BỘ CÔNG THƯƠNG

TRƯỜNG CĐ THƯƠNG MẠI VÀ DU LỊCH

GIÁO TRÌNH

MÔN HỌC: THỰC HÀNH MẠNG VÀ QUẢN TRỊ MẠNG

NGÀNH: THƯƠNG MẠI ĐIỆN TỬ

TRÌNH ĐỘ: TRUNG CẤP

(*Ban hành kèm theo Quyết định số 404 /QĐ- CĐTMDL ngày 05 tháng 07 năm 2022 của Hiệu trưởng Trường Cao đẳng Thương mại và Du lịch)*

Thái Nguyên, năm 2022

(Lưu hành nội bộ)

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 Thương mại điện tử ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Thương mại điện tử 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.

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

Giáo trình này phục vụ cho học sinh học nghề Thương mại điện tử trường Cao đẳng Thương mại và Du lịch.

Giáo trình gồm hai nội dung chính sau:

Phần 1: Mạng căn bản – Thực hành các kỹ thuật bấm dây cáp mạng, kết nối, lắp đặt các thiết bị phần cứng và cài đặt phần mềm trong hệ thống mạng nội bộ LAN

Phần 2: Quản trị mạng Windows Server – Thực hiện quản trị hệ thống mạng máy tính trên mô hình Client – Server. Cài đặt và cấu hình các dịch vụ mạng trên hệ thống này.

Giáo trình cũng cung cấp một số kiến thức lý thuyết cơ bản, dựa vào đó thực hiện các kỹ thuật , kỹ năng cần thiết để thiết kế, cài đặt mạng máy tính và cấu hình các dịch vụ trong quản trị hệ thống mạng máy tính theo mô hình Client – Server. Hy vọng sẽ có ích cho các bạn học sinh muốn tìm hiểu và xây dựng các hệ thống tin học ứng dụng phục vụ cho sản xuất, quản lý trong các doanh nghiệp. Mặc dù đã 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!

Nhóm tác giả

MỤC LỤC

GIÁO TRÌNH MÔN HỌC

1. Tên môn học: Thực hành mạng và Quản trị mạng

2. **Mã môn học:** MH20

3. Vị trí, tính chất, ý nghĩa và vai trò của môn học của môn học:

3.1. Vị trí: Môn học Thực hành mạng và Quản trị mạng là môn học chuyên môn nghề Thương mại điện tử được bố trí giảng dạy sau các môn học cơ sở trong chương trình đào tạo trình độ Trung cấp

3.2. Tính chất: Chương trình môn học Thực hành mạng và Quản trị mạng bao gồm một số nội dung cơ bản về mạng căn bản, quản trị mạng máy tính sử dụng hệ điều hành Windows Server.

3.3. Ý nghĩa và vai trò của môn học: Thực hành mạng và Quản trị mạng là môn học thực hành dành cho đối tượng là người học thuộc chuyên ngành Thương mại điện tử. Nội dung chủ yếu của môn học này nhằm cung cấp các kiến thức và kỹ năng thực hành mạng căn bản và quản trị mạng máy tính sử dụng hệ điều hành máy chủ Windows Server theo mô hình Client – Server

4. Mục tiêu môn học:

4.1. Về kiến thức:

A1. Hiểu được các bước thực hiện bấm dây cáp mạng, kết nối thiết bị và chia sẻ dữ liệu, thiết bị dùng chung trong mạng nội bộ

A2. Hiểu được các bước thực hiện cài đặt hệ điều hành Windows Server

A3. Hiểu được các bước thực hiện cài đặt các dịch vụ mạng trên hệ điều hành Windows Server theo mô hình Client – Server

4.2. Về kỹ năng

B1. Thực hiện được kỹ thuật bấm dây cáp mạng, kết nối thiết bị và chia sẻ dữ liệu, thiết bị dùng chung trong mạng nội bộ

B2. Thực hiện được các bước cài đặt hệ điều hành Windows Server

B3. Thực hiện được các bước cài đặt các dịch vụ mạng trên hệ điều hành Windows Server theo mô hình Client – Server

4.3. Về năng lực tự chủ và trách nhiệm:

C1. Ý thức được tầm quan trọng và ý nghĩa thực tiễn của mạng máy tính và quản trị mạng máy tính trong hoạt động của cơ quan, doanh nghiệp.

C2. Làm việc độc lập, làm việc theo nhóm.

C3. Tuân thủ nội quy, quy định nơi làm việc.

5. Nội dung của môn học

5.1. Chương trình khung

Mã MH	Tên môn học	Số tín	Thời gian học tập (giờ)	
			Tổng	Trong đó

		chỉ	số	Lý thuyết	Thực hành/ thực tập/ bài tập/thảo luận	Kiểm tra
I	**Các môn học chung**	**12**	**255**	**94**	**148**	**13**
MH01	Chính trị	2	30	15	13	2
MH02	Pháp luật	1	15	9	5	1
MH03	Giáo dục thể chất	1	30	4	24	2
MH04	Giáo dục quốc phòng và an ninh	2	45	21	21	3
MH05	Tin học	2	45	15	29	1
MH06	Ngoại ngữ	4	90	30	56	4
II	**Các môn học chuyên môn**	**64**	**1590**	**511**	**1035**	**44**
II.1	***Môn học cơ sở***	***15***	***225***	***184***	***31***	***10***
MH07	Kinh tế vi mô	3	45	43	-	2
MH08	Thương mại điện tử căn bản	3	45	43	-	2
MH09	Pháp luật thương mại điện tử	2	30	28	-	2
MH10	Mạng máy tính	2	30	15	14	1
MH11	Marketing điện tử	2	30	28	-	2
MH12	Quản trị cơ sở dữ liệu	3	45	27	17	1
II.2	***Các môn học chuyên môn***	***47***	***1335***	***298***	***1004***	***33***
MH13	Tiếng Anh thương mại	4	60	57	-	3
MH14	Nghiệp vụ kinh doanh TM dịch vụ	4	60	57	-	3
MH15	Quản trị tác nghiệp TMĐT	4	60	57	-	3
MH16	Nghiệp vụ vận tải, giao nhận và bảo hiểm trong TMĐT	3	45	43	-	2
MH17	Khai báo hải quan điện tử	2	30	28	-	2
MH18	Thanh toán điện tử	2	30	28	-	2
MH19	An toàn hệ thống thông tin	2	30	28	-	2
MH20	Thực hành mạng và quản trị mạng	3	90	-	86	4
MH21	TH tác nghiệp TMĐT	3	90	-	86	4
MH22	TH vận tải, giao nhận và bảo hiểm trong TMĐT	2	60	-	56	4
MH23	TH khai báo hải quan ĐT	2	60	-	56	4
MH24	Thực tập tốt nghiệp	16	720		720	
II.3	***Các môn học, mô đun tự chọn***	***2***	***30***	***28***	***-***	***2***
MH25	Kỹ năng bán hàng trực tuyến	2	30	28	-	2
MH26	Khởi sự kinh doanh	2	30	28	-	2
	Tổng cộng	**76**	**1845**	**605**	**1183**	**57**

5.2. Chương trình chi tiết môn học

Số TT	Tên chương, mục	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm tra
I	**Phần 1: Mạng căn bản**	**30**	**0**	**29**	**1**
1	Bài 1: Bấm dây cáp mạng	5	0	5	0
2	Bài 2: Kết nối thiết bị	10	0	10	0
3	Bài 3: Chia sẻ dữ liệu và máy in	14	0	14	0
	Kiểm tra	1			1
I	**Phần 2: Quản trị mạng Window server**	**60**	**0**	**57**	**3**
1	Bài 1: Cài đặt và cấu hình Windows Server	5	0	5	0
2	Bài 2: Cài đặt và cấu hình Active Directory	4	0	4	0
	Kiểm tra	1			1
3	Bài 3: Quản trị tài khoản người dùng trên Active Directory – Tạo OU, Group, User	10	0	10	0
4	Bài 4: Triển khai chính sách Group Policy	9	0	9	0
	Kiểm tra	1			1
5	Bài 5: Cài đặt và cấu hình dịch vụ DHCP	5	0	5	0
6	Bài 6: Cài đặt và cấu hình dịch vụ DNS	10	0	10	0
7	Bài 7: Triển khai dịch vụ Web với IIS	5	0	5	0
8	Bài 8: Triển khai dịch vụ FTP với IIS	5	0	5	0
9	Bài 9: Triển khai dịch vụ Email (Mail Server)	4	0	4	0
	Kiểm tra	1			1
	Cộng	**90**	**0**	**86**	**4**

6. Điều kiện thực hiện môn học:

6.1. Phòng học chuyên môn / nhà xưởng:

- Phòng học thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

6.2. Trang thiết bị máy móc:

- Máy tính, máy chiếu

6.3. Học liệu, dụng cụ, nguyên vật liệu:

- Giáo án, bài giảng.
- Phần mềm hệ điều hành Windows Server.
- Dây mạng, kìm bấm mạng, các đầu nối RJ45, Hub, Switch, Router.
- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng.

6.4. Các điều kiện khác: Không

7. Nội dung và phương pháp đánh giá:

7.1. Nội dung:

- Kiến thức: Đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức
- Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kỹ năng.
- Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp.

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

7.2. Phương pháp:

7.2. Phương pháp:

Người học được đánh giá tích lũy môn học như sau:

7.2.1. Cách đánh giá

- Áp dụng quy chế đào tạo trình độ trung cấp hệ chính quy ban hành kèm theo Thông tư số 04/2022/TT-LĐTBXH, ngày 30/3/2022 của Bộ trưởng Bộ Lao động – Thương binh và Xã hội.

- Quy định việc tổ chức thực hiện chương trình đào tạo trình độ trung cấp, trình độ cao đẳng theo niên chế hoặc theo phương thức tích lũy mô-đun hoặc tín chỉ của Nhà trường ban hành kèm theo Quyết định số 706/QĐ-CĐTMDL ngày 14 tháng 11 năm 2017 của Hiệu trưởng Trường cao đẳng Thương mại và Du lịch về tổ chức đào tạo, kiểm tra, thi, đánh giá kết quả học tập và xét công nhận tốt nghiệp

Điểm đánh giá	Trọng số

+ Điểm kiểm tra thường xuyên (Hệ số 1)	40%
+ Điểm kiểm tra định kỳ (Hệ số 2)	
+ Điểm thi kết thúc môn học	60%

7.2.2. Phương pháp đánh giá

Phương pháp đánh giá	Phương pháp tổ chức	Hình thức kiểm tra	Thời điểm kiểm tra
Thường xuyên	Thực hành	Thực hành	Sau 15 giờ.
Định kỳ	Thực hành	Thực hành	Sau 35 giờ
Kết thúc môn học	Thực hành	Thực hành	Sau 90 giờ

7.2.3. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc môn học được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến một chữ số thập phân.

- Điểm môn học là tổng điểm của tất cả điểm đánh giá thành phần của môn học nhân với trọng số tương ứng. Điểm môn học theo thang điểm 10 làm tròn đến một chữ số thập phân, sau đó được quy đổi sang điểm chữ và điểm số theo thang điểm 4 theo quy định của Bộ Lao động Thương binh và Xã hội về đào tạo theo tín chỉ.

8. Hướng dẫn thực hiện môn học

8.1. Phạm vi, đối tượng áp dụng: Môn học được sử dụng để giảng dạy cho nghề Thương mại điện tử. Tổng thời gian thực hiện môn học là: 90 giờ, giáo viên giảng các giờ thực hành.

8.2. Phương pháp giảng dạy, học tập môn học

8.2.1. Đối với người dạy:

*** Lý thuyết:** Áp dụng phương pháp dạy học tích cực bao gồm: thuyết trình ngắn, nêu vấn đề, hướng dẫn đọc tài liệu, bài tập tình huống, câu hỏi thảo luận….

* **Bài tập:** Phân chia nhóm nhỏ thực hiện bài tập theo nội dung đề ra.

*** Thực hành:** Phân chia thực hành theo nội dung đề ra.

*** Hướng dẫn tự học theo nhóm:** Nhóm trưởng phân công các thành viên trong nhóm tìm hiểu, nghiên cứu theo yêu cầu nội dung trong bài học, cả nhóm thảo luận, trình bày nội dung, ghi chép và viết báo cáo nhóm.

8.2.2. Đối với người học:

- Nghiên cứu kỹ bài học tại nhà trước khi đến lớp. Các tài liệu tham khảo sẽ được cung cấp nguồn trước khi người học vào học môn học này (trang web, thư viện, tài liệu...)

- Tham dự tối thiểu 80% các buổi giảng lý thuyết. Nếu người học vắng >20% số tiết lý thuyết phải học lại môn học mới được tham dự kì thi lần sau.

- Tự học và thảo luận nhóm: là một phương pháp học tập kết hợp giữa làm việc theo nhóm và làm việc cá nhân. Một nhóm gồm 8-10 người học sẽ được cung cấp chủ

đề thảo luận trước khi học lý thuyết, thực hành. Mỗi người học sẽ chịu trách nhiệm về 1 hoặc một số nội dung trong chủ đề mà nhóm đã phân công để phát triển và hoàn thiện tốt nhất toàn bộ chủ đề thảo luận của nhóm.

- Tham dự đủ các bài kiểm tra thường xuyên, định kỳ.
- Tham dự thi kết thúc môn học.
- Chủ động tổ chức thực hiện giờ tự học.

9. Tài liệu tham khảo:

(1) Phạm Hoàng Dũng, *Làm chủ Windows 2003 server*, Nhà xuất bản Thống Kê

(2) Microsoft. *Installing and Configuring Windows Server 2012*. Microsoft Learning, 2012.

(3) BACHKHOA-APTECH, *Quản trị hệ thống mạng Windows Server*, 2018

(4) TS Phan Thị Thu Hồng, *Bài giảng Quản trị mạng*, Học viện Nông nghiệp Việt Nam

PHẦN 1: MẠNG CĂN BẢN

❖ GIỚI THIỆU PHẦN 1

Phần 1 là phần thực hành các kiến thức mạng máy tính căn bản.

❖ MỤC TIÊU PHẦN 1

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được các kỹ thuật bấm dây cáp mạng, cách kết nối, lắp đặt các thiết bị phần cứng và cài đặt phần mềm trong hệ thống mạng nội bộ LAN.
- Vận dụng được các kiến thức trên vào thực hành.

➢ ***Về kỹ năng:***

- Thực hiện được các kỹ thuật bấm dây cáp mạng, kết nối, lắp đặt các thiết bị phần cứng và cài đặt phần mềm trong hệ thống mạng nội bộ LAN.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của việc thực hiện các kỹ thuật bấm dây cáp mạng, kết nối, lắp đặt các thiết bị phần cứng và cài đặt phần mềm trong hệ thống mạng nội bộ LAN.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP PHẦN 1

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, thao tác mẫu); yêu cầu người học thực hiện thực hành phần 1 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (phần 1) trước buổi học; hoàn thành đầy đủ bước thực hành và bài tập phần 1 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN PHẦN 1

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Phần mềm hệ điều hành Windows Server.
- Dây mạng, kìm bấm mạng, các đầu nối RJ45, Hub, Switch, Router.

- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ PHẦN 1**

- **Nội dung:**

✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức

✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.

✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: 1 điểm kiểm tra (hình thức: thực hành)

✓ Kiểm tra định kỳ: 1 điểm kiểm tra (hình thức: thực hành)

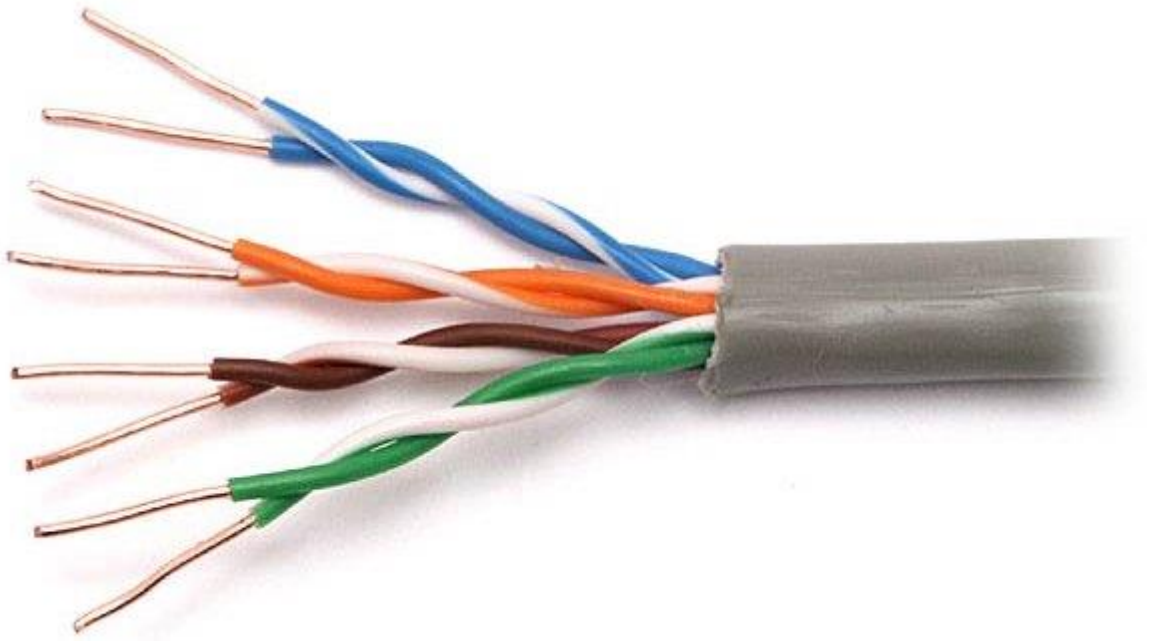
BÀI 1: BẤM DÂY CÁP MẠNG

I. Lý thuyết liên quan

1. Dây cáp mạng

Cáp mạng và cáp thông tin liên lạc là phần cứng mạng được sử dụng để kết nối một thiết bị mạng này với các thiết bị mạng khác, ví dụ, kết nối hai hoặc nhiều máy tính để chia sẻ máy in và máy scan; kết nối nhiều máy chủ với một bộ chuyển mạch Access Switch. Phạm vi bao gồm các tập hợp dữ liệu và cáp Ethernet, bao gồm cáp xoắn đôi, cáp đồng trục, cáp quang, đường dây điện, v.v... Cáp xoắn đôi, cáp đồng trục và cáp quang là những loại phổ biến nhất.

Cáp xoắn đôi là một loại dây dẫn trong đó hai dây dẫn (thường là đồng) của một mạch đơn được xoắn lại với nhau. Tại sao các cặp xoắn lại với nhau? Bởi vì hai dây dẫn mang tín hiệu tương đương nhưng ngược chiều nhau, một cặp có thể gây ra nhiễu xuyên âm tới các cặp khác và hiệu ứng trở nên mạnh mẽ hơn dọc theo chiều dài của cáp. Điều này không hề có lợi đối với việc truyền tín hiệu. Việc xoắn các cặp giảm nhiễu xuyên âm giữa các dây. Cáp xoắn đôi thường được sử dụng trong các mạng dữ liệu cho các kết nối ngắn và trung bình, vì chi phí thấp hơn so với cáp quang và cáp đồng trục.



Hình 1.1.1 – Cáp xoắn đôi

Cáp xoắn đôi được chia theo các loại sau:

- Cáp STP (Shielded Twisted Pair)

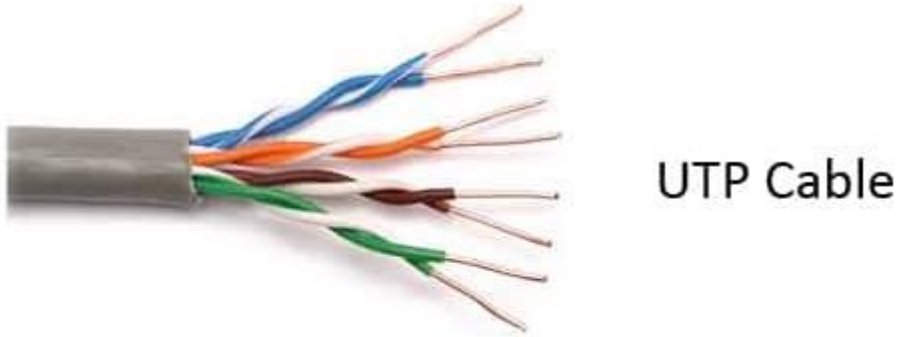
Cáp xoắn đôi được che chắn bởi vỏ chống nhiễu được gọi là cáp xoắn được bảo vệ (STP). Cáp STP được chia thành loại có vỏ chống nhiễu chung và vỏ chống nhiễu riêng. Cáp STP với vỏ chống nhiễu riêng có lá nhôm cho mỗi cặp xoắn hoặc hai cặp xoắn một. Loại vỏ chống nhiễu này bảo vệ cáp khỏi hiện tượng nhiễu điện từ bên ngoài (EMI) vào hoặc ra khỏi cáp, và cũng bảo vệ các cặp xoắn lân cận khỏi hiện tượng nhiễu xuyên âm. Cáp Overall shielded twisted pair (OSTP) có vỏ chống nhiễu chung hoặc vỏ chống nhiễu riêng trên tất cả các cặp trong cáp xoắn đôi. Loại vỏ chống

nhiễu này giúp ngăn EMI xâm nhập hoặc thoát khỏi cáp. Một cáp STP có thể có cả vỏ chống nhiễu chung và riêng.

Hình 1.1.2 – Cáp STP

- Cáp UTP (Unshielded Twisted Pair)

Cáp UTP không có vỏ chống nhiễu dễ bị ảnh hưởng bởi hiện tượng nhiễu từ bên ngoài. Vì lý do đó, loại cáp này thường được tìm thấy trong các ứng dụng điện thoại trong nhà. Cáp điện thoại ngoài trời chứa hàng trăm hoặc hàng ngàn cặp. Các cặp có cùng tốc độ xoắn trong cáp có thể phải chịu một số mức độ nhiễu xuyên âm, vì vậy các cặp dây này thường được lựa chọn cẩn thận trong một cáp lớn để giảm hiện tượng nhiễu xuyên âm.



Hình 1.1.3 – Cáp UTP

Hầu hết cáp UTP sử dụng đầu nối RJ45, trông giống như đầu nối điện thoại (RJ11) nhưng có 8 dây thay vì 4 dây.

Hình 1.1.4 – Đầu nối RJ45

Bảng sau cung cấp thông tin cơ bản về một số cáp xoắn đôi

Tên	Cấu trúc điển hình	Băng thông	Ứng dụng
Cat 3	UTP	16 MHz	Cáp Ethernet 10BASE-T và 100BASE-T4
Cat 4	UTP	20 MHz	Token Ring 16Mbit/s
Cat 5	UTP	100 MHz	Cáp Ethernet 100BASE-TX & 1000BASE-T
Cat 5e	UTP	100 MHz	Cáp Ethernet 100BASE-TX & 1000BASE-T
Cat 6	STP	250 MHz	Cáp Ethernet 10GBASE-T
Cat 6a	STP	500 MHz	Cáp Ethernet 10GBASE-T
Cat 7	STP	600 MHz	Cáp Ethernet 10GBASE-T hoặc POTS/CATV/1000BASE-T qua cáp đơn
Cat 7a	STP	1000 MHz	Cáp Ethernet 10GBASE-T hoặc POTS/CATV/1000BASE-T qua cáp đơn

+ Category 3

Cáp Category 3, thường được gọi là Cat 3, là cáp xoắn đôi không có vỏ chống nhiễu (unshielded twisted pair - UTP) được thiết kế để truyền dữ liệu đáng tin cậy lên đến 10 Mbit/giây, với băng thông có thể lên tới 16 MHz. Nó là một phần của các tiêu chuẩn cáp đồng được xác định bởi Liên minh Công nghiệp Điện tử và Hiệp hội Công nghiệp Viễn thông. Cat 3 là định dạng cáp phổ biến vào đầu những năm 1990, nhưng từ đó, nó gần như hoàn toàn được thay thế bằng tiêu chuẩn Cat 5 tương tự, nhưng mang lại tốc độ cao hơn.

+ Category 5

Cáp Category 5, thường được gọi là Cat 5, là một loại cáp xoắn đôi không có vỏ chống nhiễu được thiết kế để đảm bảo tính toàn vẹn tín hiệu cao. Tiêu chuẩn thực tế của Cat 5 xác định các tính chất điện cụ thể của dây, nhưng nó thường được đánh giá bằng khả năng Ethernet là 100 Mbit/s. Chỉ định tiêu chuẩn cụ thể của nó là EIA/TIA-568. Cáp Cat 5 thường có ba cặp xoắn mỗi inch, mỗi cặp xoắn gồm 24 dây đồng. Việc xoắn cáp làm giảm hiện tượng nhiễu điện và nhiễu xuyên âm.

Một đặc điểm quan trọng khác là dây dẫn được cách điện bằng nhựa (FEP) có độ phân tán thấp, có nghĩa là hằng số điện môi của nhựa không phụ thuộc nhiều vào tần số. Cần chú ý đặc biệt để giảm thiểu sự không phù hợp trở kháng tại các điểm kết nối.

Cáp Cat 5 thường được sử dụng trong cáp cấu trúc cho mạng máy tính như Fast Ethernet, mặc dù chúng cũng được sử dụng để truyền nhiều tín hiệu khác như dịch vụ thoại cơ bản, token ring và ATM (lên tới 155 Mbit/giây).

+ Category 5e

Cáp Category 5e là phiên bản nâng cao của Cat 5 để sử dụng với mạng 1000BASE-T (gigabit), hoặc cho các liên kết 100 Base-T đường dài (350 m, so với 100 m đối với Cat 5). Nó phải đáp ứng các tiêu chuẩn EIA/TIA 568A-5. Hầu như tất cả các dây cáp được bán dưới danh nghĩa Cat 5 thực ra là Cat 5e. Các dấu hiệu trên cáp có thể cho biết loại cáp chính xác.

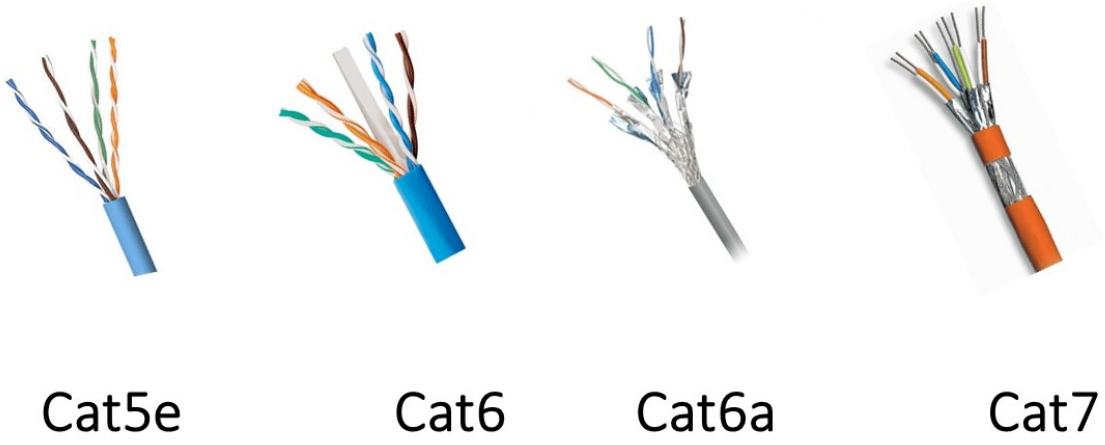
+ Category 6

Tiêu chuẩn cho Gigabit Ethernet và kết nối khác tương thích ngược với cáp Cat 5, Cat 5e và Cat 3. Cat 6 có đặc điểm kỹ thuật nghiêm ngặt hơn để đề phòng nhiễu xuyên âm và nhiễu hệ thống. Tiêu chuẩn cáp phù hợp cho các kết nối 10BASE-T, 100BASE-TX và 1000BASE-T (Gigabit Ethernet).

+ Category 7

Category 7 (CAT7), (ISO/IEC 11801:2002 category 7/lớp F), là chuẩn cáp cho Ethernet siêu nhanh và các công nghệ kết nối khác có thể tương thích ngược với cáp Ethernet CAT5 và CAT6 truyền thống. CAT7 có đặc điểm kỹ thuật nghiêm ngặt hơn để phòng hiện tượng nhiễu xuyên âm và nhiễu hệ thống tốt hơn so với CAT6. Để đạt được điều này, vỏ chống nhiễu đã được thêm vào cho từng cặp dây và toàn bộ cáp

Tiêu chuẩn cáp CAT7 đã được tạo ra để cho phép tín hiệu Ethernet 10 gigabit truyền trên 100m cáp đồng. Cáp có 4 cặp dây đồng xoắn, giống như các tiêu chuẩn trước đó. CAT7 có các đầu nối RJ-45 tương thích GG45 kết hợp tiêu chuẩn RJ-45 và một loại kết nối mới để cho phép truyền dữ liệu mượt mà hơn theo tiêu chuẩn mới. Khi kết hợp với đầu nối GG-45, cáp CAT7 có tần số truyền lên tới 600 MHz.

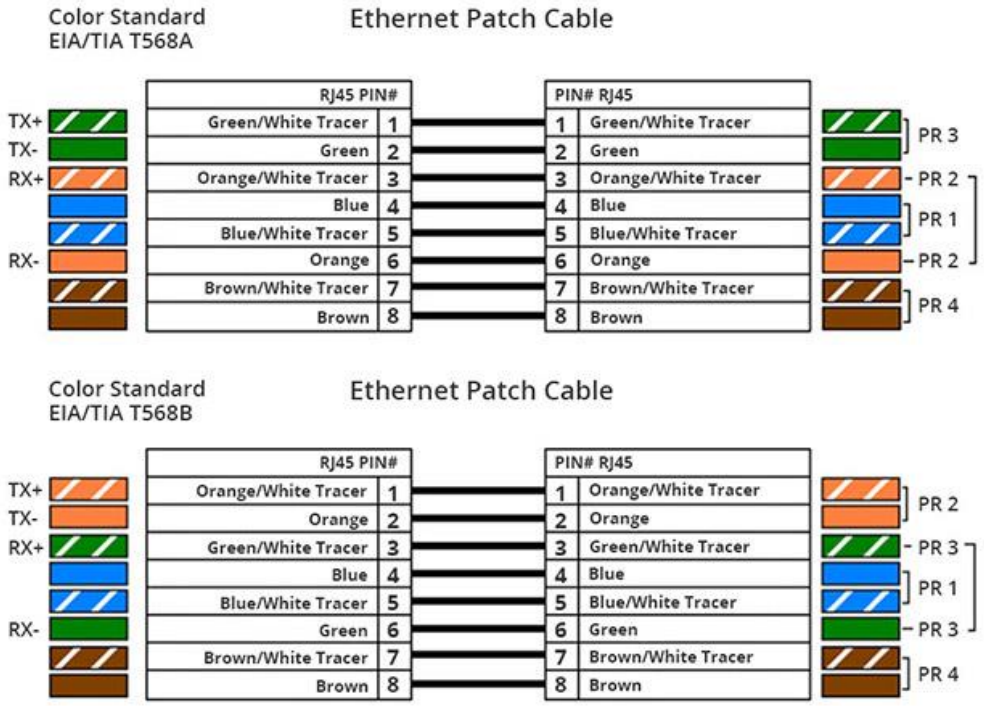


Hình 1.1.5 – Một số loại cáp xoắn đôi

2. Các chuẩn bấm dây cáp mạng

Hai tiêu chuẩn thường được sử dụng với cáp xoắn đôi là T568A và T568B. Đây là những tiêu chuẩn viễn thông từ TIA và EIA chỉ định sắp xếp pin cho đầu nối (thường là RJ45) trên cáp UTP hoặc STP. Con số 568 đề cập đến thứ tự mà trong đó các dây trong cáp xoắn đôi được gắn vào đầu nối. Tín hiệu giống hệt nhau đối với cả hai tiêu chuẩn này.

Số pin được đọc từ trái sang phải và các đầu nối theo thứ tự từ trên xuống. Lưu ý rằng các đầu ra của pin vẫn giữ nguyên, và sự khác biệt duy nhất là mã hóa màu của hệ thống dây điện.

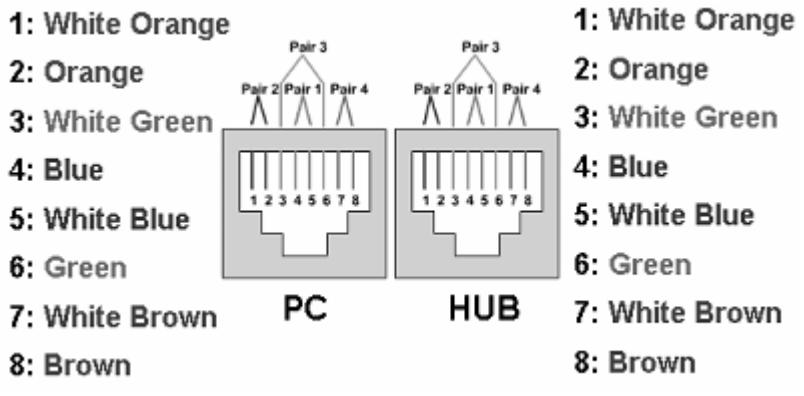


Hình 1.1.6 – Chuẩn T568A và T568B

3. Các kỹ thuật bấm cáp mạng

a) Kỹ thuật bấm dây cáp mạng thẳng

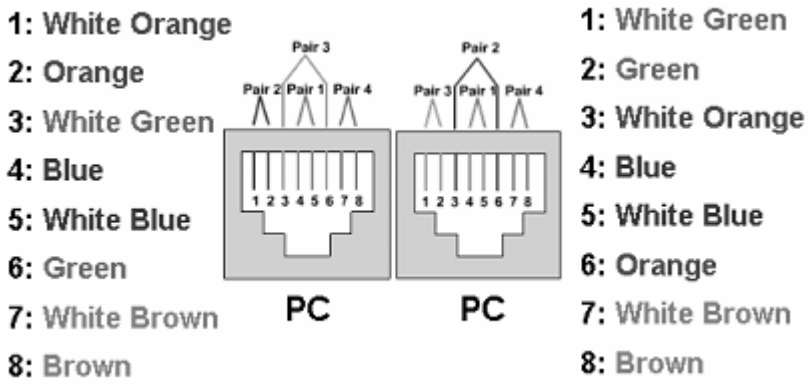
Cáp thẳng (Straight-through cable): là cáp dùng để nối PC và các thiết bị mạng như Hub, Switch, Router… Cáp thẳng theo chuẩn 10/100 Base-T dùng hai cặp dây xoắn nhau và dùng chân 1, 2, 3, 6 trên đầu RJ45. Cặp dây xoắn thứ nhất nối vào chân 1, 2, cặp xoắn thứ hai nối vào chân 3, 6. Đầu kia của cáp dựa vào màu nối vào chân của đầu RJ45 và nối tương tự.



Hình 1.1.7 - Cách đấu dây thẳng.

b) Kỹ thuật bấm dây cáp mạng chéo

Cáp chéo (Crossover cable): là cáp dùng nối trực tiếp giữa hai thiết bị giống nhau như PC – PC, Hub – Hub, Switch – Switch. Cáp chéo trật tự dây cũng giống như cáp thẳng nhưng đầu dây còn lại phải chéo cặp dây xoắn sử dụng (vị trí thứ nhất đổi với vị trí thứ 3, vị trí thứ hai đổi với vị trí thứ sáu) .



Hình 1.1.8 - Cách đấu dây chéo.

II. Trình tự thực hiện

1. Yêu cầu thực hiện

Thực hiện bấm dây cáp mạng thẳng với chuẩn bấm dây cáp mạng T568B

Kiểm tra các dây mạng sau khi bấm hai đầu

2. Thiết bị, dụng cụ, vật liệu

- Dây mạng Cat5e

- Hạt mạng RJ45

- Kìm bấm dây mạng

- Hộp kiểm tra dây mạng

3. Các bước thực hiện

Thực hiện kỹ thuật bấm dây cáp mạng thông qua 4 bước sau:

- Bước 1: Cắt vỏ dây mạng
- Bước 2: Làm gọn và sắp xếp các dây theo chuẩn
- Bước 3: Cắt đầu dây mạng
- Bước 4: Bấm đầu RJ45 cho dây mạng

Hướng dẫn chi tiết

Bước 1: Cắt vỏ dây mạng

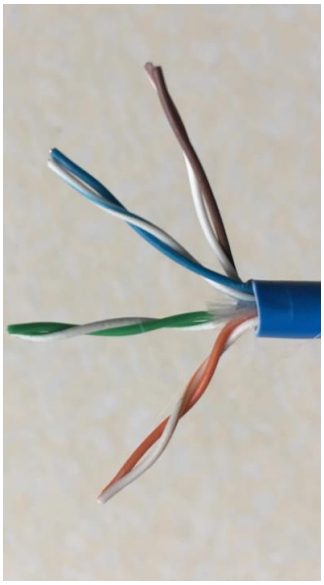
+ Đưa dây mạng vào chỗ cắt vỏ trên kìm bấm độ dài từ 2 – 2,5cm, giữ kìm ở mức lưỡi dao chạm nhẹ vào vỏ dây mạng.

+ Từ từ xoay dây mạng để lưỡi dao cắt được toàn bộ vỏ

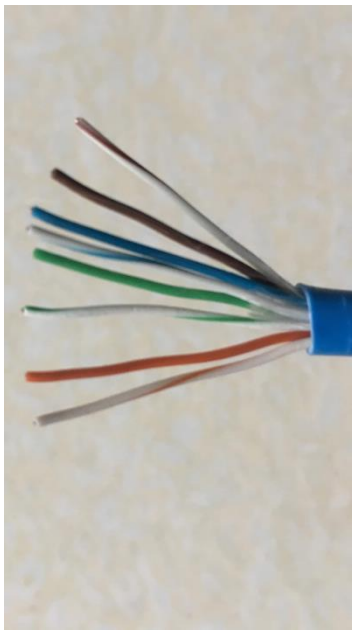
+ Rút vỏ đã cắt ra khỏi dây mạng

Bước 2: Làm gọn và sắp xếp các dây theo chuẩn

+ Tách các cặp dây xoắn và sắp xếp theo thứ tự.



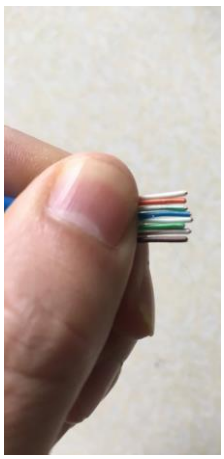
+ Vuốt thẳng các đầu dây và xếp chúng lại gần nhau



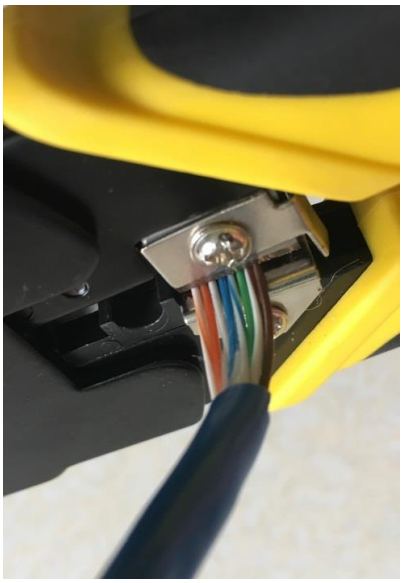
+ Sắp xếp các dây theo chuẩn

Bước 3: Cắt đầu dây mạng

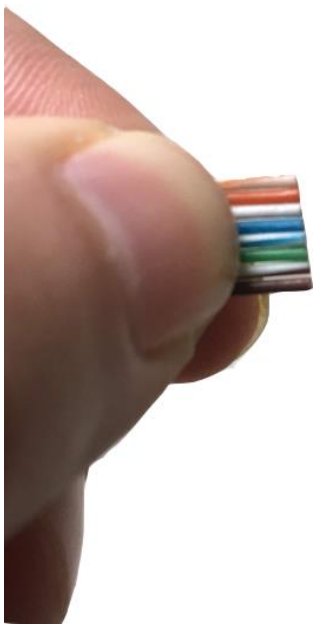
+ Giữ chặt các đầu dây đã sắp xếp và vuốt thẳng



+ Đưa dây vào vị trí dao cắt của kìm bấm

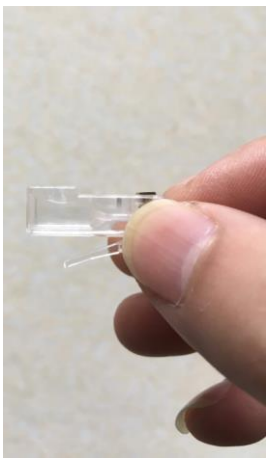


+ Để lại phần dây dài 1cm và cắt đầu thừa của dây



Bước 4: Bấm đầu RJ45 cho dây mạng

+ Lấy đầu hạt mạng RJ45 và hướng ghim cài xuống dưới



+ Tiến hành cho phần dây đã được cắt vào hạt mạng RJ45 sao cho chạm tới điểm đồng ở trong đầu cáp RJ45.

+ Cho đầu cáp RJ45 vào phần bấm đầu RJ45 của kìm mạng và bấm một lực mạnh, dứt khoát.

4. Yêu cầu kết quả

Đưa dây vừa bấm cắm vào bộ kiểm tra dây mạng. Tất cả các đèn trên bộ kiểm tra dây mạng đều sáng lần lượt theo thứ tự từ 1 đến 8

Sử dụng các dây mạng đã bấm cho bài thực hành tiếp theo

III. Sai hỏng và cách khắc phục

1. Đèn trên hộp kiểm tra dây mạng không sáng

- Nguyên nhân

Trong quá trình bấm đầu hạt mạng dây mạng đã không chạm tới điểm tiếp xúc bằng đồng trên hạt mạng RJ45

- Cách khắc phục

Thực hiện bấm đầu dây mạng theo đúng kỹ thuật

2. Đèn trên hộp kiểm tra dây mạng sáng không theo thứ tự

- Nguyên nhân

Trong quá trình sắp xếp dây đã không đúng theo chuẩn

- Cách khắc phục

Thực hiện sắp xếp dây mạng theo đúng chuẩn

3. Đèn trên hộp kiểm tra dây mạng sáng không đủ

- Nguyên nhân

Trong quá trình cắt đầu dây mạng đã cắt không đều hoặc đưa dây vào hạt mạng không đều

- Cách khắc phục

Thực hiện giữ dây mạng thật chặt, cắt dây mạng theo một đường thẳng, tiếp tục giữ chặt dây mạng khi đưa vào hạt mạng

V. Hướng dẫn ôn luyện

- Các bước thực hiện kỹ thuật bấm dây cáp
- Kỹ thuật bấm dây cáp thẳng
- Kỹ thuật bấm dây cáp chéo

BÀI 2: KẾT NỐI THIẾT BỊ

I. Lý thuyết liên quan

1. Các thiết bị liên kết mạng

a) Hub (Bộ tập trung)

Hub thường được dùng để nối mạng, thông qua những đầu cắm của nó người ta liên kết với các máy tính dưới dạng hình sao.

Hình 1.2.1 - Hub.

Người ta phân biệt các Hub thành 3 loại như sau sau:

- Hub bị động (Passive Hub): Hub bị động không chứa các linh kiện điện tử và cũng không xử lý các tín hiệu dữ liệu, nó có chức năng duy nhất là tổ hợp các tín hiệu từ một số đoạn cáp mạng. Khoảng cách giữa một máy tính và Hub không thể lớn hơn một nửa khoảng cách tối đa cho phép giữa 2 máy tính trên mạng (ví dụ khoảng cách tối đa cho phép giữa 2 máy tính của mạng là 200m thì khoảng cách tối đa giữa một máy tính và hub là 100m). Các mạng ARCnet thường dùng Hub bị động.

- Hub chủ động (Active Hub): Hub chủ động có các linh kiện điện tử có thể khuyếch đại và xử lý các tín hiệu điện tử truyền giữa các thiết bị của mạng. Quá trình xử lý tín hiệu được gọi là tái sinh tín hiệu, nó làm cho tín hiệu trở nên tốt hơn, ít nhạy cảm với lỗi do vậy khoảng cách giữa các thiết bị có thể tăng lên. Tuy nhiên những ưu điểm đó cũng kéo theo giá thành của Hub chủ động cao hơn nhiều so với Hub bị động. Các mạng Token ring có xu hướng dùng Hub chủ động.

- Hub thông minh (Intelligent Hub): cũng là Hub chủ động nhưng có thêm các chức năng mới so với loại trước, nó có thể có bộ vi xử lý của mình và bộ nhớ mà qua đó nó không chỉ cho phép điều khiển hoạt động thông qua các chương trình quản trị mạng mà nó có thể hoạt động như bộ tìm đường hay một cầu nối. Nó có thể cho phép tìm đường cho gói tin rất nhanh trên các cổng của nó, thay vì phát lại gói tin trên mọi cổng thì nó có thể chuyển mạch để phát trên một cổng có thể nối tới trạm đích.

b) Bộ chuyển mạch (switch)

Chức năng chính của switch là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (backbone) nội tại tốc

độ cao. Switch có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ Ethernet LAN hoặc Token Ring.

Hình 1.2.2 - Switch.

Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.

Switch là thiết bị giống như bridge nhưng nhiều port hơn cho phép ghép nối nhiều đoạn mạng với nhau. Switch cũng dựa vào bảng địa chỉ MAC để quyết định gói tin nào đi ra port nào nhằm tránh tình trạng giảm băng thông khi số máy trạm trong mạng tăng lên. Switch cũng hoạt động tại lớp hai trong mô hình OSI. Việc xử lý gói tin dựa trên phần cứng (chip).

Khi một gói tin đi đến Switch (hoặc Bridge), Switch (hoặc Bridge) sẽ thực hiện như sau:

- Kiểm tra địa chỉ nguồn của gói tin đã có trong bảng MAC chưa, nếu chưa có thì nó sẽ thêm địa chỉ MAC này và port nguồn (nơi gói tin đi vào Switch (hoặc Bridge)) vào trong bảng MAC.

- Kiểm tra địa chỉ đích của gói tin đã có trong bảng MAC chưa:

+ Nếu chưa có thì nó sẽ gởi gói tin ra tất cả các port (ngoại trừ port gói tin đi vào).

+ Nếu địa chỉ đích đã có trong bảng MAC:

+ Nếu port đích trùng với port nguồn thì Switch (hoặc Bridge) sẽ loại bỏ gói tin.

+ Nếu port đích khác với port nguồn thì gói tin sẽ được gởi ra port đích tương ứng.

Chú ý:

- Địa chỉ nguồn và địa chỉ đích được nói ở trên đều là địa chỉ MAC.
- Port nguồn là Port mà gói tin đi vào.
- Port đích là Port mà gói tin đi ra.

c) Router (Bộ tìm đường)

Router là một thiết bị hoạt động trên tầng mạng, nó có thể tìm được đường đi tốt nhất cho các gói tin qua nhiều kết nối để đi từ trạm gửi thuộc mạng đầu đến trạm

nhận thuộc mạng cuối. Router có thể được sử dụng trong việc nối nhiều mạng với nhau và cho phép các gói tin có thể đi theo nhiều đường khác nhau để tới đích.

Hình 1.2.3 - Router.

Khác với Bridge hoạt động trên tầng liên kết dữ liệu nên Bridge phải xử lý mọi gói tin trên đường truyền thì Router có địa chỉ riêng biệt và nó chỉ tiếp nhận và xử lý các gói tin gửi đến nó mà thôi. Khi một trạm muốn gửi gói tin qua Router thì nó phải gửi gói tin với địa chỉ trực tiếp của Router (Trong gói tin đó phải chứa các thông tin khác về đích đến) và khi gói tin đến Router thì Router mới xử lý và gửi tiếp.

Khi xử lý một gói tin Router phải tìm được đường đi của gói tin qua mạng. Để làm được điều đó Router phải tìm được đường đi tốt nhất trong mạng dựa trên các thông tin nó có về mạng, thông thường trên mỗi Router có một bảng chỉ đường (Router table). Dựa trên dữ liệu về Router gần đó và các mạng trong liên mạng, Router tính được bảng chỉ đường (Router table) tối ưu dựa trên một thuật toán xác định trước.

2. Mô hình mạng ngang hàng Workgoup (peer-to-peer)

Ở mô hình này có một nhóm máy tính mạng cùng chia sẻ tài nguyên như file dữ liệu, máy in. Đó là một nhóm logic các máy tính mà tất cả chúng có cùng tên nhóm. Ở một mạng cục bộ LAN có thể có nhiều nhóm làm việc Workgroup khác nhau cùng kết nối.

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

Với mô hình này các máy tính có quyền chia sẻ tài nguyên ngang nhau mà

không cần sự chỉ định của server. Sự quản trị về tài khoản người dùng, bảo mật cho nguồn tài nguyên chia sẻ không được tập trung hóa. Có thể kết nối tới một nhóm đã tồn tại hoặc khởi tạo một nhóm mới

Ở mô hình này không yêu cầu máy tính chạy trên hệ điều hành Windows Server. Với Workgroups thiết kế và thực hiện đơn giản, không yêu cầu lập kế hoạch có phạm vi rộng. Với nhóm máy tính dưới 10 máy và được đặt gần nhau thì mô hình mạng Workgroup là sự lựa chọn ưu việt. Tuy nhiên ở mô hình này mỗi người dùng cần có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập, nếu như có bất kì sự thay đổi nào liên quan đến tài khoản đều cần thực hiện trên tất cả các máy tính trong nhóm làm việc. Việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được sử dụng

Hình 1.2.4 – Mô hình mạng Workgroup

Mô hình Workgroup có các đặc điểm cơ bản sau:

- Các máy tính trong mạng có vai trò như nhau.
- Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy, các máy tự quản lý tài nguyên của mình.
- Không có máy tính chuyên cung cấp dịch vụ và quản lý hệ thống mạng.
- Mỗi máy tính đều đảm nhận cả 2 vai trò máy phục vụ và máy khách
- Người dùng từng máy tự quyết định về dữ liệu dùng chung
- Các máy tính tự chứng thực
- Thông tin người dùng lưu trong tập tin SAM (Security Accounts Manager) ngay chính trên máy tính cục bộ

Ưu điểm của mô hình Workgroup

- Dễ cài đặt và cấu hình
- Rẻ tiền hơn so với mạng Client-Server

Nhược điểm của mô hình Workgroup

- Không quản lý tập trung tài nguyên mạng.
- Tính bảo mật không cao: độ an toàn và bảo mật do người dùng của từng máy quyết định.
- Phù hợp với các mạng nhỏ (< =15 máy tính)

3. Địa chỉ IP

a) Thành phần và hình dạng của địa chỉ IPv4

Địa chỉ IP đang được sử dụng hiện tại (IPv4) có 32 bit chia thành 4 Octet (mỗi Octet có 8 bit, tương đương 1 byte) cách đếm đều từ trái qua phải bit 1 cho đến bit 32, các Octet tách biệt nhau bằng dấu chấm (.), bao gồm có 3 thành phần chính.

Bit 1.....Bit 32

+ Bit nhận dạng lớp (Class bit)

+ Địa chỉ của đường mạng (Net ID)

+ Địa chỉ của máy tính (Host ID).

Bit nhận dạng lớp (Class bit) để phân biệt địa chỉ ở lớp nào.

- Địa chỉ Internet biểu hiện ở dạng bit nhị phân:

x y x y x y x y. x y x y x y x y. x y x y x y x y. x y x y x y x y

x, y = 0 hoặc 1.

Ví dụ:

0 0 1 0 1 10. 0 1 1 1 1 0 1 1. 0 1 1 0 1 1 1 0. 1 1 1 0 0 0 0 0

Bit nhận dạng Octet 1 Octet 2 Octet 3 Octet 4

- Địa chỉ Internet biểu hiện ở dạng thập phân:

xxx.xxx.xxx.xxx

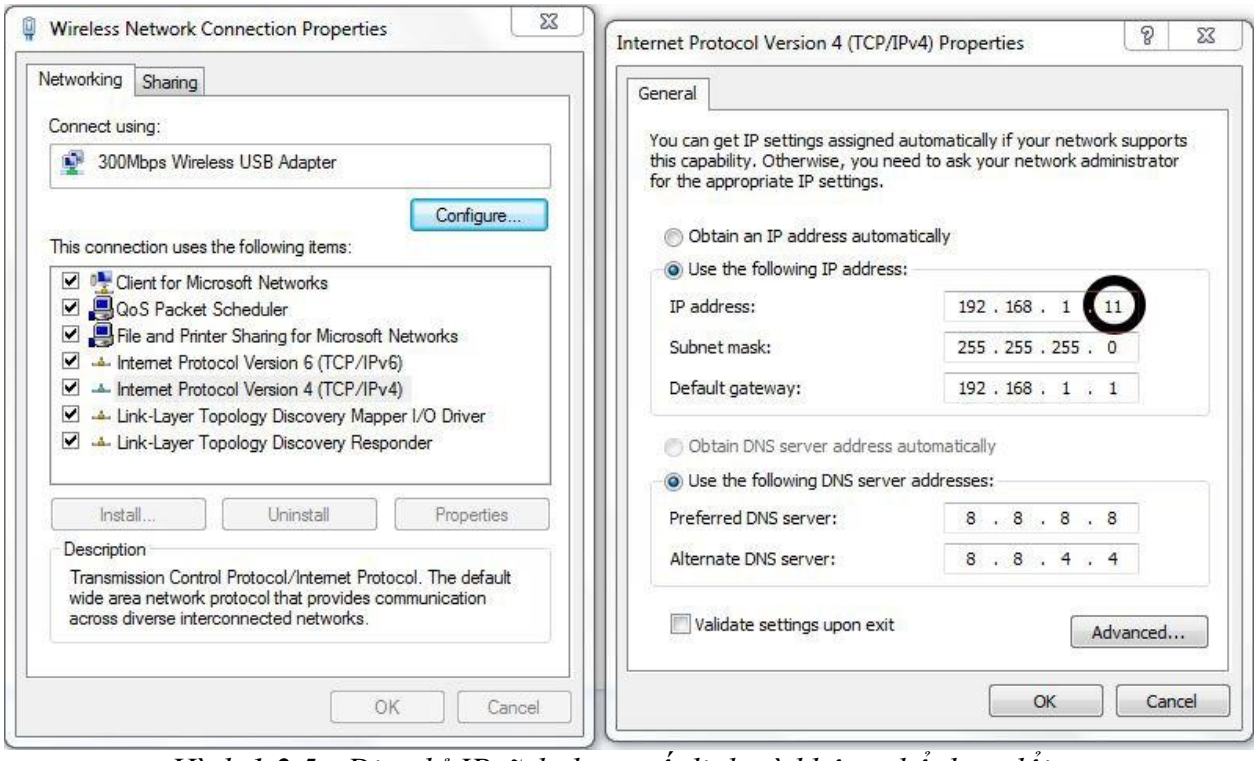
x là số thập phân từ 0 đến 9

Ví dụ: 146. 123. 110. 224

Dạng viết đầy đủ của địa chỉ IP là 3 con số trong từng Octet. Ví dụ: địa chỉ IP thường thấy trên thực tế có thể là 53.143.10.2 nhưng dạng đầy đủ là 053.143.010.002.

b) Địa chỉ IP tĩnh (Static IP)

IP tĩnh là địa chỉ được định cấu hình thủ công cho thiết bị. IP này được gọi "tĩnh" do nó không hề thay đổi khác với DHCP thay đổi mỗi khi mất và kết nối lại.



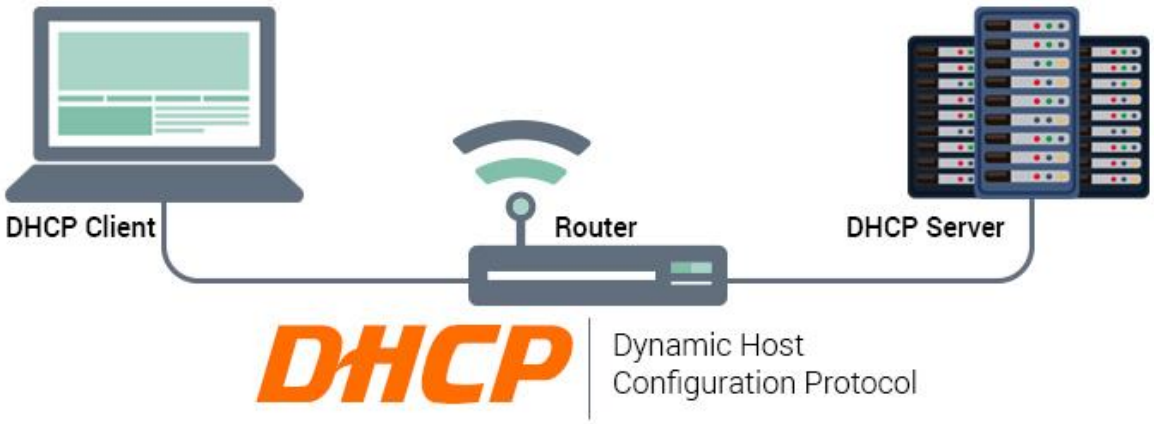
Hình 1.2.5 - Địa chỉ IP tĩnh được cố định và không thể thay đổi

Địa chỉ IP tĩnh giúp kết nối Internet nhanh chóng không cần đợi cấp phát IP. IP tĩnh còn giúp tăng tốc độ tải website, download file torrent. IP tĩnh giữ đường truyền ổn định với máy tính nằm trong hệ thống mạng nội bộ.

Bất lợi lớn của IP tĩnh chính là cấu hình thủ công. Mọi thiết bị đều yêu cầu thiết lập địa chỉ IP tĩnh và cấu hình đúng router để giao tiếp với thiết bị đó. Điều này gây mất rất nhiều thời gian khi thiết lập.

c) Địa chỉ IP động (Dynamic IP)

IP động là IP được gán tự động cho từng kết nối hoặc node của mạng. Ví dụ như điện thoại thông minh, máy tính,…IP động hoạt động ngược lại so với IP tĩnh bằng cách sử dụng phương thức DHCP. Việc gán địa chỉ IP tự động này được thực hiện bằng giao thức DHCP và luôn được thay đổi mỗi khi ngắt và kết nối lại.



Hình 1.2.6 - IP động có thể được tùy chỉnh bởi máy chủ DHCP

IP động mang nhiều ưu điểm như: tính linh hoạt, dễ cài đặt và dễ quản lý. Số lượng thiết bị kết nối sẽ ít bị giới hạn với IP động. Những thiết bị không cần thiết sẽ ngắt kết nối và giải phóng IP cho các thiết bị mới sử dụng.

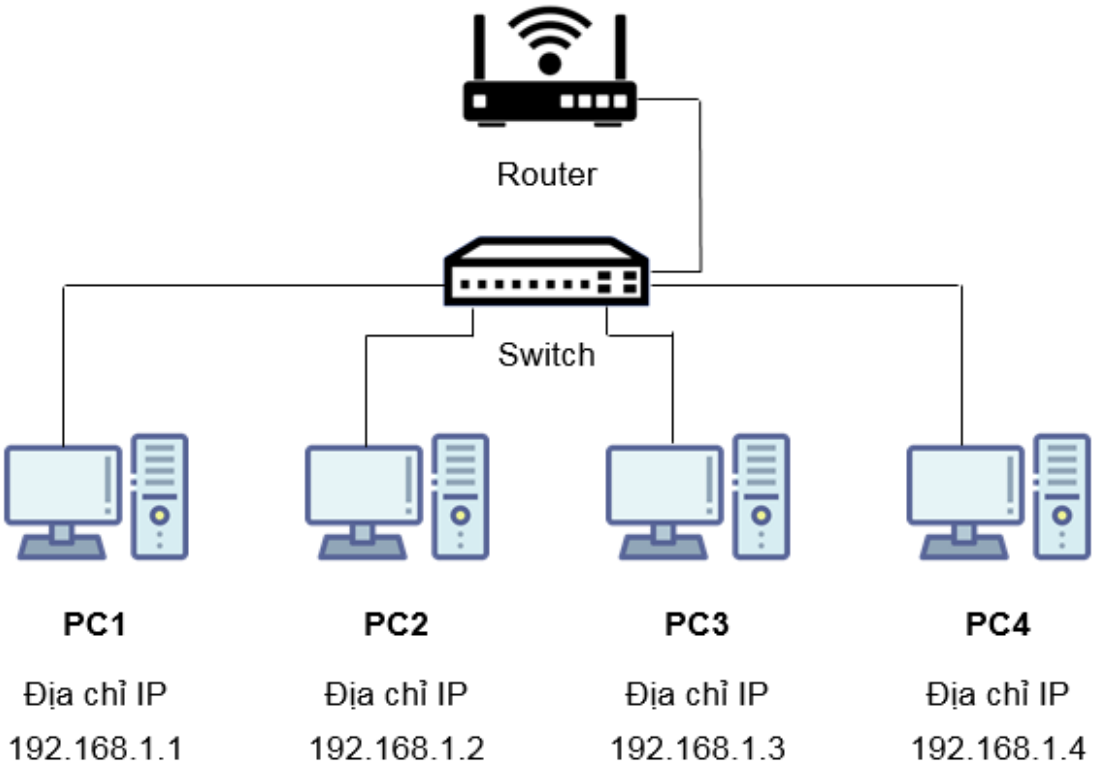
IP động được ứng dụng rộng rãi nhất. Nó tồn tại khi các hộ gia đình sử dụng IP được gán tự động từ router. Tuy nhiên, mọi thiết bị sẽ yêu cầu IP của router để máy tính truy cập vào mạng. Địa chỉ IP động của router sẽ luôn thay đổi theo định kỳ. Điều này dẫn đến việc xung đột IP khi các máy mới vào sử dụng IP của máy đang dùng trong hệ thống mạng.

II. Trình tự thực hiện

1. Yêu cầu thực hiện

- Kết nối các máy tính theo mô hình mạng ngang hàng Peer to Peer
- Cài đặt địa chỉ IP tĩnh cho các máy tính
- Thiết lập chỉ IP động cho các máy tính

Sơ đồ kết nối như sau:



2. Thiết bị, dụng cụ

- Máy vi tính

- Dây mạng đã bấm 2 đầu theo chuẩn T568B

- Switch

- Router

3. Các bước thực hiện

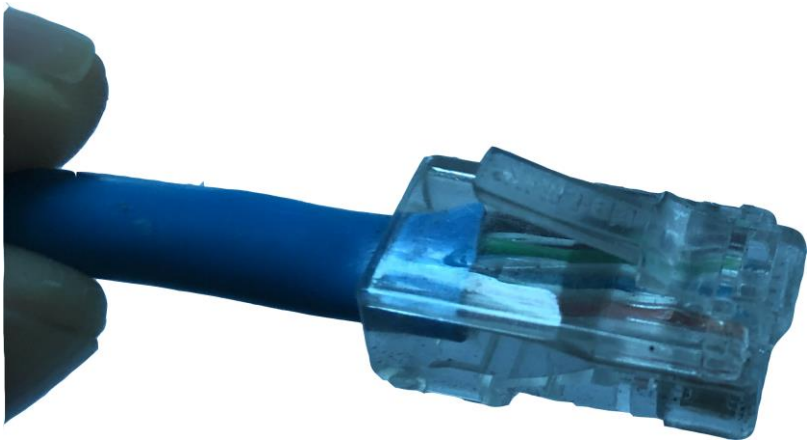
Thực hiện kỹ thuật kết nối các thiết bị thông qua 4 bước sau:

- Bước 1: Cắm dây cáp mạng từ máy tính vào Switch
- Bước 2: Cắm dây cáp mạng từ Switch vào Router
- Bước 3: Cài đặt địa chỉ IP cho các máy tính

Hướng dẫn chi tiết

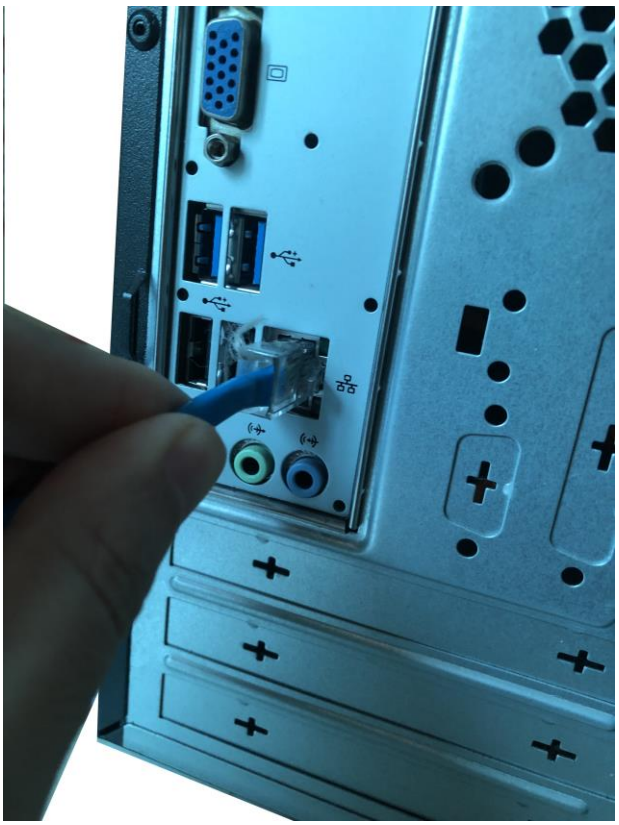
Bước 1: Cắm dây cáp mạng vào máy tính và Switch

Cầm một đầu dây cáp mạng

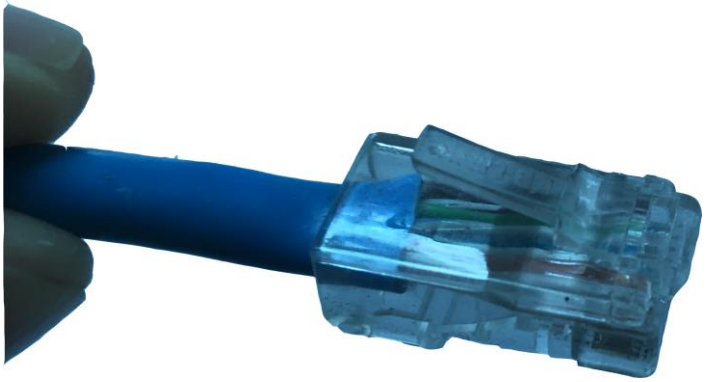


Xác định cổng cắm dây mạng trên máy tính

Cắm dây cáp mạng vào cổng cắm dây mạng trên máy tính

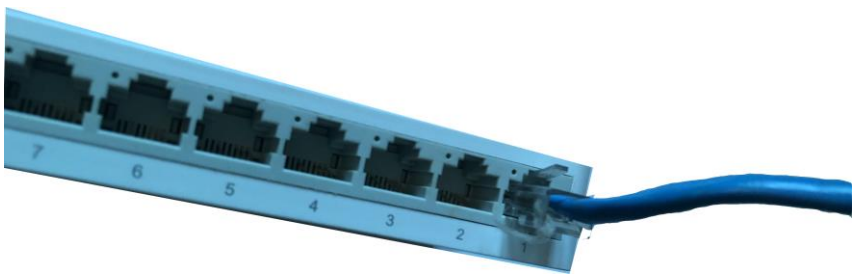


Cầm đầu dây cáp mạng còn lại



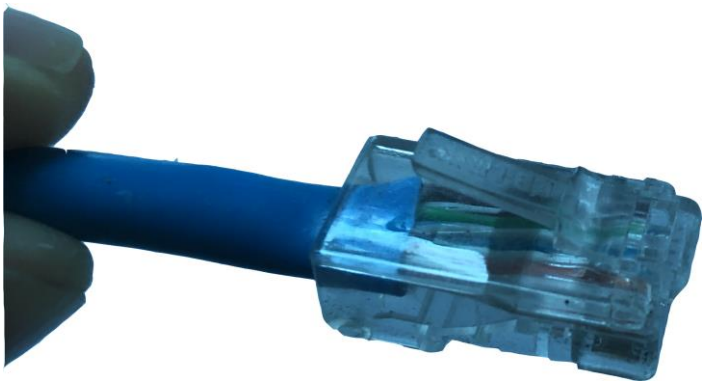
Lựa chọn một cổng cắm dây mạng trên Switch

Cắm dây cáp mạng vào cổng cắm đã lựa chọn trên Switch



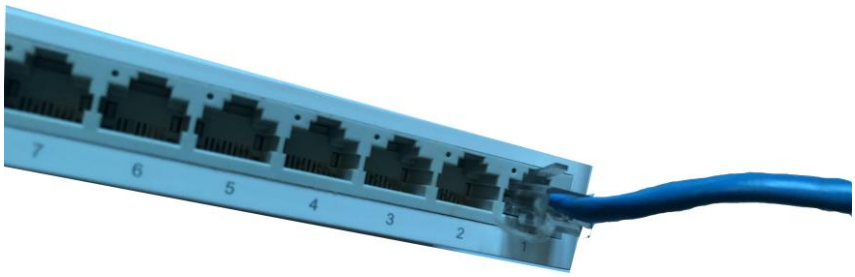
Bước 2: Cắm dây cáp mạng từ Switch vào Router

Cầm một đầu dây cáp mạng

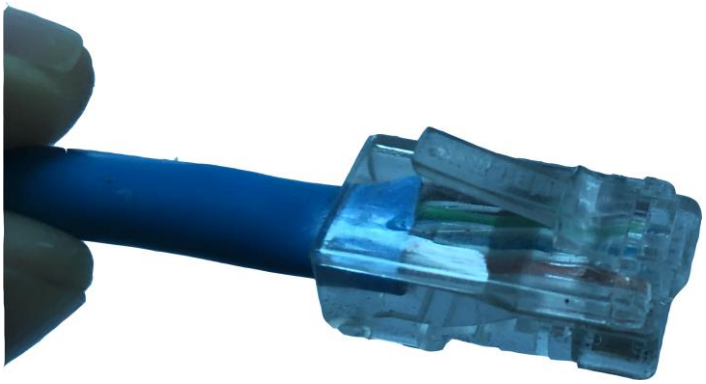


Lựa chọn một cổng cắm dây mạng trên Switch

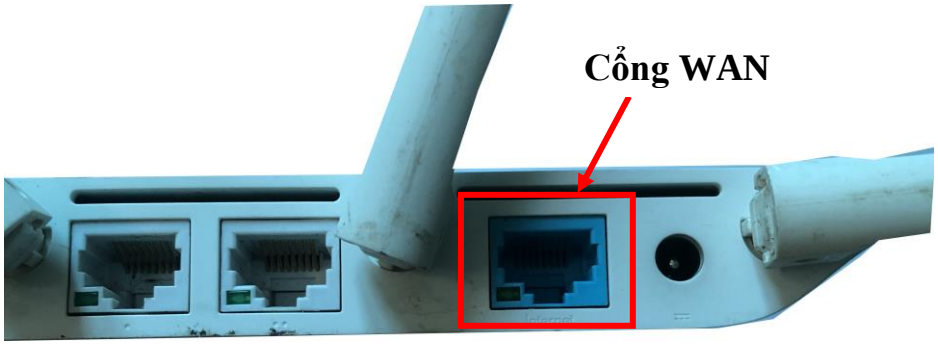
Cắm dây cáp mạng vào cổng cắm đã lựa chọn trên Switch



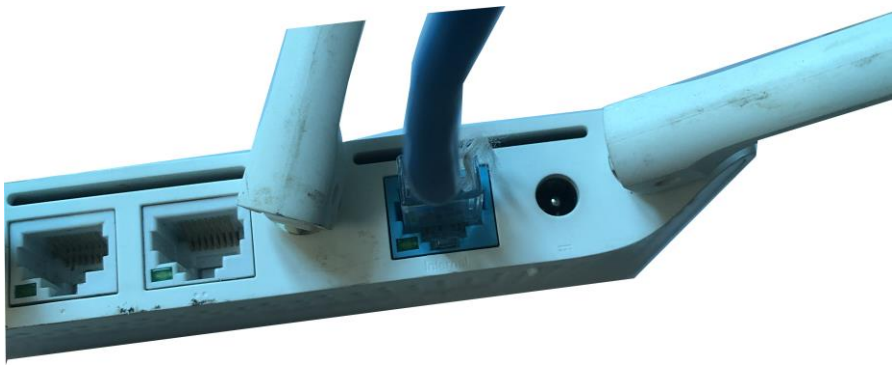
Cầm đầu dây cáp mạng còn lại



Xác định cổng cắm WAN trên Router



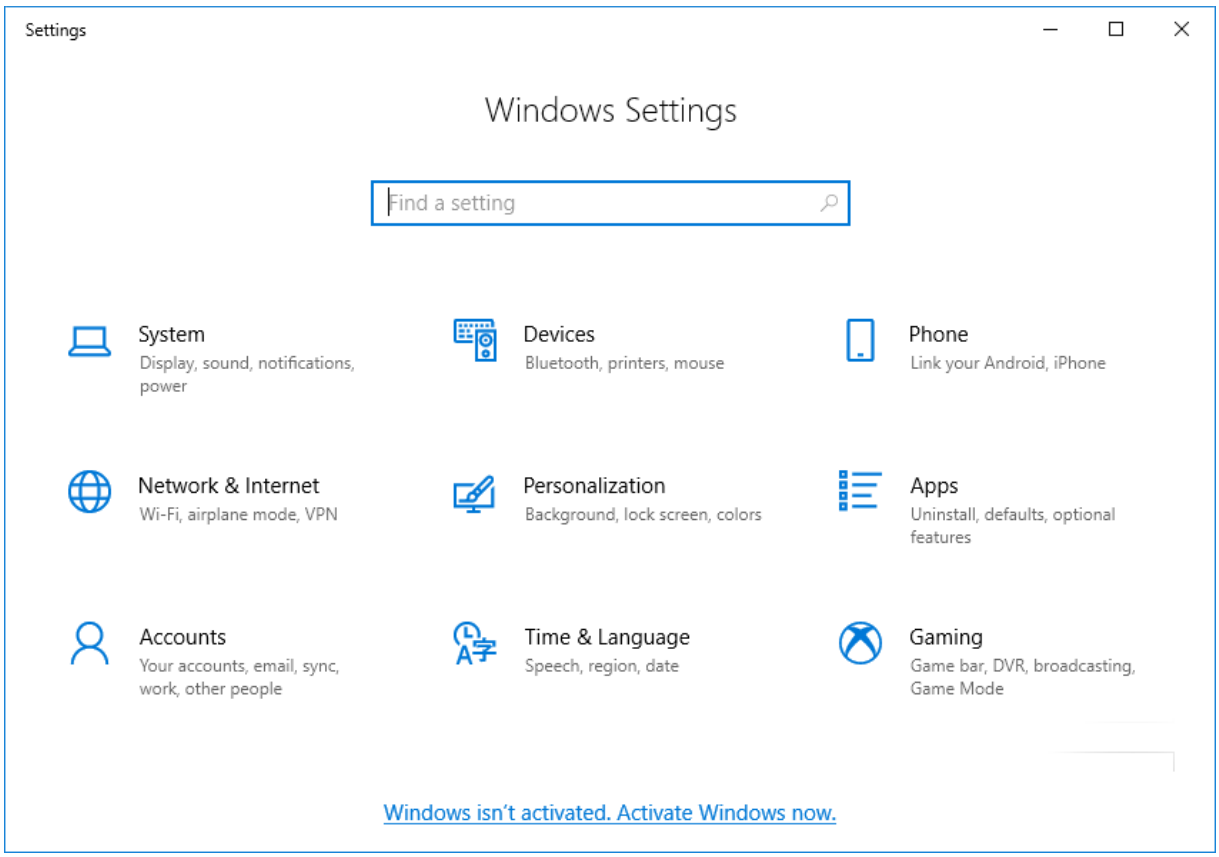
Cắm dây cáp mạng vào cổng cắm WAN trên Router



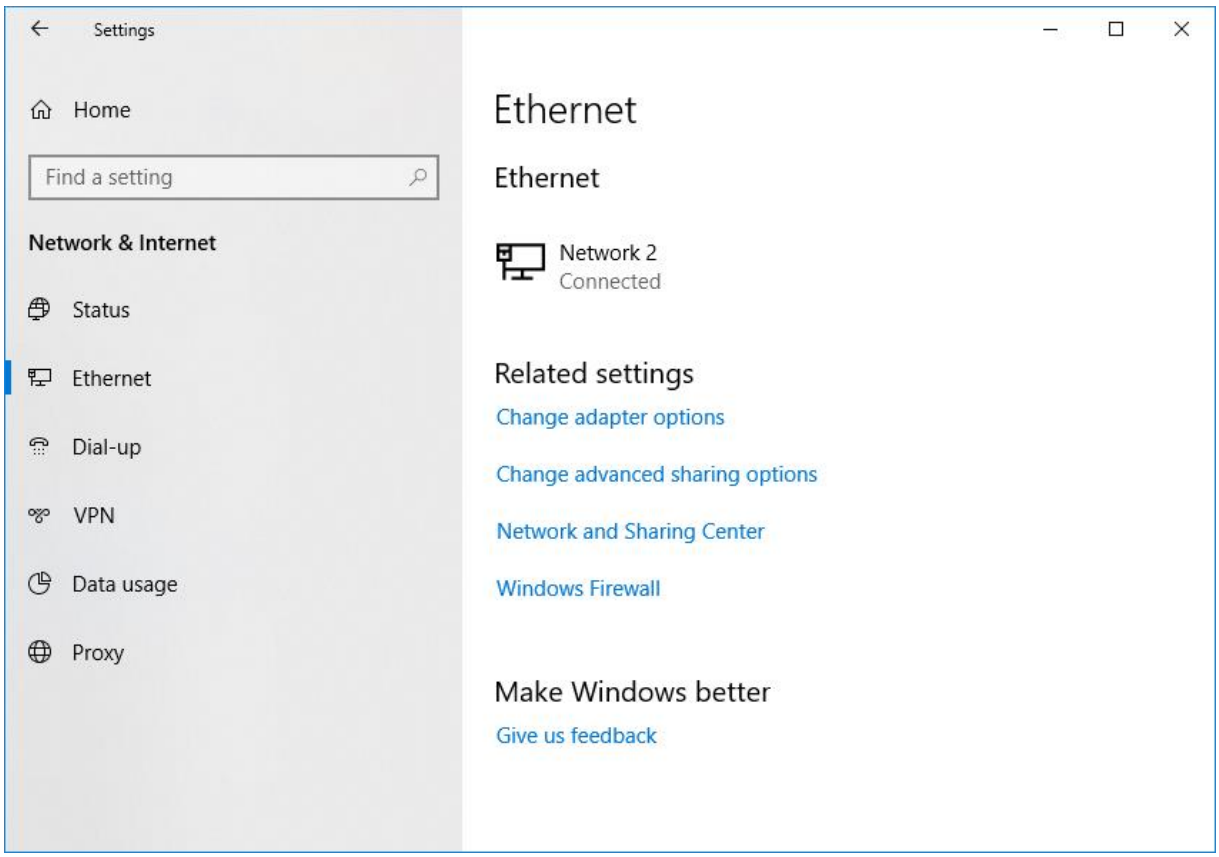
Bước 3: Cài đặt địa chỉ IP cho các máy tính

- Đặt địa chỉ IP tĩnh

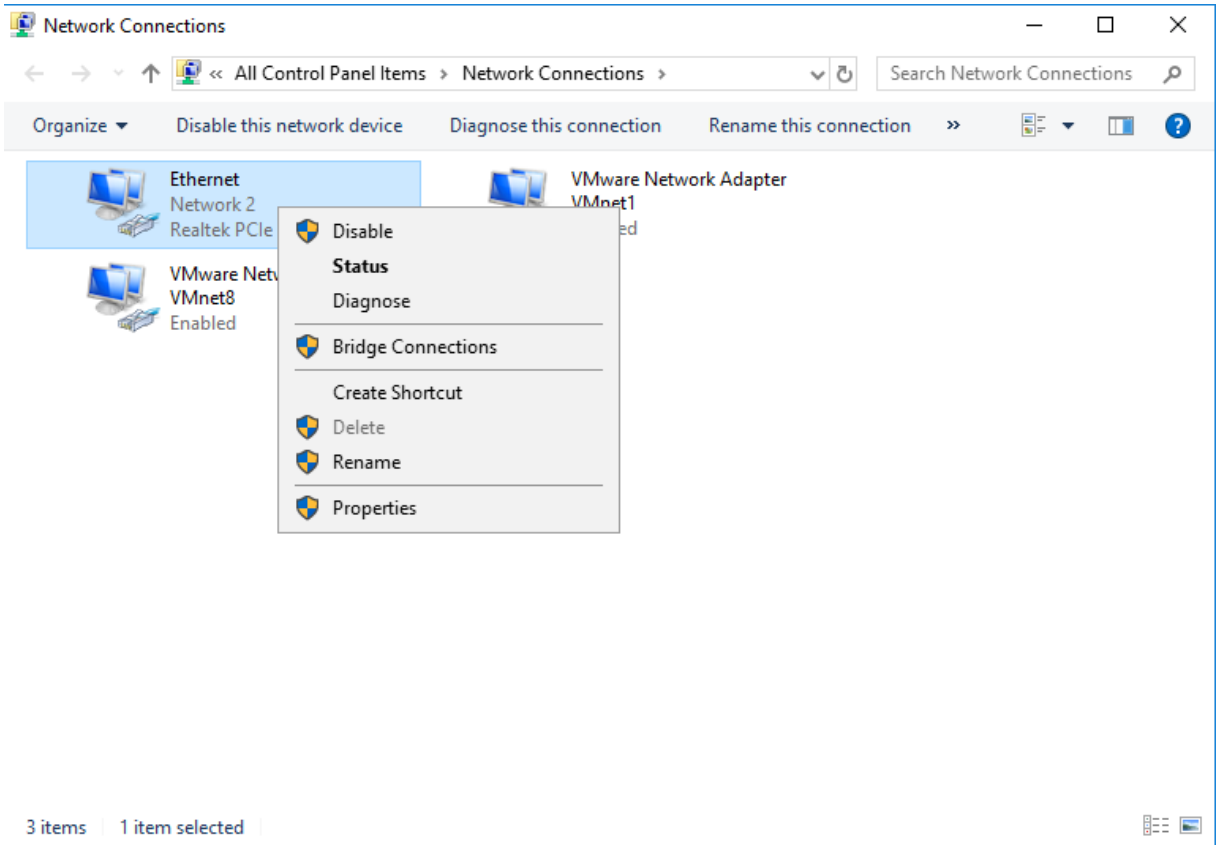
+ Trên máy PC1: Thực hiện vào ***Start / Settings***. Click vào ***Network & Internet***



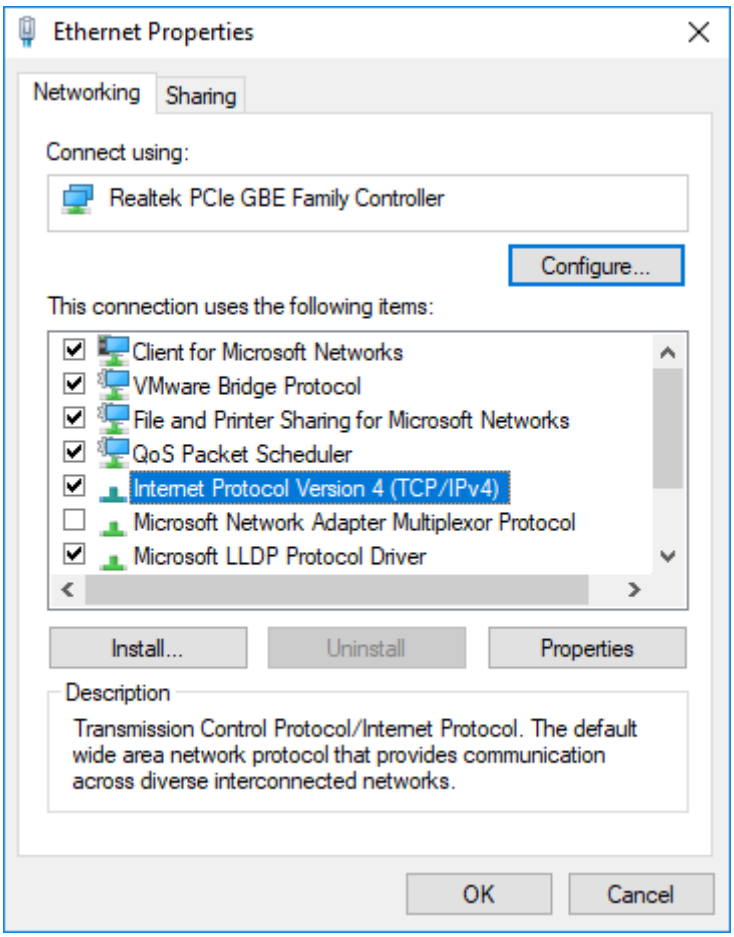
+ Trong cửa sổ tiếp theo click ***Ethernet*** sau đó click ***Change adapter options***



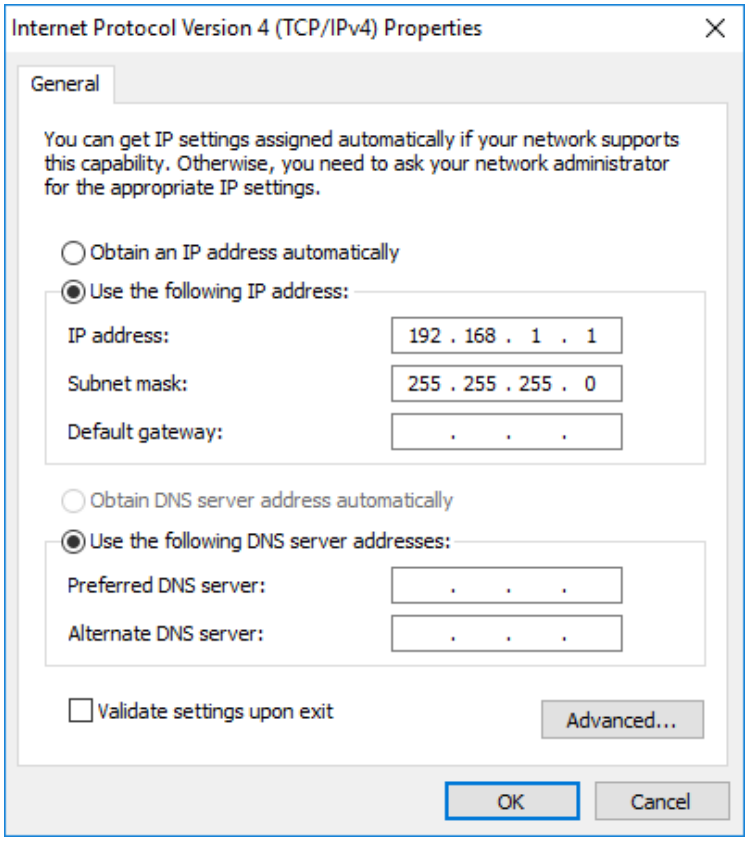
+ Tại cửa sổ ***Network Connections*** click chuột phải vào biểu tượng kết nối Internet của máy tính, chọn ***Properties***



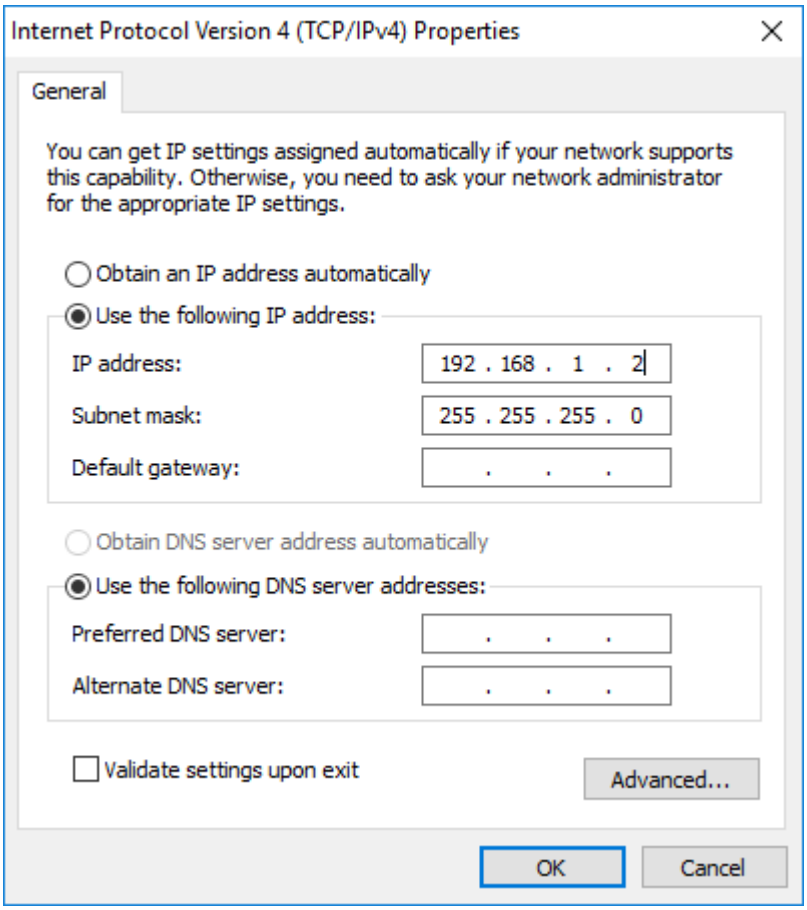
+ Tại hộp thoại ***Ethernet Properties*** chọn mục ***Internet Protocol Version 4 (TCP/IPv4)*** và click nút ***Properties***

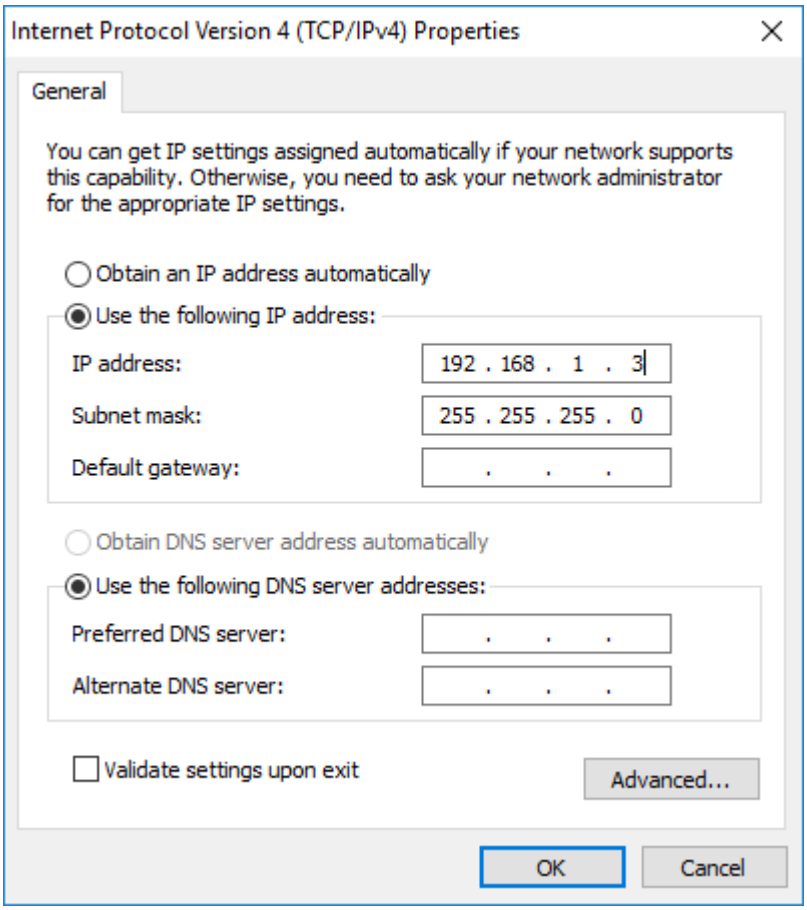


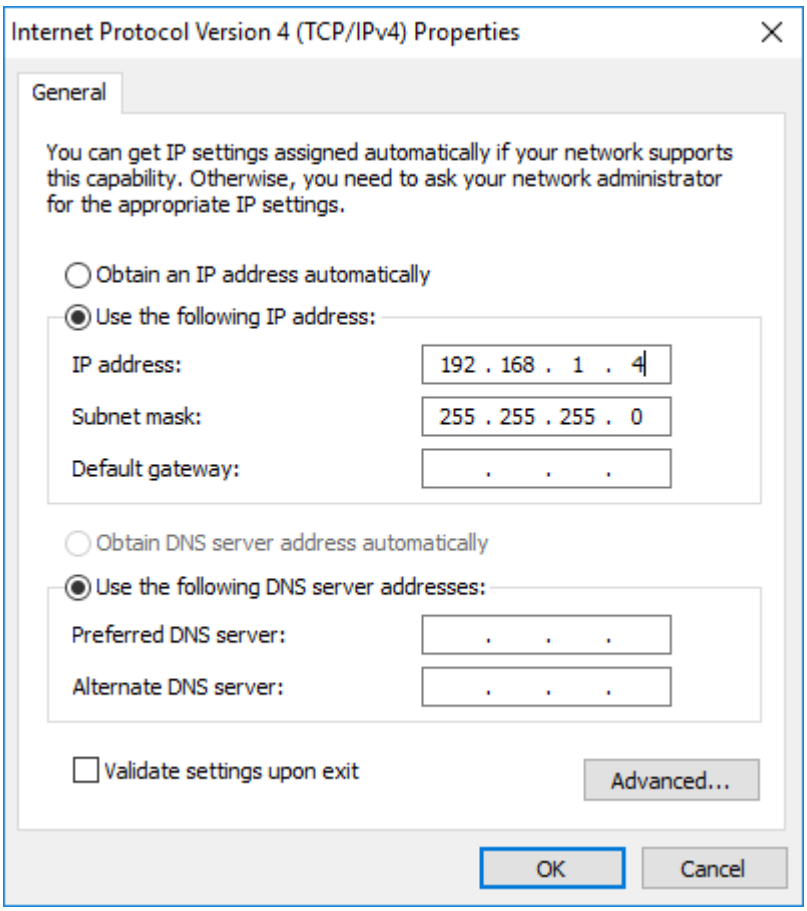
+ Trong hộp thoại tiếp theo click chọn mục ***Use the following IP address*** sau đó nhập địa chỉ IP cho máy **PC1** như hình. Click **OK**



Thực hiện tương tự, tiến hành đặt địa chỉ IP cho các máy **PC2, PC3, PC4**

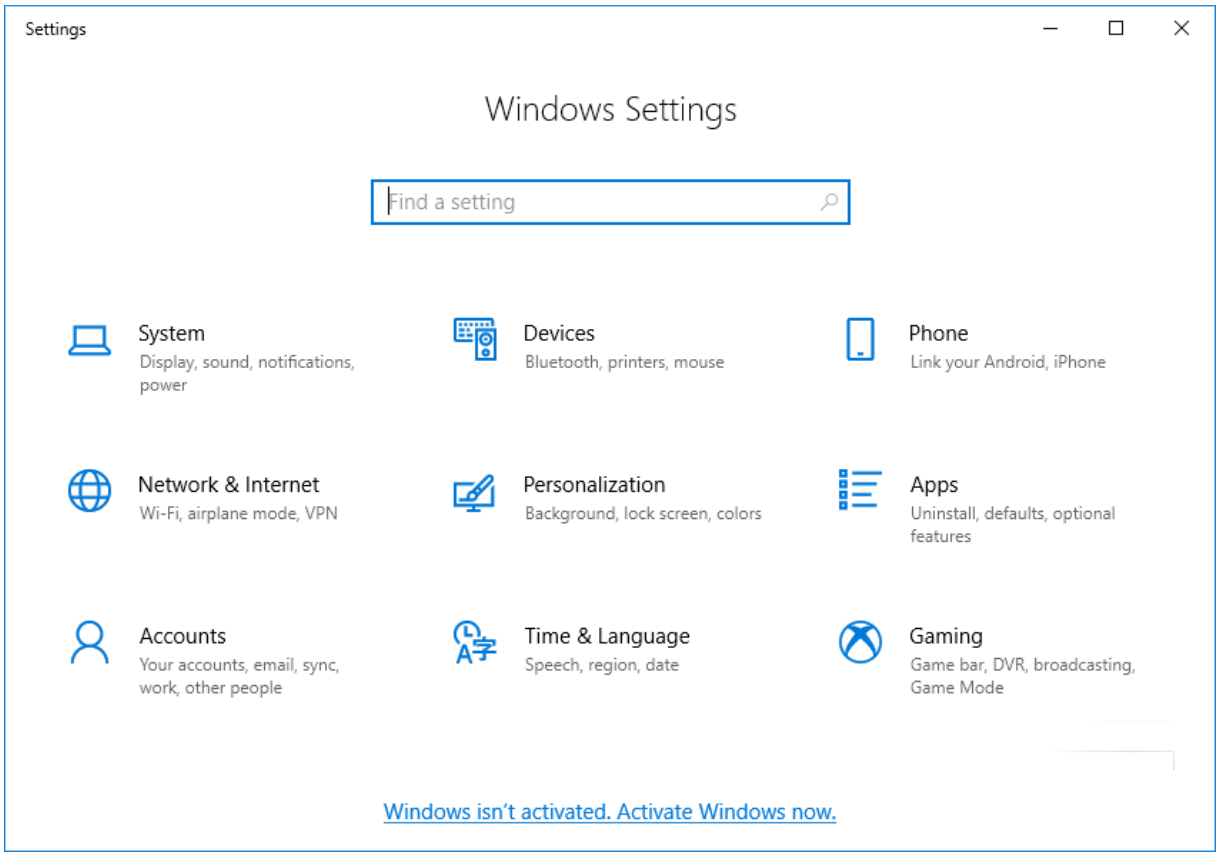




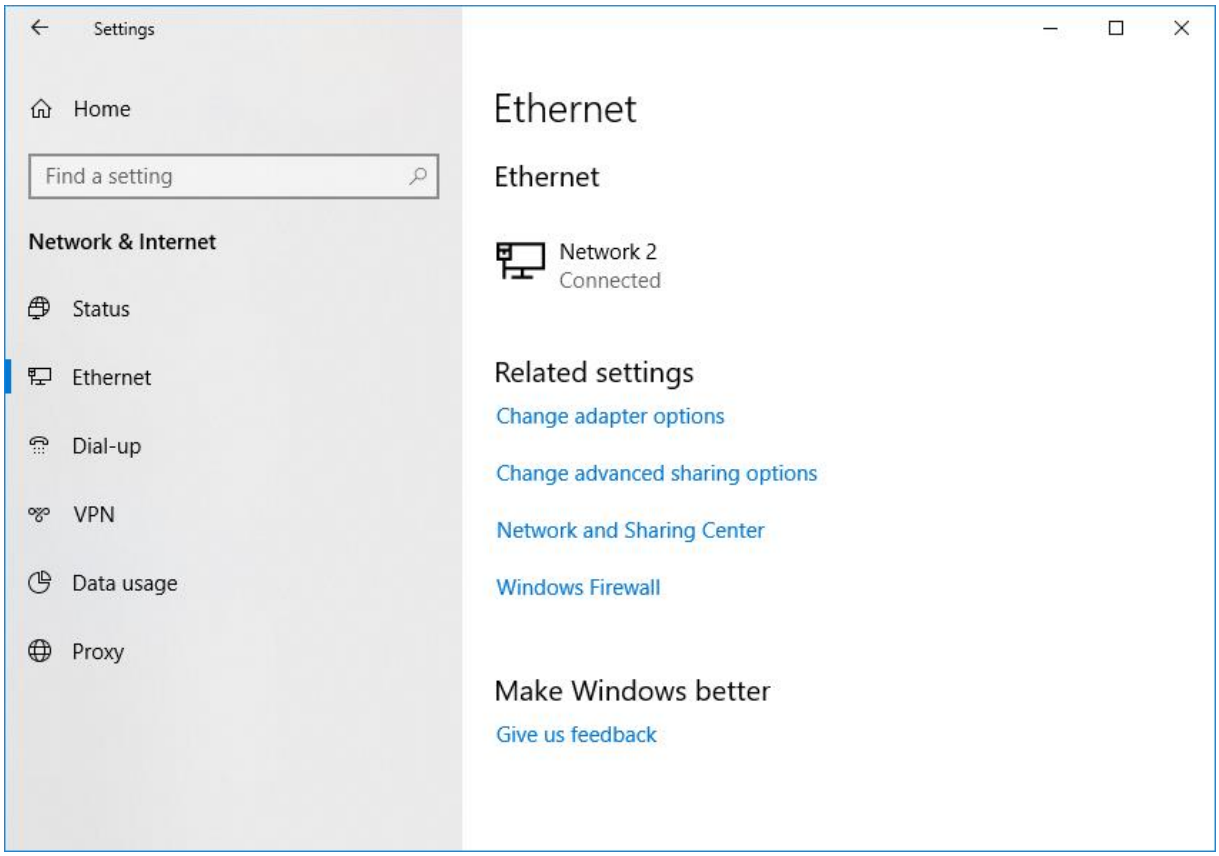


- Đặt địa chỉ IP động

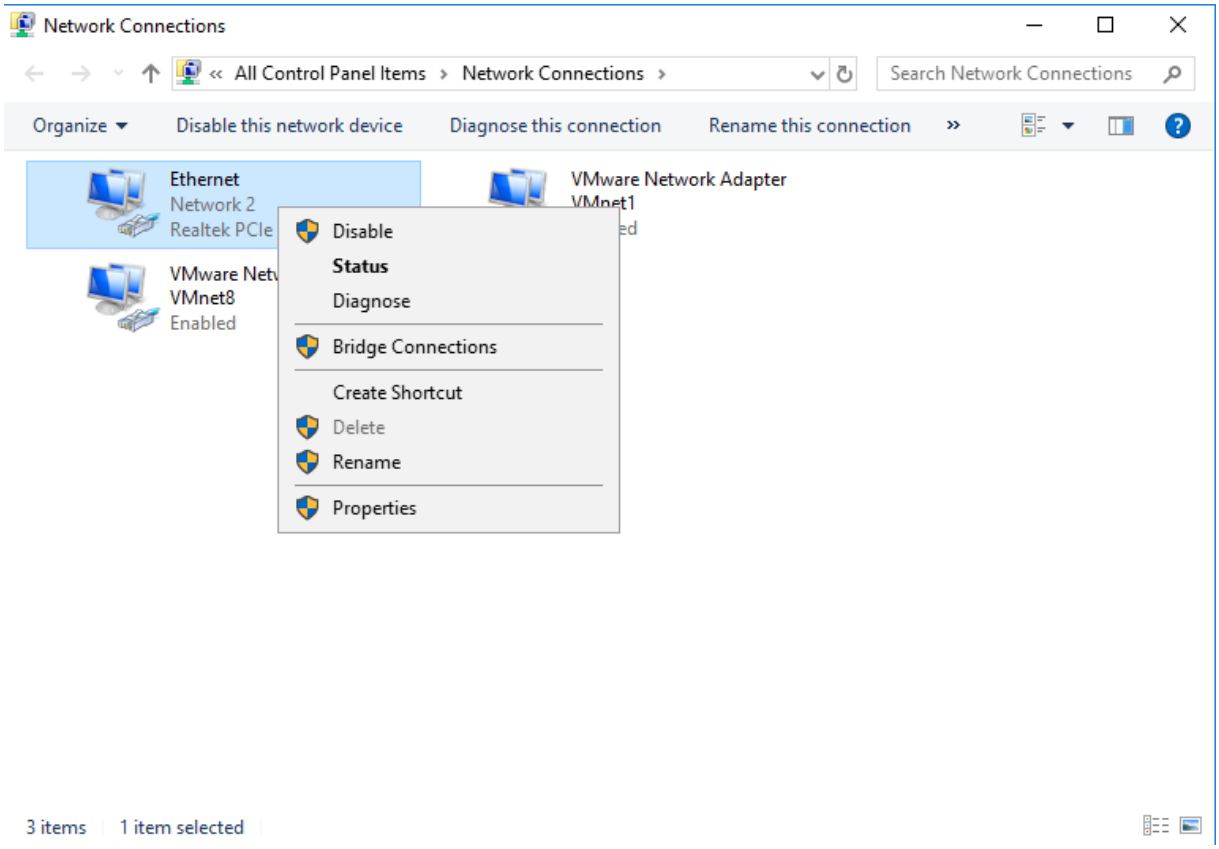
+ Trên máy PC1: Thực hiện vào ***Start / Settings***. Click vào ***Network & Internet***



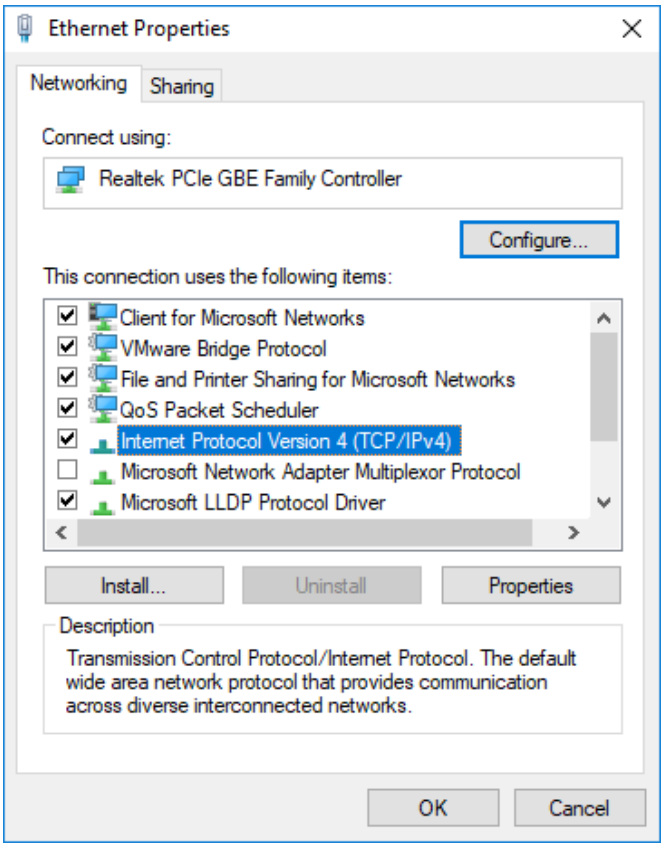
+ Trong cửa sổ tiếp theo click ***Ethernet*** sau đó click ***Change adapter options***



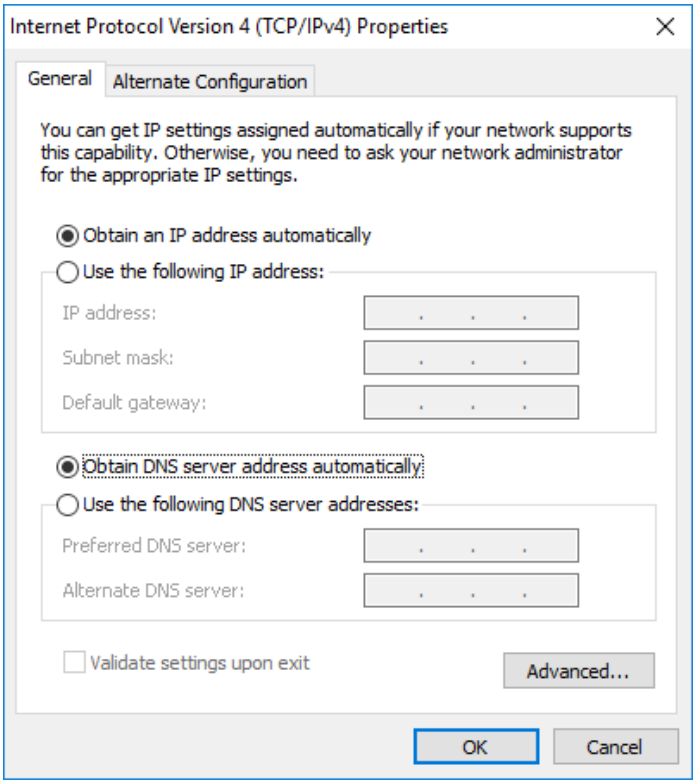
+ Tại cửa sổ ***Network Connections*** click chuột phải vào biểu tượng kết nối Internet của máy tính, chọn ***Properties***



+ Tại hộp thoại ***Ethernet Properties*** chọn mục ***Internet Protocol Version 4 (TCP/IPv4)*** và click nút ***Properties***



+ Trong hộp thoại tiếp theo click chọn mục ***Obtain an IP address automatically.*** Click ***OK***



Thực hiện tương tự cho các máy **PC2, PC3, PC4.** Khi đó địa chỉ IP của các máy PC1, PC2, PC3, PC4 sẽ do Router thiết lập tự động

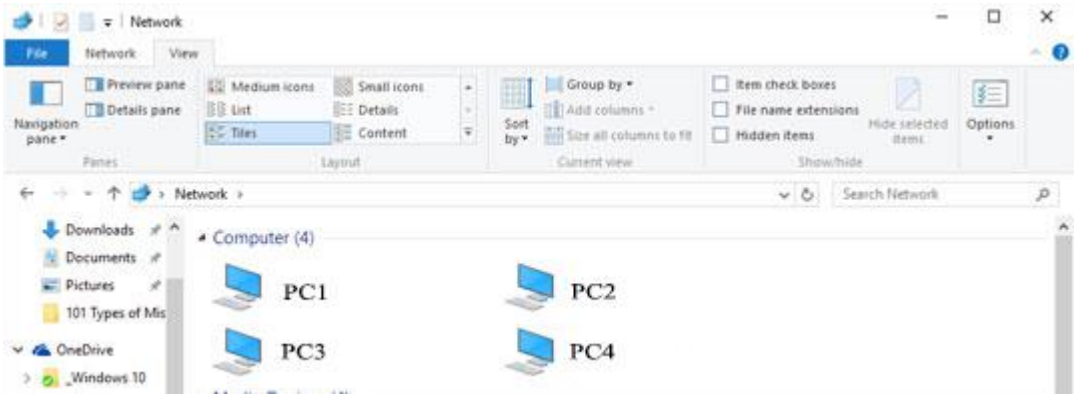
4. Yêu cầu kết quả

Kết nối các máy tính sử dụng các thiết bị liên kết mạng đúng theo sơ đồ đã ghi trong phần yêu cầu

Cài đặt thành công địa chỉ IP tĩnh cho các máy tính PC1, PC2, PC3, PC4

Thiết lập thành công địa chỉ IP động cho các máy tính PC1, PC2, PC3, PC4

Mở Network sẽ hiển thị tên các máy tính đã được kết nối với nhau



III. Sai hỏng và cách khắc phục

1. Không hiển thị các máy tính trong Network

- Nguyên nhân

Chưa đặt địa chỉ IP cho các máy tính hoặc đặt không đúng, có sự trùng lặp

- Cách khắc phục

Đặt địa chỉ IP theo đúng yêu cầu

2. Hiển thị không đầy đủ các máy tính trong Network

- Nguyên nhân

Tên các máy tính phải khác nhau không có sự trùng lặp

- Cách khắc phục

Đặt tên các máy tính đúng theo sơ đồ

3. Không cấp được địa chỉ IP động cho các máy tính

- Nguyên nhân

Cắm dây mạng không đúng vào cổng WAN trên Router

- Cách khắc phục

Cắm dây mạng vào cổng WAN trên Router

V. Hướng dẫn ôn luyện

- Thực hiện kết nối các máy tính sử dụng các thiết bị liên kết mạng
- Cài đặt địa chỉ IP tĩnh cho các máy tính

- Thiết lập địa chỉ IP động cho các máy tính

BÀI 3: CHIA SẺ DỮ LIỆU VÀ MÁY IN

I. Lý thuyết liên quan

1. Mạng nội bộ LAN

LAN có tên gọi đầy đủ là "Local Network Area" (Mạng cục bộ). Mạng LAN được hiểu là sự kết hợp của nhiều thiết bị được kết nối lại với nhau trong một hệ thống mạng tại một khu vực nhất định (Công ty, trường học, nhà ở,…). Về cơ bản: Mạng LAN được hình thành khi 2 hoặc nhiều máy tính cùng cắm vào 1 modem hoặc dạng tương tự rồi kết nối và chia sẻ các thông tin với nhau tại đó.

Mạng LAN được kết nối lại với nhau thông qua thiết bị định tuyến (Router) hay WLAN (Wireless Local Network Area) mạng LAN không dây – các máy tính kết nối vào mạng thông qua Wifi.

Sử dụng mạng LAN giúp chia sẻ dữ liệu trong nội bộ một cách nhanh chóng mà không cần phải thao tác quá nhiều.

2. Tường lửa (Windows Firewall)

Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Nó kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Nghĩa là, chỉ những traffic phù hợp với chính sách được định nghĩa trong tường lửa mới được truy cập vào mạng, mọi traffic khác đều bị từ chối.

Bất kì máy tính nào kết nối tới Internet cũng cần có firewall, giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng. Việc có một "người gác cổng" như vậy để giám sát mọi việc xảy ra rất quan trọng bởi 2 lý do:

Thứ nhất, bất kì máy tính kết nối mạng nào thường kết nối vĩnh viễn với Internet. Thứ 2, mỗi máy tính trực tuyến lại có một chữ ký điện tử riêng, được gọi là Internet Protocol address (hay còn gọi là địa chỉ IP): Nếu không có firewall hỗ trợ, nó chẳng khác gì chuyện bật tất cả đèn lên và mở rộng cửa để đón trộm vào.

Một firewall được cấu hình chính xác sẽ ngăn chặn điều này xảy ra và giúp máy tính "ẩn" một cách hiệu quả. Firewall không giống chương trình diệt virus. Thay vào đó, nó làm việc cùng với những công cụ này nhằm đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến.

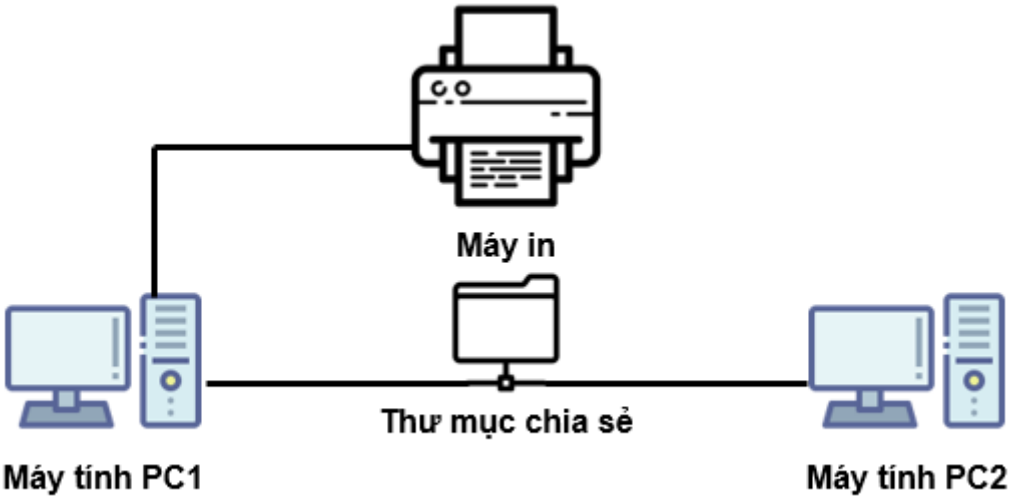
II. Trình tự thực hiện

1. Yêu cầu thực hiện

Chia sẻ thư mục Public tại ổ đĩa D trên máy PC1, truy cập vào thư mục đã chia sẻ trên máy PC2

Chia sẻ máy in trên máy PC1, kết nối máy in đã chia sẻ trên máy PC2, thực hiện lệnh in kiểm tra trên máy PC2

Sơ đồ kết nối như sau:



2. Thiết bị, dụng cụ, vật liệu

- Máy vi tính đã kết nối mạng nội bộ LAN.

- Máy in đã được cài đặt trên máy PC1

3. Các bước thực hiện

Thực hiện kỹ thuật chia sẻ dữ liệu và chia sẻ máy in thông qua 5 bước sau:

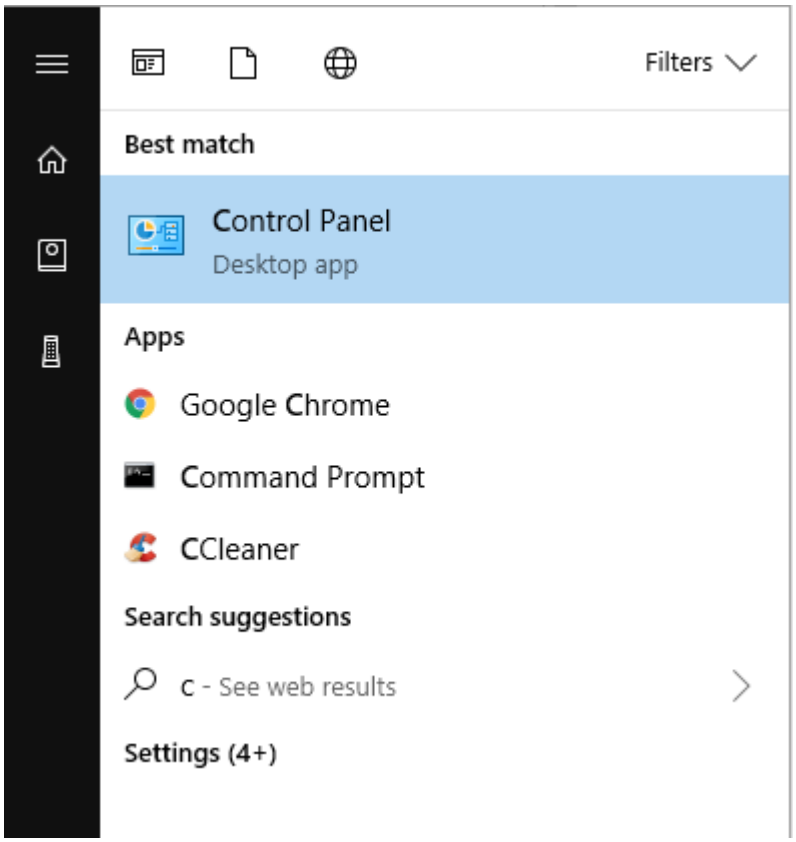
- Bước 1: Tắt tường lửa Windows Firewall

- Bước 2: Kiểm tra 2 máy tính đã thông nhau
- Bước 3: Thiết lập để vào mạng LAN
- Bước 4: Chia sẻ dữ liệu qua mạng LAN
- Bước 5: Chia sẻ máy in qua mạng LAN

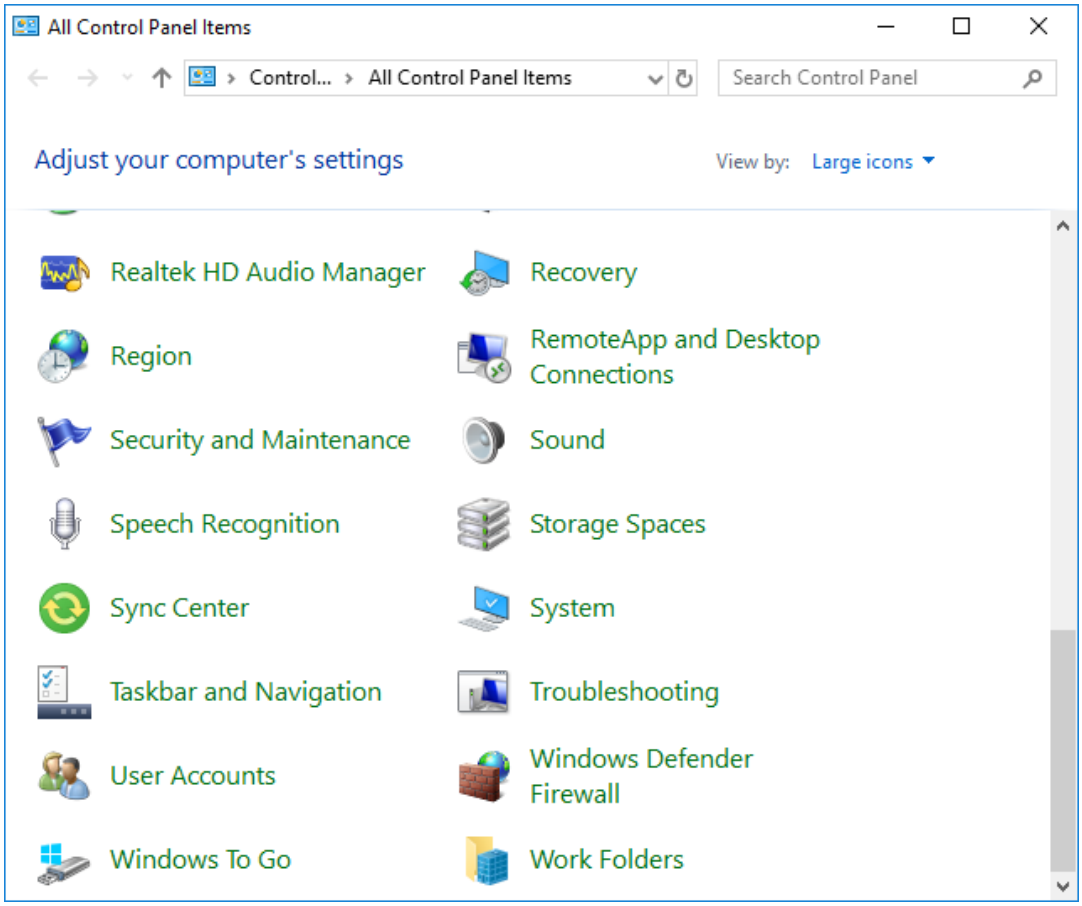
Hướng dẫn chi tiết

Bước 1: Tắt tường lửa Windows Firewall

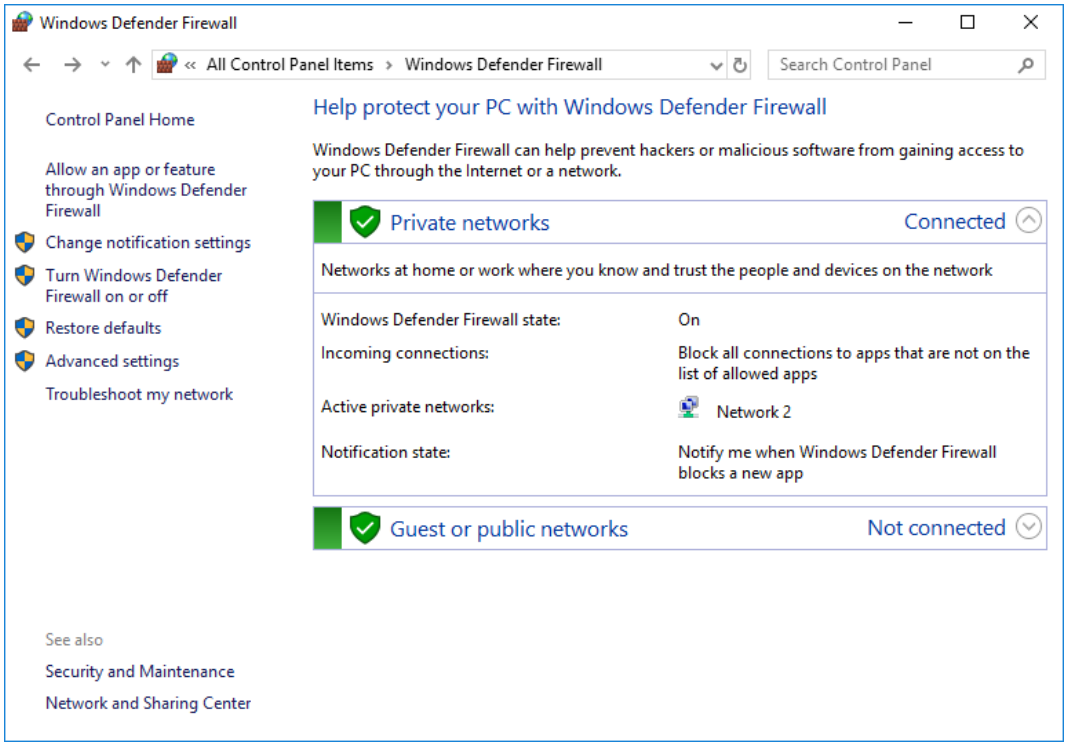
Thực hiện: Vào mục ***Control Panel***



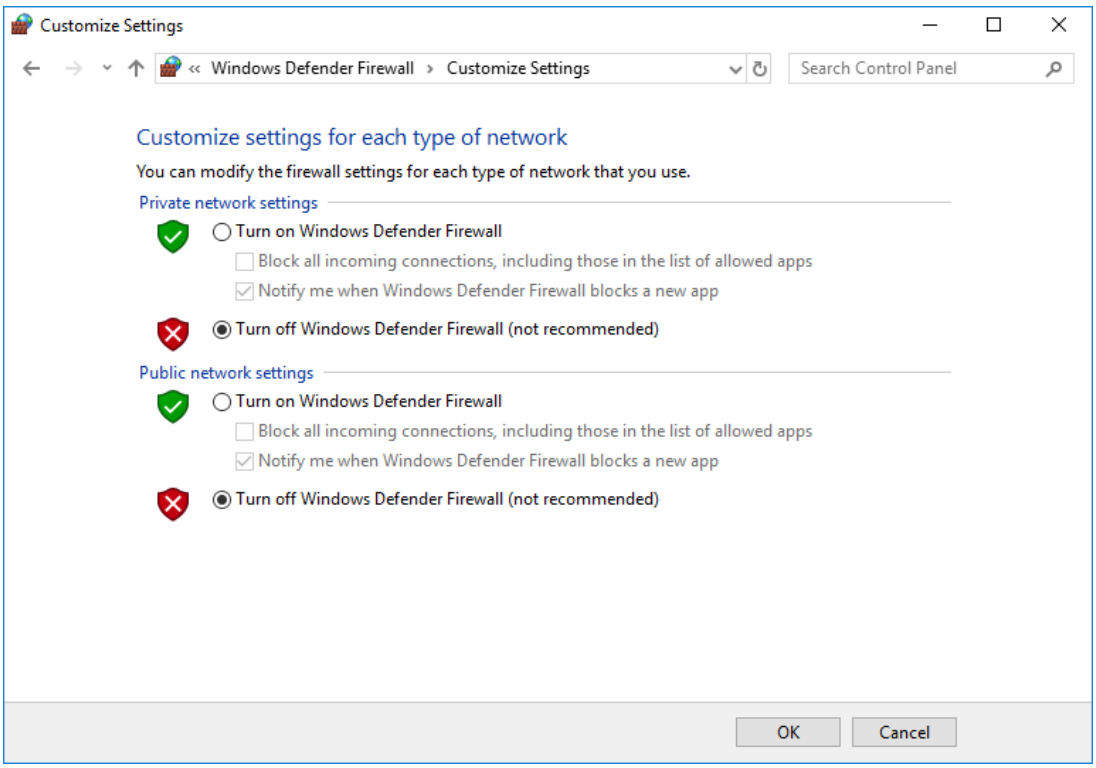
Trong hộp thoại ***All Control Panel Items*** click chuột vào mục ***Windows Defender Firewall***



Hộp thoại ***Windows Defender Firewall*** xuất hiện click vào mục ***Change notification settings***

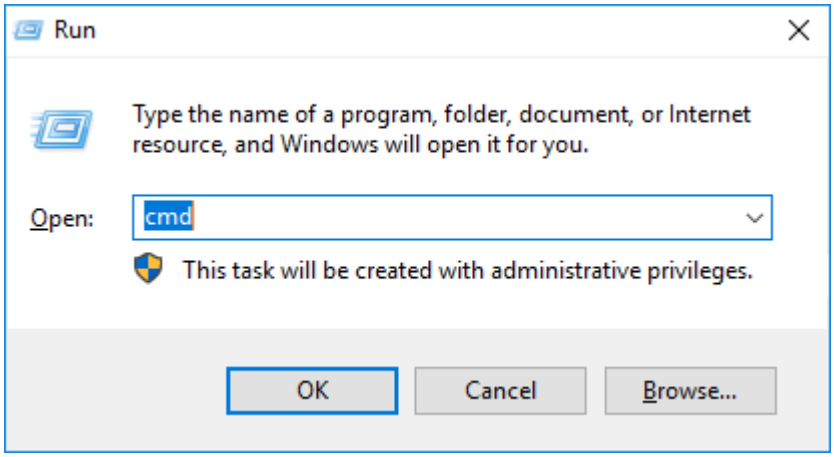


Ở hộp thoại ***Customize Settings*** click chọn ***Turn off Windows Defender Firewall (not recommended)***

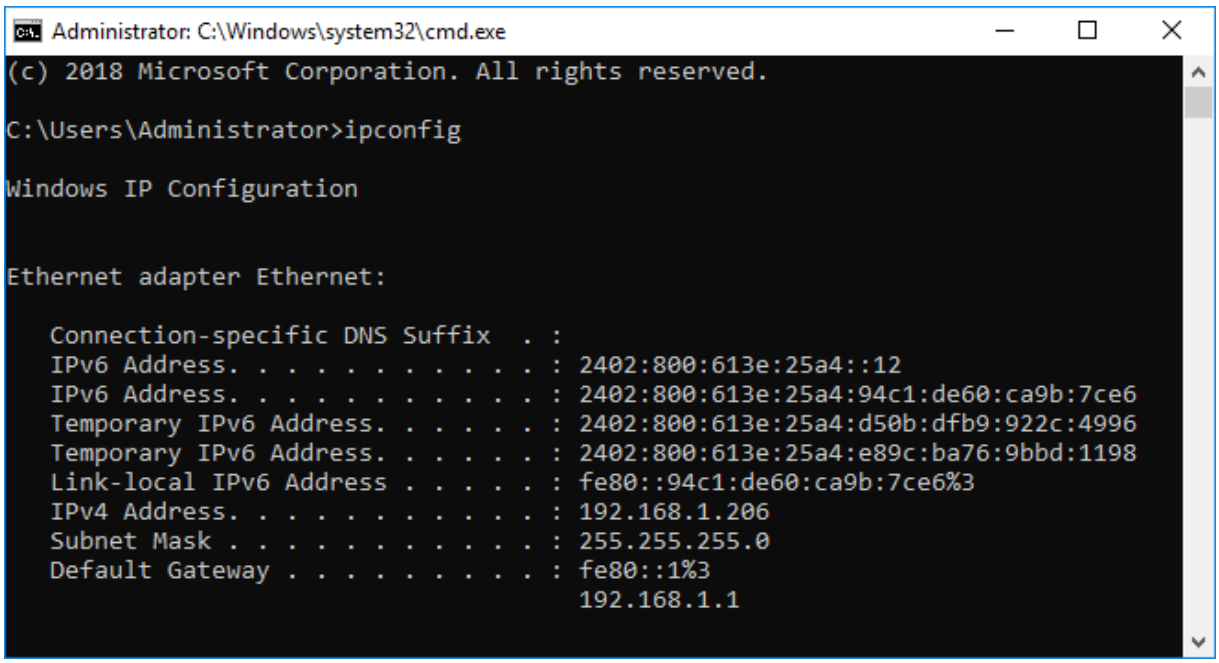


Bước 2: Kiểm tra 2 máy tính đã thông nhau

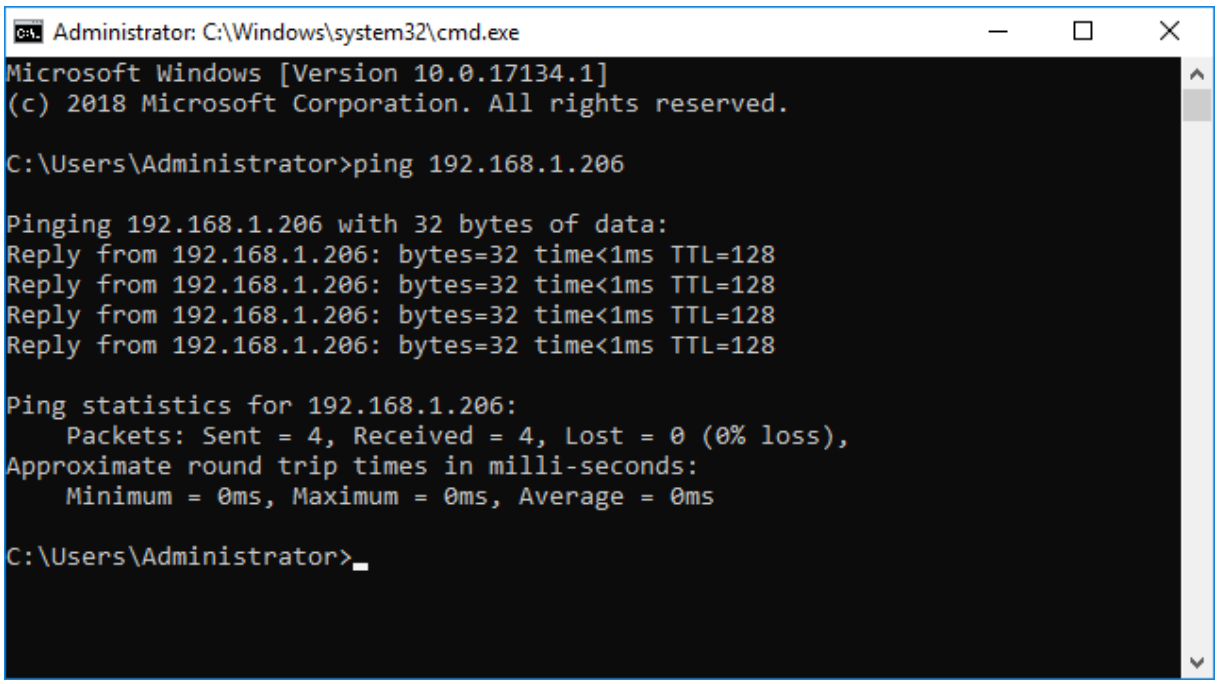
Mở hộp thoại Run (tổ hợp phím ***Windows*** + ***R***) sau đó gõ lệnh ***cmd*** rồi nhấn ***OK***



Xem địa chỉ IP của máy PC1 nhập **ipconfig** rồi bấm Enter. Chú ý dòng IPv4 Address chính là địa chỉ IP của máy PC1

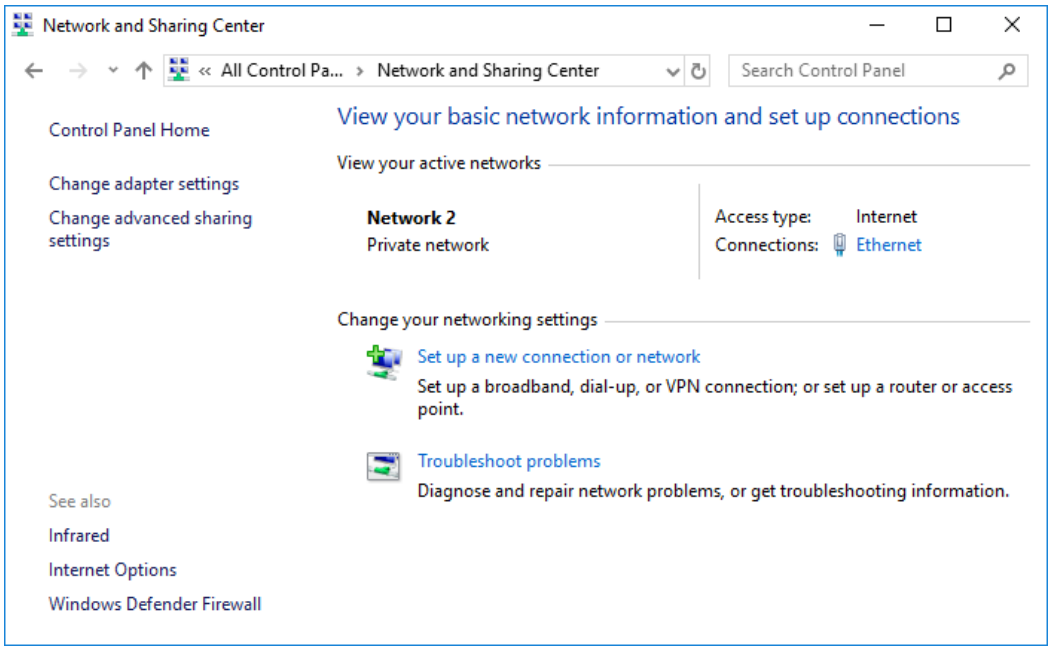


Xem địa chỉ IP của máy **PC2** sau đó nhập ***ping IP máy PC2*** rồi bấm Enter. Nếu thấy có dòng ***Reply from IP PC2*** là thành công

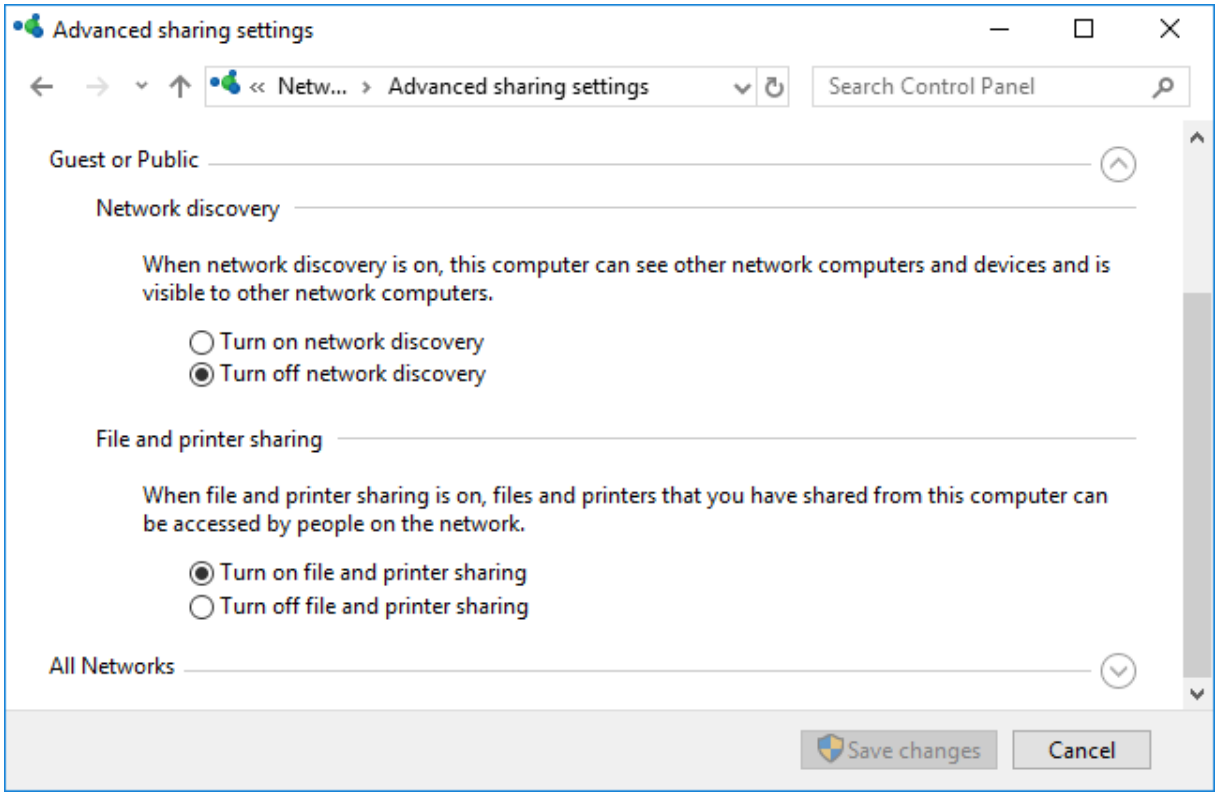


Bước 3: Thiết lập để vào mạng LAN

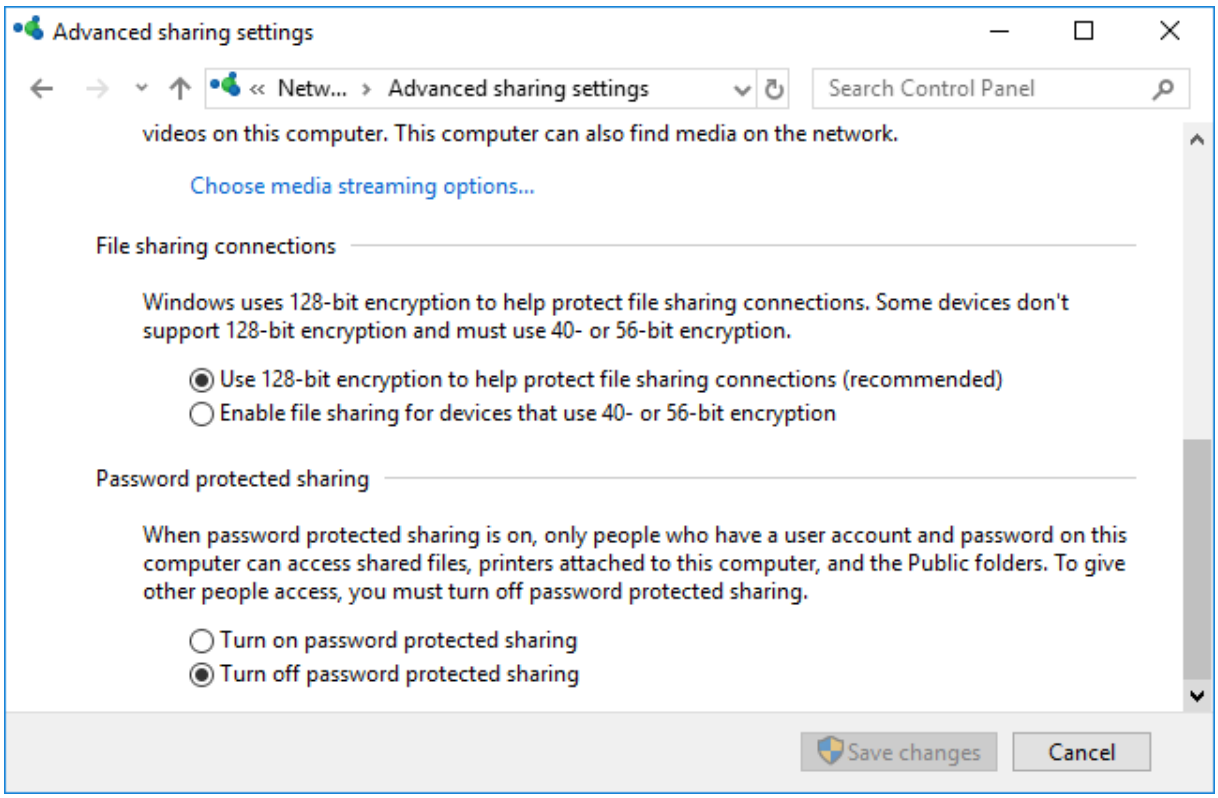
Vào ***Control Panel \ Network and Sharing Center***. Sau đó nhấn vào mục ***Change advanced sharing settings***.



Tại mục ***File and printer sharing*** click vào ***Turn on file and printer sharing***

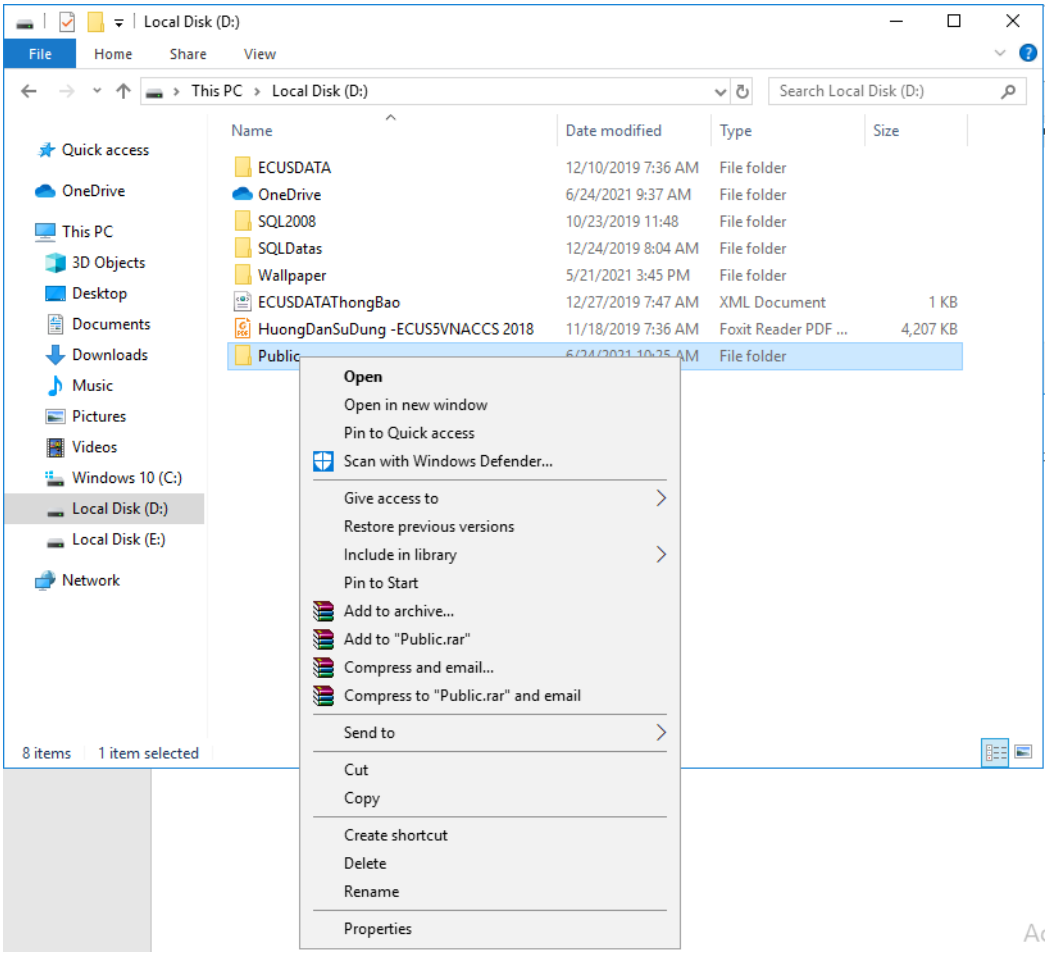


Tại mục ***Password protected sharing*** click vào ***Turn off password protected sharing***

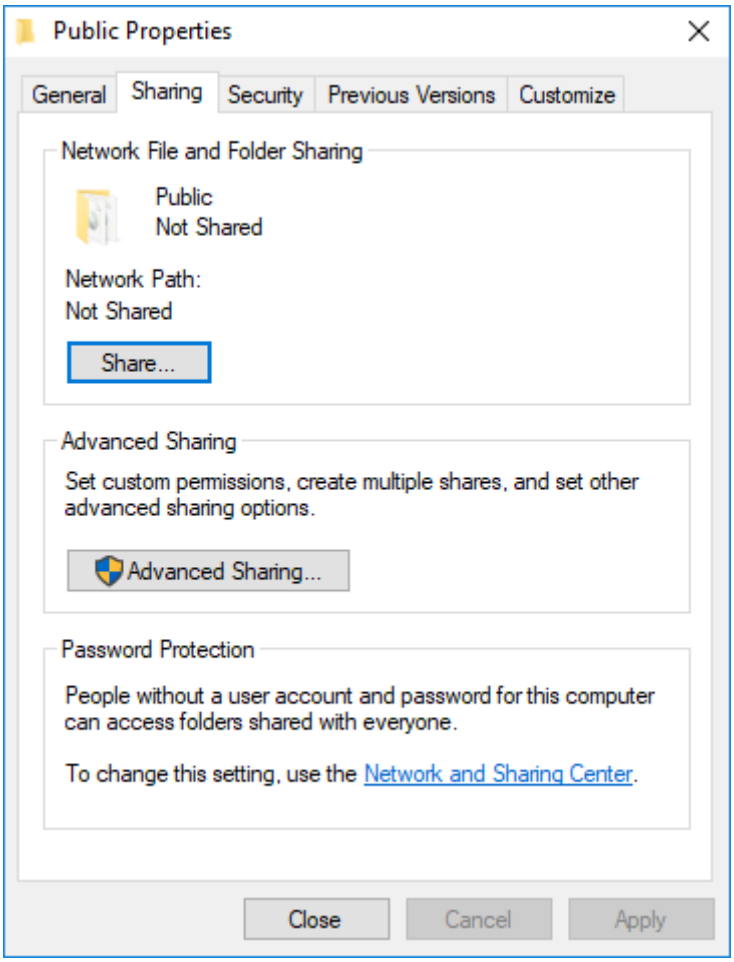


Bước 4: Chia sẻ dữ liệu qua mạng LAN

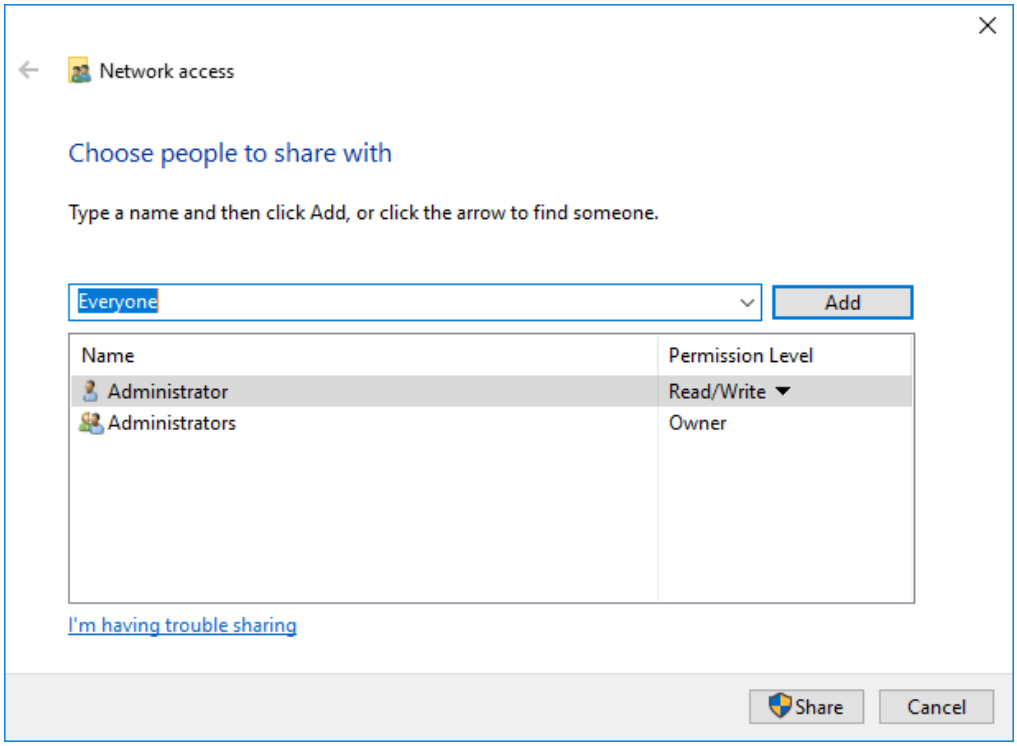
Đầu tiên, click chuột phải vào thư mục muốn chia sẻ, sau đó click chọn **Properties**



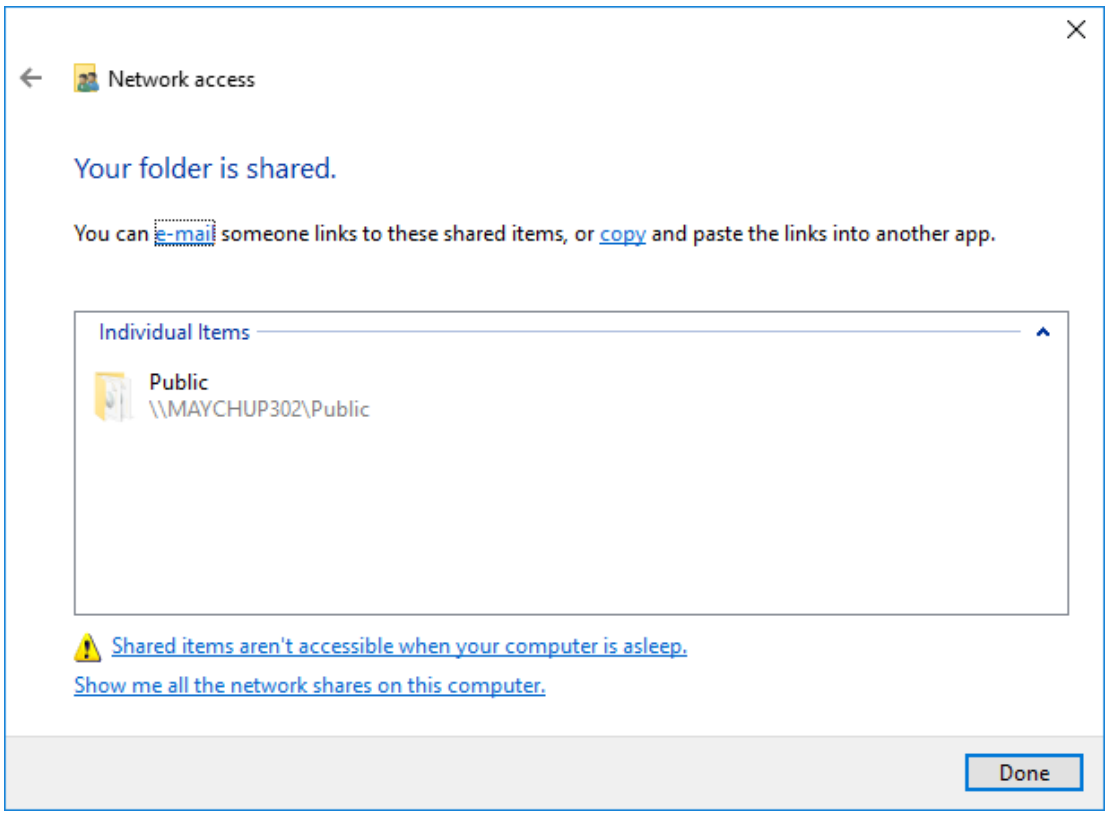
Xuất hiện cửa sổ ***Sharing Properties***. Click chọn thẻ ***Sharing***, trong mục ***Network file and Folder Sharing***, click nút ***Share***.



Ở hộp thoại tiếp theo sẽ chọn ***Everyone***. Click nút ***Add*** sau đó click nút ***Share***.

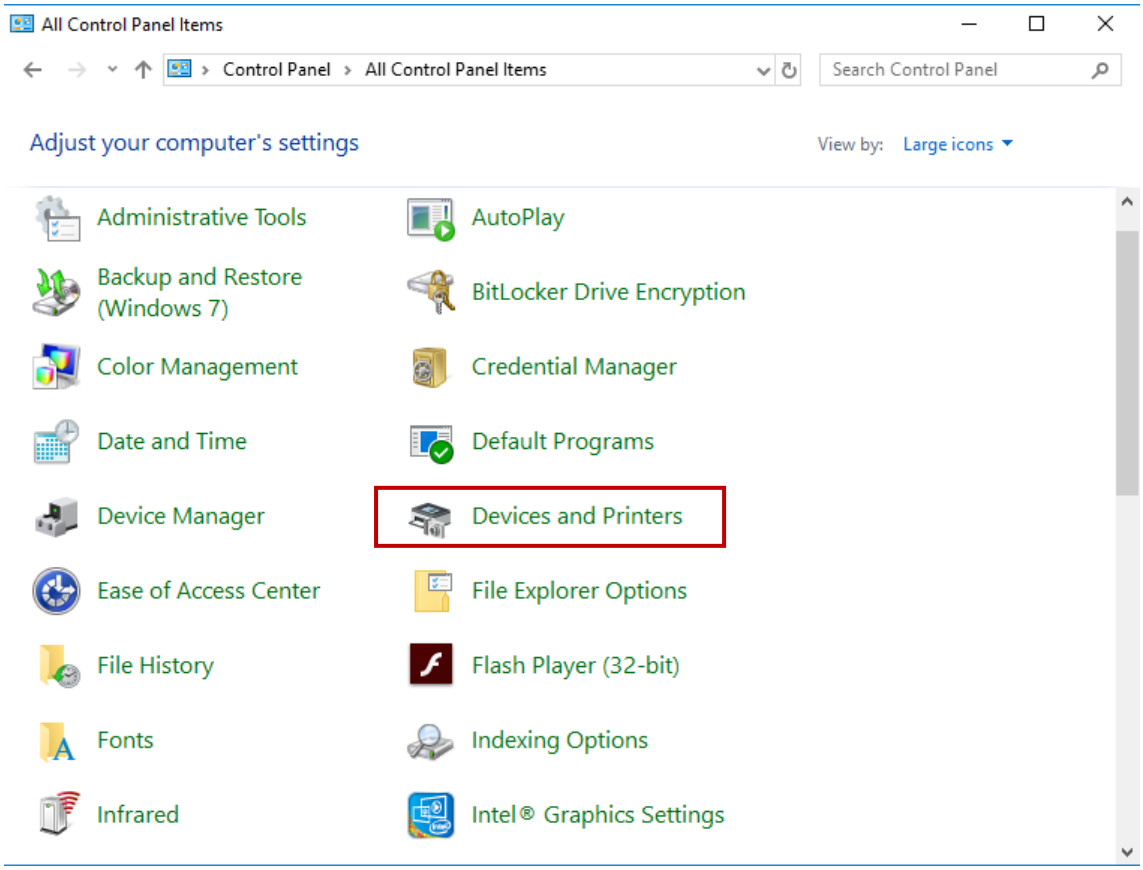


Thông báo chia sẻ thư mục thành công, click nút ***Done***

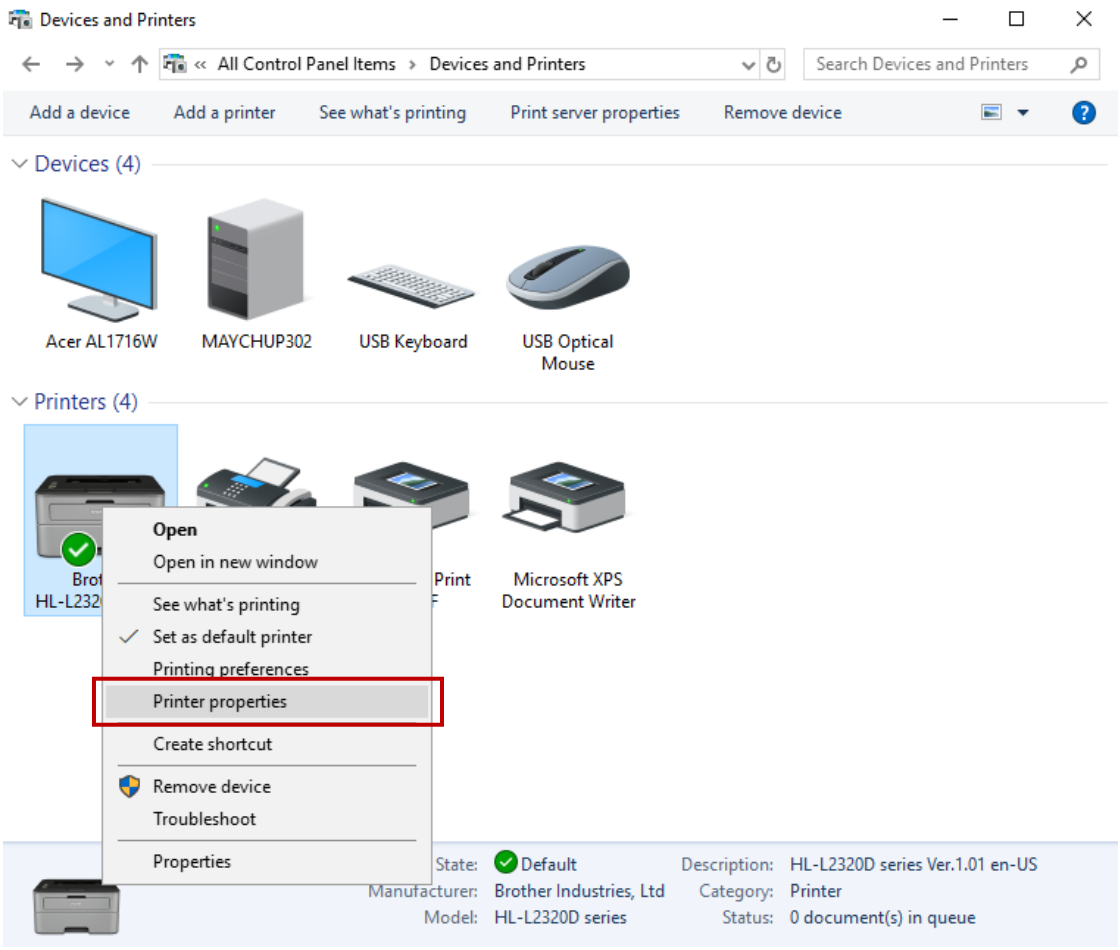


Bước 5: Chia sẻ máy in qua mạng LAN

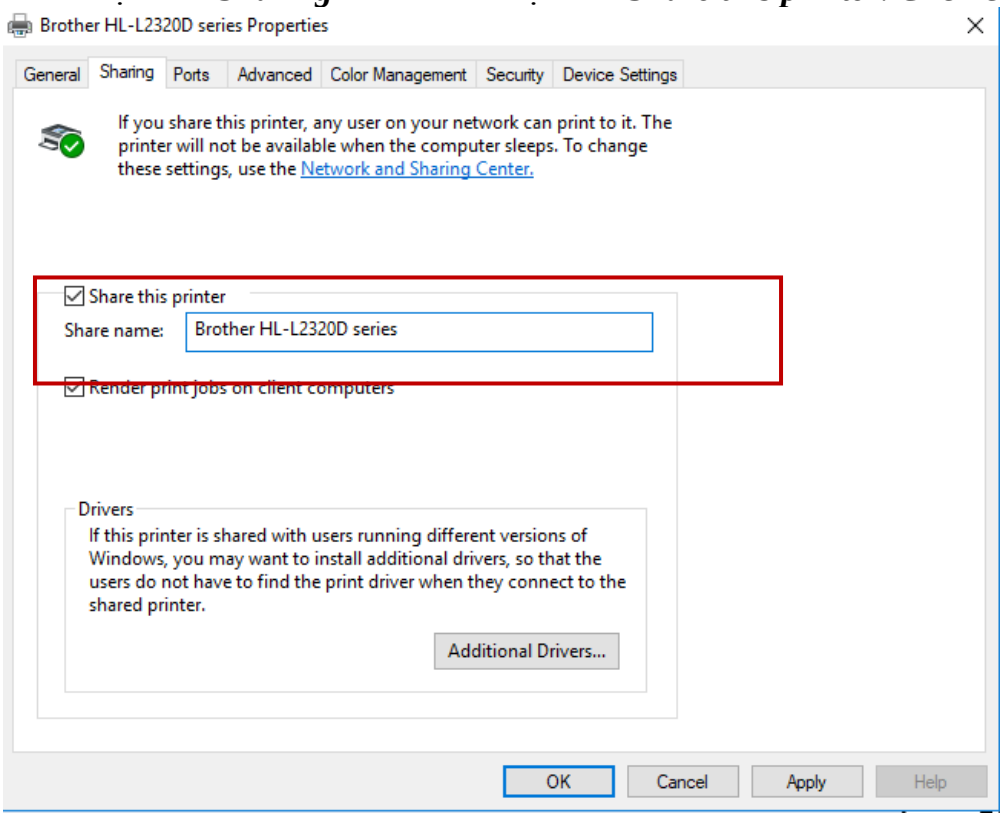
Thao tác này sẽ được thực hiện trên máy tính đang được kết nối với máy in là máy **PC1**. Vào ***Control Panel*** chọn ***Devices and Printers***



Click chuột phải vào biểu tượng máy in cần chia sẻ chọn ***Printer properties***

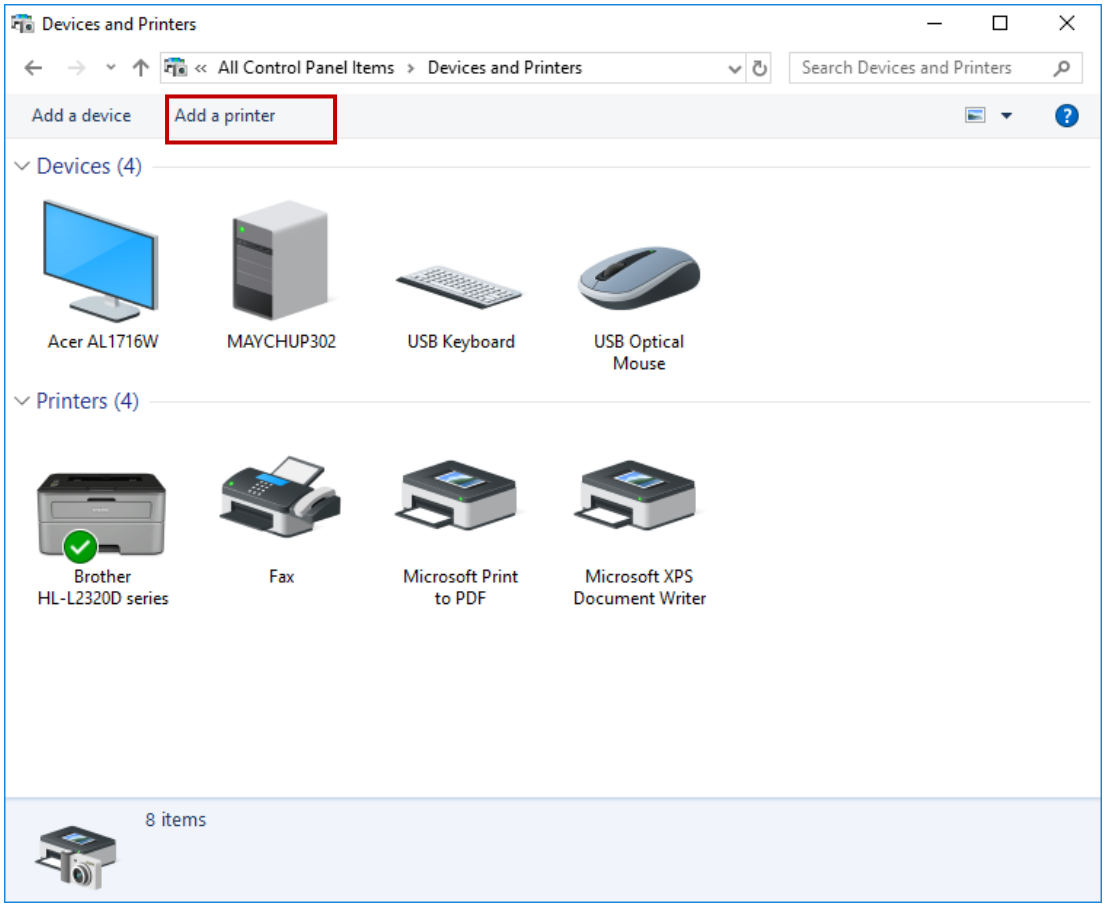


Chọn Tab ***Sharing***. Đánh dấu chọn vào ***Share this printer***. Click ***OK***

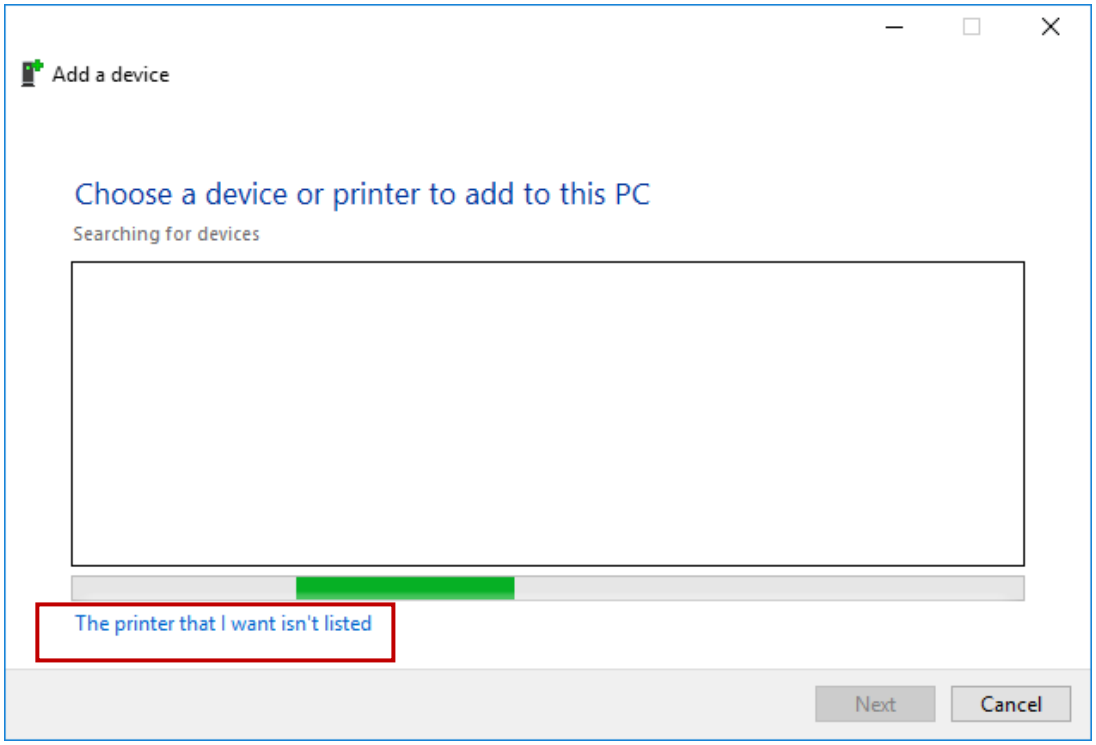


- Kết nối máy in đã chia sẻ

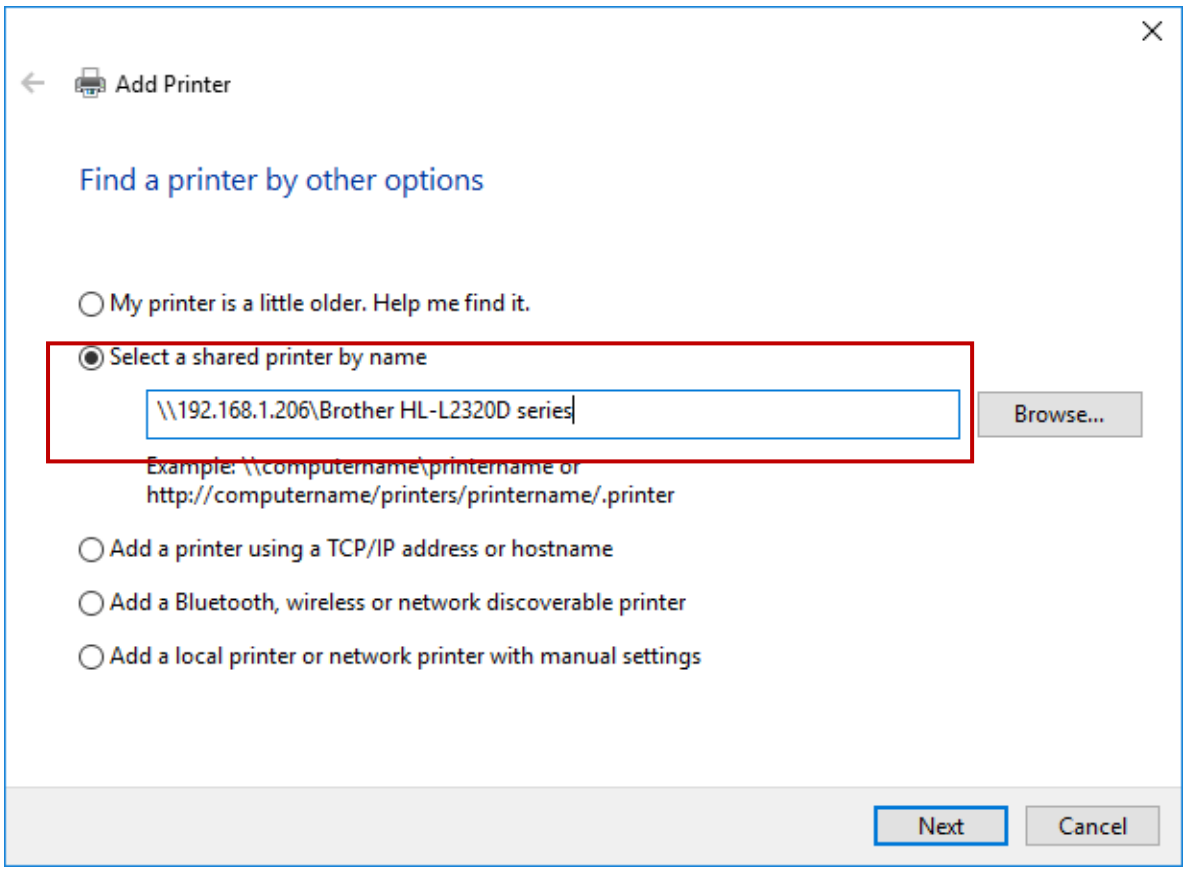
Thao tác này sẽ được thực hiện trên máy tính cần cài đặt máy in qua mạng LAN (máy PC2). Vào ***Control Panel*** chọn ***Devices and Printers***, click ***Add a Printer***



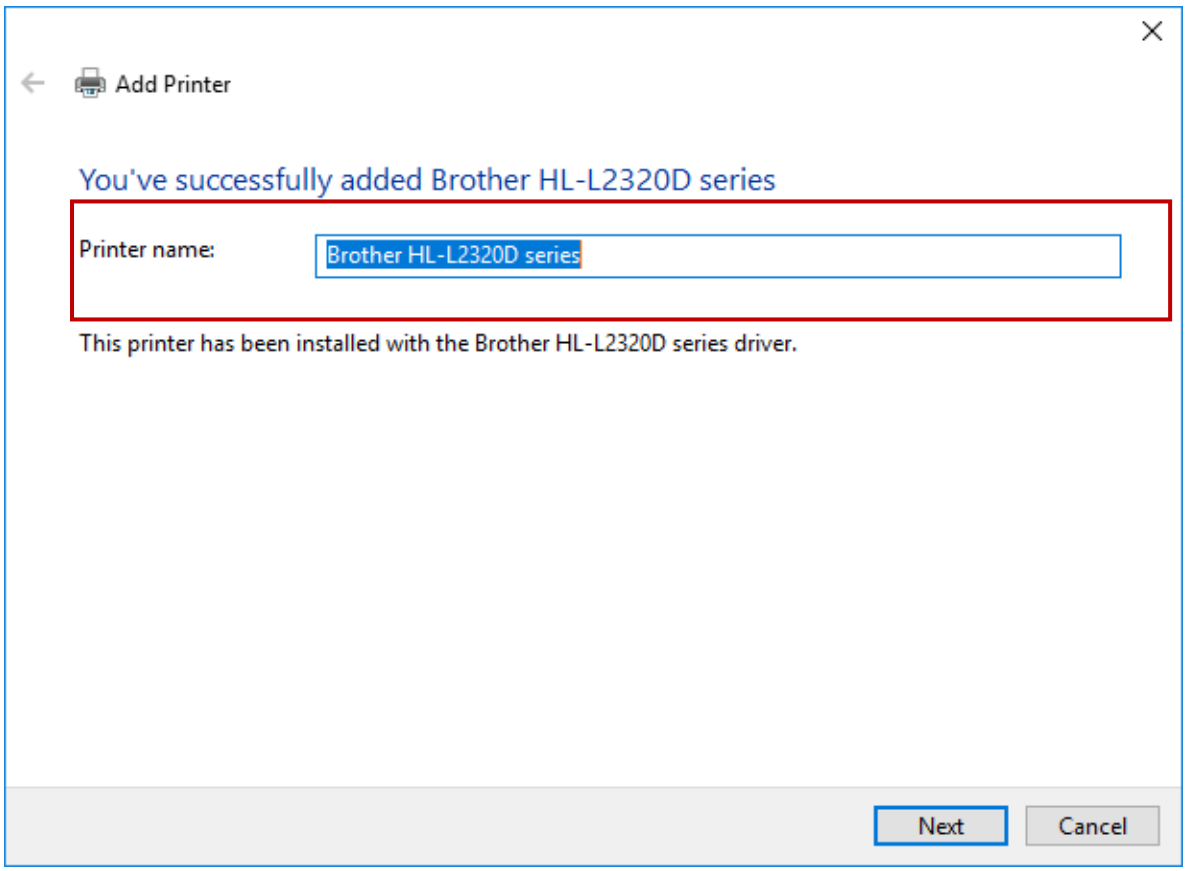
Cửa sổ hiện ra click ***The printer that I want isn't listed***



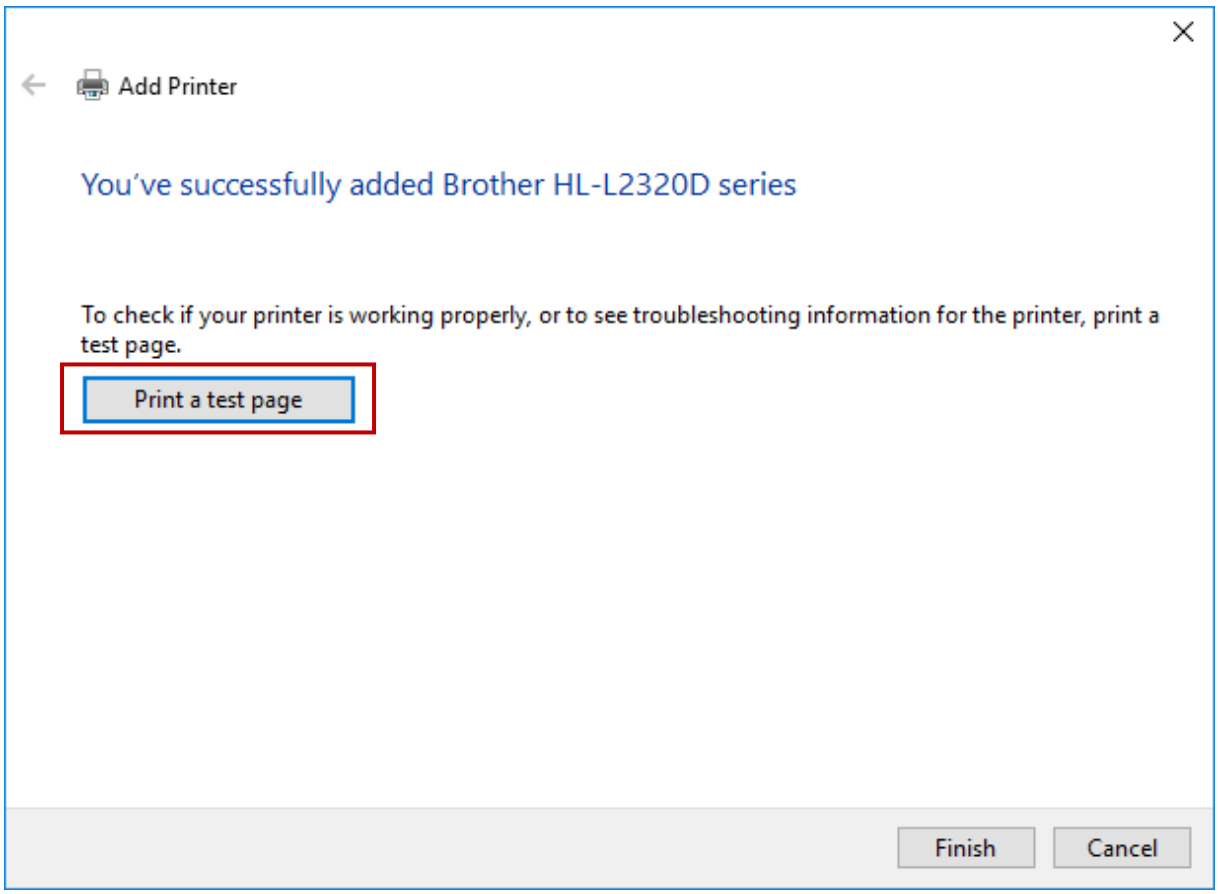
Đánh dấu vào tùy chọn ***Select a shared printer by name*** và nhập đúng tên máy tính và máy in đã chia sẻ, click ***Next.***



Đặt tên cho máy in trong ô ***Printer name***



Quá trình cài đặt đã thành công. Click ***Print a test page*** để in thử và click nút ***Finish*** để kết thúc cài đặt.



4. Yêu cầu kết quả

Kết nối các thiết bị sử dụng trong bài thực hành đúng theo sơ đồ đã ghi trong phần yêu cầu

Chia sẻ thành công thư mục đã chia sẻ trên máy tính PC1

Truy cập thành công thư mục đã chia sẻ trên máy tính PC1 trên máy tính PC2

Chia sẻ thành công máy in trên máy tính PC1

Kết nối thành công máy in đã chia sẻ trên máy tính PC1 trên máy tính PC2. Tiến hành in thử thành công

III. Sai hỏng và cách khắc phục

1. Không truy cập được thư mục đã chia sẻ trên máy tính PC1

- Nguyên nhân

Chưa tắt tường lửa Windows Firewall

Chưa chọn tính năng chia sẻ dữ liệu và máy in File and printer sharing

- Cách khắc phục

Tắt tường lửa Windows Firewall

Bật tính năng chia sẻ dữ liệu và máy in File and printer sharing

2. Khi truy cập thư mục đã chia sẻ trên máy tính PC1 bị yêu cầu mật khẩu truy cập

- Nguyên nhân

Chưa tắt tường lửa Windows Firewall

Chưa tắt tính năng yêu cầu mật khẩu khi truy cập thư mục chia sẻ Password protected sharing

- Cách khắc phục

Tắt tường lửa Windows Firewall

Tắt tính năng yêu cầu mật khẩu khi truy cập thư mục chia sẻ Password protected sharing

3. Kết nối máy in đã chia sẻ trên máy tính PC1 không thành công

- Nguyên nhân

Nhập địa chỉ IP, tên máy tính hoặc tên máy in đã chia sẻ chưa đúng

- Cách khắc phục

Kiểm tra và tiến hành nhập địa chỉ IP, tên máy tính hoặc tên máy in thật chính xác

V. Hướng dẫn ôn luyện

- Kết nối máy in với máy tính
- Chia sẻ dữ liệu giữa các máy tính
- Cài đặt máy in qua mạng nội bộ LAN

❖ TÓM TẮT PHẦN 1

Trong phần này, một số nội dung chính được thực hành:

- Bài 1: Bấm dây cập mạng.
- Bài 2. Kết nối thiết bị
- Bài 3: Chia sẻ dữ liệu và máy in

❖ BÀI TẬP PHẦN 1

- Bài 1: Thực hiện kỹ thuật bấm dây cáp mạng xoắn (cáp thẳng, cáp chéo)
- Bài 2: Thực hiện kết nối các thiết bị sử dụng dây cáp mạng và các thiết bị liên kết mạng (switch, router)
- Bài 3: Thực hiện cài đặt địa chỉ IP tĩnh cho các máy tính, tiến hành chia sẻ dữ liệu giữa các máy tính trong mạng nội bộ
- Bài 4: Thực hiện cài đặt địa chỉ IP động cho các máy tính, tiến hành chia sẻ máy in dùng chung trong mạng nội bộ

PHẦN 2: QUẢN TRỊ MẠNG WINDOW SERVER

❖ GIỚI THIỆU PHẦN 2

Phần 2 là phần thực hành các kiến thức quản trị mạng Windows Server.

❖ MỤC TIÊU PHẦN 2

Sau khi học xong phần này, người học có khả năng:

➢ ***Về kiến thức:***

- Trình bày được các bước thực hiện cài đặt hệ điều hành và các dịch vụ của máy chủ sử dụng hệ điều hành Windows Server trong hệ thống mạng nội bộ.
- Vận dụng được các kiến thức trên vào thực hành.

➢ ***Về kỹ năng:***

- Thực hiện được việc cài đặt hệ điều hành và các dịch vụ của máy chủ sử dụng hệ điều hành Windows Server trong hệ thống mạng nội bộ.

➢ ***Về năng lực tự chủ và trách nhiệm:***

- Ý thức được tầm quan trọng và ý nghĩa thực tiễn của việc thực hiện cài đặt hệ điều hành và các dịch vụ của máy chủ sử dụng hệ điều hành Windows Server trong hệ thống mạng nội bộ.
- Tích cực, chủ động và hợp tác trong học tập. Thể hiện sự nhiệt tình, trách nhiệm, tác phong nhanh nhẹn trong công việc.

❖ PHƯƠNG PHÁP GIẢNG DẠY VÀ HỌC TẬP PHẦN 2

- Đối với người dạy: sử dụng phương pháp giảng giảng dạy tích cực (diễn giảng, vấn đáp, thao tác mẫu); yêu cầu người học thực hiện thực hành phần 2 (cá nhân hoặc nhóm).
- Đối với người học: chủ động đọc trước giáo trình (phần 2) trước buổi học; hoàn thành đầy đủ bước thực hành và bài tập phần 2 theo cá nhân hoặc nhóm và nộp lại cho người dạy đúng thời gian quy định.

❖ ĐIỀU KIỆN THỰC HIỆN PHẦN 2

➢ ***Phòng học chuyên môn hóa/nhà xưởng:***

- Phòng học thực hành được trang bị hệ thống đèn đủ ánh sáng.
- Bàn ghế cho sinh viên.
- Bàn ghế giáo viên, bảng, phấn.

➢ ***Trang thiết bị máy móc:***

- Máy tính, máy chiếu

➢ ***Học liệu, dụng cụ, nguyên vật liệu:***

- Giáo án, bài giảng.
- Phần mềm hệ điều hành Windows Server.
- Dây mạng, kìm bấm mạng, các đầu nối RJ45, Hub, Switch, Router.

- Giáo trình nội bộ và các tài liệu giảng dạy khác hỗ trợ bài giảng

➢ ***Các điều kiện khác:*** Không có

❖ **KIỂM TRA VÀ ĐÁNH GIÁ PHẦN 2**

- **Nội dung:**

✓ Kiến thức: Kiểm tra và đánh giá tất cả nội dung đã nêu trong mục tiêu kiến thức

✓ Kỹ năng: Đánh giá tất cả nội dung đã nêu trong mục tiêu kĩ năng.

✓ Năng lực tự chủ và trách nhiệm: Trong quá trình học tập, người học cần:

+ Nghiên cứu bài trước khi đến lớp

+ Chuẩn bị đầy đủ tài liệu học tập.

+ Tham gia đầy đủ thời lượng môn học.

+ Nghiêm túc trong quá trình học tập.

- **Phương pháp:**

✓ Điểm kiểm tra thường xuyên: không có

✓ Kiểm tra định kỳ: 3 điểm kiểm tra (hình thức: thực hành)

BÀI 1: CÀI ĐẶT VÀ CẤU HÌNH WINDOWS SERVER 2012

I. Lý thuyết liên quan

1. Giới thiệu về Windows Server 2012

Windows Server 2012 (tên mã là Windows Server 8) là tên mã cho hệ điều hành dành cho máy chủ được phát triển bởi Microsoft. Nó là một phiên bản Windows 8 và nối tiếp phiên bản Windows Server 2008 R2. Windows Server 8 là phiên bản Windows Server đầu tiên không hỗ trợ cho các máy tính dựa nền tảng kiến trúc Itanium từ lúc ra đời Windows NT 4.0. Một phiên bản phát triển thử nghiệm (phiên bản Beta) được công bố vào ngày 9 tháng 9 năm 2011 tới các lập trình viên phát triển. Vào ngày 1 tháng 3 năm 2012, Microsoft phát hành phiên bản Beta công cộng beta (build 8250).

2. Các phiên bản của Windows Server 2012

Windows Server 2012 gồm 4 phiên bản: Datacenter, Standard, Essential, Foundation. Hãng loại bỏ 2 phiên bản dành cho người dùng doanh nghiệp vừa và nhỏ là Windows Small Business Server, Windows Home Server.

- Windows Server 2012 Standard operating system
  - Cung cấp tất cả roles và features của window server 2012
  - Hỗ trợ: 64sockets, 4TB RAM, 2 máy ảo bản quyền
- Windows Server 2012 Datacenter operating system
  - Cung cấp tất cả roles và features của window server 2012
  - Không giới hạn số máy ảo bản quyền
  - Hỗ trợ 64 sockets, 640 processor cores, 4 TB RAM
- Windows Server 2012 Foundation operating system
  - Dành cho doanh nghiệp nhỏ
  - Không thể tham gia vào miền (domain)
  - Hạn chế sever roles
  - Hỗ trợ một lõi xử lý (32GB RAM)
- Windows Server 2012 Essentials operating system
  - Phiên bản tiếp theo FOS.
  - Phải là root server trong miền.
  - Không có chức năng máy chủ Hyper-V®, Failover Clustering, Server Core, Remote Desktop Services.
  - Giới hạn 25 người dùng và 50 thiết bị.
  - Hỗ trợ hai lõi xử lý và 64 GB bộ nhớ RAM.

3. Tổng quan về quản trị windows server 2012

- Server Manager

Server Manager là công cụ đồ họa chính được sử dụng để quản lý máy tính chạy Windows Server 2012.

Server Manager console có thể được sử dụng để quản lý cả các máy chủ nội bộ và máy chủ từ xa.

Server Manager được sử dụng để quản lý các máy chủ như các nhóm

Server manager console có thể được sử dụng để thực hiện các nhiệm vụ sau đây trên cả hai máy local server và remote server:

- Add roles and features
- Launch Windows PowerShell sessions
- View events
- Perform server configuration tasks

- Administrative Tools and Remote Server Administration Tools

+ Sử dụng khi nào?

Khi người dùng sử dụng Server Manager để thực hiện một công việc (task) liên quan đến vai trò (role) hoặc tính năng (feature) cụ thể liên quan

Khi người dùng cài đặt một role hoặc feature sử dụng Server Manager locally or remote

+ Ví dụ:

Nếu người dùng sử dụng Server Manager để cài đặt DHCP role trên một server khác, thì người dùng nên cài đặt DHCP console trên máy cục bộ (local).

+ Các tools hay được sử dụng

- Active Directory Administrative Center:

Thực hiện các lệnh như nâng cấp domain/ forest functional levels, kích hoạt Active Directory Recycle Bin

Sử dụng để quản lý Dynamic Access Control.

- Active Directory Users and Computers:

Tạo và quản lý Active Directory users, computers, groups.

Tạo Organizational Units (OUs).

- DNS console

Có thể cấu hình và quản trị DNS Server role: thực hiện tạo forward and reverse lookup zones, và quản trị các bản ghi DNS.

- Event Viewer: Có thể xem các bản ghi sự kiện (events recorded) xảy ra trên Windows Server 2012.
- Group Policy Management Console

Chỉnh sửa Group Policy Objects (GPO) và Quản lý các ứng dụng của của GPO trong AD DS.

- IIS Manager Tool

Quản lý các trang web.

- Resource Monitor

Xem thông tin thời gian thực về CPU, bộ nhớ, và đĩa và sử dụng mạng.

- Task Scheduler

Quản lý việc thực hiện các nhiệm vụ theo lịch trình.

II. Trình tự thực hiện

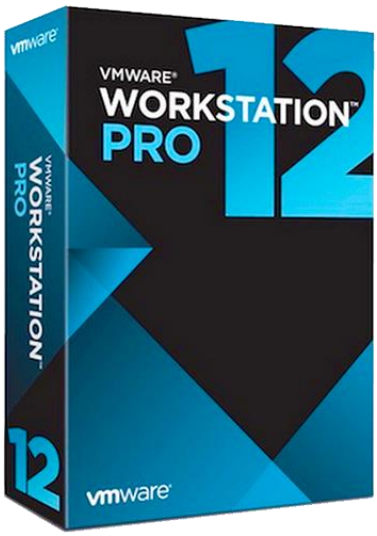
1. Yêu cầu thực hiện

- Cài đặt phần mềm máy ảo Wmware
- Cài hệ điều hành Windows server 2012 trên máy ảo Wmware
- Cấu hình hệ điều hành Windows server 2012

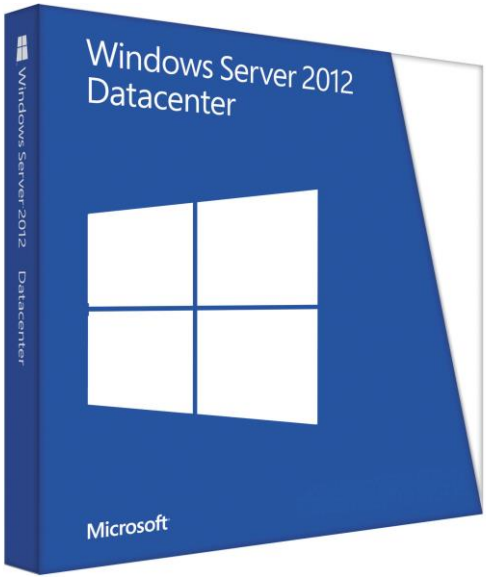
2. Thiết bị, dụng cụ, vật liệu

Máy vi tính

Phần mềm máy ảo Wmware 12 Pro



Phần mềm hệ điều hành Windows server 2012



3. Các bước thực hiện

Thực hiện cài đặt và cấu hình Windows Server 2012 thông qua 3 bước sau:

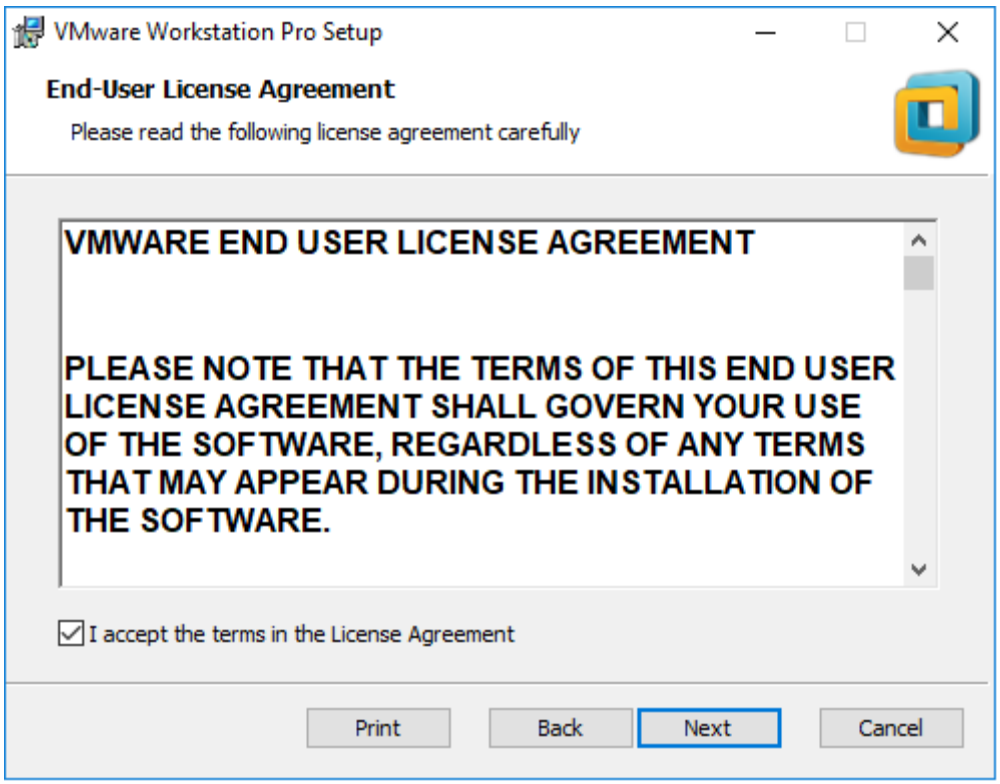
- Bước 1: Cài đặt phần mềm Vmware 12 Pro
- Bước 2: Cài đặt hệ điều hành Windows Server 2012 Datacenter (GUI)
- Bước 3: Cấu hình hệ điều hành Windows server 2012

Hướng dẫn chi tiết

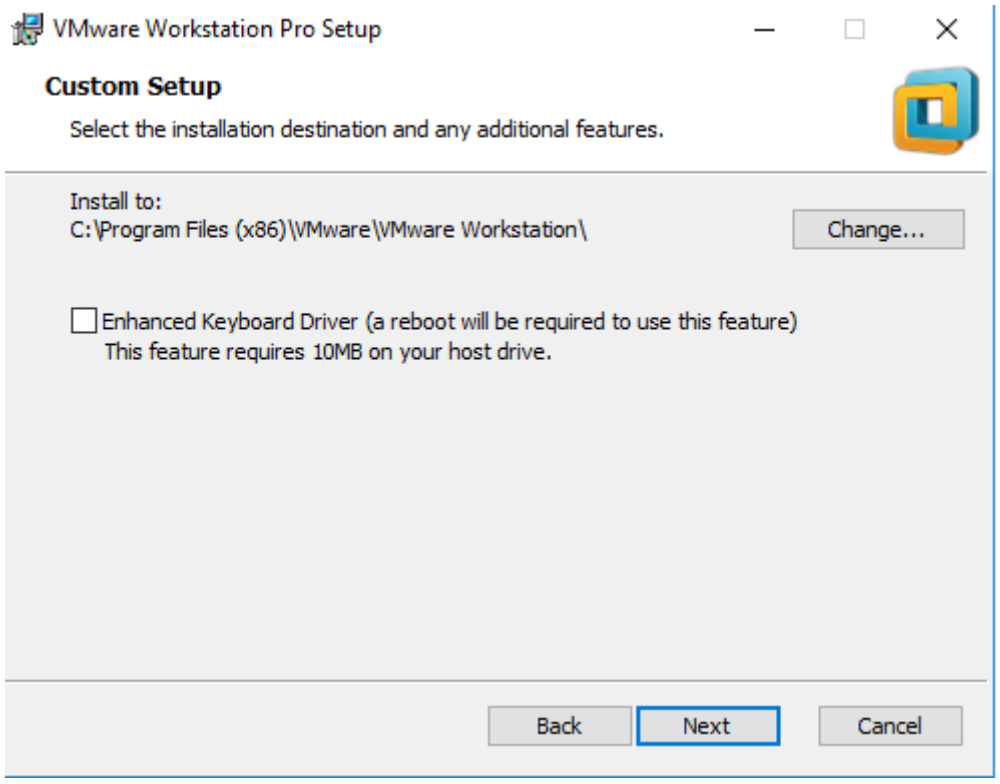
Bước 1: Cài đặt phần mềm Vmware 12 Pro

Khởi chạy file ***VMware-workstation-full-12.0.0-2985596.exe***. Sau khi phần mềm chạy lên nhấn ***Next*** để tiếp.

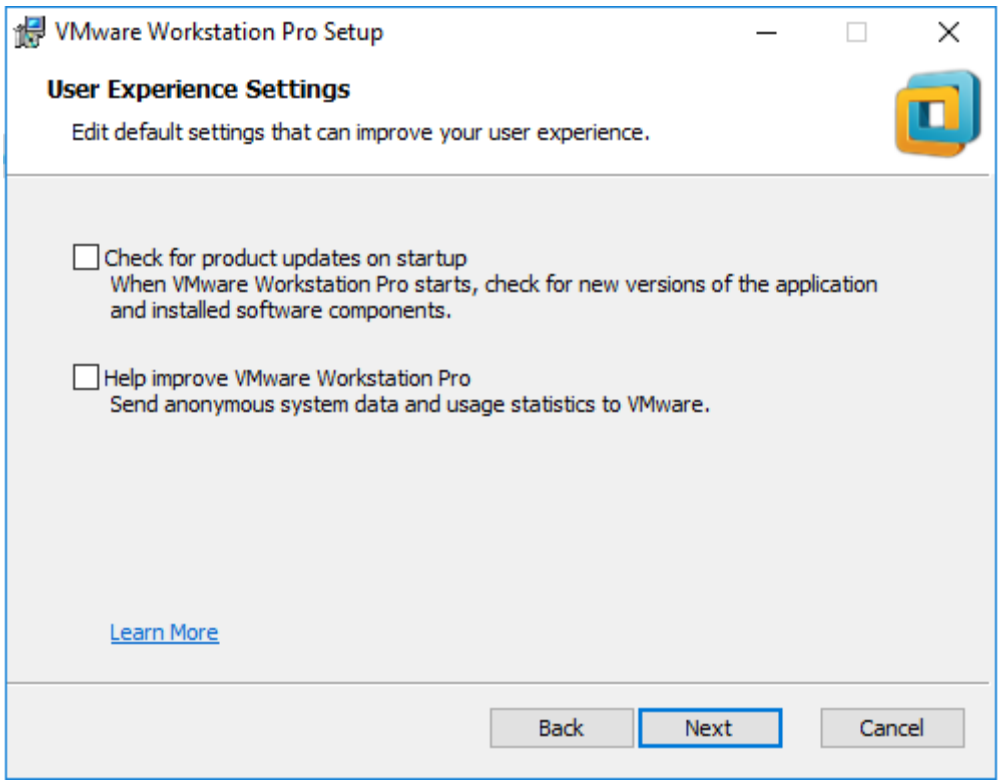
Chọn "***I accept the terms in the License Agreement***" sau đó nhấn Next để tiếp tục.



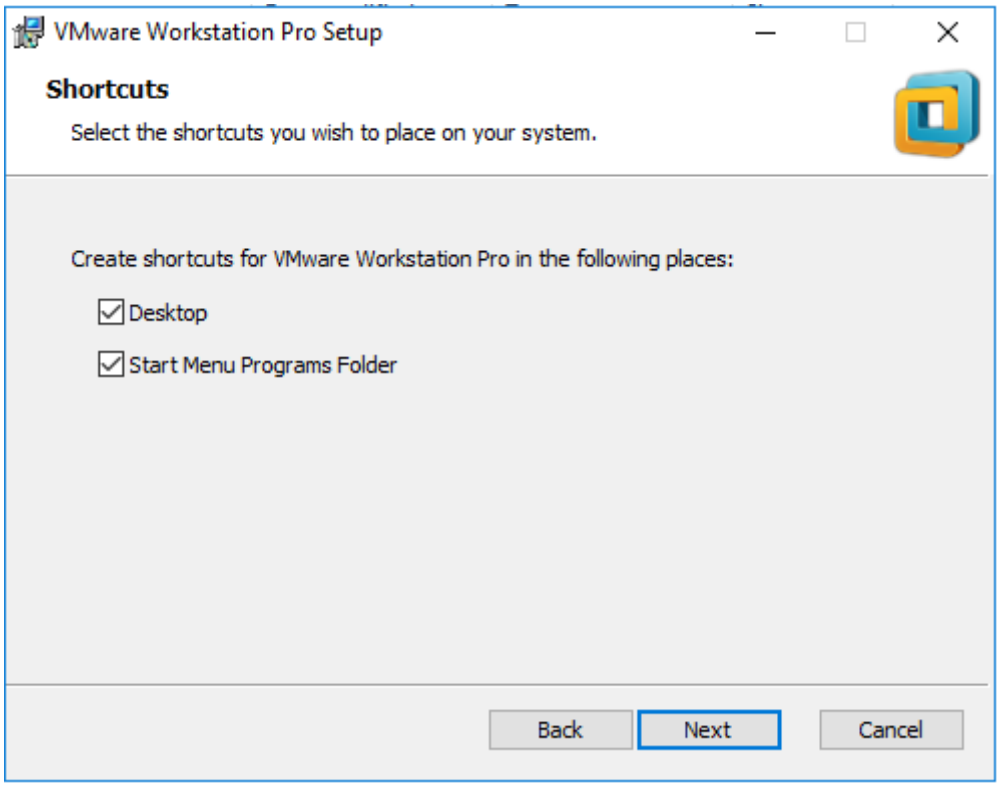
Nhấn ***Next*** để tiếp tục.



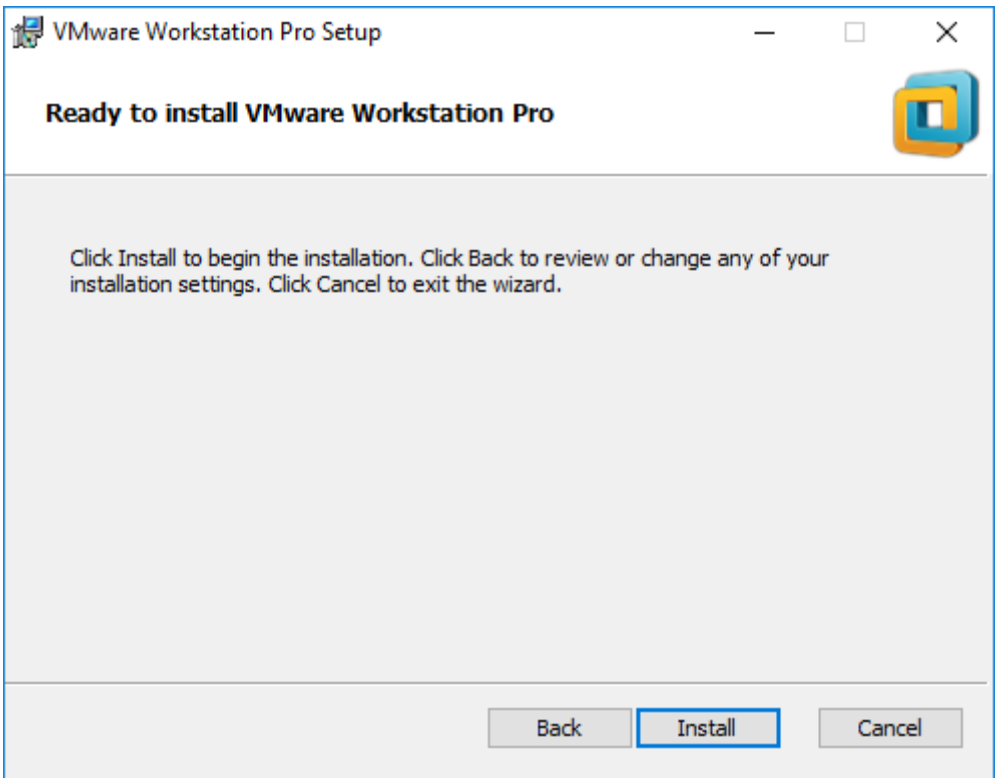
Bỏ chọn 2 phần như trong hình sau đó nhấn ***Next*** để tiếp tục.



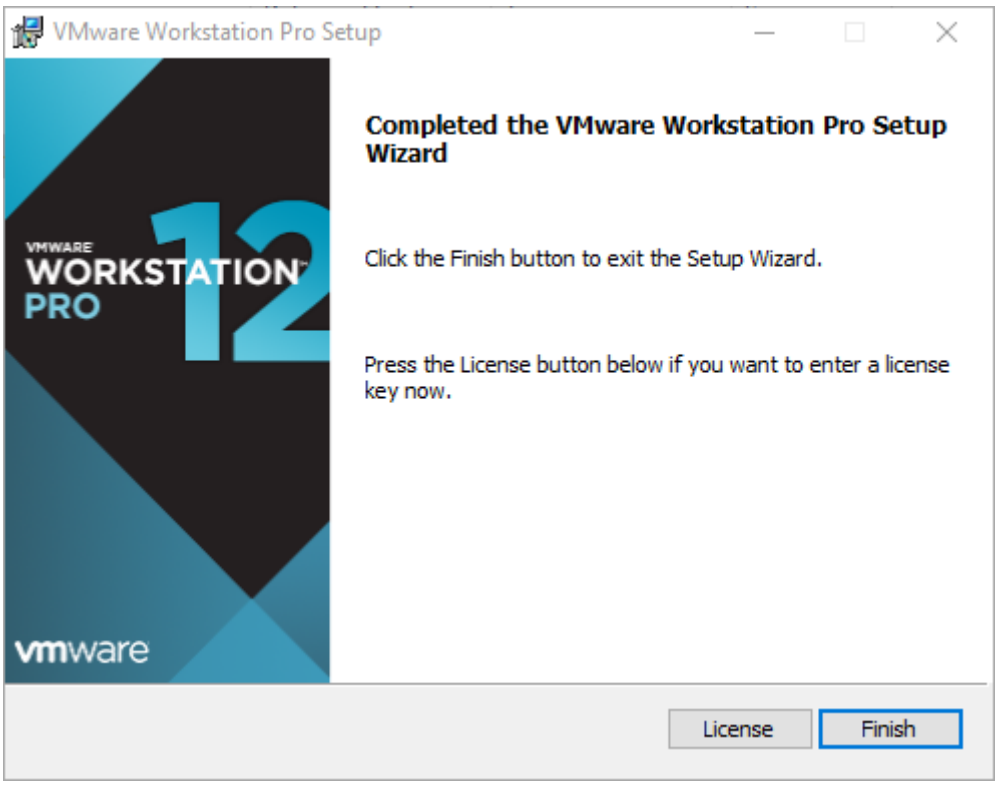
Chọn ***Desktop*** như trong hình sau đó nhấn ***Next*** để tiếp tục.



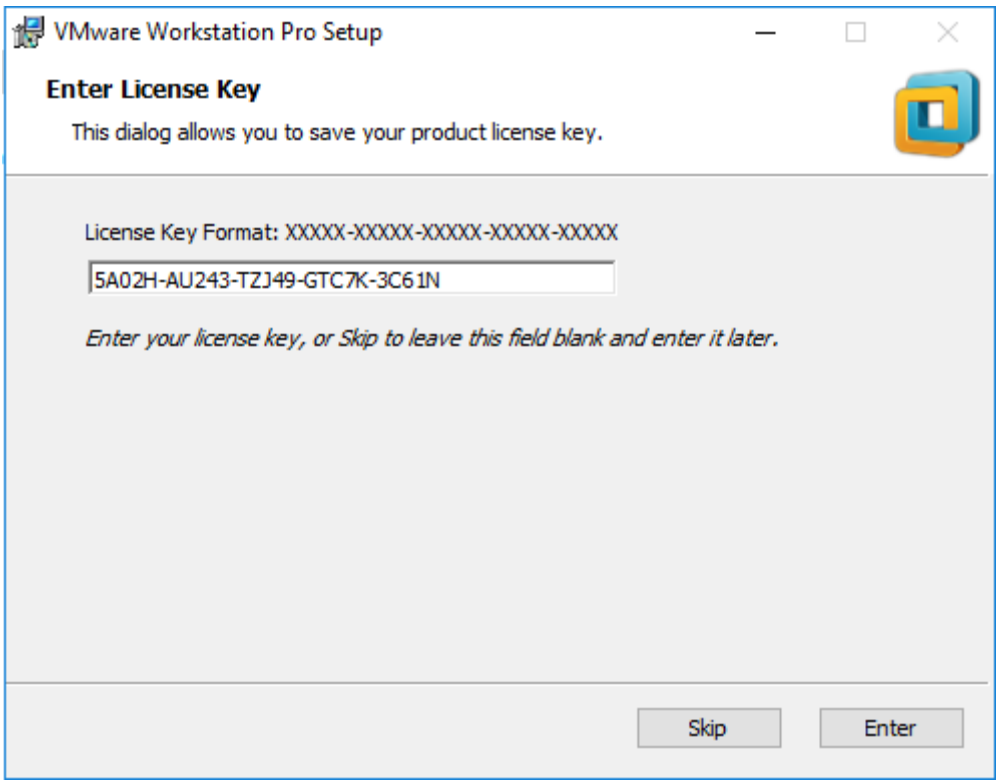
Chọn ***Install*** như trong hình để quá trình cài đặt được diễn ra.



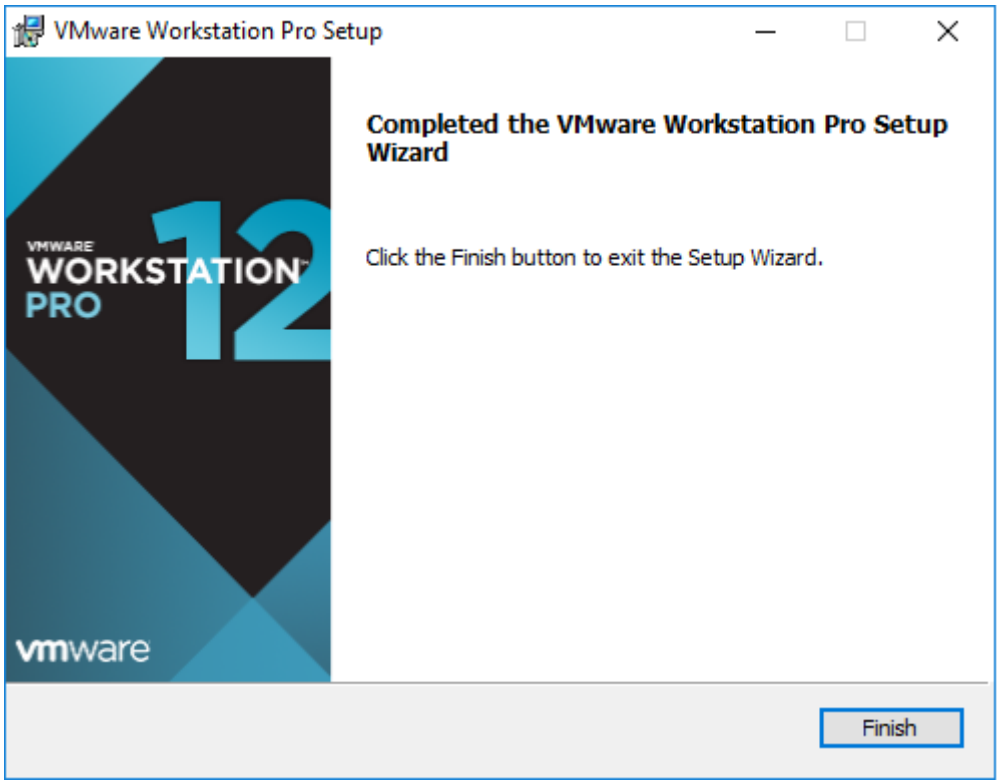
Quá trình cài đặt thành công nhấn ***License*** để kích hoạt phần mềm.



Nhập *License Key* vào khung như hình sau đó nhấn ***Enter*** để hoàn thành.

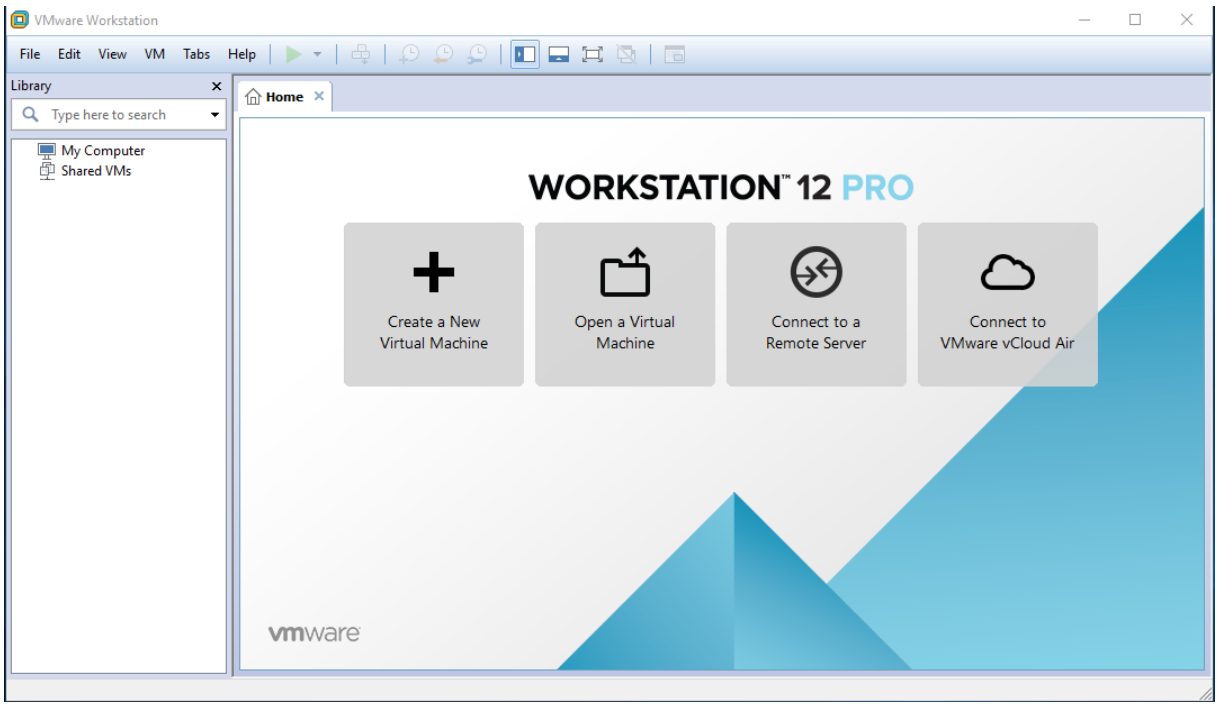


Quá trình kích hoạt phần mềm đã xong nhấn ***Finish*** để kết thúc.



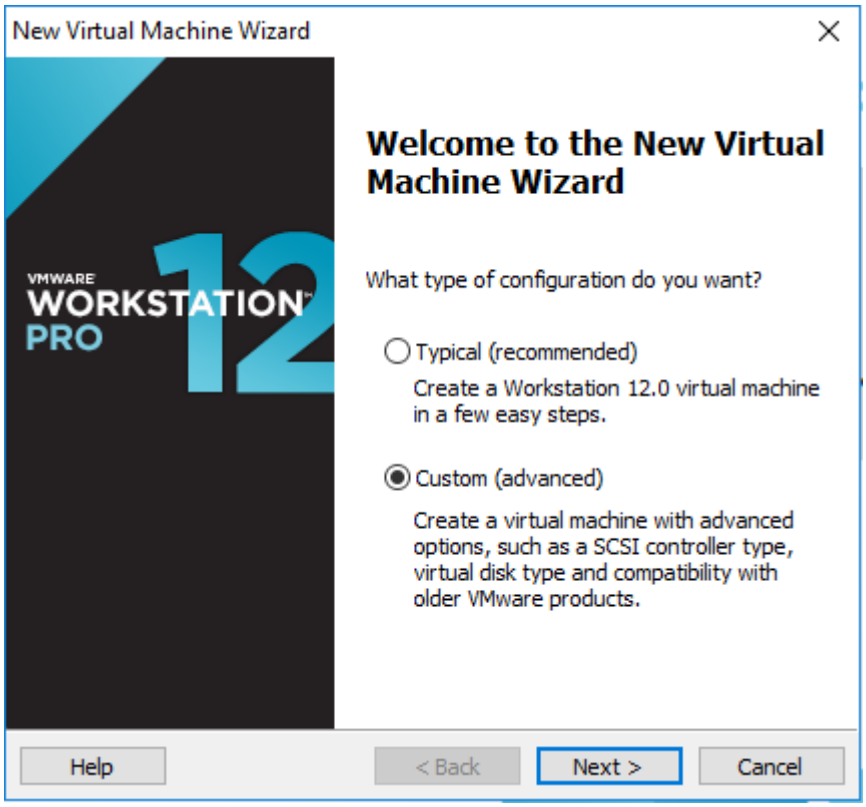
Bước 2: Cài đặt hệ điều hành Windows Server 2012 Datacenter (GUI)

Mở phần mềm máy ảo ***VMware Workstation 12 Pro***.

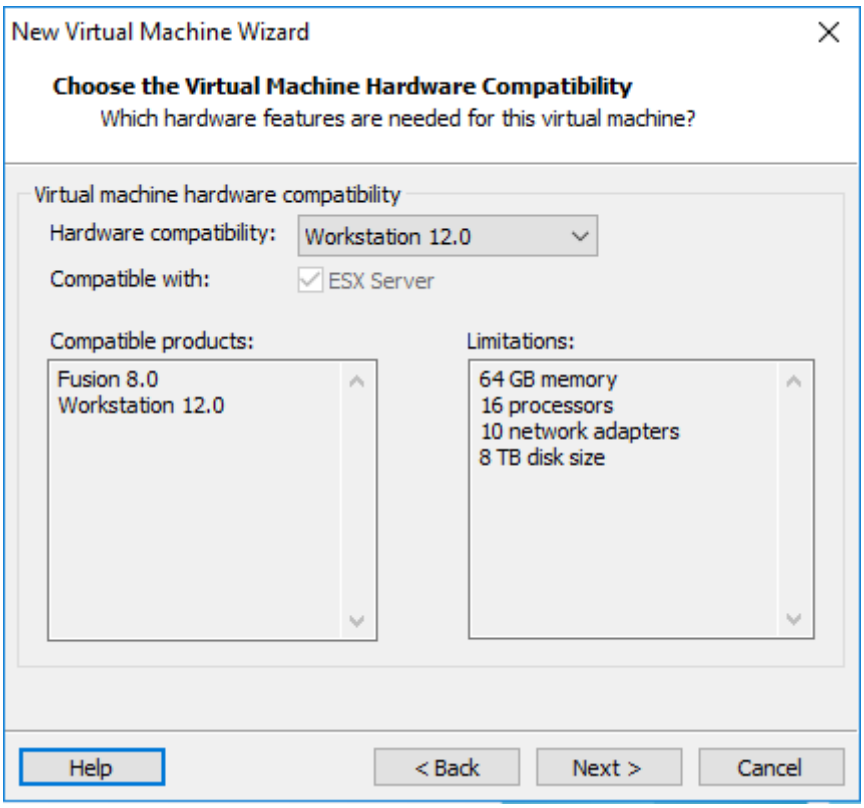


Chọn ***File / New Virtual Machine***… hoặc ấn ***Ctrl + N*** để tạo 1 máy ảo mới.

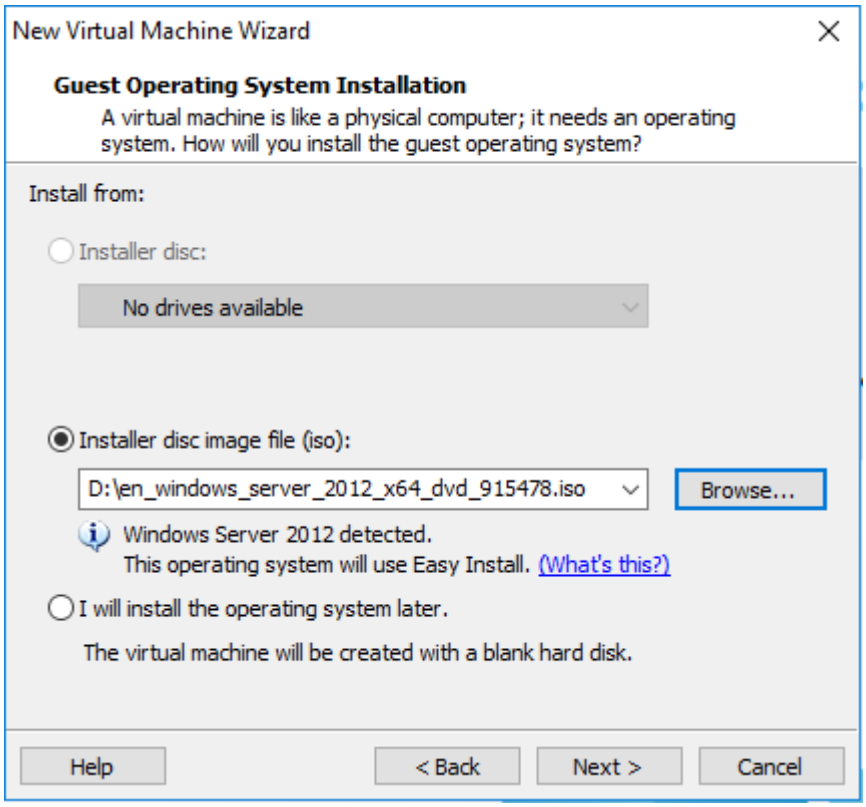
Tại cửa sổ ***New Virtual Machine Wizard***, chọn vào ***Custom (advanced).***



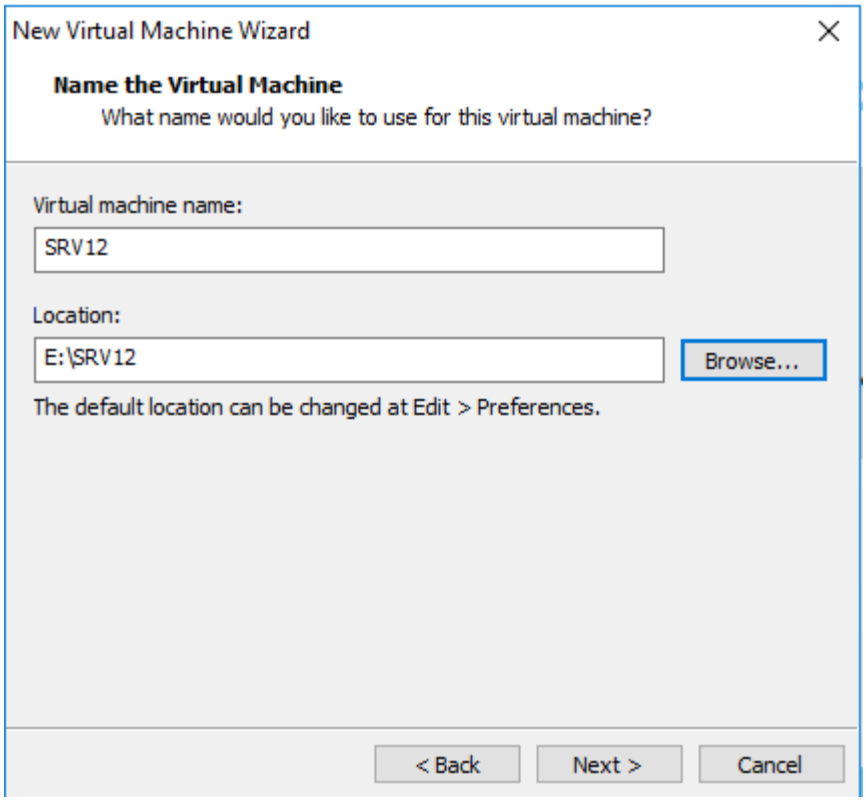
Tại cửa sổ ***Choose the Virtual Machine Hardware Compatibility***, chọn ***Workstation 12.0*** (phiên bản của VMware). Sau đó bấm ***Next.***



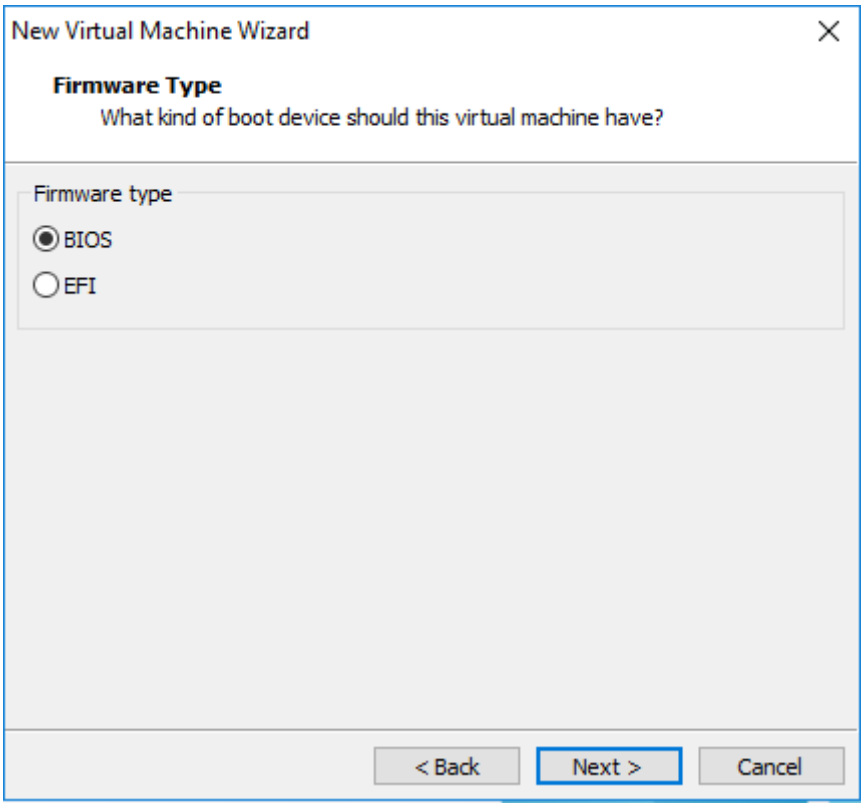
Tại cửa sổ ***Guest Operating System Installation*** chọn vào ***Installer disc image file (iso)*** để dùng file iso để cài đặt. ***Browse***… đến thư mục chứa file iso.



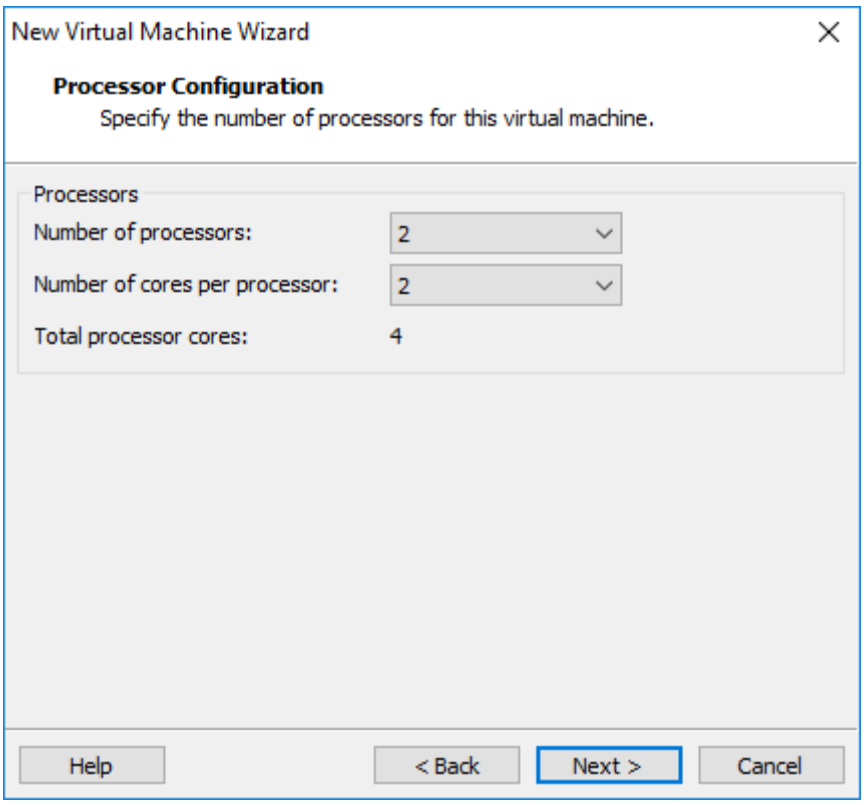
Tại cửa sổ ***Name the Virtual Machine***, sửa tên máy ảo tại ***Virtual machine name***, và chọn đường dẫn tới thư mục cần lưu máy ảo đang tạo tại ***Location/ Browse***… Sau đó bấm ***Next.***



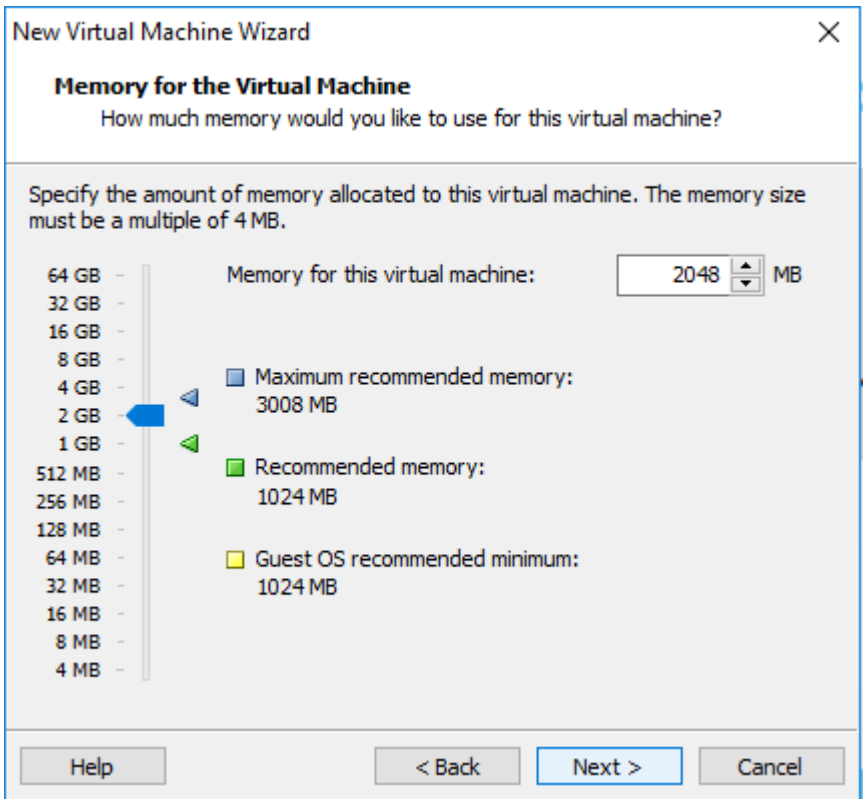
Tại cửa sổ ***Firmware Type***, chọn vào ***BIOS***



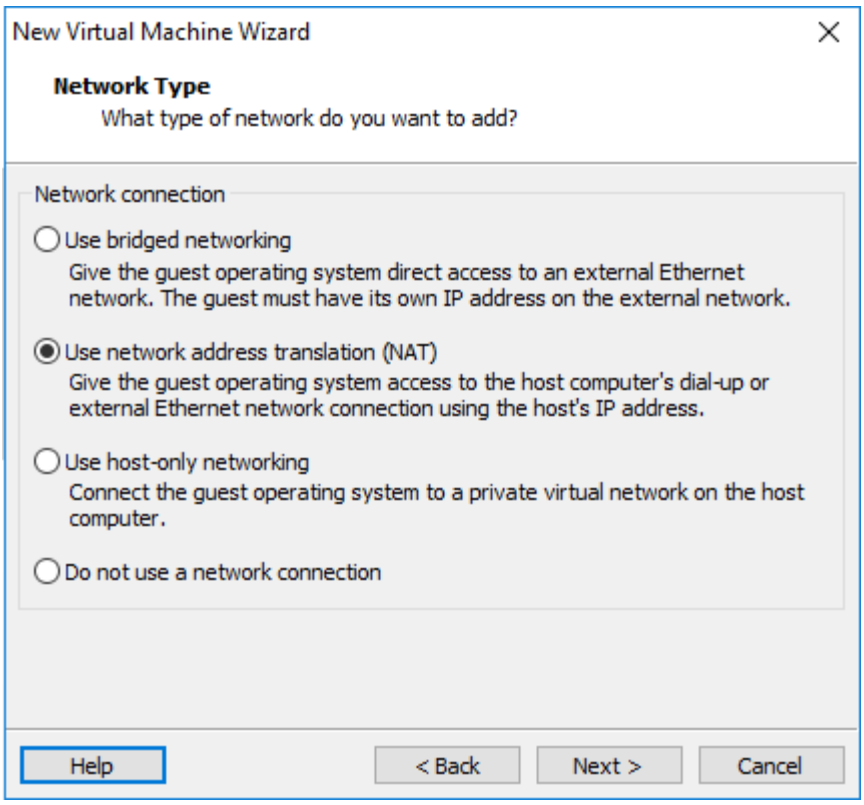
Tại cửa sổ ***Processor Configuration***, chọn như hình bên dưới.



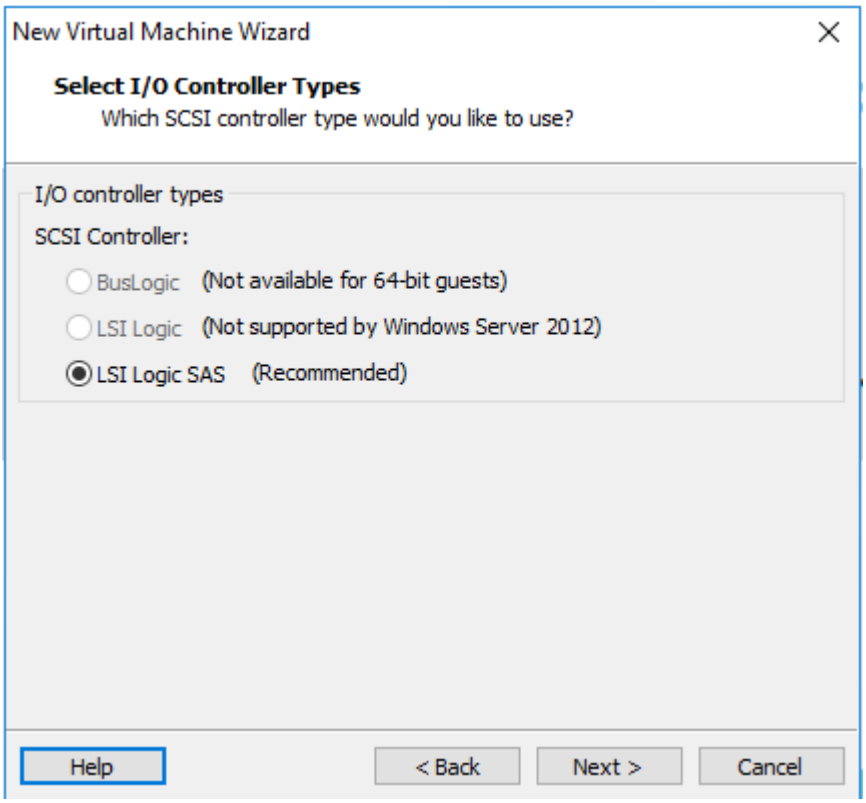
Tại cửa sổ ***Memory for the Virtual Machine***, chọn dung lượng bộ nhớ RAM.



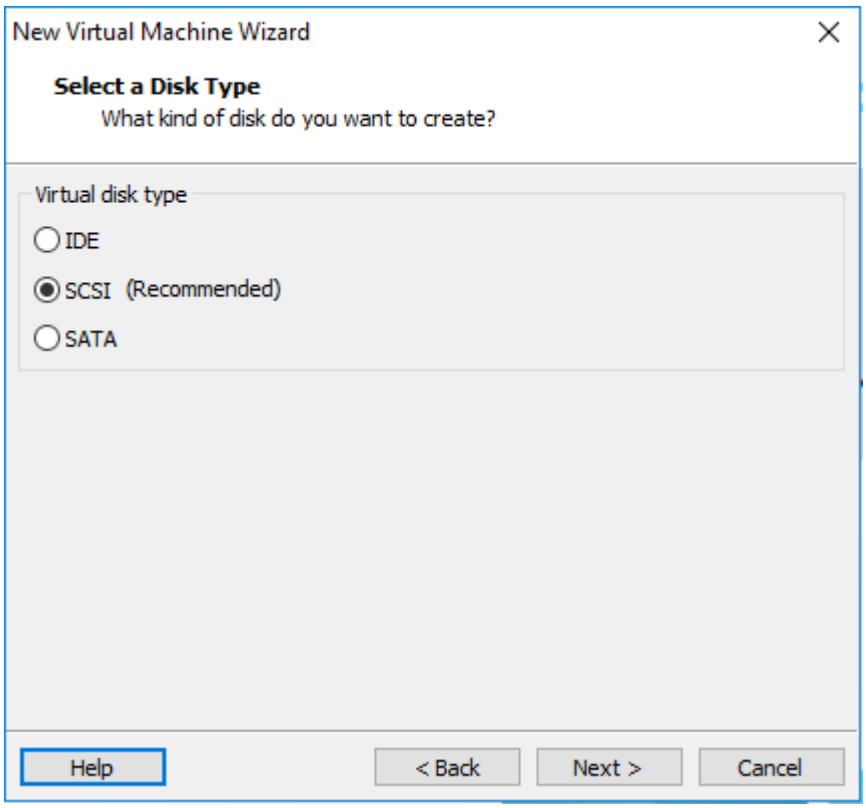
Tại cửa sổ ***Network Type***, chọn các tùy chọn card mạng cho máy ảo.



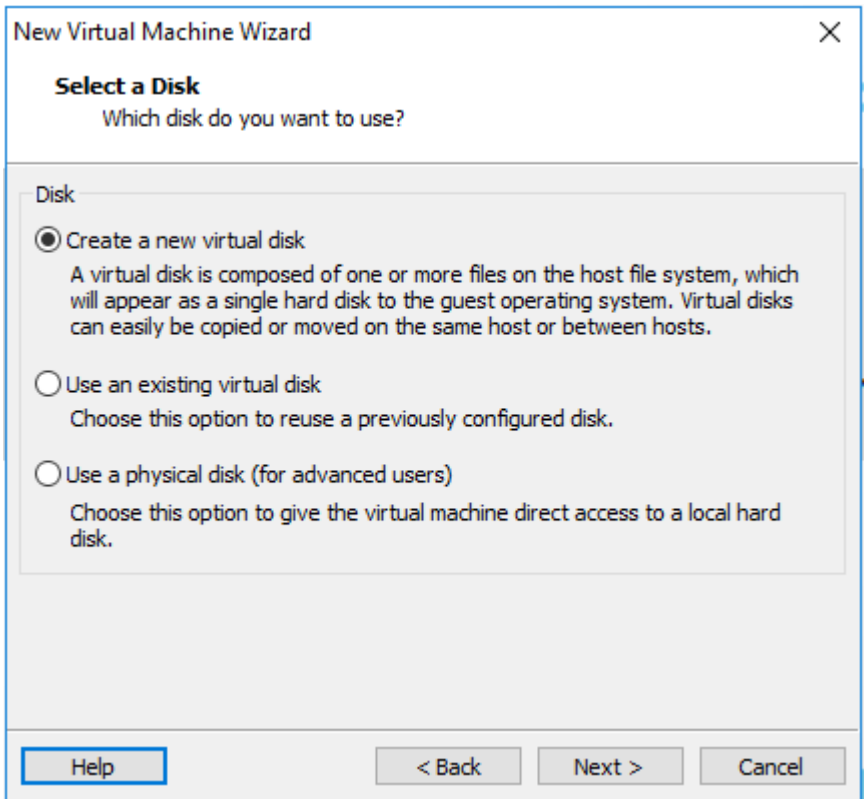
Tại cửa sổ ***Select I/O Controller Types***, chọn vào ***LSI Logic SAS (Recommended)***



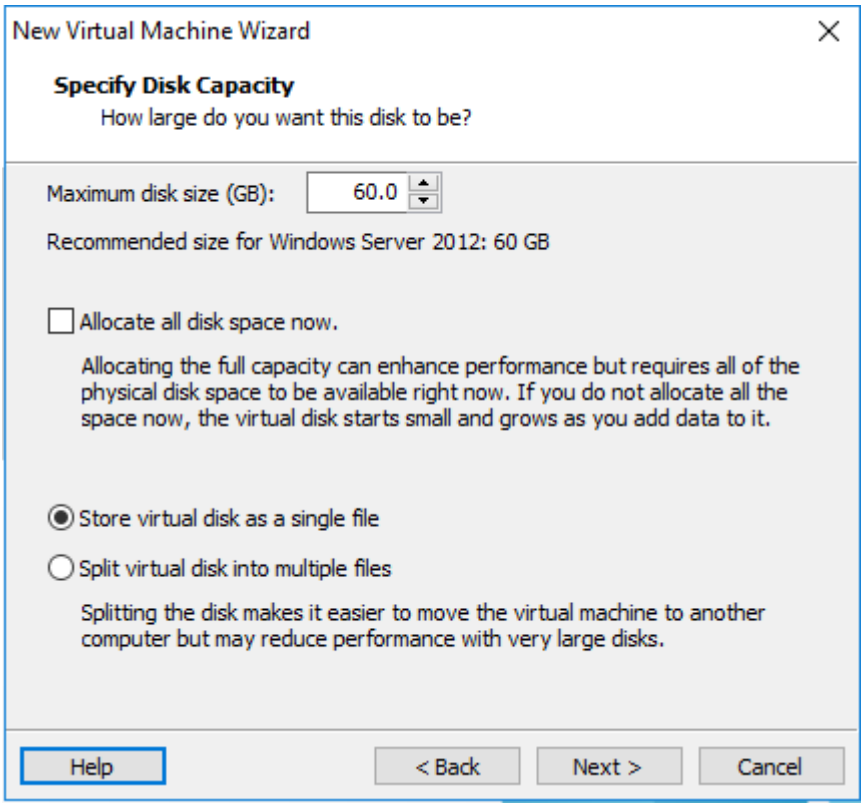
Tại ***Select a Disk Type*** ,chọn vào ***SATA***



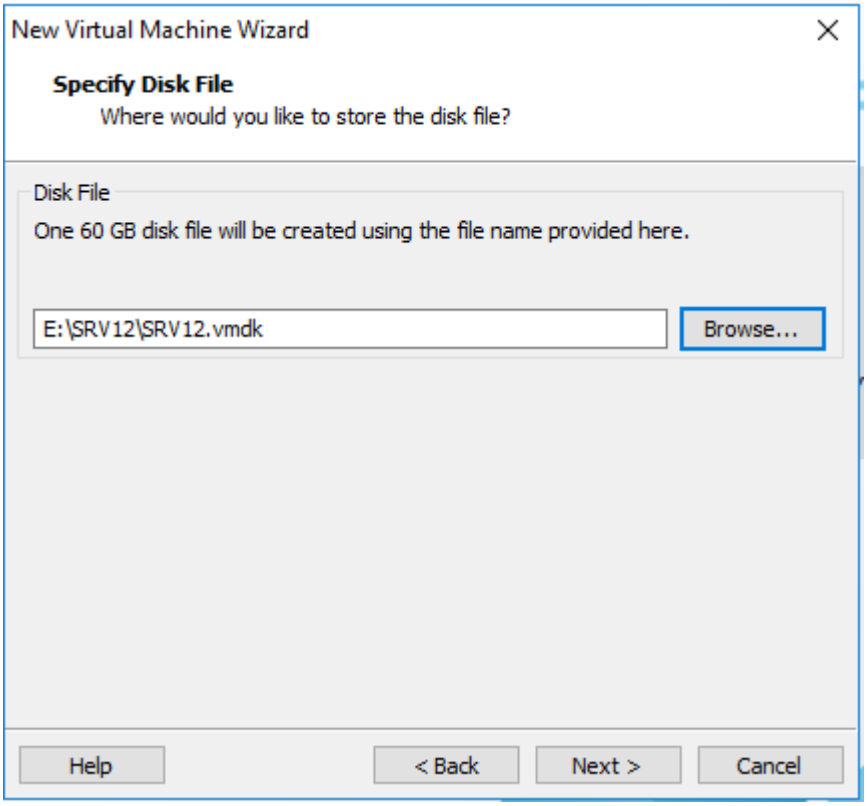
Tại cửa sổ ***Select a Disk***, chọn vào ***Create a new virtual disk*** để tạo ổ đĩa ảo.



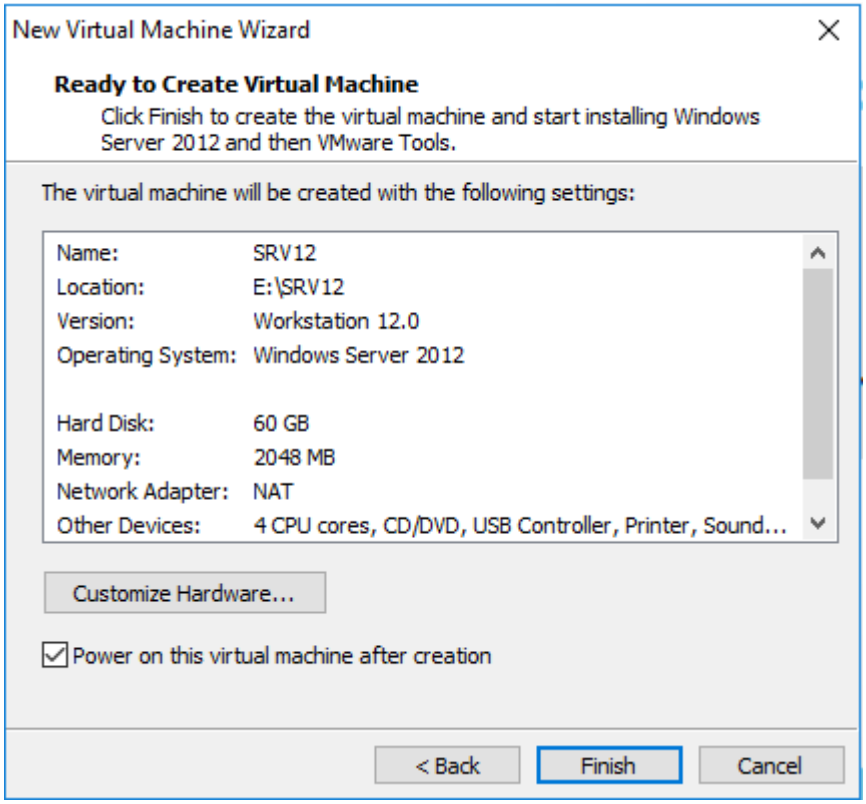
Tại ***Specify Disk Capacity***, điền vào dung lượng ổ đĩa cứng.



Tại cửa sổ ***Specify Disk File***, chọn ***Browse***… để chọn thư mục lưu file để mở máy ảo vừa tạo.



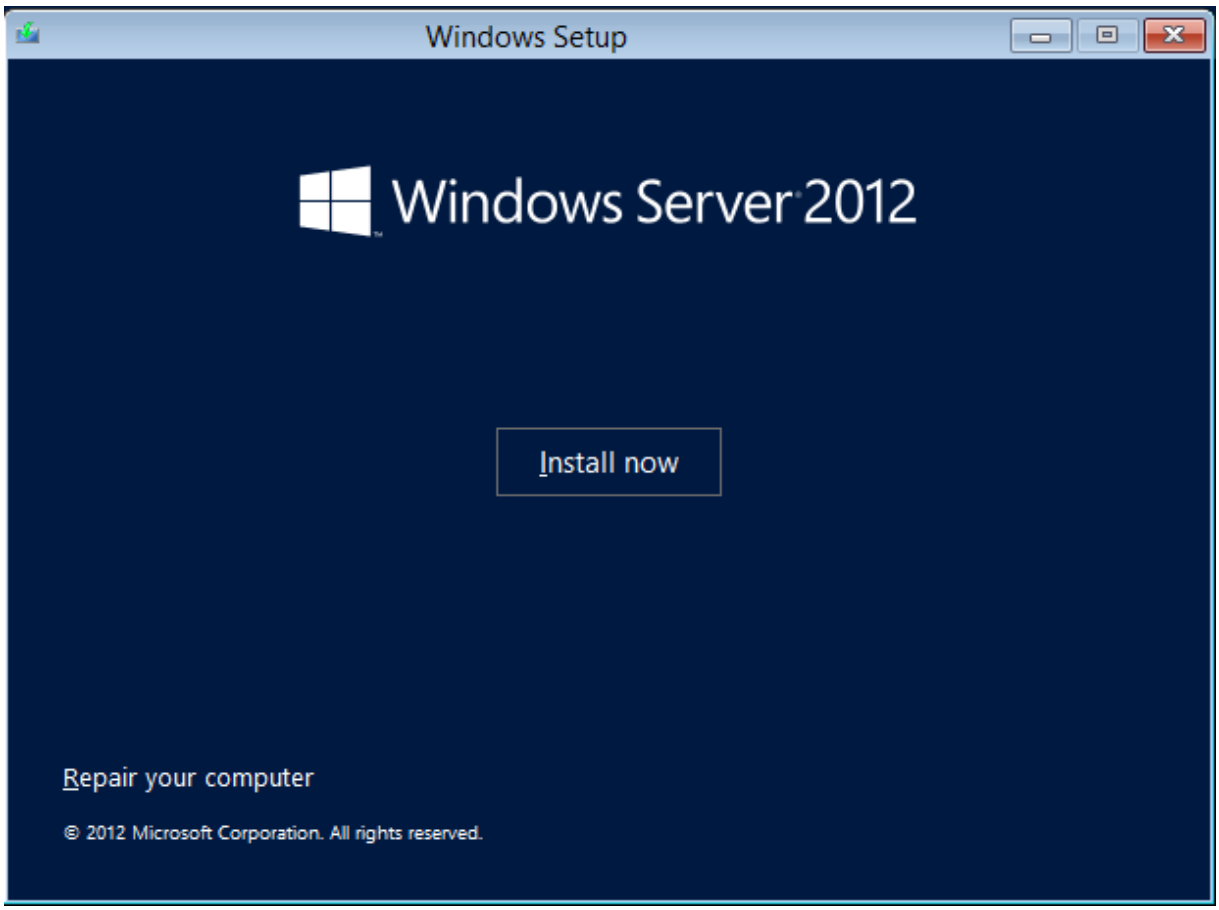
Tại cửa sổ ***Ready to Create Virtual Machine***, ấn ***Finish*** để kết thúc quá trình tạo máy ảo.



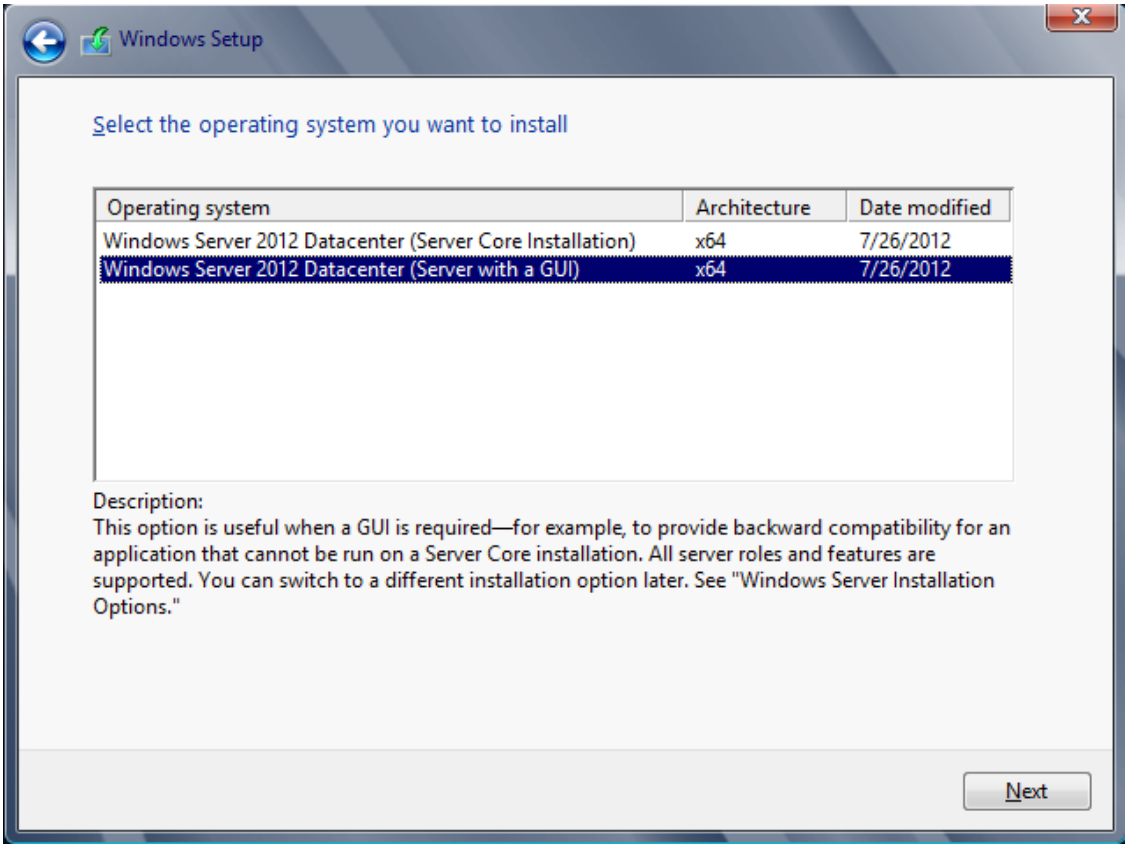
Quá trình load file diễn ra

Tại cửa sổ ***Windows Setup***, chọn các tùy chọn như hình bên dưới, ấn ***Next***

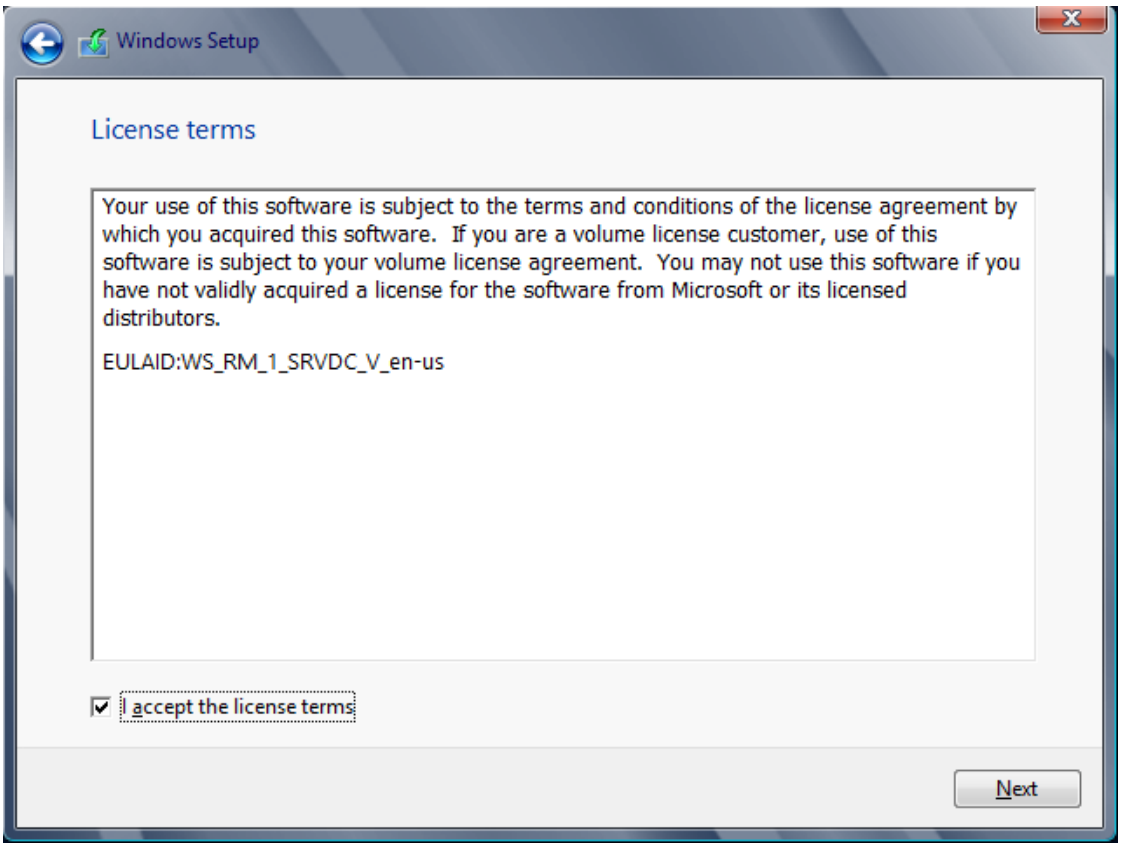
Ấn vào ***Install Now***.



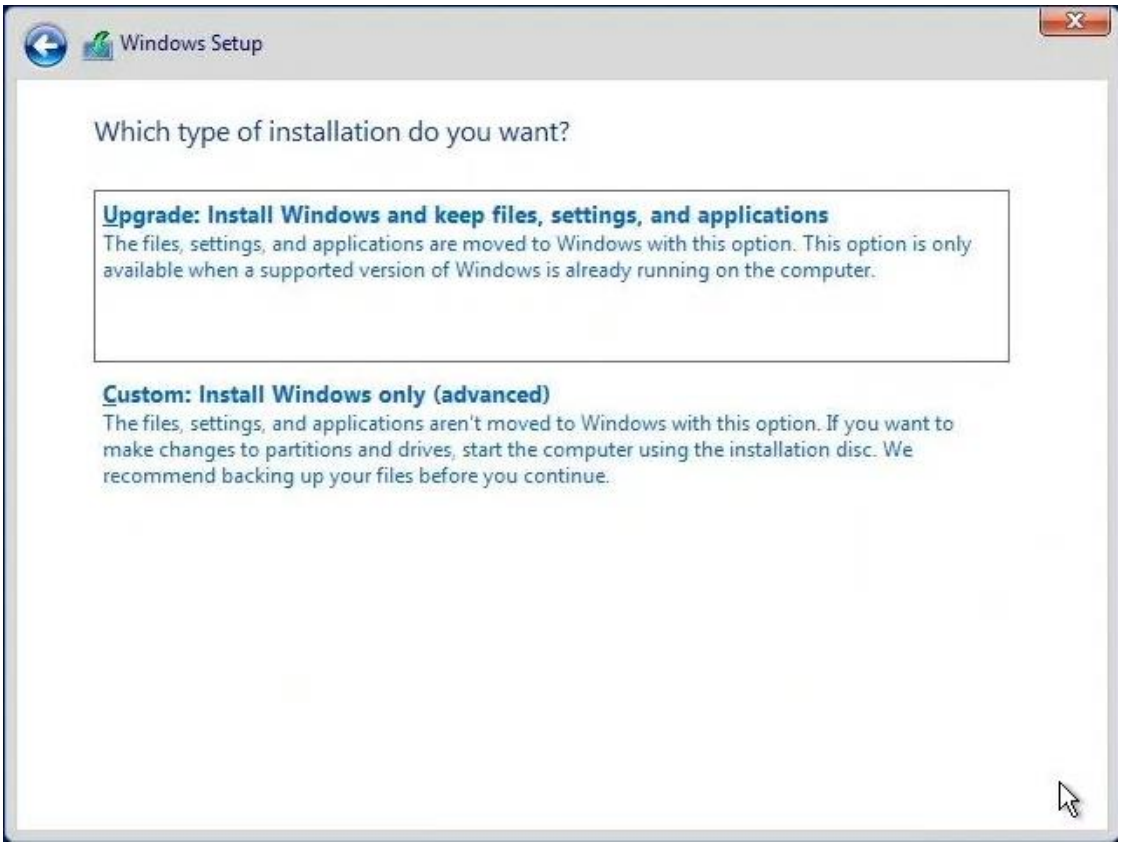
Tại cửa sổ ***Select the operating system you want to install***, chọn phiên bản ***Windows Server 2012 Datacenter Evaluation (Server with a GUI)***



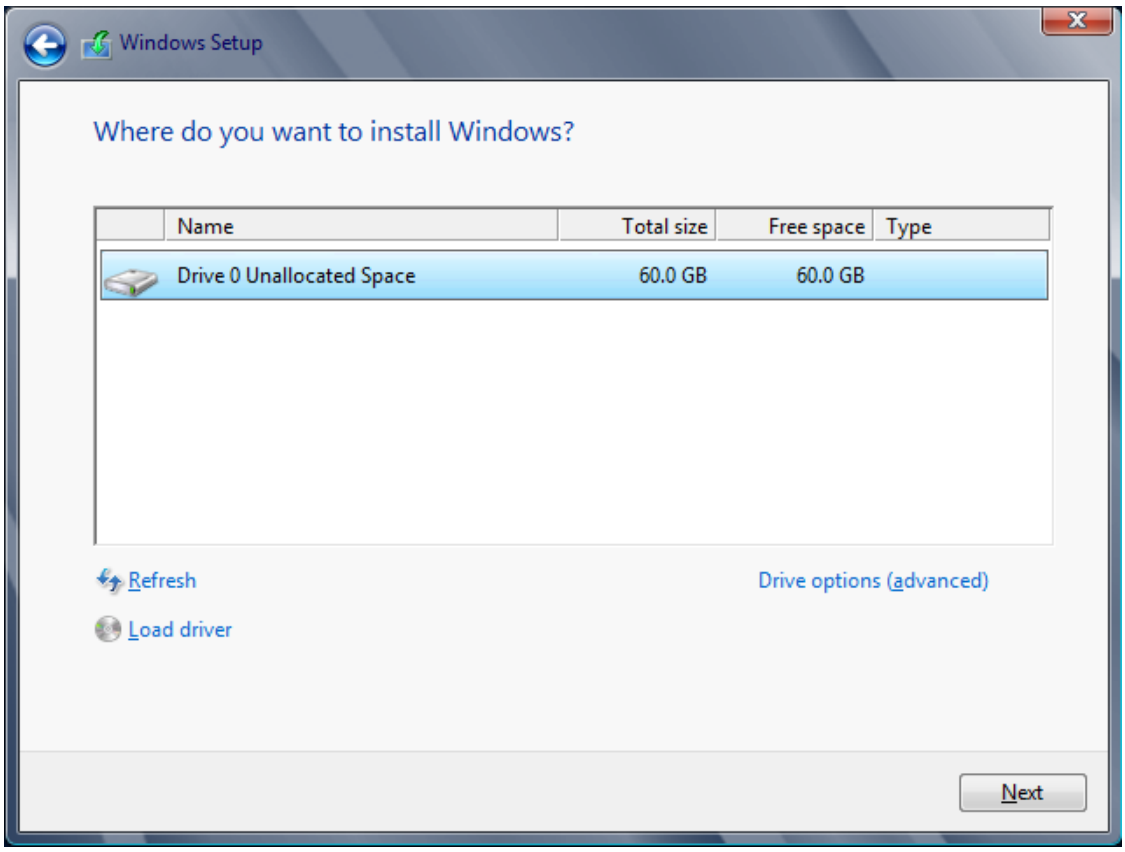
Tại cửa sổ ***License terms***, click chuột tại ***I accept the license terms***, và ấn ***Next.***



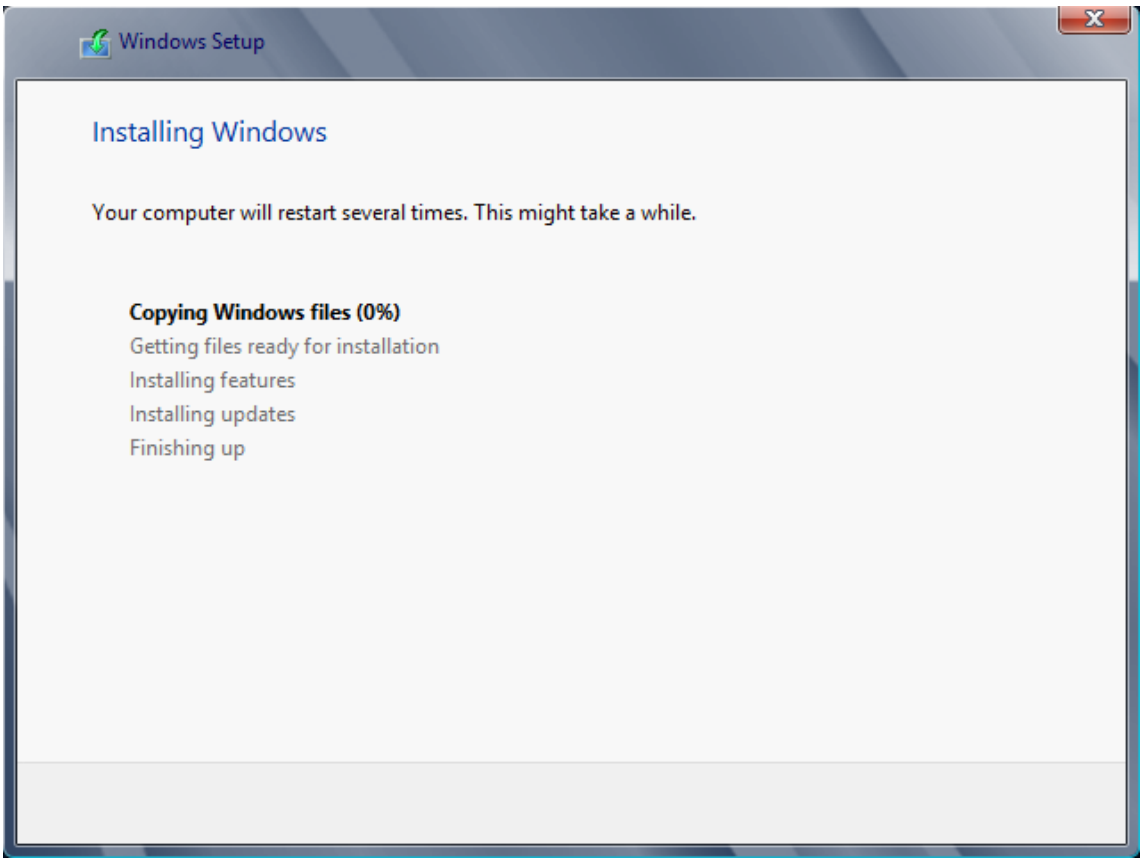
Tại cửa sổ ***Which type of installation do you want***, chọn ***Custom: Install Windows only (advanced)*** để cài đặt HĐH Windows Server 2012 mới.



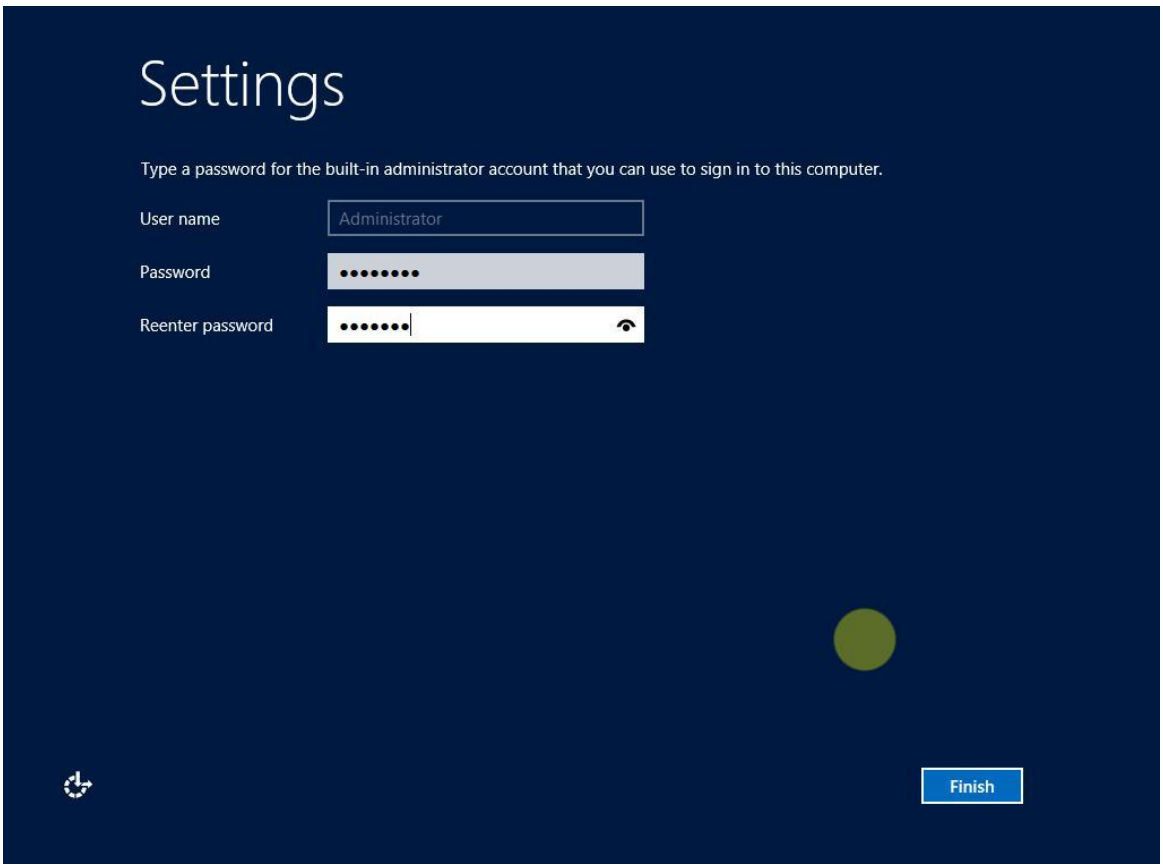
Tại cửa sổ ***Where do you want to install Windows***, chọn ổ đĩa cài đặt hệ điều hành, ấn ***Next.***



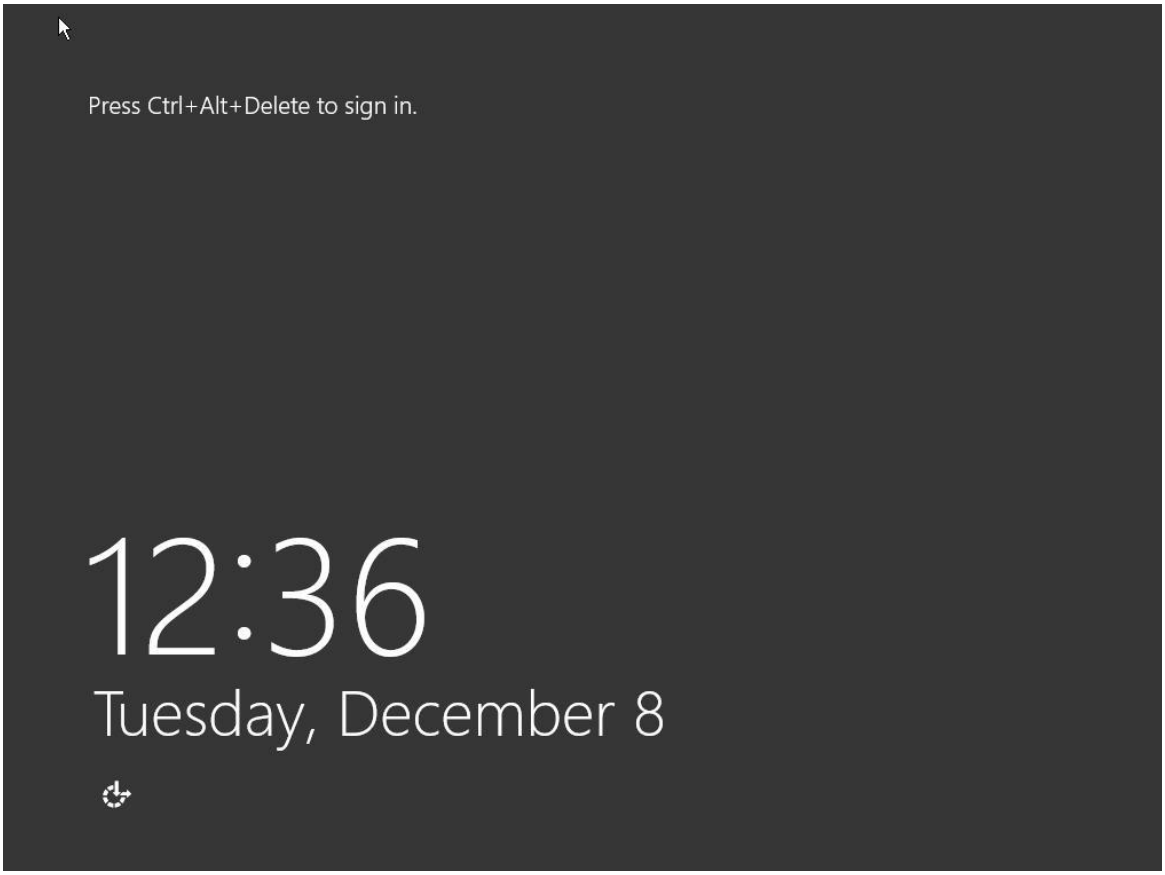
Quá trình cài đặt diễn ra.



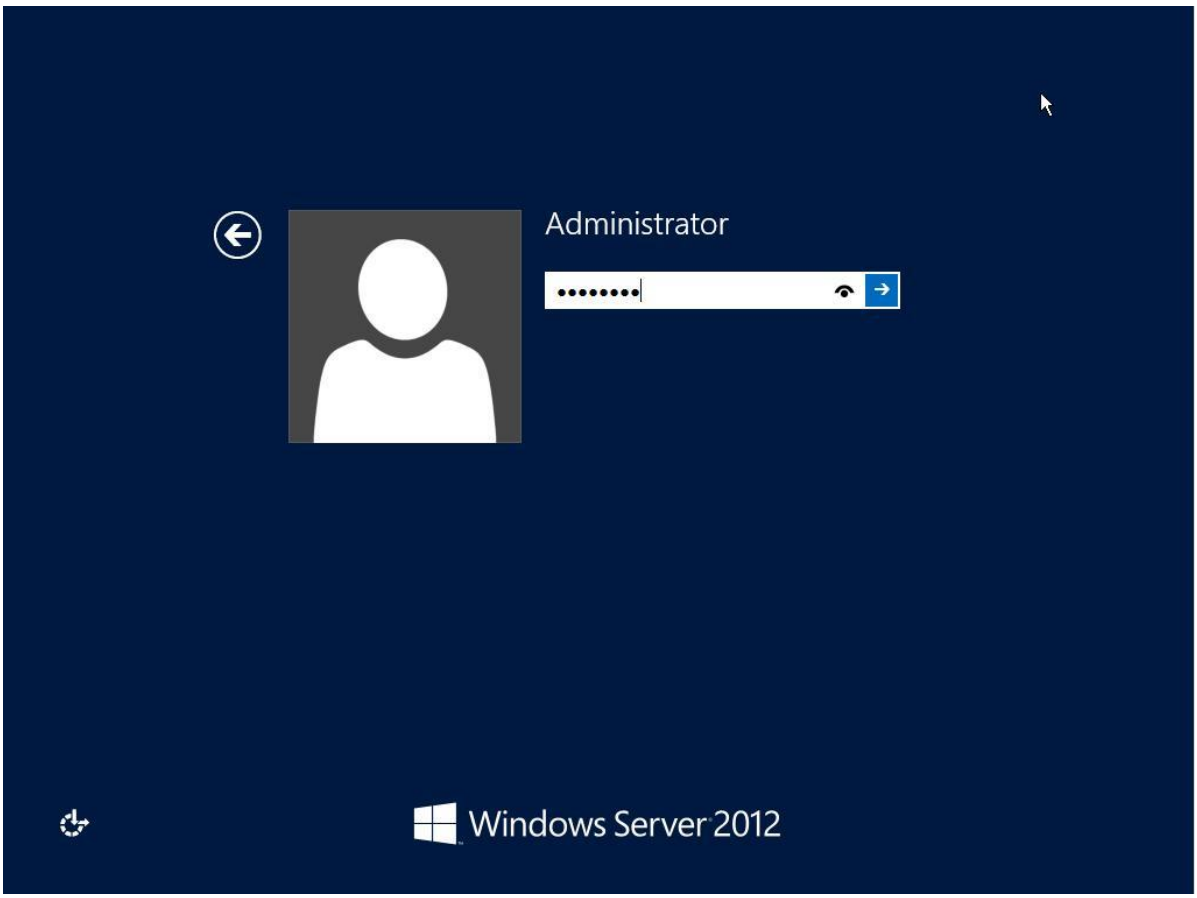
Sau khi kết thúc cài đặt, màn hình ***Settings*** hiện ra, điền ***Password*** cho ***User Administrator*** của máy. Sau đó click vào ***Finish*** để kết thúc



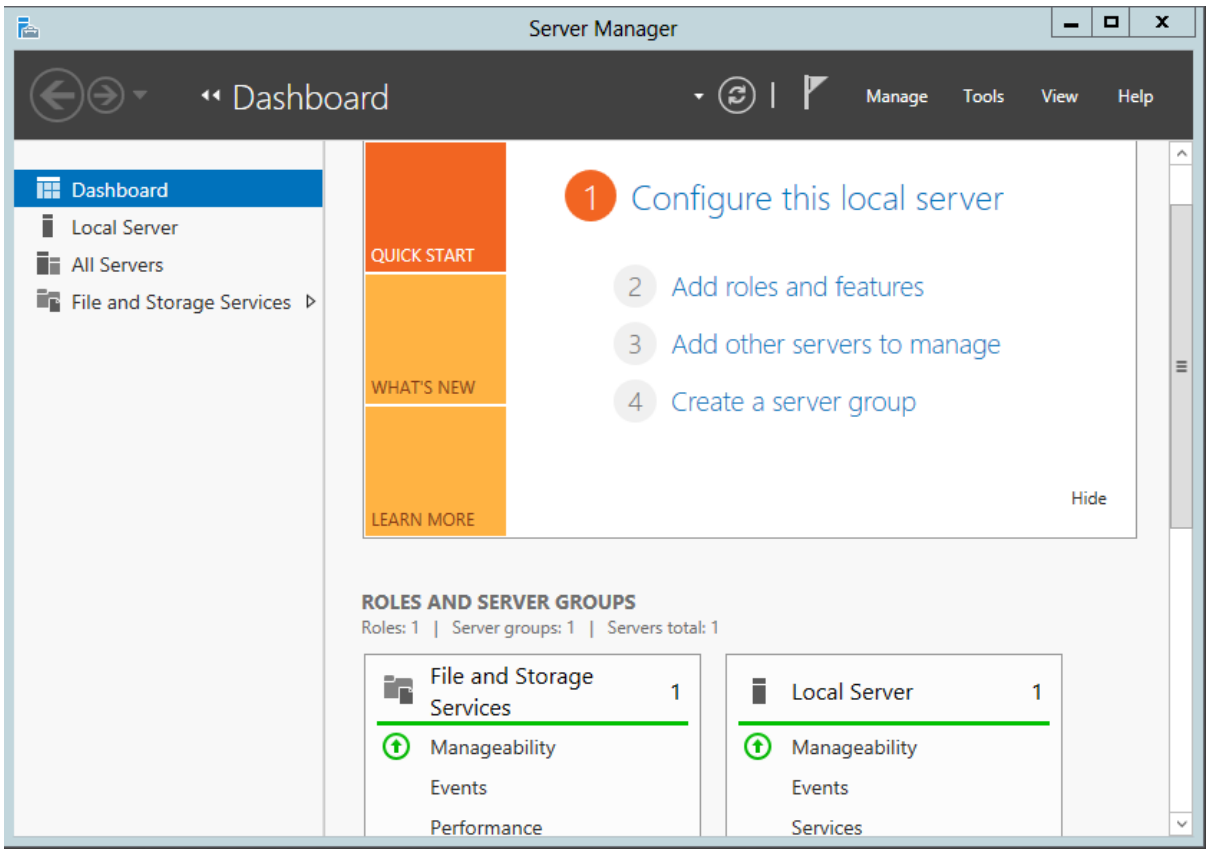
Tại đây, bấm tổ hợp phím "***Alt* + *Ctrl* + *Delete***" để Login.



Điền mật khẩu vừa tạo để đăng nhập

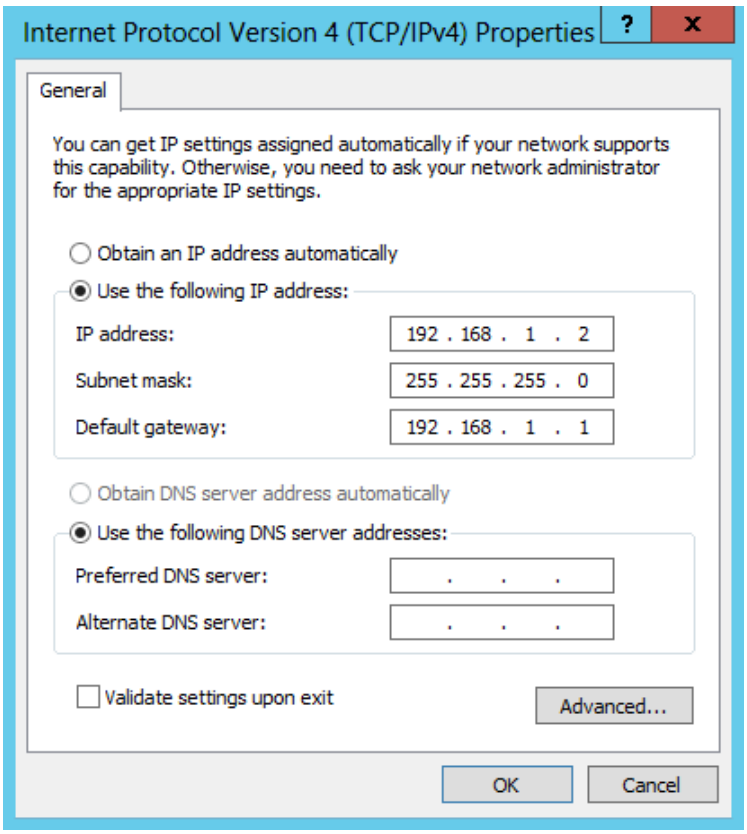


Sau khi đăng nhập thành công, mặc định màn hình ***Server Manager*** hiện ra

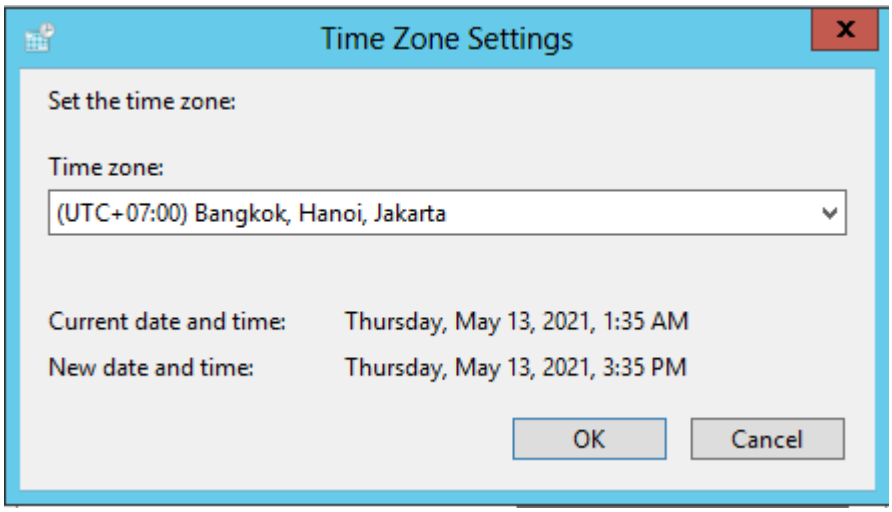


Bước 3: Cấu hình hệ điều hành Windows server 2012

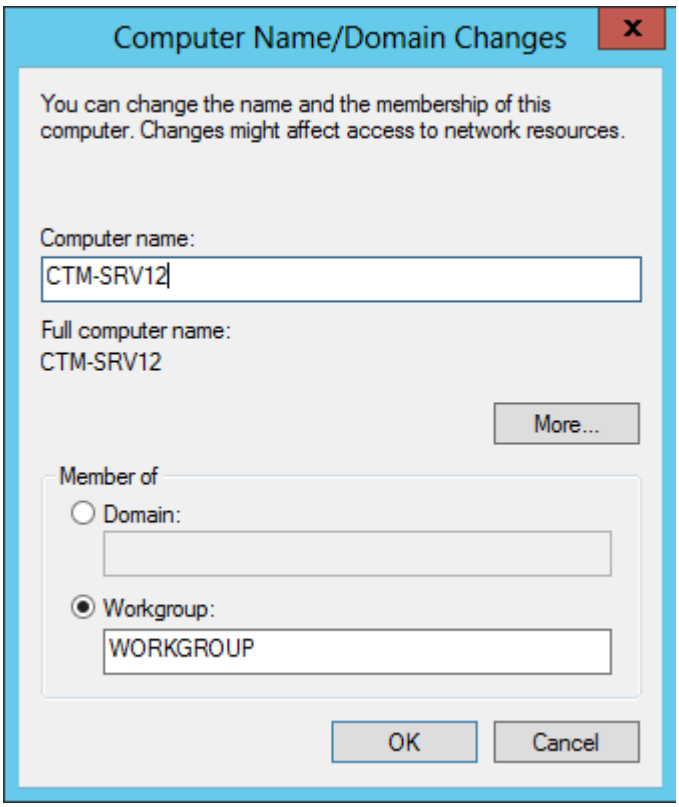
- Đặt địa chỉ *IP Address* cho máy Window Server 2012



- Thay đổi múi giờ (Time Zone) cho máy Window Server 2012



- Đặt lại tên cho máy Window Server 2012



4. Yêu cầu kết quả

Cài đặt thành công phần mềm máy ảo Vmware 12 Pro

Cài đặt thành công phần mềm hệ điều hành Windows Server 2012 Datacenter (GUI) trên phần mềm máy ảo Vmware 12 Pro

Cấu hình các thông số cơ bản trên phần mềm hệ điều hành Windows server 2012

III. Sai hỏng và cách khắc phục

1. Cài đặt phần mềm máy áo không thành công

- Nguyên nhân

- Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Nhập mã đăng ký phần mềm chưa đúng

- Cách khắc phục

- Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
- Nhập đúng mã đăng ký phần mềm

2. Cài đặt phần mềm hệ điều hành Windows Server 2012 không thành công

- Nguyên nhân

- Thực hiện các lựa chọn cài đặt trên phần mềm máy ảo chưa đúng theo hướng dẫn

- Cách khắc phục

- Thực hiện đúng các lựa chọn cài đặt theo hướng dẫn thực hành

V. Hướng dẫn ôn luyện

- Cài đặt phần mềm máy ảo Vmware 12 Pro
- Cài đặt phần mềm hệ điều hành Windows Server 2012 Datacenter (GUI) trên phần mềm máy ảo Vmware 12 Pro
- Cài đặt phần mềm hệ điều hành Windows 7 Pro trên phần mềm máy ảo Vmware 12 Pro

BÀI 2: CÀI ĐẶT VÀ CẤU HÌNH ACTIVE DIRECTORY

I. Lý thuyết liên quan

1. Dịch vụ Active Directory Domain Services

a) Giới thiệu Active Directory Domain Services (ADDS)

Dịch vụ Active Directory (AD) là một dịch vụ do hãng Microsoft nghiên cứu, xây dựng và phát triển. Active Directory (AD) là một sản phẩm, dịch vụ độc quyền của Microsoft. Đây là một dịch vụ không thể thiếu được trên tất cả các phiên bản Windows Server từ trước đến nay.

Đây là một dịch vụ thư mục quản lý các đối tượng trong hệ thống domain (vùng) theo dạng quản lý tâm trung. Active Directory là một hệ thống được chuẩn hóa với khả năng quản trị tập trung về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng.

Active Directory được sử dụng trong mô hình mạng "Server – Client". Từ khi hệ điều hành Windows Server 2000 được phát hành, Microsoft tích hợp một thành phần là Active Directory (AD). Khi máy chủ Windows sử dụng Windows 2000 Server, Windows Server 2003 hay Longhorn Server, công việc của Domain Controller (bộ điều khiển miền) là chạy dịch vụ Active Directory.

Active Directory chính là trái tim của Windows Server hay là một thành phần quan trọng trong hệ thống, tất cả mọi hoạt động diễn ra trên hệ thống đều chịu sự chi phối và điều khiển của dịch vụ Active Directory.

Từ phiên bản Windows NT4.0 trở về sau, Microsoft đã phát triển hệ thống Active Directory dùng để lưu trữ dữ liệu các Database của Domain như là lưu trữ các đối tượng bao gồm user, computer, group. gpo… cung cấp những dịch vụ (directory services) tìm kiếm, kiểm soát truy cập, ủy quyền, và đặc biệt là dịch vụ chứng thực được xây dựng dựa trên giao thức Keberos hỗ trợ cơ chế single sign-on (SSO) cho phép người dùng chỉ cần chứng thực một lần duy nhất khi đăng nhập vào hệ thống domain và có thể truy cập tất cả những tài nguyên và dịch vụ chia sẻ của hệ thống với những quyền hạn hợp lệ mà hệ thống không yêu cầu phải xác thực đăng nhập lại nhiều lần.

Với những dịch vụ Active Directory đã làm giảm nhẹ công việc quản lý và nâng cao hiệu quả hoạt động, những công việc mà hầu như không thể thực hiện được trên một hệ thống mạng ngang hàng, phân tán thì giờ đây có thể tiến hành một cách dễ dàng thông qua mô hình quản lý tập trung như đưa ra các chính sách chung cho toàn bộ hệ thống nhưng đồng thời có thể ủy quyền quản trị để phân chia khả năng quản lý trong một môi trường rộng lớn.

b) Tính năng bên trong dịch vụ Active Directory Domain Services :

Centralized Data Store – Lưu trữ dữ liệu tập trung

Toàn bộ dữ liệu, thông tin trong hệ thống được lưu trữ một cách tập trung, cho phép người dùng có thể truy cập dữ liệu từ bất cứ nơi đâu, bất cứ lúc nào đồng thời nâng cao hiệu năng quản trị của hệ thống, giảm thiểu độ rủi ro cho tài nguyên.

Scalability – Khả năng linh hoạt với nhu cầu

Active Directory cung ứng một cách linh hoạt các giải pháp quản trị khác nhau cho từng nhu cầu cụ thế trên nền tảng hạ tầng xác định của các doanh nghiệp.

Extensibility

Cơ sở dữ liệu của Active Directory cho phép nhà quản trị có thể customize và phát triển, ngoài ra còn có thể phát triển các ứng dụng sử dụng cơ sở dữ liệu này, giúp tận dụng hết khả năng, hiệu năng của Active Directory.

Manageability – Khả năng quản trị linh hoạt dễ dàng

Active Directory được tổ chức theo cơ chế của Directory Service dưới mô hình tổ chức Directory giúp các nhà quản trị có cái nhìn tổng quan nhất đối với cả hệ thống, đồng thời giúp user có thể dễ dàng truy xuất và sử dụng tài nguyên hệ thống.

Integration with Domain Name System (DNS):

DNS là một dịch vụ đi kèm rất cần thiết đối với Active Directory, trong một hệ thống mạng, các dịch vụ của Active Directory chỉ hoạt động được khi dịch vụ DNS được cài đặt. DNS có trách nhiệm dẫn đường, phân giải các Active Directory Domain Controller trong hệ thống mạng, và càng quan trọng hơn trong môi trường Multi Domain. DNS được dễ dàng tích hợp vào Active Directory để nâng cao độ bảo mật và khả năng đồng bộ hóa giữa các Domain Controller với nhau trong môi trường nhiều Domain.

Client Configuration Management:

Active Directory cung cấp khả năng quản trị các cấu hình phía client, giúp quản trị hệ thống dễ dàng hơn và nâng cao khả năng di động của user.

Policy – based administration:

Trong Active Directory, việc quản trị hệ thống mạng được đảm bảo một cách chắn chắc thông qua các chính sách quản trị tài nguyên, các quyền truy xuất trên các site, domain và các organization unit. Đây là một trong những tính năng quan trọng nhất được tích hợp vào Active Directory.

Replication of information:

Active Directory cung cấp khả năng đồng bộ dữ liệu thông tin giữa các domain, trên nền tảng, môi trường nhiều domain nhằm mục đích giảm thiểu đến mức tối đa rủi ro và nâng cao khả năng hoạt động của hệ thống mạng.

Flexible, secure authentication and authorization

Active Directory cung cấp nhiều cơ chế authentication như Kerberos, Secure Socket Layer và Transport Layer Security giúp cho việc bảo mật thông tin của user khi xác thực thông tin truy xuất tài nguyên.

Security integration

Active Directory được tích hợp mặc định trong các phiên bản Windows Server, do đó Active Directory làm việc rất dễ dàng và linh hoạt, truy xuất điều khiển trên hệ thống được định nghĩa trên từng đối tượng, từng thuộc tính của đối tượng. Không những thế, các chính sách bảo mật được áp dụng không phải đơn thuần trên local mà còn được áp dụng trên các site, domain hay OU xác định.

Directory – enable applications and infrastructure

Active Directory là một môi trường tuyệt hảo cho các nhà quản trị thiết lập các cấu hình và quản trị các ứng dụng trên hệ thống. Đồng thời Active Directory cung cấp một hướng mở cho các nhà phát triển ứng dụng (developer) xây dựng các ứng dụng trên nền tảng Active Directory thông qua Active Directory Service Interfaces.

Interoperability with other directory services

Active Directory được xây dựng trên giao thức directory service chuẩn gồm 2 giao thức là Lightweight Directory Access Protocol (LDAP) và Name Service Provider Interface (NSPI), do đó Active Directory có khả năng tương thích với các dịch vụ khác được xây dựng trên nền tảng directory service thông qua các giao thức này.

Vì LDAP là một giao thức directoy chuẩn, do đó có thể phát triển, tích hợp các sản phẩm ứng dụng trao đổi, chia sẻ thông tin với Active Directory thông qua giao thức LDAP.

Còn giao thức NSPI được hỗ trợ bởi Active Directory nằm mục đích đảm bảo và nâng cao khả năng tương thích với directoy của Exchange.

Signed and encrypted LDAP traffic

Mặc định là công cụ Active Directoy trong windows server sẽ tự động xác thực và mã hóa thông tin, dữ liệu truyền tải trên giao thức LDAP. Việc xác thực giao thức nhằm đảm bảo thông tin được gửi đến từ 1 nguồn chính thức và không bị giả mạo.

c) Cấu trúc bên trong dịch vụ Active Directory Domain Services :

Active Directory Objects:

Dữ liệu trong Active Directory như là thông tin tài khoản và các thuộc tính xoay quanh đối tượng như: users, printer, server, database, groups, computers và security policies được tổ chức như các objects (đối tượng).

Mỗi object có những thuộc tính riêng đặc trưng cho object đó, ví dụ như object user có các thuộc tính liên quan như First Name, Last Name, Logon Name, … và Computer Object có các thuộc tính như computer name cùng description.

Một số object đặc biệt bao gồm nhiều object khác bên trong được gọi là các "container", ví dụ như domain là một container bao gồm nhiều user và computer account.

Active Directory Schema:

Trong Active Directory, database lưu trữ chính là AD Schema, Schema định nghĩa các đối tượng được lưu trữ trong Active Directory. Nhưng Schema lưu trữ các đối tượng thế nào ? Thực chất, schema là một danh sách các định nghĩa xác định các loại đối tượng và các loại thông tin về đối tượng lưu trữ trong Active Directory. Về bản chất, schema cũng được lưu trữ như 1 object.

Schema được định nghĩa gồm 2 loại đối tượng (object) là: Schema Class objects và Schema Attribute objects.

Schema Class: Có chức năng như một template cho việc tạo mới các đối tượng trong AD. Mỗi Schema Class là một tập hợp các thuộc tính của đối tượng (Schema Attribute Objects). Khi tạo một đối tượng thuộc về một loại Schema Class thì Schema

Attribute sẽ lưu trữ các thuộc tính của đối tượng đó tương ứng với loại Schema Class của đối tượng.

Schema Attribute: Định nghĩa các Schema Class tương ứng với nó. Mỗi thuộc tính chỉ được định nghĩa một lần trong Active Directory và có thể thuộc nhiều Schema Class theo quan hệ một nhiều (1-m).

Mặc định thì một tập hợp các Schema Class và Schema Attribute được đóng gói sẵn chung với Active Directory. Tuy nhiên Schema của Active Directory mở ra một khả năng phát triển mở rộng Schema Class trên các Attribute có sẵn hay là tạo mới các Attribute Schema.

Tuy nhiên để có thể mở rộng phát triển với Schema AD cần chuẩn bị kỹ lưỡng thông qua các bản thiết kế rõ ràng và xem xét nhu cầu có cần thiết hay không, vì độ rủi ro trong việc này khá cao đối với các hệ thống đang hoạt động ổn định. Schema ảnh hưởng trực tiếp đến hệ thống.

Active Directory Components

Trong mô hình mạng doanh nghiệp, các components của Active Directory được sử dụng, áp dụng để xây dựng nên các mô hình phù hợp với nhu cầu các doanh nghiệp. Xét về khía cạnh mô hình kiến trúc của AD thì phân làm 2 loại là Physical và Logical.

Logical Structure (Kiến trúc luận lý)

Trong AD, việc tổ chức tài nguyên theo cơ chế Logical Structure, được ánh xạ thông qua mô hình domains, OUs, trees và forest. Nhóm các tài nguyên được tổ chức một cách luận lí cho phép dễ dàng truy xuất đến tài nguyên hơn là phải nhớ cụ thể vị trí vật lí của nó:

+ Domain: Cốt lõi của kiến trúc tổ chức luận lí trong AD chính là Domain, nơi lưu trữ hàng triệu đối tượng (objects). Tất cả các đối tượng trong hệ thống mạng trong một domain thì do chính domain đó lưu trữ thông tin của các đối tượng.
+ Active Directory được kiến tạo bởi một hay nhiều domain và một domain có thể triển khai trên nhiều physical structure. Việc access vào domain được quản trị thông qua Access Control Lists (ACLs), quyền truy xuất trên domain tương ứng với từng đối tượng.
+ OUs: OU là một container được dùng để tổ chức các đối tượng trong một domain thành các nhóm quản trị luận lí (logical). OUs cung cấp phương tiện thực hiện các tác vụ quản trị trong hệ thống như là quản trị user và resources, đó là những scope đối tượng nhỏ nhất mà có thể ủy quyền xác thực quản trị. OUs bao gồm nhiều đối tượng khác như là user accounts, groups, computers và các OUs khác tạo nên các cây OUs trong cùng một domain. Các cây OUs trong một domain độc lập với kiến trúc các cây OUs thuộc các domain khác.
+ Trees: Trees là một nhóm các domain được tổ chức theo cấu trúc hình cây với mô hình parent-child ánh xạ từ thực tế tổ chức của doanh nghiệp, tổ chức. Một domain có 1 hoặc nhiều child domain nhưng 1 child domain chỉ có 1 parent-domain. Ví dụ: Trong domain framgia.com, có các domain thấp hơn là abc.framgia.com và xyz.framgia.com thì được hiểu là Tree.
+ Forests: Forest là một thuật ngữ được đặt ra nhằm định nghĩa 1 mô hình tổ chức của AD, 1 forest gồm nhiều domain trees có quan hệ với nhau, các domain trees

trong forest là độc lập với nhau về tổ chức, nghe ra có vẻ mâu thuẫn trong mối quan hệ nhưng sẽ dễ hiểu hơn khi mối quan hệ giữa các domain trees là quan hệ Trust 2 chiều như các partners với nhau. Một forest phải đảm bảo thoả các đặc tính sau:

- Toàn bộ domain trong forest phải có 1 schema chia sẻ chung.
- Các domain trong forest phải có 1 global catalog (GC) chia sẻ chung.
- Các domain trong forest phải có mối quan hệ trust 2 chiều với nhau.
- Các tree trong 1 forest phải có cấu trúc tên (domain name) khác nhau.
- Các domain trong forest hoạt động độc lập với nhau, tuy nhiên hoạt động của forest là hoạt động của toàn bộ hệ thống.

Physical Structure: (Kiến trúc vật lý)

Xét về khía cạnh physical component của AD sẽ gồm 2 phần là Sites và Domain Controllers. Tùy thuộc vào mô hình tổ chức của công ty, người quản trị sẽ phải dùng các components này để thiết kế sao cho phù hợp.

Sites:

Site là một thuật ngữ được dùng đến khi nói về vị trí địa lý của các domain trong hệ thống. Khi hệ thống các domain được phân tán ở những vị trí địa lý, những nơi khác nhau và có quan hệ với nhau thì những nơi đặt các domain này chính là các Site

Domain Controllers

Domain Controller (DC) là 1 máy tính hay server chuyên dụng, máy ảo được triển khai cài đặt Windows Server và lưu trữ bản sao của Domain Directory (local domain database).

Một domain có thể có 1 hay nhiều domain controller, mỗi domain controller đều có bản sao dữ liệu của Domain Directory. Domain Controller chịu trách nhiệm chứng thực cho users và chịu trách nhiệm đảm bảo các chính sách bảo mật được thực thi. Các chức năng chính của Domain Controller:

+ Mỗi Domain Controller lưu trữ các bản sao thông tin của Active Directory cho chính domain đó, chịu trách nhiệm quản lí thông tin và tiến hành đồng bộ dữ liệu với các domain controller khác trong cùng một domain.
+ Domain Controller trong một domain có khả năng tự động đồng bộ dữ liệu với các DC khác trong cùng một domain. Khi thực hiện một tác vụ đối với thông tin lưu trữ trên DC, thì thông tin này sẽ tự động được đồng bộ hóa đến các DC khác. Tuy nhiên để đảm bảo sự ổn định cho hệ thống mạng cần phải có một chính sách hợp lí cho các domain trong việc đồng bộ hóa thông tin dữ liệu với một thời điểm phù hợp.
+ Mặc định để tránh các xunh động và tối ưu Database trong AD thì khi có thay đổi cập nhật trong hệ thống thì DC nào gữa 5 master roles sẽ được cập nhật trước sau đó đồng bộ các thay đổi này về các DC khác trong hệ thống mạng. Các DC trong hệ thống thường xuyên trao đổi với nhau để kiểm tra lẫn nhau về

sự thay đổ các Database. Có thể lập lịch đồng bộ này nhằm giảm thiểu băng trong trong hệ thống.

+ Domain Controller tự động đồng bộ hóa ngay lập tức các thay đổi quan trọng đối với cả domain như disable một user account.
+ Active Directory sử dụng việc đồng bộ hóa dữ liệu theo cơ chế multimaster, nghĩa là không có domain controller nào đóng vai trò là master cả, mà thay vào đó thì tất cả domain controller đều ngang hàng với nhau, mỗi domain controller lưu trữ một bản sao của database hệ thống. Các domain controller lưu trữ các thông tin dữ liệu khác nhau trong một khoảng thời gian ngắn cho đến khi thông tin các domain controller trong hệ thống đều được đồng bộ với nhau, hay nói cách khác là thống nhất dữ liệu cho toàn domain.
+ Mặc dù là Active Directory hỗ trợ hoàn toàn việc đồng bộ dữ liệu theo cơ chế multimaster nhưng thực tế thì không phải lúc nào cũng theo cơ chế này (việc thực thi không được cho phép ở nhiều nơi trong hệ thống mạng trong cùng một thời điểm).
+ Operations Master Roles (FSMO) là các roles đặc biệt được Assigned với 1 hoặc nhiều domain controllers khác để thực hiện đồng bộ theo cơ chế single-master, có thể dễ dàng nhận thấy việc thực thi operations của multimaster là sự thực thi của nhiều single-master đồng thời.
+ Hệ thống có nhiều hơn một domain hỗ trợ trong trường hợp dự phòng backup domain controller, khi một domain controller có vấn đề xảy ra thì các domain sẽ tự động chạy dự phòng, đảm bảo hệ thống luôn được ổn định.
+ Domain Controller quản lí các vấn đề trong việc tương tác với domain của users, ví dụ xác định đối tượng trong Active Directory hay xác thực việc logon của user.

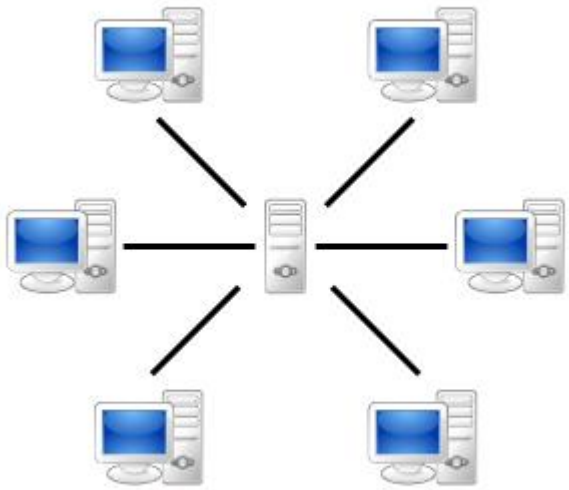
2. Mô hình mạng Domain

Một nhóm máy tính mạng cùng chia sẻ cơ sở dữ liệu thư mục tập trung được gọi là mô hình Domain. Thư mục dữ liệu chứa tài khoản người dùng và thông tin bảo mật cho toàn bộ Domain.

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

Trong một Domain, thư mục chỉ tồn tại trên các máy tính được cấu hình như máy điều khiển miền. Việc bảo mật hay quản trị trong Domain được tập trung hóa. Một domain không được xem như một vị trí đơn hoặc cấu hình mạng riêng biệt. Các máy tính trong cùng domain có thể ở trên một mạng LAN hoặc WAN. Chúng có thể giao tiếp với nhau qua bất kỳ kết nối vật lý nào.

Khác với Workgroup nếu người dùng có bất cứ thay đổi nào thì sự thay đổi đó sẽ được cập nhật tự động hóa trên toàn bộ Domain. Tuy nhiên một nhược điểm của Domain cần được nhắc tới đó chính là việc Domain phải tồn tại trước khi người dùng tham gia vào nó. Muốn tham gia Domain cần có tài khoản người dùng được người quản trị Domain cung cấp cho máy tính người dùng tới Domain đó.



Hình 2.2.1 - Mô hình mạng Domain

Mô hình Domain có các đặc điểm cơ bản sau:

- Hoạt động theo cơ chế client server
- Có ít nhất một máy tính làm chức năng điều khiển vùng (Domain Controller), máy tính này sẽ điều khiển toàn bộ hoạt động của hệ thống mạng.
- Thông tin người dùng được tập trung lại do dịch vụ Active Directory quản lý và được lưu trữ trên Domain Controller
- Quá trình xác thực đăng nhập diễn ra trên máy DC

Ưu điểm của mô hình Domain:

- Sử dụng cho mạng các tổ chức, công ty có số lượng máy tính lớn và nhu cầu dịch vụ cao
- Yêu cầu tính toàn vẹn dữ liệu và bảo mật mạng cao
- Quản lý tập trung cho toàn mạng
- Dễ dàng tích hợp những công nghệ mới
- Tận dụng sức mạnh của hệ thống máy chủ nhằm phục vụ tài nguyên cho mạng

Nhược điểm của mô hình Domain

- Kinh phí dùng để nối mạng lớn
- Sự mở rộng của mạng tuỳ thuộc hoàn toàn vào thiết bị trung tâm
- Đòi hỏi phải có nhân viên chuyên về quản trị mạng

II. Trình tự thực hiện

1. Yêu cầu thực hiện

- Nâng cấp máy chủ chạy HĐH Windows Server 2012 lên Domain Controller để quản lý miền *ctm.edu.vn.*
- Cho phép các máy trạm gia nhập vào miền *ctm.edu.vn*.

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

Sơ đồ địa chỉ IP như sau:

Thông số	*CTM-SRV12*	*CTM-WRK07*
IP Address	192.168.1.2	192.168.1.10
Subnet mask	255.255.255.0	255.255.255.0
Default gateway	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2

3. Các bước thực hiện

Thực hiện cài đặt và cấu hình Active Directory trên Windows Server 2012 thông qua 3 bước sau:

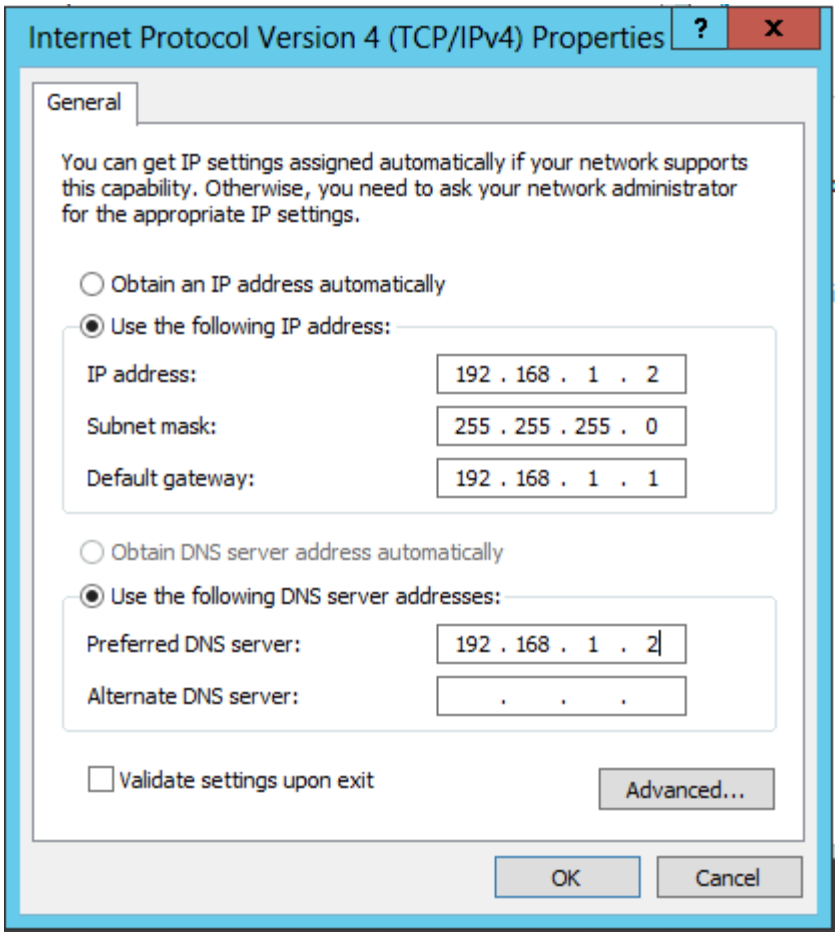
- Bước 1: Nâng cấp lên Domain Controller
- Bước 2: Cấu hình dịch vụ Active Directory Domain Services
- Bước 3: Kết nối máy trạm vào domain

Hướng dẫn chi tiết

Bước 1: Nâng cấp lên Domain Controller

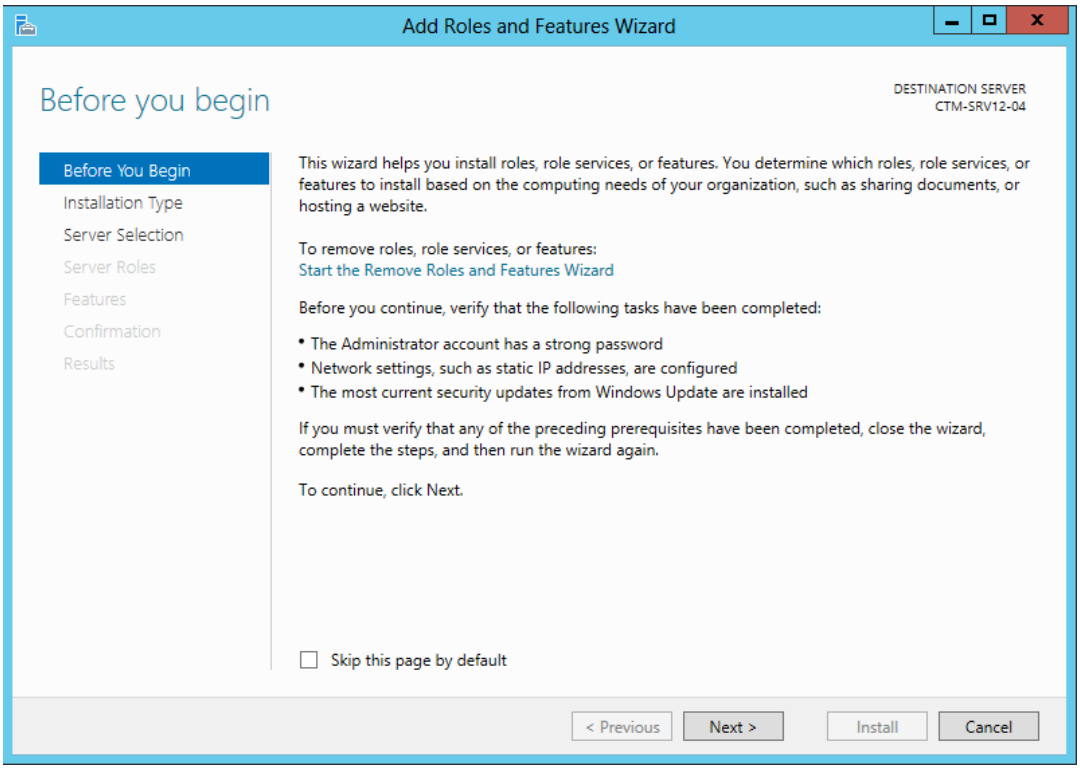
Thực hiện trên máy CTM-SVR12, nâng cấp lên Domain Controller.

Cấu hình đặt địa chỉ IP cho các máy tương ứng với sơ đồ địa chỉ IP

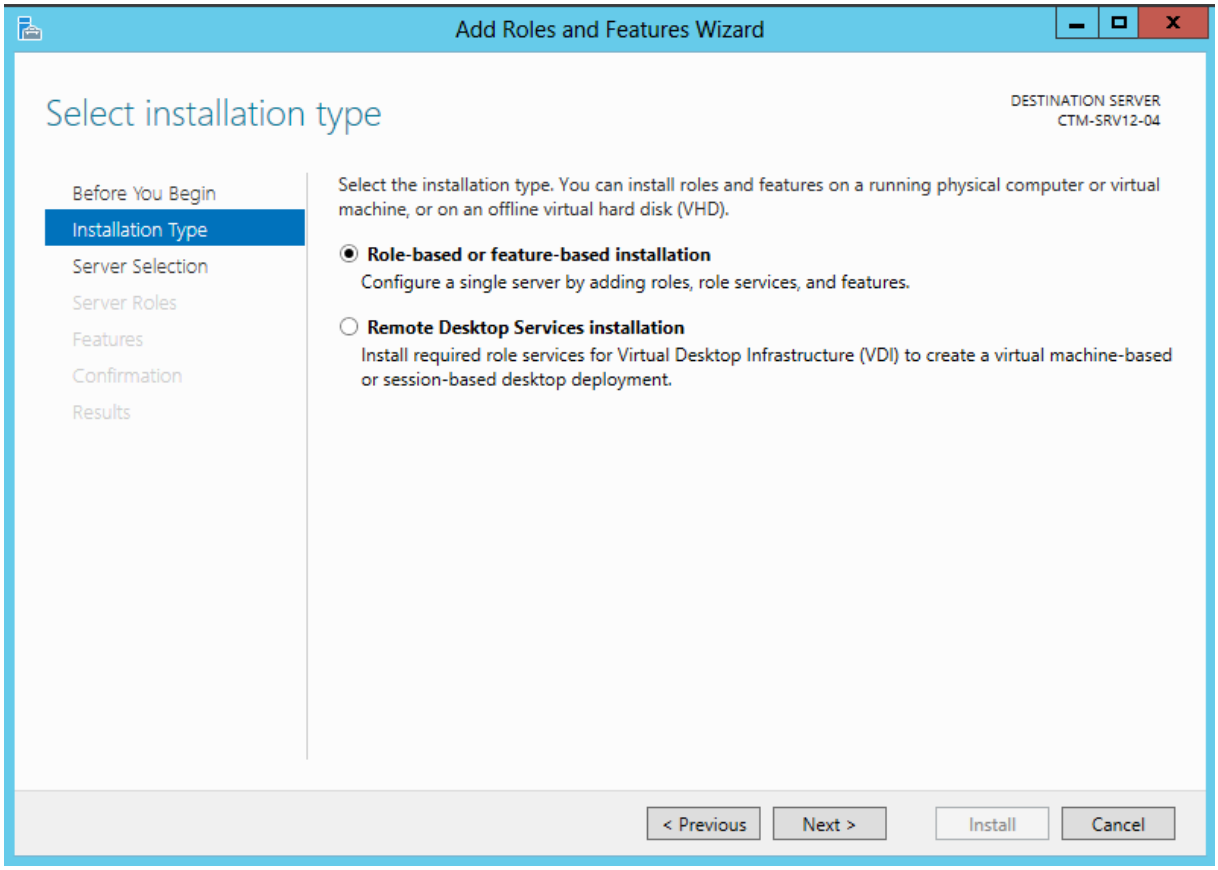


Thực hiện cài đặt dịch vụ ***Active Directory Domain Services*** trên máy CTM-SVR12:

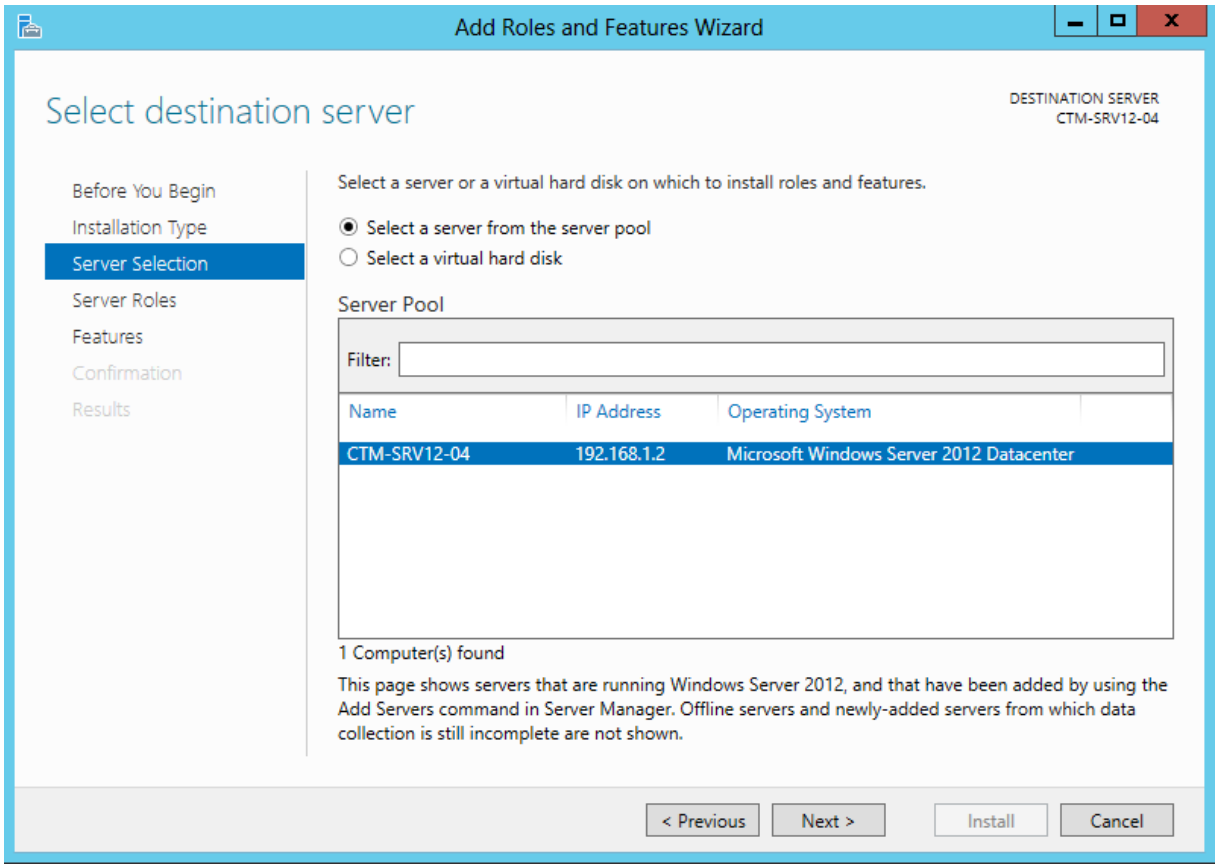
Click ***Server Manager / Add Roles and Features*** . Tại cửa sổ ***Add Roles and Features Wizard***, Click vào ***Next***.



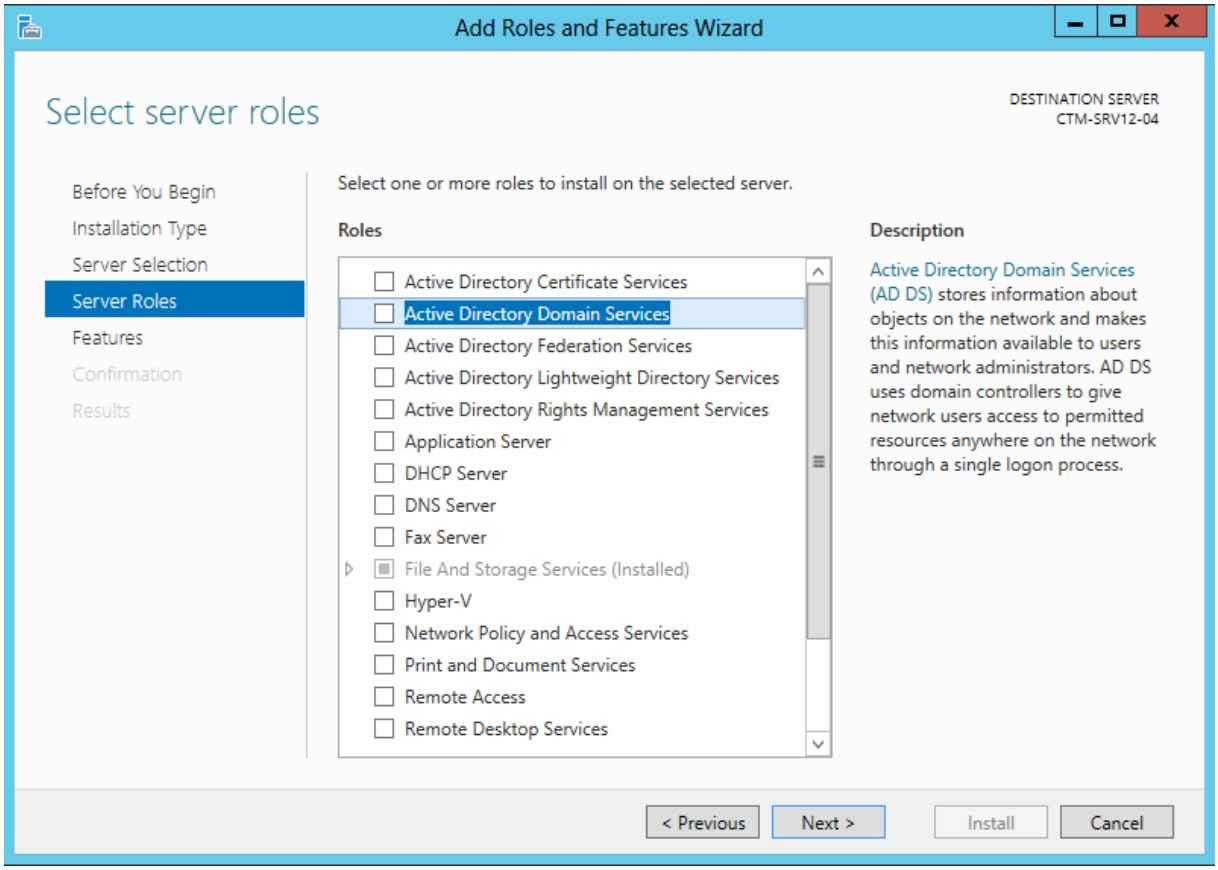
Tại Select ***installation type***, click vào ***Next***



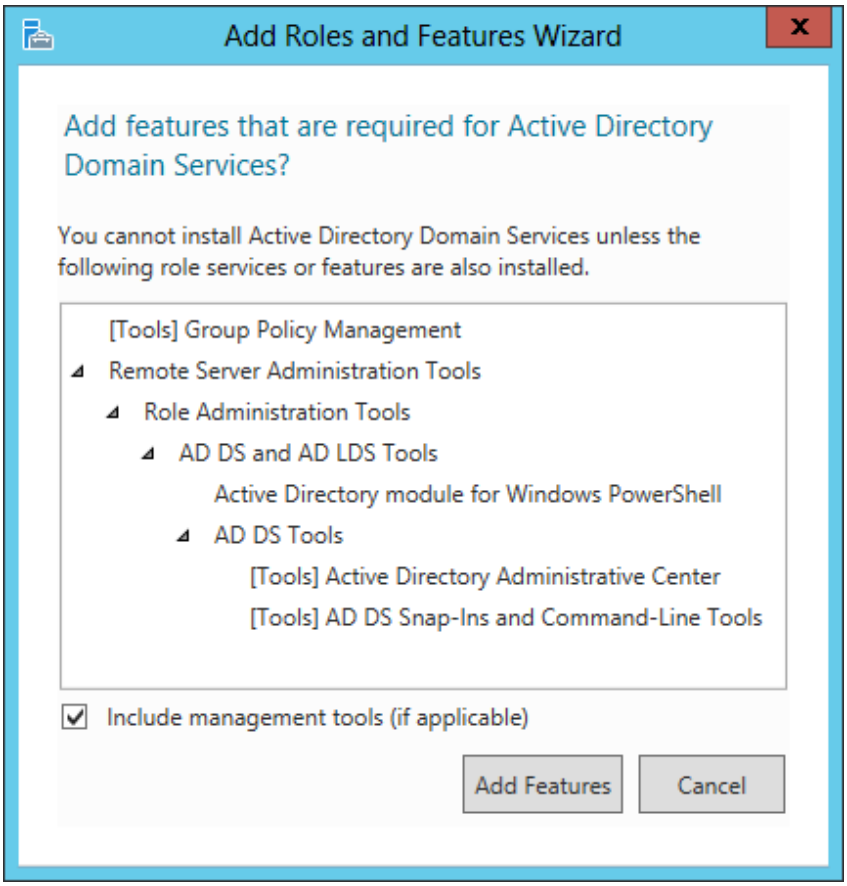
Tại ***Select destination server***, Click vào ***Next.***



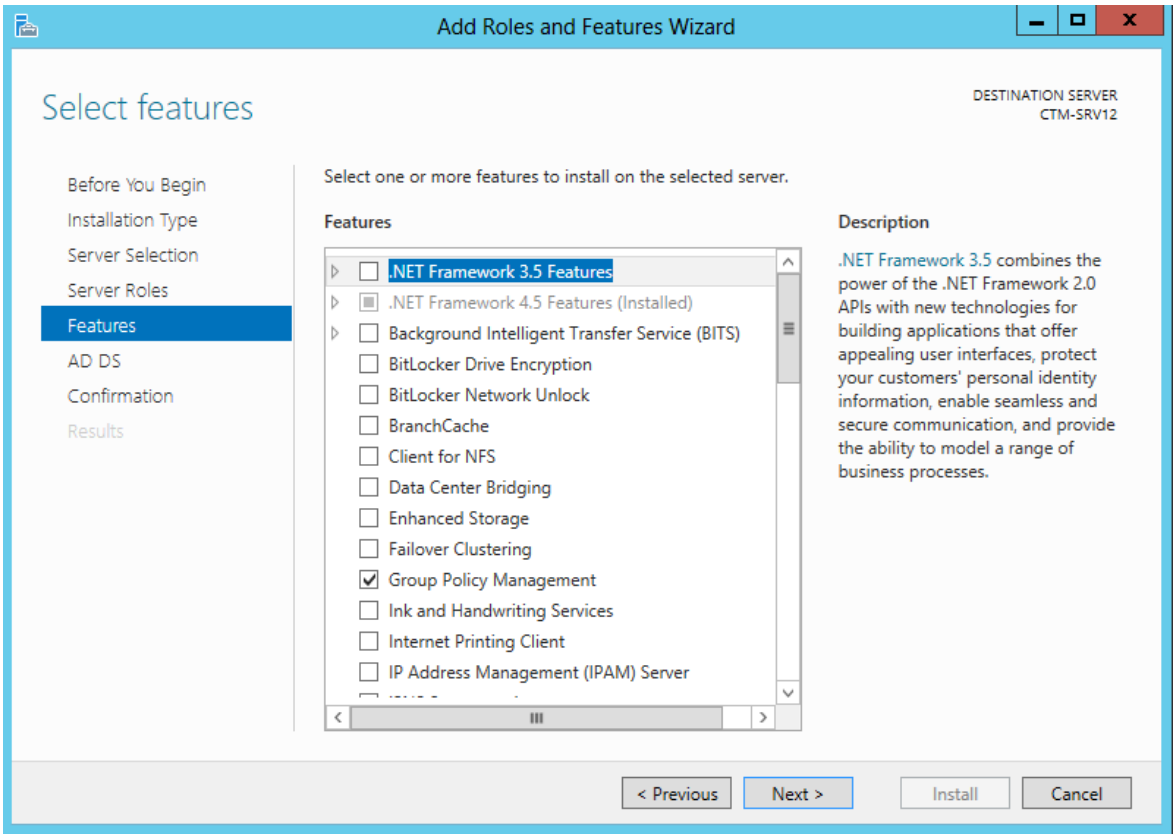
Tại ***Select server roles***, click chọn vào dịch vụ ***Active Directory Domain Services***.



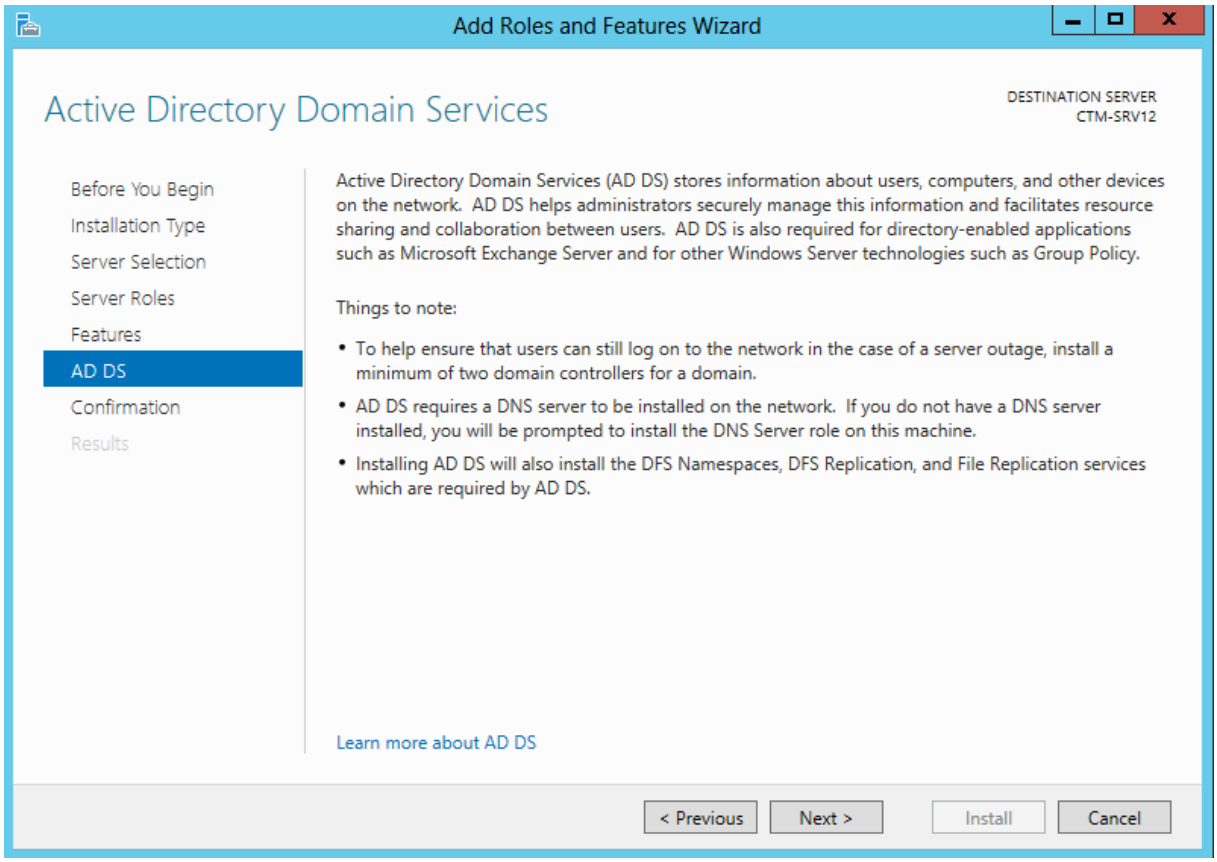
Cửa sổ ***Add Roles and Features Wizard*** hiện ra, chọn ***Add Features***.



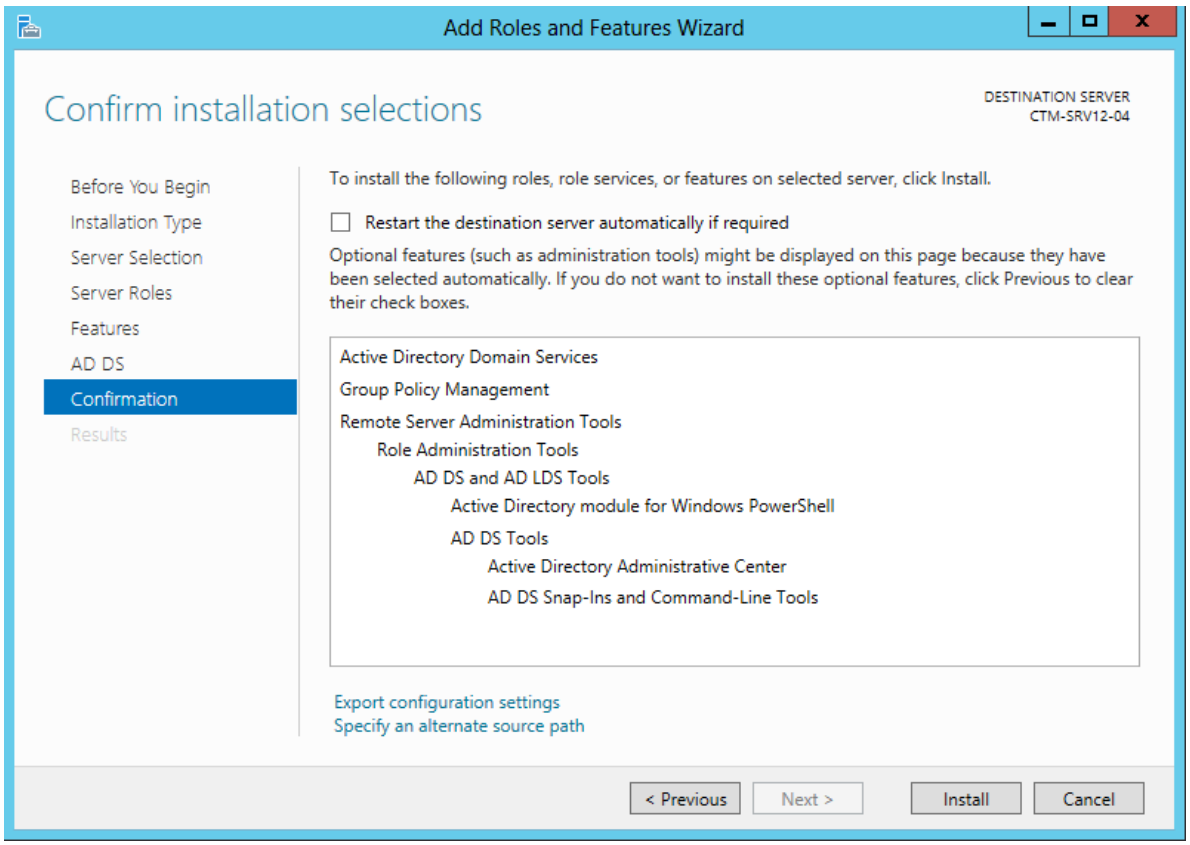
Tiếp tục ấn ***Next***, tại cửa sổ ***Select features***



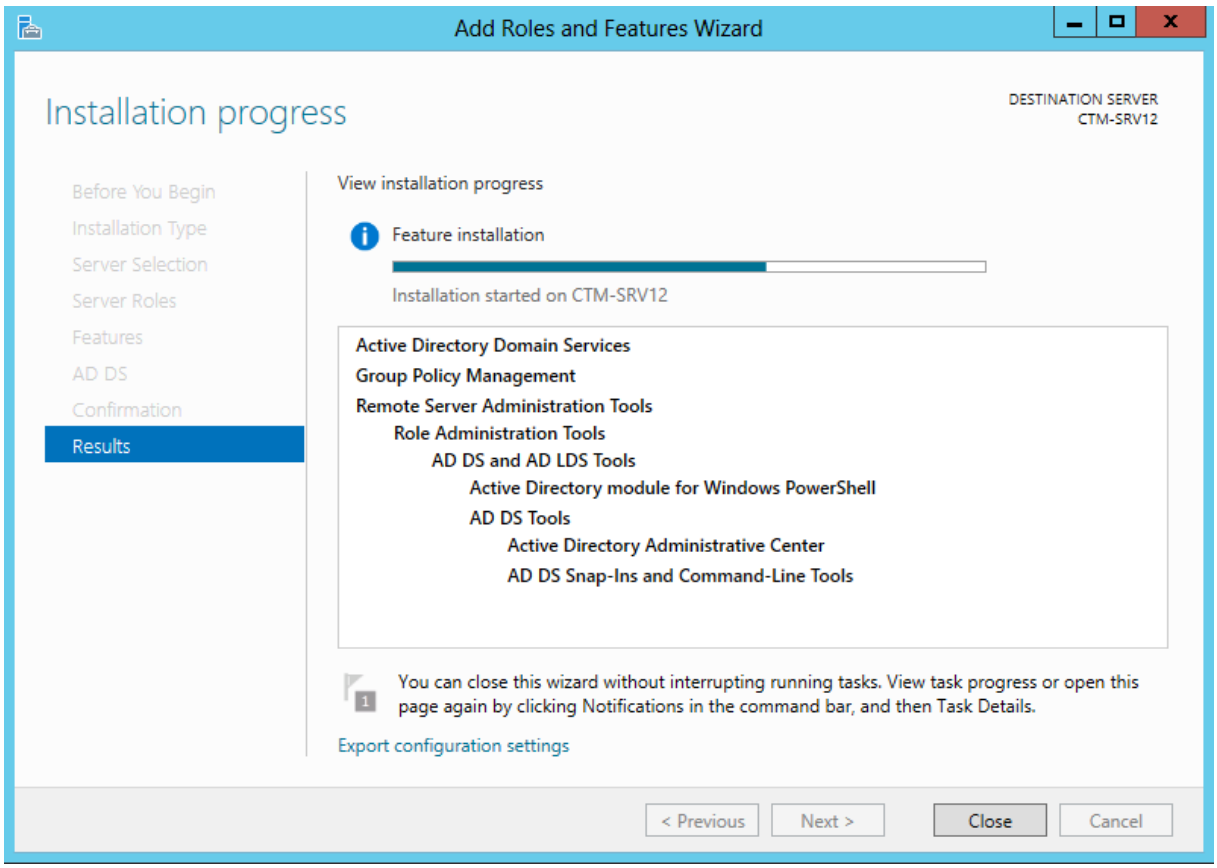
Tiếp tục ấn ***Next***



Tại cửa sổ ***Confirm installation selections***, click vào ***Install*** để cài đặt dịch vụ ***ADDS***

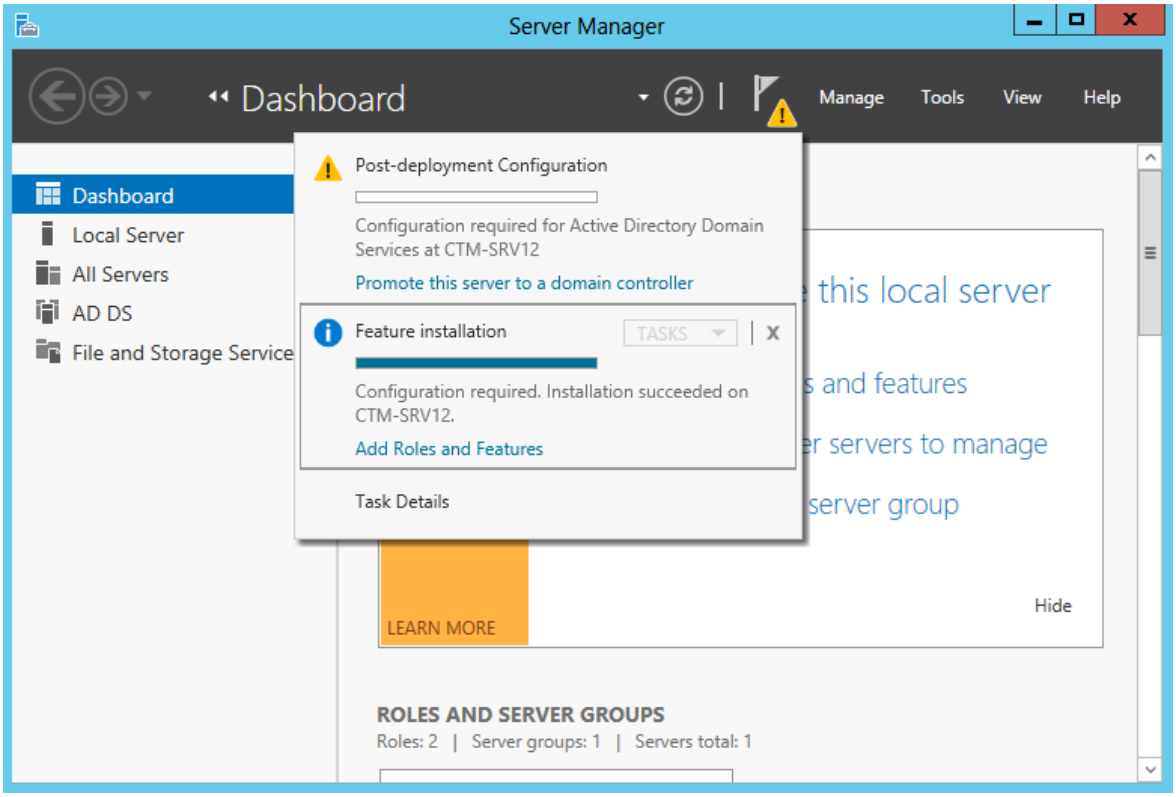


Sau khi chờ đợi 1 khoảng thời gian để dịch vụ ***Active Directory Domain Services*** được cài đặt xong. Click nút Close để hoàn thành việc cài đặt



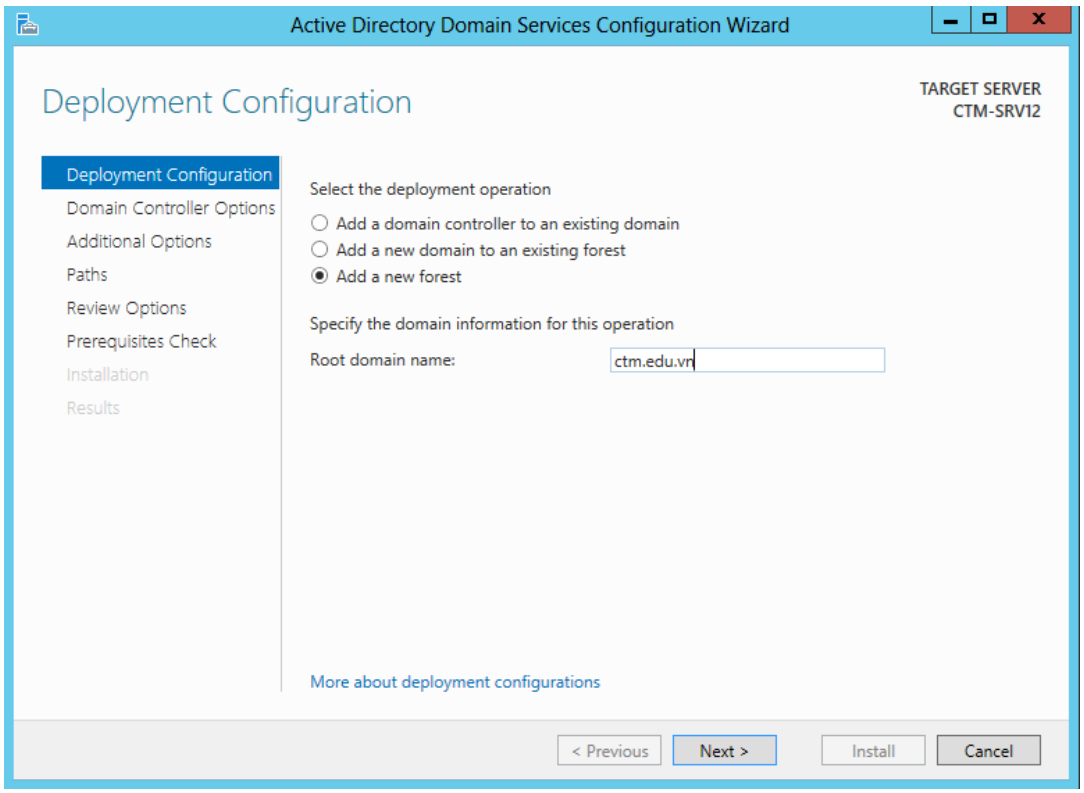
Bước 2: Cấu hình dịch vụ Active Directory Domain Services

Mở ***Notification*** của ***Server Manager***, click vào dòng chữ ***Promote this server to a domain controller*** để cấu hình

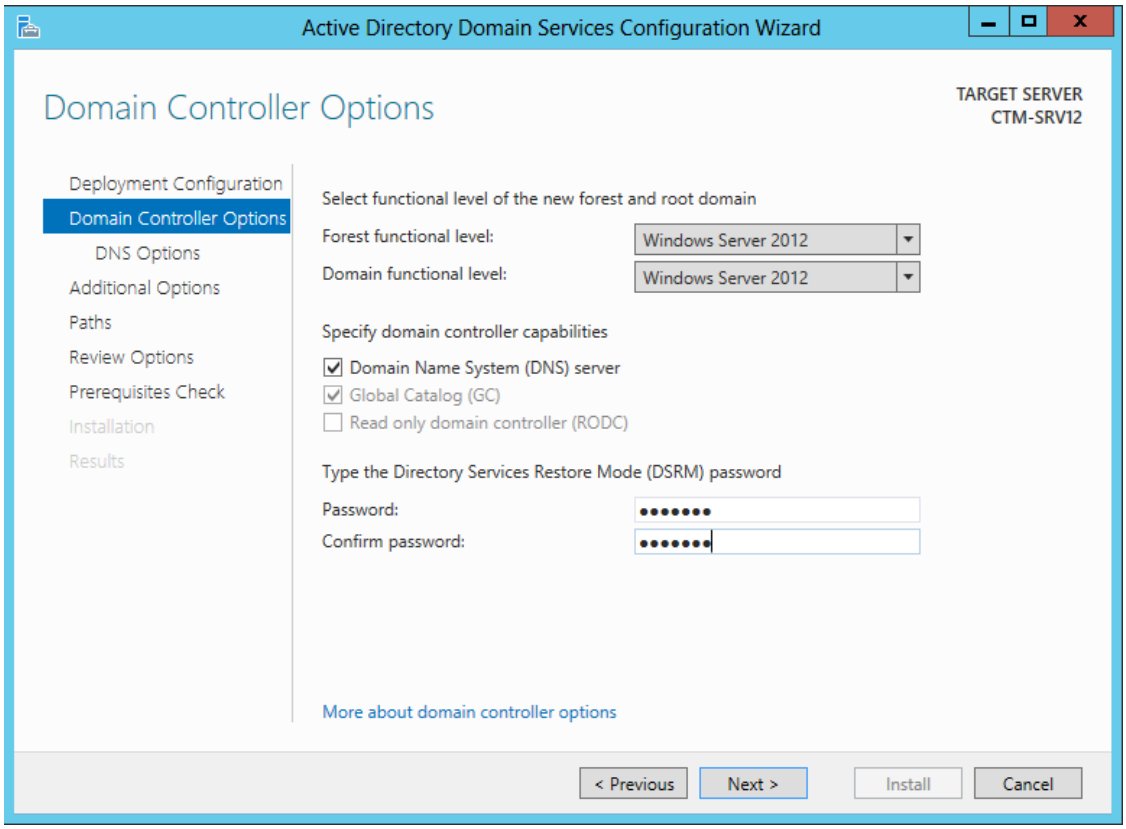


Tại cửa sổ ***Deployment Configuration.*** Trong mục ***Select the deployment operation*** , click chọn vào ***Add a new forest*** để tạo 1 domain mới.

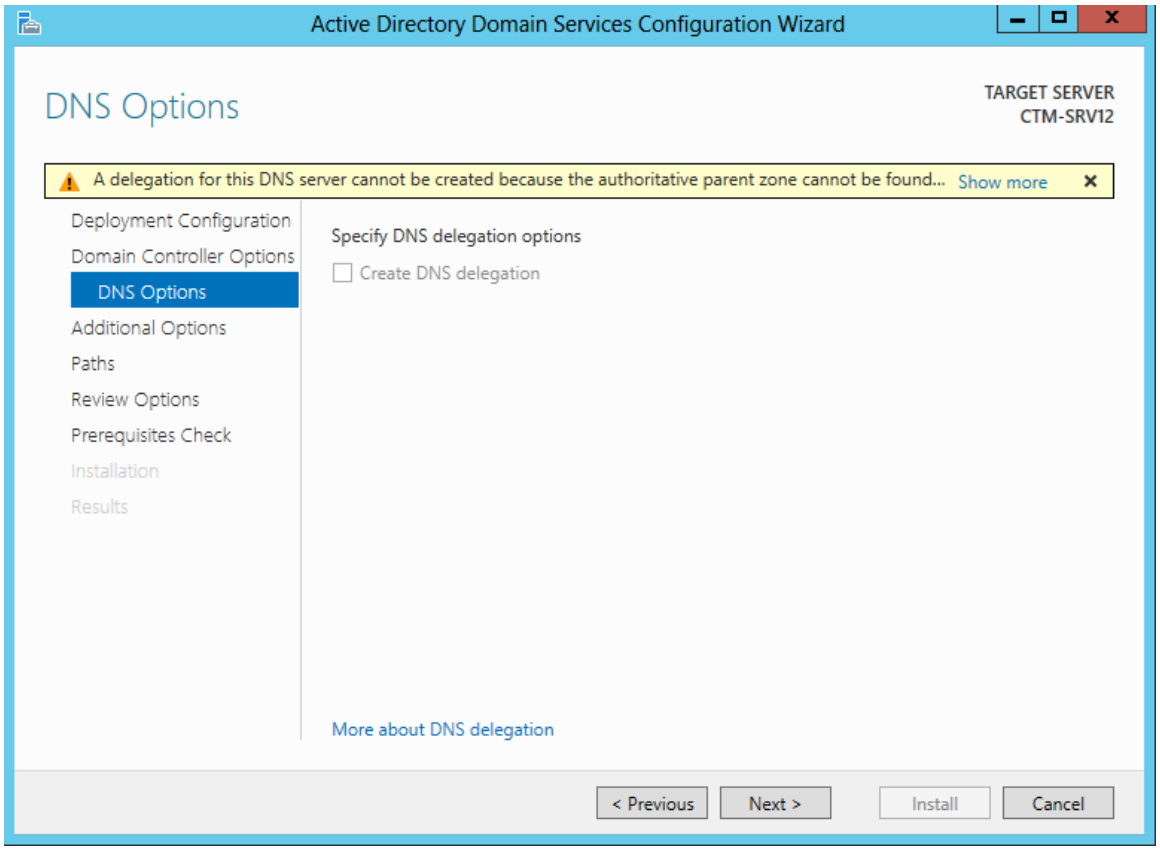
Tại ***Root domain name***, nhập vào tên miền "*ctm.edu.vn*". ***Next***



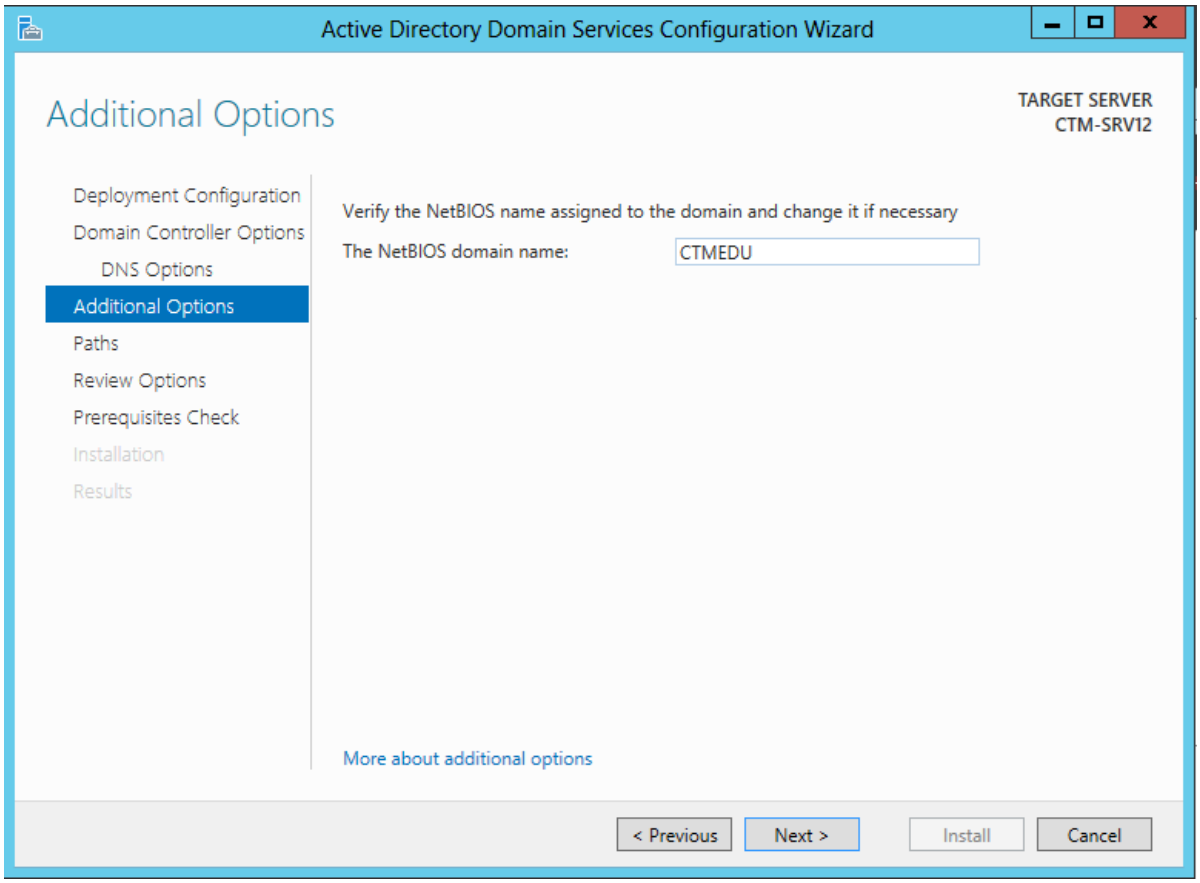
Tại ***Domain Controller Options***. Nhập mật khẩu của ***Directory Services Restore Mode (DSRM) password.*** Click ***Next.***



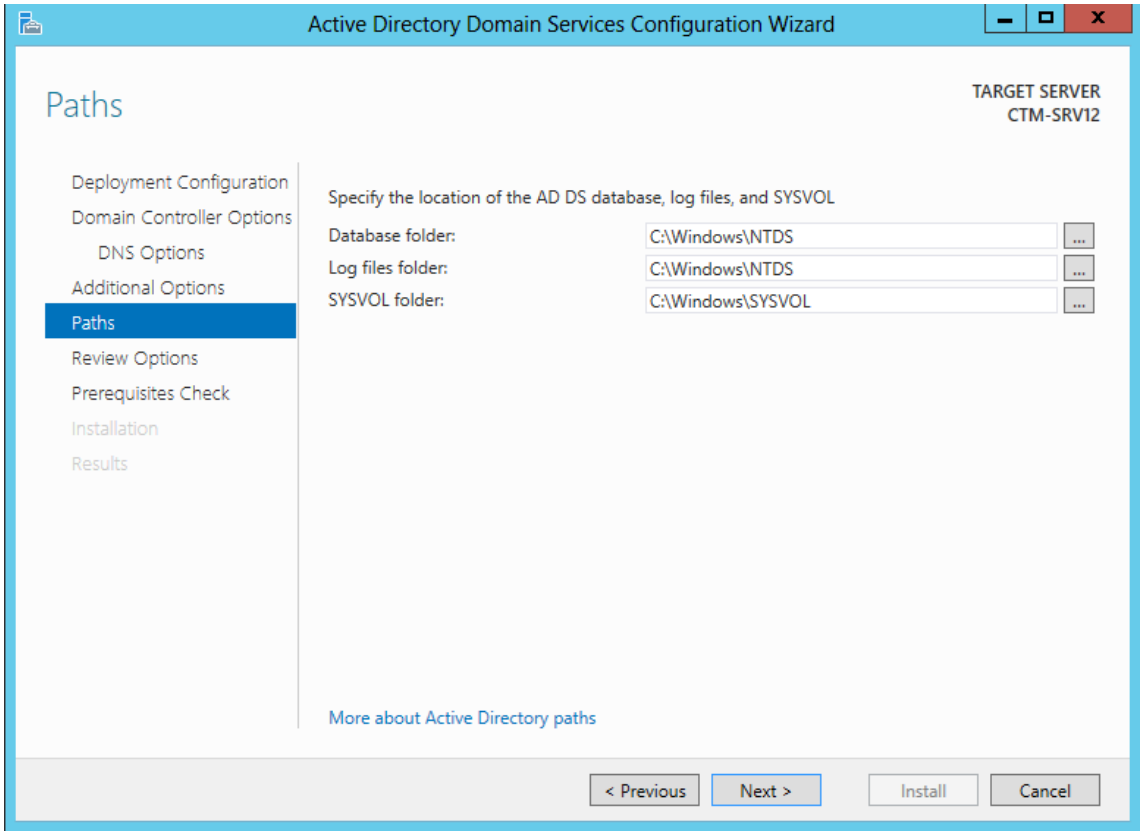
Tại cửa sổ ***DNS Options*** click ***Next***



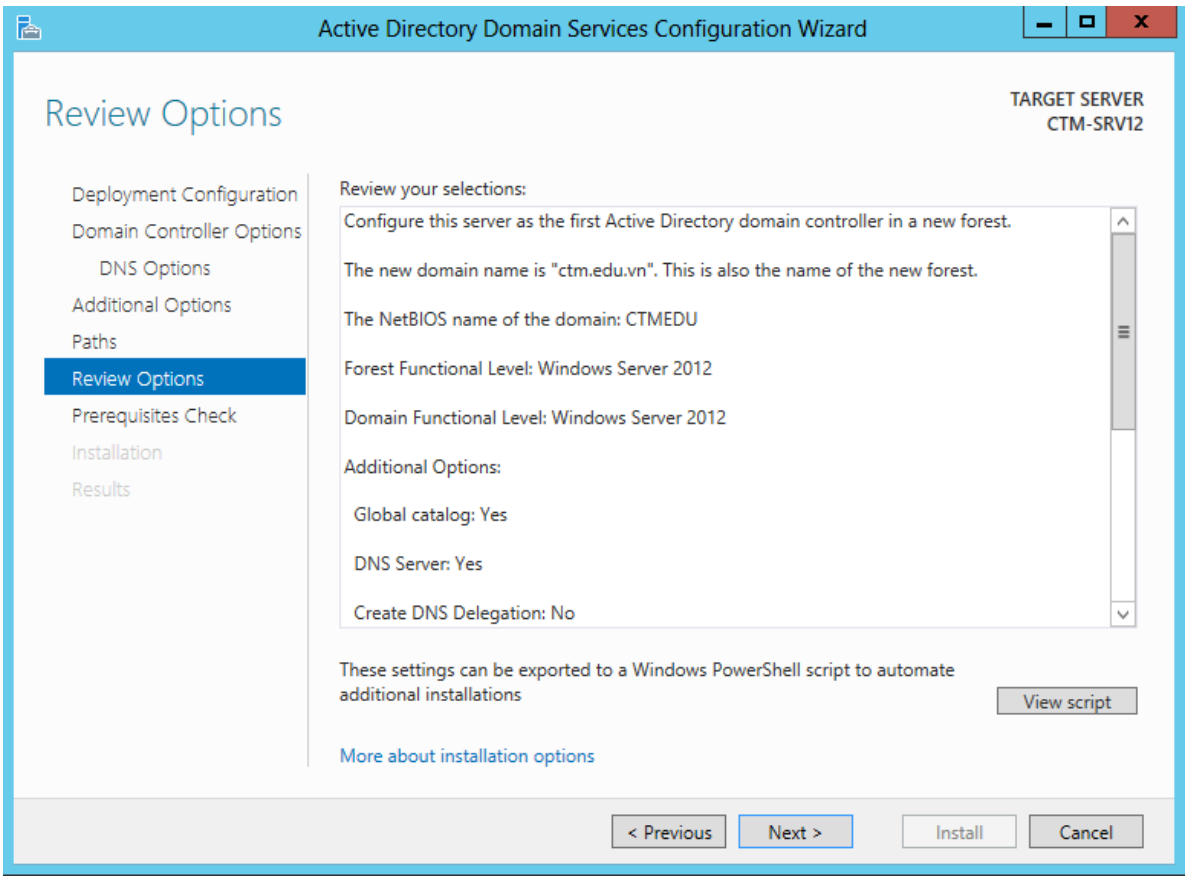
Tại ***Additional Options***, đặt tên ***NetBIOS domain name*** là ***CTMEDU***. Click ***Next***



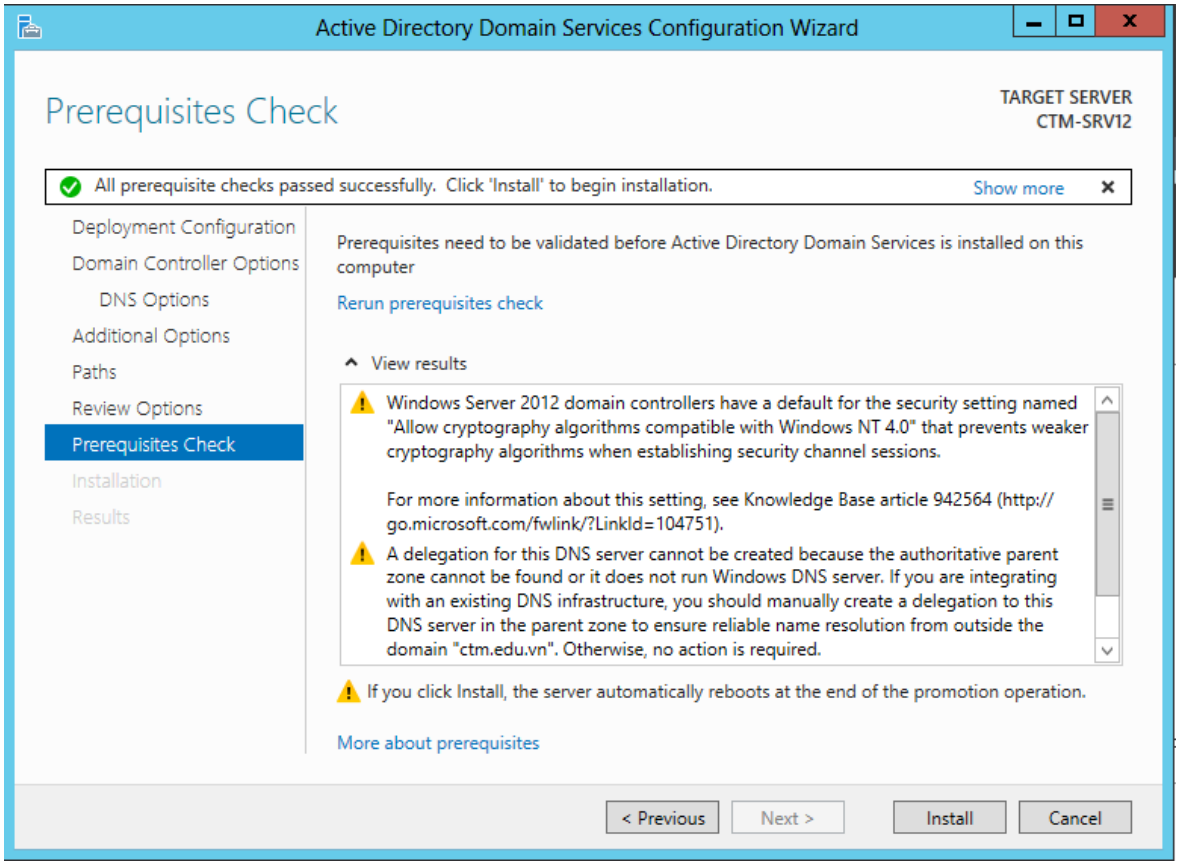
Tại cửa sổ ***Paths***, chính là đường dẫn lưu CSDL của Active Directory trong máy Domain Controller



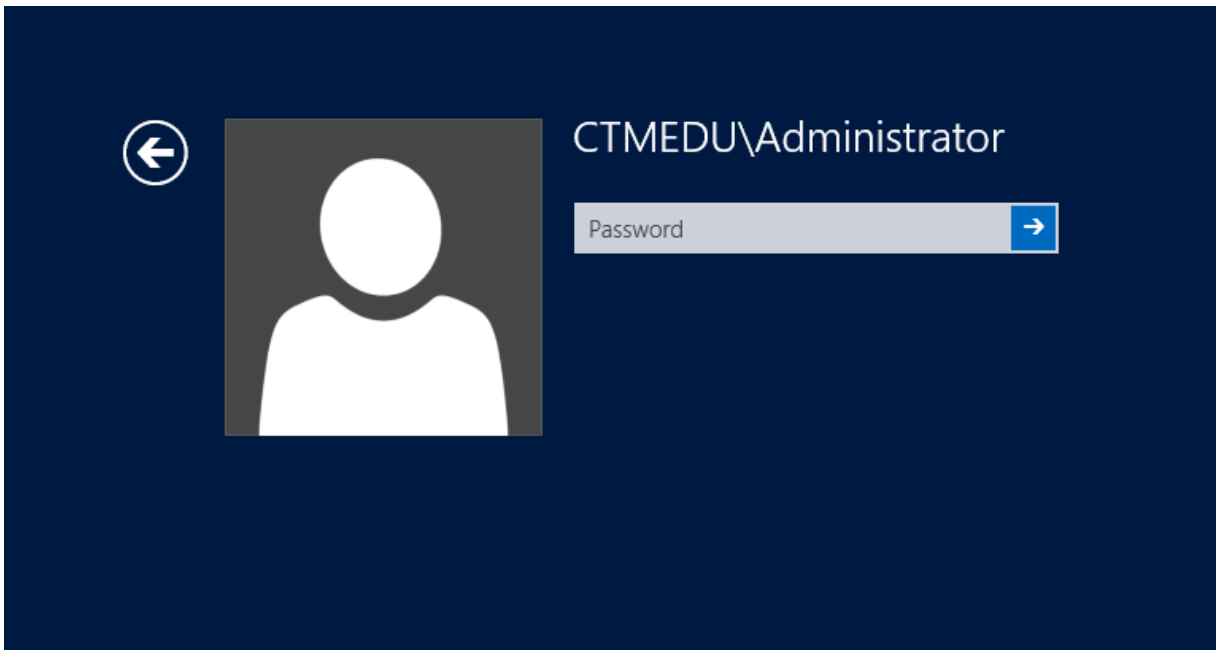
Tại cửa sổ ***Review Options***, tại đây là những thông tin đã cấu hình ở trên. Click vào ***Next***



Tại cửa sổ ***Prerequisites Check***, click vào ***Install*** để máy bắt đầu cài đặt

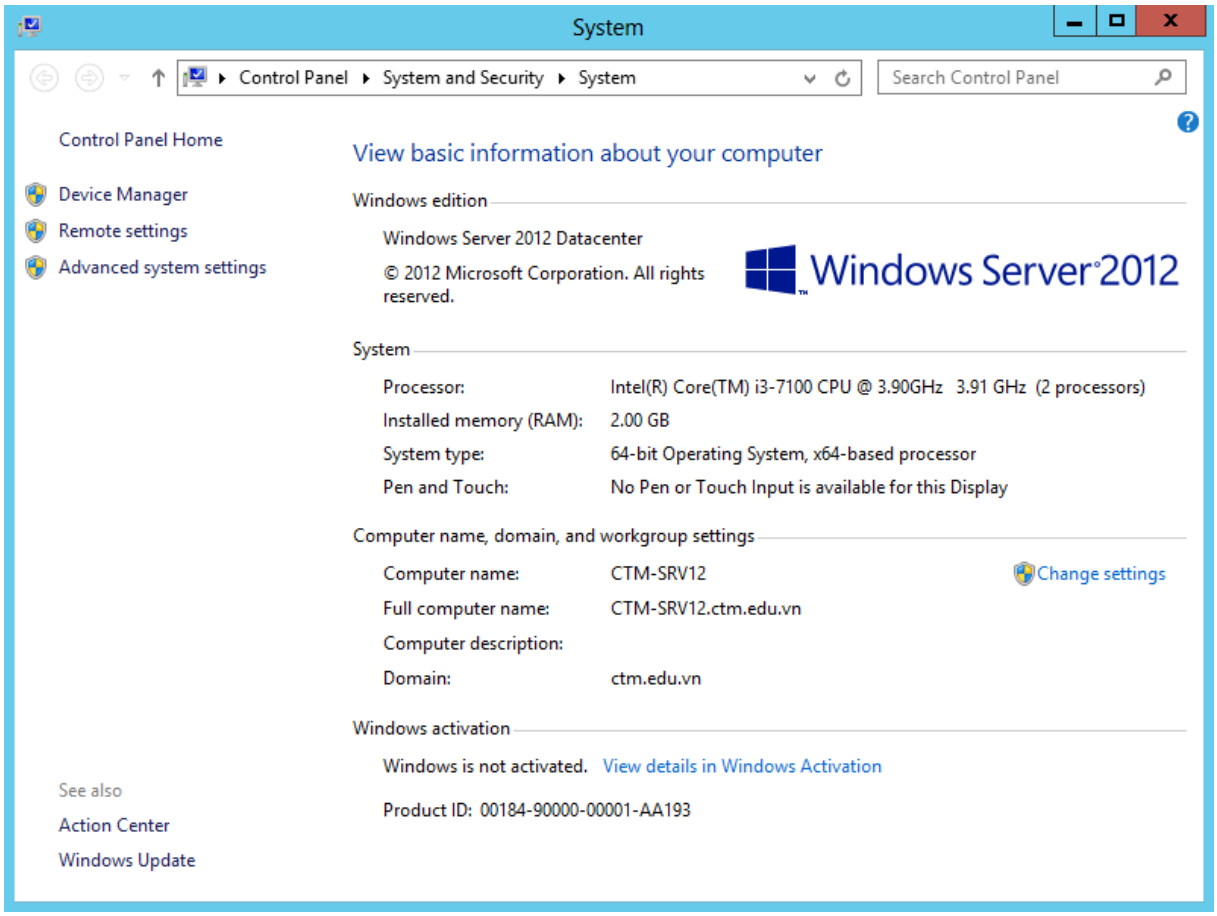


Máy chủ sau khi cài đặt sẽ tự động reset lại máy. Tại màn hình logon, nhập mật khẩu của tài khoản ***Administrator***

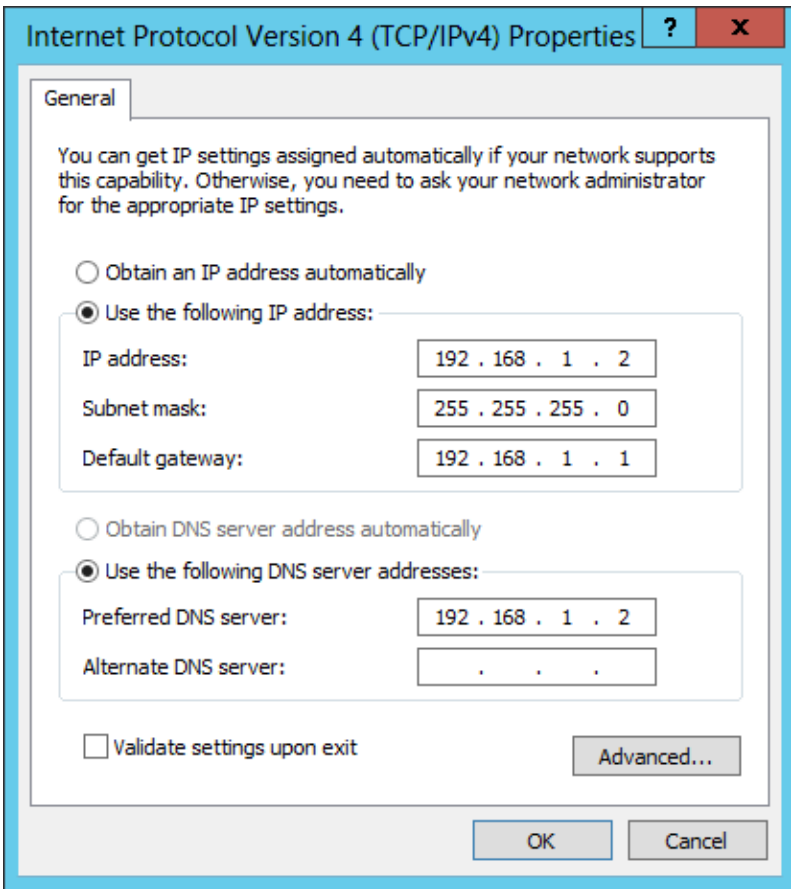


Để kiểm tra máy chủ đã nâng cấp lên Domain Controller chưa, vào ***Computer / Properties*** .

Trong cửa sổ ***System***, kiểm tra tên ***Domain tại Computer name, domain, and workgroup settings***. Domain: *ctm.edu.vn*



Kiểm tra, sửa lại địa chỉ card mạng, địa chỉ ***DNS Server*** phải trùng với địa chỉ IP của máy Domain Controller

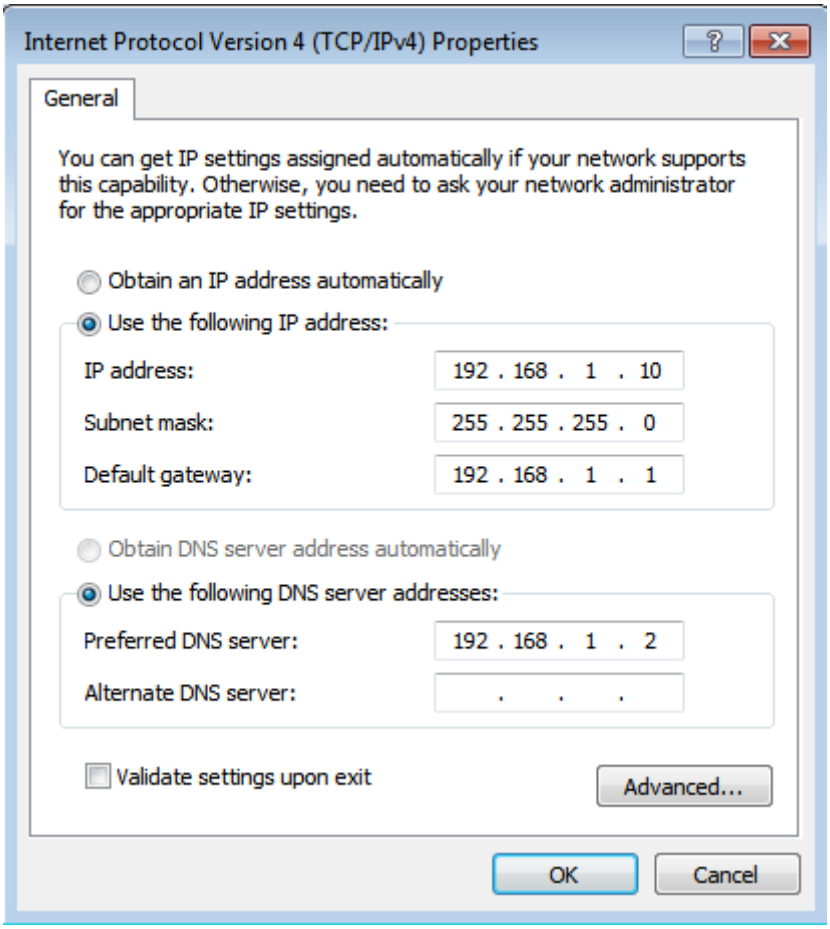


Bước 2: Kết nối máy trạm vào domain

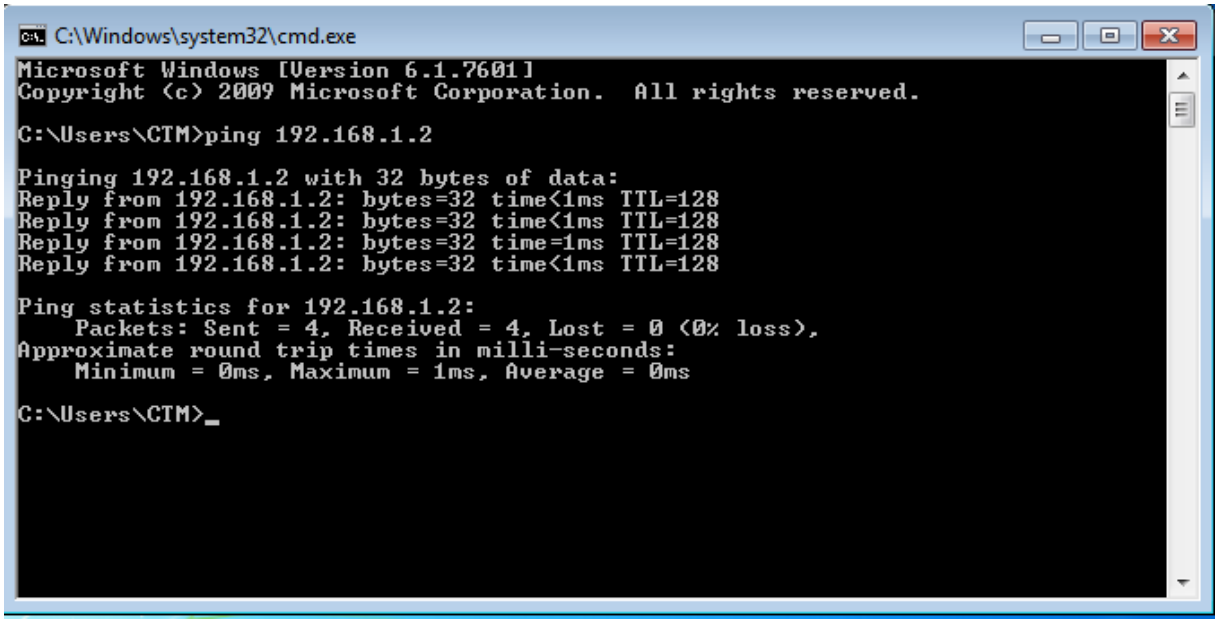
Thực hiện Join máy Client CTM-WRK07 vào Domain.

Mở máy CTM-WRK07 trên máy ảo Wmware.

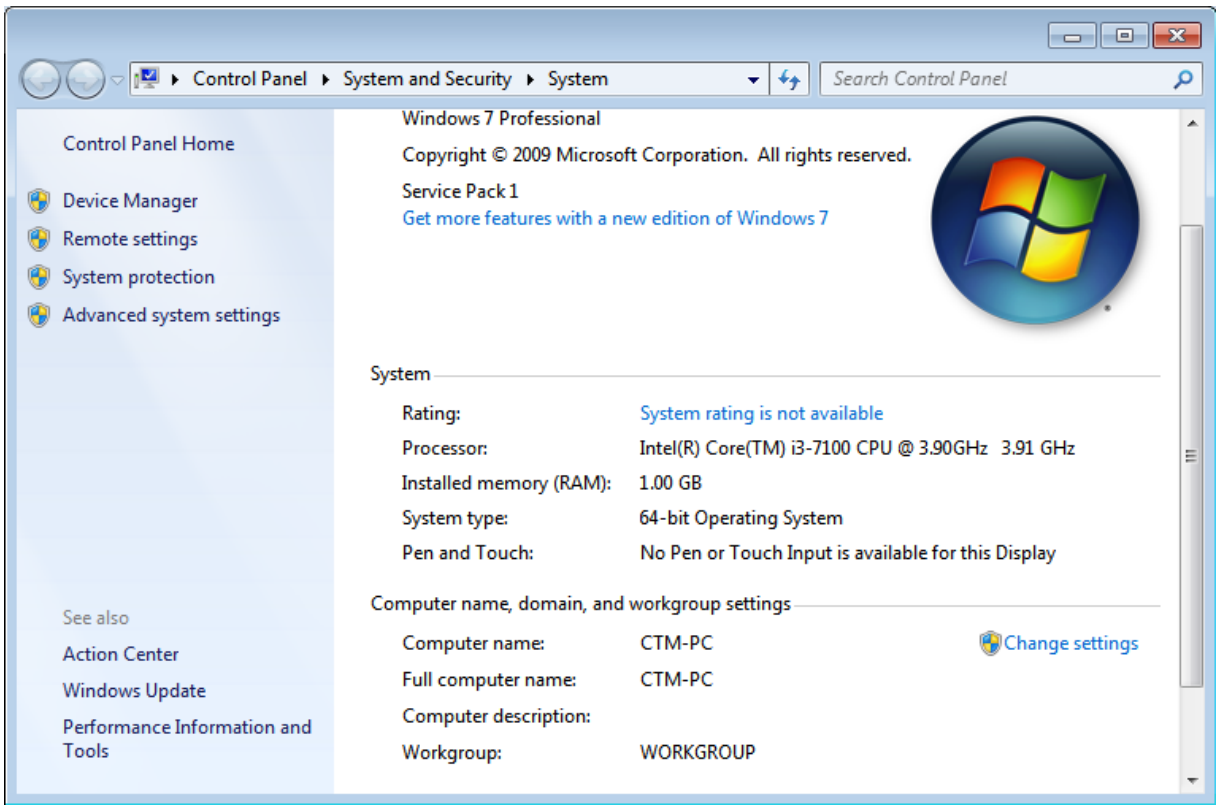
Sửa lại địa chỉ IP của máy CTM-WRK07 như sau:



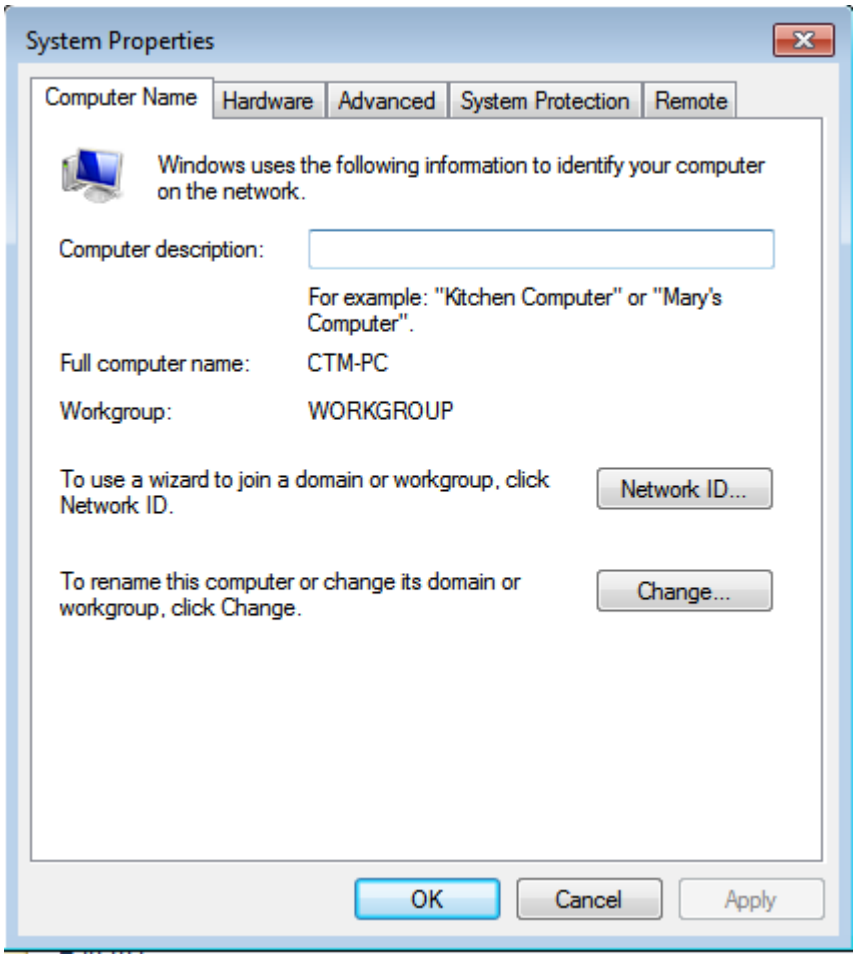
Thực hiện ping từ máy CTM-WRK07 đến máy CTM-SRV12



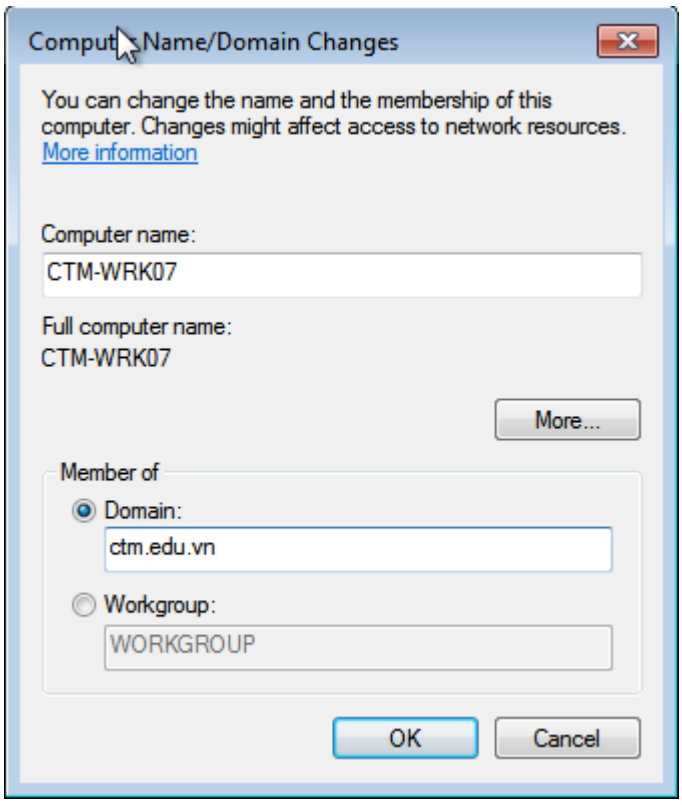
Để Join máy Client CTM-WRK07 vào Domain, vào ***My Computer / Properties / Change Settings***



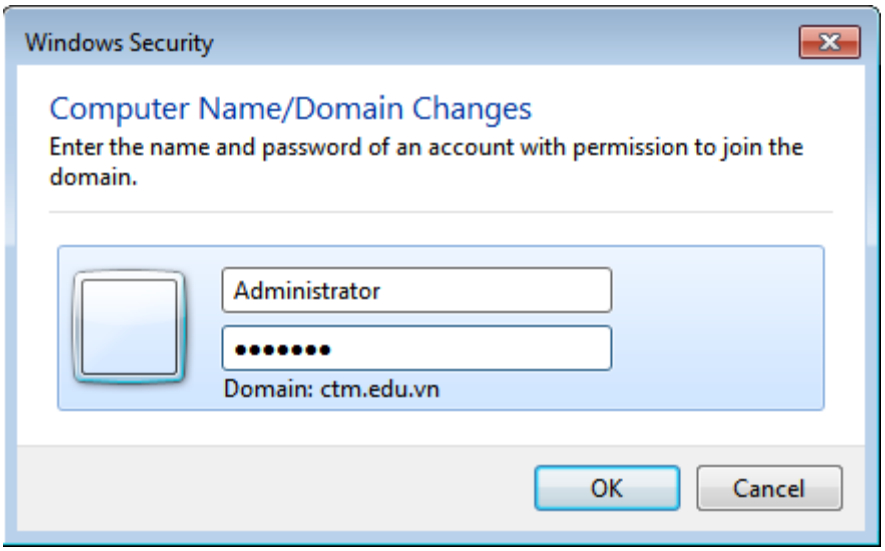
Tại cửa sổ ***System Properties***, Tab ***Computer name***, click vào ***Change***



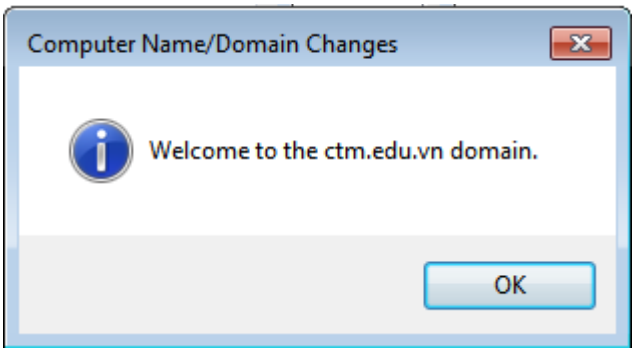
Tại cửa sổ ***Computer Name/Domain Changes***, click chọn vào ***Domain***, tại đây nhập vào tên miền của Domain (*ctm.edu.vn*)



Cửa sổ ***Windows Security***, nhập ***User*** và ***Password*** của Administrator. Click ***OK***

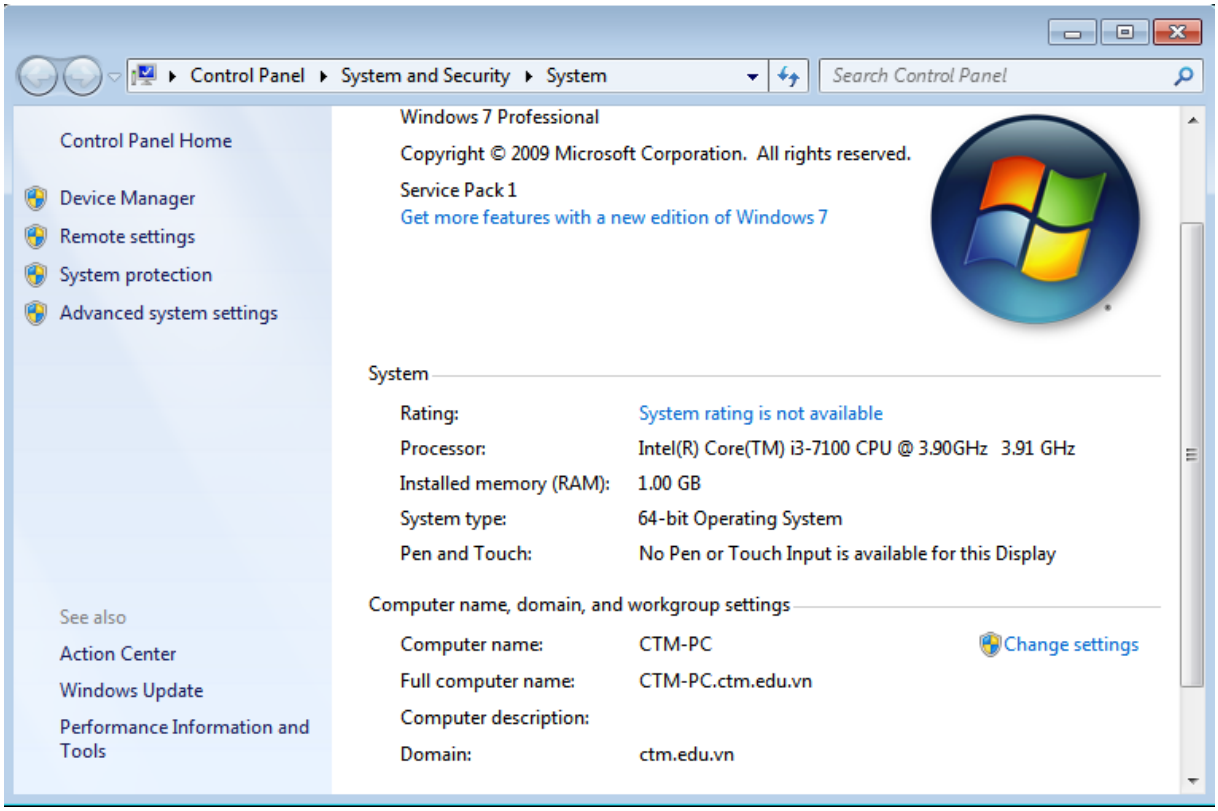


Sau khi Join vào Domain thành công, trên máy xuất hiện thông báo ***Welcome to the ctm.edu.vn domain***



Ấn vào ***OK*** để restart lại máy Client

Khởi động lại máy CTM-WRK07, kiểm tra máy đã Join vào Domain



III. Sai hỏng và cách khắc phục

1. Cài đặt dịch vụ ADDS không thành công

- Nguyên nhân

- Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Tài khoản người dùng quản trị máy chủ chưa có mật khẩu

- Cách khắc phục

- Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
- Đặt mật khẩu người dùng quản trị cho máy chủ

2. Gia nhập vào miền (domain) không thành công

- Nguyên nhân

- Thiết lập địa chỉ IP trên máy CTM-WRK07 chưa đúng
- Nhập tài khoản quản trị trên máy chủ chưa đúng

- Cách khắc phục

- Cài đặt lại địa chỉ IP trên máy CTM-WRK07
- Nhập đúng tài khoản quản trị trên máy chủ

V. Hướng dẫn ôn luyện

- Cài đặt nâng cấp máy chủ chạy HĐH Windows Server 2012 lên Domain Controller.
- Gia nhập vào miền cho các máy trạm

BÀI 3: QUẢN TRỊ TÀI KHOẢN NGƯỜI DÙNG TRÊN ACTIVE DIRECTORY – TẠO OU, GROUP, USER

Trong bài này sẽ đi tìm hiểu về quản trị tài khoản người dùng trên Active Directory, đây là một phần quản trị rất quan trong trong hệ thống Windows sử dụng Domain Controller. Các thành phần này dùng chứng thực người dùng khi truy cập hệ thống mang, thực thi các chính sách, phân quyền sử dụng tài nguyên…

I. Lý thuyết liên quan

1. Organizational Unit, Users và Groups trên Active Directory Users and Computers

a) Tổ chức (Organizational Unit)

Được gói tắt là OU, là một đối tượng trong Active Directore. OU là nơi chứa các đối tượng Active Driectory như user, computer và group. Bên trong OU cũng có thể chứa các OU.

Dùng ủy quyền quản trị (delegation of administration). Ví dụ: khi bạn có một nhóm IT Support, bạn cần ủy thác cho nhóm này quản lý một nhóm máy tính. Khi đó, bạn sẽ cần tạo một OU, đưa các máy tính cần ủy thác quyền quản trị cho nhóm IT Support. Trên OU này, nhòm IT Support sẽ có quyền chỉnh sửa thông tin, thêm, xóa các đối tượng trong OU này. Nhóm IT support này không có bất cứ quyền nào trên các OU khác.

Dùng áp dụng các chính sách (Group Policy). Group Policy sẽ được tự động áp dụng cho các đối tượng là user và computer. Ví dụ: bạn muốn một số user được map một ổ mạng từ File Server một cách tự động. Bạn sẽ tiến hành tạo một OU, sau đó đưa các user cần thực hiện chính sách vào OU này. Bạn tiến hành tạo một Group Policy cho phép map thu mục, và tiến hành link Group Policy với OU này. Các OU không link Group Policy sẽ không bị ảnh hưởng của Group Policy map ổ đĩa này. Một OU có thể được áp dụng nhiều Group Policy.

b) Nhóm (Group)

Là đối tượng của Active Directory, dùng để chứng thực và phân quyền. Group có thể được dùng để phân quyền truy cập trên các tài nguyên. Các user thành viên của Group sẽ có quyền truy cập tài nguyên mà Group đó có được phân quyền truy cập.

Thành viên (member) của Group là User và Group. Group được chứa trong các OU.

Có hai kiểu Group là security groups và distribution groups.

Security groups: được sử dụng để cấp quyền cho phép hoặc không cho phép truy cập.

Distribution groups: dùng để phân phối email (chủ yếu dùng cho Microsoft Exchange), đối với các user không cần truy cập tài nguyên hoặc login máy tính sẽ được đưa vào kiểu Group này.

Phạm vi Group (Group Scopes) gồm có :

- Domain local: Có thể có thành viên là bất kỳ domain nào trong forest, có thể cấp quyền trong cùng domain

- Global: Có thể có thành viên cùng domain, có thể cấm quyền trong bất kỳ domain nào trong forest
- Universal: Có thể có thành viên trong bất kỳ domain nào trong forest, có thể cấp quyền bất kỳ domain hoặc forest.

c) Người dùng (User)

Được cấp trực tiếp cho người dùng, là đối tượng của Active Directory, dùng để chứng thực và phân quyền. User cũng có thể dùng để phân quyền trên truy cập các tài nguyên. Thông thường, user sẽ được thừa hưởng chính sách từ Group.

User là lơp cuối cùng trong kiến trúc của Active Drectory.

User có thể là thành viên của một hoặc nhiều Group. Được chứa trong các OU.

User cũng là đối tượng chủ yếu được áp dụng các Group Policy.

d) Máy tính (Computer)

Là một đối tượng của Active Directory, giống như user, là một lớp cuối trong kiến trúc trong Active Directory. Có thể gọi computer là một user của thiết bị.

Computer cũng có thể là thành viên của một hoặc nhiều Group.

Có thể được dùng cấp quyền truy xuất tài nguyên trong hệ thống.

Computer được chứa trong các OU, cũng là đối tượng chịu tác dụng của Group Policy.

2. Cách tổ chức của OU, Group, User và Computer:

- OU (Organizational Unit):

Chứa các OU con, Groups,Users, Computer bên trong nó.

- Groups:

Một group có thể có các thành viên khác (member) là các Group khác hoặc các User.

Một Group có thể là thành viên của (member of) nhiều Group.

Group được chứa trong OU

Các Group là thành viên của (member of) của Group sẽ được thừa hưởng quyền của Group mà nó là thành viên.

- User và Computer:

Một User và Computer có thể là thành viên của (member of) một hoặc nhiều Group.

User và Computer được chứa trong OU.

User và Computer có thể được thừa kế quyền của Group mà nó là thành viên.

Trên máy cục bộ các User và Group được quản lý trong Local User and Group. Trên Active Directory, các User và Group được quản lý trong công cụ có tên là Active Directory Users and Computers.

II. Trình tự thực hiện

1. Yêu cầu thực hiện

- Tạo mới tài khoản người dùng (User)
- Tạo nhóm người dùng (Group)
- Tạo mới tổ chức (OU)

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

3. Các bước thực hiện

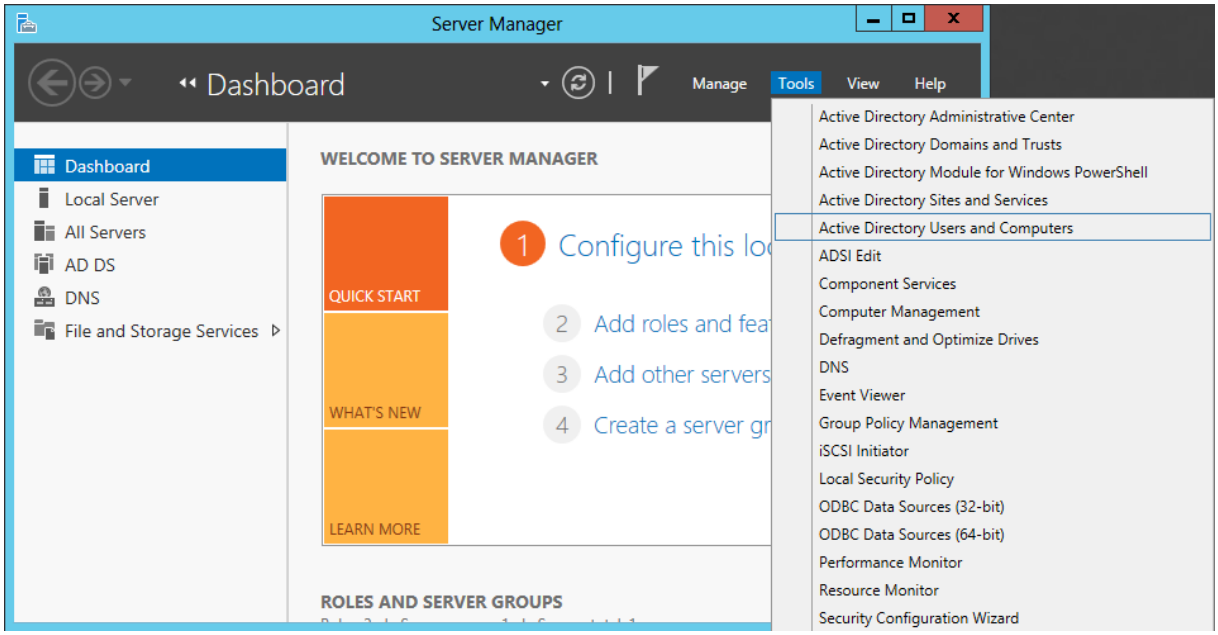
Thực hiện cài đặt quản lý Organizational Unit, Users và Groups trên Active Directory Users and Computers thông qua 3 bước sau:

- Bước 1: Tạo mới tài khoản người dùng (User)
- Bước 2: Tạo nhóm người dùng (Group)
- Bước 3: Xây dựng một Organizational Unit
- Bước 4: Chuyển qua máy Client, kiểm tra đăng nhập tài khoản User

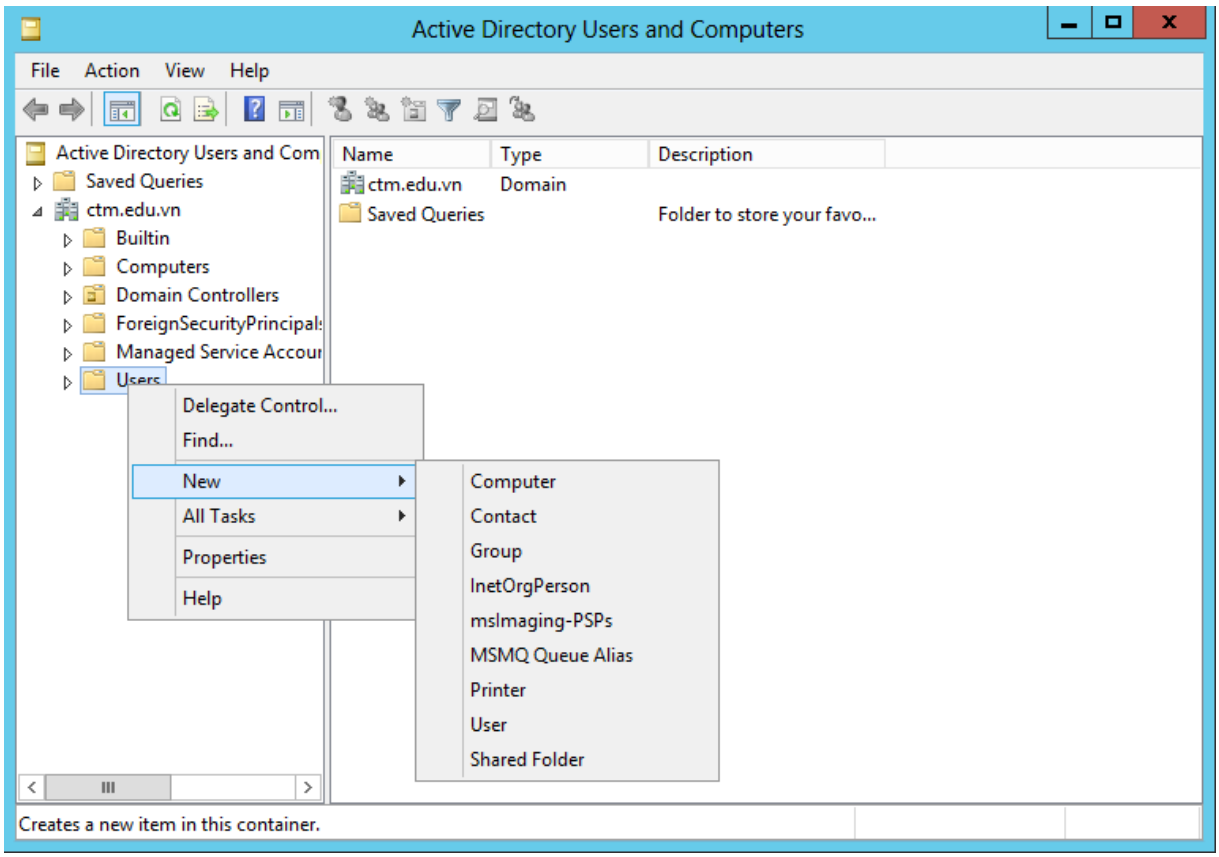
Hướng dẫn chi tiết

Bước 1: Tạo mới tài khoản người dùng (User)

Vào ***Server Manager / Tools / Active Directory User and Computer***.

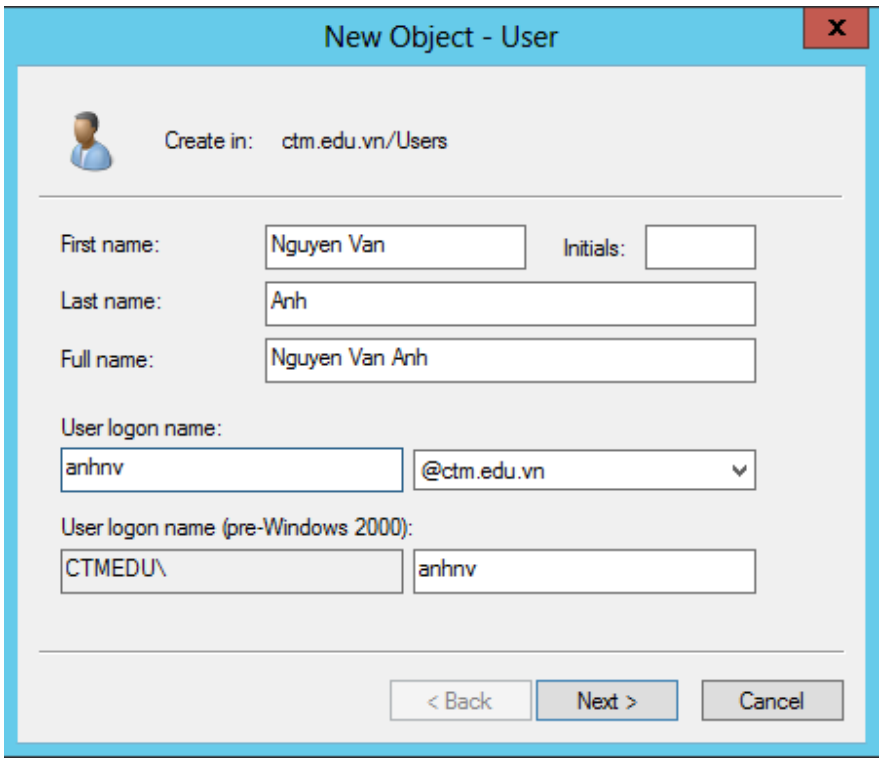


Tại ***Users***, click chuột phải chọn ***New / User***



Tại cửa sổ New Object – User, nhập vào các thông số sau:

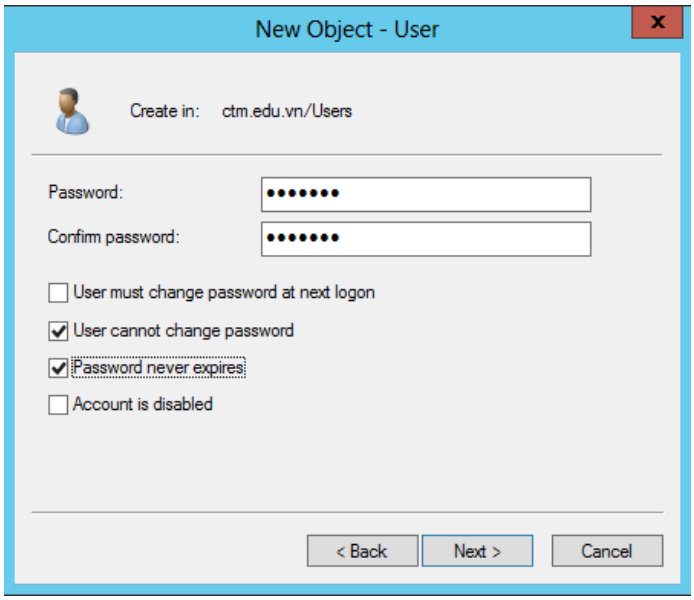
- First name: Nguyen Van
- Last name: Anh
- Full name: Nguyen Van Anh
- User logon name: anhnv (@ctm.edu.vn)



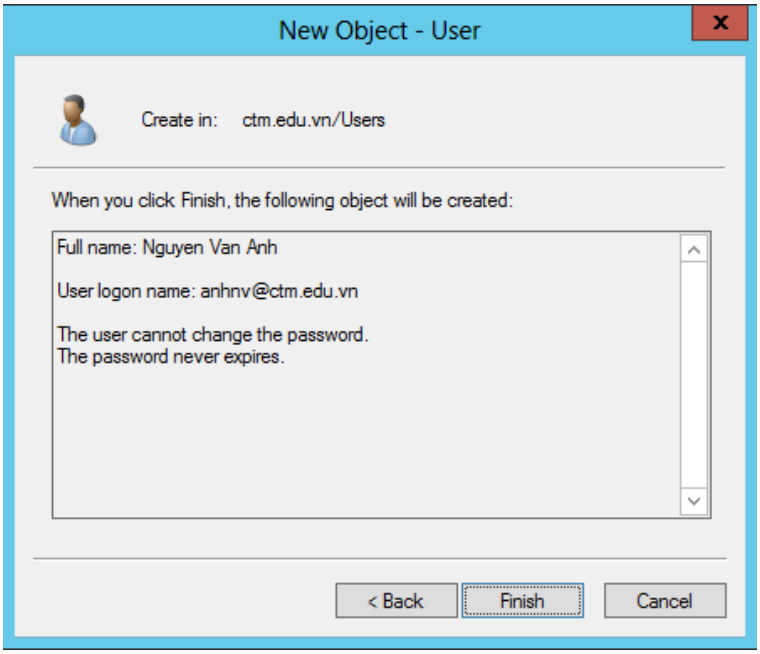
Tại cửa sổ tiếp theo, nhập vào mật khẩu (password) của tài khoản anhnv

Lưu ý:

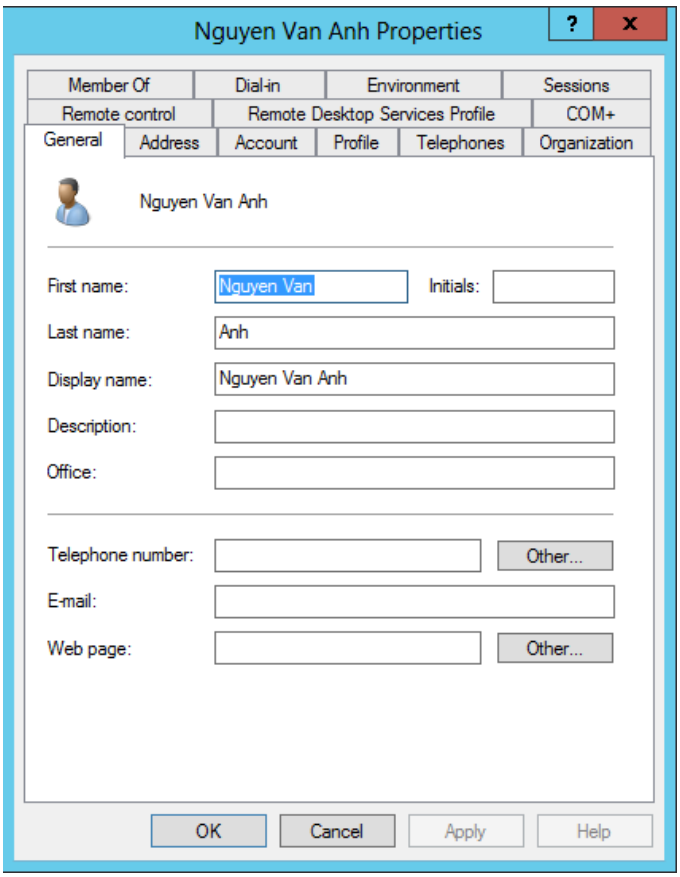
- ***User must change password at next logon***: tài khoản phải thay đổi mật khẩu trong lần đăng nhập tiếp theo (khuyến khích bỏ tùy chọn này).
- ***User cannot change password*** : Tài khoản không được thay đổi password (khuyến khích dùng tùy chọn này).
- ***Password never expires***: Mật khẩu không bao giờ hết hạn (khuyến khích dùng tùy chọn này).
- ***Account is disabled*** : Tài khoản bị khóa. (khuyến khích không dùng tùy chọn này).



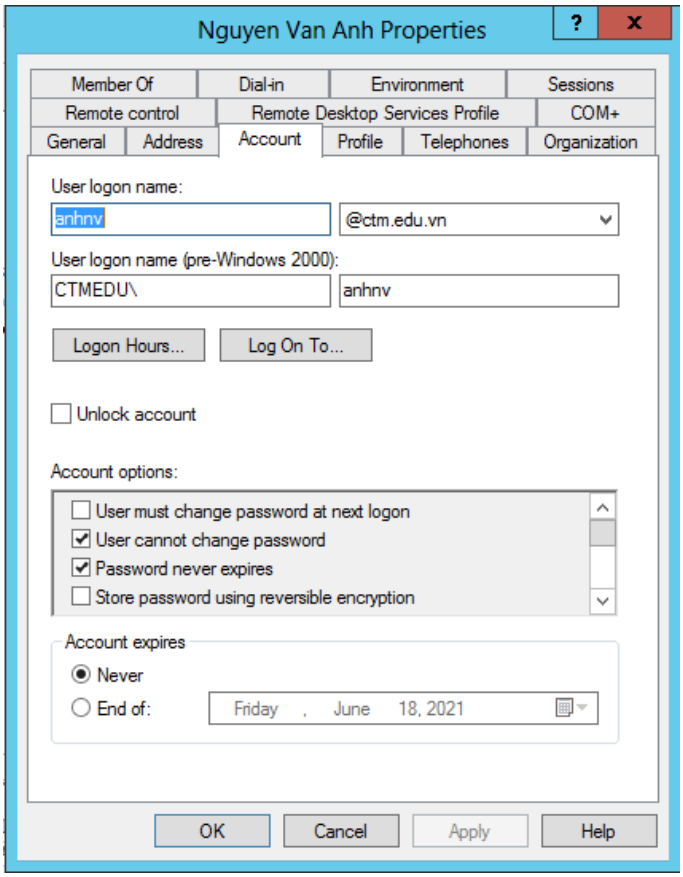
Chọn ***Finish*** để hoàn thành, ***Back*** để chỉnh sửa lại các thông tin nếu cần.



- Các thuộc tính của tài khoản người dùng

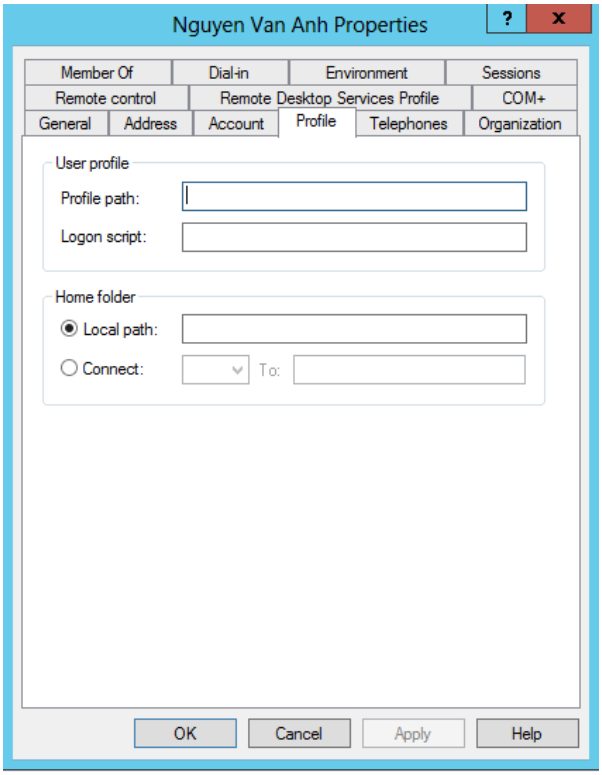


Tab ***General*** chứa các thông tin chung của người dùng. Có thể nhập thêm một số thông tin như: số điện thoại, địa chỉ mail và địa chỉ trang Web cá nhân…



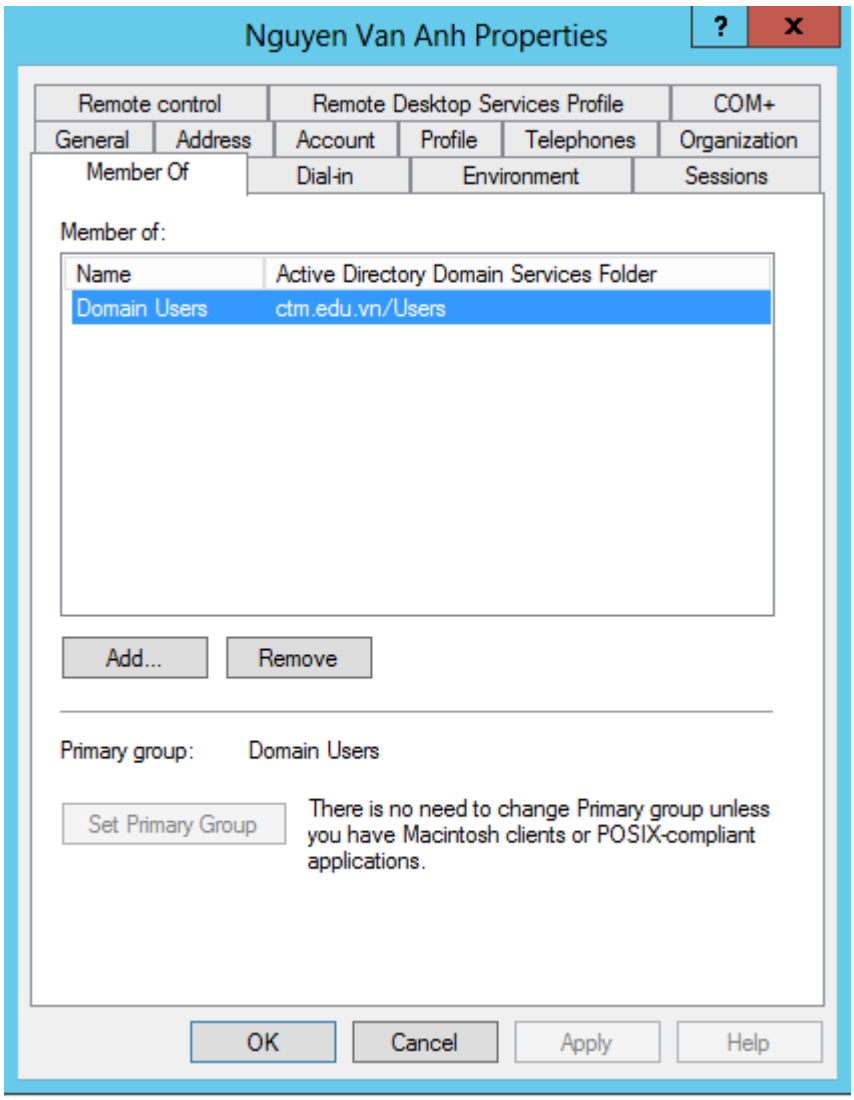
Tab ***Account*** cho phép:

- 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 thời điểm hết hạn của tài khoản…



Tab ***Profile***:

- Khai báo đường dẫn đến Profile
- Khai báo tập tin logon script: tự động thi hành khi đăng nhập hay khai báo home folder.
- 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…
- User profile tạo và duy trì tình trạng desktop (desktop settings) của từng user
- User profile có thể được lưu trên server, được dùng từ các máy client
- Có thể tạo user profile dùng cho nhiều user
- Có thể không cho phép user thay đổi tình trạng desktop

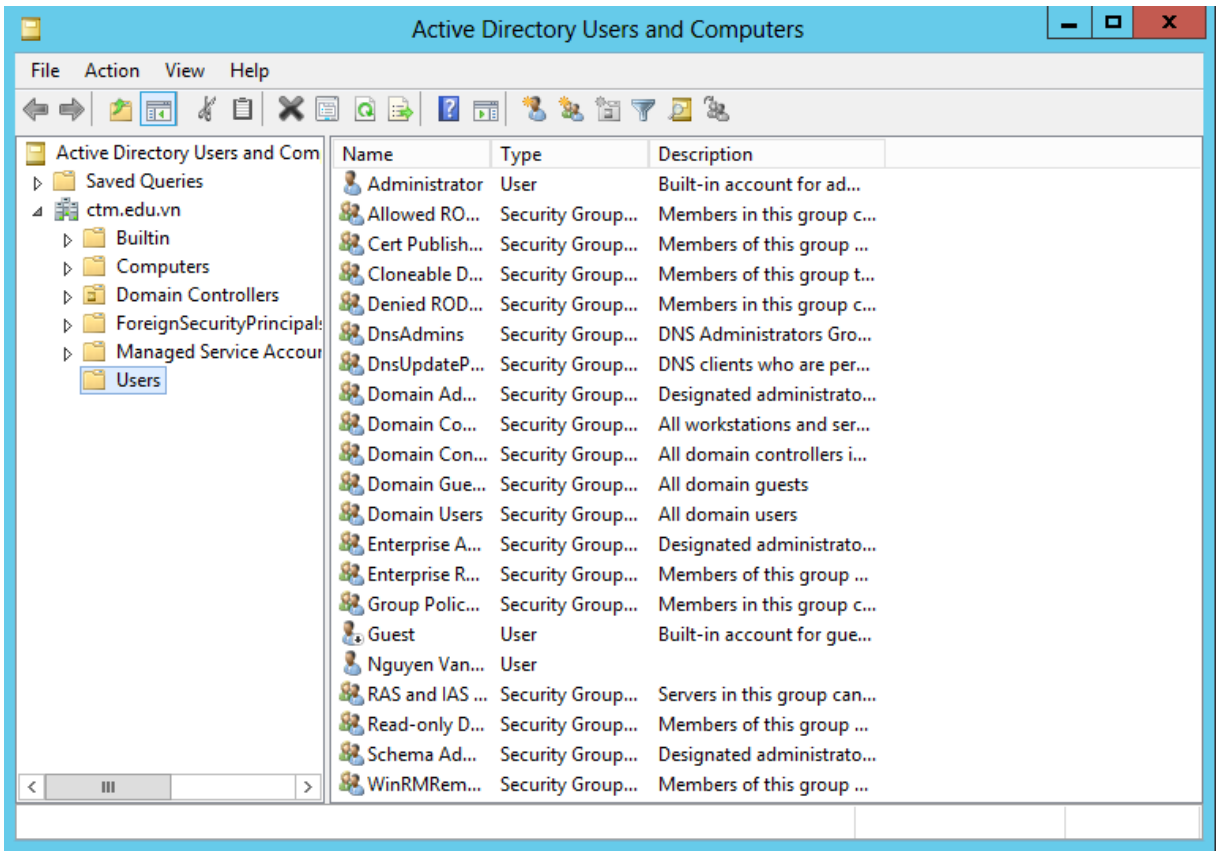


Tab ***Member Of***:

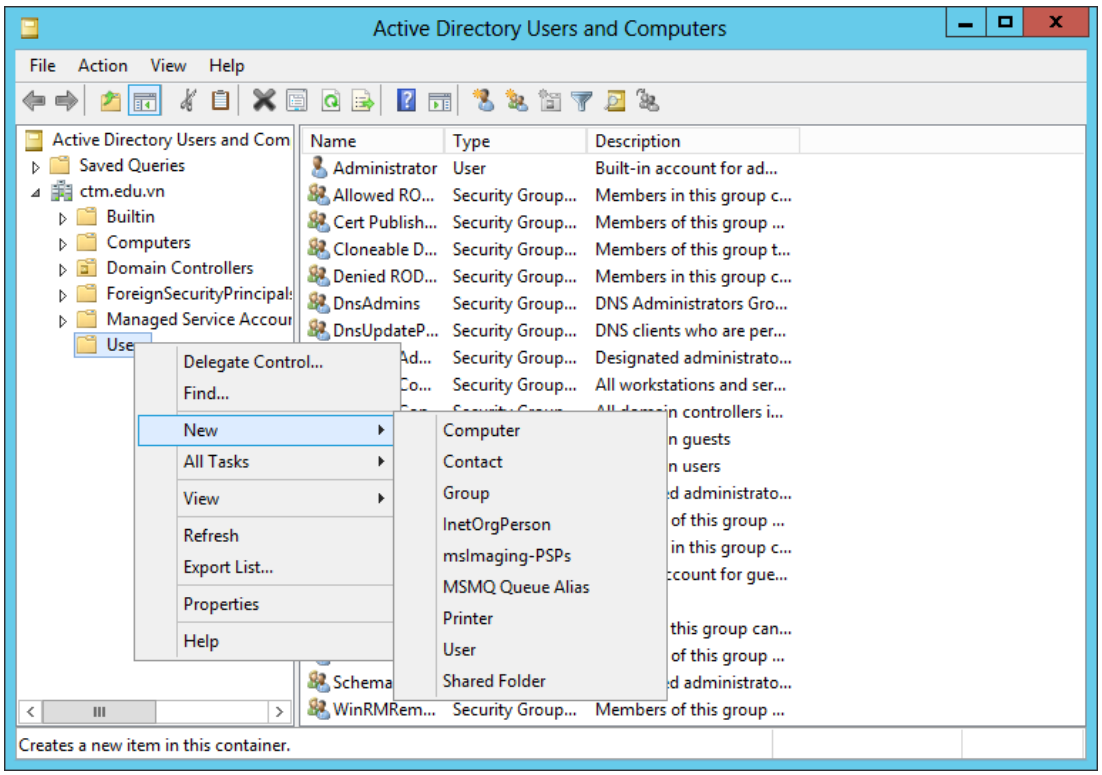
- Xem và cấu hình tài khoản người dùng hiện tại. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này.
- Muốn gia nhập vào nhóm nhấp chuột vào nút Add, hộp thoại chọn nhóm sẽ hiện ra

Bước 2: Tạo mới nhóm (Group) trên domain

Vào ***Server Manager / Tools / Active Directory User and Computer***.



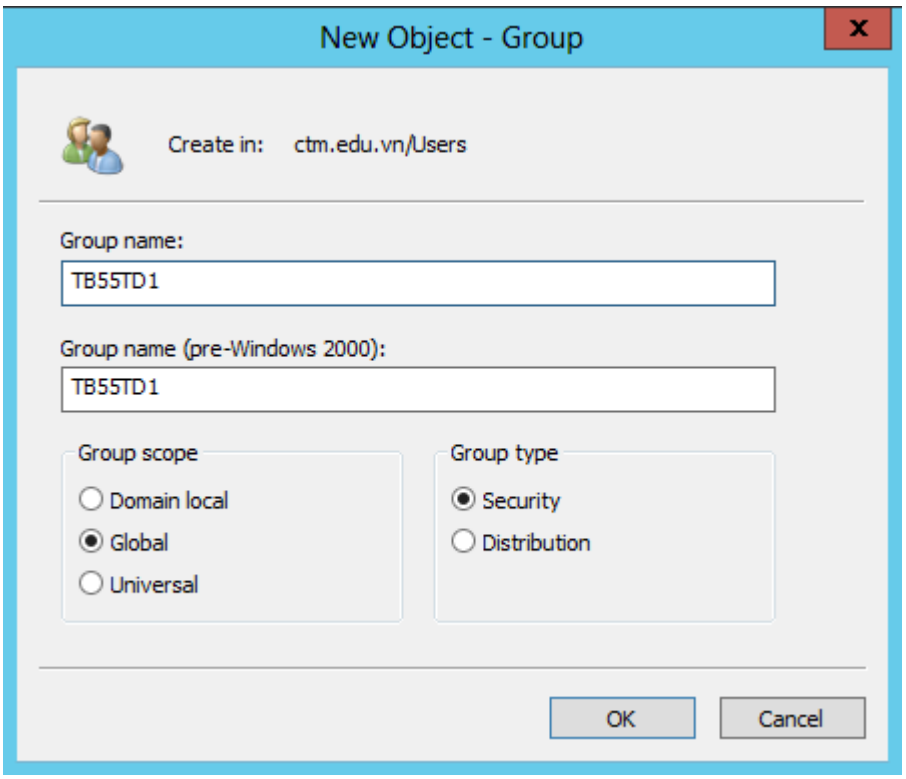
Tại ***Users*** , chuột phải chọn ***New / Group***.



Tại cửa sổ ***New object – Group***, nhập vào tên ***Group***.

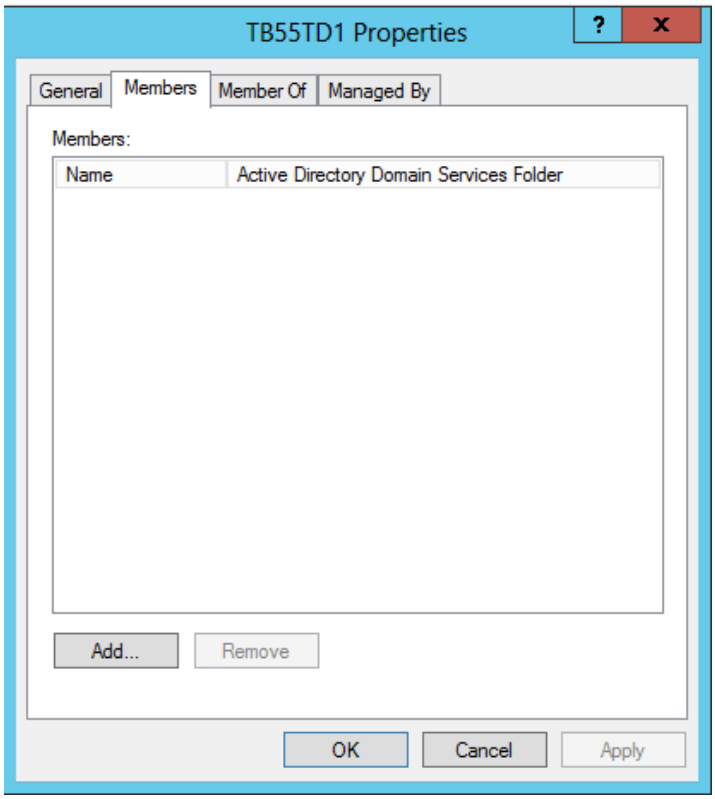
Group scope : Global

Group Type : Security

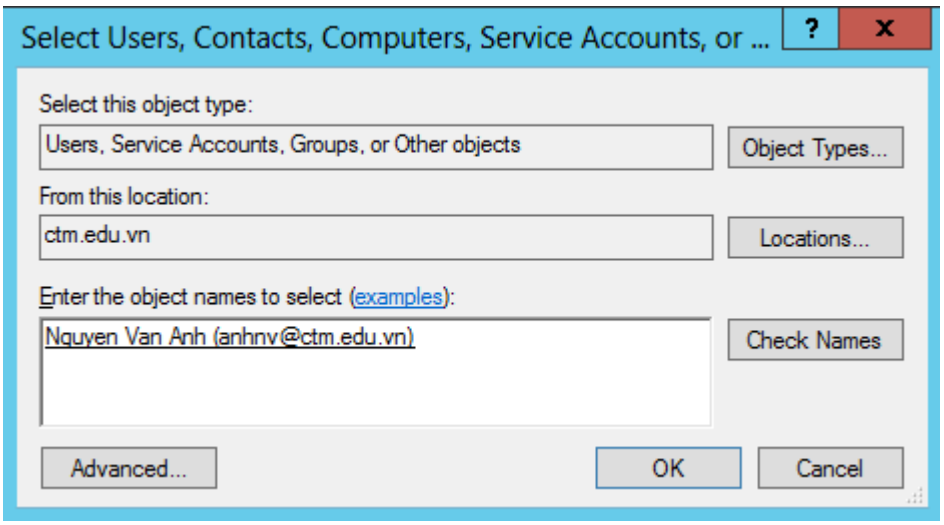


Bổ sung các user vào group vừa tạo:

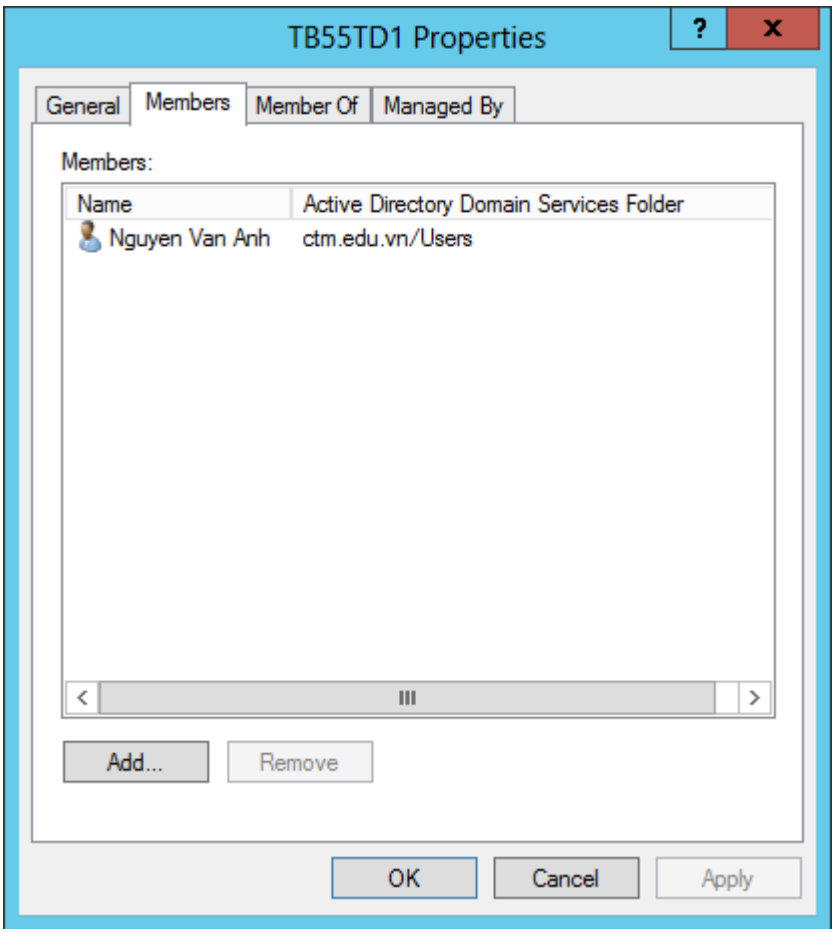
Click chuột phải tại ***Group TB55TD1***, chọn Properties. Tại cửa sổ ***TB55TD1 Properties***, chuyển sang tab ***Members***.



Click vào ***Add…***, Tại cửa sổ ***Select Users, Contacts, Computers , Service Accounts…. / Enter the object names to select*** , nhập vào User cần add vào Group (VD: nhập vào User *anhnv@ctm.edu.vn*), click vào ***Check Names*** khi nhập tên User



Add User vào Group thành công

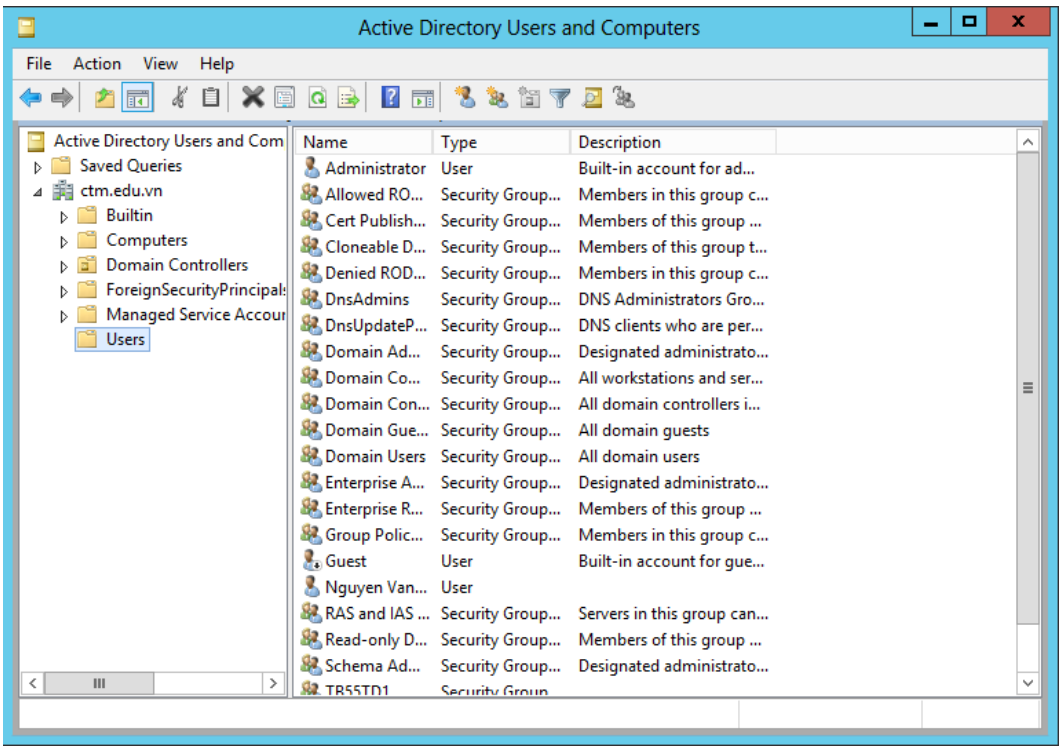


Bước 3: Xây dựng một Organizational Unit

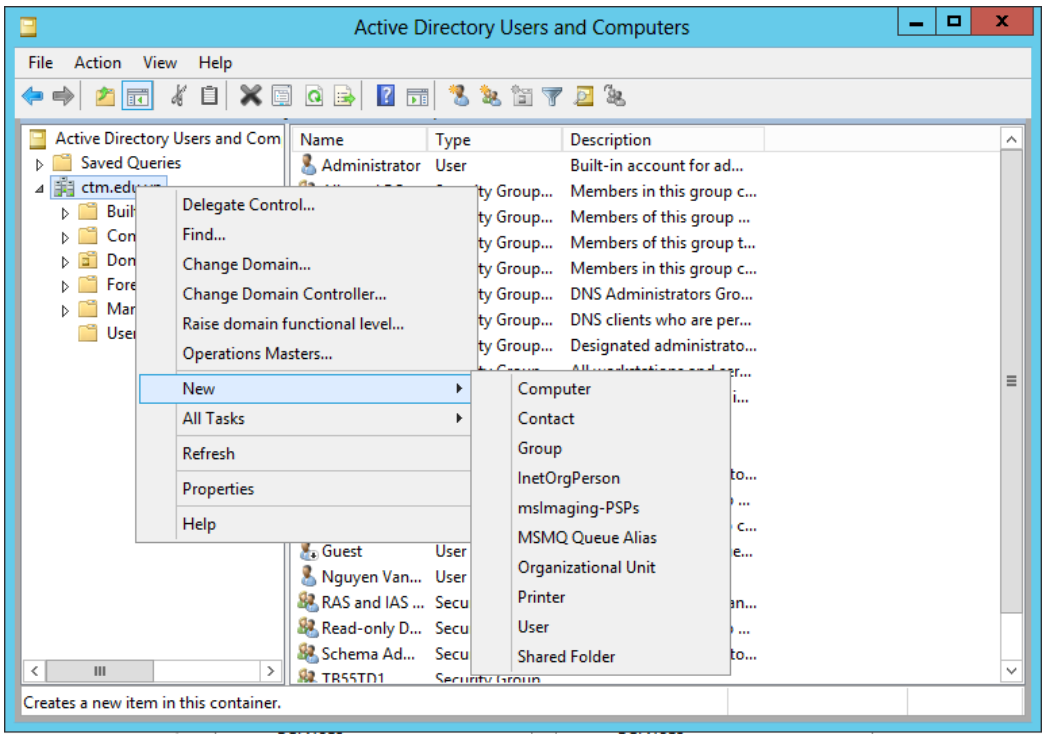
- Thực hiện trên máy CTM-SVR12, tạo OU:

Vào ***Server Manager / Tools***.

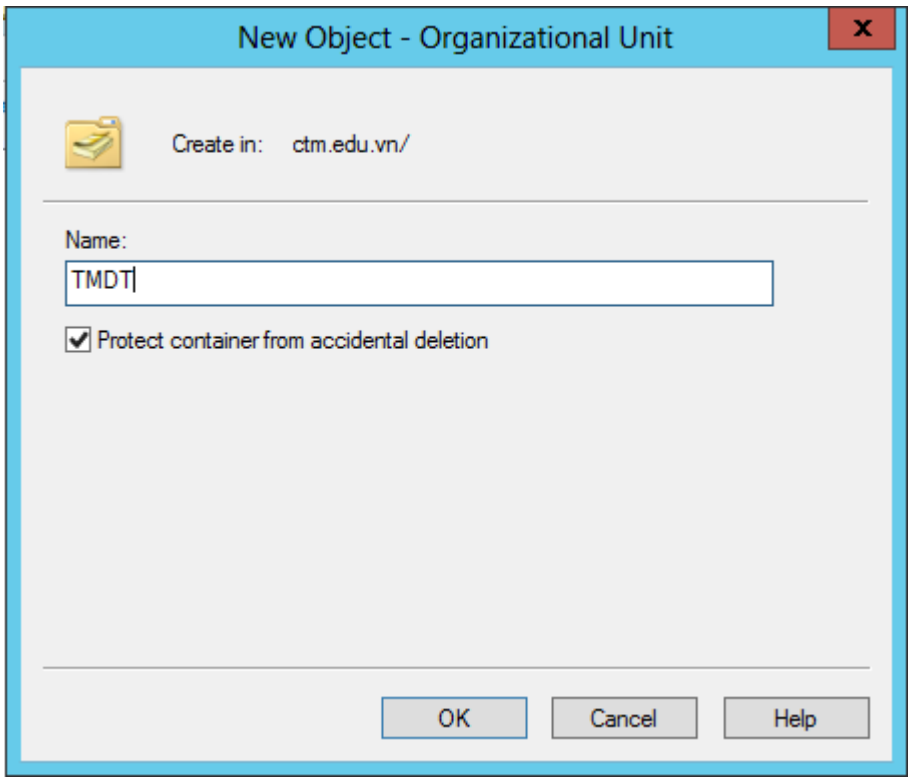
Mở dịch vụ ***Active Directory User and Computer*** để tạo các thuộc tinh.



Để tạo OU. Click chuột phải tại tên miền *ctm.edu.vn*, chọn ***New / Organizational Unit***

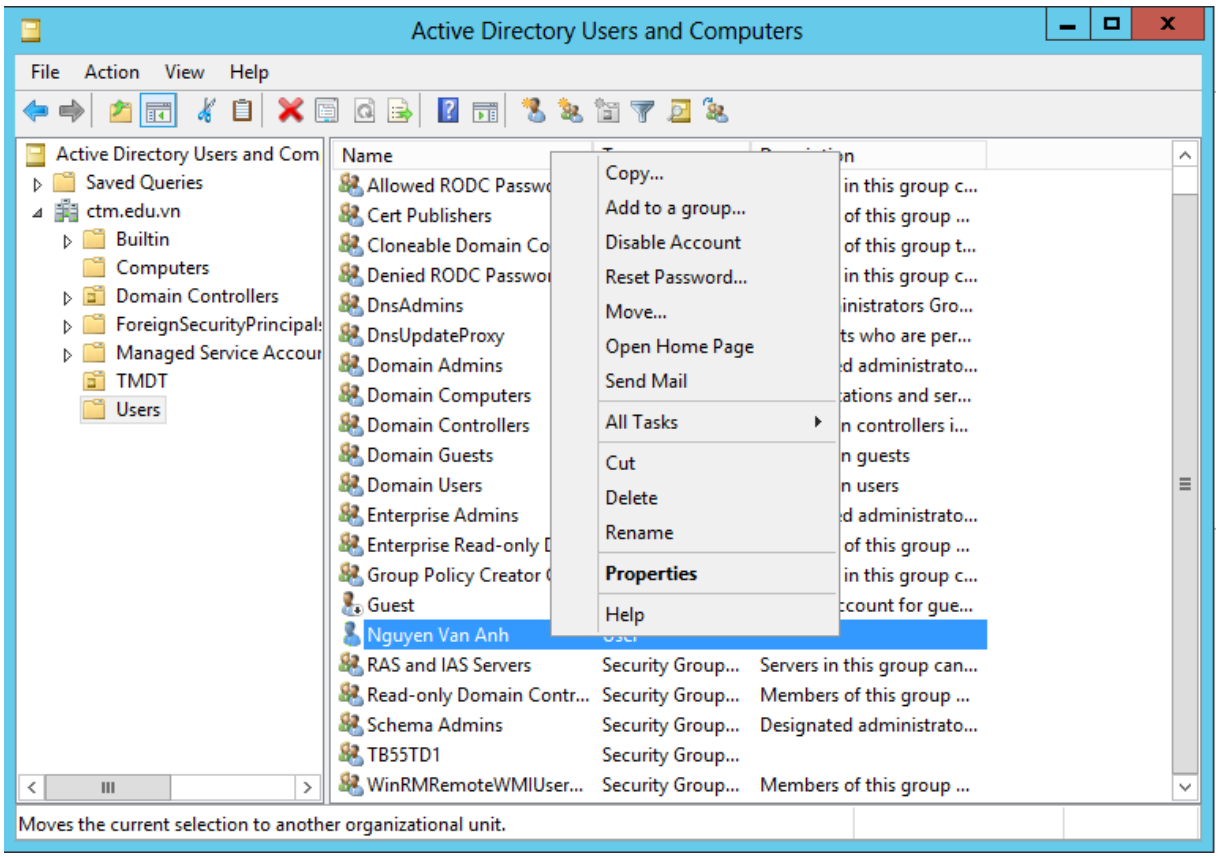


Tại cửa sổ ***New Object – Organizational Unit*** , nhập tên OU. Click ***OK.***

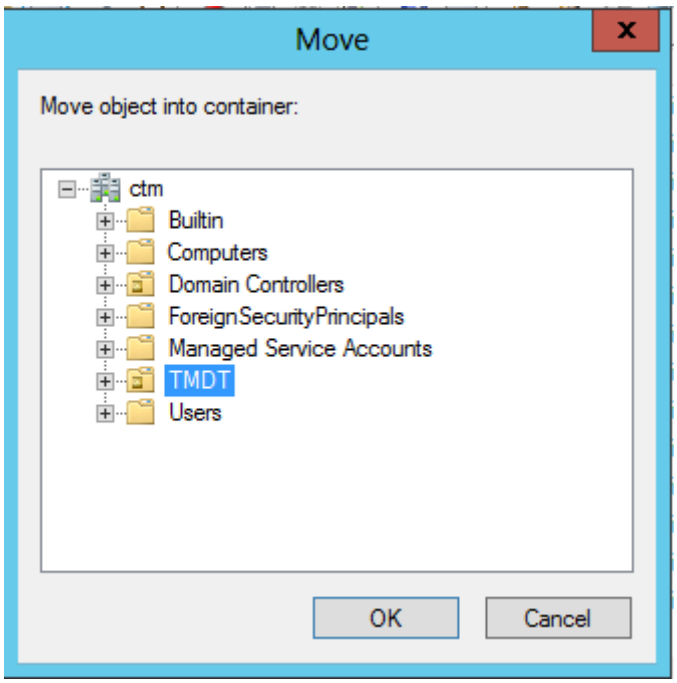


- Thêm người dùng (User) vào OU:

Click chuột phải vào tên của người dùng chọn ***Move***

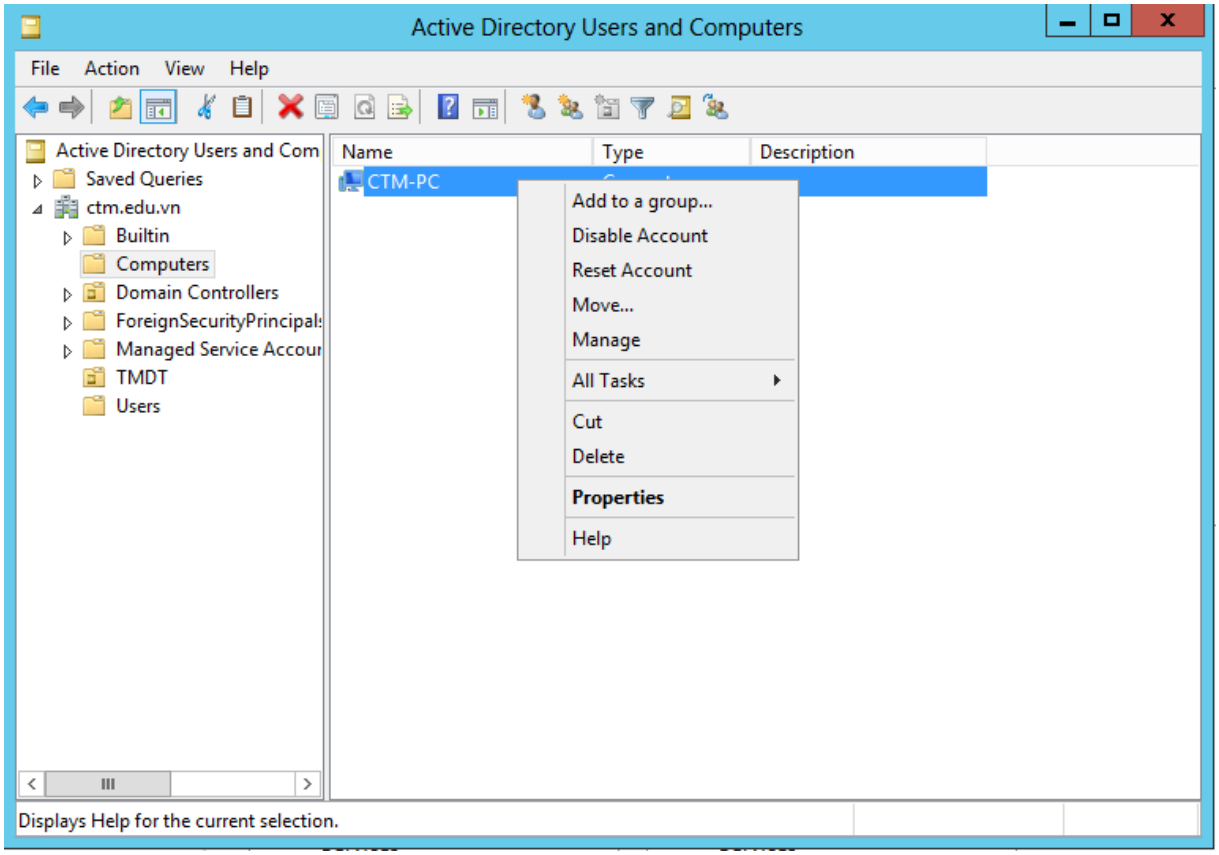


Chọn OU và click ***OK***

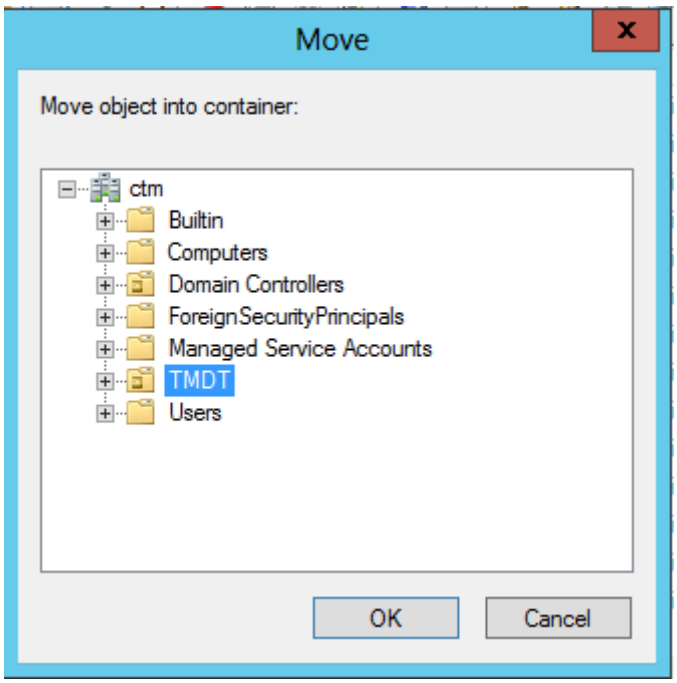


- Thêm máy tính (Computer) vào OU:

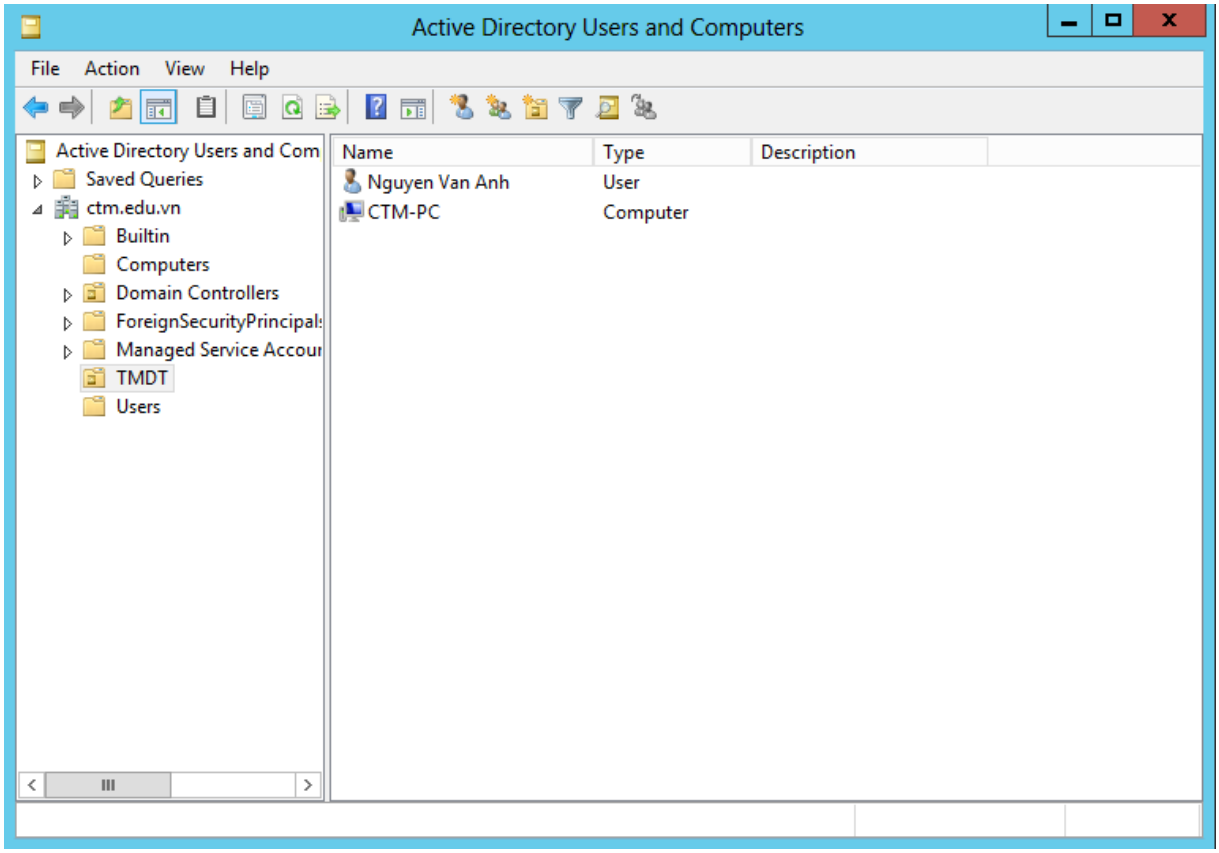
Click chuột phải vào tên máy tính chọn ***Move***



Chọn OU và click ***OK***



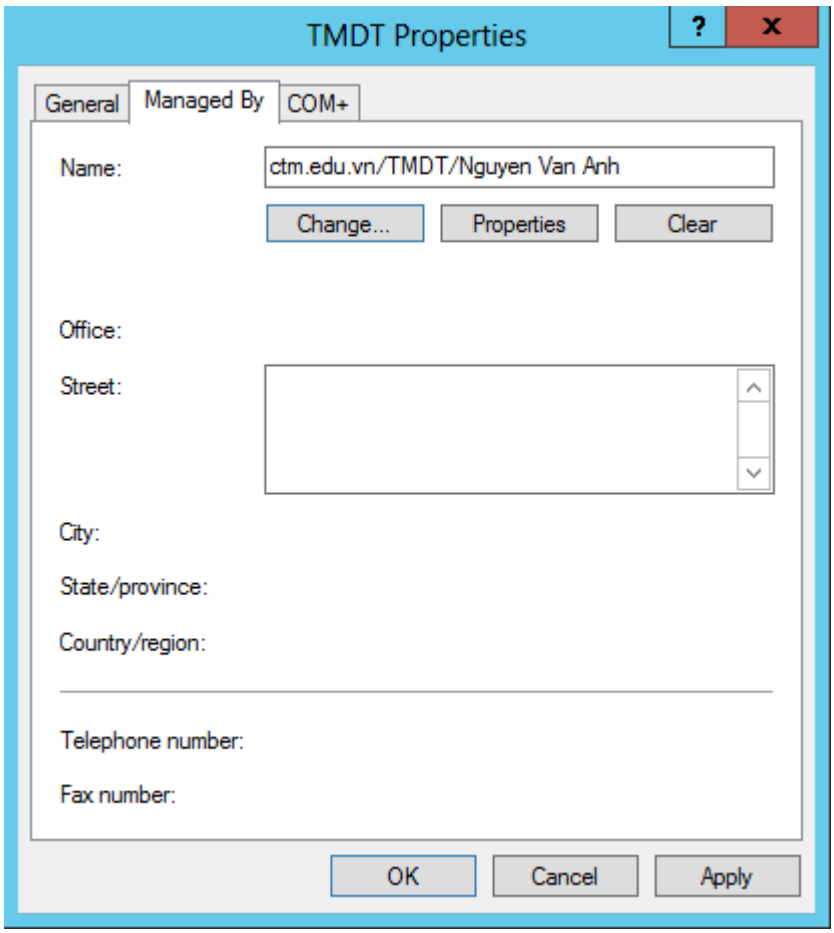
Kết quả khi thêm người dùng (User) và máy tính (Computer) vào OU



- Chỉ ra người/nhóm người sẽ quản lý OU:

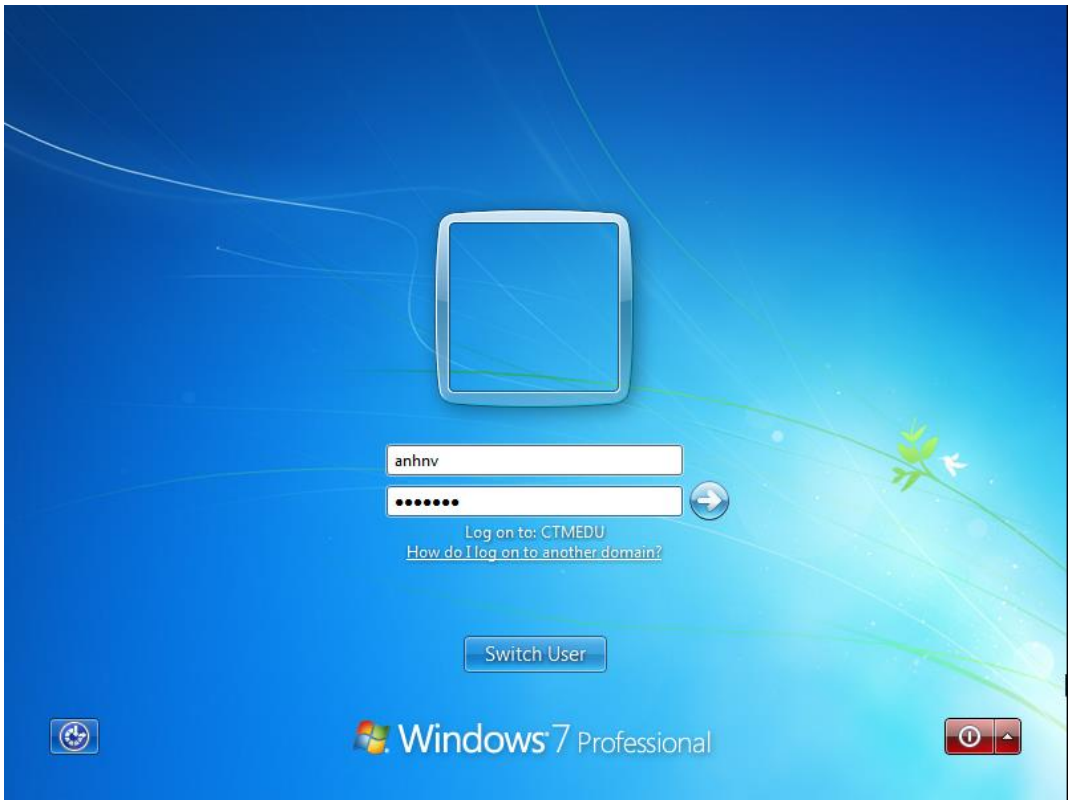
Click chuột phải vào OU, chọn ***Properties***

Trên hộp thoại ***OU Properties*** chọn ***Tab Managed By***, click chuột vào nút ***Change*** để chọn người dùng quản lý OU

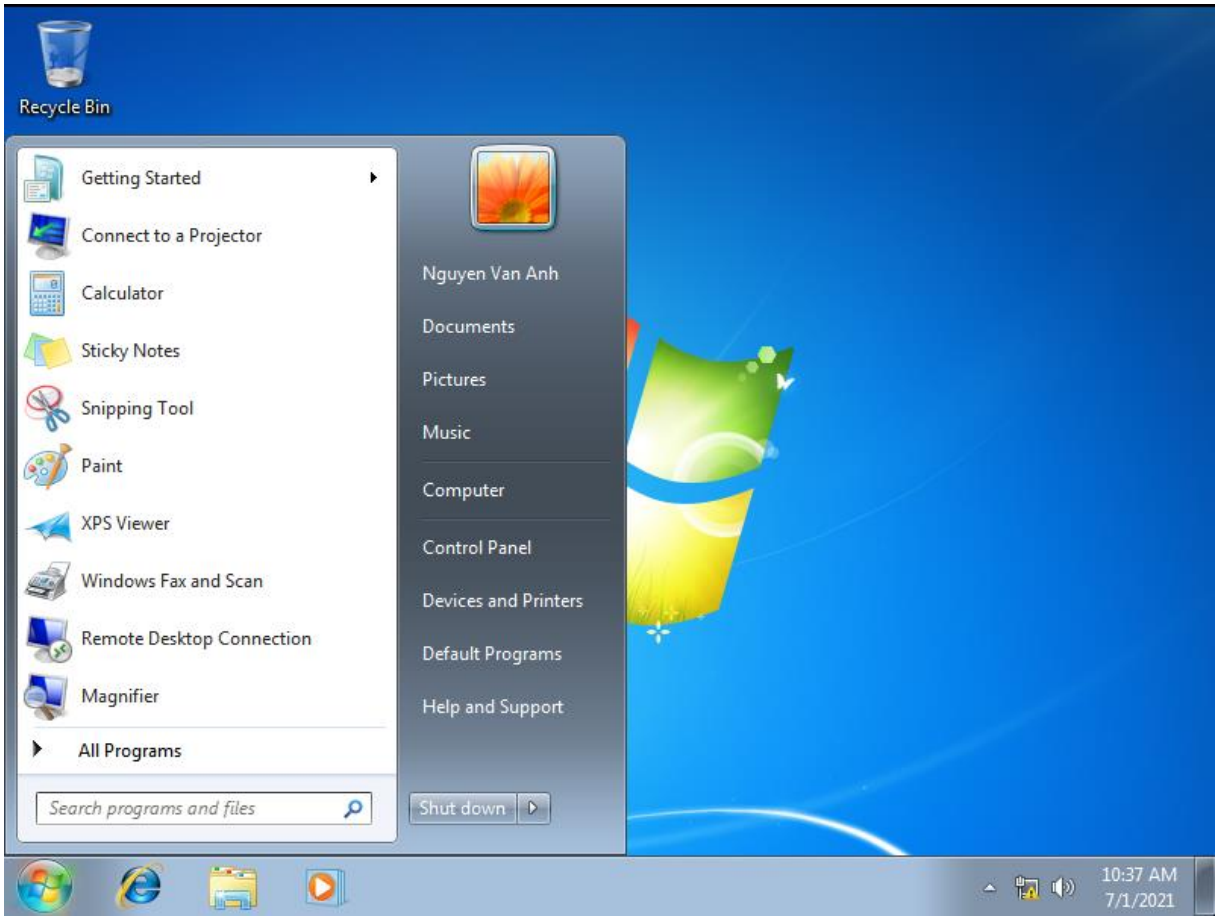


Bước 4: Chuyển qua máy Client, kiểm tra đăng nhập tài khoản User

Trên máy trạm CTM-WRK07, tiến hành đăng nhập vào Domain bằng tài khoản đã tạo



Đăng nhập thành công



III. Sai hỏng và cách khắc phục

1. Tạo tài khoản User không thành công

- Nguyên nhân

- Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Bước thiết lập mật khẩu cho tài khoản User phải theo quy tắc

- Cách khắc phục

- Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
- Đặt mật khẩu người dùng quản trị cho máy chủ

2. Gia nhập vào miền (domain) không thành công

- Nguyên nhân

- Thiết lập địa chỉ IP trên máy CTM-WRK07 chưa đúng
- Nhập tài khoản quản trị trên máy chủ chưa đúng

- Cách khắc phục

- Cài đặt lại địa chỉ IP trên máy CTM-WRK07
- Nhập đúng tài khoản quản trị trên máy chủ

V. Hướng dẫn ôn luyện

- Tạo thêm các tài khoản người dùng (User)
- Tạo thêm các nhóm người dùng (Group)
- Tạo mới các tổ chức (OU)

BÀI 4: TRIỂN KHAI CHÍNH SÁCH GROUP POLICY

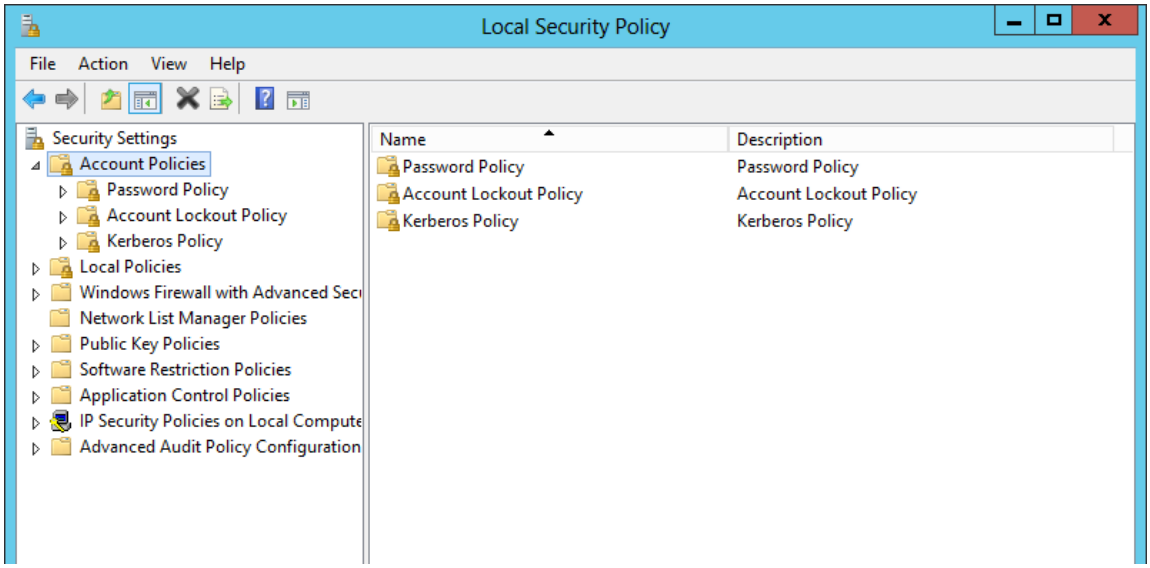
I. Lý thuyết liên quan

1. Chính sách hệ thống (System Policy)

a) Chính sách tài khoản người dùng Account policies

Account policy: được dùng để chỉ định các thông số về tài khoản người dùng khi tiến trình logon xảy ra nhằm giảm thiểu các mối đe dọa tới tài khoản.

Cấu hình: ***Server Manager / Tools / Local Security Policy***



Hình 2.4.1 – Chính sách người dùng Account Policies

- Chính sách mật khẩu (Password Policy)

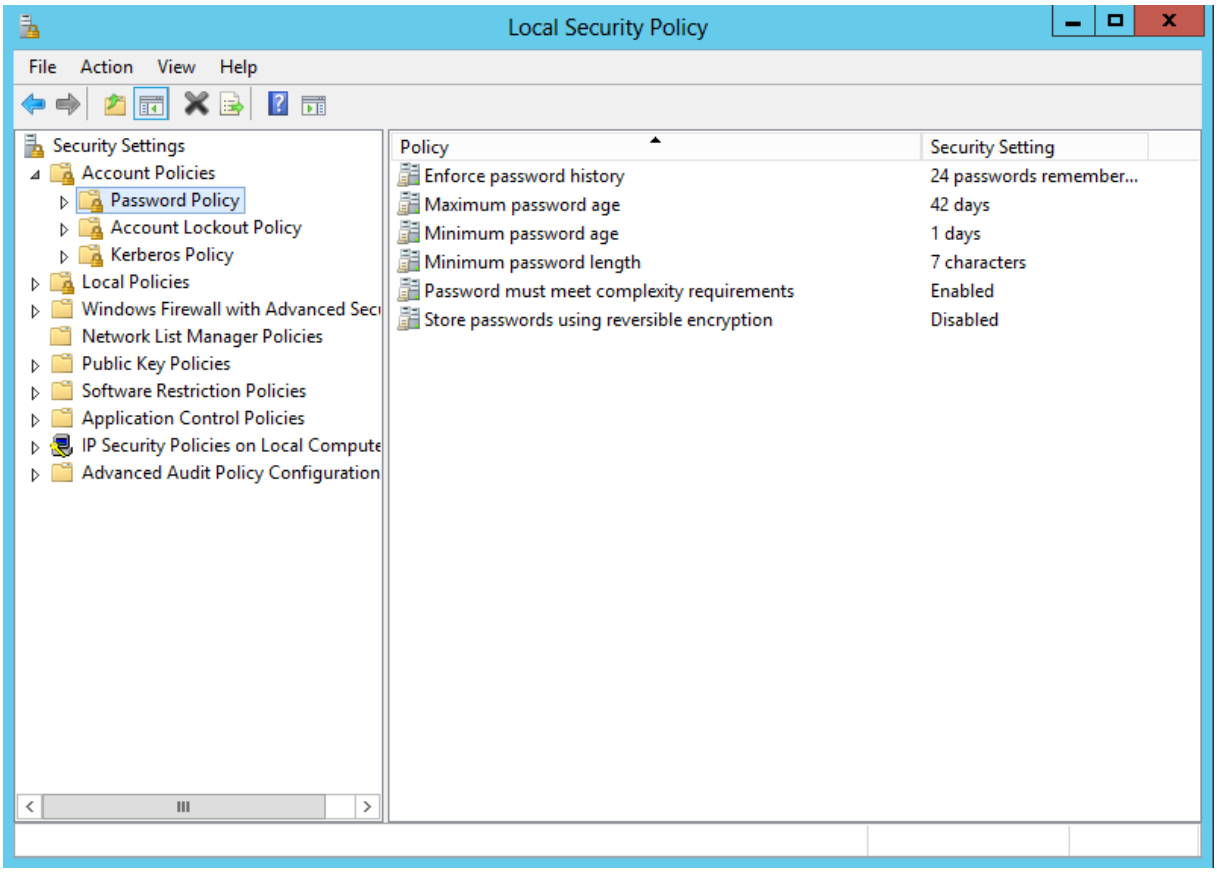
+ Đảm bảo an toàn cho mật khẩu cho tài khoản người dùng.

+ Cho phép qui định chiều dài ngắn nhất của mật khẩu, độ phức tạp của mật khẩu…

+ Các lựa chọn mặc định trong chính sách mật khẩu:

Chính sách	Mô tả	Mặc định
Enforce Password History	Số lần đặt mật mã không được trùng nhau	24
Maximum Password Age	Quy định số ngày nhiều nhất mà mật mã người dùng có hiệu lực	42
Minimum Password Age	Quy định số ngày tối thiểu trước khi người dùng có thể thay đổi mật mã	1
Minimum Password Length	Chiều dài ngắn nhất của mật mã	7
Password must meet complexity requirements	Mật khẩu phải có độ phức tạp như: có ký tự hoa, thường, ký tự số	Cho phép

Store password using reversible encryption for all users in the Domain	Mật mã người dùng được lưu dưới dạng mã hóa	Không cho phép



Hình 2.4.2 – Chính sách mật khẩu Password Policies

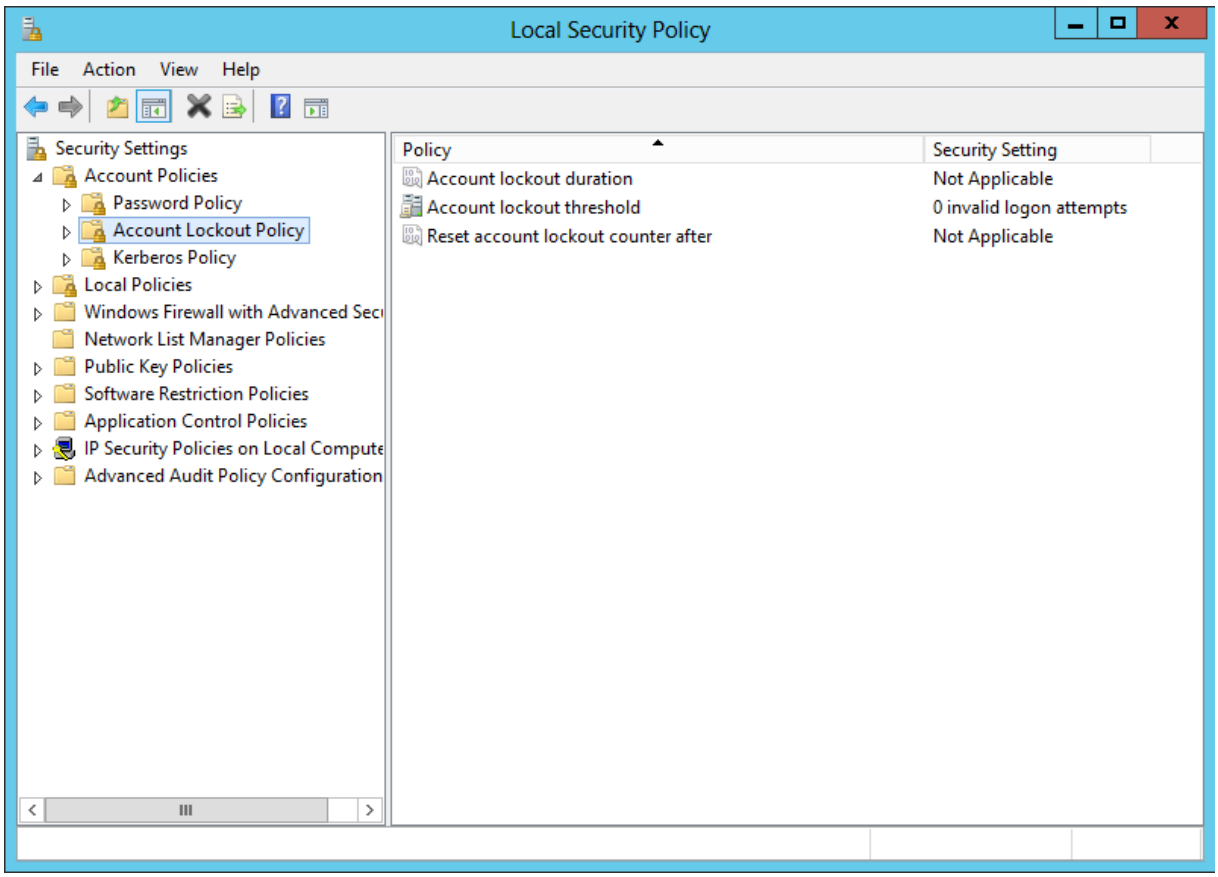
- Chính sách khóa tài khoản – Account Lockout Policy

+ Định cách thức và thời điểm khóa tài khoản

+ Hạn chế tấn công thông qua hình thức logon từ xa.

+ Các thông số cấu hình chính sách khóa tài khoản:

Chính sách	Mô tả	Mặc định
Account kockout duration	Quy định thời gian khóa tài khoản	0
Account kockout threshold	Quy định số lần cố gắng đăng nhập trước khi tài khoản bị khóa	0
Reset Account kockout counter after	Quy định thời gian đếm lại số lần đăng nhập không thành công	0

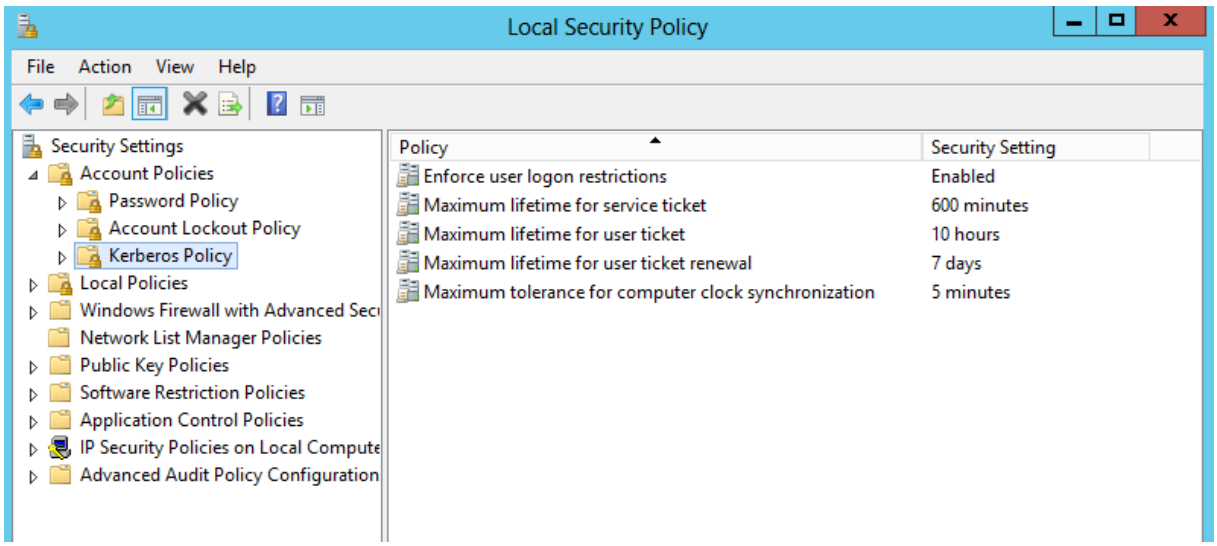


Hình 2.4.3 – Chính sách khóa tài khoản Account Lockout Policy

- Chính sách Kerberos – Kerberos Policy

+ Là một nhóm các chính sách bảo mật domain

+ Chỉ được dùng ở cấp độ domain



Hình 2.4.4 – Chính sách Kerberos Policy

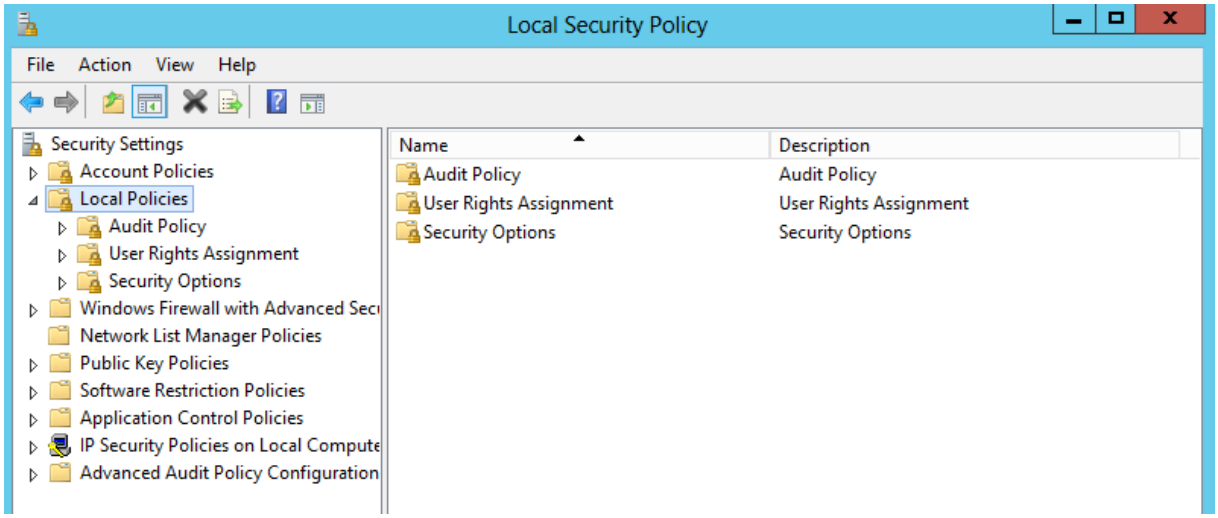
b) Chính sách cục bộ Local Policies

Local Policies cho phép thiết lập các chính sách giám sát các đối tượng (người dùng, tài nguyên dùng chung)

Cấp quyền hệ thống cho các người dùng và thiết lập các lựa chọn bảo mật.

Chính sách cục bộ gồm có:

- Chính sách kiểm toán
- Quyền hệ thống của người dùng
- Các lựa chọn bảo mật



Hình 2.4.5 – Chính sách cục bộ Local Policies

- Chính sách kiểm toán (Audit Policy)

+ Giám sát và ghi nhận các sự kiện xảy ra trong hệ thống, trên các đối tượng và các người dùng.

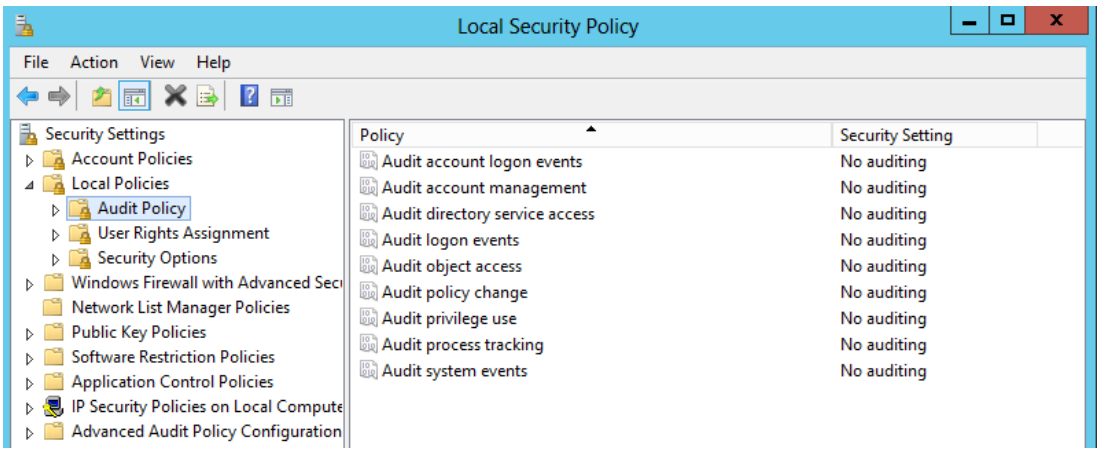
+ Các sự kiện an ninh này sẽ được gửi cho người quản trị mạng

+ Thiết lập 1 audit policy để:

- Theo dõi sự thành công hay thất bại của sự kiện
- Giảm thiểu sử dụng trái phép các nguồn tài nguyên
- Duy trì hồ sơ về hoạt động

+ Security events được lưu trong security logs.

+ Xem các ghi nhận này thông qua công cụ Event Viewer



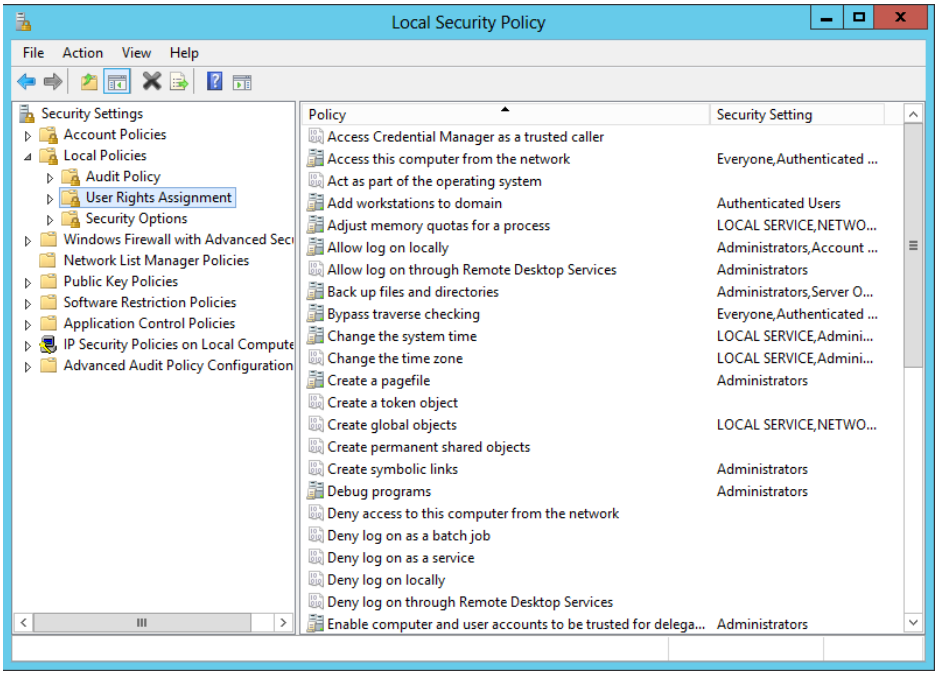
Hình 2.4.6 – Chính sách kiểm toán Audit Policy

- Quyền hệ thống của người dùng (User Rights Asignment)

+ Cách cấp quyền hệ thống cho người dùng:

- Gia nhập tài khoản người dùng vào các nhóm tạo sẵn (built-in) để kế thừa quyền (Phần User and Group)
- Dùng công cụ User Rights Assignment để gán từng quyền rời rạc cho người dùng.

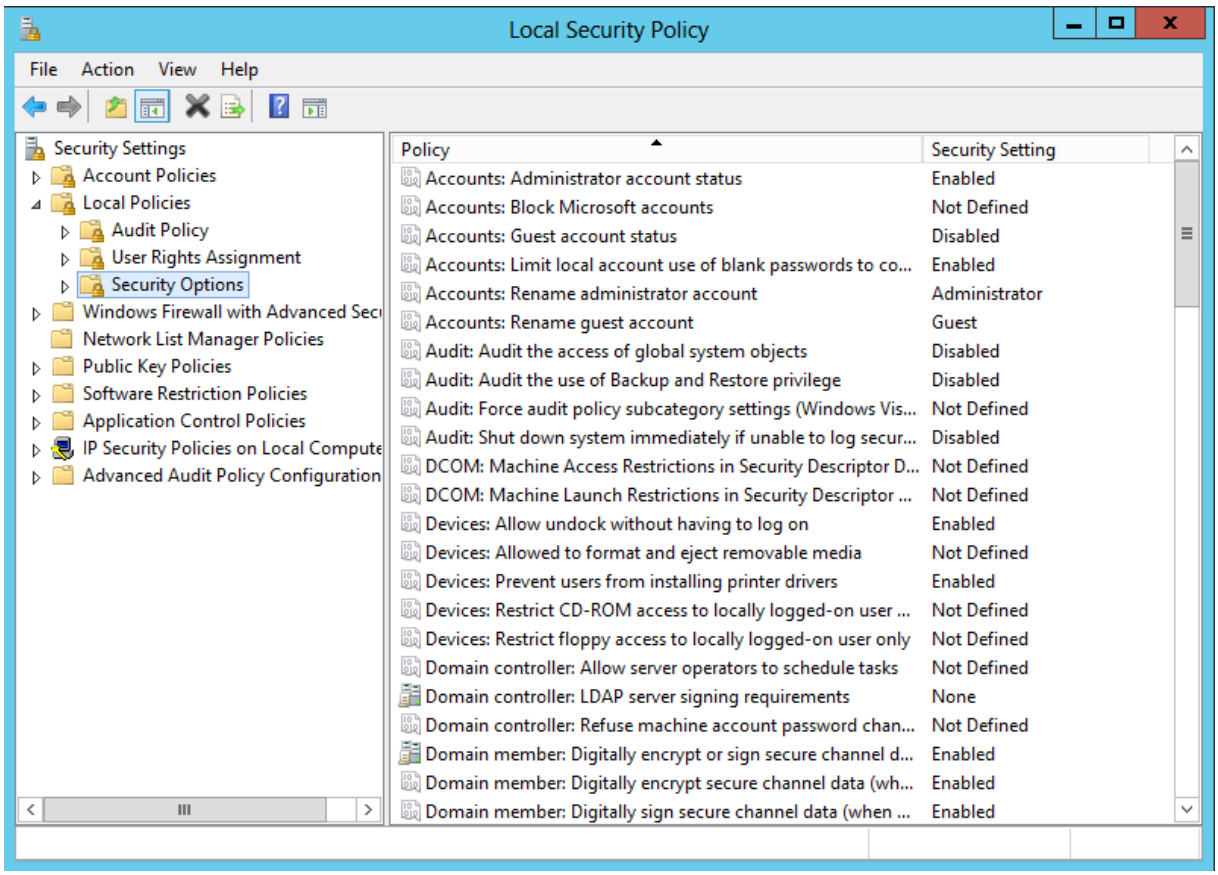
+ Thêm/ bớt quyền người dùng



Hình 2.4.7 – Quyền hệ thống của người dùng

- Các lựa chọn bảo mật - Security Options

Cho phép khai báo thêm các thông số nhằm tăng tính bảo mật cho hệ thống như: không cho phép hiển thị người dùng đã logon trước đó hay đổi tên tài khoản người dùng tạo sẵn (administrator, guest).



Hình 2.4.8 – Các lựa chọn bảo mật

2. Chính sách nhóm (Group Policy - GP)

a) Định nghĩa

Là tập hợp các thông tin cấu hình (configuration settings) tác động trên một hoặc nhiều đối tượng (users, computers) trong Active Directory hoặc trên một hệ thống (local group policy)

Các thông tin cấu hình bao gồm:

+ Chính sách nhóm cho computers:

- Desktop
- Security
- Startup/shutdown scripts

+ Chính sách nhóm cho users:

- Desktop
- Security
- Logon/logoff scripts

b) Mục đích chính sách nhóm

Quản lý môi trường làm việc của user trong site, domain, organization unit hay trong từng hệ thống

Đơn giản hóa một số thao tác quản trị

Quản trị tập trung

c) Chức năng của Group Policy

Triển khai phần mềm ứng dụng

Gán các quyền hệ thống cho người dùng

Giới hạn những ứng dụng mà người dùng được phép thi hành

Kiểm soát các thiết lập hệ thống

Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy

Đơn giản hóa và hạn chế các chương trình

Hạn chế tổng quát màn hình Desktop của người dùng

d) Các loại chính sách nhóm

- Các thiết lập chính sách được lưu trên GPO (Group Policy Object, đối tượng chính sách nhóm)

- Có 2 dạng GPO

+ Local GPO: lưu trên từng máy

+ Non local GPO: lưu trên Active Directory

II. Trình tự thực hiện

1. Yêu cầu thực hiện

Triển khai chính sách nhóm trên domain *ctm.edu.vn*:

+ Đặt màn hình nền Desktop tất cả các máy tính.

+ Khóa Registry.

+ Khóa Task Manager.

+ Cấm DOS Command.

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

Sơ đồ địa chỉ IP như sau:

Thông số	*CTM-SRV12*	*CTM-WRK07*
IP Address	192.168.1.2	192.168.1.10
Subnet mask	255.255.255.0	255.255.255.0
Default gateway	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2

3. Các bước thực hiện

Thực hiện triển khai các chính sách nhóm trên domain *ctm.edu.vn* thông qua 3 bước sau:

- Đặt màn hình nền Desktop tất cả các máy tính

- Bước 1: Chia sẻ thư mục chứa background
- Bước 2: Tạo chính sách đặt màn hình nền Desktop trên OU
- Bước 3: Kiểm tra chính sách đã đặt trên máy client

- Khóa Registry
  - Bước 1: Tạo chính sách khóa Registry trên OU
  - Bước 2: Kiểm tra chính sách đã áp đặt trên máy client
- Khóa Task Manager
  - Bước 1: Tạo chính sách khóa Task Manager trên OU
  - Bước 2: Kiểm tra chính sách đã áp đặt trên máy client
- Cấm DOS Command
  - Bước 1: Tạo chính sách Cấm DOS Command trên OU
  - Bước 2: Kiểm tra chính sách đã áp đặt trên máy client

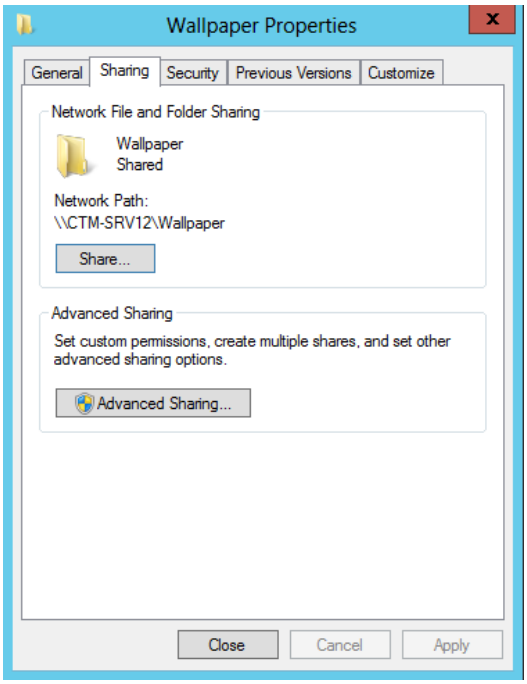
Hướng dẫn chi tiết

- Đặt màn hình nền Desktop tất cả các máy tính

Bước 1: Chia sẻ thư mục chứa background

Thực hiện trên máy CTM-SVR12.

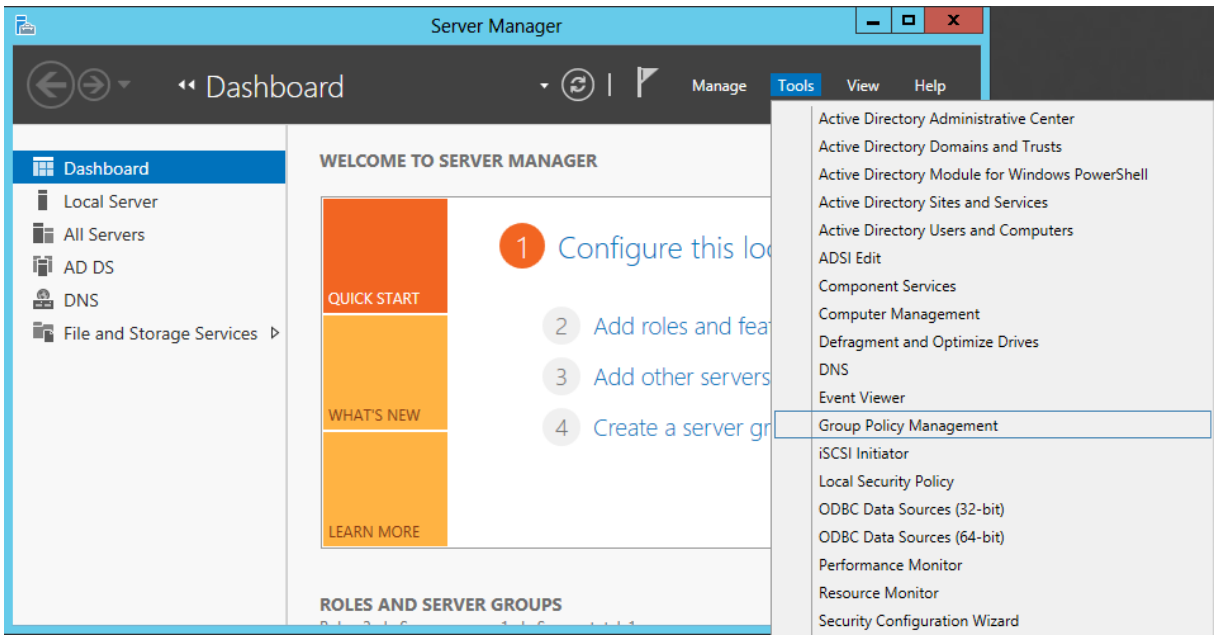
+ Tạo thư mục wallpaper trong ổ C (thư mục chứa background màn hình nền), tiến hành chia sẻ thư mục.



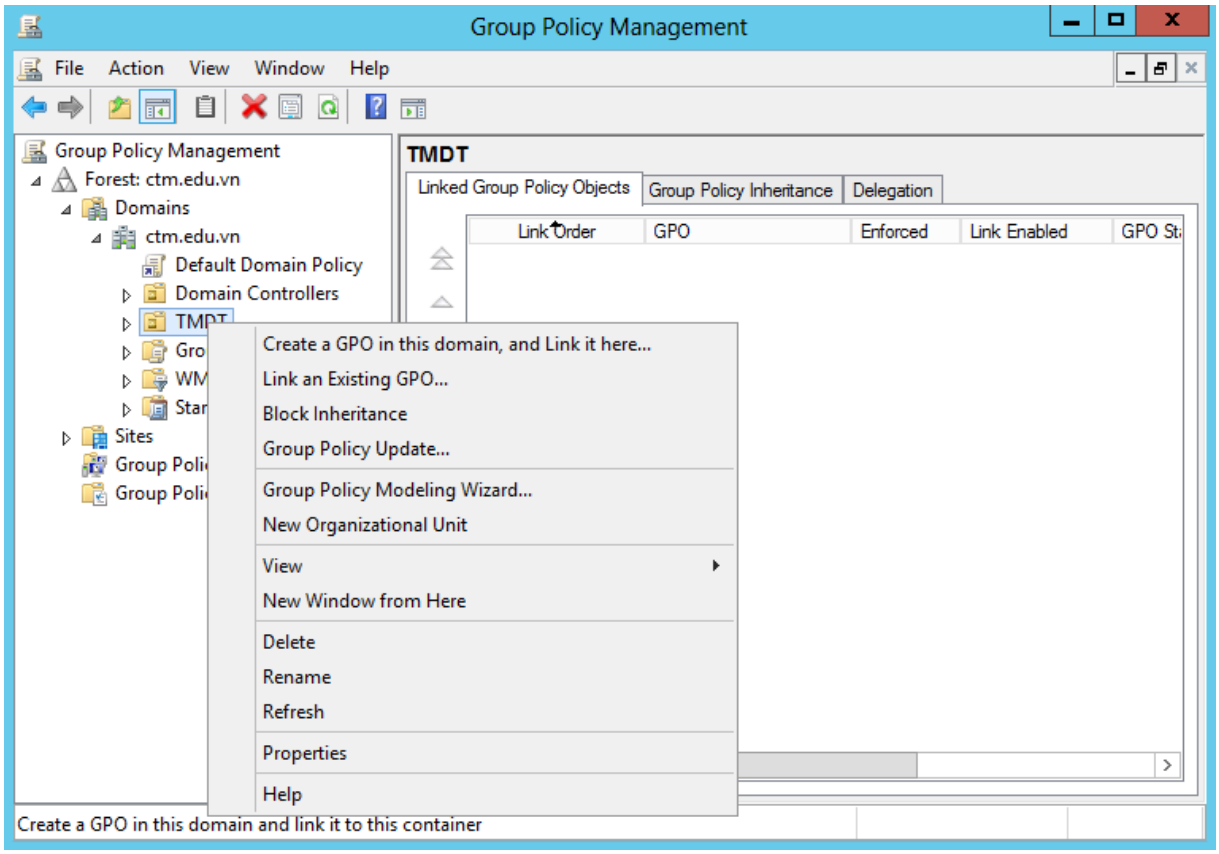
Bước 2: Tạo chính sách trên OU

Thực hiện trên máy CTM-SRV12.

Vào ***Server Manager / Tools / Group Policy Management***.

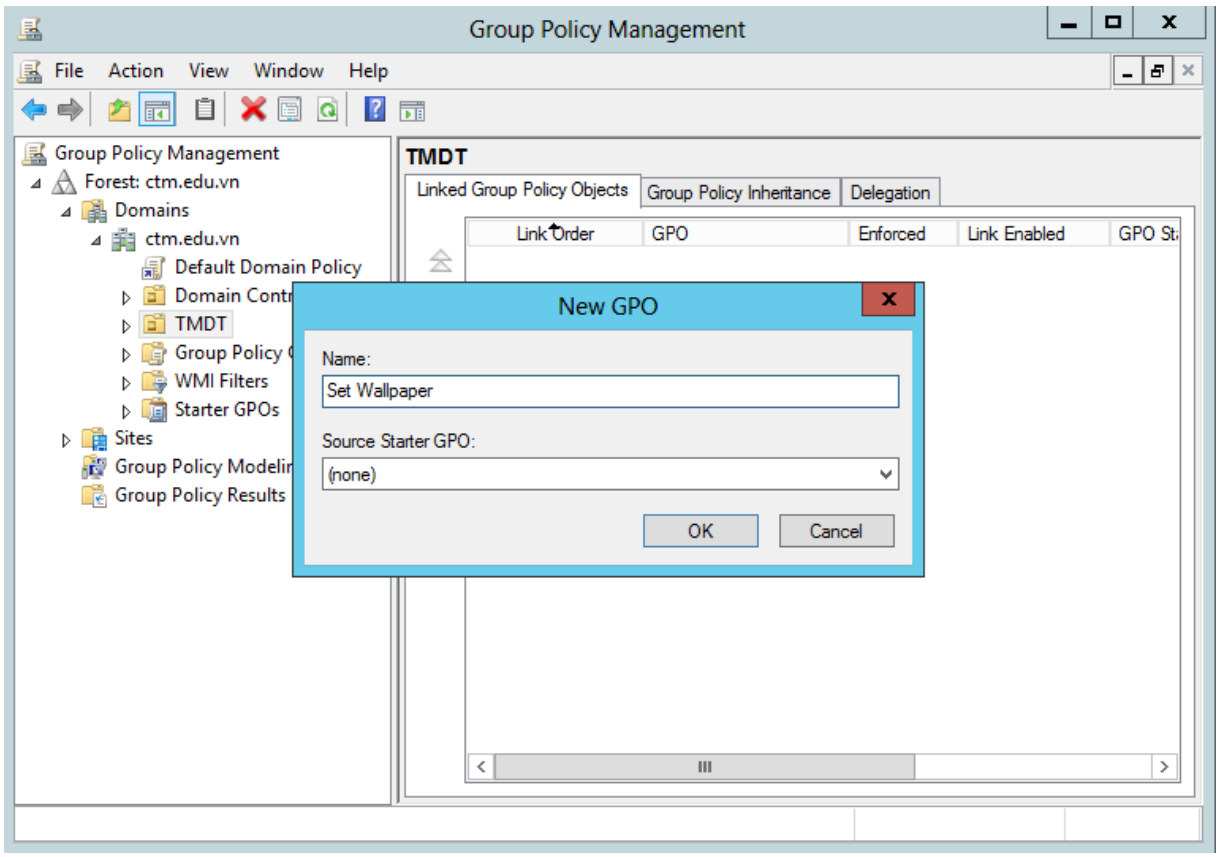


Tại cửa sổ ***Group Policy Management***, click chuột phải vào OU ***TMDT***, chọn ***Create a GPO in this domain, and Link it here…***

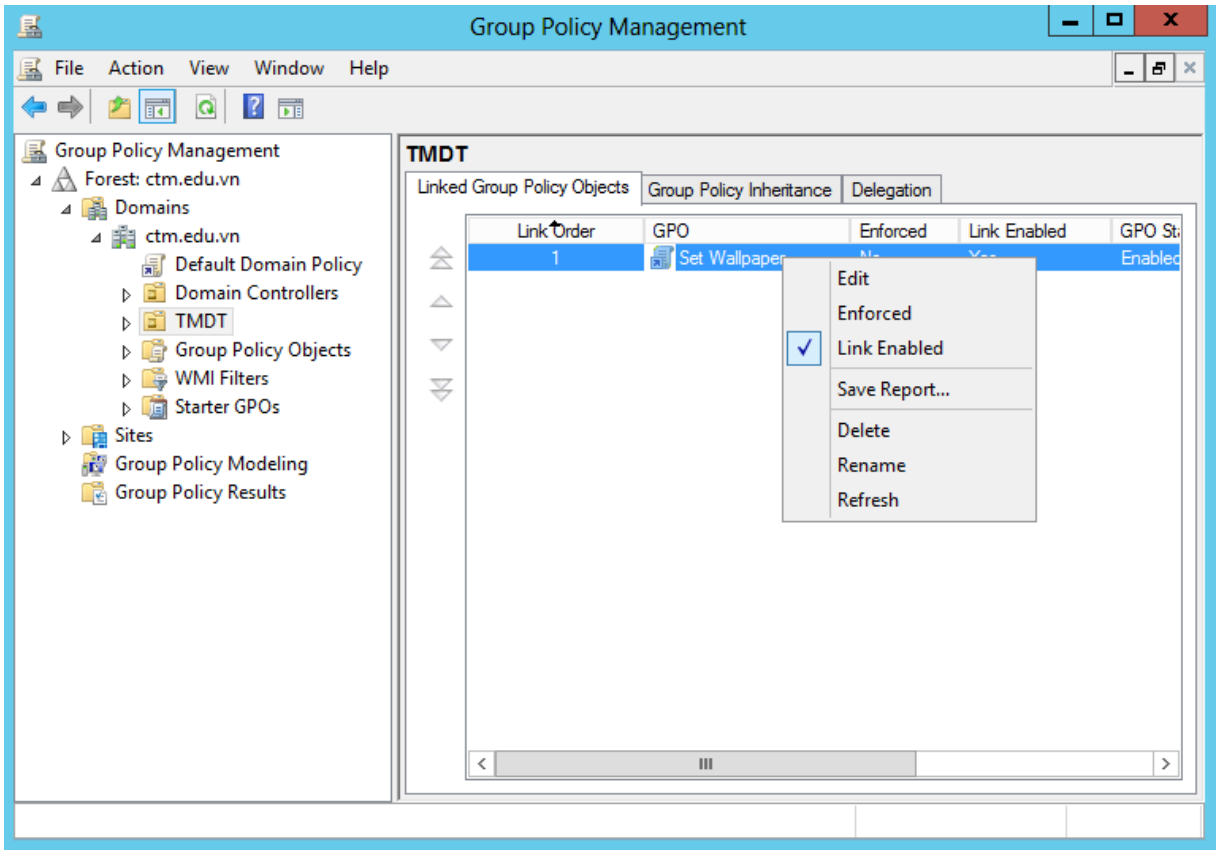


Tại cửa sổ ***New GPO***, nhập vào:

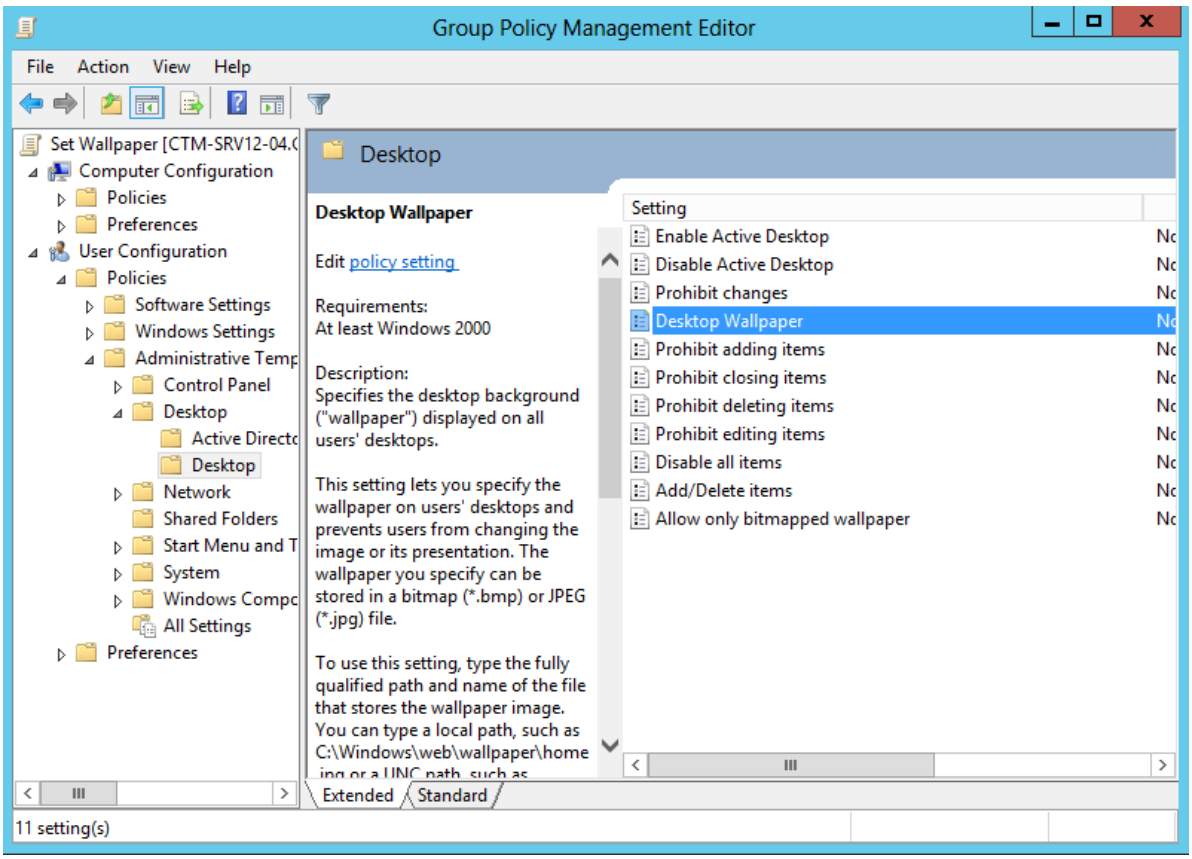
Name: ***Set Wallpaper***. Click ***OK.***



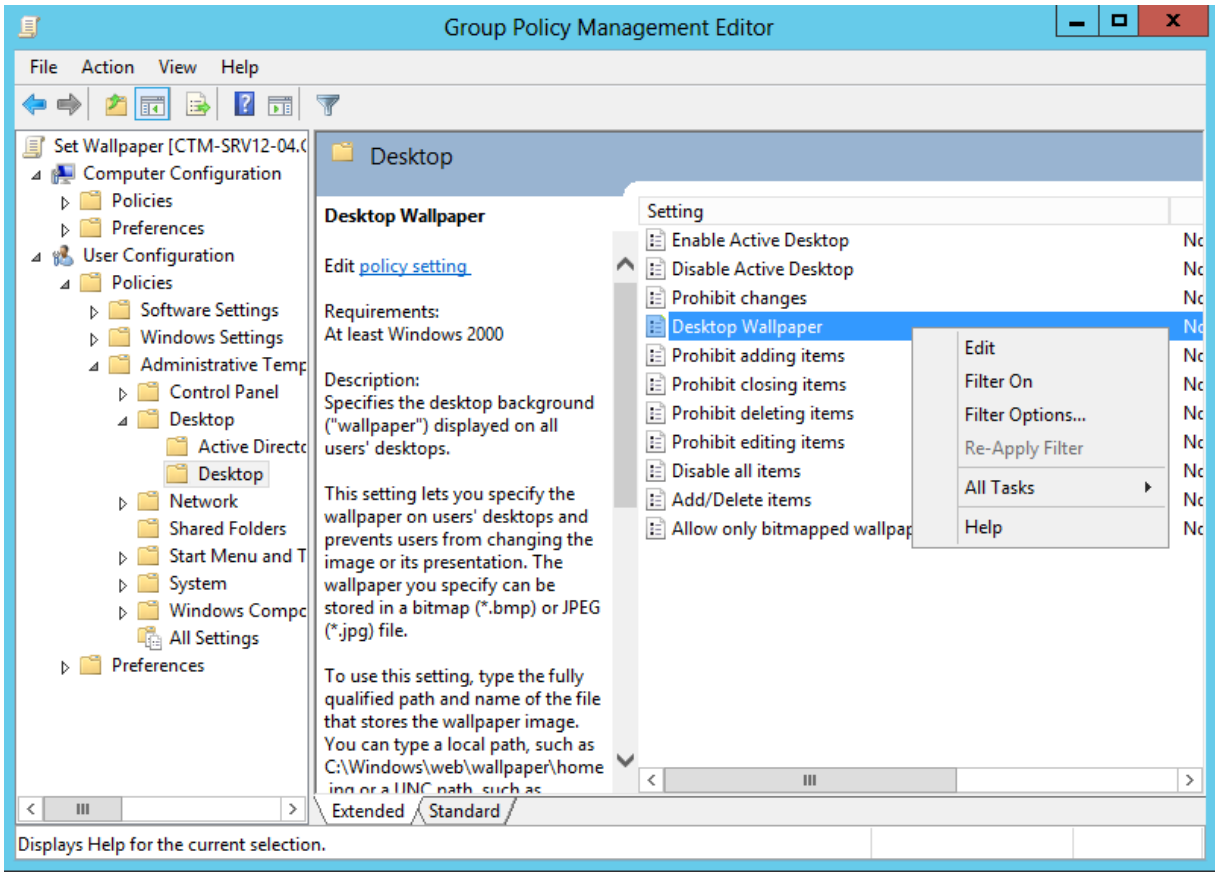
Click chuột phải tại chính sách ***Set Wallpaper*** vừa tạo, chọn ***Edit***



Tại cửa sổ ***Group Policy Management Editor***, click chọn vào ***User Configuration / Policies / Administrative Template.. / Desktop / Desktop***. Chọn vào ***Desktop Wallpaper***



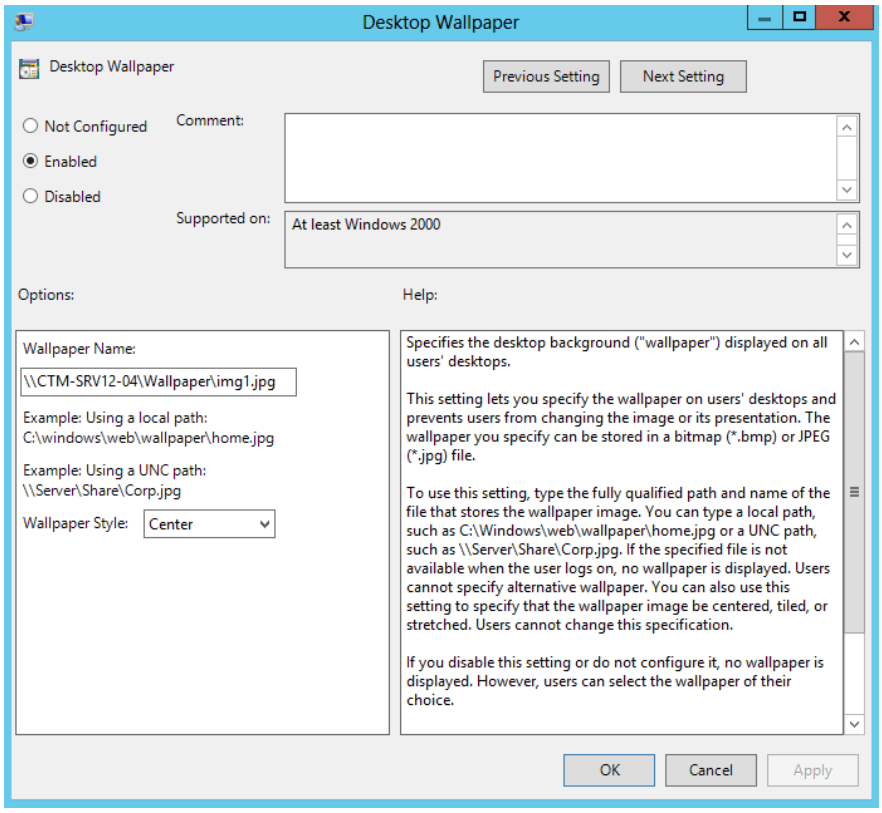
Click chuột phải vào ***Desktop Wallpaper***, chọn ***Edit***



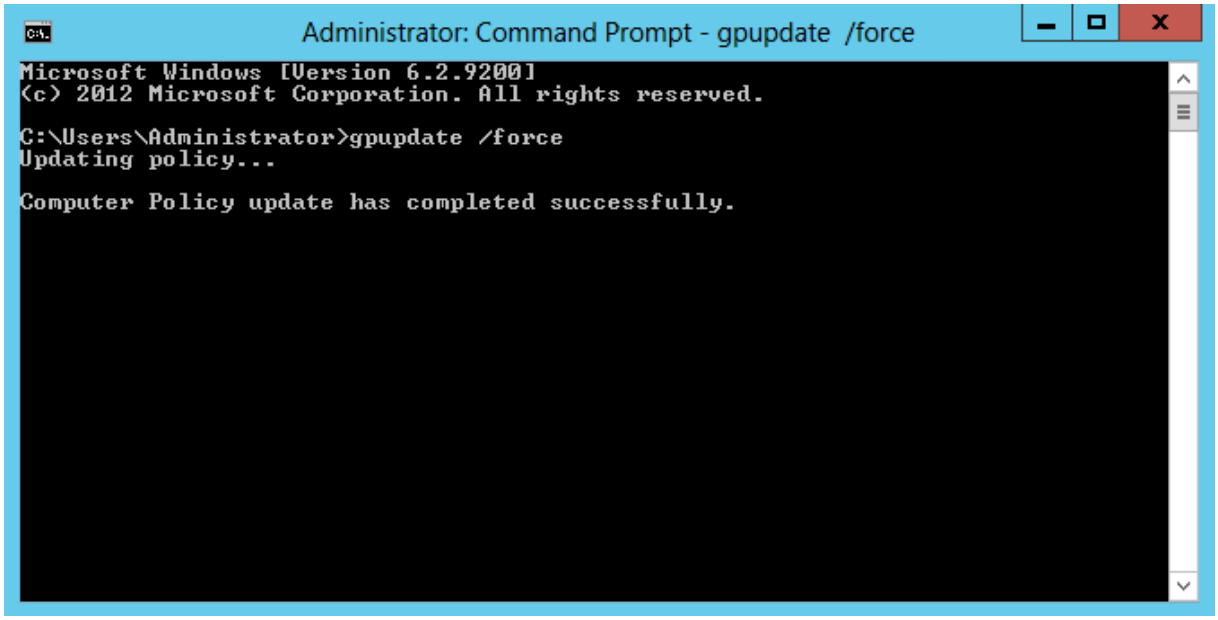
Tại cửa sổ ***Desktop Wallpaper***, click vào ***Enable***.

Tại ***Wallpaper Name***: đưa vào đường dẫn folder wallpaper vừa share ở trên.

Wallpaper Name: *\\192.168.1.2\wallpaper\abc.jpg*. Click ***Apply*** và ***OK***

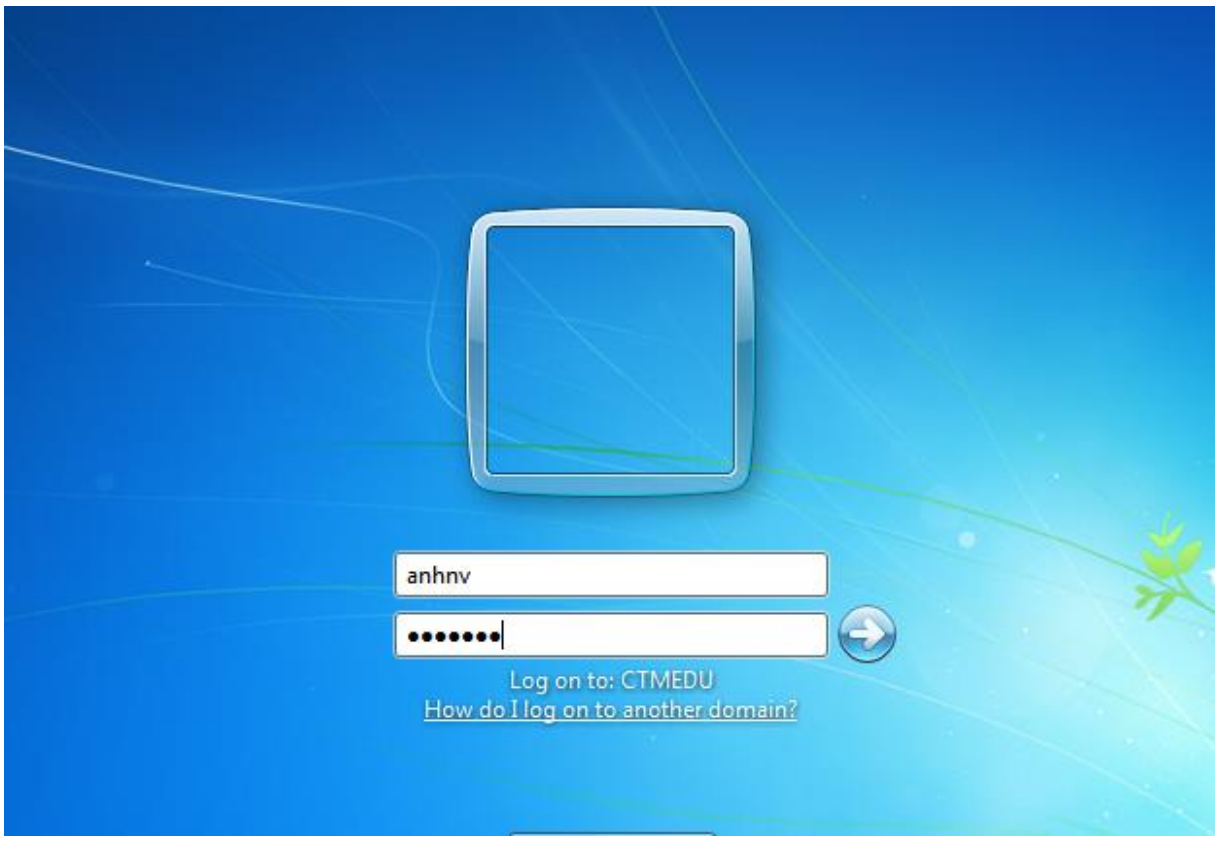


Cập nhật GPO: ***Cmd*** / gõ lệnh ***gpupdate /force***

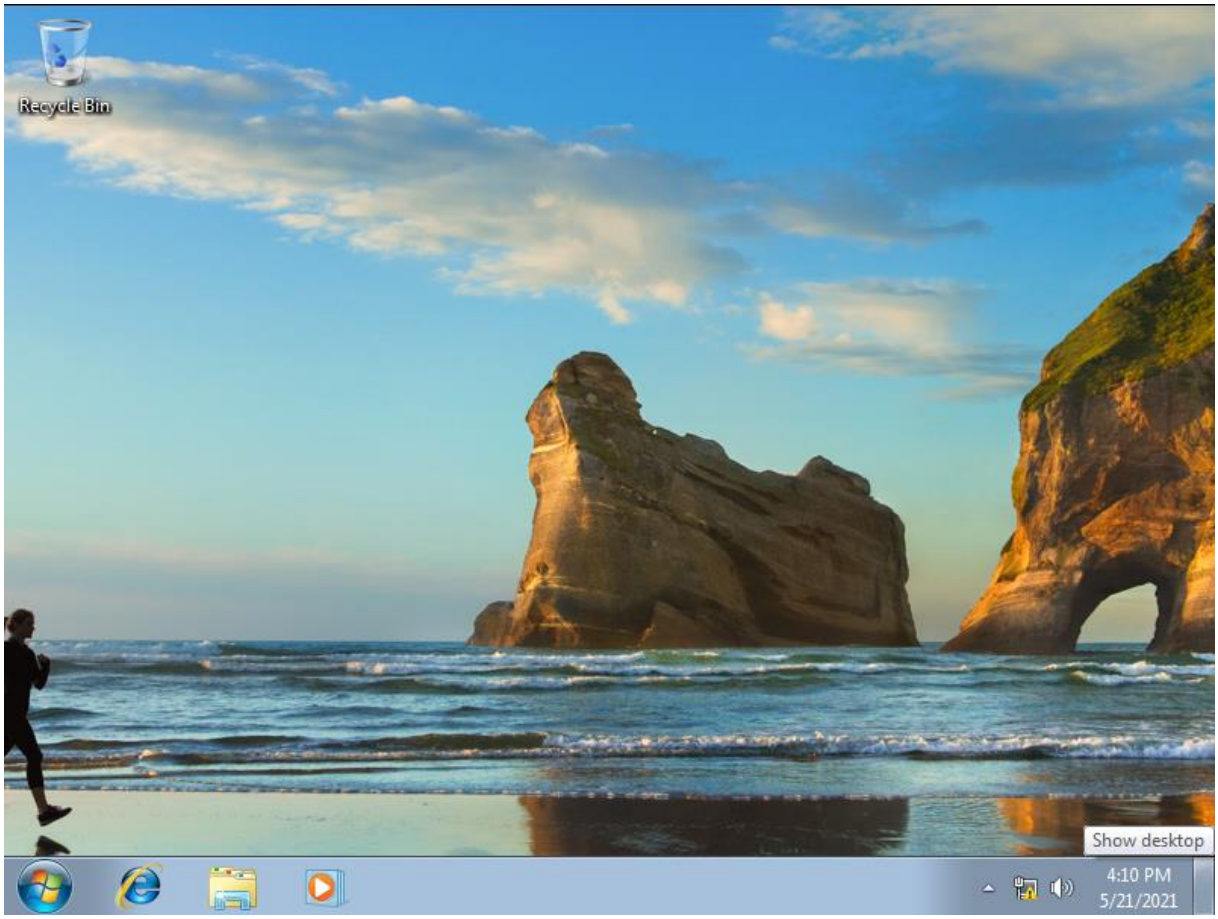


Bước 3: Kiểm tra chính sách đã đặt trên máy client

Chuyển sang máy Client CTM-WRK07, đăng nhập bằng tài khoản anhnv trong đơn vị TMDT để kiểm tra



Client đã cập nhật màn hình nền thành công



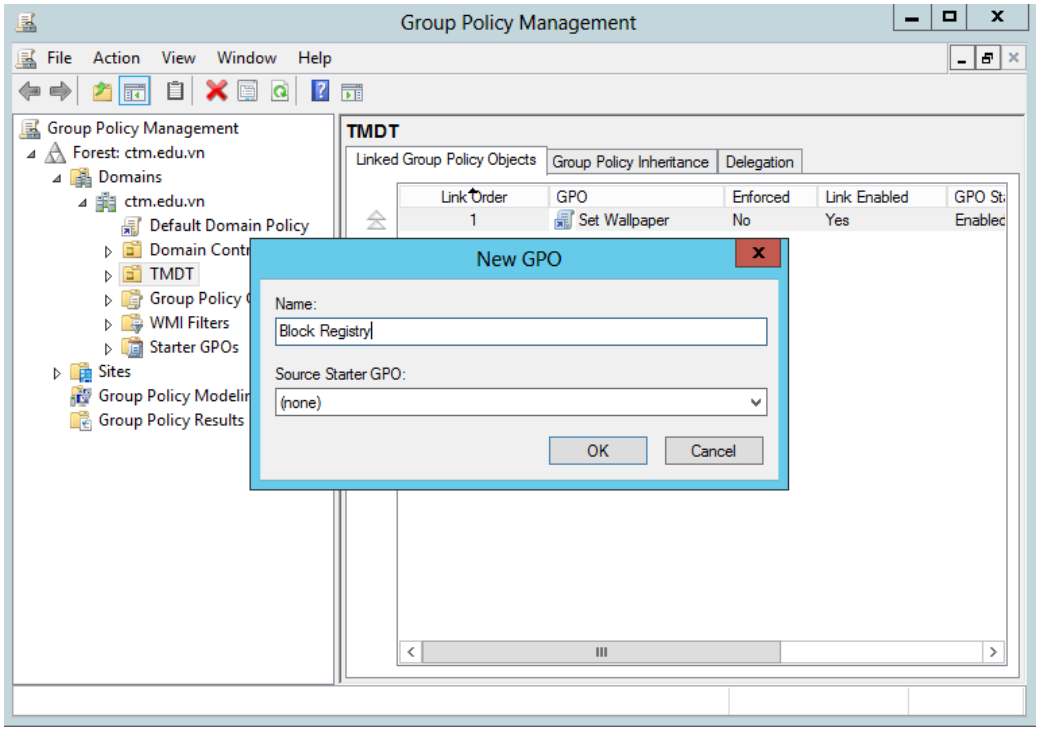
- Tạo chính sách khóa Registry

Bước 1: Tạo chính sách khóa Registry

Thực hiện trên máy CMT-SRV12.

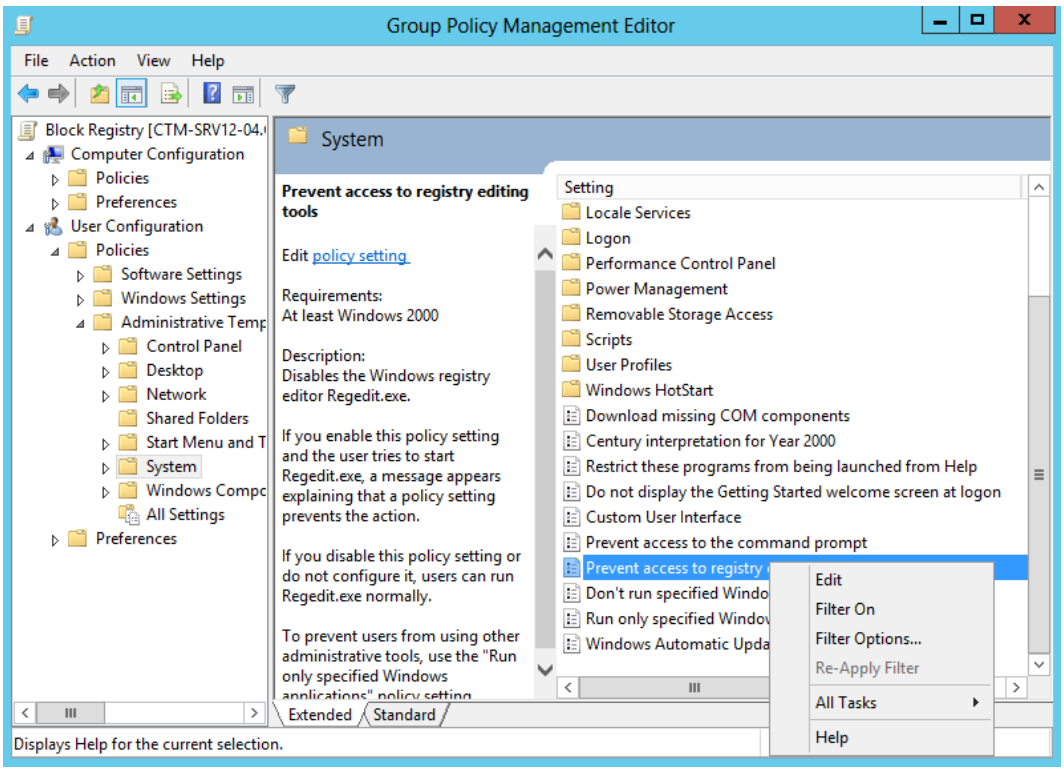
Click chuột phải tại OU ***TMDT***, chọn ***Create a GPO in this domain…***

Tại cửa sổ ***New GPO***, nhập vào tên ***Name***: *Block Registry*. Click ***OK***

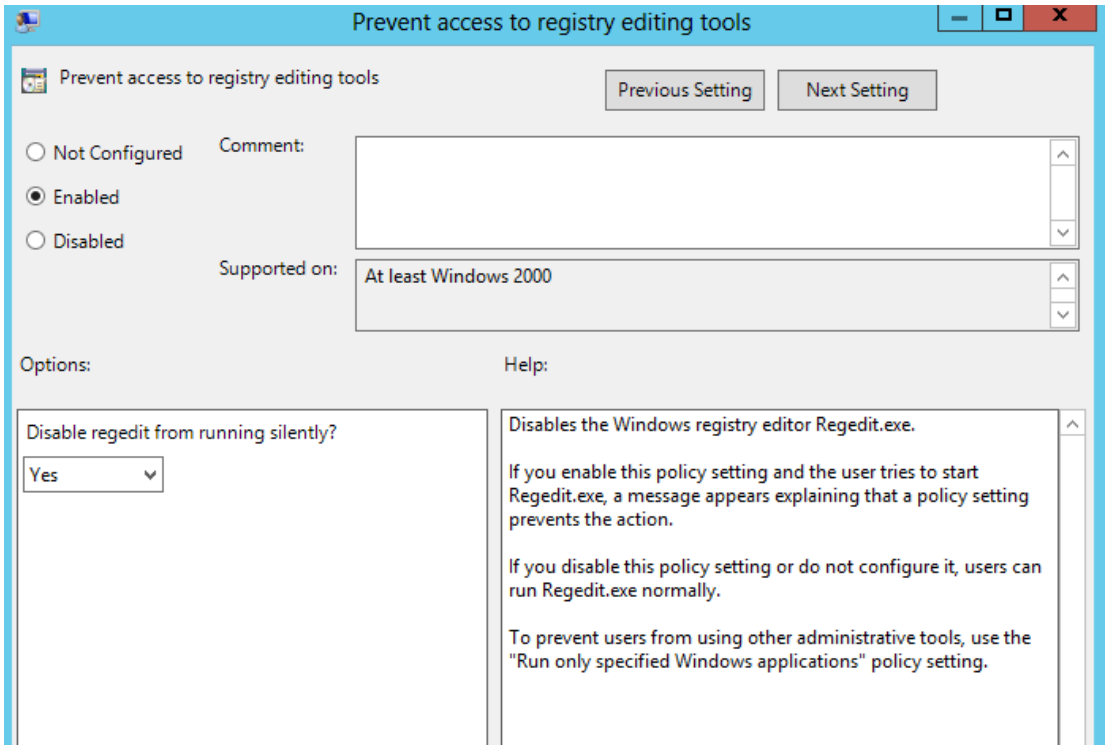


Click chuột phải vào chính sách ***Block Registry*** vừa tạo, chọn ***Edit***

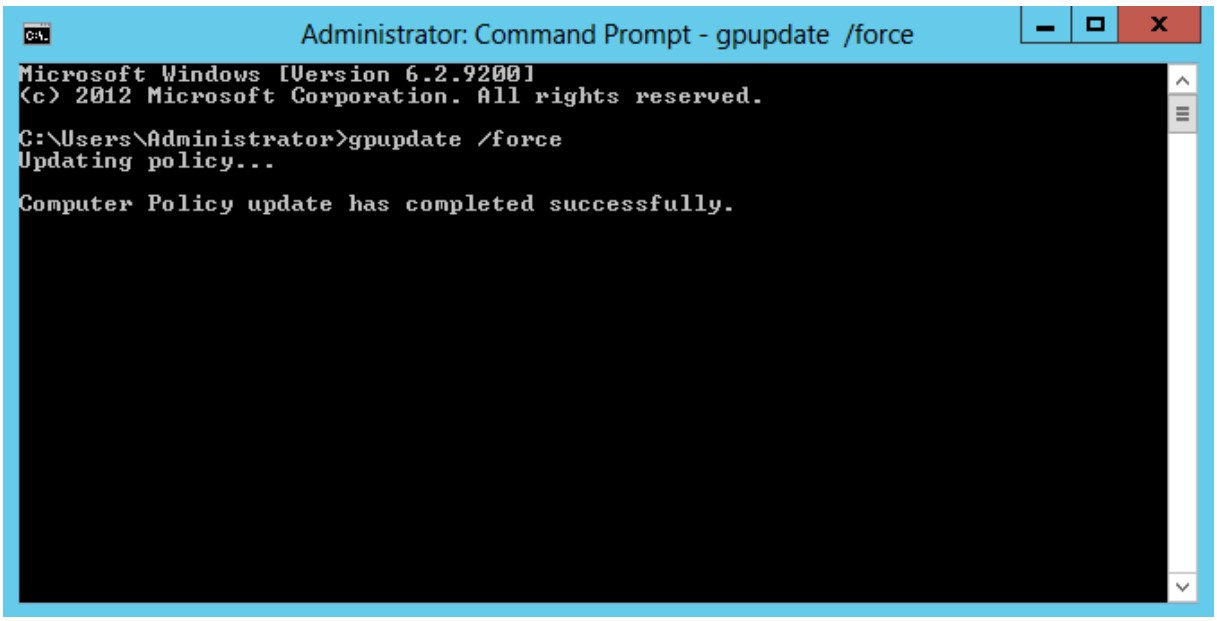
Tại cửa sổ ***Group Policy Managerment Editor***, chọn vào mục ***User Configuration / Policies / Administrative Templates .. / System*** ,chọn vào chính sách ***Prevent access to registry editing tools***., tại đây click chuột phải chọn ***Edit***.



Tại cửa sổ ***Prevent access to registry editing tools***, click chọn vào ***Enable, Apply, OK***

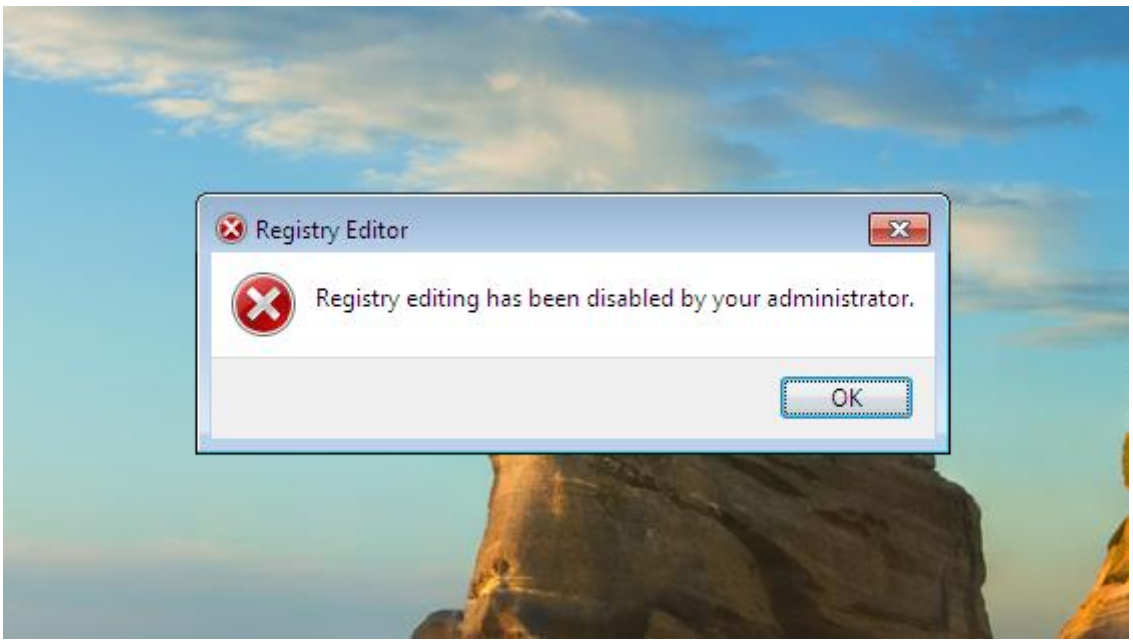


Cập nhật chính sách bằng lệnh ***gpupdate /force*** trong cmd



Bước 2: Kiểm tra chính sách đã áp đặt trên máy client

Chuyển sang máy Client CTM-WRK07, đăng nhập bằng tài khoản anhnv trong đơn vị TMDT để kiểm tra



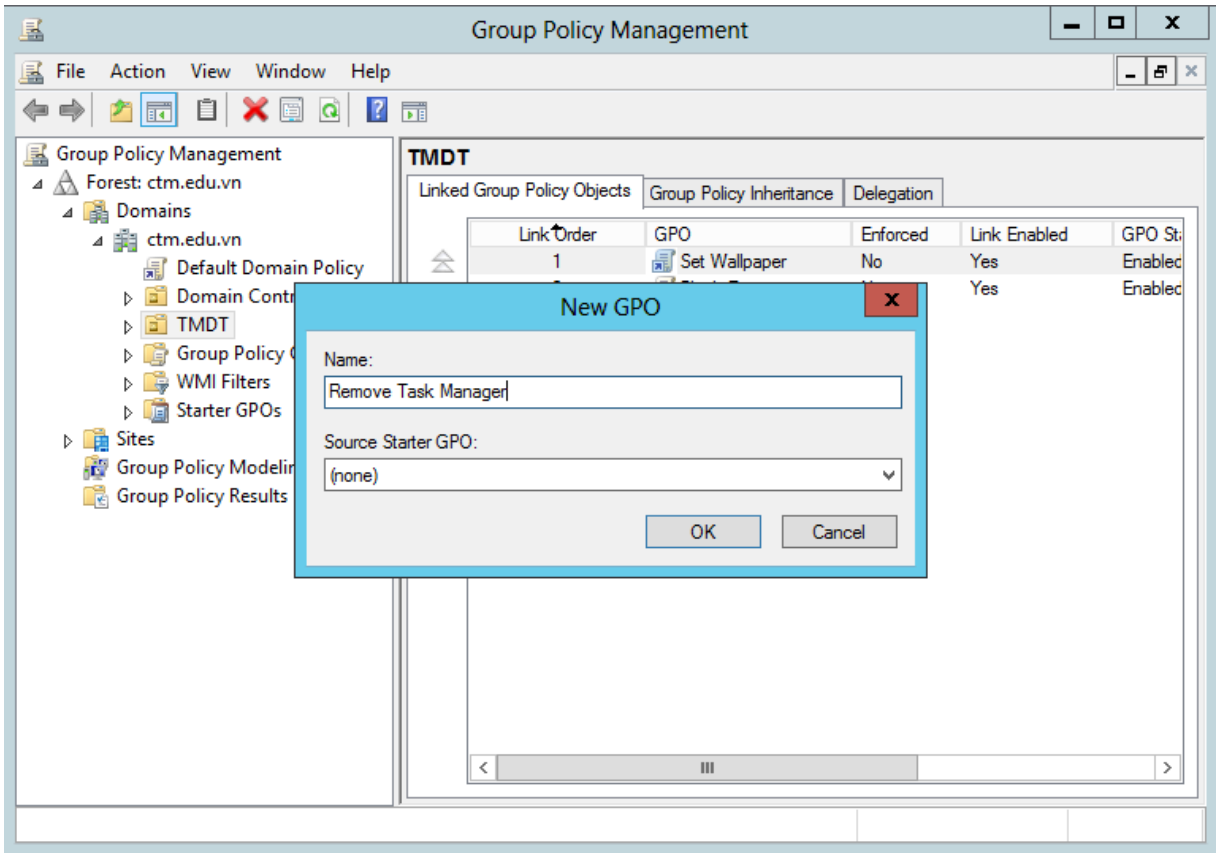
- Tạo chính sách khóa Task Manager

Bước 1: Tạo chính sách khóa Task Manager

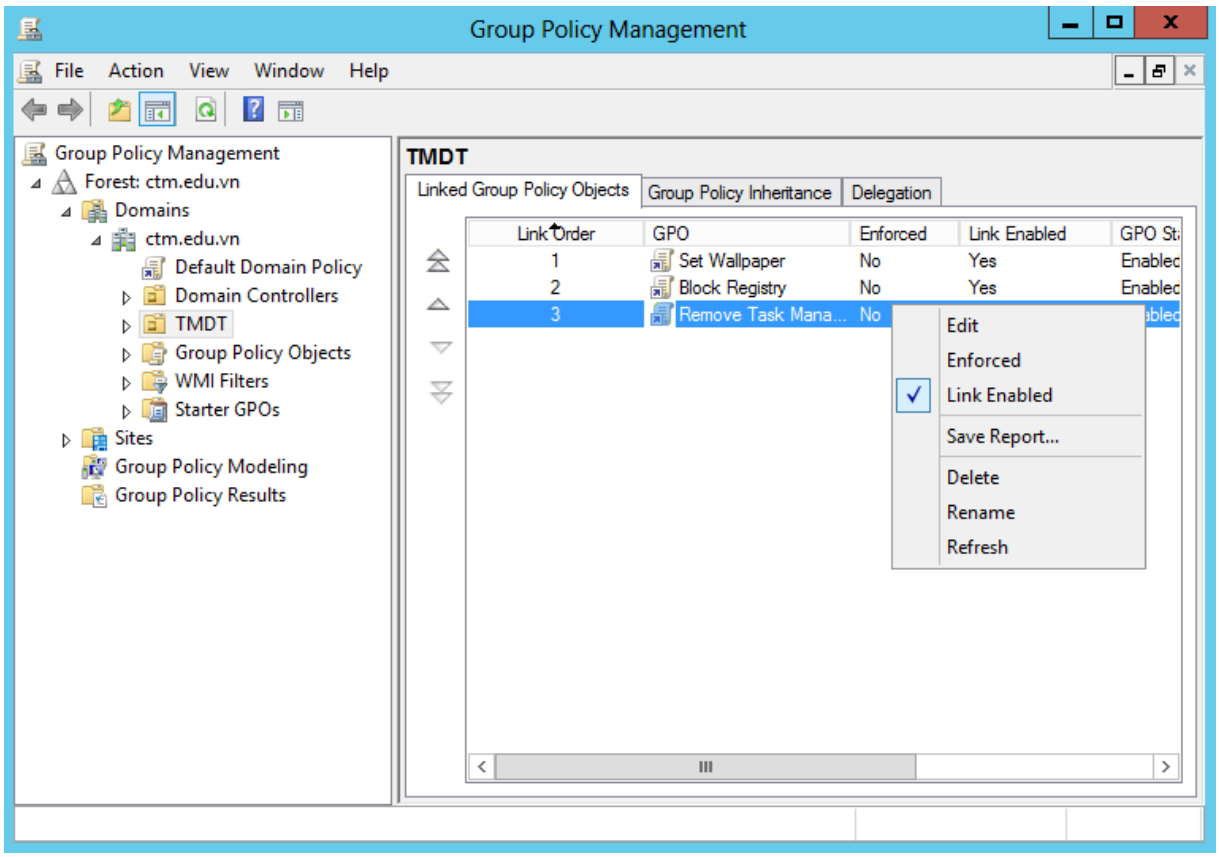
Chuyển sang máy CTM-SRV12-01.

Click chuột phải tại OU ***TMDT***, chọn ***Create a GPO in this domain…***

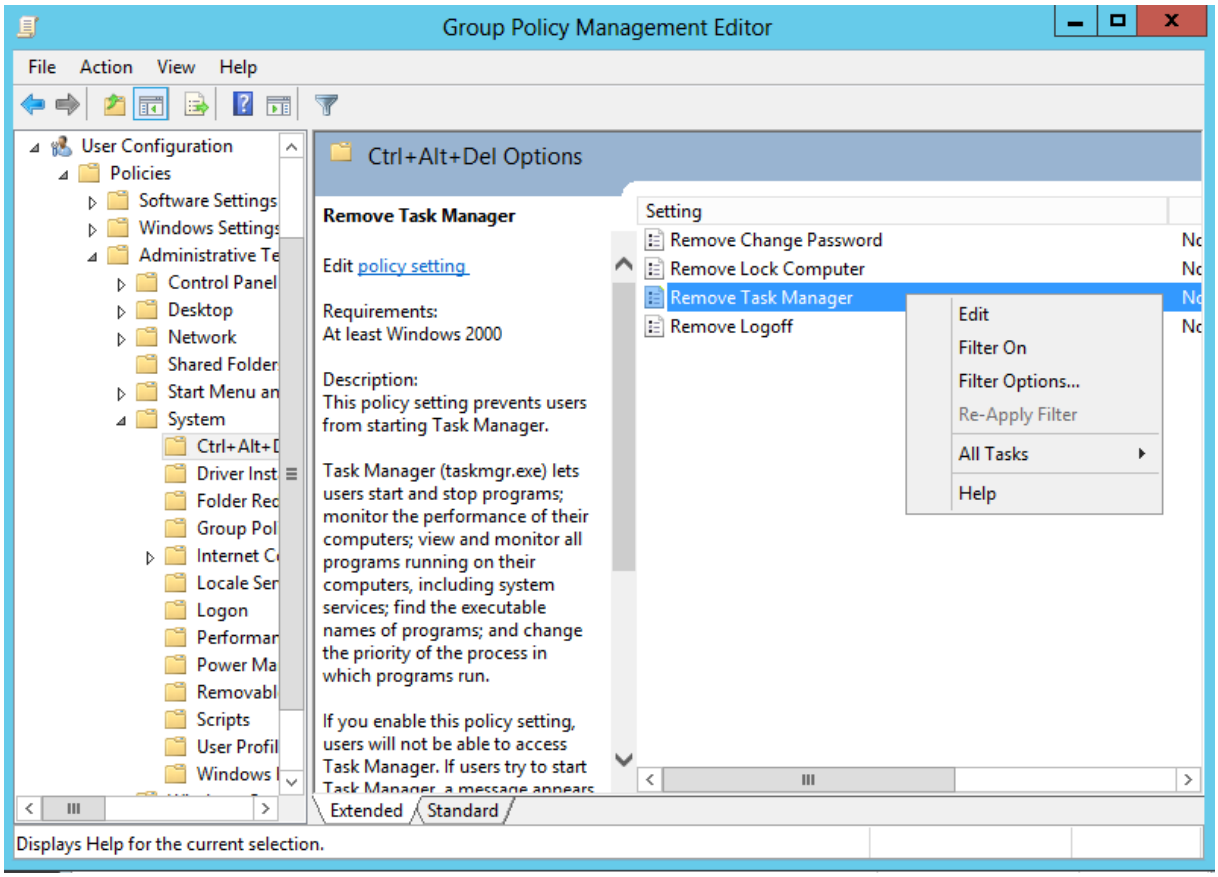
Tại cửa sổ ***New GPO***, nhập vào tên chính sách ***Name*** : *Remove Task Manager*.



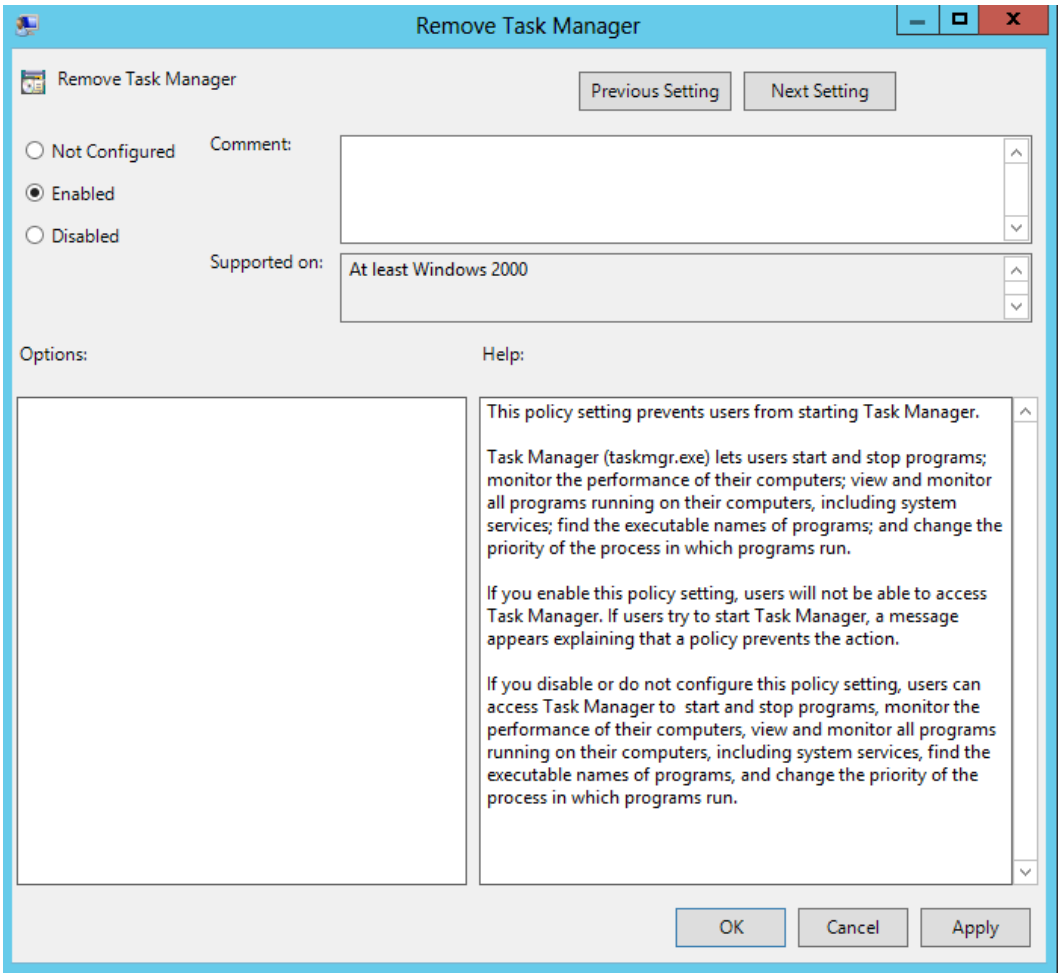
Click chuột phải vào chính sách vừa tạo, chọn ***Edit***



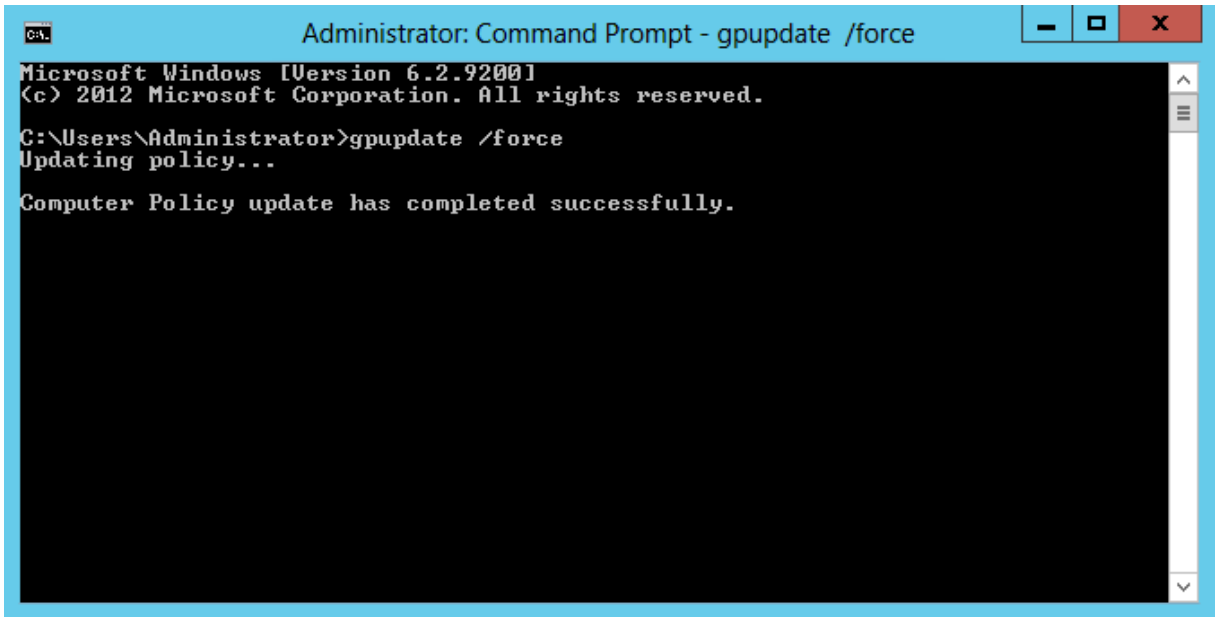
Tại cửa sổ ***Group Policy Management Editor***, chọn vào ***User Configuration / Policies / Administrative Template… / System / Ctrl+Alt+Del Options***. Click chuột phải vào chính sách ***Remove Task Manager*** chọn ***Edit***



Tại cửa sổ ***Remove Task Manager***, click vào ***Enable, Apply, OK***

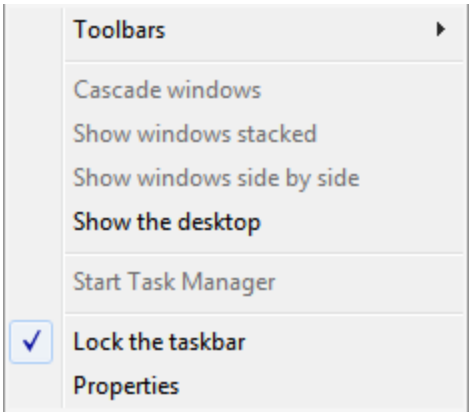


Cập nhật chính sách bằng lệnh ***gpupdate /force*** trong cmd



Bước 2: Kiểm tra chính sách đã áp đặt trên máy client

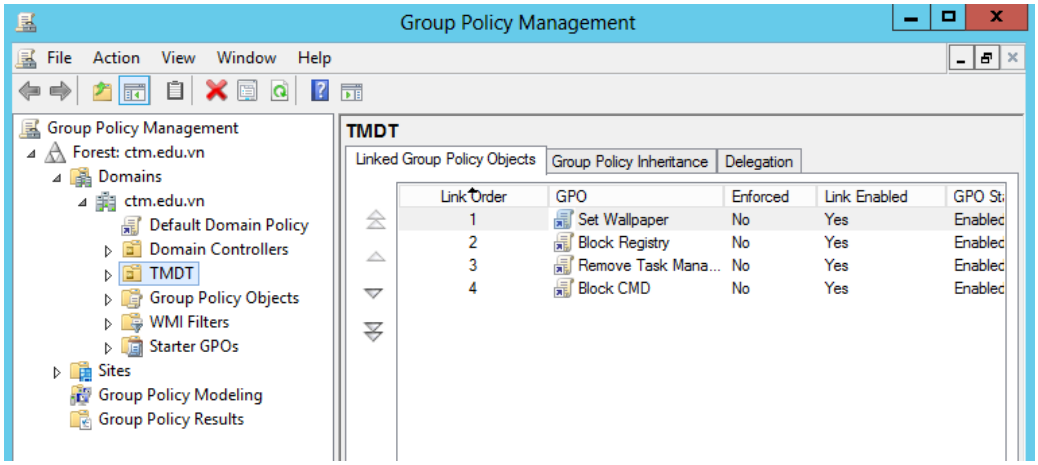
Chuyển sang máy Client CTM-WRK07, đăng nhập bằng tài khoản anhnv trong đơn vị TMDT để kiểm tra. Task Manager đã bị khóa



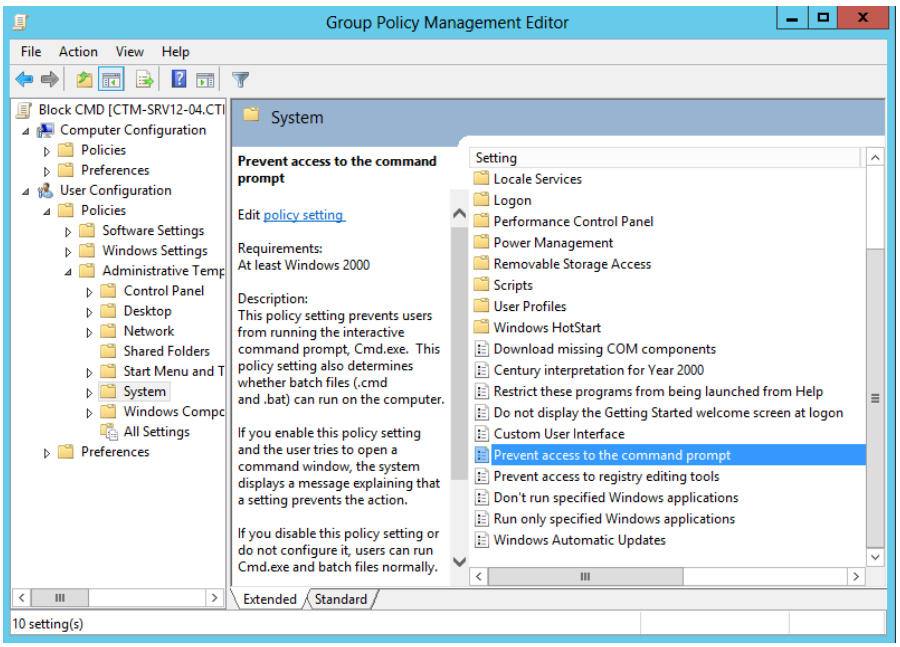
- Tạo chính sách chặn các lệnh trong cmd (Block cmd)

Bước 1: Tạo chính sách chặn các lệnh trong cmd

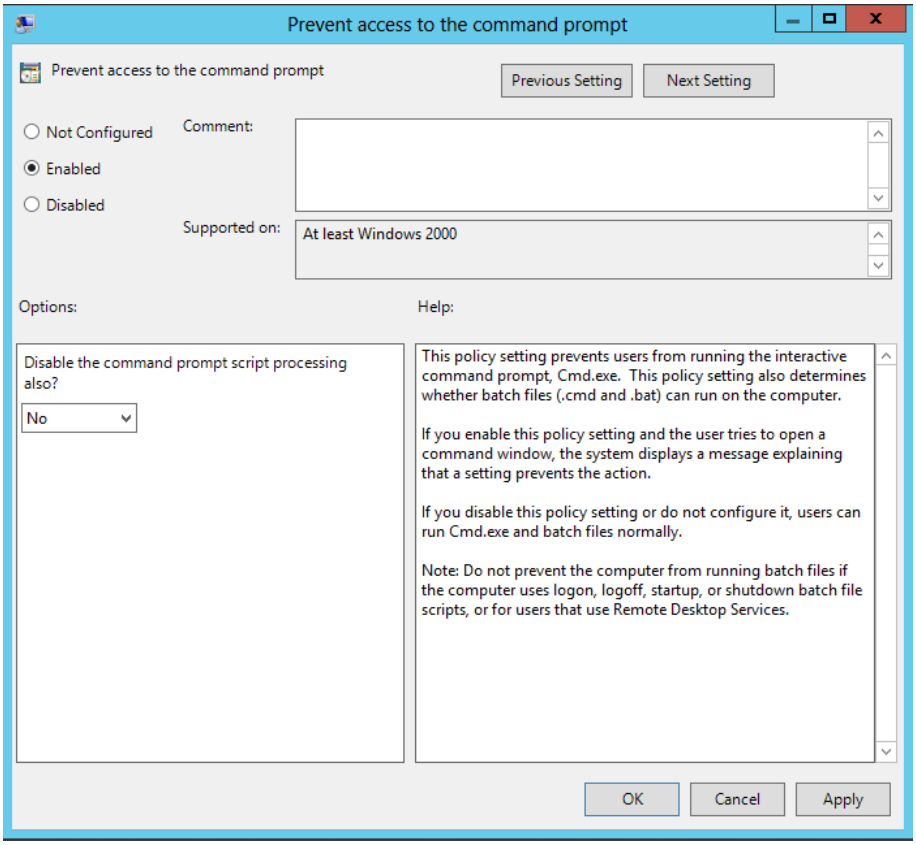
Thực hiện trên máy CTM-SRV12-01.



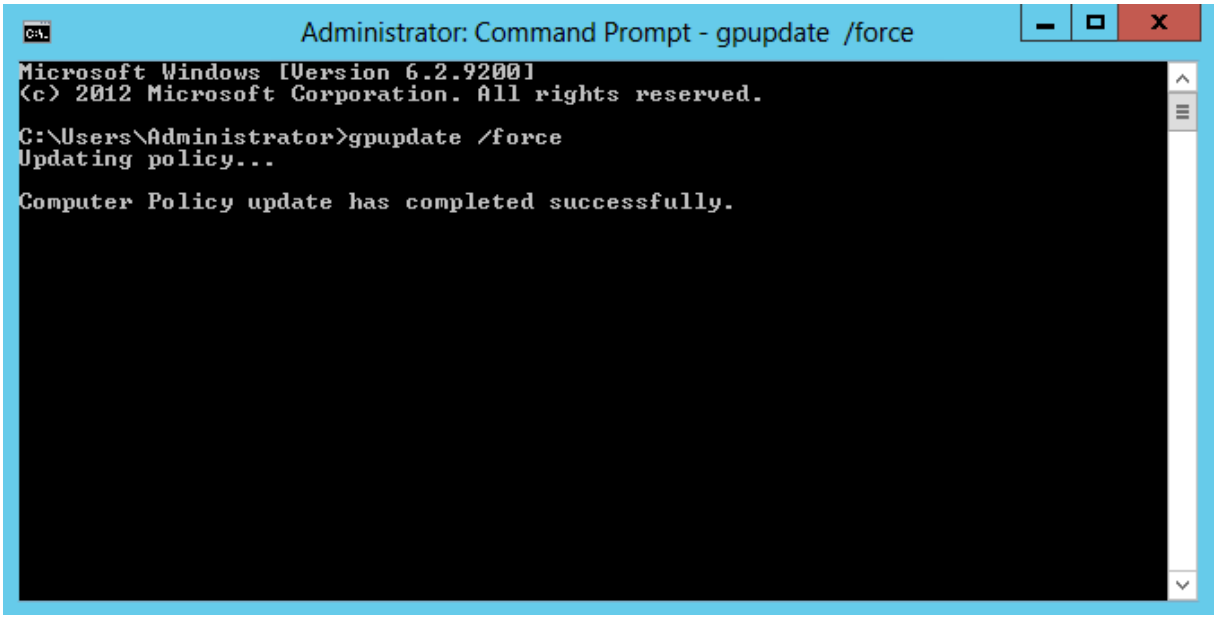
Tại cửa sổ ***Group Policy Management Editor, click vào User Configuration /… System*** , chọn vào chính sách ***Prevent access to the command prompt.***



Tại chính sách này, click chuột phải chọn ***Edit, Enable , Apply , OK***

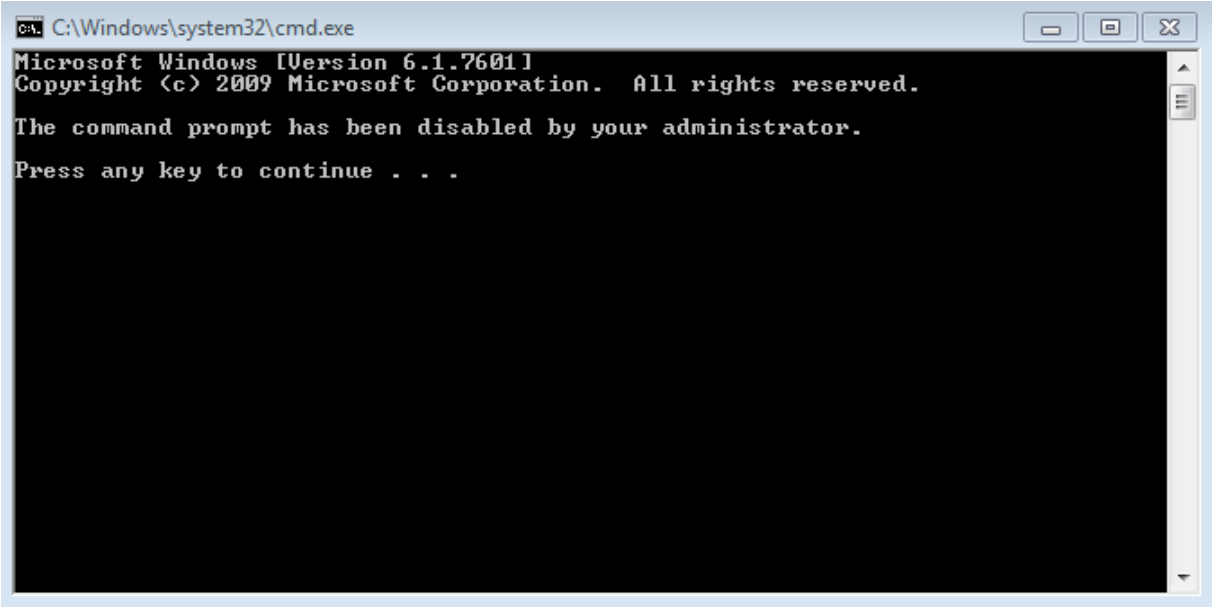


Cập nhật chính sách bằng lệnh ***gpupdate /force*** trong cmd



Bước 2: Kiểm tra chính sách đã áp đặt trên máy client

Chuyển sang máy Client CTM-WRK07 kiểm tra chính sách Block cmd



III. Sai hỏng và cách khắc phục

Triển khai các chính sách không thành công

- Nguyên nhân

- Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Chưa thực hiện lệnh gpupdate /force trên Cmd

- Cách khắc phục

- Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
- Thực hiện lệnh gpupdate /force trên Cmd

V. Hướng dẫn ôn luyện

– Triển khai thêm các chính sách

– Kiểm tra việc triển khai các chính sách trên máy trạm

BÀI 5: CÀI ĐẶT VÀ CẤU HÌNH DỊCH VỤ DHCP

I. Lý thuyết liên quan

1. Giới thiệu DHCP

DHCP được viết tắt từ cụm từ Dynamic Host Configuration Protocol (có nghĩa là Giao thức cấu hình máy chủ). DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cũng như việc cấu hình subnet mask hay cổng mặc định.

- Ưu điểm của DHCP:

+ Khắc phục được tình trạng trùng địa chỉ IP và giảm chi phí quản trị cho hệ thống mạng.

+ Giúp cho các nhà cung cấp dịch vụ (ISP) tiết kiệm được số lượng địa chỉ IP thật (Public IP).

+ Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.

+ Kết hợp với hệ thống mạng không dây (Wireless) cung cấp các điểm Hotspot như: nhà ga, sân bay, trường học…

- Nhược điểm của DHCP

DHCP mang lại nhiều ưu điểm, song bên cạnh đó cũng còn mặt hạn chế. Chẳng hạn như việc không nên sử dụng địa chỉ IP động, địa chỉ IP thay đổi đối với các thiết bị cố định và cần truy cập liên tục. Ví dụ như không nên sử dụng IP động cho các thiết bị máy in ở các văn phòng.

Mặc dù có rất nhiều lợi ích khi sử dụng DHCP, vẫn có một số hạn chế cần lưu ý. Không nên sử dụng địa chỉ IP động, địa chỉ IP thay đổi đối với các thiết bị cố định và cần truy cập liên tục như máy in và file server.

Bởi DHCP sử dụng chủ yếu với các hộ gia đình hay văn phòng. Đối với các thiết bị dùng trong văn phòng, như máy in thì việc việc gán chúng với các địa chỉ IP thay đổi không mang tính thực tiễn. Lúc đó mỗi khi kết nối với máy tính khác thì máy in đó sẽ phải thường xuyên cập nhật cài đặt để máy tính có thể kết nối với máy in.

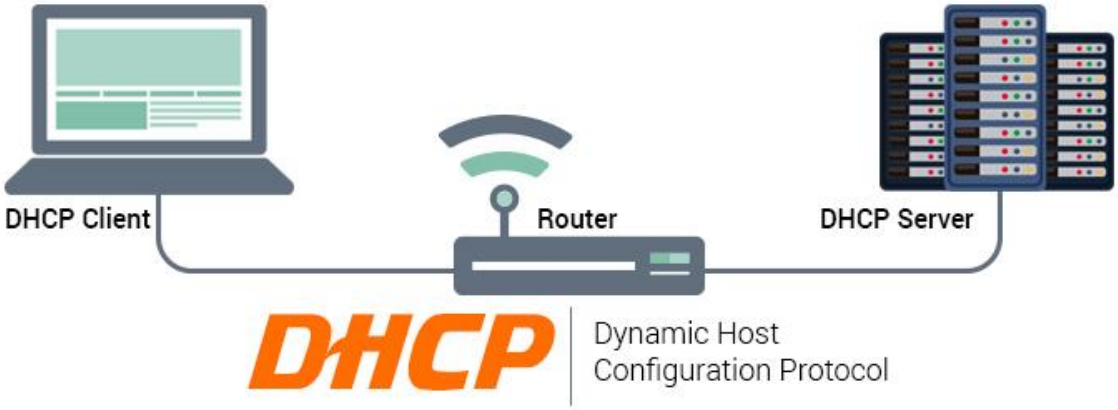
2. Hoạt động của DHCP

Được giải thích một cách ngắn gọn nhất về cách thức hoạt động của DHCP chính là khi một thiết bị yêu cầu địa chỉ IP từ một router thì ngay sau đó router sẽ gán một địa chỉ IP khả dụng cho phép thiết bị đó có thể giao tiếp trên mạng.

Như ở các hộ gia đình hay các doanh nghiệp nhỏ thì router sẽ hoạt động như một máy chủ DHCP nhưng ở các mạng lớn hơn thì DHCP như một máy chỉ ở vai trò là máy tính.

Cách thức hoạt động của DHCP còn được giải thích ở một cách khác thì khi một thiết bị muốn kết nối với mạng thì nó sẽ gửi một yêu cầu tới máy chủ, yêu cầu này gọi là DHCP DISCOVER. Sau khi yêu cầu này đến máy chủ DHCP thì ngay tại đó máy chủ sẽ tìm một địa chỉ IP có thể sử dụng trên thiết bị đó rồi cung cấp cho thiết bị địa chỉ cùng với gói DHCPOFFER

Khi nhận được IP thì thiết bị tiếp tục phản hồi lại máy chủ DHCP gói mang tên DHCPREQUEST. Lúc này là lúc chấp nhận yêu cầu thì máy chủ sẽ gửi tin báo nhận (ACK) để xác định thiết bị đó đã có IP, đồng thời xác định rõ thời gian sử dụng IP vừa cấp đến khi có địa chỉ IP mới.



Hình 2.5.1 – Hoạt động của DHCP

II. Trình tự thực hiện

1. Yêu cầu thực hiện

Cài đặt và cấu hình dịch vụ DHCP Server trên máy Server CTM-SRV12 sao cho:

- Tạo một Scope có tên là [192.168.1.0] DHCP_DEMO.
- Trừ ra các địa chỉ dành cho Gateway và các máy Server, Print là: 192.168.1.1 – 192.168.1.20.
- Cho phép các máy trạm nhận địa chỉ từ: 192.168.1.21 – 192.168.1.254
- Domain: ctm.edu.vn.
- Router: 192.168.1.1.
- DNS Server: 192.168.1.2.

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

3. Các bước thực hiện

Thực hiện triển khai cài đặt và cấu hình dịch vụ DHCP Server thông qua 3 bước sau:

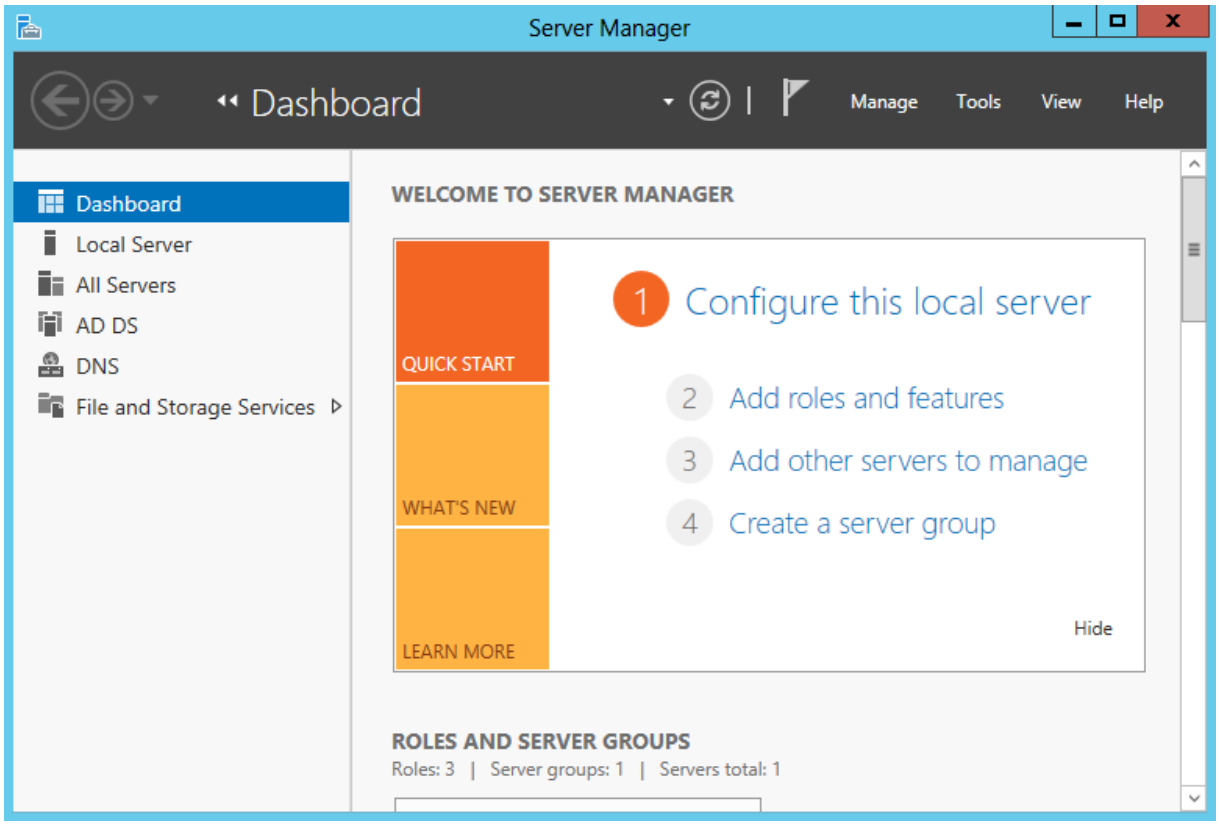
- Bước 1: Cài đặt dịch vụ DHCP Server
- Bước 2: Xác thực DHCP Server
- Bước 3: Cấu hình dịch vụ DHCP
- Bước 4: Chuyển qua máy trạm, cấu hình chế độ nhận IP động.

Hướng dẫn chi tiết:

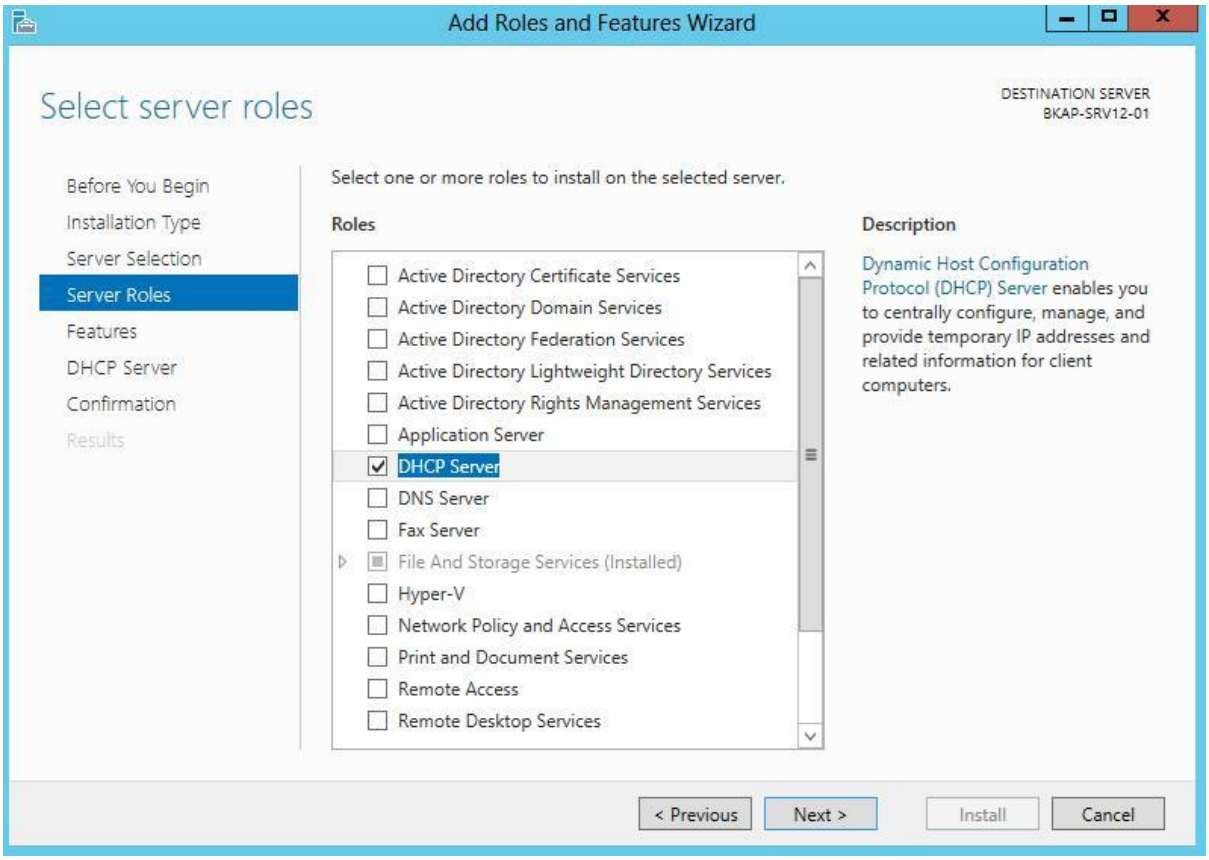
Thực hiện trên máy server CTM-SRV12:

Bước 1: Cài đặt dịch vụ DHCP Server.

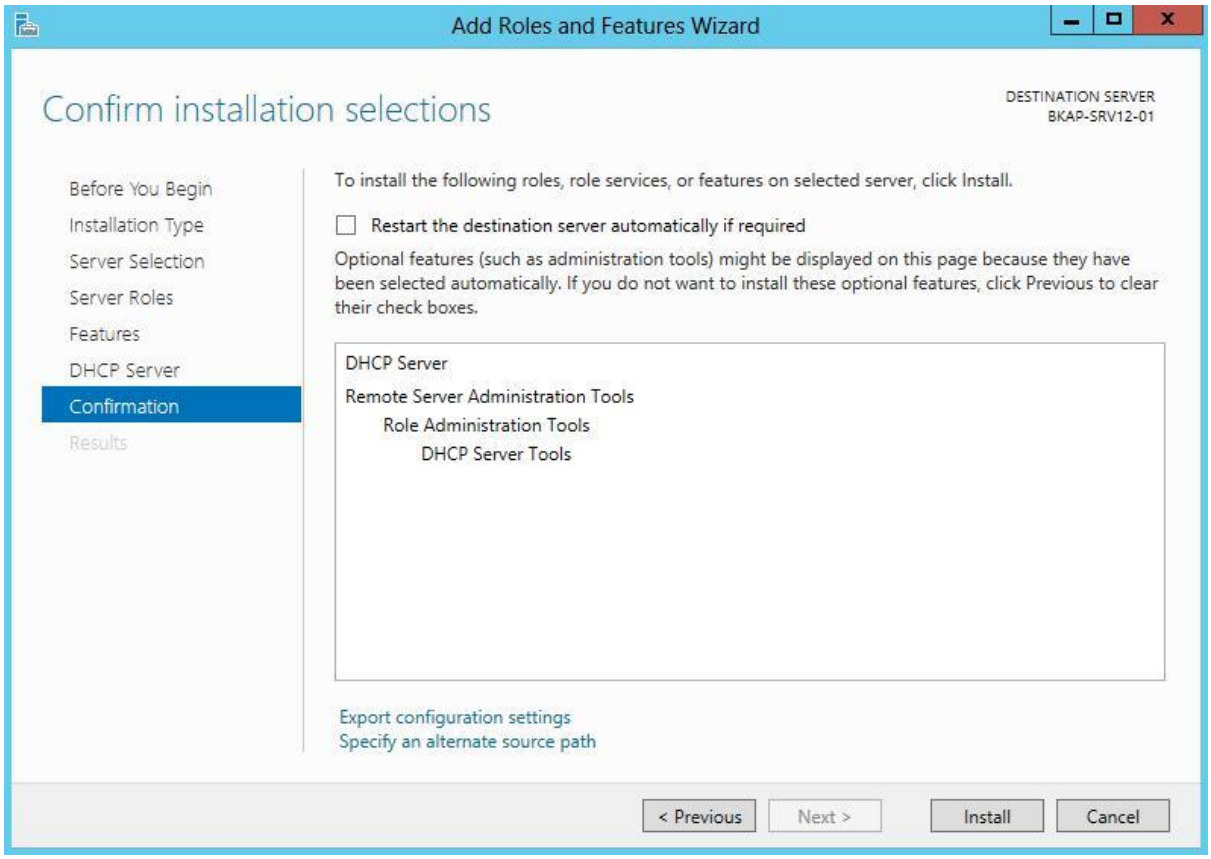
Mở ***Server Manager / Add roles and features***



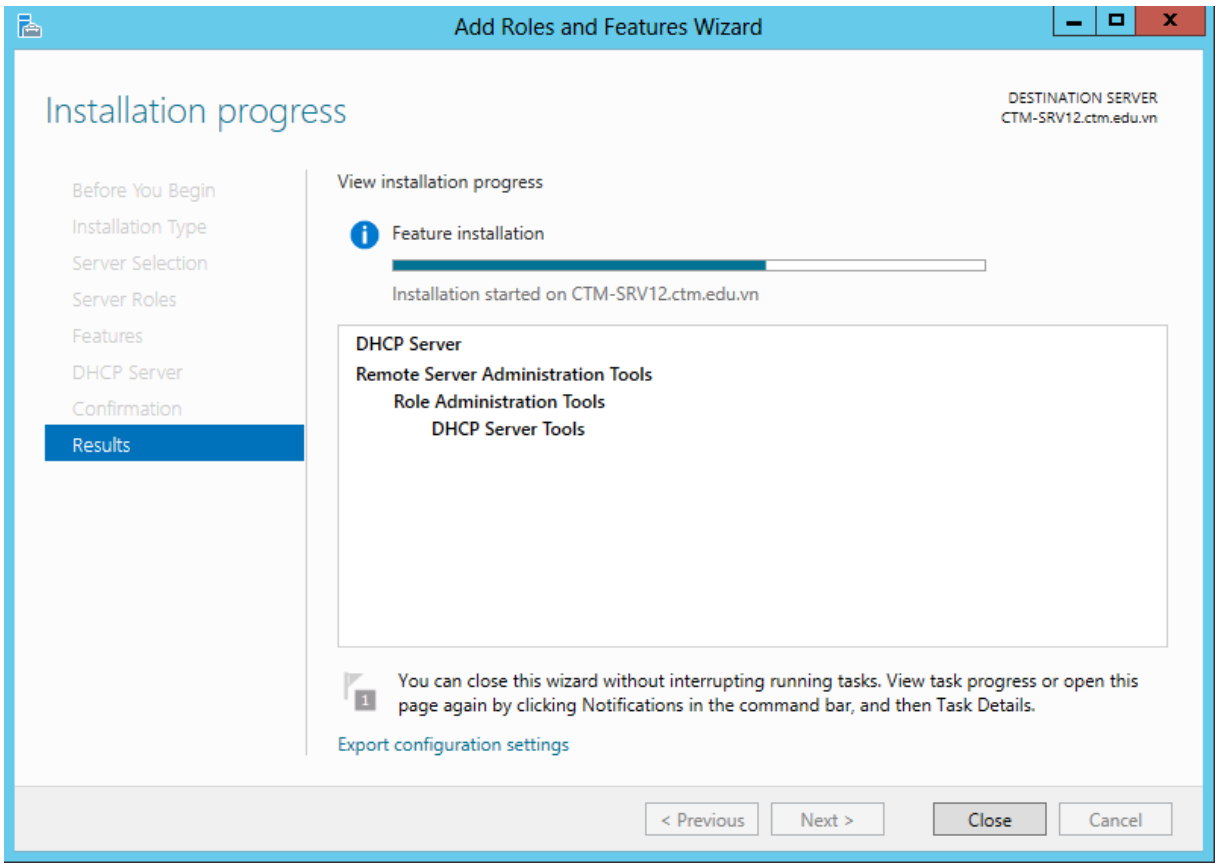
Tại cửa sổ ***Select server roles***, click chọn vào dịch vụ ***DHCP Server***. Sau đó nhấn vào ***Next***



Tại cửa sổ ***Confirm installation selections***, click vào ***Install*** để Server bắt đầu cài đặt dịch vụ DHCP

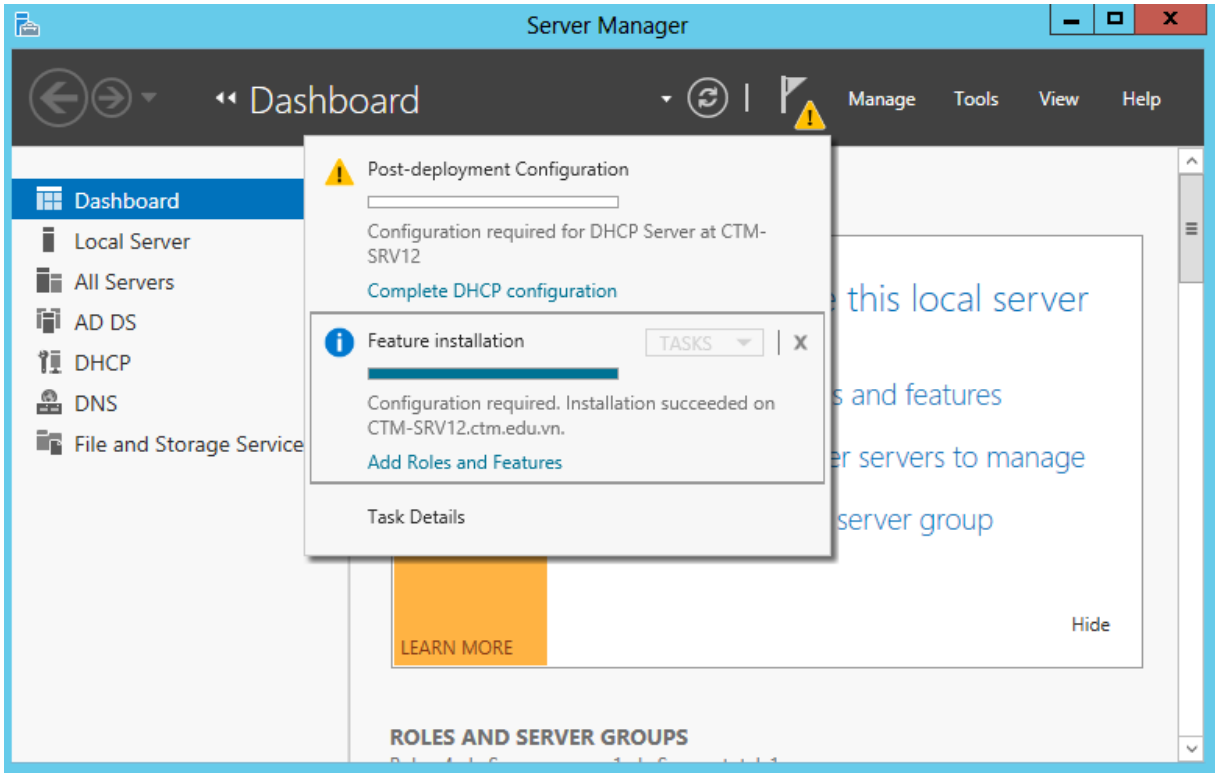


Sau khi máy chủ cài đặt xong, click vào ***Close*** để kết thúc quá trình cài đặt

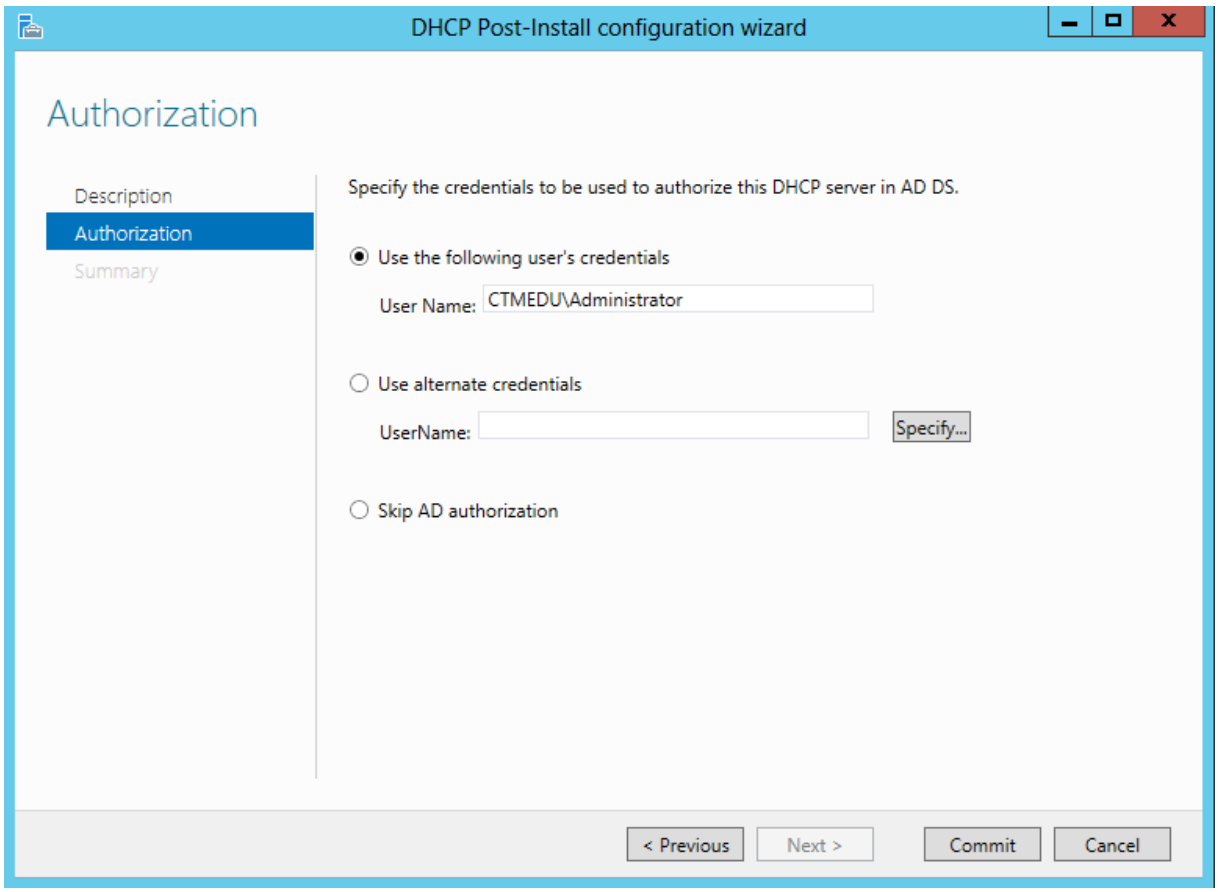


Bước 2: Xác thực DHCP Server

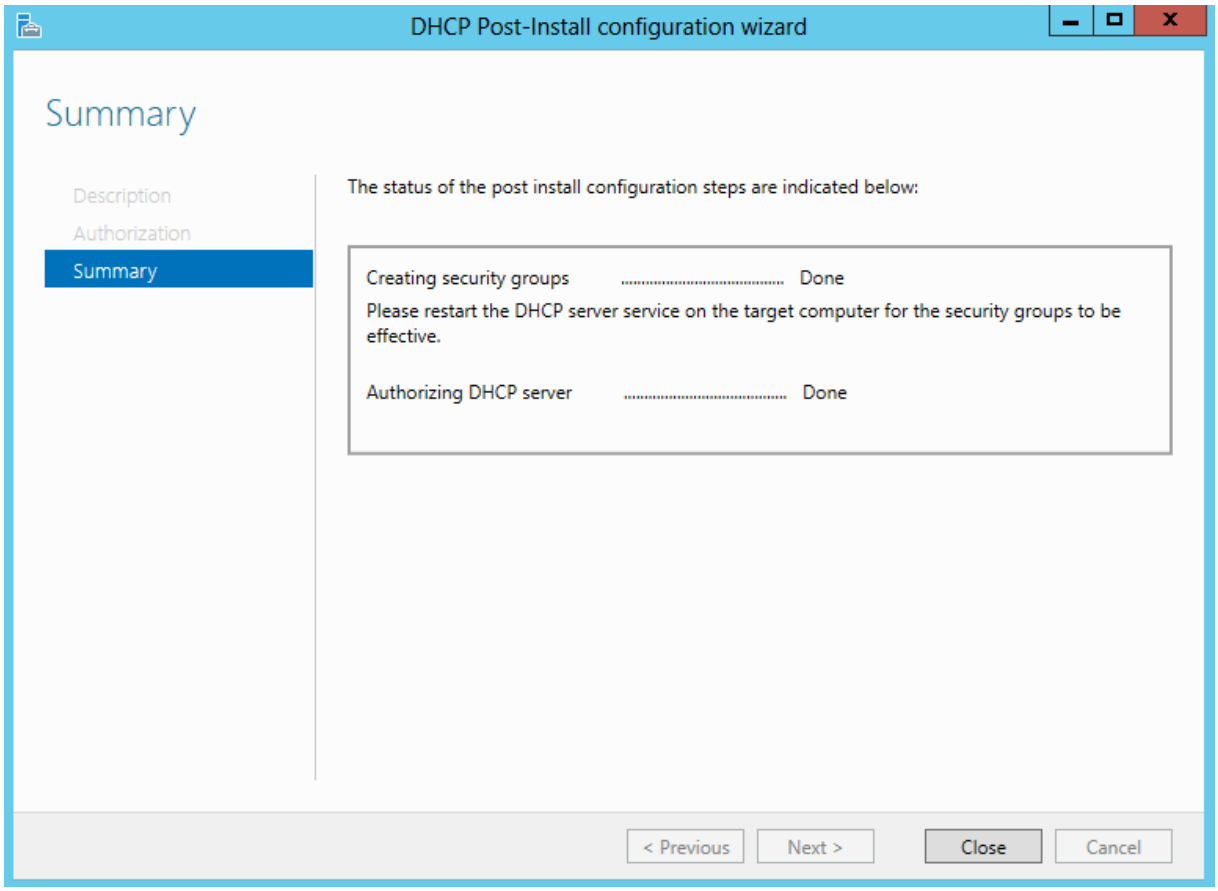
Mở ***Notification*** của ***Server Manager***, click vào dòng chữ ***Complete DHCP configuration***



Tại cửa sổ ***Authorization*** ,click vào nút ***Commit***

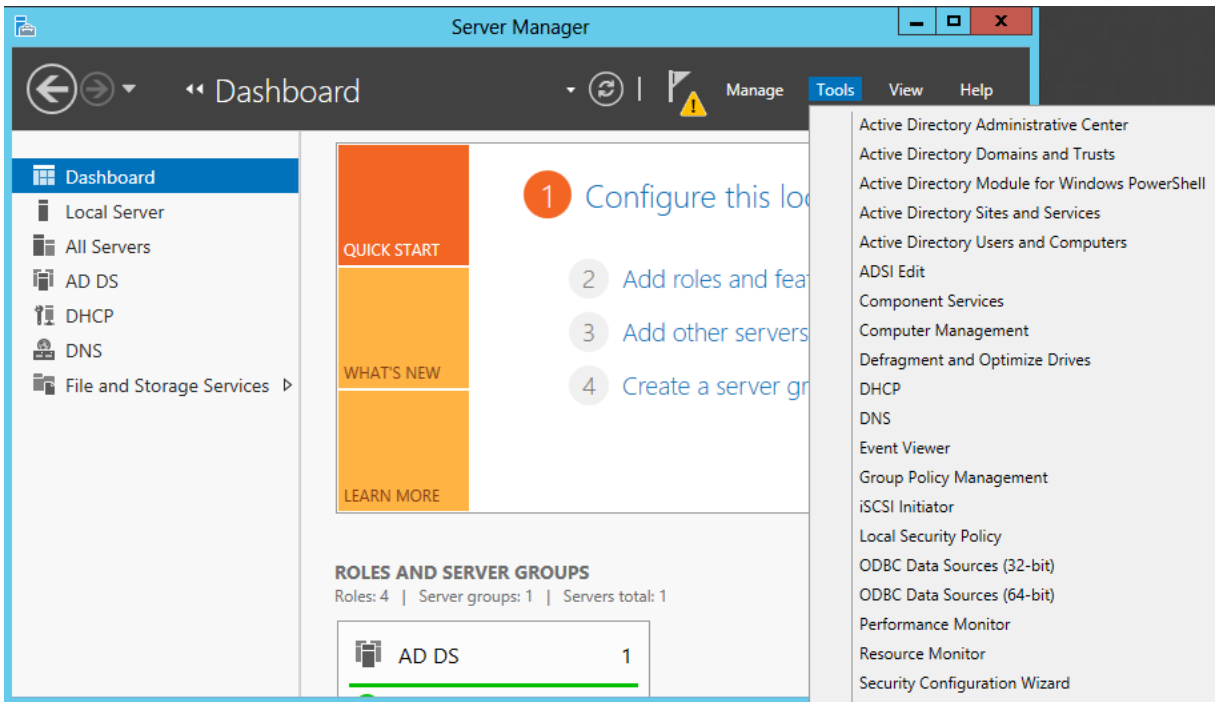


Tại cửa sổ ***Summary*** ,click vào nút ***Close***

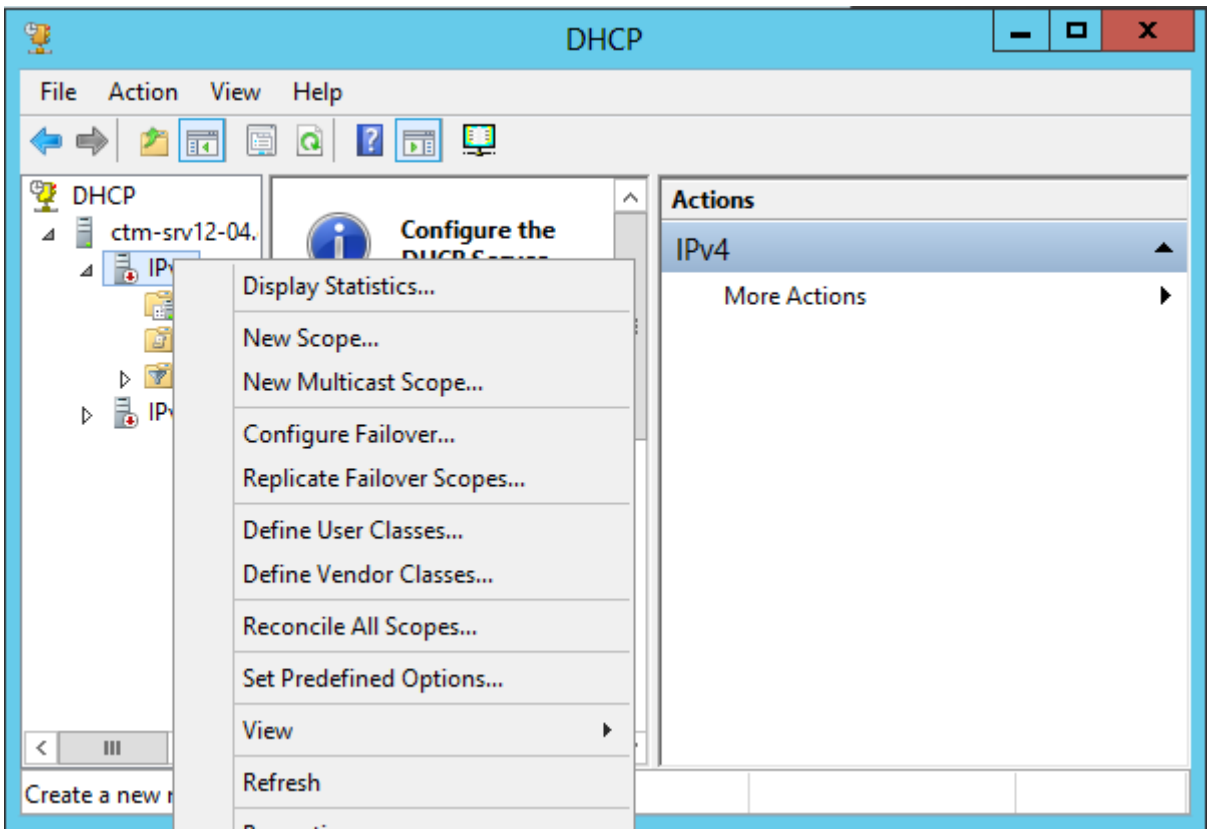


Bước 3: Cấu hình dịch vụ DHCP

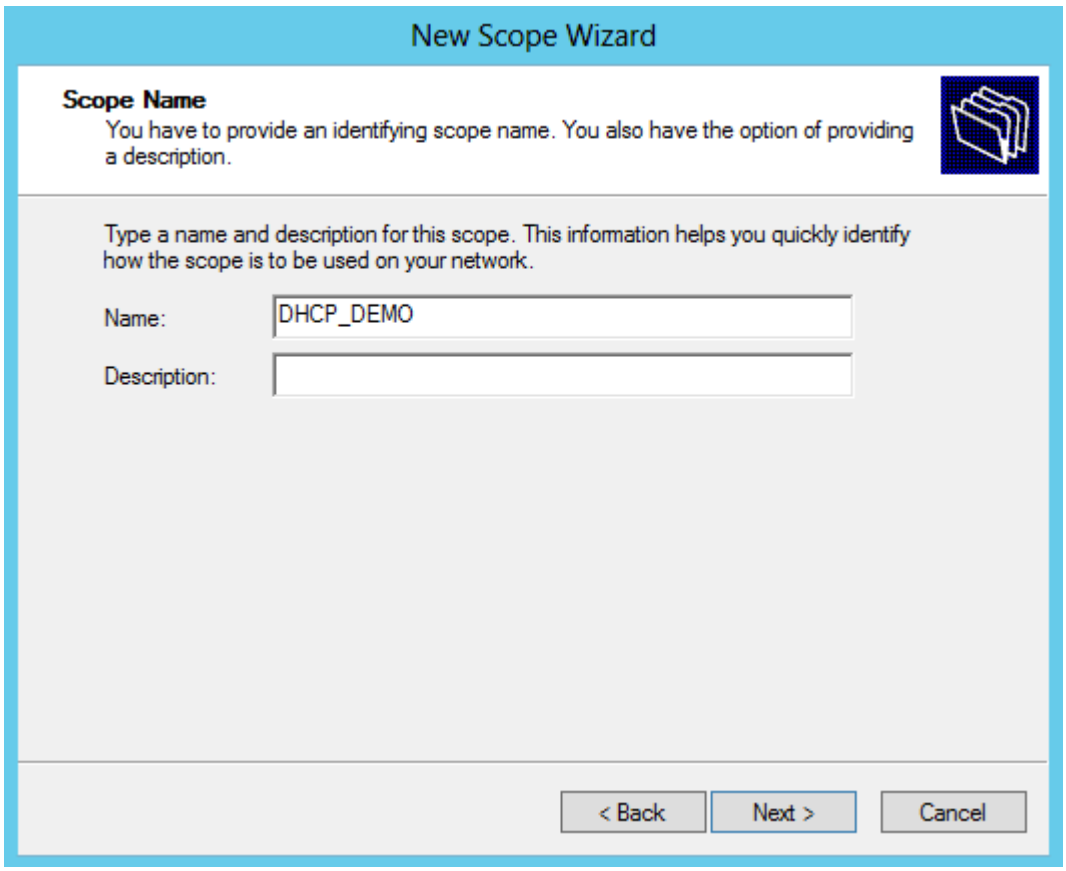
Thực hiện cấu hình dịch vụ DHCP Server: ***Vào Server Manager / Tools*** ,chọn vào ***DHCP***



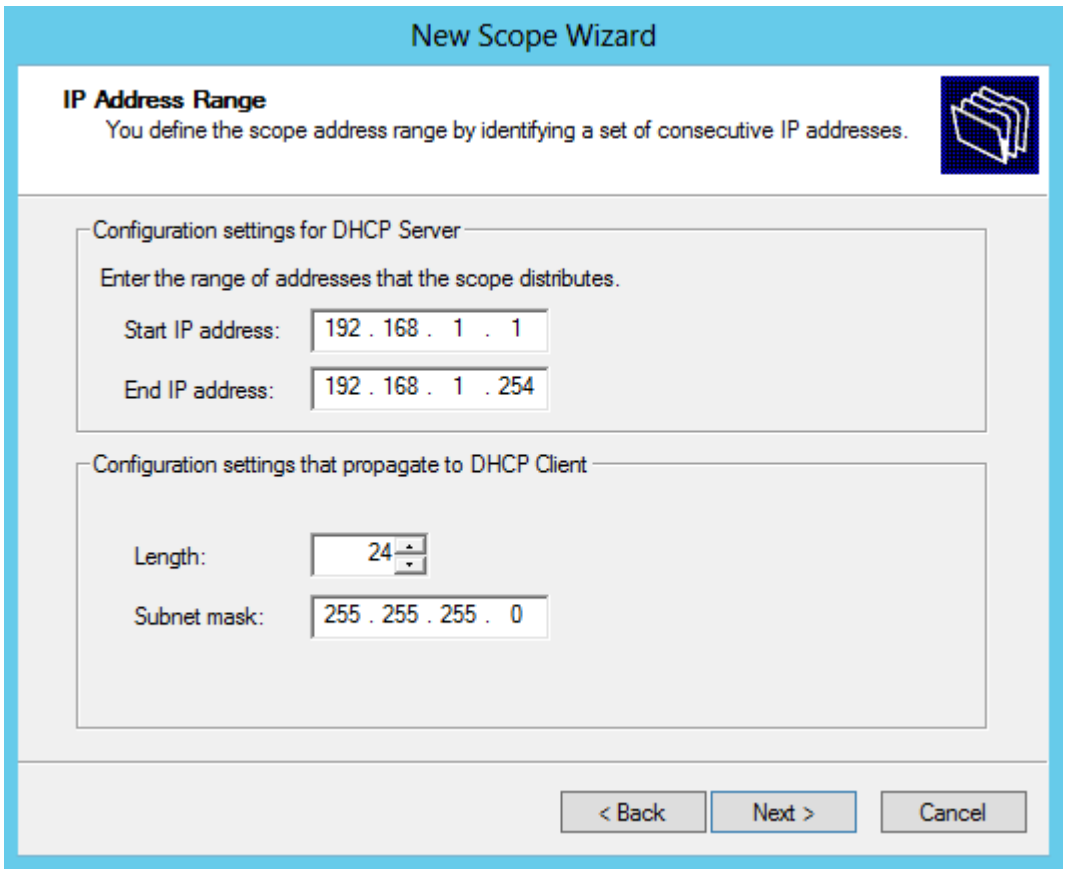
Trong cửa sổ ***DHCP***, chuột phải tại ***IPv4, chọn New Scope…***



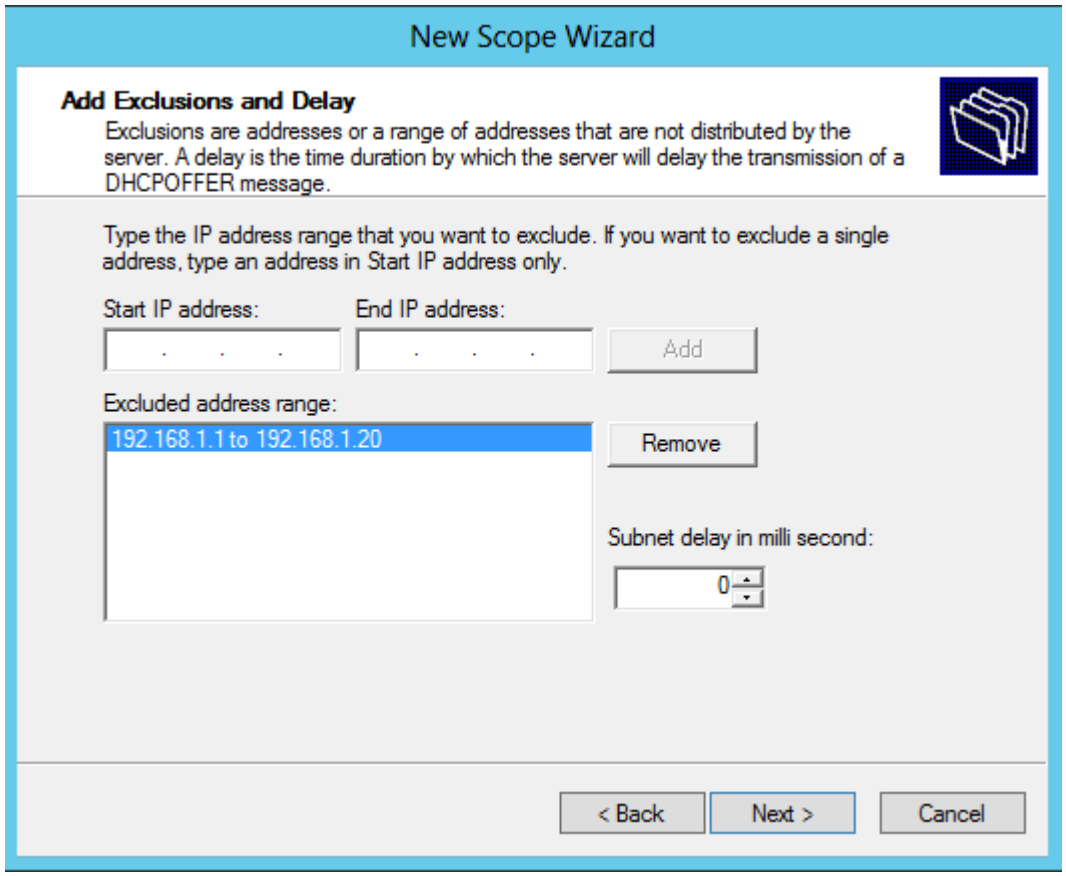
Tại cửa sổ ***Scope Name***, nhập tên của scope: *DHCP_DEMO*, sau đó click vào ***Next***



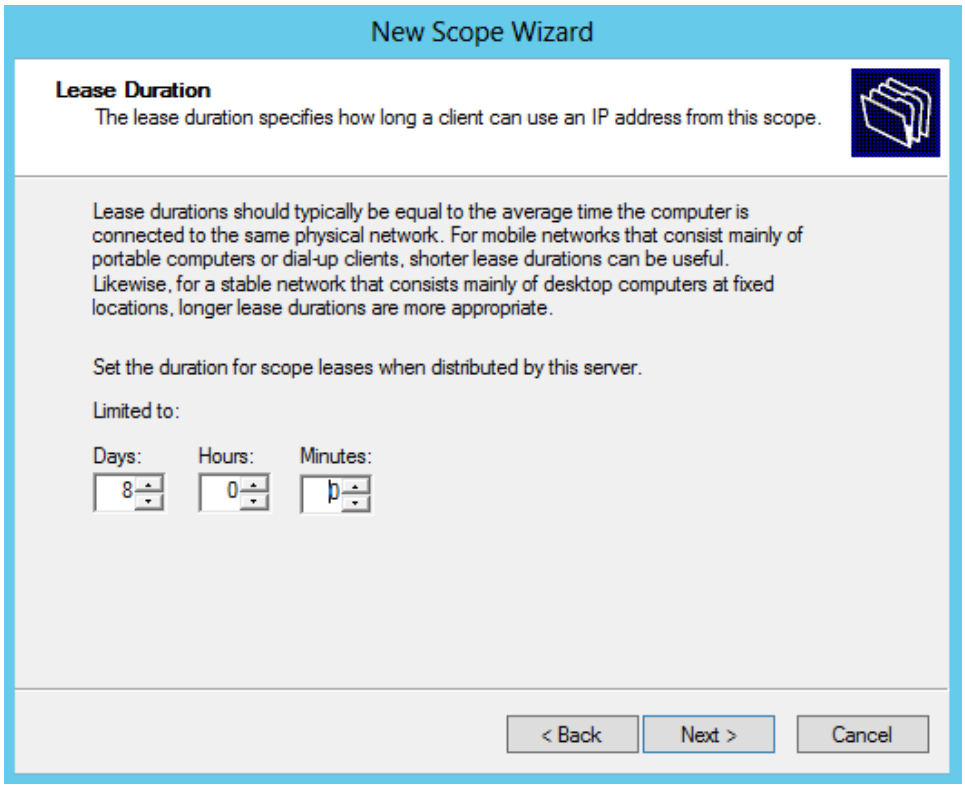
Tại cửa sổ ***IP Address Range / Start IP address và End IP address***, nhập dải địa chỉ ***IP DHCP server*** cấp phát cho toàn mạng. (*192.168.1.1 – 192.168.1.254*)



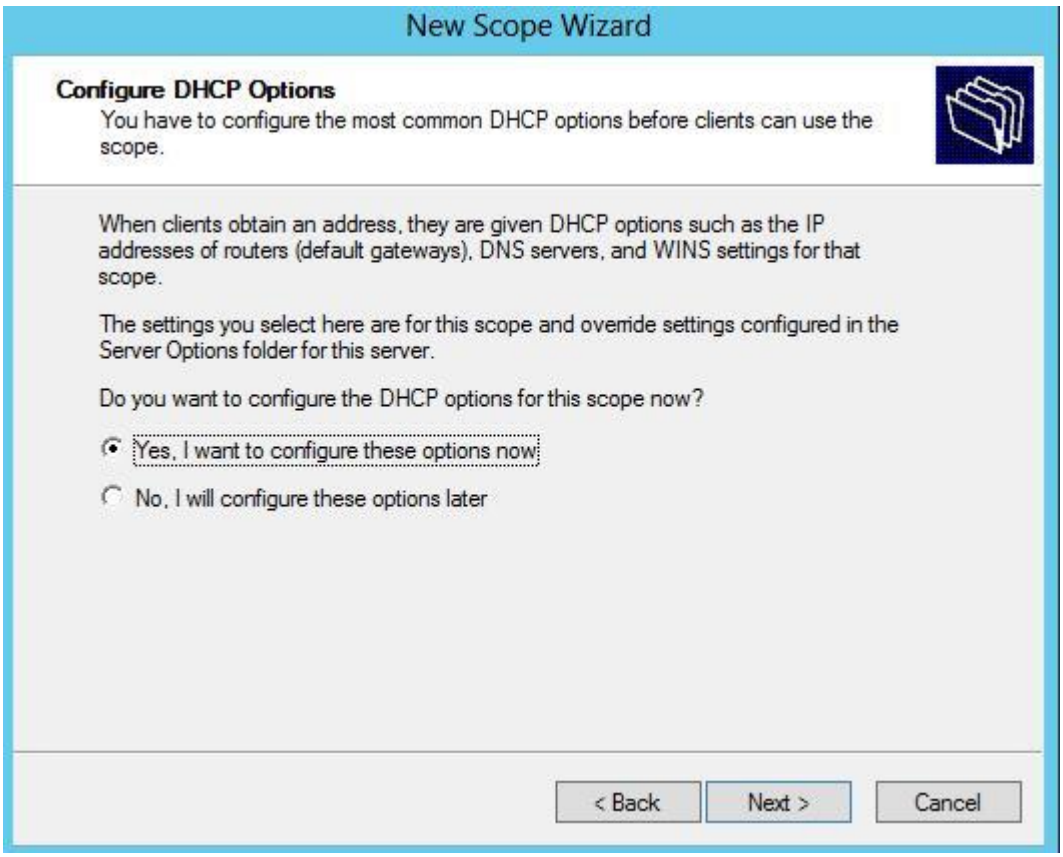
Tại cửa sổ ***Add Exclusions and Delay / Start IP address và End IP address*** nhập dải địa chỉ DHCP server trừ ra không cấp phát cho các máy Client. (*192.168.1.1 – 192.168.1.20*), sau đó click vào ***Add***



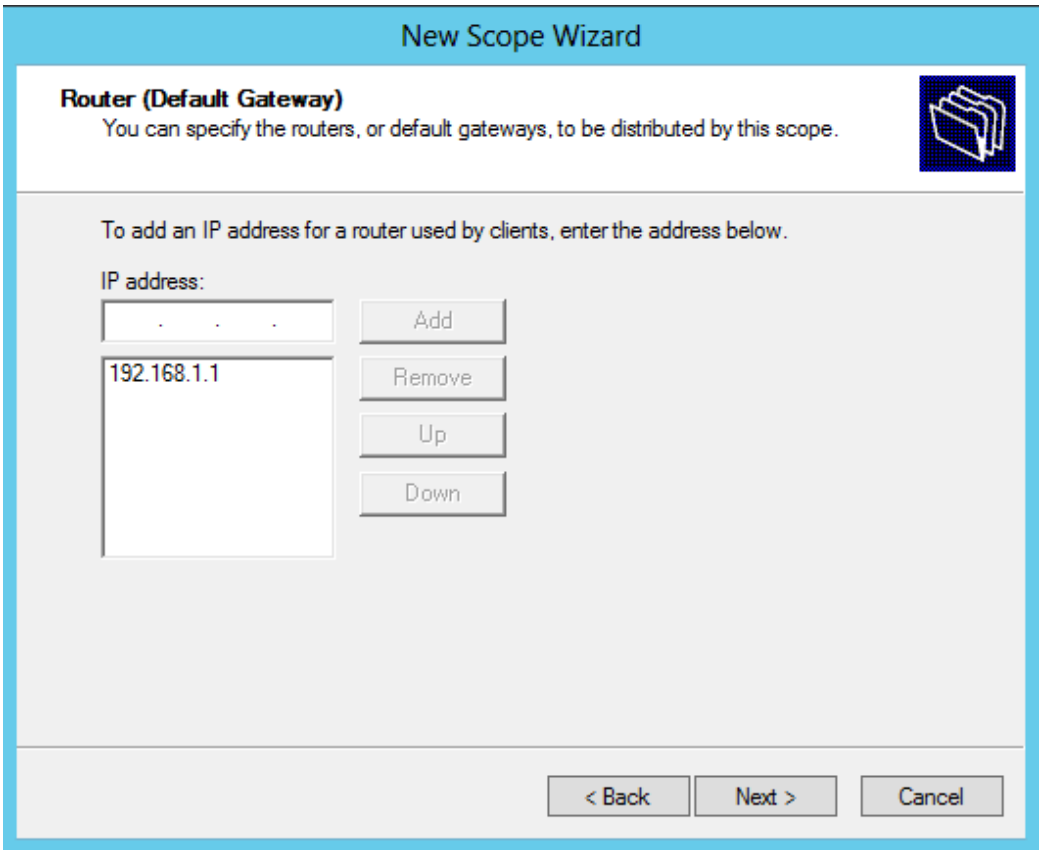
Tại cửa sổ ***Lease Duration***, đây là thời gian hiệu lực của 1 địa chỉ IP do DHCP server cấp phát xuống máy Client



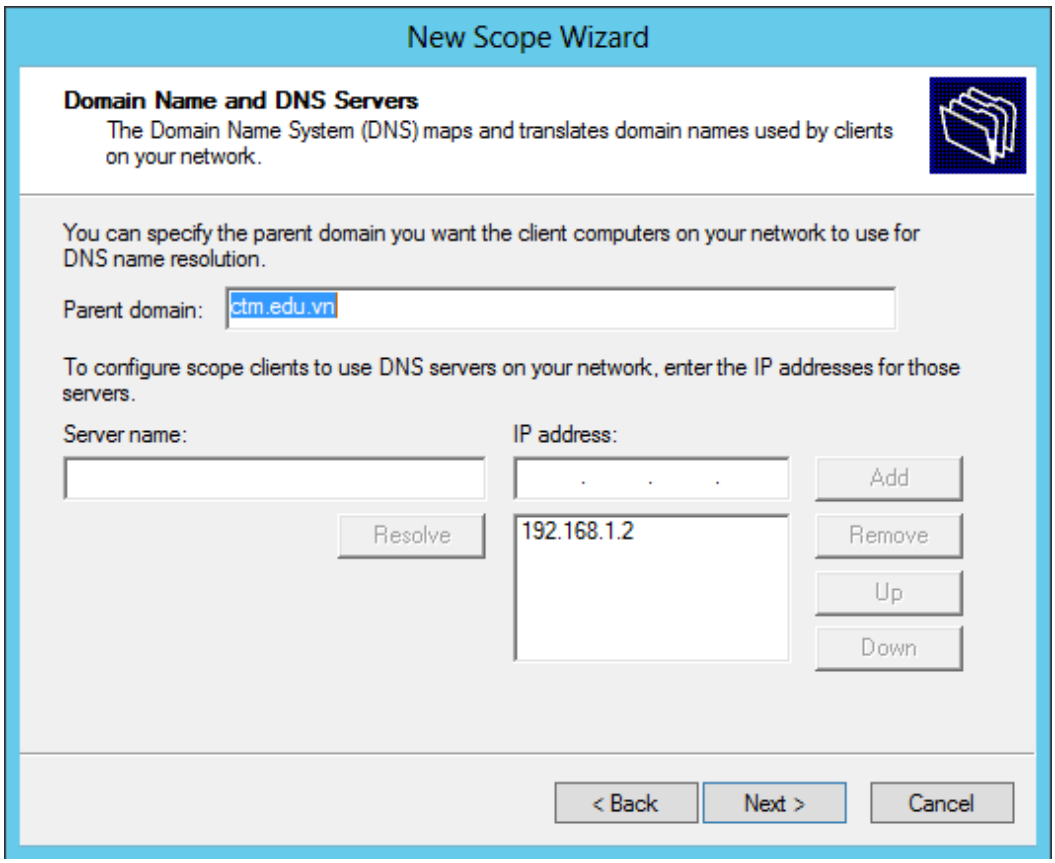
Tại cửa sổ ***Configure DHCP Options***, chọn ***Yes, I want to configure these options now***

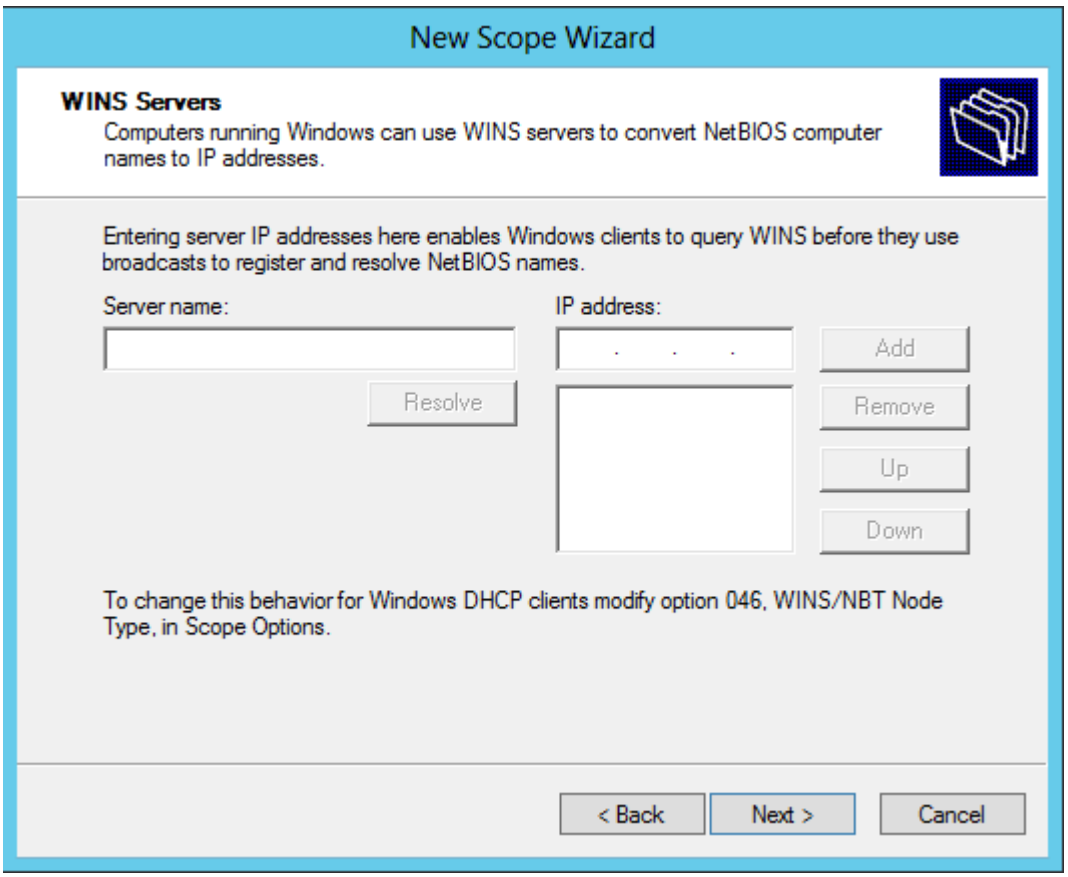


Tại cửa sổ ***Router (Default Gateway) / IP address***, nhập địa chỉ Router *192.168.1.1*, sau đó click vào ***Add***

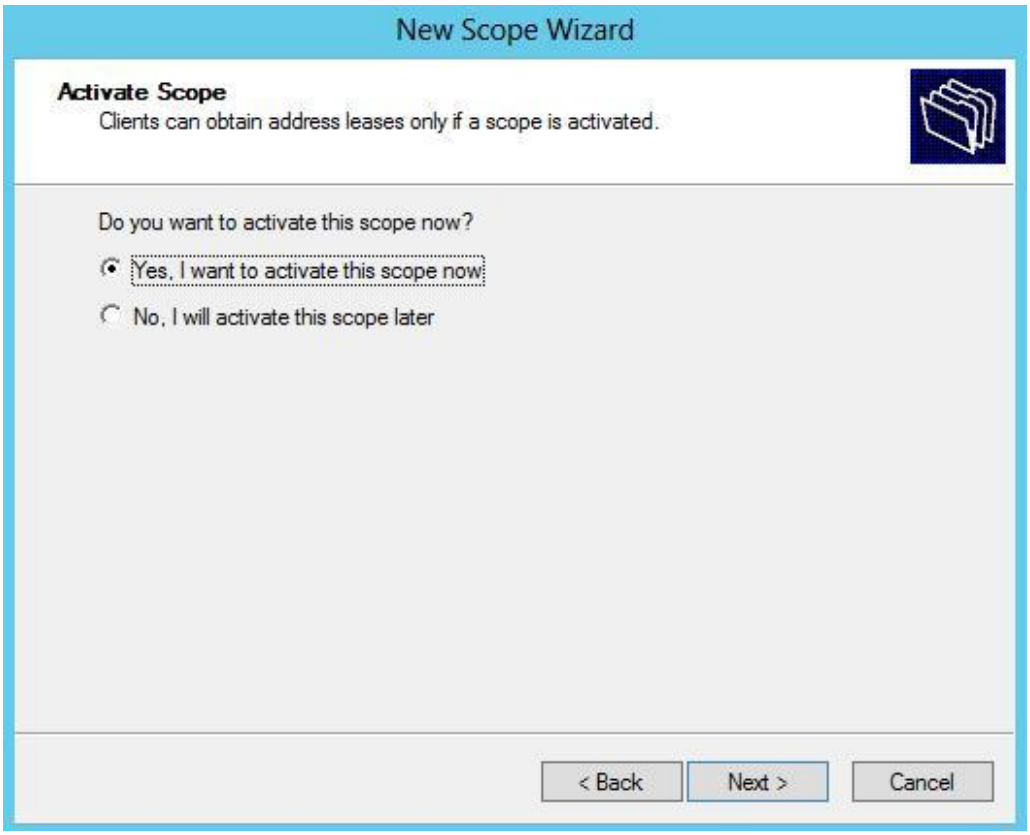


Tiếp tục click vào ***Next*** tại các cửa sổ ***Domain Name and DNS Servers*** và cửa sổ ***WINS Servers***.

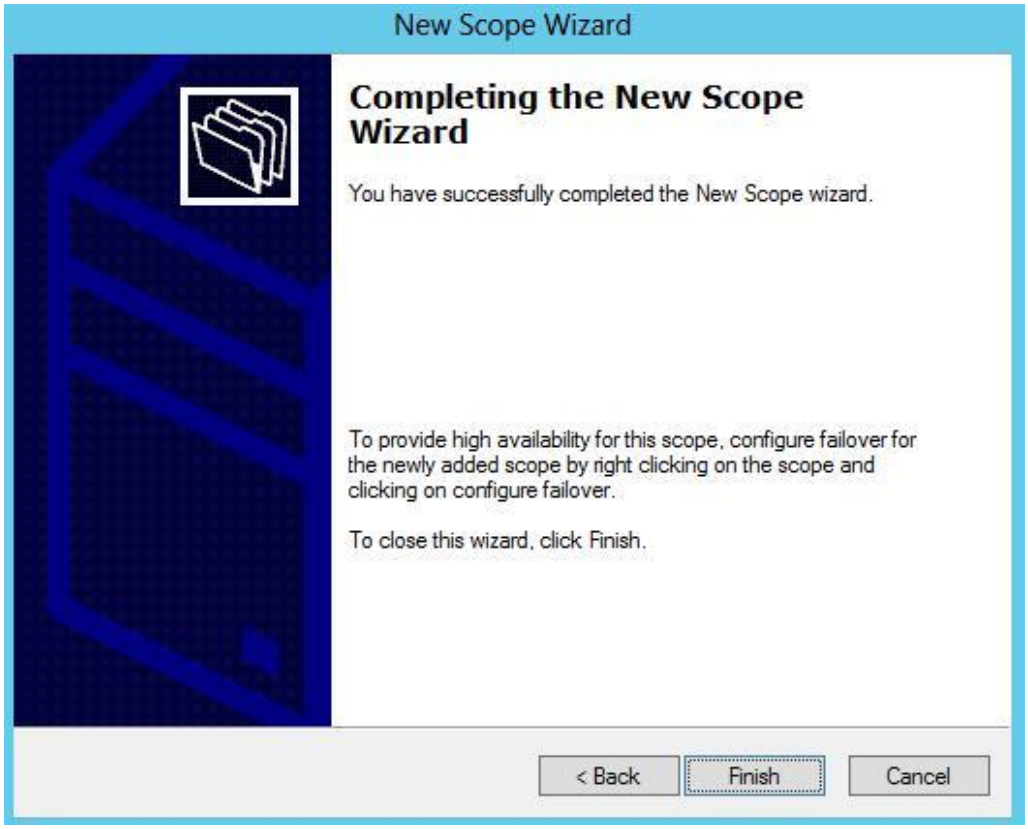




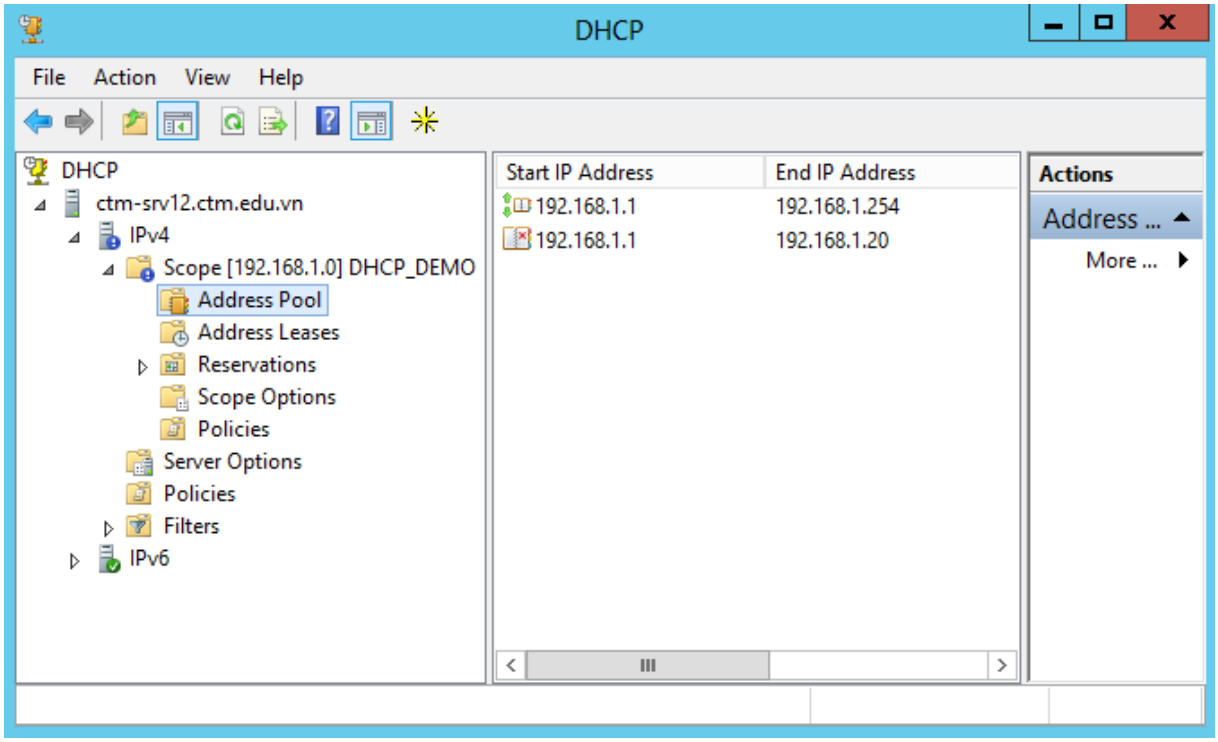
Tại cửa sổ ***Activate Scope***, chọn ***Yes, I want to activate this scope now***



Tại cửa sổ tiếp theo, click vào ***Finish*** để kết thúc quá trình cấu hình dịch vụ DHCP Server

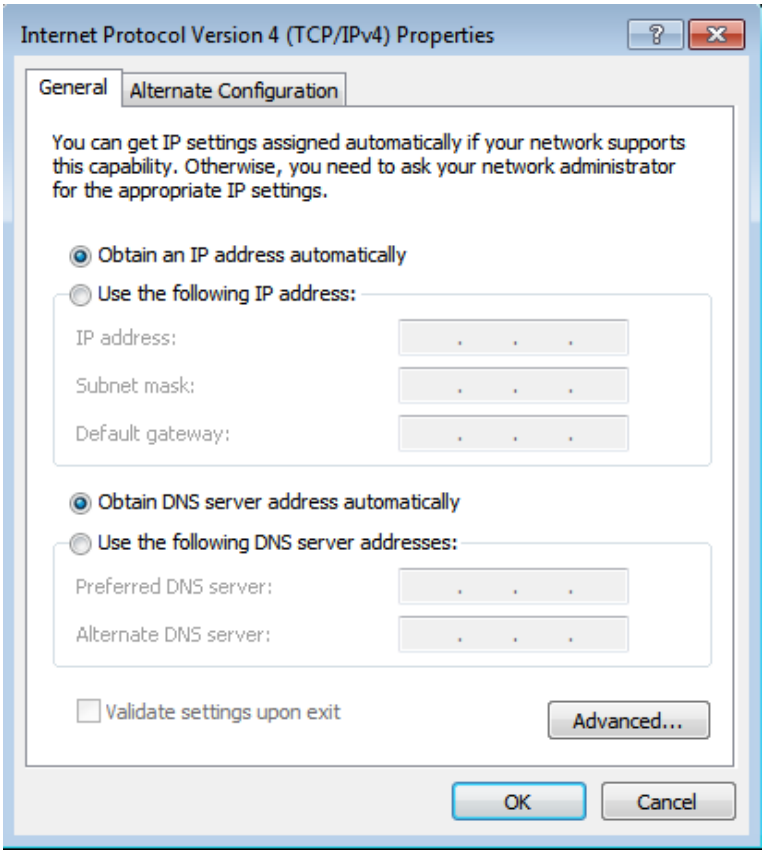


Kết quả sau khi hoàn tất việc tạo Scope DHCP_DEMO để cấp phát địa chỉ

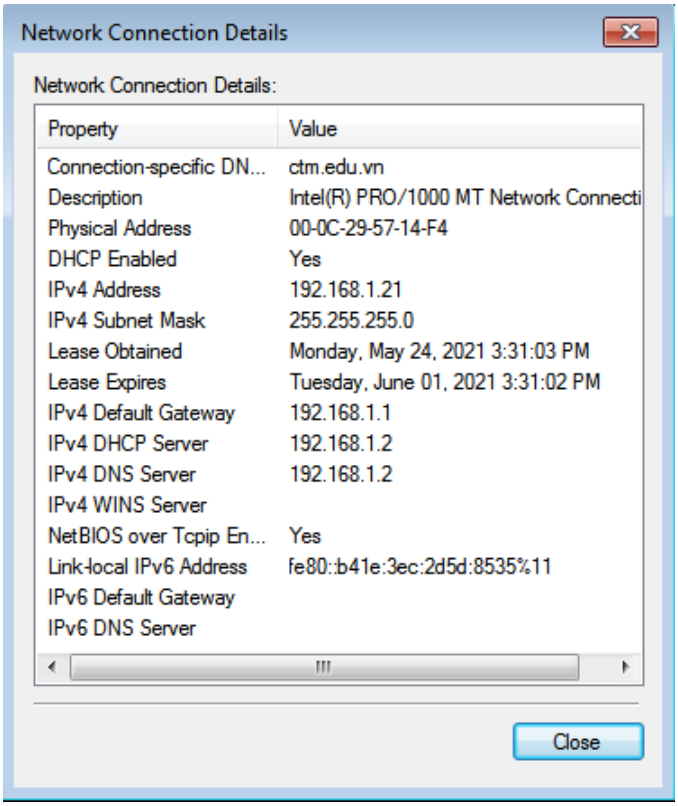


Bước 4: Chuyển qua máy trạm CTM-WRK07, cấu hình chế độ nhận IP động.

Vào card mạng của máy CTM-WRK07, chỉnh card mạng ở chế độ ***Obtain an IP address automatically***



Mở mục ***Network Connection Details*** để kiểm tra DHCP Server cấp địa chỉ IP động



III. Sai hỏng và cách khắc phục

Triển khai các chính sách không thành công

- Nguyên nhân

- Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Chưa thực hiện lệnh gpupdate /force trên Cmd

- Cách khắc phục

- Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
- Thực hiện lệnh gpupdate /force trên Cmd

V. Hướng dẫn ôn luyện

– Triển khai thêm các chính sách
– Kiểm tra việc triển khai các chính sách trên máy trạm

BÀI 6: CÀI ĐẶT VÀ CẤU HÌNH DỊCH VỤ DNS

I. Lý thuyết liên quan

1. Giới thiệu DNS

Mỗi máy tính hay thiết bị mạng tham gia vào mạng Internet đều giao tiếp với nhau bằng địa chỉ IP (Internet Protocol) . Để thuận tiện cho việc sử dụng và dễ nhớ người ta dùng tên (domain name) để xác định thiết bị đó.

Hệ thống tên miền (Domain Name System) được sử dụng để ánh xạ tên miền thành địa chỉ IP. Vì vậy, khi muốn liên hệ tới các máy, chúng chỉ cần sử dụng chuỗi ký tự dễ nhớ (domain name) như: www.microsoft.com, www.ibm.com…, thay vì sử dụng địa chỉ IP là một dãy số dài khó nhớ.

Khi DNS chưa ra đời, người ta sử dụng một file tên Host.txt. File này sẽ lưu thông tin về tên host và địa chỉ của host của tất cả các máy trong mạng, file này được lưu ở tất cả các máy để chúng có thể truy xuất đến máy khác trong mạng.

Khi đó, nếu có bất kỳ sự thay đổi về tên host, địa chỉ IP của host thì phải cập nhật lại toàn bộ các file Host.txt trên tất cả các máy.

Do vậy đến năm 1984 Paul Mockpetris thuộc viện USC's Information Sciences Institute phát triển một hệ thống quản lý tên miền mới lấy tên là Hệ thống tên miền – Domain Name .

Hệ thống tên miền này cũng sử dụng một file tên host.txt, lưu thông tịn của tất cả các máy trong mạng, nhưng chỉ được đặt trên máy làm máy chủ tên miền (DNS). Khi đó, các Client trong mạng muốn truy xuất đến các Client khác, thì nó chỉ việc hỏi DNS.

Chức năng của DNS là :

+ Phân giải địa tên máy thành địa chỉ IP và ngược lại.

+ Phân giải tên domain.

Máy chủ triển khai dịch vụ Domain Name System được gọi là Domain Name Server

2. Cách phân bổ dữ liệu quản lý Domain Name

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 miền

a) 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.

b) Phân giải IP thành tên

Để có thể phân giải tên máy tính của 1 địa chỉ IP, trong không gian tên miền người ta bổ xung thêm 1 nhánh tên miền mà được lập chỉ mục theo địa chỉ IP. Phần không gian này có tên miền là in-addr.arpa.

Mỗi node trong miền in-addr.arpa có 1 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 --> 255 của byte đầu tiên trong địa chỉ IP. Trong mỗi subdomain lại có 256 subdomain con nữa ứng với byte thứ 2. Cứ như thế và đến byte thứ 4 có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ IP tương ứng.

4. Phân loại Domain Name Server

a) Primary Name Server

Mỗi Domain phải có 1 Primary Name Server. Server này được đăng ký trên Internet để quản lý Domain. Mọi người trên Internet đều biết tên máy tính và IP của Server này. Người quản trị DNS sẽ tổ chức các cơ sở dữ liệu DNS trên Primary Name Server. Server này đảm nhận vai trò chính trong việc phân giải tất cả các máy tính trong Domain hay Zone

b) Secondary Name Server

Mỗi Domain có 1 Primary Name Server để quản lý cơ sở dữ liệu DNS. Nếu như Server này tạm ngưng hoạt động vì 1 lý do nào đó thì việc phân giải DNS bị gián đoạn. Để tránh trường hợp này người ta đã thiết kế ra 1 máy chủ dự phòng gọi là Secondary Name Server (hay còn gọi là Slave).

Khi Secondary Name Server được khởi động nó sẽ tìm Primary Name Server nào mà nó được phép lấy dữ liệu về máy. Nó sẽ copy lại toàn bộ CSDL DNS của Primary Name Server mà nó được phép transfer (quá trình này gọi là quá trình Zone Transfer). Theo 1 chu kỳ nào đó do người quản trị quy định thì Secondary Name Server sẽ sao chép và cập nhật CSDL từ Primary Name Server.

c) 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 sẽ lưu lại những thông tin 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.

5. Resource Record (RR)

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

a) SOA (Start of Authority)

Trong mỗi tập tin CSDL phải có 1 và chỉ 1 record SOA. Bảng ghi SOA này chỉ ra rằng Primary Name Server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.

Cú pháp của 1 record SOA :

[tên-miền] IN SOA [tên-DNS-Server] [địa-chỉ-email] (

Serial number;

Refresh number;

Retry number;

Experi number;

Time-to-line number)

Ví dụ:

vnnetpro.com. IN SOA server1.vnnetpro.com. sangnt.vnnetpro.com. (

1 ; serial

10800 ; refresh after 3 hours

3600 ; retry after 1 hours

604800 ; expire after 1 week

86400) ; minimum TTL of 1 day

Giải thích ý nghĩa ví dụ trên:

- Tên Domain : vnnetpro.com. phải ở vị trí cột đầu tiên và kết thúc bằng dấu chấm (.).

- IN là Internet

- server1.vnnetpro.com là tên FQDN của Primary Name Server của dữ liệu này.

- sangnt.vnnetpro.com là địa chỉ email của người phụ trách dữ liệu này. Lưu ý là địa chỉ email thay thế dấu @ bằng dấu chấm sau root.

- Dấu ( ) cho phép mở rộng ra viết thành nhiều dòng, tất cả các tham số trong dấu ( ) được dùng cho các Secondary Name Server.

Các thành phần bên trong cú pháp của record SOA:

+ Serial : áp dụng cho mọi dữ liệu trong zone và là 1 số nguyên. Trong ví dụ, giá trị này là 1 nhưng thông thường người ta sẽ sử dụng theo định dạng thời gian như

2007092001. Định dạng này theo kiểu yyyymmddnn, trong đó nn là số lần sửa đổi dữ liệu zone trong ngày. Bất kể theo định dạng nào thì luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu zone. Khi Secondary Name Server liên lạc với Primary Name Server thì trước tiên nó sẽ hỏi số serial này. Nếu số serial của máy Secondary nhỏ hơn số serial của máy Primary tức là dữ liệu trên Secondary đã cũ và sau đó máy Secondary sẽ sao chép dữ liệu mới từ máy Primary thay cho dữ liệu đang có.

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

+ Retry : nếu máy Secondary không kết nối được với máy Primary theo thời hạn mô tả trong refresh (ví dụ trường hợp máy Primary shutdown máy vào lúc đó) thì máy Secondary sẽ tìm cách kết nối lại với máy Primary theo chu kỳ thời gian được xác định trong retry. Thông thường giá trị này nhỏ hơn giá trị refresh

+ Expire : nếu sau khoản thời gian này mà máy Secondary không cập nhật được thông tin mới trên máy Primay thì giá trị của zone này trên máy Secondary sẽ bị hết hạn. Nếu bị expire thì Secondary sẽ không trả lời bất cứ 1 truy vấn nào về zone này. Giá trị expire này phải lớn hơn giá trị refresh và giá trị retry.

+ TTL : giá trị này áp dụng cho mọi record trong zone và được đính kèm trong thông tin trả lời 1 truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy DNS Server khác cache lại thông tin trả lời. Giúp giảm lưu lượng truy vấn DNS trên mạng.

b) NS (Name Server)

Record tiếp theo cần có trong zone là NS (Name Server) record. Mỗi Name Server cho zone sẽ có 1 NS record.

Cú pháp:

[domain-name] IN NS [DNS-Server-Name]

Ví dụ : Record NS sau :

vnnetpro.com. IN NS dnsserver1.vnnetpro.com.

vnnetpro.com. IN NS dnsserver2.vnnetpro.com.

chỉ ra rằng Domain vnnetpro.com có 2 Name Server là dnsserver1.vnnetpro.com và dnsserver2.vnnetpro.com

c) A (Address) và CNAME (Canonical Name)

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

Cú pháp : [tên-máy-tính] IN A [địa-chỉ-IP]

Ví dụ : record A trong tập tin db.vnnetpro

server1.vnnetpro.com. IN A 172.29.14.1

dns.vnnetpro.com. IN A 172.29.14.4

//Multi-homed hosts

server.vnnetpro.com. IN A 172.29.14.1

server.vnnetpro.com. IN A 192.253.253.1

d) AAAA

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

Cú pháp : [tên-máy-tính] IN AAAA [địa-chỉ-IPv6]

Ví dụ : Server IN AAAA 1243:123:456:7892:3:456ab

e) SRV

Cung cấp cơ chế định vị dịch vụ, Active Directory sử dụng resource record này để xác định Domain Controller, Global Catalog Servers, Lightweight Directory Access Protocol (LDAP) Server

Các thành phần trong SRV:

- Tên dịch vụ service
- Giao thức sử dụng
- Tên Domain (Domain Name)
- TTL và class
- Priority
- Weight (hỗ trợ Load Balancing)
- Port của dịch vụ
- target chỉ định FQDN cho host hỗ trợ dịch vụ.

Ví dụ : _ftp._tcp.somecompany.com. IN SRV 0 0 21 ftpsvr1.somecompany.com

_ftp._tcp.somecompany.com. IN SRV 10 0 21 ftpsvr1.somecompany.com

f) MX (Mail Exchange)

DNS dùng record MX trong việc chuyển mail lên mạng Internet. Ban đầu chức năng chuyển mail dựa trên 2 record : record MD (Mail Destination) và record MF (Mail Forwarder) records. MD chỉ ra đích cuối cùng của 1 thông điệp mail có tên domain cụ thể. MF chỉ ra máy chủ trung gian sẽ chuyển tiếp mail đến được máy chủ đích cuối cùng. Tuy nhiên việc tổ chức này hoạt động không tốt. Do đó, chúng được tích hợp lại thành 1 record là MX. Khi nhận được mail, trình chyển mail (mailer) sẽ dựa vào record MX để định đường đi của mail. Record MX sẽ chỉ ra 1 Mail Exchanger cho 1 miền – Mail Exchanger là 1 Server (chuyển mail đến mailbox local hay làm gateway chuyển sang 1 giao thức chuyển mail khác như UUCP) hoặc chuyển tiếp mail đến 1 Mail Exchanger khác (Mail Server trung gian) gần với mình nhất để đến với Server chủ cuối cùng dùng giao thức SMTP.

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

Cú pháp : [domain-name] IN MX [priority] [mail-host]

Ví dụ : vnnetpro.com. IN MX 10 mailserver.vnnetpro.com.

Chỉ ra máy chủ mailserver.vnnetpro.com là 1 Mail Exchanger cho Domain vnnetpro.com với độ ưu tiên là 10.

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

vnnetpro.com. IN MX 1 listo.vnnetpro.com.

vnnetpro.com. IN MX 1 hep.vnnetpro.com.

Trình chuyển mail (mailer) sẽ thử phân phát thư đến Mail Exchager có độ ưu tiên nhỏ nhất trước. Nếu không chuyển mail được thì Mail Exchanger với độ ưu tiên kế sẽ được chọn. Trong trường hợp có nhiều Mail Exchanger có cùng độ ưu tiên thì Mailer sẽ chọn ngẫu nhiên giữa chúng.

Chú ý : chỉ tạo MX record khi muốn nhận email từ bên ngoài Internet gửi vào Mail Exchanger của hệ thống. Khi có email đến thì nó sẽ hỏi xem DNS Server là Mail Server của hệ thống này có địa chỉ IP là gì? Lúc này DNS Server sẽ trả lời câu hỏi này bằng cách tìm thông tin trong MX record. Lúc đó DNS Server sẽ forward đến Mail Server. Các User trong local sẽ lên Mail Server lấy mail về bằng cơ chế POP3.

II. Trình tự thực hiện

1. Yêu cầu thực hiện

+ Cài đặt dịch vụ DNS trên máy CTM-SRV12.

+ Cấu hình dịch vụ DNS.

+ Cấu hình các bản ghi : A, PTR, CNAME, MX….

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

3. Các bước thực hiện

Thực hiện triển khai cài đặt và cấu hình dịch vụ DNS Server thông qua 3 bước sau:

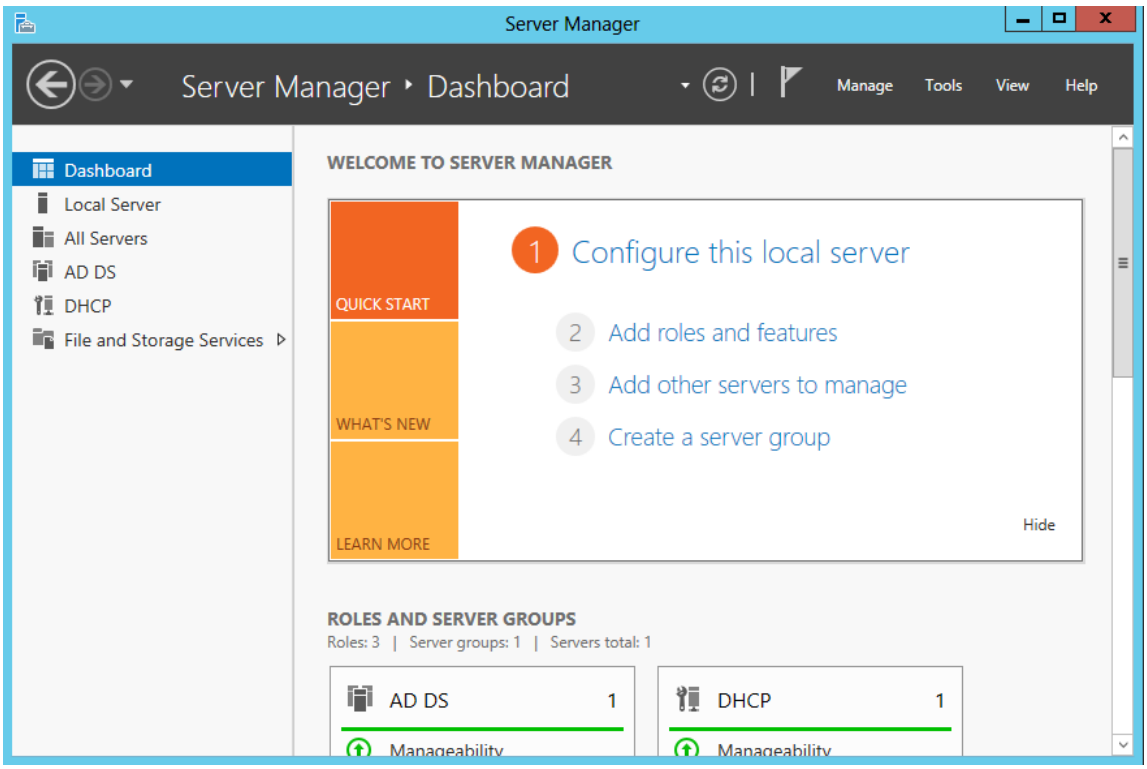
- Bước 1: Cài đặt dịch vụ DNS Server
- Bước 2: Cấu hình dịch vụ DNS
- Bước 3: Cấu hình tạo bản ghi cho máy CTM-SRV12.

Hướng dẫn chi tiết:

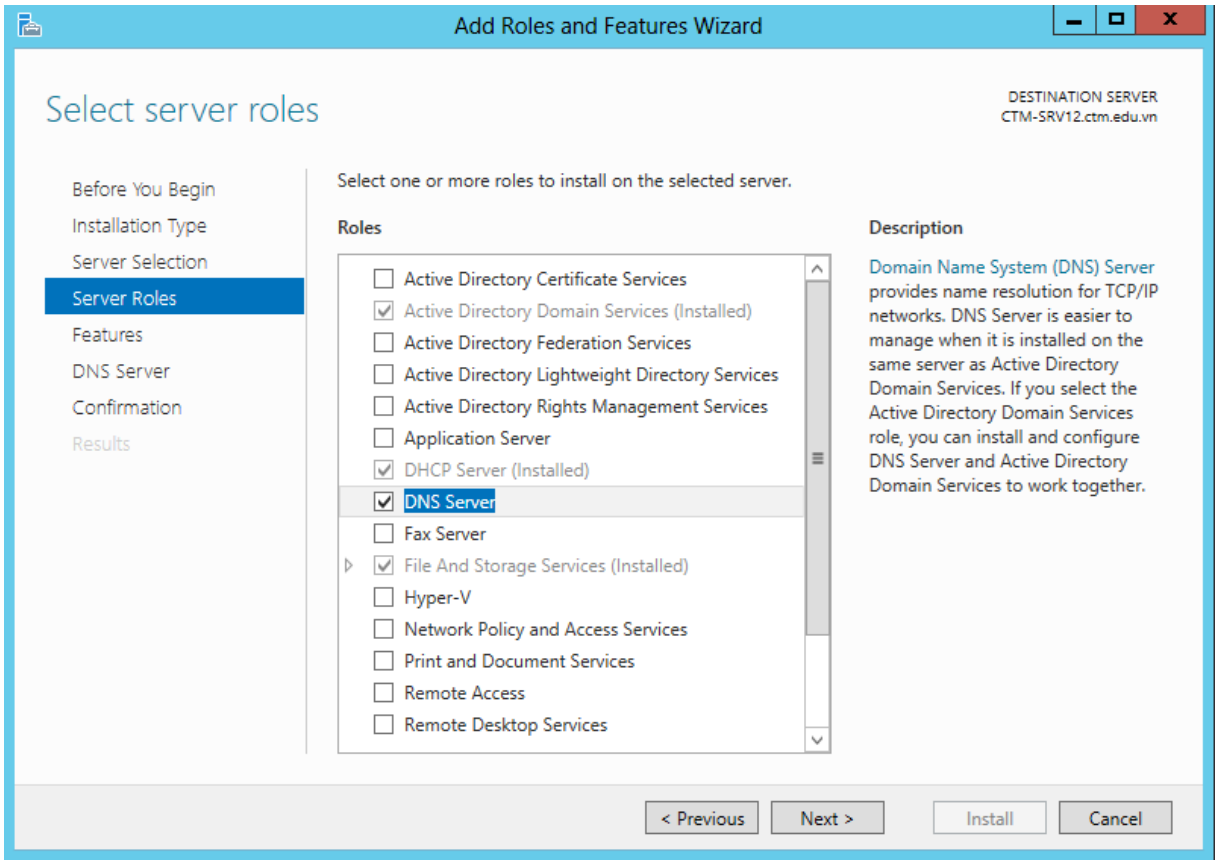
Bước 1: Cài đặt dịch vụ DNS Server

Thực hiện trên máy CTM-SRV12:

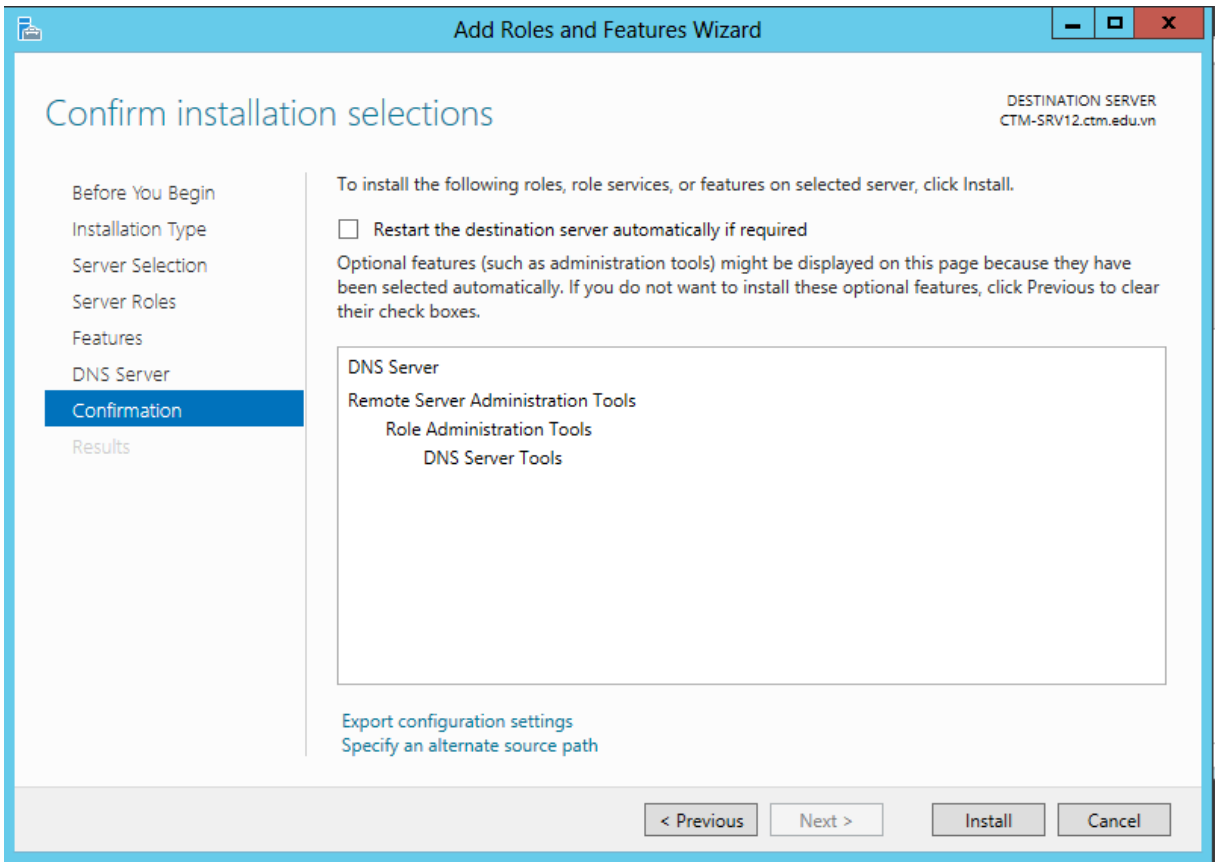
Vào ***Server Manager /Add roles and features***



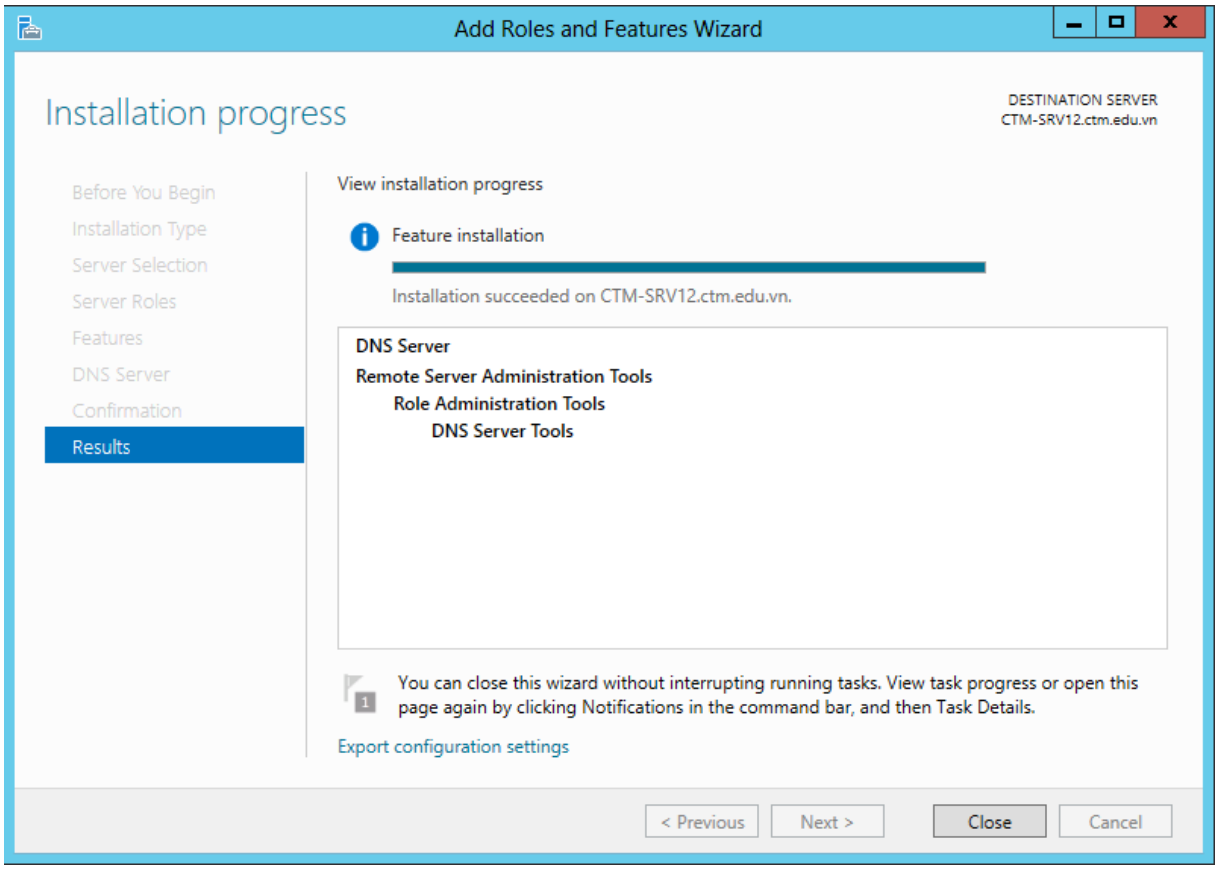
Tại cửa sổ ***Select server roles*** , click chọn vào dịch vụ ***DNS***



Tiếp tục click vào ***Next***, tại cửa sổ ***Confirm installation selections***, click vào ***Install*** để Server cài đặt dịch vụ **DNS**

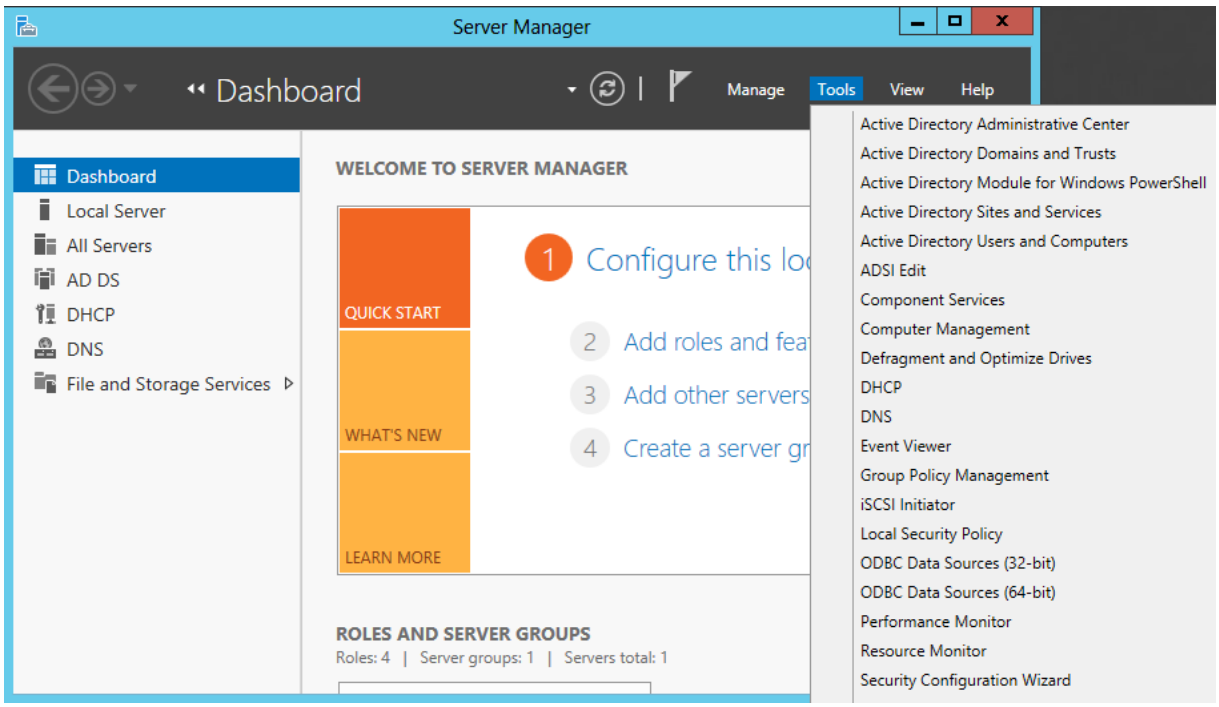


Tại cửa sổ ***Installation progress***, click vào ***Close*** để kết thúc quá trình cài đặt

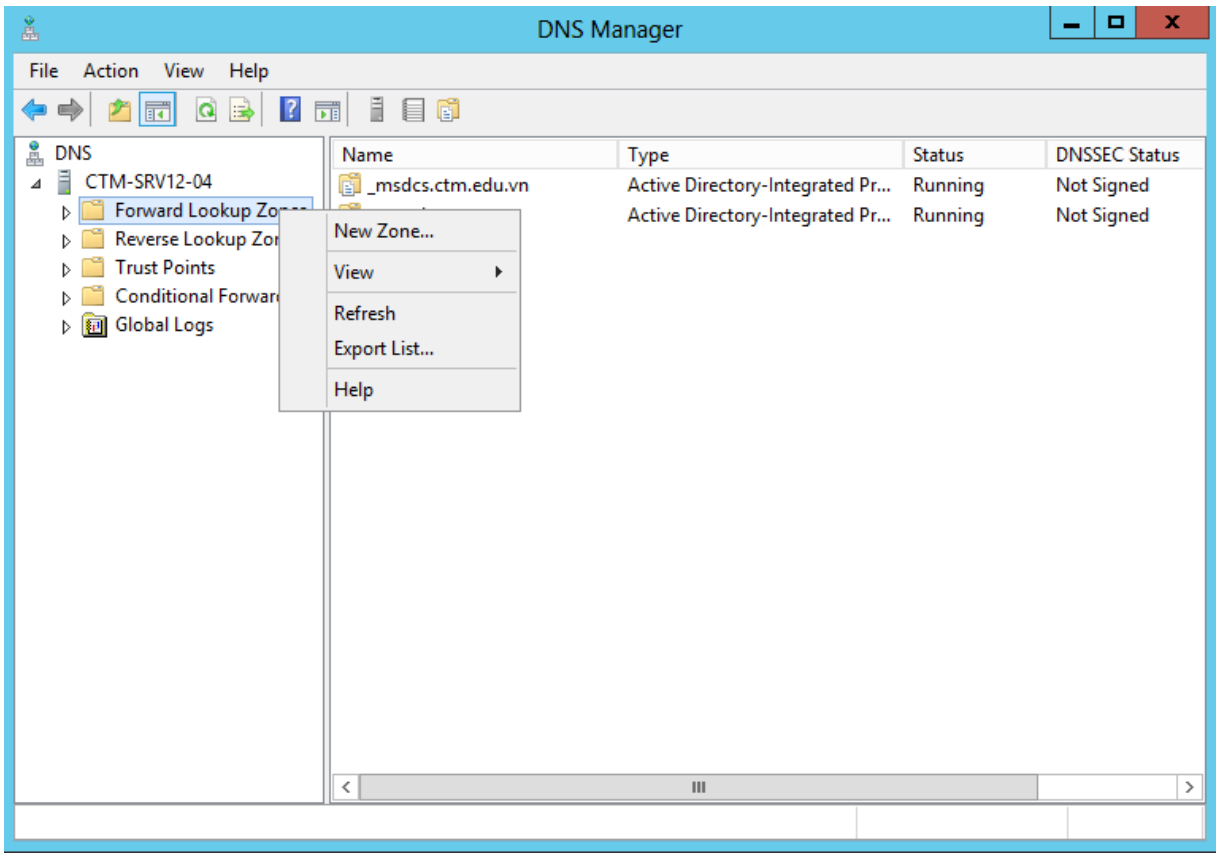


Bước 2: Cấu hình dịch vụ DNS:

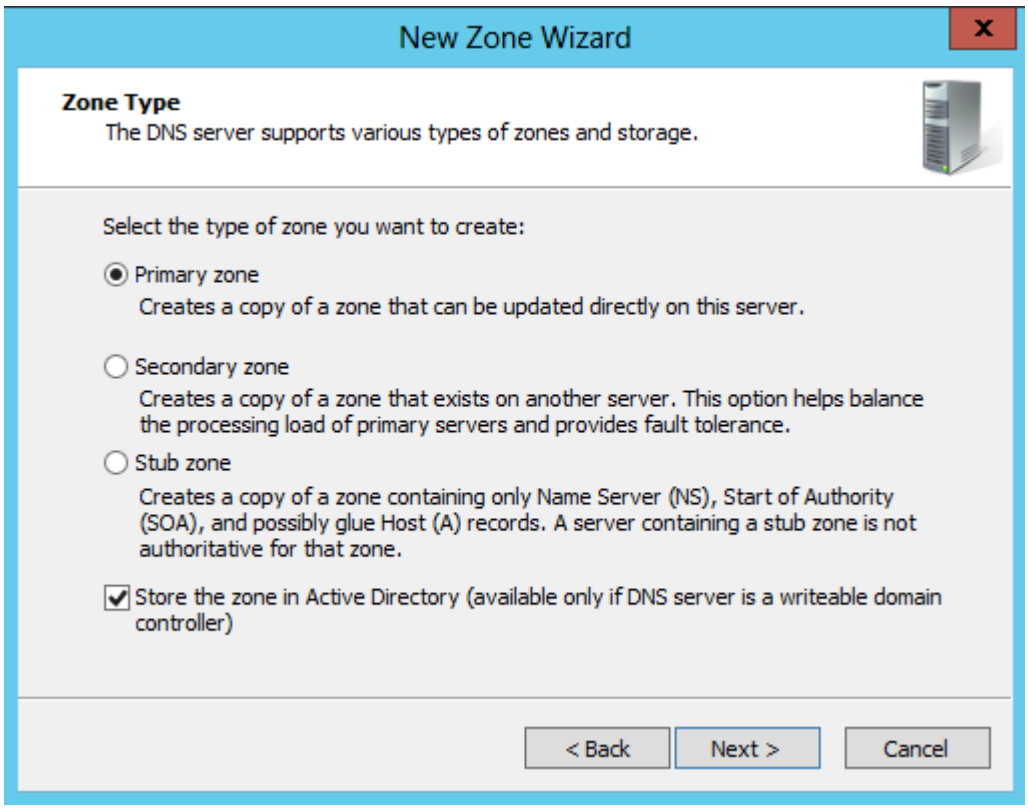
Vào ***Server Manager / Tools*** / chọn vào dịch vụ **DNS**



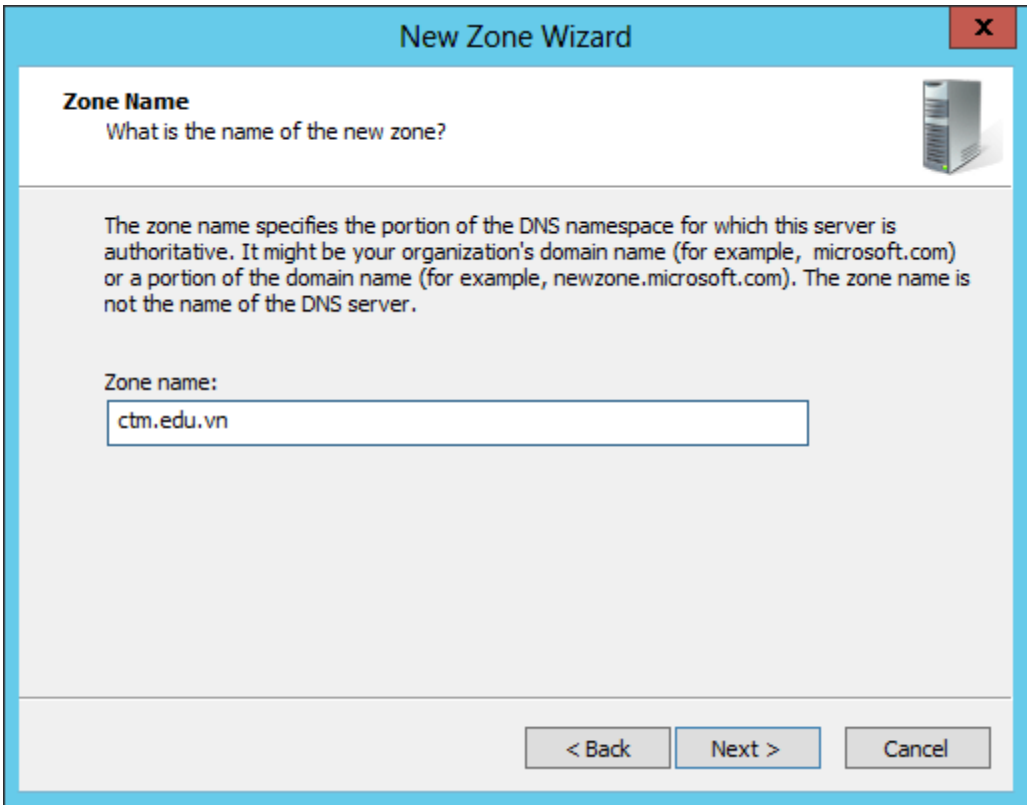
Click chuột phải tại ***Forward Lookup Zones*** chọn ***New Zone…***



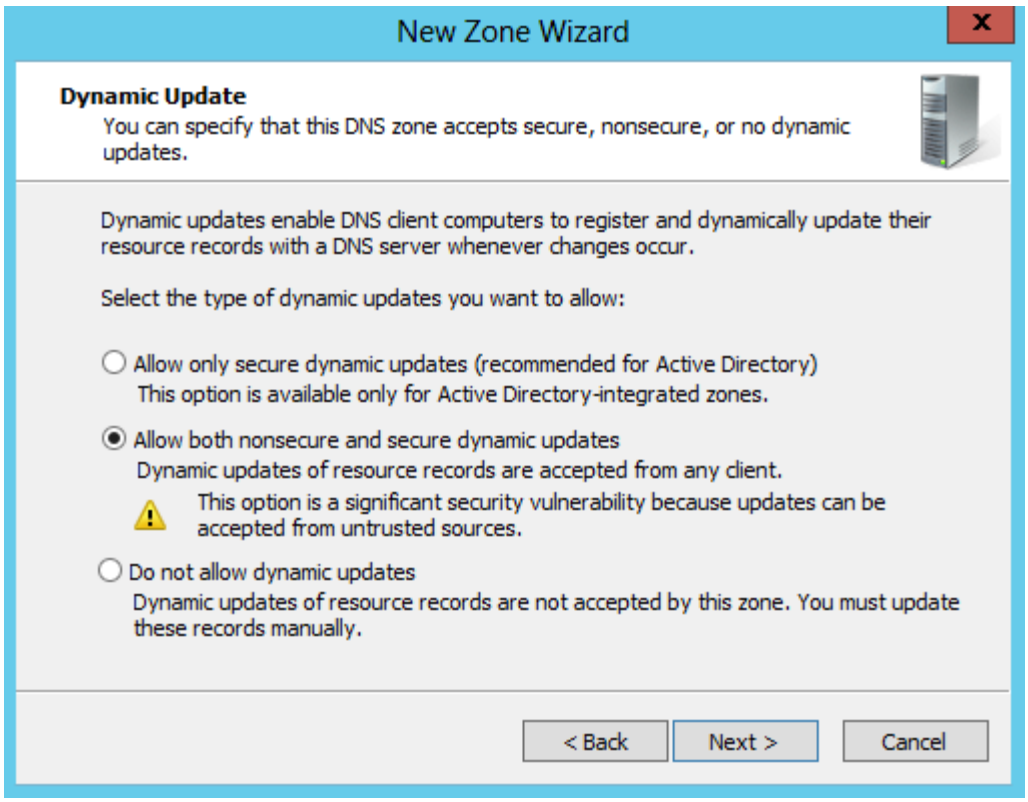
Tại cửa sổ ***Zone Type***, chọn vào ***Primary zone***



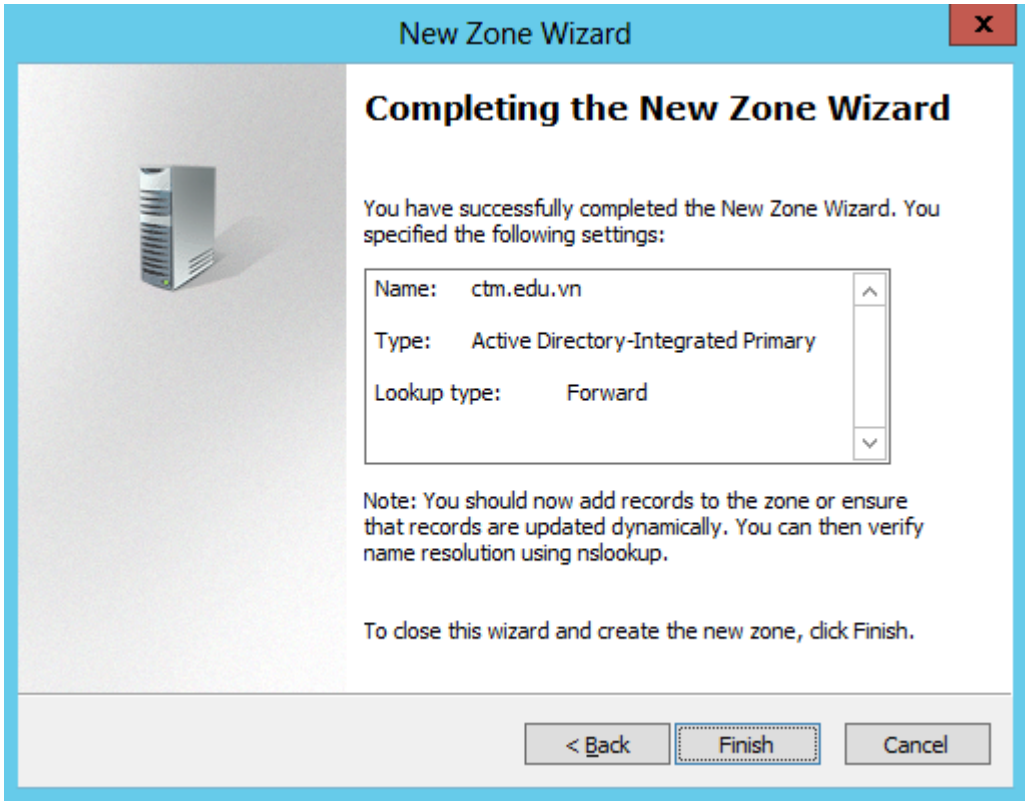
Tại cửa sổ ***Zone Name***, nhập vào tên miền: *ctm.edu.vn*



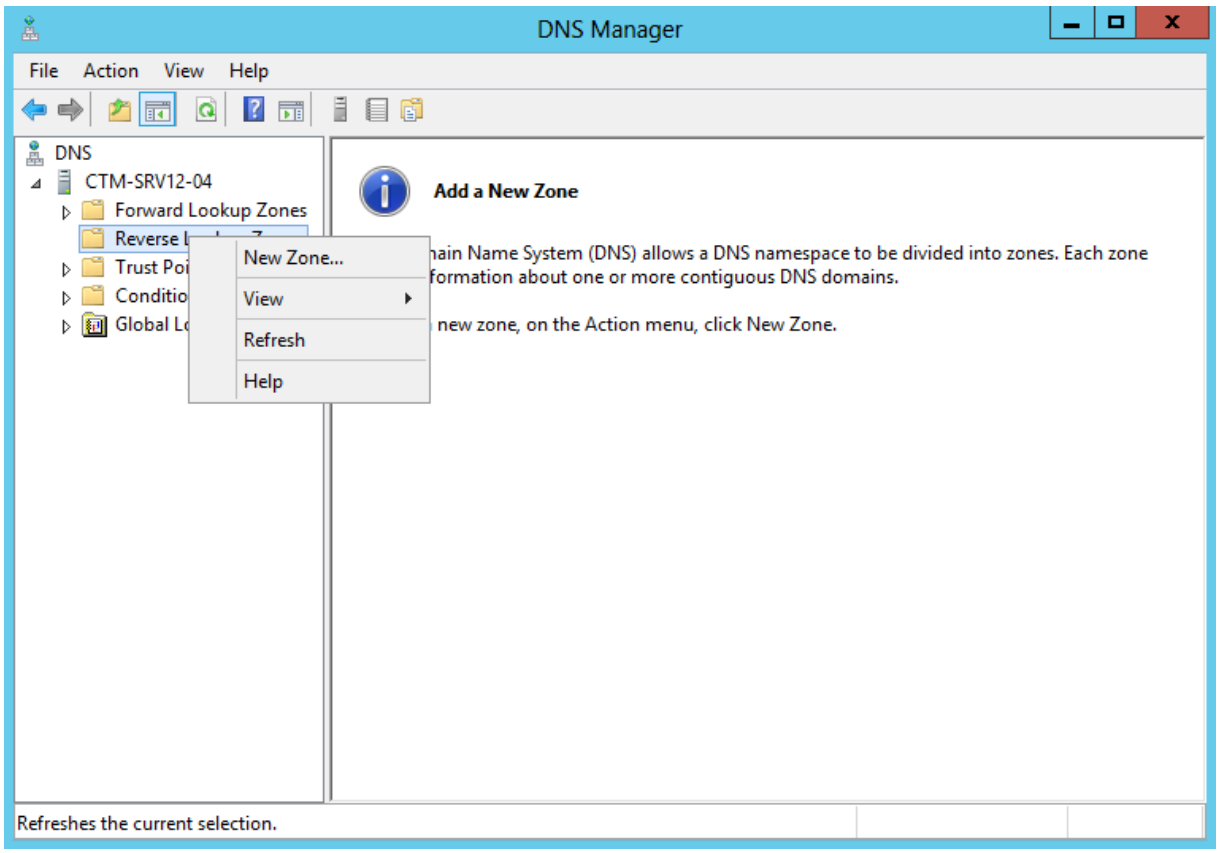
Tiếp tục click vào ***Next***, tại cửa sổ ***Dynamic Update***, chọn vào ***Allow both nonsecure and secure dynamic updates***



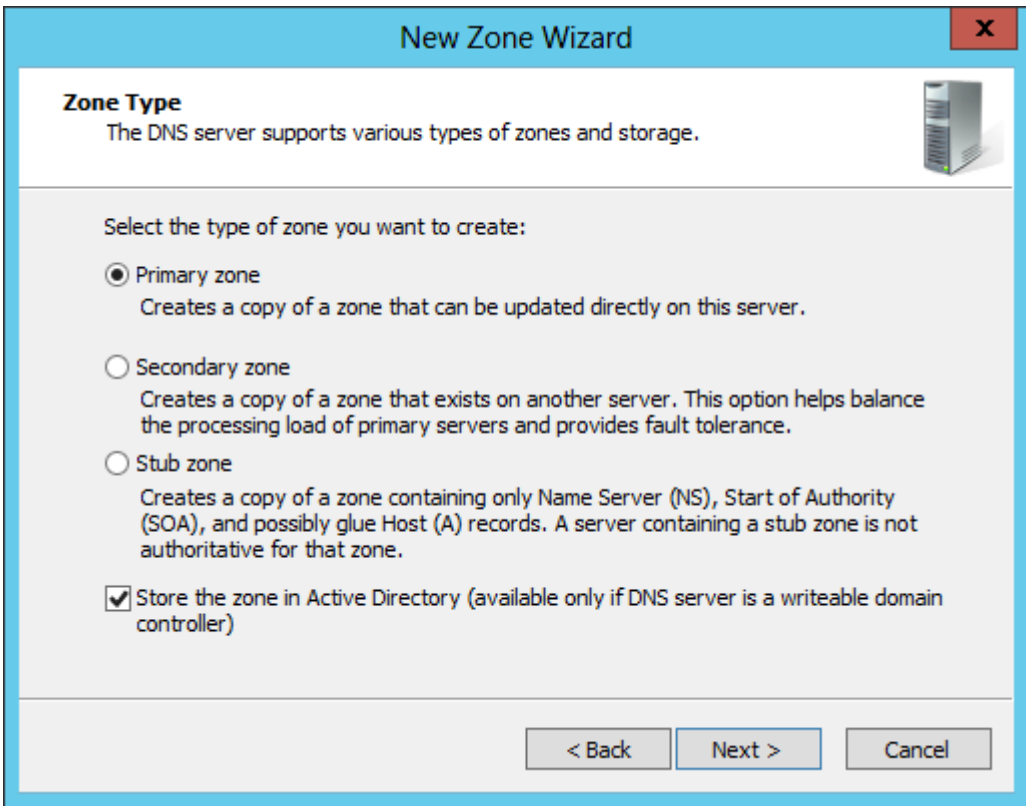
Click vào ***Finish*** để kết thúc quá trình cài đặt



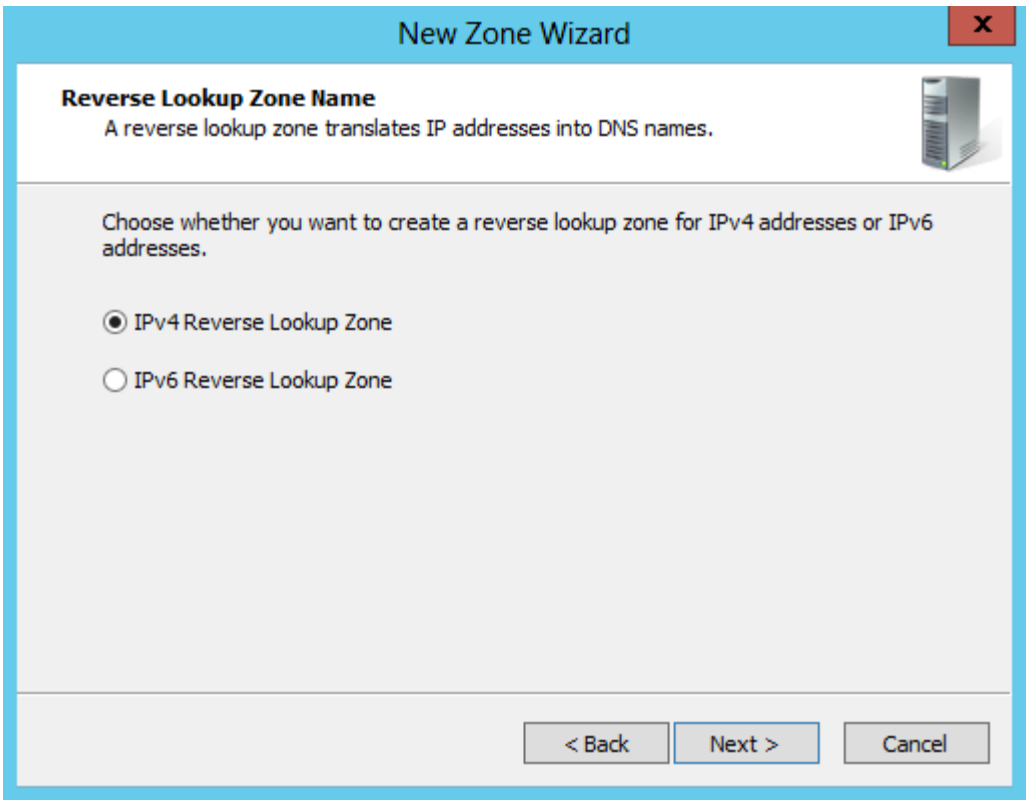
Click chuột phải tại ***Reverse Lookup Zones***, chọn vào ***New Zone***



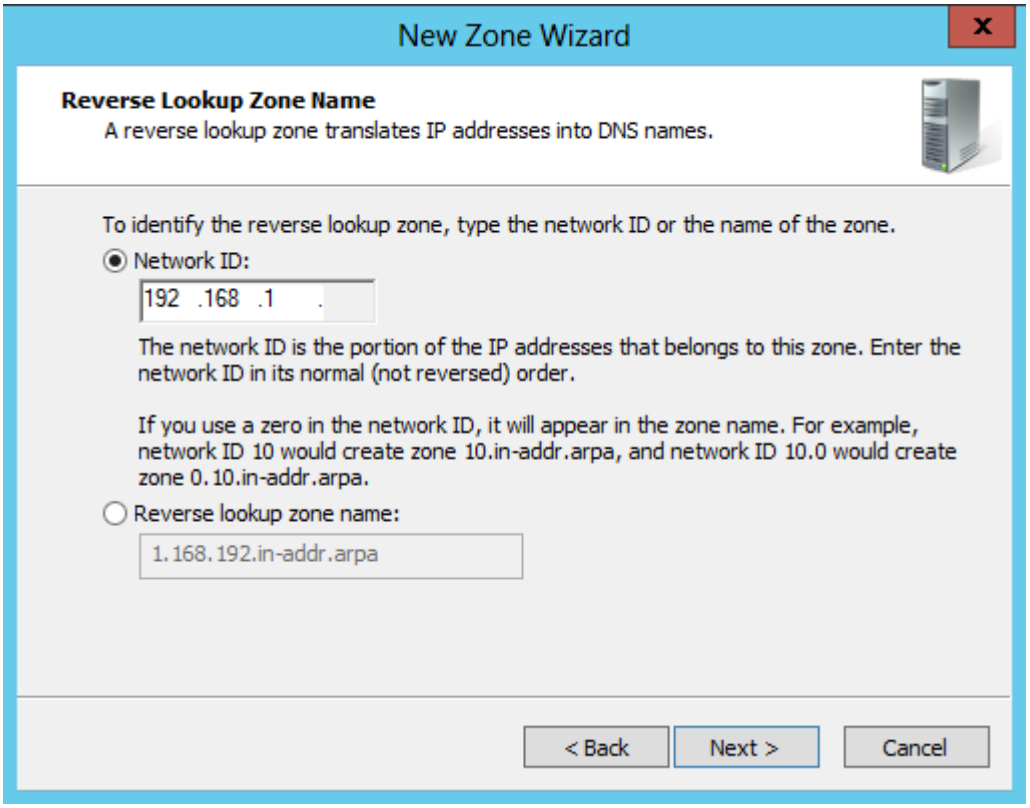
Tại cửa sổ ***Zone Type***, click chọn vào ***Primary zone***



Tại cửa sổ ***Reverse Lookup Zone Name***, click chọn vào ***IPv4 Reverse Lookup Zone***

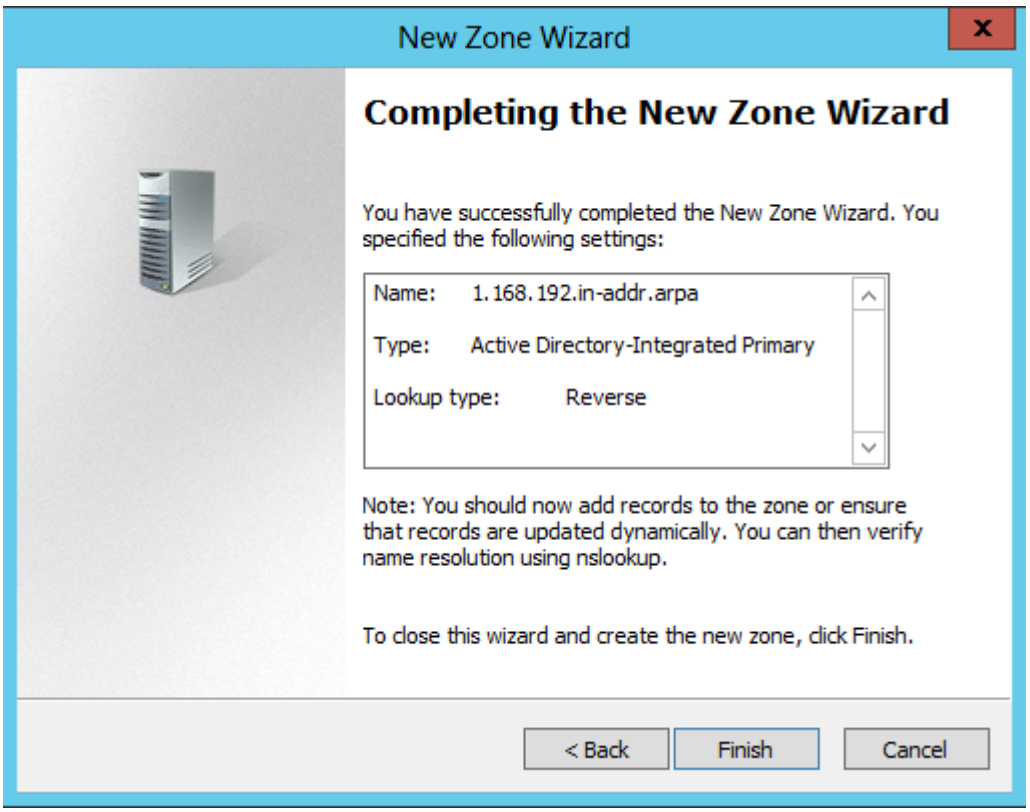


Tại cửa sổ ***Reverse Lookup Zone Name***, nhập vào ***Network ID*** :*192.168.1*



Tại cửa sổ ***Dynamic Update***, chọn vào ***Allow both nonsecure and secure dynamic updates***

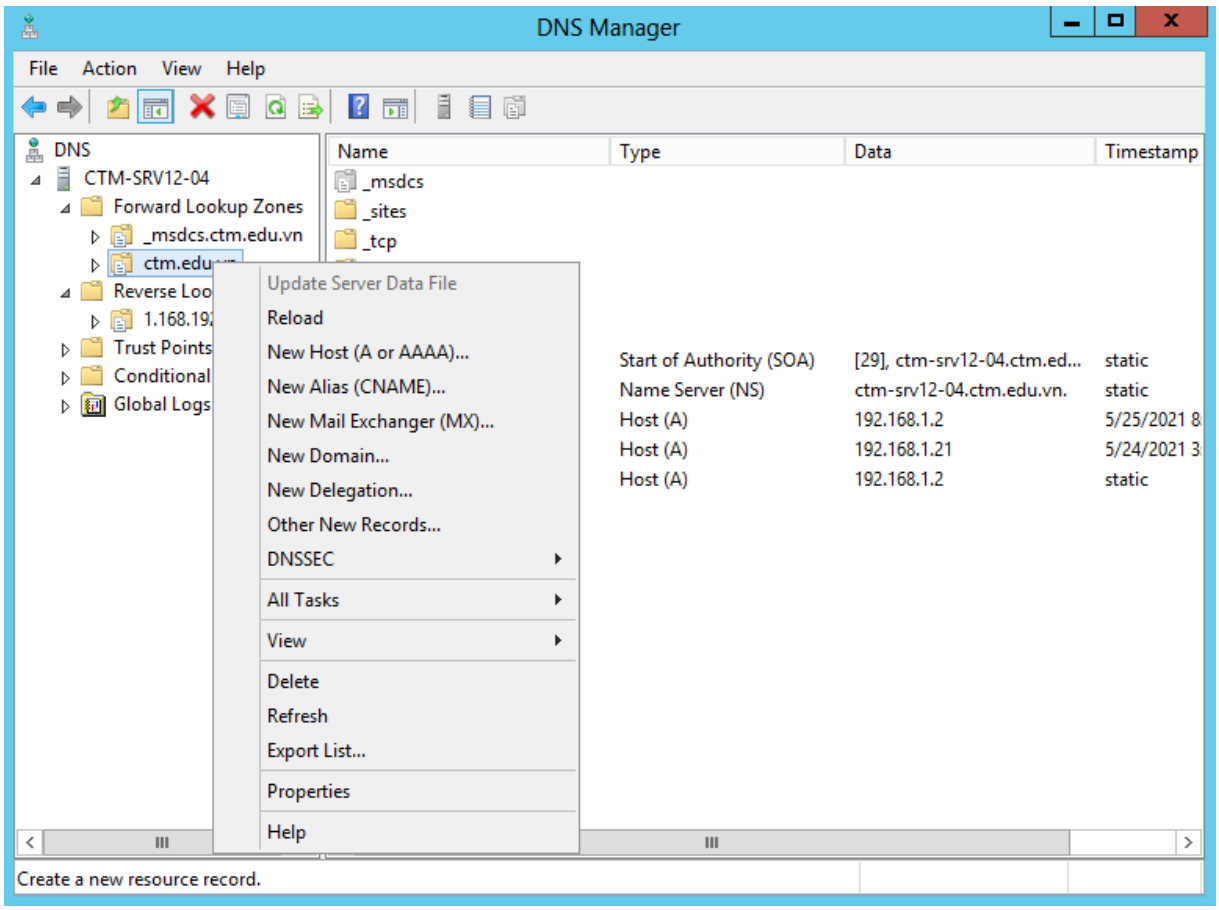
Tại cửa số tiếp theo, click chọn vào ***Finish*** để kết thúc quá trình cài đặt dịch vụ DNS



Bước 3: Cấu hình tạo bản ghi cho máy CTM-SRV12:

Click vào tên miền *ctm.edu.vn*

Click chuột phải chọn ***New Host (A or AAAA)***

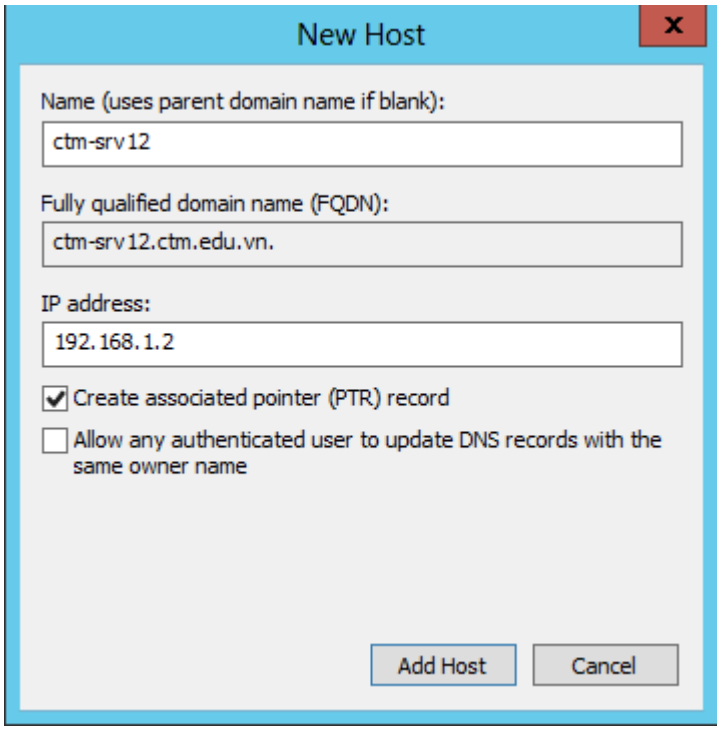


Tại cửa sổ ***New Host***:

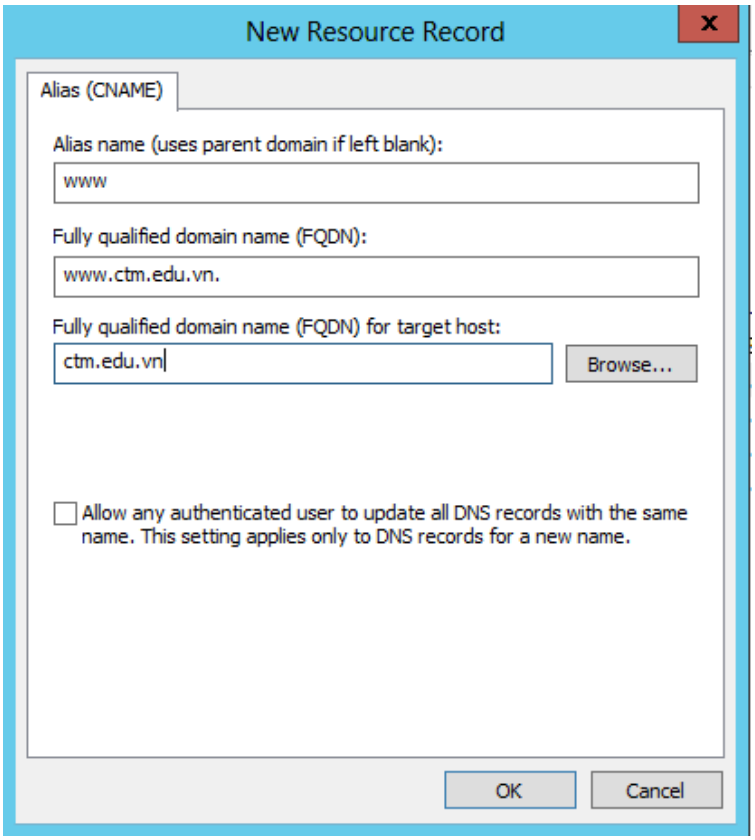
Name (users parent domain name if blank): *CTM-SRV12*

IP address : *192.168.1.2*

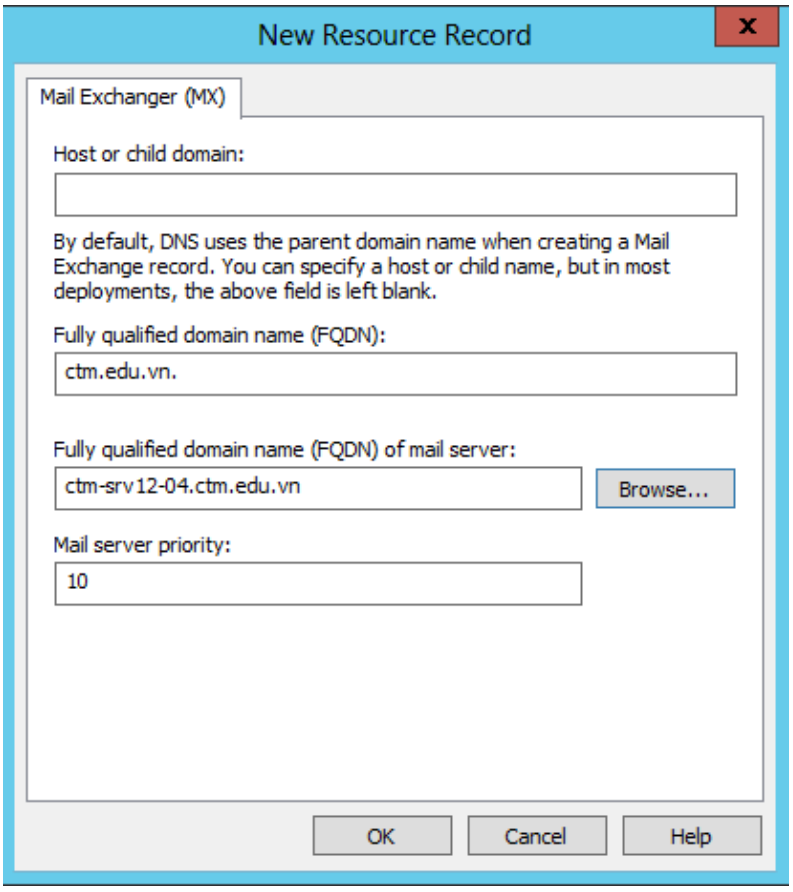
Click tại ***Create associated pointer (PTR) record***. (để máy tự động tạo bản ghi PTR)



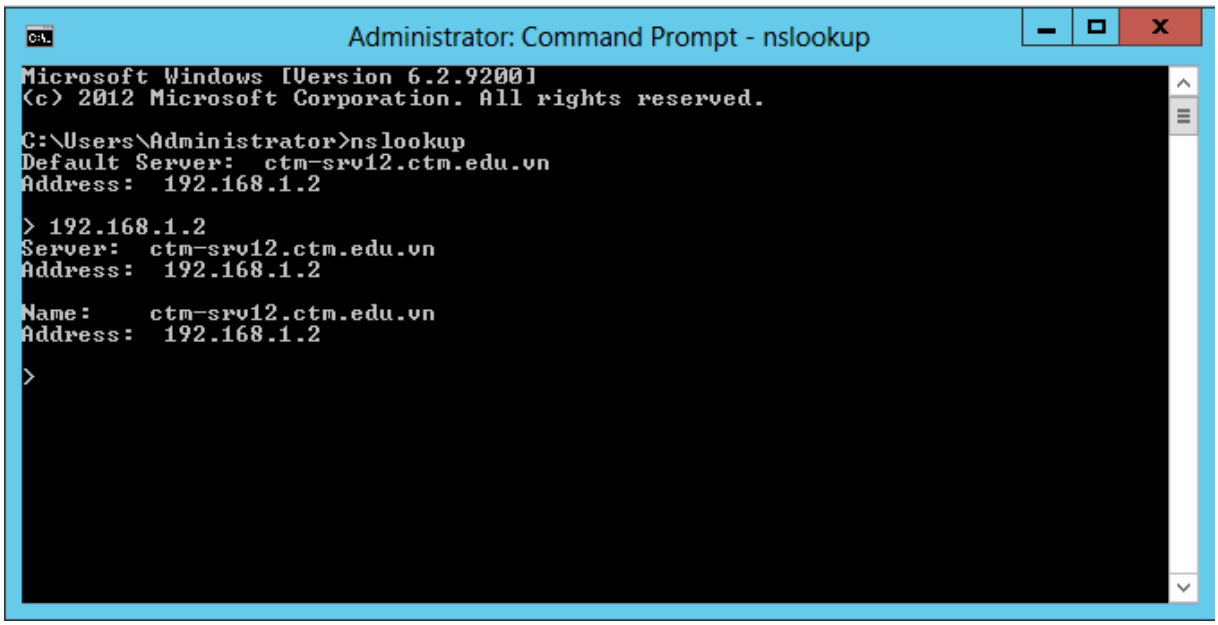
Tạo bản ghi ***CNAME***, nhập *www*



Tạo bản ghi ***Mail Exchanger (MX)***



Chuyển sang máy CTM-WRK07. Vào cmd, gõ lệnh ***nslookup*** để kiểm tra phân giải IP sang tên miền và ngược lại.



III. Sai hỏng và cách khắc phục

1. Cài đặt dịch vụ DNS không thành công

- Nguyên nhân
  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Cách khắc phục
  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành

2. Cấu hình dịch vụ DNS không thành công

- Nguyên nhân
  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Cách khắc phục
  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành

3. Thực hiện lệnh nslookup trên cmd có kết quả Default Server là Unknow

- Nguyên nhân
  - Thiết lập DNS server IPv6 của card mạng chưa đúng
- Cách khắc phục
  - Thiết lập DNS server IPv6 của card mạng là Obtain DNS server address automatically

V. Hướng dẫn ôn luyện

- Cài đặt dịch vụ DNS
- Cấu hình dịch vụ DNS
- Tạo bản ghi DNS

BÀI 7: TRIỂN KHAI DỊCH VỤ WEB VỚI IIS

I. Lý thuyết liên quan

1. Máy chủ Web (Web Server)

Web Server là máy chủ có dung lượng lớn, tốc độ cao, được dùng để lưu trữ thông tin như một ngân hàng dữ liệu, chứa những website đã được thiết kế cùng với những thông tin liên quan khác (các mã Script, các chương trình, và các file Multimedia).

Web Server có khả năng gửi đến máy khách những trang Web thông qua môi trường Internet (hoặc Intranet) qua giao thức HTTP, giao thức được thiết kế để gửi các file đến trình duyệt Web (Web Browser), và các giao thức khác.

Tất cả các Web Server đều có một địa chỉ IP (IP Address) hoặc cũng có thể có một Domain Name. Giả sử khi người sử dụng đánh vào thanh Address trên trình duyệt của máy một dòng http://www.abc.com sau đó gõ phím Enter, khi đó người sử dụng đã gửi một yêu cầu đến một Server có Domain Name là www.abc.com. Server này sẽ tìm trang Web có tên là index.htm rồi gửi nó đến trình duyệt của người sử dụng.

Bất kỳ một máy tính nào cũng có thể trở thành một Web Server bởi việc cài đặt lên nó một chương trình phần mềm Server Software và sau đó kết nối vào Internet.

Khi máy tính kết nối đến một Web Server và gửi đến yêu cầu truy cập các thông tin từ một trang Web nào đó, Web Server Software sẽ nhận yêu cầu và gửi lại những thông tin mà người sử dụng mong muốn.

Web Server Software cũng chỉ là một ứng dụng phần mềm. Web Server Software được cài đặt, và chạy trên máy tính dùng làm Web Server, nhờ có chương trình này mà người sử dụng có thể truy cập đến các thông tin của trang Web từ một máy tính khác ở trên mạng (Internet, Intranet).

Web Server Software còn có thể được tích hợp với CSDL (Database), hay điều

khiển việc kết nối vào CSDL để có thể truy cập và kết xuất thông tin từ CSDL lên các trang Web và truyền tải chúng đến người dùng.

Tất cả các Web Server đều hiểu và chạy được các file *.htm và *.html, tuy nhiên mỗi Web Server lại phục vụ một số kiểu file chuyên biệt chẳng hạn như IIS của Microsoft dành cho *.asp, *.aspx...; Apache dành cho *.php...; Sun Java System Web Server dành cho *.jsp...

Phần lớn các Web server sử dụng cổng 80, nhưng cũng có thể thay đổi để Webserver có thể cài đặt trên cổng không tiêu chuẩn nếu muốn "dấu" Web server như là một Web server đa host trên một máy tính bằng việc ánh xạ mỗi server cho một cổng khác nhau.

2. Giao thức HTTP

HTTP là chữ viết tắt từ HyperText Transfer Protocol (giao thức truyền tải siêu văn bản). Nó là giao thức cơ bản mà World Wide Web sử dụng. HTTP xác định cách các thông điệp (các file văn bản, hình ảnh đồ hoạ, âm thanh, video, và các file multimedia khác) được định dạng và truyền tải ra sao, và những hành động nào mà các Web server (máy chủ Web) và các trình duyệt Web (browser) phải làm để đáp ứng các lệnh rất đa dạng. Chẳng hạn, khi gõ một địa chỉ Web URL vào trình duyệt Web, một

lệnh HTTP sẽ được gửi tới Web server để ra lệnh và hướng dẫn nó tìm đúng trang Web được yêu cầu và kéo về mở trên trình duyệt Web. Nói cách khác, HTTP là giao thức truyền tải các file từ một Web server vào một trình duyệt Web để người dùng có thể xem một trang Web đang hiện diện trên Internet.HTTP là một giao thức ứng dụng của bộ giao thức TCP/IP (các giao thức nền tảng cho Internet).

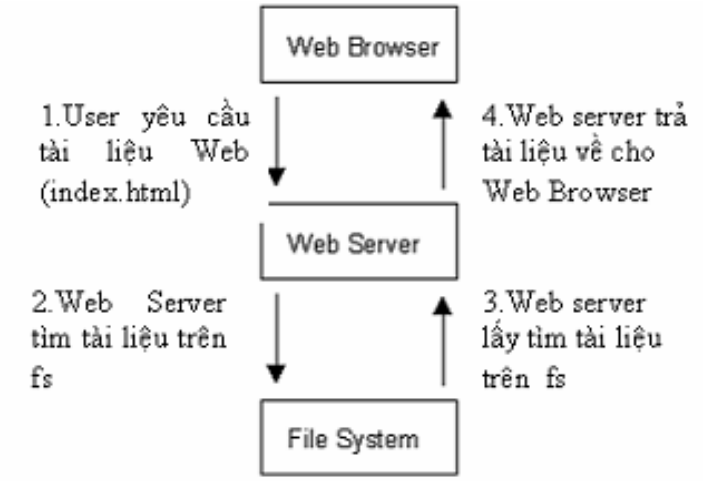
Có một tiêu chuẩn chính khác cũng điều khiển cách thức World Wide Web làm việc là HTML (HyperText Markup Language, ngôn ngữ đánh dấu siêu văn bản), có chức năng quản lý cách thức mà các trang Web được định dạng và hiển thị.

Người ta gọi HTTP là một giao thức "phi trạng thái" (stateless) bởi vì mỗi lệnh đều được thực thi một cách độc lập, lệnh sau không biết bất cứ điều gì về các lệnh đã đến trước mình. Đây chính là một hạn chế, khiếm khuyết của HTTP. Nó là nguyên nhân chính của tình trạng rất khó thực thi các trang Web có khả năng phản ứng thông minh đối với lệnh mà người dùng nạp vào. Và sự hạn chế này đang được các nhà phát triển khắc phục trong các công nghệ mới như ActiveX, Java, JavaScript và cookies.

Phiên bản mới nhất của HTTP là 1.1. So với phiên bản nguyên thủy (HTTP 1.0), phiên bản mới này truyền tải các trang Web nhanh hơn và giảm tình trạng tắc nghẽn giao thông Web.

3. Nguyên lý hoạt động của Web Server

Khi gõ địa chỉ trang web "*http://www.abc.com/*" vào trình duyệt web và nhấn Enter, trang web hiển thị ngay trên màn hình. Các bước cơ bản trong tiến trình truyền tải trang web đến màn hình người dùng bằng cơ chế hoạt động của Web server được thể hiện theo mô hình sau:



Hình 2.5.1 Tiến trình truyền tải web

Theo mô hình trên, trình duyệt web thực hiện một kết nối tới máy chủ web, yêu cầu một trang web và nhận lại nó. Sau đây, là thứ tự từng bước cơ bản xảy đến đằng sau màn hình:

Trình duyệt web tách địa chỉ website làm 3 phần:

- Phần giao thức: ("http")
- Máy chủ tên miền: (www.abc.com)
- Tên tệp: ("index.htm")

Trình duyệt liên hệ với máy chủ tên miền để chuyển đổi tên miền "www.abc.com" ra địa chỉ IP (Internet Protcol).

Sau đó, trình duyệt sẽ gửi tiếp một kết nối tới máy chủ có địa chỉ IP tương ứng qua cổng 80.

Dựa trên giao thức HTTP, trình duyệt gửi yêu cầu GET đến máy chủ, yêu cầu tệp "http://www.abc.com/index.htm" (cookies cũng sẽ được gửi kèm theo từ trình duyệt web đến máy chủ).

Tiếp đến, máy chủ sẽ gửi đoạn text dạng HTML đến trình duyệt web máy đã gởi yêu cầu (cookies cũng được gửi kèm theo từ máy chủ tới trình duyệt web, cookies được ghi trên đầu trang của mỗi trang web).

Trình duyệt web đọc các thẻ HTML, định dạng trang web và kết xuất ra màn hình.

4. Web Client

Web Client là giao diện phía người dùng đầu cuối (Client), dùng để tạo ra giao diện tương tác của người dùng đối với ứng dụng Web (User Interface).

Các công nghệ/ ngôn ngữ lập trình hỗ trợ cho WebClient

- Công nghệ: PhotoShop, Flash, Silver Light (Microsoft)v.v…
- Ngôn ngữ: html, css, javascript v.v…

Để đọc được các trang Web của ứng dụng Web trên máy người dùng phải cài các Web Client hay còn gọi là trình duyệt (Browser), ví dụ : FireFox, IE, Chrome, Coccoc (VN) v.v….

5. Các Web Server thông dụng

a) Web Server Apache

Apache hay là chương trình máy chủ HTTP là một chương trình dành cho máy chủ đối thoại qua giao thức HTTP. Apache chạy trên các hệ điều hành tương tự như Unix, Microsoft Windows, Novell Netware và các hệ điều hành khác. Apache đóng một vai trò quan trọng trong quá trình phát triển của mạng web thế giới (World Wide Web).

Apache được phát triển và duy trì bởi một cộng đồng mã nguồn mở dưới sự bảo trợ của Apache Software Foundation. Apache được phát hành với giấy phép Apache License và là một phần mềm tự do và miễn phí.

b) IIS – Internet Information Services

Microsoft Internet Information Services (các dịch vụ cung cấp thông tin Internet) là các dịch vụ dành cho máy chủ chạy trên nền Hệ điều hành Window nhằm cung cấp và phân tán các thông tin lên mạng, nó bao gồm nhiều dịch vụ khác nhau như Web Server, FTP Server,...

Nó có thể được sử dụng để xuất bản nội dung của các trang Web lên Internet/Intranet bằng việc sử dụng “Phương thức chuyển giao siêu văn bản -Hypertext Transport Protocol (HTTP)”.

c) Sun Java System Web Server (JSWS)

Sun Java System Web Server (JSWS) được phát triển dựa trên chương trình máy chủ web NCSA và được biết đến dưới một số tên như Sun ONE, Netscape Enterprise Server, và iPlanet Enterprise Server. Phần mềm của Sun cũng hoạt động được trên nhiều hệ điều hành như: HP_UX, Solaris và cả Windows. Cũng như phần lớn các chương tình máy chủ khác, Sun JSWS hỗ trợ phát triển các ứng dụng động cho các ứng dụng.

II. Trình tự thực hiện

1. Yêu cầu thực hiện

+ Cài đặt dịch vụ Web Server

+ Cấu hình dịch vụ Web

+ Xuất bản một website

+ Truy cập website tại máy Client

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

3. Các bước thực hiện

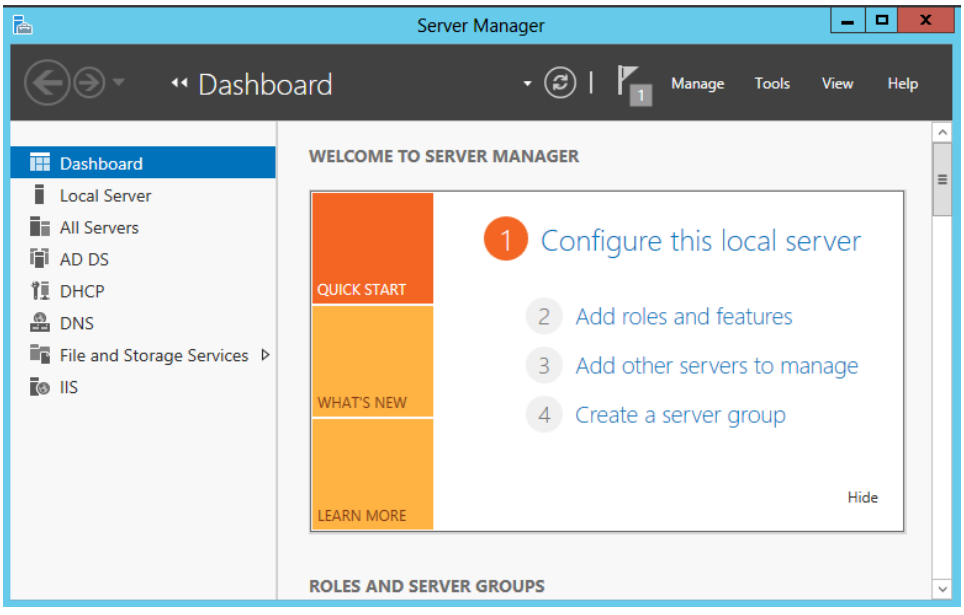
Thực hiện triển khai cài đặt và cấu hình dịch vụ Web Server thông qua 3 bước sau:

- Bước 1: Cài đặt dịch vụ Web Server
- Bước 2: Cấu hình dịch vụ Web
- Bước 3: Xuất bản một website
- Bước 4: Truy cập website tại máy Client.

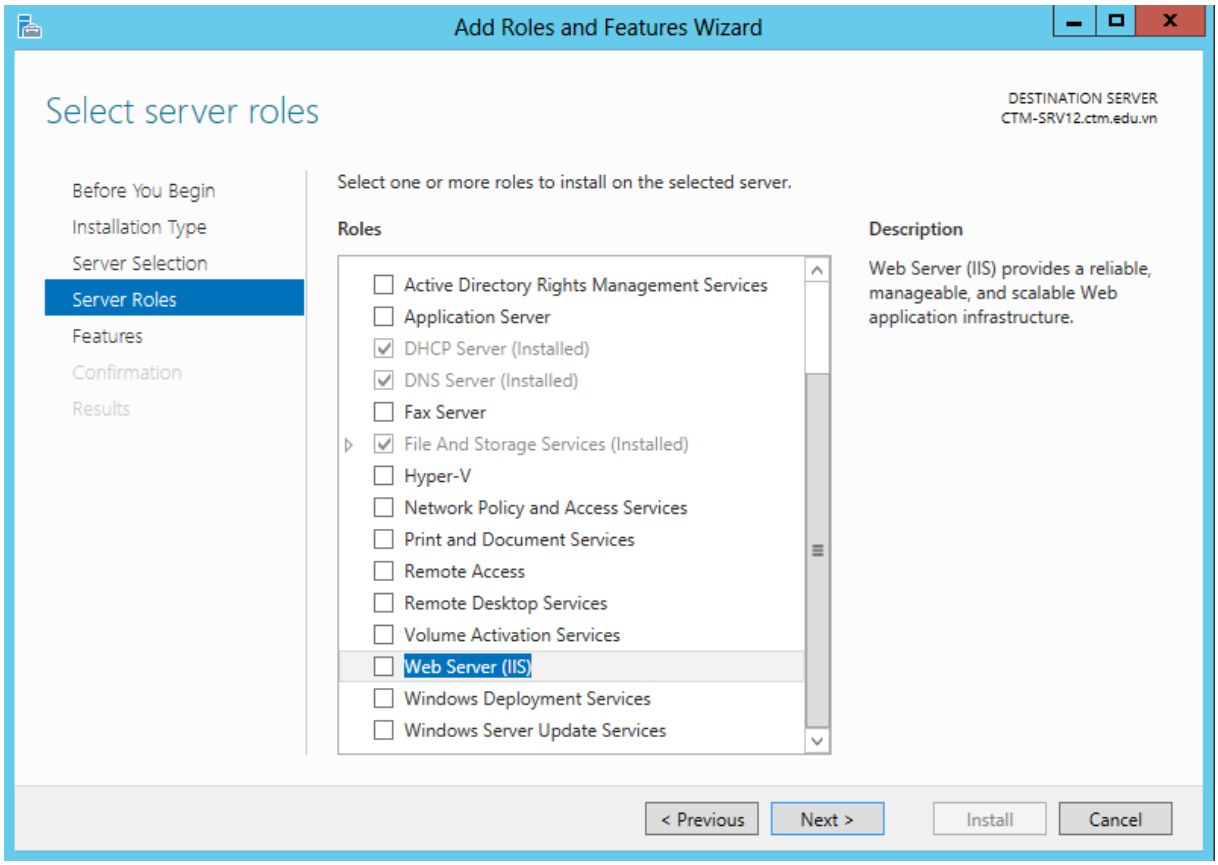
Hướng dẫn chi tiết:

Bước 1: Cài đặt dịch vụ Web Server

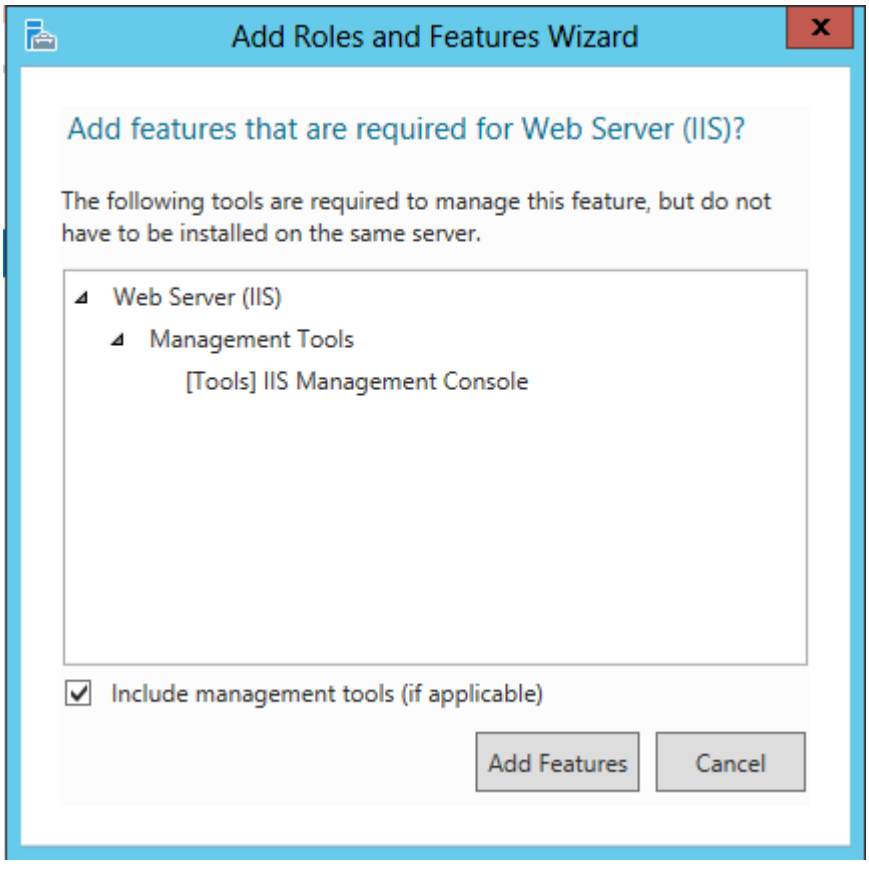
Tại ***Server Manager*** chọn ***Add roles and features***



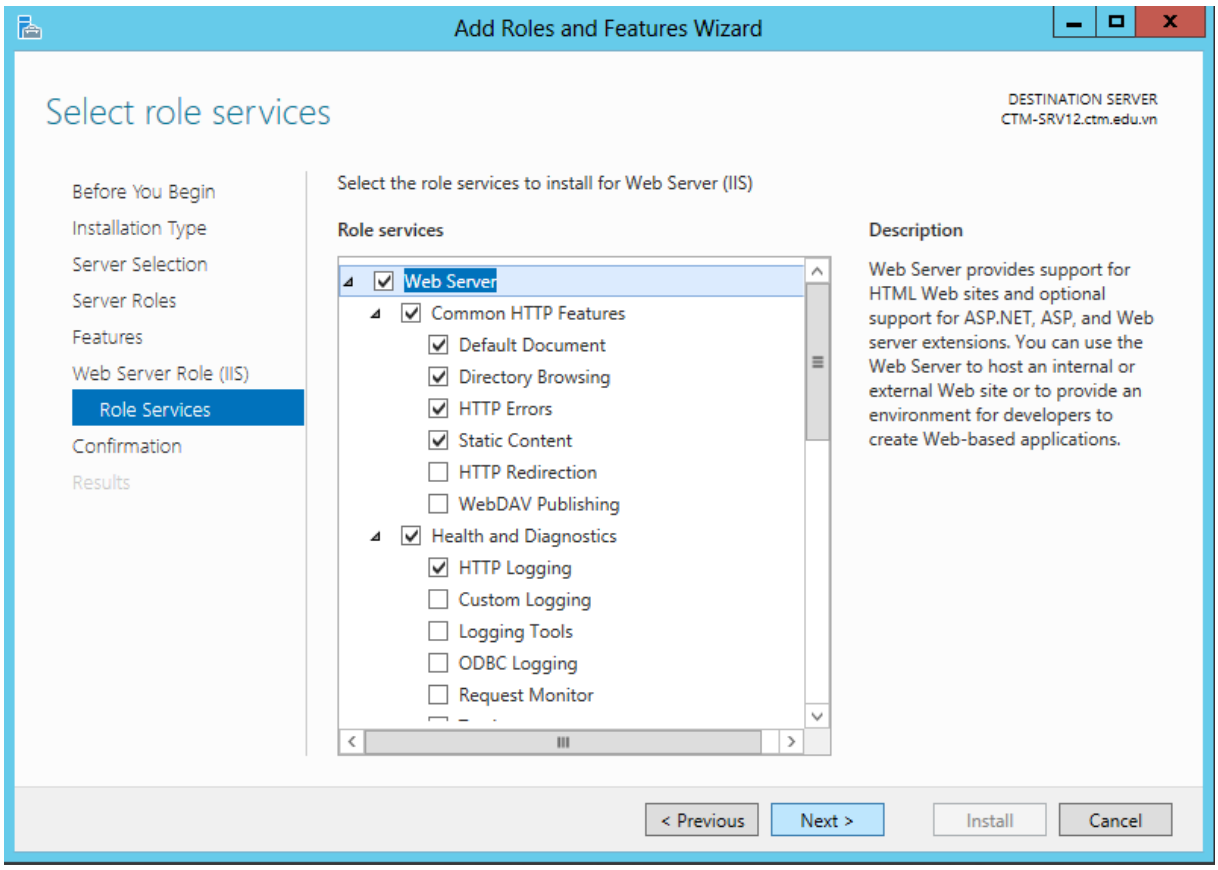
Click ***Next*** => ***Server Roles*** chọn ***Web Server (IIS)*** => Click ***Add Features***



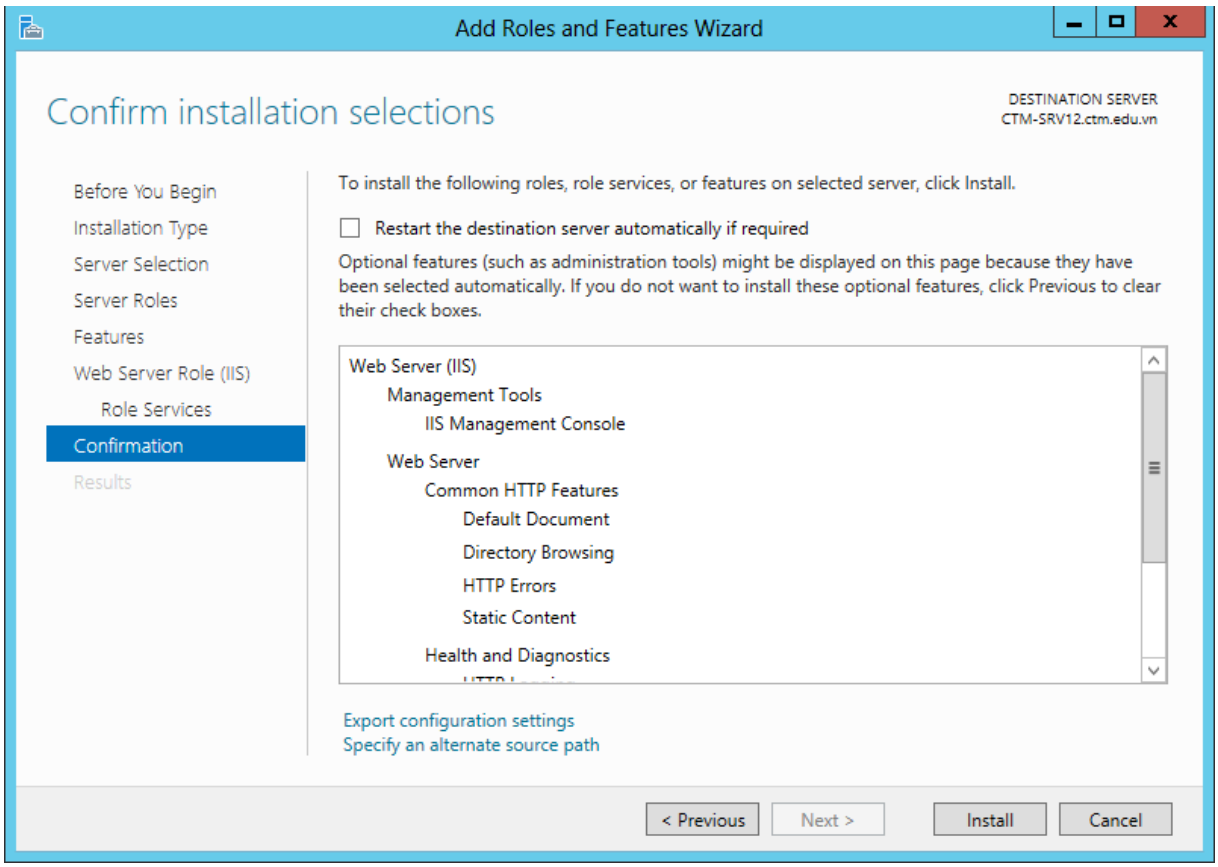
Thông báo yêu cầu những Feature quan trọng, chọn ***Add Feature***



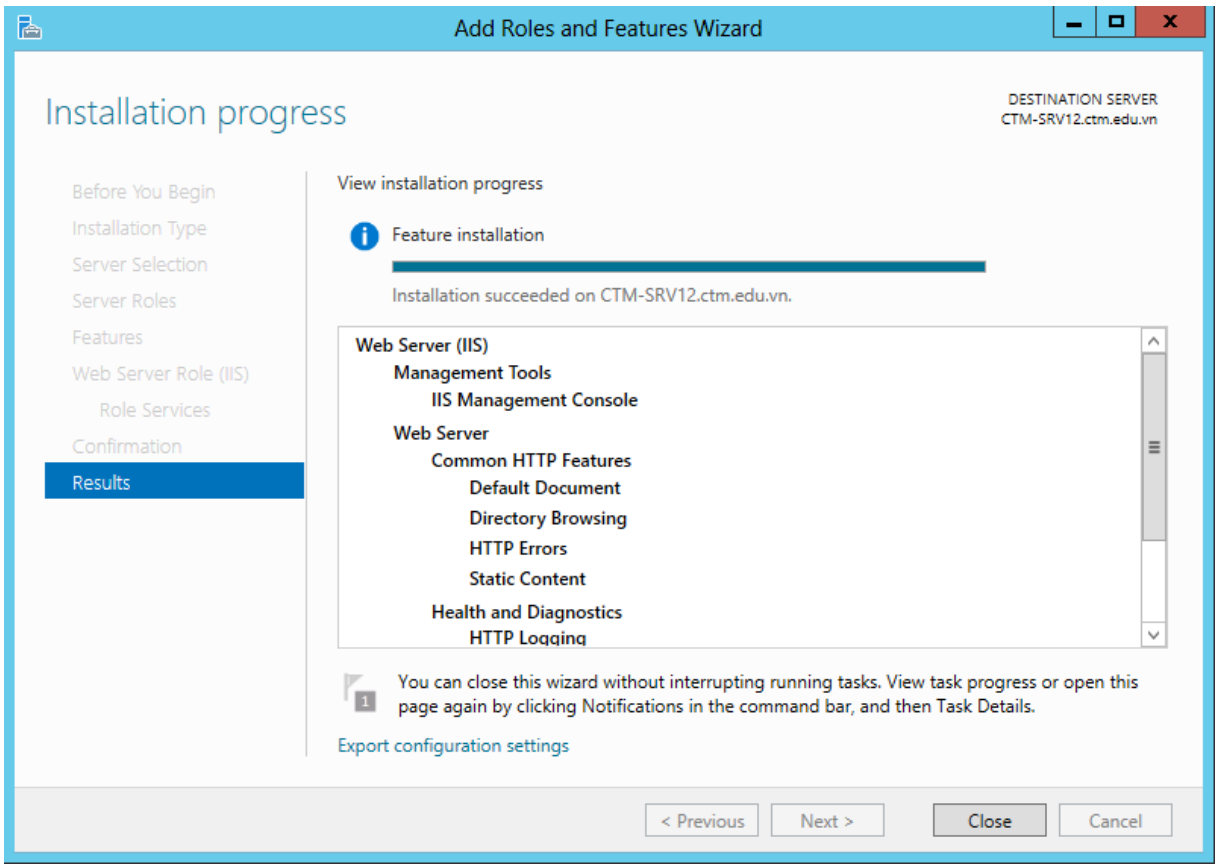
Đến phần ***Role Services***, để mặc định, click ***Next***



Tiếp theo click ***Next*** và click vào ***Install*** để cài đặt.

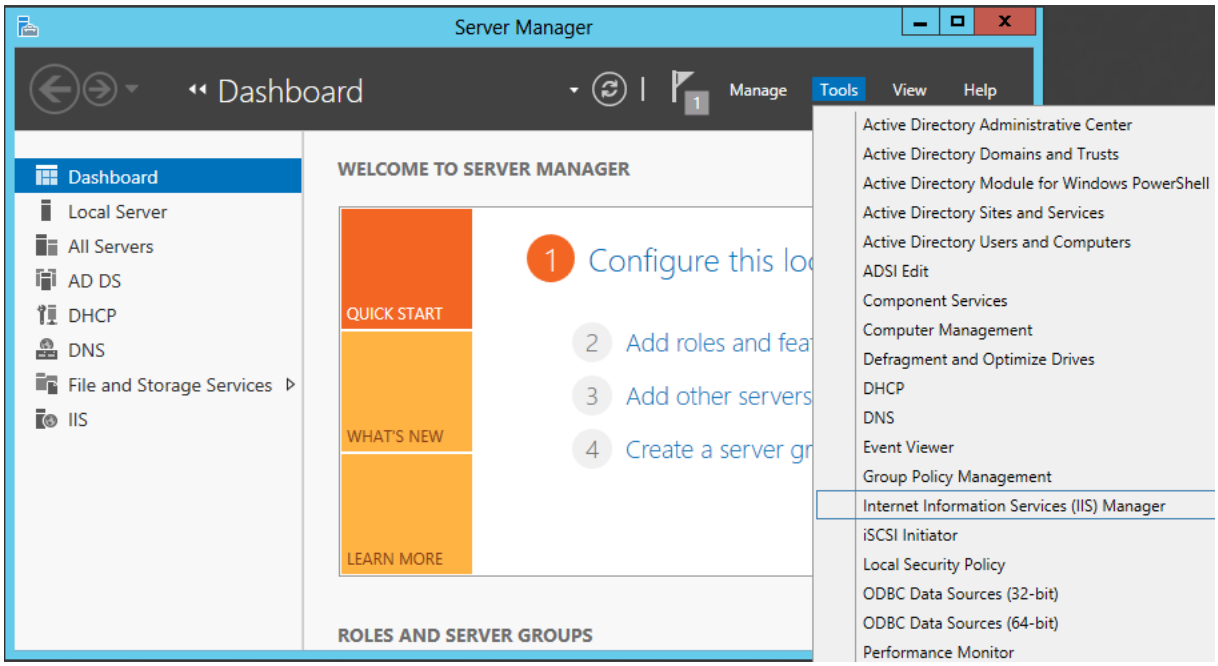


Khi quá trình cài đặt hoàn tất click vào ***Close*** để đóng.

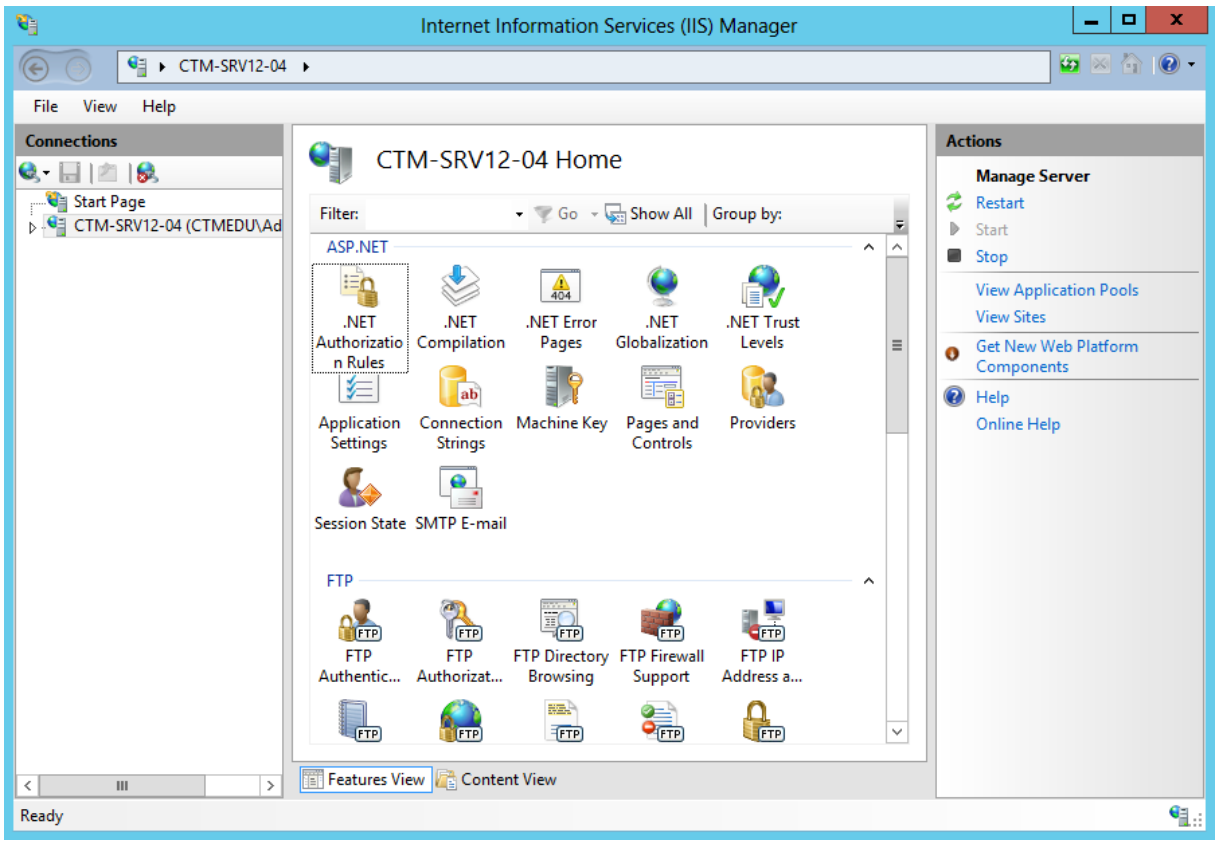


Bước 2: Cấu hình dịch vụ Web Server

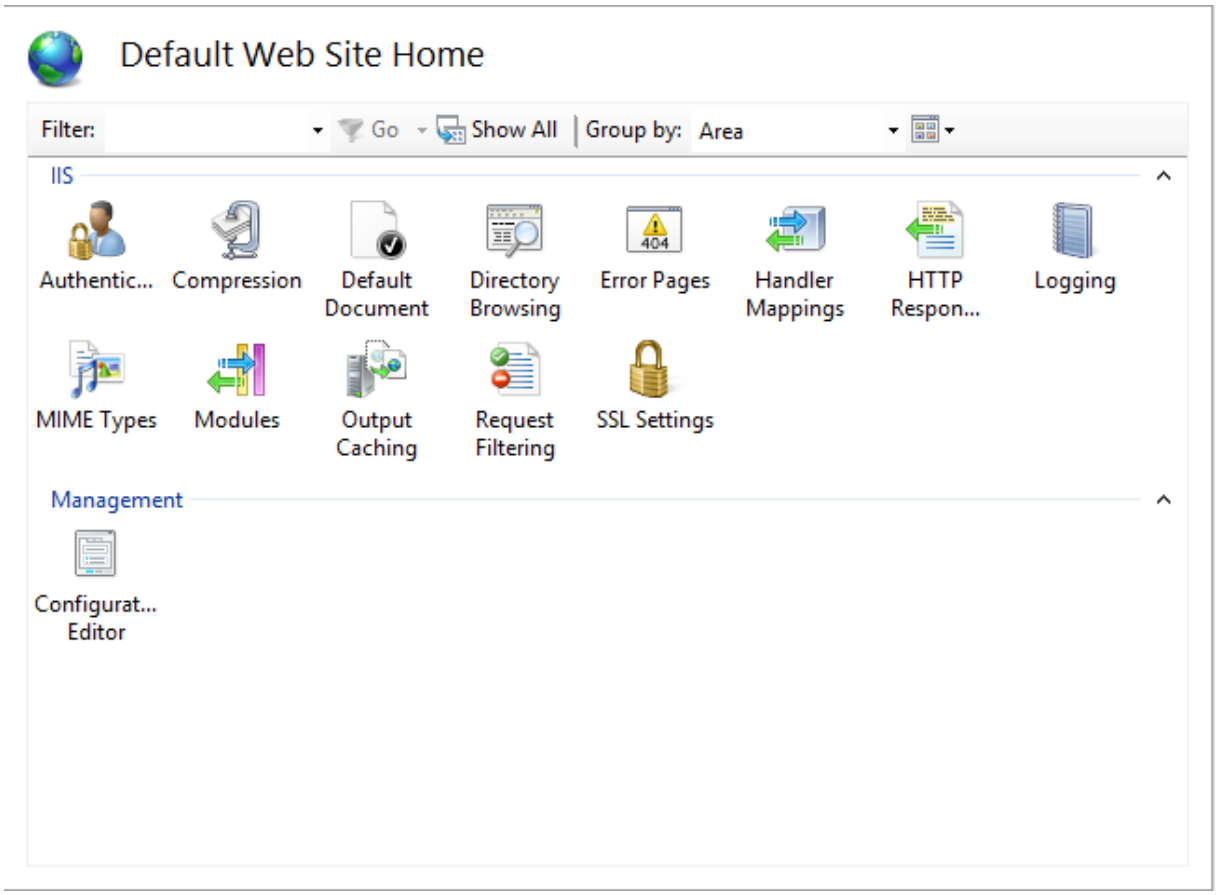
Tại hộp thoại ***Server Manager*** click vào ***Tool*** chọn ***Internet Information Service (IIS) Manager***



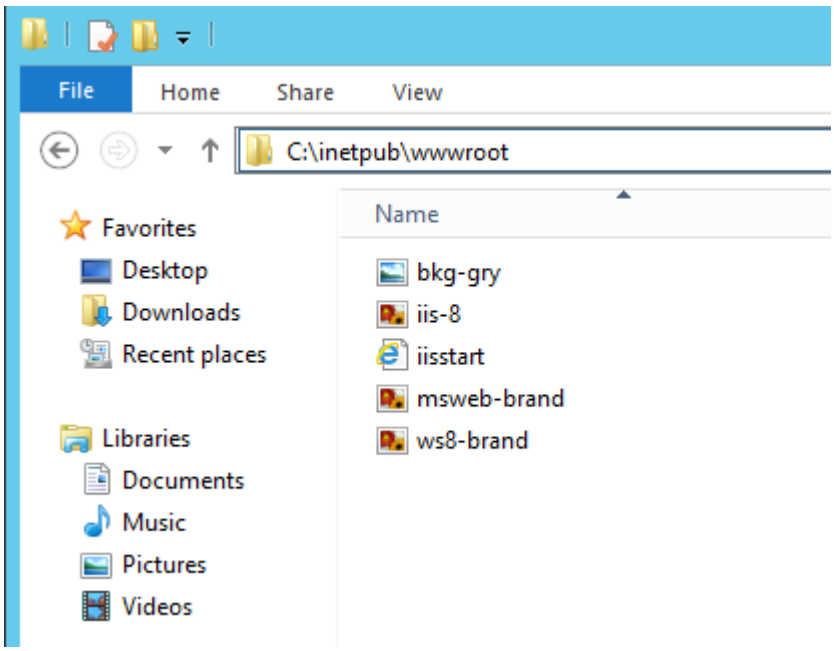
Các thông tin cấu hình có trong cửa sổ ***Internet Information Service (IIS) Manager***



Trong ***Default Website***. ***Default Document*** quy định tên trang chủ sẽ sử dụng cho website

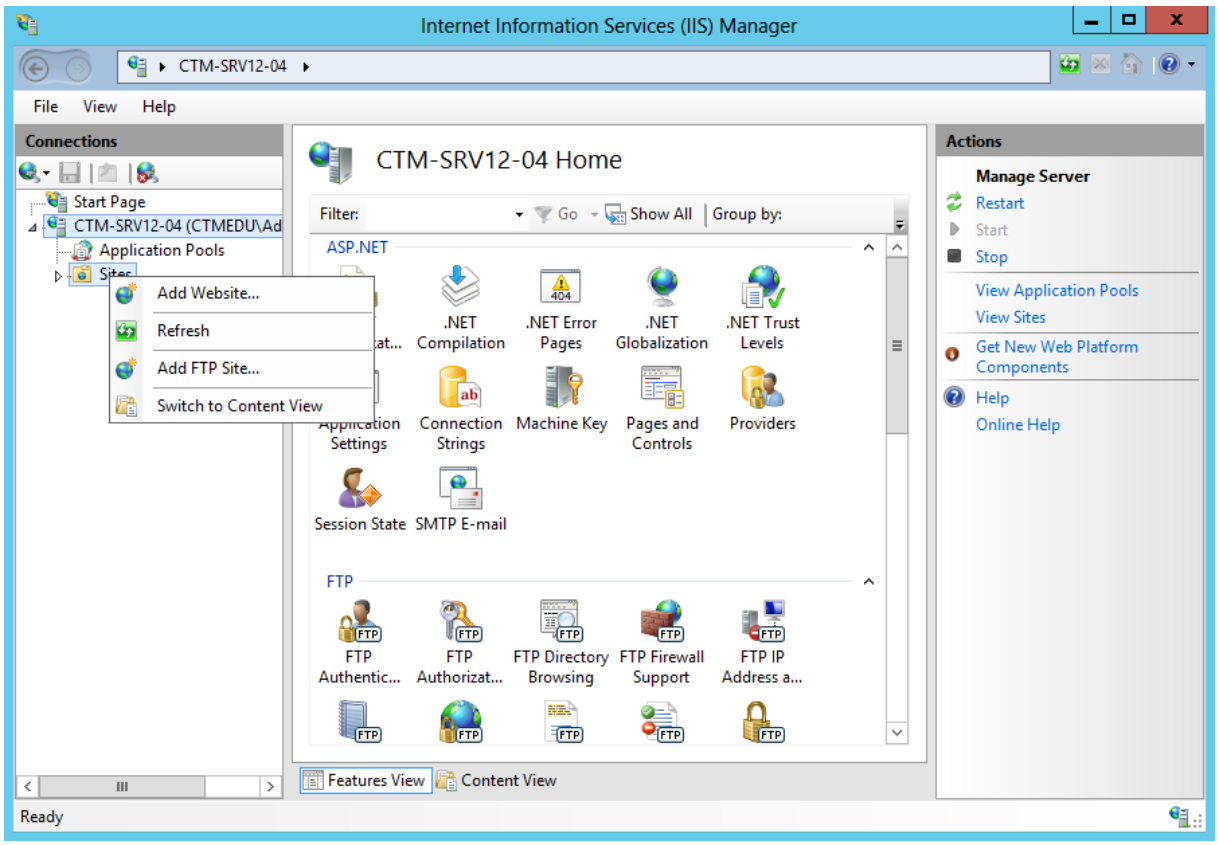


Thư mục chứa website mặc định là ***C:\\inetpub\wwwroot***

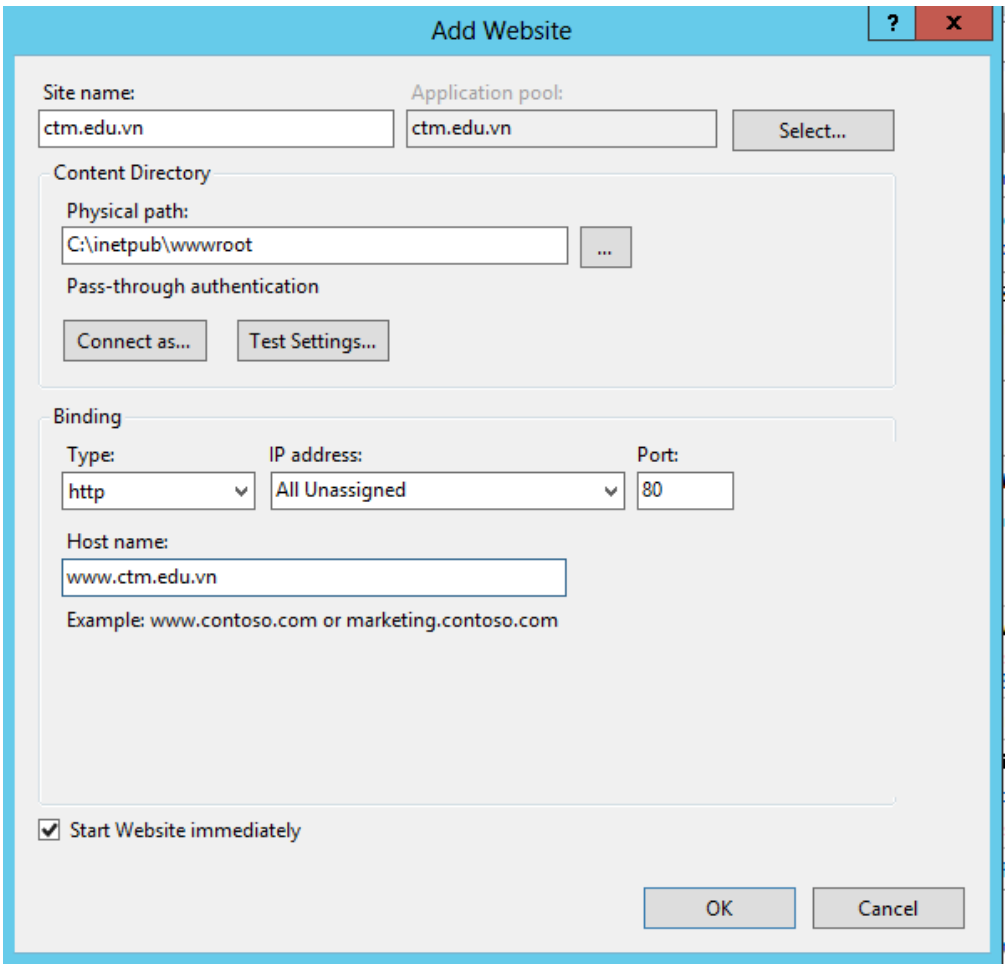


Bước 3: Xuất bản một website

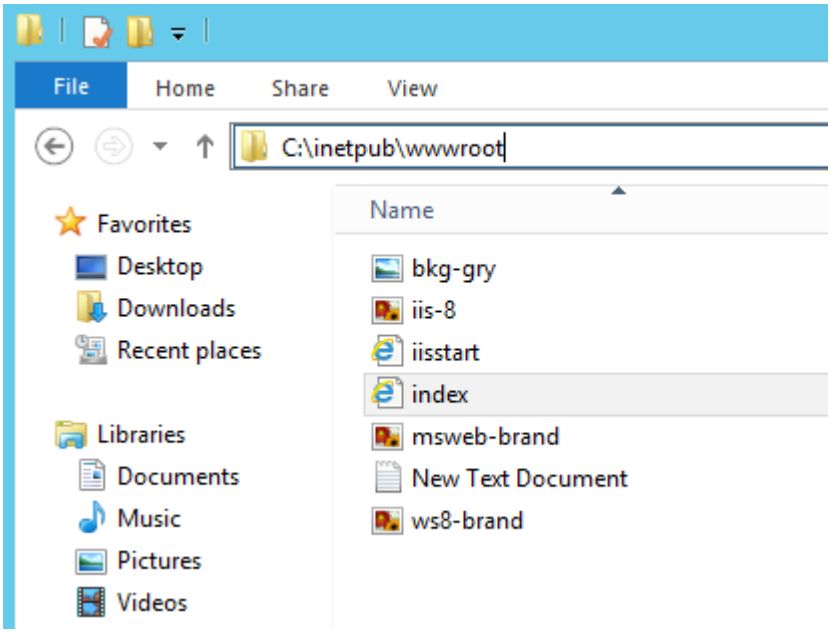
Click chuột phải vào ***Sites*** chọn ***Add Website…***



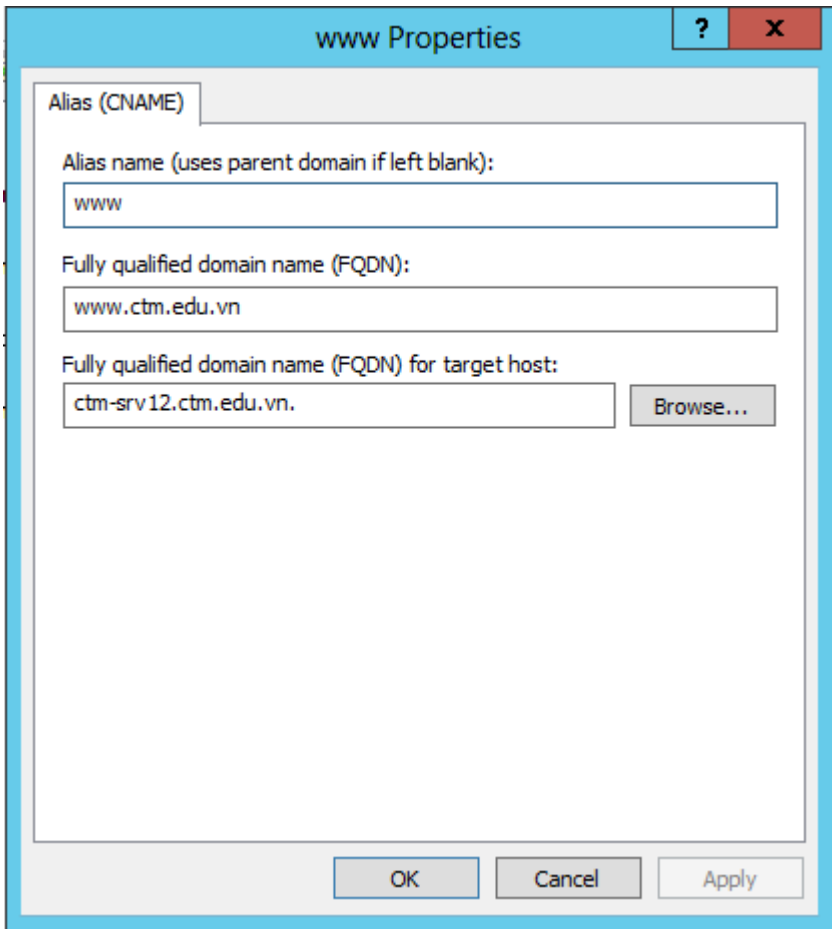
Tại hộp thoại ***Add Website***, tiến hành nhập ***Site name***, ***Physical path*** và ***Host name***



Tiến hành dùng phần mềm ***notepad*** để tạo một file ***index.html*** trong ***C:\\inetpub\wwwroot***

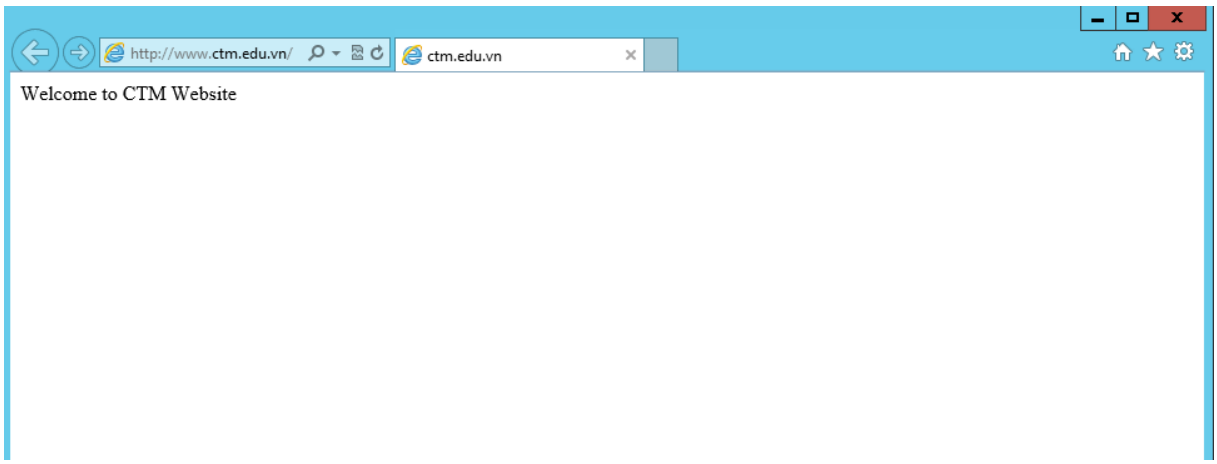


Để có thể truy cập website bằng tên miền *ctm.edu.vn.* Tiến hành tạo một ***record CNAME*** trong dịch vụ ***DNS***



Bước 4: Truy cập website tại máy Client.

Tại máy client ***CTM-WRK07***. Mở trình duyệt Web. Nhập địa chỉ website *ctm.edu.vn* vào thanh address. Kết quả thu được như hình sau



III. Sai hỏng và cách khắc phục

1. Cài đặt dịch vụ Web không thành công

- Nguyên nhân

  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn

- Cách khắc phục

  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành

2. Không truy cập được website trên trình duyệt web

- Nguyên nhân

  - Chưa tạo bản ghi CNAME trên DNS Server
  - Chưa tạo file index.html

- Cách khắc phục

  - Tạo bản ghi CNAME trên DNS Server
  - Tạo file index.html

V. Hướng dẫn ôn luyện

– Cài đặt dịch vụ Web Server

– Xuất bản thêm các website khác

BÀI 8: TRIỂN KHAI DỊCH VỤ FTP VỚI IIS

I. Lý thuyết liên quan

1. Tổng quan về FTP

FTP (File Transfer Protocol) là một dịch vụ cho phép truyền tải file giữa hai máy tính ở xa dùng giao thức TCP/IP. FTP cũng là một ứng dụng theo mô hình client-server, nghĩa là máy làm FTP Server sẽ quản lý các kết nối và cung cấp dịch vụ tập tin cho các máy trạm.

FTP Server thường là một máy tính phục vụ cho việc quảng bá các tập tin cho người dùng hoặc là một nơi cho phép người dùng chia sẻ tập tin với những người dùng khác trên Internet. Máy trạm muốn kết nối vào FTP Server thì phải được Server cấp cho một account có đầy đủ các thông tin như: địa chỉ máy Server (tên hoặc địa chỉ IP), username và password.

Các FTP server thông dụng: Wu-ftpd , ProftpD , Pureftpd , Vsftpd trên Linux hoặc dịch vụ FTP Server trên Windows Server…

Phần lớn các FTP Server cho phép các máy trạm kết nối vào mình thông qua account anonymous (account anonymous thường được truy cập với password rỗng). Các máy trạm có thể sử dụng các lệnh ftp đã tích hợp sẵn trong hệ điều hành hoặc phần mềm chuyên dụng khác để tương tác với máy FTP Server.

FTP sử dụng 2 cổng gồm: cổng 20 để truyền dữ liệu (data port) và cổng 21 dùng để truyền câu lệnh (command port)

2. Phân loại

a) Active FTP

Active FTP là 1 trong 2 chế độ hoạt động của FTP server. Trong chế độ Active FTP thì client sẽ random unprivileged port (là port N > 1023) để connect tới port command trên server là port 21. Sau đó Client sẽ lắng nghe trên port N+1 và gửi command port “port N+1” tới server. FTP server sẽ connect tới Client bằng data port mặt định của nó là port 20.

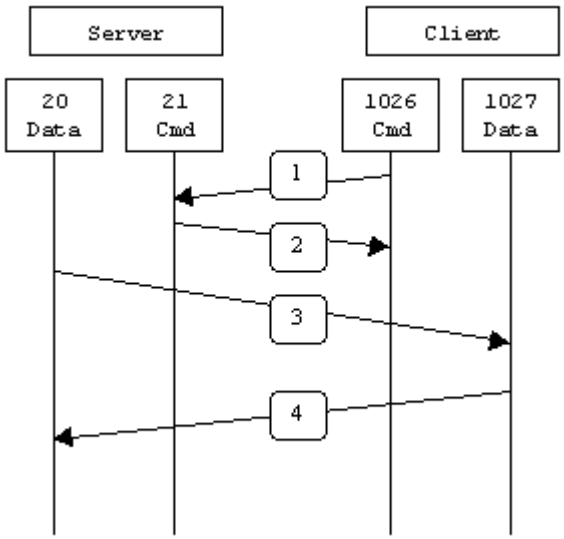
Đứng ở gốc độ Firewall Server thì để hỗ trợ cho Mode Active FTP này cần phải mở những luồng xử lý sau:

+ FTP Server phải mở port 21 để đón nhận tất cả connect tới của Client.

+ FTP Server phải mở kết nối từ port 21 đến ports > 1023 để trả lời request của Client.

+ FTP Server phải mở kết nối từ port 20 đến ports > 1023 để tạo kết nối truyền dữ liệu với Client.

+ FTP Server phải mở kết nối từ ports > 1023 đến port 20 để xác nhận kết nối với Client



Hình 2.5.2 - Active FTP mode

Ở bước 1, từ command port 1026 Client kết nối tới command port 21 của Server và gửi command port PORT 1027. Server gửi gói tin ACK (hiểu đơn giản là chấp nhận) về cho Client ở bước 2. Bước 3 Server khởi tạo kết nối từ port data 20 tới port 1027 của Client (port 1027 là port Client gửi cho Server ở bước 1). Và cuối cùng là Client gửi gói tin ACK về cho Server.

Vấn đề chính gặp phải khi sử dụng Active FTP là có thể bị mất kết nối ở phía Client. Client không khởi tạo kết nối tới port data của Server mà nó đơn giản chỉ nói với Server là tôi đang lắng nghe trên port 1027 và chờ Server kết nối tới. Nếu có tồn tại Firewall đứng trước Client thì đôi khi connection sẽ bị Blocked.

Để FTP Server làm việc ở chế độ Active, firewall phải thoả mãn:

- Cổng 21 phải được mở hướng vào cho bất cứ nguồn gửi nào để client khởi tạo kết nối.
- Cổng 21 được mở hướng ra để server trả lời về cổng điều khiển của client
- Cổng 20 được mở hướng ra để server khởi tạo kết nối vào cổng dữ liệu của client
- Cổng 20 mở hướng vào để client gửi xác nhận ACKs đến cổng data của server

b) Passive FTP

Thay vì tập trung giải quyết vấn đề bị firewall chặn ở Active mode, thì một phương thức kết nối mới cho FTP được xây dựng. đó là Passive mode.

Trong passive mode FTP Client khởi tạo 2 connections đến Server, như vậy là giải quyết được vấn đề bên phía Client Blocked connection từ Server đến data port của Client. Passive mode hoạt động như sau.

Khi khởi tạo kết nối thì Client mở 2 ports random unprivileged port local (N > 1023 and N+1). Port đầu tiên Client mở connect tới port 21 của Server. Nhưng thay thì gửi PORT command như ở Active mode thì Client sẽ gửi câu lệnh PASV command. Lúc đó Server sẽ khởi tạo a random unprivileged port (P > 1023)

và gửi P đến Client trong cái response PASV command. Lúc này Client khởi tạo connection từ port N+1 của nó tới port P trên Server và transfer data.

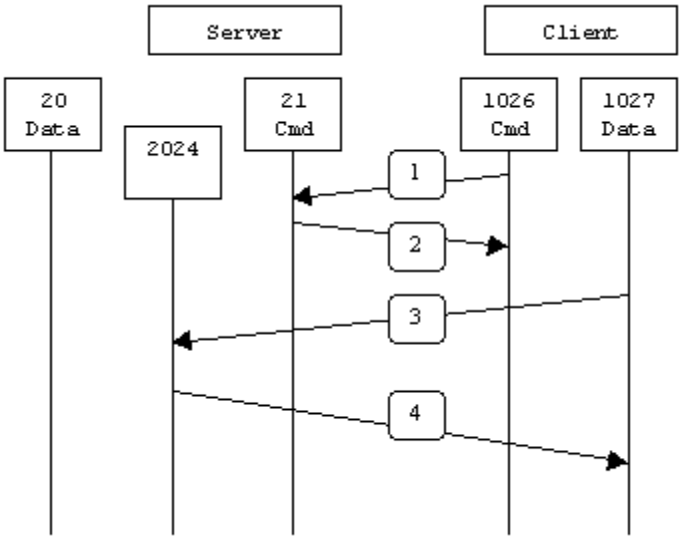
Ở phía Server, để support Passive mode FTP này thì cần phải mở những luồng connect như sau.

+ FTP Server phải mở port 21 nhận kết nối từ mọi Client.

+ FTP Server phải mở các kết nối từ port 21 đi tới các port > 1023 để trả lời (response) cho Client.

+ FTP Server phải mở các port > 1023 để nhận kết nối tới data port từ phía Client.

+ FTP Server phải mở các port > 1023 tới các port > 1023 để trả lời chấp nhận kết nối và truyền dữ liệu với Client.



Hình 2.5.3 - Passive FTP mode

Tại Step 1. Client liên lạc với Server trên command port và đưa ra câu lệnh PASV. Server trả lời ở Step 2 với PORT 1024 và nói với Client đây là port dữ liệu tôi đang lắng nghe. Step 3 Client khởi tạo data connection từ port Data của nó tới port 1024 mà Server đã gửi cho nó. Cuối cùng là Server gửi lại gói tin ACK chấp nhận.

Với Passive mode giải quyết được nhiều vấn đề ở phía Client, nhưng nó đã mở ra một range port lớn tạo nên các lỗ hổng nguy hiểm cho phía Server. Vấn đề lớn nhất ở đây là phải chấp nhận hầu hết các kết nối port > 1023 trên Server

Vì lý do này nên hầu hết các FTP Service đều được khai báo một range port nhất định, để dễ dàng kiểm soát hơn và tránh rũi ro.

Vấn đề lớn thứ 2 là phía Client không hổ trợ Passive Mode. Ví dụ như nếu dùng Solaris thì commandline FTP không hổ trợ cơ chế Passive này mà phải sử dụng FTP software client của hãng khác. ví dụ như ncftp.

Một số lượng lớn người dùng sử dụng Browser (Trình duyệt) của mình để đăng nhập vào FTP server. và trên Browser chỉ hổ trợ Passive mode.

Để FTP Server làm việc ở chế độ Passive, firewall phải thoả:

- Cổng 21 của server mở hướng vào để chấp nhận bất kỳ yêu cầu kết nối khởi tạo từ client
- Cổng 21 được mở hướng ra để server trả lời về cổng điều khiển của client
- Cổng lớn hơn 1024 của server mở hướng vào để chấp nhận yêu cầu kết nối dữ liệu từ client (do cổng P của server là ngẫu nhiên)
- Cổng lớn hơn 1024 của server mở hướng ra để trả lời ACK cho client

II. Trình tự thực hiện

1. Yêu cầu thực hiện

+ Cài đặt và cấu hình dịch vụ FTP trên máy CTM-SRV12.

+ Tạo Alias CNAME và cấp quyền cho User

+ Kiểm tra kết quả trên máy CTM-WRK07

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

3. Các bước thực hiện

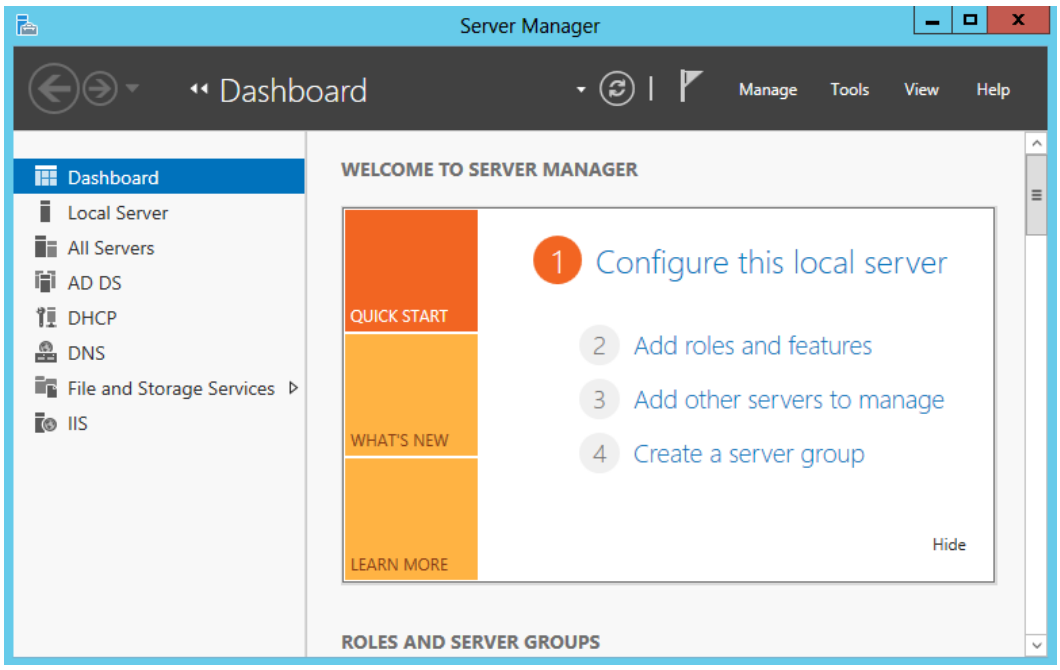
Thực hiện triển khai cài đặt và cấu hình dịch vụ FTP Service thông qua 5 bước sau:

- Bước 1: Cài đặt dịch vụ FTP Service
- Bước 2: Tạo Alias CNAME cho FPT Server
- Bước 3: Cấp quyền cho user
- Bước 4: Cấu hình FPT Service
- Bước 5: Kiểm tra kết quả trên trình duyệt web.

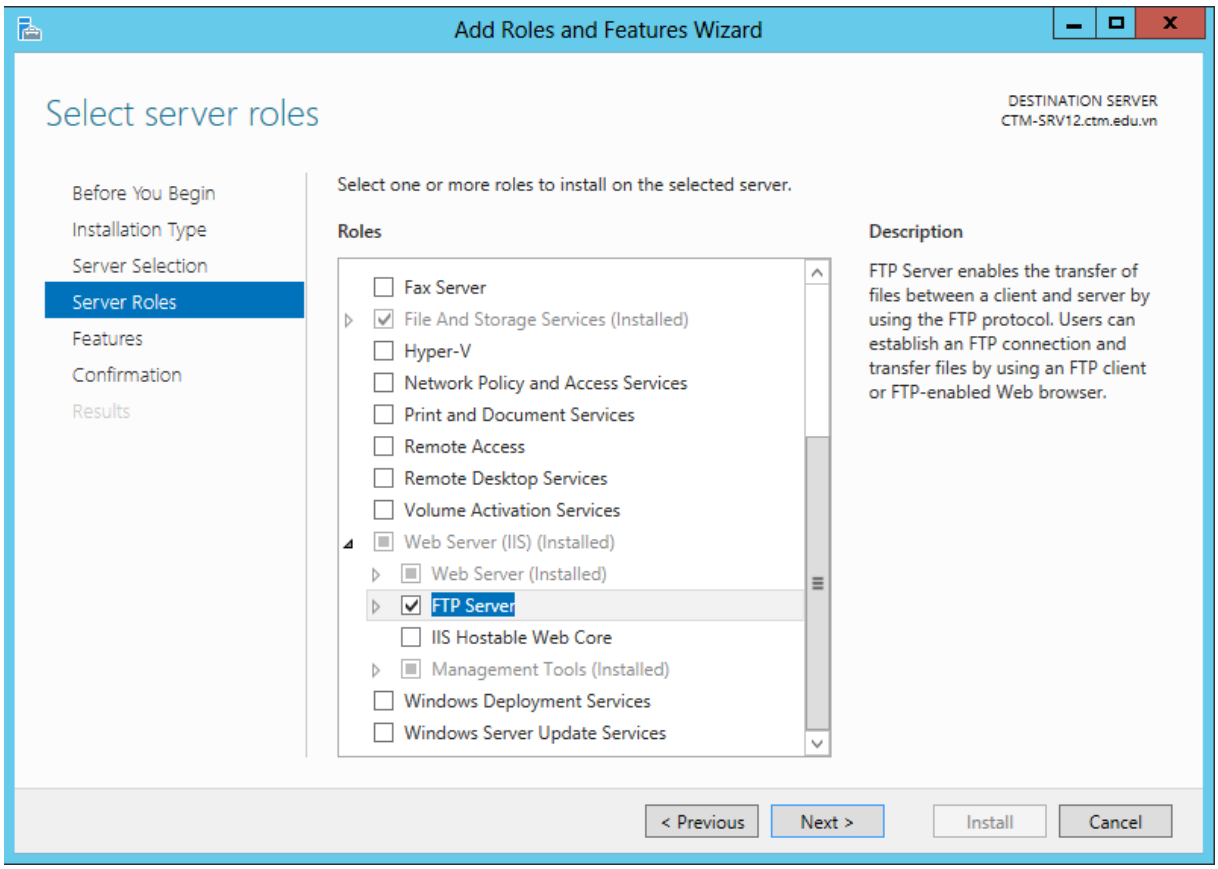
Hướng dẫn chi tiết:

Bước 1: Cài đặt FTP Service

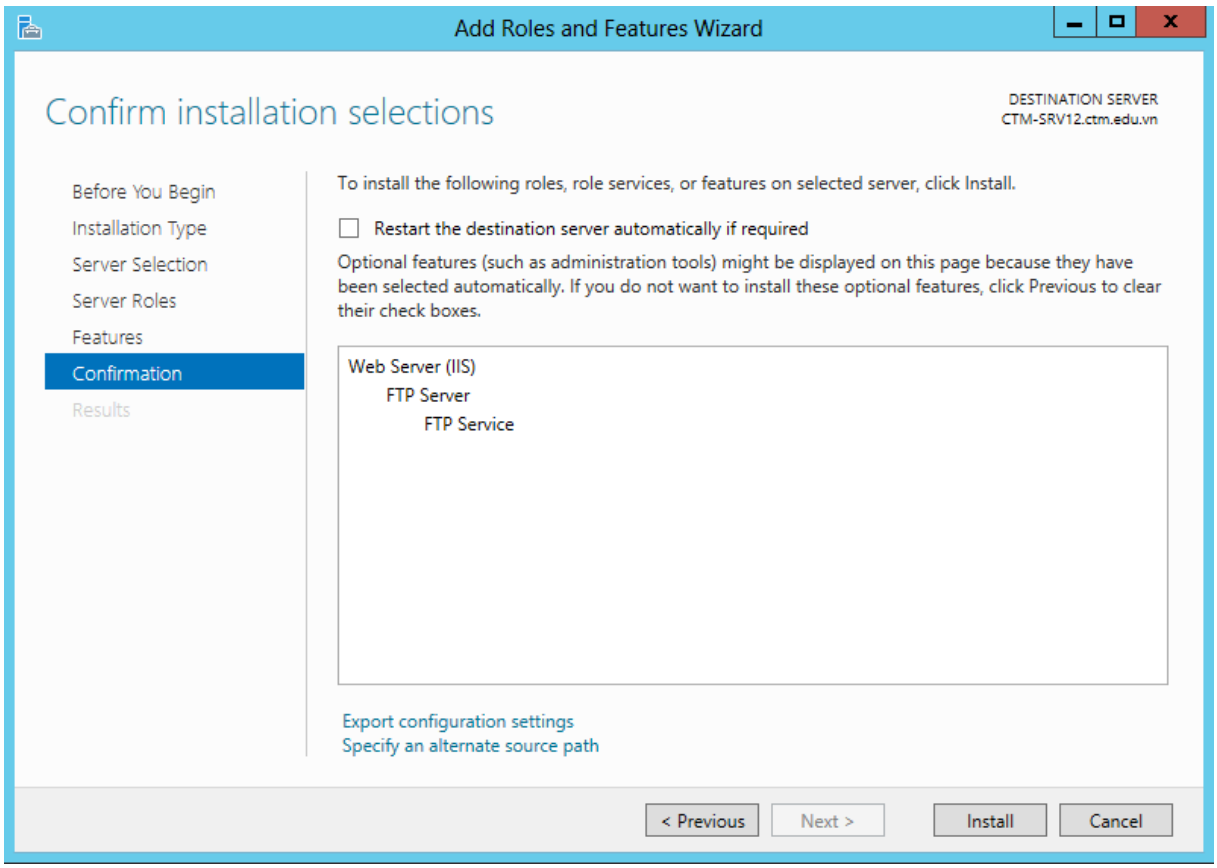
Vào ***Server Manager*** => ***Add roles and features***



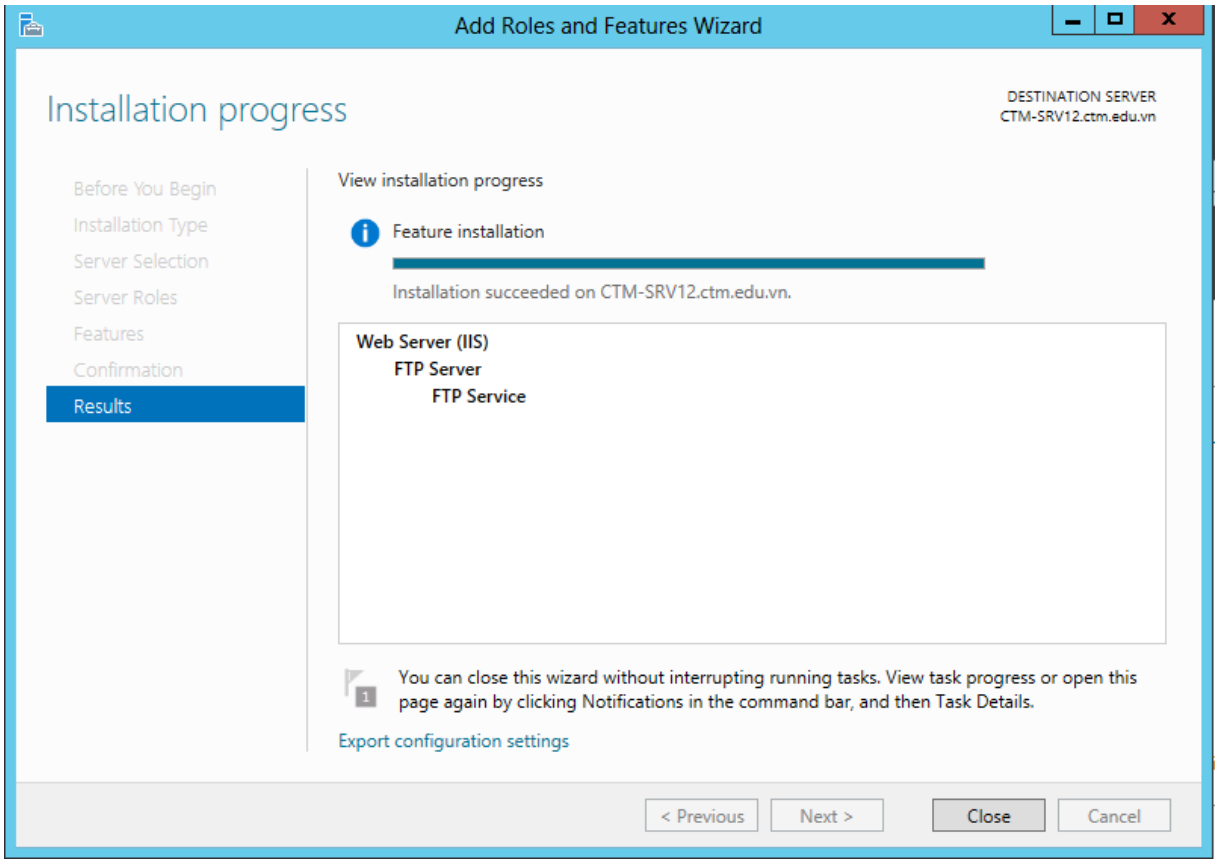
Click đến ***Server Roles*** chọn vào ***Web Server (IIS)*** và chọn ***FTP Server***.



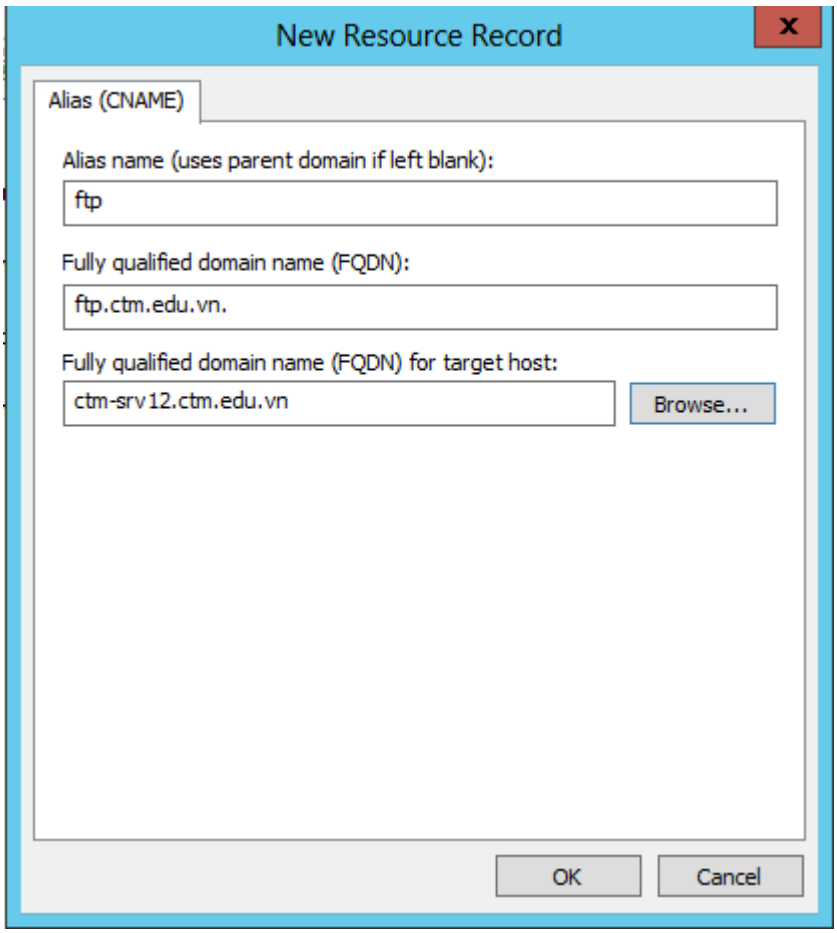
Click ***Next*** và chọn ***Install*** cài đặt



Quá trình cài đặt hoàn tất click vào ***Close***

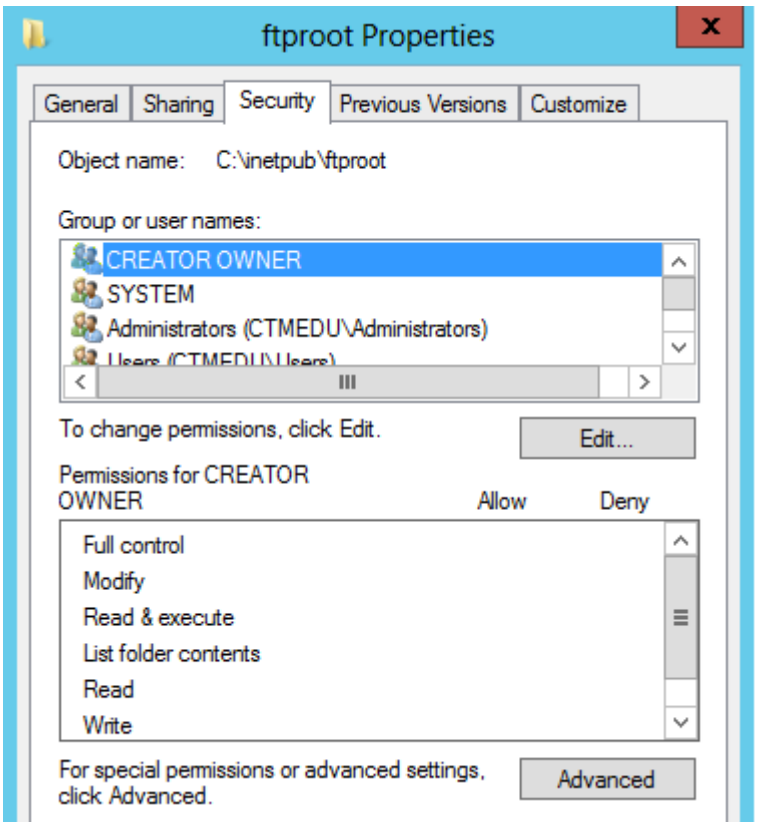


Bước 2: Tạo Alias CNAME cho FPT Server

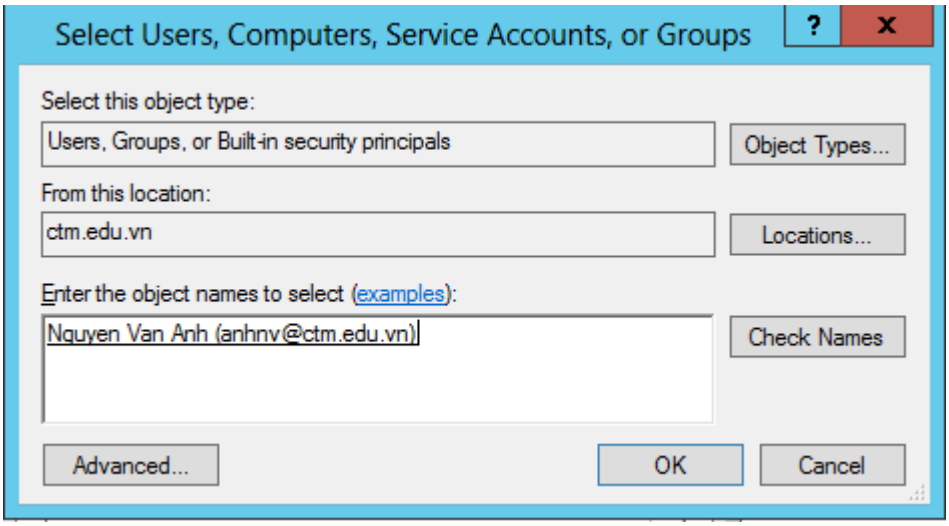


Bước 3: Cấp quyền cho user.

Tại thư mục ***ftproot***, click chuột phải chọn ***Properties***. Chọn thẻ ***Security***.

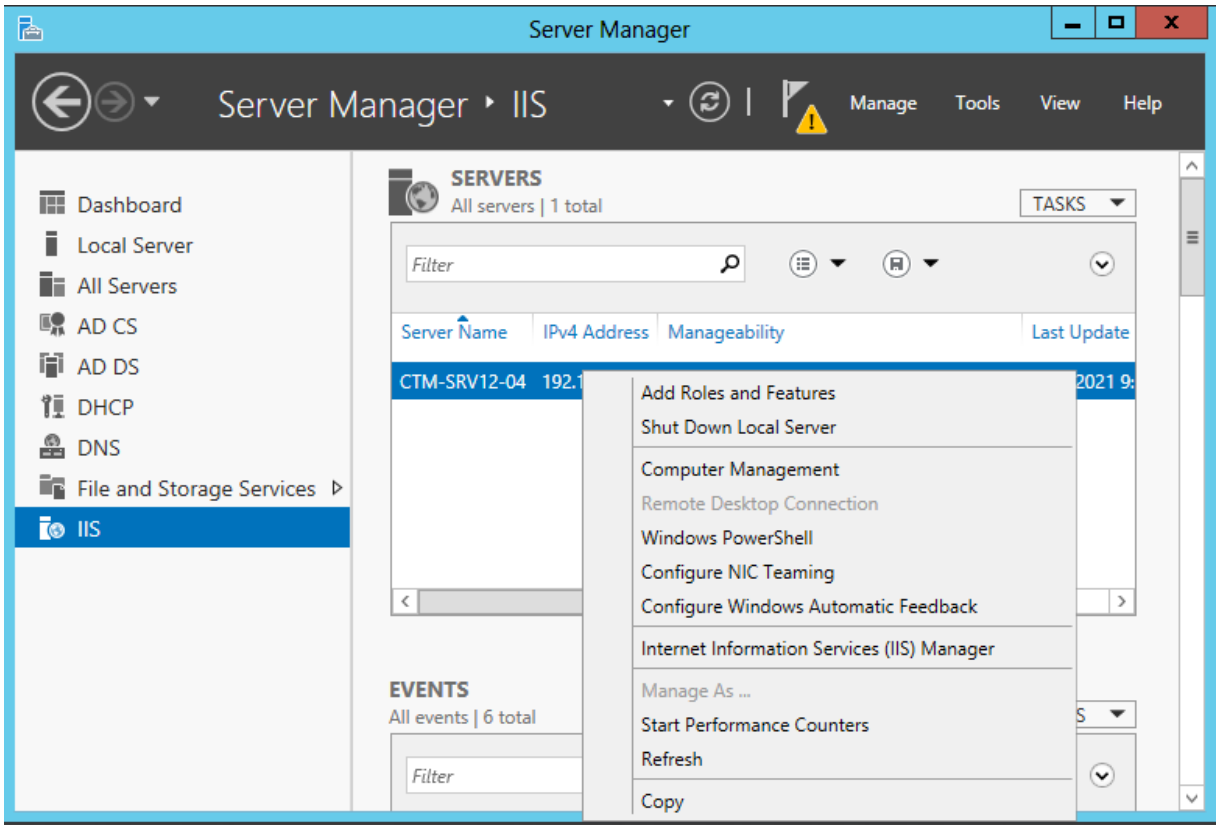


Click nút ***Edit*** và tiến hành thêm người dùng được quyền truy cập. Click ***OK***

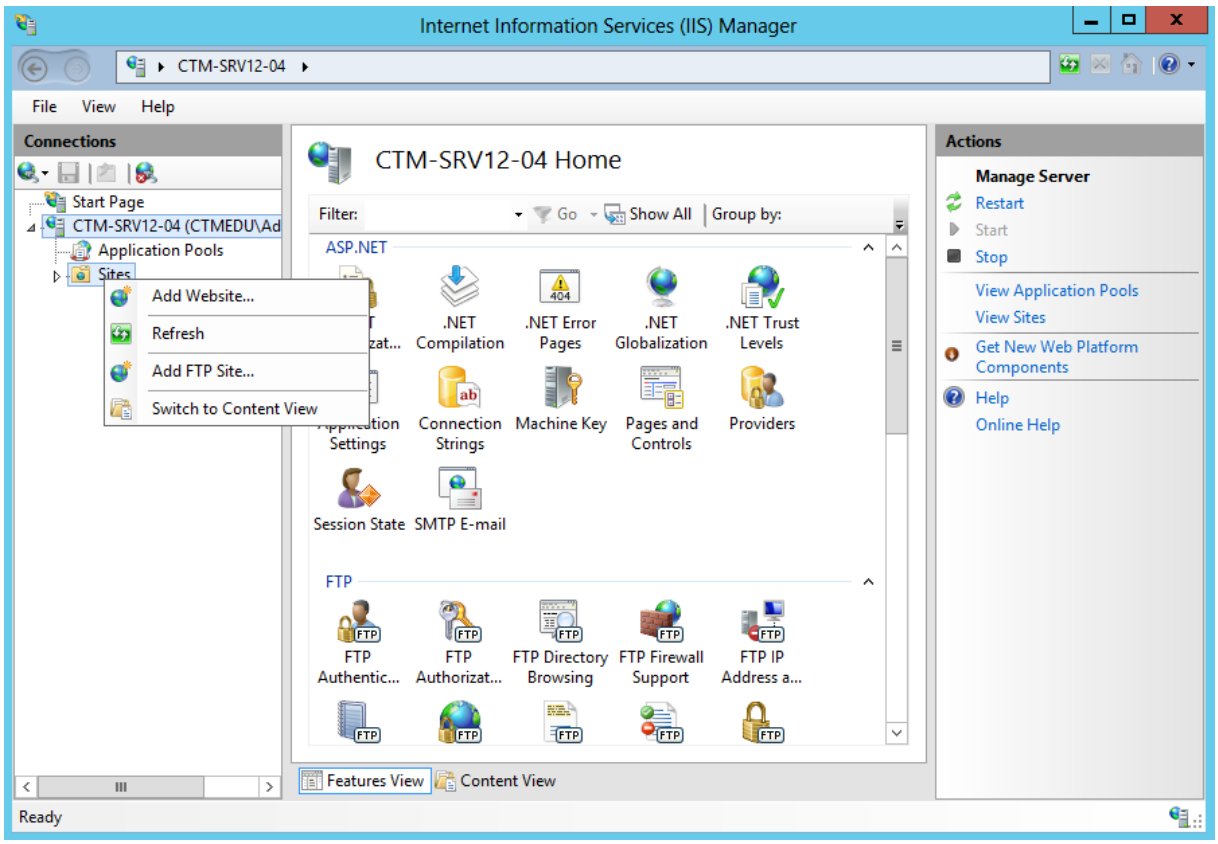


Bước 4: Cấu hình FPT Service

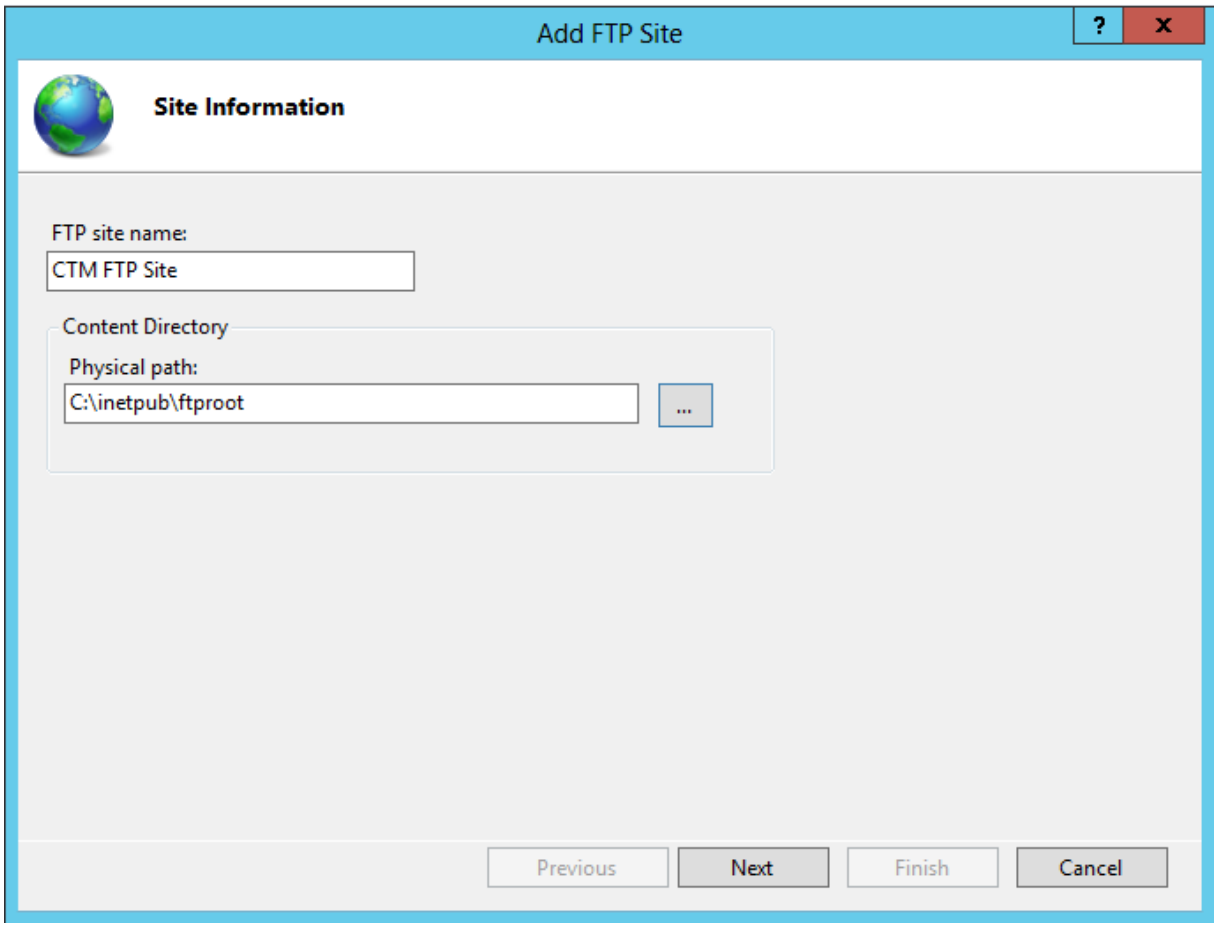
Tại ***Server Manager / IIS***. Click phải chọn ***IIS Manager***



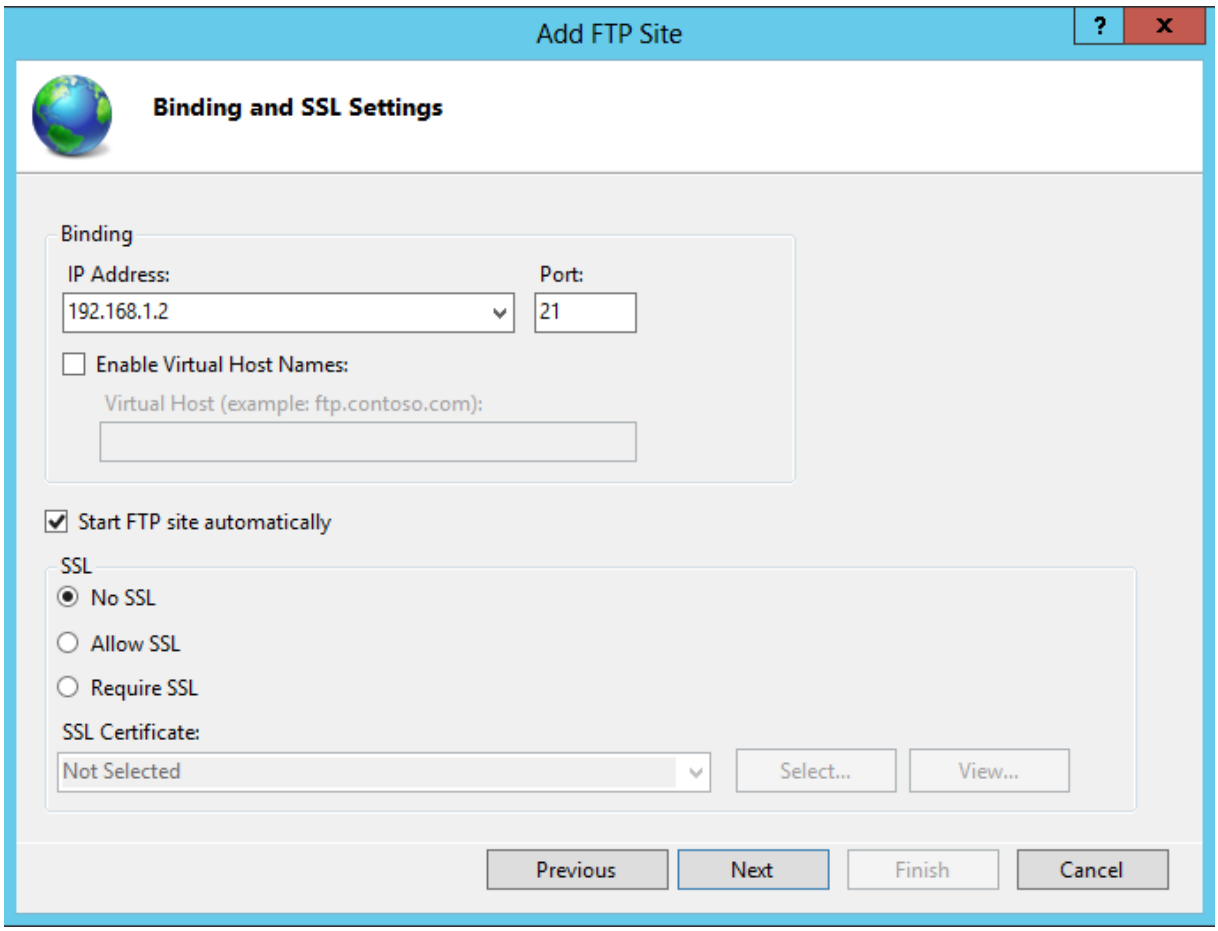
Click chuột phải vào ***Sites*** chọn ***Add FTP Site…***



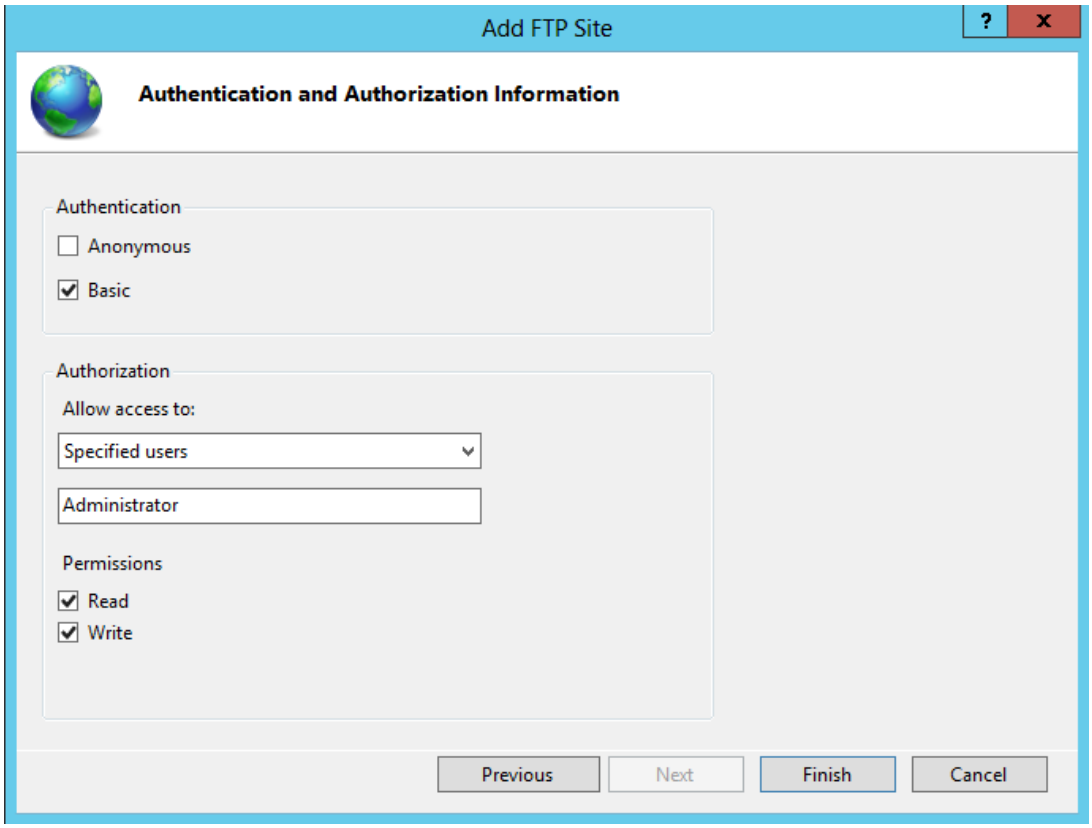
Nhập ***FTP site name*** và ***Physical path***



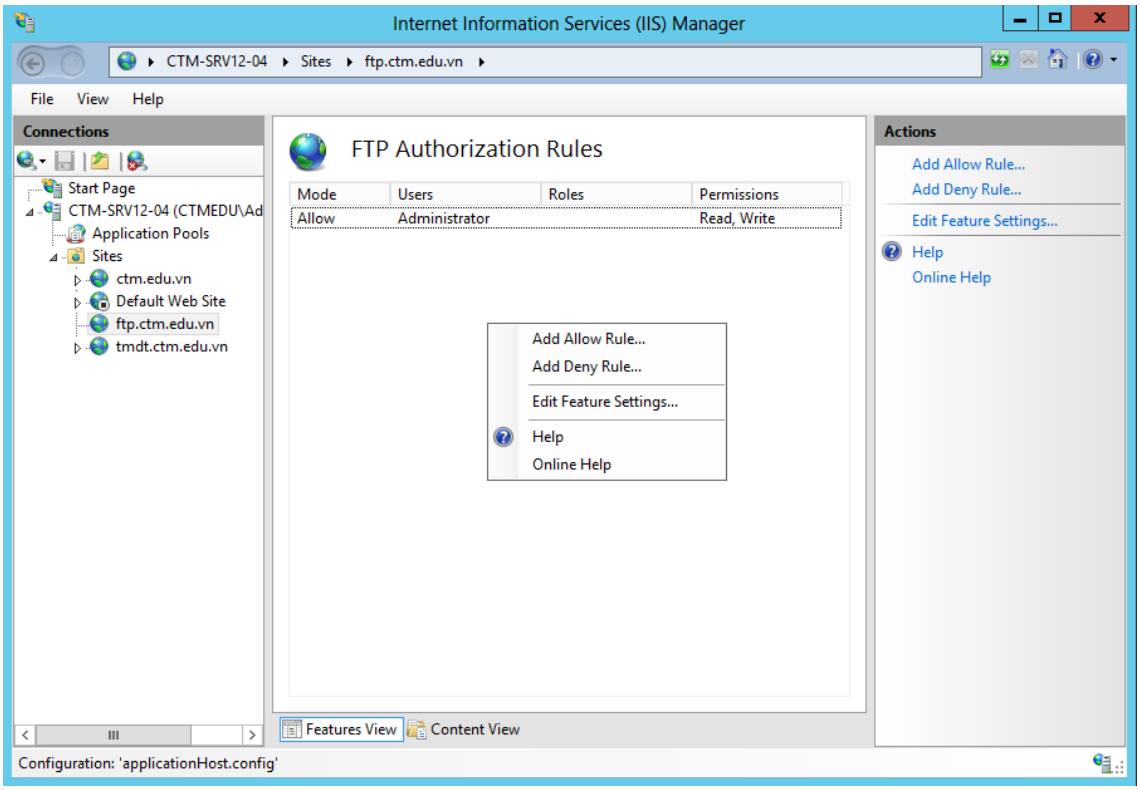
Trong hộp thoại tiếp theo nhập ***IP Address*** và ***SSL***



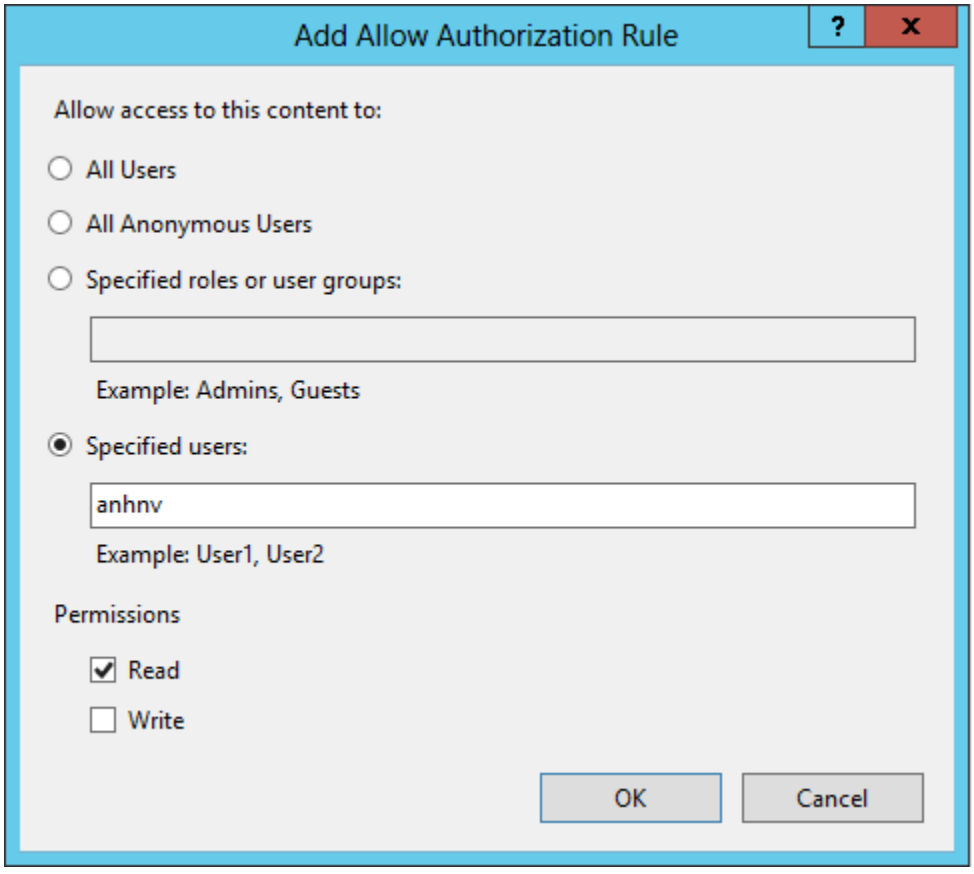
Tại ***Authentication*** chọn ***Bassic***, tại ***Authorization*** chọn vào ***Specified users*** và nhập vào tên tài khoản ***Administrator***, tại ***Permission*** chọn cả 2 ***Read*** và ***Write.***



Khi đã cấu hình xong quay lại với màn hình ***IIS manager*** chọn vào ***Authorization Rules*** sau đó click phải vào khoảng trắng chọn ***add allow rules***



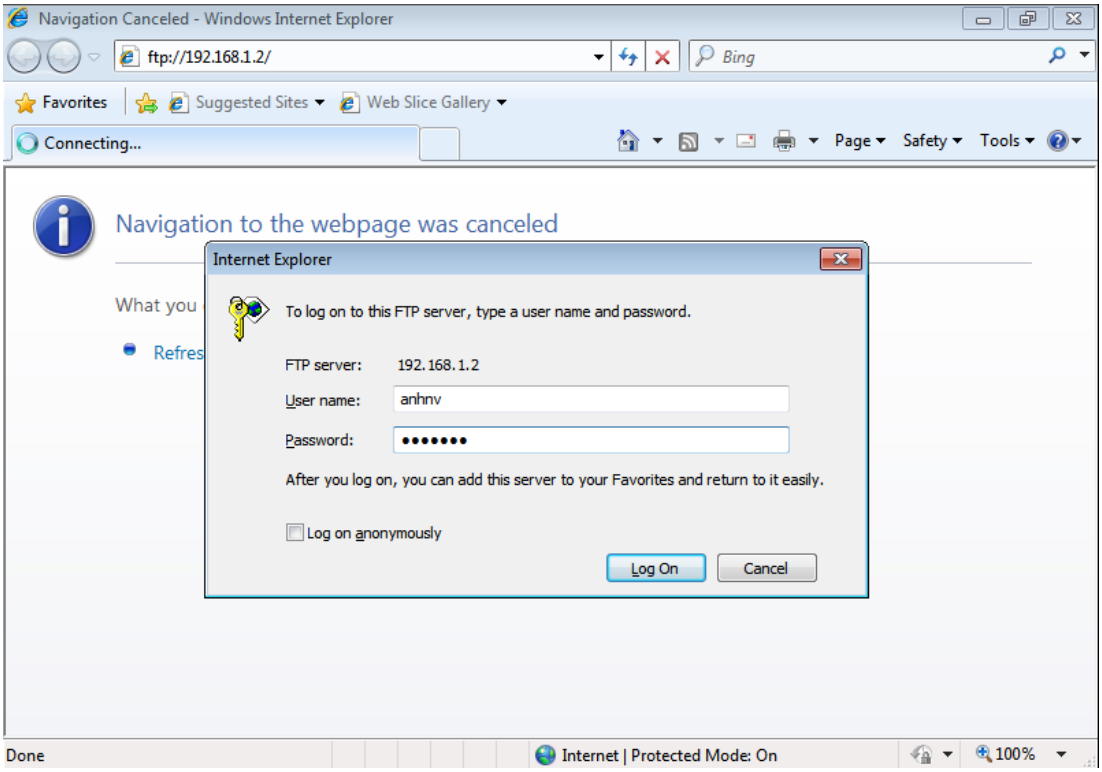
Tại ***Specified users*** nhập vào tên user và chọn ***Read***



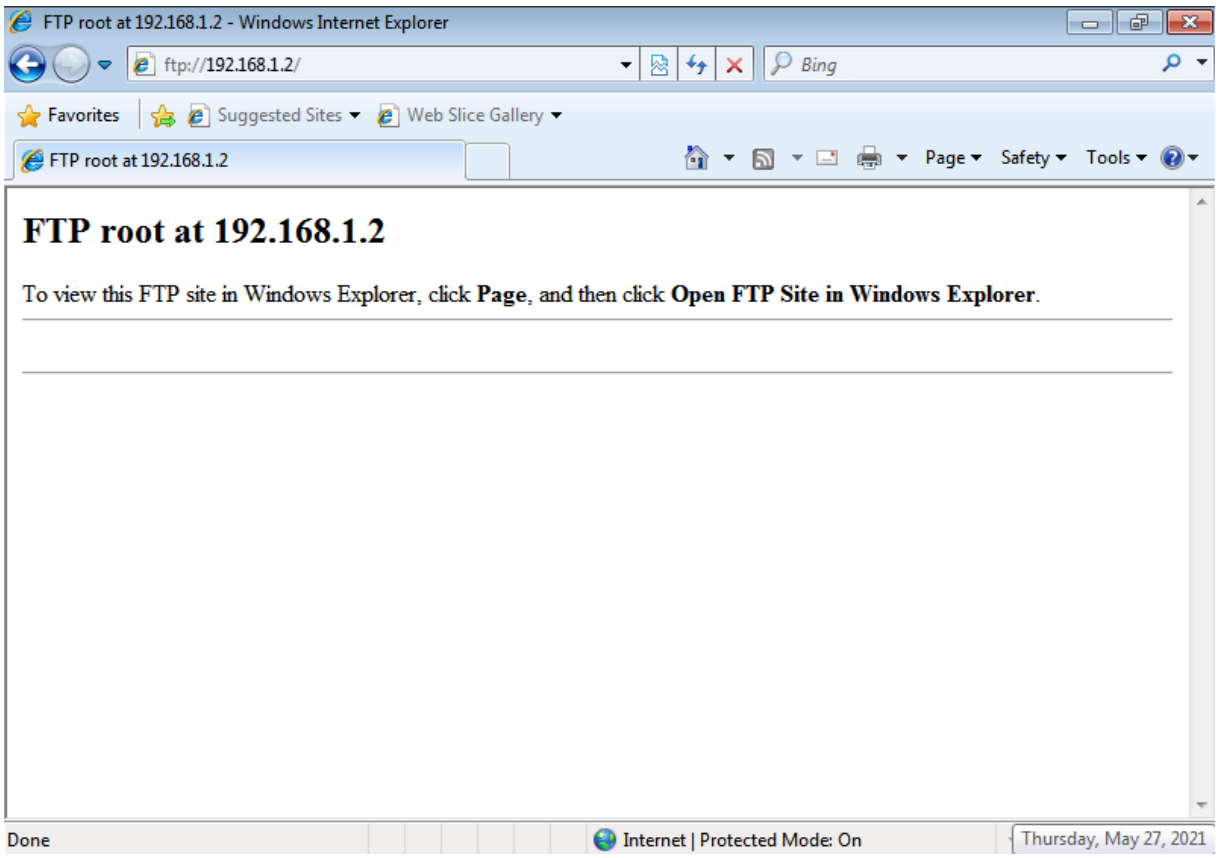
Bước 5: Kiểm tra kết quả trên trình duyệt web.

Trên máy CTM-WRK07

Mở trình duyệt nhập địa chỉ *ftp://192.168.1.2* hoặc *ftp://ftp.ctm.edu.vn* Tiến hành nhập ***Username*** và ***Password*** của tài khoản đã được cấp quyền



Kết quả sau khi đăng nhập



III. Sai hỏng và cách khắc phục

1. Cài đặt dịch vụ FTP không thành công

- Nguyên nhân
  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn
- Cách khắc phục
  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành

2. Không đăng nhập được FTP site

- Nguyên nhân
  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn
  - Chưa cấp quyền cho User truy cập
- Cách khắc phục
  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
  - Thực hiện cấp quyền cho User

3. Không truy cập được FTP site theo tên miền

- Nguyên nhân
  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn
  - Chưa tạo alias CNAME cho FTP service
- Cách khắc phục
  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
  - Tạo alias CNAME cho FTP service

V. Hướng dẫn ôn luyện

- Cài đặt và cấu hình dịch vụ FTP
- Tạo alias CNAME vầ cấp quyền truy cập cho dịch vụ FTP

BÀI 9: TRIỂN KHAI DỊCH VỤ EMAIL (MAIL SERVER)

I. Lý thuyết liên quan

1. Giới thiệu Mail Server

Mail Server là một hệ thống chuyển nhận thư từ qua các mạng máy tính. Mail server: là máy chủ dùng để nhận và gửi mail, với các chức năng chính:

Quản lý account.

Nhận mail của người gửi (của những người có account) và gửi cho người nhận hoặc mail server của người nhận.

Nhận mail từ mail server của người gửi (từ bên ngoài) và phân phối mail cho người trong hệ thống.

2. Các giao thức được sử dụng trong hệ thống mail

a) Giao thức SMTP

SMTP là giao thức tin cậy chịu trách nhiệm phân phát Mail, nó chuyển Mail từ hệ thống mạng này sang hệ thống mạng khác, chuyển Mail trong hệ thống mạng nội bộ.

SMTP là một dịch vụ hướng kết nối(connection-oriented) được cung cấp bởi giao thức TCP.

Sử dụng số hiệu cổng (well-known port) 25

SMTP: End-to-End delivery, phân phát mail trực tiếp từ trạm phát đầu đến trạm cuối nhận → điều này rất hiếm khi sử dụng.

UUCP và X.400: Lưu giữ và chuyển tiếp (store and forward): hai giao thức này di chuyển mail đi qua mỗi hop, lưu trữ thông điệp ở đây và chuyển tiếp tới hệ thống liền kề cho đến khi thư về trạm phân phát cuối cùng.

b) Giao thức POP

POP - Post Office Protocol: là giao thức cung cấp cơ chế truy cập và lưu trữ hộp thư cho người dùng

Phiên bản: POP2, POP3 được định nghĩa trong RFC 937 và 1725. POP2 sử dụng port 109 và POP3 sử dụng Port 110.

Chức năng: kiểm tra tên đăng nhập và chuyển mail của người dùng từ server tới hệ thống đọc mail cục bộ của user.

Lệnh trong POP2 và POP3 khác nhau, nhưng cùng chức năng

Các tập lệnh được sử dụng trong POP3:

- USER: username
- PASS: password
- STAT: Hiển thị số thông điệp chưa được đọc tính bằng bytes.
- RETR n: Nhận thông điệp thứ n.
- DELE n: Xoá thông điệp thứ n.
- LAST: Hiển thị thông tin message cuối cùng.

- LIST [n]: Hiển thị kích thước của thông điệp thứ n
- RSET: Không xoá tất cả thông điệp, và quay lại thông điệp đầu tiên.
- TOP n l: In ra các HEADER và dòng thứ n của thông điệp.
- NOOP : Không làm gì.

c) IMAP

Là giao thức hỗ trợ việc lưu trữ và truy xuất hộp thư của người dùng, thông qua IMAP người dùng có thể sử dụng IMAP Client để truy cập hộp thư từ mạng nội bộ hoặc mạng Internet trên một hoặc nhiều máy khác nhau.

Một số đặc điểm chính của IMAP:

Tương thích đầy đủ với chuẩn MIME.

Cho phép truy cập và quản lý message từ một hay nhiều máy khác nhau.

Hỗ trợ các chế độ truy cập "online", "offline".

Hỗ trợ truy xuất mail đồng thời cho nhiều máy và chia sẽ mailbox.

Client không cần quan tâm về định dạng file lưu trữ trên Server

d) MIME

MIME (Multipurpose Internet Mail Extensions) cung cấp cách thức kết hợp nhiều loại dữ liệu khác nhau vào trong một thông điệp duy nhất có thể được gởi qua Internet dùng Email hay Newgroup.

Thông tin được chuyển đổi theo cách này trông giống như những khối ký tự ngẫu nhiên. Những thông điệp sử dụng chuẩn MIME có thể chứa hình ảnh, âm thanh và bất kỳ những loại thông tin nào khác có thể lưu trữ được trên máy tính. Hầu hết những chương trình xử lý thư điện tử sẽ tự động giải mã những thông báo này và cho phép lưu trữ dữ liệu chứa trong chúng vào đĩa cứng. Nhiều chương trình giải mã MIME khác nhau có thể được tìm thấy trên NET.

e) Các Mail Server thông dụng

Microsoft Exchange Server: Là chương trình Mail Server rất thông dụng được Microsoft phát triển để cung cấp cho các doanh nghiệp tổ chức hệ thống thư điện tử E-mail cho người dùng.

Mdaemon: Là chương trình Mail Server do công ty Alt-N Technologies, phát triển để hỗ trợ cho các doanh nghiệp tổ chức hệ thống thư tính điện tử (E-mail) cho người dùng.

II. Trình tự thực hiện

1. Yêu cầu thực hiện

+ Cài đặt và cấu hình dịch vụ Mail Server trên máy CTM-SRV12.

+ Đăng nhập và kiểm tra thư trên Webmail

2. Thiết bị, dụng cụ, vật liệu

Một máy Server chạy HĐH Windows Server 2012 có tên là CTM-SVR12

Một máy trạm chạy HĐH Windows 7 có tên là CTM-WRK07

3. Các bước thực hiện

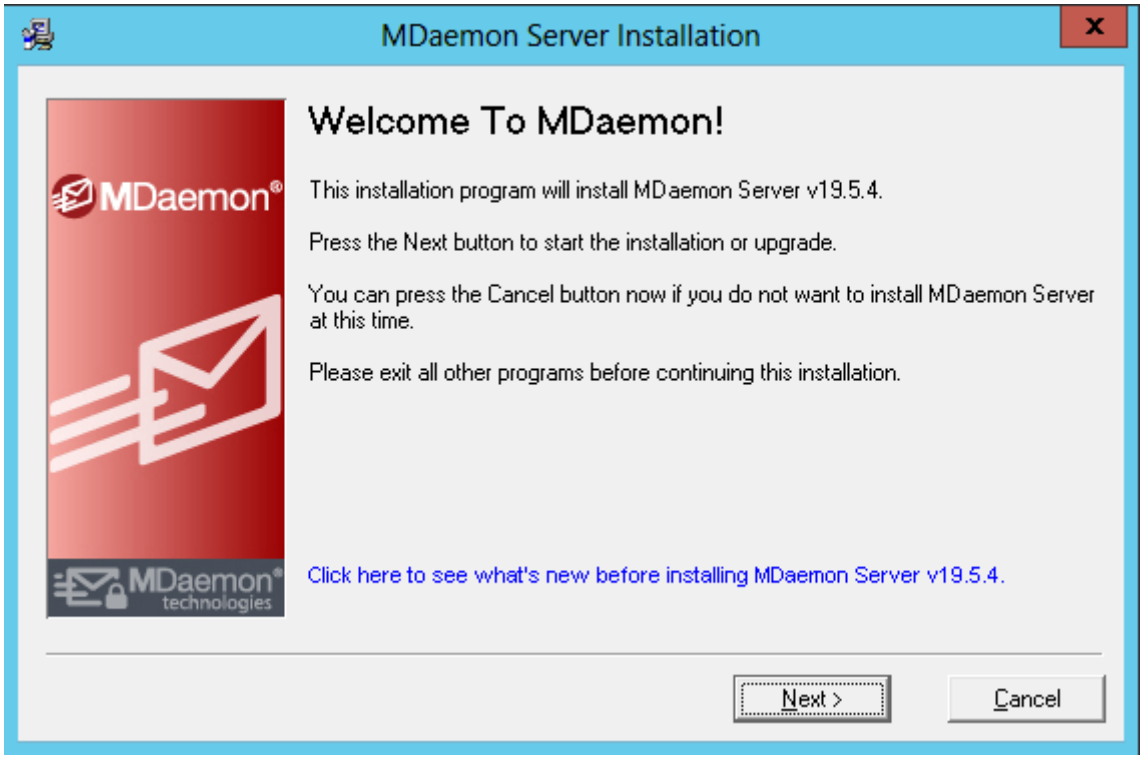
Thực hiện cài đặt và cấu hình dịch vụ Mail Server thông qua 3 bước sau:

- Bước 1: Cài đặt Mdaemon
- Bước 2: Cấu hình Mdaemon
- Bước 3: Check mail bằng giao diện Webmail

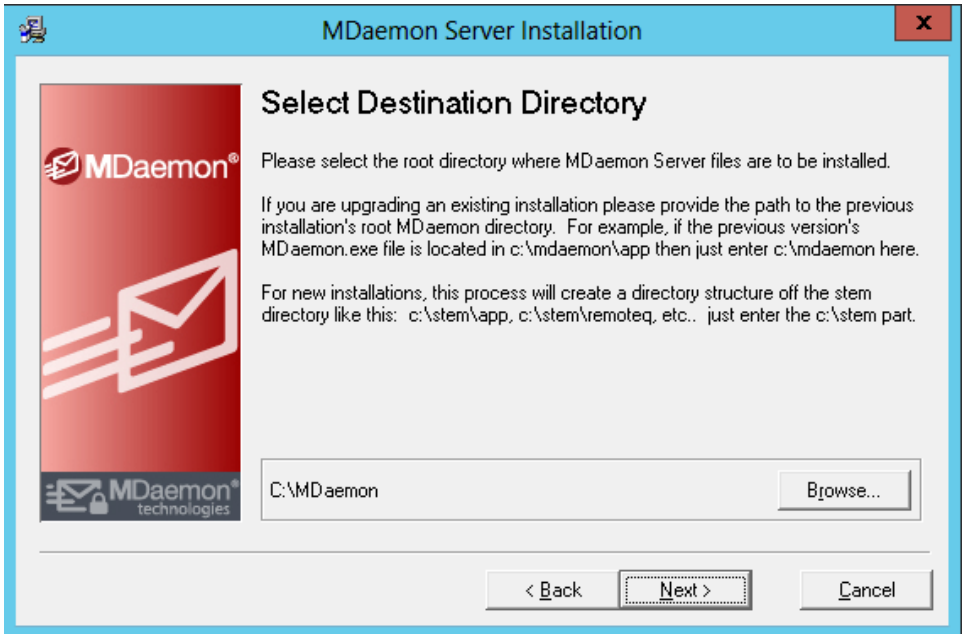
Hướng dẫn chi tiết:

Bước 1: Cài đặt Mdaemon

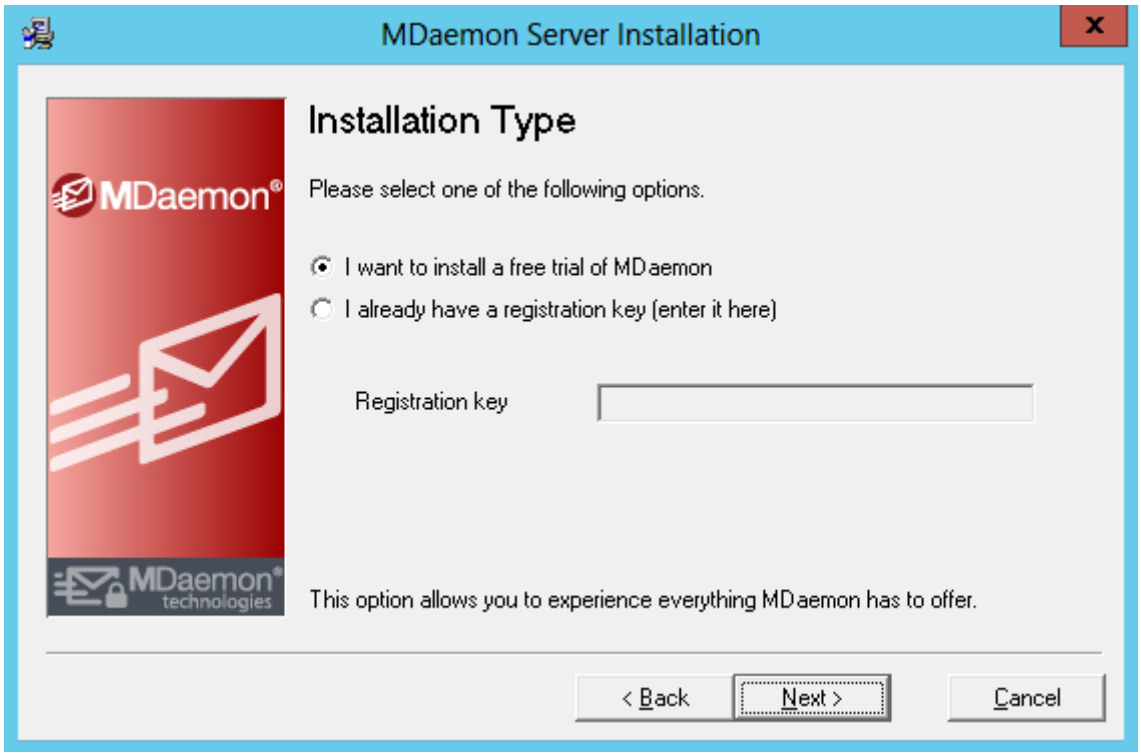
Click đúp chuột vào file cài đặt Mdaemon. Bấm ***Next*** để tiếp tục:



Chọn đường dẫn lưu trữ của chương trình, để giá trị mặc định

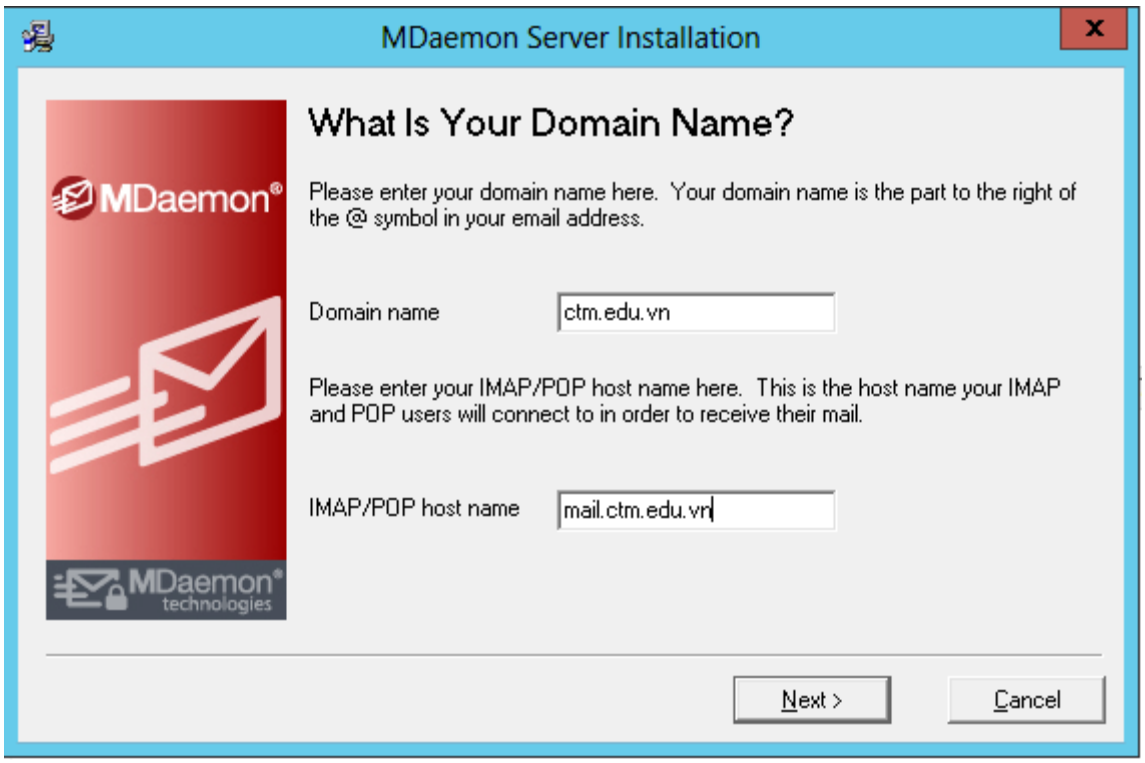


Lựa chọn phiên bản cài đặt, nếu có key đăng ký thì nhập vào ô ***Registration key***.

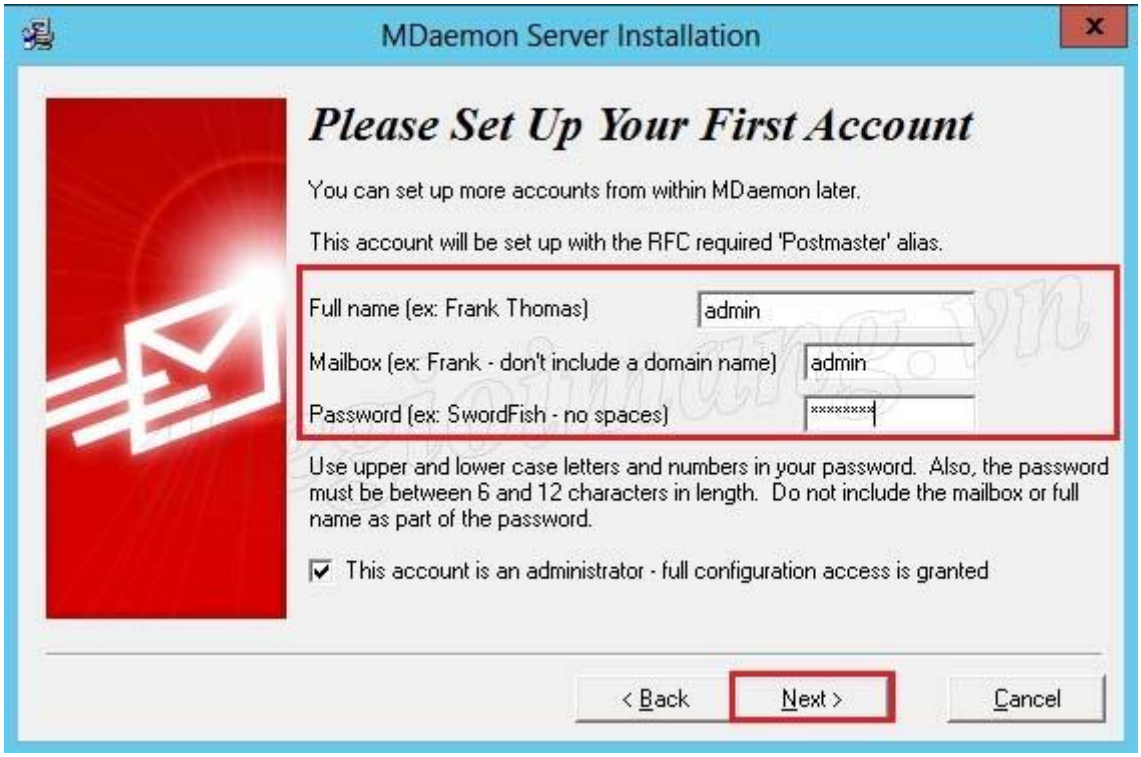


Click ***Next*** để tiến hành cài đặt

Sau khi quá trình cài đặt hoàn tất nhập vào tên của domain vào ô ***Domain name***

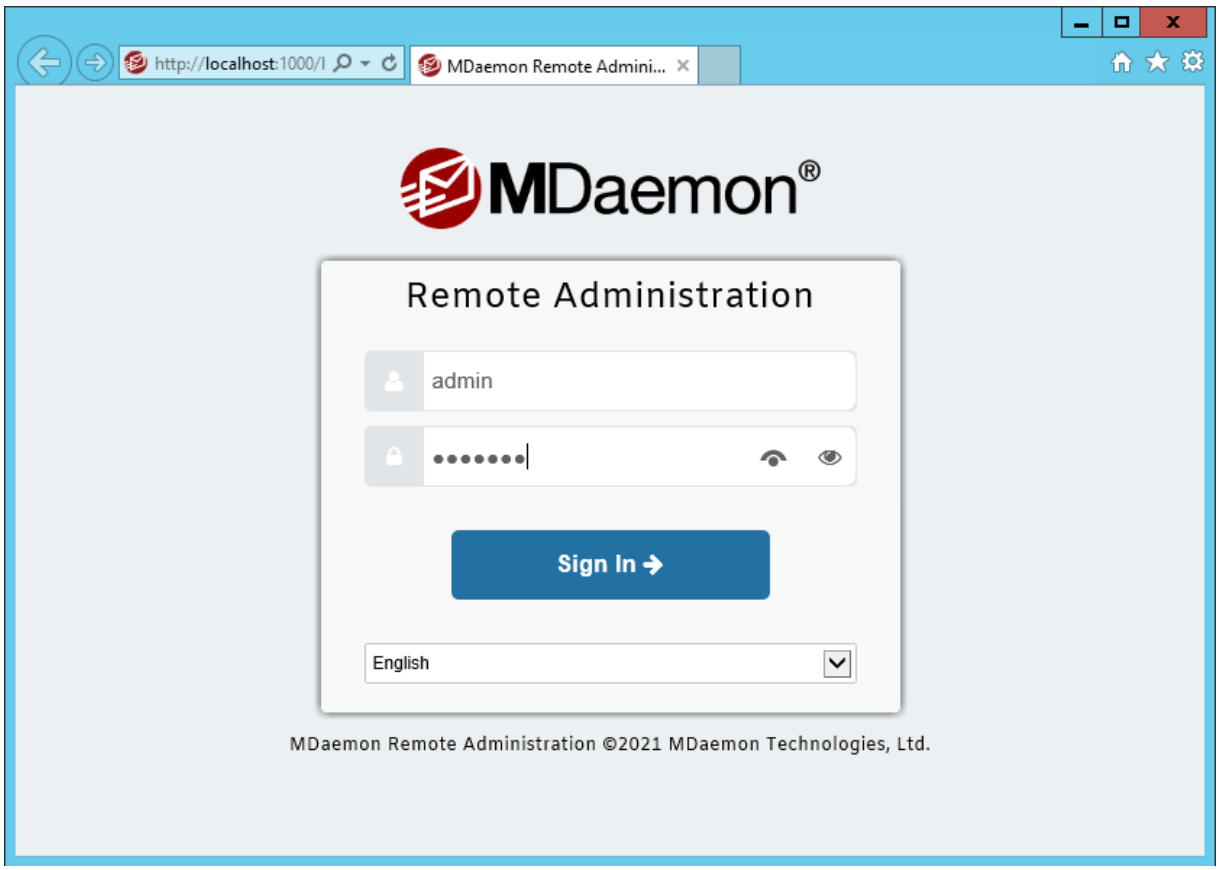


Đến bước này tạo một tài khoản administrator để quản lí mail server



Click ***Next*** sau đó Click ***Finish*** để kết thúc quá trình cài đặt

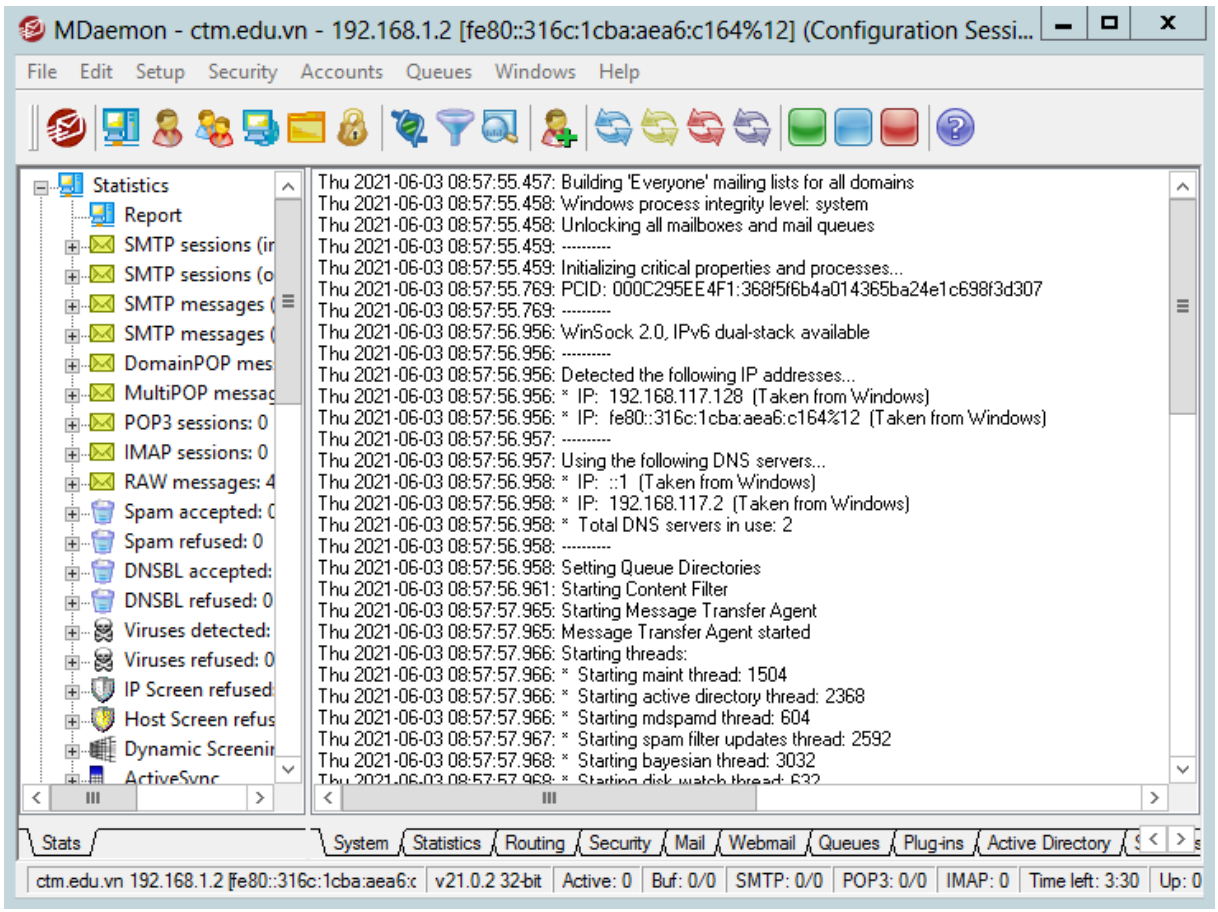
Sau khi cài đặt xong có thể truy cập vào mail server trên giao diện Web với port 1000 là web mail của Admin và port 3000 là web mail của User.



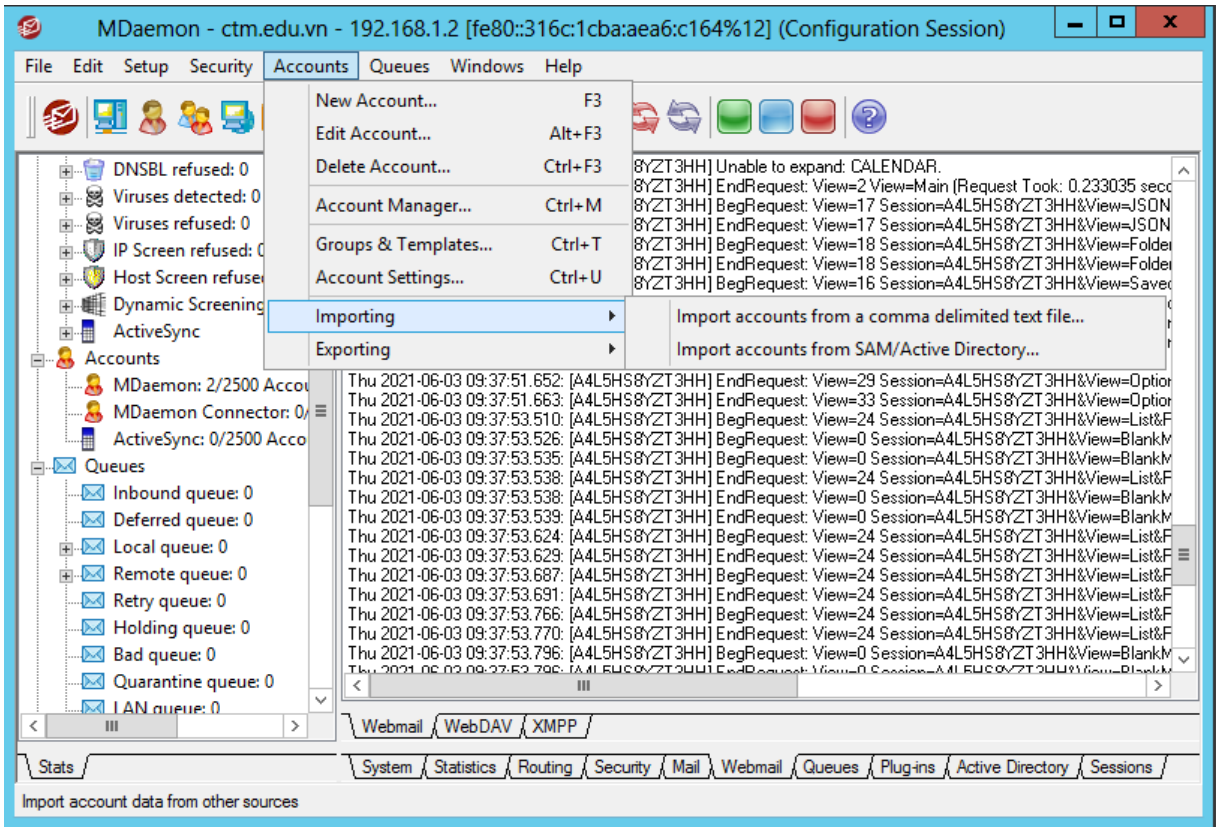
Bước 2: Cấu hình Mdaemon

Nhập người dùng (users) từ Active Directory (AD)

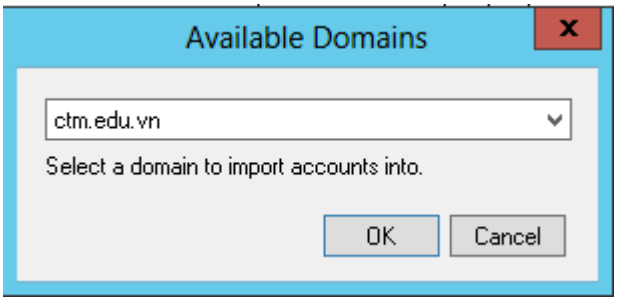
Mở ***Mdaemon configuration session***



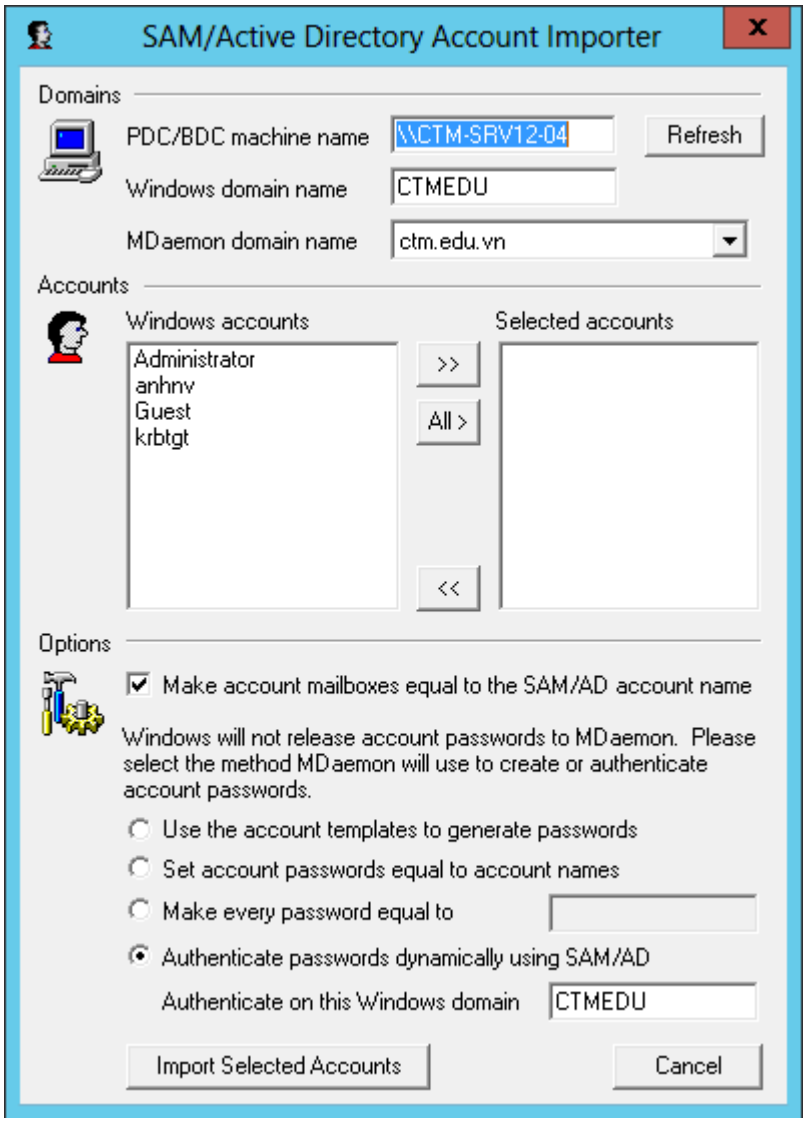
Vào menu ***Accounts*** chọn ***Inporting***, chọn ***Import accounts from SAM/Active Directory***



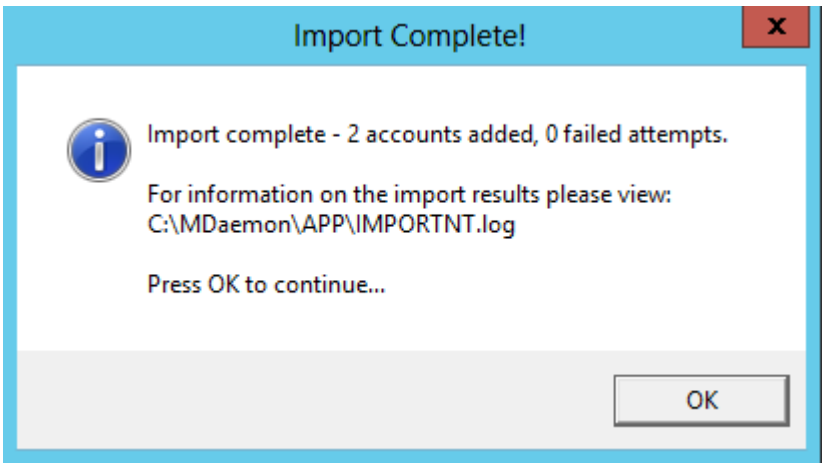
Chọn Domain trong hộp thoại ***Available Domain,*** click ***OK***



Ở hộp thoại tiếp tho, trong mục ***Windows accounts*** lựa chọn các account cần nhập vào và click nút >> sau đó click nút ***Import Selected Accounts***

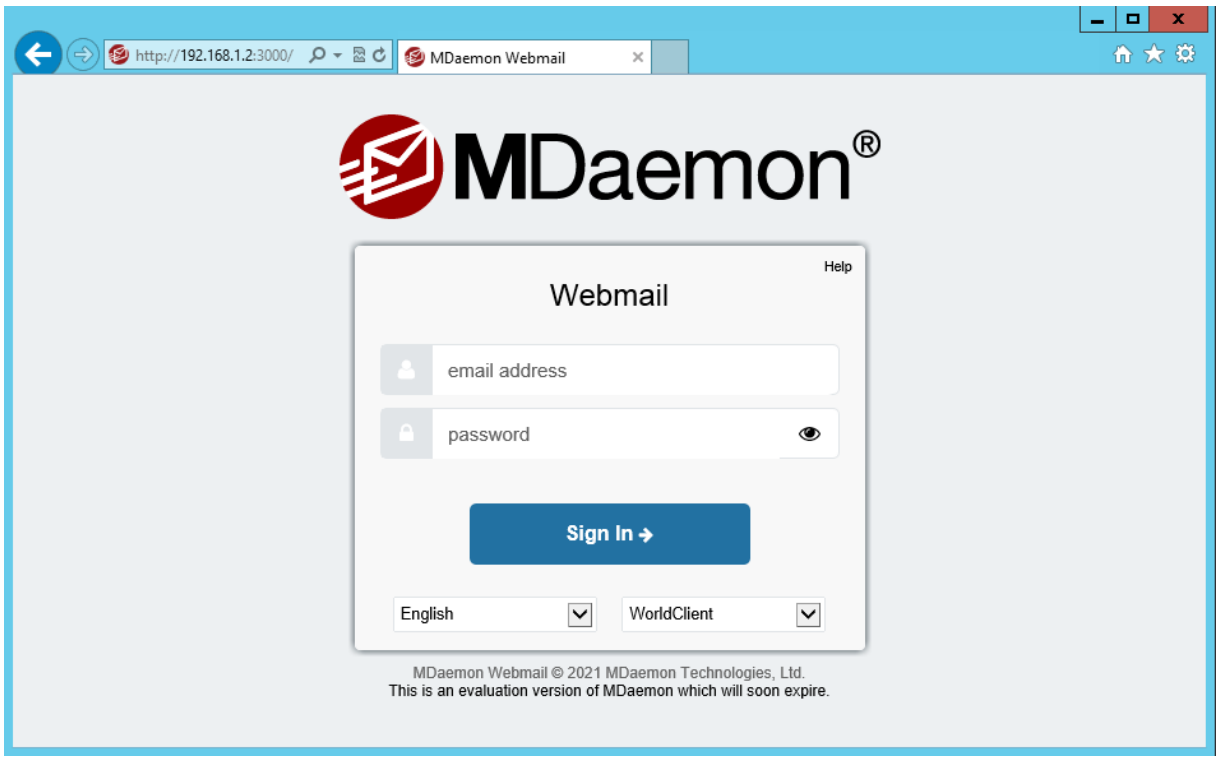


Nhập users thành công. Click OK

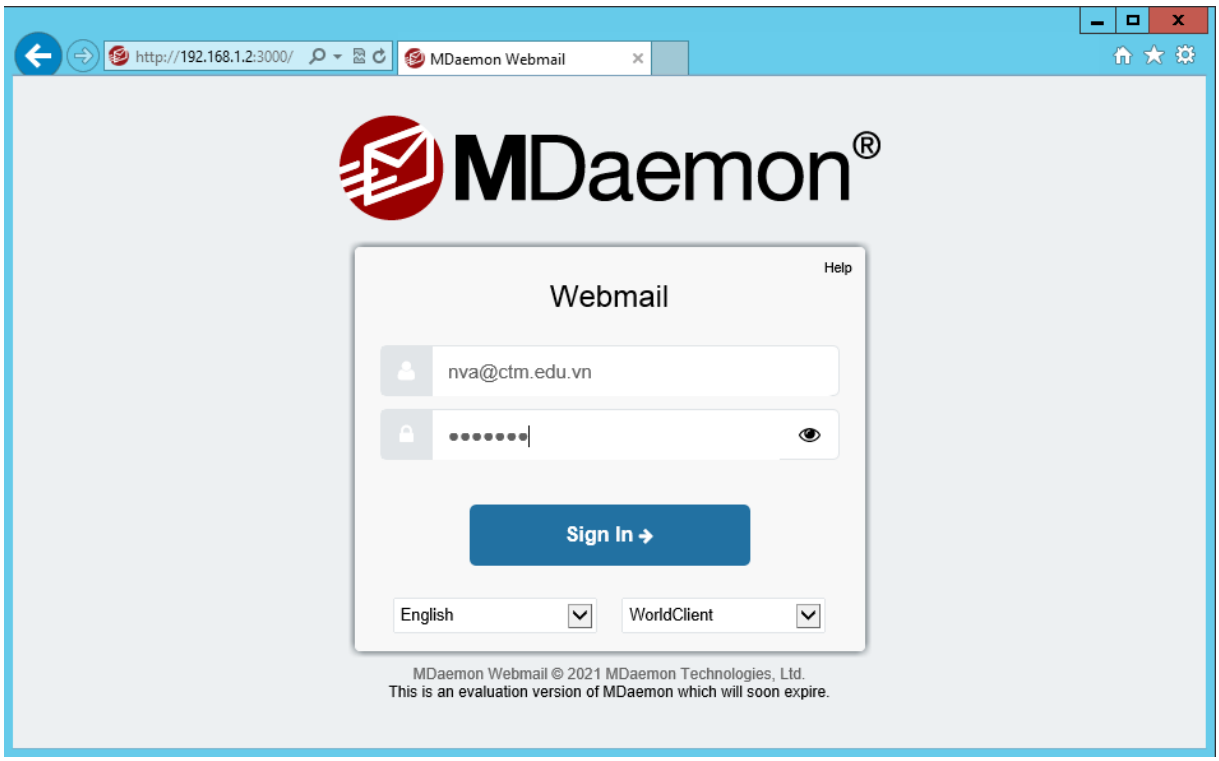


Bước 3: Check mail bằng giao diện Webmail

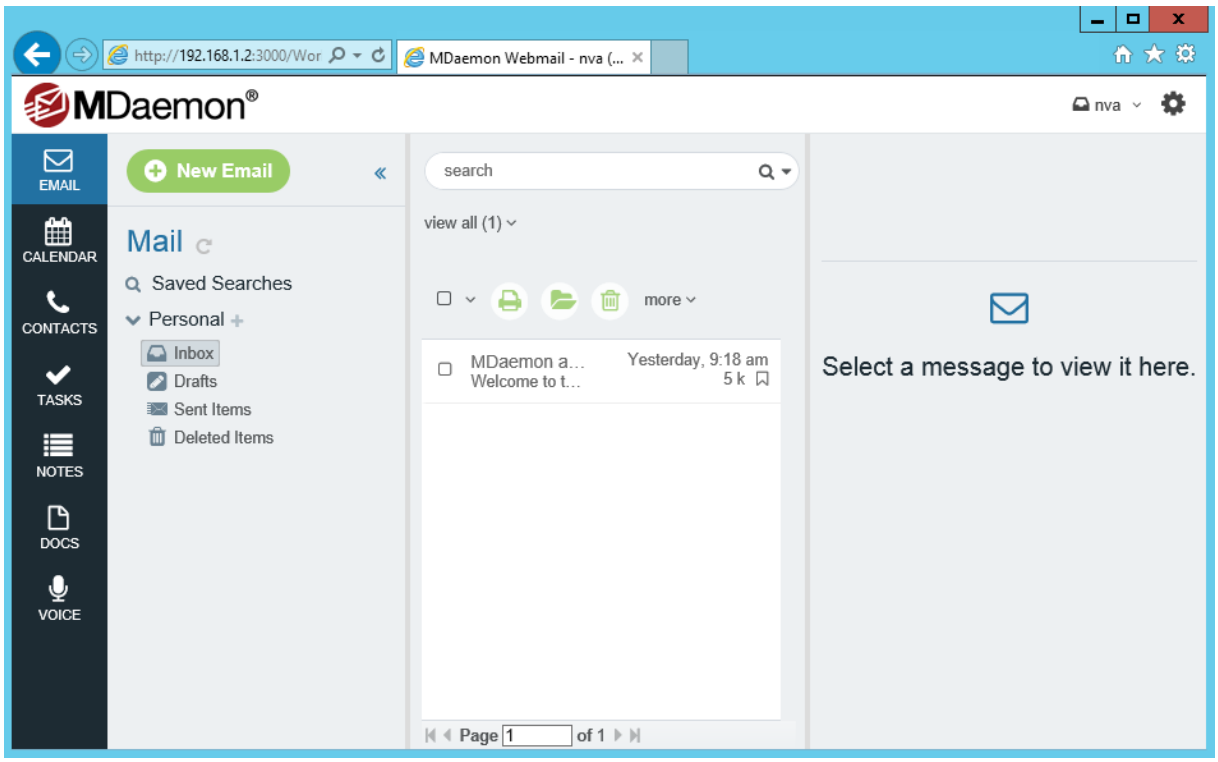
Mở trình duyệt web. Nhập địa chỉ của Webmail user với cổng 3000



Nhập tài khoản email và mật khẩu để đăng nhập



Đăng nhập thành công và kiểm tra thư mới trong mục ***Inbox***



III. Sai hỏng và cách khắc phục

1. Cài đặt và cấu hình Mail Server không thành công

- Nguyên nhân

- Thực hiện các lựa chọn chưa đúng theo hướng dẫn

- Cách khắc phục

- Thực hiện đúng các lựa chọn theo hướng dẫn thực hành

1. Đăng nhập dịch vụ Mail Server trên Webmail không thành công

- Nguyên nhân
  - Thực hiện các lựa chọn chưa đúng theo hướng dẫn
  - Chưa thực hiện việc thêm User
- Cách khắc phục
  - Thực hiện đúng các lựa chọn theo hướng dẫn thực hành
  - Thực hiện việc thêm User

V. Hướng dẫn ôn luyện

– Cài đặt và cấu hình Mail Server

– Kiểm tra việc nhận và gửi thư trên Webmail

❖ TÓM TẮT PHẦN 2

Trong phần này, một số nội dung chính được thực hành:

- Bài 1: Cài đặt và cấu hình Windows Server.
- Bài 2: Cài đặt và cấu hình Active Directory
- Bài 3: Quản trị tài khoản người dùng trên Active Directory – Tạo OU, Group, User
- Bài 4: Triển khai chính sách Group Policy
- Bài 5: Cài đặt và cấu hình dịch vụ DHCP
- Bài 6: Cài đặt và cấu hình dịch vụ DNS
- Bài 7: Triển khai dịch vụ Web với IIS
- Bài 8: Triển khai dịch vụ FTP với IIS
- Bài 9: Triển khai dịch vụ Email (Mail Server)

❖ BÀI TẬP PHẦN 2

- Bài 1: Thực hiện cài đặt và cấu hình Windows Server
- Bài 2: Thực hiện cài đặt và cấu hình Active Directory
- Bài 3: Tạo tài khoản người dùng, nhóm người dùng, tổ chức trên Active Directory
- Bài 4: Triển khai các chính sách nhóm cơ bản
- Bài 5: Cài đặt và cấu hình dịch vụ DHCP và DNS
- Bài 6: Xuất bản Website sử dụng dịch vụ IIS

TÀI LIỆU THAM KHẢO

- Phạm Hoàng Dũng, *Làm chủ Windows 2003 server*, Nhà xuất bản Thống Kê
- Microsoft. *Installing and Configuring Windows Server 2012*. Microsoft Learning, 2012.
- BACHKHOA-APTECH, *Quản trị hệ thống mạng Windows Server*, 2018
- TS Phan Thị Thu Hồng, *Bài giảng Quản trị mạng*, Học viện Nông nghiệp Việt Nam