

ĐẠI HỌC QUỐC GIA TP HCM
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 2

Đề tài: Phân quyền truy cập các đối tượng trong CSDL

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 Hương

Ngày 24 tháng 2 năm 2025



Mục lục

1	Phân công	1
2	Yêu cầu	1
3	Tạo user và phân quyền cho các user truy xuất CSDL QLBongDa	2
4	Tạo stored procedure với yêu cầu cho biết mã số, họ tên, ngày sinh, địa chỉ	6
5	Tạo stored procedure với yêu cầu như câu e, với nội dung stored được mã hóa	7
6	Thực thi 2 stored procedure trên	8
7	Cách nào để Encrypt toàn bộ 100 stored procedure	9
8	Tạo và phân quyền trên Views	10
9	Tạo và phân quyền trên Stored Procedure	14

1 Phân công

MSSV	Họ tên	Công việc	Mức độ hoàn thành
22127063	Lưu Thành Đạt	Câu a) đến câu h) Kiểm tra và chỉnh sửa script Viết báo cáo	100%
22127409	Mai Xuân Thường	Câu i) và j) Viết báo cáo	100%

Bảng 1: Bảng phân công công việc

2 Yêu cầu

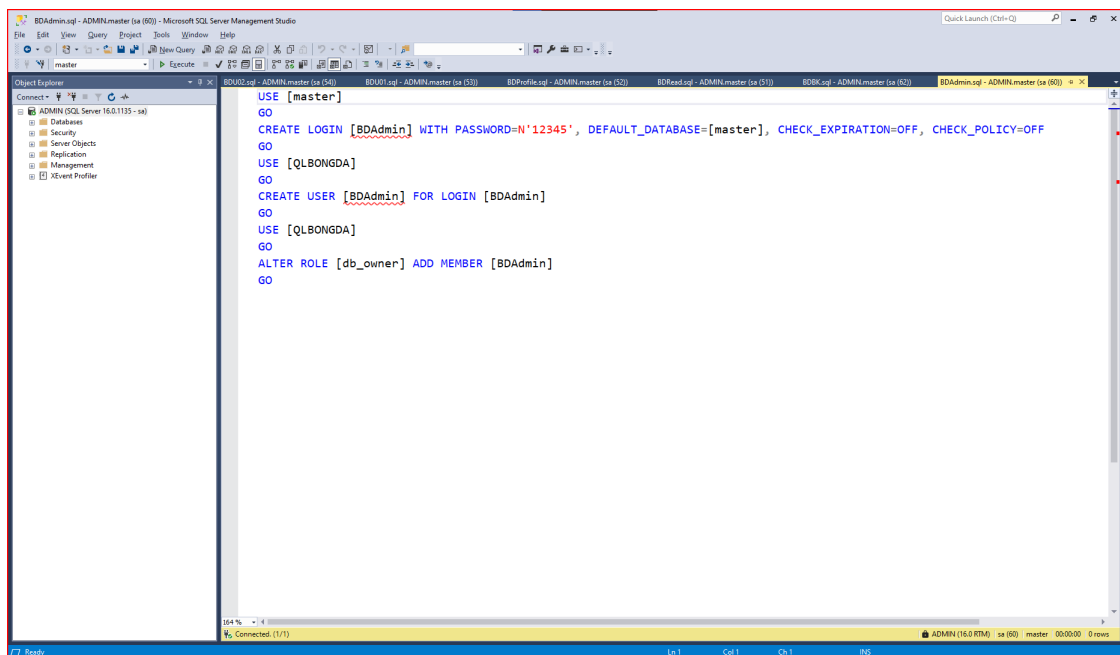
- Tạo Database có tên **QLBongDa**.
- Tạo mới các bảng **CAUTHU**, **QUOCCGIA**, **CAULACBO**, **TINH**, **HUANLUYEN-VIEN**, **SANVD**, **HLV_CLB**, **TRANDAU**, **BANGXH** theo mô tả.
- Nhập dữ liệu cho các bảng trên.
- Tạo user và phân quyền cho các user truy xuất cơ sở dữ liệu **QLBongDa**.
- Tạo stored procedure để lấy thông tin cầu thủ thuộc đội bóng “SHB Đà Nẵng” và có quốc tịch “Brazil”. Trong đó, tên đội bóng/câu lạc bộ và tên quốc tịch/quốc gia là hai tham số của stored procedure.
 - Tên stored procedure: **SP_SEL_NO_ENCRYPT**
 - Danh sách tham số: **@TenCLB**, **@TenQG**
- Tạo stored procedure với yêu cầu như trên, nhưng nội dung được mã hóa.
 - Tên stored procedure: **SP_SEL_ENCRYPT**
 - Danh sách tham số: **@TenCLB**, **@TenQG**
- Thực thi hai stored procedure trên với tham số truyền vào:
 - @TenCLB = “SHB Đà Nẵng”**

- @TenQG = ‘Brazil’

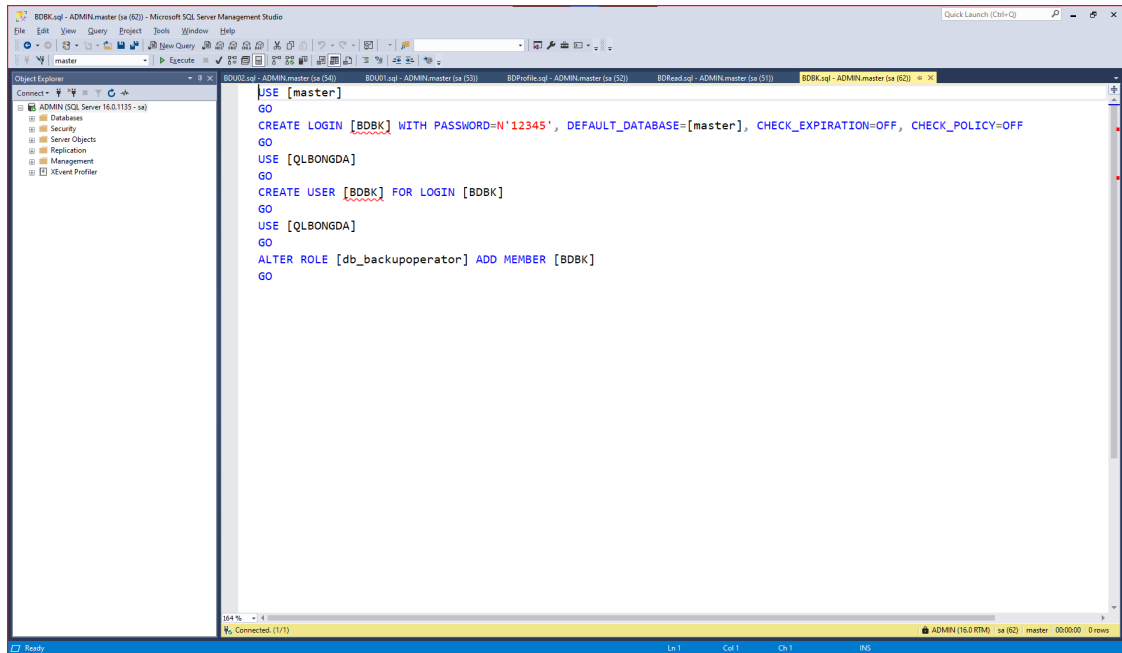
Quan sát kết quả và nhận xét.

h Giả sử trong CSDL có 100 stored procedure, có cách nào để mã hóa toàn bộ 100 stored procedure trước khi cài đặt cho khách hàng không? Nếu có, hãy mô tả các bước thực hiện.

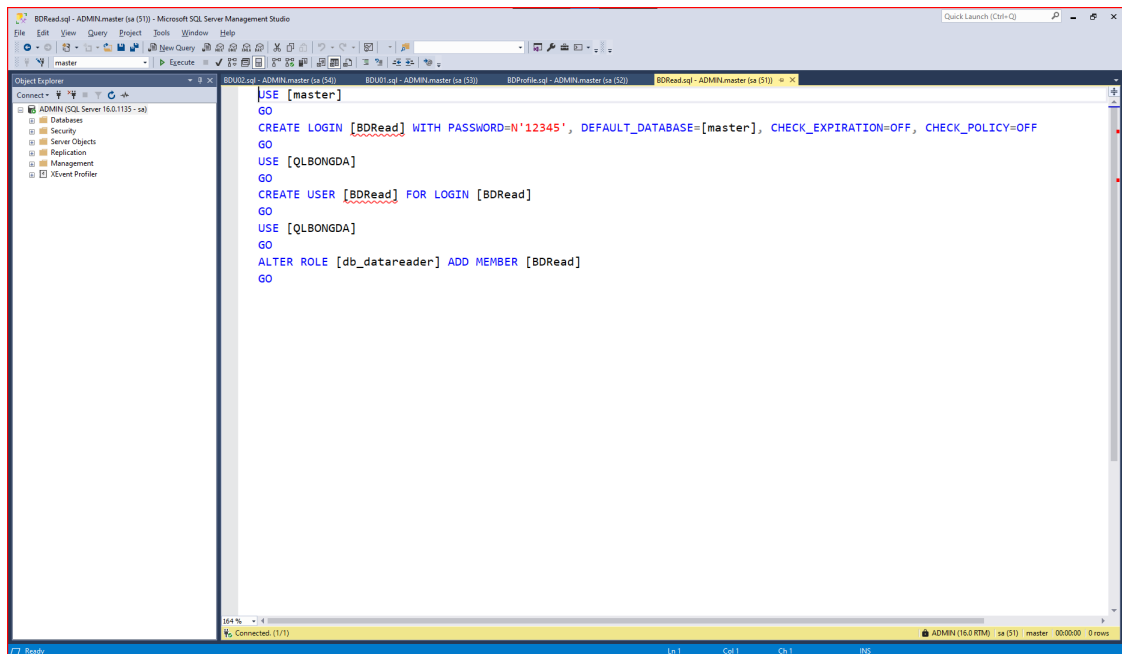
3 Tạo user và phân quyền cho các user truy xuất CSDL QLBongDa



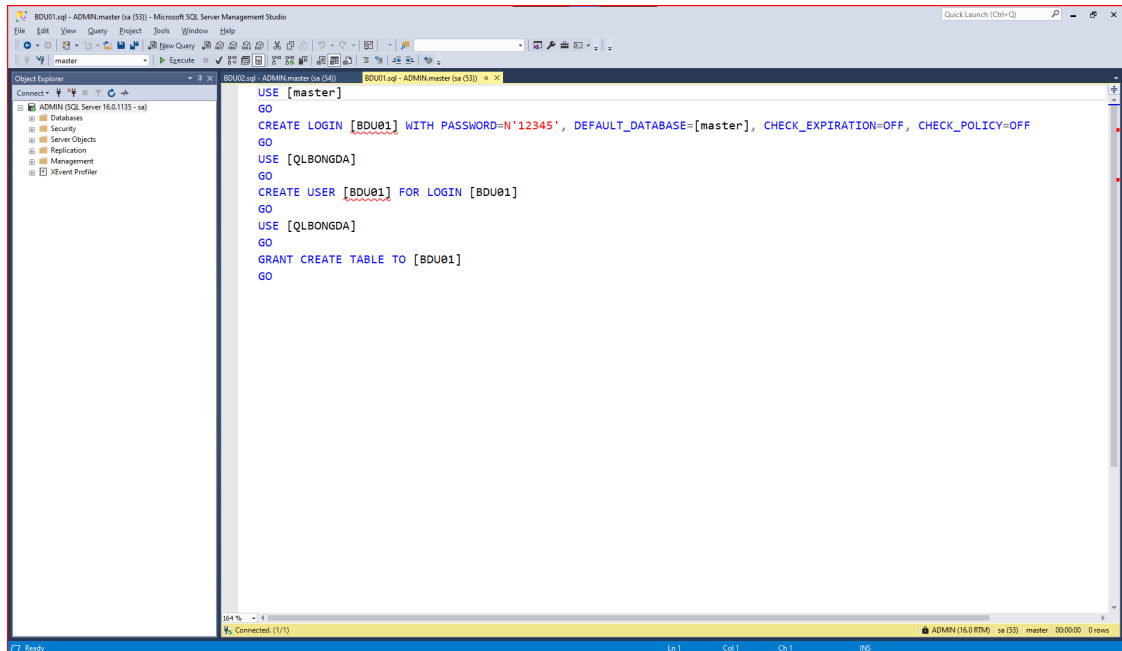
Hình 1: BAdmin



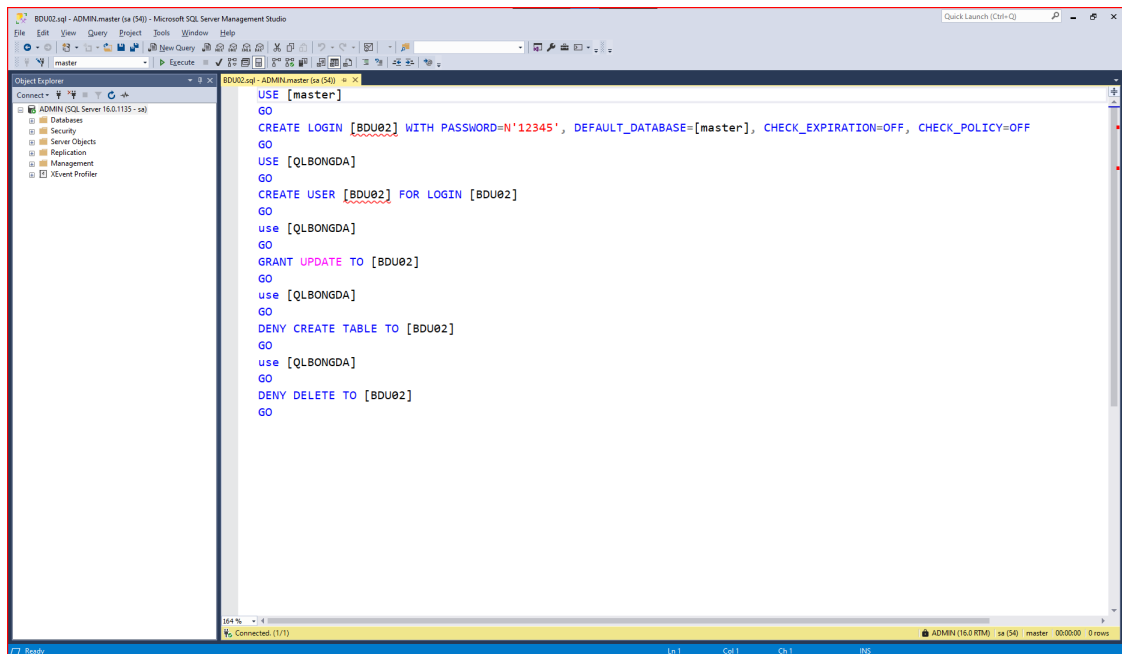
Hình 2: BDBK



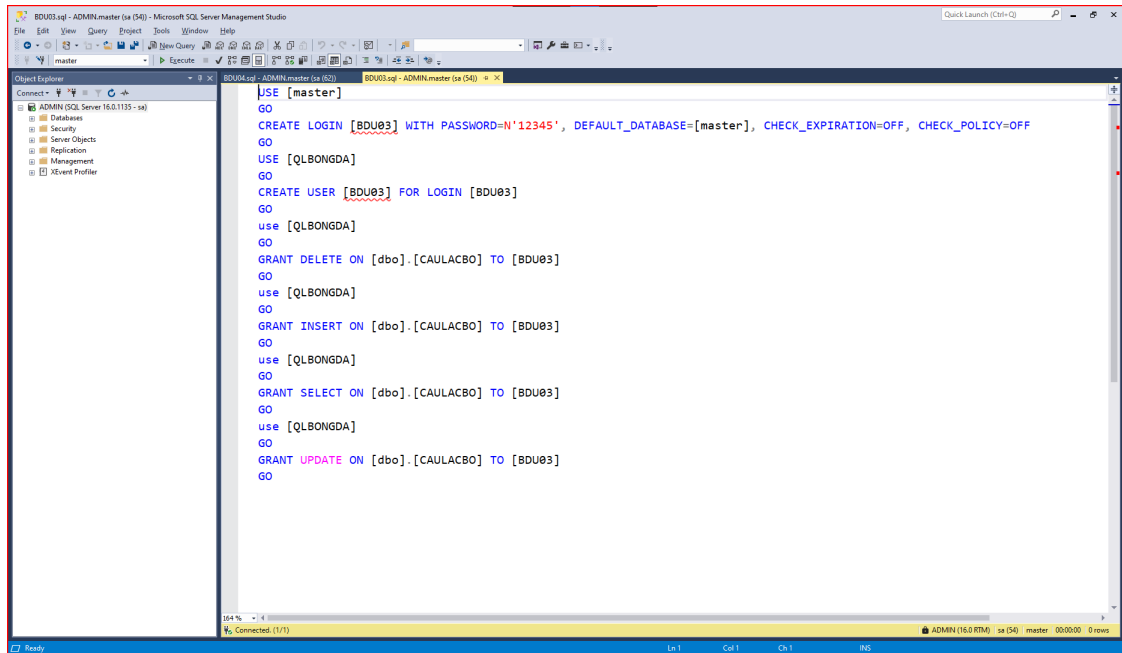
Hình 3: BDBK



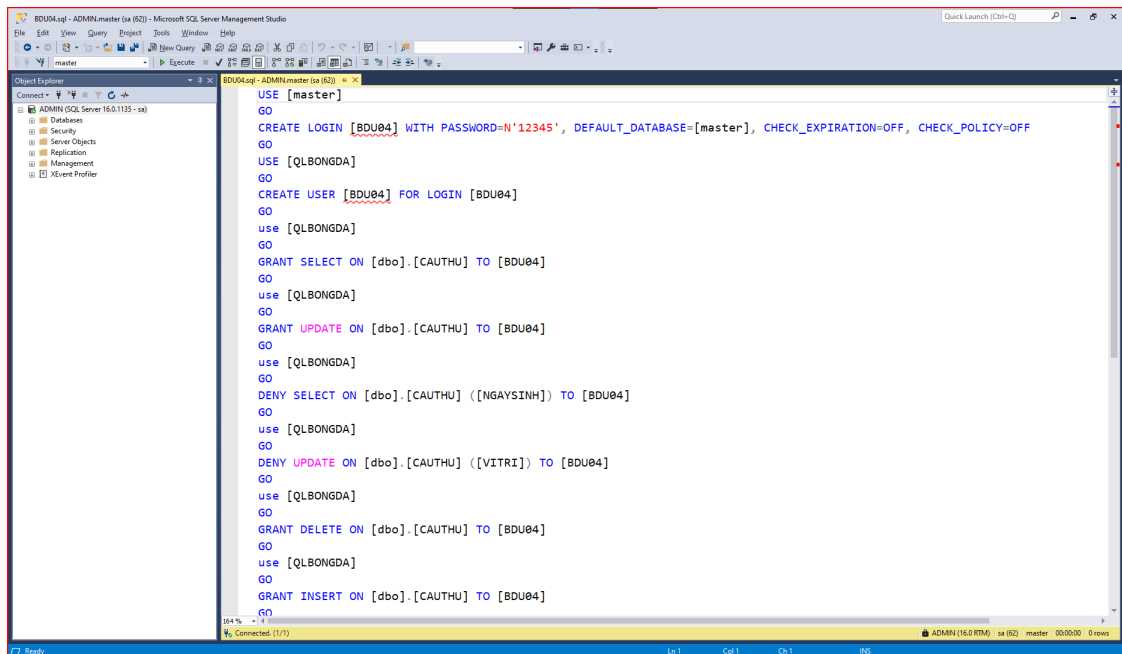
Hình 4: BDU01



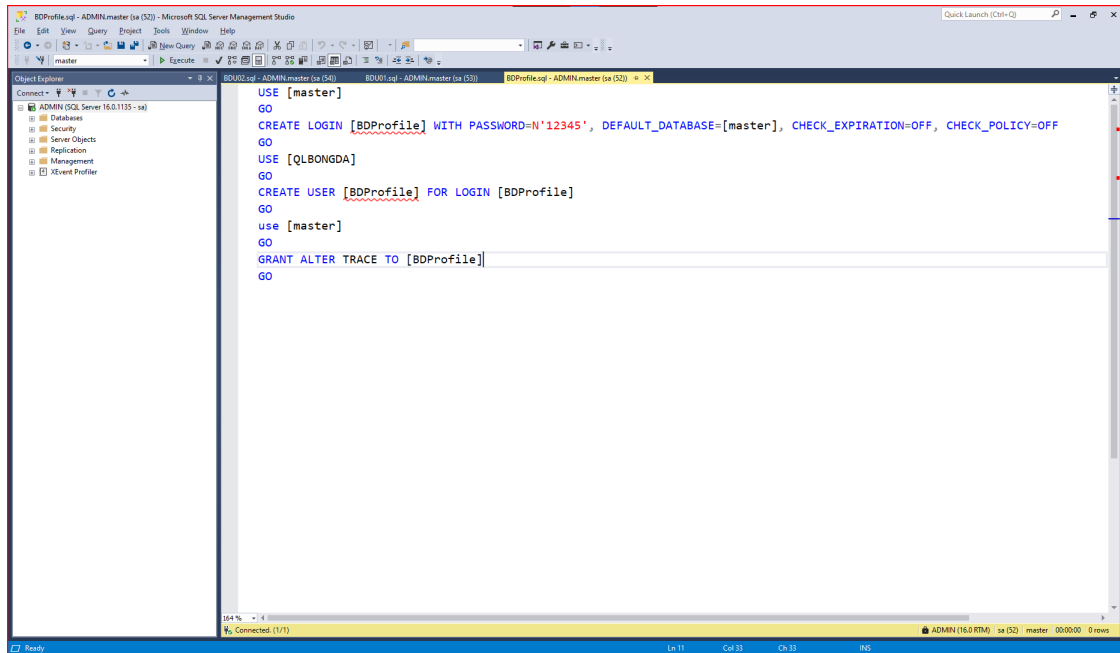
Hình 5: BDU02



Hình 6: BDU03

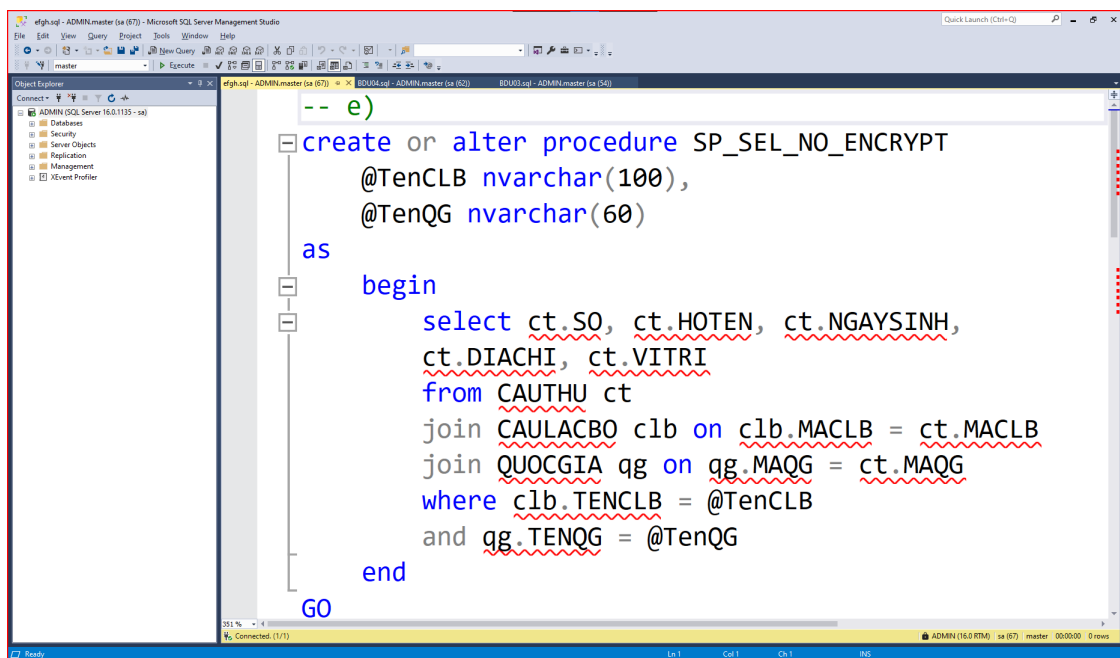


Hình 7: BDU04



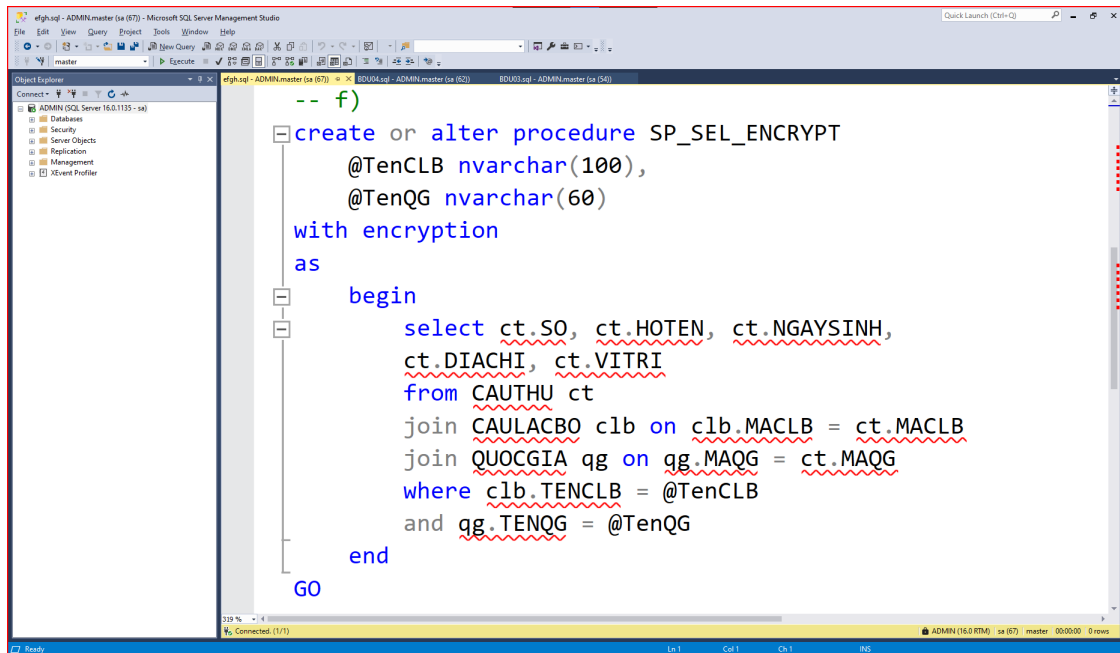
Hình 8: BDProfile

4 Tạo stored procedure với yêu cầu cho biết mã số, họ tên, ngày sinh, địa chỉ



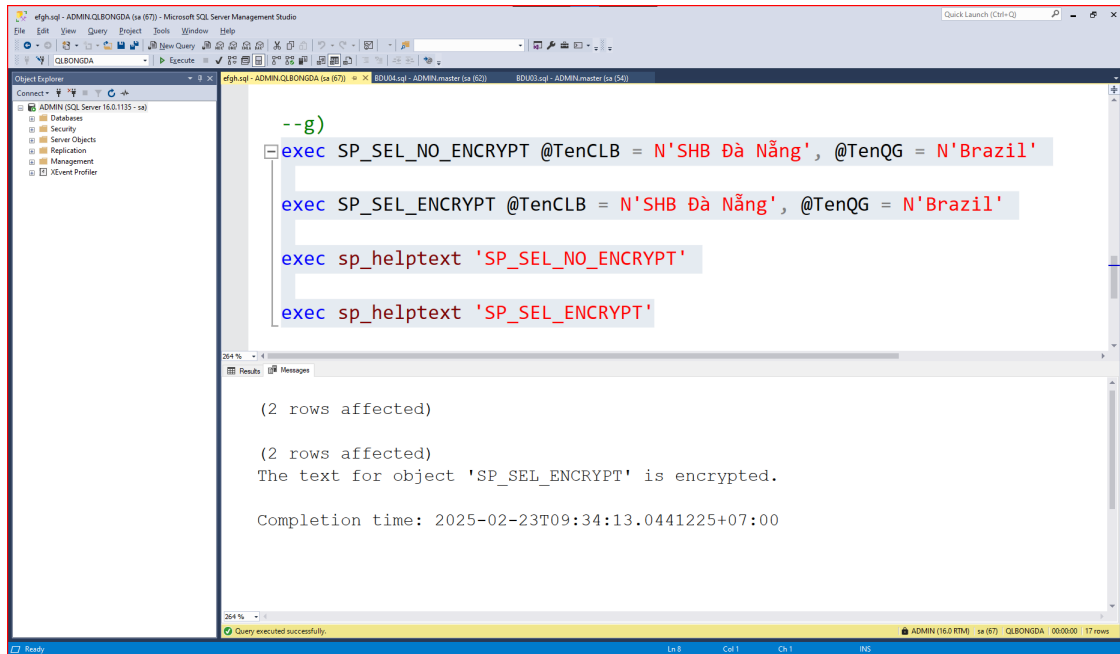
Hình 9: Stored procedure SP_SEL_NO_ENCRYPT

5 Tạo stored procedure với yêu cầu như câu e, với nội dung stored được mã hóa

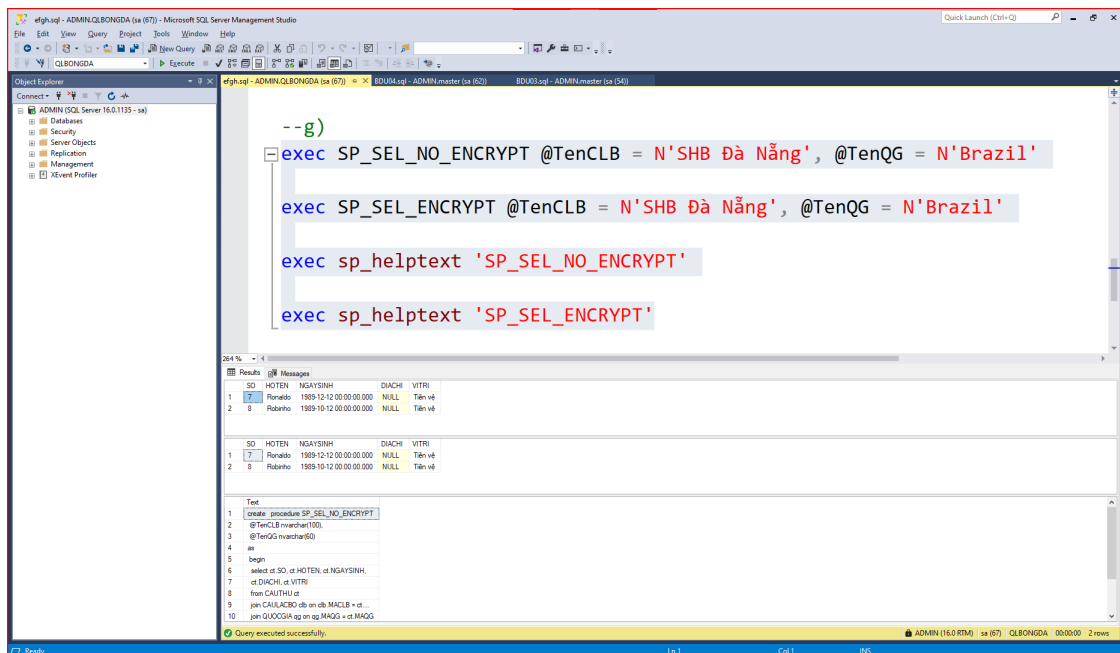


Hình 10: Stored procedure SP_SEL_ENCRYPT

6 Thực thi 2 stored procedure trên



Hình 11: Stored procedure SP_SEL_NO_ENCRYPT



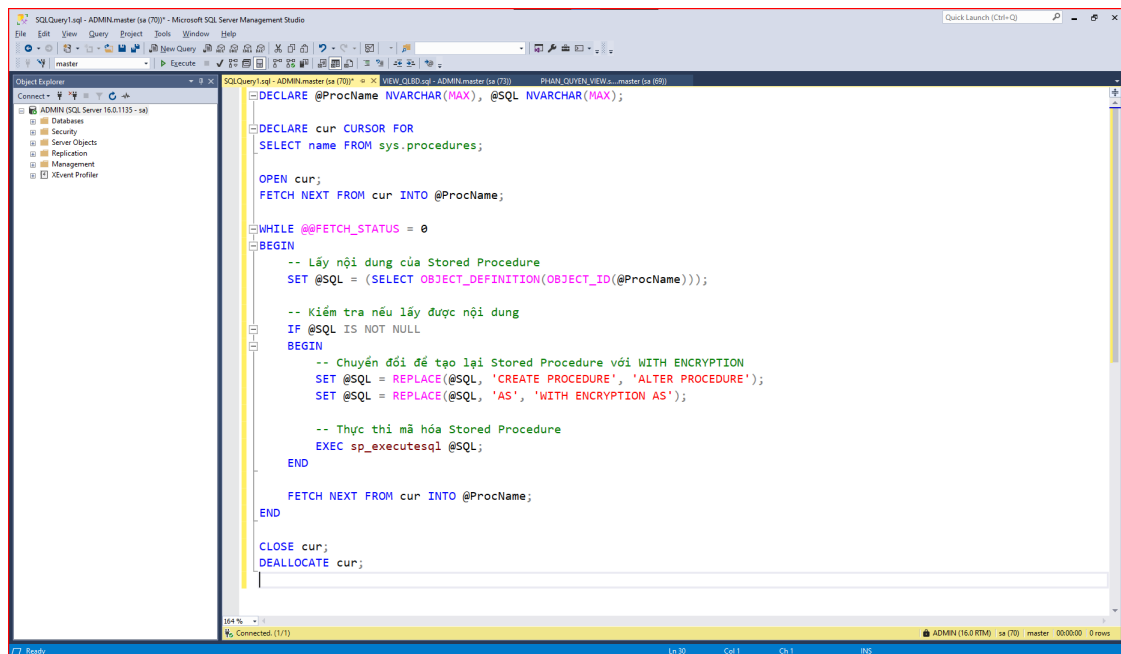
Hình 12: Stored procedure SP_SEL_ENCRYPT

Nhận xét:

- Cả 2 stored procedure đều trả về đúng kết quả yêu cầu.
- Khi dùng sp_helptext thì đối với SP_SELENCRYPT, ta không thể xem được nội dung do stored procedure này đã được mã hoá.
- Vì được mã hoá, SP_SELENCRYPT có tính bảo mật cao hơn nhưng lại làm cho việc kiểm tra, bảo trì khó hơn so với SP_SELL_NO_ENCRYPT.

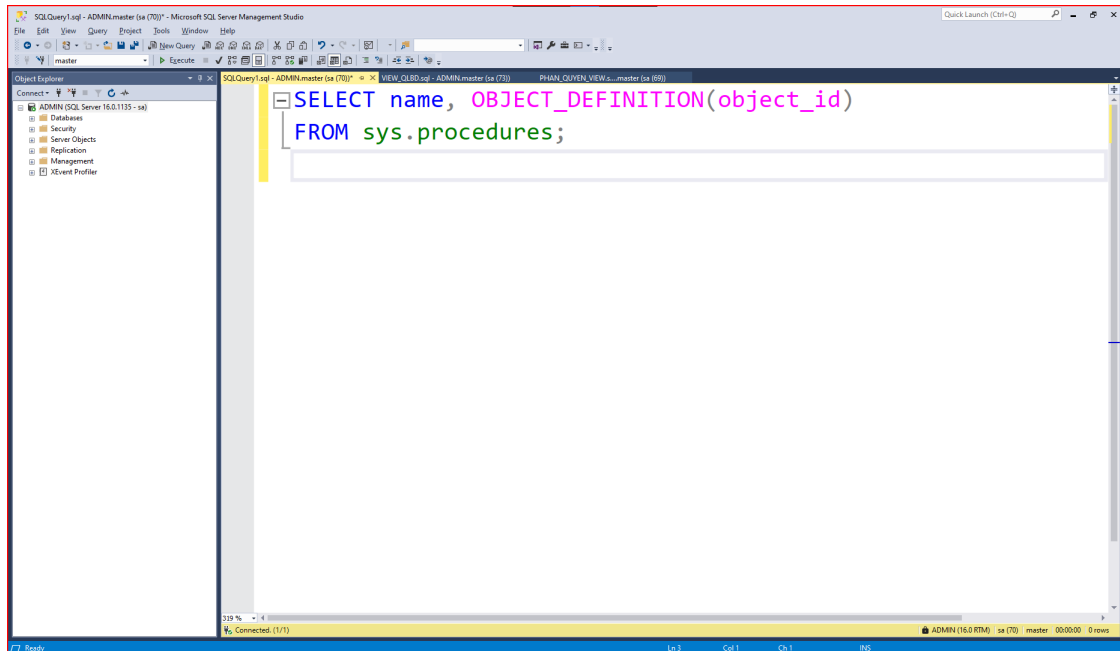
7 Cách nào để Encrypt toàn bộ 100 stored procedure

Vì không thể trực tiếp sửa đổi một Stored Procedure để thêm WITH ENCRYPTION, cần phải tạo lại chúng với tùy chọn này. Có thể sử dụng truy vấn sau để tự động tạo lại tất cả:



Hình 13: Script mã hoá tất cả stored procedure

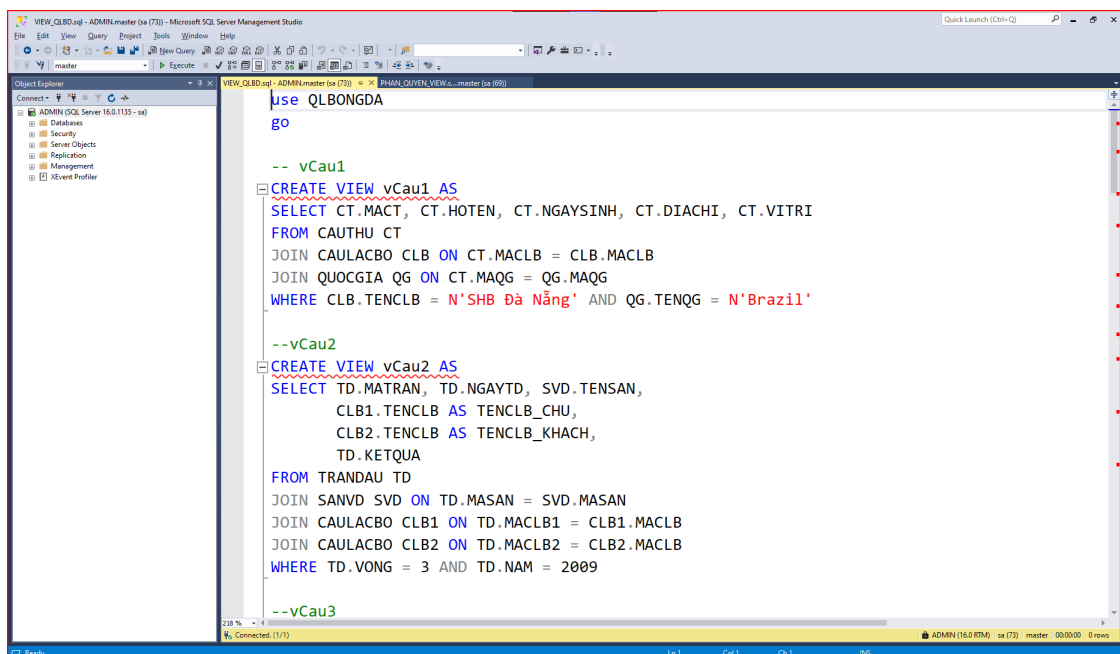
Sau khi chạy script, có thể kiểm tra xem các Stored Procedure đã được mã hóa hay chưa bằng cách chạy:



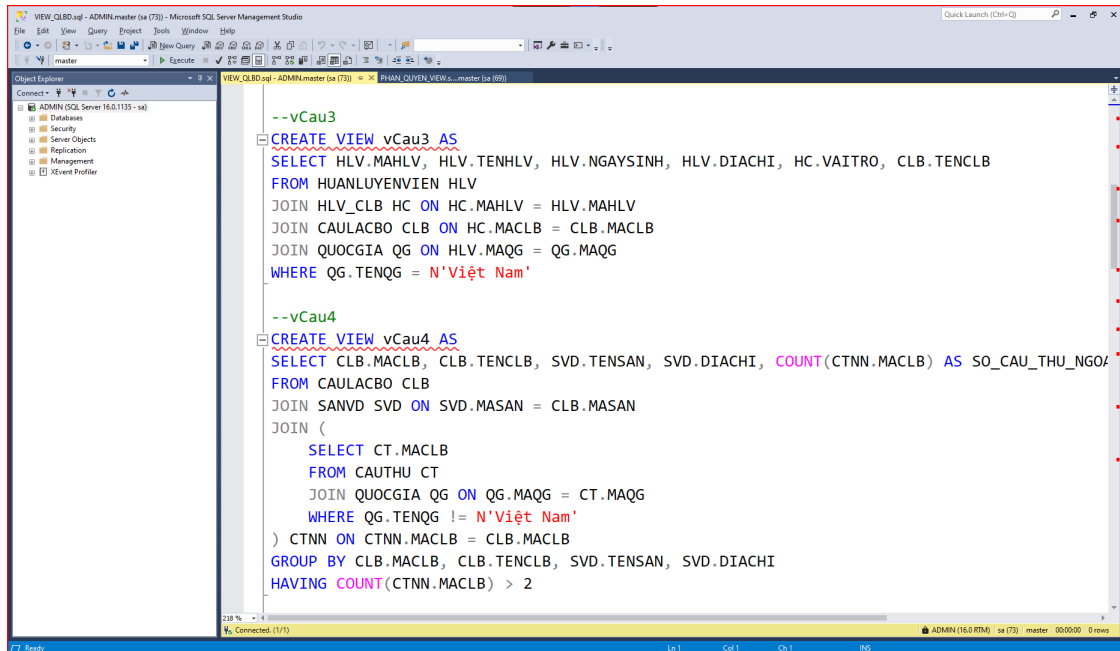
Hình 14: Script check stored procedure đã được mã hoá

Nếu một Stored Procedure đã được mã hóa, OBJECT_DEFINITION(object_id) sẽ trả về NULL.

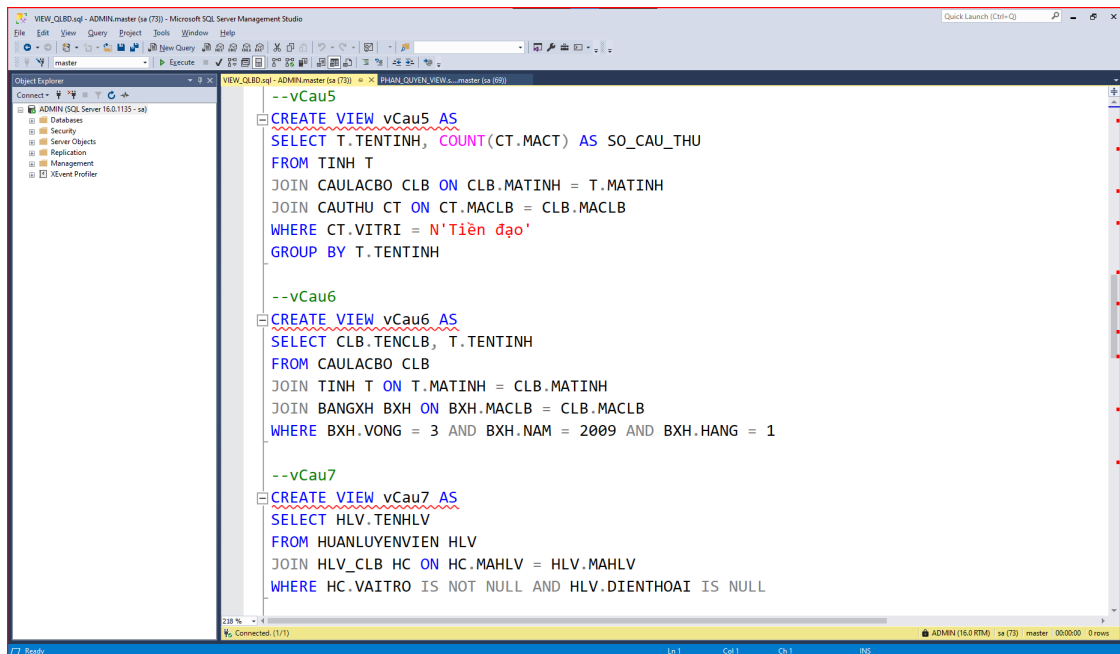
8 Tạo và phân quyền trên Views



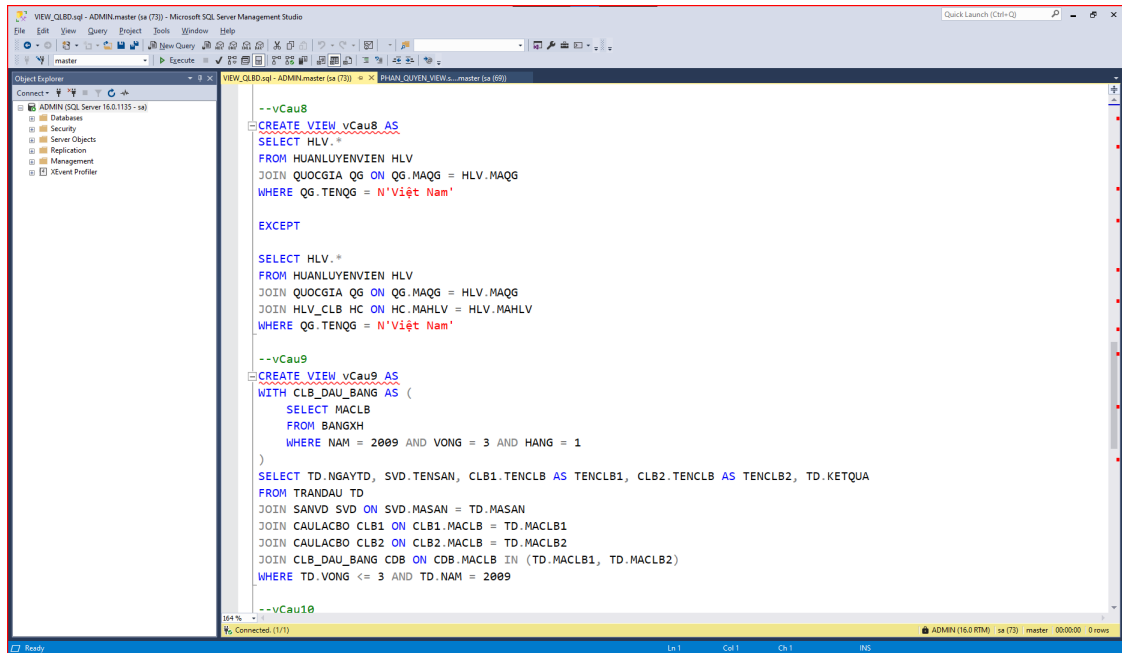
Hình 15: vCau1 - vCau2



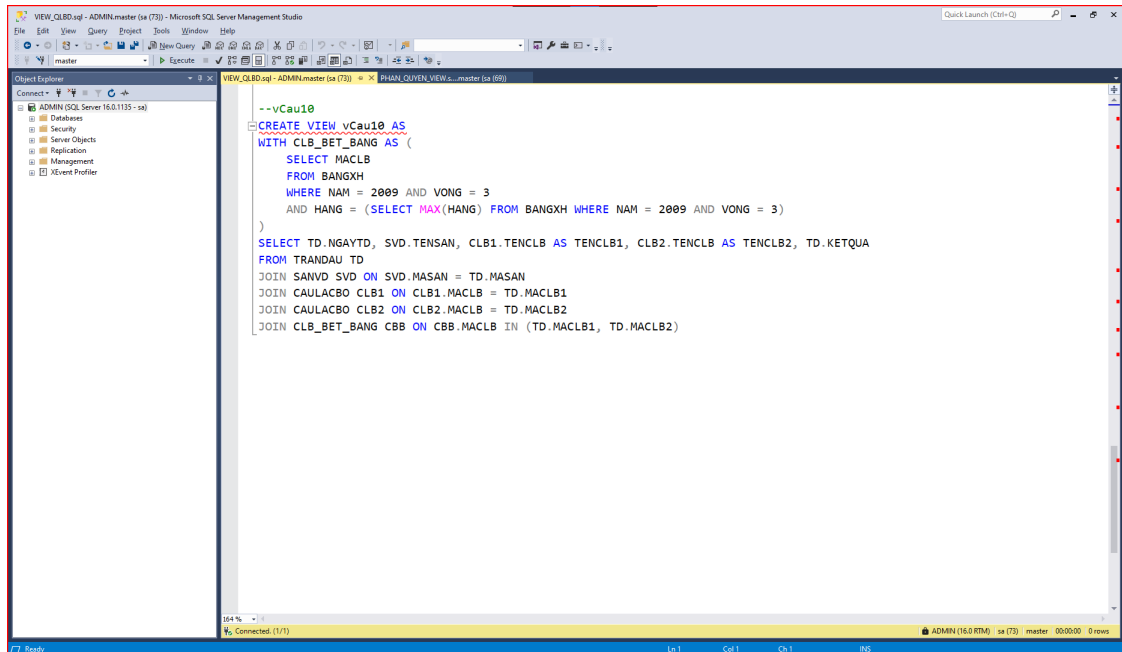
Hình 16: vCau3 - vCau4



Hình 17: vCau5 - vCau6 - vCau7



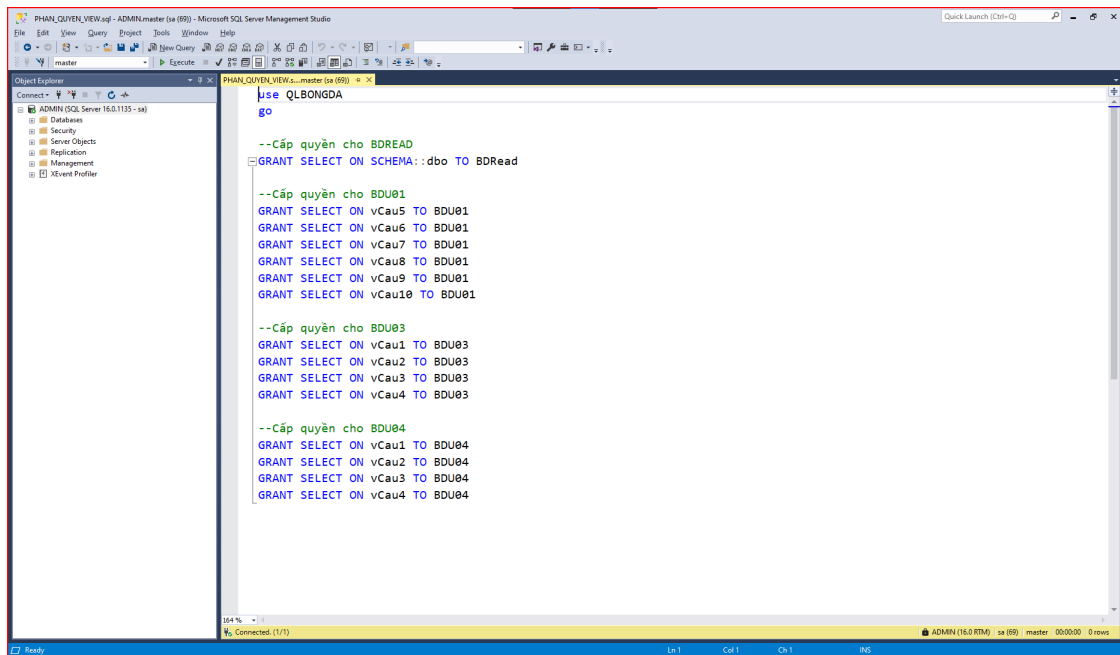
Hình 18: vCau8 - vCau9



Hình 19: vCau10

STT	Tên User	Thực thi câu select
1	BDRead	Được phép truy xuất tất cả các View
2	BDU01	Chỉ được phép truy xuất các View vCau5 - vCau10
3	BDU03	Được phép truy xuất view vCau1, vCau2, vCau3, vCau4
4	BDU04	Được phép truy xuất view vCau1, vCau2, vCau3, vCau4

Bảng 2: Bảng phân quyền cho các user

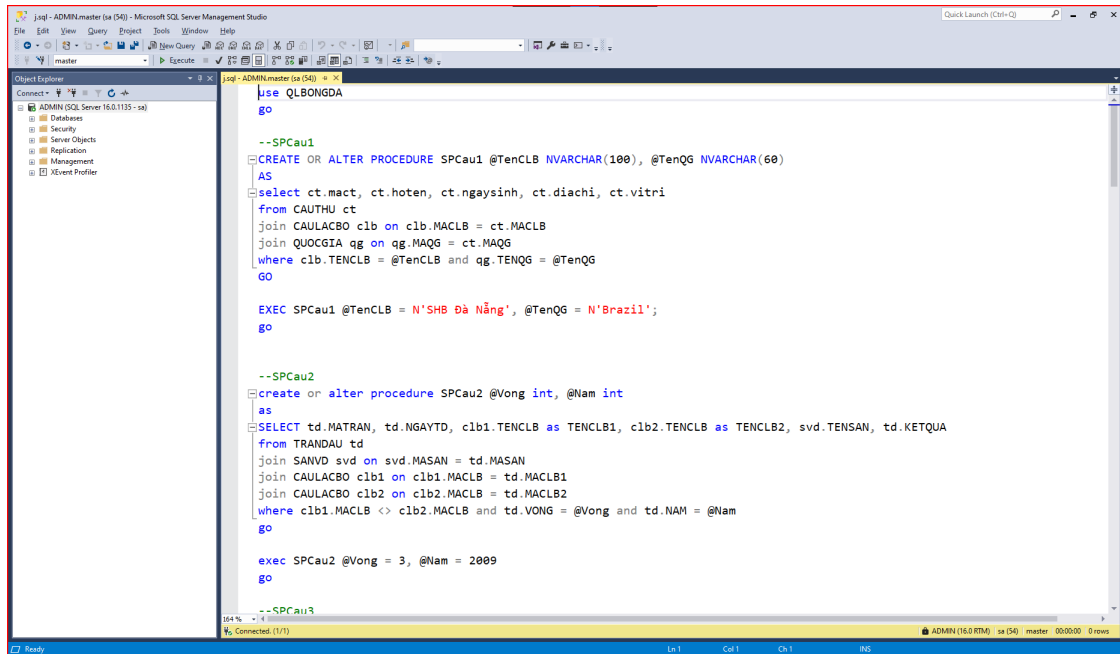


Hình 20: Phân quyền cho các user

STT	Tên User	Thực thi câu select	Giải thích kết quả
1	BDRead	SELECT * FROM vCau1 SELECT * FROM vCau5	Thành công Thành công
2	BDU01	SELECT * FROM vCau2 SELECT * FROM vCau10	Không thành công do không được phân quyền Thành công
3	BDU03	SELECT * FROM vCau1 SELECT * FROM vCau2 SELECT * FROM vCau3 SELECT * FROM vCau4	Thành công Thành công Thành công Thành công
4	BDU04	SELECT * FROM vCau1 SELECT * FROM vCau2 SELECT * FROM vCau3 SELECT * FROM vCau4	Thành công Thành công Thành công Thành công

Bảng 3: Kết quả thực thi câu lệnh select

9 Tạo và phân quyền trên Stored Procedure



```

-- QL BONGDA
go

-- SPCau1
CREATE OR ALTER PROCEDURE SPCau1 @TenCLB NVARCHAR(100), @TenQG NVARCHAR(60)
AS
select ct.mact, ct.hoten, ct.ngaysinh, ct.diachi, ct.vitri
from CAUTHU ct
join CAULACBO c1b on c1b.MACLB = ct.MACLB
join QUOCGIA qg on qg.MAQG = ct.MAQG
where c1b.TENCLB = @TenCLB and qg.TENQG = @TenQG
GO

EXEC SPCau1 @TenCLB = 'SHB Đà Nẵng', @TenQG = 'Brazil';
go

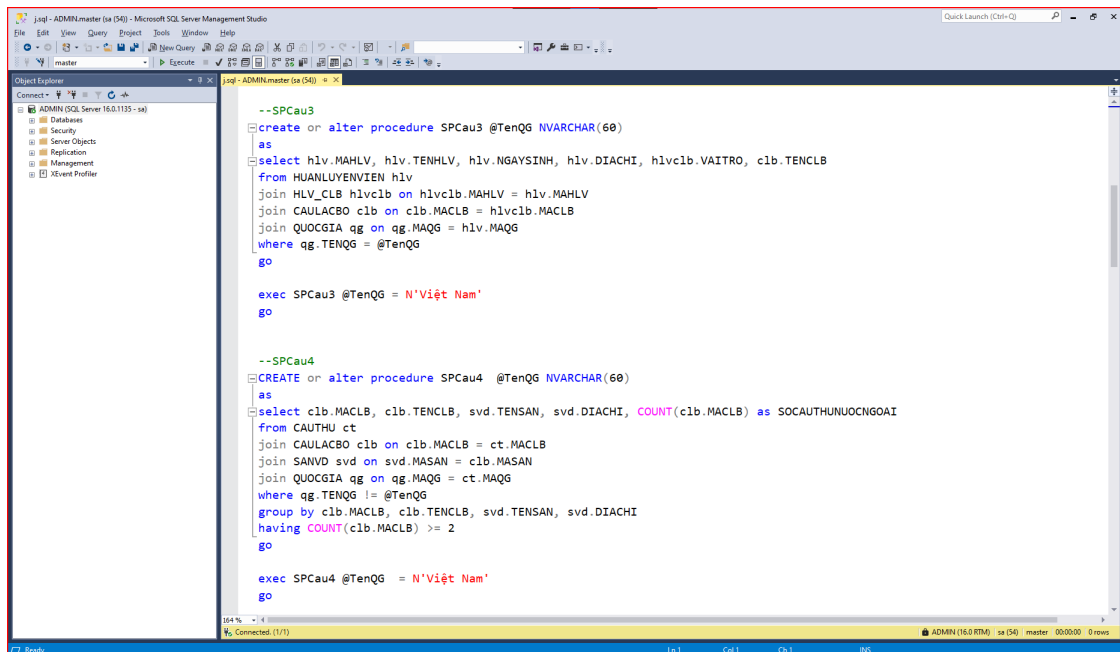
-- SPCau2
create or alter procedure SPCau2 @Vong int, @Nam int
as
SELECT td.MATRAN, td.NGAYTD, c1b1.TENCLB as TENCLB1, c1b2.TENCLB as TENCLB2, svd.TENSAN, td.KETQUA
from TRANDAU td
join SANVD svd on svd.MASAN = td.MASAN
join CAULACBO c1b1 on c1b1.MACLB = td.MACLB1
join CAULACBO c1b2 on c1b2.MACLB = td.MACLB2
where c1b1.MACLB <> c1b2.MACLB and td.VONG = @Vong and td.NAM = @Nam
go

exec SPCau2 @Vong = 3, @Nam = 2009
go

-- SPCau3

```

Hình 21: SPCau1 - SPCau2



```

-- SPCau3
create or alter procedure SPCau3 @TenQG NVARCHAR(60)
as
select hiv.MAHLV, hiv.TENHLV, hiv.NGAYSINH, hiv.DIACHI, hivclb.VAITRO, c1b.TENCLB
from HUANLUYENVIEN hiv
join HLV_CLB hivclb on hivclb.MAHLV = hiv.MAHLV
join CAULACBO c1b on c1b.MACLB = hivclb.MACLB
join QUOCGIA qg on qg.MAQG = hiv.MAQG
where qg.TENQG = @TenQG
go

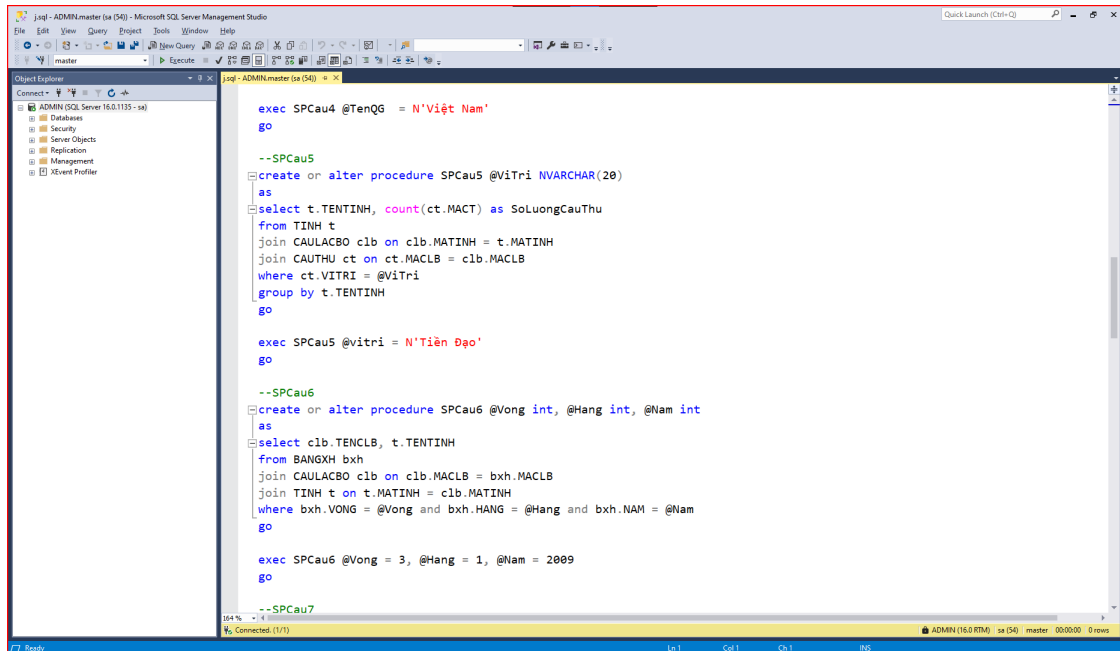
exec SPCau3 @TenQG = 'Việt Nam'
go

-- SPCau4
CREATE or alter procedure SPCau4 @TenQG NVARCHAR(60)
as
select c1b.MACLB, c1b.TENCLB, svd.TENSAN, svd.DIACHI, COUNT(c1b.MACLB) as SOCAUTHUNUOCNGOAI
from CAUTHU ct
join CAULACBO c1b on c1b.MACLB = ct.MACLB
join SANVD svd on svd.MASAN = c1b.MASAN
join QUOCGIA qg on qg.MAQG = ct.MAQG
where qg.TENQG != @TenQG
group by c1b.MACLB, c1b.TENCLB, svd.TENSAN, svd.DIACHI
having COUNT(c1b.MACLB) >= 2
go

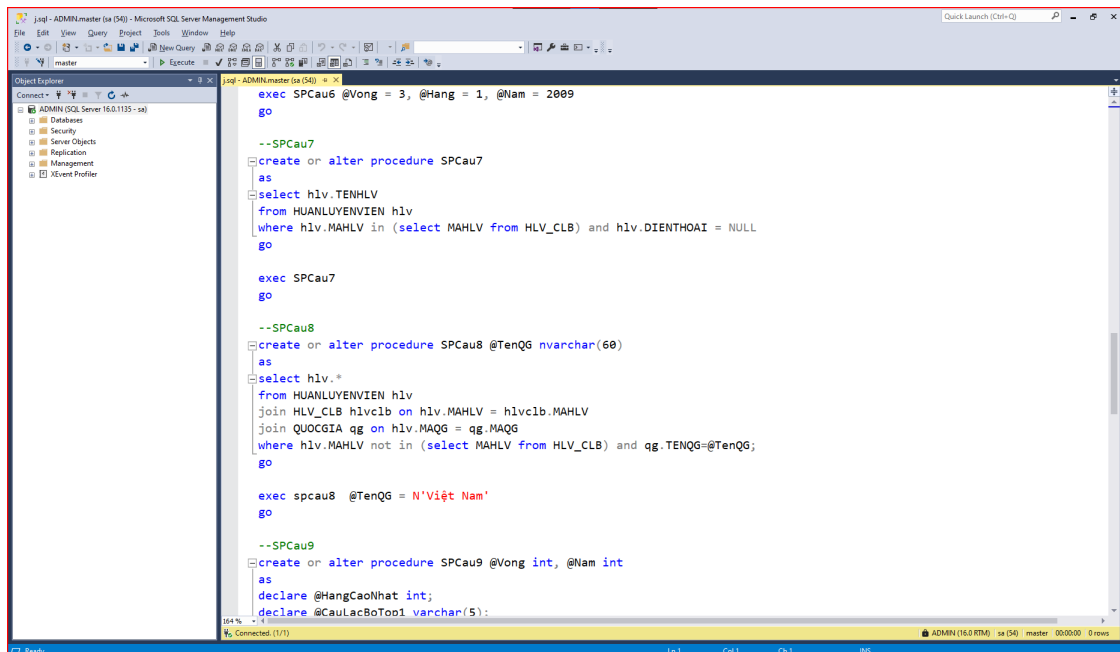
exec SPCau4 @TenQG = 'Việt Nam'
go

```

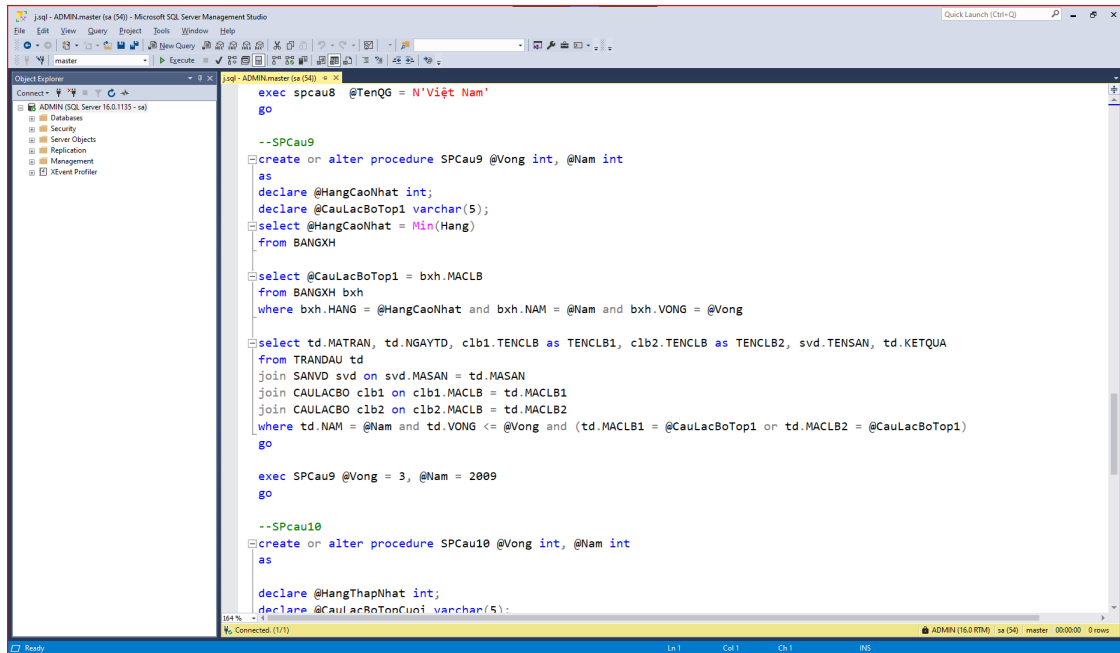
Hình 22: SPCau3 - SPCau4



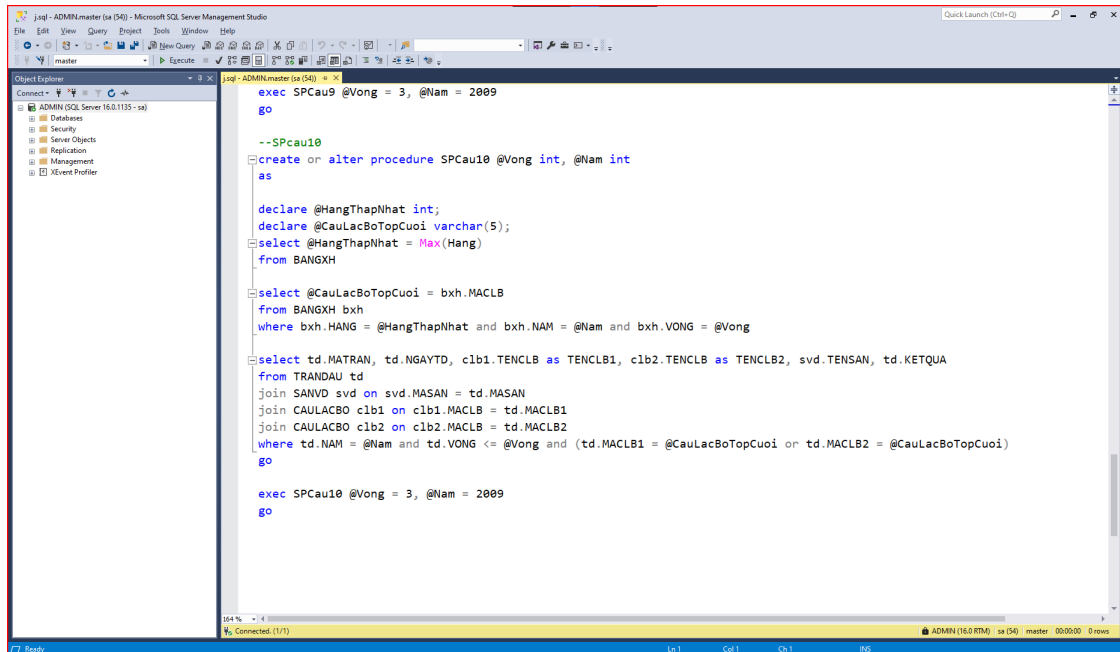
Hình 23: SPCau5 - SPCau6



Hình 24: SPCau7 - SPCau8



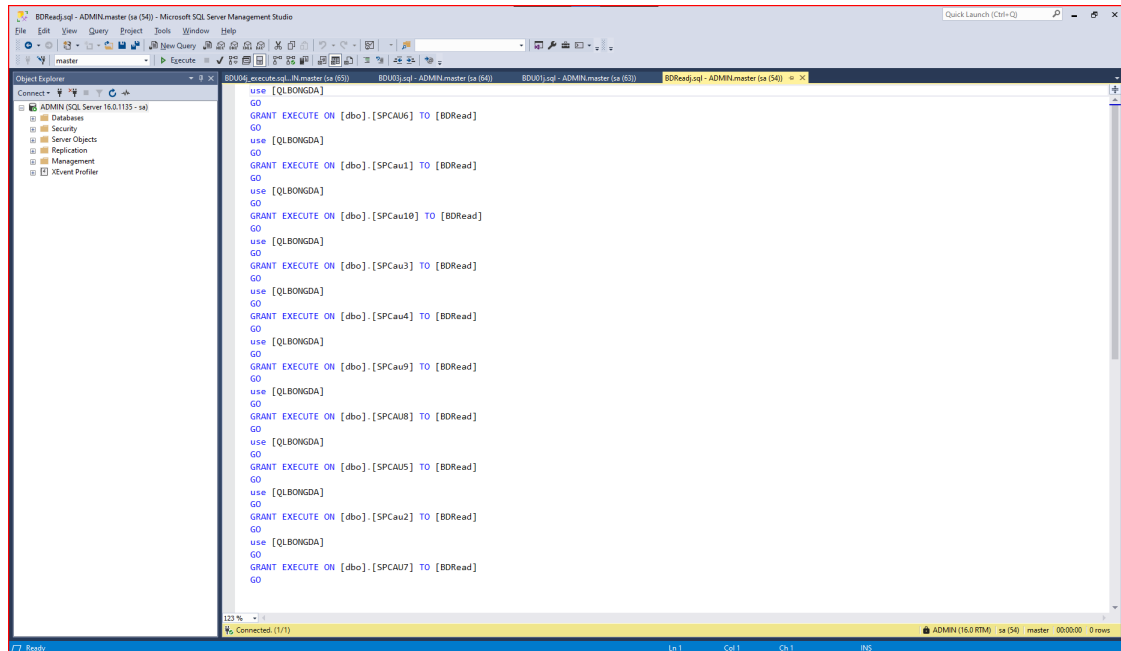
Hình 25: SPCau9



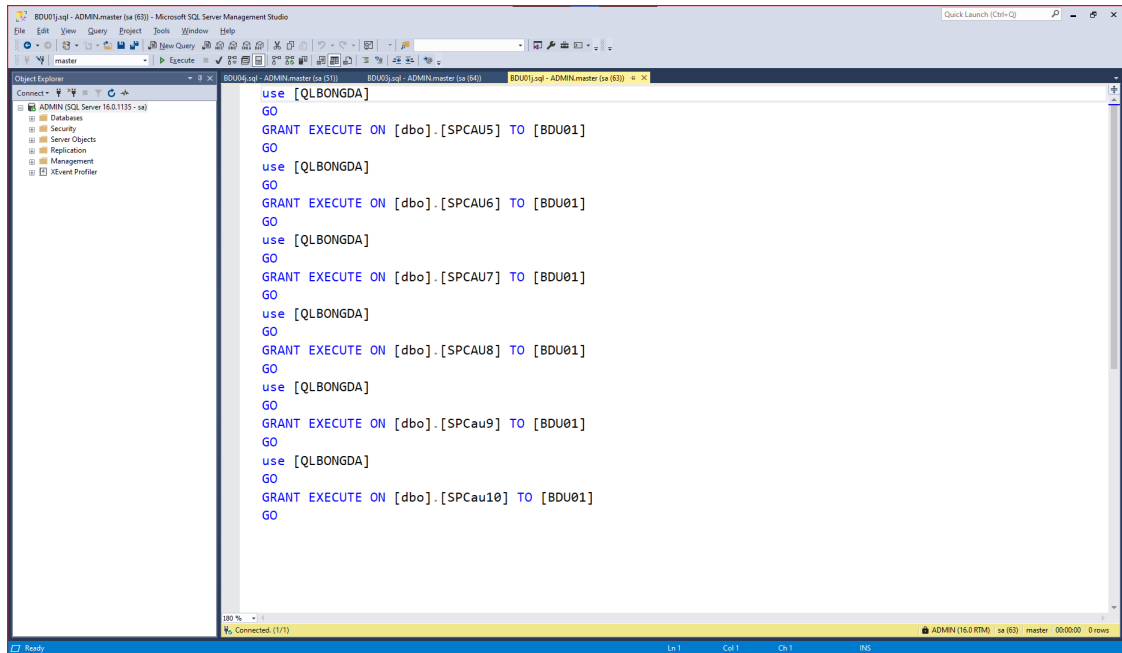
Hình 26: SPCau10

STT	Tên User	Vai trò
1	BDRead	Được phép thực thi tất cả các store procedure
2	BDU01	Chỉ được phép thực thi các store procedure SPCau5 - SPCau10
3	BDU03	Chỉ được phép thực thi các store procedure SPCau1 - SPCau4
4	BDU04	Chỉ được phép thực thi các store procedure SPCau1 - SPCau4

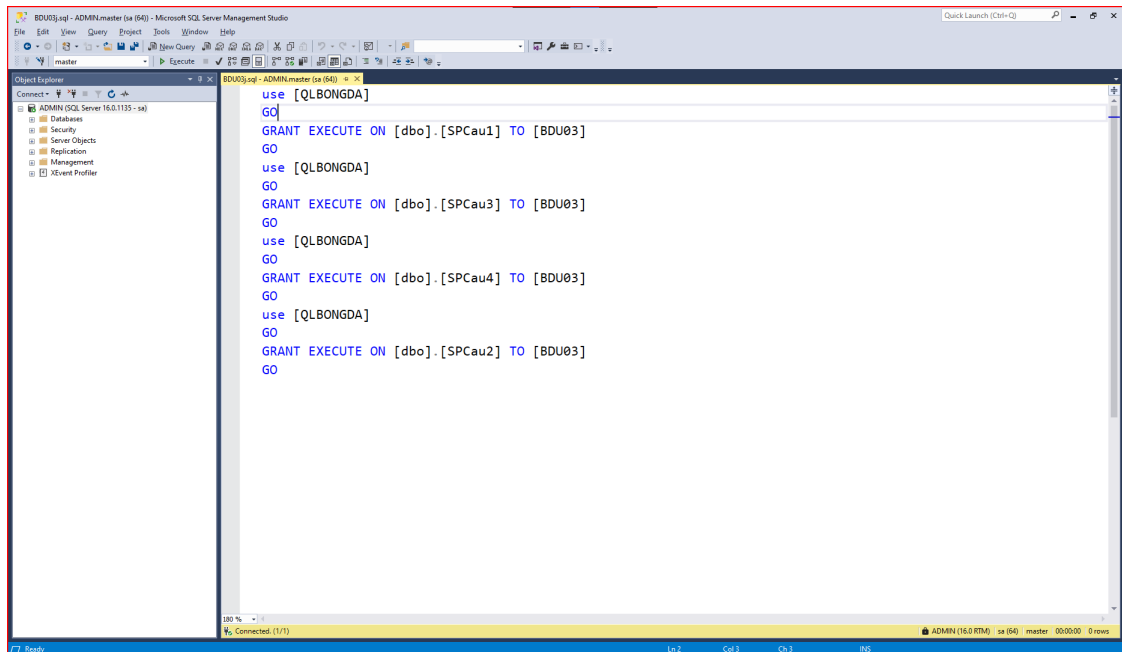
Bảng 4: Bảng phân quyền cho các user



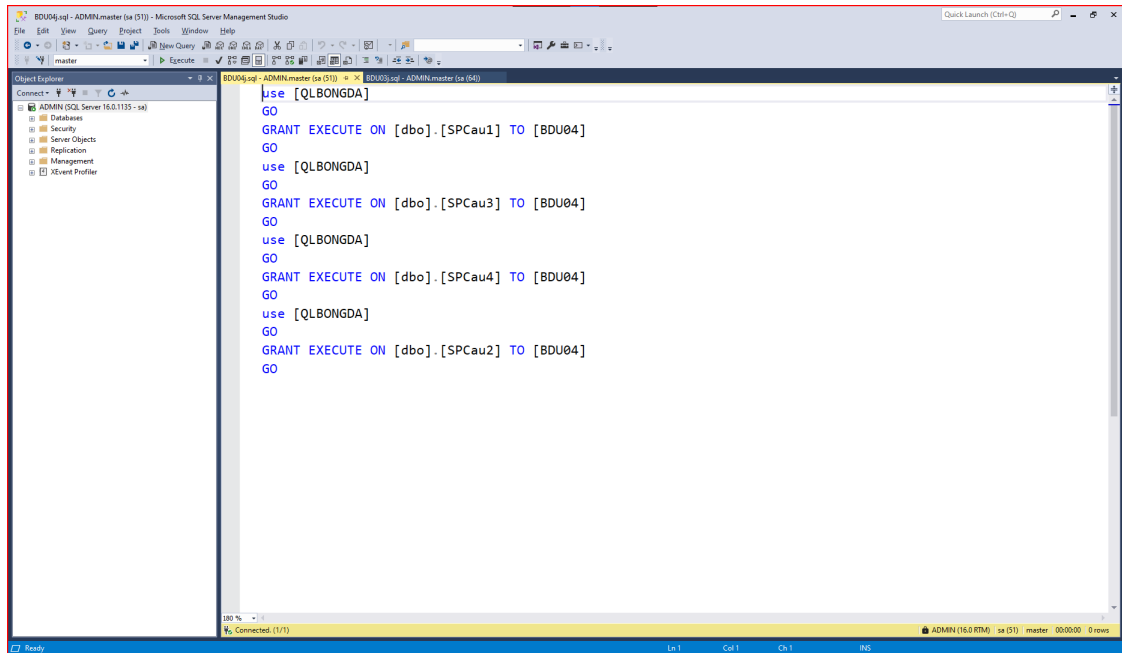
Hình 27: Phân quyền cho BDRead



Hình 28: Phân quyền cho BDU01



Hình 29: Phân quyền cho BDU03



Hình 30: Phân quyền cho BDU04

STT	Tên User	Thực thi câu exec	Giải thích kết quả
1	BDRead	EXEC SPCau1 'SHB Đà Nẵng', 'Brazil' EXEC SPCau9 3, 2009	Thành công Thành công
2	BDU01	EXEC SPCau1 'Việt Nam' EXEC SPCau10 3, 2009	Không thành công do không được phân quyền Thành công
3	BDU03	EXEC SPCau1 'SHB Đà Nẵng', 'Brazil' EXEC SPCau10 3, 2009 EXEC SPCau3 'Việt Nam' EXEC SPCau4 'Việt Nam'	Thành công Không thành công do không được phân quyền Thành công Thành công
4	BDU04	EXEC SPCau1 'SHB Đà Nẵng', 'Brazil' EXEC SPCau10 3, 2009 EXEC SPCau3 'Việt Nam' EXEC SPCau4 'Việt Nam'	Thành công Không thành công do không được phân quyền Thành công Thành công

Bảng 5: Kết quả thực thi câu lệnh exec

Tài liệu

- [1] [Cách phân quyền cho người dùng trong MS SQL Server](#)
- [2] [Học SQL Server - Bài 43. View trong cơ sở dữ liệu](#)
- [3] [Học SQL Server - Bài 45. Stored Procedures trong SQL Server](#)