TUYÊN BỐ BẢN QUYỀN

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Quản trị mạng máy tính đã được xây dựng trên cơ sở phân tích nghề, phần kỹ năng nghề được kết cấu theo các môđun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình theo các môđun đào tạo nghề là cấp thiết hiện nay.

Quản trị mạng1 là mô đun đào tạo chuyên môn nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu Quản trị mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế.

Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm!

Cần Thơ, ngày tháng năm 2021

Tham gia biên soạn

1. Chủ biên Nguyễn Hoàng Vũ

MỤC LỤC

TRANG

GIÁO TRÌNH MÔN HỌC/MÔ ĐUN

Tên môn học: QUẢN TRỊ MẠNG
Mã môn học/mô đun: MĐ17
Vị trí, tính chất, ý nghĩa và vai trò của môn học/mô đun:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong các môn học chung, trước các môn học, mô đun đào tạo cơ sở nghề.
- Tính chất: Là mô đun chuyên ngành đào tạo bắt buộc.
- Ý nghĩa và vai trò của môn học/mô đun: Thực hành tại doanh nghiệp là một môn học quan trọng trong chương trình đào, thông qua việc thực hành tại doanh nghiệp theo chuyên đề sẽ giúp sinh viên áp dụng kiến thức về Quản trị mạng đã học vào thực tế cũng như tiếp cận với thực tiễn về công nghệ mới

Mục tiêu của môn học/mô đun:

- Về kiến thức:
  + Mô tả về Windows Server 2019.
  + Trình bày cấu trúc, yêu cầu phần cứng của Windows Server.
  + Phân biệt sự khác nhau trong việc quản trị máy chủ (Server) và máy trạm (workstation).
  + Trình bày Quản lý tài khoản người dùng, nhóm và sắp xếp hệ thống hoá các tác vụ quản trị tài khoản người dùng và tài khoản nhóm
  + Trình bày các bước chia sẻ và cấp quyền truy cập tài nguyên dùng chung
  + Trình bày các bước cấu hình và quản trị in ấn của một máy phục vụ in mạng
  + Trình bày các bước cài đặt và cấu hình các dịch vụ mạng: Active Directory, DNS, DHCP.
- Về kỹ năng:
  + Cài đặt được hệ điều hành server 2019
  + Nâng cấp được máy chủ lên domain;
  + Quản trị tài nguyên mạng
  + Tạo được tài khoản người dùng, tài khoản nhóm
  + Quản lý tài khoản người dùng, nhóm và sắp xếp hệ thống hoá các tác vụ quản trị tài khoản người dùng và tài khoản nhóm
  + Chia sẻ và cấp quyền truy cập tài nguyên dùng chung
  + Lập cấu hình và quản trị in ấn của một máy phục vụ in mạng
  + Cài đặt và cấu hình các dịch vụ mạng: Active Directory, DNS, DHCP.
- Về năng lực tự chủ và trách nhiệm:
  + Có sáng kiến, tìm tòi, khám phá trong quá trình học tập và công việc
  + Có khả năng tự định hướng, chọn lựa phương pháp tiếp cận thích nghi với các bài học
  + Có năng lực đánh giá kết quả học tập và nghiên cứu của mình
  + Tự học tập, tích lũy kiến thức, kinh nghiệm để nâng cao trình độ chuyên môn

Nội dung của môn học/mô đun:

Số TT	Tên các bài trong mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
1	Bài 1: Tổng quan về Windows Server	4	2	2	
2	Bài 2: Dịch vụ tên miền (DNS)	4	2	2	
3	Bài 3: Dịch vụ thư mục (Active Directory)	8	4	4	
4	Bài 4: Quản lý người dùng và quản lý nhóm	8	4	3	
5	Bài 5: Quản lý đĩa và dữ liệu	8	4	4	1
6	Bài 6: Tạo và quản lý thư mục dùng chung	8	4	4	
7	Bài 7: Chính sách bảo mật	8	4	3	1
8	Bài 8: Cài đặt và quản trị dịch vụ DHCP	8	4	4	
9	Bài 9: Quản lý in ấn	4	2	1	1
	Tổng cộng	**60**	**30**	**27**	**3**

Bài 1: TỔNG QUAN VỀ WINDOWS SERVER
Mã bài: MĐ 17 - 01

Giới thiệu:

Bài này sẽ giới thiệu cho bạn các phiên bản của hệ điều hành Windows Server, yêu cầu phần cứng tối thiểu để cài đặt hệ điều hành này và các bước cài đặt Windows Server trên một máy tính.

Mục tiêu:

- Phân biệt được về họ hệ điều hành Windows Server;
- Cài đặt được hệ điều hành Windows Server.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Tổng quan về hệ điều hành windows server

Mục tiêu:

- Phân biệt được về họ hệ điều hành Windows Server

Windows Server 2019 là phiên bản mới nhất của hệ điều hành máy chủ do Microsoft phát hành. Windows Server 2019 được phát hành vào tháng 10 năm 2018. Được Microsoft xây dựng dựa trên nền tảng của phiên bản trước là Windows Server 2016. Những chức năng của phiên bản Windows Server 2019 đem đến nhiều cơ hội mới khi nhắc đến môi trường đám mây lai, bảo mật, lưu trữ và quản trị.

Windows Server 2019 gồm có ba phiên bản: Essentials, Standard và Datacenter. Giống như gọi, mỗi phiên bản được thiết kế để phục vụ cho các tổ chức quy mô khác nhau. Với yêu cầu ảo hóa và trung tâm dữ liệu khác nhau. Windows Server 2019 Essentials phù hợp cho nhu cầu của một cơ sở hạ tầng nhỏ. Windows Server 2019 Datacenter cung cấp phạm vi chức năng rộng nhất so với tất cả những hệ điều hành máy chủ khác của Microsoft.

Những tính năng mới của Windows Server 2019:

• Tính năng cơ sở hạ tầng siêu hội tụ cho cấp doanh nghiệp

Microsoft mất 3 năm cập nhật cho nền tảng cơ sở hạ tầng siêu hội tụ để phát hành Windows Server 2019. Vì hiện tại Microsoft đang sử dụng là lịch nâng cấp dần của Semi-Annual Channel giúp nâng cấp gia tăng cho đến lúc khả dụng.

Sau đó, cứ vài năm một lần, chúng lại tạo ra bản chính và được gọi là Long-Term Servicing Channel. Bản cập nhật chính này sẽ bao gồm bản phát hành trước đó và bản nâng cấp. Trong phiên bản mới nhất này, cơ sở siêu hội tụ sẽ được cung cấp trên một tập hợp các thành phần đi kèm với giấy phép máy chủ. Nó chính là "xương sống" của máy chủ, đặc biệt là đối với máy chủ chạy Hyper-V, nó cho phép tăng hoặc giảm khả năng thực hiện công việc mà không có thời gian chết.

• Giao diện đồ họa người dùng được cải thiện

Nhiều doanh nghiệp khi triển khai phiên bản Semi-Annual Channel của Windows Server 2016 như thiếu GUI. Chắc hẳn sẽ nhận nhiều bất ngờ khi cập nhật lên phiên bản 2019. Với bản phát hành Windows Server 2019, những chuyên gia công nghệ thông tin sẽ có giao diện đồ họa cho Windows Server.

• Công cụ quản lý máy chủ

Công cụ quản lý máy chủ Project Honolulu được chính thức phát hành khi phiên bản Windows Server 2019 đến tay người dùng. Project Honolulu là giao diện điều khiển trung tâm cho phép thực hiện việc quản lý các máy chủ không có giao diện và có giao

diện trong môi trường của họ. Việc này giúp quản trị viên dễ dàng trong việc quản lý hệ thống máy chủ của mình.

• Những cải tiến về bảo mật

Trong phiên bản Windows Server 2019, Microsoft tiếp tục cập nhật thêm các chức năng bảo mật. Giúp các tổ chức giải quyết ổn thỏa, hợp lý mô hình quản lý bảo mật của mình. Phiên bản 2019 tích hợp tính năng ATP, giúp đánh giá các vectơ chung cho những vi phạm an ninh. Tự động đăng nhập, chặn và cảnh báo cuộc tấn công nguy hiểm tiềm tàng. Ngoài ra, Windows Server 2019 cho phép các chuyên gia tận dụng tối đa những lợi thế của cơ sở dữ liệu, truyền tải mạng và các thành phần bảo mật an toàn,…Với mục đích ngăn chặn các sự xâm nhập vào hệ thống máy chủ hiện hành.

• Container hiệu quả hơn

Giảm thiểu tối đa những chi phí hoạt động công nghệ thông tin và loại bỏ nhiều máy chủ cồng kềnh bằng các Container hiệu quả hơn, nhỏ gọn hơn. Trong bản Windows Server 2019, Container nhỏ gọn hơn trước nhiều và giảm chi phí VPS từ 50 đến 80%. Bằng cách sử dụng mật độ tính toán cao hơn nhằm cải thiện các hoạt động của ứng dụng tổng, mà không tốn thêm chi phí cho các hệ thống máy chủ hay mở rộng dung lượng của phần cứng.

Những tính năng mới trong phiên bản Windows Server 2019 đã có những cải tiến đáng kể phải không nào? Việc sử dụng Windows Server 2019 sẽ giúp bảo mật dữ liệu ổn định, an toàn hơn, nhanh chóng, tốc độ và tối ưu hơn trong một môi trường có nhịp độ nhanh như hiện nay.

Thông tin chi tiết phiên bản Windows Server 2019 Datacenter

Windows Server 2019 Datacenter phù hợp môi trường đám mây và các trung tâm dữ liệu ảo hóa. Nó cung cấp các chức năng của **Windows Server 2019 Standard** và không giới hạn. Các chuyên gia có thể tạo bất kỳ số lượng máy ảo nào, cộng với một **máy chủ Hyper-V** trên từng license. Vậy, phiên bản **Windows Server 2019 Datacenter** hỗ trợ không giới hạn số lượng **Container** và **Hyper-V**. Và thêm một số tính năng khác mà không một **Windows Server** nào khác có.

Tính năng mà chỉ phiên bản **Windows Server 2019 Datacenter** mới được cung cấp là bộ điều khiển mạng. Nó cho phép quản lý cơ sở hạ tầng tập trung, cung cấp các công cụ để theo dõi, định cấu hình, khắc phục những sự cố về môi trường **mạng ảo hóa** một cách tự động. Bộ điều khiển mạng còn có thể sử dụng để giúp bạn tự động hóa cấu hình mạng thay vì định cấu hình các dịch vụ mạng và các thiết bị theo phương pháp thủ công.

Hỗ trợ **Hyper-V** của **Host Guardian** là một tính năng khác chỉ có trong phiên bản **Windows Server 2019 Datacenter**. Nó sẽ cho bạn biết nếu doanh nghiệp hoặc hoster biết về các máy chủ Hyper-V trong môi trường FC. Hơn nữa, nó còn có thể giúp bạn thực hiện quản lý các khóa được yêu cầu để khởi động máy ảo được bảo vệ. Chế độ offline của **Host Guard** cũng cho phép các máy ảo được bảo vệ bật lên khi dịch vụ không thể đạt được, mặc dù chỉ trong trường hợp cài đặt bảo mật của máy chủ Hyper-V không bị thay đổi.

Đặc biệt là phiên bản **Windows Server 2019 Datacenter** cung cấp chức năng xây dựng cơ sở siêu hội tụ. Tính đến thời điểm hiện tại, nó được xem là một trong những giải pháp hiệu quả nhất. Có thể mở rộng để tạo một trung tâm dữ liệu được xác định bằng phần mềm (**software-defined data center**). Chức năng của cơ sở hạ tầng siêu hội tụ sẽ cho phép thực hiện hợp nhất các tài nguyên điện toán, kết nối mạng thành một cùm, lưu trữ. Đây chính là cách để giúp cải thiện hiệu suất, tiết kiệm chi phí.

Thông tin chi tiết phiên bản Windows Server 2019 Standard

Phiên bản **Windows Server 2019 Standard** được thiết kế cho các môi trường ảo hóa vật lý hay tối thiểu. Với số lượng người dùng tối đa, nó dựa trên **CAL** hoặc yêu cầu giấy phép để truy cập của khách hàng. Tóm lại, phiên bản **Windows Server 2019 Standard** cung cấp các chức năng Windows Server cốt lõi. Bao gồm nhưng không giới hạn ở chức năng của phiên bản Essentials.

Ở phiên bản **Windows Server 2019 Standard** sẽ cho phép các hoạt động lai trong môi trường **Azure**. Bạn có thể kiểm kê hoặc di chuyển dữ liệu, hay cài đặt bảo mật và cấu hình khác. Từ hệ thống cũ sang phiên bản Windows Server 2019 hoặc đám mây Azure.

Windows Server 2019 Standard cho phép tập trung chia sẻ tệp của công ty bằng cách đồng bộ hóa máy chủ file với Azure. Bên cạnh đó, tính linh hoạt và hiệu suất của máy chủ file cục bộ vẫn được giữ nguyên. Các ứng dụng đang chạy trong mạng cục bộ cũng có thể sử dụng nhiều cải tiến khác nhau trên đám mây như Trí tuệ nhân tạo hay **Internet of Things**.

Khi nhắc đến ảo hóa, **Windows Server 2019 Standard** gồm có quyền sử dụng cho cả hai OSE (môi trường hệ điều hành) hoặc VM trên mỗi license, cộng với 1 máy chủ Hyper-V. Trường hợp bạn cần thêm VM trong cơ sở hạ tầng của mình thì bạn phải mua thêm license bổ sung. Để so sánh, số lượng VM được hỗ trợ trong phiên bản Datacenter là không giới hạn.

Một điểm đáng chú ý nữa là phiên bản **Windows Server 2019 Standard** chỉ hỗ trợ tối đa Hyper-V. Số lượng Windows Container mà phiên bản này hỗ trợ là không giới hạn. Ngoài ra, có sự khác biệt liên quan đến các bản backup là chức năng cho phép sao chép giữa các máy chủ nhằm mục đích khắc phục thảm họa. Không giới hạn với phiên bản **Windows Server 2019 Datacenter,** trong khi volume có sẵn trong bản Standard giới hạn ở mức 2TB.

2. Chuẩn bị cài đặt windows server

Mục tiêu:

- Nêu được cấu hình phần cứng tối thiểu để cài đặt windows server 2019.

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	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)
Bộ nhớ	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: 32 GB Khuyến nghị: 50 GB hoặc lớn hơn

	Các thiết bị lưu trữ liên tục trên các server như ổ cứng không thể là PATA. Windows Server 2019 không cho phép dùng ATA/PATA/IDE/EIDE để khởi động các ổ đĩa, trang hoặc dữ liệu.
Ổ đĩa	Ổ DVD-ROM
Màn hình	Monitor Super VGA (1024 x 768) hoặc cao hơn
Thành phần khác	Bàn phím, Chuột của Microsoft hoặc thiết bị trỏ tương thích

2.2. Tương thích phần cứng

Một bước quan trọng trước khi nâng cấp hoặc cài đặt mới Server của bạn 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** chúng ta đang hoạt động tốt, các ứng dụng và dữ liệu quan trọng đều lưu trữ trên **Server** này, nhưng theo yêu cầu chúng ta phải nâng cấp hệ điều hành **Server** hiện tại thành **Windows Server 2019**. Chúng ta cần xem xét nên nâng cấp hệ điều hành đồng thời giữ lại các ứng dùng 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 bạn được giữ lại như: người dùng (**users**), cấu hình (**settings**), nhóm (**groups**), quyền hệ thống (**rights**), và quyền truy cập (**permissions**)…
- Với nâng cấp bạn không cần cài lại các ứng dụng, nhưng nếu có sự thay đổi lớn về đĩa cứng thì bạn cần backup dữ liệu trước khi nâng cấp.
- Trước khi nâng cấp bạn 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 như bạn 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 bạn nên tham khảo thêm thông tin hướng dẫn của **Microsoft.**

Các hệ điều hành cho phép nâng cấp thành **Windows Server 2019**:

- Windows Server 2016.

2.4. Phân chia ổ đĩa

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

- **Lượng không gian cần cấp phát:** bạn 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**, **Mirroreded** hoặc là **RAID-5**.
- **Tiện ích phân chia partition:** nếu bạn định chia **partition** trước khi cài đặt, bạn có thể sử dụng nhiều chương trình tiện ích khác nhau, chẳng hạn như **FDISK** hoặc **PowerQuest Partition Magic**. Có thể ban đầu bạn 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

Bạn 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

Bạn 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, chúng ta 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.

2.7. Chọn phương án kết nối mạng

2.7.1. Các giao thức kết nối mạng

Windows Server mặc định chỉ cài một giao thức **TCP/IP**, còn những giao thức còn lại như **IPX**, **AppleTalk** là những tùy chọn có thể cài đặt sau nếu cần thiết. Riêng giao thức **NetBEUI**, **Windows Server** không đưa vào trong các tùy chọn cài đặt mà chỉ cung cấp kèm theo đĩa **DVD-ROM** cài đặt.

3. Cài đặt windows server 2019

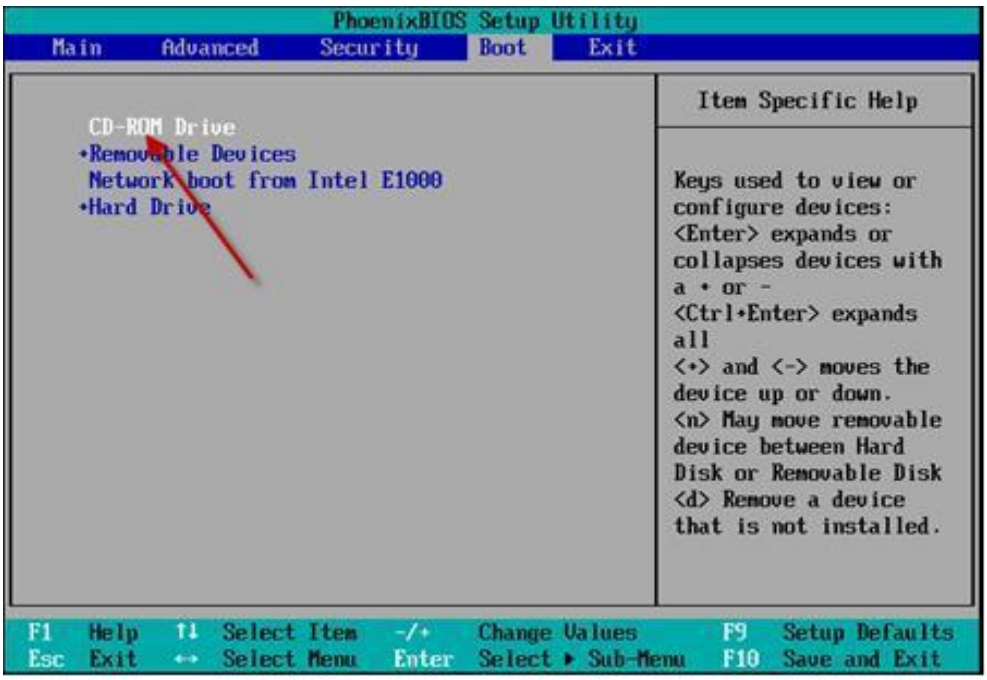
Mục tiêu:

- Cài đặt được windows server 2019.

3.1 Phương tiện cài đặt DVD

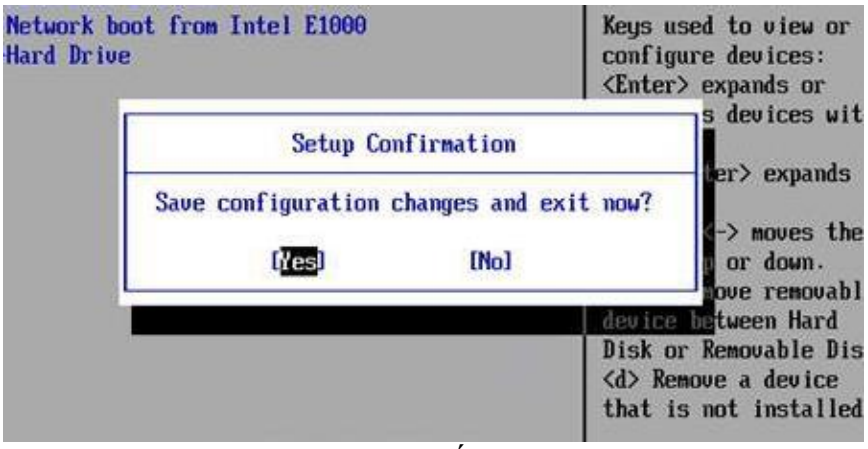
Bước 1: Cấu hình BIOS của máy tính để có thể khởi động từ ổ đĩa DVD-ROM

- Để thiết lập cho máy tính khởi động từ CD / DVD bạn khởi động máy tính và nhấn phím Del hoặc F2 tùy theo Mainboard máy tính của bạn (máy tính của tôi sử dụng phím F2).
- Sau khi vào **BIOS** bạn di chuyển đến thẻ boot và chọn boot từ CD/DVD như hình 1.1



Hình 1.1: Thiết lập máy tính khởi động từ ổ đĩa CD/DVD.

Bước 2: Sau khi hoàn tất bạn nhấn F10 để lưu cấu hình và thoát khỏi màn hình BIOS sau đó bạn khởi động lại máy tính.



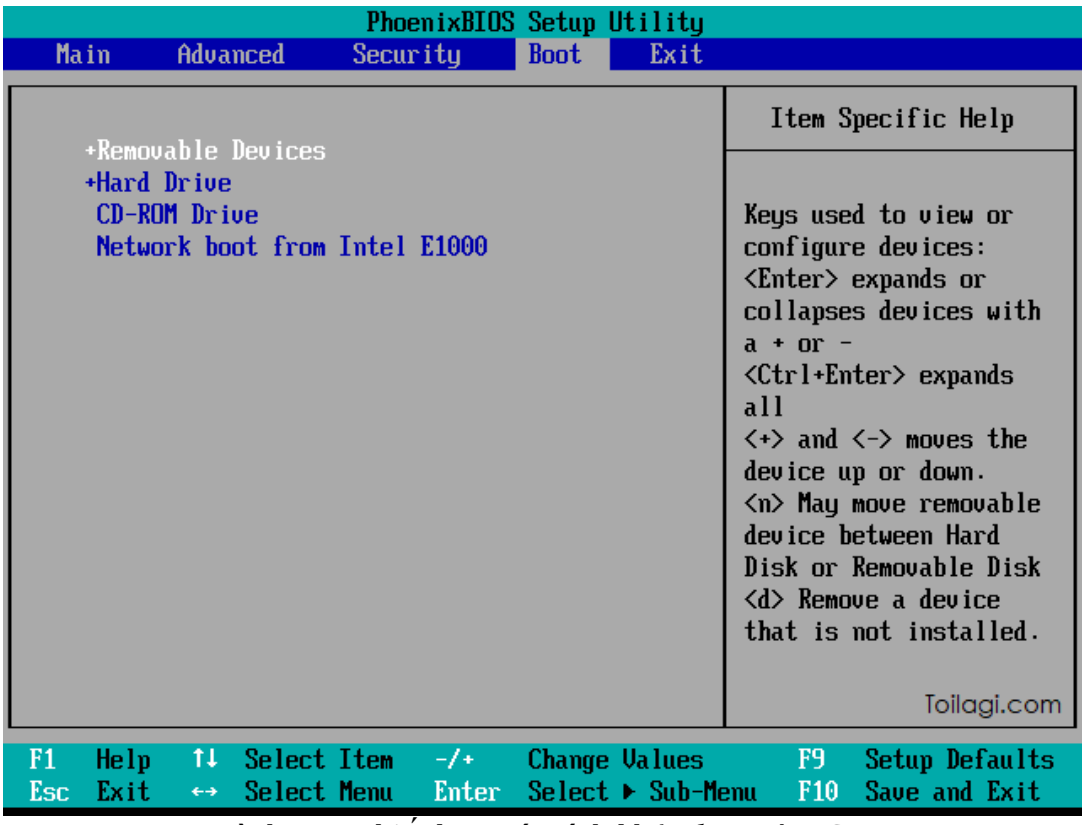
Hình 1.2: Lưu cấu hình BIOS.

Bước 3: Chèn đĩa cài đặt Windows 2019 Server vào ổ đĩa DVD-ROM và thực hiện các bước cài đặt.

3.3 Phương tiện cài đặt USB

Bước 1: Cấu hình BIOS của máy tính để có thể khởi động từ USB

- Để thiết lập cho máy tính khởi động từ CD / DVD bạn khởi động máy tính và nhấn phím Del hoặc F2 tùy theo Mainboard máy tính của bạn (máy tính của tôi sử dụng phím F2).
- Sau khi vào **BIOS** bạn di chuyển đến thẻ boot và chọn boot từ USB như hình 1.3



Hình 1.3: Thiết lập máy tính khởi động từ USB.

Bước 2: Sau khi hoàn tất bạn nhấn F10 để lưu cấu hình và thoát khỏi màn hình BIOS sau đó bạn khởi động lại máy tính.

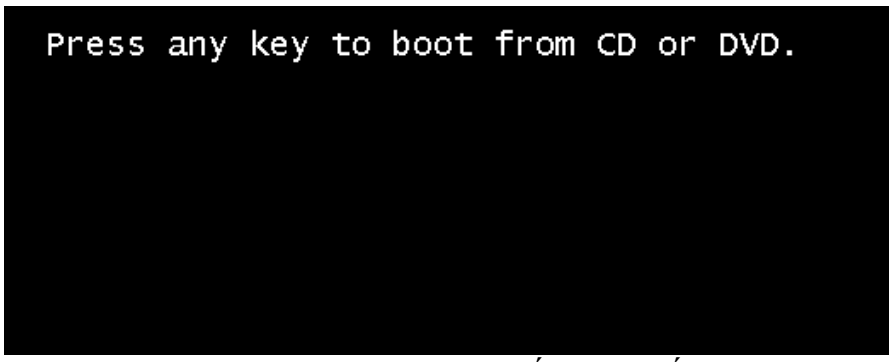
Hình 1.4: Lưu cấu hình BIOS.

Bước 3: Chèn USB cài đặt Windows 2019 Server vào ổ đĩa DVD-ROM và thực hiện các bước cài đặt.

3.3 Cài đặt windows server 2019

Bước 1: Nhấn phím để cài đặt

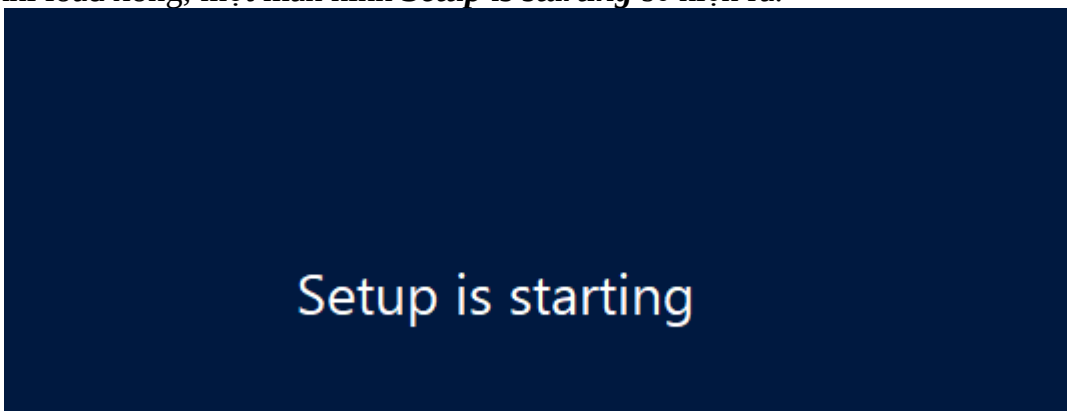
Khi máy khởi động từ phuong tiện cài đặt sẽ xuất hiện một thông báo “Press any key to continue…” yêu cầu nhấn một phím bất kỳ để bắt đầu quá trình cài đặt. Cửa sổ sẽ xuất hiện như sau:



Hình 1.5.Màn hình chờ nhấn phím bất kỳ.

Bước 2: Chờ Windows server 2019 load dữ liệu

Sau khi load xong, một màn hình ***Setup is starting*** sẽ hiện ra.



Hình 1.6. màn hình Setup is starting.

Bước 3: Chọn ngôn ngữ, múi giờ và bàn phím cho Windows server 2019:

+ **Language to Install**: Ngôn ngữ cài đặt.
+ **Time and currency format**: Định dạng ngày tháng và tiền tệ.
+ **Keyboard or input method**: Kiểu bàn phím bạn sử dụng.

- Sau khi bạn lựa chọn hoàn tất, click Next.

Hình 1.7: Lựa chọn ngôn ngữ, định dạng ngày tháng và kiểu bàn phím

Bước 4: Lựa chọn hình thức cài đặt

click nút **Install Now để cài đặt**

Hình 1.8: Install now

Bước 5: Xác định product key

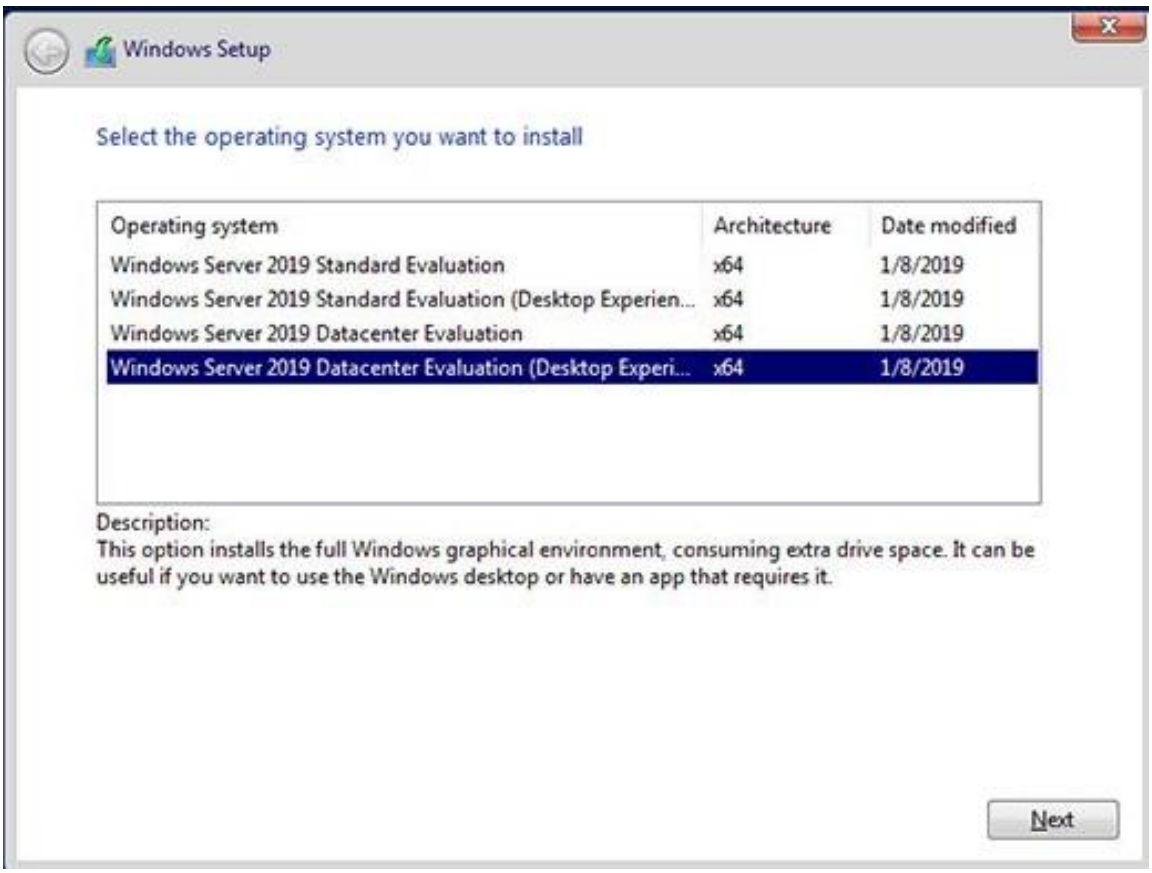
Tại khung **Type your product key for activation bạn** nhập key vào và click nút next để tiếp tục

.

Hình 1.9: Chờ nhập Product Key

Bước 6: Lựa chọn phiên bản **Windows Server 2019** muốn cài đặt.

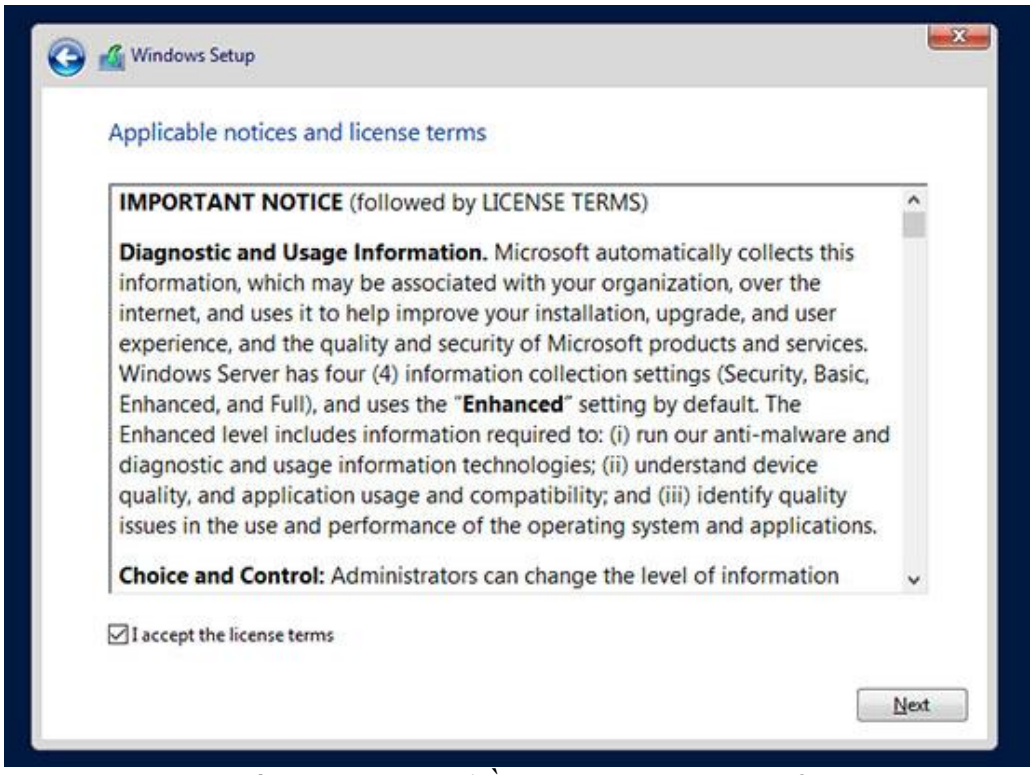
Tại khung các phiên bản **Windows Server 2019**, bạn chọn **Windows Server 2019** Enterprise (Full Installation) và **đánh dấu chọn** chọn I have selected the edition of Windows that I purchased. Click **Next** để tiếp tục.



Hình 1.10: Lựa chọn phiên bản cài đặt

Bước 7: Chấp nhận điều khoản của Microsoft

Tại bảng các điều khoản bạn click vào **I accept the license terms**, sau đó click **Next**.

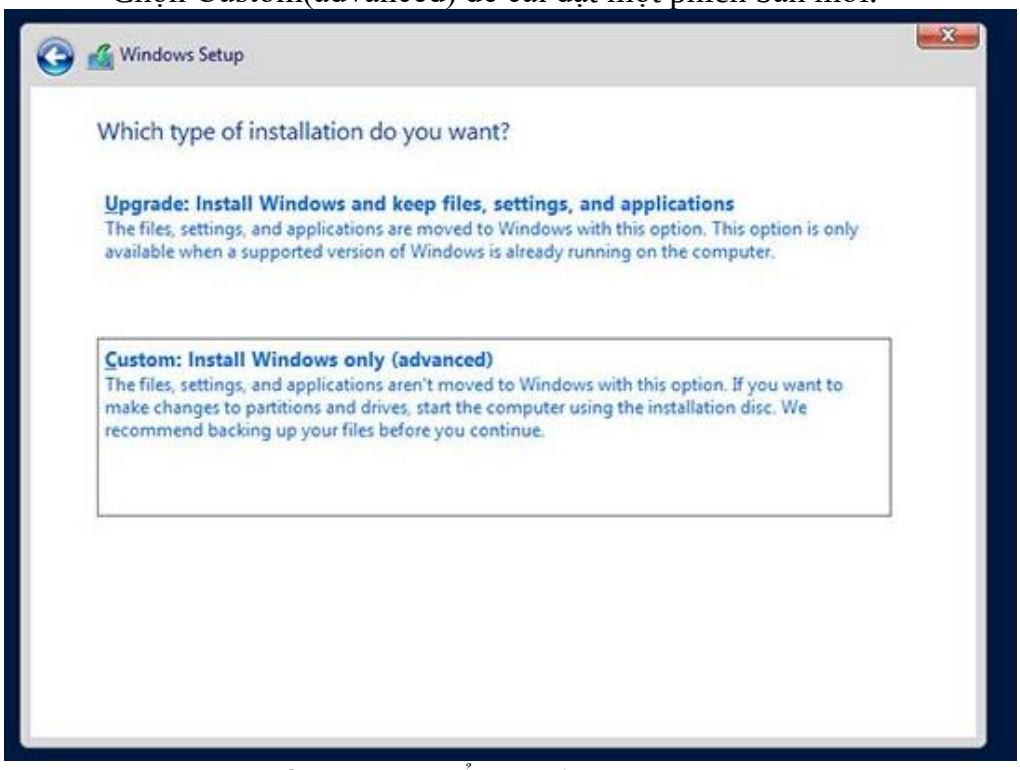


Hình 1.11: Các điều khoản của Microsoft

Bước 8: Lựa chọn các kiểu cài đặt thích hợp

- Chọn Upgrade nếu muốn nâng cấp

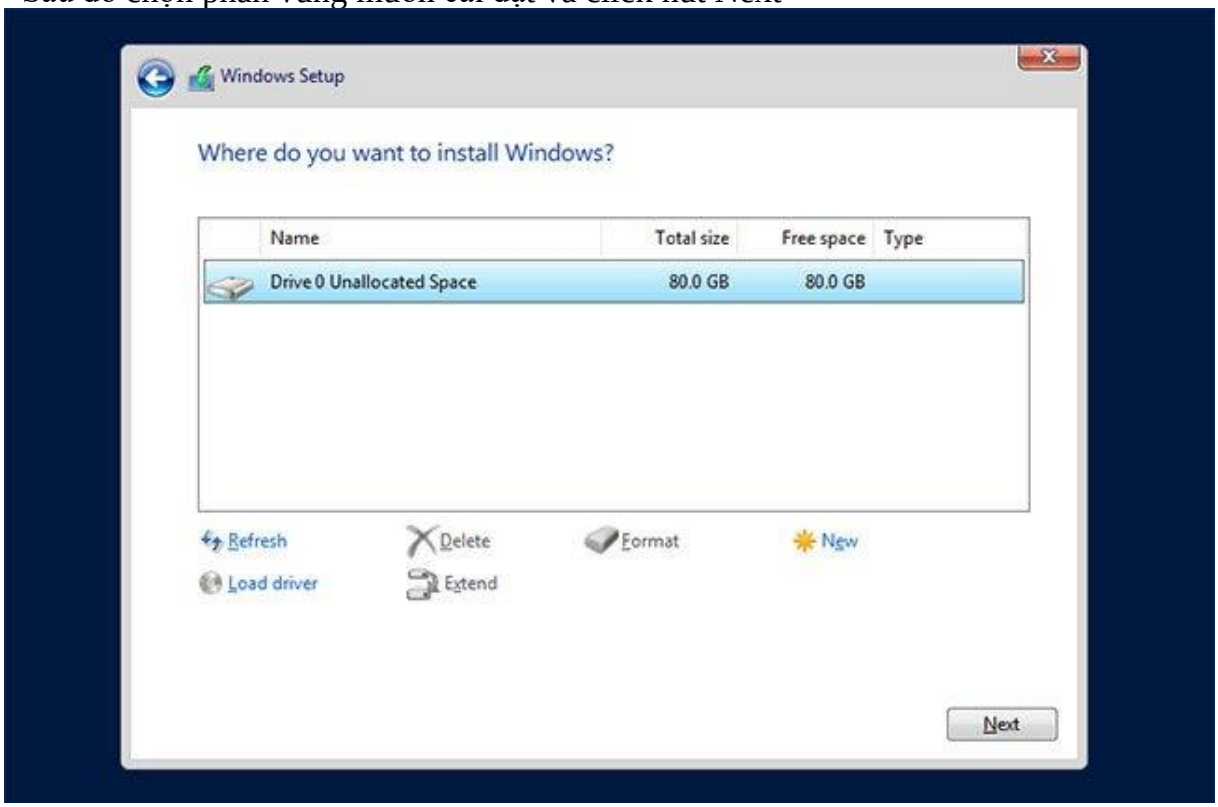
- Chọn Custom(advanced) để cài đặt một phiên bản mới.



Hình 1.12: Kiểu cài đặt của Windows server 2019

Bước 9: Chọn phân vùng cài đặt

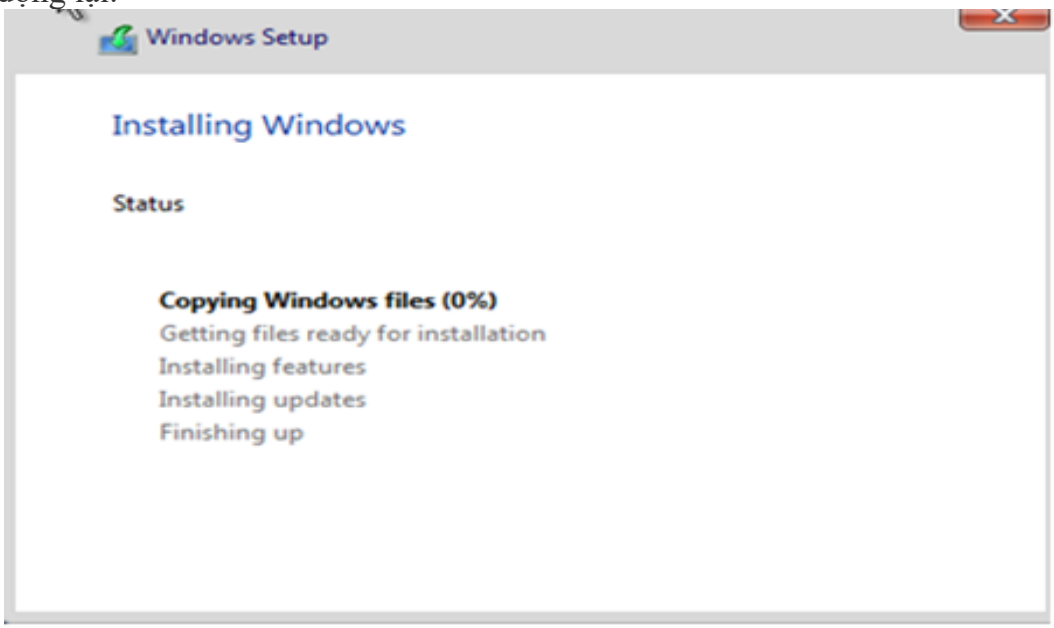
- Sau đó chọn Drive Option nếu muốn thao tác lên ổ đĩa cứng như New, Delete, Format…v.v…
- Sau đó chọn phân vùng muốn cài đặt và click nút Next



Hình 1.13: Lựa chọn các thao tác trên đĩa cứng

Bước 10: Chờ Windows Server 2019 cà đặt

Quá trình cài đặt Windows Server bắt đầu. Trong khi cài đặt, máy tính sẽ tự động khởi động lại.

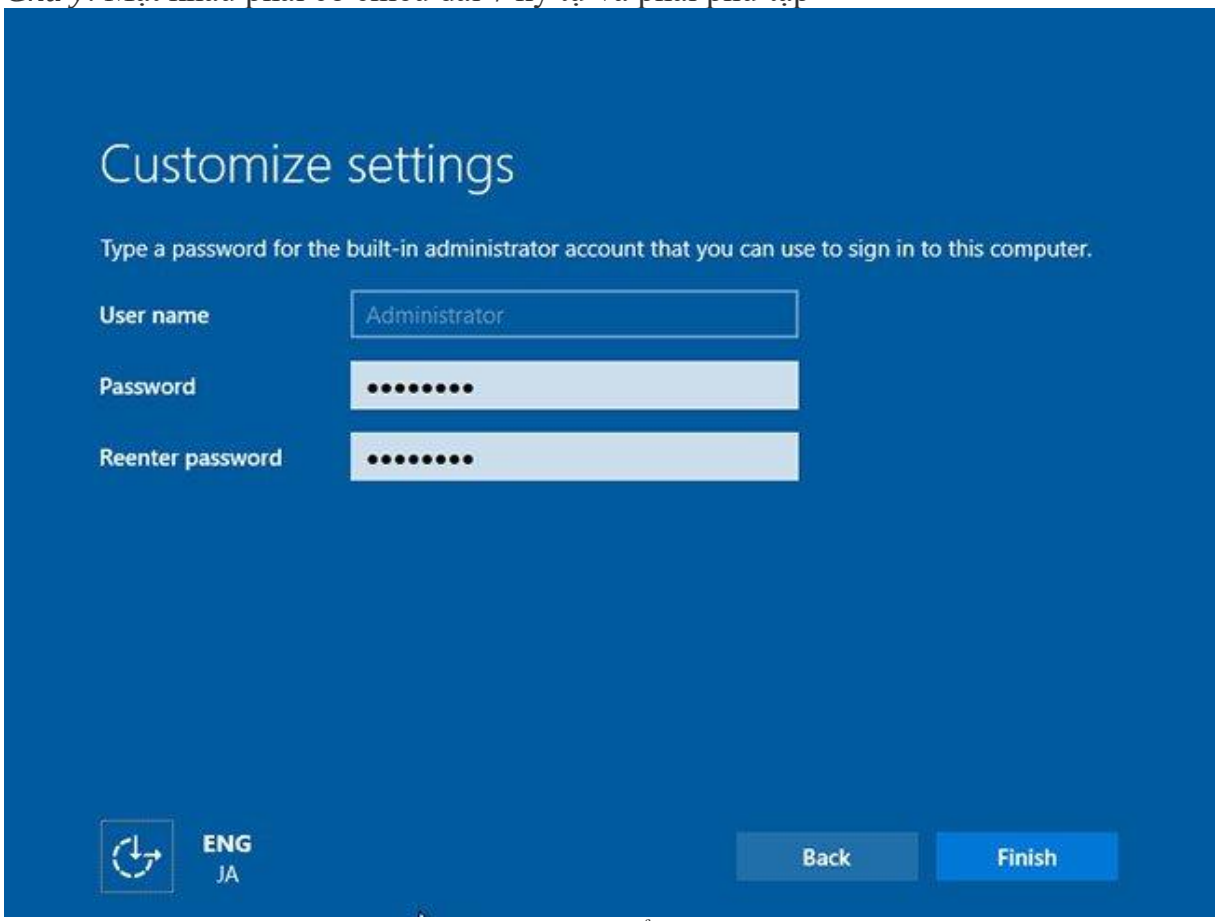


Hình 1.14 Quá trình cài đặt Windows Server 2019

Bước 11: Xác định mật khẩu cho Administrator

Đặt mật khẩu cho Administrator.

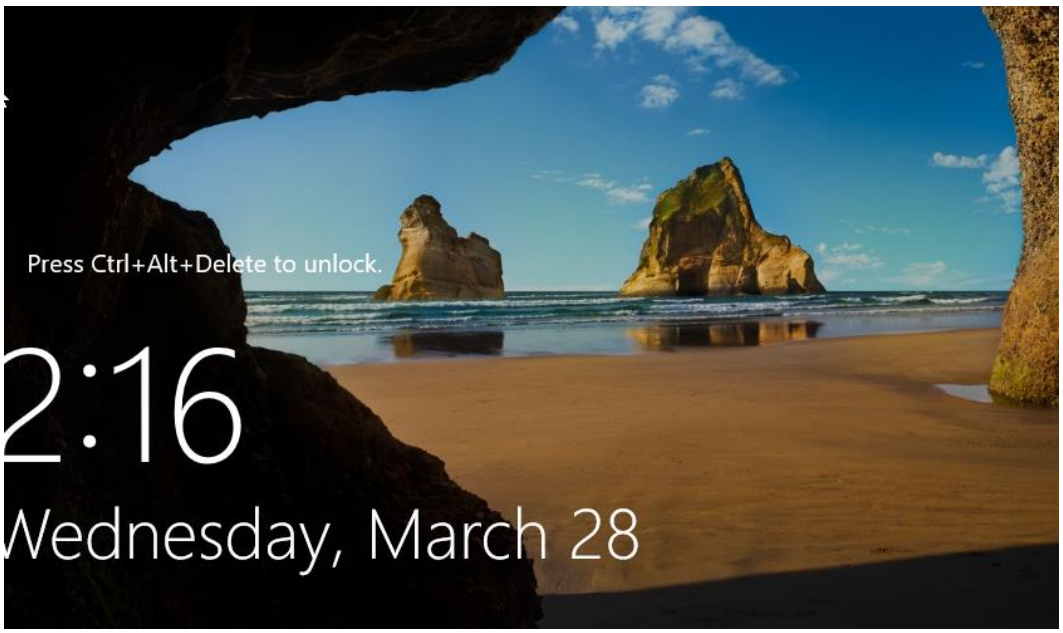
Chú ý: Mật khẩu phải có chiều dài 7 ký tự và phải phứ tạp



Hình 1.5 Đặt mật khẩu Administrator

Bước 12: Màn hình chờ đăng nhập

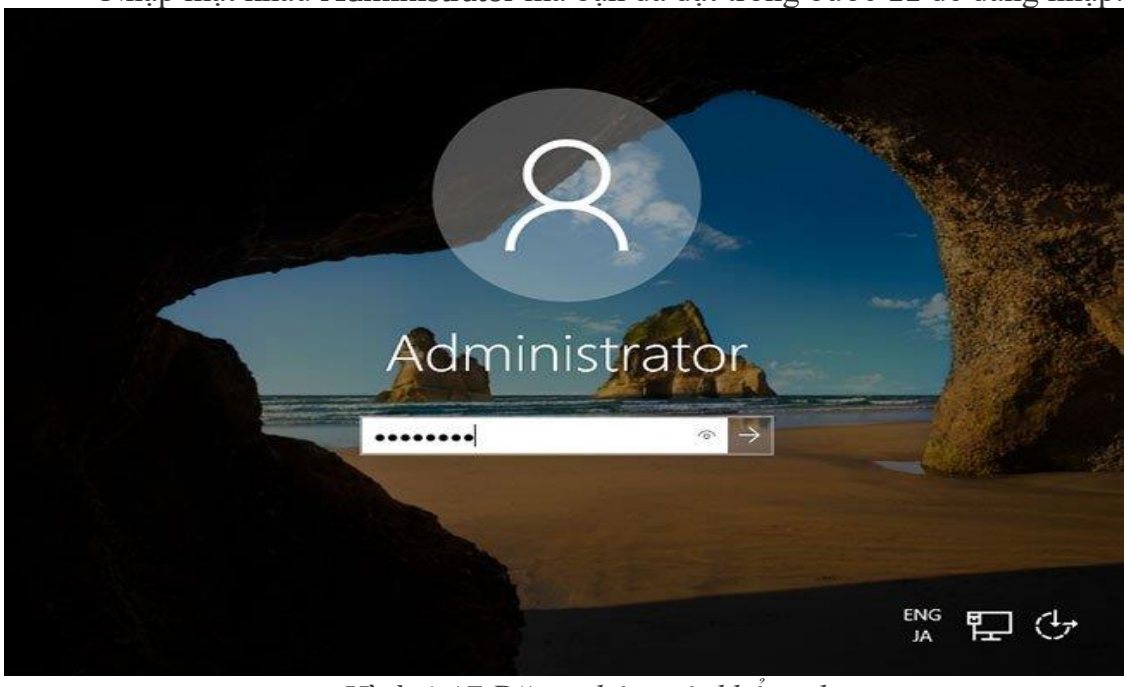
Nhấn phím **Ctrl + Alt + Del** để đăng nhập.



Hình 1.6 Chờ đăng nhập

Bước 13: Xác định mật khẩu để đăng nhập

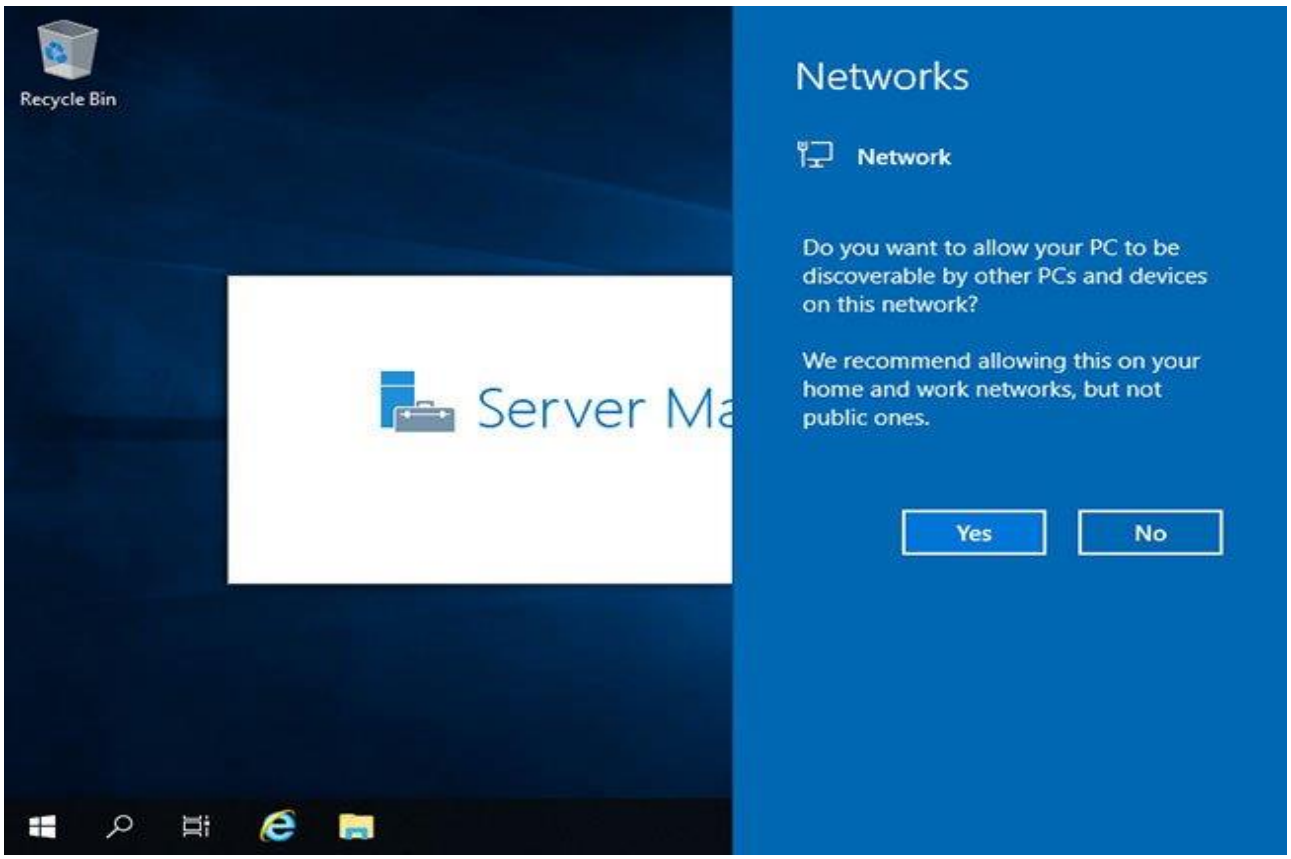
Nhập mật khẩu Administrator mà bạn đã đặt trong bước 11 để đăng nhập.



Hình 1.17 Đăng nhập mật khẩu admin

Bước 14: Xác nhận cài đặt **Networks**

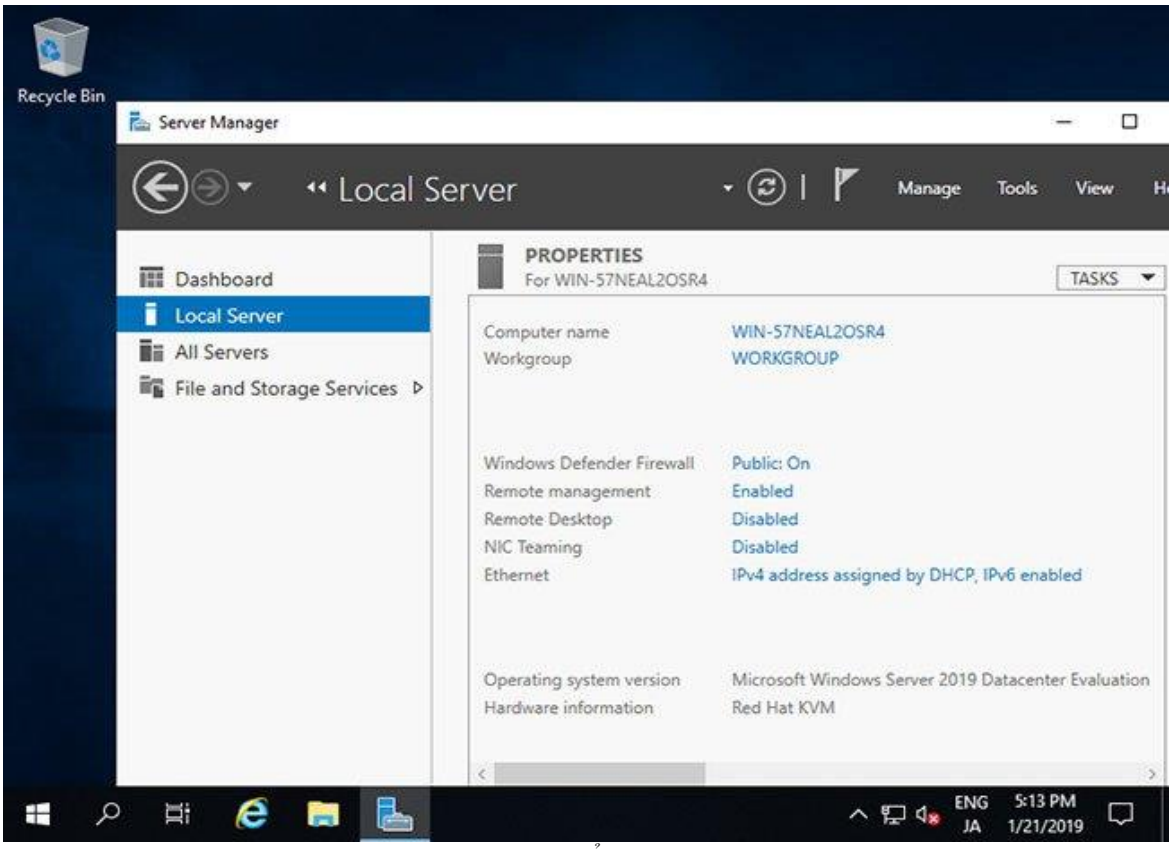
Đối với quá trình đăng nhập lần đầu, xác nhận cài đặt **Networks** được hiển thị như sau. Chọn **Yes** hoặc **No.**



Hình 1.18 Xác nhận cài đặt mạng

Bước 15: Cửa sổ Server Manger khi đăng nhập Windows Server 2019

Đây là desktop trên Windows Server 2019. Quá trình cài đặt Windows Server đã hoàn tất.



Hình 1.19 Cửa sổ Server Manger

Bài tập thực hành của học viên

1. Cài đặt hệ điều hành Windows Server 2019

Hướng dẫn thực hiện

Tham khảo mục 3 trong bài học trên.

Những trọng tâm cần chú ý:

- Cấu hình máy phải đảm bảo yêu cầu
- Phải có thiết bị lưu trữ file cài đặt.
- Thiết lập được cách Boot hệ thống, theo phương tiện cài đặt
- Chọn đúng ngôn ngữ, múi giờ, và bàn phím nhập liệu
- Thao tác đúng các bước cài đặt Windows server 2019.

Bài mở rộng và nâng cao

Hãy cài đặt nâng cấp Windows Server 2019 Standard lên Datacenter

Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được các bước cài đặt hệ điều hành Windows Server 2019
  + Trình bày được các bước cài đặt nâng cấp từ phiên bản Standard lên Datacenter cho Windows Server 2019
- Về kỹ năng:

+ Thao tác thành thạo các phương tiện Boot để cài đặt nâng cấp từ phiên bản Standard lên Datacenter cho Windows Server 2019.

+ Thực hiện đúng các thao tác cài đặt nâng cấp từ phiên bản Standard lên Datacenter cho Windows Server 2019

- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng: Đánh giá kỹ năng thực hành thực hiện các thao tác nâng cấp nâng cấp từ phiên bản Standard lên Datacenter cho Windows Server 2019.
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 2: DỊCH VỤ TÊN MIỀN (DNS)
Mã bài: MĐ 17 - 02

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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Tổng quan về DNS

Mục tiêu:

- Trình bày được cấu trúc cơ sở dữ liệu của hệ thống tên miền;
- Mô tả được sự phân cấp của hệ thống tên miền;

1.1. Giới thiệu DNS

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống phân giải tên được phát minh vào năm 1984 cho Internet, chỉ một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền. Hệ thống tên miền (DNS) là một hệ thống đặt tên theo thứ tự cho máy vi tính, dịch vụ, hoặc bất kỳ nguồn lực tham gia vào Internet. Nó liên kết nhiều thông tin đa dạng với tên miền được gán cho những người tham gia. Quan trọng nhất là, nó chuyển tên miền có ý nghĩa cho con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị khắp thế giới.

Phép tương thường được sử dụng để giải thích hệ thống tên miềnlà, nó phục vụ như một "Danh bạ điện thoại" để tìm trên Internet bằng cách dịch tên máy chủ máy tính thành địa chỉ IP

Ví dụ, www.dantri.com.vn dịch thành 208.77.188.166.

Hệ thống tên miền giúp cho nó có thể chỉ định tên miền cho các nhóm người sử dụng Internet trong một cách có ý nghĩa, độc lập với mỗi địa điểm của người sử dụng. Bởi vì điều này, World Wide Web siêu liên kết và trao đổi thông tin trên Internet có thể duy trì ổn định và cố định ngay cả khi định tuyến dòng Internet thay đổi hoặc những người tham gia sử dụng một thiết bị di động. Tên miền internet dễ nhớ hơn các địa chỉ IP như là 208.77.188.166 (IPv4) hoặc 2001: db8: 1f70:: 999: de8: 7648:6 e8 (IPv6).

Mọi người tận dụng lợi thế này khi họ thuật lại có nghĩa các URL và địa chỉ email mà không cần phải biết làm thế nào các máy sẽ thực sự tìm ra chúng.

Hệ thống tên miền phân phối trách nhiệm gán tên miền và lập bản đồ những tên tới địa chỉ IP bằng cách định rõ những máy chủ có thẩm quyền cho mỗi tên miền. Những máy chủ có tên thẩm quyền được phân công chịu trách nhiệm đối với tên miền riêng của họ, và lần lượt có thể chỉ định tên máy chủ khác độc quyền của họ cho các tên miền phụ. Kỹ thuật này đã thực hiện các cơ chế phân phối DNS, chịu đựng lỗi, và giúp tránh sự cần thiết cho một trung tâm đơn lẻ để đăng kí được tư vấn và liên tục cập nhật.Ở Việt Nam thì tất cả thông tin về IP, các bản ghi DNS,… đều do tổ chức VNNIC quản lý và cấp phát.Hệ thống DNS quốc gia có nhiệm vụ tiếp nhận và trả lời các truy vấn tên miền.VN. Hệ thống DNS quốc gia do Trung tâm Internet Việt Nam (VNNIC) quản lý.Hiện tại hệ thống tên miền quốc gia Việt Nam gồm 07 cụm máy chủ, trong đó 05 cụm máy chủ đặt trong nước (02 cụm tại thành phố Hồ Chí Minh; 02 cụm tại Hà Nội; 01 cụm đặt tại Đà Nẵng); và 02 cụm máy chủ đặt ở nước ngoài tại nhiều điểm trên thế giới.

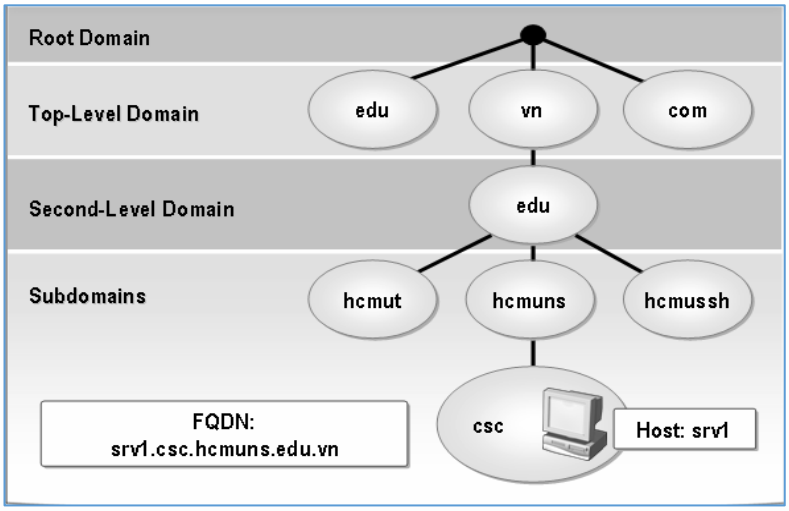
Mỗi Website có một tên (là tên miền hay đường dẫn URL:Universal Resource

Locator) và một địa chỉ IP. Địa chỉ IP gồm 4 nhóm số cách nhau bằng dấu chấm(Ipv4). Khi mở một trình duyệt Web và nhập tên website, trình duyệt sẽ đến thẳng website mà không cần phải thông qua việc nhập địa chỉ IP của trang web. Quá trình "dịch" tên miền thành địa chỉ IP để cho trình duyệt hiểu và truy cập được vào website là công việc của một DNS server. Các DNS trợ giúp qua lại với nhau để dịch địa chỉ "IP" thành "tên" và ngược lại. Người sử dụng chỉ cần nhớ "tên", không cần phải nhớ địa chỉ IP (địa chỉ IP là những con số rất khó nhớ).DNS sử dụng cổng port 53 để truyền thông tin.Đây chính là chức năng chính của một con DNS Server trong việc hỗ trợ phân giải tên miền 1 cách đơn giản, giúp người dùng đầu cuối dễ dàng nhập các địa chỉ web, địa chỉ Local mà không gặp rắc rối.

Do các DNS có tốc độ biên dịch khác nhau, có thể nhanh hoặc có thể chậm, do đó người sử dụng có thể chọn DNS server để sử dụng cho riêng mình. Có các cách chọn lựa cho người sử dụng. Sử dụng DNS mặc định của nhà cung cấp dịch vụ (internet), trường hợp này người sử dụng không cần điền địa chỉ DNS vào network connections trong máy của mình. Sử dụng DNS server khác (miễn phí hoặc trả phí) thì phải điền địa chỉ DNS server vào network connections. Địa chỉ DNS server cũng là 4 nhóm số cách nhau bởi các dấu chấm. Trong bài lab này chúng ta sẽ không để DNS auto của google hay bất cứ địa chỉ DNS Internet nào mà sẽ để DNS là địa chỉ IP của con DNS Server trong Domain.

ví dụ: Ta có bản ghi cntt.cdn.edu.vn có địa chỉ là 192.168.2.2. Để đổi địa chỉ DNS cho server hay Win 8,10 các bạn click chuột phải vào biểu tượng card mạng dưới thanh taskbar chọn Open network sharing center, click chuột phải vào card Local area network chọn properties, click đúp vào TCP/IP v4. Ở mục General, chọn Use the following IP address để gán IP tĩnh, nhập IP của DNS vào mục Preferred DNS server và Alternate DNS server, sau đó ấn OK để cấu hình hoàn tất

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

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 **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

Bên cạnh đó, mỗi nước cũng có một **top-level domain**. Ví dụ **top-leveldomain** của Việt Nam là.vn, Mỹ là.us, ta có thể tham khảo thêm thông tin địa chỉ tên miền tại địa chỉ: **http://www.thrall.org/domains.htm**

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

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 nhiều 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

Mục tiêu:

- Trình bày được sự 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

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

Mục tiêu:

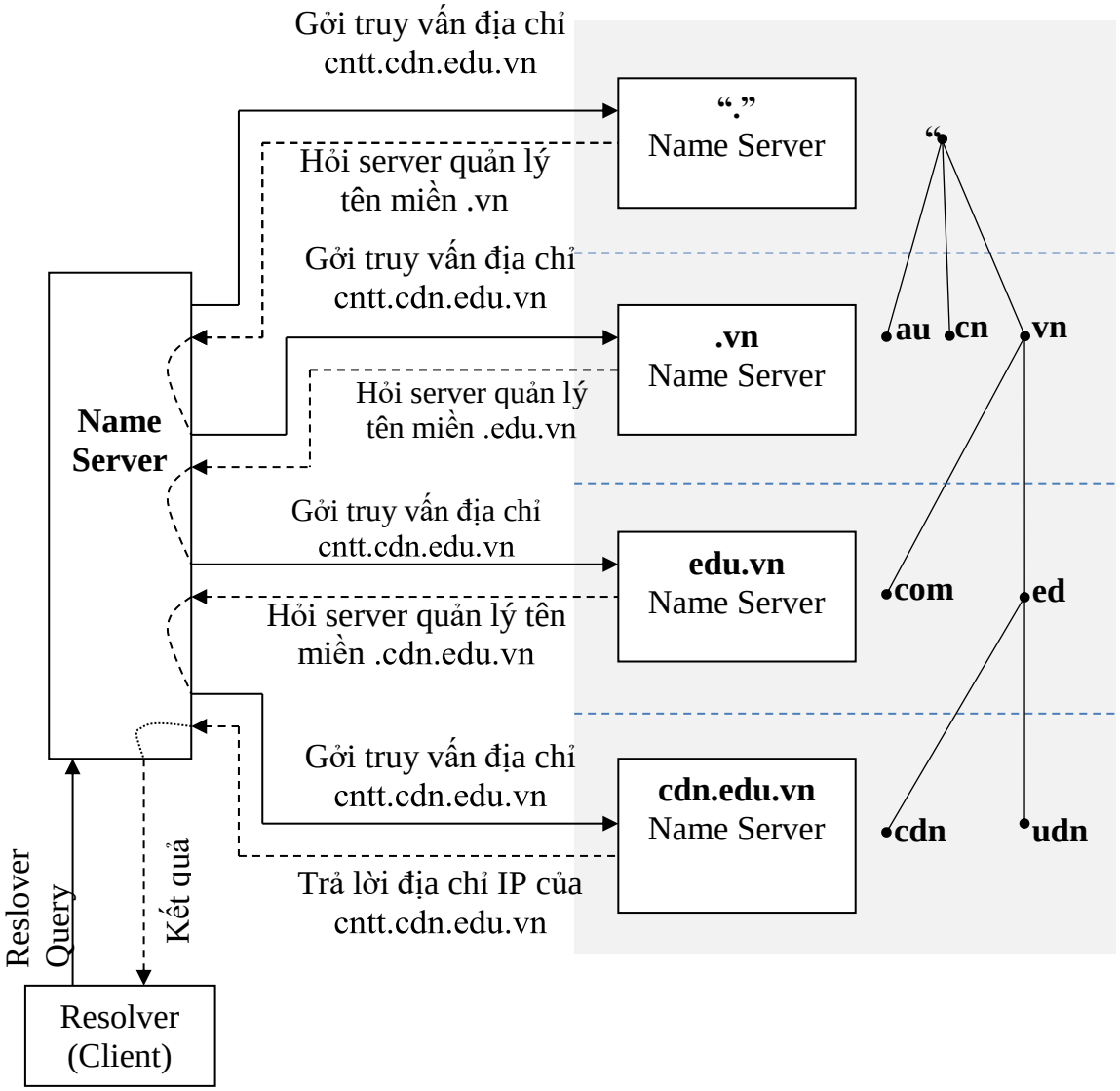
- Trình bày được cơ chế phân giải tên máy tính thành địa chỉ IP và ngược lại;

3.1. Phân giải tên thành 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**



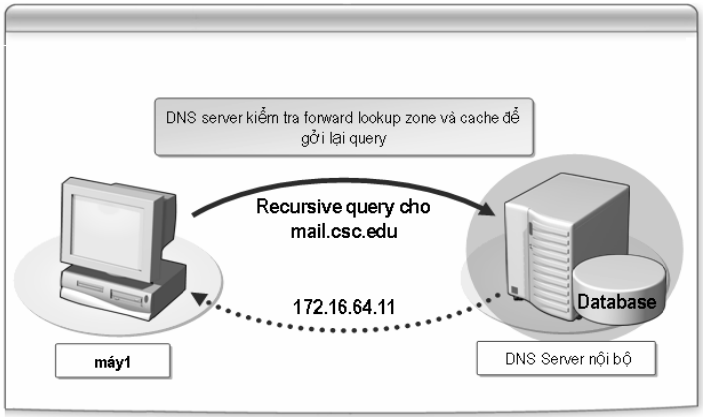
Hình 2.2 mô tả quá trình phân giải tên miền

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:

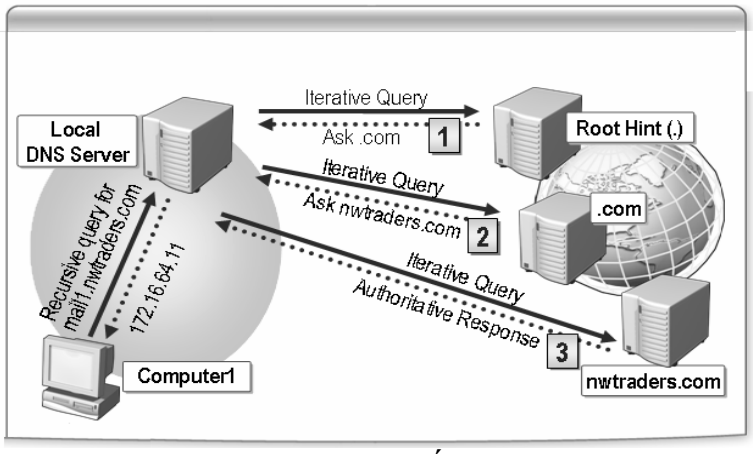
- Truy vấn đệ quy (**recursive query**): khi **name server** nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được. **Name server** không thể tham chiếu truy vấn đến một **name server** khác. **Name server** Có thể gửi truy vấn dạng đệ quy hoặc

tương tác đến **name server** khác nhưng phải thực hiện cho đến khi nào có kết quả mới thôi.



Hình 2.3 Truy vấn đệ quy

- 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.



Hình 2.4 - Truy vấn tương tác

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.

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

Mục tiêu:

- Trình bày được các 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. Fully 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 ủy 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

Mục tiêu:

- Trình bày được các loại tên Domain Server.

5.1. Primary Name Server (PDS)

Primary DNS Server (PDS) là nguồn xác thực thông tin chính thức cho các tên miền mà nó được phép quản lý. Thông tin về một tên miền do PDS được phân cấp quản lý thì được lưu trữ tại đây và sau đó có thể được chuyển sang các Secondary DNS Server (SDS).

Các tên miền do PDS quản lý thì được tạo, và sửa đổi tại PDS và sau đó được cập nhật đến các SDS

5.2. Secondary Name Server (SDS)

- DNS được khuyến nghị nên sử dụng ít nhất là hai DNS server để lưu địa chỉ cho mỗi một vùng (zone). PDS quản lý các vùng và SDS được sử dụng để lưu trữ dự phòng cho vùng, và cho cả PDS. SDS không nhất thiết phải có nhưng khuyến khích hãy sử dụng. SDS được phép quản lý tên miền nhưng dữ liệu về tên miền không phải được tạo ra từ SDS mà được lấy về từ PDS.
- SDS có thể cung cấp các hoạt động ở chế độ không tải trên mạng. Khi lượng truy vấn vùng (zone) tăng cao, PDS sẽ chuyển bớt tải sang SDS (quá trình này còn được gọi là cân bằng tải), hoặc khi PDS bị sự cố thì SDS hoạt động thay thế cho đến khi PDS hoạt động trở lại.
- SDS thường được sử dụng tại nơi gần với các máy trạm (client) để có thể phục vụ cho các truy vấn một cách dễ dàng. Tuy nhiên, cài đặt SDS trên cùng một subnet hoặc cùng một kết nối với PDS là không nên. Điều đó sẽ là một giải pháp tốt để dự phòng cho PDS, vì khi kết nối đến PDS bị hỏng thì cũng không ảnh hưởng gì tới đến SDS.
- các địa chỉ mới vào các vùng. Do đó, DNS server sử dụng một cơ chế cho phép chuyển các thông tin từ PDS sang SDS và lưu giữ trên đĩa. Khi cần phục hồi dữ liệuvề các vùng, chúng ta có thể sử dụng giải pháp lấy toàn bộ (full) hoặc chỉ lấy phần thay đổi (incrememtal).

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. Các khái niệm trong Zone

– **primary zone**: cho phép đọc và ghi cơ sở dữ liệu và có toàn quyền trong việc update dữ liệu của DNS

– **secondary zone**: cho phép đọc và ghi bản sao của sơ sở dữ liệu và muốn được cập nhật zone thì phải đồng bộ với Primary zone

– **forwarder**: là kỹ thuật cho phép name server nội bộ gửi yêu cầu truy vấn đến server khác để phân giải những tên miền bên ngoài hệ thống

– **Delegation** (sự ủy quyền): 1 miền có thể tổ chức thành miền con, mỗi miền con có thể ủy quyền cho 1 tổ chức khác, và tổ chức này phải chịu trách nhiệm duy trì thông tin trong miền này

Một trong những mục đích của DNS đó là quản trị phân tán. Ta có thể chia nhỏ việc quản lý thành nhiều phần khác nhau. Một domain có thể có nhiều subdomains.

Mỗi subdomain có thể đại diện cho một tổ chức và tổ chức đó có toàn quyền để điều khiển DNS của tổ chức đó. Việc phân quyền này làm cho DNS trở nên nhẹ hơn, ko phải quản lý tập trung bởi dữ liệu là rất lớn

7. FQDN: (Fully Qualified Domain Name)

• **Start of Authority (SOA) resource record**: định nghĩa các tham số toàn cục cho zone hoặc tên miền. Một tệp tin zone chỉ được phép chứa một mẩu tin SOA và phải nằm ở vị trí đầu tiên trước các mẩu tin khác.

• **Name server (NS) resource record**: chỉ ra Máy chủ tên miền (Name server) của zone đó.

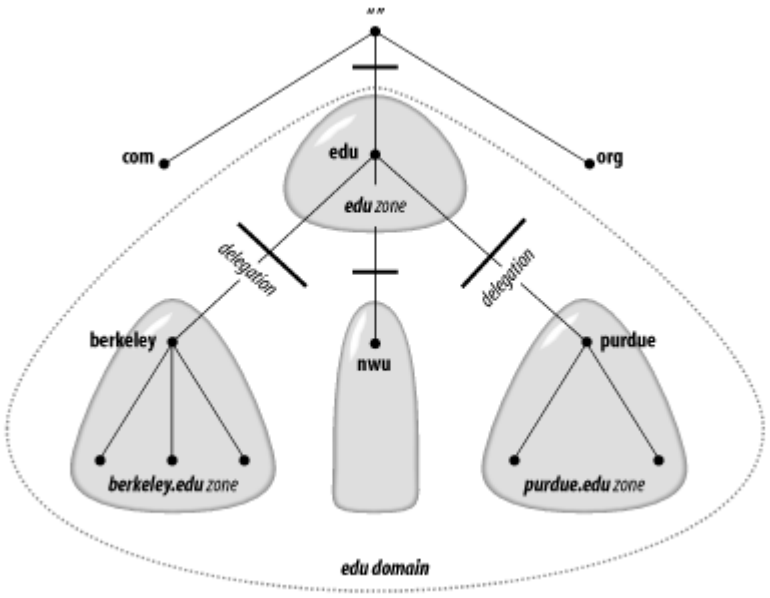
• **A Resource Records** (mẩu tin địa chỉ): mẩu tin cho biết địa chỉ IP tương ứng của một tên miền, có dạng như "example IN A 172.16.48.1"

• **PTR Records** (mẩu tin con trỏ): ngược lại với A record, PTR chỉ ra tên miền tương ứng của một địa chỉ IP, có dạng như "1.48.16.172.in-addr.arpa. IN PTR example.com."

• **CNAME Resource Records**: một dạng record giúp tạo ra biệt hiệu cho một tên miền, ví dụ mẩu tin CNAME "ftp.example.com. IN CNAME ftp1.example.com." cho phép trỏ tên miền ftp.example.com sang ftp1.example.com

• **MX Resource Records** (mẩu tin Mail exchange): chỉ ra máy chủ mail của tên miền.

• **TXT Resource Records** (mẩu tin text): chứa thông tin dạng văn bản không định dạng, thường dùng để chứa các thông tin bổ sung.-Nameserver and ZonesCác chương trình lưu trữu toàn bộ thông tin về domain namespace gọi là nameserver. Nameserver thông thường sẽ có thông tin hoàn chỉnh về một phần nào đó của domain namespace gọi là zone, zone này load từ file hoặc từ nameserver khác.



Hình 2.5 Domain được chia ra thành nhiều zone

Hình trên cho ta thấy một domain.edu được chia ra thành nhiều zone. Mỗi zone lại được phân quyền quản lý riêng.Có 2 kiểu nameserver: primary master và secondary master.

- Primary: chứa tất cả các thông tin cho domain
- Secondary: hoạt động dự phòng, đề phòng trường hợp Primary fail.

Qúa trình Primary gửi bản sao của nó đến Secondary gọi là zone transfer.

– Resolvers

Là các clients truy cập vào nameservers. Các chương trình chạy host nếu cần thông tin từ domain namespace sẽ sử dụng resolver.

Resolver quản lý:

- Truy vấn nameserver
- Quản lý các trả lời từ nameserver
- Trả thông tin về cho chương trình yêu cầu

– Querying the database: Các truy vấn dns có thể được gửi từ một DNS client (resolver) đến một DNS server hoặc giữa 2 DNS server.

Một yêu cầu DNS thực ra chỉ là một truy vấn yêu cầu đưa ra các kiểu dữ liêu(RRs). Các kiểu dữ liệu trong truy vấn này có thể là dữ liệu ánh xạ hostname->IP(RR A), mail(MX)

8. Cài đặt và cấu hình DNS

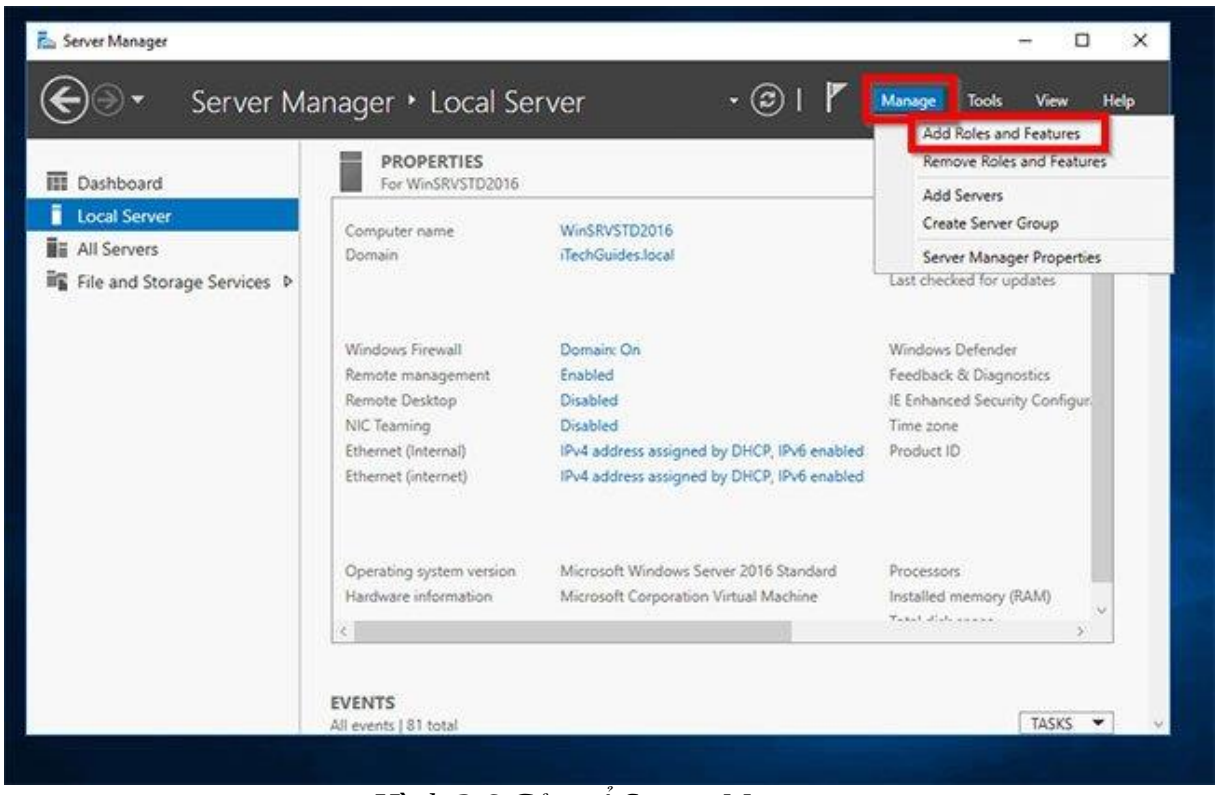
Mục tiêu:

- Thực hiện được quá trình cài đặt và cấu hình DNS.

8.1. Các bước cài đặt dịch vụ DNS

Bước 1: Mở Server Manager tiến hành cài DNS

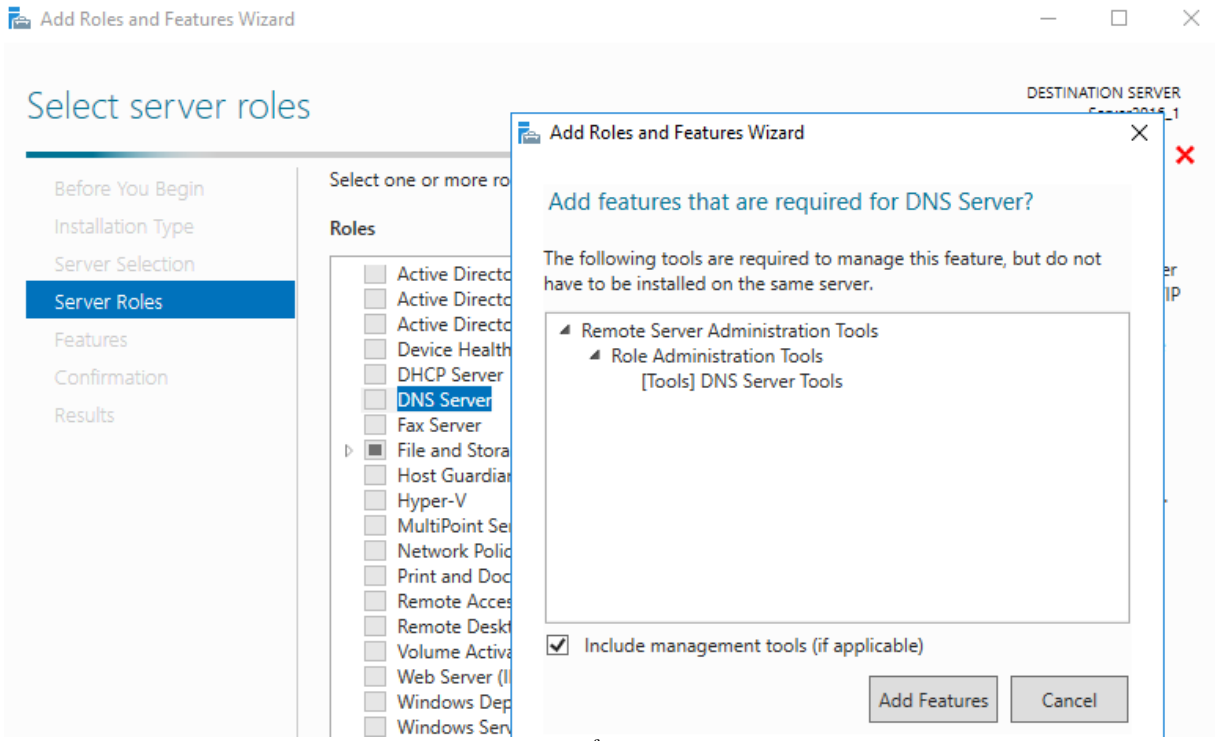
Vào Server Manager -> chọn Add role and Feature



Hình 2.6 Cửa sổ Server Manager

Bước 2: Chọn DNS Server để cài đặt

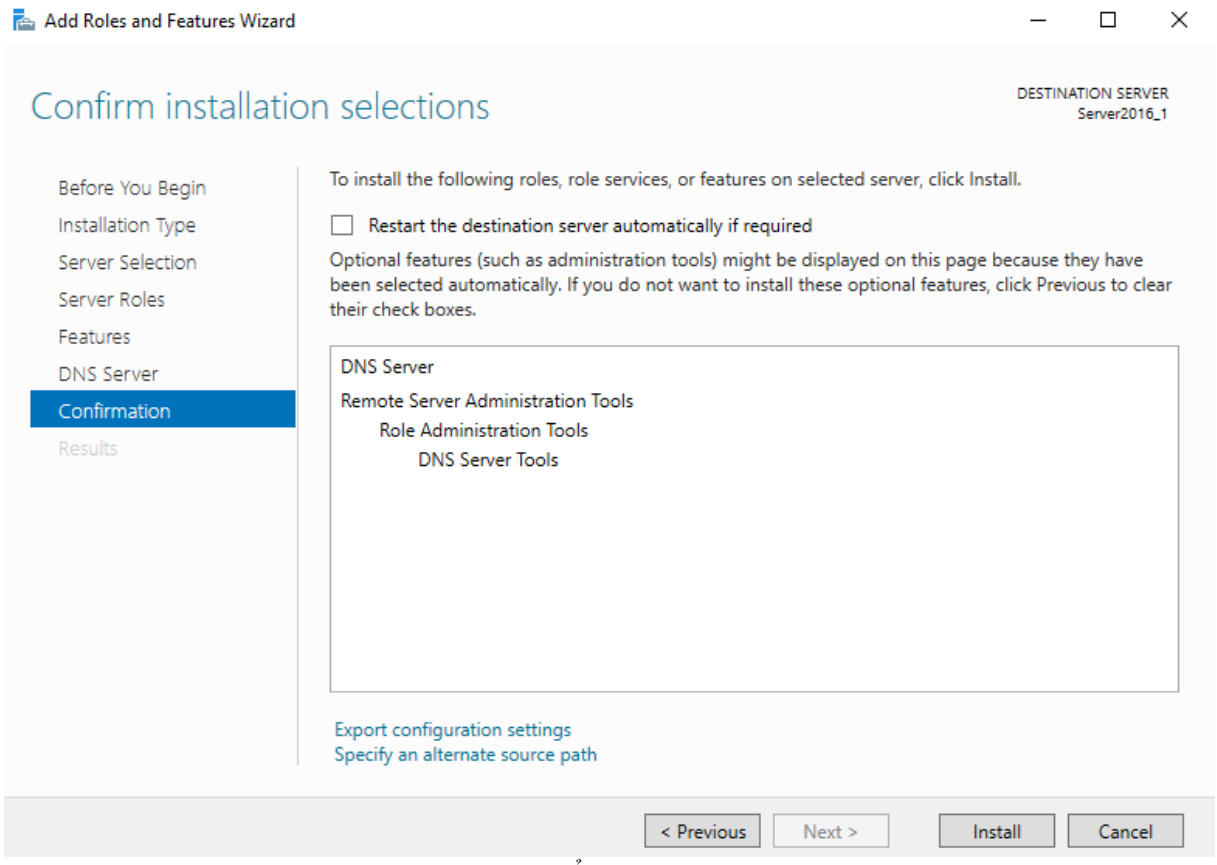
Tích vào ô DNS Server -> click Next



Hình 2.7 Cửa sổ chọn DNS Server

Bước 3: *Tiến hành cài đặt DNS Server*

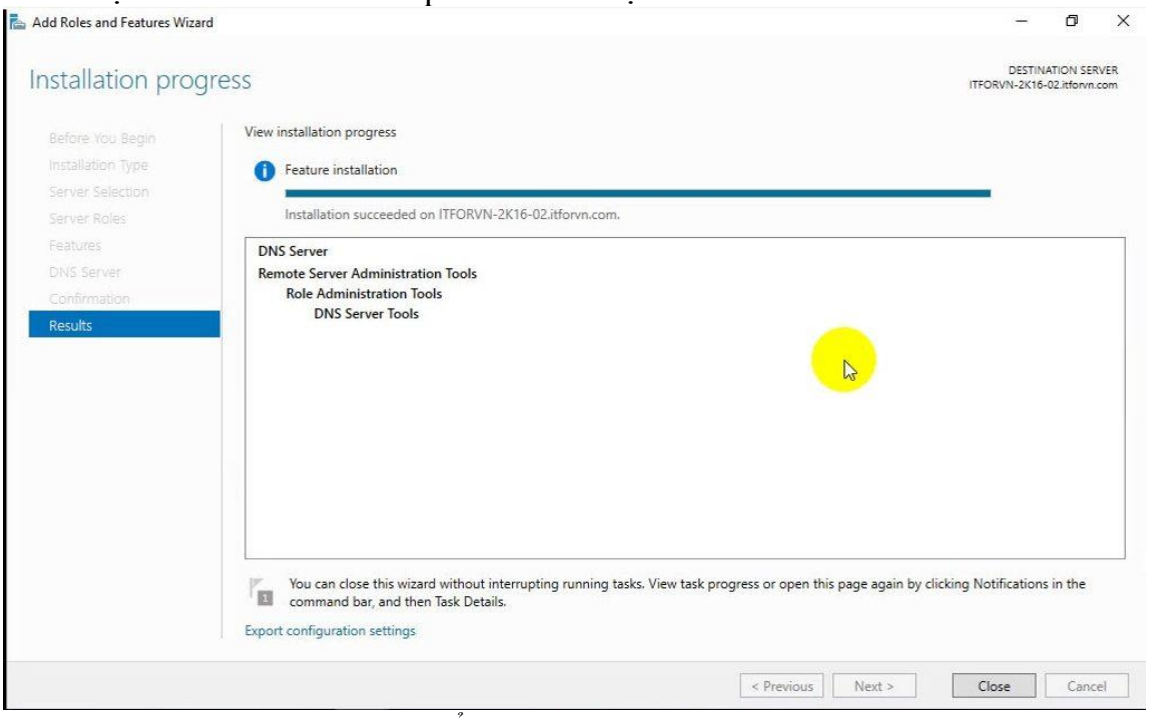
chọn Install để tiến hành quá trình cài đặt



Hình 2.8 Cửa sổ cài đặt DNS Server

Bước 4: Xác định DNS Server cài xong

Chọn Close để kết thúc quá trình cài đặt



Hình 2.9 Cửa sổ cài đặt DNS Server hoàn thành

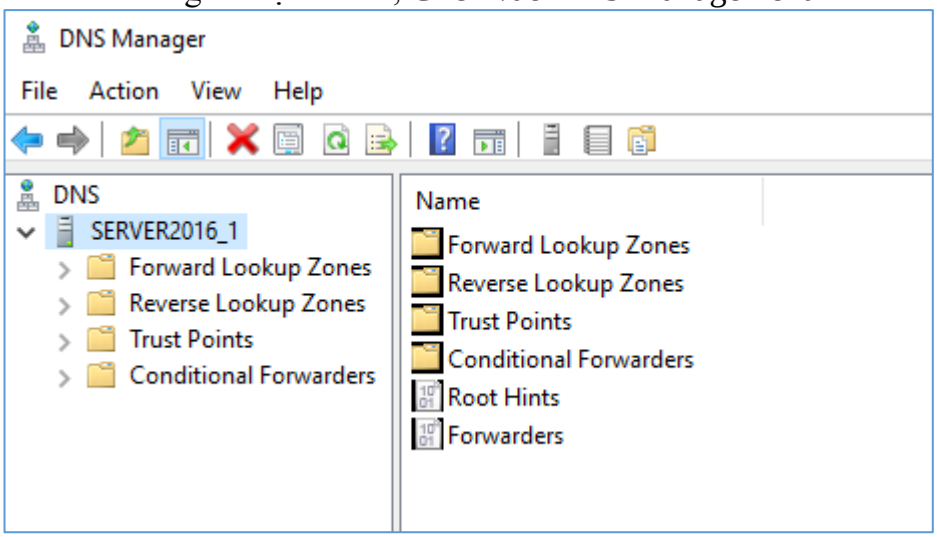
8.2. Cấu hình dịch vụ DNS

8.2.1. Tạo Forward Lookup Zones

Forward Lookup Zone để phân giải địa chỉ Tên máy (hostname) thành địa chỉ IP. Để tạo zone này ta thực hiện các bước sau:

Bước 1: Mở cửa sổ DNS Server

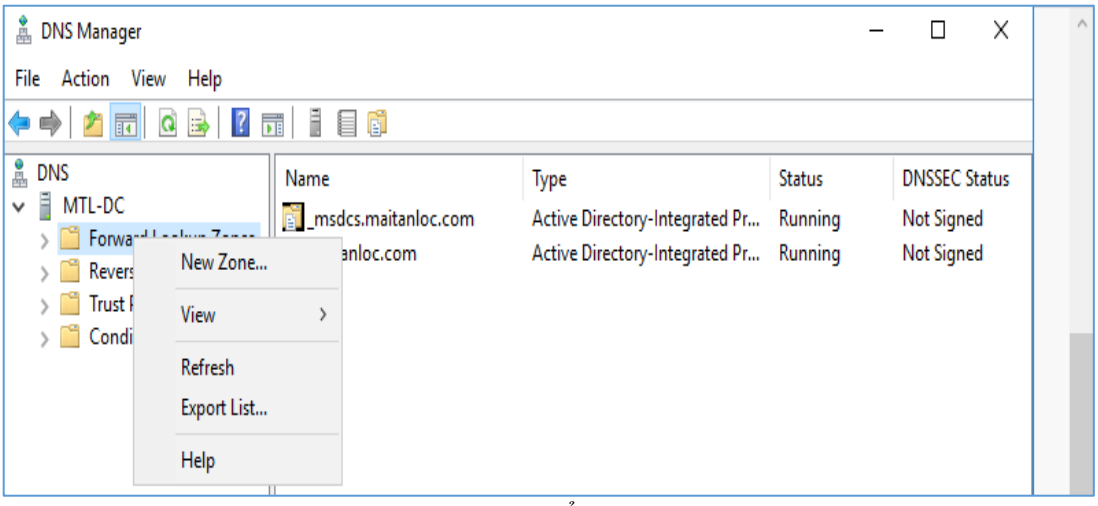
Vào Server Manager chọn Tools, Click vào DNS Management



Hình 2.10 Cửa sổ DNS Server

Bước 2: Tạo 1 zone mới

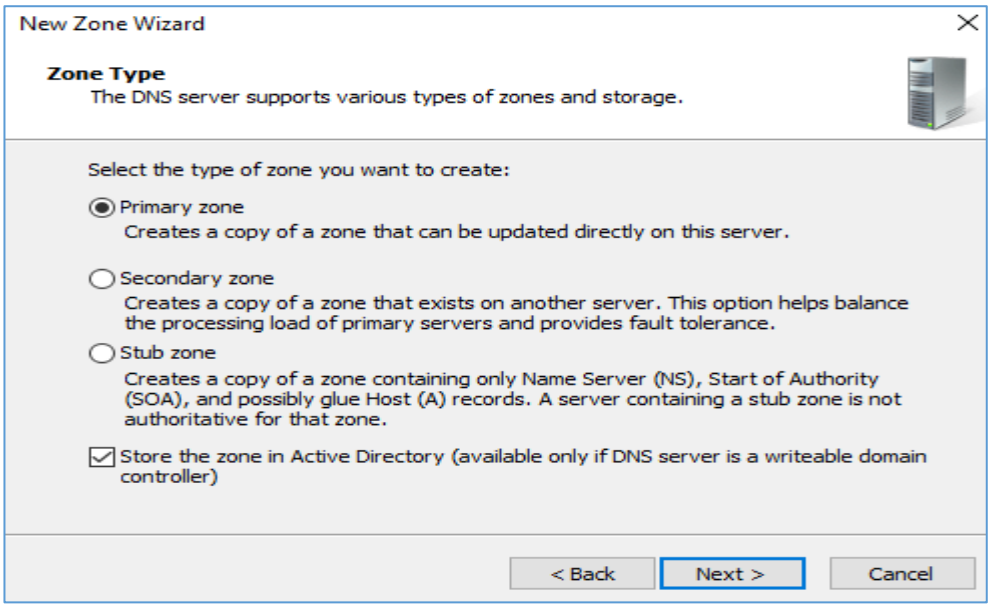
Click chuột phải vào Forward Lookup zone chọn New zone để tạo 1 zone mới vd: itforvn2.com



Hình 2.11 Cửa sổ tạo 1 zone mới

Bước 3: Chọn lựa kiểu zone mới

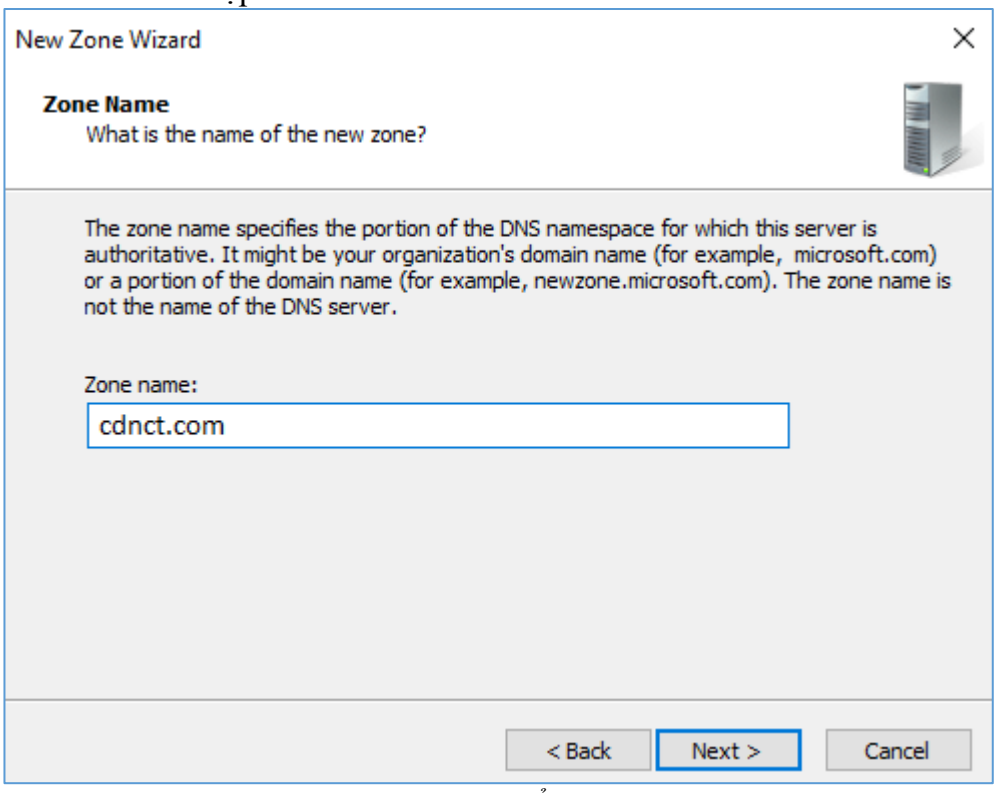
Chọn Primary zone để tạo 1 zone chính, sau đó click Next tiếp tục



Hình 2.12 Cửa sổ zone type

Bước 4: Nhập tên Domain mà zone sẽ quản lý

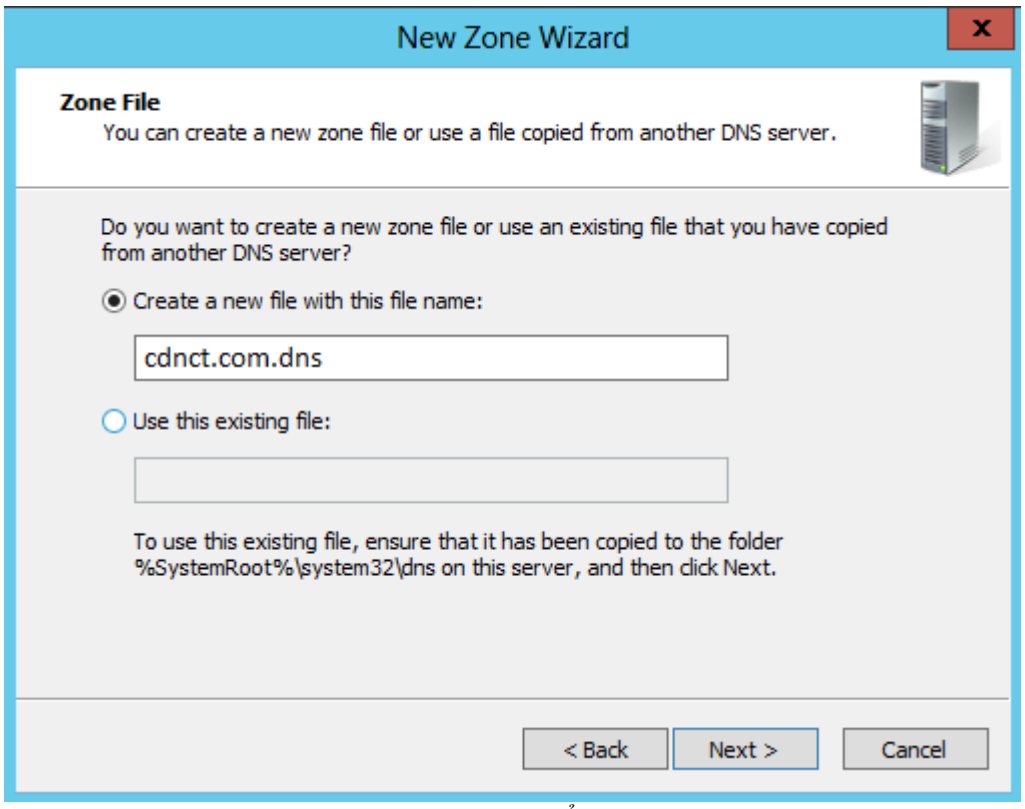
Nhập tên DNS server vào Zone name



Hình 2.13 Cửa sổ Zone name

Bước 5: Chọn hình thức tạo DNS server

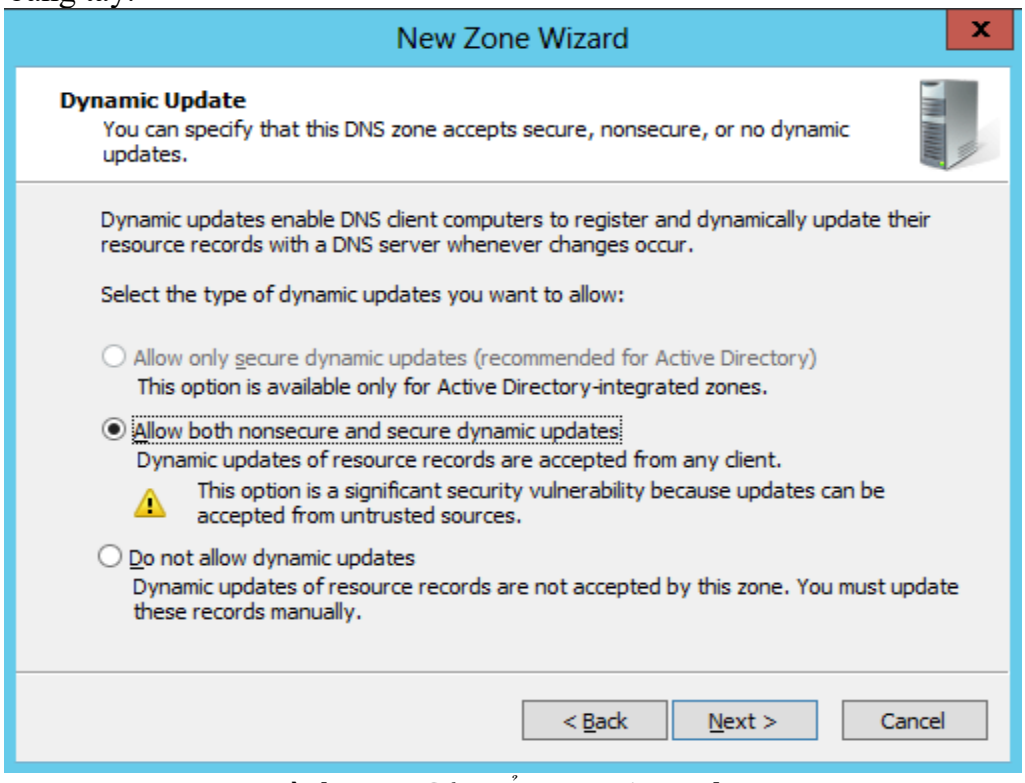
Chọn Create a new file with thí file name, nhập tên zone cần tạo



Hình 2.14 Cửa sổ Zone file

Bước 6: Chọn hình thức cập nhật cho DNS

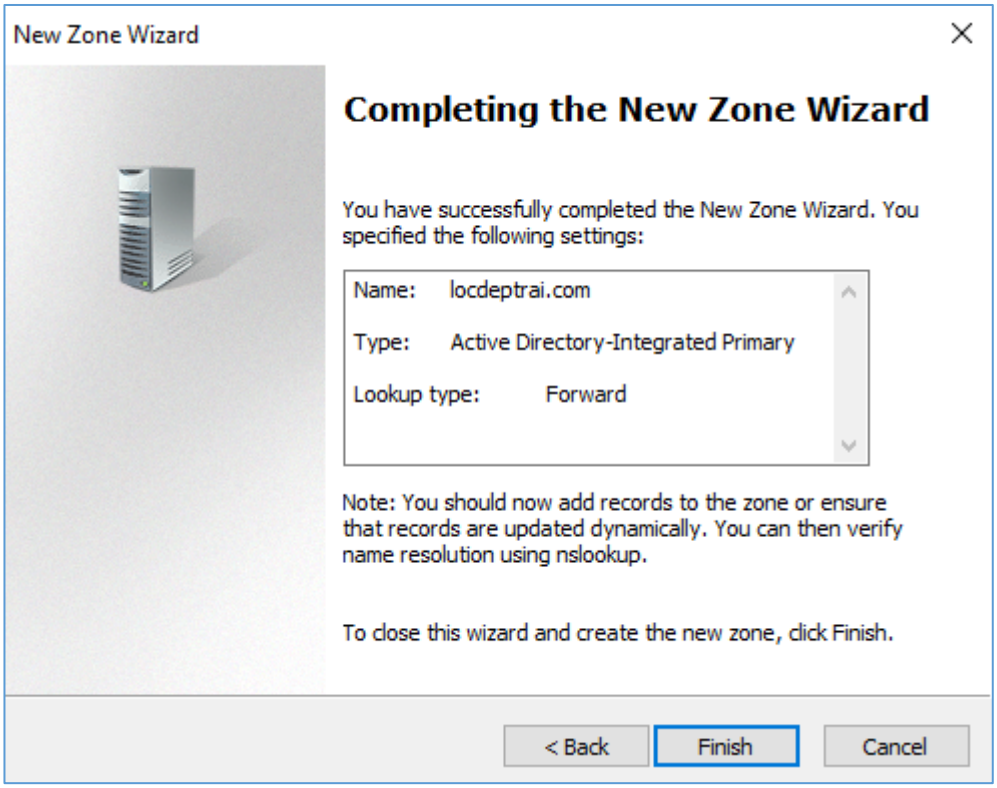
- Vì không có AD nên option đầu không hiện lên
- allow both nếu bạn muốn tự đông update Resource Record từ bất kỳ client nào. Tuy nhiên việc này không được khuyến nghị vì nó có thể gây ra các lỗ hổng bảo mật. Bởi vì việc update này có thể chấp nhận cả những nguồn không tin.
- Do not allow dynamic updates: Việc update Resource Records phải được làm bằng tay.



Hình 2.15 Cửa sổ Dynamic Update

Bước 7: Hoàn thành cấu hình DNS Server

Click vào Finish để hoàn thành việc cấu hinh DNS Server



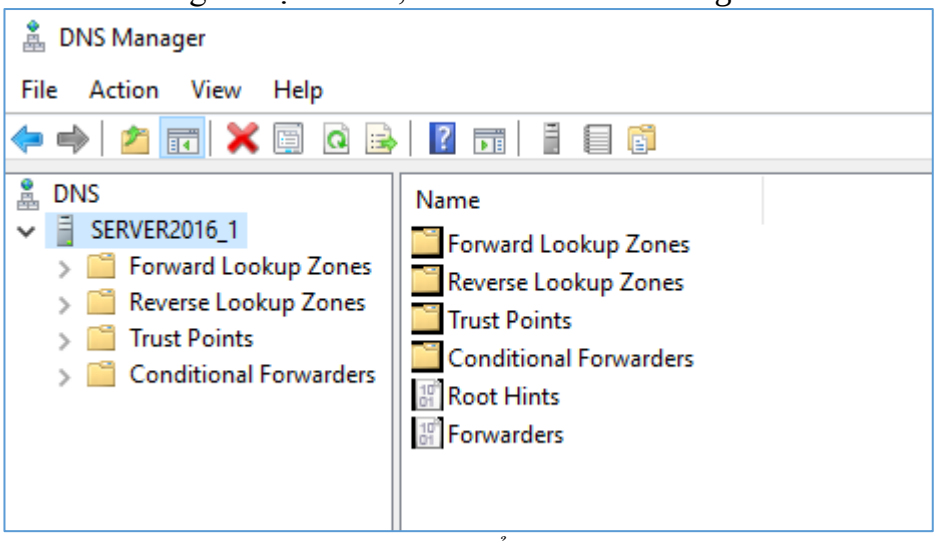
Hình 2.16 Cửa sổ hoàn thành cấu hình DNS

8.2.2. Tạo Reverse Lookup Zone

Sau khi tạo xong Foward lookup zone ta chọn vào Reverse lookup zone, click chuột phải chọn New zone.Ở Zone type click chọn vào Primary zone Tại cửa sổ Reverse Lookup Zone Name, click chọn vào IPv4

Bước 1: Mở cửa sổ DNS Server

Vào Server Manager chọn Tools, Click vào DNS Management



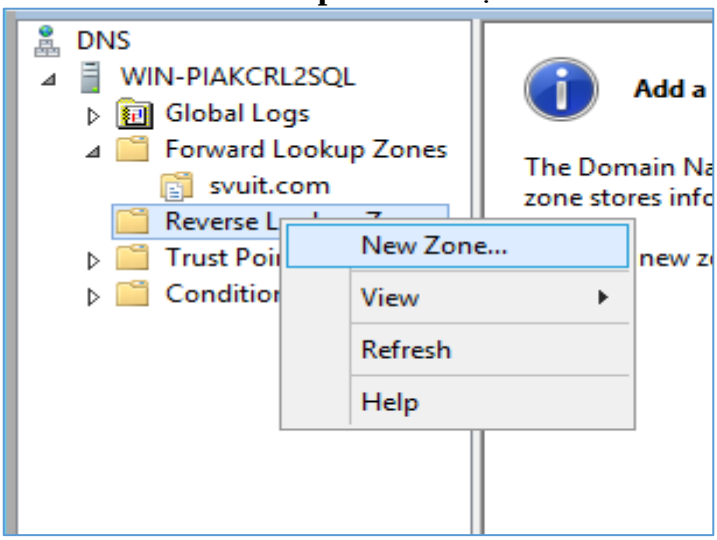
Hình 2.17 Cửa sổ DNS Server

Bước 2:

Hình 2.17 Cửa sổ

Bước 2: Tạo zone phân giải nghịch

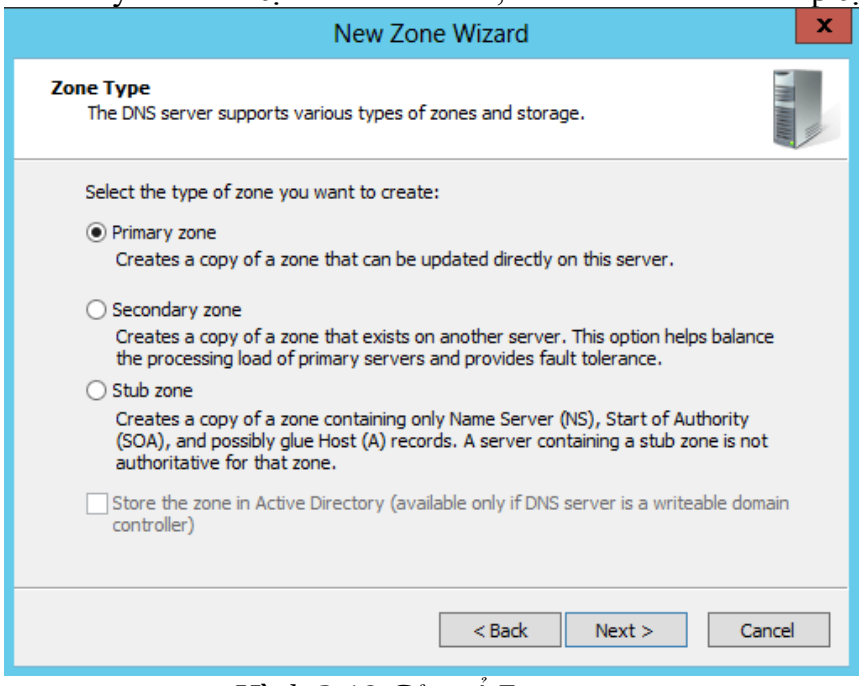
Right-click trên "**reverse Lookup Zone**" chọn new zone



Hình 2.18 Cửa sổ tạo zone phân giải nghịch

Bước 3: Chọn lựa kiểu zone mới

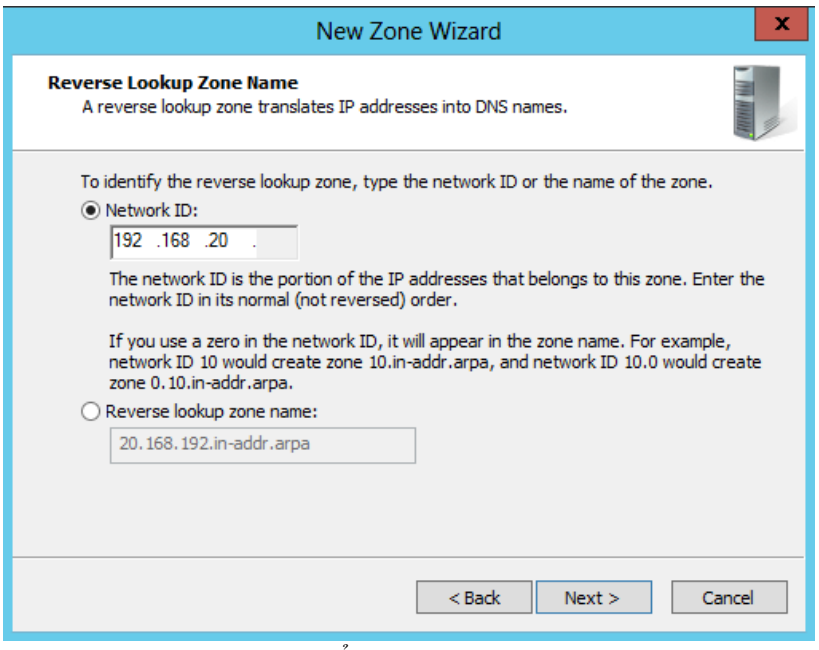
Chọn Primary zone để tạo 1 zone chính, sau đó click Next tiếp tục



Hình 2.19 Cửa sổ Zone type

Bước4: Nhập Subnet cho DNS sẽ phân giải

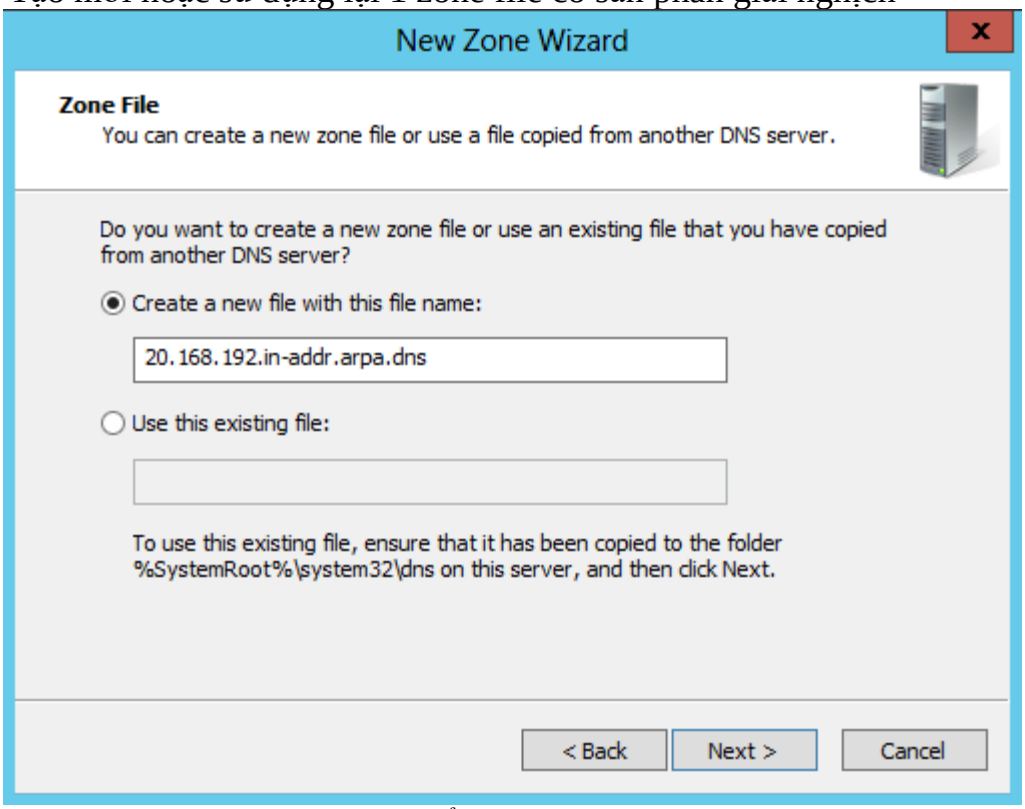
Điền Subnet mà DNS sẽ phân giải



Hình 2.20 Cửa sổ Reverse lookup zone name

Bước 5: Chọn hình thức tạo NDS server phân giải nghịch

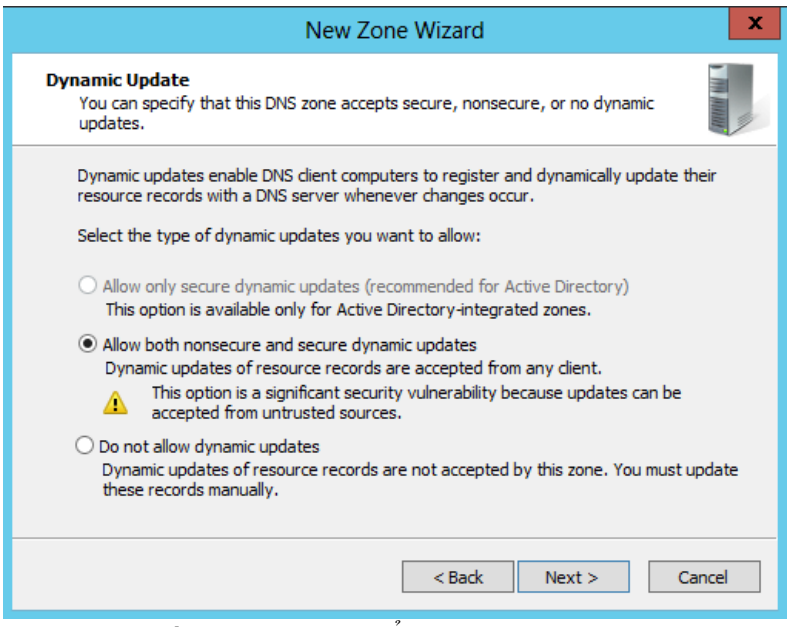
Tạo mới hoặc sử dụng lại 1 zone file có sẵn phân giải nghịch



Hình 2.21 Cửa sổ zone file phân giải nghịch

Bước 6: Chọn hình thức cập nhật

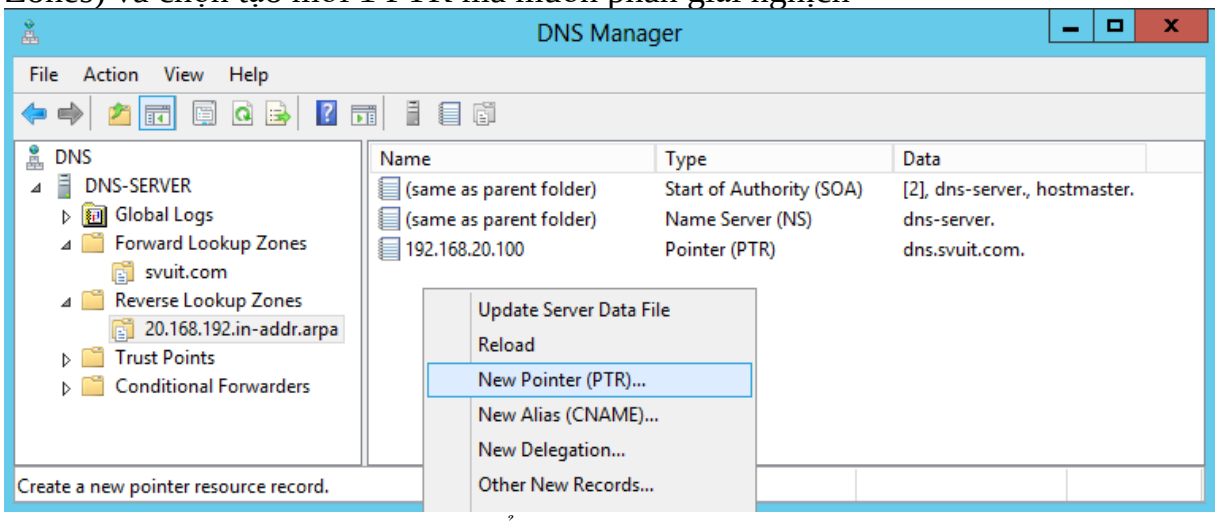
Chọn chế update tự động



Hình 2.22 Cửa sổ Dynamic Update

Bước 7: Tạo 1 PTR phân giải nghịch

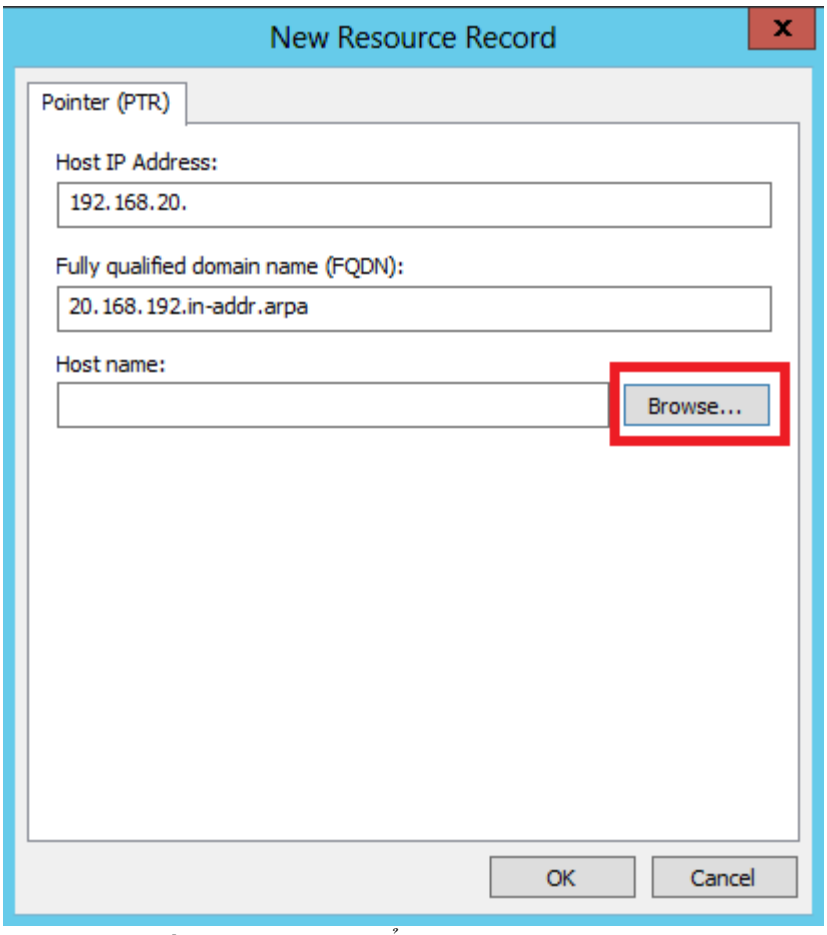
Right-click vào chỗ trống trên zone phân giải nghịch(Reverse Lookup Zones) và chọn tạo mới 1 PTR mà muốn phân giải nghịch



Hình 2.23 Cửa sổ Tạo record A phân giải nghịch

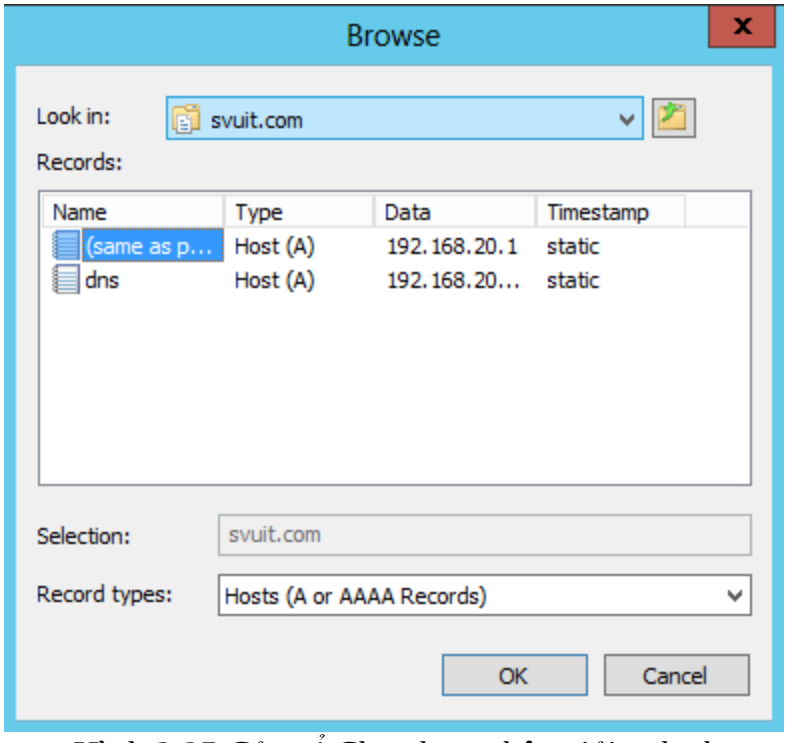
Bước 8: Cập nhập PTR cho tên server DNS

click vào Browser để trỏ đến record A mà bạn cần phân giải nghịch



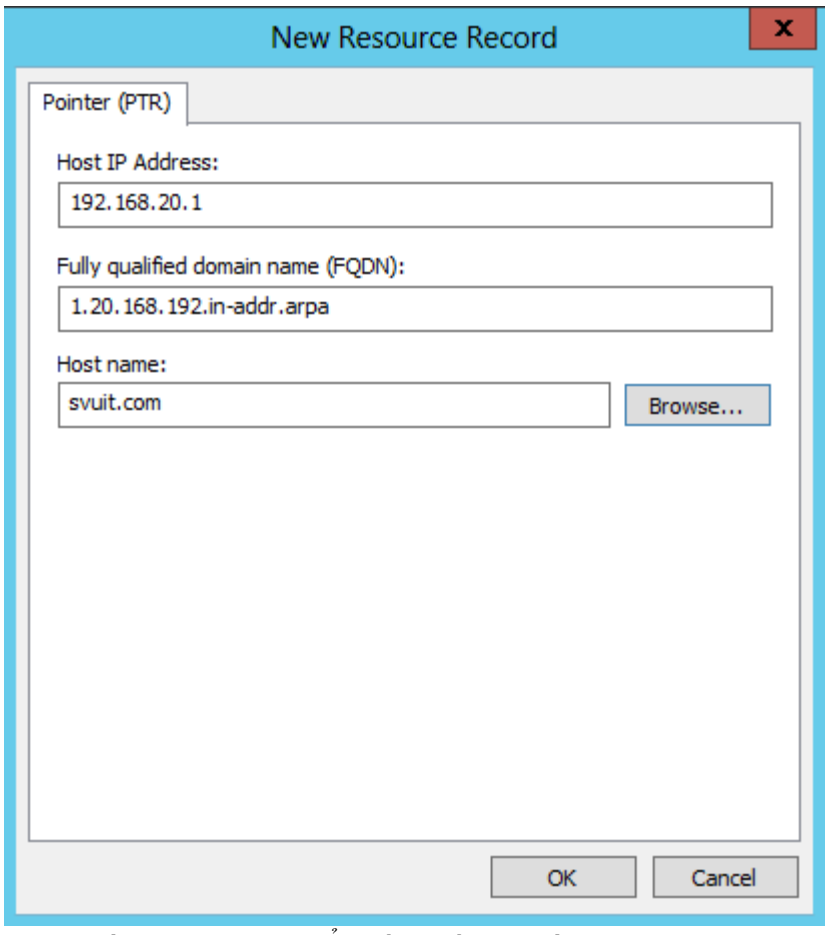
Hình 2.24 Cửa sổ New resoure record

Bước 9: Chọn record A của Web server



Hình 2.25 Cửa sổ Chọn host phân giải nghịch

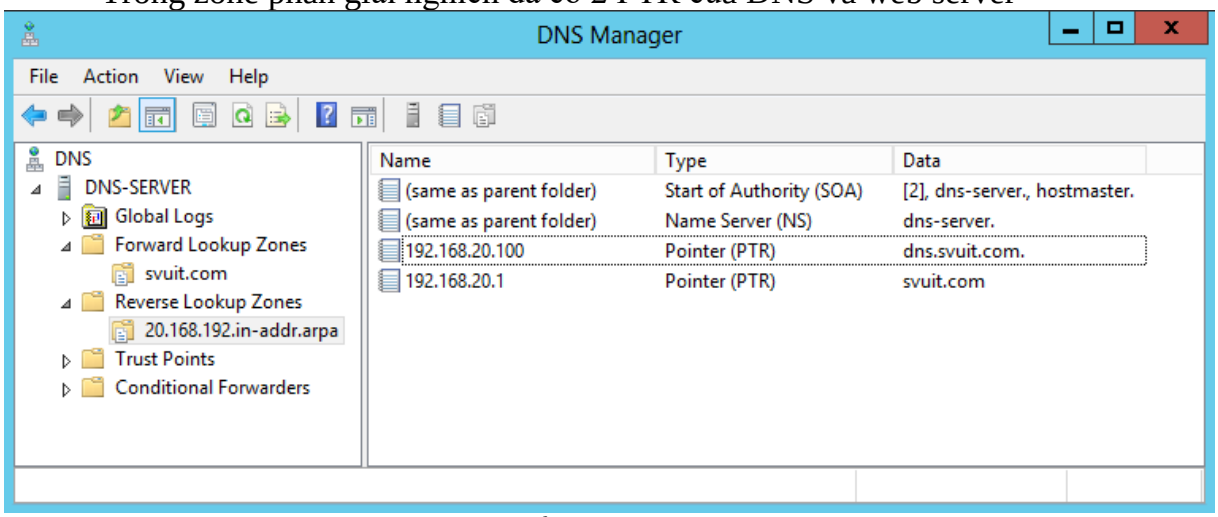
Bước 10: Xác nhận hoàn thành phân giải nghịch



Hình 2.25 Cửa sổ hoàn thành phân giải nghịch

Bước 11: Kiểm tra kết quả trong zone phân giải nghich

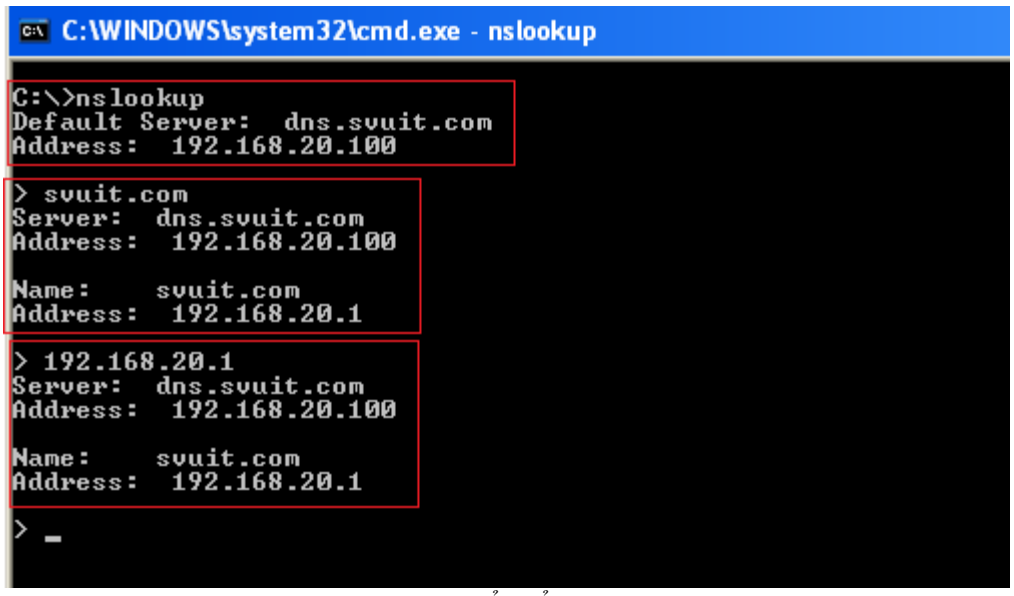
Trong zone phân giải nghich đã có 2 PTR của DNS và web server



Hình 2.26 Cửa sổ tạo zone phân giải nghich

Bước 12: Kiểm tra kết quả phân giải nghịch trên máy client

Qua máy client và tiến hành **nslookup** xem DNS đã thực hiện phân giải nghich



Hình 2.27 Cửa sổ kiểm tra trên client

Bài tập thực hành của học viên

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

Hướng dẫn thực hiện

Bài tập 1 xem chi tiết tại mục 8.1

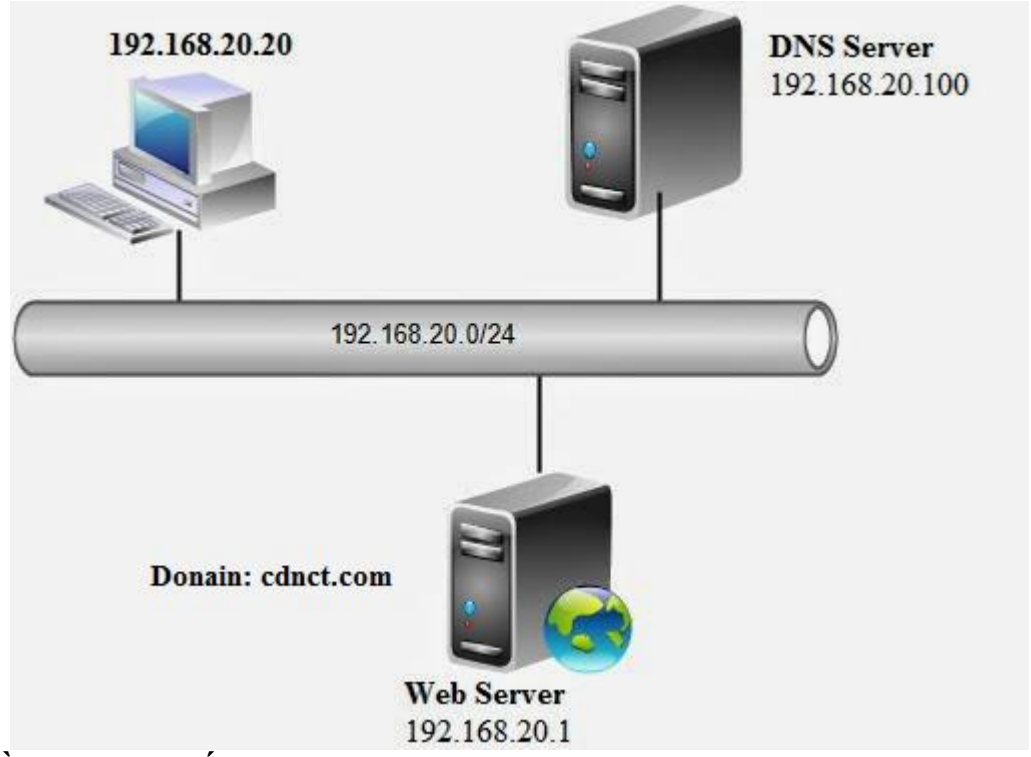
Bài tập 2 xem chi tiết tại mục 8.2

Những trọng tâm cần chú ý:

- Thiết lập địa chỉ IP cho đúng với hệ thống yêu cầu
- Mạng trong hệ thống phải thông nhau
- Địa chỉ Preferred DNS của các máy trên hệ thống là địa chỉ của máy DNS server
- Phải có tên miền để thiết lập DNS Server.
- Thiết lập được SOA phù hợp hệ thống
- Tạo Host phải dúng theo yêu cầu (A: dùng cho IPv4 và AAA: dùng cho IPv6)
- Thao tác phải đúng các bước cài đặt và cấu hình DNS Server trên Windows server 2019.

Bài mở rộng và nâng cao

Hãy cài đặt cấu hình DNS server trên Windows Server 2019 theo mô hình sau:



Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được Cơ chế phân giải tên của DNS trong Windows Server
  + Trình bày được các bước cài đặt và cấu hình DNS trong Windows Server 2019
- Về kỹ năng:
  + Thao tác thành thạo việc cài đặt và cấu hình DNS trên Windows Server 2019.
  + Thực hiện đúng phân giải thuận: Tạo zone, tạo các Records sao cho client truy cập vào cdnct.com và www.cdnct.com trên Windows Server 2019
  + Thực hiện phân giải nghịch: Sao cho client sử dụng nslookup các IP của web server, DNS... thì biết tên của các server này
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng: Đánh giá kỹ năng thực hành về các thao tác cài đặt và cấu hình NDS theo yêu cầu trên Windows Server 2019.
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 3: DỊCH VỤ THƯ MỤC (ACTIVE DIRECTORY)
Mã bài: MĐ 17 - 03

Mục tiêu của bài học:
- Trình bày được cấu trúc của Active Directory trên windows server;
- Cài đặt và cấu hình được máy điều khiển vùng.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Active Directory

Mục tiêu:

- Trình bày được cấu trúc của Active Directory trên windows server

1.1. 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.

1.2. Chức năng của Active Directory

- Lưu giữ một danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.
- Cung cấp một **Server** đóng vai trò chứng thực (**authentication server**) hoặc **Server** quản lý đăng nhập (**logon Server**), **Server** này còn gọi là **domain controller** (máy điều khiển vùng).
- Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (**index**) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng
- Cho phép chúng ta tạo ra những tài khoản người dùng với những mức độ quyền (**rights**) khác nhau như: toàn quyền trên hệ thống mạng, chỉ có quyền **backup** dữ liệu hay **shutdown Server** từ xa…
- Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (**subdomain**) hay các đơn vị tổ chức **OU** (**Organizational Unit**). Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

1.3. Directory Services

1.3.1. 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**.

1.3.2. 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. Có ba loại vật chứa là:

- **Domain**: khái niệm này được trình bày chi tiết ở phần sau.
- **Site**: một **site** là một vị trí. **Site** được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ, công ty XYZ có tổng hành dinh đặt ở **San Fransisco**, một chi nhánh đặt ở **Denver** và một văn phòng đại diện đặt ở **Portland** kết nối về tổng hành dinh bằng **Dialup Networking**. Như vậy hệ thống mạng này có ba **site**.
- **OU (Organizational Unit):** là một loại vật chứa mà bạn có thể đưa vào đó người dùng, nhóm, máy tính và những **OU** khác. Một **OU** không thể chứa các đối tượng nằm trong domain khác. Nhờ việc một **OU** có thể chứa các **OU** khác, bạn có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hoá cấu trúc của một tổ chức bên trong một domain. Bạn nên sử dụng **OU** để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.

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. Việc tìm kiếm được thực hiện xa hơn những gì đã có trong **Windows NT** và không chỉ có thể định vị được đối tượng bằng tên mà có thể bằng cả những thuộc tính của đối tượng.
- Giả sử bạn phải in một tài liệu dày 50 trang thành 1000 bản, chắc chắn bạn sẽ không dùng một máy in **HP Laserjet 4L**. Bạn sẽ phải tìm một máy in chuyên dụng, in với tốc độ 100ppm và có khả năng đóng tài liệu thành quyển. Nhờ **Global Catalog**, bạn tìm kiếm trên mạng một máy in với các thuộc tính như vậy và tìm thấy được một máy **Xerox Docutech 6135**. Bạn có thể cài đặt **driver** cho máy in đó và gửi **print job** đến máy in. Nhưng nếu bạn ở **Portland** và máy in thì ở **Seattle** thì sao? **Global Catalog** sẽ cung cấp thông tin này và

bạn có thể gửi **email** cho chủ nhân của máy in, nhờ họ in giùm.

- Một ví dụ khác, giả sử bạn nhận được một thư thoại từ một người tên **Betty Doe** ở bộ phận kế toán. Đoạn thư thoại của cô ta bị cắt xén và bạn không thể biết được số điện thoại của cô ta. Bạn có thể dùng **Global Catalog** để tìm thông tin về cô ta nhờ tên, và nhờ đó bạn có được số điện thoại của cô ta.
- 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.

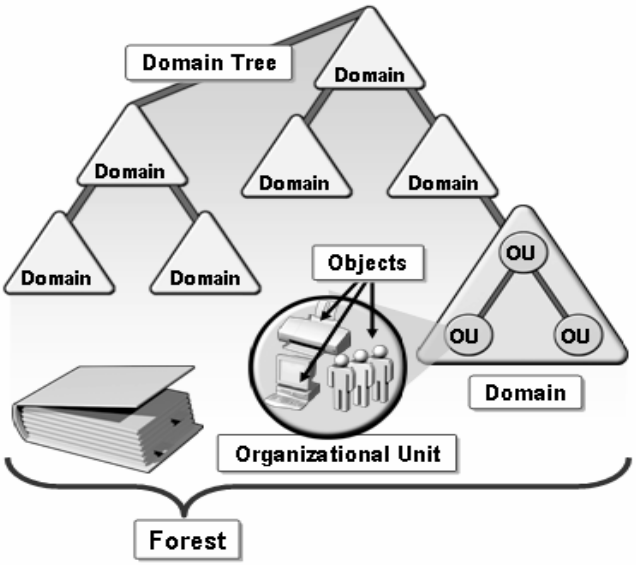
2. Các thành phần của AD

Mục tiêu:

- Trình bày được các thành phần của Active Directory.

2.1. Cấu trúc AD logic

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 Cấu trúc AD logic

2.1.1. 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**), các chính sách nhóm này chúng ta sẽ tìm hiểu ở các chương sau.

2.1.2. 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:

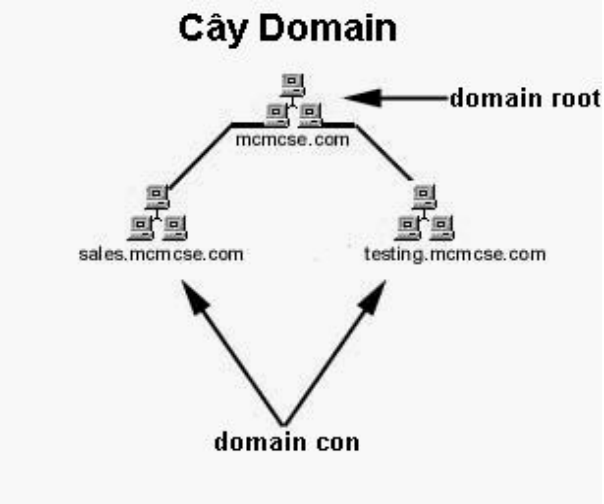
- Đóng vai trò như một khu vực quản trị (**administrative boundary**) các đối

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 đảm bảo các thông tin trên các **Server** này được được đồng bộ với nhau.

2.1.3 Domain Tree

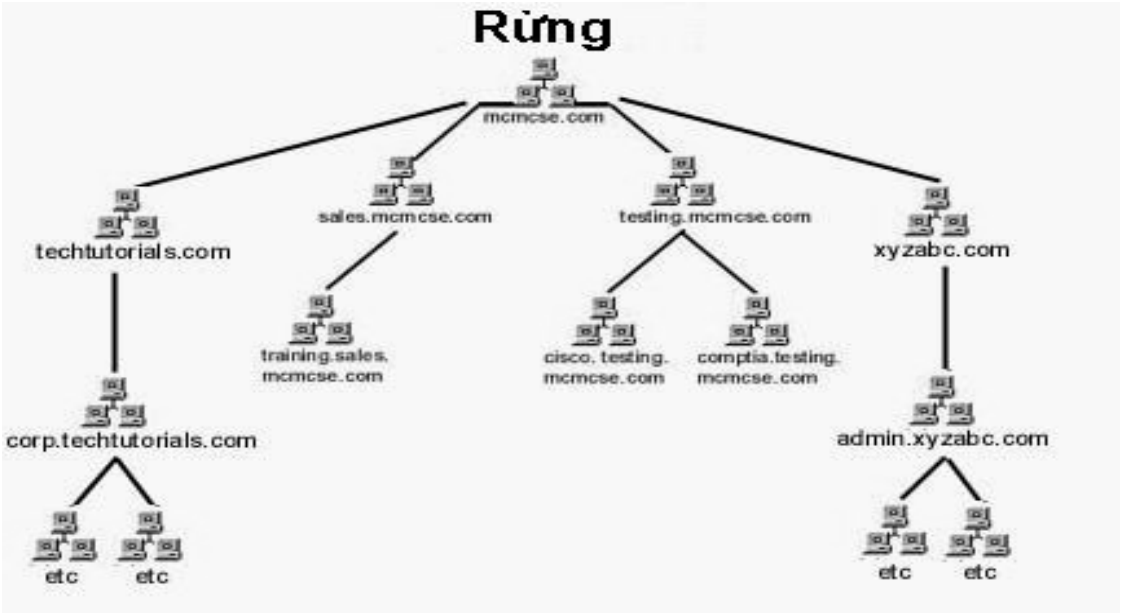
Domain Tree là cấu trúc bao gồm nhiều **domain** được sắp xếp có cấp bậc theo cấu trúc hình cây. **Domain** tạo ra đầu tiên được gọi là **domain root** và nằm ở gốc của cây thư mục. Tất cả các **domain** tạo ra sau sẽ nằm bên dưới **domain root** và được gọi là **domain** con (**child domain**). Tên 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.



Hình 3.2 cây Domain

2.1.4. 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



Hình 3.3. Rừng Domain

Trong ví dụ trên, công ty mcmcse.com thu mua được techtutorials.com và xyzabc.com và hình thành rừng từ gốc mcmcse.com

2.2. Cấu trúc AD vật lý

Gồm: sites và domain controllers.

- Địa bàn (site): là tập hợp của một hay nhiều mạng con kết nối với nhau, tạo điều kiện truyền thông qua mạng dễ dàng, ấn định ranh giới vật lý xung quanh các tài nguyên mạng.
- Điều khiển vùng (domain controllers): là máy tính chạy Windows Server chứa bản sao dữ liệu vùng. Một vùng có thể có một hay nhiều điều khiển vùng. Mỗi sự thay đổi dữ liệu trên một điều khiển vùng sẽ được tự động cập nhật lên các điều khiển khác của vùng.

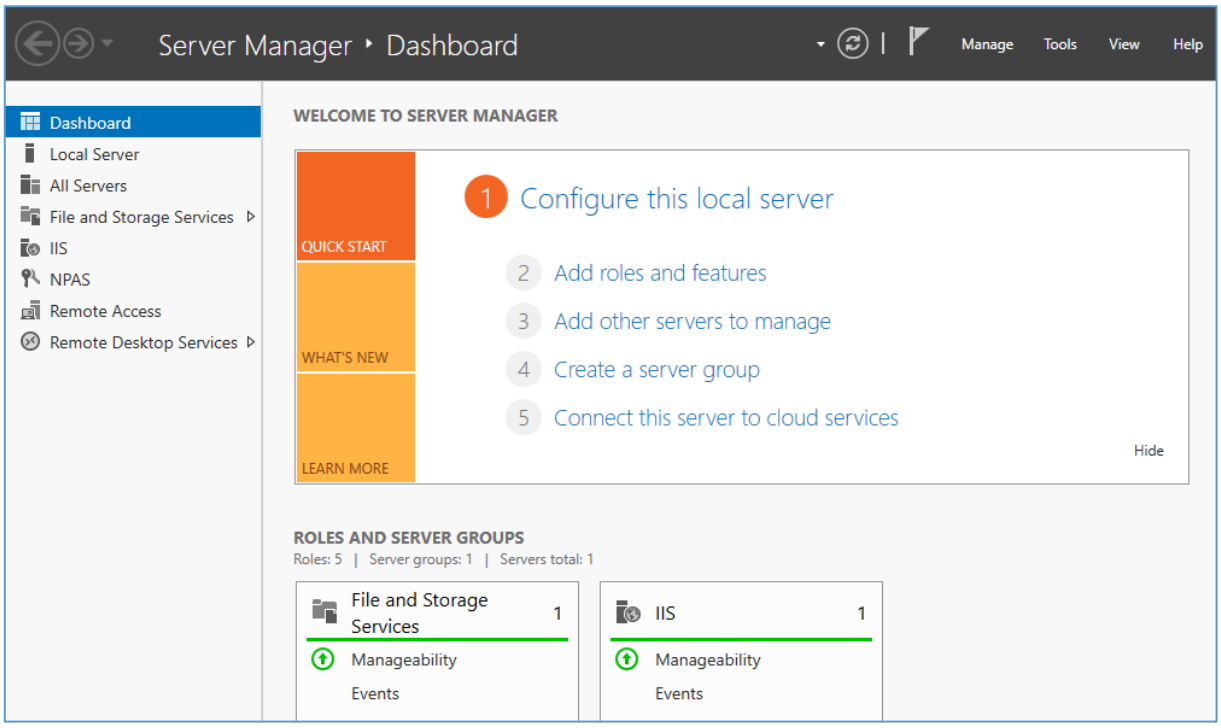
3. Cài đặt và cấu hình active directory

Mục tiêu:

- Cài đặt và cấu hình được máy điều khiển vùng.
- Gia nhập máy trạm vào máy điều khiển vùng (join domain)

3.1. Nâng cấp Server thành Domain Controller(DC)

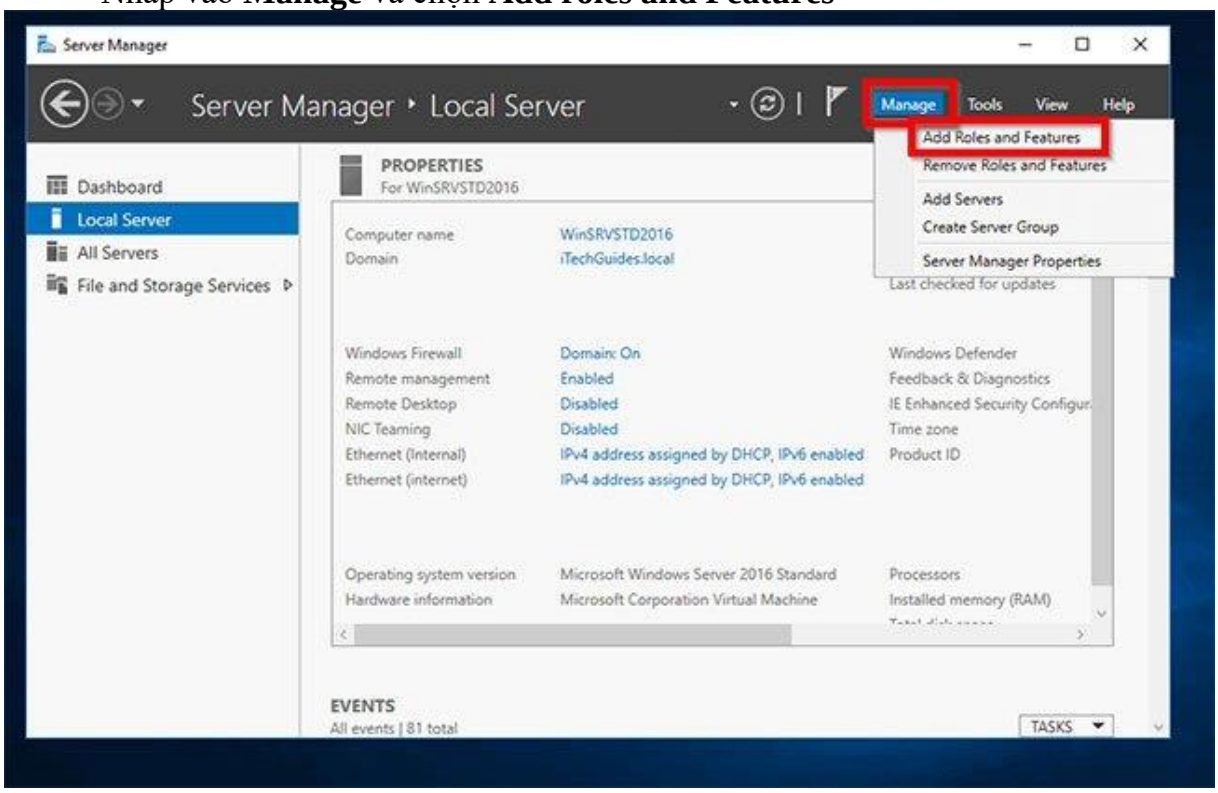
Bước 1: Đăng nhập vào server bạn muốn cài đặt Active Directory



Hình 3.4 Đăng nhập Server manager

Bước 2: Mở Add roles and Features

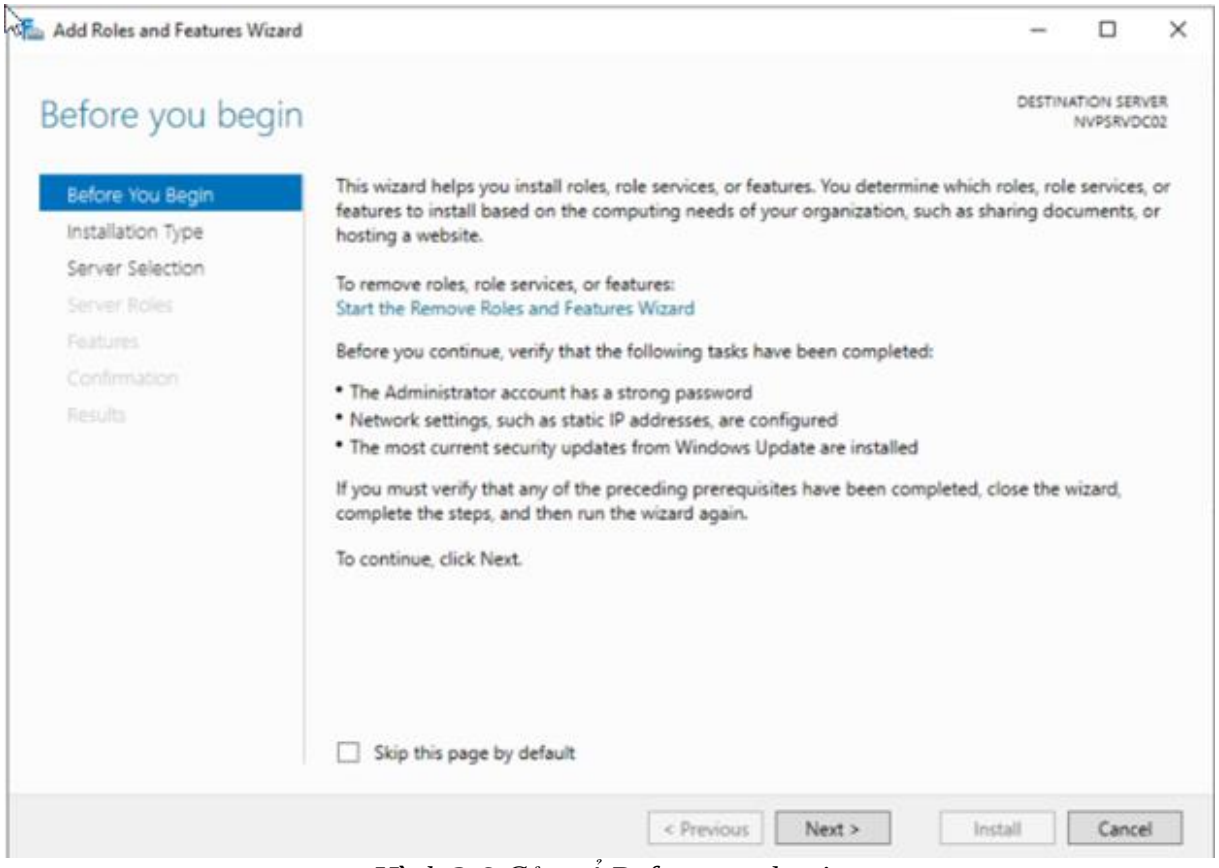
Nhấp vào **Manage** và chọn **Add roles and Features**



Hình 3.5 Mở Add roles and Features

Bước 3: Thực hiện theo wizard next

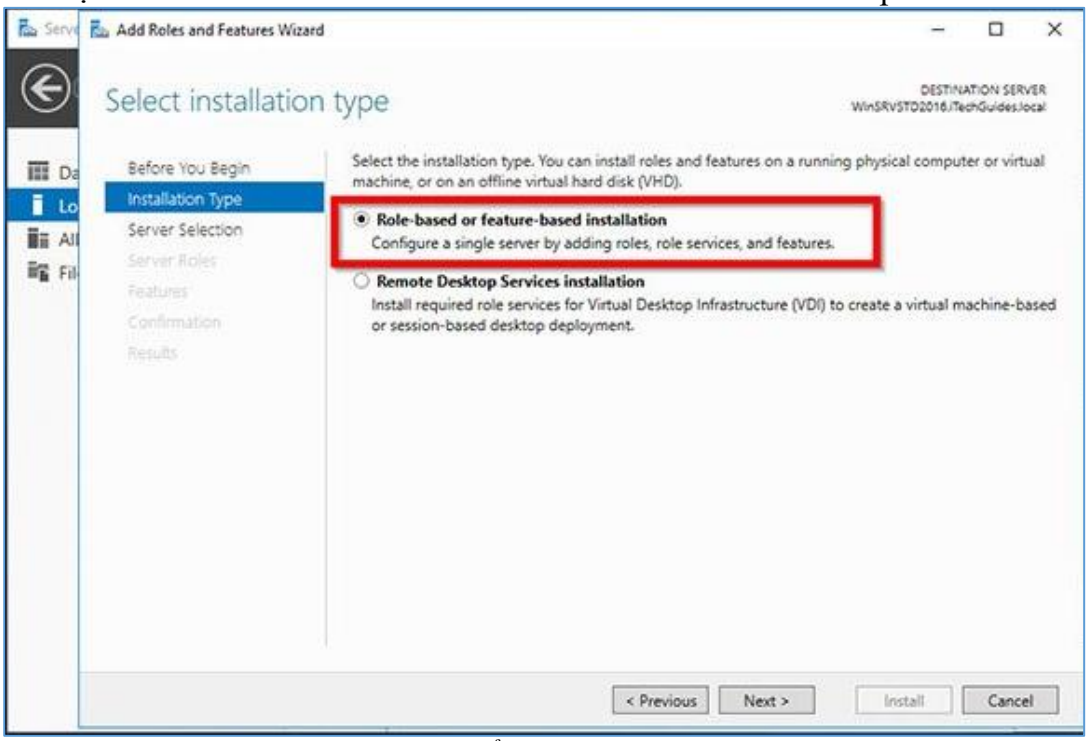
Chọn **Role-based or feature-based installation**. Sau đó nhấp vào **Next.**



Hình 3.6 Cửa sổ Before you begin

Bước 4: Chọn loại hình cài đặt

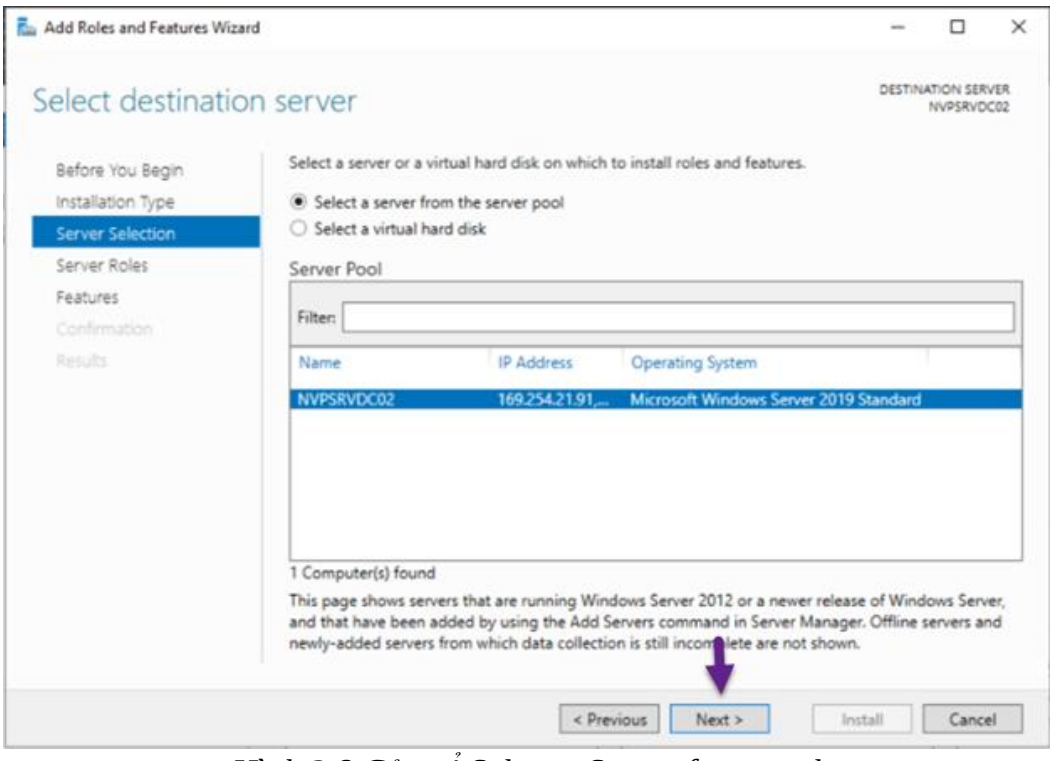
Chọn **Role-based or feature-based installation**. Sau đó nhấp vào **Next.**



Hình 3. 7 Cửa sổ Select installation type

Bước 5: Chọn Server mặc định

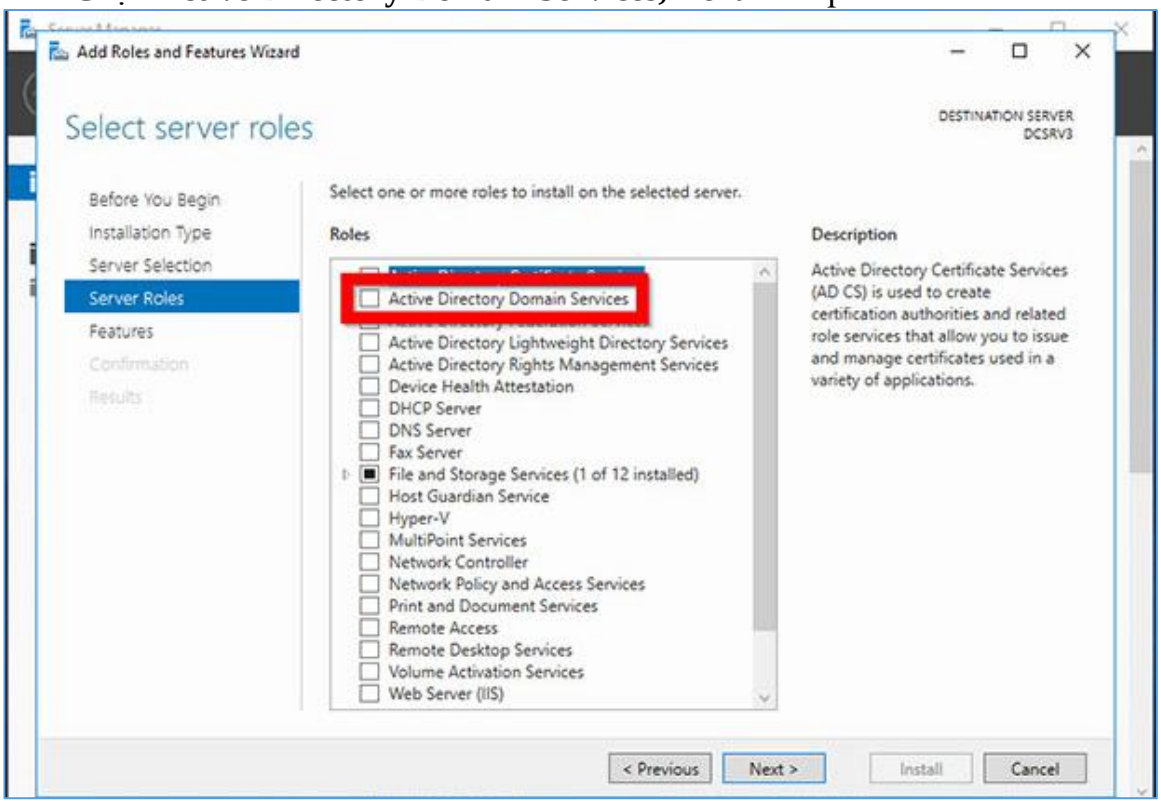
Chọn Select a Server from pool để mặc định đang chọn server ví dụ NVPSRVDC02



Hình 3.8 Cửa sổ Select a Server from pool

Bước 6: Chọn cách thức cài đặt

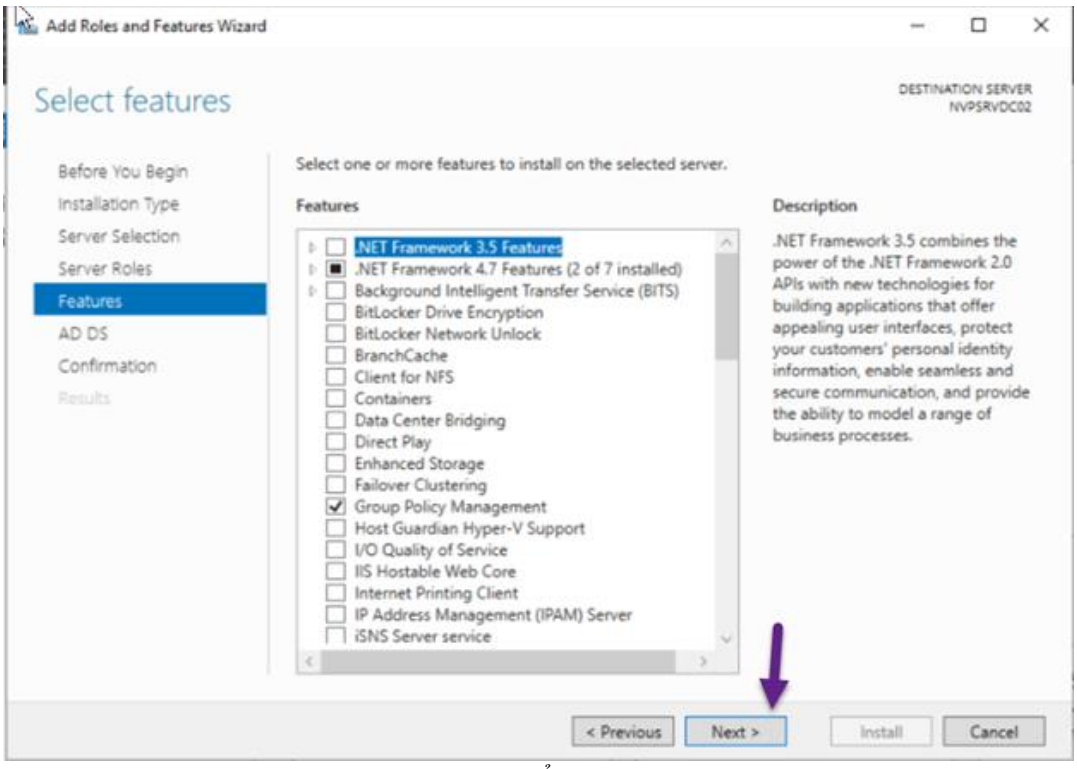
Chọn **Active Directory Domain Services,** Next để tiếp



Hình 3.9 Cửa sổ Select server roles

Bước 7: Chọn cách thức cài đặt cho AD

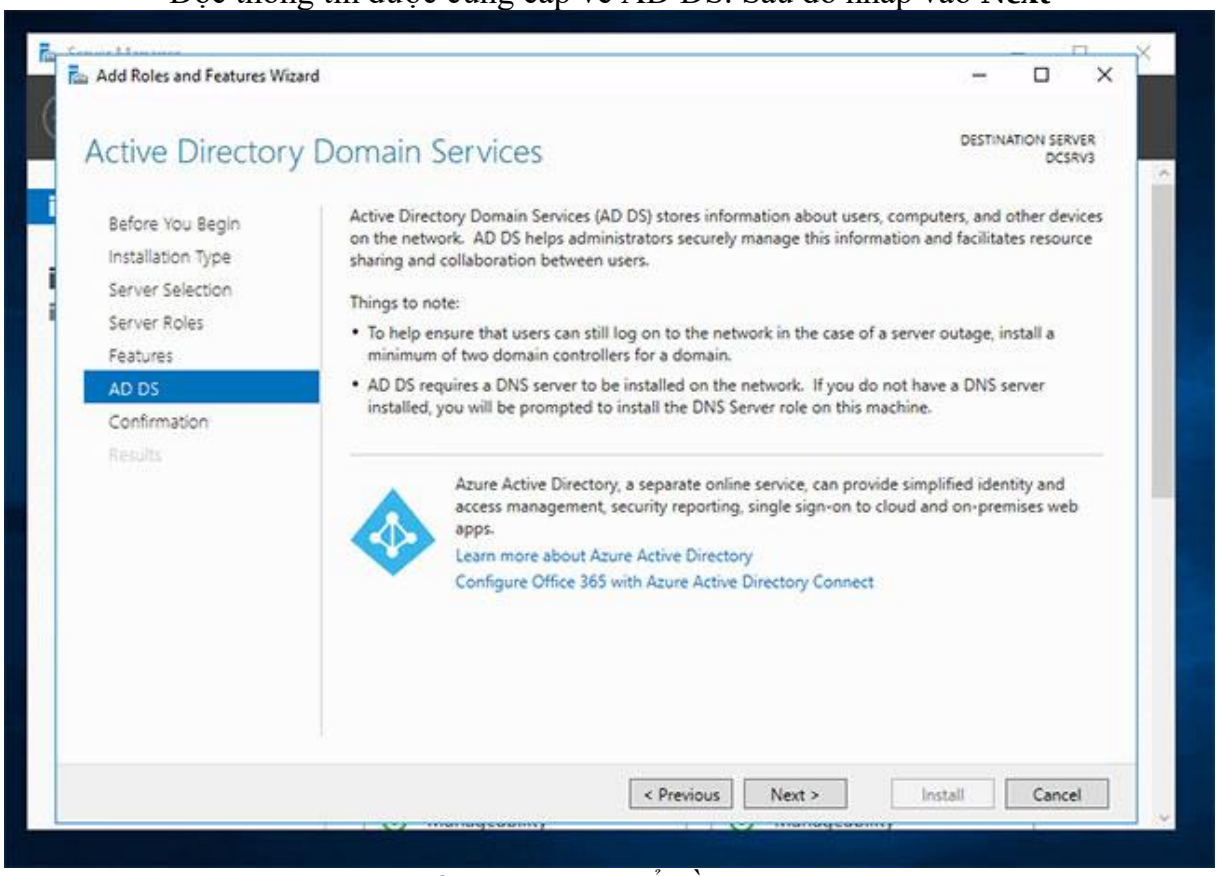
Tại Select Features-> để mặc định chọn next



Hình 3.10 Cửa sổ Select Features

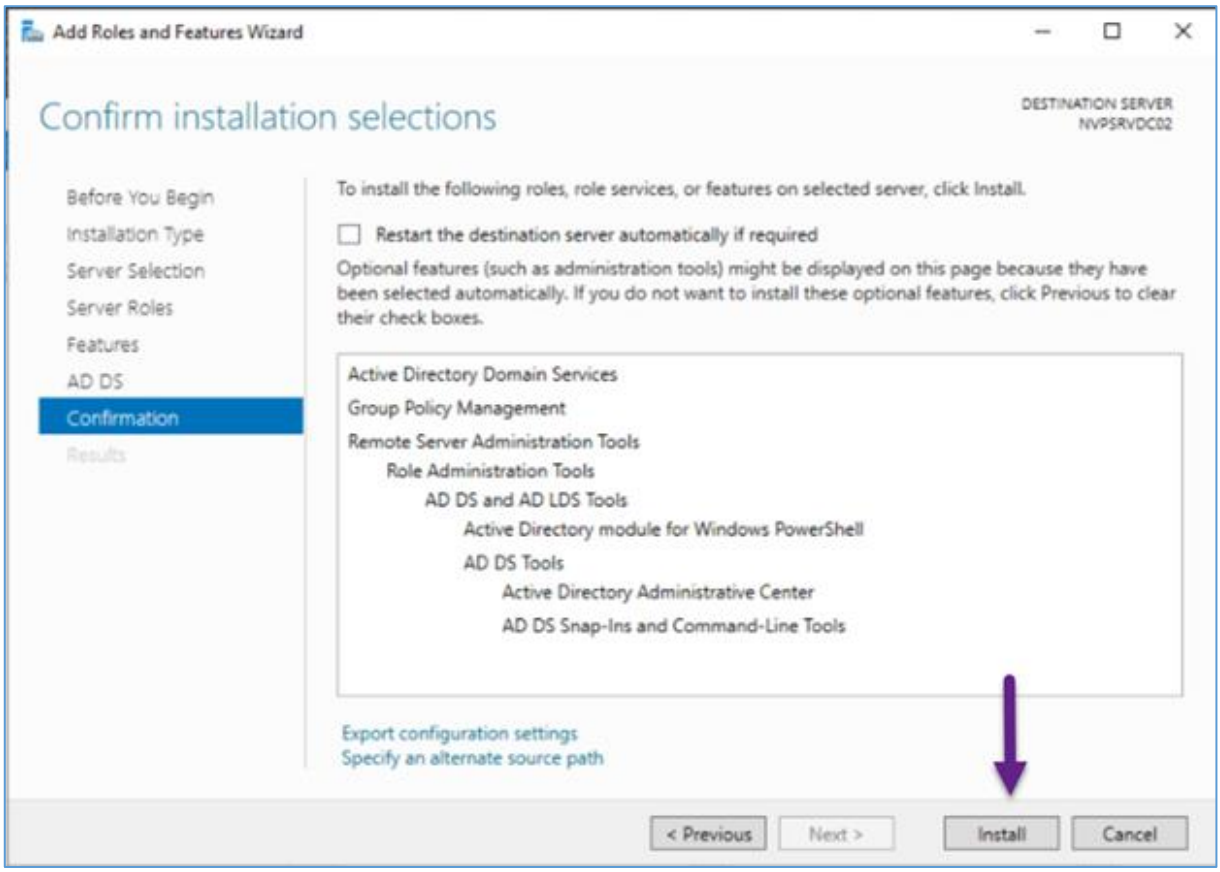
Bước 8: Chấp nhận thông tin về AD DS

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



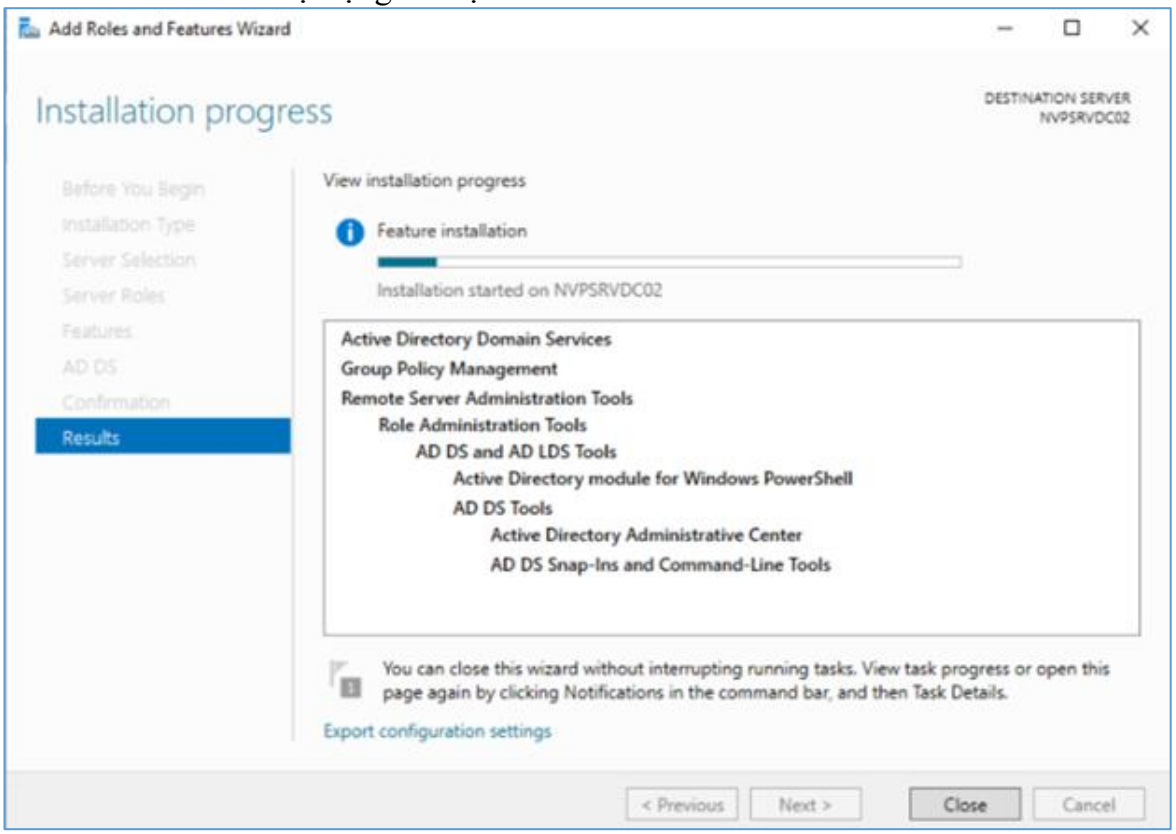
Hình 3.11 Cửa sổ về AD DS

Bước 9: Chọn Install để cài đặt



Hình 3.12 Cửa sổ cài đặt bắt đầu

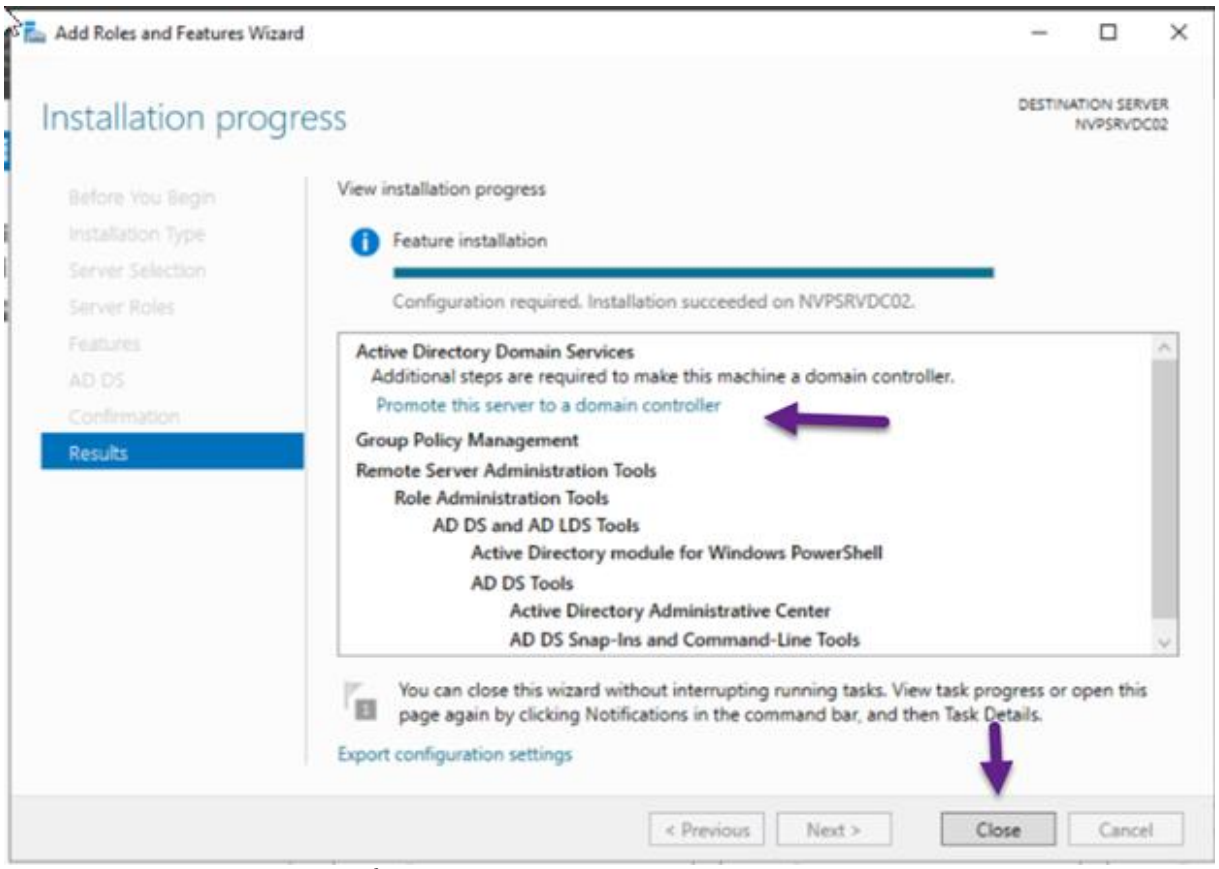
Bước 10: Chờ server tự động cài đặt ADDS



Hình 3.13 Cửa sổ Installtion progress

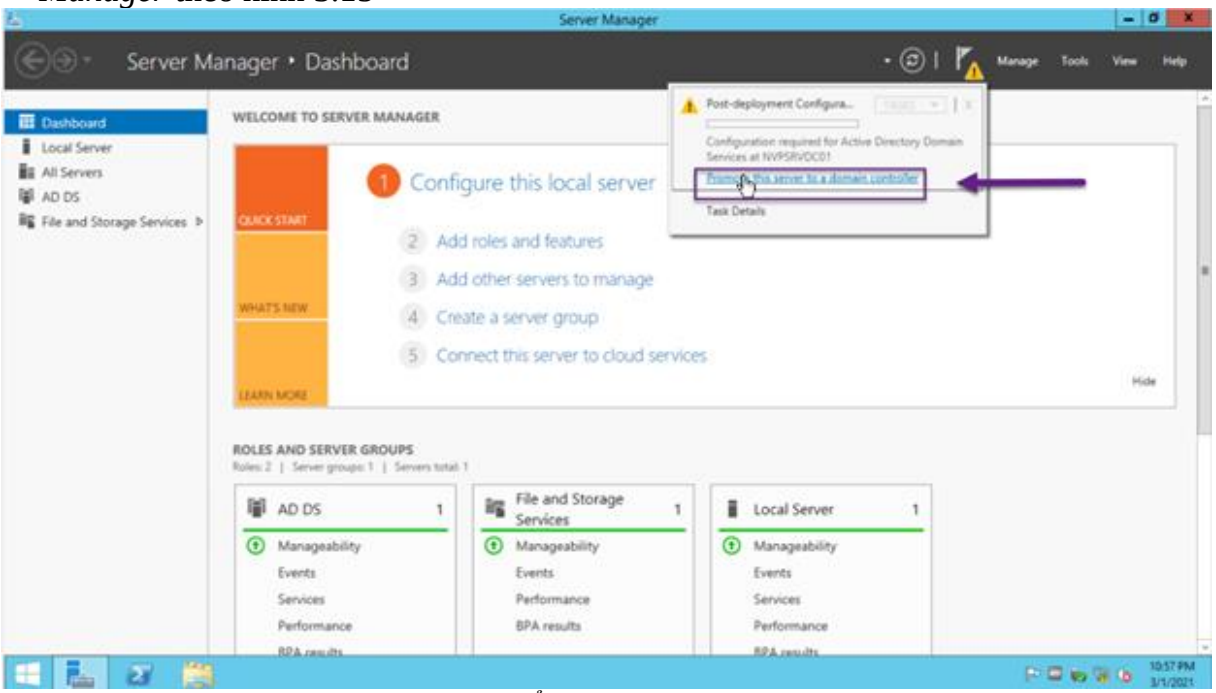
Bước 11: Tiến hành cài Domain Controler

- Cách 1: Chọn -> Promote This Server to a Domain Controller theo hình 3.14



Hình 3.14 Cửa sổ chọn Promote This Server to a Domain Controller

- Cách 2: Chọn -> Promote This Server to a Domain Controller *từ Server Manager* theo hình 3.15

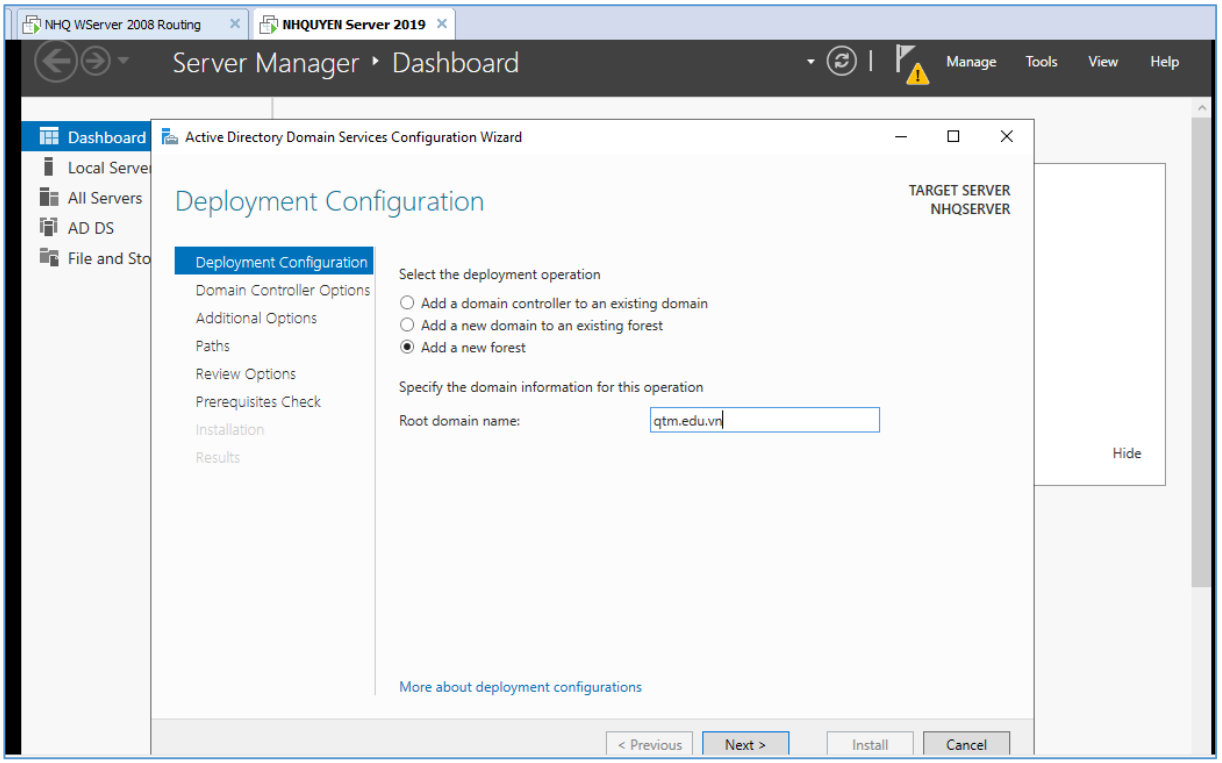


Hình 3.15 Cửa sổ cài đặt từ Server Manager

- Cách 3 Chọn start-> run->dcpromo.exe

Bước 12:

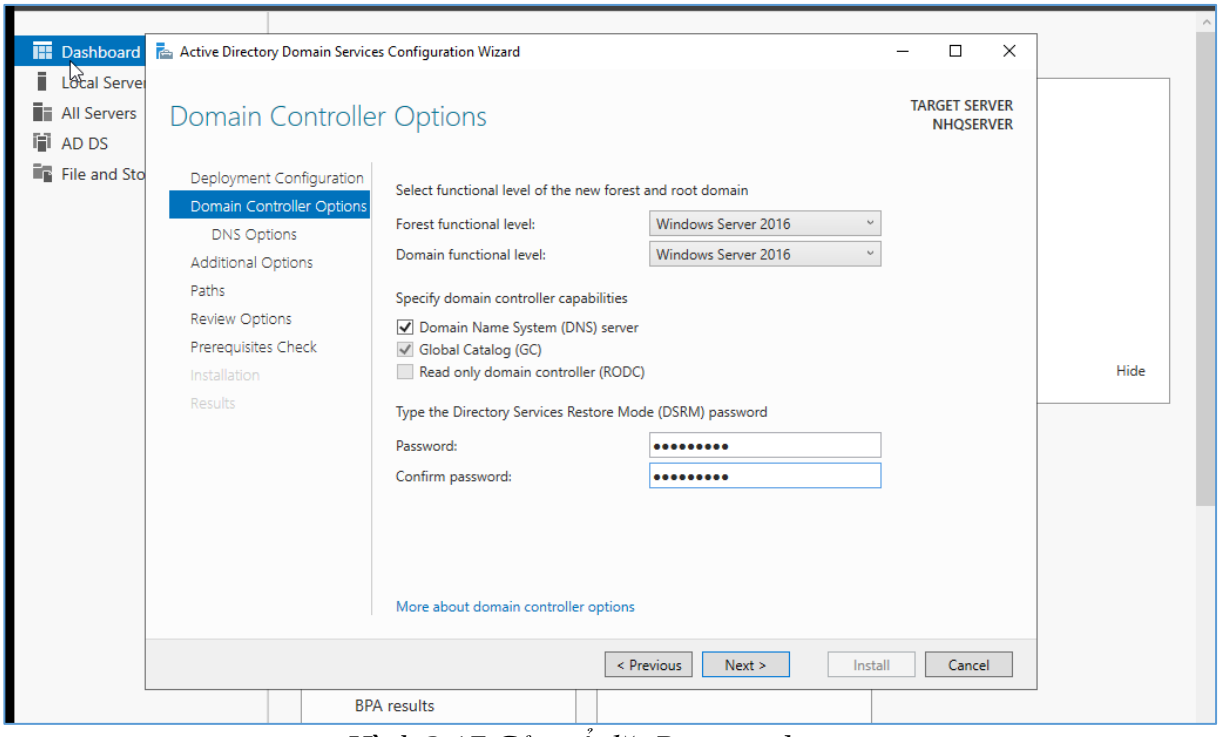
- Ở mục Deployment configuration chọn add a new forest
- Nhập tên Domain Controller vào Root domain name



Hình 3.16 Cửa sổ Deployment configuation

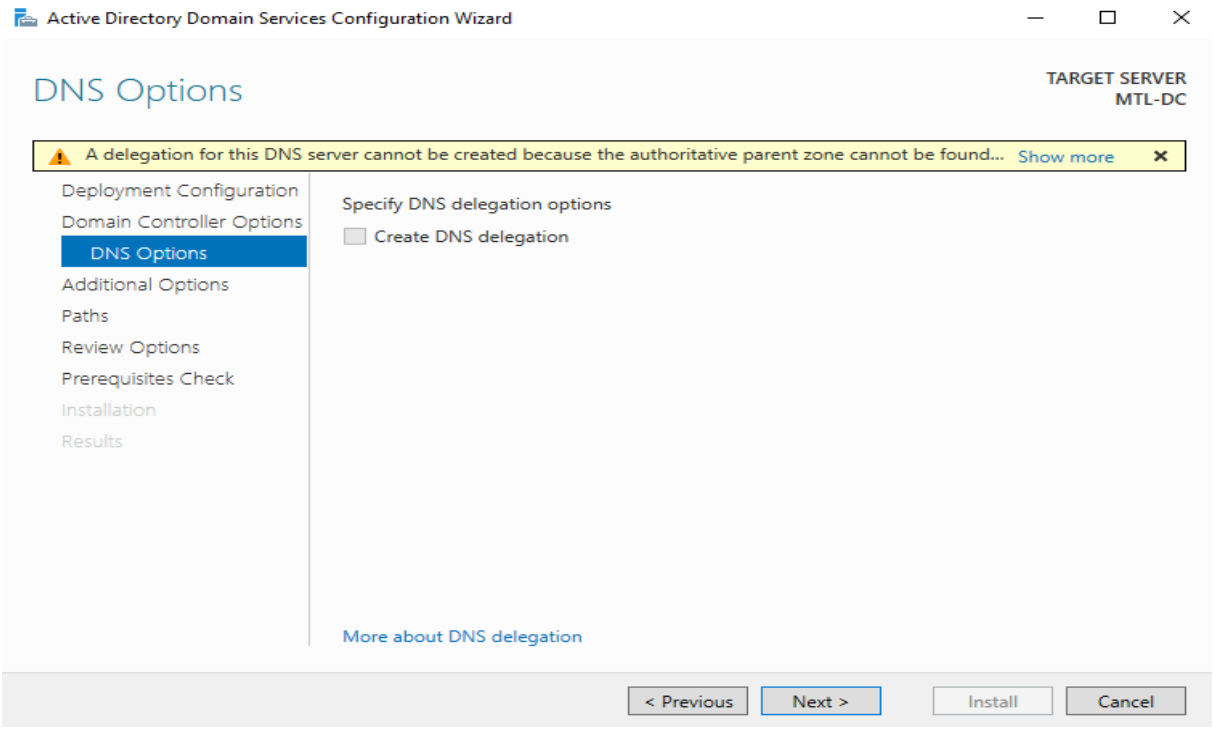
Bước 13: Chọn dòng Windows server và đặt Password nâng cấp Domain

Ở mục domain controller option nhập password để khi AD lỗi có thể truy cập chế độ restore DSRM



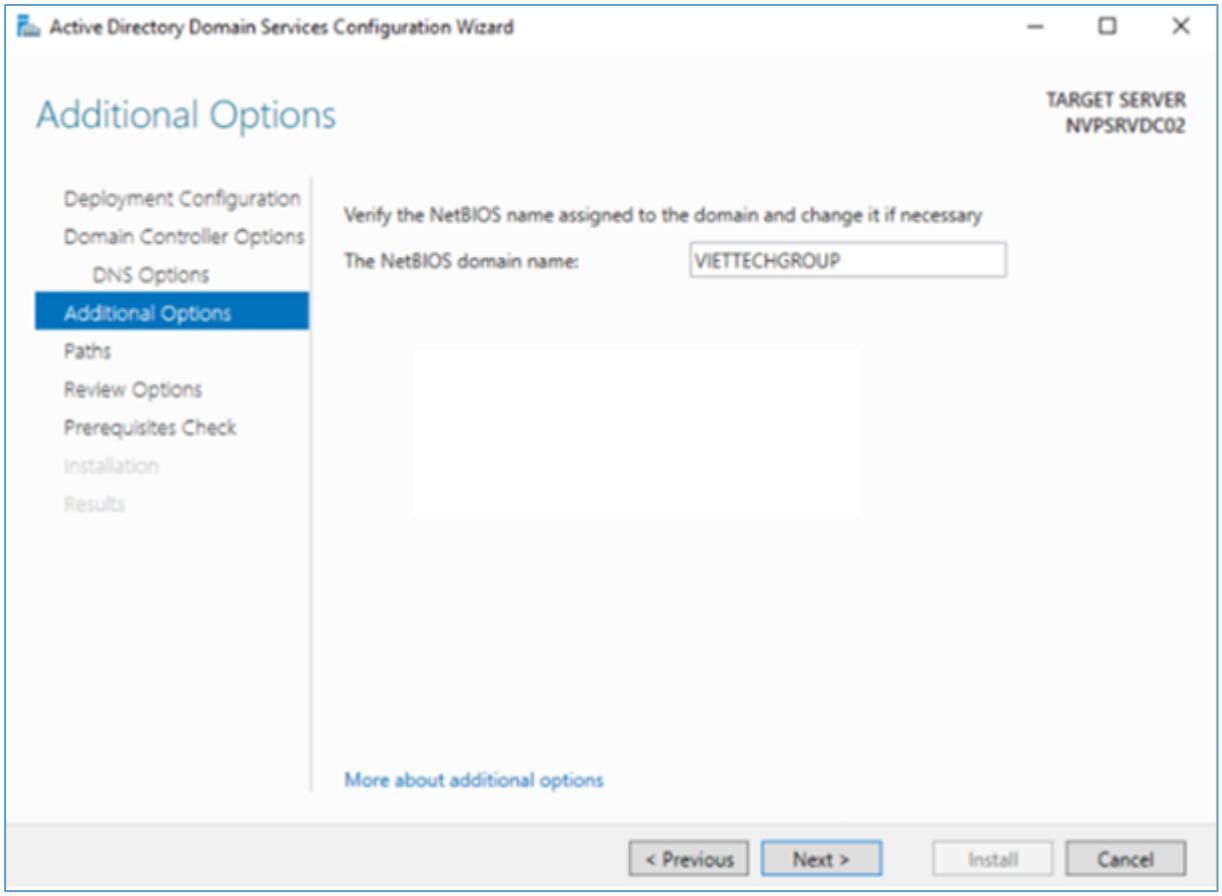
Hình 3.17 Cửa sổ đặt Password

Bước 14: Ở mục DNS Option, Additional option chúng ta ấn next và chọn install để tiến hành nâng cấp lên Domain controller



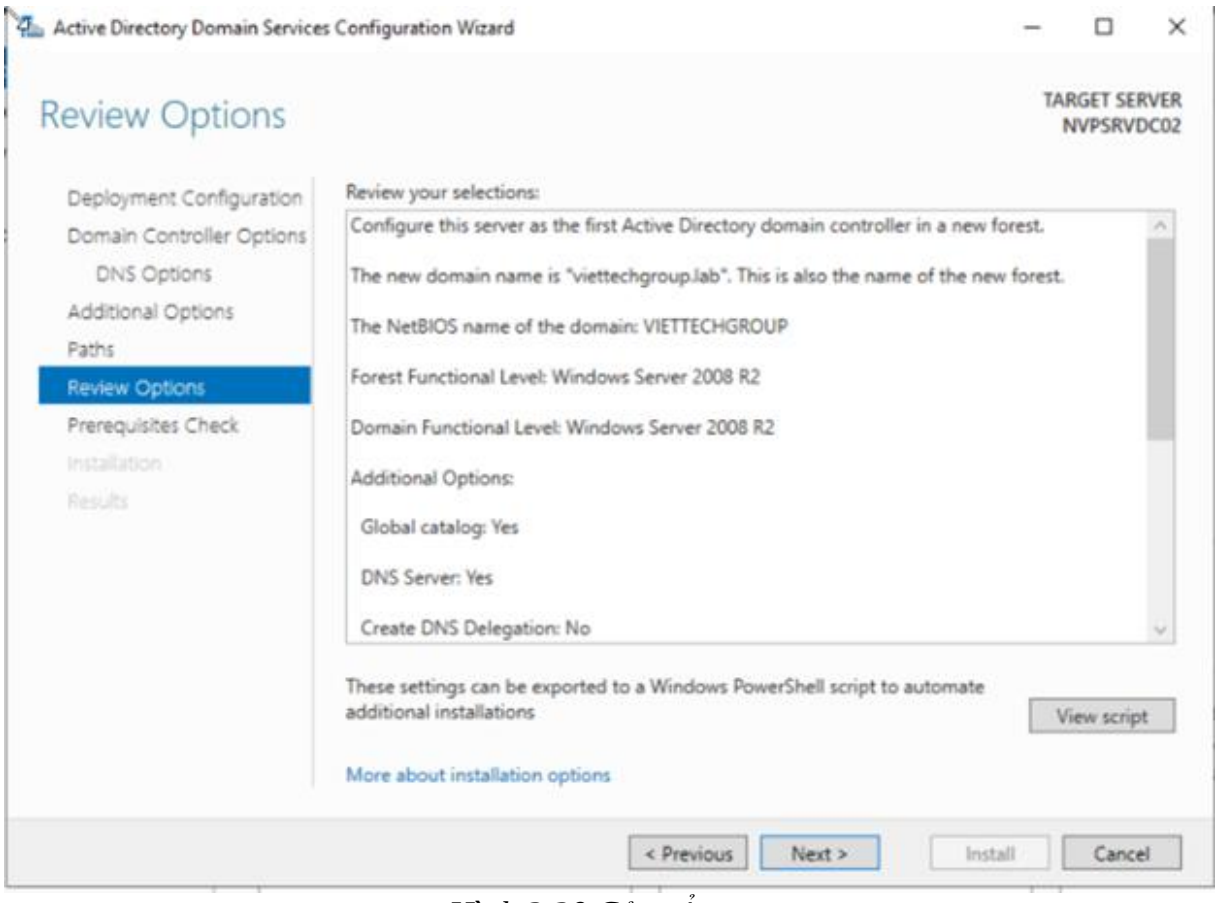
Hình 3.18 Cửa sổ

Bước 15: Chờ validate NetBios domain name



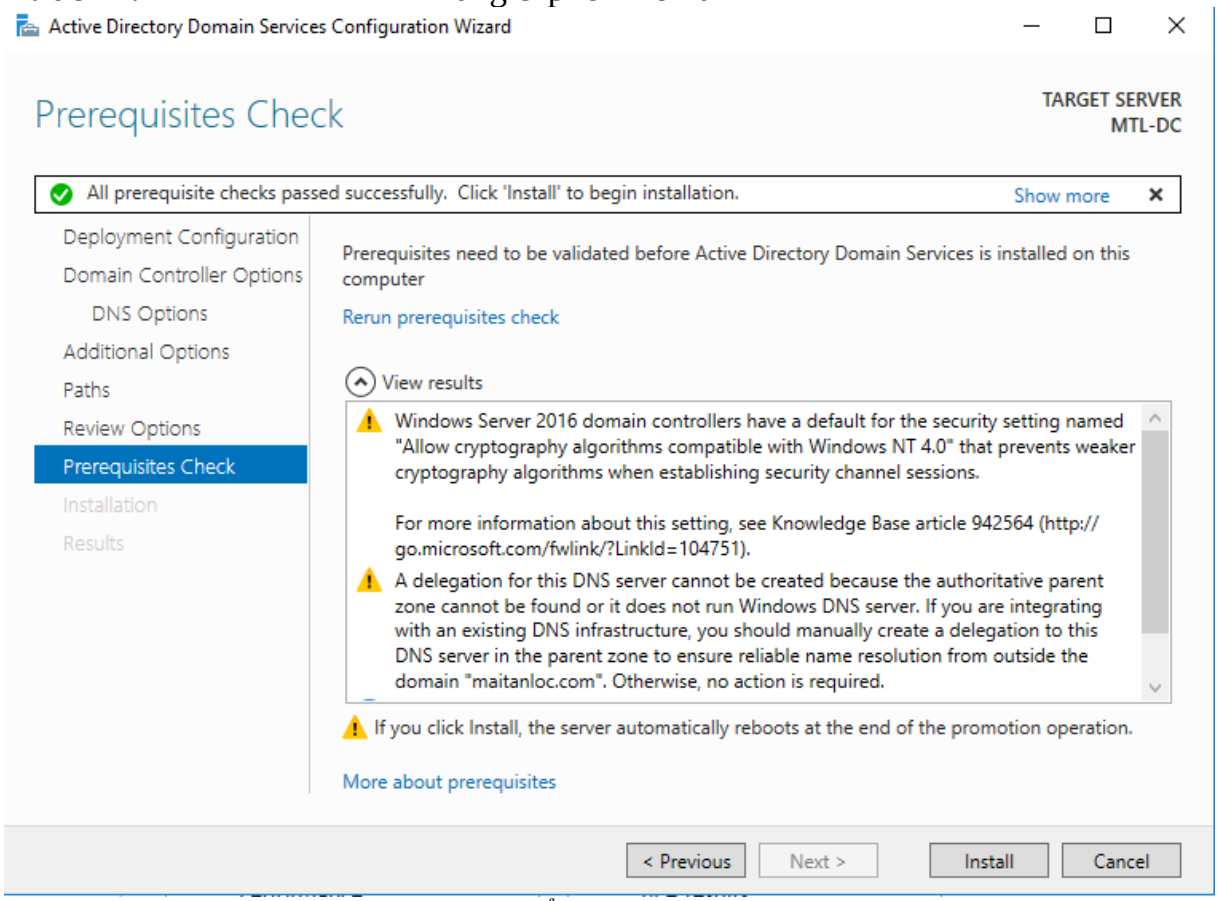
Hình 3.19 Cửa sổ Additional option

Bước 16: Để mặc định lưu trữ file



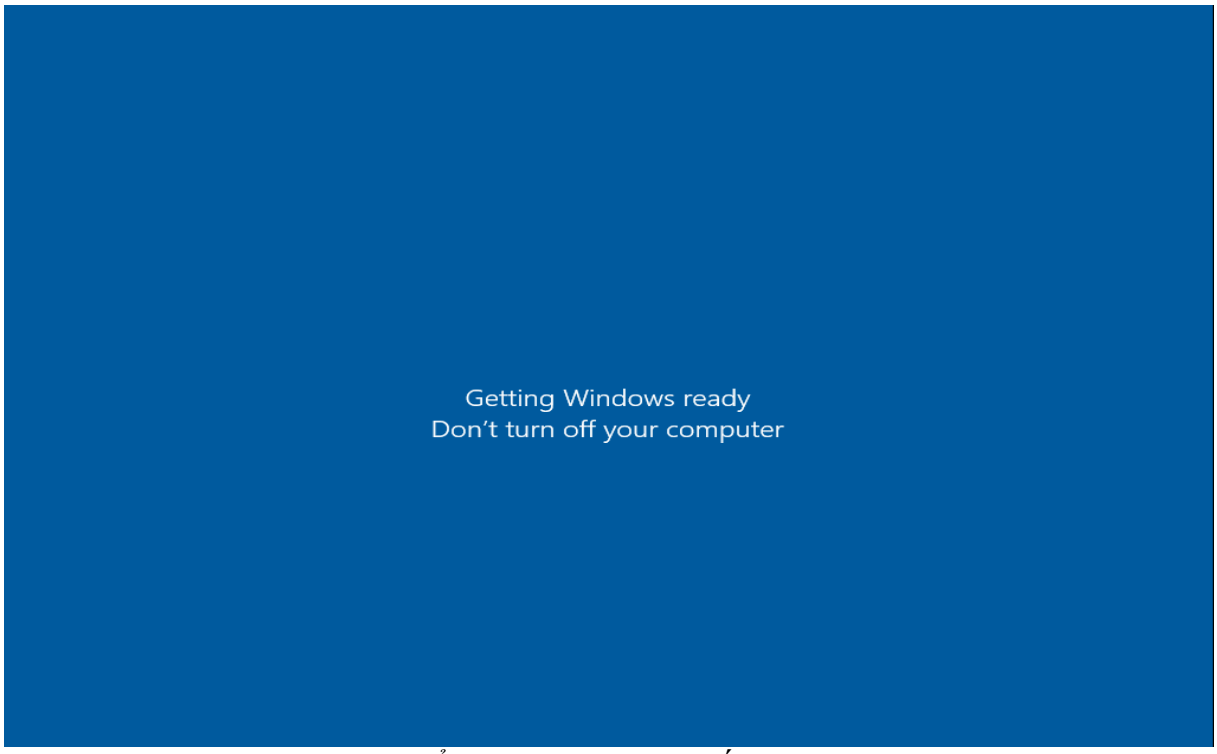
Hình 3.20 Cửa sổ

Bước 17: Click vào Install để nâng cấp lên Domain

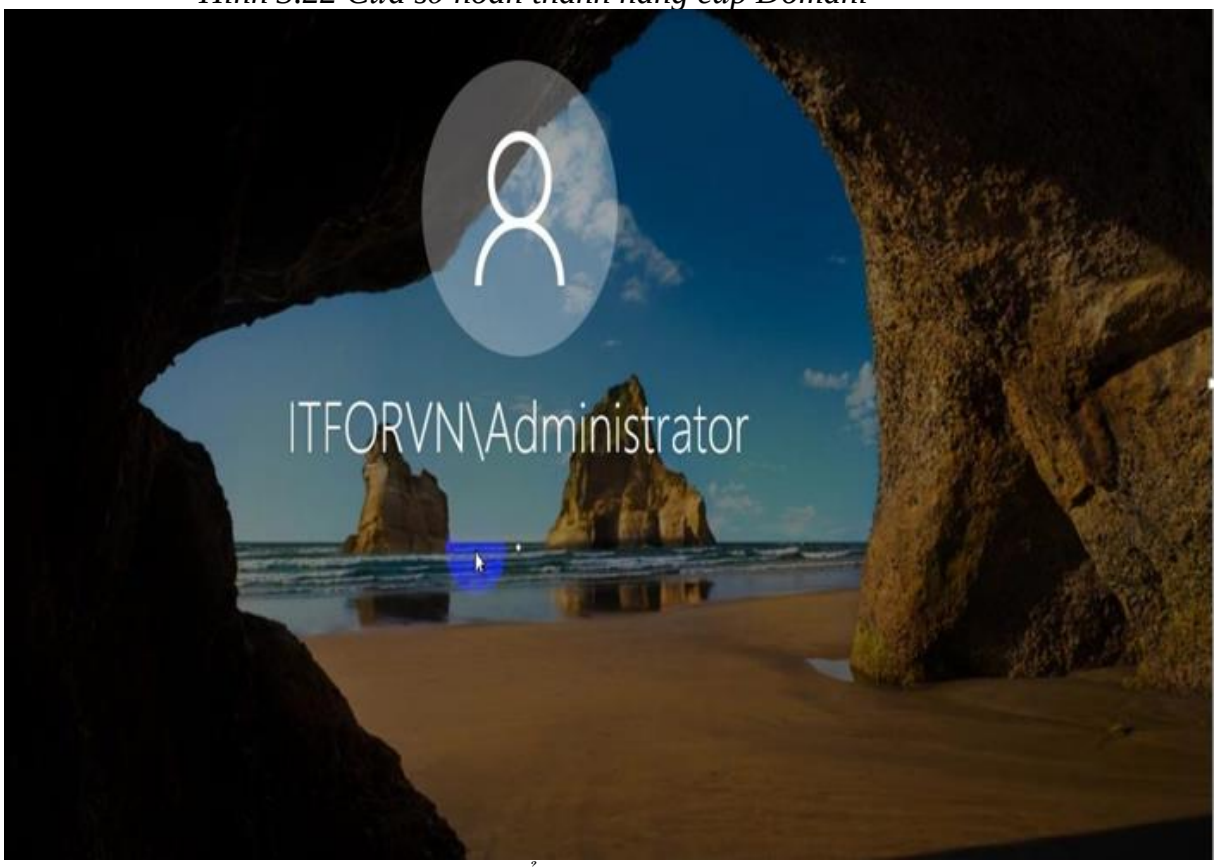


Hình 3.21 Cửa sổ Prerequisites check

Bước 18: Sau khi cài đặt xong máy sẽ tự động restart, khi đó lúc đăng nhập vào nó sẽ hiển thị là MAITANLOC\administrator thay vì chỉ administrator



Hình 3.22 Cửa sổ hoàn thành nâng cấp Domani

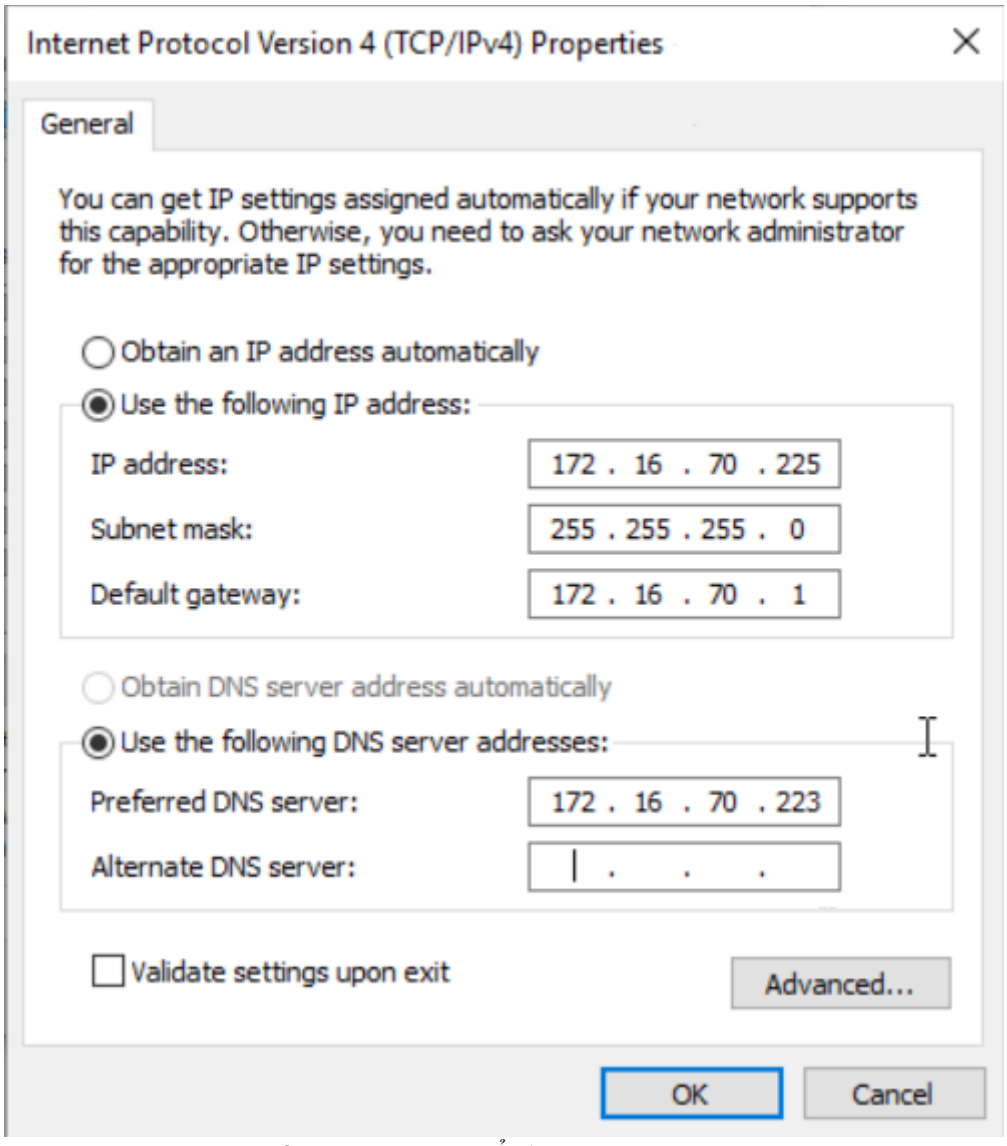


Hình 3.23 Cửa sổ đăng nhập có Domain

3.2. Gia nhập máy trạm vào Domain

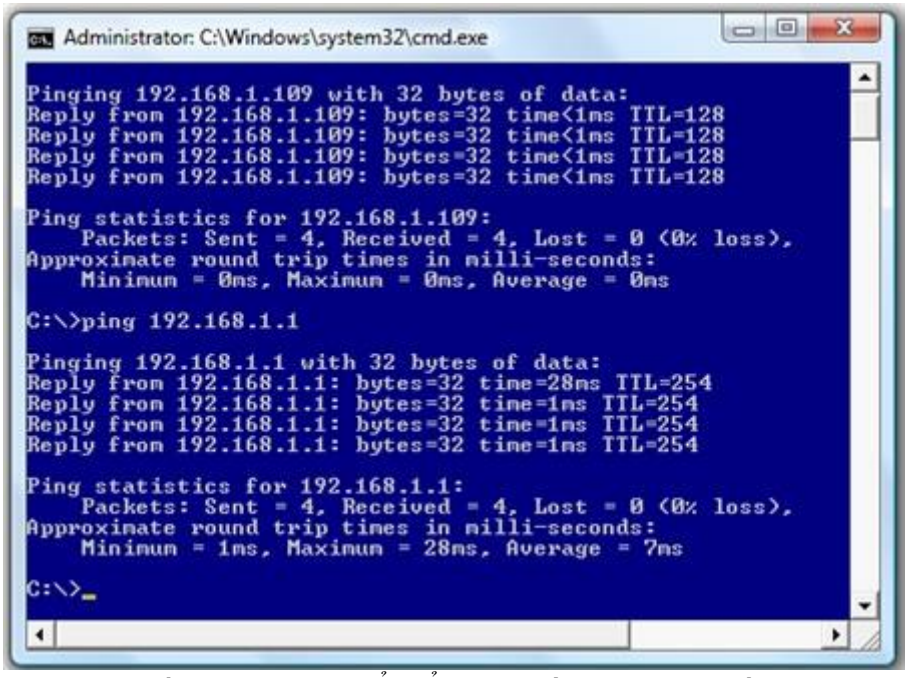
Bước 1: Định địa chỉ IP cho máy Client

Đầu tiên cấu hình lại địa chỉ IP. Ở phần DNS, nhập địa chỉ IP của domain controller ví dụ: 172.16.70.223



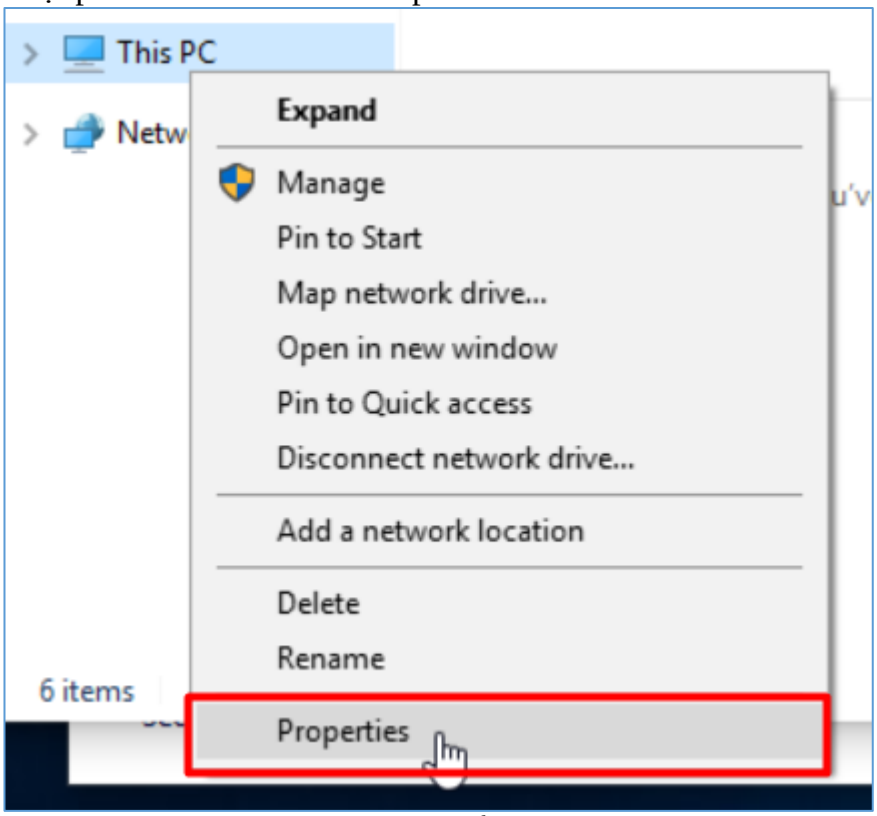
Hình 3.24 Cửa sổ đặt IP cho Client

Bước 2: Ping kiểm tra Client và DC có thông nhau không



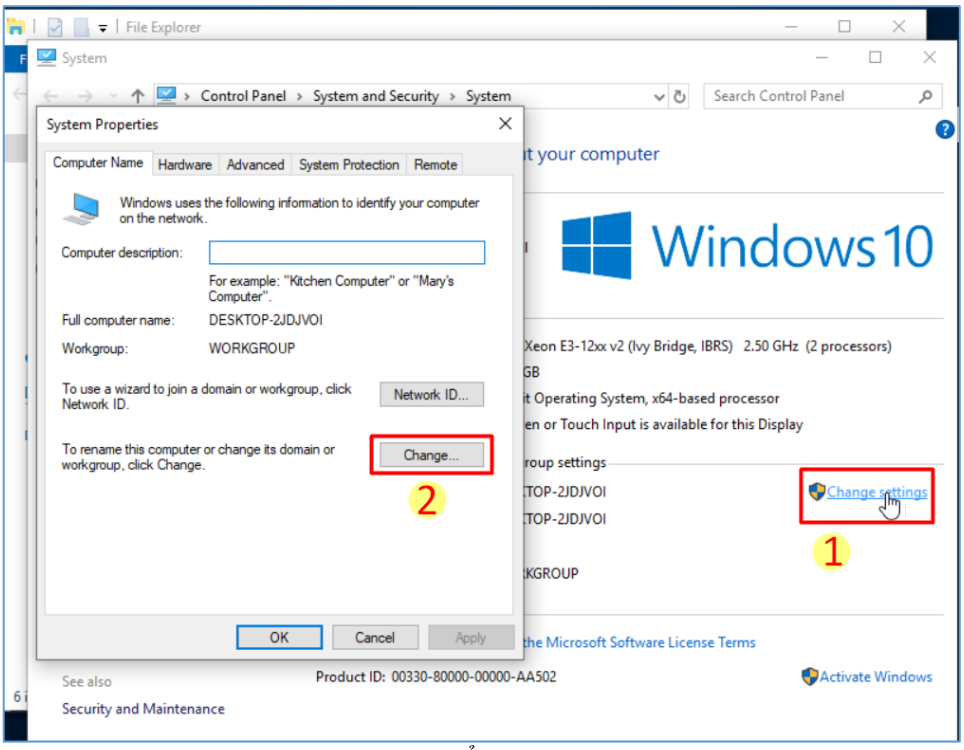
Hình 3.25 Cửa sổ kiểm tra thông nhau 2 máy

Bước 3: Chuột phải vào This PC -> Properties



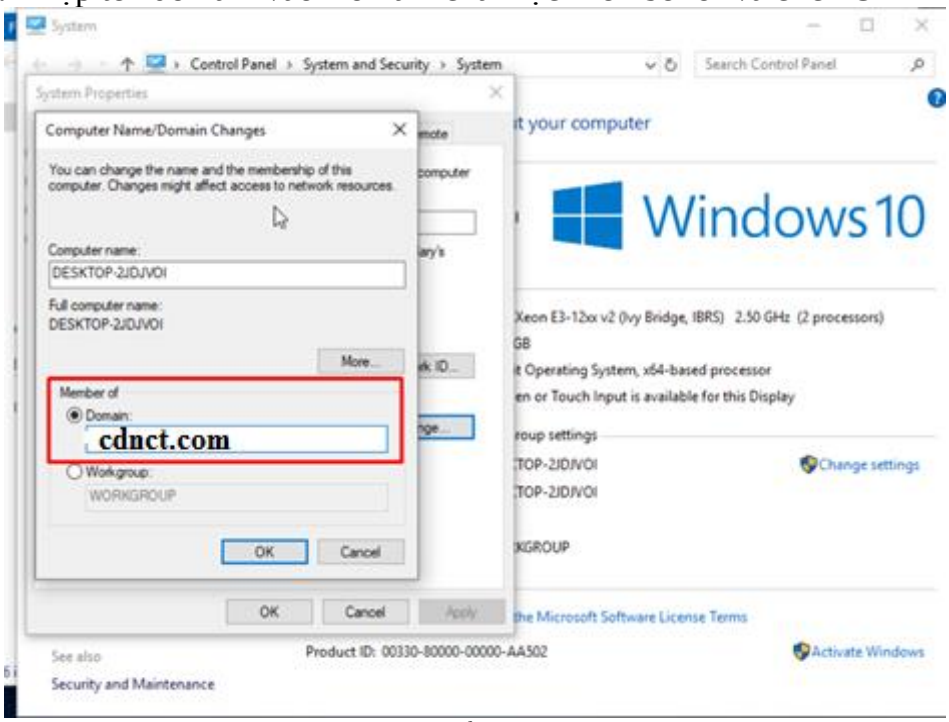
Hình 3.26 Cửa sổ Properties

Bước 4: Click Change settings -> Change



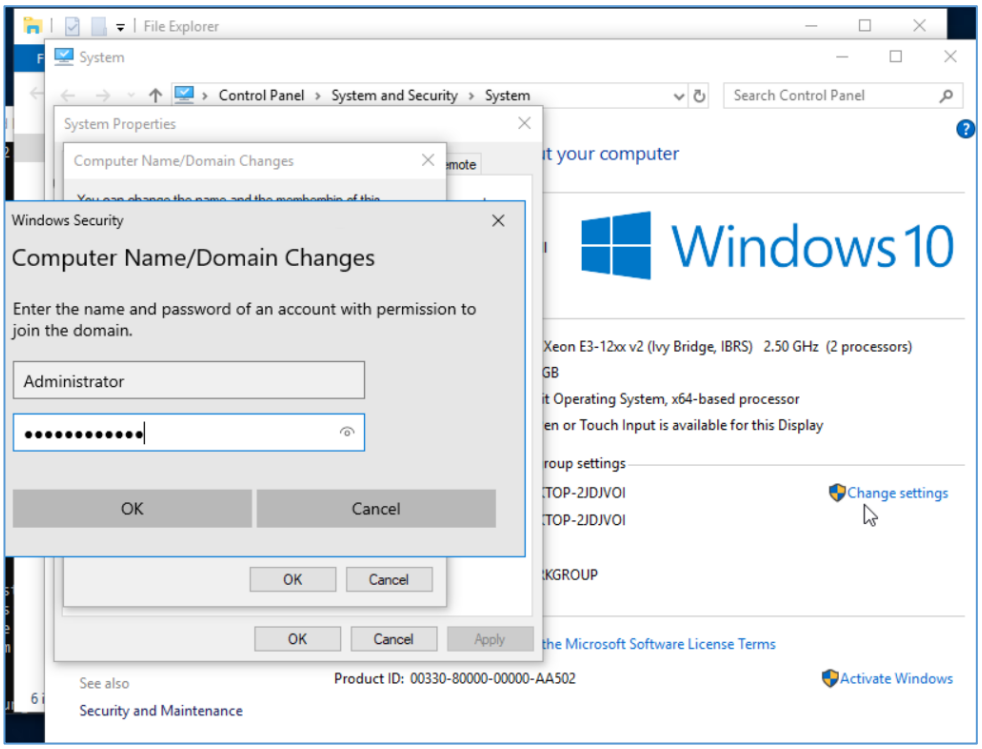
Hình 3.27 Cửa sổ System Properties

Bước 5: Nhập tên domain vào Domain của mục Member of và click OK



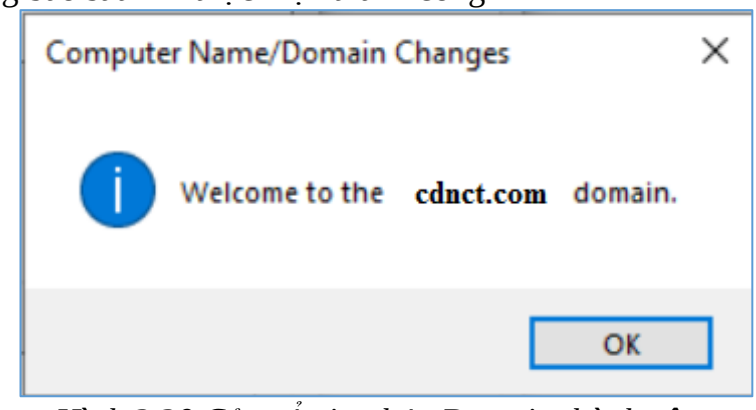
Hình 3.28 Cửa sổ gia nhập Domain

Bước 6: Nhập mật khẩu user Administrator quản lý domain controller và click OK



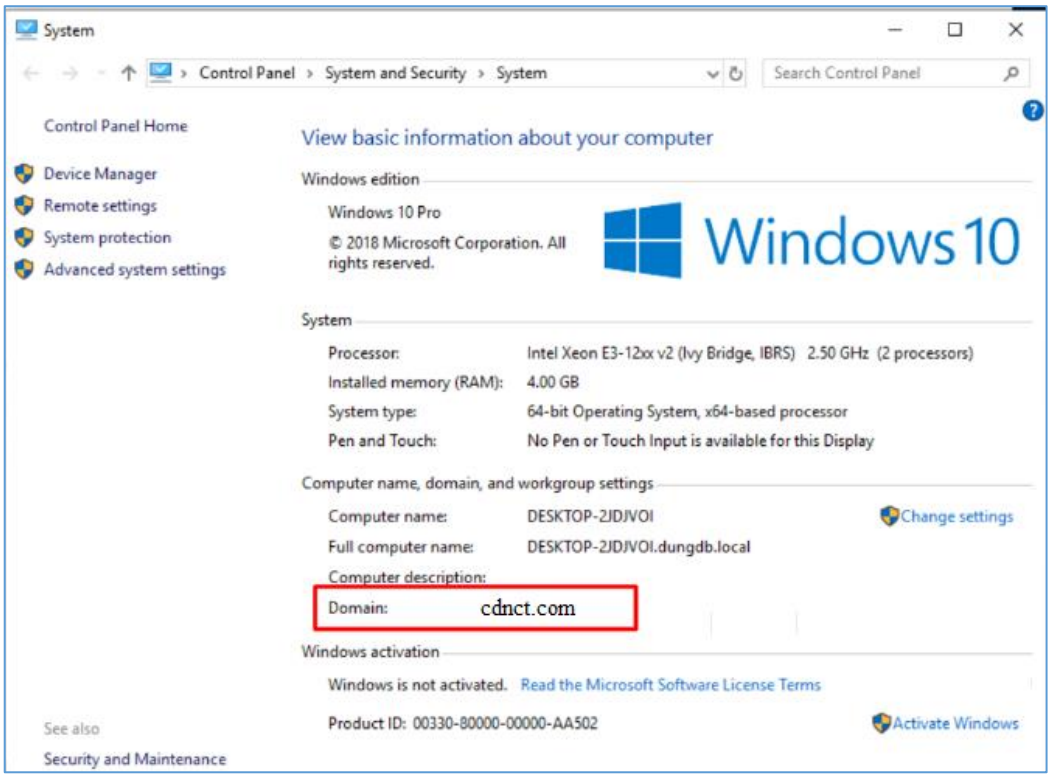
Hình 3.29 Cửa sổ xác nhận Password cho Administrator

Bước 7: Thông báo sau khi thực hiện thành công



Hình 3.30 Cửa sổ gia nhập Domain thành công

Bước 8: Sau khi reboot, máy client đã nhận domain thành công



Hình 3.30 Cửa sổ đăng nhập Domain thành công

Lưu ý:

- Khi đăng nhập vào máy client. Nếu ta nhập thông tin mật khẩu cũ thì ta chỉ đăng nhập vào máy tính đó.
- Để đăng nhập vào domain. Ta cần có thông tin tài khoản do người quản trị domain controller cung cấp. Ví dụ đăng nhập bằng user tech1@cdnct.com
- Một lưu ý nữa là: chỉ có tài khoản của người quản trị domain controller mới có thể thay đổi cấu hình hệ thống. Các user khác thì không thể. Trừ khi được phân quyền quản trị viên.
- Nếu muốn join một server chạy Windows Server vào domain, ta thực hiện các bước tương tự như trên.

Bài tập thực hành của học viên

1. Cài đặt và cấu hình Active Directory (AD) trên Windows server 2019.
2. Gia nhập máy trạm vào Domain controller.

Hướng dẫn thực hiện:

- Bài tập 1 làm theo mục 3.1 của giáo trình
- Bài tập 2 làm từng bước theo mục 3.2 của giáo trình

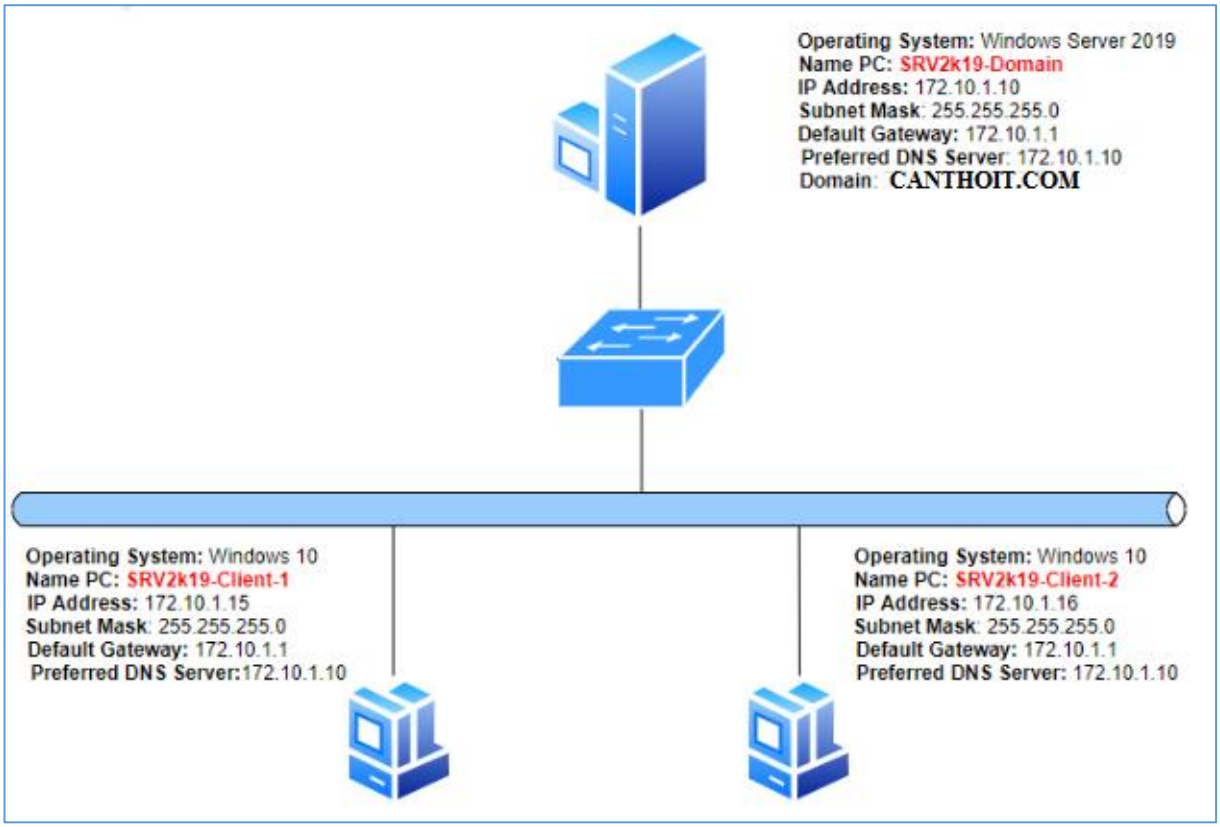
Những trọng tâm cần chú ý:

- Thiết lập địa chỉ IP cho đúng với hệ thống yêu cầu
- Mạng trong hệ thống phải thông nhau
- Đổi tên máy chủ cho phù hợp trước khi lên Domain controller
- Địa chỉ Preferred DNS của các máy trên hệ thống là địa chỉ của máy chủ Domain controller.
- Phải đăng nhập đúng user Administrator trước khi cài đặt Domain controller.
- Tên miền phải đúng qui cách và thể hiện được tổ chức lên DC.
- Thiết lập password phù hợp hệ thống và lưu lại để sau này còn sao lưu và phục hồi hệ thống khi cần thiết.

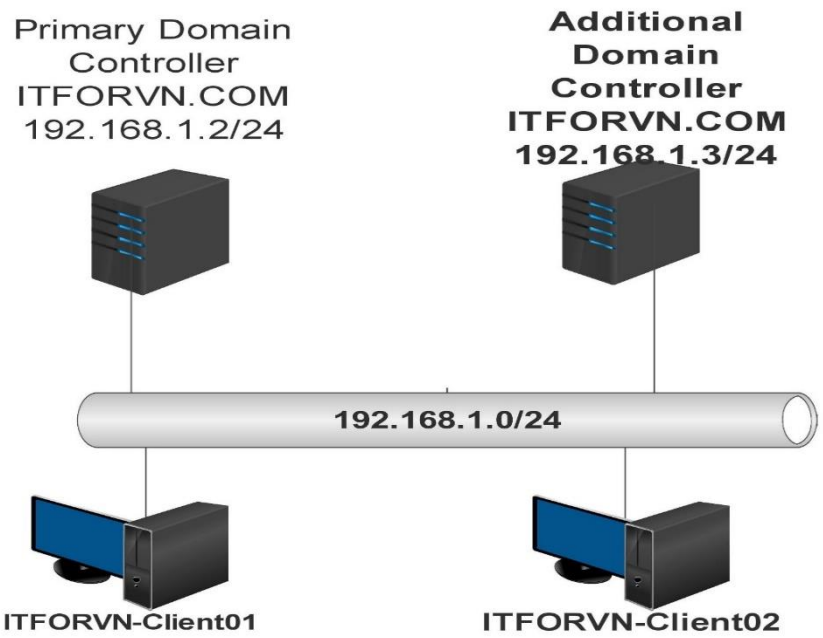
- Chọn cho đúng phiên bản hệ điều hành đang sử dụng.
- Đổi tên máy Client trước khi gia nhập DC.
- Tắt tường lửa cho máy DC và Client trên hệ thống.
- Thao tác phải đúng các bước cài đặt, cấu hình và gia nhập DC trên Windows server 2019.

Bài mở rộng và nâng cao

Bài tập 1: Hãy cài đặt và cấu hình Domain controller + DNS server trên Windows Server 2019 theo mô hình sau:



Bài tập 2: Hãy Cấu hình Additional Domain Controller trên Windows Server 2019 theo mô hình sau:



Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được Chức năng của Active Directory trong Windows Server
  + Trình bày được các bước cài đặt và gia nhập vào Domain controller trên Windows Server 2019
- Về kỹ năng:
  + Thao tác thành thạo việc cài đặt và cấu hình Active Directory trên Windows Server 2019.
  + Thao tác thành thạo việc Nâng cấp Server thành Domain Controller trên Windows Server 2019
  + Thực hiện đúng Gia nhập máy trạm vào Domain
  + Thực hiện đúng Additional Domain Controller trên hệ thống.
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng:
  + Đánh giá kỹ năng thực hành về các thao tác cài đặt Domain controller theo yêu cầu trên Windows Server 2019.
  + Đánh giá kỹ năng thực hành về các thao tác cài đặt Additional Domain controller theo yêu cầu trên Windows Server 2019.
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM
Mã bài: MĐ 17 - 04

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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

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

Mục tiêu:

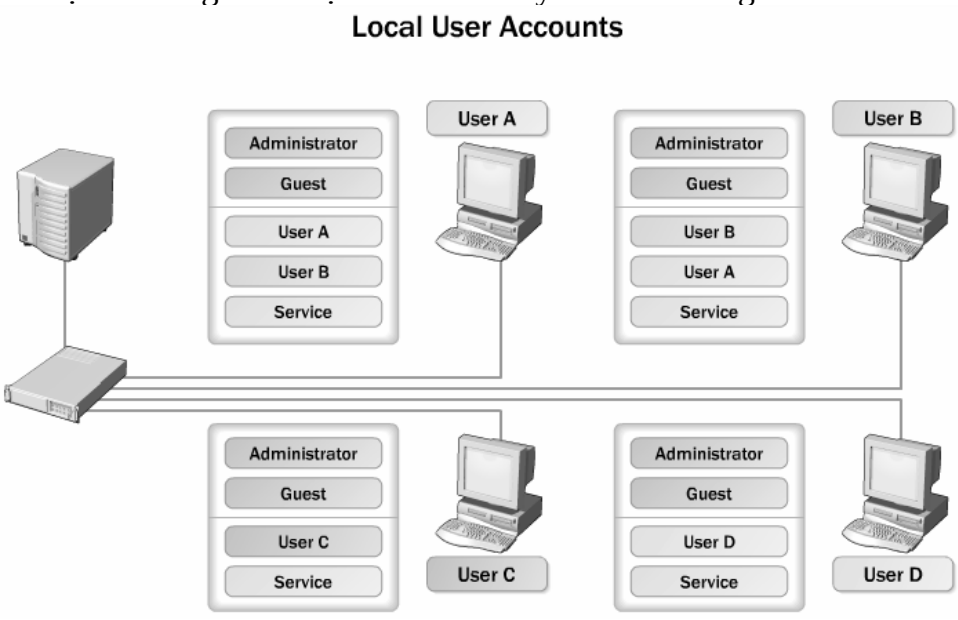
- Nêu được định nghĩa tài khoản người dùng, tài khoản nhóm.

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. Bạn tạo tài khoản người dùng cục bộ với công cụ Local Users and Group trong Computer Management (COMPMGMT.MSC). Các tài khoản cục bộ tạo ra trên máy stand-alone server, member server hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu SAM (Security Accounts Manager). Tập tin SAM này được đặt trong thư mục \Windows\system32\config

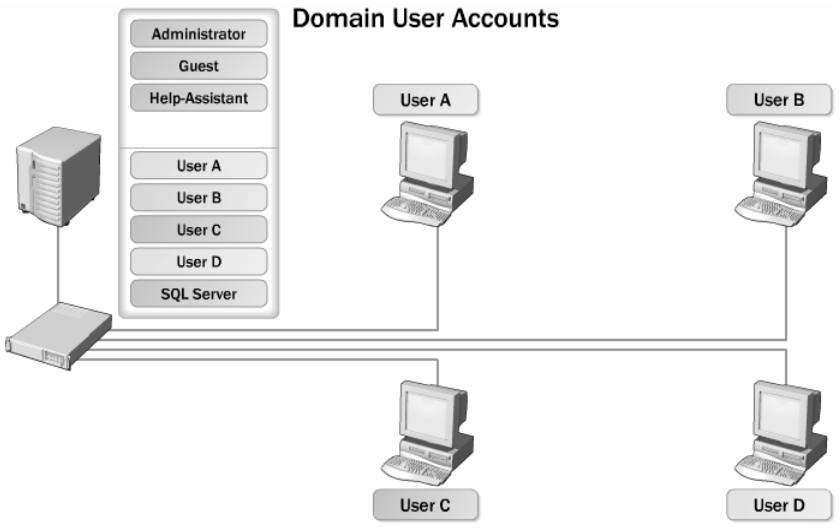


Hình 4.1 Người dùng cục bộ

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. Bạn tạo tài khoản người dùng miền với công cụ **Active Directory Users and Computer (DSA.MSC)**. Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin **NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục **\Windows\NTDS**.



Hình 4.2 Người dùng miền

1.1.3. Yêu cầu về tài khoản người dùng

- Mỗi **username** phải từ 1 đến 20 ký tự (trên **Windows Server** thì tên đăng nhập có thể dài đến 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành **Windows NT 4.0** về trước thì mặc định chỉ hiểu 20 ký tự).
- Mỗi **username** là chuỗi duy nhất của mỗi người dùng có nghĩa là tất cả tên của người dùng và nhóm không được trùng nhau.
- **Username** không chứa các ký tự sau: " / \ [ ]: ; | =, + * ? < >
- Trong một **username** có thể chứa các ký tự đặc biệt bao gồm: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới. Tuy nhiên, nên tránh các khoảng trắng vì những tên như thế phải đặt trong dấu ngoặc khi dùng các kịch bản hay dòng lệnh.

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. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (**security group**) và nhóm phân phối (**distribution group**)

1.2.1. Nhóm bảo mật

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập (permission). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các SID. Có ba loại nhóm bảo mật chính là: local, global và universal. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: local, domain local, global và universal.

Local group (nhóm cục bộ) là loại nhóm có trên các máy stand-alone Server, member server. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại

trên máy chứa nó thôi.

Domain local group (nhóm cục bộ miền) là loại nhóm cục bộ đặc biệt vì chúng là local group nhưng nằm trên máy Domain Controller. Các máy Domain Controller có một cơ sở dữ liệu Active Directory chung và được sao chép đồng bộ với nhau do đó một local group trên một Domain Controller này thì cũng sẽ có mặt trên các Domain Controller anh em của nó, như vậy local group này có mặt trên miền nên được gọi với cái tên nhóm cục bộ miền. Các nhóm trong mục Built-in của Active Directory là các domain local.

Global group (nhóm toàn cục hay nhóm toàn mạng) là loại nhóm nằm trong Active Directory và được tạo trên các Domain Controller. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền. Một nhóm global có thể đặt vào trong một nhóm local của các server thành viên trong miền. Chú ý khi tạo nhiều nhóm global thì có thể làm tăng tải trọng công việc của Global Catalog.

Universal group (nhóm phổ quát) là loại nhóm có chức năng giống như global group nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm global group và local group vì chúng dễ dàng lồng các nhóm vào nhau.

1.2.2. Nhóm phân phối

Nhóm phân phối là một loại nhóm phi bảo mật, không có SID và không xuất hiện trong các ACL (Access Control List). Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ. Chúng được dùng để phân phối thư (e-mail) hoặc các tin nhắn (message). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm MS Exchange.

1.2.3. Qui tắc gia nhập nhóm

- Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong nhóm Machine Local.
- Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong chính loại nhóm của mình.
- Nhóm Global và Universal có thể đặt vào trong nhóm Domain local.

2. Các tài khoản tạo sẵn

Mục tiêu:

- Trình bày được các tài khoản tạo sẵn.

2.1. 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 nằng trong **Container Users** của công cụ **Active Directory User and Computer**. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

Tên tài khoản	Mô tả

Administrator	**Administrator** là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt **Windows Server**. Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in…
Guest	Tài khoản **Guest** cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập **Internet** hoặc in ấn.
ILS_Anonymous_User	Là tài khoản đặc biệt được dùng cho dịch vụ **ILS**. **ILS** hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: **caller ID**, **video conferencing**, **conference calling**, và **faxing**. Muốn sử dụng **ILS** thì dịch vụ **IIS** phải được cài đặt.
IUSR_computer-name	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ **IIS** trên máy tính có cài **IIS**.
IWAM_computer - name	Là tài khoản đặc biệt được dùng cho **IIS** khởi động các tiến trình của các ứng dụng trên máy có cài **IIS**.
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (**Key Distribution Center**)
TSInternetUser	Là tài khoản đặc biệt được dùng cho **Terminal Services**.

2.2. Tài khoản nhóm Domain Local tạo sẵn

Nhưng chúng ta đã 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. Bạn cũng chú ý rằng là không có quyền xóa các nhóm đặc biệt này.

Tên nhóm	Mô tả
Administrators	Nhóm này mặc định được ấn định sẵn tất cả các quyền hạn cho nên thành viên của nhóm này có toàn quyền trên hệ thống mạng. Nhóm **Domain Admins** và **Enterprise Admins** là thành viên mặc định của nhóm **Administrators**.
Account Operators	Thành viên của nhóm này có thể thêm, xóa, sửa được các tài khoản người dùng, tài khoản máy và tài khoản nhóm. Tuy nhiên họ không có quyền xóa, sửa các nhóm trong **container Built-in** và **OU**.

Domain Controllers	Nhóm này chỉ có trên các **Domain Controller** và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các **Domain Controller** nhưng không có quyền quản trị các chính sách bảo mật.
Backup Operators	Thành viên của nhóm này có quyền lưu trữ dự phòng (**Backup**) và phục hồi (**Retore**) hệ thống tập tin. Trong trường hợp hệ thống tập tin là **NTFS** và họ không được gán quyền trên hệ thống tập tin thì thành viên của nhóm này chỉ có thể truy cập hệ thống tập tin thông qua công cụ **Backup**. Nếu muốn truy cập trực tiếp thì họ phải được gán quyền.
Guests	Là nhóm bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vãng lai không phải là thành viên của mạng. Mặc định các tài khoản **Guest** bị khóa
Print Operator	Thành viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory.
Server Operators	Thành viên của nhóm này có thể quản trị các máy server trong miền như: cài đặt, quản lý máy in, tạo và quản lý thư mục dùng chung, backup dữ liệu, định dạng đĩa, thay đổi giờ…
Users	Mặc định mọi người dùng được tạo đều thuộc nhóm này, nhóm này có quyền tối thiểu của một người dùng nên việc truy cập rất hạn chế.
Replicator	Nhóm này được dùng để hỗ trợ việc sao chép danh bạ trong **Directory Services**, nhóm này không có thành viên mặc định.
Incoming Forest Trust Builders	Thành viên nhóm này có thể tạo ra các quan hệ tin cậy hướng đến, một chiều vào các rừng. Nhóm này không có thành viên mặc định.
Network Configuration Operators	Thành viên nhóm này có quyền sửa đổi các thông số **TCP/IP** trên các máy **Domain Controller** trong miền.
Remote Desktop User	Thành viên nhóm này có thể đăng nhập từ xa vào các **Domain Controller** trong miền, nhóm này không có thành viên mặc định.
Performace Log Users	Thành viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy **Domain Controller**, nhóm này cũng không có thành viên mặc định.
Performace Monitor Users	Thành viên nhóm này có khả năng giám sát từ xa các máy **Domain Controller**.

Ngoài ra còn một số nhóm khác như DHCP Users, DHCP Administrators, DNS Administrators… các nhóm này phục vụ chủ yếu cho các dịch vụ, chúng ta sẽ tìm hiểu cụ thể trong từng dịch vụ ở giáo trình "Dịch Vụ Mạng". Chú ý theo mặc

định hai nhóm Domain Computers và Domain Controllers được dành riêng cho tài khoản máy tính, nhưng bạn vẫn có thể đưa tài khoản người dùng vào hai nhóm này.

2.3. 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 (**Win2K Pro, WinXP**) 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**.

2.4. 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 hữa 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 **Dial-up Networking**.

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

Mục tiêu:

- Sử dụng được các công cụ tạo và quản trị tài khoản người dùng và nhóm cục bộ.

3.1. Nhóm cục bộ

Mặc định khi user được tạo ra thì nó là thành viên của 1 group. **Group** là đối tượng trong hệ thống (system object), dùng để chứa thông tin quản lý user account hoặc group account khác

Chức năng của **Group** phục vụ cho công tác quản lý, phân quyền cho một nhóm các user cùng mục đích quản lý. (thay vì phân quyền chi tiết từng user thì ta dùng group cho nhanh)

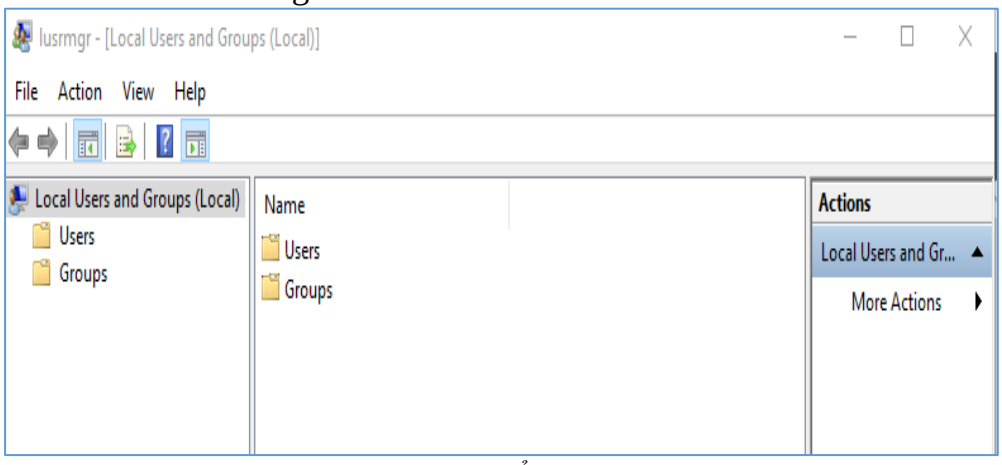
Đây là các **Group mặc định** có sẵn trên windows, dựa vào các chức năng mà ta có các group khác nhau, có 2 nhóm mặc định:

- **Nhóm 1**: có chức năng quản lý hệ thống, vd: group Administrators (tạo user, chỉnh giờ, tắt máy v.v)
- **Nhóm 2**: nhóm được phép truy cập, sử dụng tài nguyên, vd: group Users.

Tạo **group riêng**:

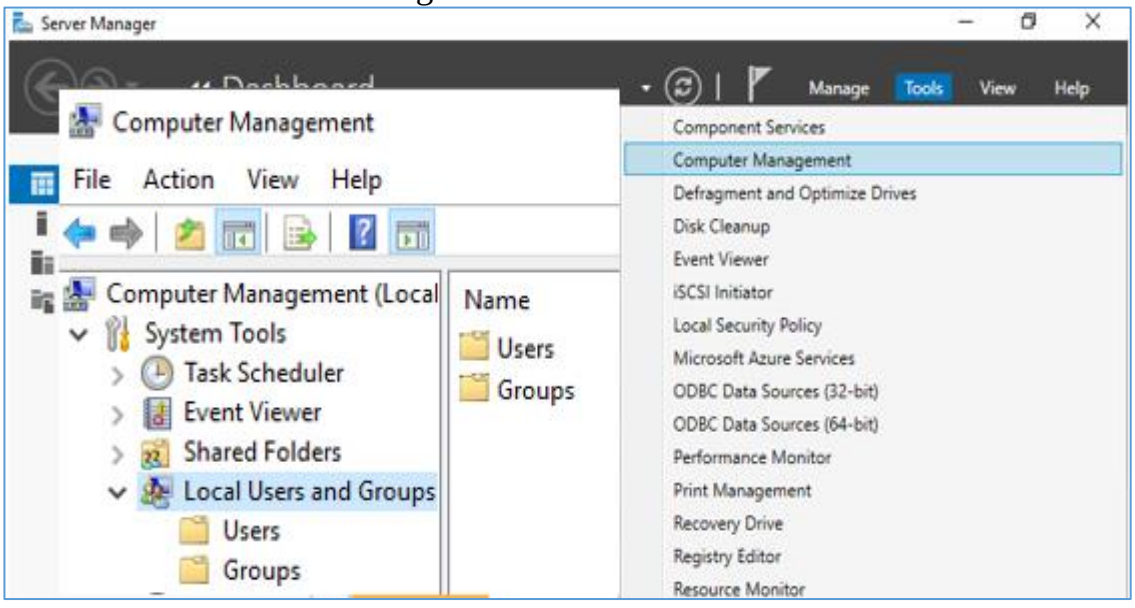
Bước 1: Mở cửa sổ tạo user

Cách 1: Start > Run: lusrmgr.msc



Hình 4.3 Cửa sổ lusrmgr.msc

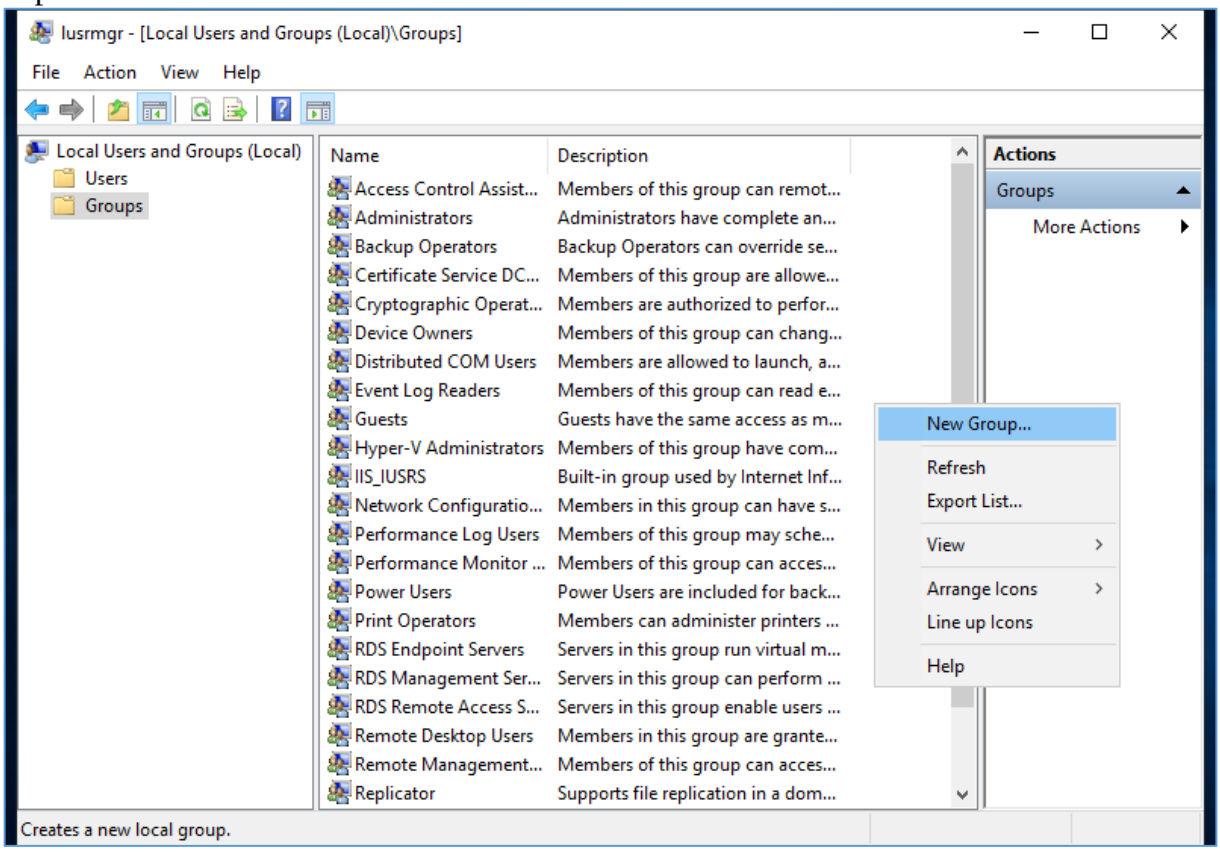
Cách 2: Vào Server manager



Hình 4.4 Cửa sổ manager

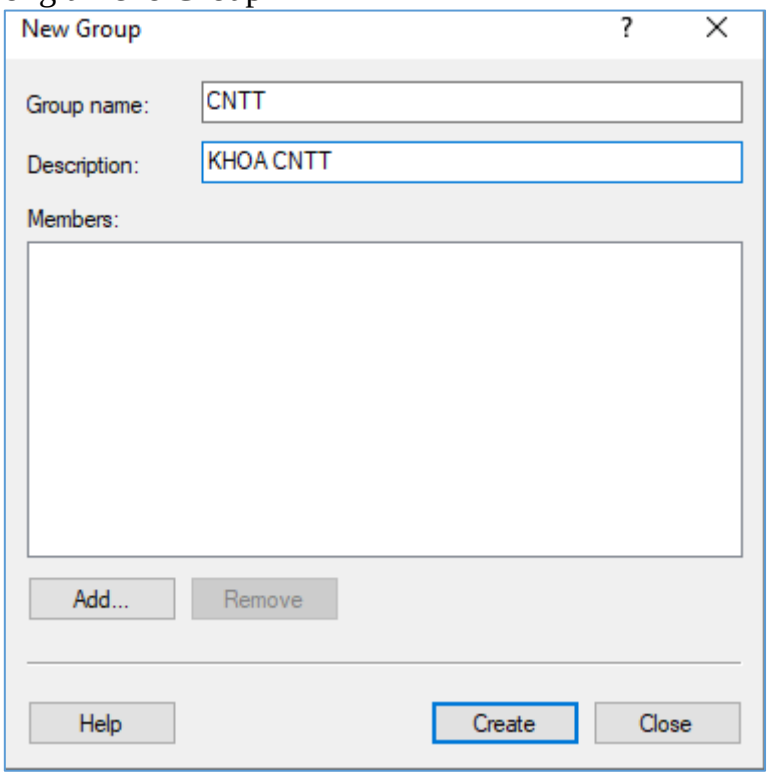
Bước 2: Tạo Group

Chọn Group khung bên trái**, sau đó Right click** -> "**Group**" để tiến hành tạo Group mới



Hình 4.4 Cửa sổ New Group

Bước 3: Nhập thông tin cho Group



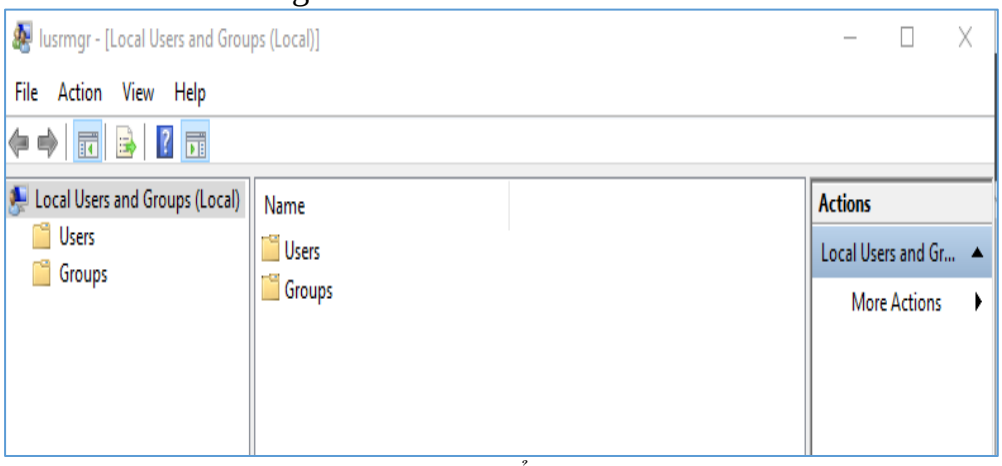
Hình 4.6. Cửa sổ tạo Group

3.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ

3.2.1. Tạo tài khoản mới

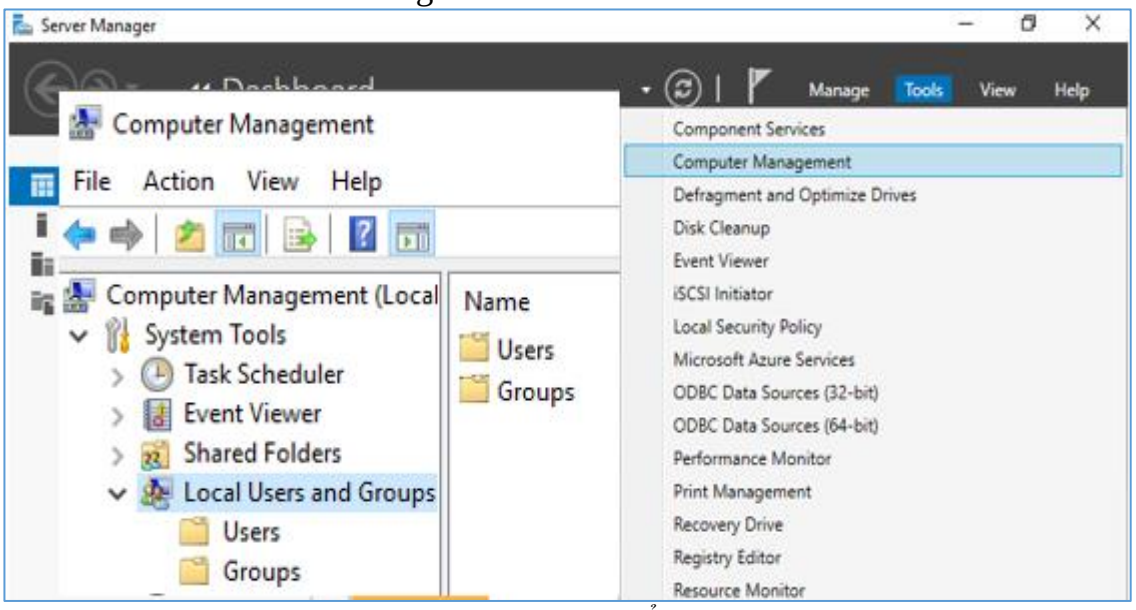
Bước 1: Mở cửa sổ tạo user

Cách 1: Start > Run: lusrmgr.msc



Hình 4.7 Cửa sổ lusrmgr.msc

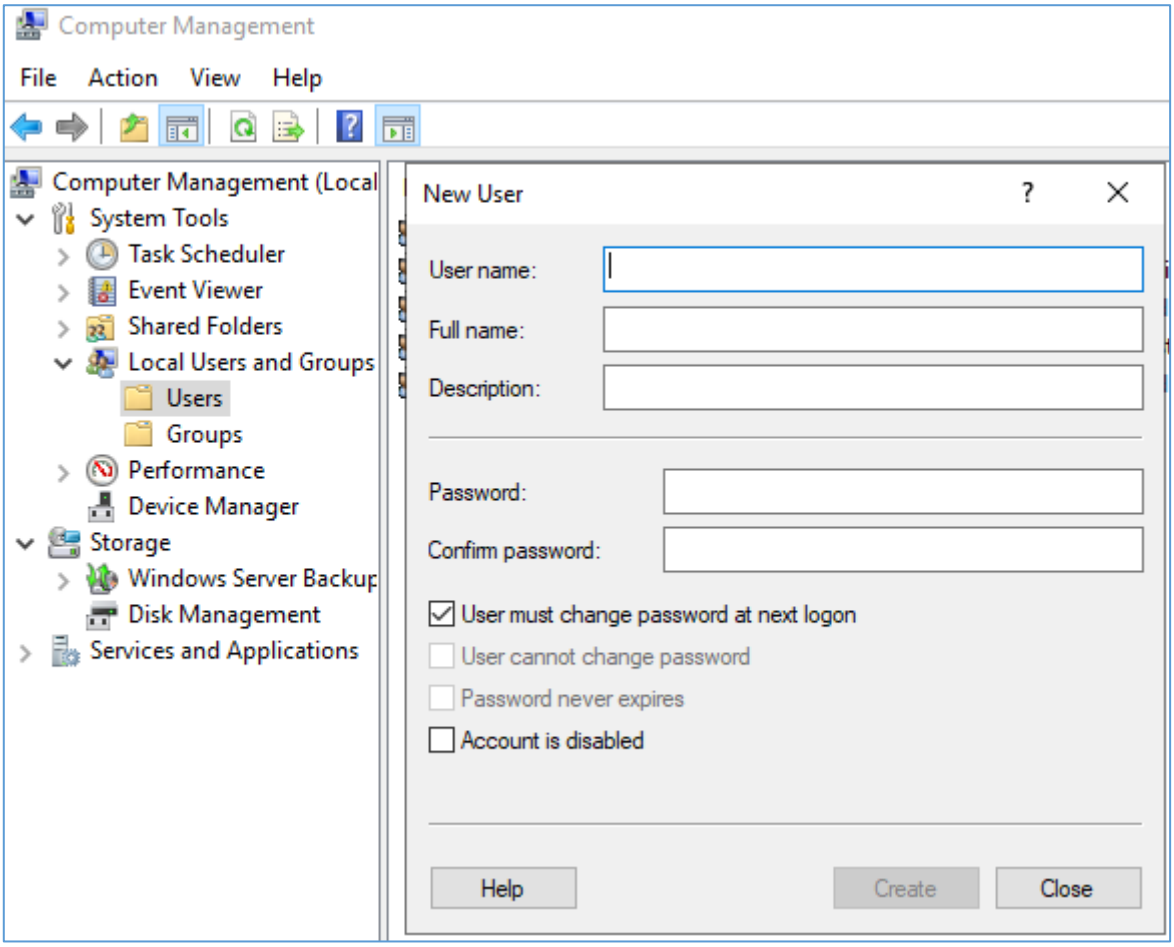
Cách 2: Vào Server manager



Hình 4.8 Cửa sổ manager

Bước 2: Tạo User

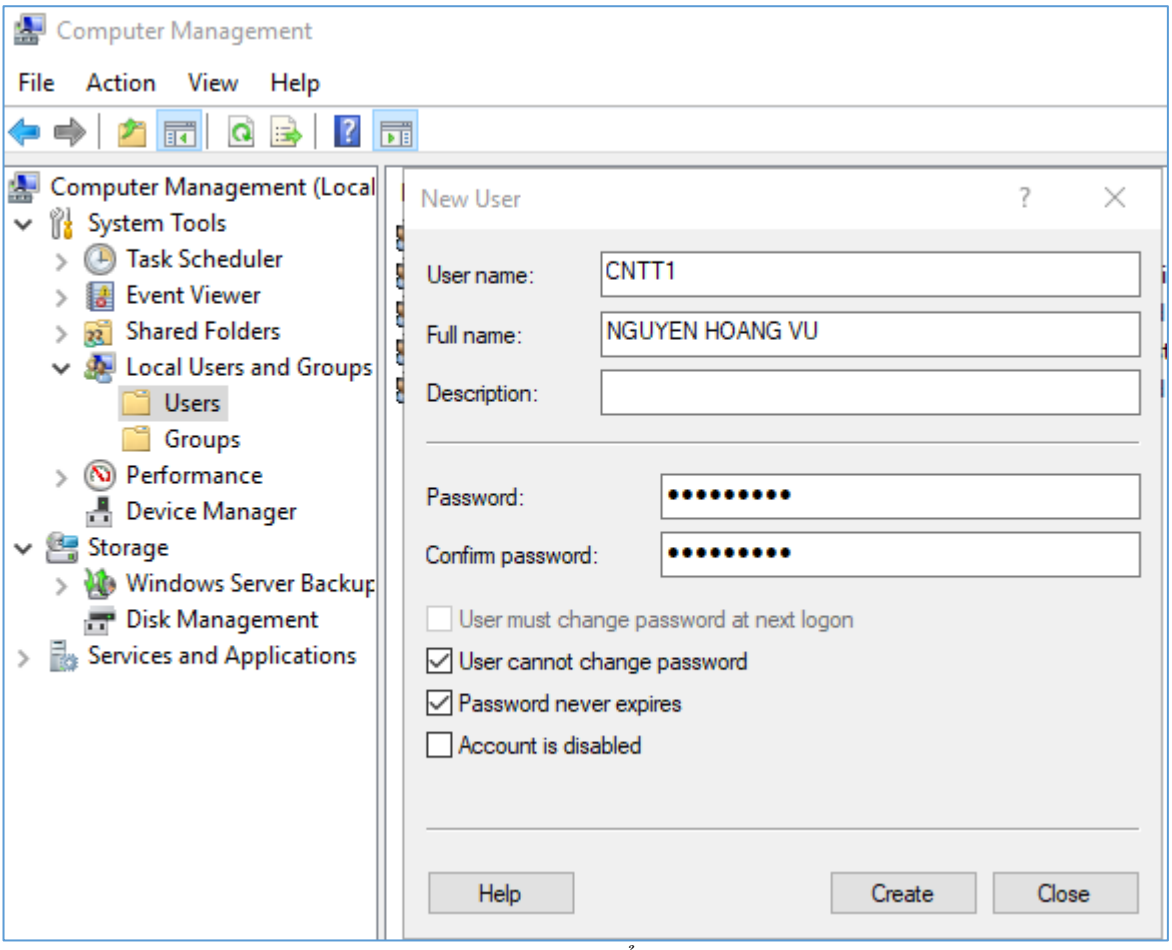
Chọn User**, sau đó Right click ->** "**New User**" để tiến hành tạo User mới



Hình 4.9 Cửa sổ New user

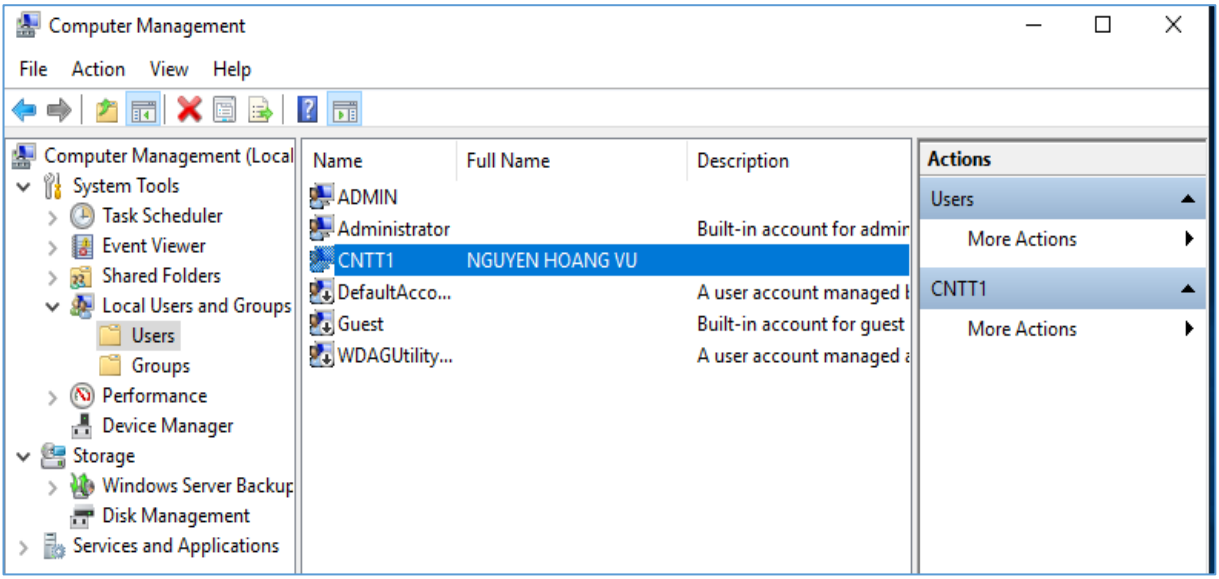
Bước 3: Nhập thông tin cho User

- **Username**: tên định danh cho tài khoản User, không phân biệt chữ hoa chữ thường.
- **Password**: thông tin mật khẩu sử dụng để đăng nhập tài khoản User. Password của các tài khoản sẽ được lưu trong file SAM với đường dẫn: "*C:\windows\system32\config*".
- **User must change password at next log on**: người dùng phải đổi password ở lần đăng nhập kế tiếp. Khi user đổi pass rồi thì "mất dấu check" ở thuộc tính này. Dùng để cho user tự đặt mật khẩu khi mới tạo account. Nếu trong quá trình sử dụng, ta thấy tài khoản này đang bị dò password thì ta sẽ yêu cầu đổi pass (hoặc user tự bấm Ctrl + Alt + Del để đổi pass).
- **User cannot change password**: người dùng không thể đổi password. Dùng tính năng này khi có các tài khoản dùng chung cho nhiều người.
- **Password nerver expired**: mật khẩu không bao giờ hết hạn, nếu không check thì mặc định mật khẩu user chỉ có giá trị trong 42 ngày. Sau 42 ngày bắt buộc người dùng phải đổi password mới. Dùng cho các tài khoản tạo ra nhằm mục đích khai báo cho các tác vụ trên hệ thống (Vd: backup phải khai báo tài khoản có quyền backup, mà chương trình backup thì chạy liên tục, khi đến 42 ngày thì nó dừng tài khoản này => backup không thể thực hiện)
- **Account is disabled**: tài khoản không thể đăng nhập hay truy xuất các tài nguyên trên hệ thống. Dùng khi có các tài khoản không sử dụng nữa, ta không nên xóa mà cứ disable.



Hình 4.10. Cửa sổ tạo user

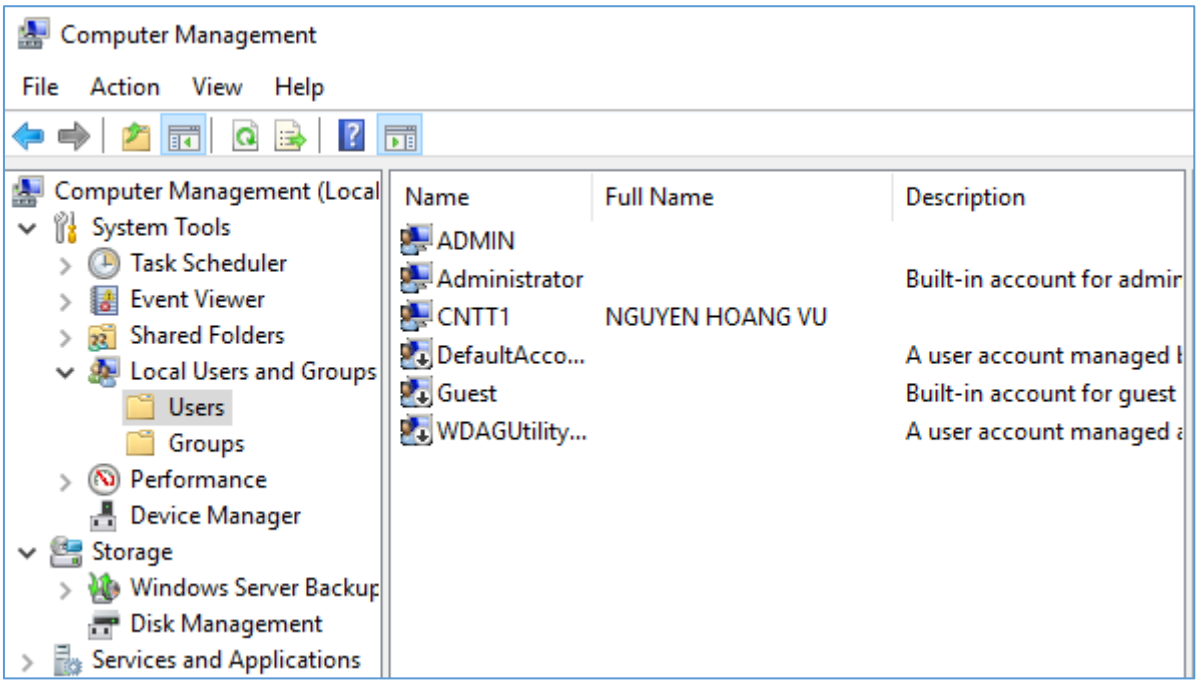
Bước 4: Xác nhận User vừa tạo



Hình 4.11 Cửa sổ quản lý user

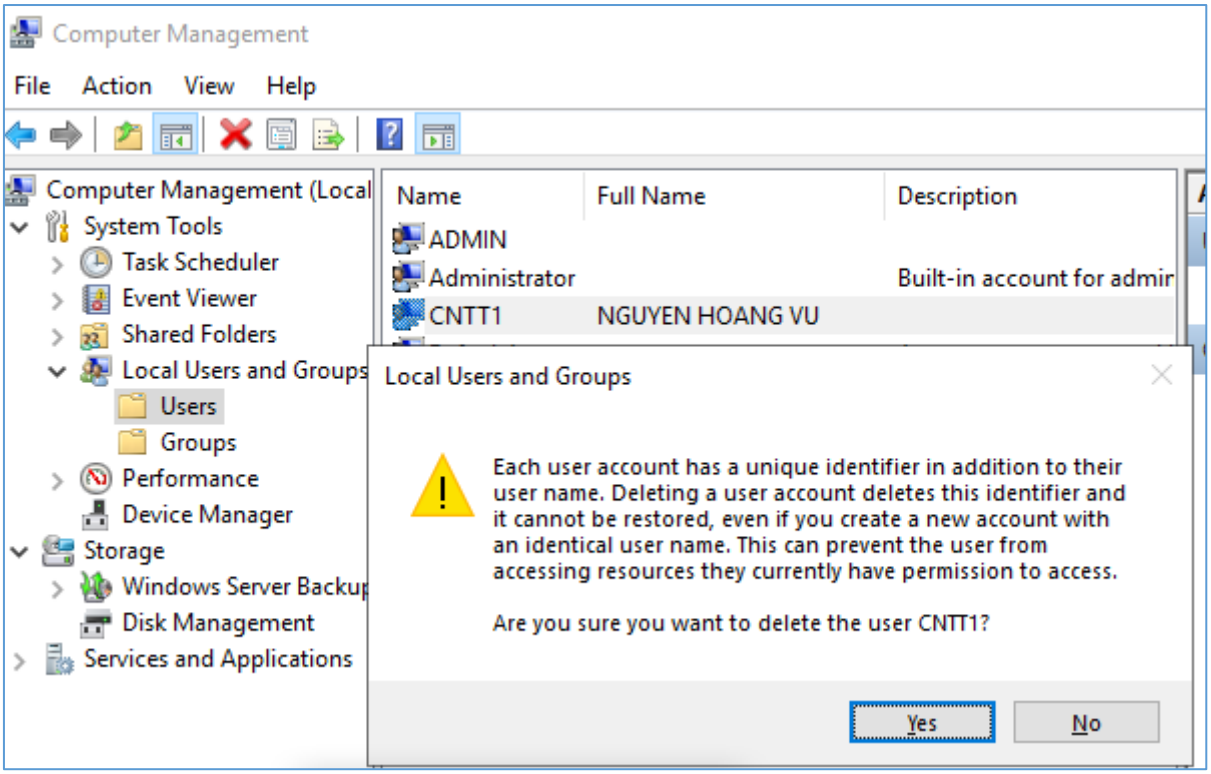
3.2.2. Xóa tài khoản

Bước 1: Mở cửa sổ quản lý User



Hình 4.12 Cửa sổ quản lý User

Bước 2: Chọn User cần xóa, nhấn phím Delete hoặc Right click lên User cần xóa, Chọn Yes để xóa



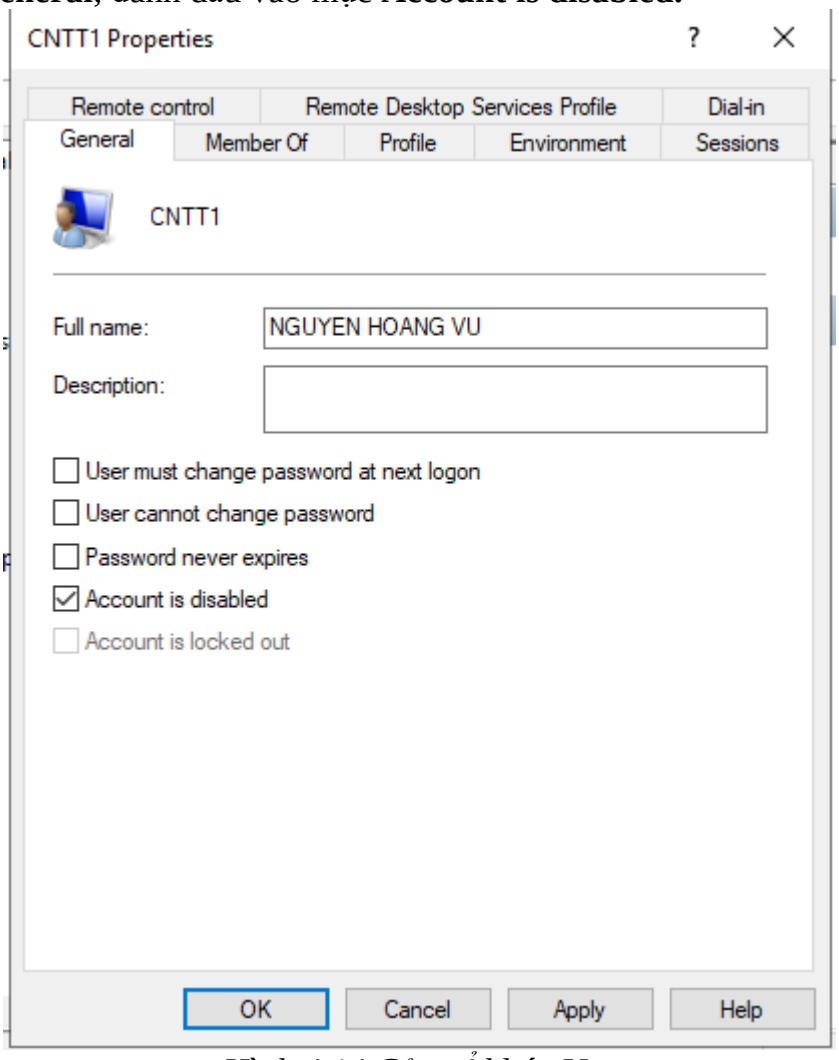
Hình 4.13 Cửa sổ xóa User

Chú ý: khi chọn **Delete** thì hệ thống xuất hiện hộp thoại hỏi bạn muốn xóa thật sự không vì tránh trường hợp bạn xóa nhầm. Bởi vì khi đã xóa thì tài khoản người dùng này không thể phục hồi được.

3.2.3 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 bạn 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.

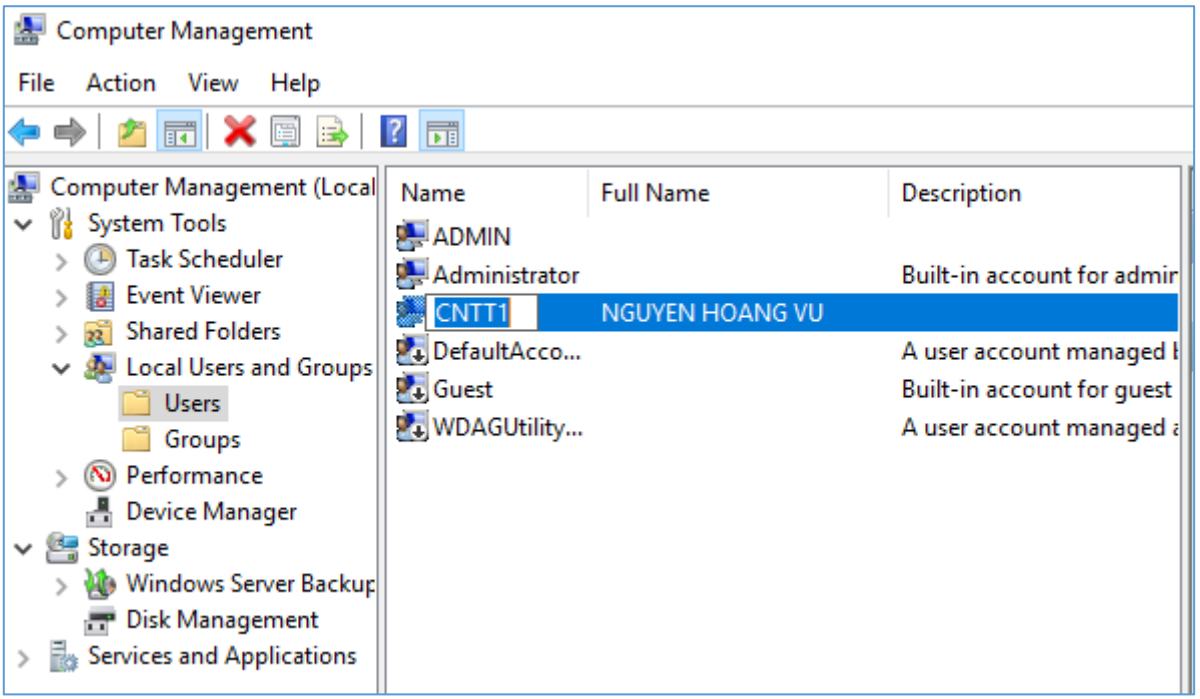
Trong **Tab General**, đánh dấu vào mục **Account is disabled.**



Hình 4.14 Cửa sổ khóa User

3.2.4 Đổi tên tài khoản

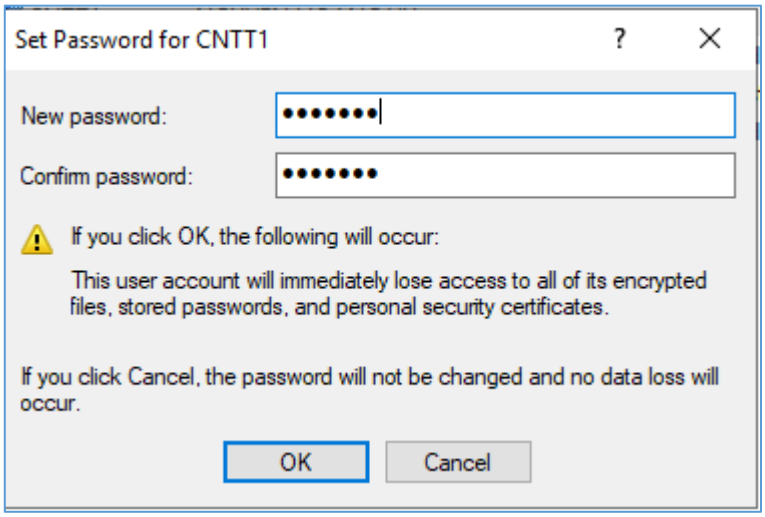
Bạn có thể đổi tên bất kỳ một tài khoản người dùng nào, đồng thời bạn cũng có thể điều chỉnh các thông tin của tài khoản người dùng thông qua chức năng này. Chức năng này có ưu điểm là khi bạn thay đổi tên người dùng nhưng **SID** của tài khoản vẫn không thay đổi. Muốn thay đổi tên tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi tên, nhấp phải chuột và chọn **Rename**.



Hình 4.15 Cửa sổ khóa User

3.2.5 Thay đổi mật khẩu

Muốn đổi mật mã của người dùng bạn mở công cụ Local Users and Groups, chọn tài khoản người dùng cần thay đổi mật mã, nhấp phải chuột và chọn **Reset password**, sau đó chọn **Proceed,** nhập **Password** mới.



Hình 4.16 Cửa sổ Set pasword cho User

4. Quản lý tài khoản người dùng và nhóm trên active directory

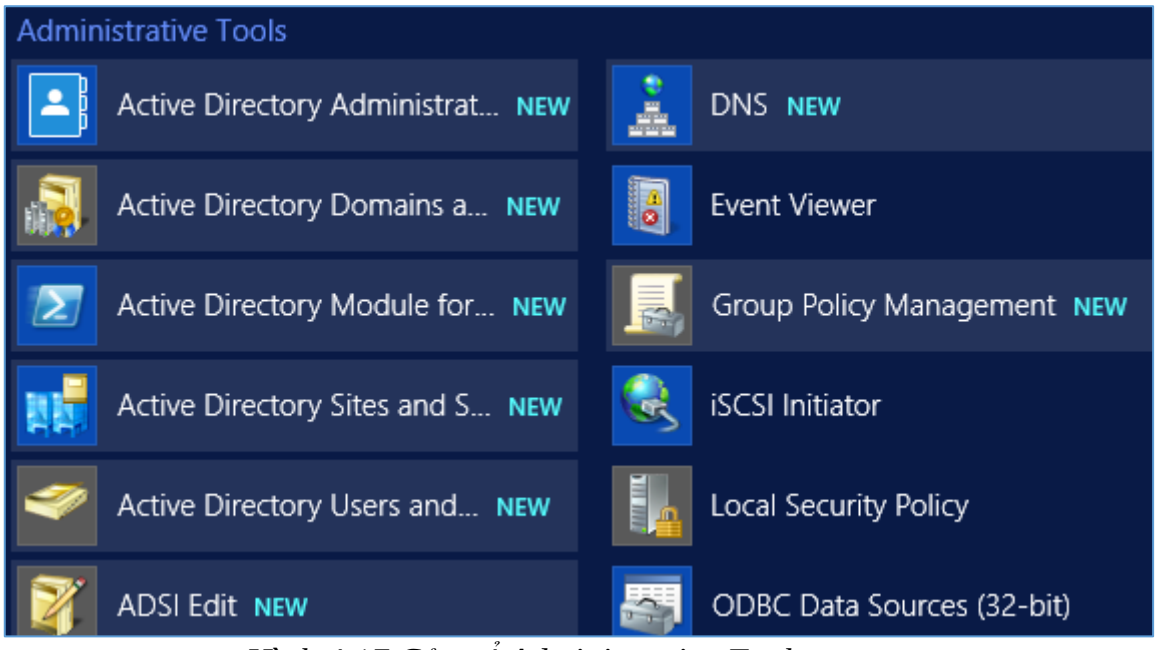
Mục tiêu:

- Sử dụng được các công cụ tạo và quản trị tài khoản người dùng và nhóm cục bộ.

4.1. Tạo mới tài khoản người dùng

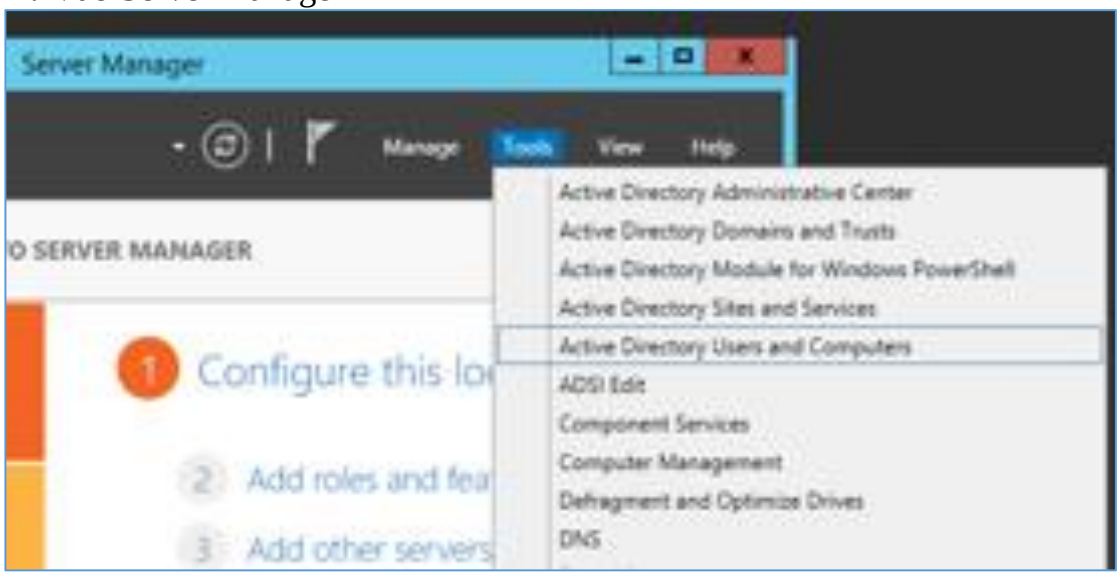
Bước 1: Mở cửa sổ tạo user

Cách 1: Start > Administrative Tools-> Active Directory User and Computers



Hình 4.17 Cửa sổ Administrative Tools

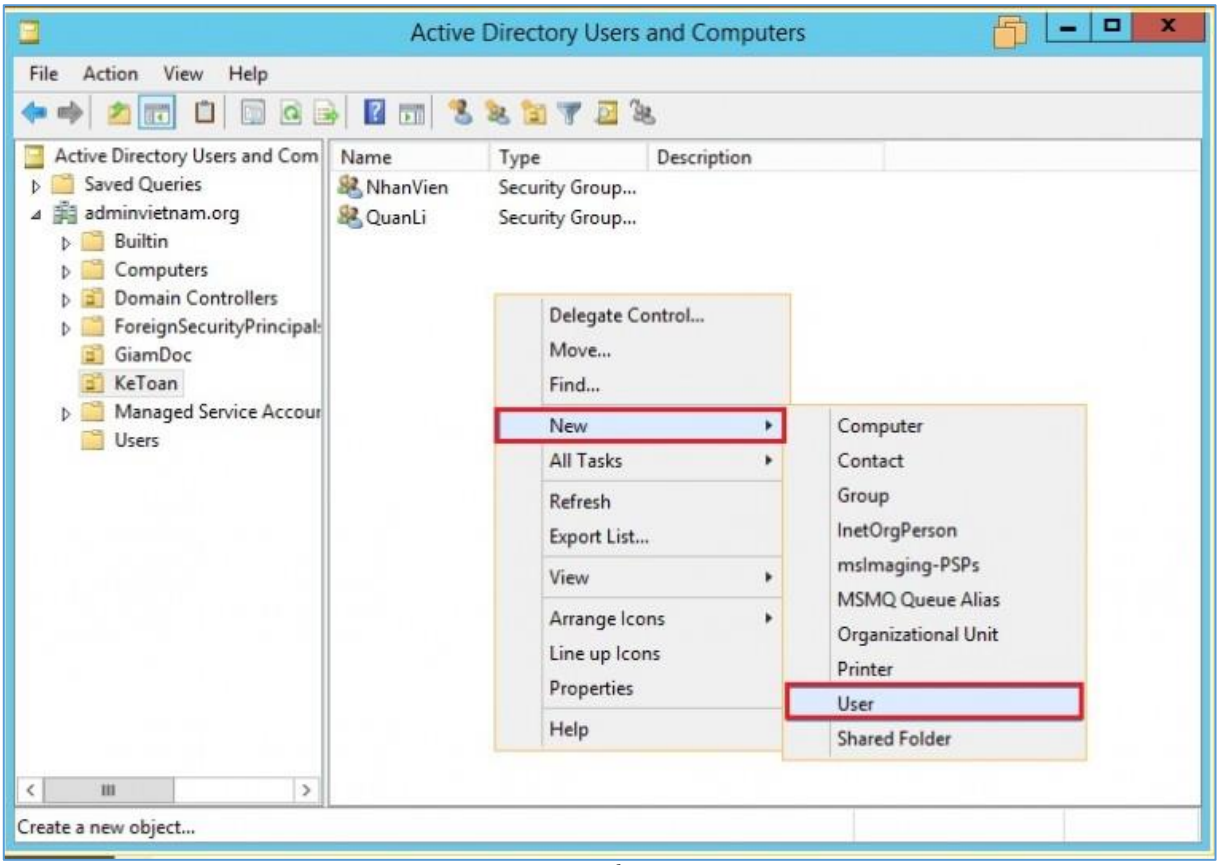
Cách 2: Vào Server manager



Hình 4.18 Cửa sổ Manager

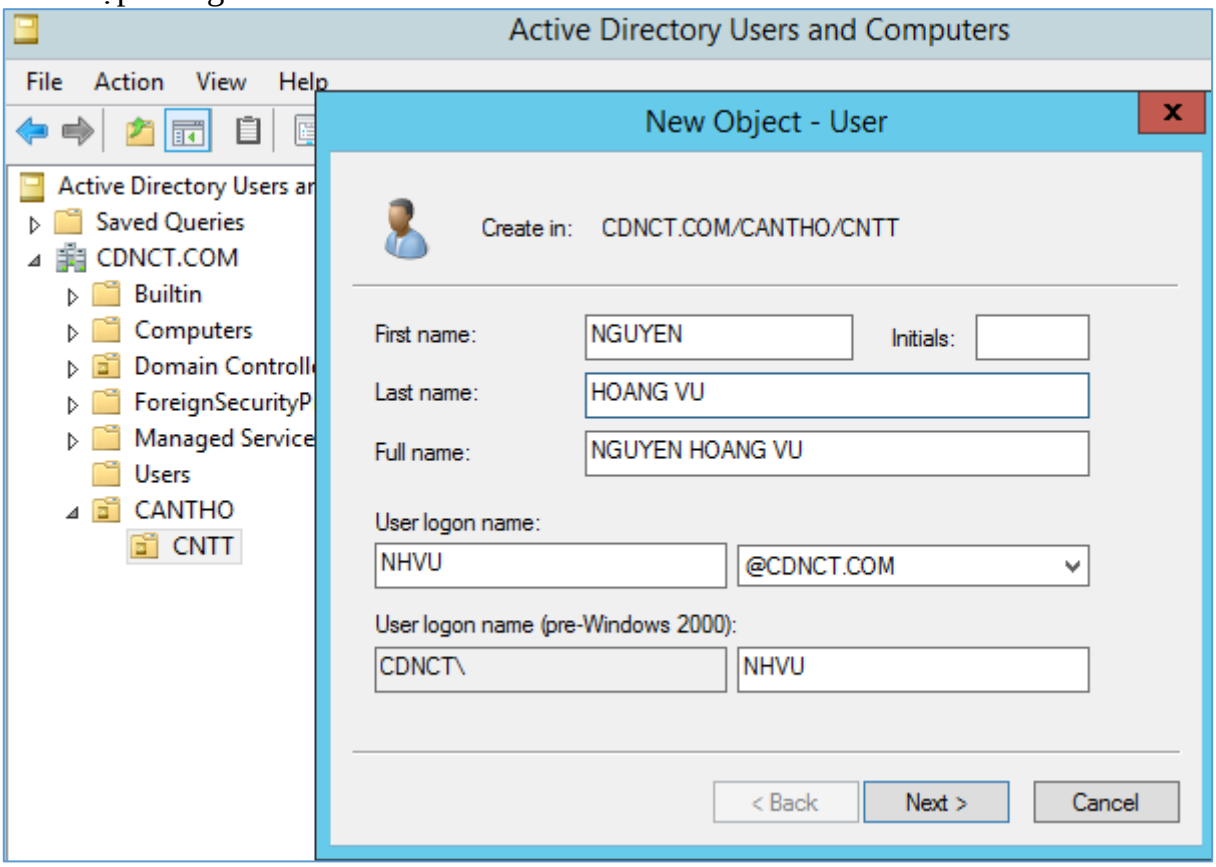
Bước 2: Tạo User

Chọn nơi chứa User**, sau đó Right click ->** "**New User**" để tiến hành tạo User mới



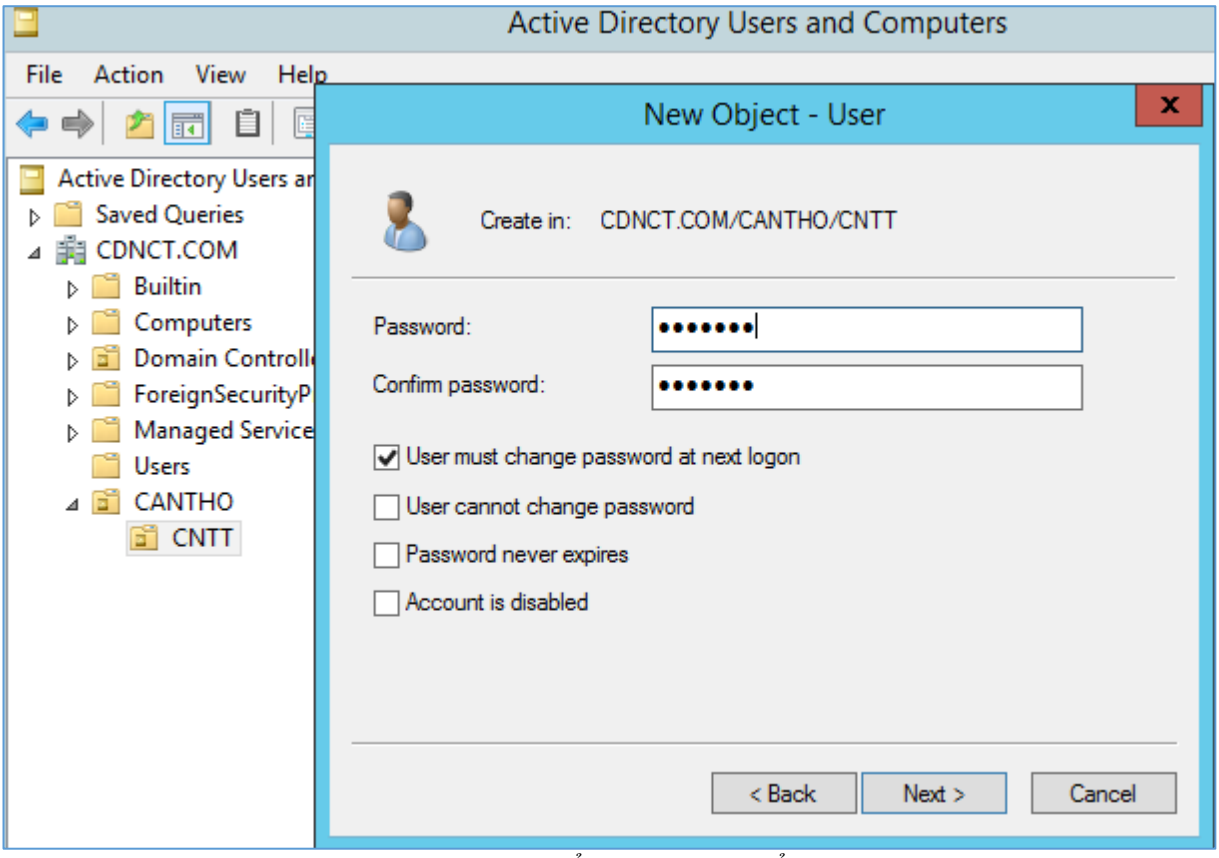
Hình 4.19 Cửa sổ New user

Bước 3: Nhập thông tin cho User



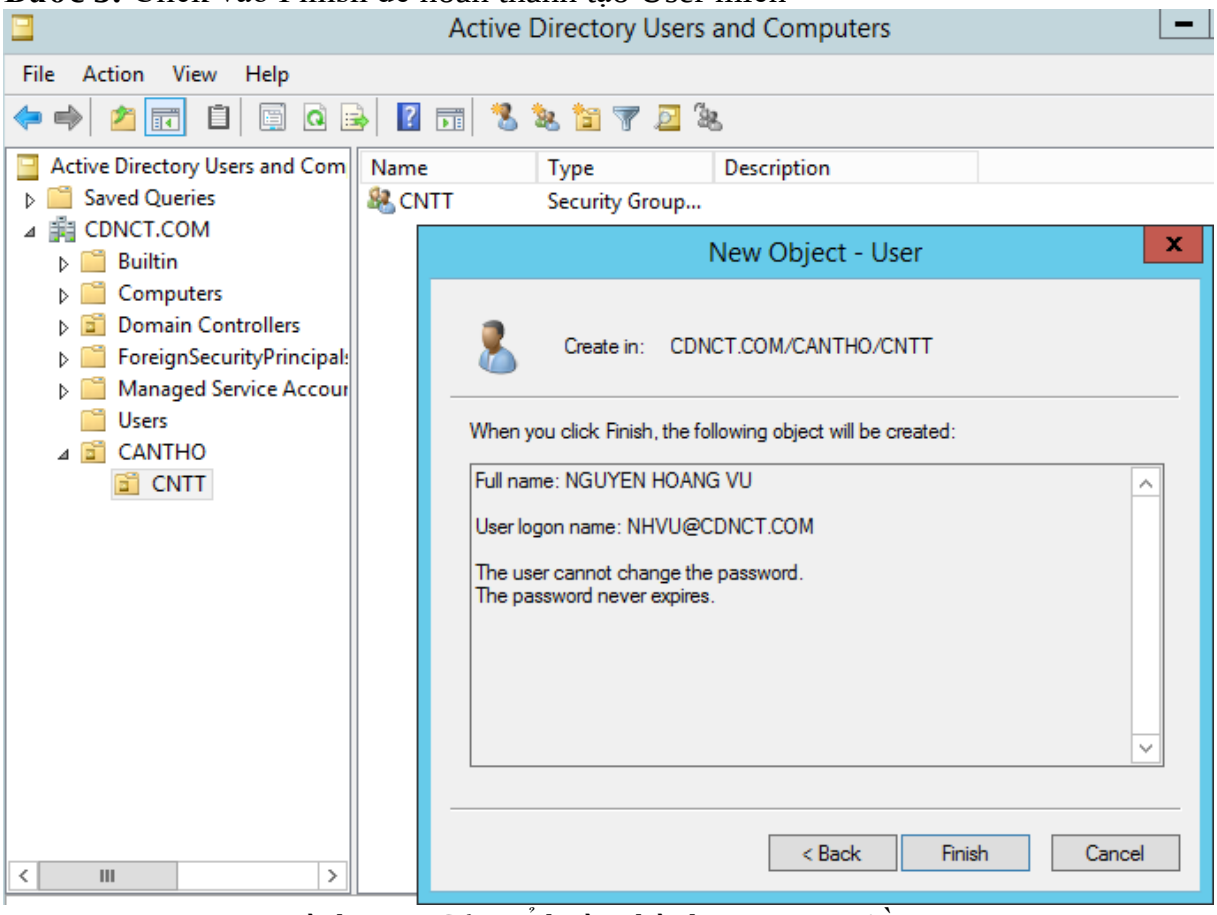
Hình 4.20. Cửa sổ tạo user

Bước 4: Xác nhận mật khẩu cho User vừa tạo



Hình 4.21 Cửa sổ nhập mật khẩu

Bước 5: Click vào Finish để hoàn thành tạo User miền



Hình 4.22 Cửa sổ hoàn thành tạo user miền

4.2. Các thuộc tính của tài khoản người dùng

4.2.1 Các thông tin mở rộng của người dùng

Tab **General** chứa các thông tin chung của người dùng trên mạng mà bạn đã nhập trong lúc tạo người dùng mới. Đồng thời bạn có thể nhập thêm một số thông tin như: số điện thoại, địa chỉ mail và trang địa chỉ trang Web cá nhân…

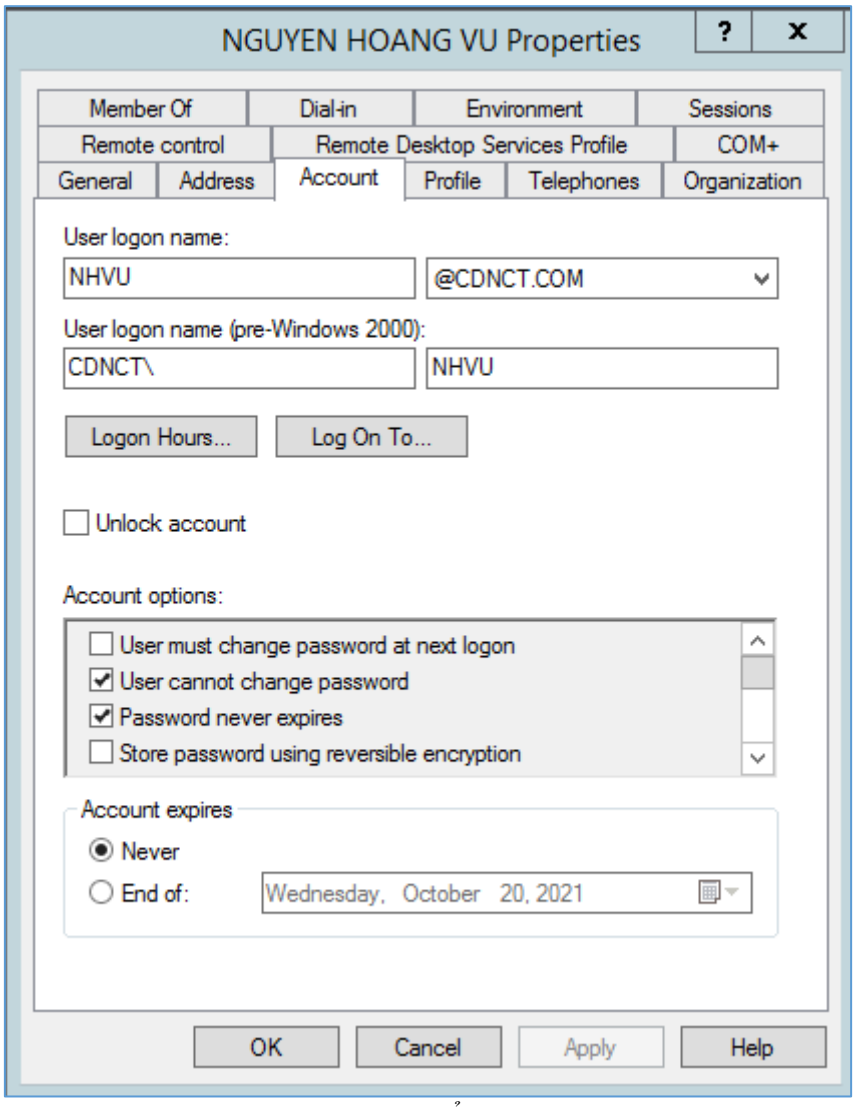
Tab **Address** cho phép bạn có thể khai báo chi tiết các thông tin liên quan đến địa chỉ của tài khoản người dùng như: địa chỉ đường, thành phố, mã vùng, quốc gia…

Tab **Telephones** cho phép bạn khai báo chi tiết các số điện thoại của tài khoản người dùng

Tab **Organization** cho phép bạn khai báo các thông tin người dùng về: chức năng của công ty, tên phòng ban trực thuộc, tên công ty …

4.2.2 Tab Account

Tab **Account** cho phép bạn khai báo lại username, quy định giờ logon vào mạng cho người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản cho người dùng, quy định thời điểm hết hạn của tài khoản...



Hình 4.23 Cửa sổ Tab Account

Điều khiển giờ logon vào mạng **(Logon Hours)**: bạn nhấp chuột vào nút Logon Hours, hộp thoại Logon Hours xuất hiện. Mặc định tất cả mọi người dùng đều được phép truy cập vào mạng 24 giờ mỗi ngày, trong tất cả 7 ngày của tuần. Khi một người dùng logon vào mạng thì hệ thống sẽ kiểm tra xem thời điểm này có nằm trong khoảng

thời gian cho phép truy cập không, nếu không phù hợp thì hệ thống sẽ không cho vào mạng và thông báo lỗi Unable to log you on because of an account restriction. Bạn có thể thay đổi quy định giờ logon bằng cách chọn vùng thời gian cần thay đổi và nhấp chuột vào nút lựa chọn Logon Permitted, nếu ngược lại không cho phép thì nhấp chuột vào nút lựa chọn Logon Denied. Sau đây là hình ví dụ chỉ cho phép người dùng làm việc từ 7h sáng đến 5h chiều, từ thứ 2 đến thứ 6.

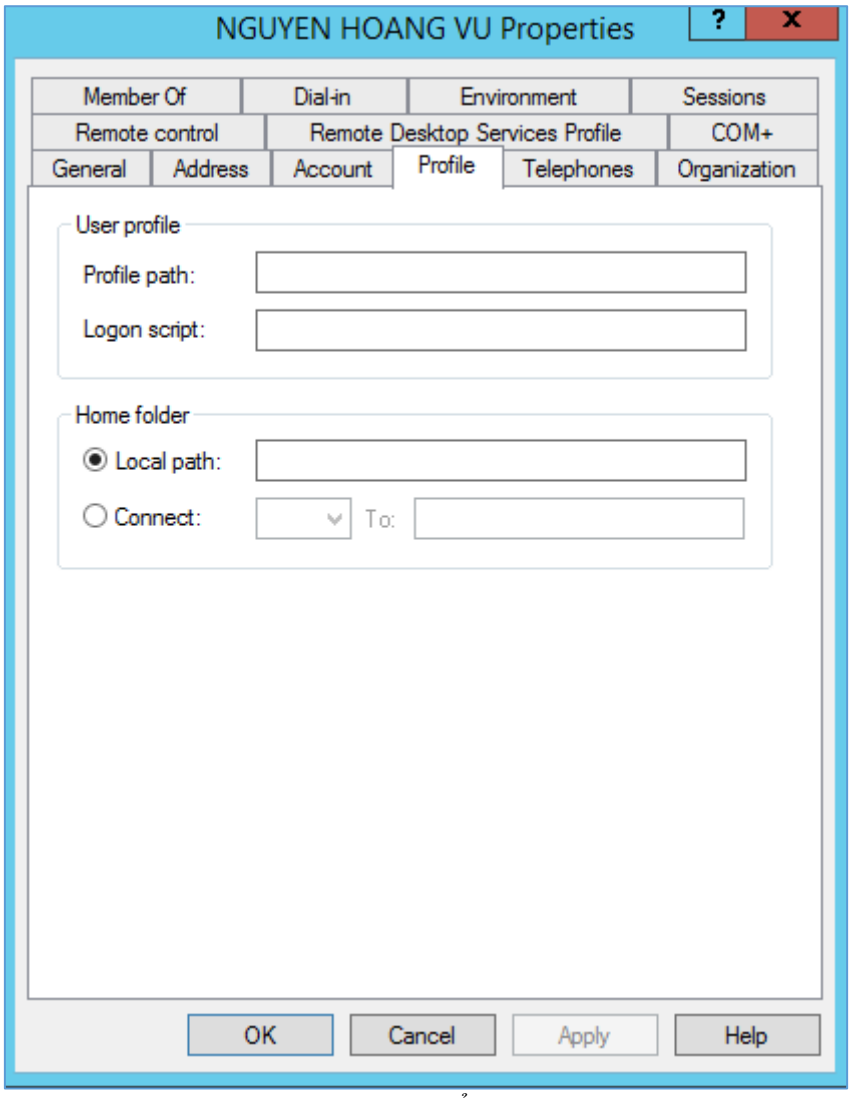
Chú ý: mặc định người dùng không bị logoff tự động khi hết giờ đăng nhập nhưng bạn có thể điều chỉnh điều này tại mục Automatically Log Off Users When Logon Hours Expire trong Group Policy phần Computer Configuration\ Windows Settings\Security Settings\ Local Policies\ Security Option. Ngoài ra bạn cũng có cách khác để điều chỉnh thông tin logoff này bằng cách dùng công cụ Domain Security Policy hoặc Local Security Policy tùy theo bối cảnh.

Chọn lựa máy trạm được truy cập vào mạng **(Log On To):** bạn nhấp chuột vào nút Log On To, bạn sẽ thấy hộp thoại Logon Workstations xuất hiện. Hộp thoại này cho phép bạn chỉ định người dùng có thể logon từ tất cả các máy tính trong mạng hoặc giới hạn người dùng chỉ được phép logon từ một số máy tính trong mạng. Ví dụ như người quản trị mạng làm việc trong môi trường bảo mật nên tài khoản người dùng này chỉ được chỉ định logon vào mạng từ một số máy tránh tình trạng người dùng giả dạng quản trị để tấn công mạng. Muốn chỉ định máy tính mà người dùng được phép logon vào mạng, bạn nhập tên máy tính đó vào mục Computer Name và sau đó nhấp chuột vào nút Add

Mục cuối cùng trong Tab này là quy định thời gian hết hạn của một tài khoản người dùng. Trong mục Account Expires, nếu ta chọn Never thì tài khoản này không bị hết hạn, nếu chọn End of: ngày tháng hết hạn thì đến ngày này tài khoản này bị tạm khóa.

4.2.3 Tab Profile

Tab Profile cho phép bạn khai báo đường dẫn đến **Profile** của tài khoản người dùng hiện tại, khai báo tập tin **logon script** được tự động thi hành khi người dùng đăng nhập hay khai báo **home folder**.



Hình 4.24 Cửa sổ Tab Profile

Trước tiên chúng ta hãy tìm hiểu khái niệm **Profile**. **User Profiles** là một thư mục chứa các thông tin về môi trường của **Windows Server** cho từng người dùng mạng. **Profile** chứa các qui định về màn hình **Desktop**, nội dung của menu **Start,** kiểu cách phối màu sắc, vị trí sắp xếp các **icon**, biểu tượng chuột…

Mặc định khi người dùng đăng nhập vào mạng, một **profile** sẽ được mở cho người dùng đó. Nếu là lần đăng nhập lần đầu tiên thì họ sẽ nhận được một **profile** chuẩn. Một thư mục có tên giống như tên của người dùng đăng nhập sẽ được tạo trong thư mục **Documents and Settings**. Thư mục **profile** người dùng được tạo chứa một tập tin **ntuser.dat**, tập tin này được xem như là một thư mục con chứa các liên kết thư mục đến các biểu tượng nền của người dùng. Trong **Windows Server** có ba loại **Profile**:

Local Profile: là **profile** của người dùng được lưu trên máy cục bộ và họ tự cấu hình trên **profile** đó.

Roaming Profile: là loại **Profile** được chứa trên mạng và người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, để tự động duy trì một bản sao của tài khoản người dùng trên mạng.

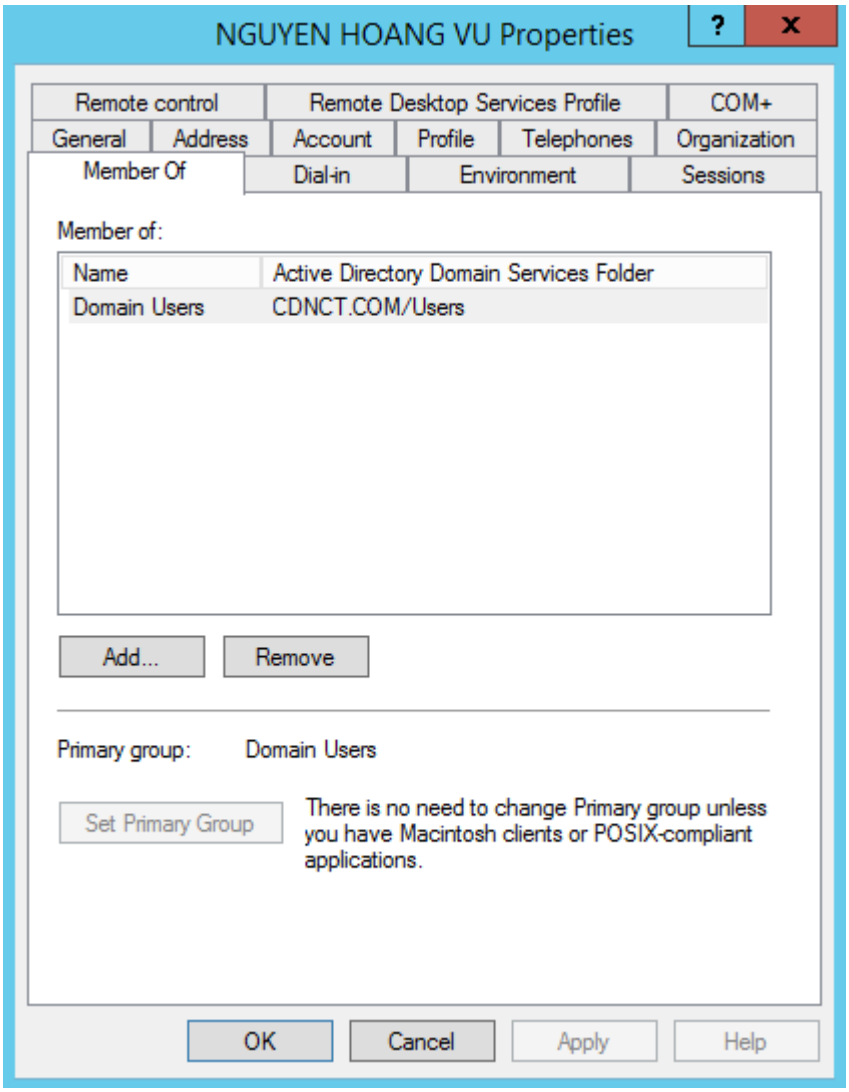
Mandatory Profile: người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, sau đó chép một profile đã cấu hình sẵn vào đường dẫn đó. Lúc đó các người dùng dùng chung **profile** này và không được quyền thay đổi profile đó.

Kịch bản đăng nhập (**logon script** hay **login script**) là những tập tin chương trình được thi hành mỗi khi người dùng đăng nhập vào hệ thống, với chức năng là cấu hình môi trường làm việc của người dùng và phân phát cho họ những tài nguyên mạng như ổ đĩa, máy in (được ánh xa từ **Server**). Bạn có thể dùng nhiều ngôn ngữ kịch bản để tạo ra **logon script** như: lệnh **shell** của **DOS/NT/Windows**, **Windows Scripting Host (WSH), VBScript, Jscript**…

Thư mục cá nhân (**home folder hay home directory**) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục nhân cho người dùng thì trong mục **Connect** bạn chọn ổ đĩa hiển thị trên máy trạm và đường dẫn mà đĩa này cần ánh xạ đến (chú ý là các thư mục dùng chung đảm bảo đã chia sẻ). Trong ví dụ này bạn chỉ thư mục cá nhân cho tài khoản Tuan là "\\server\tuan", nhưng bạn có thể thay thế tên tài khoản bằng biến môi trường người dùng như: "\\server\%username%".

4.2.4 Tab Member Of

Tab Member Of cho phép bạn xem và cấu hình tài khoản người dùng hiện tại là thành viên của những nhóm nào. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này. Muốn gia nhập vào nhóm nào bạn nhấp chuột vào nút **Add**, hộp thoại chọn nhóm sẽ hiện ra.

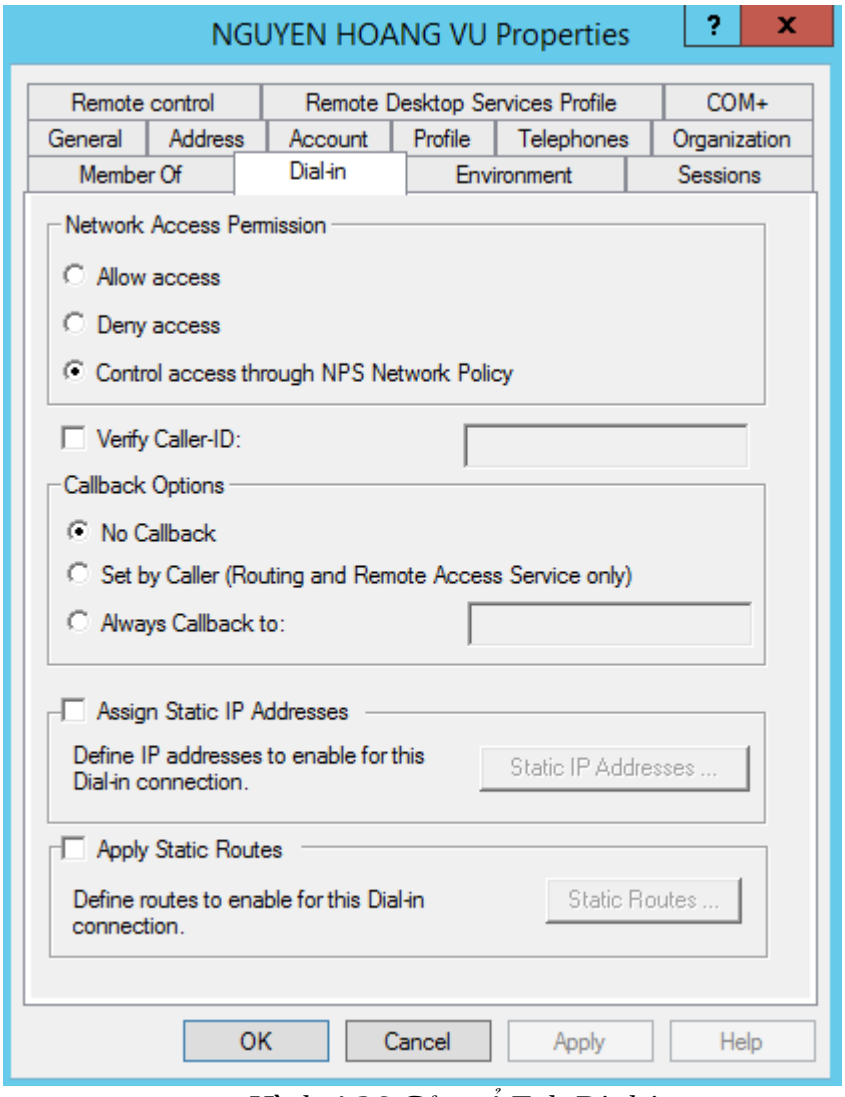


Hình 4.25 Cửa sổ Tab Member Of

Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server** tránh tình trạng tìm kiếm và hiển thị hết tất cả các nhóm hiện có trong hệ thống. Nếu bạn không nhớ tên nhóm thì chấp nhận nhấp chuột vào nút **Advanced** và **Find Now** để tìm hết tất cả các nhóm
Nếu bạn muốn tài khoản người dùng hiện tại thoát ra khỏi một nhóm nào đó thì bạn chọn nhóm sau đó nhấp chuột vào nút **Remove**.

4.2.5 Tab Dial-in

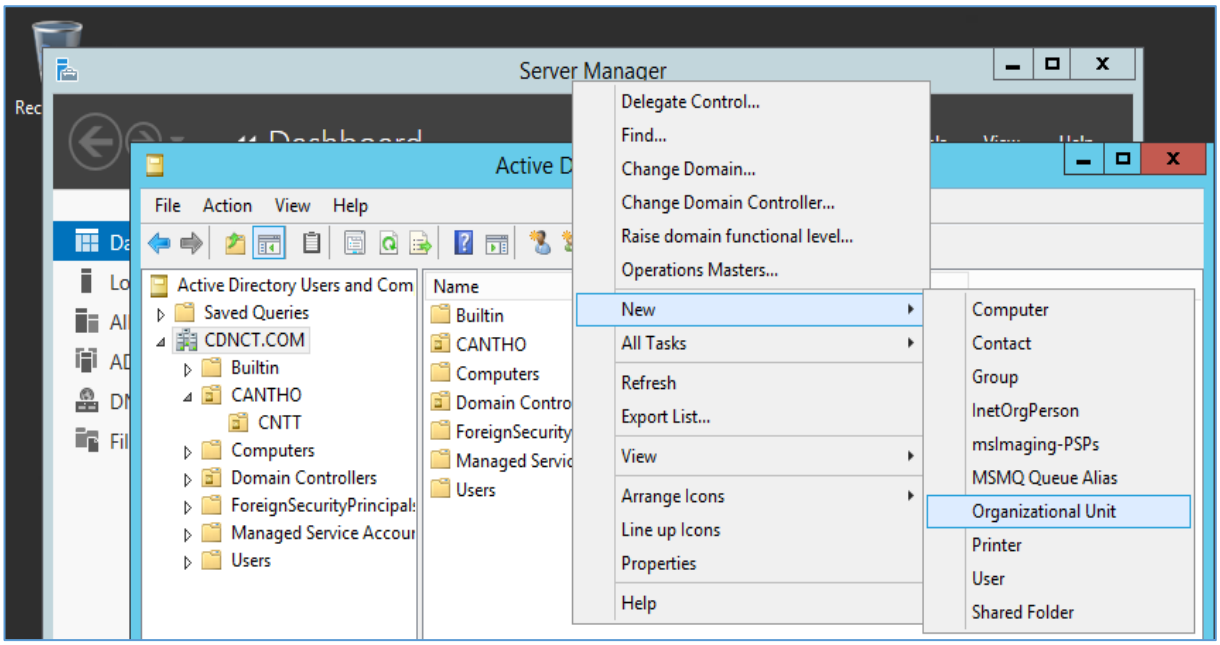
Tab **Dial-in** cho phép bạn cấu hình quyền truy cập từ xa của người dùng cho kết nối **dial-in** hoặc **VPN**, chúng ta sẽ khảo sát chi tiết ở chương **Routing and Remote Access**



Hình 4.26 Cửa sổ Tab Dial-in

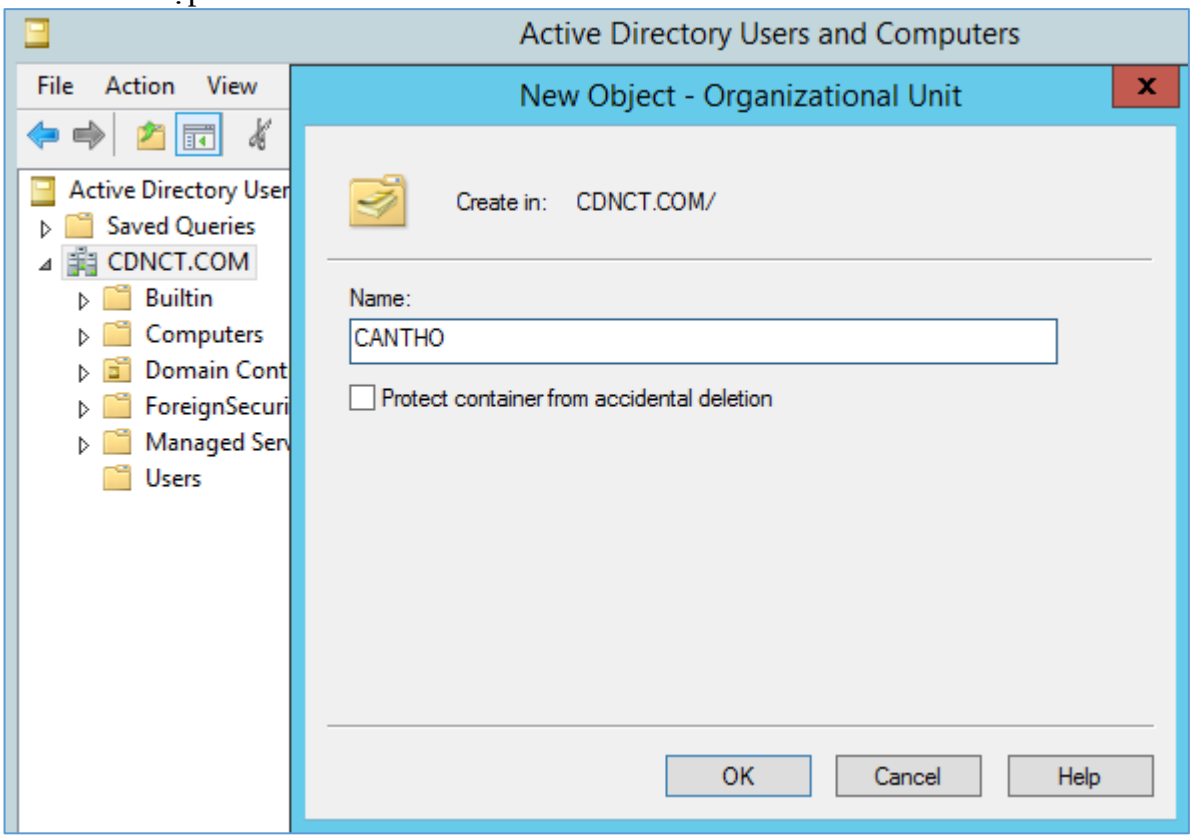
4.3. Tạo mới tổ chức trên active directory

Bước 1: Chọn miền chứa tổ chức, Right click chon New, Organizational Unit



Hình 4.27 Cửa sổ tạo tổ chức

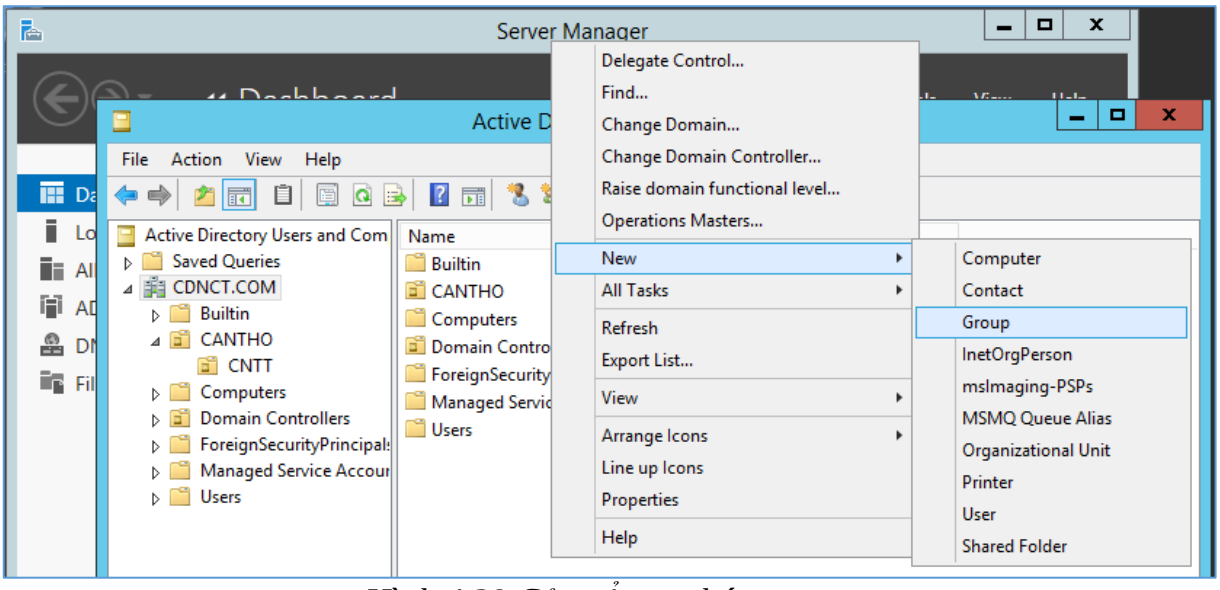
Bước 2: Nhập tên tổ chức



Hình 4.28 nhập tên tổ chức

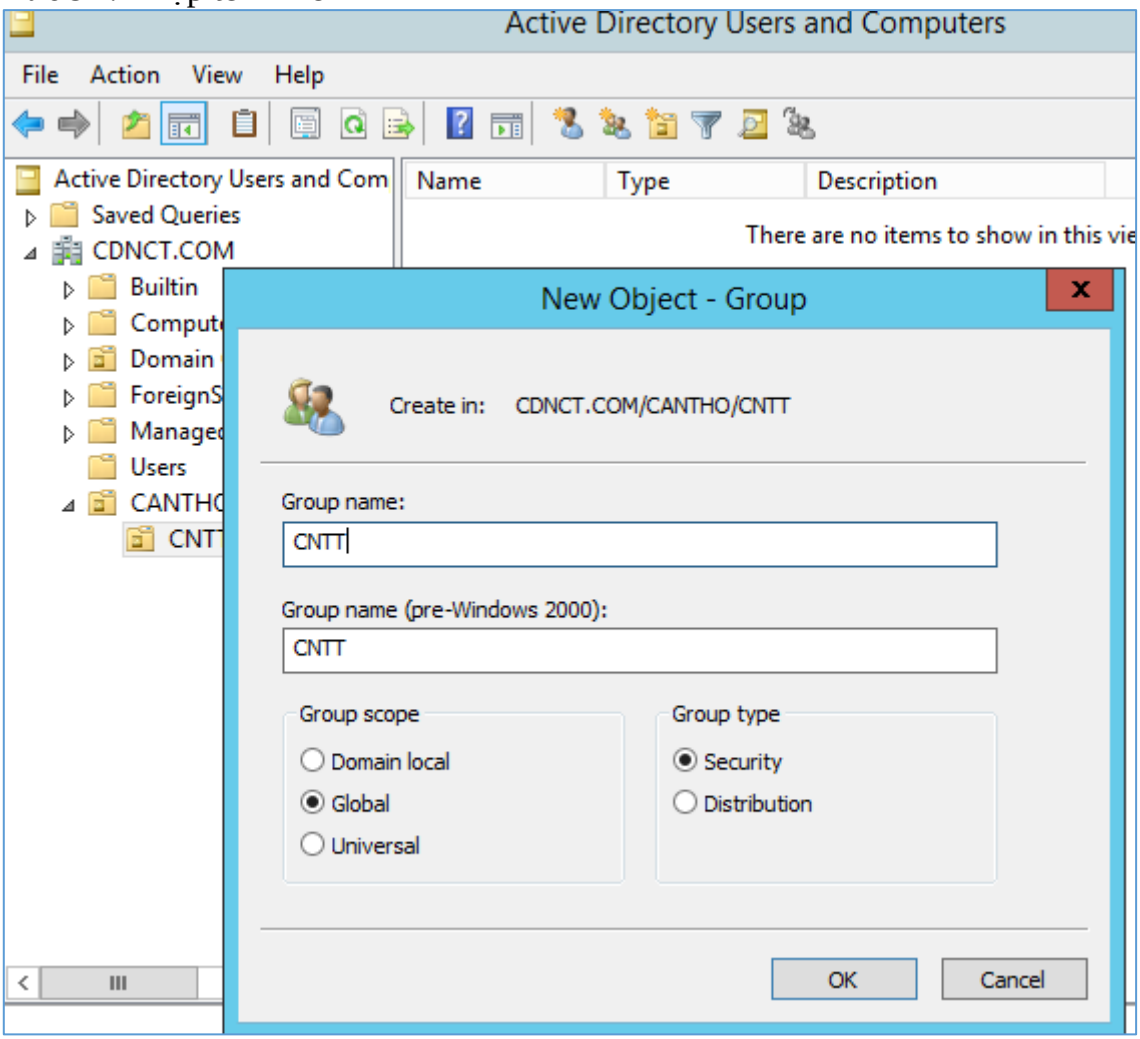
4.4. Tạo mới nhóm trên active directory

Bước 1: Chọn nơi chứa nhóm, Right click chon New, Group



Hình 4.29 Cửa sổ tạo nhóm

Bước 2: Nhập tên Nhóm



Hình 4.30 nhập tên nhóm

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

Windows Server 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 server** 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** của **Windows**.

4.4.1 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]
Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị danh sách của tất cả các tài khoản người dùng trên máy tính
- [**Username**]: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị. Tên của tài khoản người dùng có thể dài đến 20 ký tự.
- [**Password**]: ấn định hoặc thay đổi mật mã của tài khoàn người dùng. Một mật mã phải có chiều dài tối thiểu bằng với chiều dài quy định trong chính sách tài khoản người dùng. Trong **Windows** thì chiều dài của mật mã có thể dài đến 127 ký tự, nhưng trên hệ thống **Win9X** thì chỉ hiểu được 14 ký tự, do đó nếu bạn đặt mật mã dài hơn 14 ký tự thì có thể tài khoản này không thể **logon** vào mạng từ máy trạm dùng **Win9X**.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows Server** là **primary domain controller** hoặc **Windows Professional** là thành viên của máy **Windows Server domain**.
- [**/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.
- [**/active:{no | yes}**]: cho phép hoặc tạm khóa tài khoản người dùng. Nếu tài khoản bị khóa thì người dùng không thể truy cập các tài nguyên trên máy tính. Mặc định là cho phép (**active**).
- [**/comment:"text"**]: cung cấp mô tả về tài khoản người dùng, mô tả này có thể dài đến 48 ký tự.
- [**/countrycode:nnn**]: chỉ định mã quốc gia và mã vùng.
- [**/expires:{date | never}**]: quy định ngày hết hiệu lực của tài khoản người dùng.
- [**/fullname:"name"**]: khai báo tên đầy đủ của người dùng.
- [**/homedir:path**]: khai báo đường dẫn thư mục cá nhân của tài khoản, chú ý đường dẫn này đã tồn tại.
- [**/passwordchg:{yes | no}**]: chỉ định người dùng có thể thay đổi mật mã của mình không, mặc định là có thể.
- [**/passwordreq:{yes | no}**]: chỉ định một tài khoản người dùng phải có một mật mã, mặc định là có mật mã.
- [**/profilepath:[path]**]: khai báo đường dẫn **Profile** của người dùng, nếu không hệ thống sẽ tự tạo một profile chuẩn cho người dùng lần **logon** đầu tiên.
- [**/scriptpath:path**]: khai báo đường dẫn và tập tin **logon script**. Đường dẫn này có thể là đường dẫn tuyệt đối hoặc đường dẫn tương đối (ví dụ: %systemroot%\System32\Repl\Import\Scripts).
- [**/times:{times | all}**]: quy định giờ cho phép người dùng logon vào mạng hay máy tính cục bộ. Các thứ trong tuần được đại diện bởi ký tự: M, T, W, Th, F, Sa,

Su. Giờ ta dùng AM, PM để phân biệt buổi sáng hoặc chiều. Ví dụ sau chỉ cho phép người dùng làm việc trong giờ hành chính từ thứ 2 đến thứ 6: "M,7AM-5PM; T,7AM-5PM; W,7AM-5PM; Th,7AM-5PM; F,7AM-5PM;"

- [**/workstations:{computername[,...] | *}**]: chỉ định các máy tính mà người dùng này có thể sử dụng để logon vào mạng. Nếu **/workstations** không có danh sách hoặc danh sách là ký tự '*' thì người dùng có thể sử dụng bất kỳ máy nào để vào mạng.

4.4.2 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]

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị tên của Server và tên của các nhóm trên Server đó.
- [**Groupname**]: chỉ định tên nhón cần thêm, mở rộng hoặc xóa.
- [**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows Server** là **primary domain controller** hoặc **Windows Professional** là thành viên của máy **Windows Server domain**.
- [**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.

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

Trên hệ thống **Windows Server**, **Microsoft** phát triển thêm một số lệnh nhằm hỗ trợ tốt hơn cho dịch vụ **Directory** như: **dsadd**, **dsrm**, **dsmove**, **dsget**, **dsmod**, **dsquery**. Các lệnh này thao tác chủ yếu trên các đối tượng **computer, contact, group, ou, user, quota.**

- **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**.

Ví dụ:

- Tạo một **user** mới:
  dsadd user "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn" –samid hv10 –pwd 123
- Xóa một **user**: dsrm "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn"

- Xem các **user** trong hệ thống: **dsquery user**
- Gia nhập **user** mới vào nhóm:
  dsmod group “CN=hs, CN=Users, DC=netclass, DC=edu, DC=vn”
  addmbr “CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn”
-

Bài tập thực hành của học viên

1. Trên máy Domain Controller tạo OU có tên CANTHO.
2. Trong OU CANTHO tạo 2 nhóm có tên là Ke Toan và Nhan Su.
3. Trong mỗi nhóm tạo 3 user.
4. Chỉ cho phép các user logon vào mạng từ 7:00am-6:00pm.
5. Tạo Home Folder cho các user.

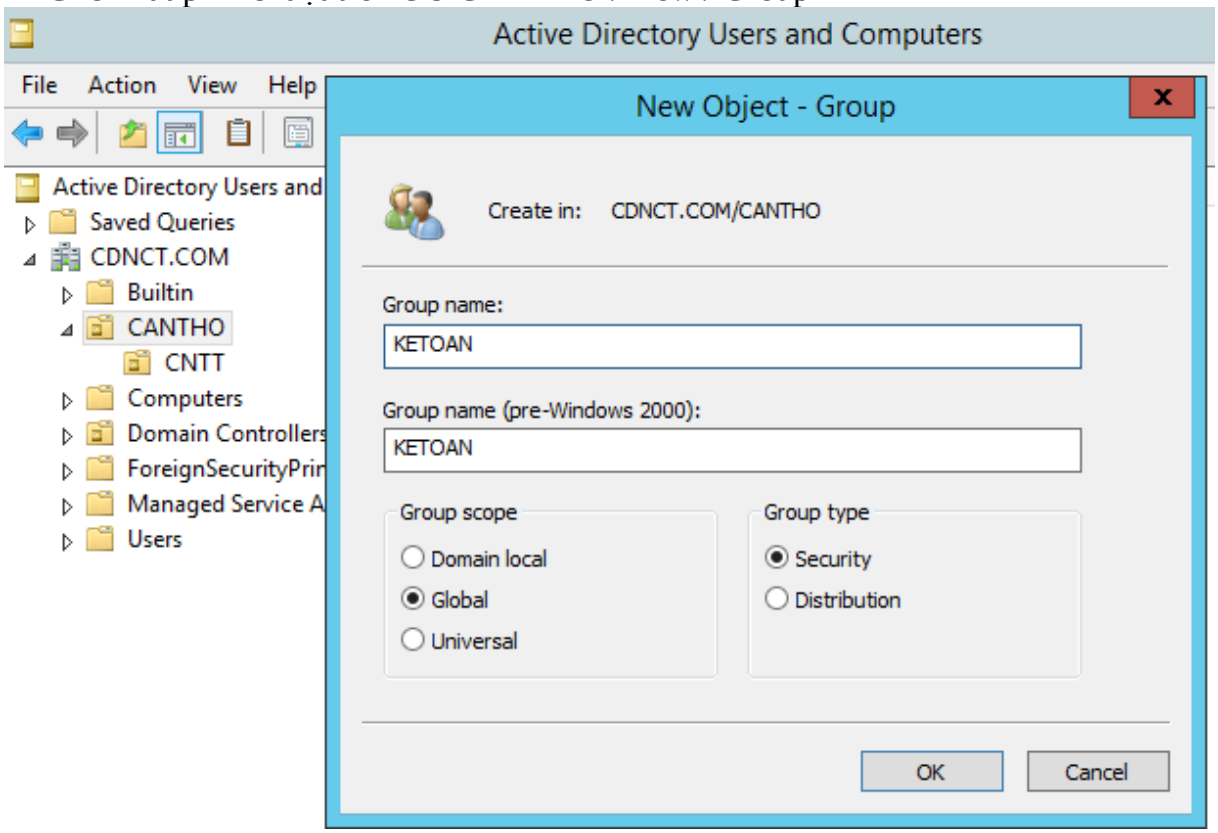
Hướng dẫn thực hiện:

1. Tạo OU có tên CANTHO

Xem 2 bước ở mục 4.3

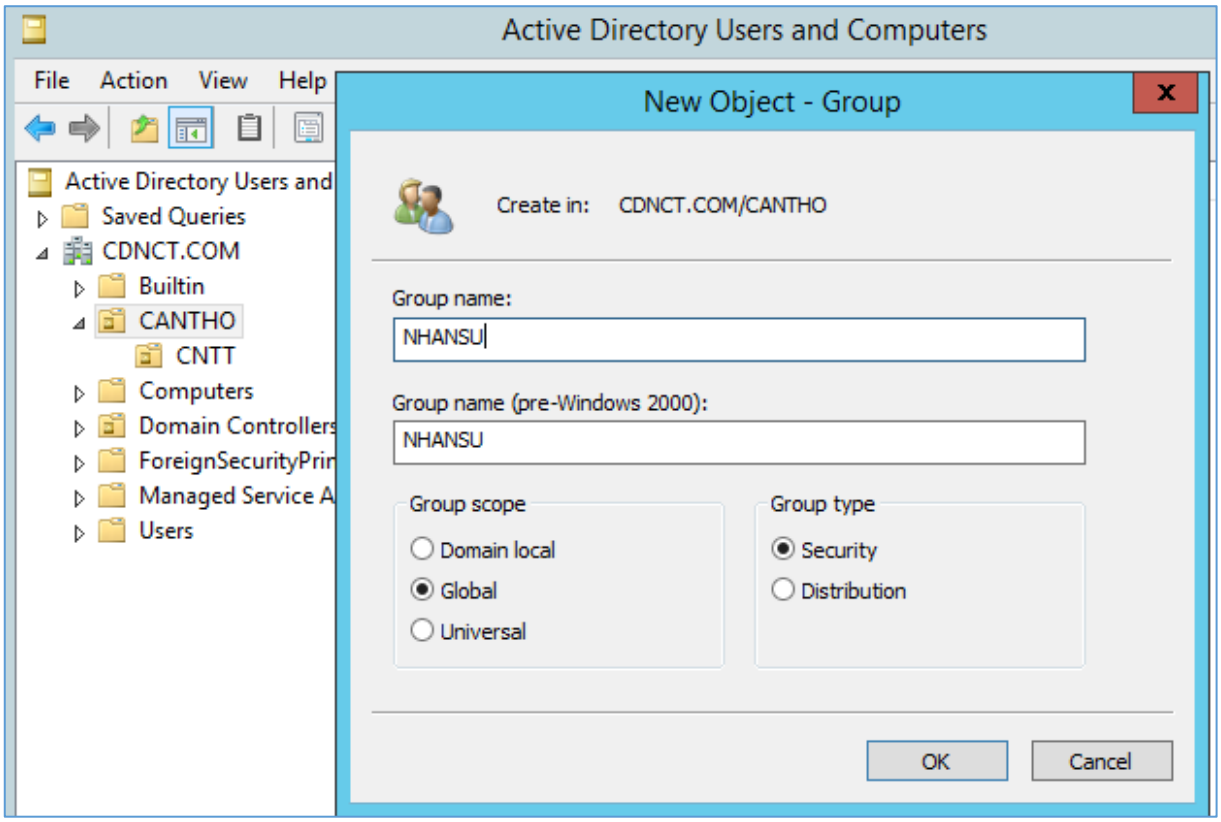
2. Trong OU CANTHO tạo 2 nhóm có tên là Ke Toan và Nhan Su:

☞ Click nút phải chuột trên OU ***CANTHO*** / New / Group như hình sau:



Hình 4.31 nhập tên nhóm ketoan

☞ **Tương tự tạo Group “Nhan Su”**



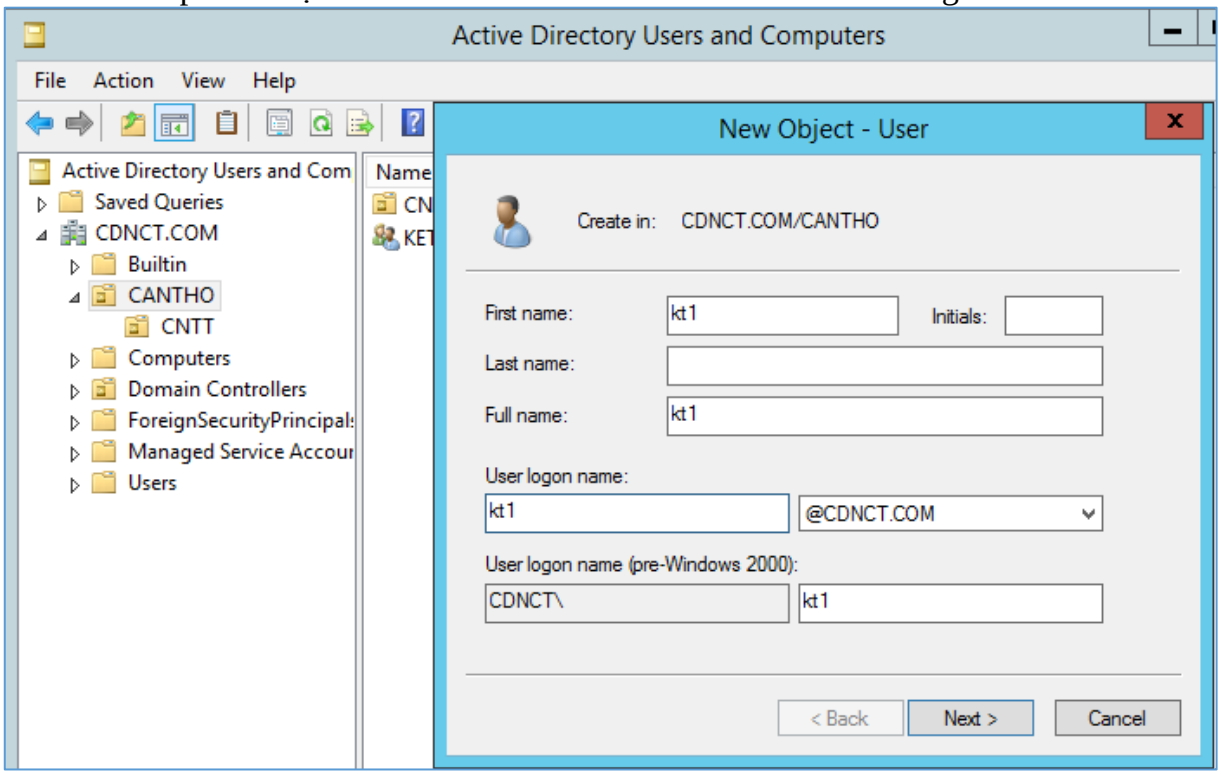
Hình 4.31 nhập tên nhóm nhansu

3. Trong mỗi nhóm tạo 3 user:

a). Tạo Users

(Chú ý: Sau khi tạo xong các User hãy nhập các thông tin về các User đó như: Số điện thoại, địa chỉ, email, địa chỉ Web, nhập tên người quản lý....)

☞ Click nút phải chuột trên OU ***CANTHO*** / New / User / điền thông tin cho user kt1

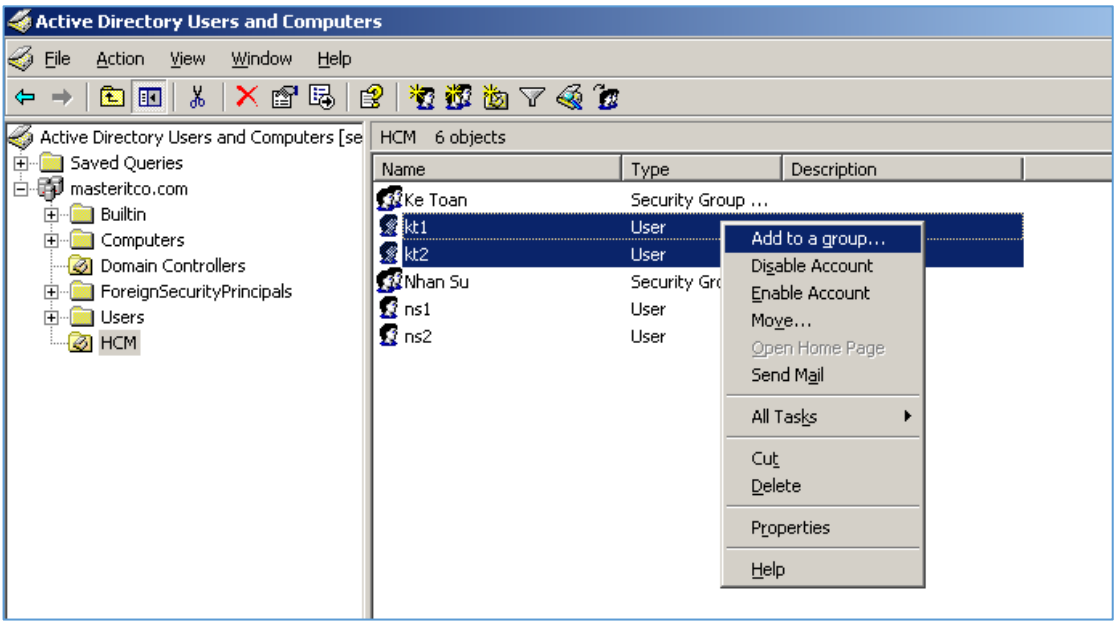


Hình 4.31 nhập tên user kt1

☞ **Lặp lại tương tự cho các user KT2, KT3, NS1, NS2, NS3**

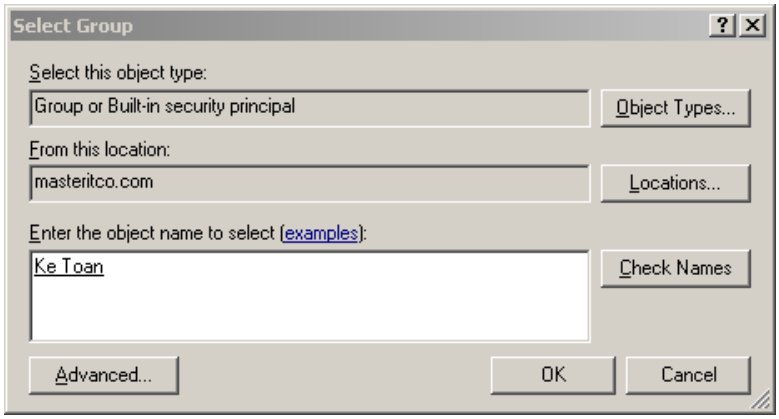
b). Thiết lập Users thuộc Group:

Bước 1: Chọn 3 user KT1, KT2 và KT3 / click nút phải chuột trên 3 user / Add to a group



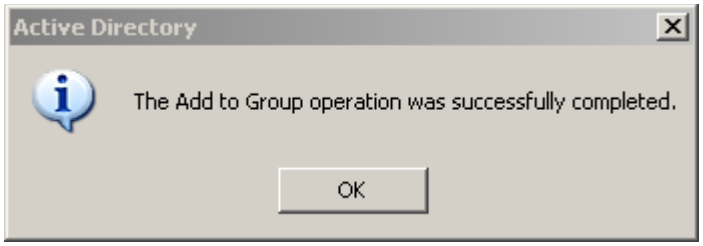
Hình 4.32 Add user vào group

Bước 2: Gõ tên nhóm "Ke Toan" / Check Names / xuất hiên gạch chân trên group "Ke Toan"



Hình 4.32 Chọn group ketoan

Bước 3: xác nhận cho user vào nhóm



Hình 4.33 xác nhận thành công

☞ Làm tương tự với các user NS1, NS2 và NS3 để đưa vào nhóm "Nhan Su"

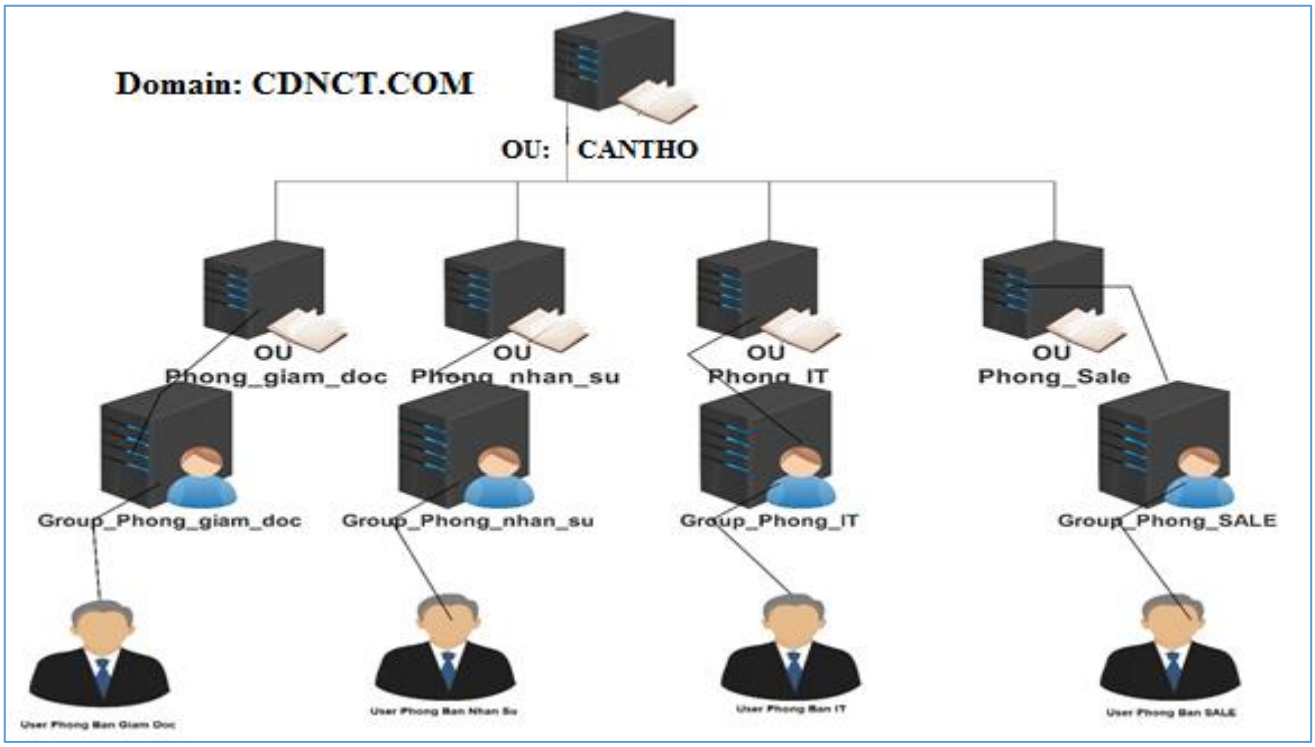
Những trọng tâm cần chú ý:

- Tạo các OU đúng yêu cầu và phải được thay đổi khi cần
- Tạo và cấp quyền đúng cho các user trên hệ thống
- Đưa các user vào đúng Group theo yêu cầu
- Cấp và giới hạn đúng các thuộc tính cho từng nhóm User.

- Thiết lập quyền đăng nhập vào hệ thống như đúng tên, đúng giờ

Bài mở rộng và nâng cao

Bài tập: Hãy cài đặt và Cấu hình bài Lab trên Windows Server 2019 theo mô hình sau:



Yêu cầu đánh giá kết quả học tập

Nội dung

– Về kiến thức:
  + Trình bày được tài khoản người dùng, nhóm cục bộ và miền
  + Phân biệt được tài khoản người dùng, nhóm cục bộ và miền
– Về kỹ năng:
  + Thao tác thành thạo quản lý được tài khoản người dùng và nhóm trên hệ thống Windows Server 2019.
  + Thực hiện được cấp quyền cho tài khoản người dùng và nhóm
  + Kiểm soát được hoạt động truy cập của người dùng
  + Thao tác thành thạo việc Nâng cấp Server thành Domain Controller trên Windows Server 2019
  + Thực hiện đúng Gia nhập máy trạm vào Domain
  + Thực hiện đúng Additional Domain Controller trên hệ thống.
– Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

– Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
– Về kỹ năng:
  + Đánh giá kỹ năng thực hành về các thao tác cấp quyền cho tài khoản người dùng và nhóm
  + Đánh giá kỹ năng thực hành về các thao tác quản lý, kiểm soát trên Windows Server 2019.

– Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 5: QUẢN LÝ ĐĨA VÀ DỮ LIỆU
Mã bài: MĐ 17 - 05

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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Cấu hình hệ thống tập tin

Mục tiêu:

- Phân biệt được các loại định dạng hệ thống tập tin trên đĩa cứng.

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: **FAT**, **FAT32** và **NTFS**. Nếu bạn định sử dụng các tính năng như bảo mật cục bộ, nén và mã hoá các tập tin thì bạn nên dùng **NTFS**. Bảng sau trình bày khả năng của từng hệ thống tập tin trên **Windows Server**:

Khả năng	FAT	FAT32	NTFS
Hệ điều hành hỗ trợ	Hầu hết các hệ điều hành	Windows 95/98/ 2000/XP/2003/ Vista/7/2008/8/ 2012/10/2016/ 2019	Windows XP/2003/ Vista/7/2008/8/201 2/10/2016/ 2019
Hỗ trợ tên tập tin dài	256 ký tự trên Windows	256 ký tự	256 ký tự
Sử dụng hiệu quả đĩa	Không	Có	Có
Hỗ trợ nén đĩa	Không	Không	Có
Hỗ trợ hạn ngạch	Không	Không	Có
Hỗ trợ mã hoá	Không	Không	Có
Hỗ trợ bảo mật cục bộ	Không	Không	Có
Hỗ trợ bảo mật trên mạng	Có	Có	Có
Kích thước Volume tối đa được hỗ trợ	4GB	32GB	1024GB

Trên **Windows Server/Windows/NT**, bạn có thể sử dụng lệnh **CONVERT** để chuyển đổi hệ thống tập tin từ **FAT, FAT32** thành **NTFS**. Cú pháp của lệnh như sau:

CONVERT [ổ đĩa:] /fs:ntfs

2. Cấu hình đĩa lưu trữ

Mục tiêu:

- Phân biệt được các loại đĩa lưu trữ trên windows server.

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. Bạn có thể tạo ba partition primary

và một partition extended. Với partition extended, bạn có thể tạo ra nhiều partition logical.

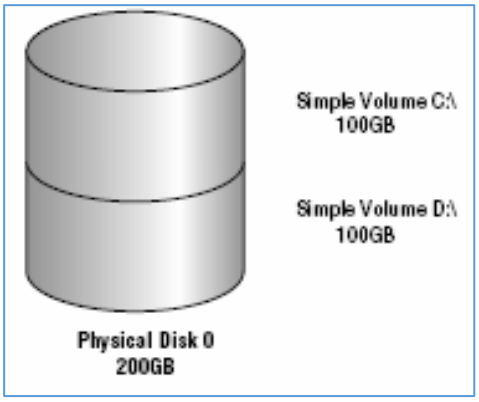
2.2. Dynamic storage

Đây là một tính năng mới của Windows Server. 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 và Windows. Windows Server/ Windows hỗ trợ năm loại volume dynamic: simple, spanned, striped, Mirroreded 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.

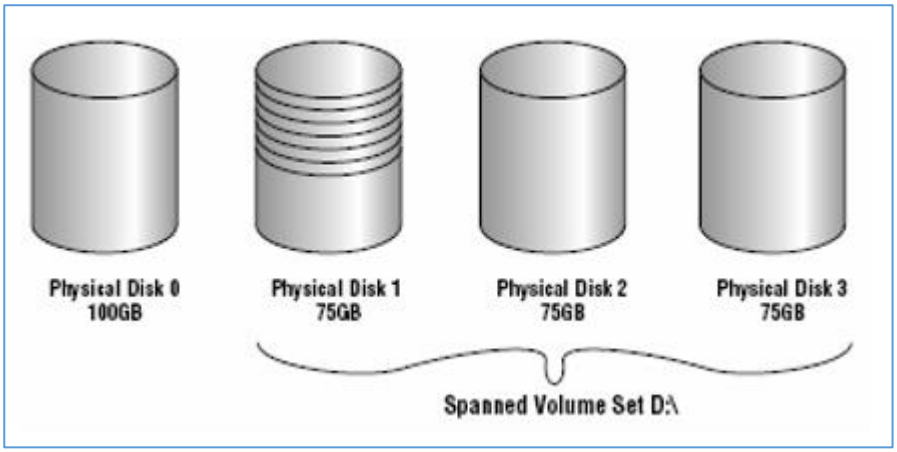
Chứa không gian lấy từ một đĩa **dynamic** duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục. Hình sau minh hoạ một đĩa vật lý được chia thành hai **volume** đơn giản.



Hình 5.1 Volume simple

2.2.2 Volume spanned.

Bao gồm một hoặc nhiều đĩa **dynamic** (tối đa là 32 đĩa). Sử dụng khi bạn 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.



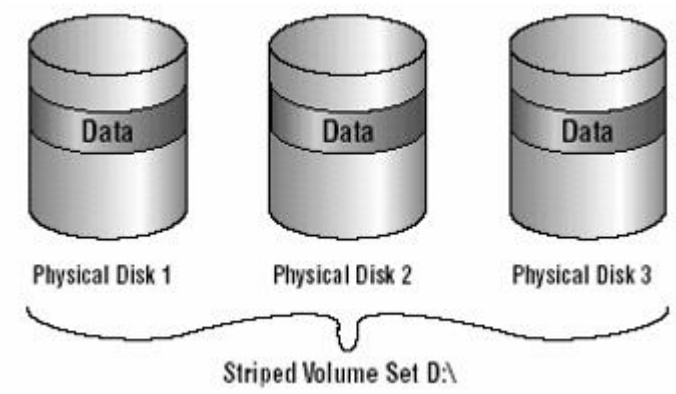
Hình 5.2 Volume spanned

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 (tối đa là 32). Do dữ liệu được ghi tuần tự lên từng dãy, nên bạn 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.

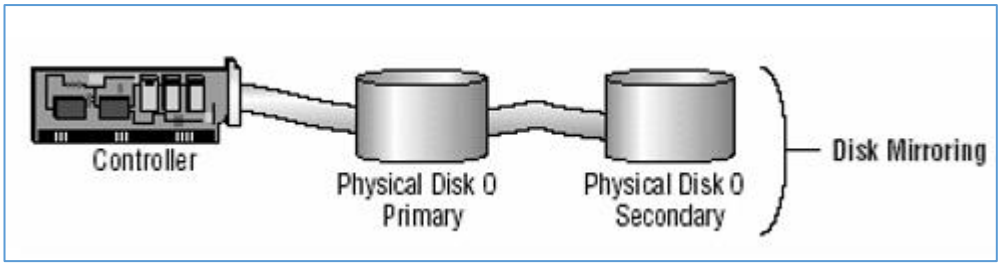


Hình 5.3 Volume striped

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

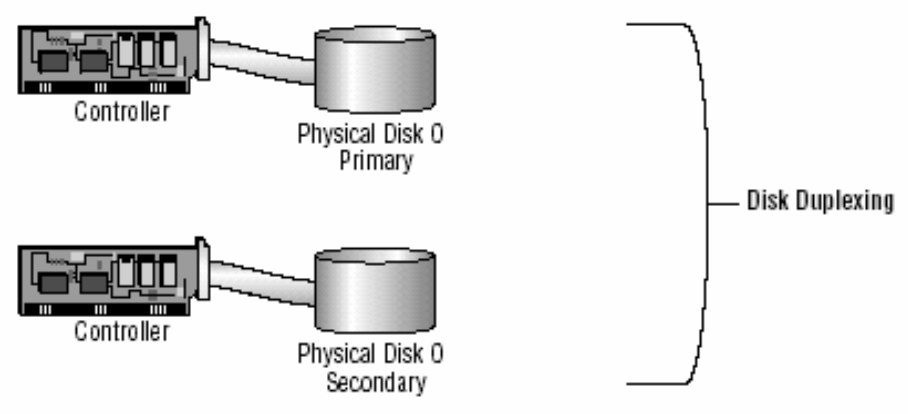
2.2.4 Volume Mirroreded.

Là hai bản sao của một **volume** đơn giản. Bạn 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 Volume Mirroreded

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

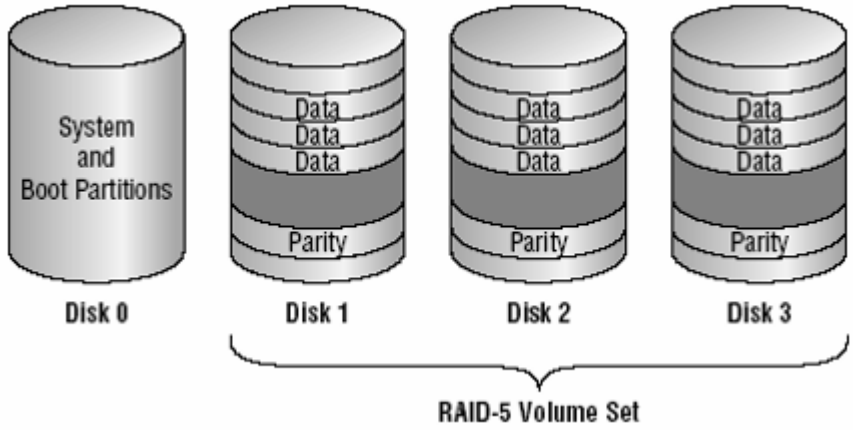


Hình 5.5 Volume Mirroreded duplexing

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 (tối đa là 32).



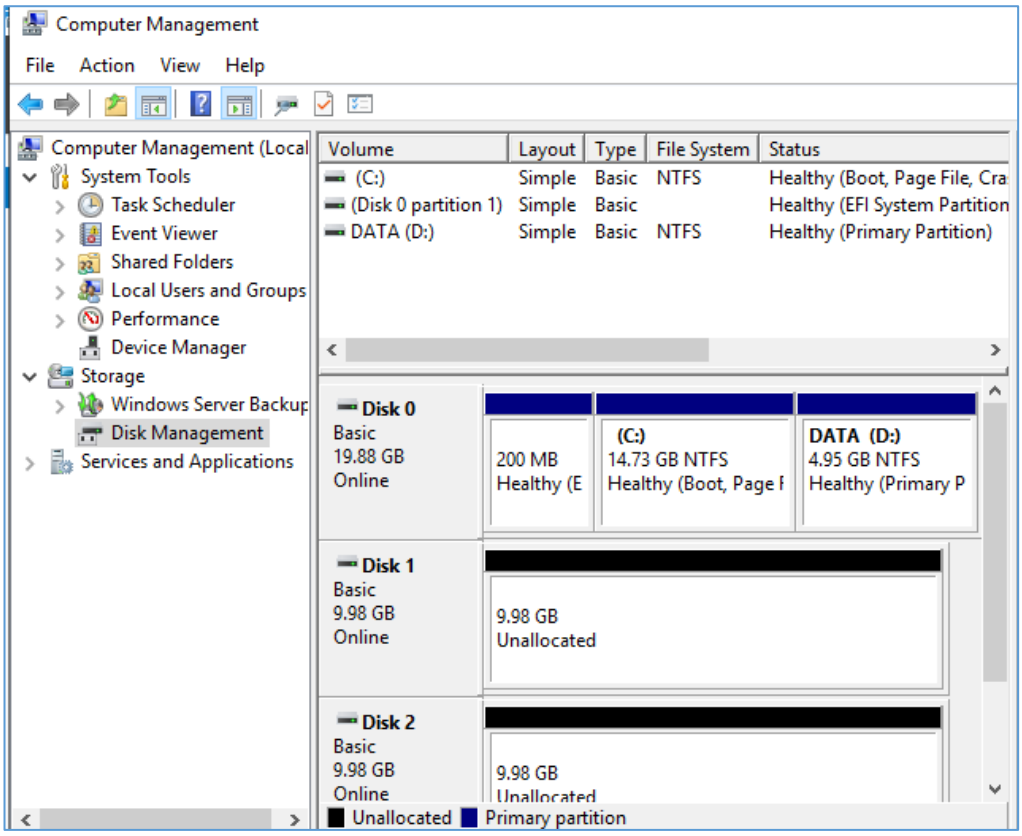
Hình 5.6 Volume Volume RAID-5

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

Mục tiêu: Sử dụng được công cụ Disk Manager để quản lý đĩa cứng.

Disk Manager là một tiện ích giao diện đồ hoạ phục vụ việc quản lý đĩa và volume trên môi trường Windows và Windows Server. Để có thể sử dụng được hết các chức năng của chương trình, bạn phải đăng nhập vào máy bằng tài khoản Administrator. Vào menu Start \ Programs \ Administrative Tools \ Computer Management. Sau đó mở rộng mục Storage và chọn Disk Management. Cửa sổ Disk Management xuất hiện như sau:

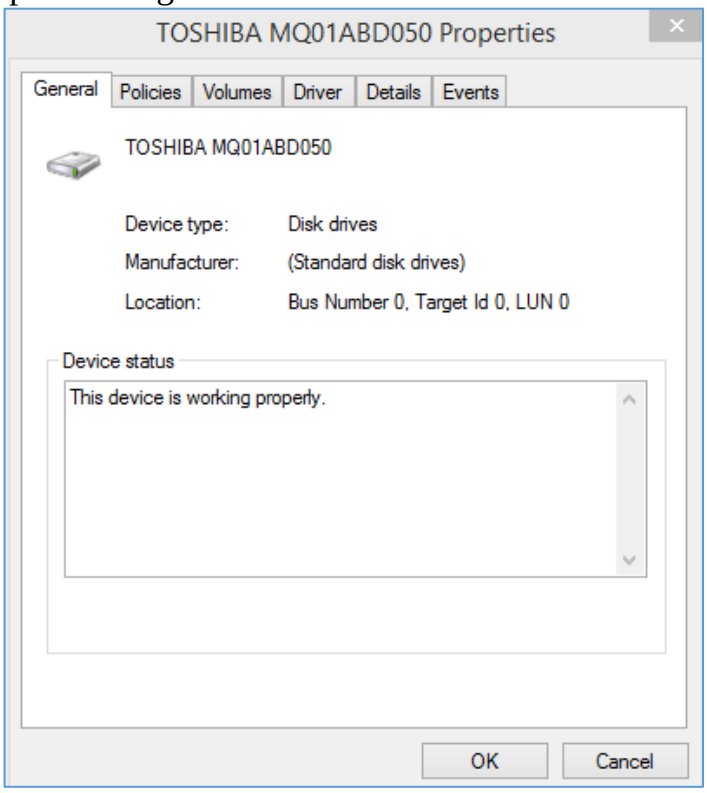


Hình 5.7 Volume Disk Manager

3.1. Xem thuộc tính của đĩa

Nhấp phải chuột lên ổ đĩa vật lý muốn biết thông tin và chọn Properties. Hộp thoại Disk Properties xuất hiện như sau:

Hộp thoại cung cấp các thông tin:



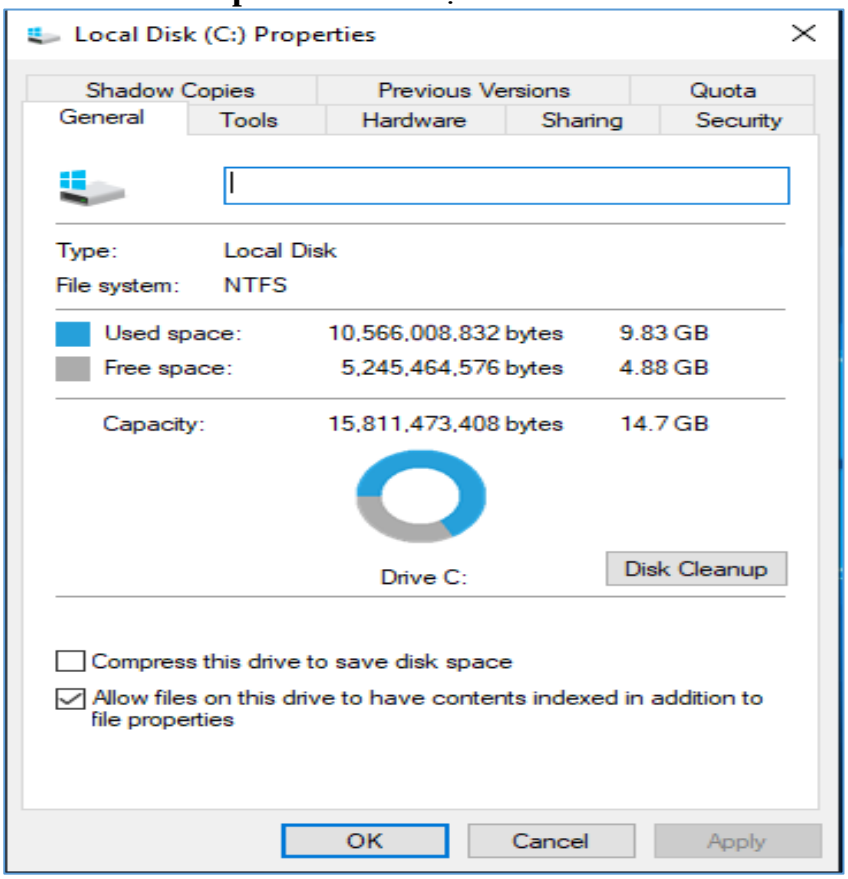
Hình 5.8 Disk Properties

- 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

Trên một ổ đĩa **dynamic**, bạn sử dụng các **volume**. Ngược lại trên một ổ đĩa **basic**, bạn sử dụng các đĩa cục bộ (**local disk**). **Volume** và đĩa cục bộ đều có chức năng như nhau, do vậy các phần sau dựa vào đĩa cục bộ để minh hoạ. Để xem thuộc tính của một đĩa cục bộ, bạn nhấp phải chuột lên đĩa cục bộ đó và chọn **Properties** và hộp thoại **Local Disk Properties** xuất hiện.



Hình 5.9 Local Disk Properties

3.2.1 Tab General.

Cung cấp các thông tin như nhãn đĩa, loại, hệ thống tập tin, dung lượng đã sử dụng, còn trống và tổng dung lượng. Nút **Disk Cleanup** dùng để mở chương trình **Disk Cleanup** dùng để xoá các tập tin không cần thiết, giải phóng không gian đĩa.

3.2.2 Tab Tools.

Bấm nút **Check Now** để kích hoạt chương trình **Check Disk** dùng để kiểm tra lỗi như khi không thể truy xuất đĩa hoặc khởi động lại máy không đúng cách. Nút **Backup Now** sẽ mở chương trình **Backup Wizard**, hướng dẫn bạn các bước thực hiện việc sao lưu các tập tin và thư mục trên đĩa. Nút **Defragment Now** mở

chương trình **Disk Defragment**, dùng để dồn các tập tin trên đĩa thành một khối liên tục, giúp ích cho việc truy xuất đĩa.

3.2.3 Tab Hardware

Liệt kê các ổ đĩa vật lý **Windows Server** nhận diện được. Bên dưới danh sách liệt kê các thuộc tính của ổ đĩa được chọn.

3.2.4 Tab Sharing

Cho phép chia sẻ hoặc không chia sẻ ổ đĩa cục bộ này. Theo mặc định, tất cả các ổ đĩa cục bộ đều được chia sẻ dưới dạng ẩn (có dấu **$** sau tên chia sẻ).

3.2.5 Tab Security

Chỉ xuất hiện khi đĩa cục bộ này sử dụng hệ thống tập tin **NTFS**. Dùng để thiết lập quyền truy cập lên đĩa. Theo mặc định, nhóm **Everyone** được toàn quyền trên thư mục gốc của đĩa.

3.2.6 Tab Quota

Chỉ xuất hiện khi sử dụng **NTFS**. Dùng để quy định lượng không gian đĩa cấp phát cho người dùng.

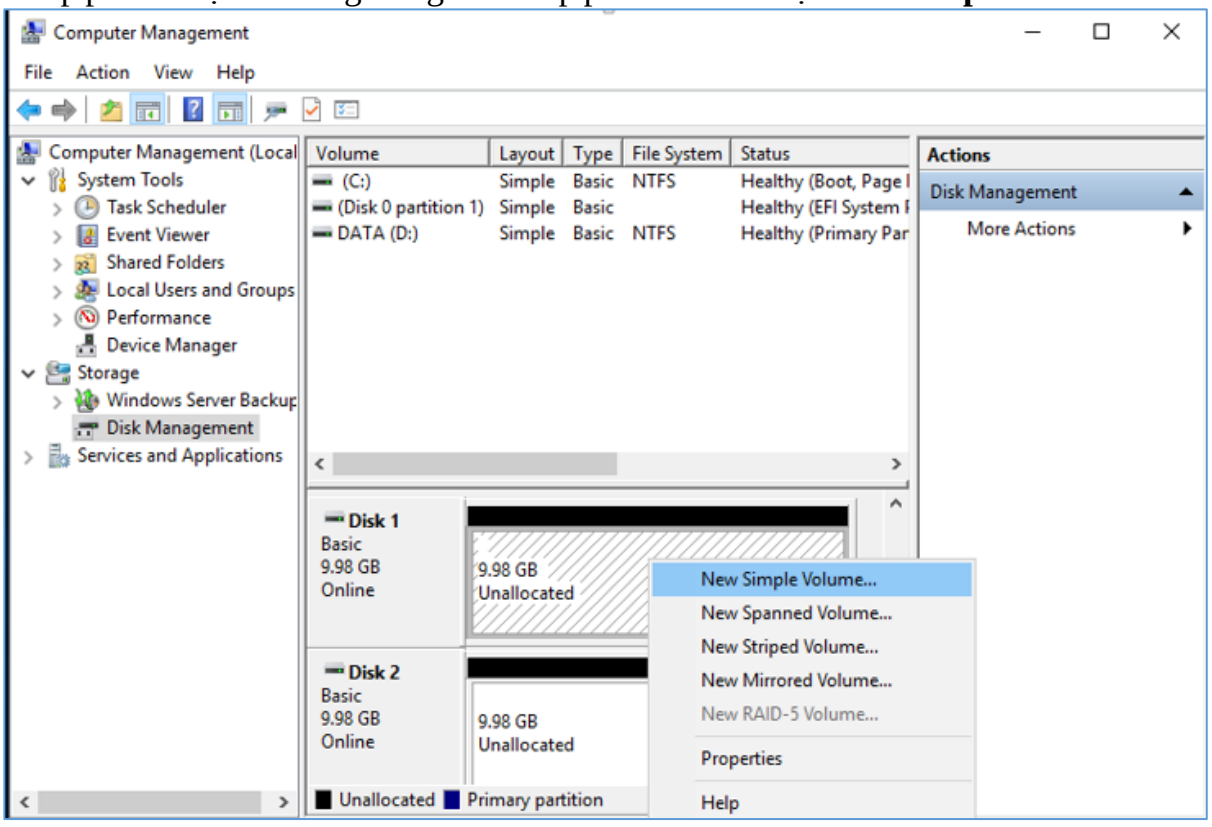
3.2.7 Shadow Copies

Shadow Copies là dịch vụ cho phép người dùng truy cập hoặc khôi phục những phiên bản trước đây của những tập tin đã lưu, bằng cách dùng một tính năng ở máy trạm gọi là **Previous Versions**.

3.3. Tạo partition volume mới

Nếu bạn còn không gian chưa cấp phát trên một đĩa **basic** thì bạn có thể tạo thêm **partition** mới, còn trên đĩa **dynamic** thì bạn có thể tạo thêm **volume** mới. Phần sau hướng dẫn bạn sử dụng **Create Partition Wizard** để tạo một **partition** mới:

Nhấp phải chuột lên vùng trống chưa cấp phát của đĩa chọn **New simple volume**.

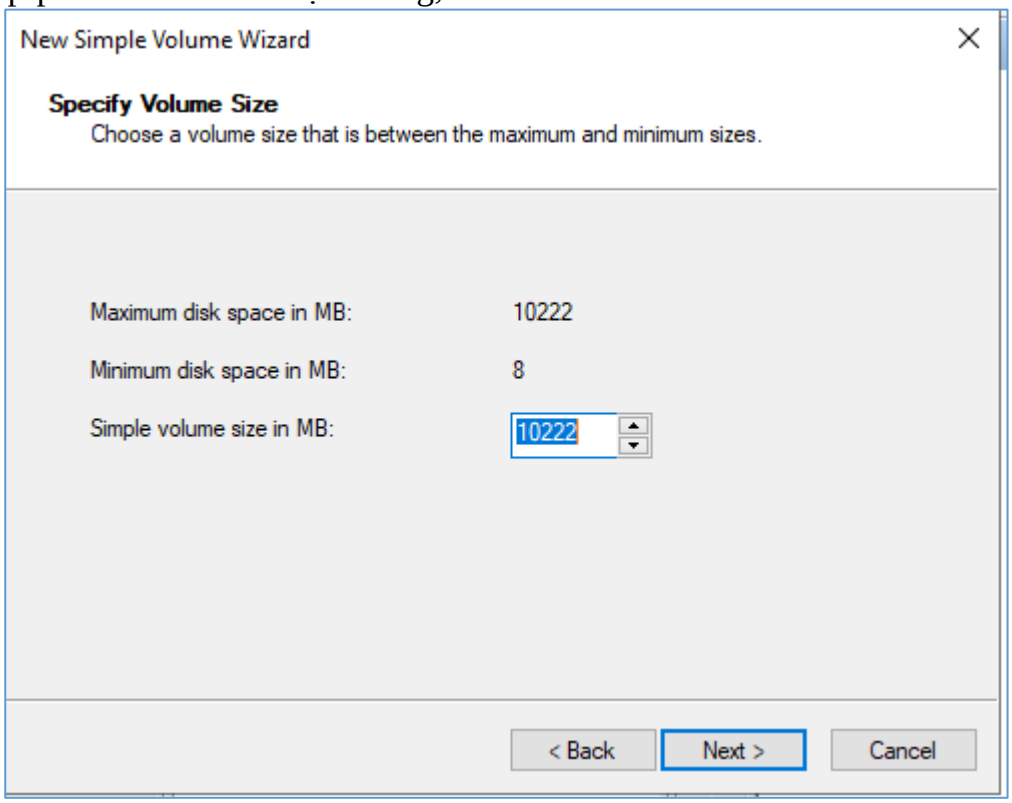


Hình 5.10 New simple volume

Xuất hiện hộp thoại **Create Partition Wizard**. Nhấn nút **Next** trong hộp thoại này.

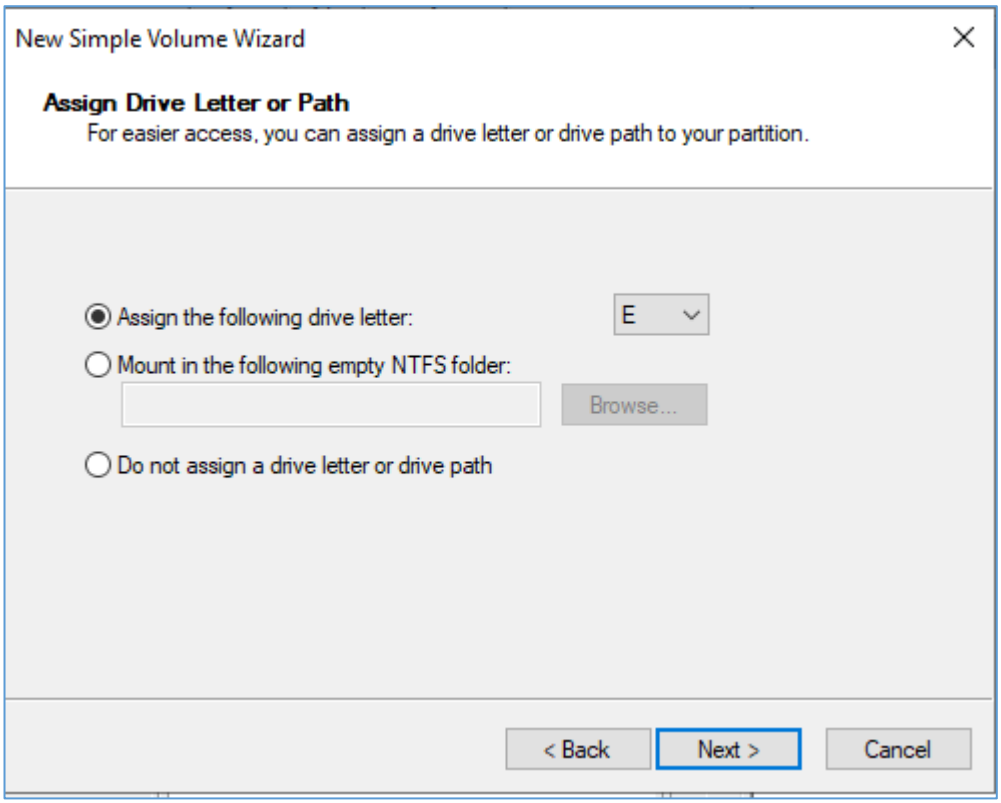
Trong hộp thoại **Select Partition Type**, chọn loại **partition** mà bạn định tạo. Chỉ có những loại còn khả năng tạo mới được phép chọn (tuỳ thuộc vào ổ đĩa vật lý của bạn). Sau khi chọn loại **partition** xong nhấn **Next** để tiếp tục.

Tiếp theo, hộp thoại **Specify Partition Size** yêu cầu bạn cho biết dung lượng định cấp phát. Sau khi chỉ định xong, nhấn **Next**.



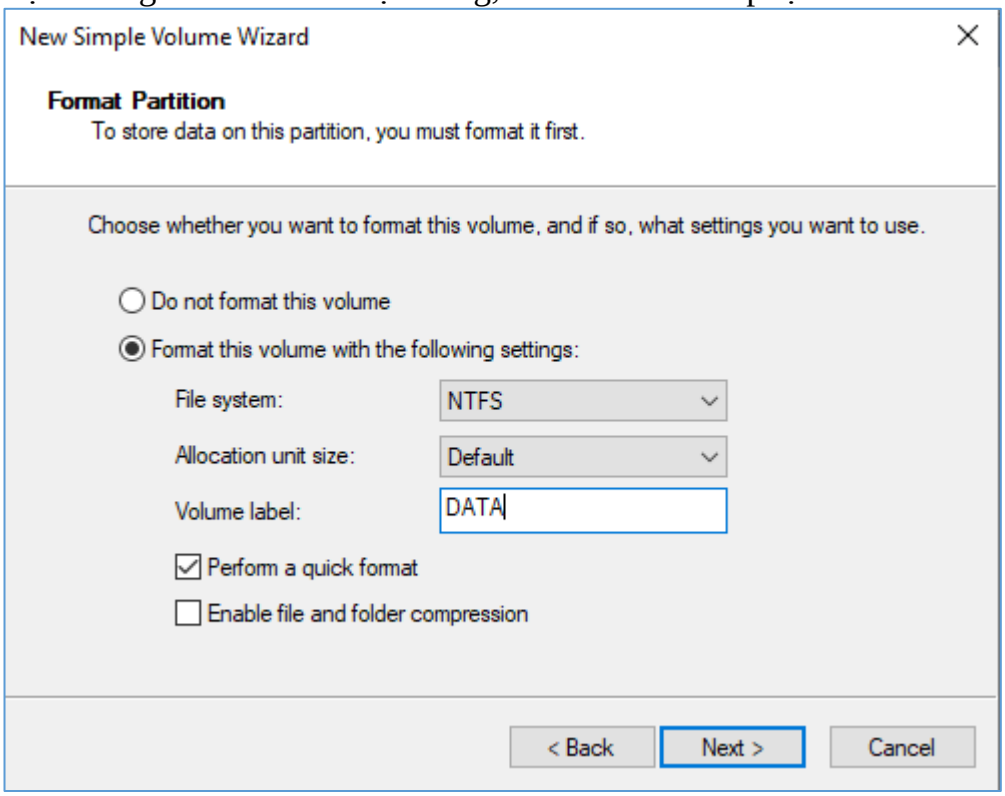
Hình 5.11 Nhập dung lượng đĩa

Trong hộp thoại **Assign Drive Letter or Path**, bạn có thể đặt cho **partition** này một ký tự ổ đĩa, hoặc gắn (**mount**) vào một thư mục rỗng, hoặc không làm đặt gì hết. Khi bạn chọn kiểu gắn vào một thư mục rỗng thì bạn có thể tạo ra vô số **partition** mới. Sau khi đã quyết định xong, nhấn **Next** để tiếp tục.



Hình 5.12 Chọn tên ổ đĩa

Hộp thoại **Format Partition** yêu cầu bạn quyết định có định dạng **partition** này không. Nếu có thì dùng hệ thống tập tin là gì? đơn vị cấp phát là bao nhiêu? nhãn của **partition** (**volume label**) là gì? có định dạng nhanh không? Có nén tập tin và thư mục không? Sau khi đã chọn xong, nhấn **Next** để tiếp tục.



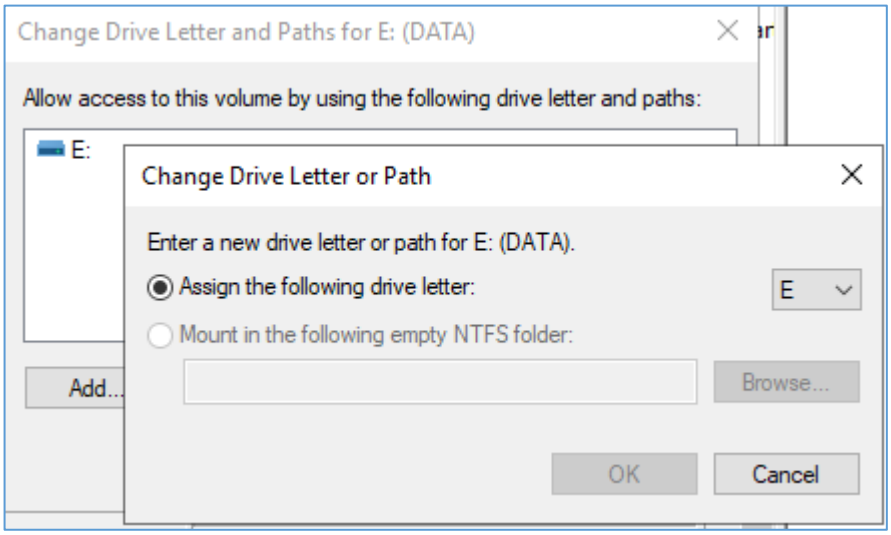
Hình 5.13 Định dạng phân vùng

Hộp thoại **Completing** the **Create Partition Wizard** tóm tắt lại các thao tác sẽ thực hiện, bạn phải kiểm tra lại xem đã chính xác chưa, sau đó nhấn **Finish** để bắt

đầu thực hiện.

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 5.13 Thay đổi ký tự ổ đĩa

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**, bạn có thể xoá nó đi. Để thực hiện, trong cửa sổ **Disk Manager**, bạn 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 bạn xác nhận lại lần nữa thao tác này.

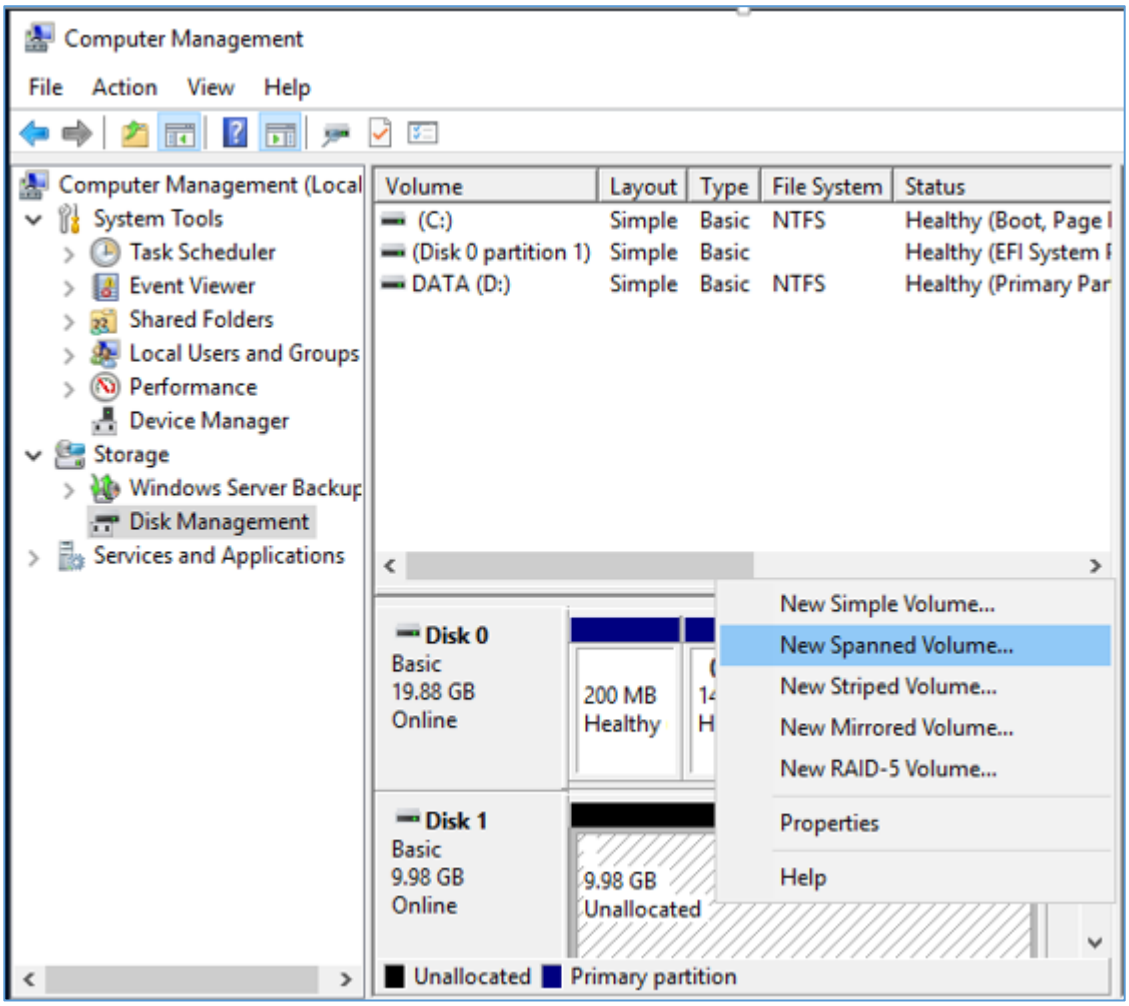
3.7. Cấu hình Dynamic Storage

3.7.1 Chuyển chế độ lưu trữ.

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.

3.7.2 Tạo Volume Spanned.

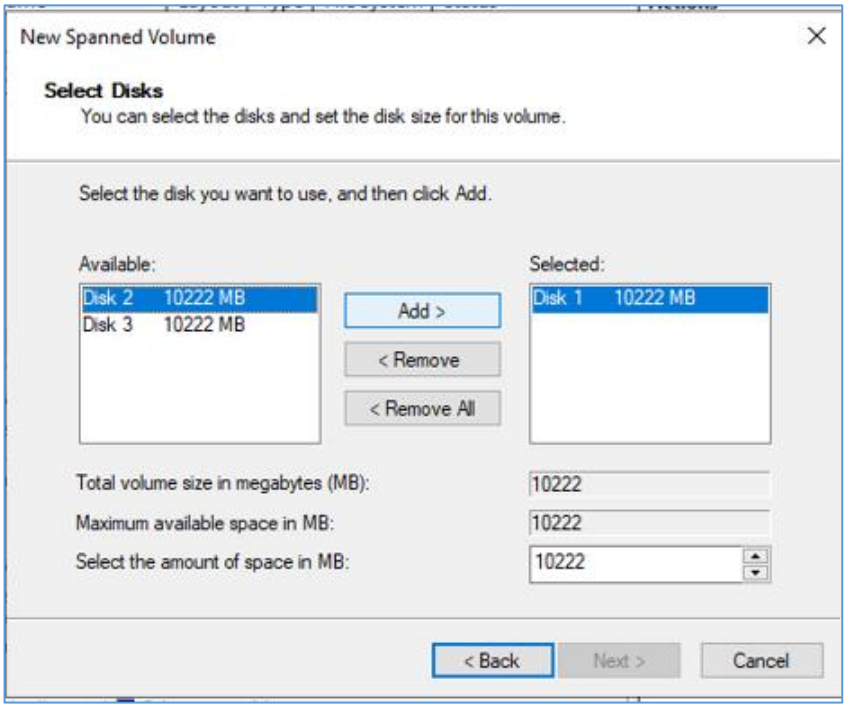
Trong công cụ **Disk Management**, bạn nhấp phải chuột lên vùng trống của đĩa cứng cần tạo **Volume Spanned**



Hình 5.14 New Spanned Volume

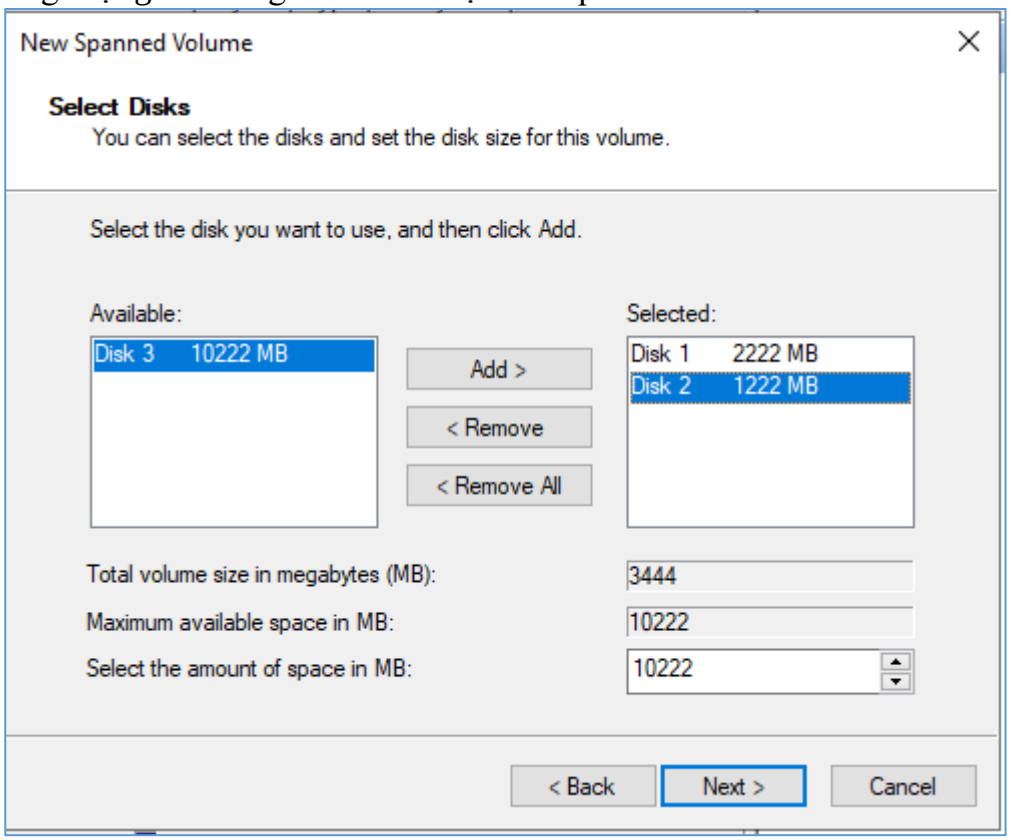
Bạn chọn những đĩa cứng dùng để tạo **Volume** này, đồng thời bạn cũng nhập kích thước mà mỗi đĩa giành ra để tạo **Volume**.

Chú ý đối với loại **Volume** này thì kích thước của các đĩa giành cho **Volume** có thể khác nhau.



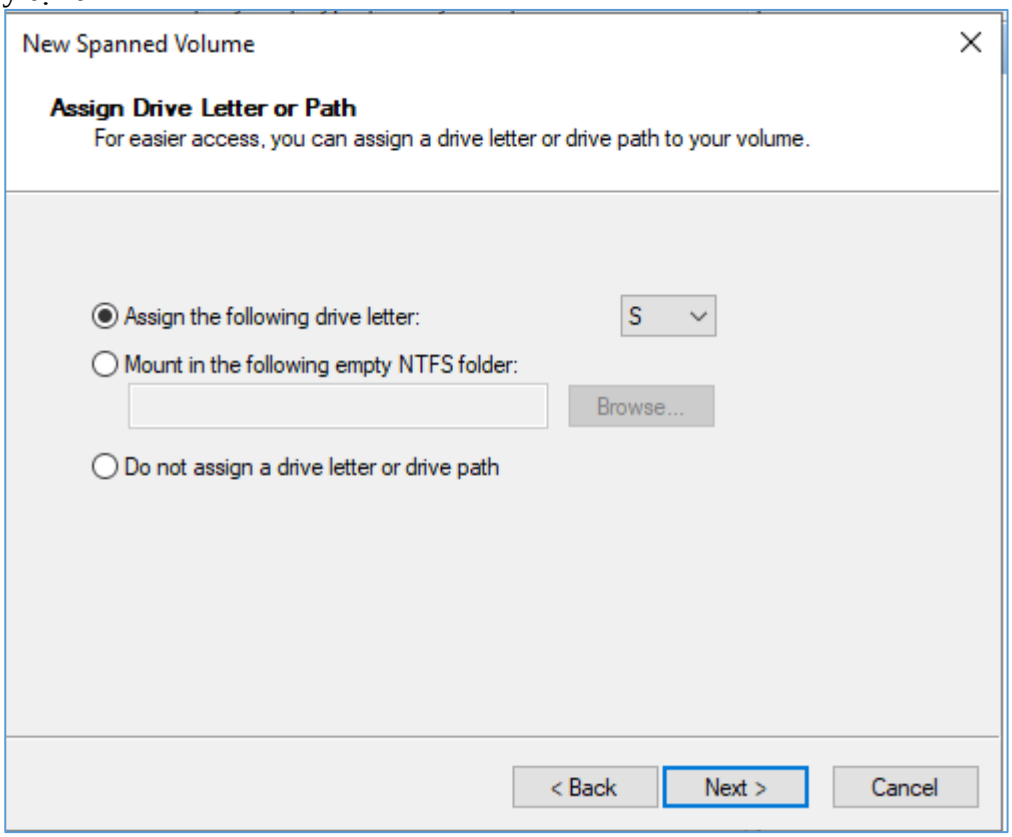
Hình 5.15 chọn đĩa tạo Spanned

Nhập dung lượng cho từng volume để tạo đĩa Spanned.



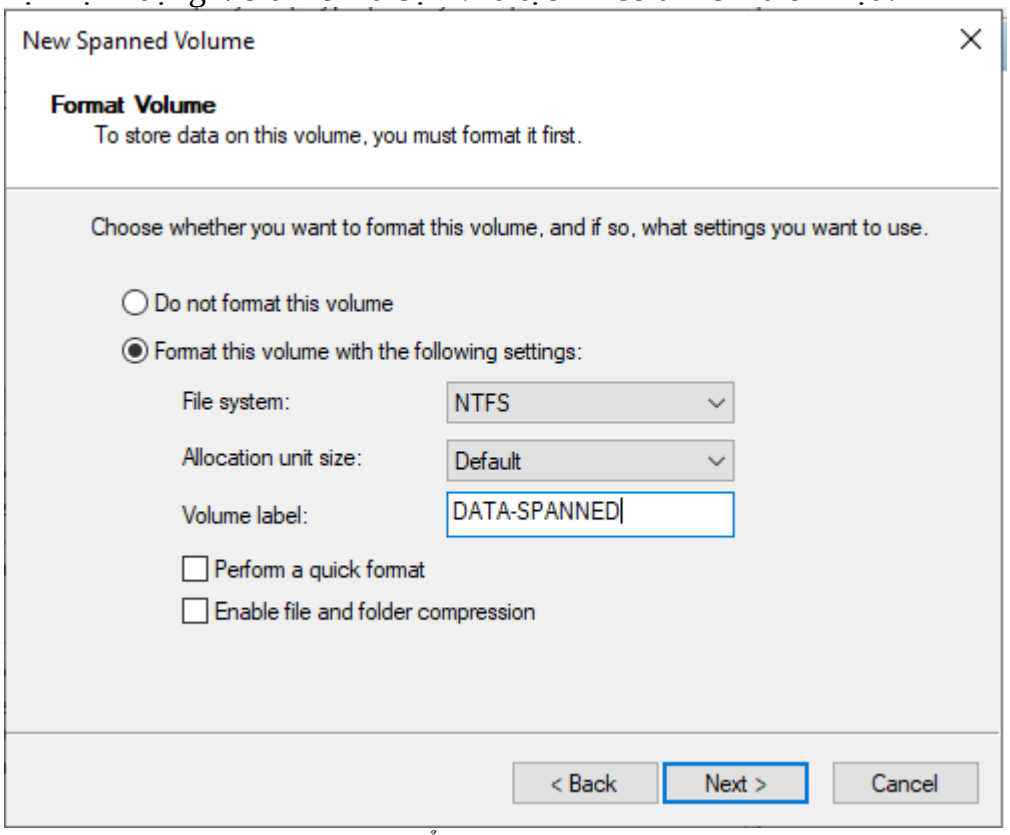
Hình 5.16 Nhập dung lượng đĩa

Chọn ký tự làm nhản đĩa



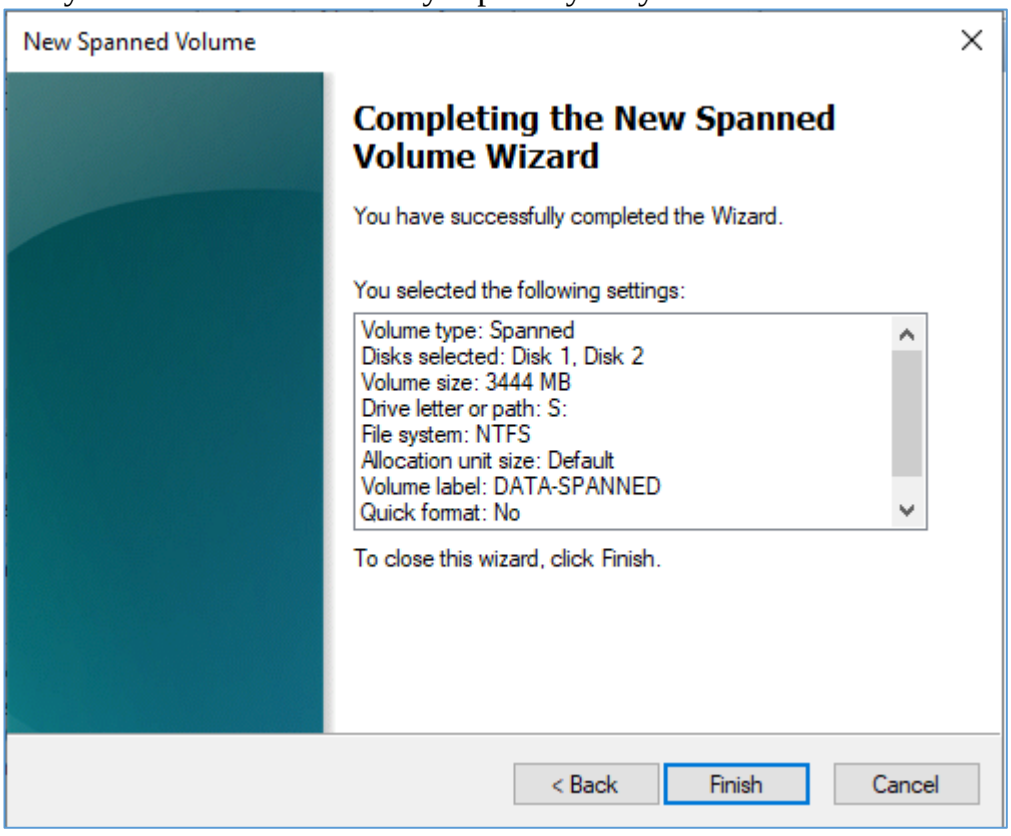
Hình 5.17 Chọ nhản cho đĩa

Bạn định dạng **Volume** mà bạn vừa tạo để có thể chứa dữ liệu.



Hình 5.18 Cửa sổ định dạng đĩa cho Spanned

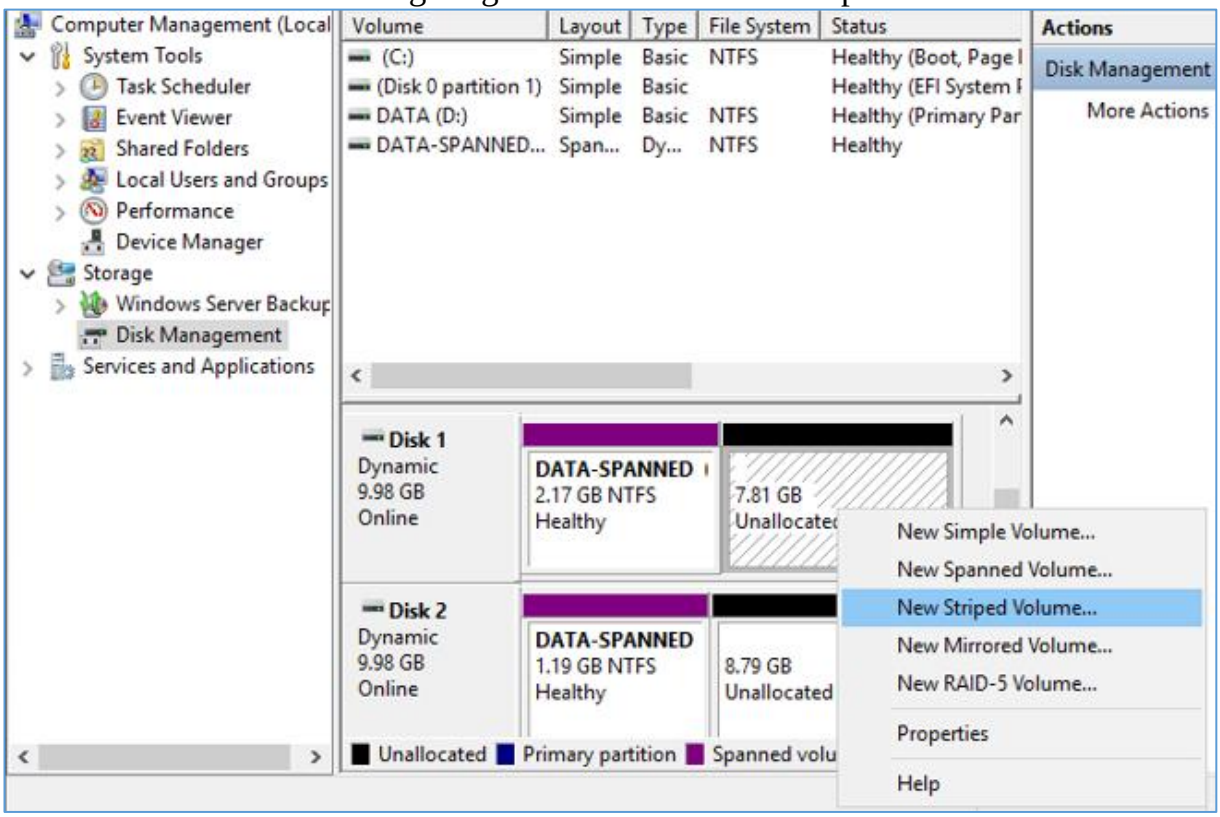
Đến đây đã hoàn thành việc tạo **Volume**, bạn có thể lưu trữ dữ liệu trên **Volume** này theo cơ chế đã trình bày ở phần lý thuyết.



Hình 5.19 Cửa sổ hoàn thành

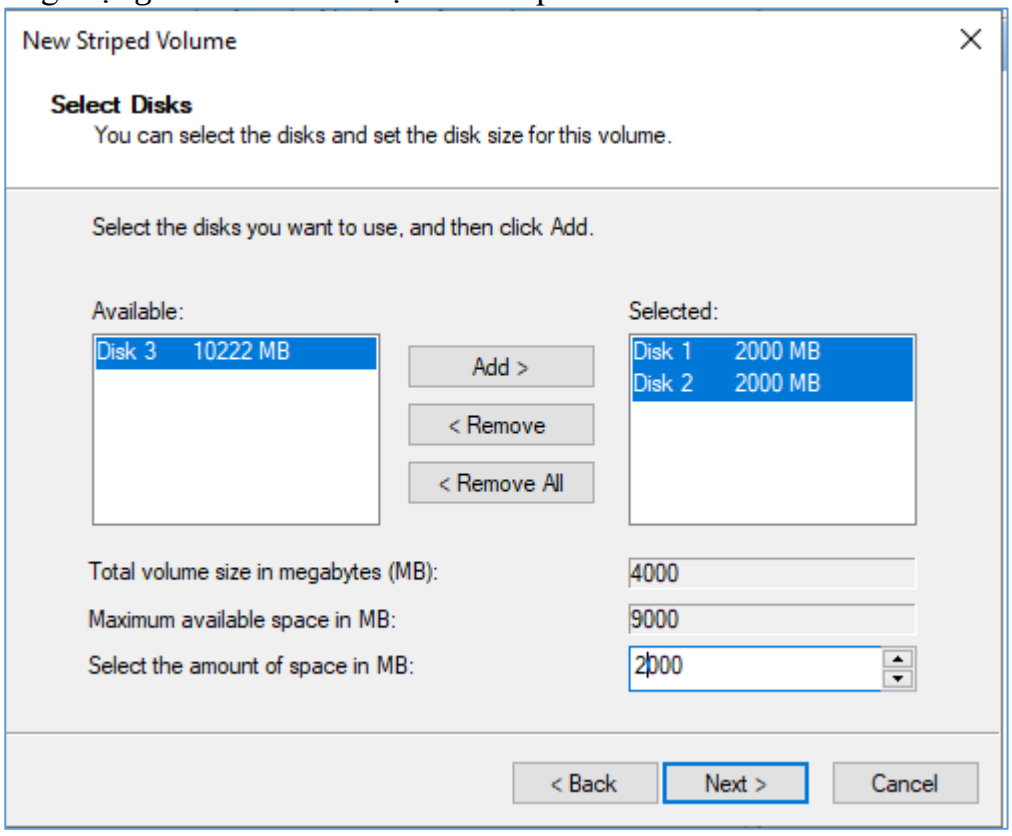
3.7.3 Tạo Volume Striped

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.



Hình 5.20 Cửa sổ tạo đĩa Striped

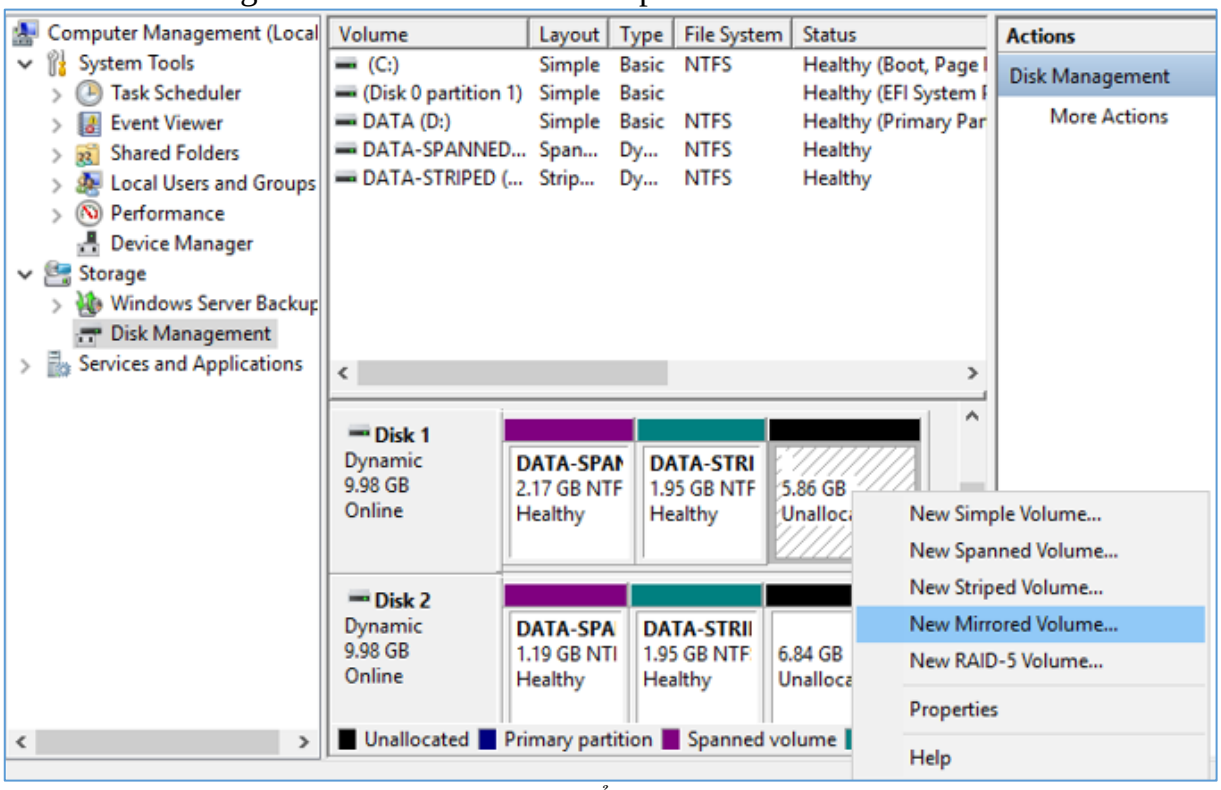
Nhập dung lượng cho volume để tạo đĩa Striped.



Hình 5.21 Nhập dung lượng đĩa cho Striped

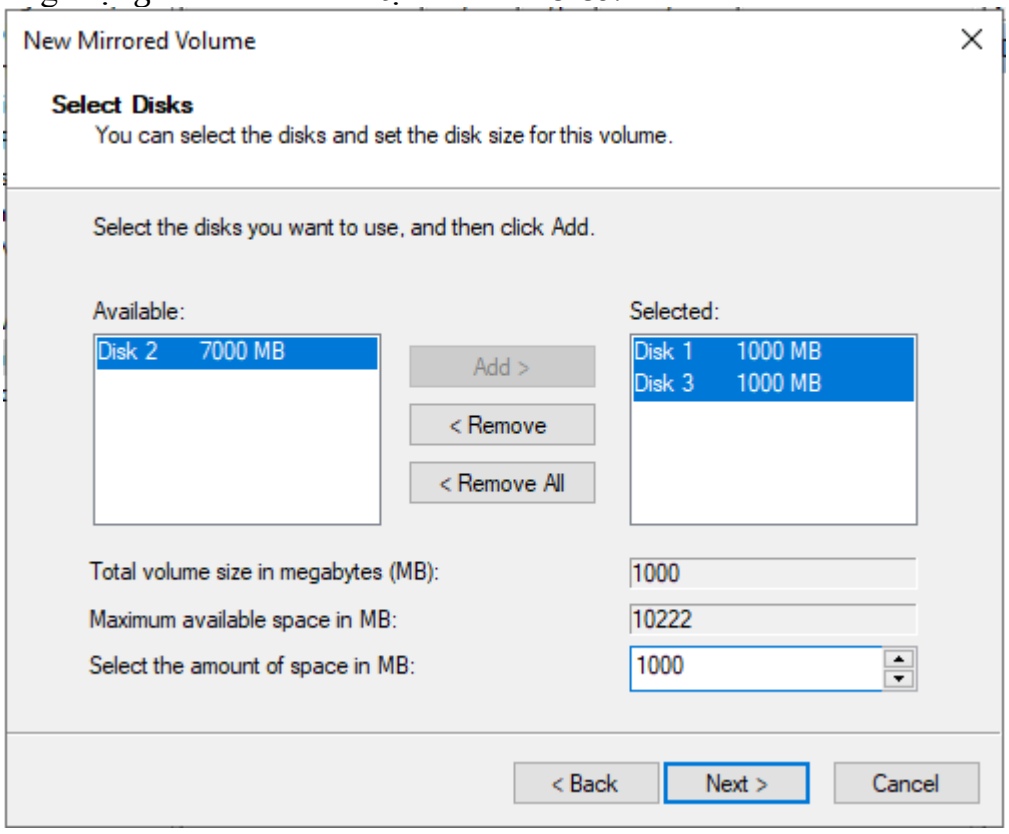
3.7.4 Tạo Volume Mirrored.

Các bước tạo **Volume Mirrored** cũng tương tự như Spanned, 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.



Hình 5.22 Cửa sổ tạo đĩa Mirrored

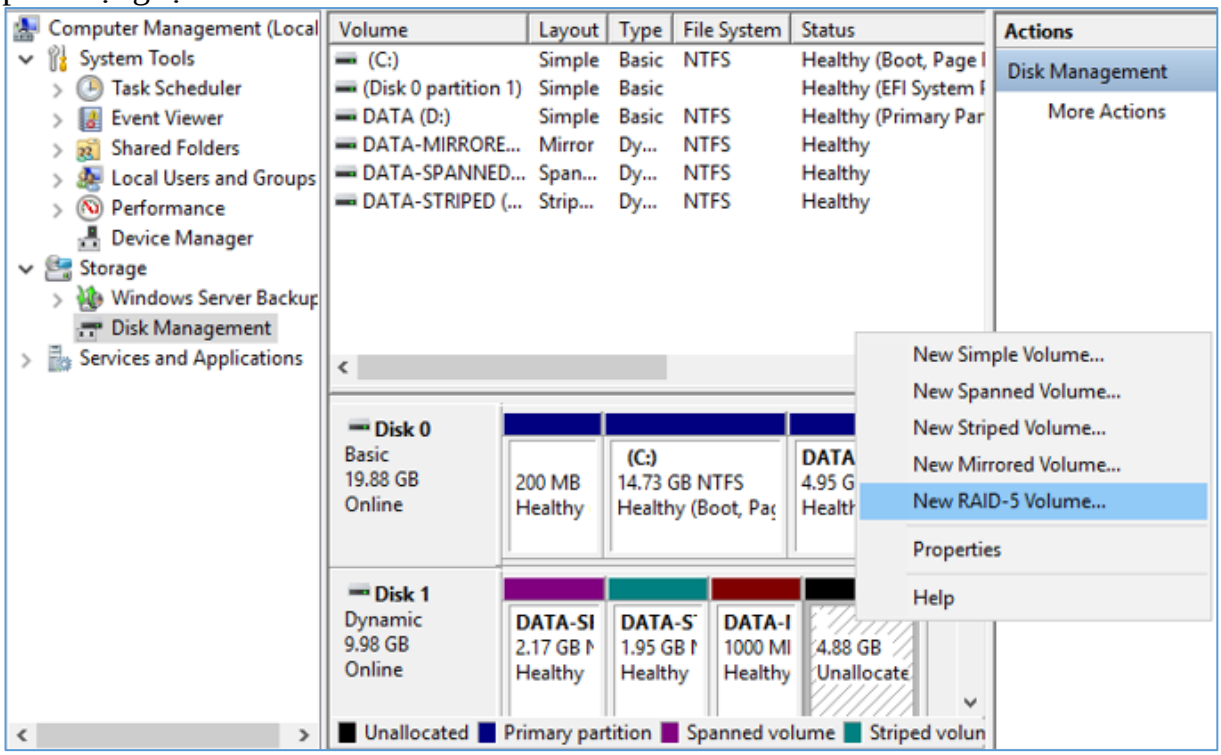
Nhập dung lượng cho volume để tạo đĩa Mirrored.



Hình 5.23 Nhập dung lượng đĩa cho đĩa Mirrored

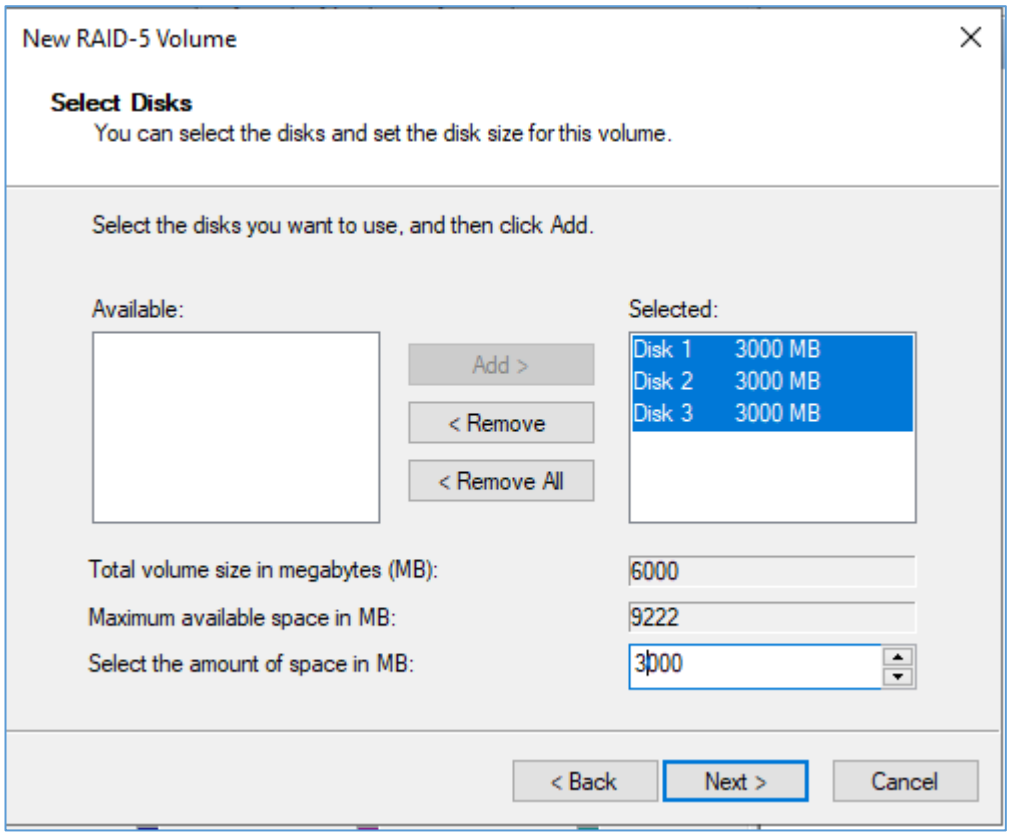
3.7.5 Tạo Volume Raid-5.

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.



Hình 5.24 Cửa sổ tạo đĩa Volume Raid-5

Nhập dung lượng cho volume để tạo đĩa *Volume Raid-5*.



Hình 5.25 Nhập dung lượng đĩa cho đĩa Volume Raid-5

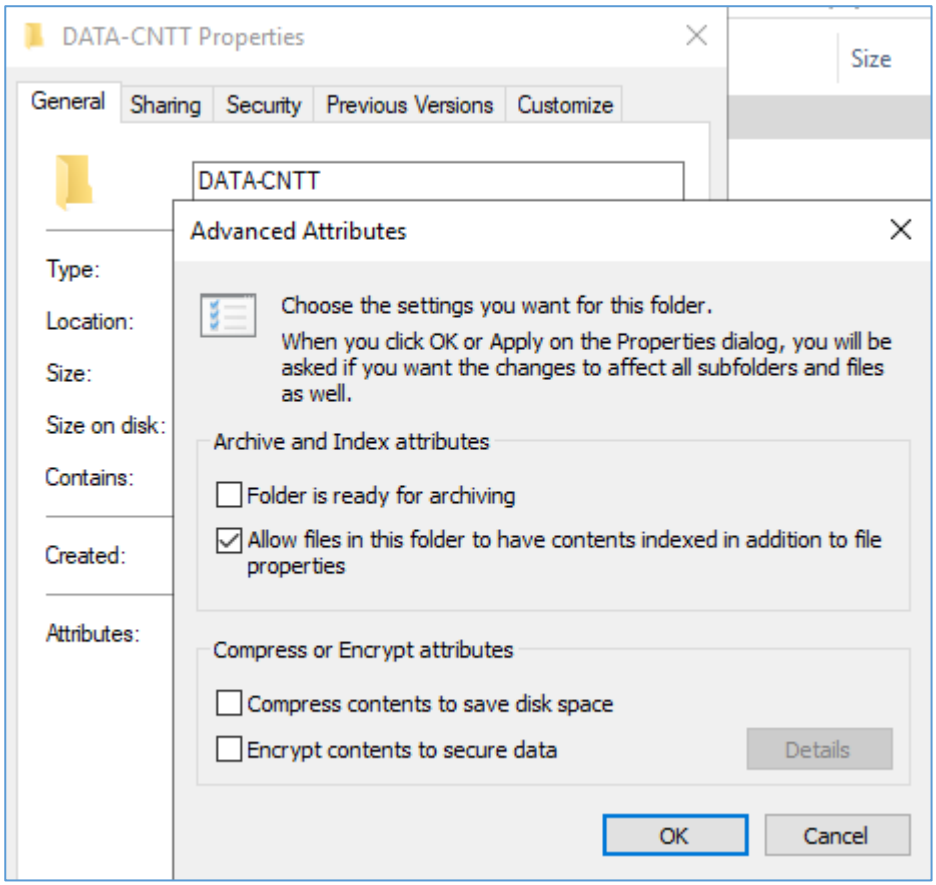
4. Quản lý việc nén dữ liệu

Mục tiêu:

- Sử dụng được công cụ nén dữ liệu.

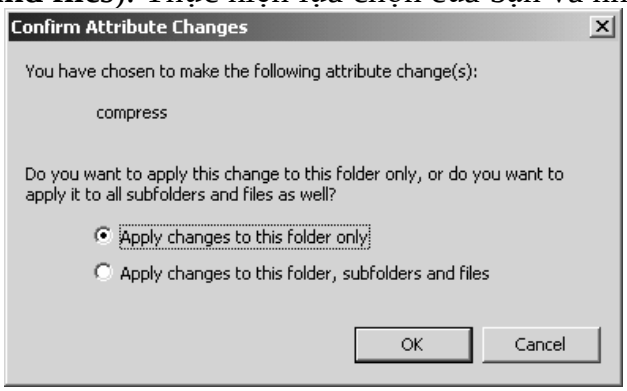
Nén dữ liệu là quá trình lưu trữ dữ liệu dưới một dạng thức chiếm ít không gian hơn dữ liệu ban đầu. **Windows Server** hỗ trợ tính năng nén các tập tin và thư mục một cách tự động và trong suốt. Các chương trình ứng dụng truy xuất các tập tin nén một cách bình thường do hệ điều hành tự động giải nén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



Hình 5.26 Cửa sổ Attribute

Nhấn chọn **OK** trong hộp thoại **Properties** để xác nhận thao tác. Nếu bạn định nén một thư mục, hộp thoại **Confirm Attribute Changes** xuất hiện, yêu cầu bạn 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 của bạn và nhấn **OK**.



Hình 5.24 Cửa sổ giải nén

Để thực hiện việc giải nén một thư mục/tập tin, bạn 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).

Mục tiêu:

- Cấp phát được hạn ngạch sử dụng dung lượng đĩa cứng cho người sử dụng.

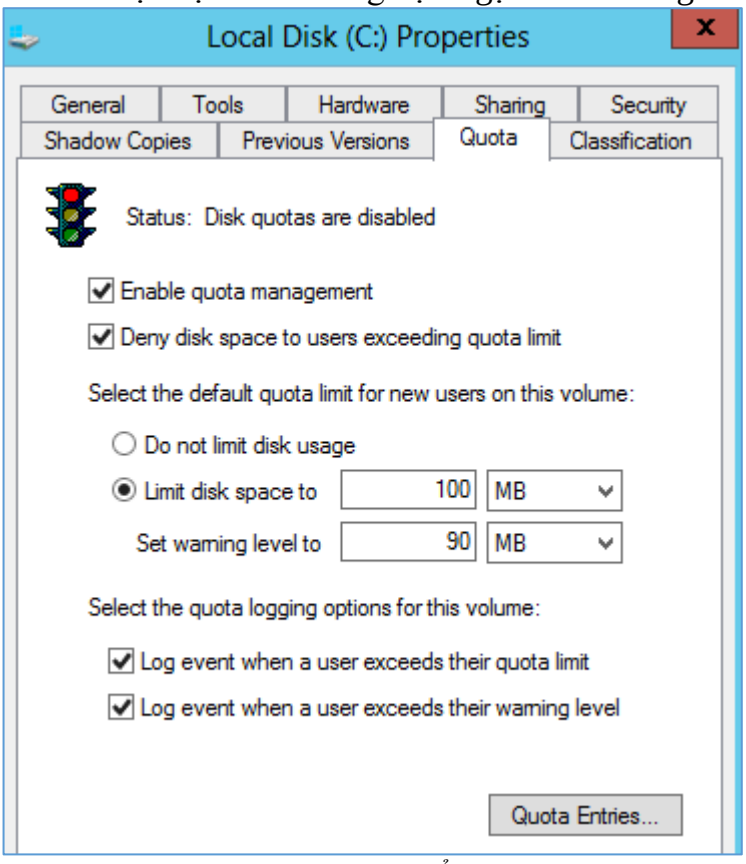
Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một **volume NTFS**. Bạn có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

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.

Bạn cấu hình hạn ngạch đĩa bằng hộp thoại **Volume Propertise** đã giới thiệu trong phần trên. Bạn cũng có thể 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 5.25 Cửa sổ Quota

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 bạn 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 bạn dự định áp đặt hạn ngạch cho tất cả các người dùng, bạn phải chỉ định hạn ngạch ngay từ khi tạo lập **volume**.

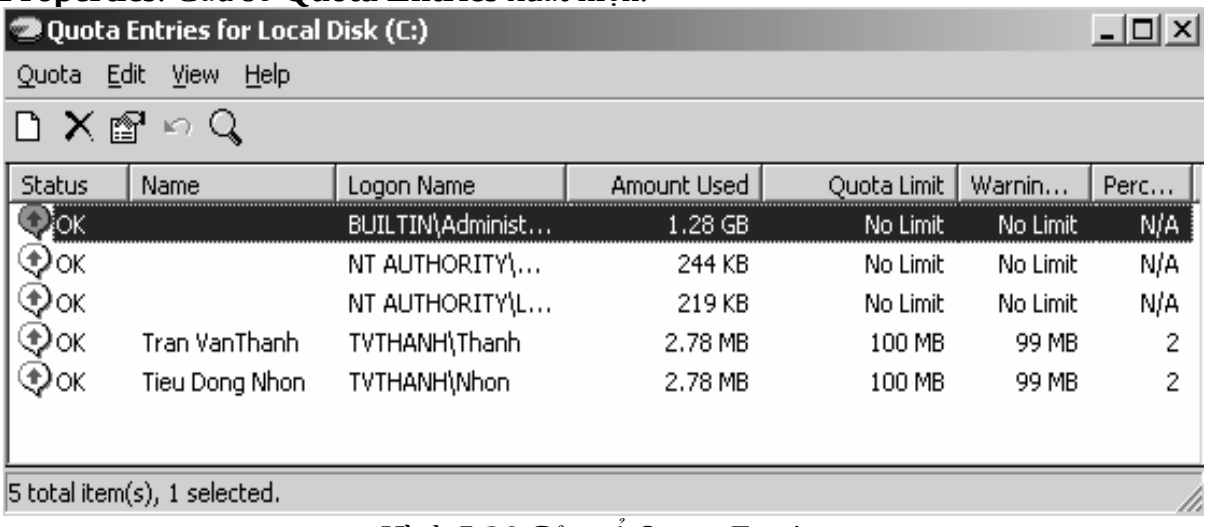
Để thực hiện, bạn mở hộp thoại **Volume Properties** và chọn tab **Quota**. Đánh dấu chọn mục **Enable quota management** và điền vào các giá trị giới hạn sử dụng và giới hạn cảnh báo.

5.3. Chỉ định hạn ngạch cho từng cá nhân.

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

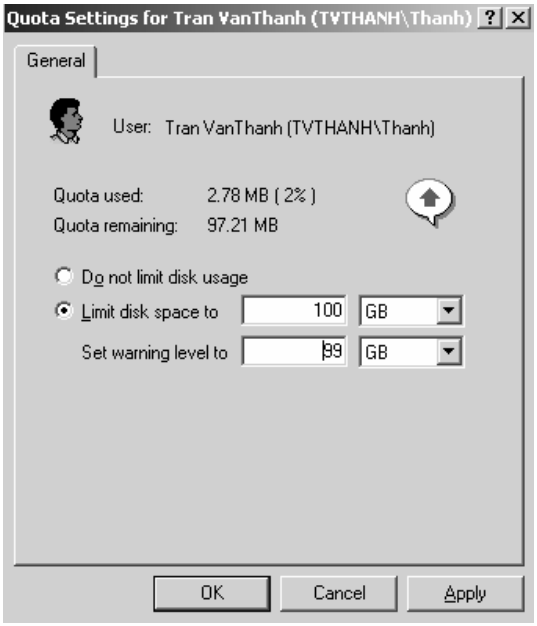
- Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ phải có được lượng không gian đĩa trống lớn.
- Hoặc là người dùng đã tạo nhiều tập tin trên **volume** trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Bạn phải tạo riêng một giới hạn mới áp dụng cho người đó.

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



Hình 5.26 Cửa sổ Quota Entries

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 bạn thay đổi các giá trị hạn ngạch.



Hình 5.27 Cửa sổ Quota Setting

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**, bạn 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

Mục tiêu:

- Sử dụng được công cụ mã hóa dữ liệu.

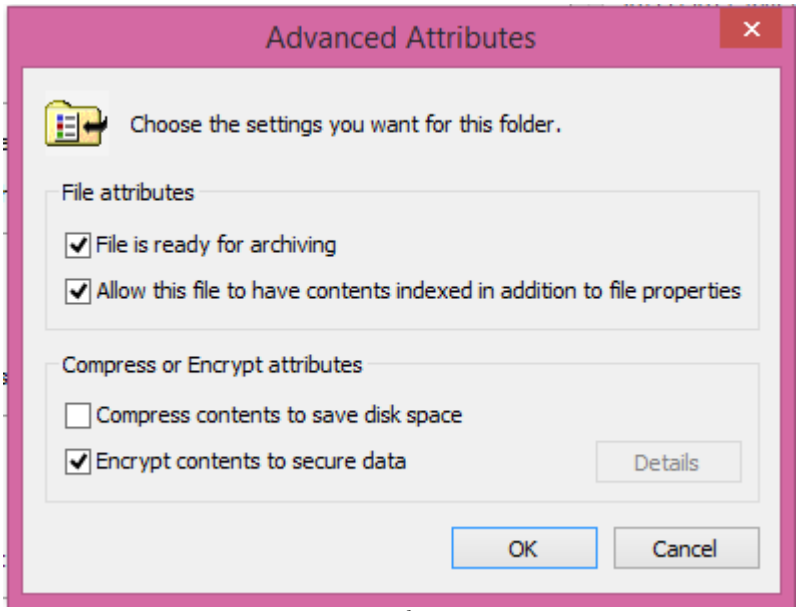
EFS (Encrypting File System) là một kỹ thuật dùng trong **Windows Server** dùng để mã hoá các tập tin lưu trên các **partition NTFS**. Việc mã hoá sẽ bổ sung thêm một lớp bảo vệ an toàn cho hệ thống tập tin. Chỉ người dùng có đúng khoá mới có thể truy xuất được các tập tin này còn những người khác thì 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**.

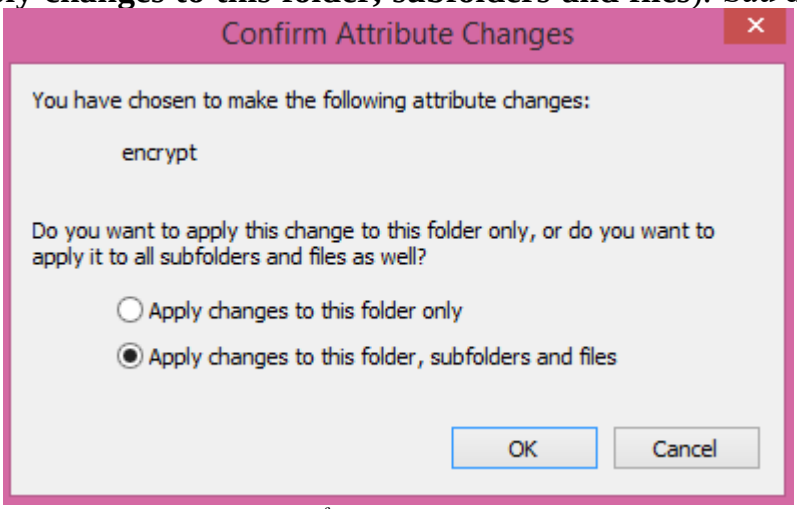
Trong hộp thoại **Properties**, nhấn nút **Advanced**.

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



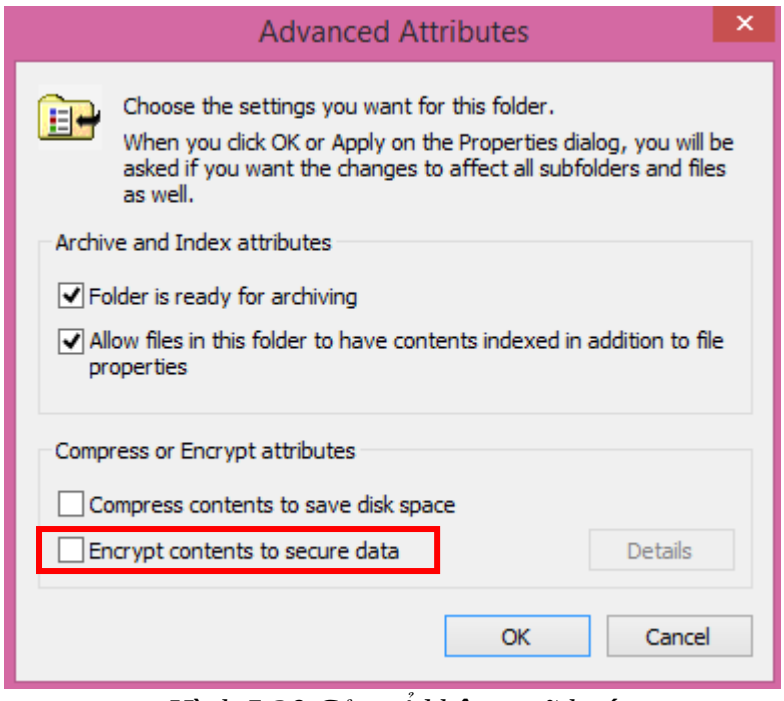
Hình 5.28 Cửa sổ mã hoá dữ liệu

Trở lại hộp thoại **Properties**, nhấn **OK**, xuất hiện hộp thoại **Confirm Attribute Changes** yêu cần bạn 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**.



Hình 5.29 Cửa sổ Confirm Attribute Changes

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**.



Hình 5.30 Cửa sổ không mã hoá

Bài tập thực hành của học viên

1. Quản lý đĩa theo **Basic Disk: Ổ thứ 1 (Disk 0):** chia làm 2 phần phân vùng 1 phân vùng chứa hệ thống trên Windows server 2019 và 1 phân vùng chứa dữ liệu có tên DATA.
2. Quản lý đĩa theo **Dynamic Disk:** Disk 1, Disk 2**,** Disk 3
   a. Tạo đĩa **Spanned** Volume từ với Disk 1 là 10GB, Disk 2 là 15GB và đặt tên là DATA-SPANNED
   b. Tạo đĩa **Striped** Volume từ với Disk 1, Disk 3 có từ với dung lượng là 10GB và và đặt tên là DATA-STRIPED
   c. Tạo đĩa **Mirrored** Volume từ với Disk 2, Disk 3 có từ với dung lượng là 20GB và và đặt tên là DATA- MIRRORED
   d. Tạo đĩa **RAID-5** Volume từ với Disk 1, Disk 2, Disk 3 có từ với dung lượng là 30GB và và đặt tên là DATA- RAID
   3. Thiết lập hạn ngạch đĩa (disk quota) cho đĩa DATA của Disk 0, các user được cấp 2GB.

Hướng dẫn thực hiện:

- Bài tập 1 làm theo các bước trong mục 3.3 của giáo trình
- Bài tập 2 làm các bước trong mục 3.7 của giáo trình
- Bài tập 3 làm theo mục 5 của giáo trình

Những trọng tâm cần chú ý:

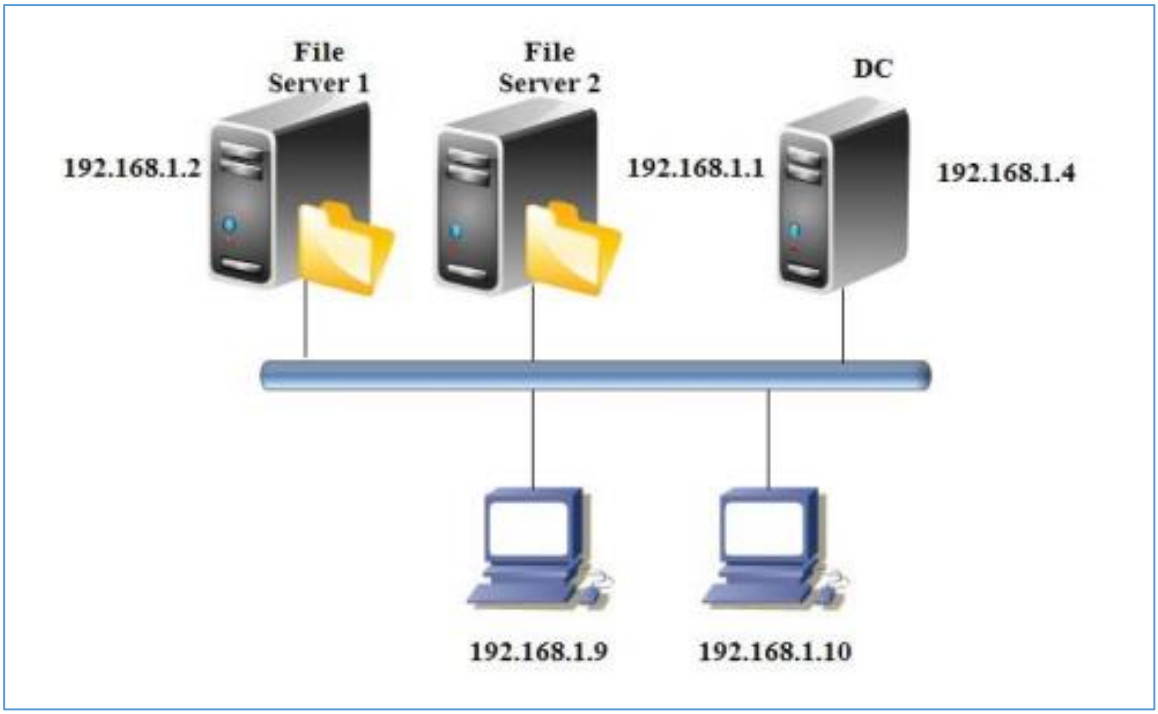
- Chọn ổ đĩa cho đúng để không bị lỗi hệ thống.
- Khi nâng cấp từ Basic lên Dynamic dữ liệu trên các phân vùng được bảo toàn
- Trong khi đó nếu hạ từ Dynamic xuống Basic thì dữ liệu hoàn toàn bị xoá sạch
- Convert đĩa phải thích hợp, đúng yêu cầu
- Khi chúng ta cho phép user lưu trữ dữ liệu trên file server phải đúng dung lượng.

- Cần phải làm đặt hạn ngạch lưu trữ cho user để tránh tăng đáng kể dung lượng không cần thiết của file server. Phải đăng nhập đúng user Administrator trước khi cài đặt Domain controller.
- Thiết lập password phù hợp hệ thống và lưu lại để sau này còn sao lưu và phục hồi hệ thống khi cần thiết.
- Chọn cho đúng phiên bản hệ điều hành đang sử dụng.
- Disk Quota – thiết lập hạn ngạch đĩa cho user lưu trữ cho đúng phân vùng.
- Tắt tường lửa cho máy DC và Client trên hệ thống.
- Thao tác phải đúng các bước Quản lý đĩa và giới hạn đĩa trên Windows server 2019.

Bài mở rộng và nâng cao

Tình huống: Khi chúng ta cho phép user lưu trữ dữ liệu trên file server (dùng Map Network Drive), user có thể lưu trữ phim, video v.v làm tăng đáng kể dung lượng không cần thiết của file server. Vì vậy ta có nhu cầu áp đặt hạn ngạch lưu trữ cho user (Disk Quota – thiết lập hạn ngạch đĩa cho user lưu trữ).

Mô hình



Yêu cầu:

- Sử dụng Disk Quota - File Server Resource Manager (FSRM) Hạn chế lưu trữ file theo định dạng (vd: cấm file exe, cấm flv, mp4, …) theo mô hình như trên
- Cân bằng tải file Server. Nhằm đáp ứng nhu cầu cho người dùng khi có sự truy cập nhiều hoặc có sự cố mất kết nối ở server File Server

Yêu cầu đánh giá kết quả học tập

Nội dung

– Về kiến thức:
  + Trình bày được Chức năng Quản lý đĩa và giới hạn đĩa trên Windows Server
  + Trình bày được các bước Quản lý đĩa và giới hạn đĩa trên Windows Server 2019

– Về kỹ năng:
  + Thao tác thành thạo việc Quản lý đĩa trên Windows Server 2019.

+ Thao tác thành thạo việc giới hạn đĩa trên Windows Server 2019
+ Thực hiện đúng Cân bằng tải file Server trên Windows Server 2019

– Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

– Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
– Về kỹ năng:
+ Đánh giá kỹ năng thực hành về các thao tác Quản lý đĩa và giới hạn đĩa trên Windows Server 2019.
+ Đánh giá kỹ năng thực hành về File server resource manager trên Windows Server 2019.
+ Thực hiện đúng Cân bằng tải file Server trên Windows Server 2019
– Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 6: TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG
Mã bài: MĐ 17 - 06

Mục tiêu:

- Trình bày các loại quyền truy cập dữ liệu;
- Tạo và quản lý các thư mục dùng chung trên mạng.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Tạo thư mục dùng chung

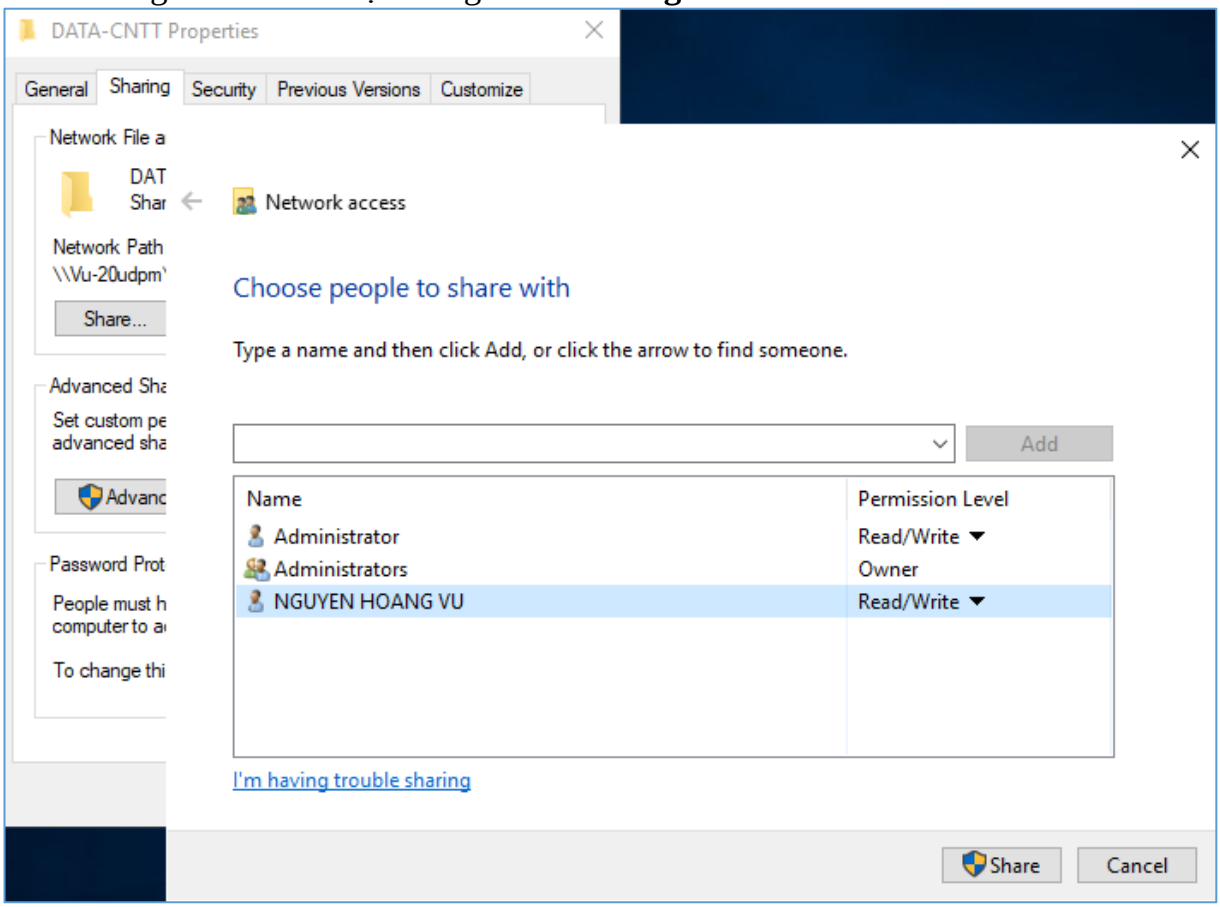
Mục tiêu:

- Chia sẻ được thư mục dùng chung
- Trình bày được quyền truy thư mục dùng chung.

1.1. Chia sẻ thư mục dùng 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, bạn phải **logon** vào hệ thống với vai trò người quản trị (**Administrators**) hoặc là thành viên của nhóm **Server Operators**, tiếp theo trong **Explorer** bạn nhấp phải chuột trên thư mục đó và chọn **Properties**, hộp thoại **Properties** xuất hiện, chọn **Tab Sharing**.

Ý nghĩa của các mục trong **Tab Sharing**:



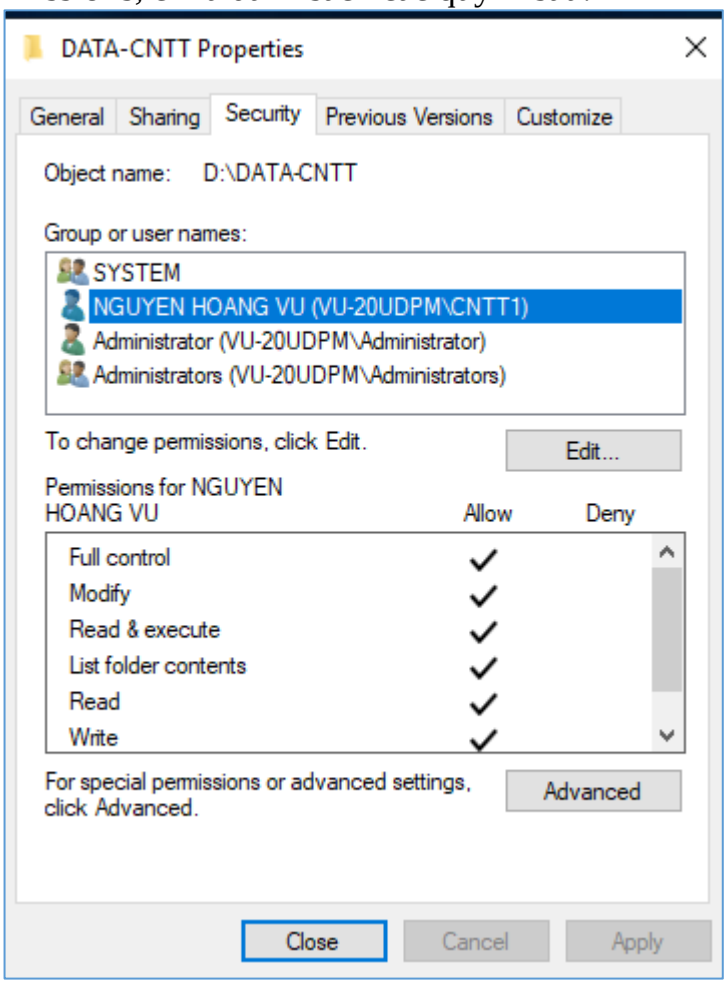
Hình 6.1 Cửa sổ chọn user và phân quyền

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

1.2. Cấu hình Share Permissions

Bạn 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:

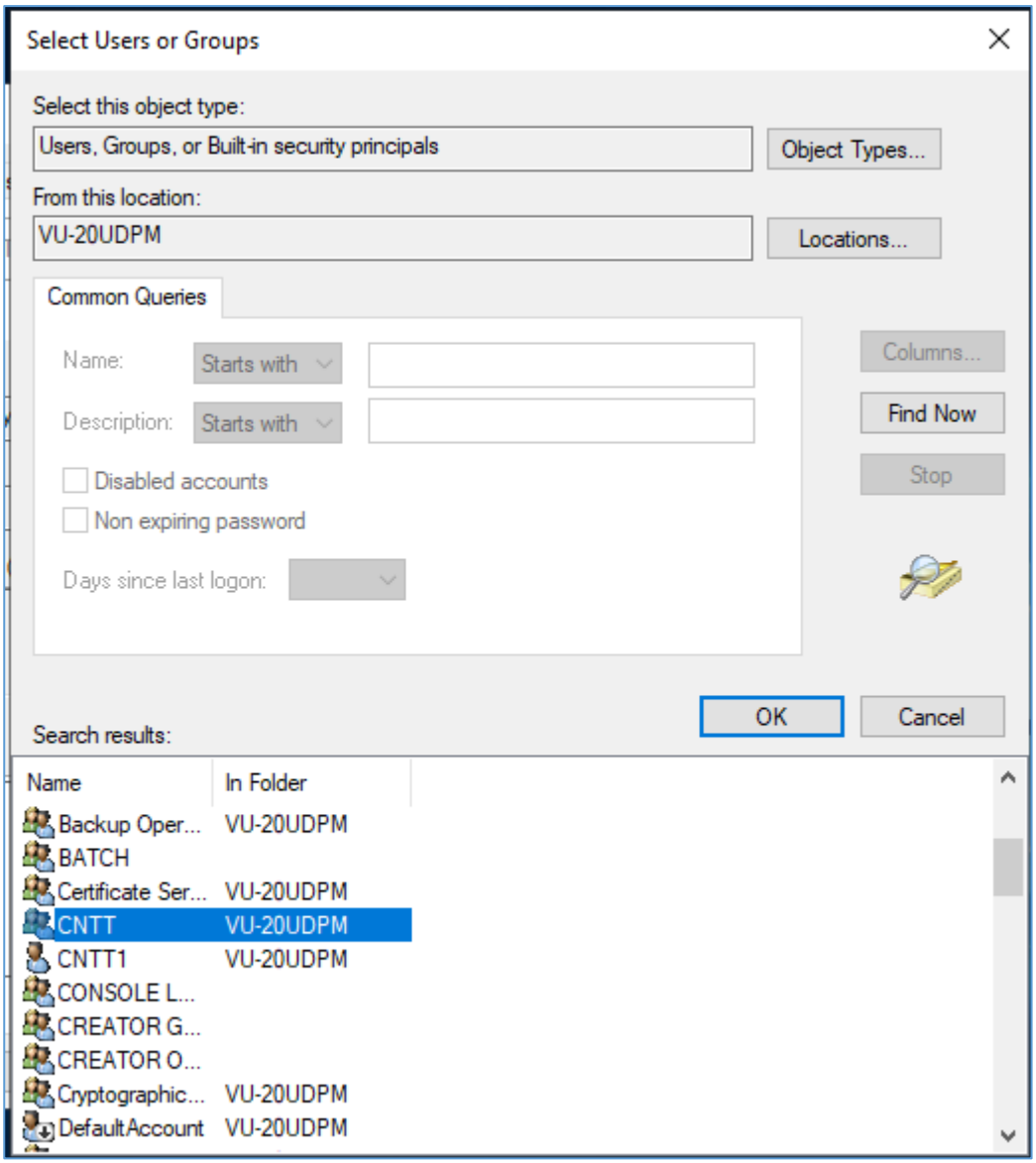


Hình 6.2 Cửa sổ Security

- **Full Control**: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- **Modify**: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.
- **Read & execute:** cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ.
- **Read**: cho phép người dùng xem các tập tin trong thư mục chia sẻ.
- **Write**: cho phép người dùng xem tao các tập tin trong thư mục chia sẻ

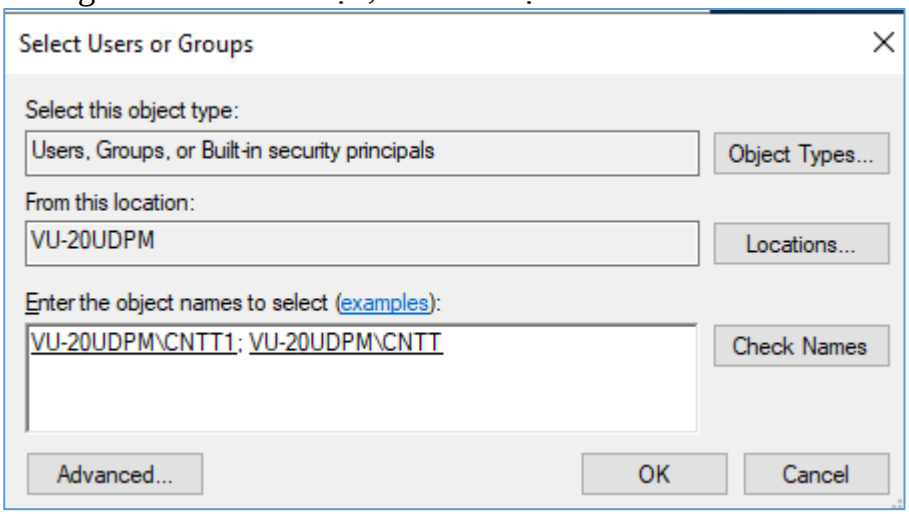
Bạn muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Edit/add,** sau đó chọn

Anvanced.



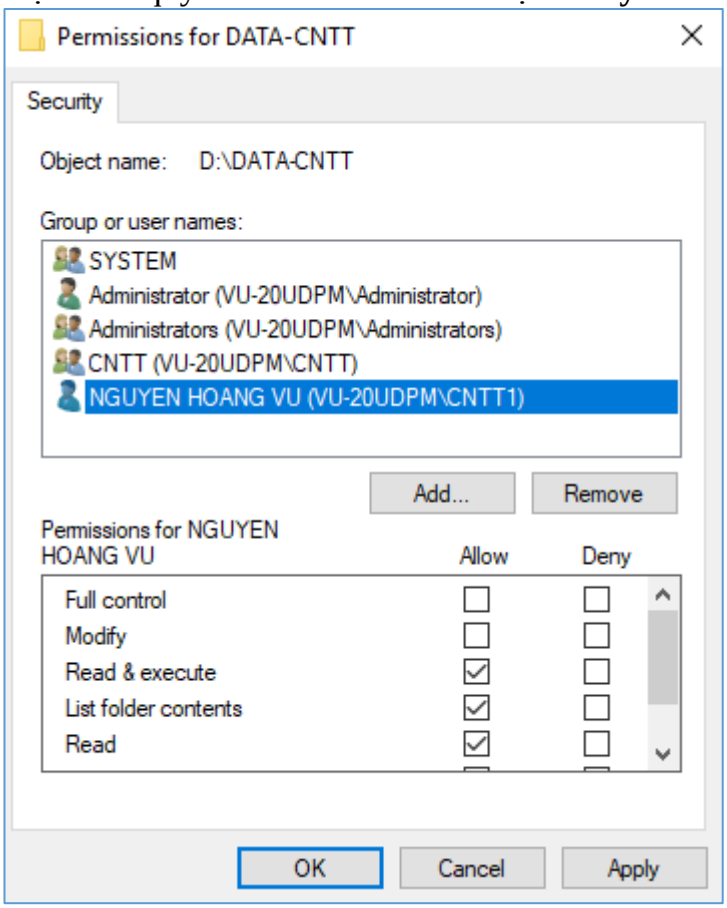
Hình 6.3 Cửa sổ chọn user

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 6.4 Cửa sổ xác nhận User và group

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 6.5 Cửa sổ phân 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

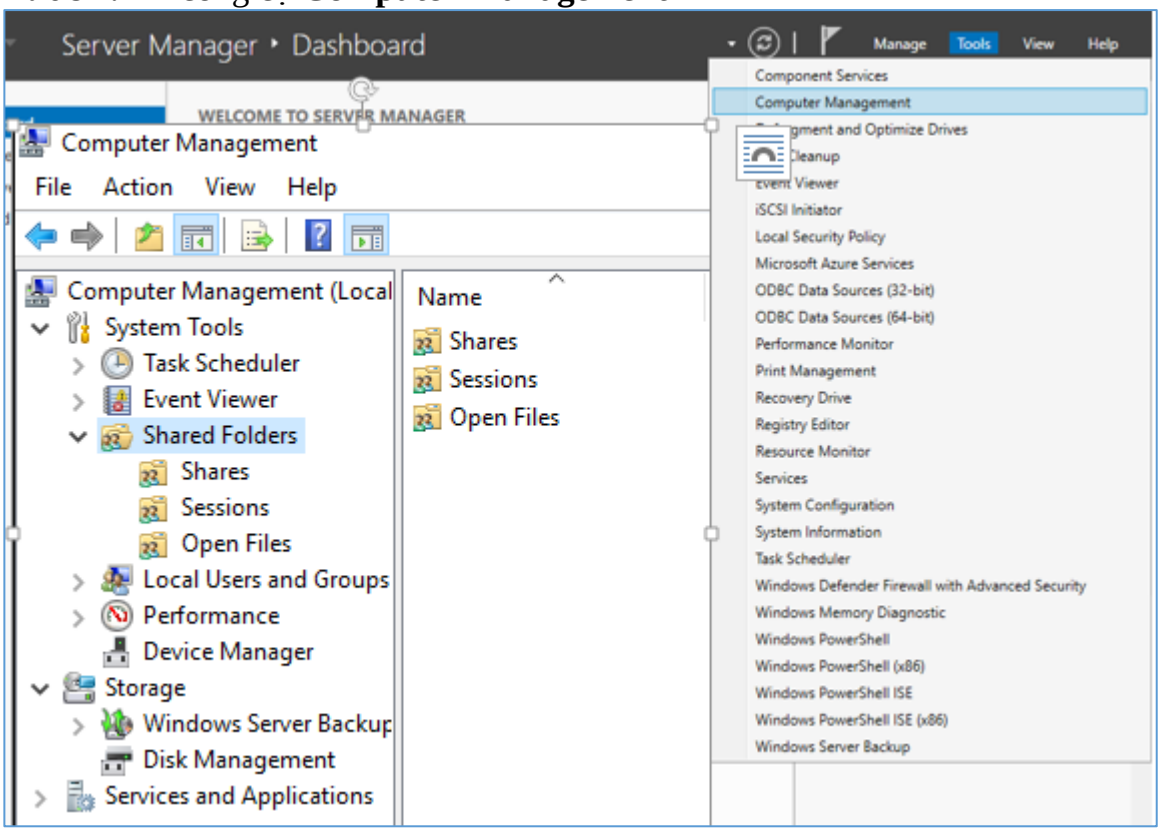
Mục tiêu:

- Trình bày được quyền truy thư mục dùng chung.

2.1. Xem các thư mục dùng chung

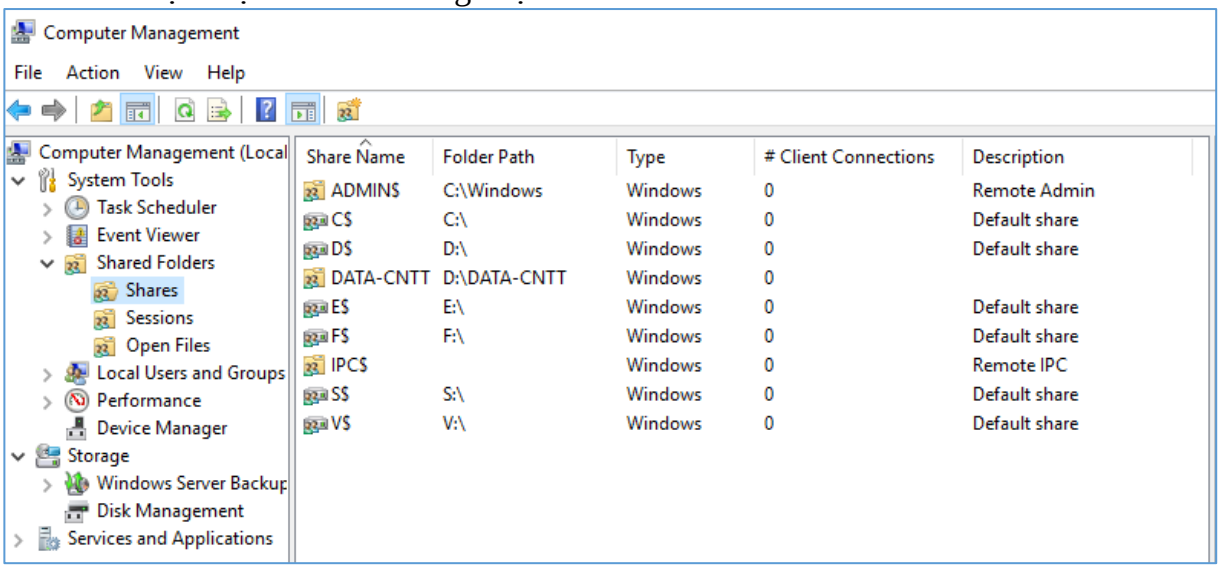
Mục **Shared Folders** trong công cụ **Computer Management** cho phép bạn tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục **Shares**. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (**share name**) là dấu **$** thì tên thư mục dùng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

Bước 1:Mở công cụ **Computer Management**



Hình 6.6 Cửa sổ xem thư mục share

Bước 2: chọn mục **Shared** trong Mục **Shared Folders**



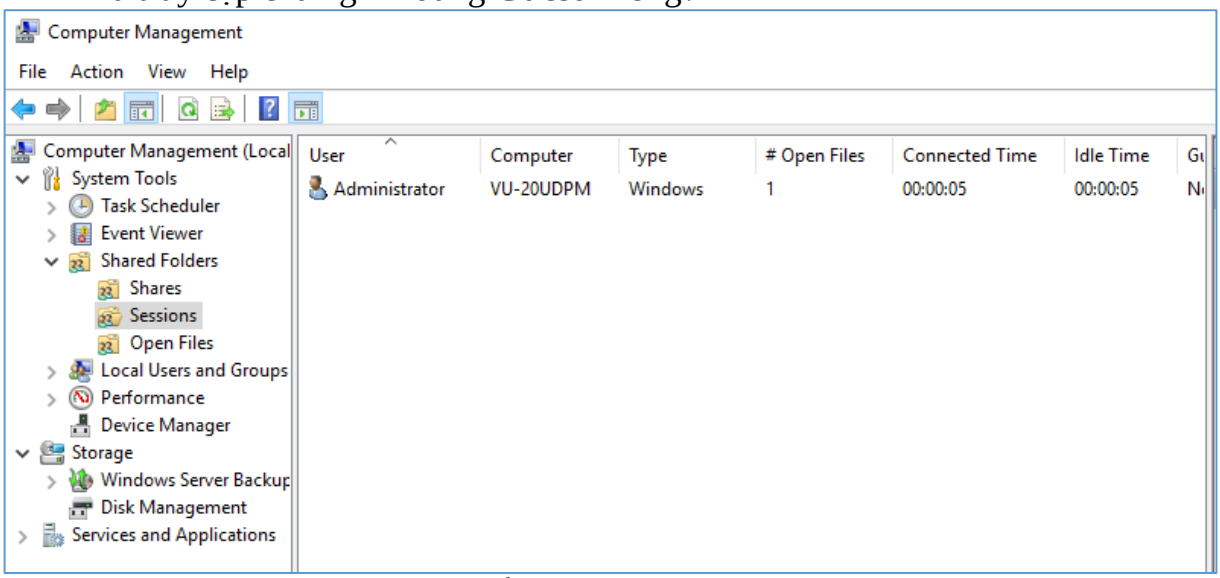
Hình 6.7 Cửa sổ hiển thị các thư mục share

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 bạn 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.
- Phải là truy cập của người dùng **Guest** không?

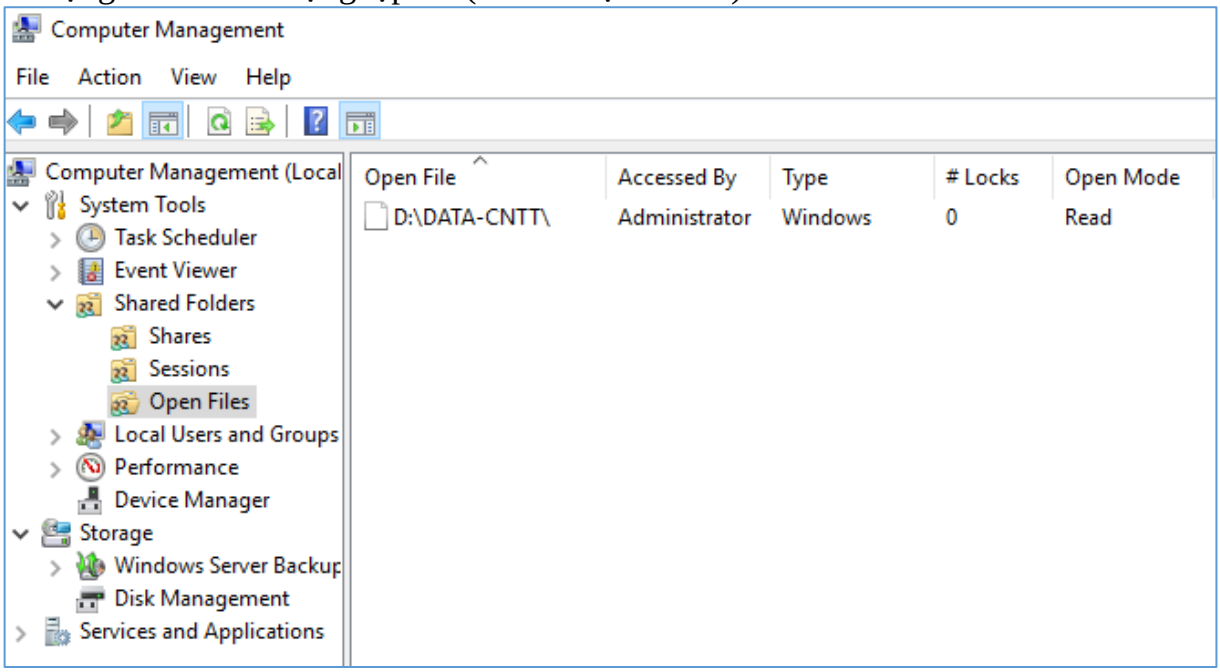


Hình 6.8 Cửa sổ xem User truy cập thư mục

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 bạn 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**).



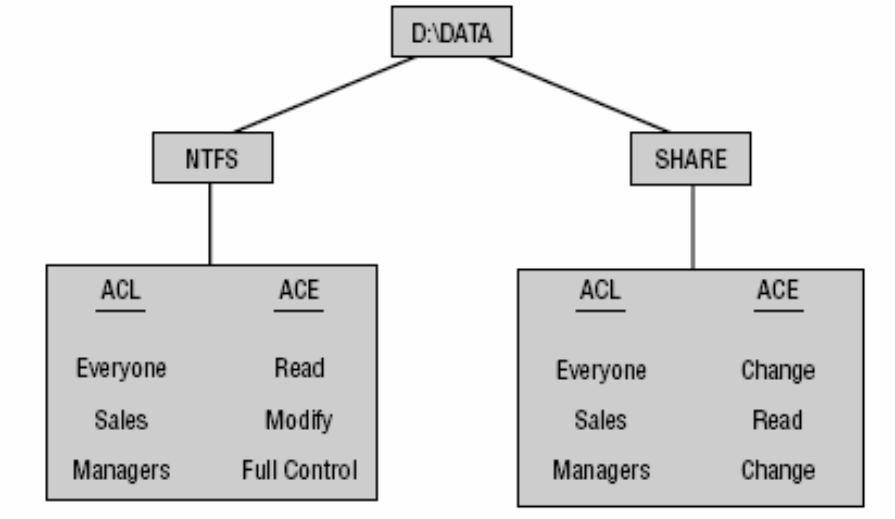
Hình 6.9 Cửa sổ Xem các tập tin đang mở

3. Quyền truy cập ntfs

Mục tiêu:

- Phân được quyền truy cập dữ liệu dùng trong hệ thống mạng.

Có hai loại hệ thống tập được dùng cho **partition** và **volume** cục bộ là **FAT** (bao gồm **FAT** và **FAT32**). **FAT partition** không hỗ trợ bảo mật nội bộ, còn **NTFS partition** thì ngược lại có hỗ trợ bảo mật; có nghĩa là nếu đĩa cứng của bạn định dạng là **FAT** thì mọi người đều có thể thao tác trên các file chứa trên đĩa cứng này, còn ngược lại là định dạng **NTFS** thì tùy theo người dùng có quyền truy cập không, nếu người dùng không có quyền thì không thể nào truy cập được dữ liệu trên đĩa. Hệ thống **Windows Server** dùng các **ACL (Access Control List)** để quản lý các quyền truy cập của đối tượng cục bộ và các đối tượng trên **Active Directory**. Một **ACL** có thể chứa nhiều **ACE (Access Control Entry)** đại diện cho một người dùng hay một nhóm người.



Hình 6.10 Phân quyền truy

3.1. Các quyền truy cập của NTFS

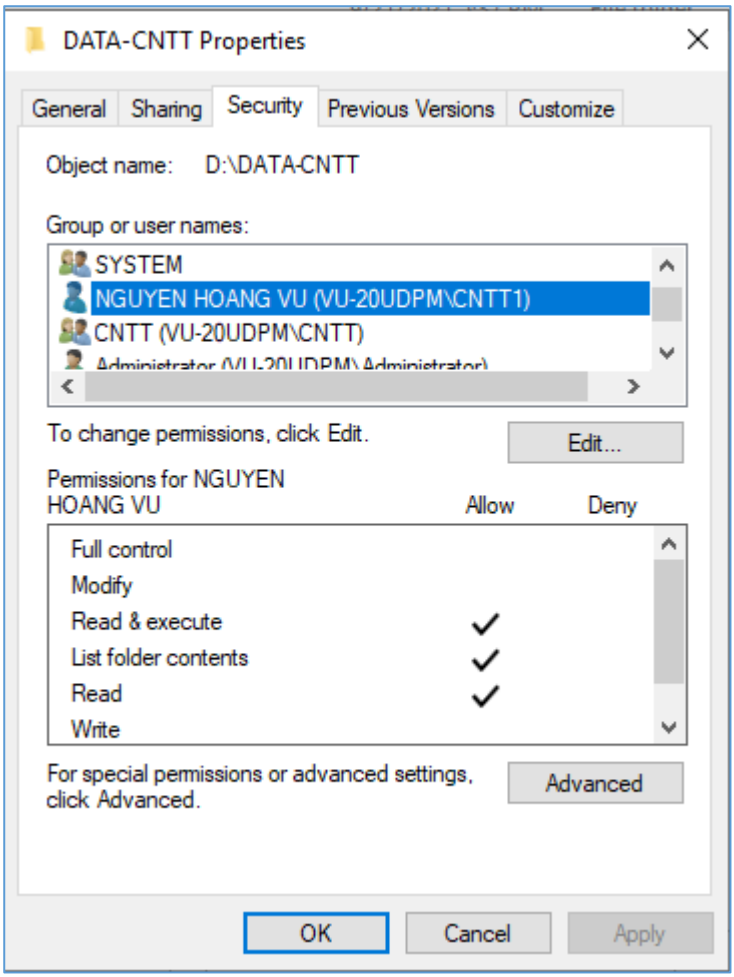
Tên quyền	Chức năng
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
List Folder/Read Data	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Read Attributes	Đọc các thuộc tính của các tập tin và thư mục
Read Extended Attributes	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

3.2. Các mức quyền truy cập được dùng trong NTFS

Tên quyền	Full Control	Modify	Read& Execute	List Folder Contents	Read	Write
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					

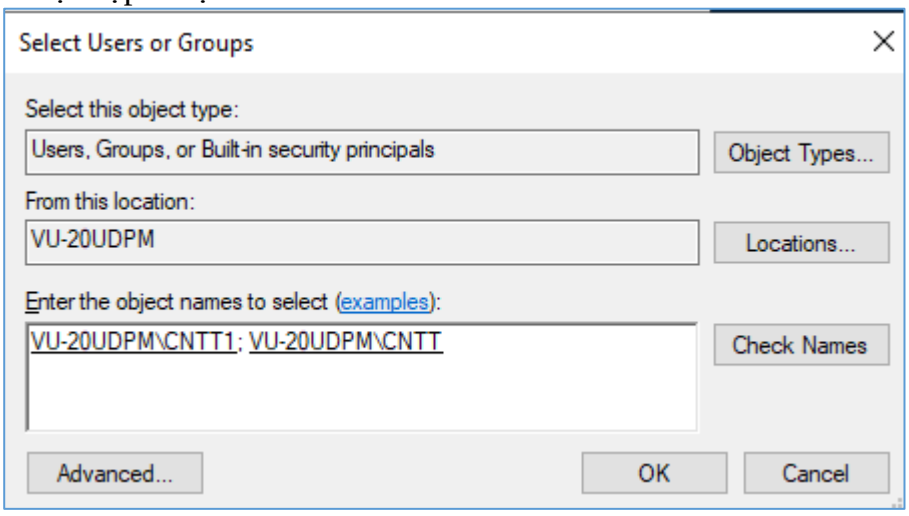
3.3. Gán quyền truy cập NTFS trên thư mục dùng chung

Bạn 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. Nếu ổ đĩa của bạn định dạng là **FAT** thì hộp thoại chỉ có hai **Tab** là **General** và **Sharing**. Nhưng nếu đĩa có định dạng là **NTFS** thì trong hộp thoại sẽ có thêm một **Tab** là **Security**. 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. Bạn nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.



Hình 6.11 Gán quyền truy cập NTFS

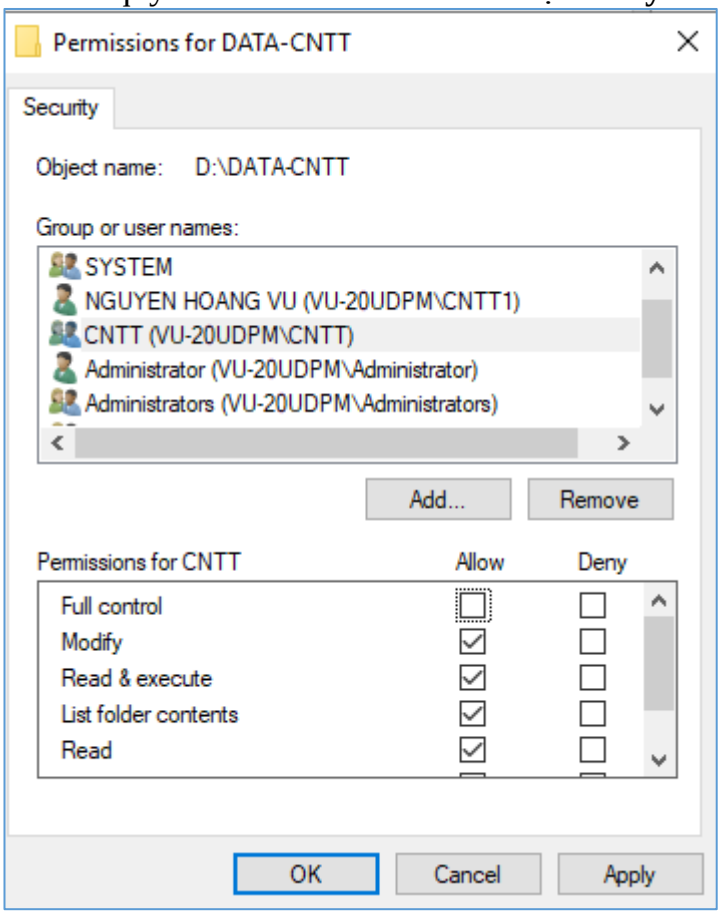
Muốn cấp quyền truy cập cho một người dùng, bạn nhấp chuột vào nút **Add**, hộp thoại chọn lựa người dùng và nhóm xuất hiện, bạn chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút **Add** để thêm vào danh sách, sau đó nhấp chuột vào nút **OK** để trở lại hộp thoại chính.



Hình 6.12 Cửa sổ xác nhận User và group

Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mà bạn mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách

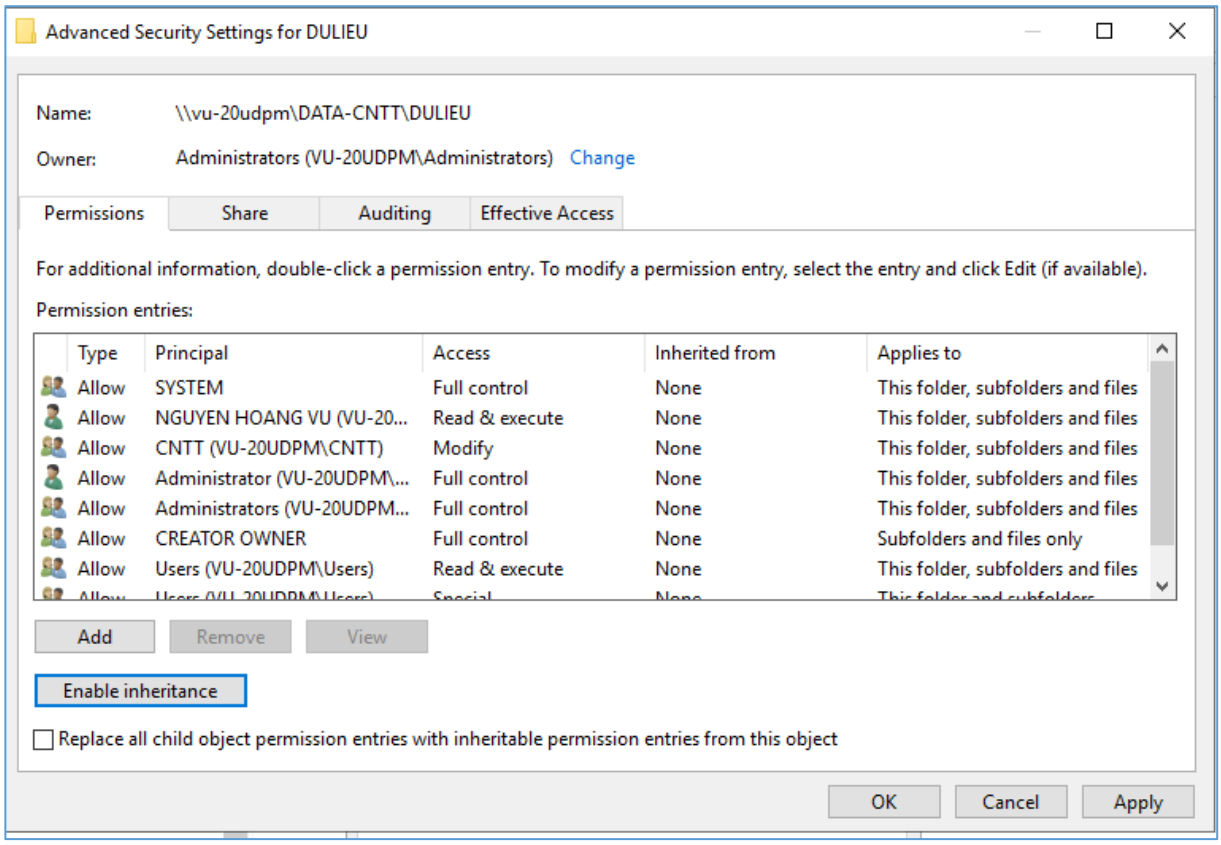
quyền, bạn muốn cho người dùng đó có quyền gì thì bạn đánh dấu vào phần **Allow**, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục **Deny**.



Hình 6.13 Cửa sổ cấp quyền User và group

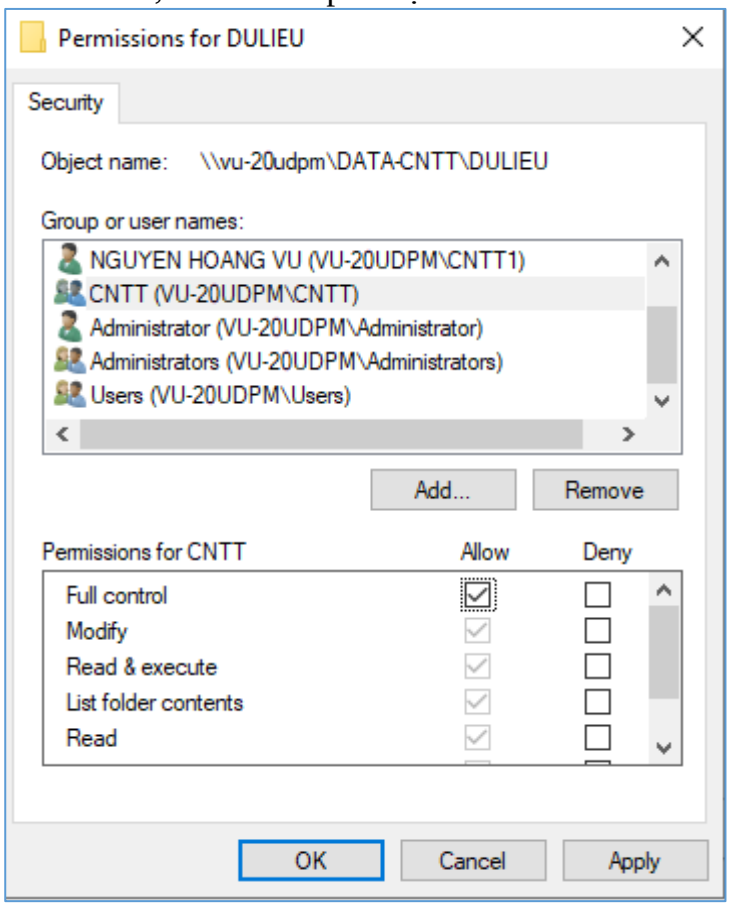
3.4. Kế thừa và thay thế quyền của đối tượng con.

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 6.14 Cửa sổ Kế thừa và thay thế quyền

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



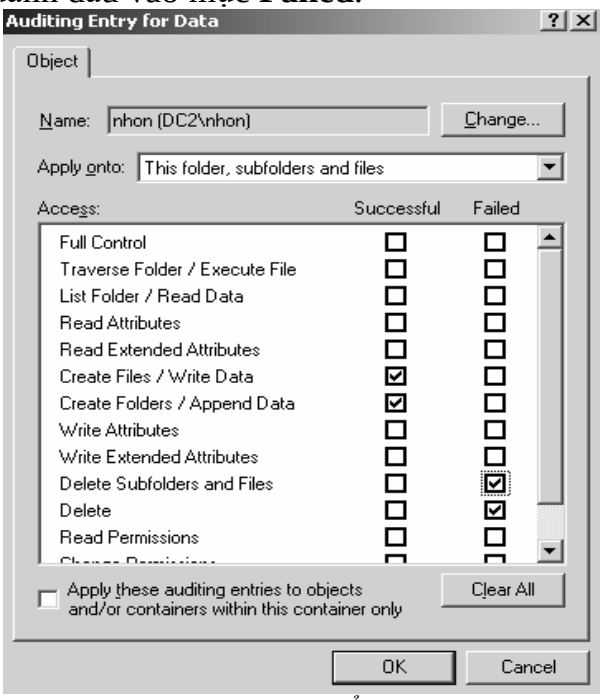
Hình 6.15 Cửa sổ cấp quyền

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

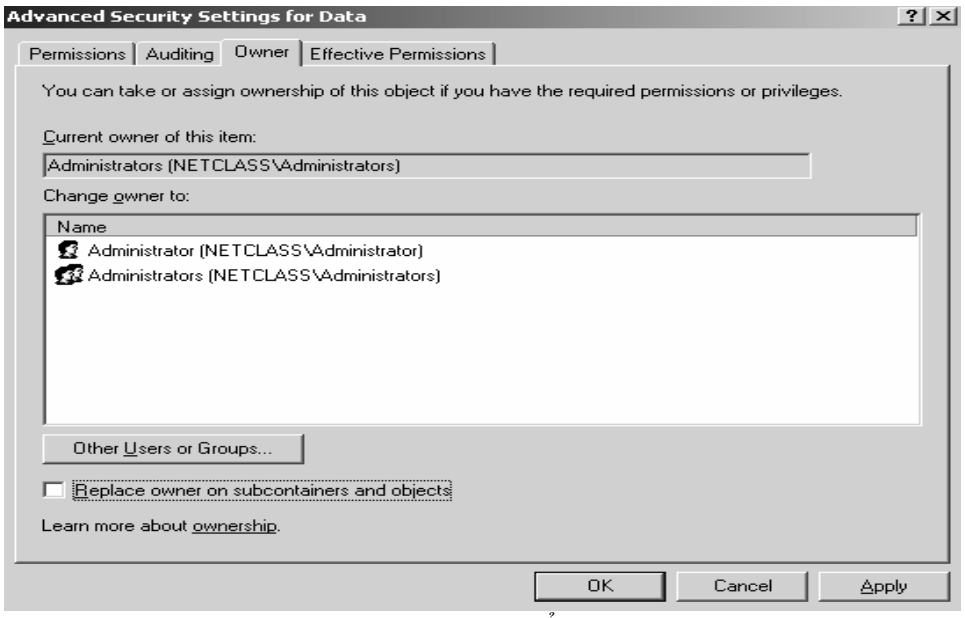
Bạn muốn giám sát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Auditing**, nhấp chuột vào nút **Add** để chọn người dùng cần giám sát, sau đó bạn muốn giám sát việc truy xuất thành công thì đánh dấu vào mục **Successful**, ngược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



Hình 6.16 Cửa sổ Auditing

3.7. Thay đổi người sở hữu thư mục

Bạn 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 bạn cũng có thể thay đổi người và nhóm người sở hữu thư mục này bằng cách nhấp chuột vào nút **Other Users or Groups**.



Hình 6.17 Cửa sổ Owner

4. DFS

Mục tiêu:

- Phân biệt được các loại hệ thống DFS.
- Triển khai thực hiện được hệ thống 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 bạn 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 bạn 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.

Bảng 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. - Người dùng truy xuất hệ thống DFS thông qua đường dẫn \\servername\dfsname.	- Là hệ thống **DFS** dựa trên nền **Active Directory** nên có chính dung lỗi cao. - Hệ thống **DFS** sẽ tự động đồng bộ giữa các **Domain Controller** và người dùng có thể truy xuất đến **DFS** thông qua đường dẫn

Bài tập thực hành của học viên

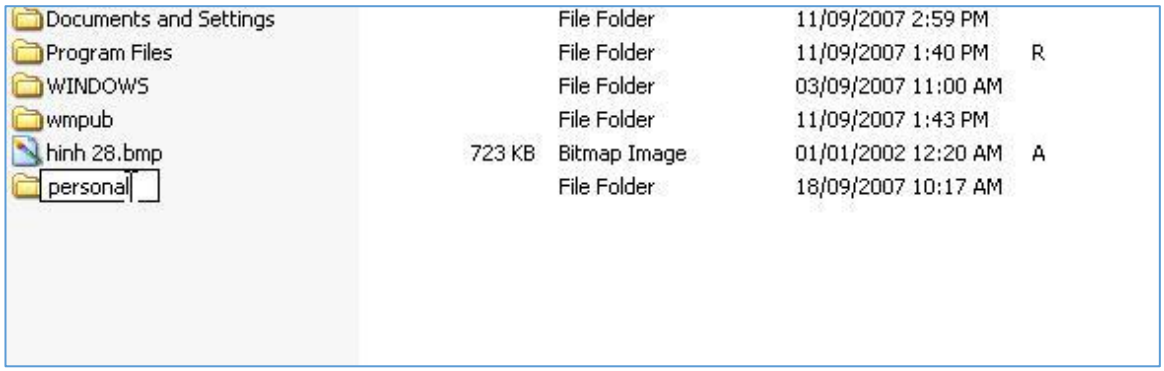
1. Tạo thư mục có tên Personal trên ổ đĩa bất kỳ.

2. Chia sẻ và phân quyền truy cập thư mục này.

Hướng dẫn trả lời:

1. Tạo thư mục có tên Personal trên ổ đĩa bất kỳ.

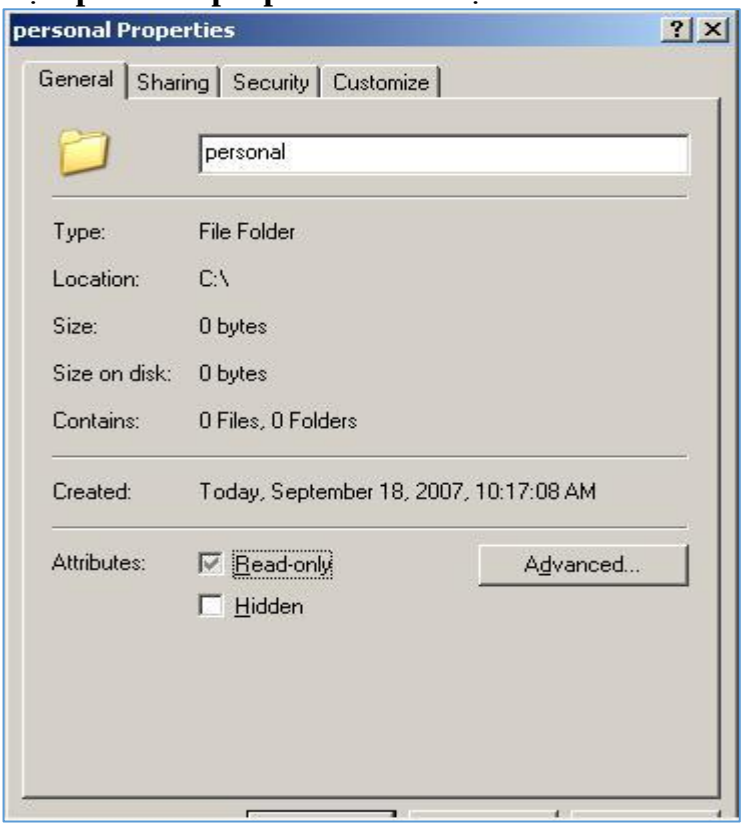
Mở ổ đĩa cần tạo folder để share, ở đây tôi chọn là ổ C, các bạn có thể tùy chọn một ổ đĩa khác bất kỳ, **right click** chọn **new**, chọn **folder,** và đặt tên cho folder này là **personal**



Hình 6.18 Cửa sổ tạo folder

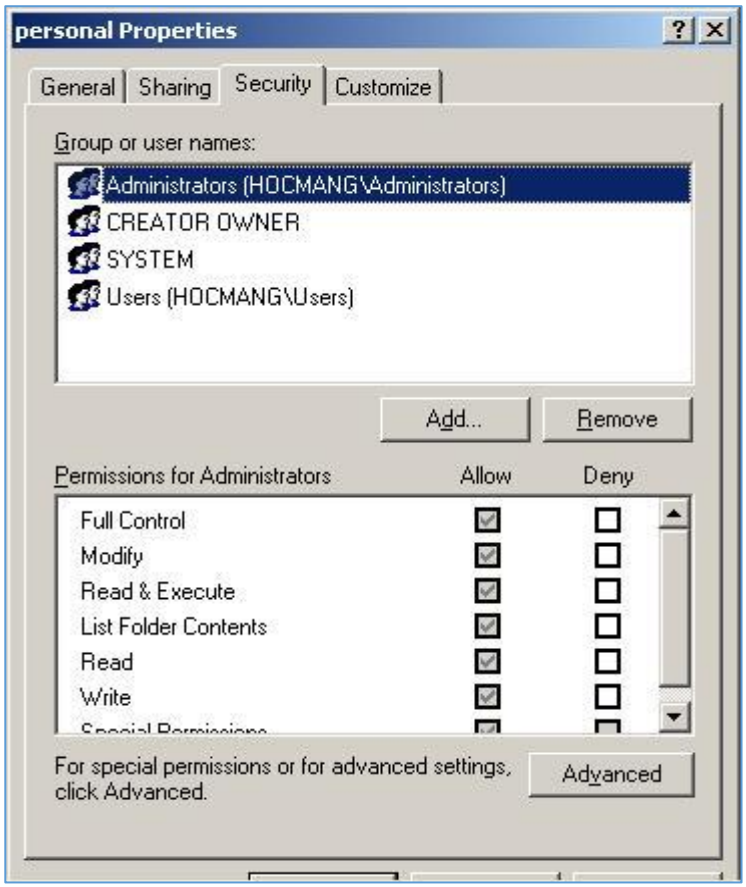
2. Chia sẻ và phân quyền truy cập thư mục này.

Ta sẽ cấu hình một số thuộc tính của **folder** này, right click vào **folder** này, chọn **properties**, hộp thoại **personal properties** xuất hiện:



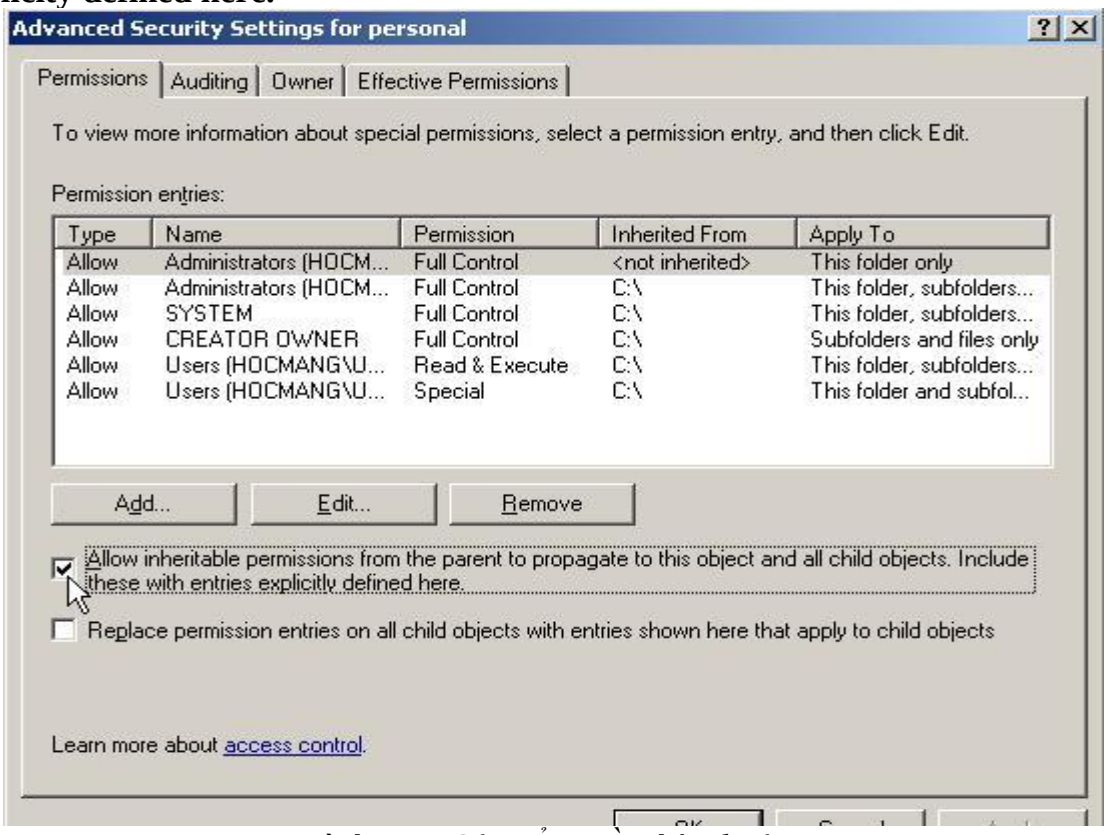
Hình 6.19 Cửa sổ personal properties

Click vào tab **Securiy** để cấu hình **NTFS permission** trên folder này. Trên tab Security, click nút **Advanced**



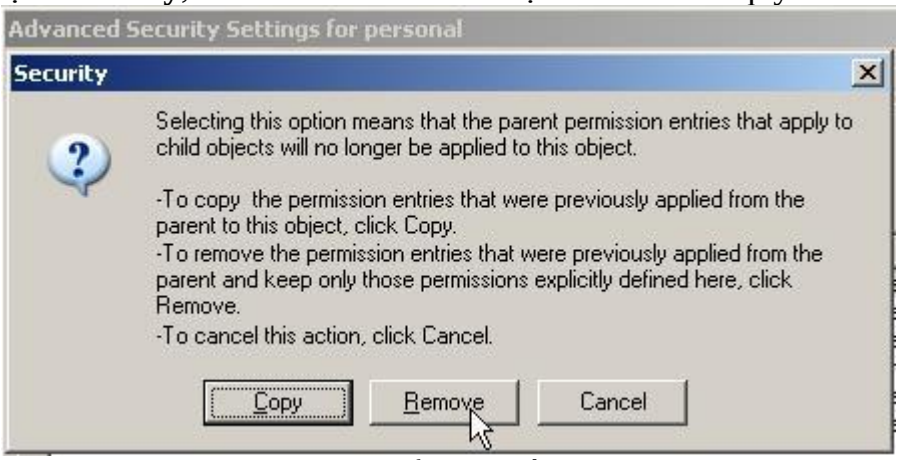
Hình 6.20 Cửa sổ Security

Trong hộp thoại **Advanced Security Setting for personal**, bạn ngắt quyền thừa hưởng bằng cách loại bỏ dấu check ra khỏi mục **Allow inheritable permissons from the parent to propagate to this object and all child object. Include these with entries explicity defined here.**



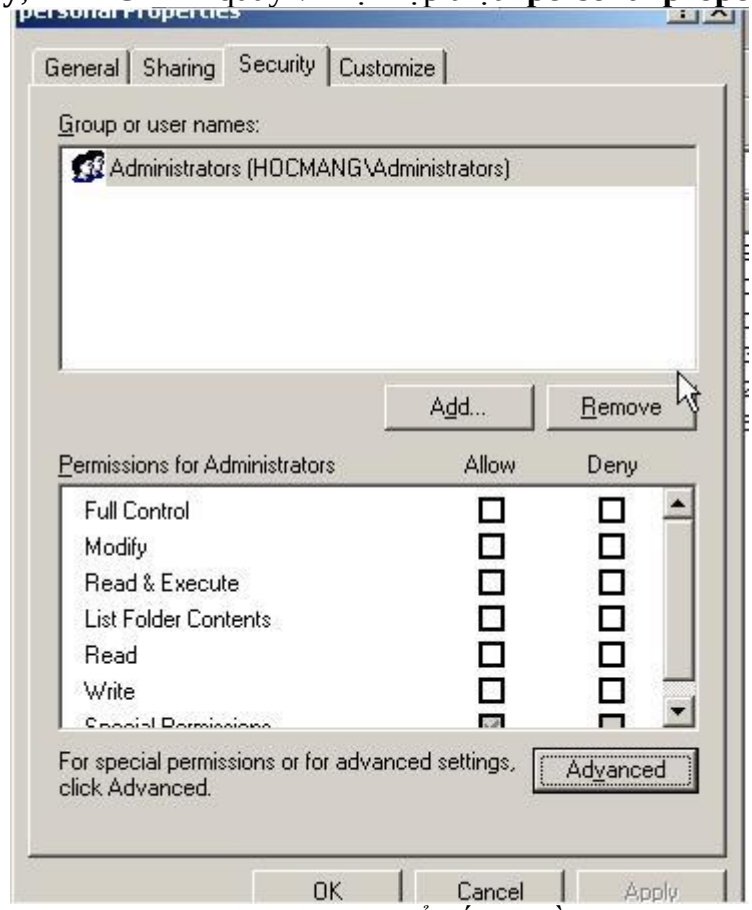
Hình 6.21 Cửa sổ quyền thừa hưởng

Trên hộp thoại **Security**, click nút **Remove** để loại bỏ tất cả các quyền thừa hưởng



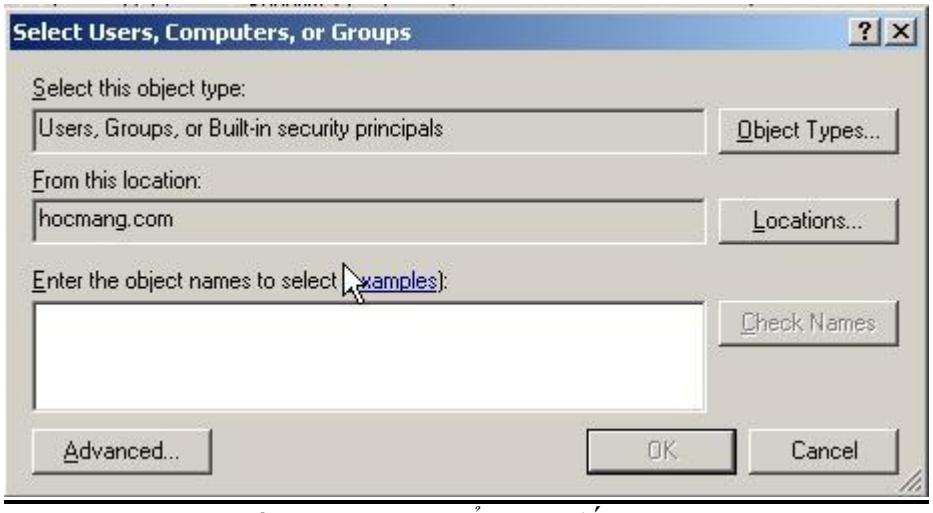
Hình 6.22 Cửa sổ bỏ quyền thừa hưởng

Xong nhấn **apply**, nhấn **OK** để quay về hội hộp thoại **personal properties**



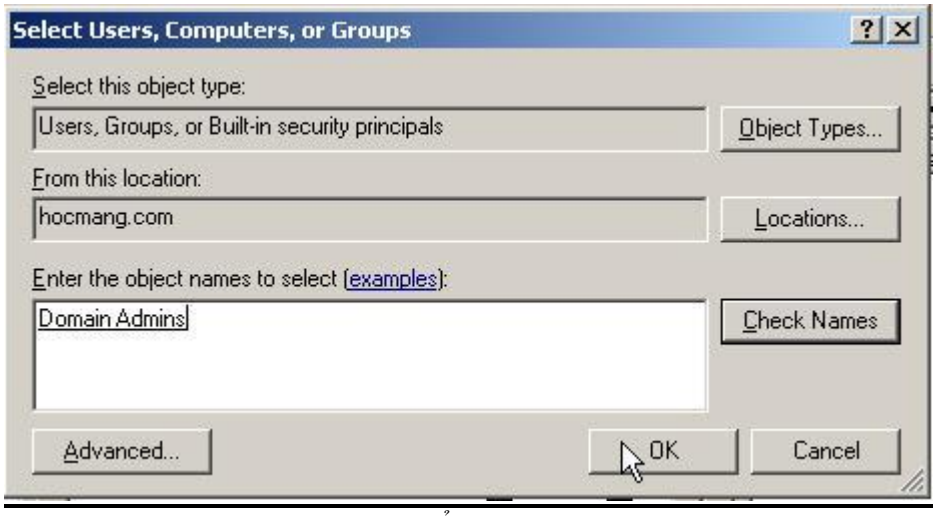
Hình 6.23 Cửa sổ cấp quyền

Trong hộp này các bạn nhấn **add**, sẽ xuất hiện hộp thoại **Select user**, **computer**, or **groups**



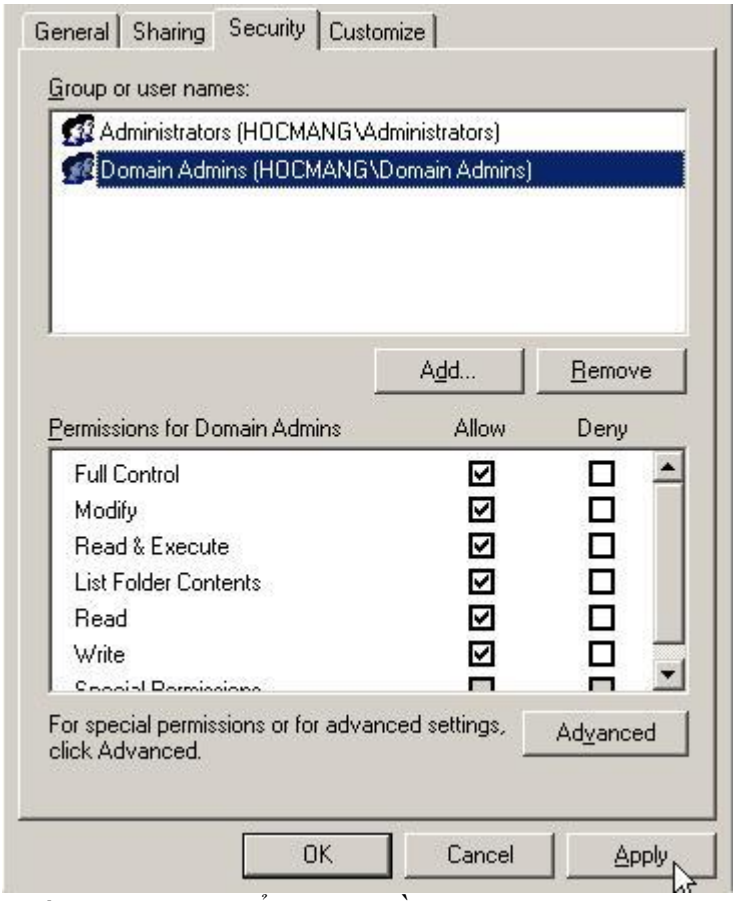
Hình 6.23 Cửa sổ chọn đối tượng

Nhập vào hộp text **Enter the object names to select (examples):** group **Domain Admins** rồi click vào nút **check names.** Group Domain **Admins** sẽ được gạch dưới, click **ok**



Hình 6.24 Cửa sổ chọn User và group

Trong hộp thoại **Personal Properties**, cấp quyền **Full Control** cho group **Domain Admins** bạn mới thêm vào. Click **apply**

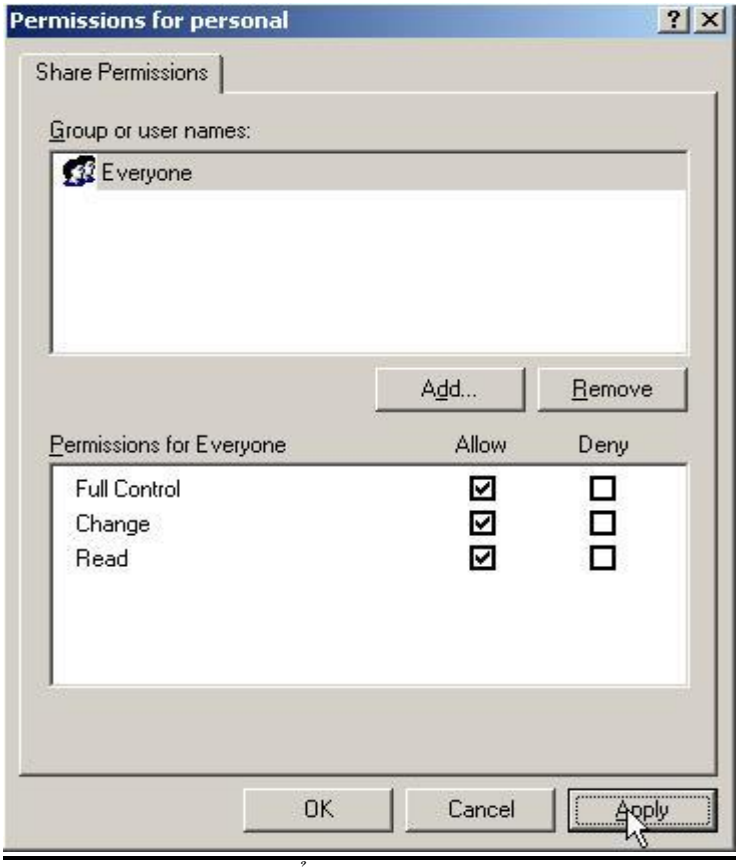


Hình 6.25 Cửa sổ Full quyền cho Domain Admins

Sau đó di chuyển qua tab **sharing**, trên tab **sharing**, đánh dấu chọn vào mục **share this folde**r để share folder này. Click vào nút **Permission** để ấn quyền share cho folder

Hình 6.26 Cửa sổ chia sẻ personal

Trong hộp thoại **permission for personal**, đánh dấu chọn vào mục **Full Control** trong cột **Allow** để cấp quyền **full control** cho **everyone group.** Click **apply** rồi click **ok**.



Hình 6.27 Cửa sổ Full control cho Everyone

Click apply và rồi click ok để đóng hộp thoại Personal Properties

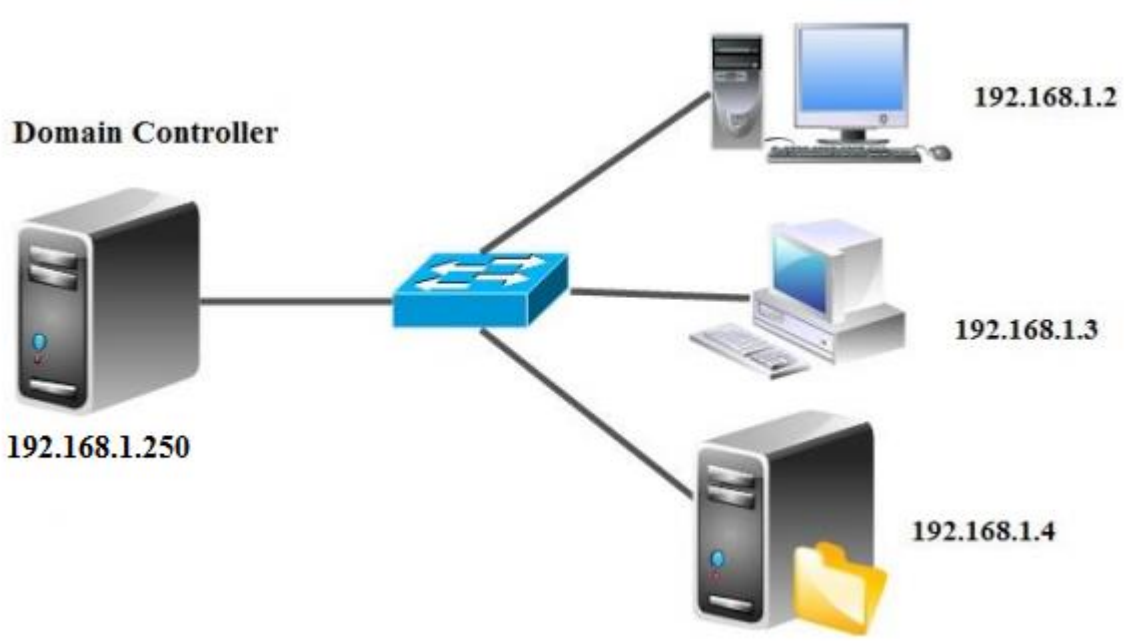
Những trọng tâm cần chú ý:

- Chọn ổ đĩa dữ liệu để chia sẻ cho đúng để không bị lỗi hệ thống.
- Cấp quyền cho đúng theo nhóm user và group cho từng folder
- Gán quyền truy cập cho các folder đúng với user và group
- Truy cập hệ thống kiểm tra xem phiên làm việc, xem user nào đang mở thư mục chia sẻ.
- Khi chúng ta cho phép user lưu trữ dữ liệu trên file server phải đúng dung lượng.
- Thực hiện đúng việc Kế thừa và thay thế quyền của đối tượng con.
- Tắt tường lửa cho máy DC và Client trên hệ thống.
- Thao tác phải đúng các bước tạo và quản lý thư mục dùng chung trên Windows server 2019.

Bài mở rộng và nâng cao

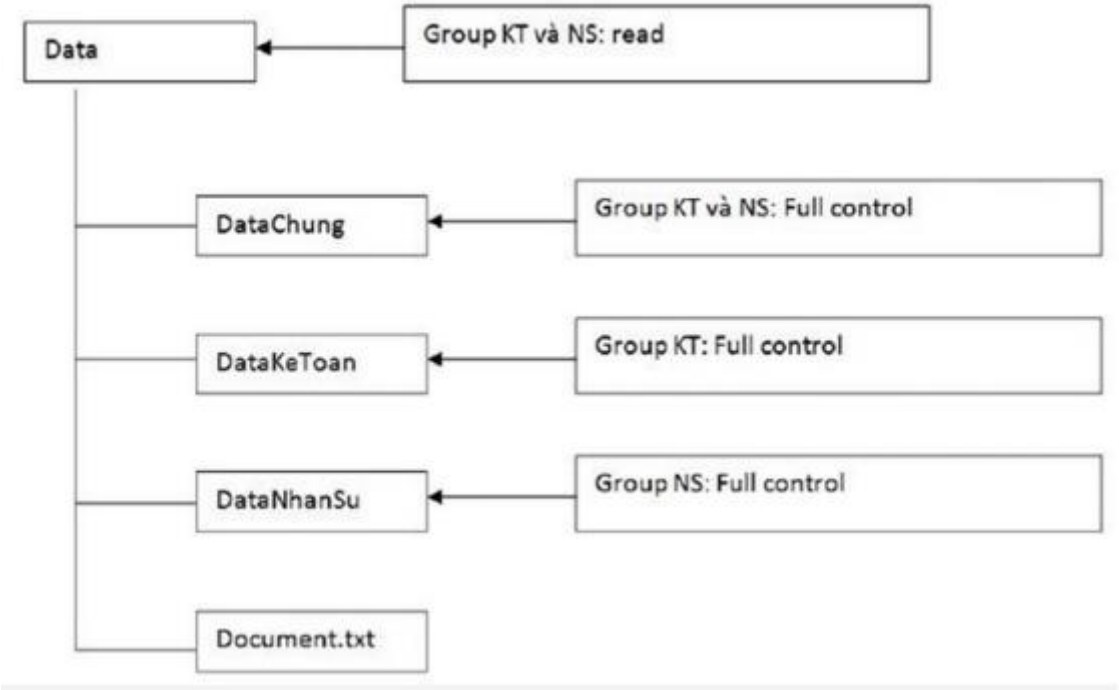
Tình huống: Chia sẻ và phân quyền các folder cho các user trong hệ thống với những chức năng mở rộng của NTFS

Mô hình



Yêu cầu:

- Tạo cây thư mục như sau



- Tạo 2 tài khoản NS1 và NS2 thuộc group NS và 2 tài khoản KT1, KT2 thuộc group KT

a) Thực hiện việc gán quyền như hình trên
b) Trong Folder DataKeToan, không cho tài khoản KT1 truy xuất
c) Tạo 2 Folder con trong DataNhanSu bằng tài khoản NS1, đăng nhập bằng NS2
d) Xóa 1 Folder mà NS1 vừa tạo, sau đó tạo 2 folder cùng cấp với folder vừa xóa
e) Thiết lập nguyên tắc "Không xóa dữ liệu của người khác"
f) Dùng Ns2 để loại bỏ hoàn toàn các tài khoản khác trên folder vừa tạo (bao gồm Administrators, System vv...)
g) Dùng Administrator để lấy lại quyền owner trên folder mà Ns2 đã thiết lập.

Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được Chức năng Chia sẻ, cấu hình, quản lý thư mục dùng chung trên Windows Server 2019
  + Trình bày được Chức năng DFS và Quyền truy cập NTFS trên Windows Server 2019
- Về kỹ năng:
  + Thao tác thành thạo việc Chia sẻ, cấu hình, quản lý thư mục dùng chung trên hệ thống.
  + Thao tác thành thạo việc cấp phát, thu hồi Quyền truy cập NTFS trong cục bộ hoặc Domain trên Windows Server 2019
  + Thực hiện đúng yêu cầu Tài khoản NS1 không xóa folder mà NS2 tạo và Lấy quyền lại cho admin khi bị NS2 xóa bỏ.
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng:
  + Đánh giá kỹ năng thực hành về việc Chia sẻ, cấu hình, quản lý thư mục dùng chung trên hệ thống.
  + Đánh giá kỹ năng thực hành về cấp phát, thu hồi Quyền truy cập NTFS trong cục bộ hoặc Domain trên Windows Server 2019.
  + Đánh giá kỹ năng thực hành về yêu cầu Tài khoản NS1 không xóa folder mà NS2 tạo và Lấy quyền lại cho admin khi bị NS2 xóa bỏ
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 7: CHÍNH SÁCH BẢO MẬT
Mã bài: MĐ 17 - 07

Mục tiêu:

- Trình bày các loại chính sách
- Thiết lập các chính sách cục bộ trên hệ thống.
- Thiết lập các chính sách miền trên hệ thống
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Giới thiệu chung về GPO

Group Policy là tập hợp các thiết lập cấu hình cho Computer và Users, xác định cách thức để các chương trình, tài nguyên mạng và hệ điều hành làm việc với người dùng và máy tính trong 1 tổ chức. Mục đích sử dụng GPO nhằm triển khai các chính sách từ miền máy chủ Domain Controller xuống Users. Group Policy có thể dùng để triển khai phần mềm cho một hoặc hoặc nhiều máy trạm nào đó một cách tự động; để ấn định quyền hạn cho một số người dùng mạng, để giới hạn những ứng dụng mà người dùng được phép chạy; để kiểm soát hạn ngạch sử dụng đĩa trên các máy trạm; để thiết lập các kịch bản (script) đăng nhập (logon), đăng xuất (logout), khởi động (start up), và tắt máy (shut down)

Group Policy chỉ áp dụng trên các máy Windows Server NT/ 2000 / 2003 / 2008 / 2012 /2016 /2019 … và chủ yếu áp dụng cho các Site, Domain và Organization Unit. Các chính sách nhóm được áp dụng cho các đối tượng như Site, domain, OU được gọi là GPO (Group Policy Objects)

Trên mỗi máy Windows Server 2019 cũng có 1 bộ công cụ Group Policy được gọi là Local Group Policy và sẽ chỉ áp dụng cho chính máy này khi máy đó không tham gia vào miền.

Các Group Policy Objects được lưu trữ trong cơ sở dữ liệu của Active Directory. Chương trình để tạo ra và chỉnh sửa GPO có tên là Group Policy Object Editor (đây là 1 dạng console tên là gpedit.msc, console của Active Directory Users and Computers là dsa.msc)

2. Chức năng của Group Policy

Các Group Policy có thể dùng để triển khai cài đặt phần mềm xuống các máy trạm trong miền một cách tự động. Dùng để ấn định các quyền hạn cho người dùng trong mạng.

Giới hạn phần mềm được cài đặt trên máy Client, giới hạn những ứng dụng được phép chạy trên máy Client. Kiểm soát hạn ngạch sử dụng ổ đĩa cứng trên máy Client. Thiết lập các kịch bản (Script) cho đăng nhập (Logon), đăng xuất (Logout), khởi động (Startup), tắt máy (Shutdown), đơn giản hóa việc quản lý các máy Client. GPO định hướng lại một số thư mục quan trọng trên máy Client và còn rất nhiều chức năng khác nữa tùy thuộc vào nhu cầu của người quản trị.

Một số chú ý trong GPO: Các GPO chỉ có thể hiện hữu trong miền Active Directory, GPO mất tác dụng đối với những máy client khi chúng được xóa khỏi miền và các máy tính Local chỉ có thể sử dụng Local Group Policy

3. Chính sách cục bộ

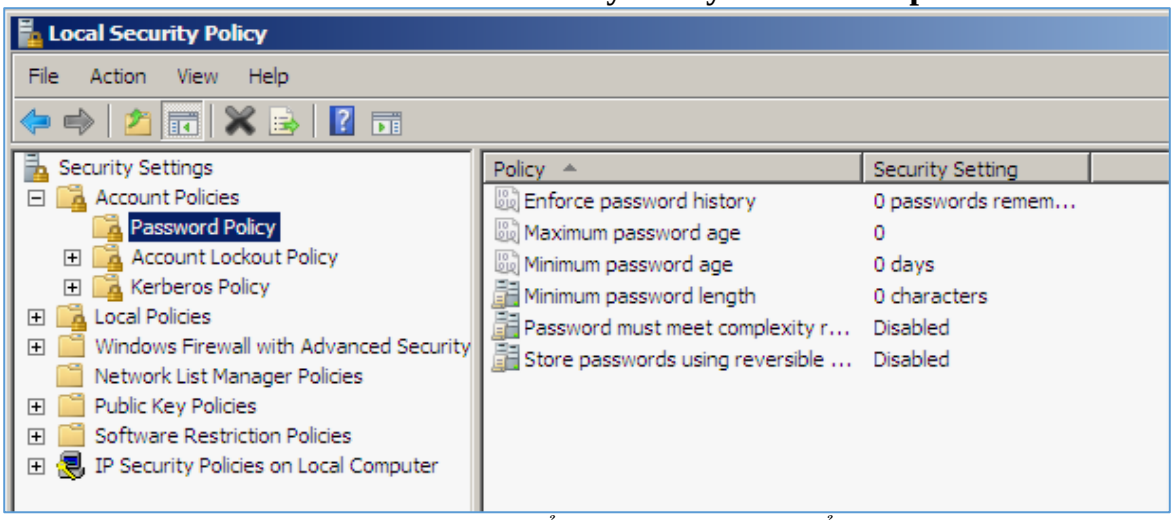
3.1 Account Policy

- **Password Policies:** Bao gồm các chính sách liên quan đến mật khẩu tài khoản của người sử dụng tài khoản trên máy.

- **Enforce password history:** Với những người sử dụng không có thói quen ghi nhớ nhiều mật khẩu, khi buộc phải thay đổi mật khẩu thì họ vẫn dùng chính mật khẩu cũ để thay cho mật khẩu mới, điều này là một kẽ hở lớn liên quan trực tiếp đến việc lộ mật khẩu. Thiết lập này bắt buộc một mật khẩu mới không được giống bất kỳ một số mật khẩu nào đó do ta quyết định. Có giá trị từ 0 đến 24 mật khẩu.
- **Maximum password age:** Thời gian tối đa mật khẩu còn hiệu lực, sau thời gian này hệ thống sẽ yêu cầu ta thay đổi mật khẩu. Việc thay đổi mật khẩu định kỳ nhằm nâng cao độ an toàn cho tài khoản, vì một kẻ xấu có thể theo dõi những thói quen của bạn, từ đó có thể tìm ra mật khẩu một cách dễ dàng. Số giá trị từ 1 đến 999 ngày, giá trị mặc định là 42 ngày.
- **Minimum password age:** Xác định thời gian tối thiểu trước khi có thể thay đổi mật khẩu. Hết thời gian này bạn mới có thể thay đổi mật khẩu của tài khoản, hoặc bạn có thể thay đổi ngay lập tức bằng cách thiết lập giá trị là 0. Giá trị từ 0 đến 999 ngày.
- **Minimum password length:** Độ dài nhỏ tối thiểu của mật khẩu tài khoản (tính bằng số ký tự nhập vào). Độ dài của mật khẩu có giá trị từ 1 đến 14 ký tự. Thiết lập giá trị là 0 nếu không muốn sử dụng mật khẩu. Giá trị mặc định là 0.
- **Password must meet complexity requirements:** Quyết định độ phức tạp của mật khẩu, nếu tính năng này có hiệu lực, mật khẩu của tài khoản ít nhất phải đạt những yêu cầu sau:+ Không chứa tất cả hoặc một phần tên tài khoản người dùng.+ Độ dài nhỏ nhất là 6 ký tự.+ Chứa 3 hoặc 4 loại ký tự sau: Các chữ cái thường (a->z), các chữ cái hoa (A->Z>), các chữ số (0->9) và các ký tự đặc biệt.
  Độ phức tạp của mật khẩu được coi là bắt buộc khi tạo mới hoặc thay đổi mật khẩu, mặc định là: *Disable*.
- **Store password using reversible encryption fo all user in the domain:** Lưu trữ mật khẩu sử dụng mã hóa ngược cho tất cả các người sử dụng domain. Tính năng cung cấp sự hỗ trợ cho các ứng dụng giao thức, nó yêu cầu sự am hiểu về mật khẩu người sử dụng. Việc lưu trữ mật khẩu sử dụng phương pháp mã hóa ngược thực chất giống như việc lưu trữ các văn bản mã hóa các thông tin bảo vệ mật khẩu. Mặc định: *Disable*.

3.1.1 Password policy

Vào **Aministrator ➔ Local Sercurity Policy ➔ Account policies**



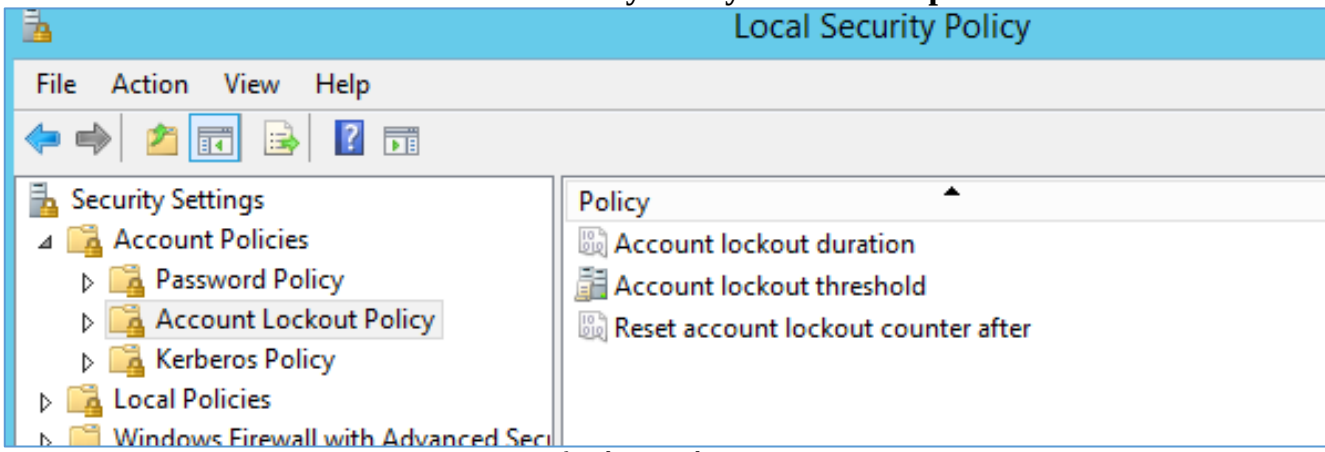
Hình 7.1 Cửa sổ chính sách mật khẩu

Trong này bao gồm các mục:

- **Password must meet complexity** …: khi đặt password cho wins phải có đủ độ phức tạp.(hoa, thường, số, ký tự đặc biệt). Mặc định tính năng này sẽ bị disable, để gia tăng chế độ bảo mật nên chọn Enable
- **Minimum password age**: mặc định giá trị này là 0 nếu ta thay nó bằng con số khác 0 VD là 3 chẳng hạn thì user chỉ có quyền thay đổi password 3 ngày một lần mà thôi.
- **Minimum password length**: Độ dài tối thiểu của password
- **Enforce password history**: nhớ bao nhiêu password không cho đặt trùng.
- **Store password using reversible** …: mã hoá password.

3.1.2 Account lockout policy

Vào **Aministrator ➔ Local Sercurity Policy ➔ Account policies**



Hình 7.2 Cửa sổ cấp quyền đăng nhập

- **Account lockout threshold**: để khoá account khi đăng nhập sai.
- **Account lockout duration**: khoá account trong 30 phút khi đang nhập sai.
- **Reset account lockout counter after**: xoá bộ nhớ đánh pass.

3.2. Local Policy

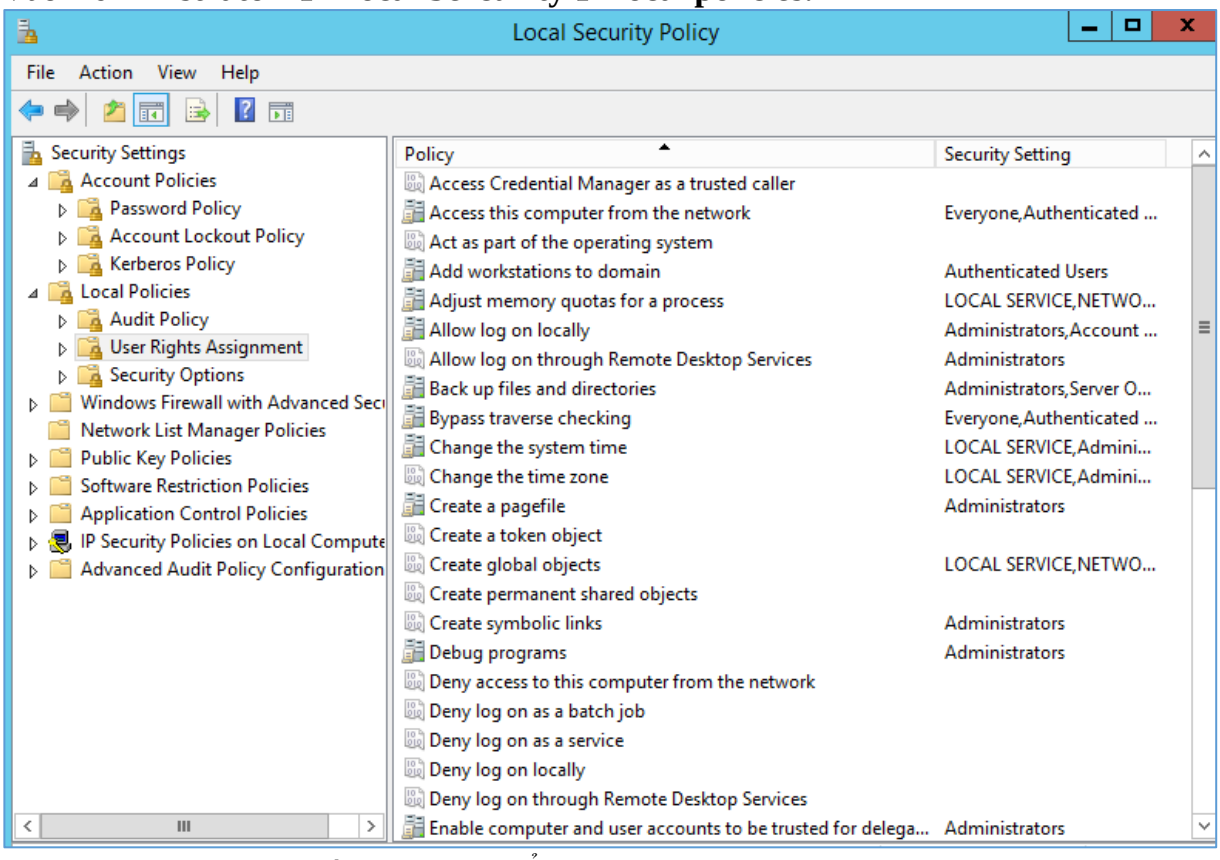
- **User rights Assignments:** Ấn định quyền cho người dùng.Quyền của người dùng ở đây bao gồm các quyền truy cập, quyền backup dữ liệu, thay đổi thời gian cho hệ thống….Trong phần này để cấu hình cho một mục nào đó, click đúp chuột lên mục và click Add user or group để trao quyền mặc định cho user hoặc group theo yêu cầu.
- **Access this computer from the network:** Với những kẻ tò mò, tốt nhất chúng ta không cho phép chúng truy cập vào máy tính của mình. Với thiết lập này ta có thể tùy ý thêm, bớt quyền truy cập vào máy cho bất ký tài khoản nào hoặc nhóm nào.
- **Act as part of the operating system:** Chính sách này chỉ định tài khoản nào sẽ được phép hoạt động như một phần của hệ thống. Mặc định Administrator có quyền cao nhất, có thể thay đổi bất kỳ thiết lập nào của hệ thống, được xác nhận như bất kỳ một người dùng, vì thế có thể sử dụng tài nguyên hệ thống như bất kỳ người dùng nào. Chỉ có những dịch vụ chứng thực ở mức thấp mới yêu cầu đặc quyền này.
- **Add workstation to domain:** Thêm một tài khoản hoặc nhóm vào miền. Chính sách này chỉ hoạt động trên hệ thống sự dụng Domain Controller. Khi được thêm vào miền, tài khoản này sẽ có thêm các quyền hoạt động trên dịch vụ thư mục (Active Directory), có thể truy cập tài nguyên mạc như một thành viên trong domain.
- **Adjust memory quotas for a process**: Chỉ định những ai được phép điều chỉnh chi tiêu bộ nhớ dành cho một quá trình xử lý. Chính sách này có làm tăng hiệu

suất hệ thống nhưng nó có thể bị lạm dụng phục vụ cho những mục đích xấu như tấn công từ chối dịch vụ DoS (Dial of Service).

- **Allow logon through Terminal Services:** Terminal services là một dịch vụ cho phép đăng nhập từ xa đến máy tính. Chính sách này sẽ quyết định giúp chúng ta những ai được phép sử dụng dịch vụ Terminal services để đăng nhập hệ thống.
- **Backup files add directories:** Tương tự như các chính sách trên, ở đây cấp phép ai đó có quyền backup dữ liệu.
- **Change the system time:** Cho phép người sử dụng nào có quyền thay đổi thời gian của hệ thống.
- **Create global objects**: Cấp quyền cho ai có thể tạo ra các đối tượng dùng chung.
- **Force shutdown from a remote system:** Cho phép ai có quyền tắt máy qua hệ thống điều khiển từ xa.
- **Shutdown the system:** Cho phép ai có quyền shutdown máy.
- **Deny access to this computer from the net…:** Cấm user không được phép truy xuất đến máy.
- **Deny logon localy:** Cấm User Logon cục bộ.
- **Deny logon through Terminal Services:** Cấm User Remote Desktop.
- **Logon localy:** Thiết lập người dùng Logon cục bộ.

3.2.1. User rights assignment

Vào **Administrator ➔ Local Sercurity➔Local policies.**

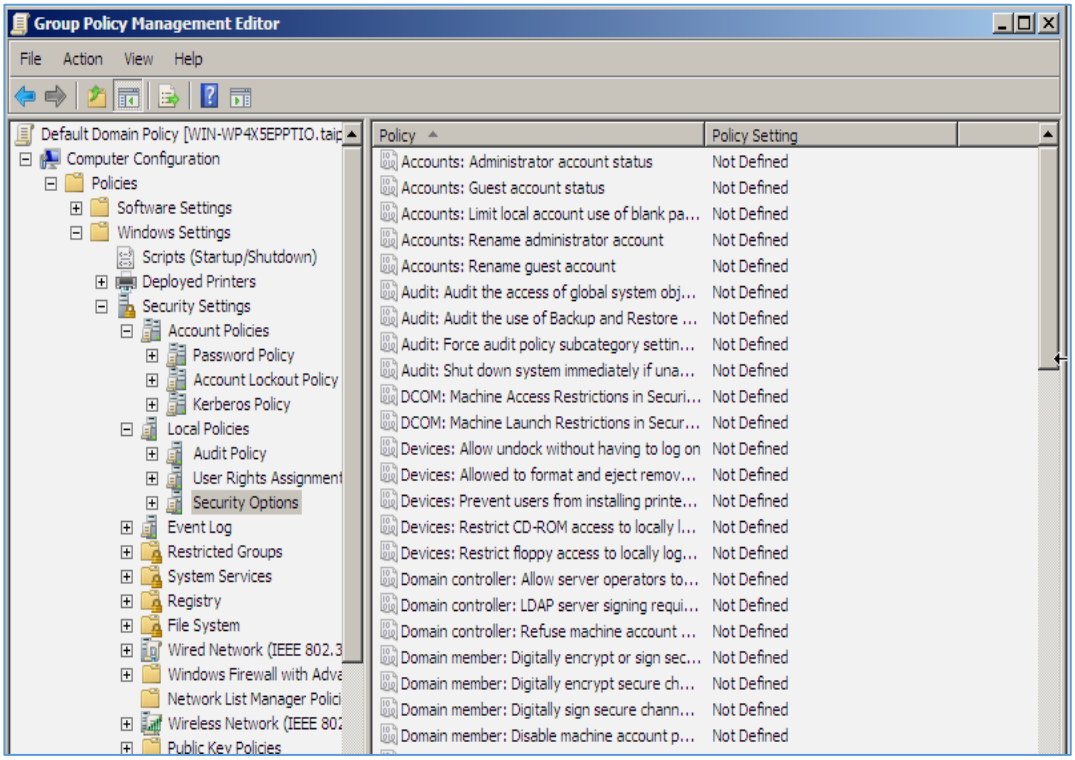


Hình 7.3 Cửa sổ User rights assignment

- **Deny logon locally**: chọn user không cho đăng nhập vào máy tính.
- **Change the system time**: những người được thay đổi giờ hệ thống.
- **Shutdown the system**: những người có quyền tắt máy.
- **Allow log on through Terminal Services**: cho phép đăng nhập.
- **Log on as a Service**: đăng nhập như một dịch vụ.

Và còn rất nhiều tính năng khác

3.2.2.Sercurity options



Hình 7.4 Cửa sổ xem User truy cập thư mục

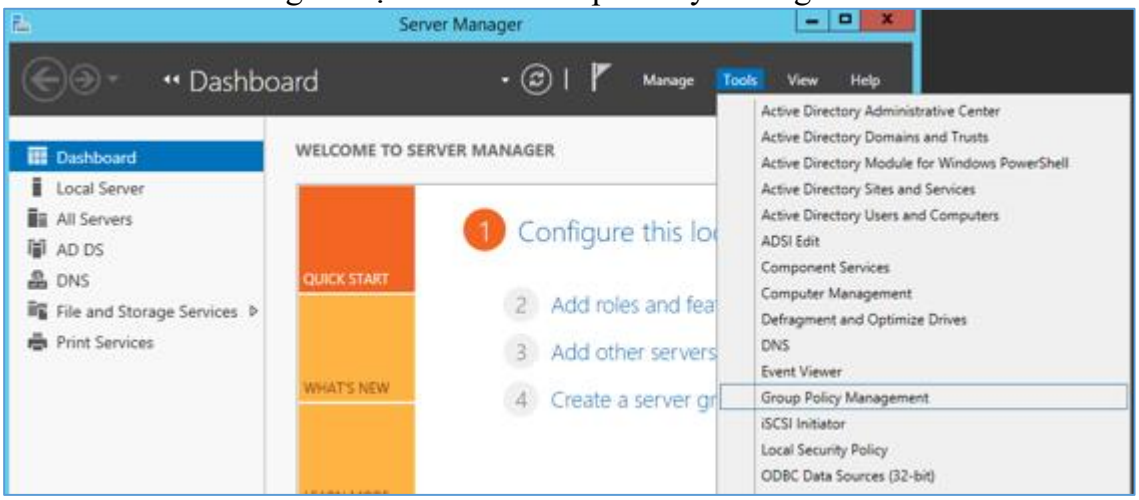
- **Account: Administrator account status:** Trạng thái hoạt động của Administrator.
- **Account: Guest account status:** Trạng thái hoạt động của User Guest.
- **Account: Limit local account use of blank password to console:** Đăng nhập không cần password.
- **Account: Rename administrator account:** Đổi tên Administrator.
- **Account: Rename guest account**: Đổi tên Guest.
- **Devices: Prevent users from installing printer drivers:** Không cho phép cài Printer
- **Devices: Restrict CD-ROM access to localy logged-on user only:** Cấm truy nhập xa từ CD-ROM.
- **Interactive: Do not require CTRL + ALT + DEL:** Bỏ Ctrl + alt + Del
- **Interactive: Message text for users attempting to logon:** Đặt tiêu đề khi logon.
- **Interactive: Message title for users attempting to log on:** Đặt tiêu đề khi logon
- **Interactive: Number of previous logons to cache in cache:** Cache kho logon
- **Shutdown:** Allow system to be shut down
- **Shutdown: Allow system to be shut down without having to log on:** Shutdown không cần logon.
- **Shutdown: Clear virtual memory pagefile.** Xóa bộ nhớ ảo khi Shutdown.
- **Interactive logon**: **Do not display last user name**: Khi user logout máy cửa sổ đăng nhập sẽ không ghi lại account user vừa logon.

- **Interactive logon**: **Message text for users attempting to log on**: Bạn có thể nhắn gởi một nội dung nào đó tới các user trước khi họ logon vào máy với nội dung nhắn gởi ở đây.
- **Interactive logon**: **Message title for users attempting to log on**: Bạn nhập tiêu đề của hộp nội dung nhắn gởi vào đây.

Chú ý: để triển khai các GPO xuống Client ta dùng lệnh "gpupdate /force" trong CMD

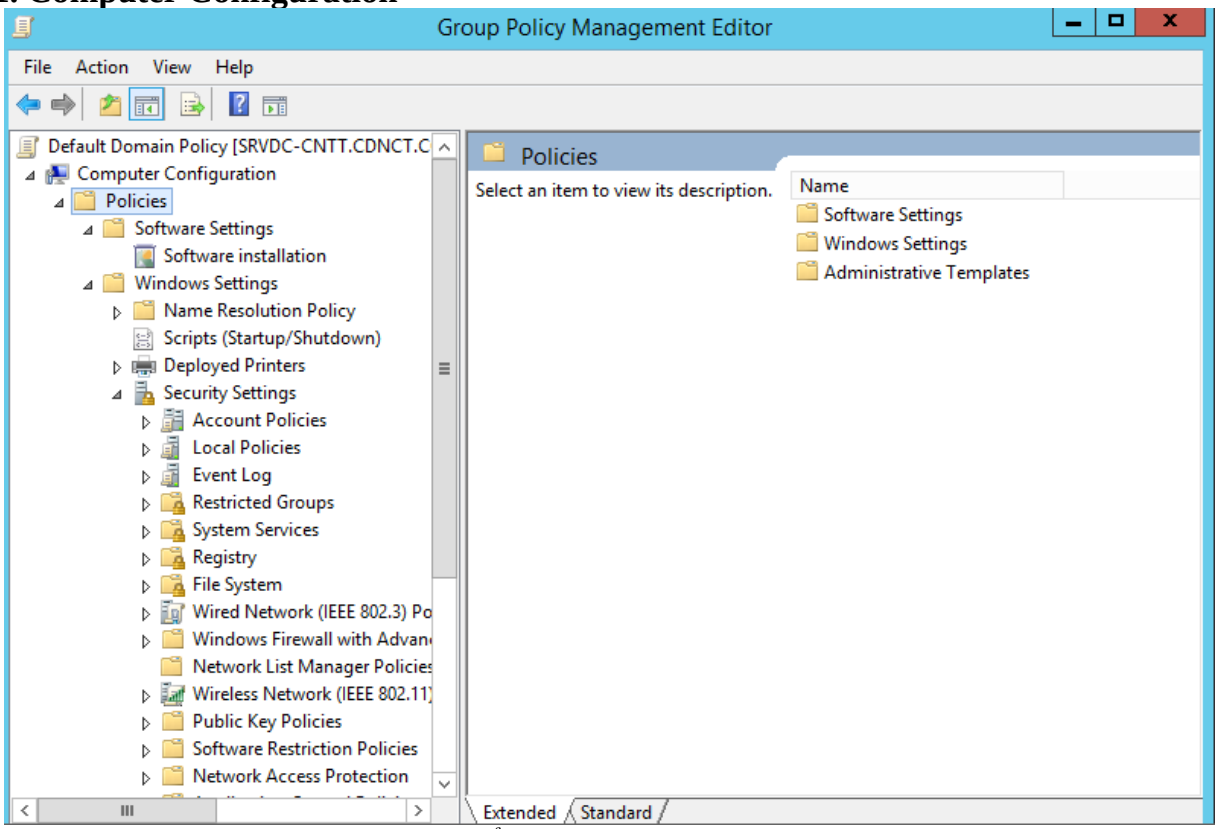
4.Cấu hình Group Policy Object

Vào Server Manager chọn Tools / Group Policy Management



Hình 7.5 Cửa sổ mở GPO

4.1. Computer Configuration



Hình 7.6 Cửa sổ Computer Configuration DC

Windows Setting:

Tại đây có thể tinh chỉnh, áp dụng các chính sách về vấn đề sử dụng tài khoản, quản lý việc khởi động và đăng nhập hệ thống…

- Scripts: (startup/Shutdown): Có thể chỉ định cho Windows sẽ chạy một mã nào đó khi Windows Startup hoặc Shutdown.

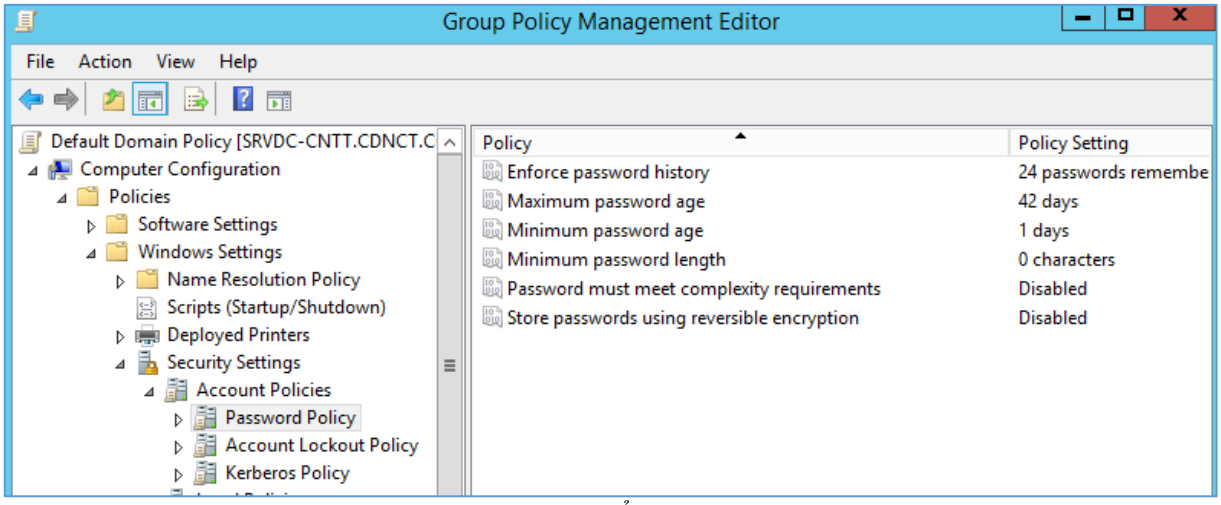
- Security setting: Các thiết lập bảo mật cho hệ thống, các thiết lập này được áp dụng cho toàn bộ hệ thống chứ không riêng người dùng nào.

Account Policies: Các chính sách áp dụng cho tài khoản người dùng.

Local Policy: Kiểm định chính sách, những tùy chọn quyền lợi và chính sách an toàn cho người dùng cục bộ.

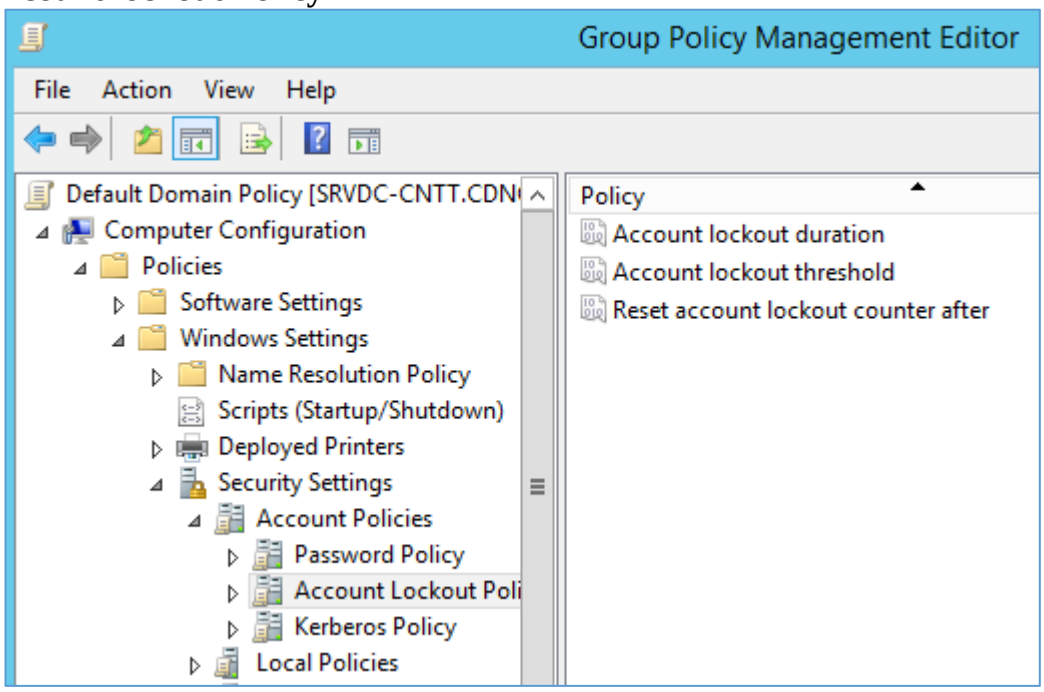
Public Key Policies. Các chính sách khóa dùng chung.

4.1.1. Acount Policies.



Hình 7.6 Cửa sổ pasword DC

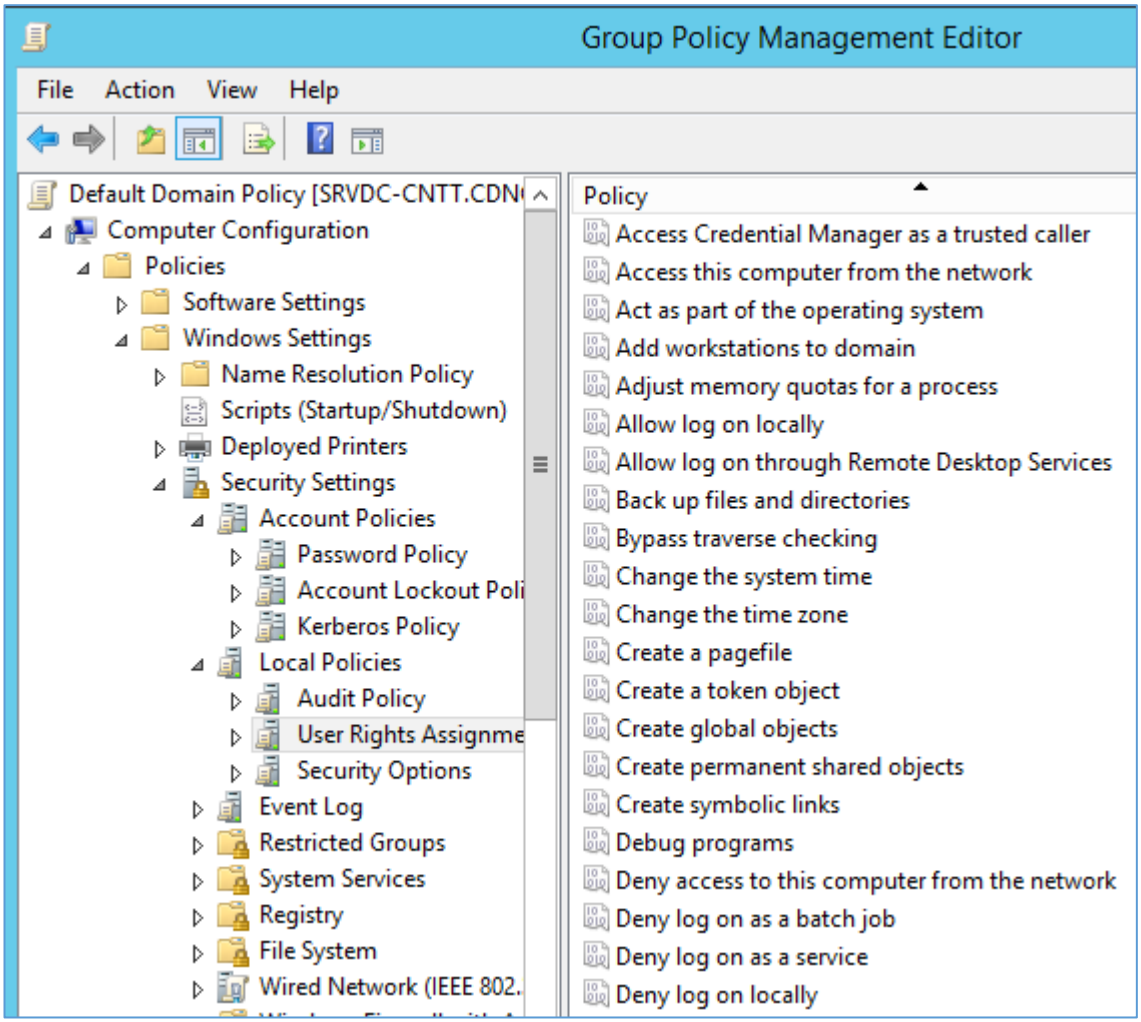
4.1.2 Acount lockout Policy



Hình 7.6 Cửa sổ Acount lockout Policy DC

4.2 Local Policy DC

a. User rights Assignments



Hình 7.6 Cửa sổ Acount lockout Policy DC

+ **Access this computer from the network:** Với những kẻ tò mò, tốt nhất chúng ta không cho phép chúng truy cập vào máy tính của mình. Với thiết lập này ta có thể tùy ý thêm, bớt quyền truy cập vào máy cho bất kỳ tài khoản nào hoặc nhóm nào.

+ **Act as part of the operating system:** Chính sách này chỉ định tài khoản nào sẽ được phép hoạt động như một phần của hệ thống. Mặc định Administrator có quyền cao nhất, có thể thay đổi bất kỳ thiết lập nào của hệ thống, được xác nhận như bất kỳ một người dùng, vì thế có thể sử dụng tài nguyên hệ thống như bất kỳ người dùng nào. Chỉ có những dịch vụ chứng thực ở mức thấp mới yêu cầu đặc quyền này.

+ **Add workstation to domain:** Thêm một tài khoản hoặc nhóm vào miền. Chính sách này chỉ hoạt động trên hệ thống sự dụng Domain Controller. Khi được thêm vào miền, tài khoản này sẽ có thêm các quyền hoạt động trên dịch vụ thư mục (Active Directory), có thể truy cập tài nguyên mạc như một thành viên trong domain.

+ **Adjust memory quotas for a process**: Chỉ định những ai được phép điều chỉnh chi tiêu bộ nhớ dành cho một quá trình xử lý. Chính sách này có làm tăng hiệu suất hệ thống nhưng nó có thể bị lạm dụng phục vụ cho những mục đích xấu như tấn công từ chối dịch vụ DoS (Dial of Service).

+ **Allow logon through Terminal Services:** Terminal services là một dịch vụ cho phép đăng nhập từ xa đến máy tính. Chính sách này sẽ quyết định giúp chúng ta những ai được phép sử dụng dịch vụ Terminal services để đăng nhập hệ thống.

+ **backup files add directories:** Tương tự như các chính sách trên, ở đây cấp phép ai đó có quyền backup dữ liệu.

+ **Change the system time:** Cho phép người sử dụng nào có quyền thay đổi thời gian của hệ thống.

+ **Create global objects**: Cấp quyền cho ai có thể tạo ra các đối tượng dùng chung.

+ **Force shutdown from a remote system:** Cho phép ai có quyền tắt máy qua hệ thống điều khiển từ xa.

+ **Shutdown the system:** Cho phép ai có quyền shutdown máy.

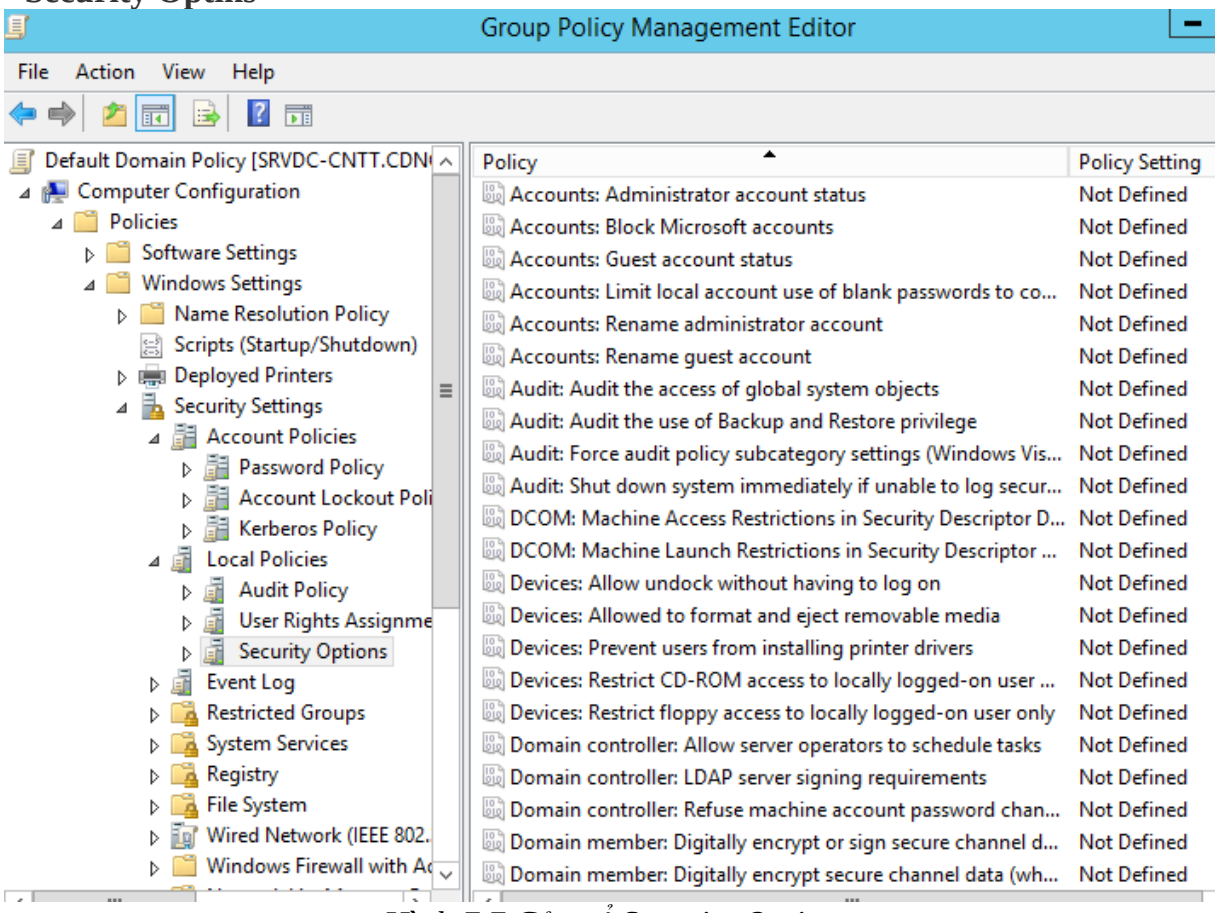
+ **Deny access to this computer from the net…:** Cấm user không được phép truy xuất đến máy.

+ **Deny logon localy:** Cấm User Logon cục bộ.

+ **Deny logon through Terminal Services:** Cấm User Remote Desktop.

+ **Logon localy:** Thiết lập người dùng Logon cục bộ.

- Security Optins



Hình 7.7 Cửa sổ Security Optins

+ **Account: Administrator account status:** Trạng thái hoạt động của Administrator.

+ **Account: Guest account status:** Trạng thái hoạt động của User Guest.

+ **Account: Limit local account use of blank password to consolo:** Đăng nhập không cần password.

+ **Account: Rename administrator account:** Đổi tên Administrator.

+ **Account: Rename guest account**: Đổi tên Guest.

+ **Devices: Prevent users from installing printer drivers:** Không cho phép cài Printer

+ **Devices: Restrict CD-ROM access to localy logged-on user only:** Cấm truy nhập xa từ CD-ROM.

+ **Interactive: Do not require CTRL + ALT + DEL:** Bỏ Ctrl + alt + Del

+ Interactive: Message text for users attempting to logon: Đặt tiêu đề khi logon.

+ Interactive: Message title for users attempting to log on: Đặt tiêu đề khi logon

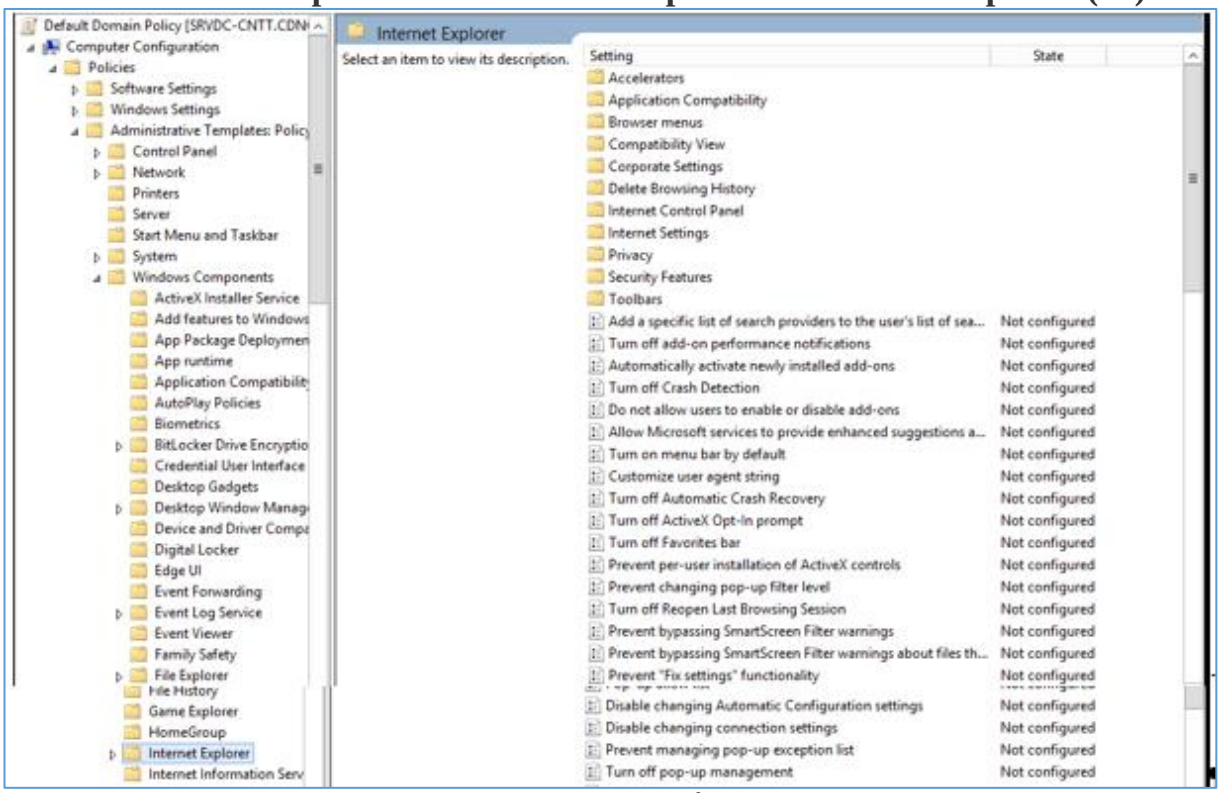
+ Interactive: Number of previous logons to cache in cache: Cache kho logon

+ Shutdown: Allow system to be shut down

+ Shutdown: Allow system to be shut down without having to log on: Shutdown không cần logon.

+ Shutdown: Clear virtual memory pagefile. Xóa bộ nhớ ảo khi Shutdown.

- Administrator Templates -> Windows Components -> Intenet Explorer (IE)



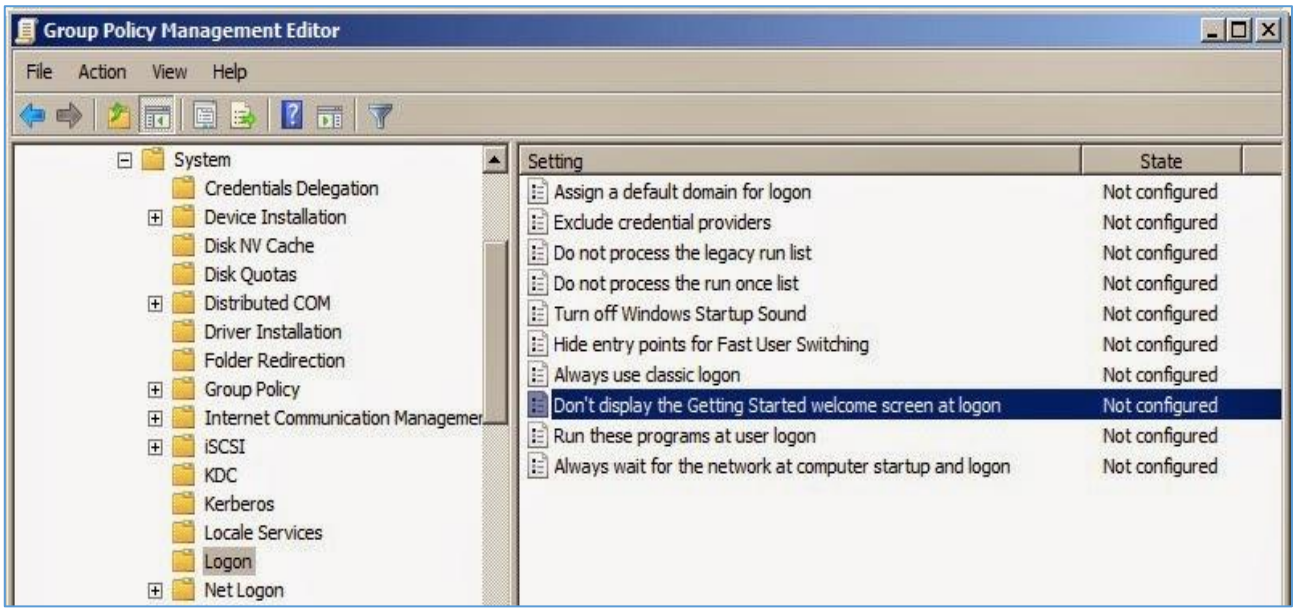
Hình 7.8 Cửa sổ IE

+ Security Zones: Use only machine settings: Bắt buộc tất cả các User đều chung một mức độ Security như nhau.

+ Security Zones: Do not allow users to change policies: Trong Security Zone có danh sách các Site nguy hiểm do người dùng thiết lập, Enable tùy chọn sẽ không co thay đổi danh sách đó (Tốt nhất là giấu thẻ Security).

+ Disable Periodic Check for Internet Explorer software updates: Ngăn không cho IE tự động Update.

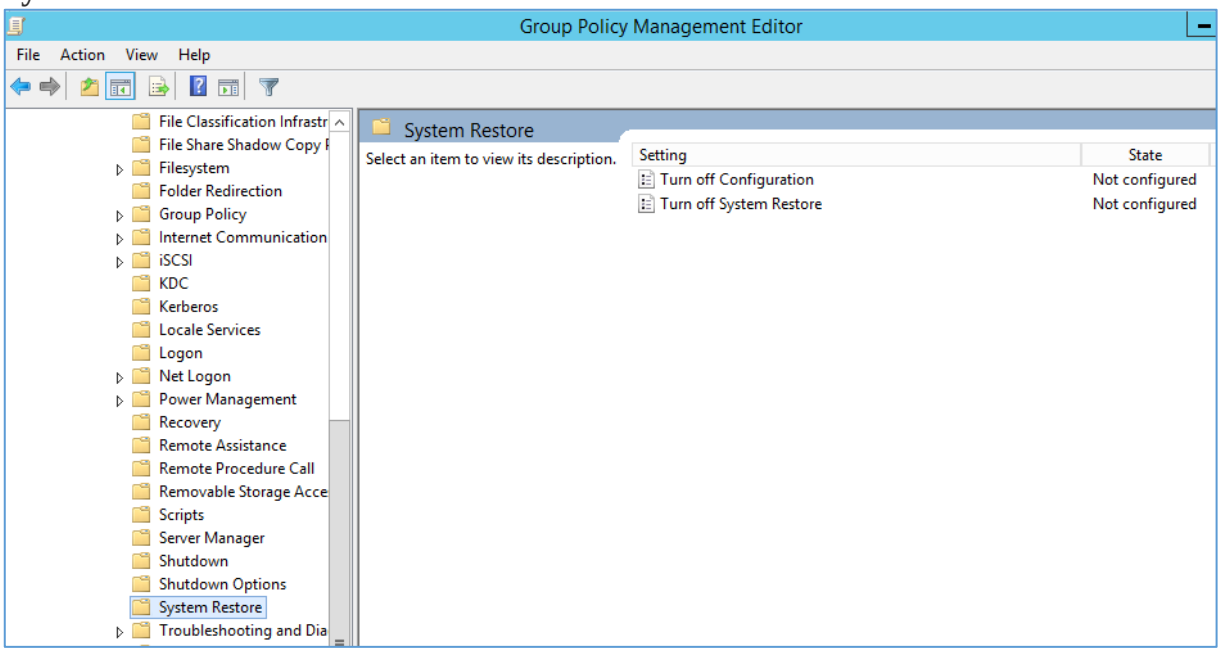
- Administrator Templates -> System -> Logon



Hình 7.9 Cửa sổ Logon

+ Don't display the Getting Started welcome screen at logon: Ẩn màn hình Welcome khi User đăng nhập vào hệ thống.

- Computer Configuration -> Policies – > Administrative Templates – > System -> Systemstore

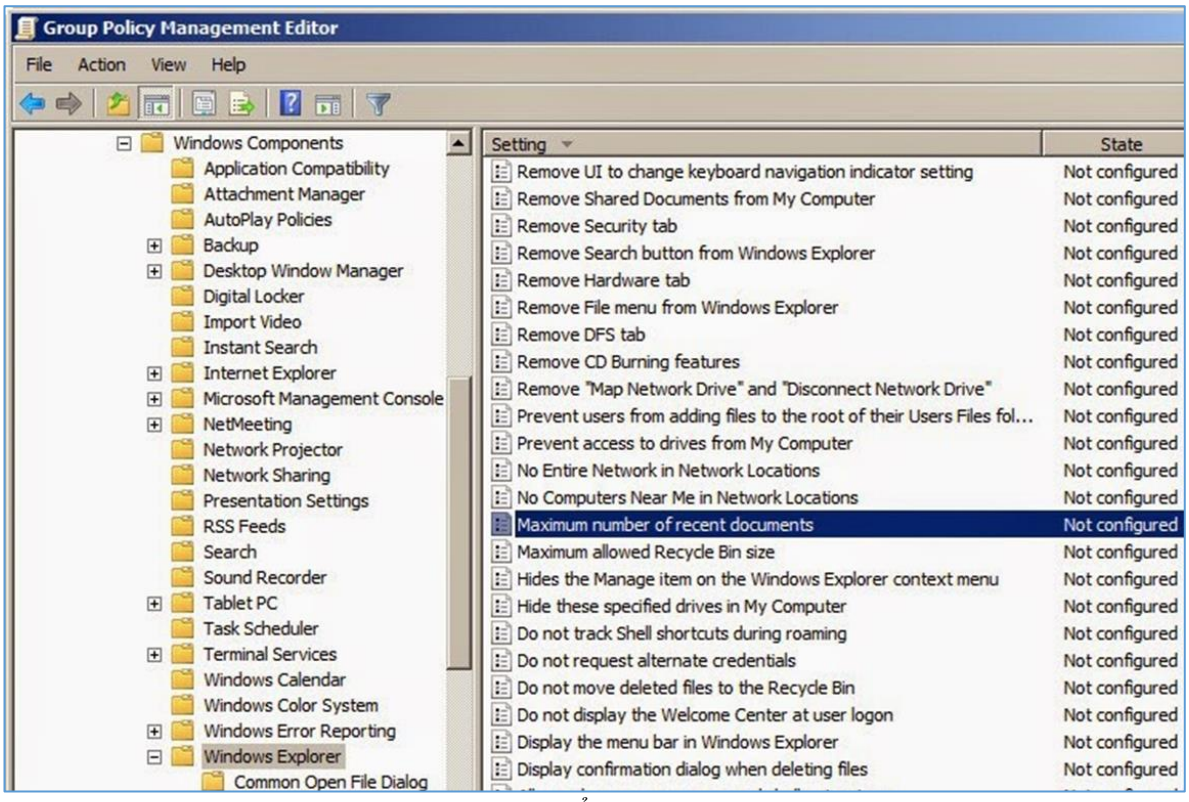


Hình 7.10 Cửa sổ Systemstore

+ Turn off System Restore: Tắt System Restore, khi user gọi System Restore thì xuất hiện thông báo "System Restore has been turn off by group policy. To turn on System Restore, contact your domain Administrator".

+ Turn off Configuration: Chỉ có tác dụng khi System Restore được kích hoạt, tính năng này vô hiệu hóa phần thiết lập cấu hình của System Restore.

- User configuration – > Administrator Templates – > Windows Components – > Windows Expolorer



Hình 7.11 Cửa sổ Windows Expolorer

+ **Maximum number of recent documents:** Quy định số lượng tài liệu đã mở hiển thị trong My Recent Documents.

+ **Do not move deleted files to the Recycle Bin:** File bị xóa sẽ không được đưa vào Recycle Bin.

+ **Maximum allowed Recycle Bin size:** Giới hạn dung lượng Recycle Bin, tính bằng đơn vị phần trăm dung lượn của ổ đĩa cứng.

+ **Removes the Folder Options menu item from the Tools menu.** Ẩn Folder Option.

+ **Remove Search button from Windows Expolorer**. Ẩn Search trong Explorer.

+ **Remove Windows Explorer's default context menu**. Ẩn context khi click chuột phải.

+ **Hides the manage item the Windows Expolorer context**. Ẩn manage khi click chuột phải vào My Computer.

+ **Hide these specfied drivers in My Computer.** Ẩn ổ đĩa (access qua Addresss).

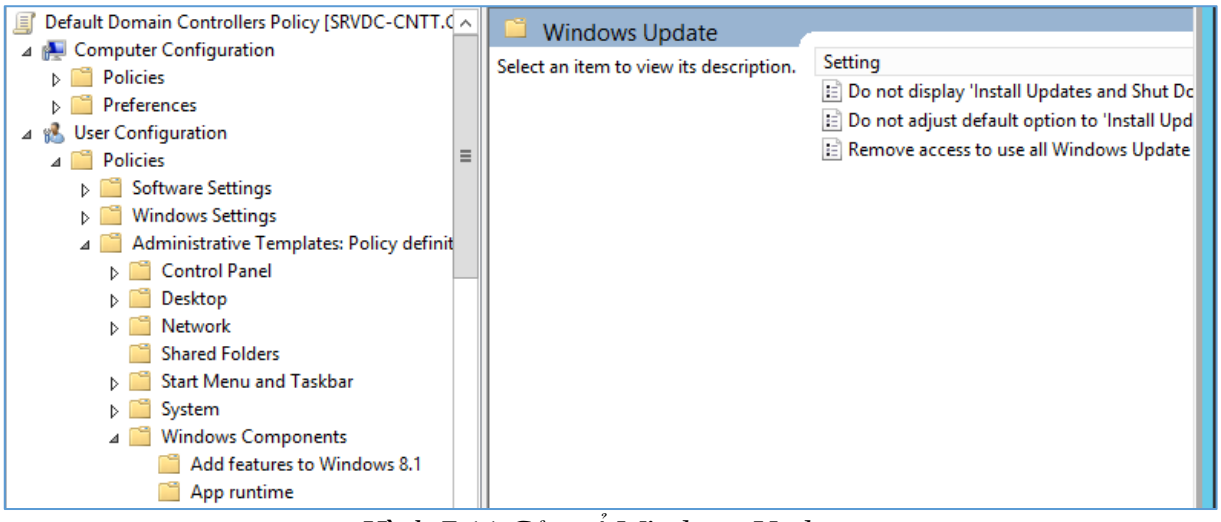
+ **Prevent access to drivers from My Computer**. Ngăn truy cập các ổ đĩa.

+ **Remove Hardware tab**. Ẩn tab Hardware.

+ **Remove DFS tab**. Ẩn tab DFS.

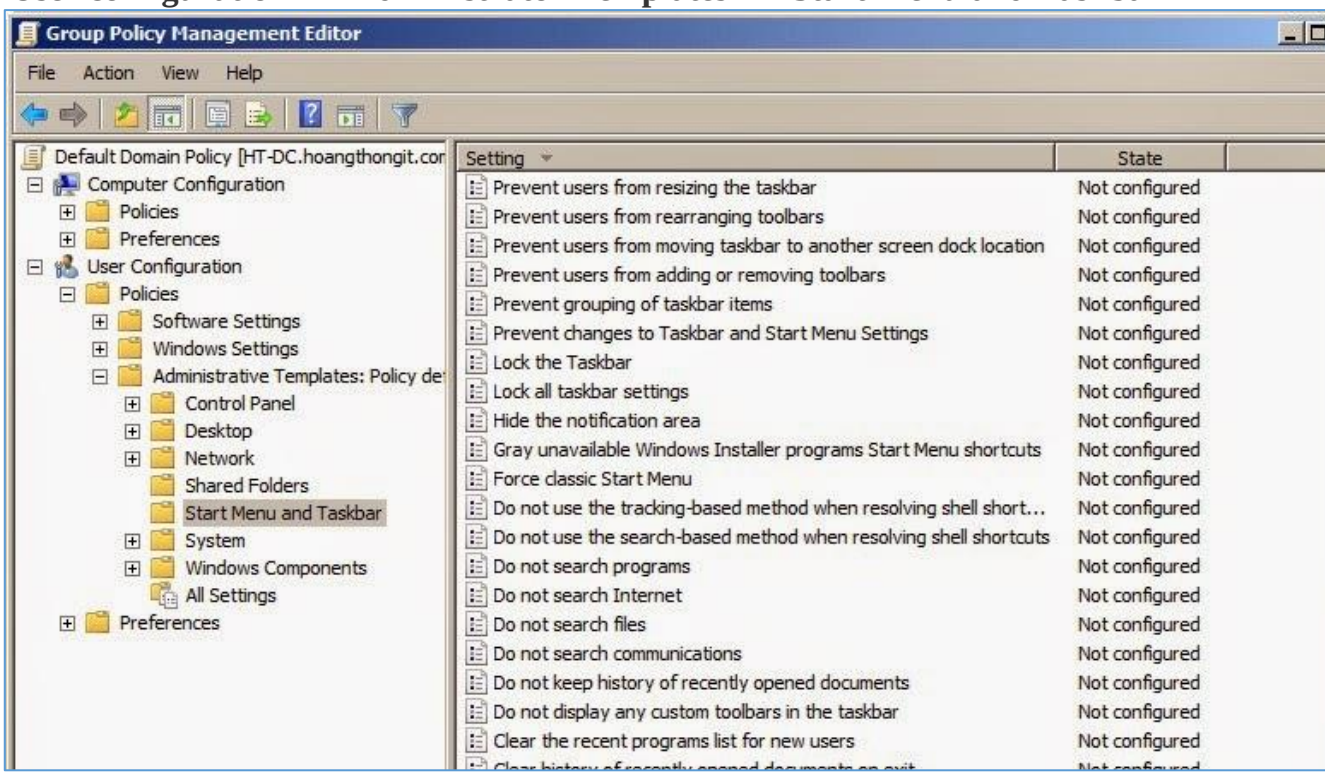
+ **Remove Security tab.** Ẩn tab Security.

- User configuration – > Administrator Templates – > Windows Components – > Windows Update



Hình 7.11 Cửa sổ Windows Update

User configuration – > Administrator Templates – > Start Menu and Taskbar



Hình 7.11 Cửa sổ Start Menu and Taskbar

+ **Remove Logff on the Start Menu.** Ẩn Logff ở Start Menu.

+ **Remove and prevent access to the Shut Down command.** Ẩn Shut Down.

+ **Remove Drag-and-drop context menus on the Start Menu.** Cấm Drag Drop (kéo thả)

+ **Prevent changes to Taskbar and Start Menu Settings.** Không thay đổi các thuộc tính đã thiết lập.

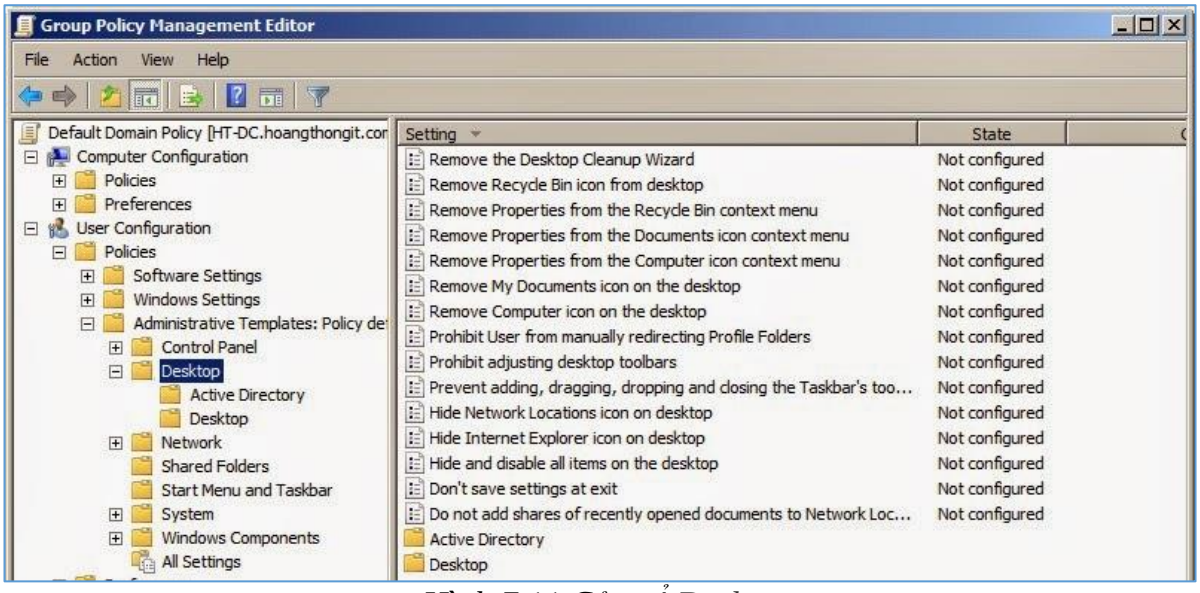
+ **Clear history of recently opened documents on exit.** Không lưu tập tin trong My Document.

+ **Lock the Taskbar**. Khóa Taskbar.

+ **Remove user name from Start Menu**. Không hiển thị tên trên Start Menu.

+ **Do not display any custom toolbars in the taskbar**. Ẩn toolbars.

User configuration – > Administrator Templates – > Desktop



Hình 7.11 Cửa sổ Desktop

+ **Hide and disbale all items on the desktop.** Ẩn biểu tượng trên Desktop.

+ **Remove My Documents icon on the desktop**. Ẩn icon My Documents trên desktop.

+ **Remove My Computer icon on the desktop.** Ẩn icon My Computer trên desktop.

+ **Remove Recycle Bin icon on the desktop**. Ẩn icon Recycle Bin trên desktop.

+ **Don't save settings at exit**. Không thay đổi thiết lập sau khi tắt máy.

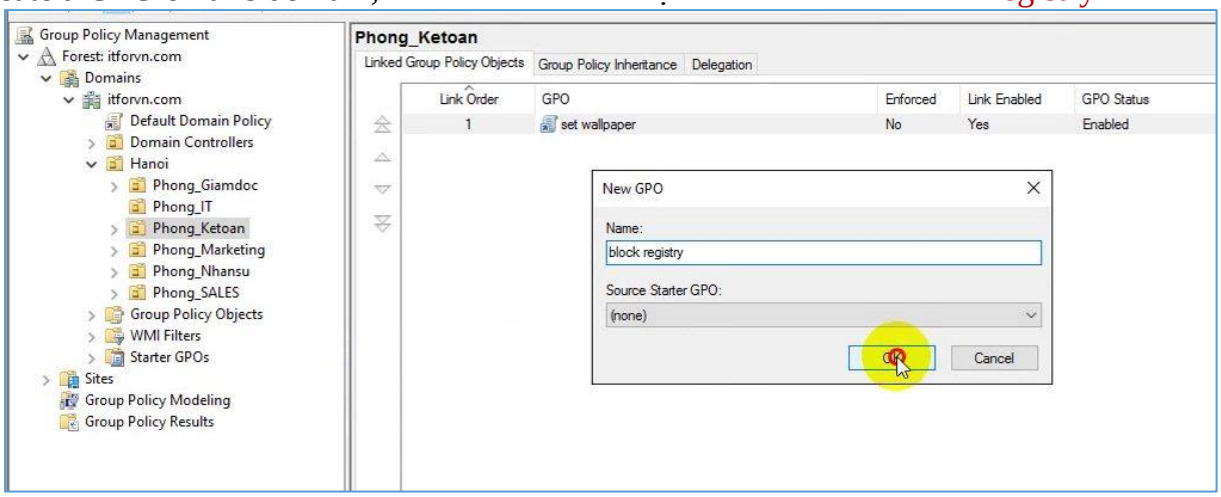
Bài tập thực hành của học viên

1. Khóa Registry trên nhóm KETOAN (không cho người dùng có thể truy cập và can thiệp sửa xóa vào hệ thống gây lỗi Win)
2. Khóa Task Manager NHANSU.
3. Khóa command Prompt trên phòng KINHDOANH

Hướng dẫn trả lời:

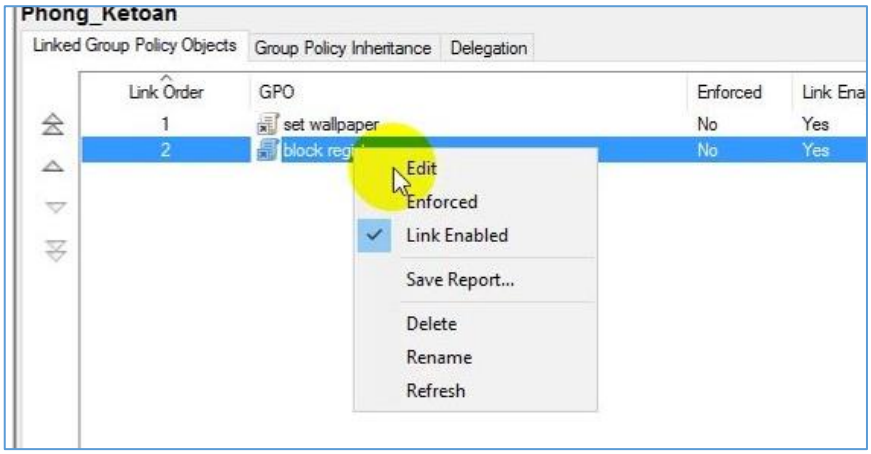
1. Khóa Registry trên nhóm KETOAN**.**

Mở Group Policy Management lên chọn OU Phong_Ke_toan, click chuột phải chọn Create a GPO on this domain, and link it here và tạo 1 GPO tên là Block Registry



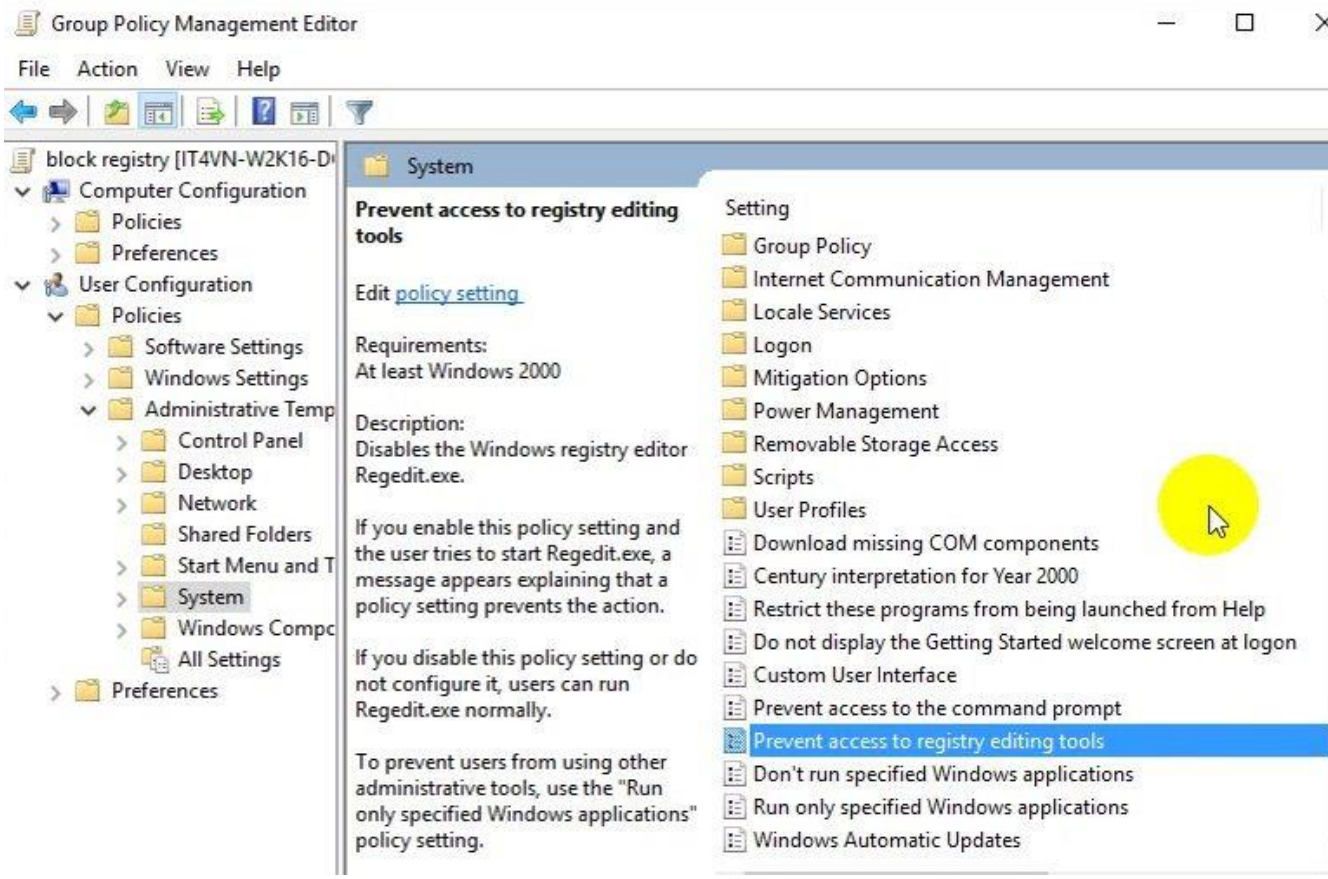
Hình 7.12 Tạo GPO cho Ketoan

Click vào GPO ta vừa tạo click chuột phải chọn Edit



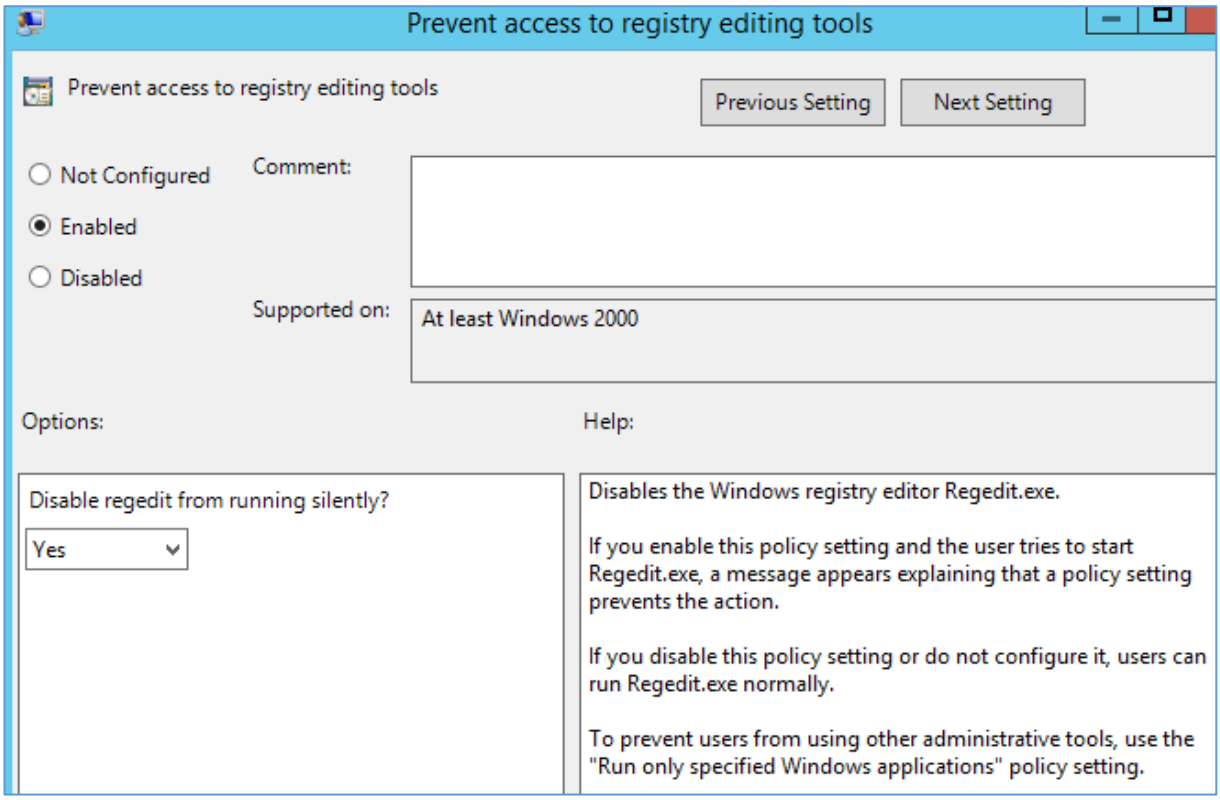
Hình 7.13 Hiệu chỉnh GPO

Chọn User Configuration / Policies / Administrative Template: … / System / Prevent access to registry editing tools



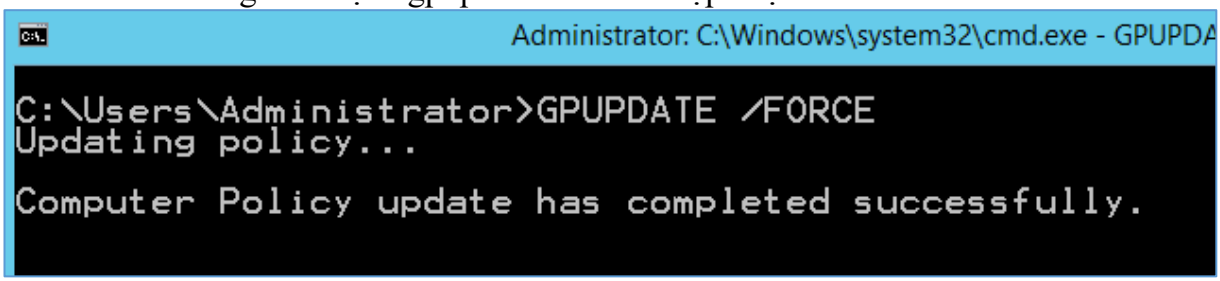
Hình 7.14 Mở registry

Click đúp vào Prevent access to registry editing tools chọn Enabled và Apply, OK



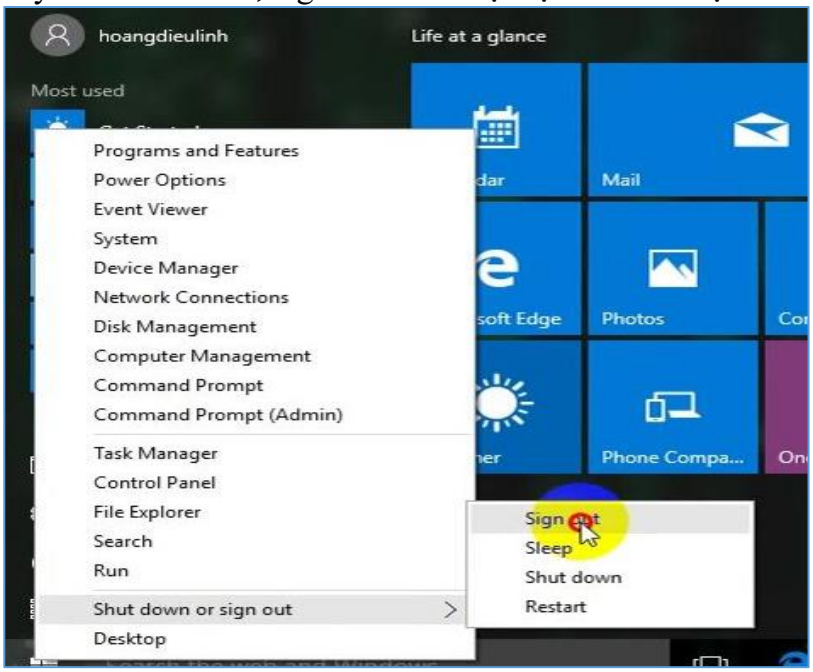
Hình 7.15 Bật Enabled cho registry

Mở CMD lên và gõ câu lệnh gpupdate /force để cập nhật chính sách cho Clients



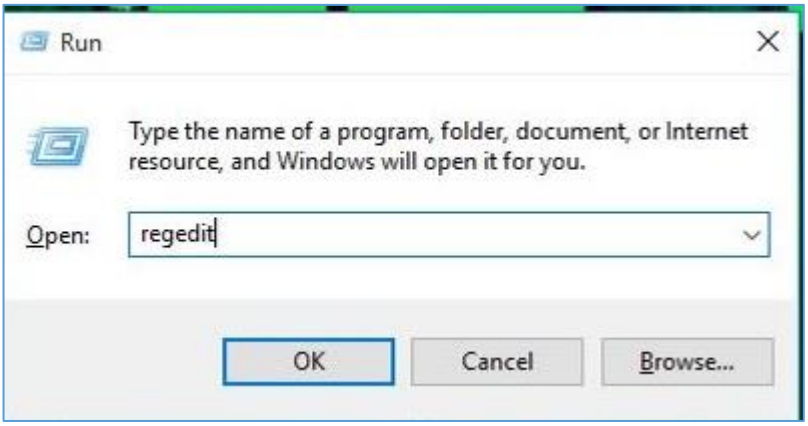
Hình 7.16 Update cho GPO

Chuyển sang máy Win 10 Client, sign out user hiện tại và lon in lại



Hình 7.17 Cửa sổ sign out user

Ấn tổ hợp phím Windows + R gõ regedit để truy cập nhanh vào Registry nhưng ta thấy rằng nó đã bị khóa. Như vậy ta đã cấm người dùng truy cập vào Registry để chỉnh sửa,… thành công.

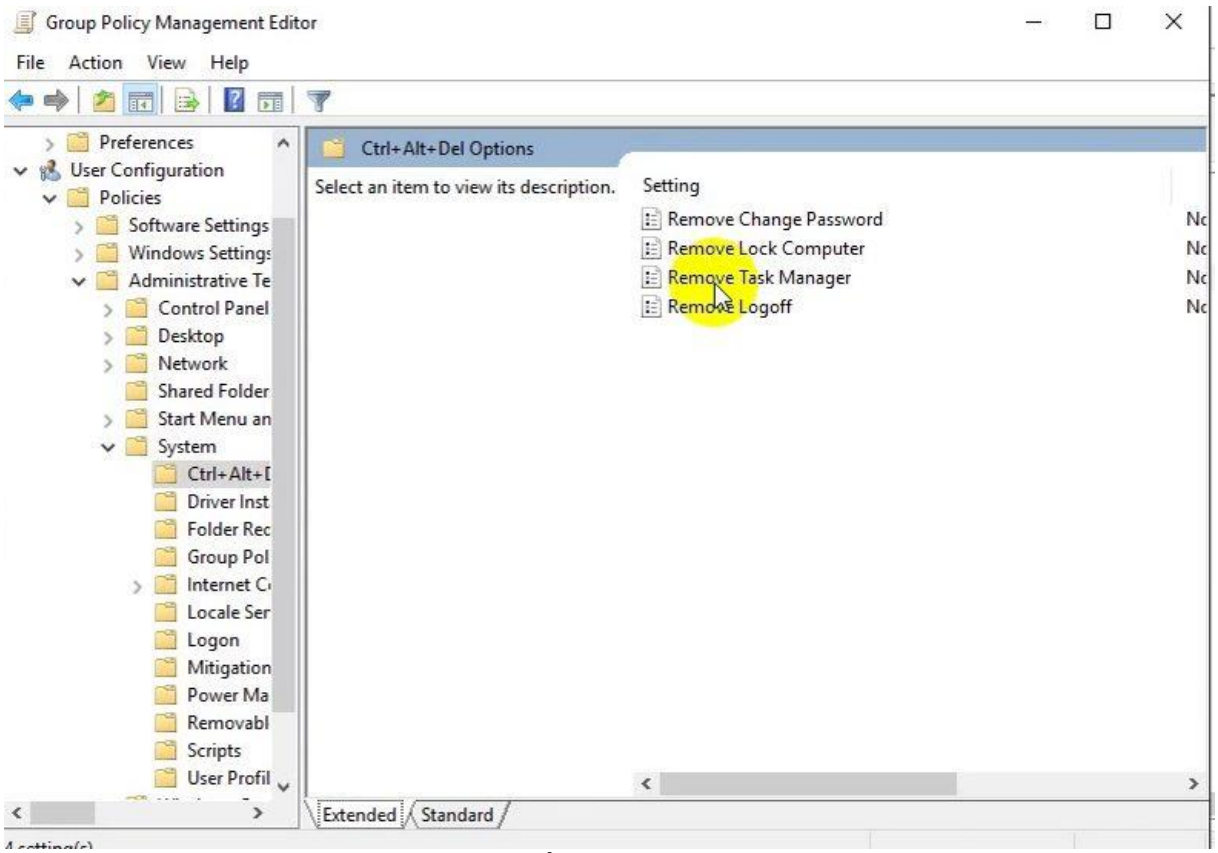


Hình 7.18 Cửa sổ gõ lệnh

Hình 7.18 Cửa sổ báo lỗi truy cập Registry

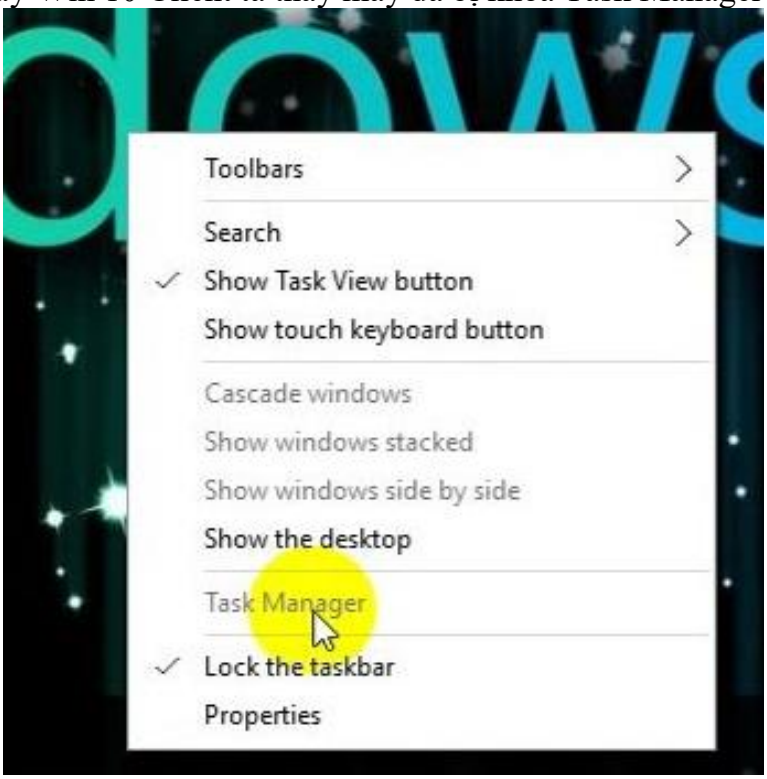
2. Khóa Task Manager NHANSU.

Mở GPO, Right click vào phòng NHANSU, User Cofiguration, Administrative temp, System, Ctrl+Alt+Del



Hình 7.19 cấu hình Task Manager

Chuyển sang máy Win 10 Client ta thấy máy đã bị khóa Task Manager

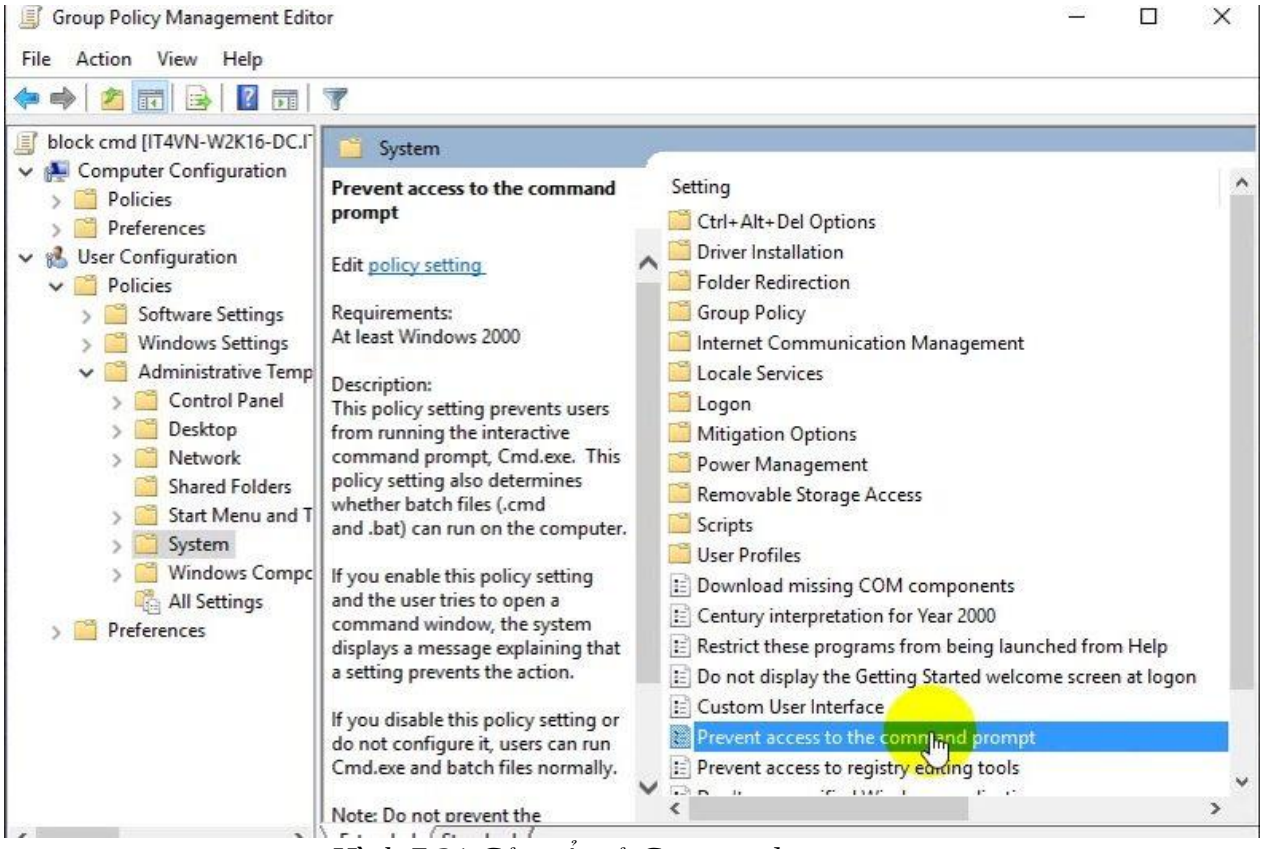


Hình 7.20 Task Manager bị khóa

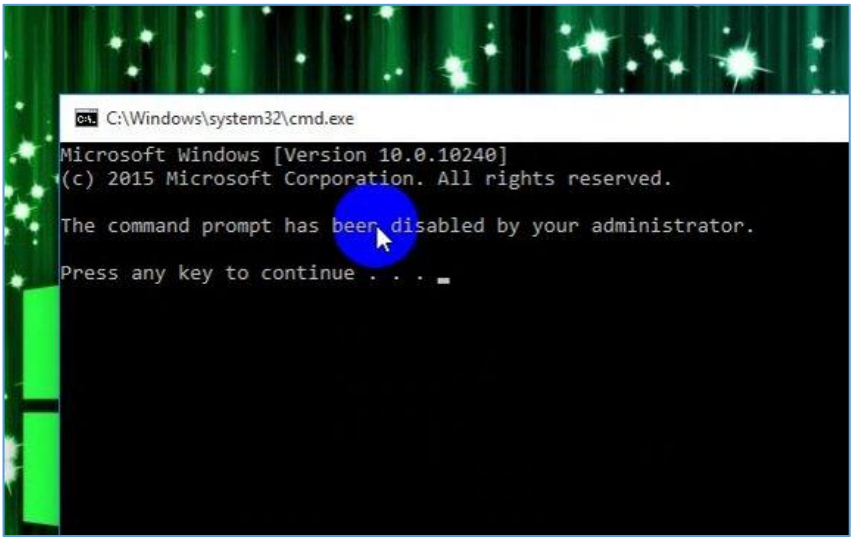
3. Khóa command Prompt trên phòng KINHDOANH

Tạo 1 Group Policy cho Phong_ke_toan là block cmd, chọn Edit, chọn User Configuration / Policies / Administrative Templates: … / Systems / Prevent Access to the command prompt

Click chuột phải vào Prevent access to the command prompt chọn Enabled, Apply OK



Hình 7.21 Cửa sổ mở Command prompt



Hình 7.22 Command prompt bị khóa

Những trọng tâm cần chú ý:

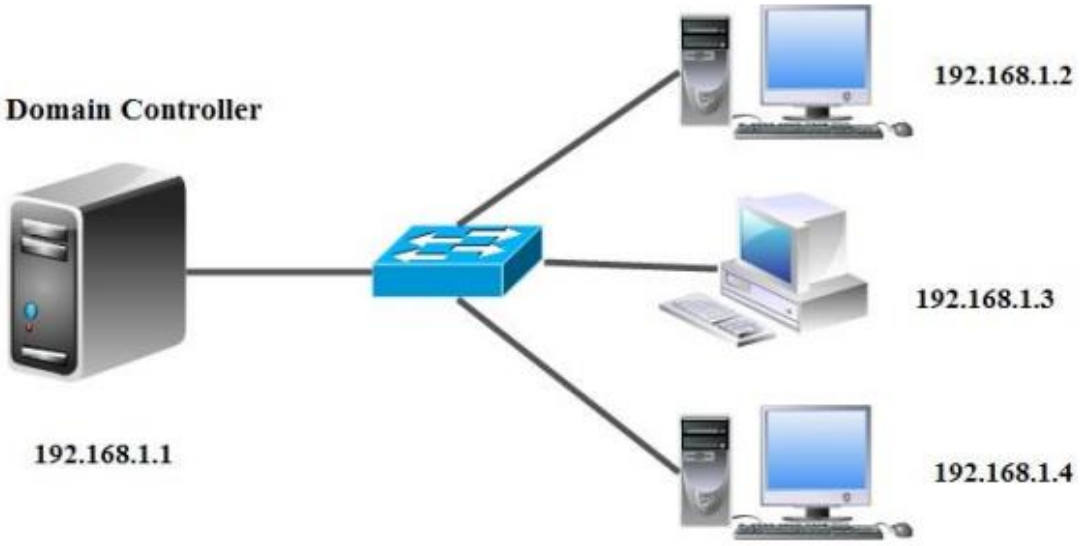
- Tạo các phòng ban để thiết lập chính sách đúng yêu cầu.
- Tạo các OU, Group và User theo phòng ban
- Thiết lập chính sách bảo mật cho đúng các bước
- Máy Client đảm bảo truy cập vào hệ thống để test.
- Khi chúng ta cho phép user lưu trữ dữ liệu trên file server phải đúng dung lượng.
- Tắt tường lửa cho máy DC và Client trên hệ thống.

- Thao tác phải đúng các bước cấp phép chính sách cho hệ thống.

Bài mở rộng và nâng cao

Tình huống: Chia sẻ và phân quyền các folder cho các user trong hệ thống với những chức năng mở rộng của NTFS

Mô hình



Yêu cầu:

Phòng KETOAN

+Ẩn icon trên màn hình Desktop

+ Ẩn item trong control panel

Phòng NHANSU

+ Cấm đổi theme

+ Không cho sửa địa chỉ IP

+ Khóa start menu and taskbar

Phòng KINHDOANH

+ Không cho sử dụng ứng dụng

+ Hiển thị câu chào khi đăng nhập

+ Khóa control panel

Map ổ đĩa bằng Group Policy Object cho các phòng ban: **KETOAN-> K (dung lượng 30GB); NHANSU -> N (**dung lượng **10GB); KINHDOANH -> H (**dung lượng **20GB);**

Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được Chức năng Chia sẻ, cấu hình, quản lý thư mục dùng chung trên Windows Server 2019
  + Trình bày được Chức năng DFS và Quyền truy cập NTFS trên Windows Server 2019
- Về kỹ năng:
  + Thao tác thành thạo việc Chia sẻ, cấu hình, quản lý thư mục dùng chung trên hệ thống.

    + Thao tác thành thạo việc cấp phát, thu hồi Quyền truy cập NTFS trong cục bộ hoặc Domain trên Windows Server 2019
    + Thực hiện đúng yêu cầu Tài khoản NS1 không xóa folder mà NS2 tạo và Lấy quyền lại cho admin khi bị NS2 xóa bỏ.
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng:
    + Đánh giá kỹ năng thực hành về việc Chia sẻ, cấu hình, quản lý thư mục dùng chung trên hệ thống.
    + Đánh giá kỹ năng thực hành về cấp phát, thu hồi Quyền truy cập NTFS trong cục bộ hoặc Domain trên Windows Server 2019.
    + Đánh giá kỹ năng thực hành về yêu cầu Tài khoản NS1 không xóa folder mà NS2 tạo và Lấy quyền lại cho admin khi bị NS2 xóa bỏ
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 8: CÀI ĐẶT VÀ QUẢN TRỊ DỊCH VỤ DHCP
Mã bài: MĐ 17 - 08

Mục tiêu:
- Mô tả được sự hoạt động của dịch vụ DHCP;
- Cài đặt và cấu hình được dịch vụ DHCP.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Giới thiệu dich vụ DHCP

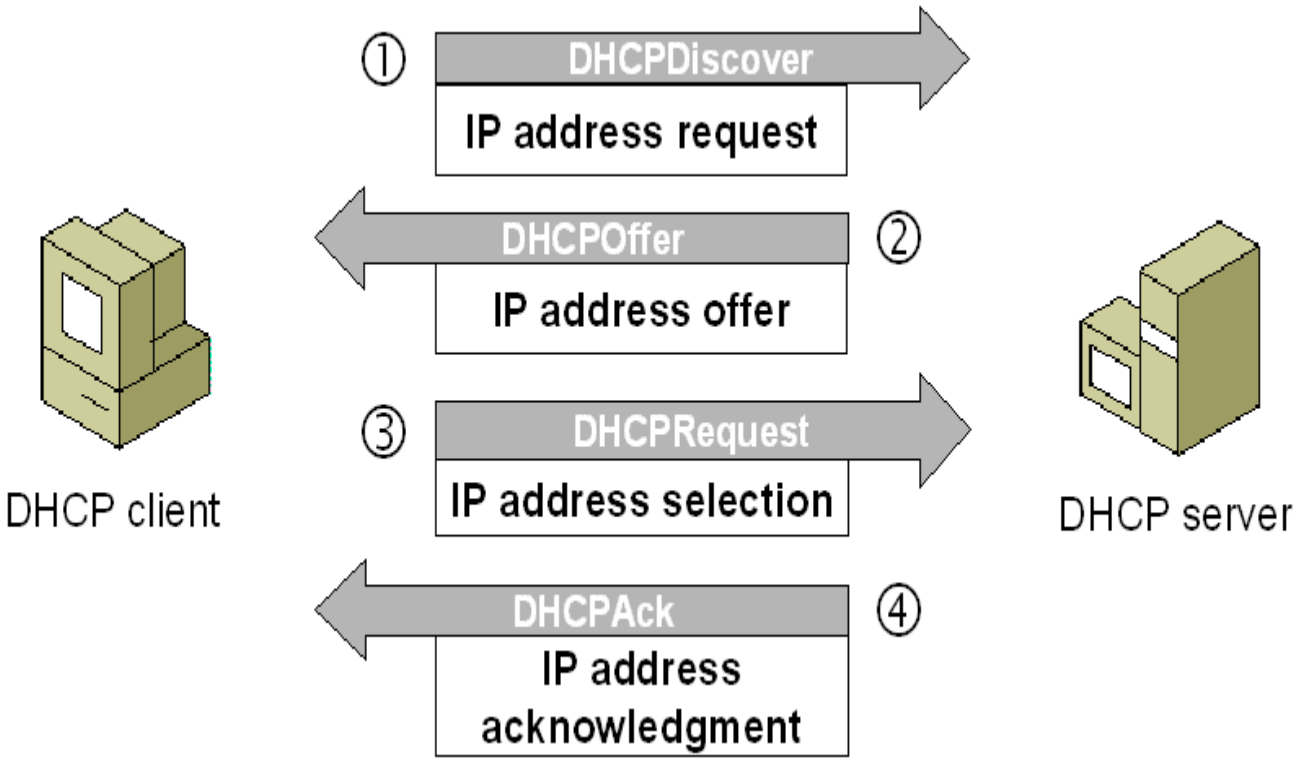
Mục tiêu:

- Trình bày được khái niệm DHCP.
- Cài đặt được dịch vụ DHCP.
- Cấu hình được máy phục vụ DHCP.

- **DHCP** là viết tắt của **Dynamic Host Configuration Protocol**, là giao thức Cấu hình Host Động được thiết kế làm giảm thời gian chỉnh cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho khách hàng khi họ vào mạng. Dich vụ DHCP là một thuận lợi rất lớn đối với người điều hành mạng. Nó làm yên tâm về các vấn đề cố hữu phát sinh khi phải khai báo cấu hình thủ công.

- DHCP server là một máy chủ có cài đặt dịch vụ DHCP. Nó có chức năng quản lý sự cấp phát địa chỉ IP động và các dữ liệu cấu hình TCP/IP. Ngoài ra còn có nhiệm vụ trả lời khi DHCP Client có yêu cầu về hợp đồng thuê bao.

- DHCP client là dịch vụ có sẵn trên các máy trạm. Nó dùng để đăng ký, cập nhật thông tin về địa chỉ IP và các bản ghi DNS cho chính máy trạm đó. DHCP client sẽ gửi yêu cầu đến DHCP server khi nó cần đến 1 địa chỉ IP và các tham số TCP/IP cần thiết để làm việc trong mạng nội bộ và trên Internet.



Hình 8.1 Sơ đồ nguyên lí hoạt động của DHCP

2. Hoạt động của giao thức

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. Ưu điểm của DHCP:

– Quản lý TCP/IP tập trung

Thay vì phải quản lý địa chỉ IP và các tham số TCP/IP khác vào một cuốn sổ nào đó (đây là việc mà quản trị mạng phải làm khi cấu hình TCP/IP bằng tay) thì DHCP server sẽ quản lý tập trung trên giao diện của nó. Giúp các nhà quản trị vừa dễ quản lý, cấu hình, khắc phục khi có lỗi xảy ra trên các máy trạm.

– Giảm gánh nặng cho các nhà quản trị hệ thống

Thứ nhất, trước đây các nhà quản trị mạng thường phải đánh cấu hình IP bằng tay (gọi là IP tĩnh) nhưng nay nhờ có DHCP server nó sẽ cấp IP một cách tự động cho các máy trạm. Nhất là trong môi trường mạng lớn thì sự cần thiết và hữu ích của dịch vụ mạng này mới thấy rõ ràng nhất.

Thứ hai, trước đây với kiểu cấu hình bằng tay thì người dùng họ có thể thay đổi IP. Anh thì táy máy thích vọc chơi, có anh thay đổi lung tung DNS server sau đó quên không nhớ IP của DNS server là gì để đặt lại cho đúng lại ới quản trị mạng, có anh đặt IP làm trùng với IP của người khác, anh khác đặt IP trùng với Defaul Gateway … làm cho quản trị mạng khốn khổ vì phải chạy. Nhưng kiểu này không có ở IP động đâu nhé.

Anh nào thích thay đổi cũng chịu chết. Chỉ có người quản trị DHCP server họ mới có quyền thích làm gì thì làm thôi.

– Giúp hệ thống mạng luôn được duy trì ổn định

Điều đó hiển nhiên rồi. Địa chỉ IP cấp phát động cho các máy trạm lấy từ dải IP cấu hình sẵn trên DHCP server. Các tham số (DG, DNS server …) cũng cấp cho tất cả các máy trạm là chính xác. Sự trùng lặp IP không bao giờ xảy ra. Các máy trạm luôn luôn có một cấu hình TCP/IP chuẩn. Làm cho hệ thống hoạt động liên tục, vừa giảm gánh nặng cho người quản trị vừa tăng hiệu quả làm việc cho user nói riêng và doanh nghiệp nói chung.

– Linh hoạt và khả năng mở rộng

Người quản trị có thể thay đổi cấu hình IP một cách dễ dàng khi cơ sở hạ tầng mạng thay đổi. Do đó làm tăng sự linh hoạt cho người quản trị mạng. Ngoài ra DHCP phù hợp từ mạng nhỏ đến mạng lớn. Nó có thể phục vụ 10 máy khách cho đến hàng ngàn máy khách.

So sánh việc cấu hình TCP/IP "thủ công"(manual) và bằng DHCP (tự động)

Cấu hình TCP/IP cho "thủ công":

Khi bạn cấu hình TCP/IP cho các client, bạn phải gán cho nó một địa chỉ IP, điều này sẽ hay dẫn đến việc bạn nhập vào sai IP, và việc này dẫn đến việc tìm ra lỗi sẽ khó khăn hơn. Và vấn đề thường xuyên nảy sinh là sẽ bị duplicate IP (trùng địa chỉ). Hơn nữa, công việc của người Admin sẽ nhiều hơn (admin còn nhiều việc khó hơn phải làm… ví dụ khi bạn cấp IP cho 200 máy thì bạn phải đến từng máy một mà cấp cho nó IP, subnet mask, defaut gateway…, và khi dời đoạn mạng này sang đoạn mạng khác thì bạn phải cấu hình TCP/IP lại).

Khi dùng DHCP:

DHCP server tự động cấp tấc cả thông tin cấu hình cần thiết cho DHCP client. Điều đó có nghĩa là các client sử dụng cấu hình thông tin chính xác, tránh được các lỗi thường gặp khi cấu hình bằng tay như trên. Và nó cũng tự động cập nhật thông tin để cập nhật sự thay đổi cấu trúc mạng mà không cần phải cấu hình lại địa chỉ IP của client.(Nguồn: http://tinsp211.forums-free.com/)

4. Các thuật ngữ dùng trong DHCP:

– DHCP Server: máy quản lý việc cấu hình và cấp phát địa chỉ IP cho Client

– DHCP Client: máy trạm nhận thông tin cấu hình IP từ DHCP Server

– Scope: phạm vi liên tiếp của các địa chỉ IP có thể cho một mạng.

– Exclusion Scope: là dải địa chỉ nằm trong Scope không được cấp phát động cho Clients.

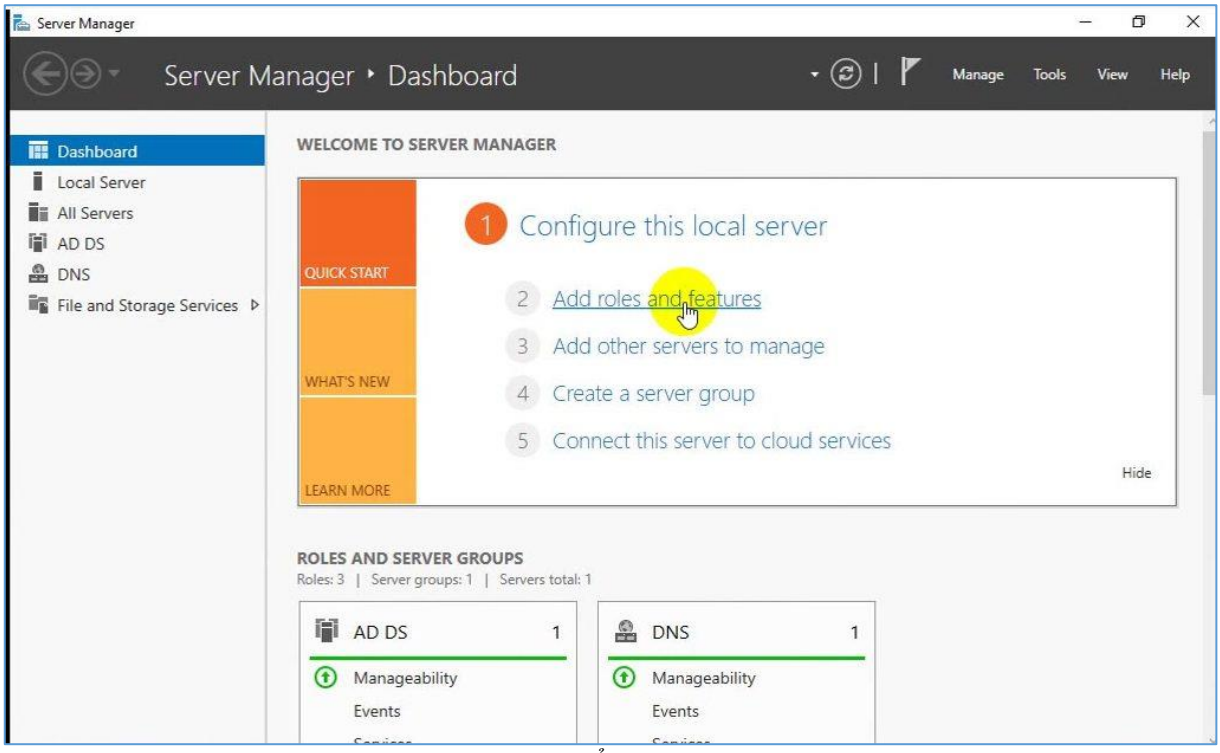
– Reservation: Địa chỉ đặt trước dành riêng cho máy tính hoặc thiết bị chạy các dịch vụ (tùy chọn này thường được thiết lập để cấp phát địa chỉ cho các Server, Printer,…..)

– Scope Options: các thông số được cấu hình thêm khi cấp phát IP động cho Clients như DNS Server(006), Router(003)

5. Cài đặt và cấu hình DHCP

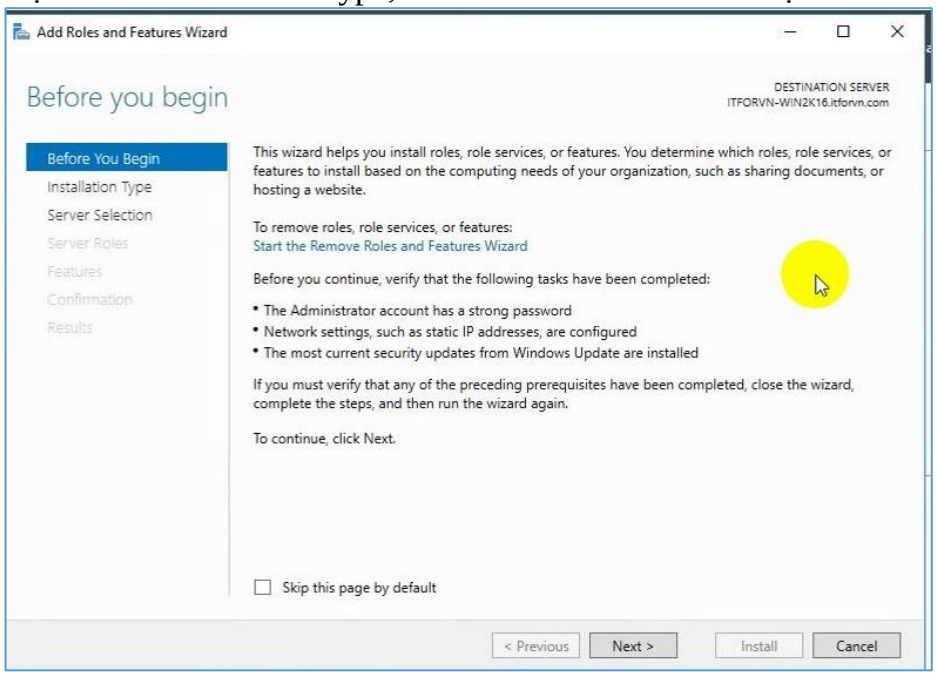
5.1 Các bước cài đặt DHCP

Bước 1: Vào Server Manager chọn Add roles and features



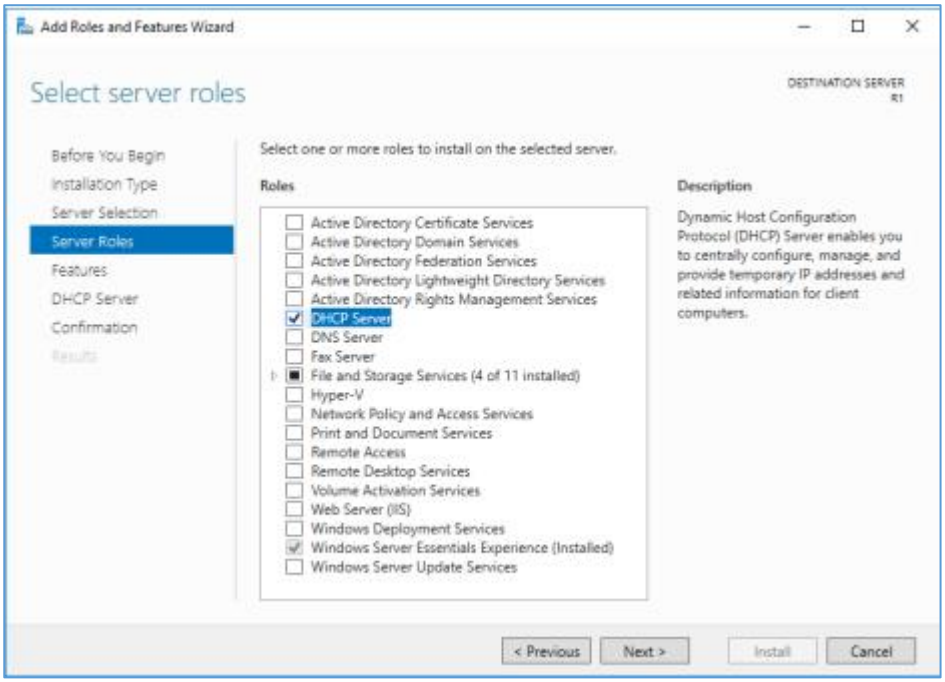
Hình 8.2 Cửa sổ Server Manager

Bước 2: Chọn Select installation type, select destination server chọn next



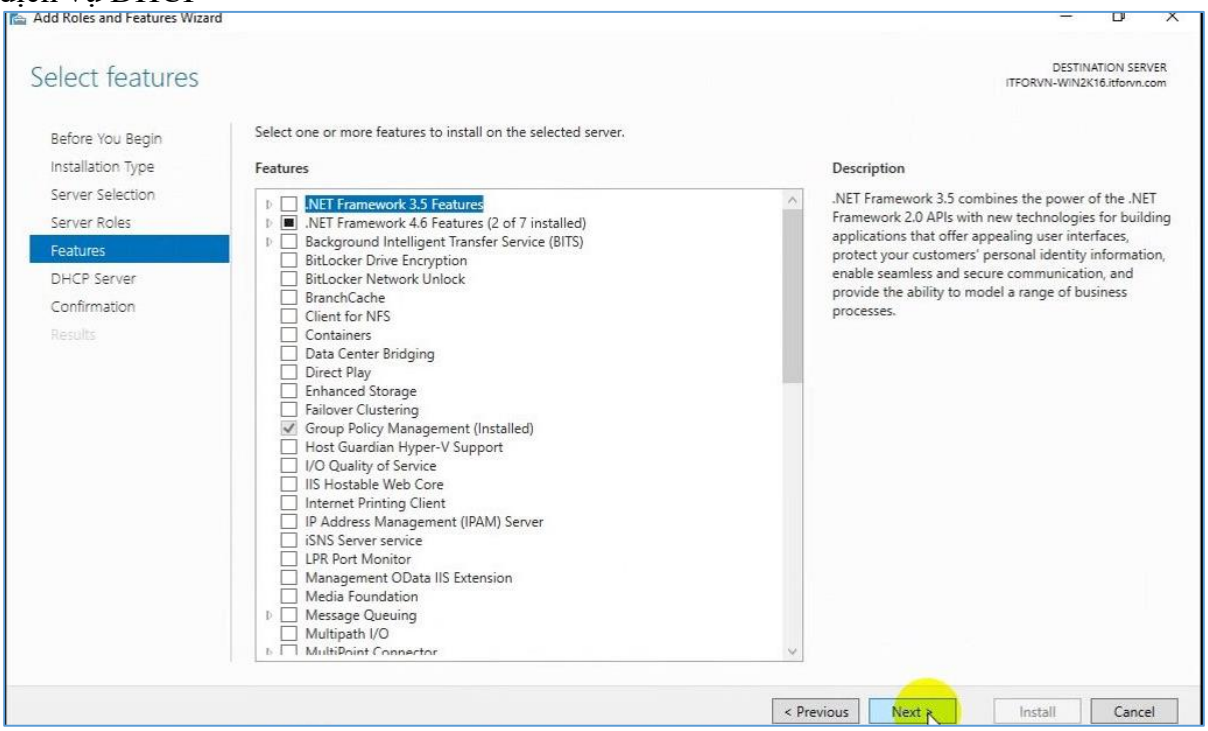
Hình 8.3 Cửa sổ Before you begin

Bước 3: Ở mục Select server role chọn DHCP server và ấn next và Add features



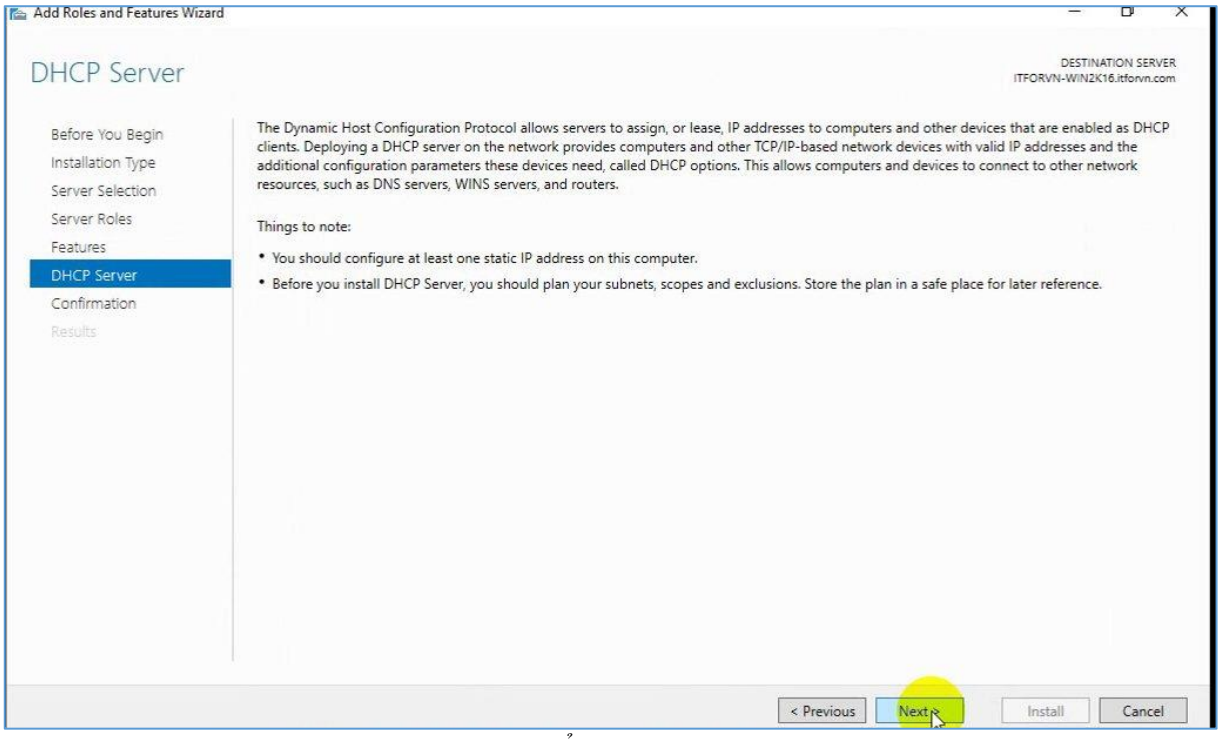
Hình 8.4 Cửa sổ chọn dịch vụ

Bước 4: Ở các mục còn lại các bạn ấn next liên tục và chọn Install để tiến hành cài đặt dịch vụ DHCP



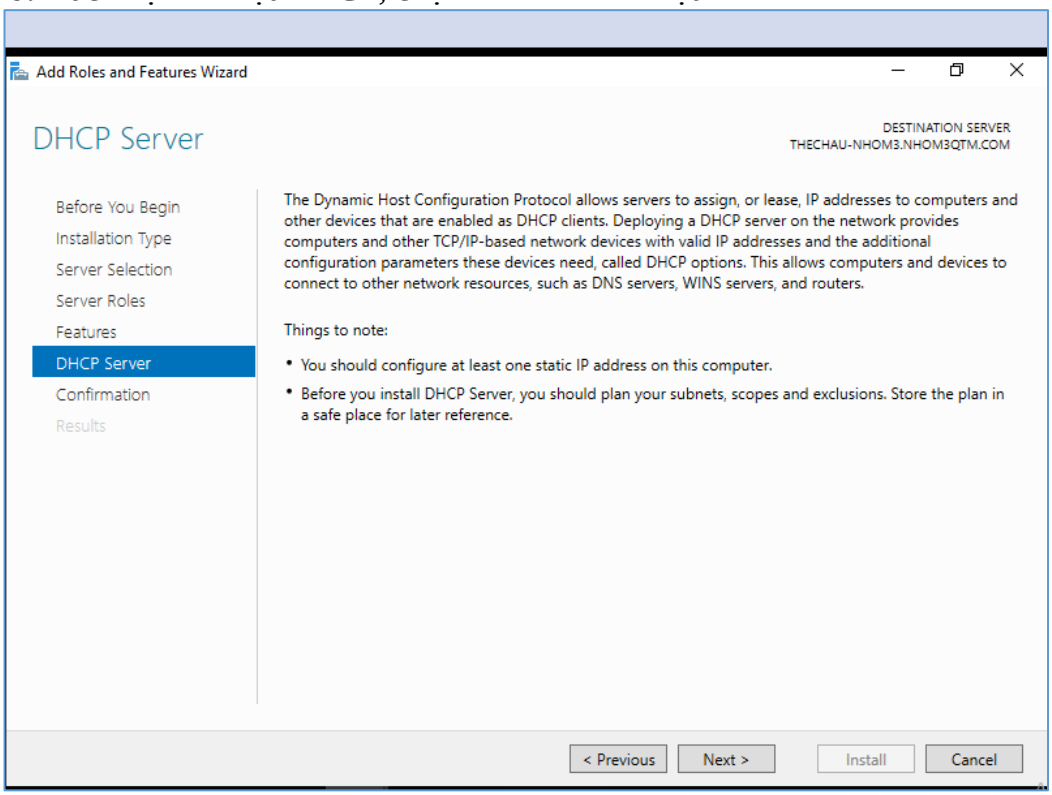
Hình 8.5 Cửa sổ chọn lựa cho hệ thống

Bước 5: Chọn Next tiếp tục cài đặt DHCP



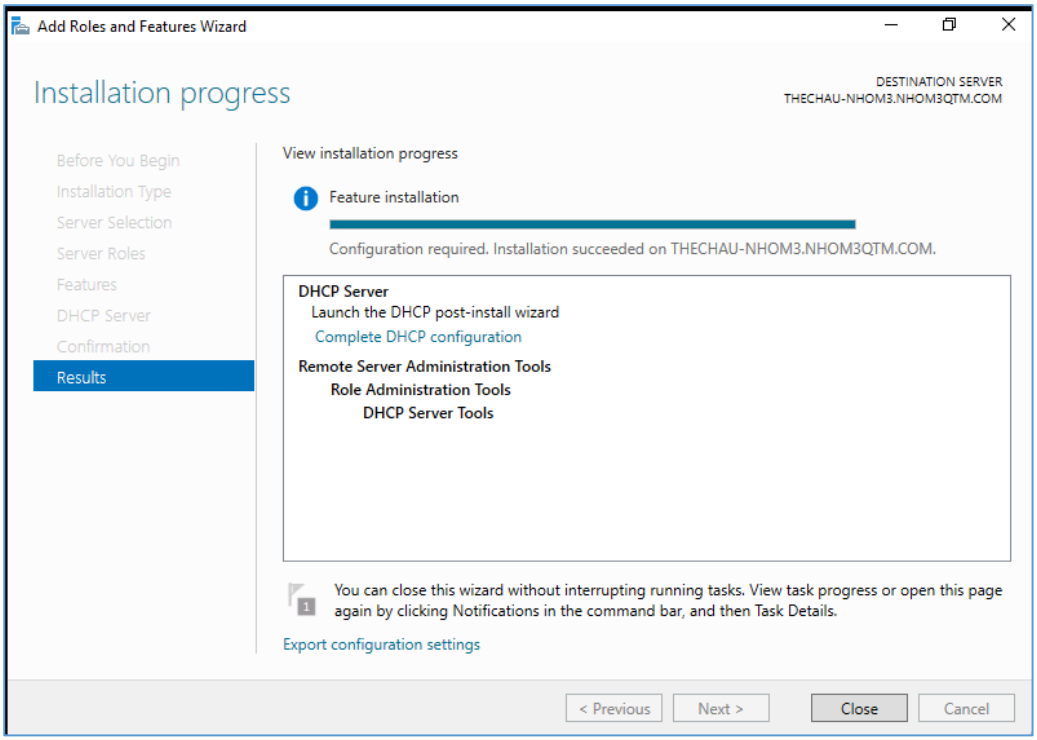
Hình 8.6 Cửa sổ chú thích cho DHCP

Bước 6: Xác nhận cài đặt DHCP, chọn Install để cài đặt



Hình 8.7 Cửa sổ xác nhận cài đặt

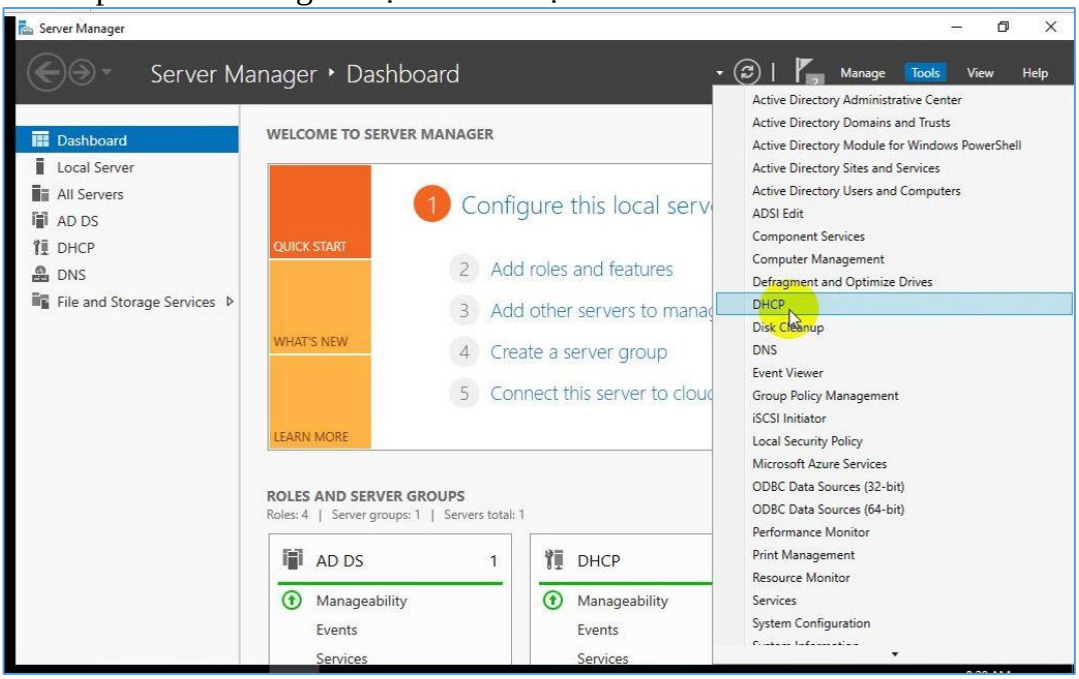
Bước 7: Nhấp vào Close để đóng quá trình cài đặt



Hình 8.8 Cửa sổ hoàn thành cà đặt

5.2. Cấu hình dịch vụ DHCP

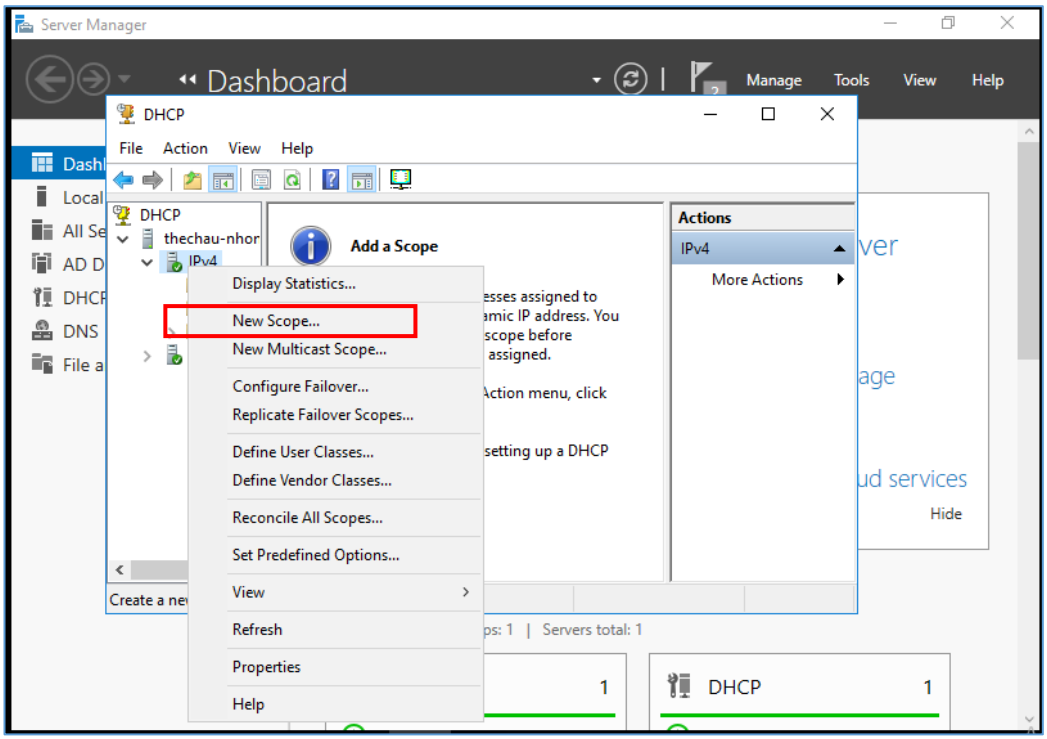
Bước 1 - Nhấp Server manager chọn Tools chọn DHCP để cấu hình



Hình 8.9 Cửa sổ mở DHCP để cấu hình

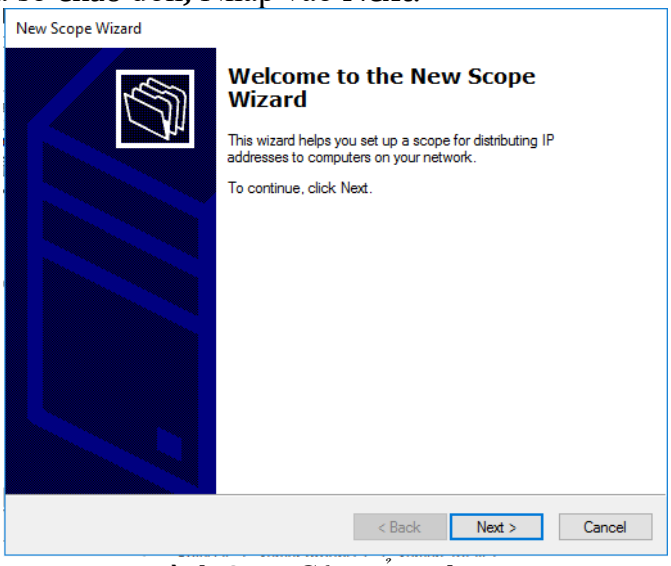
Bước 2: Tạo **Scope**

Nhấp chuột phải vào **IPv4** → Chọn "**New Scope**".



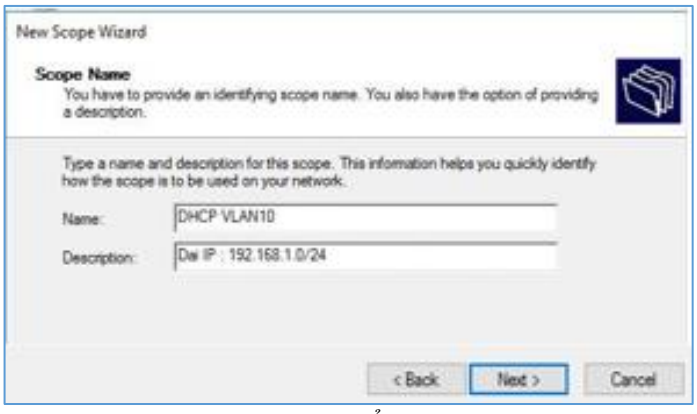
Hình 8.10 Cửa sổ New Scope

Bước 3: Cửa sổ chào đón**,** Nhấp vào **Next**.



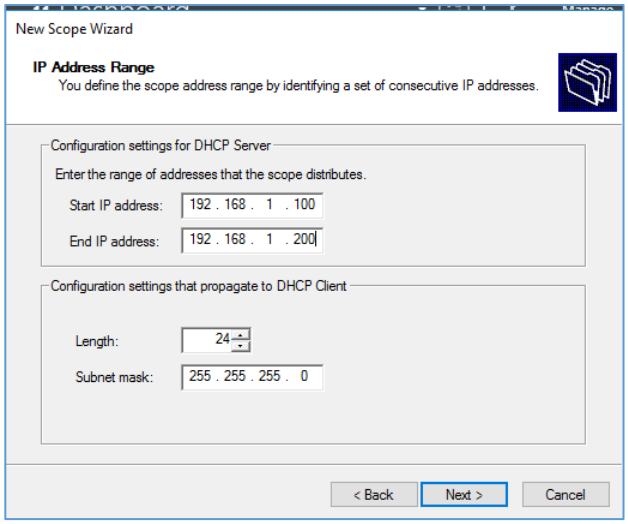
Hình 8.11 Cửa sổ Welcome

Bước 4: Nhập **Scope Name** và mô tả như được hiển thị trong ảnh chụp màn hình sau và sau đó chọn **Next**.



Hình 8.12 Cửa sổ Scope Name

Bước 5: Nhập địa chỉ **IP Start** và **End**, **Subnet mask**, để **Length** mặc định "**24**" cho mạng con lớp C → bấm **Next**.

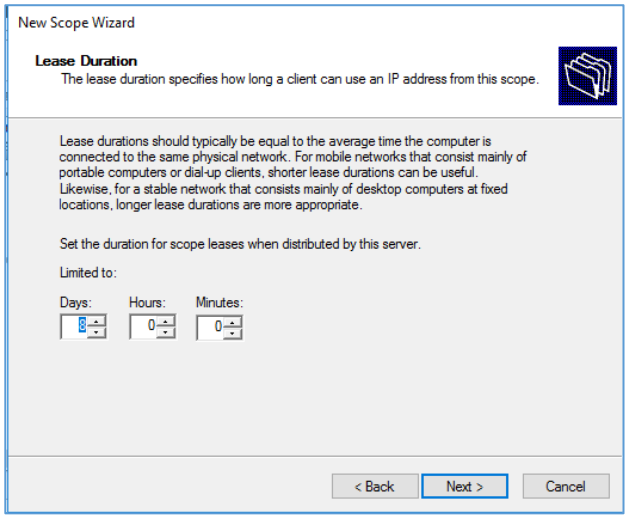


Hình 8.13 Phạm vi IP cho phép

Bước 6: Nhập phạm vi IP của bạn trong danh sách loại trừ. Nếu bạn có thiết bị trên mạng yêu cầu địa chỉ IP tĩnh, hãy đảm bảo rằng phạm vi bị loại trừ thuộc phạm vi **Start** và **End** được chỉ định trước đó → nhấp vào **Next**.

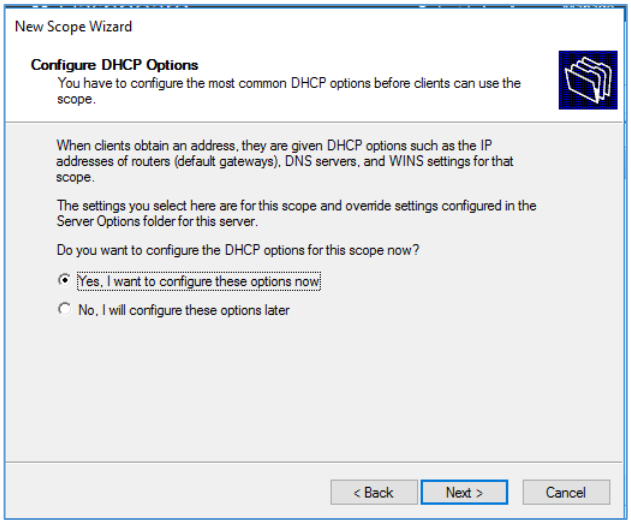
Hình 8.14 Phạm vi IP loại trừ

Bước 7: Nhập thời hạn mong muốn cho IP được chỉ định hoặc để mặc định → sau đó nhấp **Next**.



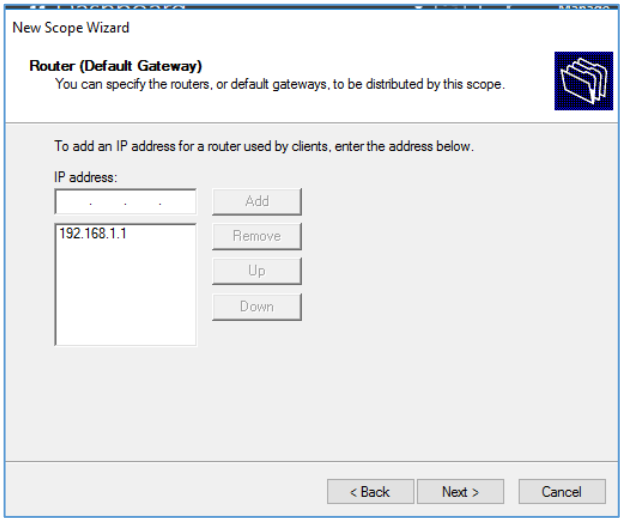
Hình 8.15 thời hạn cấp phát IP

Bước 8: Chọn "**Yes, I want to configure these options now**" → sau đó bấm vào **Next**.



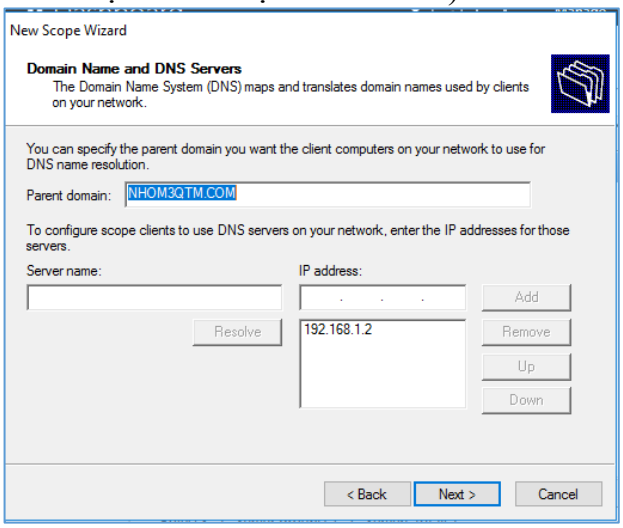
Hình 8.16 Chấp nhận cấu hình

Bước 9: Nhập cổng mặc định là IP Router của bạn → sau đó nhấn **Next**.



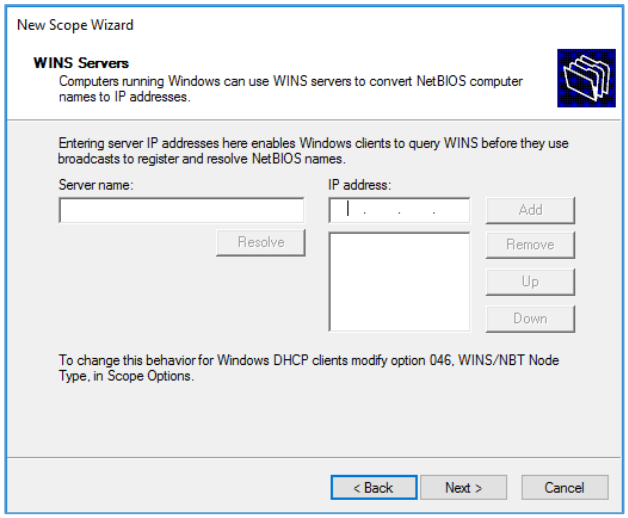
Hình 8.17 Xác định IP Router

Bước 10: Thêm **DNS IP** → nhấn **Next** (chúng ta có thể đặt Google DNS hoặc nếu nó là một môi trường Domain bạn có thể đặt DC IP ở đó) → sau đó nhấn **Next.**



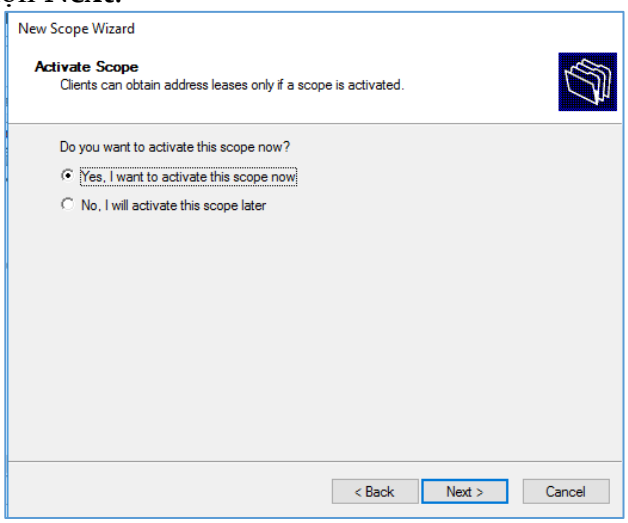
Hình 8.18 Xác nhận IP cho DNS server

Bước 11: Chỉ định **WINS Server** của bạn nếu có → và sau đó nhấp **Next**.



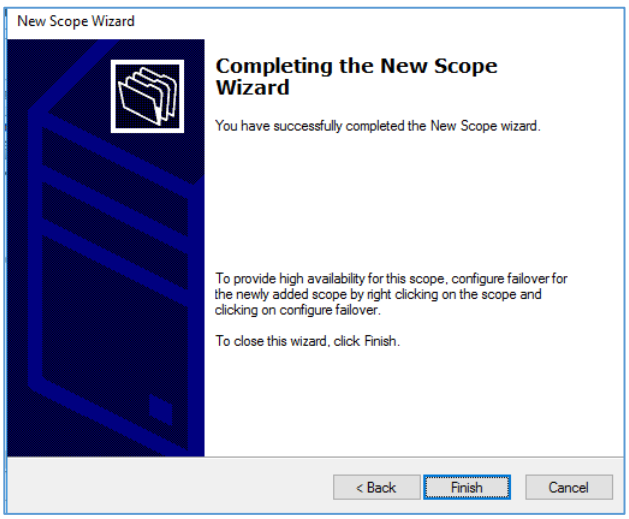
Hình 8.19 Xác nhận IP cho WIN server

Bước 12: Chọn tùy chọn "**Yes, I want to activate this scope now**" để kích hoạt phạm vi ngay lập tức → chọn **Next**.



Hình 8.20 Kích hoạt phạm vi

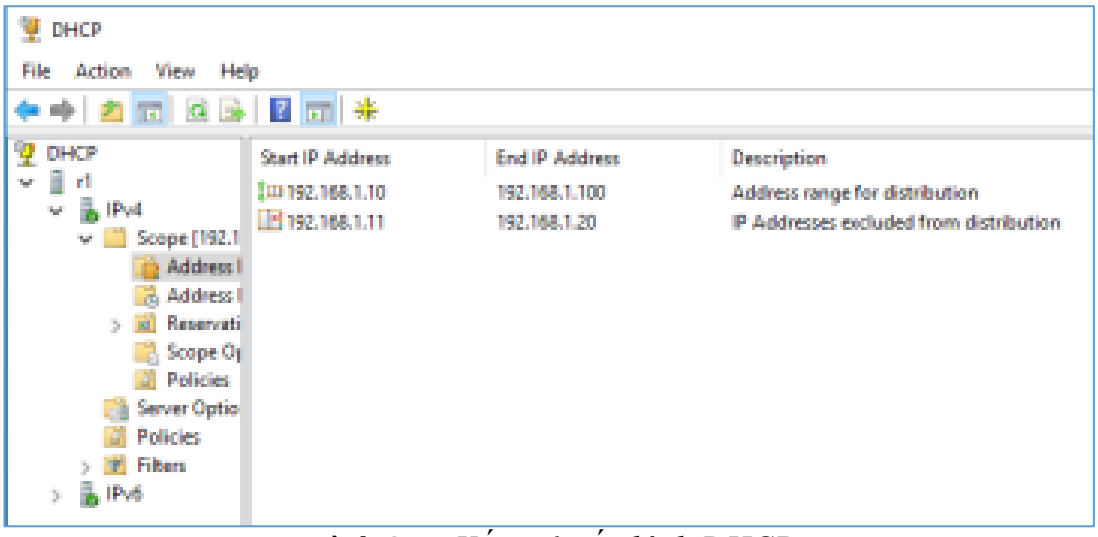
Bước 13: Nhấn **Finish**.



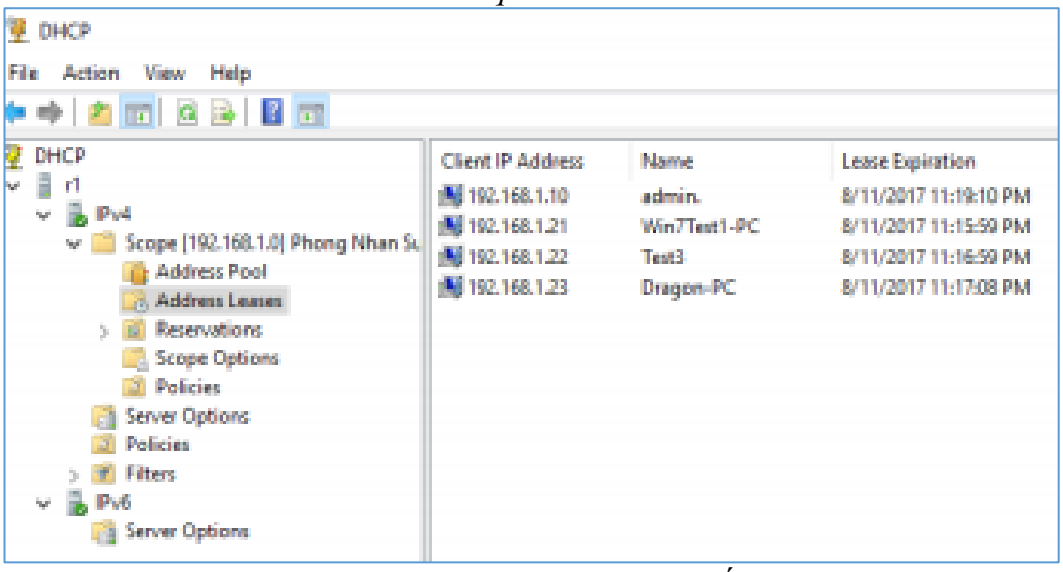
Hình 8.21 Hoàn thành cấu hình DHCP

Bước 14: Kết quả cấu hình

Nhấn refresh lại để được kết quả như trong hình



Hình 8.22 Kết quả cấu hình DHCP

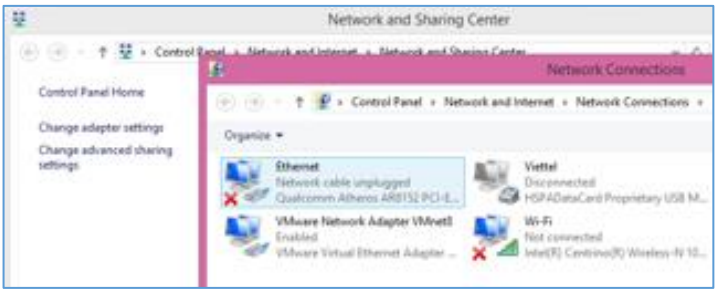


Hình 8.23 Dãy IP bị chặn không cấp phép

5.3. Cấu hình IP động cho máy Client

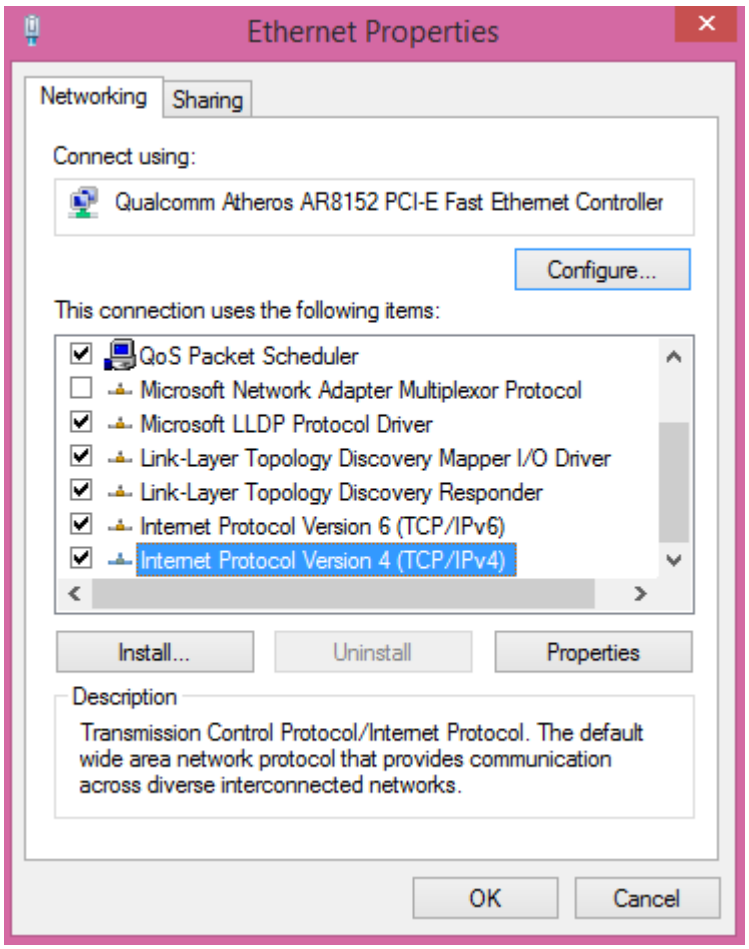
Bước 1: Cấu hình IP động cho Client

Vào **Control Panel \ Network and Internet \ Network and Sharing Center**



Hình 8.24 Mở card mạng

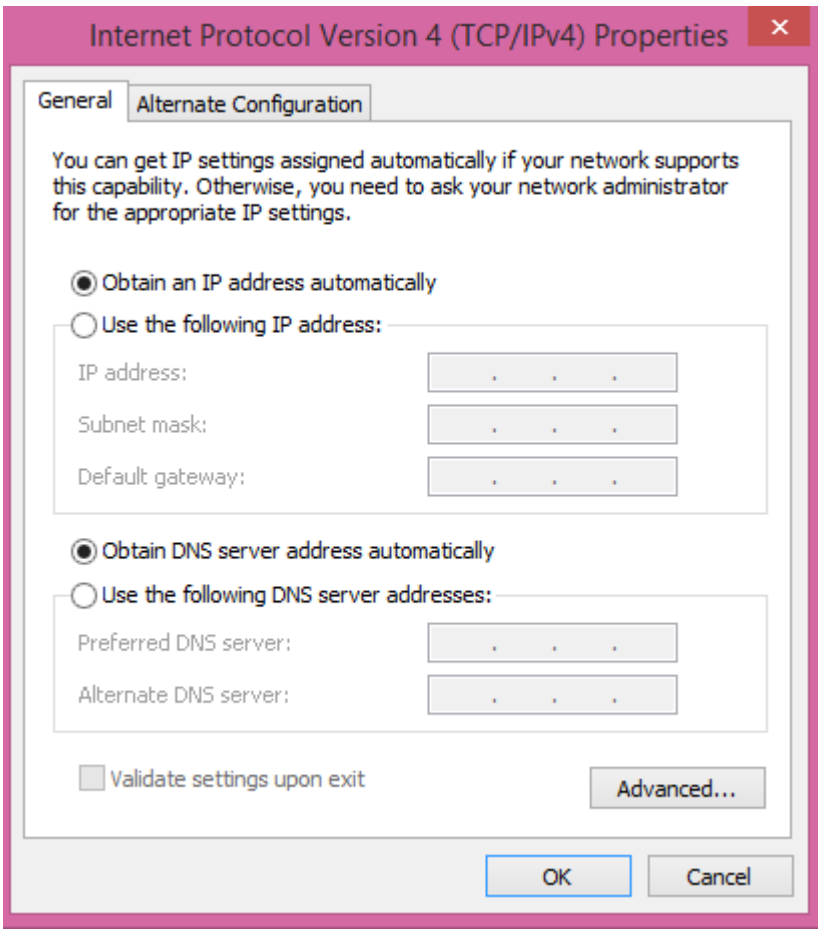
Bước 2: Mở Properties card mạng



Hình 8.25 Thuộc tính card mạng

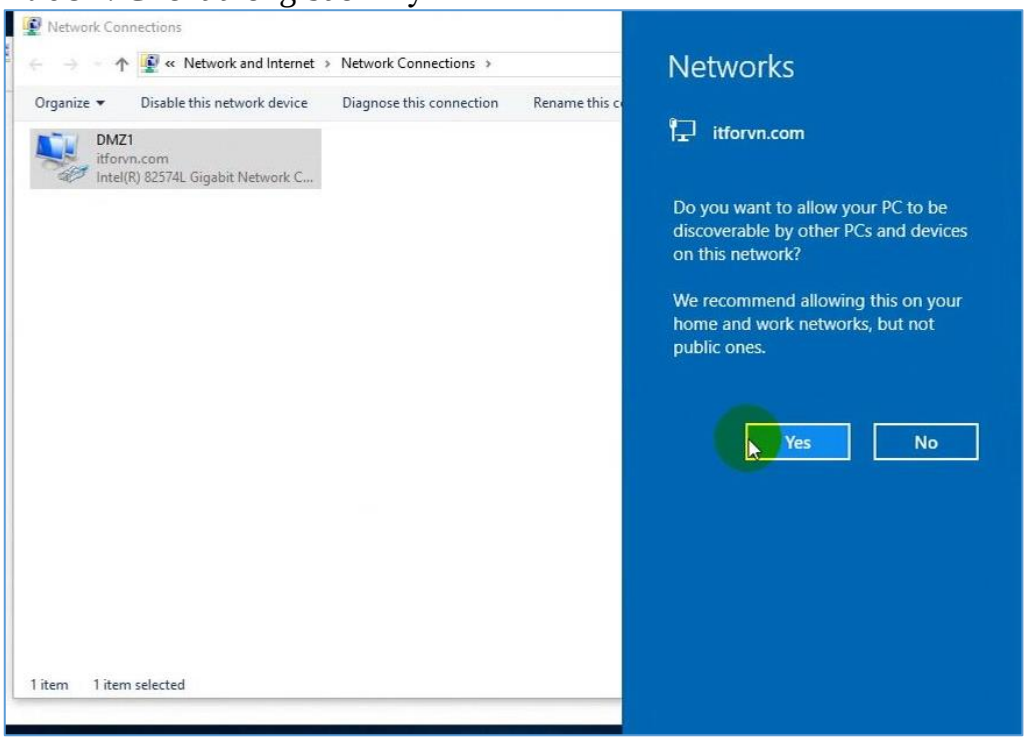
Bước 3: Cấu hình IP động

Chọn sang Obtain an IP address automatically và Obtain an DNS server address automatically



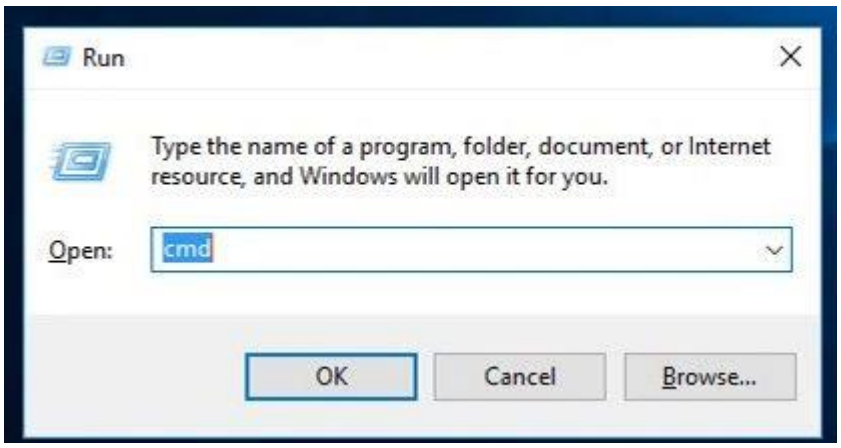
Hình 8.26 Địa chỉ IP động

Bước 4: Client thông báo thay đổi IP



Hình 8.27 Client thông báo thay đổi IP

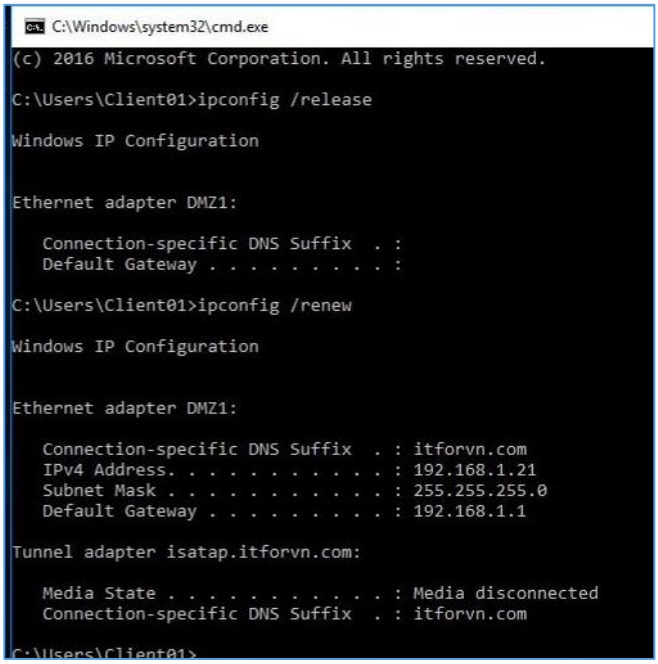
Bước 5: Mở CMD, vào Run gõ CMD



Hình 8.28 Chạy CMD

Bước 6: Xin IP động từ DHCP

Mở CMD lên gõ ipconfig /release và ipconfig /renew nếu cần xin cấp lại IP động



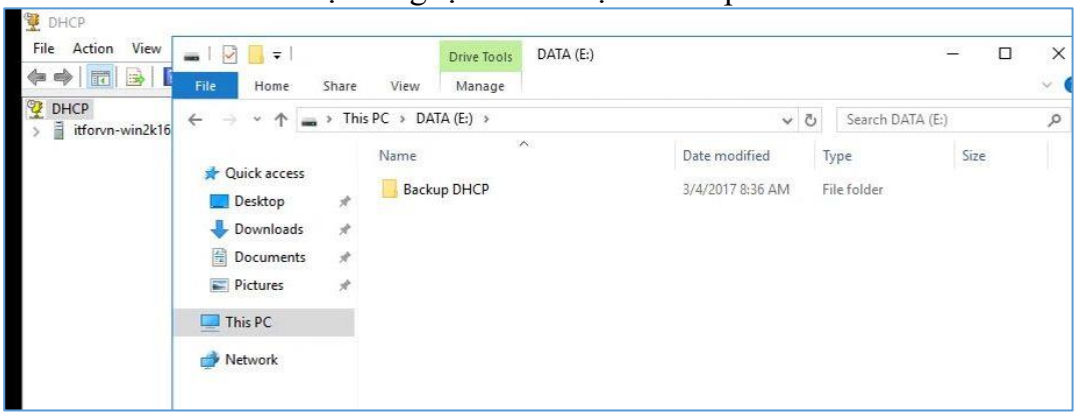
Hình 8.29 Xin IP động

6. Backup và Restore DHCP

6.1 Backup DHCP

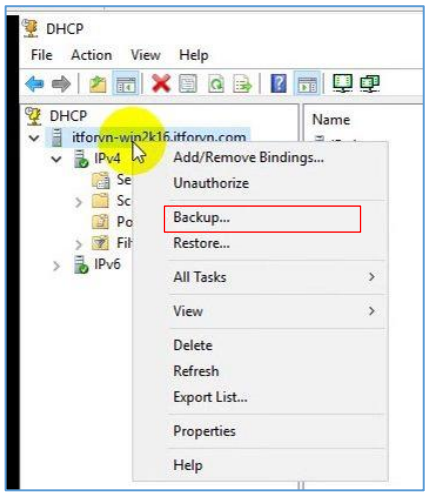
Bước 1: Tạo thư mục sẽ lưu file backup

Vào ổ E khác với ổ hệ thống tạo 1 thư mục Backup DHCP



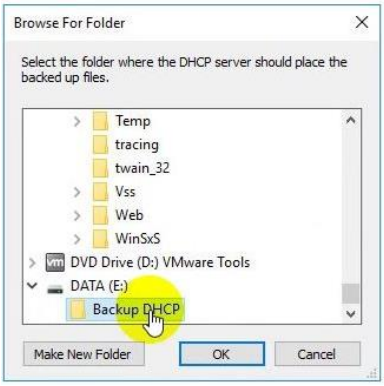
Hình 8.30 Tạo thư mục

Bước 2: Mở cấu hình DHCP chọn Backup



Hình 8.31 Mở cử sổ Backup

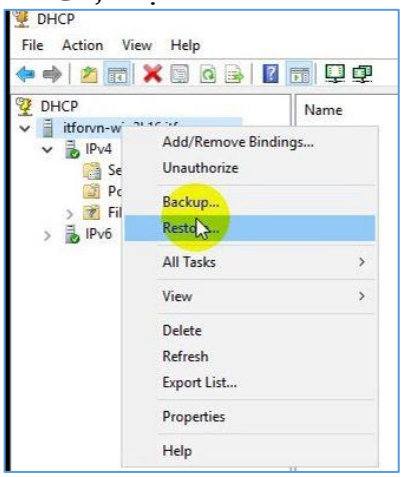
Bước 3: Chọn nơi lưu file Backup



Hình 8.32 Chọn nơi lưu file backup

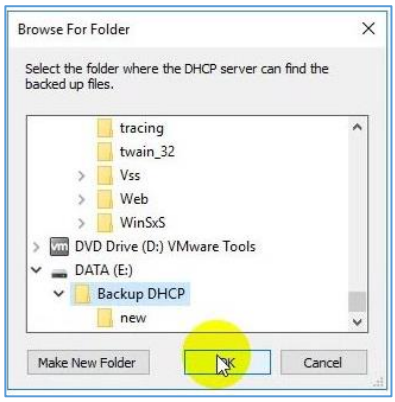
6.2 Restore DHCP

Bước 1: Mở cửa sổ cấu hình DHCP, chọn Restore



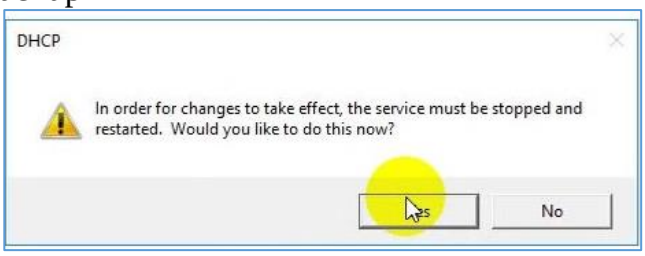
Hình 8.33 Cửa sổ Restore

Bước 5: Chọn file đã Backup



Hình 8.34 chọn file backup

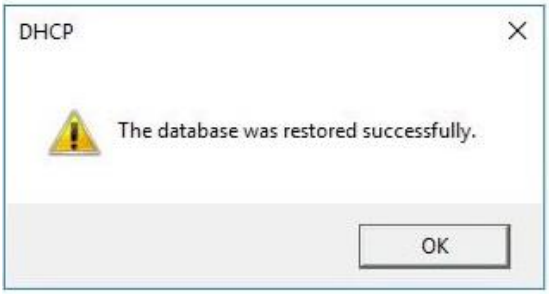
Bước 6: Xác nhận backup



Hình 8.35 Chấp nhận backup

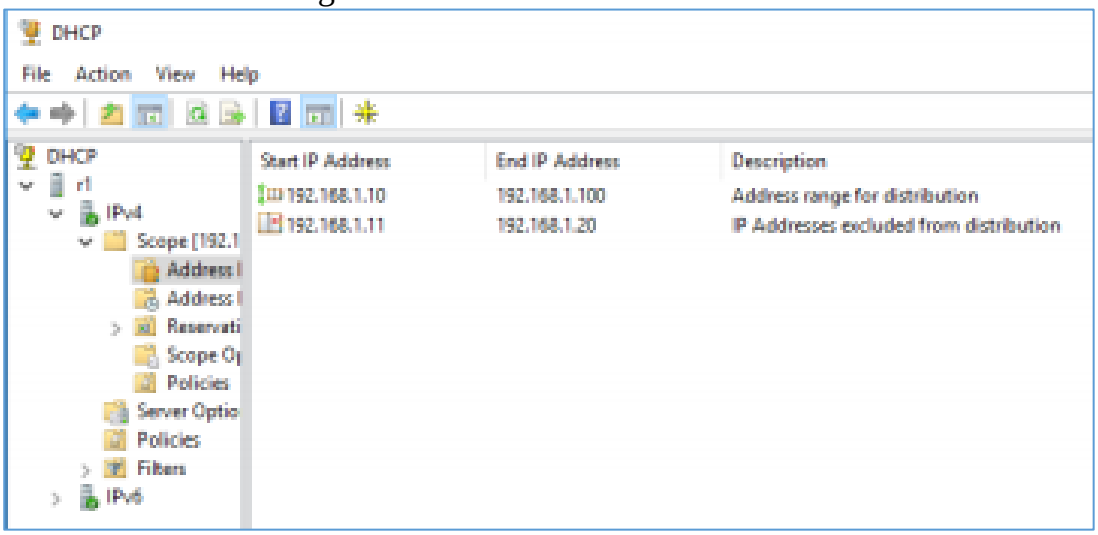
Hình 8.34 chọn file backup

Bước 7: Xác nhận backup thành công



Hình 8.36 Hoàn thành backup

Bước 8: Restore thành công



Hình 8.37 Backup thành công

Bài tập thực hành của học viên

1. Cài đặt và cấu hình dịch vụ DHCP
2. Tạo file Sao lưu và phục hồi DHCP

Hướng dẫn thực hiện:

- Bài tập 1 Thực hiện theo từng bước trong mục 5của giáo trình
- Bài tập 2 Thực hiện theo các bước trong mục 6 của giáo trình
- Bài tập 3 làm theo mục 5 của giáo trình

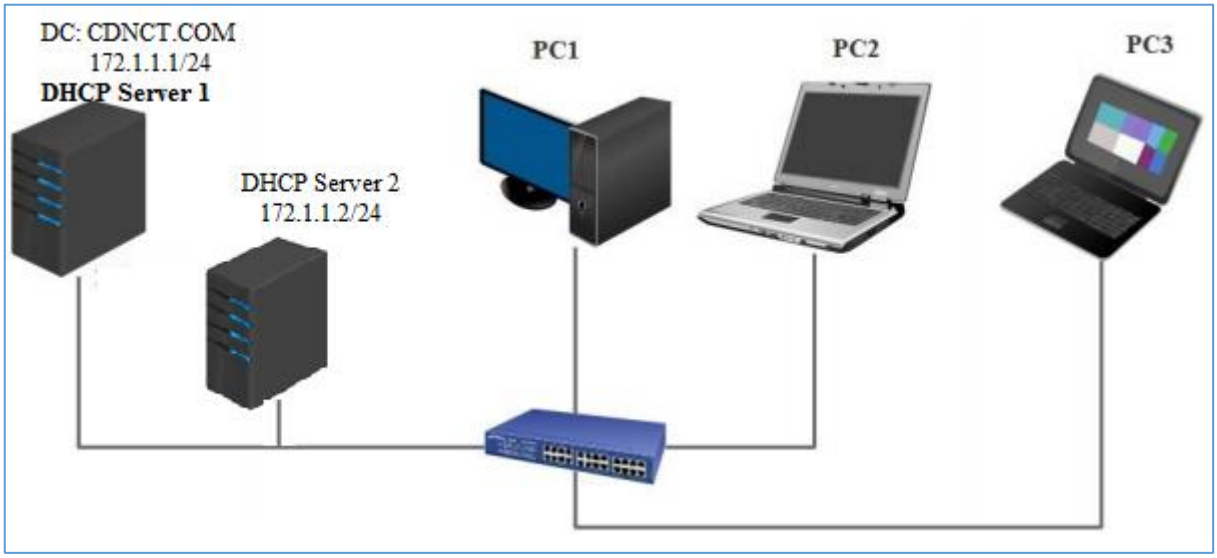
Những trọng tâm cần chú ý:

- Xác định đúng server để cài đặt và cáu hình DHCP.
- Xác định đúng dãy IP cấp phát cho từng nhóm mạng
- Thực hiện đúng thao tác chặn IP để dành không cho cấp phát
- Thực hiện đúng IP Router cho hệ thống.
- Thiết lập đúng DNS cho hệ thống.
- Client phải cùng hệ thống mạng được cấp IP động.
- Chọn đĩa lưu trữ file Backup cho an toàn khi có sự cố phục hồi lại.
- Thao tác phải đúng các bước cài đặt, cấu hình và backup, restore cho DHCP.

Bài mở rộng và nâng cao

Cài đặt và cấu hình DHCP Failover theo 2 cơ chế: Load Balancing và Hot Standby trong Windows Server 2019, theo mô hình sau

Mô hình



Hình 8.38 mô hình DHCP

Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được Chức năng và Hoạt động dich vụ DHCP trên Windows Server
  + Trình bày được các bước Quản lý dich vụ DHCP trên Windows Server 2019
- Về kỹ năng:
  + Thao tác thành thạo cài đặt, cấu hình DHCP trên Domain Controller.
  + Thao tác được Load Balancing và Hot Standby Windows Server 2019
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng:
  + Đánh giá kỹ năng thực hành cài đặt, cấu hình DHCP trên Domain Controller.
  + Đánh giá kỹ năng thực hành về được Load Balancing và Hot Standby.
  + Thực hiện đúng Cân bằng tải file Server trên Windows Server 2019
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Bài 9: QUẢN TRỊ MÁY IN
Mã bài: MĐ 17 - 09

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.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Giới thiệu

- Máy in là công cụ đắc lực trong văn phòng. Tuy nhiên, không phải ai cũng biết thiết lập máy in sao cho tốn ít chi phí và đạt hiệu quả cao nhất cho công việc.

- Đơn cử là người dùng thường kết nối máy in vào một máy tính, sau đó chia sẻ máy in này cho tất cả các máy tính khác trong cùng một mạng LAN. Điều này sẽ bị hạn chế mỗi khi in vì lệnh in từ các máy khác sẽ chạy qua máy đang chia sẻ, sau đó tùy theo độ ưu tiên (metric) của lệnh in mà thực hiện. Một bất cập khác cũng khá quan trọng là máy đang chia sẻ sẽ phải trong trạng thái hoạt động liên tục, nếu không các lệnh in sẽ đi đến máy này và bị dừng lại, và như thế máy in sẽ không thể nhận được các lệnh đã yêu cầu.

2.Cài đặt máy in

Mục tiêu:

- Cài đặt được máy in cho server và qua mạng.

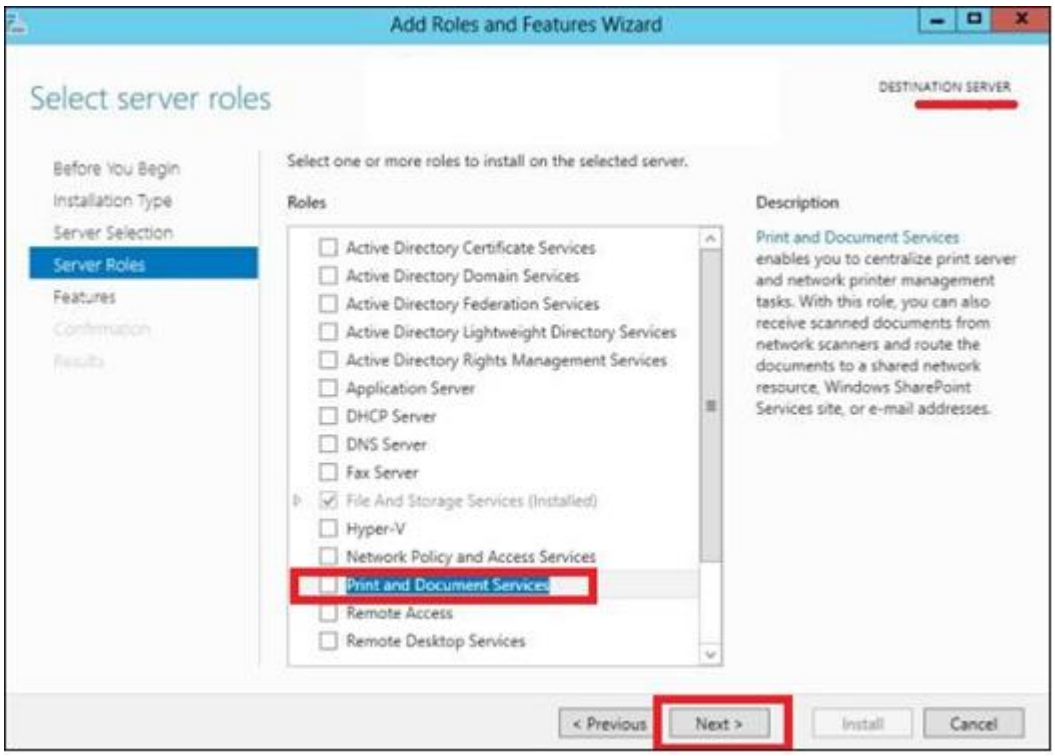
Trước khi bạn có thể truy xuất vào thiết bị máy in vật lý thông qua hệ điều hành **Windows Server** thì bạn phải tạo ra một máy in **logic**. Nếu máy in của bạn có tính năng **Plug and Play** thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành **Windows Server**. Tiện ích **Found New Hardware Wizard** sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn cho bạn từng bước để cài đặt máy in. Nếu hệ điều hành nhận diện không chính xác thì bạn dùng đĩa **DVD** được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Ngoài ra, bạn cũng có thể tự mình thực hiện tạo ra một máy in **logic** bằng cách sử dụng tiện ích **Add Printer Wizard**. Để có thể tạo ra một máy in **logic** trong **Windows Server** thì trước hết bạn 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**).

2.1 Cài đặt dịch vụ máy in

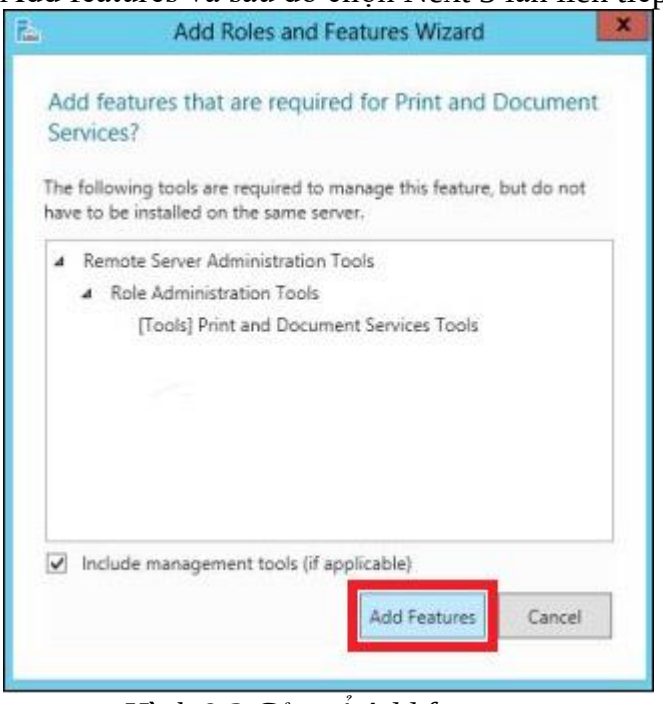
Bước 1 - Đi đến Server Manager > Manage > Add Roles and Features > Next > Chọn Role-based installation hoặc Feature-based installation, rồi chọn tiếp Select a server from the server pool. Cuối cùng, bấm Next.

Khi đã thực hiện xong các bước trên, tại danh sách Roles, hãy tìm Print and Document Services. Sau đó, một cửa sổ sẽ mở ra.



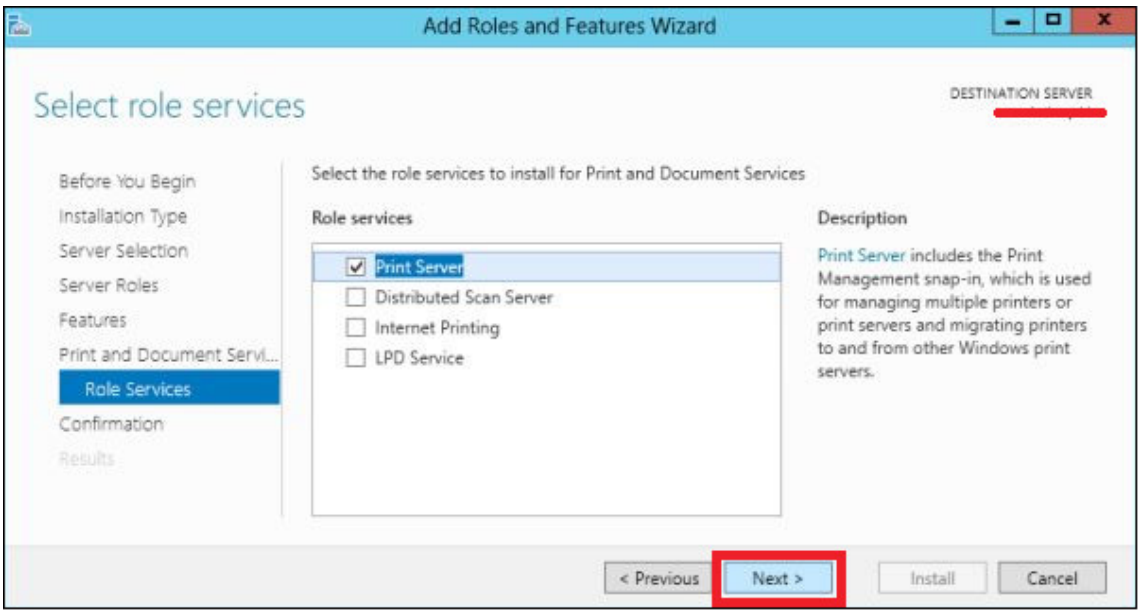
Hình 9.1 Chọn dịch vụ máy in

Bước 2 - Nhấp vào Add features và sau đó chọn Next 3 lần liên tiếp.



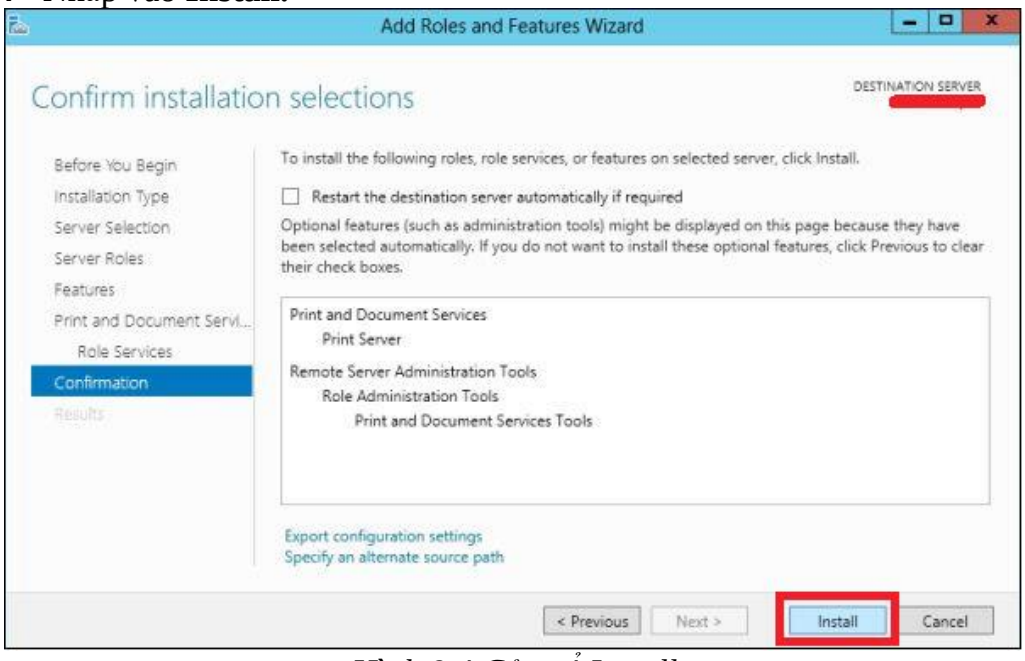
Hình 9.2 Cửa sổ Add features

Bước 3 - Chọn **Print Server**, rồi bấm **Next.**



Hình 9.3 Chọn dịch vụ máy in

Bước 4 - Nhấp vào **Install.**



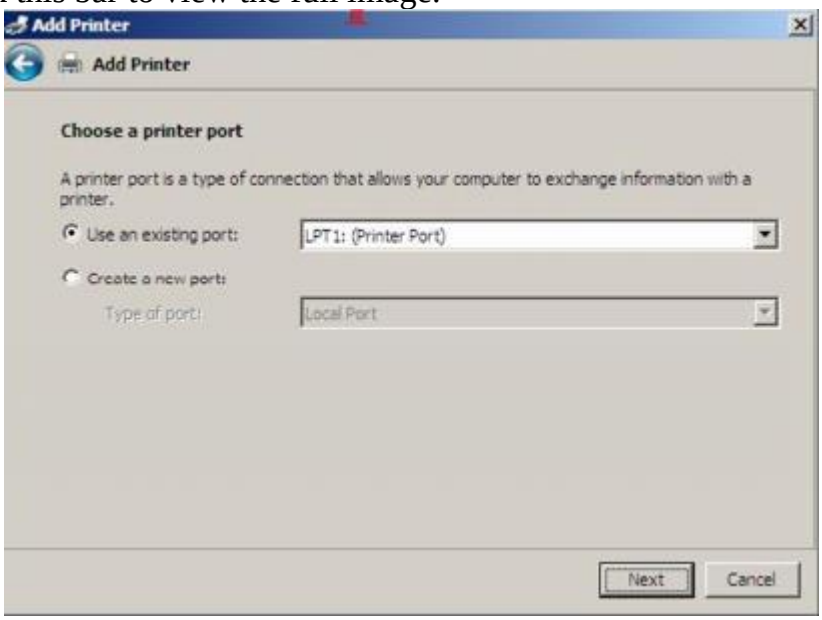
Hình 9.4 Cửa sổ Install

2.2 Cài đặt Printer trên Print Server

Bước 1: Chọn Add a local printer (Canon LBP-1260)

Hình 9.5 Cửa sổ Add printer

Bước 2: Click this bar to view the full image.



Hình 9.6 chọn port

Bước 3: Chọn máy inCanon LBP-1260

Hình 9.7 chọn máy in

Bước 4: Xem kết quả cài đặt

Hình 9.8 các máy in được cài đặt

2. Quản lý thuộc tính máy in

Mục tiêu:

- Trình bày được các thuộc tính của 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.

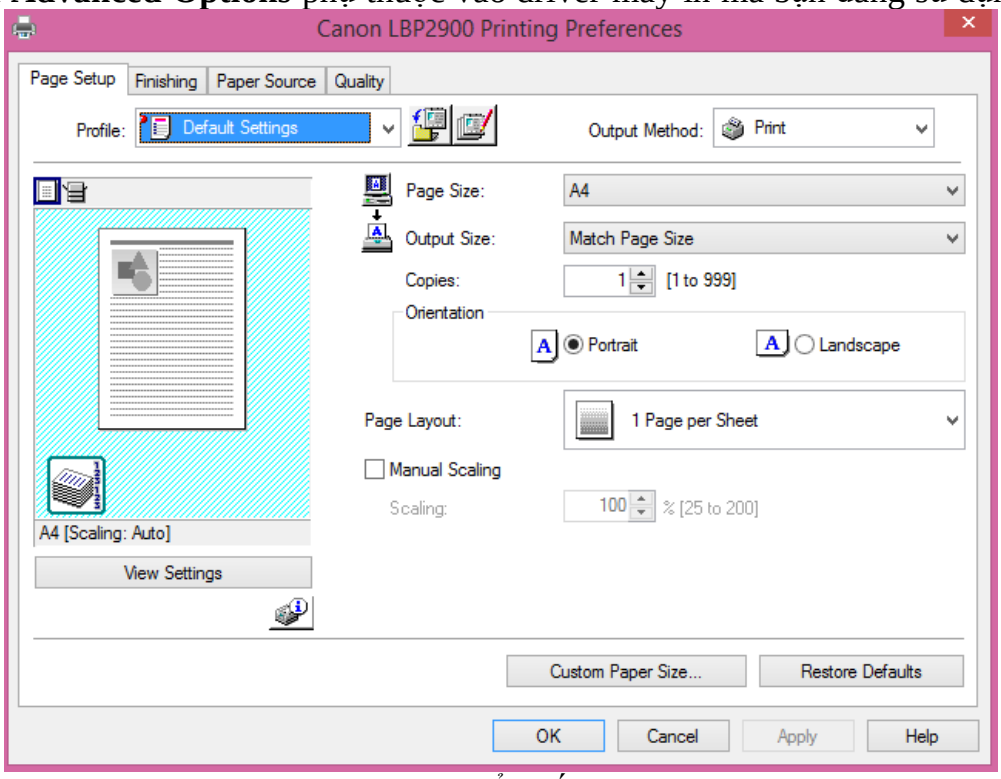
2.2. Giấy và chất lượng in

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**

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

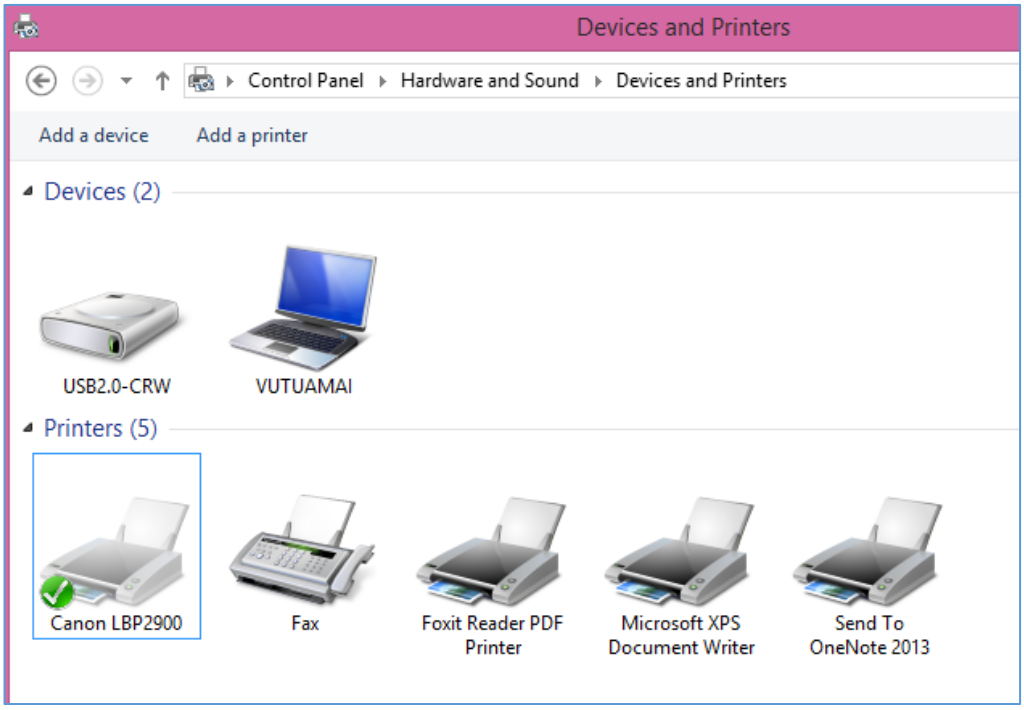
hộp thoại **Advanced Options** phụ thuộc vào driver máy in mà bạn đang sử dụng.



Hình 9.9 Cửa sổ thiết lập máy in

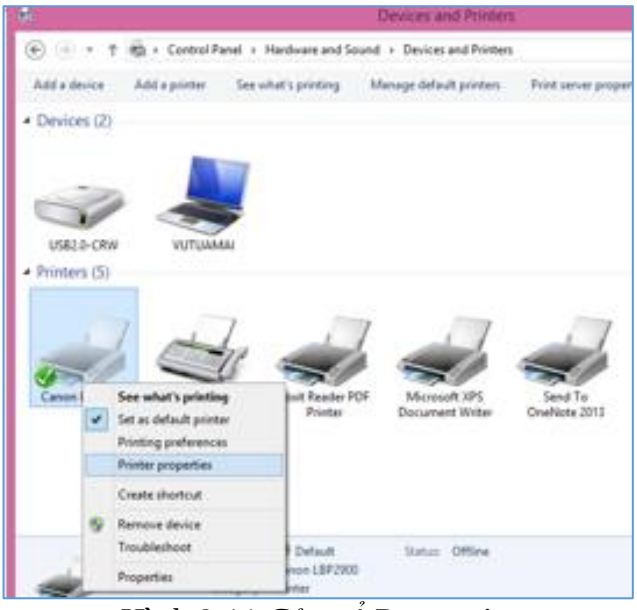
3. Cấu hình chia sẻ máy in

Bước 1: Mở Control Panel\Hardware and Sound\Devices and Printers



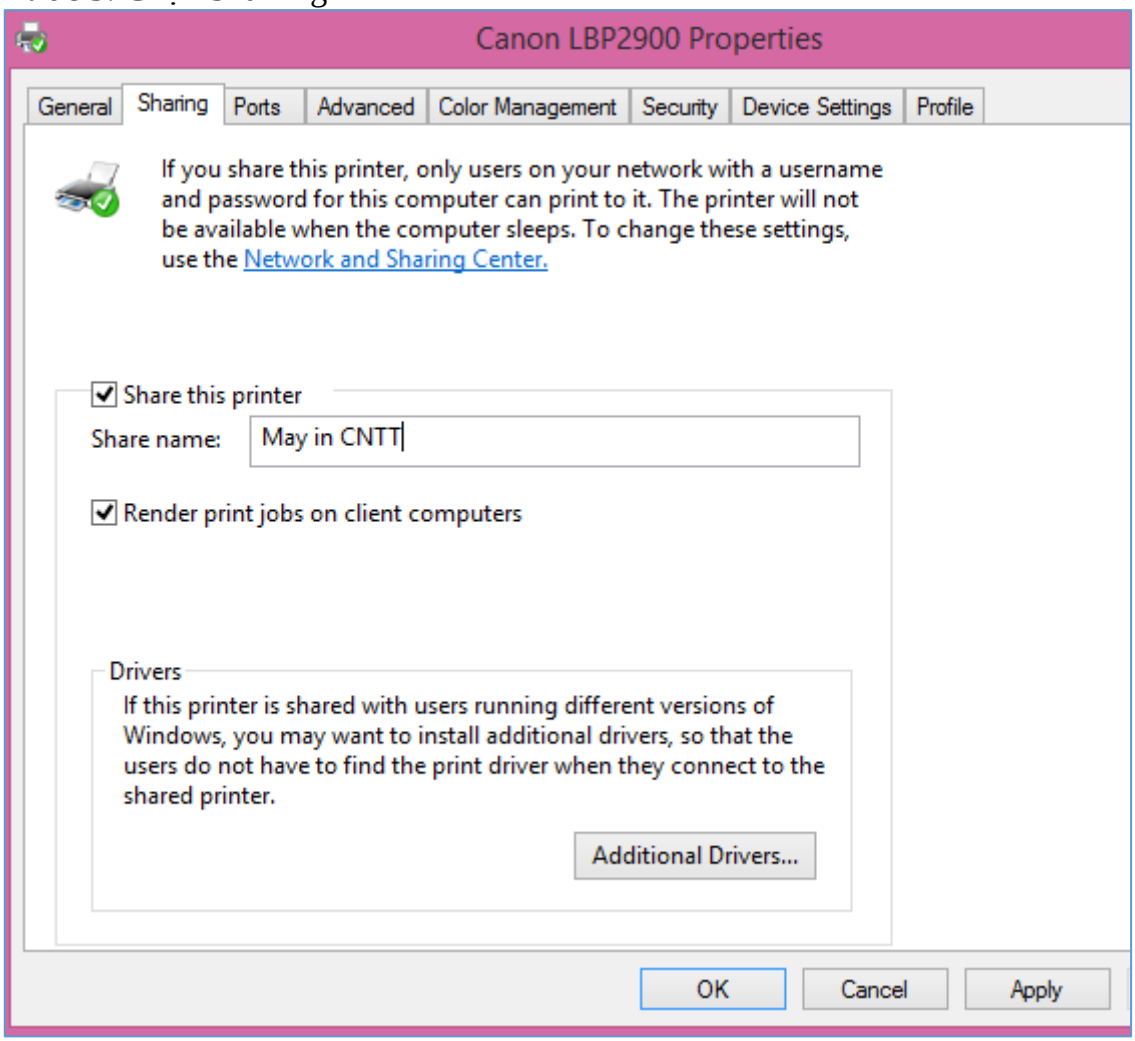
Hình 9.10 mở xem máy in

Bước 2:



Hình 9.11 Cửa sổ Properties

Bước 3: Chọn Sharring



Hình 9.12 Cửa sổ chia sẻ máy in

4. Cấu hình thông số port

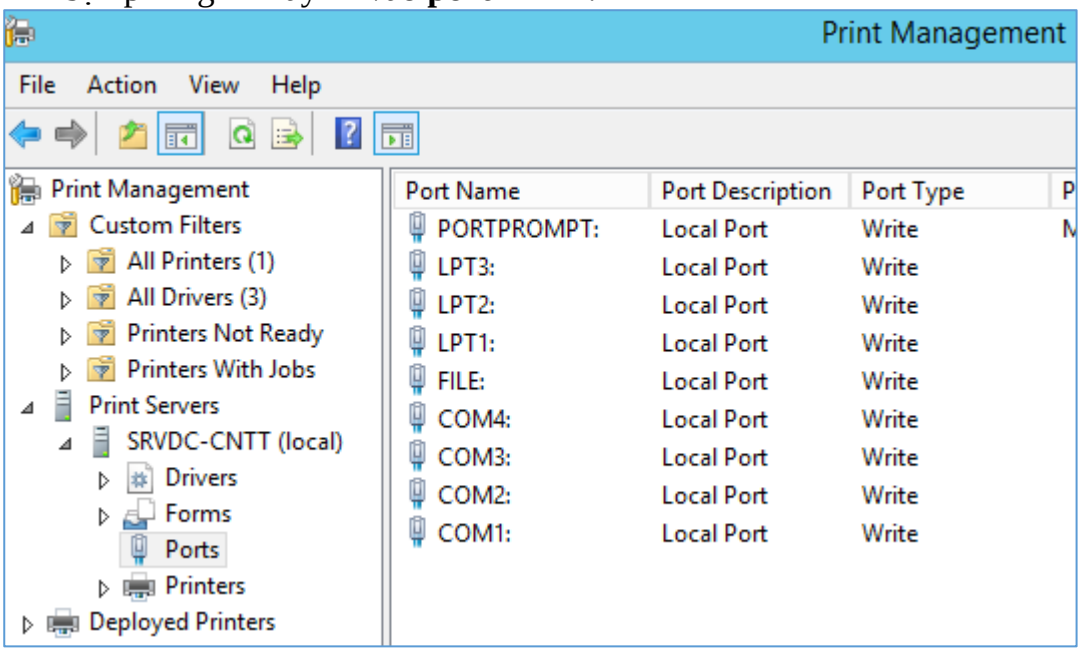
Mục tiêu:

- Trình bày được ý nghĩa các thông số trong tab 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**.



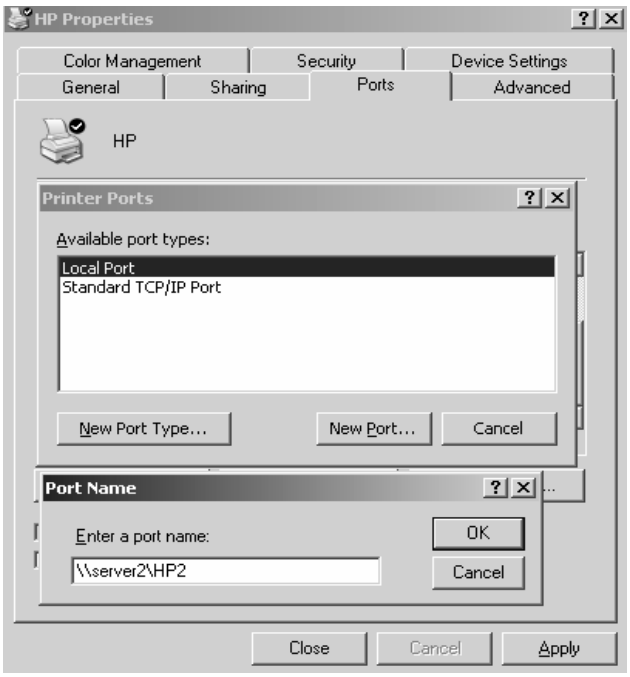
Hình 9.13 Cửa sổ cổng máy in

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.

4.2. Printer Pooling

Printer pool được sử dụng nhằm phối hợp nhiều máy in vật lý với một máy in **logic**, được minh họa như hình bên dưới. Lợi ích của việc sử dụng **printer pool** là máy in rảnh đầu tiên sẽ thực hiện thao tác in ấn cho bạn. Tính năng này rất hữu dụng trong trường hợp ta có một nhóm các máy in vật lý được chia sẻ cho một nhóm người dùng, ví dụ như là nhóm các thư ký

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 Pooling** 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 9.14 Thêm Port máy in

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

Nếu một máy in vật lý của bạn bị hư, bạn 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, trước hết bạn phải đảm bảo máy in mới phải có **driver** giống với máy in cũ. Sau đó, trong **Tab Port**, bạn nhấp chuột vào nút **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.**

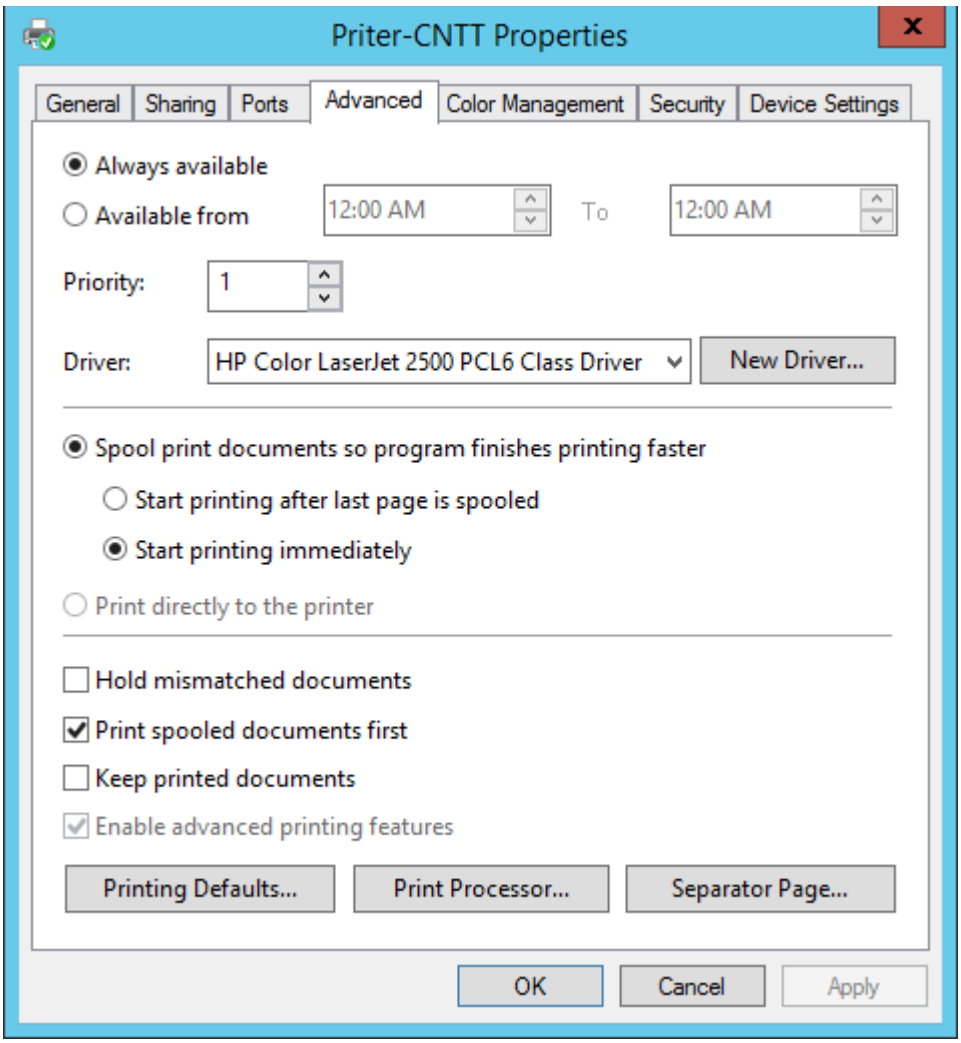
5. Cấu hình tab advanced

Mục tiêu:

- Trình bày được ý nghĩa các thông số trong 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:



Hình 9.15 đặc tính của máy in

5.2. Khả năng sẵn sàng phục vụ của máy in

Thông thường, chúng ta cần kiểm tra khả năng sẵn sàng phục vụ của máy in trong trường hợp chúng ta có nhiều máy in cùng sử dụng một thiết bị in. Mặc định thì tùy chọn **Always Available** luôn được bật lên. Do đó, người dùng có thể sử dụng máy in 24 tiếng một ngày. Để giới hạn khả năng phục vụ của máy in, bạn chọn **Available From** và chỉ định khoảng thời gian mà máy in sẽ phục vụ. Ngoài khoảng thời gian này, máy in sẽ không phục vụ cho bất kì người dùng nào.

5.3. Độ ưu tiên (Printer Priority)

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

5.4. Print Driver

Mục **Drive**r trong **Tab Advanced** cho phép bạn chỉ định driver sẽ dùng cho máy in. Nếu bạn 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 bạn thực hiện cập nhật cũng như thêm driver mới.

5.5. Spooling

Khi bạn cấu hình tùy chọn **spooling**, bạn cần chỉ định rõ các tác vụ in ấn sẽ được đẩy ra đường ống máy in hay được gửi trực tiếp đến thiết bị máy in. **Spooling** có nghĩa là các thao tác in ấn sẽ được lưu trữ xuống đĩa thành một hàng đợi trước khi các thao tác in này được gửi đến máy in. Có thể xem **spooling** giống như là bộ điều phối in ấn nếu như tại một thời điểm có nhiều người dùng cùng lúc gởi yêu cầu đến máy in. Theo chế độ mặc định, tùy chọn **spooling** sẽ được bật lên sẵn.

5.6. Print Options

Phía dưới **Tab Advance** có chứa bốn tùy chọn in ấn. Đó là các tùy chọn:

- **Hold Mismatched Documents**: tùy chọn này hữu dụng trong trường hợp bạn sử dụng chế độ nhiều biểu mẫu trong một máy in. Mặc định thì tùy chọn này sẽ không được bật lên. Các tác vụ sẽ được in theo chế độ **first-in-first-out (FIFO).** Nếu bạn bật tùy chọn này lên, hệ thống sẽ chọn ưu tiên in trước những tác vụ có chung một biểu mẫu.
- **Print Spooled Documents First**: tùy chọn này qui định rằng các tác vụ in ấn được điều hướng xong trước các loại tác vụ lớn khác. Điều này có nghĩa là các tác vụ in ấn sẽ có độ ưu tiên lớn hơn các loại tác vụ khác trong quá trình điều hướng. Mặc định thì tùy chọn này luôn được bật lên giúp gia tăng hiệu quả làm việc của máy in.
- **Keep Printed Documents**: tùy chọn này qui định rằng các tác vụ in ấn phải được xóa khỏi hàng đợi điều hướng in ấn khi các tác vụ này đã hòan tất quá trình in. Thông thường, bạn muốn xóa các tác vụ in ấn ngay khi nó bắt đầu in bởi vì nếu chúng ta tiếp tục lưu trữ các tác vụ này trong hàng đợi điều hướng và đợi cho đến khi chúng được in xong mới xóa thì sẽ phải tốn dung lượng ổ đĩa cho việc lưu trữ. Mặc định thì tùy chọn này sẽ không được bật lên.
- **Enable Advanced Printing Features**: tùy chọn này qui định rằng bất kì các tính năng mở rộng nào mà máy in của bạn có hỗ trợ ví dụ như **Page Order** và **Pages Per Sheet** nên được bật lên. Mặc định thì tùy chọn này luôn được bật lên. Chỉ trong trường hợp xảy ra các vấn đề về tương thích thì bạn có thể tắt tùy chọn này. Ví dụ như bạn đang sử dụng **driver** cho một thiết bị máy in tương tự nhưng nó không hỗ trợ tất cả các tính năng của máy in. Trong trường hợp đó, bạn nên tắt tùy chọn này đi.

5.7. Printing Defaults

Nút **Printing Defaults** nằm ở góc trái phía dưới của **Tab Advance**. Nếu bạn nhấp chuột vào nút **Printing Defaults**, hộp thoại **The Printing Preferences** sẽ xuất hiện. Đây cũng chính là hộp thoại sẽ xuất hiện khi bạn nhấp chuột vào nút **Printing Preferences** trong **Tab General**

5.8. Print Processor

ộ xử lý in ấn được sử dụng để qui định **Windows Server** có cần phải thực hiện các xử lý bổ sung trong công việc in ấn hay không. Bộ xử lý in ấn **WinPrint** mặc định được cài đặt và được **Windows Server** sử dụng. Bộ xử lý in ấn **WinPrint** có thể hỗ trợ một vài kiểu dữ liệu.

Theo mặc định thì hầu hết các ứng dụng trên nền **Window** sử dụng chuẩn **EMF (enhanced metafile)** để gởi các tác vụ đến máy in. Chuẩn **EMF** dùng kiểu dữ liệu **RAW**. Kiểu dữ liệu này sẽ báo với bộ xử lý in ấn là tác vụ này không cần phải sửa đổi độ ưu tiên khi in. Điều này là do nhà sản xuất phần mềm qui định.

Bảng danh sách các kiểu dữ liệu được bộ xử lý in ấn trong **Windows Server** hỗ trợ:

Kiểu dữ liệu	Mô tả
RAW	Không làm thay đổi tài liệu in ấn
RAW (FF appended)	Không làm thay đổi tài liệu in ấn ngoại trừ việc thêm vào một kí tự **form- feed**
RAW (FF Auto)	Không làm thay đổi tài liệu in ấn ngoại trừ việc kiểm tra xem có cần thêm vào một kí tự **form-feed** hay không
NT EMF 1.00x	Thường điều hướng các tài liệu được gửi từ các máy tính **Window** khác
TEXT	Phiên dịch tất cả các kiểu dữ liệu văn bản đơn giản và máy in sẽ thực hiện in bằng cách sử dụng các lệnh văn bản chuẩn.

5.9. Separator Pages

Separator pages được sử dụng tại thời điểm bắt đầu của mỗi tài liệu nhằm mục đích định dạng rõ người dùng nào đã thực hiện việc in tài liệu này. Nếu như máy in không được chia sẻ thì chế độ **Separator pages** vô hình chung sẽ gây ra lãng phí giấy in. Nếu trong trường hợp máy in được chia sẻ cho nhiều người dùng thì chế độ **Separator pages** sẽ hữu dụng trong việc phân phối các tác vụ in ấn đã hoàn tất.

Để thêm một **Separator page**, bạn thực hiện như sau: nhấp chuột vào nút **Separator page** nằm ở góc phải phía **dưới Tab Advance**. Hộp thoại **Separator page** hiện ra, bạn nhấp chuột vào nút **Browse** để chọn tập tin **Separator page** nào bạn muốn sử dụng.

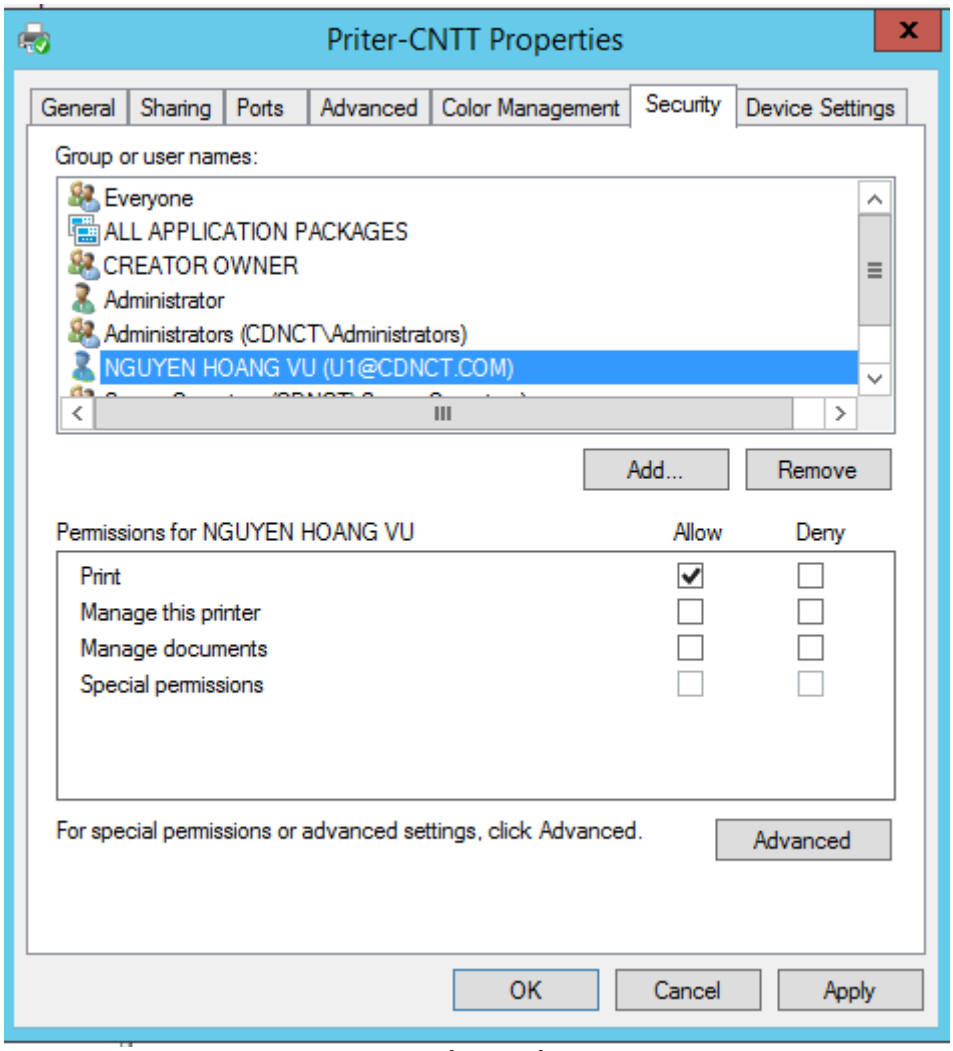
6. Cấu hình tab security

Mục tiêu:

- Phân được quyền truy cập máy in đúng yêu cầu của người sử dụng.

6.1. Giới thiệu Tab Security

Chúng ta có thể kiểm soát quyền truy cập vào máy in **Windows Server** của người dùng cũng như các nhóm người dùng bằng cách cấu hình quyền in ấn. Chúng ta có thể cho phép hoặc không cho phép người dùng truy xuất máy in. Chúng ta cấp quyền in ấn cho người dùng và nhóm người dùng thông qua **Tab Security** trong hộp thoại **Properties** của máy in.



Hình 9.16 Cấp quyền cho user

Bảng phân quyền in ấn cho người dùng

Quyền hạn	Mô tả
Print	Cho phép người dùng hoặc một nhóm người dùng có thể kết nối và gửi tác vụ In ấn đến máy in.
Manage Printers	Cho phép thực hiện thao tác điều khiển, quản lý máy in. Với quyền này, người dùng hoặc nhóm người dùng có thể dừng hoặc khởi động lại máy in, thay đổi cấu hình của bộ điều tác, chia sẻ hoặc không chia sẻ máy in, thay đổi quyền in ấn, và quản trị các thuộc tính của máy in.
Manage Documents	Cho phép người dùng quản lý các tài liệu in qua các thao tác dừng việc in, khởi động lại, phục hồi lại, hoặc là xoá tài liệu ra khỏi hàng đợi máy in. Người dùng không thể điều khiển trạng thái của máy in.
Special Permissions	Bằng cách chọn **Tab Advanced** trong hộp thoại **Print Permissions**, bạn có thể quản lý các quyền đặc biệt

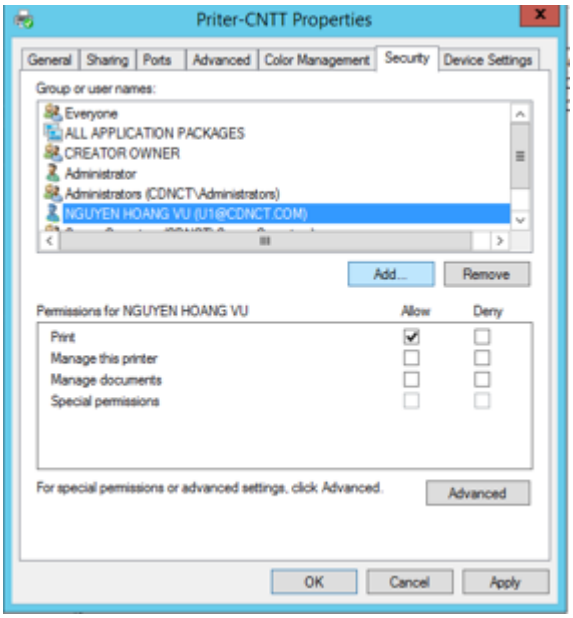
Theo mặc định, bất kì khi nào một máy in được tạo ra, các quyền in ấn mặc định sẽ được thiết lập. Bảng các quyền in ấn mặc định:

Nhóm quyền	Được phép in	Quản lý in	Quản lý tài liệu in
Administrators	X	X	X
Creator Owner			X
Everyone	X		
Print Operators	X	X	X
Server Operators	X	X	X

6.2. Cấp quyền in cho người dùng/nhóm người dùng

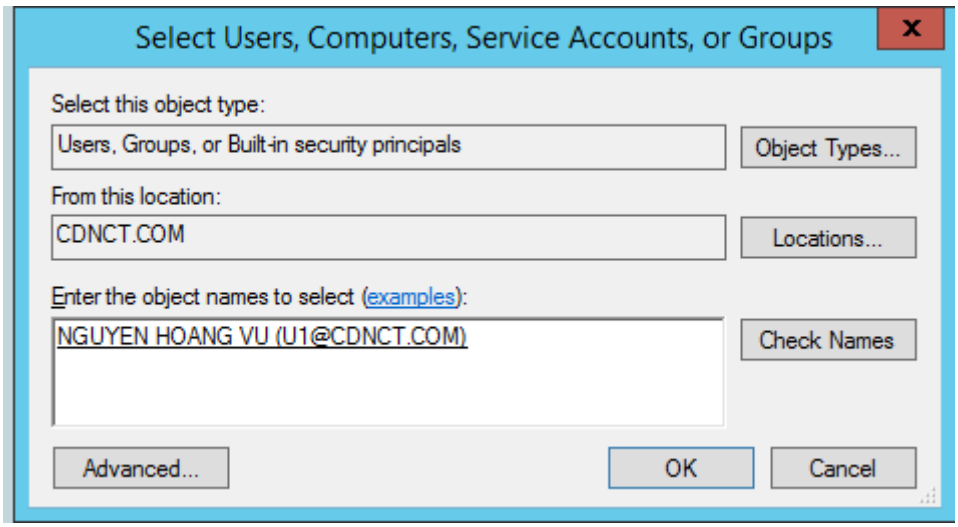
Thông thường, bạn có thể chấp nhận quyền in ấn mặc định đã được thiết lập sẵn. Tuy nhiên, trong một số trường hợp đặc biệt, bạn cần phải hiệu chỉnh lại các quyền in cho thích hợp. Ví dụ: Công ty của bạn vừa trang bị cho phòng **Marketing** một máy in **laser** màu đắt tiền, bạn không muốn ai cũng được phép sử dụng máy in này. Trong trường hợp này, trước tiên bạn phải bỏ tùy chọn **Allow checkbox for the Everyone group**. Sau đó, thêm nhóm **Marketing** vào trong danh sách của **Tab Security**. Cuối cùng bạn cấp cho nhóm **Marketing** quyền **Print**. Muốn thêm các quyền in ấn, bạn thực hiện các bước sau:

Bước 1. Ở **Tab Security** trong hộp thoại **Properties** của máy in, nhấp chuột vào nút **Add.**



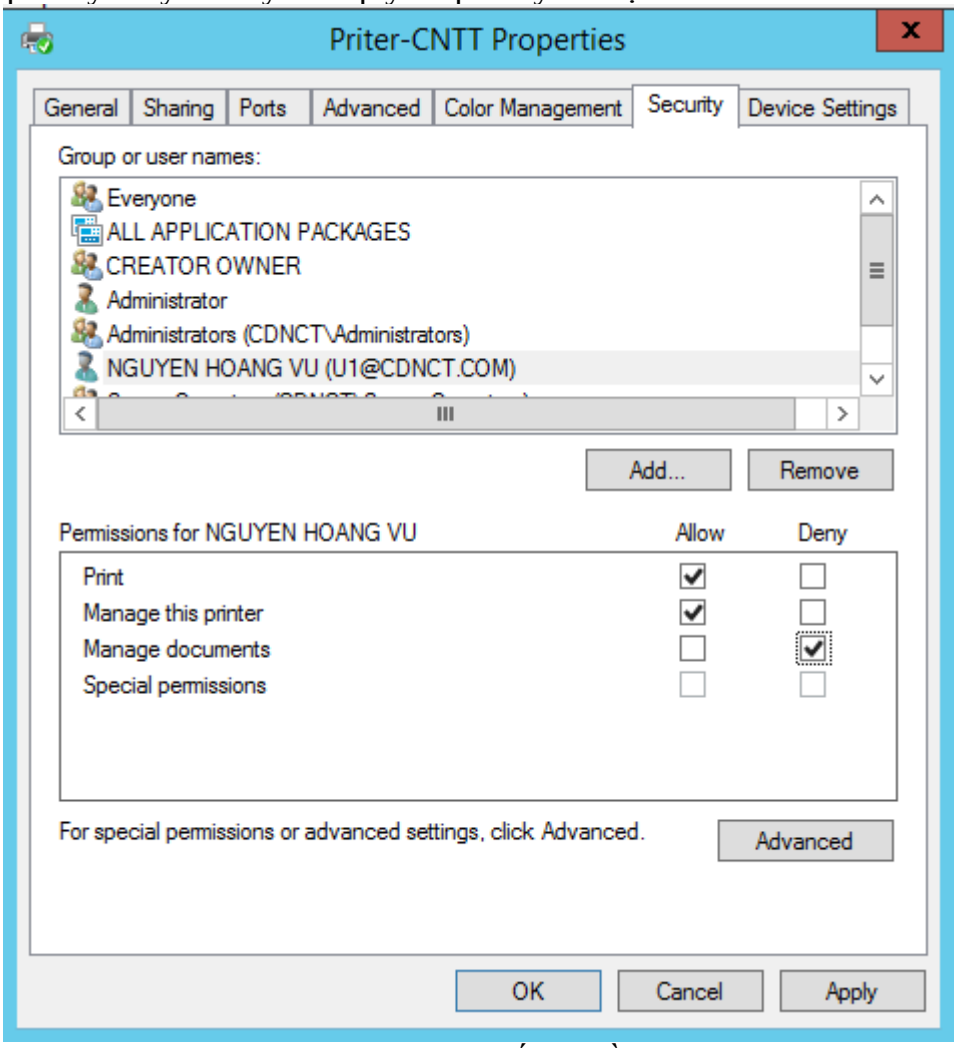
Hình 9.17 Thêm User và group

Bước 2. Hộp thoại **Select Users**, **Computers**, **Or Groups** xuất hiện, bạn nhập vào tên của người dùng hoặc nhóm người dùng mà bạn định cấp quyền in ấn rồi nhấp chuột vào nút **Add**. Sau đó, bạn chọn tất cả các người dùng mà bạn muốn cấp quyền và nhấp chuột vào nút **OK.**



Hình 9.18 Chọn User và group

Bước 3. Chọn người dùng hoặc nhóm người dùng từ danh sách các phân quyền, sau đó chọn **Allow** để cấp quyền hoặc chọn **Deny** để không cấp quyền in ấn, các quyền quản lý máy in hay các quyền quản lý tài liệu in.



Hình 9.19 Cấp quyền

Để loại bỏ một nhóm có sẵn trong danh sách phân quyền, ta sẽ chọn nhóm đó và nhấp chuột vào nút **Remove.** Nhóm vừa chọn sẽ không còn được liệt kê trong **Tab Security** nữa và không thể được cấp bất kì quyền hạn in ấn nào.

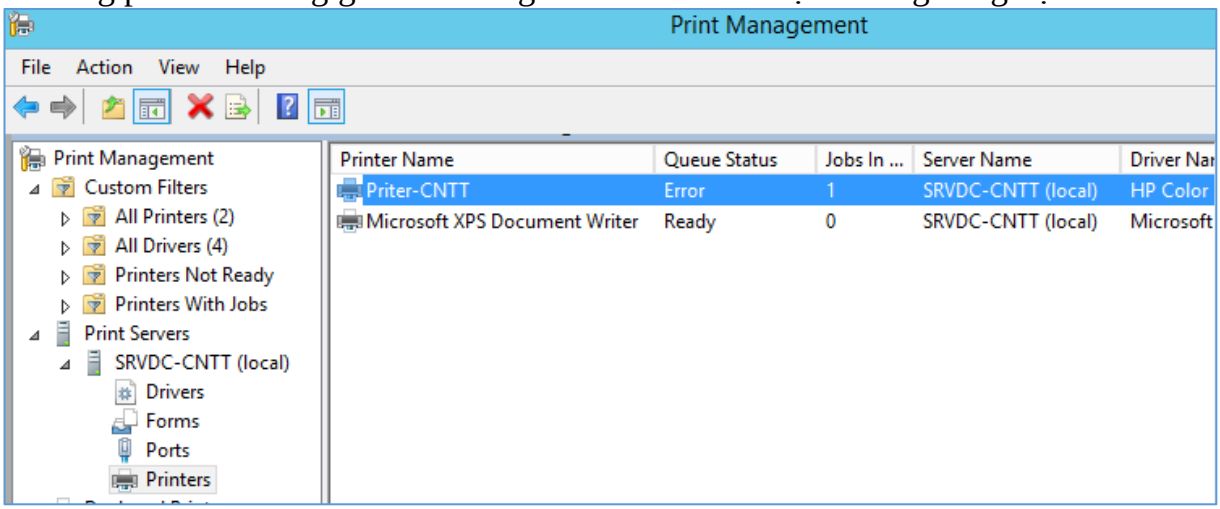
7. Quản lý print server

Mục tiêu:

- Quản lý được máy in mạng.

7.1. Hộp thoại quản lý Print Server

Print Server là một một máy tính trên đó có định nghĩa sẵn các máy in. Khi người dùng gửi một yêu cầu in ấn đến một máy in mạng, thì trước tiên, yêu cầu đó phải được gửi đến **Print Server**. Nói cách khác **Print Server** sẽ có nhiệm vụ quản lý tất cả các máy in **logic** đã được tạo ra trên máy tính. Với tư cách là một **Print Server**, máy tính này phải đủ mạnh để hỗ trợ cho việc đón nhận các tác vụ in ấn và nó cũng phải đủ không gian đĩa trống để chứa các tác vụ in trong hàng đợi.



Hình 9.19 Quản lý máy in

Bạn có thể quản lý **Print Server** bằng cách cấu hình các thuộc tính trong hộp thoại **Print Server Properties**. Chúng ta mở hộp thoại **Print Server Properties** bằng cách: mở hộp thoại **Printers And Faxes**, chọn **File** rồi chọn tiếp **Server Properties**. Hộp thoại **Print Server Properties** bao gồm các **Tab: Forms, Ports, Drivers** và **Advanced.**

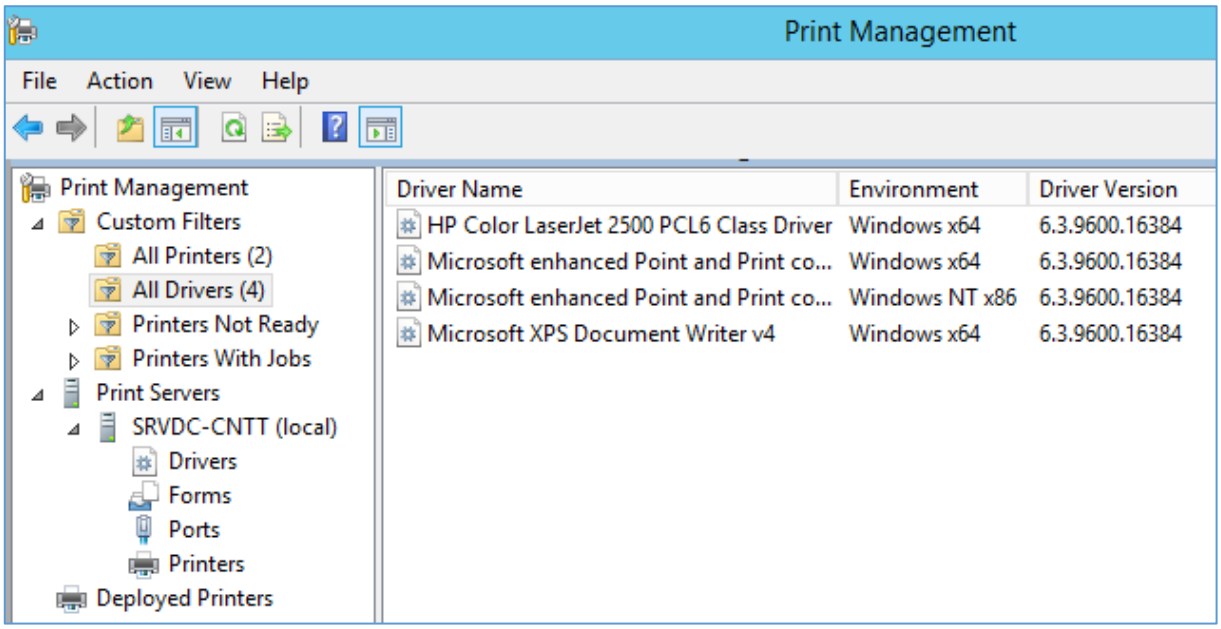
7.2. Cấu hình các thuộc tính Port của Print Server

Trong hộp thoại **Printer Server Properties**, bạn mở **Tab Port**. **Tab** này cũng tương tự như **Tab Port** trong hộp thoại **Properties** của máy in. Sự khác nhau giữa hai **Tab Port** là: **Tab Port** trong hộp thoại **Print Server Properties** được sử dụng để quản lý tất cả các port trên **Print Server**. Còn **Tab port** trong hộp thoại **Properties** của máy in quản lý các **port** của thiết bị máy in vật lý.

7.3. Cấu hình Tab Driver

Trong hộp thoại **Printer Server Properties**, bạn mở **tab Driver**. **Tab Driver** cho phép bạn quản lý các **driver** máy in đã được cài đặt trên **Print Server**. Đối với mỗi **driver** máy in, **Tab** này sẽ hiển thị tên, môi trường và hệ điều hành mà **driver** hỗ trợ.

Sử dụng các tùy chọn trong **Tab Driver**, bạn có thể thêm vào hay loại bỏ hay cập nhật **driver** máy in. Để nhìn thấy các thuộc tính của một **driver** máy in, ta chọn **driver** cần hiển thị và nhấp chuột vào nút **Properties**. Các thuộc tính của một **driver** máy in gồm có:



Hình 9.20 Quản lý driver

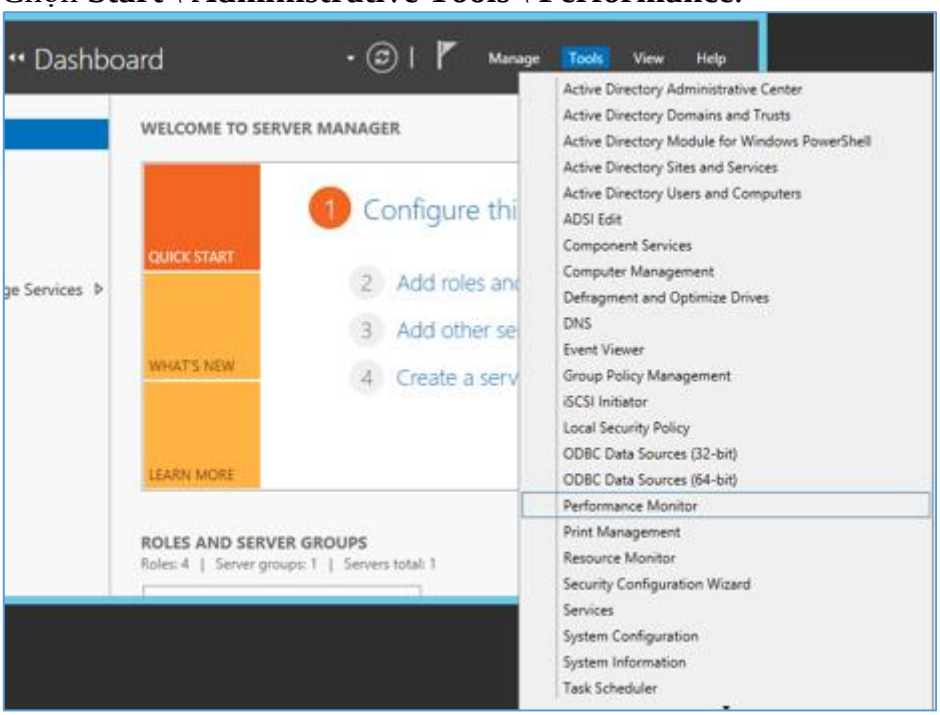
8. Giám sát trạng thái hàng đợi máy in

Mục tiêu:

- Giám sát và xử lý lỗi máy in mạng.

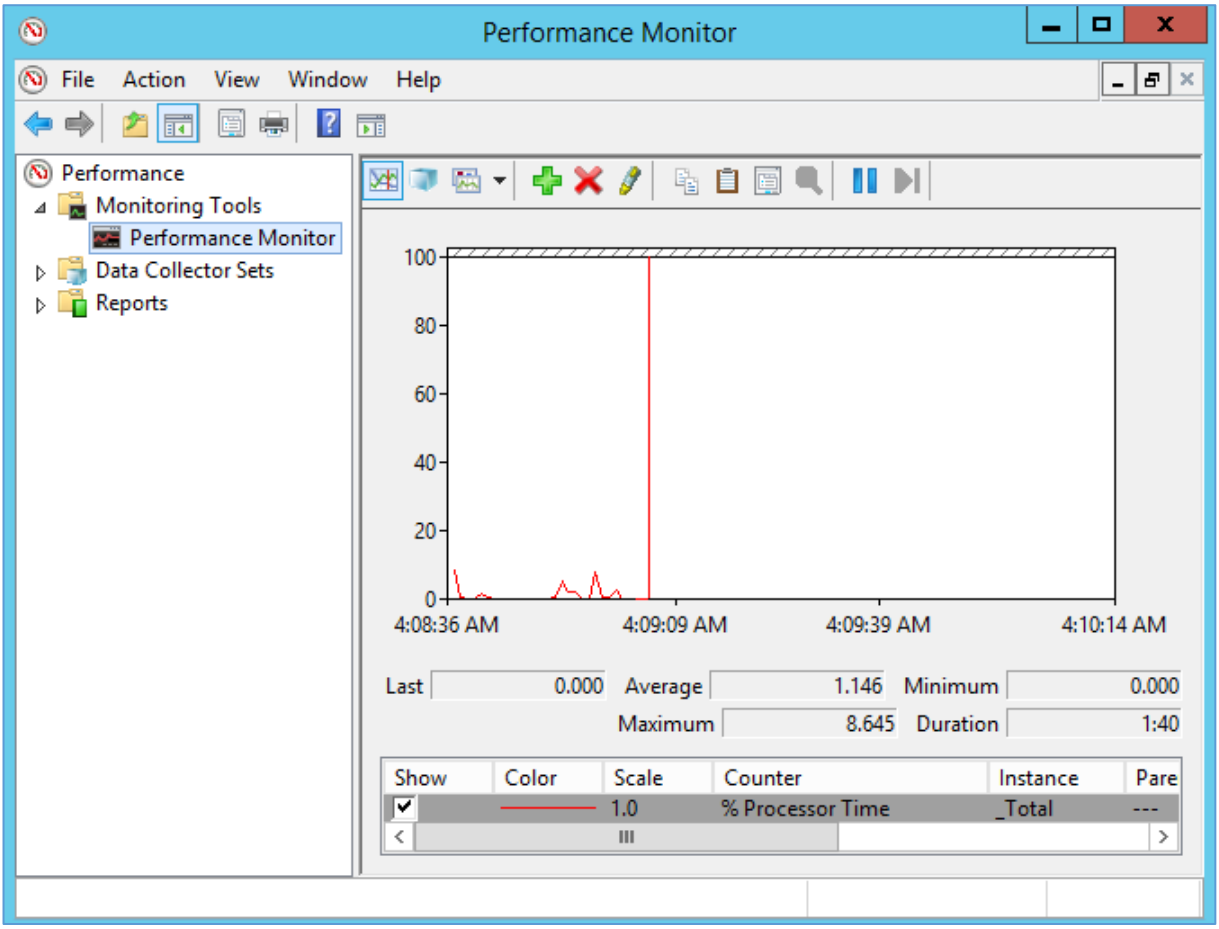
Chúng ta có thể dùng tiện ích **System Monitor** để quản lý hàng đợi máy in. **System Monitor** được dùng để theo dõi các **counter** liên quan đến thao tác thực hiện cho nhiều đối tượng máy tính. Muốn quản lý hàng đợi máy in bằng **System Monitor**, ta thực hiện theo các bước sau:

1. Chọn **Start** \ **Administrative Tools** \ **Performance**.



Hình 9.21 Chạy Performance

2. Hộp thoại **Performance** sẽ xuất hiện. Mặc định thì tiện ích **System Monitor** sẽ được chọn như hình sau:



Hình 9.22 Hộp thoại Performance

3. Nhấp chuột vào nút **Add** (có biểu tượng dấu +) để truy xuất vào hộp thoại **Add Counters**. Sau đó, nhấp chọn **Print Queue Performance Object.**

4. Trong hộp thoại **Add Counters**, bạn có thể chỉ định ra máy tính mà bạn muốn giám sát (cả máy tính cục bộ và máy tính ở xa). **Performance Object** mà bạn cần theo dõi (trong trường hợp này là hàng đợi - **Print Queue**), các **counter** mà bạn muốn theo dõi, và bạn cũng chỉ ra là bạn có muốn theo dõi tất cả các thể hiện hay là bạn chỉ muốn theo dõi một số thể hiện của **counter** được bạn lựa chọn. Nếu bạn chọn tất cả các thể hiện được lựa chọn sẽ cho phép tất cả dữ liệu của tất cả các hàng đợi in ấn đã được định nghĩa trong máy in. Còn nếu bạn chọn chỉ theo dõi một số thể hiện của **counter** thì bạn chỉ theo dõi được dữ liệu từ một số hàng đợi in ấn cá nhân.

Bài tập thực hành của học viên

1. Cài đặt 2 máy in bất kỳ, chia sẻ và phân quyền in ấn trên 2 máy in này.
2. Tìm kiếm máy in trên mạng bằng địa điểm.
3. Thiết lập độ ưu tiên và tính sẵn sàng in.

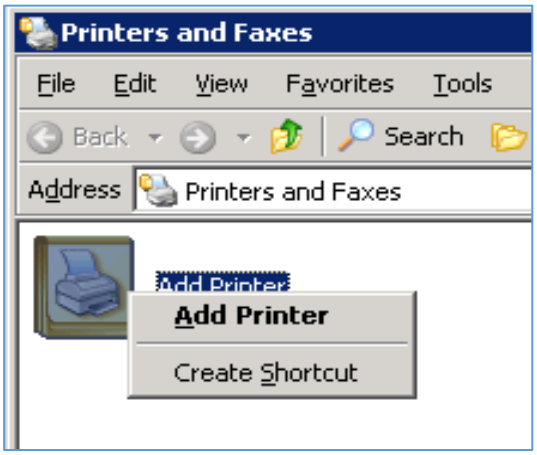
Hướng dẫn thực hiện:

1. Cài đặt 2 máy in bất kỳ, chia sẻ và phân quyền in ấn trên 2 máy in này

a). Cài đặt máy in

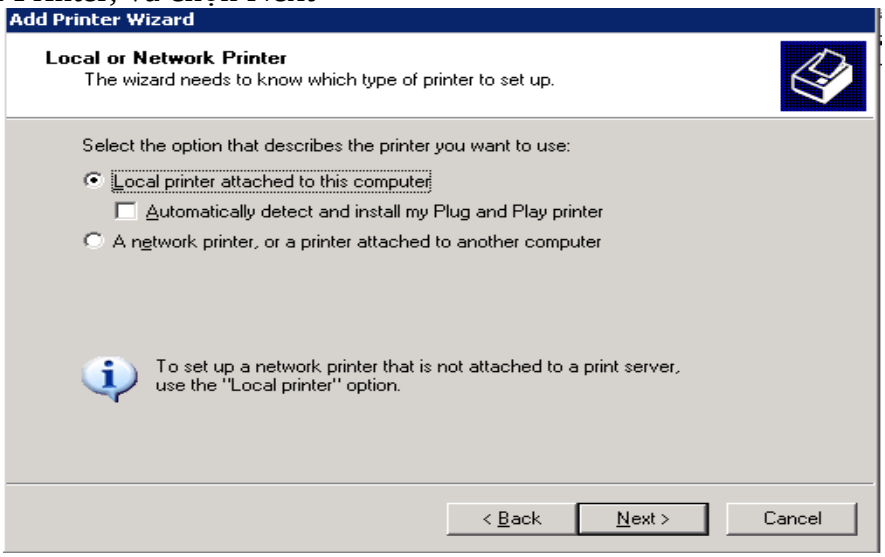
Log on vào máy với tài khoản administrator

Start \Settings\ Printers and faxes



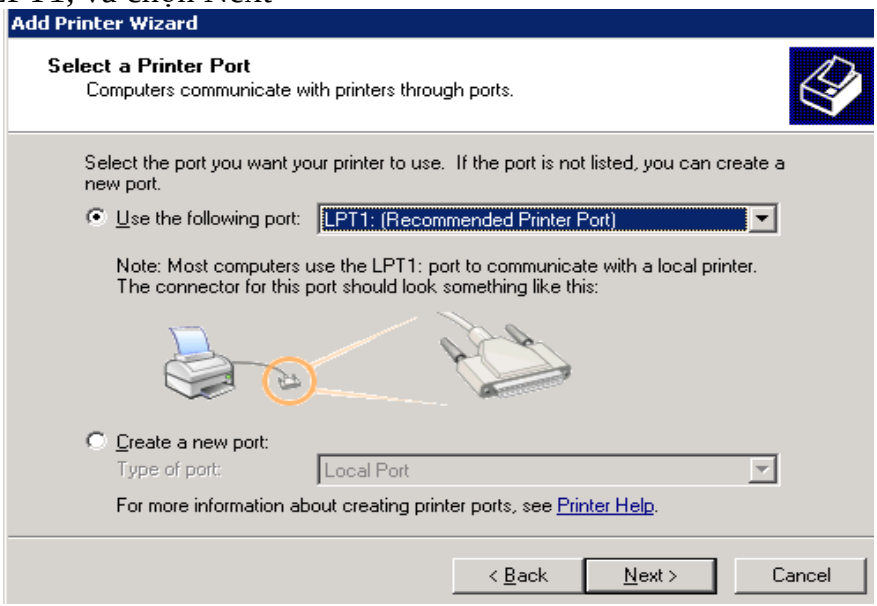
Hình 9.23 Hộp thoại thêm máy in

Chọn Local Printer, và chọn Next



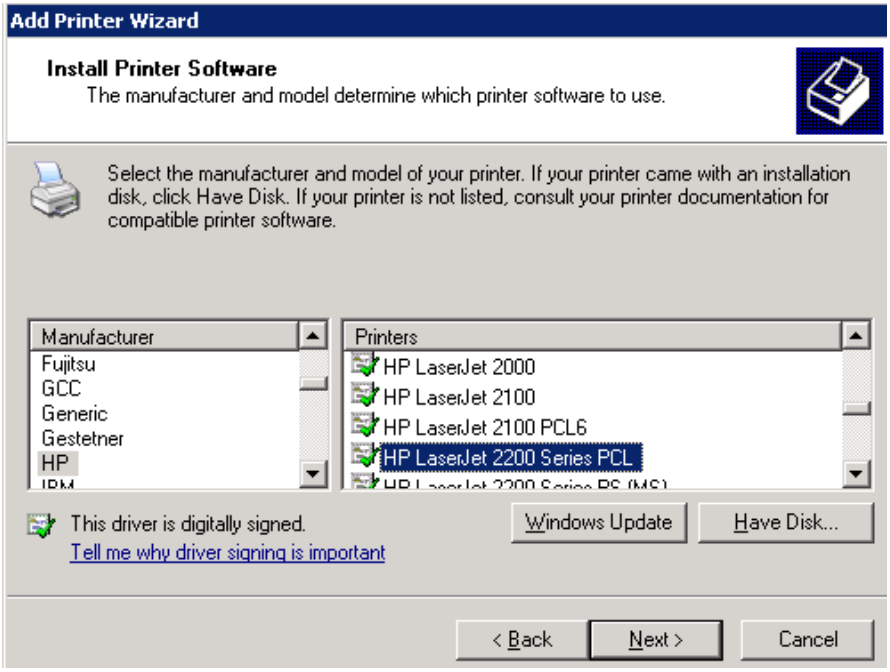
Hình 9.24 Hộp thoại chọn hình thức

Chọn port LPT1, và chọn Next



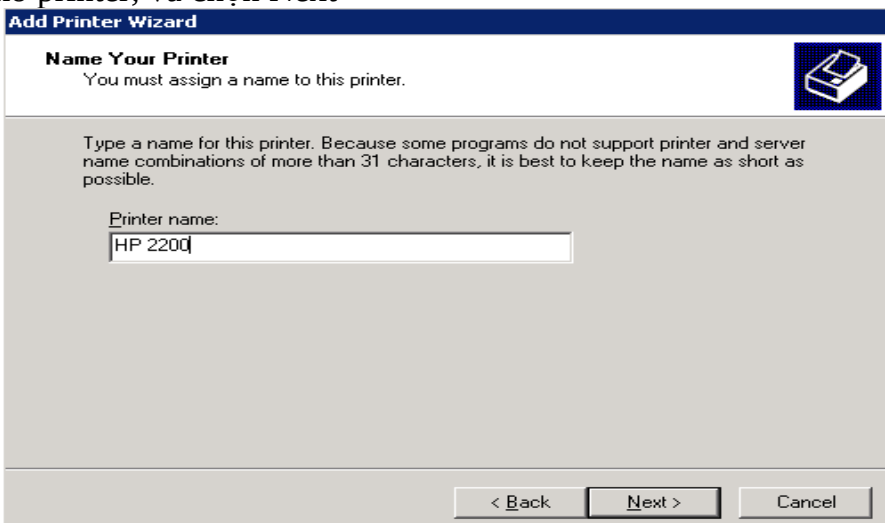
Hình 9.25 Hộp thoại chọn cổng máy in

Chọn hãng sản xuất và chọn loại máy in, và chọn Next



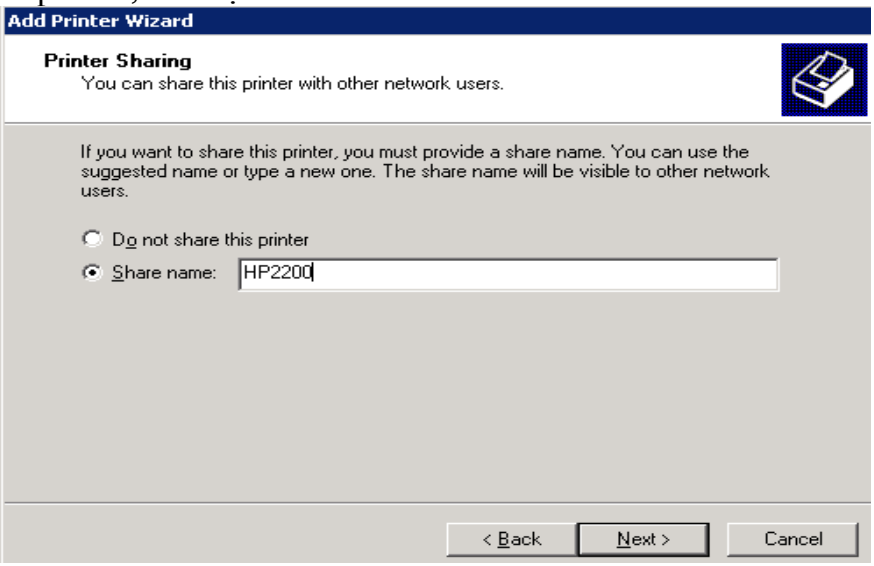
Hình 9.26 Hộp thoại Chọn loại máy in

Nhập tên cho printer, và chọn Next



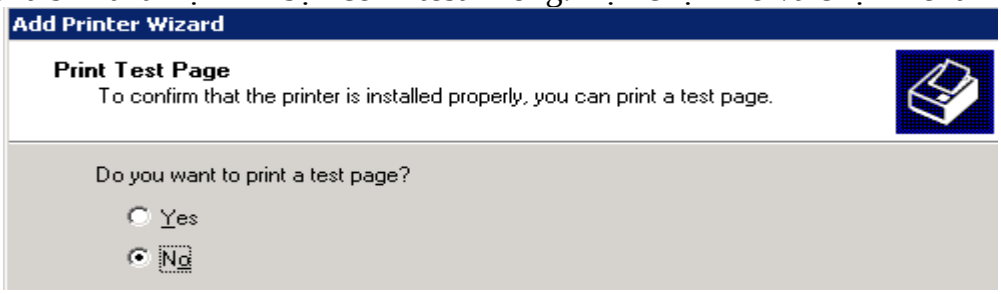
Hình 9.27 Đặt tên máy in

Tên share cho printer, và chọn Next



Hình 9.28 Đặt tên chia sẻ máy in

Nhập địa điểm của máy in(nhập tên HCM trong khung Location), và chọn Next. Cửa sổ xuất hiện hỏi bạn có in test không. Bạn chọn No và chọn Next



Hình 9.29 Không in thử máy in

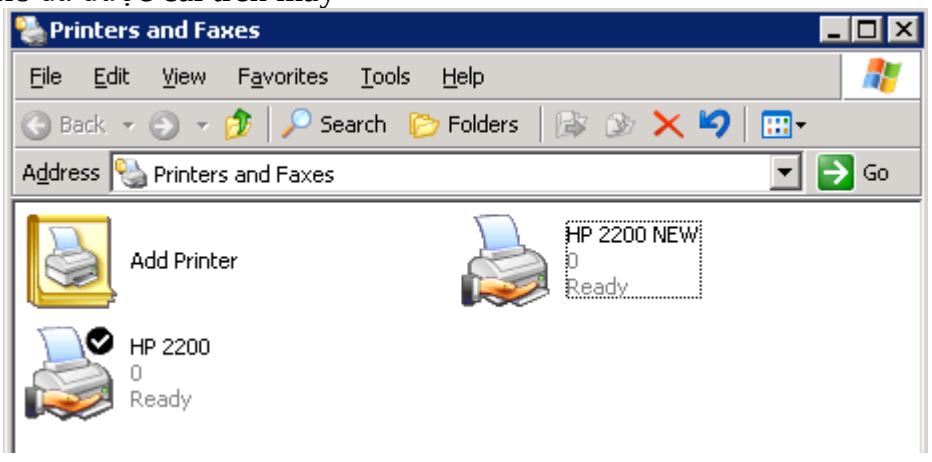
Click vào Finish để kết thúc, bạn đợi vài giây để hệ thống cài đặt

Hình 9.30 Hoàn thành cài máy in

Tương tự, cài đặt printer thứ 2:

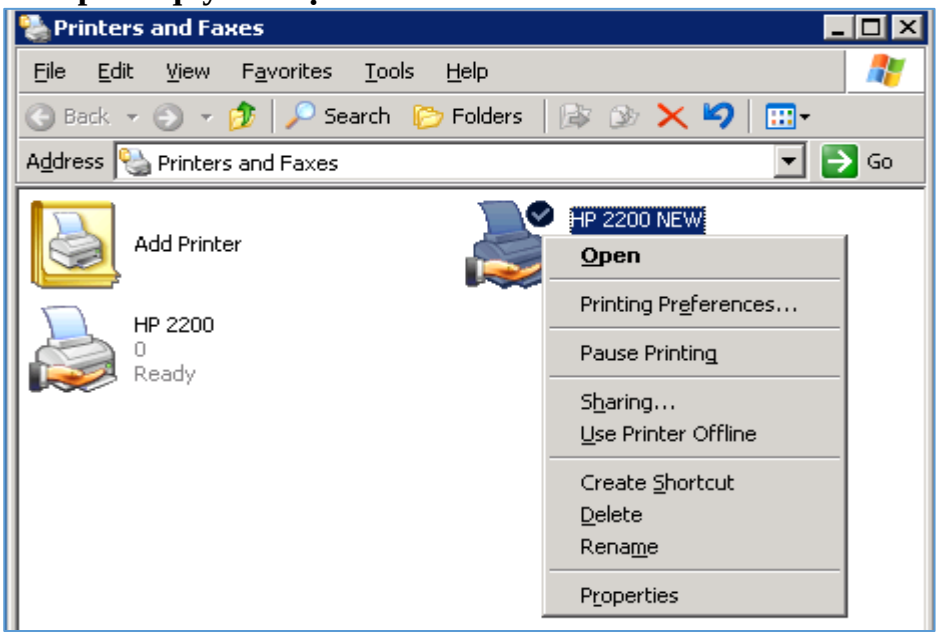
Chọn port LPT2, chọn cùng hãng HP và cùng loại máy in, đặt tên máy in là HP 2200 NEW, Share với tên là HP NEW, nhập địa điểm của máy in(nhập tên DN trong khung Location)

Hai Printers đã được cài trên máy



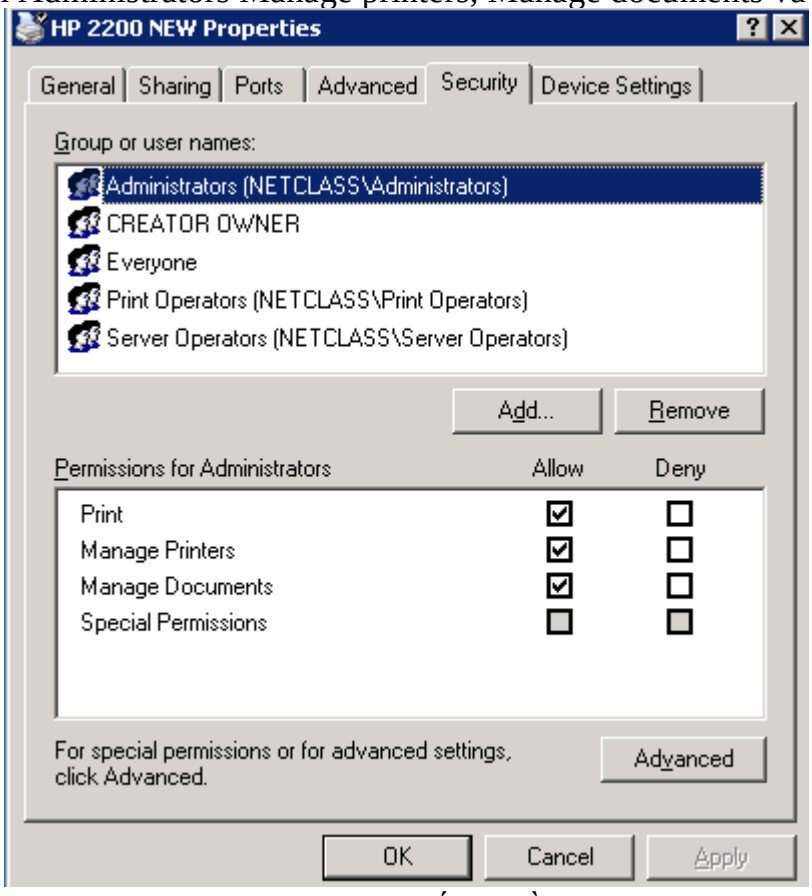
Hình 9.31 Chia sẻ máy in

b). Chia sẻ và phân quyền được in ấn:



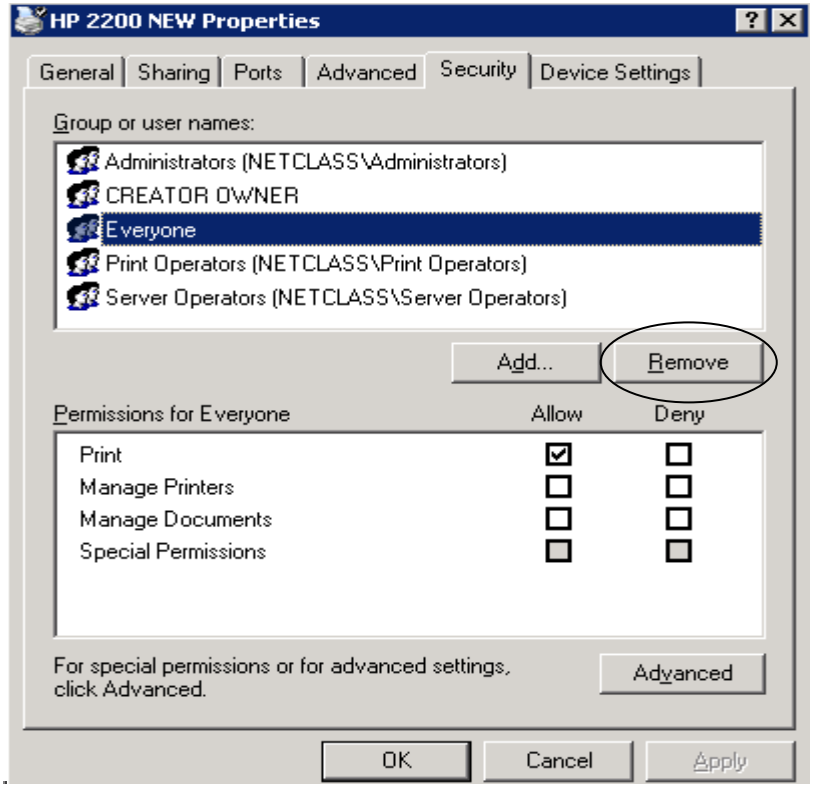
Hình 9.32 Mở thuộc tính

Gán cho nhóm Administrators Manage printers, Manage documents và print



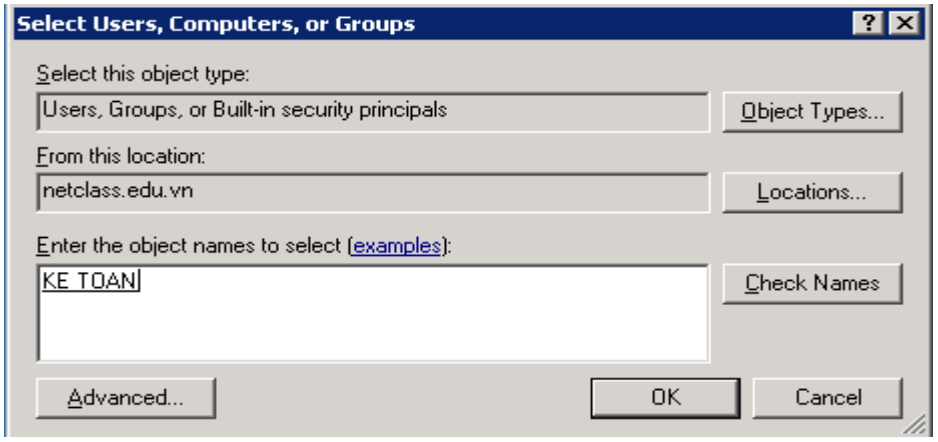
Hình 9.33 Cấp quyền

Xoá bỏ nhóm Everyone



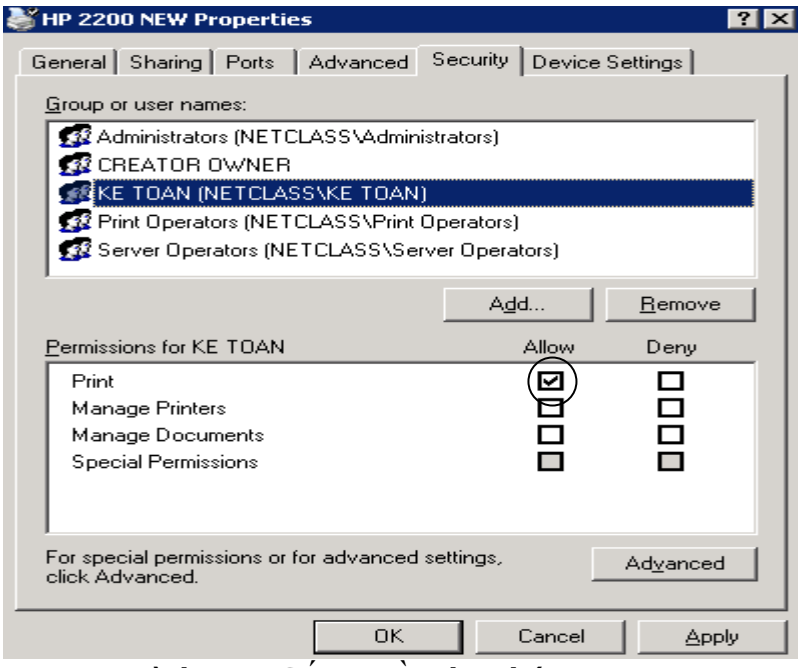
Hình 9.34 Xóa Everyone

Đưa thêm nhóm KE TOAN vào ACL



Hình 9.35 Đưa nhóm Ketoan vào

Gán cho nhóm KE TOAN được quyền Print

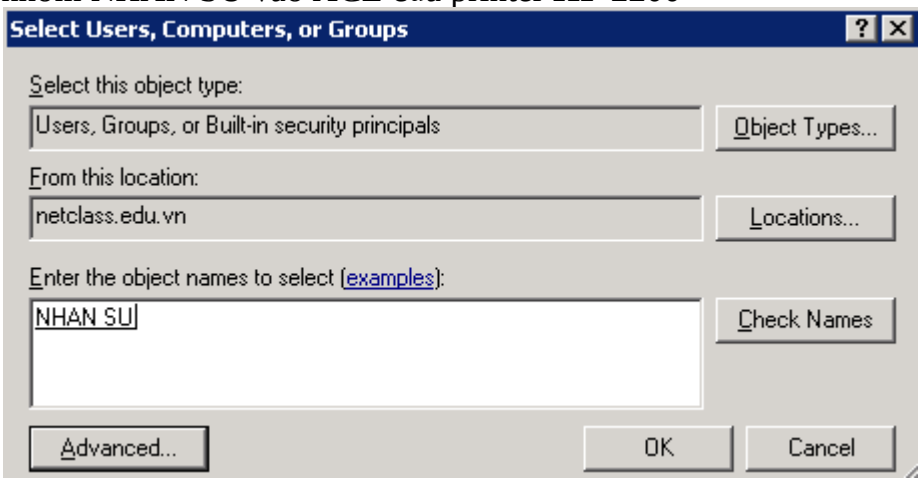


Hình 9.36 Cấp quyền cho nhóm Ketoan

Bây giờ chuyển qua làm permission cho printer HP 2200. Cách thực hiện tương tự như trên

Cho nhóm Everyone ra khỏi ACL

Đưa nhóm NHAN SU vào ACL của printer **HP 2200**

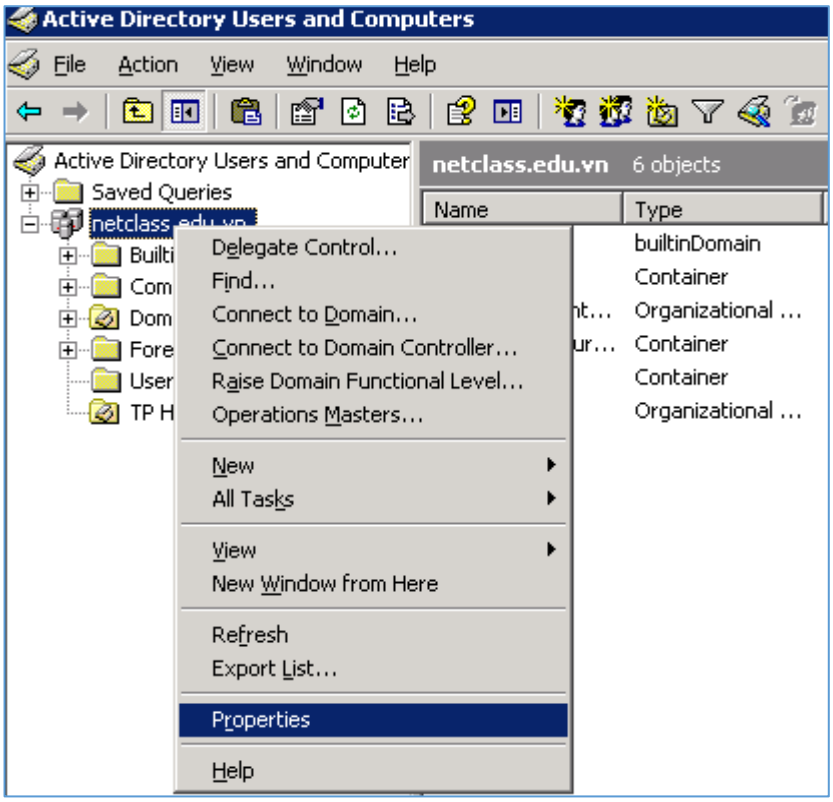


Hình 9.37 Chọn nhóm NHAN SU

Cho nhóm đó được quyền print

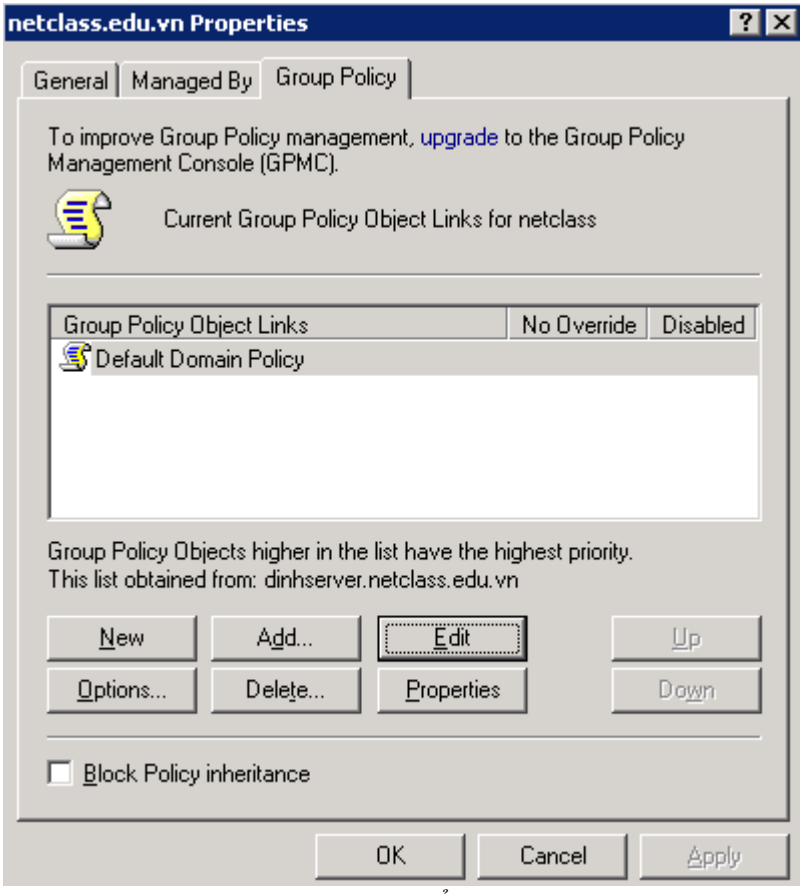
2. Tìm kiếm máy in trên mạng bằng địa điểm

Vào Active Directory Sites Users and Computers



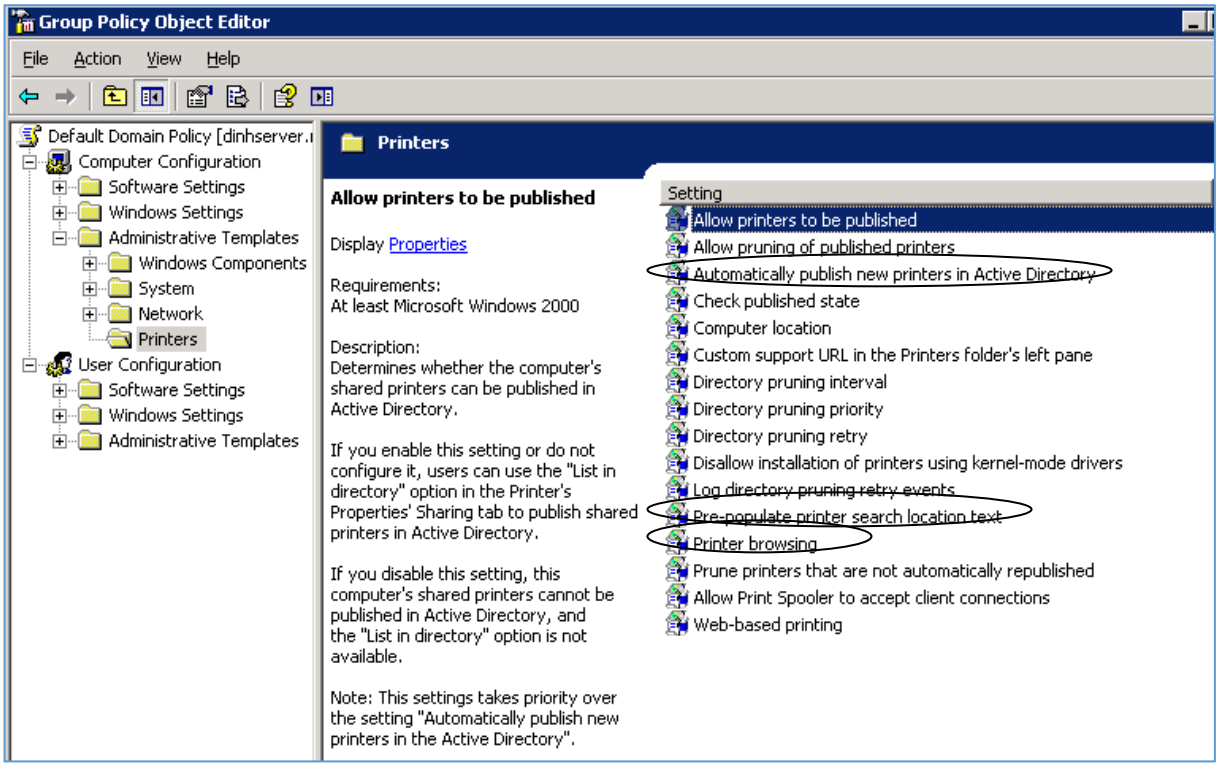
Hình 9.38 Mở Properties

Click vào properties



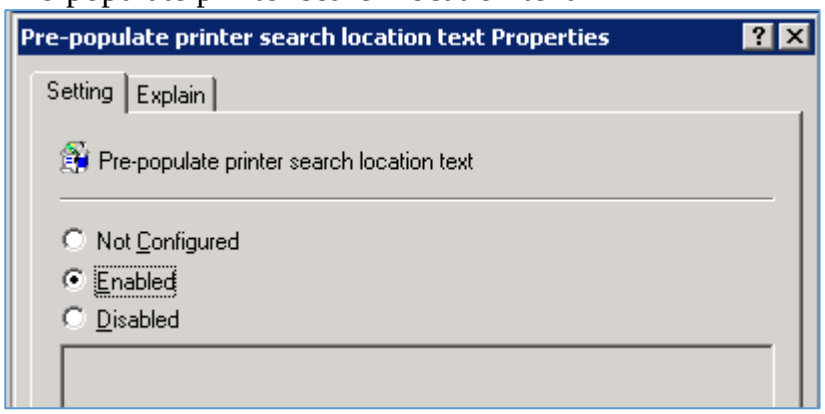
Hình 9.39 Cửa Sổ chính sách

Group policyObject Editor mở ra



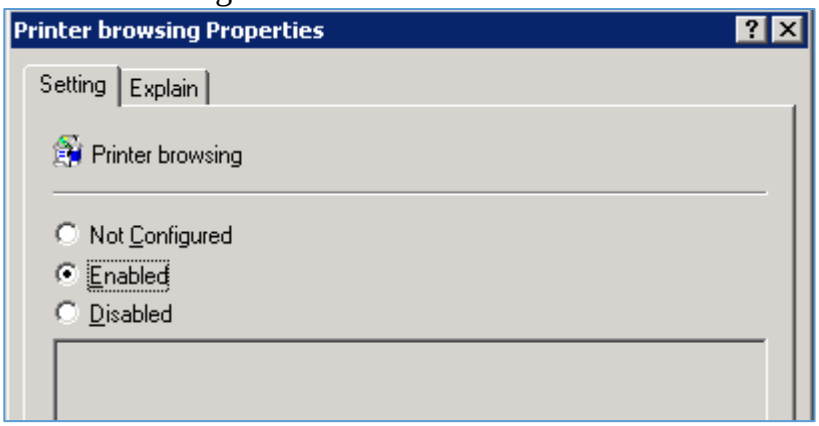
Hình 9.40 Cửa sổ Group policyObject Editor

Mở tính năng Pre-populate printer search location text



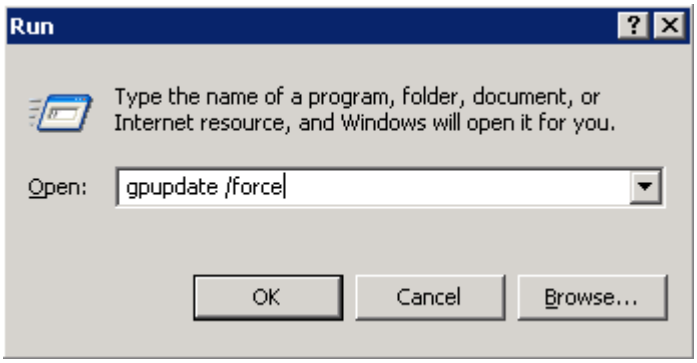
Hình 9. Mở tính năng Pre-populate

Và tính năng Printer browsing



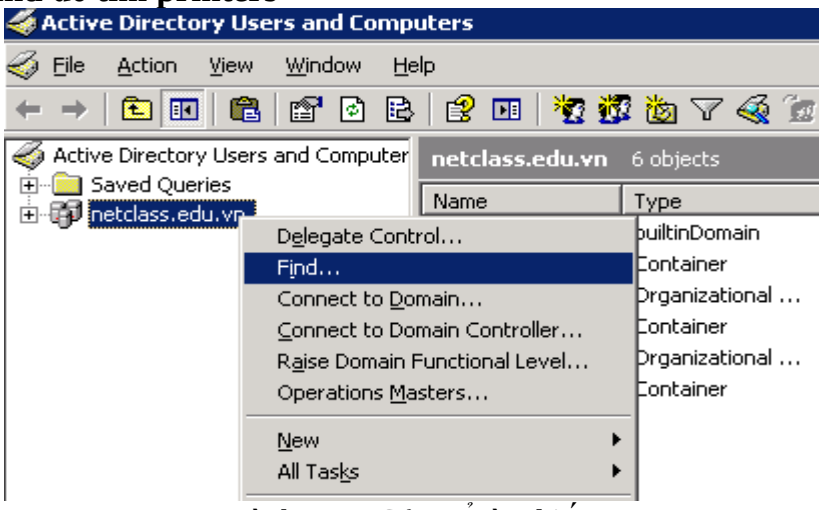
Hình 9.41 Bật tính năng Printer browsing

Refresh group policy



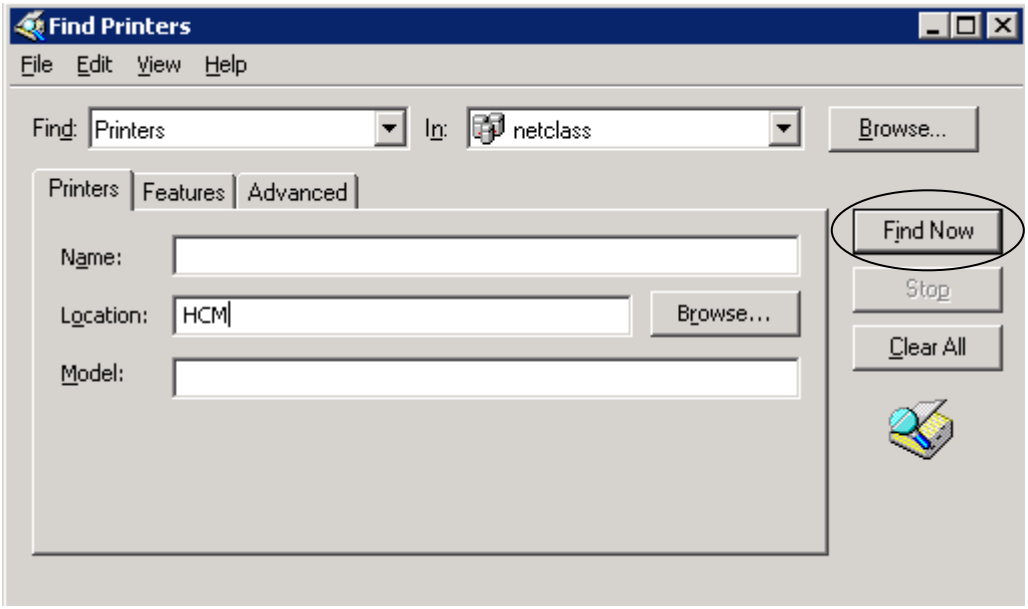
Hình 9.42 Cập nhật chính sách

Dùng lệnh Find để tìm printers



Hình 9.43 Cửa sổ tìm kiếm

Điền vào ô location

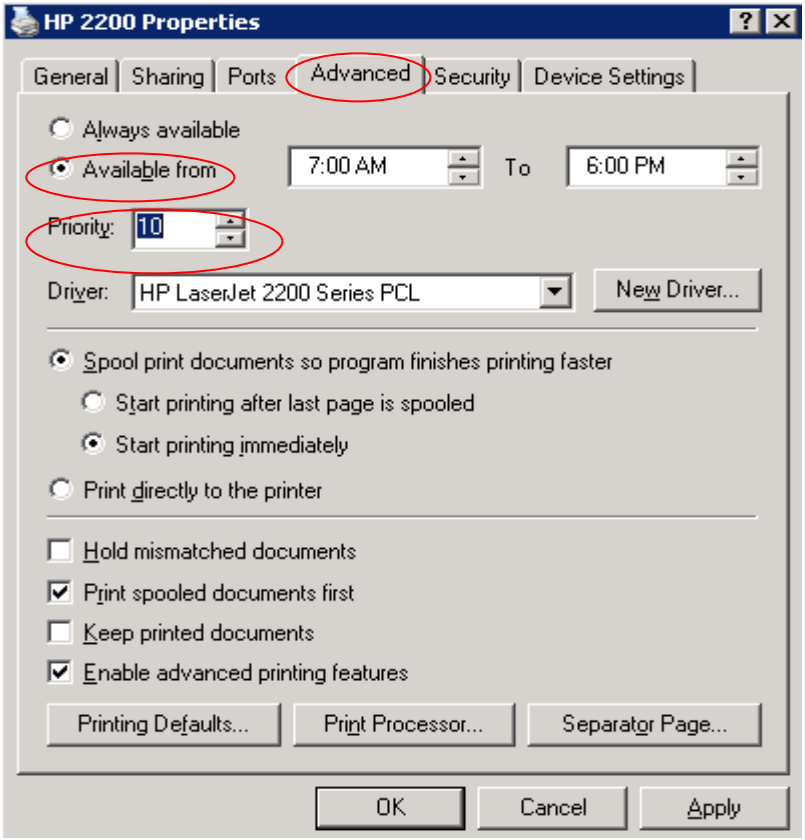


Hình 9.44 Nhập thông tin tìm kiếm

Click vào Find Now

3. Thiết lập đọ ưu tiên và tính sẵn sàng in.

Right click vào biểu tượng máy in **HP 2200** chọn **properties** để cấu hình printer pool, vào thẻ **Advanced** để cấu hình:



Hình 9.45 Chọn độ ưu tiên

Tương tự Right click vào biểu tượng máy in **HP 2200 NEW** chọn **properties,** vào thẻ **Advanced**, thay đổi giá trị bằng 50 tại khung **Priority** thì khi in trên máy in này sẽ có độ ưu tiên chậm hơn so với máy in **HP 2200.**

Những trọng tâm cần chú ý:

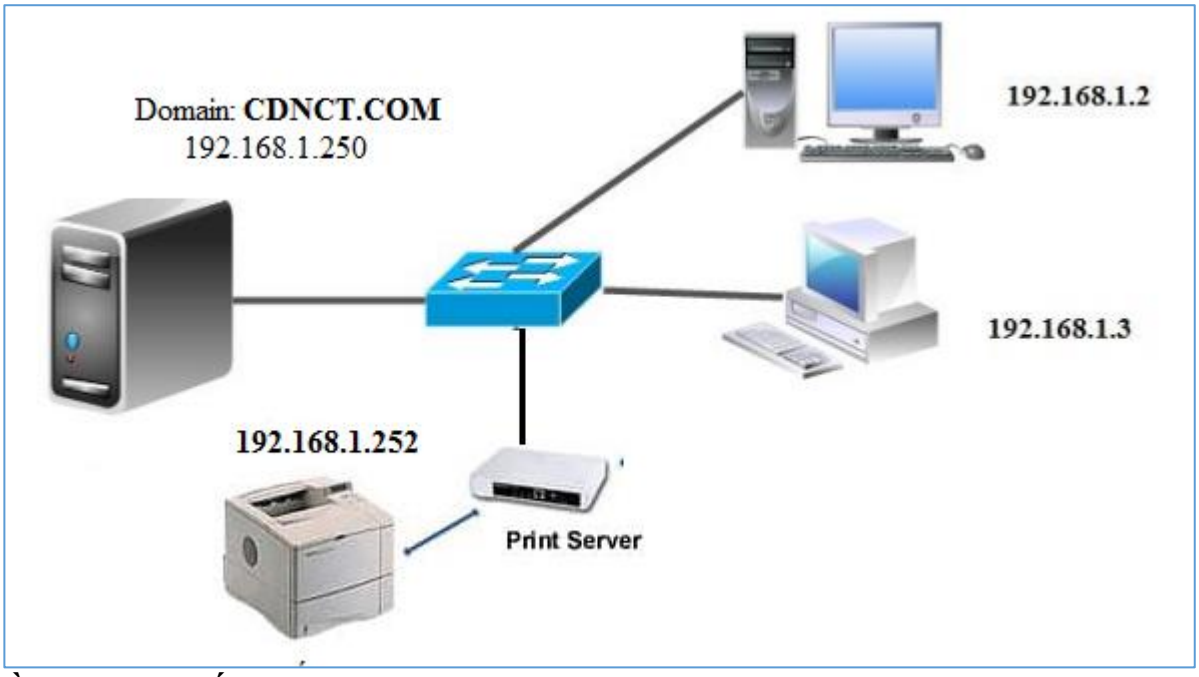
- Cài đặt được 2 máy in đúng yêu cầu của hệ thống.
- Chia sẻ đúng theo các quyền cho từng User và Group
- Cấu hình độ ưu tiên cho tưng máy và từng User và Group.
- Tìm kiếm máy in trên mạng từ các Client
- Thiết lập thời gian in cho từng User và Group
- Quản lý việc in ấn trên server
- Cấp quyền in cho người dùng/nhóm người dùng

Bài mở rộng và nâng cao

Yêu cầu:

Sử dụng dịch vụ Print Management với Group Policy để tự động cài đặt máy in và driver tự động cho các User hoặc Computer trong công ty (Mọi thứ automatic trên Server, và mọi thay đổi trên server cũng apply xuống user hết)

Mô hình



Yêu cầu đánh giá kết quả học tập

Nội dung

- Về kiến thức:
  + Trình bày được Chức năng Quản lý máy in trên Windows Server
  + Trình bày được các bước Quản lý máy in trên Windows Server 2019
- Về kỹ năng:
  + Thao tác thành thạo việc Quản lý đĩa trên Windows Server 2019.
  + Thao tác thành thạo việc sử dụng máy in chạy qua port TCP trên DC của Windows Server 2019
  + Thực hiện đúng các bước cài máy in tự động trên Server
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Phương pháp

- Về kiến thức: Đánh giá bằng hình thức kiểm tra viết, trắc nghiệm, vấn đáp.
- Về kỹ năng:
  + Đánh giá kỹ năng thực hành về các thao tác Quản lý đĩa và giới hạn đĩa trên Windows Server 2019.
  + Đánh giá kỹ năng thực hành về các bước cài máy in tự động trên Server.
  + Thực hiện đúng sử dụng máy in chạy qua port TCP
- Năng lực tự chủ và trách nhiệm: Tỉ mỉ, cẩn thận, chính xác, linh hoạt và ngăn nắp trong công việc.

Điều kiện để hoàn thành mô đun để được dự thi kết thúc mô đun:

+ Người học tham dự ít nhất 70% thời gian học lý thuyết và đầy đủ các bài học tích hợp, bài học thực hành, thực tập

+ Điểm trung bình chung các điểm kiểm tra đạt từ 5,0 điểm trở lên theo thang điểm 10;

+ Người học có giấy xác nhận khuyết tật theo quy định thì được hiệu trưởng xem xét, quyết định ưu tiên điều kiện dự thi trên cơ sở sinh viên đó phải bảo đảm điều kiện về điểm trung bình các điểm kiểm tra.

+ Số lần dự thi kết thúc mô đun theo quy định tại khoản 2 Điều 13 Thông tư 09/2017/TT-BLĐTBXH, ngày 13 tháng 3 năm 2017.

Điều kiện để được công nhận, cấp chứng nhận đạt mô đun đào tạo:

Người học được công nhận và cấp chứng nhận đạt mô đun này khi có điểm trung bình mô đun theo thang điểm 10 đạt từ 4,0 trở lên

TÀI LIỆU THAM KHẢO

[1]. Hoàn Vũ(Biên soạn), KS. Nguyễn Công Sơn(Chủ biên); *Hướng Dẫn Quản Trị Mạng Microsoft Windows Server*; Tổng Hợp TP. Hồ Chí Minh, Năm 2014.

[2]. Trung tâm Điện toán và Truyền số liệu KV1, *Giáo trình Thiết kế và xây dựng mạng LAN và WAN*; Năm 2012.

[3]. VN-GUIDE(Tổng hợp và biên dịch); *Quản Trị Mạng Microsoft Windows*; Năm 2012.

[4]. Nguyễn Thanh Quang(Sưu tầm và biên soạn), Hoàng Anh Quang(Sưu tầm và biên soạn); *Bảo Mật Và Quản Trị Mạng*; Văn Hóa Thông Tin, Năm 2006.

[5]. Phạm Hồng Tài, *Thủ Thuật Quản Trị Mạng Windows*, Thống kê, Năm 2012.