SỞ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI HÀ NỘI

TRƯỜNG TRUNG CẤP CÔNG NGHỆ VÀ DU LỊCH HÀ NỘI

GIÁO TRÌNH

MÔN ĐUN: HỆ ĐIỀU HÀNH WINDOWS SERVER

NGHỀ: CÔNG NGHỆ THÔNG TIN

TRÌNH ĐỘ: TRUNG CẤP

(Ban hành kèm theo Quyết định số: /QĐ-CNDL ngày tháng năm 2019của Hiệu trưởng Trường Trung cấp Công nghệ và Du lịch Hà Nội)

Hà Nội, năm 2019

TUYÊN BỐ BẢN QUYỀN

LỜI GIỚI THIỆU

Trong thời đại công nghệ số ngày nay hầu hết các thiết bị công nghệ đều được gắn kết với nhau thông qua hệ thống Internet. Do đó việc quản trị một hệ thống mạng ngày càng được quan tâm nhiều hơn. *Hệ điều hành Windows Sever* có một vai trò vô cùng quan trọng, nó chính là nhân tố giúp kết nối, trao đổi giữa các cá nhân và các thành phần trong xã hội. Và ngày càng khẳng định vị thế không thể thiếu trong đời sống kinh tế xã hội ở các quốc gia. Vai trò của nhà quản trị mạng ngày càng được coi trọng. Nghề quản trị mạng đang ngày càng được sự quan tâm của các bạn trẻ.

Giáo trình *"**Hệ điều hành Windows Sever***" được biên soạn dùng cho sinh viên Ngành, Nghề Quản trị mạng máy tính đồng thời cũng là tài liệu tham khảo bổ ích cho sinh viên các khối ngành kỹ thuật của trường.

Giáo trình "***Hệ điều hành Windows Sever***" đã bám sát nội dung chương trình chi tiết do nhà trường ban hành gồm 8 bài:

BÀI 1. TỔNG QUAN VỀ WINDOWS SERVER
BÀI 2. DỊCH VỤ TÊN MIỀN DNS
BÀI 3. DỊCH VỤ THƯ MỤC (ACTIVE DIRECTORY)
BÀI 4. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM
BÀI 5. QUẢN LÝ ĐĨA
BÀI 6. TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG
BÀI 7. DỊCH VỤ DHCP
BÀI 8. QUẢN LÝ IN ẤN

Nhằm cung cấp cho sinh viên một hệ thống kiến thức đầy đủ về mạng máy tính và kỹ năng quản trị mạng**.** Từ đó sinh viên sẽ có đầy đủ nền tảng cơ bản để có thể quản trị một hệ thống mạng ngoài thực tế.

Tuy đã tham khảo nhiều tài liệu nhưng chắc chắn cuốn giáo trình vẫn có những hạn chế nhất định rất mong nhận được sự góp ý của quý thầy cô, quý đồng nghiệp để cuốn giáo trình hoàn thiện hơn.

Xin chân thành cảm!

Hà Nội, ngày.....tháng.....năm 2019

Ban Biên soạn

Khoa Công nghệ thông tin

MỤC LỤC

GIÁO TRÌNH MÔ ĐUN

Tên mô đun: HỆ ĐIỀU HÀNH WINDOWS SEVER

Mã mô đun: MĐ 15

Thời gian thực hiện mô đun: 65 giờ; (Lý thuyết: 25 giờ; Thực hành: 38 giờ; Kiểm tra: 2 giờ)

I. Vị trí, tính chất của mô đun:

- Vị trí: Hệ điều hành Windows Sever thuộc nhóm các mô đun chuyên môn được bố trí giảng dạy sau khi sau khi sinh viên đã học xong các mô đun chung/đại cương, sau môn Mạng máy tính.

- Tính chất: Quản trị mạng là mô đun tự chọn, mô đun cung cấp nền tảng kiến thức về quản trị mạng bao gồm: khái niệm, chức năng, mô hình, quy trình và cách thức thực hiện. Kiến thức về thiết bị, hệ thống và các hệ điều hành mạng.

II. Mục tiêu mô đun:

- Về kiến thức:
  - Hiểu được các khái niệm, chức năng, mô hình, quy trình và cách thức quản trị một mạng máy tính
  - Hiểu rõ các thiết bị, hệ điều hành mạng, các vấn đề liên quan đến tính năng và hoạt động của chúng

- Về kỹ năng:
  - Có khả năng phân tích, thiết kế, lập kế hoạch, thực hành quản trị mạng
  - Có khả năng quản trị mạng cho các doanh nghiệm và cơ quan

- Về năng lực tự chủ và trách nhiệm:
  - Nghiêm túc trong học tập
  - Luôn chủ động khi tiếp thu kiến thức và sáng tạo khi áp dụng vào thực tế
  - Thực hiện tốt các công việc được phân công theo cá nhân hoặc theo nhóm

III. Nội dung mô đun:

1. Nội dung tổng quát và phân bổ thời gian:

Số TT	Tên chương, mục	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
1	Chương 1: TỔNG QUAN VỀ QUẢN TRỊ MẠNG	7	3	4	0
2	Chương 2: CÁC GIAI ĐOẠN QUẢN TRỊ MẠNG	8	3	4	1
3	Chương 3: TỔNG QUAN VỀ WINDOWS SERVER	8	3	5	0

Số TT	Tên chương, mục	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
4	Chương 4: TỔNG QUAN VỀ DHCP SERVER	7	2	5	0
5	Chương 5: TỔNG QUAN VỀ DNS SERVER	9	4	5	0
6	Chương 6: TỔNG QUAN VỀ ACTIVE DIRECTORY	8	3	5	0
7	Chương 7: TỔNG QUAN VỀ WEB SERVER	10	4	5	1
8	Chương 8: TỔNG QUAN VỀ MAIL SERVER	8	3	5	0
	Cộng	**65**	**25**	**38**	**2**

BÀI 1: TỔNG QUAN VỀ WINDOWS SERVER

Mã bài: MĐ15 - 01

Giới thiệu:

Windows server (máy chủ windows) là một nhánh trong hệ điều hành cho máy chủ được sản xuất bởi tập đoàn Microsoft. Chức năng của nó là giúp người dùng có thể quản lý cơ sở hạ tầng của họ một cách tin cậy, an toàn một cách tối đa và cung cấp môi trường môi trường máy chủ làm việc vững chắc.

Trong bài này trình bày tổng quan về windows server và cách cài đặt window server 2019.

Mục tiêu:

- Phân biệt được về họ hệ điều hành Windows Server;
- Cài đặt được hệ điều hành Windows Server.

Nội dung chính:

1. Giới thiệu

Sự phát triển của Windows Server được bắt đầu từ những năm 80 của thế kỉ XX. Khi mà Microsoft tiến hành những bước đầu tiên trong sản xuất hai dòng hệ điều hành là MS-DOS và Windows NT. Kỹ sư của Microsoft lúc đó đã phát triển hệ điều hành Windows NT với mục đích cung cấp tốc độ, bảo mật và độ tin cậy mà các tổ chức lớn yêu cầu trong một hệ điều hành máy chủ.

Một trong những tính năng quan trọng trong kiến trúc NT là đa xử lý đối xứng, giúp cho các ứng dụng chạy nhanh hơn trên máy có một vài bộ xử lý khác nhau. Các phiên bản sau này của Windows Server có thể được triển khai trên phần cứng tại trung tâm dữ liệu của tổ chức hoặc trên nền tảng đám mây.

Trong các phiên bản gần đây của Windows Server có thêm những tính năng chính bao gồm :

– Active Directory, với các khả năng nổi bật như : khả năng tự động hóa việc quản lý dữ liệu người dùng, bảo mật, phân phối tài nguyên, cho phép tương tác với các thư mục khác.

– Server Manager: một tiện ích giúp quản lý các vai trò của máy chủ và thực hiện các thay đổi cấu hình cho các máy local hoặc máy điều khiển từ xa.

Window Server 2012

Window Server 2012 là phiên bản Windows 8 dành cho máy chủ và là phiên bản tiếp theo của Windows Server 2008 R2. Không giống như phiên bản trước, Windows Server 2012 không hỗ trợ cho các máy tính chạy nền tảng Itanium, và có bốn phiên bản. Nhiều tính năng đã được thêm hoặc cải thiện so với Windows Server 2008 R2 (đa phần tập trung vào điện toán đám mây). Các tính ăng nổi bật như:

– Phiên bản mới cập nhật của Hyper-V, chức năng quản lý địa chỉ IP, một phiên bản mới của Windows Task Manager.

– ReFS, hệ thống tập tin mới. Windows Server 2012 đã nhận được nhiều đánh giá tốt mặc dù có cùng giao diện người dùng Metro – gây tranh cãi có trên Windows 8.

Có thể nói Window Server 2012 là phiên bản tốt ở thời điểm đó. Sự ra mắt của Window Server 2012 đã đánh bại nhưng cái tên sừng sỏi khác để vương lên đứng đầu thế giới.

Window Server 2012 R2

Đây là phiên bản nâng cấp của Window Server 2012 được ra mắt một năm sau khi phát hành. Trong phần nâng cấp này Microsoft đã tập trung cho PowerShell để phần này được mở rộng hơn. Microsoft còn tiếp tục nhắm mục tiêu vào việc đưa ra các chức năng máy chủ onsite tốt hơn, cung cấp khả năng tích hợp các dịch vụ đám mây. Hệ thống lưu trữ và ảo hóa cũng được trùng tu lại và các Web service cũng được tăng cường. Như vậy vào thời điểm đó Window Server 2012 R2 là bản nâng cấp hoàn thiện nhất của phiên bản 2012 về mặt cấu hình cũng như khả năng làm việc.

Window Server 2016

Phải trải qua 3 năm kể từ sau Window Server 2012 R2 được ra mắt thì Microsoft mới cho ra mắt thêm một hệ điều hành Window Server nữa, đó là phiên bản 2016. Đây là Nano Server, một máy chủ tương đối gọn nhẹ, với ít giao diện hơn và do đó khó bị tấn công hơn. Phiên bản Windows Server này cũng bao gồm cả Server Core. Vào năm đó Microsoft còn giới thiệu Network Controller trong Windows Server 2016, phần mềm cho phép các admin quản lý cả thiết bị mạng vật lý và ảo từ một bảng điều khiển.

Các hệ thống như VM cũng được thêm vào hệ thống mã hóa Hyper-V và có khả năng tương tác mới hơn với Docker. Công cụ này đặc biệt hữu ích cho

việc "container hóa", trong đó cho phép các quản trị viên hệ thống cung cấp phần mềm thuộc sở hữu của công ty cho các thiết bị do người dùng sở hữu.

Window Server 2019

Window Sever 2019 được phát hành vào ngay tháng 10 năm 2018, Windows Server 2019 là phiên bản mới nhất của hệ điều hành Window Server của Microsoft.

Đầu tiên là Microsoft đã mạnh tay vào phần bảo mật với việc đưa ra chức năng bảo mật tích hợp. Với tính năng này, Microsoft đã giúp các tổ chức giải quyết được mô hình quản lý bảo mật của họ. Tiếp theo đó là công cụ quản lý máy chủ Project Honolulu – một giao diện điều khiển trung tâm cho phép dễ dàng quản lý các máy chủ Windows 2019, 2016 và 2012R2 có giao diện và không có giao diện trong môi trường. Đó cũng là hai trong vô số các tính năng mới được cập nhật vào Window Server 2019 trong thời gian vừa qua.

Các phiên bản Window Server 2019 :

- Windows server 2019 Datacenter: Như các hệ điều hành đã ra trước đó, đây là phiên bản được sử dụng cho các trung tâm dữ liệu đám mây cũng như các môi trường ảo hóa cao.
- Windows server 2019 Standard: Phiên bản này đã được Microsoft để sử dụng cho các môi trường vật lý.
- Windows server 2019 Essentials: Phiên bản dành cho các doanh nghiệp có quy mô nhỏ.
- Windows server 2019 MultiPoint Premium Server: Đây là phiên bản dành riêng cho các máy chủ có chức năng lưu trữ dữ liệu, chỉ cho phép người dùng truy cập để đọc thông tin

2. Chuẩn bị cài đặt windows server

2.1. Yêu cầu phần cứng

Đối với windows Server 2019 yêu cầu về phần cứng như sau:

Thành phần	Yêu cầu
Bộ xử lý	Tối thiểu: • Bộ xử lý 64-bit 1.4 GHz • Tương thích với bộ lệnh x64

	• Hỗ trợ NX và DEP • Hỗ trợ CMPXCHG16b, LAHF/SAHF, and PrefetchW • Hỗ trợ Second Level Address Translation (EPT hoặc NPT) • Ethernet: Adapter Gigabit Ethernet (10/100/1000 Base-T) • Display Resolution: Monitor Super VGA (1024 x 768) hoặc cao hơn
Bộ nhớ	Tối thiểu: • 512 MB (2 GB với tùy chọn máy chủ cài đặt Desktop Experience) • ECC (Error Correcting Code – mã sửa lỗi) hoặc công nghệ tương tự
Không gian ổ đĩa còn trống	Tối thiểu: Tối thiểu 32GB để lưu trữ
Ổ đĩa	Ổ DVD-ROM Cổng USB cài đặt Mạng Internet
Màn hình	Super VGA (1024 x 768) hoặc cao hơn
Thành phần khác	Bàn phím, Chuột hoặc thiết bị trỏ tương thích

Bảng 1.1. Yêu cầu cấu hình thiết bị khi cài window server

2.2. Tương thích phần cứng

Một bước quan trọng trước khi nâng cấp hoặc cài đặt mới Server là kiểm tra xem phần cứng của máy tính hiện tại có tương thích với sản phẩm hệ điều hành trong họ Windows Server 2019.

2.3. Cài đặt mới hoặc nâng cấp

Trong một số trường hợp hệ thống **Server** đang hoạt động tốt, các ứng

dụng và dữ liệu quan trọng đều lưu trữ trên **Server** này, nhưng theo yêu cầu phải nâng cấp hệ điều hành **Server** hiện tại thành **Windows Server 2019**. Cần xem xét nên nâng cấp hệ điều hành đồng thời giữ lại các ứng dụng và dữ liệu hay cài đặt mới hệ điều hành rồi sau cấu hình và cài đặt ứng dụng lại. Đây là vấn đề cần xem xét và lựa chọn cho hợp lý. Các điểm cần xem xét khi nâng cấp:

- Với nâng cấp (**upgrade**) thì việc cấu hình **Server** đơn giản, các thông tin của được giữ lại như: người dùng (**users**), cấu hình (**settings**), nhóm (**groups**), quyền hệ thống (**rights**), và quyền truy cập (**permissions**)…
- Với nâng cấp không cần cài lại các ứng dụng, nhưng nếu có sự thay đổi lớn về đĩa cứng thì cần backup dữ liệu trước khi nâng cấp.
- Trước khi nâng cấp cần xem hệ điều hành hiện tại có nằm trong danh sách các hệ điều hành hỗ trợ nâng cấp thành **Windows Server 2019** không ?
- Trong một số trường hợp đặc biệt cần nâng cấp một máy tính đang làm chức năng **Domain Controller** hoặc nâng cấp một máy tính đang có các phần mềm quan trọng thì nên tham khảo thêm thông tin hướng dẫn của **Microsoft.**

2.4. Phân chia ổ đĩa

Đây là việc phân chia ổ đĩa vật lý thành các **partition logic**. Khi chia **partition**, cần phải quan tâm các yếu tố sau:

- **Lượng không gian cần cấp phát:** phải biết được không gian chiếm dụng bởi hệ điều hành, các chương trình ứng dụng, các dữ liệu đã có và sắp phát sinh.
- Cấu hình đĩa đặc biệt: **Windows Server** hỗ trợ nhiều cấu hình đĩa khác nhau. Các lựa chọn có thể là **volume simple**, **spanned**, **striped**, **mirrored** hoặc là **RAID**.
- **Tiện ích phân chia partition:** nếu dự định chia **partition** trước khi cài đặt, có thể sử dụng nhiều chương trình tiện ích khác nhau, chẳng hạn như **FDISK** hoặc **PowerQuest Partition Magic**. Có thể ban đầu chỉ cần tạo một **partition** để cài đặt **Windows Server**, sau đó sử dụng công cụ **Disk Management** để tạo thêm các **partition** khác.

2.5. Chọn hệ thống tập tin

Nên chọn hệ thống tập tin ***NTFS,*** vì nó có các đặc điểm sau: chỉ định khả

năng an toàn cho từng tập tin, thư mục; nén dữ liệu, tăng không gian lưu trữ; có thể chỉ định hạn ngạch sử dụng đĩa cho từng người dùng; có thể mã hoá các tập tin, nâng cao khả năng bảo mật.

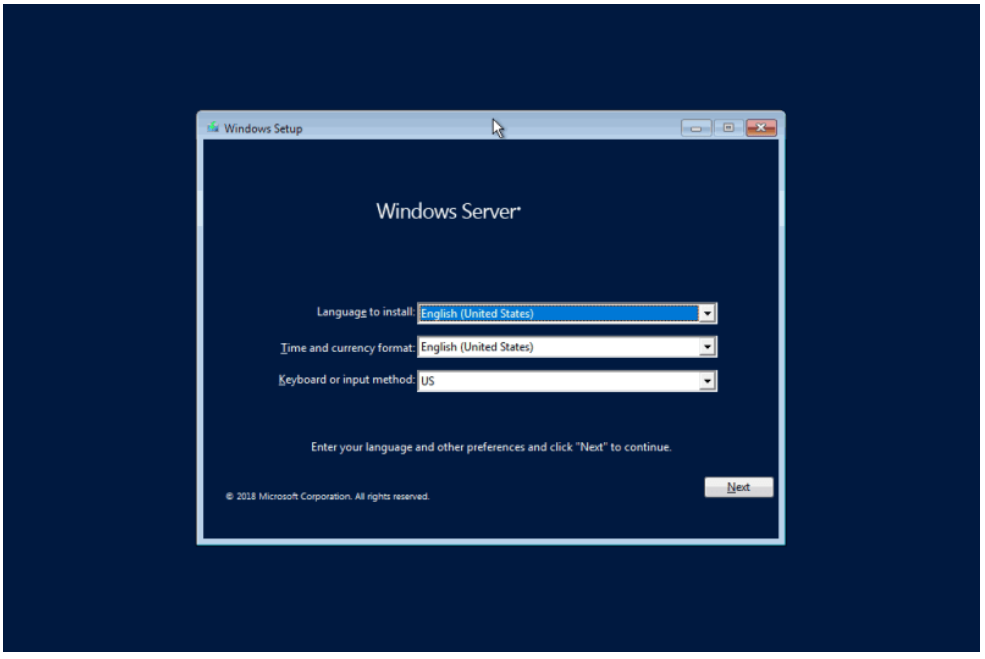
2.6. Chọn chế độ sử dụng giấy phép

Có thể chọn một trong hai chế độ giấy phép sau đây:

- **Per server licensing**: là lựa chọn tốt nhất trong trường hợp mạng chỉ có một Server và phục cho một số lượng Client nhất định. Khi chọn chế độ giấy phép này, cần phải xác định số lượng giấy phép tại thời điểm cài đặt hệ điều hành. Số lượng giấy phép tùy thuộc vào số kết nối đồng thời của các Client đến Server. Tuy nhiên, trong quá trình sử dụng chúng ta có thể thay đổi số lượng kết nối đồng thời cho phù hợp với tình hình hiện tại của mạng.
- **Per Seat licensing**: là lựa chọn tốt nhất trong trường hợp mạng có nhiều Server. Trong chế độ giấy phép này thì mỗi Client chỉ cần một giấy phép duy nhất để truy xuất đến tất cả các Server và không giới hạn số lượng kết nối đồng thời đến Server.

3. Cài đặt windows server 2019

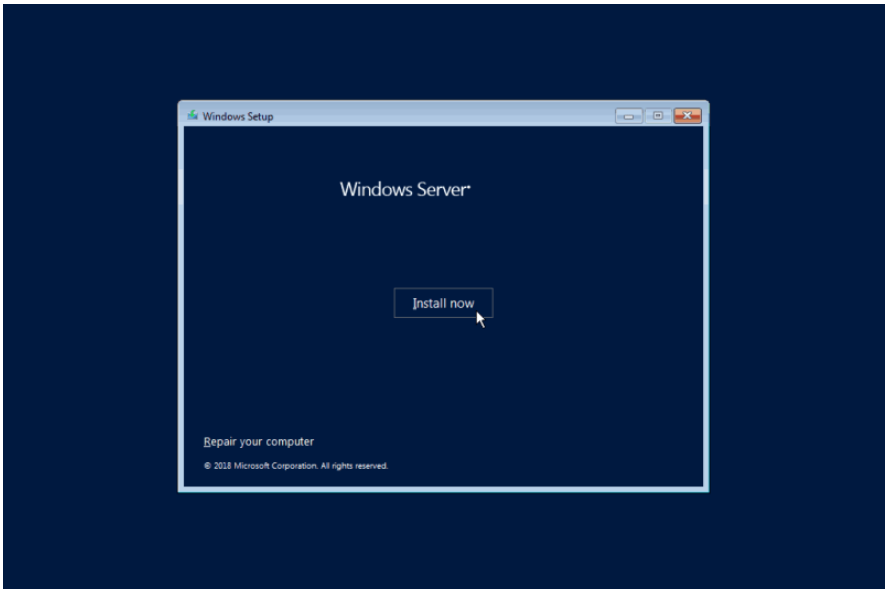
Đầu tiên cần phải tạo USB Boot hay DVD cài đặt Windows Server 2019 bằng file .iso mà chúng ta đã download từ trang chủ của Microsoft.



Hình 1.1 Chọn ngôn ngữ, múi giờ và phương pháp nhập liệu

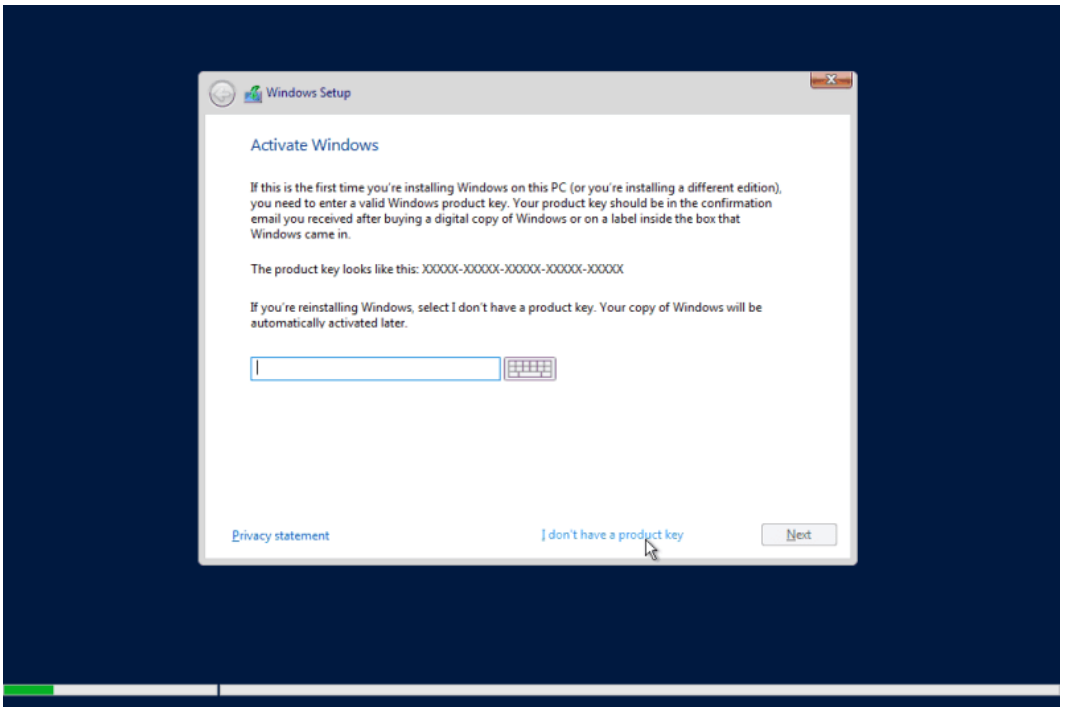
- Chọn ngôn ngữ, múi giờ và bàn phím cho Windows server 2019.

- Chọn "Next" để tiếp tục:



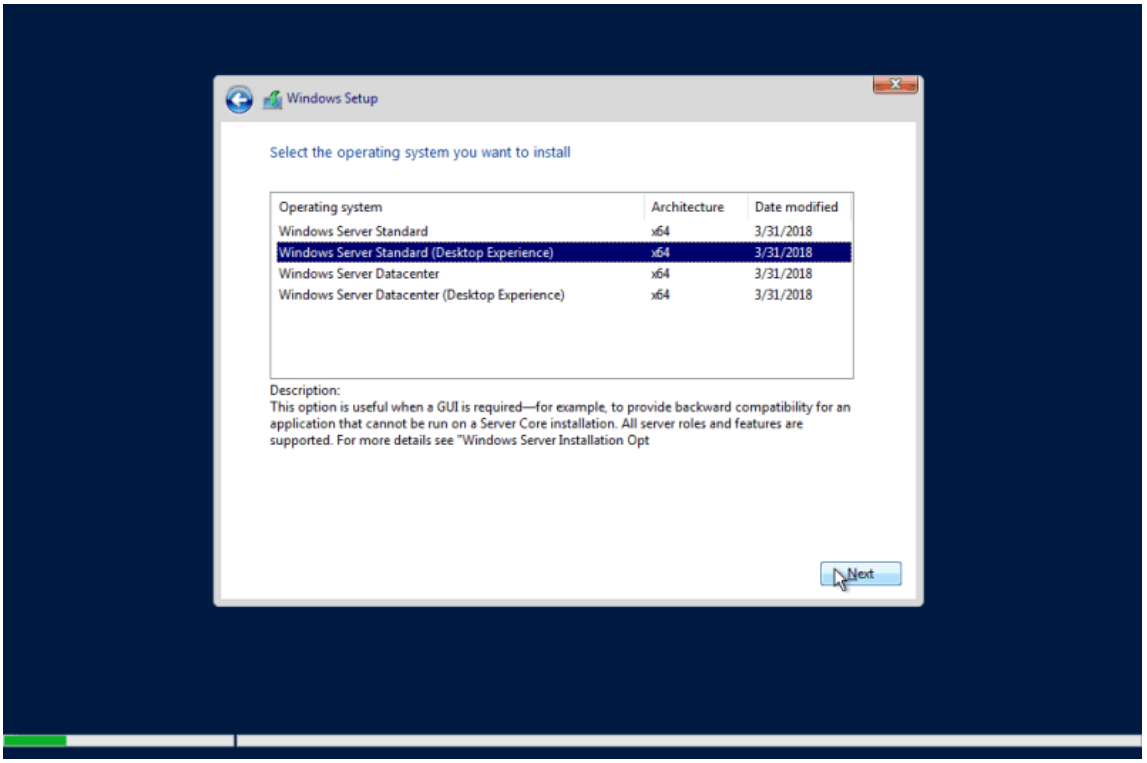
Hình 1.2 Cài đặt Windows Server 2019

- Chọn Install now để tiến hành cài đặt.



Hình 1.3 Nhập Product Key kích hoạt Windows Server 2019

- Nhập Khóa sản phẩm – Product Key để kích hoạt Windows Server 2019. Chọn Next để tiếp tục.



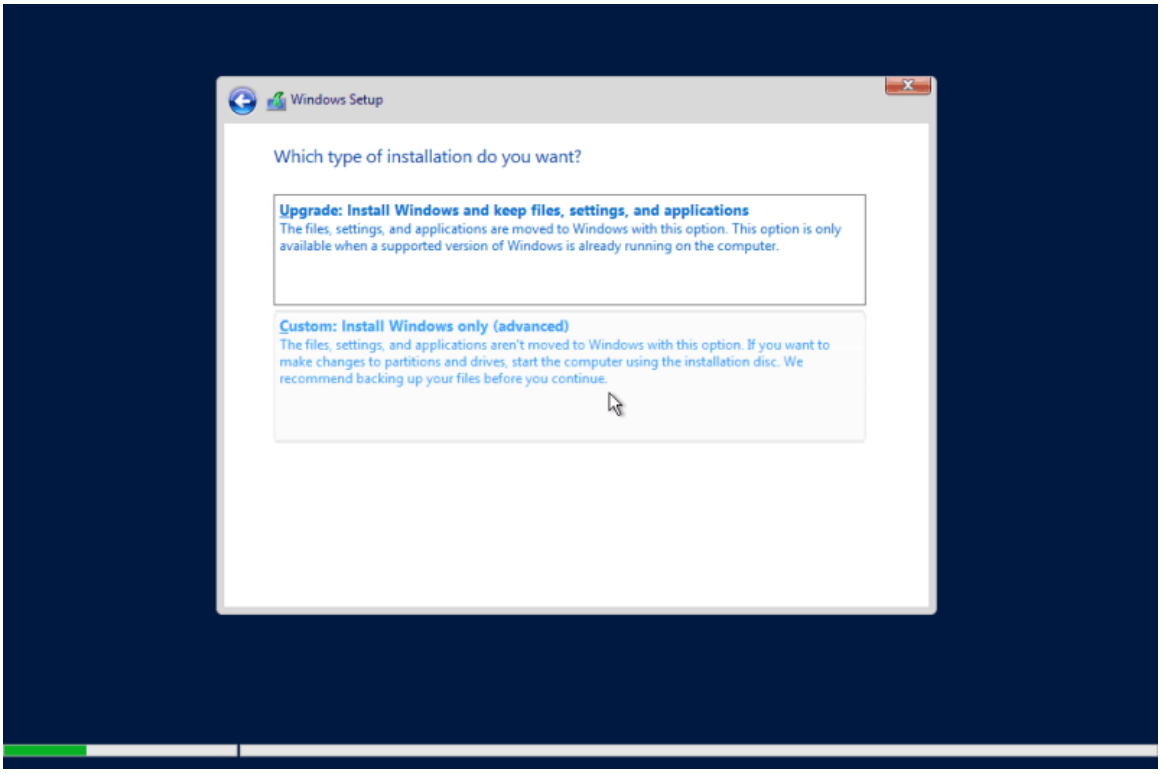
Hình 1.4 Lựa chọn hệ điều hành cài đặt

- Tại bước này, cần lựa chọn loại hệ điều hành muốn cài đặt.

- *Windows Server 2019 Standard:* Đây là bản Windows Server không có giao diện GUI mà nó sử dụng giao diện dòng lệnh Powershell. Bản này tương tự như bản cài đặt Windows Server Core.
- *Windows Server 2019 Standard (Desktop Experience)* đây là bản Windows Server có giao diện GUI của Windows 10 và giao diện Server Manager được cài đặt thêm.
- *Windows Server 2019 Datacenter (Desktop Experience)* Sử dụng cho các trung tâm dữ liệu đám mây và các môi trường ảo hóa cao.

* *Lưu ý*: khi chọn chọn bản cài đặt là **"**Windows Server 2019 Standard **"** hay **"**Windows Server 2019 Standard (Desktop Experience)**"** sẽ không thể chuyển đổi giữa 2 chế độ này. Trừ khi cài lại Windows Server 2019 từ đầu. Ở đây lựa chọn cài đặt bản **"**Windows Server 2019 Standard (Desktop) Experience**"**.

- Sau đó click **"**Next**"** để qua bước cài đặt tiếp theo. Chọn vào Check box **"**I accept license terms**"** để đồng ý với các điều khoản/điều kiện của Microsoft. Chọn Next để tiếp tục.



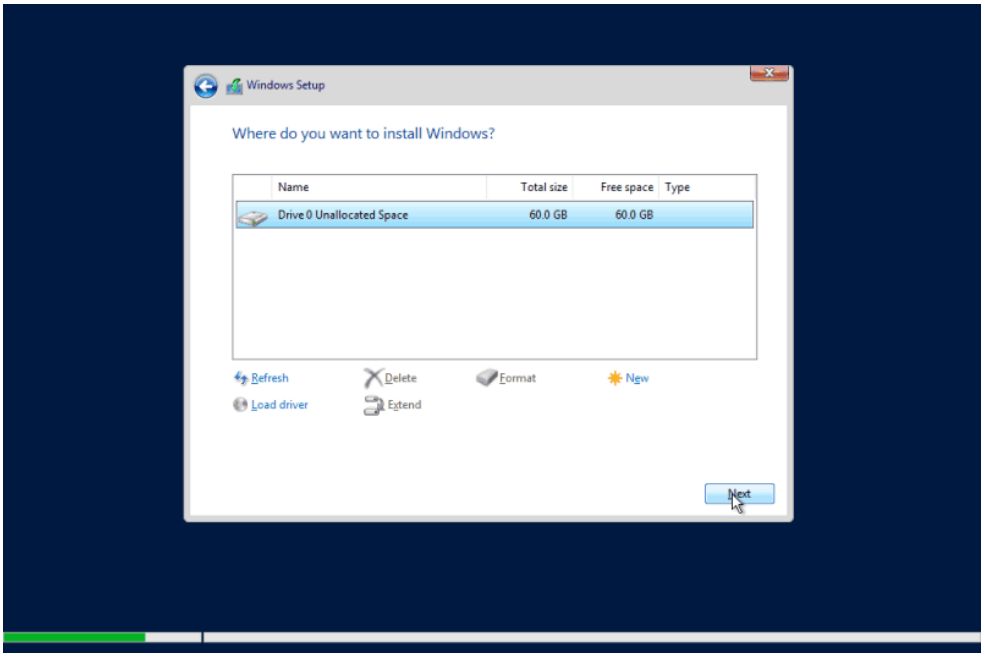
Hình 1.5 Chọn kiểu cài đặt muốn thực hiện

- Chọn Custom để cài đặt mới

- Chọn kiểu cài đặt mà muốn thực hiện là "Upgrade" hay là "Install". Ở đây sẽ tiến hành **Cài đặt mới** nên chọn dòng **"Custom: Install Windows Only (advanced)"**.

Lưu ý:* Tính năng **Upgrade (nâng cấp) có thể hiểu là cài đặt hay nâng cấp lại hệ điều hành nhưng không làm mất các chương trình đã cài đặt, bảo lưu thông tin, dữ liệu, môi trường làm việc của người sử dụng… Hạn chế của tính năng này là: những lỗi xuất hiện ở phiên bản Windows hiện tại trên thiết bị cũng sẽ được giữ nguyên khi Upgrade. Ngoài ra sau khi Upgrade, một số ứng dụng có thể sẽ gặp trục trặc dẫn đến hoạt động không mượt mà, thậm chí là không thể sử dụng.

- Tiếp theo, lựa chọn Ổ cứng để tiến hành cài đặt Windows Server 2019.

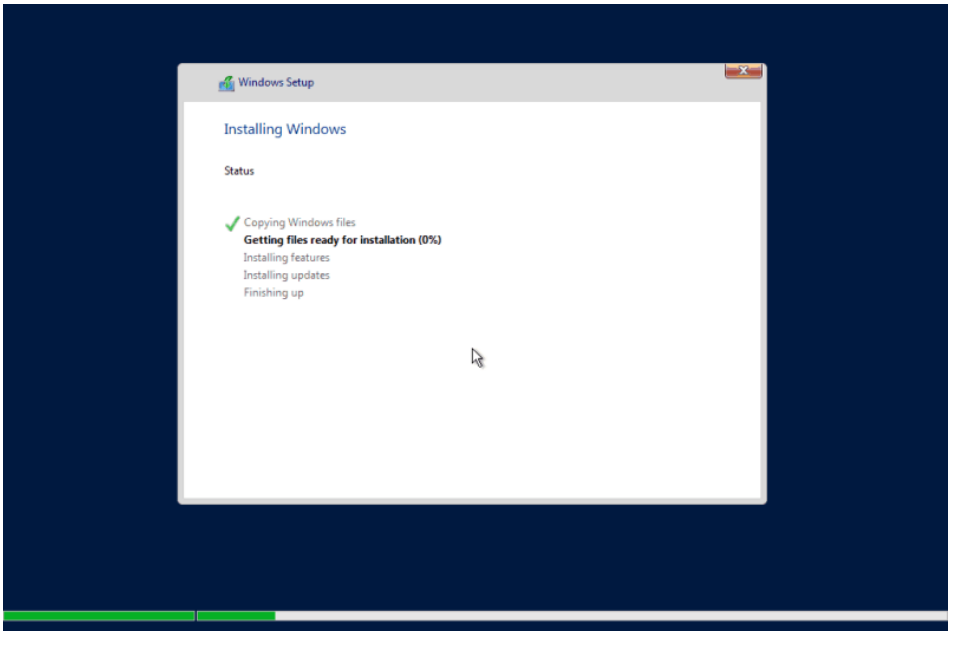


Hình 1.6 Chọn phân vùng ổ cứng để cài đặt

- Nếu muốn chia ổ thành nhiều phân vùng, chọn vào ổ sau đó ấn "New" để chia ra thành nhiều phân vùng.

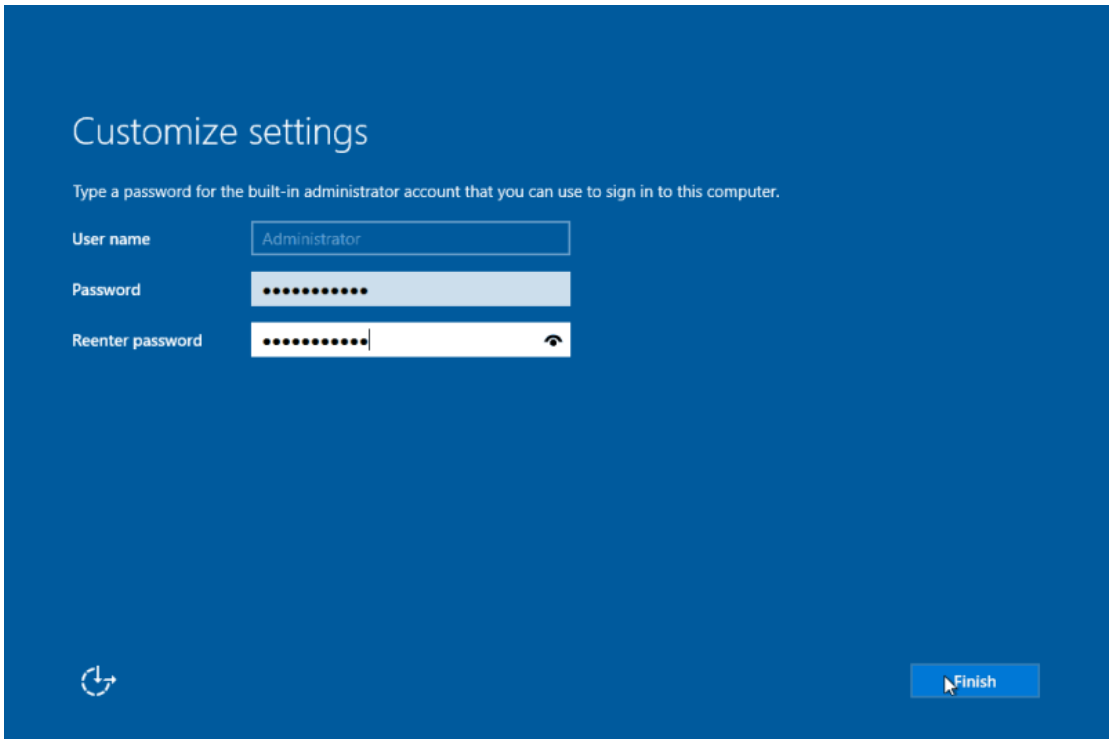
* *Lưu ý:* Dung lượng ổ cứng thấp nhất để cài đặt Windows Server 2019 là 32 GB. Tuy nhiên nên sử dụng ổ cứng nhiều hơn, khoảng 100 GB để đảm bảo Windows có đủ dung lượng ổ cứng để thực hiện các update.

- Chọn "**Next**" và đợi Windows Server 2019 tự động chép source Windows Server lên ổ cứng và tự động cài đặt.



Hình 1.7 Bắt đầu cài đặt Server 2019

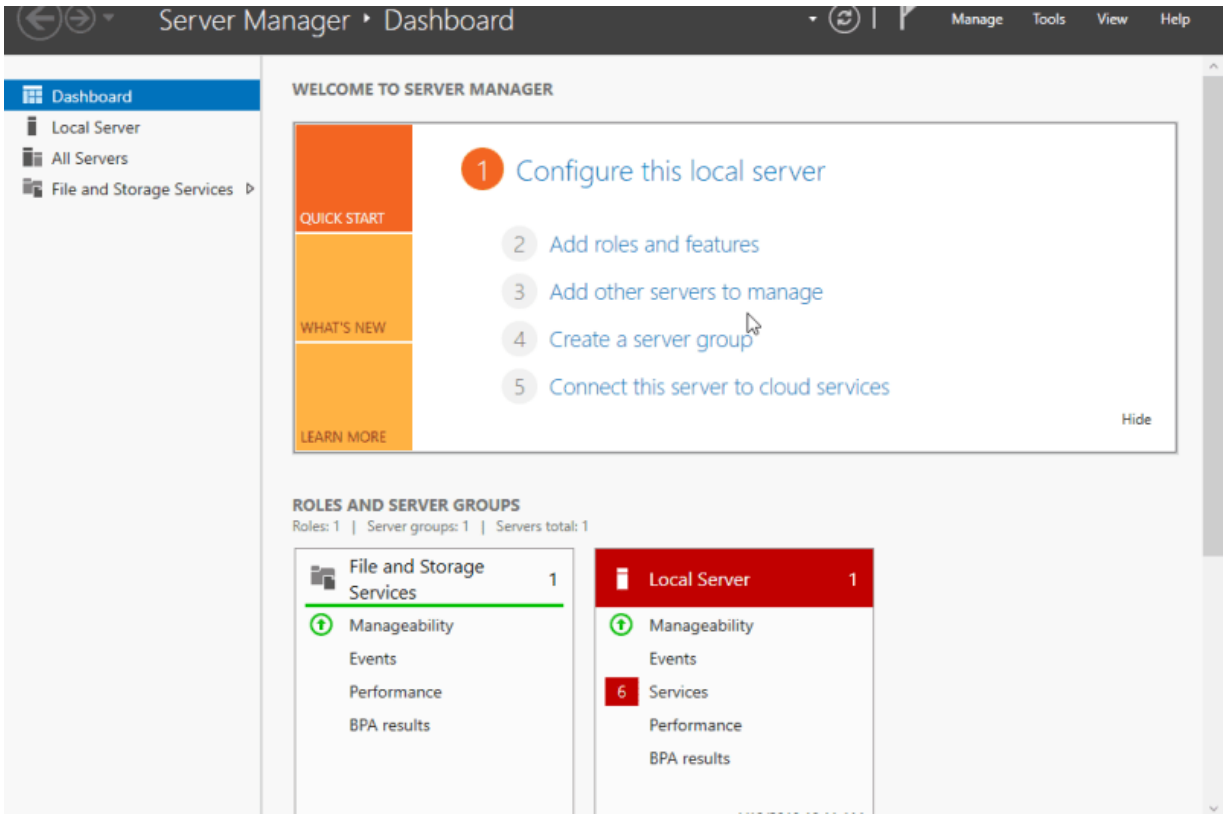
- Sau khi cài đặt Windows Server 2019 lên ổ cứng thành công thì Server/VPS sẽ khởi động lại và vào bước cuối cùng, đó là cấu hình password cho user "Administrator".



***Hình 1.8** Giao diện đăng nhập của Windows Server 2019 sau khi cài đặt xong.*

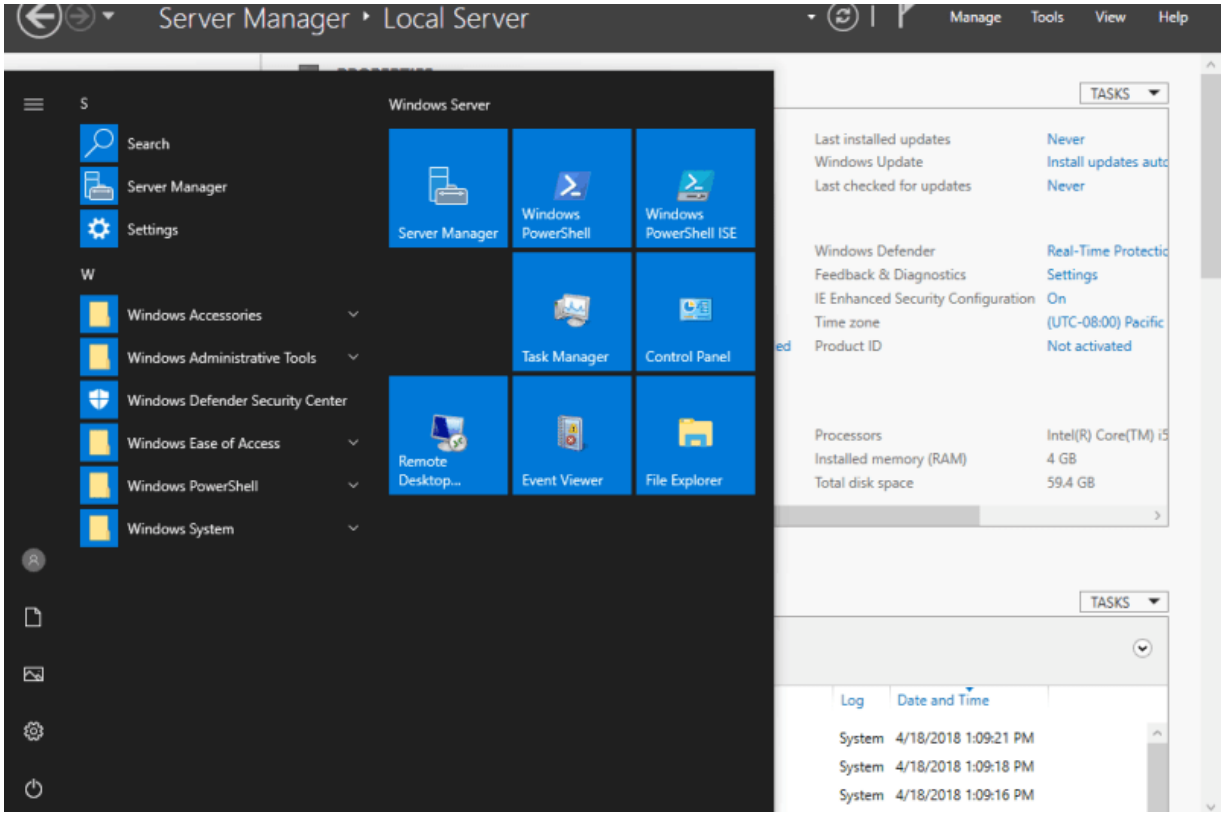
- Nhấn tổ hợp phím "**Ctrl + Alt + Del**" để vào màn hình login của Windows.

Hình 1.9 giao diện quản trị Server 2019



Hình 1.10 Giao diện quản trị Server Manager

- Giao diện Server 2019 khá tương đồng với Windows Server 2016.



Hình 1.11 Giao diện Start Menu trên Server 2019

4. Tự động hóa quá trình cài đặt

4.1. Giới thiệu kịch bản cài đặt

Kịch bản cài đặt là một tập tin văn bản có nội dung trả lời trước tất cả các câu hỏi mà trình cài đặt hỏi như: tên máy, **DVD-Key**,….Để trình cài đặt có thể đọc hiểu các nội dung trong kịch bản thì nó phải được tạo ra theo một cấu trúc được quy định trước. Để tạo ra được các kịch bản cài đặt, có thể dùng bất kỳ chương trình soạn thảo văn bản nào, chẳng hạn như **Notepad**. Tuy nhiên, kịch bản là một tập tin có cấu trúc nên trong quá trình soạn thảo có thể xảy ra các sai sót dẫn đến quá trình tự động hóa cài đặt không diễn ra theo ý muốn. Do đó, **Microsoft** đã tạo ra một tiện ích có tên là **Setup Manager** (**setupmgr.exe**) để giúp cho việc tạo ra kịch bản cài đặt được dễ dàng hơn. Sau khi có được kịch bản, có thể sử dụng **Notepad** để thêm, sửa lại một số thông tin để sử dụng kịch bản vào quá trình cài đặt tự động hiệu quả hơn.

4.2. Tự động hóa dùng tham biến dòng lệnh

Khi tiến hành cài đặt **Windows Server**, ngoài cách khởi động và cài trực tiếp từ đĩa **DVD-ROM**, còn có thể dùng một trong hai lệnh sau: **winnt.exe** dùng với các máy đang chạy hệ điều hành DOS, **windows 3.x** hoặc **Windows for workgroup**; **winnt32.exe** khi máy đang chạy hệ điều hành **Windows 9x**, **Windows NT** hoặc mới hơn. Hai lệnh trên được đặt trong thư mục **I386** của đĩa cài đặt. Sau đây là cú pháp cài đặt từ 2 lệnh trên:

winnt [/s:[sourcepath]] [/t:[tempdrive]] [/u:[answer_file]]

[/udf:id [,UDB_file]]

Ý nghĩa các tham số:

/s

Chỉ rỏ vị trí đặt của bộ nguồn cài đặt (thư mục I386). Đường dẫn phải là dạng đầy đủ, ví dụ: e:\i386 hoặc **\\server\i386**. Giá trị mặc định là thư mục hiện hành.

/t

Hướng chương trình cài đặt đặt thư mục tạm vào một ổ đĩa và cài **Windows** vào ổ đĩa đó. Nếu không chỉ định, trình cài đặt sẽ tự xác định.

/u

Cài đặt không cần theo dõi với một tập tin trả lời tự động (kịch bản). Nếu sử

dụng **/u** thì phải sử dụng **/s.**

/udf

Chỉ định tên của **Server** và tập tin cơ sở dữ liệu chứa tên, các thông tin đặc trưng cho mỗi máy

(unattend.udf).

winnt32 [**/checkupgradeonly**] [**/s:***sourcepath*] [**/tempdrive:***drive_letter***:**]

[**/unattend**[*num*]**:**[*answer_file*]] [**/udf:***id* [,*UDB_file*]]

Ý nghĩa của các tham số:

/checkupgradeonly

Kiểm tra xem máy có tương thích để nâng cấp và cài đặt **Windows 2003 Server** hay không?

/tempdrive

Tương tự như tham số /t

/unattend

Tương tư như tham số /u

4.3. Sử dụng Setup Manager để tạo ra tập tin trả lời

Setup Manager là một tiện ích giúp cho việc tạo các tập tin trả lời sử dụng trong cài đặt không cần theo dõi. Theo mặc định, **Setup Manager** không được cài đặt, mà được đặt trong tập tin **Deploy.Cab**.

Tạo tập tin trả lời tự động bằng **Setup Manager**:

(1). Giải nén tập tin **Deploy.cab** được lưu trong thư mục **Support\Tools** trên đĩa cài đặt **Windows**.

(2). Thi hành tập tin **Setupmgr.exe**

(3). Hộp thoại **Setup Manager** xuất hiện, nhấn **Next** để tiếp tục.

(4). Xuất hiện hộp thoại **New or Existing Answer File**. Hộp thoại này cho phép bạn chỉ định tạo ra một tập tin trả lời mới, một tập tin trả lời phản ánh cấu hình của máy tính hiện hành hoặc là chỉnh sửa một tập tin sẵn có. Bạn chọn **Create new** và nhấn **Next**.

(5) . Tiếp theo là hộp thoại **Type of Setup**. Chọn **Unattended Setup** và chọn **Next**.

(6). Trong hộp thoại **Product**, chọn hệ điều hành cài đặt sử dụng tập tin

trả lời tự động. Chọn **Windows Server, Enterprise Edition**, nhấn **Next**.

(7). Tại hộp thoại **User Interaction**, chọn mức độ tương tác với trình cài đặt của người sử dụng. Chọn **Fully Automated**, nhấn **Next**.

(8). Xuất hiện hộp thoại **Distribution Share**, chọn **Setup from a DVD**, nhấn **Next**.

(9). Tại hộp thoại **License Agreement**, đánh dấu vào **I accept the terms of …**, nhấn **Next**.

(10). Tại cửa sổ **Setup Manager**, chọn mục **Name and Organization**. Điền tên và tổ chức sử dụng hệ điều hành. Nhấn **Next**.

(11). Chọn mục **Time Zone** \ chọn múi giờ (**GMT+7:00) Bangkok, Hanoi, Jarkata**. Nhấn **Next**.

(12). Tại mục **Product Key**, điền **DVD-Key** vào trong 5 ô trống. Nhấn **Next**.

(13). Tại mục **Licensing Mode**, chọn loại bản quyền thích hợp. Nhấn **Next**.

(14). Tại mục **Computer Names**, điền tên của các máy dự định cài đặt. Nhấn **Next**.

(15). Tại mục **Administrator Password**, nhập vào **password** của người quản trị. Nếu muốn mã hóa **password** thì đánh dấu chọn vào mục "**Encrypt the Administrator password…**". Nhấn **Next**

(16). Tại mục **Network Component**, cấu hình các thông số cho giao thức **TCP/IP** và cài thêm các giao thức. Nhấn **Next**.

(17). Tại mục **Workgroup or Domain**, gia nhập máy vào **Workgroup** hoặc **Domain** có sẵn. Nhấn **Next**.

(18). Cuối cùng, trong thư mục đã chỉ định, **Setup Manager** sẽ tạo ra ba tập tin. Nếu bạn không thay đổi tên thì các tập tin là:

Unattend.txt: đây là tập tin trả lời, chứa tất cả các câu trả lời mà **Setup Manager** thu thập được

Unattend.udb: đây là tập tin cơ sở dữ liệu chứa tên các máy tính sẽ được cài đặt. Tập tin này chỉ được tạo ra khi bạn chỉ định danh sách các tập tin và được sử dụng khi bạn thực hiện cài đặt không cần theo dõi.

Unattend.bat: chứa dòng lệnh với các tham số được thiết lập sẵn. Tập tin này cũng thiết lập các biến môi trường chỉ định vị trí các tập tin liên quan.

4.4. Sử dụng tập tin trả lời

Có nhiều cách để sử dụng các tập tin được tạo ra trong bước trên. Bạn có thể thực hiện theo một trong hai cách dưới đây:

4.4.1. Sử dụng đĩa DVD Windows Server có thể khởi động được

Sửa tập tin **Unattend.txt** thành **WINNT.SIF** và lưu lên đĩa mềm.

Đưa đĩa DVD **Windows Server** và đĩa mềm trên vào ổ đĩa, khởi động lại máy tính, đảm bảo ổ đĩa DVD là thiết bị khởi động đầu tiên. Chương trình cài đặt trên đĩa DVD sẽ tự động tìm đọc tập tin **WINNT.SIF** trên đĩa mềm và tiến hành cài đặt không cần theo dõi.

4.4.2. Sử dụng một bộ nguồn cài đặt Windows Server

Chép các tập tin đã tạo trong bước trên vào thư mục **I386** của nguồn cài đặt **Windows Server**. Chuyển vào thư mục **I386**.

Tuỳ theo hệ điều hành đang sử dụng mà sử dụng lệnh **WINNT.EXE** hoặc **WINNT32.EXE** theo cú pháp sau:

WINNT /s:e:\i386 /u:unattend.txt

Hoặc

WINNT32 /s:e:\i386 /unattend:unattend.txt

Nếu chương trình **Setup Manager** tạo ra tập tin **Unatend.UDB** do bạn đã nhập vào danh sách tên các máy tính, và giả định bạn định đặt tên máy tính này là **server01** thì cú pháp lệnh sẽ như sau:

WINNT /s:e:\i386 /u:unattend.txt /udf:server01,unattend.udf

CÂU HỎI VÀ BÀI TẬP BÀI 1

1. Dowload hệ điều hành Windows Server 2019
2. Cài đặt hệ điều hành Windows Server 2019
3. Thiết lập chế độ tự động cài hệ điều hành Windows Server 2019

BÀI 2: DỊCH VỤ TÊN MIỀN DNS

Mã bài: MĐ 15 - 02

Giới thiệu:

Ngày nay, mạng Internet được phát triển rộng khắp trên toàn thế giới. Để có thể khai thác và sử dụng các dịch vụ và ứng dụng trên mạng Internet chúng ta cần phải xác định được vị trí của mỗi máy tính. Mỗi máy tính đều được gán bởi một địa chỉ IP đại diện cho máy tính đó trên mạng. Tuy nhiên địa chỉ dạng này rất dài, rất khó nhớ, dẫn đến việc sử dụng dịch vụ do một máy tính trên mạng cung cấp là rất khó, hệ thống DNS được sinh ra để gán cho mỗi địa chỉ IP một tên dạng chữ tương ứng, dễ nhớ. Các tên dạng chữ này được gọi là tên miền. Các tên miền này thường có ý nghĩa liên quan đến các dịch vụ được cung cấp.

Tên miền là một danh từ dịch theo kiểu nghĩa của từng từ một (word by word) từ tiếng Anh (domain name). Thực chất tên miền là sự nhận dạng vị trí của một máy tính trên mạng Internet nói cách khác tên miền là tên của các mạng lưới, tên của các máy chủ trên mạng Internet. Mỗi địa chỉ bằng chữ này phải tương ứng với một địa chỉ IP.

Trong bài này sẽ trình bày sẽ giới thiệu về cấu trúc, hoạt động và cách phân cấp hệ thống tên miền (DNS).

Mục tiêu:

- Trình bày được cấu trúc cơ sở dữ liệu của hệ thống tên miền;
- Mô tả được sự hoạt động và phân cấp của hệ thống tên miền;
- Cài đặt và cấu hình hệ thống tên miền DNS.

Nội dung chính:

1. Tổng quan về DNS

1.1. Giới thiệu DNS

Mỗi máy tính trong mạng muốn liên lạc hay trao đổi thông tin, dữ liệu cho nhau cần phải biết rõ địa chỉ IP của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ IP này rất là khó khăn. Vì vậy, **DNS (Domain Name System)** là giải pháp dùng tên thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính.

Ban đầu do quy mô mạng ARPanet (tiền thân của mạng Internet) còn nhỏ chỉ vài trăm máy, nên chỉ có một tập tin đơn HOSTS.TXT lưu thông tin về ánh

xạ tên máy thành địa chỉ IP. Trong đó tên máy chỉ là 1 chuỗi văn bản không phân cấp (flat name). Tập tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tập tin HOSTS.TXT có các nhược điểm như sau:

- Lưu lượng mạng và máy chủ duy trì tập tin HOSTS.TXT bị quá tải do hiệu ứng "cổ chai".

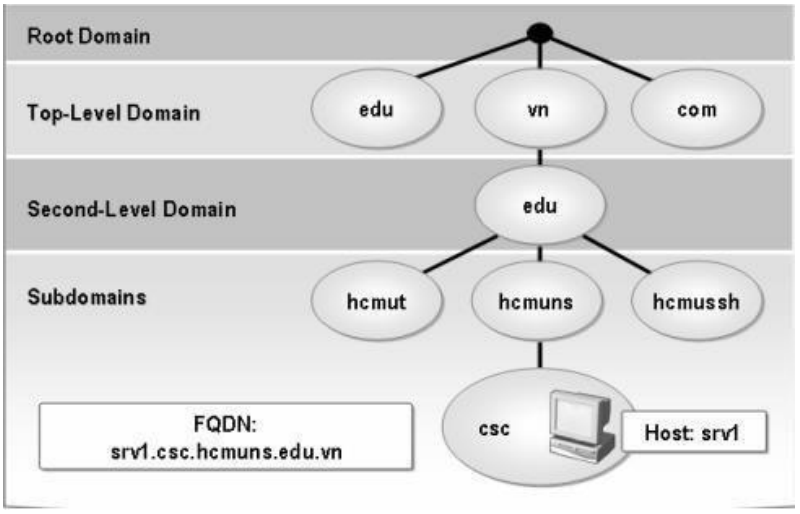
- Xung đột tên: Không thể có 2 máy tính có cùng tên trong tập tin HOSTS.TXT. Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tập tin nên có nguy cơ bị xung đột tên.

- Không đảm bảo sự toàn vẹn: việc duy trì 1 tập tin trên mạng lớn rất khó khăn. Ví dụ như khi tập tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

Tóm lại việc dùng tập tin HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó, dịch vụ DNS ra đời nhằm khắc phục các nhược điểm này. Người thiết kế cấu trúc của dịch vụ DNS là Paul Mockapetris - USC's Information Sciences Institute, và các khuyến nghị RFC của DNS là RFC 882 và 883, sau đó là RFC 1034 và 1035 cùng với 1 số RFC bổ sung như bảo mật trên hệ thống DNS, cập nhật động các bản ghi DNS …

Dịch vụ DNS hoạt động theo mô hình Client-Server: phần Server gọi là máy chủ phục vụ tên hay còn gọi là Name Server, còn phần Client là trình phân giải tên - Resolver. Name Server chứa các thông tin CSDL của DNS, còn Resolver đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (query) và gửi chúng qua đến Name Server. DNS được thi hành như một giao thức tầng Application trong mạng TCP/IP.

DNS là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình **Client-Server**. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (**replication**) và lưu tạm (**caching**). Một **hostname** trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.)



Hình 2.1 Sơ đồ tổ chức DNS

Loại tên	**Miêu tả**	**Ví dụ**
Gốc (domain root)	Nó là đỉnh của nhánh cây của tên miền. Nó xác định kết thúc của domain (fully qualified domain names FQDNs).	Đơn giản nó chỉ là dấu chấm (.) sử dụng tại cuối của tên ví như "example.microsoft.com."
Tên miền cấp một (Top-level domain)	Là hai hoặc ba ký tự xác định nước/khu vực hoặc cáctổ chức	".com", xác định tên sử dụng trong xác định là tổ chức thương mại .
Tên miền cấp hai (Second-level domain)	Nó rất đa dạng trên internet, nó có thể là tên của một công ty, một tổ chức hay một cá nhân .v.v. đăng ký trên internet.	"microsoft.com.", là tên miền cấp hai đăng ký là công ty Microsoft.
Tên miền cấp nhỏ hơn	Chia nhỏ thêm ra của tên miên cấp hai xuống thường được sử dụng như chi "example.microsoft.com." là phần quản lý tài liệu ví dụ của microsof (Subdomain) nhánh, phong ban của một cơ quan hay một chủ đề nào đó.	

Bảng 2.1 Mô tả thành phần của DNS

Cơ sở dữ liệu(CSDL) của **DNS** là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL **DNS** gọi là 1 miền (**domain**). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (**subdomain**).

Mỗi **domain** có 1 tên (**domain name**). Tên **domain** chỉ ra vị trí của nó trong CSDL **DNS**. Trong **DNS** tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm.

Tên nhãn bên phải trong mỗi **domain name** được gọi là **top-level domain**. Trong ví dụ trước srv1.csc.hcmuns.edu.vn, vậy miền ".vn" là **top-level domain**. Bảng sau đây liệt kê một số **top-level domain**.

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Bảng 2.2 Ý nghĩa một số top-level domain của tổ chức

Bên cạnh đó, mỗi nước cũng có một **top-level domain**. Ví dụ **top-leveldomain** của Việt Nam là .vn, Mỹ là .us

Ví dụ về tên miền của một số quốc gia

Tên miền quốc gia	Tên quốc gia
.vn	Việt Nam
.us	Mỹ
.uk	Anh
.jp	Nhật Bản
.ru	Nga
.cn	Trung Quốc

Bảng 2.3 Ý nghĩa một số top-level domain của quốc gia

1.2. Đặc điểm của DNS trong Windows Server

- Conditional forwarder: Cho phép **Name Server** chuyển các yêu cầu phân giải dựa theo tên domain trong yêu cầu truy vấn.

- **Stub zone**: hỗ trợ cơ chế phân giải hiệu quả hơn.

- Đồng bộ các **DNS zone** trong **Active Directory** (**DNS zone replication in Active Directory**).

- Cung cấp một số cơ chế bảo mật tốt hơn trong các hệ thống **Windows** trước đây.

- Luân chuyển (**Round robin**) tất cả các loại **RR**.

- Cung cấp nhiêu cơ chế ghi nhận và theo dõi sự cố lỗi trên **DNS**.

- Hỗ trợ giao thức **DNS Security Extensions** (**DNSSEC**) để cung cấp các tính năng bảo mật cho việc lưu trữ và nhân bản (**replicate**) **zone**.

- Cung cấp tính năng **EDNS0** (**Extension Mechanisms for DNS**) để cho phép **DNS Requestor** quản bá những **zone transfer packet** có kích thước lớn hơn 512 byte.

2. Cách phân bố dữ liệu quản lý trên tên miền

Những **root name server** (.) quản lý những **top-level domain** trên **Internet**. Tên máy và địa chỉ **IP** của những **name server** này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những **name server** này cũng có thể đặt khắp nơi trên thế giới.

Tên máy tính	Địa chỉ IP
H.ROOT-SERVERS.NET	128.63.2.53
B.ROOT-SERVERS.NET	128.9.0.107
C.ROOT-SERVERS.NET	192.33.4.12
D.ROOT-SERVERS.NET	128.8.10.90
E.ROOT-SERVERS.NET	192.203.230.10
I.ROOT-SERVERS.NET	192.36.148.17
F.ROOT-SERVERS.NET	192.5.5.241
F.ROOT-SERVERS.NET	39.13.229.241
G.ROOT-SERVERS.NET	192.112.88.4

A.ROOT-SERVERS.NET	198.41.0.4

Bảng 2.4 Tên máy và địa chỉ IP của một số name server

Thông thường một tổ chức được đăng ký một hay nhiều domain name. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều name server và duy trì cơ sở dữ liệu cho tất cả những máy tính trong domain. Những name server của tổ chức được đăng ký trên Internet. Một trong những name server này được biết như là Primary Name Server. Nhiều Secondary Name Server được dùng để làm backup cho Primary Name Server. Trong trường hợp Primary bị lỗi, Secondary được sử dụng để phân giải tên.

Primary Name Server có thể tạo ra những subdomain và ủy quyền những subdomain này cho những Name Server khác.

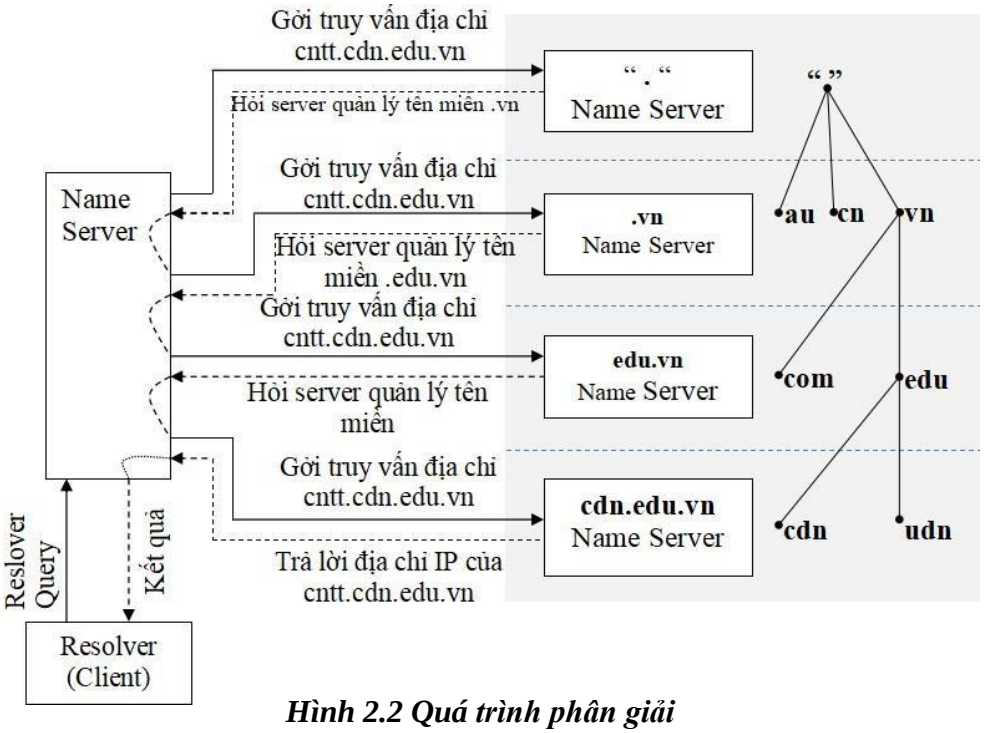
3. Cơ chế phân giải tên

3.1. Phân giải tên miền thành địa chỉ IP

Root name server : Là máy chủ quản lý các **name server** ở mức **top-level domain**. Khi có truy vấn về một tên miền nào đó thì **Root Name Server** phải cung cấp tên và địa chỉ **IP** của **name server** quản lý **top-level domain** (Thực tế là hầu hết các **root server** cũng chính là máy chủ quản lý **top-level domain**) và đến lượt các **name server** của **top-level domain** cung cấp danh sách các **name server** có quyền trên các **second-level domain** mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

Qua trên cho thấy vai trò rất quan trọng của **root name server** trong quá trình phân giải tên miền. Nếu mọi **root name server** trên mạng **Internet** không liên lạc được thì mọi yêu cầu phân giải đều không thực hiện được.

Hình vẽ dưới mô tả quá trình phân giải cntt.edu.vn trên mạng **Internet**



Hình 2.2 Quá trình phân giải

Client sẽ gửi yêu cầu cần phân giải địa chỉ **IP** của máy tính có tên cntt.DVDn.edu.vn đến **name server** cục bộ. Khi nhận yêu cầu từ **Resolver**, **Name Server** cục bộ sẽ phân tích tên này và xét xem tên miền này có do mình quản lý hay không. Nếu như tên miền do **Server** cục bộ quản lý, nó sẽ trả lời địa chỉ **IP** của tên máy đó ngay cho **Resolver**. Ngược lại, server cục bộ sẽ truy vấn đến một **Root Name Server** gần nhất mà nó biết được. **Root Name Server** sẽ trả lời địa chỉ IP của **Name Server** quản lý miền **vn**. Máy chủ **name server** cục bộ lại hỏi tiếp **name server** quản lý miền **vn** và được tham chiếu đến máy chủ quản lý miền **edu.vn**. Máy chủ quản lý **edu.vn** chỉ dẫn máy **name server** cục bộ tham chiếu đến máy chủ quản lý miền **DVDn.edu.vn**. Cuối cùng máy **name server** cục bộ truy vấn máy chủ quản lý miền **DVDn.edu.vn** và nhận được câu trả lời.

Các loại truy vấn : Truy vấn có thể ở 2 dạng :

- Truy vấn đệ quy (**recursive query**) : khi **name server** nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được. **Name server** không thể tham chiếu truy vấn đến một **name server** khác. **Name server** có thể gửi truy vấn dạng đệ quy hoặc tương tác đến **name server** khác nhưng phải thực hiện cho đến khi nào có kết quả mới thôi.
- Truy vấn tương tác (**Iteractive query**): khi **name server** nhận được truy vấn dạng này, nó trả lời cho **Resolver** với thông tin tốt nhất mà nó có được vào thời điểm lúc đó. Bản thân **name server** không thực hiện bất cứ

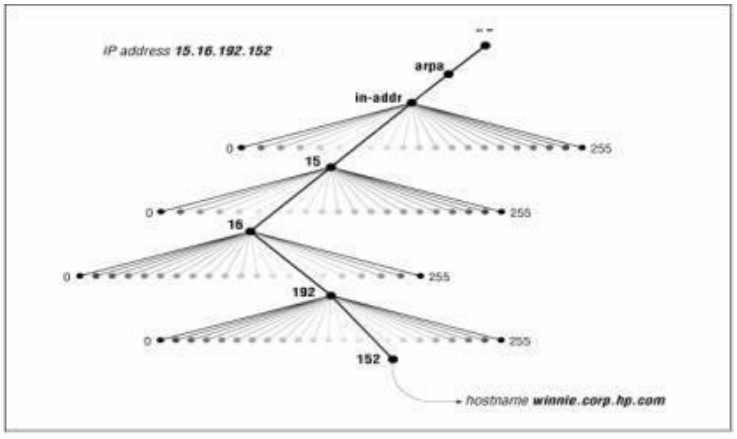
một truy vấn nào thêm. Thông tin tốt nhất trả về có thể lấy từ dữ liệu cục bộ (kể cả **cache**). Trong trường hợp **name server** không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của **name server** gần nhất mà nó biết.

3.2. Phân giải IP thành tên máy tính

Ánh xạ địa chỉ **IP** thành tên máy tính được dùng để diễn dịch các tập tin log cho dễ đọc hơn. Nó còn dùng trong một số trường hợp chứng thực trên hệ thống **UNIX** (kiểm tra các tập tin .rhost hay host.equiv). Trong không gian tên miền đã nói ở trên dữ liệu -bao gồm cả địa chỉ **IP**- được lập chỉ mục theo tên miền. Do đó với một tên miền đã cho việc tìm ra địa chỉ **IP** khá dễ dàng.

Để có thể phân giải tên máy tính của một địa chỉ **IP**, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ **IP**. Phần không gian này có tên miền là **in- addr.arpa**.

Mỗi nút trong miền **in-addr.arpa** có một tên nhãn là chỉ số thập phân của địa chỉ **IP**. Ví dụ miền **in- addr.arpa** có thể có 256 **subdomain**, tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi **subdomain** lại có 256 **subdomain** con nữa ứng với byte thứ hai. Cứ như thế và đến byte thứ tư có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ **IP** tương ứng



Hình 2.3 Phân giải IP thành tên máy tính

* *Lưu ý*: khi đọc tên miền địa chỉ **IP** sẽ xuất hiện theo thứ tự ngược. Ví dụ nếu địa chỉ **IP** của máy winnie.corp.hp.com là 15.16.192.152, khi ánh xạ vào miền in-addr.arpa sẽ là 152.192.16.15.in- addr.arpa.

4. Một số khái niệm cơ bản

4.1. Domain name và zone

Một miền gồm nhiều thực thể nhỏ hơn gọi là miền con (**subdomain**). Ví dụ, miền **ca** bao gồm nhiều miền con như **ab.ca, on.ca, qc.ca,..** . Bạn có thể ủy quyền một số miền con cho những **DNS Server** khác quản lý. Những miền và miền con mà **DNS Server** được quyền quản lý gọi là **zone**. Như vậy, một **Zone** có thể gồm một miền, một hay nhiều miền con.

Các loại **zone**:

- **Primary zone**: Cho phép đọc và ghi cơ sở dữ liệu.
- **Secondary zone**: Cho phép đọc bản sao cơ sở dữ liệu.
- **Stub zone**: chứa bản sao cơ sở dữ liệu của **zone** nào đó, nó chỉ chứa chỉ một vài **RR(Resource Record)**.

4.2. Fuly Qualified Domain Name (FQDN)

Mỗi nút trên cây có một tên gọi(không chứa dấu chấm) dài tối đa 63 ký tự. Tên rỗng dành riêng cho gốc (**root**) cao nhất và biểu diễn bởi dấu chấm. Một tên miền đầy đủ của một nút chính là chuỗi tuần tự các tên gọi của nút hiện tại đi ngược lên nút gốc, mỗi tên gọi cách nhau bởi dấu chấm. Tên miền có xuất hiện dấu chấm sau cùng được gọi là tên tuyệt đối (**absolute**) khác với tên tương đối là tên không kết thúc bằng dấu chấm. Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (**Fully Qualified Domain Name – FQDN**).

4.3. Sự uỷ quyền (Delegation)

Một trong các mục tiêu khi thiết kế hệ thống DNS là khả năng quản lý phân tán thông qua cơ chế uỷ quyền (delegation). Trong một miền có thể tổ chức thành nhiều miền con, mỗi miền con có thể được uỷ quyền cho một tổ chức khác và tổ chức đó chịu trách nhiệm duy trì thông tin trong miền con này. Khi đó, miền cha chỉ cần một con trỏ trỏ đến miền con này để tham chiếu khi có các truy vấn.

Không phải một miền luôn luôn tổ chức miền con và uỷ quyền toàn bộ cho các miền con này, có thể chỉ có vài miền con được ủy quyền.

4.4. Forwarders

Là kỹ thuật cho phép Name Server nội bộ chuyển yêu cầu truy vấn cho các Name Server khác để phân giải các miền bên ngoài.

4.5. Stub zone

Là zone chứa bảng sao cơ sở dữ liệu DNS từ master name server, Stub zone chỉ chứa các resource record cần thiết như : A, SOA, NS, một hoặc vài địa chỉ của master name server hỗ trợ cơ chế cập nhật Stub zone, chế chứng thực name server trong zone và cung cấp cơ chế phân giải tên miền được hiệu quả hơn, đơn giản hóa công tác quản trị.

4.6. Dynamic DNS

Dynamic DNS là phương thức ánh xạ tên miền tới địa chỉ IP có tần xuất thay đổi cao. Dịch vụ DNS động (Dynamic DNS) cung cấp một chương trình đặc biệt chạy trên máy tính của người sử dụng dịch vụ dynamic DNS gọi là Dynamic Dns Client. Chương trình này giám sát sự thay đổi địa chỉ IP tại host và liên hệ với hệ thống DNS mỗi khi địa chỉ IP của host thay đổi và sau đó update thông tin vào cơ sở dữ liệu DNS về sự thay đổi địa chỉ đó.

4.7. Active directory-integrated zone

Sử dụng Active Directory-integrated zone có một số thuận lợi sau:

- DNS zone lưu trữ trong trong Active Directory, nhờ cơ chế này mà dữ liệu được bảo mật hơn.

- Sử dụng cơ chế nhân bản của Active Directory để cập nhận và sao chép cơ sở dữ liệu DNS.

- Sử dụng secure dynamic update.

- Sử dụng nhiều master name server để quản lý tên miền thay vì sử dụng một master name server.

5. Phân loại Domain Name Server

5.1. Primary Name Server

Mỗi miền phải có một Primary Name Server. Server này được đăng kí trên Internet để quản lý miền. Mọi người trên Internet đều biết tên máy tình và địa chỉ IP của Server này. Người quản trị DNS sẽ tổ chức những tập tin CSDL trên Primary Name Server. Server này có nhiệm vụ phân giải tất cả các máy trong miền hay zone.

5.2. Sercondary Name Server

Mỗi miền có một Primary Name Server để quản lý CSDL của miền. Nếu như Server này tạm ngưng hoạt động vì một lý do nào đó thì việc phân giải tên máy tính thành địa chỉ IP và ngược lại xem như bị gián đoạn. Việc gián đoạn

này làm ảnh hưởng rất lớn đến những tổ chức có nhu cầu trao đổi thông tin ra ngoài Internet cao. Nhằm khắc phục nhược điểm này, những nhà thiết kế đã đưa ra một Server dự phòng gọi là Secondary(hay Slave) Name Server. Server này có nhiệm vụ sao lưu tất cả những dữ liệu trên Primary Name Server và khi Primary Name Server bị gián đoạn thì nó sẽ đảm nhận việc phân giải tên máy tính thành địa chỉ IP và ngược lại. Trong một miền có thể có một hay nhiều Secondary Name Server. Theo một chu kỳ, Secondary sẽ sao chép và cập nhật CSDL từ Primary Name Server. Tên và địa chỉ IP của Secondary Name Server cũng được mọi người trên Internet biết đến.

5.3. Caching Name Server

Caching Name Server không có bất kỳ tập tin CSDL nào. Nó có chức năng phân giải tên máy trên những mạng ở xa thông qua những Name Server khác. Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những thông tin này nhằm mục đích:

- Làm tăng tốc độ phân giải bằng cách sử dụng cache.
- Giảm bớt gánh nặng phân giải tên máy cho các Name Server.
- Giảm việc lưu thông trên những mạng lớn.

6. Resource record (RR)

RR là mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu DNS, các mẫu tin này được lưu trong các file cơ sở dữ liệu DNS (\systemroot\system32\dns).

6.1. SOA (Start of Authority)

Trong mỗi tập tin CSDL phải có một và chỉ một record SOA (start of authority). Record SOA chỉ ra rằng máy chủ Name Server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.

Cú pháp của record SOA.

[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email] (

serial number;

refresh number;

retry number;

experi number;

Time-to-live number)

- Serial : Áp dụng cho mọi dữ liệu trong zone và là 1 số nguyên. Trong ví dụ, giá trị này bắt đầu từ 1 nhưng thông thường người ta sử dụng theo định dạng thời gian như 2012032501. Định dạng này theo kiểu YYYYMMDDNN, trong đó YYYY là năm, MM là tháng, DD là ngày và NN số lần sửa đổi dữ liệu zone trong ngày. Bất kể là theo định dạng nào, luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu zone. Khi máy máy chủ Secondary liên lạc với máy chủ Primary, trước tiên nó sẽ hỏi số serial. Nếu số serial của máy Secondary nhỏ hơn số serial của máy Primary tức là dữ liệu zone trên Secondary đã cũ và sau đó máy Secondary sẽ sao chép dữ liệu mới từ máy Primary thay cho dữ liệu đang có hiện hành.

- Refresh: Chỉ ra khoảng thời gian máy chủ Secondary kiểm tra dữ liệu zone trên máy Primary để cập nhật nếu cần. Trong ví dụ trên thì cứ mỗi 3 giờ máy chủ Secondary sẽ liên lạc với máy chủ Primary để cập nhật dữ liệu nếu có. Giá trị này thay đổi tuỳ theo tần suất thay đổi dữ liệu trong zone.

- Retry: nếu máy chủ Secondary không kết nối được với máy chủ Primary theo thời hạn mô tả trong refresh (ví dụ máy chủ Primary bị shutdown vào lúc đó thì máy chủ Secondary phải tìm cách kết nối lại với máy chủ Primary theo một chu kỳ thời gian mô tả trong retry. Thông thường giá trị này nhỏ hơn giá trị refresh.

- Expire: Nếu sau khoảng thời gian này mà máy chủ Secondary không kết nối được với máy chủ Primary thì dữ liệu zone trên máy Secondary sẽ bị quá hạn. Một khi dữ liệu trên Secondary bị quá hạn thì máy chủ này sẽ không trả lời mọi truy vấn về zone này nữa. Giá trị expire này phải lớn hơn giá trị refresh và giá trị retry.

- TTL: Viết tắt của time to live. Giá trị này áp dụng cho mọi record trong zone và được đính kèm trong thông tin trả lời một truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy chủ Name Server khác cache lại thông tin trả lời. Việc cache thông tin trả lời giúp giảm lưu lượng truy vấn DNS trên mạng.

6.2. NS(Name Server)

Record tiếp theo cần có trong zone là NS (name server) record. Mỗi Name Server cho zone sẽ có một NS record.

Cú pháp:

```
[domain_name]  IN  NS  [DNS-Server_name]
```

Ví dụ: Record NS sau:

qtm.com. IN NS dnsserver.qtm.com.

qtm.com. IN NS server.qtm.com.

chỉ ra 2 name servers cho miền qtm.com

6.3. A (Address) và CNAME(Canonical Name)

Record A (Address) ánh xạ tên máy (hostname) vào địa chỉ IP. Record CNAME (canonical name) tạo tên bí danh alias trỏ vào một tên canonical. Tên canonical là tên host trong record A hoặc lại trỏ vào 1 tên canonical khác.

Cú pháp record A:

[tên-máy-tính] IN A [địa-chỉ-IP]

Ví dụ: record A trong tập tin db.qtm

server.qtm.com. IN A 172.29.14.1

diehard.qtm.com. IN A 172.29.14.4

// Multi-homed hosts

server.qtm.com. IN A 172.29.14.1

server.qtm.com. IN A 192.253.253.1

6.4. AAAA

Ánh xạ tên máy (hostname) vào địa chỉ IP version 6

Cú pháp:

[tên-máy-tính] IN AAAA [địa-chỉ-IPv6]

Ví dụ

Server IN AAAA 1243:123:456:789:1:2:3:456ab

6.5. SRV

Cung cấp cơ chế định vị dịch vụ, Active Directory sử dụng Resource Record này để xác định domain controllers, global catalog servers, Lightweight Directory Access Protocol (LDAP) servers.

Các field trong SVR:

- Tên dịch vụ service.
- Giao thức sử dụng.
- Tên miền (domain name).
- TTL và class.

- Priority.
- Weight (hỗ trợ load balancing).
- Port của dịch vụ.
- Target chỉ định FQDN cho host hỗ trợ dịch vụ.

6.6. MX (Mail Exchange)

DNS dùng record MX trong việc chuyển mail trên mạng Internet. Ban đầu chức năng chuyển mail dựa trên 2 record: record MD (mail destination) và record MF (mail forwarder) records. MD chỉ ra đích cuối cùng của một thông điệp mail có tên miền cụ thể. MF chỉ ra máy chủ trung gian sẽ chuyển tiếp mail đến được máy chủ đích cuối cùng. Tuy nhiên, việc tổ chức này hoạt động không tốt. Do đó, chúng được tích hợp lại thành một record là MX. Khi nhận được mail, trình chuyển mail (mailer) sẽ dựa vào record MX để quyết định đường đi của mail. Record MX chỉ ra một mail exchanger cho một miền - mail exchanger là một máy chủ xử lý (chuyển mail đến mailbox cục bộ hay làm gateway chuyển sang một giao thức chuyển mail khác như UUCP) hoặc chuyển tiếp mail đến một mail exchanger khác (trung gian) gần với mình nhất để đến tới máy chủ đích cuối cùng hơn dùng giao thức SMTP (Simple Mail Transfer Protocol).

Để tránh việc gửi mail bị lặp lại, record MX có thêm 1 giá trị bổ sung ngoài tên miền của mail exchanger là 1 số thứ tự tham chiếu. Đây là giá trị nguyên không dấu 16-bit (0-65535) chỉ ra thứ tự ưu tiên của các mail exchanger.

Cú pháp record MX:

[domain_name] IN MX [priority] [mail-host]

Ví dụ record MX sau :

qtm.com. IN MX 10 mailserver.qtm.com.

Chỉ ra máy chủ mailserver.qtm.com là một mail exchanger cho miền qtm.com với số thứ tự tham chiếu 10.

Chú ý: các giá trị này chỉ có ý nghĩa so sánh với nhau. Ví dụ khai báo 2 record MX:

qtm.com. IN MX 1 listo.qtm.com. qtm.com. IN MX 2 hep.qtm.com.

Trình chuyển thư mailer sẽ thử phân phát thư đến mail exchanger có số thứ tự tham chiếu nhỏ nhất trước. Nếu không chuyển thư được thì mail exchanger

với giá trị kế sau sẽ được chọn. Trong trường hợp có nhiều mail exchanger có cùng số tham chiếu thì mailer sẽ chọn ngẫu nhiên giữa chúng.

6.7. PTR (Pointer)

Record PTR (pointer) dùng để ánh xạ địa chỉ IP thành Hostname.

Cú pháp:

[Host-ID.{Reverse_Lookup_Zone}] IN PTR [tên-máy-tính]

Ví dụ:

Các record PTR cho các host trong mạng 192.249.249:

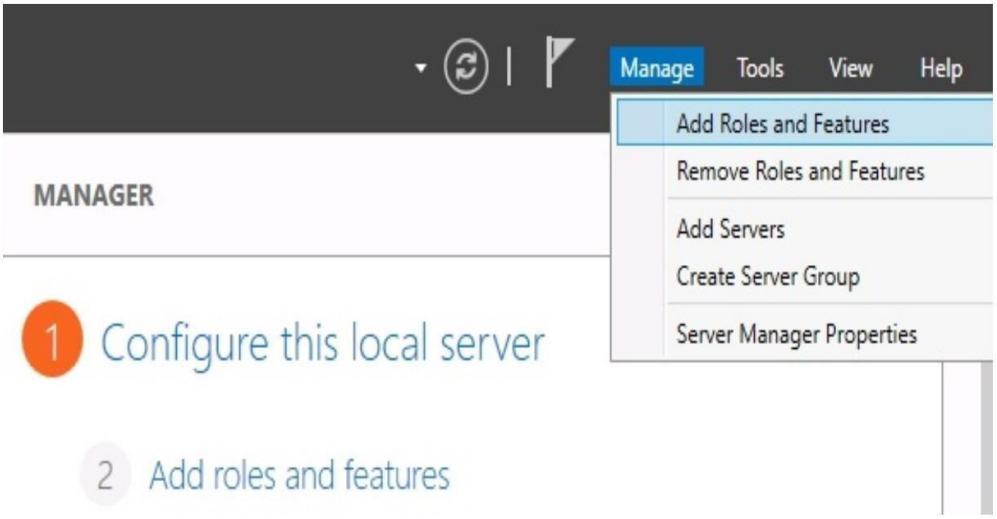
1.14.29.172.in-addr.arpa. IN PTR server.qtm.com.

7. Cài đặt và cấu hình DNS

7.1. Các bước cài đặt DNS

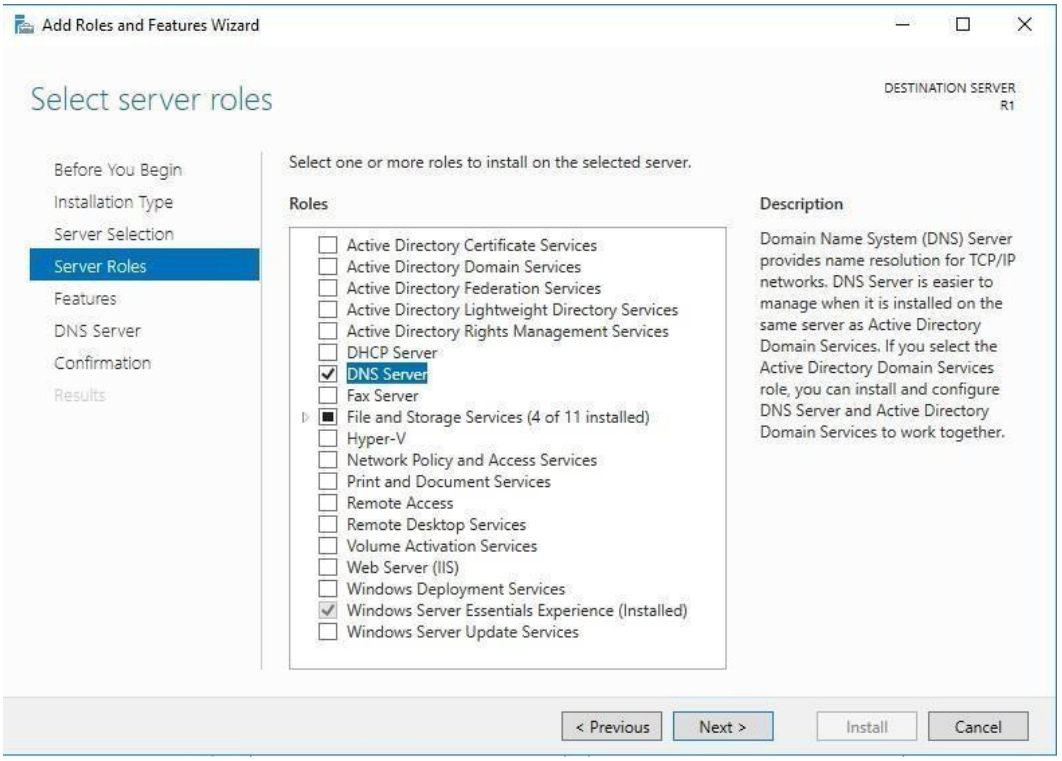
- Đặt địa chỉ IP cho máy server

- Mở Manager ->Manage->Add Roles and Features



Hình 2.4 Cài đặt và cấu hình DNS

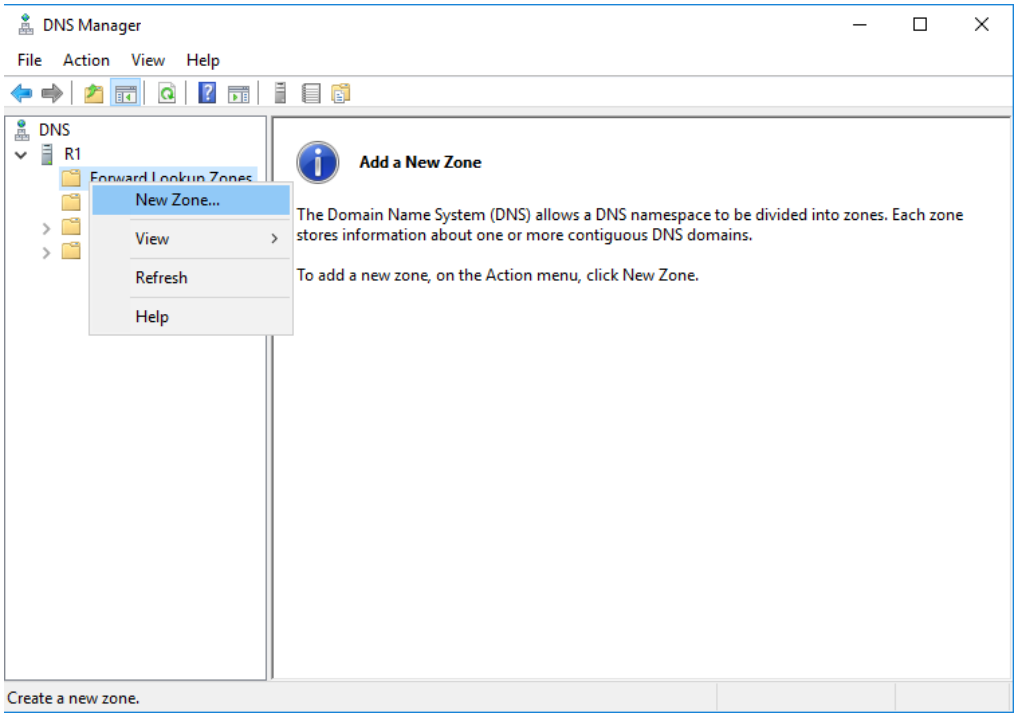
- Check vào DNS



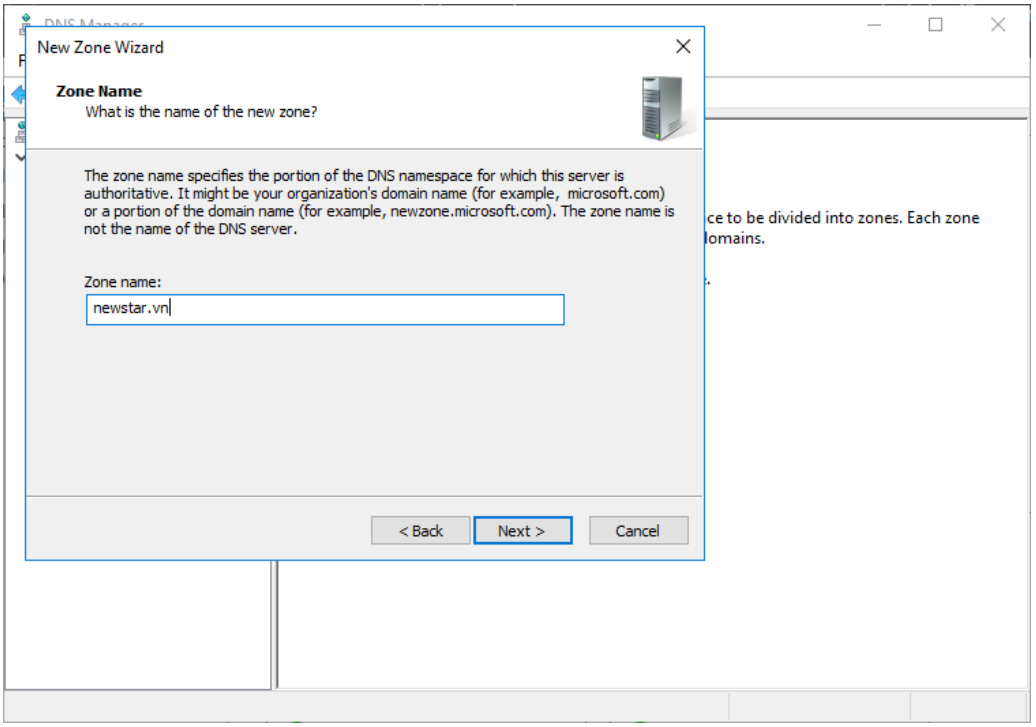
Hình 2.5 Cài Role DNS Server

7.2. Cấu hình dịch vụ DNS

+ Tạo Zone mới để phân giải tên miền

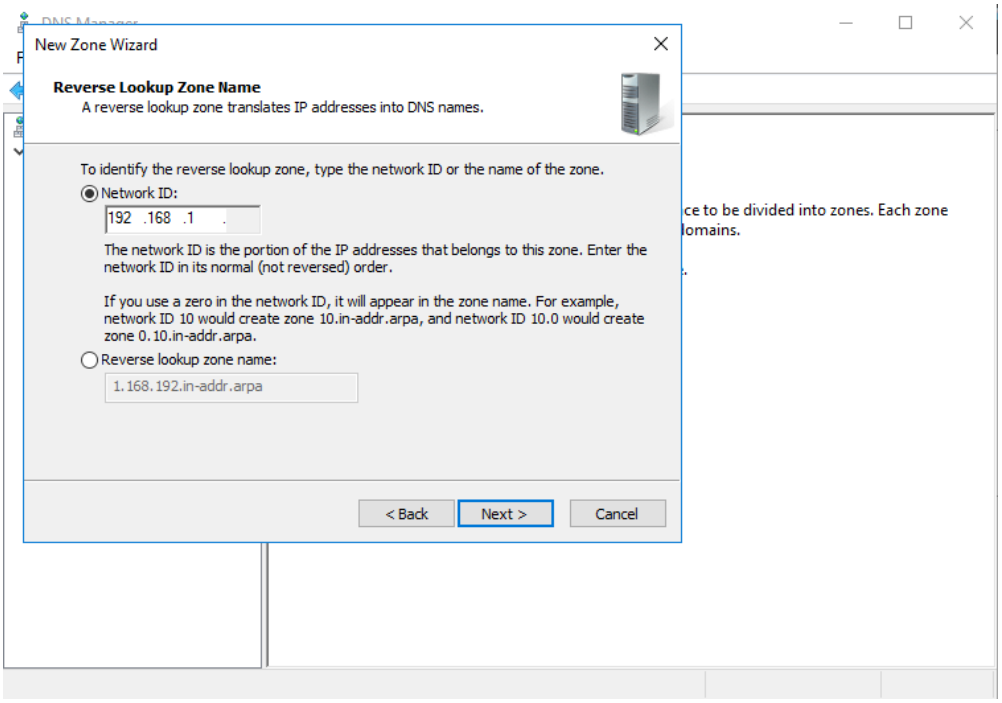


Hình 2.6 Tạo Zone mới

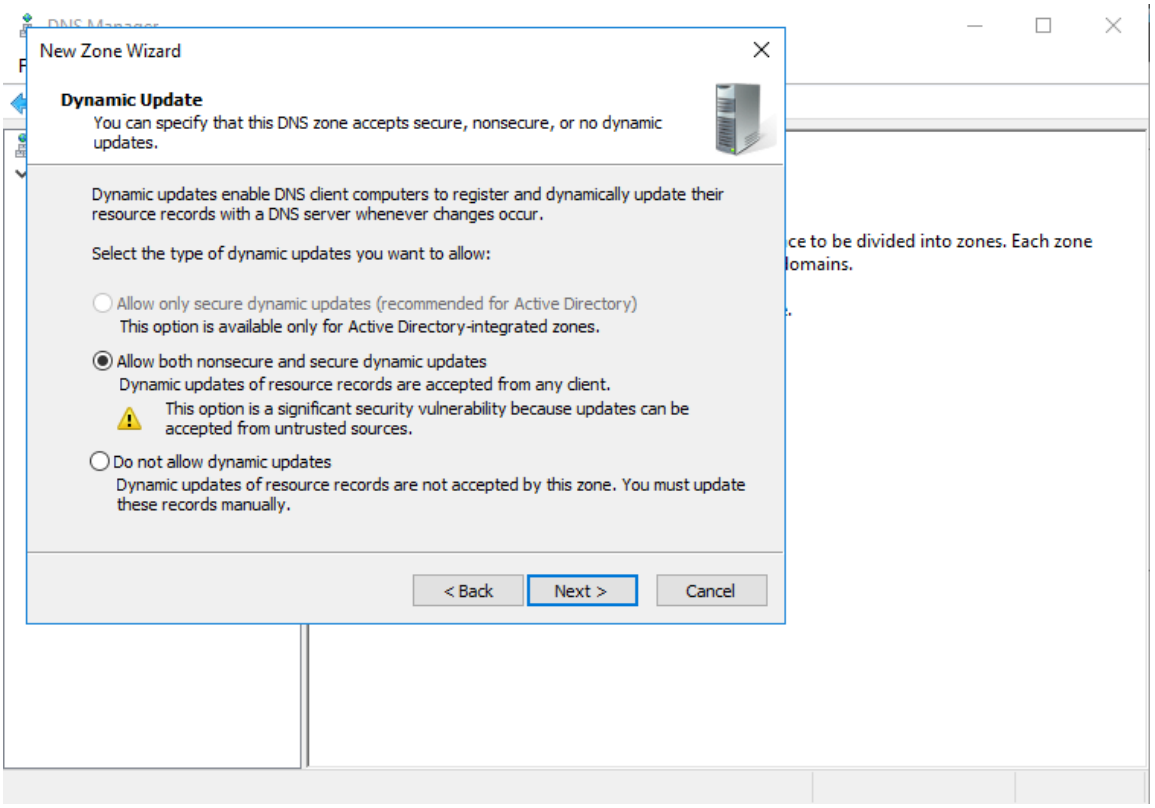


Hình 2.7 Đặt tên cho zone là newstar.vn

+ Nhập địa chỉ IP để phân giải tên miền

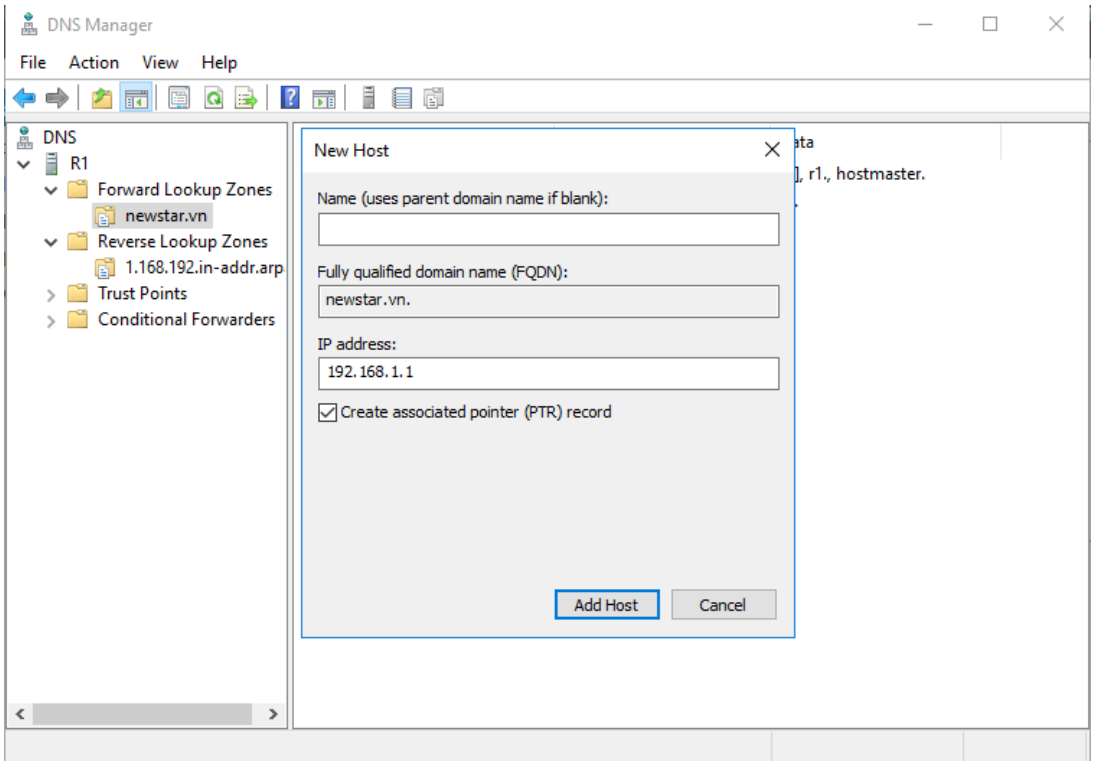


Hình 2.8 Tạo Reverse lookup zone



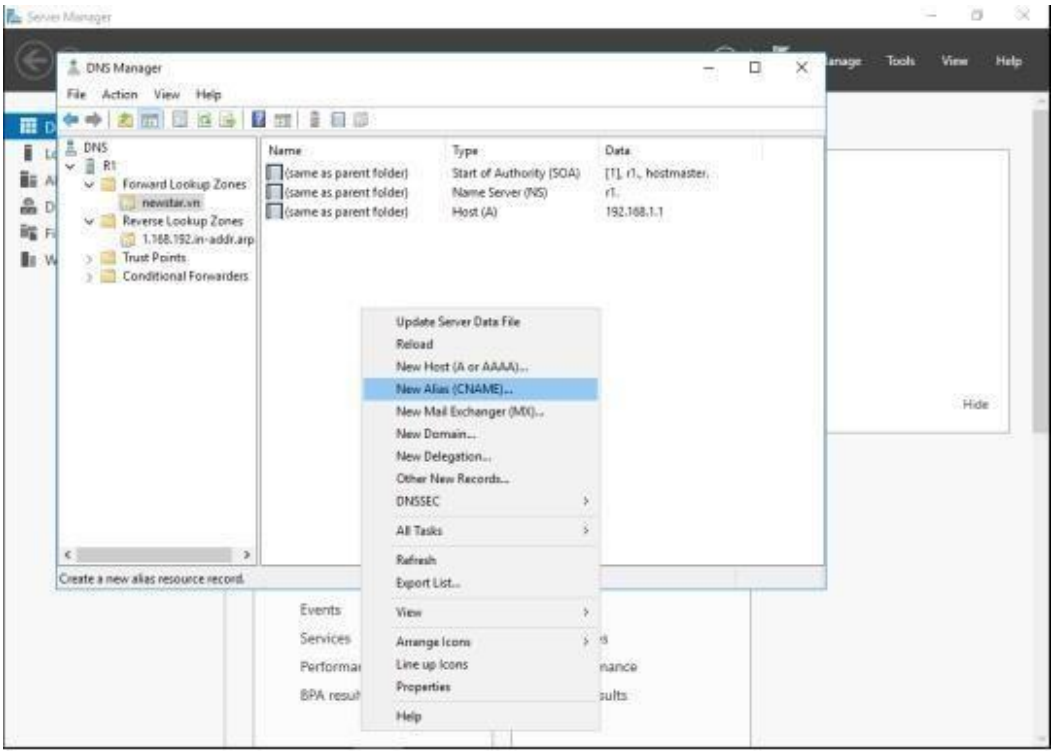
Hình 2.9 Lựa chọn phương thức Update

+ Chọn check Create associated pointer (PTR) record để tự động add IP qua Reverse lookup Zones khi thêm host vào



Hình 2.10 Tạo new host

+ Tạo mặc danh cho tên miền newstar.vn



Hình 2.11 Tạo Alias

Sao khi cấu hình xong thì phân giải thànhcông

Hình 2.12 Kết quả phân giải tên miền thành công

CÂU HỎI VÀ BÀI TẬP BÀI 2

1. Cài đặt dịch vụ DNS.
2. Cấu hình dịch vụ DNS.

BÀI 3: ACTIVE DIRECTORY

Mã bài: MĐ 15 - 03

Giới thiệu:

Active Directory là dịch vụ hệ thống quan trọng bậc nhất với vai trò quản lý dữ liệu người dùng, máy tính, groups, và các chính sách cũng như rất nhiều thông tin khác. Vì thế triển khai hệ thống Active Directory chuẩn, tránh các sự cố liên quan là điều cần thiết.

Trong bài này chúng tôi sẽ giới thiệu những kiến thức cơ bản về Active Directory và những lợi ích trong việc thực thi Active Directory. Các thông tin về các forests, domains, organizational unit và site cũng như những kiến thức cơ bản về LDAP (Lightweight Directory Access Protocol) và Group Policy

Mục tiêu:

- Trình bày được cấu trúc của Active Directory trên windows server;
- Cài đặt và cấu hình được máy điều khiển vùng.

Nội dung chính:

1. Các mô hình mạng trong môi trường Microsoft

1.1. Mô hình Workgroup

Mô hình mạng Workgroup là một nhóm máy tính mạng cùng chia sẻ tài nguyên như file dữ liệu, máy in. Nó là một nhóm logic của các máy tính mà tất cả chúng có cùng tên nhóm. Có thể có nhiều nhóm làm việc (workgroups) khác nhau cùng kết nối trên một mạng cục bộ (LAN).

Trong mô hình này, các máy tính có quyền hạn ngang nhau và không có các máy tính chuyên dụng làm nhiệm vụ cung cấp dịch vụ hay quản lý. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình. Đồng thời, các máy tính cục bộ này cũng tự chứng thực cho người dùng cục bộ.

Mô hình mạng Workgroup cũng được coi là mạng peer-to-peer bởi vì tất cả các máy trong workgroup có quyền chia sẻ tài nguyên như nhau mà không cần sự chỉ định của Server. Mỗi máy tính trong nhóm tự bảo trì, bảo mật cơ sở dữ liệu cục bộ của nó. Điều này có nghĩa là, tất cả sự quản trị về tài khoản người dùng, bảo mật cho nguồn tài nguyên chia sẻ không được tập trung hóa. Bạn có thể kết nối tới một nhóm đã tồn tại hoặc khởi tạo một nhóm mới.

1.2. Mô hình Domain

Mô hình mạng Domain (hay mô hình Server) là một nhóm máy tính mạng cùng chia sẻ cơ sở dữ liệu thư mục tập trung (central directory database). Thư mục dữ liệu chứa tài khoản người dùng và thông tin bảo mật cho toàn bộ Domain. Thư mục dữ liệu này được biết như là thư mục hiện hành (Active Directory).

Ngược lại với mô hình Workgroup, trong mô hình Domain thì việc quản lý và chứng thực người dùng mạng tập trung tại máy tính Primary Domain Controller. Các tài nguyên mạng cũng được quản lý tập trung và cấp quyền hạn cho từng người dùng. Lúc đó trong hệ thống có các máy tính chuyên dụng làm nhiệm vụ cung cấp các dịch vụ và quản lý các máy trạm.

Trong một Domain, thư mục chỉ tồn tại trên các máy tính được cấu hình như máy điều khiển miền (domain controller). Một domain controller là một Server quản lý tất cả các khía cạnh bảo mật của Domain. Không giống như mạng Workgroup, bảo mật và quản trị trong domain được tập trung hóa. Để có Domain controller, những máy chủ (server) phải chạy dịch vụ làm Domain controller (dịch vụ được tích hợp sẵn trên các phiên bản Windows Server của Microsoft; hoặc trên Linux, ta cấu hình dịch vụ Samba để làm nhiệm vụ Domain controller,…).

Một domain không được xem như một vị trí đơn hoặc cấu hình mạng riêng biệt. Các máy tính trong cùng domain có thể ở trên một mạng LAN hoặc WAN. Chúng có thể giao tiếp với nhau qua bất kỳ kết nối vật lý nào, như: Dial-up, Integrated Services Digital Network (ISDN), Ethernet, Token Ring, Frame Relay, Satellite, Fibre Channel.

2. Active Directory

2.1. Giới thiệu

AD (Active Directory) là dịch vụ thư mục chứa các thông tin về các tài nguyên trên mạng, có thể mở rộng và có khả năng tự điều chỉnh cho phép bạn quản lý tài nguyên mạng hiệu quả. Để có thể làm việc tốt với Active Directory, chúng ta sẽ tìm hiểu khái quát về Active Directory, sau đó khảo sát các thành phần của dịch vụ này.

Các đối tượng AD bao gồm dữ liệu của người dùng (user data), máy in (printers), máy chủ (servers), cơ sở dữ liệu (databases), các nhóm người dùng (groups), các máy tính (computers), và các chính sách bảo mật (security policies).

Ngoài ra một khái niệm mới được sử dụng là *container* (tạm dịch là tập đối tượng). Ví dụ Domain là một tập đối tượng chứa thông tin người dùng, thông tin các máy trên mạng, và chứa các đối tượng khác

2.2. Directory Service

2.2.1. Giới thiệu Directory Services

Directory Services (dịch vụ danh bạ) là hệ thống thông tin chứa trong NTDS.DIT và các chương trình quản lý, khai thác tập tin này. Dịch vụ danh bạ là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống Active Directory. Một hệ thống với những tính năng vượt trội của Microsoft.

2.2.2. Các thành phần trong Directory Services

Đầu tiên, bạn phải biết được những thành phần cấu tạo nên dịch vụ danh bạ là gì? Bạn có thể so sánh dịch vụ danh bạ với một quyển sổ lưu số điện thoại. Cả hai đều chứa danh sách của nhiều đối tượng khác nhau cũng như các thông tin và thuộc tính liên quan đến các đối tượng đó.

a. Object (đối tượng).

Trong hệ thống cơ sở dữ liệu, đối tượng bao gồm các máy in, người dùng mạng, các server, các máy trạm, các thư mục dùng chung, dịch vụ mạng, … Đối tượng chính là thành tố căn bản nhất của dịch vụ danh bạ.

b. Attribute (thuộc tính).

Một thuộc tính mô tả một đối tượng. Ví dụ, mật khẩu và tên là thuộc tính của đối tượng người dùng mạng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Lấy ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ IP.

c. Schema (cấu trúc tổ chức).

Một schema định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó. Ví dụ, cho rằng tất cả các đối tượng máy in đều được định nghĩa bằng các thuộc tính tên, loại PDL và tốc độ. Danh sách các đối tượng này hình thành nên schema cho lớp đối tượng "máy in". Schema có đặc tính là tuỳ biến được, nghĩa là các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được. Nói tóm lại Schema có thể xem là một danh bạ của cái danh bạ Active Directory.

d. Container (vật chứa).

Vật chứa tương tự với khái niệm thư mục trong Windows. Một thư mục có thể chứa các tập tin và các thư mục khác. Trong Active Directory, một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng.

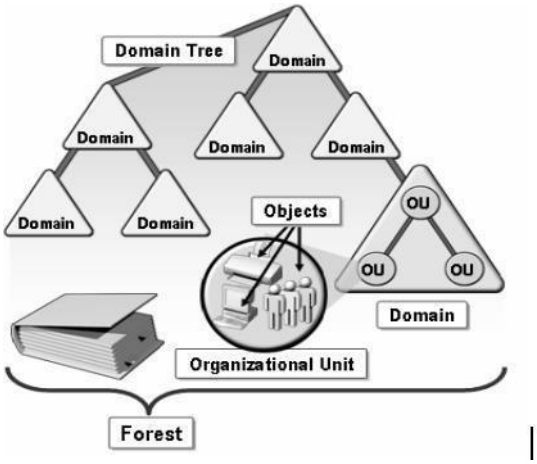
e. Global Catalog.

- Dịch vụ Global Catalog dùng để xác định vị trí của một đối tượng mà người dùng được cấp quyền truy cập. Và không chỉ có thể định vị được đối tượng bằng tên mà có thể bằng cả những thuộc tính của đối tượng.

- Khi một đối tượng được tạo mới trong Active Directory, đối tượng được gán một con số phân biệt gọi là GUID (Global Unique Identifier). GUID của một đối tượng luôn luôn cố định cho dù bạn có di chuyển đối tượng đi đến khu vực khác.

2.3. Kiến trúc của Active Directory

Gồm các thành phần: domains (vùng), organization units (đơn vị tổ chức), trees (hệ vùng phân cấp) và forests (tập hợp hệ vùng phân cấp) .



Hình 3.1 Kiến trúc của Active Directory

2.3.1. Domain

Domain là đơn vị chức năng nòng cốt của cấu trúc **logic Active Directory**. Nó là phương tiện để qui định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những qui tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các **Server** dễ dàng hơn. **Domain** đáp ứng ba chức năng chính sau:

-Đóng vai trò như một khu vực quản trị (**administrative boundary**) các đối tượng, là một tập hợp các định nghĩa quản trị cho các đối tượng chia sẻ như: có chung một cơ sở dữ liệu thư mục, các chính sách bảo mật, các quan hệ ủy quyền với các **domain** khác.

- Giúp chúng ta quản lý bảo mật các các tài nguyên chia sẻ.

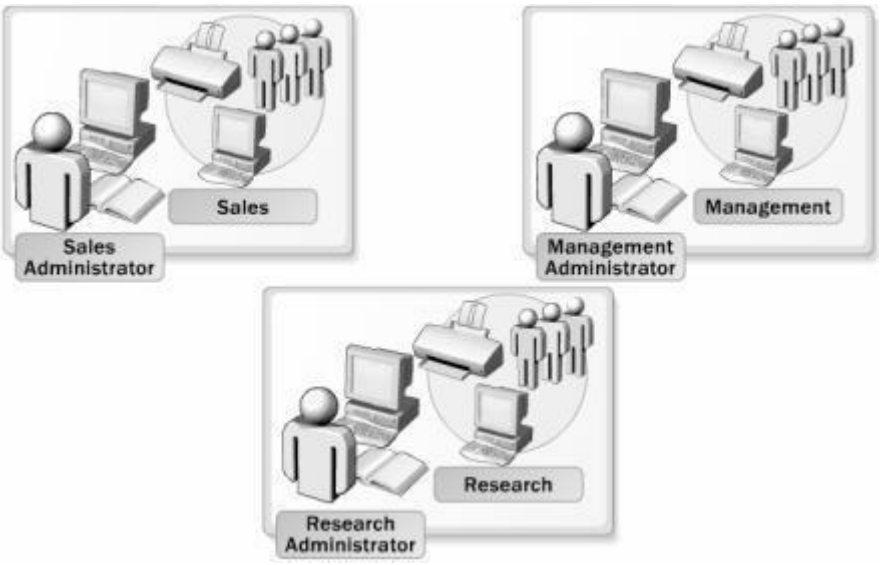
- Cung cấp các **Server** dự phòng làm chức năng điều khiển vùng (**domain controller**), đồng thời ảm bảo các thông tin trên các **Server** này được được đồng bộ với nhau.

2.3.2. Organizational Units.

Organizational Unit hay **OU** là đơn vị nhỏ nhất trong hệ thống **AD**, nó được xem là một vật chứa các đối tượng (**Object**) được dùng để sắp xếp các đối tượng khác nhau phục vụ cho mục đích quản trị của bạn. **OU** cũng được thiết lập dựa trên **subnet IP** và được định nghĩa là "một hoặc nhiều **subnet** kết nối tốt với nhau". Việc sử dụng **OU** có hai công dụng chính sau:

- Trao quyền kiểm soát một tập hợp các tài khoản người dùng, máy tính hay các thiết bị mạng cho một nhóm người hay một phụ tá quản trị viên nào đó (sub-administrator), từ đó giảm bớt công tác quản trị cho người quản trị toàn bộ hệ thống.

- Kiểm soát và khóa bớt một số chức năng trên các máy trạm của người dùng trong OU thông qua việc sử dụng các đối tượng chính sách nhóm (**GPO**).



Hình 3.2 Organizational Units

2.3.3. Domain Tree

Domain Tree là cấu trúc bao gồm nhiều **domain** được sắp xếp có cấp bậc theo cấu trúc hình cây. **Domain** tạo ra đầu tiên được gọi là **domain root** và nằm ở gốc của cây thư mục. Tất cả các **domain** tạo ra sau sẽ nằm bên dưới **domain root** và được gọi là **domain** con (**child domain**). Tên của các **domain** con phải khác biệt nhau. Khi một **domain root** và ít nhất một **domain** con được tạo ra thì hình thành một cây **domain**. Khái niệm này bạn sẽ thường nghe thấy khi làm việc với một dịch vụ thư mục. Bạn có thể thấy cấu trúc sẽ có hình dáng của một cây khi có nhiều nhánh xuất hiện.

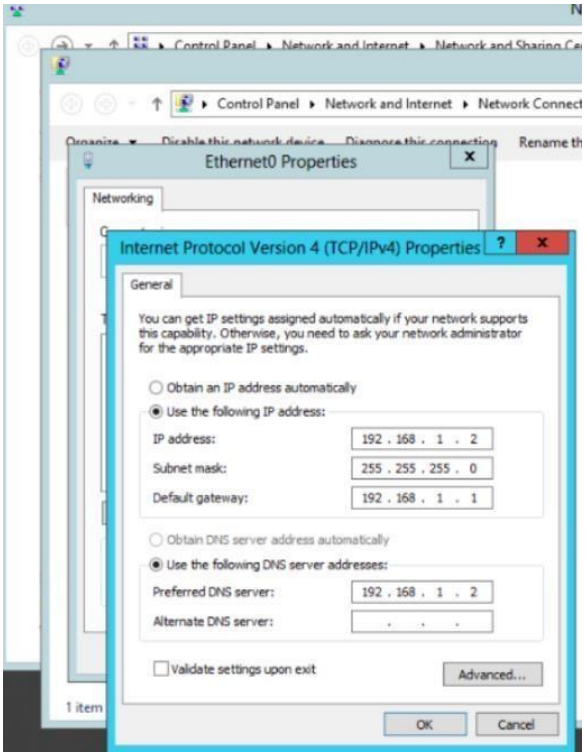
2.3.4. Forest

Forest (rừng) được xây dựng trên một hoặc nhiều **Domain Tree**, nói cách khác **Forest** là tập hợp các **Domain Tree** có thiết lập quan hệ và ủy quyền cho nhau. Ví dụ giả sử một công ty nào đó, chẳng hạn như **Microsoft**, thu mua một công ty khác. Thông thường, mỗi công ty đều có một hệ thống **Domain Tree** riêng và để tiện quản lý, các cây này sẽ được hợp nhất với nhau bằng một khái niệm là rừng.

3. Cài đặt và cấu hình Active Directory

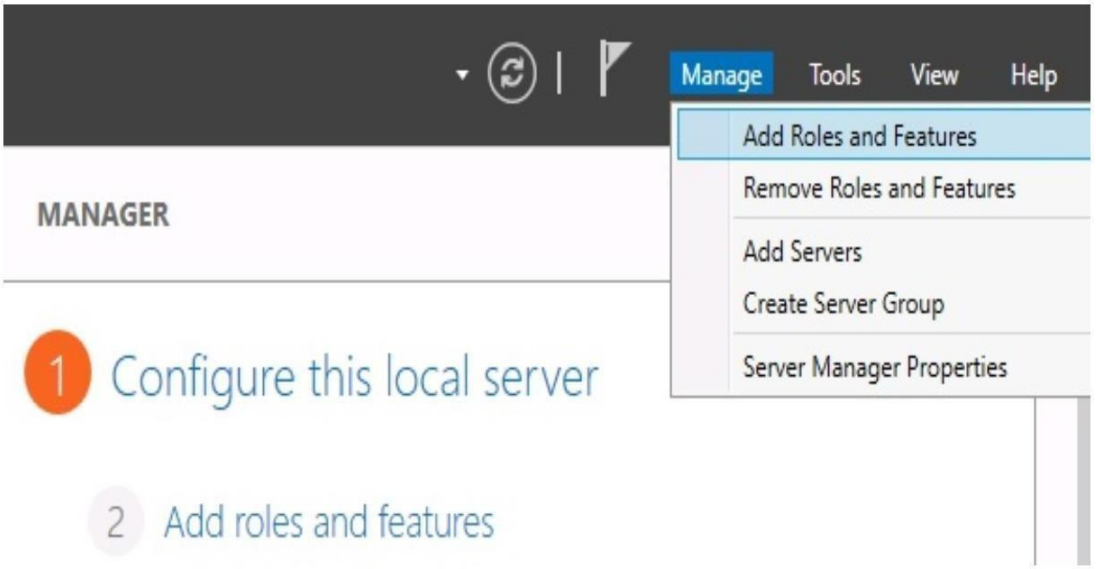
3.1. Nâng cấp Server thành Domain Controller

- Đặt IP tĩnh cho máy cần lên Domain.



Hình 3.3 Đặt địa chỉ IP cho máy

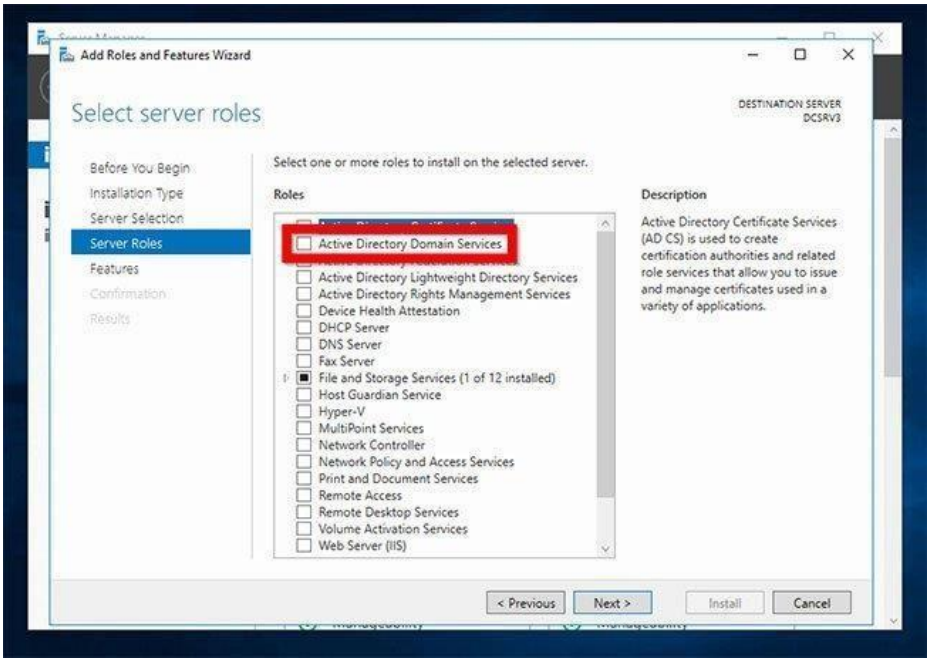
- Chọn **Add Roles and Features**



Hình 2.16 Cài đặt cấu hình AD

- Chọn **Next**

- Chọn **Active Directory Domain Services**



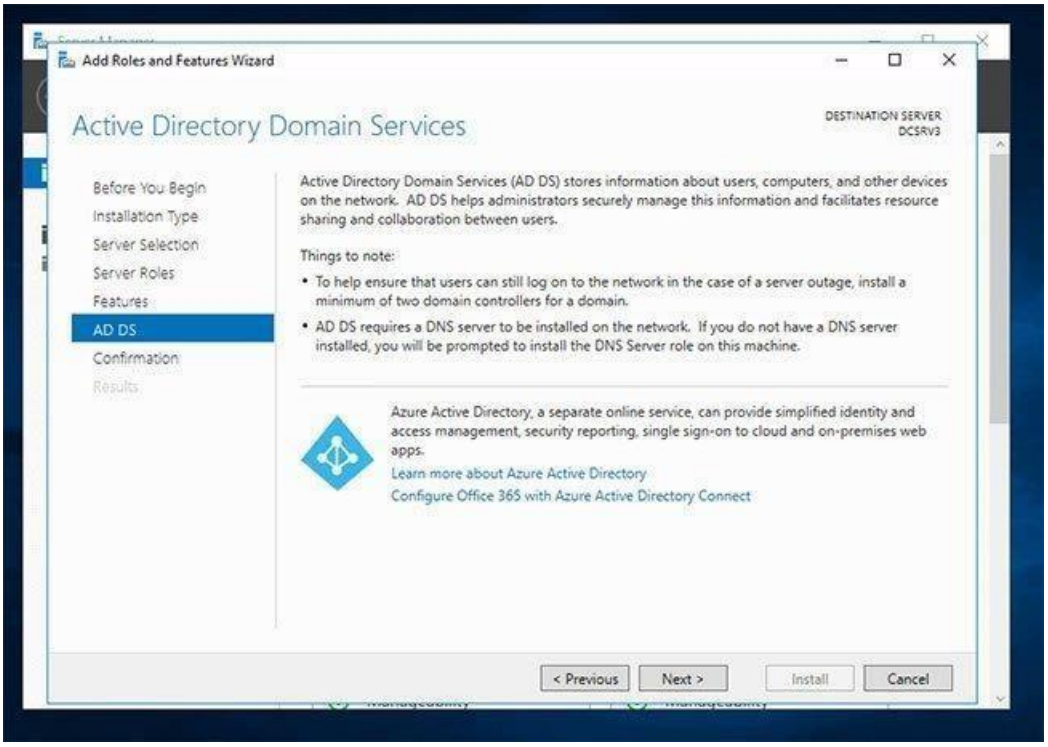
Hình 3.4 Cài đặt AD

- Khi quay lại **Select server roles**, nhấp vào **Next.**

- Sau đó tại màn hình **Select Features**, nhấp vào **Next.**

- Đọc thông tin được cung cấp về AD DS. Sau đó nhấp vào **Next.**

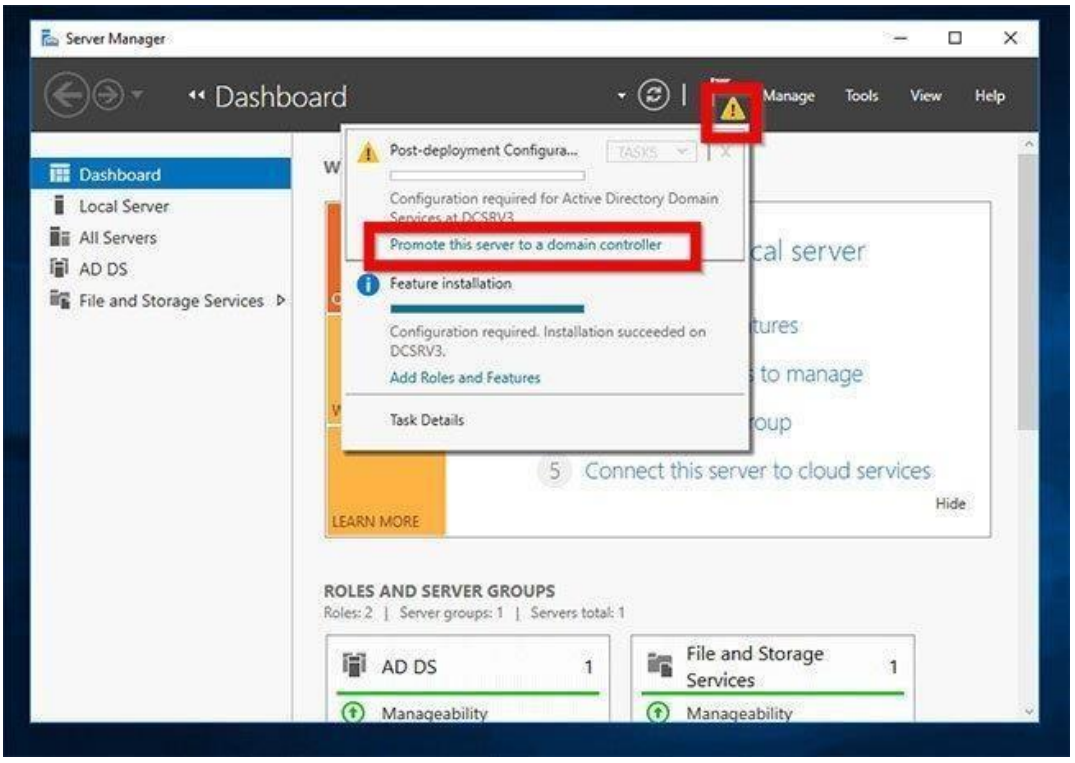
- Tại màn hình **Confirmation**, hãy xem lại các lựa chọn và nhấp vào **Install.**



Hình 3.5 Bắt đầu quá trình cài đặt

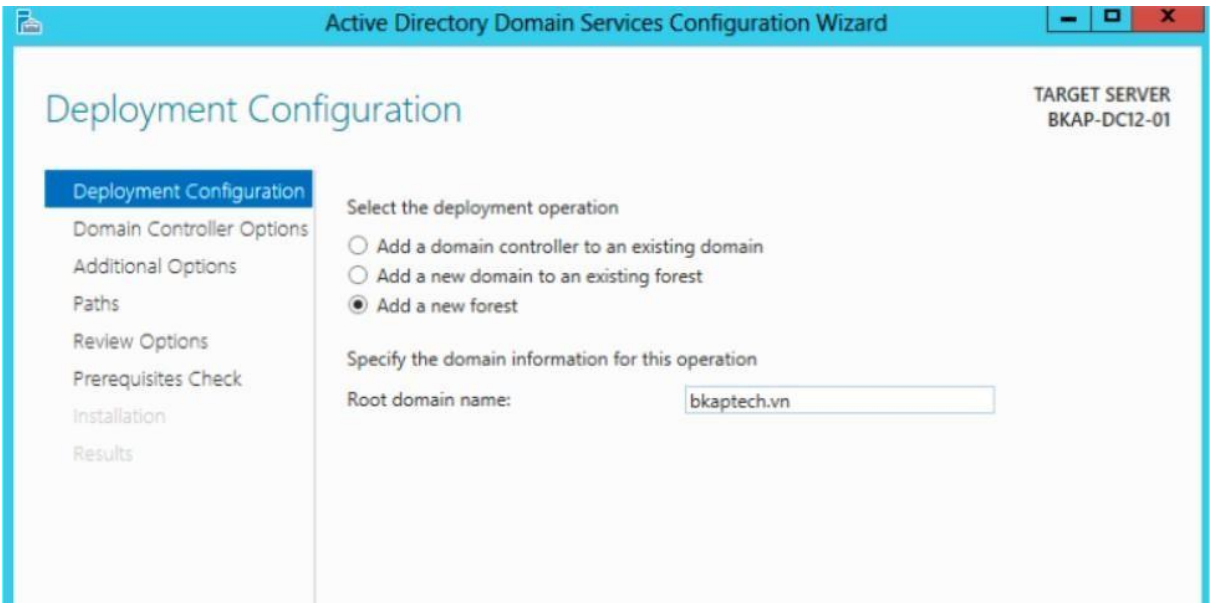
- Khi cài đặt hoàn tất, hãy nhấp vào **Close.**

- Nâng cấp lên Domain Controller



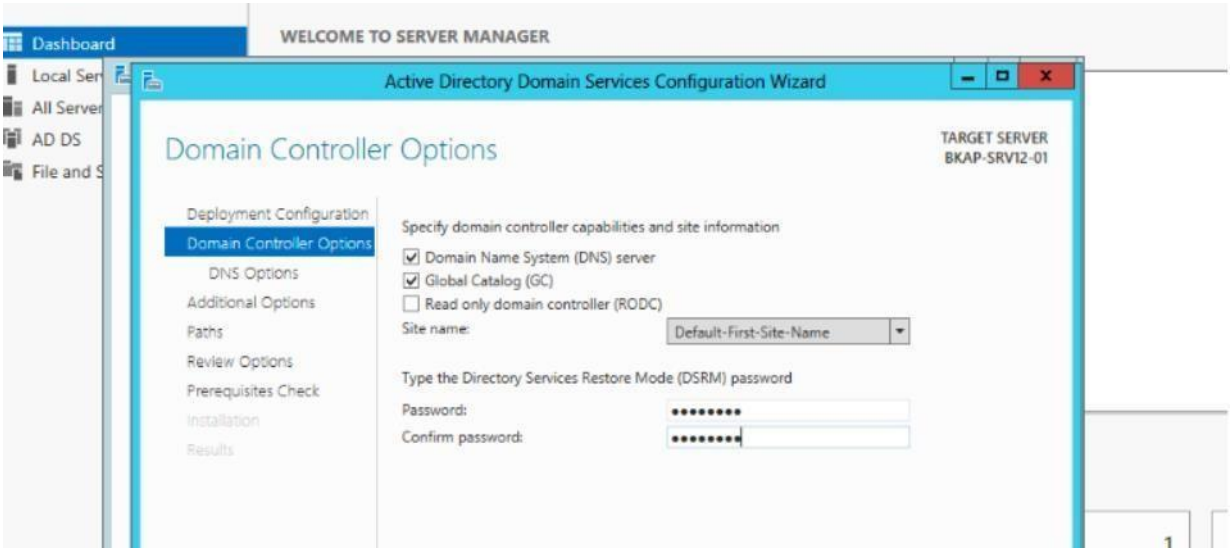
Hình 3.6 Nâng cấp lên domain

- Chọn **Add a new forest** → Nhập **Root domain name** → Chọn **Next**



Hình 3.7 Cấu hình khi nâng lên domain Controller

- Nhập mật khẩu → Chọn **Next**



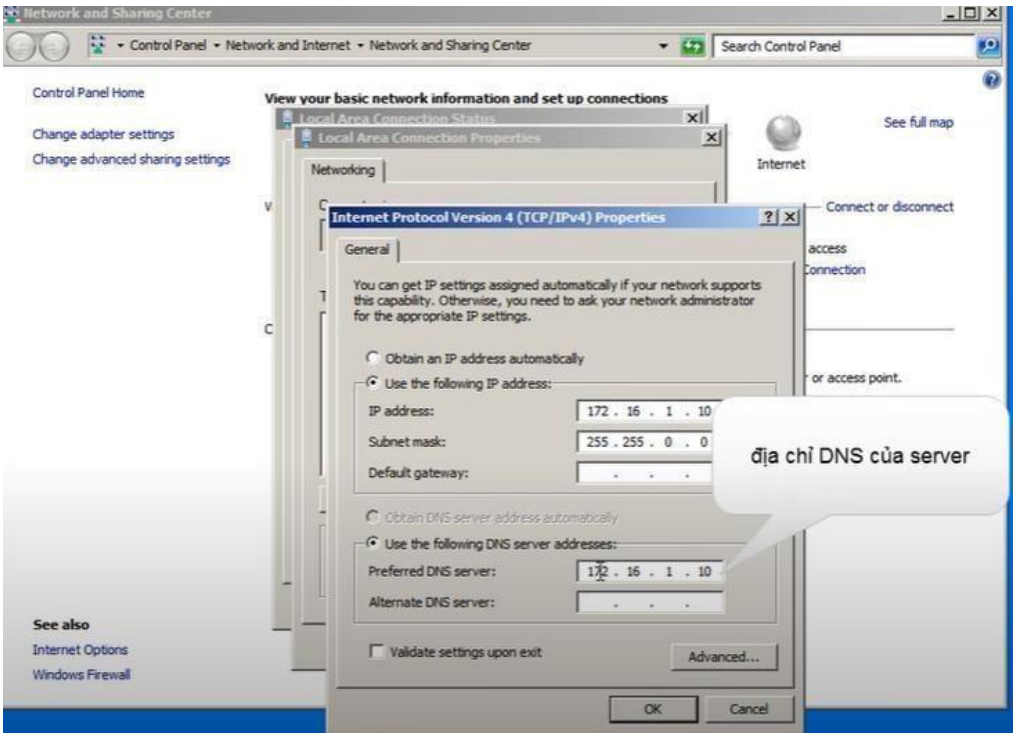
Hình 3.8 Nhập lại mật khẩu

- Chọn Install

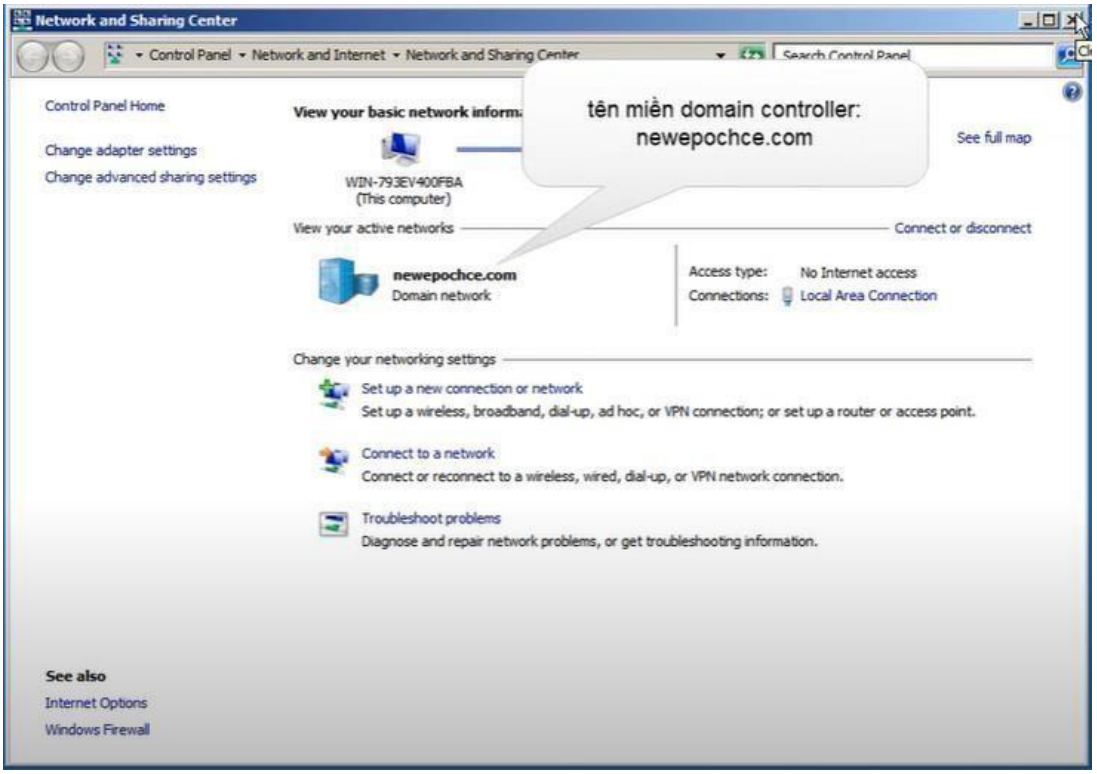
- Sau khi nâng cấp xong máy chủ sẽ khởi động lại nhấn tổ hợp phím Ctrl + Alt + Delete để đăng nhập vào máy

3.2. Gia nhập máy trạm vào domain

- Kiểm tra địa chỉ và DNS của server

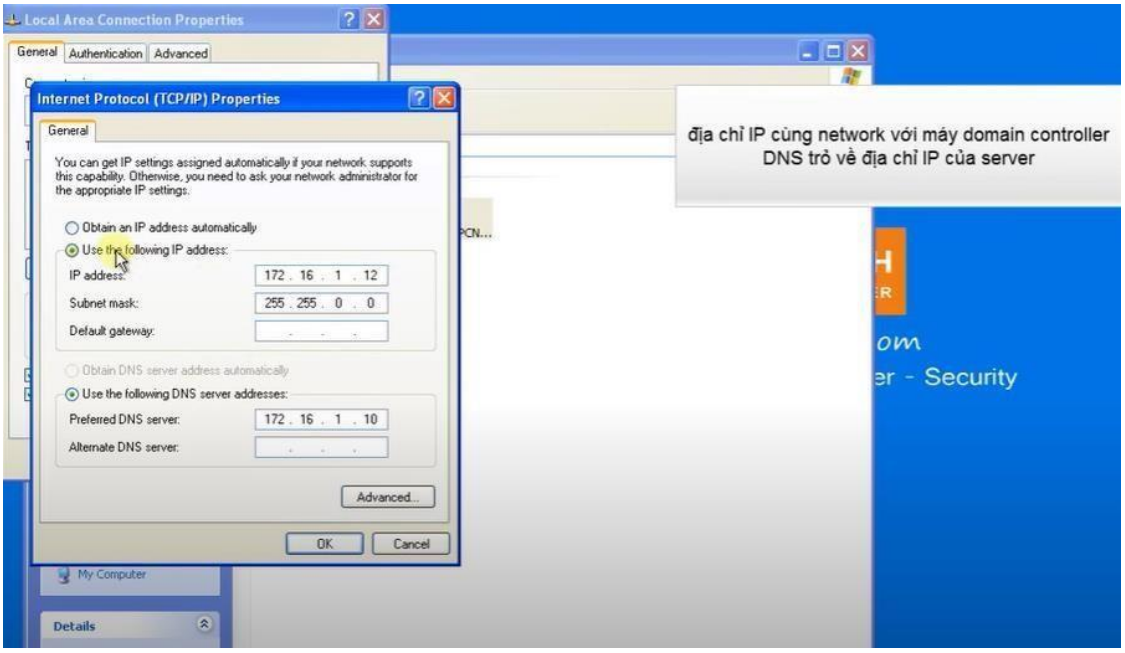


Hình 3.9 Kiểm tra địa chỉ và DNS của máy server

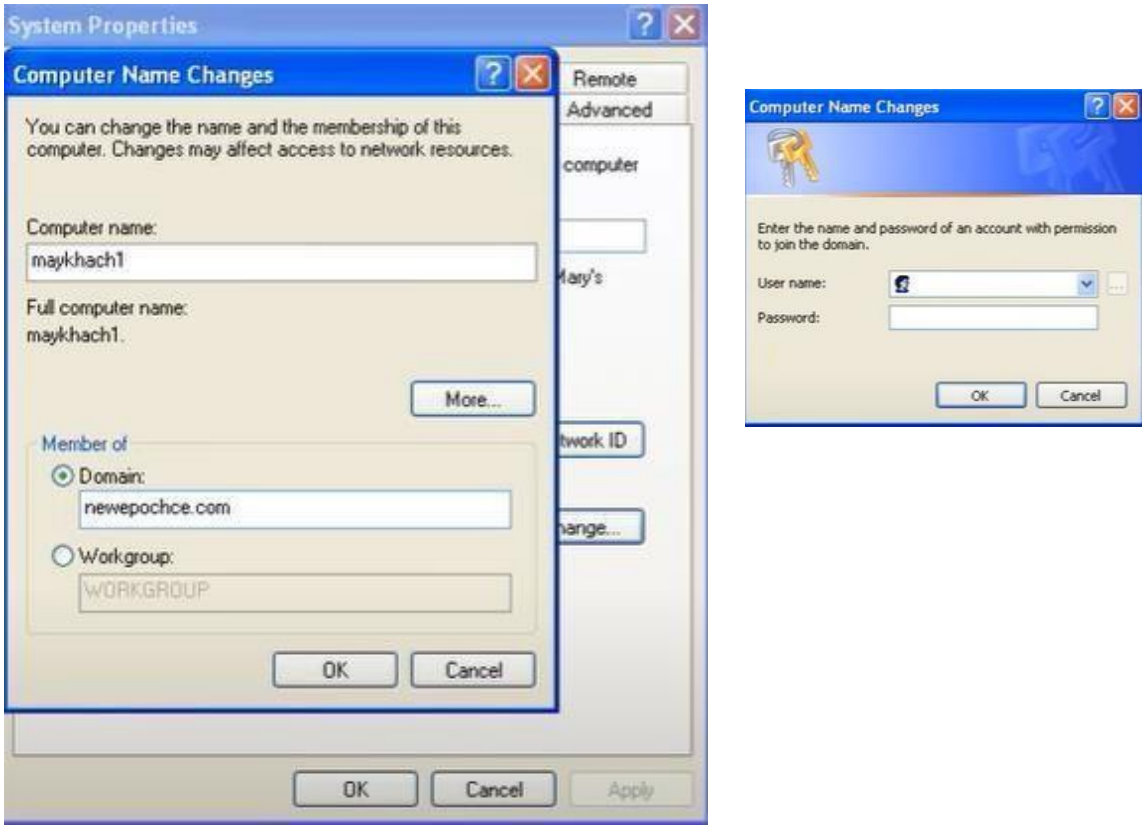


Hình 3.10 Tên miền của máy server

- Thiết lập địa chỉ và DNS cho máy client

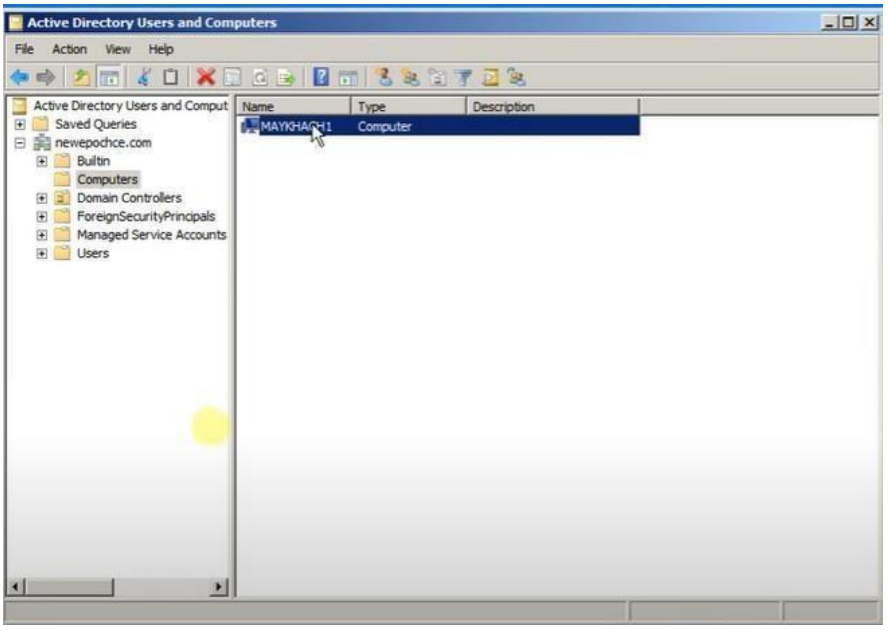


Hình 3.11 Thiết lập địa chỉ IP trên máy client



Hình 3.12 Thiết lập tên máy, domain và nhập tài khoảng administrator của domain controller để xác nhận

- Kiểm tra trên máy server



Hình 3.13 Client gia nhập vào domain thành công

3.3. Xây dựng các domain controller đồng hành

Trong các hệ thống Active Directory lớn, nếu chỉ có một Domain Controller thì Server này có thể bị quá tải khi nhiều user cùng yêu cầu chứng thực. Bên cạnh đó Khi Domain Controller này bị lỗi thì toàn bộ hệ thống sẽ bị ngưng hoạt động, các user sẽ không được chứng thực. Việc trang bị thêm một máy Domain Controller nữa sẽ giúp việc chia tải phân giải giữa các DCs cũng như CSDL của miền sẽ được lưu trữ đồng bộ trên các máy Domain Controller này. Chính vì lợi ích đó, khái niệm Additional Domain Controller ra đời, sau đây chúng ta sẽ tiến hành sử dụng thêm 1 máy Windows Server để làm Additional Domain Controller…

3.3.1. Các bước thực hiện chính xây dựng Additional Domain Controller (ADC)

Bước 1.Đặt IP cho máy ADC (máy sẽ làm Domain Controller thứ 2)

Bước 2.Nâng cấp Additional Domain Controller

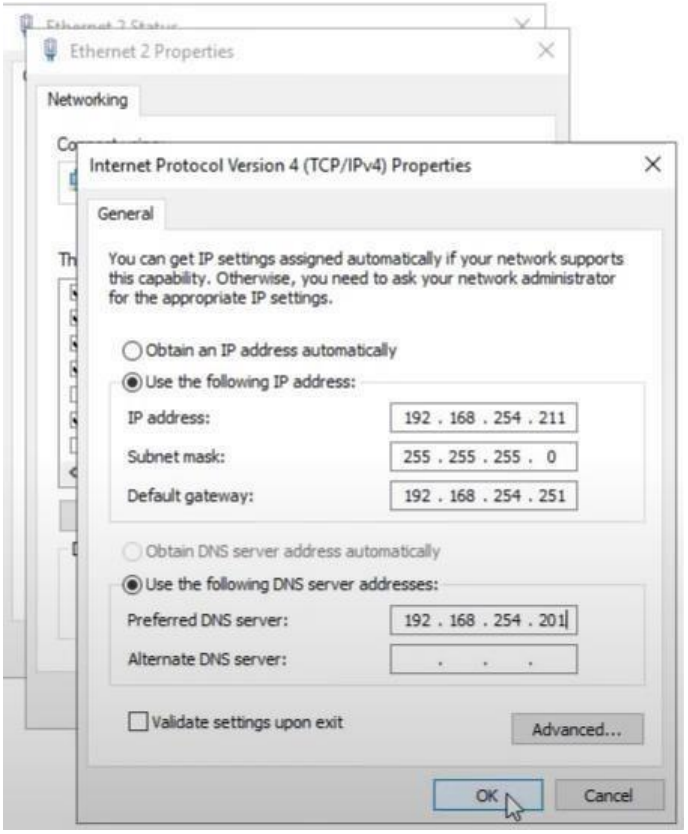
Bước 3.Bật Global Catalog

Bước 4. Kiểm tra sự đồng bộ giữa 2 máy Domain Controller

3.3.2. Chi tiết quá trình xây dựng Additional Domain Controller (ADC)

Bước 1 :

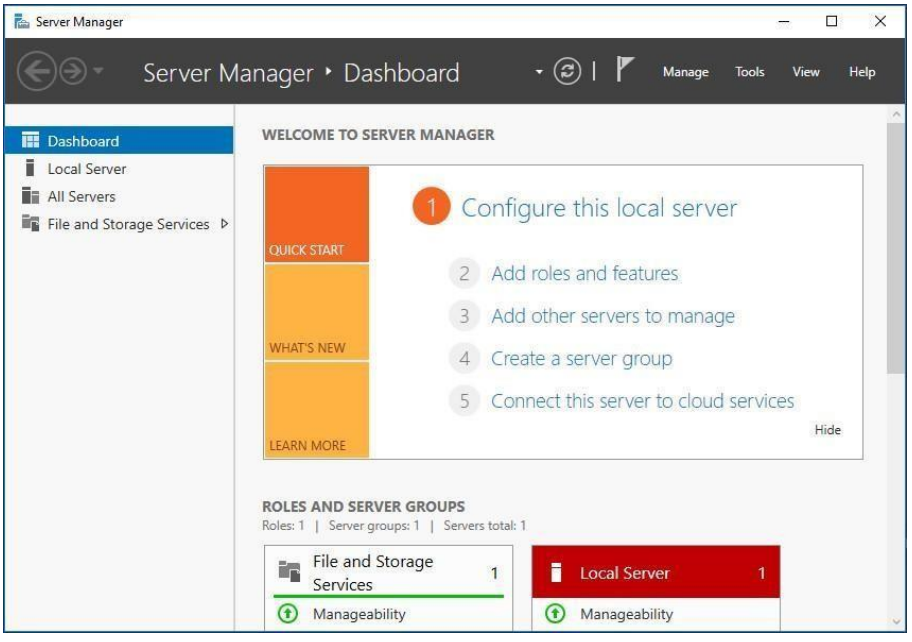
- Cấu hình IP cho máy được chọn làm ADC, với DNS là địa chỉ của máy Domain Controller thứ 1



Hình 3.14 Cấu hình IP cho máy được chọn làm ADC

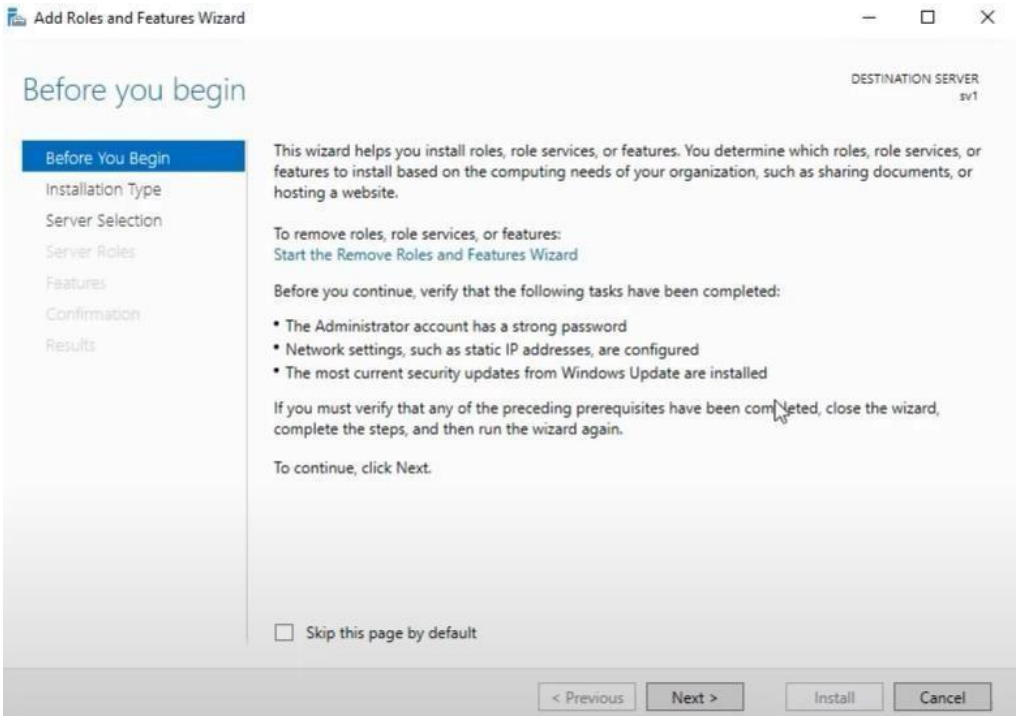
Bước 2:

- Vào công cụ Server Manager, chọn Add roles and features.



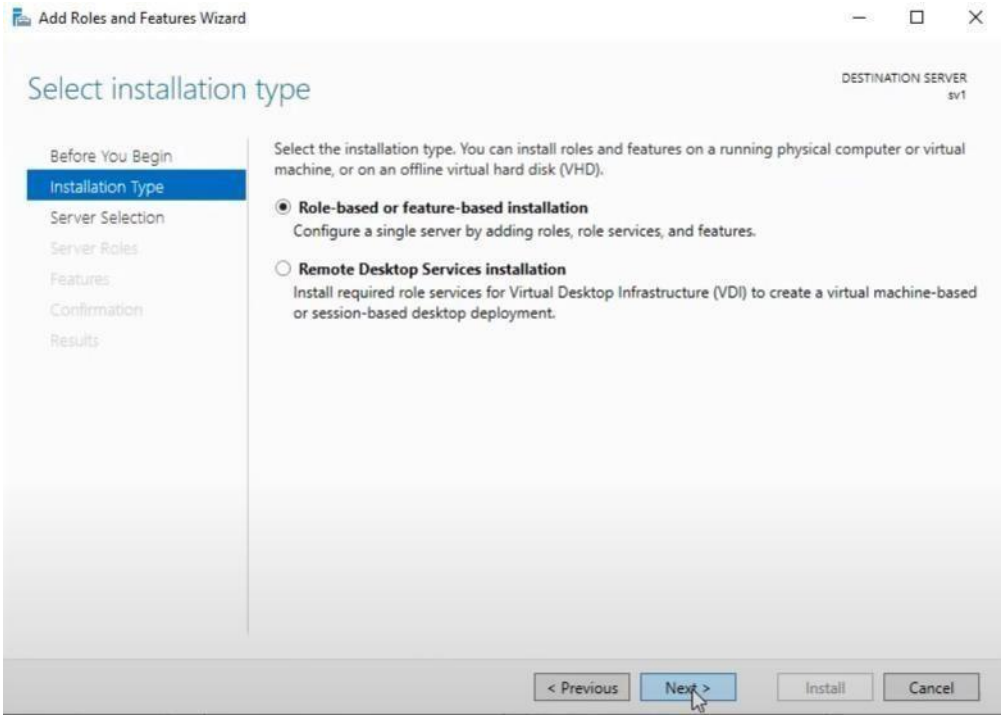
Hình 3.15 Hộp thoại Server Manager

- Trong hộp thoại Before you begin, chọn Next để tiếp tục



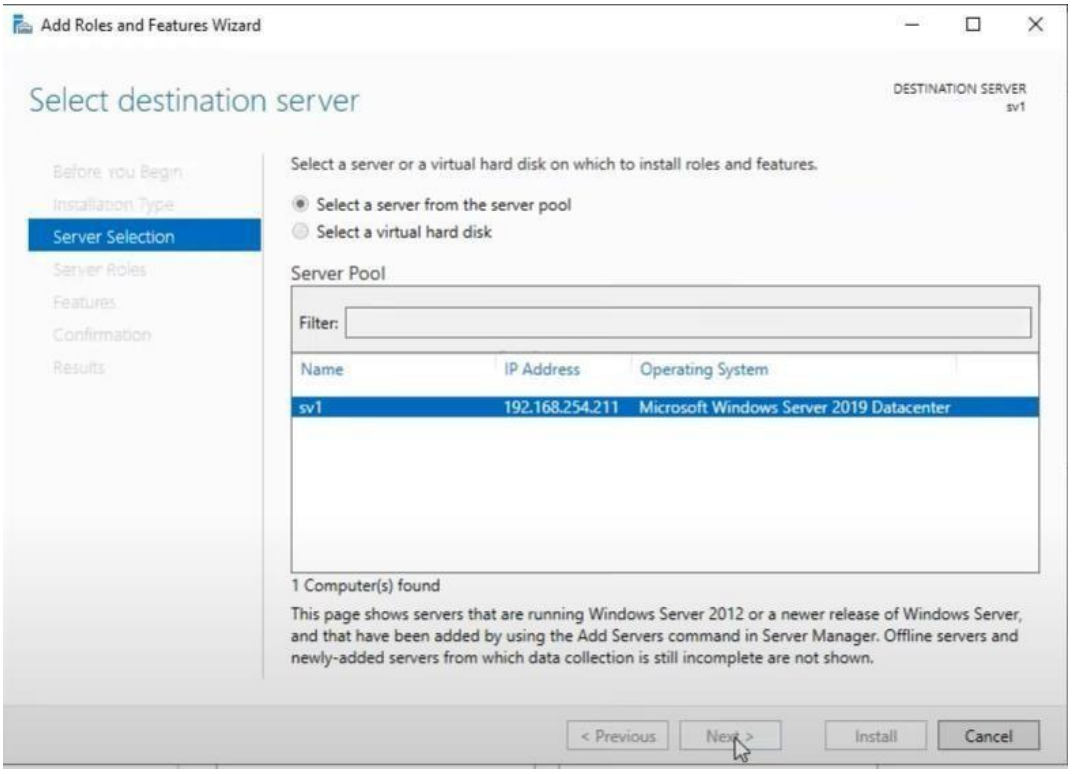
Hình 3.16 Hộp thoại Before you begin

- Trong hộp thoại Select installation type, chọn Role-based or feature-based installation, chọn Next để tiếp tục



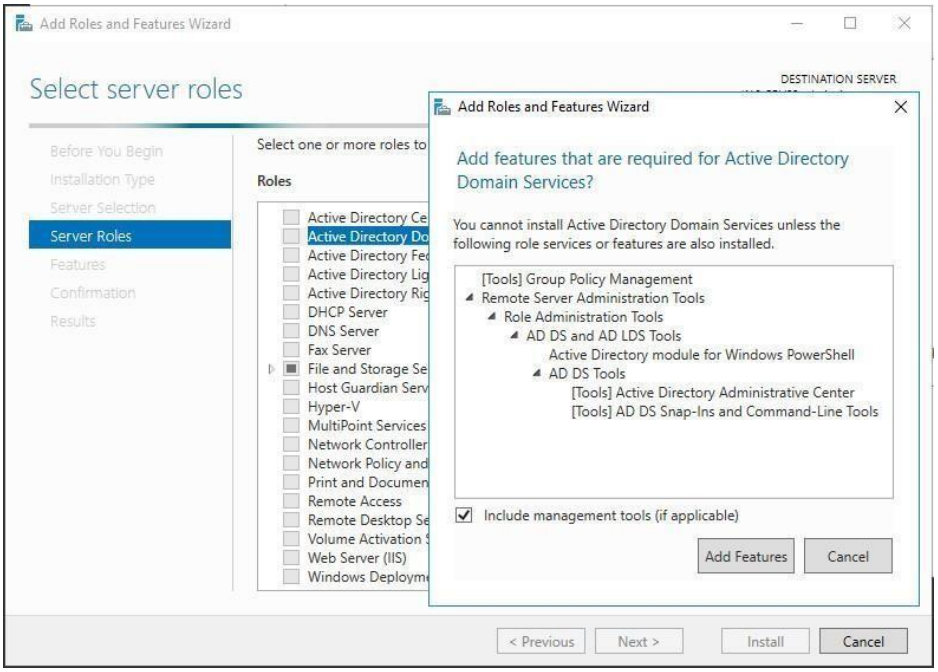
Hình 3.17 Hộp thoại Select installation type

- Trong hộp thoại Select destination server, chọn Server , chọn Next.



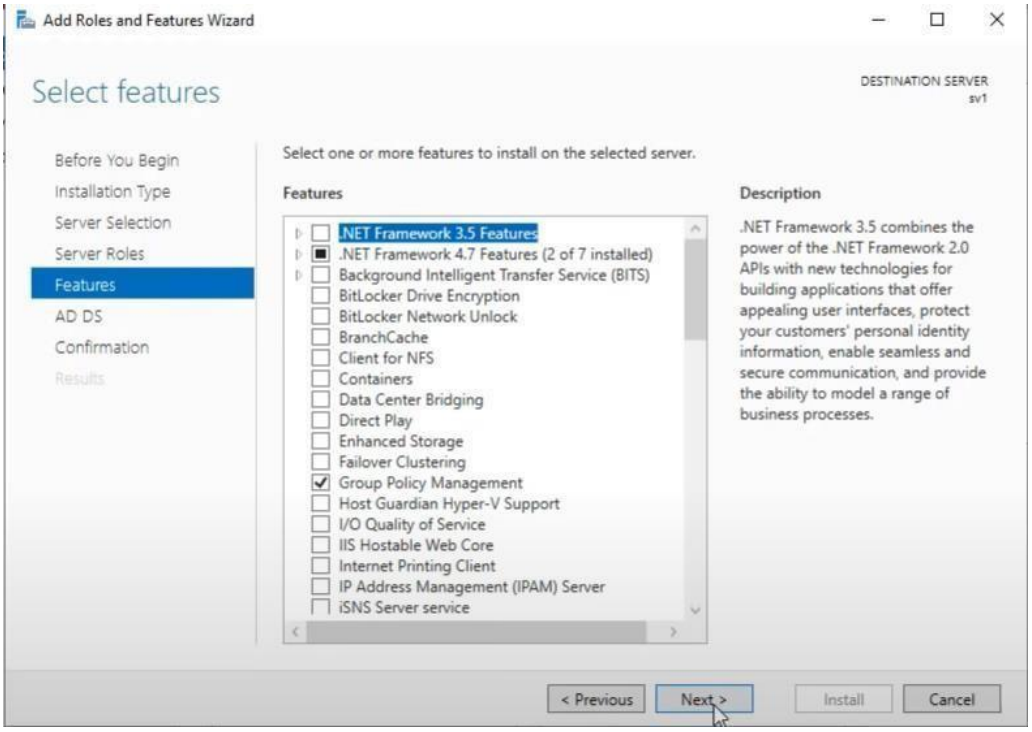
Hình 3.18 Hộp thoại Select destination

- Trong hộp thoại Select server roles, chọn mục Active Directory Domain Services, chọn Add Features



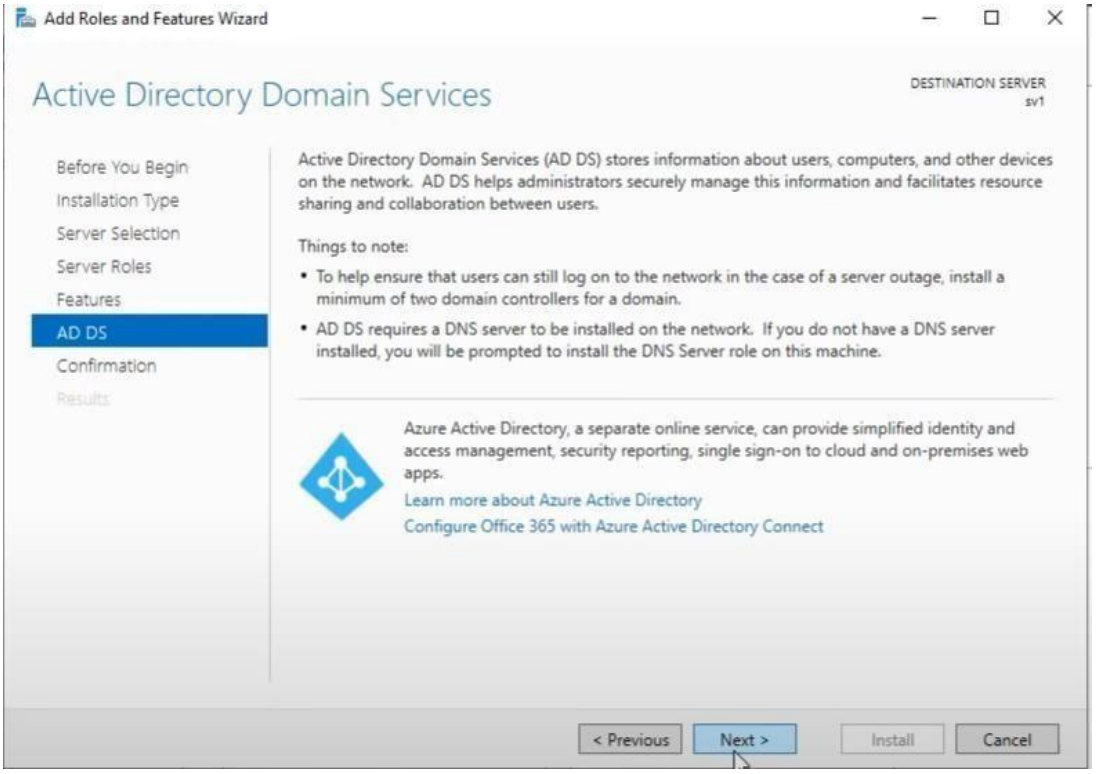
Hình 3.19 Hộp thoại Select server roles

- Trong hộp thoại Select features, chọn Next để tiếp tục.



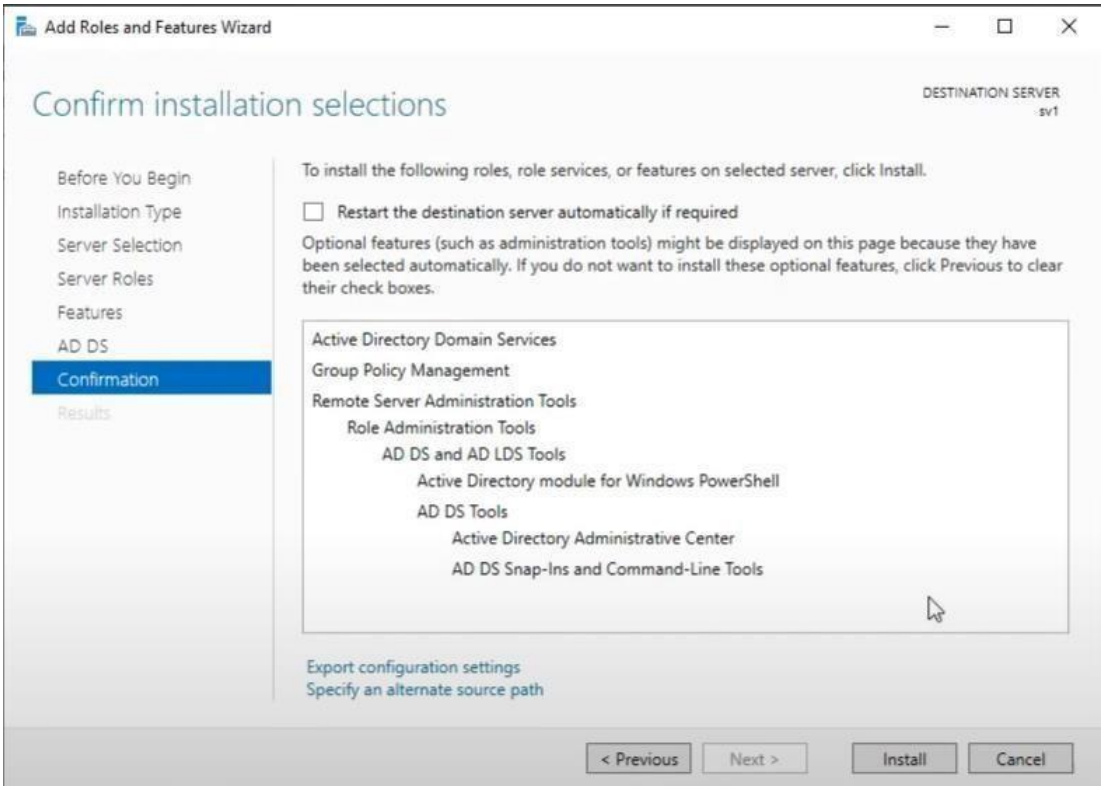
Hình 3.20 Hộp thoại Select features

- Trong hộp thoại Active Directory Domain Services, chọn Next



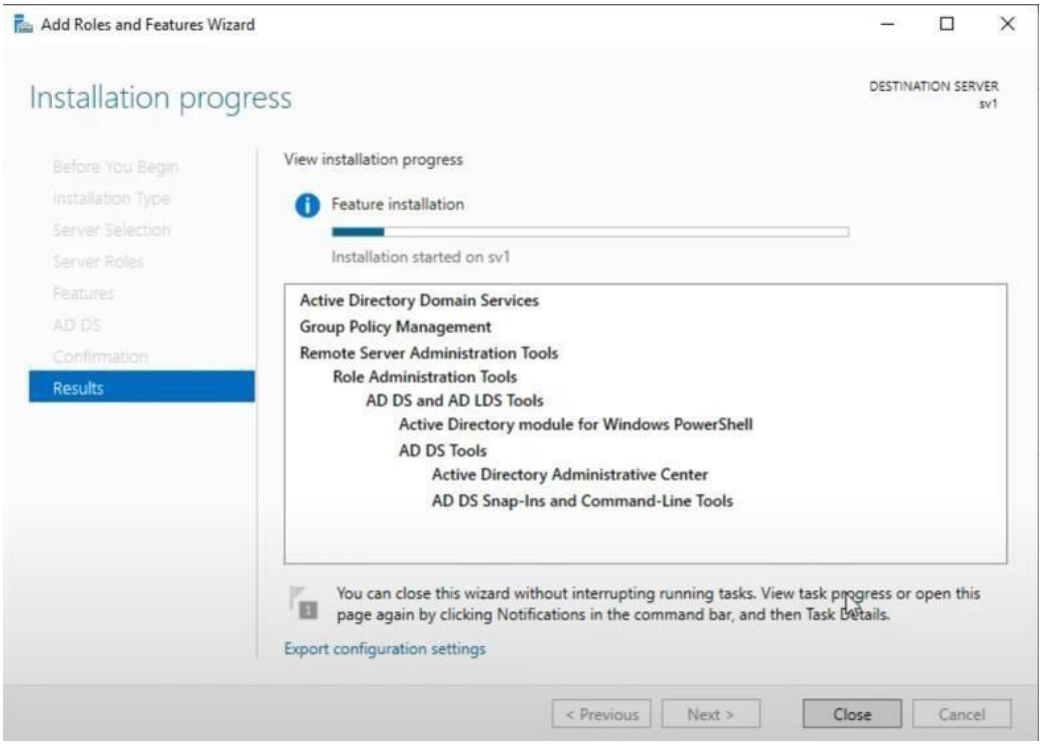
Hình 3.21 Hộp thoại Select features

- Trong hộp thoại Confirm installation selections, chọn Install.



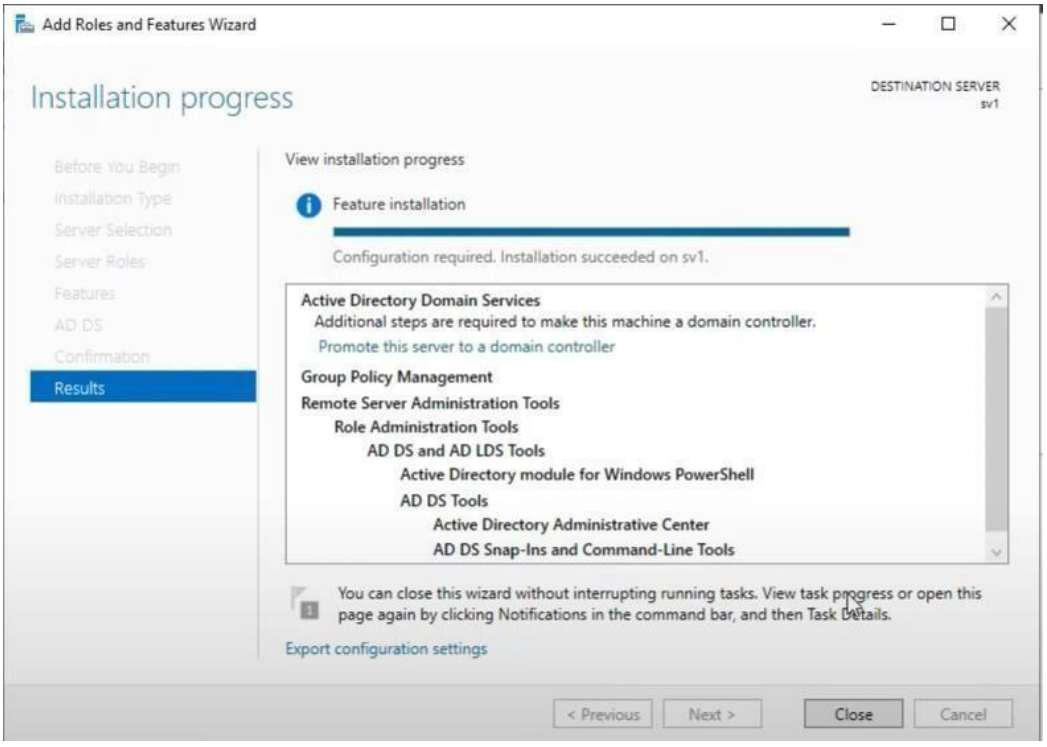
Hình 3.22 Confirm installation selections

- Quá trình cài đặt dịch vụ Active Directory Domain Services đang diễn ra.



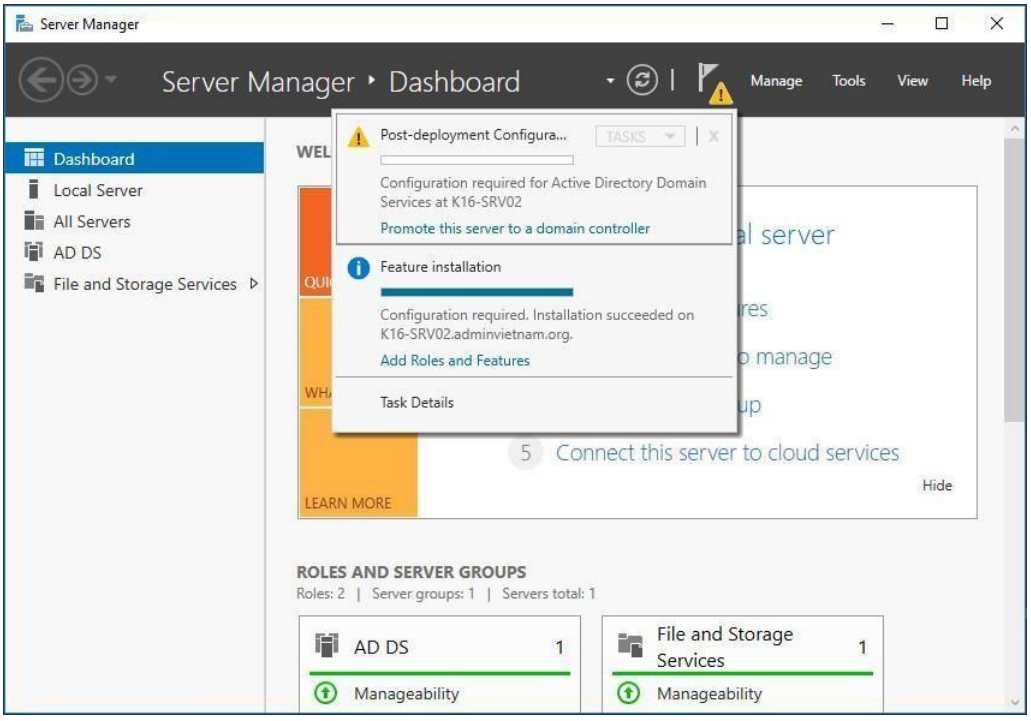
Hình 3.23 Quá trình cài đặt dịch vụ Active Directory Domain Services

- Chọn Close để hoàn tất quá trình cài đặt.



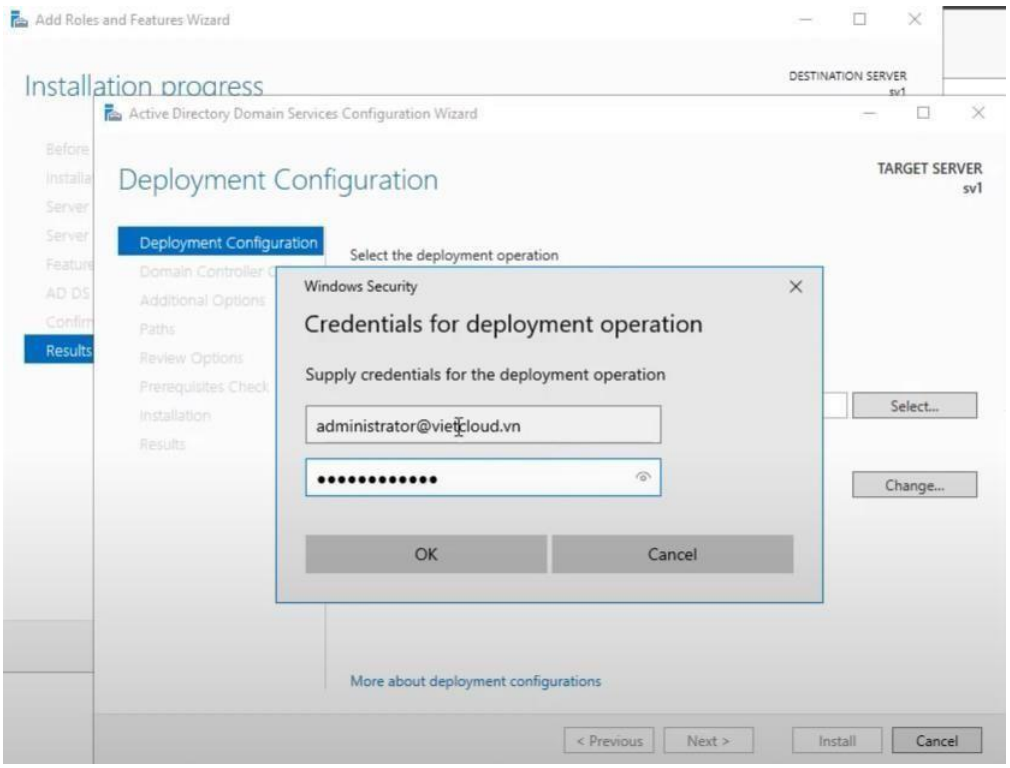
Hình 3.24 Cài đặt hoàn tất

- Trong hộp thoại Server Manager, chọn Promote this server to a domain controller.



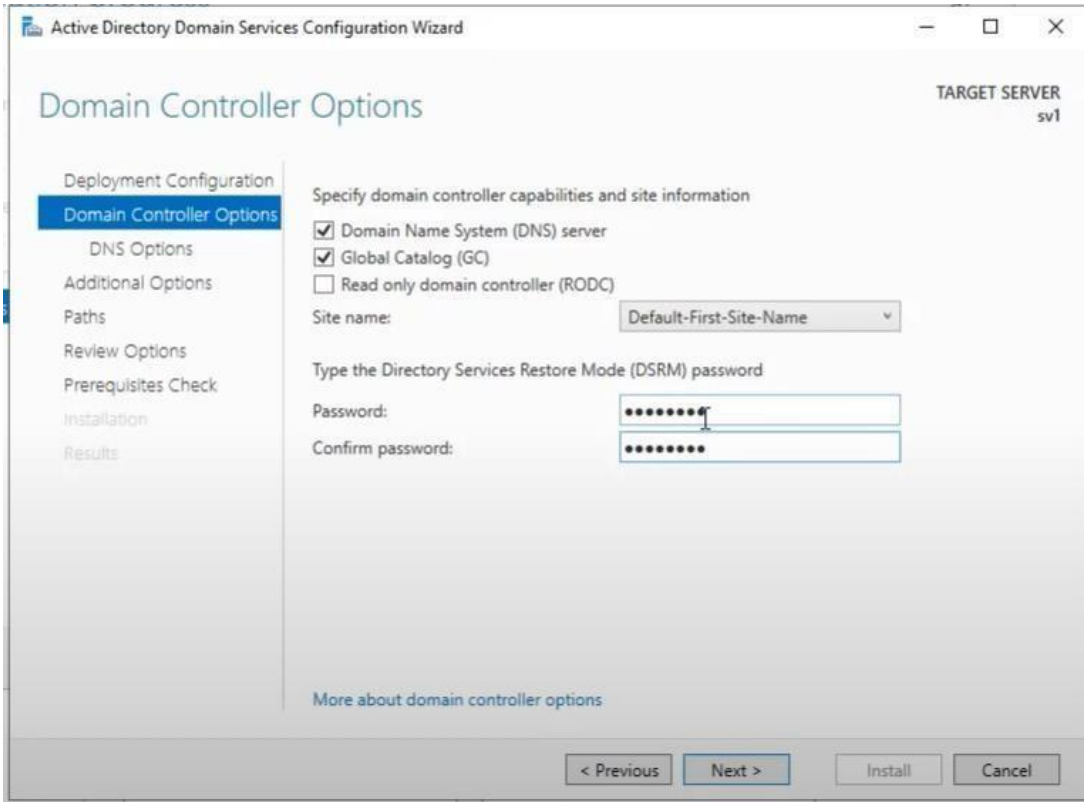
Hình 3.25 Cài đặt hoàn tất

- Trong hộp thoại Deployment Configuration, chọn Add a domain controller to an existing domain, nhấn Change, Nhập user của admin, nhấn Ok, chọn Next.



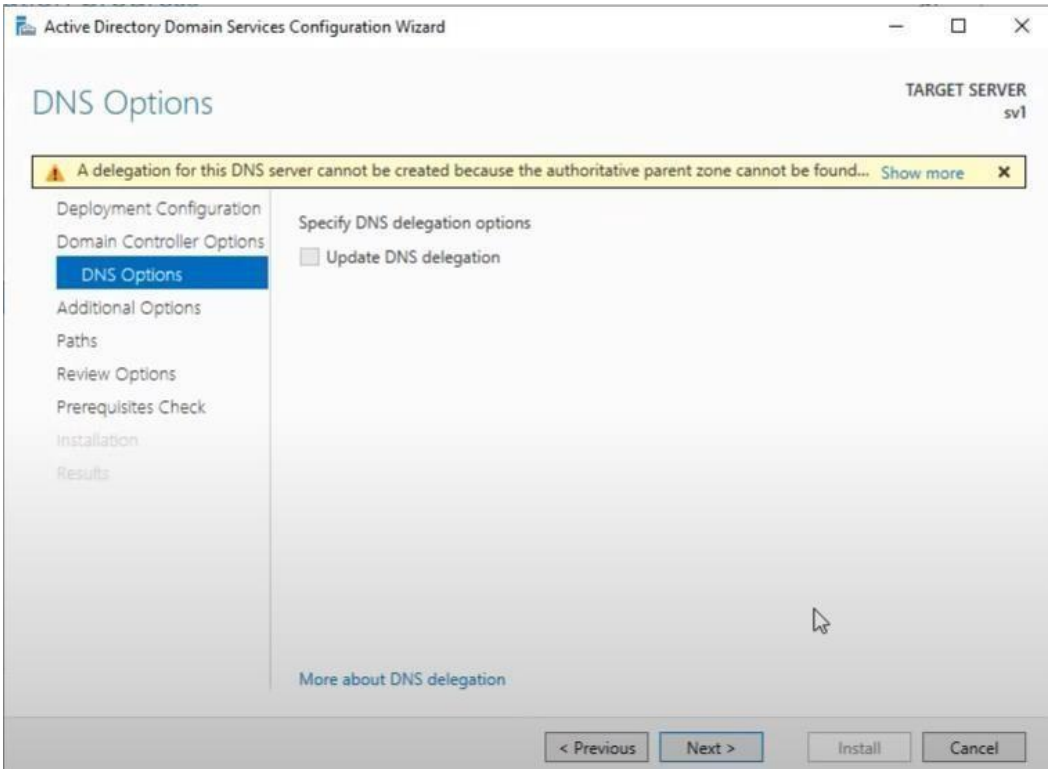
Hình 3.26 Thêm domain controller đến một domain đã tồn tại

- Trong hộp thoại Domain Controller Options, đặt mật khẩu khôi phục hệ thống Domain khi có sự cố, chọn Next.



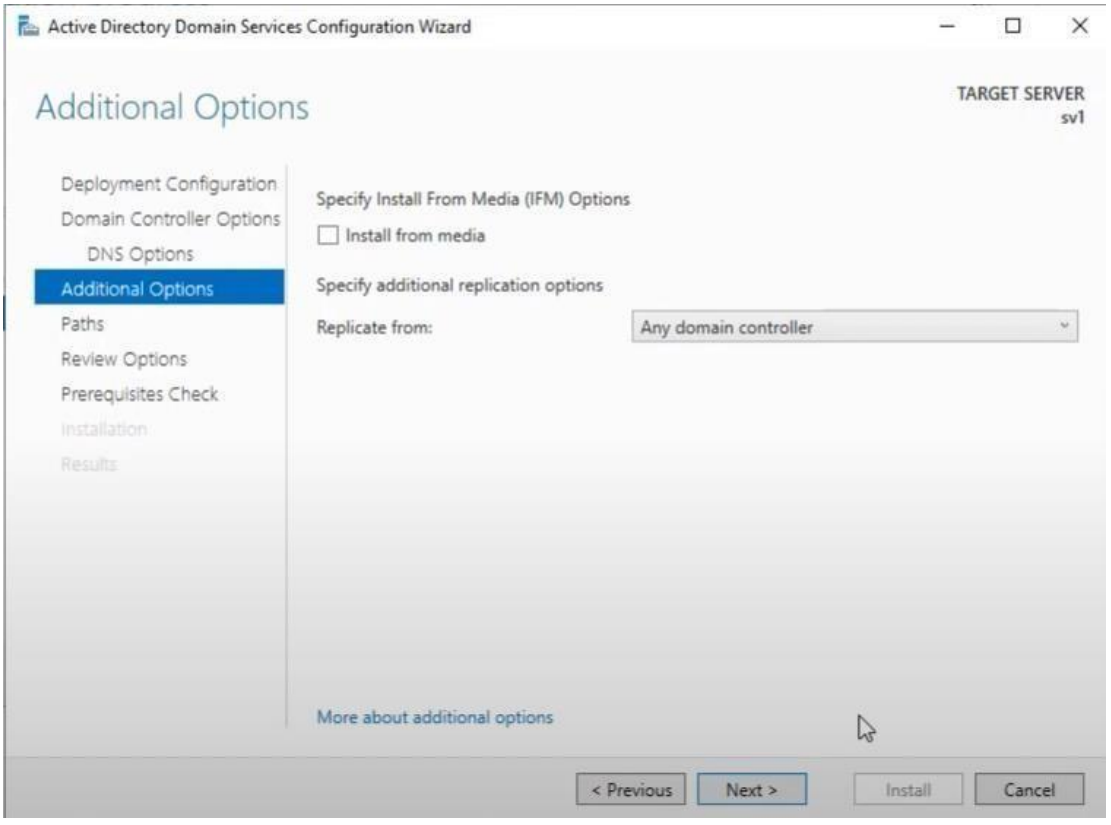
Hình 3.27 Đặt mật khẩu khi vào chế độ khôi phục hệ thống

- Trong hộp thoại DNS Options, chọn Next.



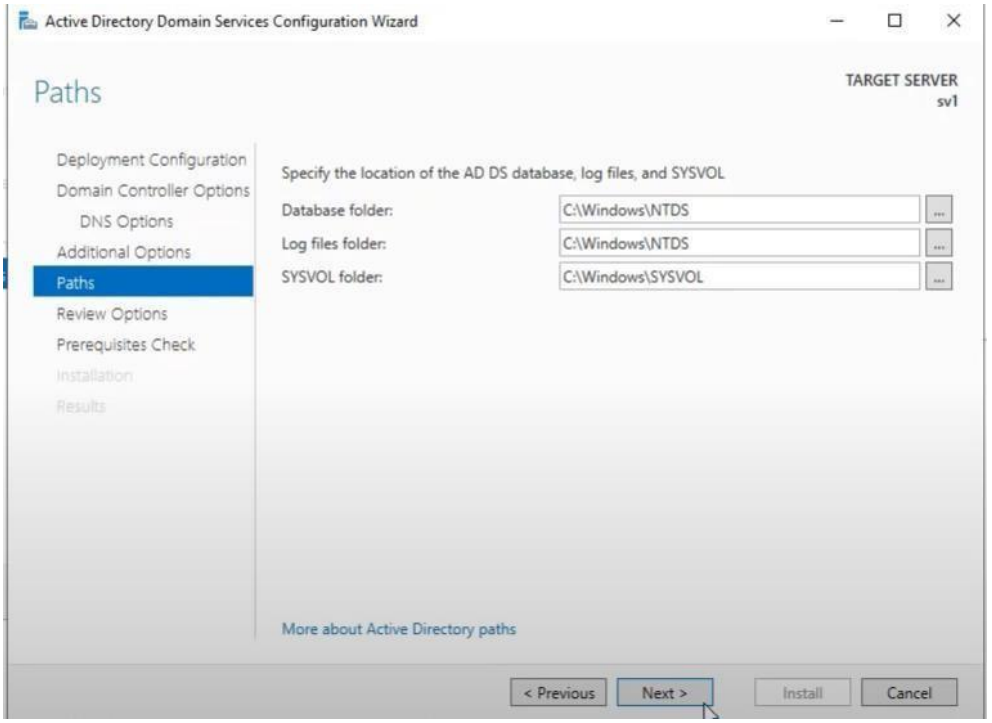
Hình 3.28 Hộp thoại DNS Options

- Trong hộp thoại Addtional Options, chọn Next.



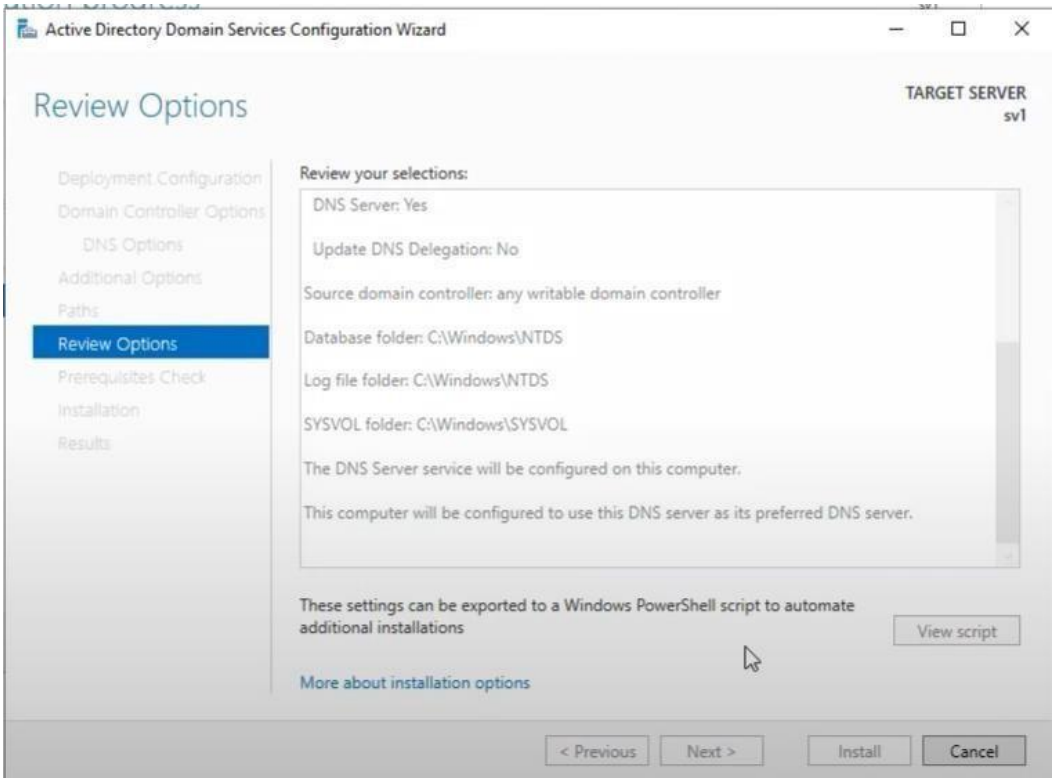
Hình 3.29 Hộp thoại Additional Options

- Trong hộp thoại Paths, chỉ định đường dẫn lưu trữ CSDL của hệ thống miền



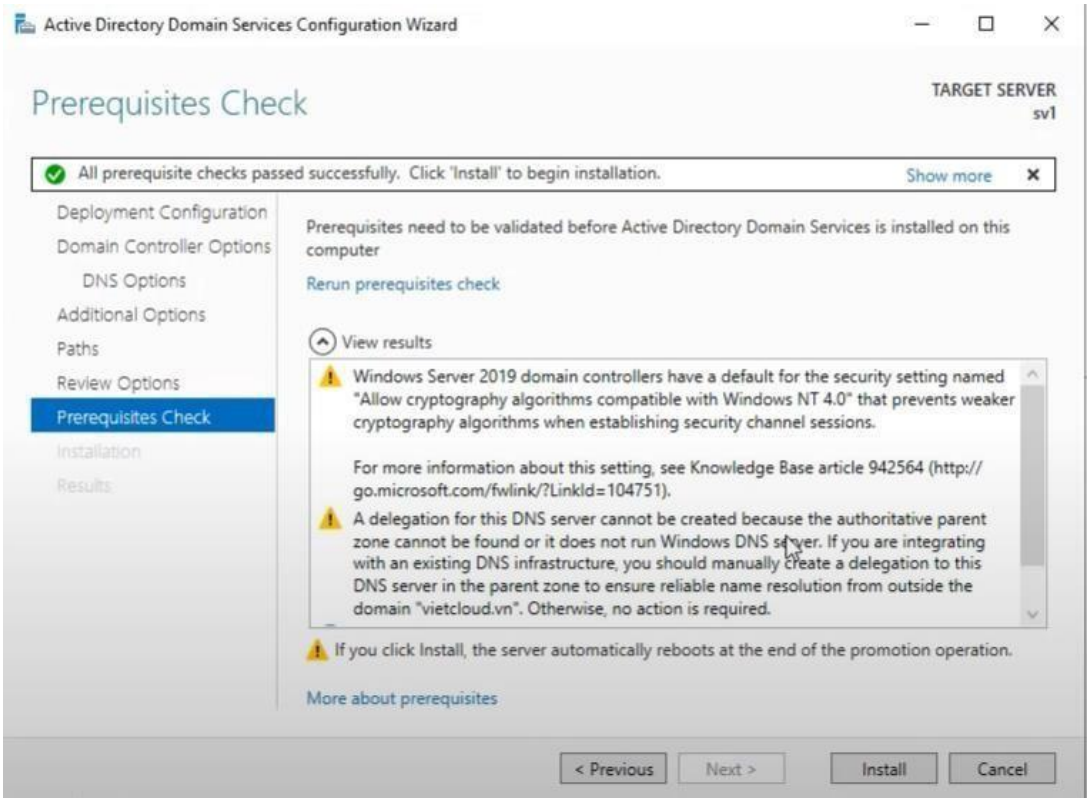
Hình 3.30 Chỉ định đường dẫn lưu trữ CSDL của hệ thống miền

- Trong hộp thoại Review Options, chọn Next.



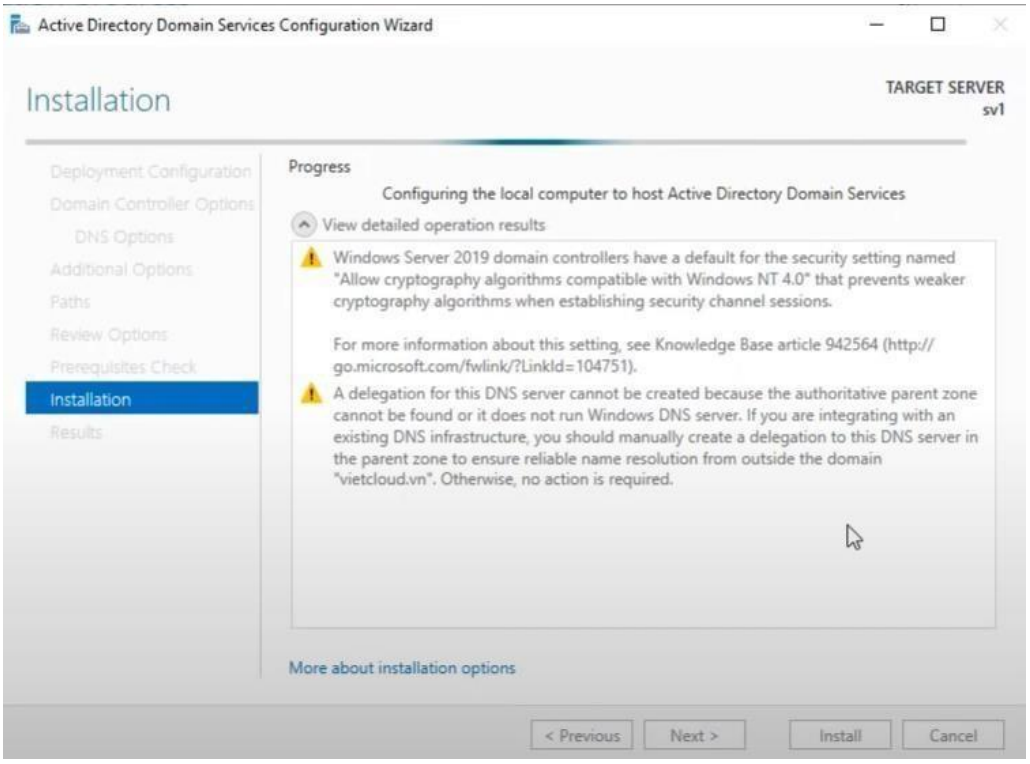
Hình 3.31 Hộp thoại Review Options

- Chọn Install



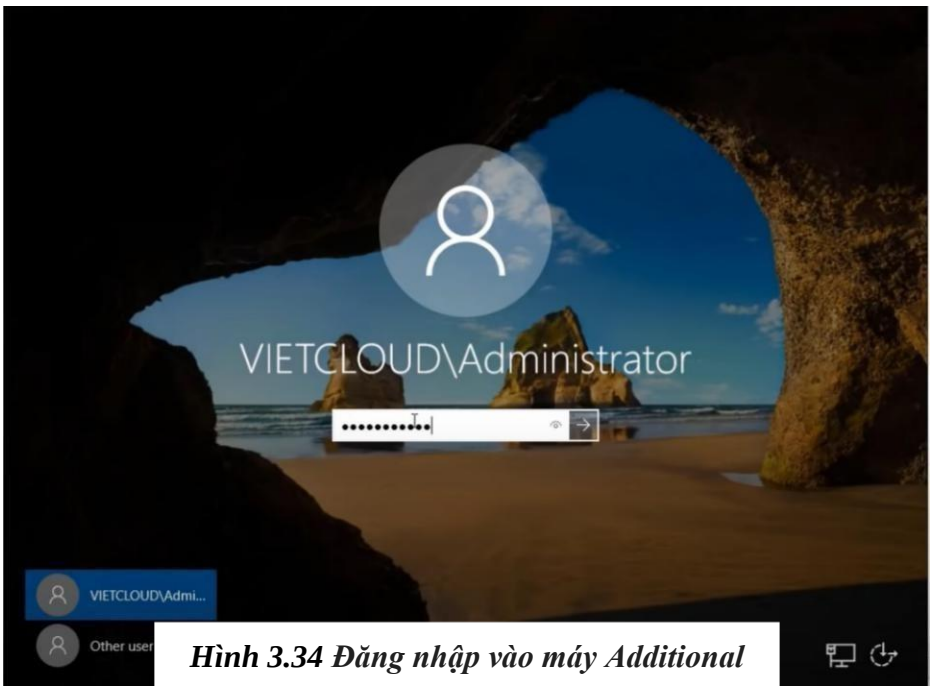
Hình 3.32 Hộp thoại Prerequisites Check

- Quá trình nâng cấp đang diễn ra.



Hình 3.33 Quá trình nâng cấp

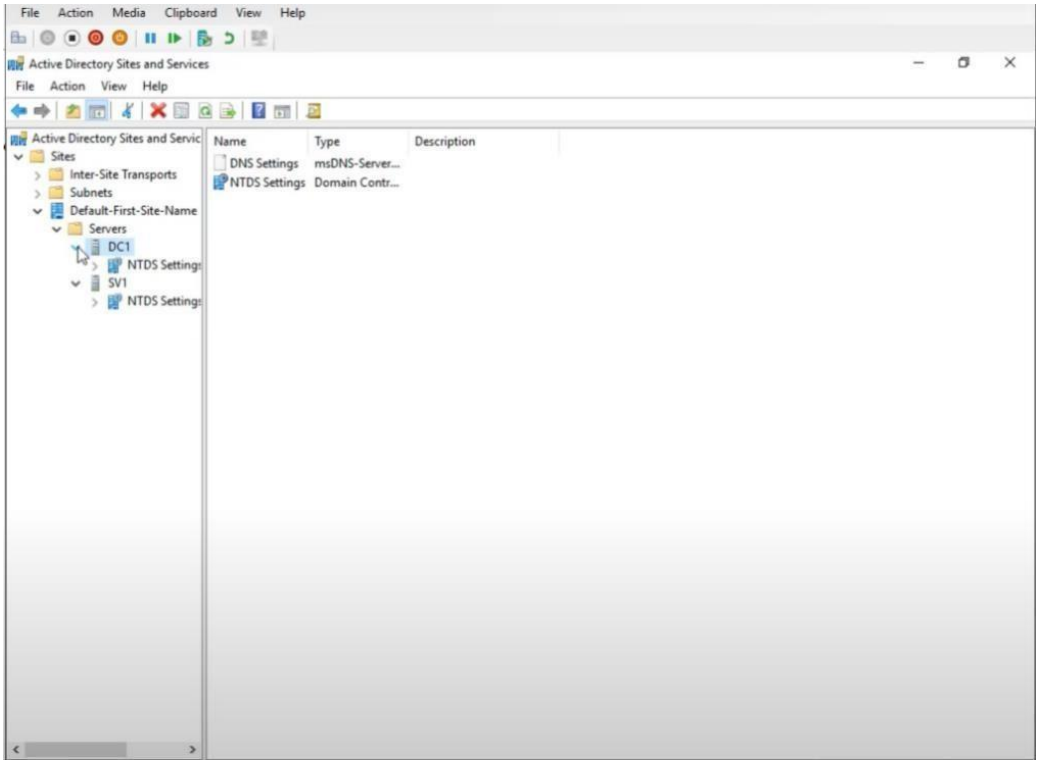
- Đăng nhập vào máy Additional Domain Controller bằng tài khoản quản trị trên miền vietcloud.vn



Hình 3.34 Đăng nhập vào máy Additional Domain Controller

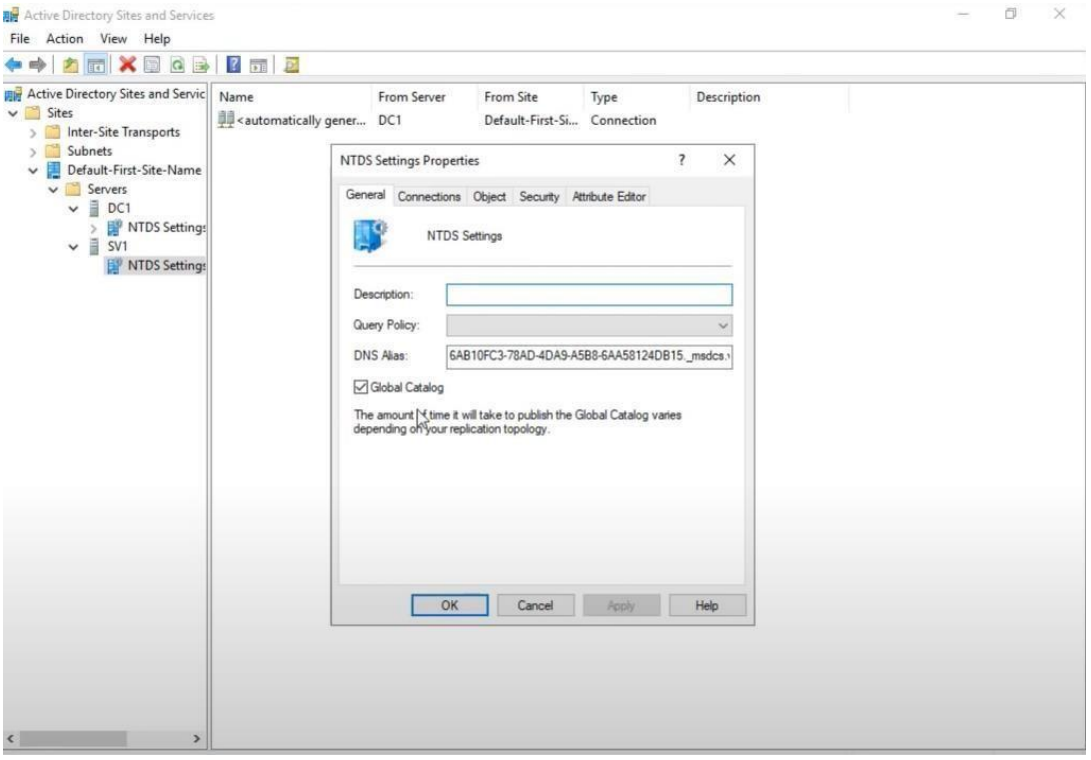
Bước 3:

- Trong Manager Server, chọn Tools, mở công cụ Active Directory Site and Service



Hình 3.35 Hộp thoại Active Directory Sites and Service

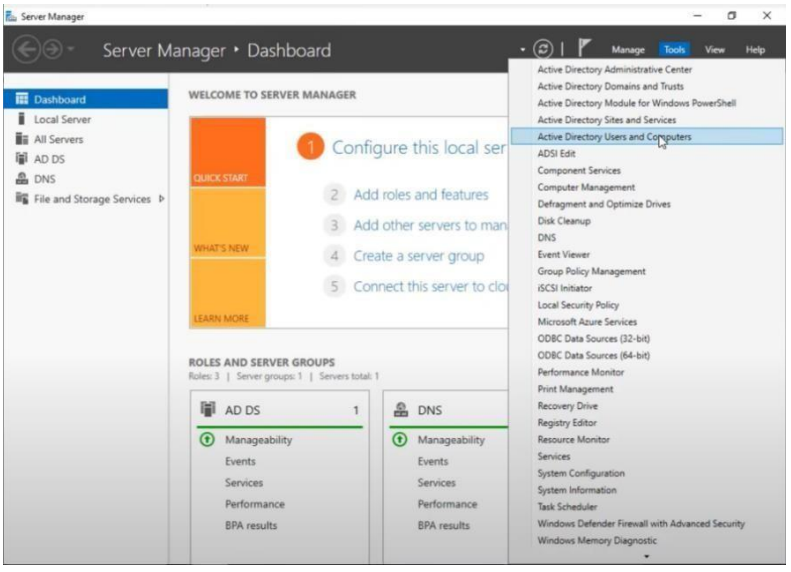
- Click chuột phải lên NTDS Settings của SV1, chọn Properties



Hình 3.36 Kiểm tra xem máy sv1 có là Global Catalog

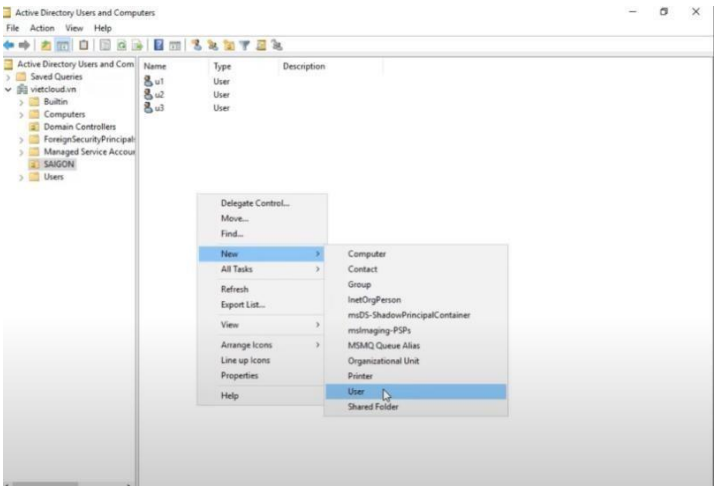
Bước 4 :

- Máy sv1: Mở Manager Server, Chọn Active Directory Users and Computer



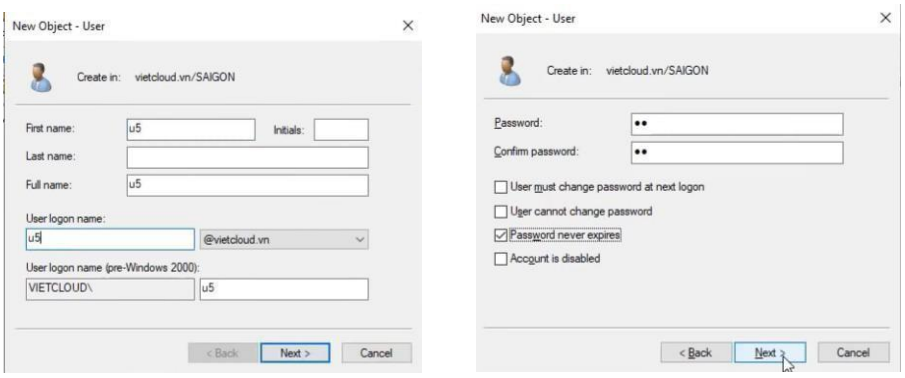
Hình 3.37 Chọn Active Directory Users and Computer từ Manager Server

- Trong group SAIGON click chuột phải cửa sổ bên phải chọn New, chọn User



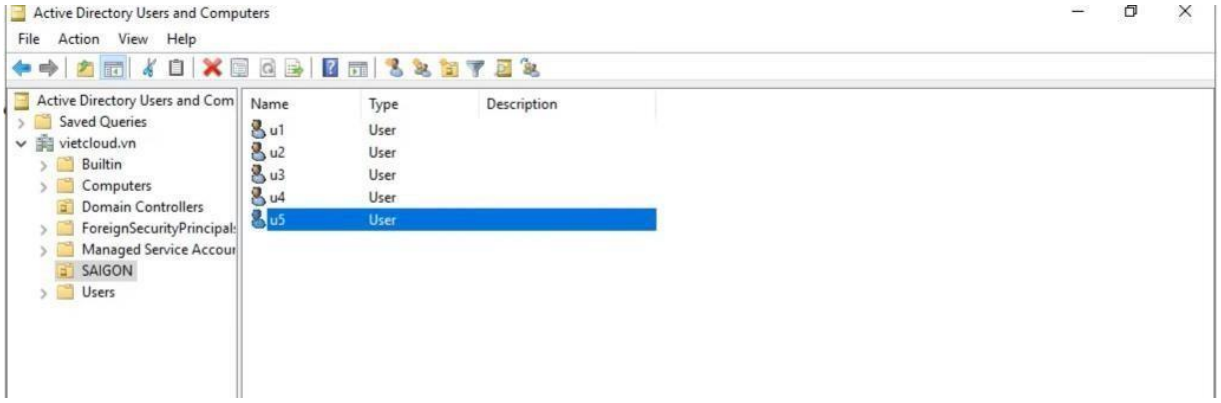
Hình 3.38 Tạo user mới trong máy sv1

- Nhập thông tin cho user, nhấn Next, nhập Password cho user, nhấn Next



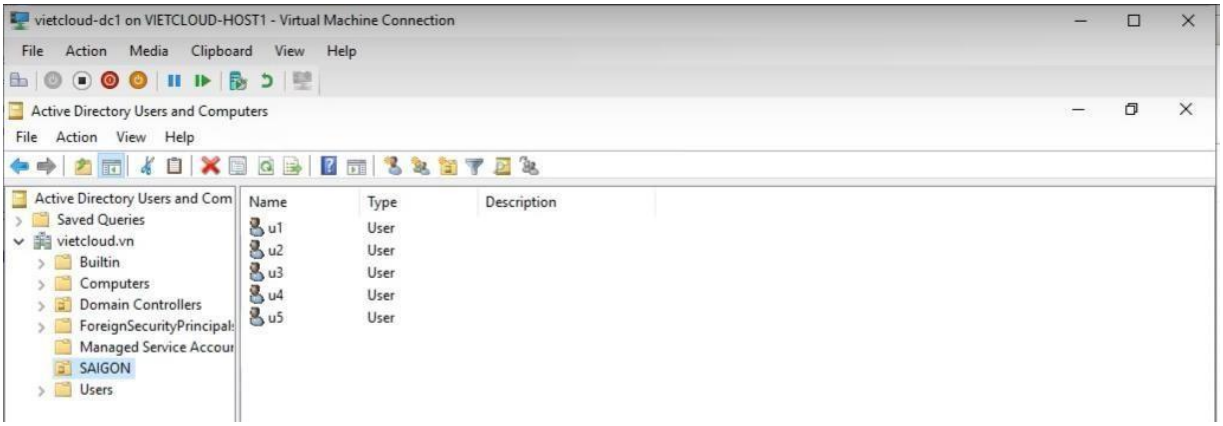
Hình 3.39 Nhập thông tin và password cho user

- Chọn Finish, ta có kết quả sau :



Hình 3.40 Kết quả sau khi tạo user

- Đăng nhập máy dc1 để kiểm tra



Hình 3.41 Users trên máy dc1

3.4. Xây dựng Subdomain

3.4.1. Các bước chính xây dựng Child Domain Controller (CDC)

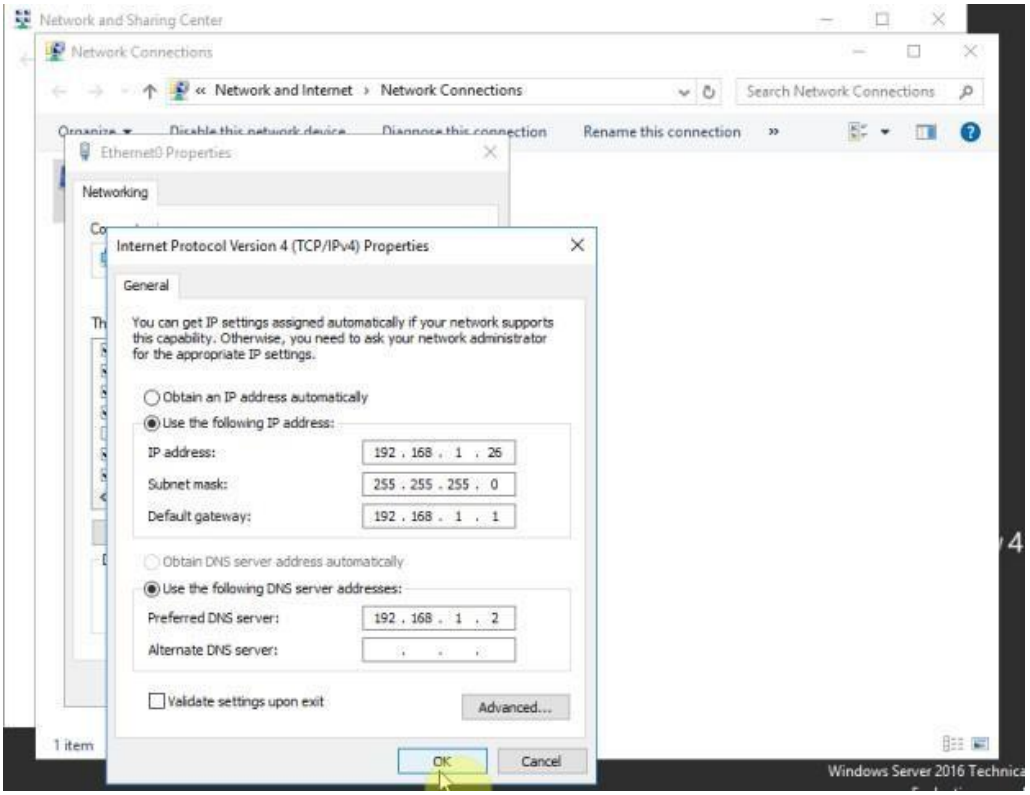
Bước 1. Đặt IP tĩnh cho máy chọn làm Child Domain Controller

Bước 2. Xây dựng Child Domain Controller

Bước 3. Đăng nhập máy CDC để kiểm tra

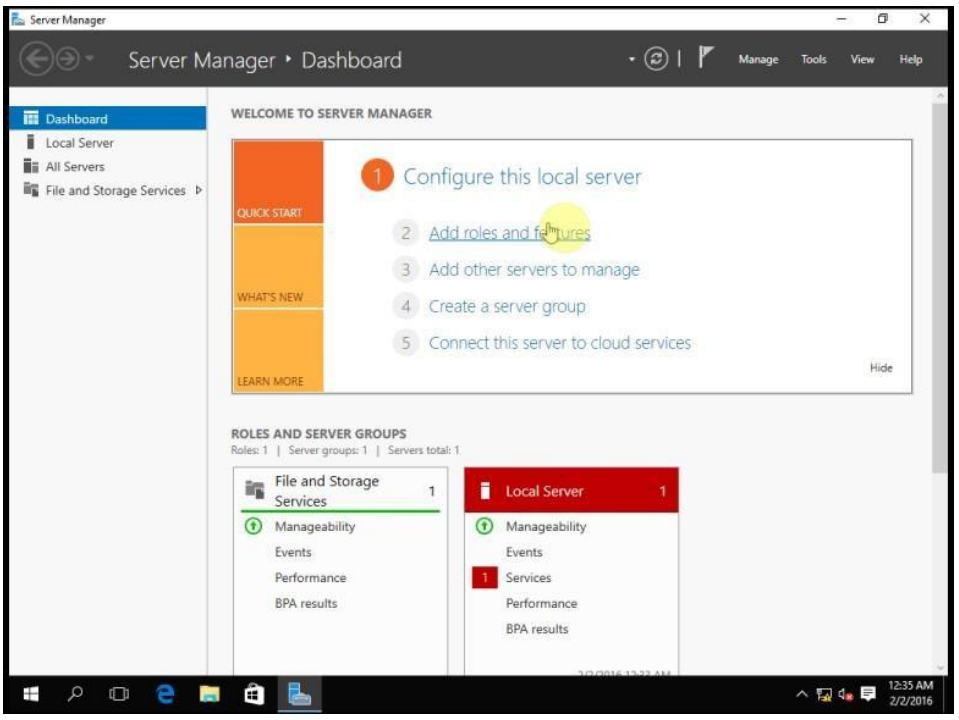
3.4.2. Chi tiết quá trình xây dựng Child Domain Controller (CDC)

- Cấu hình IP cho máy được chọn làm CDC



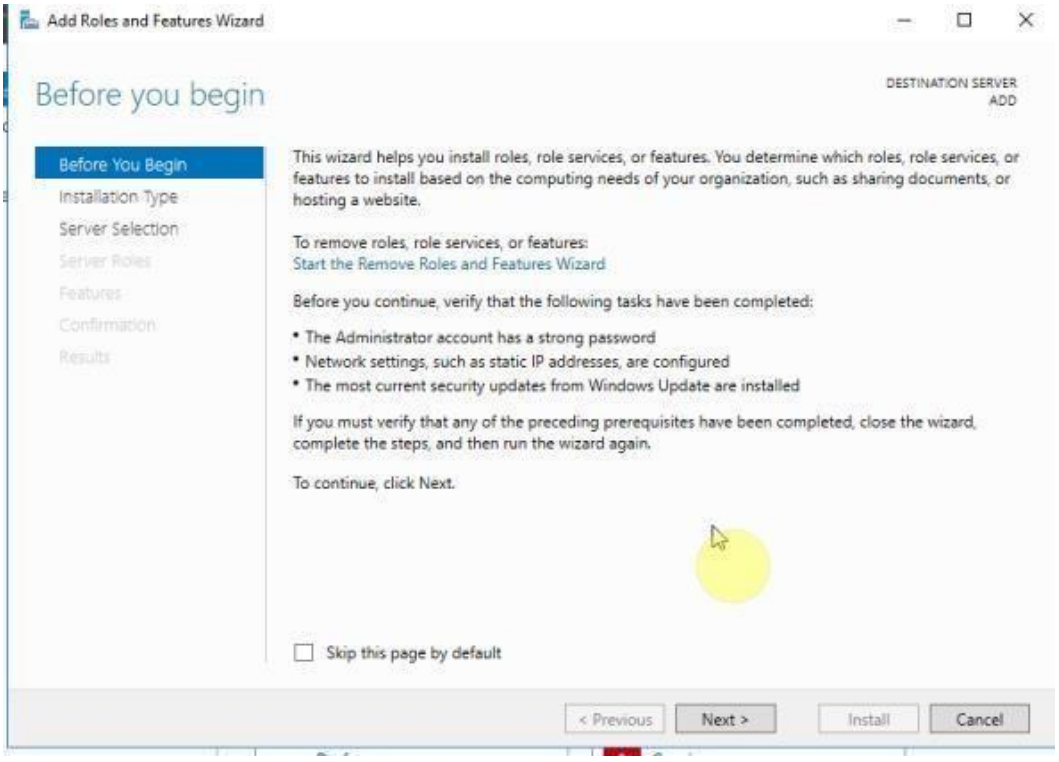
Hình 3.42 Thiết lập địa chỉ IP cho máy CDC

- Mở Server Manager , sau đó chọn Add roles and features.



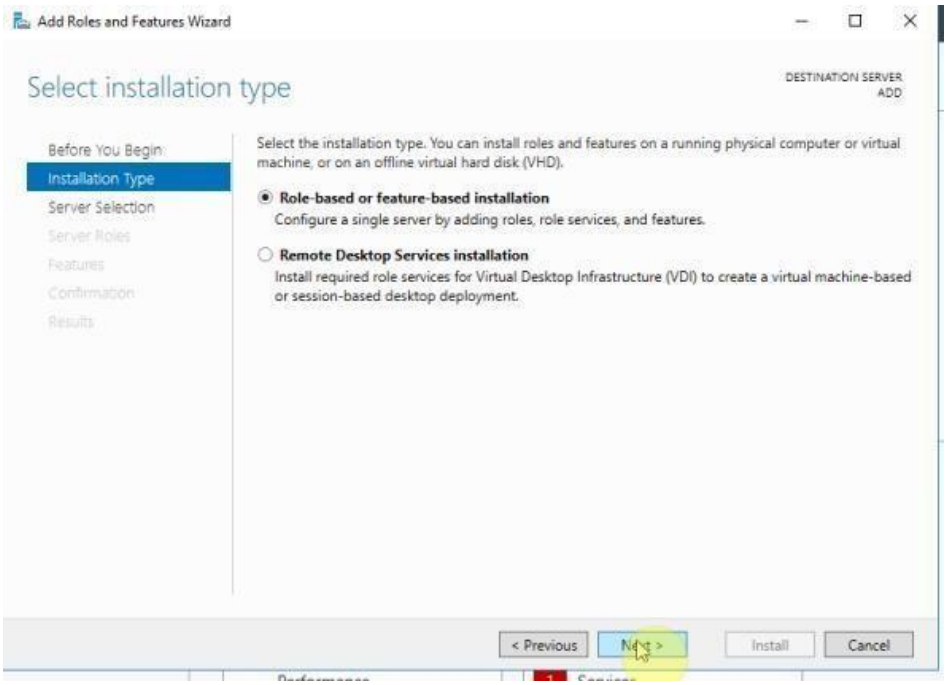
Hình 3.43 Hộp thoại Server Manager

- Màn hình giới thiệu chọn Next để qua bước tiếp theo



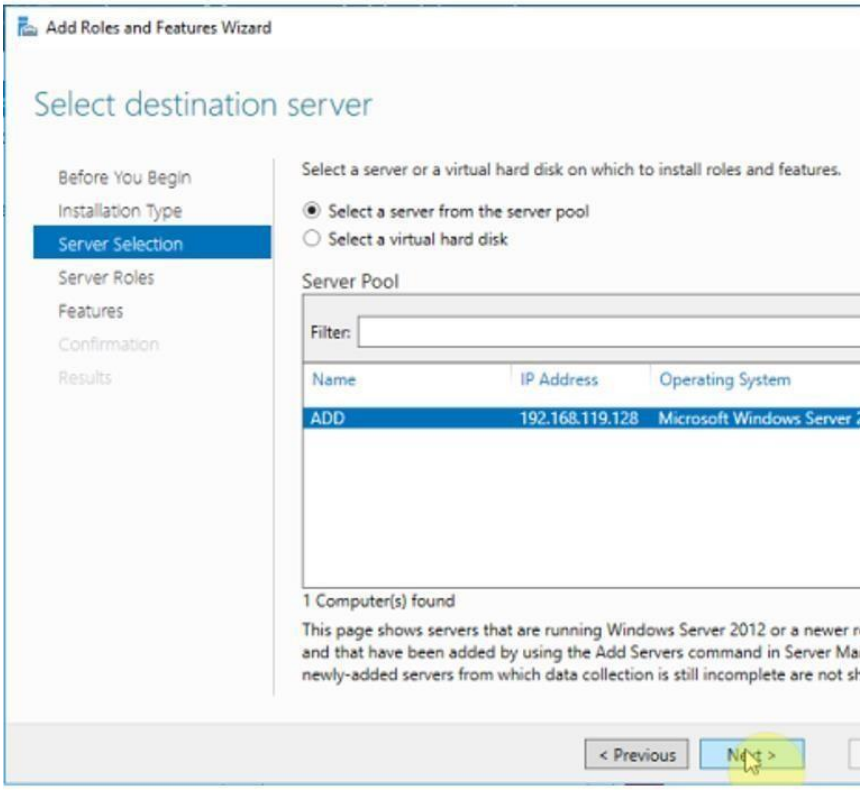
Hình 3.44 Hộp thoại Before you begin

- Chọn Role based or…..Click Next



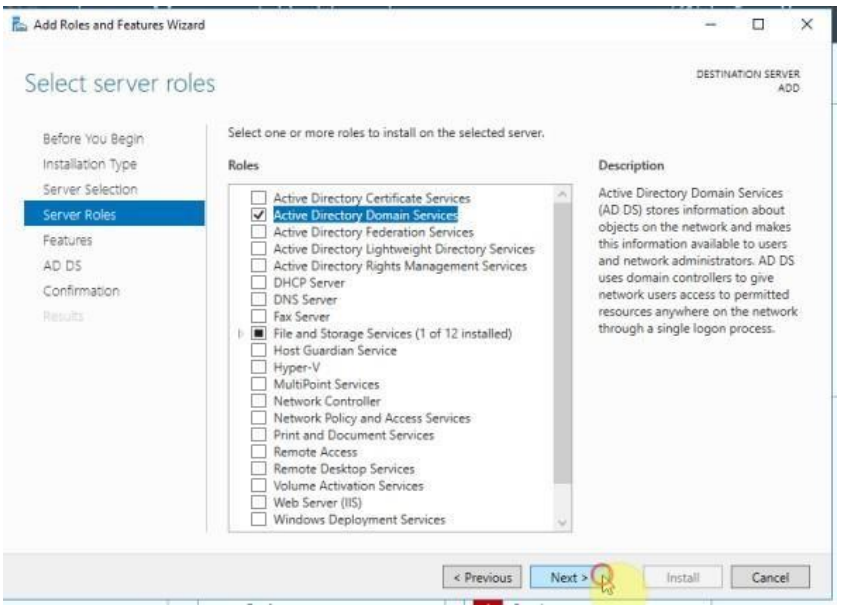
Hình 3.45 Hộp thoại Select installation type

- Chọn Select a Server from the server pool, Click Next



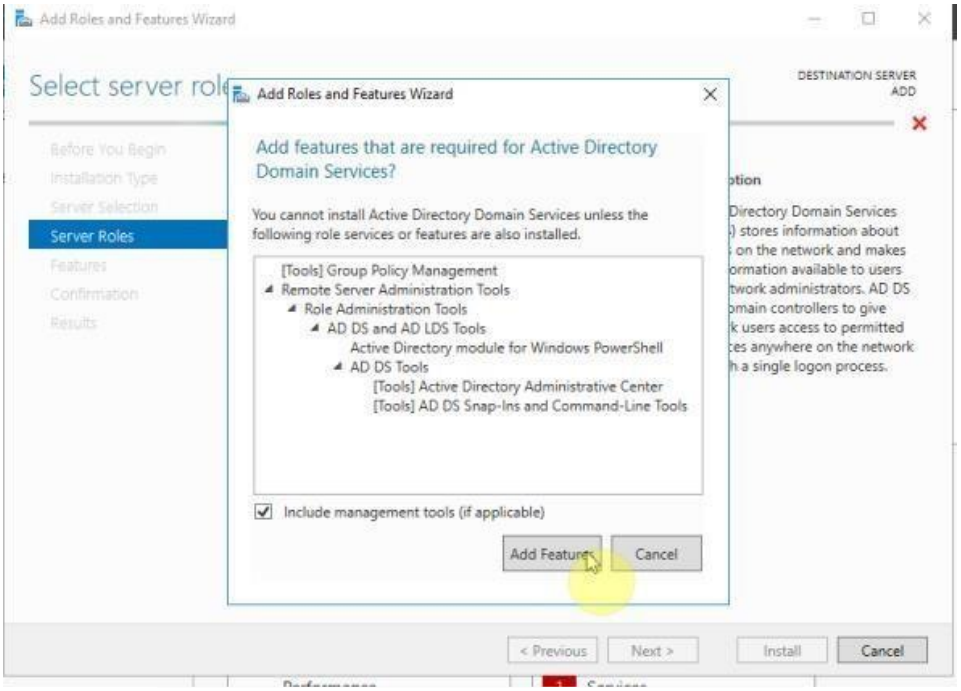
Hình 3.46 Hộp thoại Select destination server

- Ở màn hình Select Server Roles, bạn đánh dấu chọn vào Active Directory Domain Services



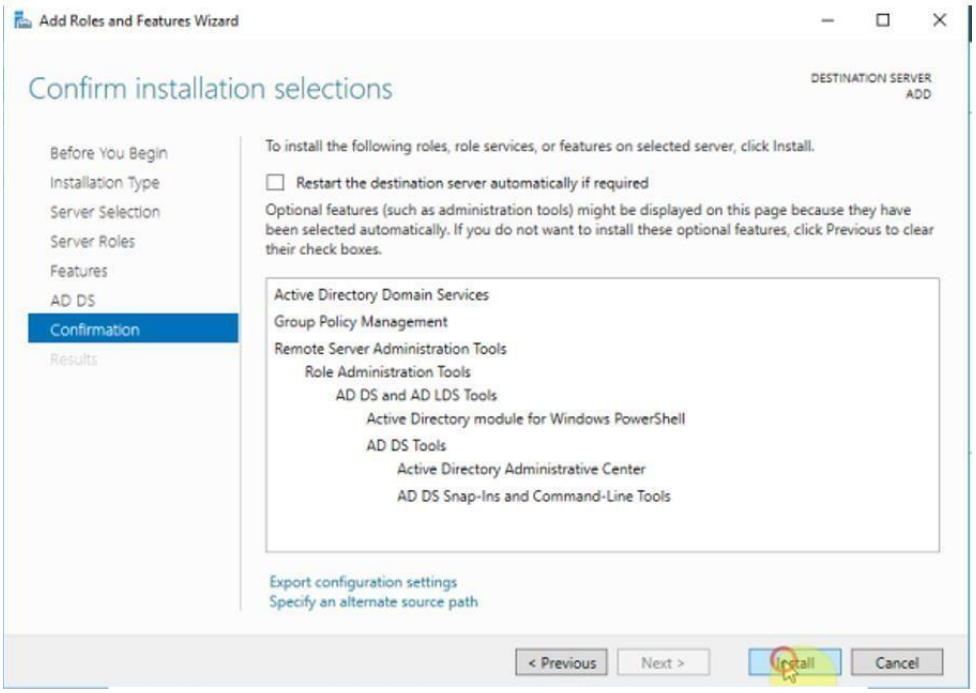
Hình 3.47 Hộp thoại Select server role

- Chọn Add Features



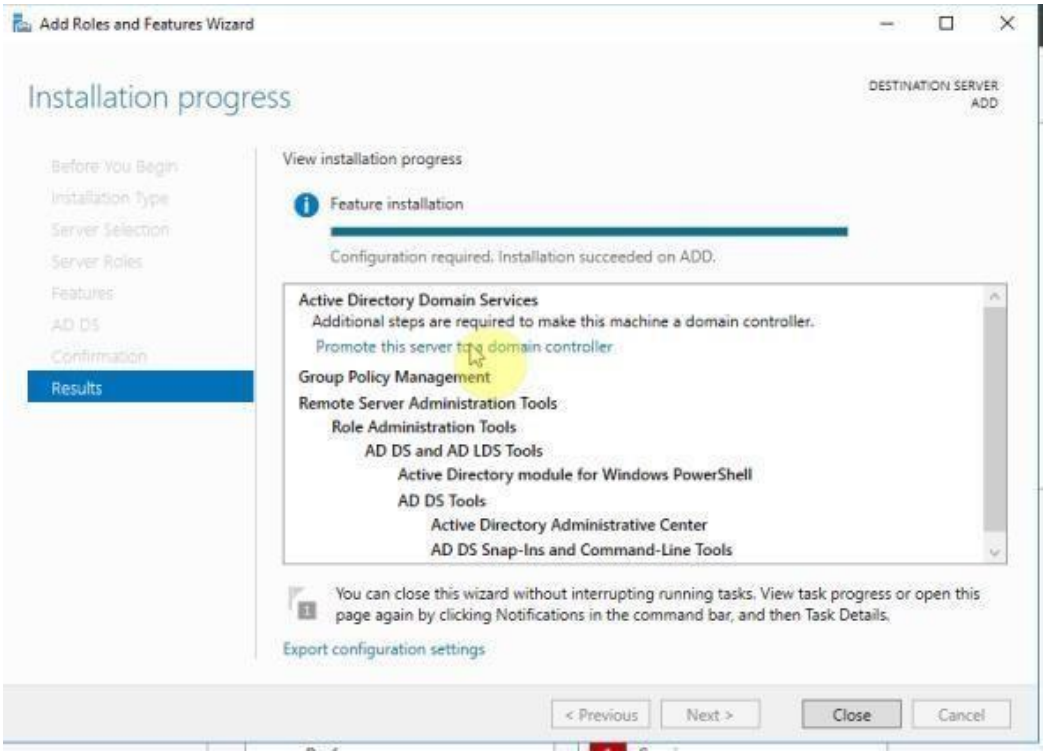
Hình 3.48 Chọn Add Features

- Các bước còn lại nhấn Next theo mặc định. Màn hình Confirm installation selections, nếu đánh dấu chọn vào ô Restart the destination server automatically if required (hệ thống sẽ tự khởi động lại khi có yêu cầu), sau đó Click Install, để bắt đầu cài đặt.



Hình 3.49 Hộp thoại Confirm installation selections

- Sau khi hoàn tất, nhấp vào Promote this Server to a domain controller.



Hình 3.50 Cài đặt hoàn tất

- Màn hình Deployment Configuration, chương trình cung cấp ba tùy chọn:

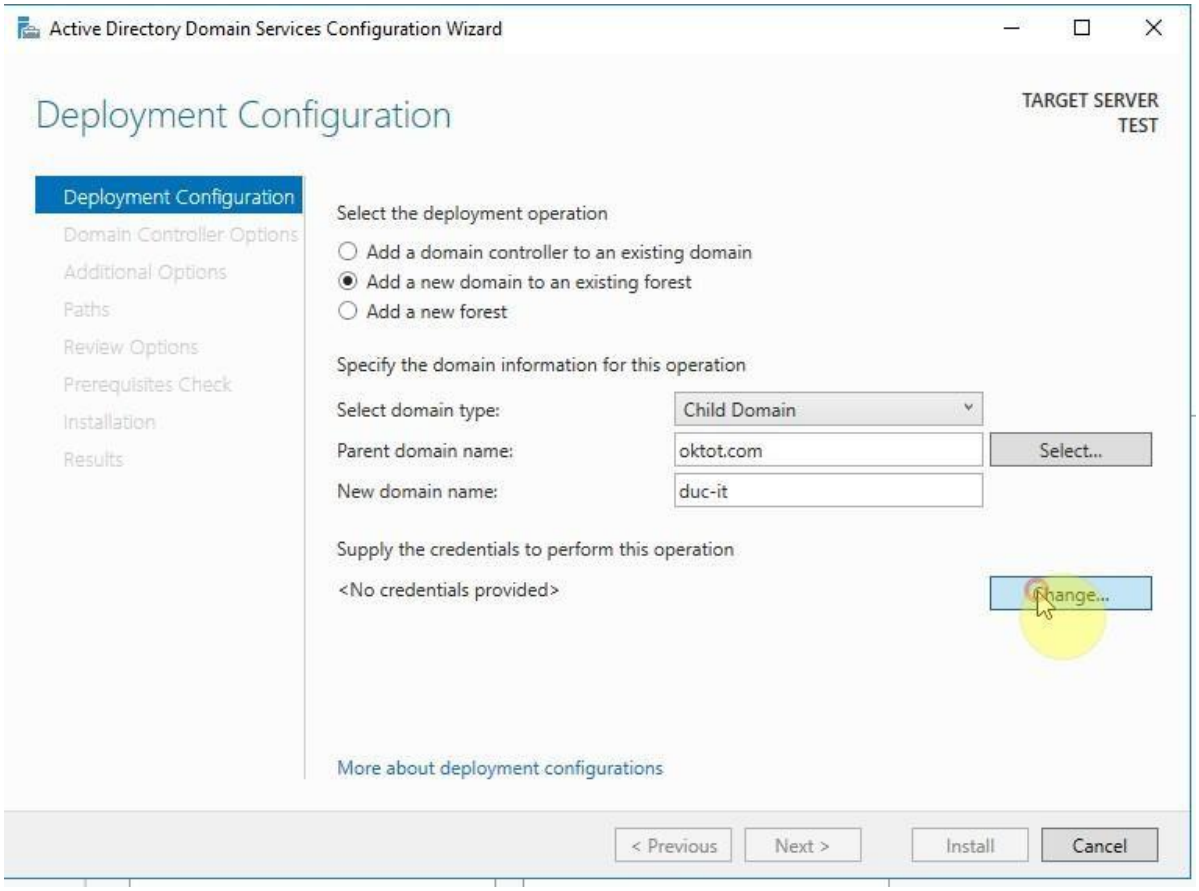
  - Add a domain controller to an existing domain: Thêm một ADC vào domain có sẵn.

- Add a new domain to an existing forest: Xây dựng domain mới trong forest có sẵn.
- Add new forest: xây dựng máy DC đầu tiên của forest.

- Do đang xây dựng CDC nên chọn vào tùy chọn đầu tiên là Add a new domain controller to an existing forest.

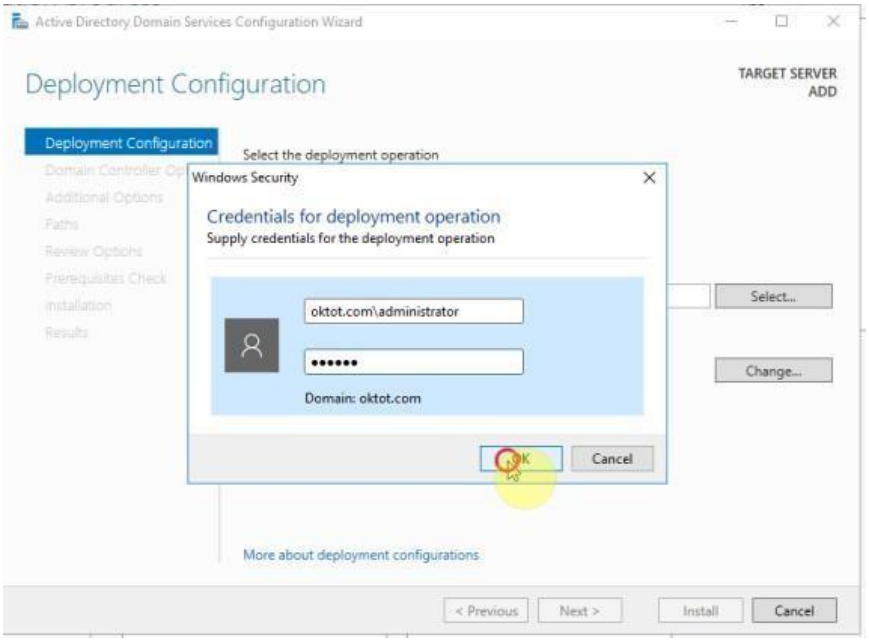
+ Mục Specify the domain information for this operation:

- Select domain type: chọn là Child Domain
- Parent domain: gõ tên domain của máy làm DC
- New domain name: gõ tên domain của máy sẽ làm child domain



Hình 3.51 Thiết lập miền con

+ Mục Supply the credentials to perform this operation, bạn phải dùng user Domain Admin thì mới có thể thực hiện việc cài CDC. Chọn Change để gõ user và password của user Domain Admin trên Domain controller



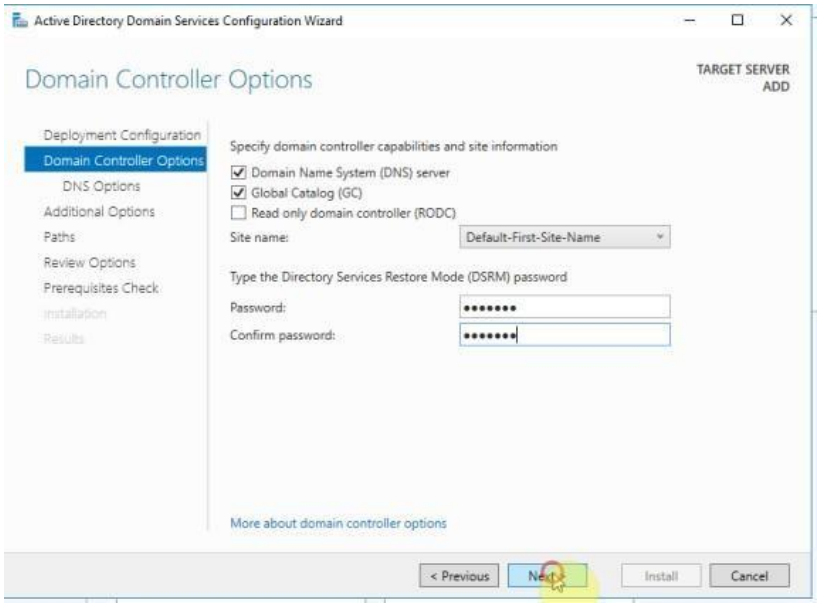
Hình 3.52 Sử dụng user Domain Admin

- Sau đó click Next

- Màn hình Domain Controller Options, check dấu chọn vào ô Domain Name System (DNS) server để cài đặt thêm DNS cho CDC.

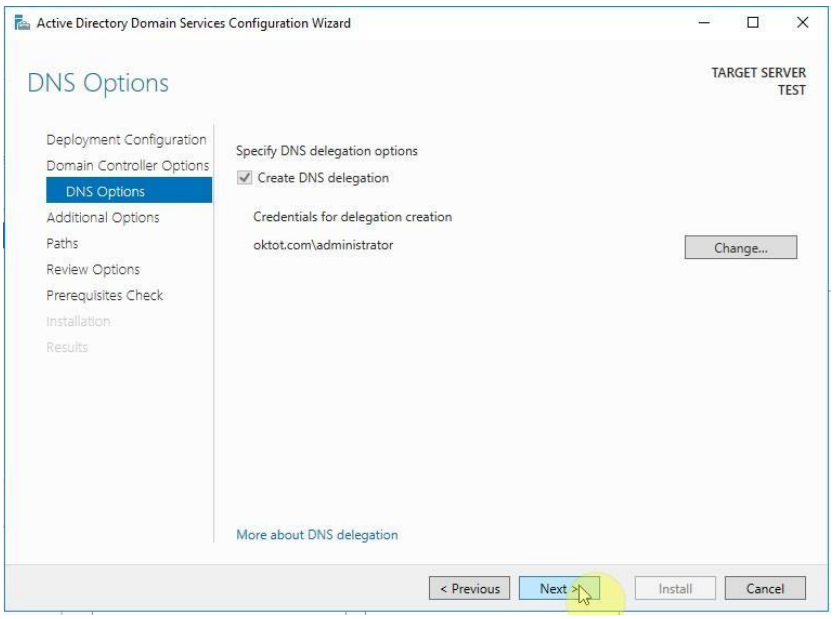
- Tiếp theo đánh dấu chọn vào ô Global Catalog (GC) để CDC có thể chứng thực khi user log on.

+ Bên dưới là mục Type the Directory Services Restore Mode (DSRM) password, nhập vào mật khẩu. Mật khẩu này sẽ được dùng để khôi phục AD ở chế độ Restore Mode.



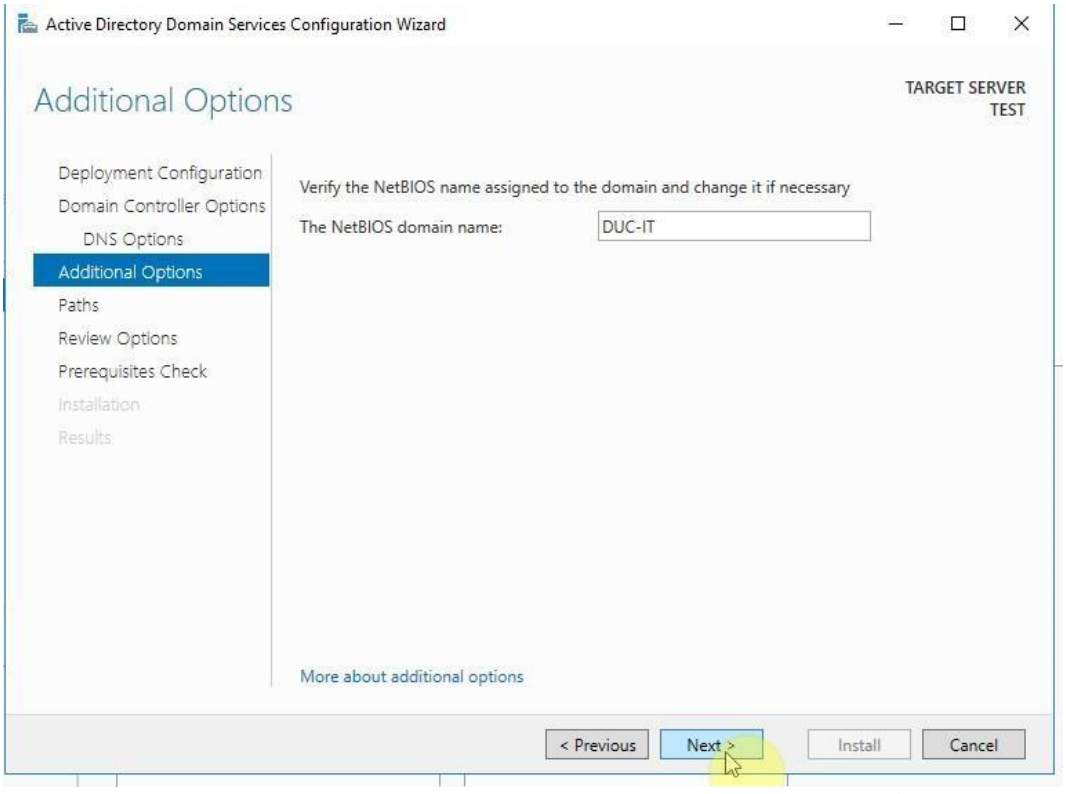
Hình 3.53 Hộp thoại Domain Controller Options

- Màn hình *DNS Options*, bạn Click Next



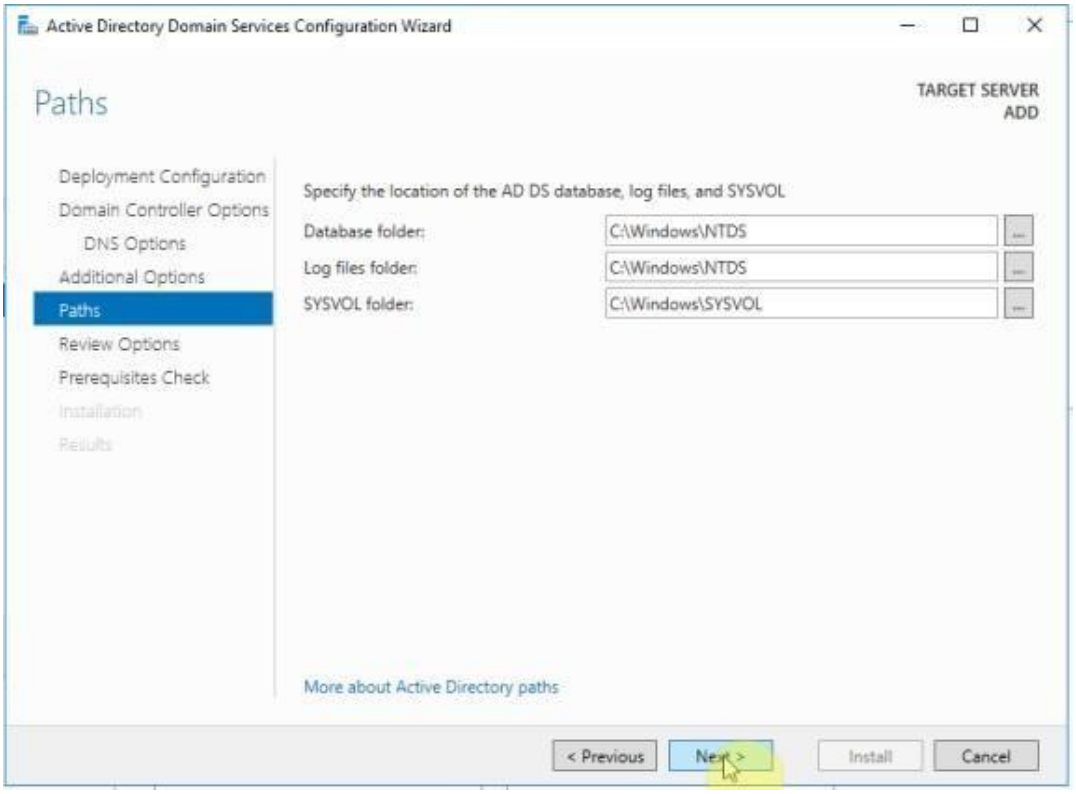
Hình 3.54 Hộp thoại Domain Controller Options

- Đặt lại tên NetBIOS hoặc sử dụng tên NetBIOS mặc định,sau đó click Next.



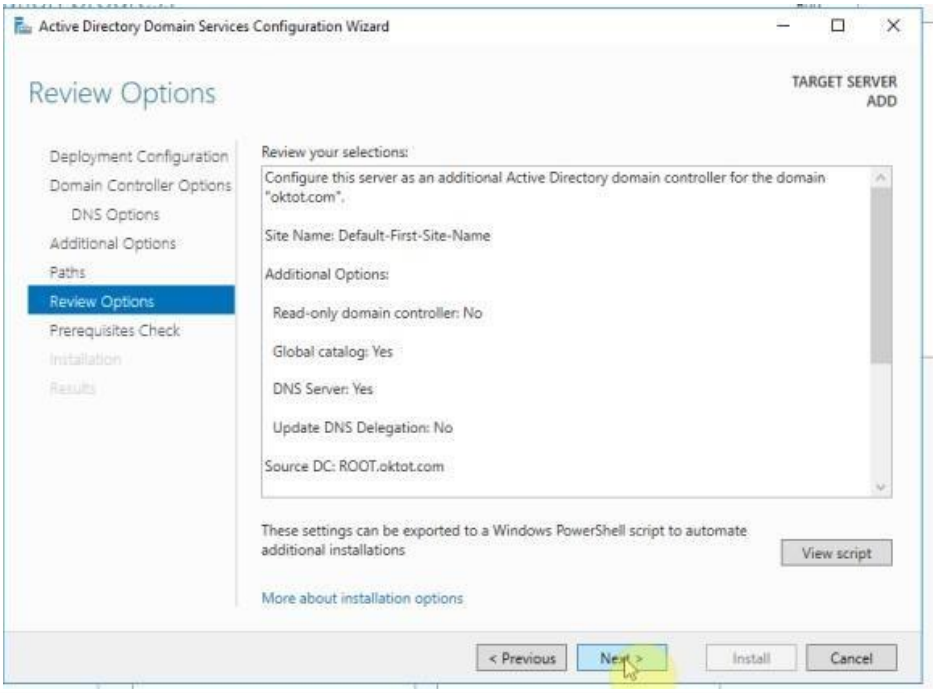
Hình 3.55 Đặt lại tên NetBIOS

- Màn hình Paths, chọn đường dẫn đến nơi cần lưu cơ sở dữ liệu của AD, log files và SYSVOL. click Next



Hình 3.56 Chọn đường dẫn đến nơi cần lưu cơ sở dữ liệu của AD

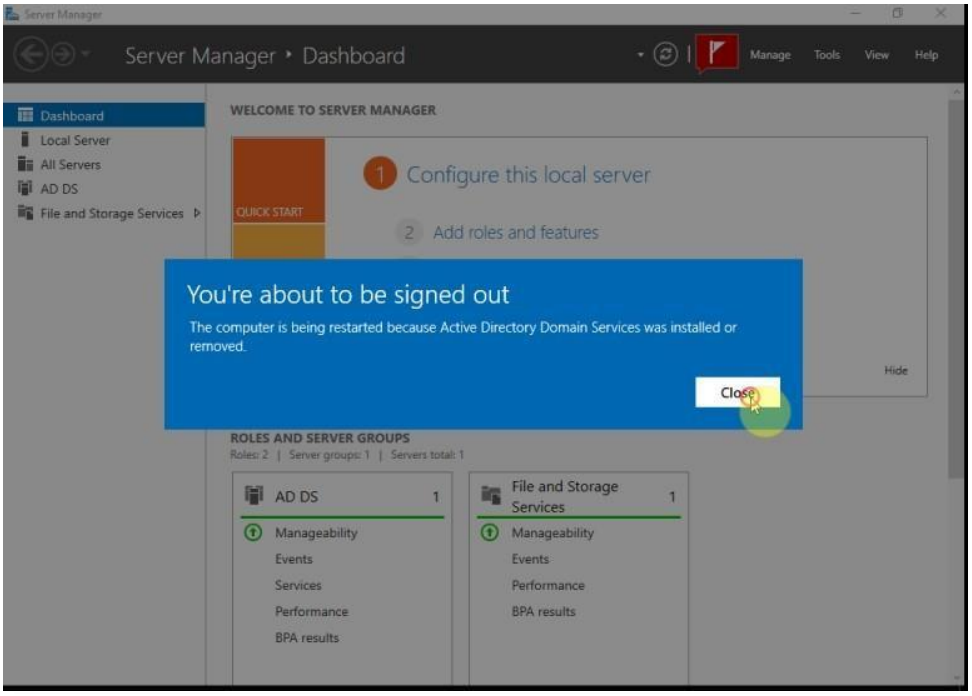
- Click Next.



Hình 3.57 Hộp thoại Review Option

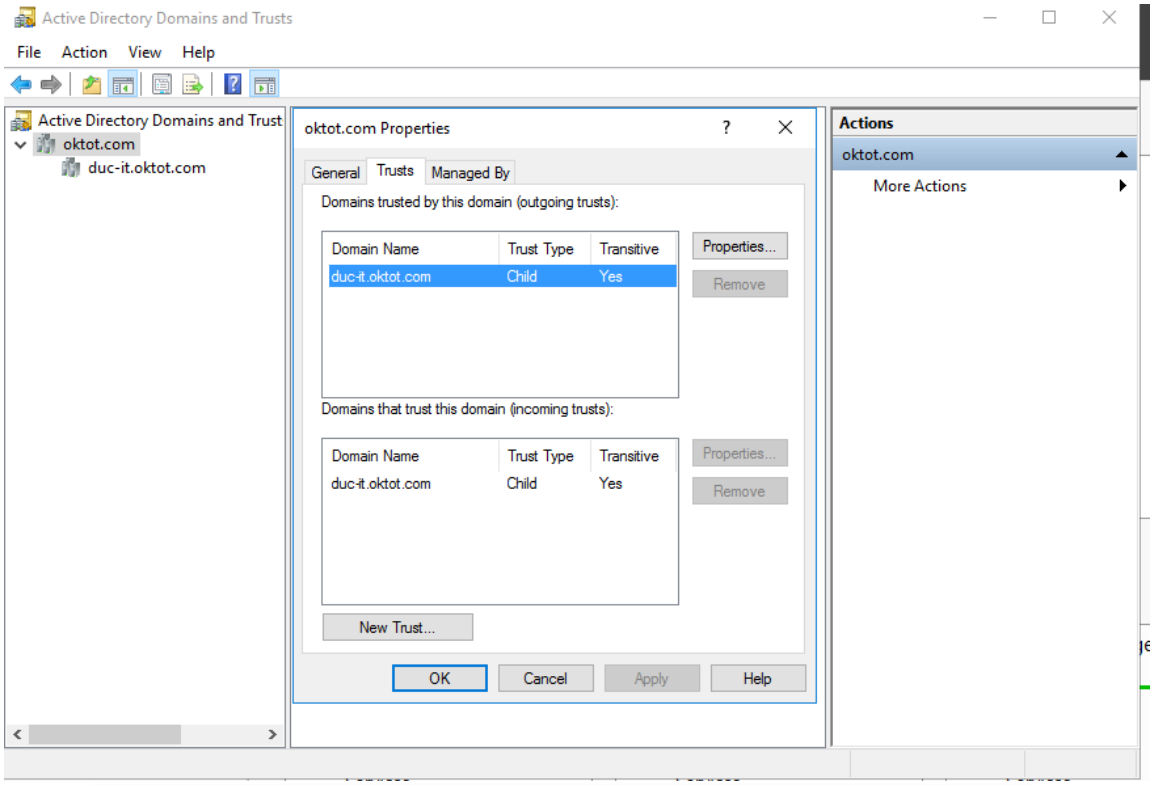
- Màn hình Prerequisites Check, khi nhận được thông báo All prerequisites check passed successfully nghĩa là quá trình kiểm tra điều kiện để cài đặt ADC đã thành công. Click Install để bắt đầu cài đặt.

- Sau khi hoàn tất, máy tính sẽ khởi động lại.



Hình 3.58 Cài đặt hoàn tất

- Sau khi khởi động, mở Server Manager > chọn Active Directory Domain an Trusts để kiểm tra.



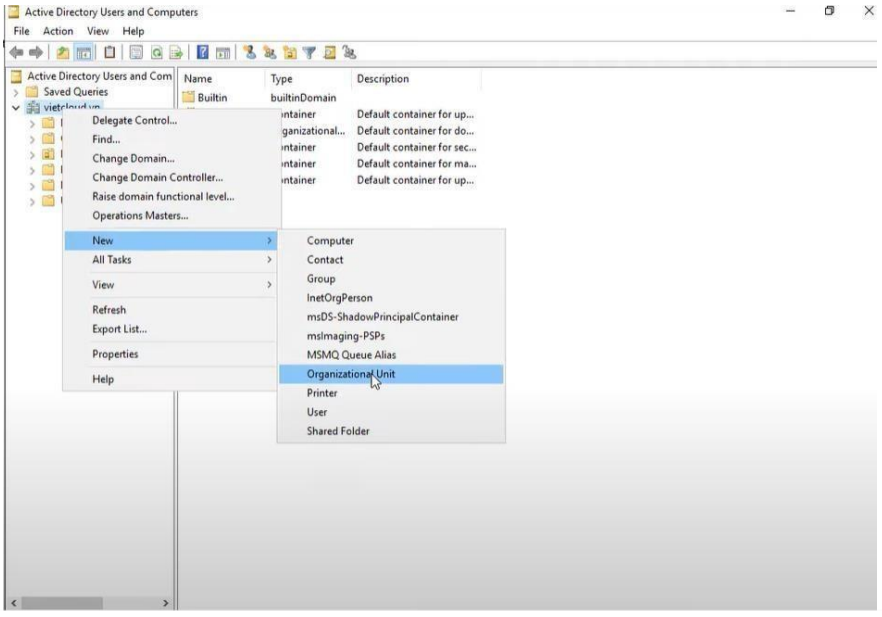
Hình 3.59 Kiểm tra sau khi cài đặt

3.5. Xây dựng Organizational Unit

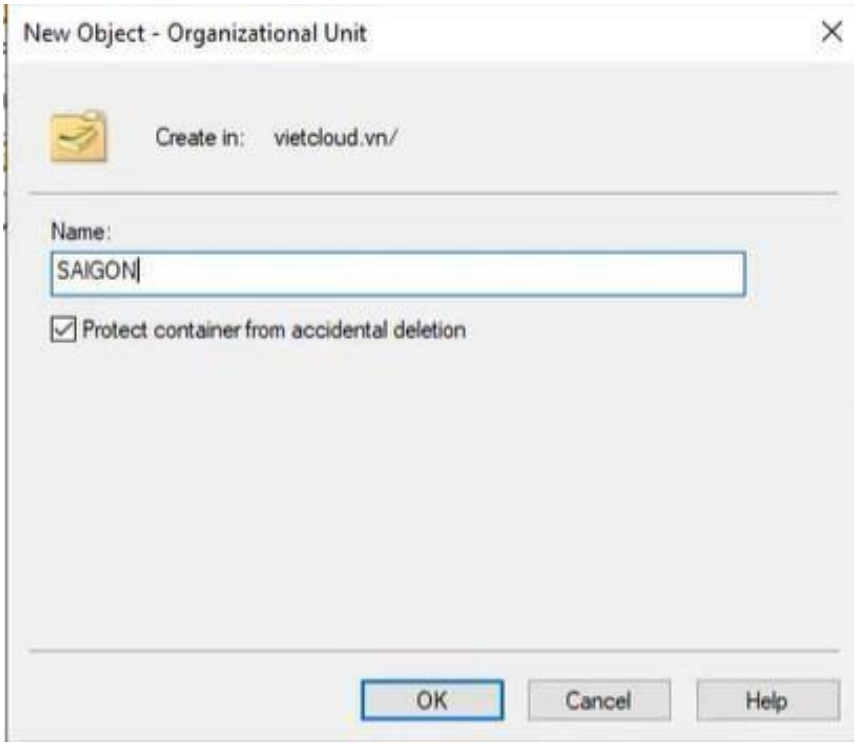
OU (Organization Unit) là 1 container sử dụng để sắp xếp các đối tượng trong 1 miền vào 1 nhóm quản trị logic. 1 OU có thể chứa các đối tượng như tài

khoản người dùng , nhóm , máy tính , các ứng dụng hoặc OU khác . OU được biểu diễn bằng biểu tượng thư mục với 1 quyển sách bên trong , nó có thể được thêm vào OU khác tạo nên cấu trúc phân cấp .

Để tạo OU vào Vào Start / Programs / Administrative Tools / Active Directory Users and Computers, click chuột phải vào tên miền chọn New ->Organization Unit



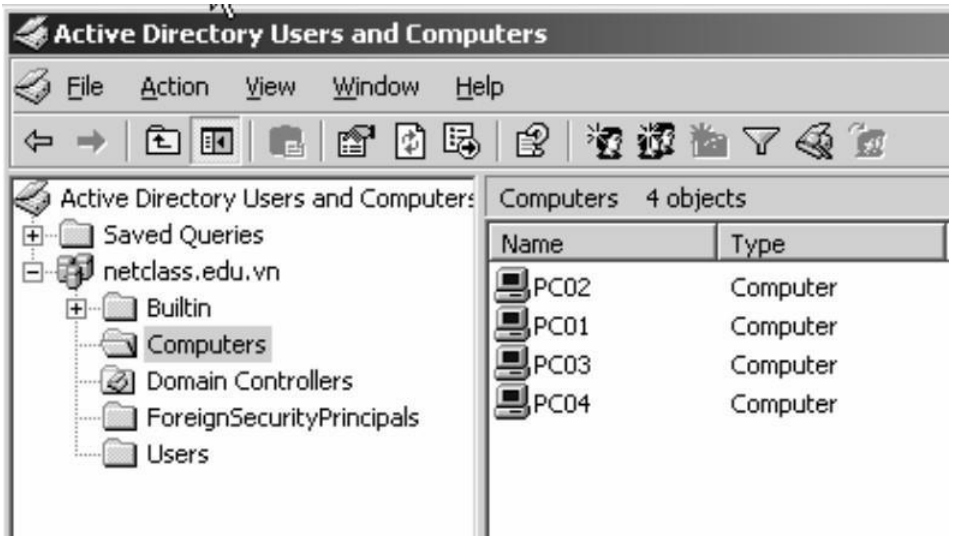
Hình 3.60 Tạo OU



Hình 3.61 Đặt tên cho OU

3.6. Công cụ quản trị các đối tượng trong Active Directory

Một trong bốn công cụ quản trị hệ thống Active Directory thì công cụ Active Directory User and Computer là công cụ quan trọng nhất và chúng ta sẽ gặp lại nhiều trong trong giáo trình này, từng bước ta sẽ khảo sát hết các tính năng trong công cụ này. Công cụ này có chức năng tạo và quản lý các đối tượng cơ bản của hệ thống Active Directory



Hình 3.62 Đối tượng trong Active Directory

Theo hình trên chúng ta thấy trong miền netclass.edu.vn có các mục sau:

- Builtin: chứa các nhóm người dùng đã được tạo và định nghĩa quyền sẵn.

- Computers: chứa các máy trạm mặc định đang là thành viên của miền. Bạn cũng có thể dùng tính năng này để kiểm tra một máy trạm gia nhập vào miền có thành công không.

- Domain Controllers: chứa các điều khiển vùng (Domain Controller) hiện đang hoạt động trong miền. Bạn cũng có thể dùng tính năng này để kiểm tra việc tạo thêm Domain Controller đồng hành có thành công không.

- ForeignSecurityPrincipals: là một vật chứa mặc định dành cho các đối tượng bên ngoài miền đang xem xét, từ các miền đã thiết lập quan hệ tin cậy (trusted domain).

Users: chứa các tài khoản người dùng mặc định trên miền

CÂU HỎI VÀ BÀI TẬP BÀI 3

1. Máy DC1 cài Windows Server 2019 (nâng cấp lên domain controller) có địa chỉ IP: 192.168.1.4. Máy Server1 cài Windows Server 2019 có địa chỉ IP: 192.168.1.10. Hãy cài đặt và cấu hình Addition Directory Controller máy Server1 và kiểm tra sự đồng bộ giữa hai máy DC1 và Server1.

2. Máy SServer có địa chỉ IP: 192.168.1.20. Hãy cài đặt và cấu hình máy SServer làm Subdomain của DC1

BÀI 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

Mã bài: MĐ 15 - 04

Giới thiệu:

Hệ điều hành Windows Server là hệ điều hành đa người dùng nên việc quản lý người dùng, nhóm rất quan trọng

Bài này sẽ giới thiệu những khái niệm về User, group, cách tạo và quả lý trên server.

Mục tiêu:

- Mô tả được tài khoản người dùng, tài khoản nhóm, các thuộc tính của người dùng;
- Tạo và quản trị được tài khoản người dùng, tài khoản nhóm.

Nội dung chính:

1. Định nghĩa tài khoản người dùng và tài khoản nhóm

1.1. Tài khoản người dùng

Tài khoản người dùng (**user account**) là một đối tượng quan trọng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng **username**. Chuỗi nhận dạng này giúp hệ thống mạng phân biệt giữa người này và người khác trên mạng từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép.

1.1.1. Tài khoản người dùng cục bộ

Tài khoản người dùng cục bộ (local user account) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy domain controller hoặc máy tính chứa tài nguyên chia sẻ.

1.1.2. Tài khoản người dùng miền

Tài khoản người dùng miền (**domain user account**) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng.

1.2. Tài khoản nhóm

Tài khoản nhóm (**group account**) là một đối tượng đại diện cho một nhóm

người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp chúng ta dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý.

2. Chứng thực và kiểm soát truy cập

2.1. Các giao thức chứng thực

Chứng thực trong Windows Server là quy trình gồm hai giai đoạn: đăng nhập tương tác và chứng thực mạng. Khi người dùng đăng nhập vùng bằng tên và mật mã, quy trình đăng nhập tương tác sẽ phê chuẩn yêu cầu truy cập của người dùng. Với tài khoản cục bộ, thông tin đăng nhập được chứng thực cục bộ và người dùng được cấp quyền truy cập máy tính cục bộ. Với tài khoản miền, thông tin đăng nhập được chứng thực trên Active Directory và người dùng có quyền truy cập các tài nguyên trên mạng. Như vậy với tài khoản người dùng miền ta có thể chứng thực trên bất kỳ máy tính nào trong miền.

Windows hỗ trợ nhiều giao thức chứng thực mạng, nổi bật nhất là:

- Kerberos V5: là giao thức chuẩn Internet dùng để chứng thực người dùng và hệ thống.

- Secure Socket Layer/Transport Layer Security (SSL/TLS): là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ Web an toàn.

2.2. Số nhận diện bảo mật SID

Tuy hệ thống Windows Server dựa vào tài khoản người dùng (user account) để mô tả các quyền hệ thống (rights) và quyền truy cập (permission) nhưng thực sự bên trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật SID (Security Identifier). SID là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không quan tâm đến các giá trị này. SID bao gồm phần SID vùng cộng thêm với một RID của người dùng không trùng lặp. SID có dạng chuẩn "S-1-5-21-D1-D2-D3-RID", khi đó tất cả các SID trong miền đều có cùng giá trị D1, D2, D3, nhưng giá trị RID là khác nhau. Hai mục đích chính của việc hệ thống sử dụng SID là:

- Dễ dàng thay đổi tên tài khoản người dùng mà các quyền hệ thống và quyền truy cập không thay đổi.

- Khi xóa một tài khoản thì SID của tài khoản đó không còn giá trị nữa, nếu có tạo một tài khoản mới cùng tên với tài khoản vừa xóa thì các quyền cũ cũng không sử dụng được bởi vì khi tạo tài khoản mới thì giá trị SID của tài khoản này là một giá trị mới

2.3. Kiểm soát hoạt động truy cập của đối tượng

Active Directory là dịch vụ hoạt động dựa trên các đối tượng, có nghĩa là người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào bộ mô tả bảo mật ACE. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy cập đối tượng.
- Định rõ quyền truy cập cho người dùng và nhóm.
- Theo dõi các sự kiện xảy ra trên đối tượng.
- Định rõ quyền sở hữu của đối tượng.

Các thông tin của một đối tượng Active Directory trong bộ mô tả bảo mật được xem là mục kiểm soát hoạt động truy cập ACE (Access Control Entry). Một ACL (Access Control List) chứa nhiều ACE, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng. ACL có đặc tính kế thừa, có nghĩa là thành viên của một nhóm thì được thừa hưởng các quyền truy cập đã cấp cho nhóm này.

3. Các tài khoản tạo sẵn

3.1.Tài khoản người dùng tạo sẵn

Tài khoản người dùng tạo sẵn (Built-in) là những tài khoản người dùng mà khi ta cài đặt Windows Server thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằm trong Container Users của công cụ Active Directory User and Computer như: Administrator, Guest,…

3.2.Tài khoản nhóm Domain Local tạo sẵn

Chúng ta thấy trong công cụ Active Directory User and Computers, container Users chứa nhóm universal, nhóm domain local và nhóm global là do hệ thống đã mặc định quy định trước. Nhưng một số nhóm domain local đặc biệt được đặt trong container Built-in, các nhóm này không được di chuyển sang các OU khác, đồng thời nó cũng được gán một số quyền cố định trước nhằm phục

vụ cho công tác quản trị và không có quyền xóa các nhóm đặc biệt này. Tài khoản nhóm Domain Local tạo sẵn như: Administrators, Domain Controllers, Guests,…

3.3.Tài khoản nhóm Global tạo sẵn

Tên nhóm	Mô tả
Domain Admins	Thành viên của nhóm này có thể toàn quyền quản trị các máy tính trong miền vì mặc định khi gia nhập vào miền các **member server** và các máy trạm đã đưa nhóm **Domain Admins** là thành viên của nhóm cục bộ **Administrators** trên các máy này.
Domain Users	Theo mặc định mọi tài khoản người dùng trên miền đều là thành viên của nhóm này. Mặc định nhóm này là thành viên của nhóm cục bộ **Users** trên các máy **server** thành viên và máy trạm.
Group Policy Creator Owners	Thành viên nhóm này có quyền sửa đổi chính sách nhóm của miền, theo mặc định tài khoản **administrator** miền là thành viên của nhóm này.
Enterprise Admins	Đây là một nhóm **universal**, thành viên của nhóm này có toàn quyền trên tất cả các miền trong rừng đang xét. Nhóm này chỉ xuất hiện trong miền gốc của rừng thôi. Mặc định nhóm này là thành viên của nhóm **administrators** trên các **Domain Controller** trong rừng.
Schema Admins	Nhóm **universal** này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức (**schema**) của **Active Directory**.

Bảng 4.1 Mô tả tài khoản nhóm Global tạo sẵn

3.4.Các nhóm tạo sẵn đặc biệt

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống Windows Server còn có một số nhóm tạo sẵn đặt biệt, chúng không xuất hiện trên cửa sổ của công cụ Active Directory User and Computer, mà chúng chỉ xuất hiện trên các ACL của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

- Interactive: đại diện cho những người dùng đang sử dụng máy tại chỗ.

- Network: đại diện cho tất cả những người dùng đang nối kết mạng đến một máy tính khác.

- Everyone: đại diện cho tất cả mọi người dùng.

- System: đại diện cho hệ điều hành.

- Creator owner: đại diện cho những người tạo ra, những người sở hữu một tài nguyên nào đó như: thư mục, tập tin, tác vụ in ấn (print job)…

- Authenticated users: đại diện cho những người dùng đã được hệ thống xác thực, nhóm này được dùng như một giải pháp thay thế an toàn hơn cho nhóm everyone.

- Anonymous logon: đại diện cho một người dùng đã đăng nhập vào hệ thống một cách nặc danh, chẳng hạn một người sử dụng dịch vụ FTP.

- Service: đại diện cho một tài khoản mà đã đăng nhập với tư cách như một dịch vụ.

- Dialup: đại diện cho những người đang truy cập hệ thống thông qua Dialup Networking.

4. Quản lý tài khoản người dùng và nhóm cục bộ

4.1. Công cụ quản lý tài khoản người dùng cục bộ

Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã. Có hai phương thức truy cập đến công cụ **Local Users and Groups**:

- Dùng như một **MMC** (**Microsoft Management Console**) snap-in.
- Dùng thông qua công cụ **Computer Management.**

Các bước dùng để chèn **Local Users and Groups snap-in** vào trong **MMC**:

- Chọn **Start \ Run**, nhập vào hộp thoại **MMC** và ấn phím **Enter** để mở cửa sổ **MMC**.

- Chọn Console \ Add\Remove Snap-in để mở hộp thoại Add\Remove Snap-in
- Nhấp chuột vào nút Add để mở hộp thoại Add Standalone Snap-in. Chọn Local Users and Groups và nhấp chuột vào nút Add. Hộp thoại Choose Target Machine xuất hiện, ta chọn Local Computer và nhấp chuột vào nút Finish để trở lại hộp thoại Add Standalone Snap-in.
- Nhấp chuột vào nút Close để trở lại hộp thoại Add\Remove Snap-in.
- Nhấp chuột vào nút OK
- Lưu Console bằng cách chọn Console \ Save, sau đó nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu console ngay trên Desktop.
- Nếu máy tính của không có cấu hình MMC thì cách nhanh nhất để truy cập công cụ Local Users and Groups thông qua công cụ Computer Management. Click phải chuột vào My Computer và chọn Manage từ pop-up menu và mở cửa sổ Computer Management. Trong mục System Tools, ta sẽ nhìn thấy mục Local Users and Groups
- Cách khác để truy cập đến công cụ Local Users and Groups là vào Start \ Programs\Administrative Tools \ Computer Management

4.2. Các tao tác cơ bản trên tài khoản người dùng cục bộ

4.2.1. Tạo tài khoản mới

Trong công cụ **Local Users and Groups**, ta nhấp phải chuột vào **Users** và chọn **New User**, hộp thoại **New User** hiển thị bạn nhập các thông tin cần thiết vào, nhưng quan trọng nhất và bắt buộc phải có là mục **Username**.

4.2.2. Xóa tài khoản

Bạn nên xóa tài khoản người dùng, nếu bạn chắc rằng tài khoản này không bao giờ cần dùng lại nữa. Muốn xóa tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần xóa, nhấp phải chuột và chọn **Delete** hoặc vào thực đơn **Action \ Delete**.

4.2.3. Khóa tài khoản

Khi một tài khoản không sử dụng trong thời gian dài bạn nên khóa lại vì lý do bảo mật và an toàn hệ thống. Nếu xóa tài khoản này đi thì không thể phục hồi lại được do đó ta chỉ tạm khóa. Trong công cụ **Local Users and Groups**, nhấp đôi chuột vào người dùng cần khóa, hộp thoại **Properties** của tài khoản xuất hiện.

Trong **Tab General**, đánh dấu vào mục **Account is disabled.**

4.2.4. Đổi tên tài khoản

Có thể đổi tên bất kỳ một tài khoản người dùng nào, đồng thời cũng có thể điều chỉnh các thông tin của tài khoản người dùng.

Muốn thay đổi tên tài khoản người dùng mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi tên, nhấp phải chuột và chọn **Rename**.

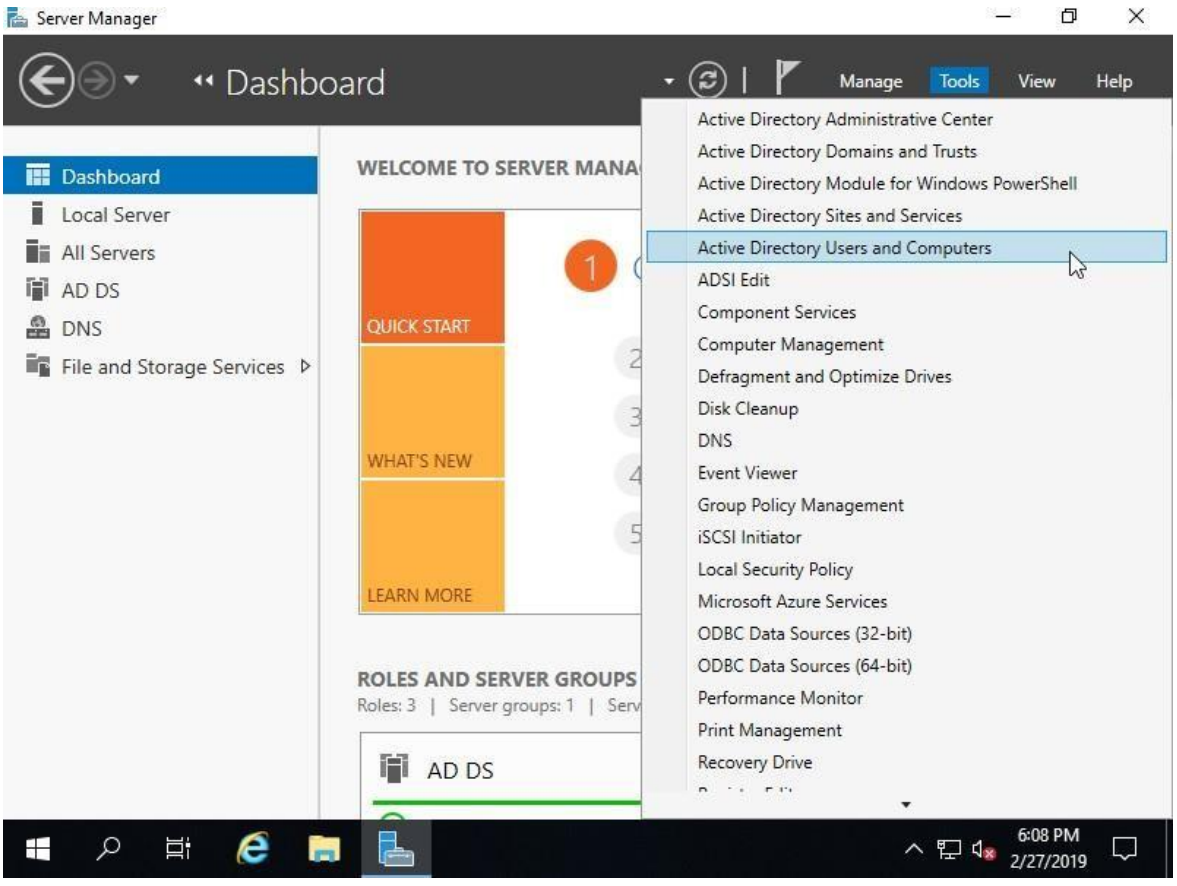
4.2.5. Thay đổi mật khẩu

Muốn đổi mật mã của người dùng mở công cụ Local Users and Groups, chọn tài khoản người dùng cần thay đổi mật mã, nhấp phải chuột và chọn Reset password.

5. Quản lý tài khoản người dùng nhóm trên Active Directory

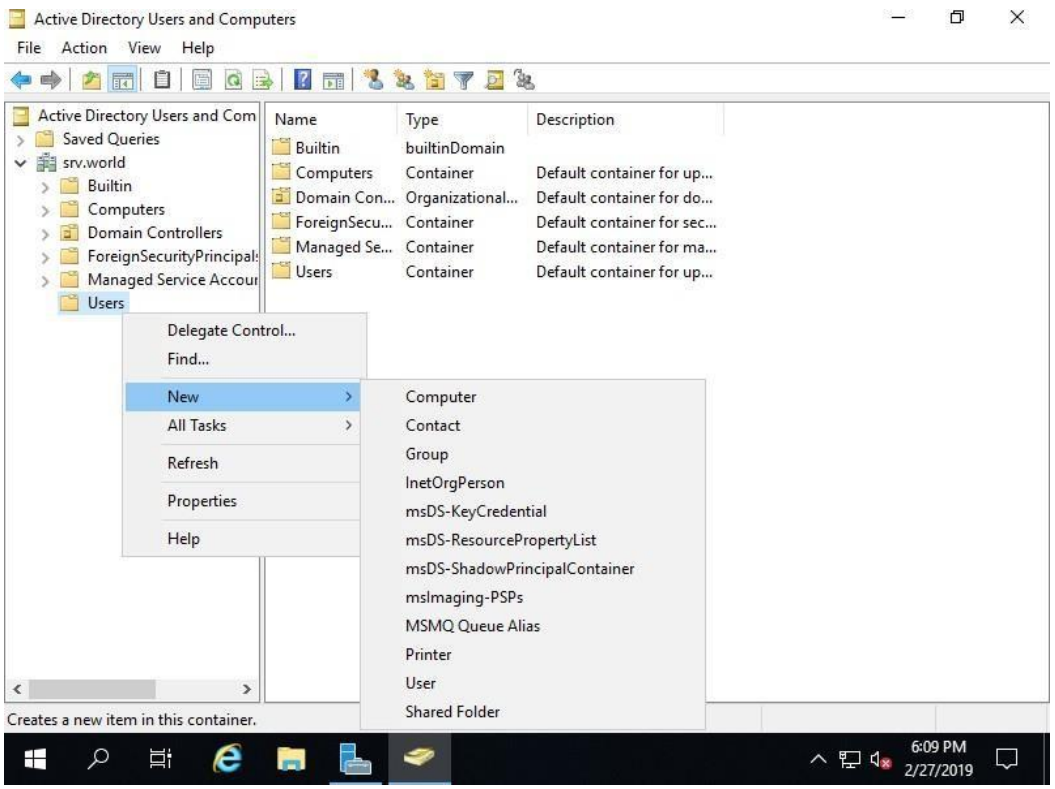
5.1. Tạo mới tài khoản người dùng

- Mở Server Manager, click Tools chọn Active Directory Users and Conputers.



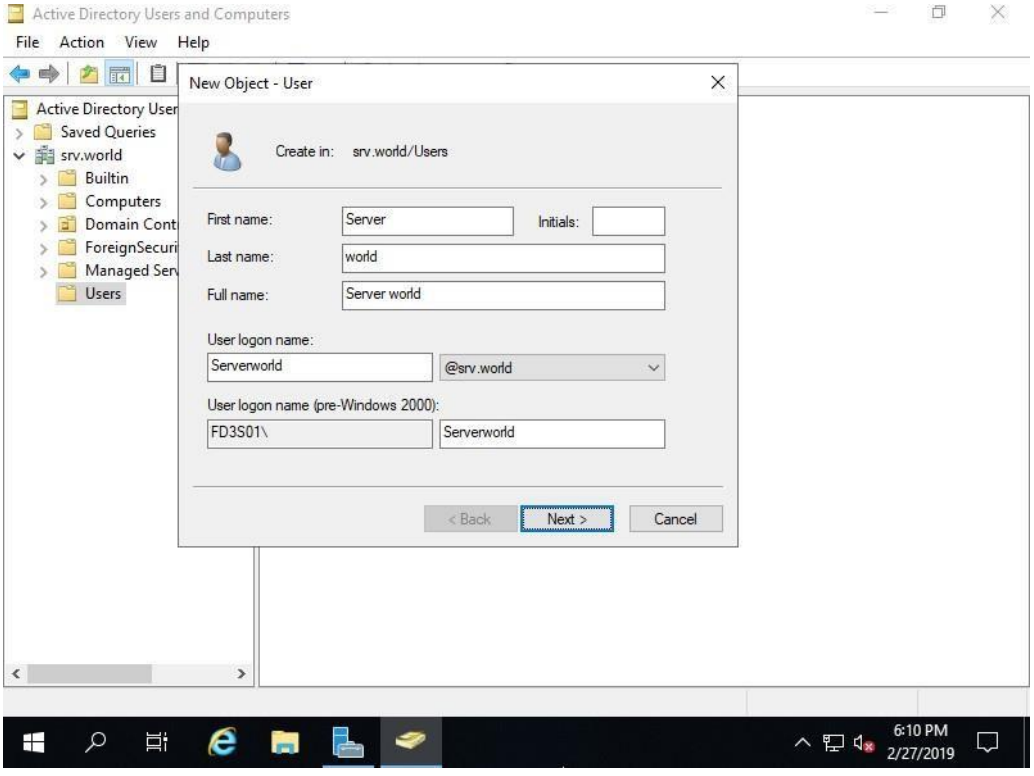
Hình 4.1 Chọn công cụ Active Directory Users and Computers

- Click chuột phải Users chọn New -> User.



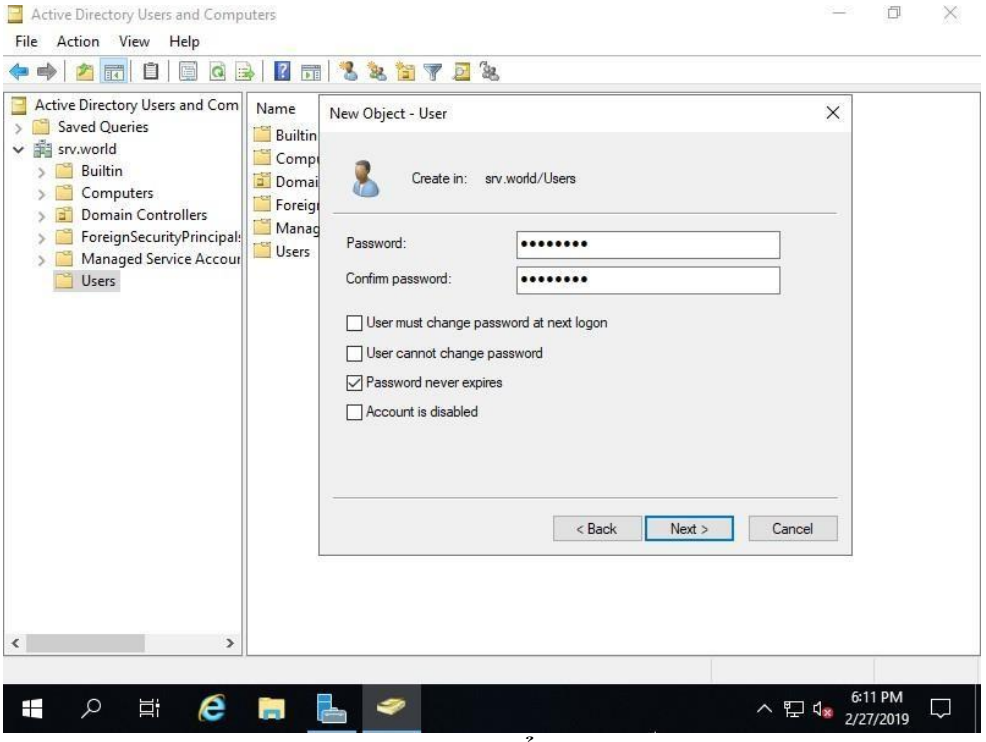
Hình 4.2 Chọn công cụ Active Directory Users and Computers

- Nhập tên mô tả người dùng, tên tài khoản logon cho người dùng, nhấn Next



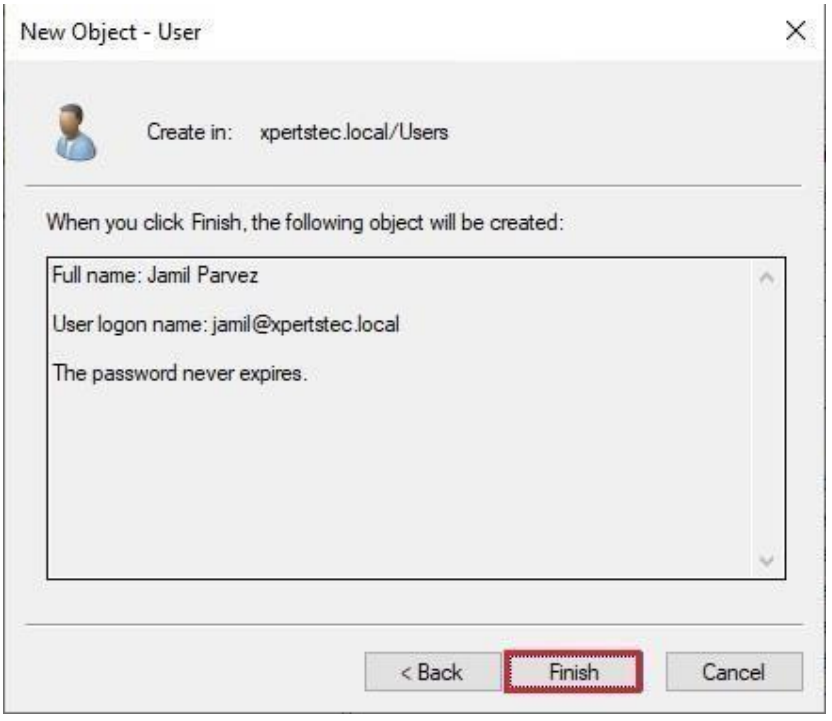
Hình 4.3 Nhập tên cho người dùng

- Nhập mật khẩu (password) của tài khoản người dùng và đánh dấu vào các lựa chọn liên quan đến tài khoản như: cho phép đổi mật khẩu, yêu cầu phải đổi mật khẩu lần đăng nhập đầu tiên hay khóa tài khoản, nhấn Next



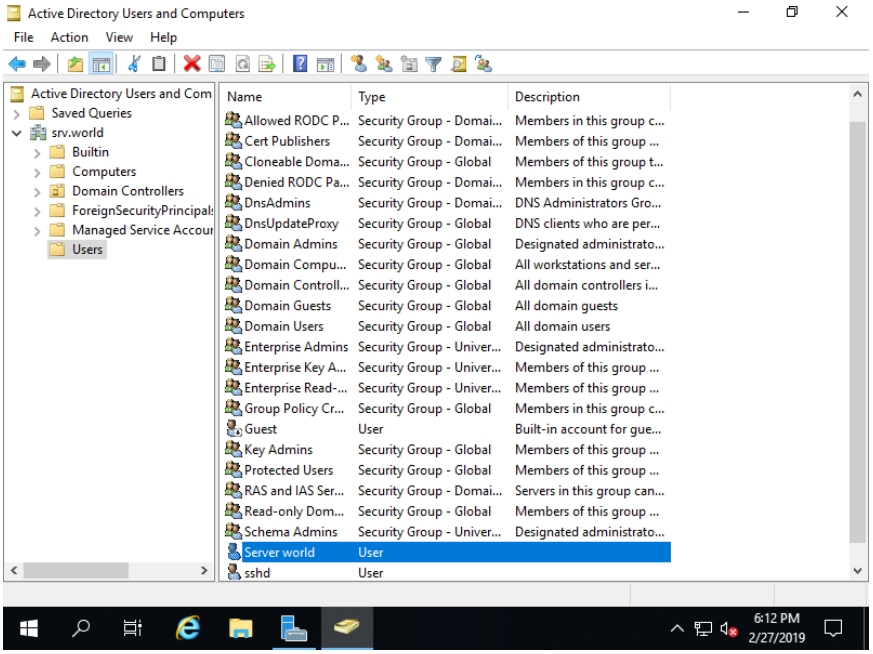
Hình 4.4 Nhập mật khẩu cho người dùng

- Click finish



Hình 4.5 Hoàn tất tạo user

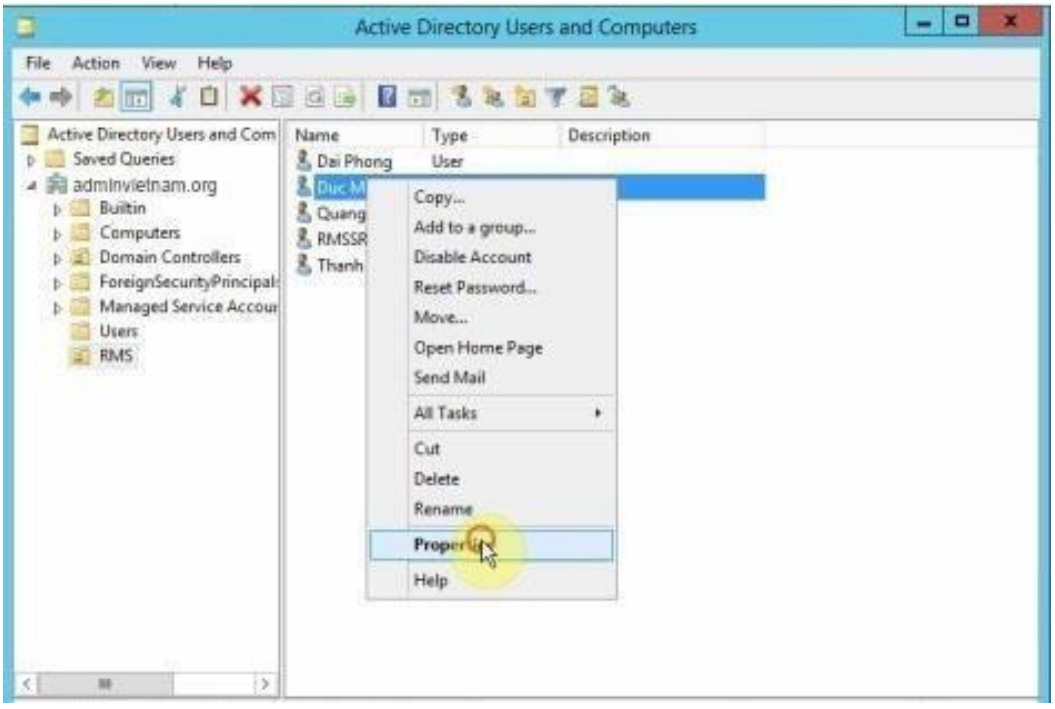
- User mới được thêm vào



Hình 4.6 Kết quả sau khi tạo user

5.2. Các thuộc tính của tài khoản người dùng

- Click phải chuột user – chọn Properties

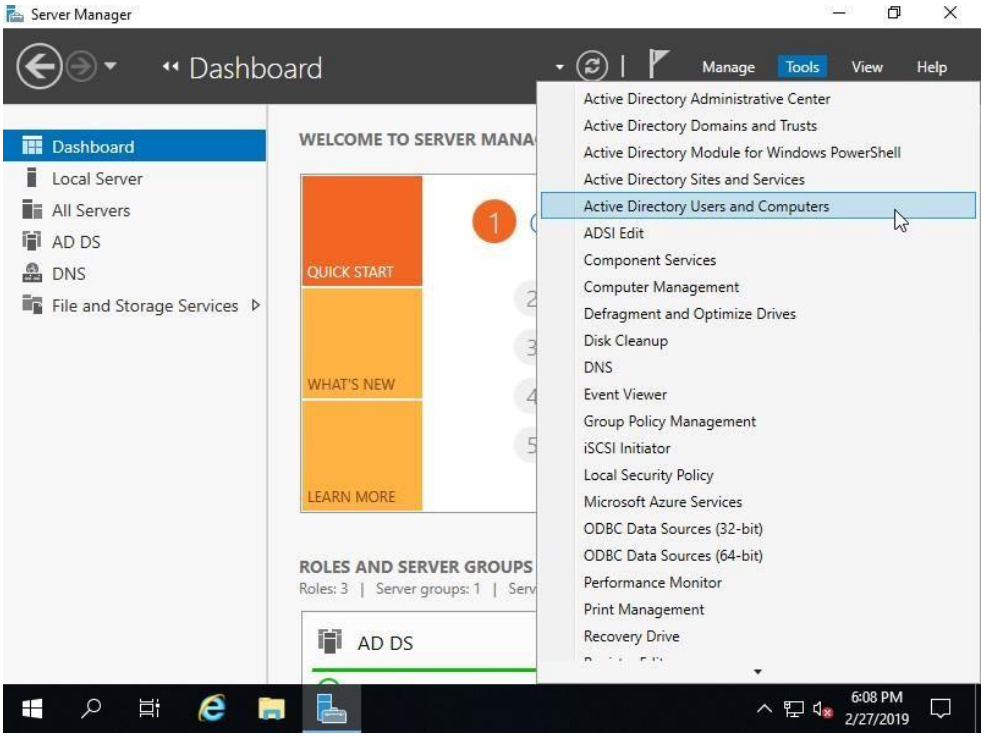


Hình 4.7 Mở thuộc tính của user

Hình 4.8 thuộc tính của user

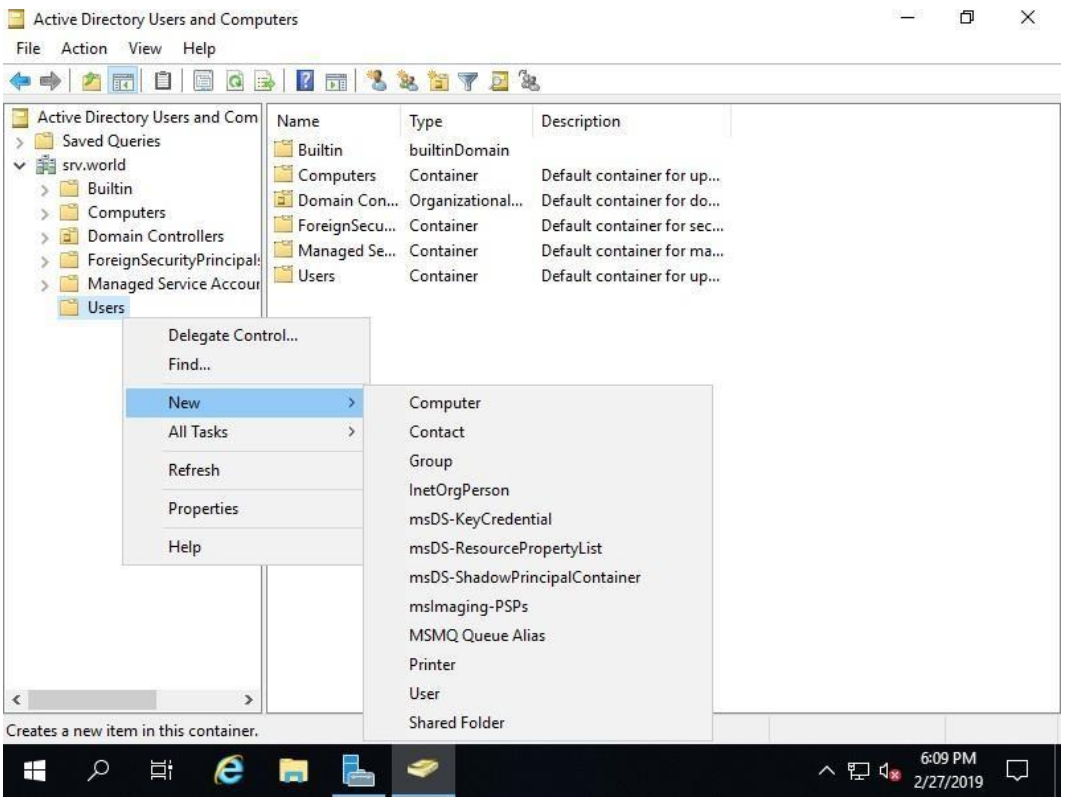
5.3. Tạo mới tài khoản nhóm

- Mở Server Manager, click Tools chọn Active Directory Users and Conputers.



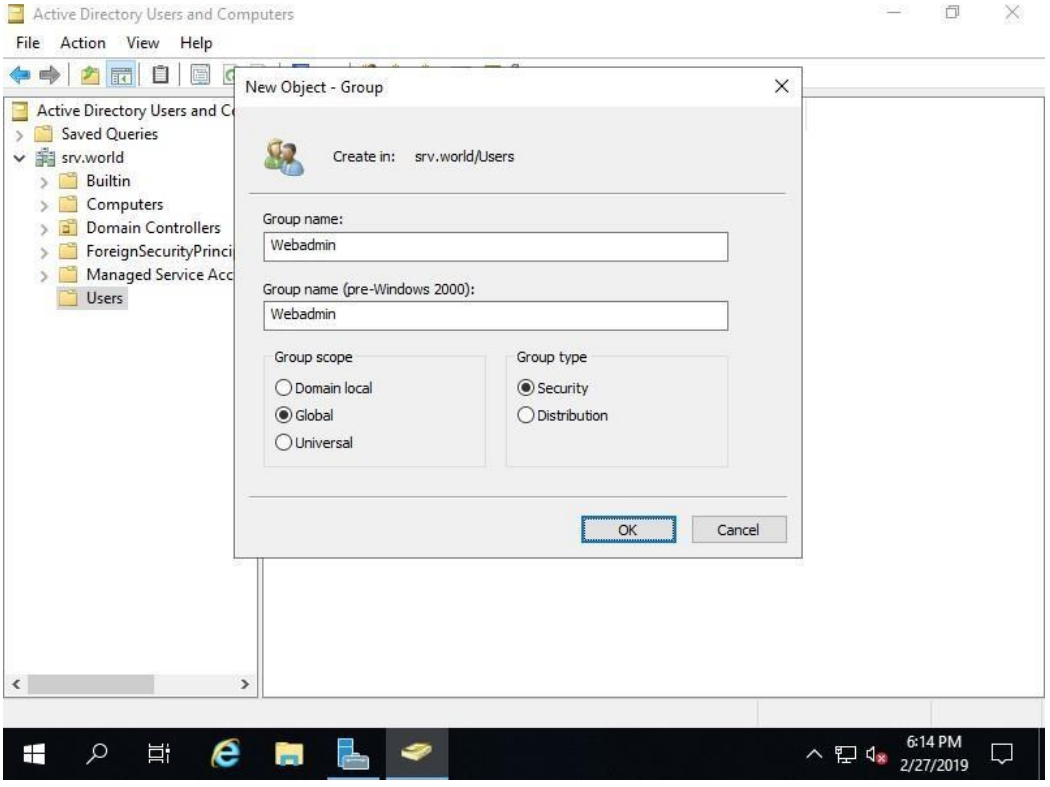
Hình 4.9 Chọn công cụ Active Directory Users and Computers để tạo nhóm

- Click chuột phải Users chọn New -> Group.



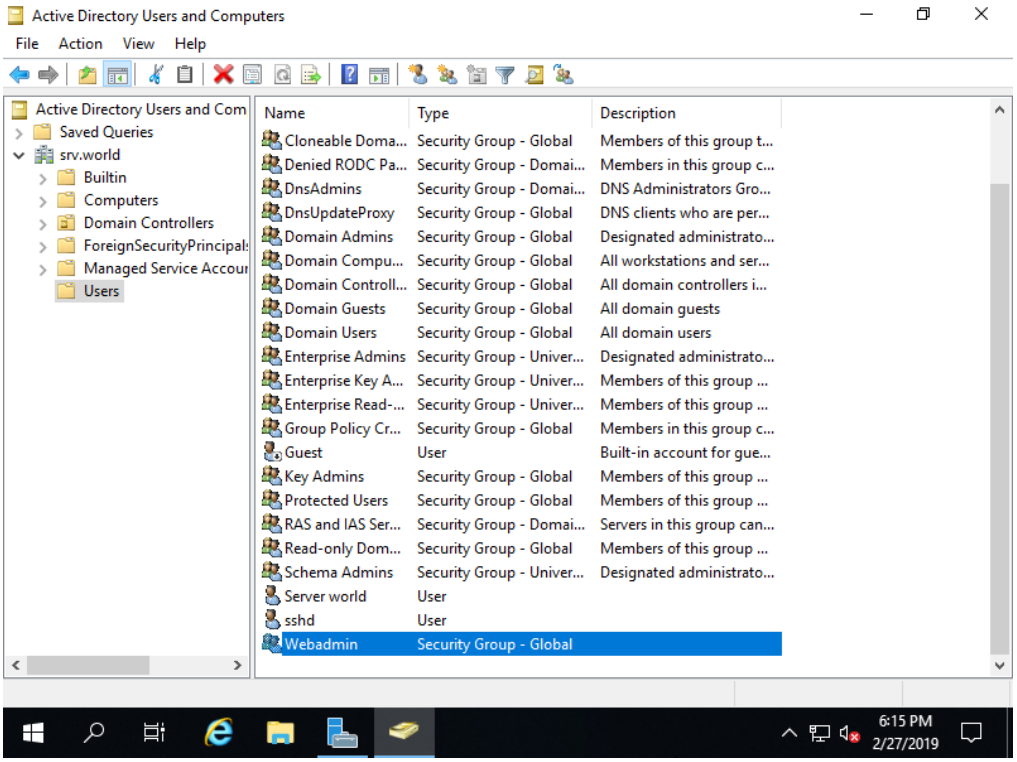
Hình 4.10 Chọn công cụ Active Directory Users and Computers để tạo nhóm

- Nhập tên nhóm, nhấn Next



Hình 4.11 Nhập tên nhóm

- Nhóm mới được thêm vào



Hình 4.12 Kết quả sau khi tạo nhóm

5.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và nhóm

Windows Server 2019 cung cấp nhiều công cụ dòng lệnh mạnh mẽ, có thể được dùng trong các tập tin xử lý theo lô (batch) hoặc các tập tin kịch bản (script) để quản lý tài khoản người dùng như thêm, xóa, sửa. Windows 2019 còn hỗ trợ việc nhập và xuất các đối tượng từ Active Directory. Hai tiện ích dsadd.exe và admod.exe với đối số user cho phép chúng ta thêm và chỉnh sửa tài khoản người dùng trong Active Directory. Tiện ích csvde.exe được dùng để nhập hoặc xuất dữ liệu đối tượng thông qua các tập tin kiểu CSV (comma-separated values). Đồng thời hệ thống mới này vẫn còn sử dụng hai lệnh net user và net group.

5.4.1. Lệnh net user

Chức năng: tạo thêm, hiệu chỉnh và hiển thị thông tin của các tài khoản người dùng . *Cú pháp:*

net user [username [password | *] [options]] [/domain]

net user username {password | *} /add [options] [/domain]

net user username [/delete] [/domain]

[**Username**]: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị.

[**Password**]: ấn định hoặc thay đổi mật mã của tài khoản người dùng.

[**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng

[**/add**]: thêm một tài khoản người dùng vào trong cơ sở dữ liệu tài khoản người dùng.

[**/delete**]: xóa một tài khoản người dùng khỏi cơ sở dữ liệu tài khoản người dùng.

5.4.2 Lệnh net group

Chức năng: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục trên Windows Server

Cú pháp:

net group [groupname [/comment:"text"]] [/domain]

net group groupname {/add [/comment:"text"] | /delete} [/domain]

net group groupname username[...] {/add | /delete} [/domain]

[**Groupname**]: chỉ định tên nhóm cần thêm, mở rộng hoặc xóa.

[**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn

[**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng.

[**username[...]**]: danh sách một hoặc nhiều người dùng cần thêm hoặc xóa ra khỏi nhóm, các tên này cách nhau bởi khoảng trắng.

[**/add**]: thêm một nhóm hoặc thêm một người dùng vào nhóm.

[**/delete**]: xóa một nhóm hoặc xóa một người dùng khỏi nhóm.

5.4.3. Các lệnh hỗ trợ dịch vụ Active Driectory trong môi trường Windows Server

- **Dsadd**: cho phép bạn thêm một **computer**, **contact**, **group**, **ou** hoặc **user** vào trong dịch vụ **Directory**.
- **Dsrm**: xóa một đối tượng trong dịch vụ **Directory**.
- **Dsmove**: di chuyển một đối tượng từ vị trí này đến vị trí khác trong dịch vụ **Directory**.
- **Dsget**: hiển thị các thông tin lựa chọn của một đối tượng **computer**,

contact, **group**, **ou**, **server** hoặc **user** trong một dịch vụ **Directory**.

- **Dsmod**: chỉnh sửa các thông tin của **computer**, **contact**, **group**, **ou** hoặc **user** trong một dịch vụ **Directory**.
- **Dsquery**: truy vấn các thành phần trong dịch vụ **Directory**.

CÂU HỎI VÀ BÀI TẬP BÀI 4

1. Trên máy Domain Controller tạo OU có tên HCM:

a. Trong OU HCM tạo 2 nhóm có tên là Ke Toan và Nhan Su.

b. Trong mỗi nhóm tạo 3 user.

c. Tìm kiếm, di chuyển và khóa một vài tài khoản người dùng bất kỳ.

d. Chỉ cho phép các user logon vào mạng từ 7:00am-6:00pm.

e. Tạo Home Folder cho các user.

f. Cho phép user chỉ lưu trữ 500MB trên Home Folder.

g. Thực hiện Account Lock-Out(cho phép user nhập sai 2 lần)

2. Tạo tài khoản người dùng và tài khoản nhóm trên miền cdcd.vn gồm:

+ Nhóm giảng viên: nhviet, cvhong, tqchau

+ Nhóm quản lý: nhduy

a. Tất cả các tài khoản người dùng trên là thành viên nhóm Backup Operators.

b. Tài khoản người dùng nhduy và nhviet phải thay đổi mật khẩu khi đăng nhập vào hệ thống lần đầu tiên

c. Người dung tqchau không được phép đổi mật khẩu từ máy trạm

d. Tạm khóa tài khoảng cvhon

e.Nhóm giảng viên được phép đăng nhập vào mạng từ 7h sáng đến 9h tối hàng ngày từ thứ 2 đến thứ 7

f. Người dung tqchau hết hạn làm việc từ ngày 22/10/2020

BÀI 5: QUẢN LÝ ĐĨA

Mã bài: MĐ 15 - 05

Giới thiệu:

Tập tin được lưu trữ trên đĩa, do đó việc quản trị đĩa là hết sức quan trọng trong việc cài đặt hệ thống tập tin

Bài này sẽ giới thiệu về các loại định dạng đĩa cứng, nén, mã hóa dữ liệu .

Mục tiêu:

- Phân biệt được các loại định dạng đĩa cứng;
- Công nghệ lưu trữ mới Dynamic storage;
- Mô tả được kỹ thuật nén và mã hoá dữ liệu.

Nội dung chính:

1. Cấu hình hệ thống tập tin

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. **Windows Server** hỗ trợ ba hệ thống tập tin khác nhau: **FAT16**, **FAT32** và **NTFS**. Nếu sử dụng các tính năng như bảo mật cục bộ, nén và mã hoá các tập tin thì bạn nên dùng **NTFS**.

2. Cấu hình đĩa lưu trữ

2.1. Basic storage

Bao gồm các partition primary và extended. Partition tạo ra đầu tiên trên đĩa được gọi là partition primary và toàn bộ không gian cấp cho partition được sử dụng trọn vẹn. Mỗi ổ đĩa vật lý có tối đa bốn partition. Có thể tạo ba partition primary và một partition extended. Với partition extended có thể tạo ra nhiều partition logical.

2.2. Dynamic Storage

Đĩa lưu trữ dynamic chia thành các volume dynamic. Volume dynamic không chứa partition hoặc ổ đĩa logic, và chỉ có thể truy cập bằng Windows Server.

Có năm loại volume dynamic: simple, spanned, striped, mirrored và RAID-5. Ưu điểm của công nghệ Dynamic storage so với công nghệ Basic storage:

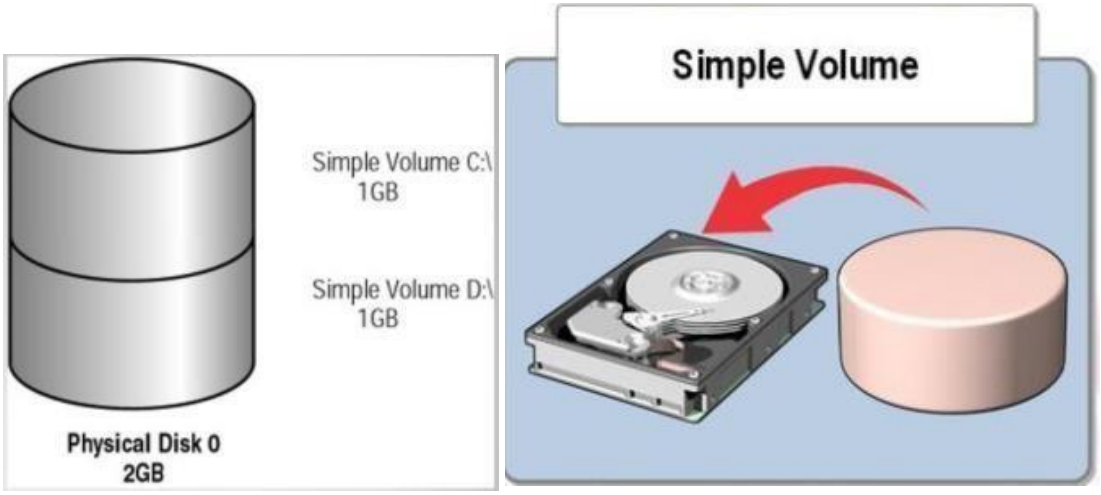
- Cho phép ghép nhiều ổ đĩa vật lý để tạo thành các ổ đĩa logic (Volume).
- Cho phép ghép nhiều vùng trống không liên tục trên nhiều đĩa cứng vật lý

để tạo ổ đĩa logic.

- Có thể tạo ra các ổ đĩa logic có khả năng dung lỗi cao và tăng tốc độ truy xuất…

2.2.1. Volume simple

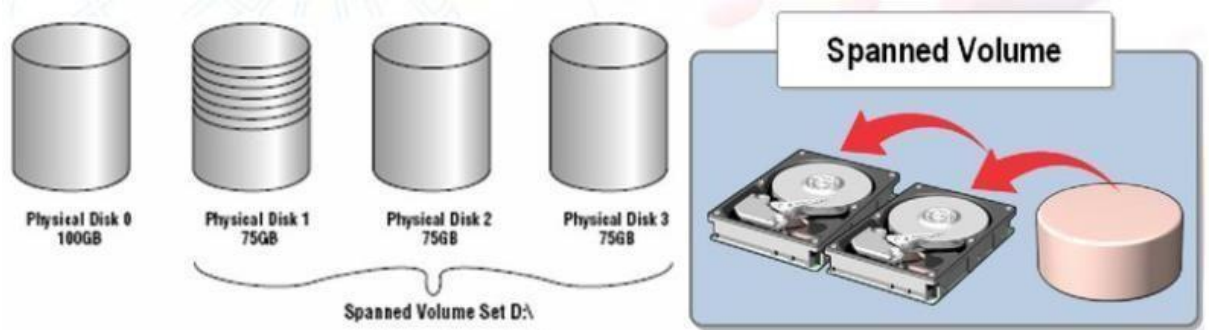
Chứa không gian lấy từ một đĩa **dynamic** duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục



Hình 5.1 Hình minh hoạ một đĩa vật lý được chia thành hai volume đơn giản.

2.2.2. Volume spanned

Bao gồm một hoặc nhiều đĩa **dynamic** (tối đa là 32 đĩa). Sử dụng khi muốn tăng kích cỡ của **volume**. Dữ liệu ghi lên **volume** theo thứ tự, hết đĩa này đến đĩa khác. Thông thường người quản trị sử dụng **volume spanned** khi ổ đĩa đang sử dụng trong **volume** sắp bị đầy và muốn tăng kích thước của **volume** bằng cách bổ sung thêm một đĩa khác.



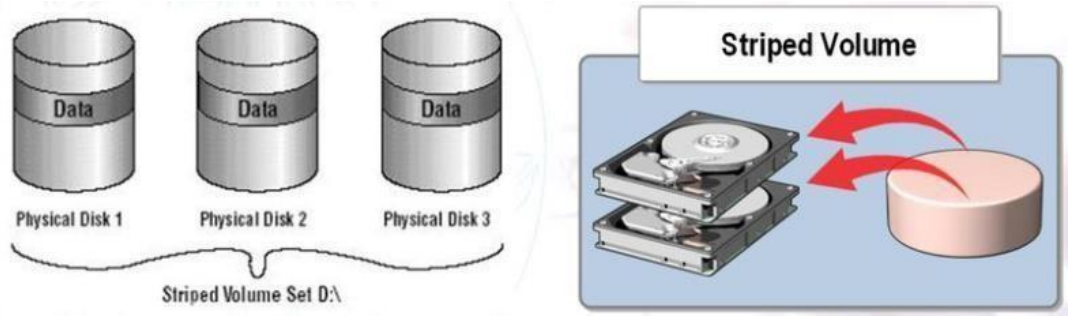
Hình 5.2 Hình minh hoạ Volume spanned

Do dữ liệu được ghi tuần tự nên **volume** loại này không tăng hiệu năng sử dụng. Nhược điểm chính của **volume spanned** là nếu một đĩa bị hỏng thì toàn

bộ dữ liệu trên **volume** không thể truy xuất được.

2.2.3. Volume striped

Lưu trữ dữ liệu lên các dãy (**strip**) bằng nhau trên một hoặc nhiều đĩa vật lý. Do dữ liệu được ghi tuần tự lên từng dãy, nên có thể thi hành nhiều tác vụ **I/O** đồng thời, làm tăng tốc độ truy xuất dữ liệu. Thông thường, người quản trị mạng sử dụng **volume striped** để kết hợp dung lượng của nhiều ổ đĩa vật lý thành một đĩa **logic** đồng thời tăng tốc độ truy xuất.

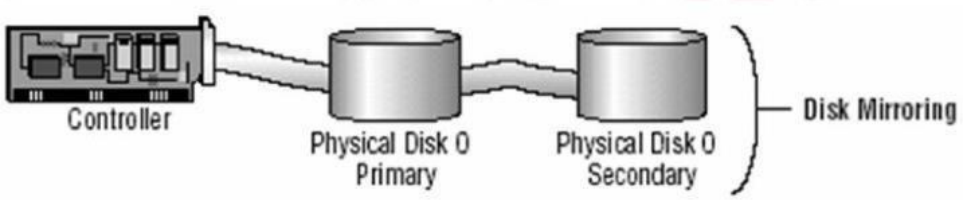


Hình 5.3 Hình minh hoạ Volume striped

Nhược điểm chính của **volume striped** là nếu một ổ đĩa bị hỏng thì dữ liệu trên toàn bộ **volume** mất giá trị.

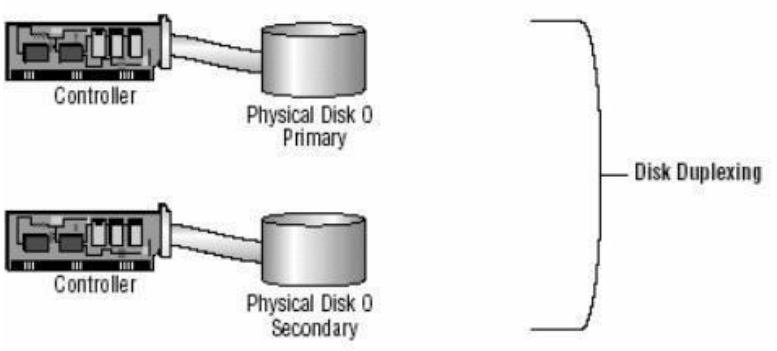
2.2.4. Volume mirrored

Là hai bản sao của một **volume** đơn giản. Dùng một ổ đĩa chính và một ổ đĩa phụ. Dữ liệu khi ghi lên đĩa chính đồng thời cũng sẽ được ghi lên đĩa phụ. **Volume** dạng này cung cấp khả năng dung lỗi tốt. Nếu một đĩa bị hỏng thì ổ đĩa kia vẫn làm việc và không làm gián đoạn quá trình truy xuất dữ liệu. Nhược điểm của phương pháp này là bộ điều khiển đĩa phải ghi lần lượt lên hai đĩa, làm giảm hiệu năng.



Hình 5.4 Hình minh hoạ Volume mirrored-Disk Miroring

Để tăng tốc độ ghi đồng thời cũng tăng khả năng dung lỗi, có thể sử dụng một biến thể của **volume mirrored** là **duplexing**. Theo cách này phải sử dụng một bộ điều khiển đĩa khác cho ổ đĩa thứ hai.

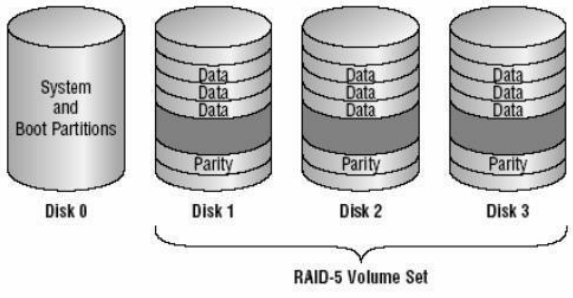


Hình 5.5 Hình minh hoạ Volume mirrored-Disk Duplexing

Nhược điểm chính của phương pháp này là chi phí cao. Để có một **volume 4GB** bạn phải tốn đến **8GB** cho hai ổ đĩa

2.2.5. Volume RAID-5

Tương tự như **volume striped** nhưng **RAID-5** lại dùng thêm một dãy (**strip**) ghi thông tin kiểm lỗi **parity**. Nếu một đĩa của **volume** bị hỏng thì thông tin **parity** ghi trên đĩa khác sẽ giúp phục hồi lại dữ liệu trên đĩa hỏng. **Volume RAID-5** sử dụng ít nhất ba ổ đĩa



Hình 5.6 Hình minh hoạ Volume RAID-5

Ưu điểm chính của kỹ thuật này là khả năng dung lỗi cao và tốc độ truy xuất cao bởi sử dụng nhiều kênh I/O.

3. Sử dụng chương trình Disk Manager

Disk Management là một tiện ích mở rộng của Microsoft Management Console cho phép quản lý toàn bộ phần cứng dựa trên ổ đĩa được Windows nhận diện.

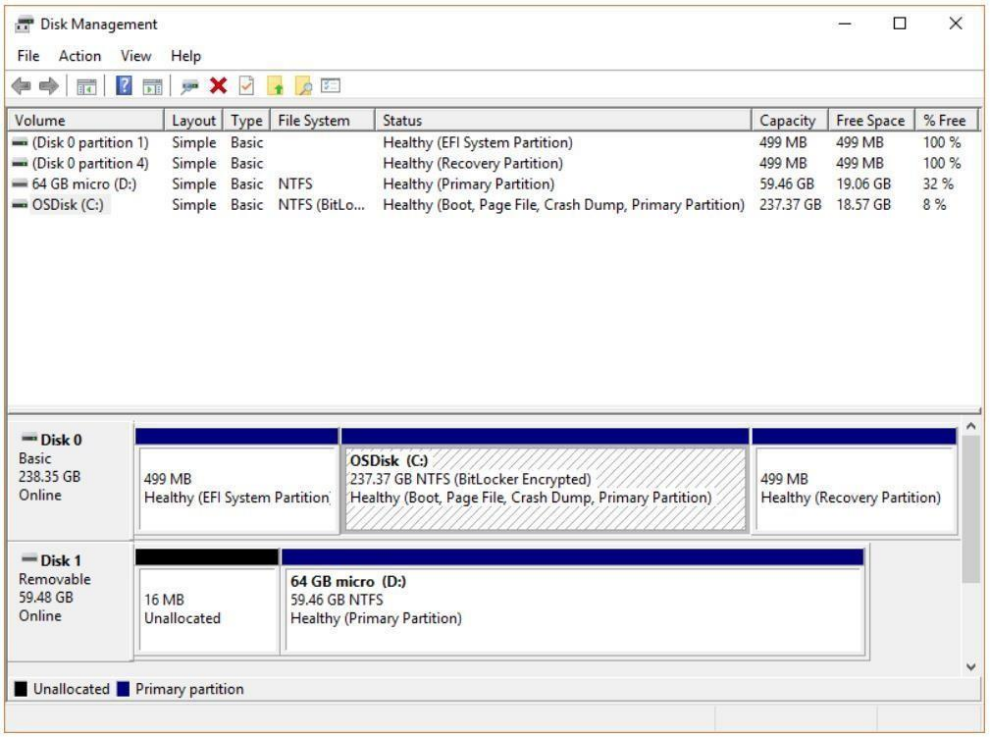
Disk Management được sử dụng để quản lý các ổ đĩa được cài đặt trong máy tính như ổ cứng (bên trong và bên ngoài), ổ đĩa quang và ổ flash. Nó có thể được sử dụng để phân vùng, định dạng, gán ký tự ổ đĩa,…

Để có thể sử dụng Disk Manager, phải đăng nhập vào máy bằng tài khoản Administrator. Mở Quản lý đĩa trong Windows Server 2019, có một số cách:

- Click chuột phải Windows biểu tượng ở phía dưới bên trái và nhấp vào Quản lý đĩa trong danh sách.

- Nhấn Windows và X cùng nhau trên bàn phím, sau đó bạn sẽ thấy Quản lý đĩa trong danh sách.

- Nhấn Windows và R trên bàn phím của bạn, gõ diskmgmt.msc và nhấn Enter



Hình 5.7 Giao diện Disk Management

3.1. Xem thuộc tính của đĩa

Nhấp phải chuột lên ổ đĩa vật lý muốn biết thông tin và chọn Properties.

Hộp thoại cung cấp các thông tin:

- Số thứ tự của ổ đĩa vật lý

- Loại đĩa (basic, dynamic, DVD-ROM, DVD, đĩa chuyển dời được, hoặc unknown)

- Trạng thái của đĩa (online hoặc offline)

- Dung lượng đĩa

- Lượng không gian chưa cấp phát

- Loại thiết bị phần cứng

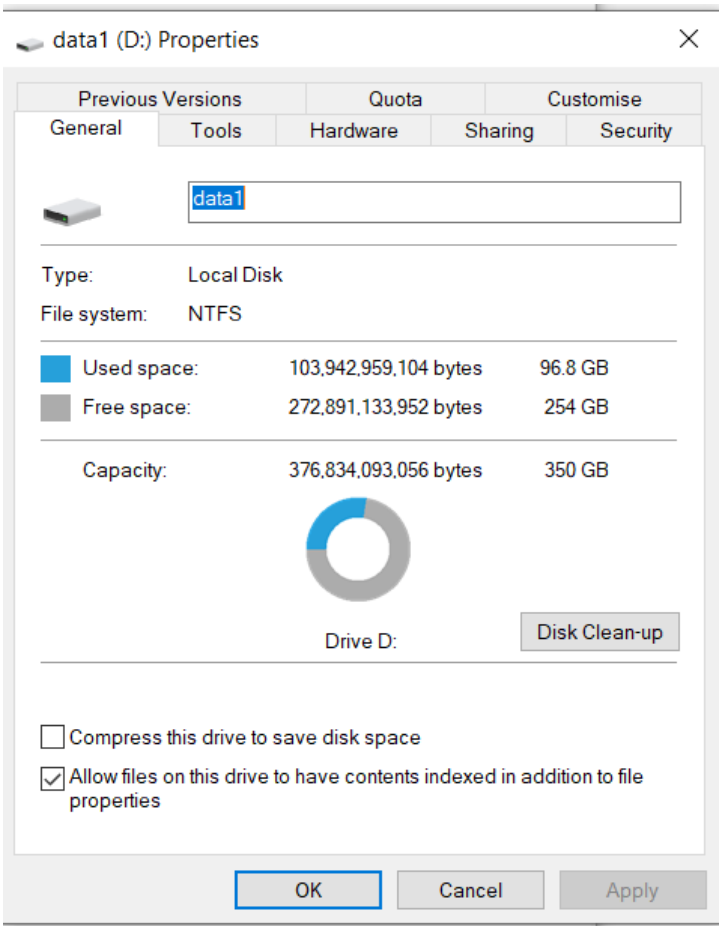
- Nhà sản xuất thiết bị

- Tên của adapter

- Danh sách các volume đã tạo trên đĩa

3.2. Xem thuộc tính của Volume hoặc đĩa cục bộ

Nhấp phải chuột lên đĩa cục bộ đó và chọn **Properties** và hộp thoại **Local Disk Properties** xuất hiện.



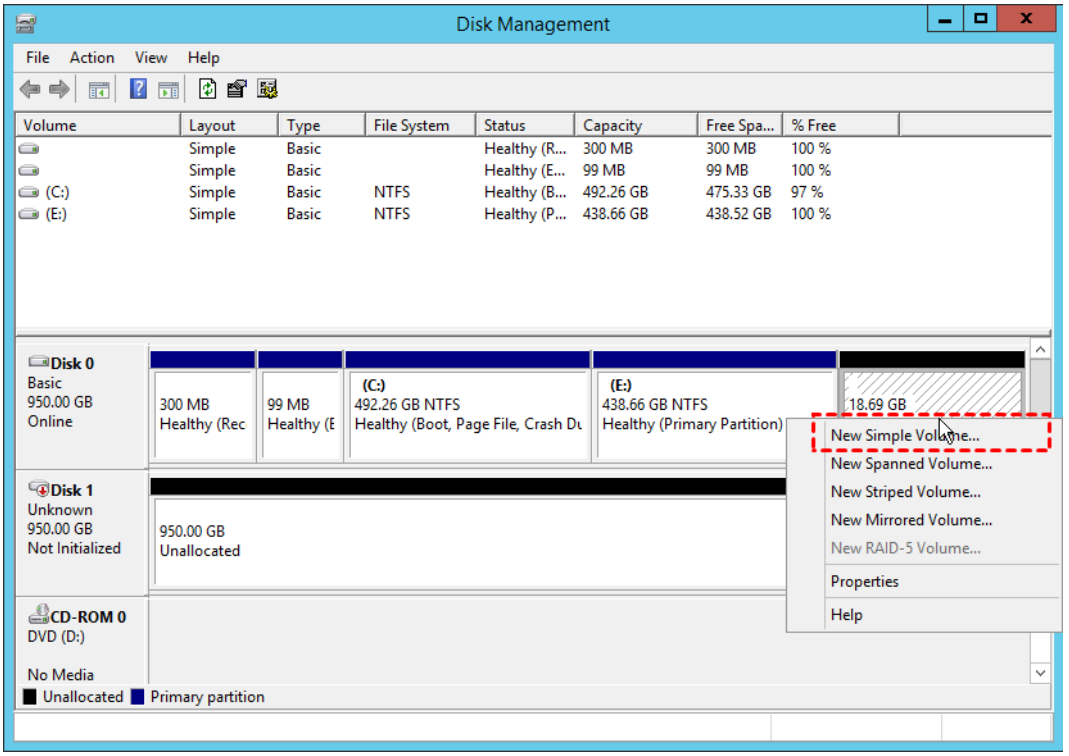
Hình 5.8 Thuộc tính của Volume hoặc đĩa cục bộ

3.3. Bổ sung thêm một ổ đĩa mới

Chỉ cần lắp thêm ổ đĩa mới vào theo hướng dẫn của nhà sản xuất mà không cần tắt máy. Rồi sau đó dùng chức năng **Action Rescan Disk** của **Disk Manager** để phát hiện ổ đĩa mới này.

3.4. Tạo partition/volume mới

- Click chuột phải vào “Unallocated space” và chọn “New Simple Volume”.

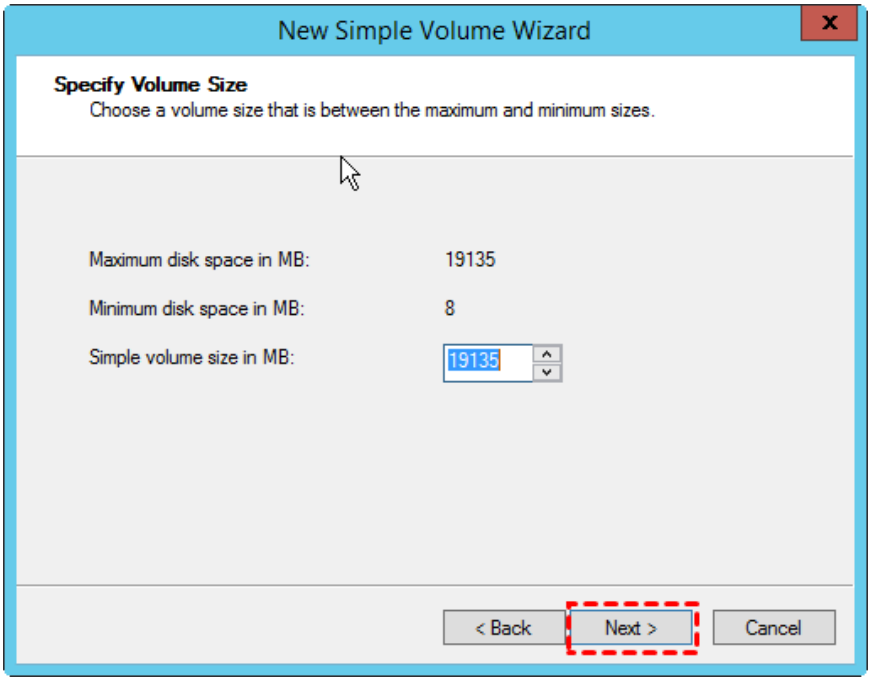


Hình 5.9 Tạo Partition mới

- Chọn Next

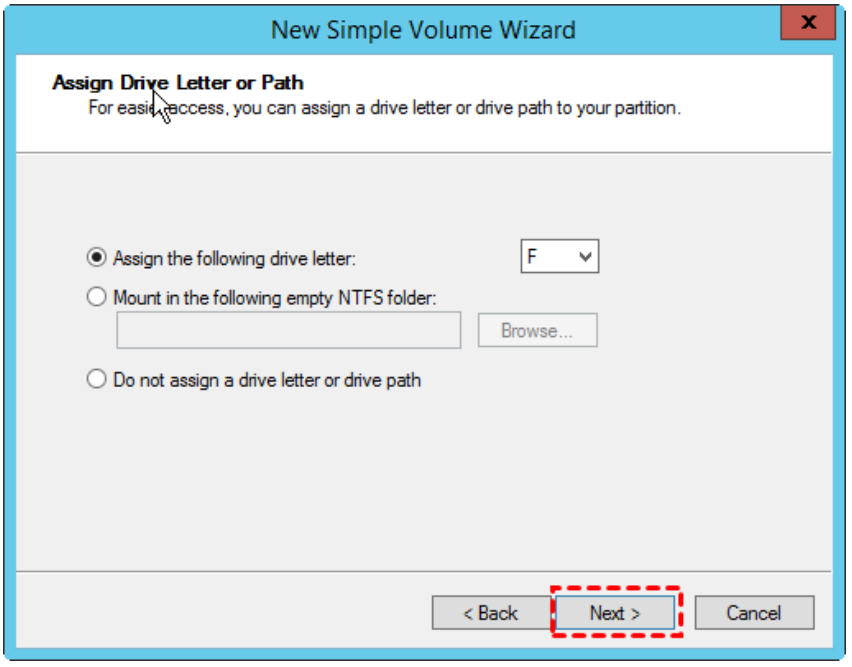
Hình 5.10 Hộp thoại New Simple Volume Winzard

- Nhập dung lượng cần cấp phát, chọn Next



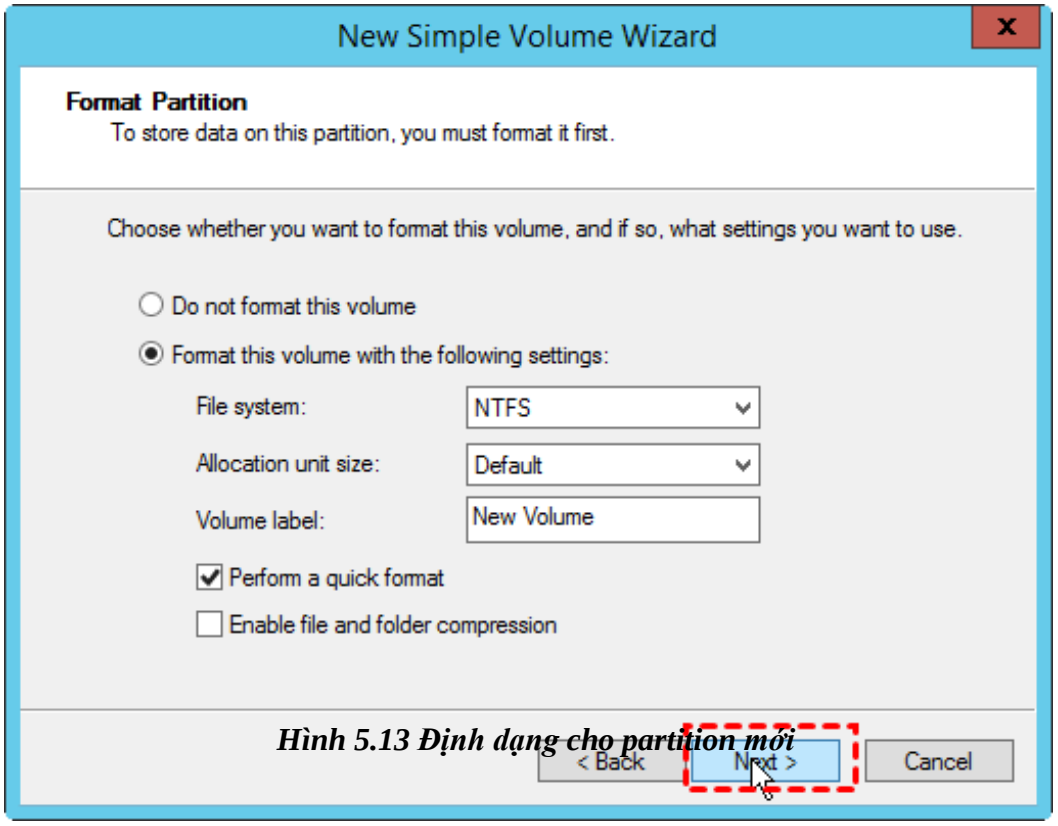
Hình 5.11 Nhập dung lượng cần cấp phát

- Đặt tên cho partition, Next



Hình 5.12 Đặt tên cho partition

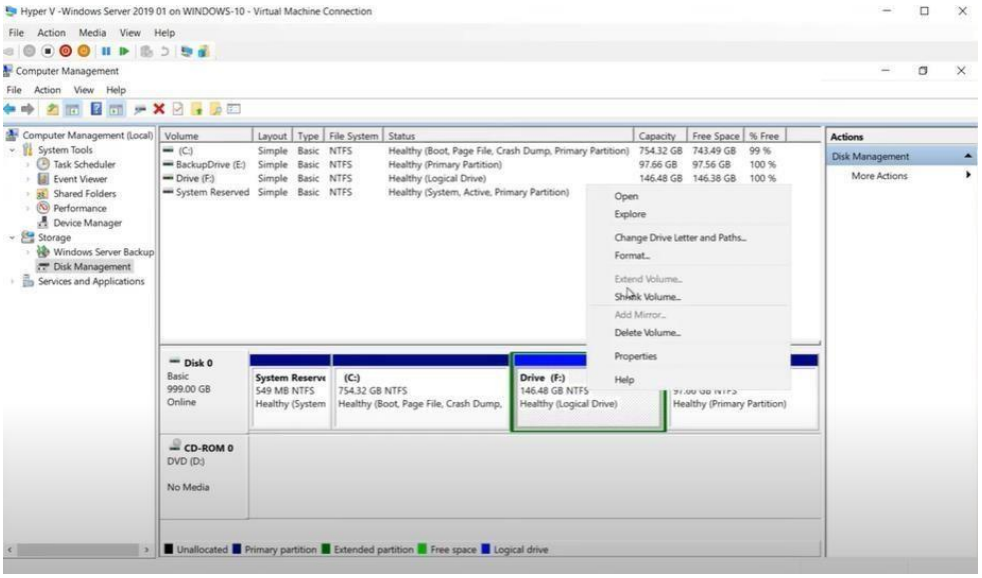
- Định dạng partition mới: exFAT, NTFS, FAT32, Click Next->Finish



Hình 5.13 Định dạng cho partition mới

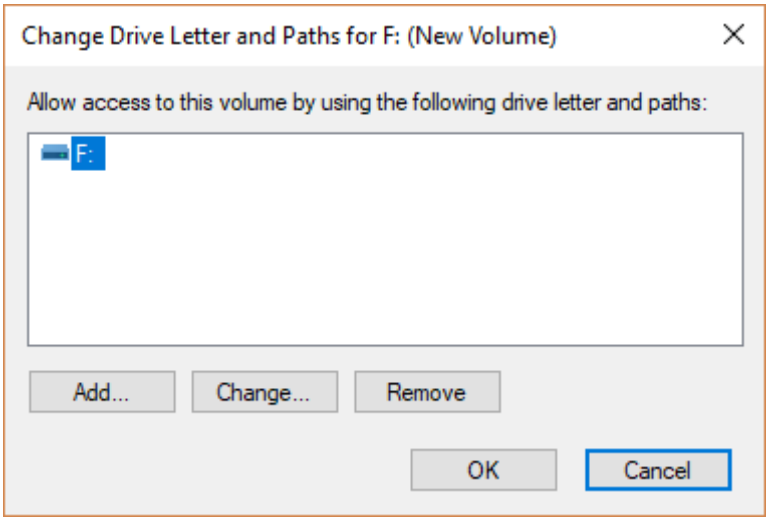
3.5. Thay đổi ký tự ổ đĩa hoặc đường dẫn

Muốn thay đổi ký tự ổ đĩa cho **partition/volume** nào, bạn nhấp phải chuột lên **volume** đó và chọn **Change Drive Letter and Path**. Hộp thoại **Change Drive Letter and Path** xuất hiện.



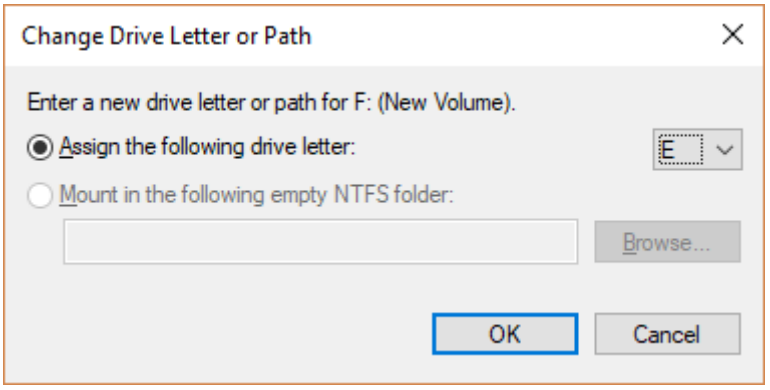
Hình 5.14 Thay đổi ký tự ổ đĩa hoặc đường dẫn

- Chọn Change -> Add



Hình 5.15 Hộp thoại Change Drive Letter and Paths

- Mở danh sách Assign a drive letter và chọn một ký tự ổ đĩa mới định đặt cho partition/volume, Click Ok



Hình 5.15 Hộp thoại Change Drive Letter and Paths

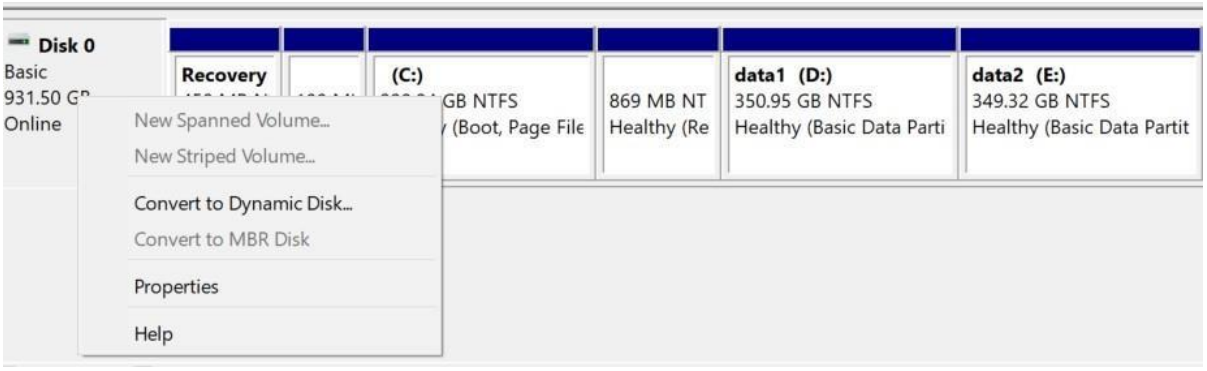
- Trong hộp thoại này, nhấn nút **Edit** để mở tiếp hộp thoại **Edit Drive Letter and Path**, mở danh sách **Assign a drive letter** và chọn một ký tự ổ đĩa mới định đặt cho **partition/volume** này. Cuối cùng đồng ý xác nhận các thay đổi đã thực hiện.

3.6. Xoá partition/volume

Để tổ chức lại một ổ đĩa hoặc huỷ các dữ liệu có trên một **partition/volume** có thể xoá nó đi. Để thực hiện, trong cửa sổ **Disk Manager**, nhấp phải chuột lên **partition/volume** muốn xoá và chọn **Delete Partition** (hoặc **Delete Volume**). Một hộp thoại cảnh báo xuất hiện, thông báo dữ liệu trên **partition** hoặc **volume** sẽ bị xoá và yêu cầu xác nhận lại lần nữa thao tác này.

3.7. Cấu hình Dynamic Storage

Để sử dụng được cơ chế lưu trữ **Dynamic**, bạn phải chuyển đổi các đĩa cứng vật lý trong hệ thống thành **Dynamic Disk**. Trong công cụ **Computer Management \ Disk Management**, bạn nhấp phải chuột trên các ổ đĩa bên của sổ bên phải và chọn **Convert to Dynamic Disk….** Sau đó đánh dấu vào tất cả các đĩa cứng vật lý cần chuyển đổi chế độ lưu trữ và chọn **OK** để hệ thống chuyển đổi. Sau khi chuyển đổi xong hệ thống sẽ yêu cầu bạn **restart** máy để áp dụng chế độ lưu trữ mới.



Hình 5.16 Chuyển đĩa cứng vật lý thành Dynamic Disk

Trong công cụ **Disk Management**, nhấp phải chuột lên vùng trống của đĩa cứng cần tạo **Volume**, sau đó chọn **New Volume.**

Tiếp theo, chọn loại **Volume** cần tạo. Trong trường hợp này chúng ta chọn **Spanned**.

Chọn những ổ đĩa dùng để tạo **Volume** này, đồng thời cũng nhập kích thước mà mỗi đĩa giành ra để tạo **Volume**. Chú ý đối với loại **Volume** này thì kích thước của các đĩa giành cho **Volume** có thể khác nhau

Gán ký tự ổ đĩa cho **Volume**

Định dạng **Volume** mà vừa tạo để có thể chứa dữ liệu.

Đến đây đã hoàn thành việc tạo **Volume**

Tạo Volume Striped

Các bước tạo **Volume Striped** cũng tương tự như việc tạo các **Volume** khác nhưng chú ý là kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng tổng các kích thước của các phần trên.

Tạo Volume Mirror.

Các bước tạo **Volume Mirror** cũng tương tự như trên, chú ý kích thước

của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng chính kích thước của mỗi phần trên.

Tạo Volume Raid-5.

Các bước tạo **Volume Raid-5** cũng tương tự như trên nhưng chú ý là loại **Volume** yêu cầu tối thiểu đến 3 đĩa cứng. Kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng 2/3 kích thước của mỗi phần cộng lại.

4. Quản lý việc nén dữ liệu

Nén dữ liệu là quá trình lưu trữ dữ liệu dưới một dạng thức chiếm ít không gian hơn dữ liệu ban đầu. **Windows Server** hỗ trợ tính năng nén các tập tin và thư mục một cách tự động và trong suốt. Các chương trình ứng dụng truy xuất các tập tin nén một cách bình thường do hệ điều hành tự động giải nén khi mở tập tin và nén lại khi lưu tập tin lên đĩa. Khả năng này chỉ có trên các **partition NTFS**. Nếu chép một tập tin/thư mục trên một **partition** có tính năng nén sang một partition **FAT** bình thường thì hệ điều hành sẽ giải nén tập tin/ thư mục đó trước khi chép đi.

Để thi hành việc nén một tập tin/thư mục, sử dụng chương trình **Windows Explorer** và thực hiện theo các bước sau:

- Trong cửa sổ **Windows Explorer**, duyệt đến tập tin/thư mục định nén và chọn tập tin/thư mục đó.

- Nhấp phải chuột lên đối tượng đó và chọn **Properties**.

- Trong hộp thoại **Properties**, nhấn nút **Advanced** trong **tab General**.

- Trong hộp thoại **Advanced Properties**, chọn mục "**Compress contents to save disk space**" và nhấn chọn **OK**.

Nhấn chọn **OK** trong hộp thoại **Properties** để xác nhận thao tác. Nếu định nén một thư mục, hộp thoại **Confirm Attribute Changes** xuất hiện, yêu cầu lựa chọn hoặc là chỉ nén thư mục này thôi (**Apply changes to this folder only**) hoặc nén cả các thư mục con và tập tin có trong thư mục (**Apply changes to this folder, subfolders and files**). Thực hiện lựa chọn và nhấn **OK**.

Để thực hiện việc giải nén một thư mục/tập tin, thực hiện tương tự theo các bước ở trên và bỏ chọn mục **Compress contents to save disk space** trong hộp thoại **Advanced Properties**.

5. Thiết lập hạn ngạch đĩa (DISK QUOTA)

Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một **volume NTFS**. Bạn có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Một số vấn đề bạn phải lưu ý khi thiết lập hạn ngạch đĩa:

- Chỉ có thể áp dụng trên các volume **NTFS**.

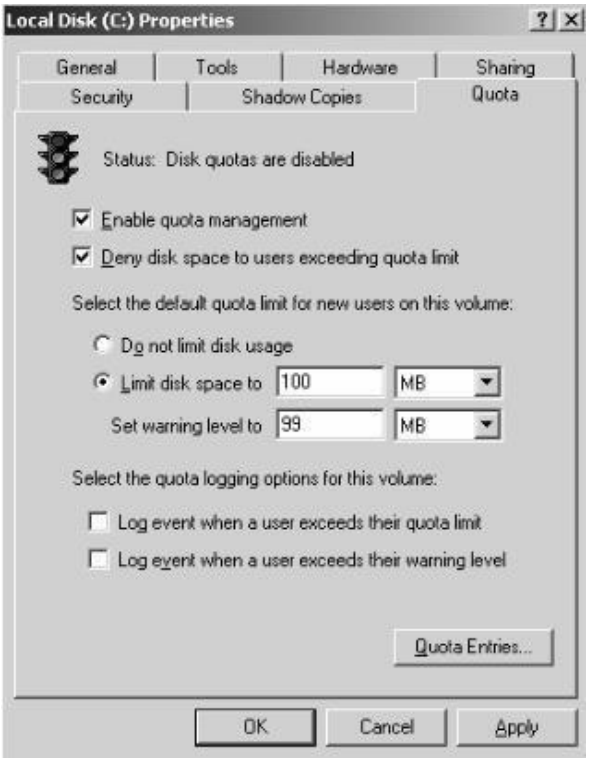
- Lượng không gian chiếm dụng được tính theo các tập tin và thư mục do người dùng sở hữu.

- Khi người dùng cài đặt một chương trình, lượng không gian đĩa còn trống mà chương trình thấy được tính toán dựa vào hạn ngạch đĩa của người dùng, không phải là lượng không gian còn trống trên **volume**.

- Được tính toán trên kích thước thật sự của tập tin trong trường hợp tập tin/thư mục được nén.

5.1. Cấu hình hạn ngạch đĩa

Để cấu hình hạn ngạch đĩa sử dụng hộp thoại **Volume Propertise** đã giới thiệu trong phần trên. Mở hộp thoại này bằng cách nhấp phải chuột lên ký tự ổ đĩa trong **Windows Explorer** và chọn **Propertise**. Trong hộp thoại này nhấp chọn **tab Quota**. Theo mặc định tính năng hạn ngạch đĩa không được kích hoạt.



Hình 5.17 Cấu hình hạn ngạch đĩa

Các mục trong hộp thoại có ý nghĩa như sau:

- **Enable quota management**: thực hiện hoặc không thực hiện quản lý hạn ngạch đĩa.

-**Deny disk space to users exceeding quota limit**: người dùng sẽ không thể tiếp tục sử dụng đĩa khi vượt quá hạn ngạch và nhận được thông báo **out of disk space.**

- **Select the default quota limit for new users on this volume**: định nghĩa các giới hạn sử dụng. Các lựa chọn bao gồm "không định nghĩa giới hạn" (**Do not limit disk space**), "giới hạn cho phép" (**Limit disk space to**) và "giới hạn cảnh báo" (**Set warning level to**).

-**Select the quota logging options for this volume**: có ghi nhận lại các sự kiện liên quan đến sử dụng hạn ngạch đĩa. Có thể ghi nhận khi người dùng vượt quá giới hạn cho phép hoặc vượt quá giới hạn cảnh báo.

Biểu tượng đèn giao thông trong hộp thoại có các trạng thái sau:

- Đèn đỏ cho biết tính năng quản lý hạn ngạch không được kích hoạt.

- Đèn vàng cho biết **Windows Server** đang xây dựng lại thông tin hạn ngạch.

- Đèn xanh cho biết tính năng quản lý đang có tác dụng.

5.2. Thiết lập hạn ngạch mặc định

Khi thiết lập hạn ngạch mặc định áp dụng cho các người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin/thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu dự định áp đặt hạn ngạch cho tất cả các người dùng, phải chỉ định hạn ngạch ngay từ khi tạo lập **volume**.

Để thực hiện, mở hộp thoại **Volume Properties** và chọn tab **Quota**. Đánh dấu chọn mục **Enable quota management** và điền vào các giá trị giới hạn sử dụng và giới hạn cảnh báo.

5.3. Chỉ định hạn ngạch cho từng cá nhân

Trong một vài trường hợp, cần phải chỉ định hạn ngạch cho riêng một người nào đó, chẳng hạn có thể là các lý do sau:

Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ

phải có được lượng không gian đĩa trống lớn.

Hoặc là người dùng đã tạo nhiều tập tin trên **volume** trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Phải tạo riêng một giới hạn mới áp dụng cho người đó.

Để thiết lập, nhấn nút **Quota Entries** trong tab **Quota** của hộp thoại **Volume Properties**. Cửa sổ **Quota Entries** xuất hiện.

Chỉnh sửa thông tin hạn ngạch của một người dùng: nhấn đúp vào mục của người dùng tương ứng, hộp thoại **Quota Setting** xuất hiện cho phép thay đổi các giá trị hạn ngạch.

Bổ sung thêm một mục quy định hạn ngạch: trong cửa sổ **Quota Entries**, vào menu **Quota** chọn mục **New Quota Entry** / xuất hiện hộp thoại **Select Users**, chọn người dùng rồi nhấn **OK** / xuất hiện hộp thoại **Add New Quota Entry**, bạn nhập các giá trị hạn ngạch thích hợp và nhấn **OK**.

6. Mã hoá dữ liệu bằng EFS

EFS (Encrypting File System) là một kỹ thuật dùng dùng để mã hoá các tập tin lưu trên các **partition NTFS**. Việc mã hoá sẽ bổ sung thêm một lớp bảo vệ an toàn cho hệ thống tập tin. Chỉ người dùng có đúng khoá mới có thể truy xuất được các tập tin này còn những người khác thì bị từ chối truy cập. Ngoài ra, người quản trị mạng còn có thể dùng tác nhân phục hồi (**recovery agent**) để truy xuất đến bất kỳ tập tin nào bị mã hoá. Để mã hoá các tập tin, tiến hành theo các bước sau:

Mở cửa sổ **Windows Explorer**. Trong cửa sổ **Windows Explorer**, chọn các tập tin và thưc mục cần mã hoá. Nhấp phải chuột lên các tập tin và thư mục, chọn **Properties**.

Trong hộp thoại **Properties**, nhấn nút **Advanced**.

Hộp thoại **Advanced Properties** xuất hiện, đánh dấu mục **Encrypt contents to secure data** và nhấn OK.

Trở lại hộp thoại **Properties**, nhấn **OK**, xuất hiện hộp thoại **Confirm Attribute Changes** yêu cần cho biết sẽ mã hoá chỉ riêng thư mục được chọn (**Apply changes to this folder only**) hoặc mã hoá toàn bộ thư mục kể các các thư mục con (**Apply changes to this folder, subfolders and files**). Sau đó nhấn **OK**.

Để thôi không mã hoá các tập tin, bạn thực hiện tương tự theo các bước trên nhưng bỏ chọn mục **Encrypt contents to secure data**.

CÂU HỎI VÀ BÀI TẬP BÀI 5

Giả thiết rằng máy Server của có 1 ổ cứng 7GB Disk 0 và 3 ổ 800MB Disk 1,2,3.

a. Hãy phân chia và tạo các volume theo yêu cầu sau:

- Volume OS dùng để cài đặt hệ điều hành, chiếm 7GB của Disk0

- Volume Software dùng để chứa phần mềm, volume này dạng Mirror gồm 400MB của Disk1 và 400MB của Disk2.

- Volume Data dạng Raid-5 gồm 400MB của 3 đĩa Disk1, Disk2 và Disk3.

b. Giả sử Disk 3 bị hư, và đã thay thể đĩa cứng mới. Hãy đồng bộ lại dữ liệu cho đĩa cứng vừa lắp vào.

c. Với hệ thống mạng như trong câu a, muốn tạo một tài nguyên chia sẻ để mọi người có thể gởi báo cáo công việc hằng tuần. Tuy nhiên, mọi người chỉ có thể để dữ liệu trên tài nguyên đó tối đa là 10MB, riêng giám đốc thì không giới hạn.

Hãy cấu hình hệ thống nhằm đáp ứng yêu cầu trên.

d. Do nhu cầu công việc, Giám đốc muốn chỉ có mình mới có thể đọc được một số nội dung chứa trong máy, dù có tháo đĩa cứng này sang máy khác thì vẫn không đọc được nội dung của này.

Hãy hướng dẫn cho Giám đốc thực hiện công việc này.

BÀI 6: TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG

Mã bài: MĐ 15 - 06

Giới thiệu:

Bài 6 cung cấp học viên kiến thức về các loại quyền: Truy cập, tạo và quản lý các thư mục dùng chung trên mạng, NTFS, DFS .

Mục tiêu:

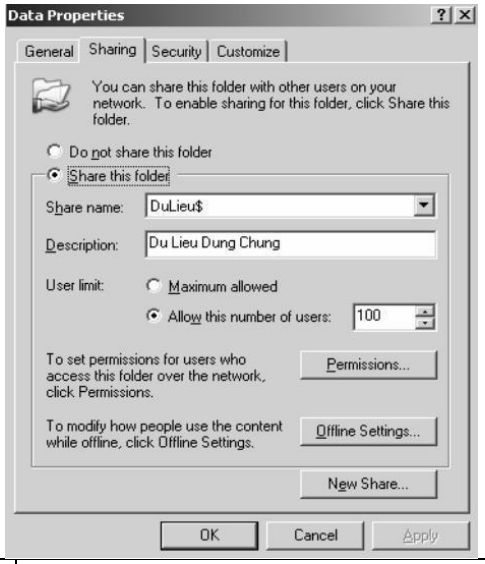
- Trình bày các loại quyền truy cập dữ liệu**;**
- Tạo và quản lý các thư mục dùng chung trên mạng.

Nội dung chính:

1. Tạo các thư mục dùng chung

1.1. Chia sẻ thư mục dung chung

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, phải **logon** vào hệ thống với vai trò người quản trị (**Administrators**) hoặc là thành viên của nhóm **Server Operators**, tiếp theo trong **Explorer** nhấp phải chuột trên thư mục đó và chọn **Properties**, hộp thoại **Properties** xuất hiện, chọn **Tab Sharing**.



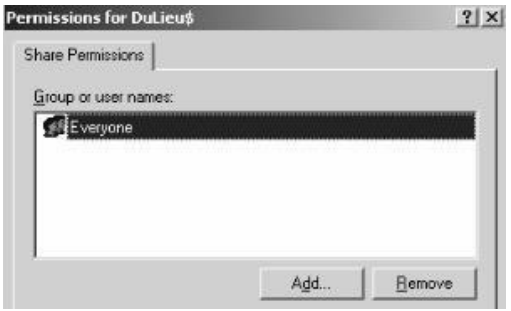
Mục	Ý nghĩa
Do not share this	Chỉ định thư mục này chỉ được phép truy cập cục

folder	bộ
Share this folder	Chỉ định thư mục này được phép truy cập cục bộ và truy cập qua mạng
Share name	Tên thư mục mà người dùng mạng nhìn thấy và truy cập
Comment	Cho phép người dùng mô tả thêm thông tin về thư mục dùng chung này
User Limit	Cho phép bạn khai báo số kết nối tối đa truy xuất vào thư mục tại một thời điểm
Permissions	Cho phép bạn thiết lập danh sách quyền truy cập thông qua mạng của người dùng
Offline Settings	Cho phép thư mục được lưu trữ tạm tài liệu khi làm việc dưới chế độ **Offline**.

Bảng 6.1 Ý nghĩa của các mục trong Tab Sharing

1.2. Cấu hình Share Permissions

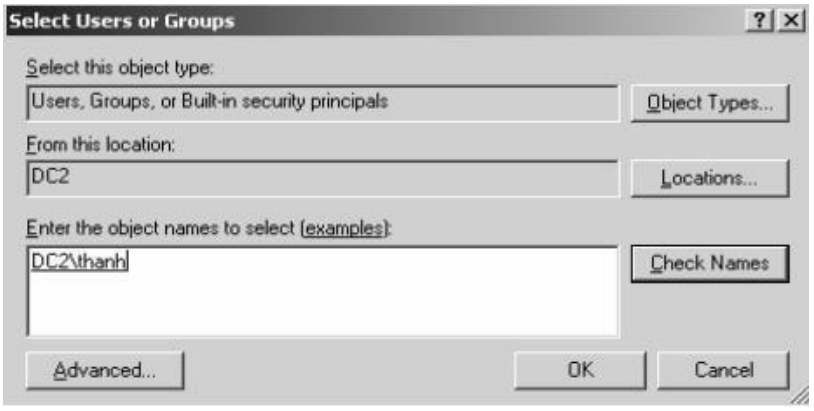
Muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng **Share Permissions**. **Share Permissions** chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với **NTFS Permissions** là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa.



Trong hộp thoại **Share Permissions**, chứa danh sách các quyền sau:

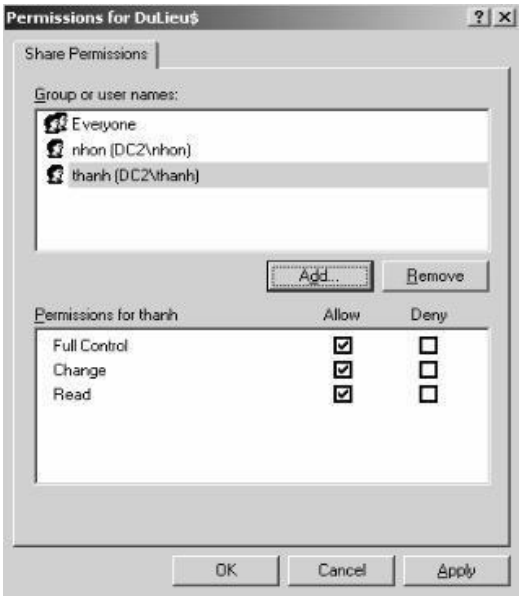
- **Full Control**: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- **Change**: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.
- **Read**: cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ. Bạn muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Add**.

Hộp thoại chọn người dùng và nhóm xuất hiện, bạn nhấp đôi chuột vào các tài khoản người dùng và nhóm cần chọn, sau đó chọn **OK**.



Hình 6.3 Hộp thoại chọn người dùng và nhóm

Trong hộp thoại xuất hiện, muốn cấp quyền cho người dùng bạn đánh dấu vào mục **Allow**, ngược lại khóa quyền thì đánh dấu vào mục **Deny**.



Hình 6.4 Chọn người dung để cấp quyền

1.3. Chia sẻ thư mục dùng lệnh netshare

Chức năng: tạo, xóa và hiển thị các tài nguyên chia sẻ. Cú pháp:

net share sharename

net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users:number | unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

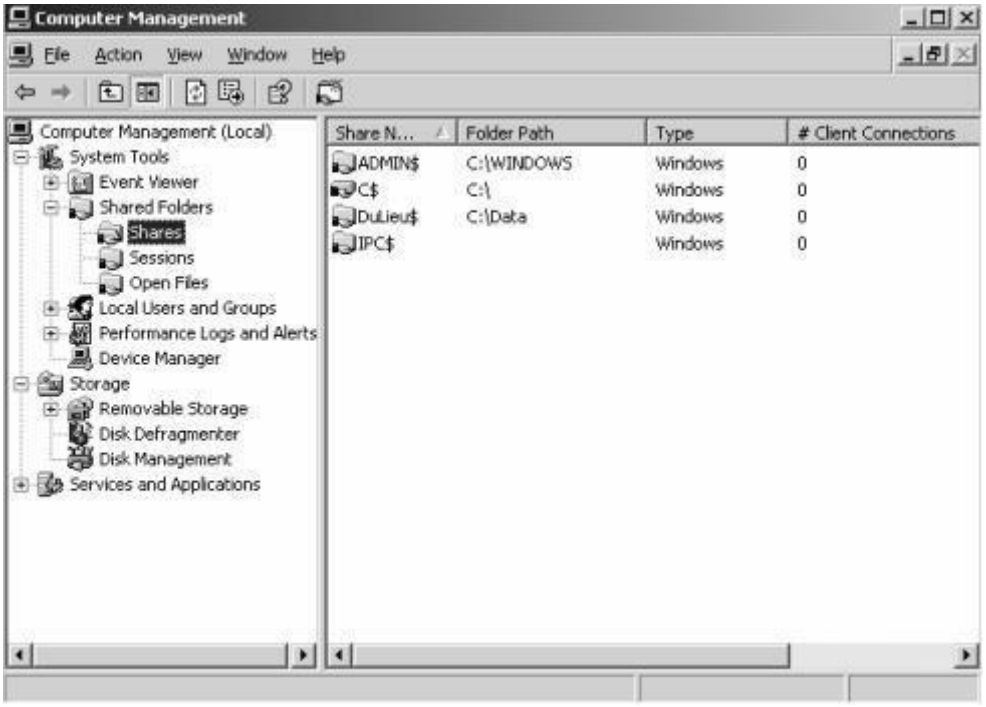
Ý nghĩa các tham số:

- [Không tham số]: hiển thị thông tin về tất cả các tài nguyên chia sẻ trên máy tính cục bộ
- [**Sharename**]: tên trên mạng của tài nguyên chia sẻ, nếu dùng lệnh **net share** với một tham số **sharename** thì hệ thống sẽ hiển thị thông tin về tài nguyên dùng chung này.
- [**drive:path**]: chỉ định đường dẫn tuyệt đối của thư mục cần chia sẻ.
- [**/users:number**]: đặt số lượng người dùng lớn nhất có thể truy cập vào tài nguyên dùng chung này.
- [**/unlimited**]: không giới hạn số lượng người dùng có thể truy cập vào tài nguyên dùng chung này.
- [**/remark:"text"**]: thêm thông tin mô tả về tài nguyên này.
- **/delete**: xóa thuộc tính chia sẻ của thư mục hiện tại.

2. Quản lý các thư mục dùng chung

2.1. Xem các thư mục dùng chung

Mục **Shared Folders** trong công cụ **Computer Management** cho phép bạn tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục **Shares**. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (**share name**) là dấu **$** thì tên thư mục dùng chung này được ẩn đi và không tìm thấy khi bạn tìm kiếm thông qua **My Network Places** hoặc duyệt các tài nguyên mạng.

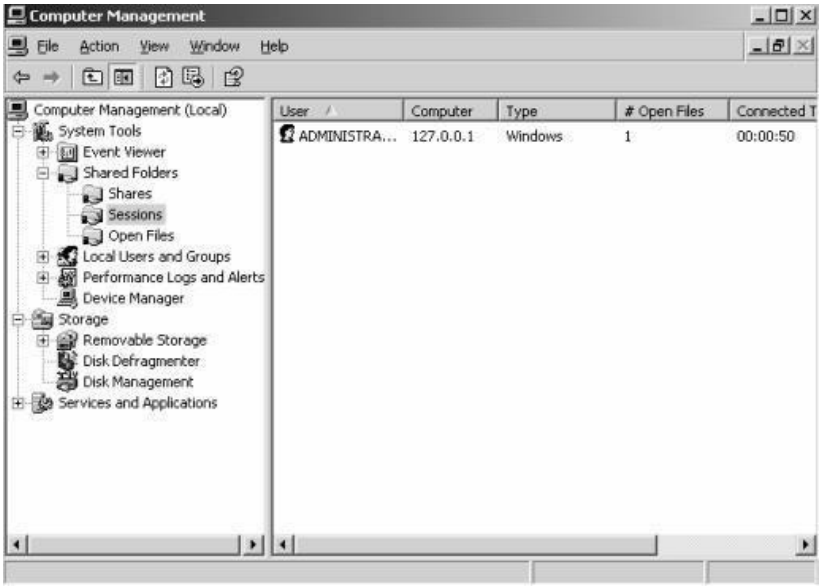


Hình 6.4 Xem thư mục dùng chung

2.2. Xem các phiên làm việc trên thư mục dùng chung

Muốn xem tất cả các người dùng đang truy cập đến các thư mục dùng chung trên máy tính chọn mục **Session**. Mục **Session** cung cấp các thông tin sau:

- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tập tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.



Hình 6.5 Xem phiên làm việc trên thư mục dùng chung

2.3. Xem các tập tin đang mở trong các thư mục dùng chung

Muốn xem các tập đang mở trong các thư mục dùng chung nhấp chuột vào mục **Open Files**. Mục **Open Files** cung cấp các thông tin sau:

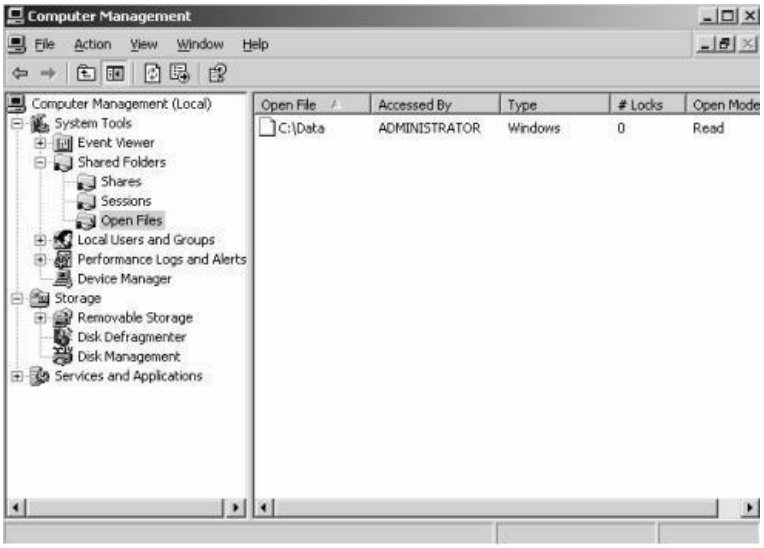
- Đường dẫn và tập tin hiện đang được mở.

- Tên tài khoản người dùng đang truy cập tập tin đó.

- Hệ điều hành mà người dùng sử dụng để truy cập tập tin.

- Trạng thái tập tin có đang bị khoá hay không.

- Trạng thái mở sử dụng tập tin (**Read** hoặc **Write**).



Hình 6.6 Xem tập tin đang mở trong thư mục dùng chung

3. Quyền truy cập NTFS

3.1. Các quyền truy cập của NTFS

Tên quyền	Chức năng
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
List Folder/Read Data	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Read Attributes	Đọc các thuộc tính của các tập tin và thư mục
Read Extended Attributes	Đọc các thuộc tính mở rộng của các tập tin và thư mục
Create File/Write Data	Tạo các tập tin mới và ghi dữ liệu lên các tập tin này
Create Folder/Append Data	Tạo thư mục mới và chèn thêm dữ liệu vào các tập tin
Write Attributes	Thay đổi thuộc tính của các tập tin và thư mục
Write Extendd Attributes	Thay đổi thuộc tính mở rộng của các tập tin và thư mục
Delete Subfolders and Files	Xóa thư mục con và các tập tin
Delete	Xóa các tập tin
Read Permissions	Đọc các quyền trên các tập tin và thư mục
Change Permissions	Thay đổi quyền trên các tập tin và thư mục
Take Ownership	Tước quyền sở hữu của các tập tin và thư mục

Bảng 6.2 Chức năng các quyền truy cập của NTFS

3.2. Các mức quyền truy cập được dùng trong NTFS

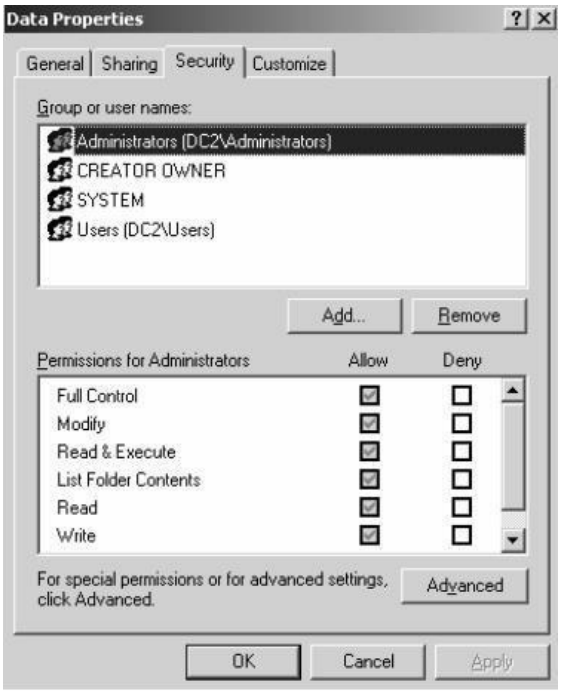
Tên quyền	Full	Modify	Read&	List	Read	Write

	Control		**Execute**	**Folder Contents**		
Traverse Folder /Execute File	X	X	X	X		
List Folder /Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create File /Write Data	X	X				
Create Folder /Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					

Bảng 6.3 Bảng mô tả các mức quyền truy cập được dùng trong NTFS

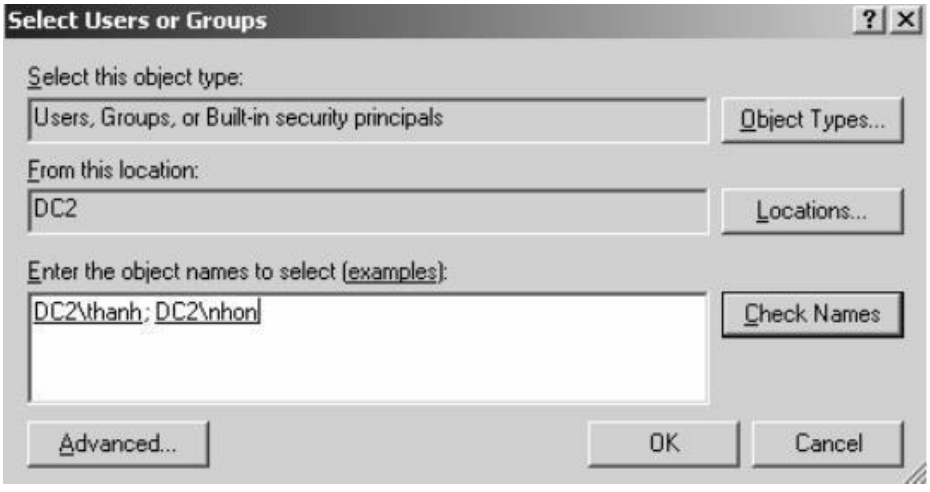
3.3. Gán quyền truy cập NTFS trên thư mục dùng chung

Muốn gán quyền **NTFS**, thông qua **Windows Explorer** bạn nhấp phải chuột vào tập tin hay thư mục cần cấu hình quyền truy cập rồi chọn **Properties**. Hộp thoại **Properties** xuất hiện. Tab này cho phép ta có thể quy định quyền truy cập cho từng người dùng hoặc một nhóm người dùng lên các tập tin và thư mục. Nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.



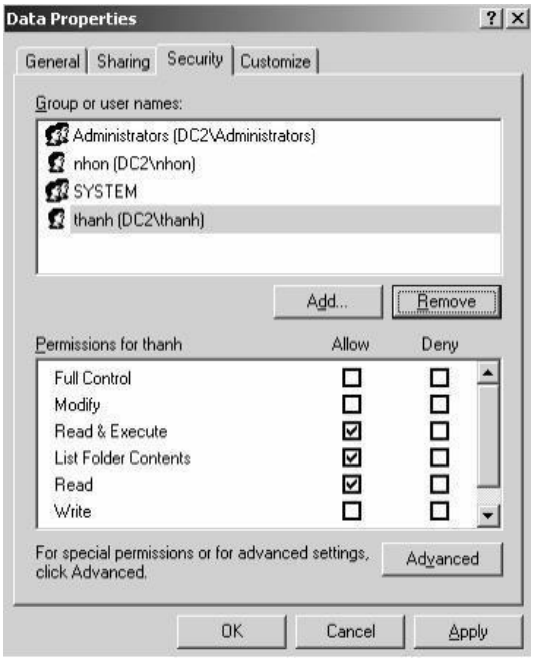
Hình 6.7 Tab Security

Muốn cấp quyền truy cập cho một người dùng, nhấp chuột vào nút **Add**, hộp thoại chọn lựa người dùng và nhóm xuất hiện, chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút **Add** để thêm vào danh sách, sau đó nhấp chuột vào nút **OK** để trở lại hộp thoại chính.



Hình 6.8 Chọn người dùng và nhóm để xuất hiện

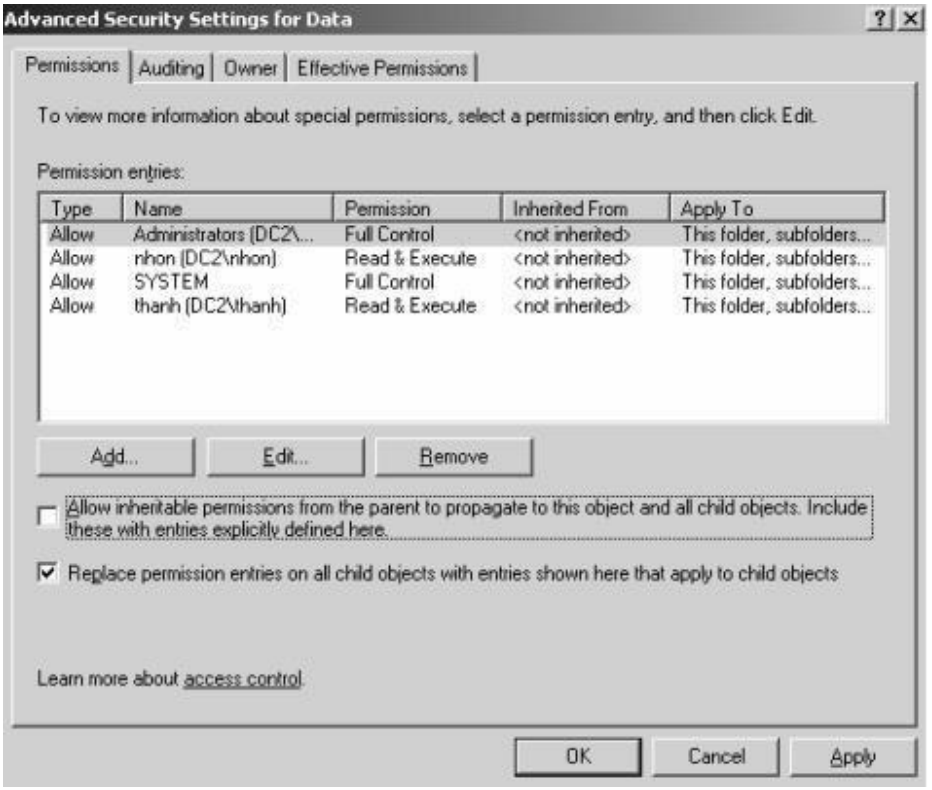
Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách quyền, muốn cho người dùng đó có quyền gì thì đánh dấu vào phần **Allow**, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục **Deny**.



Hình 6.9 Chọn người dùng và nhóm để cấp quyền

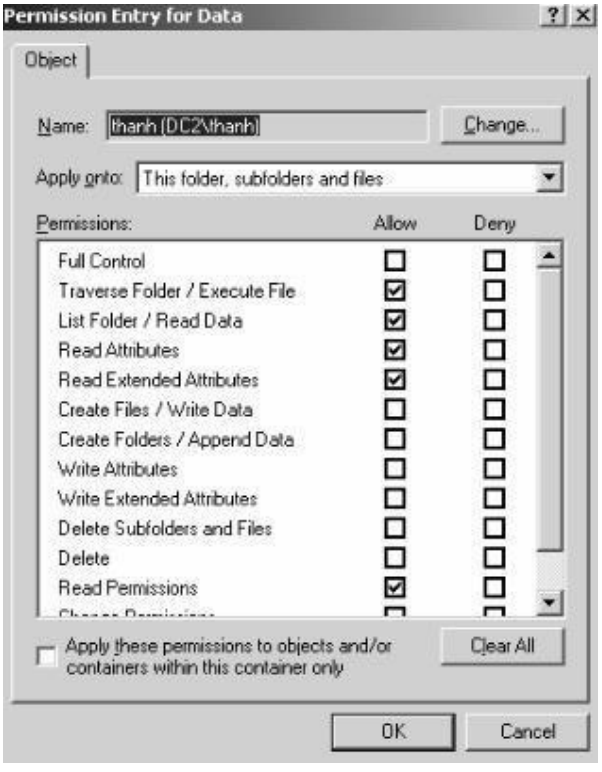
3.4. Kế thừa và thay thế quyền của đối tượng con

Trong hộp thoại chính trên, chúng ta có thể nhấp chuột vào nút **Advanced** để cấu hình chi tiết hơn cho các quyền truy cập của người dùng. Khi nhấp chuột vào nút **Advanced**, hộp thoại **Advanced Security Settings** xuất hiện, trong hộp thoại, nếu bạn đánh dấu vào mục **Allow inheritable permissions from parent to propagate to this object and child objects** thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, bạn muốn xóa những quyền thừa hưởng từ thư mục cha bạn phải bỏ đánh dấu này. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra nếu bạn đánh dấu vào mục **Replace permission entries on all child objects with entries shown here that apply to child objects** thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tập tin và thư mục con có nghĩa là các tập tin và thư mục con sẽ được thay thế quyền truy cấp giống như các quyền đang hiển thị trong hộp thoại.



Hình 6.10 Cấu hình quyền kế thừa

Trong hộp thoại này, **Windows Server** cũng cho phép kiểm tra và cấu hình lại chi tiết các quyền của người dùng và nhóm, để thực hiện, chọn nhóm hay người dùng cần thao tác, sau đó nhấp chuột vào nút **Edit.**



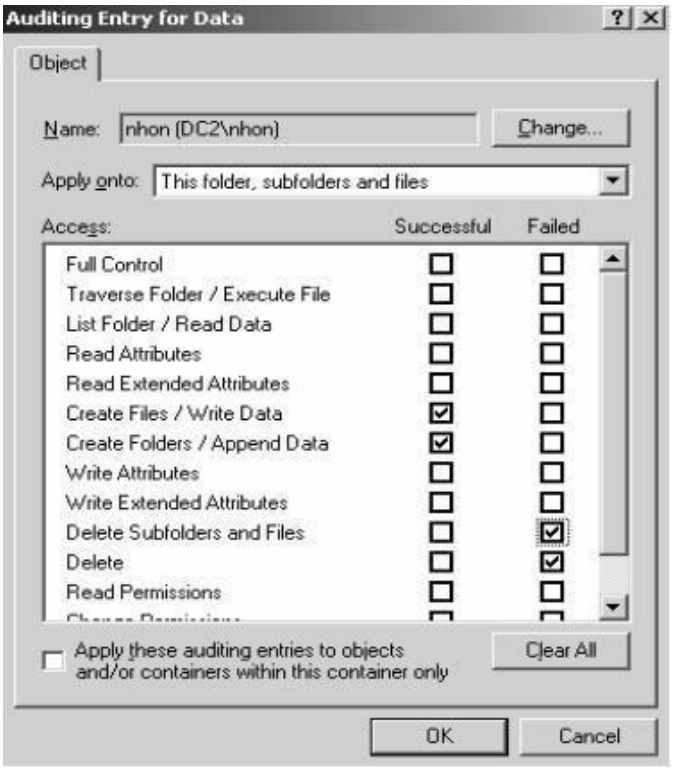
Hình 6.11 Cấu hình quyền kế thừa

3.5. Thay đổi quyền khi di chuyển thư mục và tập tin

Khi chúng ta sao chép (**copy**) một tập tin hay thư mục sang một vị trí mới thì quyền truy cập trên tập tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha chứa chúng, nhưng ngược lại nếu chúng ta di chuyển (**move**) một tập tin hay thư mục sang bất kì vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.

3.6. Giám sát người dùng truy cập thư mục

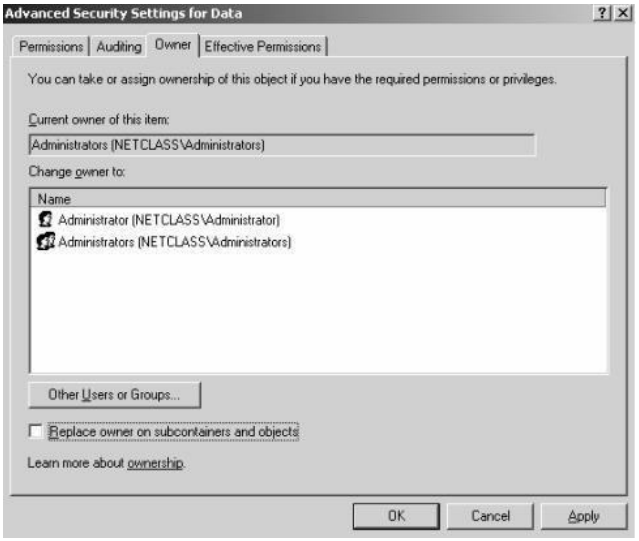
Muốn giám sát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Auditing**, nhấp chuột vào nút **Add** để chọn người dùng cần giám sát, sau đó muốn giám sát việc truy xuất thành công thì đánh dấu vào mục **Successful**, ngược lại giám sát việc truy xuất không thành công thì đánh dấu vào mục **Failed**.



Hình 6.12 Giám sát người dùng truy cập thư mục

3.7. Thay đổi người sở hữu thư mục

Muốn xem tài khoản người và nhóm người dùng sở hữa thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Owner.** Đồng thời có thể thay đổi người và nhóm người sở hữu thư mục này bằng cách nhấp chuột vào nút **Other Users or Groups**.



Hình 6.13 Thay đổi người dùng sở hữu thư mục

4. DFS

DFS (**Distributed File System**) là hệ thống tổ chức sắp xếp các thư mục, tập tin dùng chung trên mạng mà **Server** quản lý, ở đó có thể tập hợp các thư mục dùng chung nằm trên nhiều **Server** khác nhau trên mạng với một tên chia sẻ duy nhất. Nhờ hệ thống này mà người dùng dễ dàng tìm kiếm một tài nguyên dùng chung nào đó trên mạng… **DFS** có hai loại **root**: **domain root** là hệ thống **root** gắn kết vào **Active Directory** được chứa trên tất cả **Domain Controller**, **Stand-alone root** chỉ chứa thông tin ngay tại máy được cấu hình. Chú ý **DFS** không phải là một **File Server** mà nó là chỉ là một "bảng mục lục" chỉ đến các thư mục đã được tạo và chia sẻ sẵn trên các **Server**. Để triển khai một hệ thống **DFS** trước tiên chúng ta phải hiểu các khái niệm sau:

- Gốc **DFS** (**DFS root**) là một thư mục chia sẻ đại diện cho chung cho các thư mục chia sẻ khác trên các **Server**.

- Liên kết **DFS** (**DFS link**) là một thư mục nằm trong **DFS root**, nó ánh xạ đến một tài nguyên chia sẻ các **Server** khác

4.1. So sánh hai loại DFS

Stand-alone DFS	Fault-tolerant DFs
- Là hệ thống DFS trên một máy **Server** **Stand-alone**, không có khả năng dung lỗi.	- Là hệ thống **DFS** dựa trên nền **Active Directory** nên có chính dung lỗi cao.

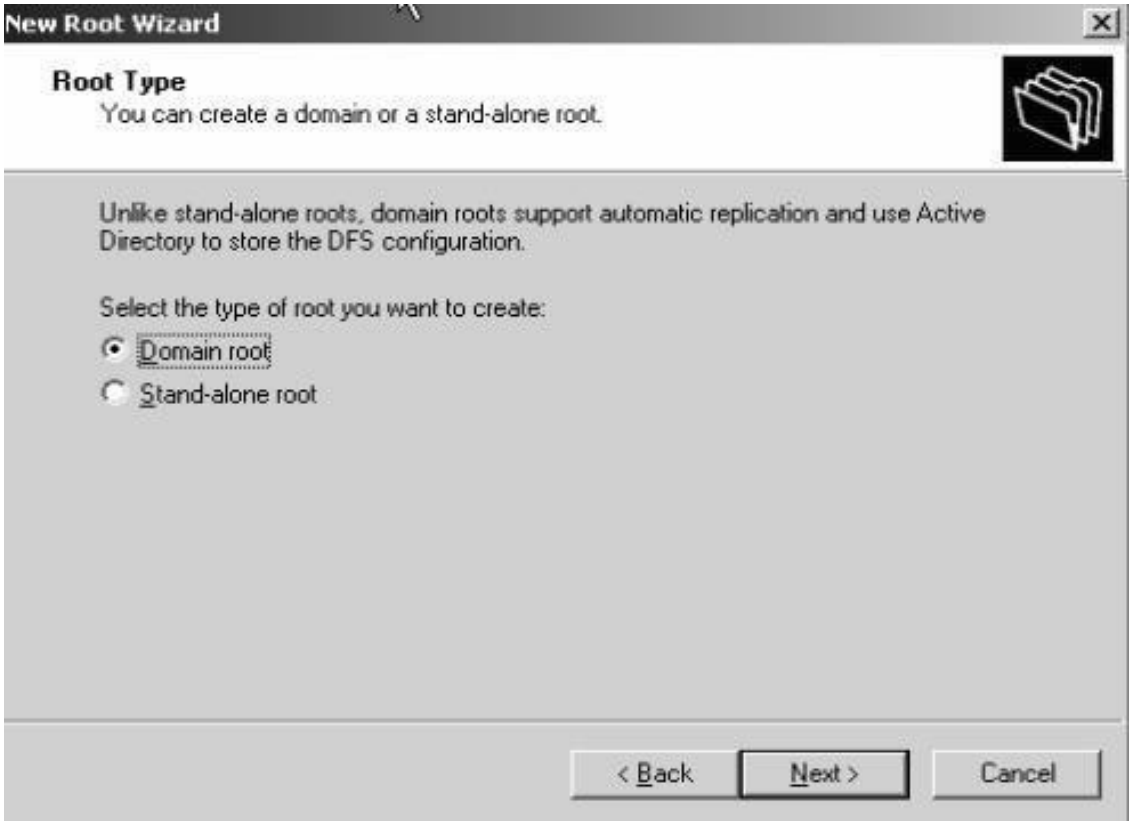
-	-
Người dùng truy xuất hệ thống DFS thông qua đường dẫn \\servername\dfsname .	Hệ thống **DFS** sẽ tự động đồng bộ giữa các **Domain Controller** và người dùng có t hể truy xuất đến **DFS** thông qua đườngdẫn **\\domainname\dfsname**.

Bảng 6.4 Bảng so sánh hai loại DFS

4.2. Cài đặt Fault-tolerant DFS

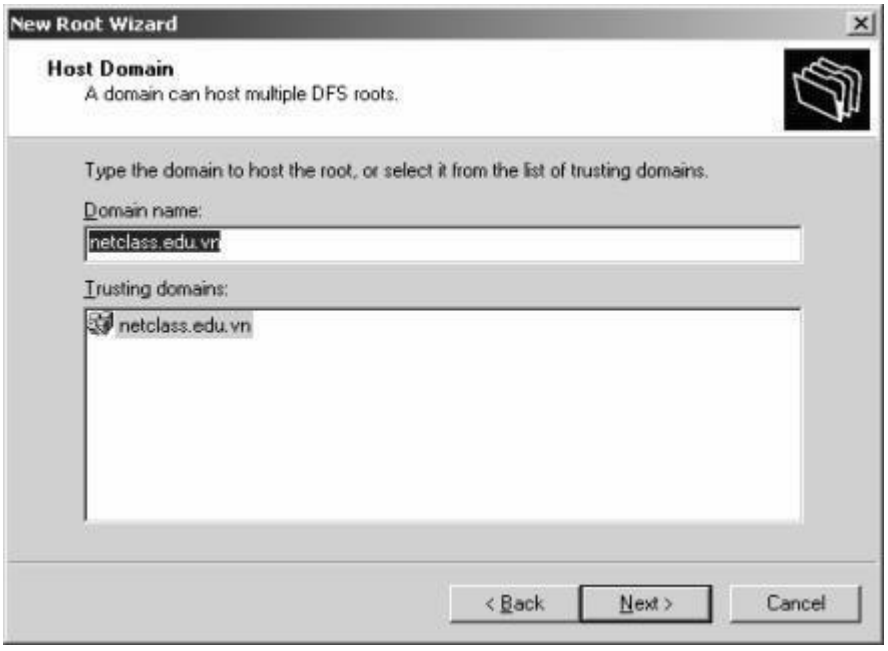
Để tạo một hệ thống **Fault-tolerant DFS** bạn làm theo các bước sau:

Bạn nhấp chuột vào **Start** -> **Programs** -> **Administrative Tools** -> **Distributed File System**. Hộp thoại **Welcome** xuất hiện, nhấn **Next** để tiếp tục. Hộp thoại **Root Type** xuất hiện, chọn mục **Domain Root**, nhấn **Next** để tiếp tục.



Hình 6.14 Hộp thoại Root Type

Hệ thống yêu cầu chọn tên miền **(domain name)** kết hợp với hệ thống **DFS** cần tạo.

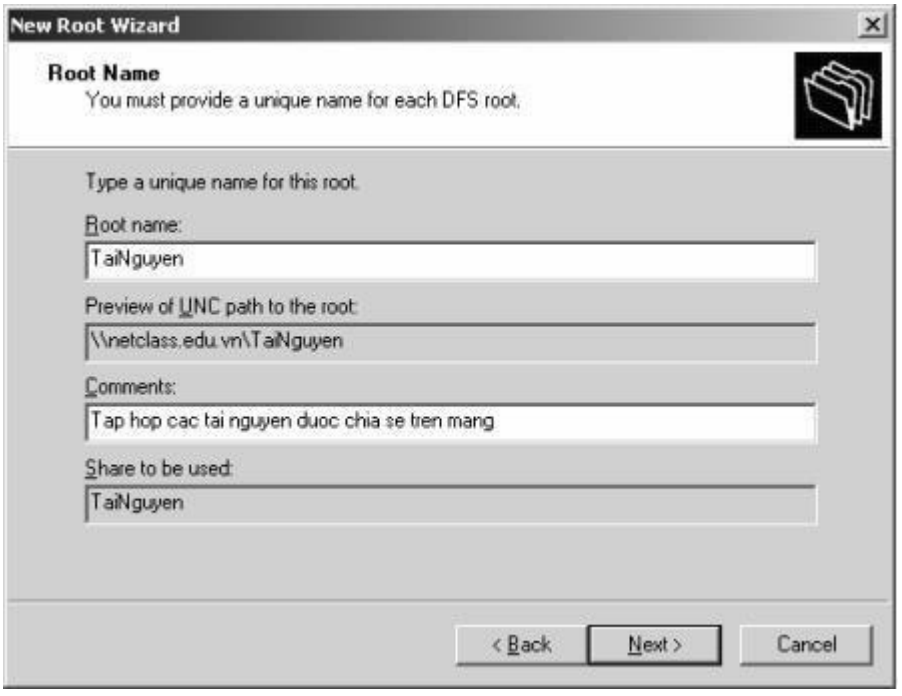


Hình 6.15 Chọn tên miền

Tiếp theo khai báo tên của **Domain Controller** chưa **root DFS** cần tạo.

Hình 6.16 Khai báo tên Domain Controller

Đến đây bạn khai báo tên chia sẻ gốc (**Root Name**) của hệ thống **DFS**, đây chính là tên chia sẻ đại diện cho các tài nguyên khác trên mạng. Bạn nhập đầy đủ các thông tin chọn **Next** để tiếp tục.

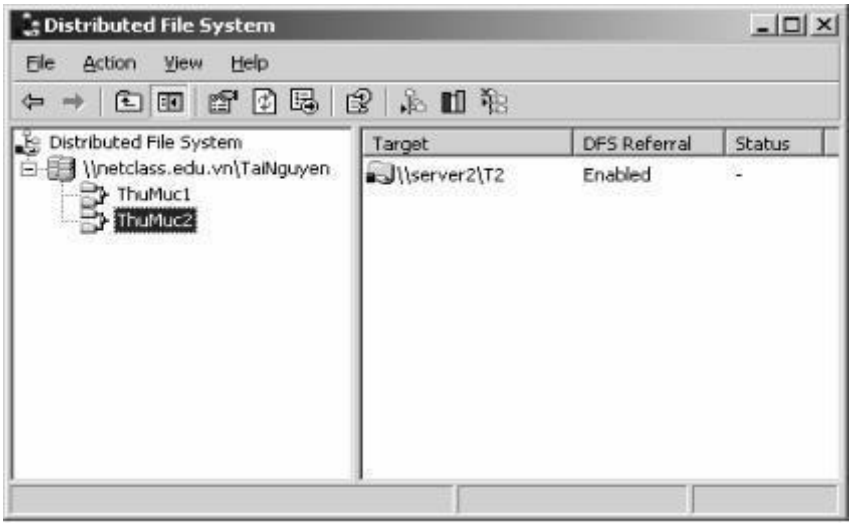


Hình 6.17 Khai báo tên chia sẻ gốc (Root Name) của hệ thống DFS

Trong hộp thoại xuất hiện, khai báo tên thư mục chia sẻ gốc của hệ thống **DFS**.

Hình 6.18 Khai báo tên thư mục chia sẻ gốc của hệ thống DFS.

Sau khi cấu hình hệ thống **DFS** hoàn tất, tạo các liên kết đến các tài nguyên dùng chung trên các **Server** khác trong mạng.



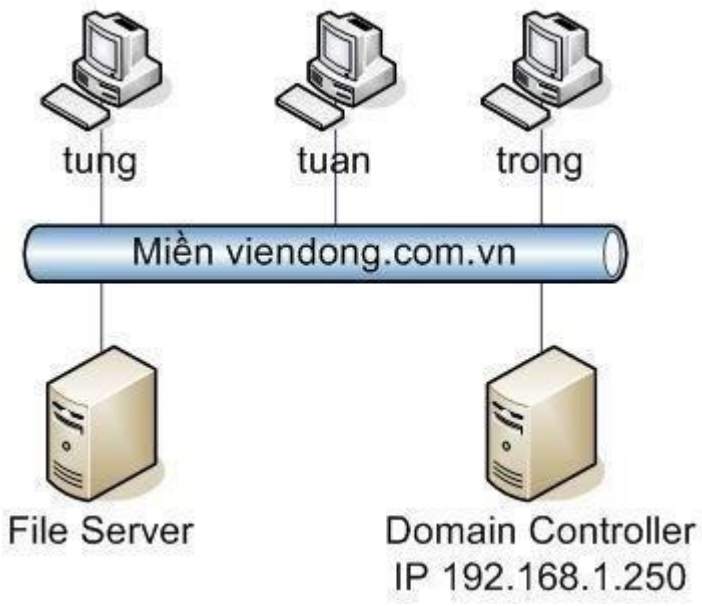
Hình 6.19 tạo các liên kết đến các tài nguyên dùng chung trên các Server khác trong mạng.

Để sử dụng hệ thống **DFS** này, tại máy trạm ánh xạ (**map**) thư mục chia sẻ gốc thành một ổ đĩa mạng. Trong ổ đĩa mạng này có thể nhìn thấy tất cả các thư mục chia sẻ trên các **Server** khác nhau trên hệ thống mạng.

Hình 6.20 ánh xạ (map) thư mục chia sẻ gốc thành một ổ đĩa mạng.

Tương tự như **Fault-tolerant DFS**, có thể tạo ra một **Stand-alone DFS** trên một máy **Server Stand-alone**, tất nhiên là hệ thống đó không có khả năng dung lỗi có nghĩa là khi **Server** chứa **DFS Root** hỏng thì các máy trạm sẽ không tìm thấy các tài nguyên chia sẻ trên các **Server** khác. Nhưng hệ thống **Stand-alone DFS** được sử dụng rộng rải vì nó đơn giản, tiện dụng.

CÂU HỎI VÀ BÀI TẬP BÀI 6



1. Thiết lập quyền người dùng trên thư mục dùng chung

Trên File Server có tài khoản người dùng và nhóm như sau:

- Nhóm BanGiamDoc gồm: Hung, Trong
- Nhóm NhanVien gồm: Diep, Tuan, Tung

Hãy tạo cấu trúc thư mục như hình sau.

Sau đó, Hãy cấp quyền truy cập cho người dùng theo yêu cầu sau:

- Mỗi người dùng có toàn quyền trên thư mục dành riêng của mình.

- Trưởng phòng của mỗi phòng ban sẽ đọc được dữ liệu của các thành viên khác trong phòng. Trưởng phòng là tài khoản đầu tiên trong danh sách của mỗi nhóm.

- Thư mục Public là thư mục dùng chung, mọi người có thể ghi dữ liệu lên đó nhưng chỉ xóa được những dữ liệu cho mình tạo ra.

- Mọi người có thể truy cập thư mục Public từ máy cục bộ hoặc từ một máy khác trong hệ thống mạng

2. Cấu hình DFS

Trên hệ thống mạng đang có, các tài nguyên chia sẻ nằm rải rác trên các máy Server khác nhau.

- Trên máy File Server đang chia sẻ thư mục Public.
- Trên máy Tuan đang chia sẻ thư mục Software.
- Trên máy Diep đang chia sẻ thư mục Music.

Mọi người dùng chỉ truy cập vào một tài nguyên chia sẻ trên máy Server có địa chỉ IP 192.168.1.250. Từ đó, mọi người có thể truy cập các tài nguyên trên.

Hãy cấu hình hệ thống theo yêu cầu trên.

BÀI 7: DỊCH VỤ DHCP

Mã bài: MĐ 15 - 07

Giới thiệu:

Ở bất cứ hệ thống mạng, cho dù là nhỏ hay lớn thì khi các thiết bị điện tử kết nối sử dụng địa chỉ IP động đều được cấp từ dịch vụ DHCP server. Tùy vào mạng lớn hay nhỏ mà DHCP sẽ thực hiện các cách khác nhau. Đối với mạng nhỏ thì DHCP cấp IP động cho các máy trạm nằm ở các thiết bị mạng như Switch, Modem, Router... còn mạng lớn thì các máy trạm sẽ nằm ở Domain. Thường các nhà quản trị sẽ sử dụng dịch vụ DHCP server có sẵn trên Windows để phát IP động cho các máy trạm chứ không sử dụng DHCP server tích hợp sẵn trong các thiết bị mạng ở phần cứng

Trong bài 7 sẽ giới thiệu về DHCP, cài đặt và cấu hình DHCP trên Window Server

Mục tiêu:

- Mô tả được sự hoạt động của dịch vụ DHCP;
- Cài đặt và cấu hình được dịch vụ DHCP.

Nội dung chính:

1. Giới thiệu

Một máy tính hay thiết bị khác phải được cấu hình theo một tham số trước khi có thể hoạt động trên một mạng. Ta phải cấu hình các tham số như tên lĩnh vực và địa chỉ IP của hệ khách, địa chỉ IP của hệ phục vụ DNS để phân giải tên của hệ chủ và mặt nạ con. Không có các tham số cấu hình này, một máy tính hay thiết bị khác không thể tương tác với các thiết bị khác trên mạng. Ngày nay hầu hết các mạng TCP/IP đều sử dụng DHCP để tự động cấp các địa chỉ IP và các tham số cho hệ khách. Khi đã cài đặt DHCP, bạn sẽ dựa vào máy phục vụ DHCP để cung cấp thông tin cơ bản cần thiết cho hoạt động nối mạng TCP/IP: địa chỉ IP, mặt nạ mạng con, bộ định tuyến mặt định, máy phục vụ DNS chính và phụ, máy phục vụ WINS chính và phụ, tên vùng DNS.

DHCP được thiết kế nhằm đơn giản hoá các tác vụ quản trị của vùng AD. DHCP được dùng để gán thông tin cấu hình. cho máy khách mạng, như vậy không những tiết kiệm được thời gian trong giai đoạn lập cấu hình. hệ thống mà còn cung cấp cơ chế tập trung cập nhật cấu hình.. DHCP cho phép chi phối hoạt động gán địa chỉ IP tại điểm tập trung.

2. Hoạt động của giao thức DHCP

Giao thức DHCP làm việc theo mô hình Client/Server . Quá trình tương tác giữa DHCP client và server sẽ diễn ra theo các bước sau :

– Đầu tiên máy client sẽ gửi đi 1 gói tin quảng bá tên là DHCP discover, nhằm yêu cầu cho việc lấy các thông tin cấu hình IP address, subnet mask, defaut getway, preferred DNS ….. lúc này, vì clinet chưa có địa chỉ ip cho nên nó sẽ dùng một địa chỉ source (nguồn) là 0.0.0.0, đồng thời cũng không biết một địa chỉ broadcast là 255.255.255.255 và sau đó gói tin DHCP Discover này sẽ quảng bá đi toàn mạng. gói tin này chứa một địa chỉ MAC (là địa chỉ mà mỗi một card mạng được nhà sản xuất cấp cho là mã để phân biệt các card mạng với nhau). Ngoài ra nó còn chứa tên của máy client để server có thể biết được client nào gởi yêu cầu đến.

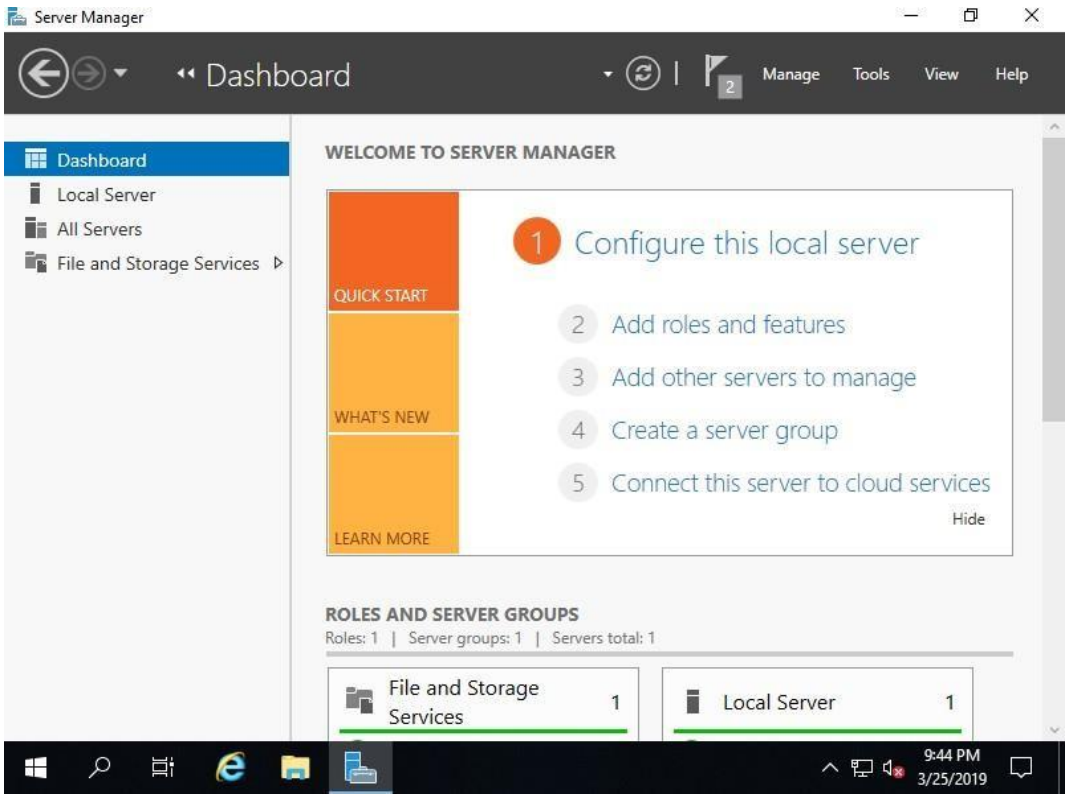
– Sau khi nhận được gói tin DHCP Discover của client, nếu có một DHCP server hợp lệ (nghĩa là nó có khả năng cung cấp địa chỉ IP cho client) thì nó sẽ trả lời lại bằng một goái tin DHCP offer. gói tin này chứa một địa chỉ ip đề nghị cho thuê trong một khoảng thời gian nhất định (mặc định là 8 ngày, sau một khoảng thời gian 50% tức 4 ngày, nó sẽ tự thu hồi IP address đã cấp nếu như client không sử dụng) kèm theo là địa chỉ MAC của client được cấp, một subnet mask và địa chỉ IP của DHCP server đã cấp phát. trong thời gian này server sẽ không cấp phát địa chỉ IP vừa đề nghị cho một client nào khác.

Máy client sau khi nhận được những lời đề nghị là gói tin DHCP Offer trên mạng (trường hợp trong mạng có nhiều hơn 1 DHCP server) sẽ tiến hành chọn lọc một gói tin phù hợp và sau đó phản hồi lại bằng một gói tin là DHCP Request (bao gồm thông tin về DHCP server cấp phát địa chỉ cho nó) để chấp nhận lời đề nghị đó. Điều này giúp cho việc các gói tin còn lại không được chấp nhận sẽ được các server rút lại và dùng để cấp phát cho client khác.

- Khi DHCP server nhận được DHCP request, nó sẽ trả lời lại DHCP client bằng gói tin là DHCP Ack nhằm mục đích thông báo là đã chấp nhận cho DHCP client đó thuê địa chỉ IP. Gói tin này bao gồm địa chỉ IP và các thông tin cấu hình khác (DNS server, Wins server….) cuối cùng client nhận được gói DHCP Ack thì cũng có nghĩa là kết thúc quá trình thuê và cấp phát địa chỉ IP và địa chỉ IP này chính thức được client sử dụng

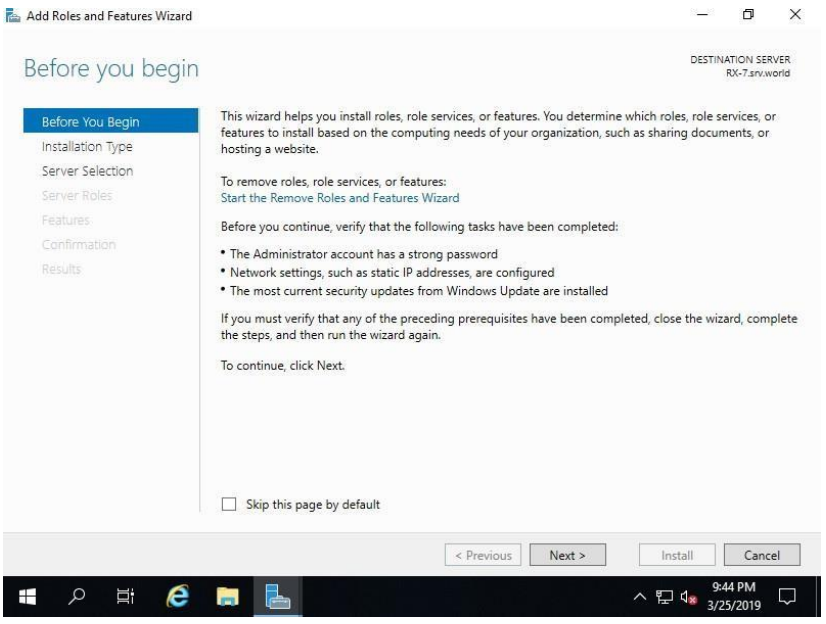
3. Cài đặt dịch vụ DHCP

- Mở Server Manager và Click [Add roles and features].



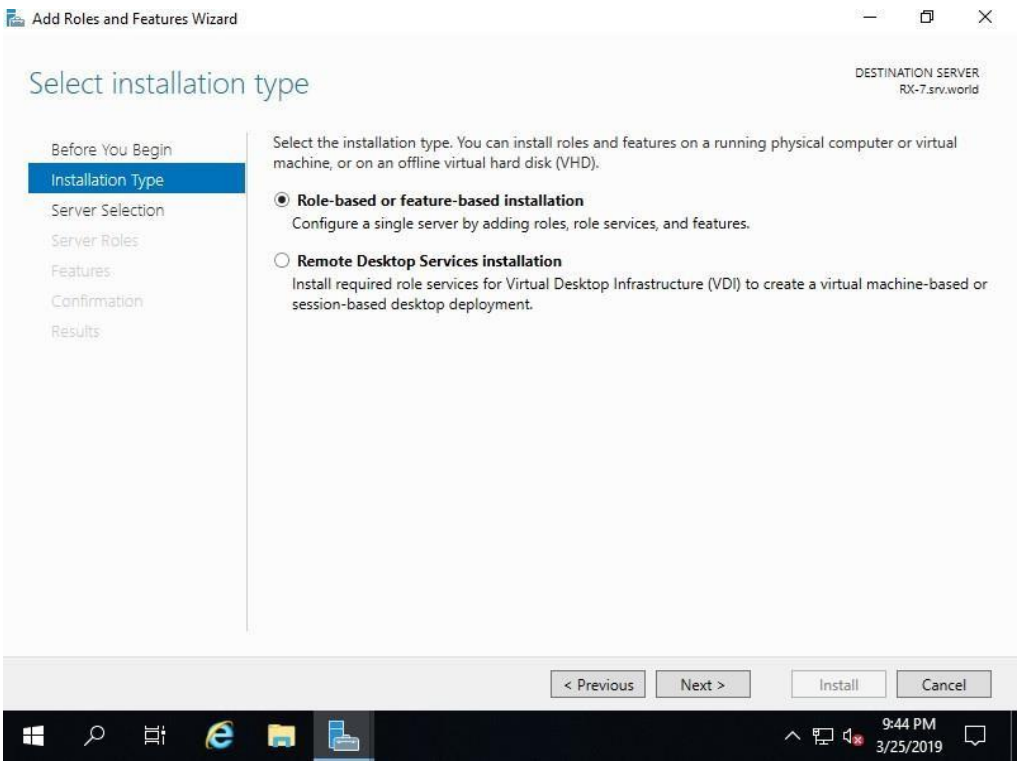
Hình 7.1 Hộp thoại Server Manager

- Click [Next]



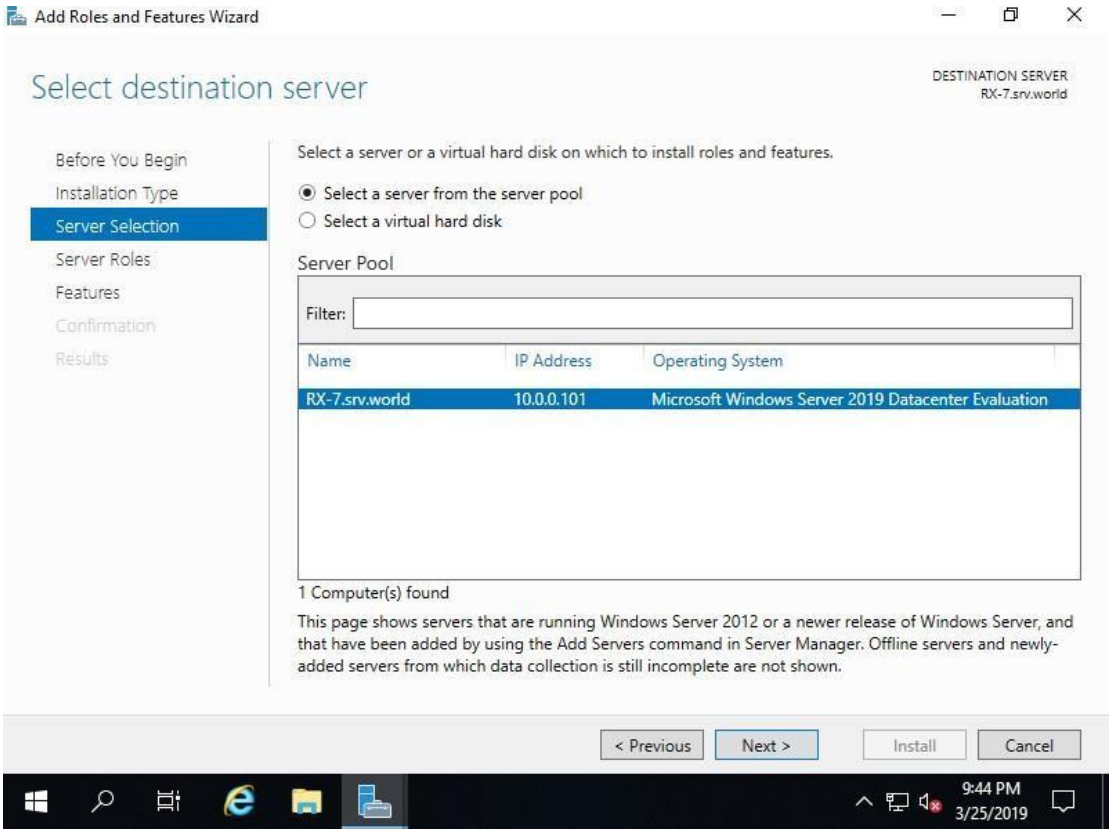
Hình 7.2 Hộp thoại Before you begin

- Chọn [Role-based or feature-based installation], click Next



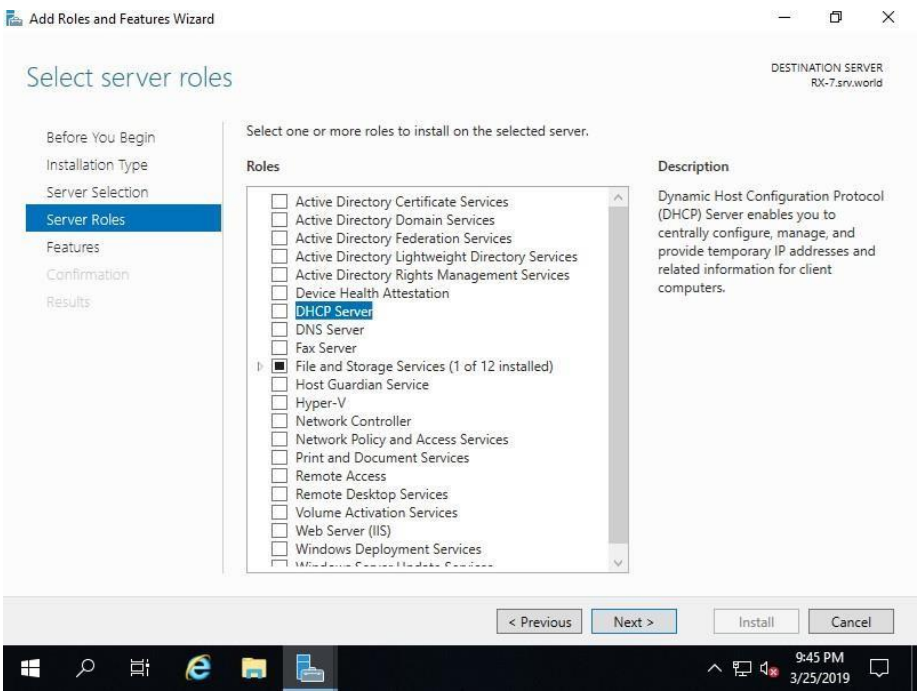
Hình 7.3 Hộp thoại Select installation type

- Chọn Select a server from the server pool, click Next



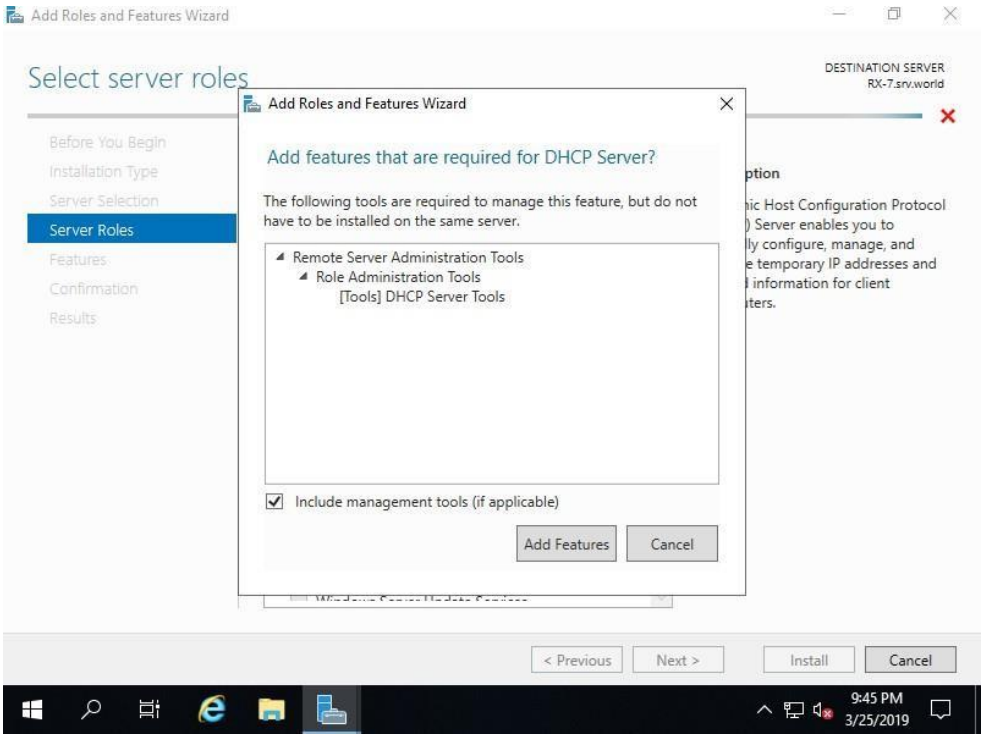
Hình 7.4 Chọn Select a server from the server pool.

- Check vào [DHCP Server], click Next



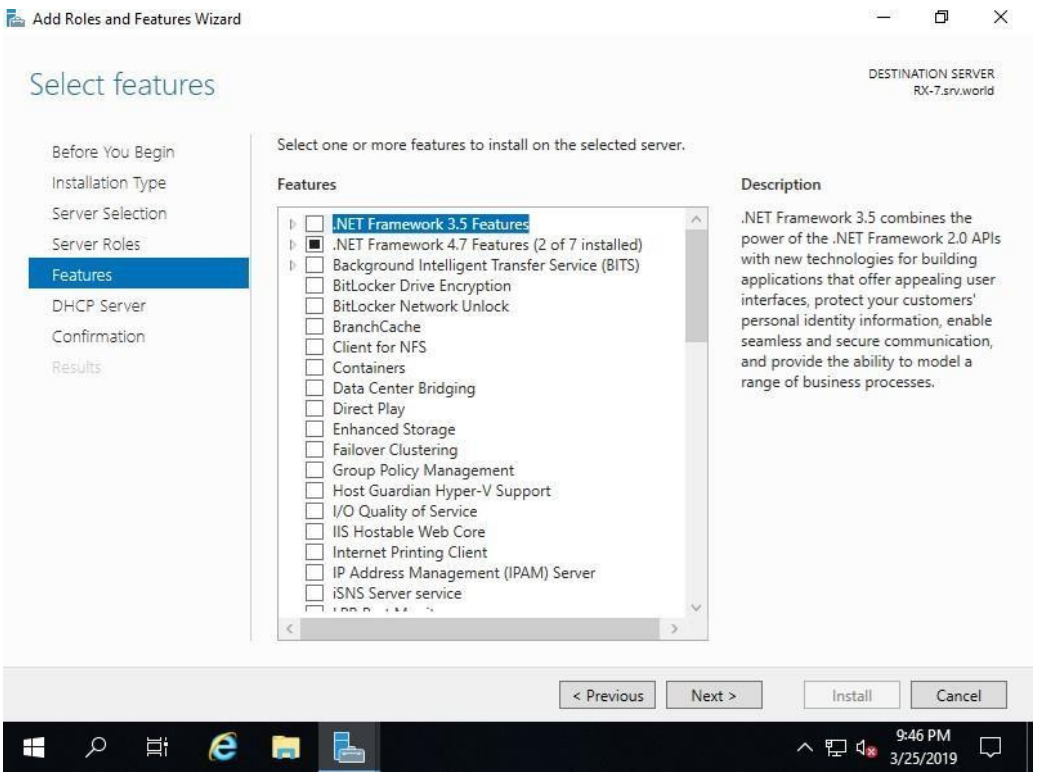
Hình 7.5 Chọn DHCP để cài đặt

- Click [Add Features] và Click [Next]



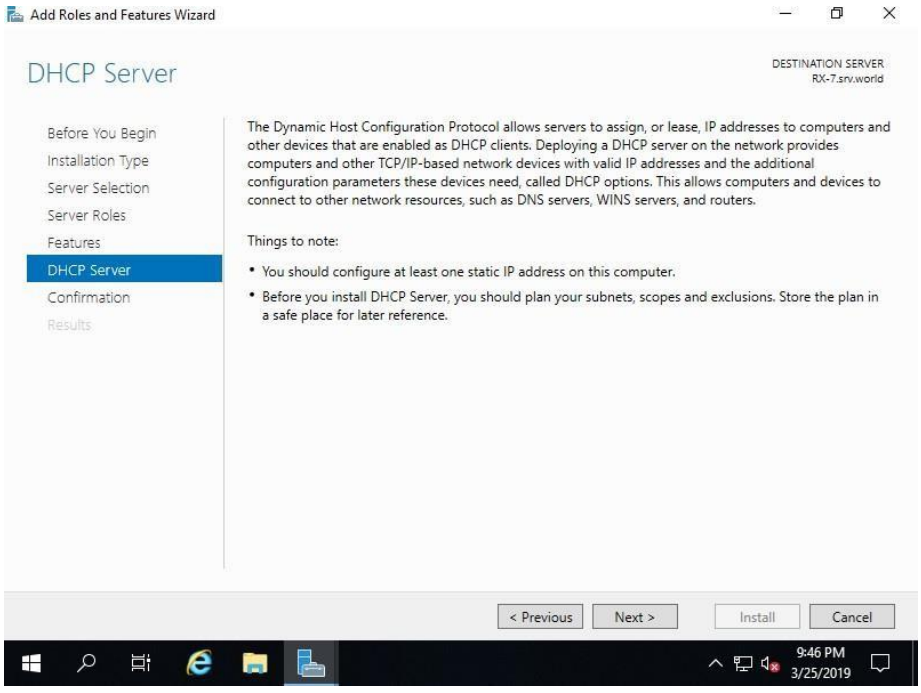
Hình 7.6 Add Features cho DHCP

- Click [Next].



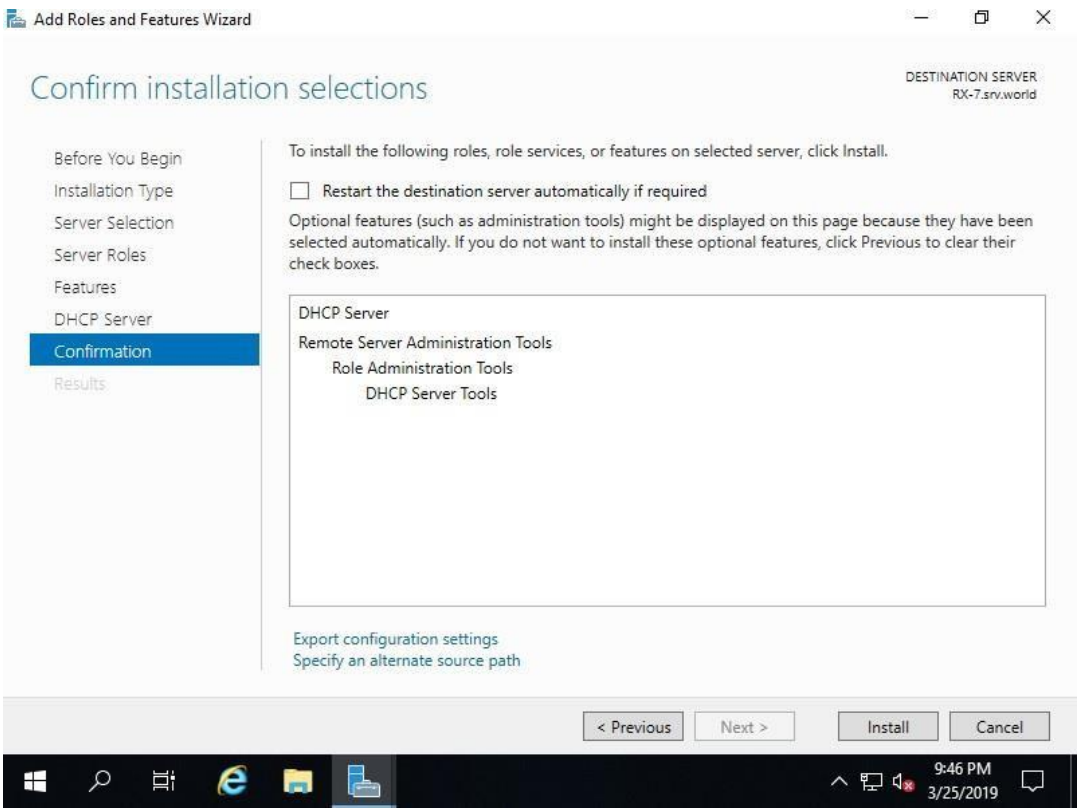
Hình 7.7 Chọn nhữn Features cần cài đặt

- Click [Next].



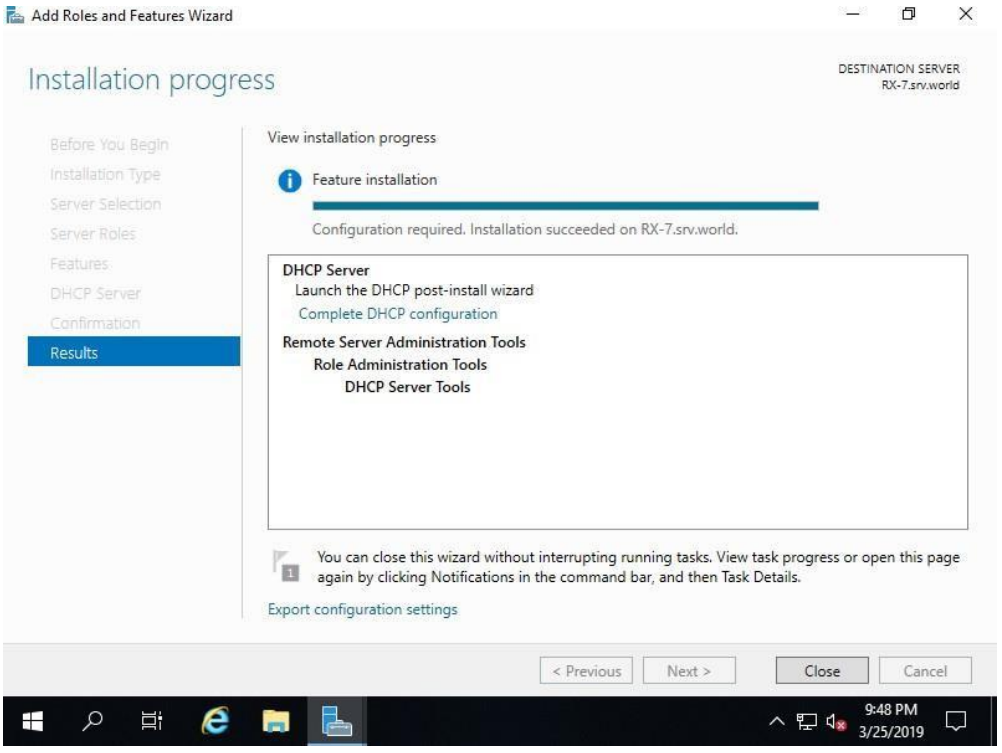
Hình 7.8 Để mặc định trong phần DHCP Server

- Click [Install].



Hình 7.9 Chọn Install để tiến hành cài

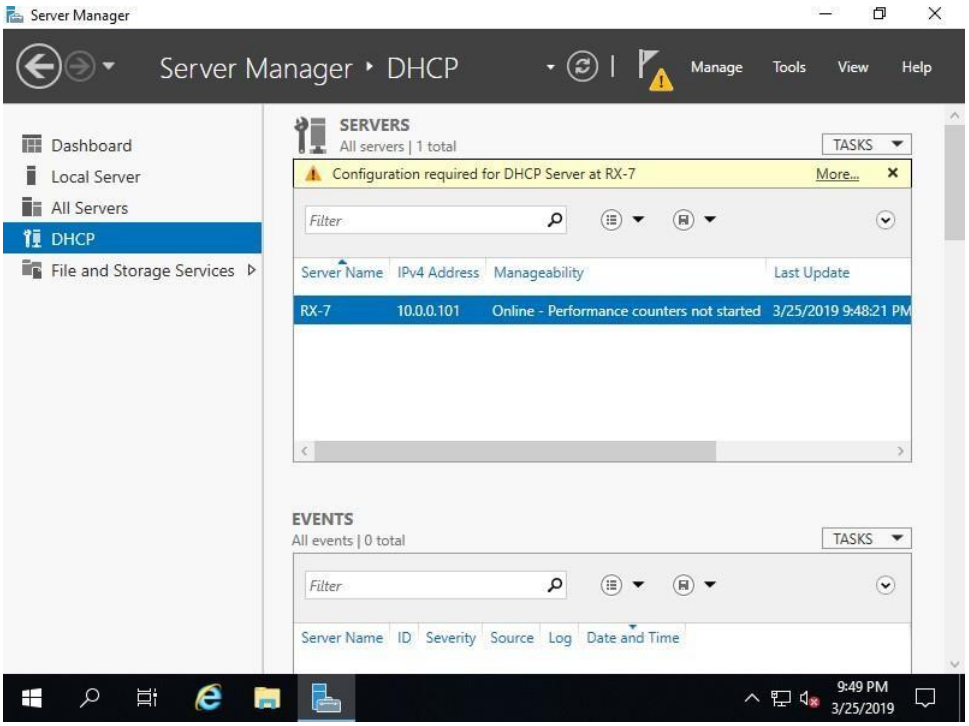
- Click [Close] để hoàn tất



Hình 7.10 Hoàn tất cài đặt

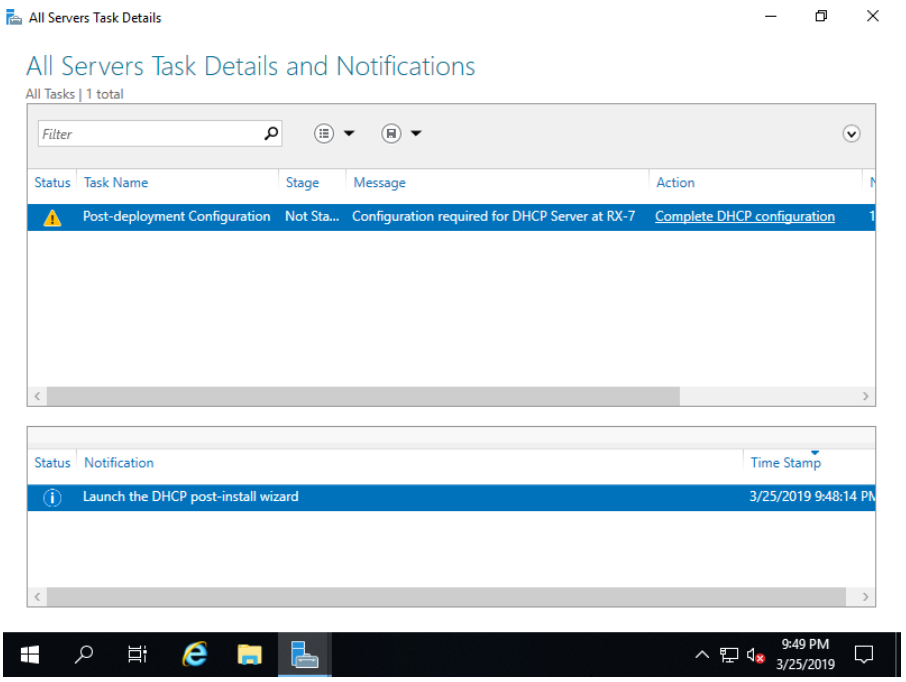
4. Chứng thực dịch vụ DHCP trong Active Directory

- Click More góc trên bên phải



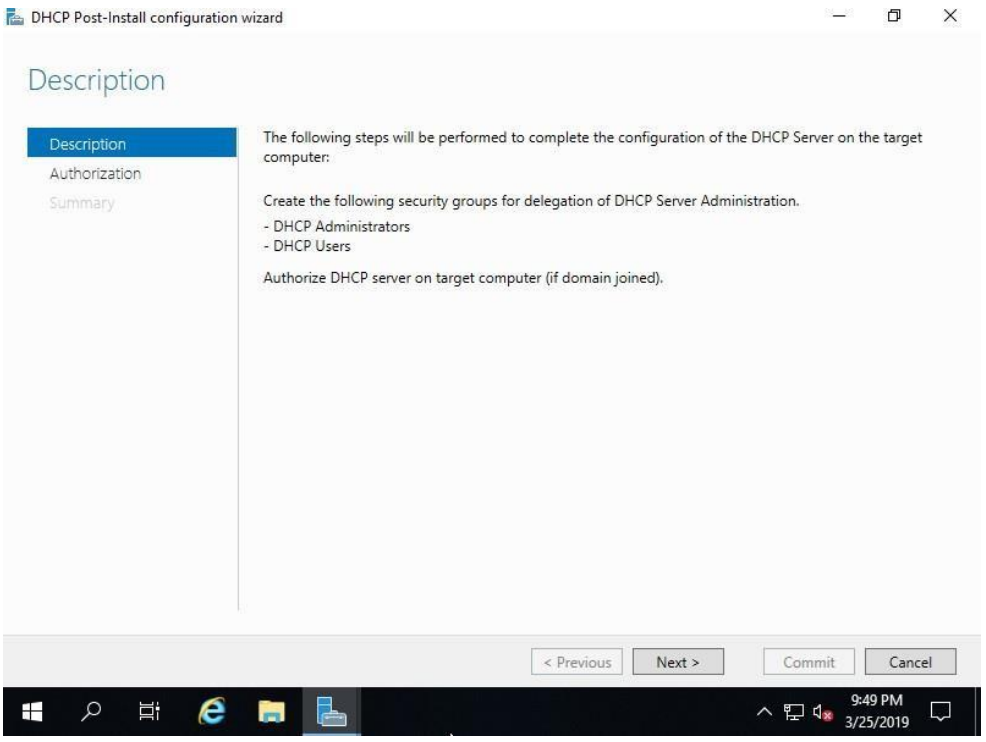
Hình 7.11 Mở hộp thoại Server Manager để bắt đầu

- Click vào link Complete DHCP configuration



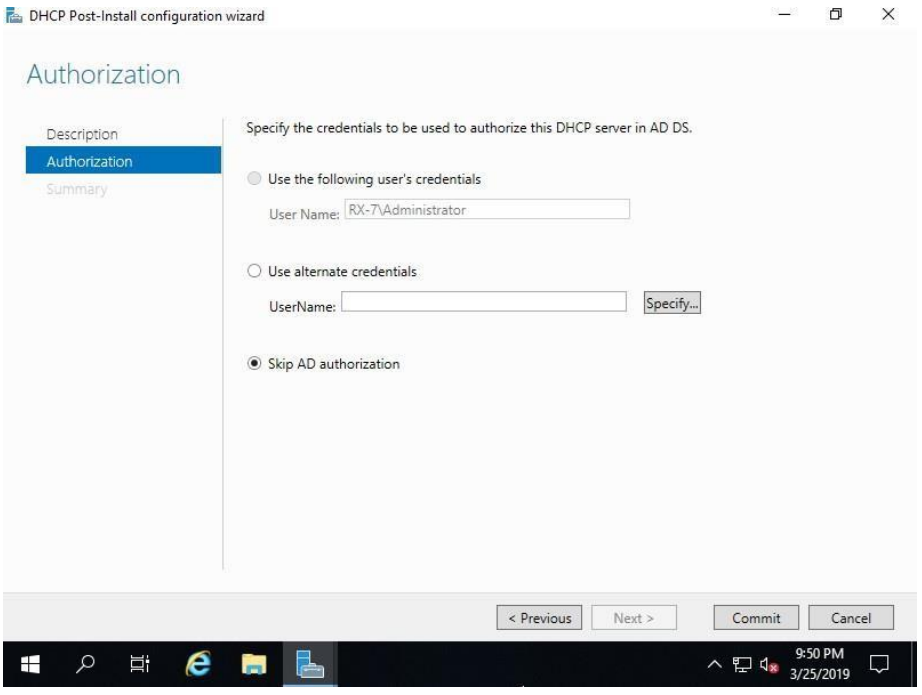
Hình 7.12 Click vào link Complete DHCP configuration

- Click Next



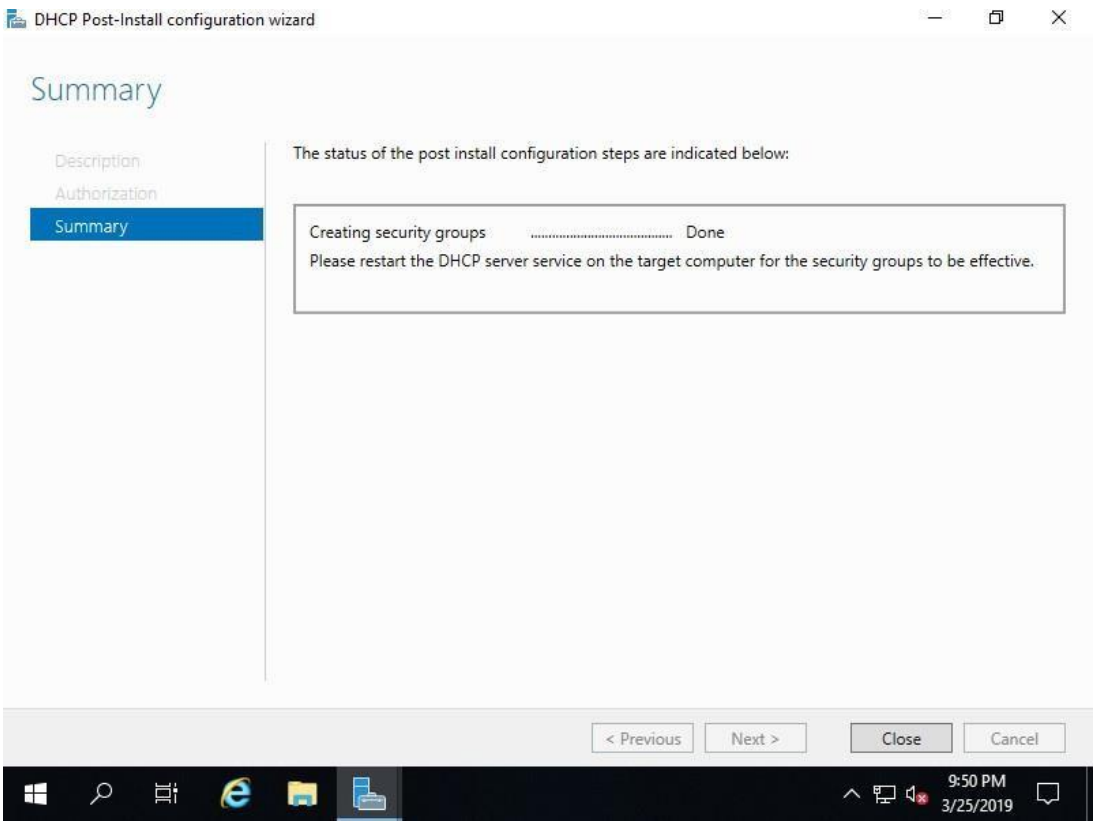
Hình 7.13 Phần Description

- Click [Commit]



Hình 7.14 Chọn dạng chứng thực

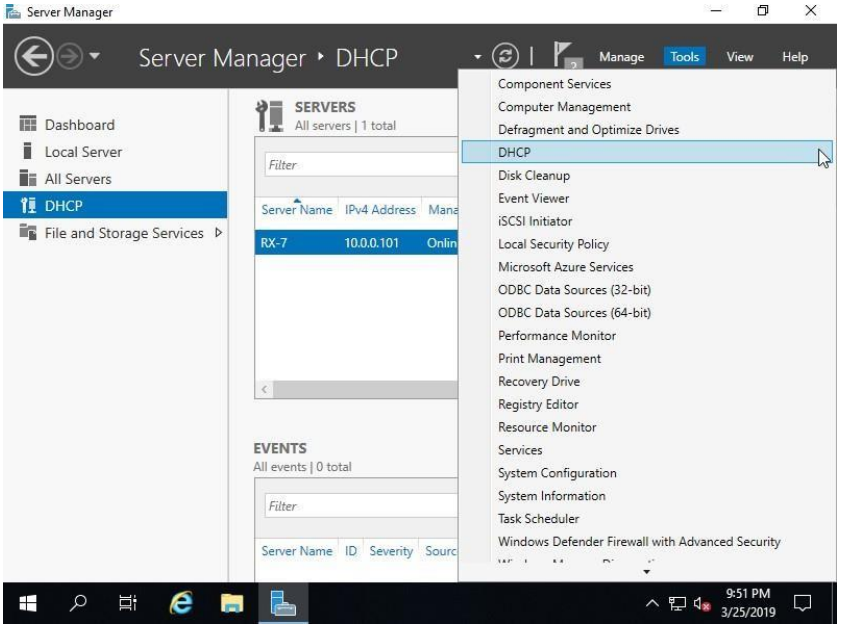
- click [Close]



Hình 7.15 Hoàn tất

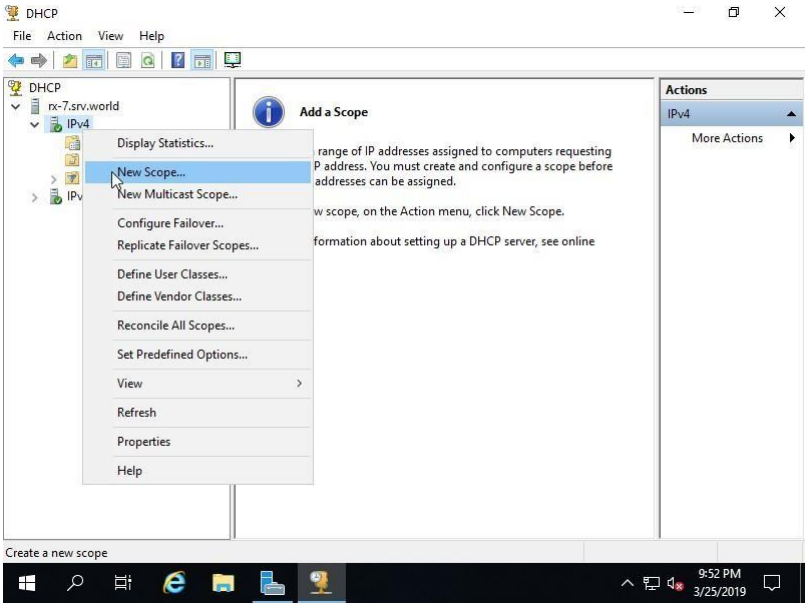
5. Cấu hình dịch vụ DHCP

Sau khi đã cài đặt dịch vụ DHCP, sẽ thấy biểu tượng DHCP trong menu Administrative Tools. Thực hiện theo các bước sau để tạo một scope cấp phát địa chỉ: Chọn menu Start / Programs / Administrative Tools / DHCP. Trong cửa sổ DHCP



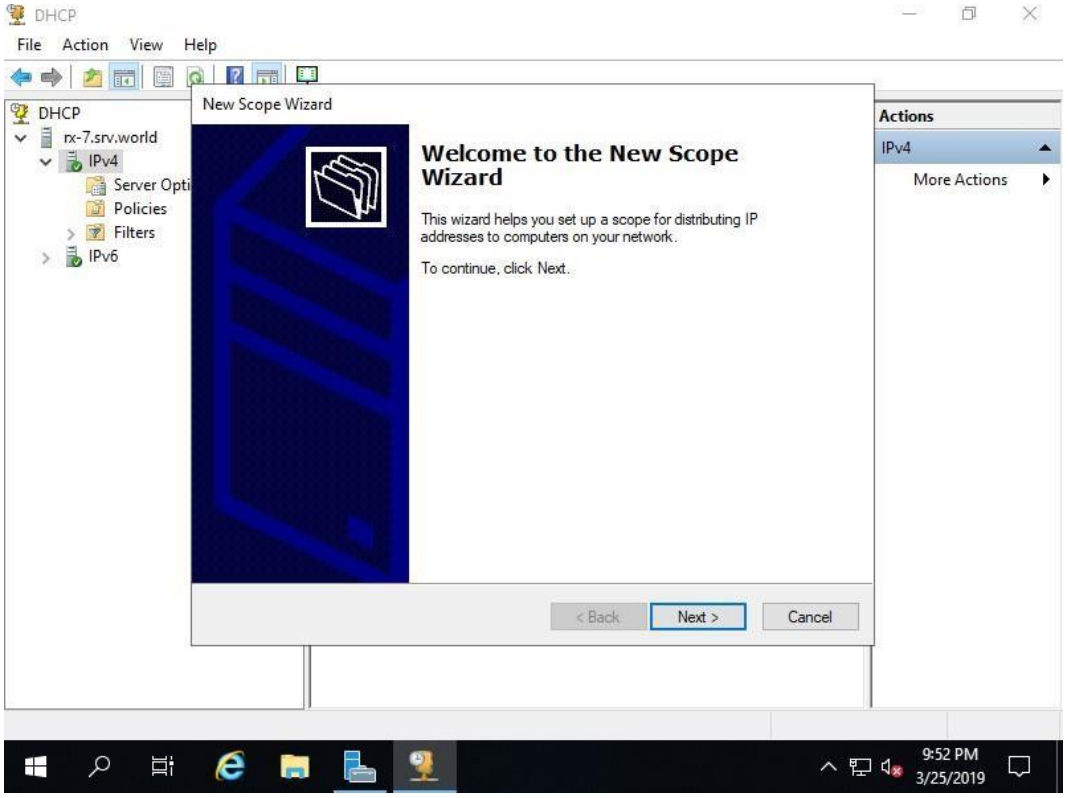
Hình 7.16 Quay lại hộp thoại Server Management mở DHCP

- Click phải chuột lên biểu tượng Server của và chọn mục New Scope trong popup menu



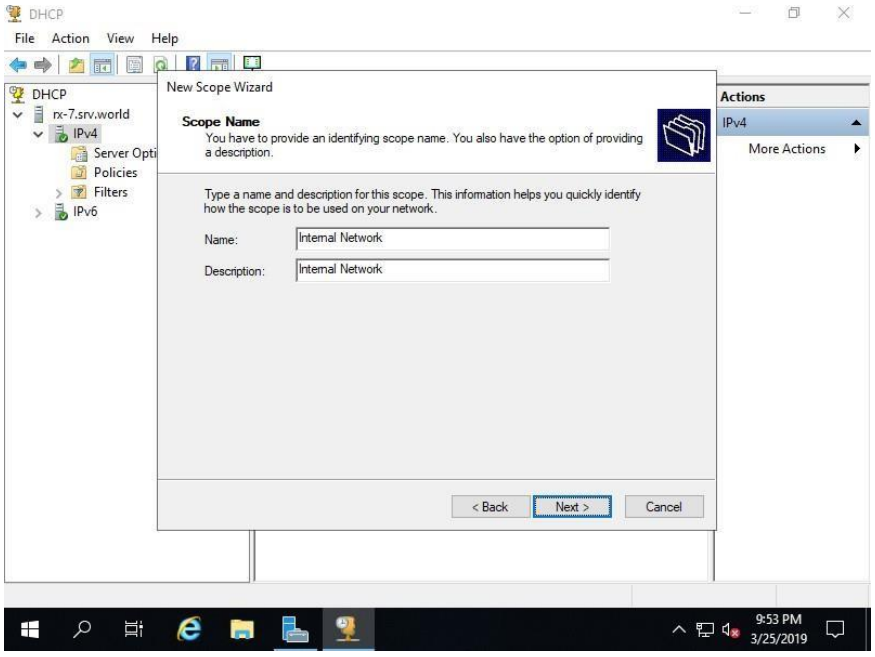
Hình 7.17 Tạo new Scope

- Hộp thoại New Scope Wizard xuất hiện. Nhấn chọn Next.



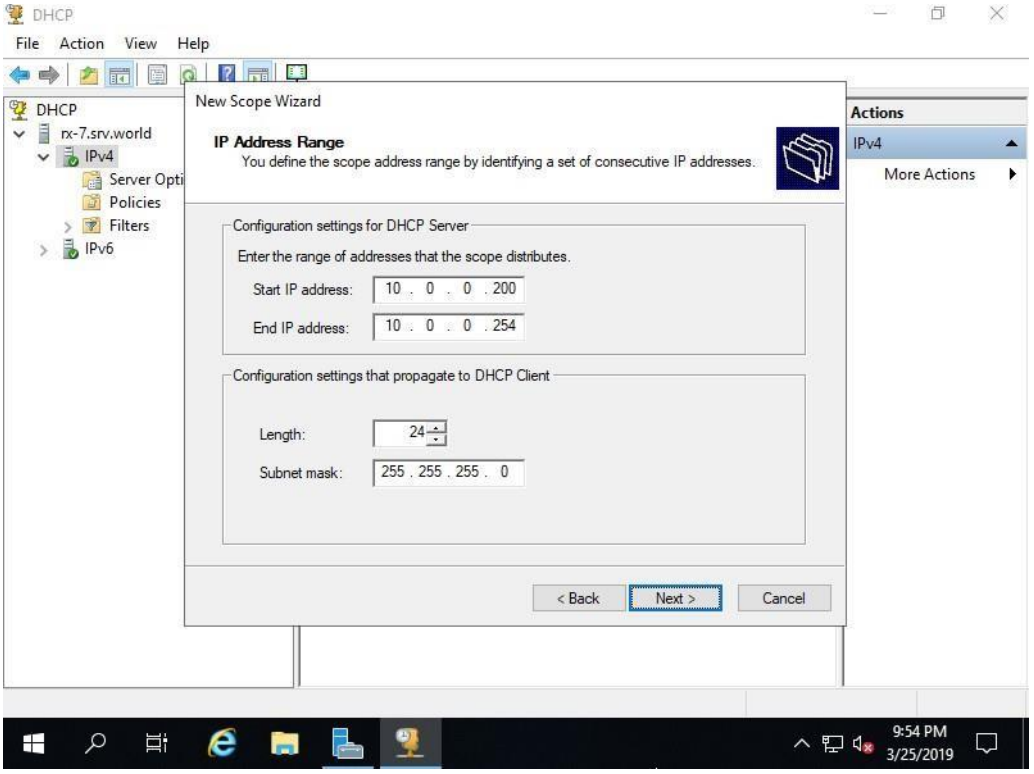
Hình 7.18 Bắt đầu tạo new Scope

- Trong hộp thoại Scope Name, nhập vào tên và chú thích, giúp cho việc nhận diện ra scope này. Sau đó nhấn chọn Next.



Hình 7.19 Đặt tên và mô tả cho Scope

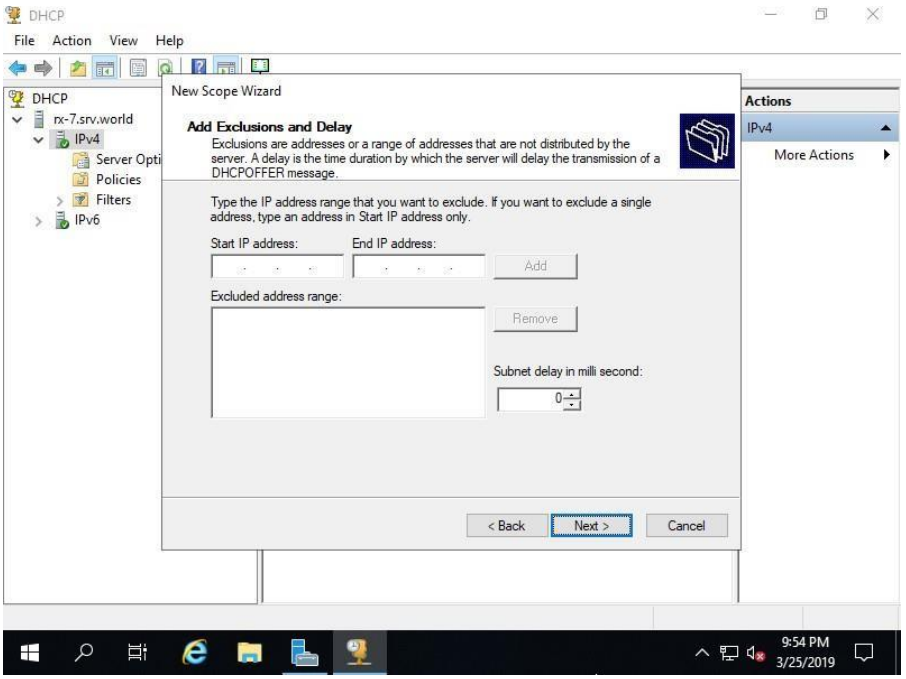
- Hộp thoại IP Address Range xuất hiện. Nhập vào địa chỉ bắt đầu và kết thúc của danh sách địa chỉ cấp phát. Sau đó chỉ định subnet mask. Nhấn chọn Next.



Hình 7.20 Thiết lập dãy địa chỉ IP cấp tự động

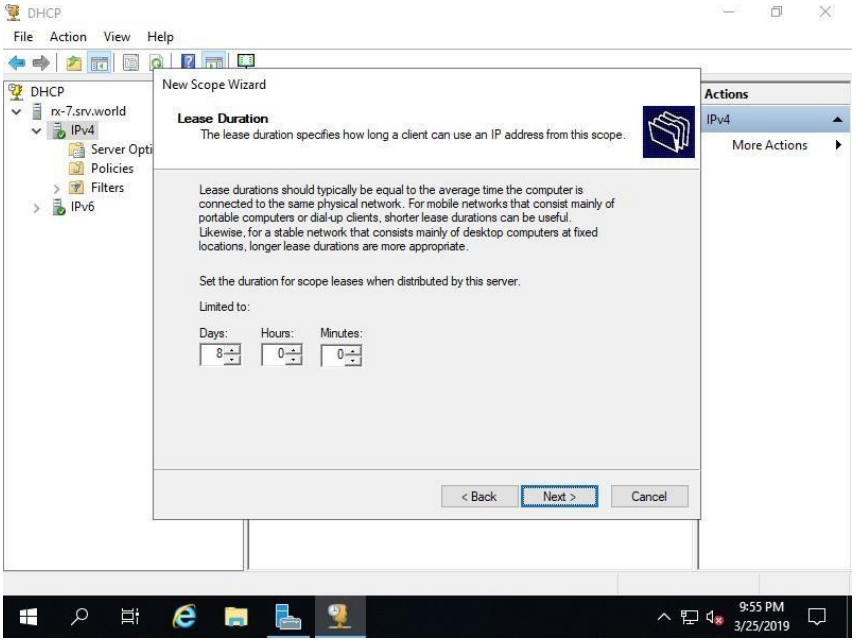
Trong hộp thoại Add Exclusions, cho biết những địa chỉ nào sẽ được loại ra khỏi nhóm địa chỉ đã chỉ định ở trên. Các địa chỉ loại ra này được dùng để đặt cho các máy tính dùng địa chỉ tĩnh hoặc dùng để dành cho mục đích nào đó. Để

loại một địa chỉ duy nhất, chỉ cần cho biết địa chỉ trong ô Start IP Address và nhấn Add. Để loại một nhóm các địa chỉ, cho biết địa chỉ bắt đầu và kết thúc của nhóm đó trong Start IP Address và Stop IP Address, sau đó nhấn Add. Nút Remove dùng để huỷ một hoặc một nhóm các địa chỉ ra khỏi danh sách trên. Sau khi đã cấu hình xong, nhấn nút Next để tiếp tục.



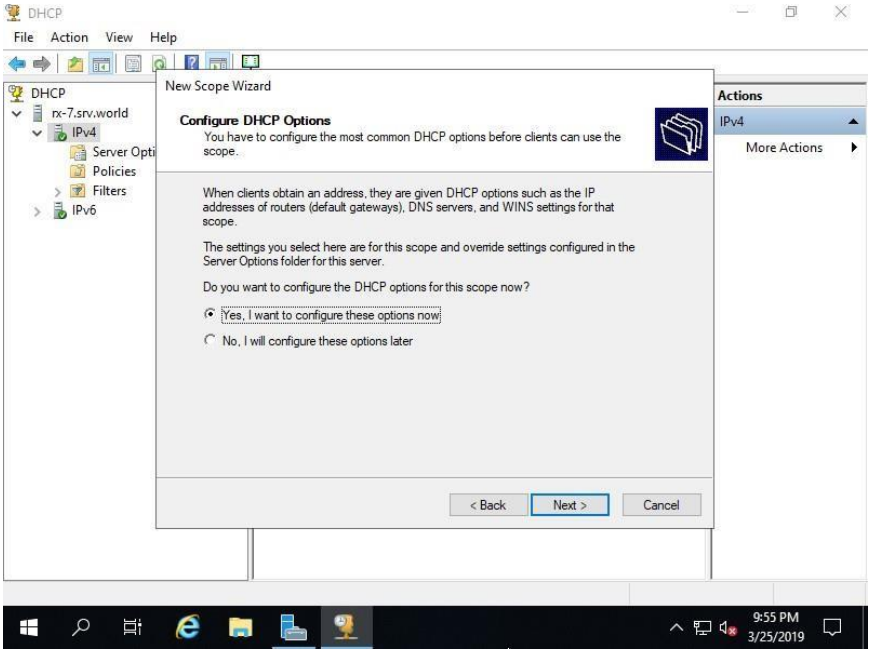
Hình 7.21 Loại trừ những IP không được cấp cho host

Trong hộp thoại Lease Duration tiếp theo, cho biết thời gian các máy trạm có thể sử dụng địa chỉ này. Theo mặc định, một máy Client sẽ cố làm mới lại địa chỉ khi đã sử dụng được phân nửa thời gian cho phép. Lượng thời gian cho phép mặc định là 8 ngày. Có thể chỉ định lượng thời gian khác tuỳ theo nhu cầu. Sau khi đã cấu hình xong, nhấn Next để tiếp tục.



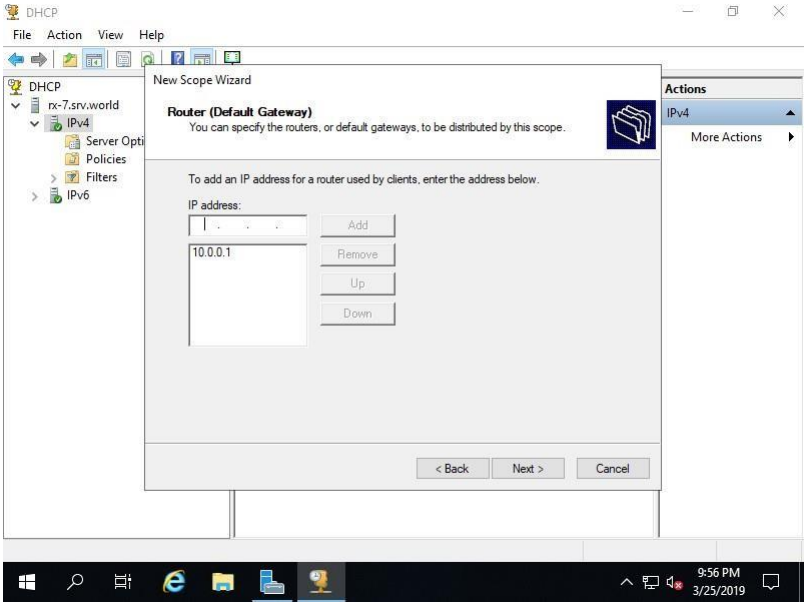
Hình 7.22 Cho biết thời gian các máy trạm có thể sử dụng địa chỉ này

Hộp thoại Configure DHCP Options xuất hiện. Có thể đồng ý để cấu hình các tuỳ chọn phổ biến (chọn Yes, I want to configure these options now) hoặc không đồng ý, để việc thiết lập này thực hiện sau (chọn No, I will configure these options later). Để mục chọn đồng ý và nhấn chọn Next



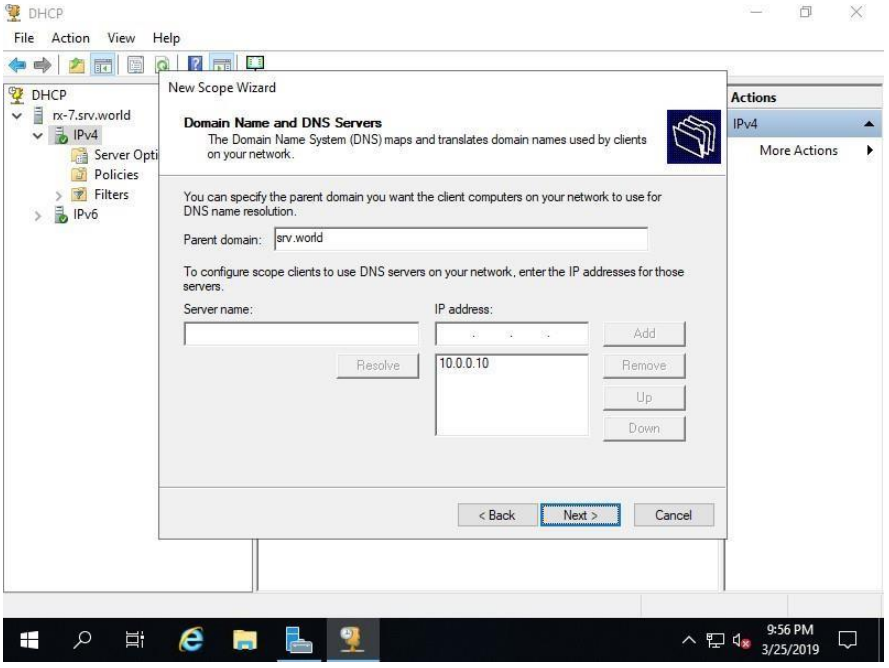
Hình 7.23 Lựa chọn cấu hình DHCP

Trong hộp thoại Router (Default Gateway), cho biết địa chỉ IP của default gateway mà các máy DHCP Client sẽ sử dụng và nhấn Add. Sau đó nhấn Next



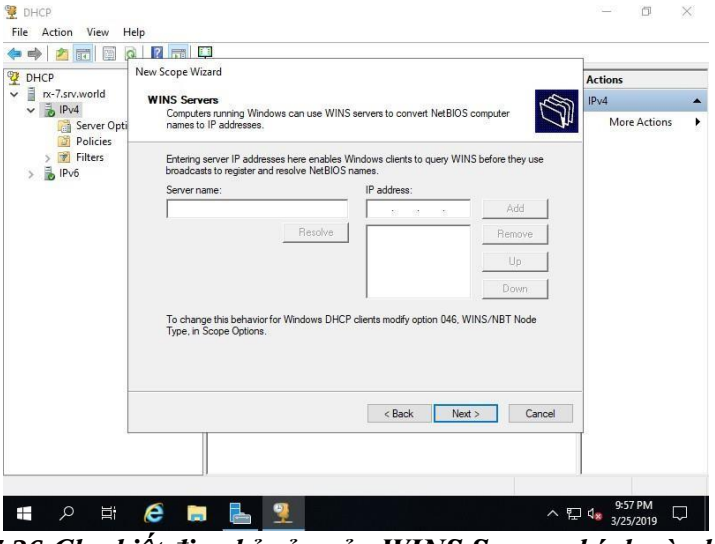
Hình 7.24 Cho biết địa chỉ IP của default gateway mà các máy DHCP Client sẽ sử dụng

Trong hộp thoại Domain Name and DNS Server, cho biết tên domain mà các máy DHCP client sẽ sử dụng, đồng thời cũng cho biết địa chỉ IP của DNS Server dùng phân giải tên. Sau khi đã cấu hình xong, nhấn Next để tiếp tục.



Hình 7.25 Cho biết tên domain mà các máy DHCP client sẽ sử dụng, đồng thời cũng cho biết địa chỉ IP của DNS Server dùng phân giải

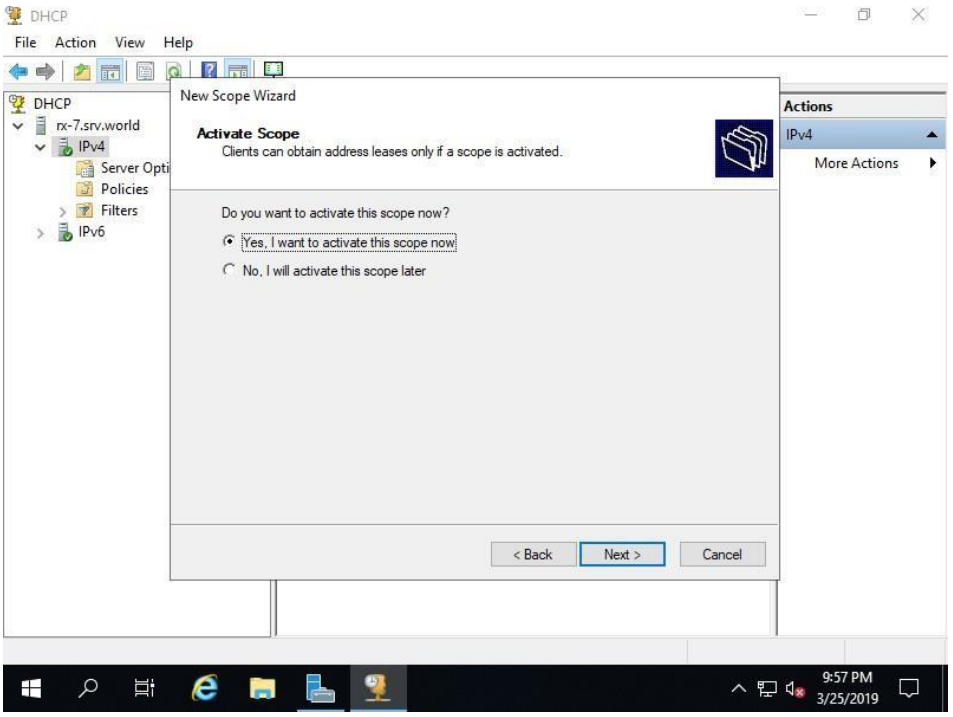
Trong hộp thoại WINS SERVER tiếp theo, cho biết địa chỉ của của WINS Server chính và phụ dùng phân giải các tên NetBIOS thành địa chỉ IP. Sau đó nhấn chọn Next. (Hiện nay dịch vụ WINS ít được sử dụng, do đó có thể bỏ qua bước này, không nhập thông tin gì hết.)



Hình 7.26 Cho biết địa chỉ của của WINS Server chính và phụ dùng phân giải các tên NetBIOS thành địa chỉ IP

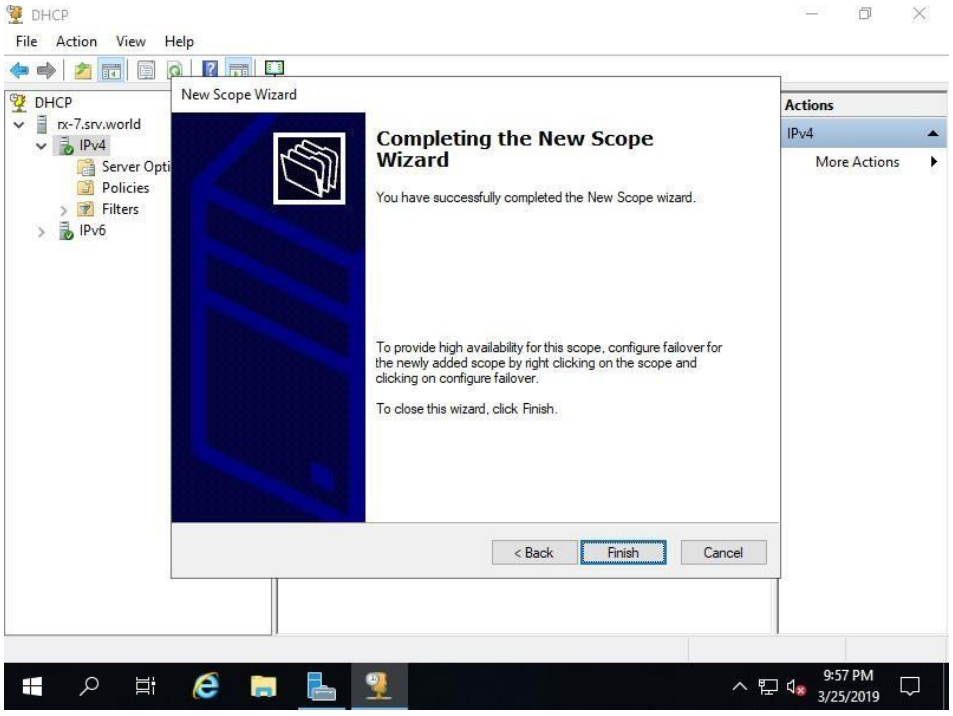
Tiếp theo, hộp thoại Activate Scope xuất hiện, hỏi có muốn kích hoạt scope này hay không. Scope chỉ có thể cấp địa chỉ cho các máy Client khi được kích

hoạt. Nếu định cấu hình thêm các thông tin tuỳ chọn cho scope thì chưa nên kích hoạt bây giờ. Sau khi đã lựa chọn xong, nhấn chọn Next



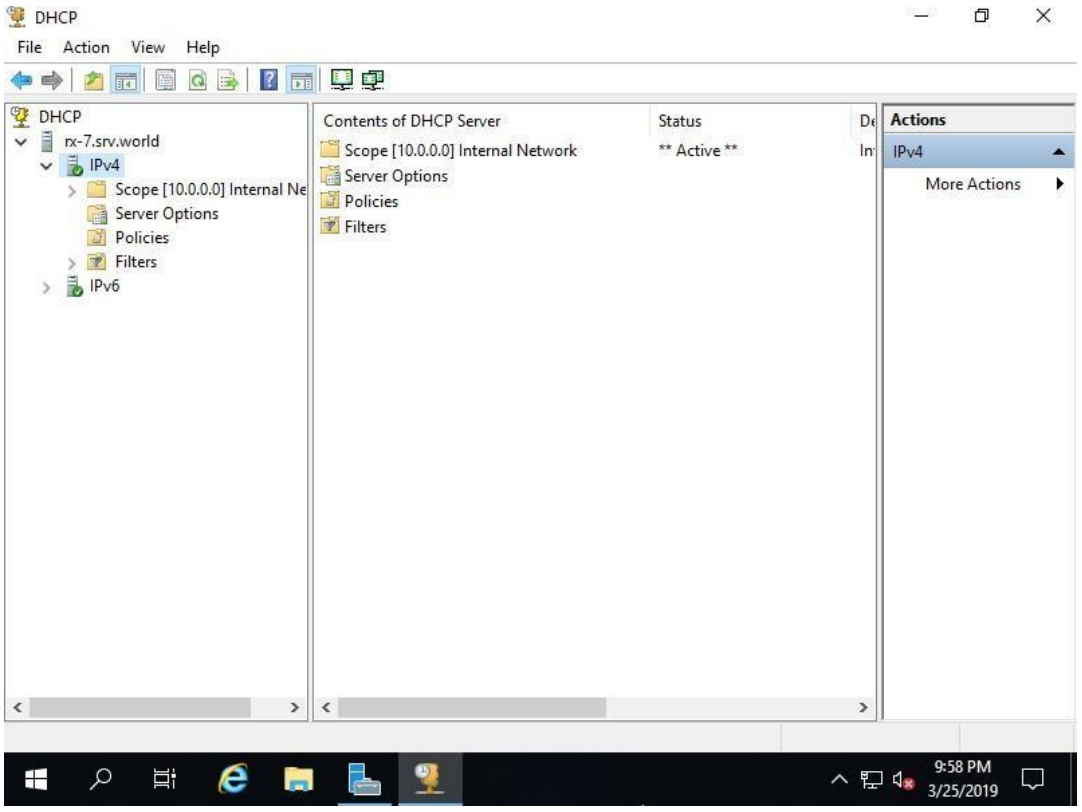
Hình 7.27 Kích hoạt scope

- Trong hộp thoại Complete the New Scope Wizard, nhấn chọn Finish để kết thúc.



Hình 7.28 Hoàn tất cấu hình

- DHCP Scope mới đã được thêm vào



Hình 7.29 Kết quả sau khi cấu hình

6. Cấu hình các tuỳ chọn DHCP

Các tuỳ chọn DHCP là các thông tin phụ gửi kèm theo địa chỉ IP khi cấp phát cho các máy Client. Có thể chỉ định các tuỳ chọn ở hai mức độ: scope và Server. Các tuỳ chọn mức scope chỉ áp dụng cho riêng scope đó, còn các tuỳ chọn mức Server sẽ áp đặt cho tất cả các scope trên toàn Server. Tuỳ chọn mức scope sẽ che phủ tuỳ chọn mức server cùng loại nếu có. Các bước thực hiện: Chọn menu Start / Programs / Administrative Tools / DHCP. Trong cửa sổ DHCP, ở ô bên trái, mở rộng mục Server để tìm Server Options hoặc mở rộng một scope nào đó để tìm Scope Options. Nhấn phải chuột lên mục tuỳ chọn tương ứng và chọn Configure Options. Hộp thoại cấu hình các tuỳ chọn xuất hiện (mức Server hoặc scope đều giống nhau). Trong mục Available Options, chọn loại tuỳ chọn bạn định cấp phát và nhập các thông cấu hình kèm theo. Sau khi đã chọn xong hoặc chỉnh sửa các tuỳ chọn xong, nhấn OK để kết thúc.

7. Cấu hình dành riêng địa chỉ IP

Giả sử hệ thống mạng của sử dụng việc cấp phát địa chỉ động, tuy nhiên trong đó có một số máy tính bắt buộc phải sử dụng một địa chỉ IP cố định trong một thời gian dài. Có thể thực hiện được điều này bằng cách dành một địa chỉ IP cho riêng máy đó. Việc cấu hình này được thực hiện trên từng scope riêng biệt. Các bước thực hiện:

Chọn menu Start / Programs / Administrative Tools / DHCP.

Trong ô bên trái của cửa sổ DHCP, mở rộng đến scope định cấu hình, chọn mục Reservation, chọn menu Action / New Reservation. Xuất hiện hộp thoại New Reservation. Đặt tên cho mục dành riêng này trong ô Reservation Name, có thể là tên của máy tính được cấp địa chỉ đó.

Trong mục IP Address, nhập vào địa chỉ IP định cấp cho máy đó. Tiếp theo, trong mục MAC Address, nhập vào địa chỉ MAC của máy tính đó (là một chuỗi liên tục 12 ký số thập lục phân). Có thể ghi một dòng mô tả về địa chỉ vào mục Description. Supported Types có ý nghĩa:

DHCP only: chỉ cho phép máy client DHCP yêu cầu địa chỉ này bằng cách sử dụng giao thức DHCP.

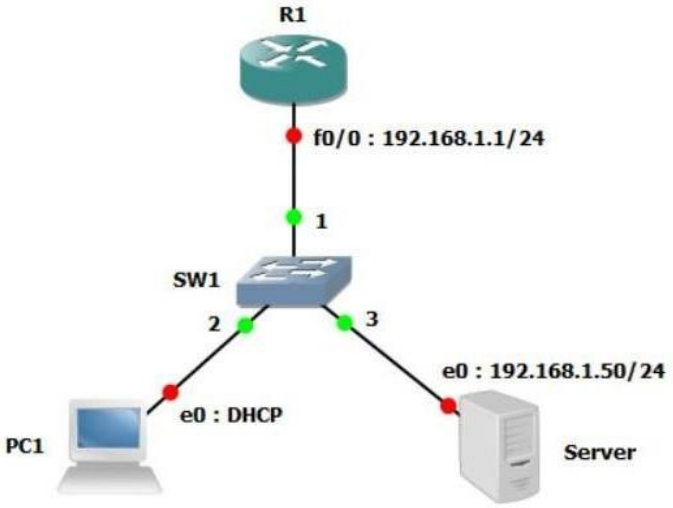
BOOTP only: chỉ cho phép máy client DHCP yêu cầu địa chỉ này bằng cách sử dụng giao thức BOOTP (là tiền thân của giao thức DHCP).

Both: máy client DHCP có thể dùng giao thức DHCP hoặc BOOTP để yêu cầu địa chỉ này. Lặp lại thao tác trên cho các địa chỉ dành riêng khác. Cuối cùng nhấn chọn Close.

CÂU HỎI VÀ BÀI TẬP BÀI 7

1. Cài đặt và cấu hình dịch vụ DHCP trên Window Server 2019

2. Cấu hình DHCP trên thiết bị router theo sơ đồ hình bên dưới



BÀI 8: QUẢN TRỊ MÁY IN

Mã bài: MĐ15 - 08

Giới thiệu:

Ngày nay, hầu hết các máy in đều được kết nối trực tiếp vào mạng, các cổng song song đã không còn tồn tại như trước kia. Khi phần cứng máy in thay đổi thì các tính năng quản lý máy in có trong máy chủ Windows cũng thay đổi theo. Mặc dù vậy không phải tất cả các thay đổi trong Windows đều do vấn đề phần cứng của máy in thay đổi mà sự thực Microsoft đã thực hiện một số thay đổi rất có giá trị để tạo sự dễ dàng hơn trong việc quản lý máy in. Họ đã thiết kế lại giao diện quản lý máy in nhằm giúp việc quản lý trở nên dễ hơn.

Trong bài 8 này sẽ hướng dẫn cách cài máy in và xử lý sự cố lỗi về máy in .

Mục tiêu:

- Mô tả về mô hình và thuật ngữ được sử dụng cho tác vụ in ấn trong Windows;
- Cài đặt một máy in logic trên một máy chủ in ấn;
- Chuẩn bị một máy chủ in ấn cho các máy trạm;
- Kết nối một máy trạm in ấn đến một máy in logic trên máy chủ in ấn;
- Quản trị hàng đợi in ấn và các đặc tính máy in;
- Xử lý sự cố các lỗi về máy in.

Nội dung chính:

1. Cài đặt máy in

Tính năng Plug and Play thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành Windows Server.

• Tiện ích Found New Hardware Wizard sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn từng bước để cài đặt máy in.

• Nếu hệ điều hành nhận diện không chính xác thì dùng đĩa CD được hãng sản xuất cung cấp kèm theo máy để cài đặt. Có thể tự cài đặt máy in bằng cách sử dụng tiện ích Add Printer Wizard.

*Phải đăng nhập vào hệ thống với vai trò là một thành viên của nhóm Administrators hay nhóm Power Users (trong trường hợp đây là một Server thành viên) hay nhóm Server Operators (trong trường hợp đây là một domain

controller) mới có thể cài đặt máy in (tạo ra một máy in logic) trong Windows Server.

Có thể tạo ra một máy in logic cục bộ tương ứng với một máy in vật lý được gắn trực tiếp vào máy tính cục bộ của mình hoặc tương ứng với một máy in mạng (máy in mạng được gắn vào một máy tính khác trong mạng hay một thiết bị Print Server).

Các bước thực hiện để cài đặt một máy in cục bộ hay một máy in mạng: Chọn Start -> Printers And Faxes. Chọn Add Printer, tiện ích Add Printer Wizard sẽ được khởi động. Chọn Next để tiếp tục. Hộp thoại Local Or Network Printer xuất hiện.

• Chọn tùy chọn Local Printer Attached To This Computer trong trường hợp bạn có một máy in vật lý gắn trực tiếp vào máy tính của mình, có thể chọn thêm tính năng Automatically Detect And Install My Plug And Play Printer.

• Chọn A Printer Attached To Another Computer nếu đang tạo ra một máy in logic ứng với một máy in mạng. Khi đã hoàn tất việc chọn lựa, chọn Next để tiếp tục. Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích Found New Hardware Wizard.

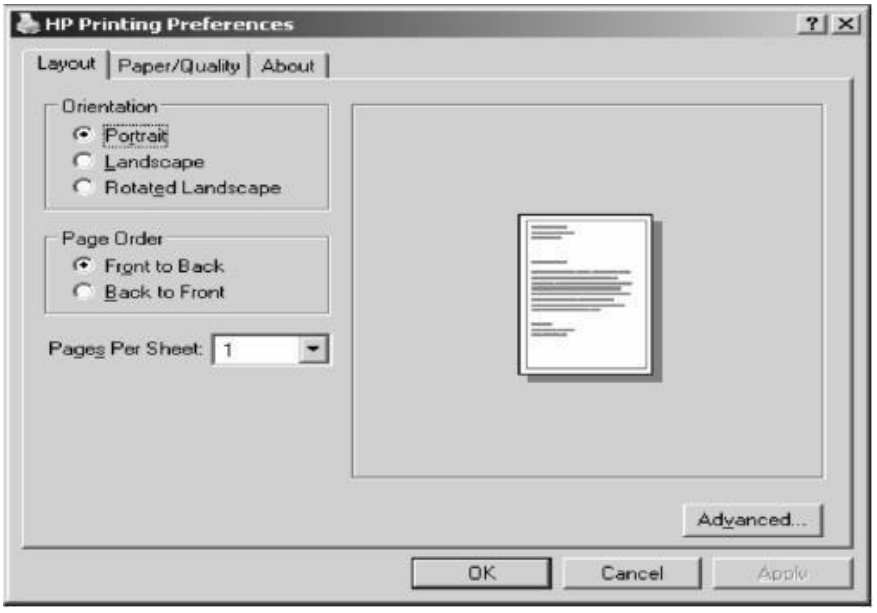
Tiện ích này sẽ hướng dẫn từng bước cài đặt driver máy in. Hộp thoại Print Test Page xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính thì nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, thì bỏ qua bước này. Chọn Next để tiếp tục.

Hộp thoại Completing The Add Printer Wizard hiện ra. Hộp thoại này xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Chọn Finish hoàn tất. Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ Printer And Faxes. Theo mặc định, máy in sẽ được chia sẻ.

2. Quản lý thuộc tính máy in

2.1. Cấu hình Layout

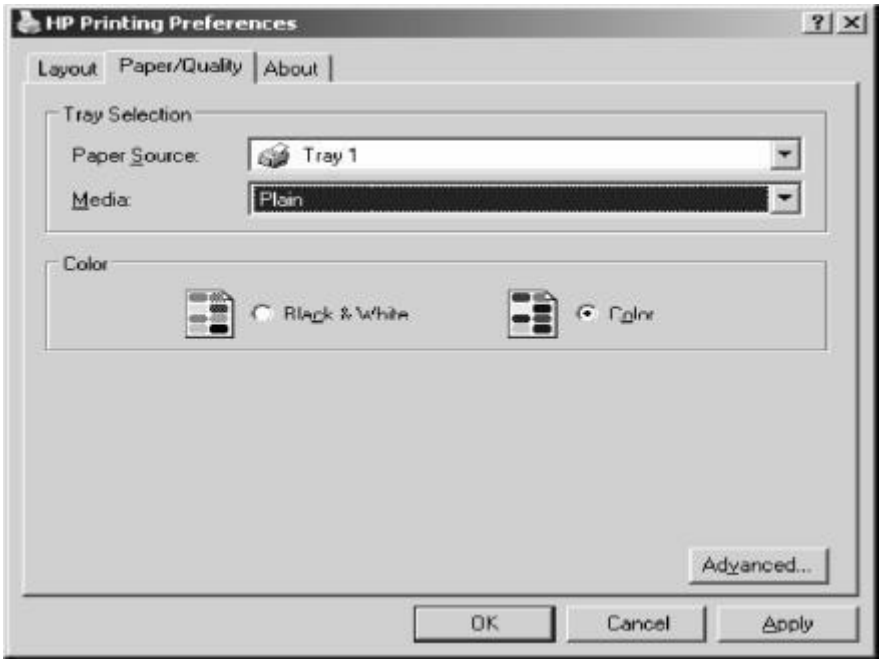
Trong hộp thoại Printing Preferences, chọn Tab Layout. Sau đó trong mục Orientation, bạn chọn cách thức in trang theo chiều ngang hay chiều dọc. Trong mục Page Order, bạn chọn in từ trang đầu đến trang cuối của tài liệu hoặc in theo thứ tự ngược lại. Trong mục Pages Per Sheet, bạn chọn số trang tài liệu sẽ được in trên một trang giấy.



Hình 8.1 Điều chỉnh trang in

2.2. Giấy và chất lượng in

Cũng trong hộp thoại Printing Preferences, để qui định giấy và chất lượng in, chúng ta chọn Tab Paper/Quality. Các tùy chọn trong Tab Paper/Quality phụ thuộc vào đặc tính của máy in. Ví dụ, máy in chỉ có thể cung cấp một tùy chọn là Paper Source. Còn đối với máy in HP OfficeJet Pro Cxi, chúng ta có các tùy chọn là: Paper Source, Media, Quality Settings và Color.



Hình 8.2 Chọn độ sắc nét và màu (nếu có) của máy in

2.3. Các thông số mở rộng

Nhấp chuột vào nút Advanced ở góc dưới bên phải của hộp thoại Printing Preferences. Hộp thoại Advanced Options xuất hiện cho phép bạn điều chỉnh các thông số mở rộng. Chúng ta có thể có các tùy chọn của máy in như: Paper/Output, Graphic, Document Options, và Printer Features. Các thông số mở rộng có trong hộp thoại Advanced Options phụ thuộc vào driver máy in mà bạn đang sử dụng.

Hình 8.3 Hộp thoại điều chỉnh thông số mở rộng của máy in

3. Cấu hình chia sẻ máy in

Nhấp phải chuột lên máy in, chọn Properties. Hộp thoại Properties xuất hiện, bạn chọn Tab Sharing.

Để chia sẻ máy in này cho nhiều người dùng, bạn nhấp chuột chọn Share this printer. Trong mục Share name, bạn nhập vào tên chia sẻ của máy in, tên này sẽ được nhìn thấy trên mạng. Bạn cũng có thể nhấp chọn mục List In The Directory để cho phép người dùng có thể tìm kiếm máy in thông qua Active Directory theo một vài thuộc tính đặc trưng nào đó.

Hình 8.4 Hộp thoại chia sẻ máy in

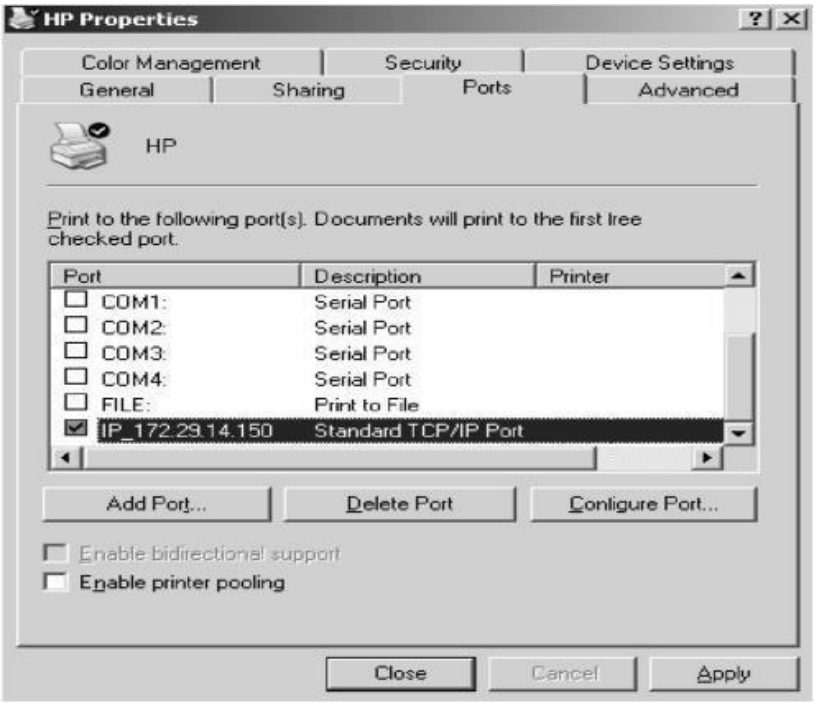
4. Cấu hình thông số Port

4.1. Cấu hình các thông số trong tab Port

Trong hộp thoại Properties, bạn chọn Tab Port để cấu hình tất cả các port đã được định nghĩa cho máy in sử dụng. Một port được định nghĩa như một interface sẽ cho phép máy tính giao tiếp với thiết bị máy in. Windows Server hỗ trợ các port vật lý (local port) và các port TCP/IP chuẩn (port logic).

Port vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính. Trong trường hợp Windows Server đang được triển khai trong một nhóm làm việc nhỏ, hầu như bạn phải gắn máy in vào port LPT1.

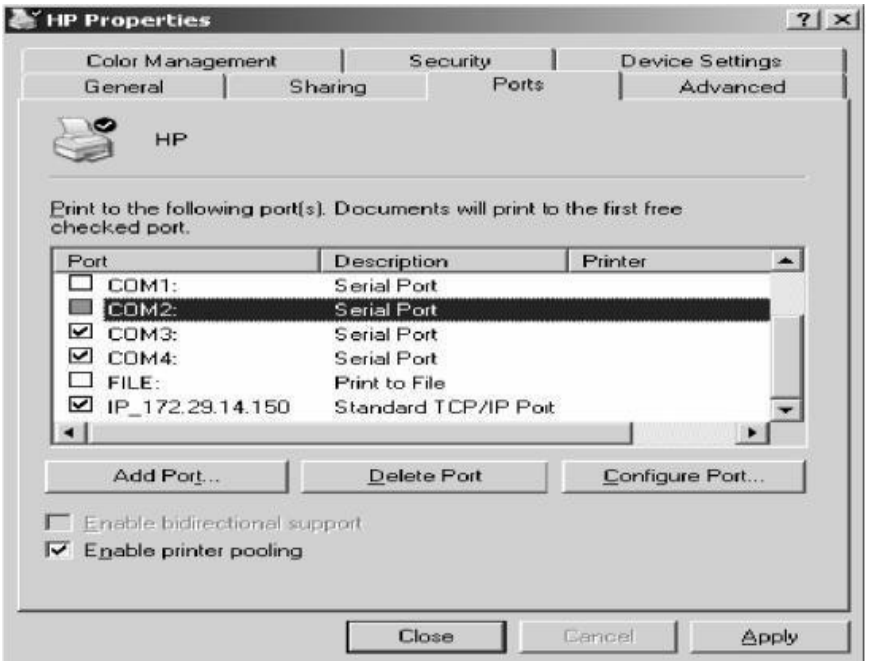
Port TCP/IP chuẩn được sử dụng khi máy in có thể kết nối trực tiếp vào mạng (trên máy in có hỗ trợ port RJ45) và máy in này có một địa chỉ IP để nhận dạng. Ưu điểm của máy in mạng là tốc độ in nhanh hơn máy in cục bộ và máy in có thể đặt bất kì nơi nào trong hệ thống mạng. Khi đó bạn cần chỉ định một port TCP/IP và khai báo địa chỉ IP của máy in mạng. Cùng với việc xoá và cấu hình lại một port đã tồn tại, bạn cũng có thể thiết lập printer pooling và điều hướng các công việc in ấn đến một máy in khác.



Hình 8.5 Hộp thoại cấu hình Port của máy in

4.2. Printer Pooling

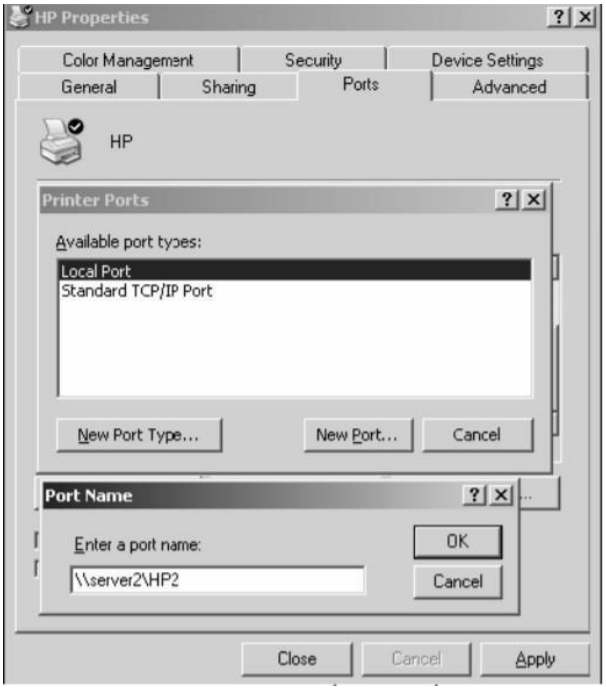
Để cấu hình một printer pool, bạn nhấp chuột vào tùy chọn Enable Printer Pooling nằm ở phía dưới Tab Port trong hộp thoại Properties. Sau đó, kiểm tra lại tất cả các port mà ta dự định gắn các máy in vật lý trong printer pool vào. Nếu ta không chọn tùy chọn Enable Printer Pool thì ta chỉ có một port duy nhất cho mỗi máy in. Chú ý tất cả các máy in vật lý trong một printer pool phải sử dụng cùng một driver máy in.



Hình 8.6 Hộp thoại bật chức năng Printer pool

4.3. Điều hướng tác vụ in đến một máy in khác

Nếu một máy in vật lý bị hư, có thể chuyển tất cả các tác vụ in ấn của máy in bị hư sang một máy in khác. Để làm được điều này, máy in mới phải có driver giống với máy in cũ.



Hình 8.7 Điều hướng tác vụ in đến máy in khác

Trong Tab Port, chọn Add Port, chọn Local port rồi chọn tiếp New Port. Hộp thoại Port Name xuất hiện, gõ vào tên UNC của máy in mới theo định dạng: \\computername\printer_sharename.

5. Cấu hình Tab Advanced

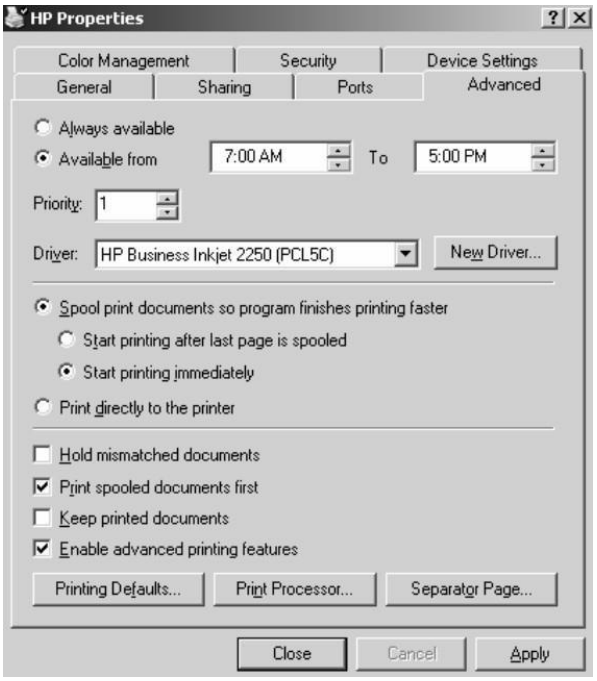
5.1. Các thông số của tab advanced

Trong hộp thoại **Properties**, bạn nhấp chuột vào **Tab Advanced** để điều khiển các đặc tính của máy in. Bạn có thể cấu hình các thuộc tính sau:

- Khả năng của máy in
- Độ ưu tiên của máy in
- Driver mà máy in sẽ sử dụng
- Các thuộc tính đồng tác (**spooling**) của máy in
- Cách thức in tài liệu theo biểu mẫu
- Chế độ in mặc định

- Sử dụng bộ xử lý in ấn nào

- Các trang độc lập



Hình 8.8 Tab Advanced

5.2. Độ ưu tiên

Khi đặt độ ưu tiên, chúng ta sẽ định ra bao nhiêu công việc sẽ được gửi trực tiếp vào thiết bị in.

Ví dụ: chúng ta có thể sử dụng tùy chọn này khi 2 nhóm người dùng cùng chia sẻ một máy in và bạn cần điều khiển độ ưu tiên đối với các thao tác in ấn trên thiết bị in này. Trong **Tab Advanced** của hộp thoại **Properties**, bạn sẽ đặt độ ưu tiên bằng các giá trị từ 1 đến 99, với 1 là có độ ưu tiên thấp nhất và 99 là có độ ưu tiên cao nhất.

Ví dụ: giả sử có một máy in được phòng kế toán sử dụng. Những người quản lý trong phòng kế toán luôn luôn muốn tài liệu của họ sẽ được ưu tiên in ra trước các nhân viên khác. Để cấu hình cho việc sắp xếp thứ tự này, ta tạo ra một máy in tên là **MANAGERS** gắn vào **port LPT1** với độ ưu tiên là 99.

Sau đó, cũng trên port **LPT1**, ta tạo thêm một máy in nữa tên là **WORKERS** với độ ưu tiên là 1. Sau đó, ta sẽ sử dụng **Tab Security** trong hộp thoại **Properties** để giới hạn quyền sử dụng máy in **MANAGERS** cho những người quản lý. Đối với các nhân viên còn lại trong phòng kế toán, ta cho phép họ sử dụng máy in. Khi các tác vụ in xuất phát từ máy in **MANAGERS**, nó sẽ đi vào hàng đợi của của máy in vật lý với độ ưu tiên cao hơn là các tác vụ xuất

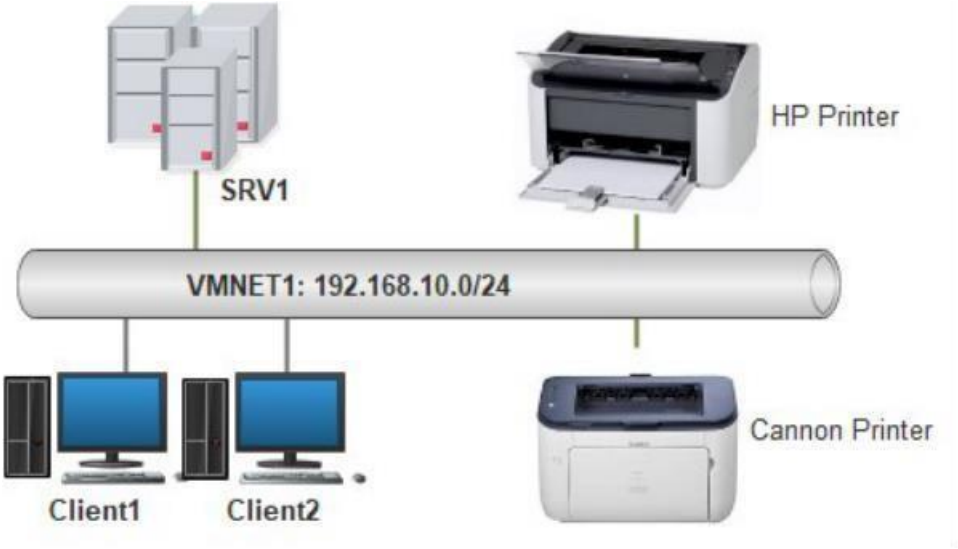
phát từ máy in **WORKERS**. Do đó, tài liệu của những người quản lý sẽ được ưu tiên in trước.

5.3. Print Driver

Mục **Drive**r trong **Tab Advanced** cho phép chỉ định driver sẽ dùng cho máy in. Nếu đã cấu hình nhiều máy in trên một máy tính thì bạn có thể chọn bất kì **driver** nào trong các **driver** đã cài đặt. Thao tác thực hiện như sau: Nhấp chuột vào nút **New Driver** để khởi động **Add Printer Driver Wizard**. **Add Printer Driver Wizard** cho phép thực hiện cập nhật cũng như thêm driver mới.

CÂU HỎI VÀ BÀI TẬP BÀI 8

Cho mô hình mạng sau:



Sử dụng dịch vụ Print Management với Group Policy để tự động cài đặt máy in và driver cho các User hoặc Computer .

BẢNG THUẬT NGỮ ANH - VIỆT

THUẬT NGỮ TIẾNG ANH	THUẬT NGỮ TIẾNG VIỆT
Access control entry	Kiểm soát hoạt động truy cập
Access control list	Danh sách điều khiển truy cập
Account	Tài khoản
Basic	Cơ bản
Built-in	Tạo sẵn
Caching	Lưu tạm
Disk management	Quản lý ổ đĩa
Domain controller	Bộ điều khiển miền
Domain name system	Hệ thống tên miền
Domain root	Gốc
Dynamic	Động
Groups	Nhóm
Iteractive query	Truy vấn tương tác
Local	Cục bộ
Mirrored	Tạo bản copy
Partition logic	Phân vùng ổ đĩa
Password	Mật khẩu
Permissions	Quyền truy cập
Port	Cổng
Properties	Thuộc tính

Recursive query	Truy vấn đệ quy
Replication	Nhân bản
Rights	Quyền hệ thống
Second-level domain	Tên miền cấp hai
Security identifier	Nhận diện bảo mật
Settings	Cấu hình
Spanned	Ghi uần tự
Storage	Lưu trữ
Striped	Ghi trên tất cả những ổ đĩa
Top-level domain	Tên miền cấp một
Upgrade	Nâng cấp
Users	Người dùng
Volume simple	Vùng không gian tương ứng
Windows server	Máy chủ windows

TÀI LIỆU THAM KHẢO

[1]. Hoàn Vũ và KS. Nguyễn Công Sơn (2004), "*Hướng Dẫn Quản Trị Mạng Microsoft Windows Server 2003",* Tổng Hợp TP. Hồ Chí Minh**.**

[2]. Nguyễn Thanh Quang và Hoàng Anh Quang (2006), "*Bảo Mật Và Quản Trị Mạng", Văn Hóa Thông Tin***.**

[3]. Phạm Hồng Tài (2002), "*Thủ Thuật Quản Trị Mạng Windows 2000", Thống kê***.**