

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM  
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG  
KHOA CÔNG NGHỆ THÔNG TIN



CAO NGUYỄN KỲ DUYÊN - 51900491

**QUẢN TRỊ HỆ THỐNG MẠNG  
DOANH NGHIỆP**

**KIẾN TẬP CÔNG NGHIỆP**

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG  
DỮ LIỆU**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM  
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG  
KHOA CÔNG NGHỆ THÔNG TIN



CAO NGUYỄN KỲ DUYÊN - 51900491

**QUẢN TRỊ HỆ THỐNG MẠNG  
DOANH NGHIỆP**

**KIẾN TẬP CÔNG NGHIỆP**

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ  
LIỆU**

Người hướng dẫn  
**Nguyễn Linh Tô**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024**

## LỜI CẢM ƠN

Em xin chân thành cảm ơn đến chị Nguyễn Linh Tố đã giúp đỡ, hướng dẫn và dìu dắt em trong quá trình tìm hiểu cho dự án CNTT 1. Nhờ như vậy, em có thể thực hiện đồ án này một cách tốt nhất và có thể đạt được một kết quả tốt nhất.

Em xin gửi lời cảm ơn chân thành đến quý công ty GREENFEED đã hỗ trợ và chia sẻ kiến thức trong quá trình em học tập và trau dồi ở đây. Sự chuyên nghiệp và tận tâm của quý công ty đã là nguồn động viên lớn giúp em có thể tận dụng trong quá trình nghiên cứu và triển khai dự án.

Và cuối cùng em cũng xin chân thành cảm ơn đến quý thầy cô trong khoa Công nghệ thông tin đã truyền đạt những kiến thức quý báu giúp em có thể hoàn thành tốt được bài báo cáo này. Khoa đã luôn sẵn sàng chia sẻ các kiến thức bổ ích cũng như chia sẻ các kinh nghiệm tham khảo tài liệu, giúp ích không chỉ cho việc thực hiện và hoàn thành đề tài nghiên cứu mà còn giúp ích cho việc học tập và rèn luyện trong quá trình thực hành tại trường Đại học Tôn Đức Thắng.

Em xin chân thành cảm ơn!

TP. Hồ Chí Minh, ngày 07 tháng 12 năm 2023

Tác giả

(Ký tên và ghi rõ họ tên)

Cao Nguyễn Kỳ Duyên

# CÔNG TRÌNH ĐƯỢC HOÀN THÀNH

## TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của chị Nguyễn Linh Tô. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong Dự án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung Dự án của mình.** Trường Đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày 07 tháng 12 năm 2023

Tác giả

(Ký tên và ghi rõ họ tên)

Cao Nguyễn Kỳ Duyên

## **TRIỂN KHAI HỆ THỐNG MẠNG DOANH NGHIỆP**

### **TÓM TẮT**

Dựa vào mô hình hệ thống mạng doanh nghiệp, dự án này sẽ triển khai trên 2 site với trụ sở chính ở miền Nam và 1 chi nhánh nằm ở miền Bắc. Cả hai site đều sẽ được thiết kế riêng biệt với đầy đủ các phòng chức năng tương ứng. Sau khi hệ thống mạng đã được cấu hình hoàn chỉnh và có thể gửi được các gói tin thành công, tiến hành quản trị hệ thống mạng với các loại dịch vụ như DNS, Active Directory Domain Services, FTP, Web Server, Group Policy Management, NTFS, Admin Template,... tạo nên một hệ thống đầy đủ chức năng. Điều này cung cấp nền tảng cho việc quản lý và điều hành mạng, đồng thời hỗ trợ các hoạt động kinh doanh của doanh nghiệp thông qua các dịch vụ IT đa dạng và hiệu quả.

## **DEPLOYMENT OF ENTERPRISE NETWORK SYSTEM**

### **ABSTRACT**

Based on the enterprise network system model, this project will be deployed across two sites, with the main headquarters located in the South and a branch in the North. Both sites will be designed independently with complete corresponding functional departments. After the network system has been fully configured and can successfully transmit packets, system management will proceed, incorporating services such as DNS, Active Directory Domain Services, FTP, Web Server, Group Policy Management, NTFS, Admin Template, establishing a comprehensive and fully functional system. This forms the foundation for network management and operation, concurrently supporting the business activities of the enterprise through diverse and efficient IT services.

## MỤC LỤC

<b>DANH MỤC HÌNH VẼ .....</b>	<b>vii</b>
<b>DANH MỤC BẢNG BIỂU .....</b>	<b>xiii</b>
<b>DANH MỤC CÁC CHỮ VIẾT TẮT.....</b>	<b>xiv</b>
<b>CHƯƠNG 1. GIỚI THIỆU VÀ KHẢO SÁT .....</b>	<b>1</b>
1.1 Giới thiệu đê tài.....	1
1.2 Khảo sát thực tế.....	1
1.3 Mô tả đê tài.....	2
<b>CHƯƠNG 2. MÔ HÌNH HỆ THỐNG .....</b>	<b>4</b>
2.1 Sơ đồ luật lý .....	4
2.2 Sơ đồ vật lý .....	4
<b>CHƯƠNG 3. THÔNG TIN CÀI ĐẶT CẤU HÌNH HỆ THỐNG .....</b>	<b>5</b>
3.1 Thông tin kết nối port trong hệ thống .....	5
3.2 Thông tin VLAN, Interface VLAN trong hệ thống .....	7
3.3 Thông tin thiết kế quy hoạch địa chỉ IP Planning .....	10
<b>CHƯƠNG 4. QUẢN TRỊ HỆ THỐNG MẠNG .....</b>	<b>13</b>
4.1 Cấu hình Server.....	13
4.1.1 DNS Server.....	13
4.1.2 Alternative DNS .....	18
4.1.3 Active Directory Domain Service .....	20
4.1.4 DHCP Server .....	25
4.1.5 Web Server .....	32
4.1.6 FTP Server .....	35

4.1.7 <i>NTP Syslog Server</i> .....	37
4.2 Group Policy Management .....	39
4.2.1 <i>Chỉnh sửa Password</i> .....	40
4.2.2 <i>Cho phép Group Users có quyền Log on Locally</i> .....	43
4.2.3 <i>Tạo và link Policy vào OU</i> .....	44
4.2.4 <i>Block Inheritance cho OU</i> .....	46
4.2.5 <i>Enforce Policy</i> .....	48
4.2.6 <i>Chỉnh thứ tự cho Policy</i> .....	50
4.2.7 <i>Một số GPO cơ bản</i> .....	52
4.3 NTFS .....	65
4.3.1 <i>Phân quyền thư mục bằng Standard Permission</i> .....	66
4.3.2 <i>Phân quyền thư mục bằng Special Permission</i> .....	75
4.3.3 <i>Take Owner Ship</i> .....	76
<b>CHƯƠNG 5. KẾT LUẬN.....</b>	<b>80</b>
5.1 Kết luận .....	80
5.2 Hướng phát triển .....	80
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>81</b>

## **DANH MỤC HÌNH VẼ**

Hình 1.2: Quá trình hình thành và phát triển của GreenFeed .....	2
Hình 2.1: Sơ đồ luận lý .....	4
Hình 2.2 Sơ đồ vật lý .....	4
Hình 4.1.1a: Hai server ở 2 site.....	13
Hình 4.1.1b: Install DNS Server ở mục add Role and Feature .....	14
Hình 4.1.1c: Sau khi đã cài đặt thành công DNS Server, tiến hành vào DNS Manager để cấu hình .....	14
Hình 4.1.1d: Nhập đường mạng của DNS Server.....	15
Hình 4.1.1e: Tương tự Tạo Zone mới ở vùng Forward .....	15
Hình 4.1.1f: Tạo bản ghi A và CNAME cho domain của Web Server.....	16
Hình 4.1.1g: Kiểm tra DNS.....	17
Hình 4.1.1h: Để thực hiện phân giải tên miền các địa chỉ ở bên ngoài mạng LAN ta sẽ cài đặt DNS recursive .....	17
Hình 4.1.1i: Mở CMD -> Nhập lệnh <b>net stop dns &amp;&amp; net start dns</b> để khởi động lại dịch vụ DNS .....	18
Hình 4.1.2a: Dùng server miền Bắc để làm DNS Alternative .....	18
Hình 4.1.2b: Tạo Zone cho Forward Lookup Zone .....	19
Hình 4.1.2c: Tạo Zone cho Reverse Lookup Zone .....	19
Hình 4.1.2d: Cấu hình backup trên cả 2 server DNS .....	20
Hình 4.1.3a: Install AD .....	21
Hình 4.1.3b: Thêm domain và password backup là 2023@yg .....	21
Hình 4.1.3c: Quản lý AD .....	22
Hình 4.1.3d: Tạo OU đại diện cho 2 site .....	22

Hình 4.1.3e: Tạo Group cho các phòng ban .....	23
Hình 4.1.3f: Tạo Users .....	23
Hình 4.1.3g: Thêm các user vào các nhóm phòng ban .....	24
Hình 4.1.3h: Sử dụng máy client để join domain .....	24
Hình 4.1.3i: Các bước join domain .....	25
Hình 4.1.3j: Restart máy và thực hiện login lại .....	25
Hình 4.1.4a: Sử dụng tên đăng nhập và mật khẩu: 2023@yg để đăng nhập vào server. ....	26
Hình 4.1.4b: Giao diện màn hình quản lý của Server .....	27
Hình 4.1.4c: Chọn Tab Manage .....	27
Hình 4.1.4d: Chọn Add Role and Feature.....	28
Hình 4.1.4e: Sau khi đã cài đặt, DHCP sẽ hiển thị ở tab Tool.....	28
Hình 4.1.4f: Chọn New Scope để tạo VLAN .....	29
Hình 4.1.4g: Tạo pool VLAN .....	29
Hình 4.1.4h: Đặt tên VLAN .....	30
Hình 4.1.4j: Nhập địa chỉ IP không cấp phát .....	30
Hình 4.1.4k: Nhập Default Gateway của VLAN .....	31
Hình 4.1.4l: Cấu hình IP tĩnh cho Server .....	32
Hình 4.1.5a: Tắt trang web mặc định của web server.....	33
Hình 4.1.5b: Tạo website mới.....	33
Hình 4.1.5c: Giao diện quản lý website .....	34
Hình 4.1.5d: Bật Directory Browsing .....	34
Hình 4.1.5e: Giao diện của trang web.....	35

Hình 4.1.6a: Cài đặt FTP ở mục IIS.....	36
Hình 4.1.6b: Cấu hình truy cập có tài khoản .....	36
Hình 4.1.7a: Chạy gpedit.msc để cài đặt NTP .....	37
Hình 4.1.7b: Bật các dịch vụ trong NTP.....	38
Hình 4.1.7c: Bật các dịch vụ trong NTP .....	38
Hình 4.1.7c: Restart dịch vụ Windows Time.....	38
Hình 4.1.7d: Cài đặt Rules cho Inbound .....	39
Hình 4.2a: Mở GPO .....	40
Hình 4.2b: Hai Policy mặc định của hệ thống .....	40
Hình 4.2.1a: Chọn Default Domain Policy => chuột phải chọn Edit .....	41
Hình 4.2.1b: Vào Password Policy .....	41
Hình 4.2.1c: Các Policy trong Password Policy .....	42
Hình 4.2.1d: Độ dài tối thiểu của password là 6 và Disable chính sách password phức tạp. ....	43
Hình 4.2.2a: Add Group có quyền được Log on Locally .....	43
Hình 4.2.2b: Cập nhật chính sách .....	44
Hình 4.2.3a: Thêm GPO mới .....	44
Hình 4.2.3b: Tạo GPO mới .....	45
Hình 4.2.3c: Edit chính sách vừa tạo .....	45
Hình 4.2.3e: Link OU với GPO vừa tạo. ....	46
Hình 4.2.3f: Máy Client sau khi áp dụng chính sách sẽ không thể mở Control Panel .....	46
Hình 4.2.4a: Block Inheritance cho OU Test.....	47
Hình 4.2.4b: OU Test sẽ có dấu chấm thang .....	47

Hình 4.2.4c: Các máy client trong OU Test sẽ thấy được Control Panel .....	48
Hình 4.2.5a: Mở Group Policy Management và chọn Enforced cho GPO "Hide Control Panel" .....	49
Hình 4.2.5b: Các máy client sau khi được áp chính sách sẽ không thể mở Control Panel .....	50
Hình 4.2.6a: Lúc này ở OU HO sẽ có 2 policy .....	50
Hình 4.2.6b: Chuyển Policy lên thứ tự 1 .....	51
Hình 4.2.6c: Precedence hiện tại của Policy ở tab Control Panel là 1 .....	51
Hình 4.2.6d: Lúc này các máy client đã có thể mở Control Panel.....	52
Hình 4.2.7a: Tạo GPO mới với tên “Remove Recycle Bin” .....	53
Hình 4.2.7b: Vào mục Remove Recycle Bin icon from desktop và enabled.....	53
Hình 4.2.7c: Link GPO vừa tạo với OU và Update chính sách .....	54
Hình 4.2.7d: Icon Recycle Bin đã mất khỏi màn hình.....	54
Hình 4.2.7e: Bật mục Hide specified Control Panel items .....	55
Hình 4.2.7f: Icon Mouse bị mất trong tab Control Panel của các máy client.....	56
Hình 4.2.7g: Enabled mục Prevent changing theme .....	57
Hình 4.2.7h: Máy client lúc này không thể đổi theme .....	57
Hình 4.2.7i: Enabled mục Prohibit access to properties of a LAN connection .....	58
Hình 4.2.j: Các máy client trong OU HO sẽ không thể chỉnh sửa địa chỉ IP .....	58
Hình 4.2.7k: Enabled mục Lock the Taskbar.....	59
Hình 4.2.7l: Taskbar đã bị khóa trên các máy client.....	59
Hình 4.2.7m: Enabled mục Prevent access to the command prompt.....	60
Hình 4.2.7n: Enabled mục Don't run specified Windows applications.....	61

Hình 4.2.7o: Ở phần List of disallowed applications => Chọn Show và nhập ứng dụng không cho sử dụng .....	61
Hình 4.2.7p: CMD khi mở sẽ có thông báo như sau.....	62
Hình 4.2.7q: Tạo GPO trong OU HO với tên “New Script” và chọn Edit .....	63
Hình 4.2.7r: Vào phần Windows Setting và chọn Logon .....	63
Hình 4.2.7s: Tạo một file logon.vbs và nhập nội dung như trên .....	64
Hình 4.2.7t: Add file vừa tạo vào logon.....	64
Hình 4.2.7u: Khi logon vào máy client sẽ hiển thị box chào như sau .....	65
Hình 4.3a: Tạo cây thư mục chứa data.....	66
Hình 4.3b: Users trong các phòng ban .....	66
Hình 4.3.1a: Share folder DATA .....	67
Hình 4.3.1b: Mở tab Advanced trên thư mục DATA .....	67
Hình 4.3.1c: Chọn Disable inheritance và chọn Convert inherited permission into explicit permission on this object.....	68
Hình 4.3.1d: Quay về cửa sổ Properties và chọn Edit .....	68
Hình 4.3.1e: Add quyền cho hai phòng ban trên .....	68
Hình 4.3.1f: Remove Group Users.....	69
Hình 4.3.1g: Các máy client truy cập thành công vào mục DATA .....	69
Hình 4.3.1h: Máy client tạo một folder bất kỳ và bị lỗi.....	70
Hình 4.3.1i: Phân quyền Full Control cho hai phòng ban.....	70
Hình 4.3.1j: Các máy ở hai phòng ban truy cập thành công vào folder CHUNG ...	71
Hình 4.3.1k: Các máy ở hai phòng ban có thể tạo và xóa folder bất kỳ trong mục CHUNG.....	72
Hình 4.3.1l: Gỡ bỏ kệ thừa.....	73

Hình 4.3.1m: Phòng Kế toán truy cập được còn IT không truy cập được.....	73
Hình 4.3.1n: Máy phòng Kế toán có thể tạo xóa file bất kỳ trong folder KETOAN	74
Hình 4.3.1o: Xóa Group KETOAN và phân quyền cho Group IT .....	74
Hình 4.3.1p: Phòng IT truy cập được còn Kế toán không truy cập được .....	75
Hình 4.3.2a: Trong cửa sổ Permission Entry for KeToan, nhấn vào liên kết Show advanced permissions.....	75
Hình 4.3.2b: Ở mục Allow, tắt dấu chọn ở ô Delete subfolders and files và Delete => Chọn OK 4 lần .....	76
Hình 4.3.2c: Máy KT2 tạo file và KT1 xóa file sẽ bị báo lỗi .....	76
Hình 4.3.3a: Phân quyền cho IT1FILE .....	77
Hình 4.3.3b: Không thể truy cập được folder IT1FILE .....	77
Hình 4.3.3c: Truy cập vào Properties của folder IT1FILE .....	78
Hình 4.3.3d: Replace owner on subcontainers and object trên file IT1FILE .....	78
Hình 4.3.3e: Administrator đã có quyền Full Control .....	79

## **DANH MỤC BẢNG BIỂU**

Bảng 1.1 Các thiết bị được sử dụng trong mô hình .....	2
Bảng 3.1: Bảng thông tin kết nối port trong hệ thống.....	7
Bảng 3.2a: Bảng thông tin VLAN HO.....	9
Bảng 3.2b: Bảng thông tin VLAN Miền Bắc.....	10
Bảng 3.3a Bảng thông tin IP khu vực Server miền Nam .....	10
Bảng 3.3b Bảng thông tin IP khu vực Server miền Bắc .....	10
Bảng 3.3c Bảng thông tin IP .....	12

**DANH MỤC CÁC CHỮ VIẾT TẮT**

VLAN	Virtual Local Area Network
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
GPO	Group Policy Object
AD DS	Active Directory Domain Services
NTP	Network Time Protocol
NTFS	New Technology File System

# CHƯƠNG 1. GIỚI THIỆU VÀ KHẢO SÁT

## 1.1 Giới thiệu về tài

Ngành công nghệ thông tin đã và đang có nhiều thay đổi to lớn và tác động sâu sắc vào cuộc sống cũng như cách sống của mỗi chúng ta. Có thể thấy, chúng ta dường như không thể cách xa được các thiết bị điện tử chẳng hạn như máy tính hay điện thoại,. Nó đã trở nên vô cùng quan trọng trong các công việc hàng ngày từ học tập cũng như công việc. Và để đáp ứng các nhu cầu trong việc giao tiếp, gửi tin nội bộ, tìm kiếm thông tin,... trong các doanh nghiệp hay trường học thì việc triển khai một hạ tầng mạng với các chức năng và bảo mật là vô cùng cần thiết cho một doanh nghiệp để tránh các cuộc tấn công nội bộ với những hậu quả vô cùng nghiêm trọng.

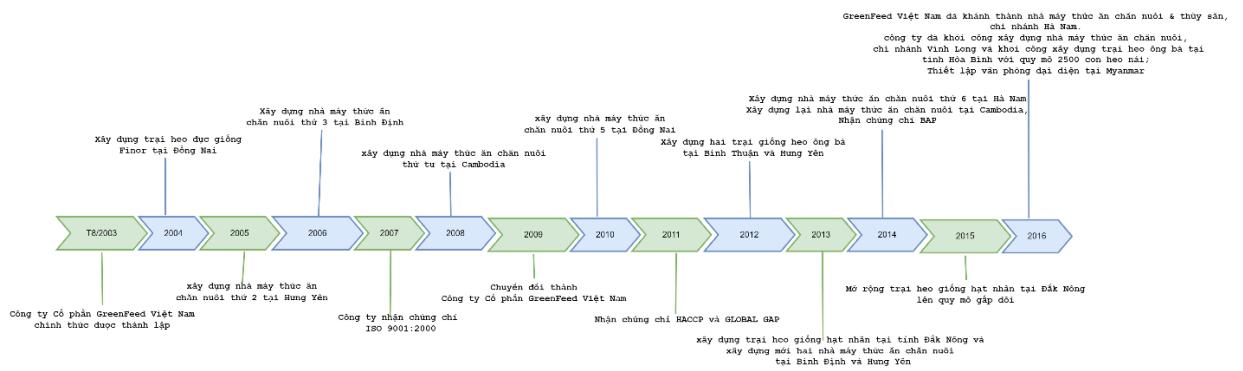
Do đó, mục đích của bài báo cáo này là nghiên cứu, phân tích những đặc điểm của hệ thống mạng, những kỹ thuật tấn công hệ thống mạng để từ đó đưa ra những giải pháp an ninh, bảo mật dựa trên các tiêu chí dựa trên hai khía cạnh: đảm bảo an toàn dữ liệu và toàn vẹn dữ liệu.

## 1.2 Khảo sát thực tế

GreenFeed VN có tên đầy đủ là Công ty Cổ phần GreenFeed Việt Nam, tiền thân là Công ty trách nhiệm hữu hạn GreenFeed Việt Nam, được thành lập vào năm 2003 với tầm nhìn đưa thương hiệu GreenFeed VN dẫn đầu trong ngành thực phẩm.

Với khởi đầu trong ngành thức ăn chăn nuôi và sản xuất thức ăn cho gia súc, gia cầm, thủy sản. Hiện nay, GreenFeed đã có hệ thống bao gồm 9 nhà máy hiện đại tại Việt Nam, Campuchia, Myanmar, Lào. Những nhà máy này được trang bị công nghệ sản xuất từ Mỹ và Châu u, công suất mỗi năm là 2 triệu tấn sản phẩm đạt tiêu chuẩn ISO 22.000, HACCP, GLOBAL GAP, BAP. Toàn hệ thống hoạt động một cách chuyên nghiệp bằng việc ứng dụng giải pháp hoạch định nguồn lực doanh nghiệp (ERP).

Quá trình hình thành và phát triển của GreenFeed



Hình 1.2: Quá trình hình thành và phát triển của GreenFeed

Dựa vào những quan sát, nghiên cứu và học tập ở đây, em đã có ý tưởng về việc triển khai và bảo mật hệ thống mạng doanh nghiệp trong ngành sản xuất. Tuy nhiên để đơn giản hóa trong quá trình nghiên cứu và triển khai, cùng với kinh nghiệm hạn chế của mình, dự án này sẽ tập trung xây dựng một hệ thống mạng nhỏ hơn chỉ với 2 site.

Đối với hệ thống mạng trên, những thiết bị cần thiết để sử dụng sẽ bao gồm những thiết bị sau:

STT	Thiết bị	Hãng	Số lượng
1	Router	Cisco	4
2	Multilayer Switch	Cisco	7
3	Switch Access	Cisco	8
4	Laptop, PC	Dell	Theo thực tế
5	Server	Windows	2

Bảng 1.1 Các thiết bị được sử dụng trong mô hình

### 1.3 Mô tả đề tài

Công ty sản xuất này có một trụ sở chính tại miền Nam và một chi nhánh tại miền Bắc, với sự phân bổ rõ ràng của các phòng ban như sau:

Tại văn phòng miền Nam:

Tầng 1: Lễ tân và phục vụ khách hàng

Tầng 2: Nhân sự, Bộ phận Marketing, và Kế toán

Tầng 3: Phòng IT

Tầng 4: Kiểm toán, Truyền thông, và Phát triển bền vững

Tầng 5: Phòng của Giám đốc và Phó giám đốc

Tại văn phòng miền Bắc, có một chuỗi nhà máy sản xuất và các phòng ban chính như sau:

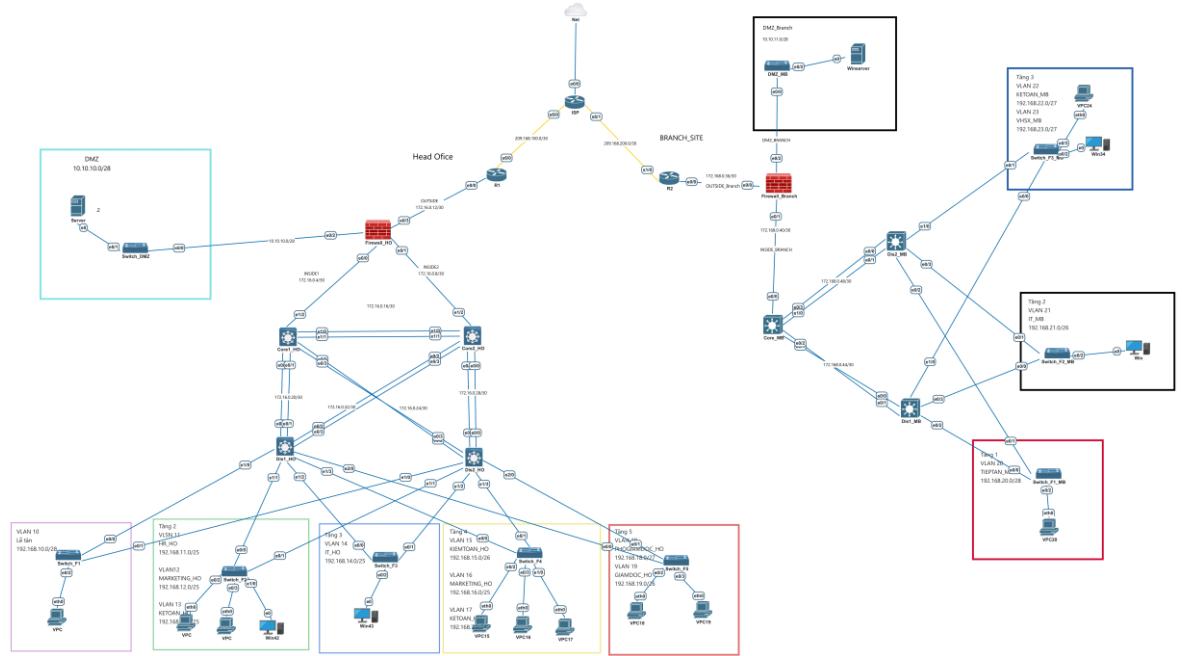
Khu văn phòng với các bộ phận Kế toán, IT, Quản lý, và phòng họp.

Khu nhà máy sản xuất, được quản lý bởi Bộ phận Tự động hóa.

Sau khi triển khai hệ thống mạng thành công với các chức năng cơ bản, công ty sẽ tiếp tục quản trị hệ thống mạng. Các dịch vụ cơ bản trên Windows Server và Group Policy Management sẽ được sử dụng để quản lý các máy client. Máy chủ sẽ chứa các Roles như DHCP, Mail, DNS, Web, FTP, và AAA, cung cấp nền tảng cho các hoạt động kinh doanh và sản xuất hiệu quả.

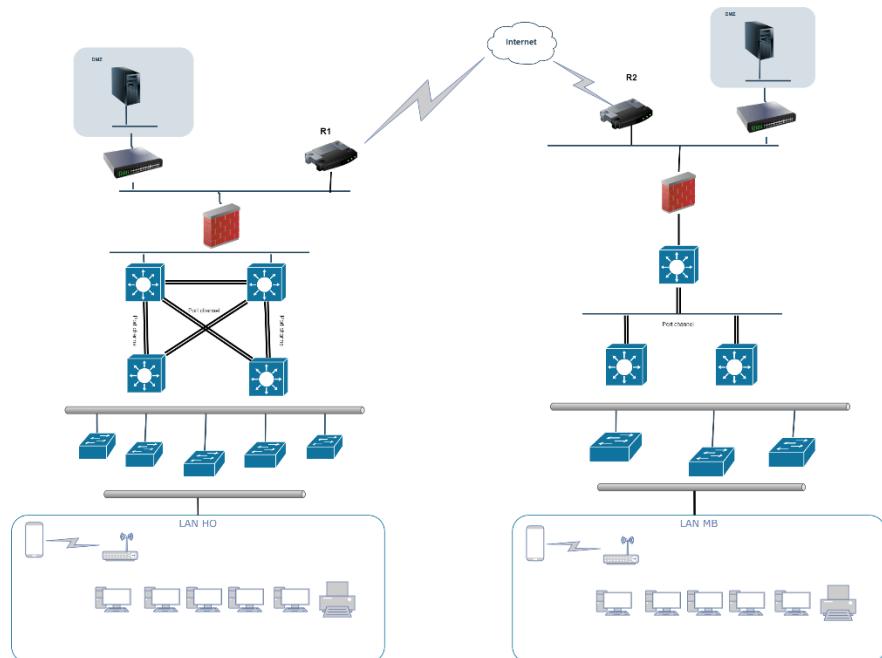
## CHƯƠNG 2. MÔ HÌNH HỆ THỐNG

### 2.1 Sơ đồ luận lý



Hình 2.1: Sơ đồ luận lý

### 2.2 Sơ đồ vật lý



Hình 2.2 Sơ đồ vật lý

## CHƯƠNG 3. THÔNG TIN CÀI ĐẶT CẤU HÌNH HỆ THỐNG

### 3.1 Thông tin kết nối port trong hệ thống

Source to destination	Source Interface	Destination Interface	Protocol	Trunking/VLAN
<b>Server to Switch DMZ</b>	e0	e0/1	Ethernet	
<b>Router Firewall to Switch DMZ</b>	e0/2	e0/0	Ethernet	
<b>Router Firewall to R1</b>	e0/3	e0/0	Ethernet	
<b>Router Firewall to Core 1</b>	e0/0	e1/2	Ethernet	
<b>Router Firewall to Core 2</b>	e0/1	e1/2	Ethernet	
<b>Core 1 to Core 2</b>	port-channel 3	port-channel 3	Ethernet	Port-channel
<b>Core 1 to Dis1_HO</b>	port-channel 1	port-channel 1	Ethernet	Port-channel
<b>Core 1 to Dis2_HO</b>	port-channel 2	port-channel 2	Ethernet	Port-channel
<b>Core 2 to Dis1_HO</b>	port-channel 2	port-channel 2	Ethernet	Port-channel
<b>Core 2 to Dis2_HO</b>	port-channel 1	port-channel 1	Ethernet	Port-channel
<b>Dis1_HO to F1_HO</b>	E1/0	e0/0	Ethernet	Trunking
<b>Dis1_HO to F2_HO</b>	E1/1	e0/0	Ethernet	Trunking
<b>Dis1_HO to F3_HO</b>	E1/2	e0/0	Ethernet	Trunking
<b>Dis1_HO to F4_HO</b>	E1/3	e0/0	Ethernet	Trunking
<b>Dis1_HO to F5_HO</b>	E2/0	e0/0	Ethernet	Trunking
<b>Dis2_HO to F1_HO</b>	E1/0	e0/1	Ethernet	Trunking

<b>Source to destination</b>	<b>Source Interface</b>	<b>Destination Interface</b>	<b>Protocol</b>	<b>Trunking/VLAN</b>
<b>Dis2_HO to F2_HO</b>	E1/1	e0/1	Ethernet	Trunking
<b>Dis2_HO to F3_HO</b>	E1/2	e0/1	Ethernet	Trunking
<b>Dis2_HO to F4_HO</b>	E1/3	e0/1	Ethernet	Trunking
<b>Dis2_HO to F5_HO</b>	E2/0	e0/1	Ethernet	Trunking
<b>F1_HO to LETAN_HO</b>	e0/2	e0	Ethernet	VLAN
<b>F2_HO to HR_HO</b>	e0/2	e0	Ethernet	VLAN
<b>F2_HO to MARKETING_HO</b>	e0/3	e0	Ethernet	VLAN
<b>F2_HO to KETOAN_HO</b>	e1/0	e0	Ethernet	VLAN
<b>F3_HO to IT_HO</b>	e0/2	e0	Ethernet	VLAN
<b>F4_HO to KIEMTOAN_HO</b>	e0/2	e0	Ethernet	VLAN
<b>F4_HO to TRUYENTHONG_HO</b>	e0/3	e0	Ethernet	VLAN
<b>F4_HO to PTBV_HO</b>	e1/0	e0	Ethernet	VLAN
<b>F5_HO to GIAMDOC_HO</b>	e0/2	e0	Ethernet	VLAN
<b>F5_HO to PHOGIAMDOC_HO</b>	e0/3	e0	Ethernet	VLAN
<b>R1 to ISP</b>	S6/0	S6/0	Serial	
<b>ISP to R2</b>	S6/1	S1/0	Serial	
<b>R2 to Firewall_Branch</b>	E0/0	E0/0	Ethernet	
<b>Firewall_Branch to DMZ_MB</b>	E0/2	E0/0	Ethernet	

<b>Source to destination</b>	<b>Source Interface</b>	<b>Destination Interface</b>	<b>Protocol</b>	<b>Trunking/VLAN</b>
<b>Firewall_Branch to Core_MB</b>	E0/1	E0/0	Ethernet	
<b>DMZ_MB to Server_MB</b>	E0/2	E0	Ethernet	
<b>Core_MB to Dis1_MB</b>	port-channel1	Port-channel 1		
<b>Core_MB to Dis2_MB</b>	port-channel2	Port-channel 2		
<b>Dis1_MB to F1_MB</b>	E0/2	E0/0		Trunking
<b>Dis1_MB to F2_MB</b>	E0/3	E0/0		Trunking
<b>Dis1_MB to F3_MB</b>	E1/0	E0/0		Trunking
<b>Dis2_MB to F1_MB</b>	E0/2	E0/1		Trunking
<b>Dis2_MB to F2_MB</b>	E0/3	E0/1		Trunking
<b>Dis2_MB to F3_MB</b>	E1/0	E0/1		Trunking
<b>F1_MB to TIEPTAN_MB</b>	E0/2	E0		VLAN
<b>F2_MB to IT_MB</b>	E0/2	E0		VLAN
<b>F3_MB to VHSX_MB</b>	E0/2	E0		VLAN
<b>F3_MB to KETOAN_MB</b>	E0/3	E0		VLAN

Bảng 3.1: Bảng thông tin kết nối port trong hệ thống

### 3.2 Thông tin VLAN, Interface VLAN trong hệ thống

 Khu vực miền Nam

<b>PHÒNG BAN</b>	<b>VLA N ID</b>	<b>NAME</b>	<b>IP SIZ E</b>	<b>GATEWAY</b>	<b>IP RANGE</b>
LỄ TÂN	10	LETAN_HO	14	192.168.10.1/ 28	192.168.10.1 - 192.168.10.1 4
NHÂN SỰ	11	HR_HO	80	192.168.11.1/ 25	192.168.11.1 - 192.168.11.1 26
MARKETING	12	MARKETING_HO	80	192.168.12.1/ 25	192.168.12.1 - 192.168.12.1 26
KẾ TOÁN	13	KETOAN_HO	100	192.168.14.1/ 25	192.168.14.1 - 192.168.14.1 26
IT	14	IT_HO	90	192.168.14.1/ 25	192.168.14.1 - 192.168.14.1 26
KIỂM TOÁN	15	KIEMTOAN_HO	60	192.168.15.1/ 26	192.168.15.1 - 192.168.15.6 2
TRUYỀN THÔNG	16	TRUYENTHONG_ HO	80	192.168.16.1/ 25	192.168.16.1 -

<b>PHÒNG BAN</b>	<b>VLA N ID</b>	<b>NAME</b>	<b>IP SIZ E</b>	<b>GATEWAY</b>	<b>IP RANGE</b>
					192.168.16.1 26
<b>PHÁT TRIỂN BỀN VỮNG</b>	17	PTBV_HO	40	192.168.17.1/ 26	192.168.17.1 - 192.168.17.6 2
<b>GIÁM ĐỐC</b>	18	GIAMDOC_HO	30	192.168.18.1/ 27	192.168.18.1 - 192.168.18.3 0
<b>PHÓ GIÁM ĐỐC</b>	19	PHOGIAMDOC_H O	40	192.168.19.1/ 26	192.168.19.1 - 192.168.19.6 2
<b>KHÁCH HÀNG</b>	200	GUEST	200		

Bảng 3.2a: Bảng thông tin VLAN HO

 Khu vực miền Bắc

<b>PHÒNG BAN</b>	<b>VLAN ID</b>	<b>NAME</b>	<b>IP SIZE</b>	<b>GATEWAY</b>	<b>IP RANGE</b>
<b>TIẾP TÂN</b>	20	TIEPTAN_MB	10	192.168.20.1/28	192.168.20.1 - 192.168.20.14
<b>IT</b>	21	IT_MB	40	192.168.21.1/26	192.168.21.1 - 192.168.21.126

<b>PHÒNG BAN</b>	<b>VLAN ID</b>	<b>NAME</b>	<b>IP SIZE</b>	<b>GATEWAY</b>	<b>IP RANGE</b>
<b>KẾ TOÁN</b>	22	KETOAN_MB	20	192.168.22.1/27	192.168.22.1 - 192.168.22.30
<b>VẬN HÀNH SẢN XUẤT</b>	23	VHSX_MB	30	192.168.23.1/27	192.168.23.1 - 192.168.23.30

Bảng 3.2b: Bảng thông tin VLAN Miền Bắc

### 3.3 Thông tin thiết kế quy hoạch địa chỉ IP Planning

<b>SERVER</b>	<b>IPV4</b>	<b>GATEWAY</b>	<b>NETWORK</b>
<b>DNS, WEB, MAIL, FTP, DHCP. RADIUS</b>	10.10.10.2/28	10.10.10.1	10.10.10.0

Bảng 3.3a Bảng thông tin IP khu vực Server miền Nam

<b>SERVER</b>	<b>IPV4</b>	<b>GATEWAY</b>	<b>NETWORK</b>
<b>FTP, WEB, MAIL, DHCP. RADIUS</b>	10.10.11.2/28	10.10.11.1	10.10.11.0

Bảng 3.3b Bảng thông tin IP khu vực Server miền Bắc

<b>STT</b>	<b>Devices</b>	<b>Interface</b>	<b>Ipv4</b>	<b>Network</b>
<b>1</b>	Dis1_HO	Port-channel 1	172.16.0.21/30	172.16.0.20

<b>STT</b>	<b>Devices</b>	<b>Interface</b>	<b>Ipv4</b>	<b>Network</b>
		Port-channel 2	172.16.0.33/30	172.16.0.32
<b>2</b>	Dis2_HO	Port-channel 1	172.16.0.29/30	172.16.0.28
		Port-channel 2	172.16.0.25/30	172.16.0.24
		Port-channel 1	172.16.0.22/30	172.16.0.20
<b>3</b>	Core1_HO	Port-channel 2	172.16.0.26/30	172.16.0.24
		Port-channel 3	172.16.0.17/30	172.16.0.16
		e1/2	172.16.0.5/30	172.16.0.4
		Port-channel 1	172.16.0.30/30	172.16.0.28
<b>4</b>	Core2_HO	Port-channel 2	172.16.0.34/30	172.16.0.32
		Port-channel 3	172.16.0.18/30	172.16.0.16
		e1/2	172.16.0.9/30	172.16.0.8
		Port-channel 1	172.16.0.30/30	172.16.0.28
<b>5</b>	Firewall_HO	e0/0	172.16.0.6/30	172.16.0.4
		e0/1	172.16.0.10	172.16.0.8
		e0/2	10.10.10.1	10.10.10.0
		e0/3	172.16.0.13	172.16.0.12
<b>6</b>	R1	e0/0	172.16.0.14	172.16.0.12
		S6/0	209.168.100.1	209.168.100.0
<b>7</b>	ISP	S6/0	209.168.100.2	209.168.100.0

<b>STT</b>	<b>Devices</b>	<b>Interface</b>	<b>Ipv4</b>	<b>Network</b>
		S6/1	209.168.200.2	209.168.200.0
		E0/0	DHCP	Internet
<b>8</b>	R2	E0/0	172.16.0.38	172.16.0.36
		S1/0	209.168.200.1	209.168.200.0
<b>9</b>	Firewall_Branch	E0/0	172.16.0.37	172.16.0.36
		E0/1	172.16.0.42	172.16.0.40
		E0/2	10.10.11.1	10.10.11.0
<b>10</b>	Core_MB	E0/0	172.16.0.41	172.16.0.40
		Port-channel1	172.16.0.46	172.16.0.44
		Port-channel2	172.16.0.50	172.16.0.48
<b>11</b>	Dis1_MB	Port-channel1	172.16.0.45	172.16.0.44
<b>12</b>	Dis2_MB	Port-channel1	172.16.0.49	172.16.0.48

Bảng 3.3c Bảng thông tin IP

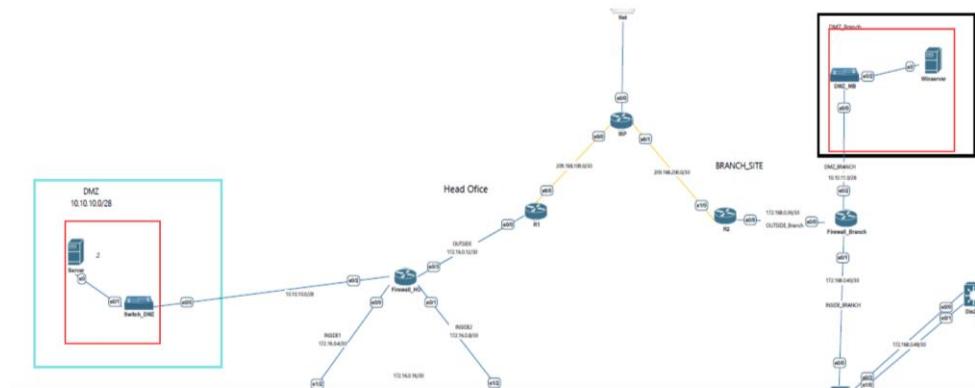
## CHƯƠNG 4. QUẢN TRỊ HỆ THỐNG MẠNG

### 4.1 Cấu hình Server

#### 4.1.1 DNS Server

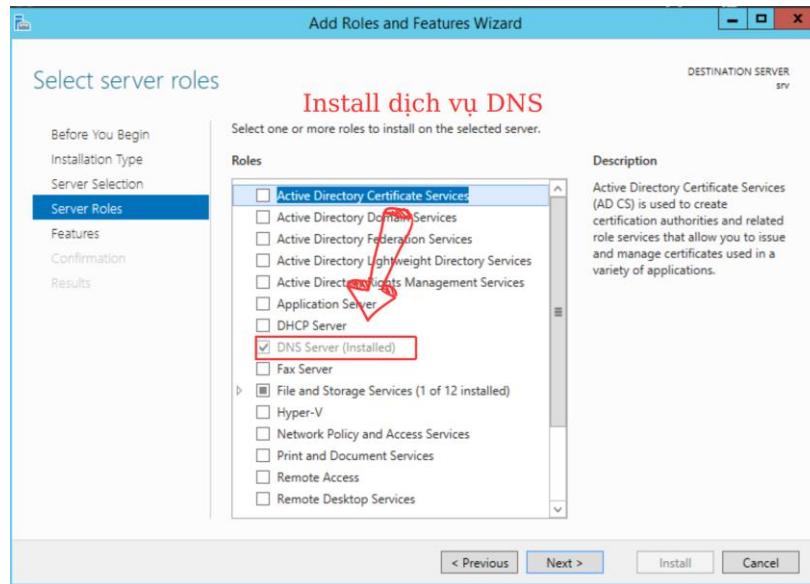
DNS - Domain Name System là một hệ thống phân giải tên miền bao gồm cả TCP/IP. DNS là then chốt trong việc duyệt web, mail,... Mỗi thiết bị kết nối với Internet có một địa chỉ IP duy nhất để xác định trong hệ thống mạng, tuy nhiên nó rất khó nhớ. Vì vậy, DNS sẽ giúp phân giải các địa chỉ IP trên thành những tên miền dễ nhớ (chẳng hạn như google.com).

Trong đồ án này, hệ thống mạng của chúng ta sẽ có hai site bao gồm site chính là head office và chi nhánh ở miền Bắc, cho nên chúng ta sẽ sử dụng 2 server và cấu hình các dịch vụ trên 2 server này.

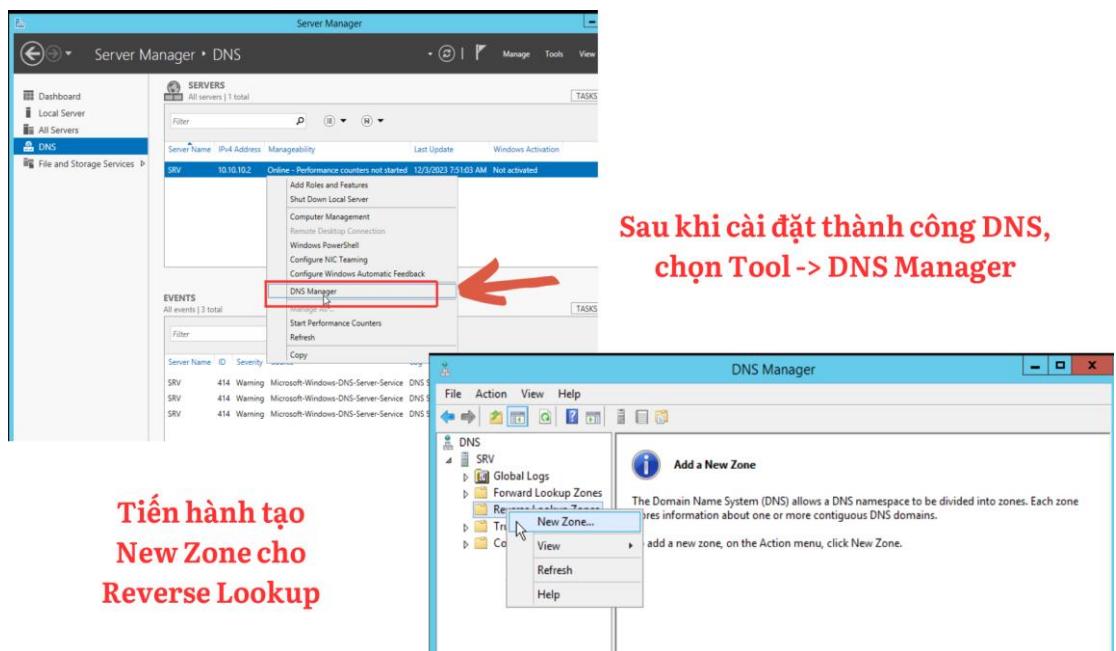


Hình 4.1.1a: Hai server ở 2 site

Một số bước để cấu hình DNS



Hình 4.1.1b: Install DNS Server ở mục add Role and Feature

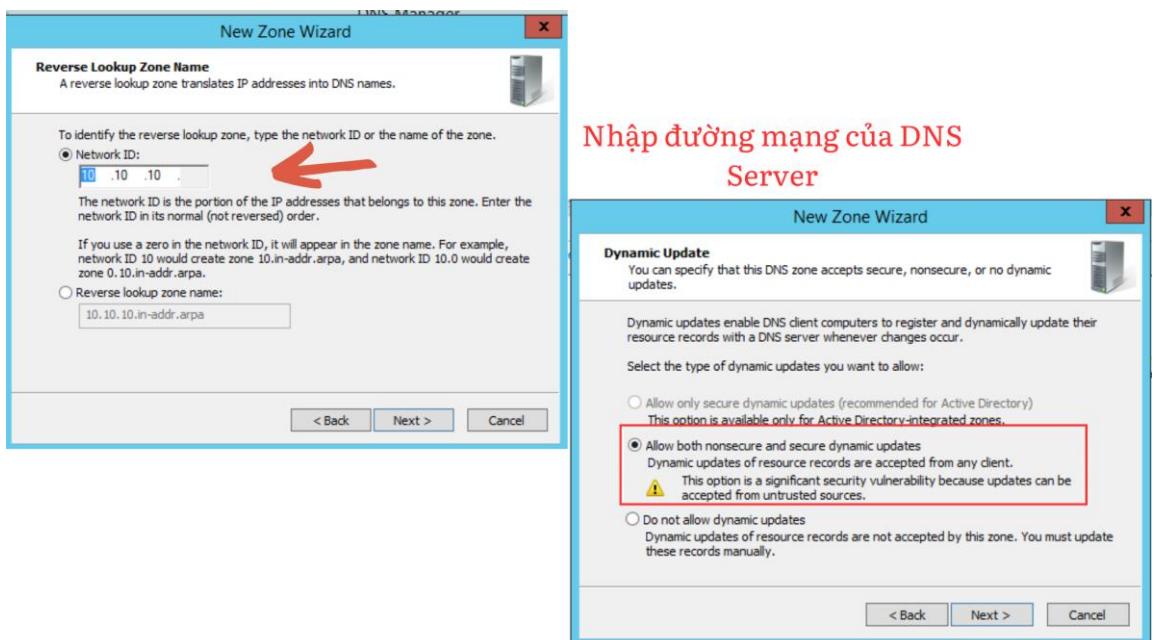


Hình 4.1.1c: Sau khi đã cài đặt thành công DNS Server, tiến hành vào DNS Manager để cấu hình

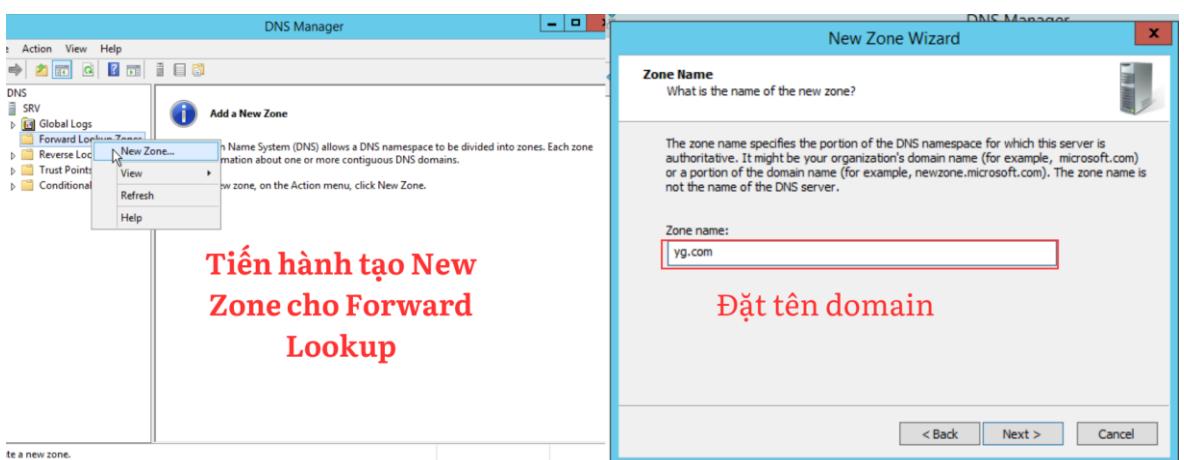
Chúng ta sẽ cần chú ý đến hai mục là Forward Lookup Zones và Reverse Lookup Zone. Đây là hai vùng có trách nhiệm giúp cho máy chủ DNS chuyển đổi giữa địa chỉ IP và tên miền và ngược lại.

Đối với Forward Lookup Zone: được sử dụng để chuyển đổi tên miền thành địa chỉ IP. Khi một máy client truy cập một tên miền bất kỳ, máy chủ DNS sẽ tra cứu trong vùng này để xác định IP tương ứng với tên miền đó.

Đối với Reverse Lookup Zone: được sử dụng để chuyển đổi ngược lại từ IP về tên miền. Khi một máy client nhập địa chỉ IP trên thanh tìm kiếm, máy chủ DNS sẽ tra cứu trong Reverse Lookup Zone để xác định tên miền tương ứng.



Hình 4.1.1d: Nhập đường mạng của DNS Server



Hình 4.1.1e: Tương tự Tạo Zone mới ở vùng Forward

Ta sẽ có một số bản ghi cơ bản mà chúng ta sẽ gặp sau khi tạo zone name

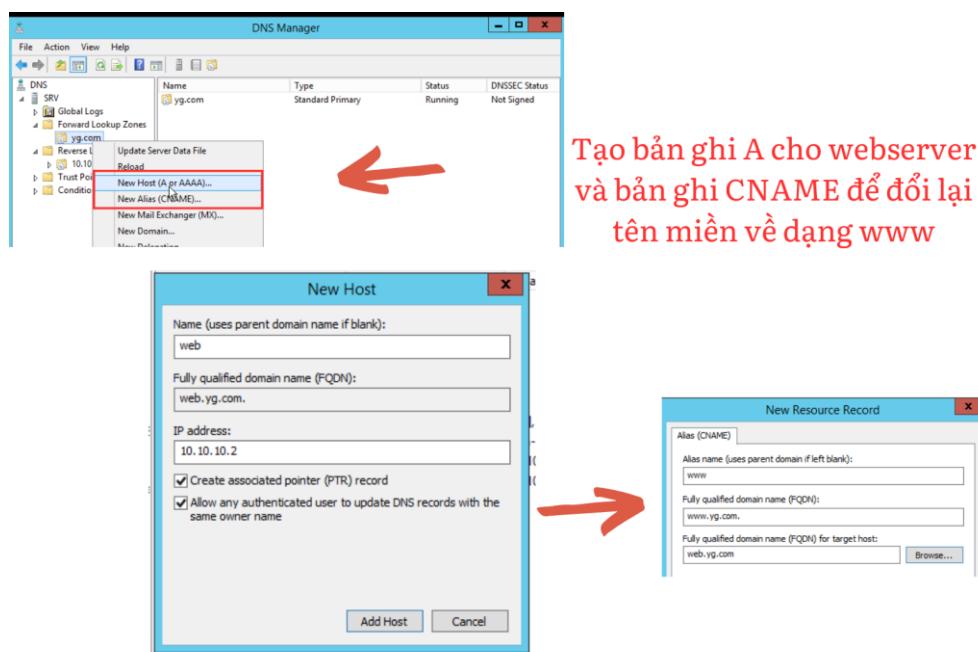
- Bản ghi A và AAAA: đây là hai bản ghi dùng để ánh xạ một tên miền với A là địa chỉ IPv4 và AAAA là địa chỉ IPv6

Ví dụ: ta có một domain web.yg.com với bản ghi A: 10.10.10.3 và AAAA: 2001:db8:badc:A::3

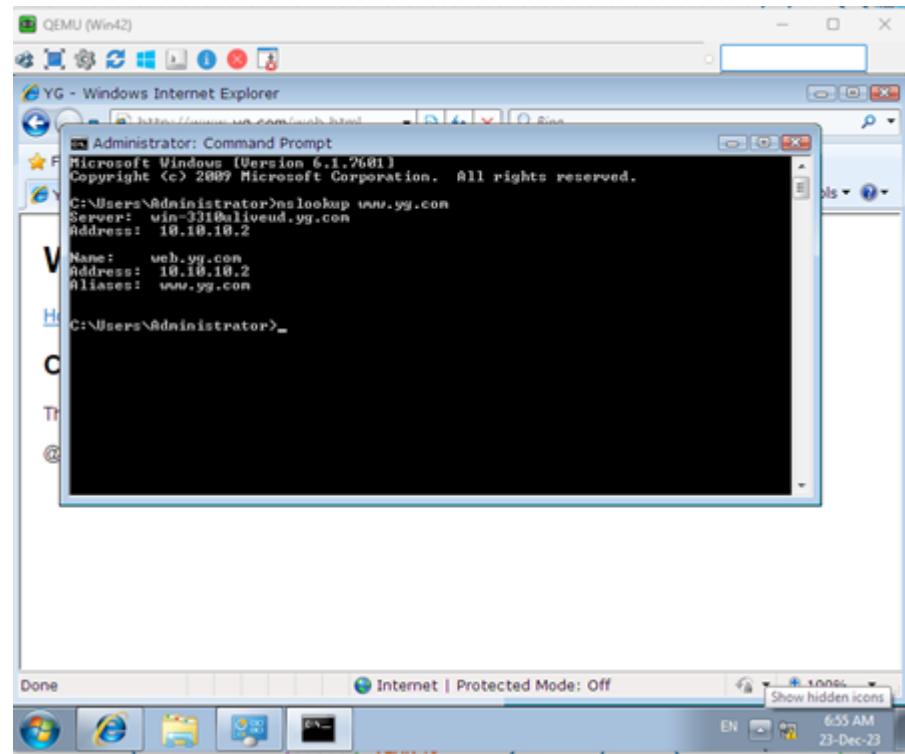
- Bản ghi CNAME: đây là bản ghi được sử dụng để tạo ra một bản định danh chính thức cho một tên miền

Ví dụ: Ta có web.yg.com là tên miền mặc định của trang web và chúng ta muốn đổi cấu trúc của tên miền thành: www.yg.com thì chúng ta sẽ sử dụng bản ghi CNAME để thực hiện điều đó.

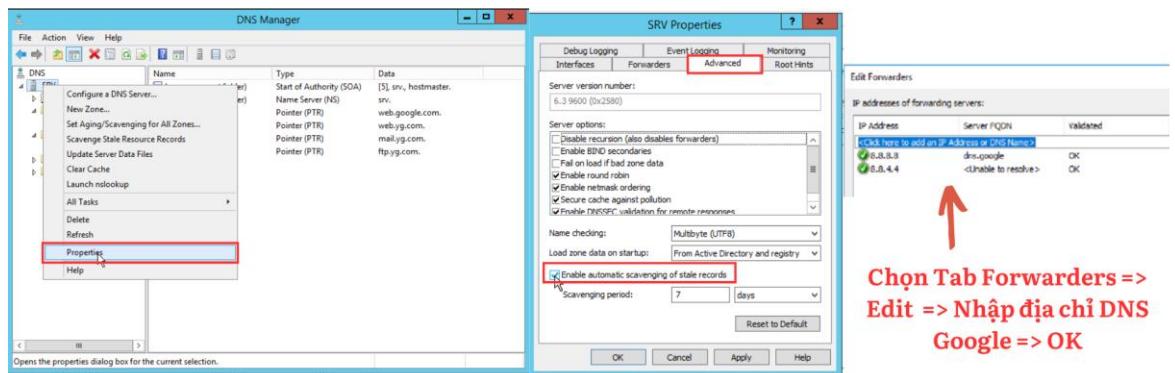
- Bản ghi MX(Mail Exchange Record): Đây là bản ghi dùng để xác định máy chủ email chấp nhận thư điện tử cho một tên miền cụ thể.



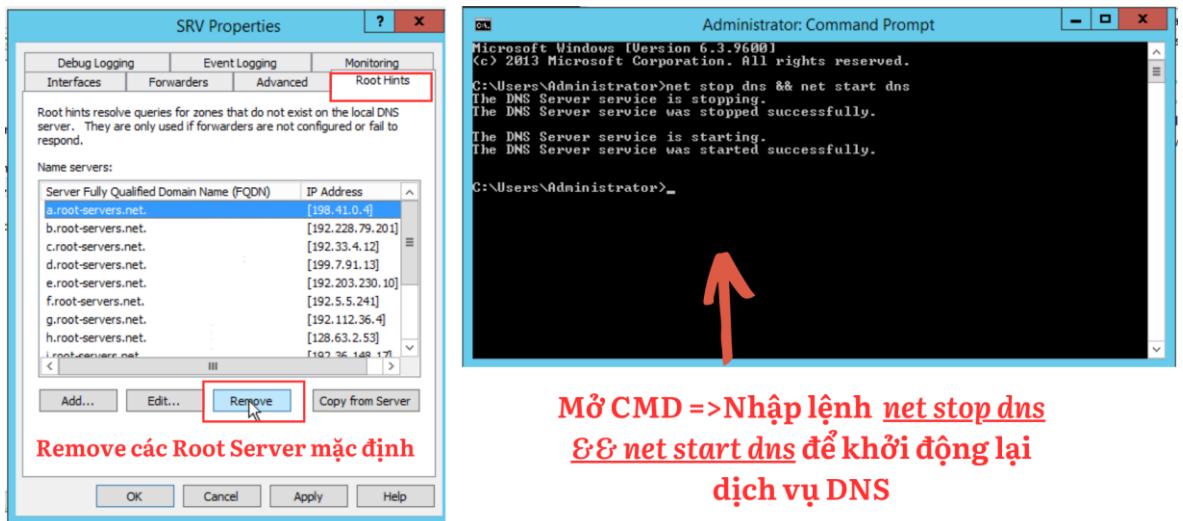
Hình 4.1.1f: Tạo bản ghi A và CNAME cho domain của Web Server



Hình 4.1.1g: Kiểm tra DNS



Hình 4.1.1h: Để thực hiện phân giải tên miền các địa chỉ ở bên ngoài mạng LAN ta sẽ cài đặt DNS recursive



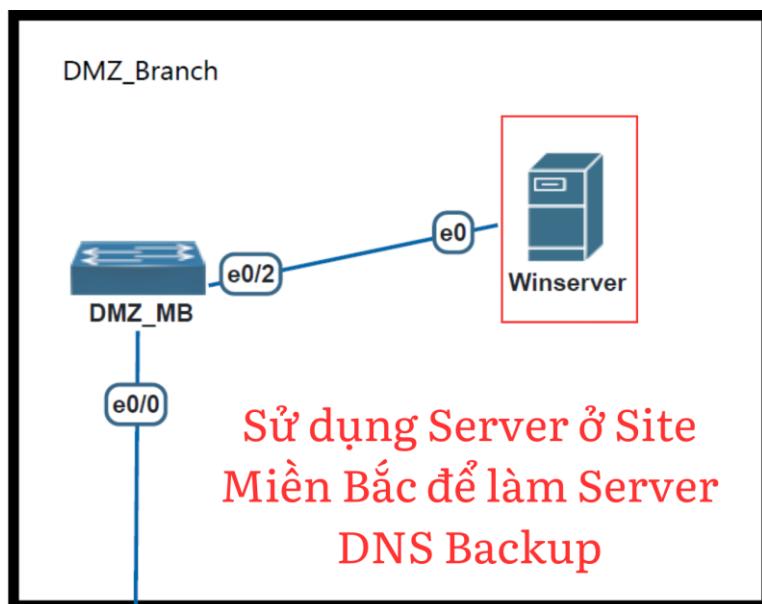
Mở CMD => Nhập lệnh net stop dns  
&& net start dns để khởi động lại  
dịch vụ DNS

Hình 4.1.1i: Mở CMD -> Nhập lệnh **net stop dns && net start dns** để khởi động lại dịch vụ DNS

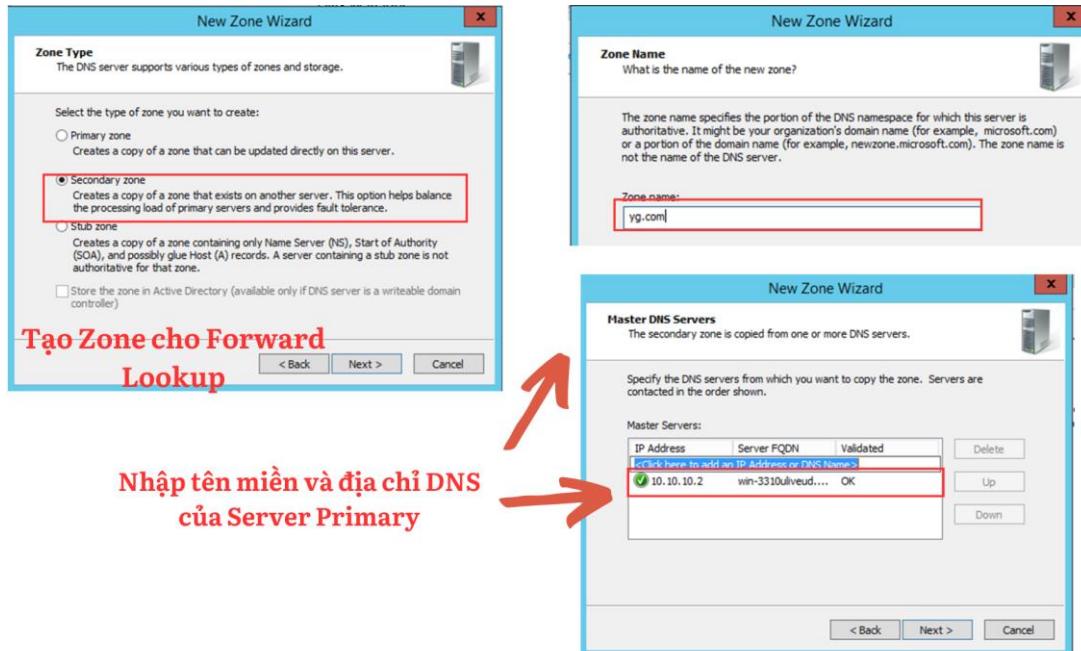
#### 4.1.2 Alternative DNS

Alternative DNS hay còn gọi là DNS thay thế, là một thuật ngữ mà người ta sử dụng để ám chỉ các dịch vụ DNS khác nhau mà người dùng có thể sử dụng thay vì sử dụng DNS mặc định được cấu hình bởi nhà cung cấp dịch vụ Internet (ISP).

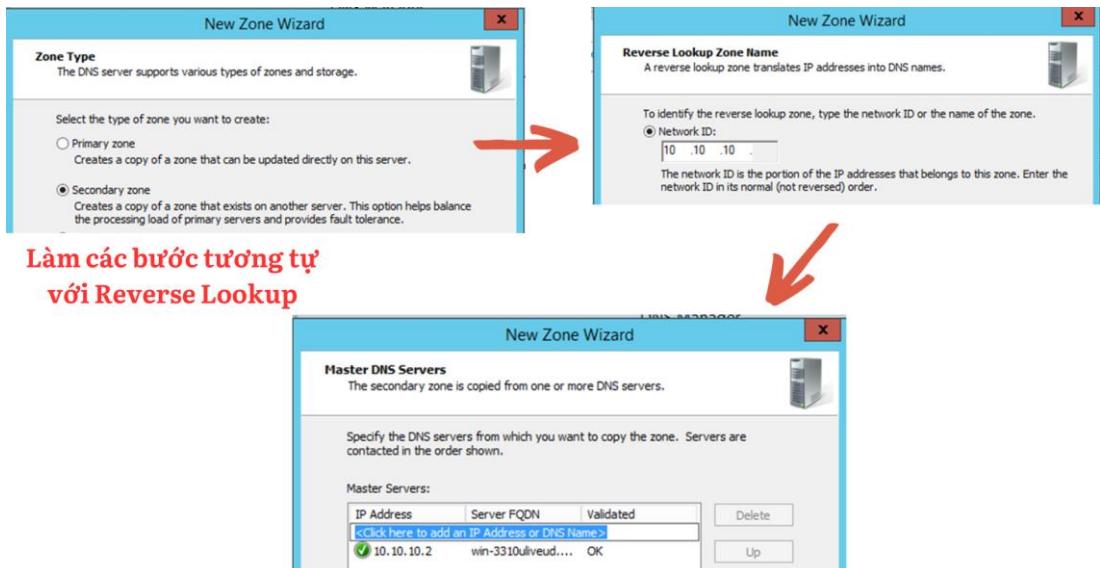
Các bước cấu hình DNS Alternative



Hình 4.1.2a: Dùng server miền Bắc để làm DNS Alternative

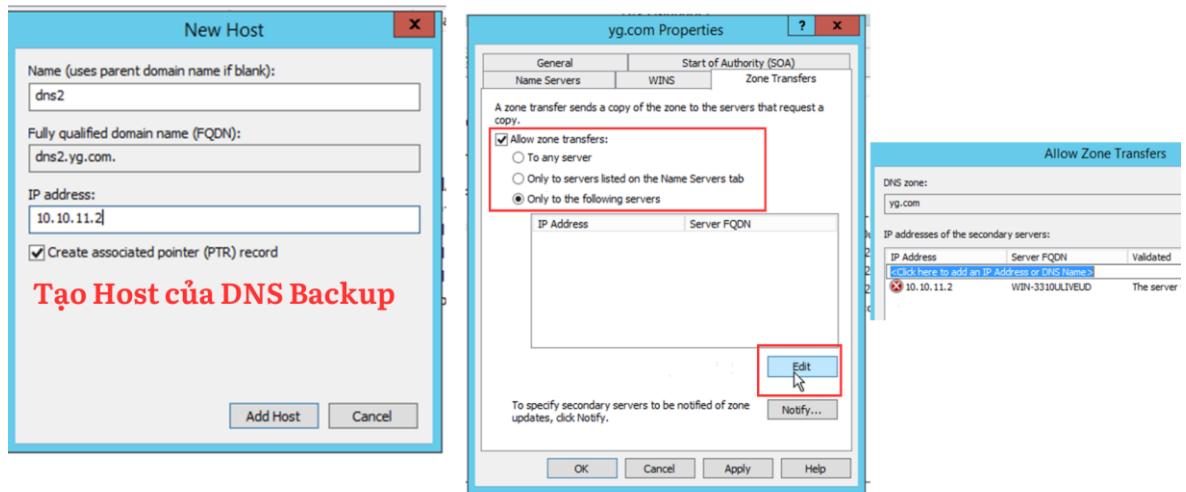


Hình 4.1.2b: Tạo Zone cho Forward Lookup Zone



Hình 4.1.2c: Tạo Zone cho Reverse Lookup Zone  
Cấu hình DNS trên DNS primary

### Vào DNS 1 => Properties

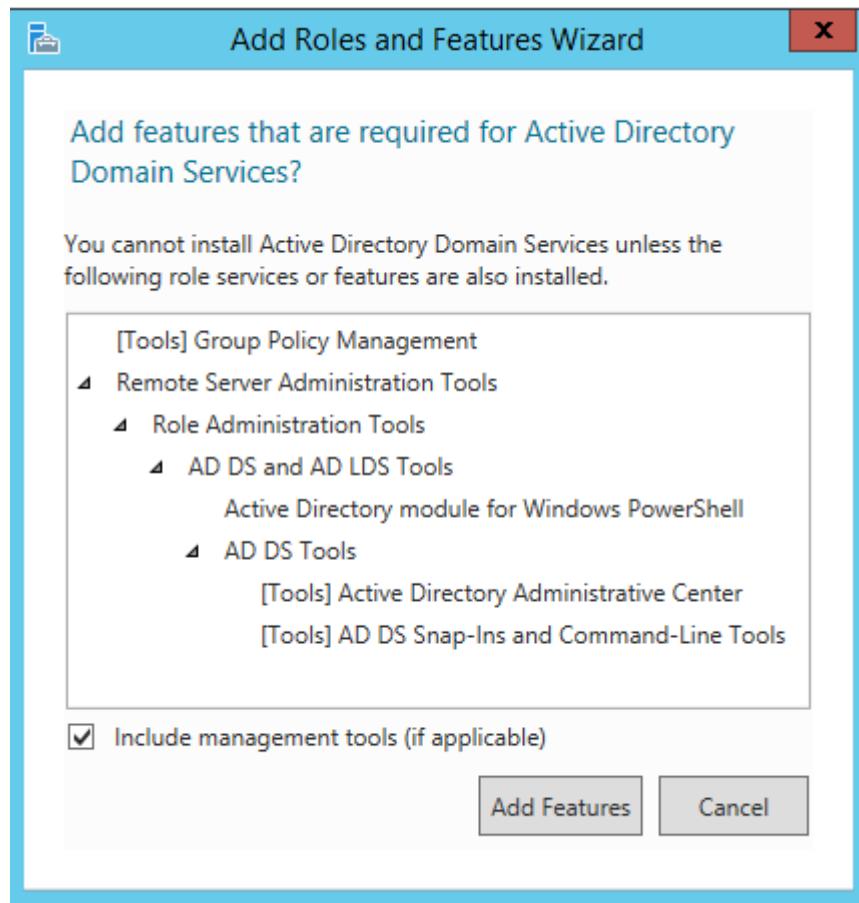


### Thực hiện tương tự với Reverse Lookup và trên Server Backup

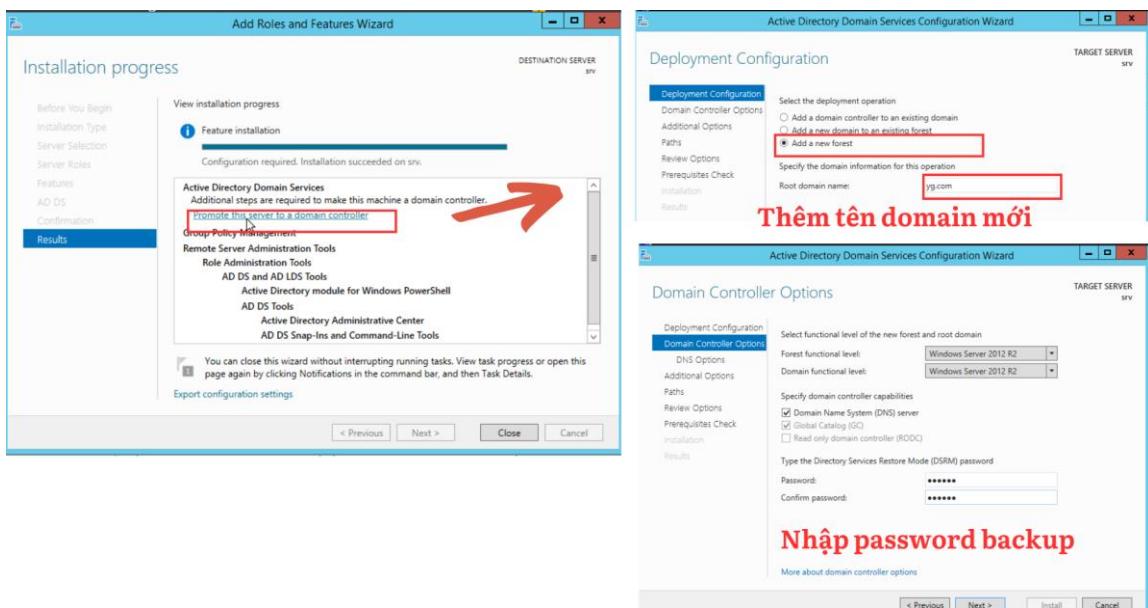
Hình 4.1.2d: Cấu hình backup trên cả 2 server DNS

#### 4.1.3 Active Directory Domain Service

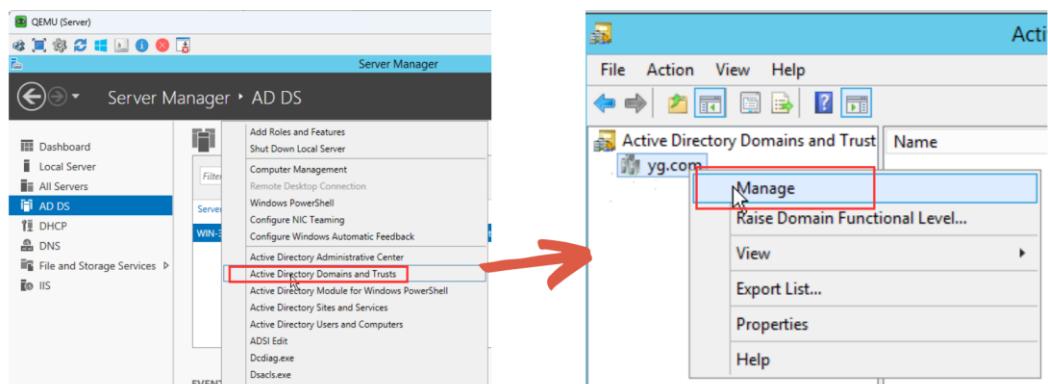
Active Directory Domain Services (AD DS) là dịch vụ lưu trữ thông tin thư mục và xử lý tương tác của người dùng với domain. AD DS xác minh quyền truy cập khi người dùng đăng nhập vào thiết bị hoặc cố gắng kết nối với máy chủ qua mạng. AD DS kiểm soát người dùng nào có quyền truy cập vào từng tài nguyên, cũng như chính sách nhóm.



Hình 4.1.3a: Install AD

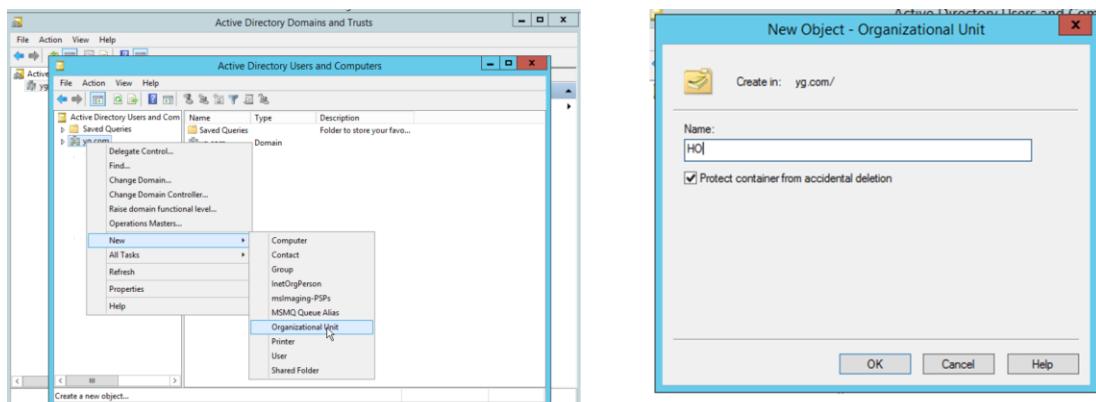


Hình 4.1.3b: Thêm domain và password backup là 2023@yg



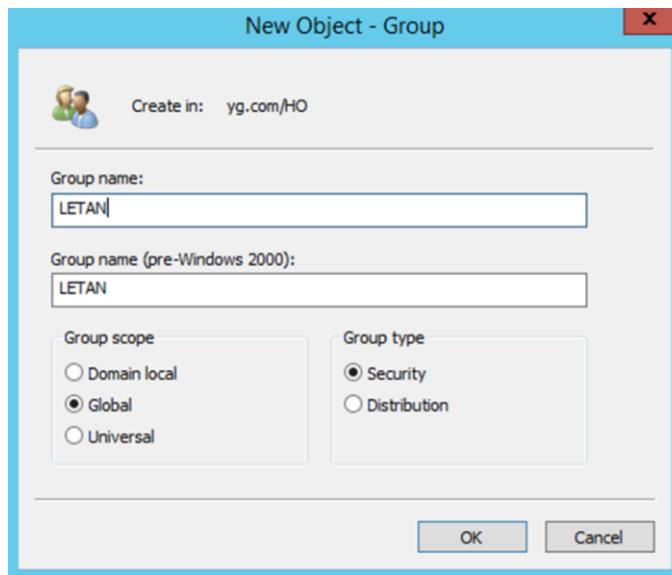
Vào mục ADD and Trusts và tiến hành  
quản lý AD

Hình 4.1.3c: Quản lý AD



Tạo hai OU đại diện cho site Head Office  
và site Branch

Hình 4.1.3d: Tạo OU đại diện cho 2 site



Sau khi đã tạo các OU,  
tiếp tục tạo các Group  
cho các phòng ban

Hình 4.1.3e: Tạo Group cho các phòng ban

Active Directory Users and Computers

yg.com

New Object - User

First name: Kim Initials: [ ]

Last name: Tran Dang Thien Full name: Kim Tran Dang Thien

User logon name: kim.tdt @yg.com

User logon name (pre-Windows 2000): YG\_ ktm.tdt

New Object - User

First name: Duyen Initials: [ ]

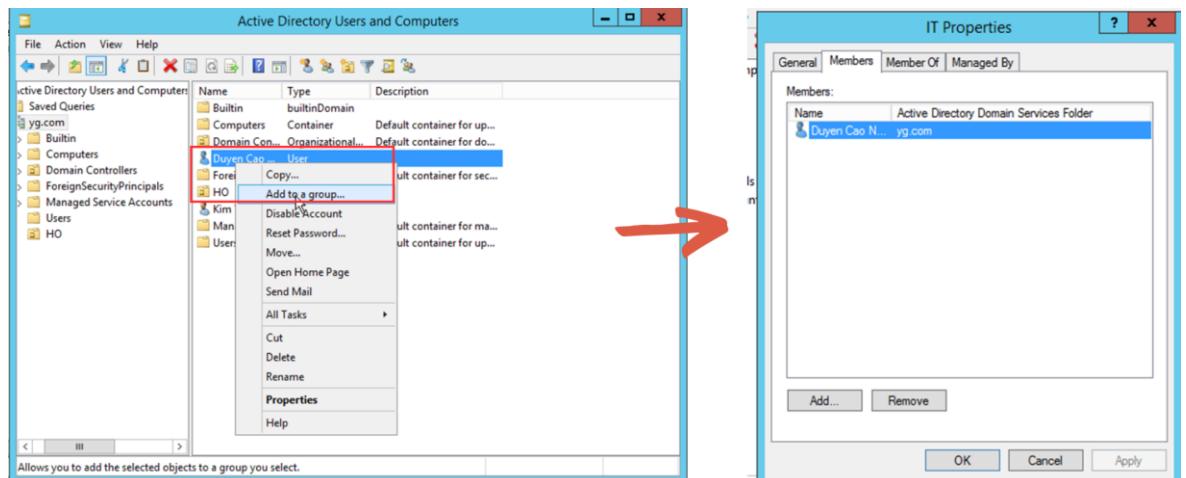
Last name: Cao Nguyen Ky Full name: Duyen Cao Nguyen Ky

User logon name: duyen.cnk @yg.com

User logon name (pre-Windows 2000): YG\_ duyen.cnk

Hình 4.1.3f: Tạo Users

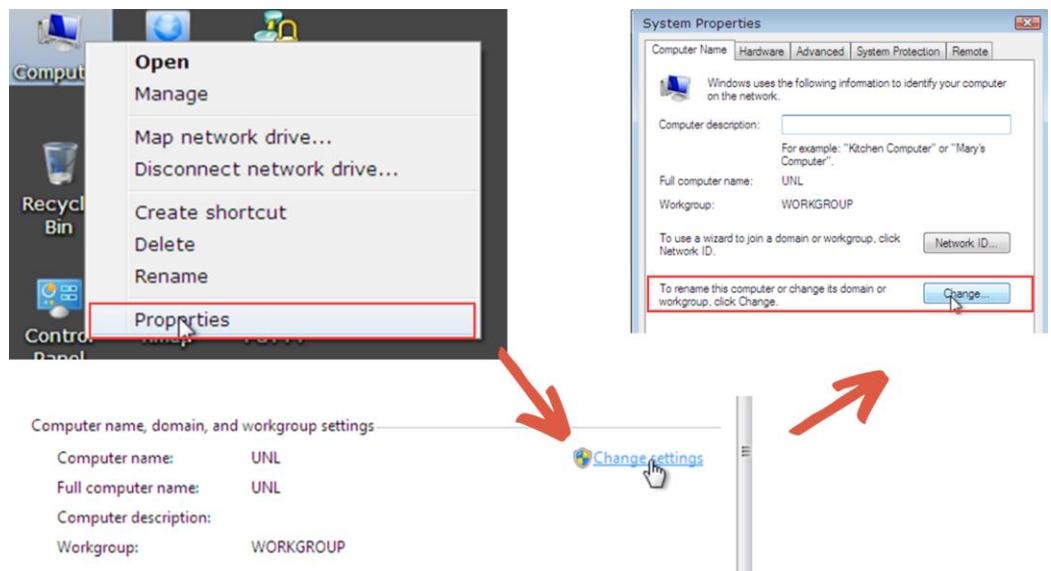
Sau khi đã tạo xong các User, chúng ta sẽ thêm các user đó vào các phòng ban phù hợp. Ở đây, em sẽ thêm hai user vừa tạo vào 2 nhóm IT và Kế toán.



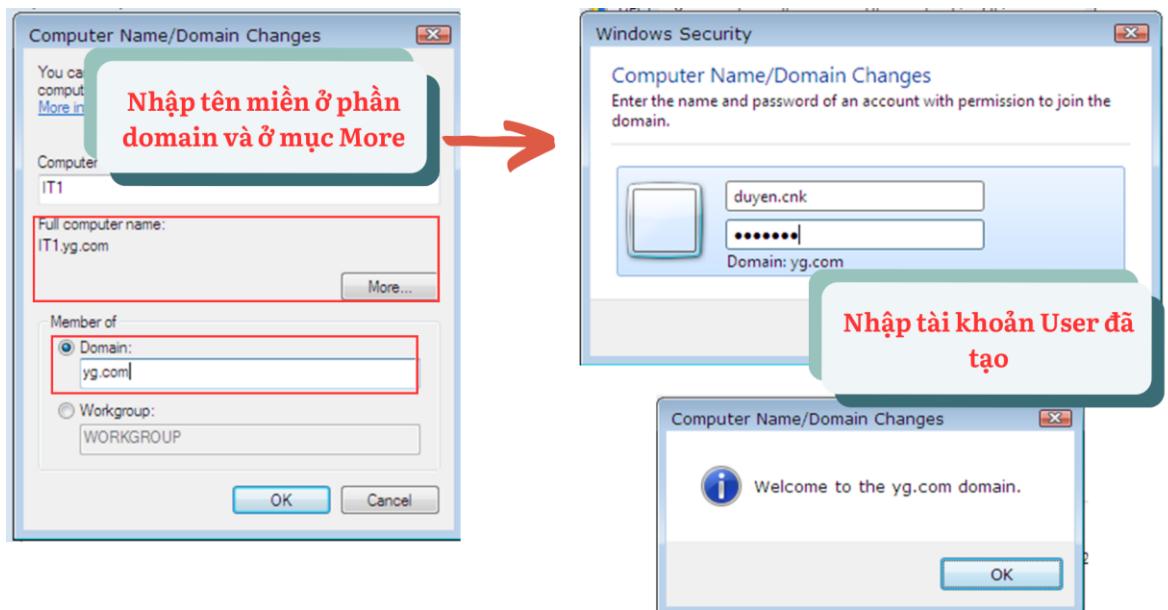
Hình 4.1.3g: Thêm các user vào các nhóm phòng ban

Sau khi đã tạo xong tất cả các nhóm phòng ban và tài khoản người dùng, chúng ta sẽ sử dụng các máy client ở các tầng để tiến hành join domain.

Giả sử em sẽ sử dụng máy client ở phòng IT để join vào domain:

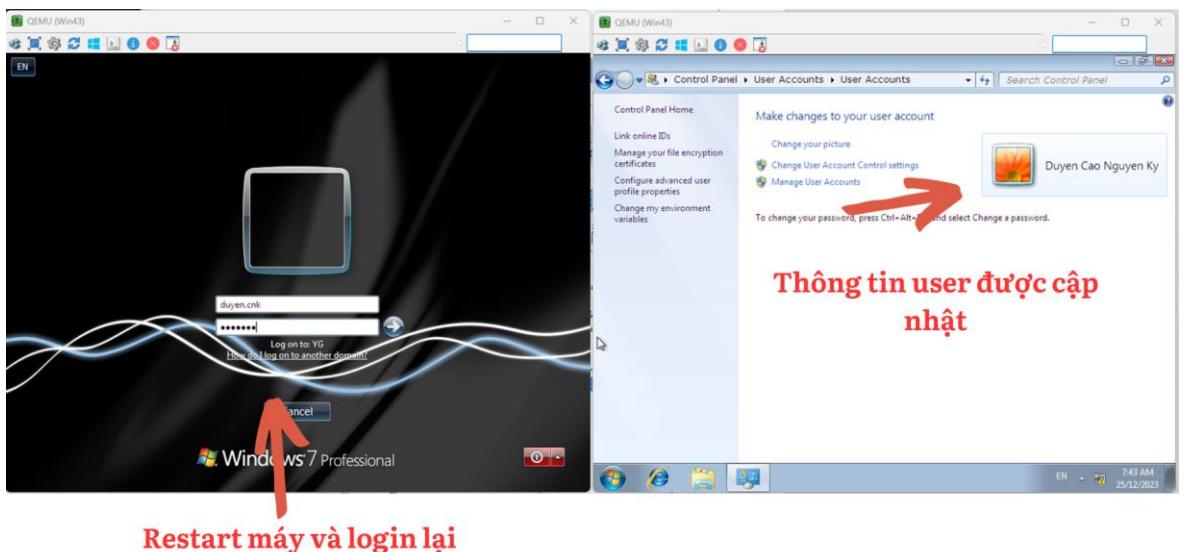


Hình 4.1.3h: Sử dụng máy client để join domain



Hình 4.1.3i: Các bước join domain

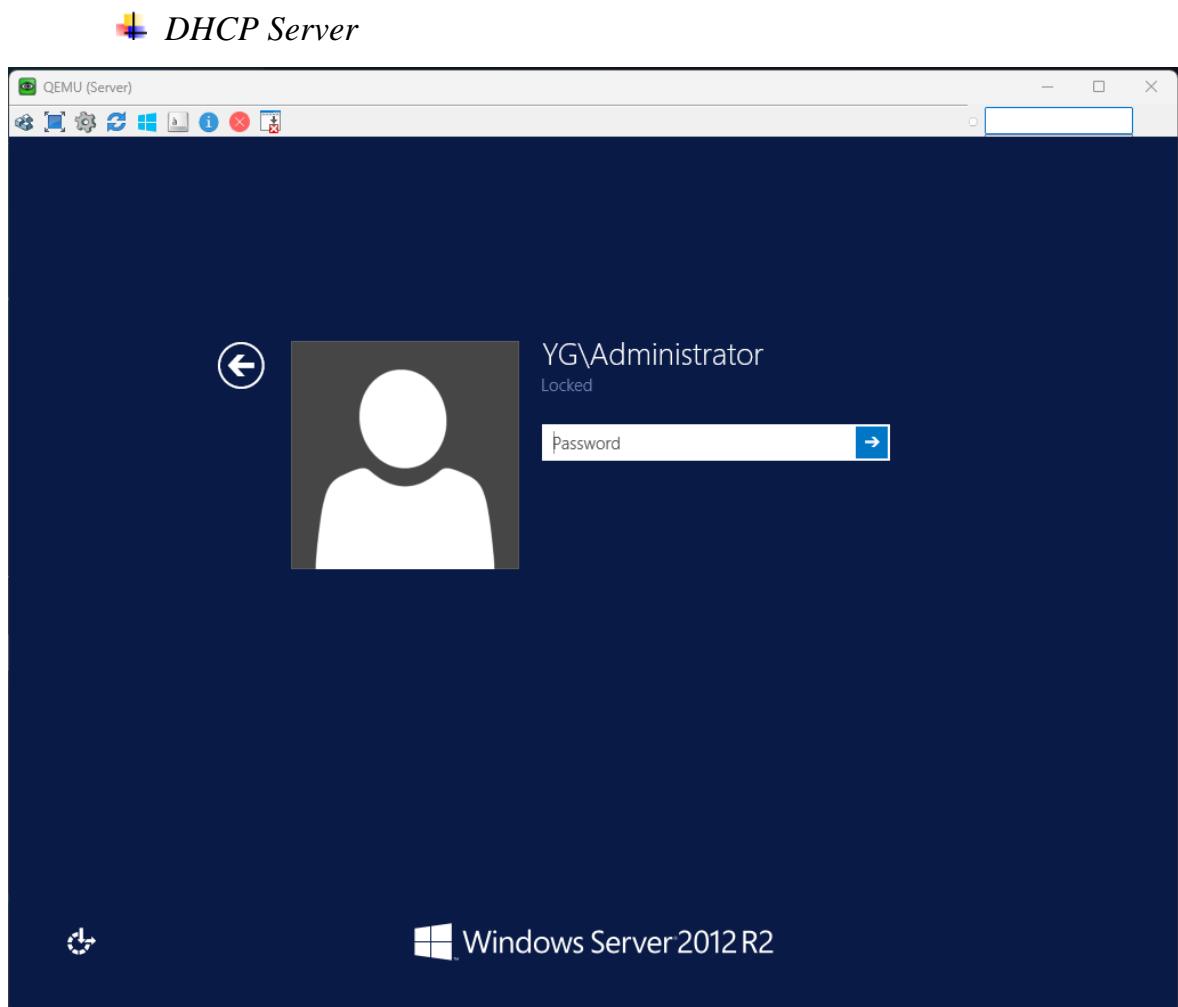
Sau khi đã join domain thành công, thiết bị sẽ tự động restart và yêu cầu người dùng đăng nhập lại .



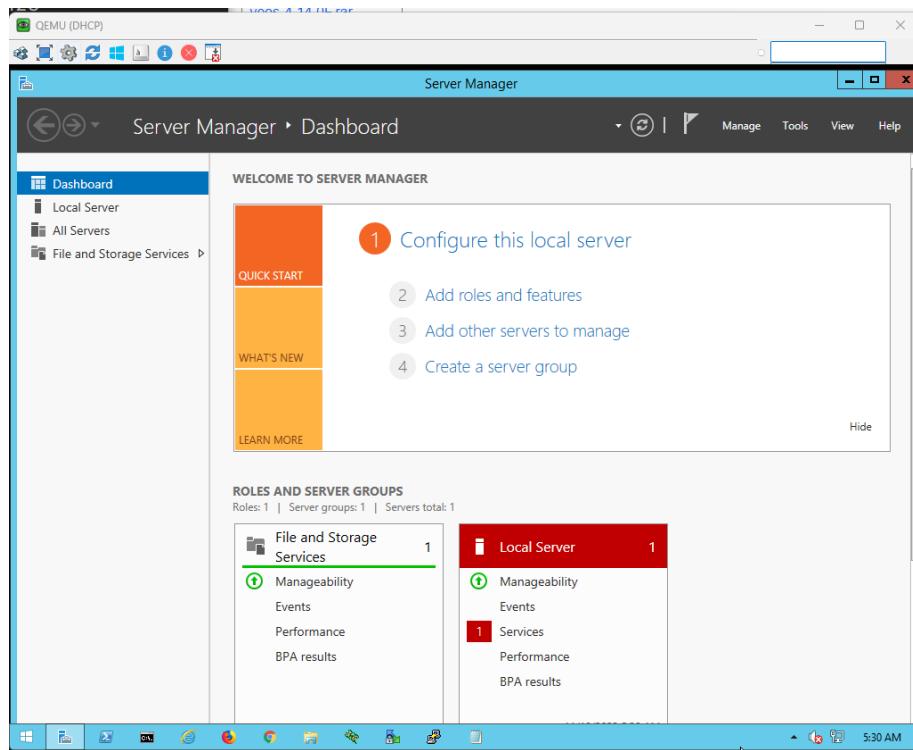
Hình 4.1.3j: Restart máy và thực hiện login lại

#### 4.1.4 DHCP Server

Dựa vào bảng IP VLAN đã chia bằng phương thức VLSM, chúng ta sẽ tiến hành cấu hình và tạo các VLAN trên máy chủ DHCP và sử dụng ip helper-address ở Switch Distribute để lấy IP từ DHCP Server.

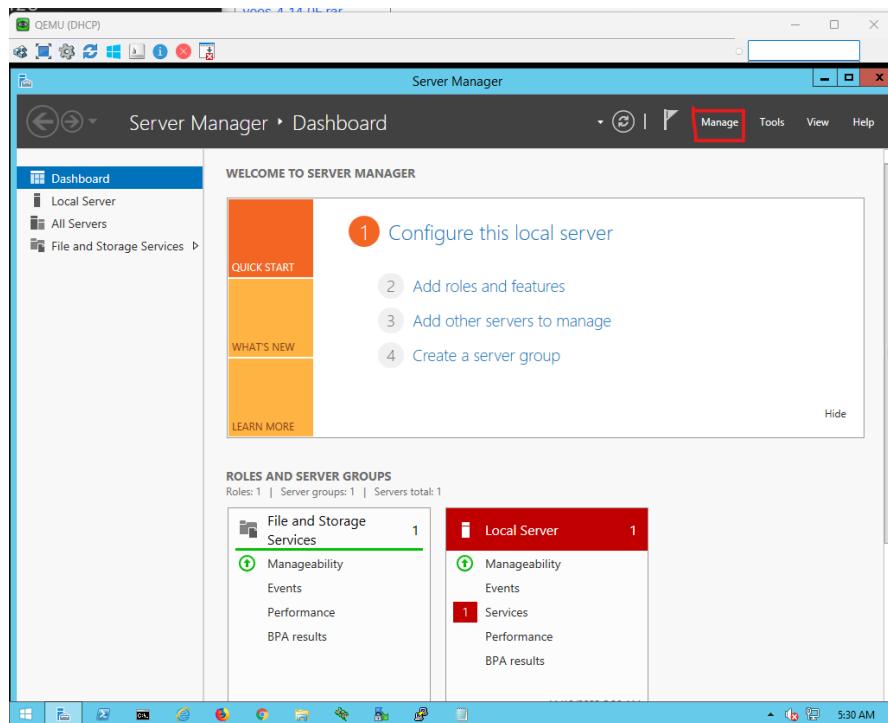


Hình 4.1.4a: Sử dụng tên đăng nhập và mật khẩu: 2023@yg để đăng nhập vào server.

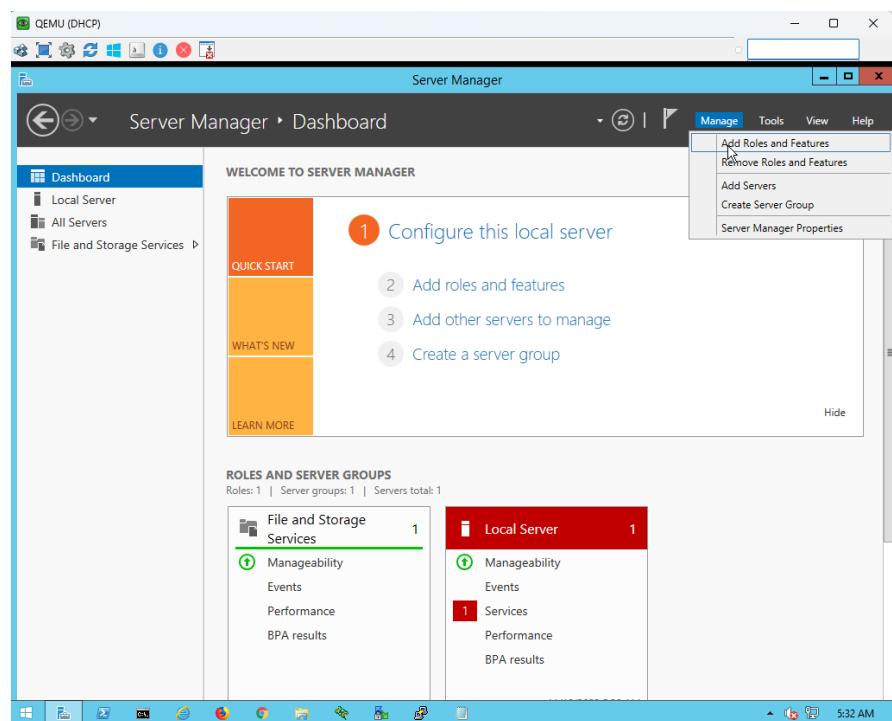


Hình 4.1.4b: Giao diện màn hình quản lý của Server

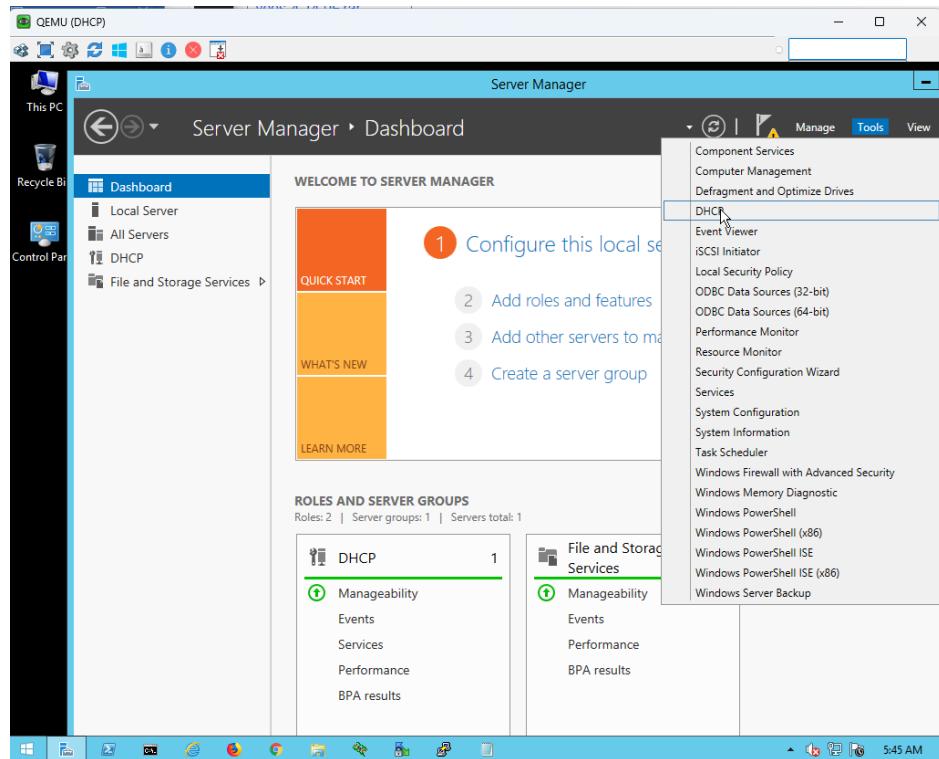
#### Các bước setup DHCP:



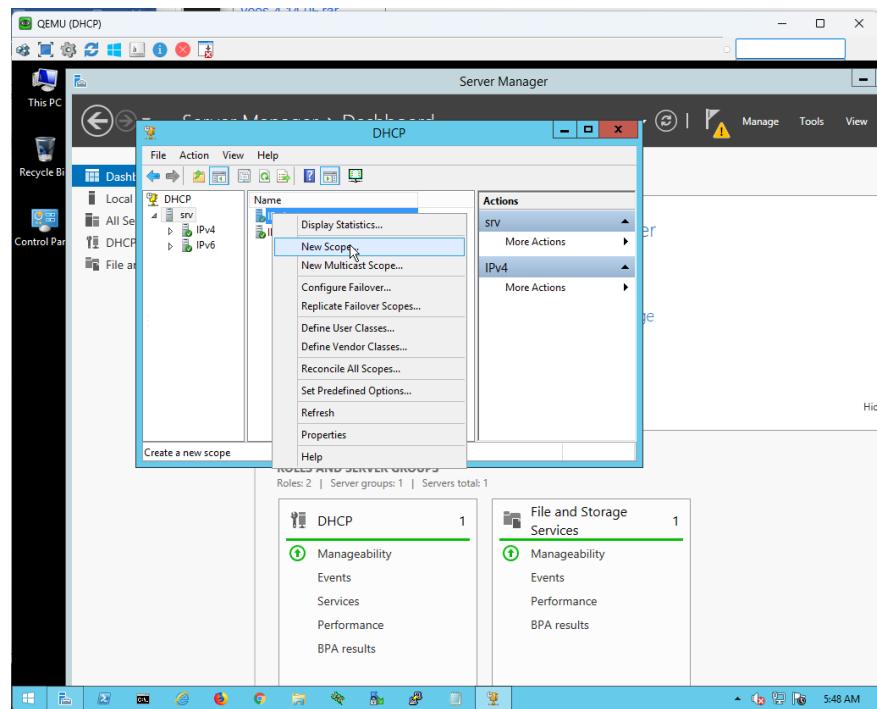
Hình 4.1.4c: Chọn Tab Manage



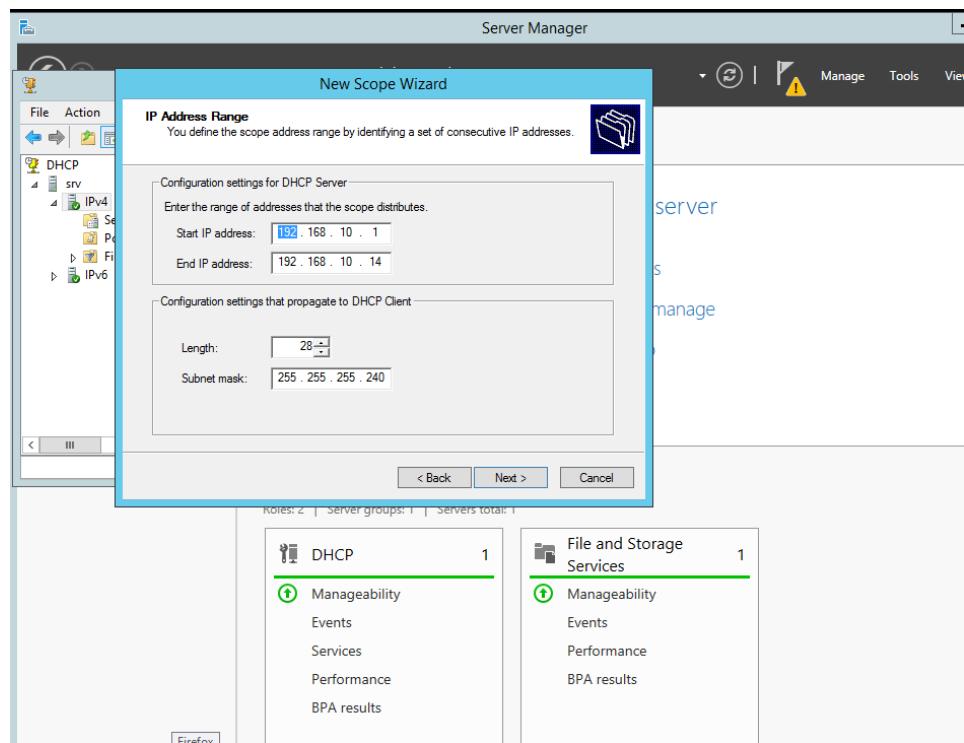
Hình 4.1.4d: Chọn Add Role and Feature



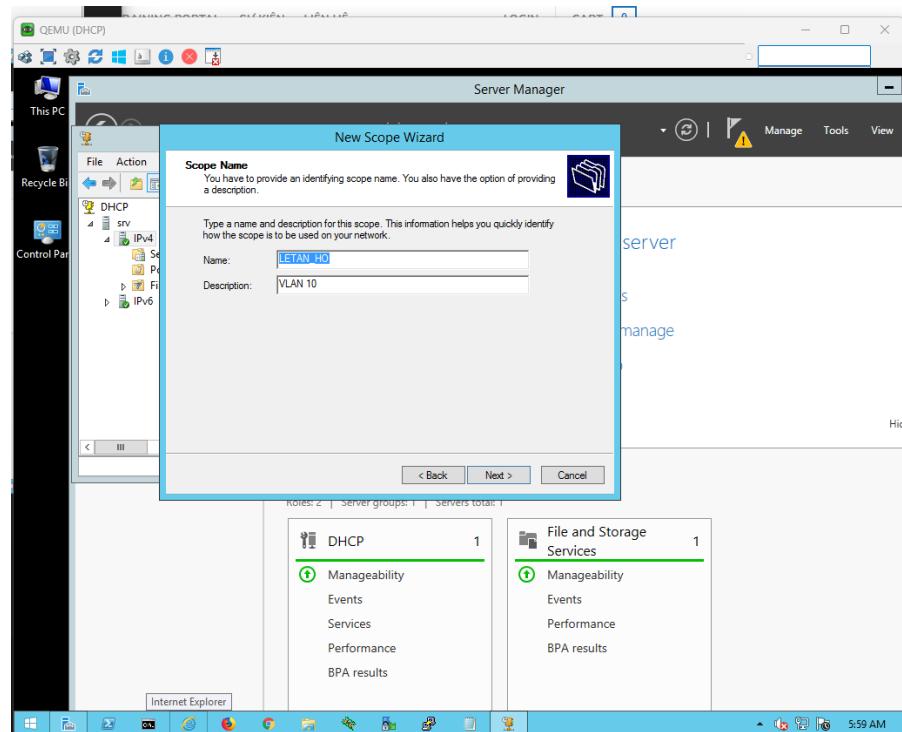
Hình 4.1.4e: Sau khi đã cài đặt, DHCP sẽ hiển thị ở tab Tool



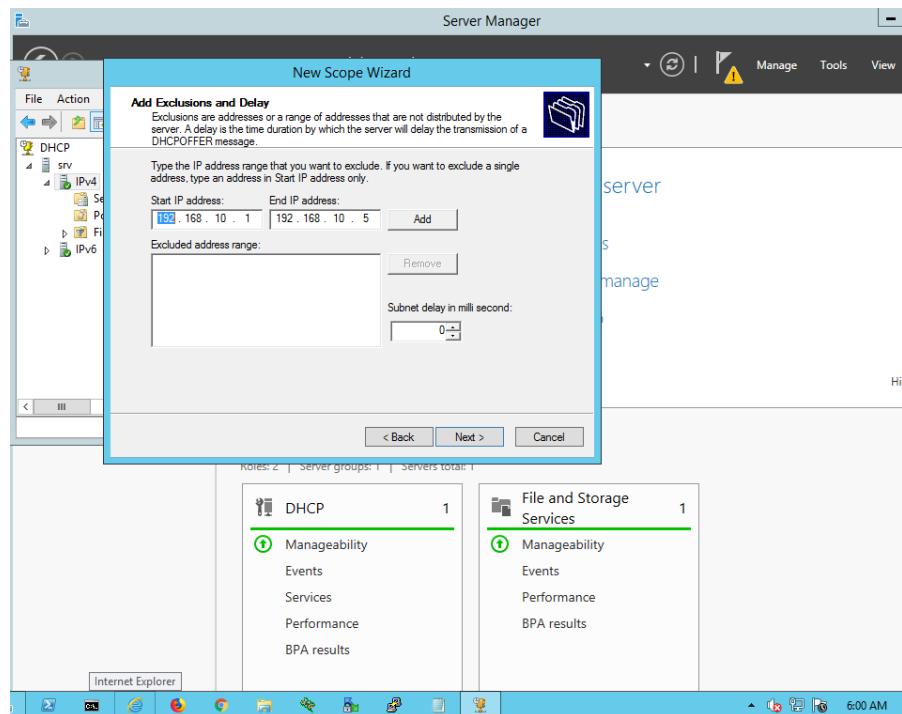
Hình 4.1.4f: Chọn New Scope để tạo VLAN



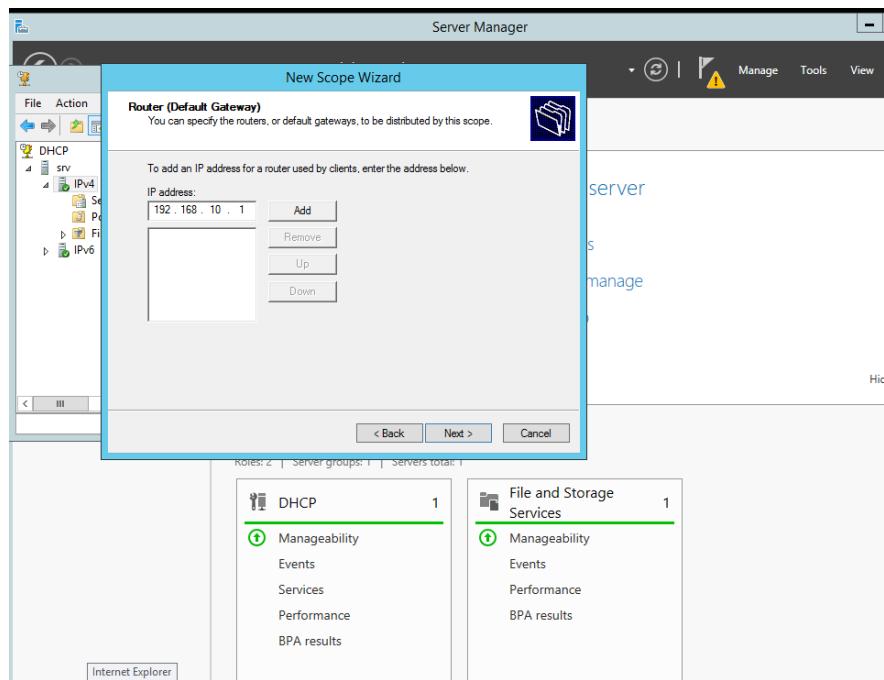
Hình 4.1.4g: Tạo pool VLAN



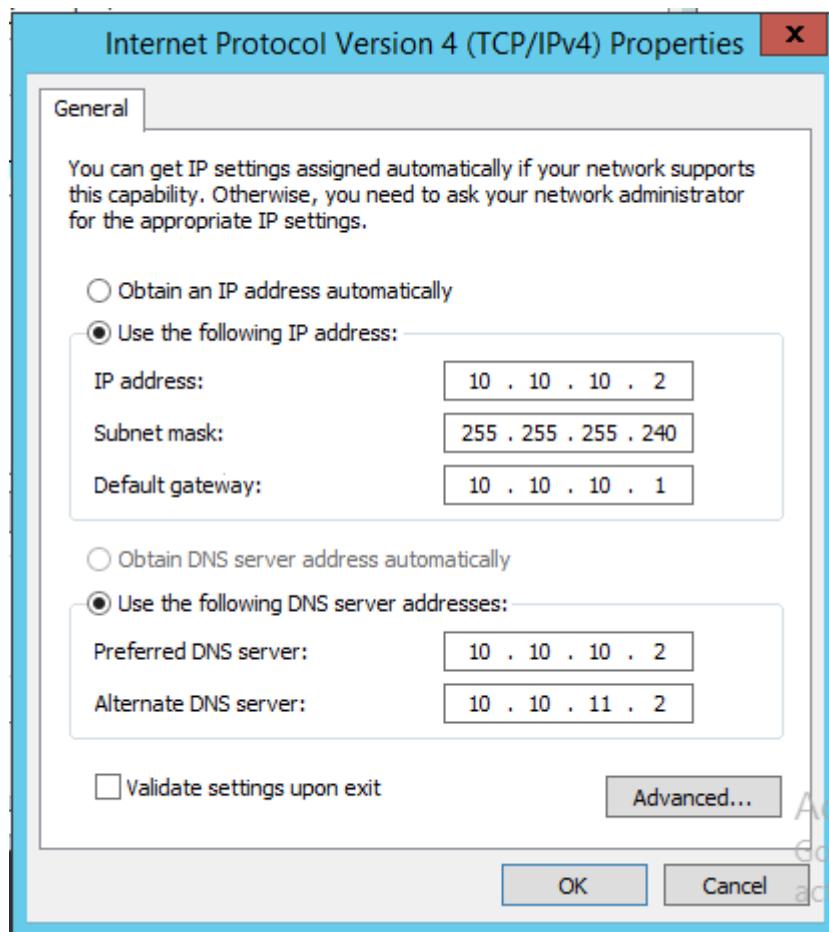
Hình 4.1.4h: Đặt tên VLAN



Hình 4.1.4j: Nhập địa chỉ IP không cấp phát



Hình 4.1.4k: Nhập Default Gateway của VLAN



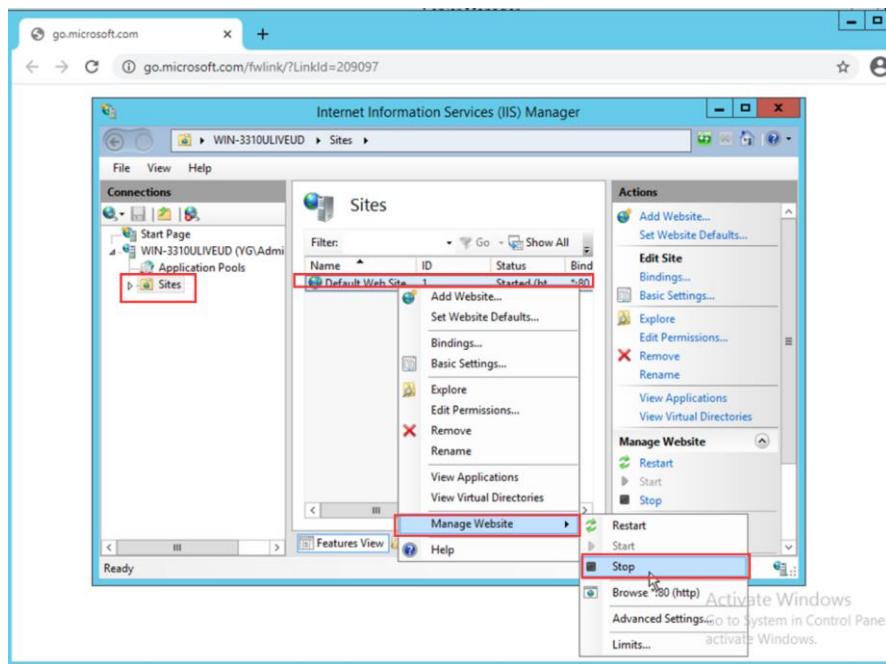
Hình 4.1.4l: Cấu hình IP tĩnh cho Server

Tạo các pool VLAN còn lại ở hai site tương tự các bước trên.

#### **4.1.5 Web Server**

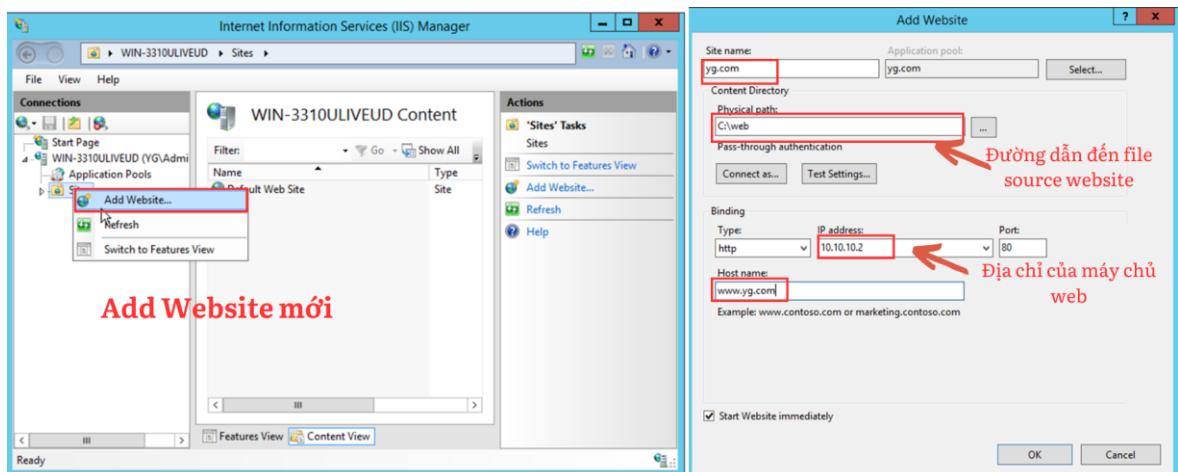
Máy chủ Web là thành phần giúp lưu trữ và xử lý các yêu cầu của người dùng Internet. Tương tự các bước cấu hình các máy chủ khác, chúng ta sẽ cài đặt roles IIS (Internet Information Services).

Sau khi đã cài đặt thành công dịch vụ IIS, ở màn hình quản lý IIS sẽ có giao diện như sau:



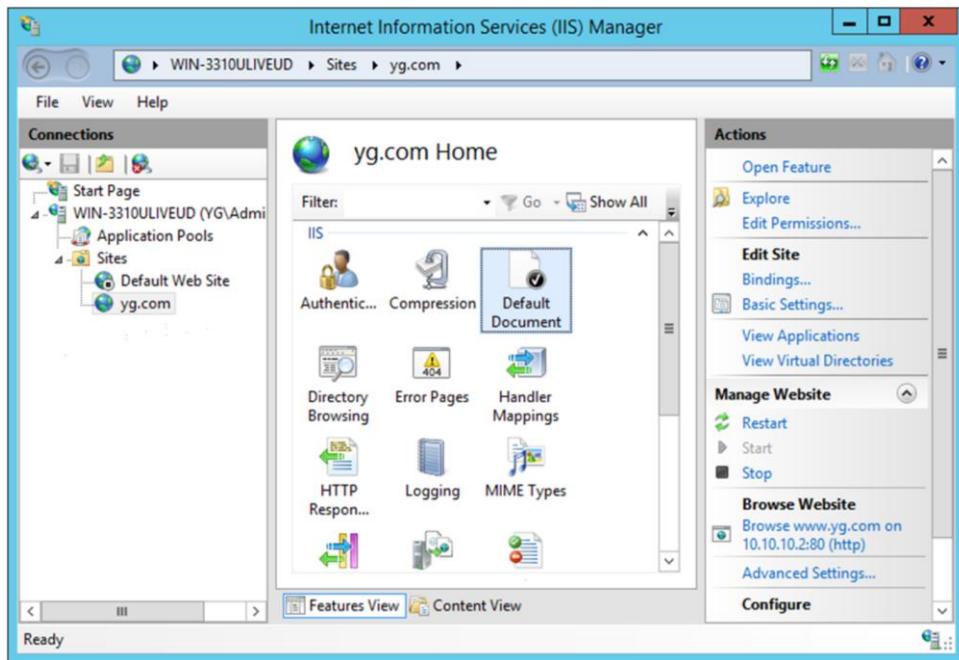
Hình 4.1.5a: Tắt trang web mặc định của web server

Chúng ta có thể thêm source web vào các ô đĩa của Server, sau đó gán vào đường dẫn khi tạo website mới.



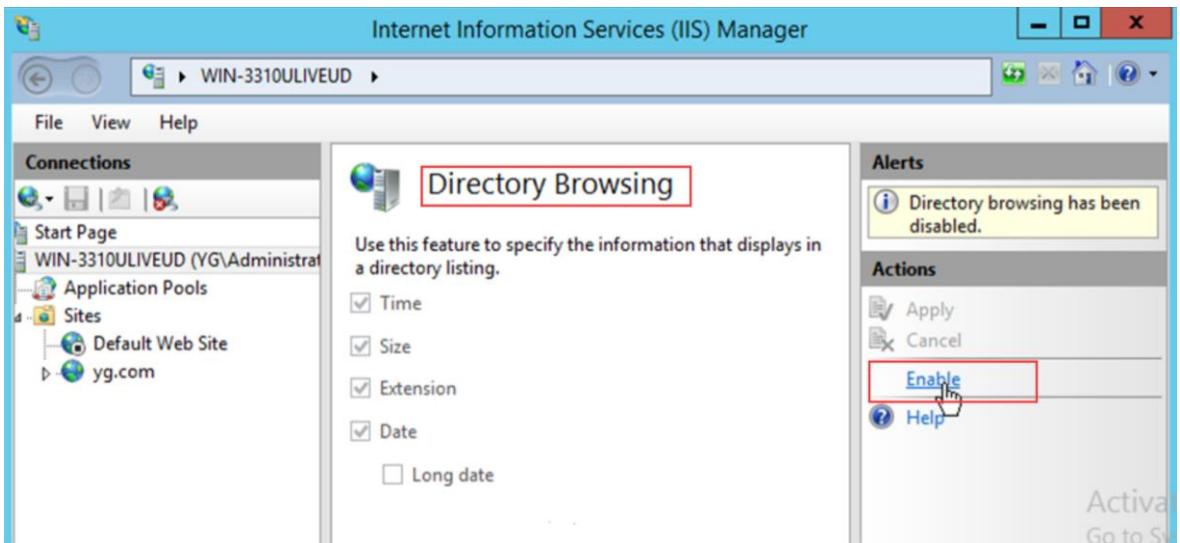
Hình 4.1.5b: Tạo website mới

Sau khi tạo thành công website, giao diện quản lý sẽ hiển thị như sau:



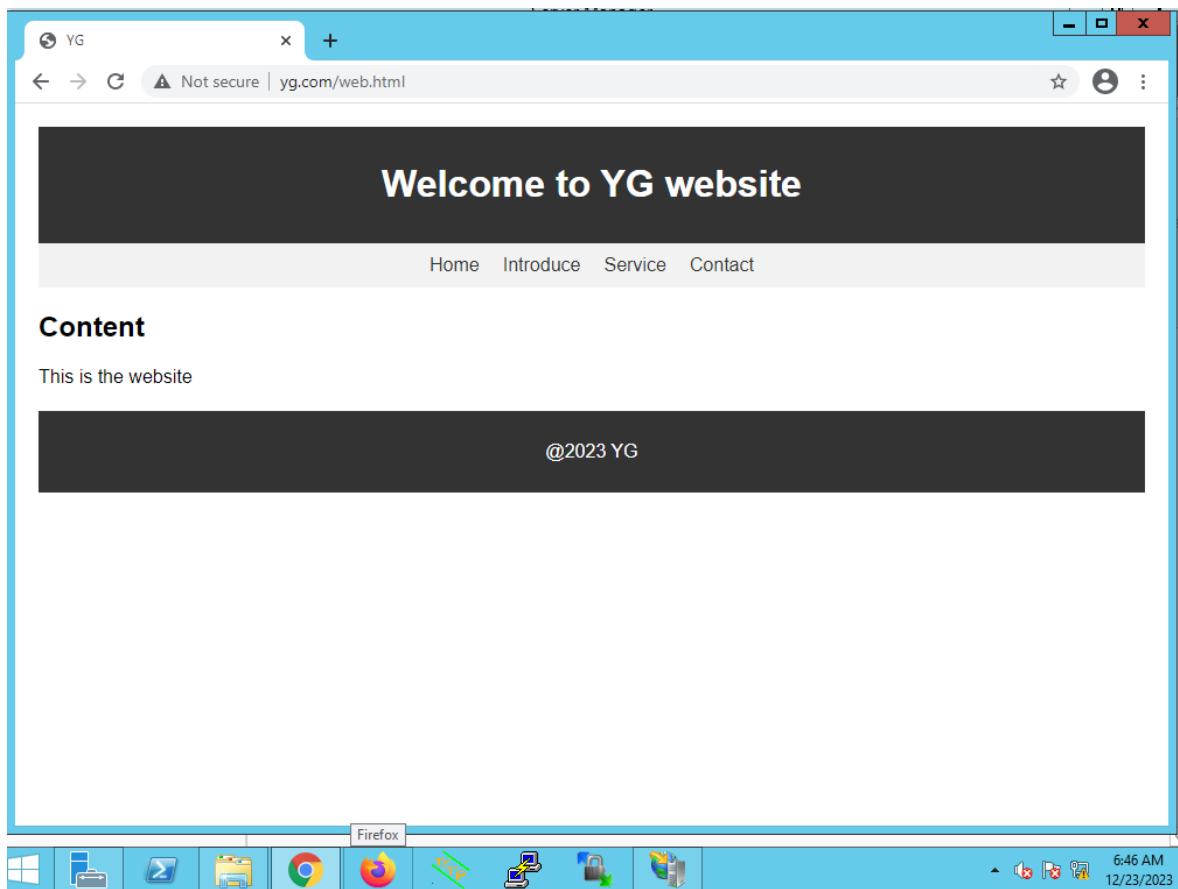
Hình 4.1.5c: Giao diện quản lý website

Để có thể vào được trang web vừa tạo, chúng ta cần phải đến mục Directory Browsing và chọn Enable.



Hình 4.1.5d: Bật Directory Browsing

Sau đó sử dụng máy chủ hoặc máy client để vào thử trang web.

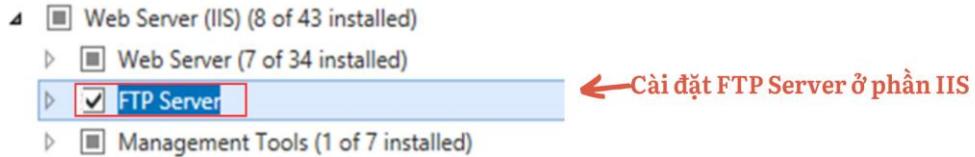


Hình 4.1.5e: Giao diện của trang web

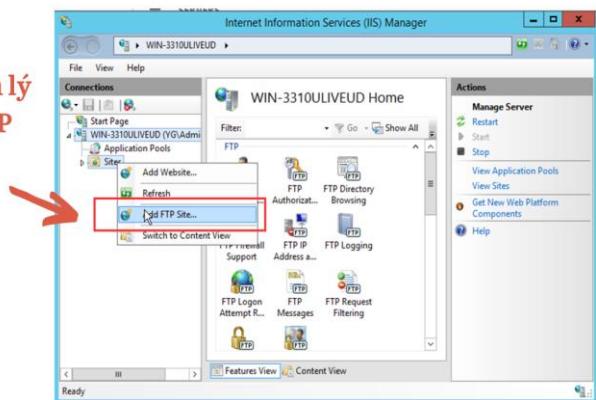
#### 4.1.6 FTP Server

FTP server – File Transfer Protocol là một loại phần mềm hoặc dịch vụ trên mạng được sử dụng để lưu trữ và quản lý các tập tin và thư mục và cho phép người dùng truy cập và truyền tải chúng qua mạng Internet. FTP server thường được sử dụng để chia sẻ và truyền tải tệp tin và dữ liệu giữa các máy tính trên mạng, đặc biệt là trong các doanh nghiệp.

Đối với dịch vụ FTP sẽ nằm trong Webserver, chúng ta sẽ chọn vào Webserver, sau đó chọn FTP Server.

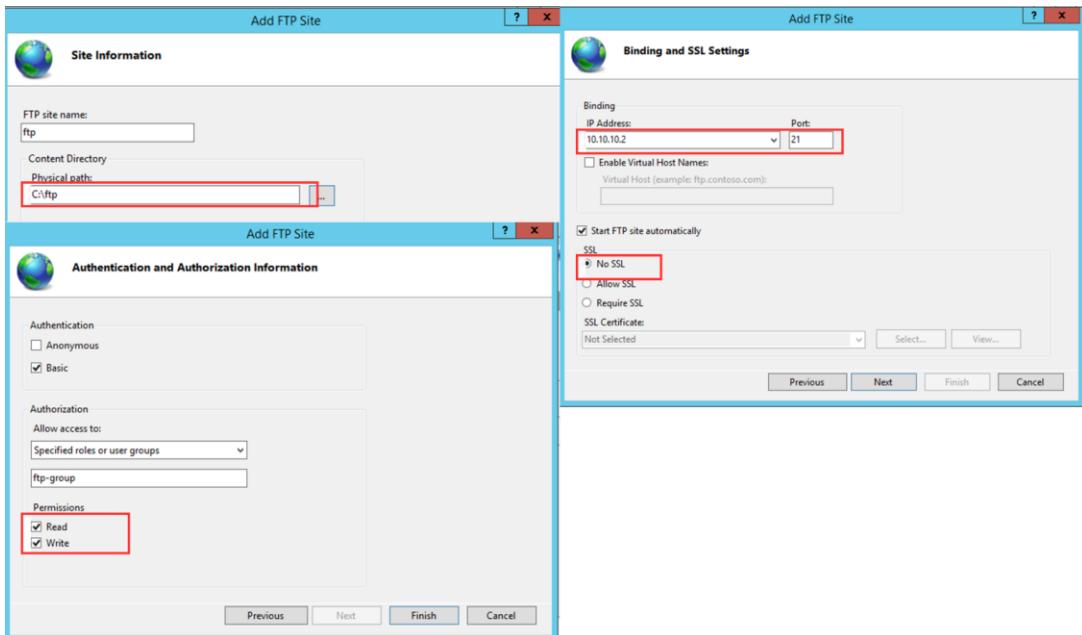


Sau khi cài đặt thì vào phần quản lý  
 IIS sẽ xuất hiện trường Add FTP  
 Site



Hình 4.1.6a: Cài đặt FTP ở mục IIS

Sau khi đã cài đặt thành công FTP vào máy chủ, chúng ta sẽ tiến hành xây dựng FTP cho phép người dùng có tài khoản mới được truy cập. Tài khoản này sẽ được tạo trên Server File Service

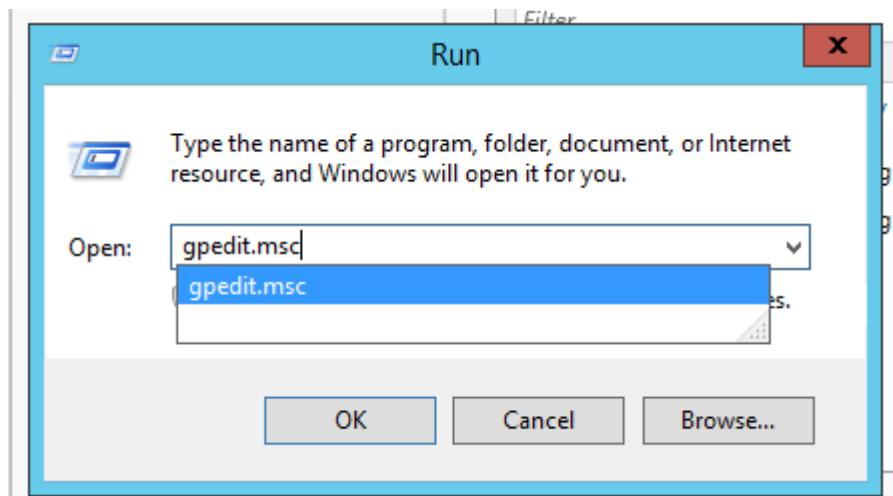


Hình 4.1.6b: Cấu hình truy cập có tài khoản

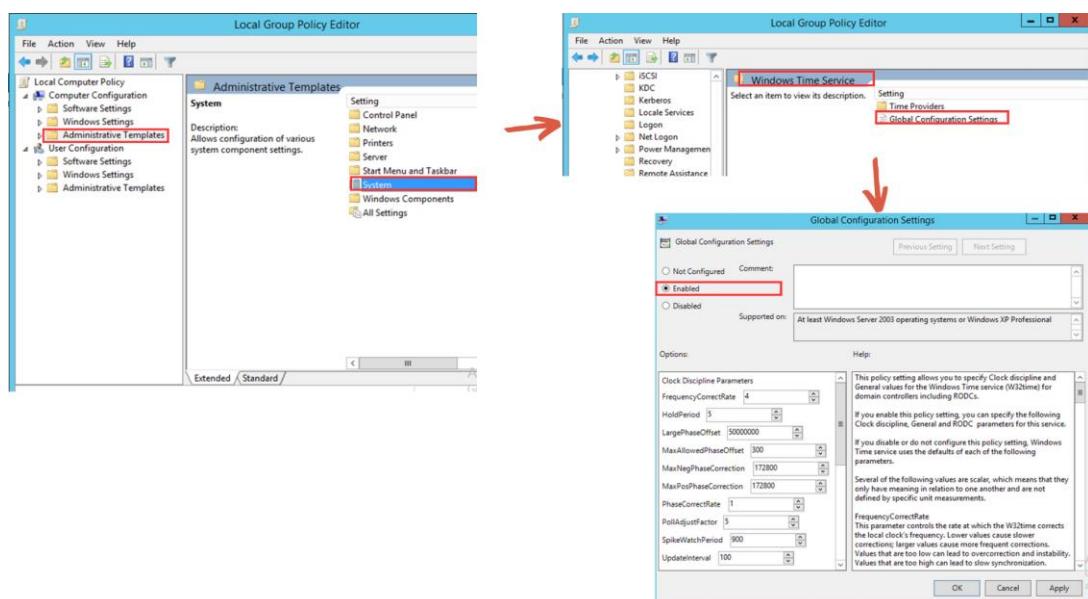
#### 4.1.7 NTP Syslog Server

NTP – Network Time Protocol, là một dịch vụ quan trọng không chỉ cho các thiết bị của Cisco mà hầu hết mọi thiết bị mạng. Bất kỳ thiết bị nào cũng cần được đồng bộ hóa chính xác với nguồn thời gian đáng tin cậy như máy chủ NTP.

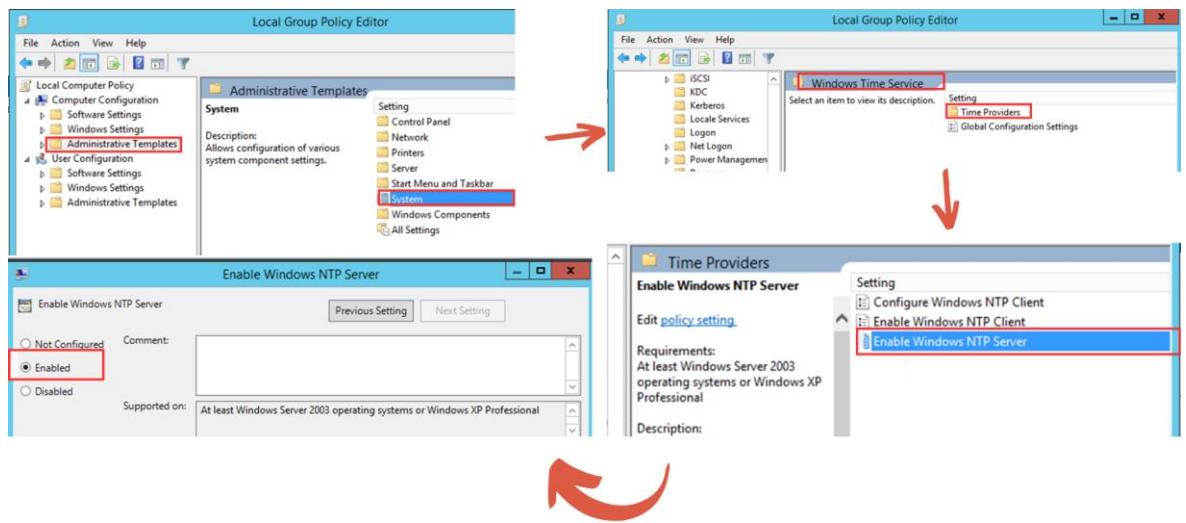
Để cài đặt dịch vụ NTP trên máy chủ, chúng ta sẽ mở Windows + R và nhập ‘gpedit.msc’



Hình 4.1.7a: Chạy gpedit.msc để cài đặt NTP

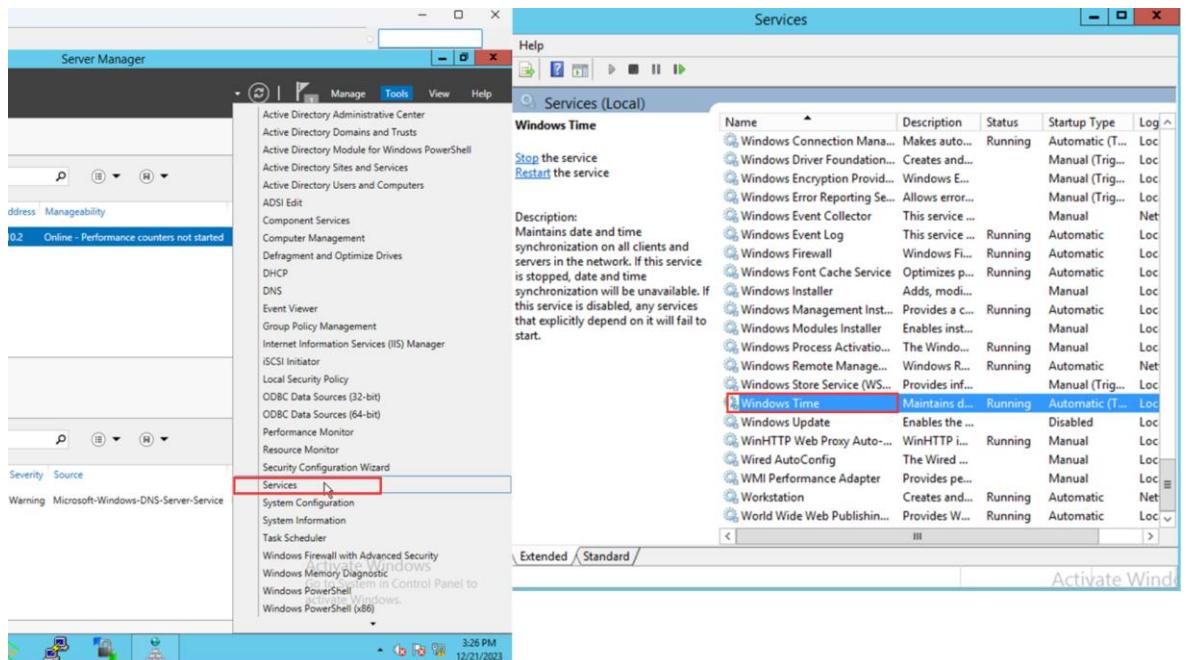


Hình 4.1.7b: Bật các dịch vụ trong NTP

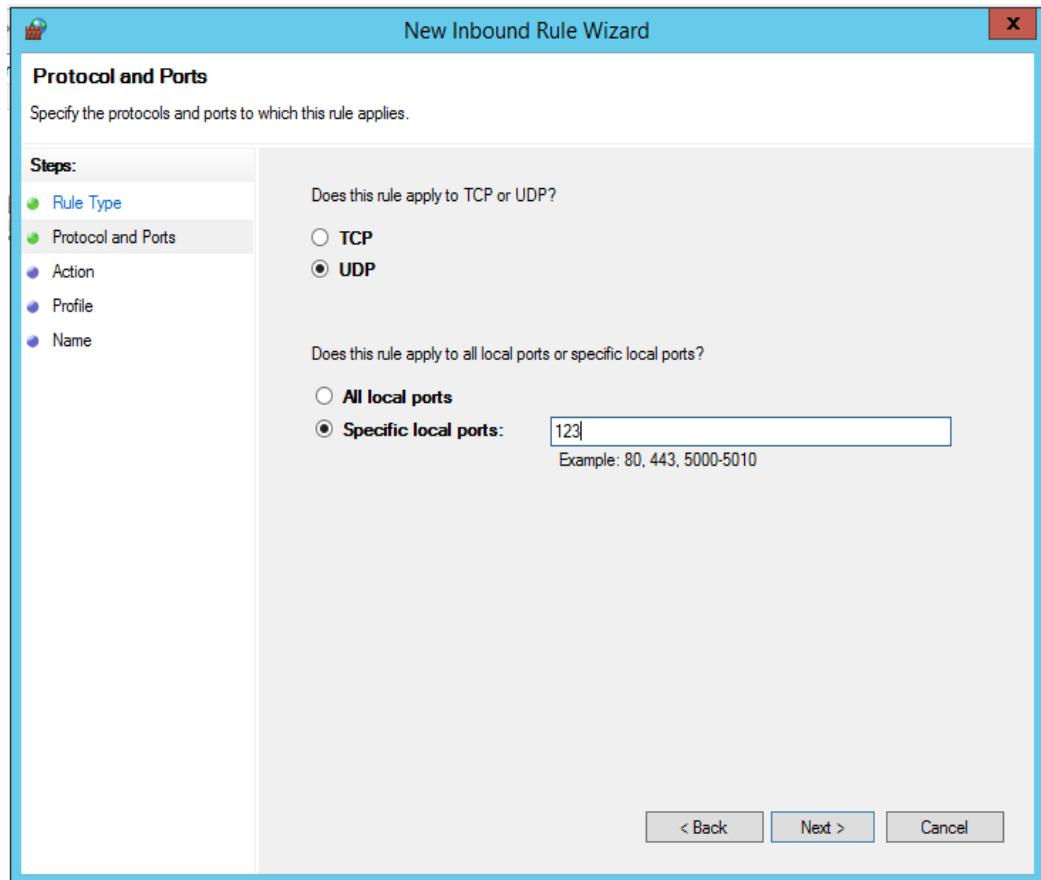


Hình 4.1.7c: Bật các dịch vụ trong NTP

Sau khi đã cấu hình xong, vào Tool => Service để bật Windows Time lên.



Hình 4.1.7c: Restart dịch vụ Windows Time

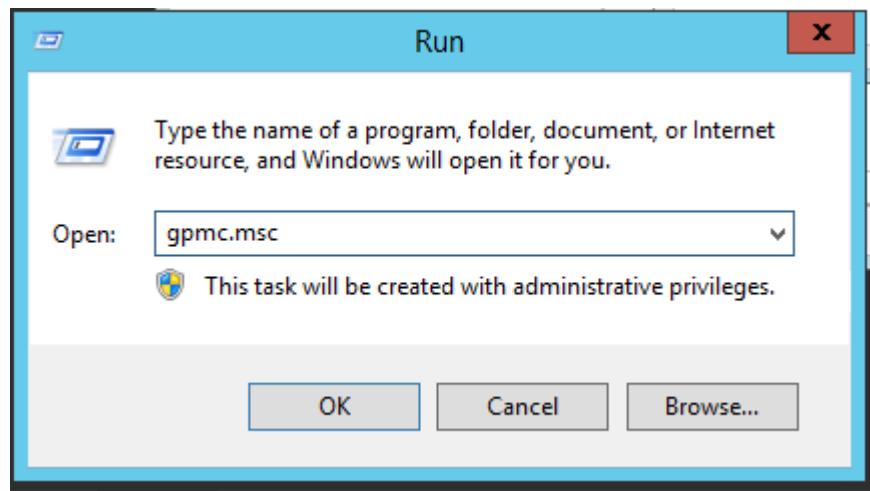


Hình 4.1.7d: Cài đặt Rules cho Inbound

## 4.2 Group Policy Management

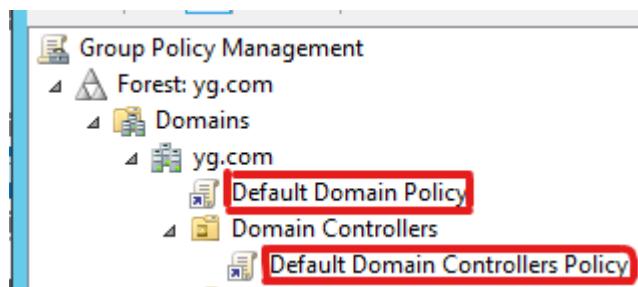
Group Policy là tập hợp các rules nhằm kiểm soát môi trường làm việc của nhân viên trong môi trường Domain. Group Policy giúp kiểm soát được user có thể làm gì và không được làm gì trên hệ thống máy tính.

Để mở GPO, chúng ta sẽ sử dụng tổ hợp phím Windows + R để mở hộp thoại Run và nhập lệnh gpmc.msc



Hình 4.2a: Mở GPO

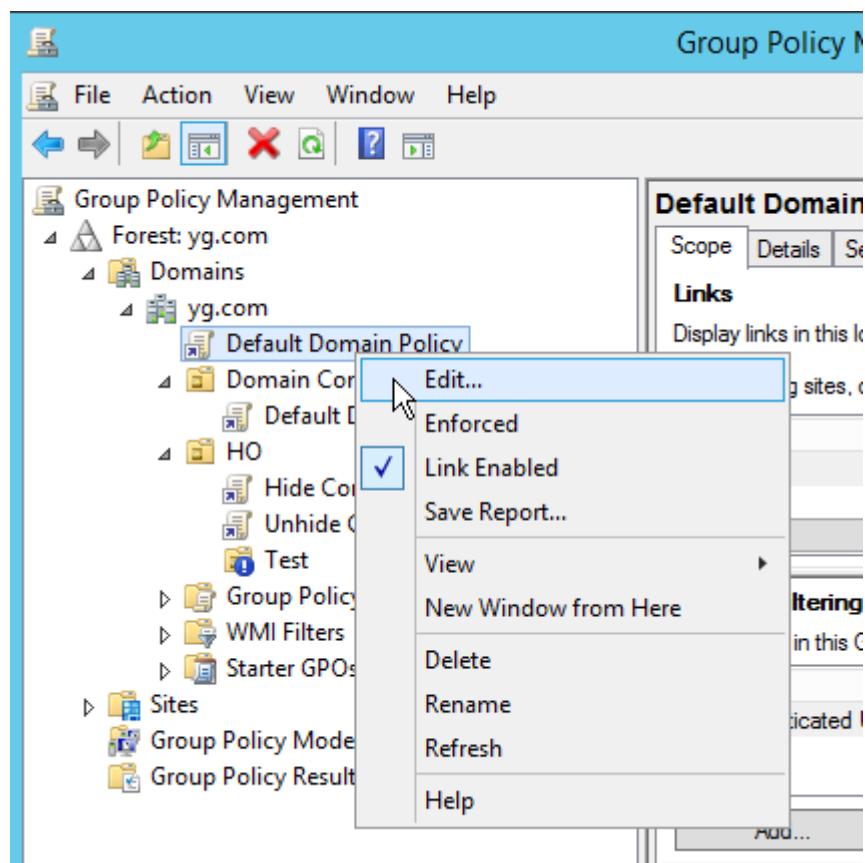
Trong GPO sẽ có 2 chính sách mặc định là Default Domain Controller Policy (áp dụng cho DC), Default Domain Policy (Áp dụng cho toàn hệ thống).



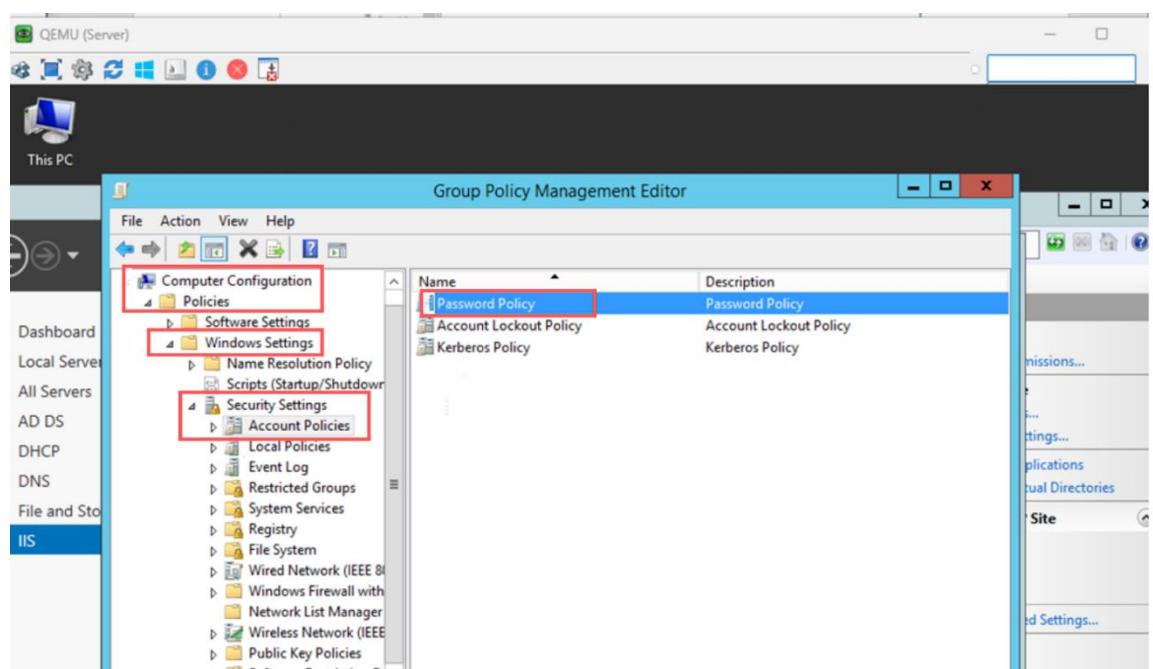
Hình 4.2b: Hai Policy mặc định của hệ thống

Bắt đầu tạo các Policy đơn giản.

#### **4.2.1 *Chỉnh sửa Password***



Hình 4.2.1a: Chọn Default Domain Policy => chuột phải chọn Edit



Hình 4.2.1b: Vào Password Policy

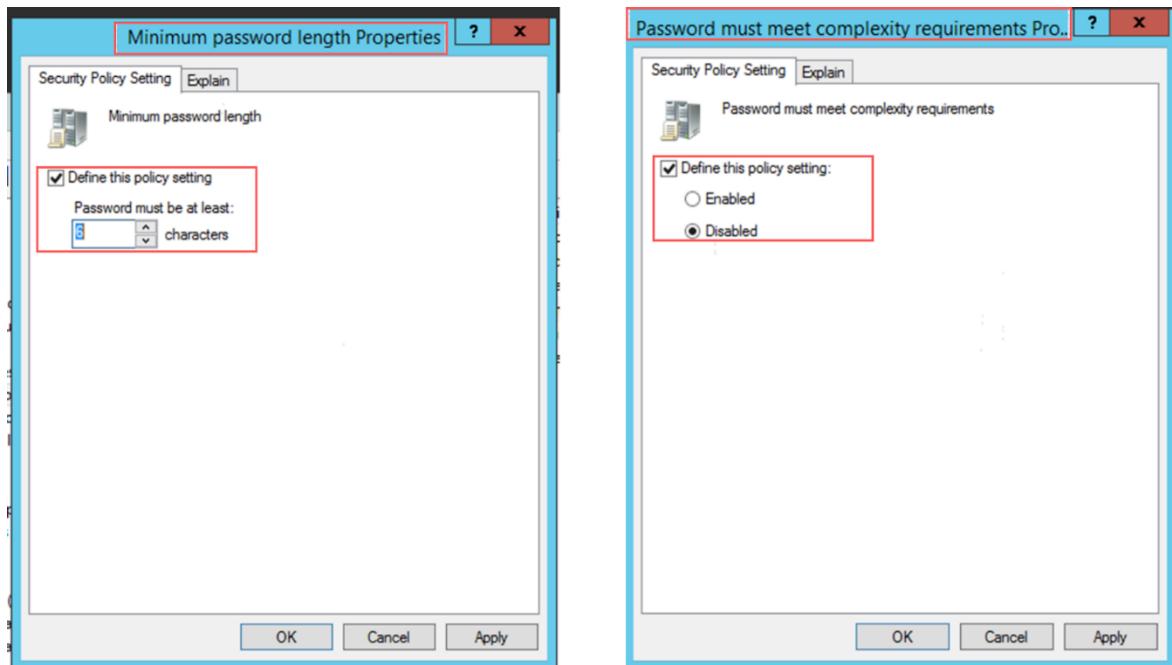


Hình 4.2.1c: Các Policy trong Password Policy

Trong Password Policy sẽ bao gồm một số chính sách cơ bản, bao gồm:

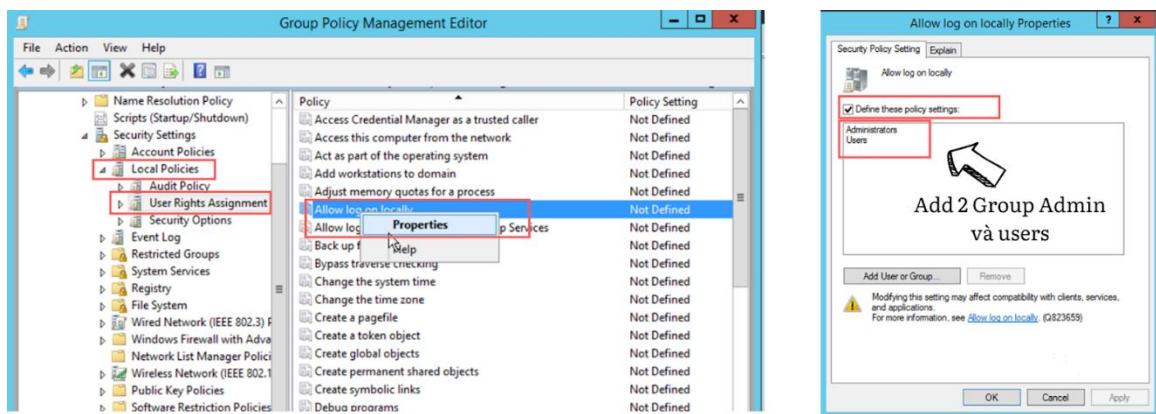
1. **Enforce password history:** Thực thi lịch sử mật khẩu, nhớ 24 mật khẩu gần đây nhất. Buộc người dùng phải tạo mật khẩu mới, giá trị mặc định là 24, có nghĩa nếu người dùng chưa sử dụng đủ 24 mật khẩu mới sẽ không thể sử dụng lại một mật khẩu.
2. **Maximum password age:** Tuổi đời tối đa của mật khẩu, sẽ hết hạn sau 42 ngày.
3. **Minimum password age:** Tuổi đời tối thiểu của mật khẩu, hết hạn sau 1 ngày. Cài đặt này giúp Enforce password history từ chối người dùng thay đổi mật khẩu quá thường xuyên, mặc định là một ngày, có nghĩa là sau 1 ngày thì người dùng mới có thể thay đổi mật khẩu khác.
4. **Minimum password length:** Độ dài mật khẩu tối thiểu 7 ký tự
5. **Password must meet complexity requirements:** Mật khẩu yêu cầu phải đáp ứng đủ các nguyên tắc:
  - Người dùng không thể sử dụng tên tài khoản hoặc tên người dùng, không được phép sử dụng 2 ký tự của tên liên tiếp.
  - Bao gồm 3 ký tự khác nhau từ bất kỳ số, chữ hoa, chữ thường mà ký tự đặc biệt (@,\$,&,#).
  - Có ít nhất 6 ký tự

6. Store password using reversible encryption: Không lưu trữ mật khẩu bằng mã hóa có thể đảo ngược, có nghĩa là mật khẩu có thể được giải mã và xem ở dạng văn bản thuần túy.



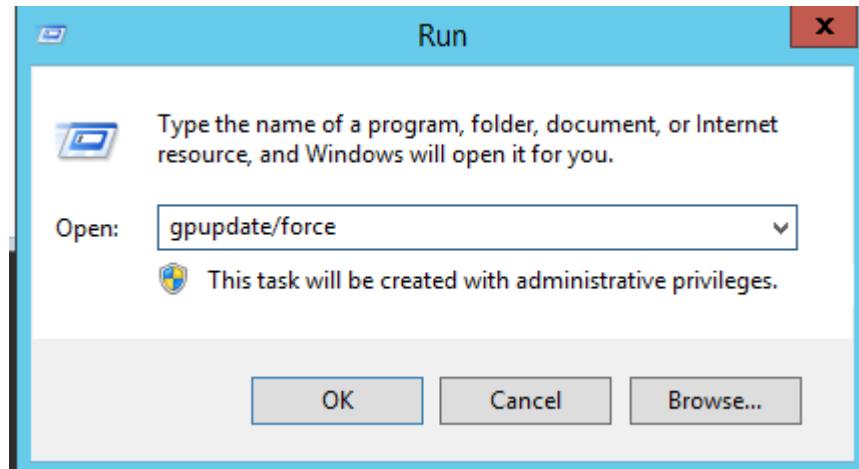
Hình 4.2.1d: Độ dài tối thiểu của password là 6 và Disable chính sách password phức tạp.

#### 4.2.2 Cho phép Group Users có quyền Log on Locally



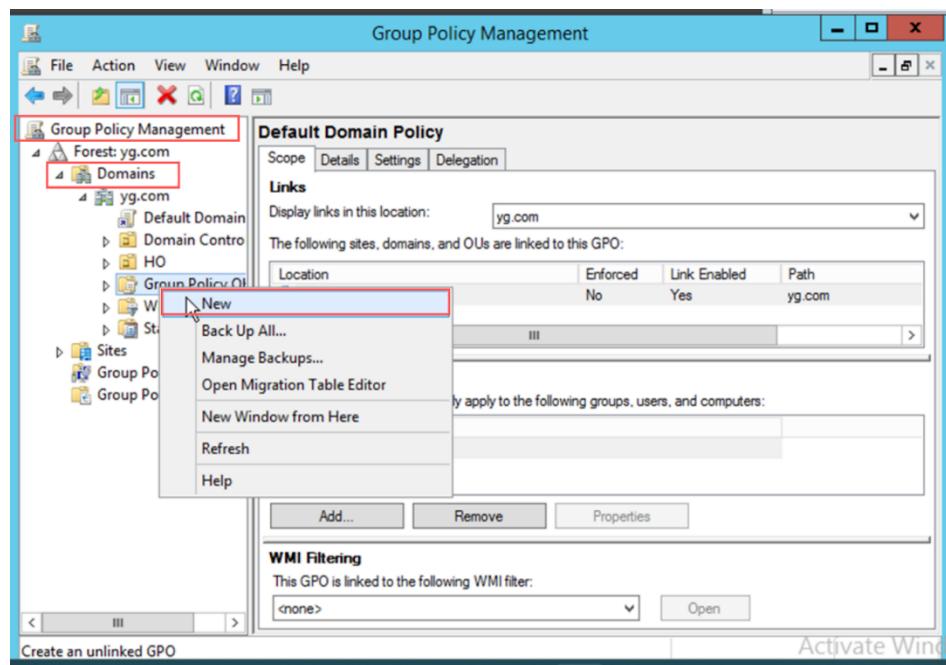
Hình 4.2.2a: Add Group có quyền được Log on Locally

Sau khi chỉnh sửa chính sách thành công, chúng ta sẽ cập nhật lại chính sách đó.



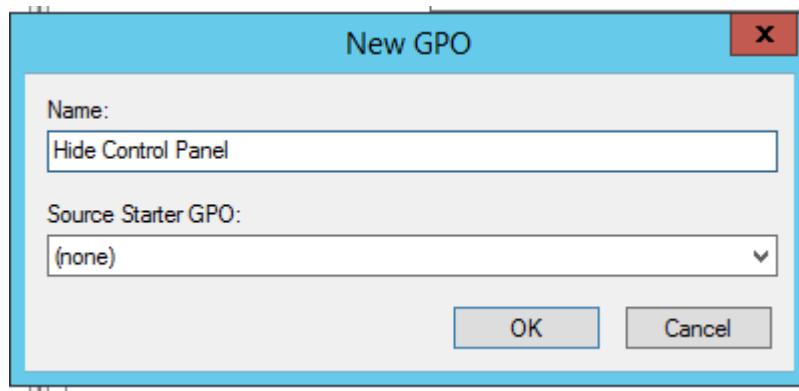
Hình 4.2.2b: Cập nhật chính sách

### 4.2.3 Tạo và link Policy vào OU

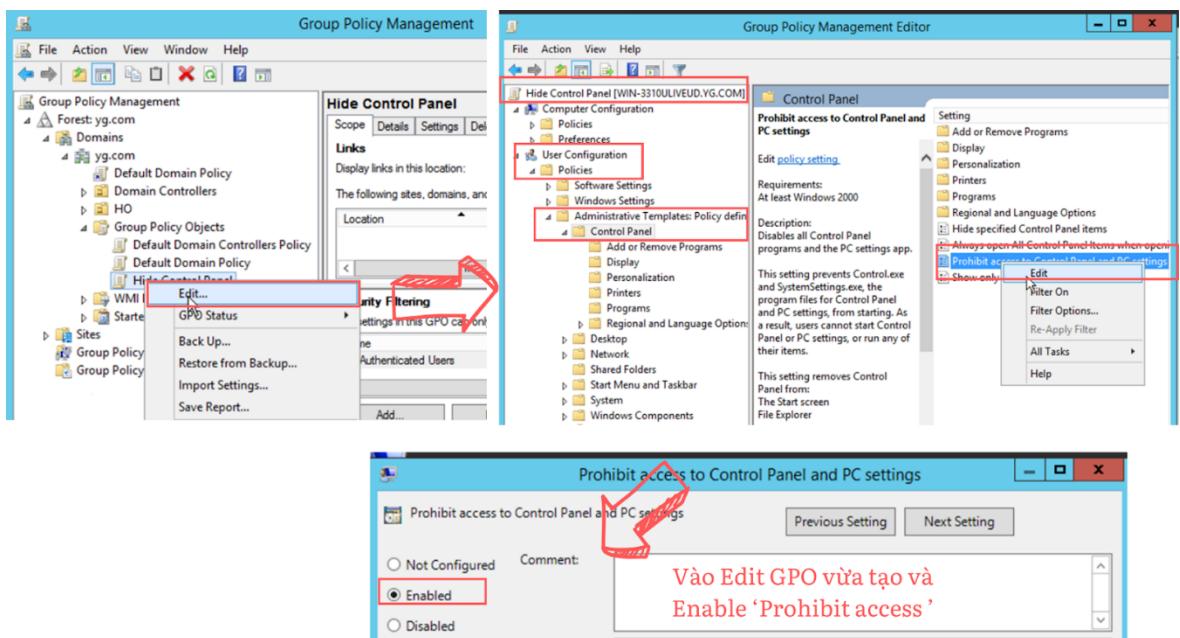


Hình 4.2.3a: Thêm GPO mới

Tạo một chính sách mới, ở đây sẽ là chính sách ẩn tab Control Panel

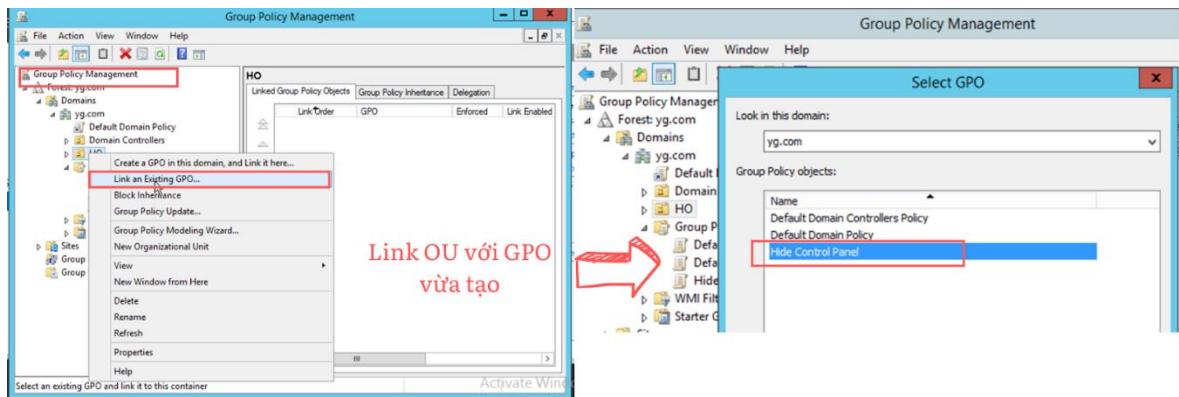


Hình 4.2.3b: Tạo GPO mới

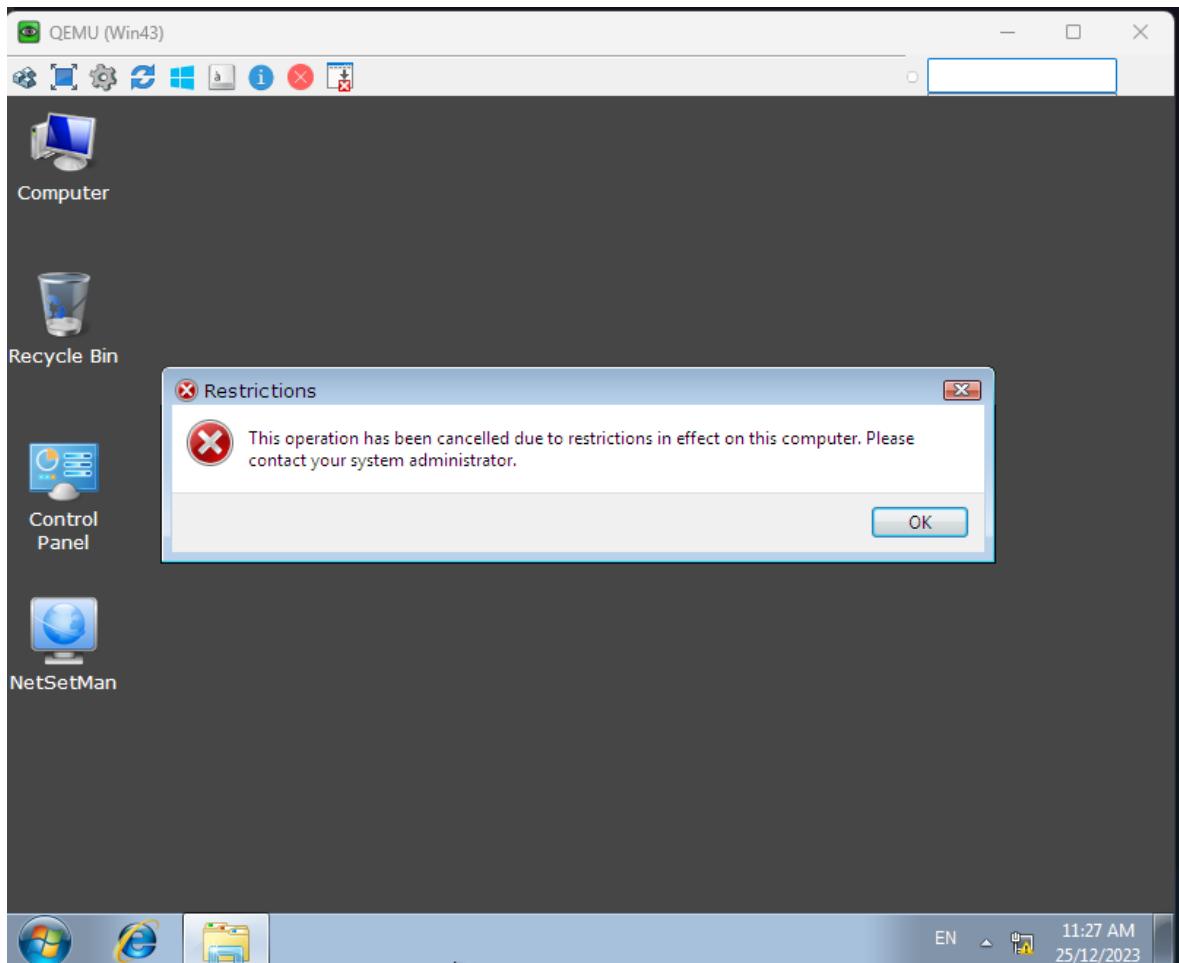


Hình 4.2.3c: Edit chính sách vừa tạo

Quay trở lại màn hình Group Policy Management, và link OU với GPO vừa tạo.



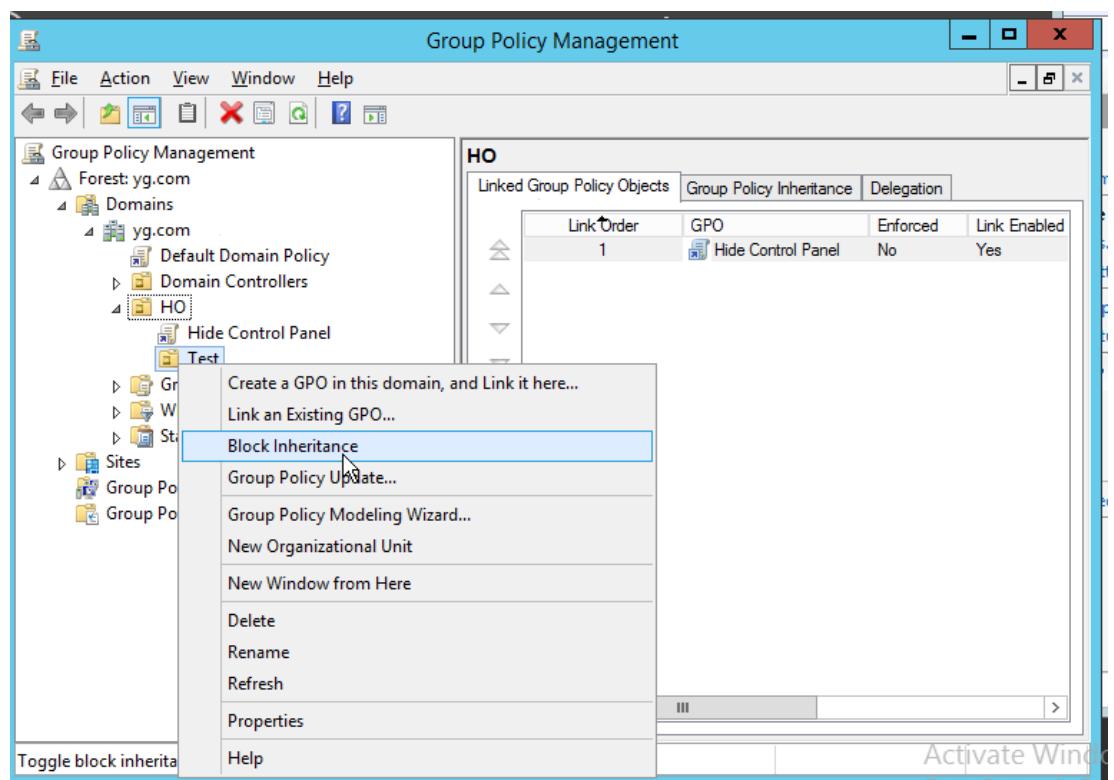
Hình 4.2.3e: Link OU với GPO vừa tạo.



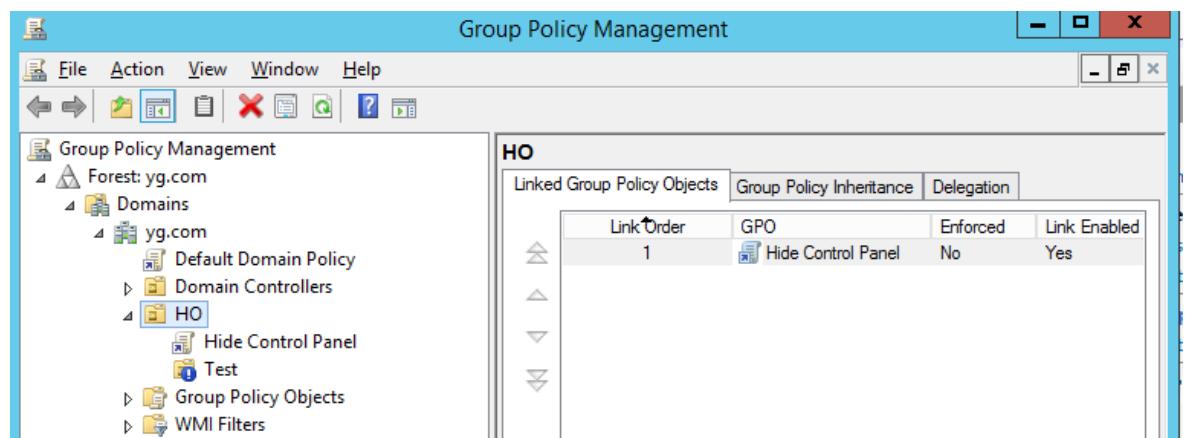
Hình 4.2.3f: Máy Client sau khi áp dụng chính sách sẽ không thể mở Control Panel

#### **4.2.4 Block Inheritance cho OU**

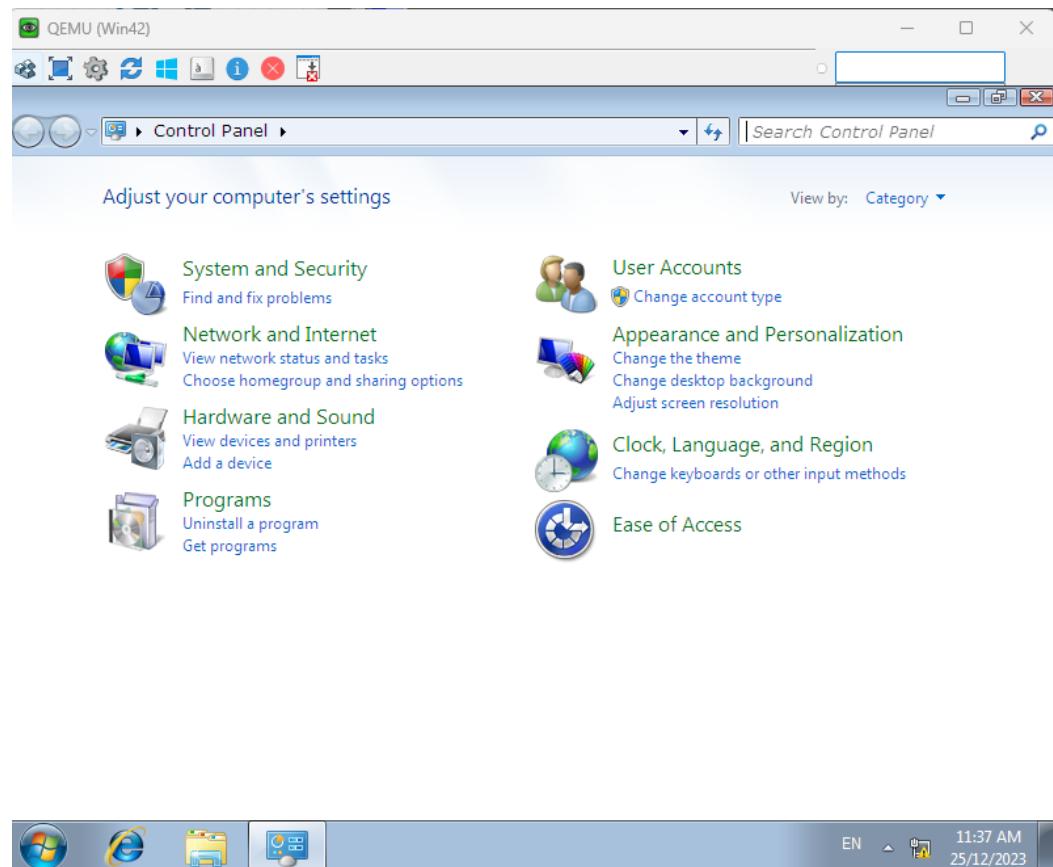
Tạo một OU Test trong OU HO sau đó mở Group Policy Management và chọn Block Inheritance cho OU Test.



Hình 4.2.4a: Block Inheritance cho OU Test.

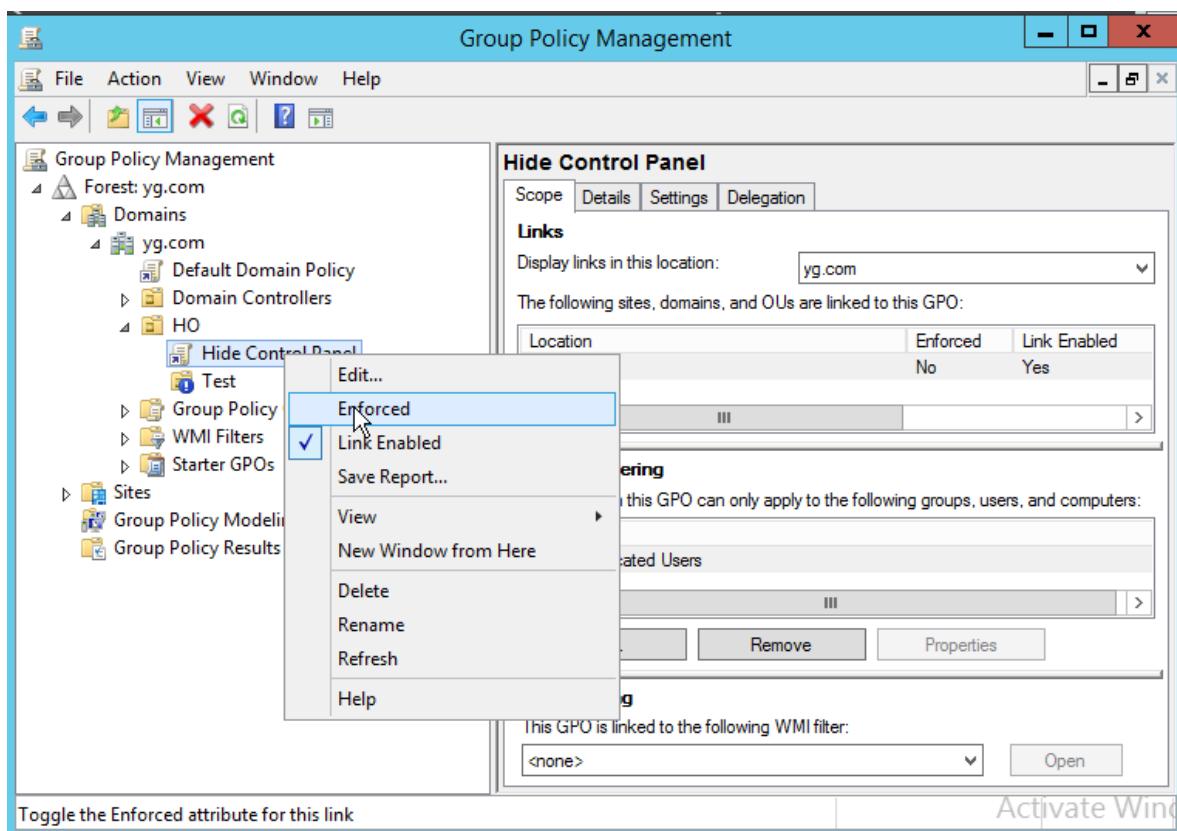


Hình 4.2.4b: OU Test sẽ có dấu chấm thang



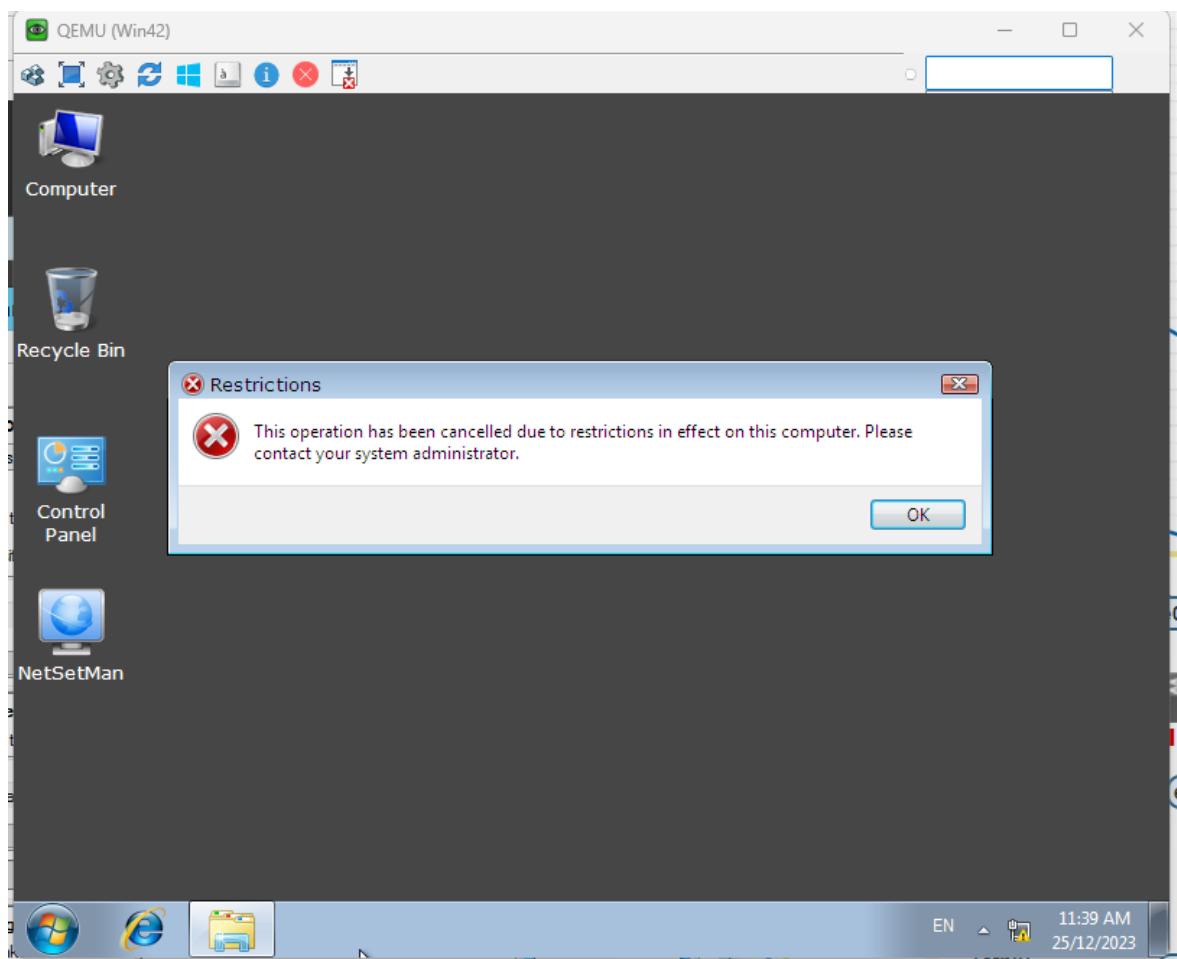
Hình 4.2.4c: Các máy client trong OU Test sẽ thấy được Control Panel

#### 4.2.5 *Enforce Policy*



Hình 4.2.5a: Mở Group Policy Management và chọn Enforced cho GPO "Hide Control Panel"

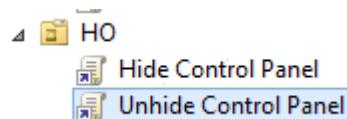
Khi chọn Enforced cho chính sách ẩn Control Panel, nó sẽ bắt buộc áp dụng tất cả chính sách trong OU. Loại bỏ tất cả các chính sách dưới OU kể cả khi có cấu hình Block Inheritance.



Hình 4.2.5b: Các máy client sau khi được áp chính sách sẽ không thể mở Control Panel

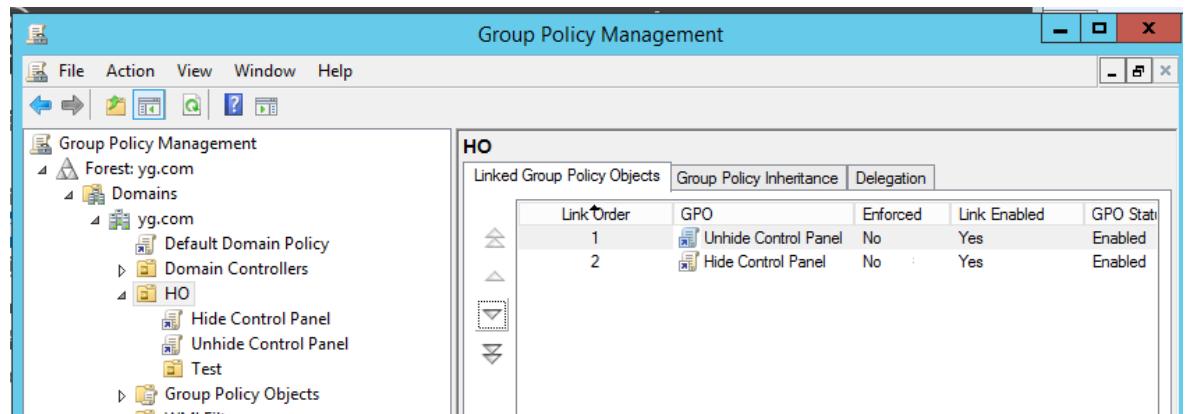
#### 4.2.6 *Chỉnh thứ tự cho Policy*

Trước khi chúng ta sắp xếp thứ tự cho Policy, chúng ta cần tắt các Enforced và Block Inheritance đã test ở các phần trên. Sau đó tạo thêm một GPO với tên “Unhide Control Panel” sau đó chọn Disable khi edit GPO. Tương tự như các bước trước đó, chúng ta sẽ link GPO này vào OU HO.



Hình 4.2.6a: Lúc này ở OU HO sẽ có 2 policy

Chúng ta có thể thấy thứ tự hiện tại là Policy Unhide Control Panel nằm ở vị trí thứ 2, điều này có nghĩa chính sách ẩn sẽ có quyền cao nhất hiện tại. Do đó chúng ta cần đưa chính sách Unhide lên trên đầu.

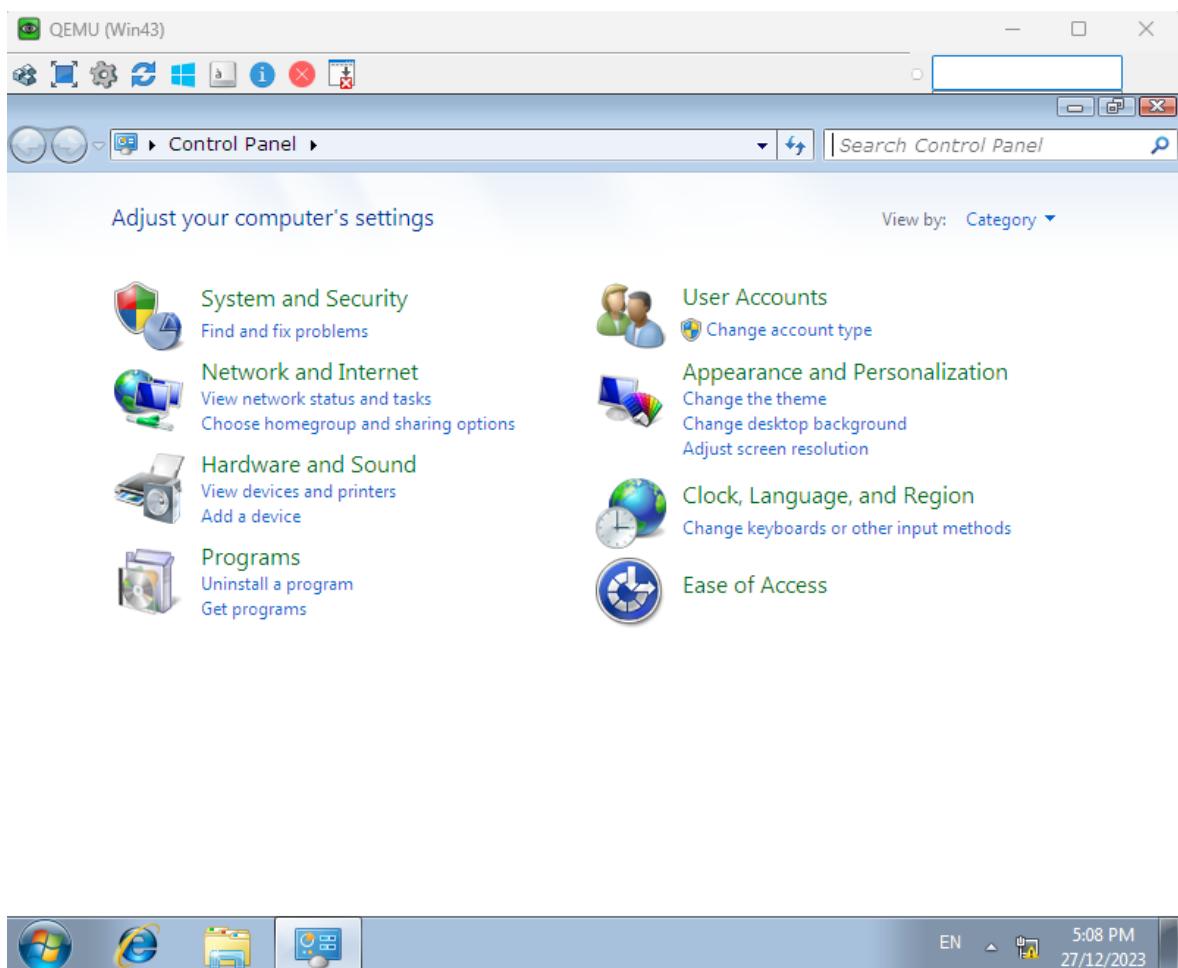


Hình 4.2.6b: Chuyển Policy lên thứ tự 1

Precedence	GPO	Location	GPO Status	WMI Status
1	Unhide Control Panel	HO	Enabled	No
2	Hide Control Panel	HO	Enabled	No
3	Default Domain Policy	yg.com	Enabled	No

Hình 4.2.6c: Precedence hiện tại của Policy ẩn tab Control Panel là 1

Lưu ý: Sau khi tạo chính sách phải luôn nhớ update chính sách đó.

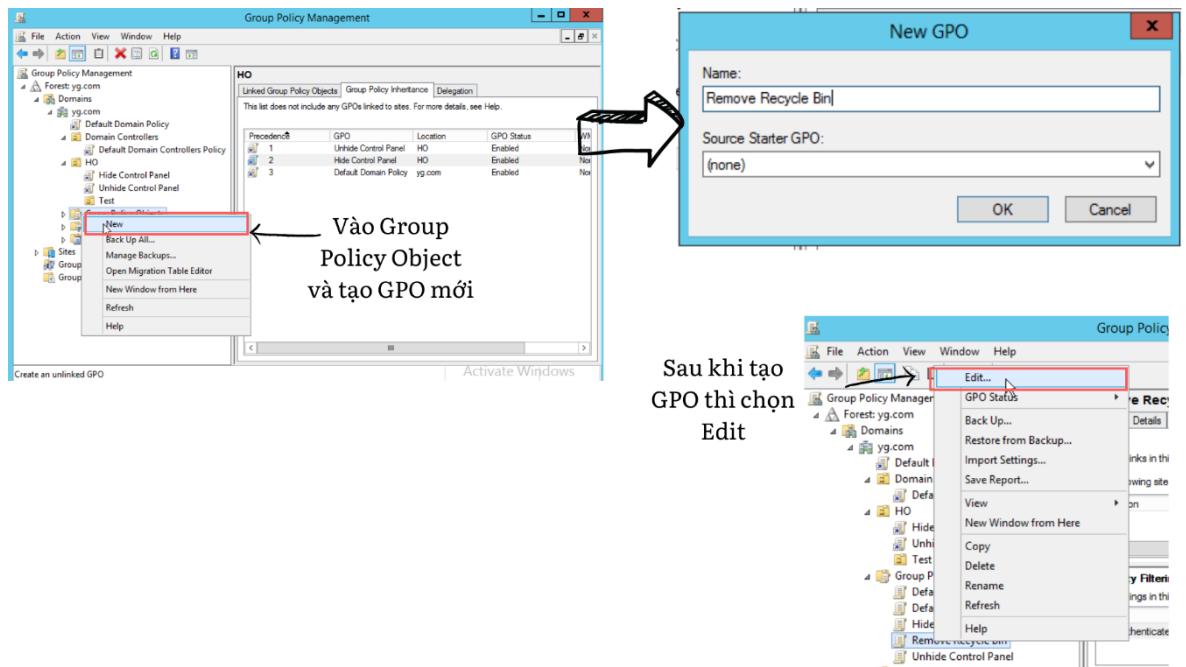


Hình 4.2.6d: Lúc này các máy client đã có thể mở Control Panel.

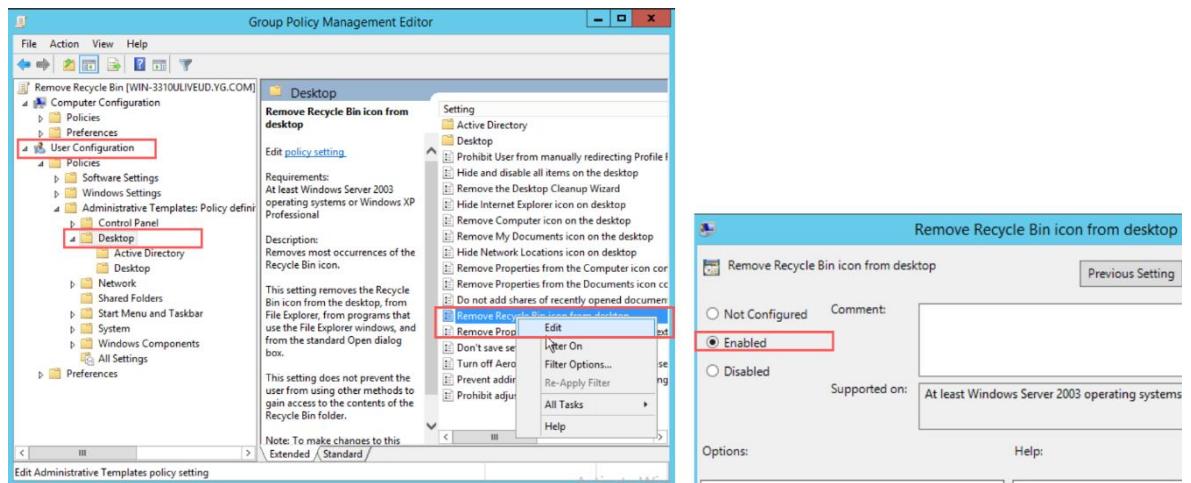
Ta có thể thấy, trong cùng 1 OU nếu áp chung 2 policy (không Enforce) thì policy nào có giá trị Link Order nhỏ thì sẽ có độ ưu tiên cao hơn. Nếu áp chung 2 policy (cả 2 policy đều Enforce) thì policy nào có giá trị Link Order nhỏ thì sẽ có độ ưu tiên cao hơn. Nếu áp chung 2 policy (1 policy Enforce và 1 policy không Enforce) thì policy Enforce sẽ có độ ưu tiên cao hơn.

#### **4.2.7 Một số GPO cơ bản**

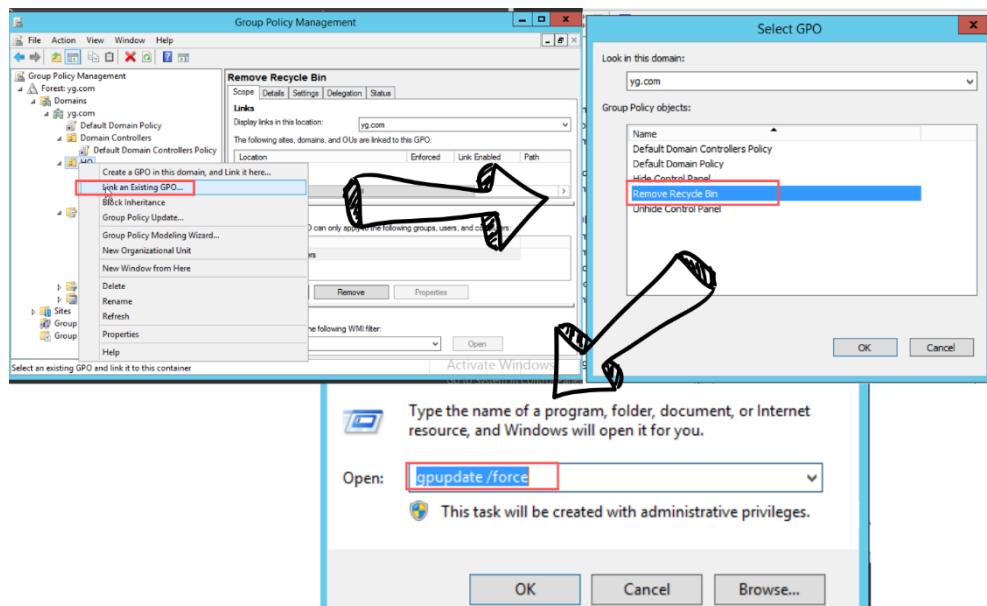
❖ **Ấn icon trên màn hình Desktop**



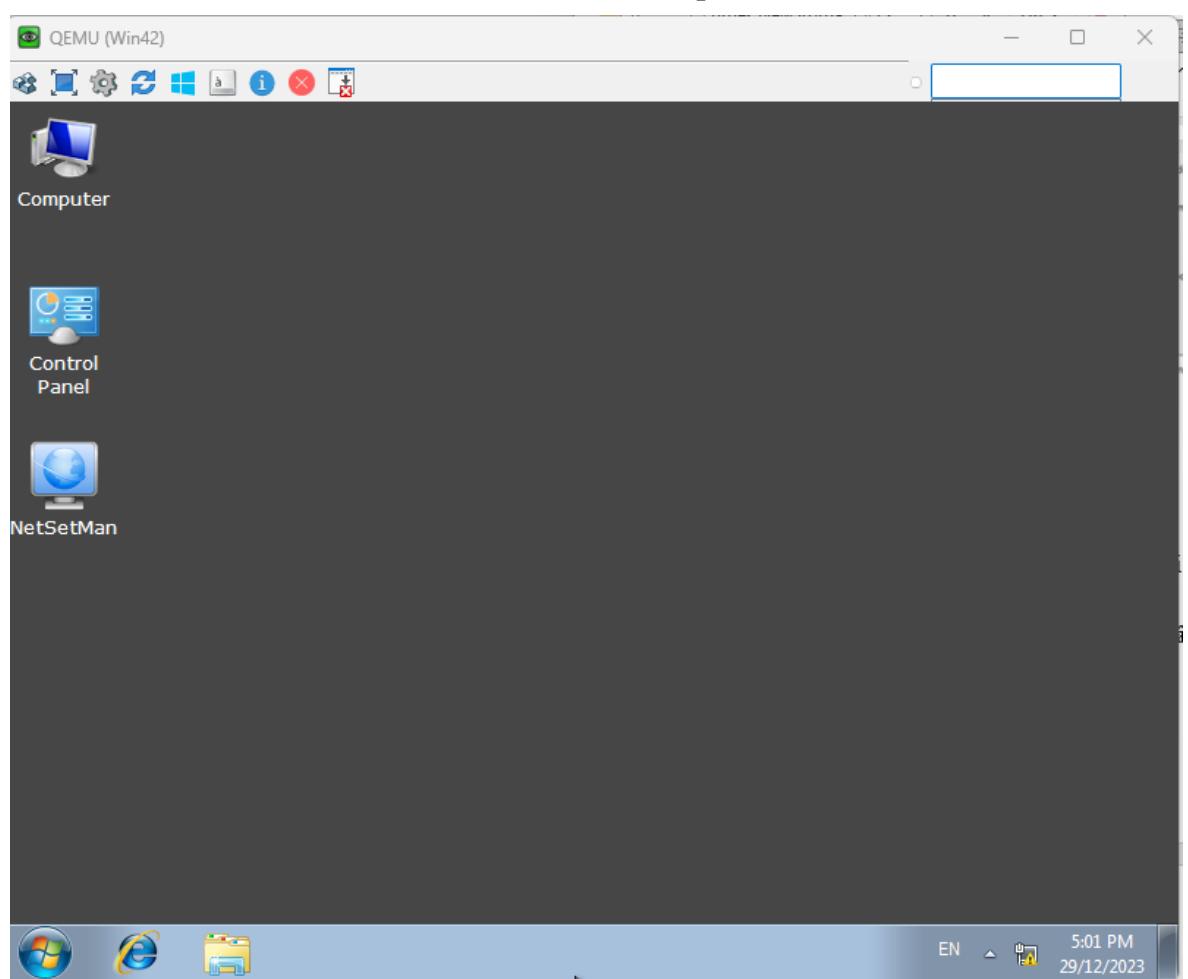
Hình 4.2.7a: Tạo GPO mới với tên “Remove Recycle Bin”



Hình 4.2.7b: Vào mục Remove Recycle Bin icon from desktop và enabled



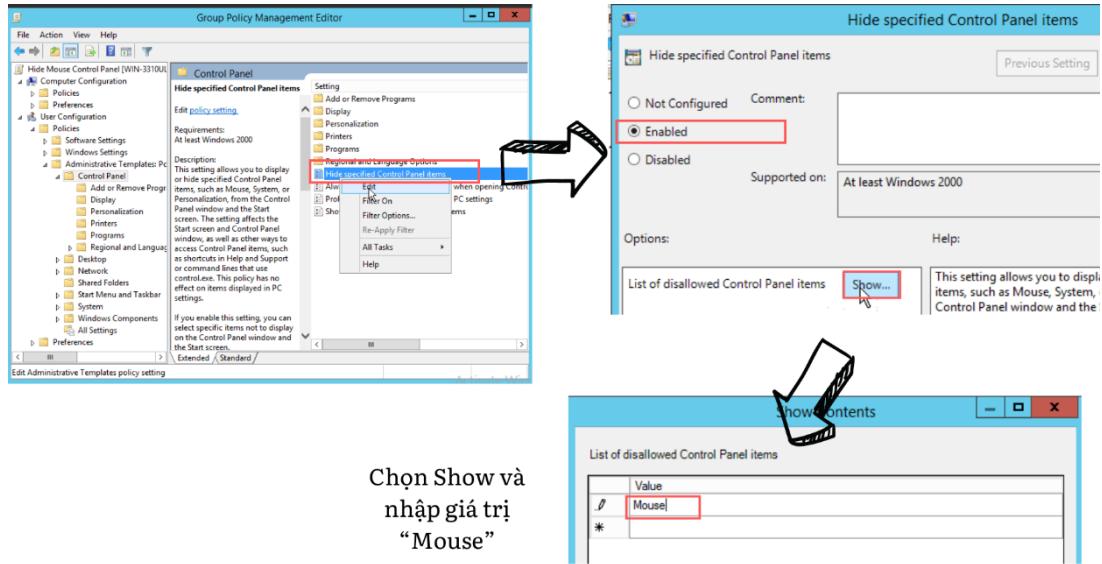
Hình 4.2.7c: Link GPO vừa tạo với OU và Update chính sách



Hình 4.2.7d: Icon Recycle Bin đã mất khỏi màn hình

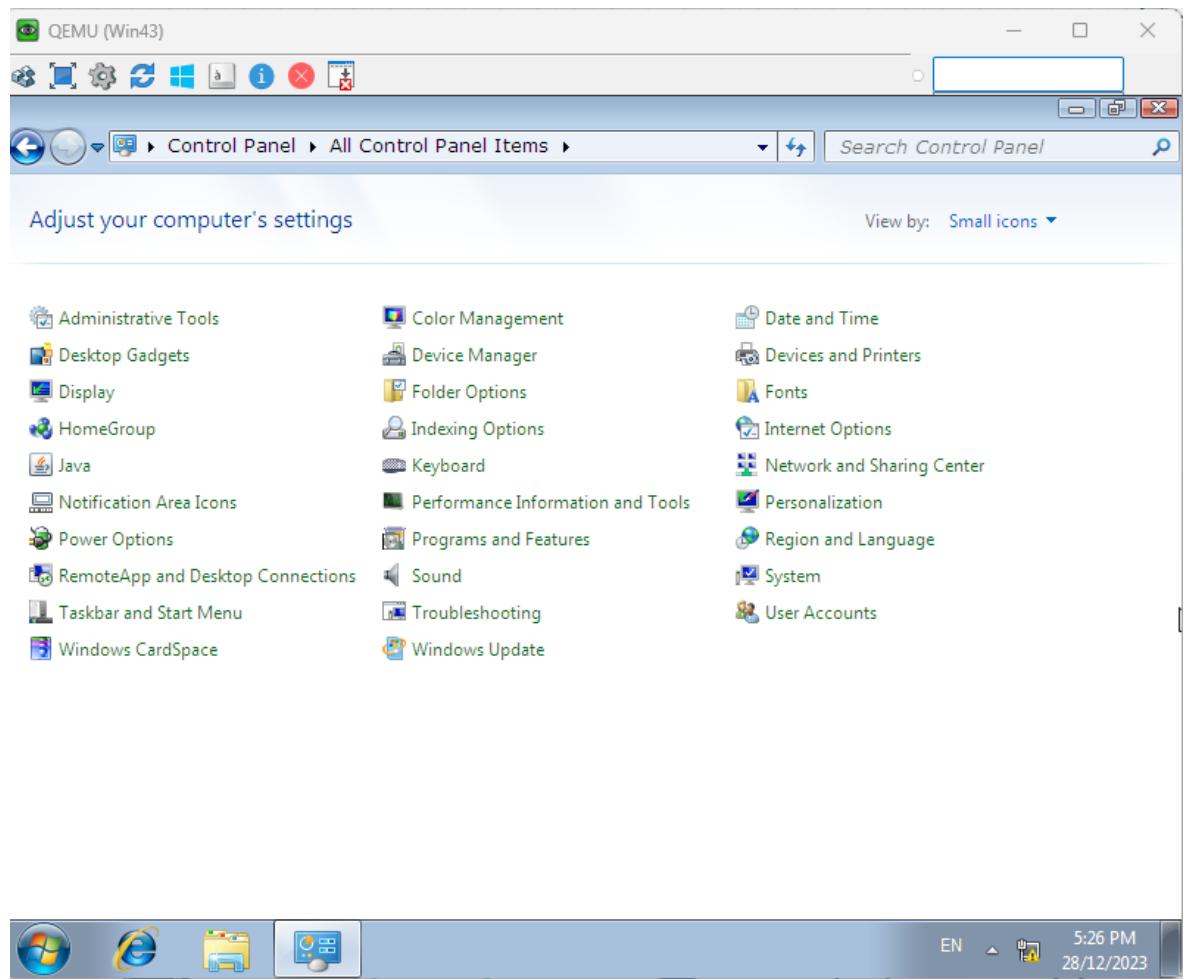
### Ân item trong Control Panel

Tương tự như các bước trên, chúng ta vẫn sẽ tạo GPO trước tiên với tên “Hide Mouse Control Panel” sau đó vào edit GPO vừa tạo.



Hình 4.2.7e: Bật mục Hide specified Control Panel items

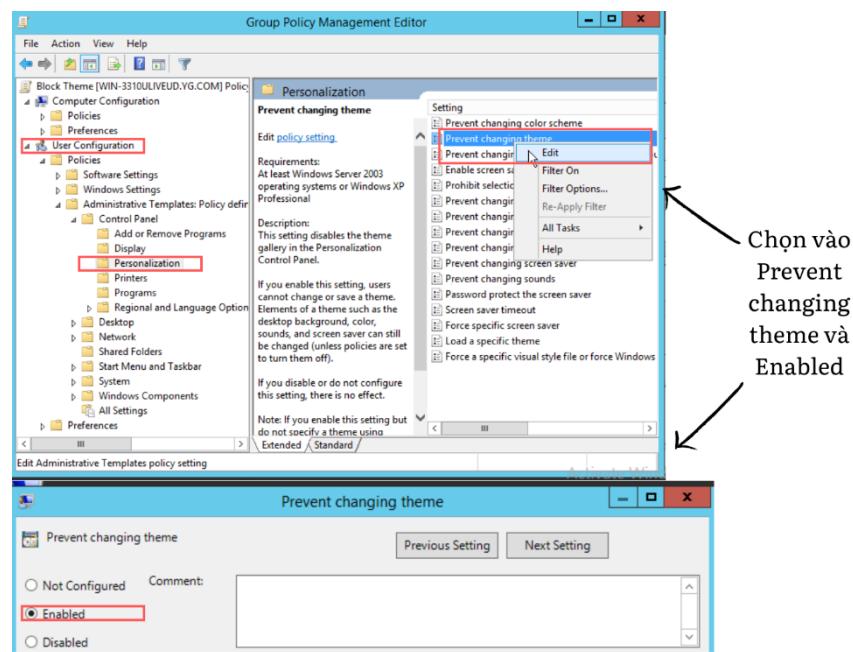
Sau đó thực hiện các bước link với OU và update chính sách tương tự như các bước trên.



Hình 4.2.7f: Icon Mouse bị mất trong tab Control Panel của các máy client

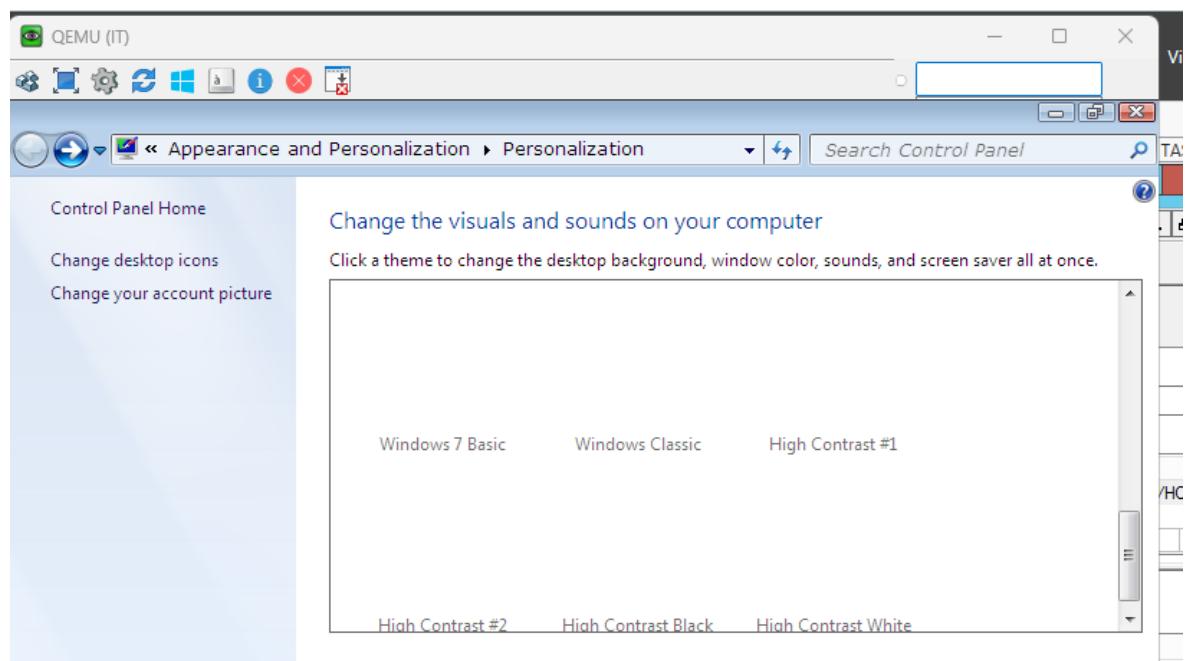
### Cấm đổi Theme

Tạo một GPO với tên là Block Theme và chọn Edit GPO vừa tạo.



Hình 4.2.7g: Enabled mục Prevent changing theme

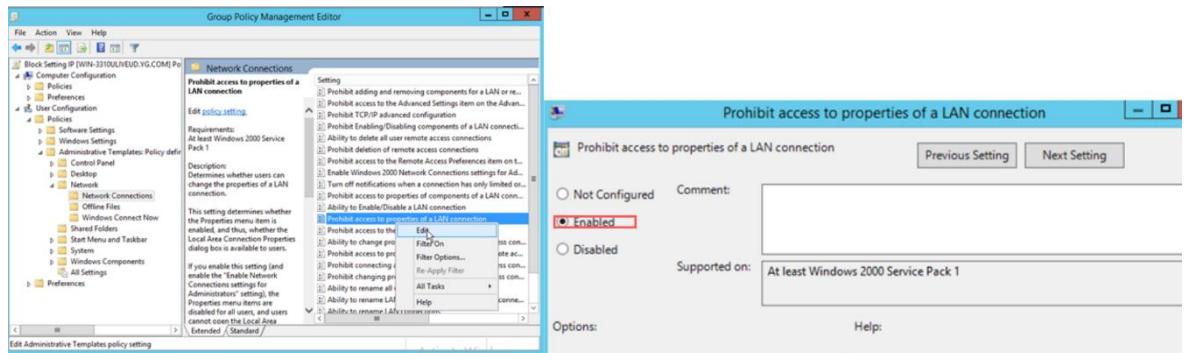
Link GPO và update GPO tương tự các bước trên.



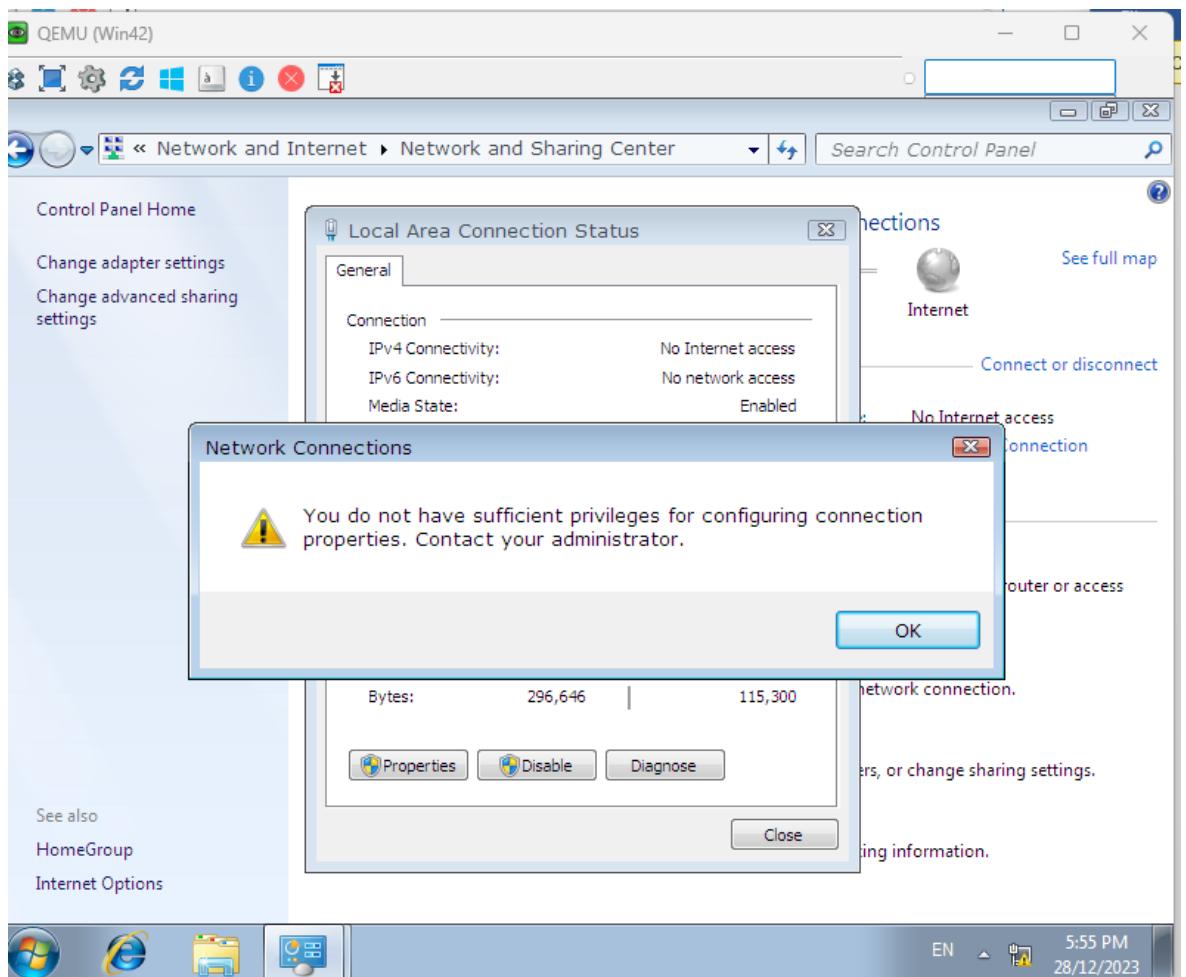
Hình 4.2.7h: Máy client lúc này không thể đổi theme

### Không cho sửa địa chỉ IP

Tạo một GPO với tên “Block Setting IP”



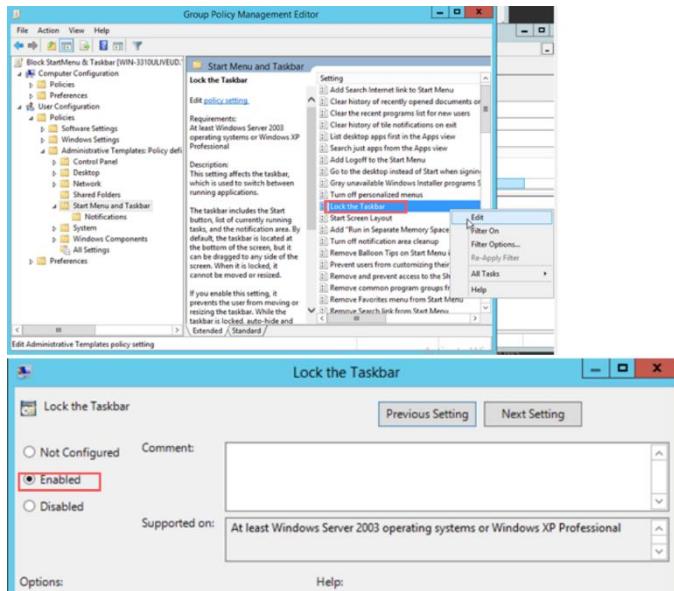
Hình 4.2.7i: Enabled mục Prohibit access to properties of a LAN connection



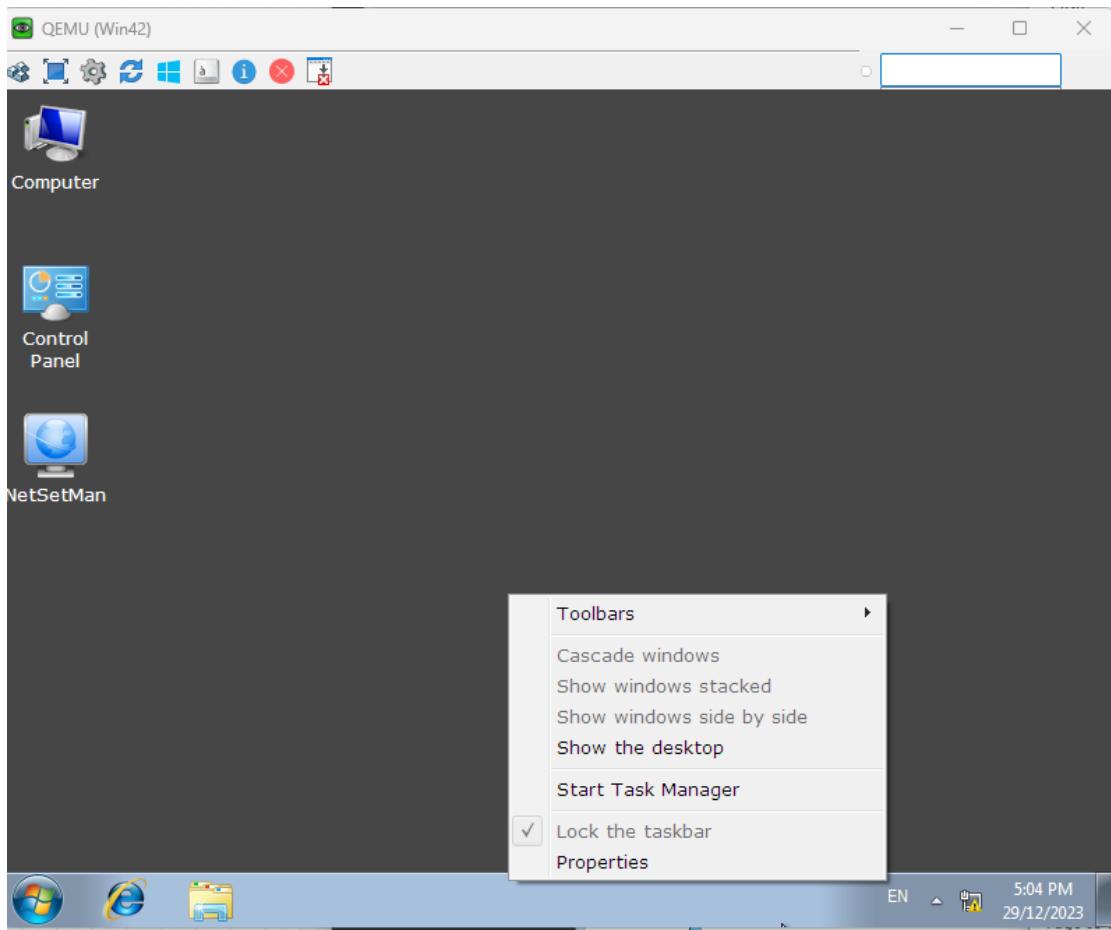
Hình 4.2.j: Các máy client trong OU HO sẽ không thể chỉnh sửa địa chỉ IP

### Khóa Start Menu và Taskbar

Tạo GPO với tên Block StartMenu & Taskbar



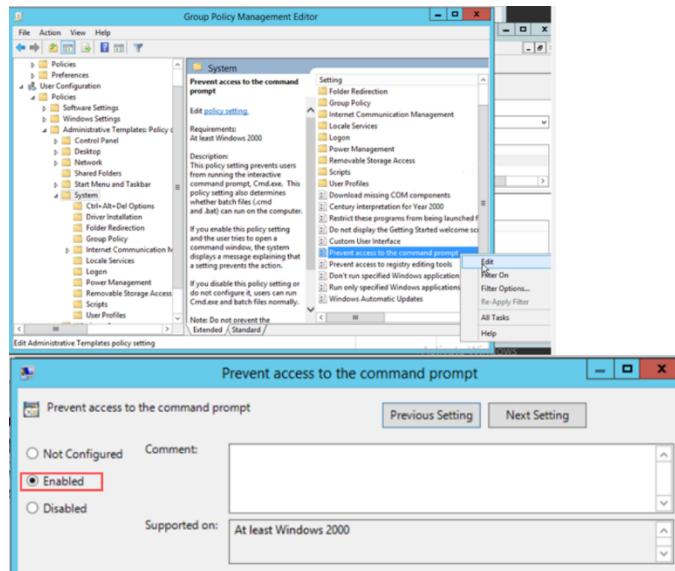
Hình 4.2.7k: Enabled mục Lock the Taskbar



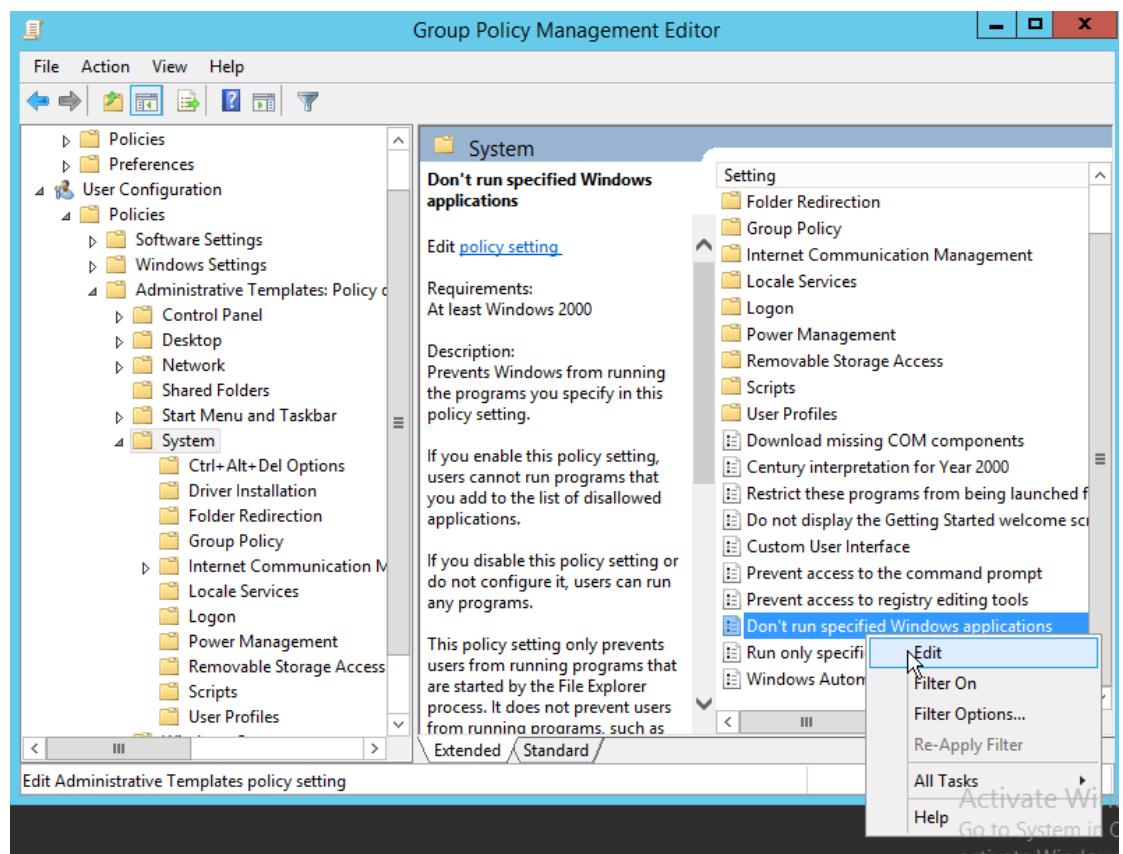
Hình 4.2.7l: Taskbar đã bị khóa trên các máy client

## Không cho sử dụng ứng dụng

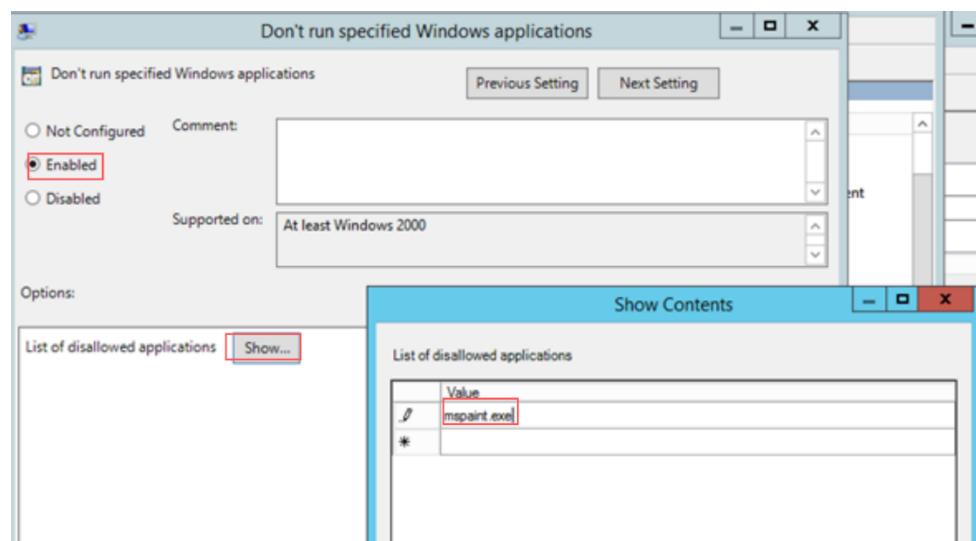
Tạo một GPO với tên “Block App”



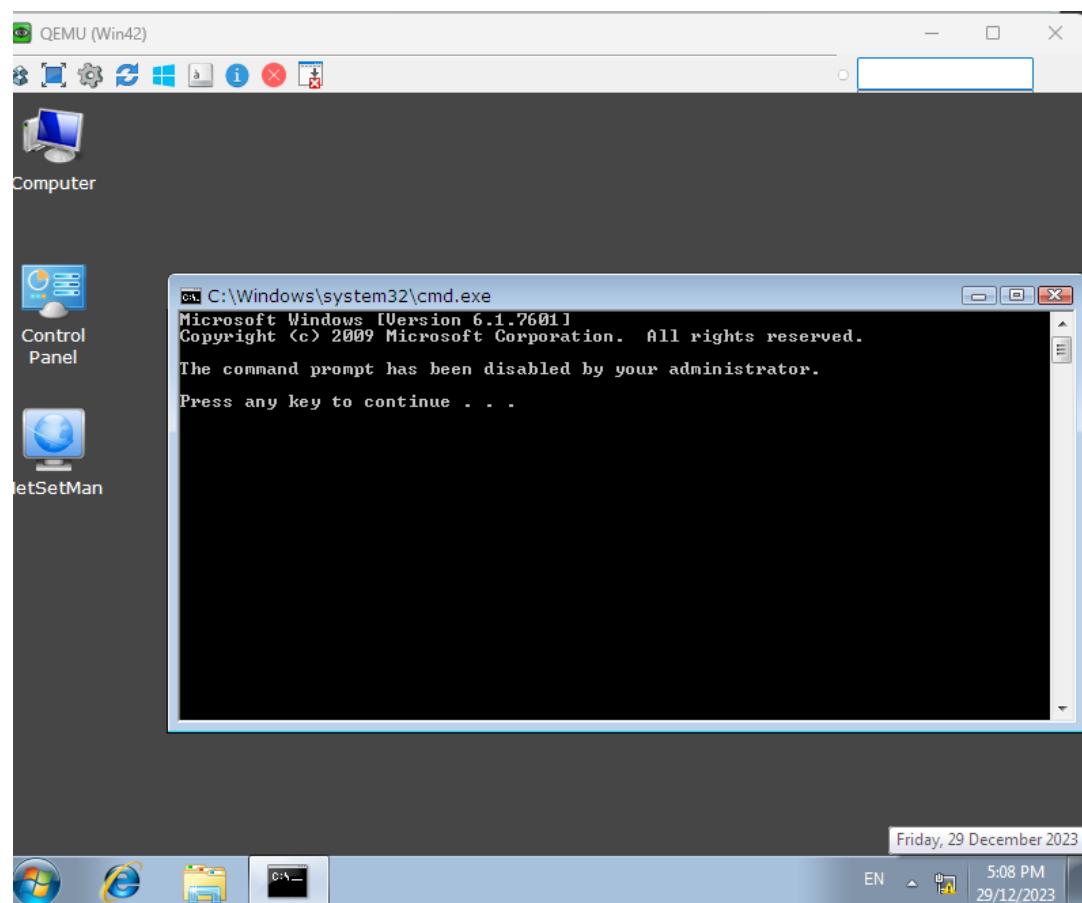
Hình 4.2.7m: Enabled mục Prevent access to the command prompt



Hình 4.2.7n: Enabled mục Don't run specified Windows applications

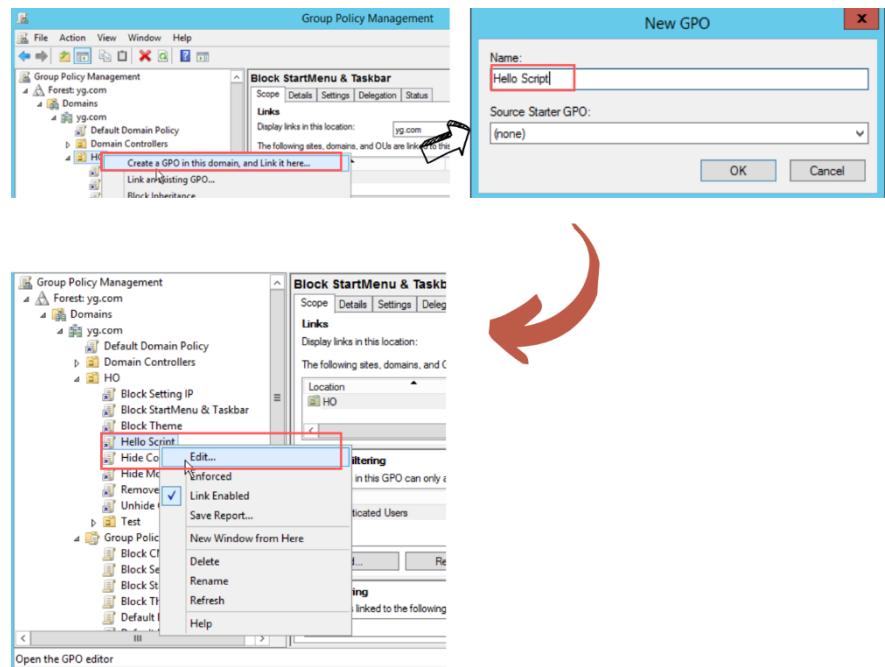


Hình 4.2.7o: Ở phần List of disallowed applications => Chọn Show và nhập ứng dụng không cho sử dụng

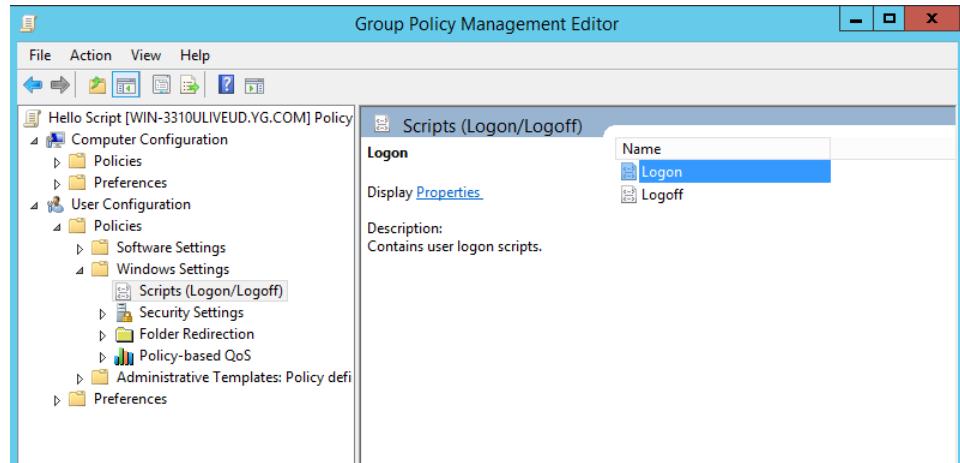


Hình 4.2.7p: CMD khi mở sẽ có thông báo như sau

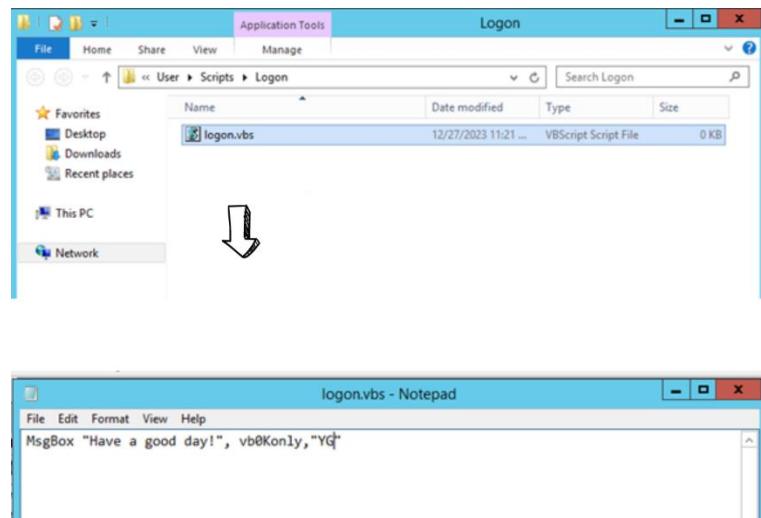
➡ **Hiển thị câu chào khi đăng nhập**



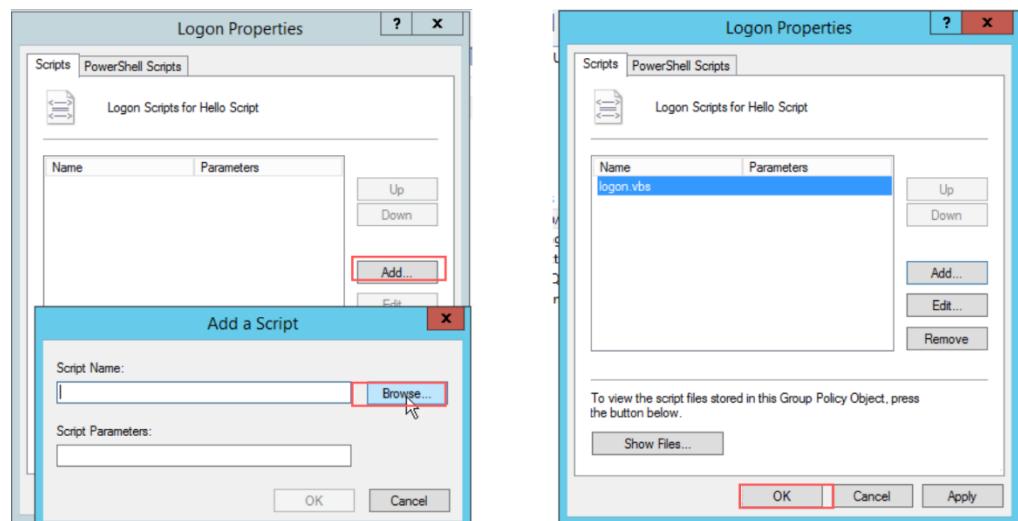
Hình 4.2.7q: Tạo GPO trong OU HO với tên “New Script” và chọn Edit



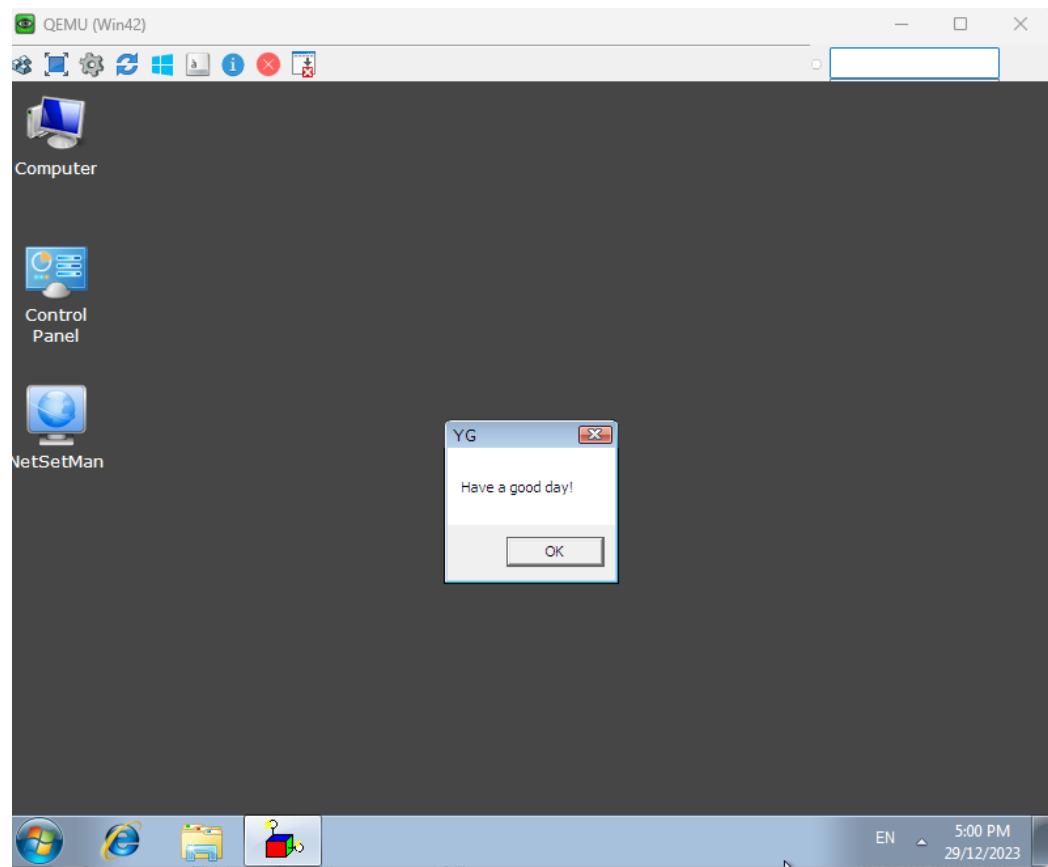
Hình 4.2.7r: Vào phần Windows Setting và chọn Logon



Hình 4.2.7s: Tạo một file logon.vbs và nhập nội dung như trên



Hình 4.2.7t: Add file vừa tạo vào logon



Hình 4.2.7u: Khi logon vào máy client sẽ hiển thị box chào như sau

### 4.3 NTFS

NTFS (New Technology File System), là một loại hệ thống tập tin đạt tiêu chuẩn cho hệ điều hành Windows NT.

Một số tính năng chính của NTFS:

- Khả năng hỗ trợ định dạng ổ đĩa lớn hơn 2GB
- Hỗ trợ mã hóa tệp
- Hỗ trợ kiểm soát truy cập tệp
- Hỗ trợ các tính năng bảo mật khác

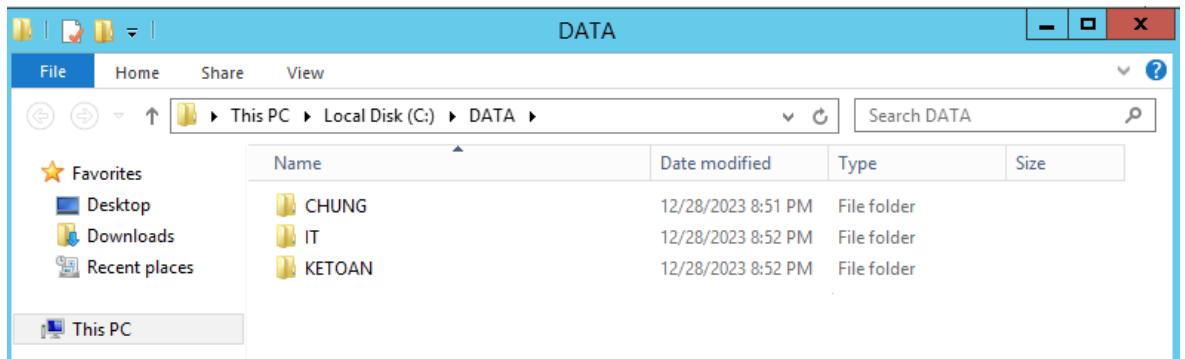
Bước đầu tiên chúng ta cần tạo cây thư mục trên máy chủ Windows:

C:\DATA

CHUNG

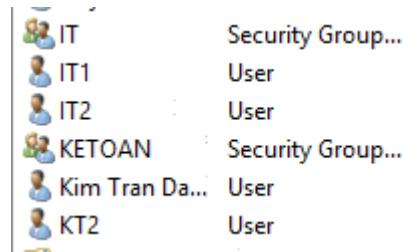
KETOAN

IT



Hình 4.3a: Tạo cây thư mục chứa data

Ở mỗi Group sẽ tạo thêm 2 user trong hai phòng ban



Hình 4.3b: Users trong các phòng ban

### **4.3.1 Phân quyền thư mục bằng Standard Permission**

Ở cây thư mục chúng ta sẽ có 3 file chứa data, trong đó:

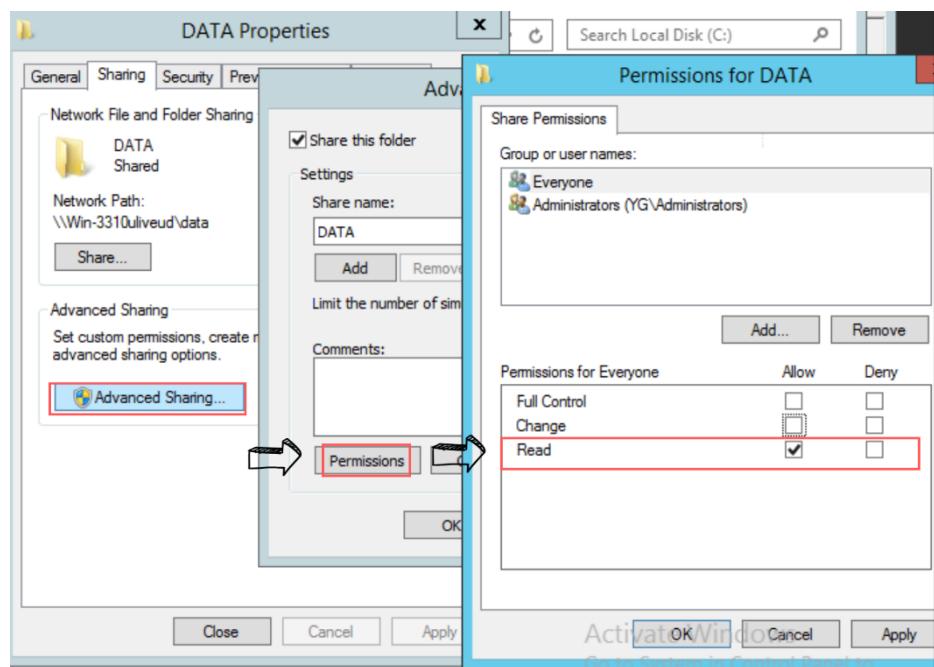
DATA: Cả hai phòng ban sẽ có quyền Read

CHUNG: Cả hai phòng ban sẽ có quyền Full

KETOAN: Phòng kế toán sẽ có quyền Full Group IT không có quyền

IT: Phòng IT có quyền Full, phòng kế toán không có quyền.

Thực hiện chia sẻ folder cho tất cả mọi người với quyền Read

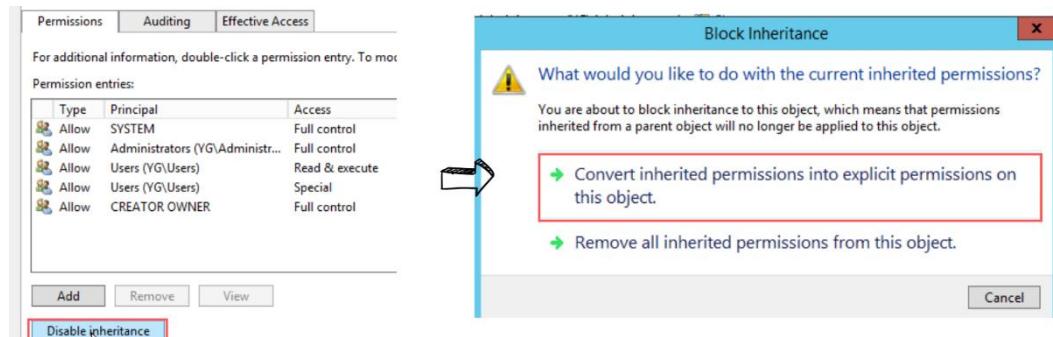


Hình 4.3.1a: Share folder DATA

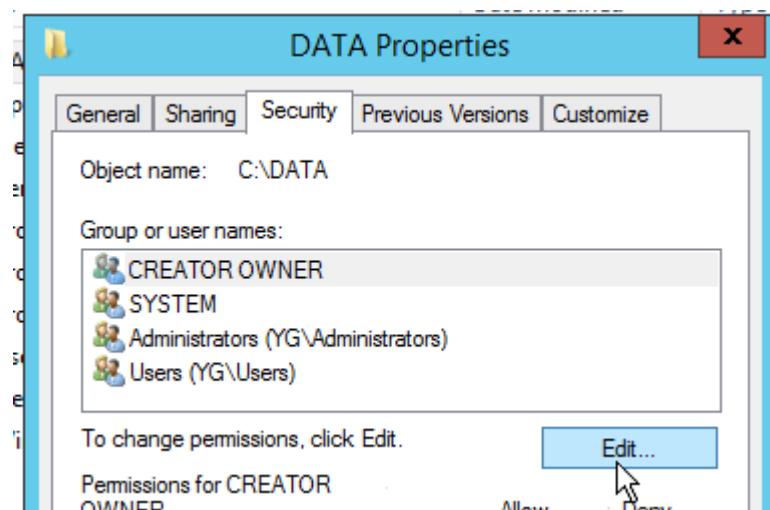
Màn hình Advanced

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (YG\Administrators)	Full control	C:\	This folder, subfolders and files
Allow	Users (YG\Users)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (YG\Users)	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

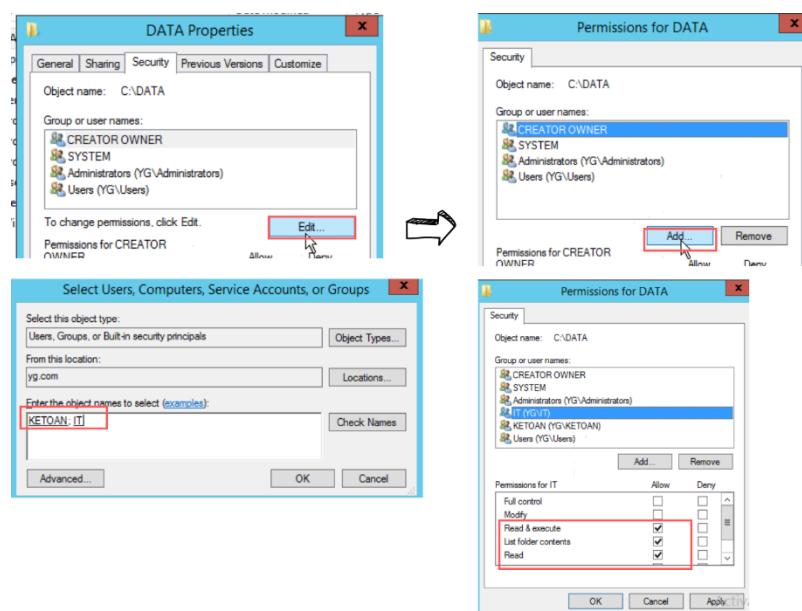
Hình 4.3.1b: Mở tab Advanced trên thư mục DATA



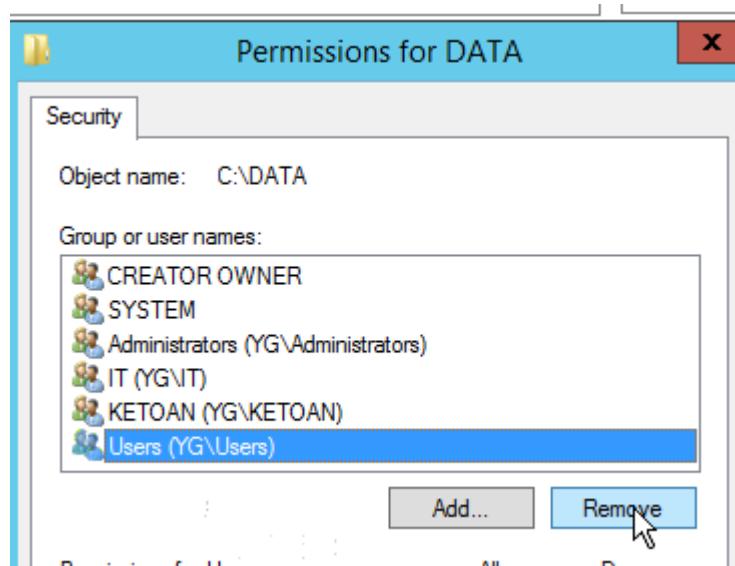
Hình 4.3.1c: Chọn Disable inheritance và chọn Convert inherited permission into explicit permission on this object



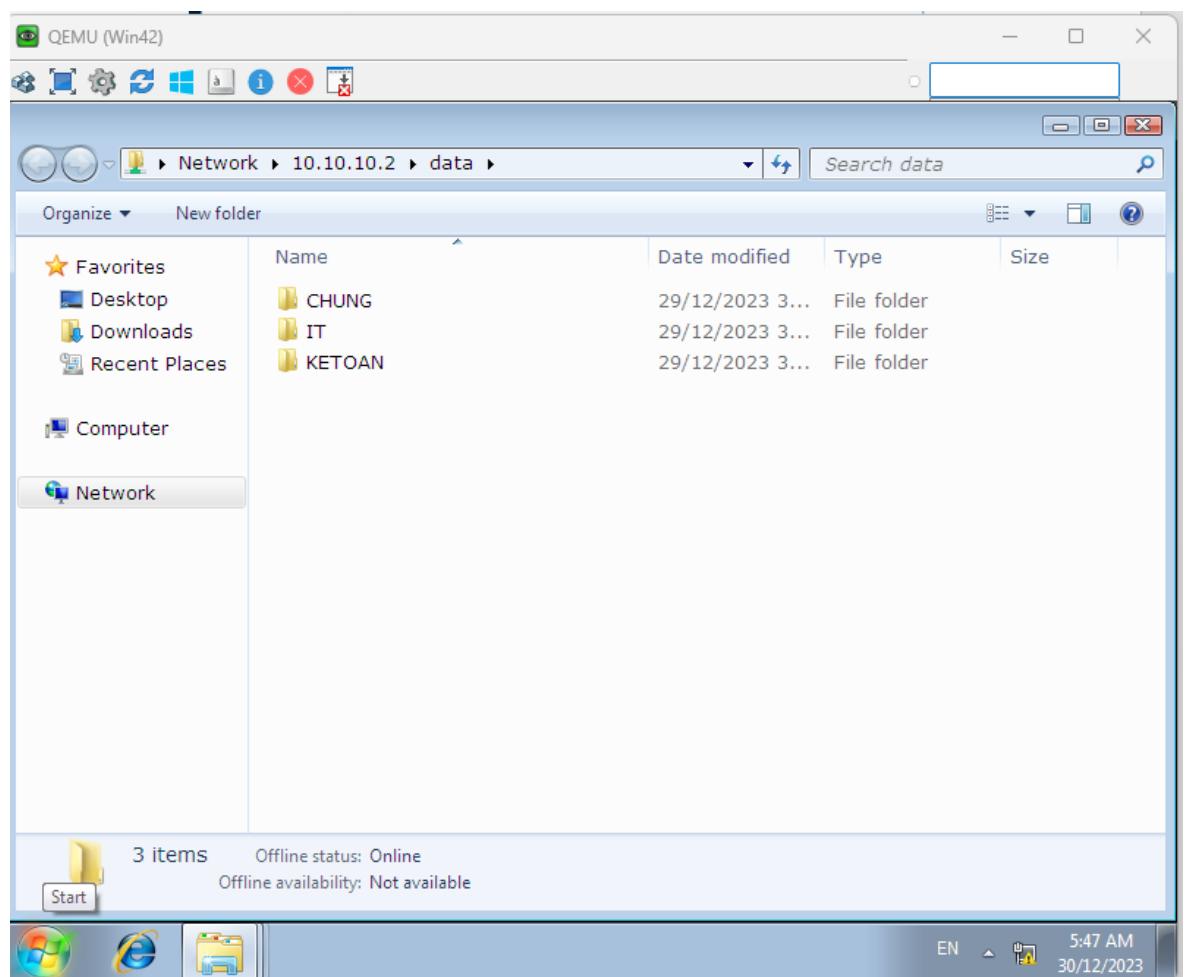
Hình 4.3.1d: Quay về cửa sổ Properties và chọn Edit



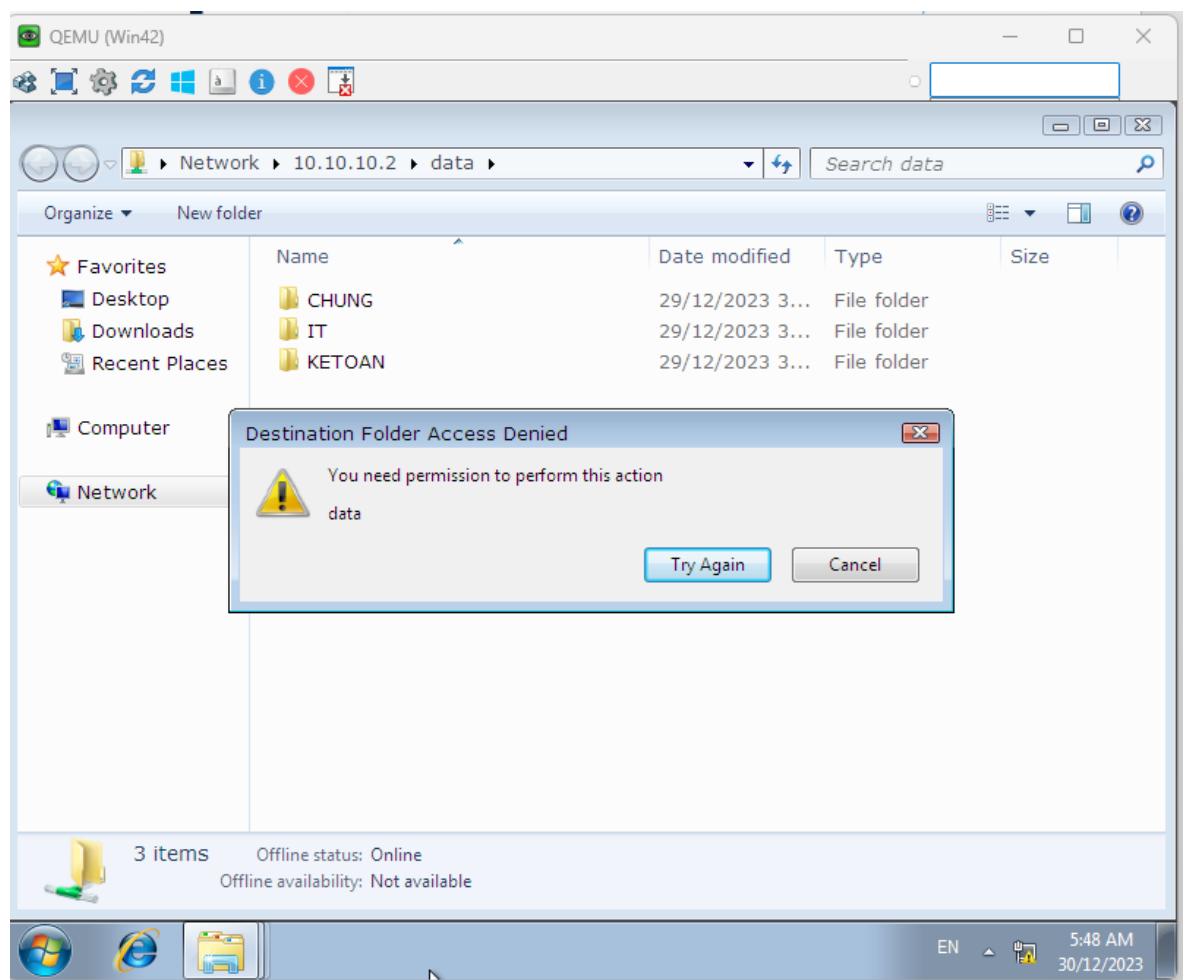
Hình 4.3.1e: Add quyền cho hai phòng ban trên



Hình 4.3.1f: Remove Group Users



Hình 4.3.1g: Các máy client truy cập thành công vào mục DATA



Hình 4.3.1h: Máy client tạo một folder bất kỳ và bị lỗi

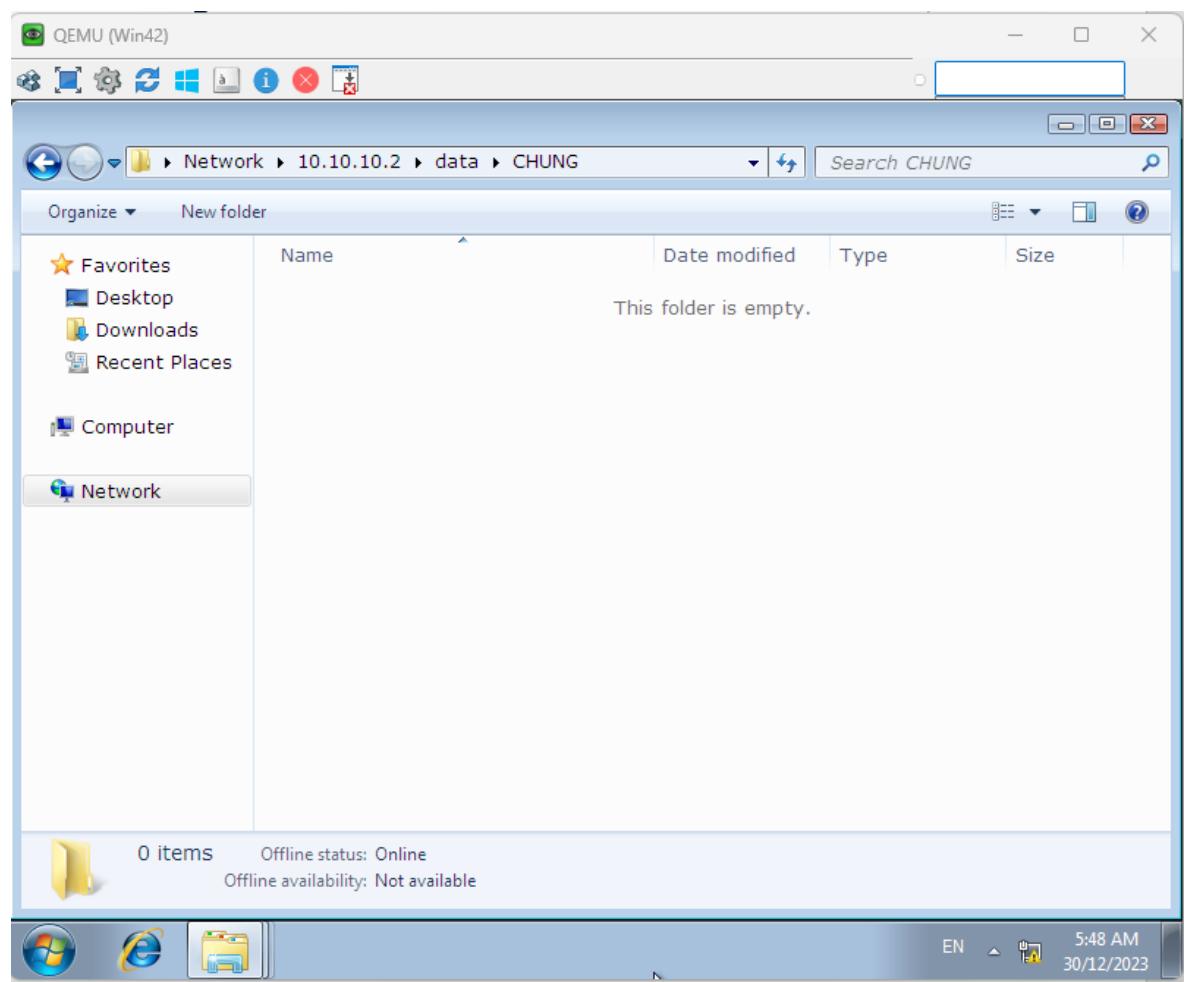
### Phân quyền thư mục CHUNG

Group or user names:	Permissions for IT	Permissions for KETOAN
Everyone, SYSTEM	Allow: Full control, Modify	Allow: Full control, Modify, Read & execute
IT (YGVIT), KETOAN (YG\KETOAN)	Allow: Full control, Modify	Allow: Full control
Administrator, Administrators (YG\Administrators)		

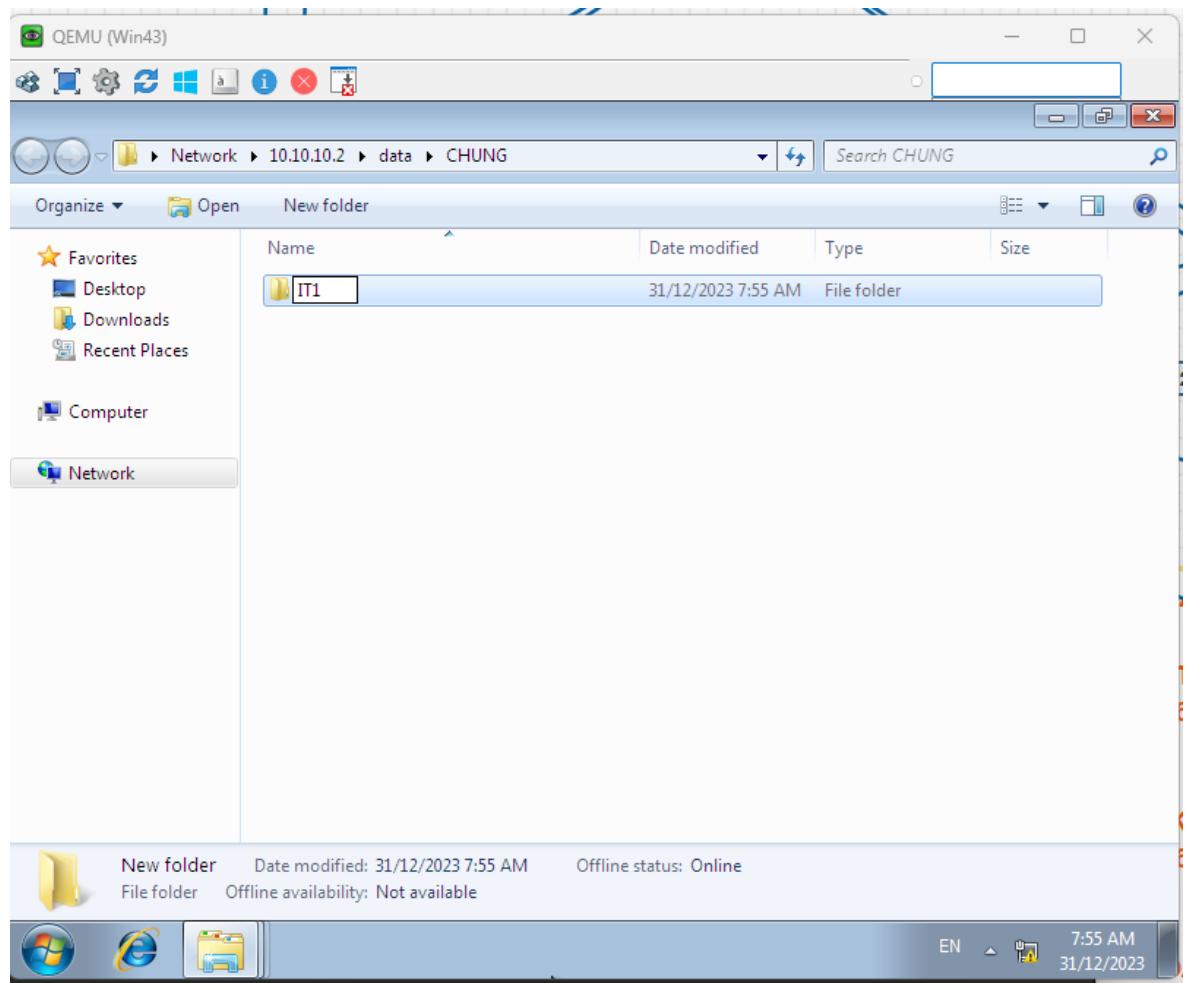
  

Group or user names:	Permissions for KETOAN
KETOAN (YG\KETOAN)	Allow: Full control

Hình 4.3.1i: Phân quyền Full Control cho hai phòng ban



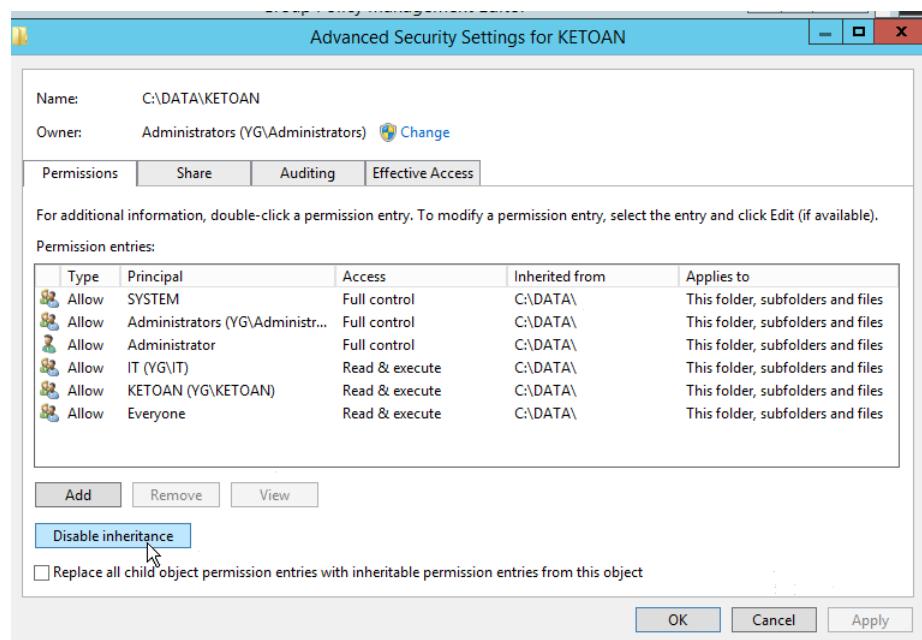
Hình 4.3.1j: Các máy ở hai phòng ban truy cập thành công vào folder CHUNG



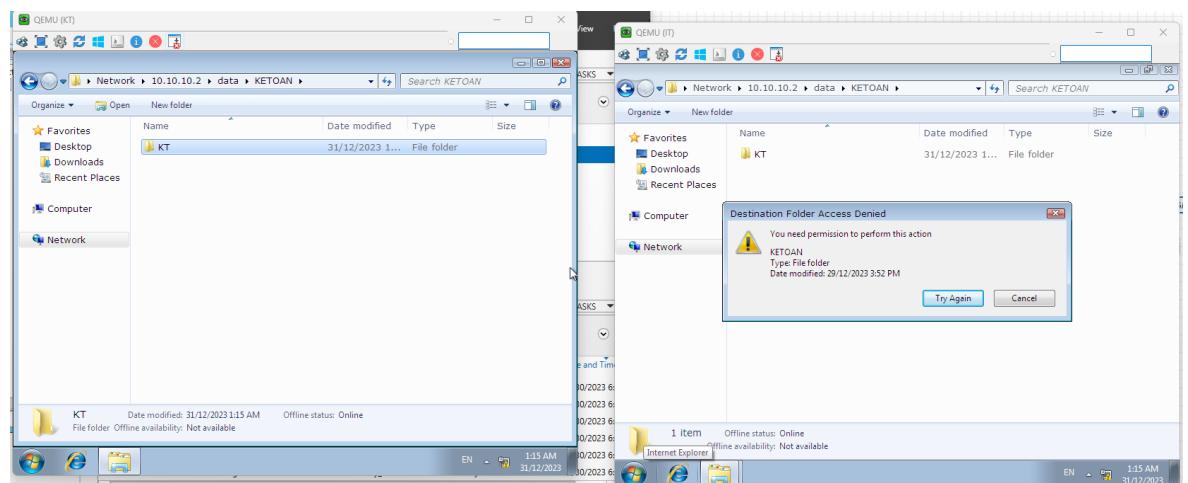
Hình 4.3.1k: Các máy ở hai phòng ban có thể tạo và xóa folder bất kỳ trong mục CHUNG

#### Phân quyền cho thư mục KETOAN

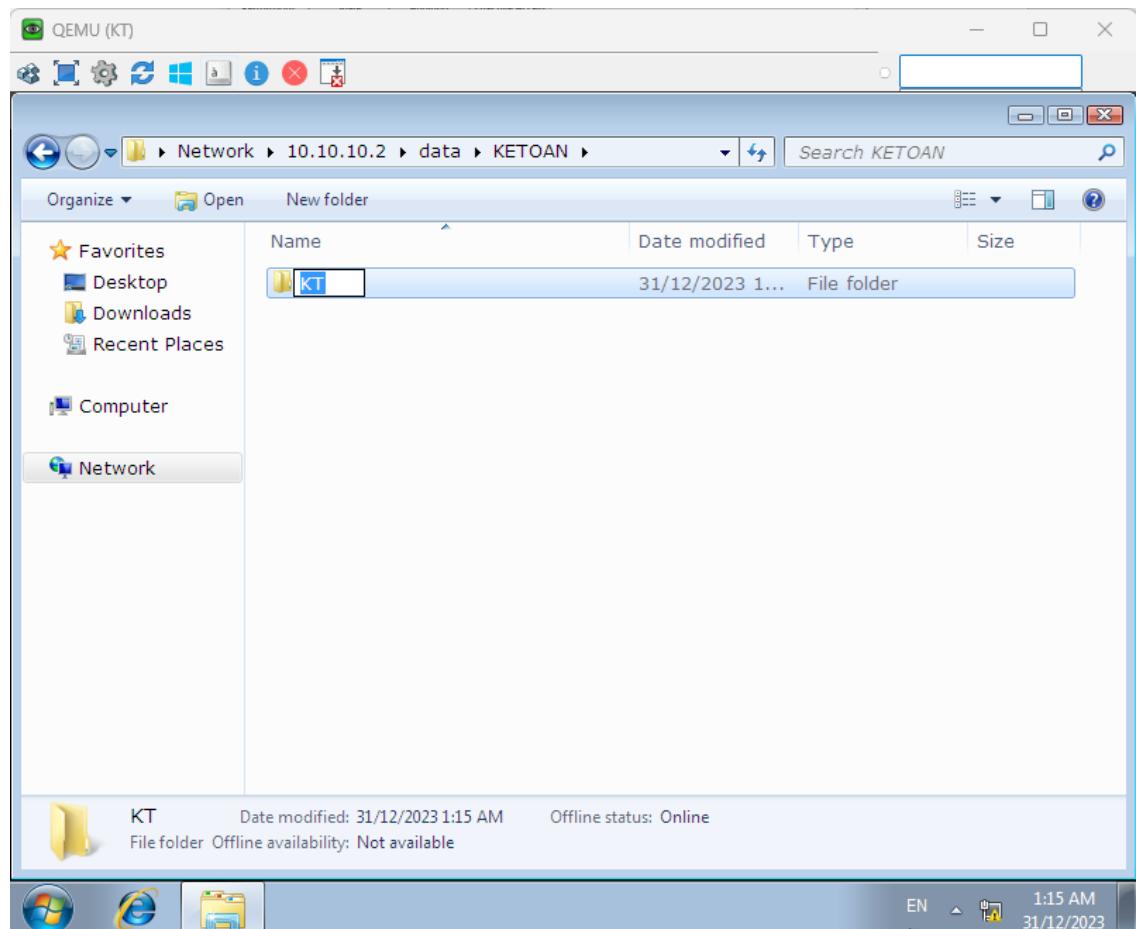
Tương tự vào mục Properties của thư mục KETOAN và đến phần Permission



Hình 4.3.1l: Gỡ bỏ kế thừa



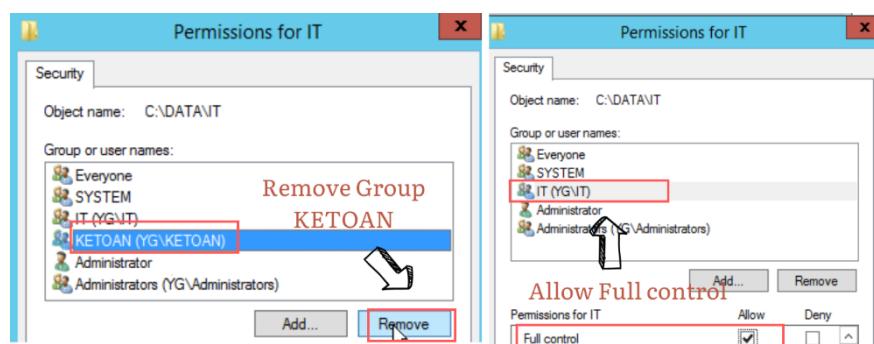
Hình 4.3.1m: Phòng Kế toán truy cập được còn IT không truy cập được



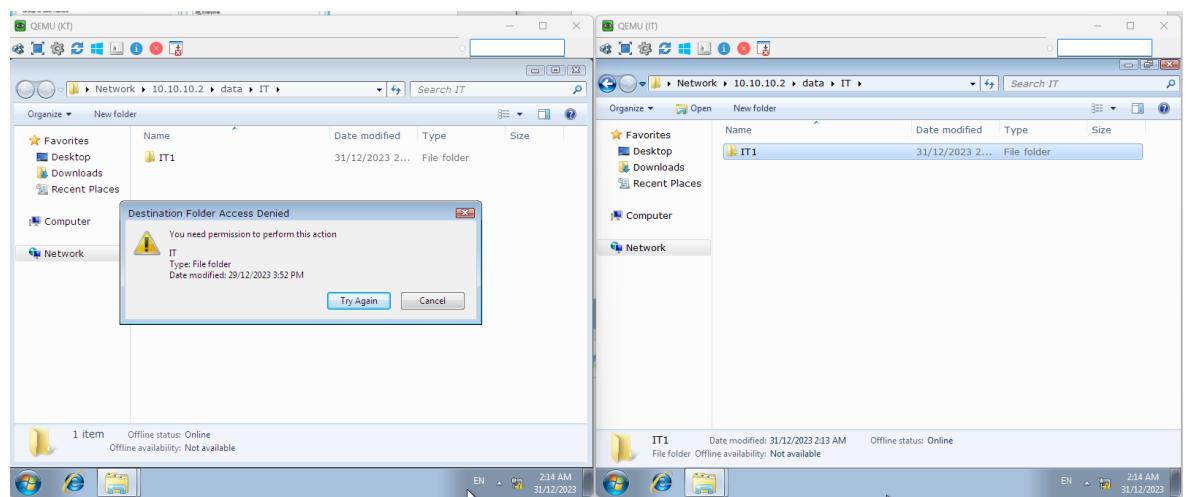
Hình 4.3.1n: Máy phòng Kế toán có thể tạo xóa file bất kỳ trong folder KETOAN

#### Phân quyền cho thư mục IT

Tương tự các bước như phân quyền ở mục KETOAN



Hình 4.3.1o: Xóa Group KETOAN và phân quyền cho Group IT

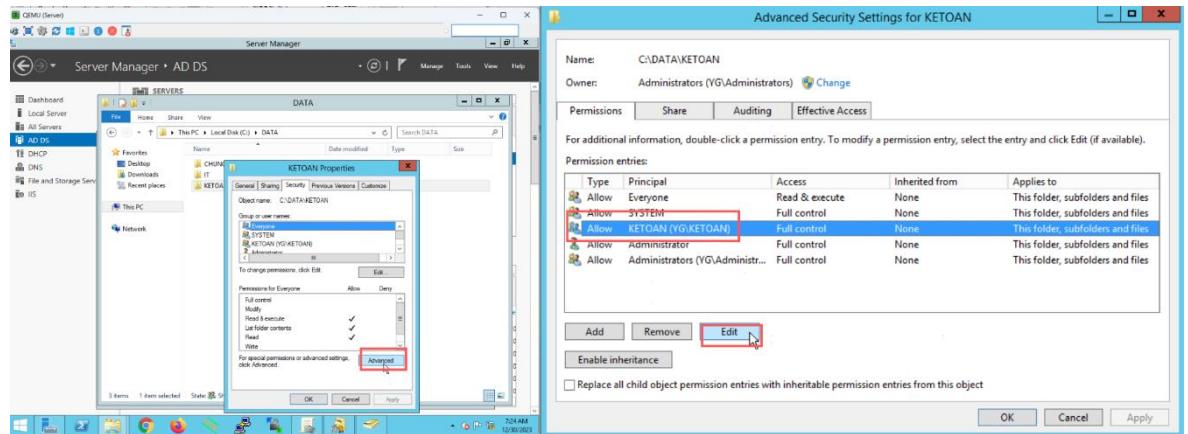


Hình 4.3.1p: Phòng IT truy cập được còn Kế toán không truy cập được

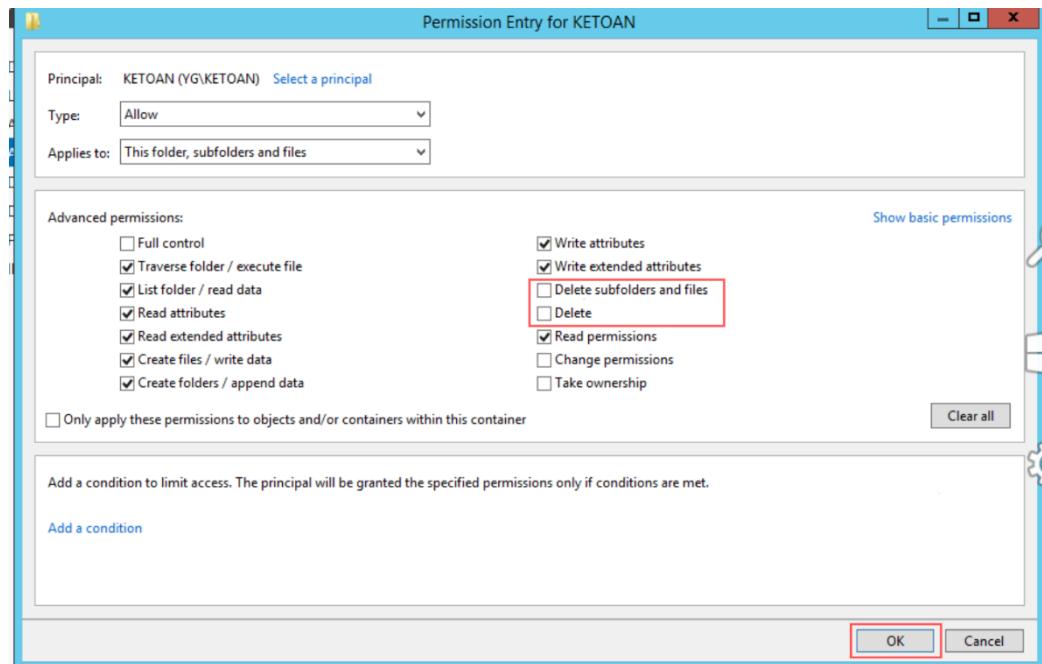
### 4.3.2 Phân quyền thư mục bằng Special Permission

Phân quyền theo yêu cầu: File do User nào tạo ra thì chỉ User đó mới xóa được

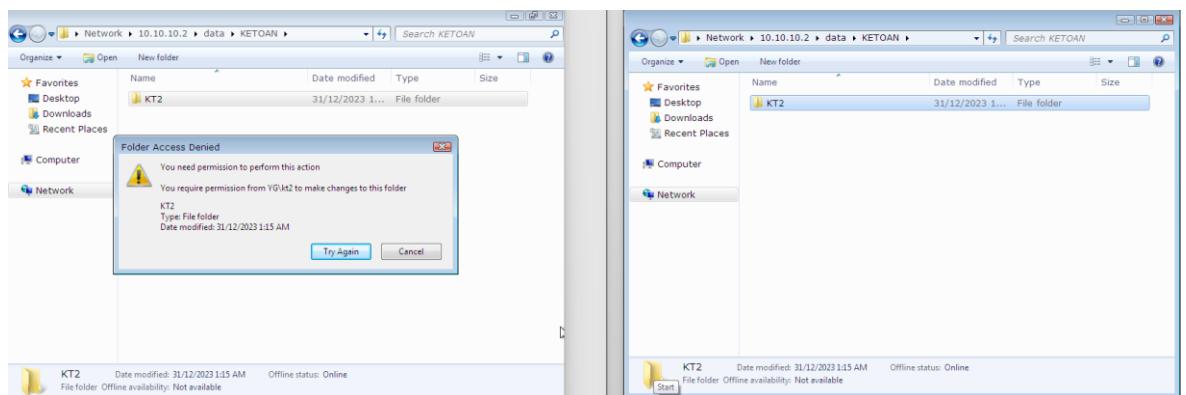
Vào mục Permission của folder KETOAN và chọn Edit



Hình 4.3.2a: Trong cửa sổ Permission Entry for KeToan, nhấn vào liên kết Show advanced permissions



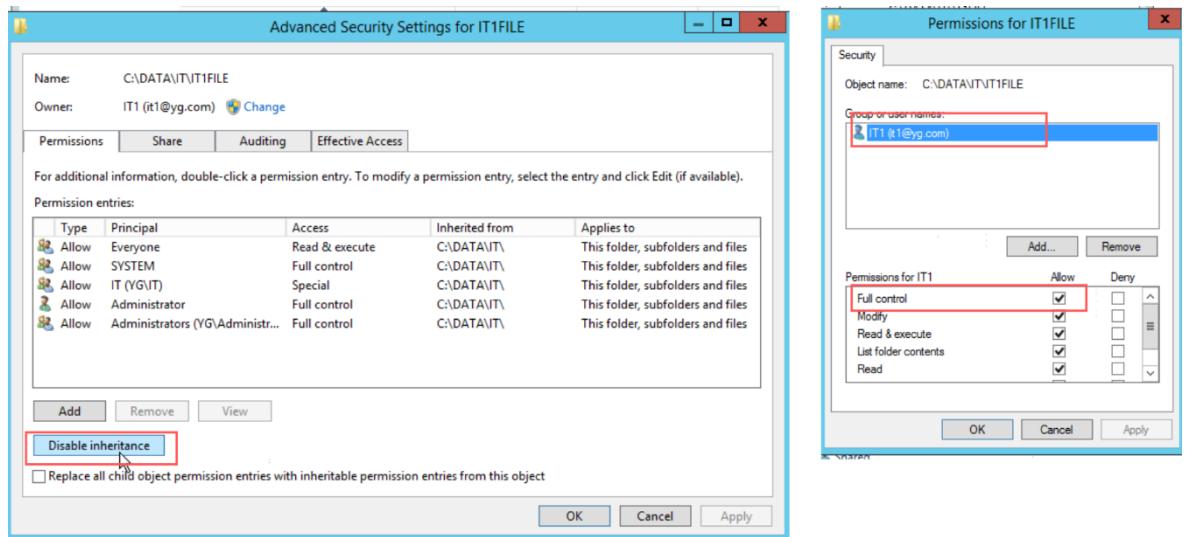
Hình 4.3.2b: Ở mục Allow, tắt dấu chọn ở ô Delete subfolders and files và Delete  
=> Chọn OK 4 lần



Hình 4.3.2c: Máy KT2 tạo file và KT1 xóa file sẽ bị báo lỗi

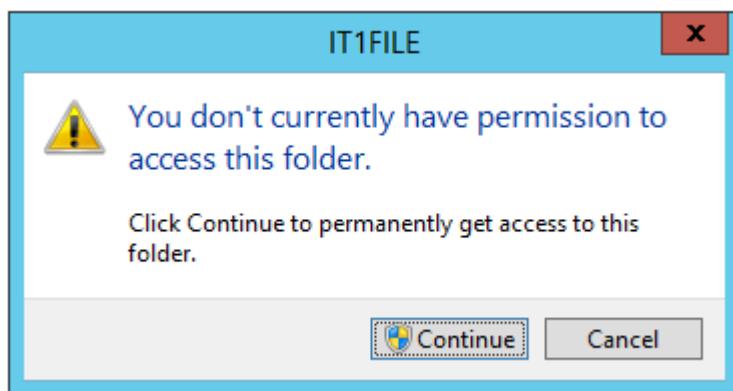
### 4.3.3 Take Ownership

Vào máy IT và truy cập vào folder IT, sau đó tạo thêm một folder IT1FILE

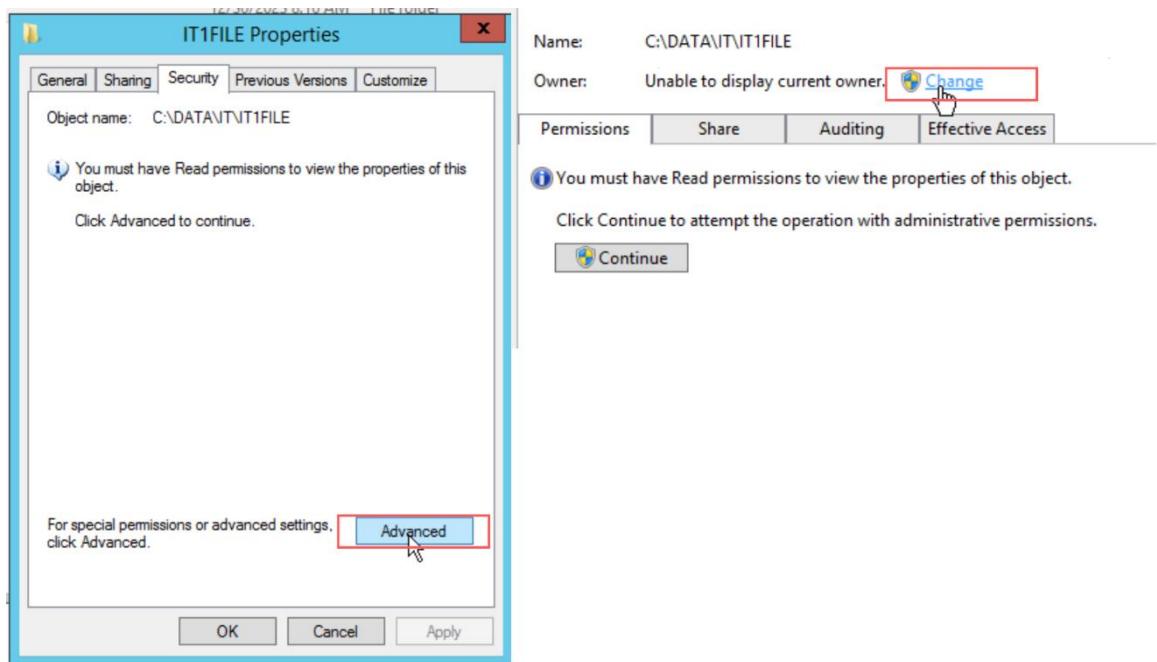


Hình 4.3.3a: Phân quyền cho IT1FILE

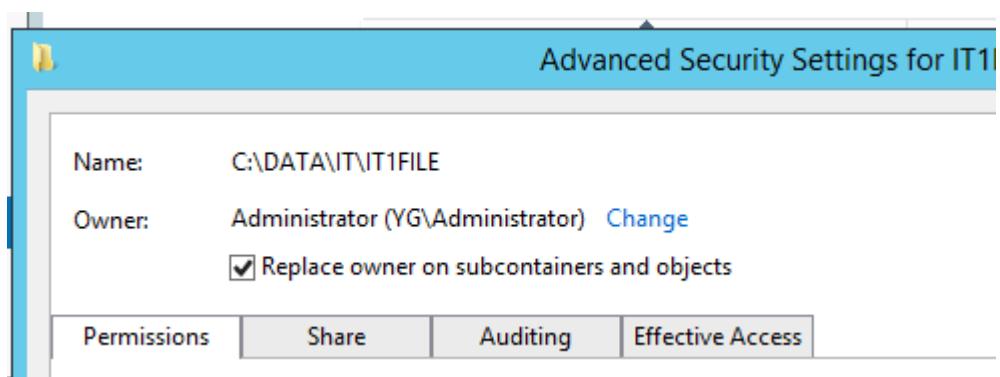
Logon vào Administrator và truy cập vào folder IT1FILE bị báo lỗi không thể  
truy cập được



Hình 4.3.3b: Không thể truy cập được folder IT1FILE



Hình 4.3.3c: Truy cập vào Properties của folder IT1FILE



Hình 4.3.3d: Replace owner on subcontainers and object trên file IT1FILE



Hình 4.3.3e: Administrator đã có quyền Full Control

## CHƯƠNG 5. KẾT LUẬN

### 5.1 Kết luận

Mô hình mạng doanh nghiệp sau khi được hoàn thiện dựa vào các kiến thức của MCSA để có thể quản trị hệ thống. Bằng cách áp dụng các Group Policy Management, NTFS, các chính sách và các rules chủ yếu cần có trong doanh nghiệp đã được triển khai, góp phần ngăn chặn các truy cập trái phép, bảo vệ dữ liệu quan trọng của doanh nghiệp. Ngoài ra việc triển khai các dịch vụ cơ bản như DNS, DHCP, Active Directory Domain, NTP,... đã góp phần giúp cho hệ thống hoạt động trơn tru và hiệu quả hơn.

### 5.2 Hướng phát triển

Hệ thống mạng hiện tại vẫn còn một số nhược điểm do hạn chế về tài nguyên để triển khai, khiến cho một số dịch vụ không đủ bộ nhớ để có thể thực hiện. Nếu có cơ hội, em sẽ phát triển thêm một số tính năng để nâng cao hiệu suất và sự linh hoạt của hệ thống chẳng hạn như sử dụng Windows Deployment Service để cài đặt hệ điều hành cho các máy client thông qua máy chủ DHCP. Điều này sẽ giúp giảm nhiều thời gian và công sức cài đặt hệ điều hành thủ công cho từng máy. Ngoài ra, em cũng sẽ triển khai Deploy Software để cài đặt các ứng dụng tự động cho người dùng hoặc máy tính thông qua chính sách GPO. Điều này sẽ giúp đảm bảo rằng tất cả các máy tính đều có các ứng dụng cần thiết và được cập nhật phiên bản mới nhất. Cuối cùng, em sẽ tìm hiểu thêm về việc triển khai cân bằng tải cho dịch vụ Web và File. Điều này sẽ giúp cải thiện hiệu suất và độ tin cậy của hệ thống khi có nhiều người dùng truy cập hoặc xảy ra sự cố.

## TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Hoàng, L. B. (2017, April 1). Hướng dẫn cài đặt DNS trên Windows Server 2012. sinhvientot.net. <https://sinhvientot.net/huong-dan-cai-dat-dns-tren-windows-server-2012/>

[2] Phong T. (2020, June 24). Hướng dẫn cài đặt DHCP Role trong Windows Server 2012. Quantrimang.com. <https://quanzimang.com/cong-nghe/huong-dan-cai-dat-dhcp-role-trong-windows-server-2012-154329>

[3] TopDev, & TopDev. (2021, November 18). Cài đặt FTP Server trên Windows Server. TopDev. <https://topdev.vn/blog/cai-dat-ftp-server-tren-windows-server/>

[4] Anh, T. T. (2022, September 28). [Tự học MCSA MCSE 2016]-Lab 14-Cấu hình IIS Web Server trên Windows Server 2016 - ITFORVN. ITFORVN. <https://itforvn.com/tu-hoc-mcsa-mcse-2016-lab-14-cau-hinh-iis-web-server-tren-windows-server-2016/>