THỰC HÀNH

Quản trị và Bảo trì hệ thống

MỤC LỤC

Contents
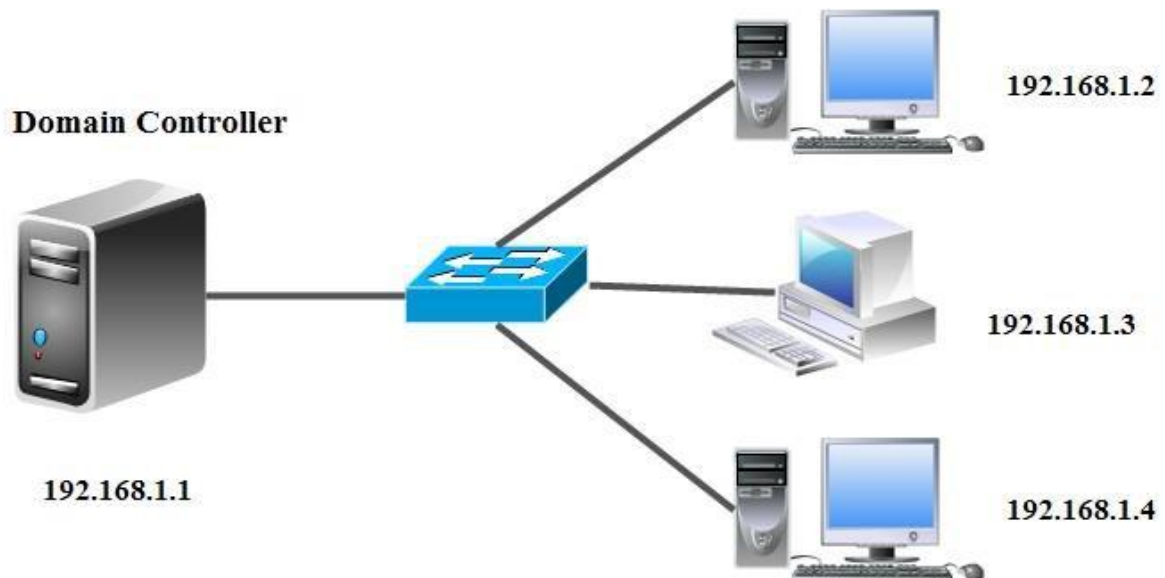
1   Triển khai hệ thống Domain

Sau khi học bài này học sinh viên có khả năng nâng cấp một máy Windows Server 2016 thành một máy Domain Controller, giúp các máy con gia nhập vào hệ thống domain mà ta đã nâng cấp
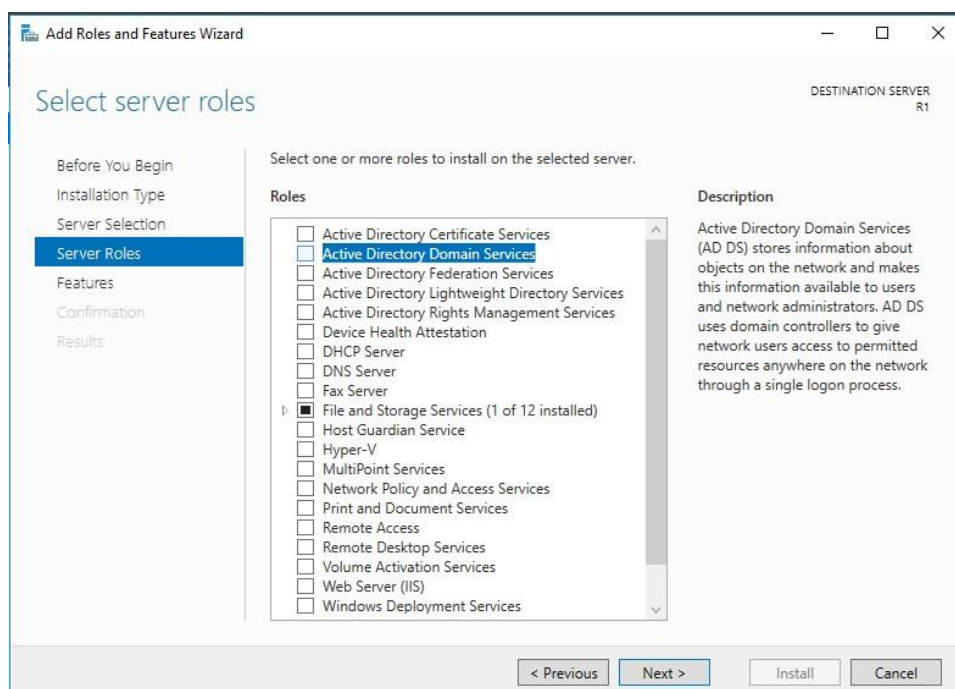
☐   Chuẩn bị:
+ Một máy server 2016
+ Một máy Client windows 7

☐   Mô hình
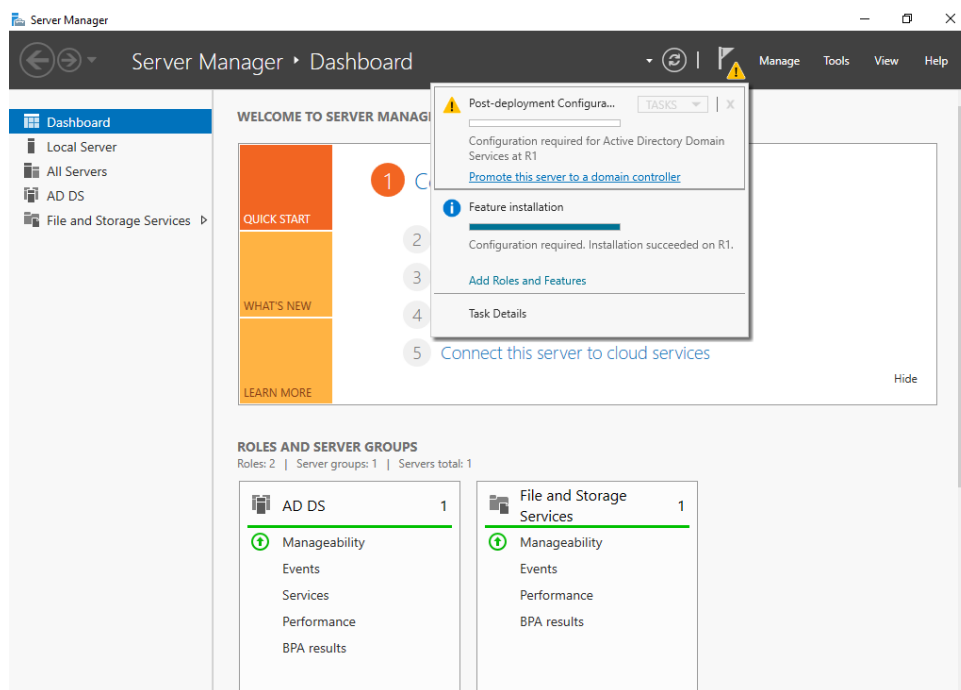

☐   Kết quả đạt được
☐   Máy client join vào domain, đăng nhập tài khoản ở ADDS trên máy client

☐   Thực hiện

☐ Khi đặt địa chỉ IP cho Server thì phải trỏ DNS về chính Server vì nó sẽ là nơi để phân giải tên miền mà ta sẽ sử dụng trong quá trình nâng cấp domain
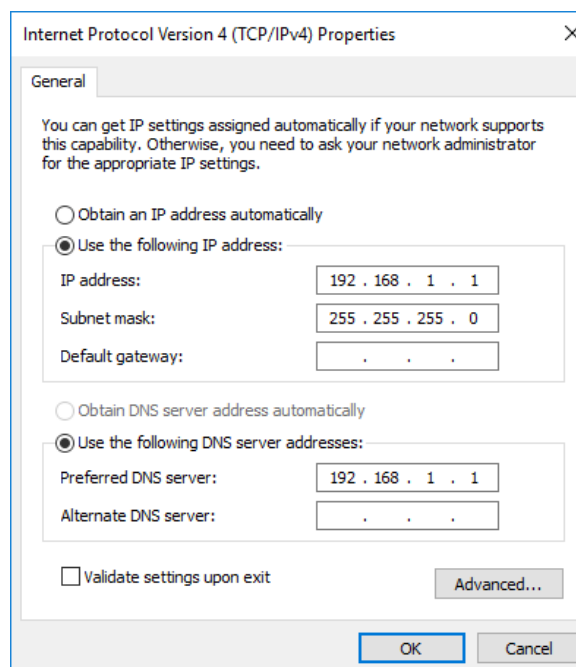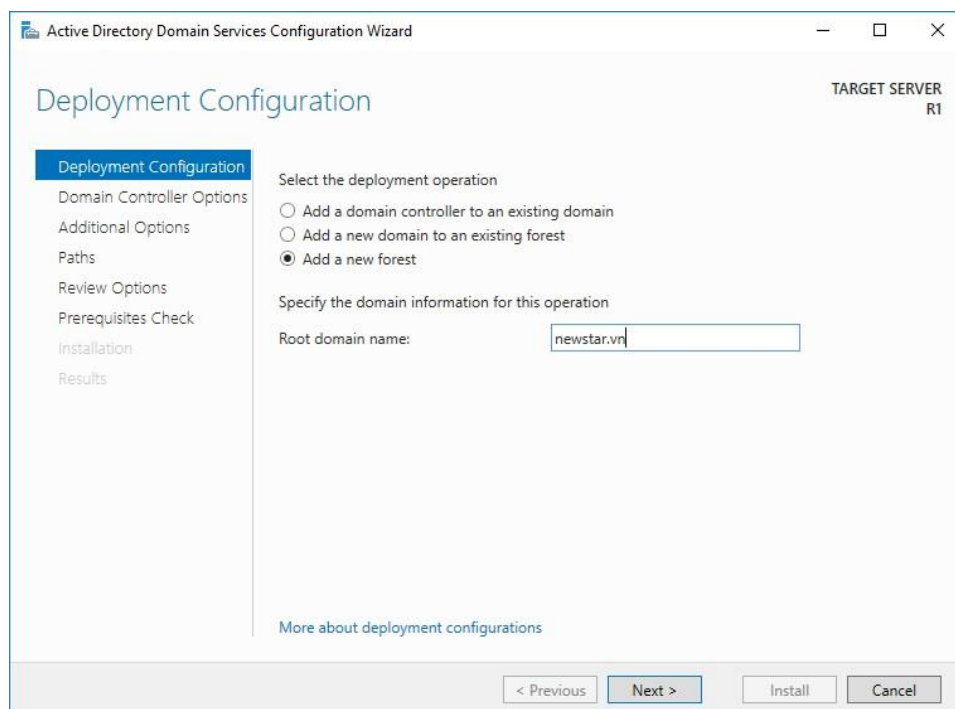
Hình 12-1: Đặt IP cho Server Domain
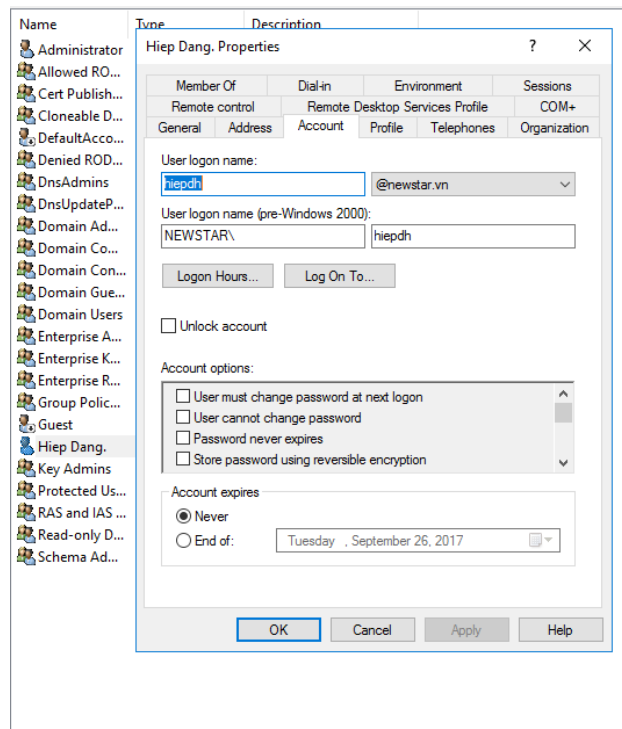

Hình 12-2: Cài dịch vụ ADDS
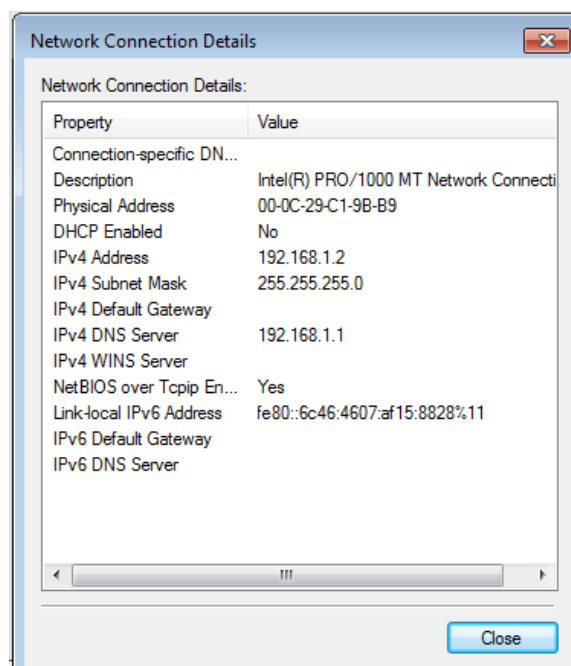
Hình 12-3: Cài Domain

Hình 12-4: Nhập tên domain

☐ Quá trình nâng cấp domain đã xong, ta tiến hành tạo tài khoản trên domain

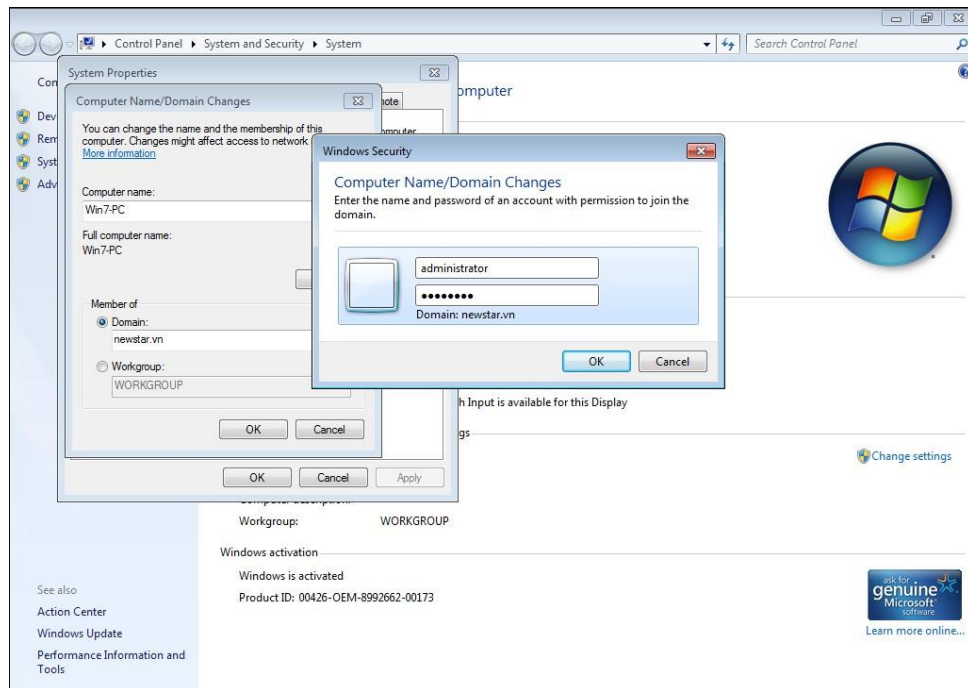*Hình 12-5: Tạo tài khoản trên domain*

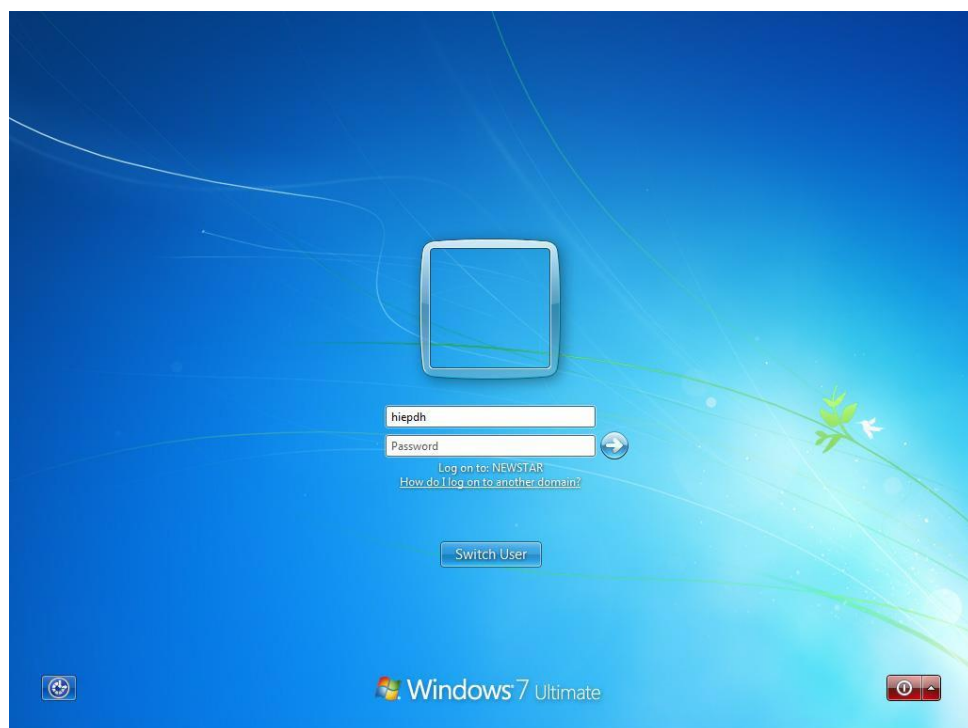☐ Đặt Ip trên máy client, trở DNS về Domain Controller

Hình 12-6: Đặt IP trên máy Client

☐ Tiến hành gia nhập domain, nhập phải chuột vào My computer chọn vào Property ☐change setting ☐Change, check mục Domain nhập tên domain

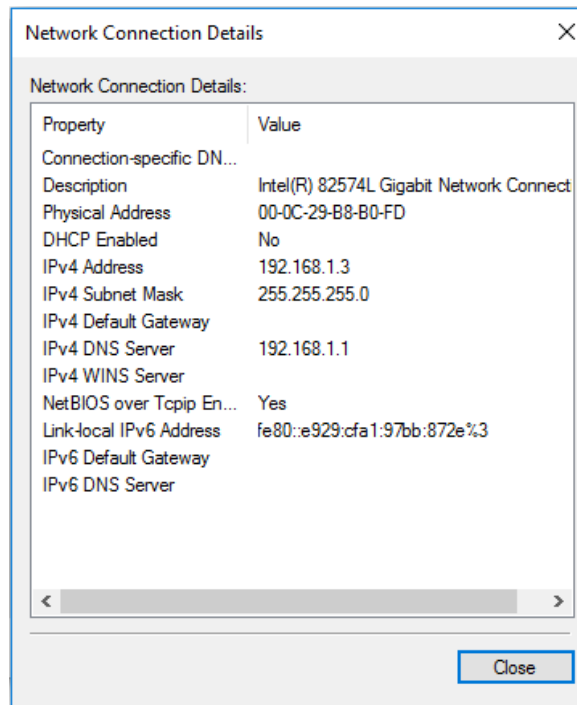vào. Sau đó có thông báo yêu cầu nhập tài khoản bên Domain, Nhập tài khoản administrator
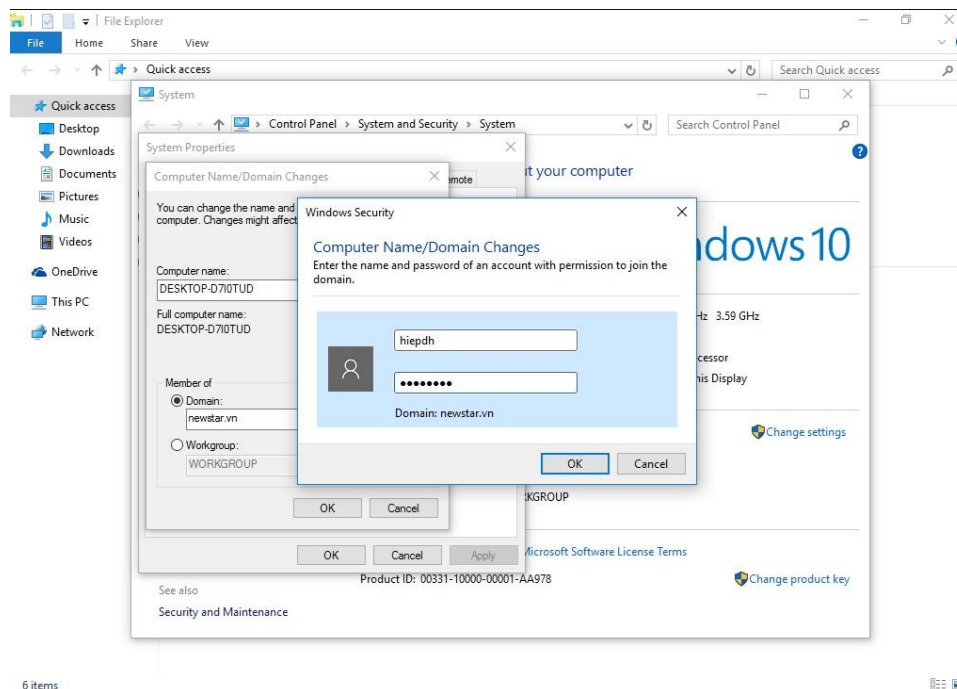

Hình 12-7: Nhập tài khoản trên domain

Hình 12-8: Đăng nhập tài khoản hiepdh

☐ Thực hiện gia nhập Domain trên máy windows 8
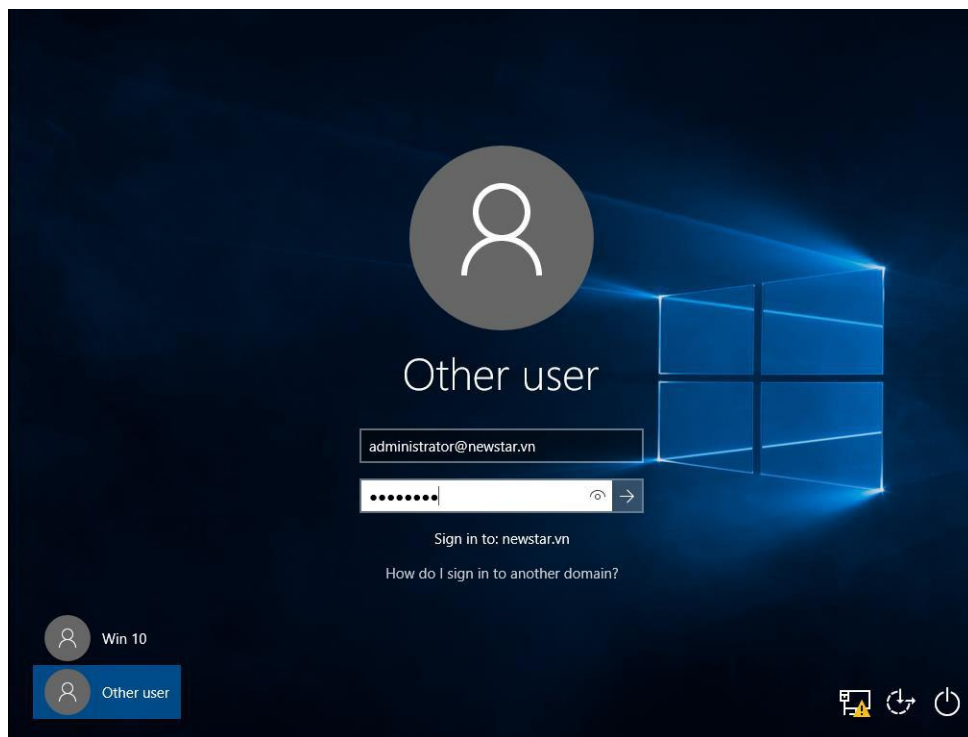

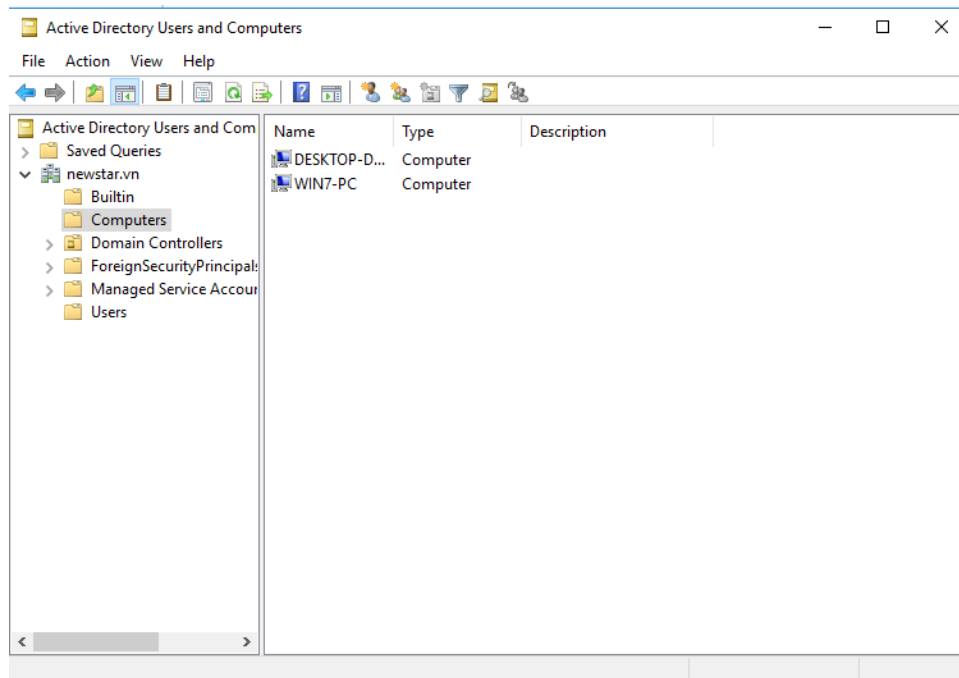*Hình 12-9: Đặt IP trên máy Client*

Hình 12-10: Đăng nhập tài khoản hiepdh trên domain

Hình 12-11: Đăng nhập tài khoản Administrator domain trên máy client

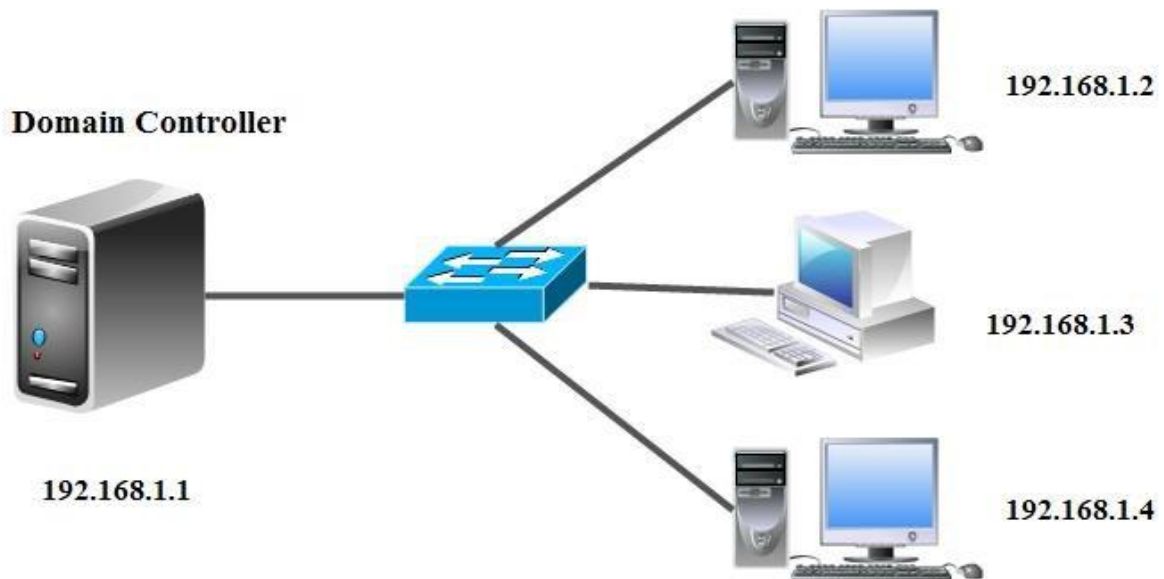☐ Sau khi gia nhập xong vào máy Domain ta sẽ thấy các máy client đã gia nhập
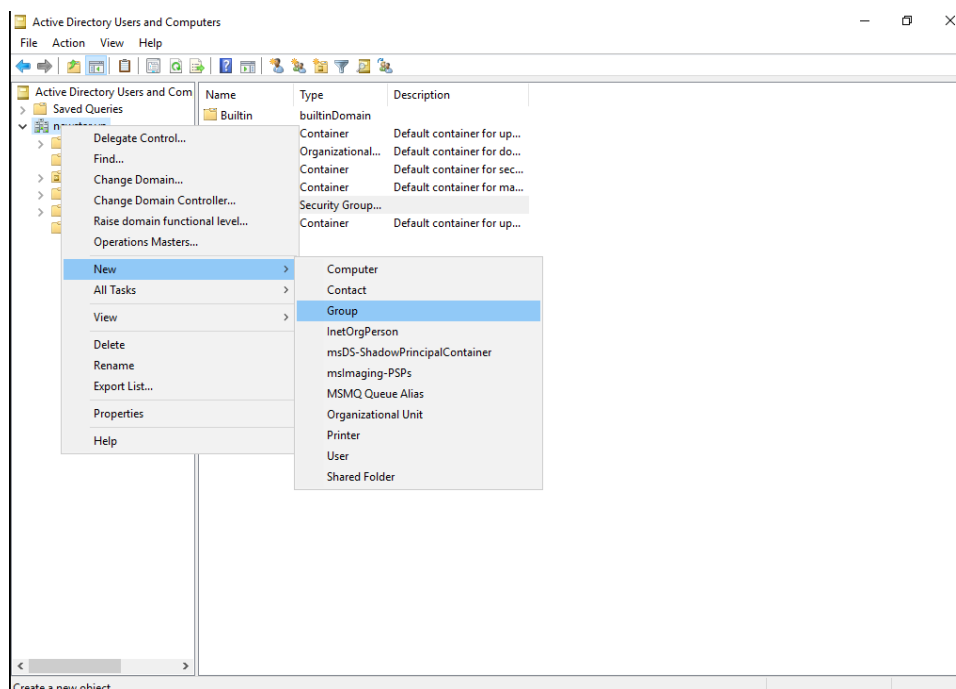

Hình 12-12: Các máy Join domain

2. Bảo mật ADDS và tài khoản người dùng

Sau khi học bài này học viên có thể tạo các đối tượng như OU, Group, User bằng giao diện và bằng dòng lệnh
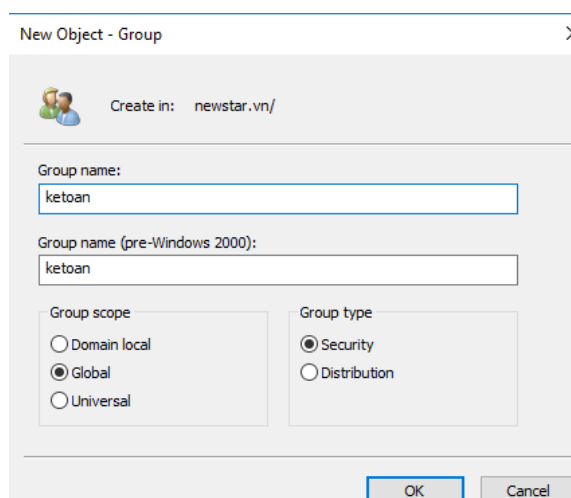
- Chuẩn bị:
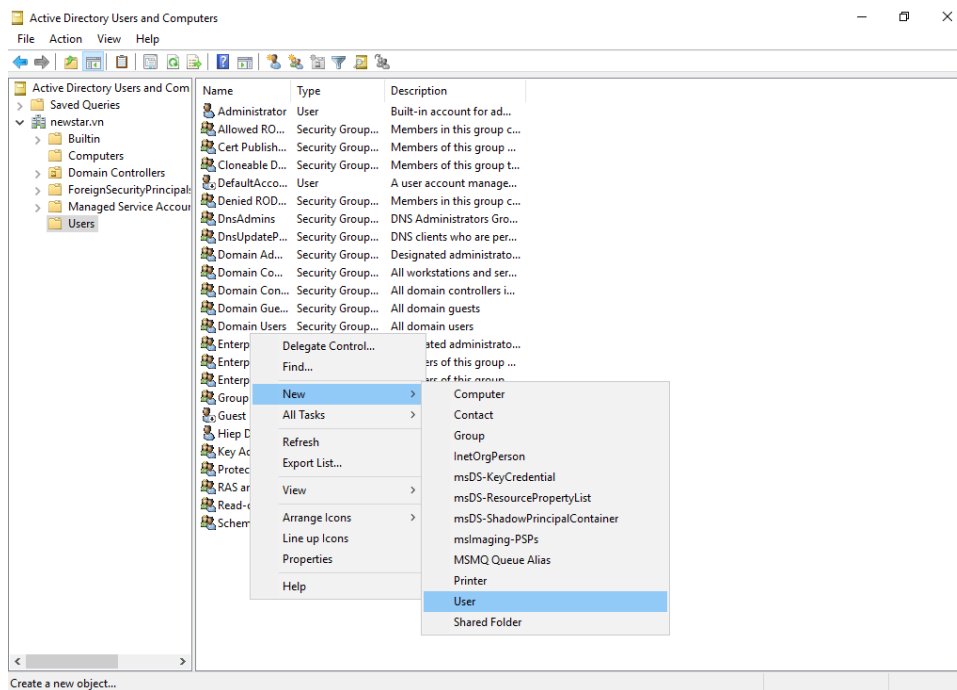   - Một máy server 2016 đã lên DC
    - Một máy Client windows 7
- Mô hình

- Kết quả đạt được
    - Tạo OU, User, Group
    - Hiệu chỉnh các chính sách tạo password bằng giao diện
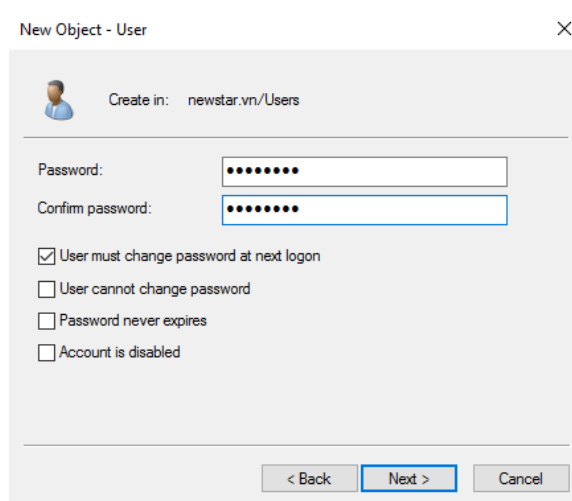- Thực hiện
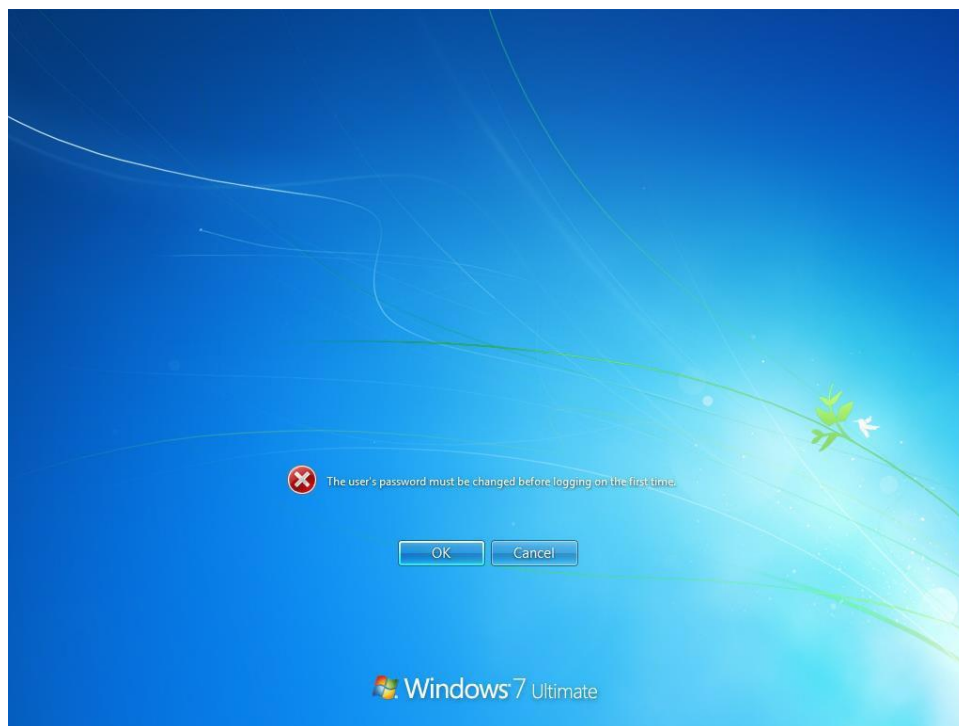- Tạo OU, Group, User bằng giao diện

Hình 13-1: Tạo Group

Hình 13-2: Định nghĩa Group

Hình 13-3: Tạo User

Hình 13-4: Nhập password với chính sách thay đổi pass ở lần đăng nhập đầu tiên

Hình 13-5: Yêu cầu đổi Password ở máy Client

Hình 13-6: Chọn chính sách không cho đổi Password
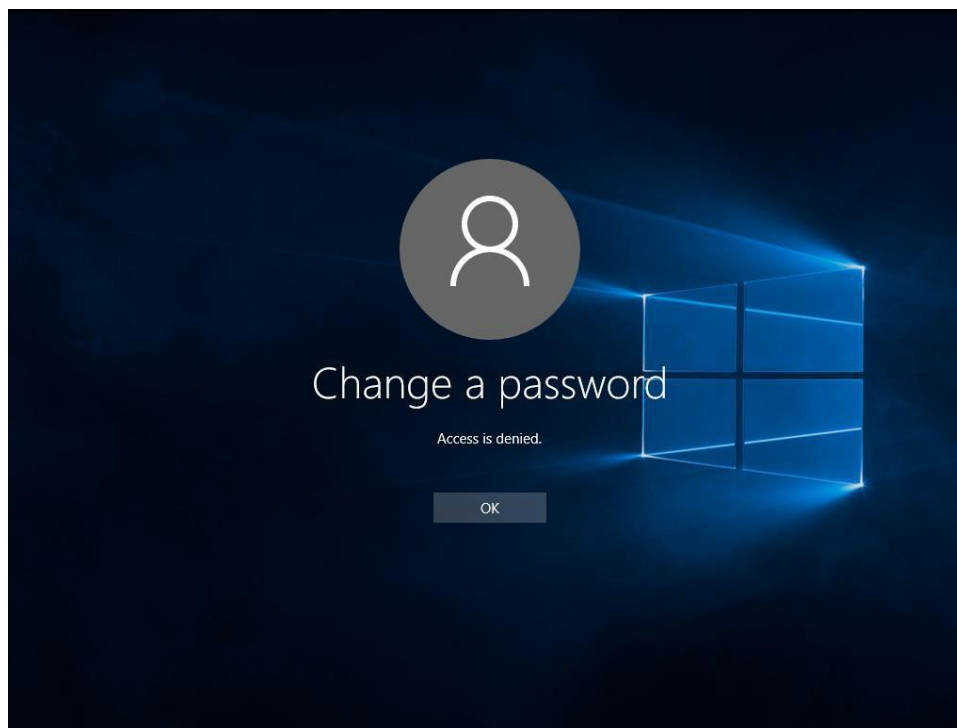
Hình 13-7: Không cho đổi Password

Hình 13-8: Password không hết hạn
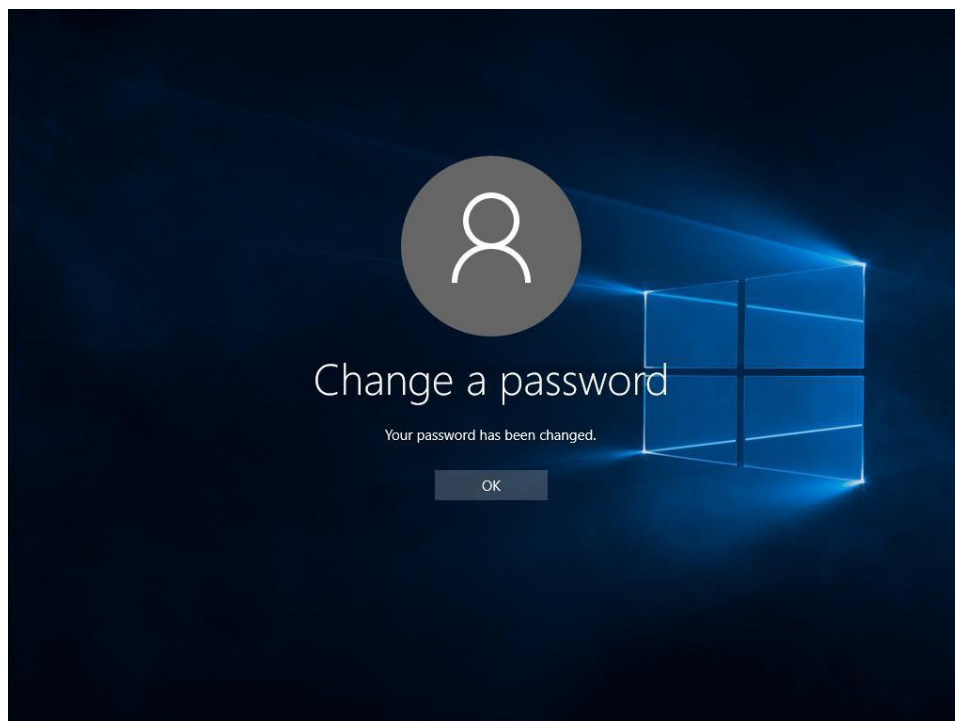
Hình 13-9: Đổi Password

Hình 13-10: Tài khoản vô hiệu hóa
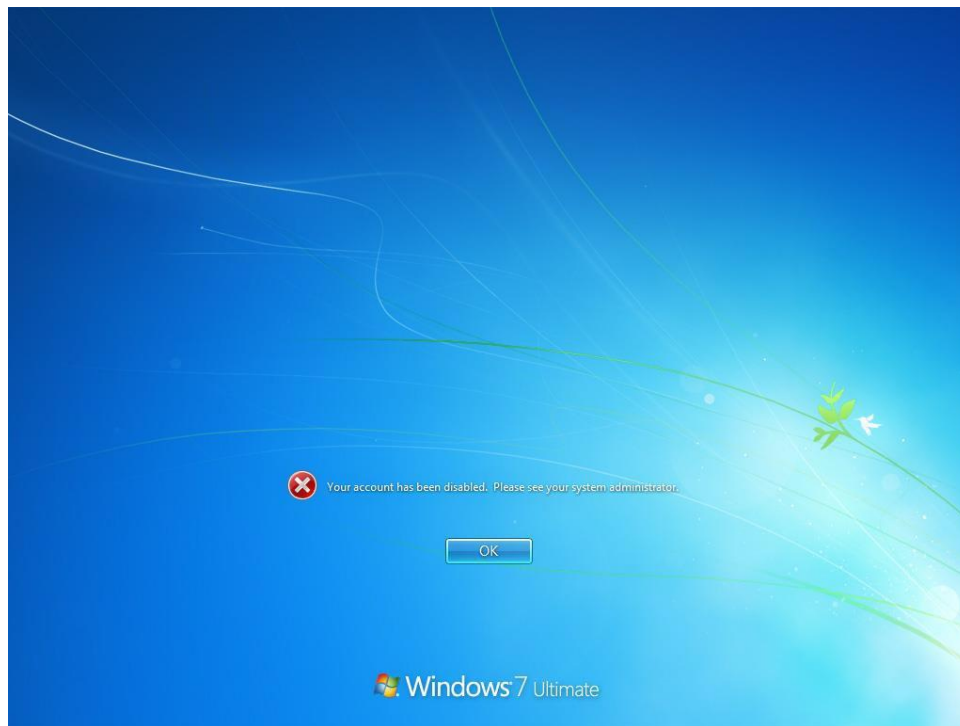
Hình 13-11: Tài khoản đã vô hiệu hóa
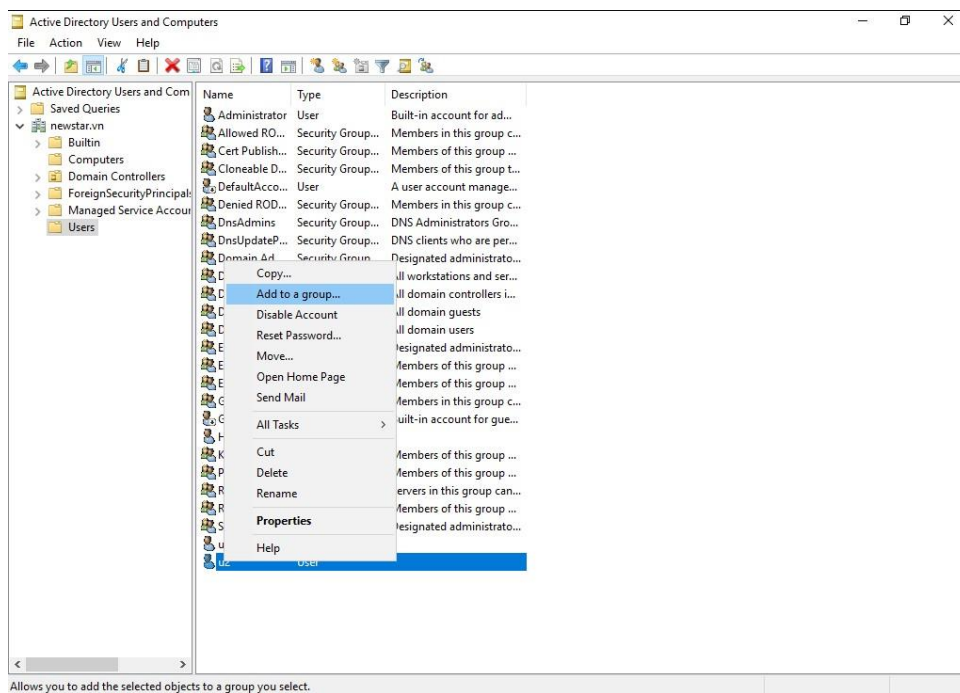
Hình 13-12: Đưa tài khoản vào group

Hình 13-13: Tài khoản đã đưa vào Group
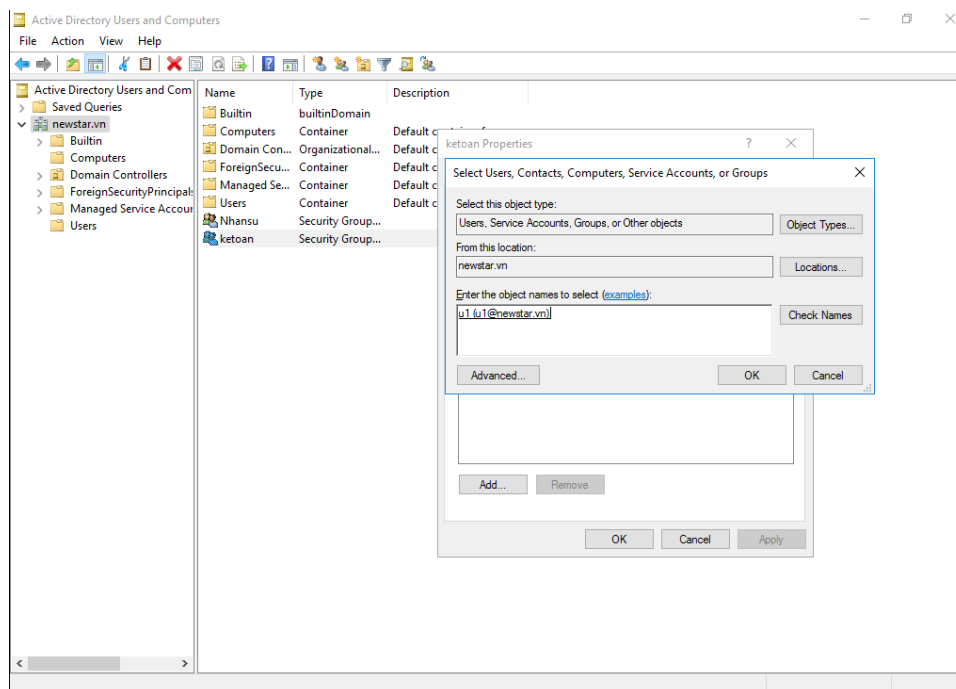
Hình 13-14: Add tài khoản vào group
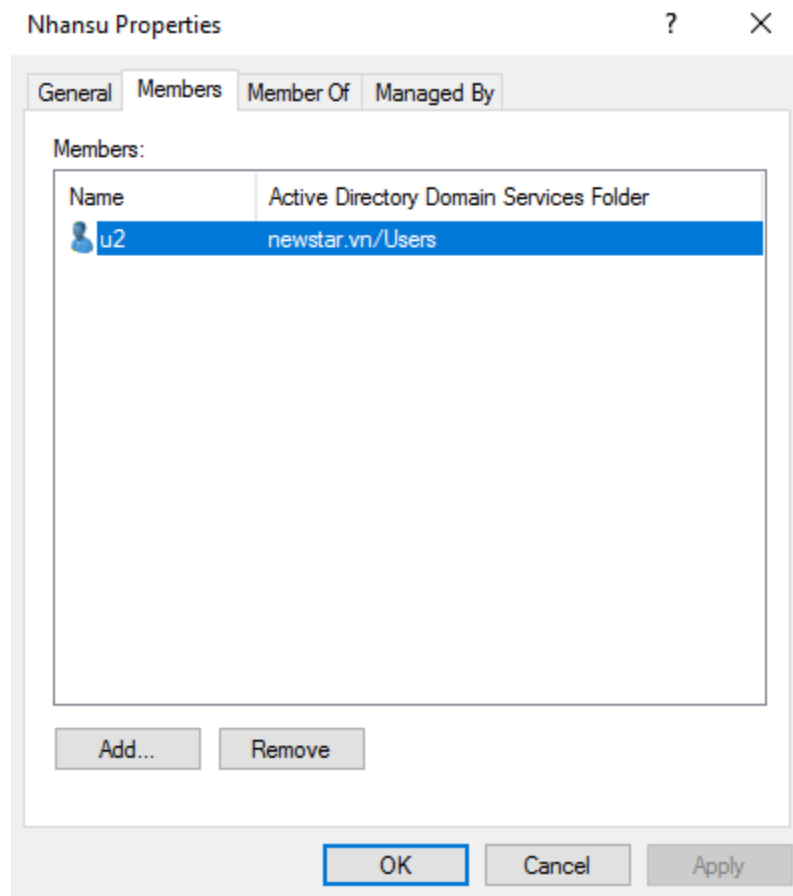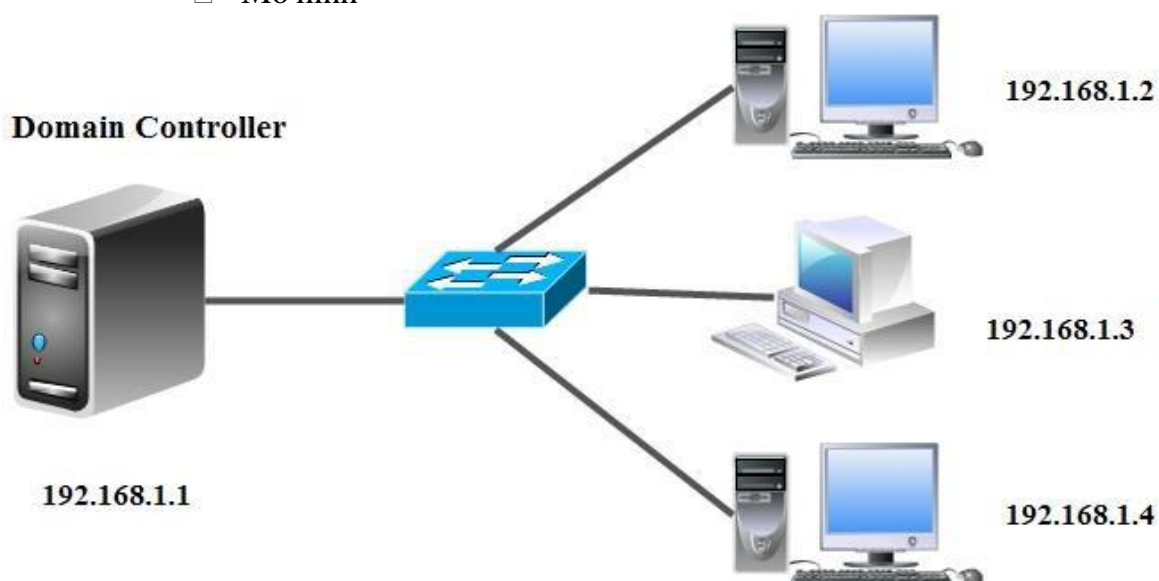
Hình 13-15: Tạo OU

## 2   Bảo mật ADDS và tài khoản người dùng

☐ Chuẩn bị:
   ☐ Một máy server 2016 đã lên DC
   ☐ Một máy Client windows 7
☐ Mô hình


☐ Kết quả đạt được
   ☐ Đăng nhập tài khoản user trên Domain (trừ administrator)
   ☐ Điều chỉnh chính sách lưu lại password còn 2 ngày
   ☐ Điều chỉnh chính sách tuổi thọ tối đa password còn 10 ngày
   ☐ Điều chỉnh chính sách tuổi thọ nhỏ nhất password còn 1 ngày
☐ Thực hiện

☐ Trong GPO mặc định này có 2 chính sách là Default Domain Controller Policy (Chính sách này áp dụng cho DC), Default Domain Policy (Áp dụng cho toàn hệ thống)
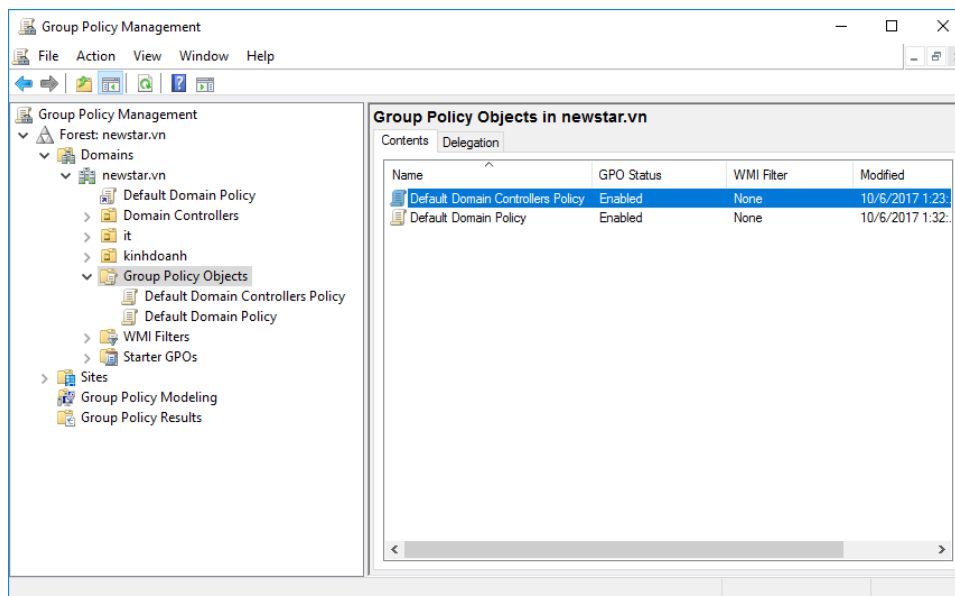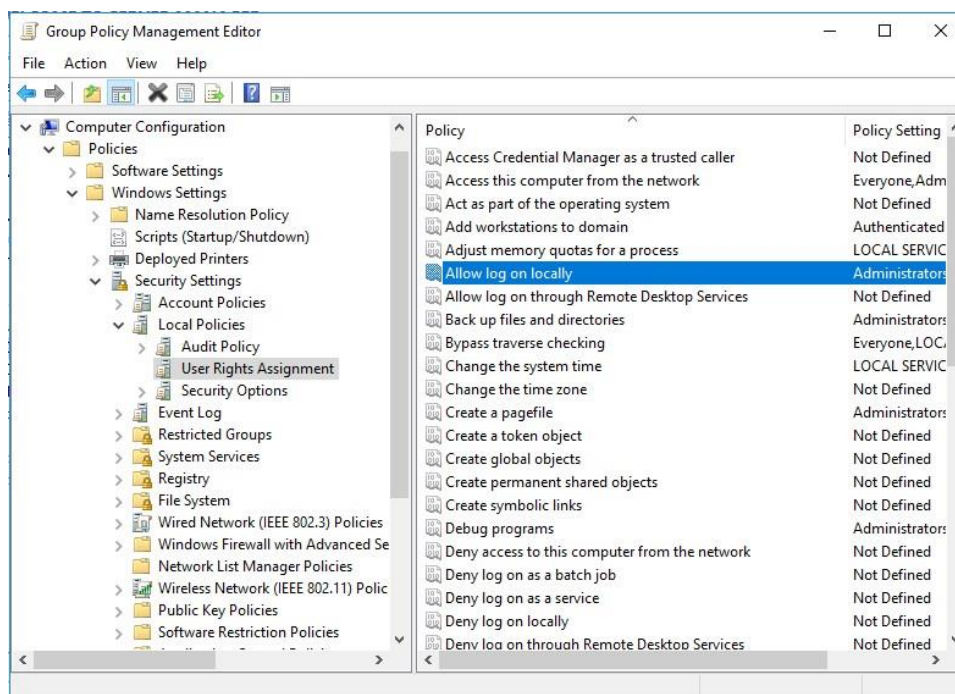

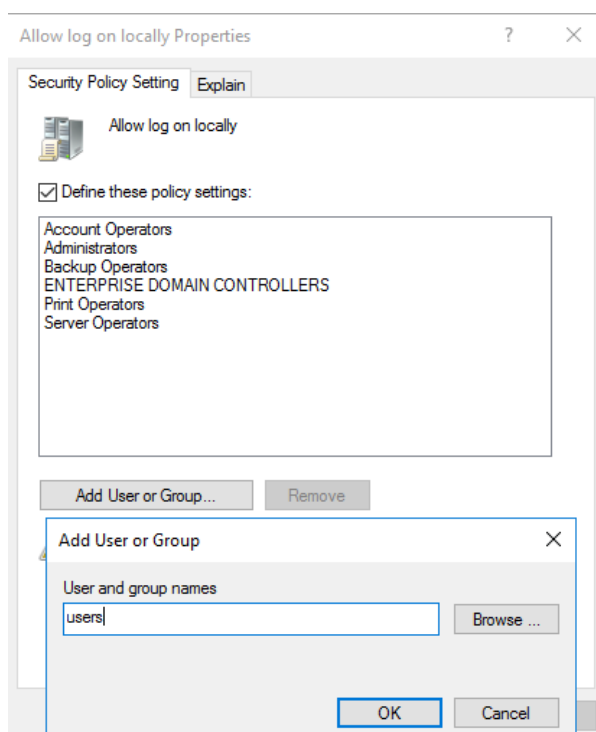*Hình 14-1: Các GPO mặc định*

☐ Mặc định trên DC không cho User (chỉ cho Administrator). Ta tiến hành điều chỉnh cho DC sao cho User vẫn đăng nhập bình thường
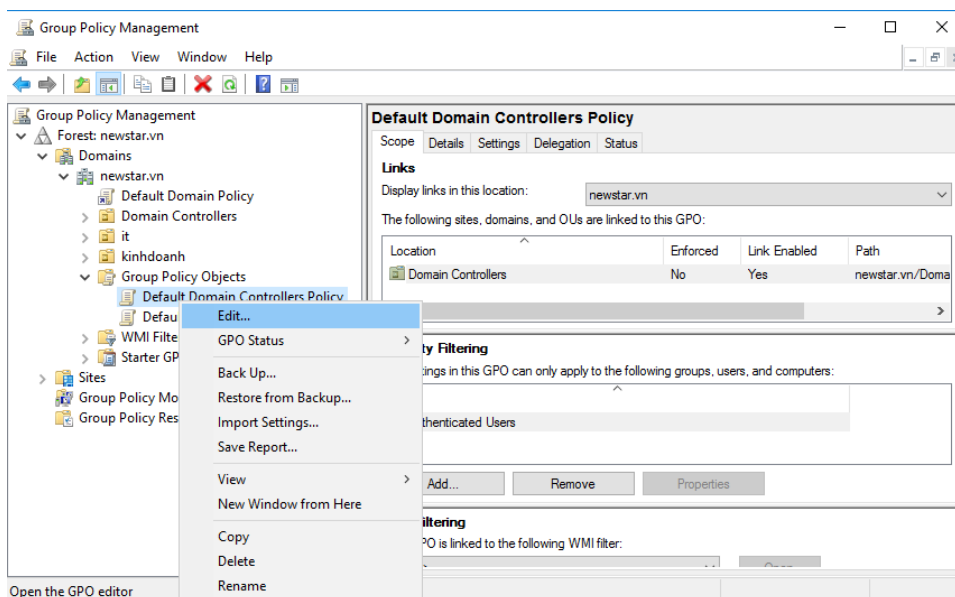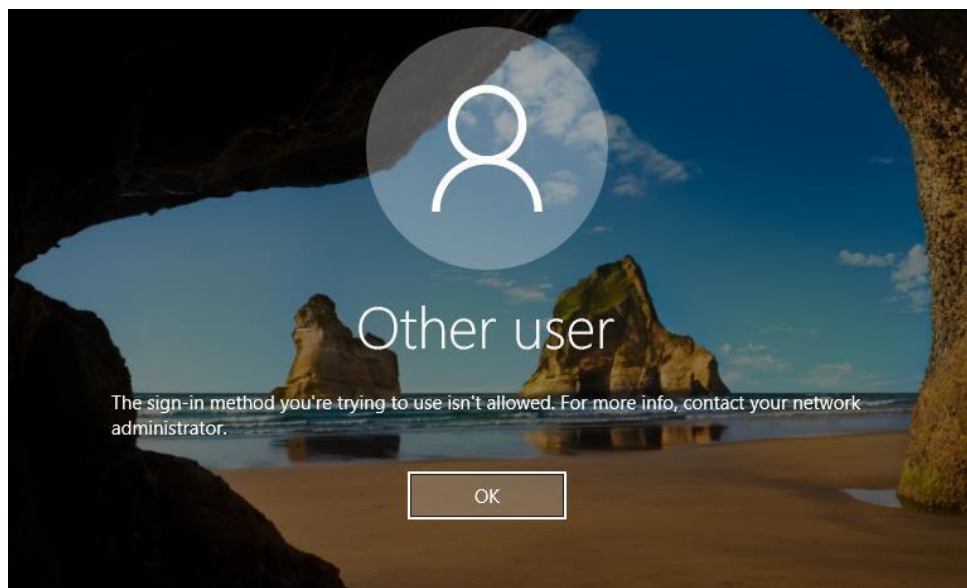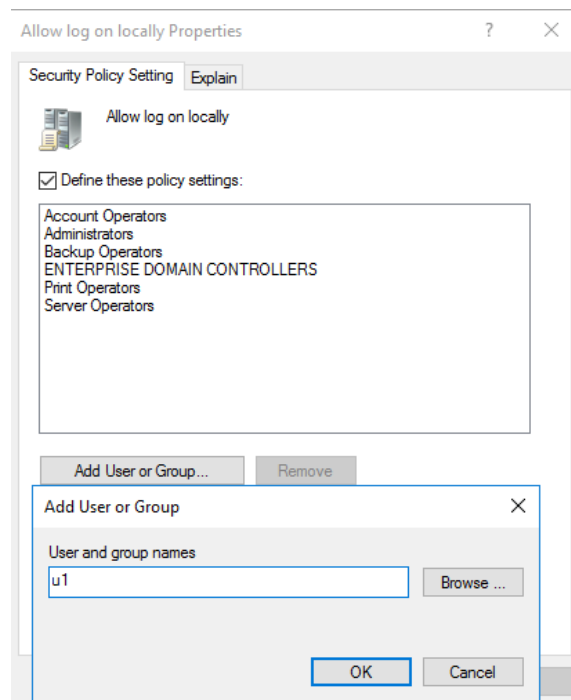

Hình 14-2: Chỉnh sửa GPO
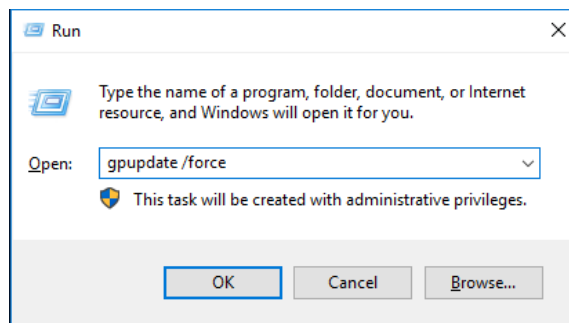
Hình 14-3: Chỉnh sửa đăng nhập local
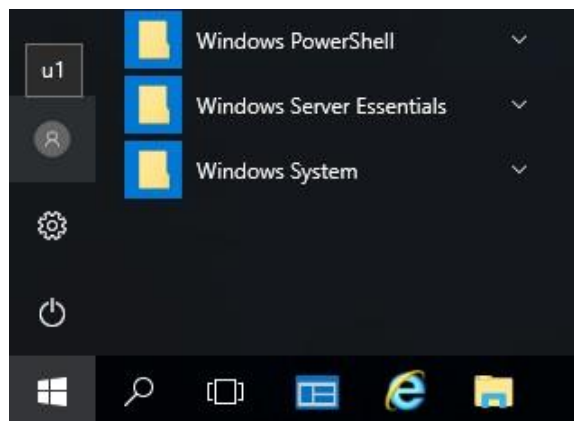

Hình 14-4: Add group Users

Hình 14-5: Tài khoản không đăng nhập được trên DC
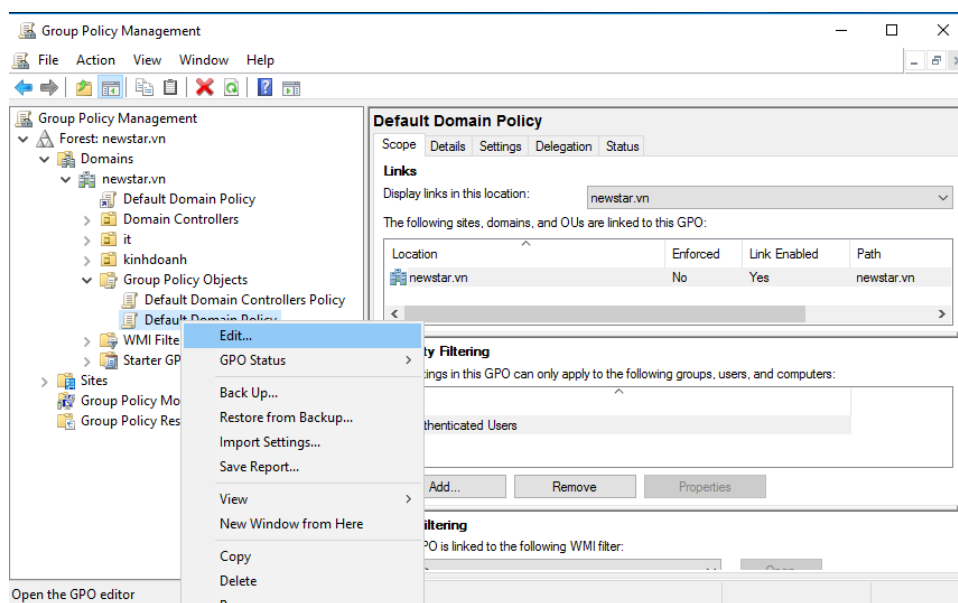

Hình 14-6: Add user u1
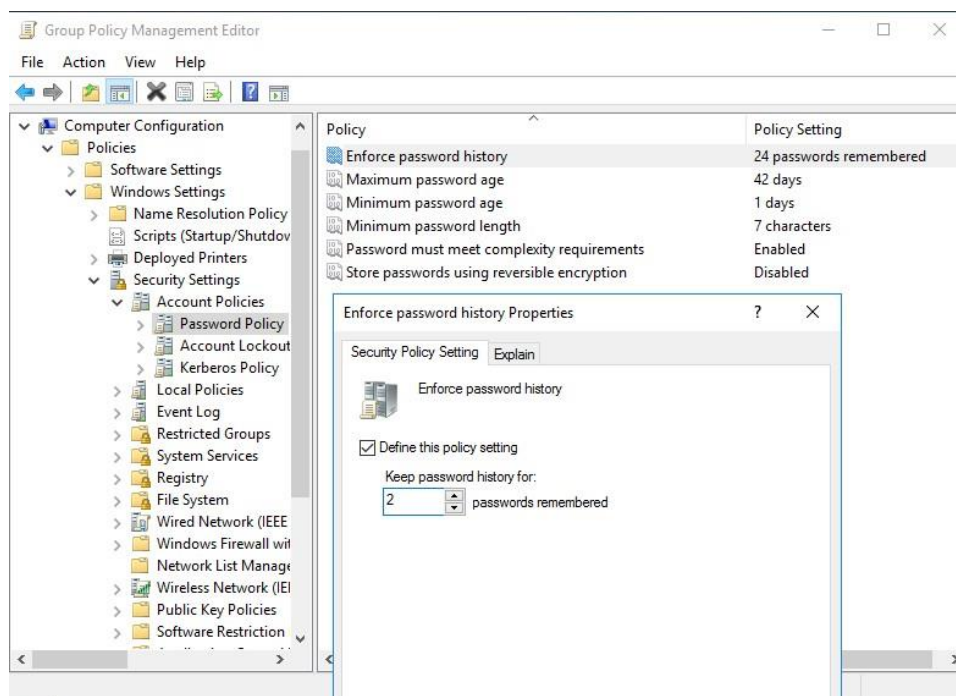
Hình 14-7: Cập nhật chính sách
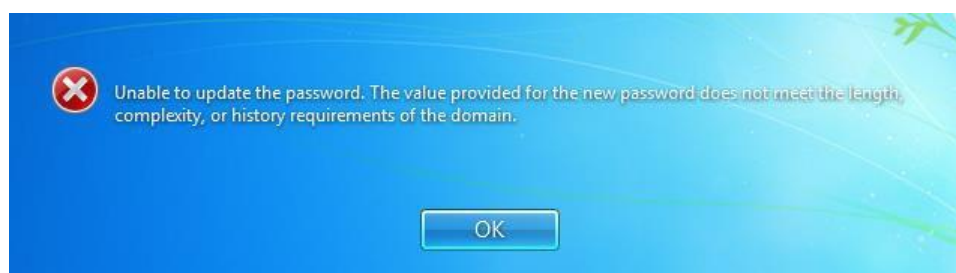

Hình 14-8: U1 đăng nhập trên DC

☐ Hiệu chỉnh chính sách Password sẽ áp dụng cho tất cả các tài khoản trong hệ thống
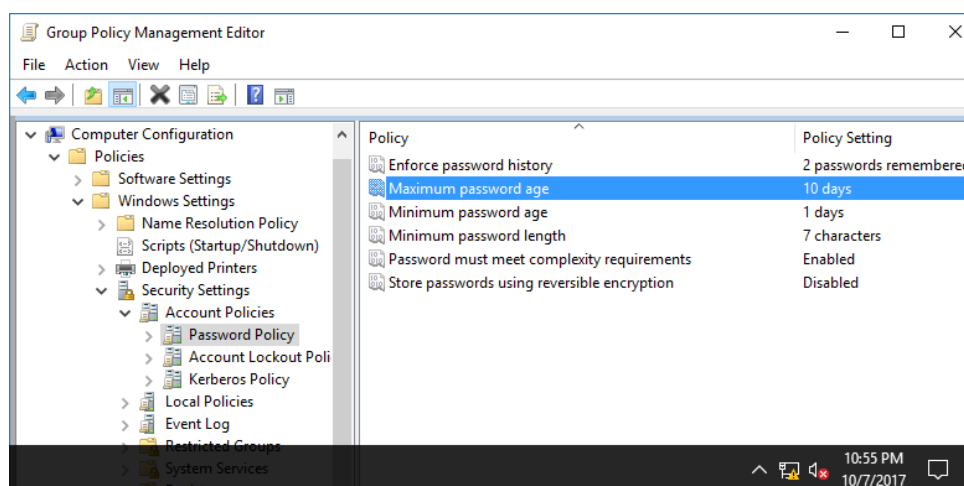

Hình 14-9: Chỉnh sửa trên Default Domain Policy

Hình 14-10: Chỉnh lại số lượng Password nhớ là 2 ngày
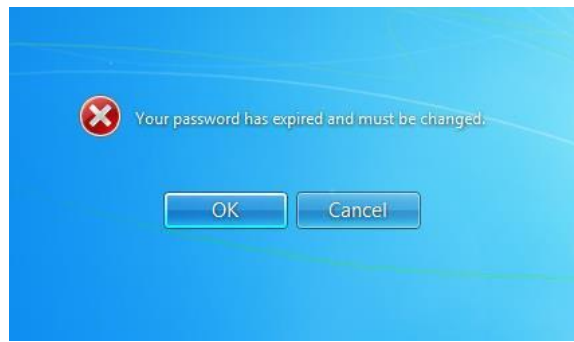

Hình 14-11: Đổi lại Password cũ không thành công
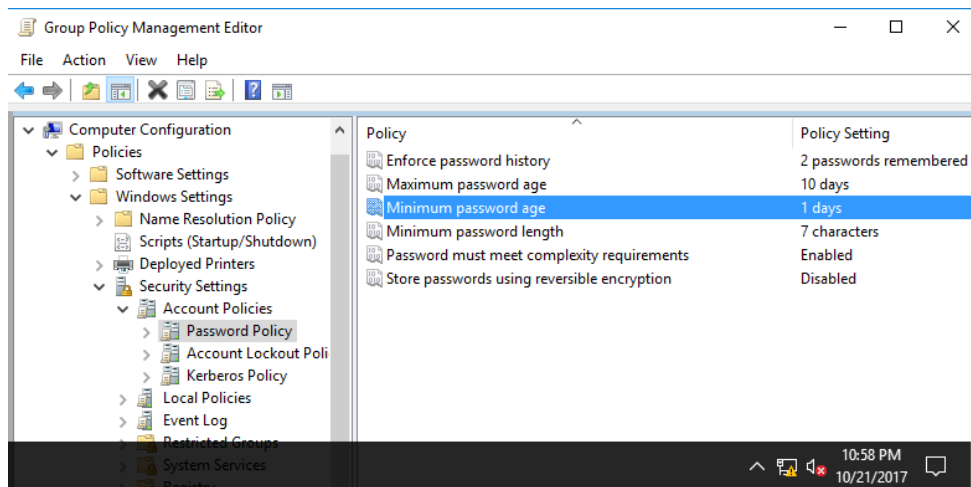

Hình 14-12: Yêu cầu thời gian tối đa đổi password là 10 ngày
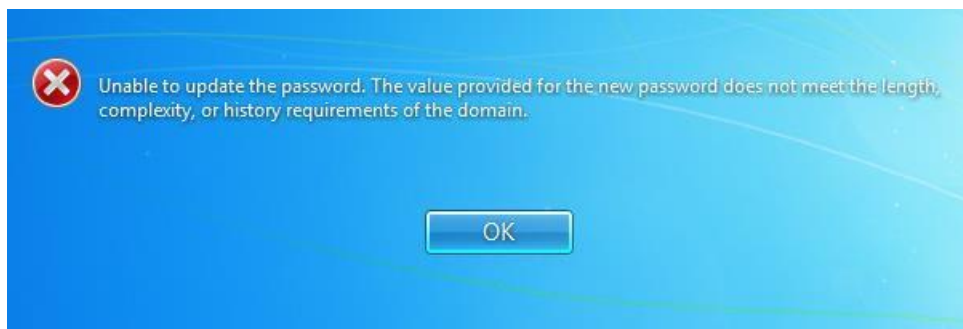
Hình 14-13: Yêu cầu đổi Password

Hình 14-14: Thời gian tối thiểu là 1 ngày
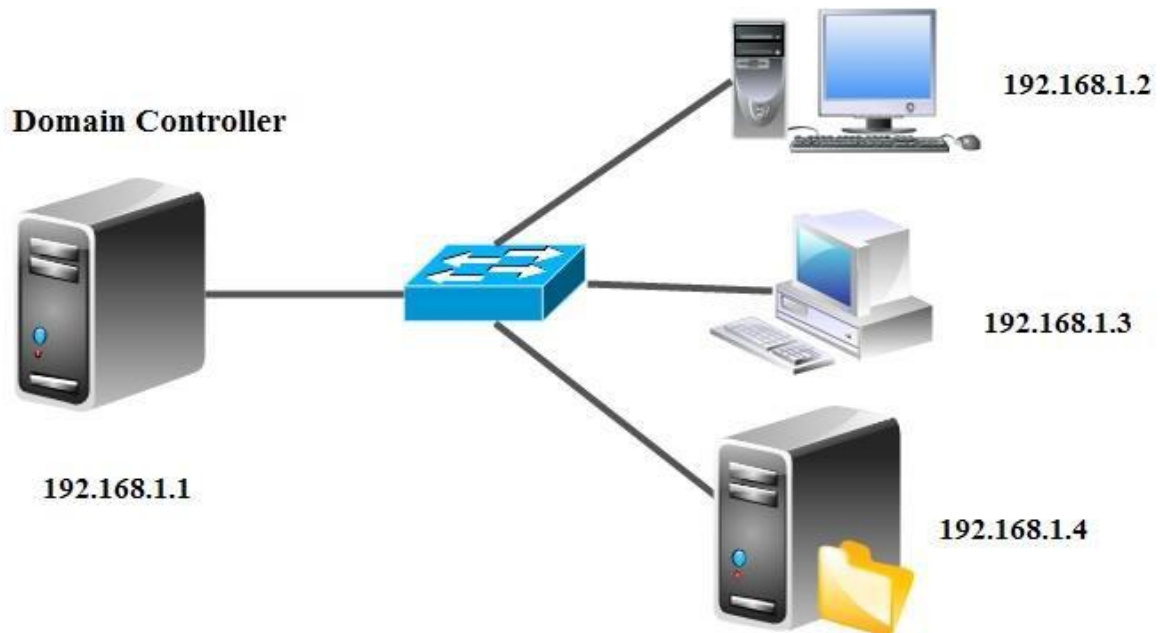

*Hình 14-15: Không được đổi Password*

☐ Điều chỉnh các chính sách còn lại

3 Quản trị chia sẻ và phân quyền

Sau khi học bài này học viên có khả năng chia sẻ và phân quyền các folder cho các user trong hệ thống với những chức năng mở rộng của NTFS

- Chuẩn bị:
  - Một máy server 2016 đã lên DC
  - Một máy Client windows 7
- Mô hình

Domain Controller

192.168.1.1

192.168.1.2

192.168.1.3

192.168.1.4

- Kết quả đạt được
  - Tài khoản NS1 không xóa folder mà NS2 tạo
  - Lấy quyền lại cho admin khi bị NS2 xóa bỏ
- Thực hiện
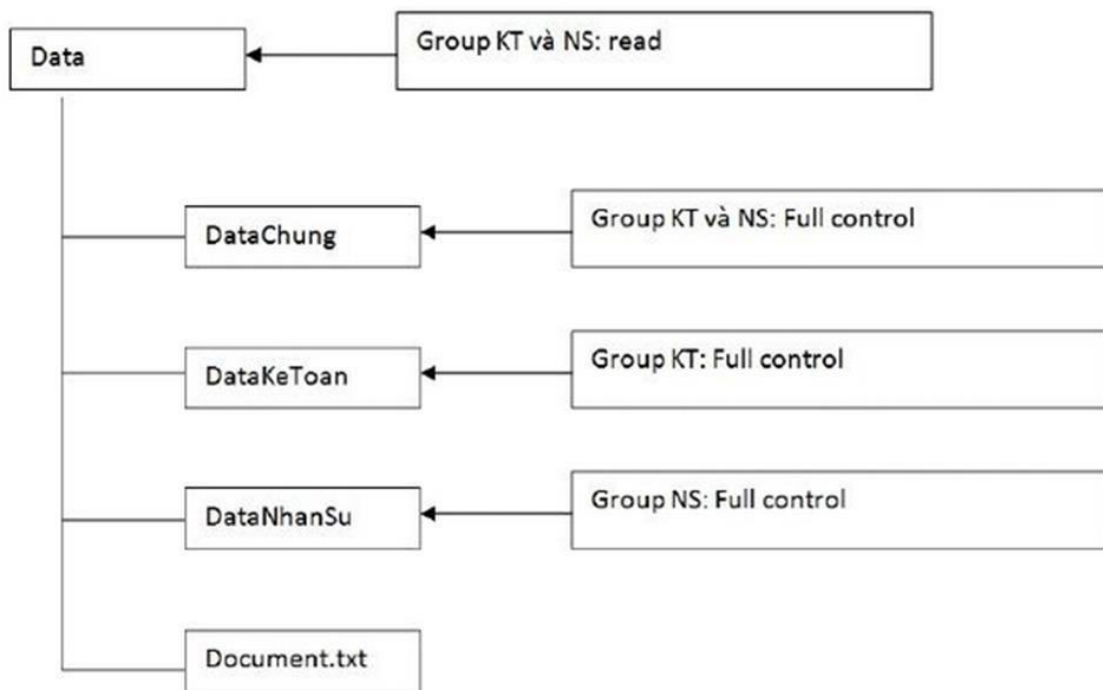
Tạo 2 tài khoản NS1 và NS2 thuộc group NS và 2 tài khoản KT1, KT2 thuộc group KT

a) Thực hiện việc gán quyền như hình trên

b) Trong Folder DataKeToan, không cho tài khoản KT1 truy xuất

c) Tạo 2 Folder con trong DataNhanSu bằng tài khoản NS1, đăng nhập bằng NS2

d) Xóa 1 Folder mà NS1 vừa tạo, sau đó tạo 2 folder cùng cấp với folder vừa xóa

e) Thiết lập nguyên tắc "Không xóa dữ liệu của người khác"

f) Dùng Ns2 để loại bỏ hoàn toàn các tài khoản khác trên folder vừa tạo (bao gồm Administrators, System vv...)

g) Dùng Administrator để lấy lại quyền owner trên folder mà Ns2 đã thiết lập.

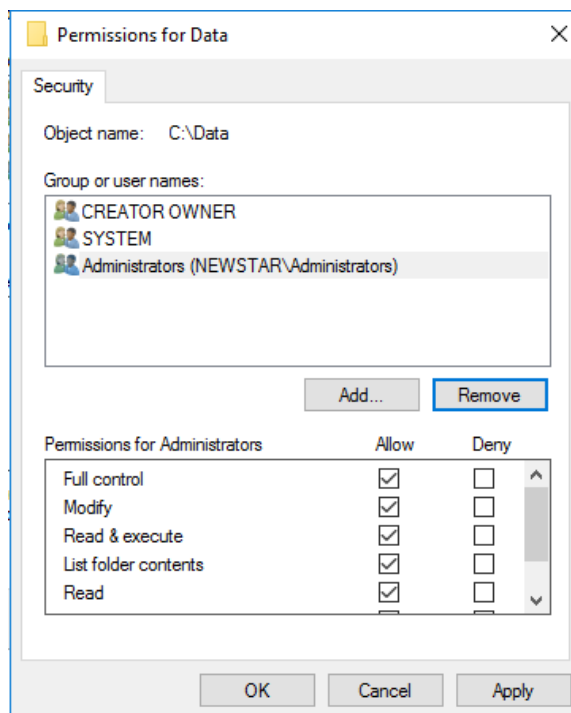☐ Thực hiện chia sẻ tất cả mọi người với quyền Full Control
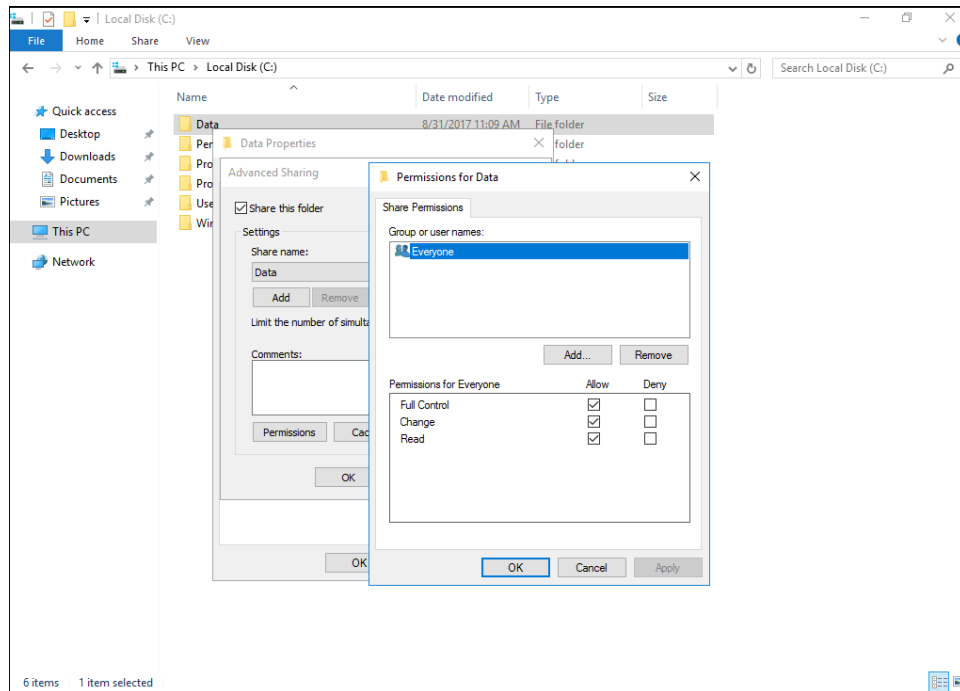
Hình 15-1: Share folder Data Everyone quyền FC

☐ Gõ bỏ kế thừa: Security ☐advanced ☐Change pemission ☐Disible inherited ☐convert inherited
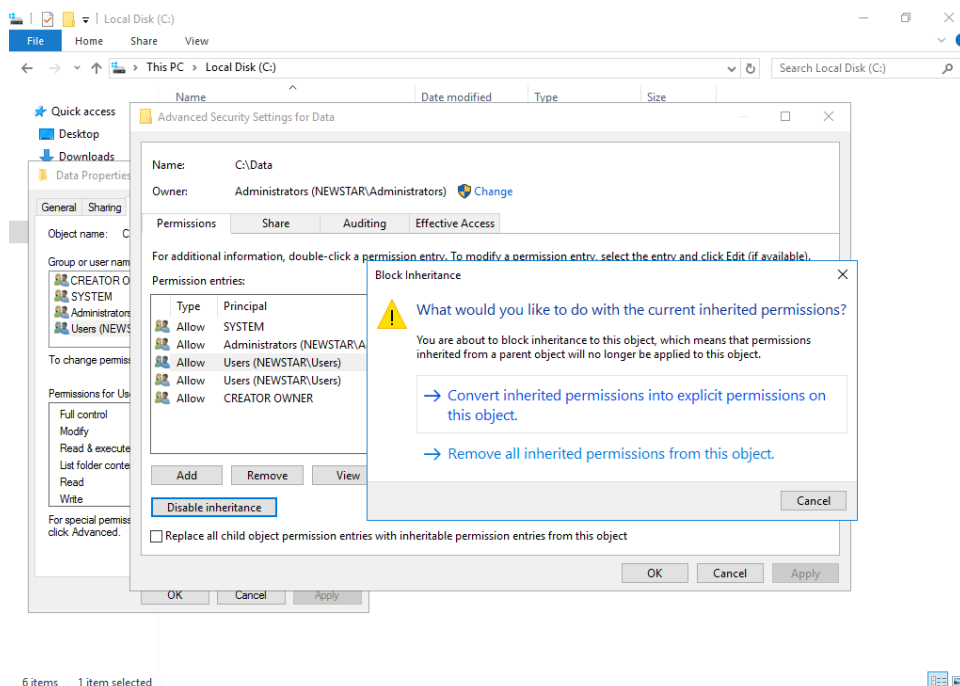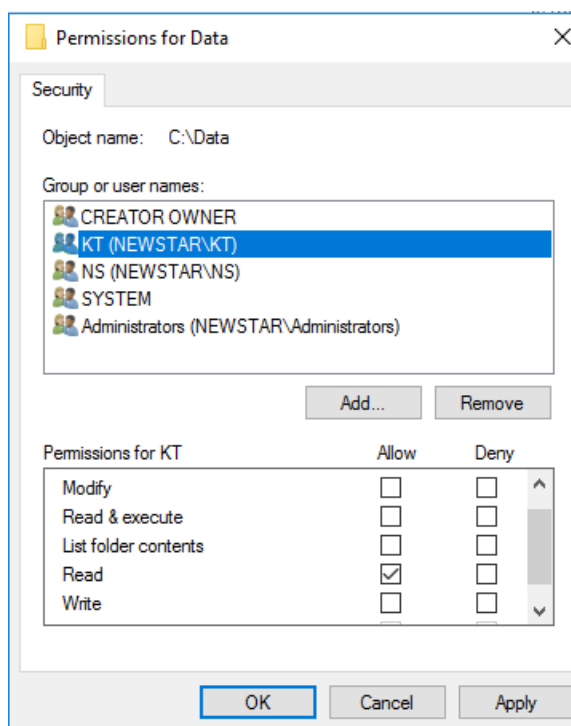

Hình 15-2: Xóa bỏ kế thừa

Tiến hành xóa group users, thêm nhóm KT và NS
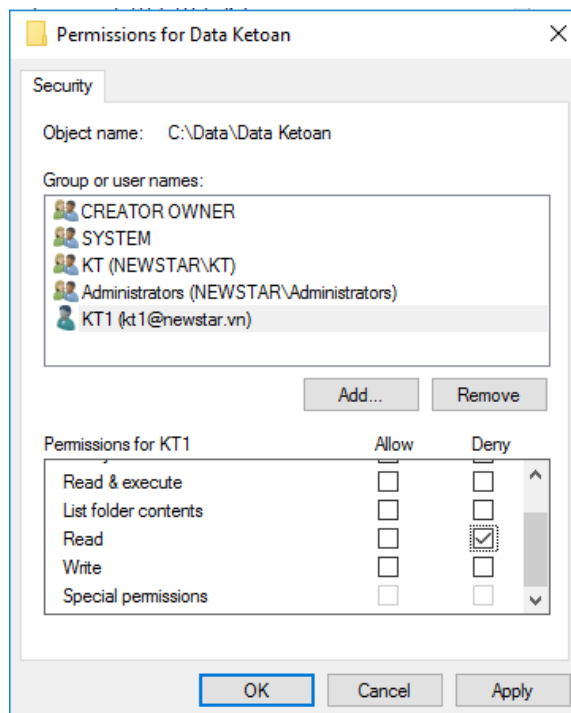

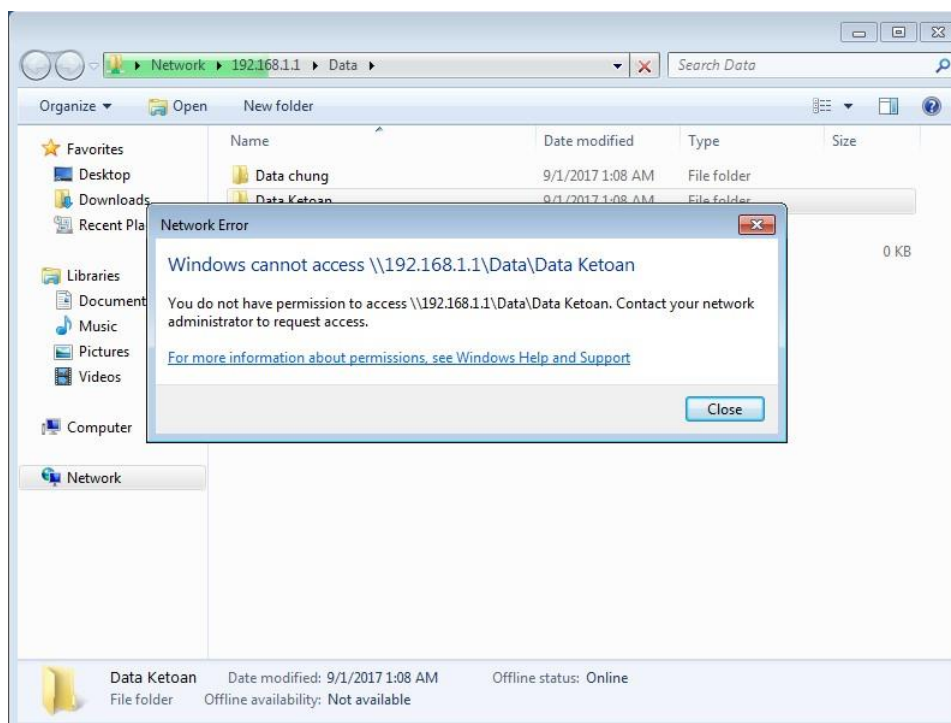*Hình 15-3: Xóa bỏ group Users*

Hình 15-4: Phân quyền cho Group KT và NS

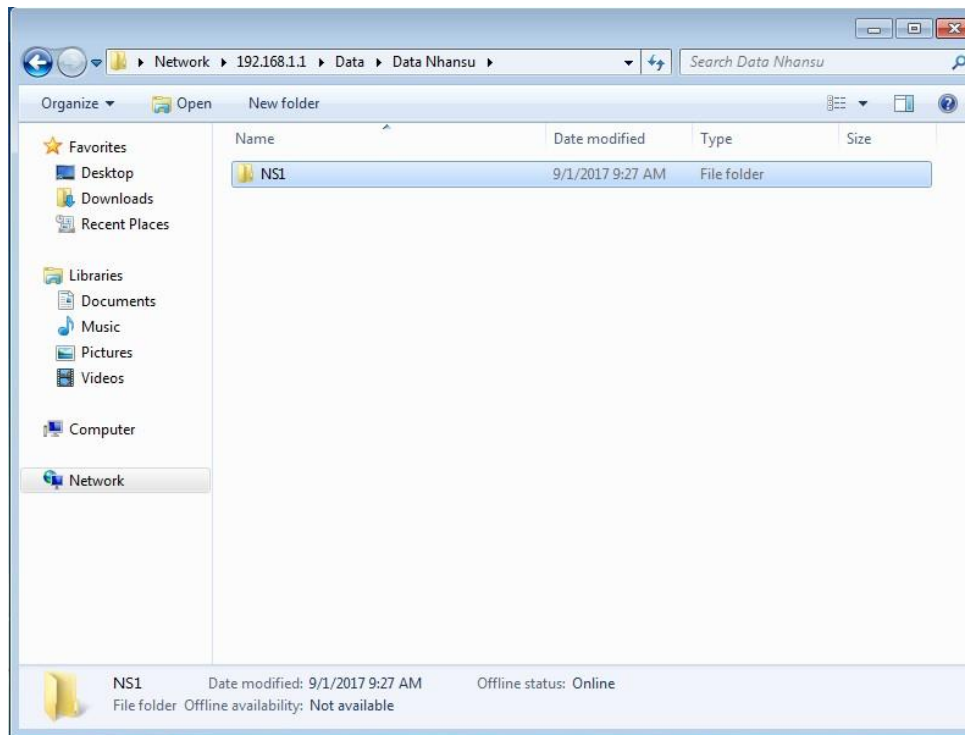☐ Thực hiện gán quyền cho KT1 bị cấm truy xuất
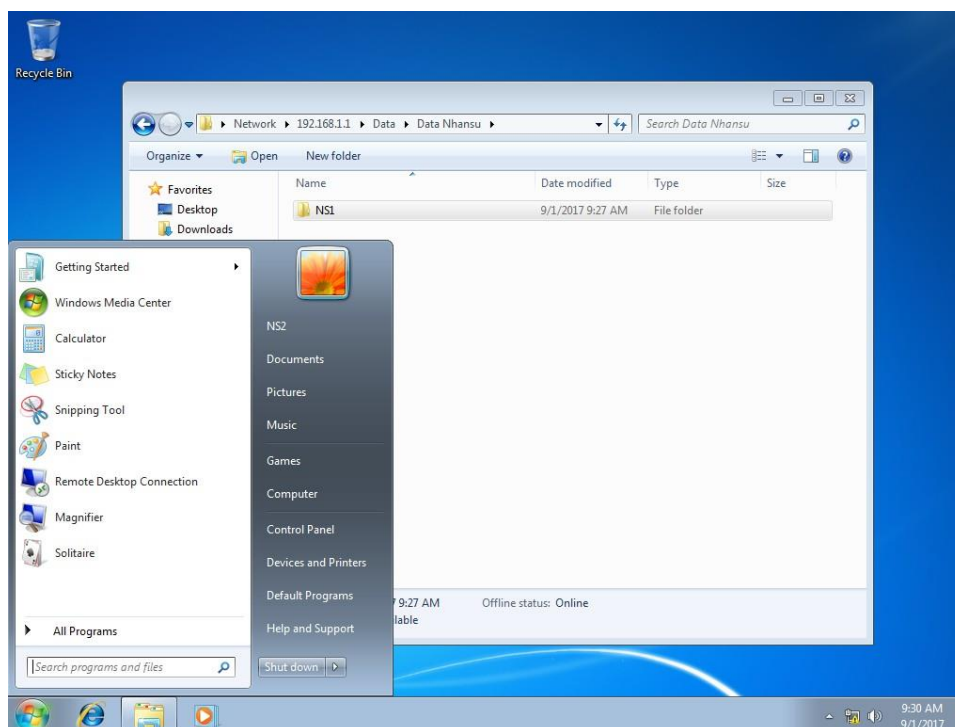

Hình 15-5: Chặn KT1 truy xuất

Hình 15-6: KT1 không được truy cập

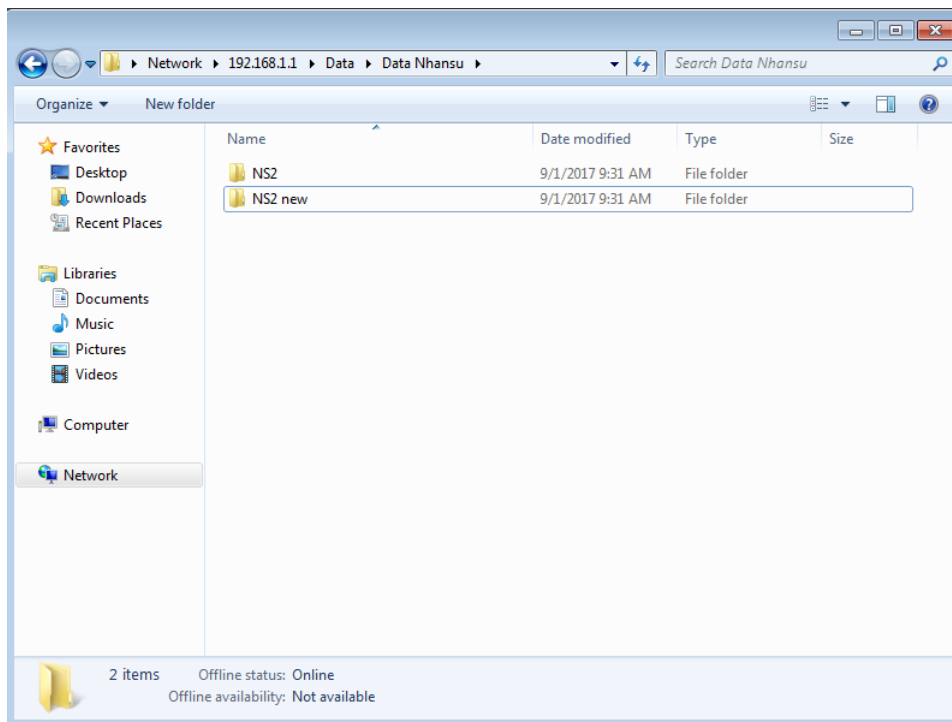☐ Dùng tài khoản NS1 tạo folder NS1, đăng nhập bằng NS2 truy cập vào có thấy folder của NS1 tạo hay không?
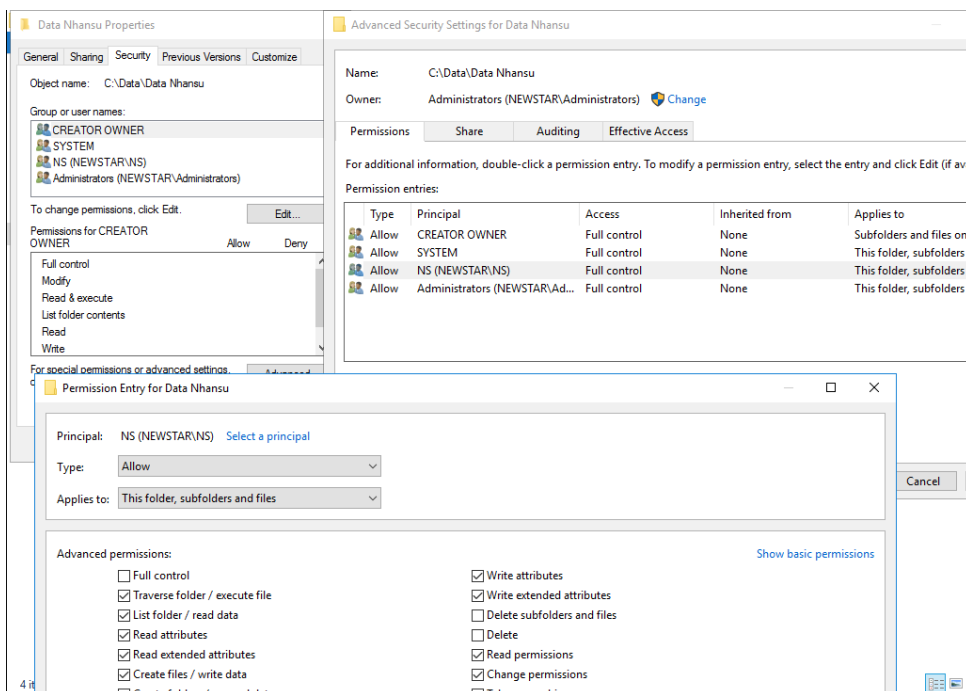

Hình 15-7: NS1 tạo Folder

Hình 15-8: NS2 đăng nhập

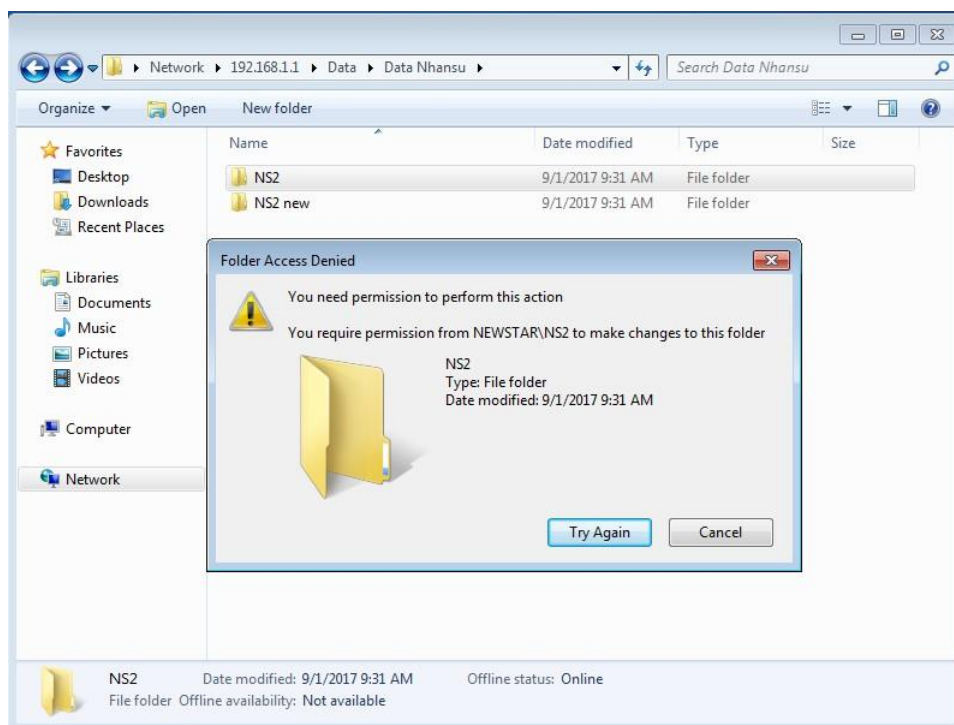☐ NS2 đã xóa được folder NS1 tạo, đồng thời tạo 2 folder khác đồng cấp

Hình 15-9: NS2 tạo folder

☐ Thiết lập nguyên tắc không xóa dữ liệu của người khác. Người nào tạo thì người đó được quyền xóa
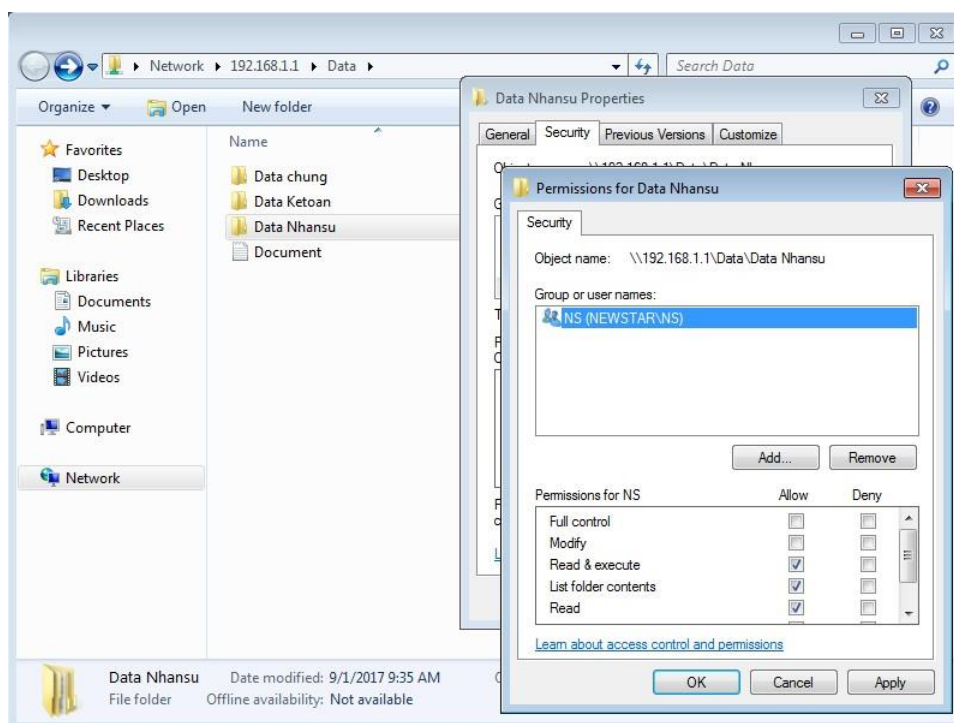

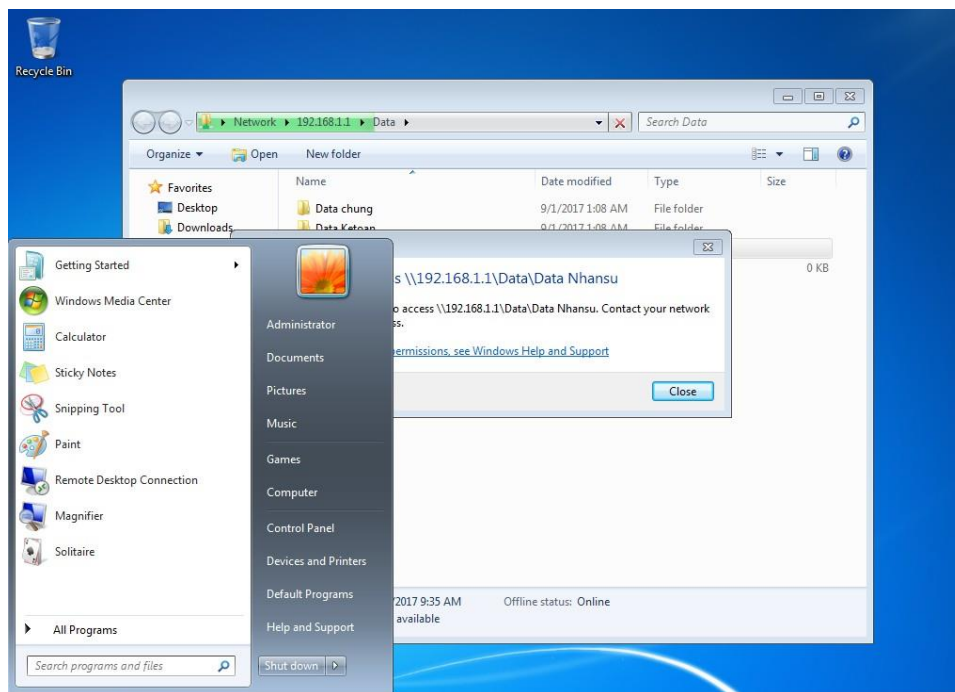*Hình 15-10: Bỏ 2 dấu check Delete subfolder and file và Delete*

Hình 15-11: NS1 không được xóa dữ liệu NS2

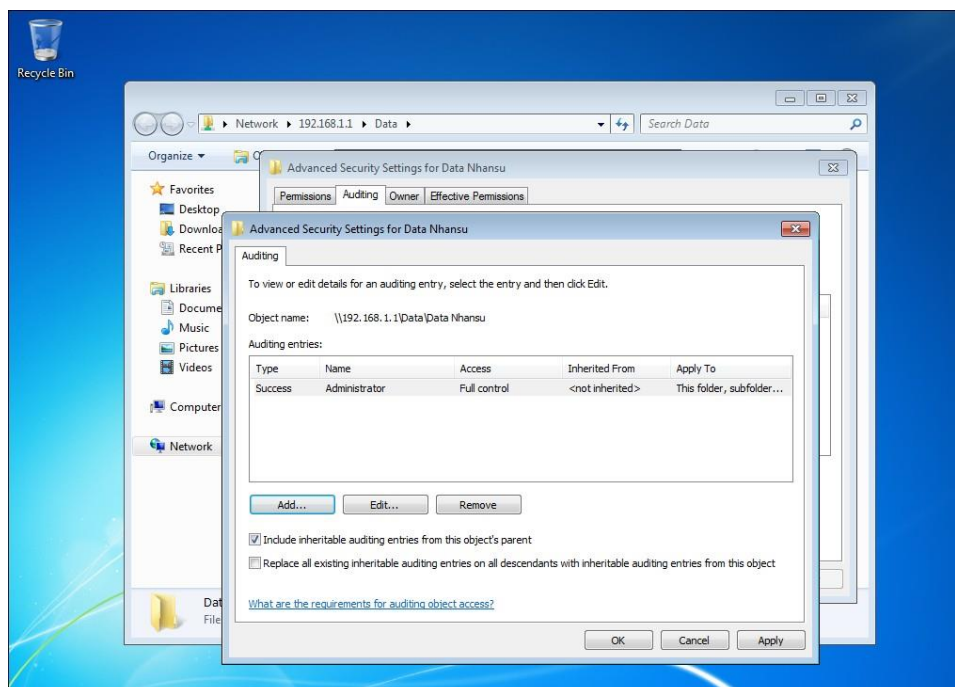☐ Dùng NS2 loại bỏ hoàn toàn tất cả nhưng tài khoản khác

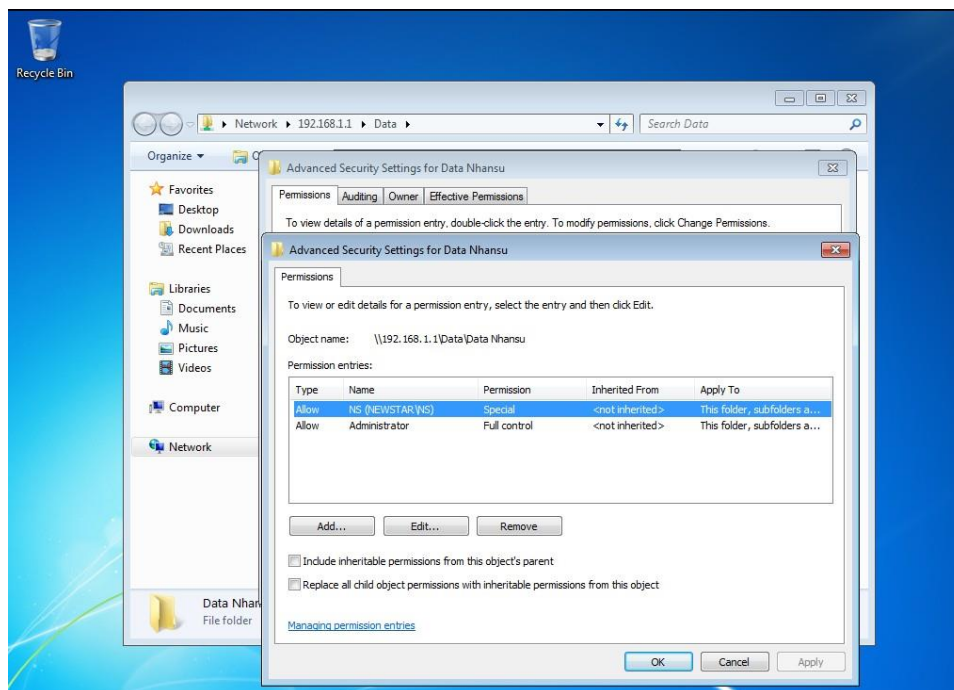*Hình 15-12: NS2 xóa hết tài khoản khác*
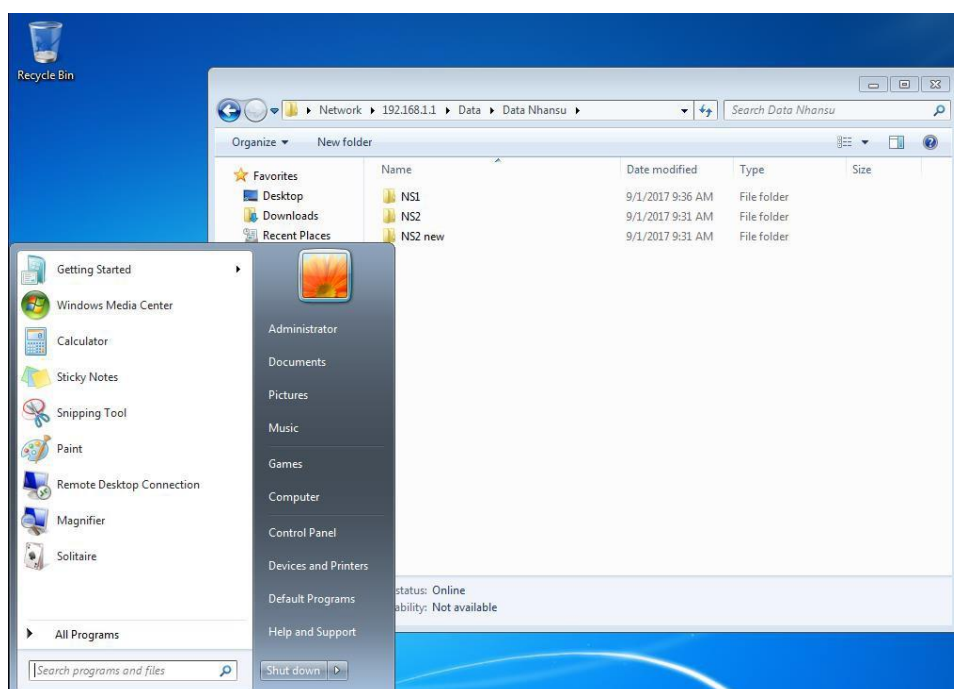
Hình 15-13: Admin không thể truy cập vào Datanhansu

 Admin lấy lại quyền

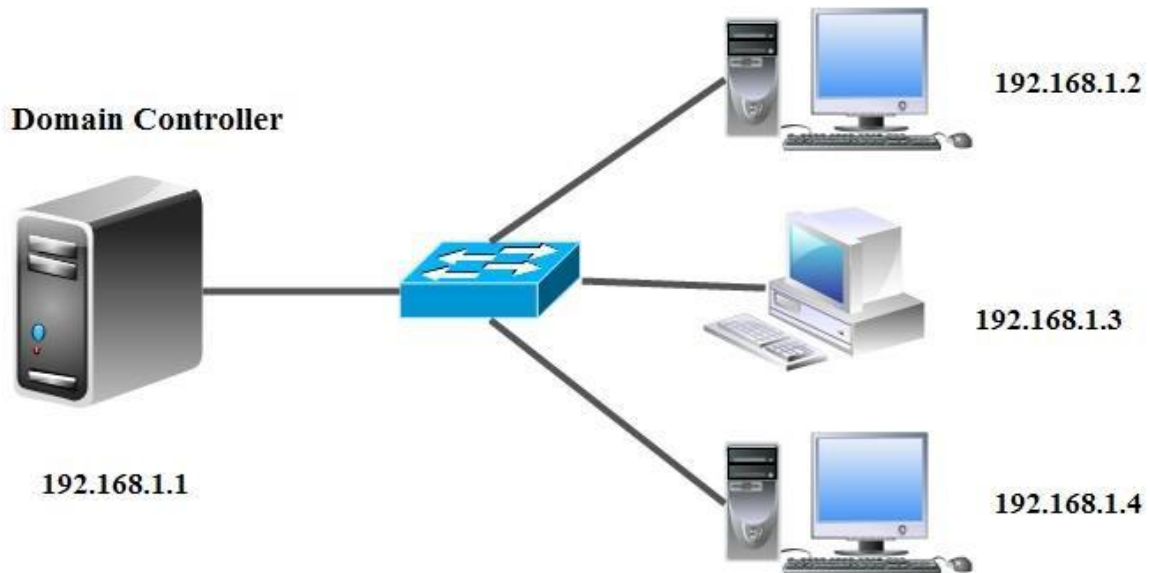*Hình 15-14: Admin lấy quyền lại*

Hình 15-15: Đã lấy lại quyền

Hình 15-16: Admin đã đăng nhập và truy cập vào folder

4 Triển khai và quản lý GPO

Sau khi học bài này sinh viên có khả năng tạo ra các chính sách cho các đối tượng

- Chuẩn bị:
 - Một máy server 2016 đã lên DC
  - Một máy Client windows 7
- Mô hình

Domain Controller

192.168.1.2

192.168.1.3

192.168.1.1

192.168.1.4

- Kết quả đạt được
  - Ẩn icon trên màn hình Desktop
  - Ẩn item trong control panel
  - Cấm đổi theme
  - Không cho sửa địa chỉ IP
  - Khóa start menu and taskbar
  - Không cho sử dụng ứng dụng
  - Hiển thị câu chào khi đăng nhập
- Thực hiện
❖ Ẩn icon trên màn hình Desktop
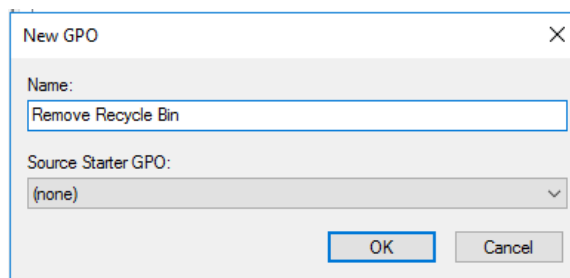
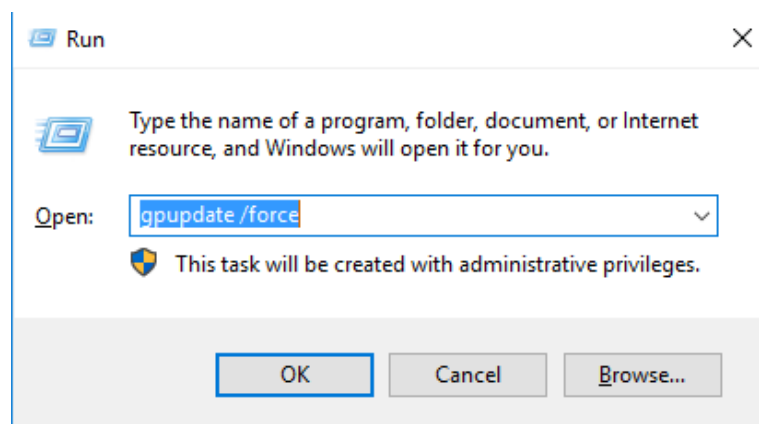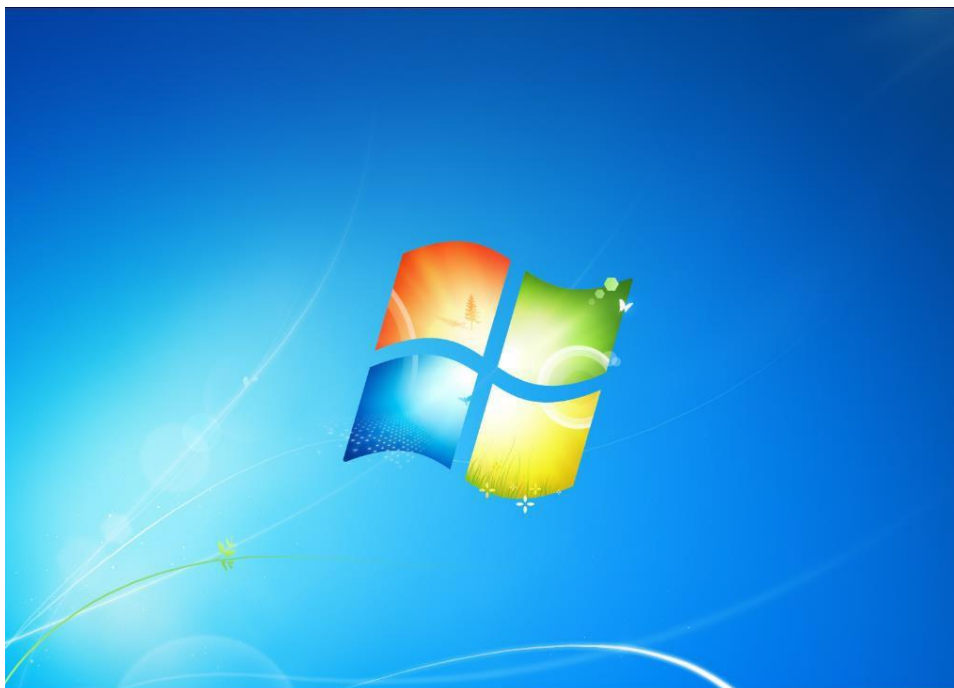*Hình 16-1: Thêm GPO*
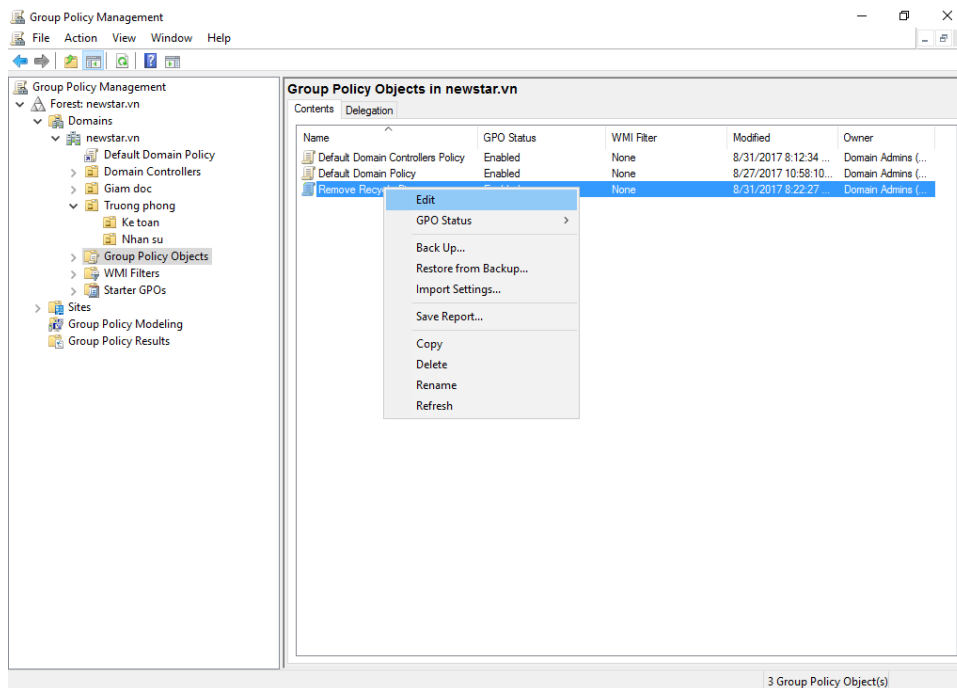
Hình 16-2: Chỉnh sửa GPO
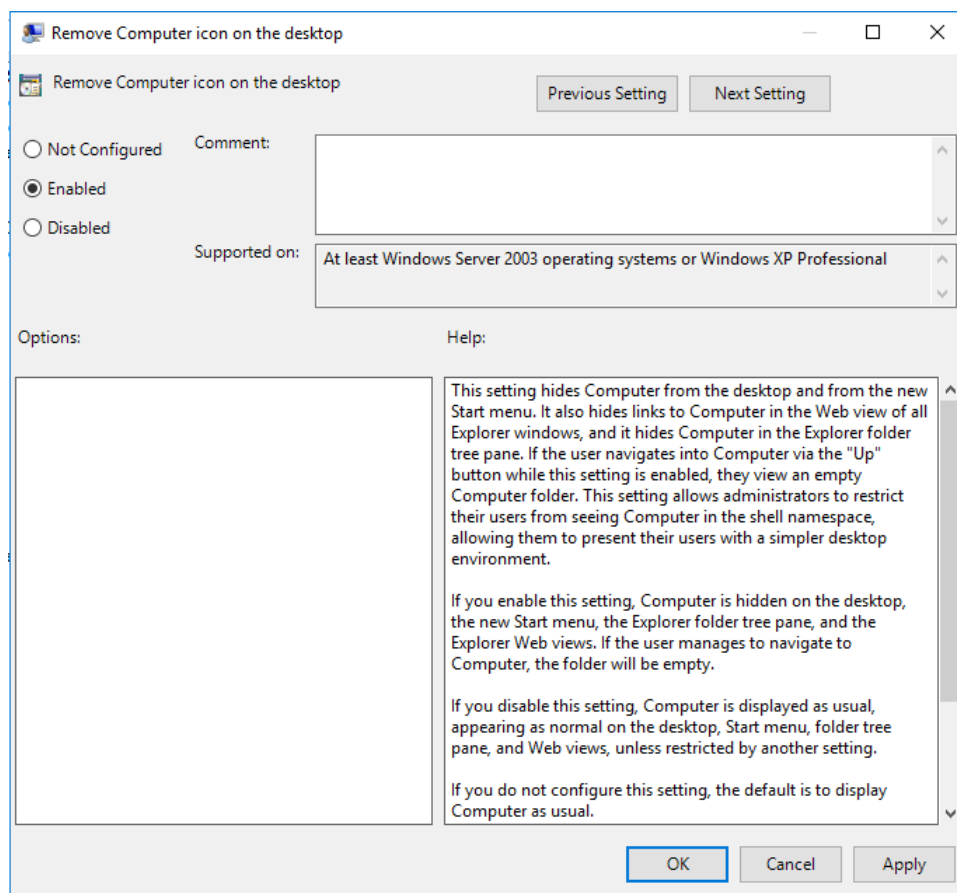
*Hình 16-3: Enable tính năng trên GPO*

Hình 16-4:Cập nhật GPO

Hình 16-5: Icon đã mất trên máy Client

Thao tác trên GPO với các yêu cầu trên Desktop hình bên dưới

|		
📁 Active Directory		
📁 Desktop		
📄 Prohibit User from manually redirecting Profile Folders	Not configured	No
📄 Hide and disable all items on the desktop	Not configured	No
📄 Remove the Desktop Cleanup Wizard	Not configured	No
📄 Hide Internet Explorer icon on desktop	Not configured	No
📄 Remove Computer icon on the desktop	Enabled	No
📄 Remove My Documents icon on the desktop	Not configured	No
📄 Hide Network Locations icon on desktop	Not configured	No
📄 Remove Properties from the Computer icon context menu	Not configured	No
📄 Remove Properties from the Documents icon context menu	Not configured	No
📄 Do not add shares of recently opened documents to Networ...	Not configured	No
📄 Remove Recycle Bin icon from desktop	Enabled	No
📄 Remove Properties from the Recycle Bin context menu	Not configured	No
📄 Don't save settings at exit	Not configured	No
📄 Turn off Aero Shake window minimizing mouse gesture	Not configured	No
📄 Prevent adding, dragging, dropping and closing the Taskbar...	Not configured	No
📄 Prohibit adjusting desktop toolbars	Not configured	No

Hình 16-6: Hãy Enable những tính năng còn lại
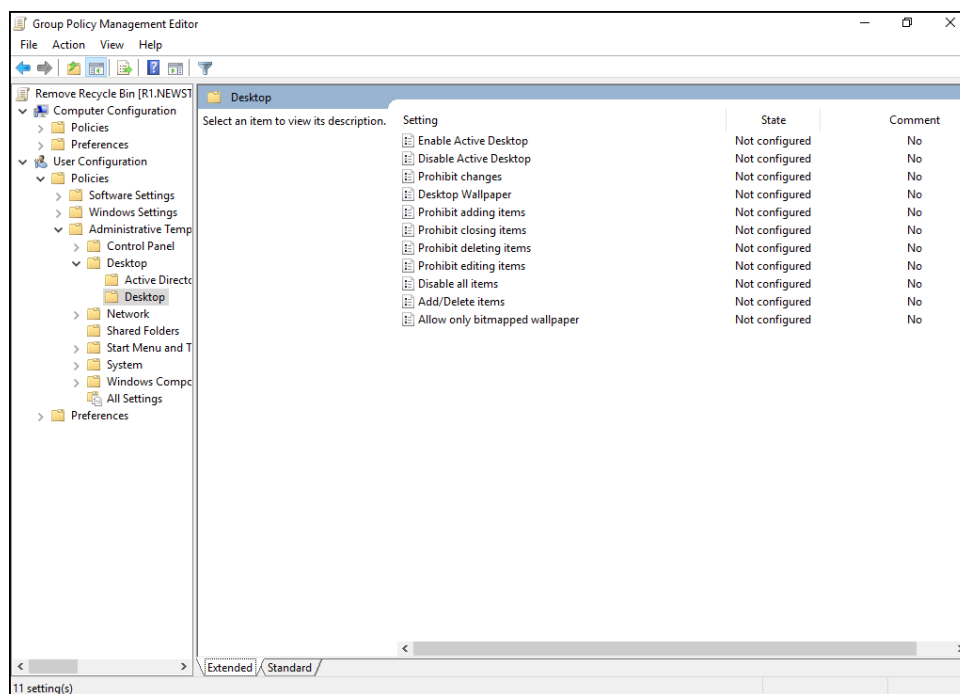
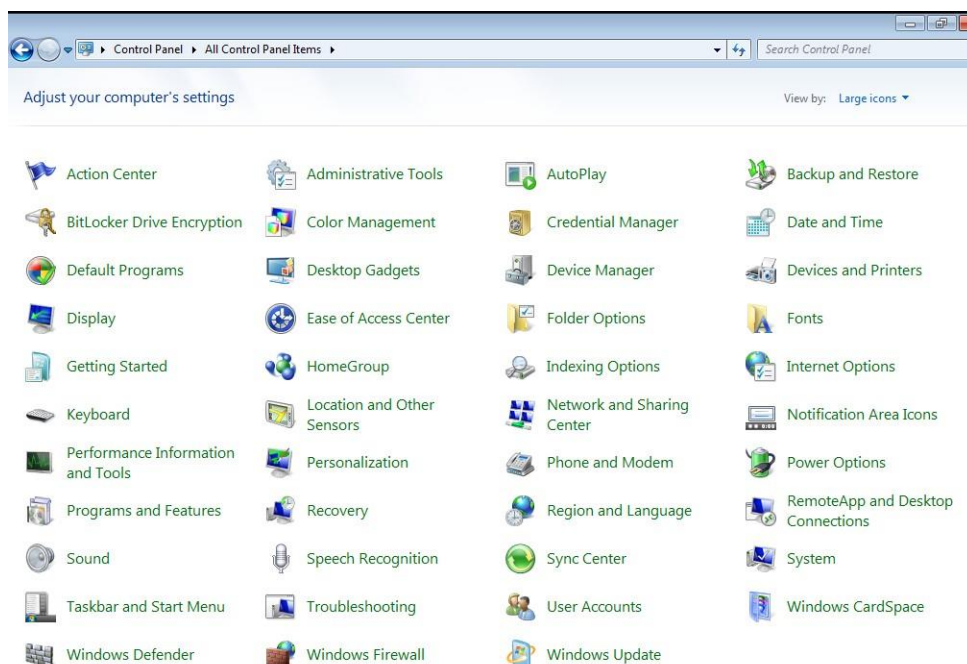*Hình 16-7: Enable các tính năng còn lại*

Hình 16-8: Enable các tính năng còn lại

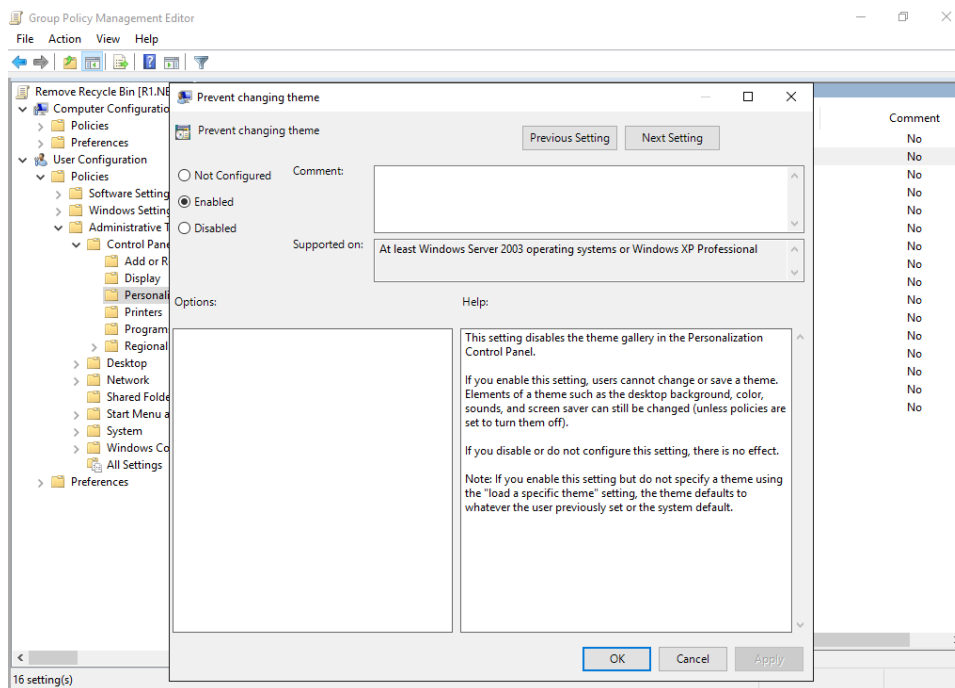❖ **Ẩn một vài item trong Control panel**
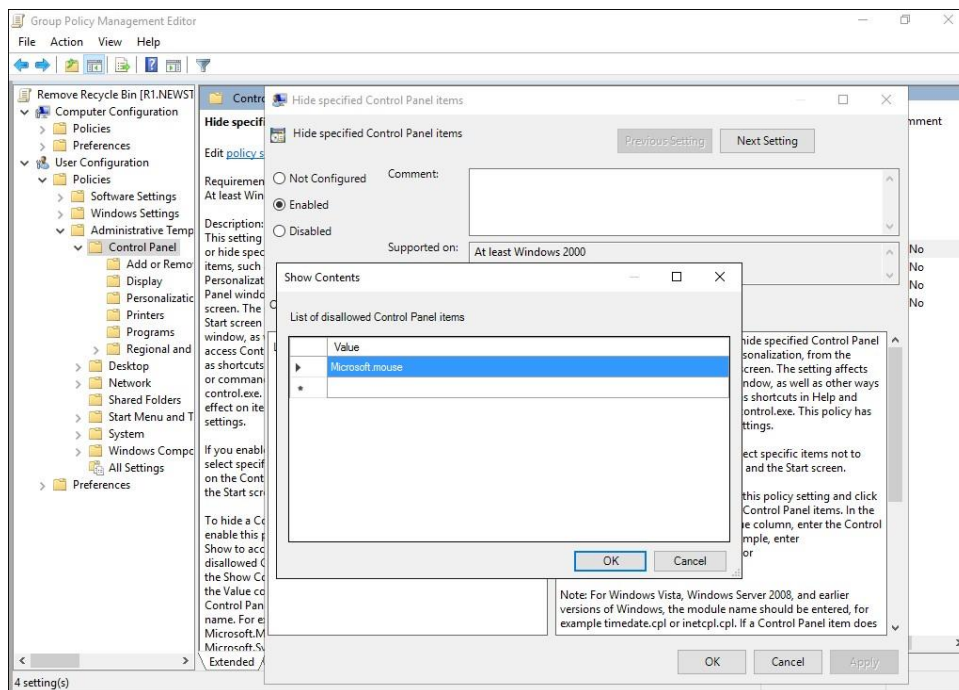
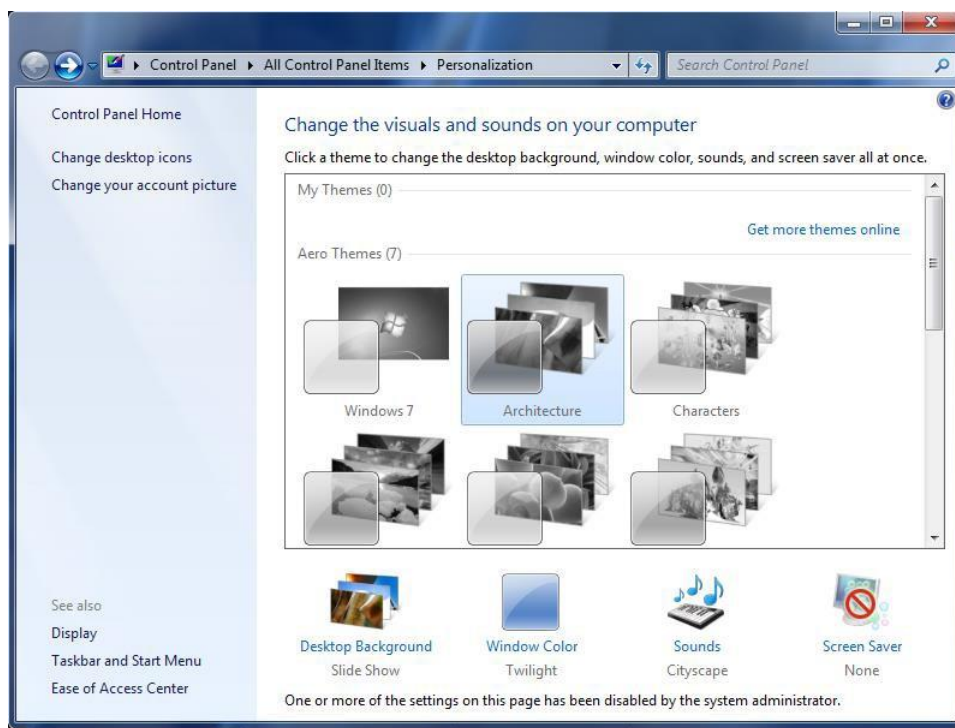*Hình 16-9: Ẩn Mouse trong Control Panel*

Hình 16-10: Mouse đã mất
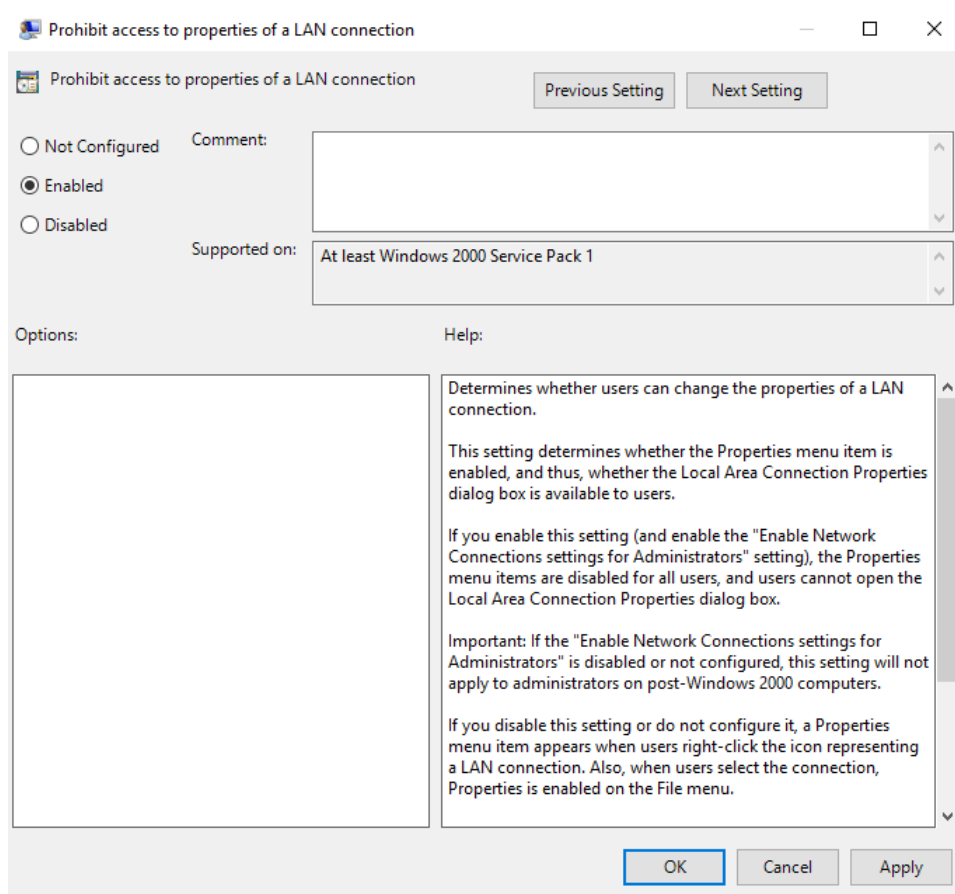
❖ **Thay đổi theme**

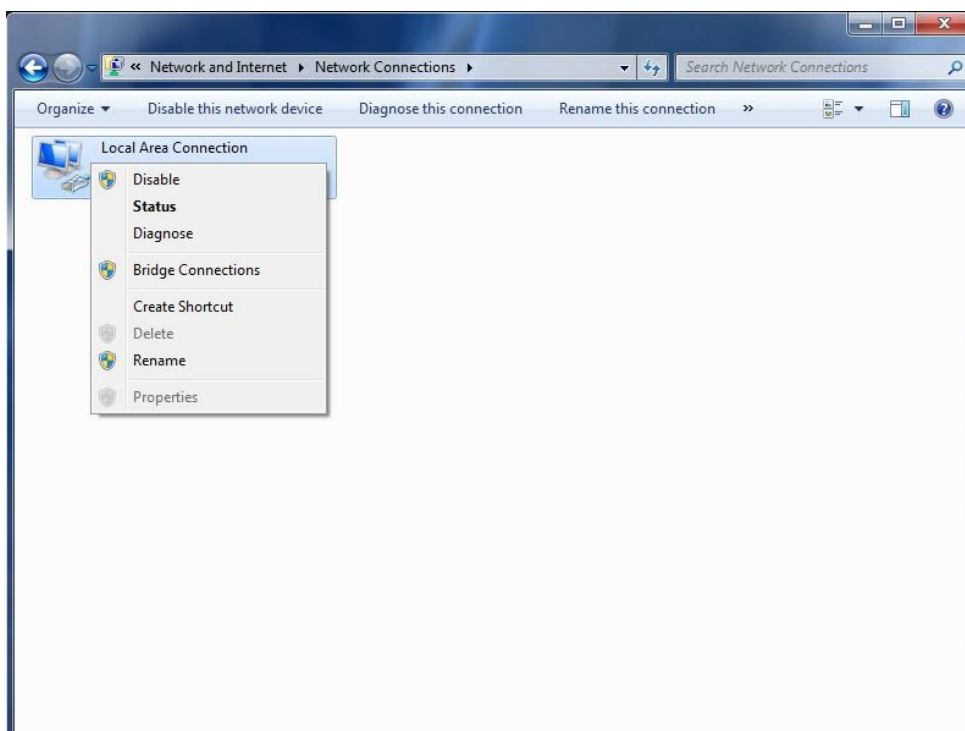*Hình 16-11: Enable tính năng chặn đổi theme*
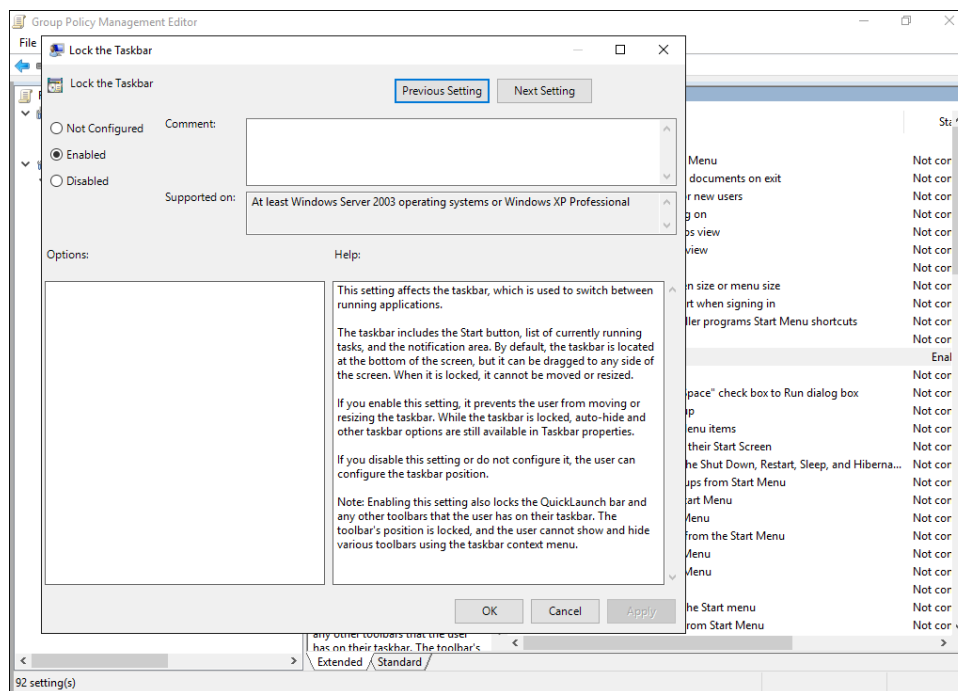

Hình 16-12: Uer không được đổi Theme

❖ **Chặn sửa IP**

Hình 16-13: Enable tính năng

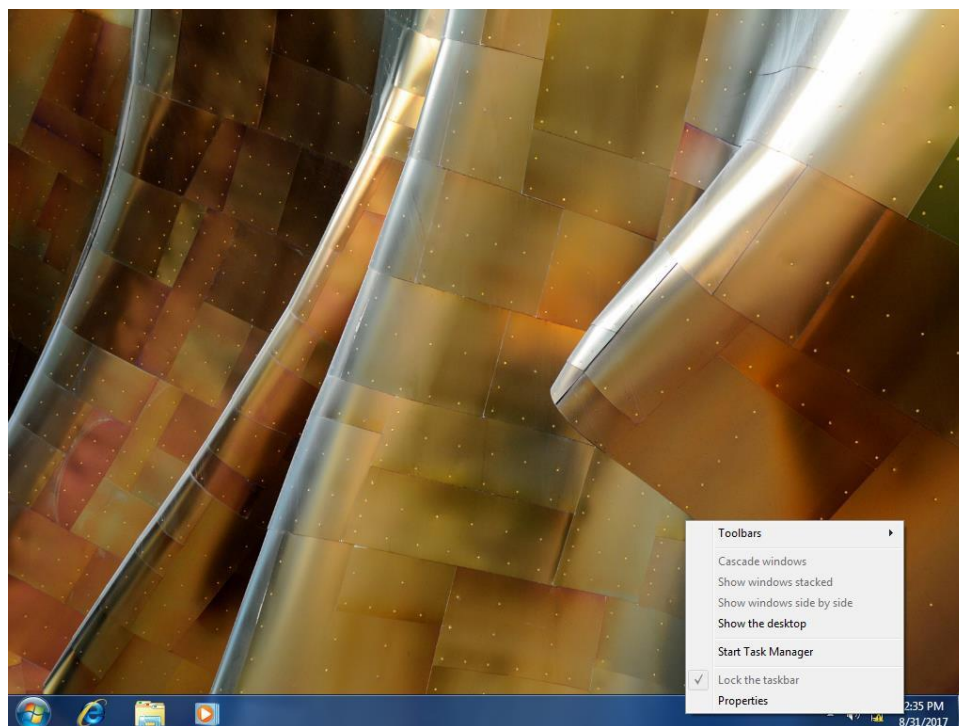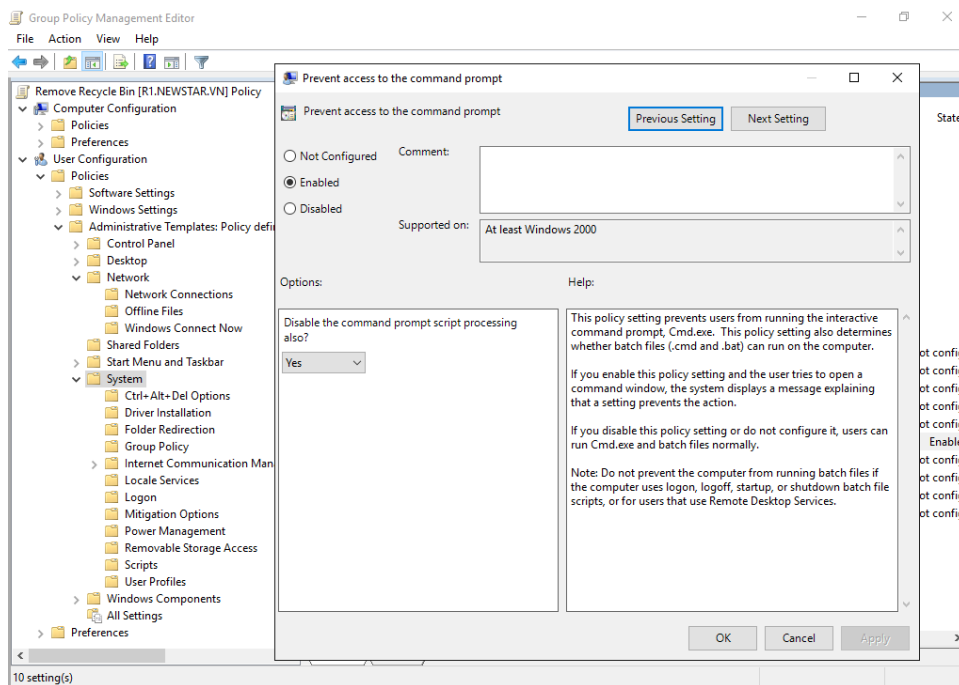*Hình 16-14: Không chỉnh được IP*

❖ **Start Menu and Taskbar**

Hình 16-15: Enble tính năng

Hình 16-16: Taskbar đã bị khóa

❖ **System**

Hình 16-17: Enable tính năng

Hình 16-18: CMD đã bị chặn

❖ **Windows Components**
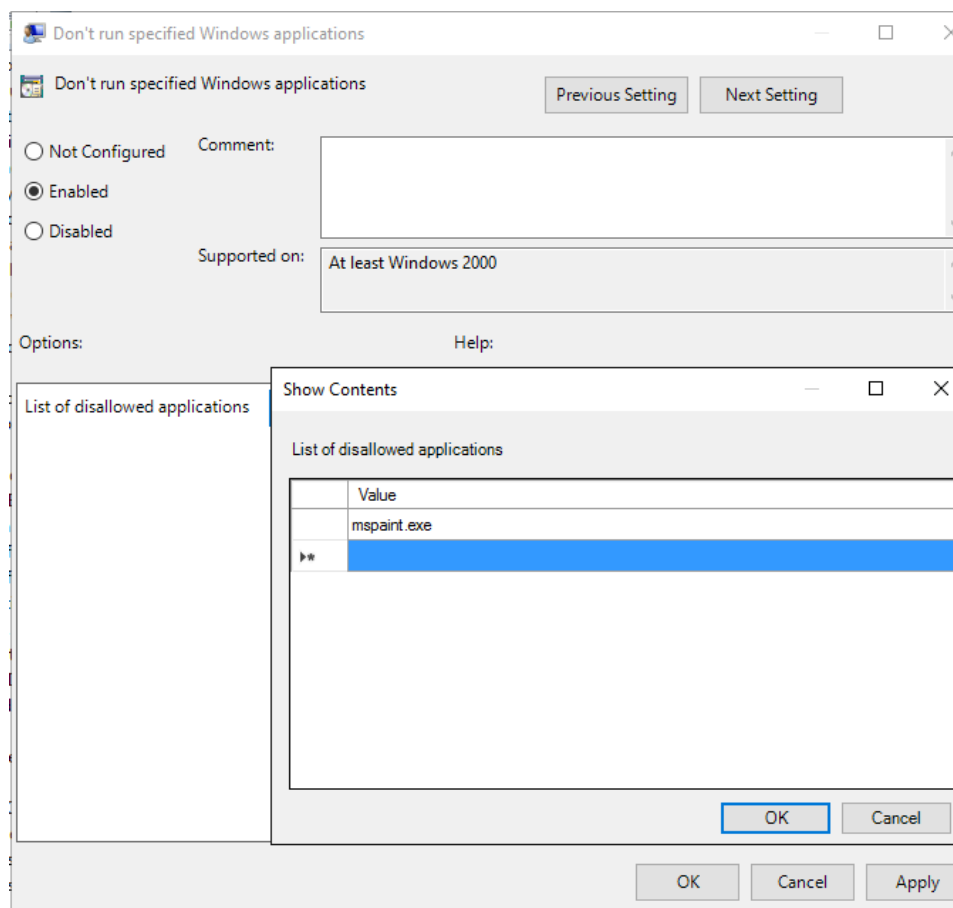
Hình 16-19: Enable tính năng

Hình 16-20: Truy cập phần mềm Paint đã bị chặn

5   Disk Quota

Sau khi học bài này sinh viên có khả năng giới hạn được dụng lượng ổ đĩa và chỉ định những file nào được chép vào thư mục đó

⬜ Chuẩn bị:
   + Một máy server 2016
   + Một máy Windows 7

⬜ Mô hình
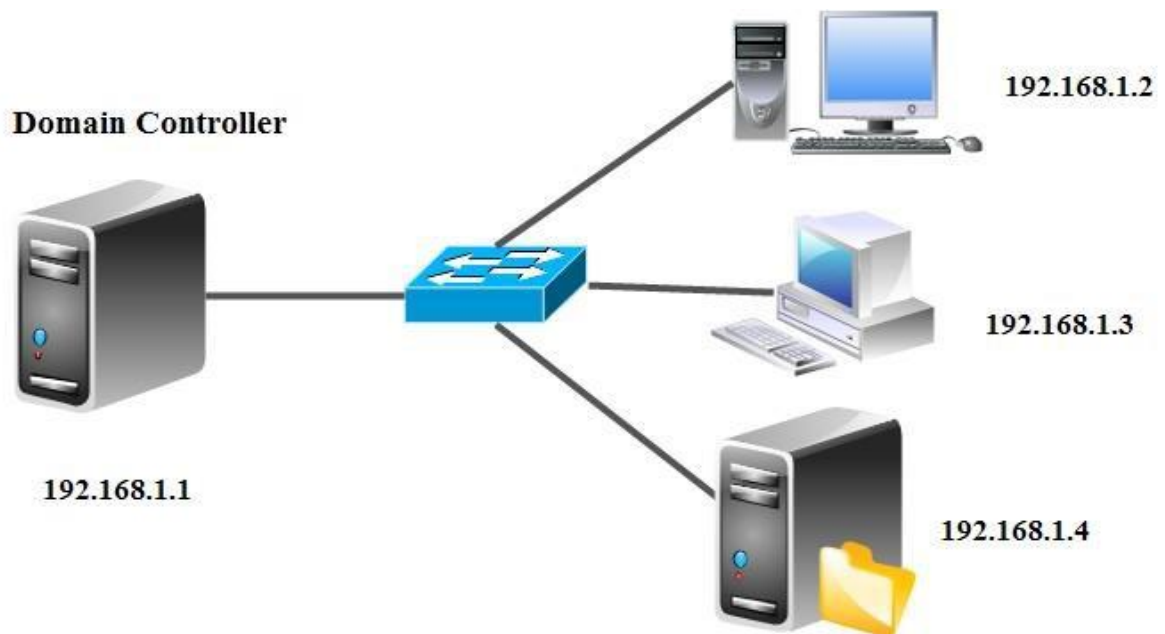
⬜ Kết quả đạt được
   ⬜ Mỗi User có một giới hạn ổ đĩa mạng và không cho chép file exe vào trong ổ đĩa mạng đó
⬜ Thực hiện
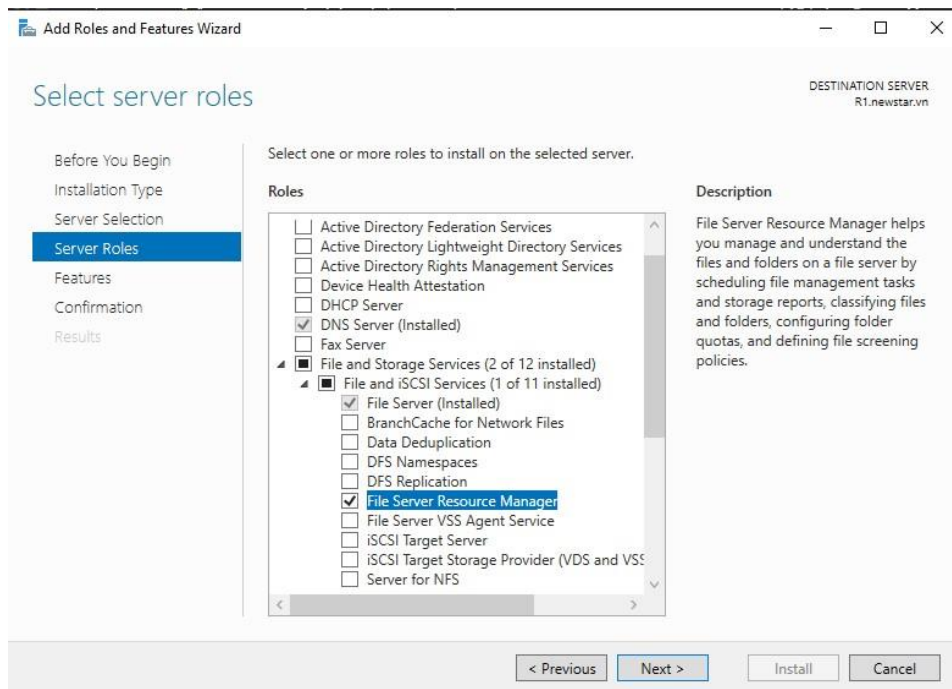
Hình 18-1: Cài FSRM
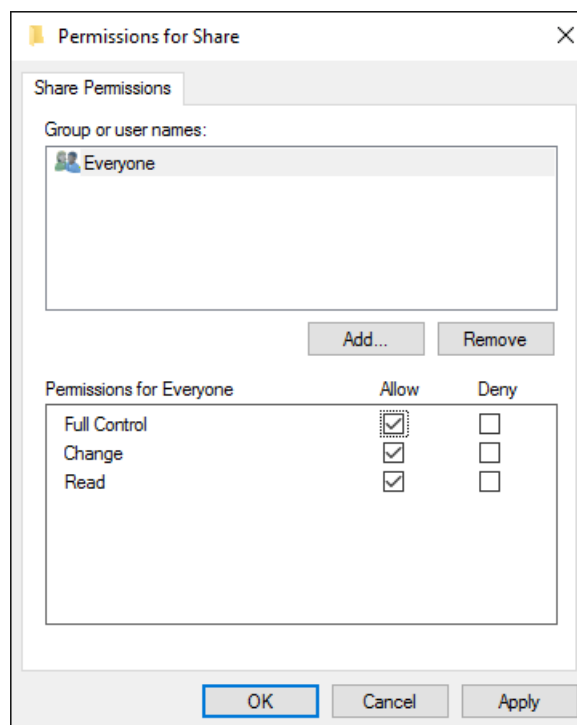
Hình 18-2: Share Folder
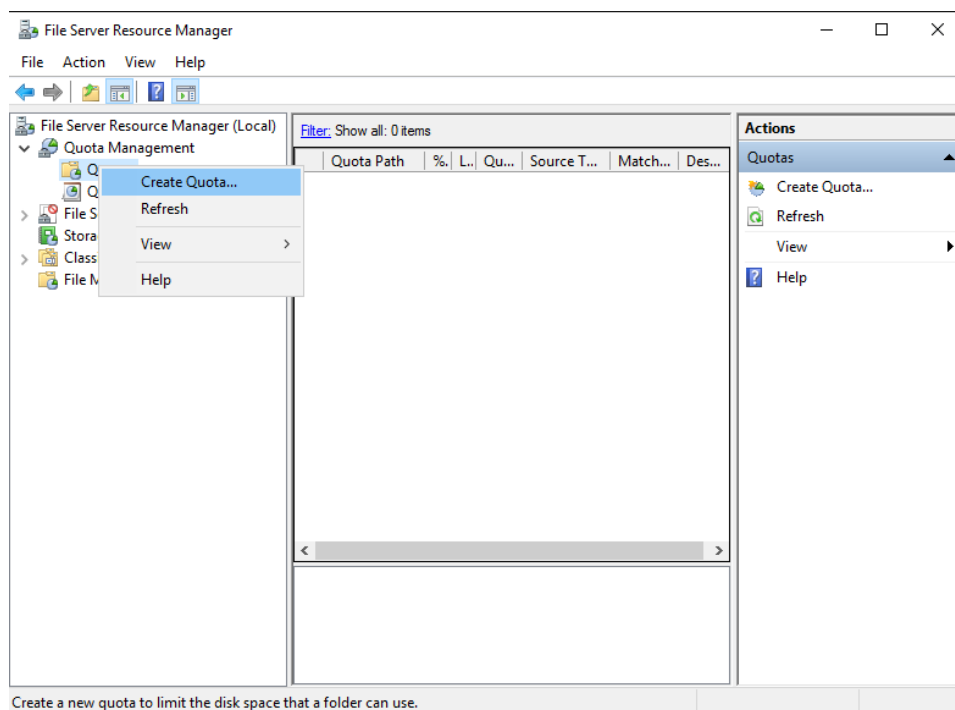
Hình 18-3: Tạo Quota
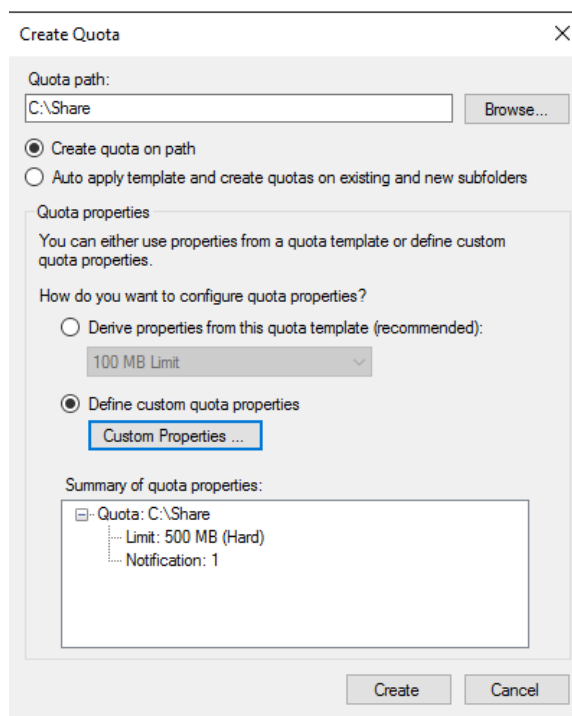
Hình 18-4: Chọn Folder share
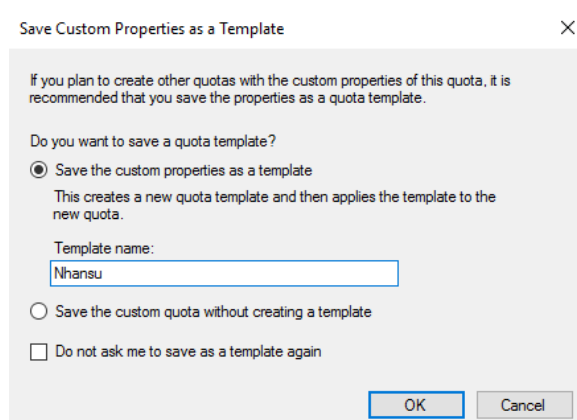
Hình 18-5: Đặt tên cho mẫu vừa làm

☐ Tiến hành chép file lớn hơn 500MB sẽ thông báo lỗi là không đủ dung lượng
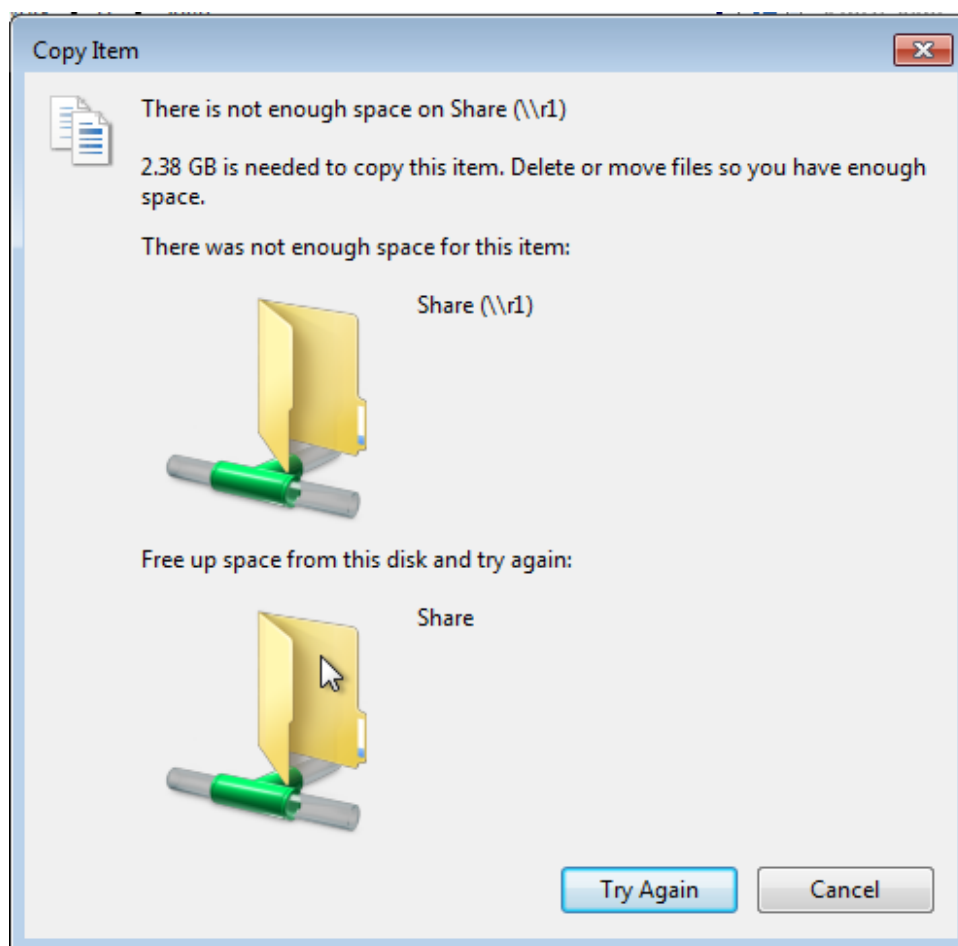
Hình 18-6: Cảnh báo không đủ ổ đĩa
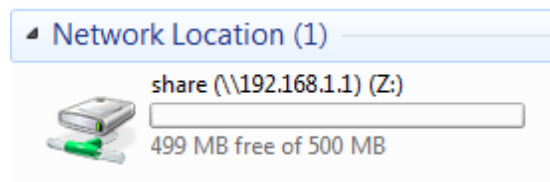
Hình 18-7: Ổ đĩa mạng map cho client
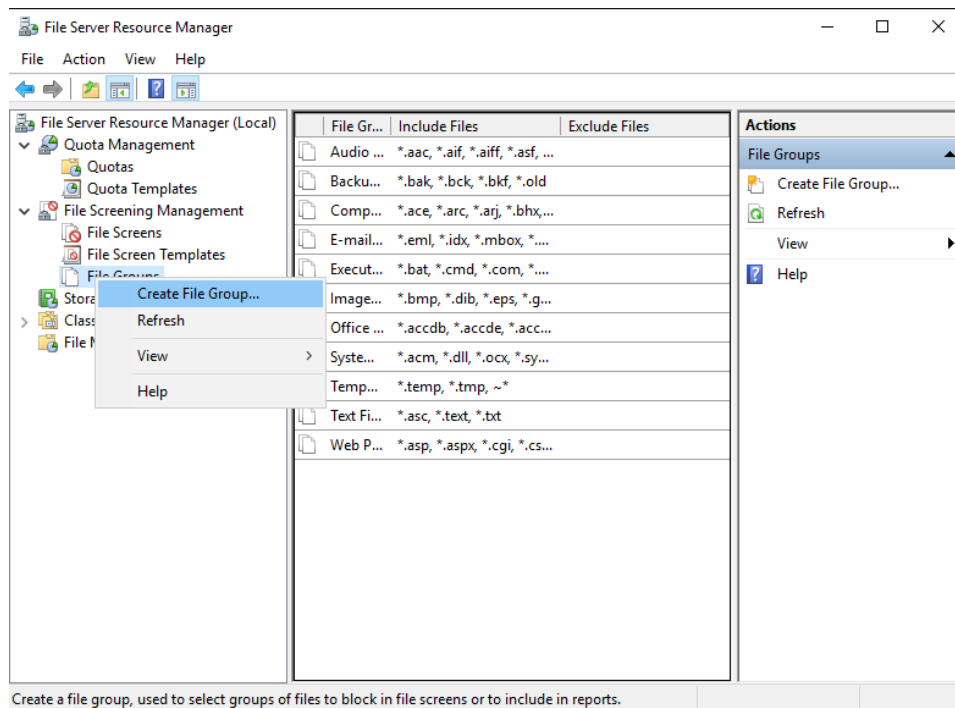
Hình 18-8: Tạo chính sách file

Tạo ra một group điều kiện file. Muốn cấm file nào thì nhập phần mở rộng vào Files to include, ngược lại thì nhập vào File to exclude
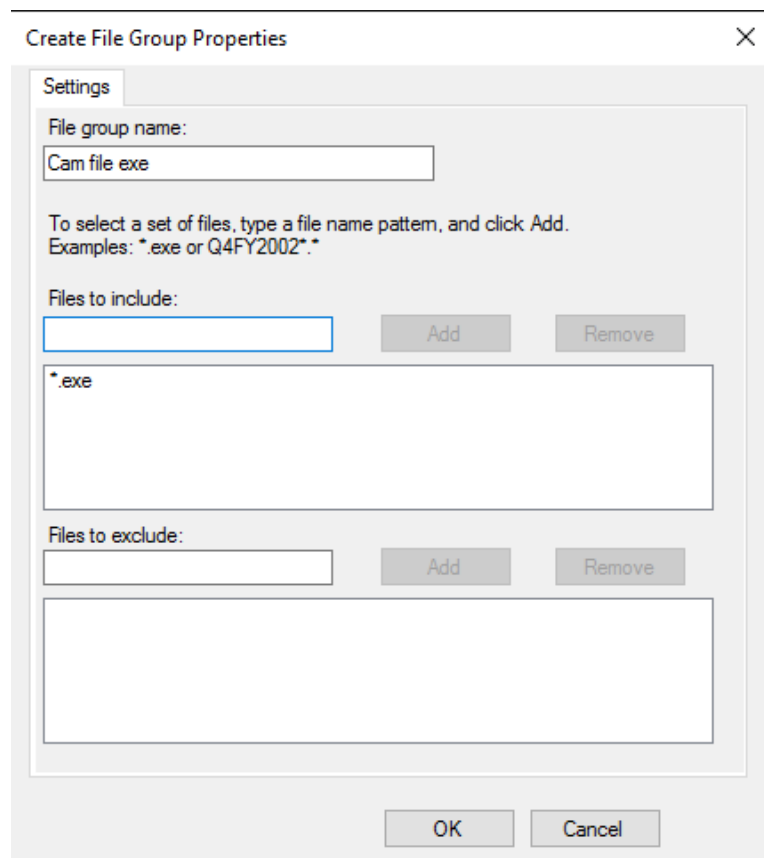
Hình 18-9: Cấm file exe

□ Đã tạo ra những quy luật cần gán những quy luật đó cho folder nào
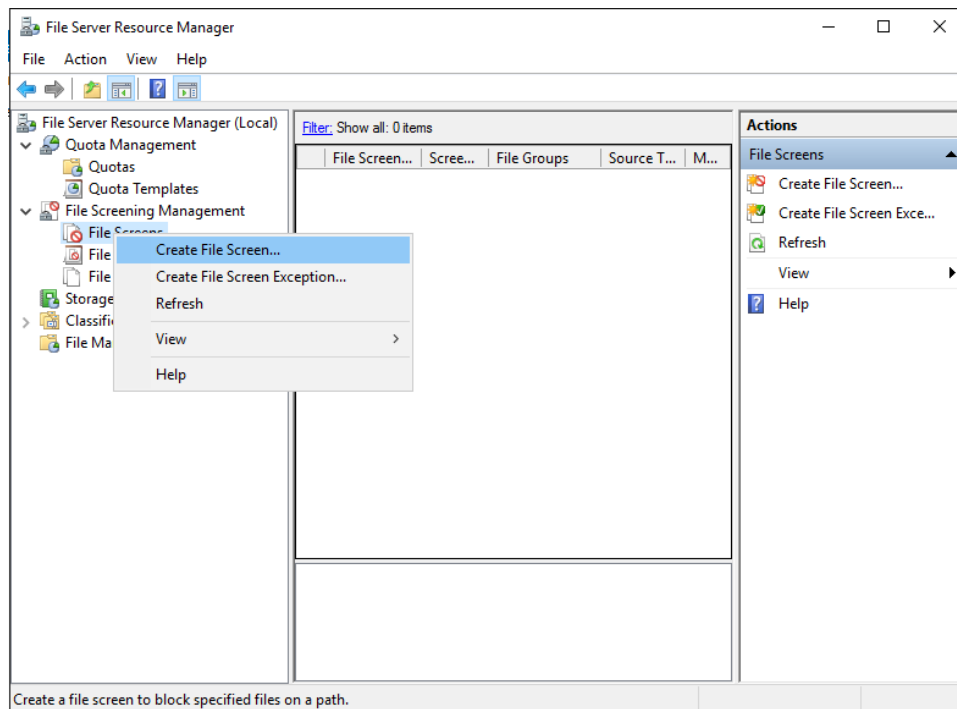
Hình 18-10: Tạo ra file Screen
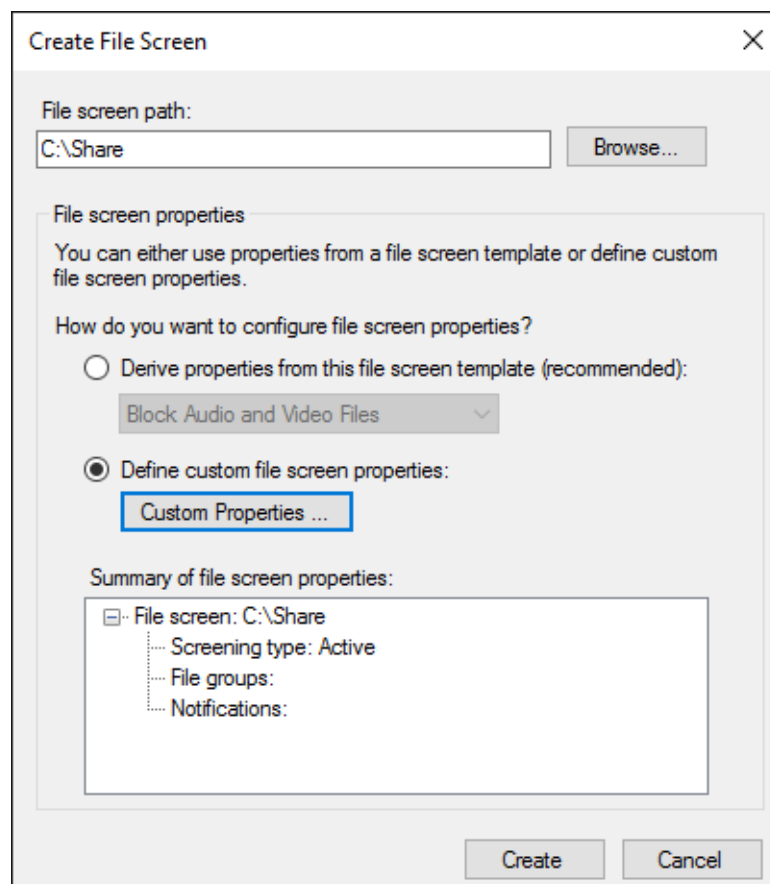
Hình 18-11: Chọn Custom Properties
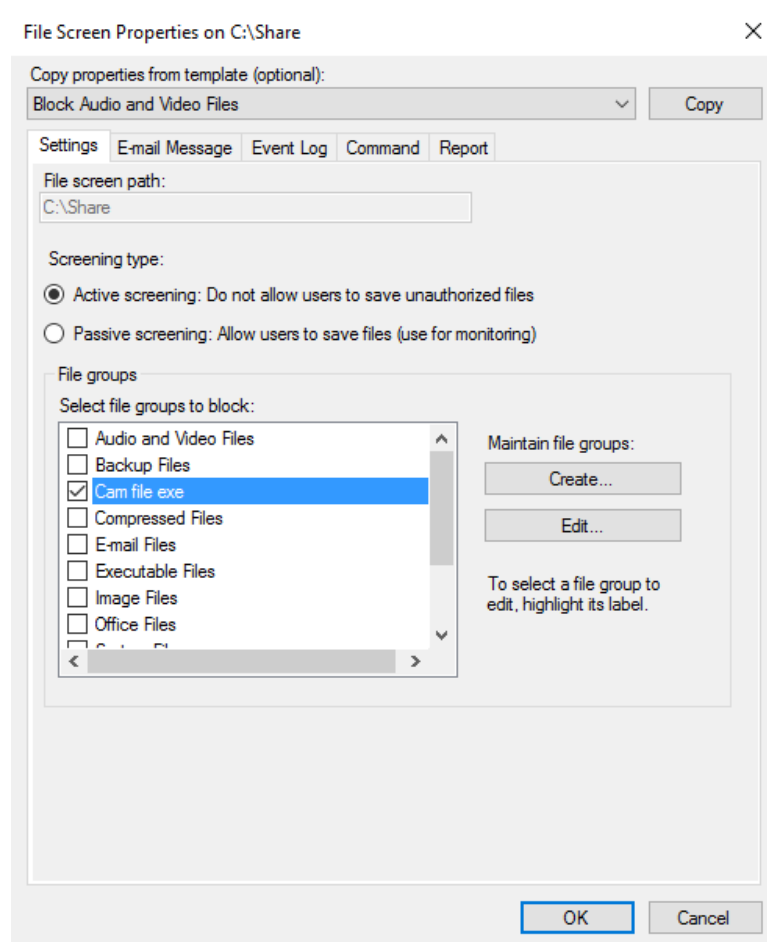
Hình 18-12: Chọn temple đã tạo
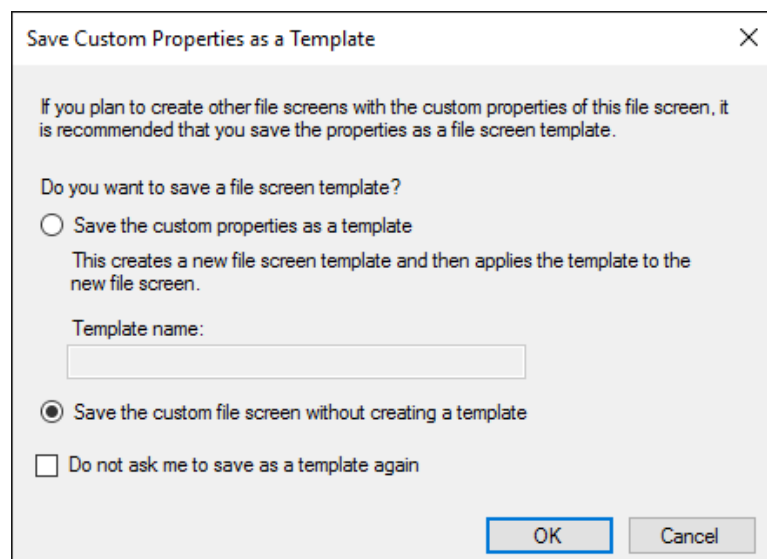
Hình 18-13: Lưu thay đổi lại

- ☐ Tiến hành chép file exe vào folder mà ta đã tạo. Lúc đó sẽ có cảnh báo là không có quyền để chép file đó, nếu chép file khác thì được
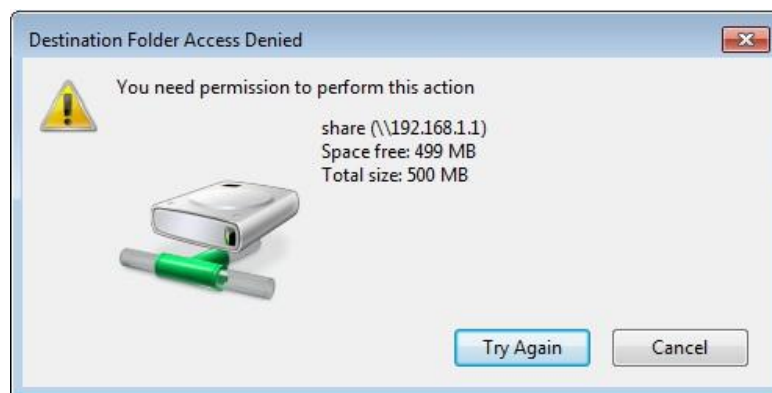
Hình 18-14: Không có quyền chép file
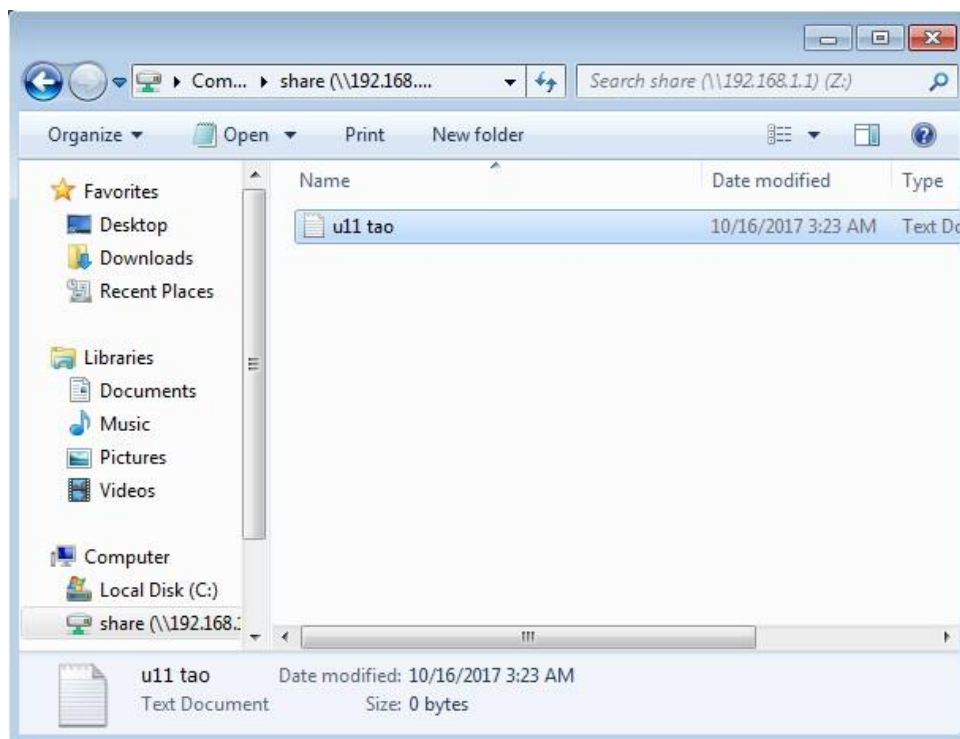
Hình 18-15: File khác tạo thì được

6   Triển khai Deploy Software

Sau khi học bài này xong sinh viên có thể cài ứng dụng tự động cho các user hoặc cho các pc thông qua chính sách GPO

⬜ Chuẩn bị:
+ Một máy server 2016 đã lên domain
+ Một máy windows 7

⬜ Mô hình

Domain Controller

192.168.1.2

192.168.1.3

192.168.1.4

192.168.1.1
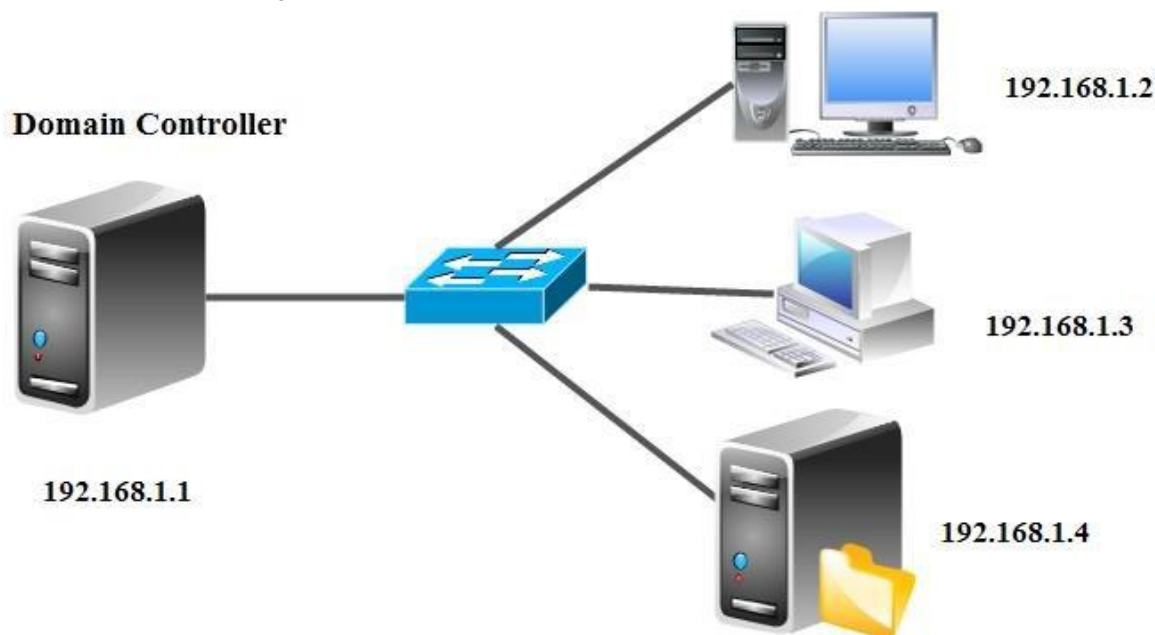
⬜ Kết quả đạt được
⬜ Cài phần mềm foxit reader khi đăng nhập tài khoản ở máy client
⬜ Thực hiện

⬜ Thực hiện tạo OU và 2 user u1, u2 nằm trong OU nhansu
⬜ Tiến hành tạo GPO mang tên deploy software
⬜ Link từ GPO deploy software sang OU nhansu
⬜ Cập nhật chính sách GPO bằng lệnh gpupdate /force
⬜ Thực hiện trên máy DC
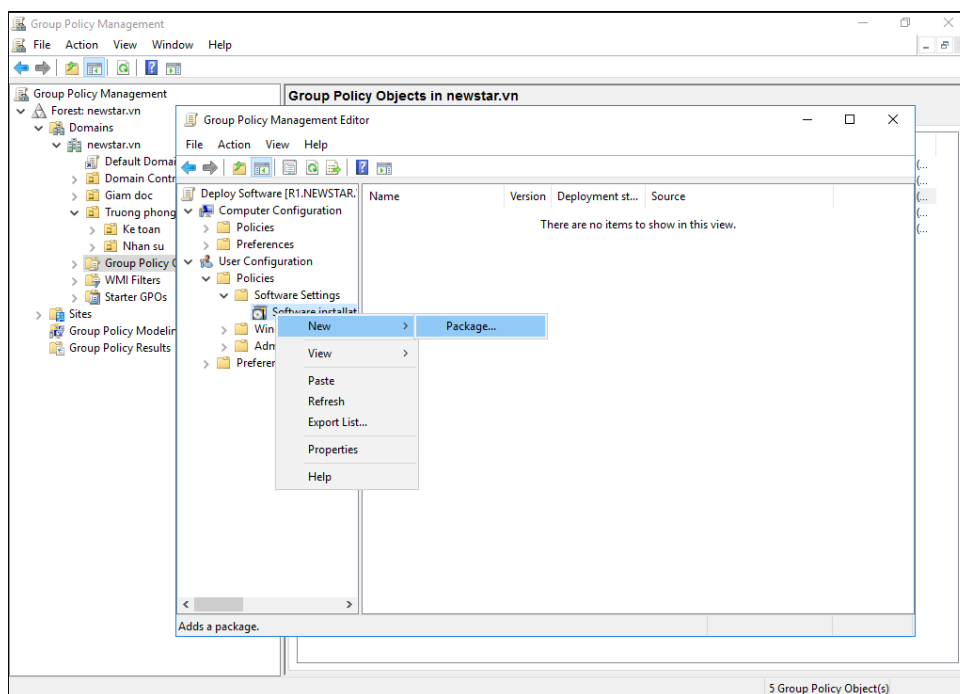
Hình 19-1: Chọn phần mềm
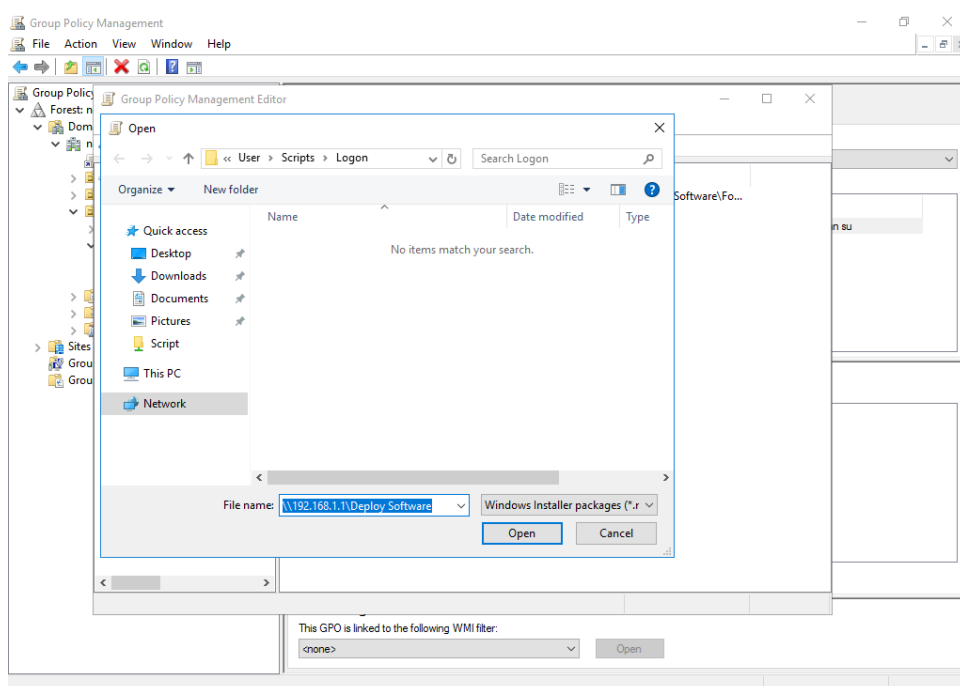
Hình 19-2: Đường dẫn mạng lưu trữ phần mềm
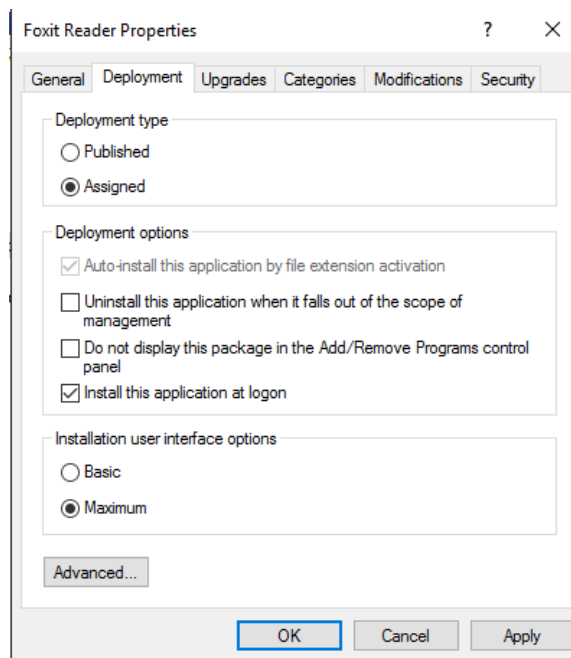
Hình 19-3: Chọn Assigned

☐ Truy cập ở máy Client với tài khoản u1
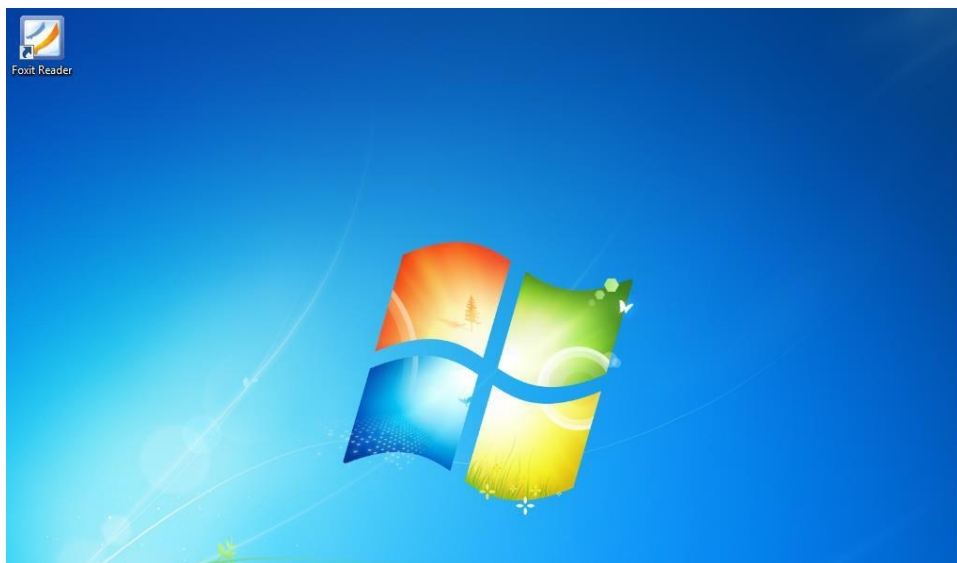
Hình 19-4: Kết quả của máy client

7 Domain đồng cấp

Sau khi học bài này xong người học có khả năng sự cân bằng cho Domain, dự phòng cho domain

☐ Chuẩn bị:
  + Một máy windows server đã lên DC
  + Một máy windows server join Domain
  + Một máy windows 7
☐ Mô hình
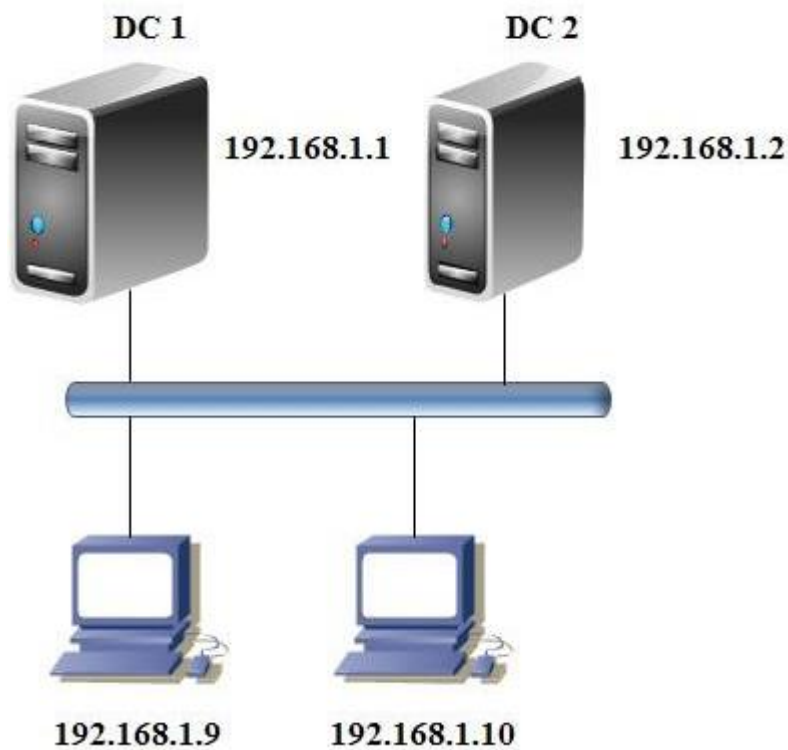
☐ Kết quả đạt được
  ☐ Tạo U1 và U2 bên Primary sẽ thấy bên Secondary
  ☐ Chuyển 5 role quản trị sang cho R2
  ☐ Sau đó dùng lệnh chuyển 5 role từ R2 sang R1
☐ Thực hiện
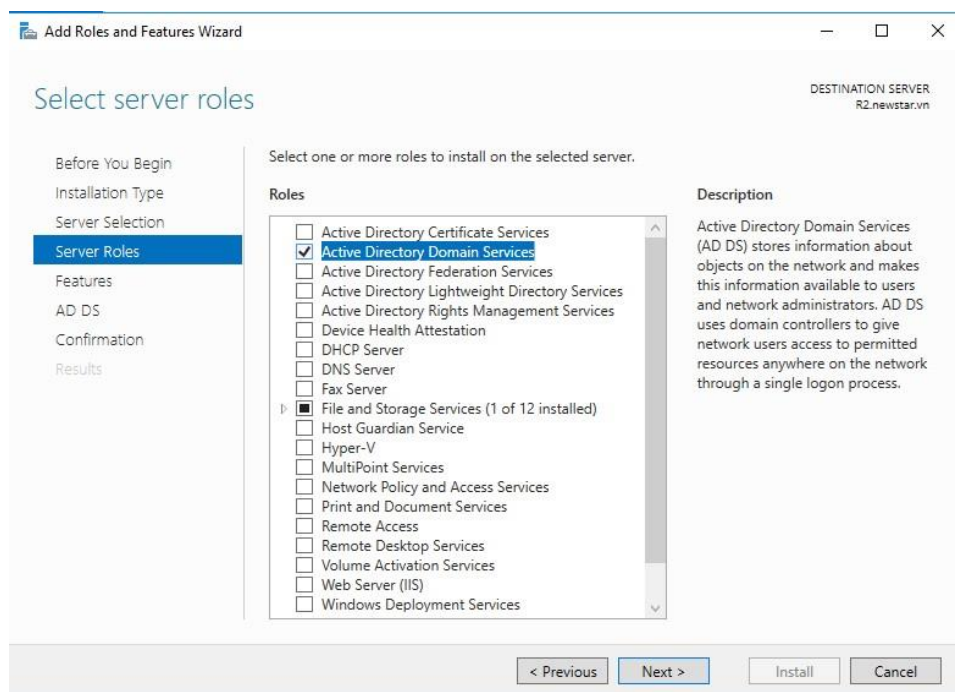
Hình 22-1: Cài đặt ADDS
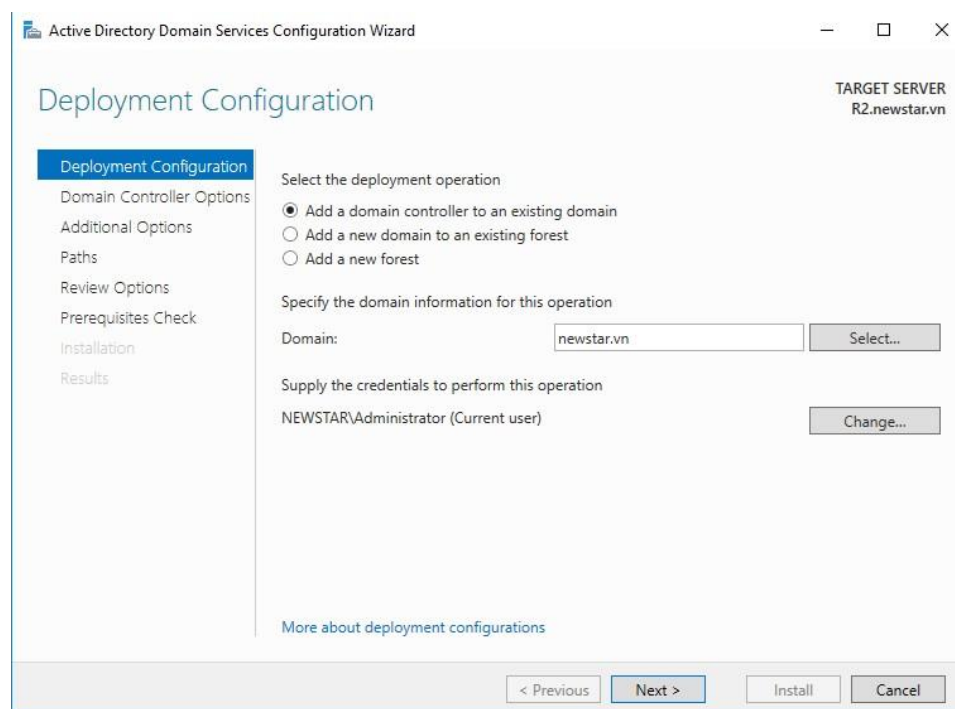
Hình 22-2: Chọn mục đầu tiên
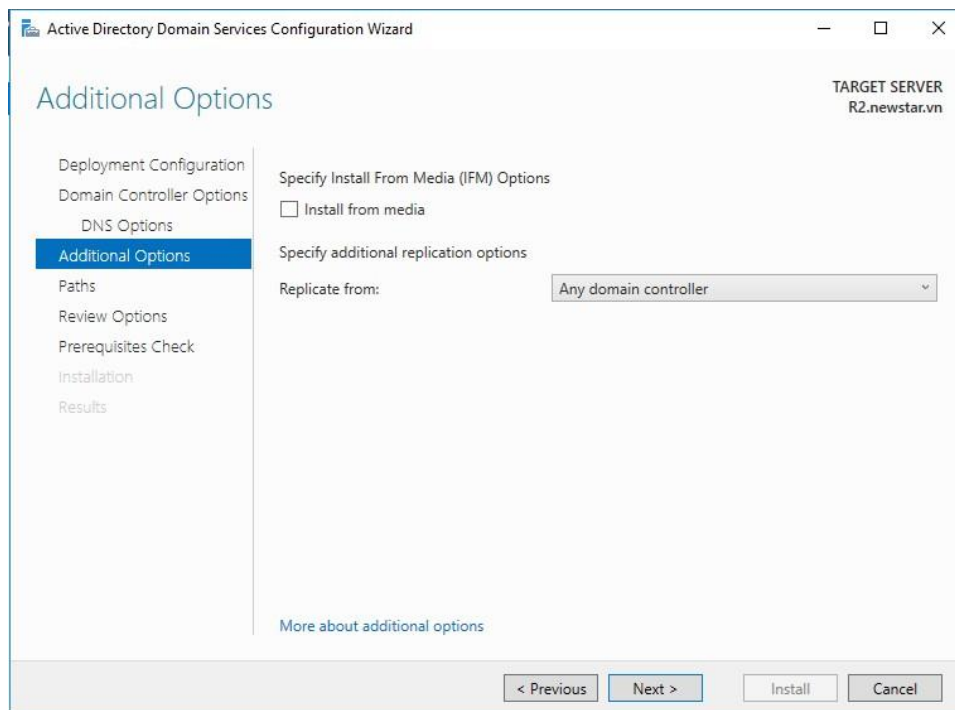
Hình 22-3: Cập nhật giữa các domain

☐ Tạo user U11 và U12 ở domain Priamary sau đó qua domain Secondary
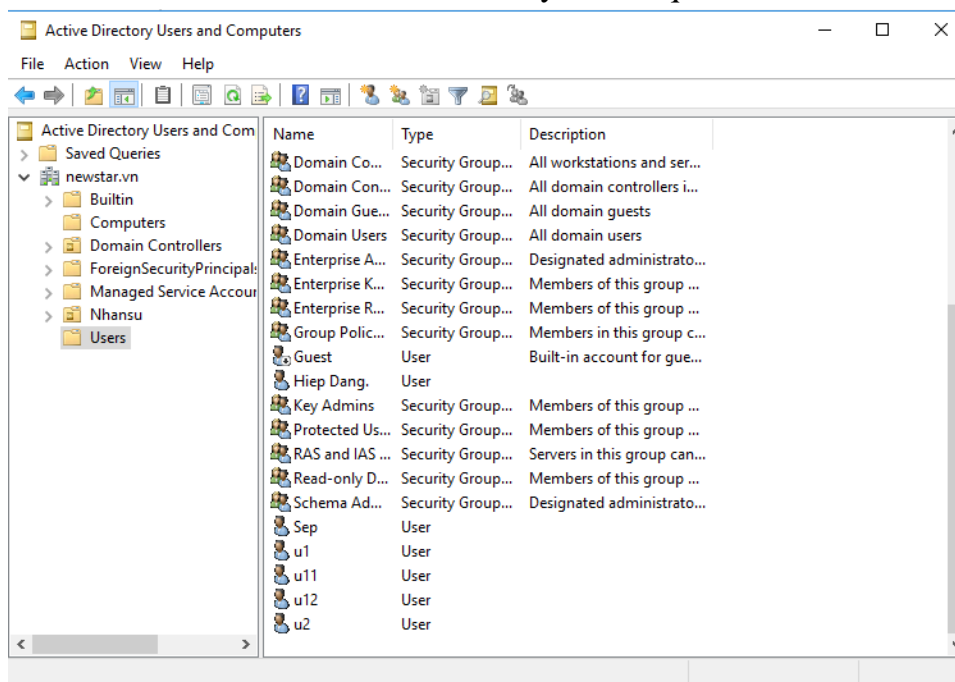
Hình 22-4: U11 và U12 đã cập nhật

☐ Trên một hệ thống domain sẽ có 5 role để quản lý tài nguyên cho domain. Ở đây ta tiến hành chuyển đổi role qua lại giữa 2 domain chính phụ
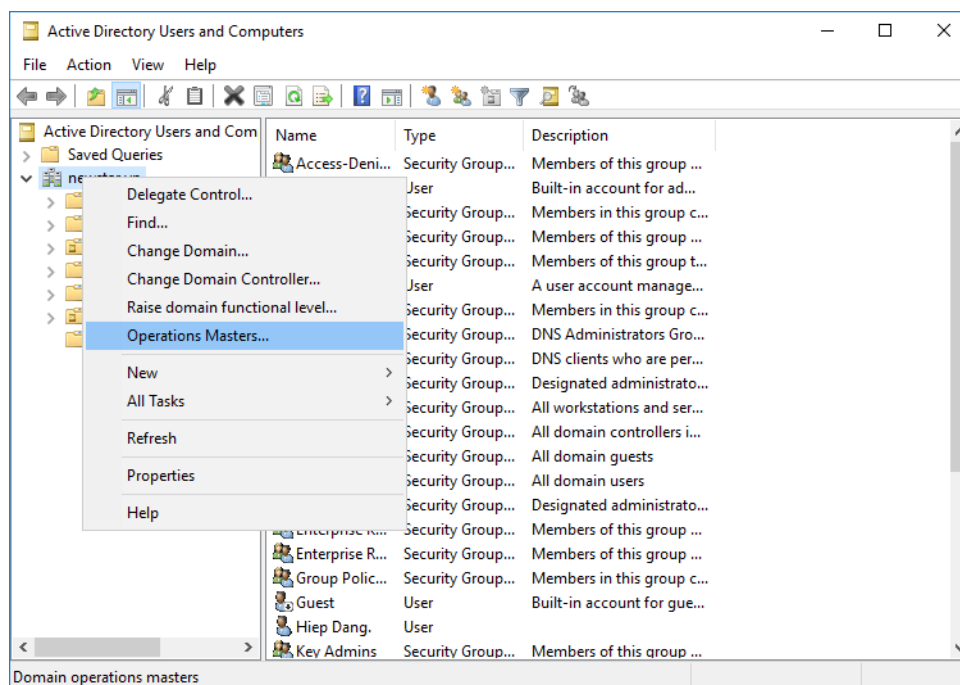
Hình 22-5: Chọn vào Operations Master

 Chuyển đổi RID qua R2: Change
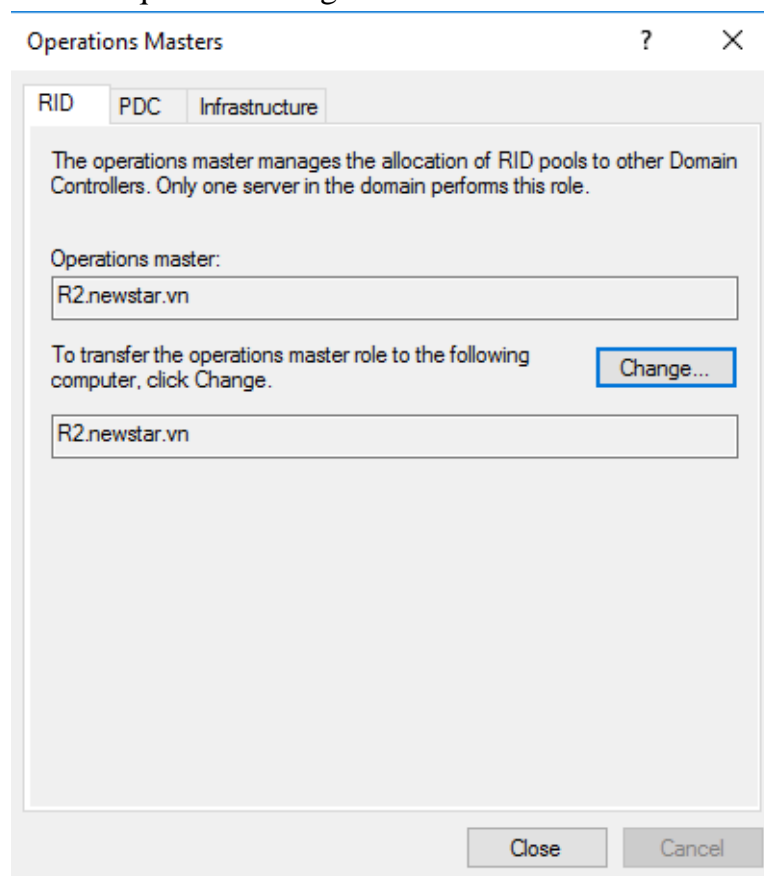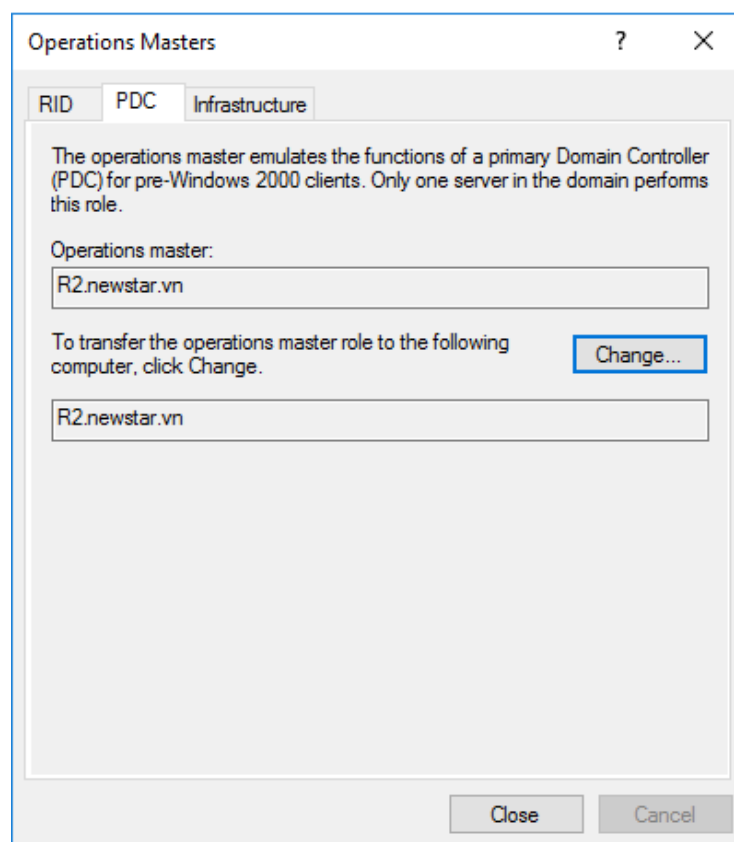
Hình 22-6: Chuyển đổi PDC qua R2
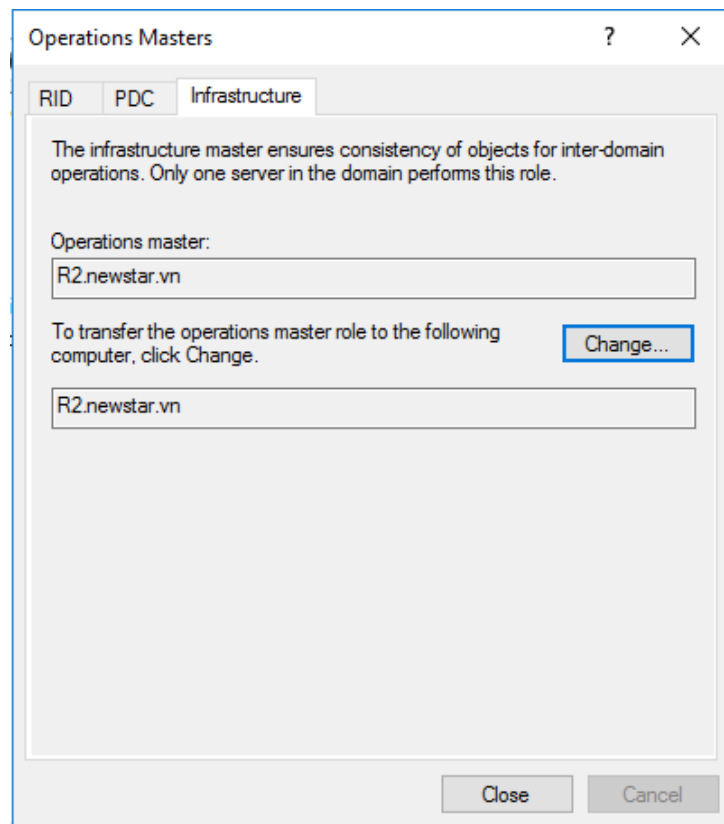
Hình 22-7: Chuyển đổi Infrastructure qua R2

☐ Chọn vào Active Directory Domain and Truts để chuyển R2
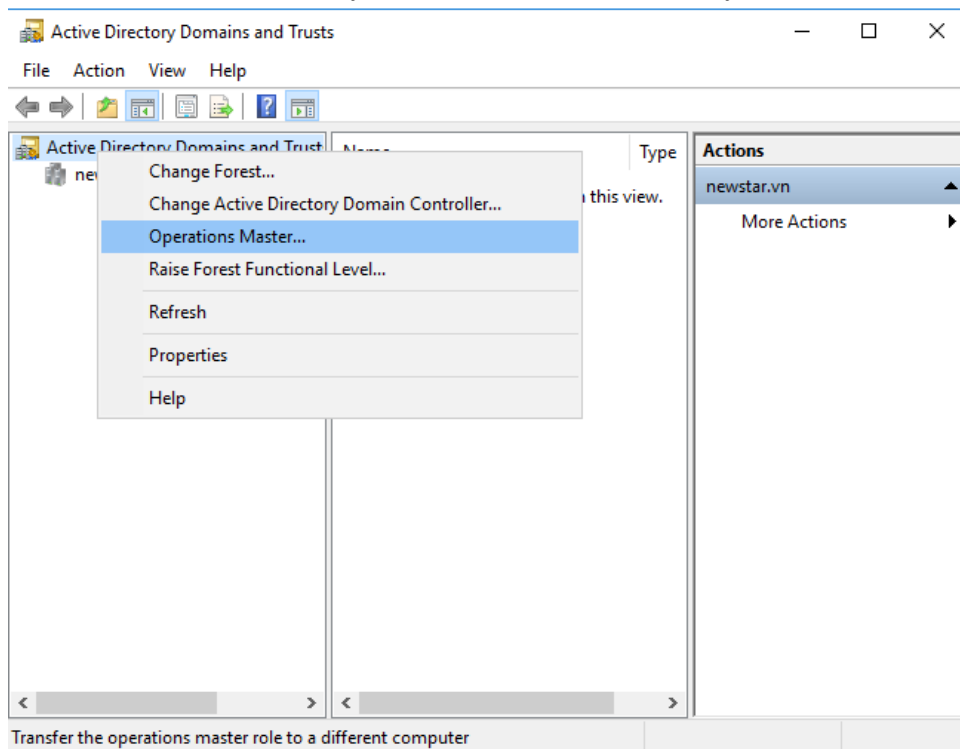
Hình 22-8: Chuyển đổi Role Schema
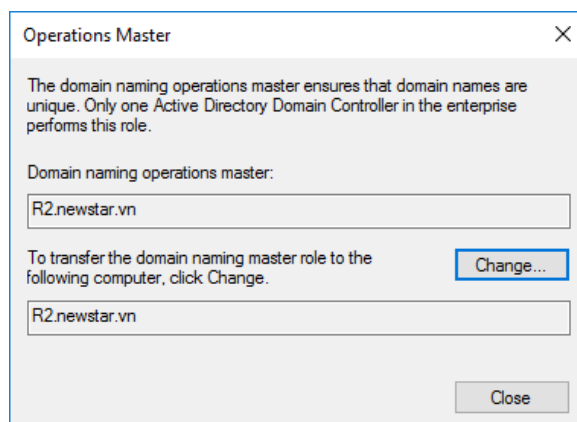
Hình 22-9: Chuyển đổi Role qua R2
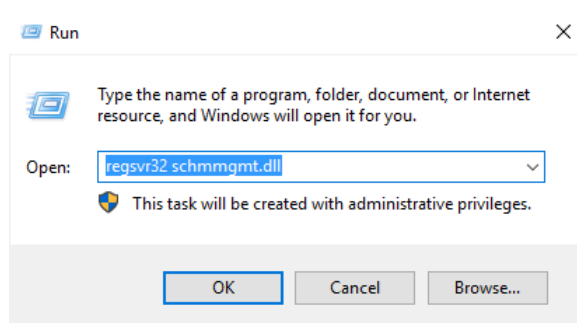
Hình 22-10: Mở Snap-in trên CMD
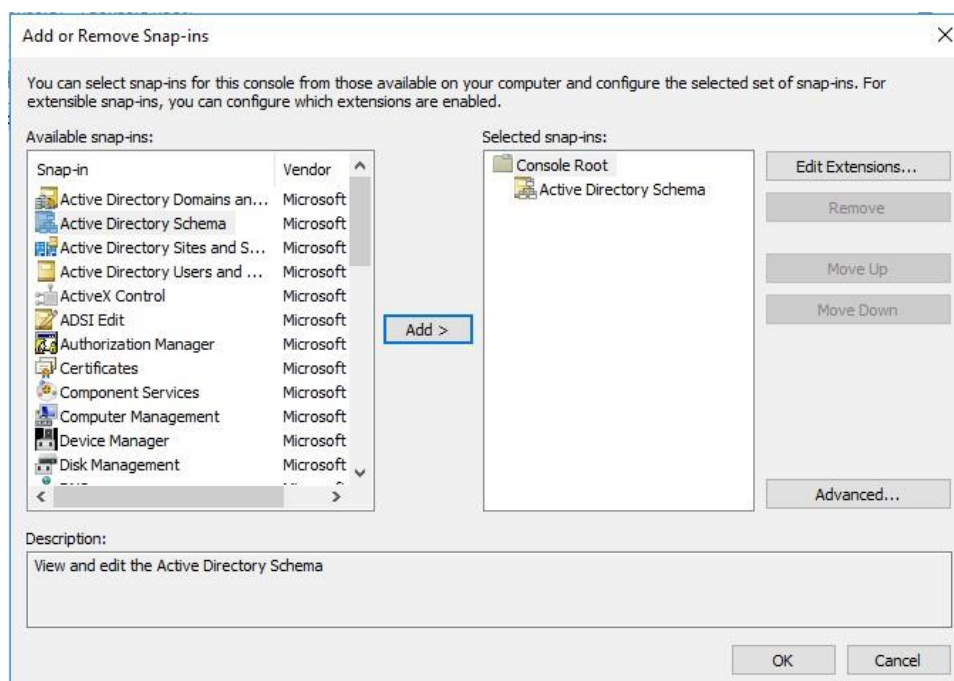
Hình 22-11: Add ADS
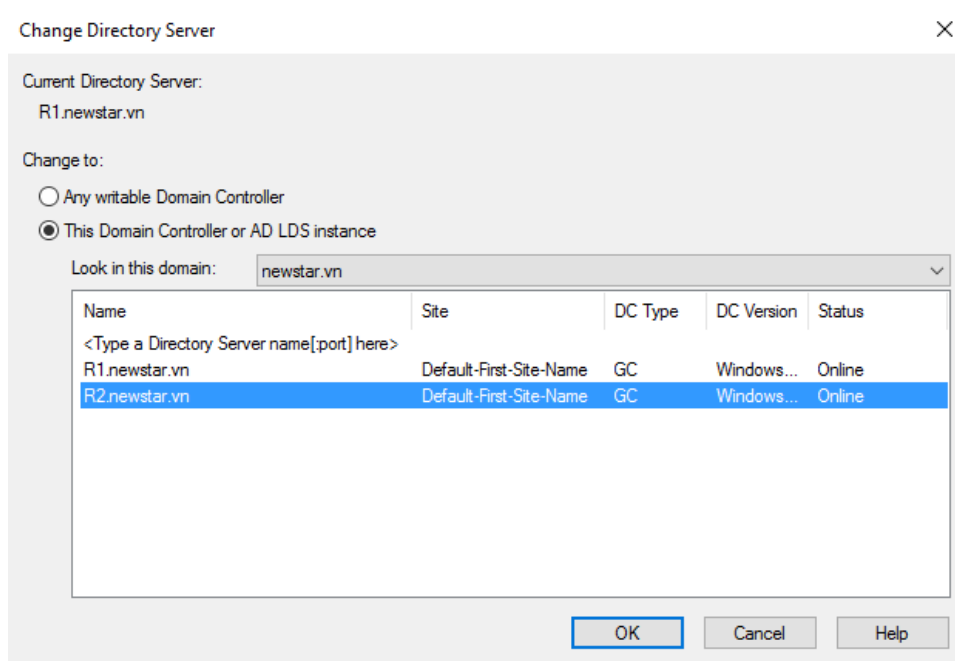
Hình 22-12: Chọn Server muốn add
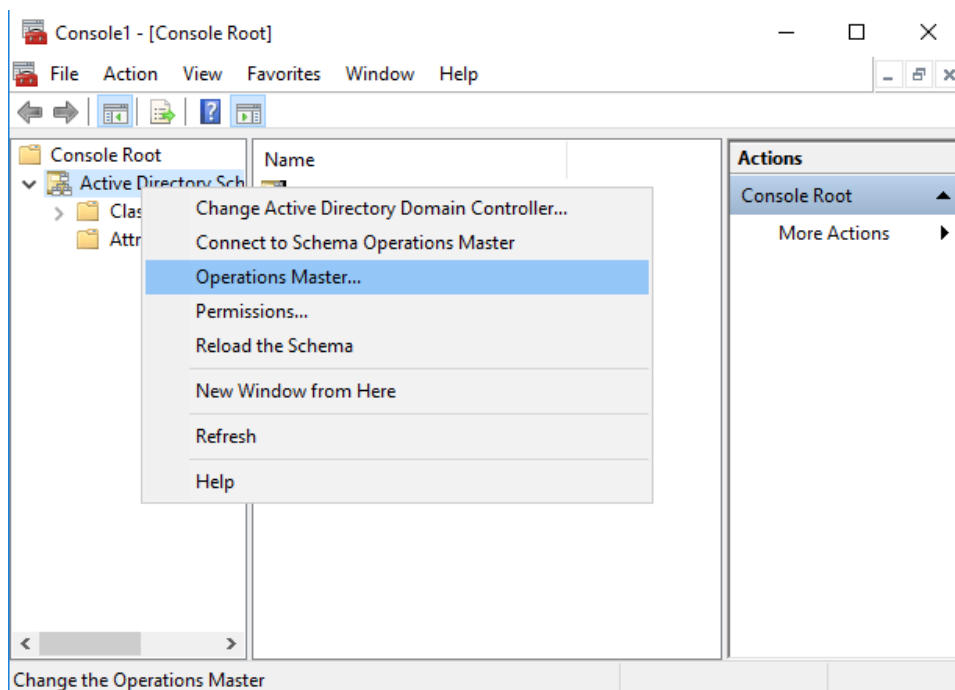
Hình 22-13: Chọn vào Operations Master
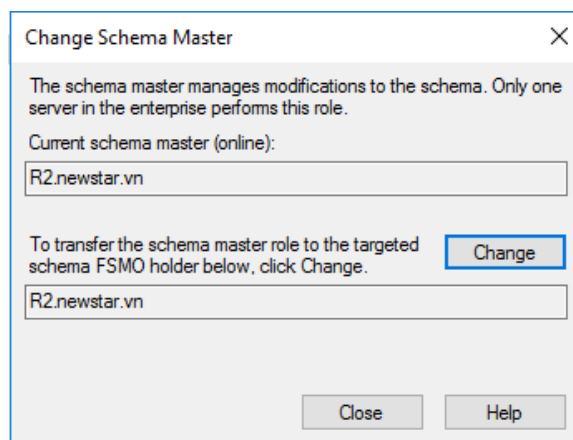
Hình 22-14: Chọn change

Hình 22-15: Các Role đã chuyển qua R2

☐ Thực hiện chuyển các Role bằng lệnh, ngồi trên R1

Hình 22-16: Kết nối tới R1

☐
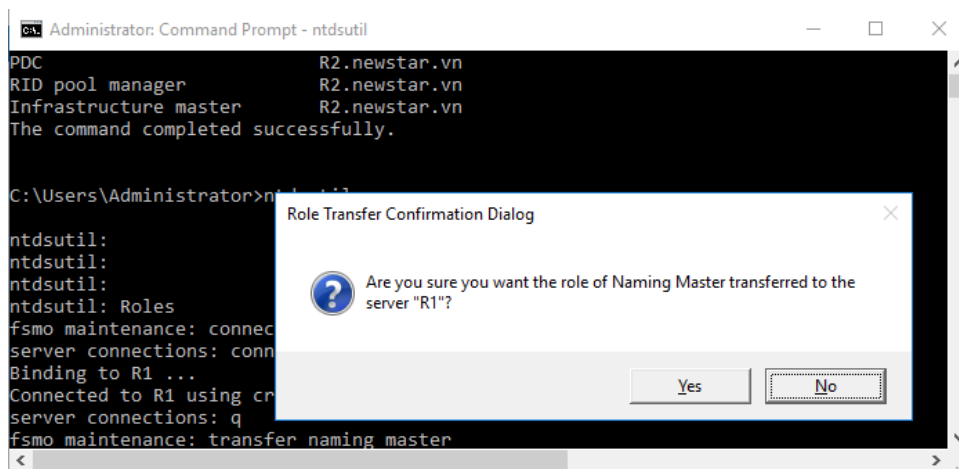
Hình 22-17: Chuyển Role sang R1
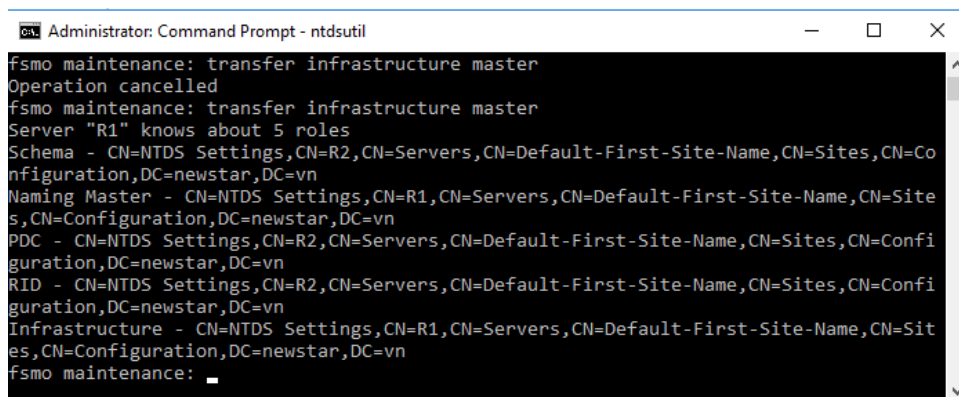
Hình 22-18: Chuyển Role Infrastructure sang R1
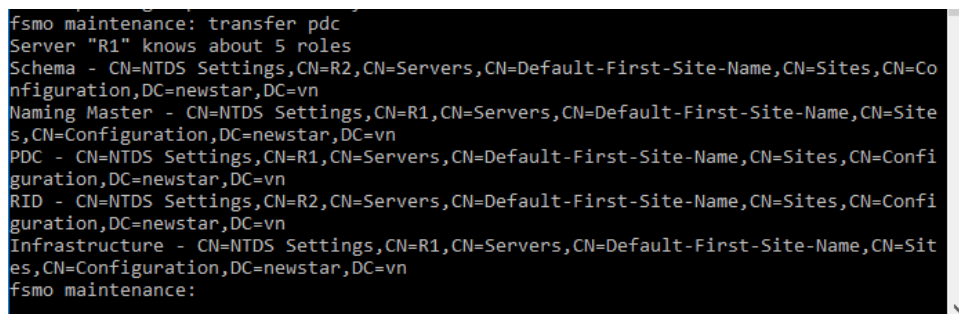
Hình 22-19: Chuyển Role PDC sang R1
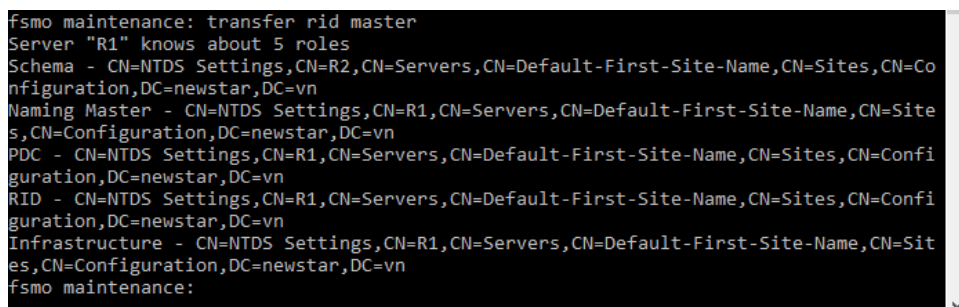
Hình 22-20: Chuyển Role RID sang R1

Hình 22-21: Chuyển Role Schema sang R1

Hình 22-22: Quá trình chuyển đổi thành công

8   Domain con

Sau khi học xong bài này sinh viên có khả năng xây dựng một domain con. Một domain không chịu chính sách của domain cha
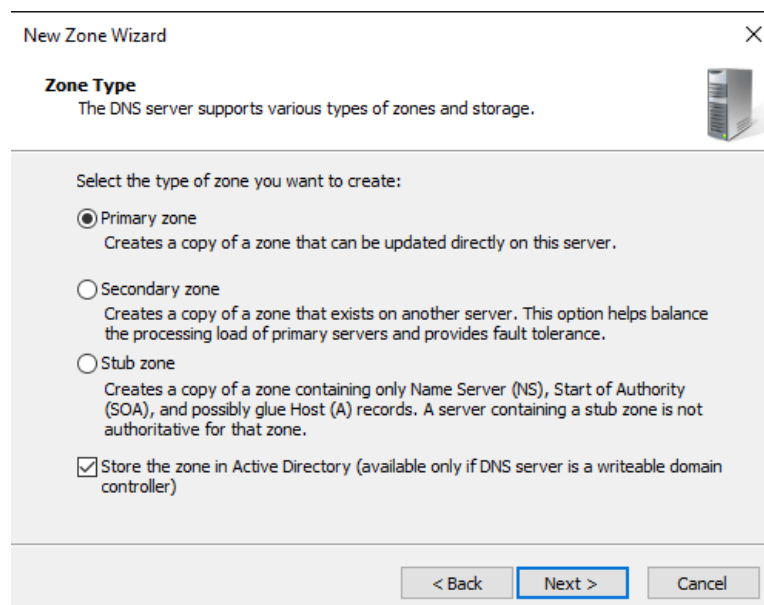
- ☐ Chuẩn bị:
  + Một máy windows server đã lên DC
  + Một máy windows server join Domain
  + Một máy windows 7
- ☐ Mô hình
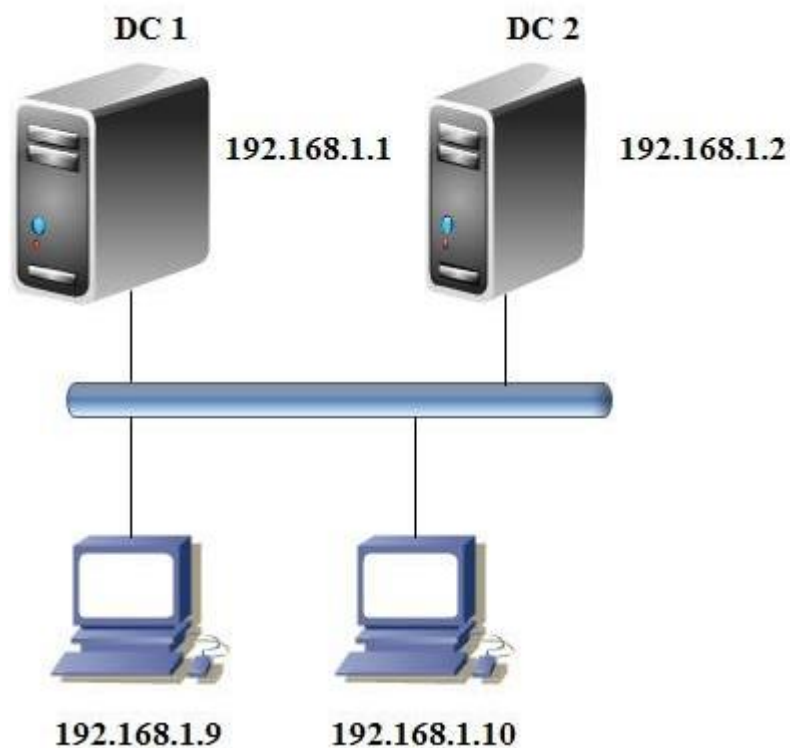
- ☐ Kết quả đạt được
  - ☐ Điều chỉnh chính sách Password ở domain con, tạo u1 không ảnh hưởng chính sách domain cha
  - ☐ Thực hiện
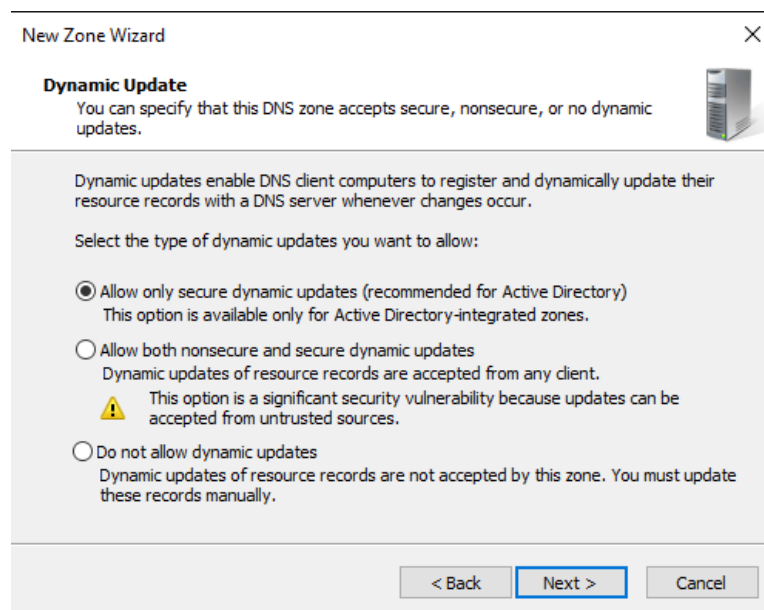- ☐ Thực hiện cấu hình DNS domain con trên R1
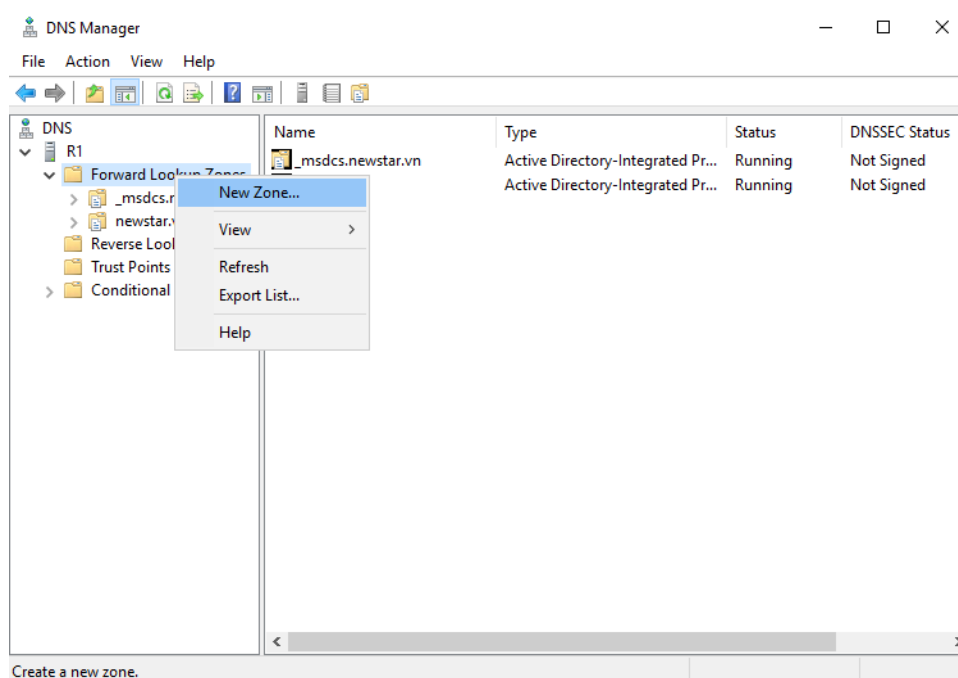
Hình 23-1: Chọn New Zone

Hình 23-2: Primary zone
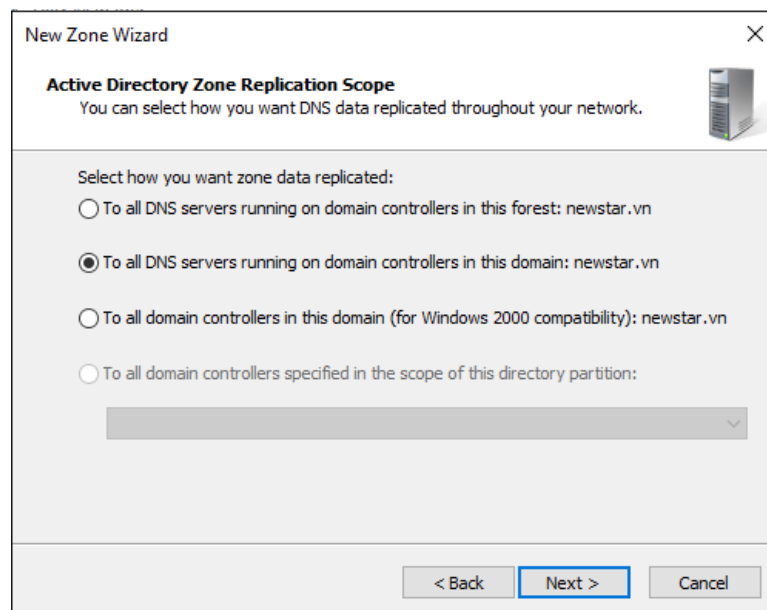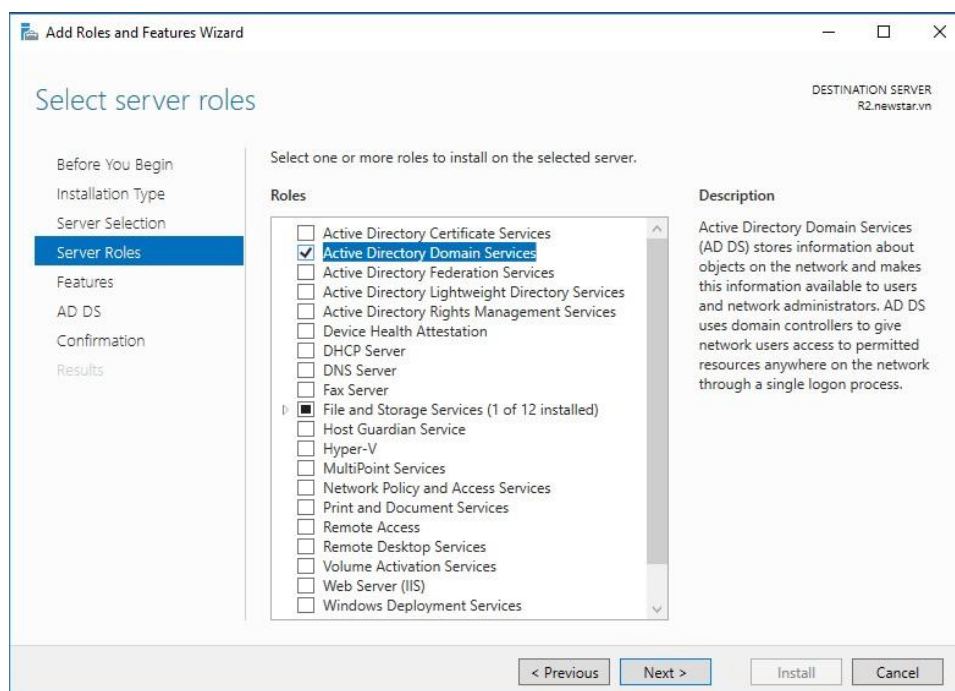
Hình 23-3: Cập nhật với domain newstar
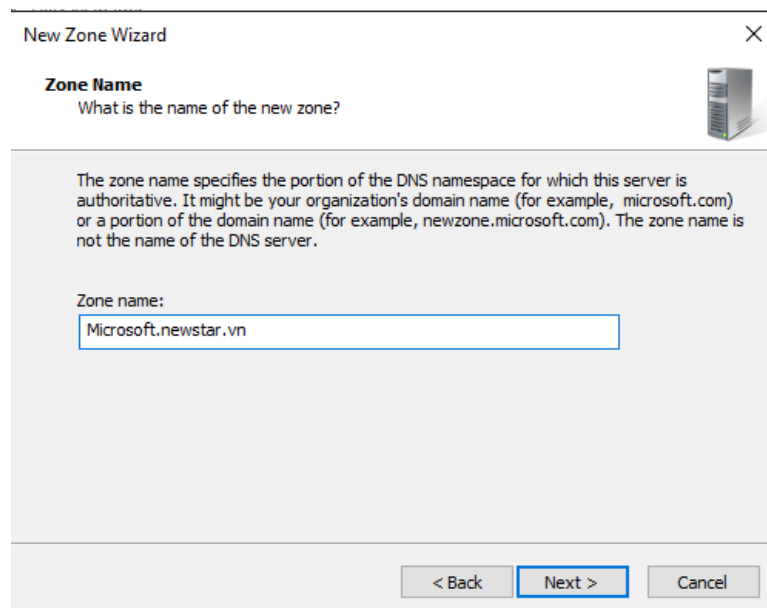
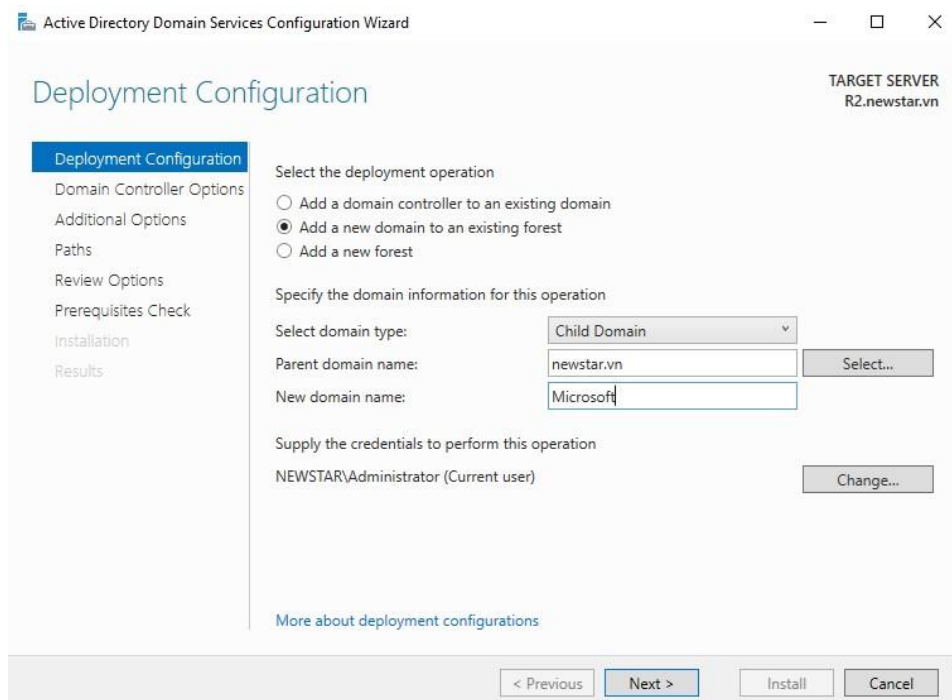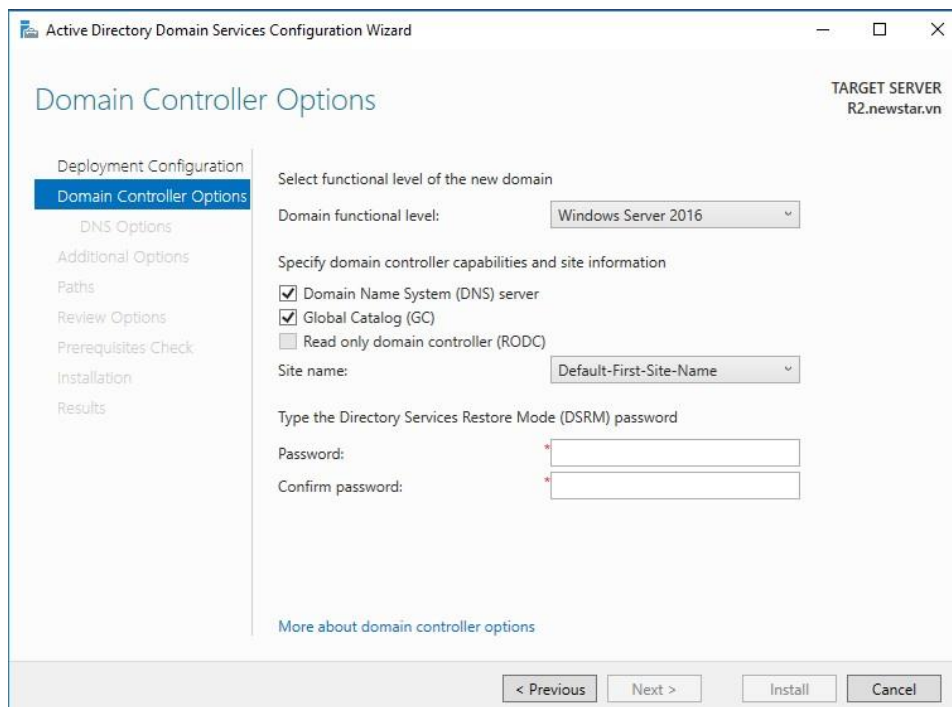*Hình 23-4: Tạo zone domain con*

Hình 23-5: Cập nhật với domain

☐ Tạo domain con trên R2

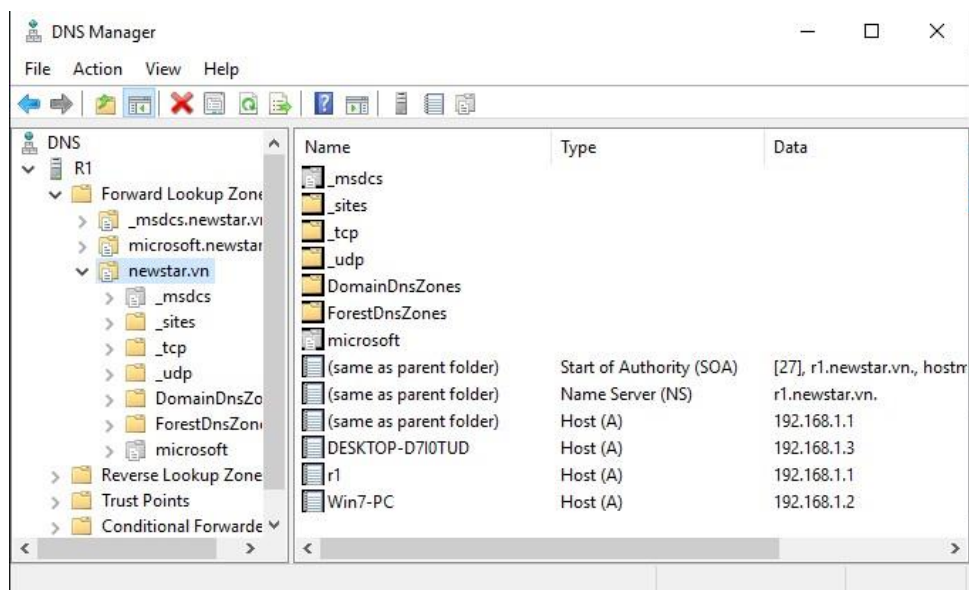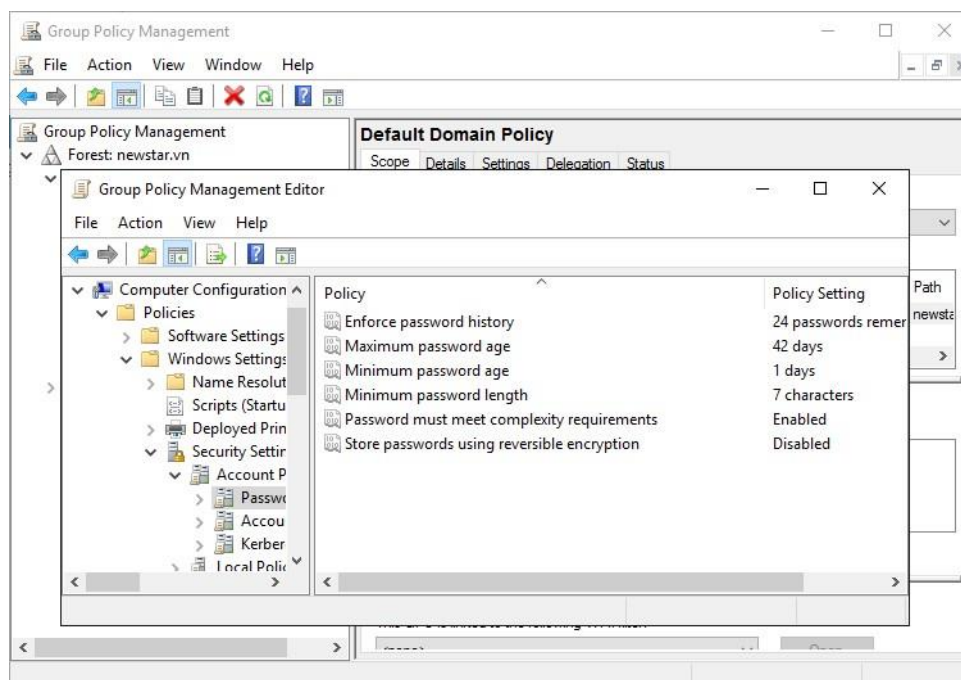*Hình 23-6: Cài ADDS*

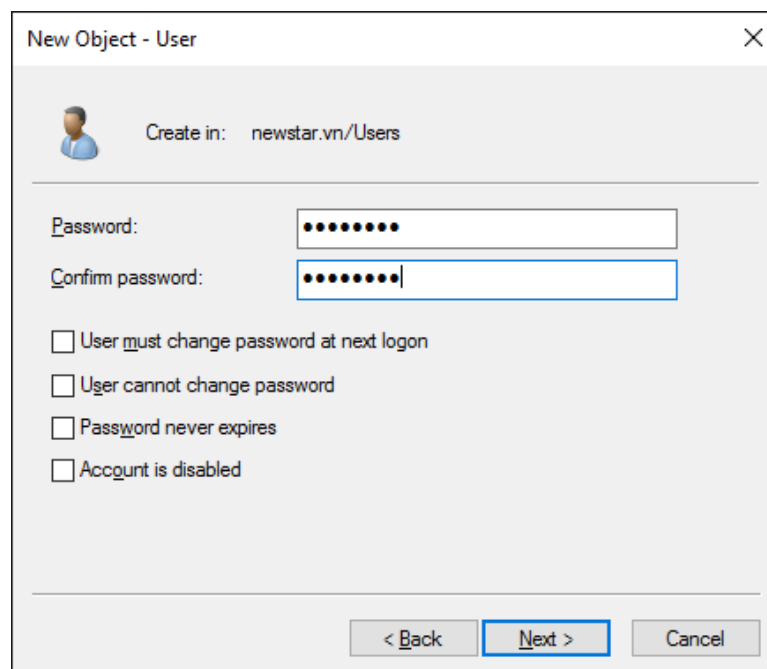*Hình 23-7: Domain con microsoft.newstar.vn*

Hình 23-8: Domain Controller Options

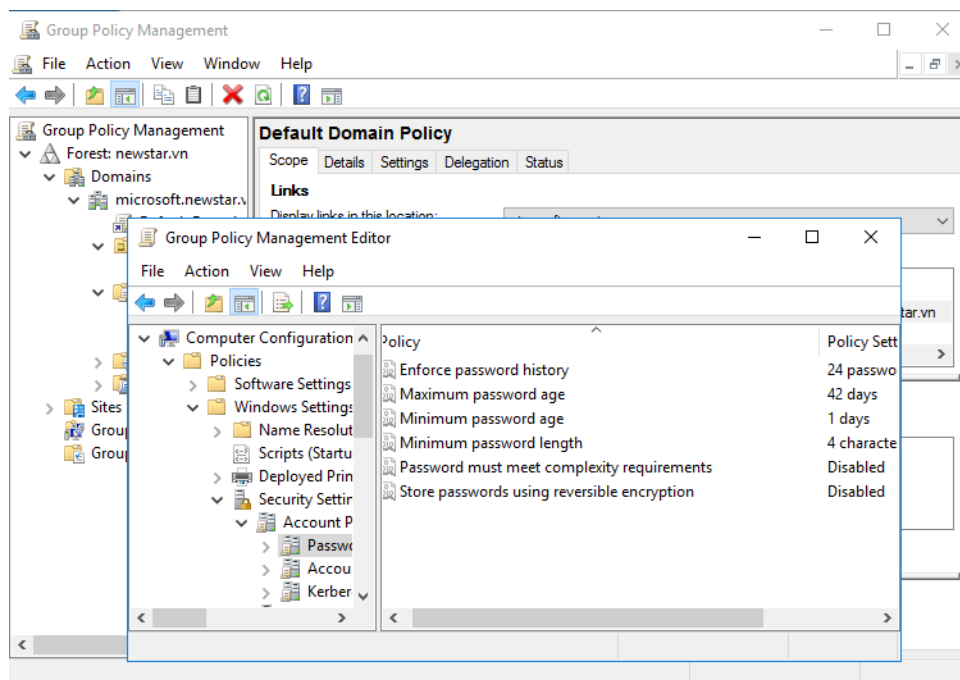*Hình 23-9: Đã cập nhật domain vào domain cha*
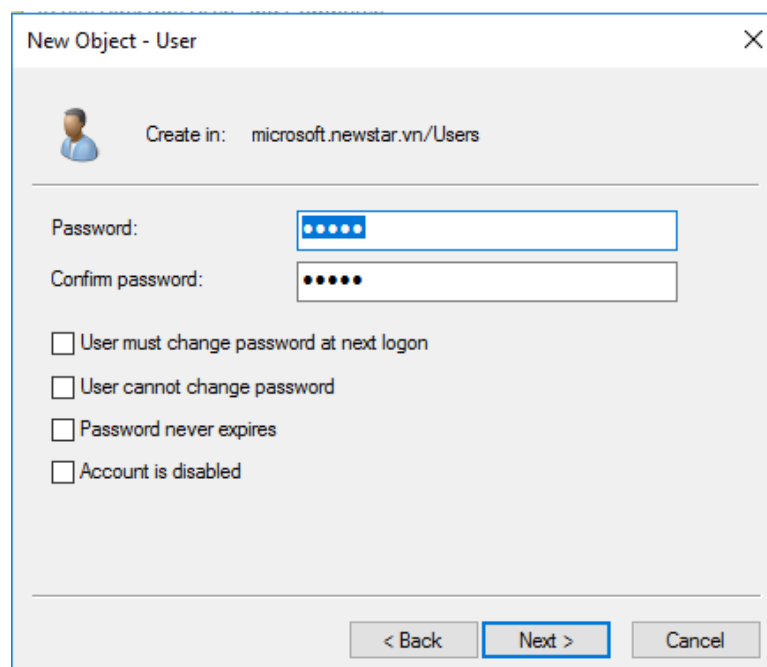

Hình 23-10: Dùng chính sách áp cho domain cha

Hình 23-11: Tạo user cho domain cha

Hình 23-12: Điều chỉnh chính sách domain con
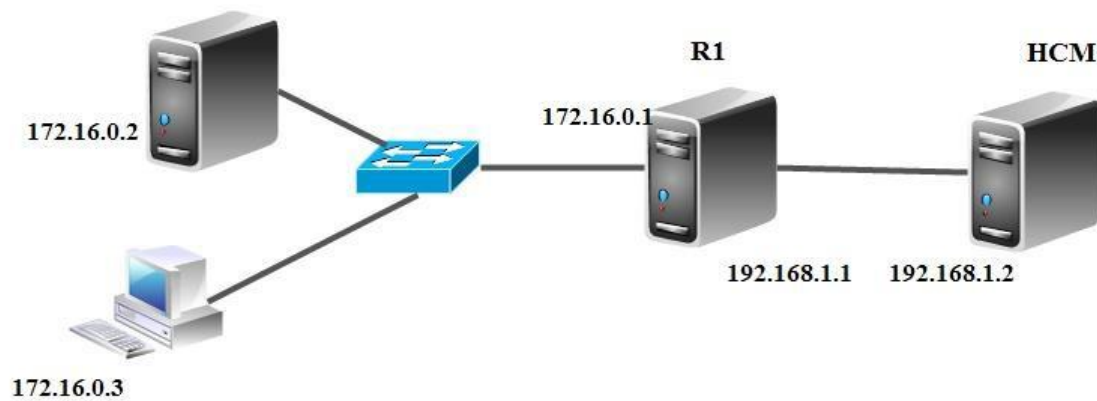
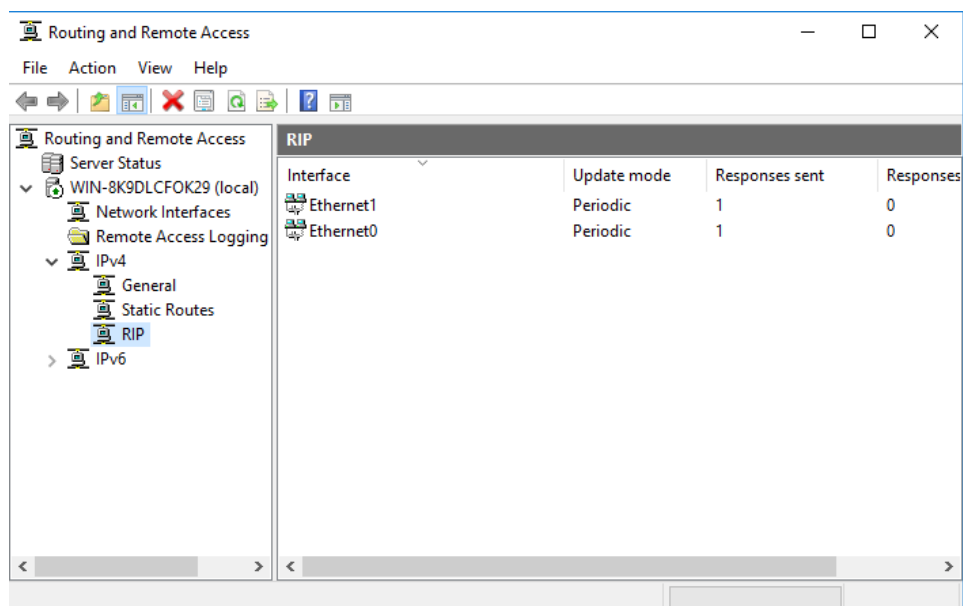*Hình 23-13: Tạo user với chính sách ở domain con*

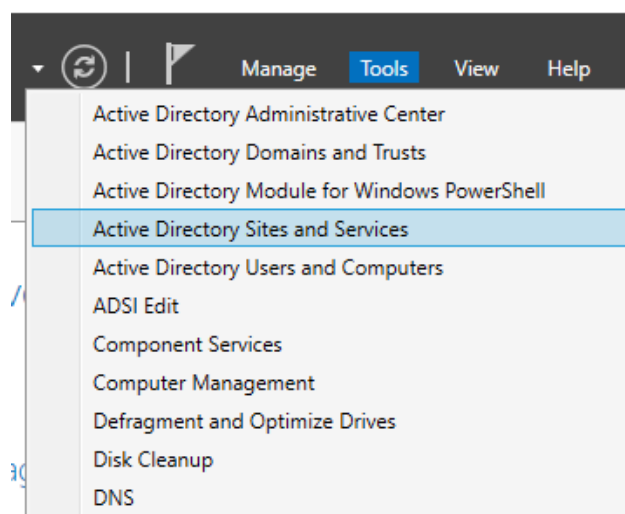# 9   Chia site domain

  □   Chuẩn bị:
      + Một máy windows server đã lên DC
      + Một máy windows server join Domain
      + Một máy windows 7
  □   Mô hình

Hanoi

  □   Kết quả đạt được
      □ Tạo U1 ở domain HCM sau đó ngắt kết nối ở router, u1 vẫn
         đăng nhập được ở site Hanoi
  □   Thực hiện
□ Thực hiện join domain cho R2
□ Thực hiện định tuyến giữa hai mạng
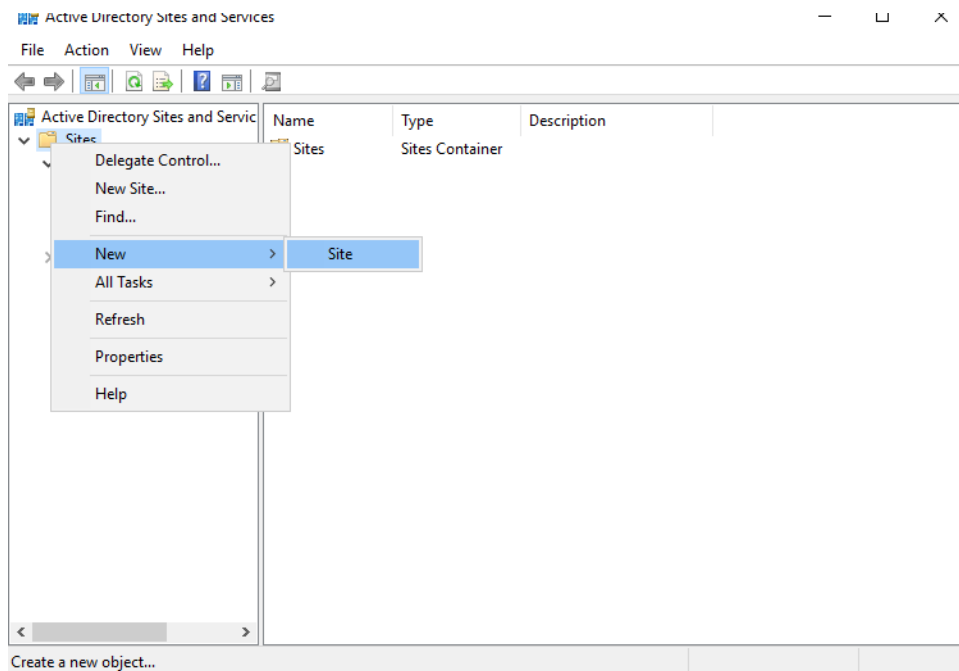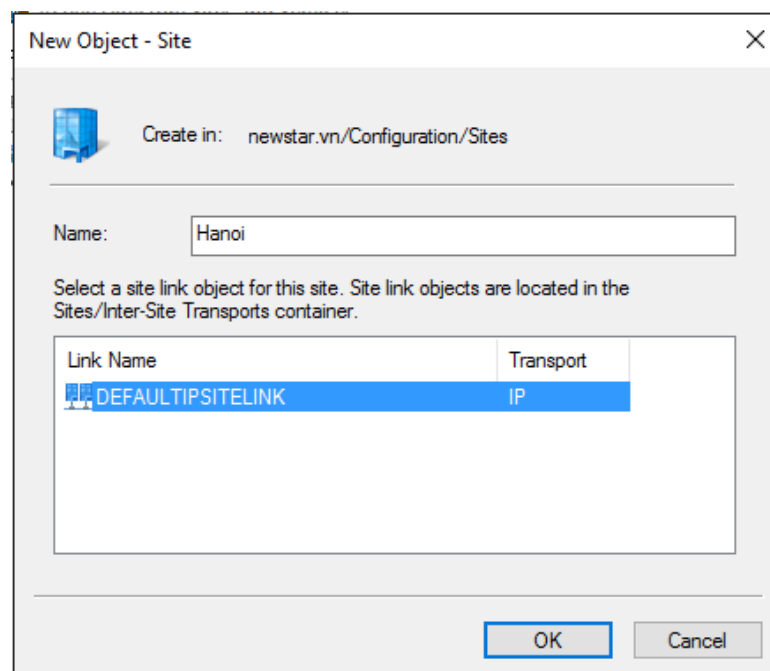
Hình 24-1: Card mạng tham gia định tuyến

Hình 24-2: Chọn ADSS

Hình 24-3: New □Site

Hình 24-4: Thêm site Hanoi

Hình 24-5: Site Hanoi được tạo
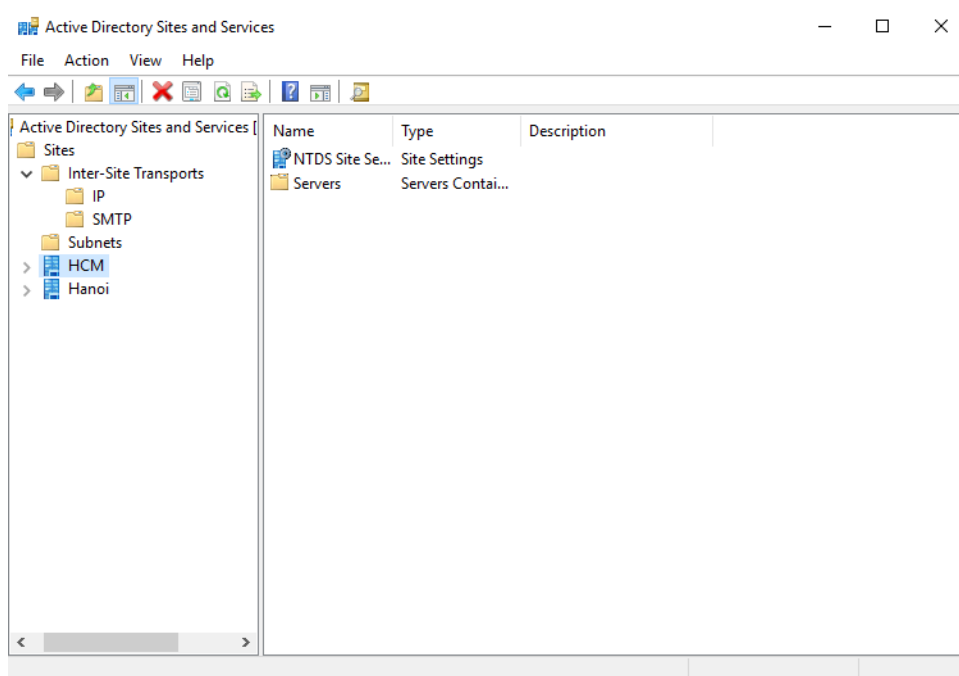
Hình 24-6: Chỉnh sửa file mặc định thành HCM
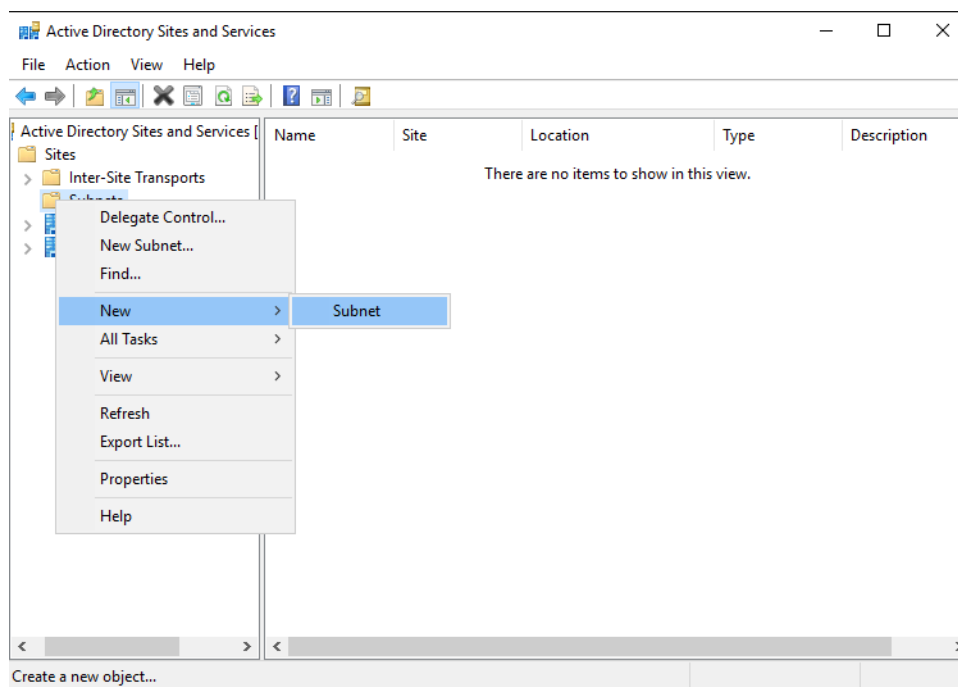
Hình 24-7: Thêm Subnet

Hình 24-8: Thêm network ở site Hanoi

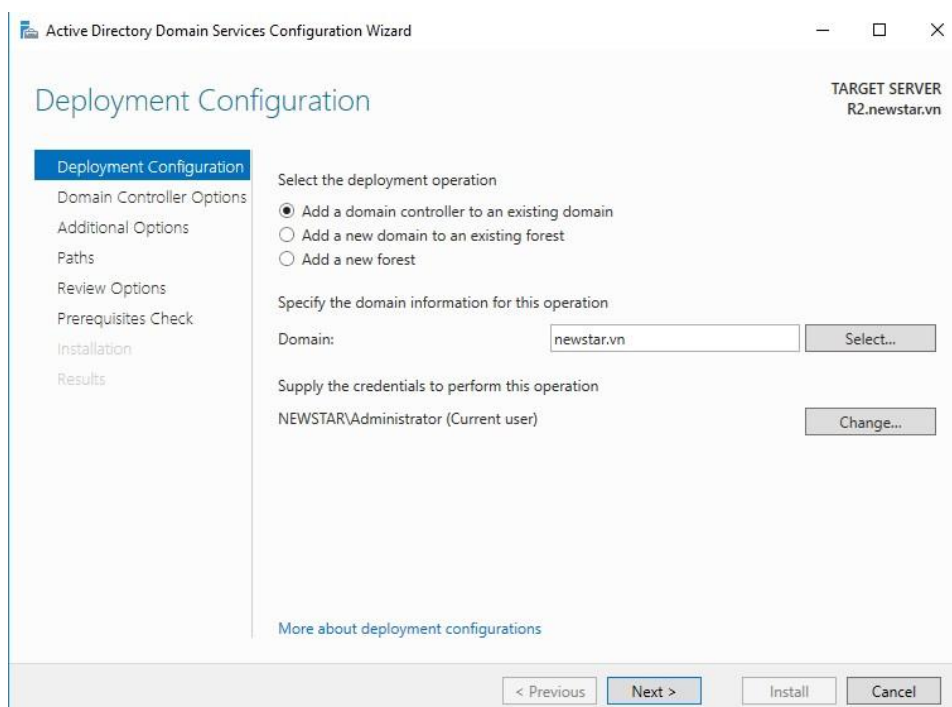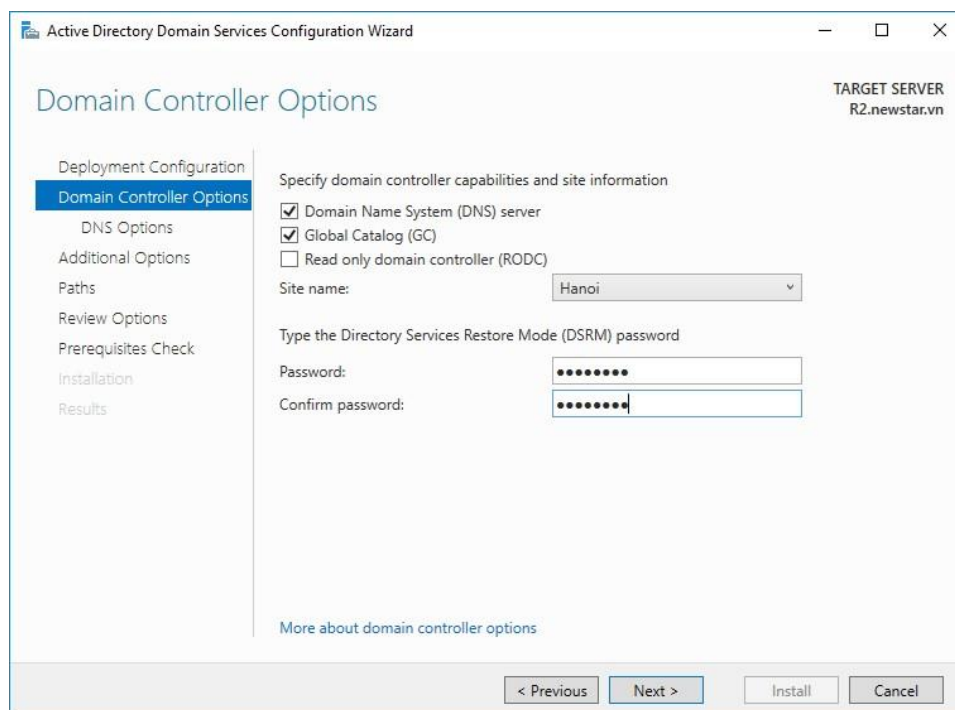*Hình 24-9: Thêm network ở site HCM*

☐ Tiến hành nâng cấp lên domain đồng cấp
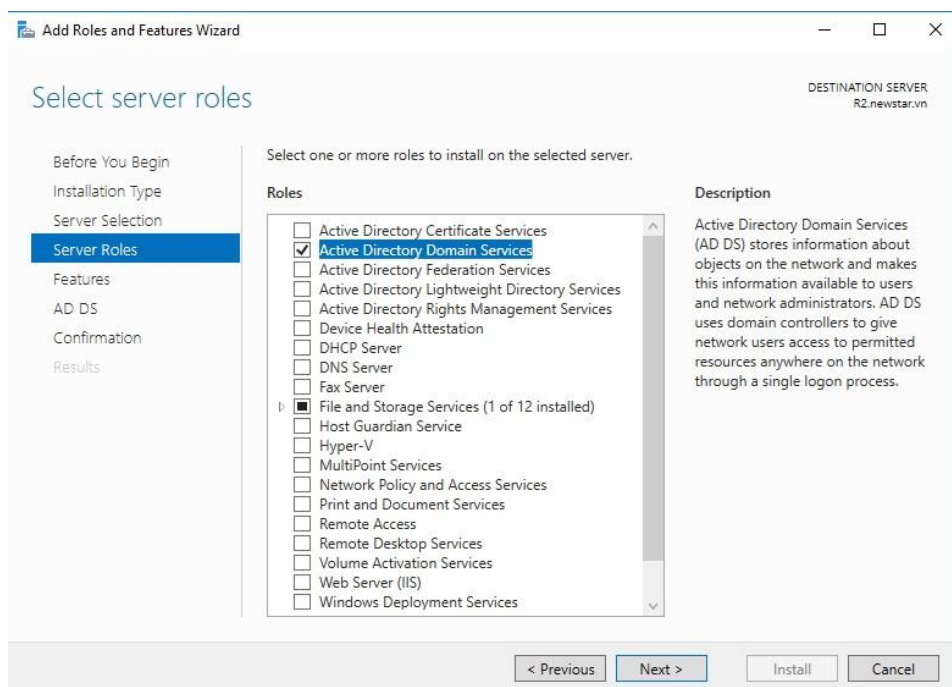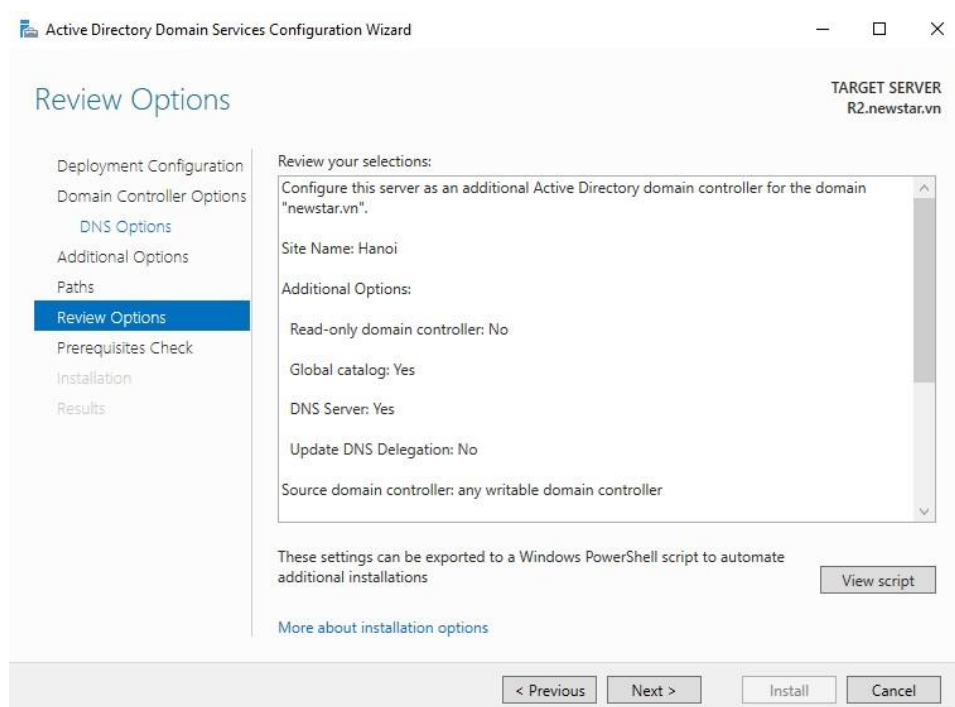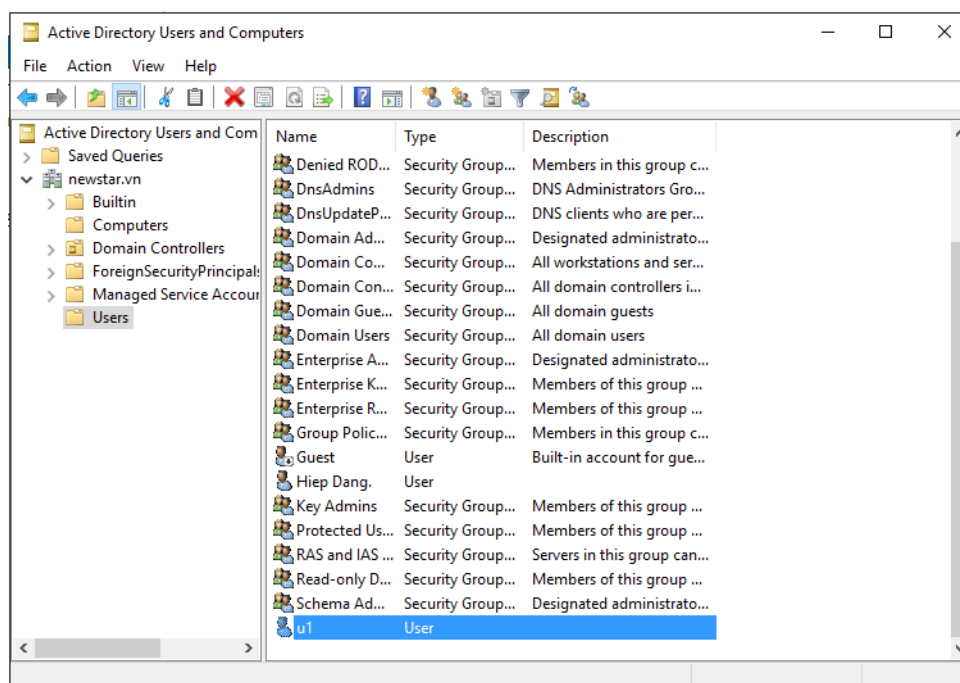
Hình 24-10: Cài ADDS

Hình 24-11: Chọn mục đầu tiên

Hình 24-12: Chọn vào site Hanoi

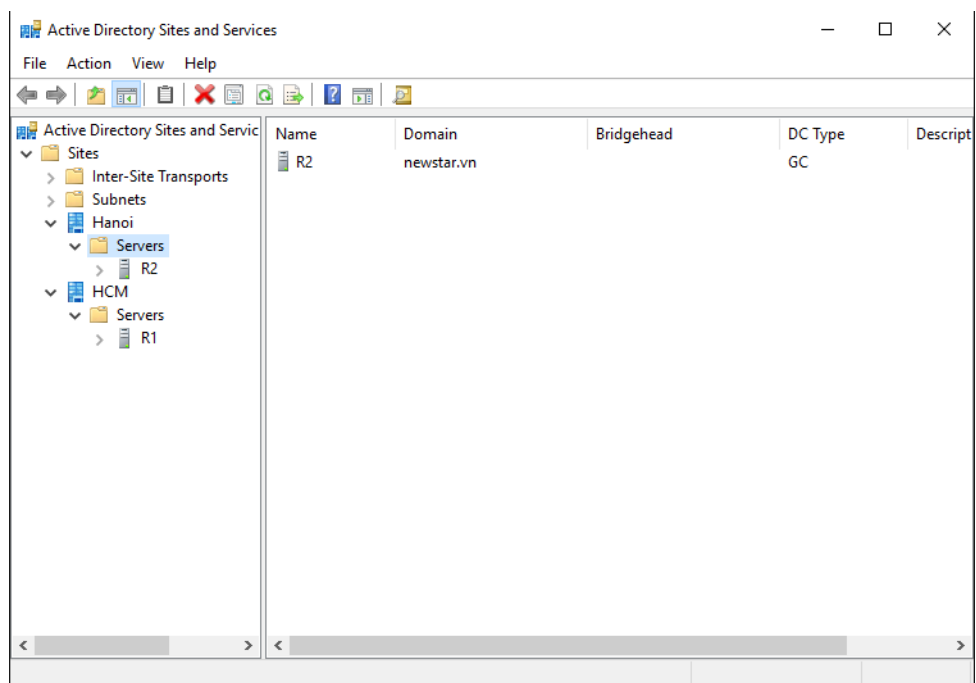*Hình 24-13: Thông tin cấu hình đã thiết lập*

Hình 24-14: Tạo user U1 trên R1

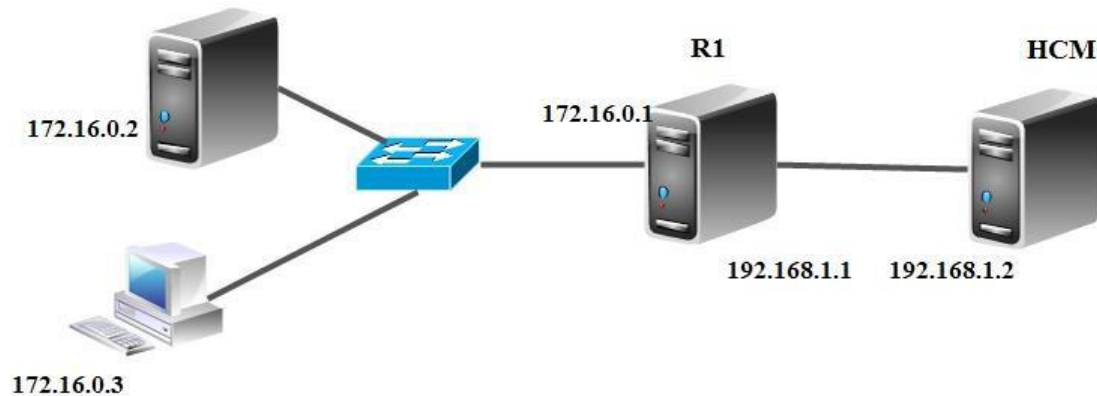*Hình 24-15: User U1 đăng nhập ở site Hanoi*

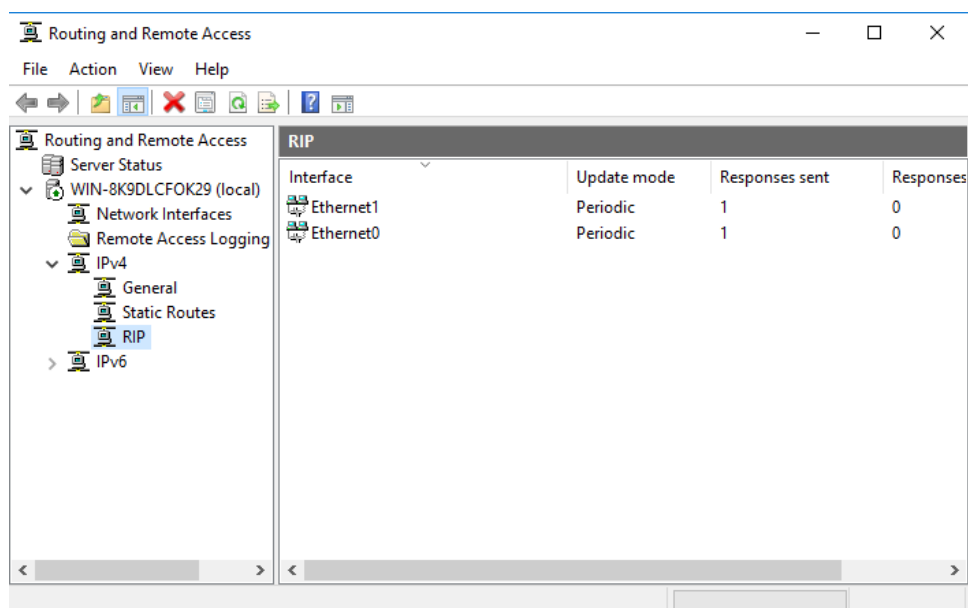*Hình 24-16: Site Hanoi có R2*

10   Read Only Domain

  □ Chuẩn bị:
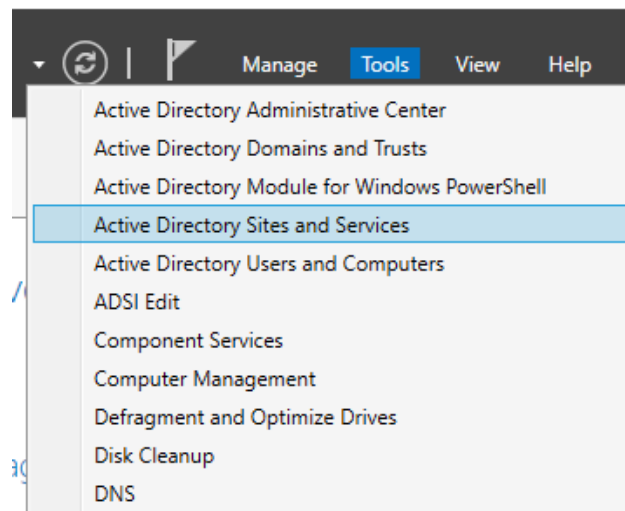 □ Một máy windows server đã lên DC
  □ Một máy windows server join Domain
  □ Mô hình

Hanoi

  □ Kết quả đạt được
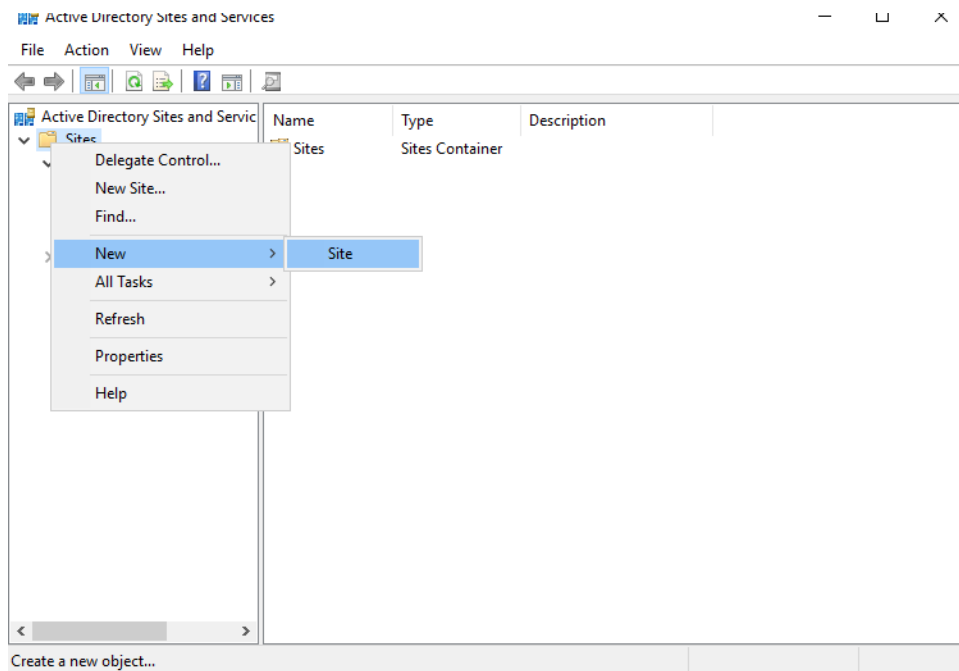 □ Tạo U1 ở domain HCM sau đó ngắt kết nối ở router, u1 vẫn
     đăng nhập được ở site Hanoi
  □ Thực hiện

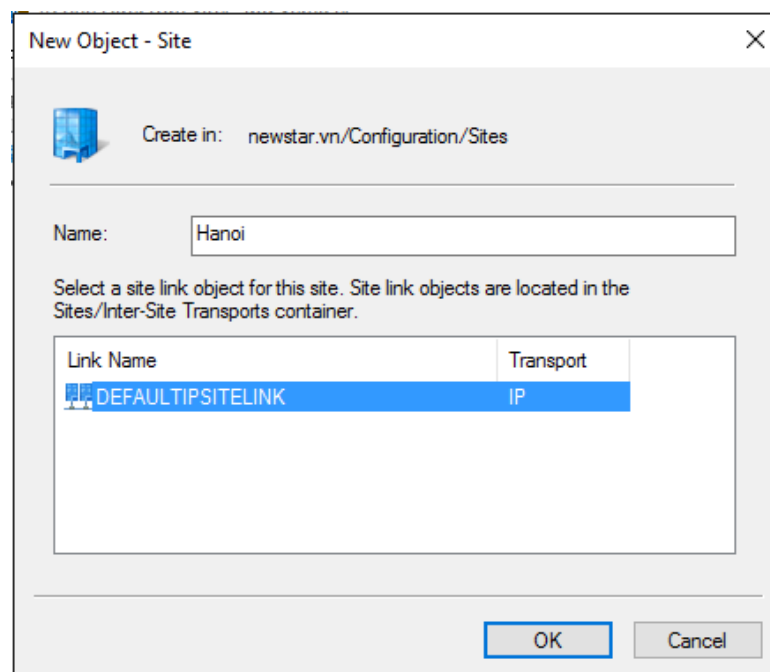*Hình 25-1: Card mạng tham gia định tuyến*

Hình 25-2: Chọn ADSS

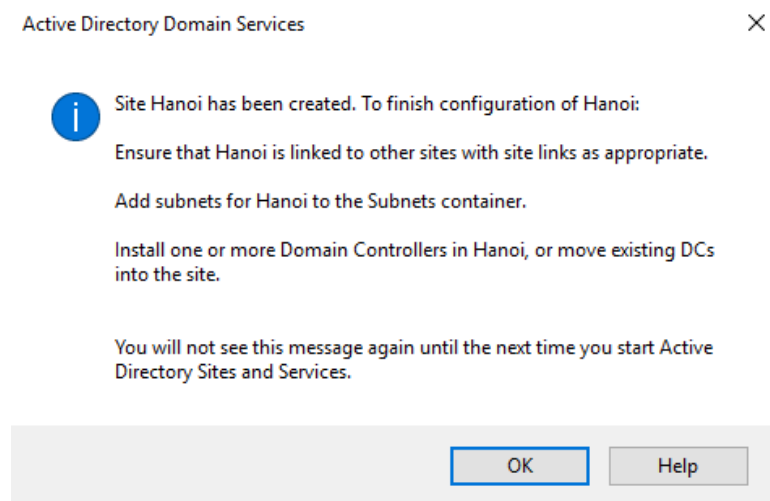*Hình 25-3: New □ Site*

Hình 25-4: Thêm site Hanoi

Hình 25-5: Site Hanoi được tạo
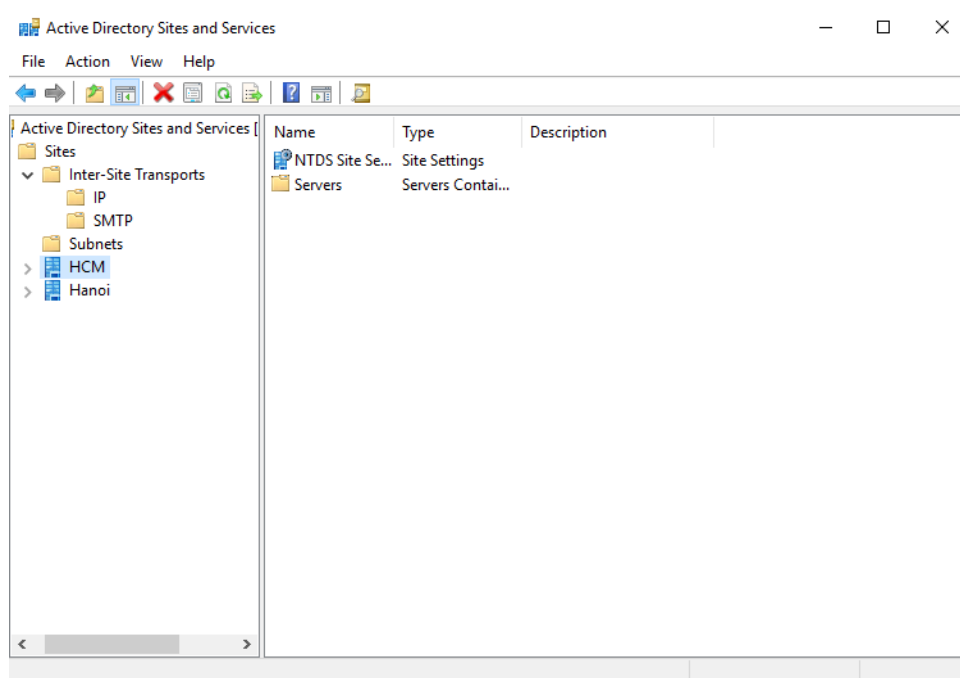
Hình 25-6: Chỉnh sửa file mặc định thành HCM
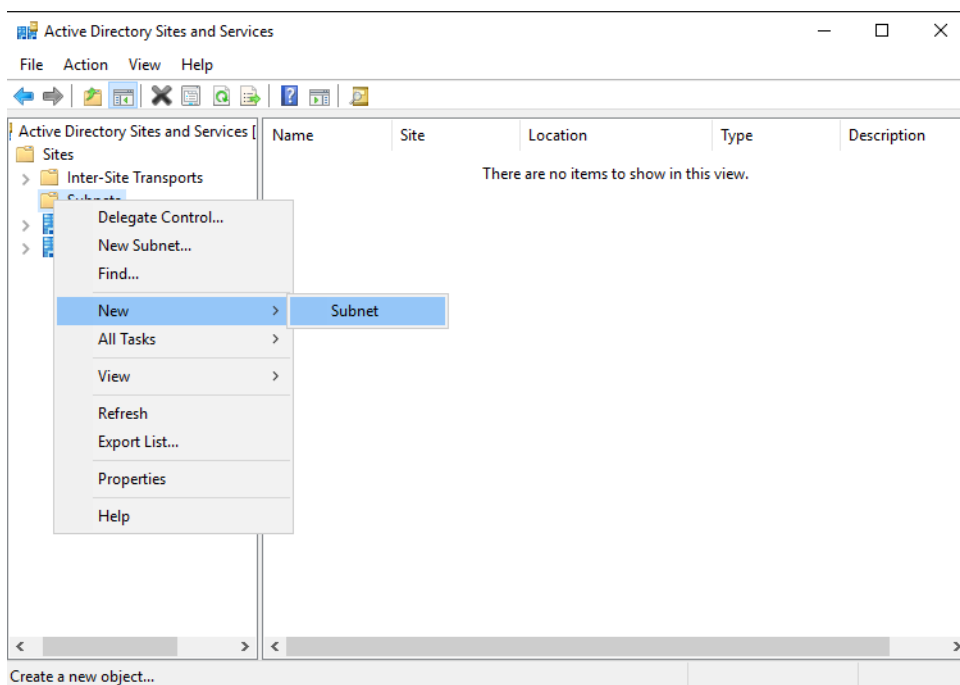
Hình 25-7: Thêm Subnet
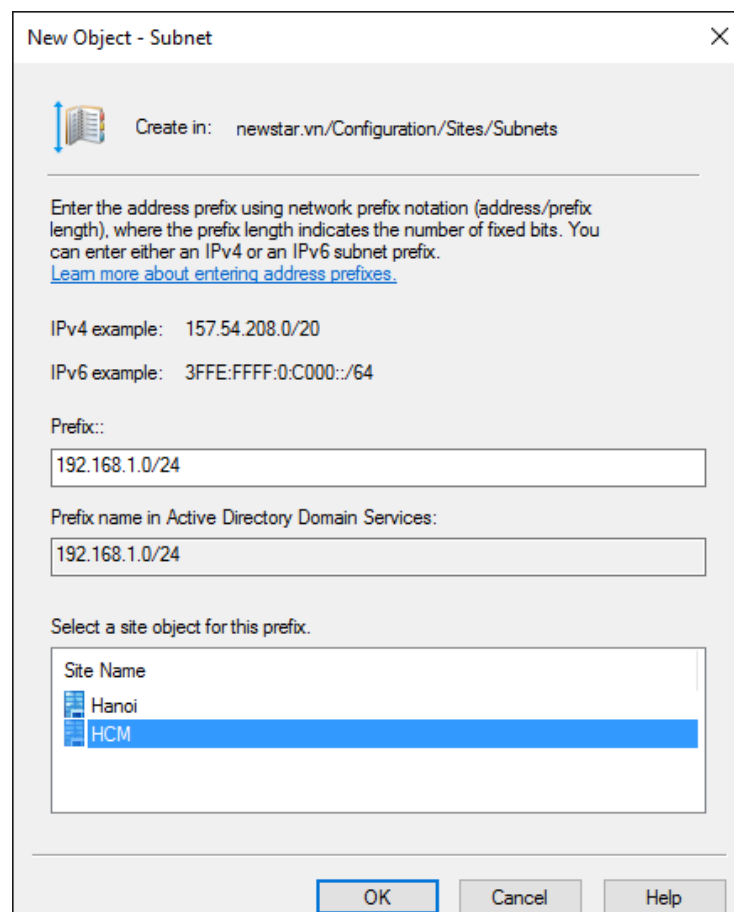
Hình 25-8: Thêm network ở site Hanoi

Hình 25-9: Thêm network ở site HCM

☐ Tiến hành nâng cấp lên domain RODC
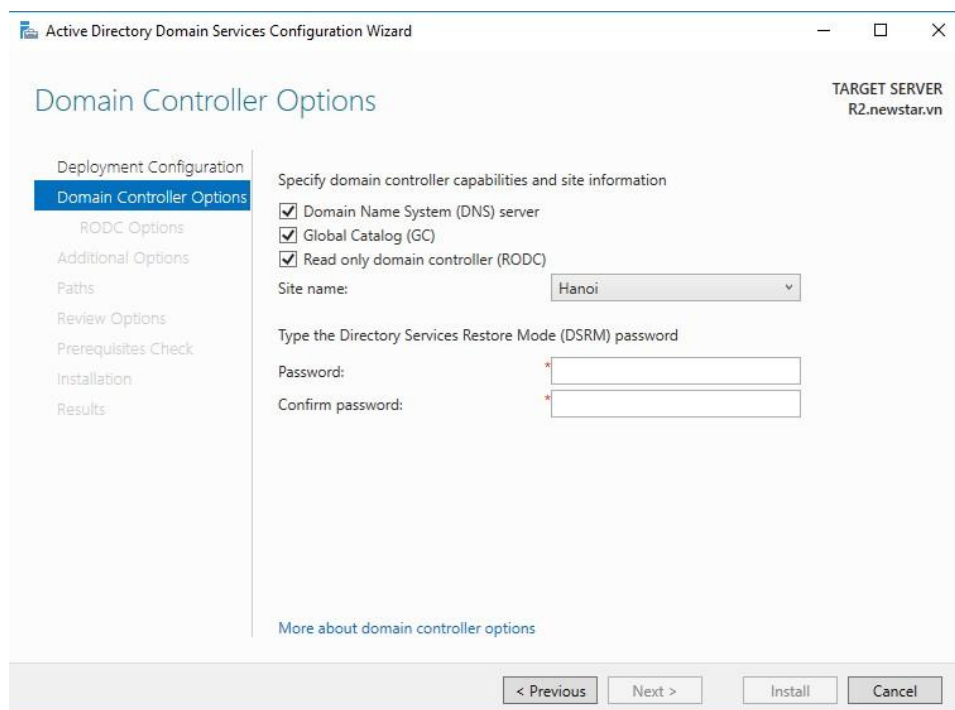
Hình 25-10: Chọn RODC
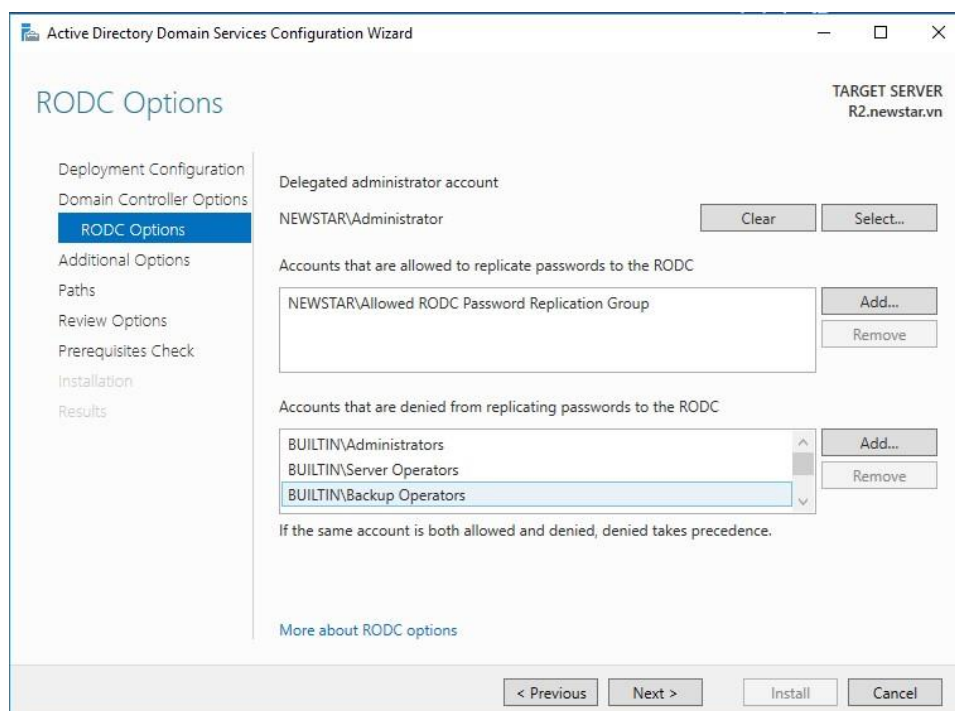
Hình 25-11: Thiết lập RODC
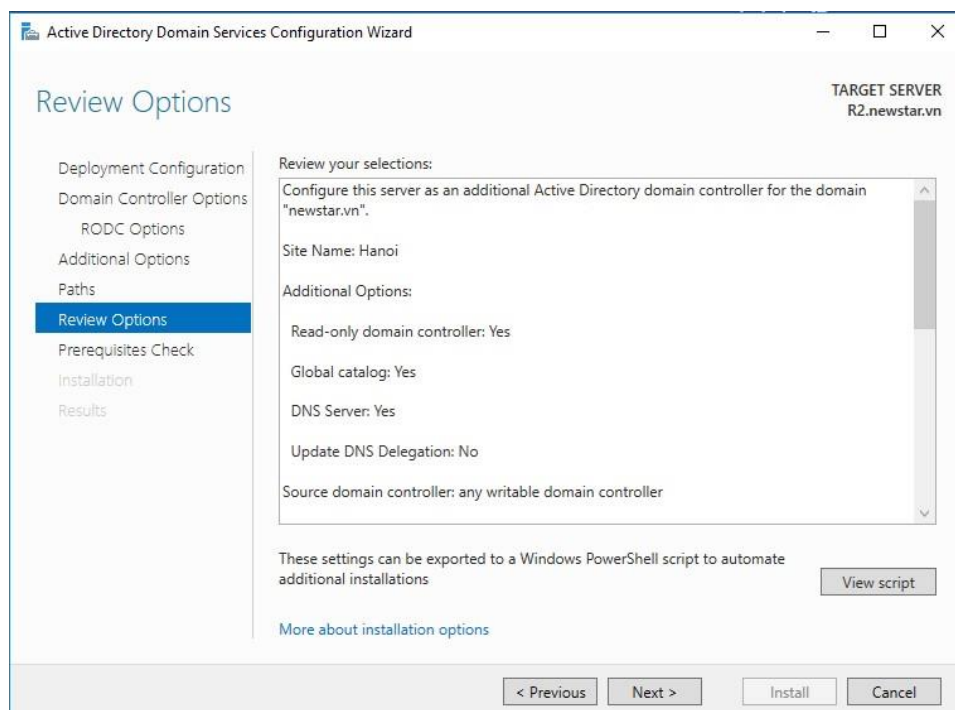
Hình 25-12: Thông số cấu hình RODC
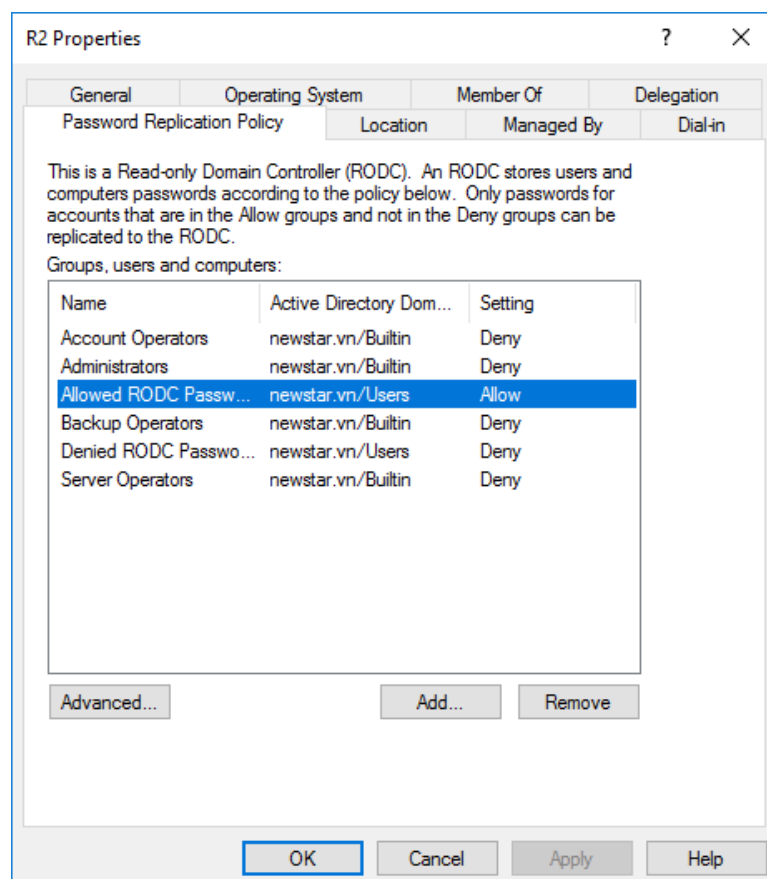
Hình 25-13: Thêm Group
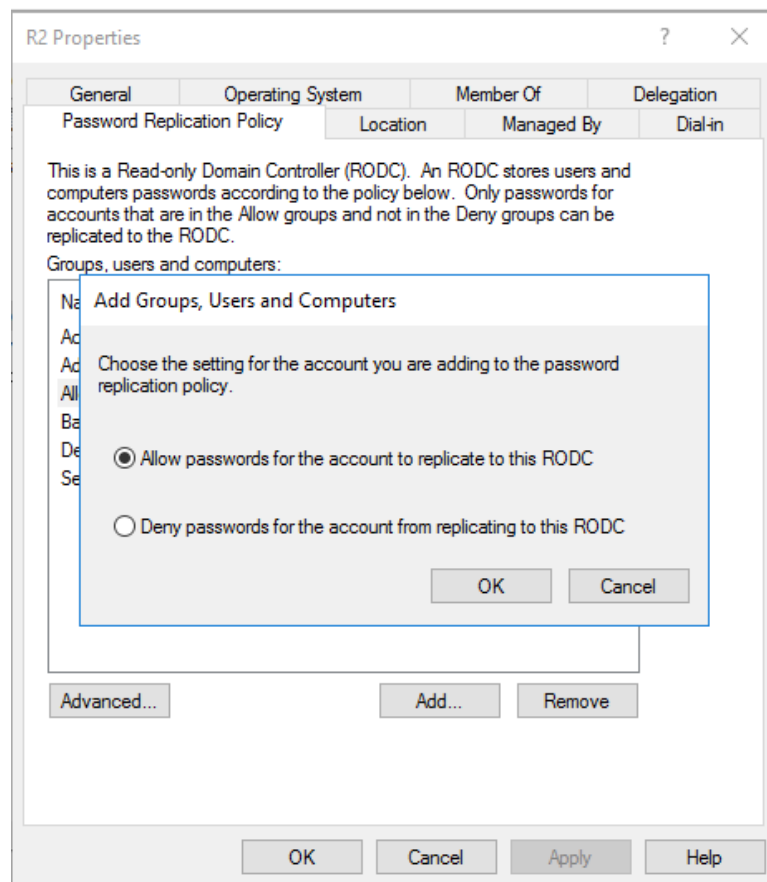
Hình 25-14: Tài khoản quản lý RODC
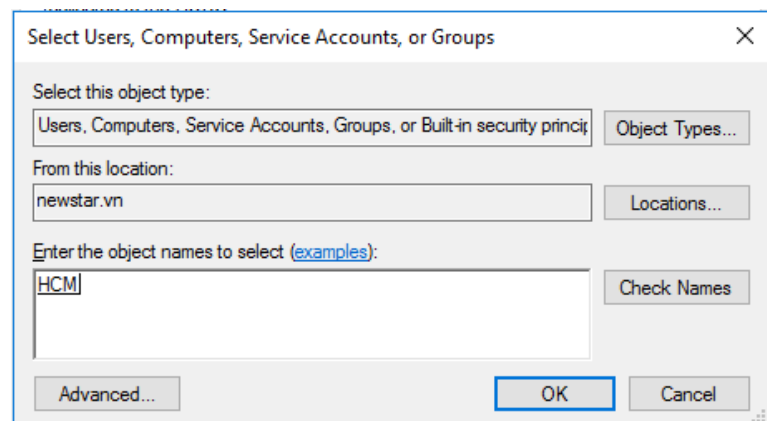
Hình 25-15: Chọn Group
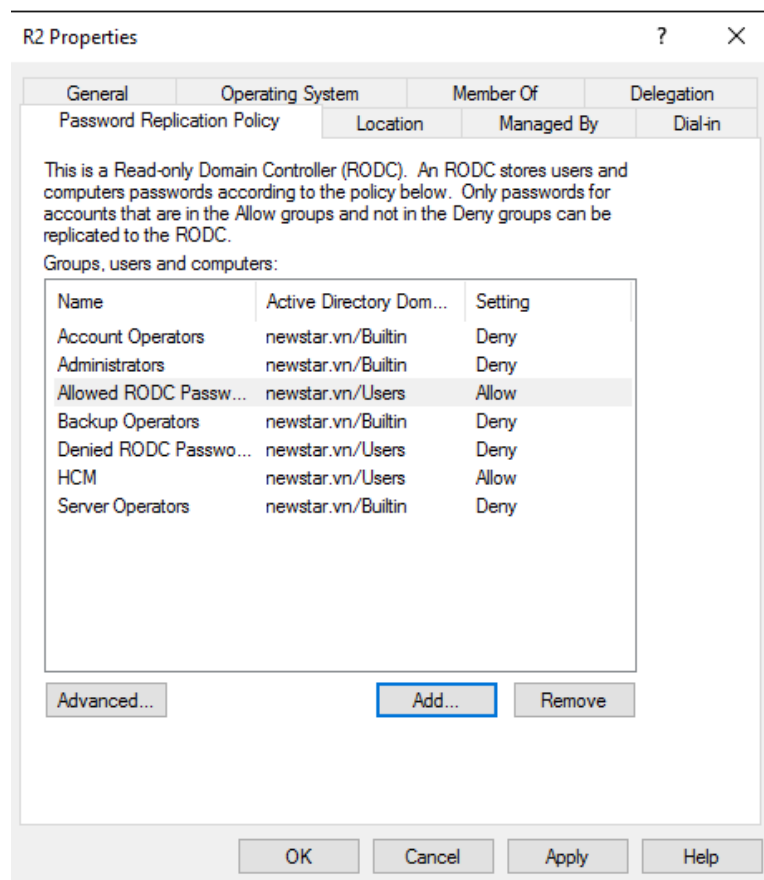
Hình 25-16: Tài khoản đã được thêm

11   Trust domain

Sau khi học bài này xong sinh viên có khả năng xây dựng hệ thống quản lý domain của 2 domain khác nhau

☐ Chuẩn bị:

+ Một máy server chưa cài hệ điều hành

+ Một file iso server 2016

☐ Mô hình
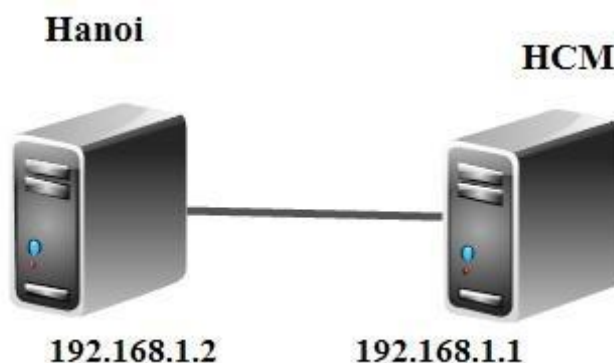
☐ Kết quả đạt được

☐ Tạo tài khoản u1 ở domain newstar sang domain test đăng nhập thành công

☐ Share folder ở domain newstar sang domain test truy cập thành công

Thực hiện

☐ Để thự hiện bài này phải tạo hai domain với tên khác nhau. DNS của 2 domain được forward hai lại với nhau
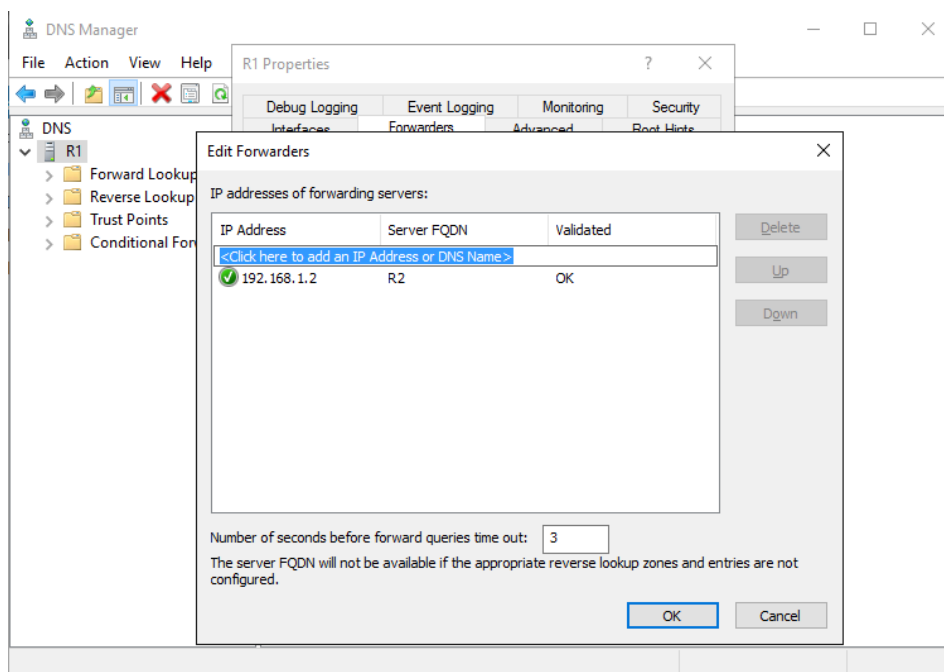
Hình 26-1: Forward DNS ở R1
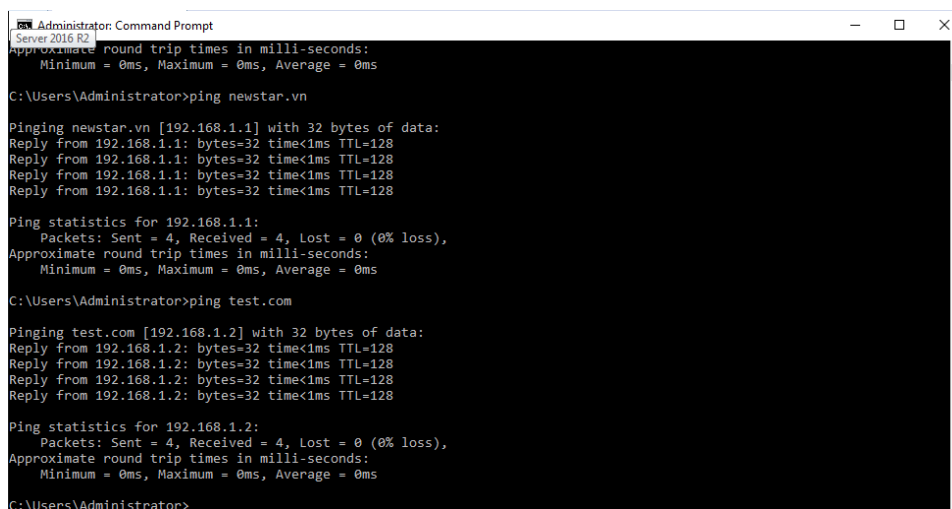
Hình 26-2: kiểm tra kết nối bằng tên
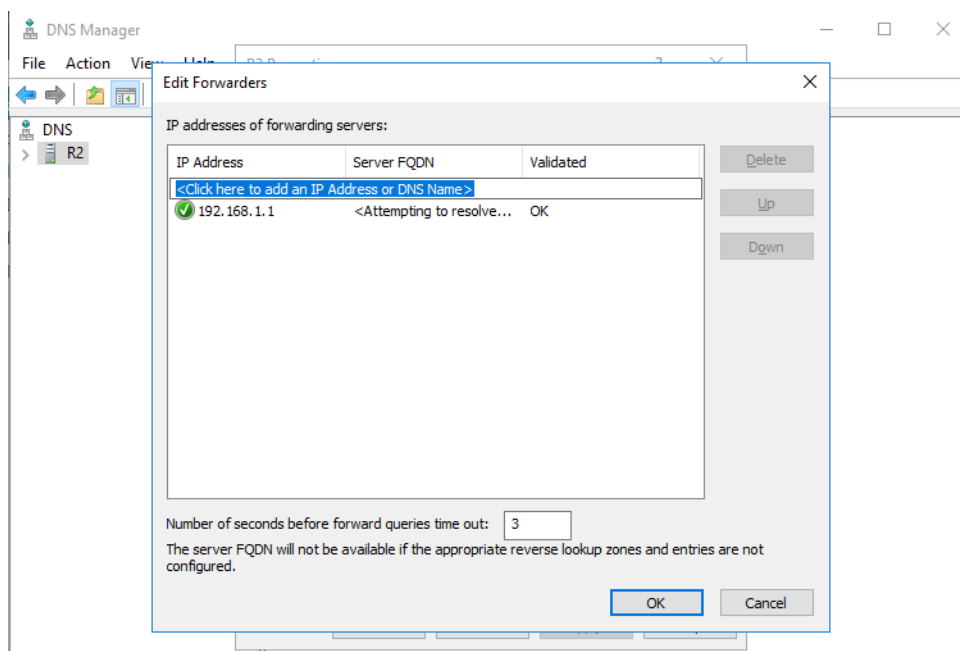
Hình 26-3: Forword DNS ở R2
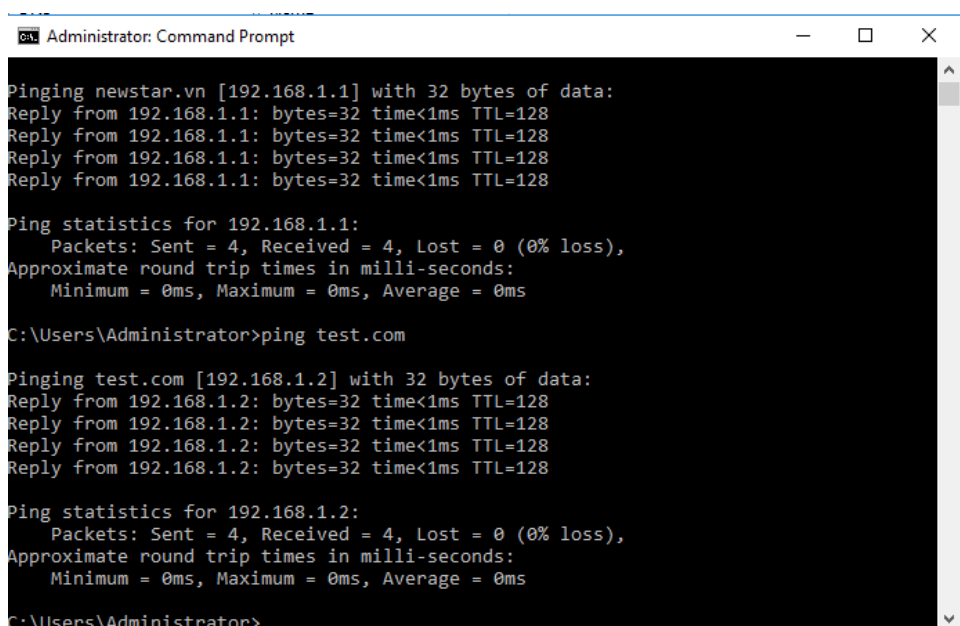
Hình 26-4: Kiểm tra kết nối bằng tên
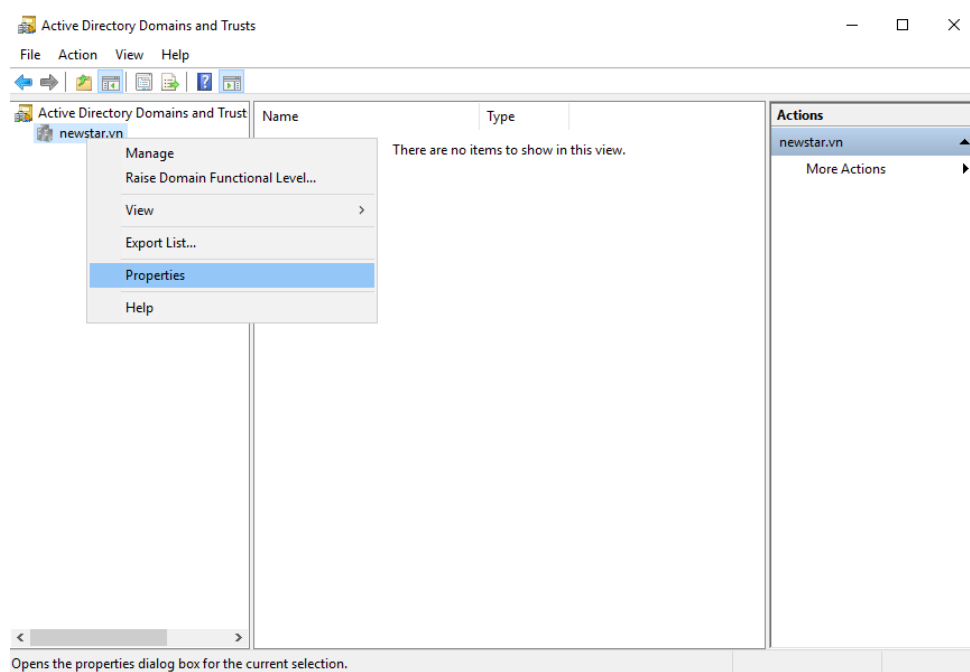
Hình 26-5: Chọn ADDT
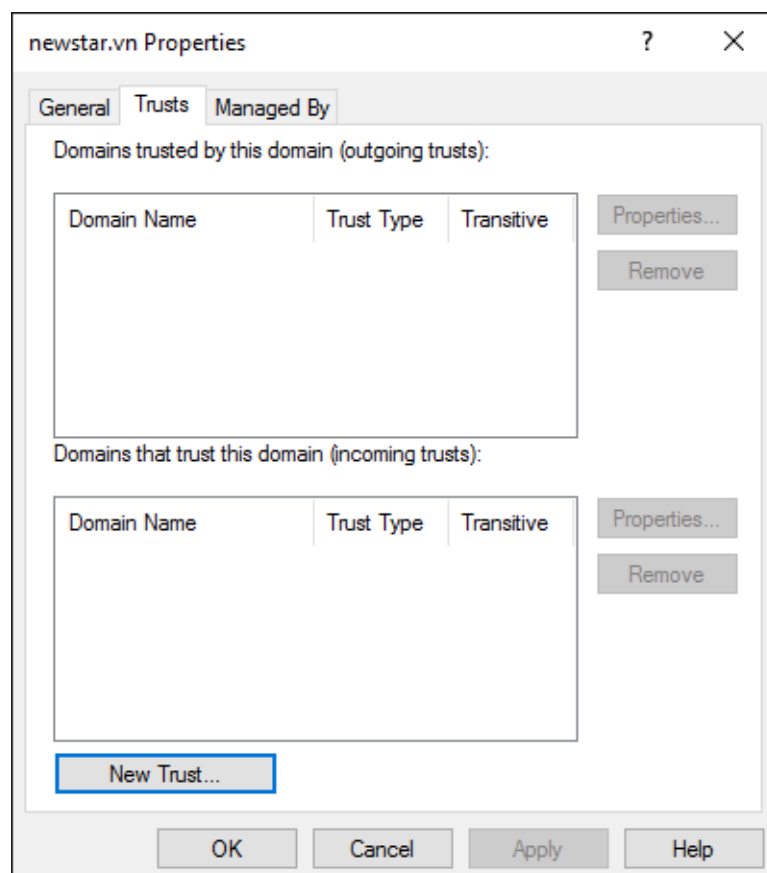
Hình 26-6: Properties newstar

Hình 26-7: Màn hình chào
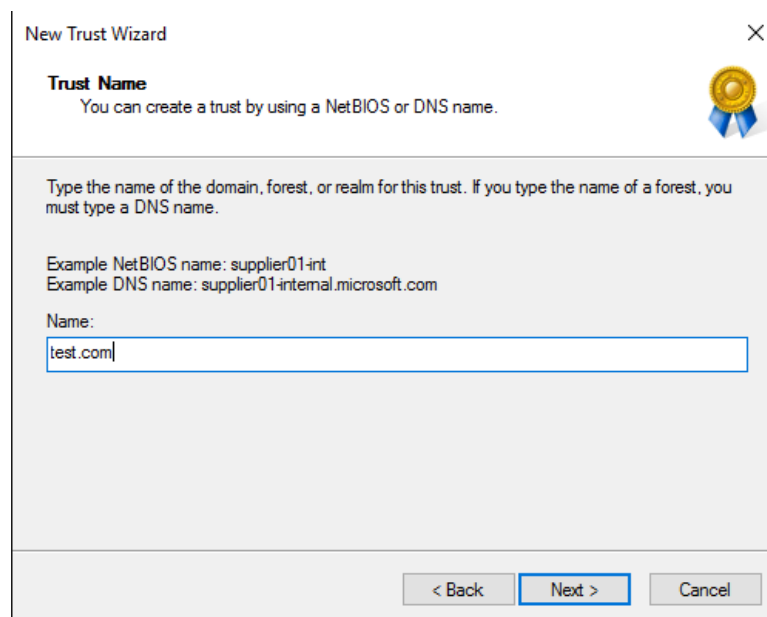
Hình 26-8: Nhập test.com
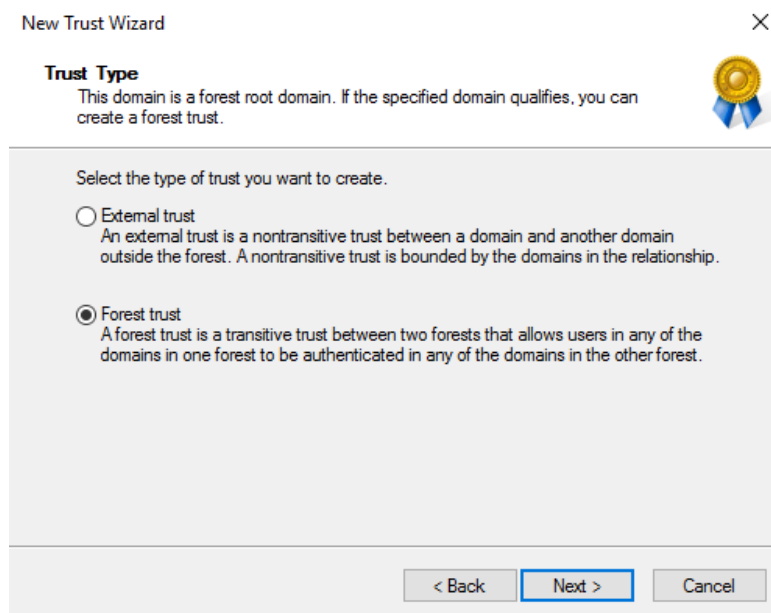
Hình 26-9: Forest trust
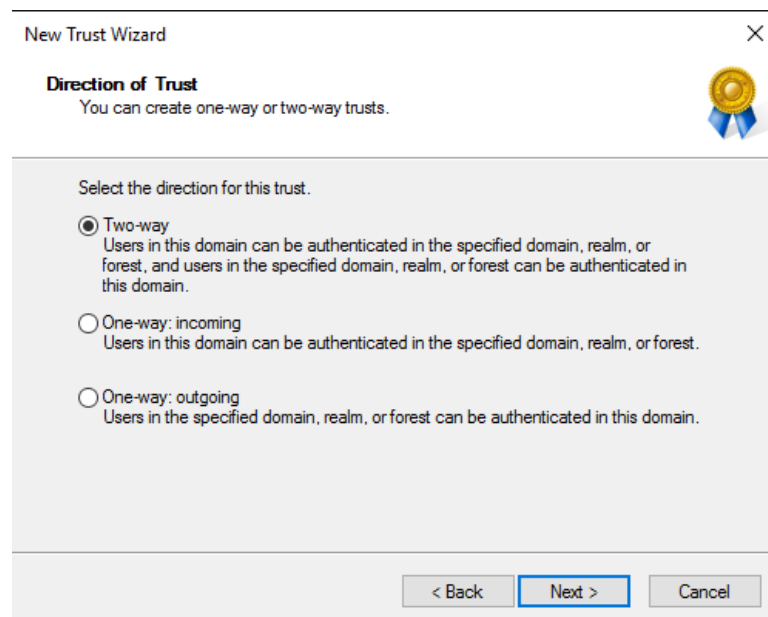
Hình 26-10: Two-way
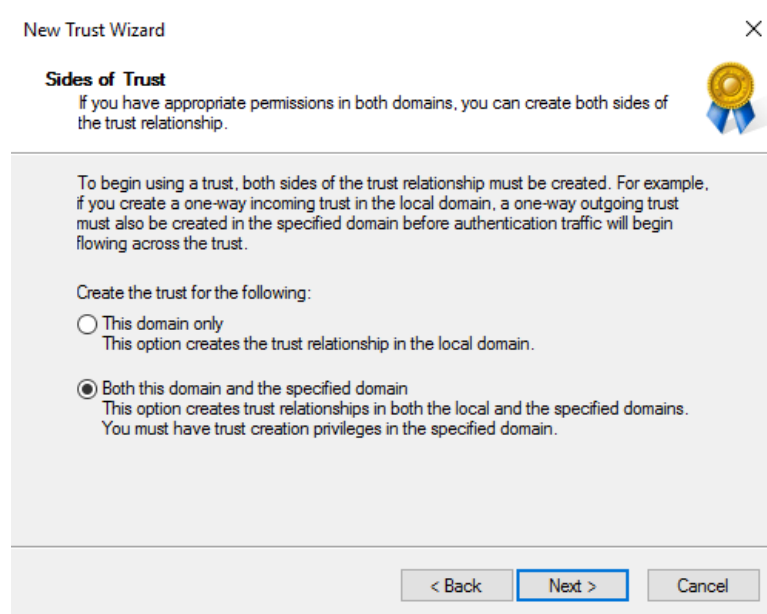
Hình 26-11: Both this domain
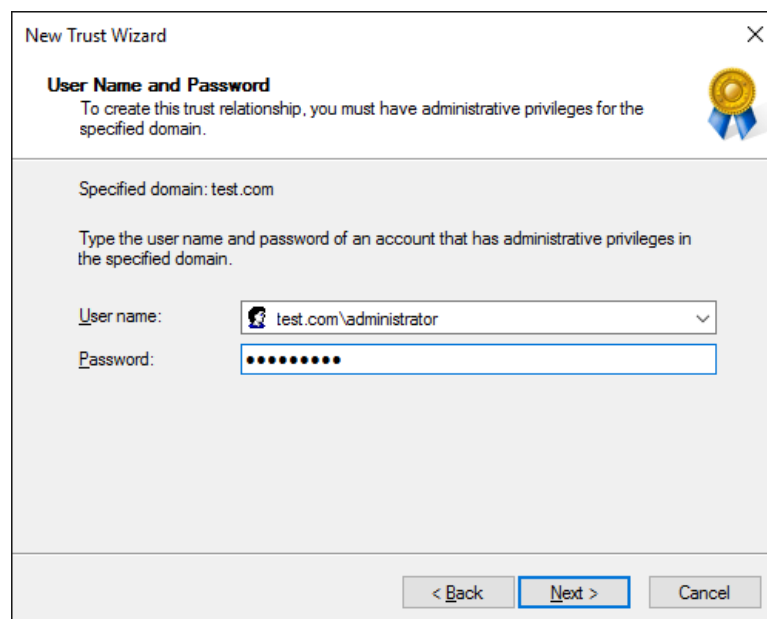
Hình 26-12: Nhập tài khoản của domain test
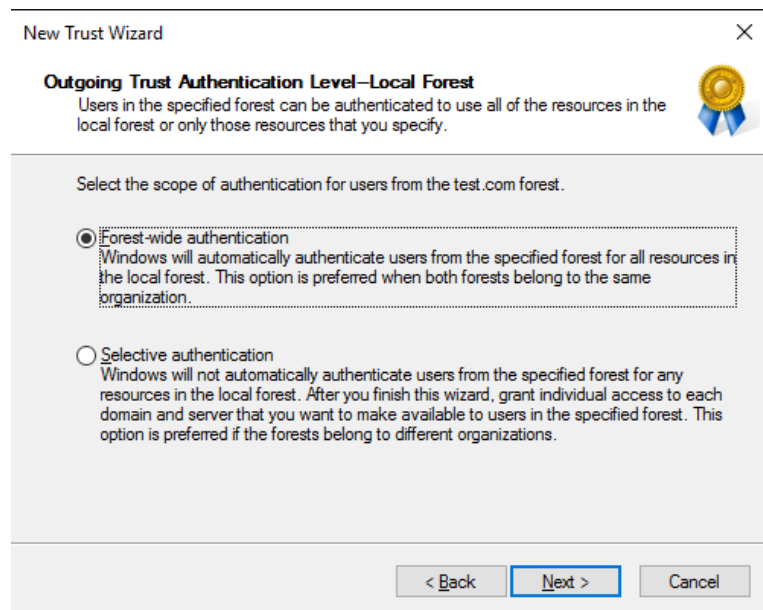
Hình 26-13: Chọn chứng thực chiều in
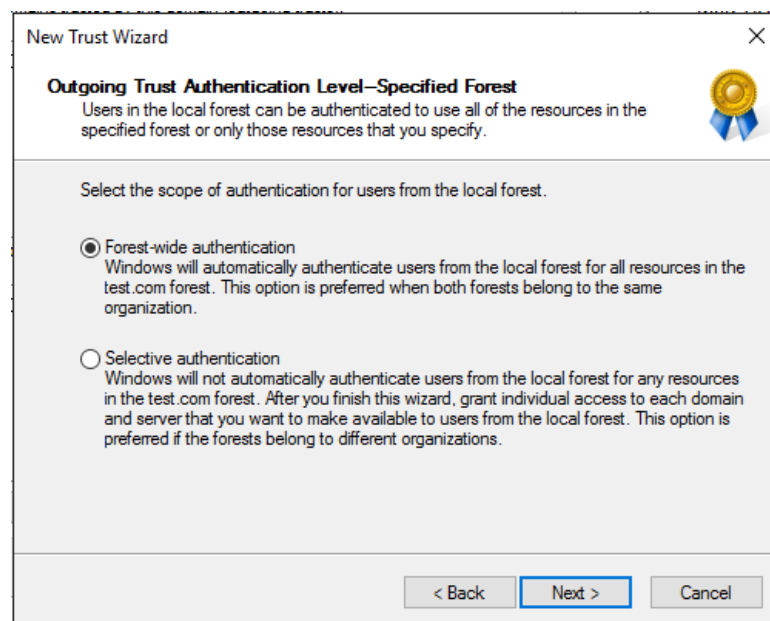
Hình 26-14: Chọn chứng thực chiều out
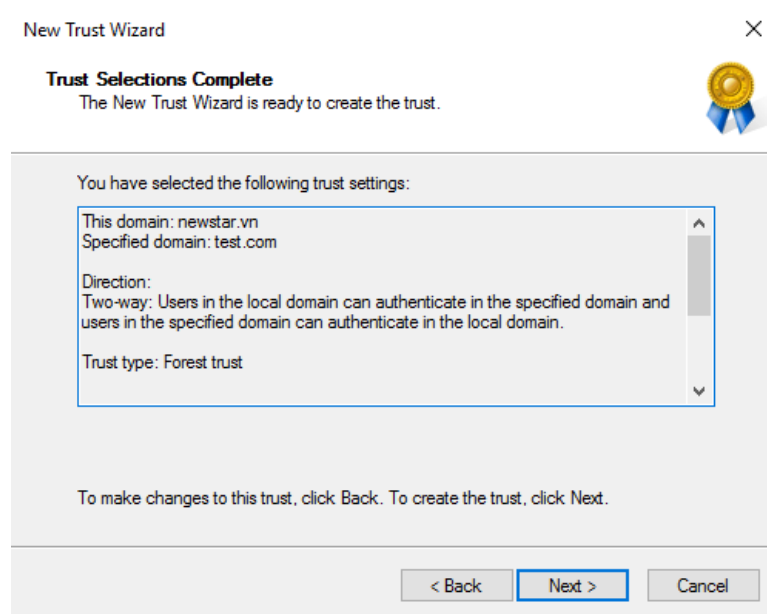
Hình 26-15: Quá trình thiết lập thành công
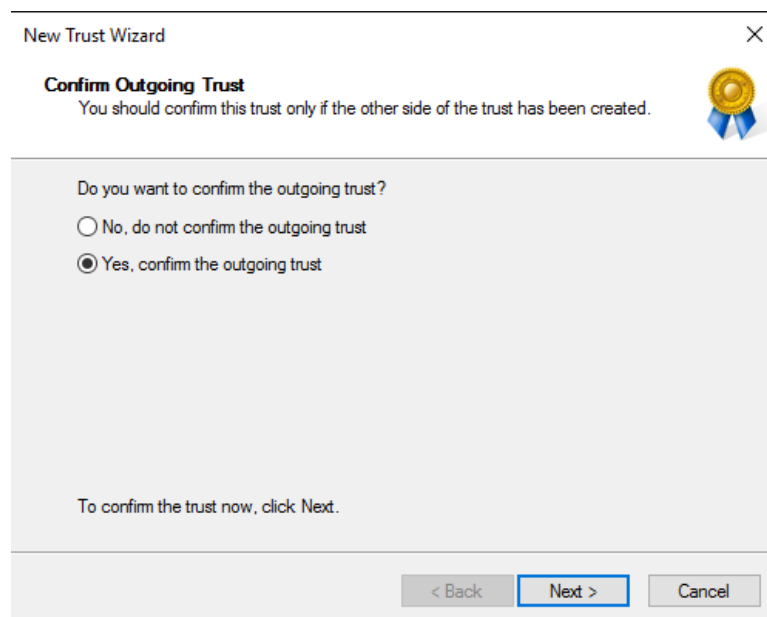
Hình 26-16: Thiết lập chiều out thành công
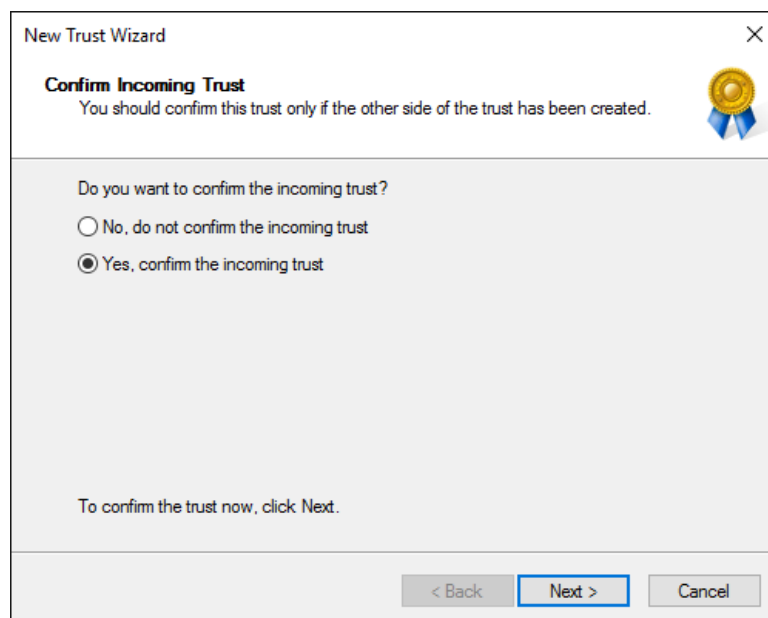
Hình 26-17: Thiết lập chiều in thành công

Hình 26-18: Thiết lập thành công
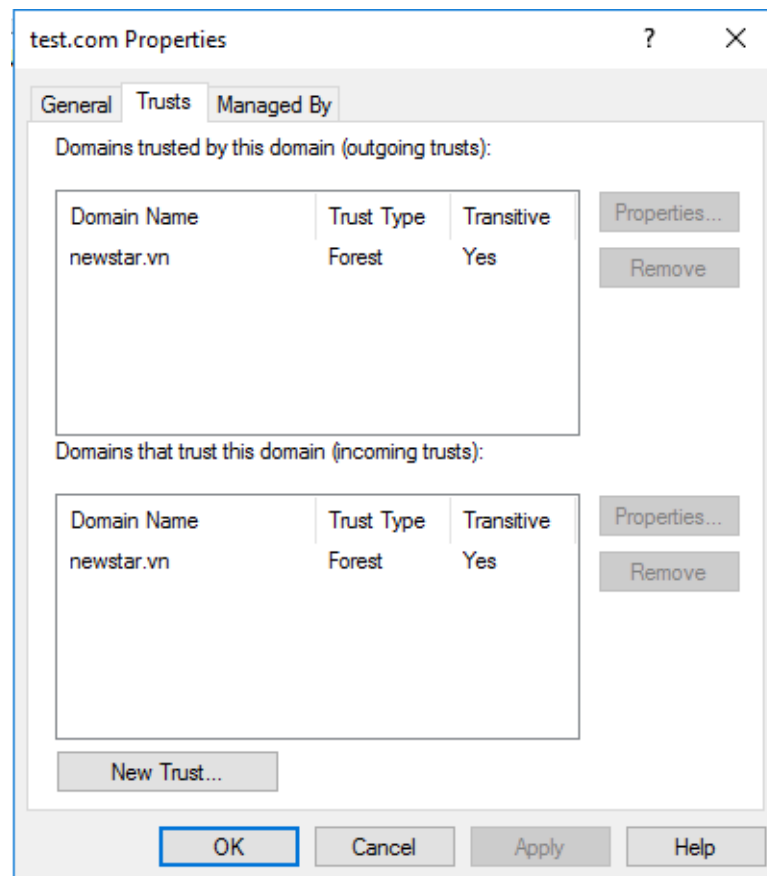
Hình 26-19: Trust thành công
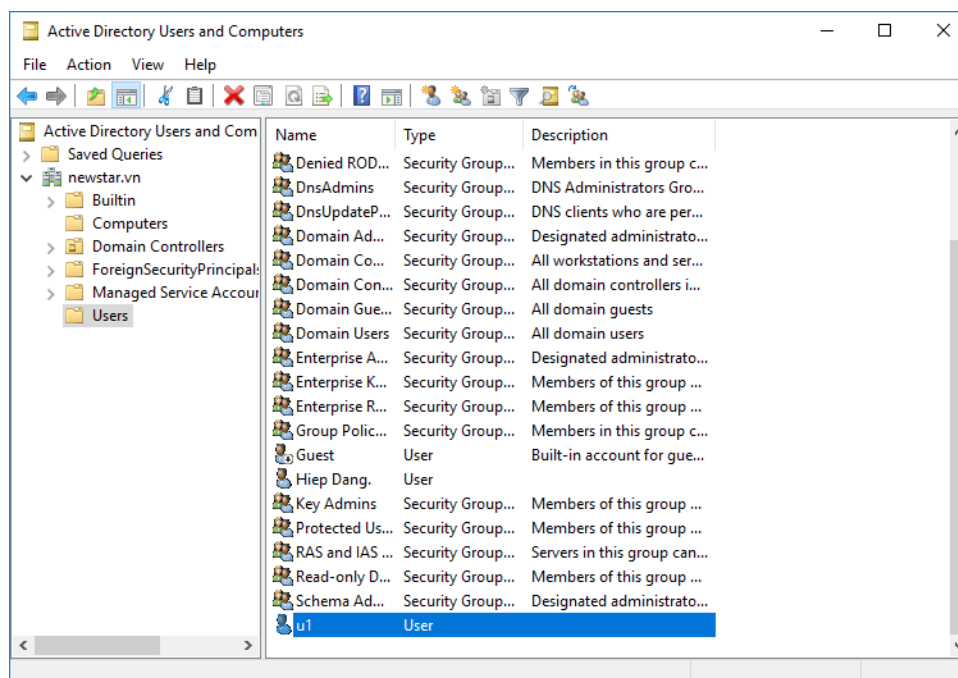
Hình 26-20: Tạo user U1 ở domain newstar

Hình 26-21: Đăng nhập U1 ở domain test

☐ Tạo folder Data trên domain newstar. Sau đó cho User U2 ở domain test truy
cập
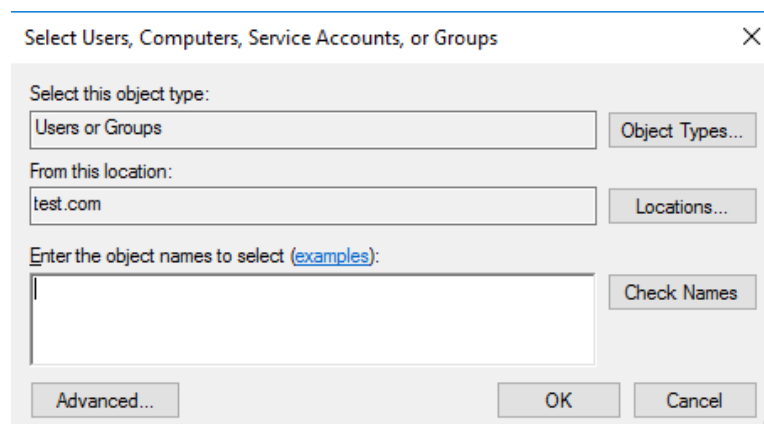
Hình 26-22: Chọn tài khoản domain test để truy cập vào tài folder
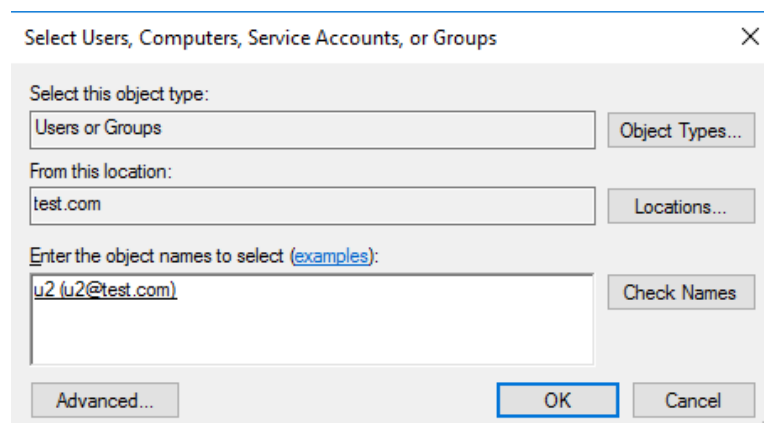
Hình 26-23: Chọn tài khoản U2 trên domain test
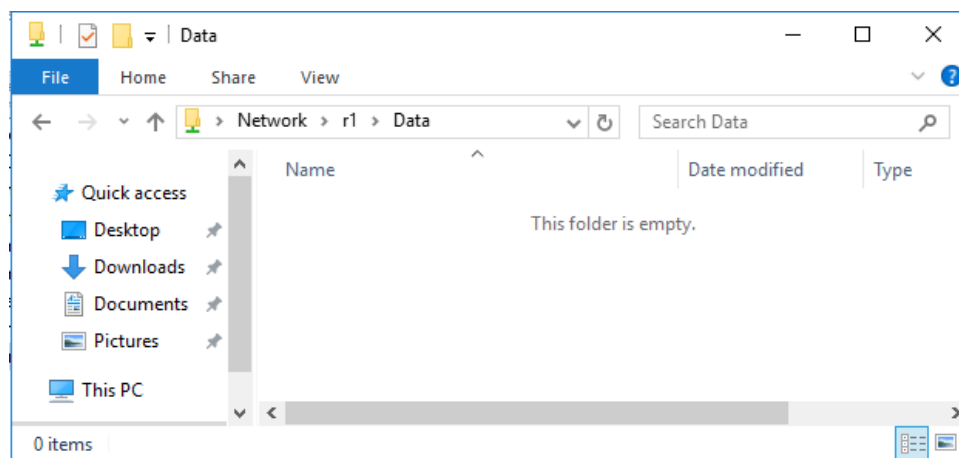
Hình 26-24: U2 truy cập vào folder Data

12. Windows server backup

Khi làm công tác quản trị mạng vấn đề an toàn dữ liệu luôn được chúng ta chú trọng với các công việc đảm bảo cho chúng luôn ở mức độ an toàn cao. Không may một ngày nào đó cả hệ thống bị nhiễm virus trầm trọng, phòng chứa server rủi ro xảy ra hoả hoạn… những gì còn lại bây giờ là một hệ thống với dữ liệu bị tàn phá nặng nề hoặc mọi thứ đã biến thành tro khi cháy nổ xảy ra.Chính vì thế Windows khuyến cáo bạn nên sao lưu dự phòng dữ liệu sang một nơi khác vị trí địa lý với nơi đặt server và nếu tốt hơn là sao lưu dự phòng với tần suất mỗi ngày một lần là tốt hơn cả.

Nhưng hãy tượng tượng xem không lẽ mỗi ngày ta phải sao lưu cả hệ thống hàng chục thậm chí hàng trăm **GB** ra đĩa và đem cất đi, ngày qua ngày thì chi phí cho ta đầu tư để dự phòng dữ liệu có lẽ là một con số khổng lồ mà với qui mô nhỏ may ra còn kham nổi, nhưng với những công ty có đến hàng trăm máy thì e ra có vẻ kinh khủng quá

Chuẩn bị:
PC1: Windows server 2008
PC2: Windows server 2008
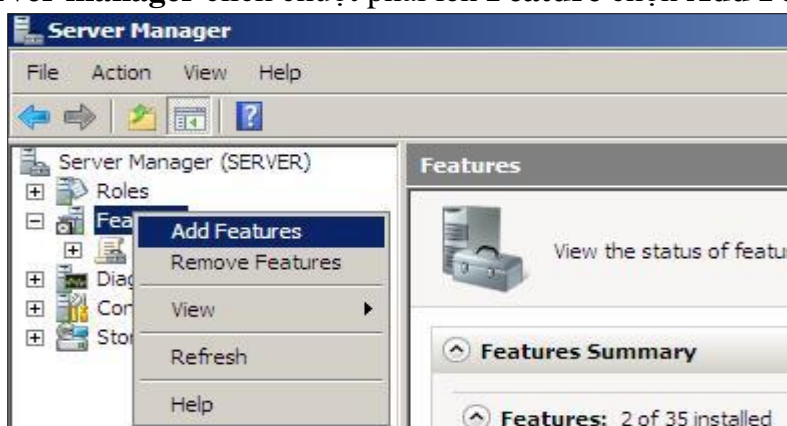PC2: Tạo User **U1** password **123** . Tạo và Share thư mục **BACKUP** trên ổ **C** phân quyền cho **U1** quyền **Everyone- Full control** trên thư mục này.
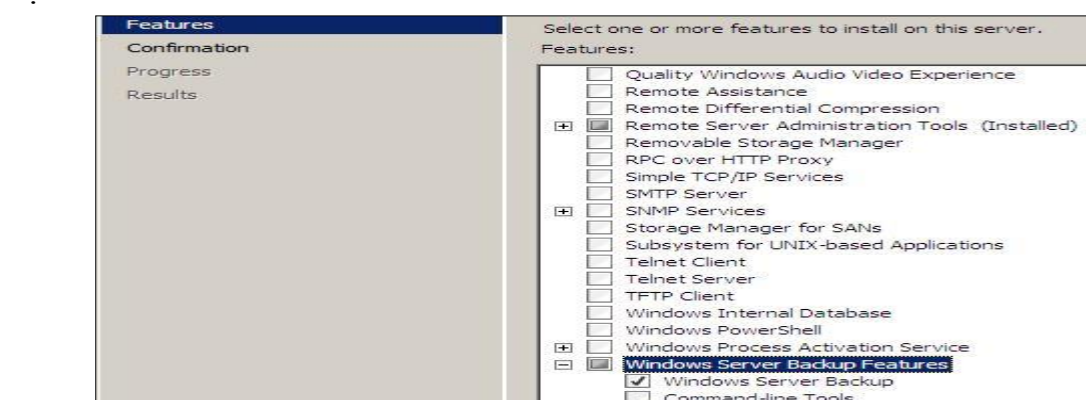
Thực hiện: Trên PC1
 1. **BACKUP**
B1: Mở **server manager** click chuột phải lên **Feature** chọn **Add Features**

B2: Màn hình **Welcom** chọn **next** chọn **Windows server backup Features** chọn **next** chọn **Install**

B3: Tạo thư mục **C:\DATA** và 2 File text tên **Dulieu1.txt và Dulieu2.txt**
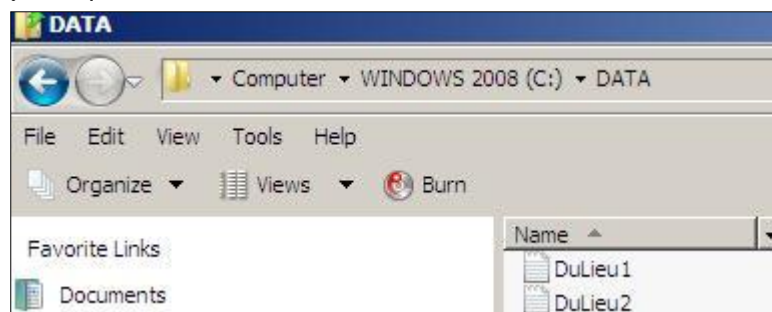
B4: Mở **Windows server backup** trong **Administrtive tools** khung **Action** chọn **Backup one**
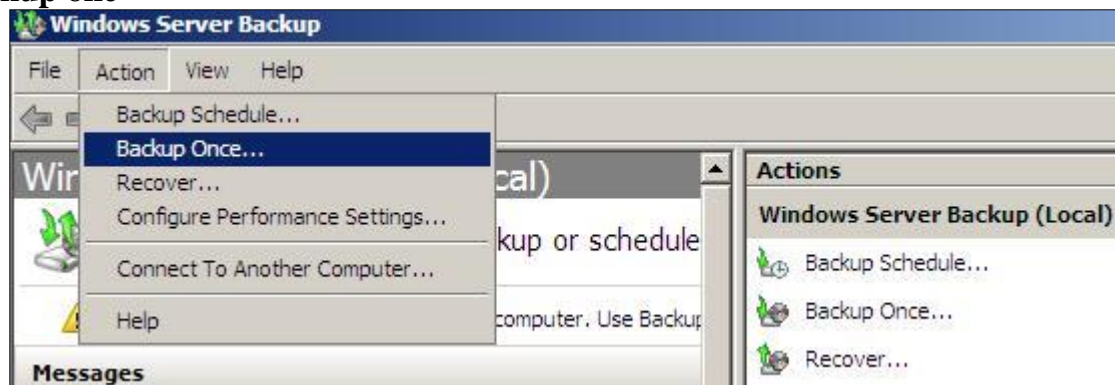
B5: Cửa sổ **Backup Options** chọn **Different Options** chọn **next**

B6: Hộp thoại **Select Backup configuration** chọn **Custom** chọn **Next**

B7: Hộp thoại **Select backup items** Chọn **Server(C)** Bỏ dấu check trước dòng **Enable system recovery** chọn **next**
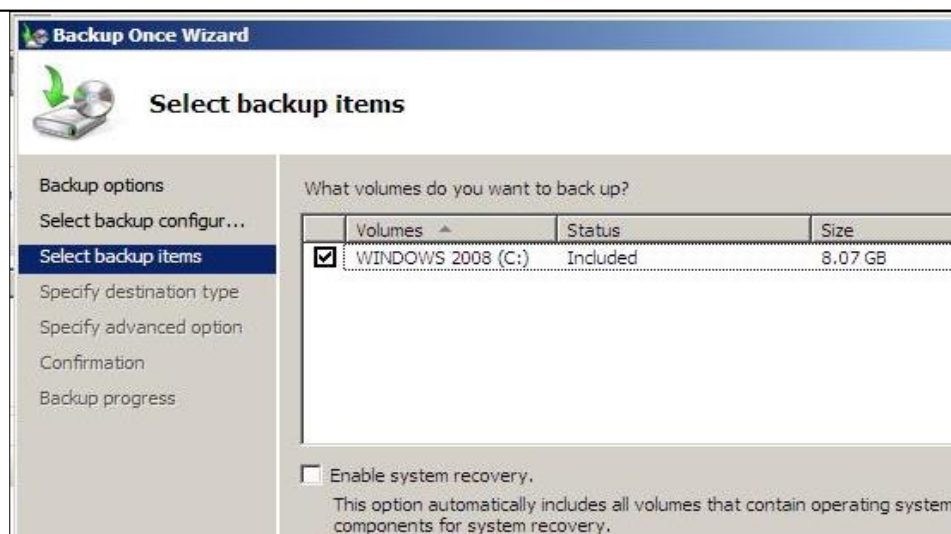
B8: Hộp thoại **Specify destination type** chọn **Remote shared folder** chọn

B9: Trong phần **Type the path to the Remote shared folder** gõ **\\PC2\BACKUP**
 Chọn **Do not inherit** chọn **next**

B10: Hộp thoại xác nhận quyền: điền vào **U1** password **123** chọn **OK**

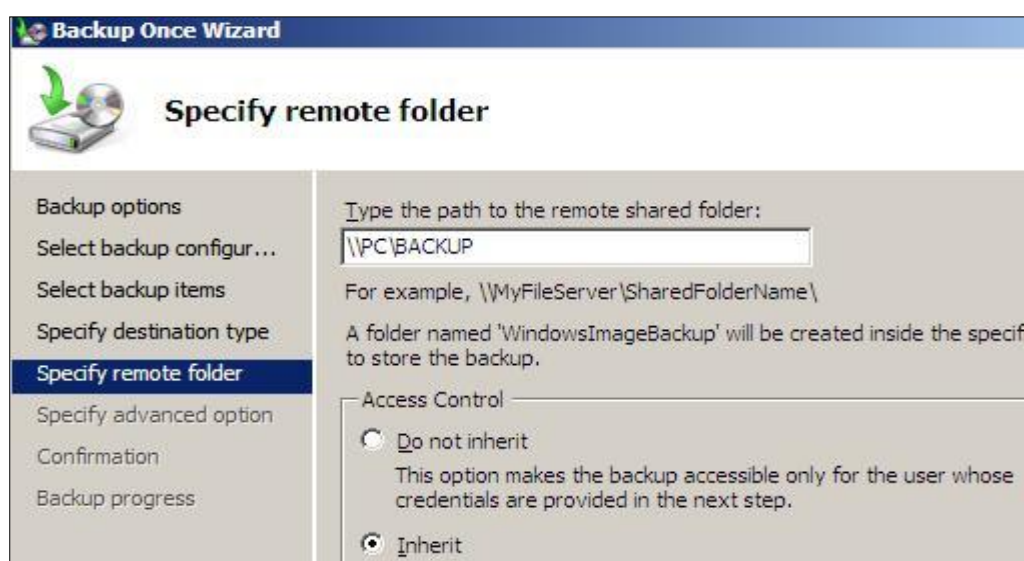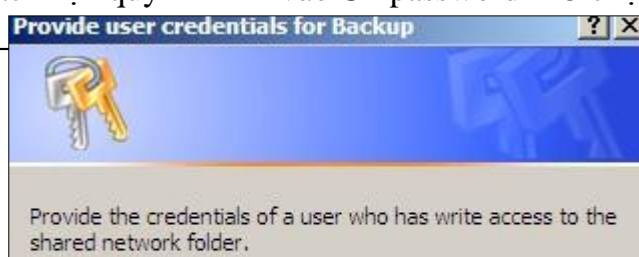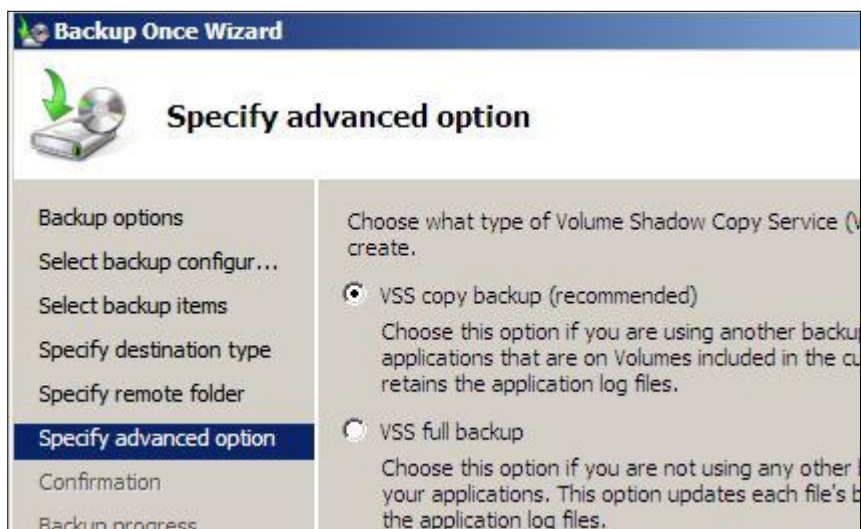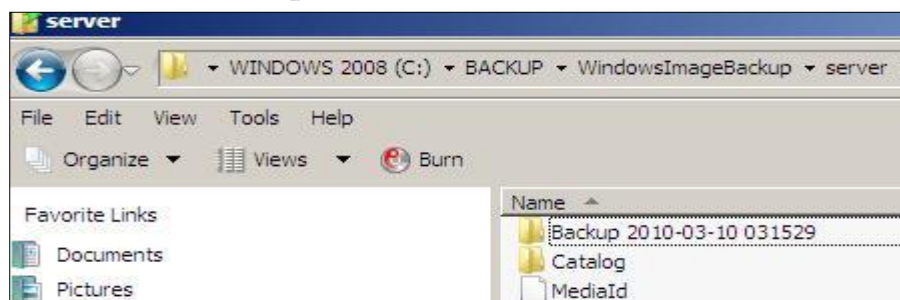B11: Hộp thoại **Specify advanced option** chọn **vss copy backup (recommended)** chọn **next** chọn **next**

B12: Chọn **Backup** sau khi Backup xong chọn **Close**
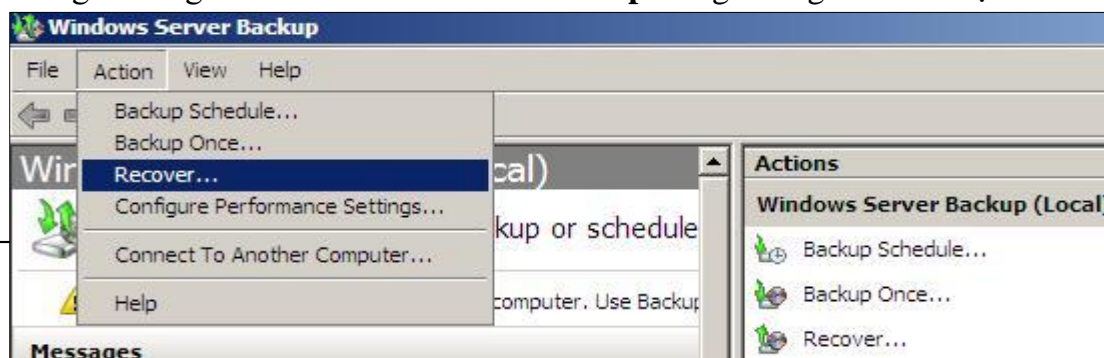
B13: Trên **PC2** mở thu mục **BACKUP** chọn **WindowsImageBackup** chọn **PC1 Quan sát nơi chứa các file backup từ PC1**

2. RECOVER

Trước khi Restore giả lập mất dữ liệu bằng cách **PC1** xóa thư mục **DATA**

Tiến hành khôi phục dữ liệu

B1: Trong chương trình **Windows server Backup** trong khung **Action** chọn **Recover**
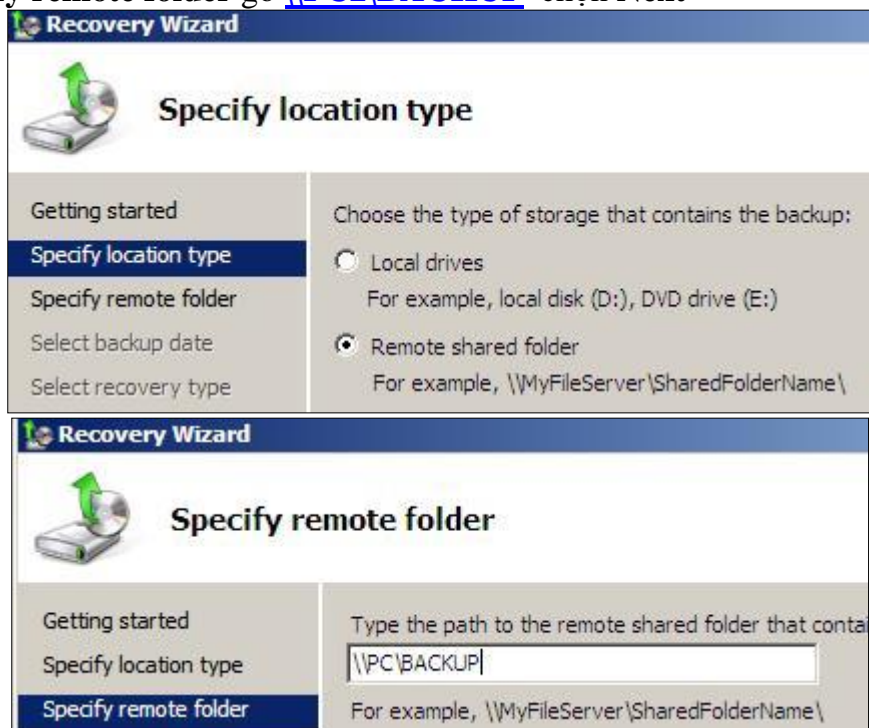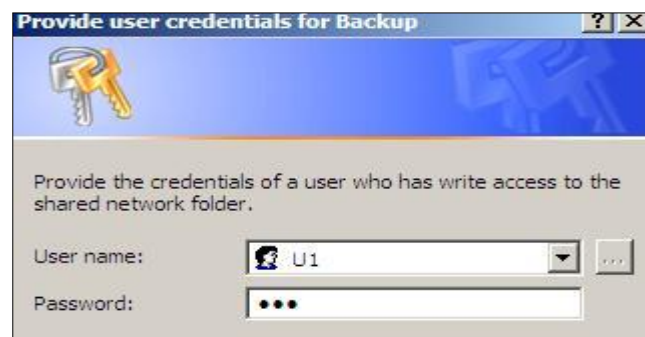
B2: Hộp thoại **Getting started** chọn **Another server** chọn **next**

B3: **Specify remote folder** gõ **\\PC2\BACKUP** chọn **Next**

B4: Điền **usename** và **password** của **U1** chọn **Ok**

B5: **Select backup** date chọn **next**

B6: **Select recovery type** chọn **Files and folders** chọn **next**

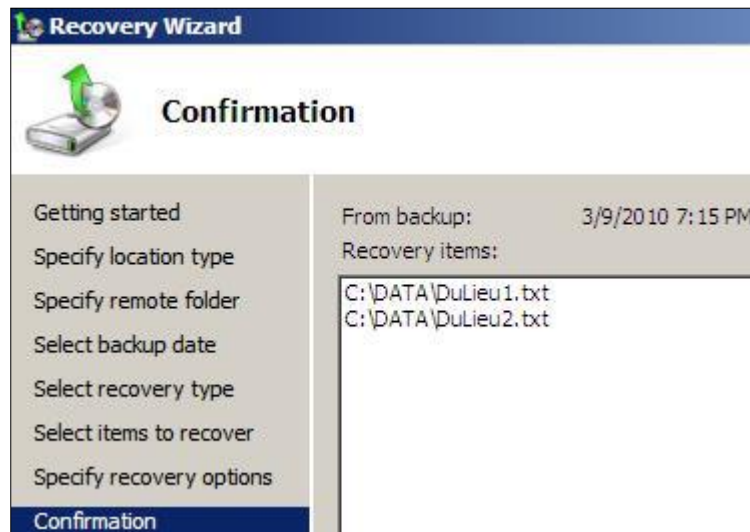B7: **Select Items to recover** chọn thư mục **DATA** chọn **next**

B8: **Specify recovery options** giữ mặc định chọn **next**

B9: chọn **Recover**

Kiểm tra trên **PC1**: Sau khi Recover hoàn tất , mở ổ C quan sát thấy Folder **DATA** và các File trong **DATA** đã được khôi phục.