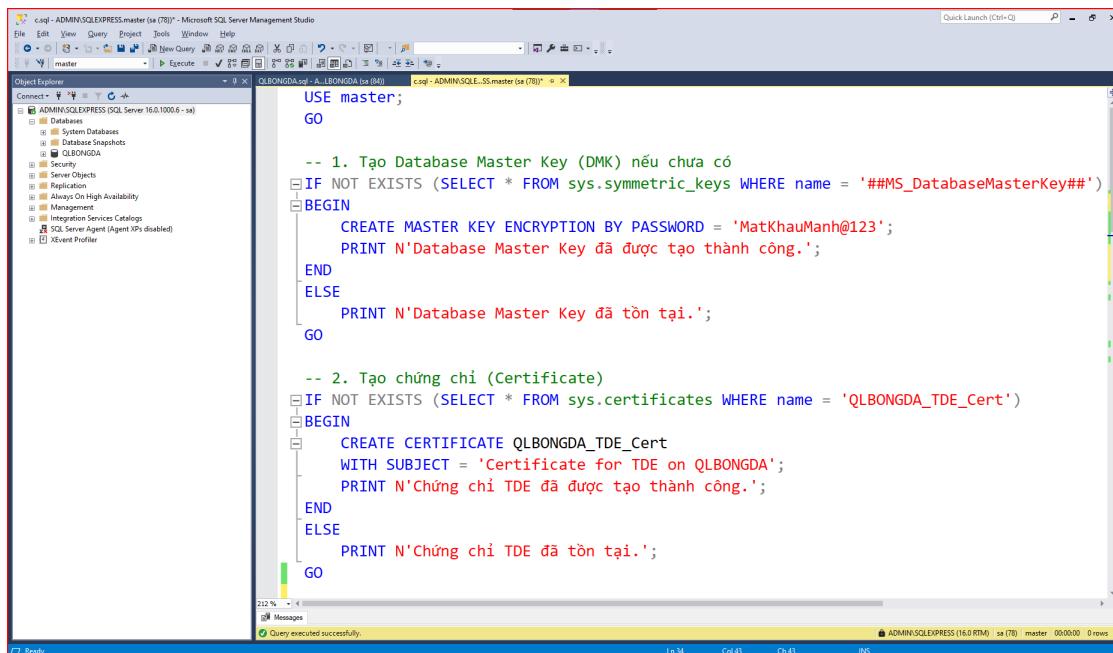


Hình 18: Chọn vị trí cho file data và log của database



Hình 19: Restore thành công

4 Viết script mã hóa CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia V-League” trong Lab02 sử dụng TDE.



```

USE master;
GO

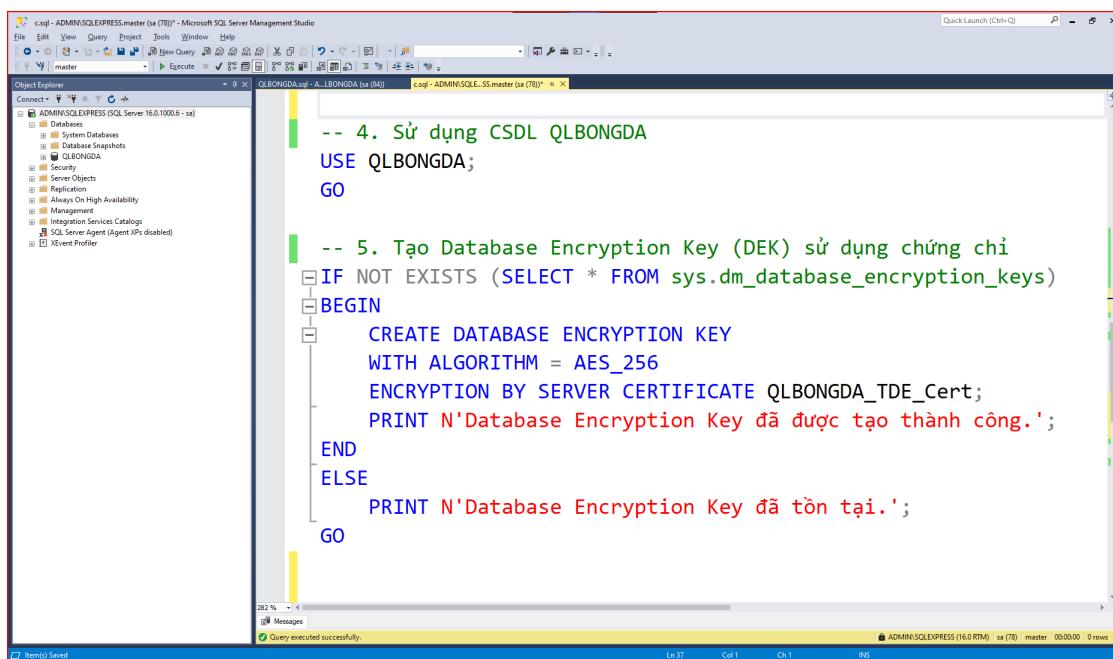
-- 1. Tạo Database Master Key (DMK) nếu chưa có
IF NOT EXISTS (SELECT * FROM sys.symmetric_keys WHERE name = '#MS_DatabaseMasterKey#')
BEGIN
    CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MatKhuManh@123';
    PRINT N'Database Master Key đã được tạo thành công.';
END
ELSE
    PRINT N'Database Master Key đã tồn tại.';
GO

-- 2. Tạo chứng chỉ (Certificate)
IF NOT EXISTS (SELECT * FROM sys.certificates WHERE name = 'QLBONGDA_TDE_Cert')
BEGIN
    CREATE CERTIFICATE QLBONGDA_TDE_Cert
        WITH SUBJECT = 'Certificate for TDE on QLBONGDA';
    PRINT N'Chứng chỉ TDE đã được tạo thành công.';
END
ELSE
    PRINT N'Chứng chỉ TDE đã tồn tại.';
GO

```

Query executed successfully.

Hình 20: Stored procedure tạo master key và certificate cho Transparent data encryption (TDE)



```

-- 4. Sử dụng CSDL QLBONGDA
USE QLBONGDA;
GO

-- 5. Tạo Database Encryption Key (DEK) sử dụng chứng chỉ
IF NOT EXISTS (SELECT * FROM sys.dm_database_encryption_keys)
BEGIN
    CREATE DATABASE ENCRYPTION KEY
        WITH ALGORITHM = AES_256
        ENCRYPTION BY SERVER CERTIFICATE QLBONGDA_TDE_Cert;
    PRINT N'Database Encryption Key đã được tạo thành công.';
END
ELSE
    PRINT N'Database Encryption Key đã tồn tại.';
GO

```

Query executed successfully.

Hình 21: Tạo key TDE

Báo cáo Lab 5

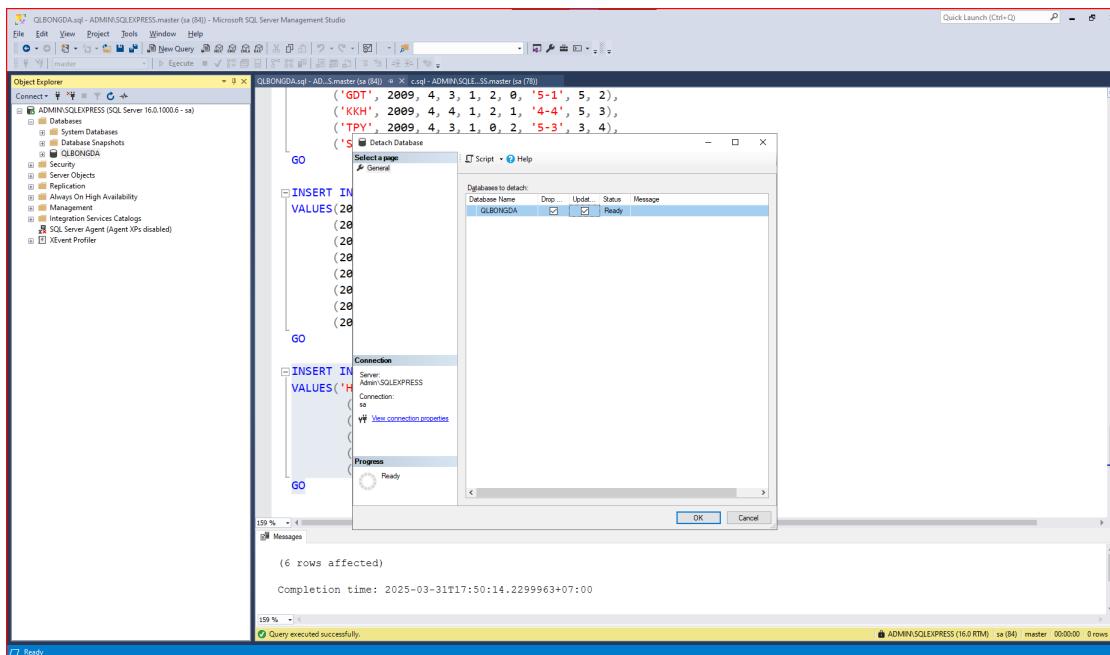
The screenshot shows the Microsoft SQL Server Management Studio interface. In the Object Explorer, the database 'QLBONGDA' is selected under 'ADMIN:SQLEXPRESS (SQL Server 16.0.1000.6 - sa)'. In the main query window, the following T-SQL code is executed:

```
-- 6. Bật TDE cho CSDL QLBONGDA
ALTER DATABASE QLBONGDA
SET ENCRYPTION ON;
PRINT N'Transparent Data Encryption đã được bật.';
GO
```

The status bar at the bottom indicates 'Query executed successfully.'

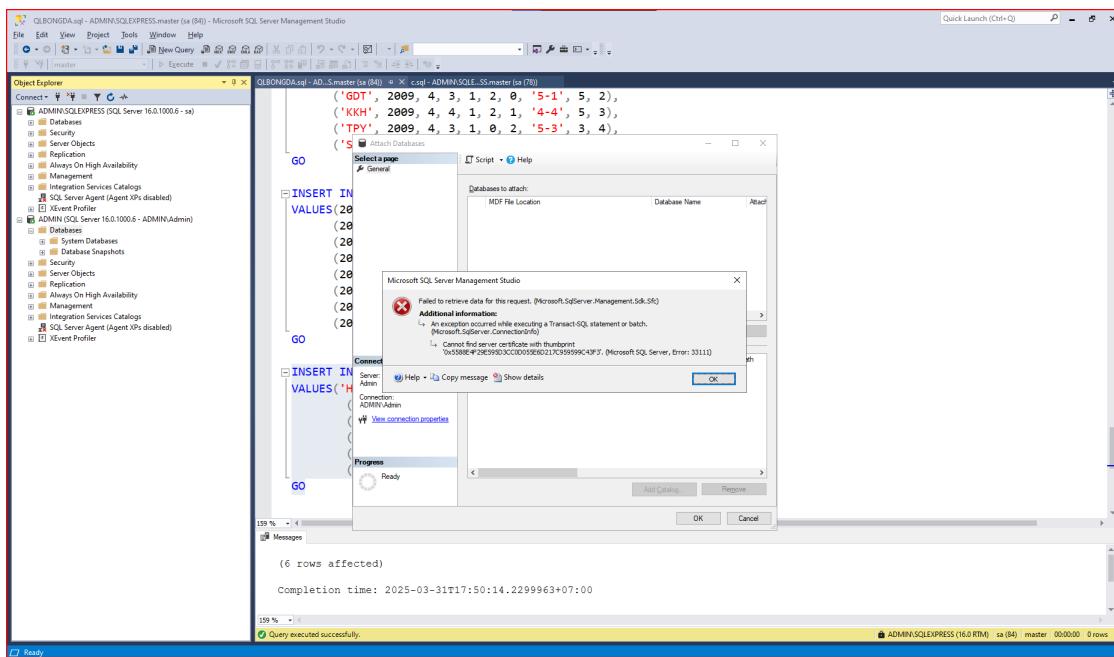
Hình 22: Mã hoá database QLBongDa bằng TDE

5 Thực hiện Detach và Attach CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia VLeague” trong Lab02 đã mã hóa TDE từ server A sang server B.



Hình 23: Làm các bước detach như câu a)

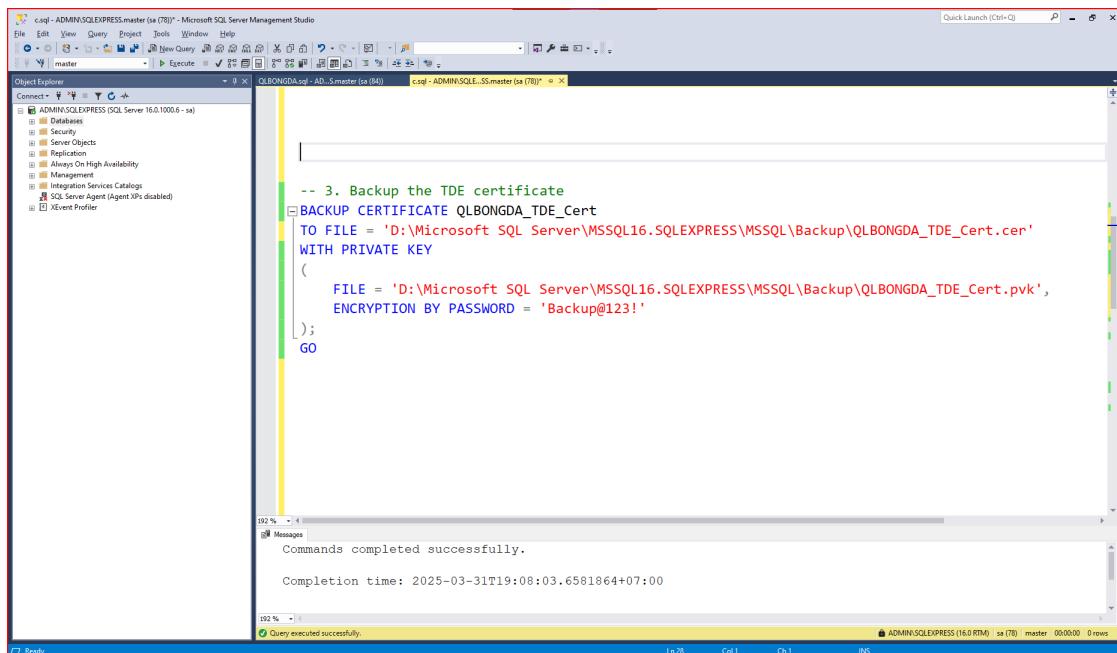
Báo cáo Lab 5



Hình 24: Attach thất bại

Detach database QLBongDa từ server A và Attach sang server B lúc này thất bại là do ở server B lúc này chưa tồn tại master key và certificate đã dùng để mã hoá database QLBongDa. Nếu không có certificate này ở server B thì SQL Server sẽ không giải mã được database QLBongDa để truy cập.

6 Nếu kết quả câu lệnh thất bại, mô tả các bước thực hiện để xử lý lỗi trên



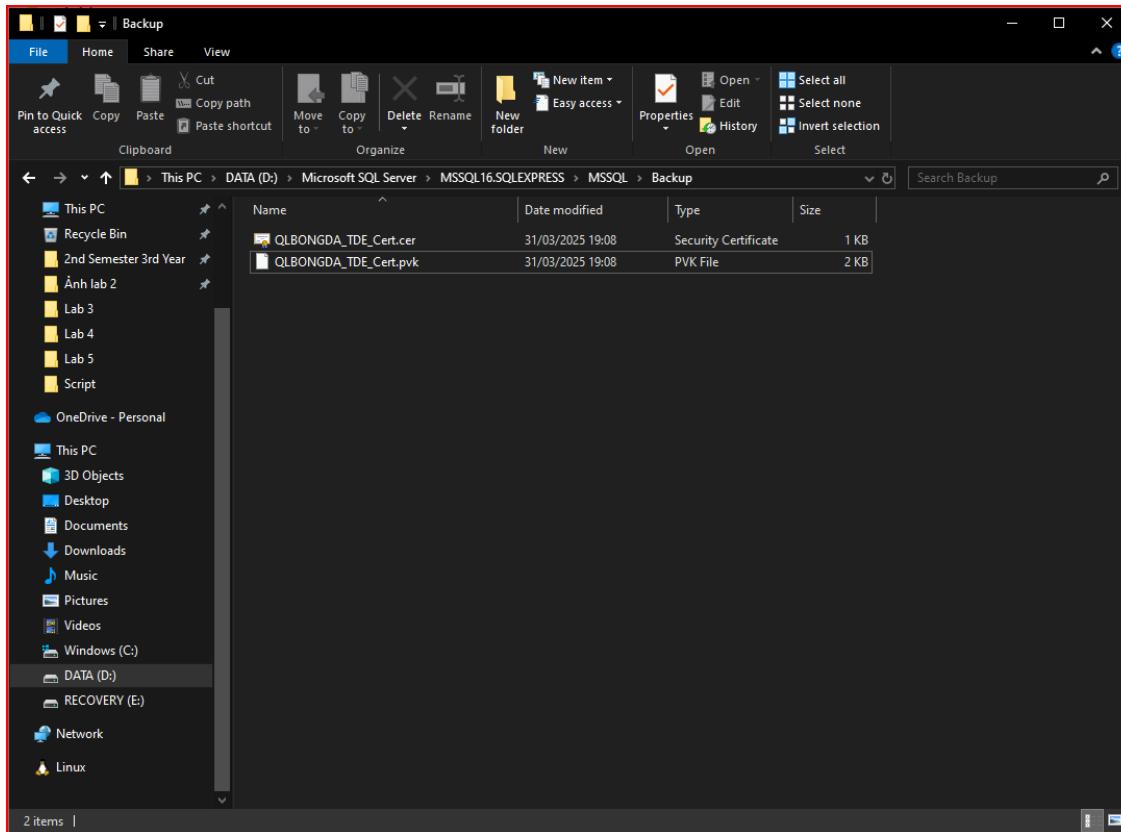
```
-- 3. Backup the TDE certificate
BACKUP CERTIFICATE QLBONGDA_TDE_Cert
TO FILE = 'D:\Microsoft SQL Server\MSSQL16.SQLEXPRESS\MSSQL\Backup\QLBONGDA_TDE_Cert.cer'
WITH PRIVATE KEY
(
    FILE = 'D:\Microsoft SQL Server\MSSQL16.SQLEXPRESS\MSSQL\Backup\QLBONGDA_TDE_Cert.pvk',
    ENCRYPTION BY PASSWORD = 'Backup@123!'
)
GO
```

Messages
Commands completed successfully.
Completion time: 2025-03-31T19:08:03.6581064+07:00

Query executed successfully.

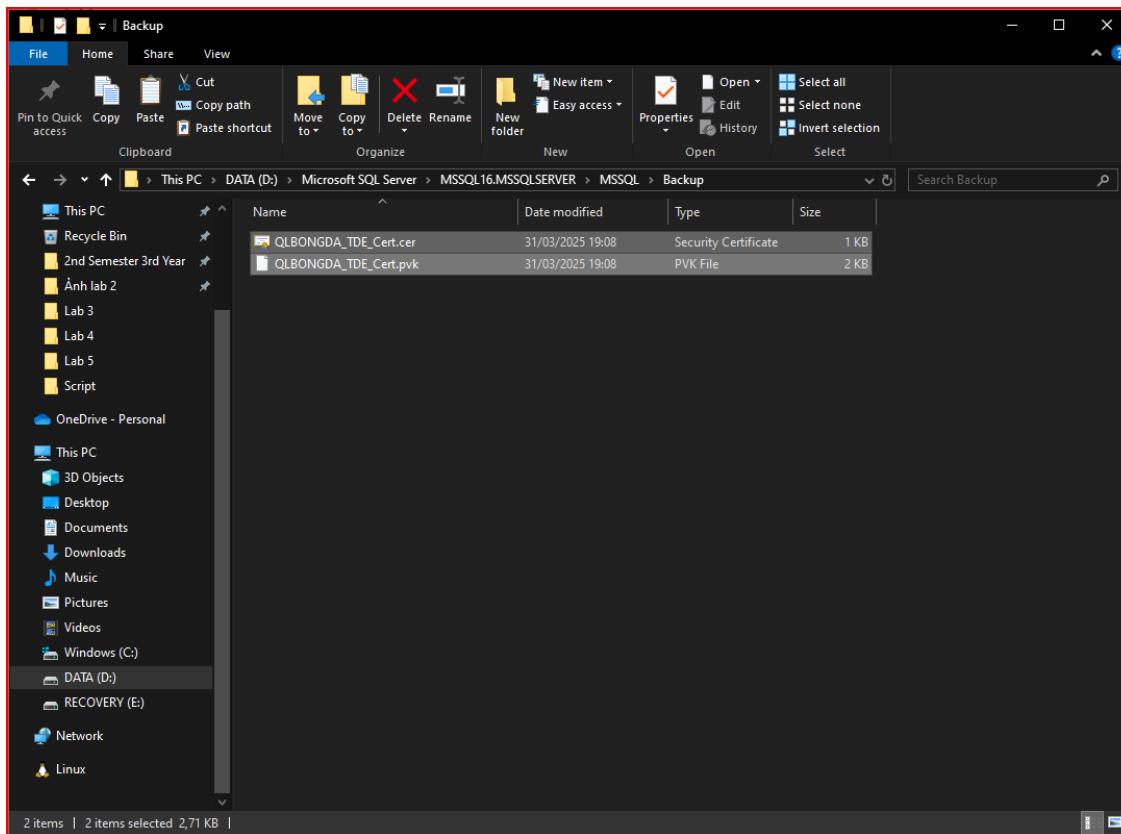
Hình 25: Backup master key và certificate của server A

Báo cáo Lab 5



Hình 26: Copy 2 file backup vừa tạo từ server A sang server B

Báo cáo Lab 5



Hình 27: Copy 2 file backup vừa tạo từ server A sang server B

```

USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MatKhauMạnh@123';
GO

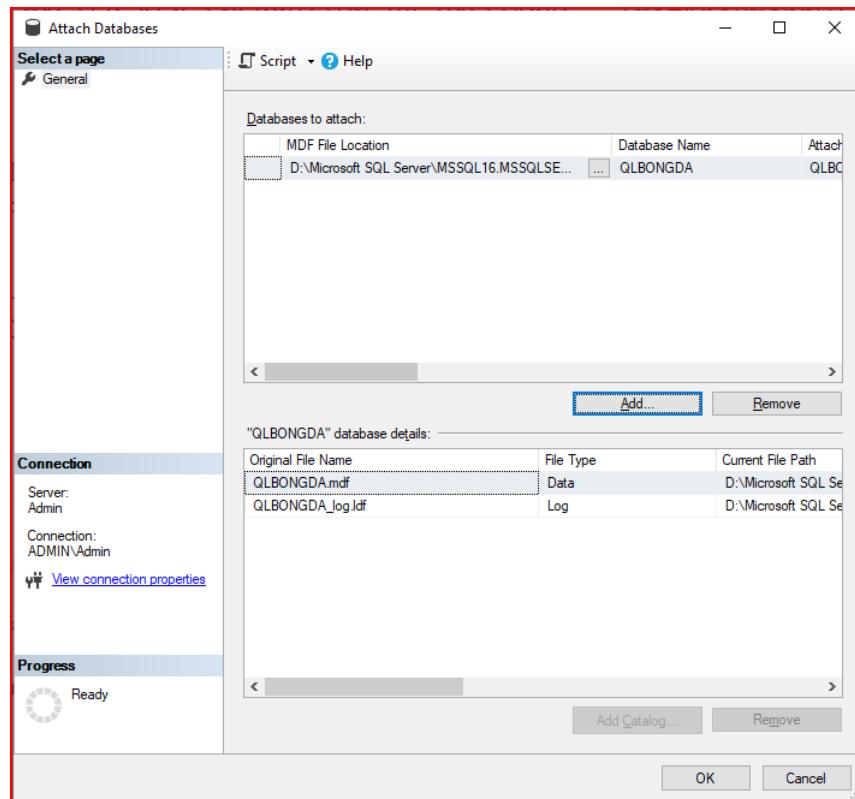
CREATE CERTIFICATE QLBONGDA_TDE_Cert
FROM FILE = 'D:\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Backup\QLBONGDA_TDE_Cert.cer'
WITH PRIVATE KEY
(
    FILE = 'D:\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Backup\QLBONGDA_TDE_Cert.pvk',
    DECRYPTION BY PASSWORD = 'Backup@123!'
);
GO

```

The screenshot shows the SSMS interface with a query window titled 'e.sql - ADMINmaster (ADMIN\Admin (T2)) - Microsoft SQL Server Management Studio'. The Object Explorer on the left shows the database structure. The query window contains T-SQL code to create a master key and a certificate named 'QLBONGDA_TDE_Cert' using the backup files 'QLBONGDA_TDE_Cert.cer' and 'QLBONGDA_TDE_Cert.pvk'. The command 'GO' is used multiple times to separate the statements. The status bar at the bottom indicates 'Commands completed successfully.' and 'Completion time: 2025-03-31T19:15:29.4659156+07:00'.

Hình 28: Tạo master key và certificate từ 2 file backup

Báo cáo Lab 5



Hình 29: Attach database QLBongDa

```

USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MatKhuManh@123';
GO

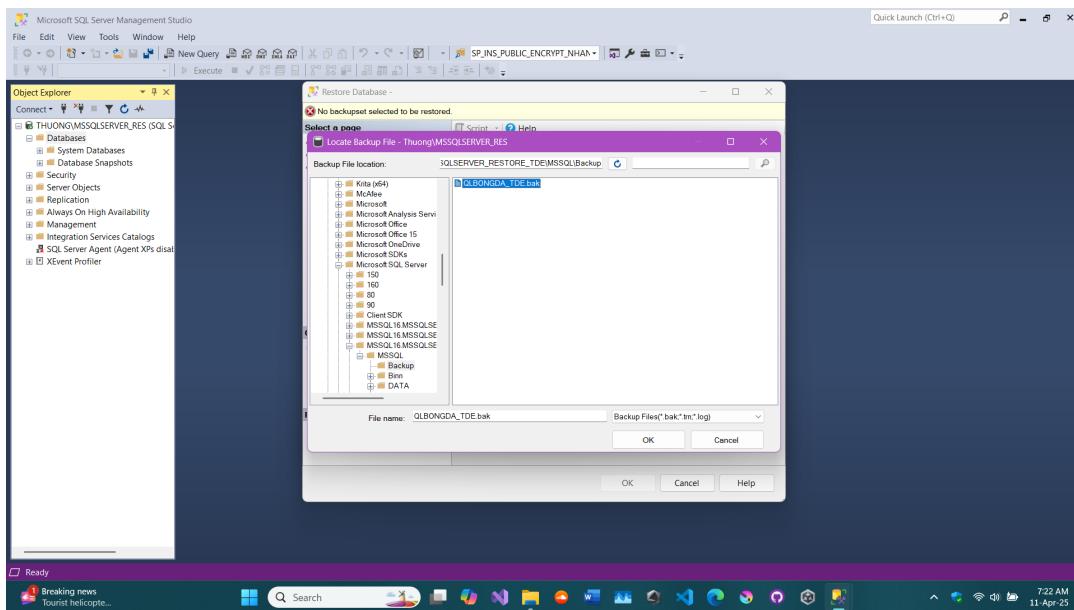
CREATE CERTIFICATE QLBONGDA_TDE_Cert
FROM FILE = 'D:\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Backup\QLBONGDA_TDE_Cert.cer'
WITH PRIVATE KEY
(
    FILE = 'D:\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Backup\QLBONGDA_TDE_Cert.pvk',
    DECRYPTION BY PASSWORD = 'Backup@123!'
);
GO

```

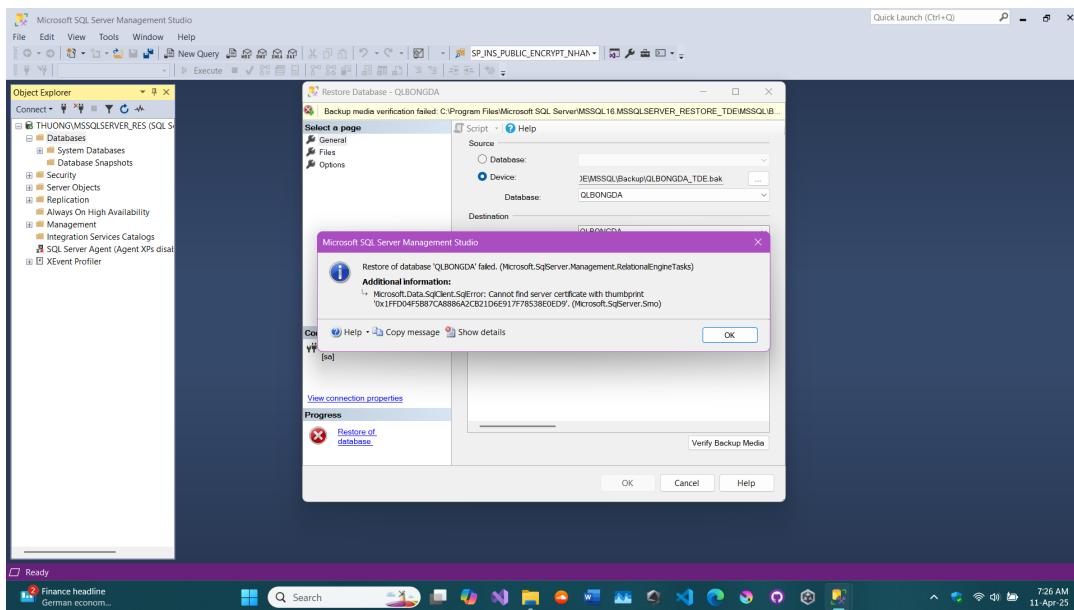
The status bar at the bottom of the SSMS window indicates: 'Commands completed successfully.' and 'Completion time: 2025-03-31T19:15:29.4659156+07:00'. A message bar at the bottom says 'Query executed successfully.'

Hình 30: Attach thành công

7 Thực hiện Backup và Restore CSDL quản lý “Quản lý Giải bóng đá vô địch quốc gia VLeague” trong Lab02 đã mã hóa TDE từ server A sang server B.



Hình 31: Thủ restore lại database



Hình 32: Restore thất bại

Backup database QLBongDa từ server A và Restore sang server B lúc này thất bại là do ở server B lúc này chưa tồn tại master key và certificate đã dùng để mã hoá database QLBongDa. Nếu không có certificate này ở server B thì SQL Server sẽ không giải mã được database QLBongDa để truy cập.

8 Nếu kết quả câu f là thất bại, mô tả các bước thực hiện để xử lý lỗi trên

```

USE master;
GO

-- Sao lưu cơ sở dữ liệu QLBONGDA ra file .bak
BACKUP DATABASE QLBONGDA
TO DISK = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER89\MSSQL\Backup\QLBONGDA_TDE.bak';

-- Tạo Master Key nếu chưa có (chỉ thực hiện 1 lần duy nhất trên server)
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MatKhauManh@123';

-- Tạo chứng chỉ từ file backup đã sao lưu ở server nguồn
-- Dùng để giải mã cơ sở dữ liệu đã mã hóa bằng TDE
CREATE CERTIFICATE TDECert
FROM FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE_Cert.cer'
WITH PRIVATE KEY (
    FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE_Cert.pvk',
    DECRYPTION BY PASSWORD = 'Backup@123'
);

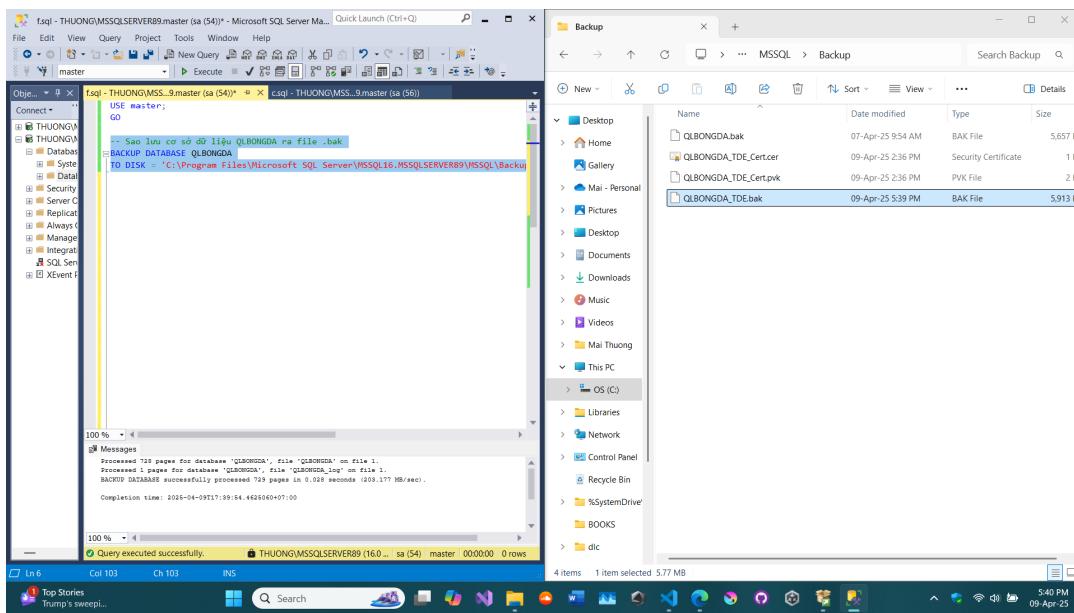
-- Kiểm tra tên logic file trong file backup (bắt buộc trước khi restore)
RESTORE FILELISTONLY
FROM DISK = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE.bak';

-- Khôi phục cơ sở dữ liệu từ bản backup TDE
RESTORE DATABASE QLBONGDA
FROM DISK = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE.bak'
WITH MOVE 'QLBONGDA' TO 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\DATA\QLBONGDA.mdf',
      MOVE 'QLBONGDA_log' TO 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\DATA\QLBONGDA_log.ldf';

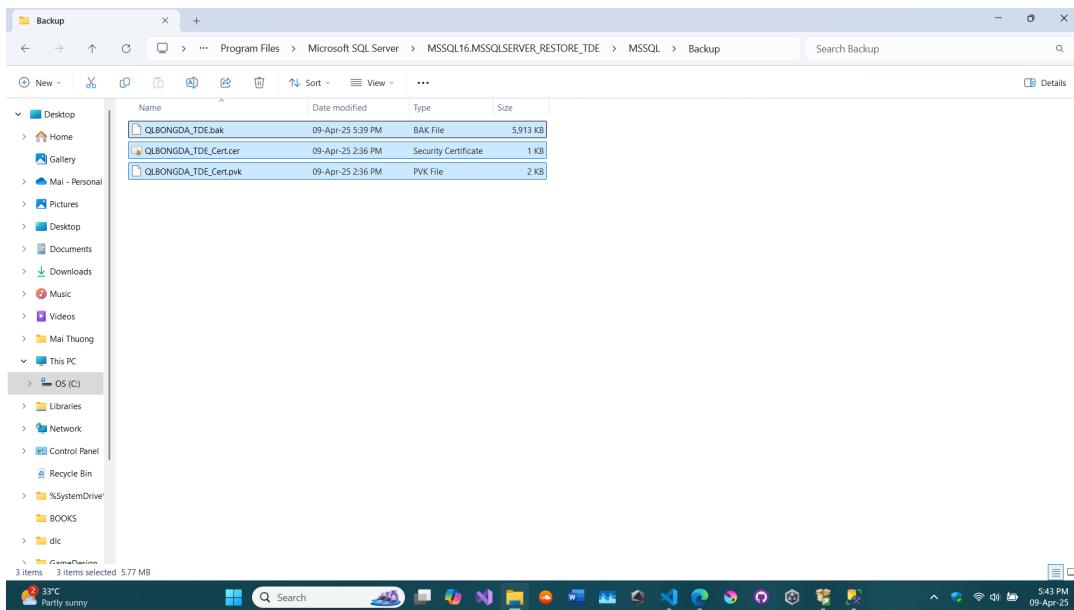
```

Hình 33: Script để restore

Báo cáo Lab 5



Hình 34: Backup database



Hình 35: Copy file backup bao gồm cả database và certificate từ server A sang server B

Báo cáo Lab 5

```

USE master;
GO

-- Sao lưu cơ sở dữ liệu QLBONGDA ra file .bak
BACKUP DATABASE QLBONGDA
TO DISK = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER89\MSSQL\Backup\QLBONGDA_TDE.bak';

-- Tạo Master Key nếu chưa có (chỉ thực hiện 1 lần duy nhất trên server)
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MatkhauManh123';

-- Tạo chứng chỉ từ file backup đã sao lưu ở server nguồn
-- Dùng để giải mã cơ sở dữ liệu đã mã hóa bằng TDE
CREATE CERTIFICATE TDECert
FROM FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE_Cert.cer'
WITH PRIVATE KEY (
    FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE_Cert.pvk',
    DECRYPTION BY PASSWORD = 'Backup@123'
);

```

Messages
Command completed successfully.
Completion time: 2023-04-09T17:45:36.3593342+07:00

Query executed successfully.

Hình 36: Script tạo lại cert

```

-- Tạo Master Key nếu chưa có (chỉ thực hiện 1 lần duy nhất trên server)
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MatkhauManh123';

-- Tạo chứng chỉ từ file backup đã sao lưu ở server nguồn
-- Dùng để giải mã cơ sở dữ liệu đã mã hóa bằng TDE
CREATE CERTIFICATE TDECert
FROM FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE_Cert.cer'
WITH PRIVATE KEY (
    FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE_Cert.pvk',
    DECRYPTION BY PASSWORD = 'Backup@123'
);

-- Kiểm tra tên logic file trong file backup (bắt buộc trước khi restore)
RESTORE FILELISTONLY
FROM DISK = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE.bak';

-- Khởi phục cơ sở dữ liệu từ bản backup TDE
RESTORE DATABASE QLBONGDA
FROM DISK = 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\Backup\QLBONGDA_TDE.bak'
WITH MOVE 'QLBONGDA' TO 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\DATA\QLBONGDA.mdf',
      MOVE 'QLBONGDA_log' TO 'C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER_RESTORE_TDE\MSSQL\DATA\QLBONGDA_log.ldf';

```

Messages
Processed 729 pages for database 'QLBONGDA', file 'QLBONGDA' on file 1.
Processed 1 pages for database 'QLBONGDA', file 'QLBONGDA_log' on file 1.
RESTORE DATABASE successfully processed 729 pages in 0.018 seconds (379.264 MB/sec).

Completion time: 2023-04-09T17:48:53.3584540+07:00

Query executed successfully.

Hình 37: Restore thành công

Tài liệu

- [1] Database detach and attach (SQL Server)
- [2] Move a database using detach and attach (Transact-SQL)
- [3] Quickstart: Backup and restore a SQL Server database with SSMS
- [4] Transparent data encryption (TDE)